クラウド移行とセキュリティ

ミッションクリティカルなアプリケーションを保護するためのベスト プラクティス

ホワイトペーパー

目次

多くの組織にとって、従来のオンプレミス データ センターからパブリック クラウド プラットフォームへの移行は最終段階にあります。完了まで残りわずか数年という場合もあるでしょう。Gartner は、2027 年までに 90% の組織が少なくとも一部のアプリケーションをパブリック クラウド上で運用するようになると予測しています。[1] 2028 年には、クラウド コンピューティングはもはや革新的な技術ではなく、ビジネスに不可欠な存在へと完全に変化を遂げているでしょう。[2] これには十分な理由があります。

クラウド環境では、従来のオンプレミスの環境と比較してリソースを迅速に増やし、新しいサービスを展開しながら、インフラ コストを削減できます。ミッションクリティカルなワークロード向けのクラウド導入に優先的に取り組むことで、現在の動的な環境において迅速に適応し、イノベーションや優れた成果を達成できます。

しかし、新たなチャンスにはリスクも伴います。

クラウドへの移行を迫られるなか、一部の組織はセキュリティのベスト プラクティスよりもデジタル トランスフォーメーションのスピードを優先しており、これによって脆弱性が生まれています。その結果、サイバー攻撃者はクラウドベースの標的に対する攻撃を、大きな利益を得るための簡単な手段とみなし、こうした脆弱性を悪用するための戦術を進化させています。

現代のハイブリッド環境やマルチクラウドの環境において、組織は場所や時間を問わず、かつてないほど自由にリソースの構築を行えます。しかし、これはパブリック クラウドのセキュリティに対する広範な懸念を伴うものであり、より優れたセキュリティ ツールやセキュリティ慣行を採用する必要性を示唆しています。

この複雑な状況に対処するために、組織はゼロトラストに目を向けています。ゼロトラストは、最新のクラウドネイティブなセキュリティ フレームワークであり、許可されたユーザーとデバイスのみが重要なクラウド リソースにアクセスできるようにするものです。適切に設計されたクラウド セキュリティ戦略によって、組織は侵害の防止、コンプライアンスの改善、顧客の信頼強化に向け、大きく前進することができます。

重要なアプリケーションをクラウドに移行する際には、特に、規制による厳しい監視下でのデータ ガバナンスやコンプライアンスを考慮して、セキュリティ戦略を再考することが重要です。

このホワイト ペーパーでは、クラウド トランスフォーメーションの安全を確保するにあたり、IT リーダーやクラウド セキュリティ部門が直面する重要なリスクについて取り上げます。また、パブリック クラウド環境のミッションクリティカルなアプリケーションを保護するために多くの組織が使用している実証済みの戦略やベスト プラクティスについても詳しく見ていきます。

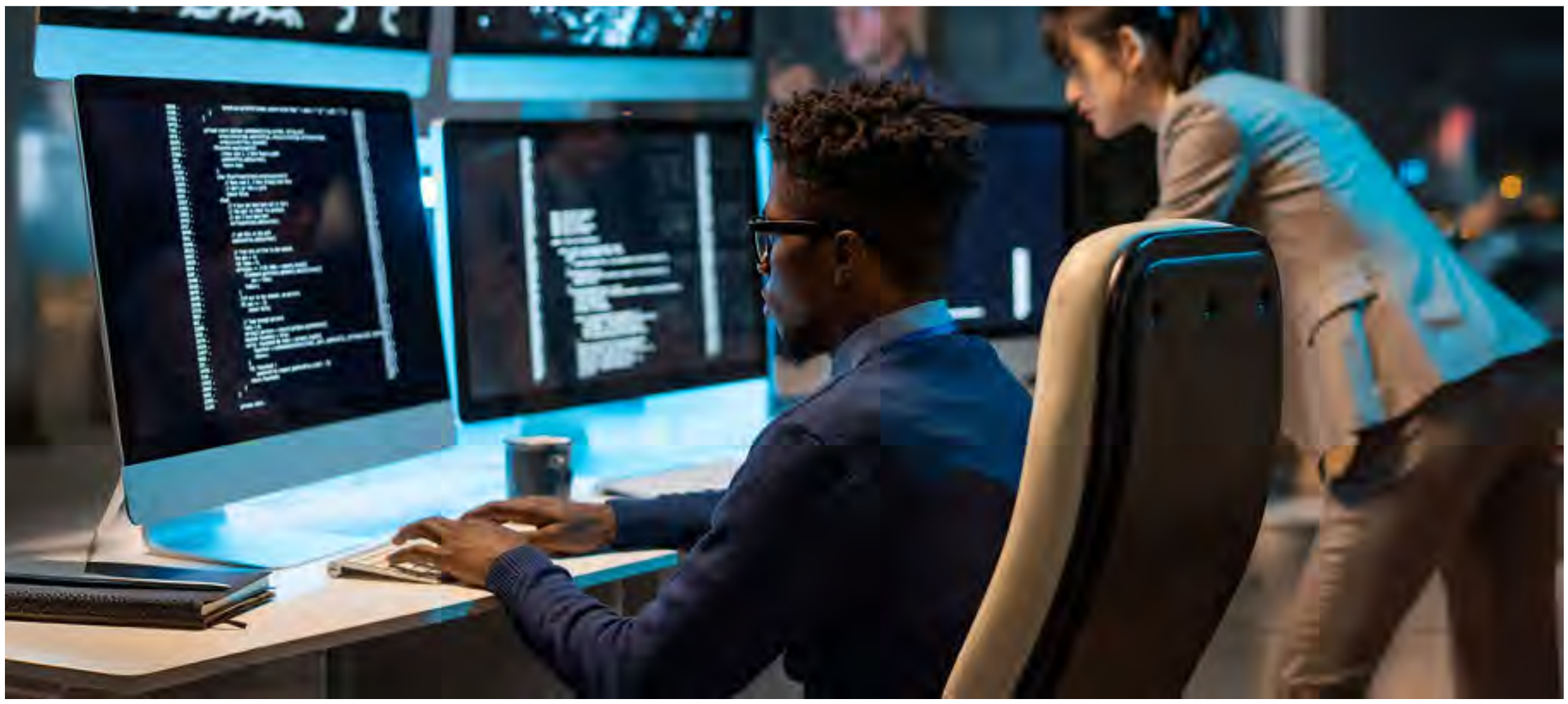
アプリケーションのパブリック クラウドへの移行で起こること

アプリケーションをパブリック クラウドに移行することは、古いレンガ造りの家を手放し、にぎやかな大都市の洗練されたモダンなマンションに引っ越すようなものです。このような移行はすばらしいものですが、複雑性も伴い、以下のようなことが起こります。

- **モノリシックなサービスからマイクロサービスへの移行：**1 つの大規模なアプリケーションは、独立した小規模なサービス (マイクロサービス) の集合体に移行します。各マイクロサービスは特定の機能を実行するように設計されており、個別に開発、展開、拡張できます。

- **API の通信の増加：**クラウドネイティブ アプリケーションは API を通じて相互に通信するため、サービス間で常にやり取りが発生する環境が生まれます。これにより、柔軟性や拡張性は高まりますが、セキュリティの脅威に対する脆弱性も増大します。

- **ワークロードの移動：**アプリケーションは 1 つのサーバー ルームに限定されず、クラウド環境上のあらゆる地域やアベイラビリティー ゾーン、ハイブリッド環境に分散するようになります。



クラウド上のミッションクリティカルなアプリケーションの保護の重要性

ミッションクリティカルなアプリケーションは、あらゆる組織の生命線であり、事業運営の維持には不可欠です。こうした重要なアプリケーションには、金融取引システム、医療プラットフォーム、産業オートメーション、企業資源計画 (ERP) システムなどがあり、完全な可用性、リアルタイムでの瞬時の処理、厳格な規制順守が求められます。

しかし、ひとたび中断が発生すれば、ビジネスや財務、企業イメージに重大な損害をもたらす可能性があり、この点が問題となります。

ミッションクリティカルなアプリケーションのクラウド移行には、拡張性、俊敏性、コスト削減などのメリットがある一方、以下のような多くの潜在的デメリットも伴います。

- **サイバー脅威に対する露出の増加：**機密性の高いデータを処理するアプリケーションは、脆弱性を悪用しようとする攻撃者の格好の標的となります。
- **運用の複雑化：**マルチクラウド環境への移行は、分散型アーキテクチャー、API 通信、動的なワークロードを生み出し、攻撃対象領域の拡大につながります。
- **コンプライアンス上の課題：**医療や金融などの業界で事業を展開する組織や政府機関は、HIPAA、GDPR、PCI DSS などの厳格なコンプライアンス フレームワークを順守する必要があり、クラウド セキュリティのガバナンスは極めて重要です。

40%

複数の環境に保存されたデータが関わる侵害の割合 [3]

想像に難くありませんが、以下のような理由から、従来のアーキテクチャーではクラウド内のミッションクリティカルなワークロードを保護できません。

1. ファイアウォール、VPN、境界ベースの防御などの従来のキュリティ ソリューションは、静的なオンプレミス環境向けに構築されており、非常に動的なクラウド ワークロードを保護する柔軟性に欠けています。
2. 従来のネットワークベースのセキュリティでは、アプリケーションレベルのきめ細かな制御を行えないため、API やマイクロサービスベースのアーキテクチャーの保護にギャップが残ります。
3. 従来のアクセス モデルは暗黙の信頼に依存しているため、認証情報ベースの攻撃、脅威のラテラル ムーブメント、内部脅威のリスクに対して脆弱です。

ミッションクリティカルなアプリケーションは高リスクの環境であり、たった一度のセキュリティ障害が壊滅的な結果に連鎖していく恐れがあります。

ダウンタイムの潜在的な影響

- 業務の停止
- 収益の減少
- 顧客からの信用の失墜

データ侵害による機密データの流出が招く結果

- 規制による罰金
- 法的紛争
- 回復不能なほどのイメージ低下

517 万ドル

パブリック クラウドに保存されたデータの侵害による損失の平均 [4]

ミッションクリティカルなアプリケーションの保護における課題

責任共有モデルとその課題

近年、クラウドは新たなテクノロジーから現代のビジネスに不可欠な基盤へと進化してきました。しかし、クラウドは本質的に安全ではないと認識することが重要です。クラウド セキュリティは、顧客とクラウド プロバイダーの間での共有責任の下に機能します。建物の構造は大家が維持する一方で、各自の部屋や所持品の安全は居住者が管理するようなものだと考えるとわかりやすいでしょう。

この責任共有モデルでは、クラウド プロバイダーは基盤となるクラウド インフラを保護し、顧客は自社のワークロード、アプリケーション、データを保護する責任を負います。しかし、クラウド プロバイダーが顧客のワークロードを完全に保護してくれるという誤解も少なくありません。このような誤解は、以下のような結果を招く可能性があります。

- **ストレージ バケットの露出：**クラウド ストレージの構成が不適切な場合、機密データの露出につながる場合があります。
- **脆弱なアイデンティティーとアクセス制御：**過度に寛容な IAM ロールは、ミッションクリティカルなアプリケーションへの不正アクセスにつながります。
- **コンプライアンス違反：**継続的な監視や施行が不十分な場合、規制上の罰則につながります。

ミッションクリティカルなアプリケーションの保護におけるセキュリティ課題の拡大

責任共有モデルの潜在的な課題に加え、クラウドにおけるミッションクリティカルなワークロードの保護には、以下のようなリスクが伴います。

- **不正なラテラル ムーブメント：**ファイアウォール、VPN、境界ベースの防御などの従来のセキュリティ モデルでは動的なクラウド環境を保護できず、不正アクセスやラテラル ムーブメントのリスクが高まります。
- **可視性のギャップ：**ハイブリッド環境やマルチクラウド環境全体で一貫したセキュリティ ポリシーを維持することは難しく、セキュリティ態勢の断片化や可視性のギャップにつながります。
- **ポリシーの標準化不足：**セキュリティ フレームワークはクラウド プロバイダーごとに異なるため、マルチクラウドの複雑さがさらなるリスクを生み出し、ポリシーの標準化が困難になります。
- **セグメンテーションの欠如：**統合されたデータ保護やセグメンテーションが不十分な場合、攻撃者は一部分を侵害した後、クラウド環境全体に拡散できます。

79%

クラウド セキュリティを最大の課題として挙げている組織の割合 [5]

クラウドのミッションクリティカルなアプリケーションを保護するための 5 つのベスト プラクティス

クラウド内のミッションクリティカルなアプリケーションを効果的に保護するには、セキュリティ ツールキットにどのような戦略を含める必要があるのでしょうか。クラウドは自動的に侵入不可能にはならないため、戦略的な計画と堅牢な防御が必要です。

クラウド セキュリティ戦略の基礎となるのは、以下の 5 つのベスト プラクティスです。これらはクラウドベースの資産を保護し、コンプライアンスを維持するうえでそれぞれ重要な役割を果たします。

1 アイデンティティーと認証に基づく最小特権アクセスの導入

- ゼロトラスト アクセス制御を採用し、許可されたユーザー、デバイス、ワークロードのみがミッションクリティカルなアプリケーションと通信できるようにします。
- IP アドレスを公開しないようにすることで、アプリケーションを不可視化します。攻撃者は、見えないものを攻撃することはできません。
- ユーザーの行動とリアルタイムのリスク分析に基づいて、アクセス ポリシーを継続的に監視、調整します。

2 ネットワークの保護からアプリケーションの保護への移行

- ネットワーク全体ではなくアプリケーションを接続することで、従来のネットワークベースのセキュリティから脱却し、バックホール、ファイアウォール、VPN の必要性を排除します。
- アプリケーションレベルでワークロードを保護するクラウド型セキュリティ ソリューションを採用し、より広範なネットワークを公開することなく安全な直接接続を確保します。
- ゼロトラスト ネットワーク アクセス (ZTNA) を活用し、アプリケーションへの安全できめ細かいアクセスを提供します。
- 攻撃対象領域を拡大させることはありません。

3 統合型の脅威対策とリアルタイムのセキュリティ検査の展開

- 侵入検知、行動分析、AI を活用した異常検知などの高度な脅威対策を導入し、サイバー脅威を特定、軽減します。
- エンドツーエンドの暗号化、情報漏洩防止 (DLP)、継続的な監視機能を提供するデータ保護ソリューションを活用します。
- 大規模なリアルタイムの脅威検査が可能なクラウド型セキュリティ プラットフォームを活用して悪意のあるアクティビティーを検出し、ミッションクリティカルなアプリケーションへの影響を未然に防ぎます。

4 ワークロード セグメンテーションの適用によるラテラル ムーブメントの防止

- マイクロセグメンテーションを適用することで、ワークロードを分離し、東西トラフィックを制限するとともに、クラウド環境での攻撃者のラテラル ムーブメントを防止します。
- 以下のような複数のクラウド レイヤーでのセグメンテーションを確保します。

A. **プロセスレベルのセグメンテーション** — ホスト内のワークロード間の通信を制限します。

B. **VPC とアベイラビリティー ゾーンのセグメンテーション** — 異なるクラウド環境間のアクセスを制限し、露出を最小化します。

C. **マルチクラウドのセグメンテーション** — AWS、Azure、Google Cloud、ハイブリッド インフラ全体で統一されたセキュリティ ポリシーを施行します。

5 自動化されたポリシー施行によるコンプライアンスの確保

- HIPAA、GDPR、PCI DSS、NIST などの業界固有の規制に沿ってクラウド セキュリティ戦略を調整します。
- 自動化されたポリシー施行とコンプライアンス監査によって、セキュリティ フレームワークに準拠した態勢を継続的に確保します。

ミッションクリティカルなアプリケーションの保護を支援する Zscaler

Zscaler は、ミッションクリティカルなアプリケーションの保護に取り組む組織を強力に支援します。クラウドネイティブの Zero Trust Exchange™ プラットフォームにより、ワークロード間の安全な直接接続を提供し、従来の VPN、ファイアウォール、バックホールの必要性を効果的に排除するとともに、アプリケーションをインターネットの脅威から保護します。ハイブリッド環境とマルチクラウド環境全体でトラフィックを継続的に検査し、脅威を検出しながら、ポリシーを施行することで、クラウド ワークロードのリアルタイムの可視性と堅牢な保護を提供します。

- **完全クラウドネイティブの Zero Trust Exchange™ プラットフォーム：**アプリケーションをインターネットに公開したり、VPN、ファイアウォール、バックホールに頼ったりすることなく、ワークロード間の安全な直接接続を提供します。
- **クラウド ワークロードのリアルタイムの可視化と保護：**ハイブリッド環境とマルチクラウド環境全体でトラフィックを継続的に検査し、脅威を検出するとともに、ポリシーを施行します。
- **自動化されたポリシー施行による安全かつコンプライアンス要件に則ったアプリケーション アクセス：**アプリケーションに対して一貫したセキュリティ ポリシーを適用し、設定ミスやコンプライアンス違反のリスクを軽減します。
- **実際の脅威の軽減：**DLP や大規模な SSL インスペクションによるデータ保護を通じ、リアルタイムのトラフィック検査、継続的な監視、AI を活用したセキュリティ分析を行い、脅威を効果的に軽減します。
- **包括的な監視と制御：**Zscaler の Cloud Connector プラットフォームは、アプリケーションやクラウド サービスへのアクセスを監視および制御し、データ フローを管理しながら、アプリケーションのセキュリティ態勢を評価します。
- **直感的なインターフェイス：**ユーザーフレンドリーなインターフェイスとポリシー エンジンによって、セキュリティ ポリシーの構成と管理を簡素化します。

Zscaler の効果の検証：SANS の製品レビューに基づくインサイト

SANS による製品レビューは、ミッションクリティカルなアプリケーションの保護における Zscaler の機能を専門的に検証したものです。[6] このレビューによると、Zscaler は主に以下の領域で優位性を持っています。

- **ゼロトラスト モデル：**Zscaler はワークロードを直接接続することで攻撃対象領域を排除し、露出とリスクを軽減します。このアプローチにより、ワークロードは発見されにくくなり、悪用されるリスクが低下します。
- **ラテラル ムーブメントの防止：**Zscaler はクラウド ワークロード全体にマイクロセグメンテーションとアイデンティティーベースのポリシーを適用し、アプリ間のセグメンテーションを通じてラテラル ムーブメントのリスクを軽減します。

SANS のレビューは、Zscaler のクラウドネイティブ セキュリティ モデルが業界をリードする存在であることを裏付けています。Zscaler は、Siemens、Micron、Mahindra Group などのグローバル企業において、最重要アプリケーションの保護、コンプライアンス要件への対応、マルチクラウド セキュリティの簡素化を支援しています。

クラウドにおける包括的なセキュリティの実現

ミッションクリティカルなアプリケーションのクラウド移行に伴って組織が直面するリスクは重大なものであり、早急な対応が必要です。しかし、適切な戦略により、安全で効率的な運用の基盤を構築することができます。

最新のゼロトラスト アーキテクチャーを活用することで、組織はあらゆる場所のアプリケーションを安全に接続して、攻撃対象領域を最小化し、ラテラル ムーブメントを防止するとともに、データが悪意のある人物にアクセスされるリスクを低減できます。これにより、クラウド セキュリティの複雑さに確実に対処し、最も価値の高い資産を包括的に保護することが可能です。

クラウドベースの資産の安全性と完全性の確保に向けた次のステップとして、デモを依頼して、クラウド ワークロード保護を根本的に簡素化する方法を直接ご確認ください。

デモを依頼する

セルフガイド演習で Zero Trust Cloud をお試しいただくことも可能です。

演習の詳細はこちら

[1] Gartner Forecasts Worldwide Public Cloud End-User Spending to Total $723 Billion in 2025

[2] Gartner Says Cloud Will Become a Business Necessity by 2028

[3] IBM Cost of Data Breach Report, 2024

[4] IBM Cost of Data Breach Report, 2024

[5] Flexera 2023 State of the Cloud Report

[6] How to Use Zero Trust to Secure Workloads in the Public Cloud, SANS, 2023

Zscaler について
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange™ は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/jp**

zscaler™

Zero Trust Everywhere