GxP 関連システムにおける AWS 製品の使用

2021 年 3 月

注記

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と利用方法について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤーまたはライセンサーからの契約上の義務または保証をもたらすものではありません。AWS の製品やサービスは、明示または暗示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任と義務は、AWS 契約により規定されます。本書は、AWS とお客様の間で締結されるいかなる契約の一部でなく、その内容を修正するものでもありません。

目次

要約

本ホワイトペーパーは、AWS における GxP に関連するコンプライアンスとセキュリティへの取り組みと、GxP の観点から AWS 製品の使用に関するガイダンスをお客様に提供します。本ホワイトペーパーのコンテンツは、バリデーション済みの GxP システムで AWS 製品を現在使用中の製薬会社や医療機器メーカーのお客様およびソフトウェアパートナーと共同で作成されました。

1 はじめに

2020 年発行の Deloitte による Global Life Sciences Outlook によると、ライフサイエンス分野におけるクラウド技術の優先順位は着実に上がっています。これは、お客様が規制された IT システムを運用するための信頼性、拡張性、安全性の高いソリューションを求めているためです。アマゾンウェブサービス (AWS) は、最も機密性の高いワークロードを、お客様がクラウドで実行できるよう設計されたクラウドサービスを提供します。これには、Good Manufacturing Practice (GMP) 、Good Laboratory Practice (GLP) 、Good Clinical Practice (GCP) 、つまり、GxP をサポートするコンピュータ化されたシステムが含まれます。GxP ガイドラインは、アメリカ食品医薬品局 (FDA) によって制定され、医療機器、医薬品、生物製剤、その他の食品および医療製品産業の安全な開発と製造を保証するために設けられたものです。

このホワイトペーパーの冒頭のセクションでは、責任共有モデルの一環でもあり、また情報セキュリティ管理のための AWS 品質管理システムにも関わる、GxP 要件をサポートするコンプライアンス、およびセキュリティに対する AWS のサービスと組織的アプローチについて概説します。その後、AWS サービスを使用しながら GxP に準拠した環境を実装する上で役に立つ情報について説明します。多くのお客様は、既に GxP 要件に関わる規制についての解釈に業界ガイダンスを活用されています。したがって、このホワイトペーパーの基礎として使用した主要な業界ガイダンスは、事実上クラウドコンピューティングの優れたプラクティスの一種である、国際製薬技術協会 (ISPE) による自動化製造実践規範 (GAMP) です。

以降のコンテンツは、GxP 環境における AWS サービスの使用に関する情報を提供していますが、お客様の GxP のポリシーと手順が規制コンプライアンス要件を満たしているか否かについては、最終的にはお客様の助言機関に相談してください。

> AWS 製品、プライバシー、データ保護に関する考慮事項について、より具体的な情報を記載したホワイトペーパーはこちらから入手可能です。https://aws.amazon.com/compliance/

1.1 AWS について

2006 年に、アマゾンウェブサービス (AWS) は、従量課金制の Web サービスの形で企業への IT インフラストラクチャサービスの提供を開始しました。今日では、AWS は世界中の国々の数十万社もの企業に利用され、信頼性が高く、スケーラブルで、低コストで運用できるインフラストラクチャプラットフォームをクラウド上で提供しています。AWS を利用することで、企業はサーバーなどの IT インフラストラクチャを、何週

間または何か月も前から計画し調達する必要がなくなりました。かわりに、何百・何千ものサーバーを数分で即座に起動し、より迅速に結果を出すことが可能です。世界中のデータセンターから 200 種類以上のフル機能サービスを提供するとともに、AWS は、コンピューティング、ストレージ、データベース、ネットワーキング、セキュリティ、分析、モバイル、開発者ツール、管理ツール、IoT、エンタープライズアプリケーションを含む幅広いグローバルクラウドベースの製品の利用を可能にしています。AWS の急速なイノベーションは、お客様がご自身やエンドユーザーにとって最も重要なことに、差別化につながらない重労働なしで、集中することを可能にします。

1.2 AWS ヘルスケアとライフサイエンス

豊富な経験と高い信頼性を備えたライフサイエンスにおけるクラウド業界のリーダーへの需要の高まりを受け、AWS は 2014 年にゲノムおよびライフサイエンス専用のプラクティスを開始しました。今日の AWS ライフサイエンスプラクティスチームは、平均 17 年以上の業界での経験、最高医療責任者 (CMO) 、最高デジタル責任者(CDO) 、医師、放射線医、研究員などの役職の経験を持つメンバーによって構成されています。AWS のゲノミクスおよびライフサイエンスのプラクティスは、医薬品、バイオテクノロジー、医療機器、ゲノミクスなどの企業やスタートアップ企業、大学、政府機関、保険者、医療機関などを含む、ライフサイエンスにおいて大規模エコシステムを持つお客様にサービスを提供しています。お客様のケーススタディーは、こちらから入手可能です。https://aws.amazon.com/health/customer-stories

AWS が持つゲノミクスおよびライフサイエンスのプラクティスのリソースに加え、お客様は AWS ライフサイエンスコンピテンシーパートナーと協力することで、費用対効果の高いストレージとコンピューティング機能、高度な分析、患者の個別化メカニズムなど、ライフサイエンスバリューチェーン全体を通じてイノベーションを促進し、効率を向上させることができます。AWS ライフサイエンスコンピテンシーパートナーは、AWS でのライフサイエンスソリューションの構築において、技術的な専門知識とお客様の成功事例を実証しています。AWS ライフサイエンスコンピテンシーパートナーの全リストは、 こちらから入手可能です。
https://aws.amazon.com/health/lifesciences-partner-solutions

1.3 AWS サービス

アマゾンウェブサービス (AWS) は、高い可用性と信頼性を実現するためのスケーラブルなクラウドコンピューティングプラットフォームを備え、お客様にさまざまなアプリケーションを実行するためのツールを提供しています。お客様のシステムやデータ

の機密性、完全性、可用性の保護を支援することは、AWS にとって、お客様からの信頼と信用の維持と同様に、最重要です。

オペレーティングシステムやデータベースエンジンなどの他の汎用 IT 製品と同様に、AWS は ISO、NIST、SOC などの数多くの IT 品質とセキュリティ基準に準拠した COTS（商用オフザシェルフ）IT サービスを提供しています。本ペーパーの目的上、ここでは COTS の定義を米国政府全体の調達およびセキュリティ評価プログラムである FedRAMP が定めた定義のとおりに使用します。FedRAMP は COTS の定義について、連邦調達規則 (FAR) を参照し、次のように概説を示しています。

- 一般的に認められているカタログに基づき、商業市場で大規模の販売、または高い競争力で提供、販売されている製品またはサービス。
- 変更やカスタマイズなしで提供される。
- 標準的な商取引条件の下で提供される。

GAMP ガイドライン下（GAMP 5: コンピュータ化システムの GxP 適合へのリスクベースアプローチ）の運用では、GxP コンプライアンス環境を実装している組織は、個々の GAMP ソフトウェアとハードウェアカテゴリ（例えば、オペレーティングシステム、データベースマネージャ、セキュリティソフトウェアなどのインフラストラクチャソフトウェアの「ソフトウェアカテゴリ 1」、またはカスタムソフトウェア、特注ソフトウェア用の「カテゴリ 5」など）を使用して AWS サービスを分類する必要があります。バリデーション済みアプリケーションに AWS サービスを利用している組織は、ほとんどの場合、「ソフトウェアカテゴリ 1」に分類しています。

AWS では、複数のカテゴリに分類される製品を提供しています。以下に、コンピューティング、ストレージ、データベース、ネットワーキングとコンテンツ配信、セキュリティとコンプライアンスにおける AWS サービスのサブセットを示します。このホワイトペーパーの後述のセクション「GxP システムでの AWS 製品」に、AWS サービスを使用して GxP コンプライアンス環境を実装する上で有益な情報が記載されています。

表 1: グループ別の AWS サービスのサブセット

グループ	AWS 製品
コンピューティング	Amazon EC2、Amazon EC2 Auto Scaling、Amazon Elastic Container Registry、Amazon Elastic Container Service、Amazon Elastic Kubernetes Service、Amazon Lightsail、AWS Batch、AWS Elastic Beanstalk、AWS

	Fargate、AWS Lambda、AWS Outposts、AWS Serverless Application Repository、AWS Wavelength、VMware Cloud on AWS
ストレージ	Amazon Simple Storage Service (Amazon S3)、Amazon Elastic Block Store (Amazon EBS)、Amazon Elastic File System (Amazon EFS)、Amazon FSx for Lustre、Amazon FSx for Windows File Server、Amazon S3 Glacier、AWS Backup、AWS Snow Family、AWS Storage Gateway、CloudEndure Disaster Recovery
データベース	Amazon Aurora、Amazon DynamoDB、Amazon DocumentDB、Amazon ElastiCache、Amazon Keyspaces、Amazon Neptune、Amazon Quantum Ledger Database (Amazon QLDB)、Amazon RDS、Amazon RDS on VMware、Amazon Redshift、Amazon Timestream、AWS Database
ネットワーキングとコンテンツ配信	Amazon VPC、Amazon API Gateway、Amazon CloudFront、Amazon Route 53、AWS PrivateLink、AWS App Mesh、AWS Cloud Map、AWS Direct Connect、AWS Global Accelerator、AWS Transit Gateway、Elastic Load Balancing
セキュリティ、アイデンティティ、コンプライアンス	AWS Identity & Access Management (IAM)、Amazon Cognito、Amazon Detective、Amazon GuardDuty、Amazon Inspector、Amazon Macie、AWS Artifact、AWS Certificate Manager、AWS CloudHSM、AWS Directory Service、AWS Firewall Manager、AWS Key Management Service、AWS Resource Access Manager、AWS Secrets Manager、AWS Security Hub、AWS Shield、AWS Single Sign-On、AWS WAF

AWS 製品の完全なポートフォリオの詳細と仕様はオンラインで公開されており、こちらから入手可能です。https://aws.amazon.com/

1.4 AWS クラウドセキュリティ

AWS のインフラストラクチャは、現在利用できるクラウドコンピューティング環境で、最も柔軟で安全に設計されたものの 1 つとなっています。これは、お客様がアプリケーションやデータを迅速かつ安全にデプロイするための、きわめてスケーラブルで信頼性の高いプラットフォームを提供するように設計されています。このインフラストラクチャは、セキュリティのベストプラクティスや基準に準拠するだけでなく、クラウド特有のニーズも考慮して構築、管理されています。AWS は、冗長化された階層型コントロール、継続的なバリデーションとテスト、広範なオートメーションを通じ

て、基盤となるインフラストラクチャのモニタリングと保護を 24 時間年中無休で行っています。

AWS クラウドを利用する利点を述べてくださるお客様からの声は数多くあり、特に AWS が提供するセキュリティ機能は、お客様のオンプレミスの機能をはるかに上回るという点を特に強調していただいています。

> 「私たちは『クラウドにおけるセキュリティ問題』に関する都市伝説について聞いてきましたが、AWSについて調べるほど、AWSは安全な環境であり、安心して使用できることがわかりました。」
>
> **- 守谷 祥広 氏、公認情報システム監査人 (CISA)、HOYA**

> 「AWSが実現するセキュリティ認証レベルを達成する方法は私たちにはありませんでした。AWSクラウドにおける顧客の論理的分離に大きな信頼を寄せています。特にAmazon VPCにより、当社の特定の要件を満たすように仮想ネットワーク環境をカスタマイズ出来ます。」
>
> **- Michael Lockhart, IT Infrastructure Manager, GPT**

> 「遠隔医療において保護された医療情報を扱う場合、セキュリティは最優先事項です。今、私たちが行っていることを続けるには、AWSが絶対に必要です。セキュリティとコンプライアンスはテーブルステークス（当たり前のように必要な要素）です。それがないなら、何も始められません。」
>
> **- Cory Costley, Chief Product Officer, Avizia**

ヘルスケアやライフサイエンス企業をはじめとする、さらに多くのお客様の声は、こちらからご覧いただけます。https://aws.amazon.com/compliance/testimonials/

IT セキュリティは、多くの場合、お客様のコアビジネスではありません。IT 部門は限られた予算で運用され、限られたリソースでデータセンターとソフトウェアのセキュリティを確保しなくてはなりません。AWS の場合は、セキュリティは我々のコアビジネスの基盤を成すため、以下で詳しく説明するように、クラウドのセキュリティの確保とお客様のクラウド内のセキュリティの確保の支援に大量のリソースが投入されています。

1.5 セキュリティ責任共有モデル

セキュリティとコンプライアンスは、AWS とお客様の間で共有される責任です。この共有モデルは、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的なセキュリティに至るまでの要素を AWS が運用、管理、制御するため、お客様の運用上の負担を軽減するために役立ちます。お客様には、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、および AWS が提供するセキュリティグループファイアウォールの設定に対する責任とその管理を担っていただきます。使用するサービス、それらのサービスの IT 環境への統合、および適用される法律と規制によって、お客様の責任範囲は異なりますので、お客様には、サービスの選択を慎重に検討していただく必要があります。

次の図は、責任共有モデルの概要を示しています。図内で区別されている責任は、通常、クラウド「の」セキュリティとクラウド「における」セキュリティと呼ばれており、以下に詳しく説明します。

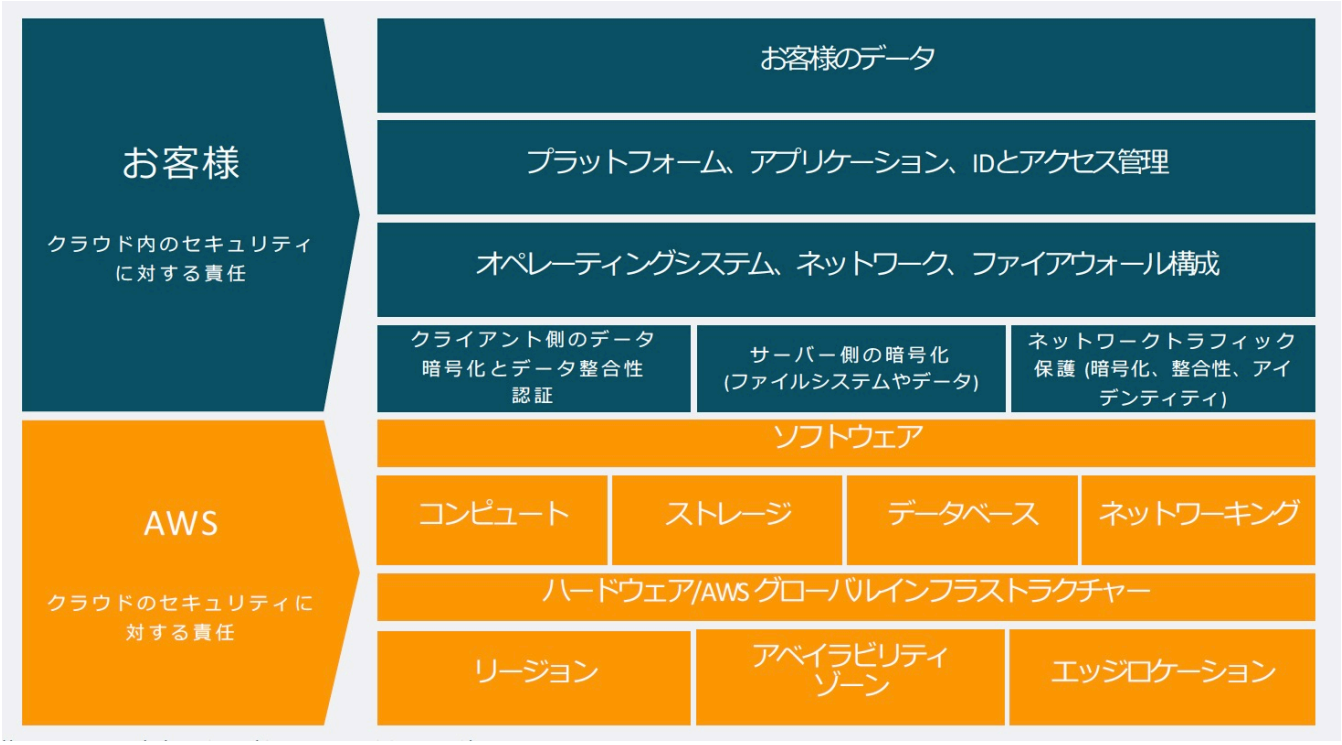

図 1: AWS 責任共有モデル

AWS は、AWS クラウドで提供されるすべてのサービスを実行するインフラストラクチャ**の**セキュリティとコンプライアンスの保護について責任を負います。クラウドセ

キュリティは AWS の最優先事項です。AWS のお客様に、最もセキュリティに配慮した組織の要件を満たすよう構築されたデータセンターやネットワークアーキテクチャの利点を活用していただけます。このインフラストラクチャは、AWS クラウドサービスを実行するハードウェア、ソフトウェア、ネットワーク、施設で構成されています。

お客様は、お客様が設定したシステムと AWS 上でプロビジョニングされたサービスで構成される、クラウド**における**セキュリティとコンプライアンスについて責任を負います。AWS クラウドにおける責任は、お客様が選択した AWS クラウドサービス、そして最終的にはお客様のセキュリティに関する責任の一環として実行する構成作業の量によって決まります。たとえば、Amazon Elastic Compute Cloud (Amazon EC2) などのサービスは、Infrastructure as a Service (IaaS) に分類されているため、必要なすべてのセキュリティ構成および管理タスクはお客様に実行していただく必要があります。Amazon EC2 インスタンスをデプロイした場合、お客様は、ゲストオペレーティングシステムの管理（更新やセキュリティパッチなど）、インスタンスにインストールしたアプリケーションソフトウェアやユーティリティの管理、AWS より各インスタンスに提供される（セキュリティグループと呼ばれる）ファイアウォールの構成に責任を負います。Amazon S3 や Amazon DynamoDB など抽象化されたサービスの場合は、インフラストラクチャレイヤー、オペレーティングシステム、プラットフォームの運用を AWS が行い、お客様はエンドポイントにアクセスしてデータを保存、取得します。お客様はデータならびにコンポーネント設定の管理 （暗号化オプションを含む）、アセットの分類、IAM ツールでの適切な権限の適用について責任を負います。

AWS のセキュリティ責任共有モデルは、IT 統制にも適用されます。AWS とお客様との間で IT 環境を運用する責任が共有されているように、IT 統制の管理、運用、検証も共有されています。もともとはお客様が管理していたであろう、AWS 環境にデプロイ済の物理インフラストラクチャに関わる統制を、AWS が管理することにより、お客様のコントロールの運用にかかる負荷を軽減することができます。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、（新しい）分散統制環境を構築する作業は、お客様の判断で行うことができます。移行後は、AWS の統制やコンプライアンスに関する文書と、このホワイトペーパーで後述するテクニックを活用し、必要に応じて統制の評価と検証の手順を実行することができます。以下は AWS、お客様、またはその両方によって管理される統制の例です。

継承される統制 - お客様が AWS から完全に継承する統制です。

- 物理統制と環境統制

共有される統制 - インフラストラクチャレイヤーとお客様レイヤーの両方に適用される統制です。ただし、コンテキストや観点は完全に異なります。共有統制では、AWS がインフラストラクチャに対する要件を提供し、お客様は AWS のサービスの使用に対して独自の統制を実装する必要があります。以下に例を示します。

- パッチ管理 – AWS はインフラストラクチャの不具合に対するパッチ適用および修復に責任を負いますが、ゲスト OS およびアプリケーションのパッチ適用の責任はお客様が負います。
- 構成管理 - AWS はインフラストラクチャのデバイスの構成を保守しますが、自社のゲストオペレーティングシステム、データベース、およびアプリケーションの構成の責任はお客様が負います。
- 啓発とトレーニング - AWS は AWS の従業員をトレーニングしますが、お客様の従業員のトレーニングはお客様が実施します。

お客様固有 – AWS のサービスにデプロイするアプリケーションに基づいて、お客様がすべての責任を負う統制です。以下に例を示します。

- データ管理 - 例えば、暗号化を有効化する Amazon S3 へのデータの配置。

統制にはお客様固有のものも存在するため、AWS はお客様による実装を容易にするためのツールとリソースを提供するよう努めています。

AWS の管理下にあるネットワークやサーバーインフラストラクチャについての、物理的および運用上のセキュリティプロセスの詳細については、AWS クラウドセキュリティを参照してください。

アマゾンウェブサービス (AWS) で実行するアプリケーションのセキュリティインフラストラクチャおよび構成を設計しているお客様は、Best Practices for Security, Identity, & Compliance をご参照ください。

1.6 AWS 認定と認証

AWS グローバルインフラストラクチャは、セキュリティのベストプラクティスに加えて多様なセキュリティコンプライアンス基準に従って設計、管理されています。AWS であれば、世界で最も安全なコンピューティングインフラストラクチャ上にウェブアーキテクチャを確実に構築できます。AWS がお客様に提供する IT インフラストラクチャは、セキュリティのベストプラクティス、および各種 IT セキュリティ基準に合わせて設計、管理されています。これには、ライフサイエンス業界のお客様に非常に関連が深い、以下が含まれます。

- SOC 1、2、3
- ISO/IEC 9001 / ISO/IEC 27001 / ISO/IEC 27017 / ISO/IEC 27018
- HITRUST
- FedRAMP
- CSA Security, Trust & Assurance Registry (STAR)

今のところ、クラウドサービスの GxP コンプライアンスを認定する具体的な制度はありません。しかし、このホワイトペーパーに記載されている統制やガイダンス、ならびに AWS が提供するさらなるリソースにより、AWS サービスと GxP の互換性について情報を得ることはできます。これらを活用し、独自の GxP コンプライアンスソリューションの設計と構築が可能です。

AWS は、AWS Artifact を通じて、セキュリティやコンプライアンスについてのレポートや厳選した一部のオンライン契約書へのオンデマンドアクセスを提供しています。レポートは NDA に基づき、AWS カスタマーアカウントからアクセスできます。AWS Artifact は、コンプライアンス関連情報を一元的に管理し提供しているリソースであり、後述する AWS コンプライアンスプログラムについての情報も参照可能です。

1.6.1 SOC 1、2、3

AWS System and Organization Controls (SOC) レポートは、重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立した第三者による審査報告書です。このレポートの目的は、お客様と監査人が、業務の運用やコンプライアンスをサポートするために確立された AWS 統制について簡単に把握できるようにすることです。

SOC 1 レポートは、ユーザー組織の財務諸表の監査に関連が深いと考えられる、サービス組織の統制を中心に設計されています。AWS SOC 1 レポートは、会計監査時に要求される可能性が高い、特定の主要な統制と、広範な使用や監査シナリオに対応する、さまざまな IT 全般統制を対象に設計されています。AWS SOC1 の統制目標には、セキュリティ組織、従業員のユーザーアクセス、論理セキュリティ、安全なデータ処理、物理的セキュリティと環境保護、変更管理、データの整合性、可用性と冗長性、インシデント処理が含まれます。

SOC 2 レポートは、統制の評価を、米国公認会計士協会 (AICPA) の Trust サービスの原則 (Trust Services Principles) で定められている基準に基づき行う認証レポートです。この原則は、AWS などのサービス組織に適用されるセキュリティ、可用性、処理の完全性、機密性、およびプライバシーに関連する主要なプラクティスの統制について定義しています。AWS SOC 2 レポートは、統制に関する運用効果と設計が、米国公認会計士

協会 (AICPA) の Trust サービスの原則 (Trust Services Principles) で示されているセキュリティと可用性の原則のクライテリアを満たすことを評価したものとなっています。このレポートは、事前に定義された、リーディングプラクティスの業界標準に基づいて、AWS のセキュリティと可用性に一層の透明性を与え、AWS の顧客データ保護に対するコミットメントをさらに詳しく示すものです。SOC 2 レポートには、AWS 統制の概要、セキュリティ、可用性、機密性に関連する AWS サービスの説明、統制に対するテスト結果が含まれます。SOC 2 レポートは、GxP コンプライアンスに関係するため、最も詳細で関連の深い SOC レポートであると評価して頂けるでしょう。

AWS は、Service Organization Controls 3 (SOC 3) レポートも発行しています。SOC 3 レポートは、AWS SOC 2 レポートを一般公開用に要約したものです。レポートには、(SOC 2 レポートに含まれる AICPA の Security Trust Principles に基づく) 統制の運用についての外部監査人の評価、AWS のマネジメントによる統制の有効性についての表明、AWS のインフラストラクチャおよびサービスの概要が含まれます。

1.6.2 FedRAMP

Federal Risk and Authorization Management Program (FedRAMP) は米国政府全体のプログラムであり、クラウドの製品やサービスに対するセキュリティ評価、認証、継続的監視に関する標準的なアプローチを提供しています。FedRAMP では NIST SP 800 シリーズを使用しており、クラウドサービスプロバイダーは、連邦情報セキュリティマネジメント法 (FISMA) に準拠した認証を受けていることを証明するために、Third-Party Assessment Organization (3PAO) （第三者評価機関） が実施する独立したセキュリティ評価を受ける必要があります。

FedRAMP による評価、認証の対象範囲となる AWS サービスについては、こちらをご覧ください https://aws.amazon.com/compliance/services-in-scope/

1.6.3 ISO/IEC 9001

ISO/IEC 9001:2015 では、組織内で効果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。この規格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、プロセスの相互作用の決定など、品質管理システム (QMS) の要件
- 経営者の責任
- 人材や組織の労働環境を含む、リソース管理

- 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
- 内部監査や是正、予防措置などの活動による QMS の測定、分析、改善

AWS ISO/IEC 9001:2015 認証は、AWS クラウドで品質管理された IT システムを開発、移行、運用するお客様を直接サポートします。お客様は、ISO/IEC 9001:2015 プログラムや業界別の品質プログラム（ライフサイエンスでの GxP、医療機器での ISO/IEC 131485 など）の取得にあたって、AWS のコンプライアンスレポートを証拠として活用可能です。

1.6.4 ISO/IEC 27001

ISO/IEC 27001:2013 は、世界で広く採用されているセキュリティ基準で、絶えず変化する脅威シナリオに適した定期的なリスク評価に基づき、企業やお客様の情報を管理するための、体系的なアプローチの要件とベストプラクティスを定めるものです。認証を取得するためには、企業やお客様情報の機密性、完全性、可用性に影響を与える情報セキュリティリスクを管理するための、体系的かつ継続的なアプローチが企業にあることを示す必要があります。

この広く認めらた国際セキュリティ基準は、AWS に以下を義務付けています。

- 脅威と脆弱性の影響を考慮した、情報セキュリティリスクを体系的に評価
- お客様およびアーキテクチャのセキュリティリスクに対処するための、包括的な情報セキュリティ管理およびその他の形態のリスク管理の設計と実施。
- 情報セキュリティ管理が継続的に我々のニーズを満たしていることを確認するための、包括的な管理プロセスの保有。

AWS は、AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO/IEC 27001 の認定を受けています。

1.6.5 ISO/IEC 27017

ISO/IEC 27017:2015 は、クラウドコンピューティングの情報セキュリティに関するガイダンスを提供し、ISO/IEC 27002、および ISO/IEC 27001 のガイダンスを補完する、クラウド固有の情報セキュリティ統制の実装を推奨しています。また、この実務規範は、クラウドサービスプロバイダーに固有の、情報セキュリティ統制の追加実装ガイダンスを提供します。

ISO/IEC 27017:2015 に適合しているということは、世界的に認められたベストプラクティスへの準拠に対する AWS の継続的なコミットメントを示すのみならず、AWS においてクラウドサービス特有の非常に精密な統制が運用されていることを証明するものです。

1.6.6 ISO/IEC 27018

ISO/IEC 27018 は、クラウドにおける個人データの保護に焦点を当てた最初の国際的な実務規範です。ISO/IEC 27018 は、ISO/IEC 情報セキュリティ規格 27002 に基づいており、パブリッククラウドの個人識別情報 (PII) に適用される ISO/IEC 27002 統制の実装ガイダンスになっています。また、既存の ISO/IEC 27002 統制セットでは対応していない、パブリッククラウド PII 保護要件に対応する追加の統制セットと関連ガイダンスも提供しています。

AWS は、国際的に認められている実務規範である ISO/IEC 27018 の認定を受けています。これは、お客様のコンテンツのプライバシーと保護に対する AWS のコミットメントを示しています。

1.6.7 HITRUST

Health Information Trust Alliance 共通セキュリティフレームワーク (HITRUST CSF) は、GDPR、ISO、NIST、PCI、HIPAA などの国内および国際的に承認された標準規格と規制を活用し、ベースラインセキュリティとプライバシー管理の包括的なセットを形成するものです。

HITRUST が作成した HITRUST CSF アシュアランスプログラムには、組織とそのビジネスパートナーが、一貫した漸進なアプローチによってコンプライアンスを管理するための、一般的な要件、手法、ツールがまとめられています。さらに、このプログラムでは、ビジネスパートナーやベンダーが、複数の要件セットに対する対応状況の評価と報告を行うことができます。

AWS のサービスの一部は、HITRUST CSF アシュアランスプログラムに基づき、認定された HITRUST CSF 評価機関による評価を受け、HITRUST CSF 認定基準への適合が認められています。認定は 2 年間有効です。認定された AWS サービスはこちらから参照してください。https://aws.amazon.com/compliance/hitrust/ GxP コンプライアンスプログラムに加えて、お客様の HITRUST CSF 認定をサポートするため、AWS のサービスが取得している AWS HITRUST CSF 認定の活用をご検討ください。

1.6.8 CSA Security, Trust & Assurance Registry (STAR)

2011 年に、クラウドセキュリティアライアンス (CSA) は、クラウドプロバイダー間におけるセキュリティプラクティスの透明性を推進するためのイニシアチブである STAR を開始しました。CSA Security, Trust & Assurance Registry (STAR) は、さまざまなクラウドコンピューティングサービスが提供するセキュリティコントロールについてを文書化し、無料で公開することで、ユーザーが、現在使用中の、または検討中のクラウドプロバイダーのセキュリティについて評価する際に役立っています。

AWS は、CSA Security, Trust & Assurance Registry(STAR)の任意のセルフアセスメントに登録しており、CSA が公開しているベストプラクティスへの準拠性を文書化しています。完了した CSA コンセンサス評価イニシアチブのアンケート(CAIQ)は、AWS のウェブサイトで公開されています。

1.7 インフラストラクチャについての説明と統制

1.7.1 クラウドモデル (クラウドの性質)

クラウドコンピューティングは、インターネットを経由したクラウドサービスプラットフォームを介し、処理能力、データベースストレージ、アプリケーションなどの IT リソースをオンデマンドで、また従量課金制で提供するものです。クラウドコンピューティングが普及した現在では、異なるモデルやデプロイ戦略が出現し、さまざまなユーザーの具体的なニーズを満たしています。異なるタイプのクラウドサービスやデプロイ方法が、異なるレベルのコントロール、柔軟性、管理を提供します。

1.7.1.1 クラウドコンピューティングのモデル

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) は、クラウド IT の基本要素から成るもので、通常はネットワーキング機能、コンピュータ（仮想または専用ハードウェア）、データストレージ領域へのアクセスを提供するものです。IaaS では、IT リソースに最高度の柔軟性と管理統制を可能にすると同時に、今日の IT 部門や開発者の多くにとってなじみ深い既存の IT リソースにも最も類似しています。 （例: Amazon Elastic Compute Cloud (Amazon EC2) ）。

Platform as a Service (PaaS)

Platform as a Service (PaaS) を使用すると、組織内で基盤となるインフラストラクチャ（通常はハードウェアとオペレーティングシステム）を管理する必要がなくなるため、お客様はアプリケーションのデプロイと管理に集中できるようになります （例: AWS Elastic Beanstalk）。リソースの調達、容量計画、ソフトウェアメンテナンス、パッチの

適用、またはアプリケーションの実行に関連するその他のわずらわしい作業について心配する必要がなくなるため、業務をより効率的に進めることができます。

Software as a Service (SaaS)

Software as a Service (SaaS) は、サービスプロバイダーが実行および管理している完成した製品を提供します。ほとんどの場合、Software as a Service という言葉は、エンドユーザーアプリケーション（例: Amazon Connect）のことを指しています。SaaS オファリングを使用すると、サービスのメンテナンスや基盤となるインフラストラクチャの管理をどのように行うかを考える必要がなくなり、特定のソフトウェアを使用する方法についてのみを考えられるようになります。SaaS アプリケーションの一般的な例は、ウェブベースの E メールです。これは、メール製品の追加機能の管理や、メールプログラムを実行しているサーバーやオペレーティングシステムのメンテナンスなしで、メールを送受信できるものです。

1.7.1.2 クラウドコンピューティングのデプロイモデル

クラウド

クラウドベースのアプリケーションは完全にクラウド上にデプロイされており、アプリケーションの全てがクラウド上で実行されます。クラウド上のアプリケーションは、クラウドコンピューティングの利点享受のため (https://aws.amazon.com/what-is-cloud-computing/)、クラウド上で作成、もしくは既存のインフラストラクチャから移行されたものです。クラウドベースのアプリケーションは、低レベルのインフラストラクチャで作成することもでき、またコアインフラストラクチャの管理、アーキテクチャ設計、スケーリングの要件からの抽象化を提供する高レベルのサービスを使用することもできます。

ハイブリッド

ハイブリッドデプロイとは、クラウドベースのリソースと、クラウド上にはない既存のリソースとの間でインフラストラクチャとアプリケーションを接続する方法です。ハイブリッドデプロイの最も一般的な方法は、クラウドと既存のオンプレミスのインフラストラクチャとの間で、クラウドのリソースを社内システムに接続することで組織のインフラストラクチャをクラウドに拡張し、大きくするというものです。AWS がお客様のハイブリッドデプロイをサポートする方法の詳細については、AWS のハイブリッドのページをご参照ください。(https://aws.amazon.com/hybrid/)。

オンプレミス

仮想化およびリソース管理ツールを使用したオンプレミスでのリソースのデプロイは、専用のリソース提供が可能なため、方法として必要になることがあります (https://aws.amazon.com/hybrid/) 。多くの場合、デプロイモデルは従来の IT インフラストラクチャと同じで、アプリケーション管理や仮想化のテクノロジーを使用してリソースの活用を促進します。

1.7.2 セキュリティ

1.7.2.1 物理的セキュリティ

Amazon 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インフラストラクチャに活かされています。AWS データセンターは、AWS 施設として外部に公開されていない施設にあります。専門のセキュリティスタッフが、ビデオによる監視、不正侵入検知システム、その他電子的手段を用いて、建物の入口とその周辺両方において、物理的なアクセスを厳密に管理しています。また、権限を有するスタッフが、2 要素認証を最低 2 回用いなければ、データセンターのフロアにアクセスすることができません。すべての訪問者は身分証明書を提示してサインインし、権限を有するスタッフが常に付き添います。AWS は、データセンターや情報へのアクセスを、それを業務上本当に必要とする従業員やベンダーに対してのみ許可しています。従業員がこれらの権限を必要とする作業を完了すると、たとえ、引き続き 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も、そのアクセス権限はすみやかに取り消されます。AWS の従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。

インフラストラクチャセキュリティに関するさらなる情報は、AWS のデータセンターコントロールに記載されています。

シングルテナントまたはマルチテナント環境

この 10 年クラウドテクノロジーが急速な発展をとげる中で、物理リソースを最大化しつつ、お客様のコストを削減するために使用された基本的な手法が、マルチテナントサービスをクラウドのお客様に提供することでした。このアーキテクチャを支援するために、AWS は強力かつ柔軟な論理的セキュリティ統制を開発、実装し、お客様間を分離させる強力な境界を作成しました。AWS において、セキュリティは最優先事項であり、お客様が GxP などのセキュリティ体制要件を達成できるよう、AWS の機能とコントロールを着実に強化し続けてきた我々の豊富な経験を実感していただけます。オンプレミス環境での運用から、AWS などのクラウドサービス事業者のソリューショ

ンを使用してみると、オンプレミスのソリューションと比較して、クラウドにおけるセキュリティ構成を効果的に最適化できることに気が付くでしょう。

AWS 論理セキュリティ機能ならびにセキュリティ統制は、データを保護するために必要な物理的な分離を実現します。この分離に自動化と柔軟性が組み合わさることで、従来の物理的に分離された環境内のセキュリティ統制と一致する、またはそれ以上に優れたセキュリティ体制が実現します。

AWS 上の論理的分離については、Logical Separation on AWS をご覧ください。

1.7.3 クラウドインフラストラクチャのクオリフィケーションアクティビティ

1.7.3.1 地域

AWS は、全世界で数百万を超えるお客様にサービスを提供しています。お客様のビジネスの成長に応じて、AWS はお客様のグローバルな要件を満たせるインフラストラクチャを提供し続けてまいります。

AWS クラウドインフラストラクチャは、AWS リージョンとアベイラビリティーゾーンを中心に構築されています。AWS リージョンとは、世界中の物理ロケーションのことで、これは複数のアベイラビリティーゾーンで構成されています。アベイラビリティーゾーンは、1 つ以上の独立したデータセンターで構成され、各データセンターは、冗長的な電源、ネットワーク、接続機能を備えており、それぞれ異なる場所に存在します。このアベイラビリティーゾーンによって、単一のデータセンターでは実現できない高い可用性、耐障害性、拡張性を備えた本番用のアプリケーションとデータベースの運用を実現しています。AWS クラウドは、世界各地の 25 以上の地理的リージョンにある 80 以上のアベイラビリティーゾーンで運用されています。また、今後アベイラビリティーゾーンとリージョンをさらに増やす計画も発表されています。AWS クラウドアベイラビリティーゾーンと AWS リージョンの詳細については、AWS グローバルインフラストラクチャをご参照ください。

各 Amazon リージョンは、他の Amazon リージョンと完全に分離されるように設計されています。これにより、最大限の耐障害性と安定性が実現します。各アベイラビリティーゾーンは独立していますが、同じリージョン内のアベイラビリティーゾーンは低レイテンシーのリンクで接続されています。AWS は、各 AWS リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理リージョン内で、インスタンスを配置し、データをストアする柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。アベイラビリティーゾーンが、典型的な大都市地域内の、洪水のリスクの少ない平野部に物理的に分離されて配

置されているという意味です(具体的な洪水ゾーンの分類は、AWS リージョンごとに異なります)。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の軽減のために、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。すべてのアベイラビリティーゾーンは、複数の Tier-1 トランジットプロバイダーに、冗長接続されています。

1.7.3.2 データロケーション

1 つのデータセンターを 1 つのリージョンとして定義することが多い他のプロバイダーとは違い、全 AWS リージョンが採用するマルチアベイラビリティーゾーン (AZ) デザインは、地理的制限がある場合にお客様にメリットを提供します。高度な可用性の実現にフォーカスしている AWS のお客様は、複数の AZ で実行するようにアプリケーションの設計をすることで、より強力な耐障害性を実現できます。AWS のインフラストラクチャにおけるリージョンは、セキュリティ、コンプライアンス、データ保護からの要求を最も高いレベルで満たします。データレジデンシー要件がある場合は、希望のロケーションに近接した AWS リージョンを選択できます。また、データが物理的に存在するリージョンについては、お客様に完全な管理権と所有権があり、地域的なコンプライアンス要件やデータレジデンシー要件は容易に満たすことができます。

これに加え、移行や継続的なワークフローのためにオンプレミスデータを AWS に移動させる際、データオンショアリングのコンプライアンスに準拠するよう使用できる、以下各種ツールとサービスがあります。AWS ウェブサイト上のクラウドへのデータ移行もあわせてご参照ください。

- ハイブリッドクラウドストレージ (AWS Storage Gateway、AWS Direct Connect)
- オンラインデータ転送 (AWS DataSync、AWS Transfer Family、Amazon S3 Transfer Acceleration、AWS Snowcone、Amazon Kinesis Data Firehose、APN パートナー製品)
- オフラインデータ転送 (AWS Snowcone、AWS Snowball、AWS Snowmobile)

1.7.3.3 容量

キャパシティプランニングに関しては、AWS はサービスとラック使用レベルの両方で容量を調べます。また、AWS のキャパシティプランニングプロセスでは、承認のための調達プロセスが自動的にトリガーされるため、AWS では追加のラグタイムを考慮する必要がありません。また、AWS はキャパシティプランニングモデル（顧客の需要によって一部通知される）に基づいて新しいデータセンター構築をトリガーします。AWS では、お客様が選択したリージョンでスペースが保証されるよう、インスタンス

を予約可能です。AWS は、FOOB (future out of bound、将来的な想定外の使用率増加) に備えた計画に活用される情報としてリザーブドインスタンス数を使用します。

1.7.3.4 稼働時間

AWS は、プラットフォーム全体にわたってさまざまなサービスの SLA (サービスレベルアグリーメント) を保持しています。本書執筆時点では、リージョン内の Amazon EC2 および Amazon EBS の 99.99%以上の月間稼働率を SLA にてコミットしています。AWS SLA の全リストは、こちら https://aws.amazon.com/legal/service-level- agreements/より参照可能です。さらに、アマゾンウェブサービスは、サービスの可用性に関する最新情報を AWS サービスヘルスダッシュボードで公開しています (https://status.aws.amazon.com/) 。組織の要件に基づき、耐障害性を考慮したアプリケーションを設計することは、セキュリティ責任共有モデルの一環として、お客様の責任であることにご注意ください。

2 AWS 品質管理システム

GxP の要件に基づく義務を負っているライフサイエンスのお客様は、GxP 規制対象の製品を設計、開発、導入する際に、品質がその製造および管理の一環として実現されていることを確認しなければなりません。この品質保証には、AWS などのクラウドサービスサプライヤーがお客様の品質システムに準拠できているかを適切に評価することも含まれます。

AWS 品質システムの詳細については、NDA（秘密保持契約）の下、AWS Artifact にアクセスし、関連文書をご参照ください。AWS では、GxP のお客様に向けて、AWS 品質システムの概念とコンポーネントに関する情報を一部以下に提供します。

2.1 品質インフラストラクチャとサポートプロセス

2.1.1 品質管理システムの認定

AWS では、品質システムに関する体系的な調査を独自に実施し、アクティビティやその結果が ISO/IEC 9001:2015 の要件に準拠しているかどうかを確認しました。そして、認証機関によって、登録範囲に記載されているアクティビティの品質管理システム (QMS) が、ISO/IEC 9001:2015 の要件に準拠していることが認められました。

AWS の品質管理システムは、2014 年以来 ISO/IEC 9001 に認証されています。レポートは、毎年 6 ヶ月間 (4 月～ 9 月/10 月～ 3 月) を対象にしており、新しいレポートは、5 月中旬と 11 月中旬にリリースされます。AWS における ISO/IEC 9001 の登録認証、

認証機関の情報、発行日および更新日については、ISO/IEC 9001 AWS コンプライアンスプログラムのウェブサイトの情報をご参照ください。
https://aws.amazon.com/compliance/iso-9001-faqs/

認証対象は、指定された範囲の AWS サービスおよび運用リージョンにおける QMS です。AWS クラウドで、全部または一部の IT システムを運用しながら ISO/IEC 9001:2015 の認証取得を進めても、協会によって自動的に認証されることはありません。しかし、AWS のような ISO/IEC 9001:2015 認定プロバイダーを使用することで、お客様の認証プロセスがより容易なものとなります。

AWS は、AWS Artifact において、AWS コンソール内の顧客アカウントを介してアクセス可能な、品質管理システムに関する詳細情報を提供しています。(https://aws.amazon.com/artifact/)

2.1.2 ソフトウェア開発アプローチ

AWS サービスの設計と開発における AWS の戦略は、お客様のユースケース、サービスのパフォーマンス、マーケティングと流通の要件、生産とテスト、法的および規制要件の観点からサービスを明確に定義することです。すべての新しいサービスの設計や現在のサービスの大幅な変更は、多領域にまたがるプロジェクト管理システムによって管理されています。要件およびサービス仕様は、法的要件や規制要件、お客様との契約上のコミットメント、サービスの機密性、完全性、可用性を品質管理システムで決定した品質目標に沿って満たすための要件を考慮したうえで、サービス開発中に確立されます。サービスレビューは、開発プロセスの一環として行われ、レビューには、セキュリティ、法的影響、規制上の影響、お客様との契約上のコミットメントに関する評価が含まれます。

また、サービス開始前に、次の要件をすべて満たす必要があります。

- セキュリティリスク評価
- 脅威モデリング
- セキュリティ設計のレビュー
- セキュアコードのレビュー
- セキュリティのテスト
- 脆弱性/侵入テスト

AWS は、サービスにオープンソースソフトウェアまたはカスタムコードを実装しています。すべてのオープンソースソフトウェア（サードパーティーからのバイナリコードまたはマシンで実行可能なコードを含む）は、実装前にオープンソースグループに

よってレビュー、承認され、公開されたアクセス可能なソースコードを有しています。AWS サービスチームが、オープンソースレビューで承認されていないサードパーティーからのコードを実装することは禁止されています。AWS によって開発されたすべてのコードは、該当するサービスチーム、および AWS セキュリティによって確認可能な状態になっています。オープンソースコードは、その性質上、Amazon 内での使用許可を付与する前に、オープンソースグループでレビューいただけます。

2.1.3 品質手順

AWS サービスの開発と運用をサポートするための AWS 品質管理システムの範囲に含まれるソフトウェア、ハードウェア、人材、不動産資産に加え、ソースコード、システム文書、運用方針と手順などの文書化された情報などがこれに含まれます（しかし、これらに限定されません）。

AWS は、組織内およびサポートする AWS 環境内の運用と情報セキュリティに対するガイダンスを示す、文書化された正式なポリシーと手順を実装しています。このポリシーでは、目的、範囲、役割、責任、管理に関するコミットメントについて取り上げています。すべてのポリシーは、一元化された場所に管理されており、従業員がアクセスできるようになっています。

2.1.4 プロジェクト管理のプロセス

新しいサービスの設計、または現在のサービスの大幅な変更は、安全なソフトウェア開発プラクティスに従い、他領域を加味したプロジェクト管理システムを通じてコントロールされます。

2.1.5 品質組織の役割

AWS セキュリティアシュランスは、従業員の AWS セキュリティポリシーに対する理解を深める責任を負っています。AWS は、組織構造、レポートライン、責任の定義に沿った情報セキュリティ機能を確立しています。また、リーダーシップの協力により、セキュリティイニシアティブに対する明確な方向性と目に見えるサポートが提供されます。

AWS は、AWS の統制環境の実装と運用効果を検証するために、内部および外部の継続的かつ独立した評価を含む、公式の監査プログラムを作成しました。

AWS では、社内および社外によるアセスメントの監査スケジュールを文書化しています。社内外関係者のニーズと期待は、AWS 統制環境の開発、実装、監査のすべての段

階を通じて考慮されます。関係者には、以下が含まれます（しかし、これらに限定されません）。

- AWS のお客様 （現在のお客様および潜在的なお客様）
- AWS の外部関係者 （外部監査人や認証機関などの規制機関）
- AWS のサービスチームやインフラストラクチャチーム、セキュリティチーム、総務チームや企業チームなどの内部関係者

2.1.6 品質プロジェクトの計画と報告

AWS の計画プロセスでは、サービス要件、プロジェクトおよび契約の要件を定義することで、確実に顧客のニーズと期待を満たす、または上回るようにします。計画は、ビジネスやサービス計画、プロジェクトチーム、品質改善計画、サービスと関連したメトリクスのレビューとその文書化、自己評価とサプライヤー監査、従業員トレーニングを組み合わせることで形になります。AWS 品質システムでは、計画が他のすべての要件と整合性がとれていることを確認するため、文書化されます。

AWS は、サービスの使用状況を継続的に監視することでインフラストラクチャのニーズを予測し、可用性のコミットメントと要件をサポートします。AWS では、インフラストラクチャの使用状況と需要を評価するために最低でも毎月、通常はより頻繁にキャパシティプランニングモデルを作成しています。さらに、AWS キャパシティプランニングモデルは、現在のリソースと将来の要件予測に基づいて、追加のリソースを取得、実装するための需要計画の作成をサポートします。

2.1.7 電子記録と電子署名

米国では、GxP 規制はアメリカ食品医薬品局 (FDA) によって施行され、連邦規則集の Title 21 (21 CFR) に記載されています。21 CFR の Part 11 には、GxP 規制対象の活動をサポートできるよう、電子記録および電子署名を作成、変更、保守、アーカイブ、取得、または配布するコンピュータシステムの要件が含まれています (EU では、EudraLex - Volume 4 - Good Manufacturing Practice (GMP) ガイドライン– Annex 11 Computerised Systems) 。
Part 11 は、FDA 規制対象のライフサイエンス組織が新しい IT 技術を採用できるようにする、また同時に電子 GxP データの信頼性を確保するためのフレームワークを実現するために作成されました。

AWS などの商用クラウドプロバイダーは、GxP 認定の対象ではありません。AWS は、ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018、ISO/IEC 9001、NIST 800-53 などの IT 品質およびセキュリティ基準に準拠して、商用オフザシェルフ (COTS) IT サービスを提

供しています。GxP 規制対象となるライフサイエンスのお客様は、自社の GxP システムを開発、運用するために、また GxP コンプライアンスおよび 21 CFR 11 への準拠を検証するために、AWS サービスを購入、使用する必要があります。

本書を、随所に記載した他の AWS リソースと組み合わせて使用し、電子記録および電子署名の要件への準拠にお役立てください。21 CFR 11 に関連した AWS サービスの使用における責任共有モデルの詳細については、付録をご参照ください。

2.1.8 企業のセルフアセスメント

AWS セキュリティアシュアランスは、コンプライアンス、適合性、品質管理システムの有効性を確保するために、AWS 監査プログラムを通じた検証アクティビティを実行し、品質管理システムの実装とメンテナンスをモニタリングします。AWS 監査プログラムには、セルフアセスメント、第三者認定監査、サプライヤー監査が含まれます。これらの監査の目的は、AWS 品質管理システムの運用効果を評価することです。セルフアセスメントは定期的に行われます。認定のための第三者による監査は、基準に基づくクライテリアに対する AWS の継続的なパフォーマンスをレビューし、全般的な改善の機会を特定するために行われます。サプライヤー監査は、AWS の供給要件に適合したサービスやマテリアルを提供するサプライヤーの能力を評価するために実行されます。

AWS では、さまざまな目標を達成する上で、AWS 統制環境の実装と運用効果を確保するために、すべてのアセスメントのスケジュールを文書化して管理しています。

2.1.9 契約のレビュー

AWS は、標準化された顧客契約に基づいてサービスを販売します。サービスが、正確に表現されている、適切に販売促進されている、また適正な価格で提供されていることをお約束できるよう、顧客契約はレビューされます。AWS サービス条件についてご質問がある場合は、アカウントチームにお問い合わせください。

2.1.10 是正措置および予防措置

AWS では、不適合の再発を防ぐため、品質管理システムの範囲内で、その原因を取り除くアクションを実行します。是正措置および予防措置を講じる場合は、以下の手順に従います。

1. 不適合を特定する
2. 不適合の原因を決定する

3. 不適合を再発させないための行動の必要性を評価する
4. 必要な是正措置を決定し、実施する
5. 実施されたアクションの結果を記録する
6. 実施された是正措置についてレビューする
7. 必要な予防措置を決定し、実施する
8. 実施されたアクションの結果を記録する
9. 予防措置をレビューする

是正措置の記録は、定期的に実施される AWS のマネジメント会議でレビューされています。

2.1.11 お客様からの苦情

AWS は、手順と具体的な指標によってお客様をサポートします。お客様からの報告や苦情を詳しく調査し、必要に応じて解決するための措置を取ります。https://aws.amazon.com/contact-us/にアクセスし、AWS にお問い合わせいただくか、お客様のアカウントチームに直接相談してサポートを受けることができます。

2.1.12 サードパーティーの管理

AWS には、サードパーティーとの関係を促進し、またそのパフォーマンスをモニタリングするために、サプライヤー管理チームがあります。SLA および SLO (サービスレベル目標)を実装し、パフォーマンスをモニタリングしています。

AWS は、提供してもらう作業やサービス (ネットワークサービス、サービス提供、情報交換など) に応じて、サードパーティー (請負業者やベンダーなど) との書面による契約を作成、維持し、各サードパーティーとのビジネス関係に従って適切なリレーションシップ管理メカニズムを実装しています。AWS は、契約上の義務に対するパフォーマンスを評価するリスクベースアプローチを使用して、定期的なレビューを行い、サードパーティーのパフォーマンスをモニタリングします。

2.1.13 トレーニングの記録

AWS では、すべてのレベルの従業員が経験豊富であり、職務のスキル領域や指定されたその他のトレーニングを受けます。トレーニングを継続的に提供するため、また品質に影響を与える各オペレーション (プロセス) をふまえた適切なトレーニングであるかを確認するため、トレーニングのニーズを識別しています。特別な条件下で作業する必

要がある、または専門的なスキルを必要とする従業員は、その能力を獲得するためのトレーニングを受講します。また、個人が適切なトレーニングを受けていることを証明するため、各トレーニングや認定の記録は残されます。

AWS は、セキュリティと可用性に影響を及ぼすシステムの設計、開発、実装、運用、保守、監視を担当する従業員を対象に、その役割に基づき、セキュリティ意識に関するトレーニングの開発、文書化、普及活動を行い、さらに、従業員が責任を果たすために必要なリソースを提供しています。トレーニングには、（従業員の役割に関連する場合）以下が含まれますが、これらに限定されません。

- 従業員の行動規範
- 候補者の経歴の審査手順
- デスクポリシーと手順の明確化
- ソーシャルエンジニアリング、フィッシング、マルウェア
- データの処理と保護
- コンプライアンス上のコミットメント
- AWS セキュリティツールの使用
- 渡航中のセキュリティ予防策
- セキュリティと可用性に関する障害、インシデント、懸念、その他の苦情を適切な担当者に報告する方法
- 組織情報システムにおける疑わしいコミュニケーションや異常行動を認識する方法
- トレーニング目標を強化する実践演習
- HIPAA の役割

2.1.14 人事記録

AWS は、固有目標と従業員のスキル・能力との整合性の評価など、人材と人員配置の正式な評価を定期的に行います。人事記録は、社内の Amazon システムを通じて管理されています。

2.1.15 インフラストラクチャの管理

インフラストラクチャチームは、ハードウェアスケーラビリティ、可用性、監査、セキュリティ管理に対応するために、設定管理フレームワークを維持、運用しています。変

更内容を管理する自動化されたプロセスを使用してホストを一元管理することで、Amazon は高可用性、再現性、スケーラビリティ、セキュリティ、およびディザスタリカバリという目標を達成することができます。システムエンジニアやネットワークエンジニアは、これらの自動化ツールのステータスを継続的にモニタリングし、設定やソフトウェアの取得、更新に失敗したホストに対応するため、レポートをレビューします。

新しいハードウェアがプロビジョニングされると、社内で開発された設定管理ソフトウェアがインストールされます。これらのツールは、設定済みであること、またホストに割り当てられた役割によって決定された基準に準拠してソフトウェアがインストールされていることを確認するため、すべて UNIX ホスト上で実行されます。この設定管理ソフトウェアは、ホストに既にインストールされているパッケージの定期的な更新においても有効です。アクセス許可を得て有効化され、承認を受けた担当者だけが、一元管理された設定管理サーバーにログインできます。AWS は、必要に応じて AWS サービスについての変更をお客様に通知します。AWS は、継続的に進化し、既存のサービスの改善を行い、また新しいサービスや機能を頻繁に追加します。また、AWS のサービスは API によって管理されているため、AWS がサービスへの呼び出しに使用する API を変更または中止した場合、12 か月間（本書の発行時点において）、既存の API を提供し、お客様が調整できる期間を提供します。さらに、AWS は、Personal Health Dashboard で、お客様のアカウント情報に基づきサービスの健全性とステータスについて情報をお伝えするとともに、公開されている Service Health Dashboard では、AWS サービスのリアルタイム運用ステータスを地域レベルですべてのお客様に提供します。

2.2 ソフトウェア開発

2.2.1 ソフトウェア開発手順

情報システムの開発と構成をガイドするような組織のメカニズム類（ソフトウェア開発のライフサイクル管理や変更管理を含む）に関連した AWS の情報とアクティビティには、GAMP などで使用されるライフサイクルアプローチのプロジェクトステージと運用ステージが反映されます。組織メカニズムの要素には、ポリシーと基準、コード管理、デプロイメント、変更管理ツール、継続的な監視、セキュリティレビュー、緊急時の変更、アウトソーシングや不正な開発の管理、およびお客様への変更の連絡などが含まれます。

AWS におけるソフトウェア開発ライフサイクルのアクティビティには、AWS でのコード開発と変更管理のプロセスが含まれます。これらのプロセスは、外部向けおよび内部向けのコードを開発する AWS チーム全体で一元化されており、内部と外部のサービ

スチーム両方に対してプロセスが適用されます。AWS でデプロイされたコードは、最終的な利用先にかかわらず、一貫したプロセスで開発および管理されます。このプロセスでは、次のような複数のシステムが活用されます。

- 開発の一環としてコードパッケージの作成に使用される、コード管理システム
- 内部のソースコードリポジトリ
- AWS コードパイプラインがステージングされる、ホスティングシステム
- コードのテスト、承認、デプロイメント、および継続的な監視を自動化するために利用されるツール
- 変更ワークフローを、個別の扱いやすいステップに分解して変更の詳細を追跡する、変更管理ツール
- 本稼働システム内のコードまたは構成への未承認の変更を検出する監視サービス。すべての相違個所は、担当のサービスオーナーまたはチームにエスカレーションされます

2.2.2 コード管理

AWS におけるコード管理の、開発及びデプロイメント内のステップを以下にまとめます。このプロセスは、コードがまったくの新規であるか、既存のコードベースに対する変更であるかに関わらず実行されます。

1. 開発者は、AWS 管理下の開発者デスクトップ環境で実行されている、承認済みの統合開発環境内でコードを書きます。開発者は通常、次のステップに進む前に、初期ビルドテストと結合テストを行います。
2. 開発者は、レビュー目的で内部ソースコードリポジトリにコードをチェックインします。
3. コードについて、コードレビュー検証が行われます。この検証では、別の、少なくとも 1 名の担当者がコードをレビューし、承認を行います。承認済みリストは、コードレビューツール内に保持される変更不可能なログに格納されます。
4. その後内部ビルドシステムにより、コードはソースコードから適切なデプロイ可能なコードパッケージ（言語によって異なる）にビルドされます。

5. ビルドが成功すると（全結合テストの合格を含む）、コードはテスト環境にプッシュされます。
6. コードは本稼働前の環境で、自動の結合テストおよび検証テストを実施され、成功すると本稼働環境にプッシュされます。

AWS では、自社サービス内のオープンソースコードの実装を許可していますが、このようなオープンソースコードの使用は、上記の承認、パッケージング、レビュー、デプロイメント、および監視のプロセスの対象となります。バイナリまたはマシン実行コードおよびオープンソースライセンスを含むオープンソースソフトウェアは、実装前に追加のレビューと承認の対象となります。AWS では、承認済みオープンソースのリストに加え、禁止オープンソースのリストも保持しています。

2.2.3 デプロイメントおよびテスト

パイプラインとは、承認されたコードパッケージが、最初のチェックインから一連の自動（場合によっては手動）のステップを経て本稼働環境で実行されるまでのパスを意味します。自動化、テスト、承認は、パイプライン内で行われます。

AWS では、デプロイメントツールを使用してコードパイプラインを作成、表示、適用します。このツールは、ビルド済みコードの最新承認済みリビジョンを、本稼働環境に昇格させるために使用されます。

管理された段階ごとにデプロイを実施し、コードを本稼働環境にプッシュする前に継続的な承認を義務付けることが、安全なコードのデプロイメントを保証する重要な要素となります。デプロイメントプロセスの一環として、コードを本稼働環境にプッシュする前に、まずテスト環境（チームが定義した「ベータ」や「ガンマ」などの環境）にリリースするようにパイプラインが構成されています。自動品質テスト（結合テスト、構造テスト、ビヘイビアテストなど）は、コードが期待通りに機能することを確認するために、これらのテスト環境で実行されます。コードが基準から逸脱していることが判明した場合、リリースが停止され、チームにレビューが必要であることが通知されます。

これらの開発、テスト環境は本稼働環境をエミュレートした環境であり、本稼働環境への変更の影響を適切に評価し、準備するために使用されます。本稼働環境への不正なアクセスや改ざんのリスクを軽減するために、開発環境、テスト環境、本稼働環境はすべて論理的に分離されています。

このツールにより、コードを複数のリージョンにまたがってデプロイする場合は、さらに段階的な展開が義務付けられます。もしパッケージに複数の AWS リージョンのデプロイが含まれている場合、パイプラインでは単一リージョンベースのデプロイを義

務付けています。いずれかのリージョンでパッケージが結合テストに失敗した場合、パイプラインは停止され、チームにはレビューが必要であることが通知されます。

2.2.4 構成管理および変更管理

構成管理は、AWS の変更管理プロセスを使用して、情報システムの設計、開発、実装、運用中に実行されます。

既存の AWS インフラストラクチャに対する、通常業務上の変更、緊急の変更、および構成の変更は、同様のシステムの業界基準に従って許可、記録、テスト、承認、文書化されます。AWS インフラストラクチャの更新は、お客様とサービスの使用への影響を最小限に抑える形で行われます。

2.2.5 ソフトウェア

サービスに対する変更でお客様に影響を与えるものについて、AWS は変更管理に体系的なアプローチを適用し、徹底的にレビュー、テスト、承認し、十分に伝達できるようにします。AWS の変更管理プロセスは、意図しないサービスの中断を回避し、お客様へのサービスの整合性を維持できるように設計されています。本稼働環境にデプロイされる変更は、以下の段階を踏みます。

- 準備：スケジュール設定、リソースの決定、通知リストの作成、依存関係のスコープ調査、同時変更の最小化、緊急または長期間の変更のための特別なプロセスなどを含みます。
- 提出：変更管理ツールの使用による変更の文書化と要求、潜在的な影響の特定、コードレビューの実施、詳細なタイムラインとアクティビティ計画の作成、詳細なロールバック手順の作成などを含みます。
- レビューおよび承認：変更の技術的な側面について、ピアレビューが必要です。そして、ビジネスとセキュリティへの影響を適切に把握し、理解するために、変更の承認が必要です。構成管理のプロセスには、情報システムに対して提案された変更の、レビューと承認を担当する組織内の主要な担当者が含まれます。
- テスト: 適用される変更が、期待どおりに動作し、パフォーマンスに悪影響を与えることがないようにテストを行います。
- 実行：変更前および変更後の通知、タイムラインの管理、サービスの健全性とメトリクスの監視、変更の完了を含みます。

AWS サービスチームはシステムとデバイスについて、信頼できるベースライン構成を維持しています。変更が導入される前に（緊急の変更でない限り）変更管理チケットが提出され、そのチケットには影響分析、セキュリティに関する考慮事項、説明、期間、承認の情報が含まれます。変更は、影響の少ない領域から実施され、段階的に本稼働環境に移行します。影響を評価できるよう、デプロイメントは単一のシステムでテストされ、注意深く監視されます。サービス所有者が、サービス上流部への依存関係の健全性を測定できるように、設定可能なメトリクスが多数用意されています。これらのメトリクスを、しきい値とアラームを設定した上で注意深く監視します。ロールバックの手順は、変更管理(CM) チケットに記載されています。AWS サービスチームが、ロールバックをサポートするために必要な古いバージョンの AWS ベースラインパッケージと設定を保持しており、以前のバージョンはリポジトリシステムに保存されます。結合テストと検証プロセスは、ロールバックを実施する前に実行されます。可能な場合、変更は通常の変更期間中にスケジュールされます。

AWS ではパイプラインの一部である予防的な統制（コードレビューの検証、テスト環境など）に加えて、標準手順以外で行われた疑いのある変更が検出されたときに担当者に警告し通知するように設定された検知統制も使用します。AWS は、デプロイメントをチェックして、コードが本稼働環境にコミットされる前に、適切なレビューと承認が適用されていることを確認します。本稼働環境のレビューと承認に対する例外処置は、自動チケット発行とサービスチームへの通知につながります。

本稼働環境にコードをデプロイした後、AWS は多様なモニタリングプロセスを通じてパフォーマンスの継続的なモニタリングを実行します。AWS ホストの設定は、脆弱性モニタリングの一環として監視され、AWS セキュリティ基準への準拠が検証されます。変更内容の監査証跡は保持されます。

標準的な変更管理手順からの逸脱を必要とするような、本稼働システムへの緊急の変更は、インシデントに関連付けられ、適切にログに記録され、承認されます。AWS は定期的に、主要なサービスに対する変更の自己監査を行い、変更管理プロセスの品質を監視し、高い水準を維持し、継続的な改善を促進します。すべての例外は根本原因を特定するために分析され、変更をコンプライアンス準拠状態に持っていくか、必要でれば変更をロールバックするかの、適切なアクションが実行されます。その後、プロセスや人材の問題の対処と修復に向けたアクションが実行されます。

2.2.6 レビュー

外部でローンチされる製品、サービス、重要な追加機能に関する Amazon セキュリティ基準に対して、AWS は事前の内部セキュリティレビューを実施し、お客様の環境にデプロイする前にセキュリティリスクが特定され、軽減されていることを確実にします。

AWS のセキュリティレビューには、サービスデザイン、脅威モデル、および AWS のリスクプロファイルへの影響の評価が含まれます。一般的なセキュリティレビューは、サービスチームが専属チームに対してレビューリクエストを依頼し、レビュー対象物に関する詳細情報を提供することから始まります。この情報に基づいて AWS は設計を検討し、セキュリティ上の考慮事項を特定します。これらの考慮事項には、暗号化の適切な使用、データ処理の分析、規制に関する考慮事項、安全なコーディングプラクティスの遵守が含まれますが、これらに限定されません。ハードウェア、ファームウェア、仮想化ソフトウェアに対しても、ハードウェア設計、実際の実装、最終的なハードウェアサンプルなどを対象としたセキュリティレビューが実施されます。

コードパッケージの変更は、次のセキュリティアクティビティの対象となります。

- 完全なセキュリティ評価
- 脅威のモデル化
- セキュリティ設計のレビュー
- 安全なコードレビュー（手動および自動化された方法）
- セキュリティのテスト
- 脆弱性／侵入テスト

上記アクティビティが正常に完了することが、サービス開始の前提条件です。開発チームは、開発する機能のセキュリティが、セキュリティエンジニアリングの原則を満たすようにする責任があります。インフラストラクチャチームは、セキュリティ原則をサーバーやネットワークデバイスの構成に組み込み、全体を通して最小権限の原則を適用します。AWS によって特定された知見は、リスクの観点から分類され、自動化されたワークフローツールで記録管理されます。

2.2.7 製品のリリース

すべての AWS サービスについて、該当サービスのウェブサイト上で製品情報が確認できます。この情報には、サービスの主な特徴と製品の詳細、料金情報、開発者用リソース（リリースノートおよび開発者ツールを含む）、FAQ、ブログ、プレゼンテーションに加え、開発者向けガイド、API リファレンス、該当する場合はユースケース、などの追加ドキュメントが含まれます (https://aws.amazon.com/products/)。

2.2.8 お客様のトレーニング

AWS は、お客様ベースとコミュニティをサポートするために、さまざまな外部コミュニケーション方法を導入しています。お客様のエクスペリエンスに影響するような運

用上の問題について、カスタマーサポートチームに通知される仕組みが実装されています。サービスヘルスダッシュボードは、カスタマーサポートチームによって利用および管理され、広範囲に影響する可能性のある問題についてお客様に警告します。AWS クラウドセキュリティセンター (https://aws.amazon.com/security/) とヘルスケアとライフサイエンスセンター (https://aws.amazon.com/health/) では、AWS のセキュリティとコンプライアンスの詳細、およびライフサイエンス関連の有益な情報が提供されます。またお客様は、AWS サポートサービスに登録することで、カスタマーサポートチームとの直接な連絡や、お客様に影響のある問題に対する事前アラートの受信などが可能となります。

AWS では、AWS アカウントチームを通じて提供される一連のサービスとサポートに加え、クラウド関連のトピックに関する一連のトレーニングおよび認定プログラム (https://www.aws.training/) を提供しています。

3 GxP システムでの AWS 製品

このセクションでは、規制機関や業界団体からの限られた技術的なガイダンスのもとで、お客様が法令順守のニーズを満たすためにクラウドサービスを利用する際に採用したベストプラクティスをいくつか説明します。

FDA ガイダンスドキュメントの最終版である「医薬品 CGMP におけるデータインテグリティとコンプライアンス」において、「コンピュータまたは関連システム」の定義が改定され、クラウドインフラストラクチャが明確に範囲に含まれています。

> 「米国規格協会 (ANSI)」は、システムを一連の特定機能を達成するために構成された人、装置、および方法として定義しています。コンピュータまたは関連システムには、コンピュータハードウェア、ソフトウェア、周辺機器、ネットワーク、**クラウドインフラストラクチャ**、人材および関連文書（ユーザーマニュアルや標準業務手順書など）が含まれます。」

さらに、ISPE のような業界団体は、ライフサイエンスにおけるクラウドの使用に関して出版物を次々と公開しています（Getting Ready For Pharma 4.0: クラウドおよびビッグデータアプリケーションにおけるデータインテグリティ）。

本ホワイトペーパー全体にわたって説明したように、GxP 規制には固有の認証がないため、各お客様は独自のリスクプロファイルを定義しています。したがって、本ホワイトペーパーはライフサイエンスのお客様の AWS の経験に基づいていますが、お客様自身で最終的な説明責任を負い、規制上の義務を決定する必要があります。

まず、クラウドにデプロイされた場合でも、GxP 用アプリケーションのバリデーションを実施し、基盤となるインフラストラクチャをクオリフィケーションする必要があります。オンプレミスインフラストラクチャのクオリフィケーションを管理する基本原則は、仮想化クラウドインフラストラクチャにも適用されます。したがって、現在の業界ガイダンスは引き続き活用する必要があります。

従来、規制対象の企業は、インフラストラクチャのクオリフィケーションとアプリケーションのバリデーションのあらゆる側面に対する説明責任を負い、責任を果たしていました。パブリッククラウドプロバイダーの参入により、その責任の一部はクラウドサプライヤーに移行しました。規制対象の企業には依然として説明責任がありますが、現在クラウドサプライヤーは物理インフラストラクチャ、仮想化、およびサービス層のクオリフィケーションを行い、提供するサービスを完全に管理する責任を担っています。つまり、現在の大きな違いは、本ホワイトペーパーで前述したセキュリティ責任共有モデルに似た、コンプライアンス責任共有モデルがあることです。
本ホワイトペーパーの前のセクションでは、責任共有モデルの部分を AWS がどのように対応するかについて説明しました。このセクションでは、GxP 環境における責任共有モデルをどう担当するかについて推奨される方法を示します。

3.1 AWS の関与

クラウドテクノロジーの採用において、GxP コンプライアンスの達成は長い道のりです。AWS はこの道のりで、多くのお客様をサポートしてきましたが、経験には圧縮アルゴリズムは存在しません。

例えば、Core Informatics 社は、次のように述べます：

> 「AWS を使用することで、GxP コンプライアンスを維持しながら、組織の発見を迅速化することができます。AWS は私たちのビジネスを変革し、さらに重要なことは、私たちのお客様のビジネスの変革を支援できることです。」
>
> **- Richard Duffy, Vice President of Engineering, Core Informatics**

この事例の全容は、Core Informatics 社のケーススタディをご参照ください。その他のお客様事例については、AWS カスタマーサクセスをご参照ください。

業界ガイダンスは、企業がサプライヤーの関与を試み、最大限に活用し、私たちの知識、経験、さらにはドキュメントもできる限り活用することを推奨しています。これは以下のセクションおよび本ホワイトペーパー全体で提供しています。クラウドへの移行開始について相談する場合は、こちらにお問い合わせください。

3.2 ライフサイエンス組織のクオリフィケーション戦略

規制対象企業のお客様にとって懸念事項の 1 つは、現在のように多くの責任がサプライヤーと共有されている場合に、いかにしてシステムの統制をクオリフィケーションし、実証するかにあります。クオリフィケーション戦略の目的は、この質問に答えることです。一部のお客様は、クオリフィケーション戦略を包括的なバリデーション計画として考えています。この戦略では、お客様の規制ニーズに対応するために、多様な手法を用いります。

クオリフィケーション戦略をより効果的に適用するには、アーキテクチャの全体を確認する必要があります。エンタープライズ規模のお客様は通常、次のようにアーキテクチャを定義します。

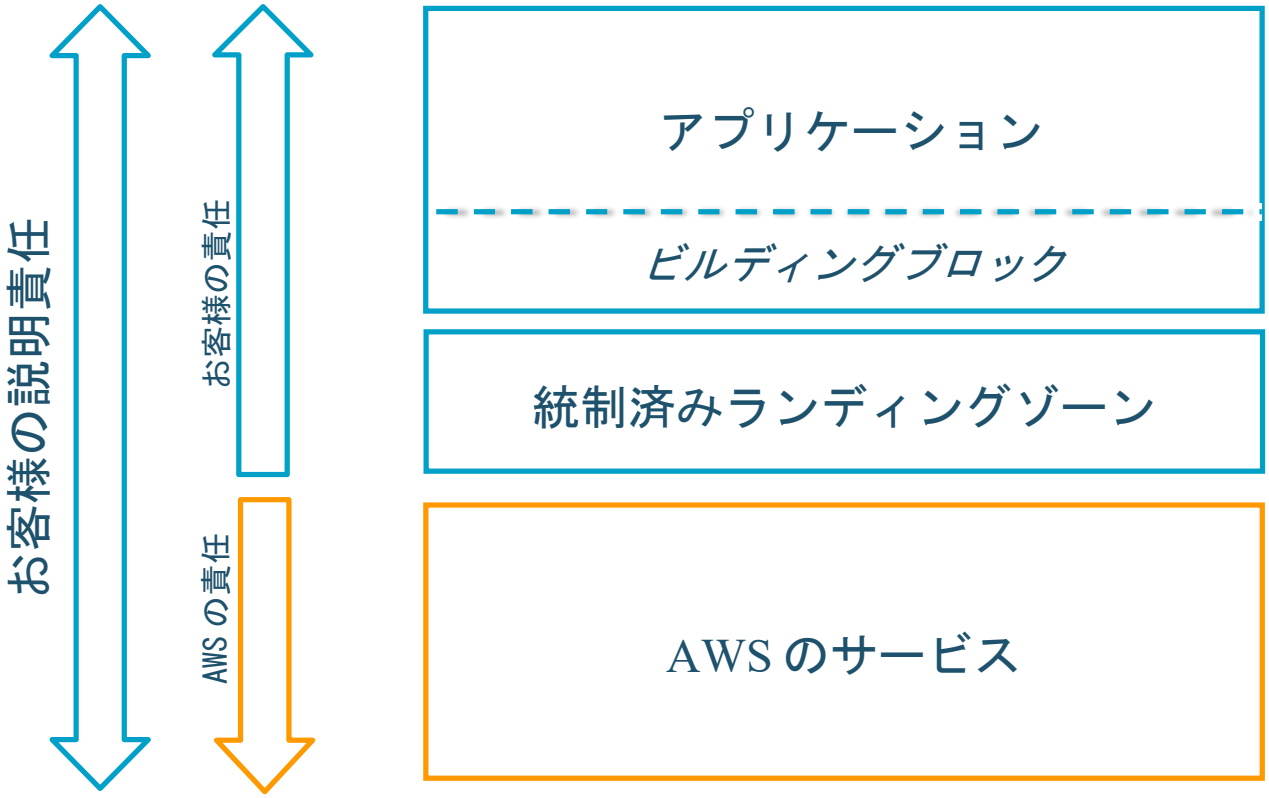

図 2: 階層型アーキテクチャ

この図は、大部分が AWS に委任されている階層型アーキテクチャを示しています。このアプローチから、4 つの主要な領域に対処するクオリフィケーション戦略を定義することができます。

1. サービスのサプライヤーとして AWS と連携する方法。
2. 統制済みランディングゾーンのクオリフィケーション。
3. ビルディングブロックのクオリフィケーション。
4. GxP アプリケーションの開発サポート。

お客様が AWS Managed Services などの、ランディングゾーンの構築、運用、メンテナンスも行うサービスプロバイダーを利用している場合も状況は若干変わります。一方で、オンプレミス上に残す必要があるワークロードについては、AWS Outposts を使用してコンピューティング、ストレージ、ネットワーキングを含む AWS サービスをお客様のサイトに拡張します。データをローカル保存できるように設定が可能で、お客様は Outposts 機器周辺のアクセスの管理に対して責任があります。オンプレミスで処理および格納されたデータは、お客様のローカルネットワーク経由でアクセスできます。この場合、お客様の責任は *AWS のサービス*の範囲にも及んでいます（***図 3***）。

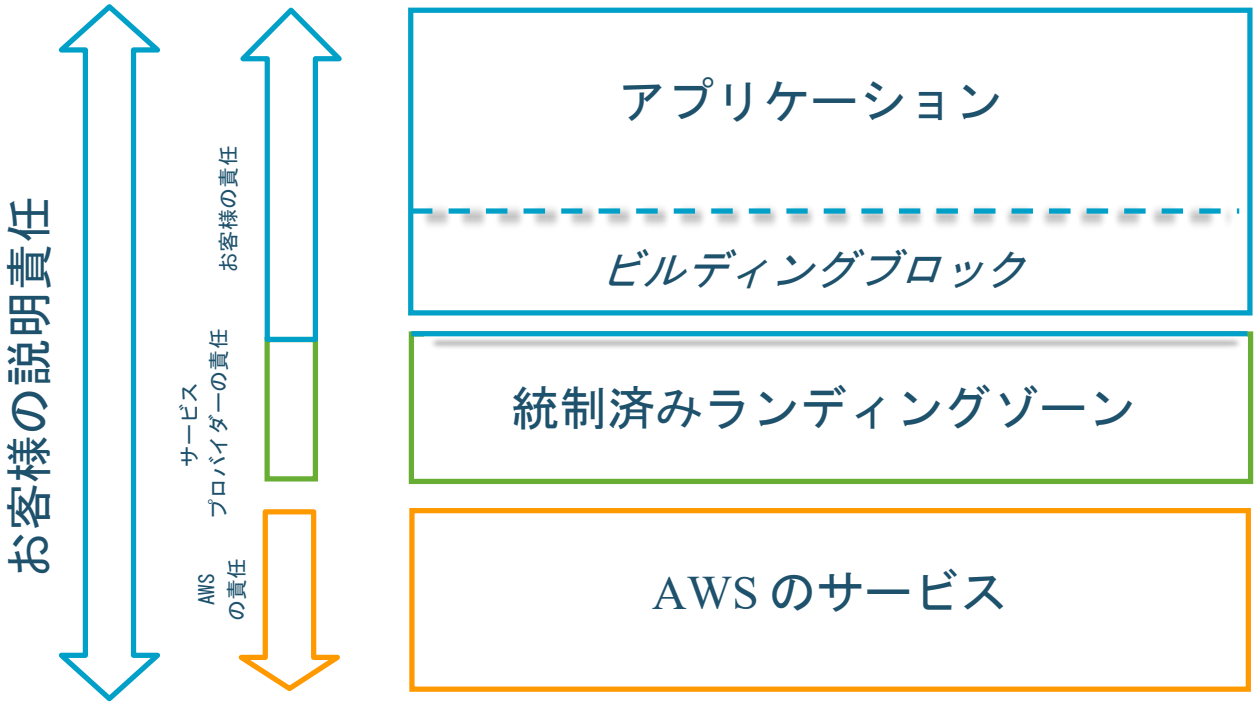

図 3: サービスプロバイダーを使用した階層型アーキテクチャ

このような状況では、さらに多くの責任がお客様によって委任されているので、通常、独自の操作を管理するために、お客様が実装している統制に対して適応を加え、同様の統制がサービスプロバイダーによって実装されていることを確認する必要があります。AWS から継

承された統制は共有され、またはお客様が維持する統制については、本ホワイトペーパーの「セキュリティ責任共有モデル」のセクションで説明しています。

このセクションでは、これらの階層の概要を説明します。階層については、本ホワイトペーパーの後述セクションでさらに説明します。

3.2.1 業界ガイダンス

以下のガイダンスは最小限ですが、お客様の環境におけるベストプラクティスです。引き続き専門家と協力して、適用される規制要件を確実に遵守する必要があります。

オンプレミスインフラストラクチャのクオリフィケーションを管理する基本原則は、同様にクラウドベースのシステムにも適用されます。したがって、この戦略では、次の ISPE GAMP Good Practice Guides（*図 4*）に基づいて、クラウドの観点から同様の業界のガイダンスを活用し、構築する手法を使用します。

- GAMP Good Practice Guide: IT インフラストラクチャの管理とコンプライアンス 第 2 版
- GAMP 5:コンピュータ化システムの GxP 適合へのリスクベースアプローチ

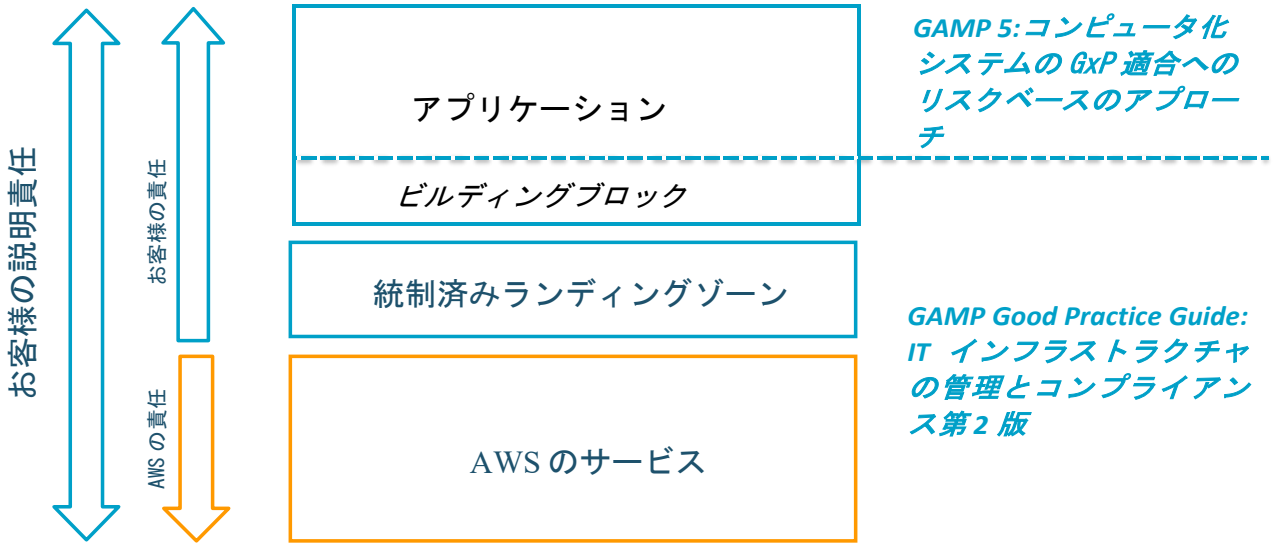

図 4: 業界ガイダンスをアーキテクチャの階層にマッピング

3.2.2 サプライヤーのアセスメントと管理

業界のガイダンスでは、サプライヤーの経験、知識、およびドキュメントを可能な限り活用することが推奨されています。しかし、現在多くの責任がサプライヤーに委ねられているため、サプライヤーに対するアセスメントはさらに重要になります。規制

対象企業は、たとえサプライヤーがそのシステムの一部について責任を負う場合でも、GxP システムが規制に準拠していることを証明する責任があります。このため、規制対象のお客様はサプライヤーに対する十分な信頼を確立する必要があります。

クラウドサービスプロバイダーに対して、オファーされたサービスを提供できるかを初めに評価するだけでなく、品質システムの適合性を判断し、体系的に準拠しているかを評価する必要があります。サプライヤーは QMS を実装していることを示し、次のような活動を管理する上で、一連の文書化された手順ならびに基準に準ずる必要があります。

- インフラストラクチャのクオリフィケーションと運用
- ソフトウェア開発
- 変更管理
- リリース管理
- 構成管理
- サプライヤー管理
- トレーニング
- システムセキュリティ

AWS QMS の詳細については、本ホワイトペーパーのソフトウェアセクションで説明します。これらの領域を満たす AWS の機能は、通常 AWS Artifact を通じて入手可能な最新の資料（AWS 認証および監査レポートなど）を確認することにより、定期的に再評価することができます。

また、責任共有モデルにまたがる運用プロセスがどのように動作するかを検討し、計画することも重要です。例えば、ランディングゾーンまたはアプリケーションの一部として使用されるサービスに対して AWS による変更を管理する方法、システム停止時のインシデント対応管理、またはクラウドサービスプロバイダーを変更する必要がある場合にポータビリティ要件を管理する方法などです。

3.2.3 統制済みランディングゾーン

ランディングゾーンの主な機能の 1 つは、開発チームが構築を行うための強固な基盤を提供し、可能な限り多くの規制要件に対処することで、開発チームの責任を排除することです。

GAMP IT インフラストラクチャの管理とコンプライアンスのガイダンス文書は、IT インフラストラクチャのクオリフィケーションに対するプラットフォームベースのアプローチに従っており、お客様のランディングゾーンを評価するニーズに完全に適合します。AWS Control Tower では、AWS がクラウドに移行する際の数千もの企業と連携した経験を通じて確立されたベストプラクティスに基づいて、新しく、安全で、マルチアカウントな AWS 環境を設定および管理するための最も簡単な方法を提供します。一般的なランディングゾーンに含まれる詳細については、AWS Control Tower の機能をご参照ください。

GAMP では、プラットフォームクオリフィケーションにアプローチするための 2 つのシナリオについても説明します。

1. 最初のシナリオは、特定のアプリケーションに依存せず、プラットフォームまたはランディングゾーンの一般的な要件を考慮します。
2. 次のシナリオでは、プラットフォームの要件を、プラットフォーム上で実行されるアプリケーションから直接引き出します。

多くのお客様が最初にランディングゾーンを構築するとき、実行されるアプリケーションの正確な性質は不明です。したがって、本ホワイトペーパーでは、シナリオ 1 に従い、特定のアプリケーションに依存しないクオリフィケーションにアプローチします。ランディングゾーンの目的は、アプリケーションチームが構築を行うための強固な基盤を提供し、可能な限り多くの規制要件に対処することで、アプリケーションチームの責任を排除することです。

3.2.3.1 ツールと自動化

多くのお客様は、一度でクオリフィケーションおよびバリデーションを行い、すべての開発チームで使用することができるよう、ランディングゾーンの一部として共通のツールおよび自動化を含めています。この共通ツールは、多くの場合、ランディングゾーンの共有サービスアカウント内にあります。

例えば、要件管理、テスト管理、CI/CD などに関係した標準ツールは、クオリフィケーションおよびバリデーションの対象とする必要があります。

同様に、IT プロセスの自動化もバリデーションする必要があります。例えば、コンピュータシステムのバリデーションプロセスにおける据付時適格性評価 (IQ) 手順を自動化できます。

3.2.3.2 AWS Managed Services の活用

ランディングゾーンを自分で構築し運用する代わりに、この責任を委任することができます。これは AWS Managed Services を利用して AWS に委任、または AWS パートナーネットワーク (APN) 内のパートナーに委任することができます。つまり、サービスプロバイダーは、AWS ベストプラクティスに基づいてランディングゾーンを構築し、業界のベストプラクティスに従って運用し、お客様の期待に応えるための十分な証拠を提供する責任があります。

3.2.4 ビルディングブロック

アプリケーションをサポートする仮想インフラストラクチャとサービスインスタンスについては、次の 2 つのアプローチがあります。

1. 特定のアプリケーションを対象に、サービスインスタンスを委託します。したがって、各アプリケーションチームは独自のクオリフィケーションアクティビティを処理しますが、アプリケーション/製品チーム間でクオリフィケーション作業が重複する可能性があります。
2. すべてのアプリケーションで使用する「ビルディングブロック」を定義します。一度クオリフィケーションした後は何度でも使用できる、標準の再利用可能なビルディングブロックを作成します。

全体的な労力を削減し、開発者の生産性を向上させるために、本ホワイトペーパーではオプション 2 の使用を前提としています。

「ビルディングブロック」は、Amazon EC2 や Amazon RDS のような単一の AWS サービスや、Amazon VPC と NAT ゲートウェイのような組み合わせた AWS サービス、あるいは 3 層ウェブアプリケーションや ML Ops スタックのような完全なスタックです。

「ビルディングブロック」のクオリフィケーションは、GAMP IT インフラストラクチャの管理とコンプライアンスのガイダンス内の「9.2 インフラストラクチャビルディングブロックのコンセプト」に準拠したプロセスに従います。

アプリケーション開発を迅速化するために、これらの標準化された事前クオリフィケーション済みのビルディングブロックのライブラリを作成し、開発チームが簡単に利用できるようにすることができます。

3.2.5 コンピュータ化システムバリデーション

サプライヤーのアセスメントおよびランディングゾーンによって強固で規制に準拠した基盤を築くことで、既存のコンピュータ化システムバリデーション(CSV) の標準業務手順書 (SOP) の改善を図ることができます。大半のお客様は、コンピュータ化シス

テムバリデーションに関する既存の SOP を既に社内に置いています。そして多くのお客様は、プロセスが時代遅れで、遅く、本質的に手作業が非常に多いと述べています。また、クラウドへの移行は、これらのプロセスを改善し、可能な限り自動化できる機会として捉えています。

前述の「ビルディングブロック」のアプローチは、開発チームにとって優れたアクセラレータであり、事前にクオリフィケーションされたビルディングブロックを組み合わせてアプリケーションの基礎を形成することができます。ただし、アプリケーションチームは、据付時適格性評価 (IQ) を含むアプリケーションのバリデーションの責任があります。

ここもまた、お客様のアプローチが異なるところです。今なお既存のプロセスに従い、ドキュメントを生成し、エンタープライズドキュメント管理システムに保管しているお客様もいます。他のお客様は、自動化を完全に採用し、ツールチェーンをバリデーションし、それらのツールに保存されているデータを証拠として活用することで、「ほぼドキュメントがない状態」を達成しています。

3.2.6 クラウド移行中のバリデーション

クオリフィケーション戦略で取り上げられる重要なポイントの 1 つは、移行中のコンピュータ化システムバリデーション(CSV) に対する包括的なアプローチです。移行作業に着手する場合は、アプリケーションのポートフォリオの分析の一部として、アーキタイプ、または類似のアーキテクチャを持つアプリケーションのグループを特定します。単一のランブックを開発し、グループ内の各アプリケーションに対して繰り返し実行できるため、移行が高速化されます。

この時点で、アプリケーションが GxP に関連している場合は、アーキテクチャタイプを対象に CSV/移行戦略を定義し、アプリケーションごとに繰り返すことができます。

3.3 サプライヤーのアセスメントとクラウド管理

前述したように、特定のクラウドインフラストラクチャとセキュリティ管理をクラウドサービスプロバイダーから継承することになるため、クラウドサービスプロバイダーへの信頼を得ることは非常に重要です。業界のガイダンスで説明されているアプローチには、ここで説明するいくつかのステップが含まれます。

3.3.1 基本的なサプライヤーアセスメント

最初の（任意の）ステップは、基本的なサプライヤーアセスメントを実行し、サプライヤーの市場での評判、知識、規制対象の業界での経験、他の規制対象企業との経験、および彼らが保有している認証を確認することです。

AWS ニュースブログ記事にある、Gartner の評価などの業界アセスメントを活用できます「AWS Named as a Cloud Leader for the 10th Consecutive Year in Gartner's Infrastructure & Platform Services Magic Quadrant」や「Customer Testimonials」。

3.3.2 ドキュメントのレビュー

サプライヤーアセスメントでは多くの場合、QMS とオペレーションを説明する、サプライヤーから入手可能な資産について深く掘り下げます。これには、認証、監査レポート、ホワイトペーパーのレビューが含まれます。詳細については、「AWS Risk and Compliance ホワイトペーパー」をご参照ください。

AWS とそのお客様は IT 環境の管理を共有するため、両者は IT 環境を管理する責任を負います。AWS 側の責任共有には、安全性の高い、管理されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をお客様に提供することが含まれます。お客様側の責任共有には、用途に合わせて安全で管理された方法で IT 環境を設定することが含まれます。お客様から使用方法と設定を AWS にお伝えいただかなくても、AWS からお客様に関わるセキュリティと管理環境についてお伝えします。そのために、AWS は次のことを行います。

- 業界の認定と独立した第三者の認証を取得します。
- AWS のセキュリティと管理に関する情報をホワイトペーパーおよびウェブサイトコンテンツで公表します。
- （必要に応じて）NDA 下において AWS のお客様に証明書、レポートなどの文書を直接提供します。

AWS のセキュリティの詳細については、AWS クラウドセキュリティをご参照ください。

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へのオンデマンドアクセスを提供し、オンライン契約を選択します。AWS Artifact で入手可能なレポートには、Service Organization Control (SOC) レポート、クレジットカード業界 (PCI) レポート、AWS セキュリティコントロールの実装と運用効果を検証する地域やコンプライアンス分野にまたがる認定機関からの証明が含まれます。AWS Artifact で入手可能な契約には、 事業提携契約 (BAA)および秘密保持契約 (NDA) が含まれます。AWS コンプライアンスの詳細については、AWS コンプライアンスをご参照ください。

AWS 認定、または AWS が提供しているコンプライアンスドキュメントについて
さらに質問がある場合は、お客様のアカウントチームにお問い合わせください。

3.3.3 サービスレベルアグリーメント (SLA)のレビュー

AWS は特定の AWS サービス向けに、サービスレベルアグリーメントを提供します。詳細については、サービスレベルアグリーメント(SLA) をご参照ください。

3.3.4 監査

メール監査 - 収集した AWS のドキュメントを補足するために、メール監査アンケート（サプライヤーアンケートとも呼ばれる）を AWS に送信して、追加情報を収集したり、疑問を解消するために質問したりすることができます。メール監査をリクエストするには、アカウントチームにお問い合わせください。

オンサイト監査 - AWS は定期的に独立した第三者による認証監査を受け、統制活動が意図したとおりに動作していることを保証しています。現在、AWS は 50 を超える監査プログラムに参加しています。これらの監査の結果は評価機関によって文書化され、AWS Artifact を通じてすべての AWS のお客様に提供されます。AWS を対象としたこれらの第三者認証と認定により、制御環境の可視性と独立したバリデーションが可能になり、お客様は個々のオンサイト監査を実行する必要がなくなります。このような認証と認定は、AWS クラウド内の IT 環境に対して特定のバリデーション作業をお客様自身で実行するという要件の緩和にも役立ちます。詳細については、本ホワイトペーパーの AWS の品質管理システムのセクションをご参照ください。

3.3.5 契約上の合意

AWS のサプライヤーアセスメントを完了したら、次のステップは、AWS サービスを使用するための契約上の合意をすることです。AWS カスタマーアグリーメントは、次から入手が可能です(https://aws.amazon.com/agreement/)。お客様は、規制内容を理解し、適切な要件が標準条件と共に契約に含まれているかどうかを判断する責任があります。AWS とのサービス契約の締結についてご質問がある場合は、アカウントチームにお問い合わせください。

3.3.6 クラウド管理プロセス

責任共有モデルにまたがる特定のプロセスがあり、通常は SOP と作業指示の形式で QMS に取り込む必要があります。

3.3.6.1 変更管理

クラウドサービスプロバイダーとの変更管理は、双方向プロセスとなります。一方で、AWS は、本ホワイトペーパーで前述したように、サービスを改善するために継続的に変更を加えています。そのまた一方で、お客様は機能のリクエストを行うこともできます。これは、AWS サービス機能の 90%がお客様からの直接的なフィードバックの結果であるため強くお勧めします。

通常、お客様は、変更の種類に適したリスクベースのアプローチを使用して、その後のアクションを決定します。

機能を追加する AWS サービスへの変更は、アプリケーションがその新機能をまだ使用していないため、通常は問題ではありません。ただし、新しい機能は、サービスのリスクプロファイルに影響し、使用を許可する必要があるかどうかを判断するために、内部アセスメントをトリガーすることがあります。QMS によって義務付けられている場合、新しい機能を許可する前に、ビルディングブロックの再クオリフィケーションをトリガーする可能性があります。

機能の廃止は、アプリケーションを壊す可能性があるため、より重要であると考えられます。機能の廃止には、サードパーティーのライブラリ、ユーティリティ、または Python などの言語のバージョンが含まれる場合があります。サービスまたは機能の廃止はまれです。廃止の通知を受け取ったら、影響アセスメントをトリガーする必要があります。影響が見つかった場合、アプリケーションチームは変更を計画し、影響を修復する必要があります。廃止の通知期間には、アセスメントと修復のための時間を考慮します。また AWS は、お客様が変更の影響を理解するお手伝いをします。

サービスの機能を変更せず、お客様への通知をトリガーしない機能の強化やバグ修正など、その他の変更も存在します。これらのタイプの変更は通常、事前承認済みの、リスクが低く、比較的一般的であり、特定の手順に従う ITIL の「標準」の変更と同義です。このクラスの変更により回帰が発生しないことを示す証拠を生成したい場合は、AWS サービスを繰り返しテストし、回帰を検出するテストベッドを作成します。

問題が明らかになった場合は、解決に向けて直ちに AWS に報告する必要があります。

3.3.6.2 インシデント管理

Amazon Security Operations チームは、業界標準の診断手順を採用して、ビジネスに影響を与えるイベントの発生時の解決を推進しています。スタッフオペレーターは、インシデントを検出し、影響と解決を管理するために、24 時間 365 日体制で対応します。プロセスの一環として、お客様のコンテンツの侵害の可能性を調査し、AWS セキュリテ

ィと AWS リーガルにエスカレーションします。法的に必要な場合、影響を受けるお客様および規制当局は、違反やインシデントが通知されます。判明したセキュリティ問題に関する情報が含まれている、AWS セキュリティ速報ページ (https://aws.amazon.com/security/security-bulletins) を購読することもできます。セキュリティ速報 RSS フィードを購読すると、セキュリティ速報 Web ページの最新のセキュリティ通知を入手することができます。

AWS が原因でない限り、ストレージ、仮想マシン、およびアプリケーションに関するインシデントの報告はお客様の責任となります。

詳細については、AWS 脆弱性レポートのウェブページをご参照ください。 https://aws.amazon.com/security/vulnerability-reporting/

3.3.6.3 カスタマーサポート

AWS は、パフォーマンスを検証するためのメトリクスを含むカスタマーサポート手順を開発し、維持しています。お客様が AWS サービスの品質目標が達成していないことを AWS に報告すると、問題は調査され、必要に応じて商業的に合理的な措置を通じて解決を図ります。AWS がお客様に影響する問題を最初に認識した場合には、契約要件に従って、または AWS サービスヘルスダッシュボードを通じて、影響を受けるお客様に通知する仕組みになっています http://status.aws.amazon.com/。

お客様のポリシーと手順が、AWS が提供するカスタマーサポートオプションと一致するようにしてください。詳細については、本ドキュメントの「お客様からの苦情」および「お客様のトレーニング」のセクションをご参照ください。

3.4 クラウドプラットフォーム/ランディングゾーンのクオリフィケーション

AWS Control Tower によって作成されたようなランディングゾーンは、セキュリティとコンプライアンスのベストプラクティスに基づく、優れた設計のマルチアカウント AWS 環境です。

ランディングゾーンには、集中ログ、セキュリティ、アカウントのベンディング、およびコアネットワーク接続の機能が含まれています。次に、可能な限り多くの規制要件を満たし、そのゾーン上で構築する開発チームの負担を効果的に取り除けるよう、ランディングゾーンに機能を組み込むことをお勧めします。ランディングゾーンとその所有チームの目的は、開発者が「仕事に適したツール」を使用できるようにガードレールと機能を提供し、さらにコンプライアンスではなく、差別化されたビジネス価値を提供することに焦点を当てることです。

例えばアカウントのベンディング機能を拡張して、アカウントのブートストラップを行うことで、ログを中央ログアカウントに自動的に送り、デフォルトの VPC を削除して承認済みの VPC （必要な場合）をインスタンス化、ベースラインスタックセットをデプロイし、据付時適格性評価 (IQ) などをサポートする標準ロールを確立することを含めることができます。Shared Services アカウントには、前述の IQ の自動化のような、一元化された機能と自動化が含まれます。集中ログアカウントは、例えばライフサイクルポリシーの使用による記録保存など、監査証跡に関する規制要件を満たすことができます。バックアップ/アーカイブ用アカウントを追加すると、アプリケーションチームが使用するアーカイブサービスと共に、標準のバックアップと復元を提供できます。

同様に、CloudEndure Disaster Recovery などのツールを使用したランディングゾーンによってディザスタリカバリ(DR) への標準化されたアプローチを提供できます。

AWS ガイダンスに準拠し、クラウドセンターオブエクセレンス (CCoE) を実装し、ランディングゾーンを製品として考える場合、CCoE チームは、規制要件を満たすためにこれらの機能をランディングゾーンに構築する責任を負います。ランディングゾーンに組み込まれている機能の数は、多くの場合、その周りの組織構造の影響を受けます。開発チームとインフラストラクチャが分割された従来の構造では、サーバーやネットワーク管理などのタスクが集中化され、これらの機能がプラットフォームに組み込まれます。製品中心の運用モデルを採用すると、開発チームはより自律的になり、多くのスタックを担当できるようになります。おそらく VPC からのスタック全体と、その上に構築されたすべてのスタックの責任も高くなります。またサーバーレスアーキテクチャでは、管理するサーバーがないため、VPC が必要ない可能性もあることを考慮してください。

GxP アプリケーションをサポートする上で基盤となるクラウドプラットフォームは、適切な設定を実証し、統制とコンプライアンスの状態を維持するためにクオリフィケーションされる必要があります。クラウドのクオリフィケーションは、従来のインフラストラクチャクオリフィケーションプロジェクトに従うことができます。このプロジェクトには、計画、仕様と設計、リスクアセスメント、クオリフィケーションテスト計画、据付時適格性評価(IQ)、運用時適格性評価 (OQ)、および引き渡し（GAMP IT のセクション 5「プラットフォームのクオリフィケーション」で説明）が含まれます。

ランディングゾーンを構成するコンポーネント（設定項目）はすべて、自動化された手段、つまり自動化されたパイプラインによってデプロイする必要があります。このアプローチは、今後のより優れた変更管理をサポートします。

インフラストラクチャプロジェクトの完了と、運用およびメンテナンス SOP の作成が完了すると、GxP ワークロードを実行できるクオリフィケーション済みのクラウドプラ

ットフォームが実現します。SOP では、アカウントのプロビジョニング、アクセス管理、変更管理などのトピックについて説明します。

3.4.1 ランディングゾーンのクオリフィケーション状態の維持

ランディングゾーンがライブ状態になったら、クオリフィケーション済みの状態で維持する必要があります。オペレーションがパートナーに委任されない限り、通常、GAMP IT インフラストラクチャの管理とコンプライアンスのセクション 6 に基づいて、クラウドプラットフォームの運用とメンテナンス SOP を作成します。

GAMP によると、変更管理、構成管理、セキュリティ管理など、管理を表示する必要がある領域がいくつかあります。GAMP ガイダンスでは、可能な限り「自動ツール」を使用する必要があることも示唆されています。以下のセクションでは、これらの管理領域と、AWS サービスが自動化にどのように役立つかについて説明します。

3.4.1.1 変更管理

変更管理プロセスでは、設定項目の変更方法を管理します。これらのプロセスには、ランディングゾーンがサポートする GxP アプリケーションに対する潜在的な影響のアセスメントを含める必要があります。前述のように、ランディングゾーンコンポーネントはすべて、自動化されたパイプラインを使用してデプロイされます。したがって、AWS CodeCommit などのソースコードリポジトリツールで変更が承認され、コミットされると、パイプラインがトリガーされ、変更がデプロイされます。ランディングゾーンを構成するさまざまなパーツには、複数のパイプラインが存在する可能性があります。

ランディングゾーンは、インフラストラクチャとオートメーションコンポーネントで構成されています。コードとしてのインフラストラクチャを使用することにより、これらの異なるコンポーネントのデプロイ方法に実際の違いはありません。

継続的なデプロイの方法を推奨します。これにより変更が自動的に構築、テスト、デプロイされることを保証し、可能な限り多くの手動ステップを排除することを目標としています。継続的なデプロイでは、このプロセスの手動性を排除し、各ステップを自動化することで、開発チームはプロセスを標準化し、コードをデプロイするための効率を上げることができます。継続的デプロイでは、リリースプロセス全体がステージを含む*パイプライン*になります。AWS CodePipeline は AWS CodeCommit、AWS CodeBuild、AWS CodeDeploy と併用が可能です。追加の承認ステップが必要なお客様のために、AWS CodePipeline は手動手順もサポートしています。

AWS サービスに対するすべての変更（手動または自動）は、AWS CloudTrail によって記録されます。

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、および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全体のアクションに関連するアカウントアクティビティをログに記録し、継続的にモニタリングし、保持できます。
CloudTrail では、AWS マネジメントコンソール、AWS SDK、コマンドラインツールなどの AWS のサービスを通じて実行されたアクションを含む、AWS アカウントアクティビティのイベント履歴を提供します。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、およびトラブルシューティングが簡素化されます。さらに、CloudTrail の使用により、AWS アカウントの異常なアクティビティを検出できます。これらの機能は、運用の分析とトラブルシューティングを簡素化するのに役立ちます。

お客様が無許可の変更や意図しない変更についてもアラートを受けたいと考えるのは当然です。AWS CloudTrail と AWS CloudWatch を組み合わせて使用することで、本稼働環境に加えられた不正な変更を検出し、迅速な修正を自動化することもできます。Amazon CloudWatch は、AWS クラウドリソースのモニタリングサービスであり、AWS CloudTrail イベントへの応答をトリガーするために使用できます (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html)。

3.4.1.2 構成管理

変更管理と密接する機能は、構成管理です。構成項目 (CI) はシステムを構成するコンポーネントであり、CI の変更は変更管理プロセスのみを通じて行う必要があります。

Infrastructure as Code は、AWS CloudFormation などのツールを使用することでプロビジョニングプロセスを自動化します。手動で実行する手順に依存するのではなく、管理者と開発者は、構成ファイルを使用してインフラストラクチャをインスタンス化できます。Infrastructure as Code は、これらの構成ファイルをソフトウェアコードとして扱います。これらのファイルは、オペレーション環境を構成するコンピューティング、ストレージ、ネットワーク、アプリケーションサービスなど、一連の成果物を生成するために使用できます。Infrastructure as Code は、自動化によって構成のドリフトを排除し、インフラストラクチャのデプロイのスピードと俊敏性を高めます。

AWS Tagging and Resource Groups を使用すると、さまざまな粒度レベルでタグを適用し AWS ランドスケープを整理できます。タグを使用すると、サービス内のリソースとコンポーネントにラベル付け、収集、整理することができます。

タグエディターを使用すると、複数のサービスおよび AWS リージョンにまたがるタグを管理できます。このアプローチを使用すると、対象ランドスケープのすべてのアプリケーション、ビジネス、データ、テクノロジーコンポーネントをグローバル規模で管理できます。

AWS Resource Group は、1 つ以上のタグを共有するリソースのコレクションです。お客様の IT ランドスケープのエンタープライズアーキテクチャビューを作成し、AWS リソースをプロジェクト単位（つまり、目指すランドスケープを実現するために進行中のプログラム）、エンティティ単位 （機能、ロール、プロセス）、およびドメイン単位（ビジネス、アプリケーション、データ、テクノロジー）のビューに統合できます。

AWS Config は AWS リソースの設定をアセスメント、監査、評価するために使用するサービスです。AWS Config では、AWS リソースの設定の継続的なモニタリングと記録が行われ、適切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。AWS Config を使用すると、設定の変更をレビューし、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判断できます。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、運用のトラブルシューティングを簡素化できます。さらに AWS Config では、AWS Config 用のコンフォーマンスパックを提供するため、管理対象またはカスタムの AWS Config ルールと AWS Config 修復アクション（21 CFR 11 のコンフォーマンスパックを含む）を使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。

お客様は AWS CloudFormation、AWS Config、タグ付け、および Resource Group を使用して、お客様の企業が使用しているクラウド資産をいつでも正確に確認できます。また、これらのサービスにより、不正なサーバーまたはシャドウアプリケーションが対象の実稼働環境に出現した際に、瞬時に簡単に検出できます。

3.4.1.3 セキュリティ管理

アマゾンウェブ サービス (AWS) で実行するアプリケーションのセキュリティインフラストラクチャおよび設定を現在設計しているお客様向けに、ベストプラクティスを定義しています。

AWS リソースでは、AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスを提供しています。

また、これらの AWS リソースでは、AWS 上での資産の識別、分類と保護や、アカウント、ユーザー、グループを使用した AWS リソースへのアクセス管理、また、クラ

ウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャ全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要を説明しています。

AWS は、クラウド内のワークロードを保護するための広範なツールセットを提供します。

完全な自動化を実装すると、開発以外のあらゆる環境に直接アクセスする必要性がなくなります。ただし、本稼働環境にアクセスする必要が生じた場合、ユーザーは明確にアクセスを要求し、適切な所有者によるアクセスのレビューと承認を行い、承認後に必要最小限の権限で、必要な期間だけの一時アクセスを取得する必要があります。その後、アクセスが許可されている期間中、ログを通じてアクティビティを追跡する必要があります。詳細については、この AWS リソースをご参照ください。

3.4.1.4 問題およびインシデント管理

AWS を使用すると、問題やインシデント管理の目標を達成する上で役立つ多くのツールや機能にアクセスできます。これらの機能により、クラウドで実行されるアプリケーションの目的に合った設定とセキュリティのベースラインを確立できます。

ベースラインからの逸脱（設定ミスなど）が発生した場合は、対応して調査する必要があります。正確に対応するには、セキュリティ問題が発生する前に AWS 環境内のセキュリティインシデント対応の基本概念と、クラウドチームの準備、教育、トレーニングを行うために考慮する必要がある課題を理解しなければなりません。使用できる統制と機能を把握し、潜在的な懸念を解決するための課題例を確認し、自動化を活用し、応答速度を向上させるために利用できる修復方法を特定することが重要です。セキュリティインシデント対応は複雑な課題になる可能性があるため、小規模から開始し、ランブックを開発し、基本的な機能を活用し、インシデント対応メカニズムの初期ライブラリを作成して、反復処理および改善することをお勧めします。この最初の作業には、セキュリティに関与していないチームも含める必要があり、法務部門を含める必要があります。これにより、チームがインシデント対応 (IR) とその選択が企業の目標に及ぼす影響をよりよく理解できるようになります。

包括的なガイドについては、AWS Security Incident Response Guide をご参照ください。

3.4.1.5 バックアップ、リストア、アーカイブ

バリデーションされたすべてのアプリケーションには、バックアップとリストア機能が必要です。したがって、この機能は統制済みランディングゾーンにおいて一元化できる共通の機能です。「バックアップとリストア」を「アーカイブとリトリーブ」と混同しないようにしてください。ただし、この 2 つの領域は一元的な機能に統合することが可能です。

クラウドベースのバックアップとリストア機能については、AWS Backup を検討してください。

AWS Backup は、完全マネージド型のバックアップサービスで、AWS のサービス全体にわたるデータのバックアップの一元化および自動化を容易にします。AWS Backup を使用すると、Amazon EBS ボリューム、Amazon EC2 インスタンス、Amazon RDS データベース、Amazon DynamoDB テーブル、Amazon EFS ファイルシステム、Amazon FSx ファイルシステム、AWS Storage Gateway ボリュームなどの AWS リソースのバックアップアクティビティを監視し、バックアップポリシーを一元的に設定できます。AWS Backup は、これまでサービスごとに実行されたバックアップタスクを自動化および統合するため、カスタムスクリプトや手動プロセスを作成する必要がありません。AWS Backup コンソールで数回クリックするだけで、お客様はバックアップスケジュールと保持管理を自動化するバックアップポリシーを作成できます。AWS Backup では、完全に管理されたポリシーベースのバックアップソリューションを提供します。バックアップ管理を簡素化し、ビジネスおよび規制のバックアップコンプライアンス要件を満たすことができます。

3.4.1.6 ディザスタリカバリ

従来のオンプレミスの状況では、ディザスタリカバリ(DR) に、プライマリデータセンターから一定の距離にある別のデータセンターが含まれていました。この別のデータセンターは、プライマリデータセンターに影響を及ぼす完全な障害が発生した場合にのみ存在します。
多くの場合、DR サイトのインフラストラクチャはアイドル状態にあるか、最善のケースでもアプリケーションの本番前のインスタンスをホストするため、本稼働環境と非同期になる危険性があります。クラウドの登場により、DR は、はるかに簡単で安価になりました。

AWS グローバルインフラストラクチャは、AWS リージョンとアベイラビリティーゾーン (AZ) を中心に構築されています。AWS リージョンには、物理的に分離し独立された複数のアベイラビリティ—ゾーンを提供します。アベイラビリティーゾーンは、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ます。アベイラビリティーゾーンを使用すると、中断することなくアベイラビリティーゾーンをまたいで自動的にフェイルオーバーを行うアプリケーションとデータベースを設計および運用できます。アベイラビリティーゾーンは、従来の 1 つ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可用性、耐障害性に優れ、スケーラブルです。

AWS アベイラビリティーゾーンを使用すると、1 つ以上のゾーンの完全な障害に対応可能なマルチ AZ アーキテクチャを簡単に作成できます。回復力をさらに高めるために、複数の AWS リージョンを使用できます。コードとしてのインフラストラクチャを使用する場合、DR リージョンのインフラストラクチャとアプリケーションを常に実行する必要はありません。災害が発生した場合、アプリケーションスタック全体を別のリージョンにデプロイできます。常に実行する必要があるコンポーネントは、データリポジトリの同期状態を維持するコンポーネントだけです。

CloudEndure Disaster Recovery などのツールを使用すると、ディザスタリカバリを自動化できます。

3.4.1.7 パフォーマンスのモニタリング

Amazon CloudWatch は、AWS クラウドリソースと AWS で実行されるアプリケーションのためのモニタリングサービスです。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、およびお客様の AWS リソースへの変更に自動的な対応が可能です。CloudWatch は、カスタマーアプリケーションのランドスケープの動作を監視し、ログに記録します。CloudWatch は、アプリケーションの動作に基づいてイベントをトリガーすることもできます。

3.5 ビルディングブロックのクオリフィケーション

お客さまは、AWS の開発者が法規制の順守と迅速な開発を維持しながら、AWS サービスを自由に使用できる方法を良く知りたがることがあります。この問題に対処するためにテクノロジーを活用できますが、プロセス設計の変更も伴います。ブロックステップからガードレールへの移動も必要になります。お客様のプロセスと IT 運用モデルに必要な変更点は、本ホワイトペーパーの対象外です。しかし 私たちはビルディングブロックをクオリフィケーションするための、サポートプロセスのコアなステップについて説明します。これは、法規制の順守をより効率的に維持するための戦略の 1 つになります。

GAMP によって定義されるインフラストラクチャビルディングブロックの概念は、個々のコンポーネントまたはコンポーネントの組み合わせをクオリフィケーションするためのアプローチであり、それらをまとめて IT インフラストラクチャを構築できます。このアプローチは AWS サービスに適用されます。

このアプローチの利点は、ビルディングブロックの 1 つのインスタンスを 1 度クオリフィケーションし、他のすべてのインスタンスが同じように実行されることを想定することで、アプリケーション全体の労力を削減できることです。また、このアプローチにより、お客様はインフラストラクチャに依存するアプリケーションすべてに対する

再クオリフィケーションや、アプリケーションの再バリデーションを必要とせずに、ビルディングブロックを変更することもできます。

3.5.1 サービスの承認

サービスの承認は、アーキテクチャガバナンスの一部として、多くのお客様が使用する技術です。つまり、規制対象のワークロードと規制対象外のワークロードにわたって使用されます。お客様は、開発チームによるサービスの使用を承認する際に、複数の規制を考慮することがよくあります。例えば、サンドボックスアカウントですべてのサービスの使用を許可しても、アプリケーションが HIPAA 規制の対象となる場合は、アカウント内のサービスを HIPAA 対象サービスのみに制限することができます。

サービスの承認は、AWS Organizations and Service Control Policies を使用して実装されます。

このアプローチを使用すると、サービスを GxP 関連のアプリケーションの一部として使用することができます。例えば、ISO、PCI、SOC、および HIPAA 適格性の組み合わせは、十分な信頼性を得ることができます。お客様は、GxP ワークロードに対する AWS サービスの承認で説明されているように、承認されたサービスに対する自動制御を実装したい場合があります。

次のビルディングブロッククオリフィケーションなど、より厳格なクオリフィケーションプロセスを踏むことを好む場合があります。

3.5.2 ビルディングブロックのクオリフィケーション

AWS のサービスの*ビルディングブロック*のクオリフィケーションは、GAMP IT インフラストラクチャの管理とコンプライアンスのガイダンス内の「インフラストラクチャビルディングブロックのコンセプト」（GAMP IT のセクション 9 ならびに付録 2）に基づくプロセスに従います。

> EU GMPによると、クオリフィケーションの
> 定義は次のとおりです。「機器が正しく動作し、実際に期待される結果につながることを証明する行動」。機器はまた、その運用期間にわたって期待される結果を生み出す必要があります。

言い換えると、お客様のプロセスが、ビルディングブロックが意図したとおりに動作し、運用期間を通じてコントロール下に置かれていることを示す必要があります。文書化された手順が準備され、実行されるとアクティビティが実際に発生したことを示す記録が生成されます。また、サービスを運営しているスタッフは、適切な訓練を受

ける必要があります。このプロセスは、多くの場合、全体的なクオリフィケーションとコミッショニング戦略、範囲、役割と責任、成果物リスト、クオリフィケーションとコミッショニングの要件を満たすために従う優れたエンジニアリングプラクティスを説明する SOP に記載されています。

AWS サービスの数が多いと、すべての AWS サービスを一度にクオリフィケーションすることは困難になります。サービスを優先順でクオリフィケーションする場合は、反復的かつリスクベースのアプローチが推奨されます。最初の優先順位付けでは、クラウドに移行する最初のアプリケーションのニーズを考慮し、クラウドサービスの需要の増加に応じて優先順位付けを再評価できます。

3.5.3 設計ステージ

3.5.3.1 要件

最初のアクティビティは、ビルディングブロックの要件を検討することです。1 つのアプローチとして、サービス API の定義を確認することです。各 AWS サービスには、そのサービスの全機能について述べている、明確に文書化された API があります。多くのサービス API は広範囲にわたり、いくつかの高度な機能をサポートしています。ただし、初期段階で高度な機能のすべてを必要とするわけではないため、既存のビジネスユースケースを考慮して範囲を絞り込むことができます。

例えば、Amazon S3 の要件を考慮する場合、バケットの作成、削除のコア機能と、オブジェクトの配置、取得、削除の機能が含まれます。ただし、まだ必要ではないため、ライフサイクルポリシー機能を範囲に含めない場合があります。これらの要件は、ビルディングブロック要件仕様、要件リポジトリにキャプチャされます。

また、機能以外の要件を考慮することも重要です。サービスの適合性を確認するために、サービスの SLA と制限を確認することができます。

3.5.3.2 ギャップ分析

アプリケーション要件が既に存在する場合は、範囲を制限するのと同じ方法で、ギャップを特定することもできます。このギャップは、Amazon S3 バケットのライフサイクル機能を範囲に組み込むなど、ビルディングブロックの機能を追加することで解決できるか、あるいはサービスが要件を満たすのに適していないため、別のビルディングブロックを使用する必要があります。

他のサービスが要件を満たしていないと思われる場合は、サービスをカスタム開発するか、サービス強化のために AWS に機能のリクエストを行うことができます。

3.5.3.3 リスクアセスメント

インフラストラクチャは、その上で実行されているバリデーション済みアプリケーションの信頼性、セキュリティ、ビジネスの継続性を確保するためのクオリフィケーションを受けています。これらの 3 つの要素は、通常、リスクアセスメントの分野に含まれます。公開された AWS SLA により AWS サービスの信頼性の情報が得られます。サービスの現在の状態と SLA への遵守履歴に関するデータは https://status.aws.amazon.com から入手できます。セキュリティの信頼性を調査するため、関連するサービスの AWS 認証を確認することができます。ビジネス継続性のために、AWS は停止やインシデントから保護するように構築されており、AWS サービスの設計もこの要素を考慮しています。そのため、中断が発生した場合、お客様への影響とサービスの継続性への影響は可能な限り最小限に抑えられます。

このステップは、GxP クオリフィケーションのためだけではありません。リスクアセスメントには、HIPAA などの他の規制に対する追加のチェックを含める必要があります。

クラウドサービスのリスクをアセスメントする際には、他のビルディングブロックとの関係性を考慮することが重要です。例えば、お客様がデータベースを VPC のプライベートサブネット内にのみ配置すると判断した場合、Amazon RDS データベースは Amazon VPC のビルディングブロックと関係性を持つ場合があります。したがって、VPC はアクセスコントロールに関する多くのリスクに対処しています。これらの依存関係はリスクアセスメントで取得され、サービス固有の追加のリスク、または周囲の運用環境では対応できない残存リスクに重点を置きます。

各クラウドサービスのビルディングブロックは、一連のリスクを識別するためのリスクアセスメントの対象となります。特定されたリスクごとに、軽減するプランが作成されます。軽減プランは、次のコンポーネントの 1 つ以上に影響を与える可能性があります。

- サービスコントロールポリシー
- コードテンプレートとしての技術設計/インフラストラクチャ
- 自動化されたコンプライアンス管理の監視と警告

リスクは、サービスコントロールポリシー (SCP) の使用によって軽減できます。サービスまたは特定の操作が危険すぎると見なされる場合、そのようなポリシーによってその使用が明示的に拒否されます。例えば SCP を使用することで、AWS マネジメントコンソールを通じて Amazon S3 オブジェクトの削除を制限できます。もう 1 つのオプシ

ョンは、特定の設定パラメータが制限またはパラメータ化される、承認された Infrastructure as Code (IaC) テンプレートの技術設計を通じて、サービスの使用を管理することです。例えば AWS CloudFormation テンプレートを使用して、Amazon S3 バケットを常にプライベートとして設定することができます。最後に、監視とアラートにフィードするルールを定義できます。例えばポリシー定義により、Amazon S3 バケットをパブリックにできないが、この設定がインフラストラクチャテンプレートで強制されていない場合、パブリック Amazon S3 バケットを対象にインフラストラクチャを監視できます。S3 バケットがパブリックとして設定されると、アラートによって修正がトリガーされます。たとえば、バケットを直ちにプライベートに変更するなどです。

3.5.3.4 技術設計

指定された要件とリスクに応じて、論理的なサービスのビルディングブロック設計とリスクまたは設計の要件までを含むトレーサビリティを記述したアーキテクチャ設計仕様が、クラウドインフラストラクチャアーキテクトによって作成されます。この設計仕様は、主にエンドユーザーとアプリケーション開発チーム向けにビルディングブロックの機能を記述します。

3.5.3.5 設計レビュー

提案された設計が、周囲の IT インフラストラクチャ設計における意図された目的に適していることを確認するために、適切なトレーニングを受けた担当者が最終チェックとして設計レビューを実行することが可能です。

3.5.4 構築ステージ

論理設計はドキュメントでも取得できますが、物理設計は AWS CloudFormation のテンプレートのように、Infrastructure as Code (IaC) のテンプレートで取得できます。この IaC テンプレートは、一貫性を保証するためのビルディングブロックのインスタンスをデプロイするために常に使用されます。アプローチの一例については、「クラウドでの GxP コンプライアンスの自動化：ベストプラクティスとアーキテクチャガイドライン」のブログ記事をご参照ください。

IaC テンプレートでは、パラメータを使用してワークロードの変動を処理します。これは多くの場合、設計作業の一環として IT 品質とセキュリティによって決定されます。サービスのリスクプロファイルに影響するパラメータと、管理が必要なパラメータ、およびユーザーが設定できるパラメータが決定されます。例えば、データベースの名前はテンプレートユーザーが設定可能で、通常はデータベースサービスのリスクプロファイルには影響はしません。ただし、暗号化管理のパラメータはリスクプロフ

ァイルに影響するため、テンプレート内で修正され、テンプレートユーザーによる変更はできません。

テンプレートは、編集可能なテキストファイルです。しかし、テンプレートに記述されたルールは、周囲の監視とアラート内でも自動化されます。例えば、データベースの暗号化設定の設定を義務付けるルールは、自動化ルールによってチェックできます。したがって、開発者は開発環境の暗号化設定をオーバーライドする可能性がありますが、その変更はバリデーション済み環境またはそれ以降の環境に進行することはできません。

この時点で、自動テストスクリプトをクオリフィケーションステップで実行に向けて準備し、テストエビデンスを生成できます。自動テストの作成者は適切なトレーニングを受ける必要があり、さらに別の適切なトレーニングを受けた担当者が自動テストのコードレビューおよび/またはランダムテストを実行して、品質レベルを確保する必要があります。

自動テストにより、ビルディングブロックが当初の期待どおりに機能することを確認します。特に変更の後で、これらのテストを再度実行することで、ビルディングブロックが期待どおりに機能し続けることを確認できます。ただし、本稼働環境開始後に何も変更されないようにするには、自動制御を特定して作成する必要があります。また Amazon S3 の例になりますが、すべてのバケットをプライベートにする必要があります。パブリックバケットが検出された場合、そのバケットはプライベートに戻され、アラートが発生し、通知が送信されます。S3 バケットを作成した個人を特定し、アクセス権限を取り消すことも可能です。

構築の最終部分は、必要な追加のガイダンスと操作マニュアルの作成と承認です。例えば、データベースを復旧する手順は、Amazon RDS ビルディングブロックの操作マニュアルに含まれる内容になります。

3.5.5 クオリフィケーションとコミッショニング段階

インフラストラクチャはすべてのビルディングブロックに対して同じ形式でデプロイされることが重要です。つまり、AWS CloudFormation を通じて、インフラストラクチャをコードテンプレートとして使用します。
したがって、通常はビルディングブロック固有のインストール手順は必要ありません。また、すべてのデプロイが仕様に従って実行され、正しい設定になっていることが確信できます。

3.5.5.1 自動化されたテスト

テストエビデンスを生成する場合は、機能要件が満たされ、特定されたすべてのリスクが軽減され、構築中に作成された自動テストの実行を通じて、ビルディングブロックが意図された用途に適していることを示すことができます。これらの自動テストの出力は、安全なリポジトリに保管され、テストエビデンスとして使用できます。

この自動化は、ビルディングブロックのテンプレートをテスト環境にデプロイし、自動テストを実行し、エビデンスをキャプチャし、スタックを再び破棄することで、継続的なコストを回避します。

テストは他のビルディングブロックと組み合わせた場合のみに意味を持ちます。例えば、NAT ゲートウェイのテストは、既存の VPC 内でのみ実行できます。代替方法の 1 つとしては、標準的なアーキタイプ 、すなわち典型的なアプリケーションアーキテクチャのための完全なスタックというコンテキスト内でテストを行うことです。

3.5.6 運用ステージへの引き渡し

引き渡しの段階では、クラウド運用チームが新しいビルディングブロックに精通し、サービス固有のオペレーションについてトレーニングを受けることができます。運用チームが新しいビルディングブロックを承認したら、サービスコントロールポリシー (SCP) を変更することでサービスを承認できます。コードテンプレートとしてのインフラストラクチャは、AWS Service Catalog または他の安全なテンプレートリポジトリに追加することで、使用できるようになります。

リスクに対する応答が SCP または監視ルールの変更である場合、これらの変更をデプロイするプロセスはこの段階でトリガーされます。

3.6 コンピュータ化システムバリデーション (CSV)

アプリケーションがクラウドで実行されている場合でも、お客様はコンピュータ化システムバリデーションのアクティビティを実行する必要があります。実際に、本ホワイトペーパーでまとめた総合的なクオリフィケーション戦略により、この CSV プロセスは以前の状態から根本的には変わらず、クラウド技術の導入を通じてアプリケーション開発チームに対する難易度は上昇しないことが保証されています。

しかし、AWS が提供する強固な基盤と統制済みランディングゾーンにより、従来の CSV プロセスの改善に注力することができます。

通常、ソフトウェア開発ライフサイクル (SDLC) が記述された、標準業務手順書 (SOP)が存在します。手順は、多くの場合「GAMP 5: コンピュータ化システムの GxP 適合へのリスクベースアプローチ」に基づいています。一般的な SOP の多くは、数多

くの手作業と承認を伴うため、プロセスの速度が遅くなります。自動化の導入が進むほど、プロセスは速くなり、ヒューマンエラーの可能性も低くなります。

IT プロセスの自動化は決して新しいことではありません。お客様は、オンプレミスの開発を対象に、何年も前から自動化ツールチェーンを導入してきました。クラウドへの移行は、これらすべて同じ機能を提供しますが、特に仮想化インフラストラクチャ分野では、いくつかの追加オポチュニティももたらします。

このセクションでは、主にクラウドを通じて利用可能になったこれらの追加機能について説明します。

3.6.1 据付時適格性評価 (IQ) の自動化

重要なのは、基盤となるビルディングブロックをクオリフィケーションしているにもかかわらず、アプリケーションチームは通常の CSV アクティビティの一環として据付時適格性評価 (IQ) の実行を含んだ、アプリケーションのバリデーションを行う必要があるということです。これにより、インフラストラクチャビルディングブロックのアプリケーション固有の組み合わせがデプロイされ、期待どおりに機能していることを実証します。ただし、各ビルディングブロック自体の機能ではなく、ビルディングブロック間の相互作用のテストに集中できます。

前述のように、開発ツールチェーンの自動化は、高性能なエンジニアリングチームにとっては新しいことではありません。CI/CD と自動テストツールの使用は、長い間存在しています。これまで不可能だったのは、インフラストラクチャのデプロイメントと IQ の手順の実行を完全に自動化することでした。

Infrastructure as Code を使用すると、このブログ記事で説明されているような、IQ ステップ自動化の可能性が開かれます。管理対象のインフラストラクチャテンプレートは、事前承認された仕様として機能します。その仕様は AWS CloudFormation によってデプロイされたスタックと比較することができます。サマリーレポートとテストエビデンスが作成されたり、あるいは差異が見つかったりした場合は、スタックを最新の正常な状態にロールバックできます。

IQ ステップが正常に完了すると、運転時適格性評価(OQ) と性能適格性評価(PQ) の自動化を続行できます。

3.6.2 アプリケーションのクオリフィケーション状態の維持

アプリケーションをデプロイした後は、当然そのアプリケーションを一定の管理状態で維持する必要があります。しかし変更管理、構成管理、セキュリティ管理、バック

アップ、リストアなどの重労働は、統制済みランディングゾーンに組み込まれており、すべてのアプリケーションチームのメリットにつながっています。

4 まとめ

GxP 適合対象のライフサイエンス分野のお客様については、AWS 製品の使用（AWS 製品を使用して開発、バリデーション、運用するアプリケーションや仮想化インフラストラクチャを含む）に対する責任は、お客様側にあります。本ホワイトペーパーの推奨事項を実行することで、お客様の品質システムのコンテキスト内で AWS 製品の使用を評価することが可能となり、GxP コンプライアンスに必要な統制を、規制対象となる製品およびシステムの構成要素として実装するような戦略を検討することができます。

5 寄稿者

本書の寄稿者は下記となります。

- Sylva Krizan PhD, Security Assurance, AWS Global Healthcare and Life Sciences
- Rye Robinson, Solutions Architect, AWS Global Healthcare and Life Sciences
- Ian Sutcliffe, Senior Solutions Architect, AWS Global Healthcare and Life Sciences

6 参考資料

詳細については、下記をご参照ください。

- AWS コンプライアンス
- AWS のヘルスケアとライフサイエンス

7 ドキュメント改訂履歴

日付	説明
2021 年 3 月	AWS の品質システム情報の要素の追加、AWS 上の GxP コンプライアンスに対するお客様のアプローチに関するガイダンスの更新。
2016 年 1 月	初版発行

付録: 21 CFR 11 の統制 – AWS サービスでの使用における責任共有について

21 CFR 11 の規制について、規制対象となる医療製品および GxP システムに対する適用はお客様の責任となり、その適用性はシステムまたは製品の使用意図によって決定されます。AWS 責任共有モデルに基づいてこれらの要件の一部はマッピングされていますが、お客様の規制上の義務を果たす責任は、お客様自身にあります。

以下に、21 CFR 11 の特定のサブパートに対し、その要件を満たすために AWS のサービスと運用、そしてお客様が責任を共有する領域について明確にしました。

21 CFR サブパート	AWS の責任	お客様の責任
11.10. クローズドシステムの管理。クローズドシステムを使用して電子記録を作成、変更、保守、または送信する者は、電子記録の真正性、完全性、および必要に応じて機密性を確保し、署名した記録が真正のものでないと署名者が容易に否認できないように設計された手順および管理を実施しなければならない。手順および管理には、次のものが含まれる。		

11.10(a)正確性、信頼性、意図されたパフォーマンスの一貫性、および無効または変更された記録に対する識別能力について、これらを確保するためのシステムのバリデーションを実施する。	AWS サービスは、SOC、ISO、PCI を含む IT 業界標準に準拠するように構築およびテストされています 。 https://aws.amazon.com/compliance/programs/ AWS が数種類の主要な統制を実装していることは、AWS のコンプライアンスプログラムおよびレポート類により客観的に証明されます。その統制とは、下記を含みますが限定されません : ソフトウェアとハードウェア両方を含む AWS 製品コンポーネントのインストールと運用に関する統制、 製品変更および構成管理の統制 リスク管理プログラム、 管理のレビュー、計画、および運用の監視、 情報の可用性、整合性、機密性に関するセキュリティ管理、 データのバックアップ、リストア、アーカイブのメカニズムを含むデータ保護の統制。 本稼働プロセス内での使用を目的として購入された資材およびサービスはすべて文書化され、使用前の文書レビュー、承認を経て仕様に準拠していることが確認されます。AWS サービスに対しては、一般公開前に最終検査とテストが実施されます。そのリリース前のレビュー手順には、すべての承認データが揃っており、すべての製品要件が満たされていることの確認が含まれます。本稼働が開始されると、AWS サービスのパフォーマンスについて継続的なモニタリングが実施されます。 加えて、AWS 製品が実証された機能を提供していることは、AWS の数多いお客様ベース、政府機関による使用認可や、業界アナリストによる	AWS 製品は、お客様のカスタムソフトウェアアプリケーションや商用オフザシェルフアプリケーション用のプライベートな仮想インフラストラクチャ環境を作成することを可能とする、基本的なビルディングブロックです。このため、お客様のデータやアプリケーション、業界にとって、固有の要件（GxP ソフトウェアバリデーションや GxP インフラストラクチャのクオリフィケーションだけでなく、21 CFR Part 11 の要件をサポートするためのバリデーションなど）を満たすために、AWS 製品を有効化（インストール）、設定、運用する責任は、お客様にあります。 ただし、従来のインフラストラクチャソフトウェア製品とは異なり、AWS 製品は高度に自動化できます。場合によっては手動で実行される紙のプロトコルの代わりに、バージョン管理された JSON [1]スクリプトを使用してクオリフィケーション基準を満たしたインフラストラクチャをプログラムで作成することができます。この自動化機能により労力が削減されるだけでなく、インフラストラクチャ環境の管理と整合性が向上し、継続的なクオリフィケーションが可能になります[2]。 お客様の環境における AWS サービスの据付時適格性評価、運用時適格性評価および性能適格性評価 (IQ/OQ/PQ) は、お客様の責任となります。また、GxP ワークロードで電子記録を管理するシステムについて、意図された用途に適しており規制要件に適合していることを実証するためのバリデーションの実施も、同様にお客様の責任となります。

21 CFR サブパート	AWS の責任	お客様の責任
	主要なクラウドサービスプロバイダーとしての認知度によっても裏付けされています。https://aws.amazon.com/documentation/ 関連する SOC2 共通基準 (CC：Common Criteria): CC1.2、CC1.4、CC3.2、CC7.1、CC7.2、CC7.3、CC7.4	
11.10(b) FDA による査察、レビュー、および複製に適した、人間が読める形式と電子形式の両方で、電子記録の正確かつ完全なコピーを作成することが可能であること。当該電子記録のレビューおよび複製を行う FDA の能力について質問がある場合は、FDA に連絡すること。	統制は業界のベストプラクティスに基づいて実施され、SLA にコミットされたパフォーマンスの期待値通りにサービスが完全かつ正確にアウトプットされることを保証します。 関連する SOC2 共通基準：A1.1	AWS 内でホストされるデータの保護を支援するため、AWS では一連のセキュリティベストプラクティスやその他のリソースを提供しています。(https://aws.amazon.com/security/security-resources/) 最終的にお客様自身が、ご自分の AWS 環境内の電子記録が正確かつ完全であることをバリデーションし、またデータの形式についても、人間や機械により読み取り可能で、かつ規制要件に従った規制当局による検査の対象として適切であるような形式を決定します。

(c)記録の保存期間全体にわたって、記録が正確かつ迅速に取得でるように記録を保護する。	統制は業界のベストプラクティスに基づいて実施され、SLA にコミットされたパフォーマンスの期待値通りにサービスが完全かつ正確にアウトプットされることを保証します。 関連する SOC2 共通基準：A1.1 AWS では、システム停止時にシステムの可用性を維持するため、そしてサービスを復旧するために必要とされる重要なシステムコンポーネントを特定しています。重要なシステムコンポーネントは、アベイラビリティー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、バックアップは維持されます。各アベイラビリティーゾーンは、高い信頼性をもって独立して運用されるように設計されています。重要な AWS システムコンポーネントのバックアップについては、複数のアベイラビリティーゾーン間で正常に複製されているか、監視されます。 AWS SOC 2 レポート CC A1.2 をご参照ください。 AWS レジリエンシープログラムには、AWS が環境内の主要なイベントまたはインシデントを特定し、対応および復旧を行うためのプロセスと手順が網羅されています。このプログラムは、コンティンジェンシー管理による従来のアプローチに基づき構築されており、ビジネス継続性とディザスタリカバリ計画の要素が取り入れられています。また、これを拡張することで、物理的に独立したアベイラビリティーゾーン (AZ) のエンジニアリングや継続的なインフラストラクチャのキャパシティプランニングなど、プロアクティブなリスク軽減戦略の重要な要素も考慮の対象とします。AWS サービスの耐障害性計画は、シニアエグゼクティブマネジメントチームおよび取	AWS 内でホストされるデータの保護を支援するため、AWS では一連のセキュリティベストプラクティスやその他のリソースを提供しています。(https://aws.amazon.com/security/security-resources/) ご自分の環境に適切なセキュリティ設定を実装することでデータの整合性を保護し、適切な権限によってのみデータとリソースが取得されることを保証する責任は、お客様にあります。また、記録保持ポリシー、およびバックアップとリカバリプロセスについても、作成とテストの責任はお客様が負います。 サービスを適切に構成および使用し、お客様のカスタマーコンテンツに対して、適切なセキュリティ、保護、およびバックアップを維持するための独自の措置を講じる責任は、お客様にあります。この措置には、暗号化技術（お客様のコンテンツを不正アクセスから保護するため）および定期的なアーカイブが含まれます。Amazon S3、Amazon Glacier、Amazon RDS などのサービスを、レプリケーションや高可用性の構成で駆使するなど、AWS のバックアップとリストアのための多様なストレージソリューションは、多くのお客様のワークロードに対応するように設計されています。https://aws.amazon.com/backup-recovery/ AWS のサービスは、耐障害設計を可能とするさまざまな機能を提供し、ビジネス継続性の維持を可能とします。たとえば、頻繁なサーバーインスタンスのバックアップやデータの冗長レプリケーション、複数の地理的リージョンや各リージョン内の複数のアベイラビリティーゾーンにまたがってデータを格納する柔軟性などの機能を提供します。よってお客

	締役会の監査委員会によって定期的にレビューされます。 AWS BCP (Business Continuity Plan) では、環境に起因するサービス障害を回避し軽減するための対策が定められています。対策にはイベントの発生前、発生中、発生後に取るべき手順について、運用上の詳細が含まれます。AWS BCP (Business Continuity Plan) 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りサポートされています。AWS は、テスト中およびテスト後に、人とプロセスのパフォーマンス、是正措置、得られた教訓を文書化して、継続的な改善を目指しています。 AWS データセンターは、サービスレベルを維持しながら、障害を予想して耐性を維持するように設計されています。障害発生時には、自動化されたプロセスによって、トラフィックが影響の生じているエリア外へと移動されます。コアアプリケーションは N+1 基準でデプロイされているため、データセンターで障害が発生した場合でも、トラフィックを残りのサイトでロードバランシングできるだけの十分な容量が残ります。 AWS SOC 2 レポート CC3.1、CC3.2、A1.2、A1.3 をご参照ください。	様は、複数のリージョンとアベイラビリティーゾーンの利点を活用するような AWS の使用計画を定める必要があります。 複数のアベイラビリティーゾーンにアプリケーションを分散することで自然災害やシステム障害など、大半の障害モードに対しても耐障害性を維持できます。AWS クラウドは、即座にスケールアップ可能な「パイロットライト」環境から、迅速なフェイルオーバーを可能にする「ホットスタンバイ」環境まで、多くの一般的なディザスタリカバリ (DR) アーキテクチャをサポートしています。DR の計画とテストはお客様自身の責任となります。

(d) システムへのアクセスを、権限の与えられた個人のみに制限すること。	AWS では物理的なセキュリティコントロールおよび論理的なセキュリティコントロールの両方を実施しています。 IT インフラストラクチャのコンポーネントを収容するすべての AWS データセンターに対する物理的なアクセスは、業務を実行するためにアクセスを必要とする、権限を持ったデータセンター従業員、ベンダー、請負業者に制限されます。データセンターへのアクセスを必要とする従業員は、まずアクセスを申請し、有効なビジネス上の理由を提示する必要があります。アクセスの要求は、最小権限の原則に基づいて付与されます。要求のなかで、担当者がデータセンターのどのレイヤーにアクセスする必要があるかが必ず指定され、時間制限が設けられます。要求は権限を持つ担当者によって確認および承認され、要求された時間が経過するとアクセスは取り消されます。 一旦許可されると、その個人は権限で指定されたエリア内の入場のみに制限されます。データセンターへのアクセスは定期的に見直されます。従業員の記録が Amazon の人事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。さらに、承認されたリクエストの期間に基づき従業員または契約者のアクセス権が失効すると、その従業員または契約者が Amazon の従業員であり続ける場合でもアクセス権は取り消されます。 論理的なアクセスについて、AWS は、ビジネス上の必要性と職務上の責任に基づいて、内部の Amazon ネットワークへのユーザーアクセス権限を制限します。AWS では、最小権限の概念を採用しており、ユーザーが職務上の機能を実行するために必要最小限のアクセス	AWS では、お客様自身が AWS サービスを構成および使用することにより、コンテンツの適切なセキュリティ、保護、およびバックアップ体制を維持できるようにしています。サービスには、お客様のコンテンツを不正アクセスから保護するための暗号化技術の使用が含まれます。環境内のデータおよび AWS アカウントへのアクセス設定の確立と検証、そしてデータやリソースへのアクセスの定期的なレビューの実行について、お客様が完全に管理し、責任を負います。AWS リソースへのアクセスを安全にコントロールできるウェブサービス、AWS Identity and Access Management (IAM) を使用して、お客様自身が、データと AWS リソースにアクセスして使用できるユーザー（認証）を管理し、そのユーザーが使用可能なデータとリソース、アクセスの方法（許可）を管理する必要があります。 IAM は、追加料金なしですべての AWS アカウントに提供される機能です。課金は、ユーザーによる他の AWS サービスの使用のみが対象となります。 https://aws.amazon.com/iam/ IAM のベストプラクティスについては、次をご参照ください。 http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html お客様の施設および資産への物理的なアクセスの維持は、お客様のみの責任となります。

	を許可しています。新規ユーザーアカウントは、最小権限のアクセス権を持って作成されます。AWS システムへのユーザーアクセス権限を取得するには、権限を持つ担当者からの承認と、アクティブなユーザーによる認証が必要です。AWS システムへのアクセス権限は、定期的なレビューの対象となります。 従業員がこれらの権限を必要としなくなった場合、その従業員のアクセス権は取り消されます。 AWS の物理的および論理的なセキュリティコントロールを検証するには、AWS SOC 2 レポート C1.2、C1.3、および CC6.1-6.6 をご参照ください。	

(e) セキュリティで保護された、コンピュータ生成タイムスタンプ付きの監査証跡を使用して、電子記録を作成、変更、または削除するようなオペレータの入力やアクションの日時を独立して記録する。記録の変更は、以前に記録された情報を見えづらくしないものとする。このような監査証跡文書は、当該電子記録について定められた期間と同じ期間保持されるものとし、FDA によるレビューおよび複製のために利用可能でなければならない。	AWS では、AWS サービスチームによる内部使用のための、コアログアーカイブ機能を提供する一元化されたリポジトリを維持しています。S3 を活用して高いスケーラビリティ、耐久性および可用性を実現することで、サービスチームは中央ログサービスで、サービスログの収集、アーカイブ、表示を行うことができます。 AWS の本稼働ホストには、セキュリティ目的のログ記録が装備されています。このサービスは、ログオン、失敗したログオン試行、ログオフなど、ホスト上のすべてのユーザーのアクションを記録します。これらのログは、疑わしいセキュリティインシデントが発生した場合の根本原因分析に使用するため、AWS セキュリティチームによって保存されアクセスできるようになっています。特定のホストのログは、そのホストを所有するチームも使用できます。サービスチームは、フロントエンドログ分析ツールを使用して、運用およびセキュリティ分析のためにログを検索することができます。 ログや監査ツールを不正なアクセス、変更、削除から保護するために、プロセスが実装されています。 AWS SOC 2 レポート CC5.1、CC7.1 をご参照ください。	監査証跡の検証と実装、電子記録のバックアップおよび保持の操作は、お客様の責任で行います。 AWS では、お客様がサービスを適切に構成および使用することにより、データのアクセス、使用、および変更 （監査証跡機能の無効化の禁止を含む）に関する適切な監査証跡およびログ記録を維持することが可能です。お客様管理下のログ（後述）は、お客様のデータへの不正な改ざんの監視および検出に使用できます。 AWS CloudTrail、AWS CloudWatch Logs、VPC フローログなどのサービスを使用すると、アカウントで行われた AWS API 呼び出しの履歴を取得でき、クラウド内の AWS データの運用をモニタリングできます。これには、AWS マネジメントコンソール、AWS SDK、コマンドラインツール、およびハイレベルの AWS サービスを経由して行われた API 呼び出しが含まれます。さらに、AWS CloudTrail をサポートするサービスを要求した AWS API 呼び出しについて、実行したユーザー名やアカウント、呼び出し元の IP アドレス、呼び出しの時間を確認することもできます。API を使用して AWS CloudTrail をアプリケーションと統合することや、組織の証跡作成を自動化し、証跡のステータスをチェックすること、管理者がログ機能を有効または無効にする方法を管理することもできます。 AWS CloudTrail は、次の 2 種類のイベントを記録します。 (1) 管理イベント: AWS サービスを対象とした標準 API アクティビティを意味します。たとえば、 AWS CloudTrail は、EC2 インスタン

	スの起動や S3 バケットの作成に係わる API 呼び出しなどの管理イベントを提供します。 (2) データイベント: Get、Put、Delete、List などの、S3 オブジェクトレベルの API アクティビティを意味します。 https://aws.amazon.com/cloudtrail/ https://aws.amazon.com/documentation/cloudtrail/ http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html

21 CFR サブパート	AWS の責任	お客様の責任
(f) 必要に応じてオペレーションシステムチェックを使用し、手順やイベントが所定の順序通りに行われるよう強制すること。	AWS には適用されません。 この要件はお客様のシステムにのみ適用されます。	お客様は、規制対象の環境内でステップおよびイベントが許可された順序通りに実施されるよう、順序付けを設定、確立、検証する責任があります。
(g) 権限チェックを使用し、システムの使用、記録への電子署名、コンピュータシステムの入出力デバイスへのアクセスや操作、記録の変更、現行の操作の実行について、許可された個人のみができるよう確実に制限すること。	AWS には適用されません。 この要件はお客様のシステムにのみ適用されます。	AWS では、お客様自身が AWS のサービスを構成および使用することにより、コンテンツの適切なセキュリティ、保護、およびバックアップ体制を維持できるようにしています。サービスには、お客様のコンテンツを不正アクセスから保護するための暗号化技術の使用が含まれます。環境内のデータおよび AWS アカウントへのアクセス設定の確立と検証、そしてデータやリソースへのアクセスの定期的なレビューの実行について、お客様が完全に管理し、責任を負います。AWS リソースへのアクセスを安全にコントロールできるウェブサービス、AWS Identity and Access Management (IAM) を使用して、お客様自身が、データと AWS リソースにアクセスして使用できるユーザー（認証）を管理し、そのユーザーが使用可能なデータとリソース、アクセスの方法 （許可）を管理する必要があります。 IAM は、追加料金なしですべての AWS アカウントに提供される機能です。課金は、ユーザーによる他の AWS サービスの使用のみが対象となります。 https://aws.amazon.com/iam/ IAM のベストプラクティスについては、次をご参照ください。 http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

21 CFR サブパート	AWS の責任	お客様の責任
(h) 必要に応じて、データ入力や操作指示のソースの有効性を判断するために、デバイス（端末装置など）のチェックを実施する。	AWS には適用されません。 この要件はお客様のシステムにのみ適用されます。	システムへ入力されるデータについて、ソースの有効性を立証し確認する責任は、お客様にあります。これには手動で確認する方法の他に、たとえば統制により使用できる入力デバイスやソースを特定のものに限定するような方法などがあります。
(i)電子記録／電子署名システムを開発、保守、または使用する者が、割り当てられたタスクを実行するために十分な教育および訓練や経験を持っていることの判定。	AWS では、目的、範囲、役割、責任、および管理上のコミットメントをテーマとした、文書化された正式なトレーニングポリシーと手順を実施しています。AWS は毎年継続的に、すべての情報システムユーザーに対してセキュリティ意識トレーニングを実施しています。このポリシーは、Amazon 社内のコミュニケーションポータルを通じて全従業員に周知されます。関連する SOC2 共通基準：CC1.3、CC1.4、CC2.2、CC2.3	お客様の AWS ユーザー（IT スタッフ、開発者、バリデーションスペシャリスト、IT 監査人を含む）に確実に AWS 製品ドキュメントを確認させ、各担当者に適していると判断された製品トレーニングプログラムを修了させる責任は、お客様にあります。AWS 製品はオンラインで、広範囲にわたって文書化されており https://aws.amazon.com/documentation/、入門ラボ、ビデオ、セルフペースオンラインコース、インストラクターによるトレーニング、AWS 認定など、幅広いユーザートレーニングと認定リソースを利用できます。 https://aws.amazon.com/training/ 担当者に対するトレーニングプログラムの妥当性の決定、および人事トレーニングや資格の文書化（研修記録、職務説明、履歴書など）の維持は、お客様の責任となります。
(j) 記録および署名の偽造を防止するために、自らの電子署名の下で実行した行為に対して当該個人に責任を負わせるポリシーを書面により確立し、遵守すること。	AWS には適用されません。 この要件はお客様のシステムにのみ適用されます。	担当者が自ら署名した電子署名の下で実行した行為に対して責任を負わせるためのポリシーの確立と施行（トレーニングおよび関連文書を含む）は、お客様の責任となります。
(k) システム関係のドキュメントに対し、下記を含む適切な管理を実施すること。		

21 CFR サブパート	AWS の責任	お客様の責任
(1) システムの運用とメンテナンス関連のドキュメントについて、配布、アクセス、使用に関する適切な管理。	AWS では、組織内およびサポートする AWS 環境内の、運用と情報セキュリティに関するガイダンスを示す文書化された正式なポリシーと手順を維持しています。ポリシーは、従業員のみがアクセスできる一元化された場所に管理されています。セキュリティポリシーは、セキュリティリーダーシップによって毎年レビューおよび承認され、当社の監査の一環として第三者監査人によって評価されます。 SOC2 共通基準 CC2.2、CC2.3、CC5.3 をご参照ください。	お客様には、システムの運用やメンテナンスに係わる文書および文書システムについて、配布、アクセス、使用に関する独自の統制を確立し、維持する責任があります。

21 CFR サブパート	AWS の責任	お客様の責任
(2) システム関係のドキュメントに対する、作成と変更を時系列で記録した監査証跡を維持するための、改訂および変更管理の手順。	AWS のポリシーと手順は、適切な担当者や管理職メンバーによる一連の承認、バージョン管理、配布のプロセスの対象となります。これらの文書は定期的にレビューされ、必要に応じて裏付けとなるデータも併せて評価され、文書が意図した用途を満たしていることが確認されます。特に指定がない限り、改訂内容はドキュメントを所有するチームによってレビューおよび承認されます。無効または廃止となったドキュメントは特定され、使用対象外となります。内部ポリシーは AWS のリーダーシップにより、少なくとも年に 1 度、もしくは AWS 環境の大幅な変更の後に、レビューおよび承認されます。AWS セキュリティには、該当する場合、Amazon 企業情報セキュリティによって確立され維持されている情報システムのフレームワークとポリシーが活用されます。 AWS サービスのドキュメントは、公開されたオンラインロケーションで管理されているため、デフォルトで最新バージョンを利用できるようになっています。 https://aws.amazon.com/documentation/ AWS SOC 2 レポート CC2.3、 CC3.4、CC6.7、CC8.1 をご参照ください。	AWS アカウント内で実行されているコンピュータ化システムに対する変更は、お客様の責任となります。システムコンポーネントについては、お客様のセキュリティと可用性のコミットメントおよびシステム要件に準拠する形で認証、設計、構成、文書化、テスト、承認、実装を行う必要があります。AWS Config などのサービスを使用することで、AWS リソースのインベントリ、構成履歴、構成変更通知を管理および記録し、セキュリティとガバナンスを実現することが可能です。AWS Config ルールを使用して、AWS Config に記録された AWS リソースの設定を自動で確認するルールを作成することも可能です。 https://aws.amazon.com/documentation/config/ お客様の環境内の変更記録および関連ログは、お客様の記録保持スケジュールに準拠する形で保持することも可能です。 お客様には、電子ドキュメントを AWS アカウント内および全体的な品質管理システムの一部として、保存、管理、追跡する責任があります。これには、システムドキュメントの開発と変更を時系列で記録する監査証跡の維持も含まれます。

21 CFR サブパート	AWS の責任	お客様の責任
§11.30 オープンシステムの管理。 **オープンシステムを使用して電子記録を作成、変更、保守、または伝送する個人は、電子記録の作成時点から受領時点を通しての電子記録の真正性、完全性、および必要に応じて機密性を保証するように設計された手順および管理を実施しなければならない。これらの手順および管理には、必要に応じて§11.10で指定されたものに加え、文書の暗号化および適切なデジタル署名に係わる基準の使用など、追加の方策が含まれ、記録の真正性、完全性、機密性を状況に応じて適切に確保するものとする。**	お客様のデータの真正性、完全性、機密性を保護し、維持するために、業界標準の統制と手順を実施しています。 AWS SOC 2 レポート C1.1-C1.2 をご参照ください。	お客様の環境内で AWS サービスの使用がオープンシステムまたはクローズドシステムの定義のどちらに合致しているか、そしてこれらの要件が適用されるか否かを判断する責任は、お客様にあります。推奨される手順と統制の詳細については、上記§11.10 内の責任の記載をご参照ください。データの完全性、真正性、機密性を維持するための、ドキュメントの暗号化や適切なデジタル署名の基準の使用など、追加措置についてはお客様の責任となります。
§11.50 署名の明示。 **(a) 署名された電子記録には、署名に関連する以下の全ての情報が明確に示されるものとする。** **(1) 活字体による署名者の氏名。** **(2) 署名が実施された日時。** **(3) その署名が意味する内容（レビュー、承認、責任、作成など）。** **(b) 本セクションの上記(a)(1)、(a)(2)、(a)(3)に記載された事項については、電子記録と同様の管理が適用され、人間が読める電子記録の形式（電子表示や印刷出力など）の一部として含まれていなければならない。**	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様は、お使いのアプリケーションが指定の署名済みの電子記録要件を満たしていることを確定し、確認する責任があります。

21 CFR サブパート	AWS の責任	お客様の責任
§11.70 署名と記録のリンク付け **電子記録上に執行された電子署名および手書きの署名はそれぞれの電子記録にリンク付けし、一般的な手段により電子記録を偽造する目的で署名を削除、複製、またはその他の方法で移管できないようにする。**	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様は、お客様のアプリケーションやシステムが、指定の署名-電子記録間リンク付けの要件を満たしていることを確定し、確認する責任があります。これには、必要なポリシー及び手順が含まれます。
サブパート C - 電子署名 **§11.100 一般的な要件。** **(a) 各電子署名は、一個人に固有のものとし、他の者に再利用させたり、再割り当てたりしてはならない。**	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様は、お客様のアプリケーションやシステムが、指定の一般的な署名要件を満たしていることを確定し、確認する責任があります。これには、電子署名のガバナンスを強制するために必要なポリシーおよび手順が含まれます。
(b)個人の電子署名または電子署名のいかなる要素についても、組織が設定、割り当て、認証、またはその他の方法で認可する際は、事前に当該個人の本人確認を行わなければならない。	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様は、お客様のアプリケーションやシステムが、指定の一般的な署名要件を満たしていることを確定し、確認する責任があります。これには、電子署名の使用前に個人の ID を検証するために必要なポリシーおよび手順が含まれます。

21 CFR サブパート	AWS の責任	お客様の責任
(c) 電子署名を使用する者は、システム内の電子署名で 1997 年 8 月 20 日以降に使用されているものについては、従来の手書き署名と同等の法的拘束力を有するものとして意図されている旨、その使用前または使用時に FDA に証明しなければならない。 **(1) その証明書は、従来の手書き署名入りの紙の文書として、Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857 宛に提出すること。** **(2) 電子署名を使用する者は、FDA からの要請があった場合、特定の電子署名がその署名者の手書き署名と同等の法的拘束力を有する旨、追加の証明または証言を提供すること。**	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様は、お客様のアプリケーションやシステムが、指定の一般的な電子署名要件を満たしていることを確定し、確認する責任があります。これには、FDA への定められた通知が必要かどうかの判断と、それに応じた文書化が含まれます。
§11.200 電子署名の構成要素と管理。		
(a) バイオメトリクスに基づかない電子署名については、下記が適用される。	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	

21 CFR サブパート	AWS の責任	お客様の責任
(1) 識別コードとパスワードなど、少なくとも 2 つの識別要素を使用する。 **(i) ある個人が、管理環境下での単一のシステムアクセスが維持された状態で一連の署名を実行する場合、最初の署名はすべての電子署名要素を使用して実行され、その後の署名は、少なくとも 1 つの電子署名要素を使用して実行される。その要素は、個人によってのみ行使・使用されるように設計されたものとする。** **(ii) ある個人が、管理環境下での単一のシステムアクセスが維持された状態ではない状態で、１回以上のシステムアクセスを実行する場合、各署名の度に、すべての電子署名要素を使用し実行しなければならない。** **(2) 電子署名は真の所有者によってのみ使用されるものとする。** **(3) 真の所有者以外の者によって個人の電子署名の使用が試みられる場合、必ず 2 人以上による共同作業が必要となるよう、管理、運用すること。**		お客様には、お客様のアプリケーションやシステムが、指定の電子署名の構成要素および管理要件を満たしていることを確定し、確認する責任があります。これには、識別構成要素の使用方法や、真の所有者による使用方法の確立が含まれます。
(b) バイオメトリクスに基づく電子署名は、真の所有者以外は絶対に使用できないように設計すること。	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様には、お客様のアプリケーションやシステムが、指定の電子署名の構成要素および管理要件を満たしていることを確定し、確認する責任があります。これには、真の所有者による使用方法の確立が含まれます。

21 CFR サブパート	AWS の責任	お客様の責任
§11.300 ID コードとパスワードの管理 **パスワードと ID コードの組み合わせに基づいて電子署名を使用する者は、そのセキュリティと完全性を保証するための管理を導入しなければならない。その管理には下記が含まれる。**		
(a) 各 ID コードとパスワードの組み合わせについて、一意性を確保し、複数の個人が同一の ID コードとパスワードの組み合わせを持つことがないようにする。	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様には、お客様のアプリケーションやシステムが、指定の電子署名の構成要素および管理要件を満たしていることを確定し、確認する責任があります。これには、パスワードと ID コードの組み合わせの一意性を確保する手順と管理の確立が含まれます。
(b) ID コードとパスワードの発行について、必ず定期的なチェック、取り消し、または改訂を行う（例:パスワードエージングなどの事象に対応するため）。	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様には、お客様のアプリケーションやシステムが、指定の電子署名の構成要素および管理要件を満たしていることを確定し、確認する責任があります。これには、パスワード発行の定期的な見直しのための手順と管理の確立が含まれます。
(c)紛失、盗難、行方不明、またはその他完全でない状態にあるかもしれないトークンやカード、そして識別コードやパスワード情報を付与、生成するその他のデバイス類については、紛失管理手順に従い電子的に無効とし、適切かつ厳格な管理の下、一時的または永久的な代替品を発行する。	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様には、お客様のアプリケーションやシステムが、指定の電子署名の構成要素および管理要件を満たしていることを確定し、確認する責任があります。これには、ID コードやパスワードを生成するデバイスで障害があるものについての、紛失管理の手順と管理の確立が含まれます。

21 CFR サブパート	AWS の責任	お客様の責任
(d) トランザクションセーフガードを使用してパスワードおよび/または識別コードの不正使用を防止し、また不正使用の試みがあったときは迅速に検出するとともに早急にシステムセキュリティ担当部署に報告し、必要に応じて組織の管理者にも報告する。	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様には、お客様のアプリケーションやシステムが、指定の電子署名の構成要素および管理要件を満たしていることを確定し、確認する責任があります。これには、ID コードやパスワードの不正使用を防止、検出、報告するための手順および管理の確立が含まれます。
(e) トークンやカードなどの、識別コードやパスワード情報を保持、生成するデバイスに対して、初期テストや定期的なテストを実施し、デバイスが正しく機能し、不正に変更されていないことを確認する。	AWS には適用されません。 この要件はお客様のアプリケーションにのみ適用されます。	お客様には、お客様のアプリケーションやシステムが、指定の電子署名の構成要素および管理要件を満たしていることを確定し、確認する責任があります。これには、ID コードまたはパスワードを生成するデバイスが適切に機能することを定期的にテストするための手順と管理の確立が含まれます。

[1] コンピューティングにおいて、JSON (JavaScript Object Notation) は AWS CloudFormation テンプレートに使用されるオープンスタンダード構文です。https://aws.amazon.com/documentation/cloudformation/

[2] https://www.continuousvalidation.com/what-is-continuous-validation/