AWS FinTech

リファレンス・アーキテクチャー

日本版

コンプライアンス・セキュリティの標準化と自動化

2018 年 1 月

注意

本書は、情報提供の目的のみのために提供されるものです。本書の発行時点における 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。本書のいかなる内容も、AWS、その関係者、サプライヤー、またはライセンサーからの保証、表明、契約的責任、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 契約により規定されます。本書は、AWS とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。

目次

要約

この文書は、AWS 環境上に、日本の金融関連規制やガイドライン、およびその他の必要とされる各種の要求事項に従ってシステムを構築するためにセキュリティやコンプライアンスの統制を実装している、あるいは実装を計画しているアマゾン ウェブ サービス (AWS) のお客様を対象としています。本文書ではAWSの金融規制・関連ガイドラインやセキュリティ・コンプライアンスの知見、最新のクラウド環境のテクノロジー、および現時点での金融機関のお客様が参照される各種ガイドラインの主な要求事項等を網羅的に整理検討し、AWS環境上に日本のFinTech向けのシステム環境をセキュアかつコンプライアントに迅速に展開することができるソリューションとして、「AWS FinTech リファレンス・アーキテクチャー 日本版」に関して解説し、その基本的なコンセプトや概要について参考情報を提供しています。この取り組みは、金融機関やFinTechのお客様がよく参照されるコンプライアンスやセキュリティ面での要求事項を責任共有モデルに従って整理し、その各種要求事項を満たすためのAWSに関連する情報、お客様の対応や実装が必要となる箇所の情報、推奨される追加の実施事項、また、AWSのサービスやオプションに関するテクノロジーの構成情報を実装したAWS CloudFormationのテンプレート等をAWSのベストプラクティスとして参考情報という形でお客様に提供するものです。本文書は、IT 部門のエンジニア、意思決定者およびセキュリティやコンプライアンス担当者向けに幅広い内容を網羅していますが、基本的なネットワーキング、オペレーティングシステム、データ暗号化、および運用上のセキュリティや特定のコンプライアンス要件等の一般的な知識にある程度精通していることを前提としています。

はじめに

アマゾン ウェブ サービス（以下AWS）では、日本におけるFISC安全対策基準へのリファレンス文書作成や、米国におけるFFIECへの監査ガイドライン文書等、AWS環境に関連した各国の金融規制や各種セキュリティ、コンプライアンスに関する情報をお客様に提供してきました。また、AWSではSOC1、SOC2、PCI DSS、ISO27001、ISO27017、ISO27018 等、AWS環境に関連した第三者監査レポートや第三者認証に関する情報を通じて、AWSの統制についても継続してお客様に情報を提供しています。そうしたこれまでのAWSの金融規制・関連ガイドラインやセキュリティ・コンプライアンスの知見、最新のクラウド環境のテクノロジー、および現時点での金融機関のお客様が参照される各種ガイドラインの主な要求事項等を網羅的に整理検討し、AWS環境上に日本のFinTech向けのベースライン・システム環境をセキュアに迅速に展開することができるソリューションとして、この度「AWS　FinTech リファレンス・アーキテクチャー 日本版」を作成し公開することになりました。コンプライアンス上の要求事項が、AWSのテクノロジーを活用してどのように満たされるのか、どのような構成が最適かという検討にはセキュリティやコンプライアンスに関する専門的な知識や経験、及びクラウドのテクノロジーに関する一定の理解が同時に必要となりますが、そうしたお客様の負担を軽減し、あらかじめ要求事項を満すように検討されたベースライン・システム環境をご活用いただくことで、日本の金融・FinTechビジネスの迅速な展開を支援させていただくことを目的とした取り組みです。

AWS FinTech リファレンス・アーキテクチャー 日本版

「AWS FinTech リファレンス・アーキテクチャー 日本版」は「AWS FinTech リファレンス・ガイド 日本版」と「AWS FinTech リファレンス・テンプレート 日本版」によって構成されています（図1-1参照）。「AWS FinTech リファレンス・ガイド 日本版」は、主なセキュリティ関連基準の各種項目を網羅的に整理し、各種要求事項を「AWSの該当事項」、「お客様の該当事項」、「推奨される追加の実施事項」として検討し、そうした要求事項に見合うようにAWSサービスの実装の対応を整理した文書です。「AWS FinTech リファレンス・テンプレート 日本版」は、そうして整理されたAWSサービスの実装や構成をAWS CloudFormationによって実装したテンプレートとシステム構成図となります。

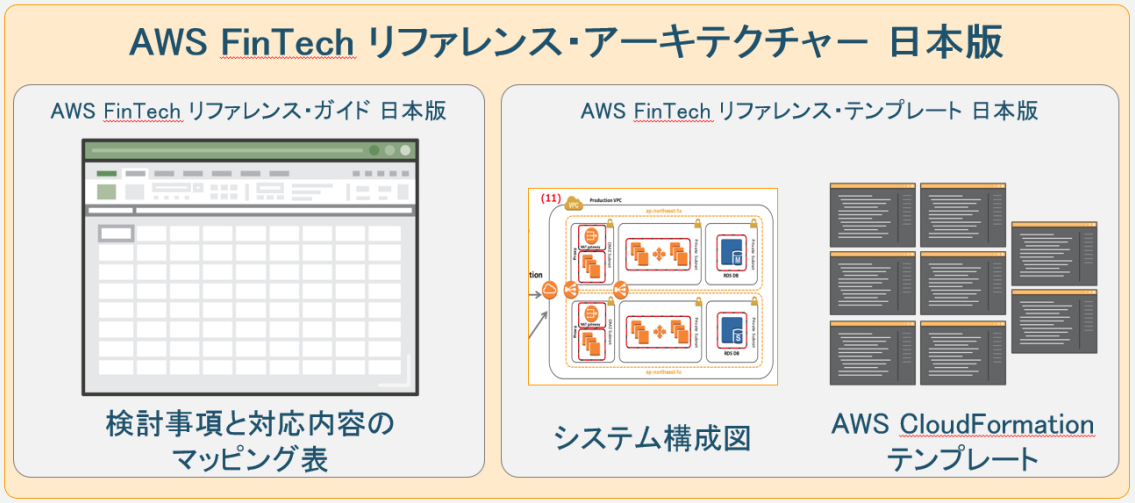

図1-1

AWS FinTech リファレンス・ガイド 日本版

特定のセキュリティやコンプライアンス等の要求事項に沿う形で検討され、作成された統制のフレームワークは、様々なシステム、業務アプリケーションを実装、運用する上でのコンプライアンス対応の効率化に貢献することになります。AWS FinTech リファレンス・ガイド 日本版では、AWSがこれまでにホワイトペーパー等で解説をしてきた「ガバナンスの自動化」、「セキュリティ・バイ・デザイン」、「クラウド上でのセキュリティ監査」等のクラウド環境における新しいセキュリティやコンプライアンスの実装や確立手法に関する概念を基にし、FISC安全対策基準、FISC API接続チェックリスト（試行版）、PCI DSS v3.2、ISO27001等の要求事項を整理検討することで統制のためのフレームワークを検討しています。さらに、こうした要求事項を満たすためのAWSのサービスを活用した機能的な実装の対応を検討し、各種要求事項、AWSサービスの実装、実装したサービスのシステム構成図における該当箇所、といった形で整理した情報を提供しています。

AWS FinTech リファレンス・テンプレート 日本版

AWS 環境上に作成するシステムについてのセキュリティや統制のフレームワークを機能で実装していく際には、標準化（スタンダーダイズ）され、自動化（オートメーション）され、再現可能な（リピータブル）なアーキテクチャーを構築していくことが重要となります。「AWS FinTech リファレンス・テンプレート 日本版」は、「AWS FinTech リファレンス・ガイド 日本版」で整理されたAWSサービスの実装にあたって、「AWS Well-Architected フレームワーク」

の概念を活用してAWSの各種ベストプラクティスに従って実装したベースライン・アーキテクチャーをAWS CloudFormationのテンプレートとして具体的に提供するものです(図1-2参照)。お客様はこのテンプレートを活用することで、セキュリティやコンプライアンスの各種要件についてあらかじめ検討された環境を標準化された形で迅速に展開可能となります。

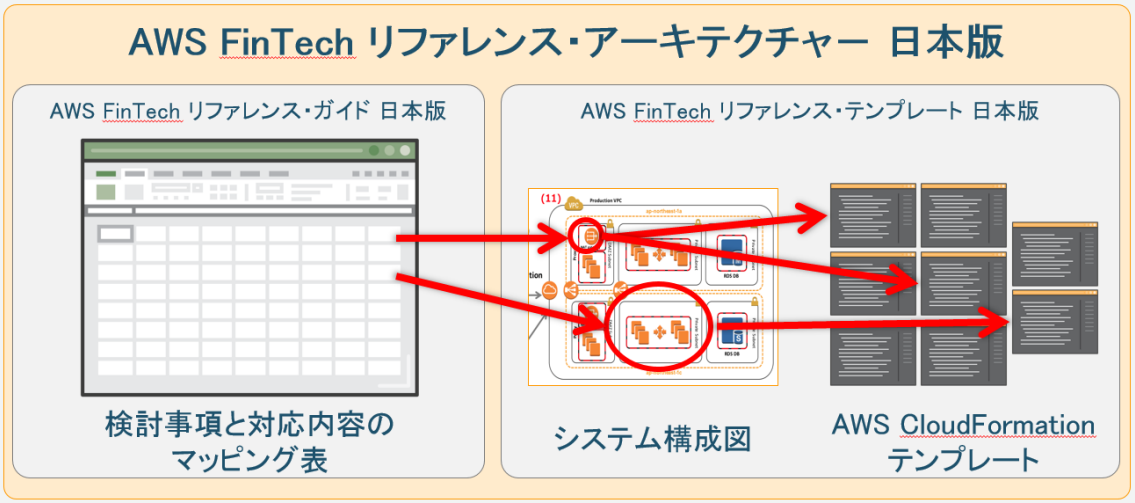

図1-2

AWS CloudFormationの詳細については下記を参照ください。

https://aws.amazon.com/jp/cloudformation/

AWS FinTech リファレンス・アーキテクチャーに関連する重要な概念

「AWS FinTech リファレンス・アーキテクチャー」のようなベースライン・アーキテクチャーを実装するためには、該当するコンプライアンスやセキュリティの要求事項に関する知識、AWSのセキュリティやコンプライアンス、ある

いはAWSのサービスに関する基本的な知識と理解、関連する情報を統合して整理検討しシステムを実装するための基礎的な概念等が必要となります。次の章から「AWS FinTech リファレンス・アーキテクチャー」についてベースとなった以下の重要な概念についてご説明します。

- AWSのセキュリティや統制環境に関する情報の検討とAWS 責任共有モデルにおけるAWS側の役割とお客様の役割の整理
- AWS 内でデプロイされているアプリケーションに対する最小限の設定要件を確立するためのアーキテクチャーベースラインの作成
- AWS Well-Architectedとセキュリティ・ピラーの概念

AWSのセキュリティとコンプライアンス

AWS 責任共有モデル

ITインフラストラクチャーをAWS 環境に移行する際、あるいはAWS環境上に新規に構築する際には、「責任共有モデル」という概念についてご理解いただくことが重要となります。「責任共有モデル」において、AWSの責任は安全性が高く統制されたプラットフォームの上で幅広い様々なサービスをユーザーに提供することにあります。また、お客様の責任は各々の用途に合わせた安全かつ統制された方法でAWS環境上にIT システムを構成し維持運用していくことにあります。AWSとお客様は「責任共有モデル」に基づき AWS環境上に構築されたお客様の IT 環境を分担して統制することになりますが、お客様は従来と同様にご利用になるIT環境全般に関する適切な統制を設計し、運用、維持、場合によっては見直しや改善を実施していく必要があります。

AWSの責任範囲について: Security OF the Cloud

AWSは、お客様のガバナンスフレームワークに AWS の統制をご理解いただいた上でAWSの環境を組み込むことができるように、AWSのIT 統制環境に関する幅広い情報をホワイトペーパー、レポート、認証書、第三者による監査レポート等を通じて提供しています。お客様はその内容について評価することでAWSの統制目標および統制に関する設計やその運用の有効性に関する合理的な確証を得ることが可能です。責任共有モデル、およびAWSのリスク管理プログラムやセキュリティポリシーについての詳細が必要なお客様は、下記の包括的な情報提供サイト参照ください。

https://aws.amazon.com/jp/compliance/
https://aws.amazon.com/jp/security/

お客様の責任範囲について: Security IN the Cloud

AWSのサービスを利用するにあたってのお客様の責任範囲は、使用するサービス、既存の 環境へのAWSサービスの統合方法やサービスの利用形態によります。また、適用される法律、規制、準拠する必要のある業種毎のガイドラインや認証等に応じても異なります。したがって、お客様には選択するサービスやその構成方法、利用方法等について、準拠するべき内容を満たすことが可能か、あるいは要求事項に見合った利用が可能かどうか、ご自身で注意深く検討していただく必要があります。

AWSが提供している監査レポートや認証書について

AWSでは監査レポートや認証についての幅広い情報をWEBサイトで公開しています。AWSの第三者監査レポートには、米国公認会計士協会AICPAのAT801および国際会計士連盟IFACのISAE3402に基づくSOC1レポート、および米国公認会計士協会AICPAのAT101に基づくSOC2やSOC3といったレポートが存在しています(2018年1月時点)。また、クレジットカードのデータの安全性に関するPCI DSS に関するレポートも利用可能です。ISO27001, ISO27017, ISO27018, ISO9001といった各種ISOに関するAWSに関する認証書もWEBサイトで提供しています。詳細は下記を参照ください。

https://aws.amazon.com/jp/compliance/
https://aws.amazon.com/jp/compliance/soc-faqs/
https://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/
https://aws.amazon.com/jp/compliance/iso-27001-faqs/
https://aws.amazon.com/jp/compliance/iso-27017-faqs/
https://aws.amazon.com/jp/compliance/iso-27018-faqs/
https://aws.amazon.com/jp/compliance/iso-9001-faqs/

AWS利用にあたってのセキュリティや統制に関する一般的な検証手順

1. AWSサービスを利用して構築するITシステム、および既存のITシステムとの統合が必要な環境の場合には、既存のIT環境とAWS上の環境全体を把握し、必要とされるシステムコンポーネントを整理し、アーキテクチャーを設計します。
2. 取り扱う業務やデータに従って必要とされるすべてのコンプライアンス、およびセキュリティ要件等を整理し、検討する項目を特定します。
3. 該当システムと適用されるコンプライアンスやセキュリティ要件、法令、などを照らし合わせて、すべてのコンプライアンス要件を満たすためAWSの責任部分、お客様の責任部分も含めてシステム全体の統制を設定し、要件を満たすために必要な確認事項と実施事項を特定します。
4. 検討項目を分析し、AWSに係る項目と、お客様に係る項目を整理し、責任共有モデルを参考にしてそれぞれの要件を明確化し、特定します。
5. AWSに関連する確認事項については、AWSのウェブサイト、ホワイトペーパー、認証書、第三者監査レポート等を利用し、必要な情報について確認します。お客様ご自身に関連する確認事項については、お客様ご自身で対応事項についての情報を確認します。
6. 必要となる実施事項については、システム的な実装が必要とされる個所と、オペレーション等の運用プロセス的な実装が必要とされる箇所を明確にします。システム的な実装でAWSに関連する箇所については、AWSサービスをどのように利用するべきか、どのような構成にするか、該当サービスに関するオプションの有効化、無効化等を検討し、実施事項に関する要件を満たすことが可能なシステムを実装していきます。AWSに直接関連しない、例えば業務アプリケーションの実装や、運用プロセス上必要となる実装等については、お客様ご自身で検討いただくことになります。
7. すべての統制項目とそれに該当する実施事項が有効かどうかをシステム全体で検討し、継続して評価していきます。

AWS環境上における監査について

クラウドにシステムを構築するお客様が増えるにつれ、クラウドコンピューティングの能力やクラウドコンピューティングの技術的な仕組みを活用した監査をどのように実施可能か等といった点について実務的に理解することが必要とされることも増えています。AWS 環境で提供される監査に活用可能なサービスを利用することでサンプルテストといった従来の手法から、包括的かつリアルタイムに近い監査やリスク管理を実施可能な環境に移行し、より精度の高い監査を実現可能となる場合もあります。こうした精度の高い監査が実現可能となった場合、従来とは異なった視点や利点が見いだせる可能性もあるでしょう。以下のような点がポイントとなりますが、詳細は下記のサイトの各種ホワイトペーパーを参照ください。

- 自動化 、標準化、スクリプトやAPIで実装可能なアーキテクチャー
- 検証可能 ― AWS CloudTrail、Amazon CloudWatch、AWS OpsWorks、AWS CloudHSM等を使用することで、監査に必要となる証拠の収集が可能です。

https://aws.amazon.com/jp/compliance/resources/

コンプライアンスとセキュリティを実装するためのアーキテクチャーの標準化

AWS 環境上に作成するシステムについてのセキュリティや統制のフレームワークを実装する際には、ある対象に一般的なシステム・ユースケースを特定し、標準化（スタンダーダイズ）され、自動化（オートメーション）され、再現可能な（リピータブル）なアーキテクチャーを構築していくことが重要です。標準化や自動化を推進することで、実績のあるベストプラクティスに従うことが可能となり、一定レベルの均一性や統一性が提供されることになります。結果として、お客様が AWS クラウド環境上でセキュアかつコンプライアントなシステムを構築するための基本的な要件を効率よく実現していくことに貢献することになります。

アーキテクチャーベースライン

AWS 内でのアーキテクチャーの標準化と自動化のための最善の方法を判断するには、事前にベースライン要件を確立します。これらは、ワークロードのほとんど (またはすべて) が準拠しなければならない最小限の共通要件です。企業のベースライン要件は通常、既存の遵守する必要のあるコンプライアンス統制、規制に関連するガイドライン、セキュリティ標準、およびベストプラクティスに沿ったものになるでしょう。一般的に、統制に係るコンプライアンス等の部門、デプロイされているシステムのモニタリング、監査、および評価にも関与する個人やチーム等が、ベースラインのコンプライアンスおよび運用要件に基づいて標準アーキテクチャーを確立することになります。

そうして作成された標準アーキテクチャーは、組織内の複数のアプリケーションやユースケースの間で共有することが可能となるでしょう。システムに求められるクオリティやセキュリティの面で一定の均一性がもたらされ、AWS 上の新しいアプリケーションのためのアーキテクチャーの設計にあたって、同様の確認を繰り返し実施するような労力や時間が削減可能となるでしょう。一元化されたクラウドモデルを持つ組織では、これらの標準アーキテクチャーがアカウントプロビジョニングまたはアプリケーションを実装していく際に活用されることで、コンプライアンス上の要求事項の遵守性やセキュリティポリシーに従ったセキュリティ機能の実装が確保されることになります。

AWS Well-Architected フレームワーク

AWS Well-Architected フレームワークは、AWS上にシステムを構築する際のアーキテクチャーに一定の原則をもたらすものです。この原則は、お客様がご自身の設計するアーキテクチャーについて優れたものであるかどうかを判断し、評価するために有益となります。アーキテクチャーそのものがAWSのベストプラクティスに従ったものであるか、改善が必要な箇所はどこか等といった点について一貫した手法で評価を実施することが可能となります。

AWSのソリューション・アーキテクトは、金融業界も含めて幅広い業界、様々なユースケースに関するアーキテクチャー上のソリューションの提供において、長年の経験があります。何千何万ものお客様のアーキテクチャーの設計とレビューを支援したその実務的な経験から、我々はクラウド上でシステム・アーキテクチャーを考える際のベストプラクティスと実効力のあるストラテ

ジーを確立しています。AWS Well-Architected フレームワークは、それらのベストプラクティスとストラテジーに基づくものです。我々は、質の高いシステムはビジネスの成功に大いに寄与し得るものと確信しています。

一般的な設計原則

AWS Well-Architected フレームワークは、汎用的な観点で利用可能なアーキテクチャーの諸原則を提供します。これらのアーキテクチャー原則は、クラウドにおける優れたシステムの設計を容易にするものです。

- 事前にキャパシティの予測が不要: クラウドでは、必要なときにより多くの、あるいはより少ないインフラストラクチャーリソースを利用可能であり、そうしたリソースの利用を適正に保つことが重要です。AWS環境ではこうした調整を自動的に行うことも可能です。
- 本番環境と同等の規模でテスト実施が可能: クラウドでは、本番規模のテスト環境を必要なときに作成し、テスト完了後に即座に削除することができます。必要な費用はテストを実行している時間分だけであり、オンプレミスにおけるテスト費用に比べ低コストで済みます。
- 自動化によりアーキテクチャーのテストが容易: オペレーションの自動化によって、低コストに同じ環境を自動的に複数作成する、あるいは複製することも容易です。手動操作による失敗の可能性がある手動作業を、リスクを気にしながら注意深く行う必要はありません。
- アーキテクチャーの進化: トラディショナルな環境では、アーキテクチャーの決定はしばしば静的な一度きりの出来事であり、システムはあまり変更されることはないでしょう。クラウドでは、自動化と必要に応じて適宜テス

トが可能なため、システム設計変更のリスクの低減が可能です。これによりシステムは時間とともに進化することが可能となり、イノベーションにつながることになります。

- データ・ドリブンなアーキテクチャー: クラウドでは、アーキテクチャーそのものがシステムワークロードにどのような影響を与えているかのデータを収集することができます。これにより、事実を元にした分析によるワークロードの改善が可能になります。
- Game dayテスティングを通じた改良: 実際の本番環境あるいは本番を想定した環境において、シミュレートされたイベントによる定期的なテストを行い、アーキテクチャーとプロセスがどのように振る舞い稼働するのかを確認してください。システムの改善点が把握できる他、問題解決に取り組む過程で組織的な経験値を得ることも可能です。

AWS Well-Architected フレームワークの 5 つのピラー

このフレームワークは、セキュリティ、信頼性、パフォーマンス効率、コスト最適化、運用性の5つのピラーで構成されています。ソリューション設計の際には、ビジネス的な背景を踏まえてこれらのピラーの間でトレードオフを考えることで、設計上の優先順位をつけることができます。例えば、開発環境では信頼性の代わりにコストを最適化したり、ミッションクリティカルなシステムではコストをかけても信頼性を向上させたりするでしょう。Eコマースのシステムでは、パフォーマンス効率が売上と顧客の購買傾向に影響を与えます。セ

キュリティと運用性については、一般的には他のピラーとのトレードオフは発生しません。この文書においてはセキュリティのピラーについてご紹介しますが、この概念はAWS FinTech リファレンス・アーキテクチャーを作成するにあたっても重要な働きをしています。

セキュリティ・ピラー

セキュリティ・ピラーの目的は、情報資産を保護し、リスク評価や緩和策を考慮することを通じて事業価値を確保することにあります。ここでは、安全なシステムをAWS環境上で設計するためのベストプラクティスを記述します。

システムのセキュリティを高めるためのアーキテクチャーに関する原則には以下のようなものが存在します。

- 強固なID基盤：最小権限の原則と権限分掌を実装し、AWSリソースへの操作を適切に認可します。集中的な権限管理で、クレデンシャルの長期保持への依存を減らします。
- トレーサビリティ：システム環境への操作や変更をリアルタイムで監視、通知、監査します。システムのログやメトリクスを統合することで自動的な対応を可能にします。
- 多層防御：単一層の保護に集中するのではなく、複数の層を保護することによってセキュリティ統制を行います。
- 自動化されたセキュリティベストプラクティス：ソフトウェアベースのセキュリティは、迅速かつ安価にスケールすることができます。バージョン管理されたテンプレートに基づくコードとして、安全な設計と統制の実装を定

義、管理します。

- 伝送中および保存されたデータの保護：重要度に応じてデータを分類し、適切に暗号化やトークン化することで、人間の操作によるデータの紛失や改変のリスクを低減します。
- セキュリティイベントへの準備：組織の要件に従い、インシデント管理プロセスを定義し、インシデントに備えます。インシデントレスポンス・シミュレーションや自動化ツールを利用して、検知・調査・復旧のスピードを早めます。

こうした原則をまとめると、セキュリティは以下の5つの領域から構成されることになります。

1. IDとアクセス管理
2. 発見的統制
3. インフラストラクチャー保護
4. データ保護
5. インシデントレスポンス

また、クラウド環境に移行する際には、前述のように「AWS責任共有モデル」を参照することにより、セキュリティやコンプライアンスの責任範囲や目的が明確になり、結果として要求事項等の達成の容易性につながることになります。AWSは物理的なインフラストラクチャーを保護する一方で、AWSのお客様はお客様に必要とされる目標そのものに集中できるからです。また、AWS環境では、セキュリティに関連するデータの可視性を高め、セキュリティイベントに対応する自動化された手段を提供するサービスも用意されています。

IDとアクセス管理

IDとアクセス管理では、適切にリソースへのアクセスの認証認可を行います。たとえば、ユーザー、グループ、サービス、ロールなどの主体を定義し、作成したポリシーをそれらの主体に関連づけ、強固なクレデンシャル管理を実現します。このような権限管理の形が認証認可の核となります。

AWSではAWS Identity and Access Management (IAM) により、適切なAWSクレデンシャルの保護が可能です。ルートユーザーなどの重要なアカウントには多要素認証 (MFA) を利用できます。また、SAML2.0などで既存のID基盤を用いたフェデレーションアクセスや、AWS Security Token Service (AWS STS) を用いた一時的なクレデンシャルによる認証も可能です。また、IAMロールやIAMポリシー、AWS Organizationsにより、最小権限の原則に基づいたきめ細やかな認可が実現できます。

発見的統制

潜在的なセキュリティ脅威やインシデントを特定するために発見的統制を実施します。発見的統制は、ガバナンスや品質、法務やコンプライアンス遵守、脅威の特定や対応の本質的要素です。たとえば、資産やその属性の棚卸により、運用ベースラインの確立する際に効果的な意思決定ができます。また、内部監査や情報システムへの統制を実施することで、日々の活動が組織のポリシーや要件を満たしているか、決められた条件の下、正しい自動通知環境が設定されているかを確認できます。これらの統制は、組織における正常ではない振る舞

いを検知すること、つまり異常検知による統制実現の重要な要素でもあります。AWSでは、Amazon CloudWatch Logsによるセキュリティログの取得や一元管理、Amazon Elasticsearch ServiceやAmazon EMR、Amazon Athenaなどのログ分析基盤、Amazon GuardDutyという脅威検知のマネージドサービスを提供しています。また、Amazon CloudWatch Eventsによる監視イベント、AWS Config Rulesによる構成変更イベント、Amazon Inspectorによるセキュリティ診断イベントなどをワークフローに統合することも可能です。

インフラストラクチャー保護

インフラストラクチャー（AWS環境上に作成するお客様の操作可能なインフラストラクチャー）保護は、ベストプラクティスや業界規制に準拠するために必要な統制で、多層防御アプローチなどが含まれます。これにより、不正アクセスや潜在的な脆弱性からシステムやサービスを保護します。たとえば、パケットフィルタリングなどの境界防御、要塞化やパッチ適用などのシステム構成管理、OSレベルの認証認可、Web Application Firewall (WAF) やAPIゲートウェイにおけるポリシー適用による保護が含まれます。AWSでは、Amazon VPC Security GroupsやNetwork ACLなどのファイアウォールによる境界防御、AWS Systems Managerによる安全なホストOS構成管理を提供しています。また、AWS WAFによるアプリケーション保護や、 AWS ShieldというDDoS攻撃緩和サービスも提供しています。

データ保護

セキュリティに影響を与える基本的な取り組みは、システム設計の前に行うべ

きです。たとえば、組織内のデータを重要度に基づいて分類し、暗号化することは、不注意や不正なアクセスからデータを保護できます。データ保護の仕組みにより、財務的損失からの保護や規制準拠という目的を達成しやすくなります。AWSでは、機械学習を用いてデータを分類するAmazon Macieというサービスを提供しています。また、重要なデータを暗号化する際の暗号鍵を効率的に管理できるAWS Key Management Service (AWS KMS) やAWS CloudHSMサービスも提供しています。伝送中のデータに関しては、電子証明書を発行・管理するAmazon Certificate Manager (ACM) を用い、SSL/TLS証明書をAmazon CloudFrontやELBに設定することで、安全な通信を実現できます。保存されたデータの暗号化に関しては、Amazon S3やAmazon EBS、Amazon RDSのサーバーサイド暗号化機能を有するものがあります。また、Amazon DynamoDBのように、クライアント側で暗号化したデータをサービス側に転送して利用するクライアントサイド暗号化が可能なサービスがあります。

インシデントレスポンス

成熟した予防的統制や発見的統制を実施したとしても、インシデントレスポンス計画を立てて、セキュリティインシデントによる被害を緩和する必要性は依然としてあります。AWS環境におけるワークロードの設計は、インシデント発生時のシステムの隔離や封じ込め、正常状態への復帰などの効果的な対応に大きく影響します。インシデントレスポンスに関する適切なツールやアクセス権を管理し、定期的にインシデントへの対応訓練をすることで、迅速な調査や復旧が確実になります。AWSでは、インシデント発生時の環境保全のため、クリーンルームとして隔離されたVPC環境を用意し、フォレンジック作業を行う

ことが可能です。フォレンジック対象となるディスクイメージを取得する場合は、Amazon EC2 APIやEBSスナップショット機能により、Amazon S3にイメージコピーします。クリーンルームVPCは、CloudFormationにより、必要なフォレンジックツールが事前構成された隔離環境を、テンプレートから簡単に構築し、インシデント対応チームのみがアクセスできるようAWS IAMでアクセス管理できます。

まとめ

AWS FinTech リファレンス・アーキテクチャー 日本版は、必要とされるコンプライアンス関連のドキュメントを参照し検討するための労力と、セキュアでコンプライアントなベースライン・アーキテクチャーの設計や評価に費やされる労力を低減します。これにより、お客様が本来実現したい業務やアプリケーションの設計や構築、およびすることを可能にします。システム環境全体のリスクを最小限化し、アーキテクチャー設計をシンプル化しながら、アプリケーションをデプロイするためのコスト、時間、および労力の削減に貢献することになります。ベースライン・アーキテクチャーの作成にあたっては、AWS Well-Architected フレームワークの原則全体、および、その中でも特にセキュリティ・ピラーの概念が活用されています。こうした原則はお客様が追加でアプリケーションを実装する場合や、アーキテクチャーを拡張する際にも同様に活用可能です。AWSのベストプラクティスを活用することで、お客様の情報資産を保護しながらビジネスへの貢献が可能なアーキテクチャーを迅速に展開することが可能となります。

本書執筆寄稿者

- 梅谷　晃宏

  本部長 日本・アジア太平洋地域担当　セキュリティ・アシュアランス本部
- 桐山　隼人

  シニアセキュリティソリューションアーキテクト　技術統括本部
- 塚田　朗弘

  シニアソリューションアーキテクト　技術統括本部