

医療情報システム向け AWS利用リファレンスの概要

2019年6月12日

V1.2

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
フィーラーシステムズ株式会社

更新履歴

#	バージョン	更新箇所	更新内容	更新日
1	1.0	全体	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

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活用されはじめています。

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ガイドライン（以下、3省3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、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の5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3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、5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3ガイドラインとは？



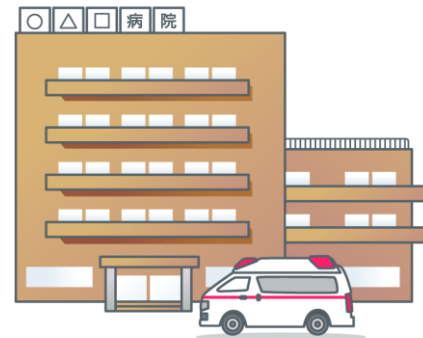
一般的に診療録に記録される情報

- 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3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「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情報処理事業向けガイドライン」

^{*1} 従来3省4ガイドラインと呼ばれる4つのガイドラインの遵守が求められてきましたが、
2018年7月の総務省ガイドラインの改定により、3省3ガイドラインとなっています。

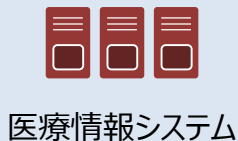
3省3ガイドライン遵守が求められる主体



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/ASP事業者 (外部委託先)
によるサービス提供

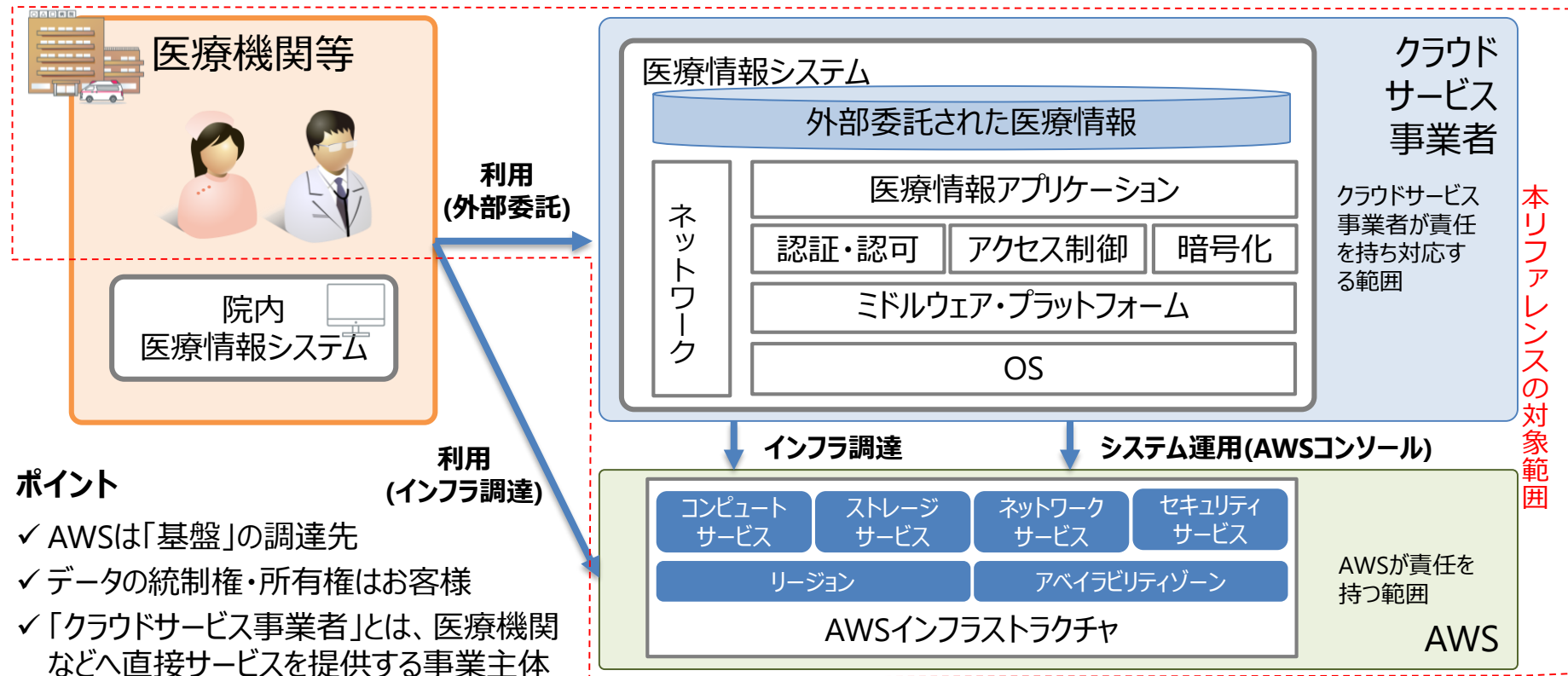
【総務省】
クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン

【経済産業省】
医療情報を受託管理する情報処理事業者向けガイドライン

【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
- ✓ 「クラウドサービス事業者」とは、医療機関など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3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3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

参照

医療情報の委託を
受けた事業者の
お客さま

参照

問合せ

支援

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
(総務省版)

医療情報システム向けAWS利用リファレンス
(経済産業省版)

基準に
対応

3省3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版)

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 (第1版)

医療情報を受託管理する情報
処理事業者向けガイドライン
(第2版)

作成

調査
協力

Amazon Web Services
Japan Inc.

Canon

キヤノン IT ソリューションズ株式会社



DXC.technology

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

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

医療情報を受託管理／医療情報システムをサービス提供されるソリューションプロバイダ

2) 整理方法

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

- AWS基準を取り入れることで対応不要な項目
- 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
- 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

⇒AWS基準で対応可能な項目の対応内容の整理

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ダンス

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版」（平成29年5月）

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 第1版」（平成30年7月）

経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン 第2版」（平成24年10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

AWS対応・認証取得済

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

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受託事業者の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

本リファレンスは2部構成になり、主要項目は以下です。

1) ガイドライン対応表（リファレンス本体）

- a. ガイドラインの要求事項
- b. AWS該当事項に関する対応内容および対応可能である根拠
 - a) 公開文書（ホワイトペーパー）
 - b) 第3者認証
 - c) AWS内部情報
- c. 受託事業者（情報処理事業者）該当事項に関する必要な対応
- d. 追加の推奨事項

2) 参考アーキテクチャー

受託事業者で必要な対応および追加の推奨事項を実施するうえで、必要なサービスの組み合わせを例示

ガイドライン対応表

ガイドラインの 要求事項	AWSインフラストラクチャーの 対応情報	AWSサービス 関連情報	クラウドサービス事 業者の対応事項	追加の推奨事項	根拠となる ISO/IEC27001 の該当箇所
<p>(表1)「」で示される実施事項 ガイドラインとして必要な実施事項</p>	<p>関連するAWS情報 AWSのインフラストラクチャー関連事項</p>	<p>AWSサービス関連情報</p>	<p>クラウドサービス事業者(お客様)の該当事項</p>	<p>推奨される追加の実施事項</p>	<p>AWS認証情報 (ISO27001, Annex A and ISO27017)</p>
<p>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。</p>	<p>AWSの従属関連の詳細、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 サービス条項-この追加条項は、お客様による特定のサー ビスのご利用に際して適用されます 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際して適 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、 サービスが適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適用、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 こととなります。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、が設定さ 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</p>	<p>-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承認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審査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 (MDA) 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/</p>	<p>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。</p>	<p>N/A</p>	<p>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.LD.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.LD.6.3.1</p>
<p>情報システムについての管理責任を負い、これについて 十分な機能的能力及び信頼を有する責任者(システム管 理者)を設置する。</p>	<p>AWSの従属関連の詳細、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 サービス条項-この追加条項は、お客様による特定のサー ビスのご利用に際して適用されます 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際して適 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/</p>	<p>-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承認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審査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 (MDA) が含まれます。 詳細、最新情報は下記を参照ください。</p>	<p>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/管理状況について監視機関等へ 定期的に報告する必要があります。</p>	<p>N/A</p>	<p>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.LD.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.LD.6.3.1</p>

ガイドライン対応表 記載例

～AWS基準を取り入れることで対応不要な項目～

ガイドライン要求事項

7.5 物理的安全対策

7.5.1 医療情報処理施設の建物に関する要求事項

(1)

情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認すること。

- 医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理が行われていること。
- 傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。
- 建物、部屋に対する不正な物理的な侵入を抑止するため、監視カメラ等の侵入検知装置を導入すること。
- 自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。

要求事項出典)

「医療情報を受託管理する情報処理事業向けガイドライン（第2版）」経済産業省の要求事項より

AWSの対応

(前略)

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。

(後略)

※正確な内容はリファレンス本体を参照ください。

ガイドライン対応表 記載例

～AWS基準を取り入れても、ユーザー対応が必要な項目～

ガイドライン 要求事項	AWSの対応	情報処理事業者・ 利用者に必要な対応	推奨される追加の 実施事項
8.2 外部保存契約終了 時の処理について 医療機関等と情報処理事業者間で廃棄処理 手順について定め、合意 しておく必要がある。	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。	情報処理事業者は医療機関等と データの廃棄処理手順について定め、 合意しておく必要があります。 情報処理事業者は、自身のデータ の統制と所有権を保持します。 (中略) 特定の方法で全データをワイプする 必要がある場合、情報処理事業者 自身で Amazon EBS のワイプ作 業を行うこともできます 。情報処理 事業者がしかるべき手順でワイプを 実施してからボリュームを削除する ことで、医療機関等との合意事項を 満たすようにします。 (後略)	AWS上に格納する機密データは、 AWS Key Management Service で管理される暗号鍵を利用して暗 号化することを推奨します。契約終 了時に 暗号鍵そのものを廃棄する ことで、データ消去に相当すると いった対応を考慮することも可能 である。 Amazon Elastic Block Store (EBS) で追加のストレージを使う場 合などはボリュームを暗号化するこ とができます。S3を使う場合はServer Side Encryptionでバケット・ファイル 単位に暗号化することができます。 (後略)

要求事項出典)

「医療情報を受託管理する情報処理事業者向けガイドライン（第2版）」経済産業省の要求事項より

※正確な内容はリファレンス本体を参照ください。

ガイドライン対応表 記載例

～AWSが対象外でユーザー対応が必要な項目～

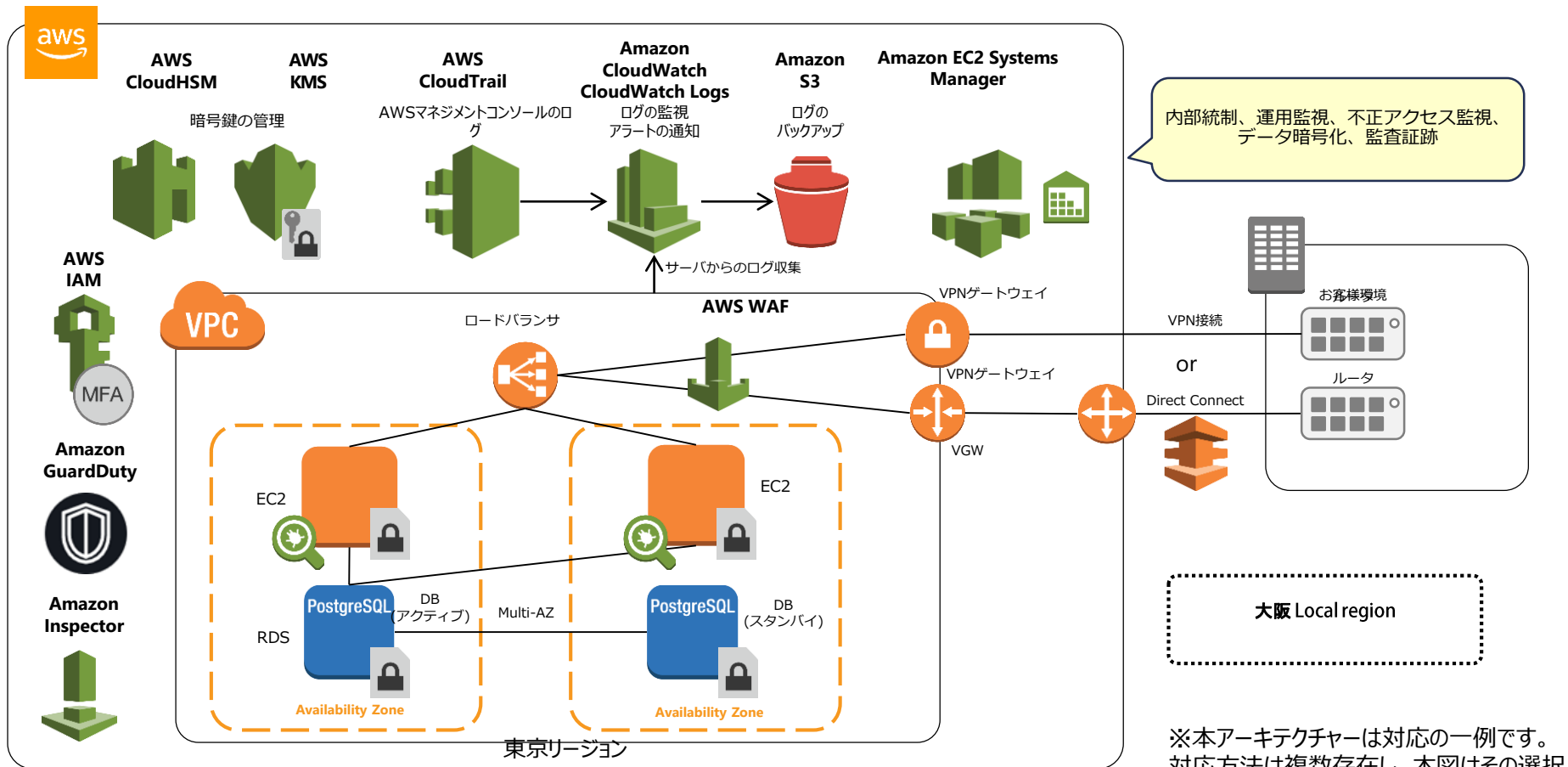
ガイドライン 要求事項	AWSの対応	情報処理事業者・ 利用者に必要な対応	推奨される追加の 実施事項
7.9 医療情報システムの 改造と保守 (1) オペレーティングシステムの アップグレード、セキュリティ パッチの適用を行う場合、 医療情報システムに対す る影響を評価し、試験結 果を確認してから実施する こと。	N/A - 左記の要件への対応は 情報処理事業者の該当事項 となります。 なお、AWS のシステム開発ライ フサイクル(SDLC) は、業界のベ ストプラクティスを組み込んでおり、 これにはAWSセキュリティによる 公式の設計レビュー、脅威のモ デリング、リスク評価の完遂など が含まれています。詳細につい ては、AWSセ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。	情報処理事業者は、OSのアップ グレード、セキュリティパッチの適用 などを医療情報システムに対し適 用評価およびテスト・実施を行う 責任があります。 また、情報処理事業者はRDSな どのマネージドサービスの利用時に は、パッチ適用の実施有無や実 施時間帯を自らコントロールする 必要があり、本番環境への適用 前に事前にステージング環境など で影響評価を行うことが求められ ます。	AWS Systems Manager やEC2 Systems Manager を利用し、OSの セキュリティパッチ適用などの 作業を自動化することがで きます。

要求事項出典)

「医療情報を受託管理する情報処理事業者向けガイドライン（第2版）」経済産業省の要求事項より

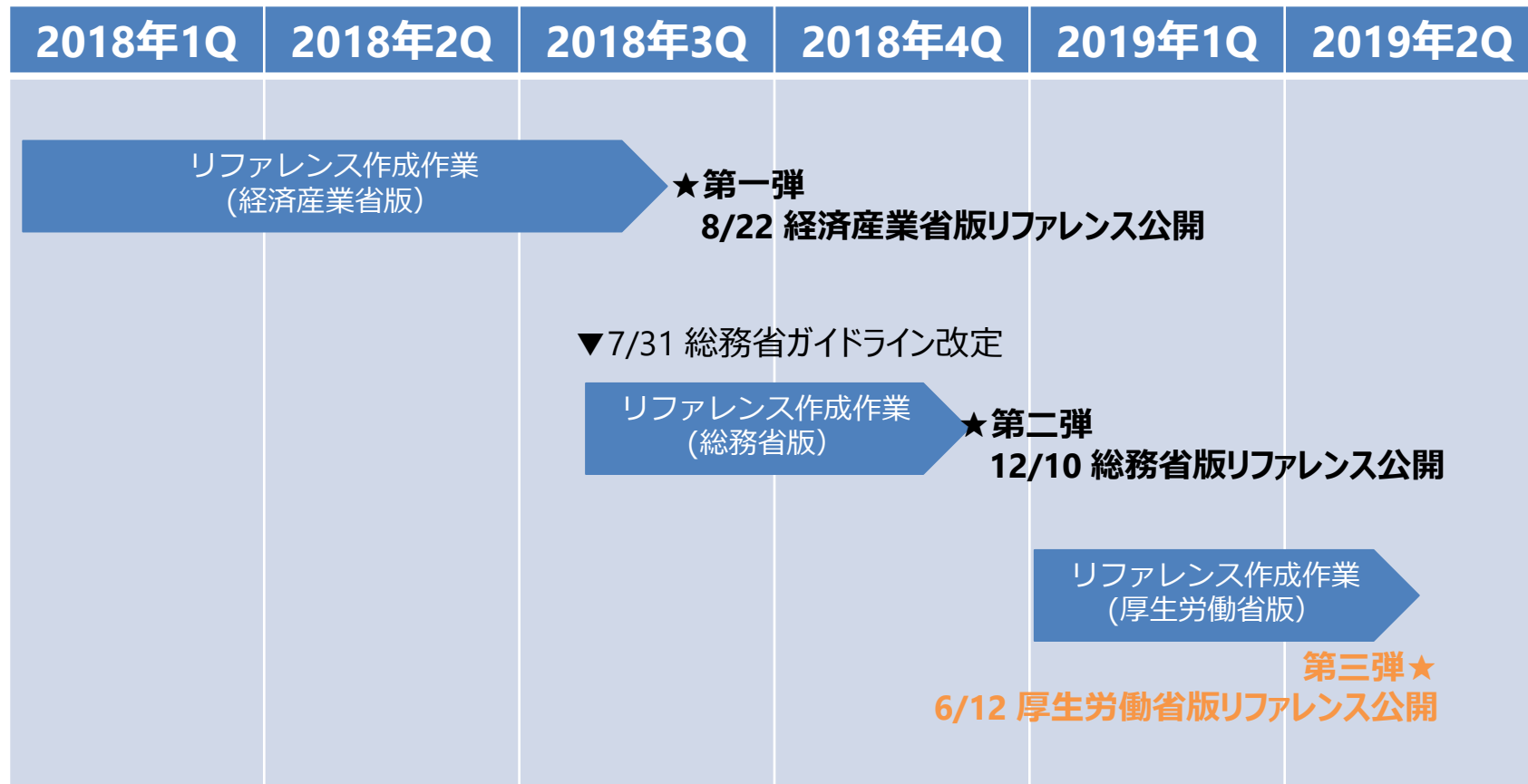
※正確な内容はリファレンス本体を参照ください。

医療情報システム向け参考アーキテクチャー



※本アーキテクチャーは対応の一例です。
対応方法は複数存在し、本図はその選択
肢を何ら制限するものではありません。

公開スケジュール



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5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う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。