データ シート

Zscaler Workload Communications

Zscaler Workload Communications は、Zscaler Zero Trust Exchange™ の機能を活用してワークロードとインターネット間のトラフィック、あらゆるクラウドやリージョンのトラフィックを保護し、ミッションクリティカルなクラウド ワークロードのセキュリティを確保します。

パブリック クラウドが普及したことで大規模なデジタル トランスフォーメーションが可能になり、複数のパブリック クラウドまたはデータセンターの SaaS アプリケーションやワークロードで機密性の高い通信やデータをホストするクラウドベースのワークロードが大量に流入しています。

そのため、これらのミッションクリティカルなワークロードを保護することは、企業が機密データの安全性を確保し、継続的な成功を収めるうえで不可欠な要素となっています。しかし、レガシー アーキテクチャーではパブリック クラウドのワークロードを十分に保護できないばかりか、ラテラル ムーブメントの増幅、運用の複雑さとコストの増大、一貫性のない脅威対策とデータ保護などの課題が生じます。

Zscaler Workload Communications は、クラウド ワークロードのセキュリティを根本的に簡素化します。Zscaler Zero Trust Exchange™ の機能を活用してワークロードとインターネット間のトラフィック、あらゆるクラウドやリージョンのトラフィックを保護し、ミッションクリティカルなクラウド ワークロードのセキュリティを確保します。

Workload Communications はラテラル ムーブメントを排除し、運用コストと複雑さを軽減し、一貫した脅威対策とデータ保護を提供することで、効果的なゼロトラスト セキュリティを実現します。

> “Zscaler Workload Communications では、ユーザーとアプリケーションの場所を問わず、両者のセキュリティ ポリシーの標準化を簡単に行えます。
>
> **Rui Cabeço 氏**、Siemens、グローバル アウトバウンド接続責任者

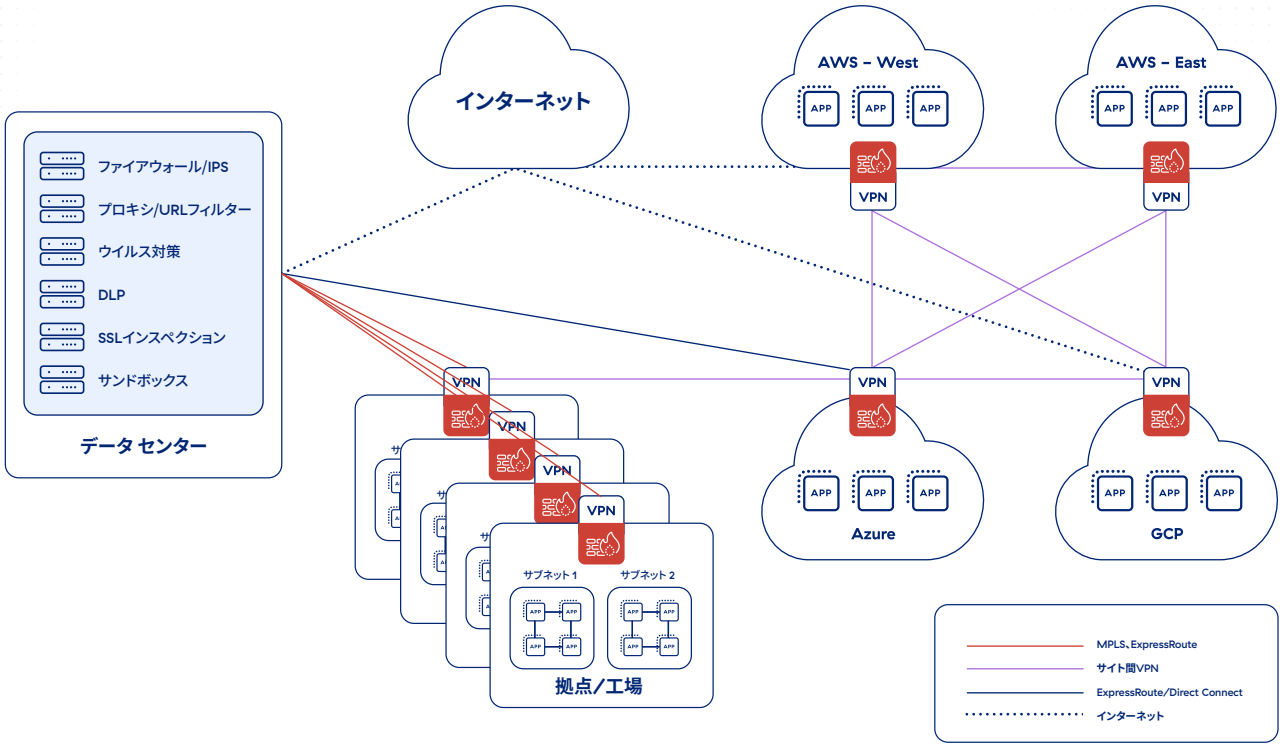
従来のクラウド ワークロード セキュリティが抱える課題

多くの企業は旧式のセキュリティ アーキテクチャーでクラウド ワークロードを保護し、以下を組み合わせて使用しています。

- パブリック クラウド サービス プロバイダーが提供するネイティブ セキュリティ ソリューション
- サードパーティー製のツール (ファイアウォール、VPN、TLS/SSL インスペクション、DLP など) による追加の保護レイヤー
- インスペクションと保護を行う従来型のオンプレミス ネットワーク セキュリティ インフラ

しかし、このアーキテクチャーには次のような課題があります。

- **脅威のラテラル ムーブメントとサイバー リスクの増幅。**サイト間 VPN やファイアウォールなどのネットワーク接続やセキュリティ ソリューションは、ネットワークをクラウド ワークロードにまで拡張するため、ラテラル ムーブメントのリスクを増幅させます。また、インターネットに接続するファイアウォールでは攻撃対象領域が拡大するため、インターネットがさまざまなクラウドやオンプレミス環境にまで広がる可能性があります。加えて、仮想アプライアンス、運用ツール、非標準ポリシーの寄せ集めがもたらす既知や未知のセキュリティ ギャップもリスクを増大させます。
- **複雑さの増加とパフォーマンスの低下。**従来のネットワークおよびセキュリティ ソリューションはクラウド ワークロードを考慮した作りにはなっていないため、サイト間 VPN を作成する必要があります。仮想ファイアウォール、プロキシ、NAT ゲートウェイなど多数のポイント製品を組み込む必要があるだけでなく、ソリューションによってはセキュリティ機能ごとに個別の VM を使用する場合があり、その結果、組立ライン形式の検査が順次行われ、遅延が発生します。これをマルチクラウド全体に適用すると、運用が非常に複雑になります。
- **コストの上昇。**旧式のネットワーク セキュリティ ポイント製品 (ファイアウォール、IPS、ルーターなど) の使用、スケーラビリティー不足を補うためのネットワーク セキュリティ インフラの過剰なプロビジョニング、そしてクラウド ネイティブ サービスの利用増加はすべて、設備投資と運用コストの上昇につながります。
- **TLS の可視性のギャップ。**TLS インスペクションは通常、コンピューティング リソースの増加を伴うため、有効にするとパフォーマンスが低下する場合があります。配布された証明書を管理したり、固定されたワークロードに除外を適用したりすると運用上の課題が生じます。また、多くの場合、スケーラビリティーを確保するためのサイバーセキュリティ インフラにかかるコストが増加します。
- **共通ログの欠如。**法的および規制上の要件により、ログを長期間保存する必要がありますが、さまざまなクラウド環境からこれらのログにアクセスして中央の SIEM インフラに保存すると、複雑さとコストが増加する可能性があります。



ゼロトラスト アーキテクチャーをクラウド ワークロードにまで拡張する Workload Communications

Workload Communications は、ゼロトラスト アーキテクチャーを使用してワークロードをインターネットやプライベート アプリケーションに接続するため、ネットワークの攻撃対象領域が排除されます。これにより、サイト間 VPN やファイアウォールへの依存度が低下し、接続が大幅に簡素化されるほか、実績のある ZIA および ZPA ポリシー フレームワークによって柔軟な転送と容易なポリシー管理が可能になります。

これらすべての基盤となるが Zscaler Zero Trust Exchange です。Workload Communications はワークロードのエグレス トラフィックをすべて Zero Trust Exchange に転送し、そこでセキュリティ ポリシーを適用してフル TLS/SSL インスペクションとアクセス制御を行います。その後、ワークロードのトラフィックはインターネット、SaaS アプリケーション、または異なるパブリック クラウドやデータ センターでホストされる他のワークロードなどの本来の宛先に転送されます。

Workload Communications を使用すると、次のようなメリットが得られます。

ラテラル ムーブメントの排除

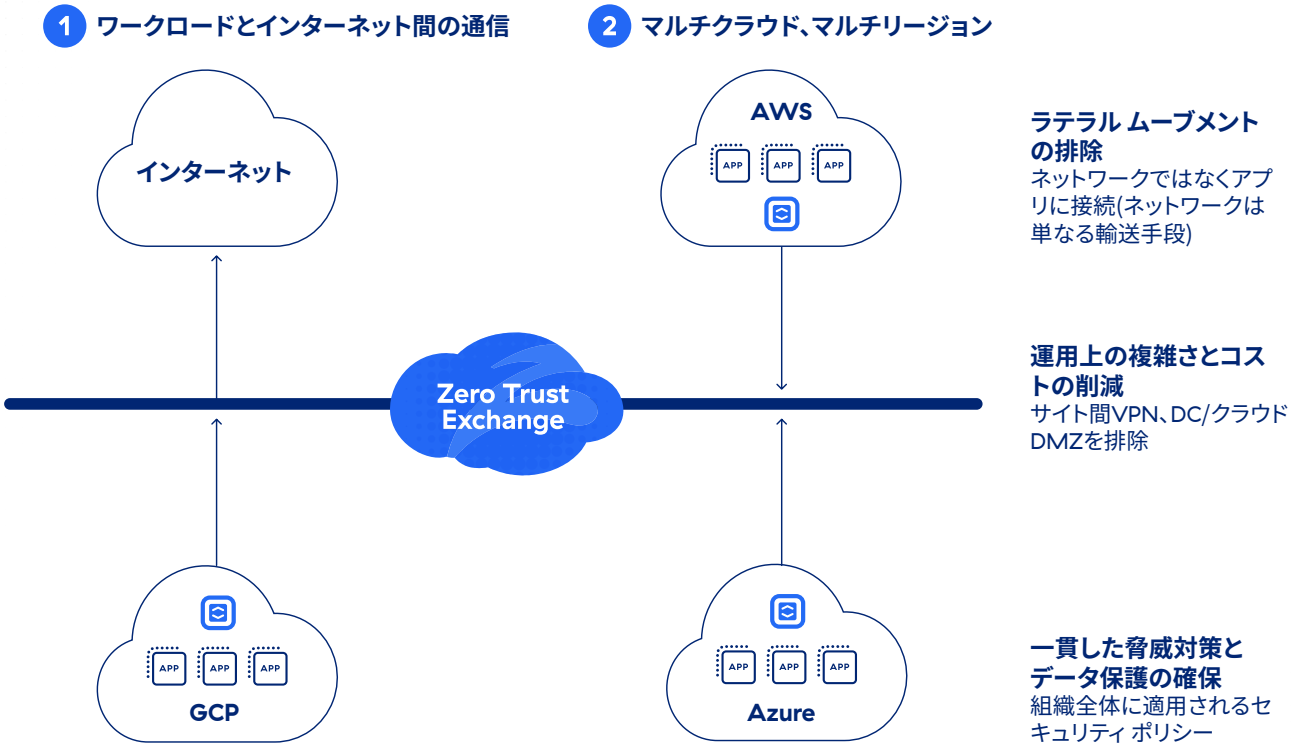
- Zscaler のゼロトラスト アーキテクチャーにより、クラウド ワークロードとアプリケーションに対して最小特権アクセスが適用されるため、クラウド ワークロードは旧式のネットワーク セキュリティ アーキテクチャーを使用する企業ネットワークではなく、承認されたワークロードにのみ接続されます。

運用コストと複雑さの軽減

- AWS、Azure、GCP などの主要なクラウド サービス プロバイダーのワークロードを 1 つの統合プラットフォームで保護します。
- Infrastructure as Code (IaC) テンプレートを使用したプログラム可能なインターフェイスと、AWS Gateway Load Balancer、AWS ユーザー定義タグ、AWS Auto Scaling などのパブリック クラウド サービス プロバイダーとの統合により、セキュリティの展開を自動化します。

一貫した脅威対策とデータ保護の実現

- クラウド ワークロード セキュリティをゼロトラストの原則にまで引き上げます。クラウド規模の TLS インスペクション、セグメンテーション (VPC/VNet、リージョン、パブリック クラウド全体)、高度な脅威対策、情報漏洩防止により、ゼロデイ攻撃を防止してデータを保護します。



Workload Communications のメリット

ワークロードのためのゼロトラスト セキュリティ。ネットワークやセキュリティに依存するこれまでの制御とは異なり、ワークロードには多数のコンテキスト属性に基づくゼロトラスト セキュリティが適用されます。

ビジネス ポリシーの施行と管理の簡素化。トラフィック転送とセキュリティのポリシー管理は、ワークロード通信の送信元または宛先に関係なく、Zero Trust Exchange で一元化および標準化されます。

クラウドへの直接接続によるエンドツーエンドの可視性。エグレス トラフィックが完全に可視化されるため、作業担当者はワークロードの通信方法を制御できます。ログ記録は一元化され、リアルタイムでストリーミングされます。また、関連付けと分析のために、ログを任意の SIEM やモニタリング ソリューションにエクスポートすることも可能です。

中央のチョークポイントを必要としないハイパースケーラビリティーとパフォーマンス。Zero Trust Exchange はハイパースケールで動作し、弾力的な水平スケーリングでワークロード トラフィックの増加に対応します。Zscaler のクラウド ネイティブ アーキテクチャーは、ネットワーク ホップとそれに伴う遅延を削減し、アプリケーションのパフォーマンスを向上させます。

信頼性の高いセキュリティのための高可用性。必要なすべてのサービスが Zero Trust Exchange で透過的に適用されるため、Workload Communications はクラウド構成要件を大幅に簡素化します。

Zero Trust Exchange が提供する合理化されたサービスによるコスト削減。Workload Communications には隠れたコストがありません。実際に利用した分のセキュリティ サービスに対してのみ料金が発生します。

Workload Communications のユースケース

ミッションクリティカルなクラウド アプリケーションの保護
ゼロデイ攻撃、データ流出、ランサムウェア攻撃からミッションクリティカルなアプリケーションを守り、事業継続性を確保します。

サイト間 VPN の排除
ゼロトラストにより、異なる VPC/VNet、リージョン、パブリック クラウドのワークロードの接続時に最小特権アクセス ポリシーが適用されます。

吸収合併に伴う統合の加速化
ネットワーク同士を接続することなく、異なるネットワーク上のアプリケーションにアクセスできるため、M&A 後の統合作業を合理化できます。統合された組織全体のセキュリティ態勢を管理し、複数の VPC、リージョン、パブリック クラウドにわたりワークロードを保護します。

クラウド 仮想デスクトップ インフラの保護
ポリシーの適用により、明示的に許可されたサイトやプライベート アプリケーションへのアクセスを制御し、クラウド インフラで提供される永続的および非永続的な VDI を保護します。

Workload Communications の主な機能

ZSCALER WORKLOAD COMMUNICATIONS プラットフォーム	
特長	**詳細**
クラウド カバレッジ	AWS、Microsoft Azure、Google Cloud Platform でのワークロードの保護をサポートします。
TLS/SSL インスペクション	無制限の TLS/SSL インスペクションで暗号化されたトラフィックに潜む脅威とデータ流出を特定します。また、プライバシーや規制の要件に基づいて、検査する Web カテゴリーまたはアプリを指定します。
ログ ストリーミング	Zscaler Nanolog Streaming Service は、世界中のすべてのワークロードのログをお客様が指定する中央リポジトリーに統合するため、管理者はクラウド ワークロードごとのトランザクション データをリアルタイムで表示およびマイニングできます。
Infrastructure as Code	Zscaler は、セキュリティ ポリシーと Cloud Connector 仮想マシンのプロビジョニングと展開を自動化する Terraform テンプレートおよびプロバイダーを提供します。

ワークロードとインターネット間を保護する ZSCALER INTERNET ACCESS	
特長	**詳細**
ワークロードとインターネット間の通信の保護	ワークロードとインターネット間の通信をサイバー脅威やデータ流出から保護します。すべての通信に対して SSL インスペクション、IPS、URL フィルタリング、データ保護が行われます。
URL フィルタリング	指定された Web カテゴリーや接続先へのワークロード アクセスを許可、ブロック、警告、または分離することで、Web ベースの脅威を阻止し、組織のポリシーに対するコンプライアンスを確保します。
高度な脅威対策	マルウェア、ランサムウェア、サプライ チェーン攻撃などの高度なサイバー攻撃を独自の高度な脅威対策で阻止します。また、組織のリスク許容度に基づいて、ポリシーを詳細に設定することもできます。
マルウェア分析	高度な AI/ 機械学習を使用して、悪意のあるインラインのペイロードに潜む未知の脅威を検出、防止、隔離することで、脅威の感染源となる攻撃を阻止します。
侵入防止	ボットネット、高度な脅威、ゼロデイ攻撃から完全に保護しながら、ワークロードに関するコンテキスト情報を取得します。クラウド IPS および Web IPS は、ファイアウォール、サンドボックス、DLP 間でシームレスに機能します。
DNS セキュリティ	不審なコマンド&コントロール接続を特定し、Zscaler の脅威検知エンジンにルーティングして、コンテンツ全体を完全に検査します。
DNS フィルタリング	既知および悪意のある接続先に対する DNS リクエストを制御、ブロックします。
ファイル制御	ワークロード アイデンティティーまたはアプリケーションに基づいて、アプリケーションへのファイルのダウンロード / アップロードをブロックまたは許可します。
帯域幅制御	帯域幅のポリシーを適用することで、ビジネスクリティカルなアプリケーションが業務に関係のないトラフィックより優先されるようにします。
動的なリスクベースのアクセスとセキュリティ ポリシー	セキュリティとアクセスのポリシーをワークロード、インターネット上の宛先、コンテンツのリスクに自動的に適応させます。
関連付けされた脅威に関するインサイト	コンテキスト化および関連付けされたアラートには脅威スコアや影響を受ける資産、重大度などに関する情報が含まれており、調査と対応にかかる時間を短縮できます。

ワークロード間を保護する ZSCALER PRIVATE ACCESS	
特長	**詳細**
ワークロード間のセグメンテーション	ZPA for Workloads を使用して、ハイブリッドでマルチクラウドな環境のワークロード間の接続と通信を保護します。
アプリの検出	特定のドメイン名と IP サブネットを使用してアプリケーションを自動的に検出してカタログ化し、プライベート アプリの資産と潜在的な攻撃対象領域に関する詳細なインサイトを取得します。
AI 活用型のアプリ セグメンテーション	ZPA で自動的に配信される ML ベースのセグメンテーションの推奨事項を適用することで、適切なアプリケーションのセグメントを迅速かつ容易に特定し、適切なアクセス ポリシーを構築します。ML ベースのセグメンテーションは、何百万ものお客様のシグナルと組織独自のアプリケーション アクセス パターンで継続的にトレーニングされた機械学習モデルによって強化され、内部の攻撃対象領域を最小化するうえで有効です。
AppProtection	脅威を明らかにするアプリケーション ペイロード全体の高性能なインラインのセキュリティ インスペクションにより、最も一般的な攻撃からプライベート アプリとインフラを保護します。OWASP Top 10 などの既知の Web セキュリティ リスクや、従来のネットワーク セキュリティ制御を回避する新たなゼロデイ脆弱性を特定してブロックします。

データ保護	
特長	**詳細**
データのインライン保護 (転送中データが対象)	ワークロードとインターネット間、ワークロード間において、フォワード プロキシと SSL インスペクション機能により、リスクの高い Web の接続先やクラウド アプリケーションへの機密情報の流れをリアルタイムで制御し、データに対する内部や外部からの脅威を阻止します。また、アプリケーションが承認されているか、管理されていないかにかかわらず、ネットワーク デバイスのログを必要とすることなく、高度なインライン保護を提供します。
完全データー致 (EDM)	企業のカスタム データのフィンガープリントを生成し、保護します。
インデックス文書一致 (IDM)	カスタム文書やフォームのフィンガープリントを生成し、保護します。
光学式文字認識 (OCR)	画像やスクリーンショットからのデータ流出を特定して防止します。

(記載されている機能をすべて網羅しているわけではありません。Zscaler エディションによって利用できる機能が異なる場合があります。)

Workload Communications 独自の価値

Workload Communications は Zero Trust Exchange 上に構築されており、あらゆるネットワークやクラウドのユーザー、デバイス、アプリをビジネス ポリシーを使用して大規模かつセキュアに接続します。

- アプリケーションとワークロードは基盤となる企業ネットワーク、VPN、WAN から独立して、相互に直接接続されます。
- アプリケーションは外部に公開されないため、攻撃対象領域は存在しません。
- 専用のマルチテナント プロキシ アーキテクチャーにより、ポリシーの保持、検査、施行が可能になります。
- 高性能なインスペクションは、拡張性を考慮して構築されたシングルスキャンおよびマルチアクセス アーキテクチャーによって実行されます。
- Zscaler Internet Access または Zscaler Private Access のポリシーを使用して、インターネットとインターネット以外のトラフィックに対するきめ細かな転送ポリシーを管理します。
- AWS、Azure、Google Cloud、オンプレミスのデータ センター全体で標準化された統一ポリシーにより、ポリシー管理、トラフィック モニタリング、ログ追跡が可能になります。

zscaler™ | 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 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.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.jp