AWS SECURITY

クラウド移行による ビジネス変革の セキュリティ ベストプラクティス

目次

注記

aws

はじめに

クラウドへの移行は、ビジネスプロセス、サービス、コスト構造、スケールの変革を伴います。また、セキュリティへのアプローチについても、モダナイズが必要になります。この機会に、オンプレミスにおけるセルフマネージドのセキュリティおよび保証の手法からフルマネージドサービスのアーキテクチャに移行し、拡張に備えた新しいビジネス変革アーキテクチャをサポートしましょう。

組織は、サードパーティーの何千ものグローバルな検証コンプライアンス要件を満たし、対応する必要があります。AWS では、クラウドでのスケーリングとセキュリティタスクの自動化をサポートし、セキュリティとコンプライアンスの責任を共有することで、組織がそれら要件に対応するのを後押ししています。セキュリティの自動化に向け変革を進めることで、設定での人的エラーが減り、ビジネスに不可欠な他の作業に専念する時間的な余裕が生まれます。

この日本語ガイドの利点

この日本語ガイドは、CISO やセキュリティ IT リーダーなど、幹部クラスのセキュリティ責任者の方に最適です。AWS クラウドで提供されているすべてのサービスが実行されるインフラストラクチャが、AWS でどのように保護されるかをご確認いただけます。また、クラウドのセキュリティおよびご利用のセキュリティサービスに関する、ご自身のロールと責任範囲についても、理解を深めることができます。

「AWS はデータセキュリティと災害対策で定評があるため、データセンターではない場所でデータが安全に保存されていることを保険業界のお客様にも容易に納得していただけます」[1]

Wesurance、ビジネス開発ストラテジスト、Roland Chang 氏

「AWS を選択したのは、さまざまなデータ保護標準への対応に役立ち、当社が必要とするスケーラビリティを実現できるためです」[2]

Climedo Health GmbH、エンジニアリングバイスプレジデント、Benjamin Sauer 氏

1「Wesurance Drives Transformation for Insurers with Innovative Digital Solutions on AWS」(Wesurance、AWS の革新的なデジタルソリューションで保険会社の変革を推進)、AWS 導入事例、2021 年
2「Climedo Health Captures Patient-centric, Compliant, and Secure Clinical Data Using AWS」(Climedo Health、AWS を使用し、規則や要件に準拠して、患者中心の安全な臨床データを取得)、AWS 導入事例、2022 年

AWS のクラウドセキュリティ

AWS は、現在利用可能なクラウドコンピューティング環境として最も柔軟性と安全性に優れた設計になっています。レガシーインフラストラクチャに対する統制と同等以上の柔軟性で、お使いの環境を安全に統制できます。AWS では、インフラストラクチャおよびアプリケーションの変更に関するコンプライアンス、保証、モニタリングに役立つツールとサポートが提供されます。また、ガードレールを使用すると、手作業でセキュリティ確認を行うことなくセキュリティのベースラインを確保でき、イノベーションが促進できます。AWS ではこのようなガードレールの作成が支援されるため、作業時間の短縮が可能になります。このような機能がセキュリティチームと IT チームを支え、セキュリティベースラインからの異常や逸脱に対するインシデント対応を自動化することにより、セキュリティに時間を割かなくて済む分、コアビジネスに専念できます。

AWS クラウドセキュリティの 5 つの利点

1 **データの優れた可視性と統制**により、誰がどこからデータにアクセスしているかという重要なインサイトを得ることができます。AWS のツールを使用すると、データがどこに保存されていて誰がデータにアクセスできるかがわかるだけでなく、組織で特定の瞬間にどのリソースが使用されているかを常に把握できます。セキュリティオートメーションおよびアクティビティモニタリングサービスを使用して、エコシステム全体の不審なアクティビティを検出することにより、拡張時のリスクを軽減します。AWS のサービスを既存のソリューションと統合して、オペレーションを合理化しましょう。

2 AWS でセキュリティタスクを自動化すると、設定の人的エラーが減ってセキュリティが向上するだけでなく、セキュリティチームに時間的な余裕ができ、デベロッパーやオペレーションチームと緊密に連携できるため、**より迅速かつ安全なコードの作成とデプロイ**が可能になります。

3 **最高水準のプライバシーとデータセキュリティを構築**する際には、世界クラスの AWS セキュリティエキスパートの支援を受けることができます。チームが 365 日 24 時間体制でシステムを継続的にモニタリングしているため、お客様のコンテンツは常に保護されます。

4 AWS には、世界中の数万ものパートナーで構成された、極めて活動的な、最大規模のコミュニティがあります。**AWS パートナーネットワーク (APN)** には、AWS のサービスを専門とする数千のシステムインテグレーターや、AWS で機能するように自社のテクノロジーを適応させた数万の独立系ソフトウェアベンダー (ISV) が参加しています。最初の移行から継続的な日常の管理まで、クラウド導入のすべての段階を保護できる、信頼の高いセキュリティパートナーとソリューションにアクセスしましょう。

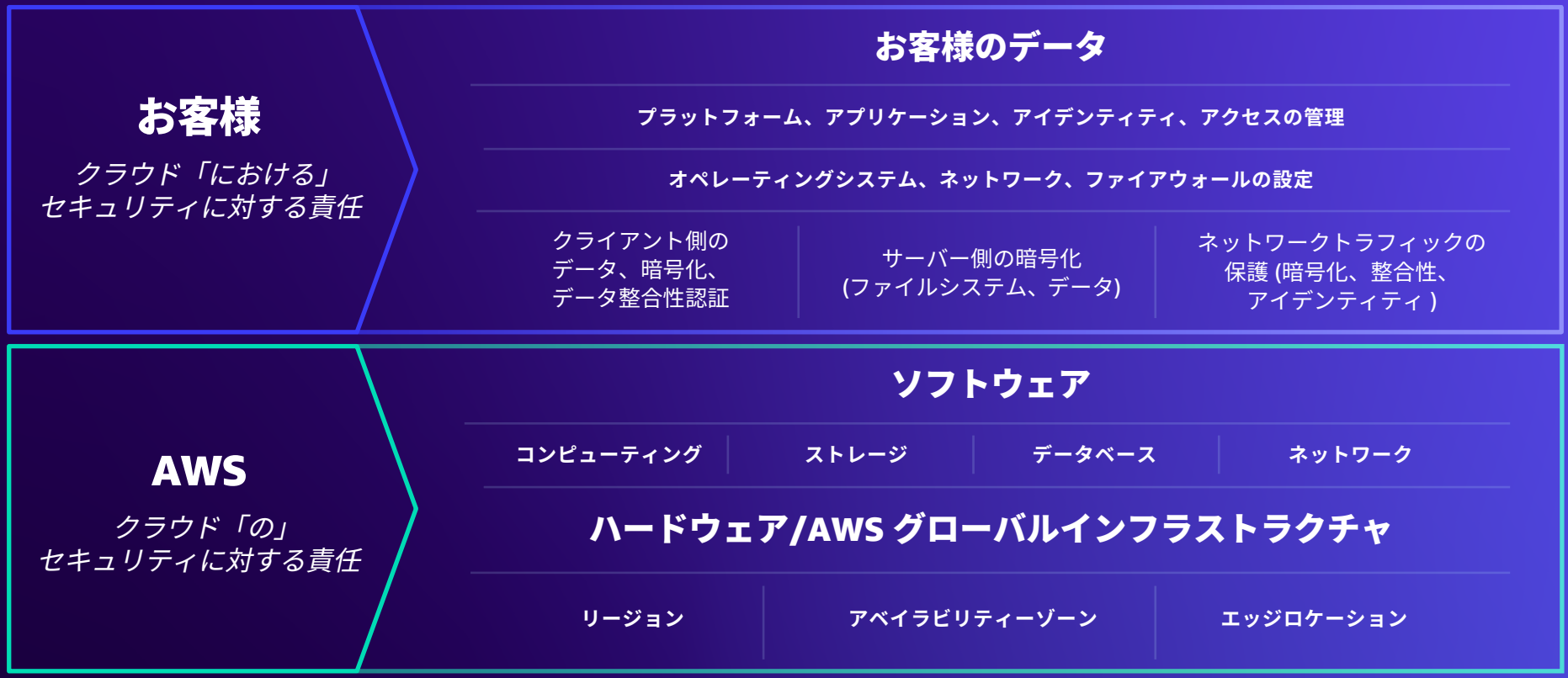
5 AWS の**最も包括的なコンプライアンス統制**を継承しましょう。AWS では、FedRamp、FIPS 140-2、GDPR、HIPAA/HITECH、NIST SP 800-171、PCI-DSS など、他のどのプロバイダーよりも多くのセキュリティ標準規格およびコンプライアンス認証に対応しています。お客様は世界中のほぼすべての規制機関のコンプライアンス要件を満たすことができます。

最高水準

チームが 365 日 24 時間体制でシステムを継続的にモニタリングしているため、お客様のコンテンツは常に保護されます。

クラウドセキュリティ - 責任共有

IT インフラストラクチャを AWS に移行すると、責任共有モデルが適用されます。この共有モデルは、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を運用する施設の物理的なセキュリティに至るまで、何層もの IT コンポーネントの運用、管理、統制を AWS が行うことで、お客様の運用上の負担を軽減するなど、さまざまな利点をもたらします。このように IT 環境の運用責任だけでなく、IT 統制の管理、運用、検証も、当社との間で分担となります。



クラウドのセキュリティは AWS が担う

AWS が提供するすべてのサービスが実行されるインフラストラクチャの保護については、AWS が責任を担います。AWS のインフラストラクチャは、AWS のサービスが運用されているハードウェア、ソフトウェア、ネットワーキング、および施設で構成されています。ホストオペレーティングシステムから施設の物理的なセキュリティまでを AWS が責任を担うことで、お客様側の運用上の負担は軽減されます。情報、ID、アプリケーション、デバイスが保護されている安心感を得られます。

AWS セキュリティ保証

AWS は業界を先導するクラウドプロバイダーとして、最も包括的なコンプライアンス統制を備えており、広く認められた**フレームワークおよびプログラム**を確立しています。これらの統制を使用すると、世界中の規制当局のコンプライアンス要件を満たし、自動的に継承できます。このため、セキュリティ保証の取り組みに要するコストを大幅に削減できるだけでなく、コンプライアンスおよび認証に関する独自のプログラムを強化できます。

AWS のユビキタスな IT 統制環境と世界中で運営する施設の有効性と効率的な運用については、サードパーティーの独立した査定によって認められています。その内容には、AWS の統制環境全体でさまざまな側面を活用したポリシー、プロセス、および統制アクティビティが含まれます。

プライバシー

プライバシーとは主に、誰がデータにアクセスできるかを制御することです。AWS を使用すると、必要なときにいつでも、組織のコンテンツに誰がアクセスしていて、組織でどのリソースを消費しているかを把握できます。このため、リソースへの適切なレベルのアクセスを常に提供できます。情報がどこに保存されているかには関係なく、アイデンティティとアクセスに対するきめ細かい制御と、リアルタイムに近いセキュリティ情報の継続的なモニタリング機能をご利用いただけます。

システム全体において構成変更やセキュリティイベントを検出するアクティビティモニタリングサービスを使用することで、リスクを軽減して成長を実現します。当社のサービスを既存のソリューションと統合して、オペレーションとコンプライアンスレポート作成を簡素化することもできます。データプライバシーについて組織に適用される法律や規制は、リージョンや地域によって異なりますが、AWS で実現する統制によって、これらへの準拠が可能になります。

コンプライアンス統制

SOC	DoD CC SRG	C5	HITRUST CSF
PCI	HIPAA BAA	K-ISMS	FINMA
ISMAP	IRAP	ENS High	GSMA
FedRAMP	MTCS	OSPAR	PiTuKri

データレジデンシー

AWS データセンターは、世界中のさまざまな場所のクラスターに構築されており、AWS リージョンと呼ばれています。顧客のコンテンツを保存する AWS リージョンは、お客様ご自身で選択します。AWS のサービスを特定の地理的要件に従って選択した場所にデプロイすることで、コンプライアンスとデータレジデンシーの要件を満たすことができます。例えば、オーストラリアのみにデータを保存したい同国の AWS のお客様の場合は、アジアパシフィック (シドニー) の AWS リージョンにのみ AWS サービスをデプロイすることを選択できます。その他の柔軟なストレージオプションについては、こちらをご覧ください。

ビジネス継続性

AWS のインフラストラクチャは高レベルの可用性を備えており、回復性のある IT アーキテクチャのデプロイに必要な機能を提供します。当社のシステムは、システムやハードウェアの障害時、お客様への影響を最小限に抑えるように設計されています。

災害対策

複数の AWS アベイラビリティーゾーンにアプリケーションを分散することで、自然災害やシステム障害など、ほとんどの障害モードで回復性を維持できます。AWS CloudEndure Disaster Recovery を使用すると、AWS で運用する物理、仮想、およびクラウドベースのサーバーについて、高速で信頼性の高い復旧が可能です。ダウンタイムとデータ損失も、最小限に抑えることができます。

3「TNEX Launches Vietnam's First Digital Bank in Nine Months on AWS」(TNEX、AWS の活用によりベトナム初のデジタル銀行を 9 か月で立ち上げ)、AWS 導入事例、2021 年

「AWS で、あらゆる機密データのセグメント化、統制、暗号化が可能です。万が一どこかのレベルで侵害を受けたとしても、すべてを匿名化、トークン化、および暗号化するようにアーキテクチャが設定されているため、データ漏洩を防ぐことができます」[3]

TNEX、CEO 兼共同創立者、Bryan Carroll 氏

クラウドにおけるセキュリティはお客様が担う

クラウドのセキュリティに関する面倒な部分は AWS が受け持ちますが、ゲストオペレーティングシステムや関連するアプリケーションソフトウェアの管理など、クラウド内のセキュリティはお客様の責任となります。

AWS リソースを安全に管理する方法

お客様の責任範囲は、使用するサービス、IT 環境でのサービス統合、適用される法律や規制によって異なります。AWS サービスを選択する際には、これらをすべて考慮する必要があります。AWS では、セキュリティとコンプライアンスに関するお客様の要件に応じて、ご利用環境のセキュリティ体制を強化するために役立つさまざまなレベルのサポートを提供しています。文書化されたベストプラクティス、各種のプロフェッショナルサービス、セキュリティ/コンプライアンス体制チェックを自動化するソリューションなどのツールやサービスもご利用いただけます。

AWS が提供するセキュリティ/アイデンティティサービスの利点

AWS では、クラウド内のセキュリティを確立できるように、セキュリティおよび規制に関するお客様の要件に合致する革新的なセキュリティサービスを幅広くご用意しています。

アイデンティティサービス

AWS のアイデンティティサービスを使用すると、あらゆるスケールでアイデンティティ、リソース、アクセス許可を安全に管理できます。AWSでは、ワークフォース向けおよび顧客向けアプリケーションのアイデンティティサービスを用意し、迅速に開始し、ワークロードとアプリケーションへのアクセスを管理できます。

データ保護

AWS では、データ、アカウント、およびワークロードを不正アクセスから保護するために役立つサービスを提供しています。**AWS のデータ保護サービス**では、暗号化、キー管理、脅威検出を行い、アカウントとワークロードを継続的にモニタリングおよび保護します。

ネットワーク保護

AWS のネットワークおよびアプリケーション保護サービスを使用すると、組織全体のネットワーク制御ポイントにきめ細かいセキュリティポリシーを適用できます。AWS のサービスはトラフィックの検査およびフィルタリングに役立ち、ホストレベル、ネットワークレベル、およびアプリケーションレベルの境界で不正なリソースアクセスを防止します。

脅威の検出

AWS が提供する継続的なモニタリングと脅威の検出サービスにより、クラウド環境内のネットワークアクティビティやアカウントの動作を継続的にモニタリングして、脅威を識別できます。

データプライバシー

AWS のコンプライアンスおよびデータプライバシーサービスにより、コンプライアンス状態を包括的に確認できます。さらに、お客様が準拠している業界標準と AWS のベストプラクティスに基づき、自動化されたコンプライアンスチェックを使用して、ご利用環境を継続的にモニタリングできます。

AWS クラウド導入フレームワーク — セキュリティの観点

安全なクラウド導入の取り組みで成功を収めるには、まず **AWS クラウド導入フレームワーク (AWS CAF)** で AWS の経験とベストプラクティスを活用しましょう。セキュリティの観点から、このフレームワークは高度なセキュリティ機能と回復性の高いワークロードを構築するためのベストプラクティスを提供します。セキュリティの準備状況を特定して優先順位を付け、データとワークロードの機密性、整合性、および可用性を実現するには、以下に示す 9 つの機能が役立ちます。一般的には、CISO、CCO、内部監査リーダー、セキュリティアーキテクトおよびエンジニアなどがステークホルダーとなります。

AWS クラウド導入フレームワークの 9 つの機能

1. セキュリティガバナンス
2. セキュリティ保証
3. アイデンティティとアクセス管理
4. 脅威の検出とモニタリング
5. 脆弱性管理
6. インフラストラクチャ保護
7. データ保護
8. アプリケーションのセキュリティ
9. インシデント対応

1 セキュリティガバナンス

セキュリティプログラムを効果的に進めるには、セキュリティに関するロール、業務責任、説明責任、ポリシー、プロセス、手順などの項目を定義、作成、保守、伝達を行う必要があります。説明責任の範囲を明確に線引きすることで、セキュリティプログラムの効果を高めることができます。

2 セキュリティ保証

セキュリティプログラムの有効性を向上するには、継続的なモニタリング、評価、および管理は不可欠です。実装した統制に対する信頼と確実性を確立することで、規制要件への効果的な対応が可能になります。

3 アイデンティティとアクセス管理

より多くのワークロードを実行し AWS 上の環境を継続的に拡張する場合、適切なユーザーが適切な条件下で適切なリソースにアクセスできるようにすることが重要です。AWS ワークロードを安全に運用するには、アイデンティティとアクセス管理が中核的な役割を果たします。人についてもマシンについても、アイデンティティの認証と承認が必要になります。アクセス許可の管理では、最小特権を適用しながら、幅広くきめ細かなアクセス制御を実現できます。

4 脅威の検出とモニタリング

ご利用環境を継続的にモニタリングし、使用中のアセットおよびリソースについて正常かつ正当な動作を識別するには、脅威の検出機能が必要になります。機械学習、異常検出、ベストプラクティスの自動チェック、インテリジェント脆弱性管理などの手法を使用することで、潜在的な設定ミス、誤動作、不正使用を迅速に判断および伝達し、修復にかかる時間を短縮できます。

5 脆弱性管理

サーバーワークロードおよびコンテナワークロードには、幅広くさまざまなソフトウェアおよびソフトウェアバージョンが動的に導入される可能性があります。潜在的な脆弱性の迅速な特定と優先順位付けを自動化して必要な修復を行うには、脆弱性の管理が重要になります。これにより、新しいソフトウェアの脆弱性に関する通知を定期的に受けることができます。

6 インフラストラクチャ保護

クラウドでの正常なオペレーションを継続し、ベストプラクティスと規制上の義務に従うには、統制手法が重要になります。情報セキュリティプログラムにおいて重要な要素は、インフラストラクチャの保護です。これは、意図しない不正アクセスや潜在的な脆弱性から、ワークロード内のシステムとサービスを確実に保護するために必要です。

7 データ保護

セキュリティに影響するような、基本的なプラクティスは常に、ワークロードを設計する前に適用しておく必要があります。これらは、規制義務の順守や規制義務への対応ミスの回避などに対応する際に不可欠です。データはすべて、保管中も転送中も暗号化は必要であり、機密データは、リスクと脆弱性を軽減するためにアカウントを分けて保存する必要があります。

8 アプリケーションのセキュリティ

ソフトウェアの開発プロセス中にセキュリティ上の欠陥を特定した場合に、時間、労力、コストの無駄を回避するには、セキュリティを最優先しましょう。アプリケーションの開発段階でセキュリティのポリシーを設定すると、セキュリティギャップを最小限に抑え安心感を得ることができます。

9 インシデント対応

セキュリティインシデントの潜在的な影響に対応し、影響を緩和するには、事前に準備しておくことが重要です。インシデントの発生時に、業務の中断を最小限に抑え、チームが処理 (問題の切り分け、阻止、フォレンジックの実行) を効率的に進めるには、セキュリティインシデントが発生する前に、適切なツールとアクセスを実装しておく必要があります。

AWS 移行戦略の策定

安全で優れたクラウド導入計画を作成する場合や、AWS の既存ワークロードを作り直す場合に、強力なセキュリティ基盤の構築に役立つ、業界で認められた標準とフレームワークがいくつか存在します。

AWS クラウド導入フレームワークは、IT ガバナンスとセキュリティ管理のシステムを構築する場合に、クラウドへの安全な移行を計画して成功を収めるうえで役立ちます。AWS Well-Architected フレームワークは、安全なインフラストラクチャを構築するとともに、AWS セキュリティベストプラクティスの準拠を自動チェックして、セキュリティの観点から AWS アカウントを継続的に評価するために活用できます。

AWS Well-Architected フレームワーク

さまざまなアプリケーションやワークロードに対応し、安全性、パフォーマンス、回復力、効率性に優れたインフラストラクチャを構築するには、**AWS Well-Architected フレームワーク**が最適です。これを活用することで、クラウドアーキテクトはワークロードレベルに集中できます。このフレームワークに含まれるセキュリティの柱は、以下に示す 5 つのコンポーネントから構成されています。

- アイデンティティとアクセス管理
- 検出
- インフラストラクチャ保護
- データ保護
- インシデント対応

AWS Well-Architected フレームワークは、適切な AWS のサービスを選択するうえで必要になる安全な実装とアプローチのガイダンスを提供しており、これらのコアセキュリティプラクティスをワークロードに実装する場合に役立ちます。

AWS セキュリティベストプラクティスの自動チェック：AWS Security Hub

組織のセキュリティ体制を維持するには、デプロイされたアカウントとリソースがセキュリティのベストプラクティスから逸脱している場合に、それらを検出できることが重要になります。**AWS Foundational Security Best Practices** (AWS 基本セキュリティベストプラクティス) 標準では、クラウドセキュリティを継続的に改善するための実用的で規範的なガイダンスを提供しており、一連の統制を利用して、すべての AWS アカウントとワークロードを継続的に評価できます。

まとめ

開始方法

AWS のセキュリティソリューションとサービスをご利用いただくことで、組織の安全性を高めながら、運用方法を変革できます。その結果、時間的な余裕が生まれ、コアビジネスに集中できるようになります。

クラウド内でワークロードを保護する方法

AWS のセキュリティ、アイデンティティ、コンプライアンスを使用して安全にクラウドに移行する方法の詳細は、以下よりご確認いただけます。

詳細はこちら ›

セキュリティに関するコンテンツ

AWS から提供されるセキュリティ関連およびお客様関連のコンテンツは、AWS Security Hub をご覧ください。さまざまなセキュリティトピックに関する役立つウェビナー、ホワイトペーパー、クイックリファレンスガイド、日本語ガイドをご利用いただけます。

詳細はこちら ›