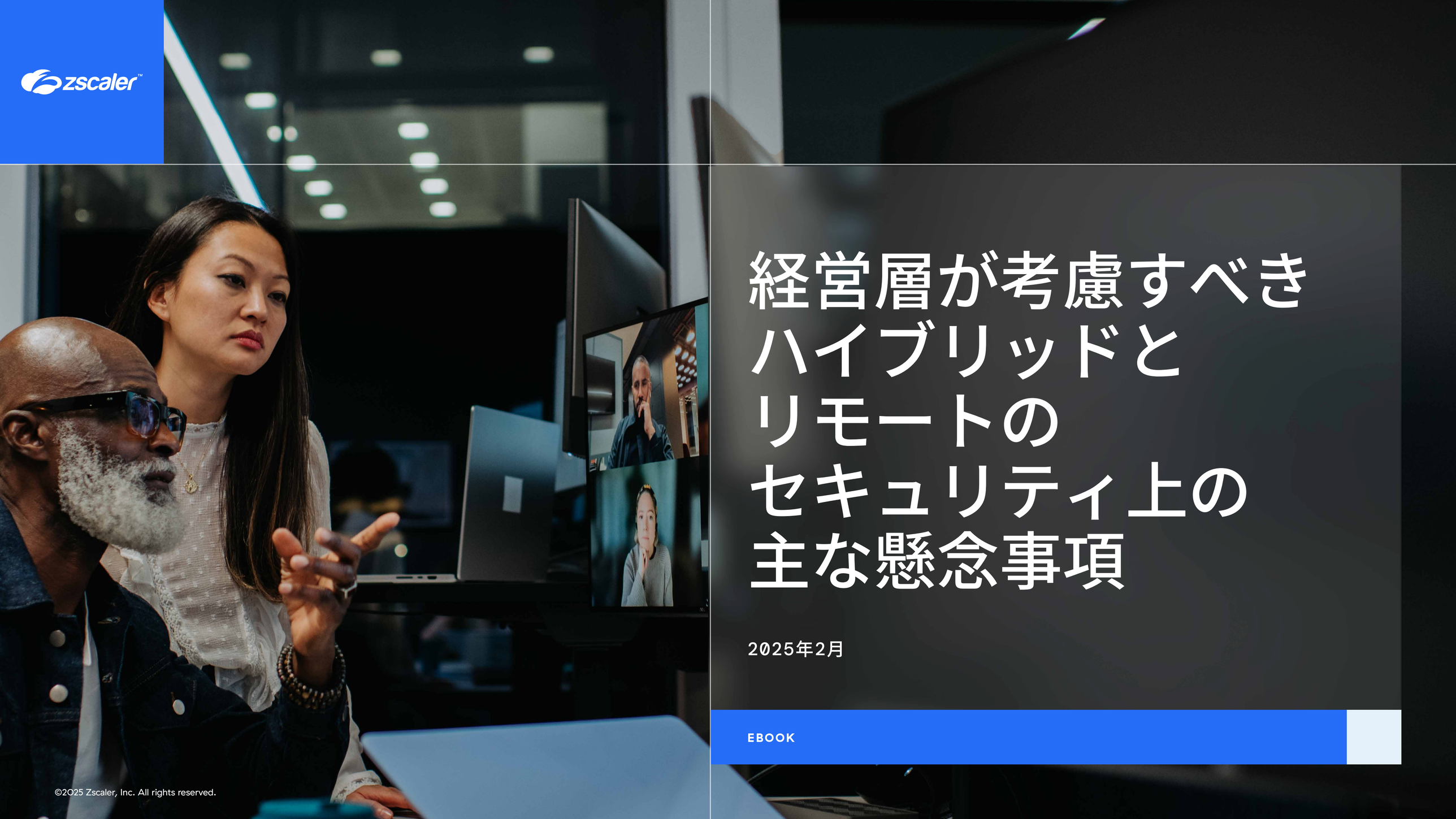


経営層が考慮すべきハイブリッドとリモートのセキュリティ上の主な懸念事項

2025年2月

EBOOK

©2025 Zscaler, Inc. All rights reserved.

目次



はじめに 3

ネットワークとリモートのセキュリティに関する重要な問題 3

進化するデジタル セキュリティ環境 4

デジタル セキュリティとリモート ワークの最近の傾向 4

リーダーが抱えるセキュリティ上の主な懸念事項 5

機密データの保護 5

内部脅威の管理 5

規制順守の徹底 5

リーダーの懸念事項を解決する戦略 6

堅牢なアイデンティティーおよびアクセス管理の実装 6

脅威の検知と対応の強化 6

定期的なセキュリティ トレーニングと意識向上プログラム 6

オフィス、ハイブリッド、リモートを保護するZscaler ソリューションの活用 7

Zscaler Internet Access (ZIA) 7

Zscaler Private Access (ZPA) 8

高度なセキュリティ機能 8

Zscalerで従業員を保護する方法 9

ファイアウォールからゼロトラストへ 9

包括的なゼロトラスト アプローチ 9

出典 9

©2025 Zscaler, Inc. All rights reserved.

はじめに

サイバー攻撃は、2024年第2四半期に全世界で前年同期比30%[1]という驚異的な増加を遂げました。リモート ワークが普及したことで攻撃対象領域が拡大し、組織はさまざまな脅威に対して脆弱になっています。ZscalerのThreatLabzが公開した暗号化された攻撃の現状レポートでは、TLS/SSLトラフィックに埋め込まれた321億件もの攻撃がZscalerクラウドで阻止されていることが明らかになりました。また、そのうちの87.2%が暗号化された脅威であり、前年から10.3%増加しています。[2] このデータは、脅威アクターが悪意のある活動を隠すために暗号化をさらに悪用するようになっている状況を浮き彫りにしています。

ファイアウォールや仮想プライベート ネットワーク(VPN)などの従来の技術は、組織のデータやアプリケーション、ネットワークを保護するうえで十分に機能しなくなっています。そのため、意思決定者やリーダーは、リモート ワーク環境の保護に関して多くの懸念を抱えており、侵害のリスクの最小化、規制や業界標準の順守、知的財産や企業秘密などの貴重なデータの窃取の防止を達成しなければならないプレッシャーに常にさらされています。

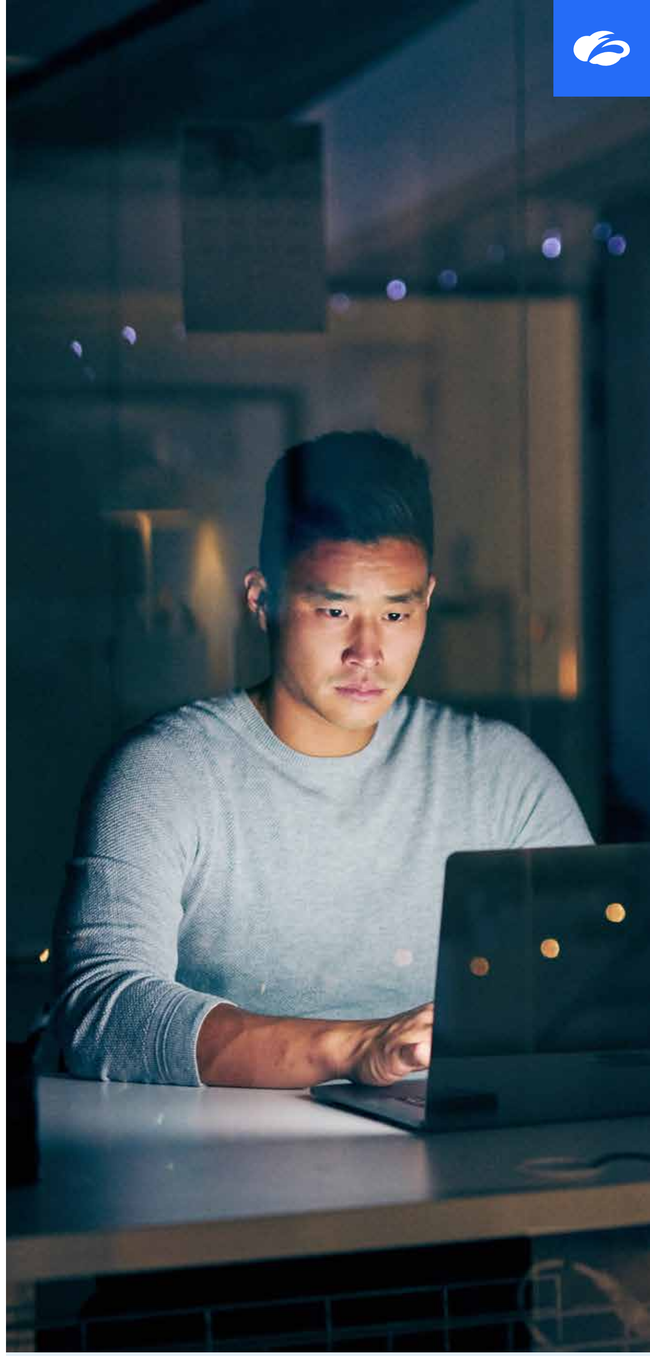
こうした課題を解消するのが、リモート ワークとハイブリッド ワークを運用する組織のネットワークを保護するように設計されたクラウドベースのゼロトラスト ソリューションです。適切なゼロトラスト テクノロジーを採用すれば、経営層はセキュリティ リスクを軽減し、組織をより適切に保護できます。

ネットワークとリモートのセキュリティに関する重要な問題

リモート ワークの導入により、データに対する組織の制御やセキュリティ アーキテクチャーの整合性が弱まる恐れがあります。セキュリティ ソフトウェアがインストールされていない、または常時監視されていない管理対象外デバイスを使用して、従業員が重要なアプリケーションを含む組織のリソースにアクセスすることもあります。

さらに、セキュリティの担当者や責任者はリモートの従業員が機密データをどのように取り扱っているのか、そして使用後にデータを削除しているのかを完全には把握できていません。従業員は個人のデバイスにデータを保存する可能性があるため、ランサムウェア攻撃やデータ侵害などの脅威に対して脆弱になります。

クラウドベースのアプリケーションへの移行は、攻撃対象領域をさらに拡大し、デジタル インフラのセキュリティをこれまで以上に複雑にしています。



©2025 Zscaler, Inc. All rights reserved.



進化するデジタル セキュリティ環境

パンデミックが起きる前は、ネットワークと機密データを保護するためにファイアウォールとVPNで十分だったかもしれません。しかし、リモート ワークとハイブリッド ワークにより、現在のデジタル環境を保護する方法について全面的な変革が必要とされています。

デジタル セキュリティとリモート ワークの最近の傾向

リモートの従業員がさまざまな場所で作業するには、必然的に組織のリソースにアクセスする必要があります。多くの組織は、リモート ワークに対応して生産性を向上させるために、クラウドベースのSoftware as a Service (SaaS)アプリケーションを採用していますが、分散している従業員のネットワーク全体にSaaSを展開すると、攻撃対象領域が拡大し、不正アクセスやセキュリティ侵害のリスクが高まります。

また、サイバー犯罪者はクレデンシャル スタッフィングやゼロデイ攻撃などのより高度な戦術を開発しており、サイバーセキュリティに関して経営層の負担が増しています。実際、米国は依然としてランサムウェアの最大の標的となっており、攻撃全体の49.95%を占めています。次いで英国、ドイツ、カナダ、フランスが主な標的となっています。[3]こうした攻撃は、組織の評判と顧客の信頼を損なうだけでなく、データ プライバシーとセキュリティの規制違反のリスクにもつながります。もちろん、金銭的なリスクも避けられません。

こうした傾向を踏まえて、経営層やセキュリティ リーダーは次のような新しいセキュリティ対策を採用しています。

- **ゼロトラスト アーキテクチャー**:「決して信頼せず、常に検証する」という原則に従い、すべてのユーザーとBYODを含むデバイスを検証します。
- **人工知能(AI)と機械学習(ML)を活用した脅威検出**:高度なサイバー攻撃を事前予防的に特定し、軽減します。
- **アプリケーション セグメンテーション**:脅威のラテラル ムーブメントを防止します。
- **エンドポイント セキュリティ**:リモートの従業員が使用するデバイスの保護に重点を置いています。AIを活用したソリューションは、エンドポイントに影響を与える前に脅威を検出して阻止し、分散した従業員を強力に保護します。

©2025 Zscaler, Inc. All rights reserved.

リーダーが抱えるセキュリティ上の主な懸念事項

リモート ワークとハイブリッド ワークが普及し、クラウドベースのソリューションの使用が増えるなかで、ビジネス リーダーやCISOは、境界ベースのセキュリティを超えて対策を考える必要があります。

機密データの保護

保護されていないネットワークから従業員が組織のデータにアクセスし、それを個人のデバイスに保存すると、不正アクセスやデータの誤った取り扱いのリスクが高まります。リモート ワーク環境で機密データを保護する方法として、次の3つが挙げられます。

- **エンドツーエンドの暗号化**：保存データや転送中データ、特に保護されていないチャネルで転送されるデータを保護します。
- **アイデンティティーおよびアクセス管理**：許可された従業員のみが必要なデータにアクセスして使用できるようにします。
- **情報漏洩防止**：偶発的なデータ流出や侵害を軽減します。

内部脅威の管理

オンサイトやリモートの従業員による偶発的または意図的な行動によって、システムのセキュリティが危険にさらされる場合があります。たとえば、新入社員がフィッシング詐欺の被害に遭ったり、不満を抱いている従業員が組織の機密データを悪用したりするかもしれません。こうした問題にロールベースのアクセス制御、最小特権アクセス ポリシー、行動分析で対処すれば、内部脅威のリスクを最小限に抑えられます。

規制順守の徹底

多数の政府が消費者の個人情報を保護するために、一般データ保護規則(GDPR)やカリフォルニア州消費者プライバシー法(CCPA)など、データ保護とプライバシーに関する法律を施行しています。さらに、医療保険の相互運用性と説明責任に関する法律(HIPAA)など、業界固有の規制もあります。リモート ワーク環境でこれらの規制要件を順守するには、徹底したガバナンス戦略が必要です。



©2025 Zscaler, Inc. All rights reserved.

リーダーの懸念事項を解決する戦略

現代の作業環境におけるセキュリティ上の複雑な課題に対処するために、経営層には次のような戦略の検討が求められます。

堅牢なアイデンティティーおよびアクセス管理の実装

アイデンティティーおよびアクセス管理(IAM)は、組織のネットワークとシステムへの不正アクセスを防ぐ効果的な方法です。これにより、適切なユーザーだけが業務に必要なアプリケーションやデータにアクセスできるようになります。

IAMは機密データへの不必要な公開を減らし、攻撃対象領域を最小限に抑えます。境界ベースのセキュリティとは異なり、ユーザーのデバイスや場所を問わず、より厳格にアクセスを制御できます。リーダーは、柔軟なIAMソリューションと統合に対応するプラットフォームの実装を検討する必要があります。

脅威の検知と対応の強化

サイバー犯罪者は常に攻撃手口を進化させているため、セキュリティ リーダーも組織の戦略を強化し、高度な脅威の検知と対応で攻撃を阻止する必要があります。そのためには、AI/MLモデルでネットワークトラフィックとユーザーの行動を監視し、異常を自動的に検知するソリューションを実装することが重要です。

また、AI/MLは、侵害されたデバイスやファイルをリアルタイムで隔離するゼロトラスト ソリューションも強化するため、脅威への迅速な対応が可能になり、事前予防的なサイバーセキュリティ アプローチが実現します。MLのアルゴリズムでは、新たな脅威を特定して阻止しながら、潜在的な脆弱性を絞り込むこともできます。

定期的なセキュリティ トレーニングと意識向上プログラム

セキュリティに関するポリシーやツールの効果は、それを使用する人によって決まります。CISOの80%は、2026年までに従業員の過失と人的リスクがサイバーセキュリティの主な懸念事項になると考えています。[4] リモート ワーク環境の従業員は、セキュリティ担当者に常に直接助けを求めることができるとは限らず、特に脆弱な存在です。結果として、遅延や取り返しのつかない損害につながりかねません。

以上のような状況を軽減する手段として有効なのが、継続的なセキュリティ トレーニングです。こうしたトレーニングを定期的に実施することで、従業員は既存の脅威、新たな脅威、進化する脅威について理解を深め、絶えず変化する脅威環境に警戒を怠らないようにするためのベスト プラクティスを身につけることができます。リモート ワークのベスト プラクティス、パスワード管理、データの安全な取り扱いについて各部門を教育すると同時に、サイバーセキュリティの全社的なルールやプロセスに関するトレーニングを定期的に実施し、デバイスやデータ、アプリケーションへのアクセスが侵害された場合の対処方法に関する明確なリソースを提供することが重要です。

©2025 Zscaler, Inc. All rights reserved.

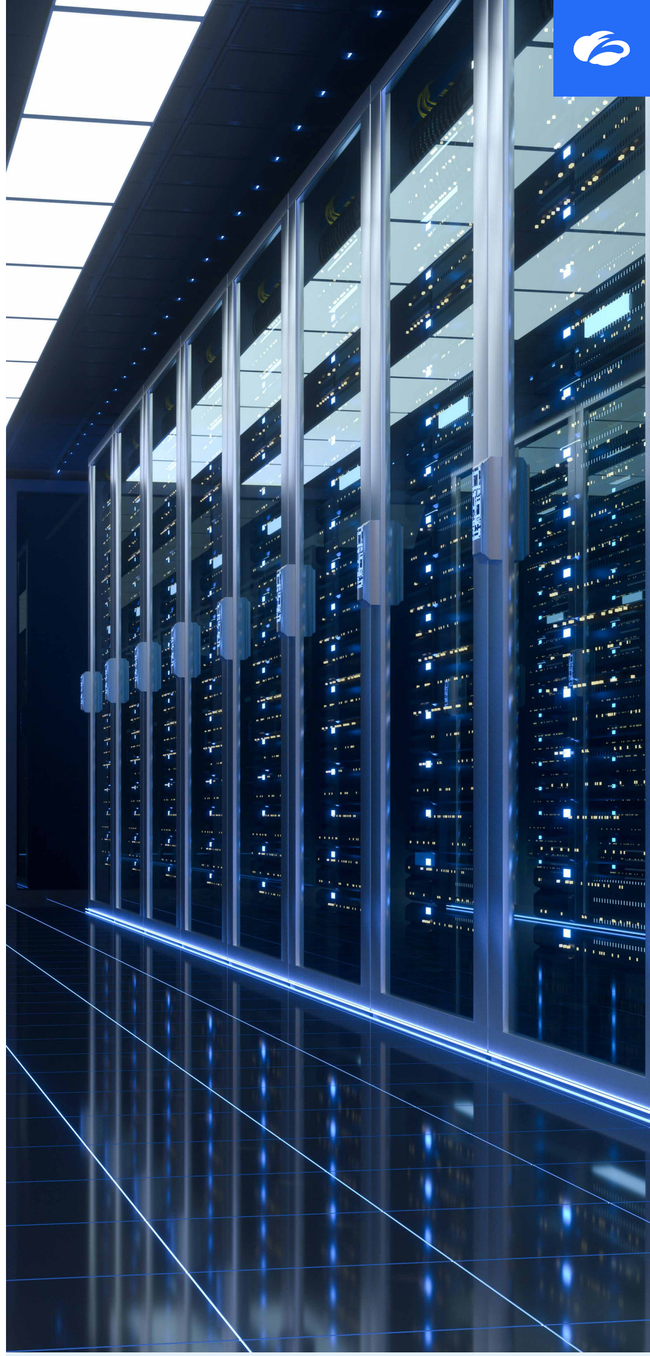
オフィス、ハイブリッド、リモートを保護するZscalerソリューションの活用

Zscalerが提供するクラウドベースのゼロトラスト ソリューションは、ビジネス リーダーが脅威の進化に合わせて現在と将来のあらゆる作業環境を保護できるように設計されています。Zscaler Zero Trust Exchange™には次のコア ソリューションが含まれており、各部門が包括的なセキュリティを確保できるようにします。

Zscaler Internet Access (ZIA)

Zscaler Internet Access: AIを活用したクラウドネイティブなゼロトラスト ソリューションであり、リモート ワーカーのデジタル セキュリティを強化します。すべてのTLS/SSLトラフィックを大規模に検査するゼロトラスト プロキシ アーキテクチャーを使用して、アイデンティティー、コンテキスト、ビジネス ポリシーに基づいてユーザーとアプリ間に直接接続を確立します。次の主な機能でSaaSとWebベースのアプリへのシームレスで安全なアクセスを確保します。

- **クラウドネイティブなセキュアWebゲートウェイ(SWG):** AIを活用したリアルタイムの分析とURLフィルタリングにより、高度な攻撃を検出して防止しながら、安全で高速なWebエクスペリエンスを提供します。
- **AI/MLベースの高度な脅威対策**：ボットネット、ランサムウェア、コマンド&コントロール、危険なファイル共有、悪意のあるアクティブ コンテンツ、クロスサイト スクリプティング、詐欺サイトなどの高度な脅威を阻止します。
- **AIを活用したURLフィルタリング**：フィッシングやランサムウェアなどの高度な脅威を阻止し、利用規定を適用することで、ユーザーがWebアプリを安全に閲覧できるようにします。
- **クラウド アクセス セキュリティ ブローカー(CASB):**統合された保護によって、クラウド アプリとデータの保護、脅威の阻止、SaaSとIaaS環境全体の規制順守を実現します。
- **情報漏洩防止(DLP):**完全なインライン検査、完全データー致(EDM)、インデックス文書一致(IDM)、機械学習を活用して転送中のデータを保護します。
- **動的なリスクベースのポリシー**：ユーザー、デバイス、アプリ、コンテンツの継続的なリスク分析に基づく動的なアクセス制御で、活動中の脅威を阻止しながら、将来の変化にも対応できる防御を実現します。
- **ゼロトラスト ファイアウォール**：すべてのポートとプロトコルにわたるユーザー トラフィックに対して高速かつ安全なネットワーク内外の接続とローカル インターネット ブレイクアウトを可能にします。ハードウェアやソフトウェアの更新管理は一切不要です。
- **AIを活用したブラウザー分離**：Webセッションをピクセル データに変換してユーザーのブラウザーに表示させることで、データ流出やデバイス感染を防止しながら、ネイティブに近いWebエクスペリエンスを確保します。
- **DNSセキュリティ**：リスクの高い悪意のあるドメインをフィルタリングし、悪意のあるペイロードや機密データを転送するためのDNSトンネリングの使用を阻止します。



©2025 Zscaler, Inc. All rights reserved.

Zscaler Private Access (ZPA)

Zscaler Private Access:業界初のAI活用型ゼロトラスト ネットワーク アクセス(ZTNA)ソリューションであり、すべてのユーザーにゼロトラスト アクセスを提供するクラウドネイティブな製品です。ZPAは、攻撃対象領域を最小化しながらプライベート アプリケーションへの直接接続を提供し、ユーザーとアプリ間のAI活用型セグメンテーションで脅威のラテラル ムーブメントを排除します。また、統合されたトラフィック検査、アプリケーション保護、データ保護の機能で高度な攻撃を防ぎます。ハイブリッド ワークを保護するZPAの主な機能には、次のようなものがあります。

- **AI活用型のアプリ セグメンテーション**:アプリケーションを自動的に検出します。アプリ セグメントとポリシーに関するAIからの推奨事項を活用することで、攻撃対象領域の削減とラテラル ムーブメントの防止を図れます。
- **ワークロード間のセグメンテーション**:AWSやAzureなどのハイブリッド環境とマルチクラウド環境でクラウドのワークロード間通信を保護します。
- **特権リモート アクセス**:リモート ワーカーやサード パーティーに機密性の高いRDP、SSH、VNC本番環境システムへのクライアントレス リモート アクセスを提供します。
- **Private Service Edge:** ZTNAをオンプレミスのユーザーにも適用し、最小特権アクセスによるユーザーからプライベート アプリケーションへの直接接続を可能にします。
- **事業継続性**:接続障害やブラック スワン現象の発生時にも、ミッションクリティカルなアプリケーションへのアクセスをポリシーを施行しながら中断なく提供します。
- **エクストラネット アプリケーションのサポート**:ビジネス パートナーやベンダーのネットワークでホストされているアプリケーションへのゼロトラスト アクセスを可能にします。
- **デジタル エクスペリエンス モニタリング**:アプリ、ネットワーク、デバイスの問題を迅速に検出して解決することで、デジタル エクスペリエンスを最適化し、ユーザーの生産性を維持します。

高度なセキュリティ機能

Zscalerは、次のような高度な機能も提供しています。

- **大規模なSSL/TLSインスペクション**:ユーザーとアプリ間のトラフィックを検査し、データを確実に保護します。
- **AIを活用したインライン脅威検出**:攻撃ベクトルが標的に到達する前に阻止します。
- **Risk360™:**リスクを明確に視覚化し、リスクの要因やインサイト、レポートを提供します。これらを活用すれば、リスクを軽減するための措置をすぐに講じることができます。

©2025 Zscaler, Inc. All rights reserved.

Zscalerで従業員を保護する方法

リモート ワーク環境のセキュリティを強化したい場合は、従来のサイバーセキュリティ ソリューションからの移行を検討する必要があります。Zscalerのゼロトラスト プラットフォームでは、さまざまな方法で簡単に移行を進められます。

ファイアウォールからゼロトラストへ

ファイアウォールやVPNは、組織のネットワークを拡張して侵入口を増やすため、現代のビジネス環境では効果が期待できません。これに対し、Zscaler Zero Trust Exchange™はインテリジェントな交換機として機能し、ユーザー デバイスの送受信トラフィックを検査して脅威を検出および阻止すると同時に、アプリケーションやクラウド リソースへの接続を安全に仲介します。

包括的なゼロトラスト アプローチ

セキュリティに対する真のゼロトラスト アプローチには、各ユーザー、デバイス、アプリケーションに合わせたアイデンティティー中心のコンテキスト対応型アクセス ポリシーが必要です。信頼できるユーザーのみが特定のリソースにアクセスできるようにするには、それらのユーザーとリソースが組織の確立された制御によって管理されている必要があります。ゼロトラスト セキュリティ フレームワークでは、場所、アイデンティティー、日時などに基づいてユーザーにアクセスを付与するルールを設定できます。Zscalerはこのプロセスの詳細な手順を提供するため、こうした制御を適切に導入できます。

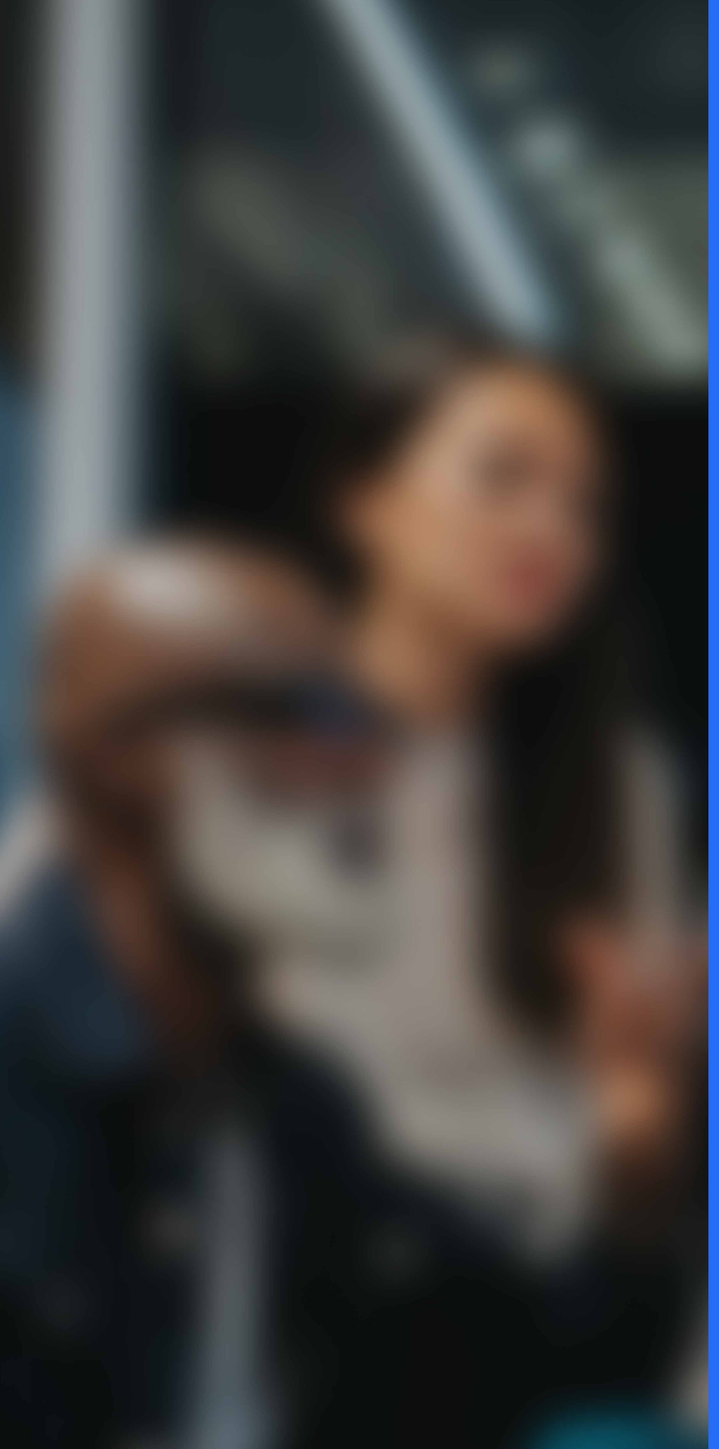
Zscalerは組織のセキュリティ態勢を改善し、分散した従業員を確実に保護します。デモを依頼してZscalerのゼロトラストを体験してください。

出典：

1. Intelligent CISO、Check Point Research unveils Q2 2024 cyberattack trends, highlighting global and UAE increases、2024年7月29日。
2. Zscaler、2024年版 ThreatLabz暗号化された攻撃の現状レポート、2024年。
3. Zscaler、2024年版 ThreatLabzランサムウェア レポート、2024年。
4. Infosecurity Magazine、70% of CISOs Expect Cyber-Attacks in Next Year, Report Finds、2024年5月21日。



©2025 Zscaler, Inc. All rights reserved.



zscaler™ | Experience your world, secured.™

©2025 Zscaler, Inc. All rights reserved. Zscaler™およびzscaler.com/jp/legal/trademarksに記載されたその他の商標は、米国および/または各国のZscaler, Inc.における(i)登録商標またはサービス マーク、または(ii)商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。

