セキュリティ＆コンプライアンス クイックリファレンス ガイド

2018

aws

注意

本書は、情報提供のみを目的としています。本書は、本書の発行日時点における AWS の最新の製品および手法を記述しており、これらは予告なく変更されることがあります。お客様は、本書の情報および AWS の製品またはサービスのあらゆる利用について、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、いかなる種類の保証も伴うことなく「現状のまま」提供されるものです。本書により、AWS、その関係者、サプライヤ、またはライセンサーの保証、表明、契約責任、条件、または確約が生じることは一切ありません。お客様に対する AWS の責任および責務は、AWS 契約により規定されています。また、本書は AWS とお客様との間の契約に属するものではなく、契約の内容を変更するものでもありません。

目次

概要

私たちは、セキュリティとコンプライアンスに対して異なった考え方を持っています。

Amazon のあらゆるサービスと同様に、お客様を成功に導けているかどうかという点を最重要なものと位置づけ、AWS のセキュリティおよびコンプライアンスプログラムにおける成果を評価しています。お客様が安全で規制に準拠したクラウド環境を運用できるように、要件に合わせる形で様々なコンプライアンス報告書、証明書、認定書をご用意しています。

Amazon Web Services（AWS）を使用すると、コスト削減と拡張性を実現しながら、同時に、堅牢なセキュリティと規制の準拠を維持することが可能です。

AWS が 主要な外部認証を
全リージョンに渡って取得 / 維持して
いること、加えて セキュリティ情報を
積極的に公開 / 開示している姿勢を
高く評価しました。
攻め続けながらも守るところは固く、
という AWS の姿勢は、これからの
金融機関にとっても共感できる部分が
多いと感じています。

福嶋 達也 氏
ソニー銀行株式会社 執行役員(システム企画部担当)

セキュリティは、AWS の最優先事項です。AWS は、お客様のデータを保護することを何よりも重視しています。AWS のお客様が利用するデータセンターとネットワークアーキテクチャは、セキュリティを非常に重要視する組織の要件でさえも満たすよう実装されています。

私たちはお客様のフィードバックを AWS サービスに継続的に取り入れることで、スケーラビリティを維持しながら、迅速なイノベーションに取り組んでいます。そのため、お客様は常に進化し続けている AWS の最新のソリューションを利用できます。また、ID とアクセス権限の管理、ロギングと監視、暗号化と鍵管理、ネットワーク分割、標準的な DDoS 保護といった、AWS の中核をなすセキュリティサービスも絶えず進化させています。

さらに、お客様のチームは、最新のセキュリティ動向に熟知した技術者の設計した高度なセキュリティサービスを利用できるため、新たなリスクに対してもリアルタイムで積極的に対処できます。これは、初期費用が掛からず、また独自のインフラストラクチャを管理する場合よりもずっと低い運用コストで、要件を満たすことが可能なセキュリティサービスを組織の成長や拡大に応じて選択できることを意味します。

セキュリティがしっかりと確保された環境は、自ずとコンプライアンスに準拠した環境となります。AWS には多数のコンプライアンスに対応可能なサービスがあり、AWS クラウド環境上に構築したお客様の規制対象ワークロードに使用することができます。これらの機能を使用すると、より高いレベルのセキュリティをよりスケーラビリティを確保しながら実現できます。クラウドベースのコンプライアンスは、高い監視機能、セキュリティ管理、および一元的な自動化機能を提供することで、導入コストの削減、運用の容易化、アジリティの向上を実現させることができます。

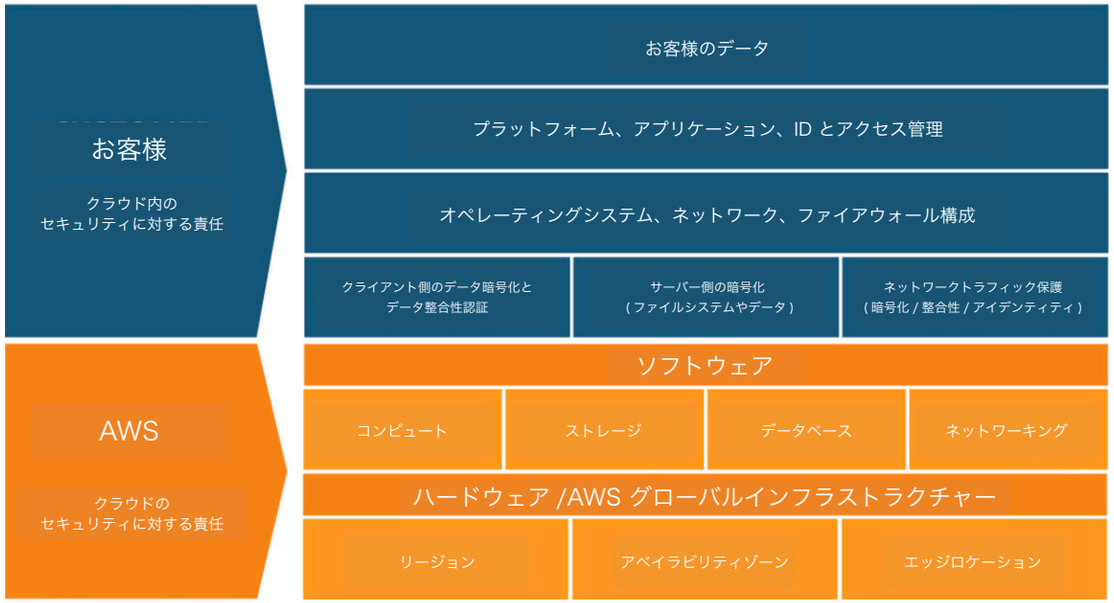
AWS を使用すると、AWS が既に AWS 環境内で運用している数多くのセキュリティ管理策を活用可能なため、お客様側で継続しなければならないセキュリティ管理が結果として減少する利点があります。お客様独自のコンプライアンスプログラムおよび認証プログラムが強化され、同時に特定のセキュリティ保証要件を維持・実施するためのコストを下げることができます。

我々は積極的な姿勢で
AWS プラットフォーム上で、
最もクリティカルな本番環境の
ワークロードの一部をデプロイ
可能であることを評価しています。
これは非常に革新的なことです

ロブ・アレクサンダー 氏
CIO, キャピタル ワン

責任共有の方法

責任共有モデル



IT インフラストラクチャーを AWS に移行する際は、左に示す責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムおよび仮想レイヤーから、サービスが運用されている施設の物理セキュリティに至るまで、IT コンポーネントの各レイヤーの運用、管理、および統制が AWS の責任範囲となり、そのためお客様の運用上の負担が軽減されます。AWS の責任範囲はクラウド環境自体のセキュリティ、お客様の責任範囲はクラウド環境上のセキュリティとなります。

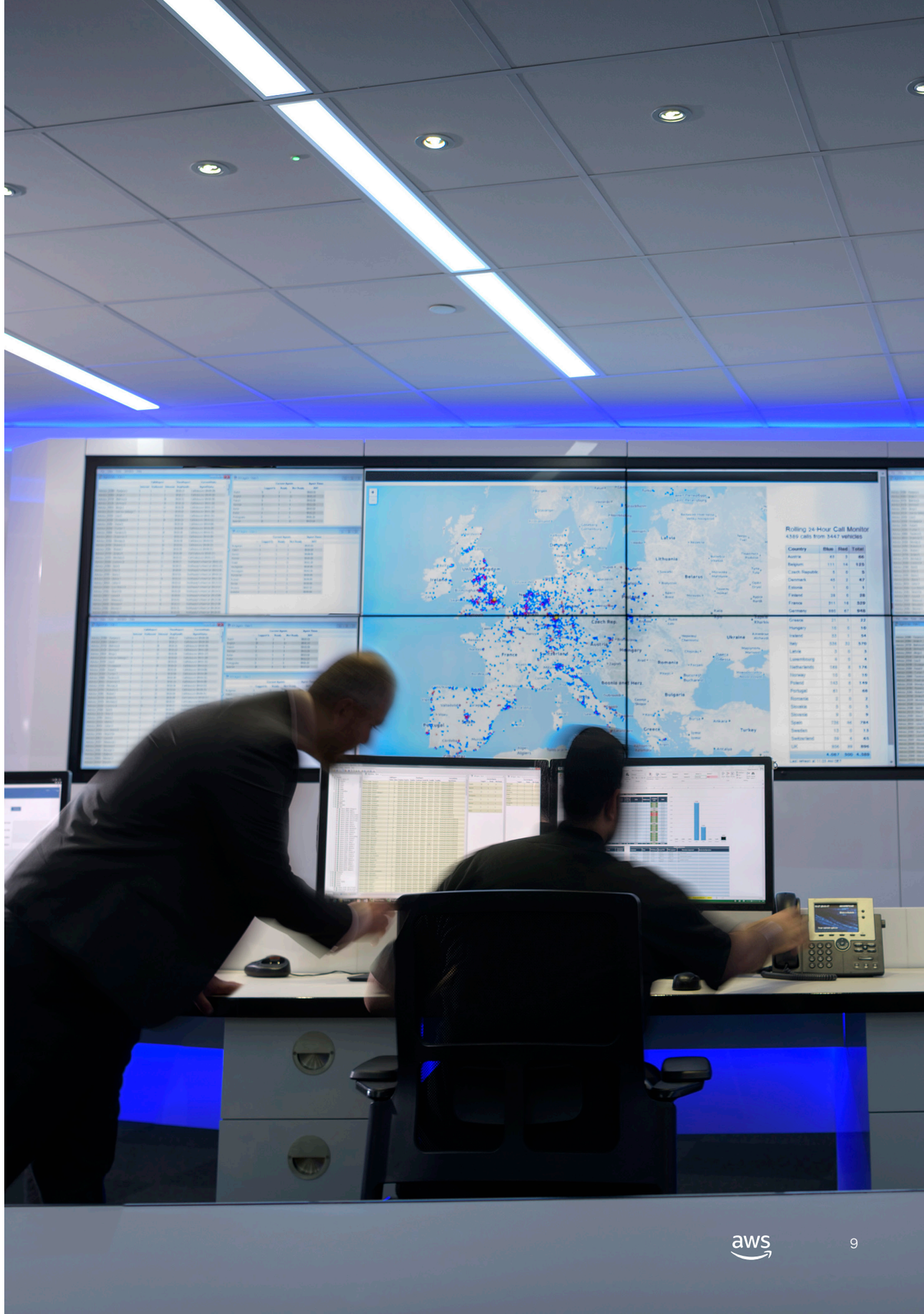
また、IT 環境の運用の責任共有と同様に、IT 統制の管理、運用、および検証も AWS と分担されます。

AWS: クラウド自体のセキュリティ

AWS では、お客様に AWS のセキュリティ管理フレームワークを最大限に活用いただけるように、プライバシーおよびデータ保護における国際的なベストプラクティスを採用したセキュリティ保証プログラムを策定しています。

AWS のユビキタスな統制環境は、世界各国にまたがる AWS のサービスおよび施設で有効に運用されています。この環境が維持されていることを検証するために、AWS では第三者による独立した評価を実施しています。AWS の統制環境には、Amazon 全体の統制環境の様々な側面を活用した方針、プロセス、および統制活動が含まれています。

この集合的統制環境は、AWS の統制フレームワークの運用の有効性を支える環境を確立し、それを維持するために必要な人員、プロセス、およびテクノロジーを網羅しています。私たちは、クラウドコンピューティング業界の主要団体が特定したクラウド固有の統制項目について、適用可能なものを AWS の統制環境に取り込んでいます。AWS は、お客様が導入可能なベストプラクティスを特定するため、そしてお客様の統制環境の管理をよりよく支援するために、こうした業界団体の動向を注視しています。



AWS では、お客様が業界および行政の要件に準拠していることを検証しやすいように、私たちのコンプライアンス体制を公開しています。AWS は、外部認証機関および独立監査人と連携し、AWS が確立・運用している方針、プロセス、および統制に関する詳細な情報をお客様に提供しています。お客様はこれらの情報を使用して、適用されるコンプライアンス基準で必要とされる統制の評価と検証の手順を実施することができます。

お客様は、AWS が提供するリスクおよびコンプライアンス計画に関する情報を、お客様のコンプライアンスフレームワークに取り込むことができます。AWS では、何千ものセキュリティ管理策を使用して、国際的な標準やベストプラクティスの遵守を監視しています。また、お客様の環境のセキュリティとコンプライアンスを監視するために、AWS Config などのサービスを提供しています。

AWS Config

AWS Config は、セキュリティと規制の準拠を実現するために AWS リソースインベントリ、構成履歴、および構成変更通知を提供する完全マネージド型サービスです。

AWS Config を使用すると、既存または削除済みの AWS リソースを検出したり、規則への全般的な適合状況を判別したり、あらゆる時点におけるリソースの詳細構成を掘り下げて調べたりすることができます。AWS Config によって、コンプライアンス監査、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を行うことができます。

お客様：クラウド内のセキュリティ

お客様の責任範囲としては、従来のデータセンターの場合と同じようにゲストオペレーティングシステムの管理（アップデートやセキュリティパッチのインストール）、そして関連アプリケーションソフトウェアの管理や、AWS より提供されるセキュリティグループファイアウォールの設定などが挙げられます。お客様の責任範囲は、使用する AWS のサービス、それらのサービスをお客様の IT 環境に統合する方法、適用される法規制に応じて異なります。

AWS リソースを安全に管理するために、次の 3 つのことを行う必要があります。

- 使用中のリソースを把握する（資産インベントリ）
- リソース上のゲスト OS およびアプリケーションのセキュリティを設定する (セキュリティ構成設定、パッチの適用、およびマルウェア対策)
- リソースへの変更を管理する（変更管理）

AWS Service Catalog

AWS Service Catalog を使用すると、AWS での使用が承認された IT サービスのカタログを作成および管理できます。この IT サービスには、仮想マシンイメージ、サーバー、ソフトウェア、データベースから包括的な多層アプリケーションアーキテクチャまで、あらゆるものが含まれます。AWS Service Catalog では、一般的に展開された IT サービスを集中管理でき、一貫性のあるガバナンスを実現し、コンプライアンス要件を満たすと同時に、ユーザーは必要な承認済みの IT サービスのみをすばやく展開できます。

Amazon GuardDuty

Amazon GuardDuty は、脅威の検知と共に、悪意のある操作や不正な動作に対する継続的なセキュリティの監視を行います。これにより、お客様による AWS アカウントとワークロードの保護が容易になります。このサービスでは、潜在的なアカウント侵害、侵害された可能性のあるインスタンス、攻撃者による偵察行為を示すアクティビティ、および知的財産などが監視の対象となります。また、データアクセスアクティビティの異常が継続的に監視され、不正アクセスや不注意によるデータ漏洩が検出されます。

保証プログラム

AWS 保証プログラムは、「認証 / 証明」、「法律 / 規制 / プライバシー」、および「準拠 / フレームワーク」の 3 つのカテゴリに分かれています。

保証プログラム

「認証 / 証明」は、第三者の独立監査人によって評価されます。AWS の認定書、監査報告書、または準拠証明書は、この監査人の評価結果に基づいています。

「法律 / 規制 / プライバシー」および「準拠 / フレームワーク」は、お客様の業界または職務に固有のものです。AWS は、コンプライアンス計画書、マッピング用資料、ホワイトペーパーなどの支援文書やセキュリティ機能を提供することによってお客様をサポートします。

これらの法律、規則、プログラムへの AWS の準拠は、正式なものではありません。これは、クラウドサービスプロバイダーが認証の対象でないか、認証が AWS の正式な上位認証 / 証明プログラムで既に対象となっているためです。

グローバル

CSA クラウドセキュリティアライアンス統制	ISO 9001 世界品質基準	ISO 27001 セキュリティ管理統制	ISO 27017 クラウド固有統制	ISO 27018 個人データ保護
PCI DSS レベル 1 ペイメントカード基準	SOC 1 監査統制報告書	SOC 2 セキュリティ、可用性、機密性報告書	SOC 3 全般統制報告書	

米国

CJIS 刑事司法情報サービス	DoD SRG DoD データ処理	FedRAMP 政府データ基準	FERPA 教育プライバシー法	FFIEC 金融機関規制
FIPS 政府セキュリティ基準	FISMA 連邦情報セキュリティマネジメント	GxP 品質のガイドラインと規制	HIPAA 保護されるべき医療情報	ITAR 国際武器規制
MPAA 保護されるべきメディアコンテンツ	NIST アメリカ国立標準技術研究所	SEC Rule 17a-4(f) 金融データ基準	VPAT / Section 508 アクセシビリティ基準	

アジア太平洋

FISC [日本] 金融情報システム	IRAP [オーストラリア] オーストラリアセキュリティ基準	K-ISMS [韓国] 韓国情報セキュリティ	MTCS Tier 3 [シンガポール] 多層クラウドセキュリティ基準	マイナンバー法 [日本] 個人情報保護

欧州

C5 [ドイツ] 運用のセキュリティの証明	Cyber Essentials Plus [英国] サイバー脅威防御	ENS High [スペイン] スペイン政府基準	G-Cloud [英国] 英国政府基準	IT-Grundschutz [ドイツ] ベースライン保護の概要

AWS の環境は常に監査され、AWS のインフラストラクチャーおよびサービスは、以下に示すものを含め、様々な地域および業界にわたる複数のコンプライアンス基準と業界認定に基づいて運用されています。お客様はこれらの認証を使用して、AWS のセキュリティ統制の実装と有効性を検証できます。AWS ではプログラムを継続的に追加しているため、最新の一覧については AWS コンプライアンスプログラムの Web サイトを参照してください。

PCI DSS

AWS は PCI DSS（Payment Card Industry Data Security Standard）に準拠するサービスプロバイダーです（2010 年から)。したがって、お客様が AWS 製品およびサービスを使用してカード所有者のデータを保管、処理、または送信する場合、お客様が自社の PCI DSS コンプライアンス認証を管理する際に AWS のテクノロジーインフラストラクチャーを信頼することができます。

ISO 27001

ISO 27001 は、情報セキュリティ管理システムの要件の概略を示す、広く採用されているグローバルセキュリティ標準であり、定期的なリスク評価に基づく企業情報および顧客情報を管理するための体系的な手法を提供します。

AWS Artifact

AWS Artifact は、AWS Management Console から利用可能なコンプライアンス自動報告ツールです。AWS Artifact を使用すると、2,500 以上のセキュリティ管理に関する報告書とその詳細を調査およびダウンロードできます。

AWS Artifact では、セキュリティおよびコンプライアンス文書（監査アーティファクトとも呼ばれます）にオンデマンドでアクセスできます。このアーティファクトを使用して、監査人または監査機関にお客様の AWS インフラストラクチャーやサービスのセキュリティおよびコンプライアンス情報を示すことができます。

監査アーティファクトの例としては、System and Organization Controls（SOC）報告書や Payment Card Industry（PCI）報告書などが挙げられます。

ISO 27017

ISO 27017 はクラウドコンピューティングの情報セキュリティの側面に関するガイダンスであり、ISO 27002 標準と ISO 27001 標準のガイダンスを補足して、クラウド固有の情報セキュリティ管理の実装を推奨しています。この実践規範は、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管理に関する実装ガイダンスを提供しています。AWS は、この ISO 27017 のガイダンスを遵守することにより、AWS が国際的に認知されているベストプラクティスへの対応に継続的に取り組み、クラウドサービスに特化した非常に正確な管理体制を備えていることを実証しています。

ISO 27018

ISO 27018 は、クラウドにおける個人データの保護に焦点を合わせた実践規範です。情報セキュリティ標準である ISO 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 27002 統制の実践ガイダンスを提供しています。AWS は、この国際的に認知されている実践規範を遵守し、独立した第三者機関からの評価を受けることにより、お客様のコンテンツのプライバシーと保護に関する AWS の取り組みを実証しています。

SOC

AWS System and Organization Controls（SOC）報告書は、AWS が重要なコンプライアンス管理および目標をどのように達成しているかを示す、独立した第三者による調査報告書です。

これらの報告書の目的は、運用およびコンプライアンスをサポートするために確立された AWS の統制を、お客様およびお客様の監査人が理解しやすくすることです。AWS の SOC 報告書には次の 3 種類があります。

- **SOC 1:** 財務報告に係る内部統制（ICFR）に関連する可能性がある AWS の統制環境に関する情報のほかに、ICFR の有効性の評価に関する情報を提供します。
- **SOC 2:** お客様および業務上の必要性があるサービスユーザーに、システムセキュリティ、可用性、および機密性に関連する AWS の統制環境についての独立した評価を提供します。
- **SOC 3:** お客様および業務上の必要性があるサービスユーザーに、AWS の統制環境についての独立した評価を提供し、AWS の内部情報を開示せずにシステムセキュリティ、可用性、および機密性に関連する情報を提供します。

FedRAMP

FedRAMP は、セキュリティ評価、認証、および継続的な監視に関する基準を確保するための米国政府プログラムであり、NIST および FISMA で定義された管理基準に従っています。

AWS は、FedRAMP に準拠したシステムを提供しています。これらのシステムは、認証を付与され、FedRAMP のセキュリティ管理策に対処し、セキュアな FedRAMP リポジトリに登録されるセキュリティパッケージに必要な FedRAMP テンプレートを使用し、認定された独立第三者評価組織（3PAO）による評価を受け、FedRAMP による継続的な監視要件を維持しています。

DoD クラウドセキュリティモデル (CSM)

米国国防総省情報システム局（DISA）によって発行され、米国国防総省（DoD）セキュリティ要件ガイド（SRG）に文書化されているクラウドコンピューティングのための標準です。この標準は、DISA インパクトレベル（IL）による独自のアーキテクチャ要件を持つ DoD ワークロード所有者のための認証プロセスを提供します。

HIPAA

医療保険の相互運用性と説明責任に関する法令 (HIPAA) には、保護されるべき医療情報（PHI）を処理または保管する組織に対する厳格なセキュリティおよびコンプライアンス基準が盛り込まれています。AWS は、対象となる事業体および HIPAA の影響を受ける関係者が、安全な AWS 環境を活用して、PHI を処理、維持、および保管できるようにします。

コンテンツのセキュリティ保護

AWS はお客様のプライバシーに細心の注意を払っています。お客様コンテンツの所有権は常にお客様にあり、それらの暗号化、移動、保存管理もお客様に行っていただけます。AWS は、お客様が転送中や保存中のデータを簡単に暗号化でき、許可されたユーザーのみがデータにアクセスできるようするツールを提供します。

AWS CloudHSM

AWS CloudHSM サービスは、安全な鍵管理のために政府基準に基づいて設計および検証されたハードウェアセキュリティモジュール（HSM）内に暗号鍵を保護することを可能にします。データ暗号化に使用する暗号鍵を、お客様のみがアクセスできるように、安全に生成、保管、および管理できます。

サーバー側の暗号化

Amazon S3 で暗号化処理を管理する場合は、Amazon S3 のサーバー側の暗号化（SSE）を使用できます。データはお客様の要件に応じて AWS が生成した鍵またはお客様が提供した鍵のいずれかによって暗号化されます。Amazon S3 SSE を使用すると、オブジェクトを記述するときに追加の要求ヘッダーを追加するだけで、アップロード時にデータを暗号化できます。データの復号はデータの取得時に自動的に行われます。

AWS では、データプライバシーに関する現地法規制への準拠をお客様が管理できます。AWS のグローバルインフラストラクチャーは、お客様がデータの物理的な保管場所を完全に制御できるように設計されているため、データ保管場所に関する要件を満たすことが容易です。

注意：お客様およびエンドユーザーに AWS のサービスを提供する以外の目的で AWS がお客様のコンテンツにアクセスしたり使用したりすることはありません。マーケティングや広告などの独自の目的でお客様のコンテンツを使用することは一切ありません。

AWS では、お客様のデータにアクセスしているユーザーや、組織が使用しているリソースを、あらゆる時点で把握できます。ID とアクセス権限のきめ細かな管理と、ほぼリアルタイムでのセキュリティ情報の継続的な監視とを組み合わせることにより、世界のどこに情報が保管されているかにかかわらず、適切なリソースに常にアクセスできます。

AWS Identity and Access Management

Identity and Access Management（IAM）は、AWS のサービスやリソースへのアクセスの安全な管理を可能にします。IAM を使用することで、管理者は AWS ユーザーおよびグループを作成して管理し、権限を使用して AWS リソースへのアクセス可否を決定することができます。フェデレーションでは、IAM ロールをセントラルディレクトリサービスのアクセス許可にマッピングできます。

Amazon Macie

Amazon Macie は、機械学習によって、機密データを自動的に検出、分類、保護します。Amazon Macie では、個人情報（PII）や知的財産などの機密データが認識されます。また、データアクセスアクティビティの異常が継続的に監視され、不正アクセスや不注意によるデータ漏洩が検出されます。

AWS のアクティビティ監視サービスは、システム全体の構成変更とセキュリティイベントを検知するため、リスクを低減して規模を拡大することが可能になります。さらに、お客様の既存のソリューションと AWS のサービスを統合して、運用やコンプライアンス報告作成を容易にします。

AWS はお客様のコンテンツを開示しません。ただし、政府または規制機関の拘束力のある有効な命令または法律に従う必要がある場合はこの限りではありません。コンテンツを開示する必要がある場合、開示からの保護を求めることができるように、お客様に最初に通知します。

重要：AWS からお客様への通知が禁止されている場合、または Amazon 製品またはサービスの使用をめぐる違法行為の兆候が明らかな場合、AWS はコンテンツを開示する前にお客様に通知しません。

AWS Directory Service for Microsoft Active Directory

AWS Microsoft AD を使用すると、AWS クラウドで Microsoft Active Directory をセットアップして実行することや、オンプレミスの既存の Microsoft Active Directory と AWS のリソースを接続することが容易になります。

フェデレーションユーザーアクセス

フェデレーションユーザーは、AWS アカウントを持たないユーザー（またはアプリケーション）です。ロールを使用すると、フェデレーションユーザーに対して AWS リソースへのアクセス権を一定時間付与することができます。この方法は、Microsoft Active Directory、LDAP、Kerberos などの外部サービスを使用した認証が可能な AWS 以外のユーザーが存在する場合に役立ちます。

AWS CloudTrail

AWS CloudTrail は、AWS の API 呼び出しを記録し、呼び出し側の ID、時間、ソース IP アドレス、要求パラメーター、および応答要素を含むログファイルを提供します。CloudTrail が提供する呼び出し履歴を使用することで、セキュリティ分析、リソース変更追跡、およびコンプライアンス監査を行うことができます。

コンテンツが格納される場所

AWS のデータセンターは、世界中の様々な国にクラスターとして構築されています。各国に存在する個々のデータセンタークラスターは、AWS リージョンと呼ばれます。お客様は世界各地の多数の AWS リージョンにアクセスでき、1 つの AWS リージョンを使用するか、すべての AWS リージョンを使用するか、あるいは AWS リージョンをいくつか組み合わせて使用することができます。

データを物理的に格納する AWS リージョンについては、お客様が完全に管理することができるため、お客様のコンプライアンス要件やデータ保管場所の要件を容易に満たすことができます。たとえば、欧州のお客様の場合は、AWS のサービスを EU（フランクフルト）リージョンでのみ展開することを選択できます。このような選択をした場合、お客様が別の AWS リージョンを選択しない限り、コンテンツはドイツ国内にのみ格納されます。

事業継続性

AWS のインフラストラクチャーには高水準の可用性が備わっており、回復力のある IT アーキテクチャを展開するために必要な機能を提供しています。AWS のシステムは、お客様への影響を最小限に抑えて、システム障害またはハードウェア障害への耐性を持つように設計されています。

AWS クラウドは、通知を受けたときに規模を拡大する「パイロットライト」環境や、高速フェイルオーバーが可能な「ホットスタンバイ」環境などの、よく知られた多数の災害復旧アーキテクチャに対応しています。

押さえるべきポイント

- すべてのデータセンターがお客様にサービスを提供するために稼働しており、停止中のデータセンターはありません。障害発生時は自動プロセスによって、影響を受ける領域の外部にデータトラフィックを移動させます。
- アプリケーションを複数の AWS アベイラビリティーゾーンに分散させることにより、自然災害やシステム障害といった甚大な障害モードに直面しても回復力を維持できます。
- 複数の AWS アベイラビリティーゾーンで複数のインスタンスを使用し、非常に高水準の目標復旧時間と目標復旧地点を達成するようなデータ複製方法を使用することで、回復力の高いシステムをクラウド内に構築できます。
- AWS インフラストラクチャーに構築した情報システムのバックアップとリカバリの管理およびテストについては、お客様の責任範囲となります。AWS インフラストラクチャーを使用することで、第 2 の物理サイトへのインフラストラクチャー投資を行うことなく、重要な IT システムの迅速な災害復旧を実現することができます。

詳しくは、*aws.amazon.com/jp/disaster-recovery* を参照してください。

自動化

AWS のセキュリティタスクを自動化することで、手動による設定ミスを減らし、チームが業務に不可欠な他の作業に集中する時間を確保することで、セキュリティをさらに高めることができます。お客様のセキュリティチームは、セキュリティの自動化と API 統合を使用して応答性と俊敏性を高め、開発者や運用チームとの緊密な連携を容易にして、コードをより迅速かつ安全に作成して展開することができます。

新しいコードを展開するたびにインフラストラクチャーとアプリケーションのセキュリティチェックを自動化することで、セキュリティおよびコンプライアンス統制を継続的に適用でき、機密性、一貫性、および可用性を常に確保できるようになります。AWS の情報管理ツールとセキュリティツールを使用してハイブリッド環境内を自動化することで、オンプレミス環境およびレガシー環境のシームレスかつ安全な拡張機能として AWS を容易に統合できます。

Amazon Inspector

Amazon Inspector は、AWS に展開されたアプリケーションのセキュリティとコンプライアンスを向上させるための自動セキュリティ評価サービスです。Amazon Inspector は、脆弱性やベストプラクティスからの逸脱について、アプリケーションを自動的に評価します。評価の実行後には、重大度で優先順位付けしたセキュリティに関する所見の詳細リストを生成します。

お客様がすぐに利用できるように、Amazon Inspector には、共通のセキュリティベストプラクティスや脆弱性の定義に対応した、何百ものルールが収められたナレッジベースが備えられています。組み込まれたルールの一例として、リモートルートログインが有効になっているかどうかまたは脆弱なソフトウェアがインストールされていないかどうかをチェックするものがあります。これらのルールは AWS のセキュリティ研究者によって定期的に更新されています。

リソース

パートナーおよび Marketplace

AWS パートナーネットワーク（APN）ソリューションを使用すると、自動化と俊敏性を実現し、ワークロードに応じて規模を拡張し、必要な分あるいは使った分のみを支払うことができます。

AWS Marketplace では、SaaS（Software as a Service）製品などのクラウド対応のソフトウェアソリューションを、わずか数分で簡単に検索し、購入して展開し、管理できます。これらのソリューションを連携させると、様々なワークロードやユースケースに利用できるソリューションによって、オンプレミス環境では不可能な方法でお客様のデータを保護することができます。

詳しくは、*aws.amazon.com/jp/partners* および *aws.amazon.com/marketplace* を参照してください。

トレーニング

AWS トレーニングは、クラウド初心者の方、既存の IT スキルを上積みしたい方、あるいはクラウドの知識にさらに磨きをかけたい方が、クラウドの理解を深め、クラウドをさらに効果的に使用できるようお手伝いします。

詳しくは、*aws.amazon.com/jp/training* を参照してください。

クイックスタート

クイックスタートを使用すると、ベストプラクティスに従って AWS のセキュリティ設定を開始でき、コンプライアンス要件を満たすための確固たる基盤を迅速に築くことができます。

詳しくは、*aws.amazon.com/jp/quickstart* を参照してください。