AWS ホワイトペーパー

AWS Security のご紹介

AWS Security のご紹介: AWS ホワイトペーパー

Table of Contents

AWS Security のご紹介

公開日: 2021 年 11 月 11 日 (改訂履歴)

要約

アマゾン ウェブ サービス (AWS) は、高い可用性と信頼性を確保するために設計されたスケーラブルなクラウドコンピューティングプラットフォームを備え、お客様がさまざまなアプリケーションを実行するためのツールを提供しています。お客様のシステムやデータの機密性、完全性、可用性の保護を支援することは、お客様からの信頼と信用の維持と同様に、AWS にとって最も重要です。このドキュメントでは、AWS 環境内のコントロールや、セキュリティ目標の達成のために利用できる AWS が提供する製品や機能を含め、セキュリティに対する AWS のアプローチをご紹介します。

AWS インフラストラクチャのセキュリティ

AWS のインフラストラクチャは、今日利用できるクラウドコンピューティング環境の中でも、最も柔軟で安全に設計された環境の 1 つとなっています。アプリケーションやデータを迅速かつ安全にデプロイできる、極めてスケーラブルで信頼性の高いプラットフォームを提供するように設計されています。

このインフラストラクチャは、セキュリティのベストプラクティスや基準に準拠するだけでなく、クラウド特有のニーズも考慮して構築および管理されています。AWS は、基盤となるインフラストラクチャのモニタリングと保護を 24 時間年中無休で行うために、冗長化された階層型コントロール、継続的な検証とテスト、広範なオートメーションを使用しています。AWS は、これらのコントロールを新しい各データセンターや各サービスに確実にレプリケートしています。

AWS のすべてのお客様は、セキュリティ要件が最も厳しいお客様を基準に構築されたデータセンターやネットワークアーキテクチャの利点を活用できます。これは、高度なセキュリティを確保するように設計され、回復性を備えたインフラストラクチャを、従来のデータセンターの設備投資や運用オーバーヘッドなしで利用できることを意味します。

AWS はセキュリティの責任共有モデルに従い、基盤となるクラウドインフラストラクチャのセキュリティに責任を持ち、お客様は AWS でデプロイするワークロードのセキュリティに責任を持ちます (図 1)。これにより、お客様のビジネス機能に最適なセキュリティコントロールを AWS 環境に実装するために必要な柔軟性と俊敏性が確保されます。機密データの処理環境へのアクセスは厳しく制限すること、もしくは公開する情報に対してはあまり厳しくないコントロールをデプロイすることができます。

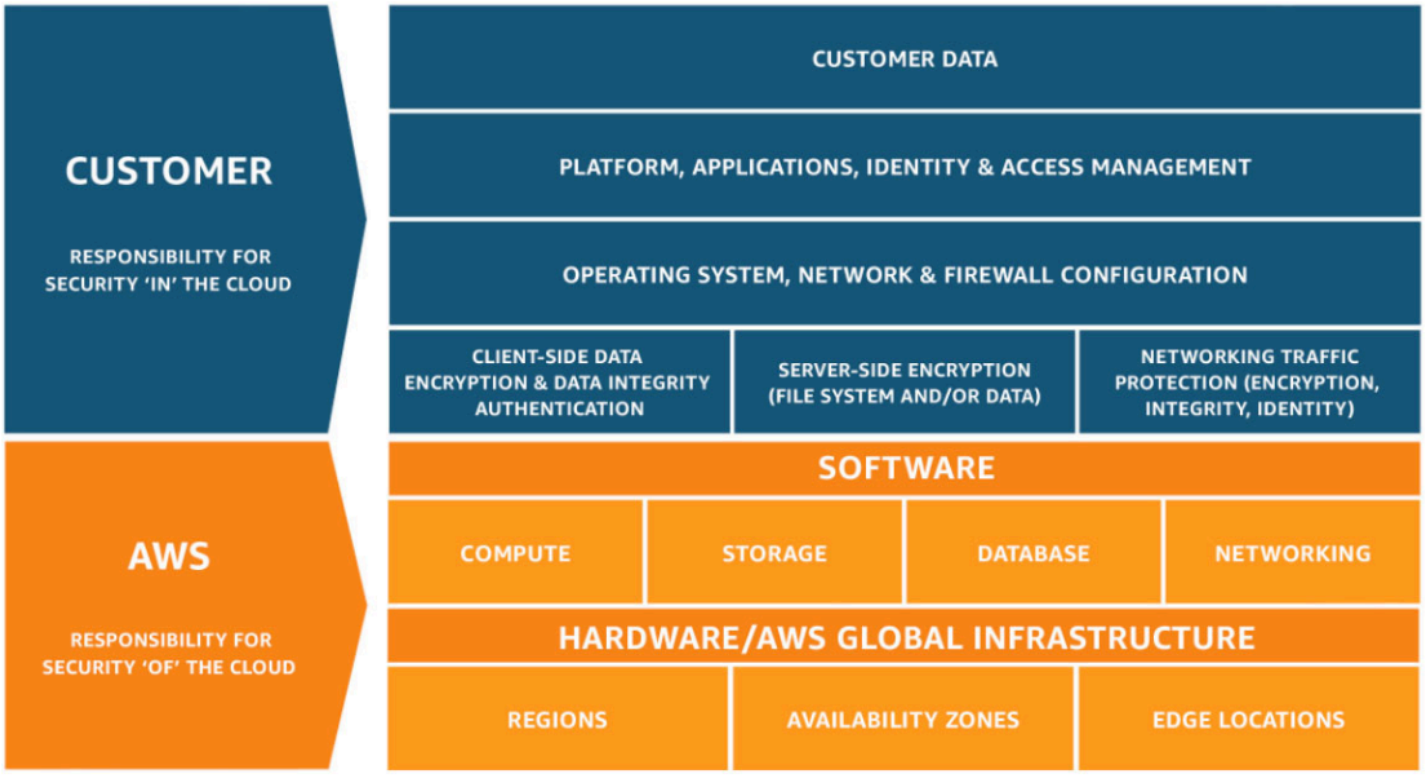

図 1: AWS のセキュリティ責任共有モデル

セキュリティ製品および機能

AWS および AWS パートナーは、お客様のセキュリティ目標を達成するために役立つさまざまなツールや機能を提供しています。これらのツールは、オンプレミス環境内にデプロイされている使い慣れたコントロールをミラーリングします。AWS には、ネットワークセキュリティ、設定管理、アクセスコントロール、データセキュリティにまたがるセキュリティ専用のツールや機能が備わっています。さらに、環境内で起きていることを完全に可視化できるモニタリングツールとログ記録ツールも備わっています。

トピック

インフラストラクチャのセキュリティ

AWS には、プライバシーを強化してネットワークアクセスを制御するための複数の機能やサービスがあります。具体的には次のとおりです。

- Amazon VPC に組み込まれたネットワークファイアウォール - これにより、プライベートネットワークを作成し、インスタンスやアプリケーションへのアクセスを制御できます。お客様は、AWS のすべてのサービスで TLS を使用し、伝送中の暗号化を制御できます。
- 接続オプション - オフィスやオンプレミス環境からのプライベート接続または専用接続を可能にします。
- DDoS 緩和テクノロジー - レイヤー 3 または 4 とレイヤー 7 で適用されます。これらは、アプリケーションやコンテンツの配信戦略の一部として適用できます。
- 自動暗号化 - AWS のグローバルおよびリージョナルネットワークでの、AWS のセキュリティで保護された設備間のすべてのトラフィックが自動的に暗号化されます。

インベントリおよび設定管理

AWS は、クラウドリソースを組織の基準やベストプラクティスに準拠させながら、迅速な移行を可能にするさまざまなツールを備えています。具体的には次のとおりです。

- デプロイツール - 組織の基準に従って AWS リソースの作成と廃止を管理します。
- インベントリおよび設定管理ツール - AWS のリソースを識別し、これらのリソースへの変更を経時的に追跡および管理します。
- テンプレート定義および管理ツール - EC2 インスタンス用の事前設定および強化された標準の仮想マシンを作成します。

データの暗号化

AWS では、クラウド内に保管中のデータのセキュリティを強化できるように、スケーラブルで効率的な暗号化機能を提供しています。具体的には次のとおりです。

- Amazon EBS、Simple Storage Service (Amazon S3)、Amazon RDS、Amazon Redshift、Amazon ElastiCache、AWS Lambda、Amazon SageMaker など、AWS のほとんどのサービスで使用できる保管中のデータの暗号化機能
- 暗号化キーを AWS 側で管理するか、独自のキーを完全に自分で管理するかを選択できる、AWS Key Management Service を含む柔軟なキー管理オプション
- コンプライアンス要件を満たす支援を行う、専用のハードウェアベースの暗号化キーストレージ (AWS CloudHSM を使用)
- 暗号化されたメッセージキュー - Amazon SQS のサーバー側暗号化 (SSE) を使用した機密データの送信に使用します。

さらに、AWS には、AWS 環境で開発またはデプロイするサービスに暗号化とデータ保護を統合するための API もあります。

アイデンティティおよびアクセスコントロール

AWS には、AWS のサービス間をまたいでユーザーアクセスポリシーを定義、適用、管理する機能があります。具体的には次のとおりです。

- AWS Identity and Access Management (IAM) は、AWS リソース全体にアクセス許可を持つ個別ユーザーアカウントに、特権アカウント用の AWS Multi-Factor Authentication を定義できます。

ソフトウェアおよびハードウェアベースの認証のオプションが含まれます。IAM では、Microsoft Active Directory や他のパートナーのサービスなど、既存のアイデンティティシステムを使用して、AWS Management Consoleや AWS のサービス API へのフェデレーティッドアクセスを従業員やアプリケーションに付与できます。

- AWS Directory Service は、社内ディレクトリとの統合およびフェデレーションにより、管理オーバーヘッドを削減し、エンドユーザーエクスペリエンスを向上させることができます。
- AWS Single Sign-On (AWS SSO) は、AWS Organizations のすべてのアカウントに対する SSO アクセスとユーザーアクセス許可を一元的に管理できます。

AWS は、その多くのサービスでネイティブの Identity and Access Management インテグレーションを提供し、さらにユーザー独自のアプリケーションやサービスとの API インテグレーションも提供しています。

モニタリングとログ記録

AWS には、AWS 環境内で起きていることを可視化できるツールや機能があります。具体的には次のとおりです。

- AWS CloudTrail を使用すると、アカウントの AWS API コールの履歴を取得することで、クラウド上の AWS デプロイをモニターできます。履歴には、AWS Management Console、AWS SDK、コマンドラインツール、高度な AWS のサービスによって作成された API コールが含まれます。また、CloudTrail をサポートするサービスの AWS API を呼び出したユーザーやアカウント、呼び出し元の IP アドレス、呼び出しの時間を確認することもできます。
- Amazon CloudWatch - わずか数分で使用を開始できる、信頼性、スケーラビリティ、柔軟性に優れたモニタリングソリューションです。独自のモニタリングシステムやインフラストラクチャを設定、管理、スケールする必要はなくなります。
- Amazon GuardDuty - 脅威検出サービスです。悪意のあるアクティビティや不正な動作を継続的にモニタリングし、AWS のアカウントとワークロードを保護します。Amazon GuardDuty は Amazon CloudWatch を介して通知を公開するため、自動化されたレスポンスをトリガーしたり、人に知らせたりできます。

これらのツールや機能を使用することで、ビジネスに影響が及ぶ前に問題を検出し、環境のセキュリティ体制を強化したり、リスクプロファイルを軽減したりできます。

AWS Marketplace のセキュリティ製品

本番ワークロードを AWS に移行することで、組織は安全な環境を維持しながら、俊敏性、スケーラビリティ、イノベーション、コスト削減を向上させることができます。AWS Marketplace は、オンプレミス環境の既存のコントロールと同等、同一、または統合された、業界をリードするセキュリティ製品を提供します。これらの製品は AWS の既存のサービスを補完します。包括的なセキュリティアーキテクチャをデプロイして、クラウド環境およびオンプレミス環境全体にさらにシームレスなエクスペリエンスを得ることができます。

セキュリティガイダンス

AWS は、AWS および AWS パートナーが提供するオンラインツール、リソース、サポート、プロフェッショナルサービスをとおしてお客様にガイダンスと専門知識を提供しています。

AWS Trusted Advisor は、カスタマイズされたクラウドエキスパートのように動作するオンラインツールで、ベストプラクティスに準拠したリソースの設定を支援します。Trusted Advisor は、お客様の AWS 環境を検査して、セキュリティギャップを埋め、コスト削減の機会を見つけ、システムのパフォーマンスを改善し、信頼性を高めます。

AWS Account Teamsは、最初の連絡先として、お客様のデプロイと実装をガイドし、セキュリティ上の問題が発生した場合に解決のための適切なリソースを紹介します。

AWS エンタープライズサポートは、応答時間は 15 分間で、専任のテクニカルアカウントマネージャーとの電話、チャット、E メールによるサポートを 24 時間年中無休で提供します。このようなコンシェルジュ型のサービスにより、お客様の問題に早急に対処します。

AWS パートナーネットワークは、オンプレミス環境の既存のコントロールと同等または同一であるか、これらと統合される、数百に及ぶ業界屈指の製品を提供しています。これらの製品は、AWS の既存のサービスを補完し、クラウド環境とオンプレミス環境にわたって包括的なセキュリティアーキテクチャと、よりシームレスなエクスペリエンスをデプロイできるようにします。また、認定を受けた世界中の数多くの AWS コンサルティングパートナーから、セキュリティとコンプライアンスのニーズに対するサポートを受けることもできます。

AWS Professional Services は、セキュリティ、リスク、コンプライアンスの専門実務を担当し、機密性の最も高いワークロードを AWS クラウドに移行するための自信と技術的能力の育成を支援します。AWS Professional Services は、実証済みの設計に基づいてお客様のセキュリティポリシーおよびプラクティスの策定をサポートします。また、お客様のセキュリティ設計が内外のコンプライアンス要件を満たすように支援します。

AWS Marketplace は、独立系ソフトウェアベンダーの数千に及ぶソフトウェアのデジタルカタログで、AWS で実行するソフトウェアの検索、テスト、購入、デプロイを容易にします。AWS Marketplace セキュリティ製品は、AWS の既存のサービスを補完し、クラウド環境とオンプレミス環境にわたって包括的なセキュリティアーキテクチャと、よりシームレスなエクスペリエンスをデプロイできるようにします。

AWS セキュリティ速報は、現在の脆弱性や脅威に関するセキュリティ速報を提供し、お客様が AWS のセキュリティエキスパートと協力して不正使用、脆弱性、侵入テストの報告などの懸念に対処できるようにします。脆弱性の報告用のオンラインリソースも用意してあります。

AWS セキュリティドキュメントは、セキュリティとコンプライアンスの目標を達成するための AWS のサービスの設定方法を記載しています。AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

AWS Well-Architected Framework は、クラウドアーキテクトが、アプリケーション向けに高い安全性、性能、障害体制、効率性を備えたインフラストラクチャを構築する際に役立ちます。AWS Well-Architected フレームワークには、情報とシステムを保護するための専用のセキュリティの柱が含まれています。主なトピックには、データの機密性と完全性、権限管理における権限の特定と管理、システムの保護、セキュリティイベントを検出する制御の確立などが含まれます。お客様は、AWS Well-Architected Tool をAWS Management Consoleから使用するか、いずれかの APN パートナーのサービスとして利用し、支援を受けることができます。

AWS Well-Architected Tool は、ワークロードの状態のレビューや、最新の AWS アーキテクチャのベストプラクティスとの比較に役立ちます。この無料ツールは、AWS Management Consoleで、オペレーショナルエクセレンス、セキュリティ、信頼性、パフォーマンス効率、コスト最適化に関する質問に回答した後に利用できます。それに応じて、AWS Well-Architected Tool から、確立されたベストプラクティスに準拠したクラウドのアーキテクチャ設計方法に関する計画が提供されます。

コンプライアンス

AWS Compliance を使用すると、お客様は AWS クラウド内でセキュリティとデータ保護を維持するために AWS に導入されている堅牢なコントロールについて理解できます。システムが AWS クラウド内で構築されると、AWS とお客様はコンプライアンスの責任を共有します。AWS のコンピューティング環境は、SOC 1/SSAE 16/ISAE 3402 (旧 SAS 70)、SOC 2、SOC 3、ISO 9001/ISO 27001、FedRAMP、DoD SRG、PCI DSS レベル 1.i など、地域や業種にまたがる認定機関からの認定を受けて、継続的に監査されています。さらに、AWS には、お客様が AWS で実行する環境のコンプライアンスを確立するのに役立つテンプレートとコントロールマッピングを提供する保証プログラムもあります。プログラムの一覧については、「AWS コンプライアンスプログラム」を参照してください。

AWS のすべてのサービスが GDPR に準拠して使用できます。つまりお客様は、サービスのセキュリティ維持のために AWS が既に実施しているすべての対策からメリットを享受するだけでなく、お客様の GDPR コンプライアンス計画の一部として AWS のサービスをデプロイできます。AWS は、GDPR に準拠したデータ処理補遺条項 (GDPR DPA) を規定しており、お客様が GDPR 契約の義務に準拠できるようにしています。AWS GDPR DPA は、AWS のサービス規約に組み込まれており、GDPR 準拠のためにこれを必要とする世界中のすべてのお客様に自動的に適用されます。Amazon.com, Inc. は、EU-US Privacy Shield の認定を受けており、AWS はこの認定の対象となります。このため、お客様が個人データを米国に転送してデータ保護義務を果たす際に役立ちます。Amazon.com Inc. の認定については、EU-US Privacy Shield のウェブサイト (https://www.privacyshield.gov/list) で確認できます。

認定された環境でオペレーションを行うことで、お客様は実行する必要がある監査の範囲とコストを縮小できます。AWS は基盤となるインフラストラクチャの評価を継続的に実行しています。この評価には、ハードウェアとデータセンターの物理的および環境的セキュリティも含まれます。したがって、お客様はこれらの認定を活用して、これらのコントロールを継承するだけでよいのです。

従来のデータセンターでは、一般的なコンプライアンス業務が手作業での定期的な業務になっていることがよくあります。これらの業務には、アセット設定の検証や管理業務に関するレポートが含まれます。さらに、結果のレポートは、発行前には既に最新ではない場合があります。AWS 環境でオペレーションを行うことで、AWS Security Hub、AWS Config、AWS CloudTrail など組み込みの自動化ツールを利用して、コンプライアンスを検証できます。これらのツールにより、監査を実行するために必要な作業量が削減されます。このような作業が定期的となり、継続的なタスクとして自動化されるようになるためです。手動の業務に費やす時間を減らすことで、企業におけるコンプラアンスの役割を、必要とされる管理負担の 1 つから、リスクを管理してセキュリティ体制を強化するための役割へと進化させることができるのです。

その他の資料

詳細については、以下のリソースを参照してください。

探したい情報	参照先
AWS でのクラウドセキュリティに関する主なトピック、リサーチ分野、トレーニングの機会	AWS クラウドセキュリティ学習
AWS クラウド導入フレームワーク。ビジネス、人、ガバナンス、プラットフォーム、セキュリティ、オペレーションという 6 つの重点分野にガイダンスをまとめたもの。	AWS クラウド導入フレームワーク
AWS に設定されている特定のコントロール、AWS をお客様の既存のフレームワークに統合する方法	アマゾン ウェブ サービス: リスクとコンプライアンス
セキュリティ、アイデンティティ、コンプライアンスに関するベストプラクティス	セキュリティ、アイデンティティ、コンプライアンスに関するベストプラクティス
セキュリティの柱 - AWS Well-Architected Framework	セキュリティの柱 - AWS Well-Architected Framework

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
ホワイトペーパーの更新	その他の資料のリンクを更新。	2021 年 11 月 11 日
ホワイトペーパーの更新	最新のサービス、リソース、テクノロジーを反映して更新	2020 年 1 月 22 日
初版公開	AWS セキュリティの紹介を公開。	2015 年 7 月 1 日

注意

お客様は、この文書に記載されている情報を独自に評価する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。