データシート

Zscaler Private Access™

業界初で唯一の次世代 ZTNA が実現する プライベート アプリへの高速かつ安全で 信頼性の高いアクセスで従業員を強力にサポート

Zscaler は、高度な接続、セグメンテーション、セキュリティ機能でプライベート アプリ アクセスを再定義し、優れたユーザー エクスペリエンスを提供すると同時にビジネスを脅威から保護します。

従来のネットワークとセキュリティのアプローチでは満たせないハイブリッド ワークが求める要件

ユーザーをプライベート アプリに接続させる際の遅延や複雑さ、リスクは、最小限に抑える必要があります。ハイブリッドワークとクラウド トランスフォーメーションによって、境界ベースのネットワーク セキュリティ モデルが根底から覆り、プライベート アプリがクラウドに移行し、ユーザーが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するようになった今、アプリケーションへのアクセスの管理に VPN やファイアウォールを使用する従来のアプローチでは、現代のクラウドファースト、モバイルファーストの環境に対応できなくなっています。

Gartner は 2025 年までに、新たに導入されるリモート アクセスの少なくとも 70% が、VPN サービスではなく主にゼロトラスト ネットワーク アクセス (ZTNA) で提供されるようになると予測しており、2021 年末の 10% 未満から大幅な増加が見込まれています。

主なメリット：

- **ハイブリッド ワークの生産性を向上**
  自宅やオフィスなど、どこにいてもプライベート アプリに高速かつシームレスにアクセスできます。
- **データ侵害のリスクを軽減**
  最小特権アクセスを適用すると同時に、アプリをインターネット上で見えなくすることで、攻撃対象領域を最小化してラテラル ムーブメントを防止します。
- **最も高度な攻撃者を阻止**
  業界初のプライベート アプリ保護と完全なインライン トラフィック インスペクションにより、侵害されたユーザーやアクティブな攻撃者からのリスクを最小限に抑えます。
- **アプリ、ワークロード、デバイスにまでゼロトラストを拡張**
  世界で最も優れた ZTNA プラットフォームが、プライベート アプリ、ワークロード、OT/IIoT デバイスに最小特権アクセスを適用します。
- **複雑な運用を簡素化**
  Zscaler のクラウドネイティブなプラットフォームが、拡張、管理、構成が複雑な VPN などの従来型のリモート アクセス ソリューションを廃止します。

過度に信頼し、必要以上のアクセス権を付与する城と堀のアーキテクチャーを悪用することで、攻撃者は従来のネットワーク セキュリティ アプローチを簡単に回避しています。他にも、次のような要素が悪用されています。

- **拡張性に欠け、高速でシームレスなユーザー エクスペリエンスを提供できないアーキテクチャー：**バックホールを必要とする VPN はコストと複雑さの問題だけでなく、現代のリモート ワーカーが許容できないほどの遅延を招きます。
- **大規模な攻撃対象領域を生み出す従来のファイアウォール、VPN、VDI、プライベート アプリ：**攻撃者は外部に公開された脆弱なリソースを見つけて攻撃します。
- **自由なラテラル ムーブメントを可能にする過剰なアクセス権：**VPN はユーザーを社内ネットワークに接続するため、攻撃者は機密情報に簡単にアクセスできます。
- **従来の制御を回避する侵害されたユーザーや内部脅威：**高度な攻撃者は認証情報を窃取してアイデンティティーを改ざんし、従来のリモート アクセス ツールや第一世代の ZTNA 製品を悪用してプライベート アプリにアクセスします。

今こそ、ユーザーを必要なアプリケーションに安全かつシームレスに接続させる手段を再考するときです。同時に、次世代 ZTNA でプライベート アプリのセキュリティも再定義する必要があります。

Zscaler Private Access™ (ZPA)

ZPA は世界で最も導入されている ZTNA プラットフォームであり、最小特権の原則を適用して、不正アクセスやラテラル ムーブメントを排除しながら、オンプレミスまたはパブリック クラウドで稼働するプライベート アプリへの安全な直接接続を提供します。包括的なセキュリティ サービス エッジ (SSE) のフレームワーク上に構築されたクラウドネイティブなサービスとして、短時間での導入を可能にし、従来の VPN やリモート アクセス ツールを置き換える形で以下を実現します。

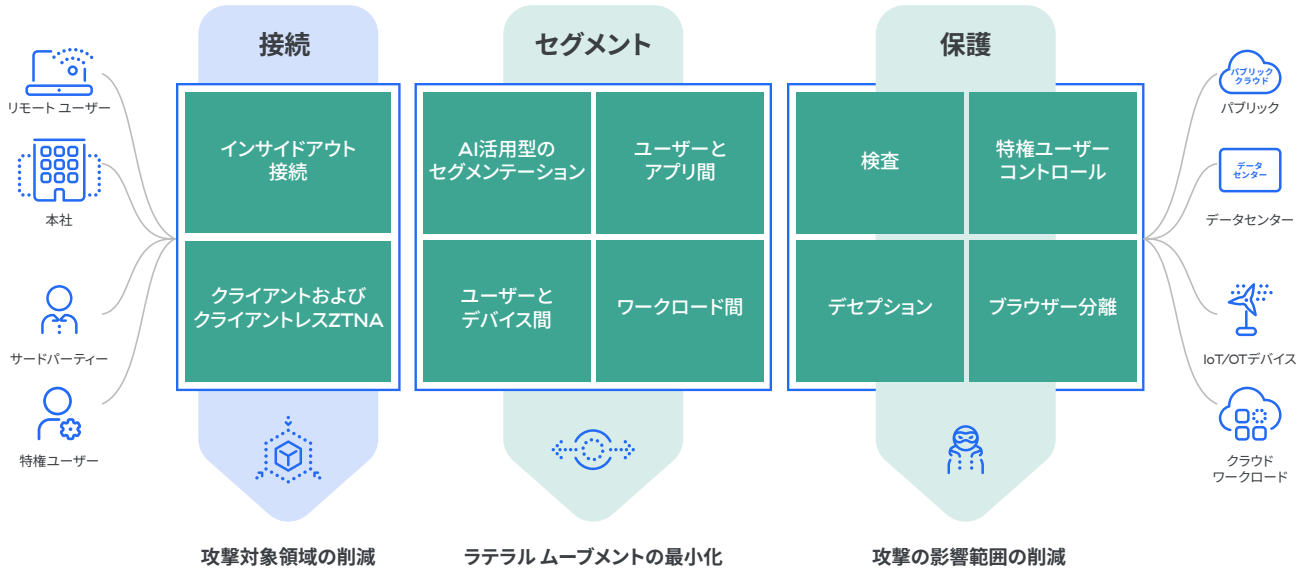
- **優れたユーザー エクスペリエンスの提供：**ユーザーを直接プライベート アプリに接続することで、従来の VPN で発生していた低速でコストのかかるバックホールを排除します。同時にユーザー エクスペリエンスの問題を常に監視し、事前予防的に解決します。
- **攻撃対象領域の最小化：**アプリケーションはインターネット上で見えなくなり、権限のないユーザーやデバイスはこれらを検知できません。ユーザーとアプリ間には内側から外側への接続が使用されるため、アプリと IP が外部に公開されることはありません。
- **最小特権アクセスの適用：**アプリケーションへのアクセスは、IP アドレスではなくアイデンティティーとコンテキストに基づいて確立されるため、ユーザーがネットワークに接続されることはありません。
- **ラテラル ムーブメントの排除：**アプリケーションをセグメント化することでユーザーがアクセスできるアプリを制限し、ラテラル ムーブメントを抑制します。
- **フル インスペクションによるサイバー攻撃の阻止：**プライベート アプリのトラフィックはインラインで検査されるため、最も一般的な Web 攻撃から防御できます。
- **データ損失の防止：**プライベート アプリ向けの統合 DLP や高度なインシデント対応、データ分類で、重要なアプリを保護します。
- **侵害されたユーザーやデバイスの検出：**統合されたデコイは、悪意のあるユーザーやデバイスを迅速に特定して削除します。

2025 年までに、新たに導入されるリモート アクセスの少なくとも 70% が VPN サービスではなく主に ZTNA で提供されるようになると予測されており、2021 年末の 10% 未満から大幅な増加が見込まれています *

— Gartner

*Gartner、Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access、Nat Smith、Mark Wah、Christian Canales、2022 年 4 月 8 日。

ZTNAの新たなユース ケースに対処するZPAの仕組み



主なユースケース

VPN からの移行

VPN はセキュリティ、スケーラビリティー、ユーザーエクスペリエンスを考慮した設計にはなっておらず、通常はリモート ユーザーのすべてのトラフィックを遠く離れたデータ センターにバックホールするため、遅延が生じ、これが結果としてユーザーのストレスにつながります。VPN は一度接続すると、ファイアウォールを越えてユーザーをトンネルでつなぎ、アプリケーションと同じネットワークに配置するため、自由にラテラル ムーブメントできる環境を生み出します。

ZPA は、VPN 特有のセキュリティ リスクを生じさせることなく、150 以上のグローバルに分散したポイント オブプレゼンス (PoP) を介してアプリケーションへの高速な直接アクセスを提供することで、これらの課題に対処します。内側から外側への接続により、アプリへのアクセスがネットワーク アクセスから切り離され、インターネットに接続されたフットプリントが排除されます。ZPA はユーザーをネットワークではなくアプリケーションに接続させるため、ユーザーは指定されたアプリにのみアクセスでき、水平方向へ移動することはできません。クラウドネイティブな性質を持つ ZPA により、IT 部門はロードバランサー、VPN コンセントレーター、その他のセキュリティデバイスなどのインバウンド ゲートウェイ アプライアンスを排除し、コスト、複雑さ、管理オーバーヘッドを削減できます。

ハイブリッドワークの保護

現代の従業員は自宅やその他の遠隔地、支店、本社など、あらゆる場所で作業しており、場所を問わない働き方が主流になったことで、従来のセキュリティの概念が大きく変化しつつあります。ZPA は場所やデバイスに左右されることなく、プライベート アプリへのシームレスで安全なアクセスを提供します。また、拠点内のユーザーに対しては、ZPA Private Service Edge を通じて同一のエクスペリエンスを確保します。

ZPA Private Service Edge を使用すると、クラウドの機能をオンプレミスにも展開し、リモート ユーザーと同じセキュリティ制御を高いパフォーマンスで施行できます。

ZPA では、高速で一貫したユーザー エクスペリエンスを実現するユニバーサル ZTNA 機能を利用できます。また、デジタル エクスペリエンス モニタリングにより、パフォーマンスの低下や障害がリアルタイムで可視化されるため、生産性の高いハイブリッド ワークが可能になります。Zscaler Zero Trust Exchange™ の一部として、統合された SSE プラットフォームがインターネット、SaaS、ワークロード、デバイス、プライベート アプリへの安全で高速な直接アクセスを実現します。

サードパーティー アクセス /VDI の代替手段

これまで、サードパーティーのアクセスは手間とコストのかかる仮想デスクトップ インフラ (VDI) や、RDP、SSH、VNC などのリモート デスクトップ クライアントに依存していたため、ユーザーはネットワークに直接接続され、内部システムは信頼できないデバイスに公開されていました。ZPA のクライアントレス アクセス機能は、コストを削減し、リスクを最小限に抑えながら、Web へのアクセスと同じくらいシンプルなサードパーティーのアクセスを可能にします。ベンダー、請負業者、パートナーは、クライアントを必要とせずに、自分のデバイスから任意の Web ブラウザーを使用して、イントラネットの Web サイト、内部システム、機器に接続できます。サードパーティー ユーザーや管理対象外デバイスをネットワークやアプリケーションから隔離し、機密データが制御不能になることなく、不正なコピー / 貼り付け、印刷、アップロード / ダウンロードから保護されます。クライアントレス アクセス機能により、IT 部門は従来の VDI の管理コストを発生させることなく、より優れたセキュアなエクスペリエンスをユーザーに提供できます。

M&A と事業分離

M&A と事業分離に際しては、ネットワークを組み合わせる必要があるケースが多くなりますが、IP が重複し、2 つの事業体の間にファイアウォールが存在するため難しくなります。ZPA は、M&A 後の統合および価値実現までの時間を劇的に加速させ、通常数か月かかるプロセスを数週間にまで短縮します。VPN を使わずにプライベートアプリへのシームレスなアクセスを提供し、複数のネットワークの統合や追加のネットワーク機器を購入する必要がなくなるため、より重要な作業に人員を充てることができます。

オペレーターのための OT および IIoT へのセキュアなアクセス

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、OT や IIoT の資産に定期的にアクセスする必要があります。ZPA は、現場や工場などのあらゆる場所から OT や IIoT 環境への安全で信頼性の高い高速アクセスを可能にします。ZPA for IoT & OT では、ジャンプホストや従来型 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ことなく、内部 RDP、SSH、VNC ターゲット システムへの完全に分離されたクライアントレス リモート デスクトップ アクセスが提供されます。

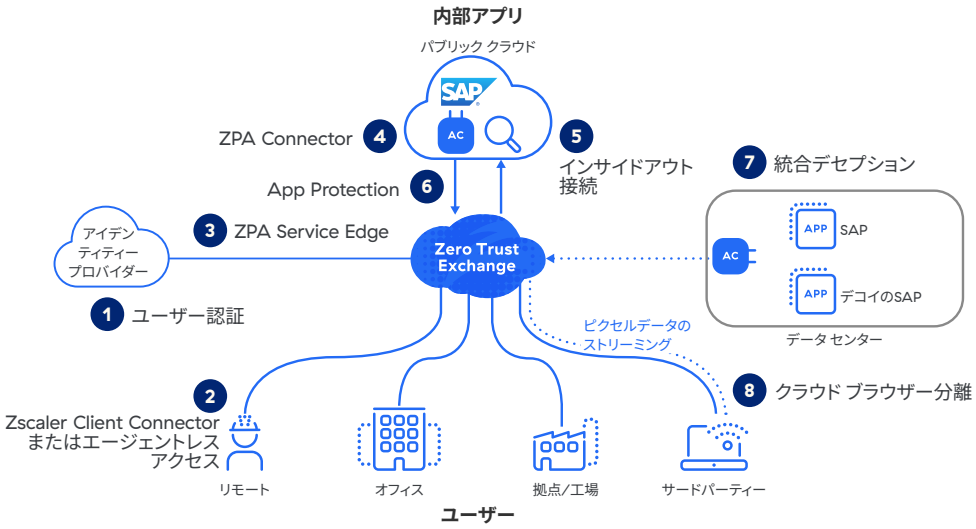
ワークロード間のセキュアな接続

現代の組織が求めているのは、プライベート、ハイブリッド、マルチクラウド環境全体の高速で安全なワークロード間接続です。ZPA for Workloads は、運用の複雑さとコストを削減しながら、すべての環境においてワークロードに対するゼロトラストベースの接続を実現します。ワークロードは ZPA の背後に隠されているためインターネットからは見えず、攻撃対象となることはありません。

拠点向けゼロトラスト接続

拠点向けゼロトラスト接続は複雑な VPN を使用することなく、拠点や工場、データ センターを安全に接続し、ビジネス 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。Zero Trust Exchange 経由でユーザーと IoT/OT デバイスをアプリケーションに接続することで、攻撃対象領域を排除し、脅威のラテラル ムーブメントを防止します。拠点向けゼロトラスト接続は複雑なルーティング、VPN、ファイアウォールを排除することで拠点間の通信を劇的に簡素化すると同時に、実績のある ZIA および ZPA 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。

ZPA は最小特権アクセスを企業全体に適用



仕組み

ユーザー (従業員、ベンダー、パートナー、請負業者) が内部アプリケーションにアクセスしようとすると、ZPA は以下の手順に従って安全な直接接続を提供します。

1. ユーザーは、既存の SAML SSO 認証情報を使用して IdP で認証します。
2. ユーザーのデバイス ポスチャーは、ユーザーのノート PC またはモバイル デバイスにインストールされた軽量の転送エージェントである Zscaler Client Connector で検証されます。ZPA は、すべての主要な EPP/EDR/XDR プロバイダー (CrowdStrike、Microsoft Defender、SentinelOne など) とのサードパーティー統合を介してデバイス ポスチャーを取り込むこともできます。
3. Zscaler のアプリが、ユーザーのトラフィックを最も近い ZPA Service Edge に転送します。ZPA Service Edge はブローカーとして機能し、ユーザーのセキュリティとアクセス ポリシーを確認します。
4. ZPA Service Edge がユーザーに最も近いアプリケーションを特定し、サーバーやアプリケーションをホストする環境にインストールされた軽量の仮想マシンである「ZPA App Connector」への安全な接続を確立します。
5. ZPA Service Edge がデバイス上の Client Connector と App Connector からの 2 つの送信トンネルを連結します。
6. ユーザーのデバイスとアプリケーションの間に接続が確立されると、App Connector が自動的にトラフィックをインラインで検査し、侵害された可能性のあるユーザーまたはデバイスからの潜在的な脅威を検知して阻止します。
7. 統合されている Zscaler Deception が、デコイ (おとり) のアプリにアクセスする侵害されたユーザーを検出し、Zero Trust Exchange 全体にわたって内部リソースへのアクセスを遮断します。
8. サードパーティー ユーザーの場合は、統合されたブラウザーベースのアクセスまたは管理対象外デバイスでのクライアントレス アクセス用の Zscaler Browser Isolation を使用してプライベート アプリに接続できます。

ZPA Service Edge には、Zscaler がクラウドでホストする ZPA Public Service Edge と、組織のインフラにてオンプレミスで実行する ZPA Private Service Edge があります。いずれの場合も Zscaler が管理するため、追加のアプライアンスは必要ありません。

主要な機能

リスクベースの ポリシー エンジン	強力なネイティブのポリシー エンジンを使用して、ユーザー、デバイス、コンテンツ、アプリケーションのリスク ポスチャーに基づいたアクセス ポリシーを継続的に検証し、認証されたユーザーのみがプライベート アプリにアクセスできるようにします。
統合された クライアント アクセスと クライアントレス アクセス	組織のハイブリッド環境に応じて、最適な保護方法を選択します。クライアントベースのアクセスでは、管理対象ユーザーが企業ネットワークの外にいる場合でも、軽量の Zscaler Client Connector エージェントを通じて保護されます。クライアントレス アクセスは、管理対象外のユーザーが任意のデバイスや Web ブラウザーからスムーズにアプリにアクセスできるようにします。
ブラウザー アクセス	BYOD およびサードパーティーのユーザーが、自分のデバイスから任意の Web ブラウザーで内部アプリにシームレスかつ安全にアクセスできるようにします。クライアントは必要ありません。
オンキャンパス ZTNA	拠点内のユーザー向けに、ユーザーをオフィス内のアプリケーションに安全に接続する ZTNA を提供します。ユニバーサル ZTNA は、ユーザーやアプリケーションの場所を問わず、ユーザーに一貫したアクセスとポリシーを提供します。
ディザスター リカバリー	ディザスター リカバリーは顧客側が管理する事業継続性ソリューションです。ZPA Private Service Edge を介して重要なプライベート アプリへのアクセス パスを作成し、ブラックスワン現象の発生時でも、ミッションクリティカルなアプリケーションにスムーズにアクセスできるようにします。
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 を活用した アプリの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。
ユーザーとアプリ間の セグメンテーション	ユーザーとアプリ間のセグメンテーションを使用して、すべてのアプリケーション アクセスが最小特権ベースで許可されるようにし、ユーザーをネットワーク上に配置することなく、承認されたユーザーのみが特定のアプリケーションに安全にアクセスできるようにします。内部のファイアウォールを使用した複雑なネットワーク セグメンテーションは必要ありません。
ユーザーとデバイス間の セグメンテーション	ユーザーとデバイス間のセグメンテーションを使用して、OT/IIoT 機器およびシステムへのすべてのアクセスが最小特権ベースで許可されるようにします。ZPA for IoT and OT により、サードパーティー ベンダーやリモート ユーザーがどこからでも機器に接続できるようになります。
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。
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。
統合デセプション	ネイティブのデセプション機能を使用して、非常に巧妙な攻撃者や内部脅威を検知して阻止します。Zero Trust Exchange 全体にわたって、侵害されたユーザーを自動的に封じ込める機能も含まれています。
統合された クラウド ブラウザー分離	BYOD を使用する請負業者や従業員に、重要な Web アプリケーションへのエアギャップ型のクライアントレス アクセスを提供します。脆弱性を抱えていたり、マルウェアに感染していたりする管理対象外のエンドポイントが、ネットワークやアプリケーションを侵害しないようにします。データ流出制御 (コピー / 貼り付け、印刷、アップロード / ダウンロード) を施行して、機密データの流出を防止します。
特権リモート アクセス	特権を持つ管理者やオペレーターが、VPN、VDI、または RDP、SSH、VNC などのリモート デスクトップ クライアントを使わずに、イントラネット Web サイト、内部システム、機器に安全に接続できるようにします。
脅威対策とデータ保護	コンテンツをすべて検査することで脅威のリスクを低減します。ユーザーとアプリ間の接続全体で、機密データを検出して管理します。
ゼロトラスト SD-WAN	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、ビジネス 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。

メリット

攻撃対象領域の最小化
脆弱な VPN を廃止してアプリをインターネットから見えなくすることで、権限のないユーザーがアプリを見つけて攻撃できないようにします。ZPA は、許可されたユーザーと特定のプライベート アプリの間に 1 つのセグメントを作成し、すべてのインバウンド接続を排除し、暗号化されたマイクロトンネルを介したユーザーのデバイスへの内側から外側へのみを許可します。また、管理者はアプリケーション検出機能を使用して不正なアプリケーション、サービス、ワークロードを自動的に検出してセグメント化できるため、攻撃対象領域がさらに減少します。

ラテラル ムーブメントの最小化
最小特権アクセスに基づく接続では、許可されたユーザーから指定のアプリケーションへの 1 対 1 のアクセスが確立されます。ネットワークへのフルアクセスは付与されないため、アプリ間またはネットワーク上でのラテラル ムーブメントは不可能になります。ZPA は IP アドレスをベースとしないため、複雑なネットワーク セグメンテーション、アクセス制御リスト (ACL)、ファイアウォール ポリシー、ネットワーク アドレス変換などを設定、管理する必要がありません。セキュリティ部門は ZPA の統合デセプション機能を使用することで、組織全体を水平移動しようとする悪意のあるユーザーや侵害されたデバイスを即座に検出し、隔離できます。

侵害されたユーザー、内部脅威、高度な攻撃者の阻止
インライン インスペクション、デセプション、情報漏洩防止機能を統合した、業界初のプライベート アプリ保護により、侵害されたユーザーやアクティブな攻撃者のリスクを最小限に抑えます。ZPA は OWASP Top 10 などの最も一般的な手法をすべてカバーし、ゼロデイ脆弱性に仮想パッチを即座に適用するカスタム シグネチャー サポートで Web 攻撃を自動的に阻止します。また、統合されたクラウド ブラウザー分離を使用して、アプリケーションへのアクセスを完全に分離し、管理対象外デバイスから機密データを保護することで、サードパーティーと BYOD のリスクを最小限に抑えます。他にも、デコイ アプリを使用する統合デセプション テクノロジーにより、セキュリティ部門は侵害されたユーザーがリソースにアクセスできないように、ネットワーク内のアクティブな脅威を封じ込めることができます。

優れたユーザー エクスペリエンスの提供
VPN クライアントへのログインとログアウトを必要としない一貫した高速接続により、これまで以上に安全で効率的なアクセス エクスペリエンスがリモート ユーザーに提供されます。サードパーティーの請負業者、ベンダー、パートナーは、クライアントをインストールすることなく、あらゆるデバイスや Web ブラウザーからスムーズにアクセスできます。ユーザーは、既存の SSO 認証情報 (Azure AD、Okta、Ping など) を使用して登録します。さらに、管理者はプライベート アプリへのアクセスの問題、ネットワークパスの停止、ネットワークの輻輳などによって生じるエンドユーザーのパフォーマンスの問題をプロアクティブに検出して解決することで、ユーザーの生産性を維持できます。

アプリ、ワークロード、デバイス全体で安全なアクセスを可能にする統合プラットフォーム
プライベート アプリやワークロード、OT/IIoT デバイスにゼロトラストを拡張し、個別のリモート アクセス ツールを簡素化して統合します。セキュリティとアクセス ポリシーを統合することで、侵害を阻止し、複雑な運用に伴う負荷を軽減します。

Zscaler Private Access のエディション

	機能	Essentials	Business	Transformation	Unlimited
プラットフォーム サービス	クラウドやデータ センターのプライベート アプリケーションへの安全なアクセスとリアルタイムの可視性	標準デバイスポスチャーの適用、ログ ストリーミング、ソース IP アンカリング、複数の IdP、状態監視	(+) データ センターへの拡張アクセス	(+) テスト環境、お客様の PKI による二重暗号化	
セグメンテーション	**App Segments** アクセス タイプ、ユーザーの権限、アプリのトラフィックに基づき、ユーザーとアプリケーション間のきめ細かいセグメンテーションに関する推奨事項を AI で生成	10	500	無制限	無制限
	App Connector お客様のサーバーを Zscaler Zero Trust Exchange に安全に接続する軽量 VM	20 ペア	50 ペア	無制限	無制限
	Private Service Edge お客様のローカル環境に展開されユニバーサル ZTNA とビジネス継続性を実現するサービスエッジ	1 ペア (仮想)	1 ペア / 5,000 ユーザー	1 ペア / 2,000 ユーザー	1 ペア / 1,000 ユーザー
侵害された ユーザーからの保護	**統合デセプション** 侵害されたユーザーを検出し、ラテラルムーブメントを阻止する統合デコイ	アドオン	Standard[1]	Advanced	Advanced Plus
	AppProtection Log4j などの既知の脆弱性のインラインでのエクスプロイトを防止し、プライベート アプリケーションのトラフィックを保護	アドオン	アドオン	✓	✓
安全なクライアントレス アクセス (サードパーティー ユーザー)	**ブラウザーベースのアクセス** BYOD および管理対象外のエンドポイント向けのブラウザー アクセス	アドオン	✓	✓	✓
	特権リモートアクセス OT システム (RDP/SSH/VNC) への安全かつクライアントレスの特権リモート アクセス	アドオン	PRA Essentials[2]	PRA Advanced[2]	PRA Advanced[2]
	プライベート アプリの データ保護のための分離 プライベート アプリにアクセスする BYOD/ 管理対象外デバイスへの情報漏洩防止	アドオン	アドオン	データ保護のための分離：Standard (100 MB/ ユーザー / 月)	データ保護のための分離：Advanced Plus (1.5 GB/ ユーザー / 月)
データの保護	**プライベートアプリ、分類、インシデント管理** プライベート アプリからの情報漏洩防止、高度なインシデント対応、データ分類	アドオン	アドオン	アドオン	✓
デジタル エクスペリエンス モニタリング	ユーザー、接続性、アプリケーションのテレメトリーを可視化し、ユーザー エクスペリエンスの問題を解決	–	Standard	Standard	Standard
Premium Support Plus	TAM サポート + 15 分以内の P1 応答	アドオン	アドオン	アドオン	✓

1. 最低 1000 の ZPA ライセンスが必要
2. システム / コンソール最大 10 件

他製品との主な違い

業界唯一の次世代 ZTNA プラットフォームである Zscaler Private Access は、優れたユーザー エクスペリエンスで高度なセキュリティを実現します。

- **最小特権アクセスのためにゼロから構築：**権限のあるユーザーに、ネットワーク全体ではなく承認されたリソースのみへの接続を許可します。これは従来の VPN では不可能です。
- **見えないアプリ＝攻撃できないアプリ：**プライベート アプリ、ワークロード、デバイスをインターネットから見えなくすることで、アプリの侵害やデータ窃取、ラテラル ムーブメントを阻止します。
- **完全なインライン検査：**プライベート アプリの悪用を特定して阻止し、最も一般的な Web 攻撃を自動的に防止し、業界最高の DLP でデータを保護することで、アプリケーションを守ります。
- **統合デセプション：**ネイティブのアプリ デセプション機能を備えた唯一の ZTNA ソリューションで、ラテラル ムーブメントの試行とランサムウェアの拡散を阻止します。
- **クライアントレス アクセス：**統合 DLP を使用して、サードパーティーに対してブラウザーベースのアクセスを提供します。
- **生産性の向上：**プライベート アプリのアクセスを完全に可視化し、ユーザー エクスペリエンスに影響を与えるユーザーの問題を検出します。
- **グローバルなエッジの展開：**世界 150 か所以上のクラウド エッジとゼロトラストを本社にまで拡張するローカルのサービス エッジで、優れたセキュリティとユーザー エクスペリエンスを実現します。
- **クラウドネイティブな基盤：**高価なオンプレミスのアプライアンスや複雑なインフラを必要としないクラウド型プラットフォームは、ビジネスの成長に合わせて拡張できます。
- **ユーザー、ワークロード、デバイス向けの統合型 ZTNA プラットフォーム：**業界で最も包括的な ZTNA プラットフォームを使用して、プライベートアプリやサービス、OT デバイスに安全に接続します。
- **拡張可能なゼロトラスト プラットフォームの一部：**完全な SSE フレームワーク上に構築された Zero Trust Exchange でビジネスを保護および強化します。

**Gartner、Magic Quadrant for Security Service Edge、Charlie Winckless、Thomas Lintemuth、Dale Koeppen、2024 年 4 月 15 日

Gartner は、Gartner リサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高のレーティング又はその他の評価を得たベンダーのみを選択するようにテクノロジーユーザーに助言するものではありません。Gartner・リサーチの発行物は、Gartner・リサーチの見解を表したものであり、事実を表現したものではありません。Gartner は、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の責任を負うものではありません。

基本的なコンポーネント

Zscaler Client Connector
ユーザーのノートパソコンやモバイル デバイス上で動作する軽量アプリケーションで、ユーザー トラフィックを最も近い Zscaler Service Edge に自動的に転送することで、セキュリティとアクセス ポリシーがすべてのデバイス、場所、アプリケーションに適用されるようにします。

Zscaler Branch Connector
物理アプライアンスと仮想アプライアンスの両形態で提供される Branch Connector は、バックホールを排除してすべての拠点とデータ センターのトラフィックを最も近い Zscaler のエッジ ロケーションに直接転送することで、アプリケーションのパフォーマンスを向上させて遅延を最小限に抑えます。Branch Connector により、ユーザー、サーバー、Client Connector をインストールできない IoT/OT デバイス、アプリケーション間の双方向通信が Zero Trust Exchange 経由を介してあらゆるネットワークで実現できます。

Zscaler Clientless Access
ユーザーは統合されたブラウザーベースのアクセス (Web、RDP、SSH、VNC)、または管理対象外デバイスでのクライアントレス アクセス用の Zscaler Browser Isolation を使用してアプリ、ワークロード、OT デバイスに安全に接続できます。

ZPA App Connector
軽量の仮想マシンで、データ センターまたはパブリック クラウドに展開されたプライベート アプリの前に配置されます。アプリをインターネットに公開しない内側から外側への接続で、承認されたユーザーと指定のアプリとの間のセキュアな接続を仲介します。

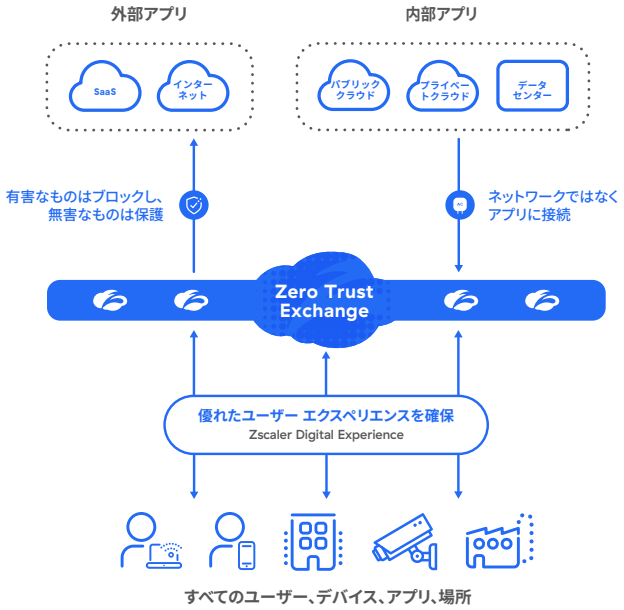
ZPA Service Edges
セキュリティとアクセス ポリシーを施行し、許可されたユーザー (Client Connector およびブラウザー アクセス経由) と特定のプライベート アプリ (App Connector 経由) 間に内側から外側への接続を確立します。Public Service Edge は世界 150 か所以上の Zero Trust Exchange でホストされており、大規模なグローバル組織の何百万人ものユーザーを同時に処理しています。Zscaler が管理する Private Service Edge はオンサイトでホストすることもできるため、オンプレミス ユーザーはローカル ネットワークを離れることなく、オンプレミス アプリケーションに最短経路でアクセスできます。

包括的な Zero Trust Exchange の一部である ZPA

Zscaler Zero Trust Exchange は、完全なセキュリティ サービス エッジ (SSE) を強化するクラウド ネイティブ プラットフォームで、ユーザー、ワークロード、デバイスを企業ネットワーク上に配置せずに接続します。これにより、ネットワークを拡張して攻撃対象領域を拡大させ、脅威のラテラル ムーブメントのリスクを高め、データ流出を防止できない境界ベースのセキュリティ ソリューションに関連するセキュリティ リスクと複雑さが軽減されます。

ユーザー、ワークロード、IIoT/OTにゼロトラストを提供するZscaler

わずか数週間で導入し、サイバー保護とユーザー エクスペリエンスを強化



技術仕様について

Zscaler のコンポーネント	サポートするプラットフォームとシステム	
Client Connector	iOS 9 以降 Android 5 以降 Windows 7 以降	macOSX 10.10 以降 CentOS 8 Ubuntu 20.04
Branch Connector	CentOS、Red Hat	VMware vCenter または vSphere Hypervisor
クライアントレス アクセス	最新の Web ブラウザー： (HTML5 対応)	Chrome Edge Firefox
App Connector	AWS CentOS、Oracle、Red Hat Microsoft Azure	Microsoft Hyper-V VMware vCenter または vSphere Hypervisor Docker ホスト

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