データ シート

Zero Trust Cloud

Zscaler Zero Trust Exchange™ でワークロードとインターネット間およびワークロード間のトラフィックを保護

デジタル トランスフォーメーションが加速するにつれ、オンプレミス、プライベート クラウド、パブリック クラウドなどのさまざまなインフラでホストされるワークロードの生成と利用が増加しています。企業の活動はこうしたワークロードのもとに成り立っているため、サイバー攻撃や情報漏洩の防止が不可欠です。

しかし、こうした課題に従来のアーキテクチャーで対処しようとしても、一貫した脅威対策とデータ保護は確保できず、攻撃対象領域が増大し、ラテラル ムーブメントのリスクが残るうえ、運用の複雑さやリスクの増大を招きます。

Zscaler Zero Trust Cloud は、ハイブリッド ワークロードのセキュリティを根本的に簡素化します。Zero Trust Exchange プラットフォームを活用して、ミッションクリティカルなワークロードやサーバーが存在するパブリック クラウドとオンプレミスのデータセンター全体にわたって、ワークロードとインターネット間およびワークロード間の送信トラフィックを保護します。

Zero Trust Cloud では、一貫した脅威対策とデータ保護の確保、攻撃対象領域の排除、ラテラル ムーブメントの阻止、複雑さや運用コストの削減を実現できます。

「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 ポリシーを簡単に標準化できます」

Siemens、グローバル アウトバウンド接続責任者、Rui Cabeço 氏

ワークロードとサーバーに対する従来のセキュリティ対策が抱える課題

現在も多くの企業が旧式のアーキテクチャーでクラウド ワークロードを保護しており、通常、以下を組み合わせて対処しています。

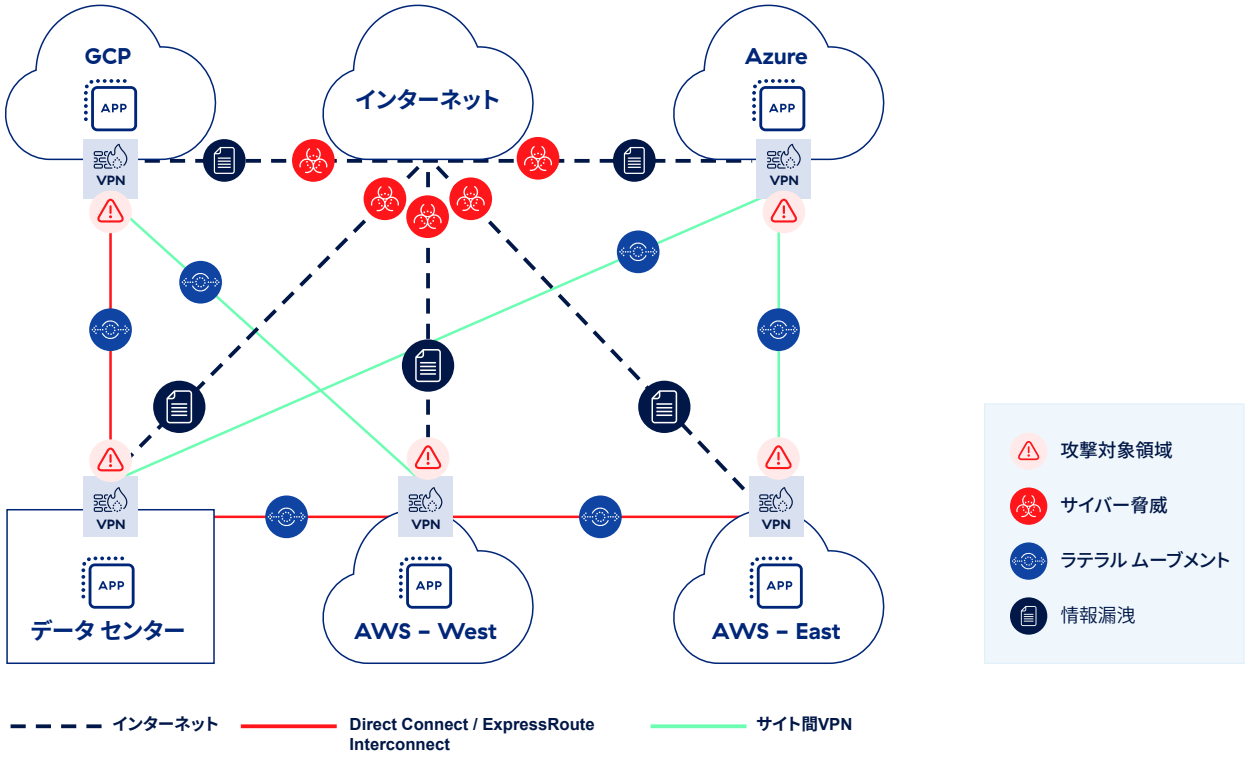
パブリック クラウド サービス プロバイダーが提供するネイティブ セキュリティ ソリューションを構成する

サードパーティー製のツール（ファイアウォール、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を展開する

検査と保護を行うために、オンプレミスのネットワーク セキュリティ インフラにトラフィックをバックホールする

これらの方法を使用すると、次のような課題が生じます。

- **攻撃対象領域とラテラル ムーブメントのリスクの増加。** ファイアウォールなどのソリューションは、ネットワークをワークロードやサーバーにまで拡張するため、ラテラル ムーブメントのリスクが高まります。さらに、インターネットに接続された各ファイアウォールは攻撃対象領域を拡大させ、インターネットからさまざまなクラウドやオンプレミス環境にまで影響を与えます。また、複数の仮想アプライアンス、オペレーション ツール、標準化されていないポリシーを寄せ集めて使用することで、既知の脅威に対しても未知の脅威に対してもカバレッジに穴が生まれ、セキュリティ リスクが増大します。
- **TLS の可視性のギャップ。** TLS インスペクションは通常、大量のコンピューティング リソースを消費するため、有効にするとパフォーマンスが低下する恐れがあります。また、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。多くの場合、拡張性を強化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も増加させます。
- **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ません。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環境全体に適用すると、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、拡張性を強化する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。
- **共通ログの欠如。** 一部の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 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。



パブリック クラウドとオンプレミスのデータ センターにまでゼロトラスト アーキテクチャーを拡張

Zero Trust Cloud 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やサーバー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させるため、ネットワークの攻撃対象領域が排除されます。同時に、ファイアウォールなどの従来のソリューション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 Zscaler Internet Access™ (ZIA) および Zscaler Private Access™ (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のが Zero Trust Exchange プラットフォームです。Zero Trust Exchange はハイパースケールで動作し、増加するワークロードやサーバーのトラフィックに柔軟に対応します。Zero Trust Cloud はワークロードやサーバーの送信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、送信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別のワークロードやサーバーなどの本来の宛先に転送されます。

Zero Trust Cloud では、次のことが可能です。

一貫性のある包括的な脅威対策とデータ保護

すべての環境に共通のセキュリティ ポリシーを施行

- TLS インスペクションと脅威対策をクラウドならではの規模で行い、ゼロデイ攻撃を防止
- DNS インスペクションとインラインのデータ保護で情報漏洩を阻止
- 厳密な制御でワークロードやサーバーがアクセスする宛先の数を制限

攻撃対象領域とラテラル ムーブメントの排除

ネットワークではなくアプリに接続して不可視化

- IP、FQDN、VPC、VNet、タグでワークロードをセグメント化し、最小特権アクセスを適用
- Zero Trust Exchange 経由でワークロードに接続させ、ネットワーク攻撃対象領域を排除
- クラウド間、クラウドとデータ センター間、リージョン間をサポート

運用コストと複雑さの軽減

すべてのワークロードを保護する単一のクラウド型プラットフォームを使用

- 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
- Infrastructure as Code (IaC) テンプレートを使用し、プログラム可能なインターフェイスを通じてセキュリティの展開を自動化
- 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を利用

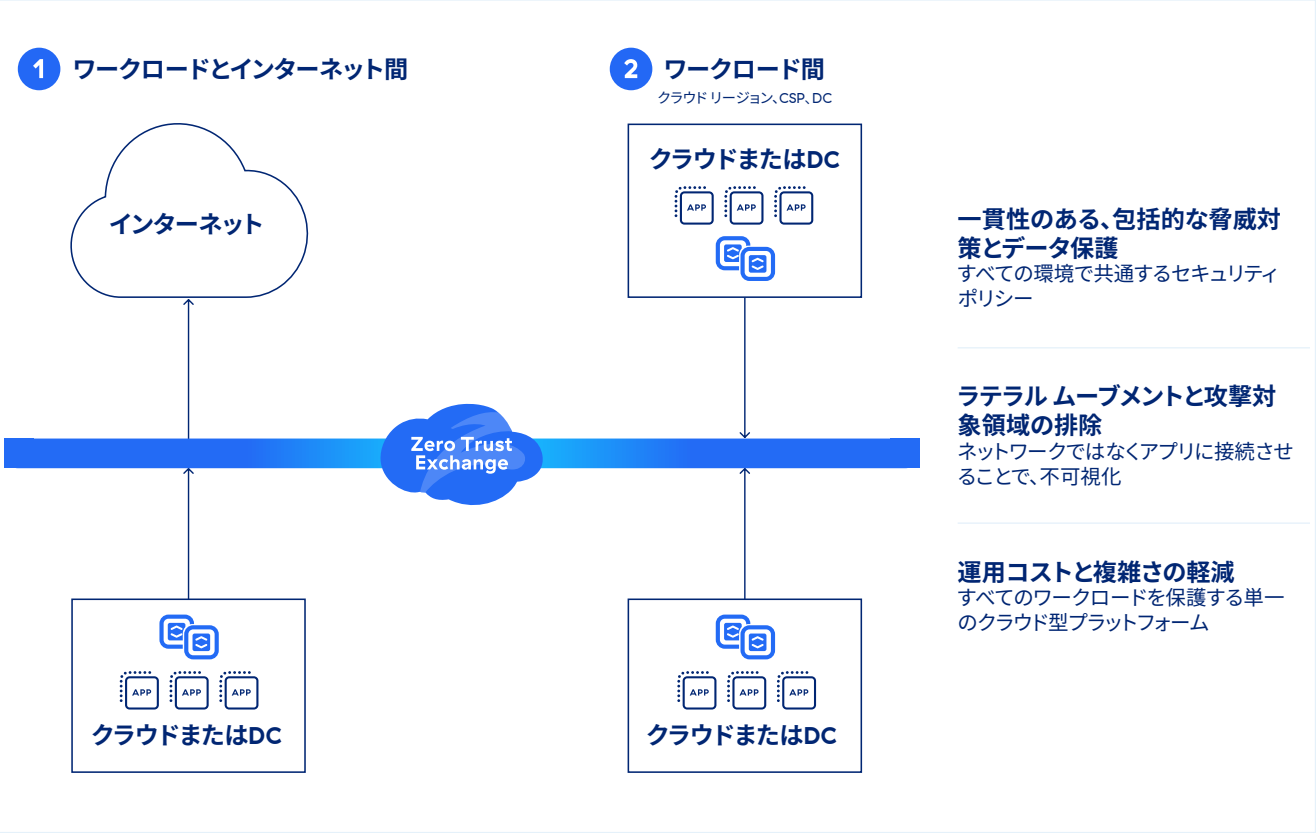


図 Zscaler Zero Trust for Workloads

Zero Trust Cloud の機能

Zero Trust Cloud 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安全に接続させます。

ゼロトラスト プロキシ アーキテクチャー：インラインに配置された専用のマルチテナント プロキシ アーキテクチャーが送信元と宛先の間に安全な接続を確立し、送信トラフィックを完全に可視化します。

クラウドならではの規模で実施される TLS 復号：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 アーキテクチャーが、高性能な検査を実行します。

アプリ間のきめ細かなセグメンテーション：すべてのワークロードとサーバーに対するゼロトラストの最小特権アクセスにより、ビジネス ポリシーの施行と管理が簡素化されます。

双方向の脅威検査：AI 活用型の脅威対策は、1 日あたり 500 兆のシグナルと 3,200 億のトランザクションを利用して、常時稼働の堅牢なランサムウェア対策、ゼロデイ脅威対策、未知のマルウェアからの保護を実現します。

インラインのデータ保護：すべてのチャネルと場所で高性能かつ大規模な DLP インスペクションを行います。

マルチクラウド対応の統合プラットフォーム：ポリシー管理、トラフィック監視、ログ追跡を提供する統合プラットフォームが標準化されたポリシーを AWS、Azure、GCP、オンプレミスのデータ センターに適用します。

Zero Trust Cloud の機能

ZSCALER ZERO TRUST CLOUD プラットフォーム	
特性	**詳細**
パブリック クラウドとオンプレミスへの対応	AWS、Microsoft Azure、Google Cloud Platform、Microsoft Azure 中国リージョン、AWS GovCloud でホストされるワークロードの保護に加えて、オンプレミスのデータ センター サーバーに対するサポートも提供します。AWS GovCloud は FedRamp 認定を取得しています。
TLS/SSL インスペクション	無制限の TLS/SSL トラフィック検査を行い、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 カテゴリーやアプリを指定することもできます。
ログ ストリーミング	Zscaler Nanolog Streaming Service は、世界中のワークロードやサーバー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。
接続のサポート	IPsec、GRE、Cloud Connector を利用して、ワークロードの送信トラフィックを Zero Trust Exchange に転送します。IPsec と GRE はワークロードとインターネット間のトラフィックを、Cloud Connector はインターネットとワークロード両方のトラフィックをそれぞれ保護します。

ワークロードとインターネット間のトラフィックを保護する ZSCALER INTERNET ACCESS	
特性	**詳細**
ワークロードとインターネット間の通信保護	ワークロードからインターネットに向かう通信をサイバー脅威や情報漏洩から保護します。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巧妙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/ML を使用して、悪意のあるペイロードに潜む未知の脅威をインラインで検出、防止、隔離することで、ペイシェント ゼロの発生を阻止します。
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。
帯域幅コントロール	帯域幅のポリシーを施行することで、業務に無関係なトラフィックよりもビジネスクリティカルなアプリケーションのトラフィックが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、サーバー、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。
コンテンツ フィルタリングとステートフル ルール	6 つのクラス、101 のカテゴリー、29 のスーパーカテゴリーにわたってポリシーでフィルタリングします。未知の URL やセーフ サーチに対しては動的コンテンツ分類を行い、IP アドレス、グループ、ホストされたアイデンティティーごとにきめ細かなポリシーを施行します。

ワークロード間のトラフィックを保護する ZSCALER PRIVATE ACCESS	
特長	**詳細**
ワークロード間のセグメンテーション	ハイブリッド環境とマルチクラウド環境全体にわたって、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、合理的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、百万単位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る ML モデルを使用して、内部の攻撃対象領域の最小化を支援します。
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**
インライン データ保護 (移動中データ)	フォワード プロキシと SSL インスペクション機能を使用して、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、データを狙う内部や外部の脅威を阻止することでワークロードとインターネット間およびワークロード間のトラフィックを保護します。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情報漏洩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。)

Zscaler Zero Trust Cloud のエディション	
エディション名	**機能**
Zero Trust for Workloads Standard	• Zero Trust for Workloads Standard の月間トラフィック 1 GB の年間サブスクリプション： • ステートフル フィルタリングと Cloud Connector を含む
Zero Trust for Workloads Advanced	• Workloads Standard エディションで利用可能なすべての機能 • ワークロード向けのインターネット アクセス：SSL/TLS インスペクション、高度な脅威対策、クラウド NSS、ソース IP アンカリング • ワークロード向けプライベート アクセス：App Segment、サブロケーション、LSS Standard、ロギングおよびレポート • ワークロード向けデータ保護：インライン Web (モニター モードのみ) • ワークロード向けサイバー脅威対策：標準ファイアウォール、DNS 制御
Zero Trust for Workloads Advanced Plus	• Workloads Advanced エディションで利用可能なすべての機能 • ワークロード向けデータ保護：インラインでのデータ保護、高度な分類 • ワークロード向けサイバー脅威対策：Firewall Advanced for Workloads、Sandbox Advanced for Workloads

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.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