aws

Unable to locate subtitle

Amazon Web Services: リスクとコンプライアンス

Amazon Web Services: リスクとコンプライアンス: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services: リスクとコンプライアンス

公開日: 2021 年 3 月 11 日 (改訂履歴)

要約

AWS は、規制の厳しい業界を含むさまざまなお客様にサービスを提供しています。当社の責任共有モデルにより、お客様は IT 環境において効果的かつ効率的にリスクを管理できるようになります。また、確立され、広く認知されているフレームワークおよびプログラムによるコンプライアンスを通じて、効果的なリスク管理が保証されます。この文書では、責任共有モデルの AWS 側でリスクを管理するために AWS が実装したメカニズムと、これらのメカニズムが効果的に実装されていることを保証するためにお客様が活用できるツールについて概説します。

はじめに

AWS およびその顧客は、IT 環境を統制します。そのため、セキュリティは責任共有です。AWS クラウドでのセキュリティとコンプライアンスの管理に関しては、各当事者に明確な責任があります。お客様の責任は、使用しているサービスによって異なります。ただし、一般的に、お客様固有のセキュリティおよびコンプライアンス要件に沿った方法で IT 環境を構築する責任はお客様にあります。

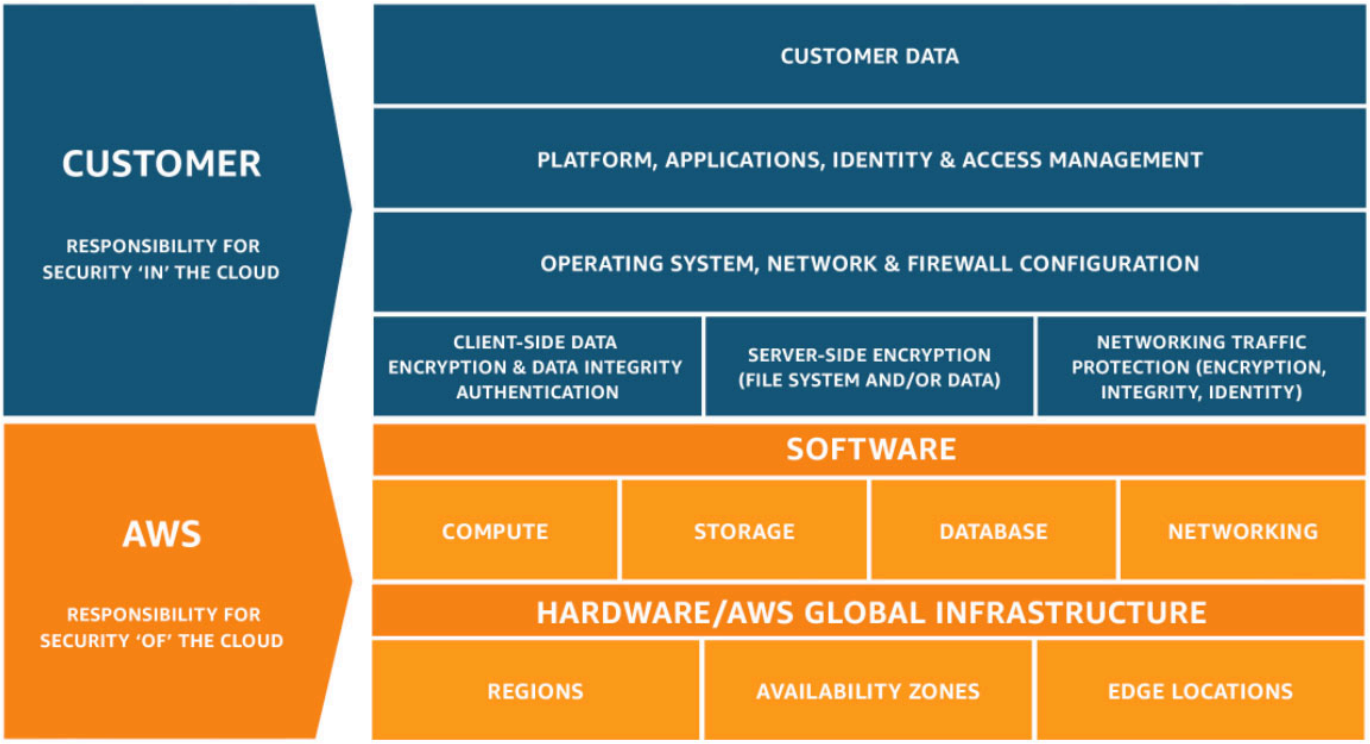
この文書では、各当事者のセキュリティにおける責任と、お客様が AWS リスクおよびコンプライアンスプログラムからどのようなメリットを得られるかについて詳しく説明しています。

責任共有モデル

セキュリティとコンプライアンスは AWS とお客様の間の責任共有です。デプロイするサービスによっては、この共有モデルによってお客様の運用上の負担を軽減できます。AWS が、ホストオペレーティングシステムや仮想化レイヤーから、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、さまざまなコンポーネントを操作、管理、および制御するためです。お客様の責任としては、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に加えて、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、および関係法令に応じて異なります。したがって、サービスの選択は慎重に行うことをお勧めします。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と防御、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、さらに厳格なコンプライアンス要件を満たすことができます。

この責任共有という特徴によって、業界固有の認定要件に適合するソリューションのデプロイを可能にする、柔軟性と顧客コントロールも提供されます。



このお客様と 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 とお客様の間で共有するのと同様に、IT 統制の管理、運用、および検証も責任共有となりま

す。AWS は、AWS 環境にデプロイされた物理インフラストラクチャに関連する統制を管理することで、お客様を支援します。お客様は AWS の統制およびコンプライアンスに関するドキュメントを使用して、必要に応じた統制の評価および検証手順を実行できます。特定の統制に対する責任が AWS とお客様の間でどのように共有されるかの例については、AWS 責任共有モデルをご覧ください。

AWS 統制の評価と統合

AWS は、技術文書、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、当社の IT 統制環境に関する幅広い情報をお客様にご提供しています。本ドキュメントは、お客様が使用する AWS の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ご理解いただくことをお手伝いするためのものです。この情報はまた、お客様の拡張された IT 環境内の統制が効果的に機能しているかどうかを明らかにし、検証するのにも有用です。

従来、内部監査人または社外監査人は、プロセスを実地検証し証拠を評価することによって、統制の設計と運用上の有効性を検証しています。お客様またはお客様の社外監査人によるこの種の直接の監視または検証は、一般的に、従来のオンプレミスデプロイにおける統制の妥当性を確認するために行われます。

サービスプロバイダー (AWS など) が使用されている場合、お客様は第三者の証明や認定をリクエストして評価できます。これらの証明と認定は、資格のある独立した第三者によって検証された統制目標と統制の設計と運用上の有効性を顧客が確認するのに役立ちます。その結果、一部の統制は AWS によって管理されているとしても、統制環境は統一されたフレームワークであり続け、お客様は、統制が効果的に機能しており、コンプライアンスレビュープロセスを迅速化していることを説明し検証できます。

AWS の第三者による証明と認定により、お客様は統制環境が可視化され、独立した検証が可能になります。このような証明と認定は、AWS クラウド内の IT 環境に対して特定の検証作業をお客様自身で実行するという要件の緩和に役立ちます。

AWS リスクおよびコンプライアンスプログラム

AWS は組織全体でリスクおよびコンプライアンスプログラムを統合しています。このプログラムは、サービスの設計とデプロイのすべての段階でリスクを管理し、組織のリスク関連活動を継続的に改善および再評価することを目的としています。AWS 統合型リスクおよびコンプライアンスプログラムの構成要素については、以下のセクションで詳しく説明します。

AWS ビジネスリスク管理

AWS にはビジネスリスク管理 (BRM) プログラムがあり、AWS の各部署と提携して、AWS の取締役会および AWS の上級管理職が AWS 全体の主要なリスクの全体像を把握できるようにしています。BRM プログラムは、AWS の機能に対する独立したリスク監督を行います。具体的には、BRM プログラムは以下を行います。

- AWS の主要機能分野のリスク評価とリスクモニタリングを実施
- リスクの特定と是正の推進
- 既知のリスクの登録の保守

リスクの是正を推進するために、BRM プログラムは取り組みの結果を報告し、必要に応じて事業全体のディレクターやバイスプレジデントにエスカレーションして、ビジネス上の意思決定を通知します。

業務管理と経営管理

AWS では、週、月、四半期ごとのミーティングとレポートを組み合わせて使用して報告し、とりわけ、リスク管理プロセスのすべての構成要素全体に確実にリスクを伝達しています。また、AWS はエスカレーションプロセスを導入して、組織全体で優先度の高いリスクを経営陣に可視化しています。これらの取り組みをまとめることで、AWS のビジネスモデルが複雑であっても、リスクが一貫して管理されるようになります。

さらに、連鎖的な責任体系により、バイスプレジデント (事業主) は事業の監督に責任を負います。このため、AWS は毎週ミーティングを実施して、運用メトリクスを確認し、ビジネスに影響が及ぶ前に主要な傾向とリスクを特定します。

役員とシニアリーダーは、AWS のカラーと中心的な価値を規定する際、重要な役割を担っています。各従業員には当社の業務行動倫理規定が配布され、従業員は定期的なトレーニングを受けます。制定されたポリシーの理解と遵守を従業員に徹底するために、コンプライアンス監査を実施します。

AWS の組織構造は、事業運営の計画、実行、統制のフレームワークを提供しています。この組織構造には役割と責任が含まれ、適切な人員配置、事業運営の効率化、そして職務の分離が可能となっています。さらに、主要人員に対する適切な報告体系も確立済みです。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、法律および規制が認める範囲での学歴、雇用歴、場合によっては経歴の検証を、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ます。

統制環境とオートメーション

AWS は、組織全体のリスクを管理する基本要素として、セキュリティコントロールを導入しています。AWS の統制環境は、AWS 全体で最低限のセキュリティ要件を実装するための基礎となる標準、プロセス、および構造で構成されています。

AWS の統制環境の一部として含まれるプロセスと標準は独立していますが、AWS は Amazon の全体統制環境の要素も活用しています。活用されるツールには次のようなものがあります。

- 職務の分担を管理するツールなど、Amazon のすべてのビジネスで使用されるツール
- 法務、人事、財務など、特定の Amazon 全体のビジネス機能

AWS が Amazon の全体的な統制環境を活用している場合、これらのメカニズムを管理する標準とプロセスは AWS のビジネスに特化して調整されます。つまり、AWS の統制環境内での使用と適用に対する期待事項は、Amazon 環境全体での使用と適用に対する期待事項とは異なる場合があります。AWS の統制環境は、最終的に AWS のサービスを安全に提供するための基盤として機能します。

統制のオートメーションは、AWS が統制環境を構成する特定の定期的なプロセスにおける人的介入を減らすための手段です。これは、効果的な情報セキュリティコントロールの実施とそれに伴うリスク管理の鍵となります。統制のオートメーションは、人間が繰り返しプロセスを実行すると必然的に発生する可能性のある、プロセス実行における潜在的な不整合を、予防的に最小限に抑えることを目指しています。統制のオートメーションにより、潜在的なプロセス偏差が排除されます。これにより、統制が設計どおりに適用されるという保証レベルが向上します。

AWS のエンジニアリングチームは、セキュリティ機能全体で AWS の統制環境をエンジニアリングし、可能なかぎり高いレベルの統制のオートメーションをサポートする責任を負っています。AWS で自動化された統制の例には、次のようなものがあります。

- ガバナンスと監督: ポリシーのバージョニングと承認

- 人事管理: トレーニングの自動配信、従業員の迅速な解雇
- 開発と設定管理: コードデプロイパイプライン、コードスキャン、コードバックアップ、統合デプロイテスト
- アイデンティティとアクセスの管理: 職務分離、アクセスレビュー、アクセス許可管理の自動化
- モニタリングとロギング: 自動ログ収集と相関付け、アラーム
- 物理的セキュリティ: ハードウェア管理、データセンターセキュリティトレーニング、アクセスアラーム、物理アクセス管理など、AWS データセンターに関連するプロセスの自動化
- スキャンとパッチ管理: 脆弱性スキャン、パッチ管理、デプロイの自動化

統制評価と継続的モニタリング

AWS では、AWS 環境内のリスクをさらに低減するために、サービスのデプロイの前後にさまざまなアクティビティを実施しています。これらのアクティビティでは、AWS の各サービスの設計および開発中にセキュリティとコンプライアンスの要件を組み込み、本番環境への移行 (ローンチ) 後にサービスが安全に稼働していることを検証します。

リスク管理とコンプライアンス活動には、2 つのローンチ前アクティビティと 2 つのローンチ後のアクティビティが含まれます。ローンチ前アクティビティは以下のとおりです。

- AWS アプリケーションセキュリティリスク管理レビューにより、セキュリティリスクが特定され軽減されたことを検証
- アーキテクチャ適性レビューにより、お客様がコンプライアンス体制との整合性を確保できるよう支援

サービスのデプロイ時には、AWS の高いセキュリティ基準を満たすために、詳細なセキュリティ要件に対する厳格な評価が実施されます。ローンチ後アクティビティは以下のとおりです。

- AWS アプリケーションセキュリティの継続的なレビューにより、サービスのセキュリティ体制が維持されていることを確認
- 脆弱性管理の継続的なスキャン

これらの統制評価と継続的なモニタリングにより、規制対象のお客様は、AWS のサービス上でコンプライアンスに準拠したソリューションを自信を持って構築できます。さまざまなコンプライアンスプログラムの対象範囲に含まれるサービスのリストについては、AWS 対象範囲内のサービスウェブページを参照してください。

AWS 認定、プログラム、レポート、および第三者による証明

AWS は定期的に独立した第三者による認証監査を受け、制御活動が意図通りに機能していることを保証しています。具体的には、AWS は、地域や業界に依存するさまざまなグローバルおよびリージョンのセキュリティフレームワークに対して監査を受けています。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 Artifact は、AWS コンプライアンスレポートにオンデマンドアクセスするための、無料セルフサービスポータルです。新しいレポートがリリースされると、AWS Artifact で利用できるようになり、お客様は AWS のセキュリティとコンプライアンスを継続的に監視し、新しいレポートに即座にアクセスできます。

国または業界の現地の規制または契約上の要件によっては、AWS はお客様または政府の監査人と直接監査を受けることもあります。これらの監査により、AWS の統制環境をさらに監督し、お客様が AWS のサービスを使用して、自信を持って、コンプライアンスを遵守し、リスクベースの方法で運用するためのツールを確実に利用できるようになります。

AWS 認定プログラム、レポート、第三者認証の詳細については、「AWS コンプライアンスプログラム」ウェブページを参照してください。サービス固有の情報については、AWS 対象範囲内のサービスウェブページもご覧ください。

CSA (クラウドセキュリティアライアンス)

AWS は、クラウドセキュリティアライアンス (CSA) Security, Trust & Assurance Registry (STAR) の自己評価に参加して、CSA が公表したベストプラクティスに準拠したコンプライアンスを文書化します。CSAは、「安全なクラウドコンピューティング環境を確保するためのベストプラクティスを定義しその認識を高めることを専門とする世界有数の組織」です。CSA コンセンサス評価イニシアティブアンケート (CAIQ) では、CSA がクラウドの顧客に期待する一連の質問が記載されています。また、クラウド監査人がクラウドプロバイダーに依頼することもあります。また、セキュリティ、統制、およびプロセスに関する一連の質問も記載されています。この質問は、クラウドプロバイダの選択やセキュリティの評価など、幅広い業務に使用できます。

AWS が CSA CAIQ に沿っていることを文書化した 2 つのリソースをお客様にご利用いただけます。1 つ目は CSA CAIQ ホワイトペーパー、2 つ目は、AWS Artifact 経由で利用できる SOC-2 統制へのより詳細な統制マッピングです。AWS の CSA CAIQ への参加に関する詳細については、 AWS CSA サイトを参照してください。

お客様のクラウドコンプライアンスガバナンス

AWS のお客様は、IT の導入方法やデプロイ場所に関わらず、自社の IT 統制環境全体にわたって適切なガバナンスを維持する責任を負います。主なプラクティスには以下のようなものがあります。

- 必要なコンプライアンス目標と要件を (関連資料等で) 理解する
- これらの目標と要件に適合する統制環境を確立する
- 組織のリスク許容度に応じて必要な検証作業を理解する
- 統制環境の運用効率を検証する

AWS クラウドへのデプロイにより、企業が各種の統制やさまざまな検証方法を適用するにあたって選択の幅が生まれます。

お客様のコンプライアンスと管理が強力な場合は、次の基本的なアプローチが考えられます。

1. AWS 責任共有モデル、AWS セキュリティのドキュメント、AWS コンプライアンスレポート、および AWS から入手できるその他の情報を、他のお客様固有の文書と共に見直します。IT 環境全体をできる限り理解し、すべてのコンプライアンス要件を包括的なクラウド管理フレームワークに文書化します。
2. AWS 責任共有モデルに示されているように、企業のコンプライアンス要件を満たすための統制目標を設計および実装します。
3. 外部の第三者が所有する統制を特定し、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、効率的に運営されていることを検証します。

この方法でコンプライアンスガバナンスにアプローチすることで、社内の統制環境をよりよく理解できます。また、実行すべき検証活動を明確にできます。

まとめ

安全性と耐障害性に優れたインフラストラクチャとサービスをお客様に提供することは、AWS にとって最優先事項です。お客様に対する当社のコミットメントは、お客様の信頼を継続的に獲得し、お客様が AWS でワークロードを安全に運用することに自信を持てるよう努めることに重点を置いています。これを実現するために、AWS には次のようなリスクおよびコンプライアンスのメカニズムが統合されています。

- 幅広いセキュリティコントロールと自動化ツールの実装
- AWS の運用効率とコンプライアンス体制の厳格な遵守を確実にする、セキュリティコントロールの継続的なモニタリングと評価
- AWS ビジネスリスクマネジメントプログラムによる独立したリスク評価
- 業務管理と経営管理の仕組み

さらに、AWS は定期的に独立した第三者による監査を受け、制御活動が意図通りに機能していることを保証しています。これらの監査は、AWS が取得している多くの認定とともに、AWS 統制環境の検証レベルをさらに高め、お客様にメリットをもたらします。

お客様が管理するセキュリティコントロールと組み合わせることで、AWS はお客様に代わって安全にイノベーションを起こし、お客様が AWS で構築する際のセキュリティ体制を改善できるよう支援しています。

寄稿者

本書の作成における寄稿者

- AWS セキュリティ、シニアプログラムマネージャー、Marta Taggart
- AWS ビジネスリスクマネジメント、リスクマネージャー、Bradley Roach
- AWS セキュリティ、シニアセキュリティスペシャリスト、Patrick Woods

その他の資料

AWS は、セキュリティと統制環境に関する情報を以下の方法でお客様に提供します。

- AWS コンプライアンスプログラムのページに記載されている、業界認定および独立した第三者による証明の取得と維持。
- AWS のセキュリティと統制の実践に関する情報を、ホワイトペーパーや AWS セキュリティブログなどのウェブサイトで、一貫して公表します。
- AWS Builders Library で、AWS がオートメーションを大規模に活用してサービスインフラストラクチャを管理する方法について詳しく説明しています。
- AWS Artifact と呼ばれるセルフサービスポータルを通じて、コンプライアンス証明書、レポート、その他のドキュメントを AWS のお客様に直接提供することで、透明性を高めます。
- AWS コンプライアンスリソースを提供し、AWS コンプライアンスに関するよくある質問ウェブページで、質問に対する回答を一貫して文書化し公開しています。
- お客様は、AWS Well-Architected Framework の設計原則に従うことで、AWS に構築するワークロードを標準以上に設定するためのアプローチ方法について、ガイダンスを得ることができます。

ドキュメントの改訂

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードをサブスクライブしてください。

update-history-change	update-history-description	update-history-date
マイナーな更新	技術的な正確性について確認	2021 年 3 月 10 日
ホワイトペーパーの更新	このバージョンには、コンプライアンスプログラムおよびスキームに関する参考情報の削除など、大幅な変更が含まれています。この情報は、AWS コンプライアンスプログラムおよびコンプライアンスプログラムによる AWS 対象範囲内のサービスウェブページから入手できるためです。また、コンプライアンスに関する一般的な質問のセクションは削除されました。この情報は AWS コンプライアンスに関するよくある質問ウェブページから入手できるようになったためです。	2020 年 11 月 1 日
初版公開	アマゾン ウェブ サービス: リスクおよびコンプライアンスに関するホワイトペーパー公開	2011 年 5 月 1 日

注意

お客様は、本書の情報について独自の評価を行う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 の現行製品と慣行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や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もなく、その内容を修正するものでもありません。