AWS リスクとコンプライアンスの概要

2017 年 1 月

注意

本文書は情報提供のみを目的としています。本文書は、発行時点における AWS の製品と対応を説明するものであり、予告なく変更される場合があります。お客様は、本文書の情報および AWS 製品またはサービスの利用について、ご自身の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、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」提供されます。本文書のいかなる内容も、AWS とその関係会社、サプライヤー、またはライセンサーからの保証、表明、および契約上の責任、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 とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

目次

要約

このホワイトペーパーでは、お客様が AWS 統制を評価するための基本的なアプローチを含め、AWS を既存の統制フレームワークに統合するための情報を提供します。

はじめに

AWS とお客様は、責任共有モデルに基づき IT 環境を統制することになります。AWS 側の責任は、安全性の高い、統制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ユーザーに提供することです。お客様側の責任は、用途に合わせて安全かつ統制された方法で IT 環境を構成することにあります。AWS はお客様に関わるセキュリティと統制環境について次のことを行います。

- インダストリー固有の認定と独立したサードパーティーによる証明を取得します (本文書で説明します)。
- AWS のセキュリティと統制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開します。
- 必要に応じ NDA に従って 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 セキュリティセンターを参照してください。

AWS コンプライアンスの詳細については、AWS コンプライアンスのページを参照してください。

また、AWS セキュリティプロセスの概要ホワイトペーパーでは、セキュリティ統制とサービス固有のセキュリティの概要について説明しています。

責任共有環境

IT インフラストラクチャを AWS に移行する際は、お客様に責任共有モデルを考慮していただく必要があります。この責任共有モデルでは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、AWS の責任範囲で様々なコンポーネントが運用、管理、コントロールされることになり、お客様の運用上の様々な負担の軽減にも貢献することになります。お客様の責任範囲としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理等、が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法律および規制に応じて異なります。したがって、お客様には選択するサービスを注意深く検討していただく必要があります。お客様は、ホストベースのファイアウォール、ホストベースの侵入検知／防御、暗号化とキー管理などのテクノロジーを利用してセキュリティを拡張し、より厳格なコンプライアンス要件を満たすことも可能です。こうした柔軟性とお客様自身による統制を可能とする責任共有モデルの特性により、特定のインダストリー固有の認証要件に適合するソリューションの実装が可能となっています。

お客様と AWS の責任共有モデルは IT 統制にも拡張されます。IT 環境を運用する責任を AWS とお客様の間で分担するのと同様に、IT 統制の管理、運用、検証も分担することになります。物理インフラストラクチャに関連した統制をお客様が管理していた場合は、AWS 環境にシステムをデプロイすることで AWS が管理することになり、お客様に関係する統制の負担が軽減されることになります。ただし、お客様によって AWS のデプロイ方法は異なります。特定の IT 統制の管理を AWS に移行することは、新しく分散型の統制環境を構築する作業と言えますが、これはお客様の判断で行うことができます。移行後は、AWS の統制とコンプライアンスの文書 (「AWS の認定とサードパーティーによる証

明」で説明します) を使用し、必要に応じて統制の評価と検証の手順を実行可能です。

厳格なコンプライアンス管理

IT システムのデプロイ方法にかかわらず、お客様はこれまでどおり、IT 統制環境全体に対する適切な管理を維持していただく必要があります。主な実施内容として、関連資料を基にしたコンプライアンスの目標と要件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づいた必要となる妥当性の把握、統制環境の運用の有効性の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が広がります。

お客様のコンプライアンスと管理が厳格な場合は、次のような基本的なアプローチも考慮可能です。

1. AWS から入手できる情報、およびその他の必要な情報をレビューして IT 環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。
2. 企業のコンプライアンス要件を満たす統制目標を設計し、実装します。
3. 社外関係者が行う統制を特定し、文書化します。
4. すべての統制目標が満たされ、すべての主な統制が設計され、その運用が有効的かどうかを検証します。

このような方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることもできます。

AWS 統制の評価と統合

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティーによる証明を通じて、AWS の IT 統制環境に関する幅広い情報をお客様に提供しています。本文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様に理解いただくために用意されています。また、この情報はお客様の（AWS 環境上に）拡張された IT 環境も含んだ統制が適切に機能しているかどうかを明らかにし、検証するのにも有効です。

従来、統制目標および統制に関する設計と運用効率の検証は、社内外の監査人がプロセスを実地検証し、証拠を評価することによって行われています。一般的に、お客様もしくはお客様の社外監査人による直接の監視または検証は、統制の妥当性を確認するために実施されます。AWS などのサービスプロバイダーを使用する場合、企業はサードパーティーによる証明および認定を要求し、評価することで、統制目標および統制に関する設計と運用効率の合理的な保証を得ることになります。その結果、お客様の主要な統制が AWS で管理されている場合でも、統制環境を統一されたフレームワークとして維持された上で、すべての統制が説明されているか、有効な統制が運用されているかどうか検証することができます。サードパーティーによる証明と AWS の認定によって、統制環境を高いレベルで検証できるだけでなく、AWS クラウドの自社の IT 環境に対して特定の検証作業を自社で実行されたいというお客様のご要望を実現できます。

AWS の IT 統制情報

AWS は、次の方法で IT 統制情報をお客様に提供します。

固有の統制定義。AWS のお客様は、AWS が管理することになる主要な統制を識別することが可能です。主要な統制とは、お客様の統制環境にとって必要不可欠なものです。例えば、年次の会計監査などのコンプライアンス要件に準拠するには、その主要な統制の運用の有効性について外部組織による証明が必要となります。そのために、AWS は Service Organization Controls 1 (SOC 1) Type II レポート（以下、Service Organizatin Controls 1 = SOC1）で幅広く詳細な IT 統制を公開しています。SOC 1 レポートの旧称は Statement on Auditing Standards (SAS) No. 70、Service Organizations レポートです。米国公認会計士協会 (AICPA) が作成し、幅広く認知された監査基準です。SOC 1 監査は、AWS で定義している統制目標および統制活動（AWS が管理するインフラストラクチャの一部に対する統制目標と統制活動が含まれます）の設計と運用の有効性の両方に関する詳細な監査です。「Type II」の表示は、レポートに記載されている各統制が、統制の妥当性に関して評価されるだけでなく、運用の有効性についても外部監査人によるテスト対象に含まれていることを示しています。AWS の外部監査人は独立し、適格な能力を有しているため、レポートに記載されている統制は、AWS の統制環境に高い信頼を置けることを示します。AWS の統制は、Sarbanes-Oxley (SOX) セクション 404 の財務諸表監査など、多くのコンプライアンス目的に合わせて検討、設計され、適切に運用されていると考えることが可能です。SOC 1 Type II レポートの利用は、一般的に他の外部認定機関からも許可されています (たとえば、ISO 27001 の監査人は顧客の評価を完成するために SOC 1 Type II レポートを要求する場合があります)。

他の固有の統制活動は、AWS の Payment Card Industry (PCI) および連邦情報セキュリティマネジメント法 (FISMA) のコンプライアンスに関連します。AWS は FISMA Moderate 基準と PCI Data Security 基準に準拠しています。これらの PCI 基準と FISMA 基準は非常に規範的であり、AWS がその公開基準に従っていることの独立した検証が求められます。

一般的な統制基準への準拠。包括的な統制基準が必要な場合には、AWS を特定の基準に従って評価することも可能です。AWS は幅広く包括的なセキュリティ基準に準拠し、安全な環境を維持するためのベストプラクティスに従っており、ISO 27001 認定を取得しています。AWS はクレジットカード情報を処理する会社にとって重要な統制に準拠しており、PCI Data Security Standard (PCI DSS) の認定を取得しています。AWS は米国政府機関から要求される幅広く詳細な統制に準拠しており、FISMA 基準に準拠しています。このような一般的な基準に準拠しているので、お客様は所定の統制およびセキュリティプロセスの包括的な特性について詳細な情報を得ることができます。また、コンプライアンスを管理するときに、それらの基準の準拠について考慮できます。

AWS のグローバルなリージョン展開

世界各地に設置されているデータセンター群は、所在地によりリージョンに分けられています。米国東部 (バージニア北部)、米国西部 (オレゴン)、米国西部 (北カリフォルニア)、AWS GovCloud (US) (オレゴン)、欧州 (アイルランド)、欧州 (フランクフルト)、アジアパシフィック (ソウル)、アジアパシフィック (シンガポール)、アジアパシフィック (東京)、アジアパシフィック (シドニー)、中国 (北京) リージョン、南米 (サンパウロ)。

AWS リージョンの最新の一覧については、AWS グローバルインフラストラクチャのページを参照してください。

AWS リスク/コンプライアンスプログラム

AWS では、お客様のガバナンスフレームワークに AWS 統制を組み込むことができるように、リスクおよびコンプライアンスプログラムに関する情報を提供しています。この情報をもとに、AWS に関する統制と管理フレームワーク全体を文書化し、フレームワークの重要な部分としてご利用いただけます。

リスク管理

AWS のシニアマネジメント層は、リスクを緩和または管理するために、リスクの特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、この戦略的事業計画を再評価します。このプロセスでは、シニアマネジメント層がその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。

さらに、AWS の 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標 (Control Objectives for Information and related Technology, COBIT) フレームワークに基づいて、情報セキュリティフレームワークとポリシーを確立しています。また、ISO 27002 の統制に基づいた ISO27001 認定フレームワーク、米国公認会計士協会 (AICPA) のトラスト・サービスの原則 (Trust Services Principles)、PCI DSS v3.1、および米国国立標準技術研究所 (NIST) 出版物 800-53 Rev 3 (連邦政府情報システムにおける推奨セキュリティ統制) を実質的に統合しています。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実施します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、第三者のセキュリティ事業者によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理された上で AWS のシニアマネジメント層に報告されます。これらのスキャンは、基礎となる AWS インフラストラクチャの健全性と（サービスの）実行可能性を確認するためのものであり、お客様固有のコンプライアンス要件に適合する必要のある、お客様自身の（インスタンスやその他の AWS 環境の設定に関する）脆弱性スキャンに置き換わることを意味するものではありません。お客様は事前に承認を得た上で、お使いの AWS インフラ環境にスキャンを実施することができますが、対象はお客様のインスタンスに限り、かつ AWS 利用規約に違反しない範囲とします。このようなスキャンについて事前に承認を受けるには、AWS 脆弱性/侵入テストリクエストフォームを使用してリクエストを送信してください。

統制環境

AWS は、Amazon 全体の統制環境の様々な側面を活用したポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスをセキュアに提供するために用意されています。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、テクノロジーを網羅しています。クラウドコンピューティング業界の主要機関が特定したクラウド固有の統制について、該当する項目を AWS の統制フレームワークに統合しました。AWS は、統制環境の管理についてお客様をより支援するために、先進的な取り組みとアイデアについて、こうした業界団体を継続的にチェックします。

Amazon の統制環境の策定は、当社のシニアマネジメント層を起点に開始されます。役員とシニアリーダーは、当社の文化と核となる価値を確立する際、重要な役割を担っています。各従業員に当社の業務行動倫理規定が配布され、定期的なトレーニングを受けます。確立されたポリシーを従業員が理解し、従っているかどうかを確認するために、コンプライアンス監査が実施されます。

AWS の組織構造が、事業運営の計画、実行、統制のフレームワークを支えています。この組織構造によって役割と責任が割り当てられ、適切な人員調達、運用の効率性、そして職務分担が構成されます。またシニアマネジメント層は、重要な人員に関する権限と適切な報告体系を構築しています。当社では従業員に対し、その職務と AWS 施設へのアクセスレベルに応じて、法律および規制が許可する範囲内での学歴、雇用歴、場合によっては経歴の確認を、採用手続きの一環として実施しています。新たに採用した従業員には体系的な入社時研修を行い、Amazon のツール、プロセス、システム、ポリシー、手順について熟知させるようにします。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実装しています。また、公開ウェブサイトでは、お客様がデータを保護するために有効な方法を解説したセキュリティホワイトペーパーを公開しています。

AWS へのお問い合わせ

AWS の独立監査人が発行したレポートや証明書の取り寄せ、または AWS のコンプライアンスの詳細についての質問は、AWS 日本担当チームおよび事業開発にお問い合わせください。お問い合わせ内容に応じて適切なチームに取り次ぎいたします。AWS のコンプライアンスの詳細については、AWS コンプライアンスサイトを参照するか、mailto:awscompliance@amazon.com まで質問を直接お送りください。

詳細情報

詳細については、以下のソースを参照してください。

- CSA Consensus Assessments Initiative Questionnaire
- AWS の認定、プログラム、レポート、およびサードパーティーによる証明
- 主要なコンプライアンスに関する質問と AWS の回答

ドキュメントの改訂

変更	説明
2017 年 9 月	日本語版発行
2017 年 1 月	新しいテンプレートに移行してください。
2016 年 1 月	英語初版発行