

# 医療情報システム向け AWS 利用リファレンス (総務省版)

2018 年 12 月 10 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（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 | 総務省版」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に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。

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

### 3.2.1

#### 組織的安全管理対策

(ア)

#### 組織・体制の整備

##### ■ ガイドラインとして必要な要求事項 Seq.1

---

①

サービスの提供についての管理責任を有する責任者を設置する。

##### ■ 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

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。

## 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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

##### サービスの管理責任

クラウドサービス事業者は、サービスの管理責任者を設置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.6 情報セキュリティのための組織

A.6.1.1

A.6.1.3

C.L.D.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係

C.L.D.6.3.1

---



### 3.2.1

#### 組織的安全管理対策

(ア)

#### 組織・体制の整備

##### ■ ガイドラインとして必要な要求事項 Seq.2

---

②

情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）を設置する。

##### ■ 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 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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

## システムの管理責任

クラウドサービス事業者は、システム管理責任者を設置する必要があります。

システム管理者は、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。

### ■ 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.6 情報セキュリティのための組織

##### A.6.1.1

##### A.6.1.3

#### C.L.D.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係

##### C.L.D.6.3.1

---

### 3.2.1

#### 組織的安全管理対策

(ア)

#### 組織・体制の整備

##### ■ ガイドラインとして必要な要求事項 Seq.3

---

③

サービスの提供に係る情報システムの運用に関する事務を統括する責任者を設置する。

##### ■ 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 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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

システムの運用管理責任

クラウドサービス事業者は、本サービスの情報システムの運用責任者を設置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.6 情報セキュリティのための組織

A.6.1.1

A.6.1.3

C.L.D.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係

C.L.D.6.3.1

---

### 3.2.1

#### 組織的安全管理対策

##### (ア) 組織・体制の整備

##### ■ ガイドラインとして必要な要求事項 Seq.4

---

#### ④

①から③に掲げた責任者の任命・解任等のルールを策定する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

##### - クラウドサービス事業者内の体制及び責任者の任命・解任等のルール

- ・サービスの提供についての管理責任を有する責任者
- ・システム管理者
- ・サービスの提供に係る情報システムの運用管理責任者

##### ■ 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.6 情報セキュリティのための組織

##### A.6.1.1

##### A.6.1.3

#### C.L.D.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係

##### C.L.D.6.3.1

#### 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

---

### 3.2.1

#### 組織的安全管理対策

##### (イ) 1

#### 守秘義務

##### ■ ガイドラインとして必要な要求事項 Seq.5

---

##### ①

サービスに係る情報及び受託した情報に関する守秘義務について、サービス提供に係る契約に含める。契約には、守秘義務に違反したクラウドサービス事業者にはペナルティが課されること、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。

##### ■ 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

N/A

## ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はデータの統制と所有権を有していますので、クラウドサービス事業者は、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。

クラウドサービス事業者は医療機関等との契約において、以下内容を盛り込む必要があります。

- ・提供サービスに係る情報および受託医療情報に関する守秘義務



- ・守秘義務違反等のペナルティ条項
- ・受託情報の取り扱いに関する医療機関等による監督に関する内容

■ 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

A.15.2

A.18 順守

A.18.1

---

### 3.2.1

#### 組織的安全管理対策

##### (イ) 2

#### 運用規定等の遵守

##### ■ ガイドラインとして必要な要求事項 Seq.6

##### ①

サービス提供に係る契約において、次項（ウ）1.に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、クラウドサービス事業者はデータの統制と所有権を有していますので、クラウドサービス事業者は、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

C.L.D.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係

C.L.D.6.3.1

A.18 順守

A.18.

---

### 3.2.1

#### 組織的安全管理対策

#### 関係ガイドラインの遵守

#### ■ ガイドラインとして必要な要求事項 Seq.7

##### ①

サービス提供に係る契約において、本ガイドラインのほか、厚生労働省ガイドライン及び経済産業省ガイドラインを遵守する旨を含める。

#### ■ 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

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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、以下の 3 省 3 ガイドラインの遵守する旨の内容をサービス契約に含める必要があります。

- ・厚生労働省「医療情報システムの安全管理に関するガイドライン」
- ・総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」
- ・経済産業省「医療情報を受託管理するクラウドサービス事業者向けガイドライン」

#### ■ 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.18 順守

### A.18.1

---

### 3.2.1

#### 組織的安全管理対策

##### (イ) 3

#### 関係ガイドラインの遵守

##### ■ ガイドラインとして必要な要求事項 Seq.8

---

##### ②

①に示す各ガイドラインの遵守状況を医療機関等に提示する際は、可能な限り具体的に行う（例えば、総務省が定める

「ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針」（平成 29 年 3 月 31 日）に定める事項に準じた情報の提供を行う等）

##### ■ 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

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、各ガイドラインの遵守状況を医療機関等に提示するためのホワイトペーパーなどを準備しておくことが求められます。ホワイトペーパーには、総務省が定める情報開示指針などに準じた可能な限り具体的な内容を盛り込む必要があります。

### ■ 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.18 順守

### A.18.1

---



### 3.2.1

#### 組織的安全管理対策

##### (ウ) 1 基本方針と管理目的の表明

##### ■ ガイドラインとして必要な要求事項 Seq.9

---

##### ①

経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、個人情報保護方針および個人情報保護規程等を策定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

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 1

#### 基本方針と管理目的の表明

##### ■ ガイドラインとして必要な要求事項 Seq.10

---

##### ②

①の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、策定した個人情報保護方針および個人情報保護規程等に、個人情報保護法及び個人情報保護委員会のガイドラインに則って、医療情報を取り扱うための安全管理措置等を実施する旨を含める必要があります。

- 組織的安全管理措置
- 人的安全管理措置
- 物理的安全管理措置
- 技術的安全管理措置

##### ■ 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.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

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 1 基本方針と管理目的の表明

##### ■ ガイドラインとして必要な要求事項 Seq.11

---

#### ③

①の指針等には、個人情報保護法の対象外の情報（死者に関する情報等）であっても、医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、策定した個人情報保護方針および個人情報保護規程等には、取り扱う個人情報を明確に定義していく必要があります。

死者に関する情報等、個人情報保護法の対象外の情報についても対象と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.8 資産の管理

##### A.8.1

##### A.8.2

##### A.8.3

##### C.L.D.8.1.5 クラウドサービスカスタマの資産の除去

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 1

#### 基本方針と管理目的の表明

- ガイドラインとして必要な要求事項 Seq.12

---

#### ④

情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーを策定する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報セキュリティ基本方針や医療情報処理にあたり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.5 情報セキュリティのための方針群

##### A.5.1

#### 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

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 1 基本方針と管理目的の表明

##### ■ ガイドラインとして必要な要求事項 Seq.13

---

##### ⑤

情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、策定した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
- クラウドサービス事業者内の体制及び施設

##### ■ 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.6 情報セキュリティのための組織

##### A.6.1

#### C.L.D.6.3 クラウドサービスカスタムとクラウドサービスプロバイダとの関係

##### C..L.D.6.3.1

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 1

#### 基本方針と管理目的の表明

##### ■ ガイドラインとして必要な要求事項 Seq.14

---

##### ⑥

情報セキュリティポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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



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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、策定した情報セキュリティ基本方針や運用管理規程等については、サービス仕様適合開示書に基づき、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

#### A.15 供給者関係

A.15.1

A.15.2



### 3.2.1

#### 組織的安全管理対策

##### (ウ) 2

#### サービス提供先の体制

##### ■ ガイドラインとして必要な要求事項 Seq.15

##### ①

サービスの提供に係る体制を、緊急時の対応も含めて明確にする。

##### ■ 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

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。

## 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

-J18

<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/>

#### ■ クラウドサービス事業者（お客様）の該当事項



クラウドサービス事業者は、「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。

クラウドサービス事業者は、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。

クラウドサービス事業者は、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

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

##### A.6 情報セキュリティのための組織

###### A.6.1

##### C.L.D.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係

###### C..L.D.6.3.1

##### 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

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 2

#### サービス提供先の体制

##### ■ ガイドラインとして必要な要求事項 Seq.16

##### ②

サービスの提供に係る体制等に関する情報（再委託による体制に関する情報を含む）の開示等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

N/A

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスの提供に係る体制等に関する情報（再委託による体制に関する情報を含む）の開示等について、サービス仕様適合開示書に基づき、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

## A.15 供給者関係

### A.15.1

### A.15.2

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 3

#### 契約書・マニュアル等の文書の管理

##### ■ ガイドラインとして必要な要求事項 Seq.17

---

##### ①

情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づき文書の管理を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報セキュリティに関する基本方針や運用管理規程等の文書作成を実施する必要があります。

また文書管理規程を作成し、その規程の則って文書を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)

#### 7.5.3 文書化した情報の管理

#### A.5 情報セキュリティのための方針群

##### A.5.1

#### 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

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 3

#### 契約書・マニュアル等の文書の管理

- ガイドラインとして必要な要求事項 Seq.18
- 

##### ②

サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）上の医療情報処理にあたり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。

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

- クラウドサービス（AWS）上の情報資産の管理方法（リスク分析）

クラウドサービス（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

- 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

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 3 契約書・マニュアル等の文書の管理

##### ■ ガイドラインとして必要な要求事項 Seq.19

---

#### ③

サービスの運用等に係るマニュアル等の文書管理に関して、開示可能範囲、開示に必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスの運用等に係るマニュアル等の文書管理に関して、開示可能範囲、開示に必要な条件等について、サービス仕様適合開示書に基づき、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

#### A.15 供給者関係

A.15.1

A.15.2

---



### 3.2.1

#### 組織的安全管理対策

##### (ウ) 3

#### 契約書・マニュアル等の文書の管理

##### ■ ガイドラインとして必要な要求事項 Seq.20

---

#### ④

医療情報の管理状況に係る資料の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）上の医療情報の管理状況に関係する資料の提供について、サービス仕様適合開示書に基づき、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

#### A.15 供給者関係

A.15.1

A.15.2

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 4

#### リスクの発現の予防、発生時の対応の方法

##### ■ ガイドラインとして必要な要求事項 Seq.21

##### ①

サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。

##### ■ AWS のインフラストラクチャー関連事項

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。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスのリスク分析並びに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リスク分析・リスク対応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.6.1.2 情報セキュリティリスクアセスメント

## 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

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 4

リスクの発現の予防、発生時の対応の方法

##### ■ ガイドラインとして必要な要求事項 Seq.22

##### ②

サービスに係るリスク分析の結果、対応措置及び事故等の発生時の対応等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

N/A

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに係るリスク分析の結果策定したリスク対応実施策並びに、事故等の発生時の対応等について、サービス仕様適合開示書に基づき、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

## A.15 供給者関係

### A.15.1

### A.15.2

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 5

#### 機器を用いる場合の機器等の管理

##### ■ ガイドラインとして必要な要求事項 Seq.23

---

##### ①

機器等の管理方法について、文書化を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、受託する医療情報や機器等の管理を文書し、その文書に則って、資産管理台帳を作成・管理を行う必要があります。

資産管理台帳の管理には、以下を含む必要があります。

- 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
- 常時閲覧可能な状態として管理
- 不正アクセス行為の記録（アクセスログの取得等）

資産管理台帳には、以下の情報を記載します。

- 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）

##### ■ 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

---



### 3.2.1

#### 組織的安全管理対策

##### (ウ) 5

#### 機器を用いる場合の機器等の管理

##### ■ ガイドラインとして必要な要求事項 Seq.24

#### ②

機器等について、台帳管理等により所在確認等を行う旨を定める。

##### ■ AWS のインフラストラクチャー関連事項

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。

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、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

クラウドサービス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

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 5

#### 機器を用いる場合の機器等の管理

##### ■ ガイドラインとして必要な要求事項 Seq.25

### ③

機器等の管理等に関する自社の運用規程について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、機器等の管理等に関する自社の運用規程について、サービス仕様適合開示書に基づき、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

#### A.15 供給者関係

A.15.1

A.15.2

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 6

#### 個人情報の記録媒体の管理方法

##### ■ ガイドラインとして必要な要求事項 Seq.26

##### ①

個人情報を記録した媒体の管理等に関する運用規程を策定する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）上の医療情報処理にあたり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。

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

- 医療情報を格納する媒体の管理（特に個人情報を含む場合）
  - 媒体の持出管理
  - 台帳管理の実施
  - キヤビネに保管の際の施錠管理
  - 媒体製造業者が定める媒体の劣化や保管期間を厳守のこと
  - 媒体廃棄の管理 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.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

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 6

#### 個人情報の記録媒体の管理方法

##### ■ ガイドラインとして必要な要求事項 Seq.27

##### ②

個人情報を記録した媒体の管理等に関する運用規程について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、個人情報記録した媒体の管理等に関する運用管理規程について、サービス仕様適合開示書に基づき、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

##### A.15 供給者関係

A.15.1

A.15.2

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 7

##### 患者等への説明と同意を得る方法

##### ■ ガイドラインとして必要な要求事項 Seq.28

##### ①

医療機関等で患者等への説明及び同意を得る際のクラウドサービス事業者の情報提供に関して、その提供範囲やクラウドサービス事業者が担う役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等で患者等への説明及び同意を得る際のクラウドサービス（AWS）を利用した情報提供に関して、その提供範囲や AWS が担う役割等について、サービス仕様適合開示書に基づき、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

## A.15 供給者関係

### A.15.1

### A.15.2

---

### 3.2.1

#### 組織的安全管理対策

(ウ) 8

#### .監査

- ガイドラインとして必要な要求事項 Seq.29
- 

①

サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等について明文化を行う。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）上の医療情報処理にあたり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。

クラウドサービス事業者は、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
- クラウドサービス事業者内の体制
- 第三者による情報セキュリティ監査等の方針及び監査内容

- 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

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 8

##### .監査

##### ■ ガイドラインとして必要な要求事項 Seq.30

---

##### ②

第三者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容を明確にする。

##### ■ 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/>

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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

A.8 資産の管理

A.8.1

A.8.2

A.8.3

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.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

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.18 順守

### A.18.1.1

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 8

##### .監査

##### ■ ガイドラインとして必要な要求事項 Seq.31

---

##### ③

監査実施について記録し、当該記録の保存・管理方法を明確にする。

##### ■ 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



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。

## 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/>

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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

A.8 資産の管理

A.8.1

A.8.2

A.8.3

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.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

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.18 順守

A.18.1.1



### 3.2.1

#### 組織的安全管理対策

##### (ウ) 8.監査

##### ■ ガイドラインとして必要な要求事項 Seq.32

---

#### ④

自社において実施する情報システム監査等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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。

<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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自社において実施する情報システム監査等について、サービス仕様適合開示書に基づき、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

##### A.15 供給者関係

##### A.15.1

##### A.15.2

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 8.監査

##### ■ ガイドラインとして必要な要求事項 Seq.33

---

##### ⑤

医療機関等に開示する監査記録等の範囲・条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等に開示する監査記録等の範囲・条件等について、サービス仕様適合開示書に基づき、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

#### A.15 供給者関係

A.15.1

A.15.2

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 9

##### 苦情・質問の受け付け窓口の設置

##### ■ ガイドラインとして必要な要求事項 Seq.34

##### ①

医療機関等の管理者からの問合せ窓口を設ける。また受付の時間帯等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に盛り込んだ医療機関等の管理者からの問合せ窓口および問合せ窓口の受付時間帯等について、サービス仕様適合開示書に基づき、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

#### A.15 供給者関係

A.15.1

A.15.2

---

### 3.2.1

#### 組織的安全管理対策

##### (ウ) 9

#### 苦情・質問の受け付け窓口の設置

- ガイドラインとして必要な要求事項 Seq.35
- 

##### ②

自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、医療機関等からの問合せ窓口を一元化する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等からの問合せ窓口を一元化する必要があります。

- 自社が提供するサービスの問合せ窓口
- 自社が契約した第三者提供のクラウドサービスを利用して提供したサービスの問合せ窓口

- 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

### 3.2.1

#### 組織的安全管理対策

##### (Ⅰ) 1

#### アクセス管理規程の策定

##### ■ ガイドラインとして必要な要求事項 Seq.36

---

##### ①

クラウドサービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、並びにアクセス管理の運用状況に関する定期的なレビューの実施等を内容とするアクセス管理規程を策定する。

##### ■ 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

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自らがサービスの運営を目的として情報システムへアクセスする際のアクセス管理規程を策定する必要があります。アクセス管理規程には以下内容を盛り込む必要があります。

- ・アクセス権限の管理
- ・アカウント管理
- ・認証およびアクセスログの収集と保存
- ・アクセスに関する運用状況の定期的なレビューの実施

##### ■ 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.9 アクセス制御

##### A.9.1

##### A.9.2

A.9.3

A.9.4

---



## 組織的安全管理対策

### (工) 1

#### アクセス管理規程の策定

##### ■ ガイドラインとして必要な要求事項 Seq.37

---

### ②

サービスの提供に係るアクセス記録（外部からのアクセス、利用者によるアクセス等を含む）の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定する。

##### ■ 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

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービス提供に係るアクセス管理規程を策定する必要があります。

アクセス管理規程には以下内容を盛り込む必要があります。

- ・外部及び利用者のアクセス記録の保存
- ・保存されたアクセス記録の定期的なレビューと改善

##### ■ 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.9 アクセス制御

##### A.9.1

##### A.9.2

##### A.9.3

##### A.9.4

## A.12 運用のセキュリティ

A.12,4

---

### 3.2.1

#### 組織的安全管理対策

##### (Ⅰ) 2

#### 委託契約に含めるべき事項

- ガイドラインとして必要な要求事項 Seq.38

---

##### ①

医療情報の取扱いに関する委託契約に、以下の内容を含める。

- ・個人情報に関して、他の情報と区別して適切に管理を行う。
- ・医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービス提供に係るアクセス管理規程を策定する必要があります。

アクセス管理規程には以下内容を盛り込む必要があります。

- ・外部及び利用者のアクセス記録の保存
- ・保存されたアクセス記録の定期的なレビューと改善

- 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

##### A.15.2

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 1

##### 施錠管理

##### ■ ガイドラインとして必要な要求事項 Seq.39

---

###### ①

サービスに供する機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う必要があります。

AWS のデータセンターを使用の場合は、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](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、クラウドサービス事業者は、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

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 1

##### 施錠管理

##### ■ ガイドラインとして必要な要求事項 Seq.40

---

##### ②

サービスに供するサーバ等を格納するラック等について、施錠管理を行う。

##### ■ 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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供するサーバ等を格納するラック等について、施錠管理を行う必要があります。

AWS のデータセンターを使用の場合は、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](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、クラウドサービス事業者は、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。

- 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、クラウドサービス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

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 1 施錠管理

##### ■ ガイドラインとして必要な要求事項 Seq.41

---

#### ③

サービスに供する媒体等を格納するキャビネット等について、施錠管理を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する媒体等を格納するキャビネット等について、施錠管理等、安全対策を実施する必要があります。

- 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、クラウドサービス事業者が媒体管理をする必要はありません。

##### ■ 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.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

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 2

#### アクセス制御

##### ■ ガイドラインとして必要な要求事項 Seq.42

---

##### ①

サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する必要があります。

- 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、クラウドサービス事業者が許可された者のみが入退できるように制限する必要はありません。

##### ■ 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

---



### 3.2.2

#### 物理的安全管理対策

##### (ア) 2

#### アクセス制御

- ガイドラインとして必要な要求事項 Seq.43

---

#### ②

サービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う必要があります。

- 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、クラウドサービス事業者が入退状況を管理をする必要はありません。

- 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

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 2

##### アクセス制御

##### ■ ガイドラインとして必要な要求事項 Seq.44

---

##### ③

サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、入退者の特定ができるような方策を講じる必要があります。

- 個人認証システム等による制御
- 個人認証システム等による制御が不可能な場合
  - ・入退に必要な暗証番号等の変更を定期的（週単位）で行う等、
- 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、クラウドサービス事業者が入退者の特定等入退管理をする必要はありません。

##### ■ 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

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 2

#### アクセス制御

##### ■ ガイドラインとして必要な要求事項 Seq.45

---

#### ④

サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。

##### ■ 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](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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付けることが求められます。

- 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、クラウドサービス事業者が入退者に名札等の着用を義務付ける必要はありません。。

##### ■ 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

### 3.2.2

#### 物理的安全管理対策

##### (ア) 2

#### アクセス制御

- ガイドラインとして必要な要求事項 Seq.46

---

##### ⑤

サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する必要があります。

- 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、クラウドサービス事業者が業務遂行に関係のない個人的所有物の持ち込みを制限する必要はありません。

- 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

---



### 3.2.2

#### 物理的安全管理対策

##### (ア) 2

#### アクセス制御

##### ■ ガイドラインとして必要な要求事項 Seq.47

---

##### ⑥

サービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。

##### ■ 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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする必要があります。

- 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、クラウドサービス事業者が上記の対応をする必要はありません。

■ 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

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 2 アクセス制御

##### ■ ガイドラインとして必要な要求事項 Seq.48

---

⑦

①～⑥につき、運用管理規程等に規定する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

- サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限すること
- サービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行うこと
- サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにすること

（但し、難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じること）

- サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付けること
- サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限すること
- サービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにすること

##### ■ 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.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

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 3

#### サービスに供する機器や媒体を保存する施設

##### ■ ガイドラインとして必要な要求事項 Seq.49

##### ①

サービスに供する機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐える機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。

##### ■ 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。

#### 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。

### 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

## ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する必要があります。

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、クラウドサービス事業者は 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](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、クラウドサービス事業者は、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.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

---

### 3.2.2

#### 物理的安全管理対策

##### (ア) 3

サービスに供する機器や媒体を保存する施設

##### ■ ガイドラインとして必要な要求事項 Seq.50

---

##### ②

①の施設を設置する建築物は、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

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。

## 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器や媒体を物理的に保存するための施設として、サービス仕様適合開示書に基づき、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

#### A.15 供給者関係

A.15.1

A.15.2

---



### 3.2.2

#### 物理的安全管理対策

##### (ア) 4

##### カメラによる監視

##### ■ ガイドラインとして必要な要求事項 Seq.51

---

##### ①

サービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する。

##### ■ 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。

##### 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。

## 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、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、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。

。

## 立ち入りの規制と監視

境界防御レイヤーへの立ち入りは、管理されています。入り口ゲートには警備員を配置し、監視カメラで警備員と訪問者を監視する監督者も配置されています。立ち入りを許可された人はバッジを渡されます。このバッジにより、多要素認証が実行され、事前に承認されたエリアへのアクセスが制限されます。

## 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 データセンター情報

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

#### 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/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する必要があります。

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を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、クラウドサービス事業者は 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](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、クラウドサービス事業者は、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



### 3.2.2

#### 物理的安全管理対策

##### (ア) 4

##### カメラによる監視

##### ■ ガイドラインとして必要な要求事項 Seq.52

---

##### ②

防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。

##### ■ 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。

## 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、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、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。

。

### 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。

## 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 データセンター情報

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

#### 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/com>

#### ■ 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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる必要があります。

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、クラウドサービス事業者は 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](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、クラウドサービス事業者は、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.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.12.4

##### A.16 情報セキュリティインシデント管理

###### A.16.1

### 3.2.2

#### 物理的安全管理対策

##### (ア) 4

##### カメラによる監視

##### ■ ガイドラインとして必要な要求事項 Seq.53

---

### ③

サービスに供する機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がいないことを確認する。

##### ■ 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。

## 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、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、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。

。

### 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。

## 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 データセンター情報

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

#### 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/com>

#### ■ 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特にあるお客様には、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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスに供する機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がないことを確認する必要があります。

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、クラウドサービス事業者は 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](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、クラウドサービス事業者は、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.12.4

##### A.12.7



## A.16 情報セキュリティインシデント管理

### A.16.1

---

### 3.2.2

#### 物理的安全管理対策

##### (イ) 1

#### 覗き見等の防止

- ガイドラインとして必要な要求事項 Seq.54
- 

##### ①

個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等の対策を行う。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用した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.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

---

### 3.2.2

#### 物理的安全管理対策

##### (イ) 1

#### 覗き見等の防止

- ガイドラインとして必要な要求事項 Seq.55
- 

##### ②

運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用した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.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

---

### 3.2.2

#### 物理的安全管理対策

##### (ウ) 1

#### 機器・媒体等の盗難・紛失防止

##### ■ ガイドラインとして必要な要求事項 Seq.56

---

##### ①

個人情報物理的に保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はデータの統制と所有権を有しています。

クラウドサービス事業者は、医療情報システムに必要な最低限の範囲で個人情報を格納・保存し、定期的に個人情報の棚卸し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.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

---

### 3.2.2

#### 物理的安全管理対策

##### (ウ) 1

#### 機器・媒体等の盗難・紛失防止

- ガイドラインとして必要な要求事項 Seq.57
- 

##### ②

個人情報が存在する PC 等の重要な機器には、盗難防止用チェーンを取り付ける。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者が、クラウドサービス（AWS）を利用した医療情報システム以外の PC などに個人情報を保存する際は盗難防止用チェーンを取り付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.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

---

### 3.2.2

#### 物理的安全管理対策

##### (ウ) 1 機器・媒体等の盗難・紛失防止

##### ■ ガイドラインとして必要な要求事項 Seq.58

---

### ③

受託する個人情報を運用や保守に用いる端末に保存しない旨、自社の運用管理規程等に定める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、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
- クラウドサービス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  
運用・保守端末へ個人情報を保存しない旨を含む
- 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ア) 1 利用者の識別

##### ■ ガイドラインとして必要な要求事項 Seq.59

---

##### ①

情報システムの利用者を特定し識別できるように、アカウントの発行を行う（複数の利用者による ID の共同利用は行わない。ただし当該情報システムが他の情報システムを利用するための ID（non interactive ID）は除く）。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、情報システムの利用者を特定し識別できるように、アカウントの発行を行うことが求められます。

##### ■ 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

### 3.2.3

#### 技術的安全管理対策

##### (ア) 1 利用者の識別

##### ■ ガイドラインとして必要な要求事項 Seq.60

---

##### ②

利用者のなりすまし等を防止するための認証を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、利用者のなりすまし等を防止するための認証を行う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

---

### 3.2.3

#### 技術的安全管理対策

##### (ア) 1

##### 利用者の識別

- ガイドラインとして必要な要求事項 Seq.61
- 

##### ③

利用者には、医療機関等においてサービスを利用する者のほか、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含める。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。利用者には、医療機関等においてサービスを利用する者、情報システムの運用者、開発に従事する者、管理者権限を有する者を含め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

---

### 3.2.3

#### 技術的安全管理対策

##### (ア) 1

##### 利用者の識別

##### ■ ガイドラインとして必要な要求事項 Seq.62

---

##### ④

情報システムの運用若しくは開発に従事する者又は管理者権限を有する者に対する ID の発行は必要最小限とし、定期的な棚卸しを行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、以下の対応が求められます。

- ・情報システムの運用者、開発者、管理者権限を有する者に対する ID の発行は必要最小限とすること
- ・ID の定期的な棚卸しを行うこと

##### ■ 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





### 3.2.3

#### 技術的安全管理対策

(ア) 2 本人識別のためにパスワードを設定する時のルール

##### ■ ガイドラインとして必要な要求事項 Seq.63

###### ①

本人の識別・認証に、ユーザIDとパスワードを組み合わせる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。

- ・利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと情報システムにアクセスできないようにする。
- ・初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。
- ・パスワードの設定に際しては、複数の文字種（英数字・大文字・小文字・記号等）を用い、また、8文字以上等、十分に安全な長さの文字列等から構成されるルールとする。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。ユーザIDとパスワードを組み合わせる場合には、それらを、本人しか知り得ない状態に保つよう対策を行うことが求められます。具体的な対策例は以下の通りです。

- ・利用者に対して、最初の利用時に初期パスワードを変更しないと情報システムにアクセスできないようにする
- ・初期パスワード以外のパスワードは、利用者本人に設定させる
- ・初期パスワード以外のパスワードは、利用者本人しか知りえない内容を設定するよう求める
- ・パスワードの設定は、複数の文字種を用い、8文字以上等、十分に安全な長さの文字列等から構成されるルールとする

##### ■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ア) 2

本人識別のためにパスワードを設定する時のルール

##### ■ ガイドラインとして必要な要求事項 Seq.64

---

##### ②

パスワード認証に係る以下のルールを実現する措置を講じる。

- ・パスワード入力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。
- ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けけない仕組みとする。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、パスワード認証に係る以下の措置を講じることが求められます。

- ・パスワード入力不成功であった場合、再入力に対して一定の不応時間を設定する
- ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けけない仕組みとする

##### ■ 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



### 3.2.3

#### 技術的安全管理対策

##### (ア) 2

本人識別のためにパスワードを設定する時のルール

- ガイドラインとして必要な要求事項 Seq.65

---

##### ③

パスワードには十分な安全性を満たす有効期間を設定する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、パスワードには十分な安全性を満たす有効期間を設定することが求められます。ただし、利用者が患者等である場合には以下の対応が必要です。

- ・他のサービスで利用しているパスワードを使わないよう促す
- ・サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする

- 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



### 3.2.3

#### 技術的安全管理対策

##### (ア) 2

本人識別のためにパスワードを設定する時のルール

- ガイドラインとして必要な要求事項 Seq.66

---

#### ④

認証に際して ID 及びパスワードによらない場合でも、上記と同等以上の安全性を確保する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。認証に際して ID 及びパスワードによらない場合でも、上記と同等以上の安全性を確保することが求められます。

- 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

### 3.2.3

#### 技術的安全管理対策

##### (ア) 3

#### パスワードの管理

- ガイドラインとして必要な要求事項 Seq.67

---

##### ①

利用者のパスワード情報は、ハッシュ値での保存を行う等、暗号化手法により、管理する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。利用者のパスワード情報は、ハッシュ値での保存を行う等、暗号化手法により、管理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.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

### 3.2.3

#### 技術的安全管理対策

##### (ア) 3

#### パスワードの管理

##### ■ ガイドラインとして必要な要求事項 Seq.68

---

##### ②

サービスに供する製品等の導入に際しては、初期パスワードを変更するだけでなく、必要なアカウントの棚卸しを行い、不要なものについては削除を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、サービスに供する製品等の導入に際しては、以下の対応が求められます。

- ・初期パスワードの変更
- ・必要なアカウントの棚卸し
- ・不要なアカウントの削除

##### ■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ア) 3 パスワードの管理

##### ■ ガイドラインとして必要な要求事項 Seq.69

---

##### ③

利用者が ID、パスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。利用者が ID、パスワードを失念した場合には、予め策定した手順で本人への通知又は再発行を行う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.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



### 3.2.3

#### 技術的安全管理対策

##### (ア) 3 パスワードの管理

##### ■ ガイドラインとして必要な要求事項 Seq.70

---

#### ④

パスワード等の情報の漏洩が生じた場合又は不正な第三者からの攻撃により漏洩した場合には、直ちに当該 ID を無効化し、あらかじめ策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。パスワード等の情報の漏洩が生じた場合又は不正な第三者からの攻撃により漏洩した場合には、直ちに以下の対応が求められます。

- ・当該 ID の無効化
- ・あらかじめ策定した手順による新規のログイン情報の再発行
- ・利用者への速やかな通知

##### ■ 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

### 3.2.3

#### 技術的安全管理対策

##### (ア) 3

#### パスワードの管理

- ガイドラインとして必要な要求事項 Seq.71
- 

##### ⑤

パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し変更できるような対応を講じる。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。パスワード等の情報の漏洩のおそれがある場合、利用者本人に通知した上で、そのパスワードを無効化し変更できるような対応が求められます。

- 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.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

### 3.2.3

#### 技術的安全管理対策

##### (ア) 3

#### パスワードの管理

- ガイドラインとして必要な要求事項 Seq.72

---

#### ⑥

利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を行う。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準の策定と運用が求められます。

- 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.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

### 3.2.3

#### 技術的安全管理対策

##### (ア) 3 パスワードの管理

##### ■ ガイドラインとして必要な要求事項 Seq.73

---

##### ⑦

利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するのに必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、利用者のパスワードの世代管理が求められます。パスワード変更は、過去に設定したパスワードを設定できないような運用で、安全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.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



### 3.2.3

#### 技術的安全管理対策

##### (ア) 3 パスワードの管理

##### ■ ガイドラインとして必要な要求事項 Seq.74

---

##### ⑧

自社において定めたパスワードポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はパスワードポリシーについて、サービス仕様適合開示書に基づき、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

#### 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

### 3.2.3

#### 技術的安全管理対策

##### (ア) 4

#### 複数要素認証への対応

##### ■ ガイドラインとして必要な要求事項 Seq.75

##### ①

情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、2 要素認証以上の認証強度のある方法による。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。情報システムの運用者、開発者、管理者権限を有する者の情報システム利用に係る認証は、2 要素認証以上の認証強度のある方法によることが求められます。

##### ■ 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



### 3.2.3

#### 技術的安全管理対策

##### (ア) 4

#### 複数要素認証への対応

##### ■ ガイドラインとして必要な要求事項 Seq.76

---

##### ②

利用者の認証で採用する認証方式について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は利用者の認証方式について、サービス仕様適合開示書に基づき、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

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

### 3.2.3

#### 技術的安全管理対策

##### (ア) 4

#### 複数要素認証への対応

##### ■ ガイドラインとして必要な要求事項 Seq.77

---

##### ③

利用者の認証において、固定式の ID・パスワードによる認証方式を採用している場合には、固定式の ID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第 5 版の公表（平成 29 年 5 月）から約 10 年後を目途に 2 要素認証について厚生労働省ガイドライン 6.5 章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。利用者の認証において、固定式の ID・パスワードによる認証方式を採用している場合は、固定式の ID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努めることが求められており、さらに 2027 年 5 月を目処に 2 要素認証に対応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

---

### 3.2.3

#### 技術的安全管理対策

##### (ア) 4

#### 複数要素認証への対応

##### ■ ガイドラインとして必要な要求事項 Seq.78

---

#### ④

利用者の認証に際して、何らかの物理的な媒体・身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段・手順を事前に定める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。利用者の認証に際して、何らかの物理的な媒体・身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段・手順を事前に定めることが求められます。

##### ■ 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



### 3.2.3

#### 技術的安全管理対策

##### (ア) 4 複数要素認証への対応

##### ■ ガイドラインとして必要な要求事項 Seq.79

---

##### ⑤

代替的手段・手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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、代替的手段・手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差を最小とすることが求められます。

##### ■ 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

---

3.2.3

技術的安全管理対策

(ア) 4

複数要素認証への対応

■ ガイドラインとして必要な要求事項 Seq.80

---

⑥

代替的手段・手順により、情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。

■ 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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。代替的手段・手順で、情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、管理することが求められます。

■ 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

---

3.2.3

技術的安全管理対策

(ア) 4

## ■ ガイドラインとして必要な要求事項 Seq.81

---

⑦

その他、一時的な利用者の認証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。

### ■ 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

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。一時的な利用者の認証方法について、サービス仕様適合開示書に基づき、医療機関等と合意することが求められます。

#### ■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (イ) 1

#### 情報管理区分

- ガイドラインとして必要な要求事項 Seq.82

---

##### ①

医療情報とそれ以外の情報を区分できる措置を講じる。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は医療情報とそれ以外の情報を区分する方式を設計・実装する必要があります。

- 推奨される追加の実施事項

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

---

### 3.2.3

#### 技術的安全管理対策

##### (イ) 1

#### 情報管理区分

- ガイドラインとして必要な要求事項 Seq.83
- 

##### ②

医療情報については、情報区分に従ってアクセス制御を行えるようにする。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報については、情報区分に従ってアクセス制御方式を設計・実装する必要があります。

- 推奨される追加の実施事項

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

---

### 3.2.3

#### 技術的安全管理対策

##### (イ) 1

##### 情報管理区分

##### ■ ガイドラインとして必要な要求事項 Seq.84

---

##### ③

仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。

##### ■ AWS のインフラストラクチャー関連事項

AWS 環境は仮想化されたマルチテナント環境です。AWS は、お客様間を隔離するために設計されたセキュリティ管理プロセス、PCI 統制、その他のセキュリティ統制を実装しています。AWS システムは、仮想化ソフトウェアによるフィルタリング処理により、お客様に割り当てられていない物理ホストや物理インスタンスにアクセスできないように設計されています。このアーキテクチャは独立 PCI 認定審査機関 (QSA) によって検証済みであり、2015 年 4 月に発行された PCI DSS 3.1 版のすべての要件に準拠することが確認されています。

注意: また、AWS にはシングルテナントのオプションもあります。ハードウェア専有インスタンスは、単一のお客様専用のハードウェアを実行する Amazon Virtual Private Cloud (Amazon VPC) で起動される Amazon EC2 インスタンスです。ハードウェア専有インスタンスを使用することで、AmazonVPC および AWS クラウドの利点をフルに活用しながら、Amazon EC2 インスタンスをハードウェアレベルで隔離できます。

詳細、最新情報は下記ホワイトペーパーを参照ください。

「主要なコンプライアンス に関する質問と AWS の回答」

[https://d1.awsstatic.com/whitepapers/compliance/Jp\\_Whitepapers/AWS\\_Answers\\_to\\_Key\\_Compliance\\_Questions\\_JP.pdf](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

##### -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/>

##### ■ クラウドサービス事業者 (お客様) の該当事項



クラウドサービス事業者は、仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる必要があります。また、Amazon Virtual Private Cloud (Amazon VPC)を活用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

---

### 3.2.3

#### 技術的安全管理対策

##### (イ) 1

#### 情報管理区分

- ガイドラインとして必要な要求事項 Seq.85

---

#### ④

医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、サービス仕様適合開示書に基づき、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.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

---

### 3.2.3

#### 技術的安全管理対策

##### (イ) 2

##### 権限設定

##### ■ ガイドラインとして必要な要求事項 Seq.86

##### ①

サービスには、医療従事者、関係職種ごとにアクセス権限・範囲等のアクセス制御が可能な機能を含める。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者には、医療従事者、関係職種ごとにアクセス権限・範囲等のアクセス制御が可能な機能を含めたサービスの提供が求められます。

#### ■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (イ) 2

##### 権限設定

- ガイドラインとして必要な要求事項 Seq.87
- 

##### ②

医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行 い、実際に設定する作業に関する役割分担も含めて合意する。なお、アクセス制御に係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行 い、実際に設定する作業に関する役割分担も含めて合意する必要があります。なお、アクセス制御に係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意することが必要です。

- 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.15 供給者関係

---

### 3.2.3

#### 技術的安全管理対策

##### (イ) 2

##### 権限設定

- ガイドラインとして必要な要求事項 Seq.88

---

##### ③

運用管理規程に従い、アクセス管理に関する運用を行い、医療機関等の求めに応じて資料を提出できるようにする。  
資料の提供に係る条件等については、サービス仕様適合開示書に基づき、医療機関等と合意する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に従い、アクセス管理に関する運用を行い、医療機関等の求めに応じて資料を提出することが必要です。資料の提供に係る条件等については、サービス仕様適合開示書に基づき、医療機関等と合意が必要です。

- 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.15 供給者関係

### 3.2.3

#### 技術的安全管理対策

##### (イ) 3

#### アクセス対象の設定

- ガイドラインとして必要な要求事項 Seq.89

---

##### ①

サービスには、受託する医療情報を患者等ごとに管理できる機能を含める。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、受託する医療情報を患者等ごとに管理できる機能をサービスに含める必要があります。

- 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ウ) (a)1

入力者及び確定者の識別及び認証に関する安全管理対策

PC 等の汎用入力端末により記録が作成される場合

##### ■ ガイドラインとして必要な要求事項 Seq.90

##### ①

e - 文書法の対象となる医療情報を含む文書等の作成に PC 等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。

・医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は e - 文書法の対象となる医療情報を含む文書等の作成に PC 等の汎用入力端末を利用する場合、医療機関等の職務権限等に応じたアクセス制御の可否を含め、システムのログイン機能やアクセスログの運用など入力者及び確定者の識別及び認証に関する仕様について、サービス仕様適合開示書に基づき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

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





### 3.2.3

#### 技術的安全管理対策

##### (ウ) (a)2

入力者及び確定者の識別及び認証に関する安全管理対策

臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合

##### ■ ガイドラインとして必要な要求事項 Seq.91

---

##### ①

e-文書法の対象となる医療情報を含む文書等の作成に臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムを利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。

・サービスとの連携におけるインタフェースの構築に関する役割分担

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はe-文書法の対象となる医療情報を含む文書等の作成に臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムを利用する場合、ネットワーク構成やインターフェース設計などの、サービスとの連携におけるインタフェースの構築に関する役割分担について、サービス仕様適合開示書に基づき、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)

N/A

---

### 3.2.3

#### 技術的安全管理対策

##### (ウ) (b)1

記録の確定手順の確立と、作成責任者の識別情報の記録に関する安全管理対策

PC 等の汎用入力端末により記録が作成される場合

##### ■ ガイドラインとして必要な要求事項 Seq.92

---

##### ①

e-文書法の対象となる医療情報を含む文書等の作成に PC 等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。

- ・確定された登録情報（入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時）に関する仕様
- ・入力された内容についての記録確定前における確認の可否等についての仕様
- ・記録の確定権限に関する仕様
- ・確定した記録の追記・削除の機能等に関する仕様
- ・確定した記録の原状回復の機能等に関する仕様
- ・記録の自動確定機能等に関する仕様
- ・代替的な確定権限の機能等に関する仕様

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は e-文書法の対象となる医療情報を含む文書等の作成に PC 等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

- 確定された登録情報（入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時）に関する仕様
- 入力された内容についての記録確定前における確認の可否等についての仕様
  - ・記録の確定権限に関する仕様
  - ・確定した記録の追記・削除の機能等に関する仕様
  - ・確定した記録の原状回復の機能等に関する仕様
  - ・記録の自動確定機能等に関する仕様
  - ・代替的な確定権限の機能等に関する仕様

## ■ 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/>

Amazon Time Sync Service を使用することで、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取得できます。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。

AWS Identity and Access Management (IAM) を使用することで、ユーザーに対して AWS へのアクセスを安全に制御することができます。

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 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ウ) (c)1

#### 更新履歴の保存に関する安全管理対策

##### .更新履歴比較機能

#### ■ ガイドラインとして必要な要求事項 Seq.93

---

##### ①

真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新前と更新後のデータが保存される、又は更新履歴等が保存される等、更新前後の内容を照らし合せることができる機能を含める。

#### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新前と更新後のデータが保存される、又は更新履歴等が保存される等、更新前後の内容を照らし合せることができる機能を含めたサービスの提供が求められます。

#### ■ 推奨される追加の実施事項

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/>

#### ■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ウ) (c)2

#### 更新履歴の保存に関する安全管理対策更新順序識別機能

##### ■ ガイドラインとして必要な要求事項 Seq.94

---

##### ①

真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新履歴が保存され、更新の順序性が識別できる機能を含める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、真正性が求められる医療情報を取り扱うサービスには一旦確定した診療録等を更新する時に更新履歴が保存され、更新の順序性が識別できる機能を含めたサービスの提供が求められます。

##### ■ 推奨される追加の実施事項

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/>

##### ■ 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

---



### 3.2.3

#### 技術的安全管理対策

##### (ウ) (d)

#### 代行入力の承認機能に関する安全管理対策

##### ■ ガイドラインとして必要な要求事項 Seq.95

---

##### ①

真正性が求められる医療情報を取り扱うサービスにおける代行入力を実施するアカウント及び権限設定に関する機能や運用方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、真正性が求められる医療情報を取り扱うサービスにおける代行入力を実施するアカウント及び権限設定に関する機能や運用方法について、サービス仕様適合開示書に基づき、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

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 Identity and Access Management (IAM) を使用することで、ユーザーに対して AWS へのアクセスを安全に制御することができます。

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 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ウ) (d)

#### 代行入力の承認機能に関する安全管理対策

##### ■ ガイドラインとして必要な要求事項 Seq.96

---

#### ②

真正性が求められる医療情報を取り扱うサービスには、代行入力の内容（代行者及び被代行者、代行対象となった記録、代行の日時等）を記録する機能を含める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、真正性が求められる医療情報を取り扱うサービスには、代行入力の内容（代行者及び被代行者、代行対象となった記録、代行の日時等）を記録する機能を含めたサービスの提供が求められます。

##### ■ 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.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

---

### 3.2.3

#### 技術的安全管理対策

##### (ウ) (d)

#### 代行入力の承認機能に関する安全管理対策

##### ■ ガイドラインとして必要な要求事項 Seq.97

---

##### ③

真正性が求められる医療情報を取り扱うサービスには、代行入力後の確定操作(承認)に関する機能を含める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、真正性が求められる医療情報を取り扱うサービスには、代行入力後に確定権限を持ったユーザによる確定操作(承認)に関する機能を含めたサービスの提供が求められます。

##### ■ 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.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

---

### 3.2.3

#### 技術的安全管理対策

##### (Ⅰ) 1

##### アクセス記録の取得

##### ■ ガイドラインとして必要な要求事項 Seq.98

###### ①

情報システムへのアクセスを記録し、一定期間保存する。

##### ■ 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/>

医療情報の監査ログ取得および参照環境の整備はクラウドサービス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/>

##### 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

##### -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](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。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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は情報システムへのアクセスを記録し、一定期間保存する必要があり、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。

「AWS CloudTrail ユーザーガイド」

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-user-guide.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.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

## 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

---

### 3.2.3

#### 技術的安全管理対策

##### (Ⅰ) 1

##### アクセス記録の取得

##### ■ ガイドラインとして必要な要求事項 Seq.99

---

##### ②

アクセス記録には、アクセスした ID、アクセス時刻、アクセス時間、アクセス対象（情報主体単位）等を含める。

##### ■ 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/>

##### -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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者が作成するアクセス記録には、アクセスした ID、アクセス時刻、アクセス時間、アクセス対象（情報主体単位）等を含める必要があります。

クラウドサービス事業者は利用する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、各ユーザーに適切にIAMユーザーを発行することで、AWS CloudTrail を使用して各ユーザー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。

「AWS CloudTrail ユーザーガイド」

<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 Identity and Access Management (IAM) を使用することで、ユーザーに対してAWSへのアクセスを安全に制御することができます。

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 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.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

A.18 順守

A.18.2

---



### 3.2.3

#### 技術的安全管理対策

##### (Ⅰ) 1

##### アクセス記録の取得

- ガイドラインとして必要な要求事項 Seq.100
- 

##### ③

アクセス記録の機能を有しない場合には、サービス仕様適合開示書に基づき、医療機関等と合意する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、アクセス記録の機能を有しない場合には、サービス仕様適合開示書に基づき、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

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。

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

N/A

---

### 3.2.3

#### 技術的安全管理対策

##### (工) 1

##### アクセス記録の取得

##### ■ ガイドラインとして必要な要求事項 Seq. 101

---

##### ④

取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するアクセス記録又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。

##### ■ 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/>

##### 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

### -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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するアクセス記録又はこれに代わる記録について、当該法定年限以上の保存期間を設ける必要があります。

たとえば、診療録は 5 年間の法的保存年限が定められているため、最低 5 年間保存する必要があります。

#### ■ 推奨される追加の実施事項

AWS Identity and Access Management (IAM) を使用することで、ユーザーに対して AWS へのアクセスを安全に制御することができます。

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 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.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

A.18 順守

A.18.2

### 3.2.3

#### 技術的安全管理対策

##### (Ⅰ) 1

##### アクセス記録の取得

##### ■ ガイドラインとして必要な要求事項 Seq. 102

---

##### ⑤

④で定める法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本項におけるアクセス記録の管理方法については、サービス仕様適合開示書で保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う。

##### ■ 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/>

##### 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

### -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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は 3.2.3「技術的安全管理対策」（Ⅰ）1④で定める法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

なお、本項におけるアクセス記録の管理方法については、サービス仕様適合開示書で保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う必要があります。

#### ■ 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.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

## 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

### 3.2.3

#### 技術的安全管理対策

##### (Ⅰ) 1

##### アクセス記録の取得

##### ■ ガイドラインとして必要な要求事項 Seq. 103

---

##### ⑥

情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。

##### ■ 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/>

##### 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

### -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](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/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録について、定期的なレビューを行い、不正なアクセス等がないことを組織的安全管理対策にて作成した「アクセス管理規程」に準じて確認する必要があります。

■ 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.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

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



### 3.2.3

#### 技術的安全管理対策

##### (Ⅰ) 1

#### アクセス記録の取得

##### ■ ガイドラインとして必要な要求事項 Seq. 104

---

⑦

⑥に関する情報の医療機関等への提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録についてに関する情報の医療機関等への提供について、サービス仕様適合開示書に基づき、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

#### 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.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

A.18 順守

A.18.2

---

### 3.2.3

#### 技術的安全管理対策

##### (工) 2

##### アクセス記録の保全のための要件

##### ■ ガイドラインとして必要な要求事項 Seq. 105

---

##### ①

アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する。

##### ■ 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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する必要があります。

クラウドサービス事業者は、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ことができます。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 ユーザー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](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](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

---



### 3.2.3

#### 技術的安全管理対策

##### (工) 2

##### アクセス記録の保全のための要件

##### ■ ガイドラインとして必要な要求事項 Seq. 106

---

##### ②

アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。

##### ■ 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](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/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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る必要があります。

クラウドサービス事業者は、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ことができます。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](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](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

---

### 3.2.3

#### 技術的安全管理対策

##### (工) 2

##### アクセス記録の保全のための要件

##### ■ ガイドラインとして必要な要求事項 Seq. 107

---

##### ③

アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。

##### ■ 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](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/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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる必要があります。

クラウドサービス事業者は、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ことができます。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](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](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

---

### 3.2.3

#### 技術的安全管理対策

##### (工) 3

##### 時刻の設定

##### ■ ガイドラインとして必要な要求事項 Seq. 108

---

###### ①

アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。

##### ■ 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/>

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う必要があります。

クラウドサービス事業者は、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](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

---

### 3.2.3

#### 技術的安全管理対策

##### (オ) 1

##### .端末表示からの漏洩対策

##### ■ ガイドラインとして必要な要求事項 Seq. 109

---

###### ①

サービスの運用・保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。

##### ■ 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](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/>

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はサービスの運用・保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める必要があります。

クラウドサービス事業者は、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、クラウドサービス事業者が ISO27001 規格に基づき、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

---

### 3.2.3

#### 技術的安全管理対策

##### (オ) 1

##### .端末表示からの漏洩対策

##### ■ ガイドラインとして必要な要求事項 Seq. 110

---

##### ②

サービスの運用・保守端末等を設置している区域は監視カメラ等により適切に監視を行う。

##### ■ 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となります。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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はサービスの運用・保守端末等を設置している区域は監視カメラ等により適切に監視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.12.7

A.16 情報セキュリティインシデント管理

A.16.1

---

### 3.2.3

#### (オ) 1

端末表示からの漏洩対策

■ ガイドラインとして必要な要求事項 Seq. 111

---

#### ③

医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ 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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、サービス仕様適合開示書に基づき、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)

N/A

---

---

### 3.2.3

#### 技術的安全管理対策

(オ) 1. 端末表示からの漏洩対策

#### ■ ガイドラインとして必要な要求事項 Seq. 112

---

④

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、利用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する、あるいは強制ログオフを行うことができるようにする。

#### ■ 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](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/>

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、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、利用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する、あるいは強制ログオフを行うことができるように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クラウドサービス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/awscloudtrail/latest/userguide/monitor-cloudtrail-log-files-with-cloudwatch-logs.html](http://docs.aws.amazon.com/ja_jp/awscloudtrail/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](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

### 3.2.3

#### 技術的安全管理対策

##### (オ) 1

##### .端末表示からの漏洩対策

##### ■ ガイドラインとして必要な要求事項 Seq. 113

---

##### ⑤

医療機関等における利用者端末への④の措置の具体的な適用について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等における利用者端末へのセッションの乗っ取りのリスクを低減するための具体的な措置の適用について、サービス仕様適合開示書に基づき、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)

N/A

---

---

### 3.2.3

#### 技術的安全管理対策

##### (カ) 1

##### ウイルスやマルウェア等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 114

---

##### ①

情報システムの構築に際しては、ウイルスやマルウェア等の混入が生じないようにするための手順を策定し、これに則って構築する。

##### ■ 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。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの構築に際し、ウイルスチェック機能等を使用するなどの、ウイルスやマルウェア等の混入が生じないようにするための手順を策定し、これに則って構築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

---

### 3.2.3

#### 技術的安全管理対策

##### (カ) 1

##### ウイルスやマルウェア等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 115

---

##### ②

ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新する。

##### ■ 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。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、ウイルス対策ソフトの運用法を定め、ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新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



### 3.2.3

#### 技術的安全管理対策

##### (カ) 1 ウイルスやマルウェア等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 116

---

##### ③

情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。

##### ■ 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。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う必要があります。

また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う必要があります。

AWS ヘネットワーク経由でプログラム等を送信するときは、事前に送信元でウイルスチェックを行う等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

### 3.2.3

#### 技術的安全管理対策

##### (カ) 1 ウイルスやマルウェア等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 117

---

#### ④

サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。

##### ■ 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。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はサービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに医療機関等に周知し、ネットワークの切断、医療基幹業務の代替運用等の必要な対応等を求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

---

### 3.2.3

#### 技術的安全管理対策

##### (カ) 1

##### ウイルスやマルウェア等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 118

---

##### ⑤

情報システムの脆弱性に関する情報は、JPCERT コーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。

##### ■ 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。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの脆弱性に関する情報を、JPCERT コーディネーションセンター

（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得するような計画を立て、常に最新の情報を確認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

### 3.2.3

#### 技術的安全管理対策

##### (カ) 2

#### 外部からの攻撃等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 119

---

###### ①

外部のネットワークと医療情報を格納する機器との接続に際しては、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。

##### ■ 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](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](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](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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、下記機能を利用して、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。

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。

■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (カ) 2

#### 外部からの攻撃等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 120

---

##### ②

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を検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。

##### ■ 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](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](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](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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、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を検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる必要があり、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。

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。

クラウドサービス事業者は、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

---

### 3.2.3

#### 技術的安全管理対策

##### (カ) 2

#### 外部からの攻撃等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 121

---

##### ③

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。

##### ■ 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](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](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](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/>

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は設置した 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

---

### 3.2.3

#### 技術的安全管理対策

##### (カ) 2

#### 外部からの攻撃等への対策

##### ■ ガイドラインとして必要な要求事項 Seq. 122

---

##### ④

ホスティングの利用時等、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。

##### ■ 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](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](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](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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、ホスティングの利用時等、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、同様の制御を行う必要があります。

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。

クラウドサービス事業者は、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

---

### 3.2.3

#### 技術的安全管理対策

(キ)

#### 応答時間に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 123

---

①

医療機関等がサービスを利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

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クを備えています。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。

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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等がサービスを利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、サービス仕様適合開示書に基づき、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

#### 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 1

##### 保存管理

##### ■ ガイドラインとして必要な要求事項 Seq. 124

---

##### ①

各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。

##### ■ AWS のインフラストラクチャー関連事項

N/A

Amazon S3 は、非常に優れた弾力性と拡張性を自動的に提供するように設計されています。多数のファイルをディレクトリに保存するときに問題が発生する標準のファイルシステムとは異なり、Amazon S3 がバケットでサポートするファイルの数に制限はありません。また、ドライブやサーバーにわたるデータをパーティションで区切るまでは保存できる総データ量に制限があるディスクドライブとは異なり、Amazon S3 バケットが保存できるバイト数は無制限です。オブジェクトをいくつでも保存でき、Amazon S3 は、情報の重複コピーの拡張と、同じリージョン内の他の場所にある他のサーバーへの分散を管理します。このすべてにおいて、Amazon の高パフォーマンスインフラストラクチャが使用されます。

##### ■ AWS サービス関連情報

##### -Amazon CloudWatch

Amazon CloudWatch は、AWS の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をモニタリングするサービスです。Amazon CloudWatch を使用して、メトリクスの収集と追跡、ログファイルの収集とモニタリング、アラームの設定、および AWS リソースへの変更に対する自動的な対応が可能です。Amazon CloudWatch は、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、およびアプリケーションやサービスに生成されたカスタムメトリクス、およびアプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、システム全体のリソース使用率、アプリケーションパフォーマンス、およびオペレーションの状態について可視性を得ることができます。これらの洞察を使用して対応し、アプリケーションのスムーズな動作を維持できます。

詳細、最新情報は下記を参照ください。

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

##### -Auto Scaling

Auto Scaling により、アプリケーションの可用性を維持できると同時に、お客様が定義する条件に応じて Amazon EC2 の能力を自動的に縮小あるいは拡張することができます。Auto Scaling を使用して、必要な数の Amazon EC2 インスタンスが確実に実行されている状態になります。また Auto Scaling によって、需要が急激に上昇したときには Amazon EC2 インスタンスの数を自動的に増やしてパフォーマンスを維持し、需要が落ち着いた状態にあるときには能力を縮小してコストを削減できます。Auto Scaling は、需要パターンが安定しているアプリケーションにも、利用量が

時間単位、日単位、週単位で変動するアプリケーションにも適しています。

詳細、最新情報は下記を参照ください。

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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、AWS サービスを利用するにあたり、左記に挙げた機能を活用し、各医療機関等が利用可能な、保存可能資源の残量を監視・拡張し、その情報を随時提供できるよう適切な設定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.12.2

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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 1

##### 保存管理

##### ■ ガイドラインとして必要な要求事項 Seq. 125

---

##### ②

医療機関等がサービスを利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等がサービスを利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、サービス仕様適合開示書に基づき、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.8 資産の管理

##### A.8.1

##### A.8.2

##### A.8.3

#### A.15 供給者関係

---



### 3.2.3

#### 技術的安全管理対策

##### (ク) 1

#### 保存管理

##### ■ ガイドラインとして必要な要求事項 Seq. 126

---

##### ③

情報システムが情報を保存する場所（内部、可搬媒体）、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等を含める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムが情報を保存するストレージや、各々の保存可能容量、保存可能期間、リスク等を運用管理規程等を含める必要があります。

##### ■ 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.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.15 供給者関係

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 1

##### 保存管理

##### ■ ガイドラインとして必要な要求事項 Seq. 127

---

##### ④

③において、他の事業者が提供するクラウドサービスを利用する場合においても、同様の情報を収集して、対応する。仮想化技術によるクラウドサービスを利用する場合には、クラウドサービス事業者が他の事業者との契約上利用可能な資源に関する情報を確認する。

##### ■ AWS のインフラストラクチャー関連事項

N/A

Amazon S3 は、非常に優れた弾力性と拡張性を自動的に提供するように設計されています。多数のファイルをディレクトリに保存するときに問題が発生する標準のファイルシステムとは異なり、Amazon S3 がバケットでサポートするファイルの数に制限はありません。また、ドライブやサーバーにわたるデータをパーティションで区切るまでは保存できる総データ量に制限があるディスクドライブとは異なり、Amazon S3 バケットが保存できるバイト数は無制限です。オブジェクトをいくつでも保存でき、Amazon S3 は、情報の重複コピーの拡張と、同じリージョン内の他の場所にある他のサーバーへの分散を管理します。このすべてにおいて、Amazon の高パフォーマンスインフラストラクチャが使用されます。

##### ■ AWS サービス関連情報

##### -Amazon CloudWatch

Amazon CloudWatch は、AWS の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をモニタリングするサービスです。Amazon CloudWatch を使用して、メトリクスの収集と追跡、ログファイルの収集とモニタリング、アラームの設定、および AWS リソースへの変更に対する自動的な対応が可能です。Amazon CloudWatch は、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、およびアプリケーションやサービスに生成されたカスタムメトリクス、およびアプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、システム全体のリソース使用率、アプリケーションパフォーマンス、およびオペレーションの状態について可視性を得ることができます。これらの洞察を使用して対応し、アプリケーションのスムーズな動作を維持できます。

詳細、最新情報は下記を参照ください。

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

##### -Auto Scaling

Auto Scaling により、アプリケーションの可用性を維持できると同時に、お客様が定義する条件に応じて Amazon EC2 の能力を自動的に縮小あるいは拡張することができます。Auto Scaling を使用して、必要な数の Amazon EC2 インスタンスが確実に実行されている状態になります。また Auto Scaling によって、需要が急激に上昇したときに

は Amazon EC2 インスタンスの数を自動的に増やしてパフォーマンスを維持し、需要が落ち着いた状態にあるときには能力を縮小してコストを削減できます。Auto Scaling は、需要パターンが安定しているアプリケーションにも、利用量が時間単位、日単位、週単位で変動するアプリケーションにも適しています。

詳細、最新情報は下記を参照ください。

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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.3「技術的安全管理対策」（ク）1③において示した運用管理規程について、AWS サービスを利用する場合においても記載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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 1 保存管理

##### ■ ガイドラインとして必要な要求事項 Seq. 128

---

⑤

③により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.3「技術的安全管理対策」（ク）1③において示した運用管理規程に定める管理方法に関する教育を、従業員等に対して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.7 人的資源のセキュリティ

##### A.7.2

#### A.18 順守

##### A.18.1

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 1

##### 保存管理

##### ■ ガイドラインとして必要な要求事項 Seq. 129

---

##### ⑥

サービスに係る委託先に対しても、③の運用管理規程に定める管理方法への対応等を求める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.3「技術的安全管理対策」（ク）1③において示した運用管理規程に定める管理方法に関する教育をサービスに係る委託先に対して行い、管理方法に準じた対応を徹底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.7 人的資源のセキュリティ

##### A.7.2

#### A.18 順守

##### A.18.1

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 2

#### バックアップルール

##### ■ ガイドラインとして必要な要求事項 Seq. 130

---

##### ①

3. 2. 1 (2) (ウ) 4. ①において実施するリスク分析結果に基づき情報システムのバックアップを取得する。バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、その内容を運用管理規程等に含める。

##### ■ AWS のインフラストラクチャー関連事項

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を使用してテープへのバックアップを実行することが可能です。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 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。

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に対して 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、最新情報は下記ホワイトペーパーを参照ください。

「主要なコンプライアンス に関する質問と AWS の回答」

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/AWS\\_Answers\\_to\\_Key\\_Compliance\\_Questions\\_JP.pdf](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

#### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。



## データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点に、すばやく簡単に復元できます。

## オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョンングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョンングによって、意図的なユーザーアクションやアプリケーション障害から簡単に復旧できます。

## ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

## アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額な専用ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれがあります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.1「組織的安全管理対策」(2)(ウ)4.①で定めた、サービスのリスク分析並びに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リスク分析・リスク対応した結果を踏まえ、バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、その内容を運用管理規程等に含める必要があります。

■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 2

##### バックアップルール

##### ■ ガイドラインとして必要な要求事項 Seq. 131

---

##### ②

①に従い取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改ざん・破壊等がないことを確認する。

##### ■ AWS のインフラストラクチャー関連事項

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を使用してテープへのバックアップを実行することが可能です。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 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。

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に対して 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、最新情報は下記ホワイトペーパーを参照ください。

「主要なコンプライアンス に関する質問と AWS の回答」

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/AWS\\_Answers\\_to\\_Key\\_Compliance\\_Questions\\_JP.pdf](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

##### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。

## データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点に、すばやく簡単に復元できます。

## オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョンングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョンングによって、意図的なユーザーアクションやアプリケーション障害から簡単に復旧できます。

## ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

## アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額な専用ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれがあります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、AWS サービスを利用するにあたり、3.2.3「技術的安全管理対策」(ク) 2①に準じ取得したバックアップについて、バックアップログや記録内容を定期的に検査し、記録内容の改ざん・破壊等がないこと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.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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 2 バックアップルール

##### ■ ガイドラインとして必要な要求事項 Seq. 132

---

##### ③

記録媒体に格納するバックアップについては、その媒体の特性（テープ／ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。

##### ■ AWS のインフラストラクチャー関連事項

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を使用してテープへのバックアップを実行することが可能です。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 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。

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に対して 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、最新情報は下記ホワイトペーパーを参照ください。

「主要なコンプライアンス に関する質問と AWS の回答」

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/AWS\\_Answers\\_to\\_Key\\_Compliance\\_Questions\\_JP.pdf](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

##### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。



## データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点に、すばやく簡単に復元できます。

## オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョンングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョンングによって、意図的なユーザーアクションやアプリケーション障害から簡単に復旧できます。

## ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

## アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額な専用ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれがあります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、AWS サービスを利用するにあたり、各バックアップの取得内容、使用開始日、使用終了日を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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 2

#### バックアップルール

##### ■ ガイドラインとして必要な要求事項 Seq. 133

---

##### ④

③の対象となるバックアップの記録媒体につき、使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。

##### ■ AWS のインフラストラクチャー関連事項

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を使用してテープへのバックアップを実行することが可能です。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 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。

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に対して 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、最新情報は下記ホワイトペーパーを参照ください。

「主要なコンプライアンス に関する質問と AWS の回答」

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/AWS\\_Answers\\_to\\_Key\\_Compliance\\_Questions\\_JP.pdf](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

#### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。

## データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点に、すばやく簡単に復元できます。

## オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョンングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョンングによって、意図的なユーザーアクションやアプリケーション障害から簡単に復旧できます。

## ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

## アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額な専用ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれがあります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.3「技術的安全管理対策」(ク) 2③の対象となるバックアップの記録媒体につき、使用終了日が近づいた場合には、終了日以前に、別のバックアップ取得設定を作成する等の対応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.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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 2

#### バックアップルール

##### ■ ガイドラインとして必要な要求事項 Seq. 134

---

##### ⑤

①～④の手順を運用管理規程等を含め、従業員等及び再委託業者に対して必要な教育を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、バックアップの手順を運用管理規程等を含め、従業員等及び再委託業者に対して必要な教育を行います。

##### ■ 推奨される追加の実施事項

N/A

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

#### A.7 人的資源のセキュリティ

---



### 3.2.3

#### 技術的安全管理対策

##### (ク) 2 バックアップルール

##### ■ ガイドラインとして必要な要求事項 Seq. 135

---

##### ⑥

バックアップに係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、バックアップに係る情報の提供について、サービス仕様適合開示書に基づき、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.7 人的資源のセキュリティ

#### A.15 供給者関係

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 3 冗長化措置

##### ■ ガイドラインとして必要な要求事項 Seq. 136

---

###### ①

情報システム、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。

##### ■ 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

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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策として、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等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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 3

##### 冗長化措置

##### ■ ガイドラインとして必要な要求事項 Seq. 137

---

##### ②

診療録等の情報をハードディスク等の記録機器に保存する場合、RAID-1 又は RAID-6 相当以上のディスク障害対策を講じる。

##### ■ 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

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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策として、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等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

---

### 3.2.3

#### 技術的安全管理対策

##### (ク) 3

#### 冗長化措置

##### ■ ガイドラインとして必要な要求事項 Seq. 138

---

##### ③

①を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.3「技術的安全管理対策」（ク）3①における対策を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、サービス仕様適合開示書に基づき、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

#### 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

### 3.2.3

#### 技術的安全管理対策

##### (ク) 3

#### 冗長化措置

##### ■ ガイドラインとして必要な要求事項 Seq. 139

---

#### ④

障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、サービス仕様適合開示書に基づき、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

#### 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

### 3.2.3

#### 技術的安全管理対策

##### (ク) 4

##### 毀損した情報の取扱い

##### ■ ガイドラインとして必要な要求事項 Seq. 140

---

###### ①

情報が毀損した場合、速やかに回復するための措置を講じ、その内容・手順等について、運用管理規程等に含める。

##### ■ AWS のインフラストラクチャー関連事項

N/A

##### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。

##### データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点に、すばやく簡単に復元できます。

##### オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョニングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョニングによって、意図的なユーザーアクションやアプリケーション障害から簡単に復旧できます。

## ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

## アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額の特許ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれがあります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

### ■ AWS サービス関連情報

N/A

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報が毀損した場合、速やかに回復するためにバックアップからの復旧手順策定等の措置を講じ、それを運用管理規程等に含める必要があります。

### ■ 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



### 3.2.3

#### 技術的安全管理対策

##### (ク) 4

##### 毀損した情報の取扱い

##### ■ ガイドラインとして必要な要求事項 Seq. 141

---

##### ②

①に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。

##### ■ AWS のインフラストラクチャー関連事項

N/A

##### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。

##### データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点で、すばやく簡単に復元できます。

##### オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョンングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョンングによって、意図的なユーザーアクシ

ョンやアプリケーション障害から簡単に復旧できます。

## ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

## アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額の専用ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれがあります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

### ■ AWS サービス関連情報

N/A

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.3「技術的安全管理対策」（ク）4①における措置によっても毀損された情報の回復が困難となる場合の医療機関等との取り決め等について、運用管理規程等に含める必要があります。

### ■ 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



### 3.2.3

#### 技術的安全管理対策

##### (ク) 4

##### 毀損した情報の取扱い

##### ■ ガイドラインとして必要な要求事項 Seq. 142

---

##### ③

②で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

N/A

##### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。

##### データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点で、すばやく簡単に復元できます。

##### オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョニングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョニングによって、意図的なユーザーアクシ

ョンやアプリケーション障害から簡単に復旧できます。

## ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

## アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額な専用ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれがあります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

### ■ AWS サービス関連情報

N/A

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.3「技術的安全管理対策」（ク）4②に記載される、毀損された情報の回復が困難となる場合において、毀損した情報に関する責任の範囲、免責条件等について、サービス仕様適合開示書に基づき、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

#### 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





### 3.2.3

#### 技術的安全管理対策

##### (ク) 5 保存データの見読性確保

##### ■ ガイドラインとして必要な要求事項 Seq. 143

---

###### ①

医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。

##### ■ 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となります。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。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-layer/>

## ■ AWS サービス関連情報

### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。

### データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点に、すばやく簡単に復元できます。

### オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョンングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョンングによって、意図的なユーザーアクションやアプリケーション障害から簡単に復旧できます。

### ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

### アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額な専用ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれが

あります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、AWS サービスを利用するにあたり、医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認するために、データバックアップのログや取得内容について確認する等の施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.5.1.1

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

### 3.2.3

#### 技術的安全管理対策

##### (ク) 5

#### 保存データの見読性確保

##### ■ ガイドラインとして必要な要求事項 Seq. 144

---

##### ②

受託する医療情報を格納する機器・媒体等の見読性確保が困難となる可能性がある場合（媒体の劣化、読取装置等のサポート切れ等）、速やかに代替的な措置を講じ、見読性確保のための対応を行う。

##### ■ 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となります。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。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/compliance/data-center/data-layer/>

## ■ AWS サービス関連情報

### スナップショットベースのデータバックアップ

Amazon EBS には、Amazon EC2 で使用する永続的なブロックストレージボリュームのみでなく、バックアップ機能もあります。Amazon EBS では、EBS ボリュームのスナップショット（バックアップ）を作成できます。その後、このスナップショットは Amazon S3 に保存されます。また、安全性と冗長性を確保するために、複数のアベイラビリティゾーンに保存されます。スナップショットは増分バックアップです。つまり、最後にスナップショットを作成した時点から、ボリューム上で変更のあるブロックだけが保存されます。これにより、スナップショットの保存にかかる時間とコストを最小限に抑えることができます。また、EBS スナップショットを使用して大規模なデータベースもバックアップできます（特に、24 時間年中無休で実行する必要があるデータベースに使用できます）。

### データベースのバックアップ

Amazon Relational Database Service (Amazon RDS) を使用すると、クラウド内でリレーショナルデータベースを簡単に設定、運用、スケールできます。Amazon RDS はコスト効率、柔軟性、スケーラビリティに優れており、データベースインスタンスのストレージボリュームスナップショットの自動作成に使用できます。ストレージボリューム全体にすべてのファイルが含まれるため、これらのスナップショットにより（個々のデータベースのみでなく）データベースインスタンス全体がバックアップされます。つまり、データベースをバックアップ保持期間中の任意の時点で、すばやく簡単に復元できます。

### オブジェクトストレージ

AWS のオブジェクトストレージサービスの Amazon S3 と Amazon Glacier では、他に類を見ない耐久性、可用性、スケーラビリティ、セキュリティが実現します。あらゆる業界のトップ企業が、自社で使用する多数のアプリケーションのデータの保存に AWS を使用しているのはこのためです。同じ理由により、AWS はバックアップ先としても理想的です。Amazon S3 では、非常に柔軟なストレージ管理機能を使用して、データのライフサイクルルールを定義できます。たとえば、頻繁にアクセスしないデータを S3 標準 - 低頻度アクセスクラスや S3 One Zone-Infrequent Access クラスに自動的に移行することや、データセットを Amazon Glacier にアーカイブすることができます。また、AWS オブジェクトストレージはバージョニングにも対応しているため、Amazon S3 バケットに保存したことがあるすべてのオブジェクトのすべてのバージョンについて、保存、取り出し、復元を行うことができます。このバージョニングによって、意図的なユーザーアクションやアプリケーション障害から簡単に復旧できます。

### ファイルストレージ

Amazon EFS は高い可用性と耐久性を備えたファイルストレージサービスで、簡単にデプロイできるファイルシステムバックアップ機能もあります。Amazon EFS を使用すると、Amazon EFS のあるファイルシステム（ソースファイルシステム）から別のファイルシステム（バックアップファイルシステム）にデータを自動的にコピーできます。また、オンプレミスのファイルシステムを AWS クラウドに直接バックアップすることもできます。バックアップのスケジュールを定義して、Amazon CloudWatch や AWS Lambda といったサービスに自動的にデプロイすることもできます。

### アーカイブストレージとコールドストレージ

企業では、内部統制または規制コンプライアンスの要件を満たすためにデータを長期間保持することが要求されています。従来、これには高額な専用ハードウェアが必要で、データボリュームが増えるにつれてストレージコストも急増するおそれがあります。AWS では、長期的なアーカイブ機能を構築するために必要なストレージサービスを利用できます。このサービスによって、費用対効果の高い方法で、数年または数十年データを保存およびバックアップできます。また、AWS のライフサイクルポリシーは自動化できるため、データを Amazon S3 から Amazon Glacier に簡単に移行できます。Amazon Glacier Vault Lock は、Write Once Read Many (WORM) ストレージを提供し、記録保持期間のコンプライアンス要件に対応するものです。

詳細、最新情報は下記を参照ください。

<https://aws.amazon.com/jp/backup-restore/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、AWS サービスを利用するにあたり、受託する医療情報を格納する機器・媒体等の見読性確保が困難となる可能性がある場合、速やかに代替的な措置を講じ、見読性確保のための対応を行うために、複数バックアップの取得やバックアップからの復旧手順の策定等の施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.5.1.1

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



### 3.2.3

#### 技術的安全管理対策

##### (ケ) 1

#### 情報システムに関するドキュメント作成

##### ■ ガイドラインとして必要な要求事項 Seq. 145

---

##### ①

情報システムにおける機器及びソフトウェアの構成図を作成する。

##### ■ AWS のインフラストラクチャー関連事項

N/A

##### 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](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/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムに関する以下のドキュメントを作成する必要があります。

・機器及びソフトウェア構成図

■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ケ) 1

##### 情報システムに関するドキュメント作成

##### ■ ガイドラインとして必要な要求事項 Seq. 146

---

##### ②

情報システムのネットワーク構成図を作成する。

##### ■ AWS のインフラストラクチャー関連事項

N/A

##### 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](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/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムに関する以下のドキュメントを作成する必要があります。

・ネットワーク構成図

■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ケ) 1

##### 情報システムに関するドキュメント作成

##### ■ ガイドラインとして必要な要求事項 Seq. 147

---

##### ③

①、②で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。

##### ■ AWS のインフラストラクチャー関連事項

N/A

##### 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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムに関し作成した以下のドキュメントについて、システム要件等の説明を追加した資料を作成する必要があります。

- ・機器及びソフトウェア構成図
- ・ネットワーク構成図

#### ■ 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

### 3.2.3

#### 技術的安全管理対策

##### (ケ) 1

#### 情報システムに関するドキュメント作成

##### ■ ガイドラインとして必要な要求事項 Seq. 148

---

##### ④

情報システムを構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。

##### ■ AWS のインフラストラクチャー関連事項

N/A

##### 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、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](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/>

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムに関する以下のドキュメントを作成する必要があります。

- ・情報システムを構成する機器及びソフトウェア等の更新の仕様等に関する資料
- ・上記資料の更新履歴

■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (ケ) 1

#### 情報システムに関するドキュメント作成

##### ■ ガイドラインとして必要な要求事項 Seq. 149

---

##### ⑤

①～④で策定した資料等を医療機関等の求めに応じて提出することについて、サービス仕様適合開示書に基づき、開示内容、範囲、条件等を医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムにおける機器及びソフトウェア、ネットワークの構成図等を、医療機関等の求めに応じて提出することについて、サービス仕様適合開示書に基づき、開示内容、範囲、条件等を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)

N/A

---

---

### 3.2.3

#### 技術的安全管理対策

##### (ケ) 2

#### 品質管理に関する運用

##### ■ ガイドラインとして必要な要求事項 Seq. 150

---

###### ①

サービスに供する機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等を含める。

##### ■ 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、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。

###### 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。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

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

##### -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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに供する機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める必要があります。



また品質管理に関する施策として、対象をクラウドサービス事業者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、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。

詳細については以下をご参照下さい。

<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](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](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

### 3.2.3

#### 技術的安全管理対策

##### (ケ) 2

#### 品質管理に関する運用

##### ■ ガイドラインとして必要な要求事項 Seq. 151

---

##### ②

サービスに供する機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。

##### ■ 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。

##### 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出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。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

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、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。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。

詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/systems-manager/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに供する機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う必要があります。

#### ■ 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](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](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

### 3.2.3

#### 技術的安全管理対策

##### (ケ) 2

#### 品質管理に関する運用

##### ■ ガイドラインとして必要な要求事項 Seq. 152

---

##### ③

サービスに係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。

##### ■ 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。

##### 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出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。

<https://aws.amazon.com/jp/compliance/data-center/data-centers/>

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、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。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。

詳細は以下 URL を参照ください。

<https://aws.amazon.com/jp/systems-manager/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに係る委託先に対しても、事業者が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める必要があります。

#### ■ 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](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](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

### 3.2.3

#### 技術的安全管理対策

##### (ケ) 2 品質管理に関する運用

##### ■ ガイドラインとして必要な要求事項 Seq. 153

---

##### ④

システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等を含める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等を含める必要があります。

##### ■ 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.18 順守

A.18.2

---

### 3.2.3

#### 技術的安全管理対策

##### (コ) 1

#### 医療機関等における無線 LAN の利用

##### ■ ガイドラインとして必要な要求事項 Seq. 154

---

##### ①

医療情報を取り扱うサービスの利用に際して、医療機関等が無線 LAN を利用する場合に必要なセキュリティ対策について、クラウドサービス事業者の役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

医療情報を取り扱うサービスの利用に際して、医療機関等が無線 LAN を利用する場合に必要なセキュリティ対策について、クラウドサービス事業者の役割分担等について、サービス仕様適合開示書に基づき、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.15 供給者関係

##### A.15.1.2

---

### 3.2.3

#### 技術的安全管理対策

##### (コ) 2

#### IoT 機器を利用したサービス提供時

##### ■ ガイドラインとして必要な要求事項 Seq. 155

---

##### ①

IoT 機器の利用を含むサービスを提供する場合、医療機関等との責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

IoT 機器の利用を含むサービスを提供する場合、医療機関等との責任分界について、サービス仕様適合開示書に基づき、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.15 供給者関係

##### A.15.1.2

---

### 3.2.3

#### 技術的安全管理対策

##### (コ) 2IoT 機器を利用したサービス提供時

##### ■ ガイドラインとして必要な要求事項 Seq. 156

---

##### ②

IoT 機器の利用を含むサービスを提供する場合、IoT 機器による医療情報システムへのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する。

##### ■ 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

##### -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](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](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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はIoT 機器の利用を含むサービスを提供する場合、IoT 機器による医療情報システムへのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する必要があります。

IoT 機器との接続ネットワーク境界に、侵入検知システム（IDS）、侵入防止システム（IPS）を導入してネットワーク上の不正なイベントを検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる場合は下記の対応が必要です。

- ・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
- ・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

#### ■ 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

---

### 3.2.3

#### 技術的安全管理対策

##### (コ) 2IoT 機器を利用したサービス提供時

##### ■ ガイドラインとして必要な要求事項 Seq. 157

---

##### ③

IoT 機器の利用を含むサービスを提供する場合、利用が想定される IoT 機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる。

##### ■ 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/>

##### -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>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、IoT 機器の利用を含むサービスを提供する場合、利用が想定される IoT 機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる必要があります。

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

### A14.2

## A.16 情報セキュリティインシデント管理

### A.16.1

---

### 3.2.4

#### 人的安全管理対策

##### (ア) 1 就業開始時における対応

##### ■ ガイドラインとして必要な要求事項 Seq. 158

---

###### ①

サービスの提供に従事する要員（被用者、派遣従業者等）については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等に含める。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス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。

クラウドサービス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。

クラウドサービス事業者と 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.18 順守

### A.18.2

---



### 3.2.4

#### 人的安全管理対策

##### (ア) 2 就業時における教育等

##### ■ ガイドラインとして必要な要求事項 Seq. 159

---

###### ①

サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育・訓練を行う。

##### ■ 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の実施しています。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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は職員・派遣従業員に対し情報セキュリティ教育（個人情報保護に関する教育を含む）を行い定期的に見直しを行う責任があります。

教育内容には、以下を含みます。

- 退職時又は契約終了時以降の守秘義務

##### ■ 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.7.2

#### A.18 順守

##### A.18.2



### 3.2.4

#### 人的安全管理対策

##### (ア) 2

#### 就業時における教育等

##### ■ ガイドラインとして必要な要求事項 Seq. 160

---

##### ②

この教育・訓練は就業開始時及び就業後定期的に行う。

##### ■ 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の実施しています。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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は職員・派遣従業員に対し情報セキュリティ教育（個人情報保護に関する教育を含む）を行い定期的に見直しを行う責任があります。

教育内容には、以下を含みます。

- 退職時又は契約終了時以降の守秘義務

##### ■ 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.7.2

### 3.2.4

#### 人的安全管理対策

##### (ア) 3

##### .退職後の守秘義務等

##### ■ ガイドラインとして必要な要求事項 Seq. 161

---

##### ①

サービスの提供に従事する要員が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。

##### ■ 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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、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

#### ■ 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.7.2

A.7.3

A.18 順守

A.18.2

---

### 3.2.4

#### 人的安全管理対策

##### (ア) 3

##### .退職後の守秘義務等

##### ■ ガイドラインとして必要な要求事項 Seq. 162

---

##### ②

サービスの提供に従事する要員が業務上管理していた個人情報については、離職時（内部の異動含む）に返却を求め、システム管理者が返却されたことを確認する。

##### ■ 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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、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

#### ■ 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.7.2

A.7.3

A.18 順守

A.18.2

---

### 3.2.4

#### 人的安全管理対策

##### (ア) 3.退職後の守秘義務等

##### ■ ガイドラインとして必要な要求事項 Seq. 163

---

##### ③

サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、上記 2.における教育・訓練に含める。

##### ■ 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](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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は職員・派遣従業員に対し情報セキュリティ教育（個人情報保護に関する教育を含む）を行い定期的に見直しを行う責任があります。

教育内容には、以下を含みます。

- 退職時又は契約終了時以降の守秘義務

#### ■ 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.7.2

### A.7.3

## A.18 順守

### A.18.2

---

### 3.2.4

#### 人的安全管理対策

##### (ア) 4

#### 守秘義務違反者への対応措置

##### ■ ガイドラインとして必要な要求事項 Seq. 164

---

##### ①

上記 1.～3.に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。

##### ■ 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

##### ■ クラウドサービス事業者（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。

機密情報管理に関する規定では、守秘義務違反時のペナルティについて、定める必要があります。

##### ■ 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.18 順守

##### A.18.2

---

### 3.2.4

#### 人的安全管理対策

(ア) 5 従業者等への教育状況・守秘義務等の状況

#### ■ ガイドラインとして必要な要求事項 Seq. 165

---

##### ①

サービスの提供に従事する要員に対する教育・訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

#### ■ 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。

<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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、クラウドサービス（AWS）を利用したサービスの提供に従事する要員に対する教育・訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供について、サービス仕様適合開示書に基づき、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

#### A.7 人的資源のセキュリティ

##### A.7.1

A.7.2

A.7.3

A.15 供給者関係

A.15.1

A.15.2

A.18 順守

A.18.2

---

### 3.2.4

#### 人的安全管理対策

##### (イ) 1 委託契約に含めるべき事項

##### ■ ガイドラインとして必要な要求事項 Seq. 166

---

###### ①

情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、当該再委託に係る契約において体制を明確にする。

##### ■ 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

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

N/A

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、当該再委託に係る契約において体制を明確にする必要があります

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/>

そのうえで、AWS インフラストラクチャーの利用について事前に医療機関などの管理者に説明を行い、体制を明確に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.15 供給者関係

A.15.1

A.15.2

A.18 順守

A.18.1

---

### 3.2.4

#### 人的安全管理対策

##### (イ) 1

##### 委託契約に含めるべき事項

##### ■ ガイドラインとして必要な要求事項 Seq. 167

---

##### ②

再委託先には、自社と同等の個人情報保護指針等を遵守させる。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、再委託先には、自社と同等の個人情報保護指針等を遵守させる必要があります。

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。  
クラウドサービス事業者はデータの統制と所有権を有しており、個人情報の保護はクラウドサービス事業者の責任です。

##### ■ 推奨される追加の実施事項

インフラストラクチャーの委託先である AWS が個人情報にアクセスできないことをみずから担保するために、データを暗号化することを推奨します。

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

##### A.15 供給者関係

##### A.15.1

##### A.15.2

##### A.18 順守

##### A.18.1

---



### 3.2.4

#### 人的安全管理対策

##### (イ) 1 委託契約に含めるべき事項

##### ■ ガイドラインとして必要な要求事項 Seq. 168

---

##### ③

再委託に係る契約に、委託業務に係る守秘義務を含める。

##### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はデータの統制と所有権を有していますので、クラウドサービス事業者は、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。

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

また、必要に応じ守秘義務契約を結ぶ必要がある場合は、営業担当者へご相談ください。

#### ■ 推奨される追加の実施事項

N/A

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



### 3.2.4

#### 人的安全管理対策

##### (イ) 1

##### 委託契約に含めるべき事項

##### ■ ガイドラインとして必要な要求事項 Seq. 169

---

##### ④

再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。

##### ■ 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。

<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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はデータの統制と所有権を有していますので、クラウドサービス事業者は、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。

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

また、必要に応じ守秘義務契約を結ぶ必要がある場合は、営業担当者へご相談ください。

#### ■ 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.15 供給者関係

##### A.15.1

A.15.2

A.18 順守

A.18.1

---

### 3.2.4

#### 人的安全管理対策

##### (イ) 1 委託契約に含めるべき事項

##### ■ ガイドラインとして必要な要求事項 Seq. 170

---

##### ⑤

再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。

##### ■ 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](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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する必要があります。

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ご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、クラウドサービス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](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/>

クラウドサービス事業者は、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/>

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クラウドサービス事業者の業務です。

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あります。) クラウドサービス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.15 供給者関係

A.15.1

A.15.2

A.18 順守

---

### 3.2.5

#### 情報の破棄に関する安全管理対策

##### (ア) 1

#### 情報の破棄の保証

##### ■ ガイドラインとして必要な要求事項 Seq. 171

---

##### ①

サービスに供する情報を格納する機器、媒体等を破棄する手順に、不可逆的な破壊・抹消等により元のデータを復元できなくする措置を含める。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける 利用者の責任範囲において、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。

① 情報を格納する機器、媒体等の破棄は AWS の責任範囲において下記の不可逆的措置が為されます。

##### 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。

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。

詳細は、「CSA Consensus Assessments Initiative Questionnaire (2017 年 5 月)」ホワイトペーパーを参照ください。

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/CSA\\_Consensus\\_Assessments\\_Initiative\\_Questionnaire\\_JP.pdf](https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/CSA_Consensus_Assessments_Initiative_Questionnaire_JP.pdf)

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、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

クラウドサービス事業者自身で 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](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.10 暗号

## A.12 運用のセキュリティ

---

### 3.2.5

#### 情報の破棄に関する安全管理対策

##### (ア) 1

#### 情報の破棄の保証

##### ■ ガイドラインとして必要な要求事項 Seq. 172

---

##### ②

情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法（電磁記録媒体の消磁・物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける 利用者の責任範囲において、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。

① 情報を格納する機器、媒体等の破棄は AWS の責任範囲において下記の不可逆的措置が為されます。

##### 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

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。

詳細は、「CSA Consensus Assessments Initiative Questionnaire (2017 年 5 月)」ホワイトペーパーを参照ください。

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/CSA\\_Consensus\\_Assessments\\_Initiative\\_Questionnaire\\_JP.pdf](https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/CSA_Consensus_Assessments_Initiative_Questionnaire_JP.pdf)

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報の破棄を実施した場合、破棄の実施担当者及び情報の削除方法を医療機関等に報告、廃棄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

クラウドサービス事業者自身で 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](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.10 暗号

### A.12 運用のセキュリティ

### A.15 供給者関係

---



### 3.2.5

#### 情報の破棄に関する安全管理対策

##### (ア) 1

#### 情報の破棄の保証

##### ■ ガイドラインとして必要な要求事項 Seq. 173

---

##### ③

①で講じる措置及び②の資料を提供するのに必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける 利用者の責任範囲において、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。

① 情報を格納する機器、媒体等の破棄は AWS の責任範囲において下記の不可逆的措置が為されます。

##### 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

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。

詳細は、「CSA Consensus Assessments Initiative Questionnaire (2017 年 5 月)」ホワイトペーパーを参照ください。

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/CSA\\_Consensus\\_Assessments\\_Initiative\\_Questionnaire\\_JP.pdf](https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/CSA_Consensus_Assessments_Initiative_Questionnaire_JP.pdf)

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.5「情報の破棄に関する安全管理対策」(ア) 1①で講じる措置及び(ア) 1②の資料を提供するのに必要な条件等について、サービス仕様適合開示書に基づき、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

クラウドサービス事業者自身で 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](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.10 暗号

### A.12 運用のセキュリティ

### A.15 供給者関係

---

### 3.2.5

#### 情報の破棄に関する安全管理対策

##### (ア) 2

#### 情報破棄手順の文書化

##### ■ ガイドラインとして必要な要求事項 Seq. 174

---

##### ①

##### ① 運用管理規定に以下の内容を定める。

- ・管理する個人情報又はこれを格納する媒体等について、サービス提供上の要否の確認を定期的に行うこと。
- ・サービス提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。
- ・サービス提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置（事前に破棄の基準等を告知する等）。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける 利用者の責任範囲において、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。

情報破棄手順の文書化及び医療機関との合意は、情報処理事業者（お客様）の責任において実施してください。

##### 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。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

##### - クラウドサービス事業者内の体制及び責任者の任命・解任等のルール

- ・管理する個人情報又はこれを格納する媒体等について定期的な棚卸し
- ・不要な個人情報及びこれを格納する媒体についての破棄手順

・廃棄手順通り実施の際、医療機関等が不測の損害を被らないようにするための措置（事前に破棄の基準等を告知する等）

■ 推奨される追加の実施事項

クラウドサービス事業者自身で 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](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.10 暗号

A.12 運用のセキュリティ

A.15 供給者関係

A.15.2.1

A.15.2.2

### 3.2.5

#### 情報の破棄に関する安全管理対策

##### (ア) 2

#### 情報破棄手順の文書化

##### ■ ガイドラインとして必要な要求事項 Seq. 175

---

##### ②

② 情報の破棄手順について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける 利用者の責任範囲において、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。

情報破棄手順の文書化及び医療機関との合意は、情報処理事業者（お客様）の責任において実施してください。

#### 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。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報破棄手順を文書化し、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

クラウドサービス事業者自身で 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](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.10 暗号

A.12 運用のセキュリティ

A.15 供給者関係

A.15.2.1

A.15.2.2

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (ア) 1

##### 保守用のアカウント

##### ■ ガイドラインとして必要な要求事項 Seq. 176

---

##### ①

情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で当該情報システムにアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲（AWS のインフラストラクチャー）において、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 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。

##### ■ 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。

詳細は「アマゾン ウェブ サービス：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://aws.amazon.com/jp/whitepapers/overview-of-security-processes/>

##### ■ AWS サービス関連情報

AWS 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します。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 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、アクセスした個人の特定をはじめ!継続的な監査対策を可能にします。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で当該情報システムにアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う必要があります。

AWS 責任共有モデルにおける AWS 責任範囲において、EC2 群の OS よりも下位のレイヤにアップグレードの適用を行なっています。

そのため、まれに「メンテナンスのために EC2 インスタンスが再起動されます。」という通知が届きます。

通知は、登録された AWS 管理者あてにメール（英文）が届き、かつ AWS Management Console で確認ができます。

再起動にかかる時間は数分程度ですが、サービス停止回避のため、指定のメンテナンス期間より前の任意の時間で再起動を行う必要があります。

AWS 責任共有モデルにおける利用者責任範囲において、情報システムの保守にかかわるアクセス権限やアクセス制限を定め、運用する必要があります。

AWS 利用者のアクティビティを記録したログ情報を元に、計画的な監査対応が求められます。

#### ■ 推奨される追加の実施事項

IAM では、AWS に対する、一時的な認証情報を作成する仕組み Temporary Security Credentials も提供されています。

これは、期限付きの認証情報（認証チケット）

であり、情報システムの保守業務のような一時的アクセスの際にご検討ください。

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

##### A.9 アクセス制御

##### A.9.1

##### A.9.2



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (ア) 1

##### 保守用のアカウント

##### ■ ガイドラインとして必要な要求事項 Seq. 177

---

##### ②

①で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲（AWS のインフラストラクチャー）において、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 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。

##### ■ 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。

詳細は「アマゾン ウェブ サービス：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://aws.amazon.com/jp/whitepapers/overview-of-security-processes/>

##### ■ AWS サービス関連情報

AWS 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します。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 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、アクセスした個人の特定をはじめ継続的な監査対策を可能にします。

## ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.6「情報システムの改造と保守に関する安全管理対策」（ア）1①で定めたアカウントで実施した作業記録を、ログ等により記録、保持する必要があります。

AWS 責任共有モデルにおける AWS 責任範囲において、EC2 群の OS よりも下位のレイヤにアップグレードの適用を行なっています。

そのため、まれに「メンテナンスのために EC2 インスタンスが再起動されます。」という通知が届きます。

通知は、登録された AWS 管理者あてにメール（英文）が届き、かつ AWS Management Console で確認ができます。

再起動にかかる時間は数分程度ですが、サービス停止回避のため、指定のメンテナンス期間より前の任意の時間で再起動を行う必要があります。

AWS 責任共有モデルにおける利用者責任範囲において、情報システムの保守にかかわるアクセス権限やアクセス制限を定め、運用する必要があります。

AWS 利用者のアクティビティを記録したログ情報を元に、計画的な監査対応が求められます。

## ■ 推奨される追加の実施事項

IAM では、AWS に対する、一時的な認証情報を作成する仕組み Temporary Security Credentials も提供されています。

これは、期限付きの認証情報（認証チケット）

であり、情報システムの保守業務のような一時的アクセスの際にご検討ください。

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

### A.9 アクセス制御

#### A.9.1

#### A.9.2

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (ア) 2

##### 保守用のアカウントの管理

##### ■ ガイドラインとして必要な要求事項 Seq. 178

---

###### ①

情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲（AWS のインフラストラクチャー）において、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 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。

##### ■ 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。

詳細は「アマゾン ウェブ サービス：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://aws.amazon.com/jp/whitepapers/overview-of-security-processes/>

##### ■ AWS サービス関連情報

AWS 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します。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 Identity and Access Management (IAM)

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、アクセスした個人の特定をはじめ!継続的な監査対策を可能にします。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する必要があります。

AWS 責任共有モデルにおける利用者責任範囲において、情報システムの保守にかかわるアクセス権限やアクセス制限を定め、運用する必要があります。

AWS 利用者のアクティビティを記録したログ情報を元に、計画的な監査対応が求められます。

##### ■ 推奨される追加の実施事項

IAM では、AWS に対する、一時的な認証情報を作成する仕組み Temporary Security Credentials も提供されています。

これは、期限付きの認証情報（認証チケット）

であり、情報システムの保守業務のような一時的アクセスの際にご検討ください。

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

#### A.9 アクセス制御

##### A.9.1

##### A.9.2

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 1

##### リモートメンテナンス

##### ■ ガイドラインとして必要な要求事項 Seq. 179

---

##### ①

リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、情報システムへの不正な侵入が生じないよう安全管理措置を講じる。

##### ■ AWS のインフラストラクチャー関連事項

##### Amazon 社からの分離

論理的に、AWS 本稼働環境のネットワークは、ネットワークセキュリティ/分離デバイスの複雑な組み合わせによって、Amazon 社内ネットワークから分離しています。AWS クラウドのコンポーネントを維持するためにアクセスする必要がある社内ネットワーク上の AWS 開発者と管理者は AWS 発券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、該当するサービスの所有者によって確認および承認されます。

承認された AWS 担当者は、ネットワーク デバイスやその他のクラウドコンポーネントへのアクセスを制限する拠点ホストを介して AWS ネットワークに接続します。このとき、すべてのアクティビティはセキュリティレビューのために記録されます。拠点ホストへのアクセスには、ホスト上のすべてのユーザーアカウントに対して SSH 公開鍵認証が必要です。AWS 開発者および管理者の論理的アクセスの詳細については、後の「AWS アクセス」をご覧ください。

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 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）により AWS へのリモートアクセスには、SSH や RDP クライアントでのアクセス及び SSL-VPN によるアクセスが可能です。

また、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もできます。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。

い。

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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、情報システムへの不正な侵入が生じないよう安全管理措置を講じる必要があります。

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クラウドサービス事業者（お客様）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](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、クラウドサービス事業者が 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](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](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.9 アクセス制御

A.12 運用のセキュリティ

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 1

##### リモートメンテナンス

##### ■ ガイドラインとして必要な要求事項 Seq. 180

---

##### ②

リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。

##### ■ AWS のインフラストラクチャー関連事項

##### Amazon 社からの分離

論理的に、AWS 本稼働環境のネットワークは、ネットワークセキュリティ/分離デバイスの複雑な組み合わせによって、Amazon 社内ネットワークから分離しています。AWS クラウドのコンポーネントを維持するためにアクセスする必要がある社内ネットワーク上の AWS 開発者と管理者は AWS 発券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、該当するサービスの所有者によって確認および承認されます。

承認された AWS 担当者は、ネットワーク デバイスやその他のクラウドコンポーネントへのアクセスを制限する拠点ホストを介して AWS ネットワークに接続します。このとき、すべてのアクティビティはセキュリティレビューのために記録されます。拠点ホストへのアクセスには、ホスト上のすべてのユーザーアカウントに対して SSH 公開鍵認証が必要です。AWS 開発者および管理者の論理的アクセスの詳細については、後の「AWS アクセス」をご覧ください。

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 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）により AWS へのリモートアクセスには、SSH や RDP クライアントでのアクセス及び SSL-VPN によるアクセスが可能です。

また、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もできます。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/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認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クラウドサービス事業者（お客様）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](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、クラウドサービス事業者が 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](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るようになります。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](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.9 アクセス制御

A.12 運用のセキュリティ

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 1

##### リモートメンテナンス

##### ■ ガイドラインとして必要な要求事項 Seq. 181

---

##### ③

サービス提供に必要な情報システムの保守をリモートメンテナンスで行う場合、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

##### Amazon 社からの分離

論理的に、AWS 本稼働環境のネットワークは、ネットワークセキュリティ/分離デバイスの複雑な組み合わせによって、Amazon 社内ネットワークから分離しています。AWS クラウドのコンポーネントを維持するためにアクセスする必要がある社内ネットワーク上の AWS 開発者と管理者は AWS 発券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、該当するサービスの所有者によって確認および承認されます。

承認された AWS 担当者は、ネットワーク デバイスやその他のクラウドコンポーネントへのアクセスを制限する拠点ホストを介して AWS ネットワークに接続します。このとき、すべてのアクティビティはセキュリティレビューのために記録されます。拠点ホストへのアクセスには、ホスト上のすべてのユーザーアカウントに対して SSH 公開鍵認証が必要です。AWS 開発者および管理者の論理的アクセスの詳細については、後の「AWS アクセス」をご覧ください。

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 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）により AWS へのリモートアクセスには、SSH や RDP クライアントでのアクセス及び SSL-VPN によるアクセスが可能です。

また、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もできます。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。

い。

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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービス提供に必要な情報システムの保守をリモートメンテナンスで行う場合、サービス仕様適合開示書に基づき、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

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](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](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.9 アクセス制御

### A.12 運用のセキュリティ

### A.15 供給者関係

### A.16 情報セキュリティインシデント管理

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 2

##### ログによる保守結果のレビュー

##### ■ ガイドラインとして必要な要求事項 Seq. 182

---

##### ①

情報システムの保守において実施した操作結果について、操作ログ等により記録し、管理する。

##### ■ 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

##### - AWS CloudTrail

AWS ユーザの操作をロギングするサービスとして AWS CloudTrail が準備されています。

AWS CloudTrail では、誰が、いつ、どのような操作をしたか（またその操作の成功/失敗）といったログが取得できます。

ロギングデータは Amazon S3 に保存されます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自身の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クラウドサービス事業者の責任です。クラウドサービス事業者は、情報システムの保守において実施した操作結果について、操作ログ等により記録し、管理する必要があります。

AWS Cloud Trail を利用の場合は、有効化後、ロギングデータは Amazon S3 に保存されます。

##### ■ 推奨される追加の実施事項

ログによる保守結果のレビューまたは保守に限定しない通常のセキュリティ・コンプライアンスのレビューには、可視化ツールを用いた運用も効率的です。

膨大になりがちなロギングデータから Amazon Elasticsearch Service で検索、その結果をグラフなど視認性の高い可視化することも可能です。

Amazon Elasticsearch Service には可視化ツールである Kibana が実装されています。

また、サードパーティ製のツールやサービスも多く準備されています。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 2

##### ログによる保守結果のレビュー

##### ■ ガイドラインとして必要な要求事項 Seq. 183

---

##### ②

取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。

##### ■ 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

##### - AWS CloudTrail

AWS ユーザの操作をロギングするサービスとして AWS CloudTrail が準備されています。

AWS CloudTrail では、誰が、いつ、どのような操作をしたか（またその操作の成功/失敗）といったログが取得できます。

ロギングデータは Amazon S3 に保存されます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自身の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クラウドサービス事業者の責任です。クラウドサービス事業者は、取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする必要があります。

AWS の場合、ロギングされたデータは、直近 7 日分はダッシュボードから確認できます。情報システムの保守業務において操作した情報を取得したログからレビューに利用できます。

##### ■ 推奨される追加の実施事項

ログによる保守結果のレビューまたは保守に限定しない通常のセキュリティ・コンプライアンスのレビューには、可視化ツールを用いた運用も効率的です。

膨大になりがちなロギングデータから Amazon Elasticsearch Service で検索、その結果をグラフなど視認性の高い可視化することも可能です。

Amazon Elasticsearch Service には可視化ツールである Kibana が実装されています。

また、サードパーティ製のツールやサービスも多く準備されています。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 3

##### 医療機関等内における保守対応

##### ■ ガイドラインとして必要な要求事項 Seq. 184

---

##### ①

情報システムの保守業務を医療機関等の施設内で行う際の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

-AWS Identity and Access Management (IAM)

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/>

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自身の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クラウドサービス事業者の責任です。クラウドサービス事業者は、クラウド上に設置されたシステムの保守業務を医療機関等の施設内で際の対応について、サービス仕様適合開示書に基づき、医療機関等と合意を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.9 アクセス制御

##### A.12 運用のセキュリティ

##### A.15 供給者関係

##### A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 4

#### 保守業務の実施報告

##### ■ ガイドラインとして必要な要求事項 Seq. 185

---

##### ①

情報システムの保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲において、EC2 群の OS よりも下位のレイヤにアップグレードの適用を行なっています。

一部のアップデートでは、その適用のためにインスタンスの短時間の再起動が必要になります。

その通知は、登録された AWS 管理者あてにメール（英文）が届き、かつ AWS Management Console で確認ができます。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う必要があります。

クラウドサービス事業者は、医療機関等に事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、サービス仕様適合開示書に基づき、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

保守業務の実施にあたり、医療機関等がサービスを利用できない状況に陥らないための対応策としては、情報システムの Active/Standby 構成をとるといったご検討をお願いします。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.15 供給者関係

#### A.16 情報セキュリティインシデント管理



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 4

##### 保守業務の実施報告

##### ■ ガイドラインとして必要な要求事項 Seq. 186

---

##### ②

①における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲において、EC2 群の OS よりも下位のレイヤにアップグレードの適用を行なっています。

一部のアップデートでは、その適用のためにインスタンスの短時間の再起動が必要になります。

その通知は、登録された AWS 管理者あてにメール（英文）が届き、かつ AWS Management Console で確認ができます。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.6「情報システムの改造と保守に関する安全管理対策」（イ）4①における通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める必要があります。

##### ■ 推奨される追加の実施事項

保守業務の実施にあたり、医療機関等がサービスを利用できない状況に陥らないための対応策としては、情報システムの Active/Standby 構成をとるといったご検討をお願いします。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.15 供給者関係

#### A.16 情報セキュリティインシデント管理

---



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 4

#### 保守業務の実施報告

##### ■ ガイドラインとして必要な要求事項 Seq. 187

---

##### ③

保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲において、EC2 群の OS よりも下位のレイヤにアップグレードの適用を行なっています。

一部のアップデートでは、その適用のためにインスタスの短時間の再起動が必要になります。

その通知は、登録された AWS 管理者あてにメール（英文）が届き、かつ AWS Management Console で確認ができます。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

##### - 保守業務の実施手順について

##### ■ 推奨される追加の実施事項

保守業務の実施にあたり、医療機関等がサービスを利用できない状況に陥らないための対応策としては、情報システムの Active/Standby 構成をとるといったご検討をお願いします。

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

##### A.9 アクセス制御

##### A.12 運用のセキュリティ

##### A.15 供給者関係

##### A.16 情報セキュリティインシデント管理

---





### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 4

#### 保守業務の実施報告

##### ■ ガイドラインとして必要な要求事項 Seq. 188

---

##### ④

③に定めた手順を医療機関等に示し、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲において、EC2 群の OS よりも下位のレイヤにアップグレードの適用を行なっています。

一部のアップデートでは、その適用のためにインスタンスの短時間の再起動が必要になります。

その通知は、登録された AWS 管理者あてにメール（英文）が届き、かつ AWS Management Console で確認ができます。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、保守業務の実施手順について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

クラウドサービス事業者は、保守業務の実施手順に基づいた保守を実施する際に必要事項等について、サービス仕様適合開示書に基づき、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

保守業務の実施にあたり、医療機関等がサービスを利用できない状況に陥らないための対応策としては、情報システムの Active/Standby 構成をとるといったご検討をお願いします。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.15 供給者関係

#### A.16 情報セキュリティインシデント管理



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 4

#### 保守業務の実施報告

##### ■ ガイドラインとして必要な要求事項 Seq. 189

---

##### ⑤

④で示された手順について、医療機関等が対応すべき事項がある場合、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲において、EC2 群の OS よりも下位のレイヤにアップグレードの適用を行なっています。

一部のアップデートでは、その適用のためにインスタンスの短時間の再起動が必要になります。

その通知は、登録された AWS 管理者あてにメール（英文）が届き、かつ AWS Management Console で確認ができます。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、保守業務の実施手順について、医療機関等が対応すべき事項がある場合、サービス仕様適合開示書に基づき、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

保守業務の実施にあたり、医療機関等がサービスを利用できない状況に陥らないための対応策としては、情報システムの Active/Standby 構成をとるといったご検討をお願いします。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.15 供給者関係

#### A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (イ) 4

##### 保守業務の実施報告

##### ■ ガイドラインとして必要な要求事項 Seq. 190

---

##### ⑥

保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲において、EC2 群の OS よりも下位のレイヤにアップグレードの適用を行なっています。

一部のアップデートでは、その適用のためにインスタンスの短時間の再起動が必要になります。

その通知は、登録された AWS 管理者あてにメール（英文）が届き、かつ AWS Management Console で確認ができます。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、保守業務実施後、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る必要があります。

クラウドサービス事業者は、保守業務実施後の対応について、サービス仕様適合開示書に基づき、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

保守業務の実施にあたり、医療機関等がサービスを利用できない状況に陥らないための対応策としては、情報システムの Active/Standby 構成をとるといったご検討をお願いします。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.15 供給者関係

#### A.16 情報セキュリティインシデント管理

---



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (ウ) 1

##### 保守で用いるデータ

##### ■ ガイドラインとして必要な要求事項 Seq. 191

---

##### ①

情報システムの動作確認に際しては、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。

##### ■ AWS のインフラストラクチャー関連事項

N/A

AWS 責任共有モデルにおける 利用者の責任範囲において、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。

情報システムの動作確認に使用するデータ、人的安全管理対策、医療機関との合意は、クラウドサービス事業者（お客様）の責任において実施してください。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自身の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クラウドサービス事業者の責任です。クラウドサービス事業者は、情報システムの動作確認に際しては、以下の点を注意しテストを実施する必要があります。

-受託した個人情報を含むデータを使用せず、テスト用のデータを使用すること

##### ■ 推奨される追加の実施事項

クラウドでは、短期間だけ使える検証環境の準備が容易であることも利点です。

情報システムの動作確認においては、個人情報を含むデータが存在する環境（本番環境）とは別に、動作確認が必要な時だけ検証環境を立ち上げ利用することが可能です。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.14 システムの取得、開発及び保守

##### A.14.1

A.14.2.1

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (ウ) 1

##### 保守で用いるデータ

##### ■ ガイドラインとして必要な要求事項 Seq. 192

---

##### ②

情報システムの動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、3. 2. 4で示す守秘義務が課された要員・委託先等により動作確認を行う旨を含めた手順を定める。

##### ■ AWS のインフラストラクチャー関連事項

N/A

AWS 責任共有モデルにおける 利用者の責任範囲において、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。

情報システムの動作確認に使用するデータ、人的安全管理対策、医療機関との合意は、クラウドサービス事業者（お客様）の責任において実施してください。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自身の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クラウドサービス事業者の責任です。クラウドサービス事業者は、情報システムの動作確認に際しては、個人情報を含むデータをやむを得ず使用する場合には、3.2.4 [人的安全管理対策]で示す守秘義務が課された要員・委託先等により動作確認を行う旨を含めた手順を定める必要があります。。

##### ■ 推奨される追加の実施事項

クラウドでは、短期間だけ使える検証環境の準備が容易であることも利点です。

情報システムの動作確認においては、個人情報を含むデータが存在する環境（本番環境）とは別に、動作確認が必要な時だけ検証環境を立ち上げ利用することが可能です。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.14 システムの取得、開発及び保守

##### A.14.1

##### A.14.2.1



A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (ウ) 1

##### 保守で用いるデータ

##### ■ ガイドラインとして必要な要求事項 Seq. 193

---

##### ③

情報システムの動作確認に際し、受託した個人情報をやむを得ず使用する場合について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

N/A

AWS 責任共有モデルにおける 利用者の責任範囲において、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。

情報システムの動作確認に使用するデータ、人的安全管理対策、医療機関との合意は、クラウドサービス事業者（お客様）の責任において実施してください。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自身の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クラウドサービス事業者の責任です。③ 情報システムの動作確認において個人情報を含むデータをやむを得ず使用する場合には、サービス仕様適合開示書に基づき、医療機関等と合意をしてください。

##### ■ 推奨される追加の実施事項

クラウドでは、短期間だけ使える検証環境の準備が容易であることも利点です。

情報システムの動作確認においては、個人情報を含むデータが存在する環境（本番環境）とは別に、動作確認が必要な時だけ検証環境を立ち上げ利用することが可能です。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.14 システムの取得、開発及び保守

##### A.14.1

##### A.14.2.1

#### A.15 供給者関係



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (ウ) 2

##### 保守目的での医療情報の持ち出し

##### ■ ガイドラインとして必要な要求事項 Seq. 194

--

##### ①

医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療機関等又はクラウドサービス事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報を格納する機器等を、保守の目的で、医療機関等又はクラウドサービス事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、手順を策定する必要があります。

・医療情報持ち出し手順等

##### ■ 推奨される追加の実施事項

N/A

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

N/A

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (ウ) 2

##### 保守目的での医療情報の持ち出し

##### ■ ガイドラインとして必要な要求事項 Seq. 195

---

##### ②

①で定める手順及び情報の提供条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、作成した医療情報持ち出し手順等及び情報の提供条件について、サービス仕様適合開示書に基づき、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)

N/A

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 1

##### データ項目の標準形式の採用

##### ■ ガイドラインとして必要な要求事項 Seq. 196

---

##### ①

診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、保健医療分野の適切な情報化を進めることを目的として制定されている、「厚生労働省標準規格」で定められているデータ項目は、当該規格を採用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)

N/A

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 1

##### データ項目の標準形式の採用

##### ■ ガイドラインとして必要な要求事項 Seq. 197

---

##### ②

厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、「厚生労働省標準規格」で定められていないデータ項目について、変換が容易なデータ形式とし、サービス仕様適合開示書に基づき、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)

N/A

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 2

##### レコード管理方法等

##### ■ ガイドラインとして必要な要求事項 Seq. 198

---

##### ①

医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を情報システムに備える。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を情報システムに備える必要があります。

##### ■ 推奨される追加の実施事項

N/A

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

N/A

---



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 2

##### レコード管理方法等

- ガイドラインとして必要な要求事項 Seq. 199

--

##### ②

①に示す機能等を備えることが困難な場合の情報システム更新・移行の手順について、サービス仕様適合開示書に基づき、医療機関等と合意する。

- 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

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報に係るマスターテーブルの変更に際してとるべき機能が困難な場合の情報システム更新・移行の手順について、サービス仕様適合開示書に基づき、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)

N/A

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 3

#### データ形式及び転送プロトコルのバージョン管理と継続性の確保

##### ■ ガイドラインとして必要な要求事項 Seq. 200

---

##### ①

データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する必要があります。

##### ■ 推奨される追加の実施事項

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挙げられます。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](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/>

クラウドサービス事業者は、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場合は下位互換性をサポートする必要があります。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.14 システムの取得、開発及び保守

##### A.14.1

##### A.14.2.1

#### A.15 供給者関係

## A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 3

#### データ形式及び転送プロトコルのバージョン管理と継続性の確保

##### ■ ガイドラインとして必要な要求事項 Seq. 201

---

##### ②

①の結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、データ形式等の変更を行った結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う必要があります。

##### ■ 推奨される追加の実施事項

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挙げられます。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](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/>

クラウドサービス事業者は、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場合は下位互換性をサポートする必要があります。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.14 システムの取得、開発及び保守

##### A.14.1

A.14.2.1

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

(エ) 3 データ形式及び転送プロトコルのバージョン管理と継続性の確保

##### ■ ガイドラインとして必要な要求事項 Seq. 202

---

③

②は、他の情報システムとのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、データ形式等の変更を行う際には、他の情報システムとのデータ連携等を考慮して行う必要があります。

クラウドサービス事業者は、医療機関等に対する互換性確保に係る情報提供について、サービス仕様適合開示書に基づき、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

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挙げられます。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](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/>

クラウドサービス事業者は、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場合は下位互換性をサポートする必要があります。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.14 システムの取得、開発及び保守

A.14.1

A.14.2.1

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 3

#### データ形式及び転送プロトコルのバージョン管理と継続性の確保

##### ■ ガイドラインとして必要な要求事項 Seq. 203

---

##### ④

データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、3. 4に示す対策を講じる。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、3.4「クラウドサービスの利用終了に関する要求事項」に示す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

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挙げられます。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](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/>

クラウドサービス事業者は、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場合は下位互換性をサポートする必要があります。

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

#### A.9 アクセス制御

#### A.12 運用のセキュリティ

#### A.14 システムの取得、開発及び保守

##### A.14.1

##### A.14.2.1



A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (工) 4

##### サービスに供する機器の劣化対策

##### ■ ガイドラインとして必要な要求事項 Seq. 204

---

###### ①

サービスに供する情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲（AWS のインフラストラクチャー）においては、AWS により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。

機器の製品寿命は AWS により管理されており、その措置も AWS により実施されます。

##### 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。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに供する情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる必要があります。

AWS のインスタンスのリタイアに関する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/knowledge-center/ec2-instance-retirement/>

##### 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カウント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。

インスタンスにリタイアが予定されている場合、インスタンスを再起動してください。それにより異なる基盤のハードウェア上に起動されます。再起動にかかる時間は数分程度ですが、サービス停止回避のため、指定のメンテナンス期間より前の任意の時間で再起動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 資産管理

A.8.1

A.8.2

A.8.3

A.12 運用のセキュリティ

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (工) 4

##### サービスに供する機器の劣化対策

##### ■ ガイドラインとして必要な要求事項 Seq. 205

---

##### ②

サービスに供する情報システムについて、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲（AWS のインフラストラクチャー）においては、AWS により様々なコンポーネントが運用、管理、コントロールされます。

一方で、ゲストオペレーティングシステム、その他の関連アプリケーションソフトウェアにおいては、利用者の責任範囲と定めています。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに供する情報システムについて、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる必要があります。

AWS 責任共有モデルにおける利用者の責任範囲において、ソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じてください。

特にゲストオペレーティングシステムのサポート終了に伴う措置が課題となるケースが多く、後継オペレーティングシステムへの移行といった措置を遅れをとらず実施してください。

##### ■ 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.8 資産管理

##### A.8.1

##### A.8.2

##### A.8.3

#### A.12 運用のセキュリティ

---



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (工) 4

##### サービスに供する機器の劣化対策

##### ■ ガイドラインとして必要な要求事項 Seq. 206

---

##### ③

サービスに供する情報システムについて、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲（AWS のインフラストラクチャー）においては、AWS により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。

機器の製品寿命は AWS により管理されており、その措置も AWS により実施されます。

一方で、一方で、ゲストオペレーティングシステム、その他の関連アプリケーションソフトウェアにおいては、利用者の責任範囲と定めています。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに供する情報システムについて、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合は、以下の対応を行う必要があります。

- 利用している医療機関等への影響を最小とするための措置を講じる
- 医療機関等が対応するために十分な期間をもって告知を行う

AWS 責任共有モデルにおける利用者の責任範囲において、ソフトウェア等の提供事業者におけるサポート終了等が生じることからサービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、その影響範囲や影響度合いを調査し、影響を最小にする措置を検討してください。

その上で、医療機関等が対応するために十分な期間をもって調整の上で措置を講じてください。

##### ■ 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.8 資産管理

##### A.8.1

A.8.2

A.8.3

A.12 運用のセキュリティ

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 4

#### サービスに供する機器の劣化対策

##### ■ ガイドラインとして必要な要求事項 Seq. 207

---

##### ④

③においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、サービス仕様適合開示書に基づき、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.8 資産管理

##### A.8.1

##### A.8.2

##### A.8.3

#### A.12 運用のセキュリティ

---



### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

(エ) 5 サービスに供する情報システムの互換性確保や他の事業者のサービスとの関係

#### ■ ガイドラインとして必要な要求事項 Seq. 208

---

①

医療情報を取り扱うサービスに供する情報システムに関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う。

#### ■ 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。

#### ソフトウェア

AWS は、変更の管理に体系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。

#### ■ AWS サービス関連情報

N/A

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報を取り扱うサービスに供する情報システムに関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う必要があります。

#### ■ 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.9 アクセス制御

A.12 運用のセキュリティ

A.14 システムの取得、開発及び保守

A.14.1

A.14.2.1

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (Ⅰ) 5

サービスに供する情報システムの互換性確保や他の事業者のサービスとの関係

##### ■ ガイドラインとして必要な要求事項 Seq. 209

---

##### ②

他のクラウドサービス事業者が提供するクラウドサービスを用いて、サービスを提供する場合には、他のクラウドサービス事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他のクラウドサービス事業者のクラウドサービスの停止・変更に伴い、自社が提供するサービスの一部又は全部の停止、変更（軽微なバージョンアップは含まない）等が生じる場合には、「4. サービスに供する機器の劣化対策」②～④に示す対応策を講じる。

##### ■ 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。

#### 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。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、利用するサービスの停止を想定し、サービスの一部やアベイラビリティゾーンの停止などが発生した際も自社サービスの提供に支障が生じないように、「Design for Failure」の考え方に従って可用性を考慮したシステムを設計・構築する必要があります。

AWS では、「Design for Failure」を含めた AWS 上でのアプリケーション実装のベストプラクティスを Well-Architected フレームワークとして公開されています。

Well-Architected フレームワークは、クラウドアーキテクトがアプリケーション向けに実装可能な、最も安全かつ高パフォーマンス、障害耐性を備え、効率的なインフラストラクチャを構築するのをサポートする目的で開発されました。このフレームワークでは、お客様とパートナーがアーキテクチャを評価するために一貫したアプローチを行い、アプリケーションのニーズに応じて時間の経過とともにスケールする設計を実装するのに役立つガイダンスを提供します。詳細は下記 URL を参照ください。

<https://aws.amazon.com/jp/architecture/well-architected/>

#### ■ 推奨される追加の実施事項

リスクマネジメントを考慮した上で、AWSリージョンの全面的な停止に備えた、別リージョンでの DR などサービス継続計画を策定しておくことを推奨します。

また、他社クラウドや自社設備での代替運用に備え、コンテナ技術などを用いた可搬性を考慮したシステム構成とすることを推奨します。

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

### A.9 アクセス制御

### A.12 運用のセキュリティ

### A.14 システムの取得、開発及び保守

#### A.14.1

#### A.14.2.1

### A.15 供給者関係

### A.16 情報セキュリティインシデント管理

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (工) 5

サービスに供する情報システムの互換性確保や他の事業者のサービスとの関係

##### ■ ガイドラインとして必要な要求事項 Seq. 210

---

##### ③

医療情報を取り扱うサービスに供する情報システムに係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他のクラウドサービス事業者のクラウドサービスの変更を行う場合には、①、②を考慮して行う。

##### ■ 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。

##### 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。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、自身が利用するサービス・ソフトウェアの更新または他クラウドサービスへの変更を行う場合は、下記について考慮したうえで更新・変更を行うことが求められます。

- ・ サービス・ソフトウェアの将来的な互換性・標準仕様変更時のリスク
- ・ 利用サービス停止時の可用性

##### ■ 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.9 アクセス制御

A.12 運用のセキュリティ

A.14 システムの取得、開発及び保守

A.14.1

A.14.2.1

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (オ) 1

##### 保守体制の変更

##### ■ ガイドラインとして必要な要求事項 Seq. 211

---

##### ①

情報システムの保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、サービス仕様適合開示書に基づき、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.9 アクセス制御

##### A.12 運用のセキュリティ

##### A.14 システムの取得、開発及び保守

##### A.14.1

##### A.14.2.1

##### A.15 供給者関係

##### A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (オ) 2 再委託先の体制

##### ■ ガイドラインとして必要な要求事項 Seq. 212

---

###### ①

情報システムの保守に関して、外部事業者はその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲において、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](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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの保守に関して、外部事業者はその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める必要があります。

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を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、クラウドサービス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](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.9 アクセス制御



A.12 運用のセキュリティ

A.14 システムの取得、開発及び保守

A.14.1

A.14.2.1

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.6

#### 情報システムの改造と保守に関する安全管理対策

##### (オ) 2

##### 再委託先の体制

##### ■ ガイドラインとして必要な要求事項 Seq. 213

---

##### ②

①の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。

##### ■ AWS のインフラストラクチャー関連事項

AWS 責任共有モデルにおける AWS 責任範囲において、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](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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、情報システムの保守に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する必要があります。

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を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、クラウドサービス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](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.9 アクセス制御

#### A.12 運用のセキュリティ

A.14 システムの取得、開発及び保守

A.14.1

A.14.2.1

A.15 供給者関係

A.16 情報セキュリティインシデント管理

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ア) 1

##### 機器・媒体の持ち出しに関する方針策定

##### ■ ガイドラインとして必要な要求事項 Seq. 214

---

##### ①

サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器・媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。

##### ■ 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るため、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

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

- 機器（サービスに関する受託情報や情報システムに関連する情報等を格納している機器）・媒体の持ち出し方針
- 機器・媒体の持ち出し手順

#### ■ 推奨される追加の実施事項

##### ①機器を介したデータ持ち出しに関して

AWS Snowball が用意するセキュリティ施策に加えて運用プロセスとして、当該サービスのリクエストの依頼者、デバイスの受領者／返送者、ならびにローカルストレージとの間のデータ複製処理の実施者に対する管理と記録が必要です。あわせて実施記録も必要です。

特に、AWS Snowball Export を利用するケースでは、既存の AWS 上の情報を外部へ持ち出す行為にあたるので、情報漏洩の観点からも作業関係者や関連作業についての管理監督には注意が必要です。

##### ②ネットワークを介したデータ持ち出しに関して

ユーザアクセス権とネットワークアクセス／経路を管理することでデータ持ち出し時の漏洩リスクを防御する対処が必要です。通常時は、AWS Direct Connect/VPC と IAM や、利用端末／デバイス管理、VPN ソフトウェアによってデータ保護します。不要または不審な情報ダウンロードを回避する観点から、新規利用端末の登録／新たな利用 IP アドレスの追加接続やファイヤーウォールの設定変更の申請時に妥当性をチェックする運用プロセスとしておくことが推奨されます。また大量のダウンストリーム・トラフィックが発生した場合には、その実行者や目的の妥当性を確認するのも重要です。

#### ■ 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.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

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ア) 1

##### 機器・媒体の持ち出しに関する方針策定

##### ■ ガイドラインとして必要な要求事項 Seq. 215

---

##### ②

①における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。

##### ■ 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

##### ①機器を介したデータ持ち出しに関して

##### -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/>

## ②ネットワークを介したデータ持ち出しに関して

### -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/>

### - AWS Identity and Access Management (IAM)

IAM を使用すると、複数の種類の、IAM ユーザーの長期的なセキュリティ認証情報（パスワード、アクセスキー、Amazon CloudFront のキーペア、SSH パブリックキー、X.509 証明書）を管理できます。

このようなユーザー認証情報の管理に加え、Multi-Factor Authentication (MFA) を義務づけることで、AWS への IAM ユーザーアクセスのセキュリティをさらに強化できます。

AWS における長期的なセキュリティ認証情報の使用の詳細については、AWS セキュリティの認証情報を参照してください。

<https://docs.aws.amazon.com/general/latest/gr/aws-security-credentials.html>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、機器・媒体の持ち出し方針や 機器・媒体の持ち出し手順に、ネットワークを通じた外部への送信についても含んだ内容にする必要があります。

#### ■ 推奨される追加の実施事項



### ①機器を介したデータ持ち出しに関して

AWS Snowball が用意するセキュリティ施策に加えて運用プロセスとして、当該サービスのリクエストの依頼者、デバイスの受領者／返送者、ならびにローカルストレージとの間のデータ複製処理の実施者に対する管理と記録が必要です。あわせて実施記録も必要です。

特に、AWS Snowball Export を利用するケースでは、既存の AWS 上の情報を外部へ持ち出す行為にあたるので、情報漏洩の観点からも作業関係者や関連作業についての管理監督には注意が必要です。

### ②ネットワークを介したデータ持ち出しに関して

ユーザアクセス権とネットワークアクセス／経路を管理することでデータ持ち出し時の漏洩リスクを防御する対処が必要です。通常時は、AWS Direct Connect/VPC と IAM や、利用端末／デバイス管理、VPN ソフトウェアによってデータ保護します。不要または不審な情報ダウンロードを回避する観点から、新規利用端末の登録／新たな利用 IP アドレスの追加接続やファイアウォールの設定変更の申請時に妥当性をチェックする運用プロセスとしておくことが推奨されます。また大量のダウンストリーム・トラフィックが発生した場合には、その実行者や目的の妥当性を確認するのも重要です。

#### ■ 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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ア) 1 機器・媒体の持ち出しに関する方針策定

##### ■ ガイドラインとして必要な要求事項 Seq. 216

---

##### ③

①で定める内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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るため、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

##### ①機器を介したデータ持ち出しに関して

##### -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/>

## ②ネットワークを介したデータ持ち出しに関して

### -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/>

### - AWS Identity and Access Management (IAM)

IAM を使用すると、複数の種類の、IAM ユーザーの長期的なセキュリティ認証情報 (パスワード、アクセスキー、Amazon CloudFront のキーペア、SSH パブリックキー、X.509 証明書) を管理できます。

このようなユーザー認証情報の管理に加え、Multi-Factor Authentication (MFA) を義務づけることで、AWS への IAM ユーザーアクセスのセキュリティをさらに強化できます。

AWS における長期的なセキュリティ認証情報の使用の詳細については、AWS セキュリティの認証情報を参照してください。

<https://docs.aws.amazon.com/general/latest/gr/aws-security-credentials.html>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に盛り込んだ、機器・媒体の持ち出し方針や 機器・媒体の持ち出し手順について、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

### ①機器を介したデータ持ち出しに関して

AWS Snowball が用意するセキュリティ施策に加えて運用プロセスとして、当該サービスのリクエストの依頼者、デバイスの受領者／返送者、ならびにローカルストレージとの間のデータ複製処理の実施者に対する管理と記録が必要です。あわせて実施記録も必要です。

特に、AWS Snowball Export を利用するケースでは、既存の AWS 上の情報を外部へ持ち出す行為にあたるので、情報漏洩の観点からも作業関係者や関連作業についての管理監督には注意が必要です。

## ②ネットワークを介したデータ持ち出しに関して

ユーザアクセス権とネットワークアクセス／経路を管理することでデータ持ち出し時の漏洩リスクを防御する対処が必要です。通常時は、AWS Direct Connect/VPC と IAM や、利用端末／デバイス管理、VPN ソフトウェアによってデータ保護します。不要または不審な情報ダウンロードを回避する観点から、新規利用端末の登録／新たな利用 IP アドレスの追加接続やファイアーウォールの設定変更の申請時に妥当性をチェックする運用プロセスとしておくことが推奨されます。また大量のダウンストリーム・トラフィックが発生した場合には、その実行者や目的の妥当性を確認するのも重要です。

### ■ 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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ア) 2

#### サービスに供する記録媒体・記録機器に関する対応

##### ■ ガイドラインとして必要な要求事項 Seq. 217

---

##### ①

サービスに供する記録媒体・記録機器に関し、以下の内容を運用管理規程に含める。

- ・管理体制及び管理方法
- ・記録媒体・記録機器の取扱い
- ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器・媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等（「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。）
- ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器・媒体等の盗難・紛失（持ち出し時の機器・媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業員等における誤送信等を含む。））が起きた場合の対応
- ・外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改ざんが生じないようにするための具体的な措置（マルウェア対策、暗号化、ファイアウォール導入等））

##### ■ 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るため、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

### ①機器を介したデータ持ち出しに関して

#### -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/>

### ②ネットワークを介したデータ持ち出しに関して

#### -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/>

#### - AWS Identity and Access Management (IAM)

IAM を使用すると、複数の種類の、IAM ユーザーの長期的なセキュリティ認証情報 (パスワード、アクセスキー、Amazon CloudFront のキーペア、SSH パブリックキー、X.509 証明書) を管理できます。

このようなユーザー認証情報の管理に加え、Multi-Factor Authentication (MFA) を義務づけることで、AWS への IAM ユーザーアクセスのセキュリティをさらに強化できます。



AWS における長期的なセキュリティ認証情報の使用の詳細については、AWS セキュリティの認証情報を参照してください。

<https://docs.aws.amazon.com/general/latest/gr/aws-security-credentials.html>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

#### - サービスに供する記録媒体・記録機器に関する内容

- ・管理体制及び管理方法
- ・記録媒体・記録機器の取扱い
- ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器・媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等
- ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器・媒体等の盗難・紛失（持ち出し時の機器・媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業員等における誤送信等を含む。））が起きた場合の対応
- ・外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改ざんが生じないようするための具体的な措置（マルウェア対策、暗号化、ファイアウォール導入等））

#### -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/>

Snowball デバイスでは、不正開封防止筐体、256 ビットの暗号化、データのセキュリティと完全な保管継続性を確保するための業界標準である Trusted Platform Module (TPM) を使用しています。暗号化キーは AWS Key Management Service (KMS) を使って管理されており、デバイスへの送信やデバイスでの保存を行うことはありません。

#### 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。

クラウドサービス事業者へ 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。

#### ■ 推奨される追加の実施事項

##### ①機器を介したデータ持ち出しに関して

AWS Snowball が用意するセキュリティ施策に加えて運用プロセスとして、当該サービスのリクエストの依頼者、デバイスの受領者／返送者、ならびにローカルストレージとの間のデータ複製処理の実施者に対する管理と記録が必要です。あわせて実施記録も必要です。

特に、AWS Snowball Export を利用するケースでは、既存の AWS 上の情報を外部へ持ち出す行為にあたるので、情報漏洩の観点からも作業関係者や関連作業についての管理監督には注意が必要です。

##### ②ネットワークを介したデータ持ち出しに関して

ユーザアクセス権とネットワークアクセス／経路を管理することでデータ持ち出し時の漏洩リスクを防御する対応が必要です。通常時は、AWS Direct Connect/VPC と IAM や、利用端末／デバイス管理、VPN ソフトウェアによってデータ保護します。不要または不審な情報ダウンロードを回避する観点から、新規利用端末の登録／新たな利用 IP アドレスの追加接続やファイアーウォールの設定変更の申請時に妥当性をチェックする運用プロセスとしておくことが推奨されます。また大量のダウンストリーム・トラフィックが発生した場合には、その実行者や目的の妥当性を確認するのも重要です。

#### ■ 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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ア) 3

##### 従業員等及び委託先に対する対応

##### ■ ガイドラインとして必要な要求事項 Seq. 218

---

##### ①

「2.サービスに供する記録媒体・記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。

##### ■ AWS のインフラストラクチャー関連事項

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。

AWS は、社員が個々の役割と責任を理解するのを助けるための、内部コミュニケーションのためのさまざまな方策を実施しています。これらの方策は、新入社員研修や、ビジネス成果の確認の面談、またビデオ会議、電子メールや Amazon のイントラネットを介した情報の掲載などの電子的手段も含まれます。

詳細については、「AWS セキュリティプロセスの概要」のホワイトペーパーを参照してください。

<http://aws.amazon.com/security>

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.7「情報及び情報機器の持ち出しについての安全管理対策」（ア）2 を盛り込んだ運用管理規程について、従業員等に教育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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ア) 3

##### 従業員等及び委託先に対する対応

##### ■ ガイドラインとして必要な要求事項 Seq. 219

---

##### ②

上記の運用管理規程については、再委託先に対しても遵守等を求める。

##### ■ AWS のインフラストラクチャー関連事項

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。

AWS は、社員が個々の役割と責任を理解するのを助けるための、内部コミュニケーションのためのさまざまな方策を実施しています。これらの方策は、新入社員研修や、ビジネス成果の確認の面談、またビデオ会議、電子メールや Amazon のイントラネットを介した情報の掲載などの電子的手段も含まれます。

詳細については、「AWS セキュリティ・プロセスの概要」のホワイトペーパーを参照してください。

<http://aws.amazon.com/security>

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.7「情報及び情報機器の持ち出しについての安全管理対策」（ア）2 を盛り込んだ運用管理規程について、再委託先に対しても同様に遵守等を求める必要があります。

##### ■ 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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ア) 4

##### 医療機関等との合意

##### ■ ガイドラインとして必要な要求事項 Seq. 220

---

##### ①

「2.サービスに供する記録媒体・記録機器に関する対応」、「3.従業員等及び委託先に対する対応」に示す情報の持ち出しに関する運用管理規程等における対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

いかなる目的であっても、AWS が、利用者の同意を得ることなく、利用者のコンテンツにアクセスしたり、それを使用したりすることはありません。マーケティングや広告のために、利用者のコンテンツを使用したり情報を抜き出したりすることはありません。

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に従うために必要な場合を除き、AWS がカスタマー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。

所定の統制によってシステムおよびデータのアクセスを制限し、AWS アクセスポリシーに従って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できるようにしています。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

利用者は、コンテンツに対するアクセスと、AWS サービスおよびリソースに対するユーザーアクセスを管理できます。利用者がこれを効果的に実施できるように、アクセス、暗号化、およびログ記録や監査支援の高性能な機能セットを用意しています (AWS CloudTrail など)。

利用者は、コンテンツを保存する AWS リージョンを選択でき、またコンテンツを保護する方法を選択できます。AWS は、転送中または保管中のコンテンツに使用できる強力な暗号化機能と、利用者自身の暗号化キーを管理するオプションを提供しています。

利用者は、コンテンツを保護する方法を選択できます。AWS は、転送中または保管中のコンテンツに使用できる強力な暗号化機能と、利用者自身の暗号化キーを管理するオプションを提供しています。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、3.2.7「情報及び情報機器の持ち出しについての安全管理対策」（ア）2 を盛り込んだ運用管理規程及び従業員等及び委託先教育について、サービス仕様適合開示書に基づき、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

AWS の提供する管理ツールを用いた管理プロセスを定め、かつ監査に向けた準備（ログ保管などの監査準備）をしておく事が推奨されます。

■ 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

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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (イ)

##### 機器・媒体の台帳管理

##### ■ ガイドラインとして必要な要求事項 Seq. 221

---

##### ①

サービスに関する情報を格納する機器・媒体等については、台帳管理等を行い、定期的に所在確認を行う。

##### ■ 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 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに関する情報を格納する 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。

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

##### ①機器を介したデータ持ち出しに関して

AWS Snowball が用意するセキュリティ施策に加えて運用プロセスとして、当該サービスのリクエストの依頼者、デバイスの受領者／返送者、ならびにローカルストレージとの間のデータ複製処理の実施者に対する管理と記録が必要です。あわせて実施記録も必要です。

特に、AWS Snowball Export を利用するケースでは、既存の AWS 上の情報を外部へ持ち出す行為にあたるので、情報漏洩の観点からも作業関係者や関連作業についての管理監督には注意が必要です。

##### ②ネットワークを介したデータ持ち出しに関して

ユーザアクセス権とネットワークアクセス／経路を管理することでデータ持ち出し時の漏洩リスクを防御する対処が必要です。通常時は、AWS Direct Connect/VPC と IAM や、利用端末／デバイス管理、VPN ソフトウェアによってデータ保護します。不要または不審な情報ダウンロードを回避する観点から、新規利用端末の登録／新たな利用 IP アドレスの追加接続やファイアウォールの設定変更の申請時に妥当性をチェックする運用プロセスとしておくことが推奨されます。また大量のダウンストリーム・トラフィックが発生した場合には、その実行者や目的の妥当性を確認するのも重要です。

#### ■ 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.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

■ 7.6.7 必須 (3)

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

## ■7.6.7 必須 (4)

## 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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 1

##### 起動パスワードの設定

##### ■ ガイドラインとして必要な要求事項 Seq. 222

---

##### ①

サービスに供する機器等については、起動パスワードの設定を行う。

##### ■ 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 管理コンソールでは、お客様の AWS アカウントに関するあらゆるクラウド管理を行うことができます。月間ご利用額をサービス別に見る、セキュリティ認証情報を管理する、新しい IAM ユーザーをセットアップするといったことが可能です。AWS コンソールで必要なサービスを見つけてそこへ移動する方法がいくつか用意されています。コンソールのホームで検索機能を利用し、セクションからサービスを選択したり、セクションを展開して AWS で提供されているすべてのサービスのリスト全体を参照したりすることができます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに供する機器等については、起動パスワードの設定を行う必要があります。

AWS 利用にあたり管理プロセスとして 2 階層の規定が必要になります。

- AWS の全てのサービスの有効化や無効化や起動／停止が可能な AWS 管理ポータルへのアクセスユーザの管理と利用記録についてです。

- リソース単位（典型的には稼働 OS）でのアクセスユーザの管理と利用記録です。

それぞれの階層で起動や停止が可能な（アドミン）ユーザとパスワードの管理が必要です。

■ 推奨される追加の実施事項

AWS 管理ポータルを利用するユーザと、VM インスタンス/OS 単位のアドミニュートラに対するユーザ／パスワード管理プロセスを定める必要があります。利用者申請、承認者／権限付与、パスワードリセット実施を含む一連のワークフローの実装が必要です。

■ 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.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



### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 1

##### 起動パスワードの設定

##### ■ ガイドラインとして必要な要求事項 Seq. 223

---

##### ②

起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。

##### ■ 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 によるパスワード・ポリシーの設定ができます。

詳細は以下を参照ください。

[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_passwords\\_account-policy.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html)

AWS での多要素認証の仕組みの導入ができます。

詳細は以下を参照ください。

[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_mfa.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html)

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、起動パスワードの設定について、以下に注意して対策を講じる必要があります。

- 推定しにくいこと

- 定期的な変更
- 第三者による不正な機器の起動がなされないこと

■ 推奨される追加の実施事項

AWS IAM によるパスワード・ポリシーの設定をし、かつ多要素認証の仕組みを導入します。

詳細は以下を参照ください。

[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_passwords\\_account-policy.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html)

[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_mfa.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 1

##### 起動パスワードの設定

##### ■ ガイドラインとして必要な要求事項 Seq. 224

---

##### ③

サービスに関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせで行う。

##### ■ 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 によるパスワード・ポリシーの設定ができます。

詳細は以下を参照ください。

[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_passwords\\_account-policy.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html)

AWS での多要素認証の仕組みの導入ができます。

詳細は以下を参照ください。

[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_mfa.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.html)

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに関する情報を格納する情報機器へのログイン及びアクセスの起動パスワードの設定について、以下に注意して対策を講じる必要があります。

- 複数の認証要素を組み合わせること

## ■ 推奨される追加の実施事項

AWS IAM によるパスワード・ポリシーの設定をし、かつ多要素認証の仕組みを導入します。

詳細は以下を参照ください。

[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_passwords\\_account-policy.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html)

[https://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_mfa.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa.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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 2

##### 機器を持ち出す場合の手順

##### ■ ガイドラインとして必要な要求事項 Seq. 225

---

##### ①

サービスに関する情報を格納する機器・媒体等を持ち出す場合の手順には、機器・媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。

##### ■ AWS のインフラストラクチャー関連事項

いかなる目的であっても、AWS が、利用者の同意を得ることなく、利用者のコンテンツにアクセスしたり、それを使用したりすることはありません。マーケティングや広告のために、利用者のコンテンツを使用したり情報を抜き出したりすることはありません。

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に従うために必要な場合を除き、AWS がカスタマー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。

唯一、外部とのデータの移動の手段として、大規模なデータ転送ソリューションの AWS Snowball が用意されていますが、標準サービスとして暗号化を含め標準手順化されています。

##### ■ 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/>

Snowball デバイスでは、不正開封防止筐体、256 ビットの暗号化、データのセキュリティと完全な保管継続性を確保するための業界標準である Trusted Platform Module (TPM) を使用しています。暗号化キーは AWS Key Management Service (KMS) を使って管理されており、デバイスへの送信やデバイスでの保存を行うことはありません。

## 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。

クラウドサービス事業者は 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。

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに関する情報を格納する機器・媒体等を持ち出す場合の手順に、以下を盛り込む必要があります。

- 機器・媒体事態に暗号化措置を施す
- 格納されている情報の暗号化
- パスワードの設定

### ■ 推奨される追加の実施事項

AWS Snowball が用意するセキュリティ施策に加えて運用プロセスとして、当該サービスのリクエストの依頼者、デバイスの受領者／返送者、ならびにローカルストレージとの間のデータ複製処理の実施者に対する管理と記録が必要です。あわせて実施記録も必要です。

特に、AWS Snowball Export を利用するケースでは、既存の AWS 上の情報を外部へ持ち出す行為にあたるので、情報漏洩の観点からも作業関係者や関連作業についての管理監督には注意が必要です。

### ■ 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.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

---



### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 3

##### 持ち出し機器等におけるアプリケーション

##### ■ ガイドラインとして必要な要求事項 Seq. 226

---

###### ①

サービスに関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。

##### ■ 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るため、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/>

Snowball デバイスでは、不正開封防止筐体、256 ビットの暗号化、データのセキュリティと完全な保管継続性を確保するための業界標準である Trusted Platform Module (TPM) を使用しています。暗号化キーは AWS Key Management Service (KMS) を使って管理されており、デバイスへの送信やデバイスでの保存を行うことはありません。

### 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。

クラウドサービス事業者が 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。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする必要があります。

#### ■ 推奨される追加の実施事項

AWS Snowball が用意するセキュリティ施策に加えて運用プロセスとして、当該サービスのリクエストの依頼者、デバイスの受領者／返送者、ならびにローカルストレージとの間のデータ複製処理の実施者に対する管理と記録が必要です。あわせて実施記録も必要です。

特に、AWS Snowball Export を利用するケースでは、既存の AWS 上の情報を外部へ持ち出す行為にあたるので、情報漏洩の観点からも作業関係者や関連作業についての管理監督には注意が必要です。

■ 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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 3

##### 持ち出し機器等におけるアプリケーション

##### ■ ガイドラインとして必要な要求事項 Seq. 227

---

##### ②

サービスに関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。

##### ■ 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るため、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/>

Snowball デバイスでは、不正開封防止筐体、256 ビットの暗号化、データのセキュリティと完全な保管継続性を確保するための業界標準である Trusted Platform Module (TPM) を使用しています。暗号化キーは AWS Key Management Service (KMS) を使って管理されており、デバイスへの送信やデバイスでの保存を行うことはありません。

### 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。

クラウドサービス事業者が 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。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスに関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める必要があります。

#### ■ 推奨される追加の実施事項

AWS Snowball が用意するセキュリティ施策に加えて運用プロセスとして、当該サービスのリクエストの依頼者、デバイスの受領者／返送者、ならびにローカルストレージとの間のデータ複製処理の実施者に対する管理と記録が必要です。あわせて実施記録も必要です。

特に、AWS Snowball Export を利用するケースでは、既存の AWS 上の情報を外部へ持ち出す行為にあたるので、情報漏洩の観点からも作業関係者や関連作業についての管理監督には注意が必要です。

■ 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.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

---



### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 4BYOD への対応

##### ■ ガイドラインとして必要な要求事項 Seq. 228

---

###### ①

サービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは禁止する。

##### ■ 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/>

## - AWS Identity and Access Management (IAM)

IAM を使用すると、複数の種類の、IAM ユーザーの長期的なセキュリティ認証情報（パスワード、アクセスキー、Amazon CloudFront のキーペア、SSH パブリックキー、X.509 証明書）を管理できます。

このようなユーザー認証情報の管理に加え、Multi-Factor Authentication (MFA) を義務づけることで、AWS への IAM ユーザーアクセスのセキュリティをさらに強化できます。

AWS における長期的なセキュリティ認証情報の使用の詳細については、AWS セキュリティの認証情報を参照してください。

<https://docs.aws.amazon.com/general/latest/gr/aws-security-credentials.html>

### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、BYOD への対応として、サービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは禁止する必要があります。

### ■ 推奨される追加の実施事項

利用者の ID/アクセス権の管理、利用端末（デバイス）と交換情報に対するセキュリティ保護対策と管理のプロセス導入の必要です。

エンドユーザー側と保守・運用目的の利用環境（リソースやネットワークアクセス経路など）の分離、および管理データの分離が必要です。

### ■ 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.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

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 4

##### BYOD への対応

##### ■ ガイドラインとして必要な要求事項 Seq. 229

---

##### ②

利用者が個人所有する機器によるサービス利用に関する対応策については、サービス仕様適合開示書に基づき、医療機関等と合意する。

なお具体的には以下の内容を参考にする。

・利用者が所有する機器からの情報漏えい等を防止する観点から、例えば、仮想デスクトップを用いて OS レベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント (MDM) やモバイルアプリケーションマネジメント (MAM) 等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。

##### ■ 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/>

#### - AWS Identity and Access Management (IAM)

IAM を使用すると、複数の種類の、IAM ユーザーの長期的なセキュリティ認証情報（パスワード、アクセスキー、Amazon CloudFront のキーペア、SSH パブリックキー、X.509 証明書）を管理できます。

このようなユーザー認証情報の管理に加え、Multi-Factor Authentication (MFA) を義務づけることで、AWS への IAM ユーザーアクセスのセキュリティをさらに強化できます。

AWS における長期的なセキュリティ認証情報の使用の詳細については、AWS セキュリティの認証情報を参照してください。

<https://docs.aws.amazon.com/general/latest/gr/aws-security-credentials.html>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、利用者が個人所有する機器によるサービス利用に関する対応策については、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

サービス仕様適合開示書に、以下の内容を参考に記載する必要があります。

#### - 利用者が所有する機器からの情報漏えい等を防止する観点

- ・仮想デスクトップを用いて OS レベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにする

- ・モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すこと

- ・医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ること等

#### ■ 推奨される追加の実施事項

利用者の ID／アクセス権の管理、利用端末（デバイス）と交換情報に対するセキュリティ保護対策と管理のプロセス導入の必要があります。

#### ■ 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.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

---

### 3.2.7

#### 情報及び情報機器の持ち出しについての安全管理対策

##### (ウ) 5 公衆無線 LAN の利用禁止

##### ■ ガイドラインとして必要な要求事項 Seq. 230

---

##### ①

業務上、サービスに関する情報を格納するモバイル端末を持ち出す場合には、公衆無線 LAN への接続は行わない。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、業務上、サービスに関する情報を格納するモバイル端末を持ち出す場合には、公衆無線 LAN への接続は行わないよう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)

N/A

---

---



### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (ア) 1

##### 障害時の責任分界

##### ■ ガイドラインとして必要な要求事項 Seq. 231

---

##### ①

障害等が生じた場合の責任分界を明確にした上で、稼動を保証するサービスの範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

お客様と AWS の責任共有モデルは、IT 統制、セキュリティとコンプライアンスの責任は、AWS とお客様の間で共有されます。この共有モデルでは、ホストオペレーティングシステムや仮想化レイヤーから、サービスが運用されている施設の物理的なセキュリティまで、さまざまなコンポーネントを AWS が運用、管理、統制することにより、お客様の運用上の負担が軽減されます。一方、お客様は、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を含む）と関連する他のアプリケーションソフトウェアの管理、ならびに AWS から提供されるセキュリティグループファイアウォールの構成に責任を負います。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、適用される法規によって異なるため、お客様は選択するサービスを慎重に検討する必要があります。また、この責任共有モデルの性質によって、お客様がデプロイを柔軟に管理できます。以下の図に示すように、この責任の相違は、通常、クラウド "の" セキュリティ、およびクラウド "における" セキュリティと表現されます。

IT 環境を運用する責任が AWS とお客様の間で共有されることと同様、IT 統制の管理、運用、検証も共有されます。AWS 環境にデプロイされた物理インフラストラクチャーに関連した統制をそれまでお客様が管理していた場合は、AWS が管理することで、お客様にかかる統制運用の負荷を軽減できます。お客様によって AWS のデプロイ方法は異なるため、特定の IT 統制の管理を AWS に移行して、(新しい) 分散統制環境を構築するかどうかはお客様が決定できます。構築後は、必要に応じて、AWS の統制およびコンプライアンスに関する文書を参照し、統制の評価と検証の手順を実行できます。

詳細は以下を参照ください。

<https://aws.amazon.com/jp/compliance/shared-responsibility-model/>

##### ■ AWS サービス関連情報

AWS では、障害耐性を高める為に、リージョンとアベイラビリティゾーンという仕組みを用意しています。

インスタンスは、リージョンと呼ばれる複数の地理的場所にプロビジョニングできます。

各リージョンには複数のアベイラビリティゾーンがあります。アベイラビリティゾーンは物理的に明確に区切られた領域であり、他のゾーンの障害の影響を受けないように設計されています。アベイラビリティゾーンは、同じリージョン内の他のゾーンに低価格かつ低レイテンシーのネットワーク接続を提供します。個別のゾーンでインスタンスを作成することにより、障害がアベイラビリティゾーン全体に影響を及ぼすことを防ぎ、アプリケーションを保護することができます。高可用性を実現

する場合は、2 つ以上のアベイラビリティゾーンにまたがるようにリソースをデプロイを設計してください。

事業継続および災害対策（BC/DR）ポリシーに関連するツールについては、ユーザー側で用意する必要があります。  
AWS リージョンを使用して、ネットワークレイテンシーおよび規制コンプライアンスを管理します。特定のリージョンに保存されたデータは、そのリージョンの外部にはレプリケートされません。ビジネス上のニーズによりデータを異なるリージョンにレプリケートする必要がある場合は、お客様の責任において行います。

AWS は、各リージョンが存在する国および州（該当する場合）に関する情報を提供します。お客様は、コンプライアンスおよびネットワークレイテンシーの要件を考慮して、データを保存するリージョンを選択する必要があります。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、障害等が生じた場合の責任分界を明確にした上で、稼動を保証するサービスの範囲について、サービス仕様適合開示書に基づき、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

稼働するアプリケーション（システム）に求められる可用性SLAに沿って、AWSの提供するサービスの選択、複数のアベイラビリティゾーンやリージョンを利用、及び復旧方法も考慮します。

広域災害などを想定した DR 向けに複数のリージョンを利用する場合には、利用ユーザー側からのアクセス手段と経路についても、復旧プロセスの中に含めておく必要があります。

#### ■ 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.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.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.16.1.1

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

---

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (ア) 2

#### 医療機関への情報提供

##### ■ ガイドラインとして必要な要求事項 Seq. 232

---

###### ①

医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、サービス仕様適合開示書に基づき、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

通常時、AWS Direct Connect を利用したプライベートネットワークの利用であっても、利用者側の被災ケースを勘案し、インターネット接続の環境を準備しておく必要があります。アクセスの有効化の手順や時期については、BCP で規定します。

非常時に利用するアカウントが必要な場合、AWS Organizations と IAM を利用し、アカウントの登録／削除に対応します。

IAM にて、AWS リソースを管理するためにコンソールへのアクセス権が必要な特権管理者と、AWS のコンテンツへのアクセス権が必要なエンドユーザーの 2 つにいて、通常と災害非常時のアカウント登録／削除の手順・体制を勘案しておく必要があります。特権管理者が被災する場合も考えられる為、BCP 体制としても特権管理者の体制定義には注意が必要です。

##### ■ 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.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.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.16.1.1

## 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

---

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (ア) 3

#### 外部ファイル等の出力

##### ■ ガイドラインとして必要な要求事項 Seq. 233

---

##### ①

医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、サービス仕様適合開示書に基づき、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

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.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.11.2

#### 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.16.1.1

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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (ア) 4

##### 遠隔地のバックアップに関する見読性

##### ■ ガイドラインとして必要な要求事項 Seq. 234

---

##### ①

医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

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見読性が確保可能な代替手段を検討する必要があります。

広域災害を想定した別リージョンの選定とバックアップシステムとデータ複製の確保を行う場合、クラウドサービス事業者は情報処理サービスの継続の為、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.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.11.2

## 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.16.1.1

## 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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (ア) 5 見読性の確保の支援機能

##### ■ ガイドラインとして必要な要求事項 Seq. 235

---

###### ①

緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等）をサービスに含めること及びこれに必要なセキュリティ等の情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

N/

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等）をサービスに含めること及びこれに必要なセキュリティ等の情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

クラウドサービス事業者は、BCP（障害時・災害時復旧手順）を作成することで、障害または災害等により正常に稼働しなくなったコンピュータシステムを復旧させるための手続きを明確にします。併せて、バックアップシステムへの切り替え時の社内システムへの影響確認、切り戻しについて考慮します。データセンター側の被災と、利用者側の被災の2つの要素があり、いずれか、または両方を含むケースについて計画に勘案する必要があります。

##### ■ 推奨される追加の実施事項

通常時、AWS Direct Connect を利用したプライベートネットワークの利用であっても、利用者側の被災ケースを勘案し、インターネット接続の環境を準備しておく必要があります。アクセスの有効化の手順や時期については、BCP で規定します。

非常時に利用するアカウントが必要な場合、AWS Organizations と IAM を利用し、アカウントの登録／削除に対応します。

IAM にて、AWS リソースを管理するためにコンソールへのアクセス権が必要な特権管理者と、AWS のコンテンツへのアクセス権が必要なエンドユーザーの2つについて、通常と災害非常時のアカウント登録／削除の手順・体制を勘案しておく必要があります。特権管理者が被災する場合も考えられる為、BCP 体制としても特権管理者の体制定義には注意が必要です。

##### ■ 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.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.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.16.1.1

## 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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 1BCP 等の策定

##### ■ ガイドラインとして必要な要求事項 Seq. 236

---

###### ①

サービスに係る BCP 及びコンテンジェンシープランの策定を行う。

##### ■ AWS のインフラストラクチャー関連事項

AWS の BCP（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、感染症の爆発的な流行の脅威に対して迅速に対応するための準備として、パンデミック対応ポリシーと手順を災害復旧計画に組み込んでいます。関連したリスクに関する軽減のための戦略には、重要なプロセスをリージョン外のリソースに移動するために、どのようにスタッフを配置するかという代替モデルと、重要なビジネス業務をサポートするための危機管理の発動計画が含まれます。パンデミック計画は、国際的な健康関連機関や規制に従っていますが、国際的な関連機関との連絡窓口等も含まれています。

Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながら、システムまたはハードウェア障害に耐えられるように設計されています。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、複数のグローバルに展開されたリージョンに、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分けられており、洪水に対して低リスクの地域に存在しています。（具体的な洪水の地域に関する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接続しています。複数のリージョンやアベイラビリティゾーンを利用したシステム設計を実施することは重要です。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場合でもレジリエンスを保つことが可能です。

##### ■ AWS サービス関連情報

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。より詳細な情報を必要とするお客様は AWS のセールス担当者、あるいは <https://aws.amazon.com/jp/compliance/contact/> から AWS までご連絡ください。

障害発生時のフェイルオーバー時には、アクセス管理の一貫で DNS について考慮が必要です。

Amazon Route 53 は、可用性が高くスケーラブルなクラウドドメインネームシステム (DNS) ウェブサービスです。Amazon Route 53 は、www.example.com のような名前を、コンピュータが互いに接続するための数字の IP アドレス (192.0.2.1 など) に変換するサービスで、開発者や企業がエンドユーザーをインターネットアプリケーションにルーティングする、きわめて信頼性が高く、コスト効率の良い方法となるよう設計されています。Amazon Route 53 は IPv6 にも完全準拠しています。

詳しくは、以下を参照ください。

<https://aws.amazon.com/jp/route53/>

Elastic Load Balancing は、アプリケーションへのトラフィックを複数のターゲット (Amazon EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散します。Elastic Load Balancing は、変動するアプリケーショントラフィックの負荷を、1 つのアベイラビリティゾーンまたは複数のアベイラビリティゾーンで処理できます。Elastic Load Balancing では、3 種類のロードバランサーが用意されています。これらはすべて、アプリケーションの耐障害性を高めるのに必要な高い可用性、自動スケーリング、堅牢なセキュリティを特徴としています。

詳しくは、以下を参照ください。

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

#### ■ クラウドサービス事業者 (お客様) の該当事項

クラウドサービス事業者は、サービスに係る BCP 及びコンテンジェンシープランの策定を行う必要があります。

#### ■ 推奨される追加の実施事項

AWS の複数のアベイラビリティゾーンやリージョンを利用した復旧も考慮します。

また、災害時に重要なデータのバックアップ・リストア可能とするようなデータのマイグレーションやストレージをサポートする AWS サービスとその機能の使用について考慮いただくことは非常に重要です。スケールダウンした形で、あるいは本番環境と同様のスケールで AWS 環境上に DR サイトを構築する場合には、コンピューティングリソースがどのぐらい必要になるかといったことも同様に考慮が必要となります。さらに災害時に重要な点としては、AWS 環境上でコンピューティングリソースをどのように素早く立ち上げるのかといったことや、AWS 環境上ですでに稼働している DR システムに対してどのようにフェイルオーバーを実施するのか、といったことも挙げられます。

#### ■ 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.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.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.16.1.1

## 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

---

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 1

##### BCP 等の策定

##### ■ ガイドラインとして必要な要求事項 Seq. 237

---

##### ②

①で策定する BCP 及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。

##### ■ AWS のインフラストラクチャー関連事項

AWS の BCP（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、感染症の爆発的な流行の脅威に対して迅速に対応するための準備として、パンデミック対応ポリシーと手順を災害復旧計画に組み込んでいます。関連したリスクに関する軽減のための戦略には、重要なプロセスをリージョン外のリソースに移動するために、どのようにスタッフを配置するかという代替モデルと、重要なビジネス業務をサポートするための危機管理の発動計画が含まれます。パンデミック計画は、国際的な健康関連機関や規制に従っていますが、国際的な関連機関との連絡窓口等も含まれています。

Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながら、システムまたはハードウェア障害に耐えられるように設計されています。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、複数のグローバルに展開されたリージョンに、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分けされており、洪水に対して低リスクの地域に存在しています。（具体的な洪水の地域に関する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接続しています。複数のリージョンやアベイラビリティゾーンを利用したシステム設計を実施することは重要です。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場合でもレジリエンスを保つことが可能です。

##### ■ AWS サービス関連情報

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。より詳細な情報を必要とするお客様は AWS のセールス担当者、あるいは <https://aws.amazon.com/jp/compliance/contact/> から AWS までご連絡ください。

障害発生時のフェイルオーバー時には、アクセス管理の一貫で DNS について考慮が必要です。

Amazon Route 53 は、可用性が高くスケーラブルなクラウドドメインネームシステム (DNS) ウェブサービスです。Amazon Route 53 は、www.example.com のような名前を、コンピュータが互いに接続するための数字の IP アドレス (192.0.2.1 など) に変換するサービスで、開発者や企業がエンドユーザーをインターネットアプリケーションにルーティングする、きわめて信頼性が高く、コスト効率の良い方法となるよう設計されています。Amazon Route 53 は IPv6 にも完全準拠しています。

詳しくは、以下を参照ください。

<https://aws.amazon.com/jp/route53/>

Elastic Load Balancing は、アプリケーションへのトラフィックを複数のターゲット (Amazon EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散します。Elastic Load Balancing は、変動するアプリケーショントラフィックの負荷を、1 つのアベイラビリティゾーンまたは複数のアベイラビリティゾーンで処理できます。Elastic Load Balancing では、3 種類のロードバランサーが用意されています。これらはすべて、アプリケーションの耐障害性を高めるのに必要な高い可用性、自動スケーリング、堅牢なセキュリティを特徴としています。

詳しくは、以下を参照ください。

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

#### ■ クラウドサービス事業者 (お客様) の該当事項

クラウドサービス事業者は、サービスに係る BCP 及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める必要があります。

#### ■ 推奨される追加の実施事項

AWS の複数のアベイラビリティゾーンやリージョンを利用した復旧も考慮します。

また、災害時に重要なデータのバックアップ・リストア可能とするようなデータのマイグレーションやストレージをサポートする AWS サービスとその機能の使用について考慮いただくことは非常に重要です。スケールダウンした形で、あるいは本番環境と同様のスケールで AWS 環境上に DR サイトを構築する場合には、コンピューティングリソースがどのぐらい必要になるかといったことも同様に考慮が必要となります。さらに災害時に重要な点としては、AWS 環境上でコンピューティングリソースをどのように素早く立ち上げるのかといったことや、AWS 環境上ですでに稼働している DR システムに対してどのようにフェイルオーバーを実施するのか、といったことも挙げられます。

#### ■ 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.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.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.16.1.1

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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 1

##### BCP 等の策定

##### ■ ガイドラインとして必要な要求事項 Seq. 238

---

##### ③

①で策定した BCP 及びコンテンジェンシープランに基づくサービス内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

AWS の BCP（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、感染症の爆発的な流行の脅威に対して迅速に対応するための準備として、パンデミック対応ポリシーと手順を災害復旧計画に組み込んでいます。関連したリスクに関する軽減のための戦略には、重要なプロセスをリージョン外のリソースに移動するために、どのようにスタッフを配置するかという代替モデルと、重要なビジネス業務をサポートするための危機管理の発動計画が含まれます。パンデミック計画は、国際的な健康関連機関や規制に従っていますが、国際的な関連機関との連絡窓口等も含まれています。

Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながら、システムまたはハードウェア障害に耐えられるように設計されています。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、複数のグローバルに展開されたリージョンに、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分けされており、洪水に対して低リスクの地域に存在しています。（具体的な洪水の地域に関する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接続しています。複数のリージョンやアベイラビリティゾーンを利用したシステム設計を実施することは重要です。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場合でもレジリエンスを保つことが可能です。

##### ■ AWS サービス関連情報

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。より詳細な情報を必要とするお客様は AWS のセールス担当者、あるいは <https://aws.amazon.com/jp/compliance/contact/> から AWS までご連絡ください。

障害発生時のフェイルオーバー時には、アクセス管理の一貫で DNS について考慮が必要です。

Amazon Route 53 は、可用性が高くスケーラブルなクラウドドメインネームシステム (DNS) ウェブサービスです。Amazon Route 53 は、www.example.com のような名前を、コンピュータが互いに接続するための数字の IP アドレス (192.0.2.1 など) に変換するサービスで、開発者や企業がエンドユーザーをインターネットアプリケーションにルーティングする、きわめて信頼性が高く、コスト効率の良い方法となるよう設計されています。Amazon Route 53 は IPv6 にも完全準拠しています。

詳しくは、以下を参照ください。

<https://aws.amazon.com/jp/route53/>

Elastic Load Balancing は、アプリケーションへのトラフィックを複数のターゲット (Amazon EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散します。Elastic Load Balancing は、変動するアプリケーショントラフィックの負荷を、1 つのアベイラビリティゾーンまたは複数のアベイラビリティゾーンで処理できます。Elastic Load Balancing では、3 種類のロードバランサーが用意されています。これらはすべて、アプリケーションの耐障害性を高めるのに必要な高い可用性、自動スケーリング、堅牢なセキュリティを特徴としています。

詳しくは、以下を参照ください。

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

#### ■ クラウドサービス事業者 (お客様) の該当事項

クラウドサービス事業者は、BCP 及びコンテンジェンシープランに基づくサービス内容について、サービス仕様適合開示書に基づき、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

AWS の複数のアベイラビリティゾーンやリージョンを利用した復旧も考慮します。

また、災害時に重要なデータのバックアップ・リストア可能とするようなデータのマイグレーションやストレージをサポートする AWS サービスとその機能の使用について考慮いただくことは非常に重要です。スケールダウンした形で、あるいは本番環境と同様のスケールで AWS 環境上に DR サイトを構築する場合には、コンピューティングリソースがどのぐらい必要になるかといったことも同様に考慮が必要となります。さらに災害時に重要な点としては、AWS 環境上でコンピューティングリソースをどのように素早く立ち上げるのかといったことや、AWS 環境上ですでに稼働している DR システムに対してどのようにフェイルオーバーを実施するのか、といったことも挙げられます。

#### ■ 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.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.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.16.1.1

## 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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 2

##### 非常時のサービスの運用

##### ■ ガイドラインとして必要な要求事項 Seq. 239

---

###### ①

非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

緊急時においても、利用者に対する情報利用のサービスに基本的に違いはありません。災害対策時におけるアクセス手段／経路とアカウント管理のプロセスにより、必要なセキュリティ要件を満たします。

サイト障害や広域災害向けに利用可能な複数のアベイラビリティゾーンやリージョンを用意しています。

利用者視点では、別リージョンへのアクセス手段や経路について予め利用者側プロセスとして配慮ください。

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

被災時に別リージョンを使うケースでは、個々のサービスやアクセスについては、通常時提供されるものと何ら違いはありません。もし、被災時に限定した特別なアカウントの作成をする必要がある場合には、以下の機能を活用した管理・運用が可能です。

**IAM ユーザーとアクセス権の管理** - IAM でユーザーを作成し、ユーザーに個別のセキュリティ認証情報（アクセスキー、パスワード、多要素認証 デバイス）を割り当てるか一時的セキュリティ認証情報をリクエストすることによって、AWS のサ

ービスやリソースへのアクセス権をユーザーに付与します。ユーザーにどの操作の実行を許可するかを、管理者がコントロールできます。IAM ユーザーは次のユーザーになることができます。

- ・AWS リソースを管理するためにコンソールへのアクセス権が必要な特権管理者。
- ・AWS のコンテンツへのアクセス権が必要なエンドユーザー。
- ・AWS のデータにプログラムでアクセスする権限が必要なシステム担当者。

AWS Organizations は、作成し一元管理する組織に、複数の AWS アカウントを統合するためのアカウント管理サービスです。AWS Organizations には、利用者のビジネスの予算、セキュリティ、コンプライアンスのニーズをより適切に満たせるように一括請求およびアカウント管理機能が備わっています。アカウントを組織単位（OU）にグループ化し、各 OU に異なるアクセスポリシーをアタッチすることができます。

AWS Identity and Access Management (IAM) でユーザーを作成し、ユーザーに個別のセキュリティ認証情報（アクセスキー、パスワード、多要素認証 デバイス）を割り当てるか一時的セキュリティ認証情報をリクエストすることによって、AWS のサービスやリソースへのアクセス権をユーザーに付与します。ユーザーにどの操作の実行を許可するかを、管理者がコントロールできます。IAM ユーザーは次のユーザーになることができます。IAM の詳細については、<https://aws.amazon.com/iam/> のウェブサイトを参照してください。

AWS Organizations の組織単位（OU） 内に 5 レベルまでネストできるため、アカウントグループを柔軟に構成できます。AWS Organizations の詳細については、<https://docs.aws.amazon.com/organizations/> のウェブサイト参照してください。

ユーザーは AWS Organizations ポリシーと IAM ポリシーの両方で許可されているものだけにアクセスできます。どちらかがオペレーションをブロックすると、ユーザーはそのオペレーションにアクセスできません。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、サービス仕様適合開示書に基づき、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

通常時、AWS Direct Connect を利用したプライベートネットワークの利用であっても、利用者側の被災ケースを勘案し、インターネット接続の環境を準備しておく必要があります。アクセスの有効化の手順や時期については、BCP で規定します。

非常時に利用するアカウントが必要な場合、AWS Organizations と IAM を利用し、アカウントの登録／削除に対応します。

IAM にて、AWS リソースを管理するためにコンソールへのアクセス権が必要な特権管理者と、AWS のコンテンツへのアクセス権が必要なエンドユーザーの 2 つにいて、通常と災害非常時のアカウント登録／削除の手順・体制を勘案して

おく必要があります。特権管理者が被災する場合も考えられる為、BCP 体制としても特権管理者の体制定義には注意が必要です。

■ 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.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.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.16.1.1

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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 2

##### 非常時のサービスの運用

##### ■ ガイドラインとして必要な要求事項 Seq. 240

---

##### ②

非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。

##### ■ AWS のインフラストラクチャー関連事項

緊急時においても、利用者に対する情報利用のサービスに基本的に違いはありません。災害対策時におけるアクセス手段／経路とアカウント管理のプロセスにより、必要なセキュリティ要件を満たします。

サイト障害や広域災害向けに利用可能な複数のアベイラビリティゾーンやリージョンを用意しています。

利用者視点では、別リージョンへのアクセス手段や経路について予め利用者側プロセスとして配慮ください。

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

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し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、および運用状態の統合的な確認を行うことができます。CloudWatch では、モニタリングデータと運用データをログ、メトリクス、イベントという形で収集し、AWS やオンプレミスサーバーで作動する AWS リソース、アプリケーション、およびサービスを統合的に提供できます。CloudWatch を使用して、高解像度アラームの設定、ログとメトリクスの並列的な可視化、自動化



したアクションの実行、問題のトラブルシューティング、およびインサイトの発見を行うことができます。これにより、アプリケーションを最適化し、スムーズに実行することができます。

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、および運用とリスクの監査を行えるように支援する AWS のサービスです。ユーザー、ロール、または AWS のサービスによって実行されたアクションは、CloudTrail にイベントとして記録されます。イベントには、AWS マネジメントコンソール、AWS Command Line Interface、および AWS SDK と API で実行されたアクションが含まれます。

CloudTrail は、作成時に AWS アカウントで有効になります。AWS アカウントでアクティビティが発生した場合、そのアクティビティは CloudTrail イベントに記録されます。CloudTrail コンソールで、[イベント履歴] に移動して簡単に最近のイベントを表示できます。AWS アカウントのアクティビティおよびイベントの継続的な記録については、「証跡を作成する」を参照してください。

AWS アカウントアクティビティの可視性は、セキュリティと運用のベストプラクティスにおける重要な側面です。CloudTrail を使用して、AWS インフラストラクチャ全体のアカウントアクティビティを表示、検索、ダウンロード、アーカイブ、分析、応答できます。アクションを実行したユーザーやアプリケーション、対象のリソース、イベントの発生日時、およびその他の詳細情報を識別して、AWS アカウントのアクティビティの分析と対応に役立てることができます。

API を使用して CloudTrail をアプリケーションに統合したり、組織用の証跡の作成を自動化したり、作成した証跡の状態を確認したり、CloudTrail イベントをユーザーが表示する方法を制御したりすることもできます。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う必要があります。

#### ■ 推奨される追加の実施事項

AWS CloudTrailとCloud Watchを利用した災害対策中の監視アカウント／イベントの管理体制とプロセスを準備します。

#### ■ 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.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.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.16.1.1

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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 2

##### 非常時のサービスの運用

##### ■ ガイドラインとして必要な要求事項 Seq. 241

---

##### ③

非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。

##### ■ AWS のインフラストラクチャー関連事項

緊急時においても、利用者に対する情報利用のサービスに基本的に違いはありません。災害対策時におけるアクセス手段／経路とアカウント管理のプロセスにより、必要なセキュリティ要件を満たします。

サイト障害や広域災害向けに利用可能な複数のアベイラビリティゾーンやリージョンを用意しています。

利用者視点では、別リージョンへのアクセス手段や経路について予め利用者側プロセスとして配慮ください。

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

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し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、および運用状態の統合的な確認を行うことができます。CloudWatch では、モニタリングデータと運用データをログ、メトリクス、イベントという形で収集し、AWS やオンプレミスサーバーで作動する AWS リソース、アプリケーション、およびサービスを統合的に提供できます。CloudWatch を使用して、高解像度アラームの設定、ログとメトリクスの並列的な可視化、自動化

したアクションの実行、問題のトラブルシューティング、およびインサイトの発見を行うことができます。これにより、アプリケーションを最適化し、スムーズに実行することができます。

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、および運用とリスクの監査を行えるように支援する AWS のサービスです。ユーザー、ロール、または AWS のサービスによって実行されたアクションは、CloudTrail にイベントとして記録されます。イベントには、AWS マネジメントコンソール、AWS Command Line Interface、および AWS SDK と API で実行されたアクションが含まれます。

CloudTrail は、作成時に AWS アカウントで有効になります。AWS アカウントでアクティビティが発生した場合、そのアクティビティは CloudTrail イベントに記録されます。CloudTrail コンソールで、[イベント履歴] に移動して簡単に最近のイベントを表示できます。AWS アカウントのアクティビティおよびイベントの継続的な記録については、「証跡を作成する」を参照してください。

AWS アカウントアクティビティの可視性は、セキュリティと運用のベストプラクティスにおける重要な側面です。CloudTrail を使用して、AWS インフラストラクチャ全体のアカウントアクティビティを表示、検索、ダウンロード、アーカイブ、分析、応答できます。アクションを実行したユーザーやアプリケーション、対象のリソース、イベントの発生日時、およびその他の詳細情報を識別して、AWS アカウントのアクティビティの分析と対応に役立てることができます。

API を使用して CloudTrail をアプリケーションに統合したり、組織用の証跡の作成を自動化したり、作成した証跡の状態を確認したり、CloudTrail イベントをユーザーが表示する方法を制御したりすることもできます。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる必要があります。

#### ■ 推奨される追加の実施事項

AWS CloudTrailとCloud Watchを利用した災害対策中の監視アカウント／イベントの管理体制とプロセスを準備します。

#### ■ 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.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.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.16.1.1

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

---

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 2

##### 非常時のサービスの運用

##### ■ ガイドラインとして必要な要求事項 Seq. 242

---

##### ④

非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。

##### ■ AWS のインフラストラクチャー関連事項

緊急時においても、利用者に対する情報利用のサービスに基本的に違いはありません。災害対策時におけるアクセス手段／経路とアカウント管理のプロセスにより、必要なセキュリティ要件を満たします。

サイト障害や広域災害向けに利用可能な複数のアベイラビリティゾーンやリージョンを用意しています。

正常復帰（切り戻し）後に、サービス停止するものがあれば、当該期間の記録（ログ）を確認をして、必要な対処が可能です。

##### ■ AWS サービス関連情報

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、および運用とリスクの監査を行えるように支援する AWS のサービスです。ユーザー、ロール、または AWS のサービスによって実行されたアクションは、CloudTrail にイベントとして記録されます。イベントには、AWS マネジメントコンソール、AWS Command Line Interface、および AWS SDK と API で実行されたアクションが含まれます。

CloudTrail は、作成時に AWS アカウントで有効になります。AWS アカウントでアクティビティが発生した場合、そのアクティビティは CloudTrail イベントに記録されます。CloudTrail コンソールで、[イベント履歴] に移動して簡単に最近のイベントを表示できます。AWS アカウントのアクティビティおよびイベントの継続的な記録については、「証跡を作成する」を参照してください。

AWS アカウントアクティビティの可視性は、セキュリティと運用のベストプラクティスにおける重要な側面です。CloudTrail を使用して、AWS インフラストラクチャ全体のアカウントアクティビティを表示、検索、ダウンロード、アーカイブ、分析、応答できます。アクションを実行したユーザーやアプリケーション、対象のリソース、イベントの発生日時、およびその他の詳細情報を識別して、AWS アカウントのアクティビティの分析と対応に役立てることができます。

API を使用して CloudTrail をアプリケーションに統合したり、組織用の証跡の作成を自動化したり、作成した証跡の状態を確認したり、CloudTrail イベントをユーザーが表示する方法を制御したりすることもできます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等と合意する基準に基づいて、BCP（障害時・災害時復旧手順）を作成し、その中で、災害時のアクセス手段と非常用アカウントについて、正常復帰後、速やかに無効化を図る必要があります。

■ 推奨される追加の実施事項

被災時の対処期間に相当する記録（ログ）を CloudTrail を使って確認し、復旧切り戻し作業の一貫で必要な対処を BCP プロセスとして定めておく必要があります。

■ 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.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.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.16.1.1

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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 3

#### サイバー攻撃等への対応

##### ■ ガイドラインとして必要な要求事項 Seq. 243

---

###### ①

サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。

##### ■ AWS のインフラストラクチャー関連事項

AWS はインターネット上の攻撃を防ぎ、高可用性・セキュリティの確保および回復力を得られるように、ツール・ベストプラクティスおよびサービスを提供することをお約束します。私達は最近、2018 年版の DDoS に対する AWS のベストプラクティス（英語のみ）のホワイトペーパーをリリースしました。今回のアップデートでは、DDoS 攻撃への対策を強化するのに役立つ、以下の新しく開発された AWS サービスを考慮に入れています：

このホワイトペーパーは、DDoS 攻撃に対する回復力のあるアプリケーションを構築するための規範的な DDoS ガイダンスを提供します。ボリューム型攻撃やアプリケーション層に対する攻撃など、さまざまな攻撃タイプを紹介し、各攻撃タイプを管理する上で最も効果的なベストプラクティスを説明します。また、DDoS 緩和戦略に適合するサービスや機能および、それぞれがどのようにアプリケーションを保護するのに役立つのかについて要点を説明します。

詳しくは、以下を参照ください。

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/DDoS\\_White\\_Paper\\_JP.pdf](https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/DDoS_White_Paper_JP.pdf)

##### ■ AWS サービス関連情報

Elastic Load Balancing や Amazon Elastic Compute (EC2) などの AWS リージョン内で利用できるサービスを利用することで、所定のリージョン内で DDoS 攻撃に対する高い耐性を持ち、予期しないトラフィック量に対処できるように拡張するシステムを構築することができます。Amazon CloudFront、AWS WAF、Amazon Route53、Amazon API Gateway などの AWS エッジロケーションで利用できるサービスを利用することで、エッジロケーションのグローバルネットワークを活用し、アプ

リケーションの耐障害性を向上させつつ大量のトラフィックに対応することができます。このようなサービスを利用してインフラストラクチャ層とアプリケーション層への DDoS 攻撃に対する耐性を高める事ができます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる必要があります。

##### ■ 推奨される追加の実施事項

2018 年版の DDoS に対する AWS のベストプラクティス（英語のみ）のホワイトペーパーは、DDoS 攻撃に対する回復力のあるアプリケーションを構築するための規範的な DDoS ガイダンスを提供されています。ボリューム型攻撃や



アプリケーション層に対する攻撃など、さまざまな攻撃タイプを紹介され、各攻撃タイプを管理する上で最も効果的なベストプラクティスの説明がされています。こちらに、そった準備をします。

詳しくは、[https://d1.awsstatic.com/whitepapers/Security/DDoS\\_White\\_Paper.pdf](https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf) の原文を参照ください。

## ■ 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.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.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.16.1.1

#### 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



### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 3 サイバー攻撃等への対応

##### ■ ガイドラインとして必要な要求事項 Seq. 244

---

##### ②

①の場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。

##### ■ AWS のインフラストラクチャー関連事項

AWS はインターネット上の攻撃を防ぎ、高可用性・セキュリティの確保および回復力を得られるように、ツール・ベストプラクティスおよびサービスを提供することをお約束します。私達は最近、2018 年版の DDoS に対する AWS のベストプラクティス（英語のみ）のホワイトペーパーをリリースしました。今回のアップデートでは、DDoS 攻撃への対策を強化するのに役立つ、以下の新しく開発された AWS サービスを考慮に入れています：

このホワイトペーパーは、DDoS 攻撃に対する回復力のあるアプリケーションを構築するための規範的な DDoS ガイドンスを提供します。ボリューム型攻撃やアプリケーション層に対する攻撃など、さまざまな攻撃タイプを紹介し、各攻撃タイプを管理する上で最も効果的なベストプラクティスを説明します。また、DDoS 緩和戦略に適合するサービスや機能および、それぞれがどのようにアプリケーションを保護するのに役立つのかについて要点を説明します。

詳しくは、以下を参照ください。

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/DDoS\\_White\\_Paper\\_JP.pdf](https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/DDoS_White_Paper_JP.pdf)

##### ■ AWS サービス関連情報

Elastic Load Balancing や Amazon Elastic Compute (EC2) などの AWS リージョン内で利用できるサービスを利用することで、所定のリージョン内で DDoS 攻撃に対する高い耐性を持ち、予期しないトラフィック量に対処できるように拡張するシステムを構築することができます。Amazon CloudFront、AWS WAF、Amazon Route53、Amazon API Gateway などの AWS エッジロケーションで利用できるサービスを利用することで、エッジロケーションのグローバルネットワークを活用し、アプ

リケーションの耐障害性を向上させつつ大量のトラフィックに対応することができます。このようなサービスを利用してインフラストラクチャ層とアプリケーション層への DDoS 攻撃に対する耐性を高める事ができます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サイバー攻撃対応として、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等速やかに報告を行う必要があります。

##### ■ 推奨される追加の実施事項

Ddosに限らずサイバー攻撃が多様化・行動化してきており、最新の EDR（Endpoint Detection and Response）による攻撃検出と対応の追加配備が推奨される。

■ 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.11.2

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.16.1.1

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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 3

##### サイバー攻撃等への対応

##### ■ ガイドラインとして必要な要求事項 Seq. 245

---

##### ③

①の場合において、医療機関等が行う必要のある所管官庁への連絡・報告のために提供する資料の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関と合意する。

##### ■ AWS のインフラストラクチャー関連事項

AWS はインターネット上の攻撃を防ぎ、高可用性・セキュリティの確保および回復力を得られるように、ツール・ベストプラクティスおよびサービスを提供することをお約束します。私達は最近、2018 年版の DDoS に対する AWS のベストプラクティス（英語のみ）のホワイトペーパーをリリースしました。今回のアップデートでは、DDoS 攻撃への対策を強化するのに役立つ、以下の新しく開発された AWS サービスを考慮に入れています：

このホワイトペーパーは、DDoS 攻撃に対する回復力のあるアプリケーションを構築するための規範的な DDoS ガイドンスを提供します。ボリューム型攻撃やアプリケーション層に対する攻撃など、さまざまな攻撃タイプを紹介し、各攻撃タイプを管理する上で最も効果的なベストプラクティスを説明します。また、DDoS 緩和戦略に適合するサービスや機能および、それぞれがどのようにアプリケーションを保護するのに役立つのかについて要点を説明します。

詳しくは、以下を参照ください。

[https://d1.awsstatic.com/whitepapers/compliance/JP\\_Whitepapers/DDoS\\_White\\_Paper\\_JP.pdf](https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/DDoS_White_Paper_JP.pdf)

##### ■ AWS サービス関連情報

Elastic Load Balancing や Amazon Elastic Compute (EC2) などの AWS リージョン内で利用できるサービスを利用することで、所定のリージョン内で DDoS 攻撃に対する高い耐性を持ち、予期しないトラフィック量に対処できるように拡張するシステムを構築することができます。Amazon CloudFront、AWS WAF、Amazon Route53、Amazon API Gateway などの AWS エッジロケーションで利用できるサービスを利用することで、エッジロケーションのグローバルネットワークを活用し、アプ

リケーションの耐障害性を向上させつつ大量のトラフィックに対応することができます。このようなサービスを利用してインフラストラクチャ層とアプリケーション層への DDoS 攻撃に対する耐性を高める事ができます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サイバー攻撃対応として、医療機関等が行う必要のある所管官庁への連絡・報告のために提供する資料の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関と合意する必要があります。

##### ■ 推奨される追加の実施事項

組織体制としてセキュリティ・オフィサーを置き、セキュリティ対処における計画・実施・監督／監査ができるようにすることが推奨される。セキュリティ監査や報告について、運用プロセスを規定しておく必要があります。

■ 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.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.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.16.1.1

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

### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 3

##### サイバー攻撃等への対応

##### ■ ガイドラインとして必要な要求事項 Seq. 246

---

##### ④

③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の執行が及ぶ場所に設置する。

##### ■ AWS のインフラストラクチャー関連事項

AWSは、世界中のデータセンターにあるサーバーで実行されています。データセンターは、地理的リージョン別に整理されており、各種法令に基づき利用者がサービス稼働させる場所を選択できるように、複数のリージョンとアベイラビリティゾーンを用意しています。

##### ■ AWS サービス関連情報

##### - 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。

詳しくは、以下を参照ください。

<https://aws.amazon.com/jp/about-aws/global-infrastructure/>

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者はサイバー攻撃対応として、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の執行が及ぶ場所に設置する必要があります。

##### ■ 推奨される追加の実施事項

適合させる必要がある法令に基づき、利用するリージョンを選択します。外部公開が不要なリソースについては、AWS Direct Connect や VPN など使って閉域網を構築し、インターネット側とネットワーク的に分離する事が推奨されます。

##### ■ 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

## 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.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.16.1.1

## 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



### 3.2.8

#### 災害等の非常時の対応についての安全管理対策

##### (イ) 4

#### サービス回復後のデータ整合性の確保

##### ■ ガイドラインとして必要な要求事項 Seq. 247

---

##### ①

非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定・検証方法の規定等）を講じる。

##### ■ AWS のインフラストラクチャー関連事項

AWS の BCP（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、世界中のデータセンターにあるサーバーで実行され、どのデータセンターにおいても同様のサービスを利用可能としています。障害発生時に別リージョンへフェイルオーバーした後、正常系への復帰をする場合は、復帰先となるリージョンやアベイラビリティゾーンを指定する事になります。この正常復帰（フェイルバック）の仕組みとしては、フェイルオーバーをもう1度実行する事になります。

##### ■ AWS サービス関連情報

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。より詳細な情報を必要とするお客様は AWS のセールス担当者、あるいは

<https://aws.amazon.com/jp/compliance/contact/> から AWS までご連絡ください。

障害発生時のフェイルオーバー時には、アクセス管理の一貫で DNS について考慮が必要です。

Amazon Route 53 は、可用性が高くスケーラブルなクラウドドメインネームシステム（DNS）ウェブサービスです。

Amazon Route 53 は、www.example.com のような名前を、コンピュータが互いに接続するための数字の IP アドレス（192.0.2.1 など）に変換するサービスで、開発者や企業がエンドユーザーをインターネットアプリケーションにルーティングする、きわめて信頼性が高く、コスト効率の良い方法となるよう設計されています。Amazon Route 53 は IPv6 にも完全準拠しています。

詳しくは、以下を参照ください。

<https://aws.amazon.com/jp/route53/>

Elastic Load Balancing は、アプリケーションへのトラフィックを複数のターゲット（Amazon EC2 インスタンス、コンテナ、IP アドレスなど）に自動的に分散します。Elastic Load Balancing は、変動するアプリケーショントラフィックの負荷を、1 つのアベイラビリティゾーンまたは複数のアベイラビリティゾーンで処理できます。Elastic Load Balancing では、3 種類のロードバランサーが用意されています。これらはすべて、アプリケーションの耐障害性を高めるのに必要な高い可用性、自動スケーリング、堅牢なセキュリティを特徴としています。

詳しくは、以下を参照ください。

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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定・検証方法の規定等）を講じる必要があります。

クラウドサービス事業者は、BCP（障害時・災害時復旧手順）を作成することで、障害または災害等により正常に稼働しなくなったコンピュータシステムを復旧させるための手続きを明確にします。併せて、バックアップシステムへの切り替え時の社内システムへの影響確認、切り戻しについて考慮します。データセンター側の被災と、利用者側の被災の2つの要素があり、いずれか、または両方を含むケースについて計画に勘案する必要があります。

#### ■ 推奨される追加の実施事項

AWS の複数のアベイラビリティゾーンやリージョンを利用した復旧も考慮します。

また、災害時に重要なデータのバックアップ・リストア可能とするようなデータのマイグレーションやストレージをサポートする AWS サービスとその機能の使用について考慮いただくといったことは非常に重要です。スケールダウンした形で、あるいは本番環境と同様のスケールで AWS 環境上に DR サイトを構築する場合には、コンピューティングリソースがどのぐらい必要になるかといったことも同様に考慮が必要となります。さらに災害時に重要な点としては、AWS 環境上でコンピューティングリソースをどのように素早く立ち上げるのかといったことや、AWS 環境上ですでに稼働している DR システムに対してどのようにフェイルオーバーを実施するのか、といったことも挙げられます。

フェイルバックについて専用のサービスが用意されている訳ではないので、もう1度別のリージョン／アベイラビリティゾーンへのフェイルオーバーを実行する事になる為、そのプロセスについても規定しておく必要があります。利用者の BCP ポリシーによっては、最初のフェイルオーバー後は、その環境を正常系として利用継続する事も考えられるので、それも含め BCP/BCM のプロセス規定が重要になります。

データ整合については、限定的な障害で複数のデータソースが存在する場合でなければ、齟齬は発生しませんが、配慮が必要な場合は予めバックアップとリストアについての運用ポリシーとプロセスについて配慮が必要です。

#### ■ 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.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.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.16.1.1

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

### 3.2.9

#### 個人情報を含む医療情報を外部と交換する場合の安全管理対策

##### (ア) 1

#### ネットワーク経路における全般的な安全管理対策

##### ■ ガイドラインとして必要な要求事項 Seq. 248

---

##### ①

ネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を行う。

##### ■ AWS のインフラストラクチャー関連事項

##### アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

Amazon VPC 内のセキュリティ機能には、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。Amazon VPC 内で実行される Amazon EC2 インスタンスは、以下に説明する、ゲスト OS およびパケット盗聴に対する保護に関連するすべての利点を継承します。ただし、Amazon VPC 専用のセキュリティグループを作成する必要があります。お客様が作成した Amazon EC2 のセキュリティグループは、Amazon VPC 内では正常に機能しません。また、Amazon VPC のセキュリティグループには、Amazon EC2 のセキュリティグループにない追加の機能があります。たとえば、インスタンスが起動された後にセキュリティグループを変更したり、標準のプロトコル番号を持つ任意のプロトコル(TCP、UDP、または ICMP だけではなく)を指定したりできます。各 Amazon VPC は、クラウド内の独立したネットワークです。各 Amazon VPC 内のネットワークトラフィックは、他のすべての Amazon VPC から独立しています。各 Amazon VPC の IP アドレス範囲は作成時に選択します。インターネットゲートウェイ、仮想プライベートゲートウェイ、またはその両方を作成し、接続して、外部接続を確立します。これは以下のコントロールの影響を受けます。

##### ■ AWS サービス関連情報

##### Amazon Virtual Private Cloud(Amazon VPC)のセキュリティ

通常、起動する Amazon EC2 インスタンスごとに Amazon EC2 アドレス空間内のパブリック IP アドレスがランダムに割り当てられます。Amazon VPC を使用すると、AWS クラウド内に独立した部分を作成して、特定の範囲内(例: 10.0.0.0/16) のプライベート(RFC 1918)アドレスを持つ Amazon EC2 インスタンスを起動することができます。VPC 内で IP アドレス範囲に基づいて同種のインスタンスをグループ化するサブネットを定義して、インスタンスおよびサブネットに出入りするトラフィックの流れを制御するルーティングとセキュリティを設定することができます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、ネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を行う必要があります。

- AWSとクライアント機器の間のネットワークについて

■ 推奨される追加の実施事項

送信の保護

HTTP または Secure Sockets Layer(SSL)を使用した HTTPS を介して AWS のアクセスポイントに接続できます。SSL は、傍受、改ざん、およびメッセージの偽造から保護するように設計された暗号プロトコルです。

■ 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.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

---

### 3.2.9

#### 個人情報を含む医療情報を外部と交換する場合の安全管理対策

##### (ア) 1

##### ネットワーク経路における全般的な安全管理対策

##### ■ ガイドラインとして必要な要求事項 Seq. 249

---

##### ②

アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置（サーバ証明書の導入等）を行う。

##### ■ AWS のインフラストラクチャー関連事項

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、さらに堅牢な保護を実装することができます。以下にいくつかの例を示します

IP スプーフィング。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。:

##### ■ AWS サービス関連情報

残念ながら、他の E メールシステムを使用すると、スパムの発信者が、E メールヘッダーを改ざんし、元のメールアドレスを偽装して、E メールが別の送信元から送られたように見せかけることができます。これらの問題を軽減するために、Amazon SES は、ユーザーの電子メールアドレスまたはドメインを確認することを要求しています。これにより、ユーザーが電子メールアドレスまたはドメインを所有していることを確認し、別のユーザーがそれを使用できないようにします。ドメインを検証するため、Amazon SES は、ドメインを管理していることの証明として Amazon SES が指定する DNS レコードを送信者がパブリッシュすることを要求します。Amazon SES は定期的にドメインの検証ステータスを見直し、有効でなくなっている場合には検証を取り消します。

Amazon SES では問題あるコンテンツが送られないよう積極的に取り組んでおり、ISP がアマゾンのドメインから受け取るメールは常に高品質です。それゆえに信頼できるメールサービスの発信元として受け取られます。すべての送信における配信性能と信頼性を最大化するために、次の機能があります。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置（サーバ証明書の導入等）を行う必要があります。

##### ■ 推奨される追加の実施事項

他の E メールシステムを使用すると、スパムの発信者が、E メールヘッダーを改ざんし、元のメールアドレスを偽装して、E メールが別の送信元から送られたように見せかけることができます。これらの問題を軽減するために、Amazon SES は、ユーザーの電子メールアドレスまたはドメインを確認することを要求しています。これにより、ユーザーが電子メールアドレスまたはドメインを所有していることを確認し、別のユーザーがそれを使用できないようにします。ドメインを検証するため、

Amazon SES は、ドメインを管理していることの証明として Amazon SES が指定する DNS レコード を送信者がパブリッシュすることを要求します。Amazon SES は定期的にドメインの検証ステータスを見直し、有効でなく なっている場合には検証を取り消します。

Amazon SES では問題あるコンテンツが送られないよう積極的に取り組んでおり、ISP がアマゾンのドメインから受け取る メールは常に高品質です。それゆえに信頼できるメールサービスの発信元として受け取られます。すべての送信における配信性能と信頼性を最大化するために、次の機能があります。

#### ■ 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.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

---

### 3.2.9

#### 個人情報を含む医療情報を外部と交換する場合の安全管理対策

##### (ア) 1 ネットワーク経路における全般的な安全管理対策

##### ■ ガイドラインとして必要な要求事項 Seq. 250

---

##### ③

経路の安全性確保のため、IPSec + IKE への対応や閉域ネットワークへの対応等及びその条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

##### 送信の保護

HTTP または Secure Sockets Layer(SSL)を使用した HTTPS を介して AWS のアクセスポイントに接続できます。SSL は、傍受、改ざん、およびメッセージの偽造から保護するように設計された暗号プロトコルです。

ネットワークセキュリティの追加レイヤーが必要なお客様のために、AWS では Amazon Virtual Private Cloud(VPC)を提供しています。これにより、AWS クラウド内にプライベートサブネットが提供され、Amazon VPC とデータセンターの間に暗号化されたトンネルを提供する IPsec 仮想プライベートネットワーク(VPN)のデバイスを使用できるようになります。VPC の設定オプションの詳細については、後の「Amazon Virtual Private Cloud(Amazon VPC)のセキュリティ」のセクションをご覧ください。

##### ■ AWS サービス関連情報

AWS Direct Connect はプレミスから AWS への専用ネットワーク接続の構築をシンプルにするクラウドサービスソリューションです。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との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を削減し、帯域幅のスループットを向上させ、インターネットベースの接続よりも安定したネットワークエクスペリエンスをお客様に提供することが可能となりました。

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との間に専用のネットワーク接続を確立することができます。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イ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るのです。仮想インターフェイスは、ニーズの変化に合わせて、いつでも設定変更できます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、AWS を含むネットワークの安全性確保の対応について、サービス仕様適合開示書に基づき、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

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.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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

(ア) 1 ネットワーク経路における全般的な安全管理対策

■ ガイドラインとして必要な要求事項 Seq. 251

---

④

ネットワーク経路におけるウイルスや不正なメッセージの混入等の改ざんに対する防護措置に関するクラウドサービス事業者の役割の範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ AWS のインフラストラクチャー関連事項

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、さらに堅牢な保護を実装することができます。以下にいくつかの例を示します

IP スプーフィング。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。:

■ AWS サービス関連情報

AWS Marketplace は、お客様が製品を構築してビジネスを営むために必要なソフトウェアやサービスを見つけ、購入し、移行して、すぐに使用し始められるオンラインストアです。

マーケットプレイスへの訪問者は AWS Marketplace の 1-Click デプロイを使って、事前設定済みのソフトウェアをすばやく起動し、時間単位または月単位の使用量に対する支払いのみで使用できます。料金の請求とお支払いは AWS で処理され、ソフトウェアの利用料金がお客様への AWS 請求書に表示されます。

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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、AWS を含むネットワーク経路におけるウイルスや不正なメッセージの混入等の改ざんに対する防護措置に関する対応についてサービス仕様適合開示書に基づき、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

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.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

---

### 3.2.9

#### 個人情報を含む医療情報を外部と交換する場合の安全管理対策

##### (ア) 1

#### ネットワーク経路における全般的な安全管理対策

##### ■ ガイドラインとして必要な要求事項 Seq. 252

---

##### ⑤

医療機関等がチャネル・セキュリティの確保を閉域ネットワークの採用に期待する場合、サービスの閉域性の範囲に関する情報について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、さらに堅牢な保護を実装することができます。以下にいくつかの例を示します

IP スプーフィング。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。:

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、AWSを含むサービスの閉域性の範囲に関する対応について、サービス仕様適合開示書に基づき、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

#### 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.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



### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 2

医療機関等からのネットワーク経路の確認

#### ■ ガイドラインとして必要な要求事項 Seq. 253

---

##### ①

医療機関等からクラウドサービス事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で経路の確認を行う。

#### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等からクラウドサービス事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で経路の確認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.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

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 2

医療機関等からのネットワーク経路の確認

#### ■ ガイドラインとして必要な要求事項 Seq. 254

---

#### ②

①において、医療機関等が外部接続するサーバ等とクラウドサービス事業者のサーバとの間の相互認証を行う。

#### ■ AWS のインフラストラクチャー関連事項

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

ネットワークサービス

アマゾン ウェブ サービスは幅広いネットワーキングサービスを提供しており、論理的に分離されたネットワークを作成 して定義し、AWS クラウドに対するプライベートネットワーク接続を確立し、高い可用性でスケーラブルな DNS サービス を使用して、低レイテンシーで高速なデータ転送のコンテンツ配信ウェブサービスをエンドユーザーに提供できます

#### ■ AWS サービス関連情報

Amazon Virtual Private Cloud(Amazon VPC)のセキュリティ

通常、起動する Amazon EC2 インスタンスごとに Amazon EC2 アドレス空間内のパブリック IP アドレスがランダムに割り当てられます。Amazon VPC を使用すると、AWS クラウド内に独立した部分を作成して、特定の範囲内(例: 10.0.0.0/16) のプライベート(RFC 1918)アドレスを持つ Amazon EC2 インスタンスを起動することができます。VPC 内で IP アドレス範囲に基づいて同種のインスタンスをグループ化するサブネットを定義して、インスタンスおよびサブネットに出入りするトラフィックの流れを制御するルーティングとセキュリティを設定することができます。

Amazon Elastic Load Balancing のセキュリティ

Amazon Elastic Load Balancing は、Amazon EC2 インスタンス群のトラフィック管理に使用され、インスタンスへのトラフィックをリージョン内のすべての Availability Zone に分散します。Elastic Load Balancing にはオンプレミスのロードバランサーという利点のほかに、以下のようなセキュリティ面でのメリットがあります。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等からクラウドサービス事業者までのネットワークにおいて、医療機関等が外部接続するサーバ等とクラウドサービス事業者のサーバとの間の相互認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

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.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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 2

医療機関等からのネットワーク経路の確認

#### ■ ガイドラインとして必要な要求事項 Seq. 255

---

#### ③

①について、事業者が保守業務を再委託している場合には、事業者と再委託先との接続では、別途なりすましを防止する策を講じる。

#### ■ 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](https://d1.awsstatic.com/whitepapers/International/jp/AWS_Security_Whitepaper.pdf)

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

Amazon 社からの分離

論理的に、AWS 本稼働環境のネットワークは、ネットワークセキュリティ/分離デバイスの複雑な組み合わせによって、Amazon 社内ネットワークから分離しています。AWS クラウドのコンポーネントを維持するためにアクセスする必要がある社内ネットワーク上の AWS 開発者と管理者は AWS 発券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、該当するサービスの所有者によって確認および承認されます。

承認された AWS 担当者は、ネットワーク デバイスやその他のクラウドコンポーネントへのアクセスを制限する拠点ホストを介して AWS ネットワークに接続します。このとき、すべてのアクティビティはセキュリティレビューのために記録されます。拠点ホストへのアクセスには、ホスト上のすべてのユーザーアカウントに対して SSH 公開鍵認証が必要です。AWS 開発者および管理者の論理的アクセスの詳細については、後の「AWS アクセス」をご覧ください。

#### ■ AWS サービス関連情報

N/A

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等からクラウドサービス事業者までのネットワークにおいて、事業者が保守業務を再委託している場合には、事業者と再委託先との接続では、別途なりすましを防止する策を講じる必要があります。

#### ■ 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.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

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 2

医療機関等からのネットワーク経路の確認

#### ■ ガイドラインとして必要な要求事項 Seq. 256

---

#### ④

厚生労働省ガイドライン第 5 版 6.11 C 項の 2 に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、サービス仕様適合開示書に基づき、医療機関等と合意する。

#### ■ AWS のインフラストラクチャー関連事項

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

送信の保護

HTTP または Secure Sockets Layer(SSL)を使用した HTTPS を介して AWS のアクセスポイントに接続できます。SSL は、傍受、改ざん、およびメッセージの偽造から保護するように設計された暗号プロトコルです。

ネットワークセキュリティの追加レイヤーが必要なお客様のために、AWS では Amazon Virtual Private Cloud(VPC)を提供しています。これにより、AWS クラウド内にプライベートサブネットが提供され、Amazon VPC とデータセンターの間に暗号化されたトンネルを提供する IPsec 仮想プライベートネットワーク(VPN)のデバイスを使用できるようになります。VPC の設定オプションの詳細については、後の「Amazon Virtual Private Cloud(Amazon VPC)のセキュリティ」のセクションをご覧ください。

#### ■ AWS サービス関連情報

Amazon CloudFront 独自 SSL

Amazon CloudFront には、ウェブサイト全体を高速化しつつ、CloudFront のどのエッジロケーションからでも HTTPS 経由でコンテンツを安全に配信する 3 つのオプションがあります。エッジロケーションからの安全な配信に加えて、オリジンフェッチ用に HTTPS 接続を使用するよう、CDN を設定することもできます。これにより、お客様のオリジンサーバーとエンドユーザーのエンドツーエンド間でデータが暗号化されます。

デフォルトでは、URL に CloudFront ディストリビューションドメイン名を使用して、コンテンツを HTTPS 接続で視聴者に配信できます (例: <https://dxxxxx.cloudfront.net/image.jpg>)。独自のドメイン名と独自の SSL 証明書を使用して HTTPS 接続でコンテンツを配信する場合は、独自 SSL 証明書機能を使用できます。

<https://aws.amazon.com/jp/cloudfront/custom-ssl-domains/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、厚生労働省ガイドライン第 5 版 6.11「外部と個人情報を含む医療情報を交換する場合の安全管理」C 項の 2 に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、サービス仕様適合開示書に基づき、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

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.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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

(ア) 3

ネットワーク経路対応に用いる機器

■ ガイドラインとして必要な要求事項 Seq. 257

---

①

ルータ等のネットワーク機器は、ISO15408 で規定されるセキュリティターゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。

■ 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

■ クラウドサービス事業者（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.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

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 3

ネットワーク経路対応に用いる機器

■ ガイドラインとして必要な要求事項 Seq. 258

---

#### ②

ネットワークで用いられる医療機関等の施設内のルータについて、これを經由して施設間を結ぶ VPN の間で送受信ができないように経路設定すること等に関するクラウドサービス事業者の役割分担について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ 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

■ クラウドサービス事業者（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.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

### 3.2.9

#### 個人情報を含む医療情報を外部と交換する場合の安全管理対策

##### (ア) 4 暗号化対策

##### ■ ガイドラインとして必要な要求事項 Seq. 259

---

###### ①

送信元と相手先の当事者間で情報そのものに対する暗号化等のセキュリティ対策を実施する。

##### ■ AWS のインフラストラクチャー関連事項

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います。

(<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 サービス関連情報

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。

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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、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、データの暗号化、改ざん検知などの対策を講じる必要があります。

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が許可されています。

##### ■ 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 Key Management Service のベストプラクティス 2017 年 4 月

AWSKeyManagementService(AWSKMS)は、マネージド型サービスであり、データの暗号化に使用する暗号化キーを簡単に作成して管理できます。AWSKMS は、ハードウェアセキュリティモジュール(HSM)を使用してキーのセキュリティを保護します。AWSKMS を使用して、AWS サービスやアプリケーションでデータを保護することができます。

AWSKeyManagementServiceの暗号化の詳細のホワイトペーパーは、データのセキュリティとプライバシーを確保するためにサービス内で実装されている設計と制御を説明しています。

### ■ 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.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

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 4

暗号化対策

#### ■ ガイドラインとして必要な要求事項 Seq. 260

---

#### ②

サービスの提供において SSL/TLS を用いる際には、TLS1.2 に対応した措置を講じる。

#### ■ 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 Certificate Manager

AWS Certificate Manager により、AWS の各種サービスとお客様の内部接続リソースで使用するパブリックとプライベートの Secure Sockets Layer/Transport Layer Security (SSL/TLS) 証明書のプロビジョニング、管理、およびデプロイを簡単に行えます。SSL/TLS 証明書は、ネットワーク通信を保護し、プライベートネットワーク上のリソースと同様にインターネット上の Web サイトのアイデンティティを確立するために使用されます。AWS Certificate Manager を使用すれば、SSL/TLS 証明書の購入、アップロード、および更新という時間のかかるプロセスを手動で行う必要がなくなります。AWS Certificate Manager を使えば、証明書のリクエスト、および Elastic Load Balancing、Amazon CloudFront ディストリビューション、Amazon API Gateway の API といった AWS のリソースでの証明書の ACM に統合された AWS でのデプロイをすばやく簡単に行うことができます。また、証明書は自動的に更新されます。また内部リソースのためのプライベート証明書を作成し、証明書ライフサイクルを中央で管理することも可能になります。ACM 統合サービスのために AWS Certificate Manager を通してプロビジョニングされたパブリック、プライベート証明書は無料です。お支払いいただくのは、アプリケーションを実行するために作成した AWS リソースの料金のみです。プライベート証明書については、プライベート CA のオペレーションとお客様の発行するプライベート証明書に対して月々お支払いいただきます。

<https://aws.amazon.com/jp/certificate-manager/>

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスの提供において SSL/TLS を用いる際には、TLS1.2 に対応した措置を講じる必要があります。

#### ■ 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.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

---

### 3.2.9

#### 個人情報を含む医療情報を外部と交換する場合の安全管理対策

##### (ア) 4

##### 暗号化対策

##### ■ ガイドラインとして必要な要求事項 Seq. 261

---

##### ③

②のほか、メールの暗号化（S/MIME 等）やファイルの暗号化への対応を医療機関等が求める場合には、その対応に必要な措置及び条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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

##### Amazon Simple Email Service(Amazon SES)のセキュリティ

Amazon Simple Email Service (SES) は、Amazon の高信頼でスケーラブルなインフラストラクチャに構築された外部配信 専用の E メール送信サービスです。Amazon SES を使用すると、E メールの配信可能性を最大限に高め、E メールの配信ステータスを常に把握することができます。Amazon SES はその他の AWS サービスと統合されているため、Amazon EC2 のようなサービスでホストされているアプリケーションから簡単に電子メールを送信することができます。

Amazon S3 ではまた、保管時のデータの暗号化用に複数のオプションを用意しています。お客様が独自の暗号化キーを管理したい場合は、Amazon S3 の暗号化クライアントのようなクライアント暗号化ライブラリを使用して、Amazon S3 に アップロードする前にデータを暗号化することができます。また、Amazon S3 で暗号化プロセスの管理を行いたい場合は、Amazon S3 のサーバーサイド暗号化(SSE)を使用できます。データは、要件に応じて、AWS により生成されたキー または指定したキーを使用して暗号化されます。Amazon S3 の SSE により、オブジェクトを書き込む際に追加のリクエストヘッダーを単純に追加するだけで、アップロード時にデータを暗号化することができます。データが取得された時に、自動的に復号化が行われます。

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、暗号化対策について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

- SSL/TLS の対応
- メール暗号化（S/MIME 等）
- ファイルの暗号化

##### ■ 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.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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 5 通信経路の暗号化対策

#### ■ ガイドラインとして必要な要求事項 Seq. 262

---

##### ①

オープンなネットワークを介して HTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行う。

#### ■ AWS のインフラストラクチャー関連事項

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

安全なアクセスポイント

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。FIPS 暗号要件への準拠を必要とするお客様をサポートするために、AWS GovCloud(米国)内の SSL 終端ロードバランサーは、FIPS 140-2 に準拠しています。

#### ■ AWS サービス関連情報

N/A

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、通信経路の暗号化対策として、オープンなネットワークを介して HTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 5 通信経路の暗号化対策

##### ■ ガイドラインとして必要な要求事項 Seq. 263

---

#### ②

SSL-VPN は、原則として使用しない。

##### ■ 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、通信経路の暗号化対策として、SSL-VPN は、原則として使用しないこととします。

##### ■ 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.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.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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 5

通信経路の暗号化対策

#### ■ ガイドラインとして必要な要求事項 Seq. 264

---

#### ③

サービス提供に際して、ソフトウェア型の IPsec 又は TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施する。

#### ■ AWS のインフラストラクチャー関連事項

アマゾンウェブサービス:セキュリティプロセスの概要 2014 年 11 月

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。

#### ■ AWS サービス関連情報

Amazon Virtual Private Cloud(Amazon VPC)のセキュリティ

通常、起動する Amazon EC2 インスタンスごとに Amazon EC2 アドレス空間内のパブリック IP アドレスがランダムに割り当てられます。Amazon VPC を使用すると、AWS クラウド内に独立した部分を作成して、特定の範囲内(例: 10.0.0.0/16) のプライベート(RFC 1918)アドレスを持つ Amazon EC2 インスタンスを起動することができます。VPC 内で IP アドレス範囲に基づいて同種のインスタンスをグループ化するサブネットを定義して、インスタンスおよびサブネットに出入りするトラフィックの流れを制御するルーティングとセキュリティを設定することができます。

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、通信経路の暗号化対策として、サービス提供に際して、ソフトウェア型の IPsec 又は TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な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.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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ア) 5

通信経路の暗号化対策

#### ■ ガイドラインとして必要な要求事項 Seq. 265

---

#### ④

医療機関等における利用者がソフトウェア型の IPsec 又は TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃についての、適切な対策に関する情報提供を行う。情報提供の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

#### ■ 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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、通信経路の暗号化対策について、サービス仕様適合開示書に基づき、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.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

---

### 3.2.9

#### 個人情報を含む医療情報を外部と交換する場合の安全管理対策

##### (ア) 6

##### 回線の品質等

##### ■ ガイドラインとして必要な要求事項 Seq. 266

---

##### ①

回線の管理、品質等に対するクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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。

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、回線の管理、品質等に対するクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、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.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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

(ア) 7 医療機関等の外部からのサービス利用

#### ■ ガイドラインとして必要な要求事項 Seq. 267

---

①

医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いる PC の作業環境に仮想デスクトップ等の技術を導入するためのクラウドサービス事業者の役割分担等につき、サービス仕様適合開示書に基づき、医療機関等と合意する。

#### ■ AWS のインフラストラクチャー関連事項

3.2.9 と同様

#### ■ AWS サービス関連情報

Amazon WorkSpaces はマネージド型で、セキュアなクラウドベースのデスクトップサービスです。Amazon WorkSpaces を使うと、Windows または Linux のデスクトップが数分でセットアップでき、すばやくスケールすることで世界中のたくさんの従業員にデスクトップを提供できます。自分が起動した WorkSpaces に対してのみ、月単位または時間単位のいずれかで支払うことができるため、従来のデスクトップやオンプレミスの VDI ソリューションに比べて、費用を削減できます。Amazon WorkSpaces では、ハードウェアのインベントリ、OS バージョンとパッチ、仮想デスクトップインフラストラクチャ (VDI) の複雑な管理作業をなくして、デスクトップ提供戦略を簡素化します。Amazon WorkSpaces では、高速で応答性の高いデスクトップをユーザーが選択し、サポートされているデバイスを使用していつでも、どこからでもアクセスできます。

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

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等の利用者が用いる PC の作業環境に仮想デスクトップ等の技術を導入するための役割分担等につき、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.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

---



### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (イ) 1

保守における通信上の安全管理対策

■ ガイドラインとして必要な要求事項 Seq. 268

---

#### ①

リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。

■ 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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、保守における通信上の安全管理対策として、リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる必要があります。

■ 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.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

---

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ウ) 1

通信経路に関する責任分界

#### ■ ガイドラインとして必要な要求事項 Seq. 269

---

##### ①

通常運用時及び非常時の医療機関等と事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版

6.11 C 項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、事業者の負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

#### ■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

#### ■ AWS サービス関連情報

N/A

#### ■ クラウドサービス事業者（お客様）の該当事項

通常運用時及び非常時の医療機関等と事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版6.11 C 項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、事業者の負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、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

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.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

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ウ) 1

通信経路に関する責任分界

- ガイドラインとして必要な要求事項 Seq. 270
- 

#### ②

交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、サービス仕様適合開示書に基づき、医療機関等と合意する。

- AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

- AWS サービス関連情報

N/A

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、サービス仕様適合開示書に基づき、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

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.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

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ウ) 1

通信経路に関する責任分界

■ ガイドラインとして必要な要求事項 Seq. 271

---

#### ③

医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、事業者が負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

■ AWS サービス関連情報

N/A

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、事業者が負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、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

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.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



### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ウ) 2

患者等が閲覧する場合の手続・責任分界

■ ガイドラインとして必要な要求事項 Seq. 272

---

#### ①

サービスにより管理する医療情報を患者等の閲覧に供する場合に、クラウドサービス事業者において対応すべきセキュリティ上の措置の条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

■ AWS サービス関連情報

N/A

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスにより管理する医療情報を患者等の閲覧に供する場合に、クラウドサービス事業者において対応すべきセキュリティ上の措置の条件、内容等について、サービス仕様適合開示書に基づき、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

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.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

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ウ) 2

患者等が閲覧する場合の手続・責任分界

■ ガイドラインとして必要な要求事項 Seq. 273

---

#### ②

医療情報を患者等の閲覧に供する場合に、医療機関等及び患者等の閲覧環境において対応すべきセキュリティ上の対応に係る情報の提供条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

■ AWS サービス関連情報

N/A

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療情報を患者等の閲覧に供する場合に、医療機関等及び患者等の閲覧環境において対応すべきセキュリティ上の対応に係る情報の提供条件、内容等について、サービス仕様適合開示書に基づき、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

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.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

### 3.2.9

個人情報を含む医療情報を外部と交換する場合の安全管理対策

#### (ウ) 2

患者等が閲覧する場合の手続・責任分界

■ ガイドラインとして必要な要求事項 Seq. 274

---

#### ③

患者等が情報を閲覧する情報システムのセキュリティに関する説明責任等におけるクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

■ AWS サービス関連情報

N/A

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、患者等が情報を閲覧する情報システムのセキュリティに関する説明責任等におけるクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、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.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.18 順守

---

### 3.2.10

法令で定められた記名・押印を電子署名で行うことについての安全管理対策

(ア)

電子証明書による電子署名

■ ガイドラインとして必要な要求事項 Seq. 275

---

①

法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合に、保健医療福祉分野 PKI 認証局の発行する署名用電子証明書へ対応することの可否を、医療機関等に対して明らかにする。

■ 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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合に、保健医療福祉分野 PKI 認証局の発行する署名用電子証明書へ対応することの可否を、医療機関等に対して明らかに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.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.18 順守

---



### 3.2.10

#### 法令で定められた記名・押印を電子署名で行うことについての安全管理対策

(ア)

電子証明書による電子署名

■ ガイドラインとして必要な要求事項 Seq. 276

---

②

保健医療福祉分野 PKI 認証局の発行する電子証明書以外の、電子署名法における認定認証事業者が発行する電子証明書を用いて、法令で定められた記名・押印を電子署名で行うサービスを提供する場合には、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、電子署名法の規定に基づく認定認証事業者の発行する電子証明書を用いなくても「電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）」第

2 条 1 項の要件を満たすことは可能であることから、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能であることを担保して、認定認証事業者以外が発行する電子証書書を利用する場合には、上記要件を担保できることを示して、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ 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

■ クラウドサービス事業者（お客様）の該当事項

保健医療福祉分野 PKI 認証局の発行する電子証明書以外の、電子署名法における認定認証事業者が発行する電子証明書を用いて、法令で定められた記名・押印を電子署名で行うサービスを提供する場合には、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、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.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.18 順守

---

### 3.2.10

法令で定められた記名・押印を電子署名で行うことについての安全管理対策

(ア)

電子証明書による電子署名

■ ガイドラインとして必要な要求事項 Seq. 277

---

③

公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名・押印を電子署名で行うサービスを提供する場合には、当該サービスにおける公的個人認証サービスに係る電子証明書の検証方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ 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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名・押印を電子署名で行うサービスを提供する場合には、当該サービスにおける公的個人認証サービスに係る電子証明書の検証方法等について、サービス仕様適合開示書に基づき、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.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.18 順守

---

### 3.2.10

#### 法令で定められた記名・押印を電子署名で行うことについての安全管理対策

(イ)

##### タイムスタンプの付与

##### ■ ガイドラインとして必要な要求事項 Seq. 278

---

①

電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、タイムスタンプの内容・検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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/>

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、タイムスタンプの内容・検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

クラウドサービス事業者は、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](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.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.18 順守

---

### 3.2.10

法令で定められた記名・押印を電子署名で行うことについての安全管理対策

(イ)

タイムスタンプの付与

■ ガイドラインとして必要な要求事項 Seq. 279

---

②

タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

#### ■ 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

3.2.10 と同様

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

クラウドサービス事業者は、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](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.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.18 順守

---



### 3.2.10

法令で定められた記名・押印を電子署名で行うことについての安全管理対策

(イ)

タイムスタンプの付与

■ ガイドラインとして必要な要求事項 Seq. 280

---

③

タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

#### ■ 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

3.2.10 と同様

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

クラウドサービス事業者は、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](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.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.18 順守

---

### 3.2.10

法令で定められた記名・押印を電子署名で行うことについての安全管理対策

(ウ)

タイムスタンプを付与する時点で有効な電子証明書の使用

■ ガイドラインとして必要な要求事項 Seq. 281

---

①

タイムスタンプを付与した情報を取り扱う場合に、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

#### ■ 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

3.2.10 と同様

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、タイムスタンプを付与した情報を取り扱う場合に、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

クラウドサービス事業者は、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](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.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.18 順守

---

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

(ア)

医療機関等によるサービス選択のための事業者情報の提供

#### ■ ガイドラインとして必要な要求事項 Seq. 282

---

①

サービスの提供に係る契約に際して、医療機関等の求めに応じて、以下の情報の提供を行う。

- ・医療情報等の安全管理に係る基本方針・取り扱い規程等の整備状況
- ・医療情報等の安全管理に係る実施体制の整備状況
- ・実績等に基づく個人データ安全管理に関する信用度
- ・財務諸表等に基づく経営の健全性

#### ■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

#### ■ AWS サービス関連情報

N/A

#### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、サービスの提供に係る契約に際して、医療機関等の求めに応じて、以下の情報の提供を行う必要があります。

- ・医療情報等の安全管理に係る基本方針・取り扱い規程等の整備状況
- ・医療情報等の安全管理に係る実施体制の整備状況
- ・実績等に基づく個人データ安全管理に関する信用度
- ・財務諸表等に基づく経営の健全性

#### ■ 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.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

---

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (イ) 1

##### 保守・運用における受託情報の閲覧制限

##### ■ ガイドラインとして必要な要求事項 Seq. 283

---

##### ①

受託した医療情報を保守・運用を行うために閲覧するのは必要最小限とする。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、受託した医療情報を保守・運用を行うために閲覧するのは必要最小限と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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (イ) 1

##### 保守・運用における受託情報の閲覧制限

##### ■ ガイドラインとして必要な要求事項 Seq. 284

---

##### ②

①の閲覧が必要な場合には、緊急時を除き、システム管理者の事前・事後の承認により実施する。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、受託した医療情報を保守・運用を行うために閲覧するのは必要最小限とするが、緊急の場合を除き、事前・事後の承認により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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (イ) 1

##### 保守・運用における受託情報の閲覧制限

##### ■ ガイドラインとして必要な要求事項 Seq. 285

---

##### ③

受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、受託した医療情報を緊急時に閲覧した場合には、システム管理者の承認を得る必要があります。

- ・閲覧した受託情報の範囲
- ・緊急で閲覧が必要な理由等

##### ■ 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.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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (イ) 1 保守・運用における受託情報の閲覧制限

##### ■ ガイドラインとして必要な要求事項 Seq. 286

---

#### ④

①～③における閲覧に係る範囲、手順等について、サービス仕様適合開示書に基づき、医療機関等と合意する。また②、③により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。

##### ■ AWS のインフラストラクチャー関連事項

#### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、保守・運用における受託情報の閲覧制限に関わる範囲、手順等について、サービス仕様適合開示書に基づき、医療機関等と合意する必要があります。

クラウドサービス事業者は、保守・運用の場合、緊急時の場合には、医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (イ) 2 受託情報の閲覧制限のための機能

##### ■ ガイドラインとして必要な要求事項 Seq. 287

---

##### ①

予定された保守・運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、予定された保守・運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等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

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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (イ) 2

##### 受託情報の閲覧制限のための機能

##### ■ ガイドラインとして必要な要求事項 Seq. 288

---

##### ②

システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、受託情報の閲覧制限のための機能として、システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる必要があります。

##### ■ 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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (ウ) 1

##### 受託情報の解析等の制限等

##### ■ ガイドラインとして必要な要求事項 Seq. 289

---

##### ①

受託した医療情報の解析・分析は、サービス提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、受託情報の解析・分析等の制限等として、サービス提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わないこととします。

##### ■ 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.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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (ウ) 1 受託情報の解析等の制限等

##### ■ ガイドラインとして必要な要求事項 Seq. 290

---

##### ②

受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、必要があります。受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う必要があります。

##### ■ 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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (ウ) 2 受託情報の解析等の第三者提供制限

##### ■ ガイドラインとして必要な要求事項 Seq. 291

---

###### ①

受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わないこととします。

##### ■ 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.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.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

### 3.3.6

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

#### (ウ) 2

受託情報の解析等の第三者提供制限

- ガイドラインとして必要な要求事項 Seq. 292
- 

#### ②

①の内容を、サービス提供に係る契約に含める。

- AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

- AWS サービス関連情報

N/A

- クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、以下の内容をサービス提供に係る契約に含める必要があります。

- 受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない

- 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.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

### 3.3.6

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

#### (ウ) 2

受託情報の解析等の第三者提供制限

■ ガイドラインとして必要な要求事項 Seq. 293

---

#### ③

医療機関等の指示に基づき、受託した医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧・取得できないように、3. 2. 3 及び 3. 2. 9 に示す対応策を講じる。

■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

■ AWS サービス関連情報

N/A

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等の指示に基づき、受託した医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧・取得できないように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

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.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

### 3.3.6

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

#### (ウ) 2

受託情報の解析等の第三者提供制限

■ ガイドラインとして必要な要求事項 Seq. 294

---

#### ④

③により、第三者提供（閲覧）を行う場合には、閲覧・取得が可能な者の ID 及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更・削除できる対応を行う。

■ AWS のインフラストラクチャー関連事項

3.2.9（ア）6 -①と同様

■ AWS サービス関連情報

N/A

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、第三者提供（閲覧）を行う場合には、閲覧・取得が可能な者の ID 及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更・削除できる対応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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (ウ) 2 受託情報の解析等の第三者提供制限

##### ■ ガイドラインとして必要な要求事項 Seq. 295

---

##### ⑤

医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。

##### ■ AWS のインフラストラクチャー関連事項

##### 3.2.9（ア）6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告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.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

### 3.3.6

#### 外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準

##### (ウ) 2

#### 受託情報の解析等の第三者提供制限

##### ■ ガイドラインとして必要な要求事項 Seq. 296

---

##### ⑥

①～⑤により第三者提供及びその報告を行うための条件、範囲等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ AWS のインフラストラクチャー関連事項

#### 3.2.9 (ア) 6 -①と同様

##### ■ AWS サービス関連情報

N/A

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、第三者提供及びその報告を行うための条件、範囲等について、サービス仕様適合開示書に基づき、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

#### 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.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

### 3.3.7

#### 個人情報の保護についての安全管理対策

(ア)

診療録等の外部保存委託先の事業者内における個人情報保護

■ ガイドラインとして必要な要求事項 Seq. 297

---

①

個人情報保護対応策を、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

■ AWS サービス関連情報

N/A

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、個人情報保護対応策を、サービス仕様適合開示書に基づき、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

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.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

### A.18.1

### 3.3.7

#### 個人情報の保護についての安全管理対策

(イ)

外部保存実施に関する患者への説明

■ ガイドラインとして必要な要求事項 Seq. 298

---

①

医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

■ AWS のインフラストラクチャー関連事項

3.2.9 (ア) 6 -①と同様

■ AWS サービス関連情報

N/A

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、サービス仕様適合開示書に基づき、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

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.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

A.18.1

### 3.4

#### クラウドサービスの利用終了に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 299

---

###### ①

サービスの一部又は全部の停止やサービス変更の場合（軽微なバージョンアップは含まない）には、サービスを利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。

##### ■ 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/>

##### 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

##### ■ クラウドサービス事業者（お客様）の該当事項



クラウドサービス事業者は、提供しているクラウドサービスの終了に関する対応（サービスを利用している医療機関等への影響を最小とするための措置）について、サービス仕様適合開示書に基づき、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

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.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

### A.18.1

---

### 3.4

#### クラウドサービスの利用終了に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 300

---

#### ②

①の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式（データ項目、項目の詳細、ファイル形式）、返却方法、条件については、サービス仕様適合開示書に基づき、医療機関等と合意する。また医療機関等のサービス利用開始後に、サービス仕様適合開示書の内容を変更する場合には、①に準じた対応策を講じる。

##### ■ 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/>

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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、提供しているクラウドサービスの終了に関する対応（受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式(データ項目、項目の詳細、ファイル形式)、返却方法）について、サービス仕様適合開示書に基づき、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

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.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

A.18.1

---

### 3.4

#### クラウドサービスの利用終了に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 301

---

#### ③

②におけるデータの返却については、厚生労働省ガイドライン第5版「5 情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、クラウドサービス事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合があるので、その旨も合わせて、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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/>

##### 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

■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、提供しているクラウドサービスの終了に関する対応（データの返却、画像データ等やパスワード等が含まれている場合のデータの返却）について、サービス仕様適合開示書に基づき、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

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.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

A.18.1

---



### 3.4

#### クラウドサービスの利用終了に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 302

---

#### ④

①においてサービスの変更を含むサービスの一部又は全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等で、②の対応は除く）、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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/>

##### 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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、提供しているクラウドサービスの終了に関する対応サービスの変更を含むサービスの一部又は全部の停止が生じる場合の医療機関等への対応の内容) について、サービス仕様適合開示書に基づき、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

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.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

A.18.1

---

### 3.4

#### クラウドサービスの利用終了に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 303

---

⑤

医療機関等の都合により医療機関等のサービス利用が終了する場合も、②、③に示す対応策を講じる。

##### ■ 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/>

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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、提供しているクラウドサービスの終了に関する対応（医療機関等によるサービス終了の場合）について、サービス仕様適合開示書に基づき、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

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.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

A.18.1

---

### 3.4

#### クラウドサービスの利用終了に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 304

---

#### ⑥

サービス提供の停止又は医療機関等におけるサービス利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。

##### ■ 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/>

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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、提供しているクラウドサービスの終了に関する対応（廃棄証明等の提供）について、サービス仕様適合開示書に基づき、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

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.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

A.18.1

---

### 3.4

#### クラウドサービスの利用終了に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 305

---

⑦

⑥に関して、医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、サービス仕様適合開示書に基づき、医療機関等と合意する。

##### ■ 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/>

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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、提供しているクラウドサービスの終了に関する対応（医療機関等へのサポート（所管官庁への情報提供含む）等）に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等）についてサービス仕様適合開示書に基づき、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

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.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

A.18.1

---

### 3.4

#### クラウドサービスの利用終了に関する要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 306

---

⑧

①～⑦についての手順等を、運用管理規程等を含める。

##### ■ 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/>

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

##### ■ クラウドサービス事業者（お客様）の該当事項

クラウドサービス事業者は、運用管理規程に以下を盛り込む必要があります。

- サービスを利用している医療機関等への影響を最小とするための措置について
- 受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式(データ項目、項目の詳細、ファイル形式)、返却方法について
- データの返却、画像データ等やパスワード等が含まれている場合のデータの返却について
- サービスの変更を含むサービスの一部又は全部の停止が生じる場合の医療機関等への対応の内容について
- 医療機関等によるサービス終了の場合の対応について
- 記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合の廃棄証明について
- 医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について

■ 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.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

A.18.1

---

### 3.5.2

#### オンライン診療システム提供事業者における要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 307

---

###### ①

オンライン診療システムにおいて、医療情報システムとの接続がある場合には、本ガイドラインの「3. 2」～「3. 4」の要求事項を、オンライン診療システムを提供するクラウドサービス事業者にも適用する。

### 3.5.2

#### オンライン診療システム提供事業者における要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 308

---

###### ②

患者側端末で利用するオンライン診療システムの機能には、オンライン診療の実施中に医療情報システムと接続する機能等を含まないこと、及びこれに関する情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。

### 3.5.2

#### オンライン診療システム提供事業者における要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 309

---

###### ③

医師が利用するオンライン診療システムを提供するクラウドサービス事業者と患者との間の責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。

### 3.6.1

#### PHR サービス事業者への要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 310

---

###### ①

PHR サービス事業者については、3. 2. 1～3. 2. 9、3. 3. 6～3. 3. 7に示す要求事項を以下のとおり読み替えるものとする。

- ・「医療情報」→「PHR で利用する医療情報 31」
- ・「医療機関等」→「患者等」
- ・「クラウドサービス事業者」→「PHR サービス事業者」



### 3.6.1

#### PHR サービス事業者への要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 311

---

#### ②

PHR サービス事業者については、3. 2. 9 (2) (イ) 2.の①の要求事項における「TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行う」とある部分を、「TLS の設定は 1.2 に限定し、信頼性の高い機関によって発行されたサーバ証明書を用いるとともに、本人性の確認を確実に実施する」と読み替えるものとする。

### 3.6.1

#### PHR サービス事業者への要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 312

---

#### ③

PHR サービス事業者については、3. 2. 3 (2) (ア) 4.の③の要求事項における「なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第 5 版の公表（平成 29 年 5 月）から約 10 年後を目途に 2 要素認証について「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。」とある部分を削除するものとする。

### 3.6.1

#### PHR サービス事業者への要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 313

---

#### ④

PHR サービス事業者については、3. 3. 6 (2) (ウ) 2. の①の要求事項における「患者本人を含め」とある部分を削除するものとする。

### 3.6.1

#### PHR サービス事業者への要求事項

##### ■ ガイドラインとして必要な要求事項 Seq. 314

---

#### ⑤

PHR サービス事業者については、3. 2. 1～3. 2. 9、3. 3. 6～3. 3. 7に示す要求事項のうち、3. 6. 3に掲げる要求事項を適用対象外とする。

### 3.6.1

#### PHR サービス事業者への要求事項

⑥

PHR サービスの提供に際しては、以下の内容を含む手順を策定し、その手順に基づいて実施したことを確認する。

- ・登録時の ID 申請者である患者等の本人確認（実在性の確認）
- ・利用時の患者等の認証（利用者の本人確認）
- ・新たに受領した医療情報の患者等の ID への紐づけ（患者本人の情報であることの確認）

### 3.6.1

PHR サービス事業者への要求事項

⑦

PHR サービス事業者については、3. 2. 1～3. 2. 9、3. 3. 6～3. 3. 7に示す要求事項のうち、上記①による読み替え後に「サービス仕様適合開示書に基づき、患者等と合意する」となる要求事項は適用対象外とし、それらの要求事項に代えて以下の対応を行うこととする。

- ・PHR サービスで取り扱う個人情報に関して、患者等からの同意の取得方法について運用管理規程を策定する。その運用管理規程には、本ガイドラインを遵守して個人情報を取り扱う旨を含める。
- ・PHR サービスの提供終了時又は契約終了時における患者等に関する医療情報の返却の範囲、方法、条件について、患者等とあらかじめ合意する。
- ・患者等の指示により、医療機関等が（自ら管理する）医療情報を患者等が契約する PHR サービス事業者へ送付する場合において、PHR サービス事業者と医療機関等との責任分界について、あらかじめ患者等に示す。
- ・PHR サービスの提供に関する患者等との合意においては、この情報が個人情報保護法上の要配慮個人情報であることや消費者保護法等の適用を受ける可能性があることを勘案して、免責事項等の内容を定める。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

（ア）

①

サービスの提供についての管理責任を有する責任者を設置する。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

(ア) ■ ガイドラインとして必要な要求事項 Seq. 318

---

②

情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）を設置する。

3.6.2(1)

組織的安全管理対策（3.2.1（2）の読替え）

(ア)

■ ガイドラインとして必要な要求事項 Seq. 319

---

③

サービスの提供に係る情報システムの運用に関する事務を統括する責任者を設置する。

3.6.2(1)

組織的安全管理対策（3.2.1（2）の読替え）

(ア) ■ ガイドラインとして必要な要求事項 Seq. 320

---

④

①から③に掲げた責任者の任命・解任等のルールを策定する。

3.6.2(1)

組織的安全管理対策（3.2.1（2）の読替え）

(イ) 1

■ ガイドラインとして必要な要求事項 Seq. 321

---

①

サービスに係る情報及び受託した情報に関する守秘義務について、サービス提供に係る契約に含める。契約には、守秘義務に違反した PHR サービス事業者にはペナルティが課されること、及び委託した情報の取扱いに対する患者等による監督に関する内容を含める。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

（イ）2

■ ガイドラインとして必要な要求事項 Seq. 322

---

①

サービス提供に係る契約において、次項（ウ）1.に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

（ウ）1

■ ガイドラインとして必要な要求事項 Seq. 323

---

①

経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

（ウ）1 ■ ガイドラインとして必要な要求事項 Seq. 324

---

②

①の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

（ウ）1 ■ ガイドラインとして必要な要求事項 Seq. 325

---

③

①の指針等には、個人情報保護法の対象外の情報（死者に関する情報等）であっても、PHR で利用する医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 326

---

#### ④

情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーを策定する。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 327

---

#### ⑤

情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を行う。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （ウ） 2

■ ガイドラインとして必要な要求事項 Seq. 328

---

#### ①

サービスの提供に係る体制を、緊急時の対応も含めて明確にする。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （ウ） 3 ■ ガイドラインとして必要な要求事項 Seq. 329

---

#### ①

情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づき文書の管理を行う。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （ウ） 3

■ ガイドラインとして必要な要求事項 Seq. 330

---

#### ②

サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理する。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （ウ） 4 ■ ガイドラインとして必要な要求事項 Seq. 331

---

#### ①

サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （ウ） 5

■ ガイドラインとして必要な要求事項 Seq. 332

---

#### ①

機器等の管理方法について、文書化を行う。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （ウ） 5 ■ ガイドラインとして必要な要求事項 Seq. 333

---

#### ②

機器等について、台帳管理等により所在確認等を行う旨を定める。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

（ウ）6

■ ガイドラインとして必要な要求事項 Seq. 334

---

①

個人情報記録した媒体の管理等に関する運用規程を策定する。

組織的安全管理対策（3. 2. 1（2）の読替え）

（ウ）8

■ ガイドラインとして必要な要求事項 Seq. 335

---

①

サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等について明文化を行う。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

（ウ）8

■ ガイドラインとして必要な要求事項 Seq. 336

---

②

第三者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容を明確にする。

### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

（ウ）8 ■ ガイドラインとして必要な要求事項 Seq. 337

---

③

監査実施について記録し、当該記録の保存・管理方法を明確にする。

### 3.6.2(1)

組織的安全管理対策（３．２．１（２）の読替え）

（ウ） 9

■ ガイドラインとして必要な要求事項 Seq. 338

---

②

自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、患者等からの問合せ窓口を一元化する。

### 3.6.2(1)

組織的安全管理対策（３．２．１（２）の読替え）

（エ） 1

■ ガイドラインとして必要な要求事項 Seq. 339

---

①

PHR サービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、並びにアクセス管理の運用状況に関する定期的なレビューの実施等を内容とするアクセス管理規程を策定する。

### 3.6.2(1)

組織的安全管理対策（３．２．１（２）の読替え）

（エ） 1

■ ガイドラインとして必要な要求事項 Seq. 340

---

②

サービスの提供に係るアクセス記録（外部からのアクセス、利用者によるアクセス等を含む）の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定する。



### 3.6.2(1)

組織的安全管理対策（3. 2. 1（2）の読替え）

#### （エ） 2

■ ガイドラインとして必要な要求事項 Seq. 341

---

#### ①

PHR で利用する医療情報の取扱いに関する委託契約に、以下の内容を含める。

- ・個人情報に関して、他の情報と区別して適切に管理を行う。
- ・PHR で利用する医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。

### 3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

#### （ア） 1

■ ガイドラインとして必要な要求事項 Seq. 342

---

#### ①

サービスに供する機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。

### 3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

#### （ア） 1

■ ガイドラインとして必要な要求事項 Seq. 343

---

サービスに供するサーバ等を格納するラック等について、施錠管理を行う。

### 3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（ア） 1 ■ ガイドラインとして必要な要求事項 Seq. 344

---

③

サービスに供する媒体等を格納するキャビネット等について、施錠管理を行う。

### 3.6.2(2)

物理的安全管理対策（３．２．２（２）の読替え）

（ア） 2

■ ガイドラインとして必要な要求事項 Seq. 345

---

①

サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する。

### 3.6.2(2)

物理的安全管理対策（３．２．２（２）の読替え）

（ア） 2

■ ガイドラインとして必要な要求事項 Seq. 346

---

②

サービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。

### 3.6.2(2)

物理的安全管理対策（３．２．２（２）の読替え）

（ア） 2

■ ガイドラインとして必要な要求事項 Seq. 347

---

③

サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。

### 3.6.2(2)

物理的安全管理対策（３．２．２（２）の読替え）

（ア） 2

■ ガイドラインとして必要な要求事項 Seq. 348

---

④

サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。

3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（ア）2

■ ガイドラインとして必要な要求事項 Seq. 349

---

⑤

サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。

3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（ア）2

■ ガイドラインとして必要な要求事項 Seq. 350

---

⑥

サービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。

3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（ア）2

■ ガイドラインとして必要な要求事項 Seq. 351

---

⑦

①～⑥につき、運用管理規程等に規定する。

### 3.6.2(2)

物理的安全管理対策（３．２．２（２）の読替え）

（ア）３

■ ガイドラインとして必要な要求事項 Seq. 352

---

①

サービスに供する機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐える機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。

### 3.6.2(2)

物理的安全管理対策（３．２．２（２）の読替え）

（ア）４

■ ガイドラインとして必要な要求事項 Seq. 353

---

①

サービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する。

### 3.6.2(2)

物理的安全管理対策（３．２．２（２）の読替え）

（ア）４

■ ガイドラインとして必要な要求事項 Seq. 354

---

②

防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。

### 3.6.2(2)

物理的安全管理対策（３．２．２（２）の読替え）

（ア）４ ■ ガイドラインとして必要な要求事項 Seq. 355

---

③

サービスに供する機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がいないことを確認する。

### 3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（イ） 1

■ ガイドラインとして必要な要求事項 Seq. 356

---

①

個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等の対策を行う。

### 3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（イ） 1 ■ ガイドラインとして必要な要求事項 Seq. 357

---

②

運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。

### 3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 358

---

①

個人情報が物理的に保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。

### 3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 359

---

②

個人情報が存在する PC 等の重要な機器には、盗難防止用チェーンを取り付ける。

### 3.6.2(2)

物理的安全管理対策（3. 2. 2（2）の読替え）

（ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 360

---

③

受託する個人情報を運用や保守に用いる端末に保存しない旨、自社の運用管理規程等に定める。

### 3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

（ア） 1 ■ ガイドラインとして必要な要求事項 Seq. 361

---

①

情報システムの利用者を特定し識別できるように、アカウントの発行を行う（複数の利用者による ID の共同利用は行わない。ただし当該情報システムが他の情報システムを利用するための ID（non interactive ID）は除く）。

### 3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

（ア） 1

■ ガイドラインとして必要な要求事項 Seq. 362

---

②

利用者のなりすまし等を防止するための認証を行う。

### 3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

（ア） 1

■ ガイドラインとして必要な要求事項 Seq. 363

---

③

利用者には、患者等においてサービスを利用する者のほか、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含める。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 1

■ ガイドラインとして必要な要求事項 Seq. 364

---

④

情報システムの運用若しくは開発に従事する者又は管理者権限を有する者に対する ID の発行は必要最小限とし、定期的な棚卸しを行う。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 2

■ ガイドラインとして必要な要求事項 Seq. 365

---

①

本人の識別・認証に、ユーザ ID とパスワードを組み合わせる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。

- ・利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと情報システムにアクセスできないようにする。

- ・初期パスワード以外のパスワードは、利用者本人が設定し、本人しか知りえない内容に限定する。

- ・パスワードの設定に際しては、複数の文字種（英数字・大文字・小文字・記号等）を用い、また、8 文字以上等、十分に安全な長さの文字列等から構成されるルールとする。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

(ア) 2 ■ ガイドラインとして必要な要求事項 Seq. 366

---

②

パスワード認証に係る以下のルールを実現する措置を講じる。

- ・パスワード入力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。
- ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

(ア) 2

■ ガイドラインとして必要な要求事項 Seq. 367

---

③

パスワードには十分な安全性を満たす有効期間を設定する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

(ア) 2 ■ ガイドラインとして必要な要求事項 Seq. 368

---

④

認証に際して ID 及びパスワードによらない場合でも、上記と同等以上の安全性を確保する。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

(ア) 3

■ ガイドラインとして必要な要求事項 Seq. 369

---

①



利用者のパスワードは、ハッシュ値での保存を行う等、暗号化して管理する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 3 ■ ガイドラインとして必要な要求事項 Seq. 370

---

②

サービスを提供する製品等の導入に際しては、初期パスワードを変更するだけでなく、アカウントの棚卸しを行い、不要なものについては削除を行う。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 3

■ ガイドラインとして必要な要求事項 Seq. 371

---

③

利用者が ID やパスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行う。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 3

■ ガイドラインとして必要な要求事項 Seq. 372

---

④

パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該 ID を無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 3

■ ガイドラインとして必要な要求事項 Seq. 373

---

⑤

パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し、変更できるような対応を講じる。

3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 3

■ ガイドラインとして必要な要求事項 Seq. 374

---

⑥

利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を行う。

3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 3 ■ ガイドラインとして必要な要求事項 Seq. 375

---

⑦

利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。

3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア） 4

■ ガイドラインとして必要な要求事項 Seq. 376

---

①

情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、2 要素認証以上の認証強度のある方法による。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア）４

■ ガイドラインとして必要な要求事項 Seq. 377

---

③

利用者の認証において、固定式の ID・パスワードによる認証方式を採用している場合には、固定式の ID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア）４

■ ガイドラインとして必要な要求事項 Seq. 378

---

④

利用者の認証に際して、何らかの物理的な媒体・身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段・手順を事前に定める。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア）４

■ ガイドラインとして必要な要求事項 Seq. 379

---

⑤

代替的手段・手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ア）４

■ ガイドラインとして必要な要求事項 Seq. 380

---

⑥

代替的手段・手順により、情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

（イ） 1

■ ガイドラインとして必要な要求事項 Seq. 381

---

①

PHR で利用する医療情報とそれ以外の情報を区分できる措置を講じる。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

（イ） 1

■ ガイドラインとして必要な要求事項 Seq. 382

---

②

PHR で利用する医療情報については、情報区分に従ってアクセス制御を行えるようにする。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

（イ） 1

■ ガイドラインとして必要な要求事項 Seq. 383

---

③

仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

(イ) 3 ■ ガイドラインとして必要な要求事項 Seq. 384

---

①

サービスには、受託する PHR で利用する医療情報を患者等ごとに管理できる機能を含める。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

(工) 1

■ ガイドラインとして必要な要求事項 Seq. 385

---

⑥

情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

(工) 2

■ ガイドラインとして必要な要求事項 Seq. 386

---

①

アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する。

3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

(工) 2

■ ガイドラインとして必要な要求事項 Seq. 387

---

②

アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。

### 3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

#### （エ） 2

■ ガイドラインとして必要な要求事項 Seq. 388

---

#### ③

アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。

### 3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

#### （エ） 3

■ ガイドラインとして必要な要求事項 Seq. 389

---

#### ①

アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。

### 3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

#### （オ） 1

■ ガイドラインとして必要な要求事項 Seq. 390

---

#### ①

サービスの運用・保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。

### 3.6.2(3)

技術的安全管理対策（3. 2. 3（2）の読替え）

（オ） 1 ■ ガイドラインとして必要な要求事項 Seq. 391

---

#### ②

サービスの運用・保守端末等を設置している区域は監視カメラ等により適切に監視を行う。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（オ） 1

■ ガイドラインとして必要な要求事項 Seq. 392

---

④

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、利用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する、あるいは強制ログオフを行うことができるようにする。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 1

■ ガイドラインとして必要な要求事項 Seq. 393

---

①

情報システムの構築に際しては、ウイルスやマルウェア等の混入が生じないようにするための手順を策定し、これに則って構築する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 1

■ ガイドラインとして必要な要求事項 Seq. 394

---

②

ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 1

■ ガイドラインとして必要な要求事項 Seq. 395

---

③

情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 1

■ ガイドラインとして必要な要求事項 Seq. 396

---

④

サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに患者等に周知し、必要な対応等を求める。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 1

■ ガイドラインとして必要な要求事項 Seq. 397

---

⑤

情報システムの脆弱性に関する情報は、JPCERT コーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 2

■ ガイドラインとして必要な要求事項 Seq. 398

---

①



外部のネットワークと PHR で利用する医療情報を格納する機器との接続に際しては、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。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 2 ■ ガイドラインとして必要な要求事項 Seq. 399

---

②

患者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を検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 2

■ ガイドラインとして必要な要求事項 Seq. 400

---

③

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。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（カ） 2

■ ガイドラインとして必要な要求事項 Seq. 401

---

④

ホスティングの利用時等、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。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

(ク) 2

■ ガイドラインとして必要な要求事項 Seq. 402

---

①

3. 2. 1 (2) (ウ) 4. ①において実施するリスク分析結果に基づき情報システムのバックアップを取得する。バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、その内容を運用管理規程等に含める。

3.6.2(3)

技術的安全管理対策 (3. 2. 3 (2) の読替え)

(ク) 2

■ ガイドラインとして必要な要求事項 Seq. 403

---

②

①に従い取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改ざん・破壊等がないことを確認する。

3.6.2(3)

技術的安全管理対策 (3. 2. 3 (2) の読替え)

(ク) 2

■ ガイドラインとして必要な要求事項 Seq. 404

---

③

記録媒体に格納するバックアップについては、その媒体の特性（テープ／ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。

3.6.2(3)

技術的安全管理対策 (3. 2. 3 (2) の読替え)

(ク) 2

■ ガイドラインとして必要な要求事項 Seq. 405

---

④

③の対象となるバックアップの記録媒体につき、使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ク） 2

■ ガイドラインとして必要な要求事項 Seq. 406

---

⑤

①～④の手順を運用管理規程等を含め、従業者等及び再委託業者に対して必要な教育を行う。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ケ） 1

■ ガイドラインとして必要な要求事項 Seq. 407

---

①

情報システムにおける機器及びソフトウェアの構成図を作成する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ケ） 1

■ ガイドラインとして必要な要求事項 Seq. 408

---

②

情報システムのネットワーク構成図を作成する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ケ） 1 ■ ガイドラインとして必要な要求事項 Seq. 409

---

③

①、②で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ケ）１

■ ガイドラインとして必要な要求事項 Seq. 410

---

④

情報システムを構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ケ）２

■ ガイドラインとして必要な要求事項 Seq. 411

---

①

サービスに供する機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等を含める。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ケ）２

■ ガイドラインとして必要な要求事項 Seq. 412

---

②

サービスに供する機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ケ）２ ■ ガイドラインとして必要な要求事項 Seq. 413

---

③

サービスに係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。

### 3.6.2(3)

技術的安全管理対策（３．２．３（２）の読替え）

（ケ）２

■ ガイドラインとして必要な要求事項 Seq. 414

---

④

システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等を含める。

### 3.6.2(4)

人的安全管理対策（３．２．４（２）の読替え）

（ア）１ ■ ガイドラインとして必要な要求事項 Seq. 415

---

①

サービスの提供に従事する要員（被用者、派遣従業者等）については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等を含める。

### 3.6.2(4)

人的安全管理対策（３．２．４（２）の読替え）

（ア）２

■ ガイドラインとして必要な要求事項 Seq. 416

---

①

サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育・訓練を行う。

### 3.6.2(4)

人的安全管理対策（３．２．４（２）の読替え）

（ア）２

■ ガイドラインとして必要な要求事項 Seq. 417

---

②

この教育・訓練は就業開始時及び就業後定期的に行う。

3.6.2(4)

人的安全管理対策（3. 2. 4（2）の読替え）

（ア）3

■ ガイドラインとして必要な要求事項 Seq. 418

---

①

サービスの提供に従事する要員が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。

3.6.2(4)

人的安全管理対策（3. 2. 4（2）の読替え）

（ア）3

■ ガイドラインとして必要な要求事項 Seq. 419

---

②

サービスの提供に従事する要員が業務上管理していた個人情報については、離職時（内部の異動含む）に返却を求め、システム管理者が返却されたことを確認する。

3.6.2(4)

人的安全管理対策（3. 2. 4（2）の読替え）

（ア）3

■ ガイドラインとして必要な要求事項 Seq. 420

---

③

サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、上記 2.における教育・訓練に含める。

### 3.6.2(4)

人的安全管理対策（3. 2. 4（2）の読替え）

（ア） 4

■ ガイドラインとして必要な要求事項 Seq. 421

---

①

上記 1.～3.に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。

### 3.6.2(4)

人的安全管理対策（3. 2. 4（2）の読替え）

（イ） 1

■ ガイドラインとして必要な要求事項 Seq. 422

---

②

再委託先には、自社と同等の個人情報保護指針等を遵守させる。

### 3.6.2(4)

人的安全管理対策（3. 2. 4（2）の読替え）

（イ） 1 ■ ガイドラインとして必要な要求事項 Seq. 423

---

③

再委託に係る契約に、委託業務に係る守秘義務を含める。

### 3.6.2(4)

人的安全管理対策（3. 2. 4（2）の読替え）

（イ） 1 ■ ガイドラインとして必要な要求事項 Seq. 424

---

④

再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。

### 3.6.2(4)

人的安全管理対策（3. 2. 4（2）の読替え）

（イ） 1

■ ガイドラインとして必要な要求事項 Seq. 425

---

⑤

再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。

### 3.6.2(5)

情報の破棄に関する安全管理対策（3. 2. 5（2）の読替え）

（ア） 2 ■ ガイドラインとして必要な要求事項 Seq. 426

---

①

運用管理規程に以下の内容を定める。

- ・管理する個人情報又はこれを格納する媒体等について、サービス提供上の要否の確認を定期的に行うこと。
- ・サービス提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。
- ・サービス提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、患者等が不測の損害を被らないようにするための措置（事前に破棄の基準等を告知する等）。

### 3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

（ア） 1

■ ガイドラインとして必要な要求事項 Seq. 427

---

①

情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で当該情報システムにアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。

### 3.6.2(6)



情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

（ア）1 ■ ガイドラインとして必要な要求事項 Seq. 428

---

②

①で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。

3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

（ア）2

■ ガイドラインとして必要な要求事項 Seq. 429

---

①

情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する。

3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

（イ）1

■ ガイドラインとして必要な要求事項 Seq. 430

---

①

リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、情報システムへの不正な侵入が生じないよう安全管理措置を講じる。

3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

（イ）1

■ ガイドラインとして必要な要求事項 Seq. 431

---

②

リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。

### 3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

#### （イ） 2

■ ガイドラインとして必要な要求事項 Seq. 432

---

#### ①

情報システムの保守において実施した操作結果について、操作ログ等により記録し、管理する。

### 3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

#### （イ） 2

■ ガイドラインとして必要な要求事項 Seq. 433

---

#### ②

取得した操作ログ等により、アクセスされた PHR で利用する医療情報についての状況をレビューする。

### 3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

#### （ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 434

---

#### ①

情報システムの動作確認に際しては、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。

### 3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

#### （ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 435

---

②

情報システムの動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、3. 2. 4で示す守秘義務が課された要員・委託先等により動作確認を行う旨を含めた手順を定める。

### 3.6.2(6)

情報システムの改造と保守に関する安全管理対策（3. 2. 6（2）の読替え）

（ウ） 2

■ ガイドラインとして必要な要求事項 Seq. 436

---

①

PHR で利用する医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、患者等又は PHR サービス事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（ア） 1

■ ガイドラインとして必要な要求事項 Seq. 437

---

①

サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器・媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（ア） 1

■ ガイドラインとして必要な要求事項 Seq. 438

---

②

①における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

(ア) 2

■ ガイドラインとして必要な要求事項 Seq. 439

---

サービスに供する記録媒体・記録機器に関し、以下の内容を運用管理規程に含める。

・管理体制及び管理方法

・記録媒体・記録機器の取扱い

・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器・媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等（「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。）

・サービスに関する情報を持ち出した場合で、当該情報を格納する機器・媒体等の盗難・紛失（持ち出し時の機器・媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業員等における誤送信等を含む。））が起きた場合の対応

・外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改ざんが生じないようにするための具体的な措置（マルウェア対策、暗号化、ファイアウォール導入等））

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

(ア) 3

■ ガイドラインとして必要な要求事項 Seq. 440

---

①

「2.サービスに供する記録媒体・記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

(ア) 3 ■ ガイドラインとして必要な要求事項 Seq. 441

---

②

上記の運用管理規程については、再委託先に対しても遵守等を求める。

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（イ） ■ ガイドラインとして必要な要求事項 Seq. 442

---

①

サービスに関する情報を格納する機器・媒体等については、台帳管理等を行い、定期的に所在確認を行う。

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（ウ） 1 ■ ガイドラインとして必要な要求事項 Seq. 443

---

①

サービスに供する機器等については、起動パスワードの設定を行う。

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 444

---

②

起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。

### 3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（ウ） 1

■ ガイドラインとして必要な要求事項 Seq. 445

---

③

サービスに関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせで行う。

3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（ウ）2 ■ ガイドラインとして必要な要求事項 Seq. 446

---

①

サービスに関する情報を格納する機器・媒体等を持ち出す場合の手順には、機器・媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。

3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（ウ）3 ■ ガイドラインとして必要な要求事項 Seq. 447

---

①

サービスに関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。

3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

（ウ）3

■ ガイドラインとして必要な要求事項 Seq. 448

---

②

サービスに関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。

3.6.2(7)

情報及び情報機器の持ち出しについての安全管理対策（3. 2. 7（2）の読替え）

(ウ) 5

■ ガイドラインとして必要な要求事項 Seq. 449

---

①

業務上、サービスに関する情報を格納するモバイル端末を持ち出す場合には、公衆無線 LAN への接続は行わない。

3.6.2(8)

災害等の非常時の対応についての安全管理対策（3. 2. 8（2）の読替え）

(イ) 1 ■ ガイドラインとして必要な要求事項 Seq. 450

---

①

サービスに係る BCP 及びコンテンジェンシープランの策定を行う。

3.6.2(8)

災害等の非常時の対応についての安全管理対策（3. 2. 8（2）の読替え）

(イ) 1

■ ガイドラインとして必要な要求事項 Seq. 451

---

②

①で策定する BCP 及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。

3.6.2(8)

災害等の非常時の対応についての安全管理対策（3. 2. 8（2）の読替え）

(イ) 3

■ ガイドラインとして必要な要求事項 Seq. 452

---

①

サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。

3.6.2(8)

災害等の非常時の対応についての安全管理対策（3. 2. 8（2）の読替え）

(イ) 3 ■ ガイドラインとして必要な要求事項 Seq. 453

---

②

①の場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、患者等に速やかに報告を行う。

3.6.2(8)

災害等の非常時の対応についての安全管理対策（3. 2. 8（2）の読替え）

(イ) 4 ■ ガイドラインとして必要な要求事項 Seq. 454

---

①

非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定・検証方法の規定等）を講じる。

3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

(ア) 1 ■ ガイドラインとして必要な要求事項 Seq. 455

---

①

ネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を行う。

3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

(ア) 1

■ ガイドラインとして必要な要求事項 Seq. 456

---

②

アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置（サーバ証明書の導入等）を行う。



### 3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

（ア） 3

■ ガイドラインとして必要な要求事項 Seq. 457

---

①

ルータ等のネットワーク機器は、ISO15408 で規定されるセキュリティターゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。

### 3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

（ア） 4

■ ガイドラインとして必要な要求事項 Seq. 458

---

①

送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施する。

### 3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

（ア） 4 ■ ガイドラインとして必要な要求事項 Seq. 459

---

②

サービスの提供において SSL/TLS を用いる際には、TLS1.2 に対応した措置を講じる。

### 3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

（ア） 5

■ ガイドラインとして必要な要求事項 Seq. 460

---

①

オープンなネットワークを介して HTTPS を利用した接続を行う際は、TLS の設定は 1.2 に限定し、信頼性の高い機関によって発行されたサーバ証明書を用いるとともに、本人性の確認を確実に実施する。

### 3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

（ア） 5

■ ガイドラインとして必要な要求事項 Seq. 461

---

②

SSL-VPN は、原則として使用しない。

### 3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

（ア） 5

■ ガイドラインとして必要な要求事項 Seq. 462

---

③

サービス提供に際して、ソフトウェア型の IPsec 又は TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施する。

### 3.6.2(9)

個人情報を含む医療情報を外部と交換する場合の安全管理対策（3. 2. 9（2）の読替え）

（イ）

■ ガイドラインとして必要な要求事項 Seq. 463

---

①

リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。

### 3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（３．３．６（２）の読  
替え）

（イ） 1 ■ ガイドラインとして必要な要求事項 Seq. 464

---

①

受託した PHR で利用する医療情報を保守・運用を行うために閲覧するのは必要最小限とする。

3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（３．３．６（２）の読  
替え）

（イ） 1

■ ガイドラインとして必要な要求事項 Seq. 465

---

②

①の閲覧が必要な場合には、緊急時を除き、システム管理者の事前・事後の承認により実施する。

3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（３．３．６（２）の読  
替え）

（イ） 1

■ ガイドラインとして必要な要求事項 Seq. 466

---

③

受託した PHR で利用する医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要  
な理由等を示して、システム管理者の承認を得る。

3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（３．３．６（２）の読  
替え）

（イ） 2

■ ガイドラインとして必要な要求事項 Seq. 467

---

①

予定された保守・運用等を行う際に受託した PHR で利用する医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。

### 3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（3.3.6（2）の読替え）

（イ） 2

■ ガイドラインとして必要な要求事項 Seq. 468

---

②

システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。

### 3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（3.3.6（2）の読替え）

（ウ） 2

■ ガイドラインとして必要な要求事項 Seq. 469

---

①

受託した PHR で利用する医療情報は、法令による場合又は患者等の指示に基づく場合を除き、第三者への提供は行わない。

### 3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（3.3.6（2）の読替え）

（ウ） 2

■ ガイドラインとして必要な要求事項 Seq. 470

---

②

①の内容を、サービス提供に係る契約に含める。

### 3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（3.3.6（2）の読替え）

#### （ウ） 2

■ ガイドラインとして必要な要求事項 Seq. 471

---

#### ③

患者等の指示に基づき、受託した PHR で利用する医療情報の第三者提供（閲覧）を行う場合には、患者等が許諾した者以外が閲覧・取得できないように、3.2.3及び3.2.9に示す対応策を講じる。

### 3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（3.3.6（2）の読替え）

#### （ウ） 2

■ ガイドラインとして必要な要求事項 Seq. 472

---

#### ④

③により、第三者提供（閲覧）を行う場合には、閲覧・取得が可能な者の ID 及び利用権限について、患者等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更・削除できる対応を行う。

### 3.6.2(10)

外部保存を受託するクラウドサービス事業者の選定基準及び情報の取扱いに関する基準（3.3.6（2）の読替え）

#### （ウ） 2

■ ガイドラインとして必要な要求事項 Seq. 473

---

#### ⑤

患者等の指示に基づいて受託した PHR で利用する医療情報の第三者提供を行った場合には、患者等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。