

医療情報システム向け AWS利用リファレンスの概要

2022年10月17日

V2.2

キヤノンITソリューションズ株式会社
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

更新履歴

#	バージョン	更新内容	更新日
1	1.0	経済産業省版リファレンス公開に伴い新規作成	2018/8/22
2	1.1	総務省版リファレンス公開に伴い更新	2018/12/10
3	1.2	厚生労働省版リファレンス公開に伴い更新	2019/6/12
4	2.0	「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（第1版）」対応に伴い更新	2020/11/27
5	2.1	厚生労働省版リファレンス改訂に伴い更新 「医療情報システムの安全管理に関するガイドライン（第5.1版）」対応	2021/4/23
6	2.2	厚生労働省版リファレンス改訂に伴い更新 「医療情報システムの安全管理に関するガイドライン（第5.2版）」対応	2022/10/17

はじめに

近年、AWSをはじめとするクラウドサービスが医療機関の課題を解決する手段として重要度を増しています。

しかし、クラウド活用の前提としてクラウド事業者が開示しているシステム仕様が厚生労働省や経済産業省、総務省が発行する医療情報システムに関する安全管理ガイドライン（以下、3省2ガイドライン）の要求事項に対応できているかを調査、解釈、判断しなければならないという難しい課題がありました。

AWSのパートナーであるキヤノンITソリューションズ株式会社、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の4社は医療機関等におけるクラウドの活用を促進することを目的に、AWSが3省2ガイドラインの各要求事項に対して、どのように適合するかを共同で調査、検討いたしました。

その成果を「**医療情報システム向けAWS利用リファレンス**」として整理し、公開していきます。リファレンスをまとめるにあたり、アマゾン ウェブ サービス ジャパンの協力を得て、これまで非公開であった情報についても調査対象としています。さらに、4社の豊富な医療・製薬分野でのシステム導入・運用経験やノウハウに基づく解釈も加えました。

医療情報管理の課題とクラウドへの期待



紙媒体での医療情報管理の課題

- ・検索閲覧の利便性
- ・保存スペースのひっ迫、物理的セキュリティ
- ・災害などによる紙記録の喪失



医療情報電子化の課題

- ・IT専門家の不足・不在
- ・システム投資負担
- ・保存容量のひっ迫、ITセキュリティ



クラウドへの期待

- ・システムコストの効率化（従量課金）
- ・IT管理からの解放
- ・保存容量を気にせず、使いたい分を使う

AWSの特徴と利点の再確認

1) 俊敏性

必要な時に必要な分だけのリソースを即座に提供可能

2) コスト最適化

使用したITサービスの分だけのコスト、変動費

3) 弾力性と拡張性

必要性に応じて即座にスケールアップ、スケールダウンが可能

4) 幅広い機能と新機能追加

2006年から毎年新サービスを継続して追加展開。継続的なサービスの進化や革新によるメリットを享受可能。

5) マネージドサービス

リソースの調達、メンテナンス、容量の使用計画といったわずらわしい作業はすべてAWSが実施

医療情報システムに関する 3省2ガイドラインとは？



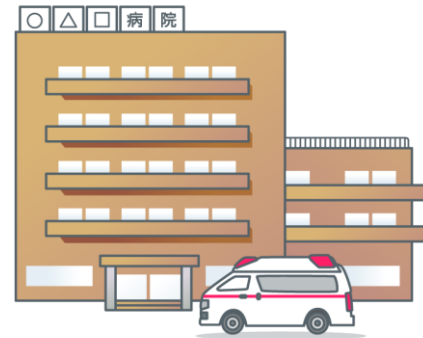
一般的に診療録に記録される情報

- 患者の基本情報 :氏名・年齢・性別・住所・保険証番号等
- 主訴（患者が来院するきっかけとなった主な訴え）
- 現病歴（現症）
- 既往歴
- 家族歴
- 社会歴
- 嗜好
- アレルギー
- 現症・身体所見
- 検査
- 入院後経過・看護記録
- 治療方針 :治療の目的

医療情報と個人情報（日本）

医療情報の保存に関して医師法・医療法などで義務が規定

- 診療録は最終診療後最低5年間は保存することが義務
- 診療録以外の診療に関する諸記録は2年間の保存が義務



改正個人情報保護法により、「**要配慮個人情報**」として明確に定義

多くの医療機関は「診療情報」を扱う「**個人情報取扱事業者**」

医療情報の安全な取り扱いを目的として医療情報システムの安全管理に関するガイドラインが制定

医療情報システムに関する要求事項

1. **電子保存に関する要求事項**（いわゆる**電子保存の三原則**）
「真正性」、「見読性」、「保存性」の確保
2. **関係省庁ガイドラインの遵守**（いわゆる**3省2ガイドライン**^{*1}）
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・経済産業省
「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」

^{*1} 従来「3省4ガイドライン」、「3省3ガイドライン」と呼ばれる厚生労働省・総務省・経済産業省発行のガイドラインやの遵守が求められてきましたが、2020年8月の総務省・経済産業省ガイドラインによる2つのガイドラインの統合・改定により、医療情報を取り扱う情報システム・サービスの提供事業者向けのガイドラインが1本化され、「3省2ガイドライン」となっています。

3省2ガイドライン遵守が求められる主体



医療機関などの関係者

- ・ 病院・診療所
- ・ 薬局
- ・ 訪問介護ステーション
- ・ 医療情報を取り扱う介護事業体
- ・ 地域医療連携を統括する組織体

利用



医療情報システム

受託開発/
運用

システム開発/運用事業者
(外部委託先)



クラウドサービス

サービス
提供

クラウド/ASP事業者 (外部委託先)
によるサービス提供

【総務省・経済産業省】

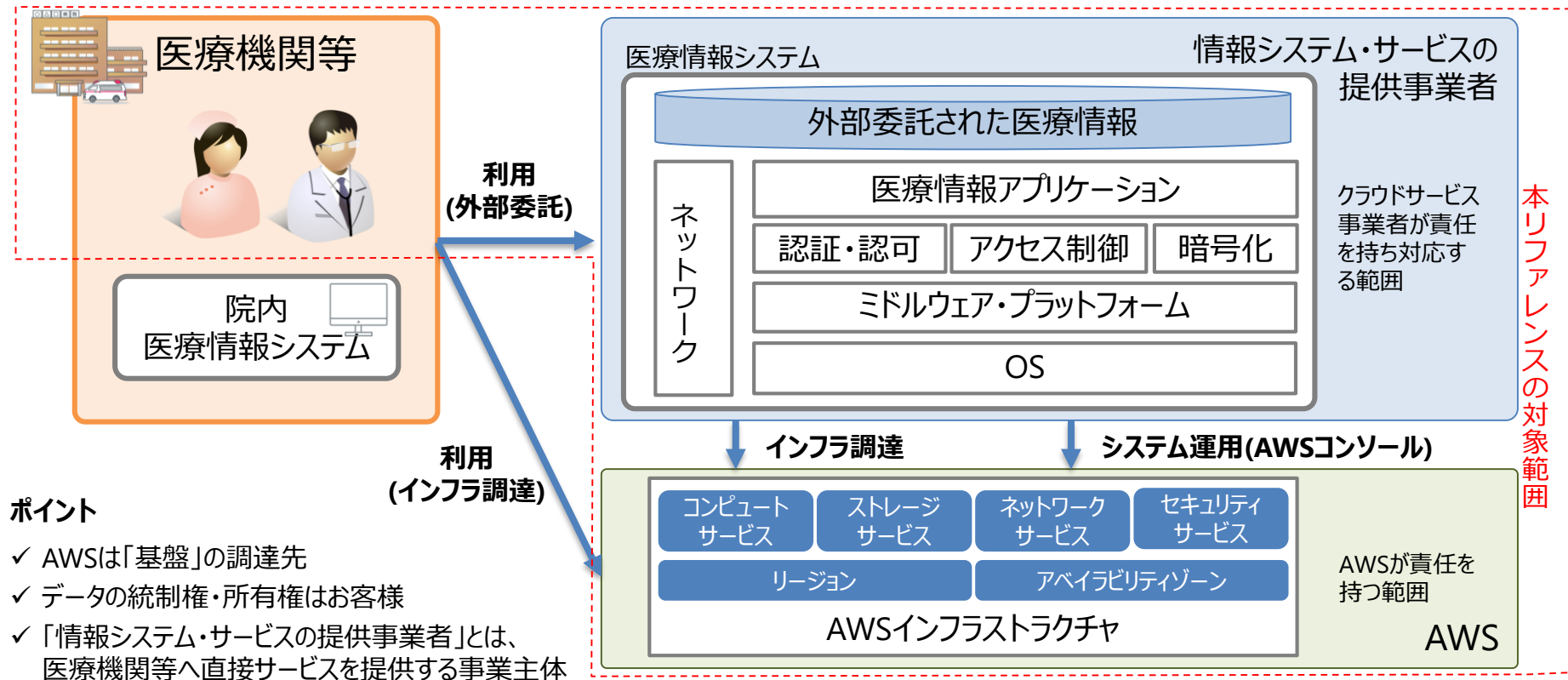
医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン

【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

医療情報システムでの AWS利用時の責任と課題

AWS利用時の責任と課題



ポイント

- ✓ AWSは「基盤」の調達先
- ✓ データの統制権・所有権はお客様
- ✓ 「情報システム・サービスの提供事業者」とは、医療機関等へ直接サービスを提供する事業主体
- ✓ 本リファレンスでは院内の医療情報システムは対象外。ただし、厚生労働省版において、医療機関等は対象に含まれる。
- ✓ 厚生労働省版リファレンスでは、医療機関等がAWSを直接利用する場合を主に想定して作成

AWS利用時の責任と課題

ガバナンス

リスク計画

準拠要件

セキュリティ

利用者
責任

- ・クラウド事業者の環境上での要件の確認
- ・クラウド事業者の責任範囲における機能や統制を確認
- ・利用者の要件に見合った機能や統制が提供されるか確認
- ・様々な要件を満たすためのサービスの構成、運用を実施

3省2ガイドラインの
数百を超える要求事項

調査

解釈

判断

負担

- ・お客様の要件に見合うように様々な監査を実施、認証を取得
- ・インフラ環境とサービスに関するコンプライアンスとセキュリティ

AWS
責任



AWSのシステム
仕様・認証

3省2ガイドラインへのAWSの適合性を調査・検討した内容をまとめた
「医療情報システム向けAWS利用リファレンス」

本リファレンスの概要と活用イメージ

医療情報の適正かつ安全な取り扱い、医療情報における適切なクラウドサービスの利用の促進

医療機関等のお客さま

医療情報を取り扱う
情報システム・サービス
事業者のお客さま

参照

参照

医療情報システム向けAWS利用リファレンス

医療情報システム向けAWS利用リファレンス
(厚生労働省版)

医療情報システム向けAWS利用リファレンス
(総務省・経済産業省版)

Update
2022

基準に
対応

3省2ガイドライン

医療情報システムの安全管理に
関するガイドライン
(第5.2版)

医療情報を取り扱う情報シス
テム・サービスの提供事業者におけ
る安全管理ガイドライン
(第1版)

問合せ

支援

作成

調査
協力

Canon

キヤノン ITソリューションズ株式会社

Orchestrating a brighter world

NEC

HITACHI
Inspire the Next

株式会社 日立システムズ

FeelerSystemZ

ITをもっとあなたのそばに

Amazon Web Services
Japan G.K.

リファレンスの使い方

1) 想定されるお客様

医療情報システムでのクラウド(AWS)活用をご検討されている医療機関等
医療情報システム・サービスのソリューションプロバイダ

2) リファレンスの種類

医療情報システム向けAWS利用リファレンス（厚生労働省版）
医療情報システム向けAWS利用リファレンス（総務省・経済産業省版）

3) 整理方法

ガイドラインで示されている対策の考え方への対応方法を検討・整理
ガイドラインの要求事項に対しAWSが対象となる項目と対象外となる項目を整理

項目	整理方法
AWS基準を取り入れることで対応不要な項目	AWS基準で対応可能な項目の対応内容の整理
AWS基準を取り入れても、ユーザーが別途対応をしなければならない項目	ユーザーが対応しなければいけない項目での対応ヒントの提示
AWSが対象外でユーザーが対応をしなければいけない項目	ユーザーが対応しなければいけない項目での対応ヒントの提示

考慮・参考にした医療情報システムに関連するガイドンス

1) ガイドライン

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 第5.2版」（令和4年3月）

総務省・経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（第1版）」（令和2年8月）

2) ISO

ISO 9001:2015 品質マネジメントシステム

ISO 27001:2014 情報セキュリティマネジメントシステム

ISO 27002:2014 情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範

ISO/IEC 27017 Cloud Security Controls

ISO/IEC 27018:2014 Personal Data Protection

3) 米国公認会計士協会（AICPA）

SOC 1 レポート

SOC 2 セキュリティレポート

SOC 3 セキュリティレポート

4) HIPAA・HITRUST CSF



AWS対応・認証取得済

本リファレンス利用するメリット

1) 責任境界

ガイドラインの要求事項ごとに、AWS・受託事業者の責任境界を把握できます。

2) 対応内容

ガイドラインの要求事項ごとに、AWSのセキュリティ対応の内容と、その根拠と成る文章とその記載箇所が把握できます。

ガイドラインに適合するAWSサービスが把握できます。

利用者の責任において実施すべき事項の対応を容易とするために用意されたAWSサービスが把握できます。

3) ガイドライン対応の効率化

1)、2) の把握と理解を通じて、システムをガイドラインの各項目に適合しているかの確認および利用者が行うべき対応が効率よく行えます。

リファレンスの特徴

1) 複数の視点から対応状況を確認

AWSの視点 … White Paper等で確認

第三者の視点 … SOCLレポートやISO認証などで確認

2) 複数社で要求事項の解釈を実施

要求事項の解釈に関する「幅」を、参加各社の構築・運用の経験・ノウハウを基に議論し、共通見解を作成

医療情報システム向けAWS利用リファレンス (厚生労働省版)

リファレンスの位置付け

1) 対象ガイドライン

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 第5.2版」

2) 位置付け

対象ガイドラインでは、「本ガイドラインは、医療情報システムの安全管理やe-文書法への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したもの」とされています。

本リファレンスは、ガイドラインの策定方針に基づき、ガイドラインで求められる**「技術的及び運用管理上の観点から求められる所要の対策」に対する対応の参照情報として整理**するものです。

また、情報処理技術の普及やサイバー攻撃の高度化に伴い、情報セキュリティを確保するための要求は拡大するとともに多様化しており、今日の環境では、一律に定めた要求事項の全てに対応することは困難になってきています。ガイドラインにおいても、「本ガイドラインは技術的な記載の陳腐化を避けるために定期的に見直す予定である。本ガイドラインを利用する場合は最新の版であることに十分留意されたい。」との位置付けを踏襲し、最新のガイドラインに対応した改訂を行ったリファレンスとなります。

リファレンス内容

本リファレンスは以下の2部構成になり、主要項目は以下です。

項目	内容
1.医療情報システム向けAWS利用リファレンス	ガイドラインの要求事項に対し、AWSのインフラストラクチャーの対応事項、お客様の対応事項、推奨される追加の対応事項をまとめたシート。 各要求事項とISO/IEC27001との対応についても記載
2.AWSサービス関連情報	対応に活用できるAWSサービスを列挙・概要を解説

ガイドラインの各要求事項に対するAWS・お客様の対応例について整理したものです。
こちらの情報を参考に要求事項への対応を検討・進めることができます。

医療情報システム向けAWS利用フェイルオーバー(厚生労働省版)				007									
Seq	項目	標準タイトル	サブ標準	番号	必須/準拠	ガイドラインとして必要要素事項 (※※は第3.0版からの追加品) (※※※は第3.0版からの変更点)	関連するAWS情報	AWSのインフラストラクチャー関連事項	AWSサービス関連事項	お客様の該当事項	検証される追加の実験事項	AWS認証情報 (ISO/IEC27001, Annex A and ISO/IEC27017)	
4章. 臨床的医療情報を扱う際の責任のあり方													
1	4.1	医療機関等の管理者の情報保護責任について	(1)	臨床系運用における責任について	必須	<p>説明責任</p> <p>医療情報システムの機能や運用方法の徹底に留意し、運用責任を担っていることを患者等に説明できるようにする責任である。この責任を果たすためには、以下のことが必要である。</p> <p>・医療情報システムの仕様や運用方法を明確に定義すること</p> <p>・仕様や運用方法が文書化した方針のとおりに機能しているかどうかを定期的に監査すること</p> <p>・監査結果を適切に報告し、必要に応じて改善すること</p> <p>・監査の結果報告があった場合は、是正対応すること</p> <p>・監査の結果を文書化し、第三者が検証可能な状況にすること</p>	<p>医療関連情報</p> <p>AWSの医療関連の領域、最新情報は下記を参照ください。</p> <p>AWS カスタマーアグリメント このカスタマーアグリメントは、お客様による当サービスのご利用について適用されるものです</p> <p>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</p> <p>AWS サービスレベルアグリメント このサービスレベルアグリメントは、お客様による特定のサービスの利用に対して適用されます</p> <p>AWS 高圧利用説明 この高圧利用説明は、当サービスの利用に際し、禁止される事項を記載したものです</p> <p>https://aws.amazon.com/jp/legal/</p>	N/A	<p>AWS 責任共有モデルに照り、データの取扱いと所有権は利用者にあります。</p> <p>説明責任に照しては、医療機関等は医療情報の取扱いと所有権を保持していますので、患者事項に同意のガイドラインを遵守する責任があります。</p>	N/A	<p>AWS 責任共有モデルのための対策</p> <p>A.5.1</p> <p>A.15 供給者管理</p> <p>A.15.1</p> <p>A.15.2</p>		
<p>リスク管理</p> <p>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策定など、戦略的リスク管理を関与してまいりました。また、少なくとも半年に一度、この戦略的リスク管理を再評価します。このプロセスは、シニアマネジメント層がその責任範囲内のリスクを特定し、これらのリスクを軽減するために適切な技術的・政策的な措置を実施することが求められます。さらに、AWSの最新環境は、さまざまな内部資料および公開資料リソースによって提供されています。AWSのコンプライアンスおよびセキュリティチームは、情報および機密性のための制御目標 (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の取組に基づいたISO 27001認定フレームワーク、米国公営会計士協会 (AICPA) のトラストサービスの原則 (Trust Services Principles, PCI DSS v3.1.1) および米国独立検閲機関報告書 (NIST) 800-53 Rev. 4 (連邦政府情報システムにおける情報セキュリティ制御) を定期的に検証しています。AWSは、セキュリティポリシーを継続し、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属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属する脆弱性と明確に、データの機密性、完全性、可用性を確保するためのものです。</p> <p>最新環境</p> <p>AWSは、Amazon全体の最新環境の様々な領域を活用したポリシー、プロセス、および制御活動を含む、包括的な最新環境を管理しています。この最新環境は、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。この最新環境は、AWSの最新フレームワークの運用の有効性を高める環境を確立し、それを維持するために必要な人財、プロセス、テクノロジーを組織しています。</p>													

各項目の説明 | 1.医療情報システム向けAWS利用リファレンス

シート内容詳細（1）

分類	項目	説明
ガイドライン 要求事項	Seq.	本リファレンスの項目通し番号
	項番	ガイドラインの章・節
	項番タイトル	ガイドライン記載の要求事項のタイトル
	番号	要求事項の小番号
	必須/推奨	要求事項必須・推奨の区分 必須・・・要求事項を満たすために必ず実施しなければならない対策（ガイドラインのC項） 推奨・・・実施しなくても要求事項を満たすことが可能であるが、説明責任の観点から 実施した方が理解を得やすい対策（ガイドラインのD項）
	ガイドラインとして必要な要求事項	法律、厚生労働省通知、他の指針等の要求事項に基づき、ガイドラインにて定められた対策事項
対応例	AWSのインフラストラクチャー関連事項	AWSインフラストラクチャーでの対策が必要なリスク対策へのAWSの対応
	AWSサービス関連情報	AWS上で利用者がリスク対策を実施するうえで活用可能なAWSサービス情報
	お客様の該当事項	AWS上で利用者が実施する対応内容・例
	推奨される追加の実施事項	必須ではないが追加で対応を推奨する内容
	AWS認証情報	要求事項に対応するISO/IEC27001 AppendixA での該当箇所

各項目の説明 | 2.AWSサービス関連情報

AWS上で利用者がリスク対策/制度上の要求事項への対応を実施する際に、活用できるAWSサービスの情報を整理したものです。

これらのAWSサービスを利用することで、効率的にガイドライン対応を進めることができます。

2.AWS サービス関連情報

サービス 種別	INDEX	AWSサービス	機能	サービス概要	詳細URL
Compute	■ E	Amazon EC2 (Amazon Elastic Compute Cloud)	仮想サーバ	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 EC2 https://aws.amazon.com/jp/ec2/?ec2-whats-new&sort-by=item.additionalFields.postDataTime&ec2-whats-new&sort-order=desc
	■ E	Amazon EBS (Amazon Elastic Block Store)	インスタンスストレージ	Amazon EBS は、Amazon EC2 にアタッチして使用するブロックストレージサービスです。(仮想ディスク) Amazon EBS で保管時のデータを暗号化する場合、EBS ボリュームごとに固有のボリューム暗号化キーが生成されます。各ボリュームキーの暗号化に使用するマスターキーは、AWS Key Management Service で柔軟に選択することができます。 ・データの廃棄について Amazon EBS 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。 お客様は、データの廃棄処理において、Amazon EBS に保存されたデータを消去することでデータを廃棄したことになりますが、さらにAWS Key Management Serviceによる暗号鍵も廃棄することで、その廃棄操作をもって廃棄証明とすることも可能になります。	■ Amazon EBS https://aws.amazon.com/jp/ebs/?ebs-whats-new&sort-by=item.additionalFields.postDataTime&ebs-whats-new&sort-order=desc ■ Amazon EBS 暗号化 https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBS-Encryption.html ■ クラウドにおける安全なデータの廃棄 https://aws.amazon.com/jp/blog/news/data-disposal/



AWSサービス関連情報は、2022年10月時点のサービス内容をもとにしたものです。最新の情報はAWS公式ウェブサイト(<https://aws.amazon.com>)にてご確認ください。

資料作成には十分注意しておりますが、資料内の説明とAWS公式ウェブサイト記載の説明に相違があった場合、AWS公式ウェブサイトの説明を優先とさせていただきます。

各項目の説明 | 2.AWSサービス関連情報

シート内容詳細

項目	説明
サービス種別	AWSサービスの分類
INDEX	分類内でのアルファベット順インデックス
AWSサービス	AWSサービス名称
機能	該当AWSサービスにおけるガイドライン対応に利用可能な機能
サービス概要	AWSサービス概要説明
詳細URL	AWSサービス詳細掲載URL

医療情報システム向けAWS利用リファレンス (総務省・経済産業省版)

リファレンスの位置付け

1) 対象ガイドライン

医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（第1版）

2) 位置付け

情報処理技術の普及やサイバー攻撃の高度化に伴い、情報セキュリティを確保するための要求は拡大するとともに多様化しており、今日の環境では、一律に定めた要求事項の全てに対応することは困難になってきています。

対象ガイドラインでは、「医療情報システム等の特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいたリスクマネジメントプロセスを定義する」との策定方針となっており、一律の要求事項は定められていません。ただし、「医療情報システム等の運用が適切であるか、リスクマネジメントを通じて、最低限確認するためのもの」として別紙2の形で最低限の対策項目が示されています。

本リファレンスは、ガイドラインの策定方針に基づき、ガイドライン別紙2の対策項目に対応した、**「最低限確認・対応すべき事項」を参照情報として整理**するものです。

リファレンス内容

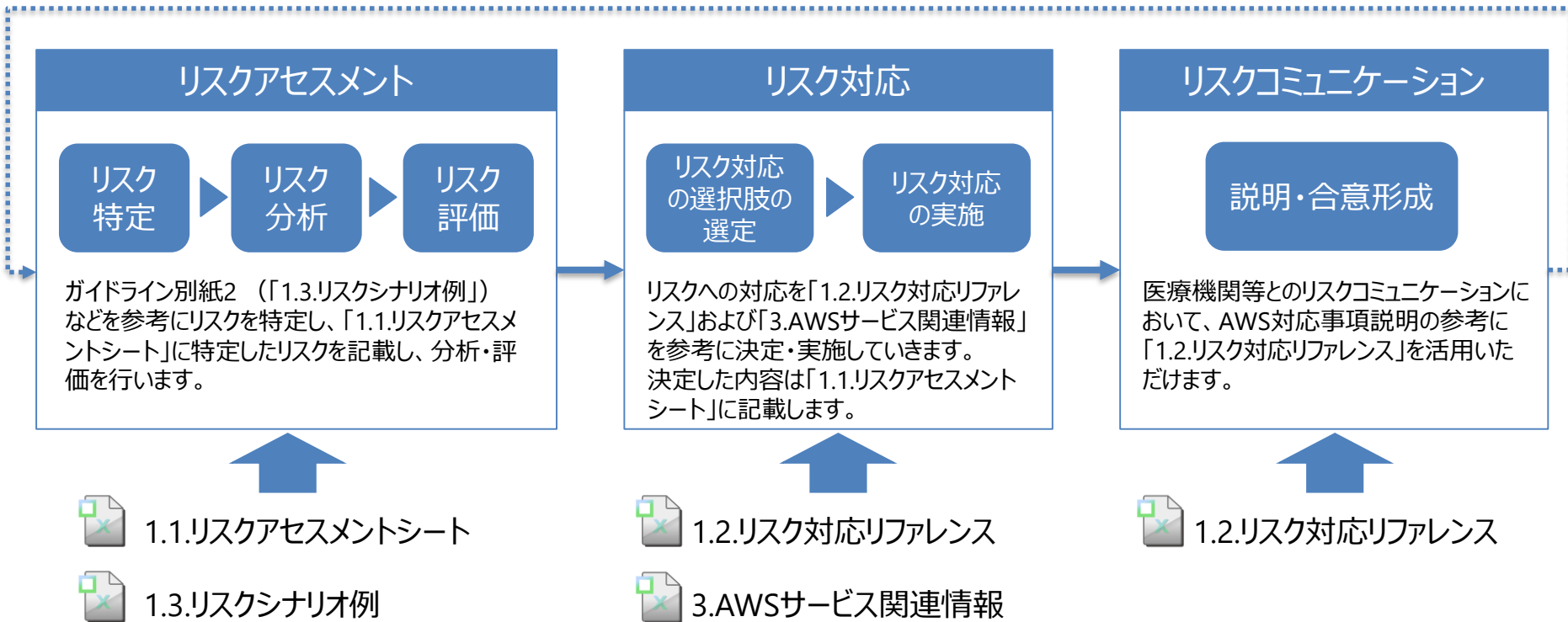
本リファレンスは以下の3部構成になり、主要項目は以下です。

項目	内容
1.リスクアセスメント	
1.1.リスクアセスメントシート	リスクアセスメントに使用するワークシート
1.2.リスク対応リファレンス	特定したリスクに対する対策例
1.3.リスクシナリオ例	ガイドライン別紙2記載の最低限確認すべきリスクシナリオ例
2.制度上の要求事項	ガイドライン6章「制度上の要求事項」の要求事項への対策例
3.AWSサービス関連情報	リスク対策に活用できるAWSサービスを列挙・概要を解説

リファレンス利用の流れ（リスクマネジメントプロセス）

リスクマネジメントプロセスの各ステップにおける、本リファレンス利用の流れを以下に示します。

継続的なリスクマネジメントの実践



各項目の説明 | 1.1.リスクアセスメントシート

リスクアセスメントのプロセスを表に整理したワークシートです。

各プロセスでの実施内容をこのシートに記載していくことで、以下成果物が作成できます。

- ・ リスクアセスメント結果一覧
- ・ リスク対応一覧
- ・ 残存するリスクの評価

記入例)

リスク特定				リスク分析		リスク評価		リスク対応								
情報流	分類	関連する脅威	特定したリスク	影響度	顕在率	リスクレベル	対応要否	対応	対策の観点	対象事業者が実施する対策	AWSが実施している対策	医療機関等へ対応を求める事項	残存するリスク	影響度	顕在率	リスクレベル
対象事業者DCの有線LAN上のネットワーク機器でアプリケーション提供(医療情報を含む可能性あり)が転送される	アプリケーション提供情報	ネットワーク上の盗聴・なりすまし	アプリケーション提供に係る情報の盗聴・なりすましが行われる	5	3	A	要	低減	人的・組織的対策	機器の管理手順を策定し、機器の設置や保守に係わる作業者全員に対して、周知し、理解したことの確認を行う。						
									...							
									物理的対策	...						
		医療情報システムの停止	対象事業者DCの有線LAN上のネットワーク機器において障害等に伴うアプリケーション提供に係る情報の滅失・破壊が生じ、見逃しや保存性は失われる	5	3	A	要		人的・組織的対策							
									物理的対策							
									技術的対策							
	施設への物理的侵入	アプリケーション提供に係る情報の物理的にアクセスされる	アプリケーション提供に係る情報の物理的にアクセスされる	5	3	A	要		人的・組織的対策							
									物理的対策							
									技術的対策							
		災害等	アプリケーション提供に係る情報処理が地震、水害、落雷、火災等並びにそれに伴う停電等により停止、不具合が生じる	5	3	A	要	低減	人的・組織的対策							
									物理的対策							
									技術的対策							

各項目の説明 | 1.1.リスクアセスメントシート

シート内容詳細（1）

プロセス	項目	説明
リスク特定	情報流	医療情報システム等の提供に関わる情報の流れを文章で表したもの
	分類	当該情報流で処理を行う対象の情報の安全管理上の重要度に応じた分類 例) 診療録や診療諸記録、処方箋、レセプト情報等は、「患者個人情報」等として分類し、「アプリケーションの設定情報」や「テストデータ」等とは区別した分類とする
	関連する脅威	医療情報システム等提供上の代表的な脅威 ガイドライン「表5-1 医療情報システム上等提供上の代表的な脅威」 ※ ISO /IEC 27005:2018の附属書C「典型的な脅威の例」を参考に、ガイドラインにて独自に整理されたものであり、医療情報に関する全ての脅威を網羅しているものではありません。したがって、対象事業者は、代表的な脅威以外の脅威についても、提供する医療情報システム等の構成に応じて検討し、リスクを特定することが求められます。
	特定したリスク	脅威が顕在化した場合に生じ得るリスク
リスク分析	影響度	当該リスクが顕在化した場合の医療情報システム等への機密性、完全性、可用性への影響度合い
	顕在化率	リスクが実際に顕在化する確率（攻撃手法が知られているリスクは顕在化率が高く、攻撃手法が知られておらず攻撃難易度が高い場合は顕在化率が低いと考えられる。）
	リスクレベル	影響度と顕在化率の掛け合わせでリスクのレベルわけを行う。 参考例) ガイドライン「表5-2 リスクレベルの分類例」

各項目の説明 | 1.1.リスクアセスメントシート

シート内容詳細（2）

プロセス	項目	説明
リスク評価	対応要否	リスクレベルに基づいたリスクへの対応要否
リスク対応	対応	リスク対応の選択肢を以下から選定 <ul style="list-style-type: none">- リスク低減- リスク回避- リスク移転（リスク共有）- リスク保有（リスク受容）
	対策の観点	リスク対策の観点を以下から選択 <ul style="list-style-type: none">- 人的・組織的対策- 物理的対策- 技術的対策
	情報システム・サービスの提供事業者の対策	AWS上で医療機関へシステム・サービスを提供する事業者として実施するリスク対策を記載
	AWSが実施している対策 <ul style="list-style-type: none">- AWSのインフラストラクチャー関連事項- AWSサービス関連情報	AWSのインフラストラクチャー関連事項 AWSインフラストラクチャーでの対策が必要なリスク対策へのAWSの対応 AWSサービス関連情報 AWS上で事業者がリスク対策を実施するうえで活用可能なAWSサービス情報
	医療機関へ対応を求める事項	対象事業者が設計したリスク対応策のうち、医療機関等による対応が必要となる内容 例）利用者ID、パスワードの管理など
	残存するリスク <ul style="list-style-type: none">- 影響度- 顕在化率- リスクレベル	リスク対策を実施し、医療機関等へ対応を求めた上で、それでも残存するリスク。 こちらについては再度リスク評価を実施し、リスクレベルの評価を実施する。

各項目の説明 | 1.2.リスク対応リファレンス

ガイドラインにて「最低限確認・対応すべき事項」とされたリスクシナリオについてのAWSおよび利用者がAWS上で取りうる対策を例示した参照シートです。

「リスク対応」を検討する際に、AWSが実施している対策の確認や、AWS上で利用者が実施する対応を検討する際に辞書的に利用できます。

1.2. リスク対応リファレンス					リスク対応		新舊システム・サービスの提供事業者の対応事項	医療機関等へ対応を求める事項
項目 (注番)	No.	内容	対応	対策の観点	対策の概要	AWSが実施している対策	新舊システム・サービスの提供事業者の対応事項	医療機関等へ対応を求める事項
					AWSのインフラストラクチャー関連事項		AWSサービス関連事項	
1	①	1.1①	権限のない第三者や内網不正による不正な閲覧や操作が行われる。	低級	人的・組織的対策	アクセス管理 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
1	②	1.1②	権限のない第三者や内網不正による不正な閲覧や操作が行われる。	低級	人的・組織的対策	アクセス管理 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
1	③	1.1③	権限のない第三者や内網不正による不正な閲覧や操作が行われる。	低級	人的・組織的対策	アクセス管理 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
2	④	1.1④	不正に出した機器や情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染	低級	人的・組織的対策	ウイルス対策 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
2	⑤	1.1⑤	不正に出した機器や情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染	低級	人的・組織的対策	ウイルス対策 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
2	⑥	1.1⑥	不正に出した機器や情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染	低級	人的・組織的対策	ウイルス対策 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
2	⑦	1.1⑦	不正に出した機器や情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染	低級	人的・組織的対策	ウイルス対策 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
2	⑧	1.1⑧	不正に出した機器や情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染	低級	人的・組織的対策	ウイルス対策 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
3	⑨	1.1⑨	情報の漏洩が不十分なまま、再利用が行われることで、情報漏洩が発生	低級	人的・組織的対策	情報の漏洩 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
3	⑩	1.1⑩	情報の漏洩が不十分なまま、再利用が行われることで、情報漏洩が発生	低級	人的・組織的対策	情報の漏洩 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。
3	⑪	1.1⑪	情報の漏洩が不十分なまま、再利用が行われることで、情報漏洩が発生	低級	人的・組織的対策	情報の漏洩 AWSは、ISO 27001 規格に合致して、AWS リソースに対する確実なアクセスについて最小限の基準を示す正式なポリシー、手順を策定しています。AWS SOCレポートには、AWS リソースに対するアクセスプロビデント	N/A	情報システム・サービスの提供事業者は、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層を策定する必要があります。アクセス管理層には以下内容を盛り込む必要があります。



「1.2.リスク対応リファレンス」シートでは、主に予防対策に注目してリスク対策例を記載しています。リスク対応には、予防対策だけでなく、発生時対策も考える必要がありますので、システム/サービスに応じた発生時対策を検討ください。

各項目の説明 | 1.2.リスク対応リファレンス

シート内容詳細

プロセス	項目	説明
リスク対応	項番	リスクシナリオの番号
	リスクシナリオ例	ガイドライン別紙2記載の最低限確認・対応すべき内容を記載したリスクシナリオの例
	対応	本リファレンスで示すリスク対策での対応の選択肢
	対策の観点	本リファレンスで示すリスク対策での対策観点
	対策の概要	本リファレンスで示すリスク対策の概要
	AWSが実施している対策 - AWSのインフラストラクチャー関連事項 - AWSサービス関連情報	AWSのインフラストラクチャー関連事項 本リファレンスで確認したリスクシナリオに対応するAWSが実施しているリスク対策 AWSサービス関連情報 本リファレンスで示す事業者のリスク対策に活用可能なAWSサービス情報 「3.AWSサービス関連情報」へのリンク
	情報システム・サービスの提供事業者の対応事項	本リファレンスで示す事業者のリスク対策例
	医療機関へ対応を求める事項	本リファレンスで示す事業者のリスク対策例を実施したうえで医療機関へ対応を求める事項

各項目の説明 | 1.3.リスクシナリオ例

ガイドライン別紙2の「最低限確認すべき事項」としてのリスクシナリオ例を一覧としてまとめたシートです。「リスク特定」を行う際の参考に利用できます。

1.3.リスクシナリオ例					
	項番	シナリオ例			厚生労働省 ガイドライン
		大項目	No.	内容	
	1	1.1. 規程・手順の策定	1.1①	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	6.3 C3
	2		1.1②	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	6.5 C10
	3		1.1③	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	6.7 C1 6.7 C2 6.7 C4(a)
	4		1.1④	持ち出した機器に格納された情報が漏洩するもしくは、持ち帰った機器から不正なプログラムが感染拡大する。	6.8 C7 6.8 D4
	5		1.1⑤	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	6.9 C1 6.9 C2 6.9 C3 6.9 C4
	6		1.1⑥	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	7.1 C【医療機関等に保存する場合】(5)3、(5)2
	7	1.2. 個人情報を含まないテストデータの利用	1.2	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	6.5 C5
	8	1.3. 守秘義務に係る契約	1.3①	医療情報システム等提供に係る職員(派遣従業員含む)のうち悪意をもった者による情報漏洩が行われる。	6.6(1) C1 6.6(1) C3 6.6(2) C1
					6.6(2) C2 6.8 C6



リスク特定は、一般的に考えられるリスクのみならず、システム/サービスの特性に応じた固有のリスクも特定していくものです。ガイドライン別紙2および本シート記載のリスクシナリオ例のみに囚われず、リスクの発見・認識を行っていただくことが重要です。

各項目の説明 | 1.3.リスクシナリオ例

シート内容詳細

プロセス	項目	説明
リスク特定	リスクの観点	「人的・組織的」、「物理的」、「技術的」の3つからなるリスクの観点
	項番	リスクシナリオ項番
	シナリオ例 - 大項目 - No - 内容	ガイドライン別紙2記載の最低限確認・対応すべき内容を記載したリスクシナリオの例 大項目 ガイドライン別紙2記載の対策の「大項目」 No ガイドライン別紙2の対策項目「大項目番号 + 小項目番号」 内容 ガイドライン別紙2の「対策項目で対応できるリスクシナリオ例」
	厚生労働省ガイドライン	リスクシナリオ例が対応する厚生労働省ガイドラインでの該当箇所

ガイドライン6章の制度上の要求事項に対するAWSが実施している対策およびAWS上で利用者が取りうる対策を例示した参照シートです。
こちらのシートの対策例を参考に、要求事項への対応を検討出来ます。

[illegible]

各項目の説明 | 2.制度上の要求事項

シート内容詳細

カテゴリ	項目	説明
制度上の要求事項	項番	ガイドライン要求事項の章・節・番号およびタイトル
	項番タイトル	
	サブ項番	
	サブタイトル	
	番号	
	ガイドラインとして必要な要求事項	ガイドライン要求事項本文
関連するAWS情報	AWSのインフラストラクチャー関連事項	本リファレンスで確認したリスクシナリオに対応するAWSが実施しているリスク対策
(リファレンス情報)	AWSサービス関連情報	本リファレンスで示す事業者のリスク対策に活用可能なAWSサービス情報 「3.AWSサービス関連情報」へのリンク
	情報システム・サービスの提供事業者（お客様）の該当事項	本リファレンスで示す事業者が必須で対応すべき内容
	推奨される追加の実施事項	必須ではないが、実施が推奨される事業者での対応方法
	AWS認証情報 (ISO/IEC27001, Annex.A and ISO/IEC27017)	該当要求項目のISO/IEC27001 Annex.AおよびISO/IEC27017とのマッピング情報

各項目の説明 | 3.AWSサービス関連情報

AWS上で利用者がリスク対策/制度上の要求事項への対応を実施する際に、活用できるAWSサービスの情報を整理したものです。

これらのAWSサービスを利用することで、効率的にガイドライン対応を進めることができます。

3.AWS サービス関連情報					
サービス 種別	INDEX	AWSサービス	機能	サービス概要	詳細URL
Compute					
	■E	Amazon EC2 (Amazon Elastic Compute Cloud)	仮想サーバ	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 EC2 https://aws.amazon.com/jp/ec2/?ref=aws_what-new&sort-by=item.additionalFields.postDataTime&ec2-what-new&sort-order=desc
	■E	Amazon EBS (Amazon Elastic Block Store)	インスタンスストレージ	Amazon EBS は、Amazon EC2 にアタッチして使用するブロックストレージサービスです。(仮想ディスク) Amazon EBS で保管時のデータを暗号化する場合、EBS ボリュームごとに固有のボリューム暗号化キーが生成されます。各ボリュームキーの暗号化に使用するマスターキーは、AWS Key Management Service で柔軟に選択することができます。 ・データの廃棄について Amazon EBS 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。お客様は、データの廃棄処理において、Amazon EBSに保存されたデータを消去することでデータを廃棄したことになりますが、さらにAWS Key Management Serviceによる暗号鍵も廃棄することで、その廃棄操作をもって廃棄証明とすることも可能になります。	■Amazon EBS https://aws.amazon.com/jp/ebs/?ref=aws_what-new&sort-by=item.additionalFields.postDataTime&ebs-what-new&sort-order=desc ■Amazon EBS 暗号化 https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/EBS-Encryption.html ■クラウドにおける安全なデータの廃棄 https://aws.amazon.com/jp/blog/news/data_disposal/
		Amazon EFS (Amazon Elastic File System)	EC2用フルマネージド型ファイルシステム	Amazon Elastic File System (Amazon EFS) は、AWS クラウドサービスおよびオンプレミスリソースで利用できる完全マネージド型の NFS ファイルシステムです。	■Amazon Elastic File System https://aws.amazon.com/jp/efs/



AWSサービス関連情報は、2020年10月時点のサービス内容をもとにしたものです。最新の情報はAWS公式ウェブサイト (<https://aws.amazon.com>)にてご確認ください。

資料作成には十分注意しておりますが、資料内の説明とAWS公式ウェブサイト記載の説明に相違があった場合、AWS公式ウェブサイトの説明を優先とさせていただきます。

各項目の説明 | 3.AWSサービス関連情報

シート内容詳細

項目	説明
サービス種別	AWSサービスの分類
INDEX	分類内でのアルファベット順インデックス
AWSサービス	AWSサービス名称
機能	該当AWSサービスにおけるガイドライン対応に利用可能な機能
サービス概要	AWSサービス概要説明
詳細URL	AWSサービス詳細掲載URL

最後に

本リファレンスの作成にあたってはビジネス上競合となりうることもある4社が、いままでの医療・製薬業界でのIT利活用のノウハウを結集し、皆様のクラウドの利活用促進を行うために、協力体制を作り、調査、検討を行い、作成した成果になります。アマゾン ウェブ サービス ジャパンにも調査など、多大な協力を頂きました。

本取り組みがクラウド活用の促進により医療業界における課題解決の一助となること、ひいては患者さんがより良い医療を受けられる環境づくりの一助になれば幸いです。

「**医療情報システム向けAWS利用リファレンス**」の入手は、下記ソリューションプロパイダまでお問い合わせください。各社のホームページからもダウンロードできるようになります。



参加各社では、医療・製薬業界でのIT利活用に向けたソリューションをご提供しております。