



■ EBOOK

マルチクラウド環境で 一貫したワークロード セキュリティを 実現する方法

目次

はじめに	3
クラウド ワークロード セキュリティの課題	4
クラウド移行が進むアプリケーションに必須のゼロトラスト セキュリティ	5
クラウド ネイティブ環境では機能しない従来のネットワーク セキュリティ	6
現代のコンピューティング エコシステムでは不十分な従来のサイバー防御	7
今求められるクラウド ワークロード保護の新たなアプローチ	8
ワークロードとインターネット間の通信の簡素化と保護	9
ワークロード間の通信の簡素化と保護	10
きめ細かいマイクロセグメンテーションの簡単な実現	11
クラウド ワークロード向けゼロトラスト ソリューションに必須の重要機能	12
ワークロード接続の保護の主なユース ケース	16
最適解となる Zscaler Workload Communications	17

はじめに

組織は、アプリケーションとワークロードを前例のないペースでパブリッククラウドに移行しています。もちろん、そこにはもっともな理由があります。

クラウドトランスフォーメーションは、コスト削減から運用効率の向上まで、さまざまなメリットをもたらします。クラウド移行は、デジタルトランスフォーメーションの重要な要素の一つです。組織の俊敏性を高めるとともに、顧客、ベンダー、サプライヤー、サードパーティー パートナーのニーズへの対応、顧客体験の向上に寄与します。

さまざまな業界にわたり、競争力を維持するためにクラウド戦略を推進する組織が増えるなか、パブリッククラウドは新たなエンタープライズ データセンターとなっています。同時に、ハイブリッド クラウド環境やマルチクラウド環境は標準的なものとなっています。最近の IDC Research の予測では、2025 年末までに、大多数の組織が生成 AI プラットフォーム、開発者ツール、インフラにパブリッククラウドを使用するようになり、クラウドの利用がオンプレミス システムを上回る見込みです。¹

市場シェアの 67% を占める上位 3 社のクラウド ベンダー

31%

aws

25%

Microsoft
Azure

11%

Google Cloud



Gartner は、2025 年までにアプリケーション ソフトウェア、インフラ、組織プロセス サービスへの IT 支出の 51% がパブリッククラウドに移行し、従来の IT への支出を上回ると予測しています。⁴

クラウドトランスフォーメーションは大きな勢いを見せており、パブリッククラウド プロバイダーの収益の総額は 2024 年末までに 8000 億ドルを超えると予想されています。² ただし、市場の大部分は次のわずか 3 社で占められています。³

- Amazon Web Services (AWS)、市場シェア 31%
- Microsoft Azure、市場シェア 25%
- Google Cloud、市場シェア 11%

こうしたパブリッククラウド プロバイダーは、コンピューティング リソースの使用における速度、俊敏性、弾力性の向上につながる新たな可能性を提供しています。これにより、開発者は新たな環境をわずか数秒で立ち上げることもできます。いずれのプロバイダーも、セルフマネージド型とマネージド型の両方で、数百種類のサービスを提供しています。

しかし、これらの要素は、特に最新のクラウド環境を保護するために従来のセキュリティ アーキテクチャーを利用し続けている組織において、新たなセキュリティ リスクの出現にもつながっています。オンプレミスのワークロードを保護するための従来のアプローチと、今日のクラウド環境で必要とされているものは根本的に異なるため、多くの場合、クラウド ワークロードの保護には大きなコストがかかり、複雑性と困難を伴います。

1. IDC Research, [IDC FutureScape: Worldwide Cloud 2024 Predictions](#), 2023 年。

2. IDC Research, [Worldwide Semiannual Public Cloud Services Tracker](#)。

3. Statista, [Cloud Infrastructure Market](#), 2024 年。

4. Gartner, [Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025](#)。

クラウド ワークロード セキュリティの課題

ワークロードのクラウド移行にあたって、セキュリティ アプローチの最新化を並行して進めない組織は、さまざまな共通の課題に直面します。



ポリシー施行の一貫性や効果の欠如によって、ワークロードがサイバー脅威や攻撃に対して無防備な状態になります。



クラウド ワークロードの保護、接続に従来のアプローチを利用すると、そのプロセスは必然的に複雑でコストのかかるものになります。ファイアウォールや仮想プライベート ネットワーク (VPN) をベースとしたサイバーセキュリティ アーキテクチャーは、今日のクラウド コンピューティング エコシステムのために設計されたものではありません。



公開されたワークロードはサイバー犯罪者に簡単に侵害され、壊滅的なランサムウェア攻撃の人質に取られます。こうした攻撃からの復旧には、多大なコストと時間がかかる場合があります。

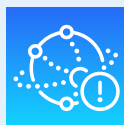


クラウド ワークロードは、他のワークロードやインターネットとの広範な通信を必要とします。従来のセキュリティ アプローチは、この常時接続に適していません。



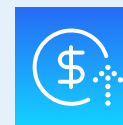
44%

2024 年にクラウドベースのデータ侵害を受けた組織の割合⁵



49%

クラウドの複雑さがコンプライアンスとセキュリティの重大な課題となっていると考える組織の割合⁶



69%

2023 年に予算を超過するクラウド支出があった組織の割合⁷

5. Thales Group, [2024 Cloud Security Study](#).

6. 同上。

7. Gartner, [2024 Cloud Spending: IT Balances Costs with GenAI Innovation](#).

クラウド移行が進むアプリケーションに必須の ゼロトラスト セキュリティ

リモートワークやハイブリッドワークが主流になるにつれ、さまざまな業界の組織がユーザーのセキュリティを確保するためにゼロトラストを採用しています。ゼロトラストアプローチでは、暗黙の信頼を付与することはありません。すべてのアクセス要求は敵対的または不正なものであると想定し、次の場合にのみアプリケーションのアクセス要求を許可します。

- アイデンティティとコンテキスト（誰が、何を、どこからリクエストしているか）を検証できる場合
- リクエストに関連するリスクを詳細に評価できる場合
- ポリシーをセッションごとに施行できる場合

クラウドに移行するアプリケーションとワークロードの数が増えるなか、アプリケーションへのアクセスに関して現在ユーザーに提供されているのと同じレベルの保護を、すべてのクラウド資産およびクラウドサービスに拡張することが不可欠です。これは、ゼロトラストベースのセキュリティをすべてのクラウドワークロードに拡張することを意味します。

従来のモノリシックアプリケーションをクラウドに移行するにあたり、組織は多くの場合、マイクロサービスアプローチを使用してリファクタリングすることを選択します。これにより、専用のクラウドデータベース、サーバーレス関数、イベントドリブンアーキテクチャーなど、クラウド独自の機能を活用することができます。また、効率が向上し、コストの削減につながるほか、動的で高度に自動化された環境を構築できます。この環境では、ワークロード間で常に通信が交わされます。

クラウドワークロードは、次のことを頻繁に行う必要があります。

- インターネットとの接続
- 他のワークロードとの通信

この種の環境では、ワークロード間で送信する必要のある通信の数が、従来のデータセンターよりもはるかに多くなります。

ワークロードとは



ワークロードは、現代のクラウドアプリケーションの構成要素です。従来のオンプレミス環境では、ほとんどのワークロードは大規模なモノリシックアプリケーション内のコンポーネントでした。しかし、今日のクラウドネイティブ環境では、アプリケーションは通常、多くのモジュール式コンポーネントやマイクロサービスで構成されています。各サービスは特定のタスクを実行し、他のサービスと通信して組織のロジックを実行します。

ワークロードの例

- コンテナ
- 仮想マシン (VM)
- 仮想デスクトップ インフラ (VDI) ファーム
- サーバーレス関数

クラウド ネイティブ環境では機能しない 従来のネットワーク セキュリティ

非常に多くの組織が、セキュリティ戦略を変更することなくクラウドトランスフォーメーションの取り組みに着手しています。しかし、従来のネットワークセキュリティアーキテクチャは、クラウドではなく、オンプレミスのデータセンター向けに構築されています。これをクラウドにリフト&シフトすることで生まれるアーキテクチャは、非常に複雑なものになるうえ、効果的ではありません。

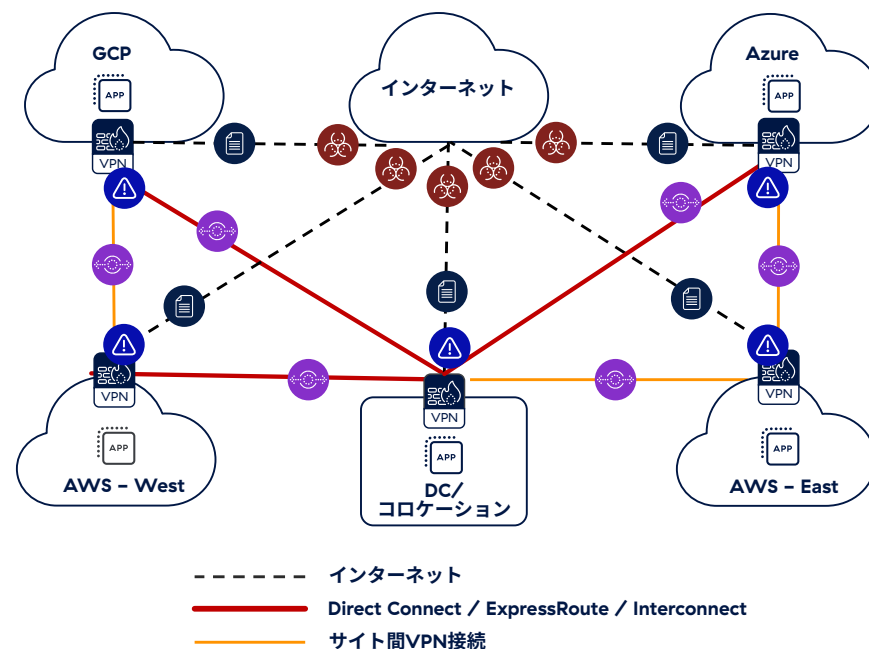
クラウドワークロードは、ワークロードどうしやインターネットとの間で安全に通信する必要があります。従来のアプローチでは、これを実現するためにファイアウォールとVPNを使用してクラウドインフラ間にルーティング可能なネットワークを構築します。これは、本質的に、組織のワイドエリアネットワーク(WAN)をクラウドに拡張する行為です。

このモデルでは、ワークロードが存在するすべての場所に仮想次世代ファイアウォール(vNGFW)を立ち上げる必要があります。ハイブリッド環境やマルチクラウド環境はあらゆる場所に存在しているため、これによってフルメッシュネットワークが構成され、各ノードが他のすべてのノードに直接接続されることになります。このアーキテクチャは非常に複雑で、管理には困難が伴います。

情報漏洩防止(DLP)やTLS/SSLインスペクションなどの追加のセキュリティ機能を実装する場合は、仮想セキュリティアプライアンスのレイヤーを追加する必要があります、いっそう複雑化します。

単一のクラウドサービスプロバイダーの環境内でも、クラウドワークロード間の南北および東西のトラフィックを保護するために、複数のvNGFWを追加で立ち上げ、管理する必要があります。

複雑さとセキュリティの課題を倍増させる ワークロード通信



攻撃対象領域



ラテラルムーブメント



サイバー脅威



情報漏洩

現代のコンピューティング エコシステムでは 不十分な従来のサイバー防御

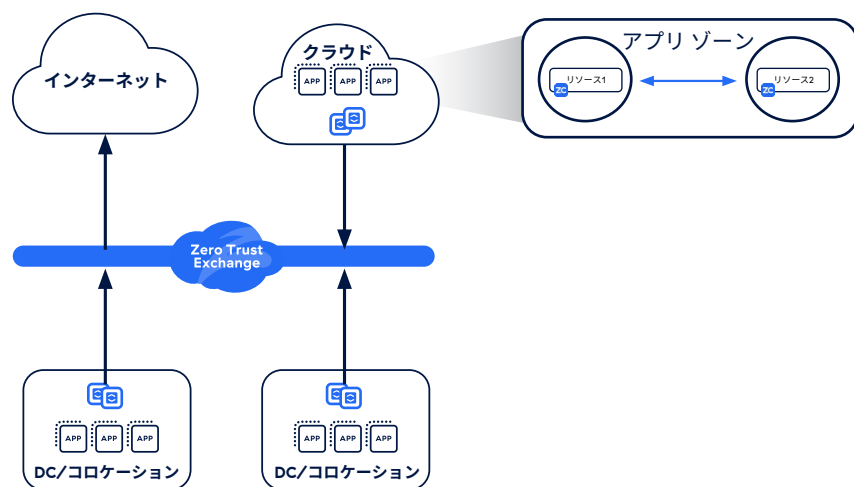
クラウド ワークロードの保護と接続に従来のアプローチを使用すると、次のような結果につながります。

- ❖ **攻撃対象領域の拡大。** 各 vNGFW は、特定可能なネットワーク上の場所を持っているため、攻撃者はこれを発見することが可能です。展開されるファイアウォールの数が多いほど、攻撃対象領域は拡大します。
- ❖ **ワークロードの侵害。** 攻撃者は、環境への侵入口を発見してそこに足場を築くと、ワークロードを侵害できるようになります。
- ❖ **脅威のラテラルムーブメント。** すべてのワークロードはメッシュ ネットワークを介して接続されているため、攻撃者は 1 つのワークロードを侵害すると、ネットワーク上でのラテラルムーブメントを通じて、他のワークロードも侵害できます。
- ❖ **機密データの抜き取り。** 攻撃者は、ネットワーク上を移動して顧客の財務情報や企業秘密などの機密データを発見し、抜き取ることができます。



今求められるクラウド ワークロード保護の 新たなアプローチ

組織は複数のクラウド サービス プロバイダーやベンダーの Infrastructure as a Service (IaaS)、Platform as a Service (PaaS)、Software as a Service (SaaS) に深く依存しており、今日のエンタープライズ コンピューティング エコシステムを保護するには、アプローチを変え、組織のセキュリティ ポリシーをネットワーク設計の中心に据える必要があります。これは、ワークロード間およびワークロードとインターネット間の直接接続に基づく、安全な最小特権アクセスを可能にすることを意味します。このようなアプローチにより、すべてのクラウド ワークロードにわたるゼロトラスト アーキテクチャーを、シンプルな形で構築、管理できます。



この最新のアプローチにより、次のことが可能になります。

- **攻撃対象領域の排除。** 従来のソリューションとは異なり、ワークロードは脅威アクターから効果的に不可視化され、本質的に攻撃対象領域全体が排除されます。
- **ワークロードの保護。** 完全なインライン コンテンツ検査とDLP 機能により、データとワークロードの堅牢なセキュリティが実現します。
- **脅威のラテラルムーブメントの防止。** ネットワークを介さず直接接続することで、ラテラルムーブメントを不可能にします。
- **データの保護。** DLP 機能に大規模な TLS/SSL インспекションを追加することで、包括的なデータ保護を大規模に提供できるようになります。
- **複雑さとコストの低減。** クラウド構成管理とセキュリティを一元化し、直接接続を可能にすることで、複雑さとコストを低減できます。

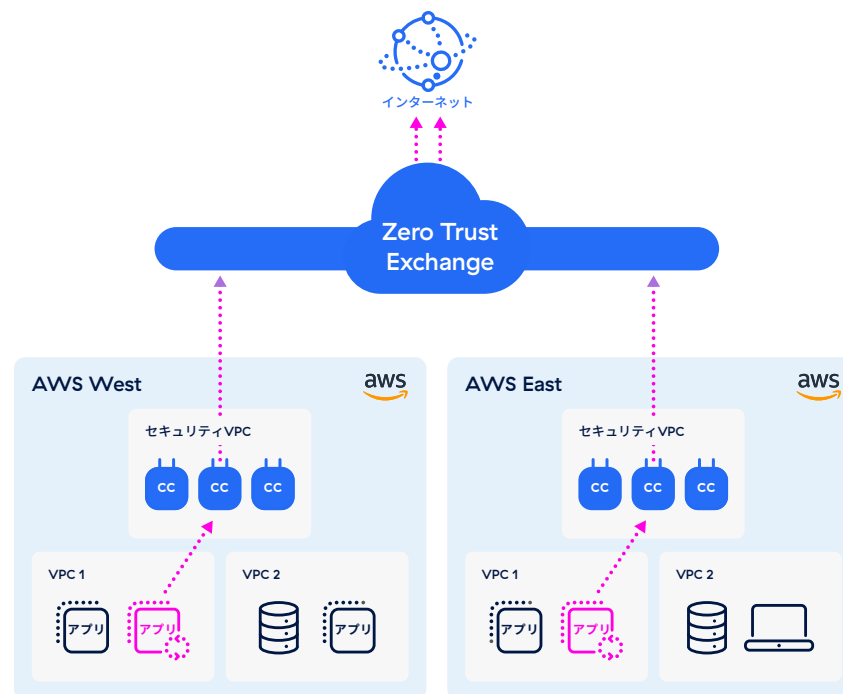
ワークロードとインターネット間の通信の簡素化と保護

すべてのクラウド ワークロードは、パブリック インターネットを介したほぼ絶え間ない通信に依存しているため、クラウド ワークロード向けのゼロトラスト ソリューションは、すべてのアウトバウンド接続を保護できなくてはなりません。また、シンプルなクラウドへの直接接続アーキテクチャーによって、パブリック クラウドにあるかエンタープライズ データ センターにあるかに関係なく、すべてのワークロードに安全なインターネット アクセスを提供できる必要があります。

ワークロードとインターネット間の通信を保護するために必要な主な機能は次のとおりです。

- プロキシベースの完全な TLS/SSL インスペクション
- 攻撃対象領域の排除
- 承認されたサイトへのアクセスのみの許可
- ゼロデイ脅威をブロックする高度なマルウェア対策

たとえば、組織のアプリが AWS West と AWS East にあり、どちらも更新が必要であるとして、リクエストは、ポリシーが施行および管理される一元的なプラットフォームに転送される必要があります。この場合に最適なのは、ゼロトラスト ポリシーを施行し、発信元と接続先を安全に接続できるソリューションです。



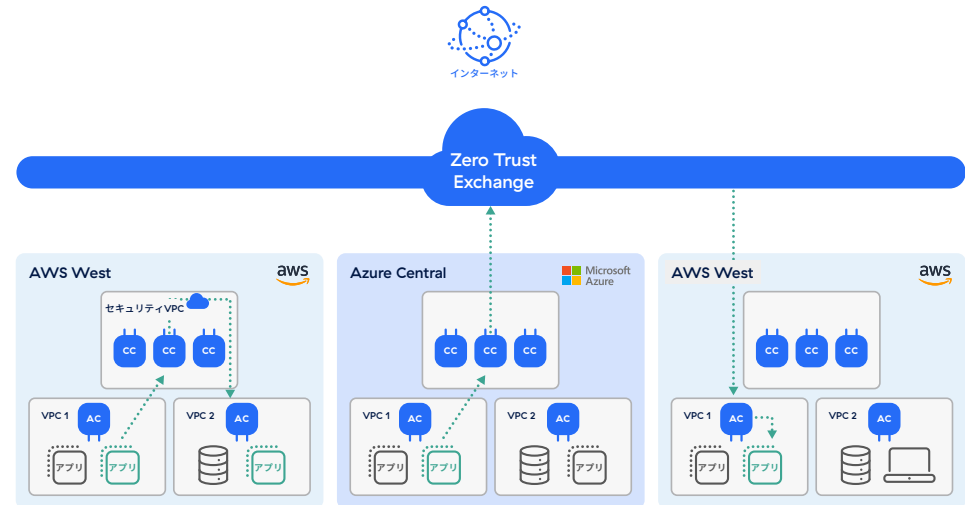
ワークロード間の通信の簡素化と保護

クラウド ワークロードにゼロトラストを適用するには、ワークロード間の安全な接続が必要です。複数のクラウド間と単一の仮想プライベート クラウド (VPC) 内の両方で通信できることは、ワークロードにとって不可欠です。これらの通信は、一元的なゼロトラスト プラットフォームを経由する必要があります。ここでセキュリティ ポリシーを適用し、アイデンティティとコンテキストを使用して信頼性を検証したうえで接続を許可します。

特に必要なのが、ワークロード内の通信を円滑化するメカニズムです。VPC 間の接続の場合、トラフィックは1つの VPC から1つの Private Service Edge にルーティングされ、そこから (別の VPC にある) 宛先のアプリへの接続が仲介されます。クラウド間の接続の場合、トラフィックは一元的なゼロトラスト プラットフォームに転送され、接続は別のクラウドにある接続先アプリに転送されます。

ワークロード間の通信を保護するために必要な主な機能は次のとおりです。

- マルチクラウドとマルチリージョン接続の保護
- VPC 間 / VNET 間の接続の保護
- ゼロトラスト ネットワーク アクセス (ZTNA) によるネットワークの攻撃対象領域の排除
- 脅威のラテラルムーブメントの阻止



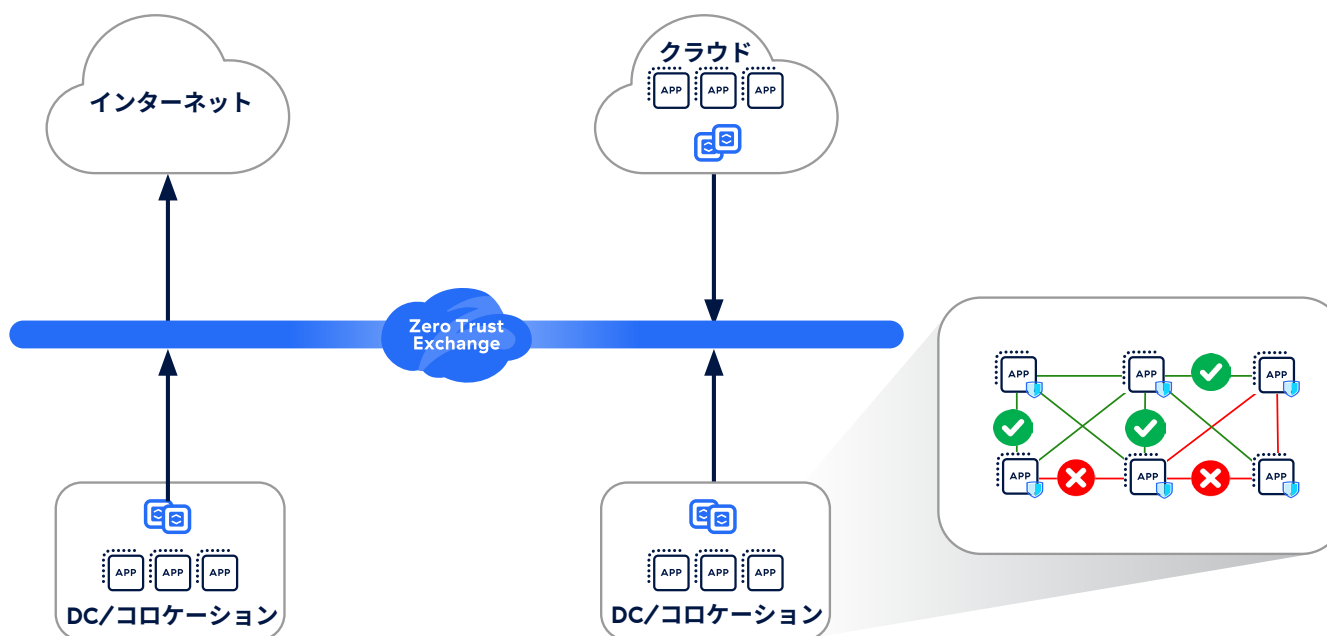
きめ細かいマイクロセグメンテーションの簡単な実現

マイクロセグメンテーションは、ゼロトラスト セキュリティのコア コンポーネントであり、個々のアプリケーションの通信要件に基づいてアプリケーションまたはワークロードのグループを小さなセグメントに分割することにより、脅威のラテラルムーブメントを防ぎます。ワークロードの通信は、自身が属するセグメント内でのみ許可され、セグメント外のワークロードと許可されていない通信を交わすことはできません。

マイクロセグメンテーションにより、組織の境界だけでなく、組織の内部ネットワーク全体にきめ細かいレベルでゼロトラスト ポリシーを施行できるようになり、オンプレミスのワークロードにもクラウドで実行されているワークロードにも、一貫した保護を拡張できます。

ワークロードのマイクロセグメンテーションに必要な主な機能は次のとおりです。

- AI を活用したリアルタイムのリソース検出
- ホストベースと非ホストベースのセグメンテーション
- VPC/VNET 内および VPC/VNET 間でのワークロードのセグメンテーション機能



クラウド ワークロード向けゼロトラストソリューションに必須の重要機能

#1: 大規模な TLS/SSL インспекションを実行する能力

今日の最も危険な脅威の多くは、暗号化されたトラフィックに紛れ込む形で隠れています。これらを検出するには、従来のアプリケーションに付きまとうパフォーマンス上の制約なく、完全な TLS/SSL インспекションを大規模に実行できる包括的なプラットフォームが必要です。

求められるのは、以下のような機能や特長を持つソリューションです。

- **無制限の容量**：パフォーマンスを懸念することなく、すべてのユーザーの TLS/SSL トラフィックを検査
- **柔軟な拡張性**：トラフィックの需要に対応
- **証明書管理の合理化**
- **きめ細かなポリシー制御**：医療機関や金融機関などのカテゴリーに属する Web サイトへの暗号化されたユーザー トラフィックを除外し、コンプライアンスを簡素化



#2: 堅牢なデータ保護機能

多層防御アプローチによるデータ保護には、パフォーマンスに影響を与えることなく、DLP ポリシーを大規模に施行する機能が必要です。これにより保護レイヤーを追加し、万が一クラウド ワークロードが侵害された場合でも、ポリシーを施行してデータの抜き取りを防ぐ仕組みを整備できます。

求められるのは、以下のような機能や特長を持つソリューションです。

- 合理化されたダッシュボード：DLP ポリシーを構成、管理
- 高度なデータ管理技術：完全データ一致 (EDM)、光学文字認識 (OCR) など
- 信頼性の高い大規模なインライン コンテンツ検査



#3: 高度な脅威対策機能

今日の最も危険で巧妙な脅威をブロックするには、すべてのワークロードのすべてのパケットを最初から最後まで完全に検査できるゼロトラスト クラウド ワークロード セキュリティ プラットフォームが必要です。これには、統合された常時オンの TLS/SSL インスペクション機能と、すべてのトラフィックに対してきめ細かなポリシーを施行する機能が求められます。

さらに、次のような機能も重要になります。

- **統合されたデセプション テクノロジー**：デコイ、ルアー、ハニーポットを使用して、最も貴重な資産を高精度かつ誤検知の少ない形で保護
- **クラウド サンドボックス**：潜在的な脅威を通過させず、隔離して検査
- **マルウェア対策**：既知のランサムウェア、スパイウェア、マルウェア、および新たな脅威をブロック



#4: 包括的なホストベースのセグメンテーション

マイクロセグメンテーションは、脅威のラテラルムーブメントを防ぎ、サイバーインシデントによる潜在的な影響範囲と損害を最小限に抑えます。ホストベースのマイクロセグメンテーションは、エンドポイントデバイスにインストールされたエージェントを利用して、より詳細な制御と可視性を提供し、アイデンティティベースのセグメンテーションの管理を容易にします。エージェントを使用することで、静的なネットワークレベルのルールではなく、人間が理解できる動的ポリシーに基づくセグメンテーションが可能になります。

特に、以下のような機能や特長を持つソリューションが求められます。

- **リアルタイムのリソース検出**：AIを活用して、組織のエコシステム内のすべてのデバイス、サービス、資産をきめ細かく可視化
- **ゼロトラストポリシーの推奨**：トラフィック分析に基づく提案
- **ゼロトラストプラットフォームとの統合**：複数のポイント製品を展開することなく、組織の環境を1か所から保護、セグメント化



ワークロード接続の保護の主なユース ケース

ワークロード接続向けのゼロトラスト ソリューションにより、組織はいくつかの重要課題を解決できます。最も一般的なものは以下の 4 つです。



インターネットへのトラフィックの保護

アプリケーションがインターネットや SaaS アプリケーションと通信する場合、サイバー攻撃や情報漏洩への対策として、出力トラフィックを検査する必要があります。Zscaler は、世界最大のインライン クラウド セキュリティ プラットフォームを運用しており、これによって、パフォーマンスへの影響やサービスの低下を引き起こすことなく、クラウドならではの規模で高度な脅威対策を実現できます。



ワークロード セグメンテーション

適切なワークロード通信ソリューションによって、きめ細かく体系的なアプローチでワークロードのセグメンテーションを行えます。これにより、VPC、リージョン、パブリック クラウドおよびプライベート クラウドのワークロード接続を制御するポリシーを簡単に適用できるようになります。



クラウド移行

これは、多くの場合、時間と手間のかかるプロセスです。どの移行戦略に従うべきかなど、多くの要素を考慮する必要があります。単純なリフト&シフトが適切なのか、アプリをリファクタリングまたは再構築すべきかなどを検討しなくてはなりません。適切なワークロード通信ソリューションを利用すれば、新たに移行したクラウド アプリをよりシンプルかつ簡単に安全に接続できます。



合併と買収 (M&A)

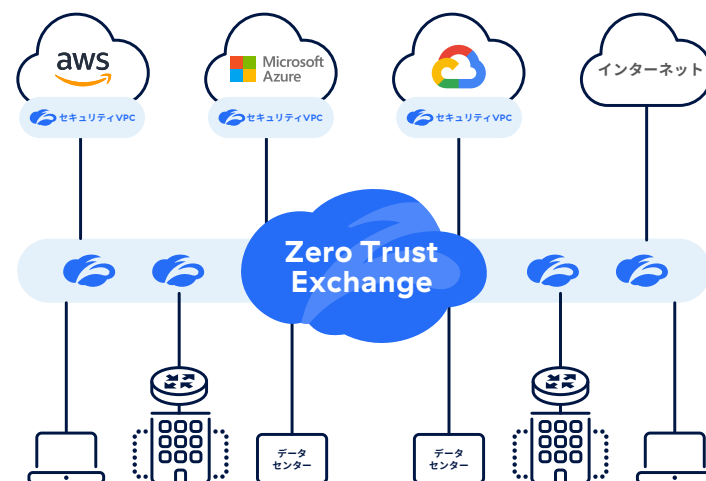
ゼロトラストベースの最新のクラウド ネイティブ ワークロード通信ソリューションを使用することで、ネットワークを再設計、リアーキテクトして接続することなく、ネットワークをまたぐ安全なアプリケーション アクセスを提供できます。

最適解となる Zscaler Workload Communications

Zscaler は、ここまで挙げたすべての機能や特長を備えた、エンドツーエンドソリューションを提供しています。Zscaler Zero Trust Exchange™ を利用することで、実績あるシンプルなクラウドへの直接接続アーキテクチャーを通じ、これまでとはまったく異なる形でワークロード通信を保護することが可能です。

Zscaler Workload Communications は、ワークロードとインターネット間の通信に対応する Zscaler Internet Access™ (ZIA)、ワークロード間の通信に対応する Zscaler Private Access™ (ZPA)、エンティティー単位のセグメント化を可能にするゼロトラスト マイクロセグメンテーション機能を組み合わせ、クラウドとオンプレミスのワークロード接続を保護する包括的なアプローチを提供します。パフォーマンスを維持してユーザーに優れたエクスペリエンスを提供できるほか、運用の拡大に伴うクラウド フットプリントの進化に対応できる拡張性も備えています。

Zscaler Workload Communications は、ニーズに合わせて拡張できる、極めて効果的なゼロトラストベースのクラウド セキュリティを実現します。このソリューションでは、弾力的な自動スケーリング機能により、トラフィックの増加に簡単に対処することが可能です。Zero Trust Exchange は、世界中に 150 か所以上のデータ センターを持ち、すでにハイパースケールで運用されています。更新はすべてお客様に代わって Zscaler が自動的に処理します。また、トランジット ゲートウェイやロード バランサーなどの機能を活用し、インフラはパブリック クラウド プロバイダーのセキュリティ インフラとネイティブに統合されています。



さらに、Zscaler Workload Communications は、ポリシー管理を簡素化、一元化します。すべてのポリシーは、使いやすい単一のコンソールで作成および更新できます。これらは Zero Trust Exchange 内で適用され、ZIA または ZPA のポリシーを活用することで、ワークロード通信に対して完全なコンテンツ検査とアイデンティティーベースの制御を施します。この通信は、Zero Trust Exchange からインターネットやクラウド環境内の他のプライベート アプリケーションなど、任意の接続先に転送できます。クラウドに追加のワークロードを展開する必要がある場合、ポリシーはいつでも簡単に拡張して適用できます。

Zscaler Workload Communications のメリットについての詳細は、Zscaler の担当者にお問い合わせください。概要は[こちらの Web ページ](#)でもご確認ください。



Experience your world, secured.™

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 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 SASE 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](https://twitter.com/zscaler) をフォローしてください。

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, ZDX™, および zscaler.com/jp/legal/trademarks に記載されたその他の商標は、米国および/または各国の Zscaler, Inc. における (i) 登録商標またはサービス マーク、または (ii) 商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。