AWS セキュリティ

クラウド トランスフォーメーションを安全に実現する

AWS 活用によるセキュリティの 6 つの利点

クラウドセキュリティに関する考えの変化

クラウドに関するトピックにおいて、セキュリティは常に最大の関心事ですが、セキュリティを語る文脈は変化しています。

今日におけるお客様の関心事は、「クラウドは安全かどうか」という段階を超えて、「クラウド上でセキュリティを確保するための推奨のベストプラクティスは何か」へと移っています。お客様は、「データにアクセスするユーザーやそのタイミングを把握するために、どのような管理が可能であるか」、コンプライアンスへの準拠を確保するために、どのようにデータにアクセスして監査するか」、そして「ハイブリッドクラウド環境をどのように保護するか」、ということを知りたいと考えています。

現在利用できるクラウドコンピューティング環境の中で、AWS が最も柔軟性が高く、安全であるという確信を持って、既に多くのお客様が重要なワークロードを移行しています。これらのお客様は、常に組織のセキュリティを高めながら、コアとなるビジネスに集中できるよう、運用の方法を変革しています。

「第一波」のお客様は、クラウド上のセキュリティが、技術的なアップグレードであると同時に、カルチャーシフトでもあることに気付きました。そして、クラウド上のデータを保護する最善の方法を検討するときに、覚えておくべき重要な利点について述べています。

クラウドに対する信頼が高まるにつれ、共有インフラストラクチャ上で実行されるアプリケーションの数も増えています。これにより、クラウド上での安全な運用を行ううえでの利点やベストプラクティスを示す、さまざまなユースケースが数多く得られています。

51%

51% の IT マネージャーが、データセンターよりもクラウド上の方がデータセキュリティが高いと述べています。

58%

58% が、クラウドが自社にとって最も安全で柔軟性とコスト効果が高いソリューションであると述べています[1]。

76%

76% の企業が、急速にセキュリティをクラウドに移行しています。これらの企業は、設計上、より動的かつ機敏で、統合されたクラウドシステムおよびネットワークシステムを選択し、本質的に安全でない静的なレガシーシステムを廃止しています。

[1] SADA systems によるパブリッククラウドに関する調査

クラウドセキュリティの 6 つの利点

クラウド移行の課題の 1 つは、クラウドの導入に対する意気込みがそれぞれ異なる組織内の複数の関係者を管理することです。

クラウドセキュリティの特有の利点がどのようなものかを理解することは、組織のセキュリティ担当者やコンプライアンス担当者の懸念事項に対応するための最初のステップとなります。

以下の 6 つの利点を考慮しているプロバイダーであれば、常に組織のセキュリティを高めながら、運用方法を変革し、リソースを解放して、コアとなるビジネスに集中するための支援を行うことができます。

1. 強固なセキュリティとコンプライアンス統制の継承

2. 高度な可視化と制御によるスケーリング

3. プライバシーとデータの保護

4. 信頼できるセキュリティパートナーとソリューションの選定

5. オートメーションによるセキュリティの向上と時間の節約

6. 革新的なセキュリティ機能による継続的な改善

1.

強固なセキュリティとコンプライアンス統制の継承

クラウドプロバイダーの選択にあたっては、お客様はそのセキュリティ統制の多くを継承して、自社のコンプライアンスプログラムや認証プログラムを強化することを認識しておく必要があります。適切なプロバイダーであれば、セキュリティの保証に必要な作業のコストを大幅に削減できます。適切なプロバイダーを選択するには、第三者による認証 (国際的に認められたセキュリティのベストプラクティスや認定、業界独自の認定) を取得していることを確認します。

これらの統制の例として、クラウドセキュリティに関する ISO 27001 や ISO 27017、クラウドプライバシーに関する ISO 27018、プライバシープログラム管理に関する ISO 27701、さらに SOC 1、SOC 2、SOC 3 など、国際的に認められたセキュリティのベストプラクティスや認定が挙げられます。適切なプロバイダーは、HIPAA や PCI DSS への準拠を達成できるよう支援するサービスも提供しているほか、米国の FedRAMP や DoD SRG、ドイツの C5、オーストラリアの IRAP、シンガポールの MTCS Tier 3 などを通じて、公共部門の認定を数多く取得しています。認定と証明の詳細なリストについては、AWS コンプライアンスプログラムに関するページ (www.aws.amazon.com/compliance/programs) をご参照ください。

> *“AWS インフラストラクチャの成熟度、および AWS のデータセンターとサービスに対するセキュリティ監査のレベルの高さにより、不安は排除されました。患者と顧客データのプライバシーとセキュリティが最優先事項であることは認識していました”*
>
> *Teva、グローバルデジタルヘルス担当バイスプレジデント、Mark Maalouf 氏*

2.

高度な可視化と制御によるスケーリング

クラウド上に保存するデータが見えなくなり、忘れ去られることはありません。データの場所と、データにアクセスしているユーザーを常に把握しておく必要があります。この情報は、データが世界のどこに保存されていても、ほぼリアルタイムでどこからでも利用可能である必要があります。

エコシステム全体で設定の変更とセキュリティリスクを検出するアクティビティモニタリングサービスを組み合わせた、きめ細かいアイデンティティ管理とアクセス管理などの主な機能を探して、必要な管理を実施します。

このような管理を実施することで、リスクを減らすだけでなく、組織をより効率的にスケールできます。このようなクラウドベースの管理とサービスが、さらに既存のソリューションと統合して、運用とコンプライアンスの報告が簡略化されることが理想です。

3.

プライバシーとデータの保護

データをクラウドに移行する際は、プライバシーに十分に配慮し、許可を得ているユーザーのみがデータにアクセスできるよう、転送時および保管時のデータを簡単に暗号化できるツールを提供しているプロバイダーを探します。

さらに、グローバルなクラウドインフラストラクチャを使用する場合は、データが物理的に置かれているリージョンを完全に管理し続ける必要があります。データの管理を維持することは、組織に適用されるリージョンや地域のデータプライバシーに関する法律や規制に準拠するうえで役立ちます。

> *(シドニーリージョンを使用するベンダーの採用は、) 製品のパフォーマンスやレイテンシーの観点から、当社にとって非常に重要です。当社のお客様はオーストラリアとニュージーランドにおり、データ主権に関しても懸念材料でした。また、柔軟性の高い一連のクラウドサービスを使用し、お客様のニーズに合わせてシステムの機能を最適化したいと考えていました”*

Mind Your Own Business、デリバリー責任者、Trevor Leybourne 氏

> *私たちのデータはヨーロッパにホストされています。これはセキュリティの観点から私たちにとって非常に重要です。AWS なら、データを保存する場所やその保存方法、アクセスできるユーザーを完全に管理できます。広範な暗号化と共に、管理がなされていることで、安心感をもたらしてくれます。Trust のデータは保護されていると確信を持っています”*

MSP Sirocco Systems、ディレクター、英国ナショナルトラスト担当、Martin Brambley 氏

4.

信頼できるセキュリティパートナーとソリューションの選定

大手のクラウドプロバイダーと連携する最大の利点の 1 つは、そのプロバイダーのパートナーやクラウドセキュリティのソリューションにアクセスできること、そしてパートナーによるコンサルティングサービスが利用できることです。利用可能なセキュリティテクノロジーやコンサルティングサービスは数多くありますが、お客様の特定のユースケースに適したもの、アクセスする場所、それらのエンゲージメントの管理方法を把握するのは困難な場合があります。

パートナーを見つける ›

適切なクラウドセキュリティパートナーがどのように支援を行うことができるか

- 適切なパートナーには、お客様がクラウド導入プロセスのどの段階にいるかを理解する深い専門知識と実績があります。このようなパートナーは、お客様が適切なタイミングで適切なヘルプを得られるよう支援します。また、ハイブリッドクラウドへの移行や、クラウドへの全面移行についてスキルを持ったパートナーを見つけることもできます。
- 既知の信用できるソリューションを使用します。多くのクラウドセキュリティパートナーは、現在お客様がオンプレミスで使用しているものと同じツールやサービスを提供し、チームとデータに対してシームレスなクラウド移行を可能にします。
- 厳しく規制された環境に対しては、最も厳格なセキュリティ要件を満たし、クラウド移行を希望する種類のワークロードを構築、デプロイ、管理するための専門知識を持ったパートナーを見つけます。
- さらに、適切なクラウドパートナーは、従量制のパートナー料金と統合された請求によって、請求に関する悩みを軽減し、すべてのクラウド経費を 1 つの請求書で管理できるようにします。

5.

オートメーションによるセキュリティの向上と時間の節約

セキュリティタスクを自動化することにより、人的な設定エラーを減らし、チームの時間をビジネスに重要な他の作業に費やせるようにして、セキュリティを高めることができます。

タスクをこれまでにない方法で自動化するために、緊密に統合できるさまざまなソリューションを探しましょう。このようなソリューションにより、セキュリティチームがデベロッパーチームや運用チームと緊密に連携しやすくなり、コードをより迅速かつ安全に作成、デプロイすることが可能になります。

> ***“セキュリティアプリケーションのデリバリー速度を高めるためにAWS への移行は重要なステップでした”***
>
> ***Southwest Airlines、サイバーセキュリティエンジニアリングディレクター、Jon Barcellona 氏***

6.

革新的なセキュリティ機能による継続的な改善

クラウド上の適切なサービスとツールにより、より速いスピードおよび、より優れた俊敏性でデータを保護できます。セキュリティチームは、まさに組織全体におけるイノベーションを後押しする存在と言えます。

このような種類の変革を実現するには、スケールが重要です。世界各地の数百万もの顧客とやり取りしている経験豊富なクラウドプロバイダーは、世界的なトレンドに関する深いインサイトを備えた熟練のエンジニアチームを擁しています。このようなチームが、セキュリティに関する新しい課題に対して優れたインサイトを提供します。こういった知識や顧客のフィードバックは、プロバイダーのインフラストラクチャやサービスに組み込まれます。このような継続的なフィードバックと改善により、強力なアイデンティティ管理とアクセス管理、検出とモニタリング、暗号化とキーの管理、ネットワークのセグメント化、DDoS からの保護といった、主要なセキュリティサービスが強化され、すべての人々に利益をもたらします。

クラウドセキュリティの成功のための次のステップ

クラウド上のセキュリティは、以下の 5 つの分野と、セキュリティを意識したクラウドアーキテクチャの設計とそのクラウドアーキテクチャへの移行に役立つ推奨のソリューションで構成されます。

アイデンティティとアクセス管理	アイデンティティとアクセス管理は、許可を得ているユーザー、グループ、またはアプリケーションのみが、内部リソースにアクセスできるようにするために重要です。プロバイダーは、サービス、アクション、リソースにまたがってユーザーのアクセス許可を定義、実施、監査し、適切な条件に従って適切なユーザーが適切なリソースにアクセスするようにします。	AWS Single Sign-On AWS Identity & Access Management AWS Organizations Amazon Cognito
発見的統制	クラウドプロバイダーは、ビジネスに影響を及ぼす前に問題を見定め、セキュリティ体制を改善し、環境のリスクプロファイルを軽減するために必要な可視性を提供する必要があります。	AWS Security Hub Amazon GuardDuty AWS CloudTrail Amazon Inspector
インフラストラクチャセキュリティ	適切なインフラストラクチャセキュリティの統制により、管理してプライバシーを高める必要がある範囲を減らし、全体的なクラウドインフラストラクチャを統制できるようになります。	AWS Firewall Manager AWS Network Firewall AWS Systems Manager AWS Web Application Firewall (WAF)
データ保護	データ管理、データセキュリティ、暗号化キーの保存を含めた、自動的なデータの暗号化および管理サービスにアクセスできるようにする必要があります。	Amazon Macie AWS Key Management Service AWS Certificate Manager AWS Secrets Manager AWS CloudHSM
インシデント対応	組織は、セキュリティインシデントの潜在的な影響に対応し、そういった潜在的な影響を軽減し、既知の良好な状態に戻すためのメカニズムを実装します。	Amazon Detective AWS Elastic Disaster Recovery

AWS Well-Architected セキュリティの柱で詳細を参照する ›

このホワイトペーパーでは、AWS で安全なワークロードを設計するための詳細なベストプラクティスガイダンスを提供します。