AWS 製品を
GxP 関連システムにおいて
使用する際の考慮事項

2016 年 1 月

注意

本書は情報提供のみを目的としています。本書は、発行時点における AWS の現行製品と慣行を表したものであり、それらは予告なく変更されることがあります。お客様は本文書の情報および AWS 製品の使用について独自に評価する責任を負うものとします。これらの情報は、明示または黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されるものです。本文書内のいかなるものも、AWS、その関係者、サプライヤ、またはライセンサーからの保証、表明、契約的なコミットメント、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間の契約に属するものではなく、また、当該契約が本文書によって修正されることもありません。

目次

1 要約

アマゾン ウェブ サービス（AWS）は 2006 年に、今ではクラウドコンピューティングとして広く知られている、ウェブサービスの形でのお客様への IT インフラストラクチャ製品の提供を開始しました。AWS は現在、世界中の 190 か国で数十万社もの企業に利用されている、信頼性が高くスケーラブルで低コストなインフラストラクチャプラットフォームを提供します。クラウドコンピューティングの主な利点の 1 つは、先行投資となるインフラストラクチャ費用を、使用量に合わせて増減する低額の変動費に移行し、お客様にとって重要な活動に費やす時間を増やす一方で、ビジネス上の差別化に直結しない IT タスクに費やす時間を減らせることにあります。

お客様は、クラウドを利用することで、物理的なデバイスなどの 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す。その代わりに、統制の観点では整合性を高め、手動操作のエラーを減らしながら、さらに迅速に結果を生み出すことのできる、自動化されたデプロイツールや手法を使用して、数百または数千の仮想マシンを瞬時に起動することも可能となります。Good Laboratory、Clinical、または Manufacturing Practices（GxP）のコンプライアンス要件を持つ企業とその監査人が AWS 製品の利点を活用するためには、新しいスキルを取得し、IT コンプライアンスをさらに迅速化、自動化し、セキュリティ志向にするため GxP ポリシーや手順の変更を検討する必要があります。

このホワイトペーパーでは、GxP での AWS 製品の使用に関するガイダンスを示します。この内容は、検証済みの 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。内容の適正性を確実にするため、AWS は追加のステップとして Lachman Consultant Services Inc.（Lachman Consultants）と連携して、このホワイトペーパーで概説されている手法を確認しました。Lachman Consultants は、FDA および 今日の製薬業界および医療機器業界に影響を及ぼす国際的な法規制の順守に関連して、最も評判の高いコンサルティング会社の 1 社です。Lachman Consultants はクラウド環境での規制対象データを維持するためのサポートに関する GxP のガイドラインを含めて、特に GxP システムの確立と開発に関連する事項において豊富な経験を持っています。Lachman Consultants の詳細については、www.lachmanconsultants.com を参照してください。

ただし、AWS 製品を使用する際に、現在の IT、ソフトウェア、およびセキュリティ手法がお客様の GxP ポリシーと手順に関して適格であることを確認するためには、引き続きお客様のアドバイザーにご相談ください。

2 はじめに

アマゾン ウェブ サービス（AWS）は、クラウドインフラストラクチャソフトウェア製品を提供していますが、事実上、世界中のあらゆる業界で重要なワークロードや規制対象のワークロードを保存、処理するために使用が増加しています。ヘルスケアおよびライフサイエンスの企業

は AWS クラウドの利点を理解し、規制対象 IT システムのコンポーネントとして AWS 製品を活用しています。これには、医療機器、製薬、生物製剤、およびその他の食品および医療製品業界における Good Laboratory Practices、Good Clinical Practices、Good Manufacturing Practices (″GxP″) をサポートする、コンピュータ化システムも含まれています。

このドキュメントでは、AWS 製品を使用して一般的な GxP のコンプライアンス事項およびデータの完全性の考慮事項に関連し、電子記録を保存または処理するコンピュータ化システムを構築したいと考えているお客様に役立つ情報を示します。

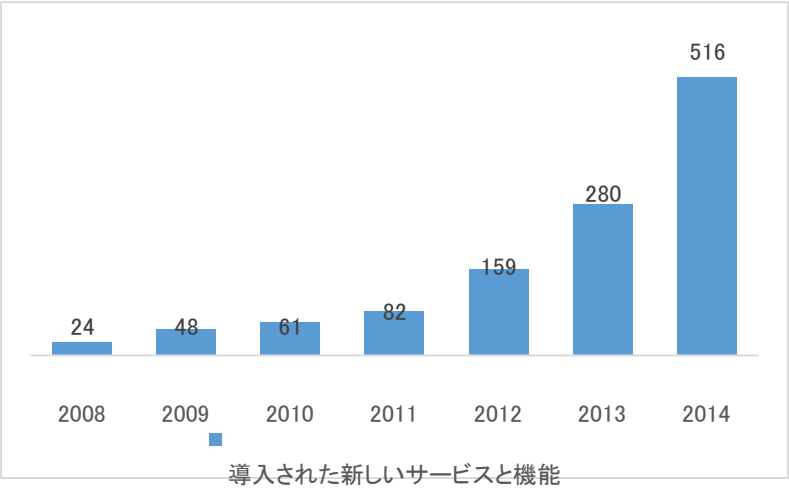
こういった情報は以下の主な点について、お客様の理解を促進するものとなっています。

- AWS 製品の対象と技術的な基本事項。
- AWS の商用クラウド製品を使用する際に、お客様が検討する必要性のある品質システムに関する考慮事項。
- AWS 製品をコンポーネントとして組み込んだ GxP システムを開発、検証、運用するお客様向けの、システム開発ライフサイクルに関する考慮事項。
- システム関連情報を規制機関に提出または提供する可能性があるお客様向けの、規制項目に関する考慮事項。

AWS 製品、プライバシー、およびデータ保護に関する考慮事項の詳細が記載されたホワイトペーパーは、https://aws.amazon.com/jp/compliance/ で参照できます。

2.1.1 AWS について

Amazon.com (NYSE: AMZN) によって 2006 年に設立されたアマゾン ウェブ サービスは、米国、オーストラリア、ブラジル、中国、ドイツ、アイルランド、日本、韓国、およびシンガポールにあるデータセンターからインターネット経由でオンデマンドで届けられる、サブスクリプション型の多様なインフラストラクチャ製品を提供する、定評のあるクラウドサービスプロバイダーです。AWS は、創業以来、お客様に迅速に新製品をお届けし、幾度にもお客様のフィードバックに基づいてそれらの製品を素早く改善するといった取り組みを実践し、クラウドコンピューティングそのものを定義する革新的な存在として位置付けられてきました。こうした革新のペースとサービスの継続的な改善は、より多くの企業がミッションクリティカルなシステムに AWS 製品の使用を選択している主な理由となっております。



お客様重視とお客様の信頼獲得は、アマゾンの文化を特徴づける重要なリーダーシッププリンシプルの一つです。お客様は AWS 製品の使用に際して、お客様のデータおよびお客様が AWS 上に構築したシステムの所有権と管理を維持し、AWS は現在のプライバシーおよびデータ保護フレームワークに従って、AWS インフラストラクチャに関する保証と透明性をお客様に提供するべく尽力します。このような事に関する詳細については、データのプライバシーに関する付録 (31 ページ) を参照してください。

- AMZN 企業情報: http://phx.corporate-ir.net/phoenix.zhtml
- リーダーシッププリンシプル: http://www.amazon.jobs/principles
- アナリストレポート: https://aws.amazon.com/resources/analyst-reports/

2.1.2 AWS のお客様

AWS は 190 か国に 100 万社を超えるアクティブなお客様を持っています。これには、オーナーが操業する創業直後の会社や小規模ビジネスから、世界的なエンタープライズや政府機関まで、事実上あらゆる業種や種類の組織が含まれます。お客様の組織内での AWS 製品の主なユーザーは、組織の IT インフラストラクチャおよびアプリケーションを構築、維持するソフトウェア開発者、ネットワークエンジニア、およびシステム管理者です。AWS は、AWS 製品を使用することにより恩恵を受けている幅広い業界と市場を含む、お客様の成功事例の包括的な一覧を提供しています (https://aws.amazon.com/solutions/case-studies/all/)。

ヘルスケアとライフサイエンス企業は、コンピュータ化されたシステムで AWS 製品を使用している、これらの企業の一部であり、AWS ヘルスウェブサイト (https://aws.amazon.com/health/) で、その事例の一部を紹介しています。

2.1.3 AWS のテクノロジー

アマゾン ウェブ サービス (AWS) は、すべての AWS 製品に組み込まれたコアテクノロジー、すなわちウェブサービス、にちなんで名付けられました。ウェブサービスは自己完結型で再利用可能なソフトウェアモジュールであり、XML[1] や JSON[2] などの標準化されたメッセージング形式を使用し、インターネットプロトコルを介して他のソフトウェアモジュールに対して機能を利用できるようにします。自己サービス管理コンソール (https://aws.amazon.com/account/) を通じてすべてオンラインで利用できる AWS 製品は、2 種類のウェブサービスに基づいており、それぞれに複数のタイプのインターフェイスがあります。

ウェブサービスのタイプ:

- Simple Object Access Protocol (SOAP)
- Representational State Transfer (REST)

AWS 製品インターフェイス:

- アプリケーションプログラミングインターフェイス (API)
- コマンドラインインターフェイス (CLI)
- グラフィカルユーザーインターフェイス (GUI)

[1] eXtensible Markup Language
[2] JavaScript Object Notation

ウェブサービスは 1 つのオペレーティングシステムやプログラミング言語には結び付けられるものではありません。異なるプログラミング言語で記述され、異なるプラットフォームで実行されているアプリケーションが、各ウェブサービスインターフェイスでサポートされている事前に定義されたアクションを使用して、インターネット (またはイントラネット) 経由でシームレスにデータを交換することができます。ウェブサービス・アプローチ (ウェブ志向アーキテクチャとも呼ばれます) の主要な利点は、ウェブサービスを使用するソフトウェアアプリケーションが、ウェブサービスの構築方法や、基になるデータが保存される方法そのものについては知る必要がなく、ウェブサービスインターフェイスが応答するアクションについて知り、それに注力するだけでよいことにあります。あるインターフェイスにおいて、特定のアクションが利用できる限り、ウェブサービスのベースとなっているコンポーネントへの変更または新しいアクションの追加は、アプリケーションそのものの動作または信頼性に影響を与えることはありません。AWS 製品でサポートされるウェブサービスアクションのリストは、完全にオンラインで文書化されています (https://aws.amazon.com/documentation/)。

仮想化やソフトウェア・デファインド・ネットワーク (Software Defined Network, SDN) などのソフトウェア定義インフラストラクチャテクノロジーは、ウェブサービステクノロジーに加えて、AWS 製品の主要な構成要素となっています。ネットワークロードバランサーやファイアウォールなど、以前は特殊な物理機器としてのみ利用できたインフラストラクチャコンポーネントは、現在ではオンデマンドのソフトウェア定義リソースとして利用できます。これにより、システム開発のタイムラインや費用が減り、ソフトウェアの自動化を通じてより高度なレベルのインフラストラク

チャ自体の標準化と管理が可能になります。

これまでのような物理的なインフラストラクチャコンポーネントそのものを包含してしまう、ソフトウェア・インフラストラクチャの拡張、ウェブ志向アーキテクチャ、最新のプログラミング手法の利点を組み合わせることで、IT の SDLC[3]、スタッフのスキル、および IT のコンプライアンスにおけるグローバルレベルでの変遷は様々な業種で推進されています。GxP システムで AWS 製品を最大限活用するための準備をしている企業は、このような変化を認識し、これに適応していこうとする企業となっています。

[3] システム開発ライフサイクル

AWS テクノロジーのメリット:

- **プラットフォームの独立性と相互運用性**: AWS 製品は多くのプログラミング言語で書かれたアプリケーションをサポートし、アプリケーションを特定のオペレーティングシステムまたはハードウェアコンポーネントに制限することはありません。
- **スケーラビリティ**: AWS 製品によるソフトウェア定義のインフラストラクチャを最新のプログラミング手法と組み合わせることで、AWS のお客様はコンピュータ化されたシステムを設計し、システムの実際の要求に応じて、迅速にリソース（およびそのコスト）を拡大または縮小できます。
- **耐障害性**: AWS 製品は AWS 製品とソフトウェアアプリケーション間の疎結合をサポートします。これにより、システムコンポーネントまたは AWS 製品が一時的に利用できなくなった場合でも、お客様は GxP システムを構築して正しく運用を継続することができます。
- **責任範囲の分離** 従来お客様がもっていた物理的なインフラストラクチャに関する責任と、仮想インフラストラクチャおよびソフトウェアに関する責任とを完全に分離されることで、GxP データへのアクセスという観点においても、物理的なアクセスと論理アクセスが分離されることになるため、重要なデータに対して、完全性に関する統制がもたらされることになります。
- **監査性**: ウェブサービスのメッセージベースの相互運用性により、AWS 製品のお客様による設定と使用を一様にログに記録、モニタリング、監査することができます。
- **コアコンピテンシーの重視**: AWS 製品の究極の利点は、お客様のビジネス上の差別化につながらないタスクを実行する時間を減らし、お客様にとって真に価値のあるタスクに多くの時間を注力可能なことにあります。

2.1.4 AWS 製品

AWS は、ユーザー設定が可能で、汎用性を持ち、ISO、NIST、SOC などの商用 IT 標準を満たす商用クラウドインフラストラクチャソフトウェア製品やオフィス生産性アプリケーションを作成しています。これはデータベースエンジン、オペレーティングシステム、プログラミング言語、イン

ターネットサービスプロバイダーなど、その他の汎用的な IT 製品やサービスと同様です。多くの組織は AWS 製品を COTS (commercial-off-the-shelf) インフラストラクチャソフトウェア製品と分類しており、これは FedRAMP と呼ばれる連邦調達プログラムを通じた米国連邦政府の COTS 項目としての AWS 製品の使用と一貫性のある概念となっています。米国の FAR (Federal Acquisition Regulation) による定義を継承する FedRAMP では、COTS アイテムは次のように定義されます。1) 確立されたカタログに基づき、商業マーケットプレイスにおいて相当な数量が競争力を持って提供、販売されている製品またはサービス、2) 変更またはカスタマイズなしに提供されている、3) 標準的な商業条件に基づいて提供されている。GxP 要件を持つ AWS のお客様は、Good Automated Manufacturing Practices (GAMP) のカテゴリ 1、規制対象の GxP 環境のコンピュータ化されたシステム用の Pharmaceutical Inspection Co-operation Scheme (PIC/S) ガイド、医療機器品質フレームワーク、Software of Unknown Provenance (SOUP) "ブラックボックス" OTS コンポーネント、または汎用コンピューティングリソースなど該当する業界毎の指定された名称によって AWS 製品を分類する責任があります。

AWS はいくつかのグループに分類される 50 以上の製品を提供しています。

グループ	AWS 製品
コンピューティング	Amazon EC2、Amazon EC2 Container Service、AWS Elastic Beanstalk、AWS Lambda、Auto Scaling
ストレージ	Amazon S3、Amazon CloudFront、Amazon EBS、Amazon EFS、Amazon Glacier、AWS Storage Gateway、AWS Snowball
データベース	Amazon RDS、Amazon DynamoDB、Amazon ElastiCache、Amazon Redshift
ネットワーキング	Amazon VPC、AWS Direct Connect、Elastic Load Balancing、Amazon Route 53
開発者用ツール	AWS CodeCommit、AWS CodePipeline、AWS CodeDeploy、AWS Tools & SDKs
管理ツール	Amazon CloudWatch、AWS CloudFormation、AWS CloudTrail、AWS Config、AWS Management Console、AWS OpsWorks、AWS Service Catalog、Trusted Advisor、AWS Tools for Windows PowerShell

分析	Amazon EMR、AWS Data Pipeline、Amazon Elastisearch Service、Amazon Kinesis、Amazon Kinesis Firehose、Amazon Machine Learning、Amazon QuickSight
モバイルおよび Internet of Things (IoT)	AWS IoT、AWS Mobile Hub、Amazon API Gateway、Amazon Cognito、AWS Device Farm、Amazon Mobile Analytics、AWS Mobile SDKs、Amazon SNS
アプリケーションサービス	Amazon API Gateway、Amazon AppStream、Amazon CloudSearch、Amazon Elastic Transcoder、Amazon FPS、Amazon SES、Amazon、SNS、Amazon SQS、Amazon SWF
エンタープライズ生産性アプリケーション	Amazon WorkSpaces、Amazon WAM、Amazon WorkDocs、Amazon WorkMail
セキュリティと識別	Identity & Access Management、AWS Directory Service、Amazon Inspector、AWS CloudHSM、AWS KMS、AWS WAF

AWS 製品、グローバルインフラストラクチャ、およびお客様のサインアップの詳細と仕様は、オンラインで参照できます。

- https://aws.amazon.com/account/
- https://aws.amazon.com/products/
- https://aws.amazon.com/documentation/
- https://aws.amazon.com/about-aws/global-infrastructure/

3 GXP システムでの AWS 製品の使用

AWS 製品の提供モデルは、物理的なオンプレミス製品ではなく、オンラインによって提供される仮想的な製品ですが、それらを GxP システムでコンポーネントとして使用する責任は同様です。この確立されたモデルにおいて、GxP システムで商用インフラストラクチャ製品をコンポーネントとして設定、使用するお客様は、いくつかの主要な領域で責任を持ちます。

- 品質システム
- システム開発ライフサイクル
- 規制関連事項・業務

3.1 品質システム

GxP システムにおいて AWS 製品を活用しようとする企業は、自社の品質システムに関するドキュメントを確認および更新する必要があります。このセクションでは、検討対象となるいくつかの主要な領域について説明します。

3.1.1 マネジメントの責任

本番稼働 GxP システムで AWS 製品を使用する前に、AWS アカウントの作成とメンテナンスの管理方法を検討する必要があります。AWS アカウントの作成はセルフサービスであり、アカウントの作成者には AWS 製品の設定とアクセス制御のフルコントロールのルートアカウント認証情報が付与されます。このため、お客様の組織内で業務遂行に責任を持つ経営陣は、AWS アカウントのガバナンスポリシーを定義して伝達し、GxP システムで使用されるアカウントが追跡されるようにするとともに、ルートアカウントの認証情報が、組織で許可された適切な人物によって管理されるようにする必要があります。さらに、AWS アカウントにパスワードポリシーを適用して、すべてのアカウントユーザーがパスワードを定期的に更新するように要求します。

お客様は、次のドキュメントを更新することを考慮にいれ、GxP システムでの AWS 製品の使用をサポートする必要があります。

- AWS アカウントのガバナンスポリシー
- 組織での購買権を持つすべてのスタッフへのメモ
- AWS アカウントの作成手順
- AWS アカウントのユーザーパスワードポリシー

3.1.2 人員

AWS のお客様は、従業員が割り当てられた職務を実行するための教育やトレーニングを受

け、経験を持っていることを確認する必要があります。職務に GxP システムでの AWS 製品の使用が含まれる場合、従業員の雇用または研修時に、AWS 製品の経験レベルを考慮する必要があります。実行されるシステムアクセスと職務のレベルは、必要な経験レベルの決定に関連し、それによって影響を受ける可能性のある職務が数多くあります。

- ソフトウェアエンジニア
- ソフトウェアテスター
- ネットワークエンジニア
- システム管理者
- セキュリティエンジニア
- 検証エンジニア
- 購買スタッフ
- 品質保証スタッフ
- 監査人

注意: 一般的に、GxP アプリケーションのエンドユーザーは直接 AWS 製品を操作せず、AWS 固有のトレーニングを必要としません。

たとえば、トレーニングは認知度向上のためのトレーニング、トレーニングの内容自体、またはテストベースの従業員の資格要件、等で構成されます。AWS および Amazon パートナーネットワーク（APN）が、次のものを含む、AWS 製品の初期的および継続的な多くのトレーニングと認定を提供しています。

- オンラインドキュメント: https://aws.amazon.com/documentation/
- 講習動画: https://aws.amazon.com/training/intro_series/
- セルフペースラボ: https://aws.amazon.com/training/self-paced-labs/
- イベントとオンラインセミナー: https://aws.amazon.com/about-aws/events/
- クラスとワークショップ: https://aws.amazon.com/training/course-descriptions/
- パートナートレーニング: https://aws.amazon.com/partners/training/
- プロフェッショナル認定: https://aws.amazon.com/certification/

お客様は、次のドキュメントを更新して、GxP システムでの AWS 製品の使用をサポートする必要があります。

- トレーニングプランと手順
- 職務の説明
- 求職、経歴書、履歴書
- トレーニング記録
- AWS 製品の認定

3.1.3 監査

GxP システムでの AWS 製品の使用を監査するお客様にとって、システムセキュリティとデータの完全性に係る統制、および SDLC の継続的な効果を評価することは重要です。AWS 製品の使用の効果的な監査を実行するには、IT 監査人はウェブサービステクノロジー、AWS 製品、JSON などの基本的なスクリプトの読み取りに精通する必要があります。監査人は、読み取り専用アクセスポリシーを通じて該当する AWS アカウントリソースに直接アクセスできることが理想的です。AWS アカウント内で、監査人と査定人は、次のような該当する製品機能設定とログデータを確認する必要があります。

- AWS アカウント認証情報
- 組織内の各種連絡先
- IAM ユーザー、グループ、ロール
- SAML および OpenID Connect 用 IAM プロバイダー
- Amazon EC2 セキュリティ設定
- S3 など、他のサービスでのリソースに基づくポリシー
- AWS Config ルール
- CloudTrail のシステムアクティビティログ
- AWS Config の変更履歴
- システムサポートケースの履歴

AWS では、GxP システムでの AWS 製品の使用の監査を準備中の監査人を支援するため、さまざまな監査ツールおよび教育リソースを用意しています。

- AWS 監査のホワイトペーパー: https://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf
- AWS 運用チェックリストのホワイトペーパー: https://s3.amazonaws.com/awsmedia/AWS_Operational_Checklists.pdf
- AWS セキュリティ監査のガイドライン: https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html
- AWS CloudTrail 製品ページ: https://aws.amazon.com/cloudtrail/
- AWS Config 製品ページ: https://aws.amazon.com/config/
- AWS Trusted Advisor ページ: https://aws.amazon.com/premiumsupport/trustedadvisor/
- セルフペース監査の qwikLAB: https://www.qwiklab.com/focuses/preview/1250?locale=en
- 実地監査人トレーニング: awsauditttraining@amazon.com

お客様は、次のドキュメントを更新して、GxP システムでの AWS 製品の使用をサポートする必要があります。

- IT 監査スケジュール
- AWS アカウントの監査手順とチェックリスト
- AWS アカウント監査レポート
- AWS 製品に関する IT 監査人の資格、履歴書、トレーニング記録

3.1.4 購入管理

従来の IT インフラストラクチャ製品の購入では、資本支出と記帳される物理的な物品に対する発注書 (Purchase Order, PO) 処理が行われます。しかし、AWS 製品の購入では、変動費として記帳されるサブスクリプションソフトウェア製品用の、公共料金支払いのような請求処理が必要になります。多くのライフサイエンス関連企業は、AWS のようなサブスクリプションによる従量制の価格モデルに対応しない可能性のある発注処理用に作成された GxP 製品に関する購入手順を保持しています。

従来の PO を使用したインフラストラクチャの購入

1. IT 部門がサーバー要件を指定
2. IT 部門が、要件に一致するサーバーと OS を特定
3. IT 部門が購買部門にリクエストを提出
4. 購買部門がサプライヤに PO を送付
5. サプライヤがサーバーを出荷
6. 資材部門が出荷品を受け入れ
7. IT 部門がサーバーと OS をインストール
8. IT 部門が OS を設定
9. IT 部門が手動でサーバーと OS を適合
10. 経理部門が支払いを行い、ハードウェア資産を資本支出として減価償却

AWS を使用したインフラストラクチャ購入プロセス

1. IT 部門がサーバー要件を指定
2. IT 部門が、要件に一致する EC2 インスタンスタイプを選択し、独自の適格な OS イメージを提供
3. IT 部門が適格なイメージを使用し、自動ログを有効にして EC2 インスタンスを起動
4. IT 部門が運用コスト用のクレジットカードを使用して EC2 の使用量を支払う

GxP システムで AWS 製品を使用するお客様は、IT に係る購入、発注手順を確認し、サブスクリプション価格とオンラインによる提供モデルに対応できるかどうかを確認する必要があります。この確認では、IT 部門、購買、および品質保証の各チームが関与し、発注、受入、および支払い、AWS アカウントの管理等に対応必要があります。AWS では、AWS アカウントの請求の理解と管理について支援させていただくドキュメントを用意しています。

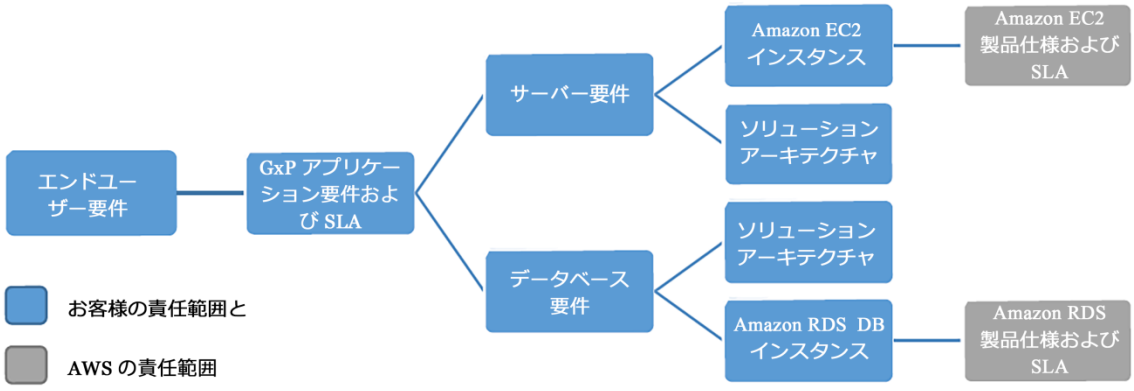
- AWS 請求およびコスト管理のホワイトペーパー: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf
- 請求明細レポートで使用量を理解する: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/detailed-billing-reports.html
- AWS 簡易見積りツール http://calculator.s3.amazonaws.com/index.html

お客様は、次のドキュメントを更新して、GxP システムでの AWS 製品の使用をサポートする必要があります。

- 購入手順
- AWS 請求明細レポート
- E メールによる PDF 版請求書

3.1.5 製品アセスメント

購入した物品やサービスが、指定した要件に一致するかどうかを確認することが、GxP 管理の主要な要件です。AWS 製品のような商業的に利用可能なインフラストラクチャコンポーネントの場合、製品仕様がユーザー要件に一致するかどうかの確認は単純です。これは、すべての AWS 製品インターフェイスの仕様と契約が完全に文書化され、お客様がご自身で確認可能なためです。AWS は個別のお客様向けに AWS 製品または SLA をカスタマイズしないため、お客様は GxP アプリケーションの要件に対応する AWS 製品の仕様および SLA を確認し、単純にマッピングすることになります。たとえば、AWS の Amazon EC2 製品および Amazon RDS 製品を使用して、構成可能な COTS ソフトウェアアプリケーションの実行を希望するお客様は、最初にアプリケーションのサーバー要件（CPU、メモリなど）とデータベース要件を文書化し、次に Amazon EC2 および Amazon RDS 製品ページに移動して、アプリケーション要件を満たす仮想サーバーファミリー（EC2 インスタンスタイプ）およびデータベースタイプ（DB インスタンスタイプ）を特定します。



GxP システムにおける SLA の概念 と、個別の AWS 製品 の SLA の役割が直結するものではないことに注目してください。GxP システムの SLA はお客様による AWS 製品の設定および使用 (つまりソリューションアーキテクチャ) をも含んで考慮されるものです。たとえば、GxP アプリケーションに、個別の単品の AWS 製品で提供されるよりも高いレベルの可用性が必要な場合、お客様は個別のソリューションを構成して、その高いレベルの可用性を達成することも可能です。よって、特定の GxP システムに対して AWS 製品の適合性を評価する場合、AWS 製品個別の検討ではなく、ソリューションアーキテクチャ全体を考慮する必要があります。

カスタム (GAMP カテゴリ 5) アプリケーションまたは医療機器に対して AWS 製品を評価する場合、製品アセスメントにおいて、システムコンテキスト、可能性のあるアーキテクチャと設計、および利用可能な AWS 製品等について、SDLC の計画フェーズ中に同時に調査していく必要があります。AWS 製品がアプリケーション要件を満たすかどうかの評価について、既存のお客様と、これから AWS をご利用になるお客様の両方をサポートするため、AWS は技術製品ドキュメントをオンラインで発行し、お客様が GxP システム設計を承認する前に AWS 製品を試せるようにしています。

- AWS 製品ドキュメント: https://aws.amazon.com/documentation/

お客様は、次のドキュメントを更新して、GxP システムでの AWS 製品の使用をサポートする必要があります。

- SDLC 手順
- GxP システム要件およびリスク評価
- GxP システムソリューションアーキテクチャ
- AWS 製品アセスメント

3.1.6 サプライヤの評価

GxP 要件を持つ組織は、サプライヤ、請負業者、およびコンサルタントを、指定された要件に見合う基本的な能力があるかどうかといった観点から評価し、選定する必要があります。お客様が製品アセスメントを実施し、AWS 製品がその GxP システムアーキテクチャの要件を満たすことができると判断された場合、次にサプライヤの評価を実施し、AWS が公開されているインターフェイスの仕様や SLA に従って AWS 製品を確実に提供できるかどうかを確認することになります。

AWS は、商業 IT 組織向けに、最新の品質、セキュリティ、および信頼性標準に準拠した、業界をリードする管理統制フレームワークを運用しています。AWS の統制に関連したコンプライアンス評価は、適格なサードパーティーの監査人によって繰り返し実施されています。また、これらの評価のコンプライアンスレポートは、AWS をサプライヤとして評価できるようにするため、お客様に公開(SOC1 等の特定のレポートの場合、機密保持契約が必要)しています。AWS のコンプライアンスレポートでは、評価対象 の AWS 製品とリージョンの範囲、および評価機関

による準拠証明が示されています。

統制	評価基準	監査人	コンプライアンスレポート
ISO 27001	ISO/IEC 17021 および 27006	EY CertifyPoint	https://aws.amazon.com/compliance/iso-27001-faqs/
ISO 27017	ISO/IEC 17021 および 27006	EY CertifyPoint	https://aws.amazon.com/compliance/iso-27017-faqs/
ISO 9001	ISO/IEC 17021	EY CertifyPoint	https://aws.amazon.com/compliance/iso-9001-faqs/
SOC 1 SOC 2	AT 801 および	EY	https://aws.amazon.com/compliance/soc-faqs/
SOC 3	AT 101 Controls、TSP Sec. 100 Trust および証明		
FedRAMP/ NIST 800-53r4	NIST 800-53a	Veris Group	https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services- aws-eastwest-us-public-cloud/
PCI-DSS v3.1 レベル 1	PCI DSS セキュリティ監査手順	Coalfire	https://aws.amazon.com/compliance/pci- dss-level-1-faqs/

AWS セキュリティプロセスの透明性と、AWS 製品の現在および過去の実績をお客様に示す追加のオンラインリソースが利用可能です。

- AWS リスクとコンプライアンスのホワイトペーパー、付録 A: CSA Questionnaire https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
- 「AWS セキュリティプロセスの概要」ホワイトペーパー
- https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
- AWS サービス状態ダッシュボードおよびステータス履歴 http://status.aws.amazon.com/

GxP のお客様は、いずれのサプライヤカテゴリも AWS 製品の使用に対応可能にするために、サプライヤの評価手順についても更新を検討する必要があります。GxP 以外のシステムで過去に AWS 製品を使用した経験のあるお客様の場合、AWS の GxP サプライヤの評価には、それらの GxP 以外のシステムのパフォーマンス履歴の確認も含める必要もあります。それには、なんらかの AWS に起因するシステム関連の検討事項、およびソリューションの構築

検討(ソリューションアーキテクチャ)を通じてお客様が対応できなかったような課題も含めるようにします。

お客様は、次のドキュメントを参照、更新して、GxP システムでの AWS 製品の使用をサポートする必要があります。

- GxP サプライヤの分類および評価手順
- GxP 以外のシステムパフォーマンスの確認
- サプライヤへの質問票を含む AWS サプライヤの評価に関するデータ
- AWS サプライヤの承認に関するレポート
- AWS コンプライアンスレポートおよびホワイトペーパー
- サプライヤアグリーメント (17 ページ) も参照してください

3.1.7 サプライヤ・アグリーメント

IT サプライヤとのアグリーメントは、GxP システムを使用する企業にとって重要です。これには、IT サプライヤ製品の重要な変更について通知するような、サプライヤからの責任共有モデルおよびコミットメントに関する文書化された明確な説明も含まれます。AWS 製品はすべてのお客様に対して標準化され、同質であるため、AWS 製品に関するアグリーメントも標準化され、AWS およびお客様の義務や、AWS 製品の変更に関する通知のメカニズム等の内容が含まれています。

AWS アグリーメントを以下に示します。6.3 AWS アグリーメントの責任共有モデル には、これらの AWS アグリーメントに含まれる GxP 関連の一部の責任範囲を示す表が含まれています。

- カスタマーアグリーメント https://aws.amazon.com/agreement/
- エンタープライズ契約 AWS セールスへの問い合わせ
- セキュリティの追加条項 AWS セールスへの問い合わせ
- カスタマーサポート https://aws.amazon.com/premiumsupport/
- サービス条件 https://aws.amazon.com/service-terms/
- 利用規定ポリシー https://aws.amazon.com/aup/
- 製品固有のサービスレベルアグリーメント (SLA):

Amazon S3	https://aws.amazon.com/s3/sla/
Amazon EC2 および EBS	https://aws.amazon.com/ec2/sla/
Amazon RDS	https://aws.amazon.com/rds/sla/
Route53	https://aws.amazon.com/route53/sla/
CloudFront	https://aws.amazon.com/cloudfront/sla/

- データ処理の追加情報
  https://aws.amazon.com/compliance/eu-data-protection/

AWS 製品を GxP システムにおいて使用するお客様は、必要とするサポートのレベルについて慎重に検討する必要があります。AWS サポートには、ベーシック、開発者、ビジネス、およびエンタープライズという 4 つの区分けがあり、緊急度ランキングのレベルと、それに関連した応答時間が異なります。規制当局による検査の際のシステム関連問題のトラブルシューティングなど、お客様の予期するサポートシナリオによりますが、AWS サポートのレベルによりお客様のリクエストに対する応答時間が決まります。現在、AWS の GxP のお客様の多くは、こうしたシナリオに対応するため、ビジネスまたはエンタープライズレベルのサポートを選択しています。

お客様は、AWS の標準化された運用およびアグリーメントモデルに準拠していることを確認するため、IT サプライヤアグリーメントポリシーを確認し、必要に応じて更新する必要があります。これは特に、サプライヤがサービスをカスタマイズし、お客様に代わってアプリケーション開発、検証、およびメンテナンスアクティビティを実行したマネージド型サービスプロバイダー、ニッチ GxP サービス、およびコロケーションプロバイダーを以前に使用したことがある企業に必要です。

お客様は、次のドキュメントを更新して、GxP システムでの AWS 製品の使用をサポートする必要があります。

- IT サプライヤアグリーメントポリシー
- 上記に示した該当するアグリーメント

3.1.8 記録およびログ

ライフサイエンス企業は、各 GxP システムについて、GxP の証明として必要な、維持すべき記録とログを識別し、保持期間中はその記録の整合性と可用性を維持することが要求されます。GxP システムで AWS 製品を使用する際に、保持可能な記録は主に GxP システム内のお客様のデータ、GxP システムソフトウェアコードと SDLC の記録、およびお客様の AWS アカウント内で利用できる、システム生成ログおよび監査証跡等で構成されます。AWS 製品で達成可能な高いレベルの自動化と最新の SDLC 手法により、かつては手動プロセスで作成された維持可能な記録の多く（紙ベースのインストールプロトコルなど）は、プログラムで実行されるコマンドを通じて生成されるようになっています。記録を生成するこの信頼性の高い方法により、変動性が低下し、GxP データの管理、および SDLC の観点の両方から、データの信頼性が確実に向上します。

自動化された IT プロセスの記録タイプと形式は、手動で生成された記録とはかなり異なるため、GxP のお客様は、維持する必要がある記録のタイプと形式を確認し、自社の記録保持ガイドラインを適切に作成する必要があります。GxP 医療機器およびアプリケーションで使用される AWS 製品は、Design History File (DHF) および Device Master Record (DMR) への記録保持の影響についても評価する必要があります。多くの場合、監査証跡やアラームなど、AWS

製品によってプログラムで生成される記録は、お客様の AWS アカウント内、または別の場所に保持のために記録を転送することにより、完全に持ち運びと維持が可能です。

お客様は、次のドキュメントを更新して、GxP システムでの AWS 製品の使用をサポートする必要があります。

- 記録保持スケジュール
- 記録タイプと形式のガイドライン
- 記録保持手順
- CloudTrail ログ
- CloudWatch アラーム
- S3 および Glacier 保持ポリシーとライフサイクルルール
- AWS サポートケースの履歴

3.2 システム開発ライフサイクル

組織の品質システム要件に加えて、各 GxP システムには、特定の機能と、それを提供するための統制された SDLC プロセスが必要です。各システムに適用される特定の機能と SDLC 統制はさまざまな要因に基づいていて、米国の 21 CFR Part 11 と 820、欧州の Annex 11 と 93/42/EEC、および各国の同等の規制から派生します。これらの規制形態の全体的な意図は、GxP システムの使用を意図されたとおりにし、データの高い信頼性を確実にすることです。これは、データが医療ケアの提供や、人の食品、薬、医療機器や、動物の食品や薬など、医療製品の安全性と効果に関する決定に使用される可能性があるためです。

GxP システム用の SDLC 統制:

- 指定された要件を満たすための設計および開発の統制
- 正確性、信頼性、および一貫性のある意図されたパフォーマンスを確実にするため、ソフトウェアアプリケーションを検証し、インフラストラクチャを適格にする
- システムユーザードキュメントを含め、本稼働環境で稼働するシステム用の変更管理および変更履歴
- 不適合（エラーなど）を検出し、対応するための本稼働環境でのシステムのモニタリング
- システム関連の苦情およびユーザーサポートケースの文書化と処理
- 減価償却を含む、システムライフサイクル全体を通じた SDLC 記録および GxP データの保持

GxP システムで必要な機能:

- 人間および機械による読み取りが可能な形式で GxP データの正確で完全なコピーを生成する機能
- データ入力の検証とデータ整合性のチェック
- ユーザーアクションのユーザーアクセスコントロールと許可のチェック
- ユーザーアクションとデータの変更に関する、安全でコンピュータによって生成され、タイムスタンプが付いた監査証跡
- ステップの許可されたシーケンスの実施チェック（ワークフローの実施など）
- 伝送中と保管時のデータの暗号化
- データに対してユーザーが許可したアクションの電子署名マニフェスト
- 電子署名と関連データ間のリンク

従来の IT インフラストラクチャモデルでこれらの要件を満たすには、一般的に手間がかかります。これは、ソフトウェアベースアプリケーションの SDLC とハードウェアベースインフラストラクチャの SDLC はかなり異なり、さまざまな製造元によって作成された物理インフラストラクチャコンポーネントの性質により、設定を維持し、インフラストラクチャ全体で変更を追跡可能にするには、数多くのマニュアルによる統制が必要になるためです。AWS 製品を使用して、物理的なインフラストラクチャ製品を仮想化され、調和されたインフラストラクチャの製品群に置き換え、インフラストラクチャ全体をソフトウェアコードとして作成、管理できるようにしています。お客様は AWS 製品を Amazon EC2 のように使用して、バージョン管理されたイメージから同等の仮想サーバーを起動し、ストレージ、データベース、およびネットワーキングを含むインフラストラクチャ全体を、ソフトウェアベースの設定テンプレートを使用して開発、バージョン管理、デプロイできます。このコードとしてのインフラストラクチャ手法により、これまでにないレベルの統制、均一性、および自動化が、アプリケーションとインフラストラクチャを含むシステム全体で SDLC にまたがって提供されます。また、開発、テスト、本稼働環境の同期では、従来の IT モデルよりもかなり処理が少なくなることを意味します。

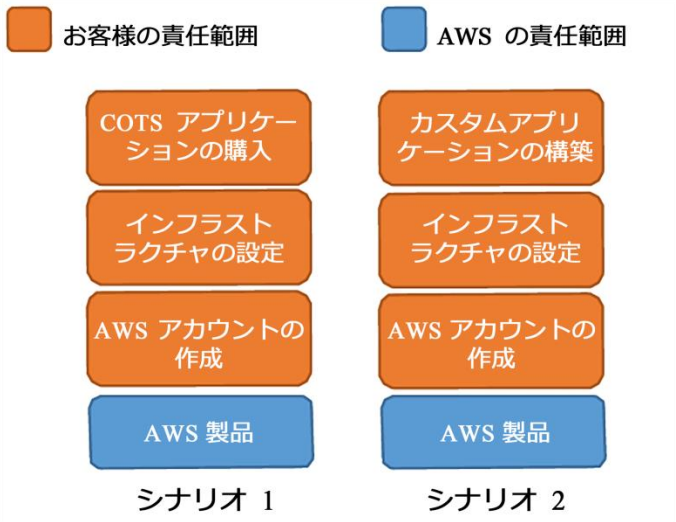
通常、AWS 製品は DevOps などの SDLC 手法と関連付けられますが、Waterfall や V-model などの SDLC は完全にサポートされます。このセクションでは、一般化された 3 フェーズの SDLC 例を使用して、GxP システムで AWS 製品を使用するお客様向けの考慮事項をいくつか説明します。

3.2.1 開発

GxP に関連したシステムの開発のためには、指定された要件にシステムを確実に一致させるために、以下に示す手順に従う必要があります。GxP システムで AWS 製品を使用するお客様は、すべての GxP システム開発作業（アプリケーションの計画、コーディング、構築、設定、テスト、検証、デプロイ、およびソフトウェア定義インフラストラクチャの構築、プロビジョニング、設定、オーケストレーション、デプロイ、資格供与、運用、等）について、完全な責任を負います。AWS がお客様に代わって GxP システムを設計または開発するものではありません。しかし、AWS 製品には、GxP システムエンジニアがシステム設計および開発アクティビティの参考として活用可能な広範囲にわたるユーザードキュメントとホワイトペーパーが用意されています。

また、GxP システムのデザイン要件には、サイバーセキュリティ要件も含める必要があり、AWS においては、NIST Special Publication 800- 13 等によって広く認められたセキュリティ計画標準や、FDA の「Content of Premarket Submissions for Management of Cybersecurity in Medical Devices（市販前申請における医療機器のサイバーセキュリティの管理）」等の該当する規制ガイダンスドキュメントに従って、GxP システムのセキュリティ計画を作成することを推奨するものです。

お客様は AWS 製品を使用して様々なタイプのシステムを構成できますが、2 つの基本的な開発シナリオがあります: 1）COTS アプリケーションの購入、または 2）カスタムアプリケーションの構築。



AWS 製品で使用する COTS ソフトウェアパッケージを評価する際に、GxP のお客様は AWS パートナーネットワーク（APN）テクノロジーパートナーと AWS Marketplace を評価に含める必要もあるでしょう。AWS テクノロジーパートナーは、AWS プラットフォーム上でホストされるか、AWS プラットフォームと統合されたソフトウェアソリューションを提供しています。AWS Marketplace は、お客様が AWS 対応ソフトウェアを購入し、その AWS アカウントに直接デプロイできるオンラインストアとなっています。

- APN テクノロジーパートナー https://aws.amazon.com/partners/technology/
- AWS Marketplace https://aws.amazon.com/marketplace/

AWS 製品は、APN ネットワークまたは AWS Marketplace 外部から商用ソフトウェアアプリケーションと一緒に使用できますが、お客様はアプリケーションのライセンスアグリーメントを確認し、製品アセスメント（3.1.5 製品アセスメントを参照）を実施して、アプリケーションの AWS 製品との互換性を判断する必要があります。APN コンサルティングパートナーからこのような要件に関しての支援を受けることも可能です。
(https://aws.amazon.com/partners/consulting/)

通常、ライフサイエンス企業は、ソフトウェアアプリケーションの構築よりも購入を好む傾向にありますが、AWS 製品を最新の SDLC 手法と組み合わせる主要な利点は、カスタムソフトウェアソリューションを迅速に、繰り返し、確実に提供できることです。遅延やエラーなど理由により、ソースコードからの手動によるソフトウェアパッケージの構築や、手動による回帰テストの実行は避けられていましたが、完全に自動化されたツールによって、そうした事象は減少さ、排除されつつあります。AWS OpsWorks、AWS CodeCommit、AWS CodePipeline などの AWS 製品は、企業独自の要件を満たす一方で、ソフトウェア開発作業の SDLC 統制の実装を合理化するために役立つ、柔軟性の高い構成が可能なツールとしてシステムエンジニアに提供されています。

お客様が GxP システムを開発し、検証、本稼働などの環境にデプロイする準備が整う、Amazon Machine Images（AMI）、AWS CloudFormation、AWS CodeDeploy、AWS Elastic Beanstalk などの AWS 製品により、整合性があり、また統制されたデプロイが簡単かつ反復して実施可能になります。また、これらのツールにより、ネットワークスタックからデータベースやストレージボリューム、コンピューティングインスタンスまで、システム環境全体のバージョンを管理すると同時にそのコピーを作成することも可能です。これらのバージョン管理されたコピーは、アーカイブや変更管理、または継続的な開発やトラブルシューティング用の新しい開発/テスト環境のプロビジョニング等のために保持することが可能です。

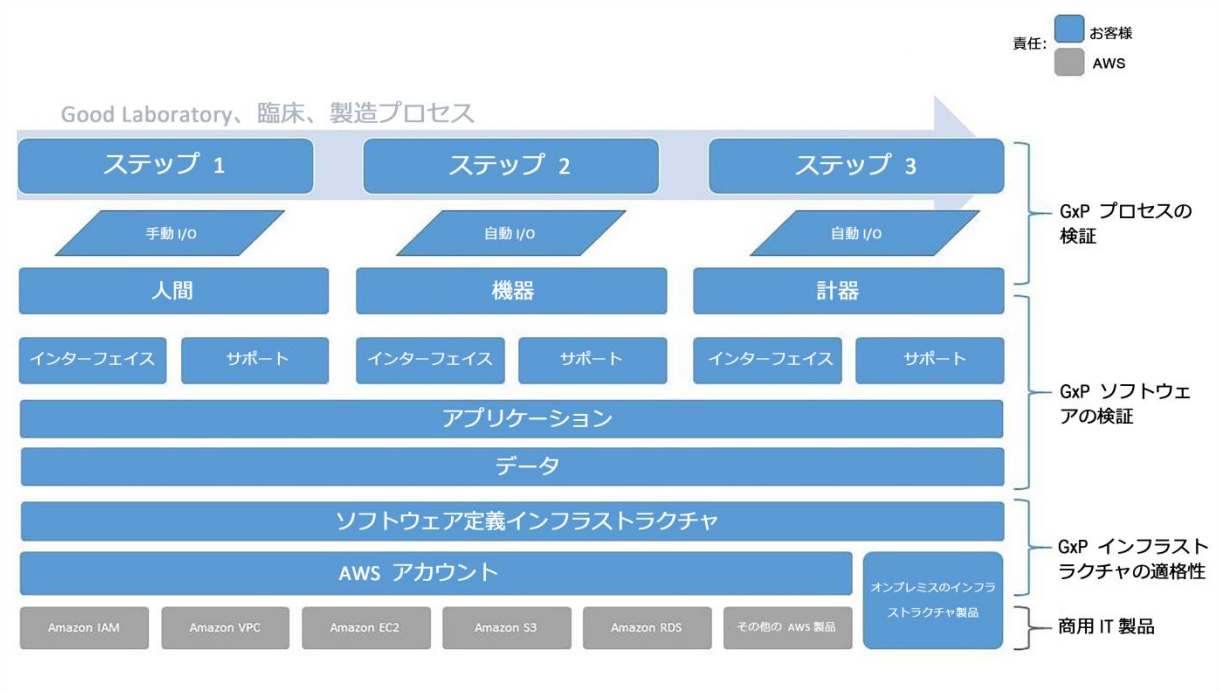
継続的な開発とデプロイ、というこの新しいモデルは、多くの業界の多くのお客様が AWS 製品を使用してビジネスを革新している主な理由の 1 つです。これらの利点を GxP システムで活用するためには、お客様の開発手法と手順の確認と更新が必要になる場合があります。

お客様は、GxP システムでの AWS 製品の使用をサポートするため、次のドキュメントについて検討する必要があります。

- SDLC 手順
- システム設計と開発計画
- 危険性の評価手順
- コード検査 SOP
- ユースケースとユーザーストーリーまたはその他の要件の仕様
- エンドユーザーのサポートを含むエンドユーザー SLA 条件
- ソフトウェアアーキテクチャ仕様
- アプリケーションの機能要件
- GxP 医療およびモバイルアプリケーション用の暫定的なリスク（または危険）分析
- AWS CloudTrail および設定ログ
- アプリケーションソースコード
- EC2 AMI および CloudFormation テンプレート
- コードのデプロイ SOP

3.2.2 検証

GxP アプリケーションを検証し、ソフトウェア仕様がユーザーニーズ要件を満たし、さらに、GxP アプリケーションが実行されるソフトウェアインフラストラクチャが、アプリケーションのシステム要件を満たすものであることを確認する必要があります。AWS 製品は完全にセルフサービスベースで提供されるため、GxP システムで AWS 製品を使用するお客様は、AWS アカウント内のすべてのソフトウェアの検証およびインフラストラクチャの適合作業に対して完全な責任を持ちます。AWS はお客様に代わってアプリケーションを開発または管理したり、お客様固有のインフラストラクチャを供給または設定をするものではありません。また、お客様に代わって GxP の検証または適合作業を実行することはできません。AWS は、AWS 製品を AWS 製品の仕様、SLA、および各種商用の IT 標準規格に準拠させる責任があり、GxP に関連したお客様には、AWS 製品を使用して構築する GxP システムを検証する責任があります。



AWS 製品を使用し、アプリケーションおよびインフラストラクチャのインストール、インスタンス化、およびデプロイ等を実施していくことは、従来の物理インフラストラクチャおよびインストールメディアとは基本的に異なったものとなります。物理インフラストラクチャ・ハードウェアの時代は、インストール作業はほとんど手動でプロトコル駆動型でした。通常、こうしたプロトコルはシステムコンポーネントごとに個別に開発、事前承認され、検査者が立ち会ってオペレーターが手動で実行することで、各ステップが正常に完了されました。完了したプロトコルは、品質担当者が確認して承認していまhした。IT の SDLC が成熟し、サーバーの仮想化が一般的になると、検証作業はまだほどんど手動であるものの、プロトコル駆動型からプロシージャ—駆動型の作業に移行しました。一部の企業はプロトコルを使用して的確な ″ゴールドイメージ″ を作成し、その後で適格なイメージを使用して、プロシージャ—に従い仮想サーバーを作成しました。

インフラストラクチャがソフトウェアで定義されるクラウド時代では、GxP システムに関わるエンジニアはシステムスタックそのもの全体をバージョン管理し、バージョン管理型インフラストラクチャ・テンプレートを使用してデプロイを自動化することができます。AWS のお客様で一般的に使用される手法の 1 つとして、適格なシステムテンプレートを作成し、それを自動化されたデプロイツールと組み合わせて使用して、個別のリソースや、開発、テスト、および検証環境全体をプロビジョニングしています。各 AWS 製品に組み込まれたウェブサービス API テクノロジーにより、RunScope や SoapUI などのサードパーティー製 API 検証ツールを活用して、以前の手動で定期的な検証で達成できたよりもはるかに頻繁に、予期されるシステム動作を適格にし、検証を実施することが可能です。

ポイントインタイムの手動作業から、こうした連続した自動的な作業へのパラダイムシフトにより、多くのライフサイエンス企業は AWS の商用クラウド製品を GxP システムのコンポーネントとして使用するにあたり、従来のハードウェアインフラストラクチャに関して従っていた GxP に係る変更管理と検証手法を再確認し、自動化されたインフラストラクチャモデルに対応できるように、更新する必要があるでしょう。

お客様は、GxP システムでの AWS 製品の使用をサポートするため、次のドキュメントについて検討する必要があります。

- SDLC 手順
- 検証手順
- IT 資格審査手順
- 自動デプロイ手順
- AWS CloudTrail および設定ログ
- アプリケーションソースコード
- EC2 AMI および CloudFormation テンプレート

3.2.3 運用

実稼働環境の運用における GxP システムの開発、実施、制御、モニタリングは、それらを継続的に仕様に準拠させていく上で重要です。エンドユーザーの問題またはシステムの逸脱が発生した場合のために、GxP システムを使用している組織は、それらの問題に対応、修正、予防するプロセスも維持していく必要があります。こうした取り組みに AWS 製品を活用することも可能です。しかし、AWS ではお客様に代わって GxP システム上で GxP システムのオペレーションやモニタリング作業を実施するものではありません。

GxP システムの原則	要件の概要	考慮事項
変更管理	実稼働環境の GxP システムへの変更は、定義されたユーザー要件にシステムを確実に一致させるために、確認または検証する必要があります。	お客様: システムのユーザー要件を定義し、AWS 製品がそれらの要件に対応できるよう設定および適合させるのは、お客様です。お客様は、実装する変更をユーザー要件および製品の設定に対して確認および検証します。 AWS: AWS は、お客様の要件または製品の設定を管理しません。したがって、AWS はお客様に代わって GxP システムの変更を確認または検証することはできません。AWS は AWS 製品の変更を確認し、製品仕様と SLA が満たされるようにします。
サービスレベルアグリーメント (SLA)	GxP システムを維持する IT 部門を含めて、GxP システムユーザーとサードパーティーの間に正式なアグリーメントが存在する必要があります。	お客様: お客様は GxP システムのサービスレベルアグリーメント (SLA) を定義し、SLA に一致するように AWS 製品を設定および使用する必要があります。 AWS: AWS 製品の SLA は GxP システムの SLA とは異なり、お客様が自身のシステム全体として規定する SLA について、AWS は管理または関与することはありません。 付録 4.3「AWS アグリーメントの責任共有モデル」を参照してください

エンドユーザーのサポート	GxP システム所有者は、エンドユーザーにサポートを提供する手順を確立します。	お客様: お客様は、GxP システムのエンドユーザーにサポートを提供します。 AWS: AWS は GxP システムエンドユーザーにサポートまたはサービスを提供しません。
バックアップ &リストア	GxP データの定期的なバックアップを行い、データの整合性と復元性の検証を含めます。	お客様: お客様は AWS 製品を設定および使用して、データの適切なセキュリティ、保護、およびバックアップを維持します。 AWS: AWS は、お客様による製品の設定について一切制御できず、お客様のコンテンツ（データ）についても把握していません。したがって、AWS はお客様に代わってお客様のコンテンツをバックアップしません。
インシデントへの対応	GxP システムインシデントの対応は、報告、評価、文書化する必要があります。	お客様: お客様はエンドユーザーおよびシステム管理者からインシデントレポートを受け取り、それらのレポートを評価、文書化します。インシデントで AWS サポートが必要な場合、お客様はサポートアグリーメントに準拠した方法を使用してサポートケースを登録することができます。 AWS: AWS は GxP システムインシデントを把握しませんが、AWS 製品の問題に関連して AWS に提出されたお客様のサポートケースは、お客様のサポートレベルアグリーメントに従って評価、調査されます。お客様のサポートケース履歴は文書化され、お客様がオンラインで表示することができます。

GxP システムの原則	要件の概要	考慮事項
是正措置と防止措置	GxP システムには、システムの不適合を是正し、防止する手順が必要です。	お客様: お客様は GxP システムの不適合の識別と追跡を管理し、必要な是正措置と防止措置を実装します。 AWS: AWS はシステムオペレーションおよび不適合について一切把握せず、システムに対する是正措置や防止措置を実装することはできません。AWS は AWS 製品の継続的な改善プログラムを維持し、このプログラムは品質およびセキュリティ証明の範囲に含まれます。

ウェブサービステクノロジーと最新の自動化されたデプロイメントの実践によって、個々のシステムコンポーネントの最小限のアップデートと最小限のダウンタイム（多くの場合ゼロダウンタイム）を可能にすることで、継続的デプロイメントを遂げることになり、それはシステムの回復性とスピードの向上につながります。 API インターフェイスの仕様が変わらない限り、お客様はシステムを利用し、使用中の機能が有効であることについて信頼することが可能です（検証する必要はあります）。AWS 製品を使用するお客様はウェブサービス API の様々な側面から利点を得ることができますが、お客様は API の停止に対して、レジリエンシーを持つようにシステムを設計する必要もあります。また、API ベースのシステムは、Remedy、ServiceNow、Sparta Systems などの変更管理システムと統合し、ソフトウェア開発およびデプロイに関するプロセスを GxP の品質に関する承認プロセスとの完全な統合に備えることも可能です。

GxP のお客様がこれらの運用上の利点を得るためには、AWS 製品との整合性の観点から運用に関する文書や記録を確認し、必要に応じてそれらを更新する必要があります。

お客様は、GxP システムでの AWS 製品の使用をサポートするため、次のようなドキュメントについて検討する必要があります。

- 変更管理手順
- 設定管理手順
- 本番環境へのリリース手順
- モニタリング手順
- AWS CloudTrail および設定に関するログ
- アプリケーションソースコード
- EC2 AMI および CloudFormation テンプレート
- お客様のサポートケースの履歴

3.3 規制事項

GxP 規制対象の業界においては、規制関連業務担当者は GxP システムのデータを使用して申告文書や登録文書を保健当局や倫理委員会等の規制当局に提出する必要があります。また、規制機関の検査に対応する手順を作成、維持し、GxP 製品を供給しようとする地域内で、常に関連する法律に対する変更を追跡する必要もあるでしょう。GxP のお客様が GxP システムで AWS 製品を使用する場合、その IT、品質保証、および規制関連業務チームが、規制関連業務に影響する可能性のあるものについて検討していくことになります。それには、以下のようなものが含まれます。

- 規制当局への提出書類
- 検査
- 検閲局および倫理委員会の要件

3.3.1 提出書類

規制当局への提出書類に対するシステムの使用は新しいことではなく、提出書類の生成、追跡、送信用のクラウドベースのソフトウェアアプリケーションがすでに存在しています。実際に、FDA は AWS 製品を使用して、openFDA.gov プラットフォームで提出書類からデータを発行しています。新たに GxP に関連してお客様が検討を必要とするのは、該当する GxP システムを提出書類の内容に含めるかどうかと、含める場合はお客様の規制チームが AWS 製品の使用にどのように対応していくかということになります。

たとえば、Picture Archiving and Communication System (PACS) などの医療機器ソフトウェアアプリケーションでは、FDA の審査用に 510k 申請書類の提出が必要になる場合があります。PACS が、AWS の Amazon EC2 Product と互換性のある一般的な x86 サーバーで実行されるように構築されている場合、PACS の 510k 申請書類で、AWS 製品については具体的に述べず、「ソフトウェアアプリケーションは、汎用のコンピューティングサーバーとともに使用されている PACS である」と述べる場合もあるでしょう。提出書類に AWS 製品を含める決定は GxP のお客様の責任であり、GxP のお客様に対して提出書類に関連する質問があった場合は、適格な規制専門家のアドバイスを求めるよう推奨するものです。

3.3.2 検査

当局は、ライフサイエンス企業とその GxP システムをいつでも検査する可能性があります。COTS の IT 製品には、当局の検査を受け、GxP システムで使用されてきた長い歴史がありますが、AWS のような GxP システムにおける COTS クラウド製品プロバイダーの使用は比較的新しく、当局の検査スタッフは、AWS 製品またはその使用に精通していない可能性があります。AWS 製品を使用する GxP システムで良好な検査結果を得るためには、いくつかの要素を含む検査準備計画を確立し、維持することを お客様にお勧めするものです。

- お客様の組織内における主要なスタッフの識別 (GxP システムでの AWS 製品の設

定と使用について、だれが精通しているか等)。

- FDA のような当局による検査の際に、これらの主要なスタッフに確実に通知し、対応を可能にするための手順。
- 当局の検査官に主要なシステム要素を迅速かつ正確に伝えるための、各 GxP システムの全般的な説明に関する概要。お客様は、次の要素をプレゼンテーション資料に含めることを検討する必要があるでしょう。
    - システム名、バージョン (該当する場合)、およびシステムの分類を含むシステムの識別
    - 主要な GxP に関連した取り組みの概要、またはシステムに依存する職務上の役割、またはその両方を含む、システムに関する説明 (他のシステムとのインターフェイスも識別する必要があります)。
    - 関連する責任範囲を含むネットワークまたはアーキテクチャ図
    - システムにアクセスする元となる物理的な場所、エンドユーザー数、インターフェイス数、および製品数を含むシステムオペレーション
    - 事業部門、技術手順、または企業手順を含むアプリケーション SOP の一覧
    - エンドユーザーの事業単位名、技術および管理責任、セキュリティオペレーションなどを含む責任範囲の概要

AWS からのトラブルシューティングサポートを必要とするシステム関連調査が発生した場合、お客様が選択した AWS サポートのレベルにより、サポートリクエストの手順と、AWS からの応答時間が決まります。

お客様は、GxP システムでの AWS 製品の使用をサポートするため、次のドキュメントについて検討する必要があります。

- 検査準備計画
- GxP システムの概要説明
- システムドキュメントの索引

3.3.3 調査参加者の個人データプライバシーの管理

臨床研究で使用される GxP システムでは、該当システムによって保管、処理、転送される個人を特定できる情報(PII)および保護された健康情報(PHI)等に対して、個人データのプライバシーに関する統制が必要になる場合もあります。その例を以下に示します。

- 調査に関する募集のためのツール
- 電子データキャプチャ (EC) システム
- データストレージおよびアーカイブ
- 診断医療機器アプリケーション
- 携帯医療機器アプリケーション

AWS 製品が関連する GxP システムを使用した、人による調査研究を行っているスポンサーや調査者は、Institutional Review Boards (IRB)、Independent Ethics Committees (IEC)、Data Access Committees (DAC) などから、調査参加者の個人情報をシステムでどのように保護しているか尋ねられる可能性があります。これには、必要なくなったときにシステムアクセスを取り消す手順を示すなど、実行されたシステムセキュリティ確認やセキュリティオペレーション統制が含まれます。PII を含む GxP システムで AWS 製品を使用しているお客様は、データの局所性と、必要に応じて、システムが実行されている AWS 製品で実装されたセキュリティおよびデータの局所性統制の要件について確実に理解する必要があります。AWS 製品のデータ局所性統制の詳細は、オンラインで参照できます。
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html)

お客様は、GxP システムでの AW 製品の使用をサポートするため、次のドキュメントについて検討する必要があります。

- PII 保護のポリシー
- データ局所性の統制計画
- GxP システム用のシステムセキュリティ計画

4 まとめ

AWS 製品の提供はインターネット経由となります。GxP のお客様は、AWS 製品を使用して開発、検証、運用するアプリケーションや仮想化されたインフラストラクチャを含めて、製品の使用について説明責任と責任を保持します。AWS 製品をコンポーネントとして組み込む GxP システムの効果的な統制を実現するために、このホワイトペーパーの推奨事項を使用して自社の品質システム、SDLC 統制、および規制項目計画を評価できます。

5 ドキュメントの改訂

次の表に、このホワイトペーパーの完全な改訂履歴を示します。

日付	説明
2016 年 1 月	初回リリース

6 付録

6.1 データプライバシーリソース

AWS では、データの保護は常に最優先事項です。お客様は AWS 製品の使用に際してデータの所有権と管理を保持し、AWS は追加のプライバシーに関連した保証と透明性をお客様に提供するべく尽力するものです。この付録では、お客様が利用可能な主要なデータプライバシーリソースの一部を示します。

- AWS データプライバシー FAQ
  https://aws.amazon.com/compliance/data-privacy-faq/
- Amazon 企業半期情報リクエストリポート
  http://d0.awsstatic.com/certifications/Information_Request_Report.pdf
- AWS サードパーティーのアクセスリスト
  http://aws.amazon.com/compliance/third-party-access/
- 米国および欧州のセーフハーバー
  https://safeharbor.export.gov/companyinfo.aspx?id=27379
- EU 指令 95/46/EC の FAQ およびモデル条項
  https://aws.amazon.com/compliance/eu-data-protection/
  http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html
- 遺伝子と表現型の米国データベース
  https://d0.awsstatic.com/whitepapers/compliance/AWS_dBGaP_Genomics_on_AWS_Best Practices.pdf
- US HIPAA Business Associate の FAQ
  https://aws.amazon.com/compliance/hipaa-compliance/

6.2 注釈付き 21 CFR Part 11

この付録では、お客様が AWS 製品を使用して、21 CFR Part 11 規制の電子記録および電子署名の要件を満たす方法の一部を紹介します。

- **アクセスコントロール**: GxP システムとデータへのアクセスは、許可されたユーザーに制限できます。お客様は、Amazon Identity and Access Management (IAM) や AWS Directory Service などの AWS 製品を使用してアクセスコントロールを実装できます。AWS のお客様は、Microsoft Active Directory など、既存のオンプレミスディレクトリを操作して、ハイブリッドクラウドデプロイ用のシームレスなアクセスコントロール環境を作成するようにアカウントのアクセスコントロールを設定することもできます。
- **GxP システム検証**: アプリケーションは AWS 環境上にデプロイして検証できます。お客様は、その組織のポリシーと手順に従って GxP システムを検証できます。
- **データの取得可能性**: AWS のお客様は、記録保持期間中はいつでも AWS アカウントから記録の正確で完全なコピーを生成および取得できます。AWS のお客様は AWS アカウント、システム、およびデータへのルート管理アクセスを維持するため、AWS 監査証跡製品と機能を有効にしている限り、いつでもデータや監査証跡を個別に取得できます。
- **監査証跡**: 安全で、コンピュータによって生成され、タイムスタンプが付いた監査証跡を、お客様が定義したポリシーに従って生成、モニタリング、ダウンロード、維持できます。AWS CloudTrail、Amazon CloudWatch などの AWS 製品により、お客様はログシステムを開発、運用して、個別のファイルオブジェクトレベルからアプリケーションレベルまで、データとシステム監査の最大レベルを満たすことができます。
- **ワークフローの実施**: GxP ワークフローアクティビティの運用システムチェックは、お客様が GxP システム用に維持する SDLC プロセスを含めて、完全に AWS のお客様によって管理されます。
- **ユーザー認証**: 許可された個人のみがシステムを使用するか、データでアクションを実行できるようにする認証チェックは、AWS アカウント内およびアプリケーション内のインフラストラクチャレベルの役割とアクセス権限グループを使用して、AWS のお客様が実装することができます。Amazon IAM などの製品により、お客様はインフラストラクチャユーザーアカウントやマシン間サービスアカウントに必要な役割、セキュリティレベル、およびトランザクションポリシーを定義できます。
- **入出力の確認**: 入力チェックと非否認の統制は、GxP データを作成、更新する人、プロセス、およびテクノロジーに大きく依存します。GxP データを手動でウェブまたはモバイルアプリケーションに入力した場合、AWS のお客様は手動プロセスの組み合わせを使用して、アプリケーションへのアクセスを付与する前に、ユーザーのトレーニングと確認を行います。アクセスを付与されると、アプリケーションレベルの制御により、必要な入力チェックが自動的に実施されます。お客様のアカウント内の AWS 製品を使用して、ワークステーションやモバイルデバイスなどのネットワークリソースの接続をモニタリングおよび制御できます。GxP データがローカルの機器、デバイスセンサー、またはアプリケーションコンピューティングプロセスから自動的に生成される場合、コンピュータのローカル環境から AWS アカウントへのデータのキューイングと転送を、Amazon Simple Queue Service (SQS) や Amazon Kinesis などさまざまな AWS 製品、またはユーザーレベルとサービスレベルのアクセスコントロールを有効にするアイデンティティ&アクセス管理ツールを使用して有効に

し、制御できます。

- **個人トレーニング**: AWS のお客様は、AWS アカウント内で GxP データおよびシステムを開発、維持、使用できます。つまり、スタッフが、割り当てられた GxP タスクを実行するための教育やトレーニングを受け、経験があるかどうかを判断するための既存のポリシーと手順に従うことができます。AWS では、お客様の IT エンジニアリングスタッフが AWS の学習目標を達成できるようにするための広範な技術ドキュメントやお客様トレーニングプログラムを用意しています。また、広範な AWS パートナーエコシステムには、サードパーティーのシステムインテグレーターと、ヘルスケアやライフサイエンスに関する資格を持ったコンサルティングパートナーが含まれます。
- **システムドキュメント**: システムドキュメントに対する適切な統制の使用は、既存の管理されたドキュメント手順とシステムを使用してお客様が達成できます。AWS 技術ドキュメントは、適切な URL およびお客様が必要とするバージョン固有の情報を使用して参照できます。さらに、AWS でのお客様ごとの仮想インフラストラクチャは、本質的にソフトウェア定義インフラストラクチャであるため、お客様はアカウントで AWS リソースを定義するために使用するコードとテンプレートの完全なセットのバージョンを管理し、アーカイブできます（「適格なインフラストラクチャ」を参照）。
- **セキュリティ統制**: 保管時および伝送時のデータ暗号化などの追加の手法は、既存のクライアント側暗号化ソリューション、Amazon Key Management Service（KMS）など AWS の広範なセキュリティ製品、サーバー側暗号化、透過的なデータ暗号化（TDS）を使用してお客様が実装できます。また、Amazon Simple Storage Service（S3）、Amazon Relational Database Service（RDS）、Amazon Elastic Load Balancer（ELB）などの製品の Secure Socket Layer（SSL）機能を使用することもできます。Amazon Virtual Private Cloud（VPC）は、お客様が仮想ネットワーキング環境を管理し、オンプレミスデータセンターと Amazon VPC 間で暗号化されたハードウェア仮想プライベートネットワーク（VPN）接続を作成し、クラウドを既存のネットワークの拡張機能として活用できるようにします。
- **電子署名**: 電子署名のマニフェスト、署名/記録のリンク、電子署名コンポーネントと制御の要件は、通常、GxP データを生成、維持するためにお客様が使用する、検証されたアプリケーションの一部として満たされます。お客様は、AWS アカウントの仮想ネットワークで既存の電子署名アプリケーションの適合性を評価するか、お客様自身で開発するカスタムのクラウドネイティブアプリケーションの一部として電子署名要件に対応できます。AWS 製品を使用してパスワード管理などの要件に対応する場合、Amazon IAM パスワードポリシーなどのすぐに使用できる機能により、お客様は特定の要件に従って独自のパスワードの複雑さや失効ポリシーを作成できます。
- **データ保持**: お客様ごとの GxP データライフサイクルおよび保持要件の手順とポリシーは、お客様の組織および適用される特定の要件によって大きく異なります。お客様が AWS アカウントで GxP データ管理ソリューションを設計、開発するときは、raw データ、派生データ、およびメタデータの記録保持ポリシーを含めて、機密性、整合性、および可用性の要件を慎重に指定する必要があります。

6.3 AWS アグリーメントの責任共有モデル

この表は、AWS 標準アグリーメントに含まれている責任範囲の概要であり、正式なものではありません。このセクションで示す責任範囲は個別の AWS 製品用であり、AWS のお客様とエンドユーザーの間の SLA 責任範囲を含みません。

トピック	責任	お客様	AWS
連絡先	AWS アカウントに関連付けられている有効な E メールアドレスの維持 (カスタマーアグリーメント 1.2)	x	
変更	AWS 製品の重要な変更または終了についてお客様に通知 (カスタマーアグリーメント 2.1)		x
変更	12 か月間にわたる前バージョンの AWS 製品 API のサポート (カスタマーアグリーメント 2.2)		x
変更	AWS 製品の機密性、完全性、可用性を確実にするために必要なセキュリティ更新プログラムの実行 https://aws.amazon.com/security/security-bulletins/		x
コンテンツ	コンテンツ (GxP 記録とアプリケーションなど) の開発、コンテンツ、運用、維持、および使用 (カスタマーアグリーメント 4.1)	x	
コンテンツ	コンテンツのセキュリティ、保護、およびバックアップ (カスタマーアグリーメント 4.2)	x	
サポート	GxP システムのエンドユーザーのサポートの提供 (カスタマーアグリーメント 4.2)	x	
サポート	お客様への基本サポート (https://aws.amazon.com/premiumsupport/)		x
プライバシー	データが存在する地理的リージョンの管理	x	