

医療情報システム向け AWS 利用リファレンス (経済産業省版)

2018 年 8 月 22 日
V1.00

キヤノン IT ソリューションズ株式会社
DXC テクノロジー・ジャパン株式会社
日本電気株式会社
株式会社日立システムズ
フィラーシステムズ株式会社

ご注意：下記の利用許諾契約書（以下「本規約」という。）をご確認ください。本規約に同意できない場合、本件ドキュメントを利用することはできません。本件ドキュメントを利用した場合、本規約に同意したものとみなされます。

利用許諾契約書

第1条（定義）

1. 「本件ドキュメント」とは、キャノンITソリューションズ株式会社、DXCテクノロジー・ジャパン株式会社、日本電気株式会社、株式会社日立システムズ、フィラーシステムズ株式会社（総称して以下「当社」という。）を提供元とする「医療情報システム向けAWS利用リファレンス」を意味します。
2. 「利用」とは、本件ドキュメントの全部または一部を使用し、複製（本件ドキュメントのダウンロードを含む。）し、改変し、翻案すること、及び本件ドキュメントを改変および翻案した本件ドキュメントについて前記の行為を行うことを意味します。
3. 「ユーザ」とは、本件ドキュメントの利用者または、利用者が所属する法人等の団体の義務のために本件ドキュメントを利用する場合には、当該法人等の団体を意味します。

第2条（本件ドキュメントの利用）

当社は、ユーザが本規約を遵守することを条件として、ユーザに対し、本件ドキュメントを利用するための非独占的権利を許諾します。

第3条（変更）

1. 当社は、ユーザの事前の承諾を得ることなく、必要に応じて本規約および本件ドキュメントを随時変更することができるものとします。なお、当該変更については、当社が別途定める場合を除き、当社が本サイト上に掲載した時点から効力を生じるものとします。本規約の変更後においてユーザが本件ドキュメントを利用することをもって、ユーザが本規約の変更同意したものとみなされます。
2. ユーザは、本規約および本件ドキュメントの内容が前項の規定のとおり変更される可能性のあることを認識し、本件ドキュメントの利用にあたっては、最新版を利用するものとします。

第4条（保証及び責任）

当社は、本件ドキュメントを現状有姿にてユーザに提供し、利用を許諾するものであり、本件ドキュメントに瑕疵が存在しないこと、本件ドキュメントが第三者の権利を侵害していないこと、および本件ドキュメントの機能がユーザの要求を満たすものであることを含め、明示的であると黙示的であるとを問わず一切保証しないものとし、本件ドキュメントの利用に付随または関連してユーザに生じたいかなる損害に対しても一切責任を負わないものとします。また、本件ドキュメントの評価、業務への適用、改変、翻案その他の利用については、ユーザがすべての責任を負うものとします。

第5条（知的財産権）

ユーザは、本件ドキュメントが当社または当社のライセンサーの財産であり、かつその一切の知的財産権は当社または当社のライセンサーに帰属していることを了解します。

第6条（契約期間）

1. 本規約は、ユーザが、本件ドキュメントの利用を開始した時点で発効し、本条第2項または第3項、第7条第2項により終了されるまで有効に存続します。
2. ユーザは、本件ドキュメント及びその複製物のすべてを廃棄及び消去することにより、本規約を終了させることがで

きます。

3. ユーザが本規約のいずれかの条項に違反した場合、本規約は直ちに終了します。

また、当該違反により当社に損害が発生した場合、当社はユーザに対し損害賠償請求をすることができます。

4. ユーザは、前項または第7条第2項によって本規約が終了した場合、速やかに、本件ドキュメント及びその複製物のすべてを廃棄または消去するものとします。

第7条（反社会的勢力との取引等の禁止）

1. ユーザは、自己（役員を含む）が反社会的勢力（暴力団を含むがこれに限らず、また団体、個人を問わない）の関係者に該当しないことをここに表明するものとし、また、当該関係者と取引し、または交際しないことを約するものとします。
2. 当社は、ユーザが前項に違反し、またはそのおそれがある場合には、何らの催告なく、直ちに本規約を終了させることができるものとします。

第8条（合意管轄）

本規約は、効力、解釈および履行を含む全ての事項について、日本国法に準拠するものとし、本規約に関し、訴訟の必要が生じた場合には、東京地方裁判所を第一審の専属的合意管轄裁判所とします。

付則

本規約は2018年8月22日から施行されます。

2018年8月22日制定

3 本ガイドラインの対象システム及び対象情報

3.1 電子媒体の選択についての考慮事項

■ 要求事項 1

必須

長期保存を目的として、これらの電子媒体を利用する場合には、製造元の保存仕様に準拠した保管を行い、見読性、保存性を損なわないように配慮すること。また電子媒体の劣化特性を考慮して、劣化が起こる前に新たな電子媒体に複写すること。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的风险アセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この

集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することになります。AWS のお客様

は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

インスタンスのリタイア

インスタンスをホストしている基盤のハードウェアで回復不可能な障害が検出されると、AWS によってインスタンスのリタイアが予定されます。予定されたリタイア日になると、インスタンスは AWS によって停止または削除されます。インスタンスのルートデバイスが Amazon EBS ボリュームである場合、インスタンスは停止されますが、その後いつでも再び起動できます。停止したインスタンスを開始すると、新しいハードウェアに移行されます。インスタンスのルートデバイスがインスタンスストアボリュームである場合、インスタンスは終了し、再び使用することはできません。

リタイアが予定されているインスタンスの特定

インスタンスのリタイアが予定された場合、イベントの前に、当該のインスタンス ID とリタイア日を記載したメールが送信されます。このメールは、アカウントに関連付けられているアドレスに送信されます。これは、AWS マネジメントコンソール へのログインに使用するメールアドレスと同じです。定期的に確認しないメールアドレスを使用している場合は、Amazon EC2 コンソールまたはコマンドラインを使用して、いずれかのインスタンスにリタイアが予定されているかどうかを判断できます。アカウントの連絡先情報を更新するには、[Account Settings] ページに移動します。

詳細および最新情報は以下 URL を参照ください。

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/instance-retirement.html

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーク環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの中には、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認

証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のお客様は、コンテンツを保存する物理的リージョンを指定できます。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しません。使用できるリージョンの完全なリストについては、AWS グローバルインフラストラクチャーのページを参照してください。

AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているため、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPsec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (<https://aws.amazon.com/kms/> を参照)。詳細については、AWS クラウドセキュリティホワイトペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 および Glacier サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。 <https://aws.amazon.com/jp/s3/faqs/>

HW 劣化等で交換が必要な際は Retirement Notice で情報処理事業者に事前に通知されます。そのため、情報処理事業者は事前に劣化が起こる前に新たな電子媒体への複写の対応が可能です。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

A.17.2.1

3 本ガイドラインの対象システム及び対象情報

3.1 電子媒体の選択についての考慮事項

■ 要求事項 2

必須

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同等に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の (AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効

です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内

で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud

(VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のお客様は、コンテンツを保存する物理的リージョンを指定できます。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しません。使用できるリージョンの完全なリストについては、AWS グローバルインフラストラクチャーのページを参照してください。

AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているため、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPsec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (<https://aws.amazon.com/kms/> を参照)。詳細については、AWS クラウドセキュリティホワイトペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 および Glacier サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長

化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。<https://aws.amazon.com/jp/s3/faqs/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

A.17.2.1

3 本ガイドラインの対象システム及び対象情報

3.1 電子媒体の選択についての考慮事項

■ 要求事項 3

必須

医療情報を格納する電子媒体として、小型半導体メモリの有益性は認められるものの、漏洩等の大きなリスクも考えられることから、原則として医療情報システムでは外部デバイスとして小型半導体メモリの使用を行うことができないよう配慮することが望ましい。必要により使用する場合、使用前には不要なデータが書き込まれていないことを確認し、使用後には電子媒体上の全てのデータを削除すること。また、利用時間及び電子媒体の移動範囲を最小にするなどの管理を行うこと。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この

責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、

イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS のお客様は、コンテンツを保存する物理的リージョンを指定できます。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しません。使用できるリージョンの完全なリストについては、AWS グローバルインフラストラクチャーのページを参照してください。

AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているので、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを

許可しています。VPC への IPSec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (<https://aws.amazon.com/kms/> を参照)。詳細については、AWS クラウドセキュリティホワイトペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 および Glacier サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。 <https://aws.amazon.com/jp/s3/faqs/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

3 本ガイドラインの対象システム及び対象情報

3.2 ネットワーク利用上の考慮事項

■ 要求事項 4

必須

保管のためのデータ移動等、ネットワーク経由での情報管理機能を提供する場合には、医療機関等と情報処理事業者側設備をつなぐネットワーク部分に適切な安全管理措置を施す必要がある。この際、安全面への配慮からは専用線と同等の回線を用いるべきである。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしていま

す。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲

の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク（VPN）接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション（CRR）は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン（AZ）のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データバ

ースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの中には、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

責任共有モデルに従って、AWS は、データセンターネットワーク、ルーター、スイッチ、ファイアウォールのようなインフラストラクチャーコンポーネントを安全な方法で設定します。クラウドでシステムに対するアクセスを制御する責任、Amazon VPC 内のネットワークセキュリティおよび安全なインバウンド/アウトバウンドネットワークトラフィックを設定する責任はお客様にあります。

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワーク体験を提供できます。

AWS Direct Connect では、お客様のネットワークと AWS Direct Connect のいずれかのロケーション間に専用のネットワーク接続を確立できます。業界標準の 802.1q VLAN を使用して、この専用接続を複数の仮想インターフェースに分割することができます。このようにすると、同じ接続を使用して、パブリックリソース（例えば Amazon S3 に格納されたオブジェクト）にはパブリック IP アドレススペースを使用してアクセスし、プライベートリソース（例えば Amazon Virtual Private Cloud (VPC) 内で実行されている Amazon EC2 インスタンス）にはプライベート IP スペースを使用してアクセスすることができるので、パブリック環境とプライベート環境の間でネットワークを分離できます。仮想インターフェースは、ニーズの変化に合わせていつでも再構成できます。

<https://aws.amazon.com/jp/directconnect/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.4

A.12.6

A.13 通信のセキュリティ

A.13.1
A.13.1.1
A.13.1.2
A.13.1.3
A.13.2
A.13.2.1
A.13.2.2
A.13.2.3
A.13.2.4

A.16 情報セキュリティインシデント管理

A.16.1.1
A.16.1.2
A.16.1.3
A.16.1.4
A.16.1.5
A.16.1.6
A.16.1.7
A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.2 ネットワーク利用上の考慮事項

■ 要求事項 5

必須

一般に専用線は利用コストが高価であることから、公衆回線上に仮想の閉域網を構築する技術等を採用することも検討対象と考えることができる。しかし、運用を適切に行うことで十分な安全性を確保することは可能であり、これまでに例として上げた種類の回線と比べて回線コストが格段に安いというメリットもあることから、適切に運用すること及び医療機関等の合意を得ることを前提として、IPsecIPsec に IKE を組み合わせ、自動鍵更新を行う設定にて、オープンなネットワーク上の VPN を採用することも可能とする。ただし、インターネットからの第三者による不正なアクセスを防止するため、医療機関等の機器と情報処理事業者側の機器において、ネットワーク境界のファイアウォールまたは VPN 装置等により、適切なアクセス制御を行うこと（「3.5.2 ネットワーク利用上の考慮事項」を参照）。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしていま

す。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲

の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク（VPN）接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション（CRR）は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン（AZ）のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データバ

ースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

責任共有モデルに従って、AWS は、データセンターネットワーク、ルーター、スイッチ、ファイアウォールのようなインフラストラクチャーコンポーネントを安全な方法で設定します。クラウドでシステムに対するアクセスを制御する責任、Amazon VPC 内のネットワークセキュリティおよび安全なインバウンド/アウトバウンドネットワークトラフィックを設定する責任はお客様にあります。

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。独自の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全にコントロールできます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。例えば、インターネットへのアクセスがあるウェブサーバーのパブリックサブネットを作成し、データベースやアプリケーションサーバーなどのバックエンドシステムをインターネットへのアクセスがないプライベートサブネットに配置できます。セキュリティグループやネットワークアクセスコントロールリストなどの複数のセキュリティレイヤーを活用し、各サブネットの Amazon EC2 インスタンスへのアクセスをコントロールすることができます。加えて、既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。

<https://aws.amazon.com/jp/vpc/>

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpn-connections.html

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_VPN.html

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.4

A.12.6

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.2 ネットワーク利用上の考慮事項

■ 要求事項 6

必須

いずれの種別の回線であっても、通信ログ及び通信状況を監視し、異常が発生した場合には迅速に対処すること。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の

様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）

または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーク環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク（VPN）接続を作成することができるので、AWS クラウドを既存のデータセンター

を拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

責任共有モデルに従って、AWS は、データセンターネットワーク、ルーター、スイッチ、ファイアウォールのようなインフラストラクチャーコンポーネントを安全な方法で設定します。クラウドでシステムに対するアクセスを制御する責任、Amazon VPC 内のネットワークセキュリティおよび安全なインバウンド/アウトバウンドネットワークトラフィックを設定する責任はお客様にあります。

Amazon CloudWatch を使用した監視を活用可能です。

https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/vpn-metricscollected.html

https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/monitoring-cloudwatch.html

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.4

A.12.6

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.16 情報セキュリティインシデント管理

A.16.1.1
A.16.1.2
A.16.1.3
A.16.1.4
A.16.1.5
A.16.1.6
A.16.1.7
A.16.1.8

3 本ガイドラインの対象システム及び対象情報

■ 要求事項 7

必須

医療情報を CD、DVD、MO 等の電子媒体を利用して情報処理事業者の施設に保存する場合の一連の手順医療機関等の医療従事者の作業手順、情報処理事業者の作業手順などを考慮し、電子媒体の交換手順について医療事業者と合意し、手順書として双方で管理すること。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフ

フレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会 (AICPA) のトラスト・サービスの原則 (Trust Services Principles)、PCI DSS v3.1、および米国国立標準技術研究所 (NIST) 出版物 800-53 Rev 3 (連邦政府情報システムにおける推奨セキュリティ統制) を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同等に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。

障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータアプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の (AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ

標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のお客様は、コンテンツを保存する物理的リージョンを指定できます。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しません。使用できるリージョンの完全なリストについては、AWS グローバルインフラストラクチャーのページを参照してください。

AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているため、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPsec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (<https://aws.amazon.com/kms/> を参照)。詳細については、AWS クラウドセキュリティホワイトペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 および Glacier サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。 <https://aws.amazon.com/jp/s3/faqs/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

3 本ガイドラインの対象システム及び対象情報

3.3 外部保存を電子媒体経由で行う場合の手順

■ 要求事項 8

必須

医療情報を CD、DVD、MO 等の電子媒体を利用して情報処理事業者の施設に保存する場合を考慮し、配送事業者の信頼性については、機密保持契約の締結が可能である、機密情報の配送に特化した配送サービスを提供している、配送状況を利用者が把握する機能を提供している等の条件により事業者を選択することで確保すること。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニ

アマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

AWS Snowball を使用する場合のみ(1)のケースが該当します配送業者

ジョブの作成時に、Snowball の送付先住所を指定します。AWS からお客様、お客様から AWS への Snowball の配送はいずれも、リージョンのキャリアが行います。Snowball が送付されるたびに、 の追跡番号が発行されます。各ジョブの追跡番号や追跡を行うウェブサイトへのリンクは、AWS Snowball マネジメントコンソール のジョブダッシュボードから確認するか、または ジョブ管理 API の API コールを使用できます。Snowball 向けにリージョンがサポートしているキャリアのリストは以下のとおりです。

- ・インドの場合、Blue Dart がキャリアです。
- ・日本の場合、西濃シエンカー株式会社がキャリアです。
- ・その他のリージョンのキャリアはすべて、UPS です。

詳細および最新情報は以下 URL を参照ください。

https://docs.aws.amazon.com/ja_jp/snowball/latest/ug/mailing-storage.html

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御

できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク（VPN）接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション（CRR）は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン（AZ）のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデー

データベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のお客様は、コンテンツを保存する物理的リージョンを指定できます。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しません。使用できるリージョンの完全なリストについては、AWS グローバルインフラストラクチャーのページを参照してください。

AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お

お客様が自身のデータの統制と所有権を有しているため、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPsec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (<https://aws.amazon.com/kms/> を参照)。詳細については、AWS クラウドセキュリティホワイトペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 および Glacier サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。 <https://aws.amazon.com/jp/s3/faqs/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

3.4 外部保存をネットワーク経由で行う場合の手順

■ 要求事項 9

推奨

医療情報をネットワーク経由で情報処理事業者の施設に保存する場合の一連の医療機関等の医療従事者の作業手順と情報処理事業者の作業手順を考慮し、管理台帳に記載すべき、転送された電子ファイルの情報については「7.2.1 資産台帳」を参照すること。管理台帳を活用して、定期的に医療機関等と情報処理事業者間における医療情報電子ファイルの真正性を検証することが望ましい。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象とな

ります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することになります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジ

ョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーク環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えて

います。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のお客様は、コンテンツを保存する物理的リージョンを指定できます。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しません。使用できるリージョンの完全なリストについては、AWS グローバルインフラストラクチャーのページを参照してください。

AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているため、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPsec トンネルも暗号化されます。加えて、お客様は AWS Key Management Systems (KMS) を活用して暗号化キーの作成と管理を行えます (<https://aws.amazon.com/kms/> を参照)。詳細については、AWS クラウドセキュリティホワイトペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。AWS では、お客様がご自分のテープバックアップサービスプロバイダーを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 および Glacier サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。 <https://aws.amazon.com/jp/s3/faqs/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.4

A.12.6

A.13 通信のセキュリティ

A.13.1

A.13.1.1
A.13.1.2
A.13.1.3
A.13.2
A.13.2.1
A.13.2.2
A.13.2.3
A.13.2.4

A.16 情報セキュリティインシデント管理

A.16.1.1
A.16.1.2
A.16.1.3
A.16.1.4
A.16.1.5
A.16.1.6
A.16.1.7
A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.4 外部保存をネットワーク経由で行う場合の手順

■ 要求事項 10

必須

医療情報をネットワーク経由で情報処理事業者の施設に保存する場合の一連の医療機関等の医療従事者の作業手順と情報処理事業者の作業手順を考慮し、ネットワーク経由の交換手順について医療機関等と合意し、手順書として双方で管理すること。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイ

アウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行

に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することになります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する

幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク（VPN）接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの中には、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療機関等とのネットワーク経由での情報交換手順を定め作業手順を作成し医療機関等と合意し管理する必要があります。

■ 推奨される追加の実施事項

交換に使用するネットワークをセキュアに保つため、情報処理事業者は専用線接続である AWS Direct Connect やインターネット VPN を利用することができます。作業手順では、これらのセキュアな回線を用いた交換手順を定めることが推奨されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.4

A.12.6

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.4 外部保存をネットワーク経由で行う場合の手順

■ 要求事項 11

推奨

ファイル転送についてインターネット標準技術である FTP プロトコルを用いる場合においては専用回線あるいは VPN 等を利用して少なくともネットワークレイヤでの安全対策を施し、パスワード及びデータ漏洩のリスクを低減すること。単一の安全対策ではなく、ネットワークレイヤでの安全対策に加えて、アプリケーションレイヤにおいても SFTP、SCP 等、セキュリティ機能が組み込まれたファイル転送プロトコルを利用するといった、多重防御を実装することが望ましい。なお、FTP のアカウント情報を不正に取得する悪意のあるコードが広範囲に被害を及ぼした事例があることから、FTP を採用する場合には FTP アクセスログを定期的に検証し、不必要な FTP アクセスが行われていないことを確認するなどの対策を行うこと。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と

同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネン

トを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ネットワークレイヤの安全対策として専用線接続である AWS Direct Connect、または VPN を使用した IPsecVPN を選択、実施することが求められます。

そのうえで、アプリケーションレイヤでの SFTP,SCP などのセキュリティ機能が組み込まれたファイル転送プロトコルを利用し、多重の安全対策が実現可能です。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.4

A.12.6

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.4 外部保存をネットワーク経由で行う場合の手順

■ 要求事項 12

必須

悪意のあるコード検査及び電子署名検証等の過程で問題が発見された場合はただちに医療機関等に通知すること。
なお、問題が発見された電子ファイルは原因特定を行う必要があることから、削除せずに情報処理装置から隔離したかたちで保管すること。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の

様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）

または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN)；事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的とし

て、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハ

ードウェア仮想プライベートネットワーク（VPN）接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション（CRR）は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン（AZ）のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、悪意のあるコード検査及び電子署名検証等の過程で問題が発見された場合はただちに医療機関等に通知する必要があります。

AWS 上で悪意のあるコード検査および電子署名検証などを行うためには 3rd Party が提供するソリューションを利用する必要があります。

AWS 上で利用可能なソリューションは、以下 URL を参照ください。

<https://esp-online.com/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.4

A.12.6

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5
A.16.1.6
A.16.1.7
A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.4 外部保存をネットワーク経由で行う場合の手順

■ 要求事項 13

推奨

医療機関等への通知については、自動的に通知メッセージを作成・送付する仕組みを設けることがコスト面でも安全面でもメリットがある。このような通知メッセージを実装する場合、メッセージ中に機微な情報が含まれる場合には、医療機関等と受託情報処理事業者を結ぶ安全なネットワーク上で転送することが原則であるが、保護されていないインターネット経由で転送する場合には、暗号技術を用いて、メッセージの機密性、完全性を確保すること

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米

国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同等に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オ

プロジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によって

アクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療機関等への通知を担う必要があります。

AWS インフラストラクチャーに関する通知については、AWS から情報処理事業者に送付されるメッセージを漏らさず確認し、サービスに影響があると想定される場合には医療機関へ通知を行う必要があります。

医療機関との通知のやりとりには安全なネットワークの利用もしくは暗号化などの安全管理策を施す必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.4

A.12.6

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.5 外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

■ 要求事項 14

必須

ASP・SaaS では計算機環境を共有する場合があります、利用者間の悪影響が発生する可能性が存在すると考えられるため、システム構築、システム運用時の考慮事項について、「3.5.2 ネットワーク利用上の考慮事項」及び「ASP・SaaS 事業者向けガイドライン」の要求事項に従い、適切な対策を行うことが要求される。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部のおよび外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのイン

ターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラ

トラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、Amazon EC2 などの計算機環境のスペックが保証されたタイプを選択することが可能です。そのため、利用者間での計算機環境の共有が悪影響を及ぼすと考えられる場合には、AWS リソースの性能保証がされたインスタンスタイプおよびストレージのプロビジョンド IOPS を利用し、共有による悪影響を排除することが可能です。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.12 運用のセキュリティ

A.12.1

A.12.1.1

A.12.1.2

A.12.1.3

A.12.1.4

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4
A.16.1.5
A.16.1.6
A.16.1.7
A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.5 外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

■ 要求事項 15

必須

ASP・SaaS 形式のサービス等を利用して医療情報をアプリケーション入力する場合の一連の医療機関等の医療従事者の作業手順と情報処理事業者の作業手順を考慮し、アプリケーション入力による医療情報の交換手順について医療事業者と合意し、手順書として双方で管理すること。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米

国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに

十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することになります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療機関等とのアプリケーションを介した情報交換手順を定め作業手順を作成し医療機関等と合意し管理する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.12 運用のセキュリティ

A.12.1

A.12.1.1

A.12.1.2

A.12.1.3

A.12.1.4

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.5 外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

■ 要求事項 16

推奨

電子署名の付与が求められる情報については、電子ファイルとして作成してファイルを転送する形をとることが望ましく、その場合には、情報処理事業者にて受け取ったファイルの電子署名を検証することになる。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただ

く必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の

(AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、電子署名の付与が求められる情報については電子ファイルとして作成し電子署名を施すことが推奨されます。また、受け取りの際には電子証明の検証を行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.12 運用のセキュリティ

A.12.1

A.12.1.1

A.12.1.2

A.12.1.3

A.12.1.4

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.5 外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

■ 要求事項 17

必須

ASP・SaaS ではウェブブラウザをクライアントとした、いわゆるウェブアプリケーションを提供することが多いと考えられる。ウェブアプリケーション特有のセキュリティ上の要求事項に配慮して、サービス提供時はもちろん、リスク評価を行い、必要に応じて定期的にアプリケーションの脆弱性検査を実施して、安全性を確認すること。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのイン

ターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することになります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラ

トラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-脆弱性レポート

AWS リソース（EC2 インスタンスや S3 バケット）が不審なアクティビティに使用されている疑いがある場合は、こちらから AWS 不正使用対策チームにご連絡ください。効率的に対応させていただくために、参考となりそうな資料（実証コード、ツール出力など）も併せてお送りください。脆弱性の性質や重大度を把握するのに役立ちます。このプロセスの一環としてお客様が AWS と共有する情報は、AWS 内で機密保持されます。お客様の許可なしにそれがサードパーティと

共有されることはありません。AWS は、ご提出いただいたレポートを確認し、追跡番号を付与します。その後、お客様へのご対応としてレポートの受理をお知らせし、プロセスの次のステップについて概要をお伝えします。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/vulnerability-reporting/>

-侵入テスト

許可のクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をクエストするには、AWS 脆弱性/侵入テストクエストフォームに必要事項を記入して、送信してください。侵入テストのクエストに関して注意すべき複数の重要事項があります。

すべての侵入テストに許可が必要です。許可をクエストするには、テストを希望するインスタンスに関連付けられているルート認証情報を使用して、AWS ポータルにログインする必要があります。これを行わないと、フォームが正しく事前入力されません。サードパーティにテストの実施を依頼する場合は、フォームに必要事項を記入して、AWS から承認が下りた時点でサードパーティに通知する必要があります。AWS では、サードパーティのテスト企業は承認されません。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ウェブアプリケーションとして医療情報システムを提供する場合、ウェブアプリケーション特有のセキュリティ上の要求事項に配慮して、リスク評価および定期的にアプリケーションの脆弱性検査を実施する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.12 運用のセキュリティ

A.12.2

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.5 外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

3.5.1 データベース利用上の考慮事項

■ 要求事項 18

必須

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセ

セキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環として

データ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーク環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク（VPN）接続を作成することができるので、AWS クラウドを既存のデータセンター

を拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ネットワーク経路の暗号化およびデータベースの暗号化等の適切なリスク低減策を実施する必要があります。

ネットワークの暗号化

AWS では、TLS/SSL を利用した HTTP 通信の暗号化が可能です。TLS/SSL 処理を AWS Elastic Load Balancing に任せるとも可能です。また、ネットワーク全体の暗号化として Amazon VPC の VPN 機能を利用した IPsec VPN を利用することも可能です。

データベースの暗号化

Amazon RDS では透過的暗号化を用いてデータベース全体を暗号化することができます。この際の暗号鍵は AWS Key Management Service で管理する独自鍵を利用することが可能です。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.10 暗号

A.10.1

A.10.1.1

A.10.1.2

A.12 運用のセキュリティ

A.12.2

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.14 システムの取得, 開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

- A.16.1.4
- A.16.1.5
- A.16.1.6
- A.16.1.7
- A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.5 外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

3.5.1 データベース利用上の考慮事項

■ 要求事項 19

必須

データベースを利用したシステムでは、内部関係者による不正行為、情報漏洩を視野に入れて対策を講じる必要がある。一般的にウェブアプリケーションの利用環境ではデータベースに直接アクセスする管理者、開発者といったアカウントはその職責上多くの権限が付与されているケースがあり、リスクが大きい。そのため「なりすまし」によってこれらのアカウントの不正使用を防ぐため、パスワードの管理を厳密に行うだけでなく、必要に応じて多要素認証などの技術を利用し十分な認証強度を確保しなければならない。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control

Objectives for Information and related Technology, COBIT) フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会 (AICPA) のトラスト・サービスの原則 (Trust Services Principles)、PCI DSS v3.1、および米国国立標準技術研究所 (NIST) 出版物 800-53 Rev 3 (連邦政府情報システムにおける推奨セキュリティ統制) を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします (お客様のインスタンスはこのスキャンの対象外です)。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、

保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムのウェブアプリケーションの利用環境では、管理者などの特権ユーザーに対し、多要素認証などの十分な認証強度の確保を行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.10.1.1

A.10.1.2

A.12 運用のセキュリティ

A.12.2

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.5 外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

3.5.1 データベース利用上の考慮事項

■ 要求事項 20

推奨

「なりすまし」が行われた際の被害を小さくするため、管理者機能を分割した上でおのおのに別の特権 ID を割り当て、それぞれの特権 ID の権限を必要最小限とする最小特権の原則を実装することが望ましい。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部のおよび外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのイン

ターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することになります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラ

トラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムの管理者権限について、権限を分割し 1 つ 1 つの特権 ID の権限を最小限にとどめる設計とすることが推奨されます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.10.1.1

A.10.1.2

A.12 運用のセキュリティ

A.12.2

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

3 本ガイドラインの対象システム及び対象情報

3.5 外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

3.5.2 ネットワーク利用上の考慮事項

■ 要求事項 21

アプリケーション入力をおこなう場合には、第三者による傍受のリスクを避けるため、アプリケーションを提供する情報処理事業者と医療機関等を接続するネットワークとして専用線あるいは VPN を利用することが要求される。インターネット VPN には傍受以外にも第三者による不正な中継（man in the middle）、サービス不能攻撃等のリスクが存在し、回線品質も、専用線や IP-VPN と比較して低いため、交換する情報に求められる機密性のレベルを判断し、コスト及び運用に対して、閉域網上に構築された VPN との比較を行い、適切なネットワークを選択すること。インターネット上の VPN を利用する場合には、第三者からの不正なアクセスを防止するため、「7.6.6 ネットワークセキュリティ管理」に示される制約に従うこと。

■ AWS のインフラストラクチャー関連事項

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同等に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の (AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効

です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動

的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療機関等と医療情報システムを接続するネットワークとして専用線あるいはVPNを利用することが求められます。

ネットワークの選定に当たっては、機密性のレベル、コストおよび運用に対して各種方式の比較を行い選定を実施する必要があります。

インターネット VPN を利用する際は、「7.6.6 ネットワークセキュリティ管理」記載の制約に従う必要があります。

■ 推奨される追加の実施事項

AWS では AWS Direct Connect を利用した専用線接続もしくは Amazon VPC の VPN 機能を利用した VPN 接続を用いて医療機関等と医療機関のネットワーク接続を行うことが推奨されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.10 暗号

A.10.1

A.10.1.1

A.10.1.2

A.12 運用のセキュリティ

A.12.2

A.13 通信のセキュリティ

A.13.1

A.13.1.1

A.13.1.2

A.13.1.3

A.13.2

A.13.2.1

A.13.2.2

A.13.2.3

A.13.2.4

A.14 システムの取得, 開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

4.1 情報処理事業者の管理者における情報保護責任について

推奨

情報処理事業者においても、医療情報という機微性の高い情報を扱うことから、医療機関等の負う責任の一端を共有していると考えるべきであり、扱う個々の情報の価値、リスク、責任について受託元の医療機関等と考えを共通した上で、システム仕様、運用計画、事業継続計画等に合意することが重要である。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント – このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 – この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント – このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米

国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）

または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS を利用した医療情報システムにおいて責任共有モデルに基づきデータの統制および所有権は情報処理事業者の責任で扱うことを前提にシステム仕様、運用計画、事業継続計画を作成、医療機関等と合意する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1
A.16.1.2
A.16.1.3
A.16.1.4
A.16.1.5
A.16.1.6
A.16.1.7
A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2
A.17.2.1

4 電子的な医療情報を扱う際の責任のあり方

4.1 情報処理事業者の管理者における情報保護責任について

■ 要求事項 23

必須

医療情報安全管理ガイドラインでは、医療機関等における管理者の善管注意義務を果たすための責任を「医療情報保護の体制を構築し管理する局面での責任」と、「医療情報について何らかの不都合な事態（典型的には情報漏洩）が生じた場合にいかなる対処をすべきかという意味での責任」とに分けて記述している。

「不都合な事態」により損害が発生した場合には損害填補責任が生じる。委託契約においては医療機関等と情報処理事業者との責任分担を予め考慮しておく必要があることから、本ガイドラインにおいては、責任分界点に関する考えとともに、上記の分類で、情報処理事業者にとって善管注意義務を果たすための責任を記述する。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

A.17.2.1

A.18 順守

A.18.1

A.18.1.1

4 電子的な医療情報を扱う際の責任のあり方

4.2 通常運用における責任について

(1)

■ 要求事項 24

必須

説明責任

医療機関等の管理者においては「電子的に医療情報を取り扱うシステムの機能や運用方法が、その取り扱いに関する基準を満たしていることを患者等に説明する責任である。」とされている。情報処理事業者にとっても医療機関等に対して同様の責任があると考え、医療情報処理に関わるシステム文書として、ハードウェア及びソフトウェアの仕様書、運用計画書、事業継続計画文書等を求めに応じて提出可能な状態におくこと、定期的な情報セキュリティ監査、システム監査等、第三者監査の実施、結果及び是正措置報告についても提出可能な状態におくこと等を委託契約事項に含め、履行する必要がある。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです
<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の

(AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのに有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

医療情報システムに関する説明責任

情報処理事業者は、AWS 上に構築する医療情報システムの仕様書・設計書などの文書を整備し、提出可能な状態にしておく必要があります。AWS ではハードウェア仕様書の代わりに、利用している AWS リソースのスペックや構成等の仕様を記載する文書を作成する必要があります。

第三者監査

情報処理事業者は定期的に第三者監査を実施し、結果および指摘事項に対する是正措置報告を提出可能な状態にしておく必要があります。AWS インフラストラクチャーに関する第三者監査結果は、AWS が取得・維持しているものが利用可能です。詳細および最新情報は以下 URL を参照ください。

AWS Compliance

<https://aws.amazon.com/jp/compliance/programs/>

AWS Artifact

<https://aws.amazon.com/jp/artifact/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

A.17.2.1

A.18 順守

A.18.1

A.18.1.1

4 電子的な医療情報を扱う際の責任のあり方

4.2 通常運用における責任について

(2)

■ 要求事項 25

必須

管理責任

情報処理事業者は医療機関等から委託を受けてシステムの運用管理を行うことから、運用状況及び管理状況について定期的に報告し、医療機関等から意見又は指摘を受けること、及び電子化された個人情報の保護に一定の知識を有する責任者を定めることが求められる。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この

集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理

的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の (AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

-Amazon CloudWatch

Amazon CloudWatch は、開発者、システムオペレーター、サイト信頼性エンジニア (SRE)、IT マネージャーのために構築されたモニタリングおよび管理サービスです。CloudWatch では、データと実用的なインサイトを利用して、アプリケーションのモニタリング、システム全体のパフォーマンスの変化に関する理解と対応、リソース使用率の最適化、運用状態の統一的な確認を行うことができます。

詳細および最新情報は以下 URL を参照ください。

<https://aws.amazon.com/jp/cloudwatch/>

■ 情報処理事業者（お客様）の該当事項

システムの運用管理責任

情報処理事業者は、システムの運用・管理状況について医療機関等へ定期的に報告する必要があります。

個人情報の管理責任

AWS では、データの統制および所有権は情報処理事業者にあり、個人情報の管理責任は情報処理事業者にあります。そのため、情報処理事業者は個人情報保護責任者を定め個人情報を管理する責任があります。

■ 推奨される追加の実施事項

Amazon CloudWatch で収集される AWS リソースの各種メトリクスを確認することで、システムの運用状況を確認することができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

A.17.2.1

A.18 順守

A.18.1

A.18.1.1

4 電子的な医療情報を扱う際の責任のあり方

4.2 通常運用における責任について

(3)

■ 要求事項 26

必須

定期的に見直し必要に応じて改善を行う責任

情報処理事業者はシステムの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行った上で医療機関等に報告し、意見又は指摘を受けることが求められる。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント – このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 – この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント – このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の (AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効

です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、定期的に現行運用管理の再評価・改善検討を実施し、医療機関等に報告する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.17.2.1

A.18 順守

A.18.1

A.18.1.1

4.3 事後責任について

(1)

■ 要求事項 27

必須

説明責任

情報処理事業者においては、事態の発生を認識次第、ただちに医療機関等に通知し、医療機関等の管理者が個々の患者、行政機関や社会へ説明・公表するために、協力して情報収集を図ることが求められる。加えて、発生しうる事態を想定した説明責任の分担を契約事項として含める必要がある。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対し

て適用されます

AWS 適正利用規約 – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集合的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

-AWS サポート

AWS では、ご利用を開始したばかりの方にも、アプリケーション開発とビジネスソリューションの構築の中で導入するサービスを増やしている方にも、成功をサポートする適切なリソースを提供したいと願っています。AWS サポートでは、現在の、または予定されているユースケースに基づき、AWS でのみ可能なツールと専門知識の組み合わせによって、すばらしい成果が得られるようお客様をサポートします。

詳細および最新情報は以下 URL を参照ください。

<https://aws.amazon.com/jp/premiumsupport/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、「何らかの不都合な事態」の発生を認識次第、ただちに医療機関等に通知し、協力して情報収集を図る必要があります。また、発生しうる事態を想定した説明責任の分担を契約事項として含める必要があります。

AWS インフラストラクチャーに関する事態を想定し、事前に必要サービスレベルの AWS サポートに加入し AWS インフラストラクチャーに発生した問題に関しても、AWS に問合せの上、医療機関へ説明が可能なようにしておくことが求められます。

■ 推奨される追加の実施事項

本番サービスを実施する環境では、24 時間 365 日の対応時間確約のサービスレベルである「ビジネス」プラン以上の AWS サポートの利用を推奨します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.17.2.1

A.18 順守

A.18.1

A.18.1.1

4 電子的な医療情報を扱う際の責任のあり方

(2)

■ 要求事項 28

必須

善後策を講ずる責任

医療情報について何らかの事故が生じた場合、速やかに善後策を講じなければならない。そのためには、前もって発生しうる事故と考えられる原因を洗い出して対応手順を策定しておくことが必要である。また、事故に対する緊急対応が完了した後で原因を確定するために、事故発生時の状況を保存あるいは記録する手順、対応過程で行われた作業を記録する手順等も策定しておくことが求められる。加えて、確定された原因にもとづき再発防止策を講じることも求められる。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです
<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の

(AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのに有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

-AWS サポート

AWS では、ご利用を開始したばかりの方にも、アプリケーション開発とビジネスソリューションの構築の中で導入するサービスを増やしている方にも、成功をサポートする適切なリソースを提供したいと願っています。AWS サポートでは、現在の、または予定されているユースケースに基づき、AWS でのみ可能なツールと専門知識の組み合わせによって、すばらしい成果が得られるようお客様をサポートします。

詳細および最新情報は以下 UR I を参照ください。

<https://aws.amazon.com/jp/premiumsupport/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報について何らかの自己が生じた場合に備え、事前に発生しうる事故と考えられる原因、対応手順を策定しておくことが求められます。

また、緊急対応後の根本原因調査のため、事故発生時の状況を保全するための手順も策定することが求められます。

根本原因調査後は、再発防止策の策定実施も求められます。

AWS 上では、AWS インフラストラクチャーに起因した事故も考えられることから、AWS サポートへ加入し、AWS サポートと連携した対応手順を策定しておく必要があります。

■ 推奨される追加の実施事項

本番サービスを実施する環境では、24 時間 365 日の対応時間確約のサービスレベルである「ビジネス」プラン以上の AWS サポートの利用を推奨します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.1.1

A.8.1.2

A.8.1.3

A.8.1.4

A.8.2

A.8.2.1

A.8.2.2

A.8.2.3

A.8.3

A.8.3.1

A.8.3.2

A.8.3.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.1.1

A.11.1.2

A.11.1.3

A.11.1.4

A.11.1.5

A.11.1.6

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1.1

A.16.1.2

A.16.1.3

A.16.1.4

A.16.1.5

A.16.1.6

A.16.1.7

A.16.1.8

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.17.2.1

A.18 順守

A.18.1

A.18.1.1

4 電子的な医療情報を扱う際の責任のあり方

(3)

■ 要求事項 29

必須

再委託先に対する責任

外部データセンター、バックアップ施設の運用管理等、一部の情報処理業務を再委託している場合、再委託先あるいは

再委託している情報処理業務において発生した事態に関する責任については、医療機関等との契約において第一義に委託先である情報処理事業者が負うべきであると考えられるが、再委託先の事業者においても責任は発生していると考えられる。互いの責任の範囲について合意し、再委託先との契約で明記しておくことが求められる。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の (AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効

です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、インフラストラクチャーの委託先である AWS の責任共有モデルに基づいた責任範囲について理解しておく必要があります。

AWS の責任共有モデルについては以下 URL を参照ください。

<https://aws.amazon.com/jp/compliance/shared-responsibility-model/>

また、AWS との契約であるカスタマーアグリーメントについても理解しておく必要があります。

<https://aws.amazon.com/jp/agreement/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.10 暗号

A.10.1.1

A.10.1.2

A.11 物理的及び環境的セキュリティ

A.11.1

A.12 運用のセキュリティ

A.12.1

A.12.6

A.12.7

A.15 供給者関係

A.15.1

A.15.2

A.16 情報セキュリティインシデント管理

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.17.2.1

A.18 順守

A.18.1

A.18.1.1

4 電子的な医療情報を扱う際の責任のあり方

4.4 ネットワーク利用時における回線事業者との責任分界点について

■ 要求事項 30

必須

医療機関等と情報処理事業者、回線事業者の責任について、
想定される障害等のそれぞれについて契約に明示するなどの対策を行う必要がある。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです
<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の

(AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

医療情報処理事業者は、AWS 上の VPC の構成・維持について責任を持ちます。また、医療機関等と AWS を接続する回線については医療機関の要件に沿う回線を選択する必要があります。選択した回線のサービスレベルと責任分界点について医療機関に明示する必要があります。

- インターネット VPN を用いた回線の場合、VPN の設定については情報処理事業者の責任となります。また、インターネット接続回線については回線事業者の SLA および契約を確認し、契約等で明示する必要があります。

- AWS Direct Connect を用いた回線の場合、Direct Connect をサポートする APN パートナーの SLA および契約を確認し、契約等で明示する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

5 医療情報の取扱いに関する知識

5.1 法令・通知

■ 要求事項 31

必須

医療情報の取扱いに関する法令・ガイドライン類を示す。医療情報の外部保存業務を請け負うことになる情報処理機関は、これらの法令・ガイドラインについて詳細を把握し、示される基準を満たすよう、対策を行うことが求められる。

「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」（平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知に添付。）

「診療録等の外部保存に関するガイドライン」（平成 14 年 5 月 31 日付け医政発第 0531005 号厚生労働省医政局長通知）

「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（平成 16 年 12 月 24 日通達、平成 18 年 4 月 21 日改正）

「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号）

「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 17 年 3 月 31 日付け医政発第 0331009 号・薬食発第 0331020 号保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知）

「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成 17 年厚生労働省令第 44 号）

「「診療録等の保存を行う場所について」の一部改正について」（平成 17 年 3 月 31 日付け医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・保険局長連名通知）

「「診療録等の保存を行う場所について」の一部改正について」（平成 22 年 2 月 1 日付け医政発第 0201 第 2 号・保発第 0201 第 1 号厚生労働省医政局長・保険局長連名通知）

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この

集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理

的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の (AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は医療機関等との契約において、受託業務の責任範囲を明確にする必要があります。また、情報処理事業者はデータの統制と所有権を有していますので、情報処理事業者は、要求事項に記載の法令・ガイドラインを遵守する責任があります。詳細については、AWS カスタマーアグリーメントを参照してください。

また、医療情報システムの基盤となる AWS インフラストラクチャーは責任共有モデルに基づき AWS の責任で管理されます。予め AWS 利用者より開示があった場合には医療情報システムが AWS 上で稼働していることは認識可能であるため相応のサポートが行われます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.18 順守

A.18.1

A.18.1.1

A.18.1.2

5 医療情報の取扱いに関する知識

5.1 法令・通知

■ 要求事項 32

必須

医療情報安全管理ガイドライン「3.3 取扱いに注意を要する文書等」に記される留意事項に従うこと。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されて

います。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

す。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報安全管理ガイドライン「3.3 取り扱いに注意を要する文書等」（医療情報システムの安全管理に関するガイドライン第 5 版では「3.4 取り扱いに注意を要する文書等」が該当箇所）に該当する文書の保存に関して留意事項に従いガイドラインに準じた取り扱いを行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1.1

A.5.1.2

A.18 順守

A.18.1

A.18.1.1

A.18.1.2

6 電子保存の要求事項について

6.1 真正性の確保に関する要求事項

■ 要求事項 33

必須

医療情報安全管理ガイドラインによれば、真正性とは「正当な権限において作成された記録に対し、虚偽入力、書き換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であること」とされる。医療情報を作成する医療従事者及び医療機関等が真正性を確保することができるよう、情報記録者が誰であるのかについて電磁的記録として認識できるよう、文書フォーマット等について医療機関等と十分な合意を形成しておくべきである。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この

責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーするこ

とで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティープラニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

譲歩処理事業者は、作業者が医療情報システム上で医療情報を作成する際のアクセスログを記録する必要があります。また、作成された記録について以後の正当性を確認するためのチェックサムなどを生成・保管する必要があります。

Amazon S3 では、S3 にアップロードするオブジェクトの MD5 チェックサムを計算し、オブジェクトをアップロードする際に、整合性を確認する MD5 チェックサム値を HTTP ヘッダーに格納することで、MD5 チェックサム値でアップロードしたファイルの整合性が検証されます。またこのチェックサムは S3 からダウンロードしたオブジェクトの整合性を検証するためにも使用できます。

詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/data-integrity-s3/>

アップロード作業者の記録とチェックサムを利用し真正性を確保することが可能です。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得, 開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.1 真正性の確保に関する要求事項

■ 要求事項 34

必須

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネン

トを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。
Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。
Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>
<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>
https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

譲歩処理事業者は、作業者が医療情報システム上で医療情報を作成する際のアクセスログを記録する必要があります。また、作成された記録について以後の正当性を確認するためのチェックサムなどを生成・保管する必要があります。

Amazon S3 では、S3 にアップロードするオブジェクトの MD5 チェックサムを計算し、オブジェクトをアップロードする際に、整合性を確認する MD5 チェックサム値を HTTP ヘッダーに格納することで、MD5 チェックサム値でアップロードしたファイルの整合性が検証されます。またこのチェックサムは S3 からダウンロードしたオブジェクトの整合性を検証するためにも使用できます。

詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/data-integrity-s3/>

アップロード作業者の記録とチェックサムを利用し真正性を確保することが可能です。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.1 真正性の確保に関する要求事項

■ 要求事項 35

必須

受入れ後はハードディスクや光学ディスク等の電子媒体に情報を書き込んで保存する。情報を保存した電子媒体について、認可されていない着脱、持出が行われていないことを保証するため、定期的に検査を行うこと。また、電子媒体上の情報に対して、認可されていない書き込み、削除が行われないように、アカウント管理、アクセス権限管理を行い、定期的に電子署名を検証する等の作業により改ざんの検出を行う。情報の預け主である医療機関等の要請により情報を提供する際にも電子署名を検証等の作業により改ざんの検出を行い、正しく元の情報を提供する。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです
<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的风险アセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の

(AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、

監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、受け入れた医療情報のアクセスログを取得・保管し、定期的に不正持ち出しが無いか棚卸を行う必要があります。

不正な改ざんが行われていないことを確認するため、チェックサムを用いた定期的な改ざん検知を実施する必要があります。

また、医療機関への情報提供の際にもチェックサムを用いた改ざん検知を実施する必要があります。

必要な対策

- 定期的なアクセスログの棚卸（不正アクセスの有無の確認）
- 定期的な改ざんチェック（チェックサムによる整合性確認）
- 情報出力時の改ざんチェック（チェックサムによる整合性確認）

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.1 真正性の確保に関する要求事項

■ 要求事項 36

必須

情報の廃棄に関しては医療機関等からの依頼により行うことであり、処理が厳正に執り行われたことを医療機関等に対し証明する必要がある。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです
<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の

(AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者自身でワイプ作業を行うこともできます。

ハードディスク消去ツール等を用い情報処理システムで利用する論理ディスク内のデータの消去が可能ですので、物理的なハードディスクのデータ消去に頼ることなく、論理的にディスク消去を実施・確認することができます。情報処理事業者は、自身の統制下でデータの消去措置の実施記録が提出できるようワイプ作業を実施・記録を行うことが求められます。

■ 推奨される追加の実施事項

情報処理事業者自身で Amazon EBS のワイプ作業を行うこともできます。また、AWS 上に格納する機密データは、AWS Key Management Service で管理される暗号鍵を利用して暗号化することを推奨します。契約終了時に暗号鍵そのものを廃棄することで、データ消去に相当するといった対応を考慮することも可能となります。

Amazon Elastic Block Store (EBS) で追加のストレージを使う場合などはボリュームを暗号化することができます。S3 を使う場合は Server Side Encryption でバケット・ファイル単位に暗号化することができます。また、サーバサイド暗

号化のみでなく、必要に応じてクライアントサイド暗号化の利用を検討してください。

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得, 開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.2 見読性の確保に関する要求事項

■ 要求事項 37

必須

見読性とは「電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできること」とされる。それぞれの情報に求められる見読可能となるまでの時間的要求について、医療機関等と合意しておくことが求められる。情報処理設備との間にはネットワークが介在することから、ネットワークの可用性について十分に検討する必要がある。特に、データ容量が大きい高精細デジタル画像である医用画像（レントゲンデータ等）を扱う場合は、ネットワークの回線容量について配慮しておくこと。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事

業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性およ

び脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、

高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は見読性を損なうことが無いよう、医療機関へのサービス内容と AWS のネットワーク帯域を考慮する必要がある。（ネットワーク帯域保証は AWS の範疇？）

--

情報処理事業者は、見読性を損なうことが無いよう、医療機関等との間で見読可能となるまでの時間（通常時・障害時）について合意しておく必要があります。

また、ネットワークの可用性・スループットについては医療機関とあらかじめ検討の上、要件として必要な際は帯域保証型のネットワークサービスの採用を行う必要があります。

AWS Direct Connect および AWS Direct Connect をサポートする APN パートナーの回線を採用することで、帯域保証型のネットワークを AWS との間で確立可能です。

■ 推奨される追加の実施事項

AWS では、医療情報システムを医療機関等のエンドユーザーと接続するためにインターネット以外の選択肢も用意されています。

AWS Direct Connect を利用することで、エンドユーザの拠点から AWS への専用ネットワーク接続を簡単に確立することができ、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。

<https://aws.amazon.com/jp/directconnect/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.2 見読性の確保に関する要求事項

■ 要求事項 38

必須

診療は24時間365日行われるものであるため、情報処理事業者においても同様にサービス提供を行う必要がある。医療機関等に情報処理機能を提供する事業者は、自らも重要インフラの一部に相当するという意識を持ち、適切な事業継続計画を策定すること。

■ AWSのインフラストラクチャー関連事項

AWSの法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所に

バックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、24 時間 365 日の診療を支えるインフラの一部として適切な事業継続計画を策定する必要があります。

■ 推奨される追加の実施事項

AWS を使用すると、各リージョン内の複数のアベイラビリティゾーンだけでなく、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。

情報処理事業者は、複数のアベイラビリティゾーンをまたがったシステム構成を構築（Multi-AZ 構成）することで、これらの AWS が提供する可用性を用いた事業継続計画の策定が可能です。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.2 見読性の確保に関する要求事項

■ 要求事項 39

必須

システムの更新、アプリケーションの変更等に伴い、電子保存された医療情報の読み出しに関する互換性を失わないように配慮することが求められる。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 – この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント – このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集合的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対す

る、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1

の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要

件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するた

めの仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、システムの更新、アプリケーションの変更前後において、保存された医療情報のフォーマットについて互換性を維持することが求められます。

■ 推奨される追加の実施事項

医療情報の読み出しに当たっては、互換性確保の観点から厚生労働省標準規格（用語集やコードセット、保存形式、メッセージ交換手続等）等の標準形式（HL7、DICOM など）での出力が可能とする機能を設けることが推奨されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.2 見読性の確保に関する要求事項

■ 要求事項 40

必須

情報処理事業者側の経営上の判断または経済的理由等から、サービス提供を終了せざるを得ない状況も想定される。このような状況においても、医療機関等の業務継続に悪影響を与えないよう、預託データの速やかな返却、他情報処理事業者へのサービス移管を可能とする配慮を行う必要がある。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 – この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント – このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的风险アセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集合的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対す

る、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1

の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することになります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ

標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、受領データを医療機関等に返却するためのデータ出力機能を用意することが求められます。

また、他情報処理事業者への移管をスムーズなものとするため、出力形式は厚生労働省標準規格（用語集やコードセット、保存形式、メッセージ交換手続等）等の標準形式（HL7、DICOM など）での出力が可能とする機能を設けることが推奨されます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.2 見読性の確保に関する要求事項

■ 要求事項 41

必須

アプリケーション入力の場合は医療情報安全管理ガイドラインの「5 情報の相互運用性と標準化について」に示されている、基本データセット、標準的な用語集、コードセット、データ交換のための国際的な標準規格について、十分に理解し、実装するアプリケーションにおいて提供サービスの可用性、データの互換性の確保に務めること。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するもの

です

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 - この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。

障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータアプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の (AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、

保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、「医療情報安全管理ガイドライン「5 情報の相互運用性と標準化について」」にて示される各種標準規格を十分に理解しアプリケーションの実装および提供サービスの可用性・データ互換性を確保する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

■ 要求事項 42

必須

保存性とは「保存性とは、記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されること」とされる。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント – このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです
<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部のおよび外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情

報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに

充分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要

件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するた

めの仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は Amazon S3 や Amazon EBS、Amazon RDS の Multi-AZ 構成を格納先として使うことで医療情報の長期保存を可能とします。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.3 保存性の確保に関する要求事項

■ 要求事項 43

必須

情報処理装置には利用に耐える耐用期間が製造ベンダにより定められているので、その耐用期間を越えないよう及び事業に支障を来たさないよう余裕を持った交換計画を策定しておくこと。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対して適用されます

AWS 適正利用規約 – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです
<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのに有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オ

プロジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によって

アクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS インフラストラクチャーに対する AWS の定期的な変更などの変更管理について、AWS からの以下の手段を通じた通知を確認し、サービスに影響が発生することが予測される場合には、事業に支障をきたさないようメンテナンス計画を策定し対応する必要があります。

- ・E メール
- ・AWS Service Health Dashboard
- ・AWS Personal Health Dashboard

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

6 電子保存の要求事項について

6.3 保存性の確保に関する要求事項

■ 要求事項 44

推奨

例えば病院又は診療所に勤務する医師による診療に関する診療録においては、医師法 24 条の 2 にあるように、5 年間の保存義務が規定されている。文書の種類によっては診療録よりも長期の保存が義務づけられたものもあるため、情報処理事業者においても、各種文書の保存義務より長期の保存が可能であるよう、事業継続に配慮することが望まれる。

■ AWS のインフラストラクチャー関連事項

AWS の法務関連の詳細、最新情報は下記を参照ください。

AWS カスタマーアグリーメント - このカスタマーアグリーメントは、お客様による当サービスのご利用について規定するものです

AWS サービス条件 - この追加条件は、お客様による特定のサービスのご利用に対して適用されます

AWS サービスレベルアグリーメント - このサービスレベルアグリーメントは、お客様による特定のサービスのご利用に対し

て適用されます

AWS 適正利用規約 – この適正利用規約は、当サービスの利用に関して、禁止される事項を記載したものです

<https://aws.amazon.com/jp/legal/>

責任共有環境

IT インフラストラクチャーを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することとなります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、最高レベルのサービスの可用性を達成することも可能です。

キャパシティの計画

AWS はサービスの利用状況を継続的にモニタリングし、アベイラビリティに関するコミットメントと要件をサポートするためにインフラストラクチャーを整備しています。AWS は、少なくとも月次のキャパシティプランニングモデルを維持し、インフラストラクチャーの使用と需要を評価しています。このモデルは将来の需要の計画をサポートし、情報の処理量、通信量、監査ログストレージの容量などが考慮されています。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監

視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、前項の対応策を用い、各種文書の保存義務より長期の保存を可能とする観点での事業継続計画を策定しておくことが推奨されます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定

■ 要求事項 45

必須

医療情報安全管理ガイドラインでは、外部情報保存受託機関に対して「プライバシーマーク制度や不足なく適用範囲を定めた適用宣言書に基づく ISMS 認定制度等による公正な

第三者の認定を受けていること」としている。医療情報の秘匿性の高さを考えれば、この方針は必要と考えられる。本ガイドラインにおいても同様にプライバシーマーク認定・ISMS 認証等の公正な第三者の認定を取得することを必要な要件とする。

■ AWS のインフラストラクチャー関連事項

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の

(AWS 環境上に) 拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関しては下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。ISO 認証書についてもダウンロード可能です。

<https://aws.amazon.com/jp/artifact/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

AWS セキュリティのベストプラクティスを参考に、ISMS を実装可能です。

https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスについて説明しています。また、AWS での資産の識別と分類と保護、アカウント、ユーザー、グループを使用した AWS リソースへのアクセスの管理、また、クラウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャー全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要についても説明しています。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

N/A

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定

7.1.1 ISMS 認証取得時の考慮事項

■ 要求事項 46

必須

情報処理事業者が医療情報処理の安全確保を目的として ISMS 認証を取得する場合には、受託した医療情報を扱う部門、部署を全て含むよう適用範囲を設定した上で ISMS 認証を取得することが求められる。すでに ISMS 認証を取得しているが適用範囲が上記部門、部署全体をカバーしていない場合は、適用範囲を再設定して取得しなおすことが求められる。加えて、医療情報システムに対しては、本ガイドラインで示される安全管理策を基準とした第三者機関による情報セキュリティ監査等を定期的に（少なくとも一年に一回以上の頻度で）実施して、十分な情報セキュリティレベルを確保していることを検証することが望まれる。医療情報の高い機微性、完全性の要求を鑑みて、通常の ISMS 認証取得プロセス、維持プロセスに加え、以下の推奨事項を満たすよう本ガイドラインを活用すること。

■ AWS のインフラストラクチャー関連事項

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのに有効です。AWS から提供可能な第三者認証や監査レポートに関しては下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。ISO 認証書についてもダウンロード可能です。

<https://aws.amazon.com/jp/artifact/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

AWS セキュリティのベストプラクティスを参考に、ISMS を実装可能です。

https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスについて説明しています。また、AWS での資産の識別と分類と保護、アカウント、ユーザー、グループを使用した AWS リソースへのアクセスの管理、また、クラウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャー全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要についても説明しています。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

N/A

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定

7.1.1 ISMS 認証取得時の考慮事項

(1)

■ 要求事項 47

推奨

認証取得あるいは更新の際に ISMS の安全管理策として、本ガイドライン「7 医療情報を受託管理する情報処理事業における安全管理上の要求事項」にて提示する安全管理策を盛り込むことが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業（お客様）の該当事項

AWS セキュリティのベストプラクティスを参考に、ISMS を実装可能です。

https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスについて説明しています。また、AWS での資産の識別と分類と保護、アカウント、ユーザー、グループを使用した AWS リソースへのアクセスの管理、また、クラウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャー全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要についても説明しています。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

N/A

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定

7.1.1 ISMS 認証取得時の考慮事項

(2)

■ 要求事項 48

推奨

受託管理する医療情報の入り口から出口まで包括的に ISMS の適用範囲とすることが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

AWS セキュリティのベストプラクティスを参考に、ISMS を実装可能です。

https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスについて説明しています。また、AWS での資産の識別と分類と保護、アカウント、ユーザー、グループを使用した AWS リソースへのアクセスの管理、また、クラウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャー全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要についても説明しています。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

N/A

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定

7.1.1 ISMS 認証取得時の考慮事項

(3)

■ 要求事項 49

推奨

安全管理措置が適切に適用されていることを、医療機関等が委託先事業者を選定する際に確認できるよう、医療機関等の要請に応じて適用宣言書の閲覧を即座に行うことができるよう準備を行っておくことが望ましい（適用宣言書には医療情報を取り扱うために特別に配慮している管理策を明確にすること）。

■ AWS のインフラストラクチャー関連事項

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関しては下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。ISO 認証書についてもダウンロード可能です。

<https://aws.amazon.com/jp/artifact/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

AWS セキュリティのベストプラクティスを参考に、ISMS を実装可能です。

https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスについて説明しています。また、AWS での資産の識別と分類と保護、アカウント、ユーザー、グループを使用した AWS リソースへのアクセスの管理、また、クラウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャー全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要についても説明しています。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

N/A

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定

7.1.2 医療情報の受託管理業務を実施するまでの認証及び監査の流れ

■ 要求事項 50

必須

医療情報を受託管理する業務を行う情報処理事業者が ISMS 認証を取得する際には、図 12「医療情報の受託管理業務を実施するまでの認証及び監査の流れ」に従って、その適用範囲及び管理策が本ガイドラインで示す基準に従っているかどうかを確認し、必要であれば再（拡大）審査を受けること。

■ AWS のインフラストラクチャー関連事項

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関しては下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。ISO 認証書についてもダウンロード可能です。

<https://aws.amazon.com/jp/artifact/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

AWS セキュリティのベストプラクティスを参考に、ISMS を実装可能です。

https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスについて説明しています。また、AWS での資産の識別と分類と保護、アカウント、ユーザー、グループを使用した AWS リソースへ

のアクセスの管理、また、クラウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャー全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要についても説明しています。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

N/A

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定

7.1.2 医療情報の受託管理業務を実施するまでの認証及び監査の流れ

■ 要求事項 51

推奨

本ガイドラインに従って ISMS 認証を取得した後に第三者による情報セキュリティ監査等を受け、監査結果を医療機関等に提示することが望まれる。

■ AWS のインフラストラクチャー関連事項

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関しては下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。ISO 認証書についてもダウンロード可能です。

<https://aws.amazon.com/jp/artifact/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

AWS セキュリティのベストプラクティスを参考に、ISMS を実装可能です。

https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスについて説明しています。また、AWS での資産の識別と分類と保護、アカウント、ユーザー、グループを使用した AWS リソースへのアクセスの管理、また、クラウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャー全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要についても説明しています。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

N/A

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

■ 要求事項 52

本ガイドラインで示す情報処理業務においては医療機関等から預かる情報個々の分類を正確に行う必要がある。預託された情報の種別等を記載した台帳等を作成し、その管理を厳密に行うこと。当該台帳には患者情報等、個人を特定できる情報を含まないよう、記載情報の構成に留意すること。但し、「3 本ガイドラインの対象システム及び対象情報」で示した医療情報交換経路(1)(2)では、情報の分類を行うことができないため、合理的な範囲で本章の記述に従うこと。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は預託された医療情報について、台帳を作成し、厳密に管理することが求められます。ただし、台帳に患者情報等の個人情報が含まれないよう配慮する必要があります。

■ 推奨される追加の実施事項

N/A

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.1 資産台帳

■ 要求事項 53

必須

医療情報が完全な状態にあることを保証するために資産台帳等を適切に維持管理することを目的として、以下の管理策を適用すること。なお、資産台帳等の媒体は、紙文書、電子ファイルのいずれでも良いが、媒体特有の脅威について把握し、適切な管理策を追加すること。

■ AWS のインフラストラクチャー関連事項

N/A

AWS では、お客様からの信頼を最優先にしています。AWS は 190 を超える国のエンタープライズ、教育機関、および政府機関を含む 100 万を超えるアクティブカスタマーにサービスを提供しています。金融サービスやヘルスケアの提供者、および政府機関といったお客様が私たちのことを信頼し、機密性の非常に高い情報を預けてくださっています。

AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。お客様からの信頼を維持することは継続的なコミットメントであり、今後も私たちが導入したプライバシーとデータセキュリティに関するポリシー、プラクティスおよびテクノロジーについてお知らせするよう努力を続けていきます。コミットメントには次のような事項が含まれます。

カスタマーコンテンツの所有権と管理権:

アクセス:

お客様は、自分のカスタマーコンテンツ、および AWS のサービスとリソースへのアクセスを管理します。お客様がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録の高性能な機能セットを用意しています (AWS CloudTrail など)。いかなる目的であっても、当社がお客様の同意なくカスタマーコンテンツにアクセスしたり、それを使用することはありません。

ストレージ:

コンテンツを保存するリージョンはお客様に選択していただけます。お客様の同意なしに、当社がカスタマーコンテンツを、お客様が選択したリージョンの外に移動したり複製したりすることはありません。

セキュリティ:

お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。

カスタマーコンテンツの開示:

法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。

セキュリティ保証:

当社では、お客様による当社のセキュリティ管理環境の確立、オペレーション、および活用をサポートするため、プライバシーとデータを保護するグローバルなベストプラクティスを使用したセキュリティ保証プログラムを展開しています。これらセキュリ

データの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、それぞれ個別に検証されています。

<https://aws.amazon.com/jp/compliance/data-privacy-faq/>

■ AWS サービス関連情報

-AWS Artifact

AWS Artifact では、AWS のセキュリティおよびコンプライアンスレポートと特定のオンライン契約にオンデマンドでアクセスできます。AWS Artifact には、Service Organization Control (SOC)、Payment Card Industry (PCI) レポート、AWS セキュリティ制御の実装と運用の有効性を検証する、さまざまな地域やコンプライアンス垂直市場の認定機関からの認定が含まれます。AWS Artifact で利用可能な契約には、事業提携契約 (BAA) と機密保持契約 (NDA) が含まれます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/artifact/>

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7.2 情報資産管理

7.2.1 資産台帳

(1)

■ 要求事項 54

必須

医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、受託する医療情報の資産管理台帳の作成を含む管理策を文書として規定し、管理を行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.2 情報資産管理

7.2.1 資産台帳

(2)

■ 要求事項 55

必須

預託された情報の全てを資産台帳に記録すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、受託した医療情報のすべてについて管理（受領、保存、配送、複製、編集、閲覧、廃棄等）に関する記録を上記で作成した資産管理台帳に記録する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.1 資産台帳

(3)

■ 要求事項 56

必須

必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、資産管理台帳を適切な権限を持つ職員が常時閲覧可能な状態として管理する必要があります。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.1 資産台帳

(4)

■ 要求事項 57

必須

資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、資産管理台帳を適切な権限を持つ職員（業務遂行上必要最低限の作業者）のみにアクセスを制限する必要があります。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.2 情報資産管理

7.2.1 資産台帳

(5)

■ 要求事項 58

必須

資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、資産管理台帳を電磁的記録として管理する場合、不正アクセス行為の記録を行う必要があります。

■ 推奨される追加の実施事項

ファイルサーバなどで資産管理台帳を管理する場合、ファイルサーバーのアクセスログを取得するとともに、セキュリティ侵害に対するログを有効化し、保管することが推奨されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.1 資産台帳

(1)

推奨

資産台帳等を紙文書として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について検出・記録できるような仕組みを実装することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

AWS では、お客様からの信頼を最優先にしています。AWS は 190 を超える国のエンタープライズ、教育機関、および政府機関を含む 100 万を超えるアクティブカスタマーにサービスを提供しています。金融サービスやヘルスケアの提供者、および政府機関といったお客様が私たちのことを信頼し、機密性の非常に高い情報を預けてくださっています。

AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。お客様からの信頼を維持することは継続的なコミットメントであり、今後も私たちが導入したプライバシーとデータセキュリティに関するポリシー、プラクティスおよびテクノロジーについてお知らせするよう努力を続けていきます。コミットメントには次のような事項が含まれます。

カスタマーコンテンツの所有権と管理権:

アクセス:

お客様は、自分のカスタマーコンテンツ、および AWS のサービスとリソースへのアクセスを管理します。お客様がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録の高性能な機能セットを用意しています (AWS CloudTrail など)。いかなる目的であっても、当社がお客様の同意なくカスタマーコンテンツにアクセスしたり、それを使用することはありません。

ストレージ:

コンテンツを保存するリージョンはお客様に選択していただけます。お客様の同意なしに、当社がカスタマーコンテンツを、お客様が選択したリージョンの外に移動したり複製したりすることはありません。

セキュリティ:

お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。

カスタマーコンテンツの開示:

法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービス

の利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。

セキュリティ保証:

当社では、お客様による当社のセキュリティ管理環境の確立、オペレーション、および活用をサポートするため、プライバシーとデータを保護するグローバルなベストプラクティスを使用したセキュリティ保証プログラムを展開しています。これらセキュリティの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、それぞれ個別に検証されています。

<https://aws.amazon.com/jp/compliance/data-privacy-faq/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えて

います。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、資産管理台帳を紙文書として管理する場合、不正閲覧・持ち出しなどの不正行為を検出・記録できる仕組みを構築することが推奨されます。

■ 推奨される追加の実施事項

資産管理台帳を格納するキャビネットや保管庫の鍵を別担当者管理とする、もしくは電子錠などとし、アクセスの記録を取得できる仕組みを構築することが推奨されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.1 資産台帳

(2)

■ 要求事項 60

推奨

資産台帳等に記録する情報には次のようなものが考えられる。

整理番号

資産の名称（医療情報の名称）

資産の医療情報としての種別

データ形式及び見読化手段

資産の所在地と複製の可否及び複製の所在地

資産を保存する情報処理装置、電子媒体の識別番号等

資産を扱う医療機関等業務の概要

情報処理事業者における管理責任者

設定されたアクセス権限とアクセス権限者

資産の発生日時、保有する期限、廃棄予定日

資産に対する処理の履歴（保存、配送、複製、廃棄等）

■ AWS のインフラストラクチャー関連事項

N/A

AWS では、お客様からの信頼を最優先にしています。AWS は 190 を超える国のエンタープライズ、教育機関、および政府機関を含む 100 万を超えるアクティブカスタマーにサービスを提供しています。金融サービスやヘルスケアの提供者、および政府機関といったお客様が私たちのことを信頼し、機密性の非常に高い情報を預けてくださっています。

AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、

AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。お客様からの信頼を維持することは継続的なコミットメントであり、今後も私たちが導入したプライバシーとデータセキュリティに関するポリシー、プラクティスおよびテクノロジーについてお知らせするよう努力を続けていきます。コミットメントには次のような事項が含まれます。

カスタマーコンテンツの所有権と管理権:

アクセス:

お客様は、自分のカスタマーコンテンツ、および AWS のサービスとリソースへのアクセスを管理します。お客様がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録の高性能な機能セットを用意しています (AWS CloudTrail など)。いかなる目的であっても、当社がお客様の同意なくカスタマーコンテンツにアクセスしたり、それを使用することはありません。

ストレージ:

コンテンツを保存するリージョンはお客様に選択していただけます。お客様の同意なしに、当社がカスタマーコンテンツを、お客様が選択したリージョンの外に移動したり複製したりすることはありません。

セキュリティ:

お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。

カスタマーコンテンツの開示:

法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。

セキュリティ保証:

当社では、お客様による当社のセキュリティ管理環境の確立、オペレーション、および活用をサポートするため、プライバシーとデータを保護するグローバルなベストプラクティスを使用したセキュリティ保証プログラムを展開しています。これらセキュリティの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、それぞれ個別に検証されています。

<https://aws.amazon.com/jp/compliance/data-privacy-faq/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内

で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。
Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key

Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、資産管理台帳に以下の管理項目を設け受領した医療情報を管理することが推奨されます。

整理番号

資産の名称（医療情報の名称）

資産の医療情報としての種別

データ形式及び見読化手段

資産の所在地と複製の可否及び複製の所在地

資産を保存する情報処理装置、電子媒体の識別番号等

資産を扱う医療機関等業務の概要

情報処理事業者における管理責任者

設定されたアクセス権限とアクセス権限者

資産の発生日時、保有する期限、廃棄予定日

資産に対する処理の履歴（保存、配送、複製、廃棄等）

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得, 開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7.2 情報資産管理

7.2.2 情報の分類

(1)

■ 要求事項 61

必須

情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。

■ AWS のインフラストラクチャー関連事項

N/A

AWS では、お客様からの信頼を最優先にしています。AWS は 190 を超える国のエンタープライズ、教育機関、および政府機関を含む 100 万を超えるアクティブカスタマーにサービスを提供しています。金融サービスやヘルスケアの提供者、および政府機関といったお客様が私たちのことを信頼し、機密性の非常に高い情報を預けてくださっています。

AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。お客様からの信頼を維持することは継続的なコミットメントであり、今後も私たちが導入したプライバシーとデータセキュリティに関するポリシー、プラクティスおよびテクノロジーについてお知らせするよう努力を続けていきます。コミットメントには次のような事項が含まれます。

カスタマーコンテンツの所有権と管理権:

アクセス:

お客様は、自分のカスタマーコンテンツ、および AWS のサービスとリソースへのアクセスを管理します。お客様がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録の高性能な機能セットを用意しています (AWS CloudTrail など)。いかなる目的であっても、当社がお客様の同意なくカスタマーコンテンツにアクセスしたり、それを使用することはありません。

ストレージ:

コンテンツを保存するリージョンはお客様に選択していただけます。お客様の同意なしに、当社がカスタマーコンテンツを、お客様が選択したリージョンの外に移動したり複製したりすることはありません。

セキュリティ:

お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。

カスタマーコンテンツの開示:

法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。

セキュリティ保証:

当社では、お客様による当社のセキュリティ管理環境の確立、オペレーション、および活用をサポートするため、プライバシーとデータを保護するグローバルなベストプラクティスを使用したセキュリティ保証プログラムを展開しています。これらセキュリティの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、それぞれ個別に検証されています。

<https://aws.amazon.com/jp/compliance/data-privacy-faq/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は受領した医療情報の種別決定の際（分類）に必要な指針および決定された種別毎に必要なリスク分析・管理方法の規定を行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.2 情報の分類

(2)

必須

情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。

■ AWS のインフラストラクチャー関連事項

N/A

AWS では、お客様からの信頼を最優先にしています。AWS は 190 を超える国のエンタープライズ、教育機関、および政府機関を含む 100 万を超えるアクティブカスタマーにサービスを提供しています。金融サービスやヘルスケアの提供者、および政府機関といったお客様が私たちのことを信頼し、機密性の非常に高い情報を預けてくださっています。

AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。お客様からの信頼を維持することは継続的なコミットメントであり、今後も私たちが導入したプライバシーとデータセキュリティに関するポリシー、プラクティスおよびテクノロジーについてお知らせするよう努力を続けていきます。コミットメントには次のような事項が含まれます。

カスタマーコンテンツの所有権と管理権:

アクセス:

お客様は、自分のカスタマーコンテンツ、および AWS のサービスとリソースへのアクセスを管理します。お客様がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録の高性能な機能セットを用意しています (AWS CloudTrail など)。いかなる目的であっても、当社がお客様の同意なくカスタマーコンテンツにアクセスしたり、それを使用することはありません。

ストレージ:

コンテンツを保存するリージョンはお客様に選択していただけます。お客様の同意なしに、当社がカスタマーコンテンツを、お客様が選択したリージョンの外に移動したり複製したりすることはありません。

セキュリティ:

お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。

カスタマーコンテンツの開示:

法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービス

の利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。

セキュリティ保証:

当社では、お客様による当社のセキュリティ管理環境の確立、オペレーション、および活用をサポートするため、プライバシーとデータを保護するグローバルなベストプラクティスを使用したセキュリティ保証プログラムを展開しています。これらセキュリティの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、それぞれ個別に検証されています。

<https://aws.amazon.com/jp/compliance/data-privacy-faq/>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者（所有者・管理責任者）は、情報資産の棚卸などを通じ情報の分類が正しく行われていることを情報資産の棚卸等を通じ定期的に確認する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.2 情報の分類

(3)

■ 要求事項 63

必須

預託される情報に対して分類にもとづいたリスク分析を実施すること。

■ AWS のインフラストラクチャー関連事項

N/A

AWS では、お客様からの信頼を最優先にしています。AWS は 190 を超える国のエンタープライズ、教育機関、および政府機関を含む 100 万を超えるアクティブカスタマーにサービスを提供しています。金融サービスやヘルスケアの提供者、および政府機関といったお客様が私たちのことを信頼し、機密性の非常に高い情報を預けてくださっています。

AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。お客様からの信頼を維持することは継続的なコミットメントであり、今後も私たちが導入したプライバシーとデータセキュリティに関するポリシー、プラクティスおよびテクノロジーについてお知らせするよう努力を続けていきます。コミットメントには次のような事項が含まれます。

カスタマーコンテンツの所有権と管理権:

アクセス:

お客様は、自分のカスタマーコンテンツ、および AWS のサービスとリソースへのアクセスを管理します。お客様がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録の高性能な機能セットを用意しています (AWS CloudTrail など)。いかなる目的であっても、当社がお客様の同意なくカスタマーコンテンツにアクセスしたり、それを使用することはありません。

ストレージ:

コンテンツを保存するリージョンはお客様に選択していただけます。お客様の同意なしに、当社がカスタマーコンテンツを、お客様が選択したリージョンの外に移動したり複製したりすることはありません。

セキュリティ:

お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。

カスタマーコンテンツの開示:

法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。

セキュリティ保証:

当社では、お客様による当社のセキュリティ管理環境の確立、オペレーション、および活用をサポートするため、プライバシーとデータを保護するグローバルなベストプラクティスを使用したセキュリティ保証プログラムを展開しています。これらセキュリティの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、それぞれ個別に検証されています。

<https://aws.amazon.com/jp/compliance/data-privacy-faq/>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は受領した医療情報の種別決定の際（分類）に必要な指針および決定された種別毎に必要なリスク分析・管理方法の規定を行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.2 情報の分類

(4)

■ 要求事項 64

必須

リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。

■ AWS のインフラストラクチャー関連事項

N/A

AWS では、お客様からの信頼を最優先にしています。AWS は 190 を超える国のエンタープライズ、教育機関、および政府機関を含む 100 万を超えるアクティブカスタマーにサービスを提供しています。金融サービスやヘルスケアの提供者、および政府機関といったお客様が私たちのことを信頼し、機密性の非常に高い情報を預けてくださっています。

AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。お客様からの信頼を維持することは継続的なコミットメントであり、今後も私たちが導入したプライバシーとデータセキュリティに関するポリシー、プラクティスおよびテクノロジーについてお知らせするよう努力を続けていきます。コミットメントには次のような事項が含まれます。

カスタマーコンテンツの所有権と管理権:

アクセス:

お客様は、自分のカスタマーコンテンツ、および AWS のサービスとリソースへのアクセスを管理します。お客様がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録の高性能な機能セットを用意しています (AWS CloudTrail など)。いかなる目的であっても、当社がお客様の同意なくカスタマーコンテンツにアクセスしたり、それを使用することはありません。

ストレージ:

コンテンツを保存するリージョンはお客様に選択していただけます。お客様の同意なしに、当社がカスタマーコンテンツを、お客様が選択したリージョンの外に移動したり複製したりすることはありません。

セキュリティ:

お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中

または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。

カスタマーコンテンツの開示:

法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。

セキュリティ保証:

当社では、お客様による当社のセキュリティ管理環境の確立、オペレーション、および活用をサポートするため、プライバシーとデータを保護するグローバルなベストプラクティスを使用したセキュリティ保証プログラムを展開しています。これらセキュリティの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、それぞれ個別に検証されています。

<https://aws.amazon.com/jp/compliance/data-privacy-faq/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は受領した医療情報の種別決定の際（分類）に必要な指針および決定された種別毎に必要なリスク分析・管理方法の規定を行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.2 情報の分類

(5)

■ 要求事項 65

必須

分類がわかるように情報にラベルをつけること（電磁的記録にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること）。

■ AWS のインフラストラクチャー関連事項

N/A

AWS では、お客様からの信頼を最優先にしています。AWS は 190 を超える国のエンタープライズ、教育機関、および政府機関を含む 100 万を超えるアクティブカスタマーにサービスを提供しています。金融サービスやヘルスケアの提供者、および政府機関といったお客様が私たちのことを信頼し、機密性の非常に高い情報を預けてくださっています。

AWS ではカスタマーコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツがどこに保存されるかをお客様ご自身に決定していただき、移動中でも保管中でもコンテンツを保護し、AWS のサービスとリソースに対するユーザーからのアクセスを管理できるようにしています。また、カスタマーコンテンツに対する不正なアクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。お客様からの信頼を維持することは継続的なコミットメントであり、今後も私たちが導入したプライバシーとデータセキュリティに関するポリシー、プラクティスおよびテクノロジーについてお知らせするよう努力を続けていきます。コミットメントには次のような事項が含まれます。

カスタマーコンテンツの所有権と管理権:

アクセス:

お客様は、自分のカスタマーコンテンツ、および AWS のサービスとリソースへのアクセスを管理します。お客様がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録の高性能な機能セットを用意しています（AWS CloudTrail など）。いかなる目的であっても、当社がお客様の同意なくカスタマーコンテンツにアクセスしたり、それを使用することはありません。

ストレージ:

コンテンツを保存するリージョンはお客様に選択していただけます。お客様の同意なしに、当社がカスタマーコンテンツを、お客様が選択したリージョンの外に移動したり複製したりすることはありません。

セキュリティ:

お客様は、自分のカスタマーコンテンツの安全をどのように確保するかを選択できます。私たちはお客様のために、移動中または保管中のコンテンツの強力な暗号化機能を準備しています。暗号化キーをお客様ご自身で管理するオプションも用意されています。

カスタマーコンテンツの開示:

法令、または政府機関もしくは規制当局による有効かつ拘束力のある命令を遵守するために必要な場合を除き、お客様のコンテンツを開示することはありません。そうすることが禁止されている場合または Amazon の製品もしくはサービスの利用に関連した違法行為の存在を明確に示すものがある場合を除き、Amazon ではカスタマーコンテンツの開示に先立ってお客様に通知し、お客様が開示からの保護を求められるようにします。

セキュリティ保証:

当社では、お客様による当社のセキュリティ管理環境の確立、オペレーション、および活用をサポートするため、プライバシーとデータを保護するグローバルなベストプラクティスを使用したセキュリティ保証プログラムを展開しています。これらセキュリティの保護プロセスおよび管理プロセスは、複数のサードパーティーによる独立した評価によって、それぞれ個別に検証されています。

<https://aws.amazon.com/jp/compliance/data-privacy-faq/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

譲歩処理事業者は、受領・分類した情報にラベル付けを行う必要があります。なお、電磁的記録へのラベリング方法については、詳細および安全性について医療機関等に確認・承認を得る必要があります。

■ 推奨される追加の実施事項

AWS では各種リソースにタグを付与することが可能です。

タグとは、AWS リソースに付けるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもお客様側が定義します。タグを使用すると、AWS リソースを目的、所有者、環境などさまざまな方法で分類することができます。同じ型のリソースが多い場合に役立ちます — 割り当てたタグに基づいて特定のリソースをすばやく識別できます。たとえば、アカウントの各インスタンスの所有者とスタックレベルを追跡しやすくするため、Amazon EC2 インスタンスに対して一連のタグを定義できます。

AWS 各種リソースへのタグ付けは以下 URL を参照ください。

Amazon EC2 リソースのタグ付け（EBS を含む）

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/Using_Tags.html#tag-basics

Amazon S3 リソースのタグ付け

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/object-tagging.html

Amazon Glacier リソースのタグ付け

https://docs.aws.amazon.com/ja_jp/amazonglacier/latest/dev/tagging.html

Amazon EFS リソースのタグ付け

https://docs.aws.amazon.com/ja_jp/efs/latest/ug/manage-fs-tags.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.2 情報の分類

(6)

■ 要求事項 66

必須

各ラベルに応じた処理方式（保存、配送、複製、廃棄等）を定めること。

■ AWS のインフラストラクチャー関連事項

N/A

デバイスの管理

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

<https://aws.amazon.com/jp/compliance/data-center/data-layer/>

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は受領した医療情報の種別決定の際（分類）に必要な指針および決定された種別毎に必要なリスク分析・管理方法の規定を行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.2 情報資産管理

7.2.2 情報の分類

(1)

■ 要求事項 67

推奨

情報の処理について履歴を取得し、資産台帳等に記録することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

デバイスの管理

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が

説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

<https://aws.amazon.com/jp/compliance/data-center/data-layer/>

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、受託した医療情報のすべてについて管理（受領、保存、配送、複製、編集、閲覧、廃棄等）に関する記録を上記で作成した資産管理台帳に記録する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.3 組織的安全管理策（体制、運用管理規程）

■ 要求事項 68

必須

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報処理にあたり組織的安全管理策を規定し以下を設置する必要があります。

- 情報セキュリティ基本方針の策定
- 管理・作業責任者の任命
- 作業手順書の整備
- 個人情報保護方針の策定・文書化

■ 推奨される追加の実施事項

情報セキュリティマネジメントシステム(ISMS)および個人情報管理システムを構築し、組織のプロセス及びマネジメント構造全体の一部とし、かつ、その中に組み込み、第三者の監査を受けることが推奨されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得, 開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

■ 要求事項 69

必須

医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、策定した情報セキュリティ基本方針を医療機関の求めに応じて提出できる状態にしておく必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.3 組織的安全管理策（体制、運用管理規程）

(2)

■ 要求事項 70

必須

個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、策定した個人情報保護方針を医療機関の求めに応じて提出できる状態にしておく必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.3 組織的安全管理策（体制、運用管理規程）

(3)

■ 要求事項 71

必須

個人情報保護に関しては、医療機関等の監督の下に行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、個人情報保護に関して医療機関等の監督の元実施する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.3 組織的安全管理策（体制、運用管理規程）

(4)

■ 要求事項 72

必須

情報処理の安全管理に関わる手順書、運用管理規程を整備すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、医療情報処理にあつた各作業を安全に取り扱うための手順書および運用管理規程を整備する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.3 組織的安全管理策（体制、運用管理規程）

(5)

■ 要求事項 73

必須

運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関等及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、運用管理規程に以下を盛り込む必要があります。

- 情報セキュリティに対する組織的取り組み方針
- 情報処理事業者内の体制及び施設、
- 外部事業者との契約書の管理
- 情報処理に関わるハードウェア・ソフトウェアの管理方法
AWS リソースの管理方法も含む
- リスクに対する予防およびリスク発現事の対応
- 医療情報を格納する媒体の管理
- 第三者による情報セキュリティ監査
- 問合せ窓口の設置・対応

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.4 医療情報の伝達経路におけるリスク評価

■ 要求事項 74

必須

医療情報の取扱に際しては高い機密性が求められていることに配慮しなければならない。機密性を確保するためには、医療情報の移動する範囲を限定することが必要である。情報の入り口から保管場所、電子媒体であれば適切な保護機能と一定の強度を備えた保管庫、電磁的記録であれば適切なアクセス管理を施されたデータベース、ファイルサーバ等に保存されるまでの経路、及び医療機関等に医療情報を提供する経路、最終的に情報を廃棄する経路を認識し、その経路上に存在する脅威を列挙してリスク評価を行うことが要求される。アプリケーション利用の場合には、アプリケーション固有の脅威を考慮する必要がある。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報が流通する経路および保管媒体をすべて洗い出し、想定されるリスクを評価する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A14.2

A.16 情報セキュリティインシデント管理

A.16.1

7.4 医療情報の伝達経路におけるリスク評価

■ 要求事項 75

必須

アプリケーション開発及び試験の段階で、これらの脆弱性を検出するための試験を十分に実施し、検出された脆弱性に対する対策を施すこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムの開発・試験の過程で脆弱性診断試験を実施し、検出された脆弱性に対する対策を実施する必要があります。

AWS では申請に基づき脆弱性検査を行うことが許可されるポリシーが確立されています。AWS のポリシーに基づき、「AWS 脆弱性/侵入テストリクエストフォーム」必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。

- ・すべての侵入テストに許可が必要です。

- ・許可をリクエストするには、テストを希望するインスタンスに関連付けられているルート認証情報を使用して、AWS ポータルにログインする必要があります。これを行わないと、フォームが正しく事前入力されません。サードパーティにテストの実施を依頼する場合は、フォームに必要事項を記入して、AWS から承認が下りた時点でサードパーティに通知する必要

があります。AWS では、サードパーティのテスト企業は承認されません。

・AWS のポリシーでは、以下のリソースに対するテストのみが許可されます。

EC2

RDS

Aurora

CloudFront

API ゲートウェイ

Lambda

Lightsail

DNS Zone Walking

・現時点において、AWS のポリシーでは、スモール RDS インスタンスまたはマイクロ RDS インスタンスのテストは許可されていません。m1.small、t1.micro、または t2.nano の EC2 インスタンスのテストは許可されていません。これは、他のお客様と共有する可能性のあるリソースのパフォーマンスに悪影響が及ぶ可能性を未然に防ぐためです。

詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.1 医療情報処理施設の建物に関する要求事項

(1)

■ 要求事項 76

必須

情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認すること。

-医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理が行われていること。

-傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。

- 建物、部屋に対する不正な物理的な侵入を抑止するため、監視カメラ等の侵入検知装置を導入すること。
- 自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。

■ AWS のインフラストラクチャー関連事項

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同等に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

ISO9001

ISO 9001 では、組織内で効率的な品質管理を実現するために必要な構造、責任、手順の文書化とレビューに対する、プロセス重視のアプローチについて概説されています。この標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

品質マニュアルの文書化、文書管理、決定プロセスの相互作用など、品質管理システムの要件

経営者の責任

人材および組織の作業環境など、リソースの管理

設計から納品までの手順を含むサービスの開発

顧客満足度

内部監査、是正措置、予防措置などの活動による QMS の測定、分析、改善

AWS における「品質」とは、機密性、可用性、整合性、セキュリティの要件を満たすことができる製品と機能と定義しています。

AWS の ISO9001 に関する詳細、最新情報は下記を参照ください。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

AWS のデータセンター

サイトの選択

AWS は、場所を選択する前に、始めに環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。当社のアベイラビリティゾーン間は物理的に分離されており、相互に独立して構築されています。

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

可用性

AWS は、システムの可用性を維持し、停止の場合にサービスを復元するために必要となる重要なシステムコンポーネントを特定しています。そうした重要なシステムコンポーネントは、アベイラビリティゾーンと呼ばれる複数の独立した場所にバックアップされます。各アベイラビリティゾーンは、高い信頼性を保ちながら、各々独立して運用するように設計されています。アベイラビリティゾーンはお互いに接続されているため、アベイラビリティゾーン間で自動的にフェイルオーバーすることで、中断なく実行できるようなアプリケーションを簡単に設計可能です。これにより、高いレジリエンシーと、サービスの可用性がもたらされることとなりますが、それは自ずとシステムデザインの一部として機能することになります。AWS のお客様は、アベイラビリティゾーンとデータレプリケーションの活用により、目標復旧時点と非常に短い目標復旧時間を実現し、

最高レベルのサービスの可用性を達成することも可能です。

物理アクセス

従業員によるデータセンターへのアクセス

AWS は、権限を持つ担当者のみデータセンターへの物理的なアクセスを許可しています。データセンターへのアクセスを必要とするすべての担当者は、まずアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づき許可されますが、個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があります。アクセスの期限が設定されます。申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。

第三者のデータセンターへのアクセス

第三者のアクセスについては、承認された AWS の担当者が申請する必要があり、その担当者は第三者によるアクセスを申請し、業務上の正当性を詳しく説明する必要があります。これらの申請は最少権限の原則に基づいて付与されます。申請では個人がアクセスを必要とするデータセンターのレイヤーを指定する必要があります。期限が設定されます。これらの申請は権限を持つ人物のみが審査して承認し、請求した期限が過ぎた後は、アクセスが取り消されます。入場を許可された担当者は、その権限で指定されたエリアのみに入場が制限されます。訪問者バッジを与えられた担当者は、現場への到着後身分証明書を提示して署名後に入場を許可され、権限を持つスタッフが常に付き添いを行います。

。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびこれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関して、詳細、最新情報は下記のサイトをご参照ください。

AWS コンプライアンス情報

<https://aws.amazon.com/jp/compliance/>

AWS セキュリティ情報

<https://aws.amazon.com/jp/security/>

AWS ISO 関連情報

<https://aws.amazon.com/jp/compliance/iso-27001-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27017-faqs/>

<https://aws.amazon.com/jp/compliance/iso-27018-faqs/>

<https://aws.amazon.com/jp/compliance/iso-9001-faqs/>

AWS FISC 関連情報

<https://aws.amazon.com/jp/compliance/fisc/>

AWS SOC 関連情報

<https://aws.amazon.com/jp/compliance/soc-faqs/>

AWS PCI DSS 情報

<https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/>

■ AWS サービス関連情報

-グローバルインフラストラクチャー

AWS クラウドは世界中の 18 個の地理的リージョンと 1 つのローカルリージョンにある 55 個のアベイラビリティゾーンで運用されており、さらに 4 つのリージョン（バーレーン、香港特別行政区、スウェーデン、米国で 2 番目の AWS GovCloud リージョン）と 12 個のアベイラビリティゾーンが追加される予定です。

AWS のリージョンとアベイラビリティゾーン

AWS クラウドインフラストラクチャーはリージョンとアベイラビリティゾーン ("AZ") を中心として構築されます。AWS リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立・隔離されたアベイラビリティゾーンがあります。これらのアベイラビリティゾーンを利用することで、従来の単一のデータセンターまたは複数のデータセンターインフラストラクチャーよりも優れた、高可用性と耐障害性を併せ持つアプリケーションやデータベースをより簡単・効率的にデザインおよび運用することができます。データまたはアプリケーションを更に広範囲に渡る地域に展開する必要があるお客様には、AWS ローカルリージョンが役立ちます。AWS ローカルリージョンは現在の AWS リージョンを補うための単一のデータセンターです。すべての AWS リージョンと同じように、AWS ローカルリージョンは完全に他の AWS リージョンから隔離されています。AWS クラウドは世界中の 18 個の地理的リージョンと 1 つのローカルリージョンにある 55 個のアベイラビリティゾーンで運用されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/about-aws/global-infrastructure/>

■ 情報処理事業者（お客様）の該当事項

AWS は米国における HIPAA に対応した医療情報システムのクラウド基盤として多くの事業者に利用された実績を有し、セキュアで柔軟かつ低コストのクラウドサービスを実現可能な AWS 環境において、医療情報システムの様々な要件に対応するため各種サービスや関連情報を提供していますが、情報処理事業者は AWS のデータセンターについて、不正アクセス防止、傍受、盗撮等の不正行為の防止、不正な物理的な侵入の防止、建物自体の防災対策が適切に実施されていることを確認する必要があります。

AWS セキュリティプロセスの概要については以下 URL を参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監

査中に外部の独立監査人によって確認されているため、情報処理事業者は、確認時点で有効な上記レポートおよび認証を確認することで、AWS がサービス実施時に適切な管理区域への立ち入り確認を実施していることを間接的に確認できます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策

(1)

■ 要求事項 77

必須

医療情報システムを設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策

(2)

■ 要求事項 78

必須

有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策

(3)

■ 要求事項 79

必須

有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認すること（履歴の保全については「7.6.12 ログの取得及び監査」を参照）。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるい

は領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策

(4)

■ 要求事項 80

必須

情報処理事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した情報処理事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、情報処理事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておくこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

- ① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策
- (5)

■ 要求事項 81

必須

情報処理事業者の職員は、情報処理事業者の専有する領域にて、情報処理事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策

(6)

必須

職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、情報処理事業者職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策

（7）

■ 要求事項 83

必須

情報処理事業者の職員の業務に応じて執務室内に滞在できる時間を指定すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策

(8)

■ 要求事項 84

必須

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合実施すべき安全管理策

(1)

■ 要求事項 85

推奨

機械式の認証装置で利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN40）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

- ② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合
(1)

■ 要求事項 86

必須

データセンターを運営する外部事業者が、①と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認すること。

■ AWS のインフラストラクチャー関連事項

データセンターのアクセス確認

データセンターへのアクセスは、定期的に確認されます。従業員がAmazon またはアマゾン ウェブ サービスの従業員でなくなった場合には、従業員記録が Amazon の HR システムで終了処理され、アクセス権は自動的に取り消されます。さらに、承認された申請期間に従って従業員または請負業者のアクセスの有効期限が切れると、その後に Amazon またはアマゾン ウェブ サービスの従業員である場合であっても、そのアクセス権限は速やかに取り消されます。

データセンターのアクセスログ

AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。

データセンターへのアクセスの監視

AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。

サーベイランスと検出

CCTV

サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ (CCTV) によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。

データセンターのエントリポイント

物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバイスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。

侵入検知

データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロセスとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合もあります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合もあります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は AWS のデータセンターについて、不正アクセス防止、傍受、盗撮等の不正行為の防止、不正な物理的な侵入の防止、建物自体の防災対策が適切に実施されていることを確認する必要があります。

AWS セキュリティプロセスの概要については以下 URL を参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されているため、情報処理事業者は、確認時点で有効な上記レポートおよび認証を確認することで、AWS がサービス実施時に適切な管理区域への立ち入り確認を実施していることを間接的に確認できます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

- ② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合
(2)

■ 要求事項 87

必須

医療情報システムの設置されるサーバラックには施錠を行い、定められた情報処理事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行うこと。

■ AWS のインフラストラクチャー関連事項

データセンターのアクセス確認

データセンターへのアクセスは、定期的に確認されます。従業員が Amazon またはアマゾン ウェブ サービスの従業員でなくなった場合には、従業員記録が Amazon の HR システムで終了処理され、アクセス権は自動的に取り消されます。さらに、承認された申請期間に従って従業員または請負業者のアクセスの有効期限が切れると、その後に Amazon またはアマゾン ウェブ サービスの従業員である場合であっても、そのアクセス権限は速やかに取り消されます。

データセンターのアクセスログ

AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。

データセンターへのアクセスの監視


AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。

サーベイランスと検出

CCTV

サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ (CCTV) によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。

データセンターのエントリポイント

物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバイスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。

侵入検知

データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アク

セス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロシージャとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合があります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合があります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は AWS のデータセンターについて、不正アクセス防止、傍受、盗撮等の不正行為の防止、不正な物理的な侵入の防止、建物自体の防災対策が適切に実施されていることを確認する必要があります。

AWS セキュリティプロセスの概要については以下 URL を参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監

査中に外部の独立監査人によって確認されているため、情報処理事業者は、確認時点で有効な上記レポートおよび認証を確認することで、AWS がサービス実施時に適切な管理区域への立ち入り確認を実施していることを間接的に確認できます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合 (3)

■ 要求事項 88

必須

情報処理事業者が医療情報システムの設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録すること。

■ AWS のインフラストラクチャー関連事項

データセンターのアクセス確認

データセンターへのアクセスは、定期的に確認されます。従業員が Amazon またはアマゾン ウェブ サービスの従業員でなくなった場合には、従業員記録が Amazon の HR システムで終了処理され、アクセス権は自動的に取り消されます。さらに、承認された申請期間に従って従業員または請負業者のアクセスの有効期限が切れると、その後に Amazon またはアマゾン ウェブ サービスの従業員である場合であっても、そのアクセス権限は速やかに取り消されます。

データセンターのアクセスログ

AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。

データセンターへのアクセスの監視


AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。

サーベイランスと検出

CCTV

サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ (CCTV) によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。

データセンターのエントリポイント

物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバイスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。

侵入検知

データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロシージャとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合もあります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合もあります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

- AWS ではデータセンターへの立ち入りが許可されていないため、情報処理事業者がサーバラックを開錠することはありません。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

- ② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合
(4)

■ 要求事項 89

必須

データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム、医療情報に影響を与えないことを確認すること。

■ AWS のインフラストラクチャー関連事項

データセンターのアクセス確認

データセンターへのアクセスは、定期的に確認されます。従業員が Amazon またはアマゾン ウェブ サービスの従業員でなくなった場合には、従業員記録が Amazon の HR システムで終了処理され、アクセス権は自動的に取り消されます。さらに、承認された申請期間に従って従業員または請負業者のアクセスの有効期限が切れると、その後に Amazon またはアマゾン ウェブ サービスの従業員である場合であっても、そのアクセス権限は速やかに取り消されます。

データセンターのアクセスログ

AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。

データセンターへのアクセスの監視

AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。

サーベイランスと検出

CCTV

サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ (CCTV) によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。

データセンターのエントリポイント

物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用い

て、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバイスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。

侵入検知

データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロシージャとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合もあります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合もあります。また、監査人は電子アクセス制御デバイスや監視カメラなど

の機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS Personal Health Dashboard を利用することで、医療情報システムに影響を与える可能性がある変更の予定に関する事前通知を受け取ることができます。この通知を利用し、医療情報システムへの影響を確認することが求められます。

AWS Personal Health Dashboard の積極的な通知

ダッシュボードでは将来の見通しに関する通知も利用でき、E メールやモバイル通知などの複数のチャネルでアラートを設定することが可能なため、適切なタイミングで重要な情報を受け取って、影響を与える可能性がある変更予定を計画的に立てることができます。たとえば、EC2 インスタンスのいずれかに影響する可能性のある AWS ハードウェアメンテナンスアクティビティが発生した場合には、計画を立てるのに役立つ情報が含まれるアラートを受け取って、来たるべき変更に関連する問題に対し事前に対応できます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

- ② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合
(5)

■ 要求事項 90

必須

医療情報システムであることが、同じデータセンター内に立ち入る他事業者にはわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしないこと。

■ AWS のインフラストラクチャー関連事項

データセンターのアクセス確認

データセンターへのアクセスは、定期的に確認されます。従業員が Amazon またはアマゾン ウェブ サービスの従業員でなくなった場合には、従業員記録が Amazon の HR システムで終了処理され、アクセス権は自動的に取り消されます。さらに、承認された申請期間に従って従業員または請負業者のアクセスの有効期限が切れると、その後に Amazon またはアマゾン ウェブ サービスの従業員である場合であっても、そのアクセス権限は速やかに取り消されます。

データセンターのアクセスログ

AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。

データセンターへのアクセスの監視

AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもちています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。

サーベイランスと検出

CCTV

サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ (CCTV) によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。

データセンターのエントリポイント

物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバイスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。

侵入検知

データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロセスとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合もあります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合もあります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合

(1)

■ 要求事項 91

推奨

医療情報システムの設置されるサーバラックの施錠装置については、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

■ AWS のインフラストラクチャー関連事項

データセンターのアクセス確認

データセンターへのアクセスは、定期的に確認されます。従業員が Amazon またはアマゾン ウェブ サービスの従業員でなくなった場合には、従業員記録が Amazon の HR システムで終了処理され、アクセス権は自動的に取り消されます。さらに、承認された申請期間に従って従業員または請負業者のアクセスの有効期限が切れると、その後に Amazon またはアマゾン ウェブ サービスの従業員である場合であっても、そのアクセス権限は速やかに取り消されます。

データセンターのアクセスログ

AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。

データセンターへのアクセスの監視

AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。

サーベイランスと検出

CCTV

サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ（CCTV）によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。

データセンターのエントリポイント

物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバイスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。

侵入検知

データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、

技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロシージャとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合もあります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合もあります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

③ 外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合 (1)

■ 要求事項 92

必須

サーバ環境を運営する外部事業者が、①及び②と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認すること。

■ AWS のインフラストラクチャー関連事項

(①及び②の安全管理策については上記①及び②をご参照ください。)

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御

できます。

Amazon VPC は、セキュリティグループやネットワークアクセス制御リストなどの高度なセキュリティ機能を提供し、インスタンスレベルおよびサブネットレベルで受信/送信に対してフィルタリングが可能です。加えて、Amazon S3 に格納したデータはアクセスを制限することができるので、VPC 内のインスタンスからのみアクセスを許可することも可能となります。必要に応じて、さらなる分離を目的としたカスタマーごとに占有ハードウェア上で実行するハードウェア専用インスタンスを起動することもできます。

<https://aws.amazon.com/jp/vpc/>

ハードウェア専用インスタンスは、お客様専用のハードウェアの VPC で実行される Amazon EC2 インスタンスです。ハードウェア専用インスタンスは、他の AWS アカウントに属するインスタンスとは、ホストハードウェアのレベルで物理的に分離されます。

<https://aws.amazon.com/jp/ec2/purchasing-options/dedicated-instances/>

■ AWS サービス関連情報

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は AWS のデータセンターについて、不正アクセス防止、傍受、盗撮等の不正行為の防止、不正な物理的な侵入の防止、建物自体の防災対策が適切に実施されていることを確認する必要があります。

AWS セキュリティプロセスの概要については以下 URL を参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されているため、情報処理事業者は、確認時点で有効な上記レポートおよび認証を確認することで、AWS がサービス実施時に適切な管理区域への立ち入り確認を実施していることを間接的に確認できます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(1)

■ 要求事項 93

必須

不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持すること。

■ AWS のインフラストラクチャー関連事項

デバイスの管理

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、完全に停止するまで AWS の統制から除外されることはありません。

データセンターのアクセス確認

データセンターへのアクセスは、定期的に確認されます。従業員が Amazon またはアマゾン ウェブ サービスの従業員でなくなった場合には、従業員記録が Amazon の HR システムで終了処理され、アクセス権は自動的に取り消されます。さらに、承認された申請期間に従って従業員または請負業者のアクセスの有効期限が切れると、その後に Amazon またはアマゾン ウェブ サービスの従業員である場合であっても、そのアクセス権限は速やかに取り消されます。

データセンターのアクセスログ

AWS データセンターへの物理アクセスは、記録、監視され、そうした情報は保持されることになります。AWS は論理的および物理的なモニタリングシステムから取得した情報を、必要に応じてセキュリティを向上させるために相関性を確認します。

データセンターへのアクセスの監視

AWS ではグローバルセキュリティオペレーションセンターを使用してデータセンターを監視しています。このグローバル・セキュリティ・オペレーションセンターは、モニタリング、対処優先順位の決定、および決定された処理を実施について責任をもっています。データセンターのアクセスを管理、モニタリングし、ローカルのチームと関連サポートチームと協力し、対処優先順位の決定、コンサルティング、分析、送信を行い、24 時間 365 日グローバルレベルのサポートを提供しています。

サーベイランスと検出

CCTV

サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ（CCTV）によって録画されています。画像イメージは、法律およびコンプライアンスに関する要件に従って保持されます。

データセンターのエントリポイント

物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。権限を付与されたスタッフは、多要素認証のメカニズムを利用してデータセンターにアクセスします。サーバールームへの入り口は、ドアがこじ開けられた場合や開け放したままの場合にデバ

イスでアラームを鳴らし、インシデント対応を開始するように設置された装置で保護されています。

侵入検知

データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。サーバールームの入り口および出口は、入場または退場が許可される際に多要素認証を各個人に求める装置で保護されています。これらのデバイスは、許可なくドアがこじ開けられた場合や開け放したままの場合にはアラームを鳴らします。また、ドアのアラームデバイスは、多要素認証を提供せずにデータレイヤーに入場または退場した事例を検出するよう設定されてもいます。アラームは即時のログ記録、分析、および応答のため、24 時間 365 日にわたり AWS セキュリティオペレーションセンターに即時に送信されます。

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロシージャとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合もあります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合もあります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

-AWS Systems Manager

AWS Systems Manager は、AWS でご利用のインフラストラクチャーを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェースで AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager では、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon RDS インスタンスなどのリソースをアプリケーションごとにグループ化し、運用データを表示できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができます。また、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャーでも安全に運用、管理できます。

詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/systems-manager/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムを構成する AWS リソースのリストを作成・維持する必要があります。

■ 推奨される追加の実施事項

AWS Systems Manager を利用することで、EC2 などの仮想サーバのインスタンスのインベントリ情報を収集・リスト化することが可能です。

AWS Systems Manager では、インスタンスとそこにインストールされたソフトウェアに関する情報が収集されるため、システムの設定とインストールされたアプリケーションを把握するのに役立ちます。アプリケーション、ファイル、ネットワーク設定、Windows サービス、レジストリ、サーバーロール、アップデート、およびその他のシステムプロパティに関するデータを収集できます。収集したデータを利用して、アプリケーションアセットの管理、ライセンスの追跡、ファイル整合性のモニタリング、従来のインストーラによってインストールされていないアプリケーションの検出などを行えます。

AWS Systems Manager の詳細については以下 URL を参照ください。

<https://aws.amazon.com/jp/systems-manager/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(2)

■ 要求事項 94

必須

医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS Systems Manager

AWS Systems Manager は、AWS でご利用のインフラストラクチャーを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェースで AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager では、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon RDS インスタンスなどのリソースをアプリケーションごとにグループ化し、運用データを表示できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができます。また、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャーでも安全に運用、管理できます。

詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/systems-manager/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムを構成する仮想サーバーなどの AWS リソースに不要なアプリケーションをインストールしないことが必要です。

■ 推奨される追加の実施事項

AWS Systems Manager を利用することで、EC2 などの仮想サーバのインスタンスのインベントリ情報を収集・リスト化することが可能です。収集された情報を基に、必要なアプリケーションのみがインストールされているか否かを確認いただくことができます。

AWS Systems Manager では、インスタンスとそこにインストールされたソフトウェアに関する情報が収集されるため、システムの設定とインストールされたアプリケーションを把握するのに役立ちます。アプリケーション、ファイル、ネットワーク設定、Windows サービス、レジストリ、サーバーロール、アップデート、およびその他のシステムプロパティに関するデータを収集できます。収集したデータを利用して、アプリケーションアセットの管理、ライセンスの追跡、ファイル整合性のモニタリング、従来のインストーラによってインストールされていないアプリケーションの検出などを行えます。

AWS Systems Manager の詳細については以下 URL を参照ください。

<https://aws.amazon.com/jp/systems-manager/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

(3)

■ 要求事項 95

必須

医療情報等が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムにアクセスする端末について覗き見防止フィルター等のセキュリティ対策を実施する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(4)

■ 要求事項 96

必須

医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにすること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は医療情報システムのアプリケーションとして、端末上に永続的に医療情報が保存されない仕組みを構築することが求められます。

■ 推奨される追加の実施事項

AWS Workspaces を用いることで、仮想デスクトップ環境（VDI）を構築することができ、端末に医療情報を含むデータを保存することなく医療情報システムの利用環境を提供することが可能です。

データを安全に保つ

Amazon WorkSpaces は Amazon 仮想プライベートネットワーク（VPC）内でデプロイされ、各ユーザーに永続的に暗号化されたストレージボリューム AWS クラウド内で与え、AWS Key Management Service（KMS）と統合します。ローカルデバイスにはユーザーデータは保存されません。そのためユーザーデータのセキュリティは向上し、全体的なリスク表面積は減少します。

AWS Workspaces の詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/workspaces/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(5)

■ 要求事項 97

必須

火災発生時の消火設備が機器に損傷を与えないよう配慮すること。

■ AWS のインフラストラクチャー関連事項

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

運用サポートシステム

パワー

データセンターの電力システムは、完全に冗長化され、運用に影響を与えることなく管理が可能となっています。1 日 24 時間体制で、年中無休で稼働しています。AWS は、施設内の重要かつ不可欠な業務に対応するために、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源がデータセンターに備わっていることを保証しています。

空調と温度

AWS データセンターは、環境を制御するとともに、サーバーやその他のハードウェアの適切な運用温度を保ち、過熱を防ぎ、サーバー停止の可能性を減らすためのメカニズムを使用しています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。

火災検出と鎮火

AWS データセンターは、自動火災検出システムおよび鎮火システムが設置されています。火災検出システムにおいては、ネットワークスペース、機械的スペース、インフラストラクチャスペース内で煙検出センサーが使用されています。また、これらのエリアは鎮火システムによっても保護されています。

漏水検出

漏水を検出するため、AWS は水があることを検出するシステムをデータセンターに備えています。水が検出された場合、それ以上の水害を防ぐために水を除去するメカニズムが備わっています。

インフラストラクチャーのメンテナンス

設備の保守

AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内の

システムの継続的な運用性を維持しています。機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。

環境管理

AWS は、問題の速やかな特定を可能にするため、電氣的、機械的なシステムおよび設備をモニタリングしています。これは継続的な監査ツールと、建物管理および電氣的なモニタリングシステムを通じて提供される情報を利用して行われます。予防的メンテナンスが実行され、設備の運用に関しての継続性が保たれています。

緊急時に備えたバックアップ装置

水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。チームおよびシステムは、温度と湿度を監視して制御することで、過熱を防止し、サービス停止が起こらないようにします。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(6)

■ 要求事項 98

必須

医療情報システムを配置する室内での喫煙、飲食を禁止すること。

■ AWS のインフラストラクチャー関連事項

レイヤーごとのアクセスレビュー

他のレイヤーと同じように、インフラストラクチャー・レイヤーへのアクセスは業務ニーズに基づくように制限されています。レイヤーごとのアクセス確認が実装され、各レイヤーに立ち入る権限については、デフォルトでは付与されません。特定のレイヤーに立ち入る具体的なニーズがある場合のみ、そのレイヤーへの限定したアクセスが許可されます。

装置の保守点検は日常業務の一環

AWS チームは、マシン、ネットワーク、およびバックアップ装置に対する診断を実行し、常時および緊急時に正常に稼働していることを確認しています。データセンターの装置およびユーティリティに対する日常保守点検は、日常業務の一環です。

緊急時に備えたバックアップ装置

水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。チームおよびシステムは、温度と湿度を監視して制御することで、過熱を防止し、サービス停止が起こらないようにします。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(7)

■ 要求事項 99

必須

医療情報システムを配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮すること。

■ AWS のインフラストラクチャー関連事項

レイヤーごとのアクセスレビュー

他のレイヤーと同じように、インフラストラクチャー・レイヤーへのアクセスは業務ニーズに基づくように制限されています。レイヤーごとのアクセス確認が実装され、各レイヤーに立ち入る権限については、デフォルトでは付与されません。特定のレイヤーに立ち入る具体的なニーズがある場合のみ、そのレイヤーへの限定したアクセスが許可されます。

装置の保守点検は日常業務の一環

AWS チームは、マシン、ネットワーク、およびバックアップ装置に対する診断を実行し、常時および緊急時に正常に稼働

していることを確認しています。データセンターの装置およびユーティリティに対する日常保守点検は、日常業務の一環です。

緊急時に備えたバックアップ装置

水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。チームおよびシステムは、温度と湿度を監視して制御することで、過熱を防止し、サービス停止が起こらないようにします。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(8)

■ 要求事項 100

必須

それぞれの装置は製造元または供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行うこと。

■ AWS のインフラストラクチャー関連事項

レイヤーごとのアクセスレビュー

他のレイヤーと同じように、インフラストラクチャー・レイヤーへのアクセスは業務ニーズに基づくように制限されています。レイヤーごとのアクセス確認が実装され、各レイヤーに立ち入る権限については、デフォルトでは付与されません。特定のレイヤーに立ち入る具体的なニーズがある場合のみ、そのレイヤーへの限定したアクセスが許可されます。

装置の保守点検は日常業務の一環

AWS チームは、マシン、ネットワーク、およびバックアップ装置に対する診断を実行し、常時および緊急時に正常に稼働していることを確認しています。データセンターの装置およびユーティリティに対する日常保守点検は、日常業務の一環です。

緊急時に備えたバックアップ装置

水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。チームおよびシステムは、温度と湿度を監視して制御することで、過熱を防止し、サービス停止が起こらないようにします。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムを構成する AWS リソースとして Amazon EC2 などを使用している場合は、AWSより通知されるHWの交換通知（Retirement Notice）を確認し、メンテナンスに伴うHWの停止前に他HWへの仮想サーバーの移動を計画する必要があります。

詳細は以下 URL を参照ください。

Amazon EC2 インスタンスのリタイア

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/instance-retirement.html

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(9)

■ 要求事項 101

必須

保守点検で障害不良等が発見された際の対応作業等を行う際には情報処理事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにすること。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消

去してから持ち出すこと。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択すること。

■ AWS のインフラストラクチャー関連事項

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにす

るとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロセスとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合があります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合があります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

(10)

■ 要求事項 102

必須

医療情報システムを設置するサーバラックについては以下の安全管理策を実施すること。

- 震災時に転倒することが無いよう確実に設置すること。
- 熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されていること。
- 扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。

■ AWS のインフラストラクチャー関連事項

AWS のデータセンターでは、最新式の革新的な建築的、工学的アプローチを採用しています。AWS は大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWS プラットフォームとそのインフラストラクチャーに活かされているものです。AWS は日本に存在する AWS サービスで利用されるデータセンターに対する地球科学的な変化のリスクを考慮し、最新式の免震装置の採用を始めとして、そのようなリスクの影響を最小限にするために真剣に取り組んできました。日本のデータセンターは日本の震災に関する規格に準拠するように設計されています。AWS におけるデータセンターの事業継続性は、Amazon Infrastructure Group の指示に従って管理されています。

<https://aws.amazon.com/jp/compliance/jp-dr-considerations/>

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

運用サポートシステム

パワー

データセンターの電力システムは、完全に冗長化され、運用に影響を与えることなく管理が可能となっています。1 日 24 時間体制で、年中無休で稼働しています。AWS は、施設内の重要かつ不可欠な業務に対応するために、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源がデータセンターに備わっていることを保証しています。

空調と温度

AWS データセンターは、環境を制御するとともに、サーバーやその他のハードウェアの適切な運用温度を保ち、過熱を防ぎ、サーバー停止の可能性を減らすためのメカニズムを使用しています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。

火災検出と鎮火

AWS データセンターは、自動火災検出システムおよび鎮火システムが設置されています。火災検出システムにおいては、ネットワーキングスペース、機械的スペース、インフラストラクチャスペース内で煙検出センサーが使用されています。また、これらのエリアは鎮火システムによっても保護されています。

漏水検出

漏水を検出するため、AWS は水があることを検出するシステムをデータセンターに備えています。水が検出された場合、それ以上の水害を防ぐために水を除去するメカニズムが備わっています。

インフラストラクチャーのメンテナンス

設備の保守

AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。

環境管理

AWS は、問題の速やかな特定を可能にするため、電氣的、機械的なシステムおよび設備をモニタリングしています。これは継続的な監査ツールと、建物管理および電氣的なモニタリングシステムを通じて提供される情報を利用して行われます。予防的なメンテナンスが実行され、設備の運用に関しての継続性が保たれています。

緊急時に備えたバックアップ装置

水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。チームおよびシステムは、温度と湿度を監視して制御することで、過熱を防止し、サービス停止が起こらないようにします。

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に

従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロシージャとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティーの監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合もあります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合もあります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

■ 要求事項 103

必須

起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「7.6.14 作業者アクセス及び作業者 ID の管理」に従うこと。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。（<https://aws.amazon.com/jp/compliance/resources/>） AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact（<https://console.aws.amazon.com/artifact>）を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(12)

■ 要求事項 104

必須

情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施すること。

■ AWS のインフラストラクチャー関連事項

冗長性

データセンターは、サービスレベルを維持しつつも、障害を未然に防ぐように、また障害に耐え得るように設計されています。障害時には、自動プロセスによって、影響のあったエリアからトラフィックが移動されます。重要なアプリケーションは N+1 の基準でデプロイされています。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

ビジネス継続性と災害復旧

BCP(BUSINESS CONTINUITY PLAN) ; 事業継続計画

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

運用サポートシステム

パワー

データセンターの電力システムは、完全に冗長化され、運用に影響を与えることなく管理が可能となっています。1 日 24 時間体制で、年中無休で稼働しています。AWS は、施設内の重要かつ不可欠な業務に対応するために、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源がデータセンターに備わっていることを保証しています。

空調と温度

AWS データセンターは、環境を制御するとともに、サーバーやその他のハードウェアの適切な運用温度を保ち、過熱を防ぎ、サーバー停止の可能性を減らすためのメカニズムを使用しています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。

火災検出と鎮火

AWS データセンターは、自動火災検出システムおよび鎮火システムが設置されています。火災検出システムにおいては、ネットワークスペース、機械的スペース、インフラストラクチャスペース内で煙検出センサーが使用されています。また、これらのエリアは鎮火システムによっても保護されています。

漏水検出

漏水を検出するため、AWS は水があることを検出するシステムをデータセンターに備えています。水が検出された場合、それ以上の水害を防ぐために水を除去するメカニズムが備わっています。

インフラストラクチャーのメンテナンス

設備の保守

AWS は電気および機械に関連する設備をモニタリングし、予防的なメンテナンスを実施して、AWS データセンター内のシステムの継続的な運用性を維持しています。機器のメンテナンス手順は資格を持っている担当者が実行し、文書化されたメンテナンススケジュールに従って完了されます。

環境管理

AWS は、問題の速やかな特定を可能にするため、電氣的、機械的なシステムおよび設備をモニタリングしています。これは継続的な監査ツールと、建物管理および電氣的なモニタリングシステムを通じて提供される情報を利用して行われます。予防的なメンテナンスが実行され、設備の運用に関しての継続性が保たれています。

緊急時に備えたバックアップ装置

水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。チームおよびシステムは、温度と湿度を監視して制御することで、過熱を防止し、サービス停止が起こらないようにします。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS リソースに障害が発生した際も業務継続が可能なように、Multi-AZ 構成での冗長化・バックアップ対策を実施することが求められます。

■ 推奨される追加の実施事項

なお、AWS の SLA は Multi-AZ 構成が前提となっているため、SLA の適用を受ける意味でも Multi-AZ 構成でのシステム構築を推奨します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(13)

■ 要求事項 105

必須

不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用すること。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、

「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。(<https://aws.amazon.com/jp/compliance/resources/>) AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact (<https://console.aws.amazon.com/artifact>) を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

悪意のあるソフトウェアに対する AWS のプログラム、プロセス、および手続きは、ISO 27001 規格に合わせています。詳細については、ISO 27001 規格の附属書 A ドメイン 12 を参照してください。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになり

ます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/I144>

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.3 情報処理装置のセキュリティ

(1)

■ 要求事項 106

推奨

情報伝送に用いるケーブル類については直接の傍受リスクについて配慮することが望ましい。

■ AWS のインフラストラクチャー関連事項

データレイヤー

テクノロジーとチームの連携によるセキュリティの強化

データレイヤーに立ち入るための許可を取得するには、必須の手順があります。これには、承認されたユーザーによる、アクセス申請の確認と承認が含まれます。この間に、脅威検知システムと電子的な侵入検知システムで監視し、脅威や不審な行動が確認された場合は、自動的にアラートをトリガーします。たとえば、ドアを無理やり開けたり、解放したままにするとアラームが起動されることになります。監視カメラの配備と録画映像の保存については、法律および契約上の要件に従っています。

物理的および技術的な侵入の阻止

サーバールームへのアクセスポイントは、多要素認証を義務付ける電子制御デバイスで厳重に保護されています。また、技術的な侵入を阻止するためにも備えがあります。AWS サーバーはデータの削除を試みる従業員に警告することができます。万一、違反が発生した場合には、サーバーが自動的に無効化されます。

サーバーとメディアの厳重な監視

ユーザーデータの保存に使用されるメディアストレージデバイスは「クリティカル」と分類されて、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている技法を使用してメディアを停止します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制対象です。

サードパーティーの監査者によるプロセスとシステムの検証

AWS は、2,600 を超える要件について、1 年を通じて外部の監査機関による監査を受けています。サードパーティー

の監査人が当社データセンターを監査する場合、セキュリティの認証を受けるために必要な規定のルールに従っているかどうか厳密に査察されます。コンプライアンスプログラムとその要件によっては、メディアの取り扱い方と廃棄の方法について外部の監査人が従業員を面接する場合があります。また、監査人は監視カメラの録画内容を確認したり、データセンターのすべての入り口や通路を確認したりする場合があります。また、監査人は電子アクセス制御デバイスや監視カメラなどの機器をしばしば検査します。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.4 情報処理装置の廃棄及び再利用に関する要求事項

(1)

■ 要求事項 107

必須

ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認すること。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、

NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、完全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。

このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者自身でワイプ作業を行うこともできます。

ハードディスク消去ツール等を用い情報処理システムで利用する論理ディスク内のデータの消去が可能ですので、物理的なハードディスクのデータ消去に頼ることなく、論理的にディスク消去を実施・確認することが推奨されます。

■ 推奨される追加の実施事項

情報処理事業者自身で Amazon EBS のワイプ作業を行うこともできます。また、AWS 上に格納する機密データは、AWS Key Management Service で管理される暗号鍵を利用して暗号化することを推奨します。契約終了時に暗号鍵そのものを廃棄することで、データ消去に相当するといった対応を考慮することも可能となります。

Amazon Elastic Block Store (EBS) で追加のストレージを使う場合などはボリュームを暗号化することができます。S3を使う場合は Server Side Encryption でバケット・ファイル単位に暗号化することができます。また、サーバサイド暗号化のみでなく、必要に応じてクライアントサイド暗号化の利用を検討してください。

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.4 情報処理装置の廃棄及び再利用に関する要求事項

(2)

■ 要求事項 108

必須

サーバ等の BIOS パスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去すること。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信

信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.4 情報処理装置の廃棄及び再利用に関する要求事項

(3)

■ 要求事項 109

必須

ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証すること。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、

監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.4 情報処理装置の廃棄及び再利用に関する要求事項

(4)

■ 要求事項 110

必須

ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等の求めに応じ、速やかに提出できるよう整備すること。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション（CRR）は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者自身でワイプ作業を行うこともできます。

ハードディスク消去ツール等を用い情報処理システムで利用する論理ディスク内のデータの消去が可能ですので、物理的なハードディスクのデータ消去に頼ることなく、論理的にディスク消去を実施・確認することができます。情報処理事業者は、自身の統制下でデータの消去措置の実施記録が提出できるようワイプ作業を実施・記録を行うことが求められます。

■ 推奨される追加の実施事項

情報処理事業者自身で Amazon EBS のワイプ作業を行うこともできます。また、AWS 上に格納する機密データは、AWS Key Management Service で管理される暗号鍵を利用して暗号化することを推奨します。契約終了時に暗号鍵そのものを廃棄することで、データ消去に相当するといった対応を考慮することも可能となります。

Amazon Elastic Block Store (EBS) で追加のストレージを使う場合などはボリュームを暗号化することができます。S3を使う場合は Server Side Encryption でバケット・ファイル単位に暗号化することができます。また、サーバサイド暗号化のみでなく、必要に応じてクライアントサイド暗号化の利用を検討してください。

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.4 情報処理装置の廃棄及び再利用に関する要求事項

(1)

■ 要求事項 111

推奨

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション（CRR）は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS 上でデータの統制と所有権を有していますので、要件に応じてデータの保持を管理するのは情報処理事業者の責任です。

ハードディスク消去ツール等を用い情報処理システムで利用する論理ディスク内のデータの消去が可能ですので、物理的なハードディスクのデータ消去に頼ることなく、論理的にディスク消去を実施・確認することができます。情報処理事業者は、自身の統制下でデータの消去措置の実施記録が提出できるようワイプ作業を実施・記録を行うことが求められます。

■ 推奨される追加の実施事項

情報処理事業者自身で Amazon EBS のワイプ作業を行うこともできます。また、AWS 上に格納する機密データは、AWS Key Management Service で管理される暗号鍵を利用して暗号化することを推奨します。契約終了時に暗号鍵そのものを廃棄することで、データ消去に相当するといった対応を考慮することも可能となります。

Amazon Elastic Block Store (EBS) で追加のストレージを使う場合などはボリュームを暗号化することができます。S3 を使う場合は Server Side Encryption でバケット・ファイル単位に暗号化することができます。また、サーバサイド暗号化のみでなく、必要に応じてクライアントサイド暗号化の利用を検討してください。

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

■ 要求事項 112

推奨

保存されている情報の重要性に合わせて適切な方式を選択し、医療機関等側に選択の合理的な理由を説明、合意を得た上で実施することが望ましい。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を

保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。

Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション（CRR）は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。I6

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐

久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。

Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。

<https://aws.amazon.com/jp/iam/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS 上でデータの統制と所有権を有していますので、要件に応じてデータの保持を管理するのは情報処理事業者の責任です。

情報処理事業者は医療機関等との合意形成のプロセスを策定し、情報の重要性毎に適切な廃棄・消去方法を SLA などで明示し、プロセスに則り医療機関等に説明し合意を得たうえで実施することが推奨されます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.5 情報処理装置の外部への持ち出しに関する要求事項

(1)

■ 要求事項 113

必須

情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.5 情報処理装置の外部への持ち出しに関する要求事項

■ 要求事項 114

必須

持ち出した機器を再度設置するための適切な検証手順を策定すること。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を 保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追 跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイ クルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終 的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、 NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安 全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.5 情報処理装置の外部への持ち出しに関する要求事項

(1)

■ 要求事項 115

推奨

持ち出し手順に含まれる事項には次のようなものが考えられる。

- 装置の持ち出し申請書のフォーマット（申請者情報、承認者情報、対象機器情報、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失・損傷した場合の対応策、等）
- 申請承認プロセス
- 返却確認プロセス、等。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

- 情報処理事業者が AWS リソースを構成する情報処理装置を持ち出すことはできません。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.5 物理的安全対策

7.5.5 情報処理装置の外部への持ち出しに関する要求事項

■ 要求事項 116

推奨

返却時の検証手順に含まれる事項には次のようなものが考えられる。

- 装置の動作確認
- 盗聴装置等、情報の安全性を脅かす装置の有無
- 悪意のあるプログラムの検出作業
- 収められている情報の検証作業（不正な改ざん等）、等。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を 保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追 跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイ クルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終 的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、 NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安 全に停止するまで AWS の統制から除外されることはありません。

最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

- 情報処理事業者が AWS リソースを構成する情報処理装置を持ち出すことはできません。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(1)

■ 要求事項 117

必須

保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。

■ AWS のインフラストラクチャー関連事項

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

装置の保守点検 AWS チームは、マシン、ネットワーク、およびバックアップ装置に対する診断を実行し、常時および緊急時に正常に稼働していることを確認しています。データセンターの装置およびユーティリティに対する日常保守点検は、日常業務の一環です。緊急時のバックアップ装置水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。チームおよびシステムは、温度と湿度を監視して制御することで、過熱を防止し、サービス停止が起こらないようにします。不測の事態への備え AWS は、自然災害や火災など、環境上の脅威の可能性に対して事前の対策を講じています。当社データセンターを保護する 2 つの方法として、自動センサーと応答装置を設置しています。漏水検知デバイスは、自動ポンプを作動させて漏水を除去し、損害を防止して、従業員に問題を知らせることができます。同様に、自動火災検知および消火装置は危険を軽減し、AWS の従業員と消防士に問題を知らせることができます。複数のアベイラビリティゾーンによる高可用性事実上他のすべてのテクノロジーインフラストラクチャプロバイダと異なる点として、各 AWS リージョンには複数のアベイラビリティゾーンが存在しています。各アベイラビリティゾーンは 1 つ以上の相互に独立したデータセンターで構成されます。各データセンター間は物理的に離れており、冗長性のある電源とネットワーキングを備えています。アプリケーションの高い可用性やパフォーマンスが重要なお客様は、同じリージョンの複数のアベイラビリティゾーン間でアプリケーションをデプロイして、耐障害性や低レイテンシーを実現できます。アベイラビリティゾーンは高速なプライベート光ファイバーネットワークで相互に接続されているため、アプリケーションがアベイラビリティゾーン間で中断なく自動的にフェイルオーバーできるようなアーキテクチャを簡単に設計できます。シミュレーションと反応の測定 AWS ビジネス継続性プランは、自然災害による混乱の回避および軽減方法を示すオペレーションプロセスガイドであり、イベントが起こる前、イベントの最中、およびイベント後の詳しい対処ステップを定めるものです。不測の事態に備え、影響を軽減するために、AWS は定期的にビジネス継続性プランをテストし、さまざまなシナリオをシミュレートする演習を実施しています。チームとプロセスの対応を文書化し、学習した成果と、反応率を高めるために必要と思われる是正処置をまとめています。混乱から迅速に立ち直る訓練と準備が整っています。これには、エラーに伴うダウンタイムを最小限に抑えるための秩序を保った復旧プロセスなどが含まれます。詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

関連する統制に関しては AWS の SOC1、SOC2 レポートをご参照ください。

<https://aws.amazon.com/jp/compliance/soc-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

ソフトウェア変更がもたらす影響を評価する手段として、例えばプログラム作成段階からの継続的なテストの実行、実装内容の相互レビューなどが上げられます。AWS CodePipeline、AWS CodeBuild 等を利用し、継続的インテグレーション環境を実装することができます。

<https://aws.amazon.com/jp/blogs/news/category/developer-tools/aws-codepipeline/>また、AWS CodeCommit は Pull Request 機能を提供しているため、開発中のソースコードレビューに活用することができます。

https://docs.aws.amazon.com/ja_jp/codecommit/latest/userguide/pull-requests.html モバイルアプリの実機並列テスト実行には AWS Device Farm が利用できます。

<https://aws.amazon.com/jp/device-farm/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(2)

■ 要求事項 118

必須

変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。

■ AWS のインフラストラクチャー関連事項

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部のおよび外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフ

フレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会 (AICPA) のトラスト・サービスの原則 (Trust Services Principles)、PCI DSS v3.1、および米国国立標準技術研究所 (NIST) 出版物 800-53 Rev 3 (連邦政府情報システムにおける推奨セキュリティ統制) を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

変更管理

既存の AWS インフラストラクチャーに対する定期的な変更、緊急の変更、および設定の変更は、類似するシステムの業界基準に従って、許可、記録、テスト、承認、および文書化されます。AWS インフラストラクチャーを更新するにあたり、お客様とお客様によるサービスの使用に対する影響は最小限に抑えられます。サービスが悪影響を受ける可能性がある場合、AWS は E メールまたは AWS Service Health Dashboard (<http://status.aws.amazon.com/>) を通じて顧客に通知します。

関連する統制に関しては AWS の SOC1、SOC2 レポートをご参照ください。

<https://aws.amazon.com/jp/compliance/soc-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムに変更を加える際、業務及び環境に与える影響を最小限に抑える方法を検討する必要があります。

■ 推奨される追加の実施事項

AWS では、Amazon EC2 などの即時調達可能なリースを用い、オンプレミスでは実現が難しかったデプロイ戦略をとることができます。

既存システムに変更を加える際は、AWS を利用し変更に関わる影響を最小限に抑える以下のデプロイ戦略をとることが推奨されます。

- ・ブルーグリーンデプロイメント
- ・レッドブラックデプロイメント
- ・ローリングアップデート

上記戦略をとることで、コスト効率よく、新旧のバージョンを並行稼働させながら変更の妥当性をチェックし、チェックが正常に完了した場合のみ、新バージョンを本番環境へ適用することが可能となります。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(3)

■ 要求事項 119

必須

医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報の保存・交換のデータ形式、プロトコルが変更される場合、変更前のデータ形式・プロトコルの利用者が存在する間は下位互換性をサポートする必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(4)

■ 要求事項 120

必須

情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施すること。

■ AWS のインフラストラクチャー関連事項

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同等に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集合的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

変更の実稼動環境への投入は通常、最も影響の小さいエリアへの段階的配備から開始されます。デプロイは単一のシステムでテストされ、影響が評価できるよう綿密にモニタリングされます。サービスの所有者は、数多くの設定可能な評価指標を保有しています。これは、そのサービスの上流工程に対する依存関係の健全度を評価するものです。3つの測定値が、閾値と設定中のアラームとともに注意深くモニタリングされます。ロールバック手順は、変更管理（CM）チケットで文書化されています。

可能な場合、変更は通常の変更時間帯に予定されます。標準の変更管理手順と異なる手順を必要とする実稼動システムに対する緊急の変更は、インシデントと関連付けられており、必要に応じて記録され、承認されます。

AWS は、重要なサービスの変更に対する自己監査を定期的に行っており、品質をモニタリングしながら高い基準を維持することによって、変更管理プロセスの継続的な改善に貢献しています。例外は分析され、根本的な原因が決定されて適切な措置が取られます。変更はコンプライアンスに従うようにされるか、または必要に応じてロールバックされます。その後プロセスまたは人的問題を解決して修正するための措置が取られます。

AWS では、定期的な保守やシステムのパッチ適用を実行するために、システムをオフラインにする必要はありません。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。インスタンス自体の保守はお客様が統制します。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムの保守作業について、停止時間を最小限にとどめるよう計画をたて実施する必要があります。

AWS では、AWS Well-Architected Framework に基づく複数のアベイラビリティゾーンに跨るシステム構成（Multi-AZ 構成と呼ぶ）を取ることや、AWS の利点を活かした Blue-Green Deployment などのデプロイ戦略を立案することで、停止時間を最小限に留めるようにすることが可能です。

■ 推奨される追加の実施事項

AWS ElasticBeanstalk を利用することで、ローリングデプロイメントや Blue-Green デプロイメントなどの保守作業に伴う停止時間を最小限に留めることが可能なデプロイ戦略が取れる環境がマネージドサービスとして提供されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

■ 要求事項 121

必須

情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。

■ AWS のインフラストラクチャー関連事項

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この

集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

ソフトウェア

AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、十分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。実稼働環境にデPLOYされる変更には、以下の対応が行われます：

- ・ 検証：変更の技術的側面について専門家による検証が必要です。
- ・ テスト：適用されている変更は、予想どおりに動作し、パフォーマンスに悪影響を与えないことを確認するためにテストされます。
- ・ 承認：すべての変更は、ビジネスへの影響を適切に監視し、それらの影響についての情報を提供するために、承認される必要があります。

変更の実稼働環境への投入は通常、最も影響の小さいエリアへの段階的配備から開始されます。デPLOYは単一のシステムでテストされ、影響が評価できるよう綿密にモニタリングされます。サービスの所有者は、数多くの設定可能な評価指標を保有しています。これは、そのサービスの上流工程に対する依存関係の健全度を評価するものです。3つの測定値が、閾値と設定中のアラームとともに注意深くモニタリングされます。ロールバック手順は、変更管理（CM）チケットで文書化されています。

可能な場合、変更は通常の変更時間帯に予定されます。標準の変更管理手順と異なる手順を必要とする実稼働システムに対する緊急の変更は、インシデントと関連付けられており、必要に応じて記録され、承認されます。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムに変更に関し適切な変更手順を策定し、医療機関と実施について通知・承認を得る必要があります。

■ 推奨される追加の実施事項

AWS では、Amazon EC2 などの即時調達可能なリースを用い、オンプレミスでは実現が難しかったデプロイ戦略をとることができます。

既存システムに変更を加える際は、AWS を利用し変更に関わる影響を最小限に抑える以下のデプロイ戦略をとることが推奨されます。

- ・ブルーグリーンデプロイメント
- ・レッドブラックデプロイメント
- ・ローリングアップデート

上記戦略をとることで、医療機関の業務への影響を軽減することが可能です。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(6)

■ 要求事項 122

必須

不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。

■ AWS のインフラストラクチャー関連事項

セキュリティ設計の原則

AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。静的コード分析ツールは、標準ビルドプロセスの一環として実行され、配備される全ソフトウェアは、注意深く選択された業界の専門家によって実行される反復侵入テストを受けます。当社のセキュリティリスク査定のレビューは、設計段階に開始され、この作業はソフトウェアの立ち上げ後まで継続します。

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自

動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムに利用するソフトウェアについて改ざん検知ソフトウェアなどを用いた整合性検査を定期的の実施する必要があります。

AWS リソース上に配置されたオブジェクトについては、推奨される追加の実施事項で説明する方法で整合性検査が可能です。

■ 推奨される追加の実施事項

AWS では、ソフトウェアやファイルの改ざん検知を常時実施するソフトウェアとして OSS の AIDE が利用可能です。AIDE を使用することで、Amazon EBS 上に配置されたファイルの改ざん検知を常時実施することが可能です。また、Amazon S3 では、S3 にアップロードするオブジェクトの MD5 チェックサムを計算し、オブジェクトをアップロードする際に、整合性を確認する MD5 チェックサム値を HTTP ヘッダーに格納することで、MD5 チェックサム値でファイルの整合性が検証されます。またこのチェックサムは S3 からダウンロードしたオブジェクトの整合性を検証するためにも使用できます。詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/data-integrity-s3/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(7)

■ 要求事項 123

必須

医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。

■ AWS のインフラストラクチャー関連事項

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同等に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象とな

ります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

セキュリティ設計の原則

AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。静的コード分析ツールは、標準ビルドプロセスの一環として実行され、配備される全ソフトウェアは、注意深く選択された業界の専門家によって実行される反復侵入テストを受けます。当社のセキュリティリスク査定のレビューは、設計段階に開始され、この作業はソフトウェアの立ち上げ後まで継続します。

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムに関する脆弱性検査を定期的実施し、把握した脆弱性について管理台帳等を用い、システムへの影響や対策などを管理する必要があります。

■ 推奨される追加の実施事項

AWS では、Amazon Inspector を用い、医療情報システムの基盤に対する定期的な脆弱性検査を自動化できます。自動化した脆弱性検査結果は、CSV およびレポートとして出力することが可能です。出力した検査結果を用い台帳を作成して管理することが可能です。

Amazon Inspector の詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/inspector/>

Amazon Inspector 評価レポート

https://docs.aws.amazon.com/ja_jp/inspector/latest/userguide/inspector_reports.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6.1 情報処理装置及びソフトウェアの保守

(8)

■ 要求事項 124

必須

潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。

■ AWS のインフラストラクチャー関連事項

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部的および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同等に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

セキュリティ設計の原則

AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。静的コード分析ツールは、標準ビルドプロセスの一環として実行され、配備される全ソフトウェアは、注意深く選択された業界の専門家によって実行される反復侵入テストを受けます。当社のセキュリティリスク査定のレビューは、設計段階に開始され、この作業はソフトウェアの立ち上げ後まで続きます。

AWS は、ハイパーバイザーおよびネットワーキングサービスなど、お客様へのサービス提供をサポートするシステムにパッチを適用する責任を持ちます。この処理は、AWS ポリシーに従い、また ISO 27001、NIST、および PCI の要件に準拠して、必要に応じて実行します。お客様が使用しているゲストオペレーティングシステム、ソフトウェア、およびアプリケーションの統制については、お客様が行い、お客様がそれらのシステムにパッチを適用する責任を持ちます。

詳細は以下 URL 掲載のホワイトペーパー「AWS リスクとコンプライアンス」の P23 を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-risk-and-compliance/>

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートロ

グインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

-AWS systems Manager

AWS Systems Manager は、AWS でご利用のインフラストラクチャーを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェースで AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager では、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon RDS インスタンスなどのリソースをアプリケーションごとにグループ化し、運用データを表示できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができます。また、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャーでも安全に運用、管理できます

セキュリティとコンプライアンスの維持

AWS Systems Manager では、インスタンスのパッチ、設定、およびカスタムポリシーに対するスキャンを実行し、セキュリティとコンプライアンスの維持に役立てることができます。パッチのベースラインの定義、アンチウイルス定義の更新、ファイアウォールポリシーの適用が可能です。また、大規模なサーバー群でも、各サーバーに手動でログインすることなく、リモートで管理できます。Systems Manager では、データベース文字列のようなプレーンテキストや、パスワードのような秘密データなど、設定データを一元的に管理するストアが利用できます。これにより、機密データと構成データをコードから分離できます。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者はゲスト OS のセキュリティ更新を含む更新およびパッチ適用を制御する必要があります。

AWS が提供する Windows および Linux ベースの AMI は最新のパッチによって定期的に更新されますので、実行中の Amazon AMI インスタンスでデータまたはカスタム設定を保存する必要がない場合は、最新の更新された AMI で新しいインスタンスを再作成できます。さらに、Amazon Linux AMI の更新は、Amazon Linux yum リポジトリを通して提供されます。

また、推奨される追加の実施事項で説明する AWS Systems Manager Patch Manager を使用することでパッチ適用を自動化することが可能です。

■ 推奨される追加の実施事項

AWS Systems Manager Patch Manager を使用することで、セキュリティ関連の更新パッチをマネージドインスタンスに適用するプロセスを自動化することが可能です。

Patch Manager のパッチベースラインには、リリースから数日以内にパッチを自動承認するためのルールと、承認済みパッチおよび拒否済みパッチのリストが含まれています。パッチ適用を Systems Manager の メンテナンスウィンドウ タスクとして実行するようスケジュールすることで、パッチを定期的にインストールできます。また、パッチは、Amazon EC2 タグを使用して個別のインスタンスまたは大規模なグループのインスタンスにインストールできます。

Patch Manager は、AWS Identity and Access Management (IAM)、AWS CloudTrail、Amazon CloudWatch Events と連携して、イベント通知や使用状況の監査機能を含む安全なパッチ適用体験を提供します。詳細は以下 URL を参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-patch.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(9)

■ 要求事項 125

必須

修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。

■ AWS のインフラストラクチャー関連事項

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。さらに、AWS の 統制環境は、さまざまな内部および外部のリスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（Control Objectives for Information and related Technology, COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会（AICPA）のトラスト・サービスの原則（Trust Services Principles）、PCI DSS v3.1、および米

国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。この集成的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、テクノロジーを網羅しています。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、独立した第三者であるセキュリティ会社によって脆弱性および脅威の外部評価が定期的に実行されます。これらの評価における発見や推奨事項は、分類整理されて AWS シニアマネジメント層に報告されます。さらに、AWS 統制環境は、定期的な内部および外部の監査とリスク評価の対象となります。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

セキュリティ設計の原則

AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。静的コード分析ツールは、標準ビルドプロセスの一環として実行され、配備される全ソフトウェアは、注意深く選択された業界の専門家によって実行される反復侵入テストを受けます。当社のセキュリティリスク査定のレビューは、設計段階に開始され、この作業はソフトウェアの立ち上げ後まで続きます。

ソフトウェア

AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、十分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。実稼働環境にデプロイされる変更には、以下の対応が行われます：

- ・ 検証：変更の技術的側面について専門家による検証が必要です。
- ・ テスト：適用されている変更は、予想どおりに動作し、パフォーマンスに悪影響を与えないことを確認するためにテストされます。
- ・ 承認：すべての変更は、ビジネスへの影響を適切に監視し、それらの影響についての情報を提供するために、承認される必要があります。

変更の実稼動環境への投入は通常、最も影響の小さいエリアへの段階的配備から開始されます。デプロイは単一のシステムでテストされ、影響が評価できるよう綿密にモニタリングされます。サービスの所有者は、数多くの設定可能な評価指標を保有しています。これは、そのサービスの上流工程に対する依存関係の健全度を評価するものです。3つの測定値が、閾値と設定中のアラームとともに注意深くモニタリングされます。ロールバック手順は、変更管理（CM）チケットで文書化されています。

可能な場合、変更は通常の変更時間帯に予定されます。標準の変更管理手順と異なる手順を必要とする実稼動システムに対する緊急の変更は、インシデントと関連付けられており、必要に応じて記録され、承認されます。

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

-AWS systems Manager

AWS Systems Manager は、AWS でご利用のインフラストラクチャーを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェースで AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager では、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon RDS インスタンスなどのリソースをアプリケーションごとにグループ化し、運用データを表示できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができます。また、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャーでも安全に運用、管理できます

セキュリティとコンプライアンスの維持

AWS Systems Manager では、インスタンスのパッチ、設定、およびカスタムポリシーに対するスキャンを実行し、セキュ

リティとコンプライアンスの維持に役立てることができます。パッチのベースラインの定義、アンチウイルス定義の更新、ファイアウォールポリシーの適用が可能です。また、大規模なサーバー群でも、各サーバーに手動でログインすることなく、リモートで管理できます。Systems Manager では、データベース文字列のようなプレーンテキストや、パスワードのような秘密データなど、設定データを一元的に管理するストアが利用できます。これにより、機密データと構成データをコードから分離できます。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムに適用を予定している修正パッチについて、入手時にパッチが改ざんされていないこと、およびパッチの有効性を検証する必要があります。

パッチの有効性検証では、開発環境やステージング環境に事前にパッチを適用し、有効性およびシステムに悪影響が無いことを検証することが推奨されます。

■ 推奨される追加の実施事項

AWS Systems Manager Patch Manager を使用することで、AWS が確認済みの改ざんがされていないパッチが利用可能です。

AWS Systems Manager Patch Manager を使用する際も、ステージング環境などに事前にパッチを適用し有効性の検証およびシステムへの悪影響が無いことを確認することが推奨されます。ステージング環境へのパッチ適用も AWS Systems Manager Patch Manager を使用してパッチ適用を自動化することが可能です。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(10)

■ 要求事項 126

必須

保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「7.6.5 第三者が提供するサービスの管理」の管理策を実施すること。

選定した外部事業者について医療機関等に報告し、合意を得ること。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

AWS のセキュリティおよびデータプライバシーについては、Customer Agreement 第 3 条をご参照ください。

<https://aws.amazon.com/jp/legal/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は AWS を含む利用している基盤について報告し、合意を得る必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.1 情報処理装置及びソフトウェアの保守

(1)

■ 要求事項 127

推奨

変更手順に含まれる事項には次のようなものが考えられる。

- 変更についての影響が及ぶ関係者への通知プロセス
- 装置の変更申請書のフォーマット（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等）
- 申請承認プロセス
- 変更試験プロセス

- 変更作業に支障が発生した場合の復旧手順
- 変更終了確認プロセス
- 変更に伴う影響を監視するプロセス、等。

■ AWS のインフラストラクチャー関連事項

変更管理 変更管理

既存の AWS インフラストラクチャーに対する定期的な変更、緊急の変更、および設定の変更は、類似するシステムの業界基準に従って、許可、記録、テスト、承認、および文書化されます。AWS インフラストラクチャーを更新するにあたり、お客様とお客様によるサービスの使用に対する影響は最小限に抑えられます。サービスが悪影響を受ける可能性がある場合、AWS は E メールまたは AWS Service Health Dashboard (<http://status.aws.amazon.com/>) を通じて顧客に通知します。

詳細については、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」

(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、要求事項に含まれる点を網羅した変更管理システムを構築し、そのプロセスに則り変更作業を実施することが推奨されます。

■ 推奨される追加の実施事項

AWS CodePipeline を用いることで、ソフトウェアの変更管理からテスト・デプロイまでのプロセスを定義することができます。ソフトウェアデリバリーパイプラインの中ではテスト結果の確認や承認などの手動ステップを含めることで、ガイドライン推奨事項にある変更管理プロセスの実装および承認のエビデンスの管理が可能です。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7.6 技術的安全対策

7.6.2 開発施設、試験施設と運用施設の分離

(1)

必須

情報処理に供するアプリケーションについては、情報処理事業者自身で開発したアプリケーションを用いること。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、情報処理事業に用いるアプリケーション、パッケージソフトウェアの安全性を確保するために、機能および安全性を十分確認する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.2 開発施設、試験施設と運用施設の分離

■ 要求事項 129

必須

ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設を用いて行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムを運用する本番環境と開発環境を分離し、独立して運用する必要があります。

■ 推奨される追加の実施事項

AWS CloudFormation を使用することで、インフラストラクチャーをコードとしてモデル化し、容易に再現可能な環境を構築することができます。

これにより、本番システムを運用する環境とは分離した開発用環境を必要ときに素早く構築し、使用することができます。

AWS CloudFormation については以下 URL を参照ください。

<https://aws.amazon.com/jp/cloudformation/>

また、Amazon VPC を使用することで、環境間をネットワーク的に分離し、独立した環境として運用することが可能です。

Amazon VPC については以下 URL を参照ください。

<https://aws.amazon.com/jp/vpc/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7.6 技術的安全対策

7.6.2 開発施設、試験施設と運用施設の分離

■ 要求事項 130

必須

開発施設では悪意のあるコードが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には「7.6.3 悪意のあるコードに対する管理策」に従うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、インターネット等の不特定多数が利用するネットワークと接続する際は、「7.6.3 悪意のあるコードに対する管理策」に記載のある要求事項に対応する必要があります。

■ 推奨される追加の実施事項

AWS では、医療情報システムを医療機関等のエンドユーザーと接続するためにインターネット以外の選択肢も用意されています。

AWS Direct Connect を利用することで、エンドユーザの拠点から AWS への専用ネットワーク接続を簡単に確立することができ、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。

<https://aws.amazon.com/jp/directconnect/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.2 開発施設、試験施設と運用施設の分離

(4)

必須

不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改ざん防止、検知策を実施すること

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、開発したソフトウェアを本番環境へデプロイする前の変更管理プロセスの一環として、ソフトウェアの整合性検査を実施することが求められます。

■ 推奨される追加の実施事項

AWS CodeCommit は、Amazon Web Services がホストするバージョン管理サービスです。資産（ドキュメント、ソースコード、バイナリファイルなど）をプライベートにクラウドに保存および管理することができます。

AWS Code Commit ではリポジトリ内のデータは、転送中と不使用時のいずれも暗号化されます。AWS KMS と統合されている AWS Code Commit では、暗号化オペレーションや復号オペレーションの両方に関する暗号化コンテキストが指定されています。暗号化コンテキストは AWS KMS で使用される追加の認証情報であり、データの整合性を調べるために使用できます。

AWS Code Commit および暗号化コンテキストの詳細は以下 URL を参照ください。

https://docs.aws.amazon.com/ja_jp/codecommit/latest/userguide/welcome.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.2 開発施設、試験施設と運用施設の分離

(5)

■ 要求事項 132

必須

運用施設に保存されている医療情報を開発施設及び試験施設にコピーしないこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、本番環境上の医療情報を開発環境および試験環境にコピーしないようシステムを運用することが求められます。

■ 推奨される追加の実施事項

AWS Identity and Access Management を使用し、本番環境にアクセス可能な担当者と開発環境・試験環境にアクセス可能な担当者を分離できます。

担当者の権限を分離することで、環境間の機密データコピーを論理的に制限し、ルールを強制することが可能です。

AWS IAM の詳細は以下の URL を参照ください。

<https://aws.amazon.com/jp/iam/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7.6 技術的安全対策

7.6.2 開発施設、試験施設と運用施設の分離

(6)

必須

医療情報を開発及び試験用データとして直接、利用しないこと。利用する場合には、個人情報の消去及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等にし、了解を得た上で利用すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、開発及び試験データとして本番環境の医療情報を利用しないようにする必要があります。また、利用する場合でも個人情報をマスクし、元データを復元できない状態とするなど、元データの流出・漏えいを防ぐ手段を講じその安全性について医療機関に説明・了解を得る必要があります。

■ 推奨される追加の実施事項

Amazon Macie を利用し、開発及び試験用 AWS アカウントに個人情報が混入していないかや誤って使用されていないか検知することが可能です。

Amazon Macie は、機械学習によって AWS 内の機密データを自動的に検出、分類、保護するセキュリティサービスです。Macie では、個人情報（PII）や知的財産などの機密データが認識されます。また、ダッシュボードやアラートが提供されるため、データのアクセスや移動状況を確認できます。

Amazon Macie の詳細については以下の URL を参照ください。

<https://aws.amazon.com/jp/maciek/>

※Amazon Macie は 2018 年 6 月時点で米国の一部リージョンのみの提供となっていますので、東京リージョンでの利用はできません。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.2 開発施設、試験施設と運用施設の分離

(1)

■ 要求事項 134

推奨

ソフトウェアに悪意のあるコードが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、開発したソフトウェアを本番環境へデプロイする前の変更管理プロセスの一環として、ソフトウェアの整合性検査を実施することが求められます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.3 悪意のあるコードに対する管理策

(1)

■ 要求事項 135

必須

最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。

■ AWS のインフラストラクチャー関連事項

ウイルス対策および悪意のあるソフトウェア対策に関する AWS のプログラム、プロセス、および手続きは、ISO27001 規格に合わせています。詳細については、AWS SOC レポートを参照してください。

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

-AWS systems Manager

AWS Systems Manager は、AWS でご利用のインフラストラクチャーを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェースで AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager では、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon RDS インスタンスなどのリソースをアプリケーションごとにグループ化し、運用デー

タを表示できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができます。また、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャーでも安全に運用、管理できます

セキュリティとコンプライアンスの維持

AWS Systems Manager では、インスタンスのパッチ、設定、およびカスタムポリシーに対するスキャンを実行し、セキュリティとコンプライアンスの維持に役立てることができます。パッチのベースラインの定義、アンチウイルス定義の更新、ファイアウォールポリシーの適用が可能です。また、大規模なサーバー群でも、各サーバーに手動でログインすることなく、リモートで管理できます。Systems Manager では、データベース文字列のようなプレーンテキストや、パスワードのような秘密データなど、設定データを一元的に管理するストアが利用できます。これにより、機密データと構成データをコードから分離できます。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムに対してウイルス対策や悪意のあるコードに対する対策を実施し、対応反意を確認する必要があります。また、最新の脅威に関する情報収集に努める必要があります。

■ 推奨される追加の実施事項

AWS ではセキュリティ速報の形で、AWS に関連する脆弱性情報および対処について AWS セキュリティセンターに掲載されます。この情報を利用して最新の脅威についての情報収集が行えます。また、個人や企業、セキュリティ担当チームがよくウェブサイトやフォーラムに各自の勧告を掲載しています。関連性がある場合は、このようなサードパーティのリソースへのリンクも AWS セキュリティ情報に含めています。

<https://aws.amazon.com/jp/security/security-bulletins/>

また、AWS のパートナーからウイルスやマルウェア対策のソフトウェアが AWS 対応製品として提供されているので、そちらを利用して医療情報システムの脅威対策を実施することが可能です。

AWS 対応のウイルス・マルウェア対策ツールは以下から検索可能です。

<https://esp-online.com/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.3 悪意のあるコードに対する管理策

(2)

■ 要求事項 136

必須

悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。

- リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信）
- リスク評価の結果として必要であれば定期的にスキャンを実施
- 電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン
- 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新
- 管理者以外による設定変更やアンインストールの禁止

■ AWS のインフラストラクチャー関連事項

ウイルス対策および悪意のあるソフトウェア対策に関する AWS のプログラム、プロセス、および手続きは、ISO27001 規格に合わせています。詳細については、AWS SOC レポートを参照してください。

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

-AWS systems Manager

AWS Systems Manager は、AWS でご利用のインフラストラクチャーを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェースで AWS のさまざまなサービスの運用データを確認

でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager では、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon RDS インスタンスなどのリソースをアプリケーションごとにグループ化し、運用データを表示できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができます。また、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャーでも安全に運用、管理できます

セキュリティとコンプライアンスの維持

AWS Systems Manager では、インスタンスのパッチ、設定、およびカスタムポリシーに対するスキャンを実行し、セキュリティとコンプライアンスの維持に役立てることができます。パッチのベースラインの定義、アンチウイルス定義の更新、ファイアウォールポリシーの適用が可能です。また、大規模なサーバー群でも、各サーバーに手動でログインすることなく、リモートで管理できます。Systems Manager では、データベース文字列のようなプレーンテキストや、パスワードのような秘密データなど、設定データを一元的に管理するストアが利用できます。これにより、機密データと構成データをコードから分離できます。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムに対して以下の機能を持つウイルス対策や悪意のあるコードの対策ソフトウェアを導入し適切な設定を行う必要があります。

- ・リアルタイムスキャン
- ・定期スキャン
- ・データの外部への書き出し・読み出し時のオンデマンドスキャン
- ・定義ファイル/スキャンエンジンの定期的なアップデート
- ・管理者以外による設定変更やアンインストールの禁止

■ 推奨される追加の実施事項

AWS のパートナーからウイルスやマルウェア対策のソフトウェアが AWS 対応製品として提供されているので、そちらを利用して医療情報システムの脅威対策を実施することが可能です。

AWS 対応のウイルス・マルウェア対策ツールは以下から検索可能です。

<https://esp-online.com/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.3 悪意のあるコードに対する管理策

(3)

■ 要求事項 137

必須

一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策が行われていること。

■ AWS のインフラストラクチャー関連事項

ウイルス対策および悪意のあるソフトウェア対策に関する AWS のプログラム、プロセス、および手続きは、ISO27001 規格に合わせています。詳細については、AWS SOC レポートを参照してください。

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

-AWS systems Manager

AWS Systems Manager は、AWS でご利用のインフラストラクチャーを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェースで AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager では、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon RDS インスタンスなどのリソースをアプリケーションごとにグループ化し、運用デー

タを表示できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができます。また、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャーでも安全に運用、管理できます

セキュリティとコンプライアンスの維持

AWS Systems Manager では、インスタンスのパッチ、設定、およびカスタムポリシーに対するスキャンを実行し、セキュリティとコンプライアンスの維持に役立てることができます。パッチのベースラインの定義、アンチウイルス定義の更新、ファイアウォールポリシーの適用が可能です。また、大規模なサーバー群でも、各サーバーに手動でログインすることなく、リモートで管理できます。Systems Manager では、データベース文字列のようなプレーンテキストや、パスワードのような秘密データなど、設定データを一元的に管理するストアが利用できます。これにより、機密データと構成データをコードから分離できます。

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ウイルス対策や悪意のあるコードの対策ソフトウェアが適切に動作していることを定期的に確認する必要があります。適切に動作していない場合には、利用者への警告や管理者への通報・またはネットワークからの隔離などの対策を行う必要があります。

■ 推奨される追加の実施事項

AWS のパートナーからウイルスやマルウェア対策のソフトウェアが AWS 対応製品として提供されているので、そちらを利用して医療情報システムの脅威対策を実施することが可能です。

AWS 対応のウイルス・マルウェア対策ツールは以下から検索可能です。

<https://esp-online.com/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.4 ウェブブラウザを使用する際の要求事項

(1)

必須

ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ウェブブラウザの接続するサーバを業務上必要なサーバに限定することが求められます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.4 ウェブブラウザを使用する際の要求事項

(2)

■ 要求事項 139

必須

ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash 等のプログラムコードをダウンロード及び実行することができない設定になっていること（管理ソフトウェアが実行されるサーバのみを認可する）。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムを扱うウェブブラウザの設定を適切に管理する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.4 ウェブブラウザを使用する際の要求事項

(3)

■ 要求事項 140

必須

認可したサイトからダウンロードされるコードについても「7.6.3 悪意のあるコードに対する管理策」に即して検査されること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、ブラウザを利用し認可したサイトからダウンロードしたオブジェクトについても「7.6.3 悪意のあるコードに対する管理策」に即した対策を実施する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.4 ウェブブラウザを使用する際の要求事項

(1)

■ 要求事項 141

推奨

ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムを扱うウェブブラウザの設定を適切に管理する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(1)

■ 要求事項 142

第三者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認すること。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS は米国における HIPAA に対応した医療情報システムのクラウド基盤として多くの事業者に利用された実績を有し、セキュアで柔軟かつ低コストのクラウドサービスを実現可能な AWS 環境において、医療情報システムの様々な要件に対応するため各種サービスや関連情報を提供していますが、情報処理事業者は自らが提供するサービスにとって必要な観点から、AWS より提供されるサービスの安全管理策及び SLA を確認する必要があります。

AWS セキュリティプロセスの概要については以下 URL を参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

AWS が提供する SLA は以下 URL を参照ください。

<https://aws.amazon.com/jp/legal/service-level-agreements/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.15 供給者関係

A.15.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(2)

■ 要求事項 143

必須

サービスの実施、運用、維持について定期的に検証すること。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS サービスの実施、運用、維持が適切に行われていることの根拠となる各種規格の認証を取得しサードパーティの独立監査人による監査が現在も有効であるかを確認する必要があります。

AWS の各種認証に関する証明書は以下 URL で確認することができます。

<https://aws.amazon.com/jp/compliance/programs/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(3)

必須

サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。
詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS のお客様は、お客様のデータの統制と所有権を保持します。

医療情報システムに関するサービス実施は情報処理事業者の業務です。

AWS が提供するマネージドサービスを利用する際には、AWS から行われる事前・事後のメンテナンス通知が行われます。

（緊急の場合には事後となる場合もります。）情報処理事業者はこれらの通知を確認する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(4)

必須

サービスを実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れないこと。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS は、適用法令の許容範囲で、従業員の雇用前審査の一環として、その従業員の役職や AWS 施設へのアクセスレベルに応じた犯罪歴の確認を行っています。AWS SOC レポートには、経歴検証のための統制に関する追加の詳細情報が記載されています。

このため、情報処理事業者は、確認時点で有効な AWS SOC レポートを確認することで、AWS がサービス実施時に不正な人員を受け入れていないことを間接的に確認できます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(5)

■ 要求事項 146

必須

サービス実施中に第三者が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯すること。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されているため、情報処理事業者は、確認時点で有効な上記レポートおよび認証を確認することで、AWS がサービス実施時に適切な管理区域への立ち入り確認を実施していることを間接的に確認できます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(6)

■ 要求事項 147

必須

サービス実施にともなう処理施設内への立ち入り手順に関しては、情報処理事業者の職員の入室、退室手順に準ずること。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP への準拠のため、監査中に外部の独立監査人によって確認されているため、情報処理事業者は、確認時点で有効な上記レポートおよび認証を確認することで、AWS がサービス実施時に適切な管理区域への立ち入り確認を実施していることを間接的に確認できます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(7)

■ 要求事項 148

必須

サービスの変更時には、引き続き安全性が維持されていることについて適切な検証を行うこと。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS のシステム開発ライフサイクル(SDLC) は、業界のベストプラクティスを組み込んでおり、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスク評価の完遂などが含まれています。詳細については、AWS セキュリティプロセスの概要を参照してください。

これらは ISO 27001 規格に準拠した形で実施されているため、情報処理事業者は、確認時点で有効な ISO27001 認証を確認することで、間接的にサービス変更時に安全性が維持されていることについて確認ができます。また、AWS は、サービス状態ダッシュボードにサービスの可用性に関する最新情報を公開していますので、こちらでサービスの可用性について情報処理事業者にて確認ができます。status.aws.amazon.com を参照してください。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.16 情報セキュリティインシデント管理

A.16.1

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(8)

■ 要求事項 149

必須

医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第 4.1 版」6.8 章 C 項の管理策を実施すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業には、医療情報システムの保守点検作業を外部事業者に実施する際には適切な安全管理策を実施させる義務があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.5 第三者が提供するサービスの管理

(1)

■ 要求事項 150

推奨

外部事業者がサービスを実施する際は、情報処理事業者もしくは外部事業者の正規職員が管理している状況で作業を行うことが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS はお客様に AWS のサービスを提供するにあたり、サードパーティのクラウドプロバイダーは一切使用していません。詳細については以下ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Answers_to_Key_Compliance_Questions_JP.pdf

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(1)

■ 要求事項 151

必須

セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行うこと。

■ AWS のインフラストラクチャー関連事項

安全なネットワークアーキテクチャ

ファイアウォールや他の境界デバイスなどのネットワークデバイスは、ネットワークの外部境界およびネットワーク内の主要な内部境界で通信を監視および制御するために用意されています。これらの境界デバイスでは、ルールセット、アクセスコントロールリスト（ACL）、および設定が採用され、強制的に特定の情報システムサービスに情報が流れます。

ACL、つまりトラフィックフローのポリシーは、各マネージドインターフェースに設定され、トラフィックの流れを監視して流します。ACL ポリシーは Amazon 情報セキュリティによって承認されます。これらのポリシーは、AWS の ACL 管理ツールを使用して自動的にプッシュされ、確実にマネージドインターフェースで最新の ACL が実行されます。

詳細は「AWS: セキュリティプロセスの概要」ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする

一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLs.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業（お客様）の該当事項

AWS では、Amazon VPC 内のセキュリティ機能として、セキュリティグループ、ネットワーク ACL、ルーティングテーブル、外部ゲート

ウェイなどがあります。この各アイテムは補完的なもので、インターネットへの直接アクセス有効にするか、他のネットワークにプライベート接続するかを選択することで拡張できる、安全で独立したネットワークを提供します。

情報処理事業は、上記機能を利用して、医療情報システムに適切なアクセス制御を実施することが求められます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(2)

■ 要求事項 152

必須

セキュリティゲートウェイでは、不正な IP アドレスを持つトラフィックが通過できないように設定すること（接続機器類の IP アドレスをプライベートアドレスとして設定して、ファイアウォール、VPN 装置等のセキュリティゲートウェイを通過しようとするトラフィックを IP アドレスベースで制御する等）。

■ AWS のインフラストラクチャー関連事項

Amazon EC2 インスタンスは、なりすましたネットワークトラフィックを送信できません。AWS によって管理される、ホストベースのファイアウォールインフラストラクチャーでは、インスタンスは、ソース IP または

MAC アドレスがインスタンス自身のものでないトラフィックを送信できません。

詳細は「AWS: セキュリティプロセスの概要」ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLS.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

AWS では、Amazon VPC 内のセキュリティ機能として、セキュリティグループ、ネットワーク ACL、ルーティングテーブル、外部ゲート

ウェイなどがあります。この各アイテムは補完的なもので、インターネットへの直接アクセス有効にするか、他のネットワークにプライベート接続するかを選択することで拡張できる、安全で独立したネットワークを提供します。

情報処理事業者は、上記機能を利用して、医療情報システムに適切なアクセス制御を実施することが求められます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(3)

■ 要求事項 153

必須

ルータ等のネットワーク機器は、安全性が確認できる機器を利用すること。

■ AWS のインフラストラクチャー関連事項

AWS データセンター環境では、サーバー、ラック、ネットワークデバイス、ハードドライブ、システムハードウェアコンポーネント、構成要素など、データセンターに配送され、受け取られるすべての新しい情報システムコンポーネントについて、データセンターマネージャーへの通知と事前の承認が必要です。アイテムは各 AWS データセンターの配送ドックに届けられ、梱包の損傷または不正開封について検査された後で、AWS 正社員によって署名されます。アイテムは、配送到着時に AWS 資産管理システムおよびデバイス在庫追跡システムでスキャンされて登録されます。

受領されたアイテムは、データセンター内の機器保管室に配置され、データセンターのフロアに設置されるまで、アクセスにはスワイプバッジと PIN の組み合わせが必要になります。アイテムは、スキャン、追跡、殺菌され、承認を受けてデータセンターから出されます。

詳細は、「AWS リスクとコンプライアンス」ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLS.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得, 開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(4)

■ 要求事項 154

必須

ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限すること。

■ AWS のインフラストラクチャー関連事項

AWS では、インバウンドとアウトバウンドの通信およびネットワークトラフィックをより包括的に監視することを考え、限られた数のクラウドへのアクセスポイントを戦略的に設置しました。このようなお客様のアクセスポイントは API エンドポイントと呼ばれ、安全な HTTP アクセス（HTTPS）を許可します。これにより、ご利用のストレージまたは AWS 内のコンピューティングインスタンスとの安全な通信セッションを確立できます。

詳細は「AWS: セキュリティプロセスの概要」ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLS.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(5)

■ 要求事項 155

必須

医療機関等との接続ネットワーク境界には侵入検知システム（IDS）、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行うこと。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィック

をコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLS.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの

徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、IDS または IPS を設置し、不正なイベント・府トラフィックの検知または遮断を行う必要があります。

■ 推奨される追加の実施事項

AWS のパートナーから IDS や IPS ソフトウェアが AWS 対応製品として提供されているので、そちらを利用してネットワークの不正イベント・トラフィック検知を実施することが可能です。

AWS 対応のソフトウェアは以下から検索可能です。

<https://esp-online.com/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(6)

■ 要求事項 156

必須

侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLS.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は設置した IDS/IPS のシグネチャ・検知ルール等の更新およびセキュリティパッチの適用を定期的に実施する必要があります。

■ 推奨される追加の実施事項

AWS のパートナーから IDS や IPS ソフトウェアが AWS 対応製品として提供されているので、そちらを利用してネットワークの不正イベント・トラフィック検知を実施することが可能です。またこれらの製品はシグネチャ・検知ルールの更新およびセキュリティパッチの適用を定期的に実施可能な製品を選ぶことをお勧めします。

AWS 対応のソフトウェアは以下から検索可能です。

<https://esp-online.com/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(7)

■ 要求事項 157

必須

侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定にしていること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLS.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は設置した IDS/IPS で検知したイベントを管理者に通知する仕組みを整備する必要があります。

■ 推奨される追加の実施事項

AWS のパートナーから IDS や IPS ソフトウェアが AWS 対応製品として提供されているので、そちらを利用してネットワークの不正イベント・トラフィックの検知時に管理者に通報する仕組みを構築することが可能です。

AWS 対応のソフトウェアは以下から検索可能です。

<https://esp-online.com/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(8)

■ 要求事項 158

必須

侵入検知の記録には不正アクセス等の事後処理に必要な項目が含まれていること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLs.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は IDS/IPS の選定にあたり、不正アクセスの事後処理に必要な情報が記録されるソフトウェアを選定する必要があります。

■ 推奨される追加の実施事項

AWS のパートナーから IDS や IPS ソフトウェアが AWS 対応製品として提供されているので、そちらを利用してネットワークの不正イベント・トラフィック検知を実施することが可能です。

AWS 対応のソフトウェアは以下から検索可能です。

<https://esp-online.com/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

(9)

■ 要求事項 159

必須

医療情報システムにおいて、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定すること。他に必要なサービスがある場合には、医療機関等の合意を得てから利用すること。

- 外部からの医療情報システムの稼働監視・遠隔保守

セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード

- オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード
- 電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス
- ファイアウォール、IDS・IPS などのセキュリティ機器に対する不正アクセス監視
- 時刻同期のための時刻配信サーバへのアクセス
- これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等）
- その他の医療情報システムの稼働に必要なサービス（外部認証サーバ、外部医療情報データベース等）

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割

り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLS.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、

総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、インターネットとの接続について、必要な範囲に限定するよう、セキュリティグループ等のアクセス制御機能を用い適切な設定を行う必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(10)

■ 要求事項 160

必須

医療情報システムのサーバ機器等への同時ログオンユーザ数（OS アカウント等）に適切な上限を設けること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムを構成する EC2 等への漏示ログオンユーザー数に適切な上限を設ける必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1
A.12.2
A.12.3
A.12.4
A.12.5
A.12.6
A.12.7

A.13 通信のセキュリティ

A.13.1
A.13.2

A.14 システムの取得，開発及び保守

A.14.1
A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(11)

■ 要求事項 161

必須

ネットワーク接続のログ（認証ログ及び接続ログ）を記録すること。

■ AWS のインフラストラクチャー関連事項

ネットワークの監視と保護

AWS は、様々な自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。

AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されてい

ます。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャンングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。

詳細は「セキュリティプロセスの概要」ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLs.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。

このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムの認証および接続ログを記録することが求められます。また、AWS リソースに対するアクセスを記録するため、AWS CloudTrail を有効化し、AWS リソースのログを記録することが推奨されます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(12)

■ 要求事項 162

必須

ネットワーク接続ログを定期的に検証し不審な活動が行われていないことを検証すること。

■ AWS のインフラストラクチャー関連事項

AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。主要なオペレーションメトリックが早期警告しきい値を超えた場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュール（常時待機体制）が採用されているので、担当者が運用上の問題にいつでも

対応することができます。ポケットベルシステムがサポートされ、アラームが迅速かつ確実に運用担当者に届きます。

詳細は「セキュリティプロセスの概要」ホワイトペーパーを参照ください。

https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLs.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちま

す。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムの認証および接続ログを定期的に検証する必要があります。

■ 推奨される追加の実施事項

認証・接続ログの監視を実施し、不正なログに対してアラートを通知するよう設定することで、常時監視が可能です。また、AWS CloudTrail ログを利用した監査レポートを定期的に生成し、検証することを推奨します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

(13)

■ 要求事項 163

必須

医療情報を保存する医療情報システムにおいて無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LAN を利用しないこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(14)

■ 要求事項 164

必須

VPN 接続を行う場合には以下の事項に従うこと。

- 接続時に VPN 装置間で相互に認証を行うこと。
- 傍受、リプレイ等のリスクを最小限に抑えるために、「7.6.11 暗号による管理策」に従い、適切な暗号技術を利用すること。
- インターネット上のトラフィックが VPN チャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。
- 複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるため VPN チャンネルを医療機関等別に構築する等の対策を実施すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスで

す。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、Amazon VPC の仮想プライベートゲートウェイを使用することで、要求事項に合致する IPsec VPN を医療機関との間で構築することが可能です。

VPN 構築時には、IP アドレスや事前共有鍵による機器間の認証および VPN チャンネル間のルーティング等に注意する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(1)

■ 要求事項 165

推奨

医療情報システムから、不正・不審なトラフィックが内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLs.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムの認証および接続ログを定期的に検証する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.6 ネットワークセキュリティ管理

(2)

■ 要求事項 166

推奨

侵入検知システム自身が攻撃・不正アクセスの対象とならないように、その存在を外部から隠す設定（ステルスモード）や、侵入検知システムへのアクセスの適切な制御を実施することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-VPC SecurityGroup

セキュリティグループは、インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックをコントロールします。VPC 内でインスタンスを起動した場合、そのインスタンスには最大 5 つのセキュリティグループを割り当てることができます。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。このため、VPC 内のサブネット内のインスタンスごとに異なるセキュリティグループのセットに割り当てることができます。起動時に特定のグループを指定しないと、インスタンスは VPC のデフォルトのセキュリティグループに自動的に割り当てられます。セキュリティグループごとに、インスタンスへのインバウンドトラフィックをコントロールするルールと、アウトバウンドトラフィックをコントロールする一連のルールを個別に追加します。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

-ネットワーク ACL

ネットワークアクセスコントロールリスト (ACL) は、1 つ以上のサブネットのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォールとして動作する、VPC 用のセキュリティのオプションレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_ACLS.html

-VPC フローログ

VPC フローログは、VPC のネットワークインターフェースとの間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログのデータは、Amazon CloudWatch Logs を使用して保存されます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示し、取得できます。フローログは、多くのタスクで役立ちます。たとえば、特定のトラフィックがインスタンスに到達していない場合のトラブルシューティングに役立ちます。これにより、制限が過度に厳しいセキュリティグループルールを診断できます。また、セキュリティツールとしてフローツールを使用し、インスタンスに達しているトラフィックをモニタリングすることができます。詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/flow-logs.html

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。

このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/H202>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guarddduty/>

■ 情報処理事業者（お客様）の該当事項

AWS では、Amazon VPC 内のセキュリティ機能として、セキュリティグループ、ネットワーク ACL、ルーティングテーブル、外部ゲート

ウェイなどがあります。この各アイテムは補完的なもので、インターネットへの直接アクセス有効にするか、他のネットワークにプライベート接続するかを選択することで拡張できる、安全で独立したネットワークを提供します。

情報処理事業者は、上記機能を利用して、医療情報システムに適切なアクセス制御を実施することが求められます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(1)

■ 要求事項 167

必須

電子媒体について情報処理事業者施設外への不要な持ち出しを行わないこと。CD、DVD、MO 等の電子媒体については、追記のできない光学メディア（CD-R、DVD-R 等）を用い、情報交換作業終了後、電子媒体を（9）に示す方式にて確実に廃棄処分すること。

■ AWS のインフラストラクチャー関連事項

AWS は、システム出力デバイスへのアクセスを、権限を持つ関係者のみに制限しています。認証を取得するアクセスでは、電子リクエストを提出し、アクセスのビジネスケースを提示して、承認された承認者によるその認証の文書による承認を取得する必要があります。AWS アクセス管理の手順は、SOC、PCI DSS、ISO 27001、および FedRAMPsm への継続的な準拠の一環として、サードパーティの監査人によって個別に確認されます。

個人の電子デバイスやリムーバブルメディアは、AWS 情報システムに接続することが禁止されています。

詳細は以下 URL 掲載のホワイトペーパー「AWS リスクとコンプライアンス」の P116 を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-risk-and-compliance/>

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS リソース以外の電子媒体の持ち出し・情報消去等を適切に管理する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(2)

■ 要求事項 168

必須

情報交換目的やバックアップ目的で MT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行うこと。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行うこと。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終

的に不要になった場合)の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS リソース以外の電子媒体の持ち出し・情報消去等を適切に管理する必要があります。

■ 推奨される追加の実施事項

AWS では、セキュアなデータ転送手段として AWS Snowball を利用し情報の物理的な搬送に利用することができます。AWS Snowball は物理的な輸送をセキュアに行うことができるように設計されたストレージアプライアンスを使用して、テラバイト規模からペタバイト規模のデータを AWS との間で移動するためのデータ転送ソリューションです。Snowball を使用すると、ネットワークのコストが高い、転送時間が長い、セキュリティに懸念があるといった、大規模なデータ転送でよく直面する課題を解決できます。

データの暗号化

Snowball を使用してデータを S3 にインポートする場合、Snowball に転送されるすべてのデータには、2 つのレイヤーの暗号化があります。

- ・暗号化のレイヤーがローカルワークステーションのメモリに適用されます。このレイヤーは、Snowball 用 Amazon S3 Adapter または Snowball クライアント を使用しているかどうかに関係なく適用されます。この暗号化では AES GCM 256 ビットキーが使用され、60 GB のデータが転送されるたびにキーが切り替わります。

- ・SSL 暗号化は、標準 Snowball との間で転送されるすべてのデータの 2 番目の暗号化レイヤーです。

AWS Snowball では、保管時のデータを保護するため、サーバー側の暗号化（SSE）が使用されます。

不正開封の検知

AWS に到着した Snowball は、アプライアンスごとに改ざんの跡がないか検査され、トラステッドプラットフォームモジュール（TPM）を使用して変更が検出されないか検証されます。AWS Snowball では、データ保護のために、不正開封防止筐体、256 ビットの暗号化、およびデータのセキュリティと完全な保管継続性を提供するための業界標準である TPM など、数重に設計されたセキュリティ機能を使用しています。

情報処理事業者に Snowball が到着したらまず、損傷や明らかな改ざんについて検査してください。Snowball に疑わしい点が見つかった場合は、内部ネットワークに接続しないでください。AWS サポートにお問い合わせいただければ、新しい Snowball をお客様宛に配送します。

データの消去

データ転送ジョブの処理と検証が完了すると、AWS では National Institute of Standards and Technology

(NIST) の「メディア衛生のためのガイドライン」に従った方法で Snowball アプライアンスのソフトウェア消去を実施します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

(3)

■ 要求事項 169

必須

電子媒体は台帳を作成して管理すること。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証すること。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持すること。

■ AWS のインフラストラクチャー関連事項

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS リソース以外の保有する電子媒体の台帳を作成し、持ち出し・持ち帰り等の記録を管理し、定期的に存在の棚卸を実施すること。また、台帳の保管期間などのルールを策定し運用することが求められます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

■ 要求事項 170

必須

電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。

■ AWS のインフラストラクチャー関連事項

AWS は、システム出力デバイスへのアクセスを、権限を持つ関係者のみに制限しています。認証を取得するアクセスでは、電子リクエストを提出し、アクセスのビジネスケースを提示して、承認された承認者によるその認証の文書による承認を取得する必要があります。AWS アクセス管理の手順は、SOC、PCI DSS、ISO 27001、および FedRAMPsm への継続的な準拠の一環として、サードパーティの監査人によって個別に確認されます。

個人の電子デバイスやリムーバブルメディアは、AWS 情報システムに接続することが禁止されています。

詳細は以下 URL 掲載のホワイトペーパー「AWS リスクとコンプライアンス」の P116 を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-risk-and-compliance/>

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS リソース以外の電子媒体について物理的な保管について安全対策を実施することが求められます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(5)

■ 要求事項 171

必須

■ AWS のインフラストラクチャー関連事項

AWS データセンターの環境については、サーバー、ラック、ネットワークデバイス、ハードドライブ、システムハードウェアコンポーネント、および建築資材といった新しい情報システムコンポーネントがデータセンターに出荷される場合、必ずデータセンターマネージャーが事前に承認する必要があり、納品時にはデータセンターマネージャーに通知する必要があります。物品は各 AWS データセンターの搬入口に配送されます。AWS の正社員は、破損や梱包が開封された痕跡がないことを検査し、署名します。物品は配達時に、AWS のアセット管理システムとデバイス在庫追跡システムによりスキャンおよび記録されます。受領された物品は、データセンターのフロアに設置されるまで、データセンター内の機器保管室に置かれま

す。機器保管室に入るには、ID カードの読み取りと PIN の入力が必要です。物品がデータセンターから搬出される場合、搬出の承認を受ける前に、その物品のスキャン、使用履歴の追跡、データの消去が行われます。AWS のアセット管理のプロセスと手順は、PCI DSS、ISO 27001、および FedRAMP sm のコンプライアンスの監査時に、社外の独立監査人によって確認されます。

詳細については、AWS クラウドセキュリティ ホワイト ペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。また、ISO 27001 規格の附属書 A ドメイン 7 を参照してください。AWS は、ISO27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS リソース以外の電子媒体についてメーカーにより指定された保管環境で保管することが求められます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(6)

■ 要求事項 172

必須

製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、他媒体に複写すること。

■ AWS のインフラストラクチャー関連事項

AWS データセンターの環境については、サーバー、ラック、ネットワークデバイス、ハードドライブ、システムハードウェアコンポーネント、および建築資材といった新しい情報システムコンポーネントがデータセンターに出荷される場合、必ずデータセンターマネージャーが事前に承認する必要がある、納品時にはデータセンターマネージャーに通知する必要があります。物品は各 AWS データセンターの搬入口に配送されます。AWS の正社員は、破損や梱包が開封された痕跡がないことを検査し、署名します。物品は配達時に、AWS のアセット管理システムとデバイス在庫追跡システムによりスキャンおよび記録されます。受領された物品は、データセンターのフロアに設置されるまで、データセンター内の機器保管室に置かれます。機器保管室に入るには、ID カードの読み取りと PIN の入力が必要です。物品がデータセンターから搬出される場合、搬出の承認を受ける前に、その物品のスキャン、使用履歴の追跡、データの消去が行われます。AWS のアセット管理のプロセスと手順は、PCI DSS、ISO 27001、および FedRAMP sm のコンプライアンスの監査時に、社外の独立監査人によって確認されます。

詳細については、AWS クラウドセキュリティホワイトペーパー(<http://aws.amazon.com/security> で入手可能) を参照してください。また、ISO 27001 規格の附属書 A ドメイン 7 を参照してください。AWS は、ISO27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS リソース以外の電子媒体についてメーカーにより指定された保管環境で保管することが求められます。電子媒体については耐用年数を把握し、限度が近づいたものは新たな機器に刷新する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(7)

■ 要求事項 173

必須

情報を保管するためにハードディスク装置を用いる場合には、RAID-1 もしくは RAID-6 相当以上のディスク障害に対する対策をとること。

■ AWS のインフラストラクチャー関連事項

Amazon S3 は極めて堅牢性の高いストレージインフラストラクチャーを提供しています。オブジェクトは冗長化のため、同一の Amazon S3 リージョン内の複数施設に分散した複数のデバイスに保存されます。一旦格納されると、Amazon S3 は冗長性が失われた場合にすばやく検出して修復することによってオブジェクトの堅牢性を維持します。Amazon S3 は、チェックサムを用いて、格納されているデータの完全性を定期的に検証しています。破損が検出されると、冗長データを使用して修復されます。S3 に保存されるデータは、1 年間にオブジェクトの 99.999999999% の堅牢性と 99.9% の可用性を提供するよう設計されています。

詳細については、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」

(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon

Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、EC2 上で EBS を使用してハードディスクの RAID 構成を組むなどのディスク障害対策を実施する必要があります。

■ 推奨される追加の実施事項

Amazon EBS では、従来のベアメタルサーバーで利用できる標準的な RAID 設定はすべて使用できます。ただしその RAID 設定が、お使いのインスタンスのオペレーティングシステムでサポートされている必要があります。これは、RAID がすべてソフトウェアレベルで実現されるためです。単一のボリュームで実現できる以上の I/O パフォーマンスを実現するため、RAID 0 では複数のボリュームをともにストライピングできます。インスタンスでの冗長性確保のため、RAID 1 では 2 つのボリュームを同時にミラーリングできます。

Amazon EBS ボリュームのデータは、同じアベイラビリティゾーン内の複数のサーバーにレプリケートされます。これは、コンポーネントの 1 つに障害が発生したことが原因でデータが失われるのを防ぐためです。このレプリケーションにより、一般的なコモディティディスクドライブに比べて Amazon EBS ボリュームの信頼性が 10 倍に高まります。詳細については、Amazon EBS 製品の詳細ページの「Amazon EBS の可用性と耐久性」を参照してください。

また、重要な保護すべきデータは Amazon S3 へバックアップを取得することをお勧めします。OS イメージについては EC2 スナップショット機能を利用することで Amazon S3 上にバックアップを取得することが可能です。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(8)

■ 要求事項 174

必須

全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行うこと。

■ AWS のインフラストラクチャー関連事項

AWS では、ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS リソースを含む電子媒体に格納される情報について機密レベルを示すラベル付けを行う必要があります。

■ 推奨される追加の実施事項

AWS では各種リソースにタグを付与することが可能です。

タグとは、AWS リソースに付けるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもお客様側が定義します。タグを使用すると、AWS リソースを目的、所有者、環境などさまざまな方法で分類することができます。同じ型のリソースが多い場合に役立ちます — 割り当てたタグに基づいて特定のリソースをすばやく識別できます。たとえば、アカウントの各インスタンスの所有者とスタックレベルを追跡しやすくするため、Amazon EC2 インスタンスに対して一連のタグを定義できます。

AWS 各種リソースへのタグ付けは以下 URL を参照ください。

Amazon EC2 リソースのタグ付け（EBS を含む）

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/Using_Tags.html#tag-basics

Amazon S3 リソースのタグ付け

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/object-tagging.html

Amazon Glacier リソースのタグ付け

https://docs.aws.amazon.com/ja_jp/amazonglacier/latest/dev/tagging.html

Amazon EFS リソースのタグ付け

https://docs.aws.amazon.com/ja_jp/efs/latest/ug/manage-fs-tags.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(9)

■ 要求事項 175

必須

電子媒体を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認すること。

■ AWS のインフラストラクチャー関連事項

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

詳細については、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」

(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(1)

■ 要求事項 176

推奨

物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については情報処理事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得ること。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。

■ AWS のインフラストラクチャー関連事項

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

詳細については、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」

(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。

アセットの管理

AWS のアセットは、AWS が所有するアセットの所有者、場所、ステータス、メンテナンス、および 関連する詳細情報を保存および追跡するインベントリ管理システムを通じて、一元管理されています。アセットは、調達後にスキャンおよび追跡され、メンテナンス中のアセットは、所有権、ステータス、およびメンテナンス終了時に、チェックおよびモニタリングされます。

メディアの破壊

ユーザーデータの保存に使用されるメディアストレージデバイスは AWS によって「クリティカル」と分類され、そのライフサイクルを通じて非常に重要な要素として適切に取り扱われます。AWS では、デバイスの設置、修理、および破棄（最終的に不要になった場合）の方法について厳格な基準が設けられています。ストレージデバイスが製品寿命に達した場合、NIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄します。ユーザーデータを保存したメディアは、安全に停止するまで AWS の統制から除外されることはありません。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/controls/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者がハードディスク消去ツール等を用いしかるべき手順でワイプを実施してからボリュームを削除することで、医療機関等との合意事項を満たすようにし、実施した記録を提出する必要があります。

■ 推奨される追加の実施事項

情報処理事業者自身で Amazon EBS のワイプ作業を行うこともできます。また、AWS 上に格納する機密データは、AWS Key Management Service で管理される暗号鍵を利用して暗号化することを推奨します。契約終了時に暗号鍵そのものを廃棄することで、データ消去に相当するといった対応を考慮することも可能となります。

Amazon Elastic Block Store (EBS) で追加のストレージを使う場合などはボリュームを暗号化することができます。S3 を使う場合は Server Side Encryption でバケット・ファイル単位に暗号化することができます。また、サーバサイド暗号化のみでなく、必要に応じてクライアントサイド暗号化の利用を検討してください。

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(2)

■ 要求事項 177

推奨

医療情報システムにおいてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除することが望ましい。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS では、ISO 27001 規格に基づき、AWS リソースに論理的アクセスを認める基準を規定するポリシー文書および手順書を作成済みです。AWS SOC 1 Type II レポートには、AWS リソースに対するアクセスのプロビジョニング管理のために実施している統制の概要が記載されています。

詳細については、「AWS セキュリティプロセスの概要」(<http://aws.amazon.com/security> で入手可能)を参照してください。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療情報システムを構成するサーバーについて不要なデバイスドライバがインストールされていないこと、認められないデバイスの接続を防止する措置を講ずることが望ましい。

■ 推奨される追加の実施事項

AWS Systems Manager を使用することで、OS のインベントリ情報の収集・管理することができます。また、AWS Config を合わせて使用することで、インベントリの変更履歴を管理することができます。これらを利用し、不要なデバイスドライバの追加などを監視・検知することが可能です。

詳細は以下 URL を参照ください。

AWS Systems Manager

<https://aws.amazon.com/jp/systems-manager/>

AWS Config

<https://aws.amazon.com/jp/config/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.7 電子媒体の取扱

(3)

■ 要求事項 178

推奨

不要なデバイスドライバが追加されていないことを定期的に検証することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS では、ISO 27001 規格に基づき、AWS リソースに論理的アクセスを認める基準を規定するポリシー文書および手順書を作成済みです。AWS SOC 1 Type II レポートには、AWS リソースに対するアクセスのプロビジョニング管理のために実施している統制の概要が記載されています。

詳細については、「AWS セキュリティプロセスの概要」(<http://aws.amazon.com/security> で入手可能)を参照してください。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は OS に不要なデバイスドライバが追加されていないことを定期的に検証する必要があります。

■ 推奨される追加の実施事項

AWS Systems Manager インベントリマネージャーを使用して、医療情報システムに利用している OS にインストールされているアプリケーションのインベントリ情報を収集することができます。このインベントリ情報を利用して定期的な検証を行うことができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.8 情報交換に関するセキュリティ

(1)

■ 要求事項 179

必須

次の情報交換方法について予め合意しておくこと。

- 情報を電子媒体に記録して交換する際の手順
- 情報をネットワーク経由で文書ファイル形式にて交換する際の手順
- 情報をネットワーク経由でアプリケーション入力にて交換する際の手順
- 情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順

■ AWS のインフラストラクチャー関連事項

AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。

AWS は、システム出力デバイスへのアクセスを、権限を持つ関係者のみに制限しています。認証を取得するアクセスでは、電子リクエストを提出し、アクセスのビジネスケースを提示して、承認された承認者によるその認証の文書による承認を取得する必要があります。AWS アクセス管理の手順は、SOC、PCI DSS、ISO 27001、および FedRAMPsm への継続的な準拠の一環として、サードパーティの監査人によって個別に確認されます。

個人の電子デバイスやリムーバブルメディアは、AWS 情報システムに接続することが禁止されています。

詳細は以下 URL 掲載のホワイトペーパー「AWS リスクとコンプライアンス」の P116 を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-risk-and-compliance/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療機関等と情報交換方法について予め合意しておく必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.8 情報交換に関するセキュリティ

■ 要求事項 180

必須

■ AWS のインフラストラクチャー関連事項

AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。

AWS は、システム出力デバイスへのアクセスを、権限を持つ関係者のみに制限しています。認証を取得するアクセスでは、電子リクエストを提出し、アクセスのビジネスケースを提示して、承認された承認者によるその認証の文書による承認を取得する必要があります。AWS アクセス管理の手順は、SOC、PCI DSS、ISO 27001、および FedRAMPsm への継続的な準拠の一環として、サードパーティの監査人によって個別に確認されます。

個人の電子デバイスやリムーバブルメディアは、AWS 情報システムに接続することが禁止されています。

詳細は以下 URL 掲載のホワイトペーパー「AWS リスクとコンプライアンス」の P116 を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-risk-and-compliance/>

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。

AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接

続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、情報交換時に以下の事項を実施する必要があります。

- ・発送者、受領者を確認し、発送・受領の記録を行う。
- ・発送者の行為を確実に記録する証跡（発送伝票や電子署名、ログイン認証および履歴の記録）の保存
- ・交換情報の機密レベルの事前合意
- ・交換情報のセキュリティスキャン

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.8 情報交換に関するセキュリティ

(3)

■ 要求事項 181

必須

物理的に情報を搬送する際には以下の対策を実施すること。

- 医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。
- 配送時の作業員については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。
- 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。
- 配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。
- 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。
- 電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。

■ AWS のインフラストラクチャー関連事項

AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。AWS データセンターの環境については、サーバー、ラック、ネットワークデバイス、ハードドライブ、システムハードウェアコンポーネント、および建築資材といった新しい情報システムコンポーネントがデータセンターに出荷される場合、必ずデータセンターマネージャーが事前に承認する必要があり、納品時にはデータセンターマネージャーに通知する必要があります。物品は各 AWS データセンターの搬入口に配送されます。AWS の正社員は、破損や梱包が開封された痕跡がないことを検査し、署名します。物品は配達時に、AWS のアセット管理システムとデバイス在庫追跡システムによりスキャンおよび記録されます。受領された物品は、データセンターのフロアに設置されるまで、データセンター内の機器保管室に置かれます。機器保管室に入るには、ID カードの読み取りと PIN の入力が必要です。物品がデータセンターから搬出される場合、搬出の承認を受ける前に、その物品のスキャン、使用履歴の追跡、データの消去が行われます。AWS のアセット管理のプロセスと手順は、PCI DSS、ISO 27001、および FedRAMP sm のコンプライアンスの監査時に、社外の独立監査人によって確認されます。また、AWS は従業員にセキュリティポリシーおよびセキュリティトレーニングを提供することで、情報セキュリティに関する役割と責任について教育しています。Amazon の基準またはプロトコルに違反した従業員は調査され、適切な懲戒(警告、業績計画、停職、解雇など) が実施されます。詳細については、AWS クラウドセキュリティホワイトペーパー(<http://aws.amazon.com/security> で

入手可能) を参照してください。また、ISO 27001 規格の附属書 A ドメイン 7 を参照してください。AWS は、ISO27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

■ AWS サービス関連情報

-AWS Snowball

Snowball はセキュリティに考慮して設計されたデバイスを使用するペタバイト規模のデータ転送ソリューションで、AWS クラウド内外に大容量データを転送できます。Snowball を使用すると、高いネットワークコスト、長時間かかる転送、セキュリティ面の懸念といった、大規模なデータ転送に関する一般的な課題を解決できます。お客様は、分析データ、ゲノミクスデータ、動画ライブラリ、画像リポジトリ、バックアップの移行に Snowball を使用しています。また、データセンターの閉鎖、テープの置き換え、アプリケーション移行のプロジェクトで一部をアーカイブするために使用しています。Snowball を使うとデータを簡単、迅速、安全に転送でき、コストは高速インターネットによるデータ転送の 5 分の 1 ほどで済みます。最新、詳細情報は下記を参照ください。

<https://aws.amazon.com/jp/snowball/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、医療機関等と合意する基準に基づいて物理的な情報搬送にセキュリティ対策を実施する必要があります。

■ 推奨される追加の実施事項

AWS では、セキュアなデータ転送手段として AWS Snowball を利用し情報の物理的な搬送に利用することができます。AWS Snowball は物理的な輸送をセキュアに行うことができるように設計されたストレージアプライアンスを使用して、テラバイト規模からペタバイト規模のデータを AWS との間で移動するためのデータ転送ソリューションです。Snowball を使用すると、ネットワークのコストが高い、転送時間が長い、セキュリティに懸念があるといった、大規模なデータ転送でよく直面する課題を解決できます。

データの暗号化

Snowball を使用してデータを S3 にインポートする場合、Snowball に転送されるすべてのデータには、2 つのレイヤーの暗号化があります。

- ・暗号化のレイヤーがローカルワークステーションのメモリに適用されます。このレイヤーは、Snowball 用 Amazon S3 Adapter または Snowball クライアント を使用しているかどうかに関係なく適用されます。この暗号化では AES GCM 256 ビットキーが使用され、60 GB のデータが転送されるたびにキーが切り替わります。

- ・SSL 暗号化は、標準 Snowball との間で転送されるすべてのデータの 2 番目の暗号化レイヤーです。AWS Snowball では、保管時のデータを保護するため、サーバー側の暗号化 (SSE) が使用されます。

不正開封の検知

AWS に到着した Snowball は、アプライアンスごとに改ざんの跡がないか検査され、トラステッドプラットフォームモジュー

ル (TPM) を使用して変更が検出されないか検証されます。AWS Snowball では、データ保護のために、不正開封防止筐体、256 ビットの暗号化、およびデータのセキュリティと完全な保管継続性を提供するための業界標準である TPM など、数重に設計されたセキュリティ機能を使用しています。

情報処理事業者に Snowball が到着したらまず、損傷や明らかな改ざんについて検査してください。Snowball に疑わしい点が見つかった場合は、内部ネットワークに接続しないでください。AWS サポートにお問い合わせいただければ、新しい Snowball をお客様宛に配送します。

データの消去

データ転送ジョブの処理と検証が完了すると、AWS では National Institute of Standards and Technology (NIST) の「メディア衛生のためのガイドライン」に従った方法で Snowball アプライアンスのソフトウェア消去を実施します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.8 情報交換に関するセキュリティ

(4)

■ 要求事項 182

電子的に情報を転送する際には以下の対策を実施すること。

- 送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。

認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。

- 送受信する経路は適切な方法で傍受のリスクから保護されていること。

- 受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。
- 送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。

■ AWS のインフラストラクチャー関連事項

AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。

AWS ネットワークは、作業負荷に応じてセキュリティと弾力性のレベルを選択できるように設計されています。詳細については、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」

(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。

■ AWS サービス関連情報

-AWS Direct Connect

AWS Direct Connect により、お客様の設備から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコスト削減、帯域幅のスループットが向上し、インターネットベースの接続よりも均質なネットワークエクスペリエンスを提供できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/directconnect/>

-Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) では、AWS クラウドの論理的に分離されたセクションをプロビジョニングし、お客様が定義した仮想ネットワーク内の AWS リソースを起動することができます。自分の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を完全に制御できます。VPC では、リソースやアプリケーションに安全かつ簡単にアクセスできるよう、IPv4 と IPv6 を両方とも使用できます。Amazon VPC のネットワーク設定は容易にカスタマイズできます。既存のデータセンターと自分の VPC 間にハードウェア仮想プライベートネットワーク (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/vpc/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、電子的に情報転送を実施する際に、相手先の正当性検証、認証、通信経路の保護、改ざん検知などの対策を講じる必要があります。

■ 推奨される追加の実施事項

AWS では、AWS アカウントやリソースを不正使用から保護するためのさまざまなツールや機能を提供されています。これには、アクセスコントロールのための認証情報、暗号化されたデータ転送のための HTTPS エンドポイント、個別の IAM ユーザーアカウントの作成、セキュリティモニタリングのためのユーザーアクティビティのログ記録、および Trusted Advisor セキュリティチェックが含まれます。どの AWS サービスを選択するかにかかわらず、これらすべてのセキュリティツールを利用できます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.13 通信のセキュリティ

A.13.1

A.13.2

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.16 情報セキュリティインシデント管理

A.16.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.9 医療情報システムに対するセキュリティ要求事項

(1)

■ 要求事項 183

必須

■ AWS のインフラストラクチャー関連事項

N/A

医療情報システムに対するセキュリティ対策は情報処理事業者の該当事項となります。

AWS では、ISO27001 規格に準拠した環境の分離を行っています。詳細については、ISO27001 規格の附属書 A ドメイン 12 を参照してください。AWS は、ISO27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、本番環境と開発・テスト環境を作成および保持する機能を持つことができます。たとえば、CloudFormation テンプレートを用い、本番環境と同等の構成を持った開発・テスト環境を任意のタイミングで展開および終了することができ、開発テスト環境のみに開発ツール類を配置することが可能です。

■ 推奨される追加の実施事項

開発ツール類を運用システム上に配置しないことももちろんのこと、AWS IAM の機能を用い、IAM ユーザに付与するポリシーで、本番環境へのアクセスが必要ないユーザには権限を与えないよう、最小権限の原則に則ったユーザ管理を行うことが可能になります。または、本番環境とそれ以外の環境で AWS アカウント単位で分離してしまうことで、より強い分割を行うことができます。AWS Organizations を使うことで、アカウントの作成・管理および各 AWS サービスへのアクセス制御が容易になります。AWS Organizations については下記を参照ください。

<https://aws.amazon.com/jp/organizations/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.9 医療情報システムに対するセキュリティ要求事項

(2)

■ 要求事項 184

必須

情報処理に不必要なファイル等を運用システム上におかないこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、運用システム上に必要のないファイルを配置しない等のセキュリティ対策を実施する必要があります。

■ 推奨される追加の実施事項

不必要なファイルの追加や改ざんなどを検知するために AWS のリポジトリではあらかじめ AIDE が用意されており利用することができます（Linux のみ）。AIDE ではシステム内のファイルやレポジトリ、あるいはソースコードなどが変更された際に管理者に通知するための改ざん検知が行えます。

AWS AIDE は、AWS の AMI のリポジトリにデフォルトで組み込まれている AMI を利用することで、EC2 インスタンスで利用することができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.9 医療情報システムに対するセキュリティ要求事項

(3)

■ 要求事項 185

必須

業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、ソフトウェアの品質を確保するために、機能および自社システムとの整合性を十分確認する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.9 医療情報システムに対するセキュリティ要求事項

(4)

■ 要求事項 186

必須

運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS リソースに関しては、AWS CloudFormation テンプレート等の構成管理用ファイルで定義し、そのテンプレートを使って環境の構築を行うことで、テンプレートファイルをシステムコンポーネントのインベントリとして扱うことができます。デプロイされた AWS 上のシステムに情報処理事業者がインストールするソフトウェアのインベントリ管理については、情報処理事業者の責任となります。

■ 推奨される追加の実施事項

ライブラリプログラムなどのソフトウェアについては、AWS CodeCommit を利用することで版、変更管理が行えます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.9 医療情報システムに対するセキュリティ要求事項

(5)

■ 要求事項 187

必須

システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、システムで利用している AWS リソースに対し、AWS IAM や Amazon S3 を使用して、監査ログのライフサイクルや状態を管理する必要があります。AWS IAM、AWS CloudTrail によって取得した各作業者の操作ログファイルを Amazon S3 にアーカイブし、該当 S3 バケットへのアクセスログ取得を有効にすることで、監査ログへのアクセスを自動的に記録することができます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.10 アプリケーションに対するセキュリティ要求事項

(1)

■ 要求事項 188

必須

提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。

■ AWS のインフラストラクチャー関連事項

N/A

アプリケーションの脆弱性検査および対策は情報処理事業者の該当事項となります。

AWS のシステム開発ライフサイクル(SDLC) は、業界のベストプラクティスを組み込んでおり、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスク評価の完遂などが含まれています。詳細については、AWS セキュリティプロセスの概要を参照してください。また、詳細については、ISO 27001 規格の附属書 A ドメイン 14 を参照してください。AWS は、ISO27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact (<https://console.aws.amazon.com/artifact>) を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示し

た詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者はアプリケーションの脆弱性・安全性検査を定期的実施し対策を行う責任があります。

AWS では、対象をお客様のインスタンスに限定し、かつ AWS 利用規約に違反しない限り、お客様はご自身のクラウドインフラストラクチャーのスキャンを実施する許可をリクエストできます。このようなスキャンについて事前に承認を受けるには、AWS 脆弱性／侵入テストリクエストフォームを使用してリクエストを送信してください。

<https://aws.amazon.com/jp/security/penetration-testing/>

■ 推奨される追加の実施事項

AWS Systems Manager はパッチ管理機能を提供しており、マネージドインスタンスにパッチを適用するプロセスを自動化します。インスタンスをスキャンして見つからないパッチのレポートを表示したり、見つからないパッチをスキャンして自動的にインストールしたりできます。Patch Manager のパッチベースラインには、リリースから数日以内にパッチを自動承認するためのルールと、承認および拒否されたパッチのリストが含まれています。パッチ適用を Systems Manager の メンテナンス時間 タスクとして実行するようスケジュールすることで、パッチを定期的にインストールできます。また、パッチは、Amazon EC2 タグを使用して個別のインスタンスまたは大規模なグループのインスタンスにインストールできます。Patch Manager の詳細は以下を参照ください。

http://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-patch.html

AWS Config は、AWS リソースの設定を評価、監査、審査できるようにするサービスです。Config では、AWS リソースの設定が継続的にモニタリングおよび記録されるため、必要な設定に対する記録された設定の評価を自動的に実行できます。Config を使用すると、AWS リソース間の設定や関連性の変更を確認し、詳細なリソース設定履歴を調べ、社内ガイドラインで指定された設定に対する全体的なコンプライアンスを確認できます。これにより、コンプライアンス監査、

セキュリティ分析、変更管理、運用上のトラブルシューティングを簡素化できます。AWS Config の詳細は以下を確認ください。<https://aws.amazon.com/jp/config/>

Amazon Inspector を使用すると、AWS 評価ターゲット (AWS リソースの集合体) に対処が必要な潜在的なセキュリティ上の問題が存在するかどうかを評価できます。

https://docs.aws.amazon.com/ja_jp/inspector/latest/userguide/inspector_introduction.html

Amazon Inspector では、以下のルールパッケージを利用できます。

- ・共通脆弱性識別子 (CVE)
- ・Center for Internet Security (CIS) ベンチマーク
- ・セキュリティのベストプラクティス
- ・実行時の動作の分析

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.10 アプリケーションに対するセキュリティ要求事項

(2)

■ 要求事項 189

必須

アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。

これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者はアプリケーション稼働に利用する第三者のソフトウェアについて最新の公開される脆弱性情報を把握し迅速に対策を取る責任があります。

Amazon Inspector を使用すると、AWS 評価ターゲット（AWS リソースの集合体）に対処が必要な潜在的なセキュリティ上の問題が存在するかどうかを評価できます。

https://docs.aws.amazon.com/ja_jp/inspector/latest/userguide/inspector_introduction.html

Amazon Inspector では、以下のルールパッケージを利用できます。

- ・共通脆弱性識別子（CVE）
- ・Center for Internet Security（CIS）ベンチマーク
- ・セキュリティのベストプラクティス
- ・実行時の動作の分析

■ 推奨される追加の実施事項

AWS Systems Manager はパッチ管理機能を提供しており、マネージドインスタンスにパッチを適用するプロセスを自動化します。インスタンスをスキャンして見つからないパッチのレポートを表示したり、見つからないパッチをスキャンして自動的にインストールしたりできます。Patch Manager のパッチベースラインには、リリースから数日以内にパッチを自動承認するためのルールと、承認および拒否されたパッチのリストが含まれています。パッチ適用を Systems Manager の メンテナンス時間 タスクとして実行するようスケジュールすることで、パッチを定期的にインストールできます。また、パッチは、Amazon EC2 タグを使用して個別のインスタンスまたは大規模なグループのインスタンスにインストールできます。Patch Manager の詳細は以下を参照ください。

http://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-patch.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6.10 アプリケーションに対するセキュリティ要求事項

(3)

■ 要求事項 190

必須

アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業者はアプリケーションに適切な認証・認可方式を整理し、設計・実装する必要があります。

■ 推奨される追加の実施事項

認証機能の実装時に Amazon Cognito を使用することで、ユーザーのサインアップとサインイン、および OAuth2.0 の機能をアプリケーションに追加できます。Facebook などのソーシャルアカウントでのフェデレーションログインにも対応しており、ユーザを役割に応じたグループに分けて管理することができます。Cognito はフルマネージドサービスであるため、利用することでパスワード等の個人情報を AWS のお客様ご自身のサーバ上で管理する必要がなくなります。Amazon Cognito の機能は公式な AWS ドキュメントにて整理されている他、ご利用中の Cognito User Pools の認証方式などを含む設定情報はマネジメントコンソールおよび AWS CLI/SDK を使っていつでも表示、確認可能です。また、AWS CloudFormation は Amazon Cognito をサポートしているため、CloudFormation のテンプレートとして Amazon Cognito の設定情報を記述し、管理していくことで、常に本番環境との差異がない設計情報の列挙、整理を兼ねることができます。Amazon Cognito についての詳細は下記を参照ください。

<https://aws.amazon.com/jp/documentation/cognito/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.10 アプリケーションに対するセキュリティ要求事項

(4)

■ 要求事項 191

必須

アプリケーションにて医療事業者側の作業者を認証する情報（ID／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は利用者のパスワードを適切に保護するアプリケーションを実装する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.10 アプリケーションに対するセキュリティ要求事項

(5)

■ 要求事項 192

必須

アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者はアプリケーションに適切な認証・認可方式を整理し、設計・実装する必要があります。

■ 推奨される追加の実施事項

認証機能の実装時に Amazon Cognito を使用することで、ユーザーのサインアップとサインイン、および OAuth2.0 の機能をアプリケーションに追加できます。Facebook などのソーシャルアカウントでのフェデレーションログインにも対応しており、ユーザを役割に応じたグループに分けて管理することができます。Cognito はフルマネージドサービスであるため、利用することでパスワード等の個人情報を AWS のお客様ご自身のサーバ上で管理する必要がなくなります。Amazon Cognito の機能は公式な AWS ドキュメントにて整理されている他、ご利用中の Cognito User Pools の認証方式などを含む設定情報はマネジメントコンソールおよび AWS CLI/SDK を使っていつでも表示、確認可能です。また、AWS CloudFormation は Amazon Cognito をサポートしているため、CloudFormation のテンプレートとして Amazon Cognito の設定情報を記述し、管理していくことで、常に本番環境との差異がない設計情報の列挙、整理を兼ねることができます。Amazon Cognito についての詳細は下記を参照ください。

<https://aws.amazon.com/jp/documentation/cognito/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.10 アプリケーションに対するセキュリティ要求事項

(1)

■ 要求事項 193

推奨

アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS では安全性診断を行う専用の環境を必要なときに立ち上げ不要となったら停止または削除を行うことで、コスト効率の良い試験環境の用意が実現できます。情報処理事業者は、これらAWSのメリットを活用し試験環境を用意することが推奨されます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2
A.12.3
A.12.4
A.12.5
A.12.6
A.12.7

A.14 システムの取得、開発及び保守

A.14.1
A.14.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

(1)

■ 要求事項 194

必須

暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト等を用いること。

■ AWS のインフラストラクチャー関連事項

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。また、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、および FedRAMP の監査中に独立監査人によって確認されます。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon

Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS Key Management Service

AWS Key Management Service (KMS) は、データの暗号化に使用する暗号化キーを簡単に作成および管理できるマネージド型サービスで、キーのセキュリティを保護するために FIPS 140-2 で検証されたハードウェアセキュリティモジュールを使用します。AWS Key Management Service は、AWS の他のほとんどすべてのサービスと統合されており、これらのサービスに保存したデータが保護されます。また AWS Key Management Service は AWS CloudTrail とも統合されており、すべてのキーの使用ログを表示できるため、規制およびコンプライアンスの要求に応えるために役立ちます。最新、詳細は下記を参照ください。

<https://aws.amazon.com/jp/kms/>

-AWS CloudHSM

AWS CloudHSM は、クラウドベースのハードウェアセキュリティモジュール (HSM) です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM によって、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリといった業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は規格にも準拠しているため、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。CloudHSM は、ハードウェアのプロビジョニング、ソフトウェアへのパッチ適用、高可用性、バックアップといった時間のかかる管理タスクを自動化する完全マネージド型のサービスです。また、CloudHSM は、オンデマンドで HSM のキャパシティを追加および削除することで、簡単にスケールできます。前払いは必要ありません。

<https://aws.amazon.com/jp/cloudhsm/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、自身が管理するデータの統制と所有権を保持します。また、情報処理事業者は、システムの要件に合うラベリングおよび処理に関するポリシーおよび手続きを実装することができます。情報処理事業者のデータに対する権限制御 (IAM、S3 バケットポリシー等) や暗号化についての詳細は、AWS ウェブサイトの「アマゾンウェブサービス: セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。

■ 推奨される追加の実施事項

AWS では、重要なデータを暗号化する際の暗号鍵を効率的に管理できる AWS Key Management Service (AWS KMS) や AWS CloudHSM サービスも提供しています。伝送中のデータに関しては、電子証明書を発行・管理する Amazon Certificate Manager (ACM) を使い、SSL/TLS 証明書を Amazon CloudFront や ELB に設定することで、安全な通信を実現できます。このリファレンステンプレートでは、サンプルとして自己署名の TLS 証明書が ELB にセットされます。保存されたデータの暗号化に関しては、Amazon Simple Storage Service (S3) や Amazon Elastic Block Store (EBS) で追加のストレージを使う場合などは電子政府推奨暗号リストに掲載されている暗号アルゴリズムでボリュームを暗号化することができます。また、サーバサイド暗号化のみでなく、必要に応じてクライ

アントサイド暗号化の利用を検討してください。

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

(2)

■ 要求事項 195

必須

暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。

■ AWS のインフラストラクチャー関連事項

AWS は、AWS インフラストラクチャー内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。詳細については、ISO27001 附属書 A18.1 を参照してください。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オ

プロジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS Key Management Service

AWS Key Management Service (KMS) は、データの暗号化に使用する暗号化キーを簡単に作成および管理できるマネージド型サービスで、キーのセキュリティを保護するために FIPS 140-2 で検証されたハードウェアセキュリティモジュールを使用します。AWS Key Management Service は、AWS の他のほとんどすべてのサービスと統合されており、

これらのサービスに保存したデータが保護されます。また AWS Key Management Service は AWS CloudTrail とも統合されており、すべてのキーの使用ログを表示できるため、規制およびコンプライアンスの要求に応えるために役立ちます。最新、詳細は下記を参照ください。

<https://aws.amazon.com/jp/kms/>

-AWS CloudHSM

AWS CloudHSM は、クラウドベースのハードウェアセキュリティモジュール (HSM) です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM によって、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリといった業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は規格にも準拠しているため、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。CloudHSM は、ハードウェアのプロビジョニング、ソフトウェアへのパッチ適用、高可用性、バックアップといった時間のかかる管理タスクを自動化する完全マネージド型のサービスです。また、CloudHSM は、オンデマンドで HSM のキャパシティを追加および削除することで、簡単にスケールできます。前払いは必要ありません。

<https://aws.amazon.com/jp/cloudhsm/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は自身のデータの統制と所有権を有しており、データの暗号化および暗号鍵の漏洩対策は情報処理事業者の責任です。AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可されています。これらを活用し暗号鍵が漏洩した際は、直ちに鍵を廃棄し新たな鍵に置き換えることができる暗号鍵の管理の枠組みを構築することが求められます。詳細については、AWS クラウドセキュリティ ホワイトペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。

■ 推奨される追加の実施事項

暗号鍵の管理については、AWS Key Management Systems (KMS)を用いることで鍵へのアクセス権限をキーポリシーおよび IAM で厳密に制御することができます。例えば、通常の開発・運用担当者には本番環境で利用する暗号鍵へのアクセス権を与えず、アプリケーションがデプロイされた EC2 インスタンスからのみ暗号鍵を使うことができるような制御が可能です。KMS 上で鍵を廃棄・再発行することで鍵の漏洩対策が可能です。AWS KMS については、<https://aws.amazon.com/kms/> を参照ください。また、要件に応じて AWS CloudHSM という、クラウドベースのハードウェアセキュリティモジュール (HSM) を利用することも可能です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用でき、廃棄や再発行などの管理ができるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM は業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。AWS CloudHSM の詳細は <https://aws.amazon.com/jp/cloudhsm/> を参照ください。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

(3)

■ 要求事項 196

必須

電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとする。

■ AWS のインフラストラクチャー関連事項

AWS は、AWS インフラストラクチャー内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストに必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。詳細については、ISO27001 附属書 A18.1 を参照してください。

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は自身のシステムで利用する電子署名やネットワーク伝送経路の暗号化などで利用する電子証明書について、信頼できる組織によって発行されたものを利用する責任があります。

■ 推奨される追加の実施事項

情報処理事業は AWS Certificate Manager（ACM）を利用することで、AWS が発行する無料の証明書を利用することができます。ACM で発行された証明書は ELB および Amazon CloudFront で利用することができます。ACM によって発行された証明書は有効期限が近づくと自動的に更新処理が行われるため、更新作業忘れや作業ミスといったリスクの防止にもなります（<https://aws.amazon.com/jp/certificate-manager/>）。ELB および CloudFront では、利用する TLS バージョンの選択と固定が可能です。また、IPSec トンネルによる暗号化の他、必要に応じて Amazon Direct Connect を用いることで専用線によるプライベートなアクセスを実現することができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

■ 要求事項 197

必須

暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。

■ AWS のインフラストラクチャー関連事項

AWS は、AWS インフラストラクチャー内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。詳細については、ISO27001 附属書 A18.1 を参照してください。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS Key Management Service

AWS Key Management Service (KMS) は、データの暗号化に使用する暗号化キーを簡単に作成および管理できるマネージド型サービスで、キーのセキュリティを保護するために FIPS 140-2 で検証されたハードウェアセキュリティモジュールを使用します。AWS Key Management Service は、AWS の他のほとんどすべてのサービスと統合されており、これらのサービスに保存したデータが保護されます。また AWS Key Management Service は AWS CloudTrail とも統合されており、すべてのキーの使用ログを表示できるため、規制およびコンプライアンスの要求に応えるために役立ちます。最新、詳細は下記を参照ください。

<https://aws.amazon.com/jp/kms/>

-AWS CloudHSM

AWS CloudHSM は、クラウドベースのハードウェアセキュリティモジュール (HSM) です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM によって、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリといった業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は規格にも準拠しているため、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。CloudHSM は、ハードウェアのプロビジョニング、ソフトウェアへのパッチ適用、高可用性、バックアップといった時間のかかる管理タスクを自動化する完全マネージド型のサービスです。また、CloudHSM は、オンデマンドで HSM のキャパシティを追加および削除することで、簡単にスケールできます。前払いは必要ありません。

<https://aws.amazon.com/jp/cloudhsm/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は自身のデータの統制と所有権を有しており、データの暗号化および暗号鍵の漏洩対策は情報処理事業者の責任です。AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可されています。これらを活用し暗号アルゴリズムを切り替えができるよう配慮することが求められます。詳細については、AWS クラウドセキュリティホワイトペーパー (<http://aws.amazon.com/security> で入手可能) を参照してください。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

(5)

■ 要求事項 198

必須

医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は医療機関との間で授受するデータの検証で利用する証明書を適切に入手・管理する責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

(1)

■ 要求事項 199

推奨

暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は、AWS インフラストラクチャー内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。詳細については、ISO27001 附属書 A18.1 を参照してください。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key

Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS Key Management Service

AWS Key Management Service (KMS) は、データの暗号化に使用する暗号化キーを簡単に作成および管理できるマネージド型サービスで、キーのセキュリティを保護するために FIPS 140-2 で検証されたハードウェアセキュリティモジュールを使用します。AWS Key Management Service は、AWS の他のほとんどすべてのサービスと統合されており、これらのサービスに保存したデータが保護されます。また AWS Key Management Service は AWS CloudTrail とも統合されており、すべてのキーの使用ログを表示できるため、規制およびコンプライアンスの要求に応えるために役立ちます。最新、詳細は下記を参照ください。

<https://aws.amazon.com/jp/kms/>

-AWS CloudHSM

AWS CloudHSM は、クラウドベースのハードウェアセキュリティモジュール (HSM) です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM によって、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリといった業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は規格にも準拠しているので、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。CloudHSM は、ハードウェアのプロビジョニング、ソフトウェアへのパッチ適用、高可用性、バックアップといった時間のかかる管理タスクを自動化する完全マネージド型のサービスです。また、CloudHSM は、オンデマンドで HSM のキャパシティを追加および削除することで、簡単にスケールできます。前払いは必要ありません。

<https://aws.amazon.com/jp/cloudhsm/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は暗号モジュールで使用する外部からの調達物について、真正性・完全性を確認し利用することが推奨されます。

■ 推奨される追加の実施事項

AWS が提供する SDK には、Amazon S3 のクライアントサイド暗号化機能が含まれているので、暗号モジュール実装時に利用することができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

(2)

■ 要求事項 200

推奨

暗号鍵の生成は耐タンパー性 44 を有する IC カード、USB トークンデバイスといった安全な環境で実施することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は、AWS インフラストラクチャー内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。詳細については、ISO27001 附属書 A18.1 を参照してください。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS Key Management Service

AWS Key Management Service (KMS) は、データの暗号化に使用する暗号化キーを簡単に作成および管理できるマネージド型サービスで、キーのセキュリティを保護するために FIPS 140-2 で検証されたハードウェアセキュリティモジュールを使用します。AWS Key Management Service は、AWS の他のほとんどすべてのサービスと統合されており、これらのサービスに保存したデータが保護されます。また AWS Key Management Service は AWS CloudTrail とも統合されており、すべてのキーの使用ログを表示できるため、規制およびコンプライアンスの要求に応えるために役立ちます。最新、詳細は下記を参照ください。

<https://aws.amazon.com/jp/kms/>

-AWS CloudHSM

AWS CloudHSM は、クラウドベースのハードウェアセキュリティモジュール (HSM) です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM によって、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリといった業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は規格にも準拠しているため、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。CloudHSM は、ハードウェアのプロビジョニング、ソフトウェアへのパッチ適用、高可用性、バックアップといった時間のかかる管理タスクを自動化する完全マネージド型のサービスです。また、CloudHSM は、オンデマンドで HSM のキャパシティを追加および削除することで、簡単にスケールできます。前払いは必要ありません。

<https://aws.amazon.com/jp/cloudhsm/>

■ 情報処理事業者（お客様）の該当事項

暗号鍵の生成時に安全な環境で実施することが推奨されます。

■ 推奨される追加の実施事項

暗号鍵の管理については、AWS Key Management Systems (KMS)を用いることで鍵へのアクセス権限をキーポリシーおよび IAM で厳密に制御することができます。例えば、通常の開発・運用担当者には本番環境で利用する暗号鍵へのアクセス権を与えず、アプリケーションがデプロイされた EC2 インスタンスからのみ暗号鍵を使うことができるような制御が可能です。AWS KMS については、<https://aws.amazon.com/kms/> を参照ください。また、要件に応じて AWS CloudHSM という、クラウドベースのハードウェアセキュリティモジュール (HSM) を利用することも可能です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM は業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。AWS CloudHSM の詳細は <https://aws.amazon.com/jp/cloudhsm/> を参照ください。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

(3)

暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は、AWS インフラストラクチャー内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストに必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP への AWS の継続的な準拠のために、サードパーティーの独立監査人によって確認されます。詳細については、ISO27001 附属書 A18.1 を参照してください。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS Key Management Service

AWS Key Management Service (KMS) は、データの暗号化に使用する暗号化キーを簡単に作成および管理できるマネージド型サービスで、キーのセキュリティを保護するために FIPS 140-2 で検証されたハードウェアセキュリティモジュールを使用します。AWS Key Management Service は、AWS の他のほとんどすべてのサービスと統合されており、これらのサービスに保存したデータが保護されます。また AWS Key Management Service は AWS CloudTrail とも統合されており、すべてのキーの使用ログを表示できるため、規制およびコンプライアンスの要求に応えるために役立ちます。最新、詳細は下記を参照ください。

<https://aws.amazon.com/jp/kms/>

-AWS CloudHSM

AWS CloudHSM は、クラウドベースのハードウェアセキュリティモジュール (HSM) です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM によって、PKCS#11、Java Cryptography Extensions (JCE)、Microsoft CryptoNG (CNG) ライブラリといった業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は規格にも準拠しているので、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。CloudHSM は、ハードウェアのプロビジョニング、ソフトウェアへのパッチ適用、高可用性、バックアップといった時間のかかる管理タスクを自動化する完全マネージド型のサービスです。また、

CloudHSM は、オンデマンドで HSM のキャパシティを追加および削除することで、簡単にスケールできます。前払いはありません。

<https://aws.amazon.com/jp/cloudhsm/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は自身のデータの統制と所有権を有しており、データの暗号化および暗号鍵の管理は情報処理事業者の責任です。

■ 推奨される追加の実施事項

暗号鍵の管理については、AWS Key Management Systems (KMS)を用いることで鍵へのアクセス権限をキーポリシーおよび IAM で厳密に制御することができます。例えば、通常の開発・運用担当者には本番環境で利用する暗号鍵へのアクセス権を与えず、アプリケーションがデプロイされた EC2 インスタンスからのみ暗号鍵を使うことができるような制御が可能です。AWS KMS については、<https://aws.amazon.com/kms/> を参照ください。また、要件に応じて AWS CloudHSM という、クラウドベースのハードウェアセキュリティモジュール (HSM) を利用することも可能です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。CloudHSM で、FIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理できます。CloudHSM は業界標準の API を使用して、アプリケーションを柔軟に統合できます。また、CloudHSM は、商業的に利用可能な他のほとんどの HSM にキーをすべてエクスポートできるようになります。AWS CloudHSM の詳細は <https://aws.amazon.com/jp/cloudhsm/> を参照ください。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.11 暗号による管理策

(4)

■ 要求事項 202

推奨

電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できることが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は医療機関との間で授受するデータの検証を行う環境の整備は暗号アルゴリズムの脆弱化の影響を受けない環境で行うことが推奨されます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.12 ログの取得及び監査

(1)

■ 要求事項 203

必須

作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し、管理すること。

■ AWS のインフラストラクチャー関連事項

AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「CSA Consensus Assessments Initiative Questionnaire」を参照してください。<https://aws.amazon.com/jp/compliance/resources/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、

監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は利用する AWS 環境、ゲスト OS、ソフトウェア及びアプリケーションの監査ログを作成し管理する責任があります。AWS 環境では、各ユーザに適切に IAM ユーザを発行することで、AWS CloudTrail を使用して各ユーザの操作を記録することができます。具体的には、CloudTrail が対応している AWS へのアクセス日時、実行者、実行内容などを記録します。詳細は下記を参照ください。

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>

■ 推奨される追加の実施事項

AWS CloudTrail を使用して、すべての API イベントおよびユーザー、日時、アクションおよび結果を記録することができます。詳細については、AWS ウェブサイトを参照してください。 <https://aws.amazon.com/cloudtrail/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.12 ログの取得及び監査

(2)

■ 要求事項 204

必須

監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。

■ AWS のインフラストラクチャー関連事項

AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「CSA Consensus Assessments Initiative Questionnaire」を参照してください。 <https://aws.amazon.com/jp/compliance/resources/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、

監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は利用する AWS 環境、ゲスト OS、ソフトウェア及びアプリケーションをコントロールし、監視手順を定義する責任があります。

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察といった脅威も、

GuardDuty によって検出されます。検出された異常や脅威、例外情報をフォローアップできるよう、該当する情報が発生したとき適切な連絡先に通知される仕組みなどの整備が必要です。

■ 推奨される追加の実施事項

AWS CloudWatch は、AWS クラウドリソースと AWS 上でお客様が実行するアプリケーションのモニタリングを提供します。詳細については、AWS ウェブサイトを参照してください。 <https://aws.amazon.com/cloudwatch/> また、Amazon Macie は、機械学習によって AWS 内の機密データを自動的に検出、分類、保護するセキュリティサービスです。Amazon Macie では、個人情報（PII）や知的財産などの機密データが認識されます。また、ダッシュボードやアラートが提供されるため、データのアクセスや移動状況を確認できます。この完全マネージドサービスでは、データアクセスアクティビティの異常が継続的にモニタリングされ、不正アクセスの危険や不注意によるデータ漏洩が検出された場合には詳細なアラートが生成されます。 [https://aws.amazon.com/jp/macie/AWS CloudTrail と Amazon CloudWatch の連携設定](https://aws.amazon.com/jp/macie/AWS%20CloudTrail%20and%20Amazon%20CloudWatch%20integration) をすると、特定のオペレーションがあったときに任意の処理やアラート通知を行うことなどが可能になります。

http://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/monitor-cloudtrail-log-files-with-cloudwatch-logs.html たとえば、ログインに数回失敗した IAM ユーザが記録された場合に管理者に通知メールを送りつつ任意の AWS Lambda ファンクションを起動させ、該当 IAM ユーザをロックするなど、動的な対応処理も可能です。IAM ユーザ以外の操作についても、Amazon CloudWatch Logs エージェントを使って OS 上のログファイルを CloudWatch 上で記録することで、やはり条件に合致したログが発生した場合に自動的な対応（警告メールの送信や AWS Lambda 関数の起動など）を取ることができます。また、CloudWatch Logs のサブスクリプションを設定することで、収集したログデータを自動的に Amazon Elasticsearch Service に連携して Kibana で傾向を可視化したり、Amazon Kinesis に連携して柔軟なリアルタイム分析を実装することができます。Amazon CloudWatch Logs については下記を参照ください。

http://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html これらのサービスを活用し、不正や異常の調査（レビューに相当）と検知、およびその対応を自動化して行うことができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.12 ログの取得及び監査

(3)

■ 要求事項 205

必須

ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。

■ AWS のインフラストラクチャー関連事項

AWS 情報システムは、ISO 27001 規格に合わせて、NTP (Network Time Protocol) を介して同期される内部システムクロックを利用しています。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。

■ AWS サービス関連情報

-Amazon Time Sync Service

Amazon Time Sync Service は、Amazon EC2 インスタンスからネイティブでアクセスできる、非常に正確で信頼性の高い時間基準を提供します。Amazon の実績のあるネットワークインフラストラクチャー上に構築されたこのサービスは、AWS リージョン内の冗長性のある衛星電波参照時計や原子参照時計の集合を利用して、協定世界時 (UTC) 世界標準の現在時刻読み取りを配信します。このサービスは、継続的にモニターされる時刻インフラストラクチャーを使用して非常に可用性が高く、参照する時刻ソースのばらつきを低く抑えるように設計されています。うるう秒はアプリケーションでエラーが発生する原因になると知られており、開発者やシステム管理者が懸念していることです。Amazon Time Sync Service では、UTC に定期的に追加されるうるう秒を自動的に均す (smear) ため、お客様はうるう秒の追加によるアプリケーションエラーを心配する必要がありません。将来は、leap smear を使用しない時刻にアクセスする仕組みも提供する予定です。Amazon Virtual Private Cloud (VPC) 内で実行される EC2 インスタンスは、世界中から到達可能な IP アドレスでこのサービスにアクセスできます。

<https://aws.amazon.com/jp/about-aws/whats-new/2017/11/introducing-the-amazon-time-sync-service/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ご自身のアカウント内で起動した Amazon EC2 サーバの時刻設定を正しく保つ権利と責任を有します。AWS では Amazon Time Sync Service を提供し、VPC で実行されているすべてのインスタンスの 169.254.169.123 IP アドレスで NTP を介して利用できます。インスタンスはインターネットにアクセスする必要はなく、アクセスを許可するためにセキュリティグループルールまたはネットワーク ACL ルールを設定する必要はありません。

Amazon Linux では、デフォルトの chrony 設定で Amazon Time Sync サービスの IP アドレスを使用するように設定されています。Red Hat Enterprise Linux (RHEL)、CentOS、Fedora、および Ubuntu ディストリビューションの場合は、chrony 設定ファイルを編集して、Amazon Time Sync サービスのサーバーエントリを追加する必要があります。

あります。詳細は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/set-time.html

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.12 ログの取得及び監査

(4)

■ 要求事項 206

必須

標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。

■ AWS のインフラストラクチャー関連事項

Amazon の実績のあるネットワークインフラストラクチャー上に構築された Amazon Time Sync Service は、AWS リージョン内の冗長性のある衛星電波参照時計や原子参照時計の集合を利用して、協定世界時（UTC）世界標準の現在時刻読み取りを配信します。このサービスは、継続的にモニターされる時刻インフラストラクチャーを使用して非常に可用性が高く、参照する時刻ソースのばらつきを低く抑えるように設計されています。

Amazon Time Sync Service は、Amazon EC2 の一部として提供されており、Amazon EC2 は ISO 27001 認証に含まれています。AWS 情報システムは、ISO 27001 規格に合わせて、NTP (Network Time Protocol) を介して同期される内部システムクロックを利用しています。AWS は、ISO 27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています

https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/CSA_Consensus_Assessments_Initiative_Questionnaire_JP.pdf

■ AWS サービス関連情報

-Amazon Time Sync Service

Amazon Time Sync Service は、Amazon EC2 インスタンスからネイティブでアクセスできる、非常に正確で信頼

性の高い時間基準を提供します。Amazon の実績のあるネットワークインフラストラクチャー上に構築されたこのサービスは、AWS リージョン内の冗長性のある衛星電波参照時計や原子参照時計の集合を利用して、協定世界時 (UTC) 世界標準の現在時刻読み取りを配信します。このサービスは、継続的にモニターされる時刻インフラストラクチャーを使用して非常に可用性が高く、参照する時刻ソースのばらつきを低く抑えるように設計されています。うるう秒はアプリケーションでエラーが発生する原因になると知られており、開発者やシステム管理者が懸念していることです。Amazon Time Sync Service では、UTC に定期的に追加されるうるう秒を自動的に均す (smear) ため、お客様はうるう秒の追加によるアプリケーションエラーを心配する必要がありません。将来は、leap smear を使用しない時刻にアクセスする仕組みも提供する予定です。Amazon Virtual Private Cloud (VPC) 内で実行される EC2 インスタンスは、世界中から到達可能な IP アドレスでこのサービスにアクセスできます。

<https://aws.amazon.com/jp/about-aws/whats-new/2017/11/introducing-the-amazon-time-sync-service/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ご自身のアカウント内で起動した Amazon EC2 サーバの時刻設定を正しく保つ権利と責任を有します。AWS では Amazon Time Sync Service を提供し、VPC で実行されているすべてのインスタンスの 169.254.169.123 IP アドレスで NTP を介して利用できます。インスタンスはインターネットにアクセスする必要はなく、アクセスを許可するためにセキュリティグループルールまたはネットワーク ACL ルールを設定する必要はありません。Amazon Linux では、デフォルトの chrony 設定で Amazon Time Sync サービスの IP アドレスを使用するように設定されています。Red Hat Enterprise Linux (RHEL)、CentOS、Fedora、および Ubuntu ディストリビューションの場合は、chrony 設定ファイルを編集して、Amazon Time Sync サービスのサーバーエントリを追加する必要があります。詳細は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/set-time.html

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.12 ログの取得及び監査

(5)

■ 要求事項 207

必須

ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。

- ログデータにアクセスする作業員及び操作を制限すること。
- 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。
- ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。

■ AWS のインフラストラクチャー関連事項

AWS 事故対応プログラム（事故の検出、調査、および対応）は、ISO 27001 基準に合わせて開発されています。AWS SOC 1 Type II レポートには、AWS が実施している具体的な統制活動の詳細が記載されています。詳細については、「AWS セキュリティプロセスの概要」ホワイトペーパー（<http://aws.amazon.com/security> で入手可能）を参照してください。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション（CRR）は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの

徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS IAM や Amazon S3 を使用して、監査証跡のセキュリティを管理する必要があります。例えば、AWS CloudTrail によって記録された証跡ログファイルを保存した S3 にアクセスできる IAM ユーザを最小限に設定する、S3 のバケットポリシーで不要なアクセスを拒否する、不正なアクセスを検知できるよう監視するなどの対応が必要です。また、CloudTrail ではログファイルの整合性検証機能を提供しています。CloudTrail が配信した後でログファイルが変更、削除、または変更されなかったかどうかを判断するには、CloudTrail ログファイルの整合性の検証を使用することができます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、CloudTrail ログファイルを検出せずに変更、削除、または偽造することは計算上実行不可能になります。詳細は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html Amazon S3 は、Amazon のデータセンターに配置された複数のサーバー間で自動的にデータを複製します。また、バージョニングを使用して、Amazon S3 バケットに格納されたあらゆるオブジェクトのあらゆるバージョンを、格納、取得、復元することができます。バージョニングを使用すれば、意図せぬユーザーアクションからもアプリケーション障害方からも、簡単に回復することができます。詳細は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/Versioning.html

■ 推奨される追加の実施事項

AWS 環境の監査ログのゲスト OS やソフトウェア、アプリケーションに関するログも fluentd などのログ収集ツールを用い S3 などに格納し集中管理することを推奨します。特に AutoScaling 等の伸縮性を持つサービスを利用する際は、インスタンス上のログが永続的に保管されないため、S3 等へ転送し、予期しない消失からの保護が必要です。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.12 ログの取得及び監査

(1)

■ 要求事項 208

推奨

医療情報システムのすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「CSA Consensus Assessments Initiative Questionnaire」を参照してください。

<https://aws.amazon.com/jp/compliance/resources/>

■ AWS サービス関連情報

-Amazon Time Sync Service

Amazon Time Sync Service は、Amazon EC2 インスタンスからネイティブでアクセスできる、非常に正確で信頼性の高い時間基準を提供します。Amazon の実績のあるネットワークインフラストラクチャー上に構築されたこのサービスは、AWS リージョン内の冗長性のある衛星電波参照時計や原子参照時計の集合を利用して、協定世界時（UTC）世界標準の現在時刻読み取りを配信します。このサービスは、継続的にモニターされる時刻インフラストラクチャーを使用して非常に可用性が高く、参照する時刻ソースのばらつきを低く抑えるように設計されています。うるう秒はアプリケーションでエラーが発生する原因になると知られており、開発者やシステム管理者が懸念していることです。Amazon Time

Sync Service では、UTC に定期的に追加されるうるう秒を自動的に均す (smear) ため、お客様はうるう秒の追加によるアプリケーションエラーを心配する必要がありません。将来は、leap smear を使用しない時刻にアクセスする仕組みも提供する予定です。Amazon Virtual Private Cloud (VPC) 内で実行される EC2 インスタンスは、世界中から到達可能な IP アドレスでこのサービスにアクセスできます。

<https://aws.amazon.com/jp/about-aws/whats-new/2017/11/introducing-the-amazon-time-sync-service/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ご自身のアカウント内で起動した Amazon EC2 サーバの時刻設定を正しく保つ権利と責任を有します。AWS では Amazon Time Sync Service を提供し、VPC で実行されているすべてのインスタンスの 169.254.169.123 IP アドレスで NTP を介して利用できます。インスタンスはインターネットにアクセスする必要はなく、アクセスを許可するためにセキュリティグループルールまたはネットワーク ACL ルールを設定する必要はありません。Amazon Linux では、デフォルトの chrony 設定で Amazon Time Sync サービスの IP アドレスを使用するように設定されています。Red Hat Enterprise Linux (RHEL)、CentOS、Fedora、および Ubuntu ディストリビューションの場合は、chrony 設定ファイルを編集して、Amazon Time Sync サービスのサーバーエントリを追加する必要があります。詳細は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/set-time.html

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.12 ログの取得及び監査

(2)

推奨

監査ログに記録する事項としては次のようなものが考えられる。

- 作業情報（作業 ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元 IP アドレス）
- ファイル及びデータへのアクセス、変更、削除記録（作業 ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類）
- データベース操作記録（作業 ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元 IP アドレス、設定変更時にはその内容）
- 修正パッチの適用作業（作業 ID、変更されたファイル）
- 特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内容）
- システム起動、停止イベント
- ログ取得機能の開始、終了イベント
- 外部デバイスの取り外し
- IDS・IPS 等のセキュリティ装置のイベントログ
- サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む）

■ AWS のインフラストラクチャー関連事項

AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「CSA Consensus Assessments Initiative Questionnaire」を参照してください。

<https://aws.amazon.com/jp/compliance/resources/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ

保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、認証とアクセス管理のメカニズムを使用し、root 権限や管理者権限を有するアカウントの操作・変更・追加・削除を記録する必要があります。各ユーザに適切に IAM ユーザを発行することで、AWS CloudTrail を使用して AWS リソースに関する各ユーザの操作を記録することができます。具体的には、CloudTrail が対応している AWS へのアクセス日時、実行者、実行内容などを記録します。詳細は下記を参照ください。

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>Amazon S3 上に保管されたファイルへのアクセスは、S3 のアクセスログ機能を有効にすることによって記録できます。詳細は下記を参照ください。https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/ServerLogs.html

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6.12 ログの取得及び監査

■ 要求事項 210

推奨

監査ログを検証するため、作業者がアクセスした医療情報等を迅速に確認できるよう、作業者 ID と、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

医療情報の監査ログ取得および参照環境の整備は情報処理事業者の該当事項となります。

AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「CSA Consensus Assessments Initiative Questionnaire」を参照してください。

<https://aws.amazon.com/jp/compliance/resources/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、

保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、監査ログを迅速に確認できるよう、監査ログ参照環境を整備することが推奨されます。

■ 推奨される追加の実施事項

AWS 環境の監査ログのゲスト OS やソフトウェア、アプリケーションに関するログも fluentd などのログ収集ツールを用い S3 などに格納し集中管理することを推奨します。特に AutoScaling 等の伸縮性を持つサービスを利用する際は、インスタンス上のログが永続的に保管されないため、S3 等へ転送し、予期しない消失からの保護が必要です。S3 に格納したログを Amazon Athena で提供されるクエリサービスを用い標準的な SQL を使用し簡単に分析を行う環境を整備す

ることができます。また、Athena でスキーマ定義されたログは、Amazon QuickSight を利用し、GUI でアドホック分析・視覚化が行えます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.12 ログの取得及び監査

■ 要求事項 211

推奨

ログを集中させ問題の検出を一箇所で確実にを行うことを目的として、システムとして可能な場合は専用のログサーバにログデータを集約して分析管理することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP コンプライアンスへの AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「CSA Consensus Assessments Initiative Questionnaire」を参照してください。

<https://aws.amazon.com/jp/compliance/resources/>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、

監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ログの集中管理を行う環境の整備を行うことが推奨されます。

■ 推奨される追加の実施事項

AWS 環境の監査ログのゲスト OS やソフトウェア、アプリケーションに関するログも fluentd などのログ収集ツールを用い S3 などに格納し集中管理することを推奨します。特に AutoScaling 等の伸縮性を持つサービスを利用する際は、インスタンス上のログが永続的に保管されないため、S3 等へ転送し、予期しない消失からの保護が必要です。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6.13 アクセス制御方針

(1)

■ 要求事項 212

必須

情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること

■ AWS のインフラストラクチャー関連事項

AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。静的コード分析ツールは、標準ビルドプロセスの一環として実行され、配備される全ソフトウェアは、注意深く選択された業界の専門家によって実行される反復侵入テストを受けます。当社のセキュリティリスク査定のレビューは、設計段階に開始され、この作業はソフトウェアの立ち上げ後まで続きます。

詳細は以下の URL を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-security-processes/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

AWS 利用時には、AWS の各サービス・リソースを情報処理に用いる装置ととらえ AWS リソースを管理するために必要な ID などのセキュリティ要求事項を整理する必要があります。AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.13 アクセス制御方針

(2)

■ 要求事項 213

必須

情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること

■ AWS のインフラストラクチャー関連事項

AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。静的コード分析ツールは、標準ビルドプロセスの一環として実行され、配備される全ソフトウェアは、注意深く選択された業界の専門家によって実行される反復侵入テストを受けます。当社のセキュリティリスク査定のレビューは、設計段階に開始され、この作業はソフトウェアの立ち上げ後まで継続します。

詳細は以下の URL を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-security-processes/>

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

AWS のサービスに関する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.13 アクセス制御方針

(3)

■ 要求事項 214

必須

アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定すること。

■ AWS のインフラストラクチャー関連事項

AWS は、ISO 27001 規格に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正式なポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

<https://console.aws.amazon.com/artifact>

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

お客様は、ゲスト OS、ソフトウェア及びアプリケーションの統制を有しており、各種リソースへのアクセス権および操作権限を管理する責任があります。

■ 推奨される追加の実施事項

IAM ロール、ポリシーおよびグループを使用して、システムコンポーネントやデータへのアクセス権限を管理することができます。また、Amazon S3 ではバケットポリシーや ACL の設定により詳細なファイルの権限管理が可能です。不用意にファイルを公開してしまわないよう注意してください。S3 上のファイルへのアクセス管理については、下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/s3-access-control.html 必要なユーザにはそれぞれ AWS IAM ユーザを作成し、ユーザ情報を複数人で共有しないでください。権限を必要な範囲に限定した IAM ポリシーを、必要な担当者だけに付与する他、IAM グループを利用して同じ権限を持つ担当者群を効率的に管理することができます。また、root アカウントや特権的なユーザの利用は最小限にとどめ、該当アカウントには MFA を設定した上で通常時はアカウントをロックしておくなど、IAM のベストプラクティスに従うことをお勧めします。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.13 アクセス制御方針

(4)

■ 要求事項 215

必須

それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。

■ AWS のインフラストラクチャー関連事項

AWS は、ISO 27001 規格に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正式なポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理する

ために用意されている統制の概要が記載されています。詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。
<https://console.aws.amazon.com/artifact>

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。また、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、および FedRAMP の監査中に独立監査人によって確認されます。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムや

ワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

お客様は、ゲスト OS、ソフトウェア及びアプリケーションの統制を有しており、各種リソースへのアクセス権および操作権限を管理する責任があります。

■ 推奨される追加の実施事項

IAM ロール、ポリシーおよびグループを使用して、システムコンポーネントやデータへのアクセス権限を管理することができます。また、Amazon S3 ではバケットポリシーや ACL の設定により詳細なファイルの権限管理が可能です。不用意にファイルを公開してしまわないよう注意してください。S3 上のファイルへのアクセス管理については、下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/s3-access-control.html 必要なユーザーにはそれぞれ AWS IAM ユーザを作成し、ユーザー情報を複数人で共有しないでください。権限を必要な範囲に限定した IAM ポリシーを、必要な担当者だけに付与する他、IAM グループを利用して同じ権限を持つ担当者群を効率的に管理することができます。また、root アカウントや特権的なユーザーの利用は最小限にとどめ、該当アカウントには MFA を設定した上で通常時はアカウントをロックしておくなど、IAM のベストプラクティスに従うことをお勧めします。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.13 アクセス制御方針

(5)

■ 要求事項 216

必須

業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定すること。

■ AWS のインフラストラクチャー関連事項

AWS は、ISO 27001 規格に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正式なポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

<https://console.aws.amazon.com/artifact>

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。また、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、および FedRAMP の監査中に独立監査人によって確認されます。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要

件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するた

めの仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

お客様は、ゲスト OS、ソフトウェア及びアプリケーションの統制を有しており、各種リソースへのアクセス権および操作権限を管理する責任があります。

■ 推奨される追加の実施事項

IAM ロール、ポリシーおよびグループを使用して、システムコンポーネントやデータへのアクセス権限を管理することができます。また、Amazon S3 ではバケットポリシーや ACL の設定により詳細なファイルの権限管理が可能です。不用意にファイルを公開してしまわないよう注意してください。S3 上のファイルへのアクセス管理については、下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/s3-access-control.html 必要なユーザにはそれぞれ AWS IAM ユーザを作成し、ユーザ情報を複数人で共有しないでください。権限を必要な範囲に限定した IAM ポリシーを、必要な担当者だけに付与する他、IAM グループを利用して同じ権限を持つ担当者群を効率的に管

理することができます。また、root アカウントや特権的なユーザの利用は最小限にとどめ、該当アカウントには MFA を設定した上で通常時はアカウントをロックしておくなど、IAM のベストプラクティスに従うことをお勧めします。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.13 アクセス制御方針

(1)

■ 要求事項 217

推奨

作業者に与えられた権限外の情報や権限外の操作画面を表示しないよう権限管理を行うことが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は、ISO 27001 規格に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正式なポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。
<https://console.aws.amazon.com/artifact>

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。また、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様と

は論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、および FedRAMP の監査中に独立監査人によって確認されます。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになり

ます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

お客様は、ゲスト OS、ソフトウェア及びアプリケーションの統制を有しており、各種リソースへのアクセス権および操作権限を管理する責任があります。

■ 推奨される追加の実施事項

IAM ロール、ポリシーおよびグループを使用して、システムコンポーネントやデータへのアクセス権限を管理することができます。また、Amazon S3 ではバケットポリシーや ACL の設定により詳細なファイルの権限管理が可能です。不用意にファイルを公開してしまわないよう注意してください。S3 上のファイルへのアクセス管理については、下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/s3-access-control.html 必要なユーザにはそれぞれ AWS IAM ユーザを作成し、ユーザ情報を複数人で共有しないでください。権限を必要な範囲に限定した IAM ポリシーを、必要な担当者だけに付与する他、IAM グループを利用して同じ権限を持つ担当者群を効率的に管理することができます。また、root アカウントや特権的なユーザの利用は最小限にとどめ、該当アカウントには MFA を設定した上で通常時はアカウントをロックしておくなど、IAM のベストプラクティスに従うことをお勧めします。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.13 アクセス制御方針

(2)

■ 要求事項 218

推奨

定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は、ISO 27001 規格に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正式なポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。
<https://console.aws.amazon.com/artifact>

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。また、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC、ISO 27001、PCI、ITAR、および FedRAMP の監査中に独立監査人によって確認されます。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクテ

イティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

お客様は、ゲスト OS、ソフトウェア及びアプリケーションの統制を有しており、各種リソースへのアクセス権および操作権限を管理する責任があります。

■ 推奨される追加の実施事項

IAM ロール、ポリシーおよびグループを使用して、システムコンポーネントやデータへのアクセス権限を管理することができます。また、Amazon S3 ではバケットポリシーや ACL の設定により詳細なファイルの権限管理が可能です。不用意にファイルを公開してしまわないよう注意してください。S3 上のファイルへのアクセス管理については、下記を参照ください。

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/s3-access-control.html 必要なユーザにはそれぞれ AWS IAM ユーザを作成し、ユーザ情報を複数人で共有しないでください。権限を必要な範囲に限定した IAM ポリシーを、必要な担当者だけに付与する他、IAM グループを利用して同じ権限を持つ担当者群を効率的に管理することができます。また、root アカウントや特権的なユーザの利用は最小限にとどめ、該当アカウントには MFA を設定した上で通常時はアカウントをロックしておくなど、IAM のベストプラクティスに従うことをお勧めします。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(1)

■ 要求事項 219

必須

[作業者 ID]

作業者は情報処理装置上においてユニークな作業者 ID により識別されること。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。（<https://aws.amazon.com/jp/compliance/resources/>）AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact（<https://console.aws.amazon.com/artifact>）を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。

- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、使用してユーザーIDの管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。認証情報には、パスワード、暗号キー、デジタル署名、および証明書が含まれます。また、AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証 (MFA) を要求するオプションもあります。IAM を利用して ID のフェデレーションによる ID 管理も可能です。IAM の詳細については、下記の URL を参照ください。https://aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ 推奨される追加の実施事項

個々の作業者に割り当てる IAM ユーザについては別途作成するか、または IAM のフェデレーションを用いて外部の ID プロバイダ (Active Directory など) と連携するなどして別途管理する必要があります。IAM でユーザを管理する場合、パスワードの条件や MFA などの要件を IAM で設定できます。その他の IAM の設計、運用に関するベストプラクティスは下記の URL を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(2)

■ 要求事項 220

作業者 ID を発行する際に、既存の ID との重複を排除する仕組みを導入すること。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。（<https://aws.amazon.com/jp/compliance/resources/>） AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact（<https://console.aws.amazon.com/artifact>）を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、使用してユーザーIDの管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。認証情報には、パスワード、暗号キー、デジタル署名、および証明書が含まれます。また、AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証（MFA）を要求するオプションもあります。IAM を利用して ID のフェデレーションによる ID 管理も可能です。IAM の詳細については、下記の URL を参照ください。 https://aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html のベストプラクティスについては、下記の URL を参照してください

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ 推奨される追加の実施事項

個々の作業者に割り当てる IAM ユーザについては別途作成するか、または IAM のフェデレーションを用いて外部の ID プロバイダ（Active Directory など）と連携するなどして別途管理する必要があります。IAM でユーザを管理する場合、パスワードの条件や MFA などの要件を IAM で設定できます。その他の IAM の設計、運用に関するベストプラクティスは下記の URL を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(3)

■ 要求事項 221

複数作業で共用するためのグループ ID の利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者 ID でログオンしてからグループ ID に変更する仕組みを利用すること。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。（<https://aws.amazon.com/jp/compliance/resources/>） AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細につ

いては、AWS Artifact (<https://console.aws.amazon.com/artifact>) を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、

総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、使用してユーザーIDの管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。認証情報には、パスワード、暗号キー、デジタル署名、および証明書が含まれます。また、AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証（MFA）を要求するオプションもあります。IAM を利用して ID のフェデレーションによる ID 管理も可能です。IAM の詳細については、下記の URL を参照ください。https://aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.htmlのベストプラクティスについては、下記の URL を参照してください

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ 推奨される追加の実施事項

セキュリティ認証情報共有してはいけません。その代わりに、IAM ロールを使用します。他の IAM ユーザーに許可されている権限を指定するルールを定義できます。また、そのルールを引き受けることが許可されている IAM ユーザーを持つ AWS アカウントを指定することで、権限を委託することができます。その他の IAM の設計、運用に関するベストプラクティスは下記の URL を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(4)

■ 要求事項 222

作業者 ID の発行は医療情報システムの管理に必要な最小限の人数に留めること。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。（<https://aws.amazon.com/jp/compliance/resources/>） AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact（<https://console.aws.amazon.com/artifact>）を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになり

ます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、使用してユーザーIDの管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。認証情報には、パスワード、暗号キー、デジタル署名、および証明書が含まれます。また、AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証（MFA）を要求するオプションもあります。IAM を利用して ID のフェデレーションによる ID 管理も可能です。IAM の詳細については、下記の URL を参照ください。<https://aws.amazon.com/iam/IAM>のベストプラクティスについては、下記の URL を参照してください

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ 推奨される追加の実施事項

IAM ポリシーを作成するとき、最小限の特権を認めるという標準的なセキュリティアドバイスに従いましょう。そうすれば、タスクを実行するというリクエストのアクセス許可のみを認めることができます。ユーザーが何をする必要があるのかを決定し、それから各ユーザーに見合ったポリシーを作成します。そうすることにより、ユーザーは、それらのタスクのみを実行します。詳細は IAM の設計、運用に関するベストプラクティス（下記の URL）を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(5)

■ 要求事項 223

■ AWS のインフラストラクチャー関連事項

アカウントの確認および監査

アカウントは 90 日ごとにレビューされます。明示的な再承認が必要となり、これを行わない場合は、リソースに対するアクセス権が自動的に取り消されます。従業員の記録が Amazon のヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。Windows および UNIX のアカウントは無効となり、Amazon の権限管理システムは全システムからそのユーザーを削除します。

アクセスに関する変更リクエストは、Amazon 権限管理ツールの監査ログに記録されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。承認しない場合、アクセス権は自動的に取り消されます。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、使用してユーザーIDの管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。認証情報には、パスワード、暗号キー、デジタル署名、および証明書が含まれます。また、AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証（MFA）を要求するオプションもあります。IAM を利用して ID のフェデレーションによる ID 管理も可能です。IAM の詳細については、下記の URL を参照ください。<https://aws.amazon.com/jam/IAM>のベストプラクティスについては、下記の URL を参照してください

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ 推奨される追加の実施事項

IAM ユーザーの不要な認証情報（パスワードとアクセスキー）は削除します。たとえば、アプリケーションに使用される IAM ユーザーはパスワードを必要としません（パスワードは、AWS ウェブサイトへのサインインにのみ必要です）。同様

に、ユーザーがアクセスキーを使用しておらず、今後も使用する予定がない場合、そのユーザーがアクセスキーを持つ理由はありません。最近使用されていないパスワードやアクセスキーは削除の対象となります。使用していないパスワードまたはアクセスキーを検索するには、コンソールか API を使用するか、認証情報レポートをダウンロードします。

詳細は IAM の設計、運用に関するベストプラクティス（下記の URL）を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(6)

■ 要求事項 224

監視ログの監査時に作業者を確実に特定するため、作業者 ID は過去に使われたものを再利用しないこと。

■ AWS のインフラストラクチャー関連事項

アカウントの確認および監査

アカウントは 90 日ごとにレビューされます。明示的な再承認が必要となり、これを行わない場合は、リソースに対するアクセス権が自動的に取り消されます。従業員の記録が Amazon のヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。Windows および UNIX のアカウントは無効となり、Amazon の権限管理システムは全システムからそのユーザーを削除します。

アクセスに関する変更リクエストは、Amazon 権限管理ツールの監査ログに記録されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。承認しない場合、アクセス権は自動的に取り消されます。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6.14 作業者アクセス及び作業者 ID の管理

(7)

■ 要求事項 225

不要な作業者 ID が残っていないことを定期的に確認すること。

■ AWS のインフラストラクチャー関連事項

アカウントの確認および監査

アカウントは 90 日ごとにレビューされます。明示的な再承認が必要となり、これを行わない場合は、リソースに対するアク

セス権が自動的に取り消されます。従業員の記録が Amazon のヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。Windows および UNIX のアカウントは無効となり、Amazon の権限管理システムは全システムからそのユーザーを削除します。

アクセスに関する変更リクエストは、Amazon 権限管理ツールの監査ログに記録されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。承認しない場合、アクセス権は自動的に取り消されます。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、

AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブ
ロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty
によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの
徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、
総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクテ
ィビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch
Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムや
ワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスで
す。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監
視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他
の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。
このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになり
ます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事
業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

AWS 環境では Identity and Access Management を利用し、使用されていない IAM ユーザーやパスワードまたは
アクセスキーを検索することができます。検索を行うには、コンソールか API を使用するか、認証情報レポートをダウンロ
ードします。

詳細は IAM の設計、運用に関するベストプラクティス（下記の URL）を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(1)

■ 要求事項 226

推奨

[作業者 ID]

アクセスを許可された作業者 ID のアクセス可能範囲が許可された通りとなっていること（不正に変更されていないこと）を定期的に確認することが望ましい。

■ AWS のインフラストラクチャー関連事項

アカウントの確認および監査

アカウントは 90 日ごとにレビューされます。明示的な再承認が必要となり、これを行わない場合は、リソースに対するアクセス権が自動的に取り消されます。従業員の記録が Amazon のヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。Windows および UNIX のアカウントは無効となり、Amazon の権限管理システムは全システムからそのユーザーを削除します。

アクセスに関する変更リクエストは、Amazon 権限管理ツールの監査ログに記録されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。承認しない場合、アクセス権は自動的に取り消されます。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(1)

■ 要求事項 227

必須

[特権 ID]

特権 ID の発行は必要な最小限のものに留めること。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。<https://aws.amazon.com/jp/compliance/resources/> AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細につ

いては、AWS Artifact (<https://console.aws.amazon.com/artifact>) を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの

徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業アクセス及び作業 ID の管理

(2)

■ 要求事項 228

特権使用者に昇格可能な作業者 ID を制限すること。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。 [https://aws.amazon.com/jp/compliance/resources/ AWS SOC レポート](https://aws.amazon.com/jp/compliance/resources/AWS%20SOC%20レポート)には、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact (<https://console.aws.amazon.com/artifact>) を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユ

ーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(3)

■ 要求事項 229

特権の使用時には作業実施内容を記録すること。

■ AWS のインフラストラクチャー関連事項

既存の AWS インフラストラクチャーに対する定期的な変更、緊急の変更、および設定の変更は、類似するシステムの業界基準に従って、許可、記録、テスト、承認、および文書化されます。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、認証とアクセス管理のメカニズムを使用し、root 権限や管理者権限を有するアカウントの操作・変更・追加・削除を記録する必要があります。各ユーザに適切に IAM ユーザを発行することで、AWS CloudTrail を使用して各ユーザの操作を記録することができます。具体的には、CloudTrail が対応している AWS へのアクセス日時、実行者、実行内容などを記録します。詳細は下記を参照ください。

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-user-guide.html>Amazon S3 上に保管されたファイルへのアクセスは、S3 のアクセスログ機能を有効にすることによって記録できます。詳細は下記を参照ください。https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/ServerLogs.html

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1
A.12.2
A.12.3
A.12.4
A.12.5
A.12.6
A.12.7

A.14 システムの取得，開発及び保守

A.14.1
A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1
A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理 (4)

■ 要求事項 230

管理端末以外からの特権 ID による直接ログインを禁止すること。

■ AWS のインフラストラクチャー関連事項

AWS 本稼働環境のネットワークは、Amazon 社内ネットワークから分離されており、論理的アクセスのために個別の認証情報が必要です。Amazon 社内ネットワークは、ユーザー ID、パスワード、Kerberos に依存しています。一方、AWS 本稼働環境のネットワークは拠点ホストを介した SSH 公開キー認証が必要となります。

AWS クラウドのコンポーネントにアクセスする必要がある Amazon 社内ネットワーク上の AWS 開発者と管理者は、AWS アクセス管理システムを通して明示的にアクセスをリクエストしなければなりません。すべてのリクエストは、適切な所有者または管理者によって確認および承認されます。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、IAM ポリシーを利用することで、ソース IP アドレスなどを用いた接続元端末の制限が可能です。

詳細は IAM の設計、運用に関するベストプラクティス（下記の URL）を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得, 開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(1)

■ 要求事項 231

推奨

[特権 ID]

特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は、ISO 27001 規格に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正式なポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

<https://console.aws.amazon.com/artifact>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します (パスワードの失効を許可します)。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、使用してユーザーIDの管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。認証情報には、パスワード、暗号キー、デジタル署名、および証明書が含まれます。また、AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証（MFA）を要求するオプションもあります。IAM を利用して ID のフェデレーションによる ID 管理も可能です。IAM の詳細については、下記の URL を参照ください。 https://aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html のベストプラクティスについては、下記の URL を参照してください

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ 推奨される追加の実施事項

開発時、運用時を問わず AWS ルートアカウントの使用は推奨されません。Multi-Factor Authentication を有効化したうえで、ルートアカウントは利用せず役割に応じて IAM ユーザーを作成し利用することを推奨します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(2)

■ 要求事項 232

システムの機能として可能であれば、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改ざん、削除など不正な行為を防止することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS は、ISO 27001 規格に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正式なポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。
<https://console.aws.amazon.com/artifact>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するた

めの仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、使用してユーザーIDの管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。認証情報には、パスワード、暗号キー、デジタル署名、および証明書が含まれます。また、AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証（MFA）を要求するオプションもあります。IAM を利用して ID のフェデレーションによる ID 管理も可能です。IAM の詳細については、下記の URL を参照ください。https://aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.htmlのベストプラクティスについては、下記の URL を参照してください

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ 推奨される追加の実施事項

開発時、運用時を問わず AWS ルートアカウントの使用は推奨されません。Multi-Factor Authentication を有効化したうえで、ルートアカウントは利用せず IAM ユーザーを作成し利用することを推奨します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(1)

■ 要求事項 233

必須

[パスワード]

情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。

■ AWS のインフラストラクチャー関連事項

AWS は、ISO 27001 規格に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正式なポリシー、手続きを規定しています。AWS SOC レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」(<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介 (日本語)) を参照してください。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

<https://console.aws.amazon.com/artifact>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユ

ーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(2)

■ 要求事項 234

医療情報システムへのログイン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。

- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(3)

■ 要求事項 235

医療情報システムへのログイン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

AWS に関する ID のパスワード管理は、AWS Identity and Access Management (IAM) サービスのパスワードポリシーを利用することで、パスワードに関する複雑な要件を実装することができます。詳細については、AWS のウェブサイト (<http://aws.amazon.com/mfa>) を参照してください。

■ 推奨される追加の実施事項

IAM ユーザーのパスワードポリシーを使用して、次の操作を実行できます。

- パスワードの最小の長さを設定する。

- 大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。

- すべての IAM ユーザーが自分のパスワードを変更できるようにします。

指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。

- IAM ユーザーが以前のパスワードを再利用できないようにします。

- IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(4)

■ 要求事項 236

医療情報システムへのログイン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクテ

イティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

AWS に関係する ID のパスワード管理は、AWS Identity and Access Management (IAM) サービスのパスワードポリシーを利用することで、パスワードに関する複雑な要件を実装することができます。詳細については、AWS のウェブサイト (<http://aws.amazon.com/mfa>) を参照してください。

■ 推奨される追加の実施事項

IAM ユーザーのパスワードポリシーを使用して、次の操作を実行できます。

- パスワードの最小の長さを設定する。
 - 大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
 - すべての IAM ユーザーが自分のパスワードを変更できるようにします。
- 指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- IAM ユーザーが以前のパスワードを再利用できないようにします。
 - IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(5)

■ 要求事項 237

パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

AWS CloudTrail と Amazon CloudWatch の連携設定をすると、特定のオペレーションがあったときに任意の処理やアラート通知を行うことなどが可能になります。

http://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/monitor-cloudtrail-log-files-with-cloudwatch-logs.html たとえば、ログインに数回失敗した IAM ユーザが記録された場合に管理者に通知メー

ルを送りつつ任意の AWS Lambda ファンクションを起動させ、該当 IAM ユーザをロックするなど、動的な対応処理も可能です。IAM ユーザ以外の操作についても、Amazon CloudWatch Logs エージェントを使って OS 上のログファイルを CloudWatch 上で記録することで、やはり条件に合致したログが発生した場合に自動的な対応を取ることができます。

http://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(6)

■ 要求事項 238

パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウント

に設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- パスワードの最小の長さを設定する。
- 大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- 指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- IAM ユーザーが以前のパスワードを再利用できないようにします。
- IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになり

ます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

AWS に関係する ID のパスワード発行の際は、WS Identity and Access Management (IAM) サービスのパスワード管理機能を利用し次回ログイン時点で強制的にパスワードを変更させることができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(7)

■ 要求事項 239

パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実にすること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監

視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

■ 要求事項 240

パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムや

ワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得, 開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(9)

■ 要求事項 241

パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブ

ロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(1)

推奨

[パスワード]

作業者が医療情報システムへのログイン用パスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、作業者が設定しようとする品質の低いパスワードを認めないシステムの導入等を検討することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

IAM ユーザーのパスワードポリシーを使用して、パスワードの品質を一定以上に保証することができます。

- パスワードの最小の長さを設定する。

- 大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。

- すべての IAM ユーザーが自分のパスワードを変更できるようにします。

指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。

- IAM ユーザーが以前のパスワードを再利用できないようにします。

- IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(2)

■ 要求事項 243

パスワードの品質基準としては、パスワードを十分に長くすること（8 文字以上等）、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。

- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。

- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。

- ・IAM ユーザーが以前のパスワードを再利用できないようにします。

- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

IAM ユーザーのパスワードポリシーを使用して、パスワードの品質を一定以上に保証することができます。

- パスワードの最小の長さを設定する。

- 大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。

- すべての IAM ユーザーが自分のパスワードを変更できるようにします。

指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。

- IAM ユーザーが以前のパスワードを再利用できないようにします。

- IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(1)

■ 要求事項 244

必須

[作業者]

端末又はセッションの乗っ取りのリスクを低減するため、作業者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行うこと。

■ AWS のインフラストラクチャー関連事項

AWS は、内部者による不適切なアクセスの脅威に対処するための統制を提供しています。取得している認証とサードパーティーによる証明で、論理アクセスの予防統制と発見的統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。（<https://aws.amazon.com/jp/compliance/resources/>） AWS SOC レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact（<https://console.aws.amazon.com/artifact>）を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

AWS または IAM アカウント認証情報を使用して AWS マネジメントコンソールにサインインしてから 12 時間が経過すると、セキュリティのためにログインセッションが失効します。セッションが失効した後で作業を再開するには、再ログインの実施を強制することが可能です。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(2)

■ 要求事項 245

パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定すること。連続してログオンが失敗した場合は再入力を一定期間受け付けない機構とすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。

- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

AWS で現在使用可能なパスワードポリシー設定では、サインインの試行が指定回数失敗した後でユーザーをアカウントからロックアウトする、一般的に "ロックアウトポリシー" と呼ばれるものを作成することができないため、この種類の強化されたセキュリティを実現するには、パスワードポリシーと Multi-Factor Authentication (MFA) を組み合わせることを推奨します。もしくは追加の実施事項に記載の内容でロックアウトポリシーを実装することを推奨します。

■ 推奨される追加の実施事項

AWS CloudTrail と Amazon CloudWatch の連携設定をすると、特定のオペレーションがあったときに任意の処理やアラート通知を行うことなどが可能になります。

http://docs.aws.amazon.com/ja_jp/awsccloudtrail/latest/userguide/monitor-cloudtrail-log-files-with-cloudwatch-logs.html たとえば、ログインに数回失敗した IAM ユーザが記録された場合に管理者に通知メールを送りつつ任意の AWS Lambda ファンクションを起動させ、該当 IAM ユーザをロックするなど、動的な対応処理も可能です。IAM ユーザ以外の操作についても、Amazon CloudWatch Logs エージェントを使って OS 上のログファイルを CloudWatch 上で記録することで、やはり条件に合致したログが発生した場合に自動的な対応を取ることができます。
http://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(1)

■ 要求事項 246

推奨

[作業者]

不正なアカウントの利用又は試みが行われたことを作業者自身で検出するため、作業者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、

総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(2)

■ 要求事項 247

必須

不正なアカウントの利用を防ぐため、作業者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限することが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブ

ロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、IAM ポリシーでは、実行可能な範囲内で、どの IAM ポリシーがリソースにアクセスできるかという条件を定義します。たとえば、要求が発生しなければならない許容 IP アドレスの範囲を指定するための条件を記述できます。また、指定した日付範囲または時間範囲内でのみリクエストが許可されるように指定することもできます。また、SSL または MFA（多要素認証）の使用を必要とする条件を設定することもできます。たとえば、Amazon EC2 インスタンスを終了できるようにするため、ユーザーに対し MFA デバイスの認証を要求することもできます。

詳細は IAM の設計、運用に関するベストプラクティス（下記の URL）を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(3)

■ 要求事項 248

認可されていない作業者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると作業者 ID が存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めることが望ましい。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(4)

■ 要求事項 249

緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定することが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS クラウドのコンポーネントにアクセスする必要がある Amazon 社内ネットワーク上の AWS 開発者と管理者は、AWS アクセス管理システムを通して明示的にアクセスをリクエストしなければなりません。すべてのリクエストは、適切な所有者または管理者によって確認および承認されます。

詳細は下記の URL を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-security-processes/>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監

視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.14 作業者アクセス及び作業者 ID の管理

(5)

■ 要求事項 250

ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS クラウドのコンポーネントにアクセスする必要がある Amazon 社内ネットワーク上の AWS 開発者と管理者は、AWS アクセス管理システムを通して明示的にアクセスをリクエストしなければなりません。すべてのリクエストは、適切な所有者または管理者によって確認および承認されます。

詳細は下記の URL を参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-security-processes/>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch

Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。

AWS Identity and Access Management (IAM) サービスの Multi-Factor Authentication を有効化することで、多要素認証で AWS サービスに関係する ID を保護することができます。詳細については、AWS のウェブサイト (<http://aws.amazon.com/mfa>) を参照してください。

■ 推奨される追加の実施事項

開発時、運用時を問わず AWS ルートアカウントの使用は推奨されません。Multi-Factor Authentication を有効化したうえで、ルートアカウントは利用せず IAM ユーザーを作成し利用することを推奨します。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.15 作業者の責任及び周知

(1)

■ 要求事項 251

必須

各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護すること。

■ AWS のインフラストラクチャー関連事項

AWS 本稼働環境のネットワークは拠点ホストを介した SSH 公開キー認証が必要となります。

AWS クラウドのコンポーネントにアクセスする必要がある Amazon 社内ネットワーク上の AWS 開発者と管理者は、AWS アクセス管理システムを通して明示的にアクセスをリクエストしなければなりません。すべてのリクエストは、適切な所有者または管理者によって確認および承認されます。

詳細は下記のサイトを参照してください。

<https://aws.amazon.com/jp/whitepapers/overview-of-security-processes/>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。

・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

AWS のサービスに関係する ID や、AWS 環境上に構築したアプリケーションの ID に関する適切な管理は情報処理事業者の責任で実施していただくことになります。AWS 環境においては、AWS IAM が利用可能です。Identity and Access Management (IAM)では、使用してユーザーIDの管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、ユーザーのアクセス許可の管理を一元的に行うことができます。認証情報には、パスワード、暗号キー、デジタル署名、および証明書が含まれます。また、AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証（MFA）を要求するオプションもあります。IAM を利用して ID のフェデレーションによる ID 管理も可能です。IAM の詳細については、下記の URL を参照ください。 https://aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html のベストプラクティスについては、下記の URL を参照してください

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

パスワードやアクセス管理を適切に遵守するためには、情報処理事業者がISO27001などの規定に基づき、AWSの提

供するサービスを理解し利用いただく必要があります。ベストプラクティスの取得方法として、AWS Security Fundamentals 等のセキュリティトレーニングを受講し、理解度を確認することを推奨します。

■ 推奨される追加の実施事項

個々の作業者に割り当てる IAM ユーザについては別途作成するか、または IAM のフェデレーションを用いて外部の ID プロバイダ（Active Directory など）と連携するなどして別途管理する必要があります。IAM でユーザを管理する場合、パスワードの条件や MFA などの要件を IAM で設定できます。その他の IAM の設計、運用に関するベストプラクティスは下記の URL を参照ください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html プログラムやスクリプト内で ID・パスワードなどの認証情報を扱う場合、AWS Systems Manager の Parameter Store を用いることで安全に情報を管理することができ、ソースコードや設定ファイル内にそれらの情報をハードコーディングする必要がなくなります。Parameter Store については下記の URL を参照してください。

<https://aws.amazon.com/jp/ec2/systems-manager/parameter-store/> また、AWS リソースへのアクセス時に必要な認証情報（Access Key や Secret Access Key）については、.aws/credentials ファイルや環境変数を用いる方法の他に、EC2 のインスタンスプロファイルや AWS STS、Amazon Cognito を用いることで一時的な認証情報をその都度払い出すことができ、やはりハードコーディングを避けることができます。一時的な認証情報の取得や活用方法については、下記の URL を参照してください。

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_temp.html これらの認証情報をソースコードに含めてバージョン管理ツール（Git など）にコミットしないように注意してください。AWS では、誤った認証情報の公開を防ぐためのツールを提供しています。関連情報については、下記の URL を参照ください。<https://github.com/aws-labs/git-secrets>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.15 作業者の責任及び周知

(2)

必須

システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。

■ AWS のインフラストラクチャー関連事項

AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。

<https://aws.amazon.com/jp/compliance/resources/>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、ゲスト OS、ソフトウェア及びアプリケーションをコントロールし、監視手順を定義する責任があります。

AWS CloudWatch は、AWS クラウドリソースと AWS 上で情報処理事業者が実行するアプリケーションのモニタリングを提供します。詳細については、AWS ウェブサイトを参照してください。 <https://aws.amazon.com/cloudwatch/>

また、Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察といった脅威も、GuardDuty によって検出されます。

パスワードやアクセス管理を適切に遵守するためには、情報処理事業者が ISO27001 などの規定に基づき、AWS の提供するサービスを理解し利用いただく必要があります。ベストプラクティスの取得方法として、AWS Security Fundamentals 等のセキュリティトレーニングを受講し、理解度を確認することを推奨します。

■ 推奨される追加の実施事項

Amazon Macie を利用することによりシステムを不正アクセスから防禦する追加の管理策が実施可能です。Amazon Macie は、機械学習によって AWS 内の機密データを自動的に検出、分類、保護するセキュリティサービスです。Amazon Macie では、個人情報（PII）や知的財産などの機密データが認識されます。また、ダッシュボードやアラートが提供されるため、データのアクセスや移動状況を確認できます。この完全マネージドサービスでは、データアクセスアクティビティの異常が継続的にモニタリングされ、不正アクセスの危険や不注意によるデータ漏洩が検出された場合には詳細なアラートが生成されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.6 技術的安全対策

7.6.15 作業者の責任及び周知

(3)

■ 要求事項 253

必須

離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。

■ AWS のインフラストラクチャー関連事項

AWS は、所定の統制によってシステムとデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視可能にしています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO27001、PCI、ITAR、および FedRAMPsm の監査中に独立監査人によって確認されます。また、内部者による不適切なアクセスの脅威に対処するために特定の SOC 1 統制を規定しています。詳細については、「AWS リスクとコンプライアンスの概要」の「詳細情報」にある「主要なコンプライアンスに関する質問と AWS の回答」を参照してください。

<https://aws.amazon.com/jp/compliance/resources/>

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデプロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch

Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guarddduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、システムにアクセス可能な端末の管理を適切に行い、許可されない第三者の利用を防ぐ責任があります。

パスワードやアクセス管理を適切に遵守するためには、情報処理事業者がISO27001などの規定に基づき、AWSの提供するサービスを理解し利用いただく必要があります。ベストプラクティスの取得方法として、AWS Security Fundamentals 等のセキュリティトレーニングを受講し、理解度を確認することを推奨します。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.7 人的安全対策

(1)

■ 要求事項 254

必須

医療情報を操作する可能性のある情報処理事業者職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求めること。派遣従業員については秘密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。

■ AWS のインフラストラクチャー関連事項

AWS システムとデバイスをサポートするすべての従業員は、入社時研修の一環として、アクセス権を付与される前に機密保持契約書に署名します。さらに、オリエンテーションの一環として、利用規定および Amazon 業務行動倫理規定（行動規定）ポリシーを読んで同意することが従業員に求められます。

AWS システムとデバイスをサポートするサードパーティプロバイダーに対する従業員セキュリティ要件は、AWS の親組織である Amazon.com および各サードパーティプロバイダーとの相互機密保持契約で確立されます。Amazon リーガルカウンセルおよび AWS 調達チームが、サードパーティプロバイダーとの契約で AWS サードパーティプロバイダーの従業員セキュリティ要件を定義します。AWS の情報を扱うすべての従業員は、最低でも雇用前審査に合格し、AWS の情報へのアクセス権を付与される前に、機密保持契約書（NDA）に署名する必要があります。

AWS サードパーティの要件は、PCI DSS、ISO 27001、および FedRAMPsm への準拠のため、監査中に外部の独立監査人によって確認されます。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は職員および派遣従業員に対し、秘密保持契約の締結および情報セキュリティ教育を行う責任があります。

■ 推奨される追加の実施事項

N/A - 対象外

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.7 人的安全対策

(2)

■ 要求事項 255

必須

医療情報を操作する可能性のある情報処理事業者職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。

■ AWS のインフラストラクチャー関連事項

ISO 27001 基準に合わせて、すべての従業員は、AWS の業務行動と倫理行動に関する規範を提供され、修了時に承認を必要とする情報セキュリティトレーニングを定期的に受けています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的実施しています。詳細については、「AWS セキュリティプロセスの概要」ホワイトペーパー（<http://aws.amazon.com/security> で入手可能）を参照してください。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は職員・派遣従業員に対し情報セキュリティ教育を行い定期的に見直しを行う責任があります。

■ 推奨される追加の実施事項

N/A - 対象外

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.7 人的安全対策

(3)

■ 要求事項 256

必須

情報処理事業者職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証すること。

■ AWS のインフラストラクチャー関連事項

ISO 27001 基準に合わせて、すべての従業員は、AWS の業務行動と倫理行動に関する規範を提供され、修了時に承認を必要とする情報セキュリティトレーニングを定期的に受けています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的実施しています。詳細については、「AWS セキュリティプロセスの概要」ホワイトペーパー（<http://aws.amazon.com/security> で入手可能）を参照してください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は安全管理策違反が発生した際に、不正アクセスを防ぐ処置および不正アクセス・破壊など行為がおこなわれいないことを検証する責任があります。

■ 推奨される追加の実施事項

N/A - 対象外

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.7 人的安全対策

(4)

■ 要求事項 257

必須

医療情報を操作する情報処理事業者職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。

■ AWS のインフラストラクチャー関連事項

AWS の人事チームは、従業員およびベンダーの終了および役職の変更のために従う必要がある内部管理責任を定義しています。従業員や契約社員のアクセス権付与/解除の責任は、人事（HR）、企業運用サービス事業主によって分担されます。詳細については、「AWS セキュリティプロセスの概要」ホワイトペーパー

(<http://aws.amazon.com/security> で入手可能) を参照してください。

■ AWS サービス関連情報

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

IAM ユーザーのパスワードの複雑な要件や必須のローテーション期間を指定するパスワードポリシーを、AWS アカウントに設定することができます。

パスワードポリシーを使用して、次の操作を実行できます。

- ・パスワードの最小の長さを設定する。
- ・大文字、小文字、数値、およびアルファベット以外の文字を含む特定の文字型が必要です。
- ・パスワードでは大文字と小文字が区別されることに必ずユーザーに知らせてください。
- ・すべての IAM ユーザーが自分のパスワードを変更できるようにします。

注記：IAM ユーザーが自分のパスワードを変更できるようにすると、IAM により自動的にパスワードポリシーの表示がユーザーに許可されます。IAM ユーザーがポリシーに準拠したパスワードを作成するには、アカウントのパスワードポリシーを表示するアクセス許可が必要です。

- ・指定した期間が経過したら、IAM ユーザーにパスワードを変更するように要求します（パスワードの失効を許可します）。
- ・IAM ユーザーが以前のパスワードを再利用できないようにします。
- ・IAM ユーザーがパスワードの失効を許可したときに、アカウント管理者への連絡を強制します。

詳細、最新情報は下記を参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

-Amazon GuardDuty

Amazon GuardDuty はマネージド型の脅威検出サービスです。悪意のある操作や不正な動作を継続的に監視し、AWS アカウントとワークロードを保護します。アカウント侵害の可能性を示す異常な API コールや潜在的に不正なデブロイといったアクティビティが監視の対象となります。インスタンスへの侵入の可能性や攻撃者による偵察も、GuardDuty によって検出されます。AWS マネジメントコンソールで数回クリックすれば、使用している AWS アカウント全体にリスクの徴候がないか、Amazon GuardDuty によって何十億ものイベントの分析をすぐに始められます。GuardDuty では、総合的な脅威インテリジェンスフィードにより疑わしい攻撃者が識別され、機械学習によりアカウントやワークロードのアクティビティの異常が検出されます。潜在的な脅威が検出されると、GuardDuty コンソールと AWS CloudWatch

Events に詳細なセキュリティアラートが配信されます。こうしてアラートをすぐに活用でき、既存のイベント管理システムやワークフローシステムを簡単に統合できます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/guardduty/>

-AWS CloudTrail

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャー全体でアカウントアクティビティをログに記録し、継続的に監視し、保持できます。CloudTrail では、AWS マネジメントコンソール、AWS の SDK やコマンドラインツール、その他の AWS のサービスを使用して実行されるアクションなど、AWS アカウントアクティビティのイベント履歴を把握できます。このイベント履歴により、セキュリティ分析、リソース変更の追跡、トラブルシューティングをより簡単に実行できるようになります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/cloudtrail/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、職員の退職後の情報資産の管理に関する規定を定め運用する責任があります。

■ 推奨される追加の実施事項

N/A - 対象外

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.7 人的安全対策

(5)

必須

医療機関等との委託契約において、情報処理事業者職員との秘密保持契約を結ぶこと、情報セキュリティ教育を受けさせること、及び、規定に反して預託情報を不正に扱った際の懲罰規定等、預託情報の機密管理に関する条項を設けること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業者は医療機関等と秘密保持契約を締結する必要があります。また、職員への情報セキュリティ教育の実施および機密情報管理に関する規定を設ける必要があります。

情報処理事業者と AWS 間は、Customer Agreement 第 3 条をご参照ください。

<https://aws.amazon.com/jp/legal/>

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.7 人的安全対策

(1)

推奨

医療情報を操作する情報処理事業者職員については、規定の安全管理策に違反する行為を行った場合の懲戒手続きについて予め定めておくことが望ましい。これはサービス規程等を含めることもできる。定めた懲戒手続きについては各職員に周知し、理解したことの確認を行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

職員への情報セキュリティ教育の実施および機密情報管理に関する規定を設ける必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.5 情報セキュリティのための方針群

A.5.1

A.7 人的資源のセキュリティ

A.7.1

A.7.2

A.7.3

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.9 アクセス制御

A.9.1

A.9.2

A.9.3

A.9.4

A.10 暗号

A.10.1

A.11 物理的及び環境的セキュリティ

A.11.1

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得，開発及び保守

A.14.1

A.14.2

A.15 供給者関係

A.15.1

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

A.18 順守

A.18.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.8 情報の破棄

(1)

■ 要求事項 260

必須

CD-R 等の廃棄については「7.6.7 電子媒体の取扱」を参照すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.8 情報の破棄

(2)

■ 要求事項 261

必須

ハードディスク等の廃棄については「7.5.4 情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

N/A

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.8 情報の破棄

(3)

■ 要求事項 262

必須

情報処理事業者は医療情報安全管理ガイドラインに従って情報の破棄を行った記録を提出すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者がしかなるべき手順でワイプを実施してからボリュームを削除することで、医療機関等との合意事項を満たすようにし、実施した記録を提出する責任があります。

■ 推奨される追加の実施事項

情報処理事業者自身で Amazon EBS のワイプ作業を行うこともできます。また、AWS 上に格納する機密データは、AWS Key Management Service で管理される暗号鍵を利用して暗号化することを推奨します。契約終了時に暗号鍵そのものを廃棄することで、データ消去に相当するといった対応を考慮することも可能となります。

Amazon Elastic Block Store (EBS) で追加のストレージを使う場合などはボリュームを暗号化することができます。S3 を使う場合は Server Side Encryption でバケット・ファイル単位に暗号化することができます。また、サーバサイド暗号化のみでなく、必要に応じてクライアントサイド暗号化の利用を検討してください。

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.9 医療情報システムの改造と保守

(1)

■ 要求事項 263

必須

オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システムに対する影響を評価し、試験結果を確認してから実施すること。

■ AWS のインフラストラクチャー関連事項

N/A

左記の要件への対応は情報処理事業者の該当事項となります。

なお、AWS のシステム開発ライフサイクル(SDLC) は、業界のベストプラクティスを組み込んでおり、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスク評価の完遂などが含まれています。詳細については、AWS セ

セキュリティプロセスの概要を参照してください。また、詳細については、ISO 27001 規格の附属書 A ドメイン 14 を参照してください。AWS は、ISO27001 認証規格への対応を確認する独立監査人から、審査および認証を受けています。また、AWS は、Payment Card Industry (PCI) データセキュリティ基準(Data Security Standard/DSS)のレベル 1 に準拠しています。詳細については、AWS Artifact (<https://console.aws.amazon.com/artifact>) を使用して、PCI DSS Attestation of Compliance (AOC) と Responsibility Summary をリクエストしてください。

■ AWS サービス関連情報

-AWS Systems Manager

AWS Systems Manager は、AWS でご利用のインフラストラクチャーを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェースで AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager では、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon RDS インスタンスなどのリソースをアプリケーションごとにグループ化し、運用データを表示できます。これにより、さまざまなリソースグループのモニタリングやトラブルシューティングを迅速に行うことができます。また、リソースとアプリケーションの管理を簡素化することも可能です。運用上の問題の検出と解決に要する時間が短縮され、大規模なインフラストラクチャーでも安全に運用、管理できます

セキュリティとコンプライアンスの維持

AWS Systems Manager では、インスタンスのパッチ、設定、およびカスタムポリシーに対するスキャンを実行し、セキュリティとコンプライアンスの維持に役立てることができます。パッチのベースラインの定義、アンチウイルス定義の更新、ファイアウォールポリシーの適用が可能です。また、大規模なサーバー群でも、各サーバーに手動でログインすることなく、リモートで管理できます。Systems Manager では、データベース文字列のようなプレーンテキストや、パスワードのような秘密データなど、設定データを一元的に管理するストアが利用できます。これにより、機密データと構成データをコードから分離できます。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/systems-manager/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、OS のアップグレード、セキュリティパッチの適用などを医療情報システムに対し適用評価およびテスト・実施を行う責任があります。

また、情報処理事業者は RDS などのマネージドサービスの利用時には、パッチ適用の実施有無や実施時間帯を自らコントロールする必要があり、本番環境への適用前に事前にステージング環境などで影響評価を行うことが求められます。

■ 推奨される追加の実施事項

AWS Systems Manager や EC2 Systems Manager を利用し、OS のセキュリティパッチ適用などの作業を自動化することができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.9 医療情報システムの改造と保守

(1)

■ 要求事項 264

推奨

開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的なぜい弱性検査を行う。

■ AWS のインフラストラクチャー関連事項

N/A

左記の要件への医療情報システムの対応は情報処理事業者の該当事項となります。

なお、AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。静的コード分析ツールは、標準ビルドプロセスの一環として実行され、配備される全ソフトウェアは、注意深く選択された業界の専門家によって実行される反復侵入テストを受けます。当社のセキュリティリスク査定のレビューは、設計段階に開始され、この作業はソフトウェアの立ち上げ後まで継続します。

■ AWS サービス関連情報

-Amazon Inspector

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの調査結果を示した詳細なリストが Amazon Inspector によって作成されます。この調査結果は直接取得することもできますが、Amazon Inspector コンソールまたは API を介して入手可能な評価に関する詳細レポートの一部でも確認できます。

すぐに利用開始できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されます。詳細、最新情報は下記を参照ください。
<https://aws.amazon.com/jp/inspector/>

-脆弱性テストと侵入テスト

許可のリクエスト

任意の AWS リソースへの、または AWS リソースからの侵入テストの承認をリクエストするには、AWS 脆弱性/侵入テストリクエストフォームに必要事項を記入して、送信してください。侵入テストのリクエストに関して注意すべき複数の重要事項があります。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/security/penetration-testing/>

■ 情報処理事業者（お客様）の該当事項

利用する AWS サービスに対し AWS では AWS 環境への、または AWS 環境からの侵入テストと脆弱性スキャンを実施する許可をお客様がリクエストできるポリシーを確立されています。このポリシーを利用し、利用する AWS サービスに対し外形的な脆弱性検査が行えます。

■ 推奨される追加の実施事項

Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスで、情報処理事業者は、外形的な脆弱性診断のために本サービスを利用することができます。Amazon Inspector は、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認します。評価が実行された後、重大性の順にセキュリティの所見を示した詳細なリストが Amazon Inspector によって作成されます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.1 要求事項の識別

(1)

■ 要求事項 265

必須

医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理装置等について識別すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は、医療情報処理提供に必要な業務プロセスおよび利用する AWS サービスなどの情報処理装置等について明確にする責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.1 要求事項の識別

(2)

■ 要求事項 266

必須

業務プロセス間の相互関係を評価すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、業務プロセス完の総合関係を評価する責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.14 システムの取得、開発及び保守

A.14.1

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.1 要求事項の識別

(3)

■ 要求事項 267

必須

事業を継続するための業務プロセスの優先順位を明確にすること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、事業継続に必要な業務プロセスの優先順位付けを行う責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

7.10 医療情報処理に関する事業継続計画

7.10.1 要求事項の識別

(4)

■ 要求事項 268

必須

医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別すること。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、AWS サービスおよびソフトウェアの障害が業務プロセスに与える影響について評価を行う責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.1 要求事項の識別

(5)

■ 要求事項 269

必須

医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別すること。

■ AWS のインフラストラクチャー関連事項

複数のアベイラビリティゾーンによる高可用性

事実上他のすべてのテクノロジーインフラストラクチャープロバイダと異なる点として、各 AWS リージョンには複数のアベイラビリティゾーンが存在しています。各アベイラビリティゾーンは 1 つ以上の相互に独立したデータセンターで構成されます。各データセンター間は物理的に離れており、冗長性のある電源とネットワーキングを備えています。アプリケーションの高い可用性やパフォーマンスが重要なお客様は、同じリージョンの複数のアベイラビリティゾーン間でアプリケーションをデプロイして、耐障害性や低レイテンシーを実現できます。アベイラビリティゾーンは高速なプライベート光ファイバーネットワーキングで相互に接続されているため、アプリケーションがアベイラビリティゾーン間で中断なく自動的にフェイルオーバーできるようなアーキテクチャを簡単に設計できます。シミュレーションと反応の測定 AWS ビジネス継続性プランは、自然災害による混乱の回避および軽減方法を示すオペレーションプロセスガイドであり、イベントが起こる前、イベントの最中、およびイベント後の詳しい対処ステップを定めるものです。不測の事態に備え、影響を軽減するために、AWS は定期的にビジネス継続性プランをテストし、さまざまなシナリオをシミュレートする演習を実施しています。チームとプロセスの対応を文書化し、学習した成果と、反応率を高めるために必要と思われる是正処置をまとめています。混乱から迅速に立ち直す訓練と準備が整っています。これには、エラーに伴うダウンタイムを最小限に抑えるための秩序を保った復旧プロセスなどが含まれます。詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/> 関連する統制に関しては AWS の SOC1、SOC2 レポートをご参照ください。 <https://aws.amazon.com/jp/compliance/soc-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、利用する AWS サービスおよびソフトウェアが医療情報システムに対して持つ影響度の大きさの評価を行う責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.1 要求事項の識別

(6)

■ 要求事項 270

必須

ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG 及び PNG 等のフォーマット）で外部ファイルに出力可能とすることなどの方策を検討すること。

■ AWS のインフラストラクチャー関連事項

複数のアベイラビリティゾーンによる高可用性

事実上他のすべてのテクノロジーインフラストラクチャープロバイダと異なる点として、各 AWS リージョンには複数のアベイラビリティゾーンが存在しています。各アベイラビリティゾーンは 1 つ以上の相互に独立したデータセンターで構成されます。各データセンター間は物理的に離れており、冗長性のある電源とネットワーキングを備えています。アプリケーションの高い可用性やパフォーマンスが重要なお客様は、同じリージョンの複数のアベイラビリティゾーン間でアプリケーションをデプロイして、耐障害性や低レイテンシーを実現できます。アベイラビリティゾーンは高速なプライベート光ファイバーネットワーキングで相互に接続されているため、アプリケーションがアベイラビリティゾーン間で中断なく自動的にフェイルオーバーできるようなアーキテクチャを簡単に設計できます。シミュレーションと反応の測定 AWS ビジネス継続性プランは、自然災害による混乱の回避および軽減方法を示すオペレーションプロセスガイドであり、イベントが起こる前、イベントの最中、およびイベント後の詳しい対処ステップを定めるものです。不測の事態に備え、影響を軽減するために、AWS は定期的にビジネス継続性プランをテストし、さまざまなシナリオをシミュレートする演習を実施しています。チームとプロセスの対応を文書化し、学習した成果と、反応率を高めるために必要と思われる是正処置をまとめています。混乱から迅速に立ち直る訓練と準備が整っています。これには、エラーに伴うダウンタイムを最小限に抑えるための秩序を保った復旧プロセスなどが含まれます。詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/> 関連する統制に関しては AWS の SOC1、SOC2 レポートをご参照ください。 <https://aws.amazon.com/jp/compliance/soc-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、利用する AWS サービスが医療情報システムに対して持つ影響度の大きさの評価を行う責任があります。

システム障害が発生した場合に備え、Design for failure の考えに則りシステムの冗長化や、システム障害時にも県毒性が確保可能な代替手段を検討する必要があります。

■ 推奨される追加の実施事項

S3 のクロスリージョンレプリケーション等を用い、医療情報システムが配置されているリージョンとは別のリージョンに見読性の確保が必要なデータをバックアップしておくことを推奨します。

ただし、バックアップ先リージョンの選定にあたっては、法規制および関連ガイドラインを考慮する必要があります。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

(7)

■ 要求事項 271

必須

医療機関等に提供する情報処理サービスの継続に必要であれば、受託する医療情報のバックアップ施設等、情報処理サービスを継続するための代替情報処理施設を設置し、それらの施設に対しても本ガイドラインで提示する物理的安全対策を施すこと。

■ AWS のインフラストラクチャー関連事項

複数のアベイラビリティゾーンによる高可用性

事実上他のすべてのテクノロジーインフラストラクチャープロバイダと異なる点として、各 AWS リージョンには複数のアベイラビリティゾーンが存在しています。各アベイラビリティゾーンは 1 つ以上の相互に独立したデータセンターで構成されます。各データセンター間は物理的に離れており、冗長性のある電源とネットワーキングを備えています。アプリケーションの高い可用性やパフォーマンスが重要なお客様は、同じリージョンの複数のアベイラビリティゾーン間でアプリケーションをデプロイして、耐障害性や低レイテンシーを実現できます。アベイラビリティゾーンは高速なプライベート光ファイバーネットワーキングで相互に接続されているため、アプリケーションがアベイラビリティゾーン間で中断なく自動的にフェイルオーバーできるようなアーキテクチャを簡単に設計できます。シミュレーションと反応の測定 AWS ビジネス継続性プランは、自然災害による混乱の回避および軽減方法を示すオペレーションプロセスガイドであり、イベントが起こる前、イベントの最中、および

イベント後の詳しい対処ステップを定めるものです。不測の事態に備え、影響を軽減するために、AWS は定期的にビジネス継続性プランをテストし、さまざまなシナリオをシミュレートする演習を実施しています。チームとプロセスの対応を文書化し、学習した成果と、反応率を高めるために必要と思われる是正処置をまとめています。混乱から迅速に立ち直る訓練と準備が整っています。これには、エラーに伴うダウンタイムを最小限に抑えるための秩序を保った復旧プロセスなどが含まれます。詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/> 関連する統制に関しては AWS の SOC1、SOC2 レポートをご参照ください。 <https://aws.amazon.com/jp/compliance/soc-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、情報処理サービスの継続のため、医療情報システムが配置されているリージョンとは別のリージョンにバックアップシステムを設置することができます。

ただし、バックアップ先リージョンの選定にあたっては、法規制および関連ガイドラインを考慮する必要があります。

■ 推奨される追加の実施事項

S3 のクロスリージョンレプリケーション等を用い、医療情報システムが配置されているリージョンとは別のリージョンに見読性の確保が必要なデータをバックアップしておくことを推奨します。

ただし、バックアップ先リージョンの選定にあたっては、法規制および関連ガイドラインを考慮する必要があります。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.2 事業継続計画の立案及びレビュー

■ 要求事項 272

必須

医療情報システムのサービス提供における業務プロセス及び医療情報システムの優先順位にもとづいて、医療情報処理に関する事業継続計画を策定すること。

■ AWS のインフラストラクチャー関連事項

装置の保守点検 AWS チームは、マシン、ネットワーク、およびバックアップ装置に対する診断を実行し、常時および緊急時に正常に稼働していることを確認しています。データセンターの装置およびユーティリティに対する日常保守点検は、日常業務の一環です。緊急時のバックアップ装置水道、電気、通信、インターネット接続は、冗長性を持つよう設計されており、緊急時に中断しないように構築されています。電気系統は完全な冗長設計になっているため、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。チームおよびシステムは、温度と湿度を監視して制御することで、過熱を防止し、サービス停止が起こらないようにします。不測の事態への備え AWS は、自然災害や火災など、環境上の脅威の可能性に対して事前の対策を講じています。当社データセンターを保護する 2 つの方法として、自動センサーと応答装置を設置しています。漏水検知デバイスは、自動ポンプを作動させて漏水を除去し、損害を防止して、従業員に問題を知らせることができます。同様に、自動火災検知および消火装置は危険を軽減し、AWS の従業員と消防士に問題を知らせることができます。複数のアベイラビリティゾーンによる高可用性事実上他のすべてのテクノロジーインフラストラクチャープロバイダと異なる点として、各 AWS リージョンには複数のアベイラビリティゾーンが存在しています。各アベイラビリティゾーンは 1 つ以上の相互に独立したデータセンターで構成されます。各データセンター間は物理的に離れており、冗長性のある電源とネットワーキングを備えています。アプリケーションの高い可用性やパフォーマンスが重要なお客様は、同じリージョンの複数のアベイラビリティゾーン間でアプリケーションをデプロイして、耐障害性や低レイテンシーを実現できます。アベイラビリティゾーンは高速なプライベート光ファイバーネットワーキングで相互に接続されているため、アプリケーションがアベイラビリティゾーン間で中断なく自動的にフェイルオーバーできるようなアーキテクチャを簡単に設計できます。シミュレーションと反応の測定 AWS ビジネス継続性プランは、自然災害による混乱の回避および軽減方法を示すオペレーションプロセスガイドであり、イベントが起こる前、イベントの最中、およびイベント後の詳しい対処ステップを定めるものです。不測の事態に備え、影響を軽減するために、AWS は定期的

にビジネス継続性プランをテストし、さまざまなシナリオをシミュレートする演習を実施しています。チームとプロセスの対応を文書化し、学習した成果と、反応率を高めるために必要と思われる是正処置をまとめています。混乱から迅速に立ち直る訓練と準備が整っています。これには、エラーに伴うダウンタイムを最小限に抑えるための秩序を保った復旧プロセスなどが含まれます。詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/> 関連する統制に関しては AWS の SOC1、SOC2 レポートをご参照ください。 <https://aws.amazon.com/jp/compliance/soc-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は AWS 上に構築したアプリケーションおよび情報処理業務に関する事業継続計画を策定し、テスト・レビューを行う責任があります。AWS 上で複数のリージョンやアベイラビリティゾーンを利用できるように設計することをお勧めします。複数のアベイラビリティゾーンにアプリケーションを配置すると、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つことができます。ただし、医療情報システムでは、国内法の執行が及ぶ範囲などを考慮する必要があります。お客様が積極的に行わなければ、リージョン間でデータは複製されません。従って、このような種類のデータの配置およびプライバシーの要件を持つお客様が、規格に準拠した環境を構築できます。リージョン間の通信はすべて、パブリックなインターネットインフラストラクチャーを介して行われることに注意してください。このため、適切な暗号方式を使用して機密データを保護することをお勧めします。詳細については、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」（<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介（日本語））を参照してください。

■ 推奨される追加の実施事項

アベイラビリティゾーンのみでなく、リージョンの単位で冗長性を確保したい場合、AWS CloudFormation を利用することで本番環境のサーバ構成を任意のリージョンでいつでも展開することができます。また、Amazon RDS、Amazon S3 では、必要に応じてクロスリージョンレプリケーション機能を有効化することができます。

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1
A.12.2
A.12.3
A.12.4
A.12.5
A.12.6
A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1
A.17.2

7. 医療情報を受託管理する情報処理事業における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.2 事業継続計画の立案及びレビュー

(2)

■ 要求事項 273

必須

策定した事業継続計画について模擬試験を含めた適切な方法でレビューすること。

■ AWS のインフラストラクチャー関連事項

AWS は定期的にビジネス継続性プランをテストし、さまざまなシナリオをシミュレートする演習を実施しています。チームとプロセスの対応を文書化し、学習した成果と、反応率を高めるために必要と思われる是正処置をまとめています。混乱から迅速に立ち直る訓練と準備が整っています。これには、エラーに伴うダウンタイムを最小限に抑えるための秩序を保った復旧プロセスなどが含まれます。詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/> 関連する統制に関しては AWS の SOC1、SOC2 レポートをご参照ください。 <https://aws.amazon.com/jp/compliance/soc-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業（お客様）の該当事項

情報処理事業は AWS 上に構築したアプリケーションおよび情報処理業務に関する事業継続計画を策定し、テスト・レビューを行う責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.2 事業継続計画の立案及びレビュー

(3)

■ 要求事項 274

必須

事業継続計画について定期的に見直しを行うこと。

■ AWS のインフラストラクチャー関連事項

AWS は定期的にビジネス継続性プランをテストし、さまざまなシナリオをシミュレートする演習を実施しています。チームとプロセスの対応を文書化し、学習した成果と、反応率を高めるために必要と思われる是正処置をまとめています。混乱から迅速に立ち直る訓練と準備が整っています。これには、エラーに伴うダウンタイムを最小限に抑えるための秩序を保った復旧プロセスなどが含まれます。詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

関連する統制に関しては AWS の SOC1、SOC2 レポートをご参照ください。

<https://aws.amazon.com/jp/compliance/soc-faqs/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は AWS 上に構築したアプリケーションおよび情報処理業務に関する事業継続計画を定期的に見直すプロセスを構築する必要があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

7. 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

7.10 医療情報処理に関する事業継続計画

7.10.2 事業継続計画の立案及びレビュー

(1)

■ 要求事項 275

推奨

策定される事業継続計画には次のような事項を含むことが望ましい。

- 事前準備計画
- 「非常時」判断手順
- 関係者の召集、対応本部の設置
- 機器及び作業員の縮退措置及び代替施設の手配措置
- バックアップ施設等、代替施設への切替え措置
- 代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等）
- 障害の拡大範囲に関する判断手順、基準
- 正常復帰の判断手順、基準
- 正常復帰後の医療情報システムの点検手順（不正侵入、情報改ざん、情報破損等の検出等）
- 所管官庁への連絡体制、等

■ AWS のインフラストラクチャー関連事項

AWS の事業継続計画は、環境に起因するサービス障害の回避および軽減措置について記載されています。それには、イベントが起こる前、イベントの最中、およびイベント後の詳しいステップを定めるものです。事業継続計画は、さまざまなシナリオのシミュレーションを含むテストによってサポートされています。テスト中およびテスト後は、継続的な改善を目的として、AWS がチームとプロセスの対応、是正処置、得られた教訓を文書により記録しています。

詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/disaster-recovery/>

また、AWS は ISO 27001 基準の要件に従い、業界団体、リスクおよびコンプライアンス組織、地元機関、および規制団体との接点を維持しています。

詳細は下記のサイトを参照ください。

<https://aws.amazon.com/jp/whitepapers/overview-of-risk-and-compliance/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は事業継続計画に要求事項記載の事項を含むことが推奨されます。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1

A.17.2

8 診療録及び診療諸記録を外部に保存する際の基準

8.1 外部保存を受託する機関の選定基準および情報の取扱に関する基準

■ 要求事項 276

医療情報安全管理ガイドラインの「8.1.2 外部保存を受託する機関の選定基準および情報の取り扱いに関する基準」の「C. 最低限のガイドライン」及び「D. 推奨されるガイドライン」に従っていることを示すことができるよう、適用している安全管理策を適用宣言書の形で整理しておくことが望ましい。

■ AWS のインフラストラクチャー関連事項

AWS のサービスやソリューションに関しては、下記の URL を参照ください。

<https://aws.amazon.com/jp/solutions/>

AWS のカスタマーアグリーメントに関しては、下記の URL を参照ください。

<https://aws.amazon.com/jp/agreement/>

AWS のカスタマーアグリーメントの日本準拠法に関しての変更については下記の URL を参照ください。

<https://aws.amazon.com/jp/blogs/news/how-to-change-aws-ca-by-artifact/>

AWS の適正利用規約に関しては、下記の URL を参照ください。

<https://aws.amazon.com/jp/aup/>

AWS のサービス条件に関しては、下記のサイトを参照ください。

<https://aws.amazon.com/jp/service-terms/>

AWS のサポートに関しては、下記のサイトを参照ください。

<https://aws.amazon.com/jp/premiumsupport/>

AWS サービスレベルアグリーメント：

<https://aws.amazon.com/jp/ec2/sla/> <https://aws.amazon.com/jp/route53/sla/> <https://aws.amazon.com/jp/rds/sla/> <https://aws.amazon.com/jp/cloudfront/sla/> <https://aws.amazon.com/jp/s3/sla/>

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。これらの文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。AWS から提供可能な第三者認証や監査レポートに関しては下記のサイトをご参照ください。

<https://aws.amazon.com/jp/compliance/> <https://aws.amazon.com/jp/security/>

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

IT インフラストラクチャーを AWS に構築する際は、情報処理事業者が責任共有モデルを考慮する必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、情報処理事業者の運用上の様々な負担の軽減にも貢献することになります。情報処理事業者の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。情報処理事業者の責任範囲や対応すべき事項については、使用するサービスや、IT 環境へのサービス統合、適用される法律および規制等に応じて異なります。したがって、情報処理事業者には選択するサービスを注意深く検討する必要があります。詳細は下記の URL にある各種ホワイトペーパーをご参照ください。 <https://aws.amazon.com/jp/compliance/resources/>

■ 推奨される追加の実施事項

使用したサービス、適用した安全管理策を適用宣言書やホワイトペーパーの形で整理しておくことが推奨されます。

クラウドサービス利用についてガイドライン作成や手続きの標準化等、必要とされる場合にはAWSプロフェッショナルサービスのご利用をご検討ください。AWS プロフェッショナルサービスは、AWS クラウドを使用して期待するビジネス上の成果を実現するようお客様をサポートできる、専門家からなるグローバルチームです。詳細は下記の URL を参照ください。

<https://aws.amazon.com/jp/professional-services/>

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.18 順守

A.18.1

8 診療録及び診療諸記録を外部に保存する際の基準

8.2 外部保存契約終了時の処理について

■ 要求事項 277

医療機関等と情報処理事業者間で廃棄処理手順について定め、合意しておく必要がある。

■ AWS のインフラストラクチャー関連事項

Amazon EBS ボリュームは、ワイプ処理を行った後、未フォーマットのローブロックデバイスとしてお客様に提供されます。ワイプは再使用の直前に実施されるため、お客様に提供された時点でワイプ処理は完了しています。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 - IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン - IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オ

プロジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によって

アクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は医療機関等とデータの廃棄処理手順について定め、合意しておく必要があります。

情報処理事業者は、自身のデータの統制と所有権を保持します。業務手順上、DoD 5220.22-M（「国家産業セキュリティプログラム運営マニュアル」）や NIST 800-88（「媒体のサニタイズに関するガイドライン」）が指定するような、特定の方法で全データをワイプする必要がある場合、情報処理事業者自身で Amazon EBS のワイプ作業を行うこともできます。情報処理事業者がしかるべき手順でワイプを実施してからボリュームを削除することで、医療機関等との合意事項を満たすようにします。また、機密データの暗号化は、一般的なセキュリティのベストプラクティスです。詳細については、「AWS リスクとコンプライアンスの概要」の関連文書「CSA Consensus Assessments Initiative Questionnaire」を参照してください。（<https://aws.amazon.com/jp/compliance/resources/>） また、情報処理事業者のデータに対する権限制御（IAM、S3 バケットポリシー等）や暗号化についての詳細は、AWS ウェブサイトの「アマゾンウェブサービス:セキュリティプロセスの概要」

（<https://aws.amazon.com/jp/security/security-resources/> ⇒ AWS セキュリティプロセスのご紹介（日本語））を参照してください。

■ 推奨される追加の実施事項

AWS 上に格納する機密データは、AWS Key Management Service で管理される暗号鍵を利用して暗号化することを推奨します。契約終了時に暗号鍵そのものを廃棄することで、データ消去に相当するといった対応を考慮することも可能である。

Amazon Elastic Block Store (EBS) で追加のストレージを使う場合などはボリュームを暗号化することができます。S3 を使う場合は Server Side Encryption でバケット・ファイル単位に暗号化することができます。また、サーバサイド暗号化のみでなく、必要に応じてクライアントサイド暗号化の利用を検討してください。

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1
A.12.2
A.12.3
A.12.4
A.12.5
A.12.6
A.12.7

8 診療録及び診療諸記録を外部に保存する際の基準

8.2 外部保存契約終了時の処理について

■ 要求事項 278

ネットワークを介して医療機関等の外部に保存された情報については、確実に情報が廃棄されたことを医療機関等に保証する必要がある。

■ AWS のインフラストラクチャー関連事項

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、次のウェブサイトですぐ入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 <http://aws.amazon.com/security/>。

Amazon EBS ボリュームは、ワイプ処理を行った後、未フォーマットのローブロックデバイスとしてお客様に提供されます。ワイプは再使用の直前に実施されるため、お客様に提供された時点でワイプ処理は完了しています。業務手順上、DoD 5220.22-M (「国家産業セキュリティプログラム運営マニュアル」) や NIST 800-88 (「媒体のサニタイズに関するガイドライン」) が指定するような、特定の 방법으로全データをワイプする必要がある場合、お客様自身で Amazon EBS のワイプ作業を行うこともできます。お客様がしかるべき手順でワイプを実施してからボリュームを削除することで、コンプライアンスの要件を満たすようにします。

機密データの暗号化は、一般的なセキュリティのベストプラクティスです。AWS には、EBS ボリュームとスナップショットを AES-256 で暗号化する機能があります。EC2 インスタンスをホストするサーバーで暗号化が行われるため、EC2 インスタンスと EBS ストレージとの間を移動するデータが暗号化されます。この処理が効率的に低レイテンシーで行われるようにするために、EBS 暗号化機能は EC2 の強力なインスタンスタイプ (たとえば、M3、C3、R3、G2) だけで使用できます。

詳細に関しては「リスクおよびコンプライアンス (2015 年 12 月)」をご参照下さい。

https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

ISO 27001 基準に合わせて、AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

詳細については、ISO 27001 基準の付録 A、ドメイン 8 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。

詳細に関しては「リスクおよびコンプライアンス (2015 年 12 月)」をご参照下さい。

https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

データの永続性

データは、ボリュームを明示的に削除するまでボリュームに保持されます。削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされます。機密データを扱っている場合は、手動によるデータの暗号化や、Amazon EBS 暗号化 で保護されているボリュームへのデータの格納を検討してください。詳細については、「Amazon EBS Encryption」を参照してください。

デフォルトでは、インスタンスの起動時に作成およびアタッチされた EBS ボリュームは、インスタンスの終了時に削除されます。この動作を変更するには、インスタンスの起動時にフラグ DeleteOnTermination の値を false に変更します。値を変更すると、インスタンスが終了してもボリュームが保持されるので、そのボリュームを別のインスタンスにアタッチできます。詳細に関しては、

http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSVolumes.html を参照してください。

■ AWS サービス関連情報

-Amazon S3、Amazon Glacier

Amazon S3 標準、S3 標準 – IA、Amazon Glacier ストレージクラス内のデータは、ひとつの AWS リージョン内で通常何マイルも離れた少なくとも 3 つの物理的なアベイラビリティゾーンにわたって自動的に分散されています。

Amazon S3 1 ゾーン – IA ストレージクラスはデータをひとつの AZ に保存し、アクセスが頻繁ではなく、S3 標準ストレージのようなアベイラビリティと復旧性を要しないデータに対して低コストのオプションをお求めのお客様に最適です。

Amazon S3 は 3 種類の暗号化をサポートしています。S3 は、AWS CloudTrail との洗練された統合を提供し、監査のためにストレージ API 呼び出しアクティビティについてログ、監視、保持を行います。Amazon S3 は Amazon Macie の唯一のクラウドストレージプラットフォームで、機械学習によって AWS 内の機密データを自動的に検出、分類、保護します。S3 では、PCI-DSS、HIPAA/HITECH、FedRAMP、EU データ保護指令、FISMA といったセキュリティ標準やコンプライアンス認証をサポートしており、お客様は世界中の事実上すべての規制機関によるコンプライアンス要件を満たすことができます。Amazon S3 のインフラストラクチャーは耐久性が高く、安全かつグローバルで、優れたデータ保護を提供する堅牢な災害対策ソリューションとなります。クロスリージョンレプリケーション (CRR) は、すべての S3 オブジェクトを別の AWS リージョンにあるレプリケート先バケットに自動的にレプリケートすることも可能です。詳細、最新情

報は下記を参照ください。

<https://aws.amazon.com/jp/s3/>

<https://aws.amazon.com/jp/glacier/>

-Amazon EBS

Amazon Elastic Block Store (Amazon EBS) は、AWS クラウド内で Amazon EC2 インスタンスと組み合わせて使用できる、永続的なブロックストレージボリュームです。コンポーネントに障害が発生した場合でも高い可用性と耐久性を維持できるように、Amazon EBS の各ボリュームはアベイラビリティゾーン内で自動的にレプリケートされます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/ebs/>

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSEncryption.html

-Amazon RDS

Amazon RDS が実行されるインフラストラクチャーは、アマゾン ウェブ サービスの他のサービスに使用されるものと同じで、高い信頼性が特長です。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS は異なるアベイラビリティゾーン (AZ) のスタンバイインスタンスにデータを複製します。Amazon RDS は、重要な本稼働用データベースの信頼性を高めるために、自動バックアップ、データベーススナップショット、ホスト自動交換といったその他の特徴を多数備えています。Amazon RDS なら、データベースへのネットワークアクセスの制御も簡単です。Amazon RDS では、データベースインスタンスを Amazon Virtual Private Cloud (Amazon VPC) で稼働させることもできます。これによってデータベースインスタンスを独立させ、業界標準の暗号化 IPsec VPN を介して既存の IT インフラストラクチャーに接続することが可能になります。Amazon RDS エンジンの多くには、保管時の暗号化と転送時の暗号化が準備されています。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/rds/>

-Amazon EMR

Amazon EMR は Amazon EC2 インスタンスへのネットワークアクセスを制御するファイアウォールの各種設定を自動的に構成します。また、お客様が定義する論理的に隔離されたネットワークである Amazon Virtual Private Cloud (VPC) 内にクラスターを起動することもできます。Amazon S3 に保存されたオブジェクトの場合、AWS Key Management Service またはカスタマー管理型のキーを使用して Amazon S3 サーバー側の暗号化または Amazon S3 クライアント側の暗号化と EMRFS を使用できます。その他の暗号化オプションや Kerberos による認証を有効にすることも簡単に行えます。詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/emr/>

-AWS IAM

AWS Identity and Access Management (IAM) は、ユーザーに対して AWS へのアクセスを安全に制御するための仕組みです。

認証・認可に基づくアクセス権の管理は、アクセス対象のシステムを安全に運用する上で必要不可欠です。認証によってアクセス元が誰かを確認し、認可によって特定の条件下におけるリソースへのアクセス権限を与えます。詳細、最新情報

は下記を参照ください。

<https://aws.amazon.com/jp/iam/>

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は、電磁的記録媒体を廃棄する場合には、AWS クラウドを利用する場合も、AWS クラウドを利用しない従来の情報システムと同様に、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

8 診療録及び診療諸記録を外部に保存する際の基準

8.2 外部保存契約終了時の処理について

■ 要求事項 279

受領した情報と管理している情報の一覧の整合性を医療機関等が確認できるように、預かっている情報について台帳を維持管理することが求められる。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は受領した情報について管理台帳を作成・維持管理する責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

8 診療録及び診療諸記録を外部に保存する際の基準

8.2 外部保存契約終了時の処理について

■ 要求事項 280

台帳の操作については特定の作業員だけが行うこととし、複数人による確認等を行うことで、台帳上の情報の整合性について保証を行うこと。

■ AWS のインフラストラクチャー関連事項

N/A

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は作成した情報管理台帳のアクセスの制御および情報の整合性について管理し保証を行う責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

8 診療録及び診療諸記録を外部に保存する際の基準

8.2 外部保存契約終了時の処理について

情報処理業務の一部を再委託している場合には、再委託先においても同等の廃棄手順により確実に情報を廃棄すること。

■ AWS のインフラストラクチャー関連事項

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、次のウェブサイトですぐ入手可能な AWS クラウドセキュリティホワイトペーパーを参照してください。 <http://aws.amazon.com/security/>。

Amazon EBS ボリュームは、ワイプ処理を行った後、未フォーマットのローブロックデバイスとしてお客様に提供されます。ワイプは再使用の直前に実施されるため、お客様に提供された時点でワイプ処理は完了しています。業務手順上、DoD 5220.22-M (「国家産業セキュリティプログラム運営マニュアル」) や NIST 800-88 (「媒体のサニタイズに関するガイドライン」) が指定するような、特定の手法で全データをワイプする必要がある場合、お客様自身で Amazon EBS のワイプ作業を行うこともできます。お客様がしかるべき手順でワイプを実施してからボリュームを削除することで、コンプライアンスの要件を満たすようにします。

機密データの暗号化は、一般的なセキュリティのベストプラクティスです。AWS には、EBS ボリュームとスナップショットを AES-256 で暗号化する機能があります。EC2 インスタンスをホストするサーバーで暗号化が行われるため、EC2 インスタンスと EBS ストレージとの間を移動するデータが暗号化されます。この処理が効率的に低レイテンシーで行われるようにするために、EBS 暗号化機能は EC2 の強力なインスタンスタイプ (たとえば、M3、C3、R3、G2) だけで使用できます。

詳細に関しては「リスクおよびコンプライアンス (2015 年 12 月)」をご参照下さい。

https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

ISO 27001 基準に合わせて、AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M (国家産業セキュリティプログラム運営マニュアル) または NIST 800-88 (媒体のサニタイズに関するガイドライン) に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。

詳細については、ISO 27001 基準の付録 A、ドメイン 8 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。

詳細に関しては「リスクおよびコンプライアンス (2015 年 12 月)」をご参照下さい。

https://d0.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf

データの永続性

データは、ボリュームを明示的に削除するまでボリュームに保持されます。削除した EBS ボリュームが使用していた物理的なブロックストレージは、別のアカウントに割り当てられる前に、ゼロで上書きされます。機密データを扱っている場合は、手動によるデータの暗号化や、Amazon EBS 暗号化 で保護されているボリュームへのデータの格納を検討してください。詳細については、「Amazon EBS Encryption」を参照してください。

デフォルトでは、インスタンスの起動時に作成およびアタッチされた EBS ボリュームは、インスタンスの終了時に削除されます。この動作を変更するには、インスタンスの起動時にフラグ `DeleteOnTermination` の値を `false` に変更します。値を変更すると、インスタンスが終了してもボリュームが保持されるので、そのボリュームを別のインスタンスにアタッチできます。詳細に関しては、

http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBSVolumes.html を参照してください。

■ AWS サービス関連情報

N/A

■ 情報処理事業者（お客様）の該当事項

情報処理事業者は情報処理業務の再委託にあたり再委託先に対し同等の情報廃棄プロセスを順守させる管理責任があります。

■ 推奨される追加の実施事項

N/A

■ AWS 認証情報(ISO27001, Annex.A and ISO27017)

A.8 資産の管理

A.8.1

A.8.2

A.8.3

A.11 物理的及び環境的セキュリティ

A.11.2

A.12 運用のセキュリティ

A.12.1

A.12.2

A.12.3

A.12.4

A.12.5

A.12.6

A.12.7

A.15 供給者関係

A.15.1

A.15.2