eBook

ZTNA で ハイブリッド ワークを保護

効果的な ZTNA ソリューションに求められる 10 の機能

eBook

目次

はじめに 3

ゼロトラスト ネットワーク アクセス (ZTNA) とは 4

#1: インターネット上でアプリを見えなくすることで、攻撃対象領域を排除する 5

#2: どこからでもシームレスに接続できる 6

#3: 最小特権アクセスを施行する 7

#4: アプリ、ネットワーク、デバイスの問題を迅速に検出、修正して、ユーザーの生産性を維持する 8

#5: アプリのマイクロセグメンテーションを通じて水平移動を防止する 9

#6: 企業所有のデバイスだけでなく、BYOD のセキュアなアクセスもサポートする 10

#7: インラインのコンテンツ検査で攻撃を阻止し、脅威をブロックする 11

#8: さまざまな ID プロバイダーやソリューションとシームレスに統合する 12

#9: 統合されたデセプション テクノロジーで攻撃を阻止する 13

#10: 迅速かつ容易に展開できる 14

Zscaler Private Access が世界で最も導入されている ZTNA プラットフォームである理由 15

はじめに

私たちの働き方は大きく変わりつつあり、従業員の生産性を高める方法や場所も、わずか数年前とは違った様相をみせています。ますます多くの組織がハイブリッド ワークやリモート ワークの採用を進める中、クラウドが持つ柔軟性、スケーラビリティー、効率性を最大限に活用するために、ミッションクリティカルなアプリケーションをクラウドに移行する動きが増えています。

しかし、IT エコシステムが変容するにつれて、新たなセキュリティ上の懸念も生まれています。ハイブリッド ワークやリモート ワークの大規模な導入は、クラウドの利用拡大やモバイル アクセスの増加という側面を伴い、導入を従来型のセキュリティ ソリューション (VPN やファイアウォールなど) や旧式のアプローチで進める場合、攻撃対象領域を拡大させる可能性があります。このような状況では、攻撃対象領域が無秩序に広がるだけでなく、セキュリティ部門の可視性が制限され、インシデントの調査や問題のトラブルシューティングがより困難になります。

そこで必要となるのが、技術環境を保護するための新しいモデル、つまり現代のセキュリティと接続のニーズにより適したソリューションです。ゼロトラストはまさにこれを実現し、あらゆる業界や地域で急速に採用され始めています。

多くの組織がゼロトラスト ネットワーク アクセス (ZTNA) を選択して、ハイブリッド ワークのセキュリティ態勢を強化しています。ZTNA は、ゼロトラストを実現するための明確に定義されたフレームワークを提供します。アナリスト企業である Gartner は、現在、ZTNA の市場は猛烈な勢いで拡大しており、前年比で 60% 以上の成長を遂げていると報告しています。

「VPN の廃止」が
ZTNA を実装する
主な動機
となっています。

ゼロトラスト ネットワーク アクセス (ZTNA) とは

ZTNA は、リモート ユーザーに社内アプリやプライベート アプリへのセキュアなアクセスを提供する一連の技術や機能です。

ZTNA は、信頼付与の適応型モデルに従って動作します。このモデルでは、信頼は暗黙のうちに付与されるのではなく、詳細なポリシーで定義された、知る必要がある最小限の範囲内でアクセスが許可されます。

クラウド型のアプリやインフラの採用が増える中、多くの組織が自社のセキュリティ サービスを単一のクラウド配信型プラットフォームに統合しようとしています。これは、セキュリティ サービス エッジ (SSE) として知られており、セキュア Web ゲートウェイ (SWG)、クラウド アクセス セキュリティ ブローカー (CASB)、および ZTNA 機能で構成されます。Gartner は、セキュリティとリスク管理のリーダーに対して、ZTNA の採用から SSE 導入戦略を始めることを推奨しています。このように、ZTNA はクラウド配信型セキュリティへの取り組みの重要な第一歩となっています。

VPN インフラは、規模が大きくなるにつれてパフォーマンスが低下するほか、攻撃対象が拡大することでセキュリティ リスクが高まります。その代替として注目されているのが ZTNA です。しかし、ZTNA は VPN 以上の効果を発揮します。これを採用することで、組織は従来型のアプライアンスやそれに伴う管理費用を排除できると同時に、ユーザーにアプリへの高速の直接アクセスを提供できます。また、容易に拡張でき、管理制御と可視性も強化されます。

市場に出回る ZTNA の製品やソリューションは、必ずしもすべて同じというわけではありません。ZTNA のメリットをすべて実現するには、以降で挙げる 10 の機能を備えたソリューションを選択する必要があります。

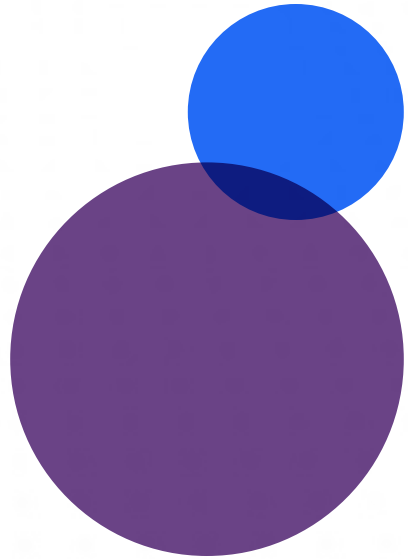
#1: インターネット上でアプリを見えなくすることで、攻撃対象領域を排除する

これまでのハブ&スポーク スタイルのネットワーク アーキテクチャーでは、アプリケーションはセキュリティ境界を侵害できる攻撃者に簡単に発見されてしまいます。

悪意のあるアクターはネットワーク内に一度侵入すると、アプリケーションなどのリソースを簡単な検索で検出できます。

真の ZTNA ソリューションでは、アプリケーションへのアクセスはセグメンテーションによって 1 対 1 で許可されるため、攻撃者が 1 つのアプリケーションにアクセスできたとしても、環境内の他のアプリケーションを発見することはできません。

すべてのアプリケーションは、直接接続を仲介する ZTNA プラットフォームの背後に隠されます。攻撃者は見えないものを標的にはできないため、ZTNA ソリューションは IP アドレスを難読化することで、送信元のアイデンティティーを隠します。つまり、このようなインサイドアウトの接続は、アプリケーションのエコシステム全体を見えなくするため、攻撃者は個々のアプリに対して標的型攻撃を仕掛けることができなくなります。



#2: どこからでもシームレスに接続できる

現在、組織の 77% はすでにハイブリッド ワークを採用しているか、採用を検討しています。

従来のネットワーク アーキテクチャーは、拠点と中央データ センター間の高価な MPLS リンクに依存しており、VPN を介してリモート ユーザーを接続します。ハイブリッド ワークやリモート ワークが主流になるにつれて、拡張できない VPN はパフォーマンスの問題を引き起こします。

それに対して、ZTNA はアプリケーションへのアクセスをネットワークへのアクセスから完全に分離するため、MPLS リンクや VPN を必要としません。クラウド型サービスとして提供される ZTNA では、企業のデータ センターにトラフィックをバックホールする必要がなくなり、代わりに、ユーザーは生産性の維持に必要なアプリケーションに素早く直接アクセスできます。

データ センターに関して言えば、世界的に展開する ZTNA プロバイダーは、ユーザーとアプリケーション間の最短の接続パスを見つけることができるという点に留意してください。可能な限りエッジに近い接続を仲介することで、従業員に快適なユーザー エクスペリエンスを提供できるようになります。

#3: 最小特権アクセスを施行する

ゼロトラストの重要な原則となっているのが、最小特権アクセスです。その定義は非常にシンプルで、ユーザーは自分の職務を遂行するために必要な最小限のレベルのアクセス権を付与されるだけで、それ以上のものは与えられないというものです。

このようなアプローチをサポートできるセキュリティ アーキテクチャーを構築するには、適切な ZTNA ソリューションが不可欠です。ソリューションは、堅牢なユーザー ID 認証メカニズムを組み込み、デバイスのコンテキストを理解し、その制御において非常にきめ細かなユーザーとアプリ間のセグメンテーションを施行する機能を備えている必要があります。これを実現するには、ZTNA はすべての主要な ID プロバイダー (IdP) プラットフォームと緊密に統合できる必要があります。

認証されたユーザーをネットワークではなく、使用が許可されたアプリケーションにのみ接続することで、IT ポリシーとビジネス ポリシーを施行できる ZTNA ソリューションが必要です。このアクセスは場所に関係なく、リモートユーザーとオンプレミスのユーザー両方に拡張される必要があり、セキュリティ制御は、場所を問わずすべてのユーザーに対して同一である必要があります。

Zscaler は、ロサンゼルス市の 18,000 人の職員にセキュアなリモート ワークを提供しています。

#4: アプリ、ネットワーク、デバイスの問題を迅速に検出、修正して、ユーザーの生産性を維持する

ゼロトラストの採用には、特に担当部門が従来の VPN で実装しようとする場合、詳細なネットワーク セグメンテーションが必要になります。

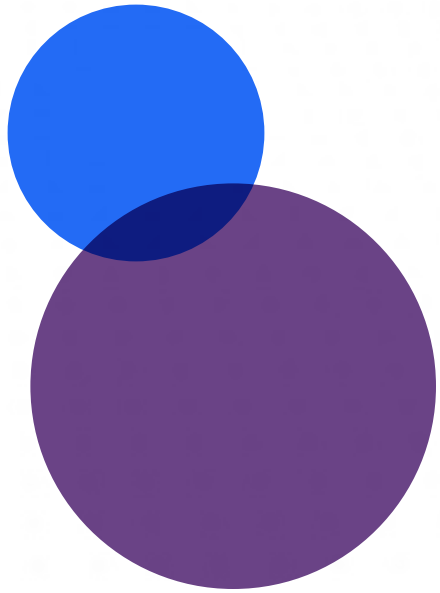
技術的な観点からも、これは簡単なことではありません。ユーザー エクスペリエンスに関しては、さらに障害が発生します。ネットワークがこのようにセグメント化されると、優れたエンド ユーザー エクスペリエンスを確保するうえで必要なエンド ユーザーのデバイスやアプリケーションのパフォーマンスに関するインサイトを得ることが非常に難しくなり、ネットワークやサービス デスクの部門にとって大きな課題となりかねません。

ZTNA ソリューションは、担当部門がこの課題を克服するうえで有効な機能を提供する必要があります。エンド ユーザーのデバイスの正常性、ネットワークのパフォーマンス、アプリケーションの可用性などに関するメトリクスを収集し、それらを簡単に確認できる単一のダッシュボードに表示することで、エンド ユーザーが問題に気づく前にサポート部門が問題を特定して修正できるようにする必要があります。

Careem は、Zscaler Digital Experience で平均復旧時間 (MTTR) を 62% 短縮しました。

#5: アプリのマイクロセグメンテーションを通じて水平移動を防止する

ZTNA ソリューションは、ソフトウェア定義のマイクロセグメンテーションを通じて、データ、ワークフロー、サービス、リソースを保護する必要があります。これは、ユーザーをネットワークではなくアプリに直接接続する必要があることを意味します。



このアプローチに従えば、セキュリティ部門はネットワーク全体の水平移動を懸念する必要がなくなります。攻撃者が 1 つのユーザー アカウントやアプリケーションを侵害できたとしても、これを超えて他の企業リソースを侵害することはできません。

ZTNA では、1 つのアプリケーションまたはリソースへの接続のみが確立され、他へのアクセスが自動的に許可されることはありません。

#6: 企業所有のデバイスだけでなく、BYOD のセキュアなアクセスもサポートする

従業員やサード パーティーに対して、エージェント アクセスとエージェントレス アクセスの両方をサポートできる ZTNA ソリューションが求められます。

従業員やサード パーティーに対して、エージェント アクセスとエージェントレス アクセスの両方をサポートできる ZTNA ソリューションが求められます。このように、ZTNA はパートナーやベンダーにリソースへのシームレスなアクセスを提供すると同時に、従業員が自分のデバイス (モバイル デバイスを含む) を業務目的で安全に使用できるようにします。

また、管理対象外デバイスの普及が進んでいるため、ZTNA ソリューションがクライアントレス アクセスをサポートできることも重要です。サポートできない場合、会社支給のデバイス上でしか従業員を保護できないことになり、現代のモバイル中心の作業環境では、大きなマイナス要素となります。

#7: インラインのコンテンツ検査で攻撃を阻止し、脅威をブロックする

すべての脅威をブロックするうえで必要な完全な可視性のために、ZTNA ソリューションはすべてのコンテンツに対してインライン検査を実行できる必要があります。

サービスに求められるのは、すべてのトラフィック (ランサムウェア、スパイウェア、ウイルスなどの危険なコンテンツの送信を隠すために使用される SSL 暗号化トラフィックを含む) を検査して、既知の正当な通信に対してのみ通過を許可することです。このインライン検査は、現在蔓延しているランサムウェア、フィッシング、ゼロデイ脅威、高度な攻撃などを確実に阻止できるように、世界中のさまざまなシグナルから培われた脅威インテリジェンスに基づく必要があります。

OWASP Top 10 は、Web アプリケーションの最も重要なセキュリティ上のリスクに関する幅広い専門家のコンセンサスを表しています。ZTNA ソリューションは、SQL インジェクション、クロスサイト スクリプティング、環境およびポート スキャナー、Cookie ポイズニングなど、最も一般的に使用されている攻撃手法を包括的にカバーしている必要があります。

Zscaler は、OWASP Top 10 をはじめ、SQL インジェクションやクロスサイト スクリプティングなどの Web アプリケーション セキュリティ上の既知のリスクをブロックします。

#8: さまざまな ID プロバイダーやソリューションとシームレスに統合する

Zscaler は、Microsoft や Okta などの ID プロバイダーや、CrowdStrike などのエンドポイントでの検知と対応 (EDR) プラットフォームと緊密に統合しています。

ゼロトラスト セキュリティは、アプリケーションやその他のリソースにアクセスしようとしているユーザーのアイデンティティーを検証することから始まります。

多くの組織が場所を問わない働き方をサポートするために、クラウドファースト戦略を採用する中、ライフサイクル全体にわたって認証とユーザー アイデンティティーを管理できるように、アイデンティティーとアクセス管理 (IAM)、アイデンティティー ガバナンスと管理 (IGA) のパートナーに注目が集まっています。

ZTNA ソリューションは、自社で採用している IAM および IGA パートナーと統合できる必要があるのはもちろんですが、時代の変化に対応できるアイデンティティーと認証戦略を考えるのであれば、業界トップクラスのテクノロジー ソリューション プロバイダーすべてと強力に連携しているプロバイダーが求められます。

#9: 統合されたデセプション テクノロジーで攻撃を阻止する

デセプション テクノロジーは、サイバーセキュリティ ソリューションの新しいカテゴリーです。

デセプション テクノロジーを用いることで、実際の環境内に存在する脅威を迅速に検知できるほか、誤検知率も非常に低くなります。このテクノロジーは、ネットワーク内に「本物らしい」デコイ (例えば、ドメイン、データベース、ディレクトリー、サーバー、アプリ、ファイル、資格情報、パンくずリスト) を実際のアセットと並べて配置して、攻撃者をおびき寄せるものです。攻撃者がデコイと接触した瞬間に情報収集を開始し、信頼性の高いアラートを生成します。

このテクノロジーを活用することで、セキュリティ部門の脅威検出能力が向上し、ビジネスが直面するリスクに関するより優れたインサイトをリアルタイムで生成できます。また、環境内の死角となる要素に適切に対処できるようになります。デセプションのデコイは、ゼロトラスト環境でトリップワイヤーの役割を果たし、侵害されたユーザー アカウントやネットワークを水平移動しようとする試みを検出します。

これは新興技術であるため、デセプション プラットフォームを備えた ZTNA ベンダーはまだ少ないものの、業界のリーダー企業はすでにこの技術を取り入れています。

KuppingerCole は、Zscaler を分散型デセプション プラットフォームのリーダーと評価しています。

#10: 迅速かつ容易に展開できる

展開に数週間から数か月かかる他のテクノロジー ソリューションとは異なり、業界をリードする ZTNA は場所に左右されることなく、わずか数日で展開できます。

Zscaler を導入したロサンゼルス市は、18,000 人の職員に対して作業場所に左右されないセキュアなアクセスをわずか 2 週間で提供しました。

Zscaler Private Access が世界で最も導入されている ZTNA プラットフォームである理由

Zscaler Private Access (ZPA) は、これらすべての機能を備えているだけでなく、それ以上の効果も発揮します。Zscaler 独自のゼロトラスト アーキテクチャー上に構築された ZPA は、最小特権の原則を適用してユーザーにプライベート アプリケーションへのセキュアな直接接続を提供する一方で、承認されていないアクセスや水平移動を排除します。クラウド型のサービスである ZPA は数時間で展開でき、従来型の VPN やリモート アクセス ツールを包括的な最新のゼロトラスト プラットフォームに置き換えます。

Zscaler Private Access には、次のような特徴があります。

- **従来型の VPN やファイアウォールを超えた優れたセキュリティ：**ユーザーはネットワークではなくアプリに直接接続されるため、攻撃対象領域を最小限に抑えて水平移動を排除します。
- **プライベート アプリへの侵害を防止：**インライン防御、デセプション、脅威の分離の機能を備えた優れたアプリ保護機能により、侵害されたユーザーによるリスクを最小限に抑えます。
- **現代のハイブリッド ワーカーに優れた生産性を提供：**リモート ユーザーをはじめ、本社や支店、サード パーティーのパートナーに対し、プライベート アプリへの超高速アクセスをシームレスに提供します。
- **ユーザー、ワークロード、デバイス向けの統合型 ZTNA：**業界で最も包括的な ZTNA プラットフォームが、従業員やパートナーをプライベート アプリ、サービス、OT/IoT デバイスに安全に接続します。

詳細をご希望の場合は、無料のデモをリクエストしてください。

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.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