データシート

Zscaler Zero Trust SD-WAN

拠点、工場、データ センターを安全に接続し、あらゆる場所のサーバーや IoT/OT デバイスにまでゼロトラスト セキュリティを拡張

ハイブリッド ワークやクラウド トランスフォーメーションが推進されたことで、プライベート アプリはクラウドに移行し、ユーザーはパブリックインターネット経由であらゆるデバイスや場所からアプリケーションにアクセスしています。こうした大きな変化によって、境界型のネットワークとセキュリティ モデルが根底から覆されつつあります。

多くの企業が拠点や工場、データセンターなどのさまざまな場所で IoT/OT デバイスを利用して業務を合理化していますが、そのほとんどがサーバーとクライアント間のワークロード通信に依存しています。クラウドとモバイルのテクノロジーが優先される現代において、アプリケーションアクセスの管理にレガシー WAN やメッシュ VPN、ファイアウォールを使用する従来のアプローチはもはや効果的とは言えません。

組織の要件が急速に変化する中で、レガシー WAN ソリューションを使い続けることは大きなリスクとなります。ネットワークベースのアクセスによる限定的なセキュリティ、攻撃対象領域の拡大、広範にわたるラテラル ムーブメントのリスク、ルーティングの複雑さなど、SD-WAN にはさまざまな課題が存在します。このネットワークにゼロトラストの原則を適用しようとすると、追加のファイアウォール アプライアンスが必要になり、コストと複雑さが増大します。

Zscaler Zero Trust SD-WAN の特長：

- **あらゆる場所でゼロトラストを実現：**場所を問わず、すべてのユーザー、デバイス、サーバー、IoT/OT を保護します。
- **アプリケーションのパフォーマンスを向上：**拠点のトラフィックは Zero Trust Exchange に直接送信されます。また、信頼されたアプリケーションのトラフィックは、直接インターネット ブレイクアウトでインターネットを介して送信されます。
- **脅威のラテラル ムーブメントを阻止：**ゼロトラストで安全な接続の基盤を構築して、東西方向のセグメンテーションを可能にします。
- **攻撃対象領域を排除：**基盤となるトランスポートから拠点とデータ センターを独立させ、Zero Trust Exchange を介して接続させます。
- **シャドー IoT デバイスを検出して分類:**トラフィックプロファイルに基づいて、デバイスを自動で分類します。
- **OT リソースへの安全なアクセスを簡素化:**ブラウザーベースのクライアントレス アクセスで、OT 資産の SSH/RDP/VNC ポートへのアクセスを保護します。
- **きめ細かな転送ポリシーを施行：**ZIA や ZPA を使用して、インターネットおよび非インターネットのトラフィックに対してポリシーを施行します。
- **プラグ&プレイ アプライアンスを展開：**ゼロタッチ プロビジョニング (ZTP) で導入が簡素化されるため、統合までの時間を短縮できます。

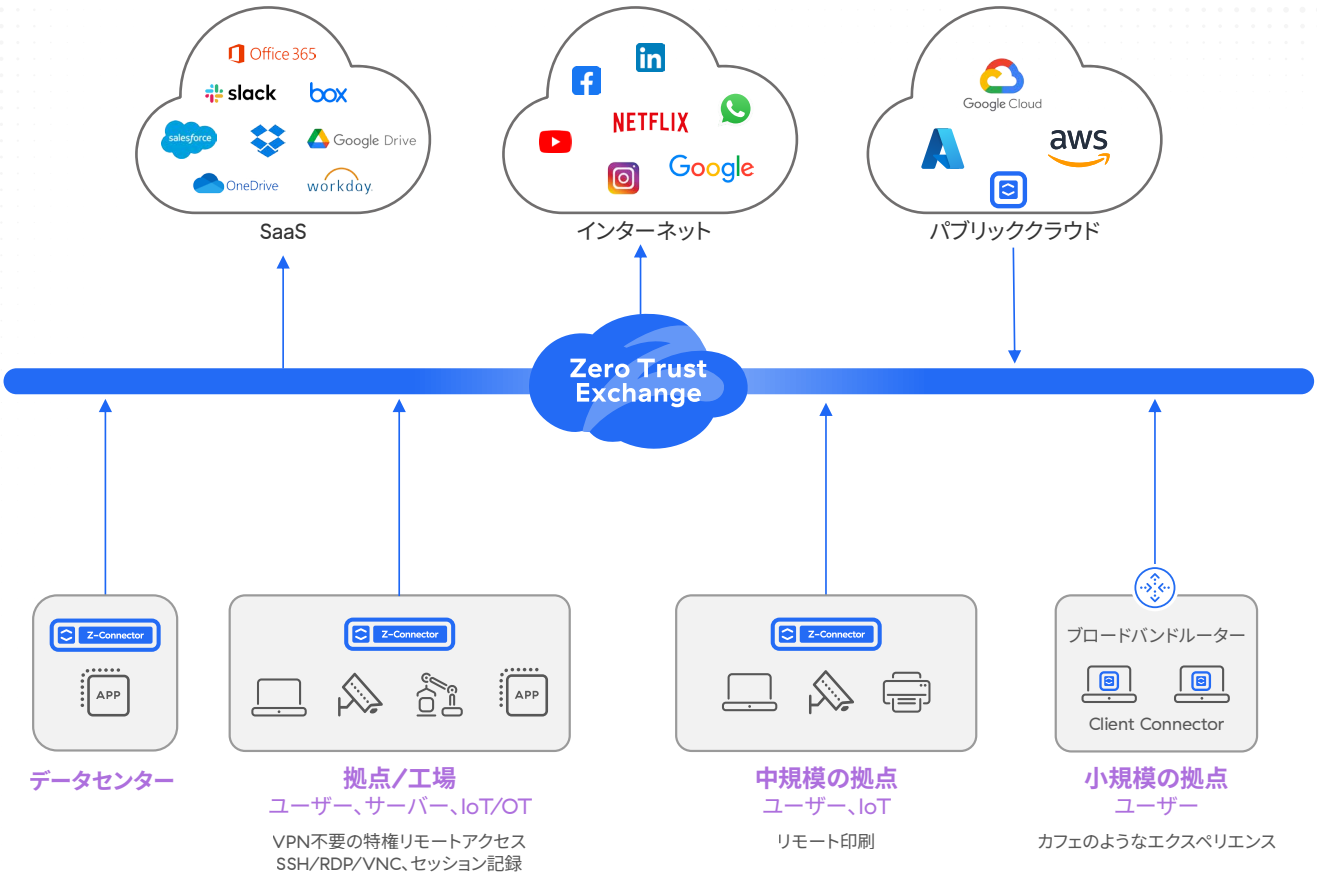

図 1: ゼロトラスト SD-WAN

ゼロトラスト SD-WAN は複雑な VPN を使用することなく、拠点、工場、データ センターを安全に接続し、組織のポリシーに基づいてユーザー、IoT/OT デバイス、アプリケーション間のゼロトラスト アクセスを確保します。

「ゼロトラスト」ではない従来の SD-WAN

従来のネットワークとセキュリティ アーキテクチャーを使用して、拠点をインターネットやパブリック クラウドまたはデータ センター環境の他のアプリケーションに接続する場合、次のような課題が生じます。

- **脅威のラテラル ムーブメントやインターネットベース攻撃のリスクの増加：**サイト間 VPN、ファイアウォール、従来型の SD-WAN などのネットワークを中心とした旧式の接続ソリューションは、信頼された組織のネットワークをインターネット経由で他のクラウドやオンプレミス環境にまで拡張するため、攻撃対象領域が拡大します。セキュリティ アプライアンスやツール、非標準ポリシーの寄せ集めは、セキュリティ範囲の既知や未知のギャップによってセキュリティ リスクが増大します。

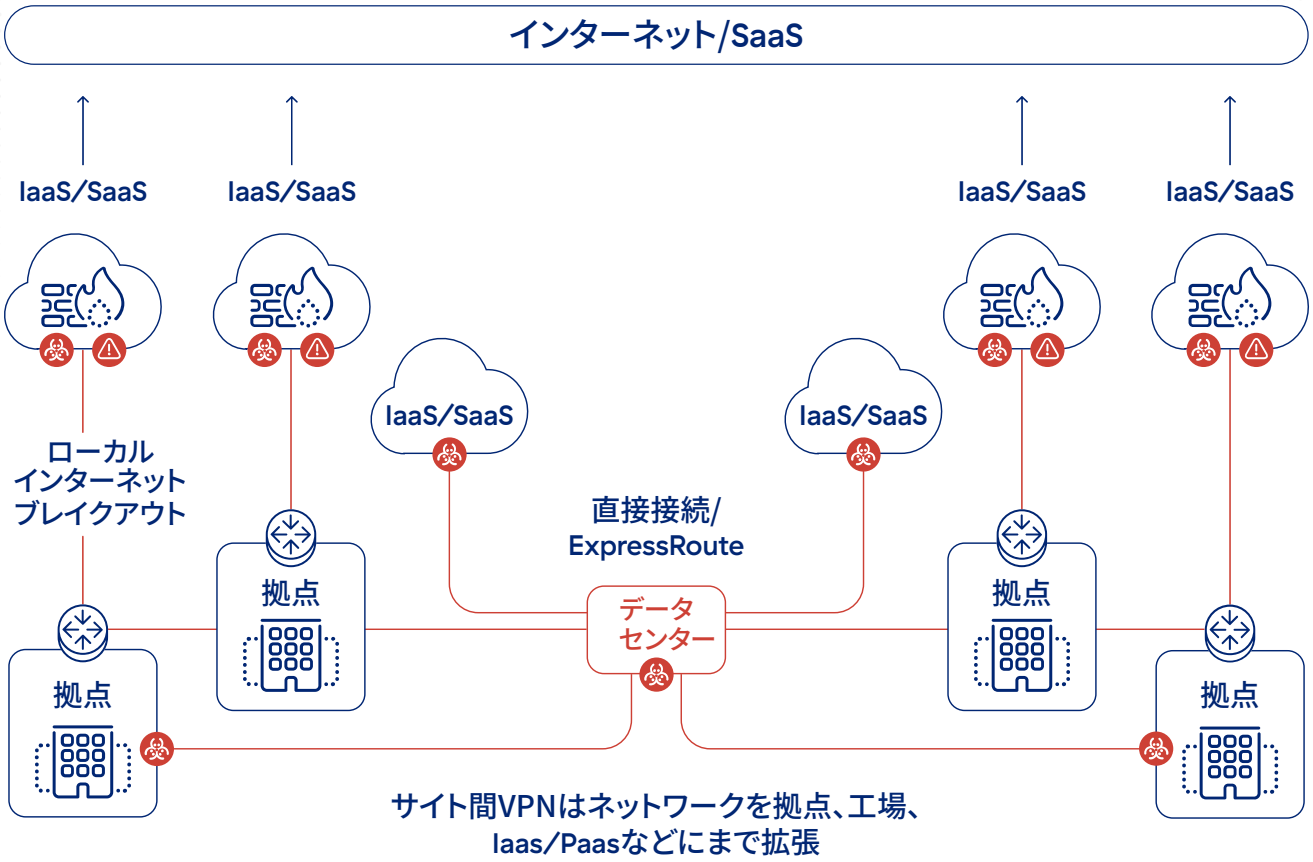

図 2: 脅威のラテラル ムーブメントとインターネットベース攻撃のリスクをもたらす従来型の SD-WAN

- **複雑さの増大：**環境の複雑化を招く要素となるのが、複雑なルーティングや複数のネットワークホップとアプライアンス、そしてレガシー モデルをクラウドに導入することで断片化したポリシーの管理などです。拠点、クラウド、データ センター全体で接続を標準化したり、セキュリティ ポリシーを施行したりすることは難しく、ネットワーク部門やセキュリティ部門にとって、こうした複雑さの管理は大きな課題となっています。
- **可視性の欠如：**拠点、データ センター、クラウドの接続パス全体を十分に可視化できないため、ネットワークとセキュリティの死角が発生します。
- **パフォーマンスとスケーラビリティーの低下：**拠点やデータセンター環境内のネットワークとセキュリティサービスの増加、トラフィックのヘアピン、一元的なセキュリティの検査や制御を目的としたチョークポイントなどがパフォーマンスとスケーラビリティーを低下させます。
- **コストの上昇：**従来のネットワークやセキュリティ アプライアンス (ファイアウォール、IPS、ルーター、その他のポイント製品など)、スケーラビリティーの欠如を補うためのネットワーク サービスのオーバープロビジョニング、クラウド ネイティブ サービスの利用の増加などにより、コストが増大します。

ゼロトラスト SD-WAN の仕組み

ゼロトラスト SD-WAN はルーターやファイアウォール、VPN などの複数の製品を排除し、インターネット接続のみで迅速に展開できるシンプルなプラグ&プレイ デバイスで軽量の拠点を構築することで、デバイス管理に伴う複雑さを解消すると同時に、拠点の全体的な機能を最適化します。ゼロトラスト SD-WAN は、ゼロトラストのネットワークオーバーレイで拠点の通信を大幅に簡素化し、実績ある ZIA と ZPA のポリシー フレームワークを使用して柔軟な転送とシンプルなポリシー管理を可能にします。

拠点からのトラフィックはすべて Zero Trust Exchange に安全に直接転送されます。ここで ZIA または ZPA のポリシーを適用し、拠点やデータ センターからの通信に対して、完全なセキュリティ検査とアイデンティティーベースのアクセス制御を行います。信頼されたアプリケーションのトラフィックは、インターネット ブレイクアウトを使用してインターネット経由で直接送信されます。この独自のアプローチは、次の 3 つの重要なメリットを提供します。

- ネットワークベースのサイト間 VPN 接続から、アイデンティティーとアプリケーションに基づいた通信に移行することで、真のゼロトラスト セキュリティを実現する。
- セキュリティを損なうことなく、従来の「城と堀」のアーキテクチャーを廃止する (Squid プロキシ、NAT ゲートウェイ、IPS などのレガシー製品は不要)。
- 一元化された自動ポリシー管理で分散型のスケーラブルな接続を必要な場所に提供し、拠点とデータ センターの通信を簡素化する。

ゼロトラスト SD-WAN のユース ケース

サイト間 VPN のリプレース

ネットワークの攻撃対象領域を増大させる要因となっているのが WAN や VPN ですが、ゼロトラスト SD-WAN は WAN を拡張したり、VPN を使用したりすることなく、拠点をプライベート アプリに直接接続させます。アプリケーションは拠点の背後に隠れて検出されず、Zero Trust Exchange 経由で指定されたエンティティーにのみアクセスできるよう制限されます。また、指定された参加者のアイデンティティー、コンテキスト、ポリシー遵守はすべてアクセスが許可される前に検証され、ネットワーク内の他の場所水平移動できないようにします。

吸収と合併

ネットワークの統合は簡単ではありません。時間がかかるばかりか、IP の重複からルーティングの問題、ネットワーク攻撃対象領域の拡大によるセキュリティリスクの増大まで、さまざまな課題が発生します。ゼロトラスト SD-WAN では、ネットワークを統合することなく、ある環境の拠点から別の環境のプライベート アプリに素早くスムーズに接続できるようになります。

インターネットへの直接アクセスを拠点に提供

多くの組織がアプリをクラウドに移行し、クラウドネイティブアプリを構築するにつれ、オンプレミスのネットワークとセキュリティ モデルは十分な効果を発揮できなくなりつつあります。Zscaler Zero Trust SD-WAN は拠点を変革するために構築されたソリューションであり、基盤となるネットワークから拠点が独立し、あらゆる宛先と安全に通信できるようにする新しいモデルを提供します。

サーバー、IoT/OT 接続のためのゼロトラスト

従業員やサードパーティー ベンダーは、生産稼働時間を最大化し、機器やプロセスの障害による中断を回避するために、定期的に IoT/OT アセットにアクセスする必要があります。IoT/OT のためのゼロトラスト SD-WAN は、RDP と SSH 対象システムへの完全に分離されたクライアントレスのリモート デスクトップアクセスを提供します。ジャンプ ホストや従来型の VPN を使用して、デバイスにクライアントをインストールする必要はありません。

シャドー IoT/OT の検出と可視化

認可されていない検出不可能なデバイスが支店のネットワークに接続すると、デバイスの脆弱性が高まるだけでなく、攻撃対象領域も拡大します。これは、IT 部門が直面している課題の 1 つです。Zscaler は、デバイスを識別、分類することで、IT 部門がデバイスの動作状況をより明確に可視化して、アクセス制御ポリシーを改善できるようにします。

Z-Connector のプラグ&プレイ アプライアンス

特長	ZT 400	ZT 600	ZT 800	ZT VM
				Z-Connector
種別	小規模から中規模の拠点	小規模から中規模の拠点	中規模から大規模の拠点	拠点やデータ センター
スループット / ハイパーバイザー	200 Mbps	500 Mbps	1 Gbps	KVM、ESXi
物理ポート	4 x GbE	6 x GbE	8 x GbE	N/A
ゼロタッチプロビジョニング	✓	✓	✓	✓
インターネットやプライベート アプリケーションのトラフィック、直接送信される WAN のトラフィックに対するきめ細かな転送ポリシー	✓	✓	✓	✓
インターネットへのトラフィックに対する URL フィルタリング、ファイル タイプ制御、クラウド ファイアウォール ポリシーの活用	✓	✓	✓	✓
IoT デバイスやサーバーに対するゼロトラストの ZPA ポリシー	✓	✓	✓	✓
一元化された可視性とログ	✓	✓	✓	✓

ZSCALER ZERO TRUST SD-WAN の機能	
特長	**詳細**
機能	
ゼロタッチ プロビジョニングと展開の自動化	• 事前定義されたテンプレートによるゼロタッチ プロビジョニング • 展開の完全自動化 • 支店の地理的情報の動的検出
インターネットとプライベートアプリのトラフィックに対するきめ細かな転送ポリシー	• インターネット経由で ZIA、ZPA、またはダイレクトにトラフィックを送信するオプション • ロケーション、サブロケーション、ロケーション グループ、5 タプル、または FQDN のトラフィックの柔軟な選択基準
統合されたゼロトラスト ポリシー	• 新しいクライアント タイプが含まれた ZPA の拡張ポリシーによるユーザーとアプリ間、IoT デバイスとアプリ間、サーバー間の統合ポリシー • ロケーションと位置ベースのポリシー • IPS、SSL プロキシ、URL フィルタリング、データ保護を含むセキュリティー ポリシーを有効化 • IoT/OT とサーバー用に構成されたポスチャーを備えた完全なセキュリティ スタック
高可用性	• HA モードで動作するゼロトラスト SD-WAN の 2 つのインスタンスが、ハードウェア障害時のバースト トラフィックと冗長性に対する追加サポートを提供 • 共通アドレス冗長プロトコル (CARP) に基づく仮想 IP アドレス (VIP) を使用したアクティブ / パッシブのフォールト トレランス • アクティブ / アクティブ回線 (シングル アプライアンス) • アクティブ / アクティブ回線 (FHRP バランシング時のデュアル アプライアンス)
一元化された可視性ときめ細かなログ	• デバイスの正常性とトラフィック モニタリングのための一元化されたダッシュボード • クラウド、データ センター、拠点の展開で利用可能なフィルタリング • すべてのポートおよびプロトコルのセッションとトランザクションの詳細なログ (すべてのパブリックおよびプライベート DNS トランザクションを含む) • 顧客の SIEM にログをストリーミングするオプションを含む、Nanolog ストリーミング サービス インフラとの完全な統合
WAN インターフェイスの終端	• デュアル ISP 接続 (イーサネット) • シングル アプライアンスでのマルチホーミング
LAN インターフェイスの管理	• 複数の L3 LAN ネットワーク • 802.1q/VLAN タギングのサポート • DHCP サーバー • DNS ゲートウェイ
デバイス上のファイアウォール ポリシー	• ローカル LAN 間 (東西) トラフィックのきめ細かなアクセス制御 • L3 アクセス制御リスト (ACL)
アプリケーションアウェアなパスの選択	• ミッションクリティカルな SaaS またはプライベート アプリケーションのための動的パスの選択 • インテリジェントな Zscaler POP 接続 • 組み込みの SLA モニタリングとフェイルオーバー
ルーティング	• 静的ルーティング
Zscaler のデータ センター / POP	• 世界中に 150 以上存在する Zscaler のデータ センターにクラウド セキュリティ プラットフォームを構築し、顧客がいる場所に戦略的に配置 • 次に利用可能なサービスの PoP へのシームレスなフェイルオーバーを備えた組み込みの可用性

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