zscaler™

EBOOK

# ファイアウォールと VPN が組織を危険にさらす 4 つの理由

# 旧式のソリューションが生み出す新たな課題

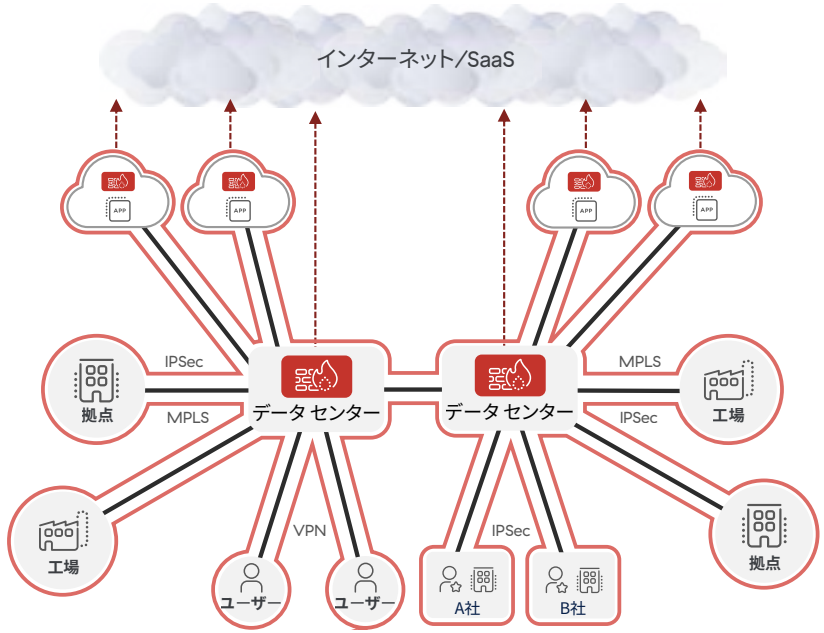
ファイアウォールと VPN は組織を危険にさらします。この 2 つは何十年にもわたって利用されてきたセキュリティ ツールであり、信頼できると考えられていますが、これこそが問題の核心なのです。両者は、現在とは働き方が大きく異なる時代に合わせて設計されたものです。これまで、ユーザーとアプリ ( 本社か拠点かを問わず ) はオンプレミスに存在していたため、それらを接続するネットワークの周囲に境界を確立するセキュリティ対策が講じられてきました。言い換えれば、ハブ&スポークのネットワークが城と堀のセキュリティ モデルによって防御されていたのです。

こうしたアプローチは、境界ベースのアーキテクチャー、ネットワーク中心のアーキテクチャー、従来のアーキテクチャーまたはレガシー アーキテクチャーなどの名称で呼ばれていますが、そのいずれも、「良いものは中に入れ、悪いものは入れない」という手法でネットワークを保護するファイアウォールや VPN などのツールを使用するものでした。

近年、多くの組織が急速に進化を遂げていますが、これには COVID-19 のパンデミックが大きく影響しています。パンデミックが発生した 2020 年に生産性を維持するには、デジタル トランスフォーメーションを加速させ、クラウド アプリとリモート ワークを新たな標準にする必要がありました。しかし、ファイアウォール、VPN、そしてこれらのツールを前提とした境界ベースのアーキテクチャーでは、この大きな変化に対応できなかったのです。なぜなら、オフプレミスのユーザー、デバイス、アプリ、クラウドによって無限に拡張されるネットワークの周囲にセキュリティ境界を構築することができなかったためです。

レガシー アーキテクチャーでデジタル トランスフォーメーションを進めようとすると、複雑性、柔軟性、コスト、生産性の面で課題が生じます。また、最も重要な点は、こうしたアーキテクチャーはサイバー リスクを増大させ、組織を危険にさらしかねないということです。その 4 つの主な理由を以下のページで解説していきます。

**ファイアウォールと VPN 中心のアーキテクチャー**



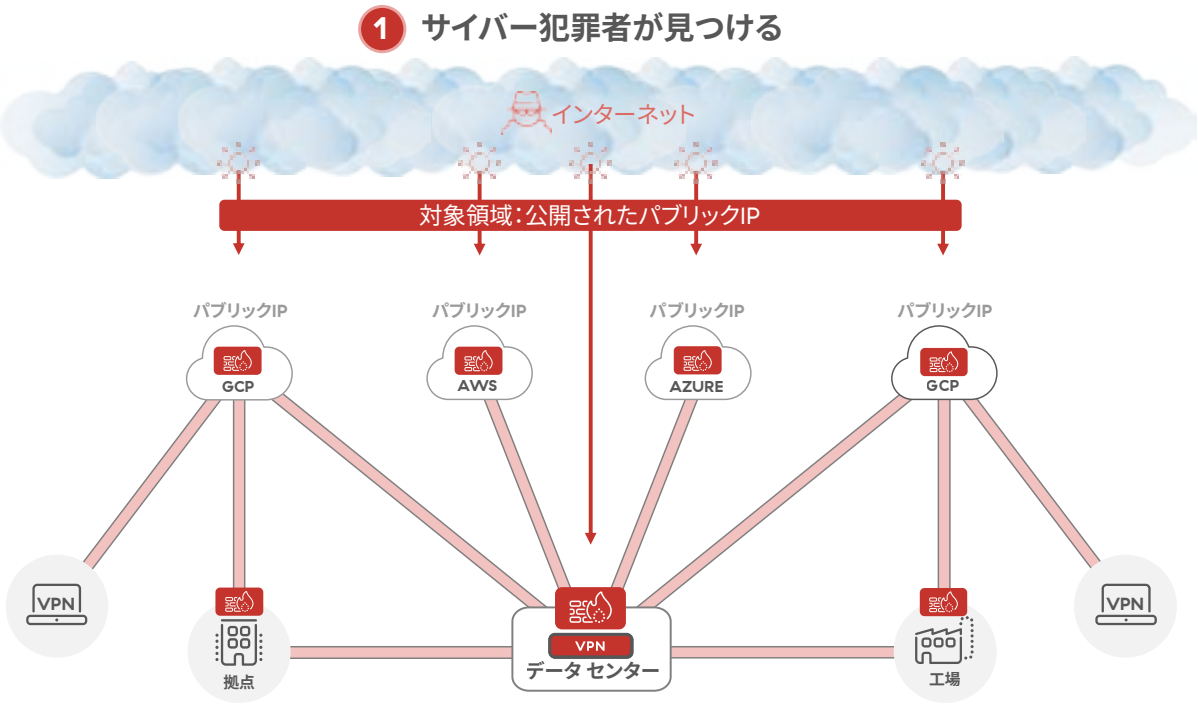

信頼されたネットワークがユーザー、サイト、アプリに接続します。
脅威対策とデータ保護はネットワークの保護に重点を置きます。

# #1 ファイアウォールと VPN は攻撃対象領域を拡大する

サイバー犯罪者は組織の防御を突破して攻撃を実行するために、常にターゲットを探しています。働き方が大きく変化し、境界ベースのアーキテクチャーによって攻撃対象領域が拡大したことで、脅威アクターはこれまで以上に簡単に攻撃価値の高いターゲットを特定できるようになっています。

前述したように、現代の環境でハブ&スポークのネットワークを使う場合、そのネットワークをリモート ユーザー、デバイス、クラウドベースのリソース、拠点にまで拡大し続ける必要があります。これは、無秩序に広がるフラットなネットワークが相互接続されたリソースにまで拡大し、そしてそのネットワークへの侵入経路としてサイバー犯罪者が悪用できる対象 ( クラウド アプリやリモート ユーザーなど ) が多数存在することを意味します。つまり、ネットワークが拡大し続けるということは、攻撃対象領域も拡大し続けるということです。

**リスクを増大させるファイアウォールと VPN 中心のアーキテクチャー**



残念ながら、境界ベースのアーキテクチャーが抱える攻撃対象領域の問題は、上記の問題よりもはるかに深刻です。その原因となっているのがファイアウォールと VPN です。これらのツールは城と堀のセキュリティ モデルがハブ&スポークのネットワークを防御するための手段と考えられていますが、意図しない結果をもたらす恐れがあります。

ファイアウォールと VPN には、パブリック インターネット上に公開されたパブリック IP アドレスがあります。これは許可された正規のユーザーが Web 経由でネットワークにアクセスし、そこに接続されているリソースとやりとりすることで、業務を遂行できるようにするためのものです。しかし、このパブリック IP アドレスは、攻撃対象を特定してネットワークへのアクセスを入手しようとする攻撃者からも見える可能性があります。

このように、ファイアウォールと VPN は攻撃対象領域を拡大するため、サイバー犯罪者にさらに多くの攻撃ベクトルを与えることになります。追加のファイアウォールや VPN を導入してセキュリティの拡張と改善を図るという一般的な戦略が、実際は攻撃対象領域の問題をさらに悪化させるという、悪循環を招いているのです。

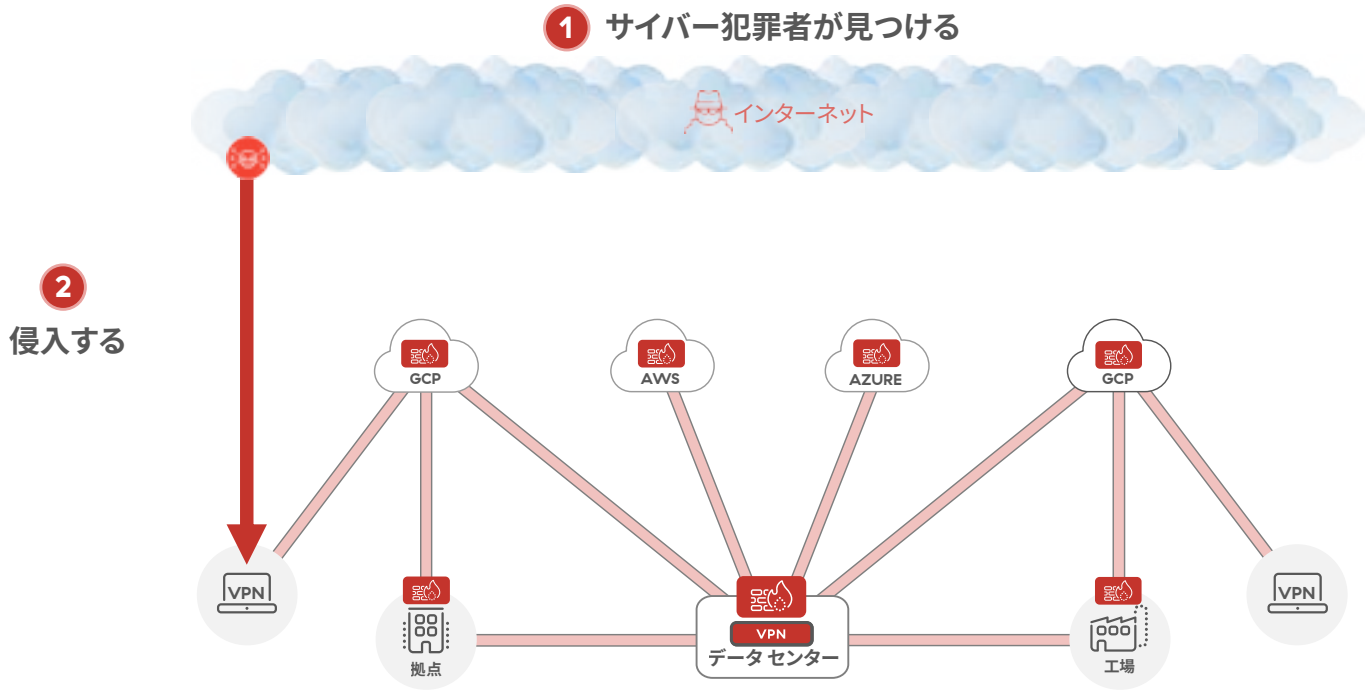
# #2 ファイアウォールと VPN では不正侵入を防止できない

サイバー犯罪者がターゲットを特定すると、組織の防御を突破するためにサイバー攻撃を開始します。繰り返しになりますが、ファイアウォールや VPN などの従来のツールでは攻撃チェーンのこの段階で組織を保護することはできません。

不正侵入を防ぐには、脅威が組織の環境に侵入して被害を与え始める前に、リアルタイムで脅威を阻止するインラインのセキュリティ ポリシーを使用する必要があります。

これはつまり、組織が業務全体のトラフィックをすべて検査し、潜在的な脅威を特定できる必要があるということです。また、Web トラフィックの 95% 以上が暗号化されているため、暗号化されたトラフィックを検査する機能も不可欠です。しかし、これこそがファイアウォールや VPN ベースのアーキテクチャーのもう 1 つの弱点なのです。

**リスクを増大させるファイアウォールと VPN 中心のアーキテクチャー**



トラフィックの復号、精査、再暗号化には膨大なコンピューティング能力が必要になるため、暗号化されたトラフィックの検査はリソースを大量に消費します。しかし、オンプレミスのハードウェア アプライアンスであっても、クラウド インスタンスの仮想アプライアンスであっても、ファイアウォールなどのセキュリティ アプライアンスでこれを行うのは簡単なことではありません。

その理由は、アプライアンスは一定レベルのサービスを提供する容量が固定されているためです。無制限に拡張できないアプライアンスでは、暗号化されたトラフィックを含む、すべてのトラフィックをリアルタイムで検査したいという組織の高まるニーズに対処できません。その結果、従来のツールやアーキテクチャーに依存している組織では、暗号化されたトラフィックが十分に検査されないばかりか、最悪の場合、検査がまったく行われないという事態も発生しています。

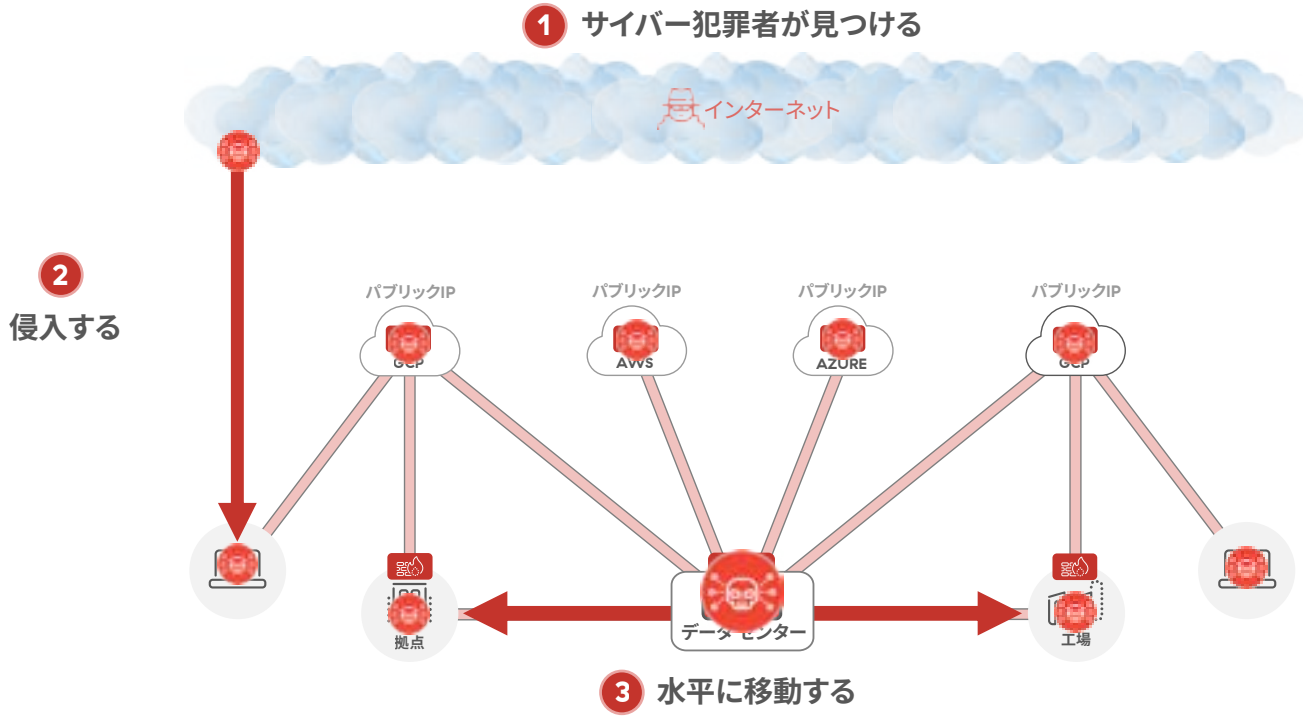
暗号化されたトラフィックを大規模に検査しない限り、脅威は検出されずに防御をすり抜けるため、攻撃者は自分たちの計画を実行できるようになります。サイバー犯罪者はこの実態に着目し、暗号化されたトラフィックを攻撃手段として使用し始めました。現在、サイバー攻撃の約 **86%** が暗号化されたトラフィックを介して発生しているため、これらを検査しない以上、防御を突破しようとする脅威の大部分を阻止できません。このように、ファイアウォールと VPN のアーキテクチャーでは不正侵入を防ぐことができないのです。

# #3 ファイアウォールと VPN は脅威のラテラル ムーブメントを招く

サイバー脅威が侵入に成功し、組織の防御を突破すると、ファイアウォールと VPN の弱点が完全に露呈します。ラテラル ムーブメントは水平方向の伝播としても知られているとおり、脅威がネットワーク上を移動してさまざまなリソース ( オンプレミスのアプリケーション、プライベート クラウドのワークロード、SaaS アプリケーションなど ) にアクセスする手法です。脅威が組織の境界を突破し、侵害するのは、1 つのアプリケーションだけではありません。脅威のラテラル ムーブメントが発生する仕組みを理解するには、「城と堀のセキュリティ」という言葉の意味を考えるとわかりやすいかもしれません。

堀は城を守るために使用されます。敵からの侵略を防ぎ、要塞内の宝石や人々を守る役割を果たします。しかし、敵が堀を越えてしまった場合、この境界防御は意味をなさなくなります。城自体に強固な防御策が施されていないため、あっという間に侵略を受けてしまうのです。

**リスクを増大させるファイアウォールと VPN 中心のアーキテクチャー**



このような城と堀モデルの弱点は、ファイアウォールや VPN が抱える課題と通じるものがあります。その理由として、一部の組織が利用し続けているハブ&スポーク ネットワークが高度に相互接続された性質を持つこと、そして城と堀のセキュリティ モデルがネットワーク全体へのアクセスを防止することに焦点を当てた脅威対策であることが挙げられます。

ファイアウォールを「堀」、VPN を「跳ね橋」、ネットワーク自体を「城」と想定してください。サイバー脅威が「堀」を越えて「城」に侵入すると、悪意のある攻撃者は接続されたリソースから別のリソースに簡単に移動し、「城」内のさまざまな「部屋」にアクセスできます。

比喩を用いずに言うと、ファイアウォールや VPN では脅威のラテラル ムーブメントが可能になり、サイバー犯罪者は侵害の範囲をネットワーク全体に拡大することができるため、多大な損害や混乱、コストを招く原因となります。どこかを侵害できるということは、あらゆる場所を侵害できるということです。この問題の解決策として頻繁に挙がるのがネットワーク セグメンテーションですが、この手法ではさらにファイアウォールを購入することになり、従来の境界ベースのツールに内在するアーキテクチャーの根本的な問題には対処できないのが実状です。

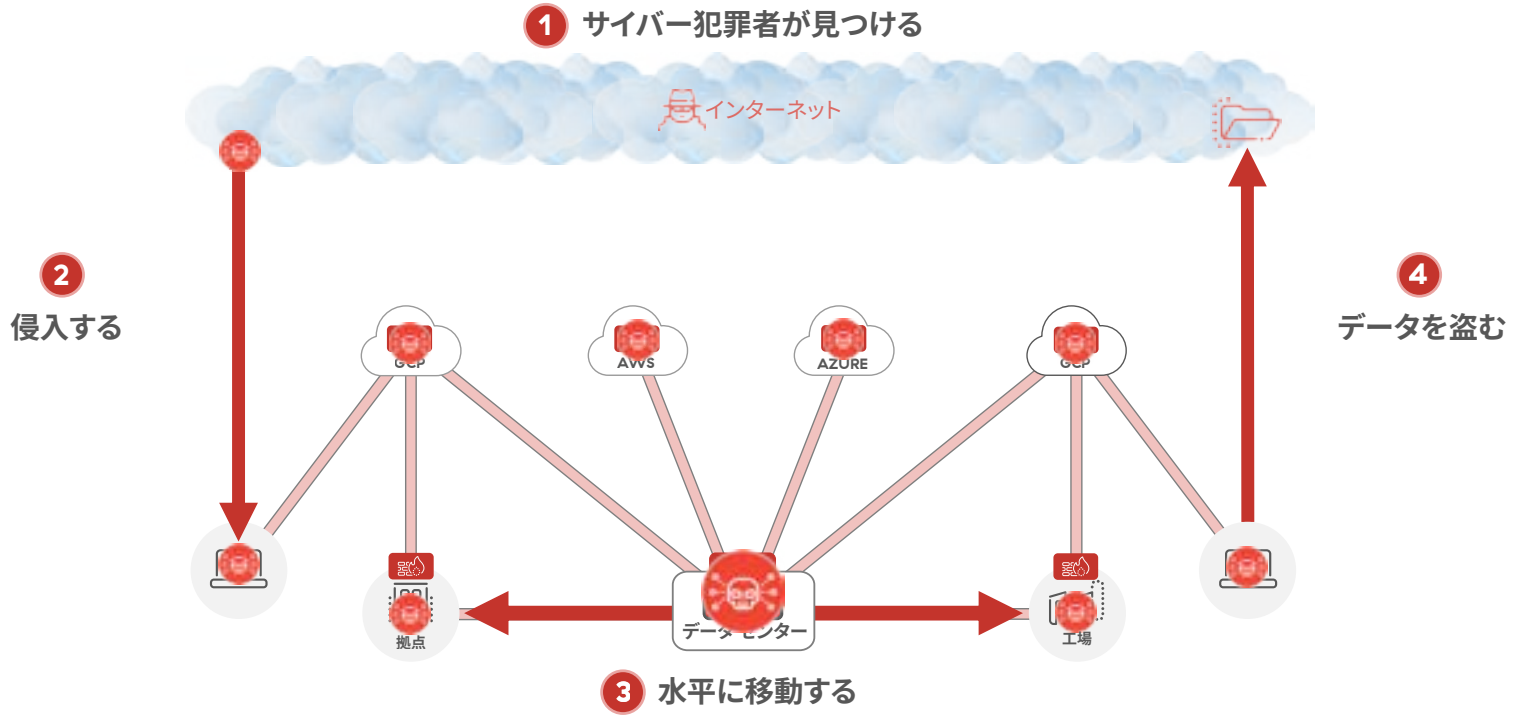
# #4 ファイアウォールと VPN はデータ漏洩を引き起こす

サイバー攻撃の大部分において、悪意のある攻撃者は単にスリルを求めて組織に侵入しようとしているわけではなく、主に機密情報を盗むことを目的としています。サイバー犯罪者は、盗み出したデータを多額の利益を得るためにダーク Web で販売したり、二重脅迫型ランサムウェア攻撃で組織に身代金を支払わせるための武器として利用したりします。いずれにしても、その影響は組織に深刻な打撃を与える恐れがあります。

サイバー犯罪者が攻撃対象領域を見つけ、防御を突破して侵入し、ラテラル ムーブメントを開始すると ( この 3 つのステップはファイアウォールと VPN によって簡単に実行できます )、特に機密性の高い情報や規制されている情報を優先して、できるだけ多くのデータを探し始めます。そして、この後にデータの持ち出しが発生します。

従来のツールで攻撃チェーンのこの最終プロセスを阻止しようとすると、再び危険な結果となり、データの流出につながります。

**リスクを増大させるファイアウォールと VPN 中心のアーキテクチャー**



前述したように、今日の Web トラフィックの 95% 以上が暗号化されており、暗号化されたトラフィックの検査には多大なコンピューティング能力が必要になります。容量が固定されたアプライアンスでは、必要に応じて拡張することができず、成長する組織が生成する大量の暗号化されたトラフィックを処理できません。ハードウェアと仮想アプライアンスの両方が抱えるこの問題は、不正侵入だけでなくデータ流出の原因にもつながります。サイバー犯罪者は、暗号化されたトラフィックを十分検査しない組織が存在することを認識しており、データを持ち出す際はこのトラフィックを優先的に使用しています。

しかし、ファイアウォールなどのツールが情報漏洩を阻止できないのは、スケーラビリティーだけが原因ではありません。従来の技術は、クラウド アプリやリモート ワーカーが登場する以前の時代に合わせて設計されたため、Google Drive、Box、Microsoft OneDrive のような SaaS アプリケーションに組み込まれた共有機能などの最新の経路からは情報漏洩を阻止できないのです。同様に、誤って「パブリック」に設定された AWS S3 バケットなど、設定ミスのあるクラウド リソースからデータが漏洩した場合、ファイアウォールや VPN、そして従来の情報漏洩防止 (DLP) ツールでは修復できません。

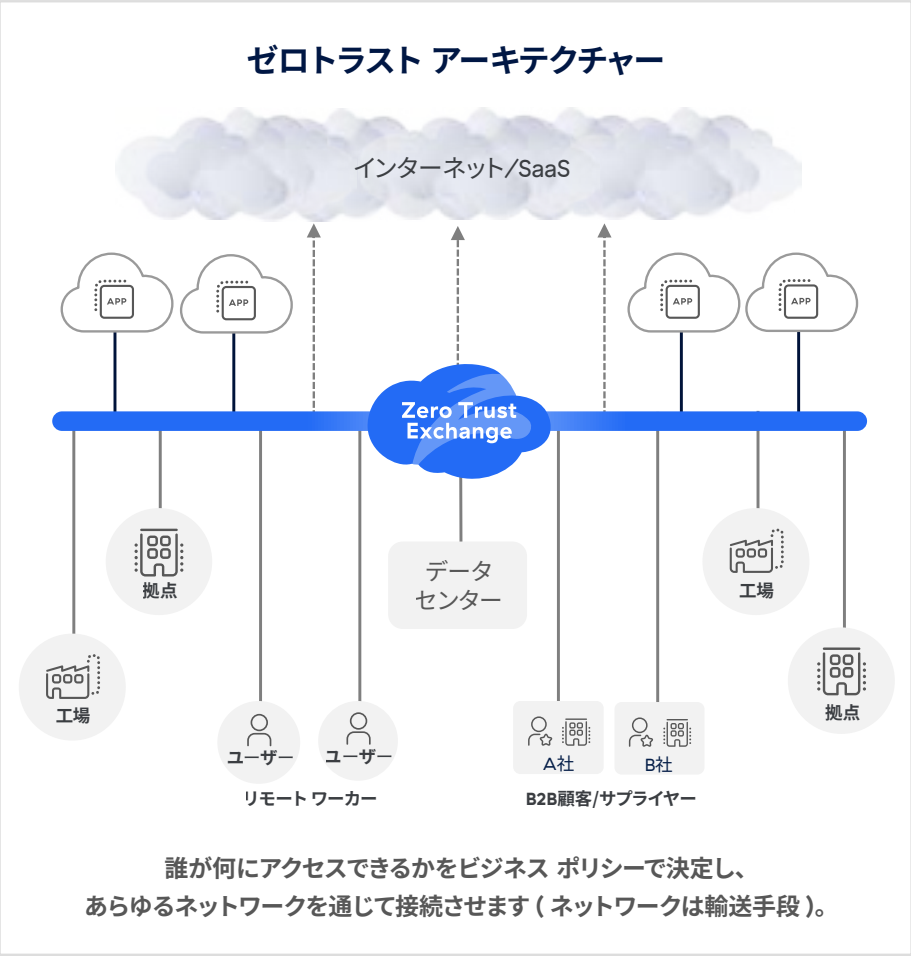
外部からの攻撃者は、こうした最新の手段を悪用して機密情報を盗もうとします。ただし、データに対する脅威はそれだけではありません。悪意のある、または不注意な内部関係者からも上記の方法で機密情報が漏洩する可能性があります。漏洩元にかかわらず、データを安全に保つにはセキュリティを進化させる必要があります。

# 4 つの課題を解消するゼロトラスト アーキテクチャー

ゼロトラストは、既存のネットワーク中心のソリューションに追加するためのツールではありません。また、単に境界ベースのアーキテクチャーの問題だけを軽減し、根本原因は解決しないというものでもありません。ゼロトラストは、最小特権アクセスの原則に基づいたアーキテクチャーであり、ファイアウォールや VPN をベースとした一般的なアーキテクチャーとは本質的に異なります。

ゼロトラスト アーキテクチャーは、グローバルなセキュリティ クラウドを最大限活用しています。このクラウドはインテリジェントな交換機として機能し、ネットワークをユーザー、ワークロード、IoT/OT デバイス、B2B パートナーに拡張することなく、セキュアな接続を実現します。同時に、ゼロトラスト クラウドはエンド ユーザーにできるだけ近い場所から、サイバー脅威対策やデータ保護などを含む包括的なソリューション スイートをサービスとして提供します。

**ゼロトラストはセキュリティと接続をネットワークから切り離し、境界ベースのアーキテクチャーからの脱却をサポートします。**



この最新のアーキテクチャーは、組織を危険にさらすファイアウォールと VPN の 4 つの課題を次の方法で解消します。

- **攻撃対象領域を最小限に抑制：**ゼロトラストを活用して、ネットワークの際限のない拡大を阻止します。また、ファイアウォール、VPN、およびそのパブリック IP を排除し、インバウンド接続を防ぎ、アプリをゼロトラスト クラウドの背後に隠します。
- **不正侵入を阻止：**脅威を特定し、セキュリティ ポリシーをリアルタイムで施行する高性能なゼロトラスト クラウドを通じて、暗号化されたトラフィックを含むすべてのトラフィックを大規模に検査します。
- **脅威のラテラル ムーブメントを防止：**最小特権アクセスの原則を維持し、ユーザー、ワークロード、デバイスをネットワーク全体ではなくアプリに直接接続します。
- **情報漏洩を阻止：**暗号化されたトラフィックや、クラウド内の保存データ、従業員のエンドポイント デバイスで使用中のデータなど、あらゆる経路からデータ流出を阻止します。

ゼロトラスト アーキテクチャーは、侵害リスクの軽減だけでなく、複雑性の軽減、ユーザーの生産性の向上、コストの節約、組織のダイナミズムの強化を実現し、ファイアウォールや VPN ベースのアーキテクチャーのさまざまな問題を解決します。

# まとめ

ゼロトラスト アーキテクチャーを求める組織に最適なプラットフォームとなるのが、AI を活用した Zscaler Zero Trust Exchange です。世界最大のセキュリティ プラットフォームとして、その規模と実績で新たな価値を提供します。

**160 以上**
世界中のデータ センター

**5,000 億以上**
保護するトランザクション
(1 日あたり )

**500 兆以上**
テレメトリー シグナル (1 日あたり )

**70 以上**
ネット プロモーター スコア

**45%**
Fortune 500 のお客様

**リーダー**
Gartner SSE の MQ

毎月開催のウェビナー「Zero Trust 101: Start Your Journey Here」に登録して、詳細をご確認ください。このウェビナーでは、誰でも理解できるように入門レベルの観点からゼロトラスト アーキテクチャーについて解説します。これはゼロトラストへの移行全体を導くように設計された 3 部構成シリーズの第 1 部です。


**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™プラットフォームは、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**

zscaler.com/jp