zscaler™

2024年版 Zscaler ThreatLabz VPNリスク レポート

Cybersecurity INSIDERS

VPN のセキュリティ、リスク、ユーザーエクスペリエンスなどの最新動向を明らかにし、組織におけるゼロトラストの導入を加速させます。

目次

概要

働き方の分散化が進み、クラウド中心の作業環境が主流になったことで、アクセス手段はこれまでの仮想プライベート ネットワーク (VPN) からゼロトラストのようなより堅牢なセキュリティ フレームワークに移行しつつあります。VPN は長年にわたって、ユーザーやオフィス全体を接続するための重要なリモート アクセス機能を提供してきました。しかし、サイバー脅威が巧妙化し、リモート ワークやクラウド技術が進化するにつれ、VPN の深刻な脆弱性が浮き彫りになっています。旧式の VPN では、認証情報が一度検証されると広範なネットワーク アクセスが許可されるため、認証情報が侵害されてしまうと、サイバー攻撃のリスクが大幅に高まります。

先日発生した VPN アプライアンスへの攻撃では、米国の防衛を含むさまざまな業界に影響を与える重大な脆弱性 (特に CVE-2023-46805、CVE-2024-21887、CVE-2024-21893) が露呈しました。これは認証バイパスの脆弱性で、昇格された権限でコマンドを実行し、デバイスのリセット後も永続化を維持できるようにします。これを受けて、米国サイバーセキュリティ インフラストラクチャー セキュリティ庁 (CISA) は緊急指令を発行し、影響を受ける VPN デバイスを直ちにネットワークから切り離すよう連邦政府機関に指示しました。

米国政府は大統領令 14028 を通じて、従来の VPN を廃止し、サイバーセキュリティを強化するためにゼロトラスト アーキテクチャーの導入を義務付けています。この指令は、国家のサイバーセキュリティを強化するための包括的戦略の一部であり、連邦政府機関に対し、発信元に関係なくすべてのアクセス要求を検証するゼロトラストを実装するよう求めるものとなっています。行政管理予算局 (OMB) が米国連邦政府ゼロトラスト戦略でこの取り組みをさらに支援していることからも、ネットワークの境界内であれば暗黙的に信頼する VPN から、あらゆるアクセス要求を継続的に検証するアプローチへの移行が喫緊であることがわかります。これらの指令と推奨事項は、進化し続けるサイバー脅威に対してゼロトラストがより強力な防御を提供するというサイバーセキュリティ コミュニティー内の総意を反映するものであり、VPN の脆弱性を突いた攻撃が増加傾向にある今、その必要性は明らかです。

こうした状況を踏まえ、多くの組織がゼロトラスト モデルの導入を急速に進めています。このモデルでは、ネットワーク境界の内外を問わず、すべてのユーザーやデバイスが本質的に信頼されず、アクセス要求ごとに細かく検証されるため、ネットワーク内でのラテラル ムーブメント (攻撃者が初期アクセスを入手してネットワークに侵入した後に行う探索活動) を防ぐ有効な手段となっています。

このレポートでは、647 人の IT プロフェッショナルおよびサイバーセキュリティ専門家を対象とした調査結果に基づいて、VPN が抱えるセキュリティやユーザー エクスペリエンスのさまざまな課題を検証し、現在のアクセス管理の複雑さ、多様なサイバー攻撃に対する脆弱性、そして組織のセキュリティ態勢を低下させるリスクを紐解いていきます。また、デジタル トランスフォーメーションを安全に加速させるフレームワークとして強固な地位を確立しているゼロトラストなど、より高度なセキュリティ モデルについても概説します。

本調査の支援者である Zscaler に深く感謝の意を表します。ゼロトラストとセキュア アクセス ソリューションに関する Zscaler の専門知識は、私たちの調査結果を有意義なものへと導いてくれました。このレポートから得られる洞察や知見は、ゼロトラスト セキュリティの道を歩む IT およびサイバーセキュリティ専門家にとって不可欠なリソースになると確信しています。

Holger Schulze、
Cybersecurity Insiders の創設者

「過去 1 年間、大企業や連邦政府機関に侵入する足掛かりとして、VPN のさまざまな脆弱性が悪用されました。VPN のようなインターネットに公開されたレガシー資産 (アプライアンスや仮想) は、攻撃者が従来のフラットなネットワークを簡単に水平移動できるようにします。企業はこの事実を認識して、頻発する VPN を標的としたサイバー攻撃に備える必要があります。また、ゼロトラスト アーキテクチャーへの移行は必須です。移行することで、VPN やファイアウォールなどの旧式の技術の廃止、攻撃対象領域の大幅な削減、TLS インスペクションによる一貫したセキュリティ制御の施行、セグメンテーションとデセプションによる攻撃影響範囲の抑制などが実現し、深刻な被害をもたらすセキュリティ侵害を防止できます」

—DEEPEN DESAI、ZSCALER の最高セキュリティ責任者、

主な調査結果

増加の一途をたどる VPN 攻撃

過去 1 年間に最低 1 回の VPN 関連のサイバー攻撃を受けた組織は 56% にも上り (前年度は 45%)、VPN を標的とした攻撃の件数と巧妙さは高まり続けています。

ゼロトラストに移行する組織が増加

組織の 78% が、今後 12 か月以内にゼロトラスト戦略を実装する予定です。また、62% が VPN とゼロトラストは根本的に異なると認識しています。

大多数の組織が VPN のセキュリティを懸念

回答者の 91% が、VPN は組織の IT セキュリティ環境を危険にさらすと考えています。旧型やパッチ未適用の VPN インフラへの依存がサイバーリスクを高めるという事実は、最近のセキュリティ インシデントからも明らかです。

VPN ではランサムウェア、マルウェア、DDoS に対抗できない

回答者は VPN の脆弱性を悪用する主な脅威として、ランサムウェア (42%)、マルウェア (35%)、DDoS 攻撃 (30%) を挙げており、従来の VPN アーキテクチャーが抱える根本的な弱点がさまざまなリスクを生み出しています。

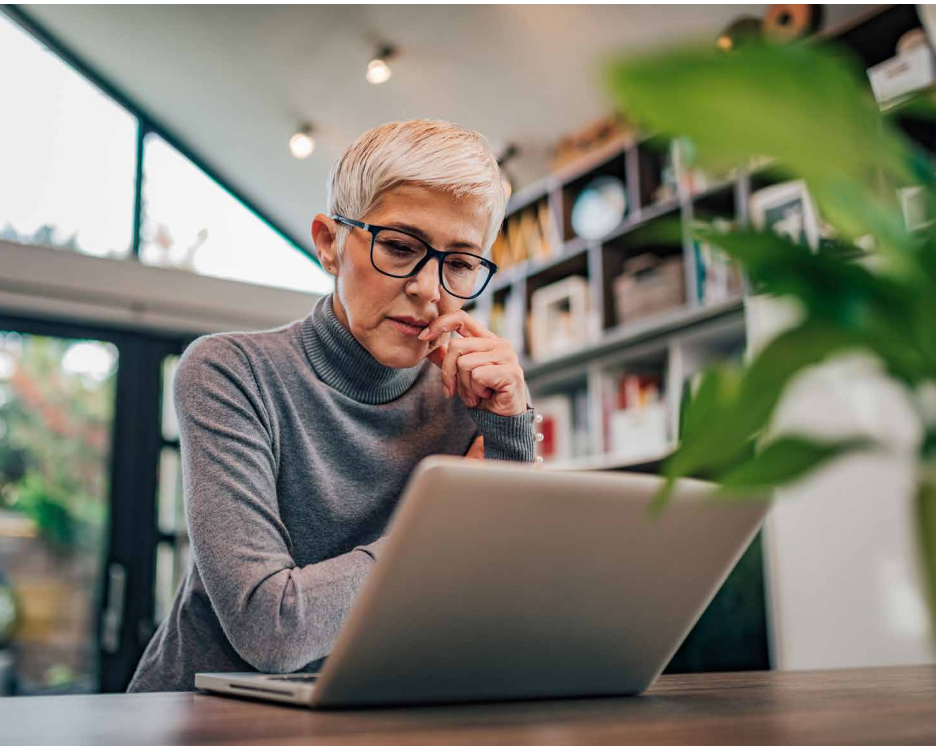
無視できないラテラル ムーブメントのリスク

VPN 攻撃を受けた組織の 53% が、脅威アクターによるラテラル ムーブメントを確認しています。これは、侵害の初期段階での封じ込めが失敗したことを意味しており、従来のフラットなネットワークのリスクの高さがあらためて顕在化しました。

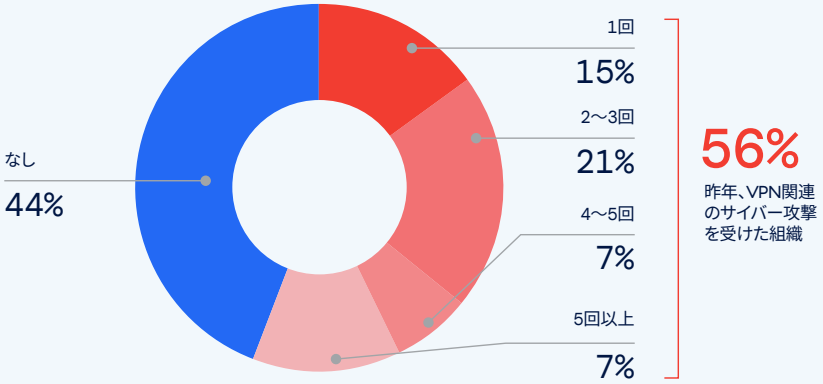
VPNのセキュリティに対する懸念

増加の一途をたどるVPN攻撃

VPN の脆弱性を悪用した攻撃は件数だけでなく、その深刻さも日々増しています。この実態からも、従来のサイバーセキュリティ対策がいかに無力であり、ネットワークの露出部分がリスクを生み出し続けているかをうかがい知ることができます。今回の調査によると、過去 1 年間に 56% の組織が VPN の脆弱性を悪用したサイバー攻撃を経験しており、前年の 45% から大幅な増加をみせています。また、41% が 2 回以上の VPN 関連の攻撃を受けており、深刻なセキュリティ ギャップがあることがわかります。



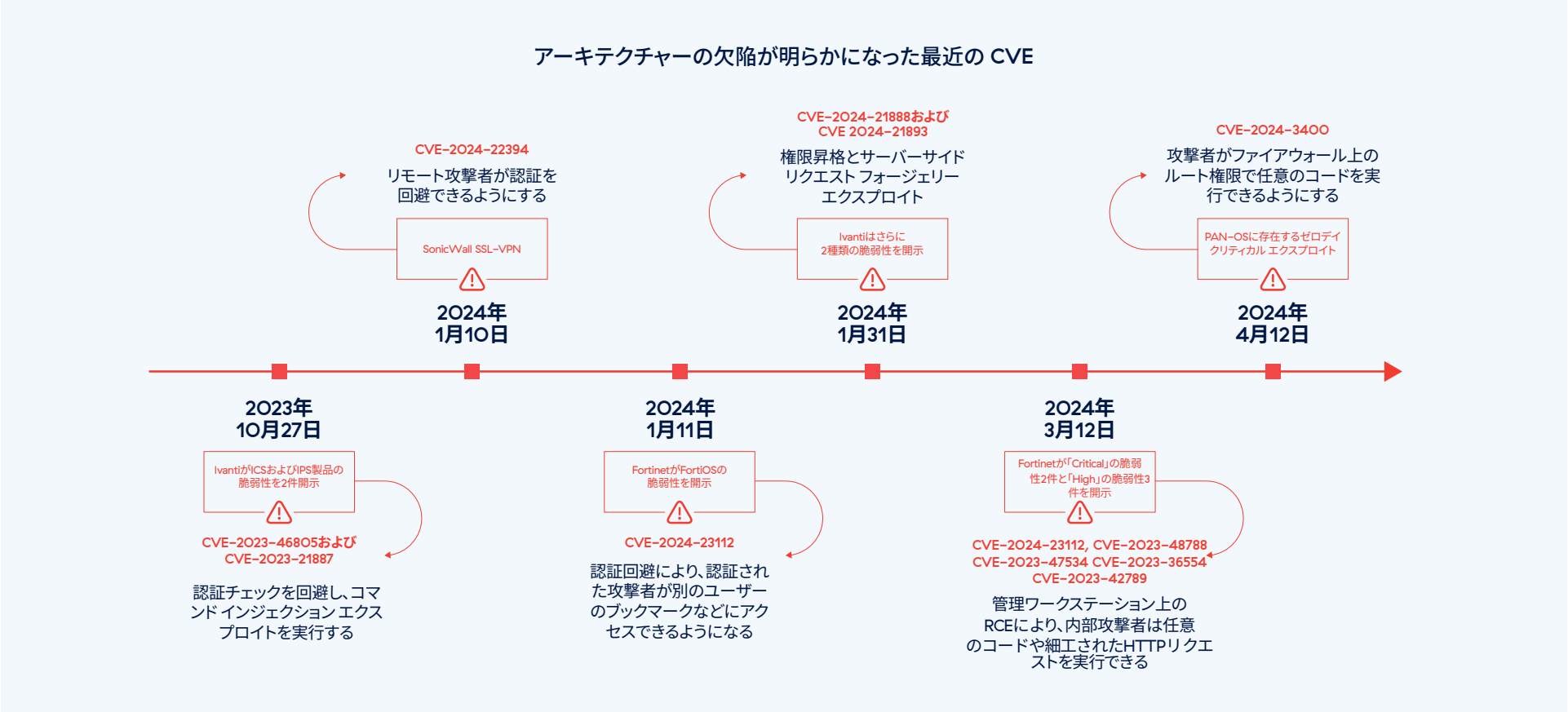
過去 1 年間に、どのくらいの頻度で VPN サーバーの脆弱性を悪用した攻撃を受けましたか？



VPN に対する攻撃は近年ますます頻発し、悪質化しています。例えば、VPN の弱点を突いたランサムウェアの事例が増えたことで (特に脆弱性が公開された直後に増加)、従来の VPN が抱える重大な欠陥が浮き彫りとなっています。攻撃者はこのような脆弱性を悪用して最初の侵入口を確保すると、ネットワークに侵入して水平移動できるようになるため、深刻なデータ侵害や運用の混乱につながる恐れがあります。

過去1年間の主なVPNの脆弱性

VPN 製品に影響を与える深刻度の高い CVE が相次いで公開されており、多くの組織がこの種の脆弱性を悪用した攻撃を経験しています。もちろん、単独のベンダーや特定の技術がソフトウェアの脆弱性の影響を受けないわけではありません。VPN の場合、各 CVE がセキュリティの単一障害点となる可能性があります。つまり VPN の脆弱性は、攻撃者が VPN 資産を侵害して永続性を確保し、ネットワークを水平移動してデータを盗むための足掛かりになり得るのです。このペースで VPN の CVE が公開され続ける限り、リモート接続に VPN を使用する企業は常にリスクを抱えることになります。



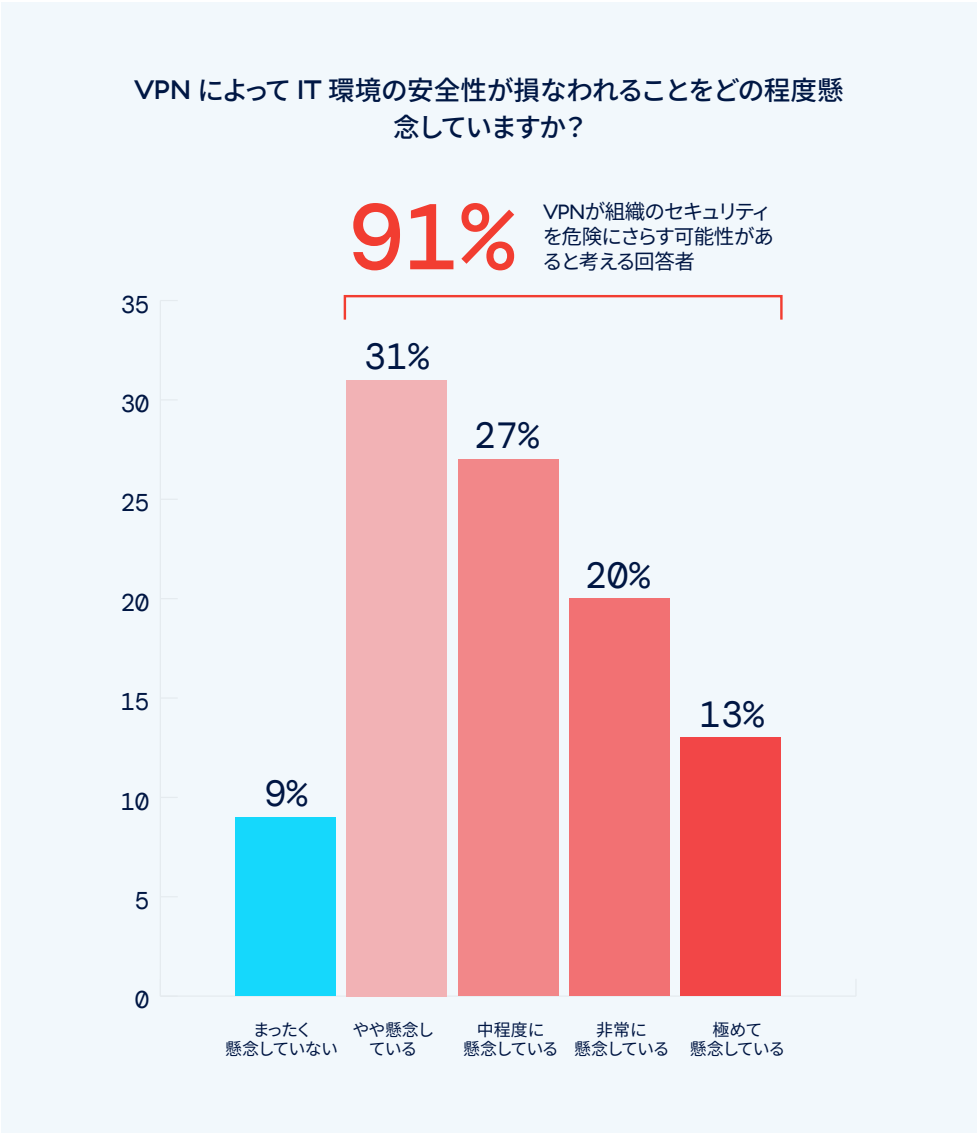
VPNセキュリティに対する懸念の高まり

今回の調査結果からも、VPN はセキュリティ リスクをもたらすという考えが浸透していることがわかり、これは VPN 技術の現在の傾向と増加する脆弱性を反映する形となっています。回答者の 91% (2023 年の 88% から大きく増加) が VPN によって IT セキュリティが危険にさらされることを懸念しており、VPN のリスクに対する意識の高まりがうかがえます。

先日、攻撃者が Ivanti VPN の重大な脆弱性を悪用してネットワークに侵入し、機密データを盗み出した攻撃が発生したため、この数字は当然の結果といえるかもしれません。CVE-2024-21888 や CVE-2024-21893 などの脆弱性を含むこれらのインシデントは、旧型やパッチ未適用の VPN インフラを使い続けることのリスクを浮き彫りにしています。さらに、VPN 固有のアーキテクチャーは、境界のない現代のデジタル環境において重大なセキュリティ リスクをもたらします。組織がクラウド サービスを導入するケースが増え、リモート ワーク モデルが進化する中で、VPN は広範なアクセス権の管理や拡大する攻撃対象領域の保護など、新たなセキュリティ上の課題に対処できなくなってきています。

こうした脆弱性やアーキテクチャー上の制限により、VPN セキュリティに対する認識が大きく変化し始めており、ゼロトラストのようなさらに動的で回復力のあるフレームワークを提唱するより幅広いサイバーセキュリティが求められるようになっています。

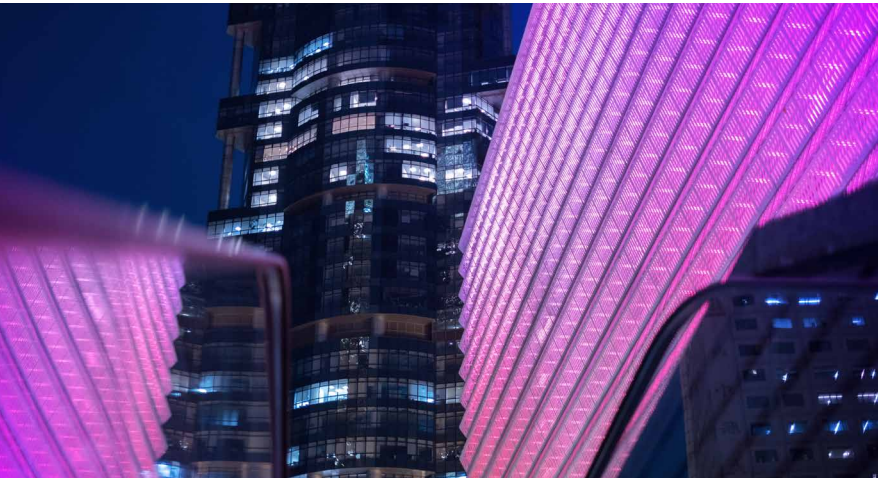
多くの組織が導入しつつあるゼロトラスト アーキテクチャーは、ネットワーク境界の中であっても、外であっても暗黙的に信頼することなく、よりきめ細かな制御を確保し、攻撃対象領域を大幅に縮小します。このような戦略を採用すれば、従来の VPN の差し迫った脆弱性に対処しながら、進化する脅威環境に適応するための事前予防的なサイバーセキュリティ アプローチに沿うことができます。

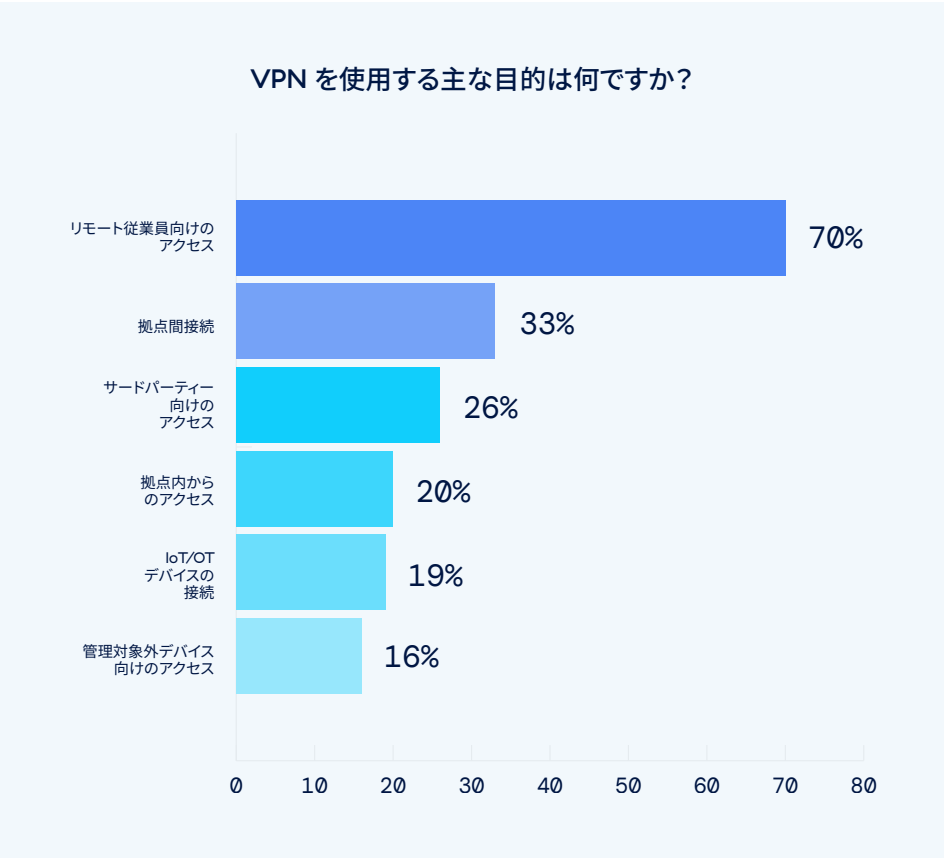


安全なアクセスが求められるユース ケース

組織で VPN を使う理由を明確にすることで、ビジネスのさまざまなシナリオにおいて、どのように安全なアクセスが優先されているのか、また、どのネットワーク ユース ケースが最もセキュリティ リスクにさらされ、より堅牢なアクセス セキュリティ戦略が必要なのかも明らかになります。

70% の組織が、主にリモート従業員のアクセスを保護するために VPN を使用しています。この広範な使用が原因で、リモート アクセスはサイバー攻撃の主な標的となっています。これに続いて 33% が拠点間接続に VPN を使用していますが、この接続が適切に保護されていない場合は攻撃経路となる可能性があるため、大きなリスクが生じます。次に挙げられたのがサードパーティー向けのアクセス (26%) で、外部関係者のセキュリティ態勢がそれぞれ異なり、セキュリティ ポリシーを制御できないため、セキュリティはさらに複雑になっています。他にも、拠点内からのアクセス (20%)、IoT/OT デバイスの接続 (19%) に VPN が使用されています。





VPN は、単純なユーザー認証で広範なネットワーク アクセスを許可するという旧式の信頼モデルに基づくため、進化し続けるサイバー脅威環境では、重要なアクセスのユース ケースにセキュリティを適切に提供できなくなっています。この広範なアクセスにより、潜在的な攻撃者が単一の侵入口を悪用してネットワーク全体を移動し、機密データを持ち出せるようになるため、組織は重大なリスクにさらされます。

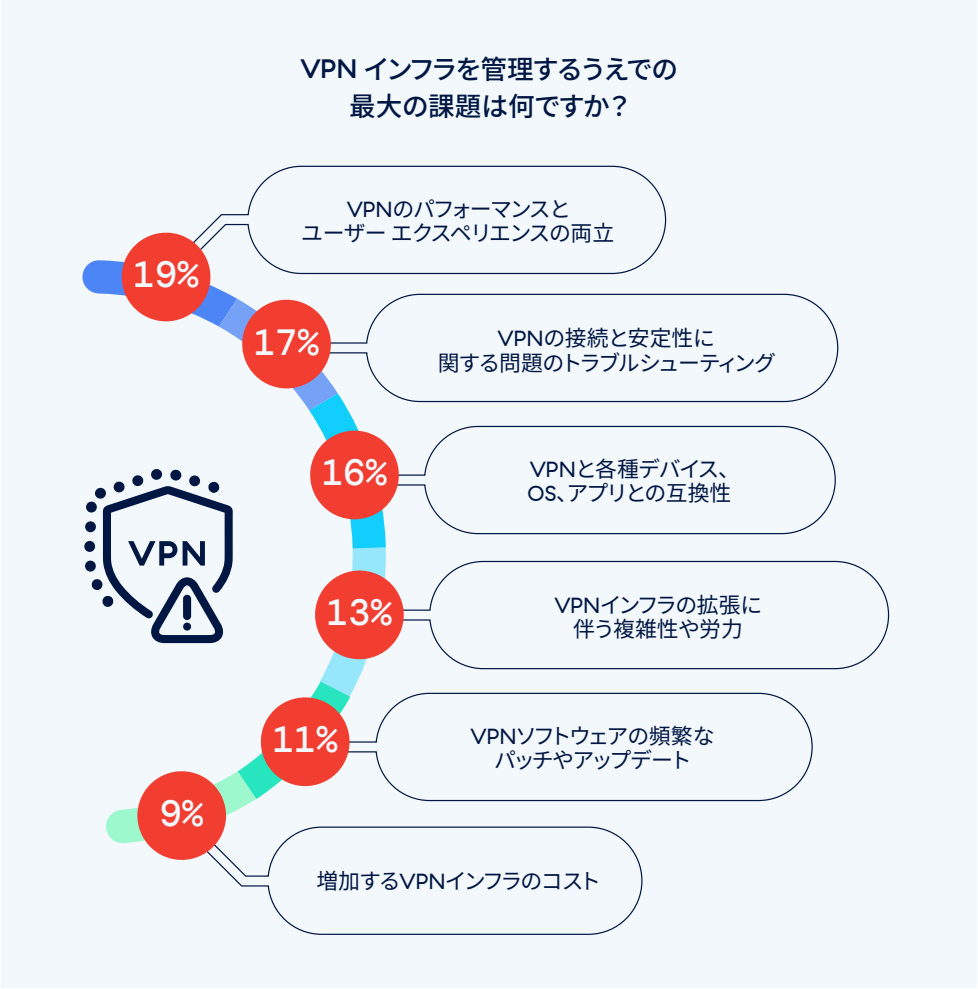
VPNの管理、パフォーマンス、ユーザー エクスペリエンス

管理上の課題

固有のセキュリティ リスクに加えて、分散したクラウド中心の作業環境では堅牢なアクセス ソリューションの要件が厳しくなるため、VPN インフラの管理は IT 部門の大きな課題となっています。IT プロフェッショナルにとっての主な管理上の課題は、VPN のパフォーマンスとユーザー エクスペリエンスの両立です (19%)。この問題は生産性に直接影響するため、非常に重要です。VPN によってネットワークの速度が低下したり、使用方法が煩雑になったりすると、従業員の満足度が低下し、ビジネス プロセスが遅くなるため、非効率的になる可能性があります。

次に多かったのが、VPN の接続と安定性に関する問題の継続的なトラブルシューティング (17%) で、これは IT 担当者の時間を浪費するだけでなく、ユーザーの混乱も招きます。また、VPN が各種デバイス、オペレーティング システム、アプリケーションと互換性がない点も課題の一つとなっており、IT プロフェッショナルの約 16% が負担に感じています。さらに、回答者の 13% が VPN インフラの拡張は複雑で、人手に依存する点を挙げており、組織の成長に伴い、ニーズが高まる中で、熟練したサイバーセキュリティ専門家の深刻な人材不足が大きな問題となっています。

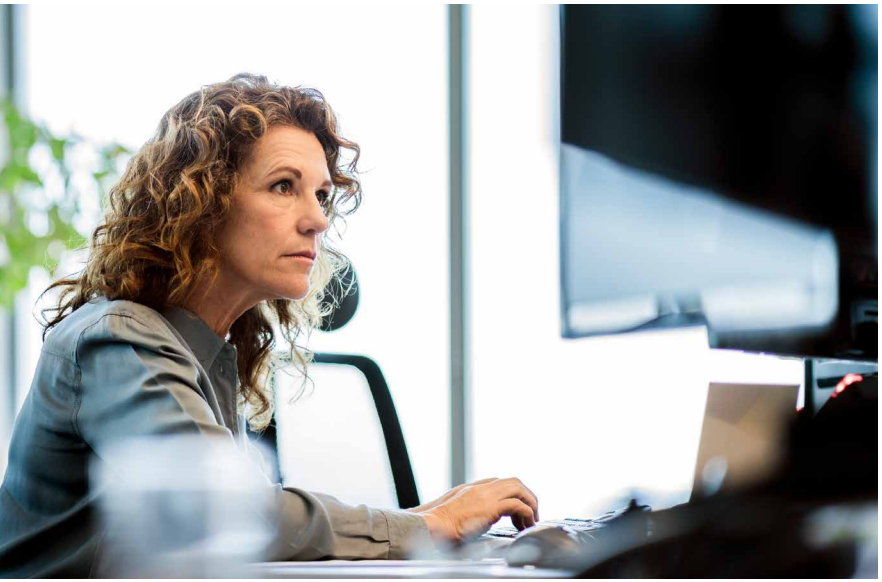
これらの洞察を考慮すると、ゼロトラスト ネットワーク アクセス (ZTNA) モデルのような、これまで以上に俊敏かつユーザーフレンドリーで、リソースをほとんど消費しない代替手段を検討する必要性は明らかです。ZTNA ではよりきめ細かな制御、スケーラビリティーの向上、管理負荷の削減が可能になるため、現代の動的なサイバーセキュリティ環境においては従来の VPN よりも優れた選択肢となります。



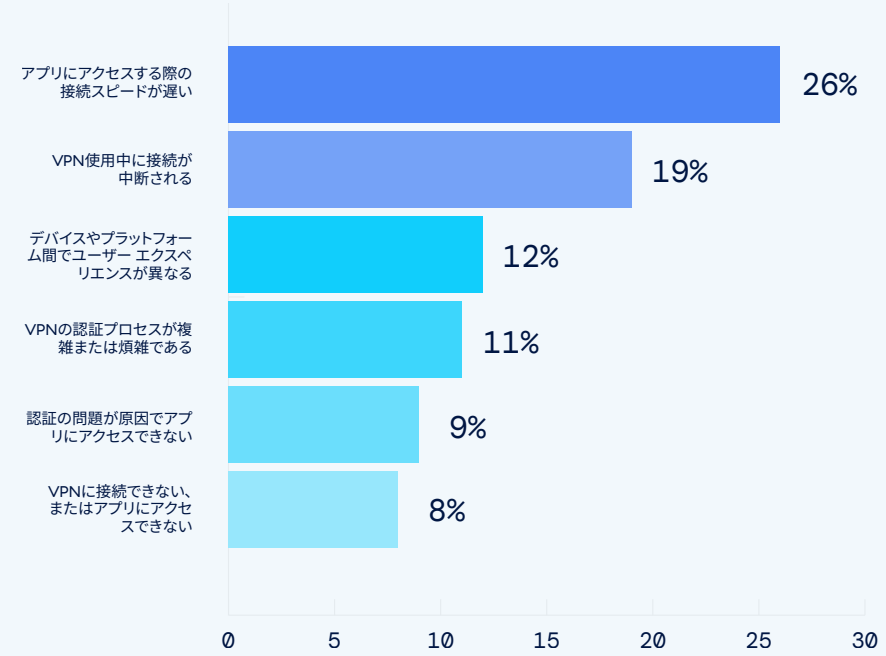
VPNユーザーが抱える一般的な課題

ユーザーが VPN を使用する際に最も不満に感じているのが、接続スピード (26%) です。特に在宅勤務の環境では、接続スピードが遅いと日常的な業務やクラウドベースのリソースへのアクセスに影響が出るため、ユーザーの生産性と満足度が大きく低下します。

次に挙げられたのが VPN 接続の切断 (19%) で、進行中の業務や通信が中断されると、ユーザー エクスペリエンスや業務の継続性に重大な問題が生じる恐れがあります。また、ユーザーの 12% がデバイスやプラットフォーム間でユーザー エクスペリエンスが異なる点を不満に感じていることからも、より安定したアクセス パフォーマンスの必要性が高まっていることがわかります。



VPN 経由でアプリにアクセスする際、ユーザーが最も不満に感じていることは何ですか？

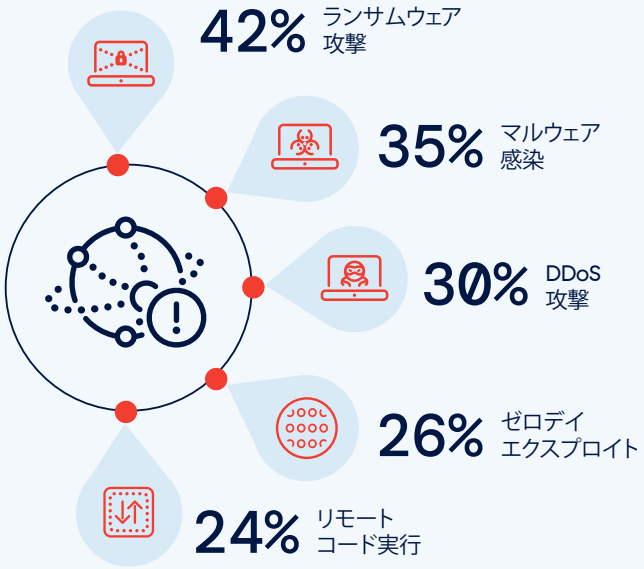


これらの課題に対処するには、さまざまなプラットフォームでより高い安定性と一貫性を確保するネットワーク アクセス ソリューションの導入を検討する必要があります。ゼロトラスト アーキテクチャーを実装すると、パフォーマンスのボトルネックを発生させることなくセキュリティを強化できるため、特に効果的です。ゼロトラスト ネットワークは接続の問題がセキュリティを低下させないようにしながら、アクセス制御を確実に施行して、さまざまなユーザー環境に適応できるようにします。

VPNの脆弱性を悪用する主な脅威

VPN の欠陥を標的としたサイバー攻撃は多様化しているため、組織はさまざまなリスクに直面しています。ランサムウェア攻撃は発生件数も多く、深刻な被害をもたらす攻撃の一つで、回答者の 42% がこの攻撃が VPN の脆弱性を悪用する可能性が高いと考えています。これに続いて、マルウェア感染 (35%)、システムの可用性、機密性、完全性を損なわせる DDoS 攻撃 (30%) が挙げられています。

組織の VPN の脆弱性を悪用する可能性が最も高いと思われる攻撃はどれですか?

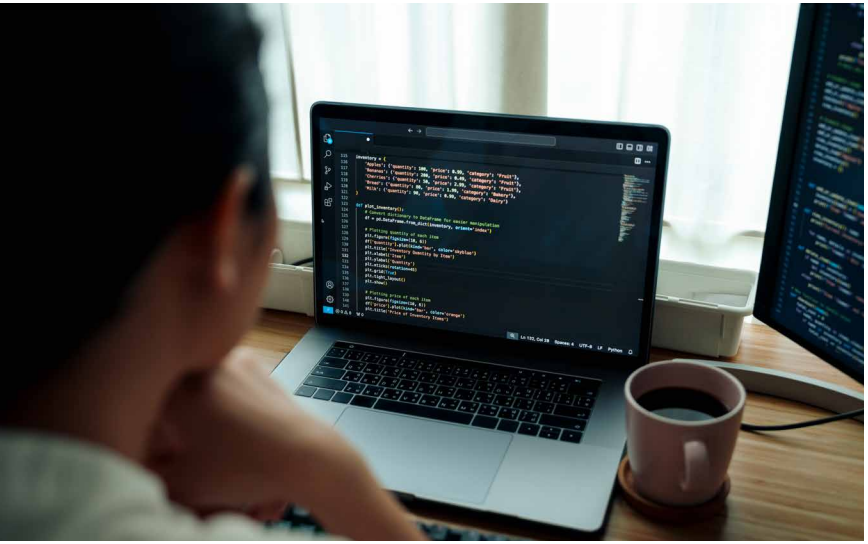


これらの脆弱性に対抗するために、ゼロトラスト モデルのような事前予防的なセキュリティ対策を採用する必要があります。ゼロトラストは発信元に関係なく、すべてのネットワーク接続に対して厳格なアクセス制御と継続的な検証を実施します。この戦略によってラテラル ムーブメントが抑制され、アクセス制御が強化されるため、VPN の弱点を突くさまざまな攻撃がもたらすリスクを効果的に軽減できます。

サードパーティーの VPNのリスク

今回の調査結果では、大多数の回答者がネットワーク セキュリティの脆弱性として、サードパーティーのVPN アクセスに深刻な懸念を示しました。回答者の 92% がこのリスクに不安を感じており、2023 年の 90% からわずかに増加しています。サードパーティーによるアクセスがサイバー脅威の侵入口となる可能性が高いという事実が、回答者の懸念を高めていると考えられます。

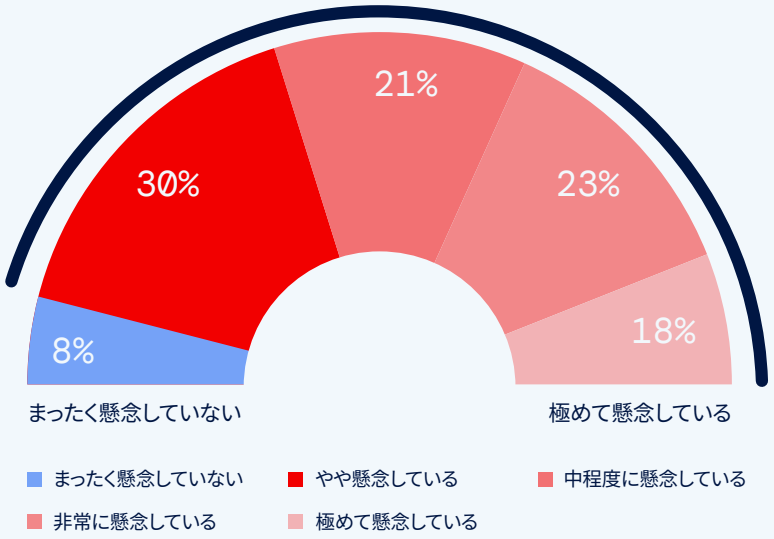
VPN の脆弱性と侵害に関する新たな洞察では、これらの懸念がさらに検証されています。従来のVPN は通常、認証情報の検証後に広範なネットワーク アクセスを提供するため、サードパーティー ベンダーのセキュリティ対策が侵害された場合にリスクが生じます。



サードパーティーの VPN アクセスがネットワークに侵入するための潜在的なバックドアとなるリスクをどの程度懸念していますか？

92%

サードパーティーのVPNアクセスがネットワークに侵入するための潜在的なバックドアとなることを懸念している回答者



組織にいま求められているのは、従来の VPN からゼロトラスト アーキテクチャーへの迅速な移行です。ゼロトラスト アーキテクチャーでは、アイデンティティーとコンテキストに基づいてアクセス要求が厳密に検証され、サードパーティー ベンダーのアクセスは業務に不可欠な特定のリソースのみに制限されます。

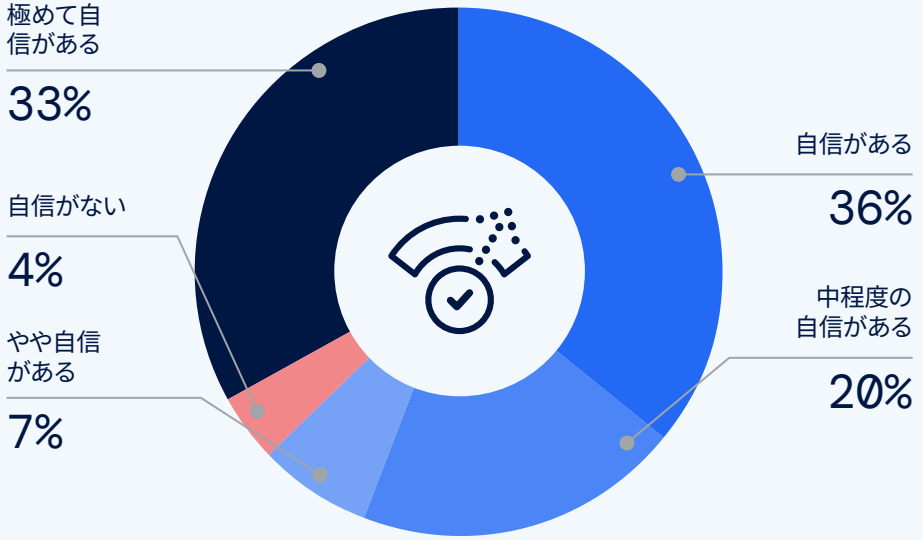
VPNインフラの
セキュリティに関する問題

VPNのセキュリティに対する過信

VPN を狙った悪質な攻撃が急増していますが、これは、一般に浸透しているセキュリティと実際のリスクとの間に乖離があるためと考えられます。十分なセキュリティ対策を講じている組織ですらも、VPN 特有の脆弱性を悪用するサイバー攻撃者の能力を過小評価する傾向にあります。69% が VPN の脆弱性に対処する自社の能力を高く評価していますが、近年見られるようなわずかな弱点を突く高度な脅威には対抗できない可能性もあります。国家支援型の脅威グループやサイバー犯罪集団が長期間パッチが適用されていないシステムを侵害するケースが頻発しているように、最近の VPN 攻撃はますます複雑化し、攻撃件数も増加の一途をたどっています。そのため、過信は特に危険です。

組織に必要なのは、厳格な脆弱性評価、頻繁なアップデート、包括的なセキュリティ意識向上トレーニングなどを取り入れ、セキュリティ態勢全般を見直すことです。VPN に過度に依存しない多層的なセキュリティ アプローチを採用することで、包括的な保護が実現します。また、このアプローチには、高度な監視、異常の検知、ゼロトラストの原則の統合が含まれている必要があります。

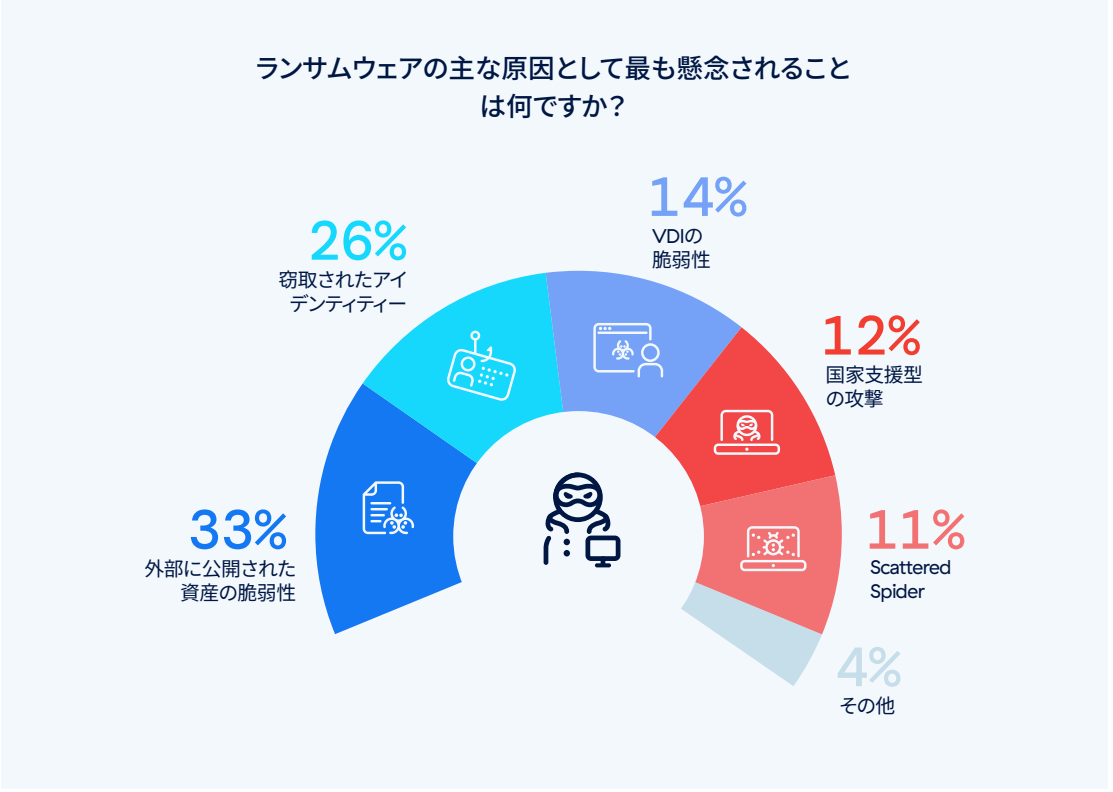
サイバーセキュリティ攻撃の原因になりかねない VPN の脆弱性を検出して軽減することについて、どの程度自信がありますか？



ランサムウェアの攻撃ベクトル

回答者の 33% がランサムウェアの潜在的な攻撃ベクトルとして、外部に公開された資産の脆弱性に懸念を示しています。これは、公開されたネットワーク サービスや Web アプリケーションに関連するリスクがランサムウェア攻撃の最初の侵入口となったインシデントが多いためと考えられます。

これに続いたのが窃取されたアイデンティティー (26%) です。攻撃者は窃取した認証情報を用いることでセキュリティ対策をすり抜け、ランサムウェアのペイロードを配信するためのアクセスを入手します。仮想デスクトップ インフラ (VDI) の脆弱性と国家支援型の攻撃への懸念はそれぞれ 14% と 12% になっており、防御しなければならないランサムウェア脅威の発生源が多岐にわたることがわかります。回答者の 11% が挙げた Scattered Spider とは、フィッシング、多要素認証疲労攻撃、SIM スワップなどの高度なソーシャル エンジニアリング戦術を使用するサイバー犯罪集団です。



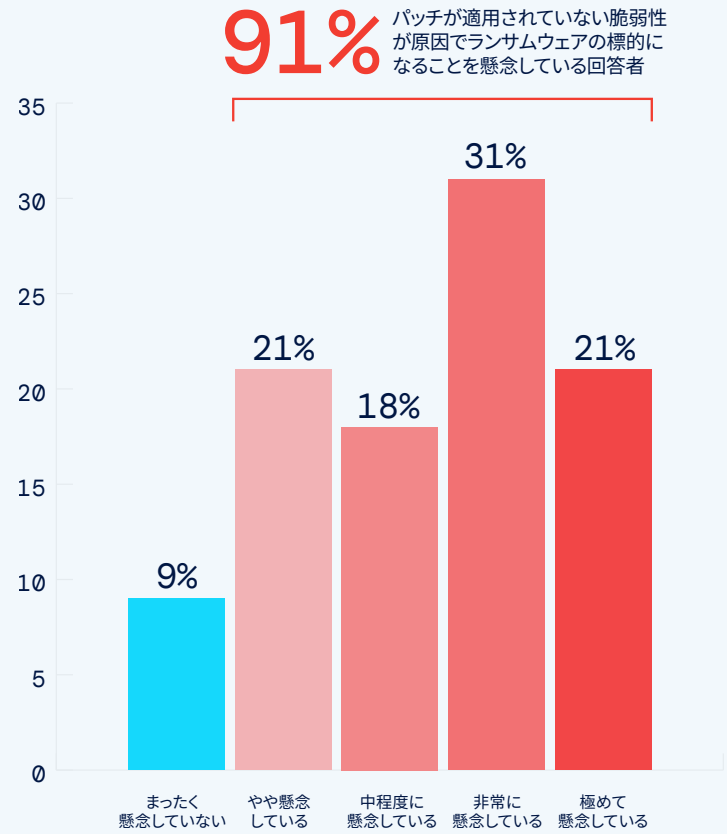
防御とアイデンティティー管理の強化は必須です。包括的な脆弱性管理プロセスを実装し、ゼロトラスト セキュリティ モデルを採用し、ネットワーク リソースへのアクセスと水平移動を阻止することで、ランサムウェア攻撃のリスクを効果的に軽減できます。

ランサムウェアへの懸念

パッチが適用されていない脆弱性が原因で、ランサムウェア攻撃を受ける可能性を非常にまたは極めて懸念している回答者は 52% となりました。パッチ未適用の脆弱性は依然としてランサムウェアの主な攻撃ベクトルであるため、これは当然の結果といえます。最近の分析からも、大多数のランサムウェア攻撃がこの種の脆弱性を悪用しており、他のサイバー攻撃よりも特に深刻な被害をもたらしていることが明らかになっています。

ランサムウェア グループはますます巧妙化しています。また、パッチを適用する前に新たに発見された脆弱性を悪用するといった高度な戦術を駆使するグループも増えています。このように攻撃サイクルのスピードはより一層早まっており、組織は重大な脆弱性に対処する時間を十分に確保できない場合があります。だからこそ、攻撃対象領域を削減する高度なセキュリティ対策を喫緊の課題として取り組む必要があります。

パッチが適用されていない脆弱性が原因でランサムウェアの標的になることをどれくらい懸念していますか？



VPN攻撃における ラテラル ムーブメント

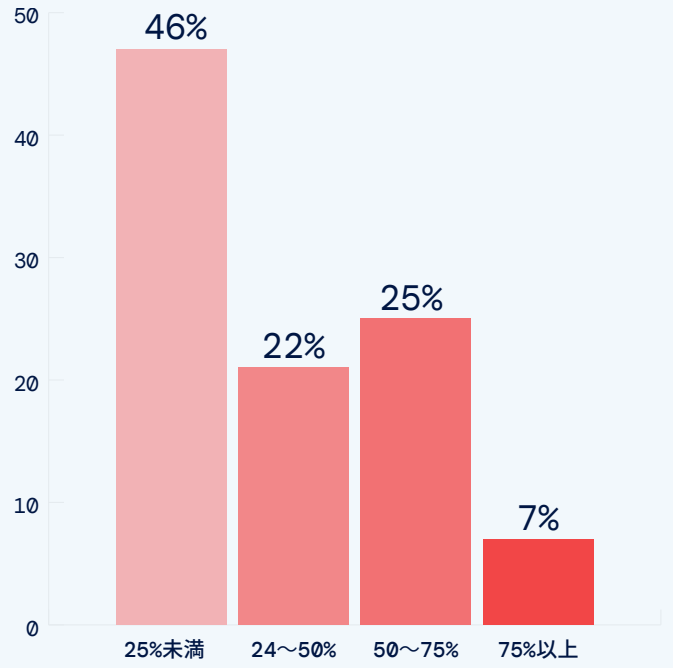
回答者の大半 (53%) が VPN 関連の攻撃の 25% 以上でラテラル ムーブメントを確認していますが、これは侵害の初期段階で適切に封じ込めが実行されなかったためです。また、攻撃の半数以上でラテラル ムーブメントを確認したのは約 3 分の 1 (32%) に上り、この数字からも、攻撃者が一度ネットワーク防御を突破すると、脅威の拡散を制御することが非常に難しくなることがわかります。

攻撃者が認証されたユーザーと同様の広範なネットワーク アクセスを入手すると、ネットワーク上を密かに移動して機密性の高い領域に狙いを定めます。そのため、VPN ではラテラル ムーブメントが重大なリスクとなります。

このように、VPN はリスクを増大させ、攻撃の範囲を最初の侵入口以外にまで拡大させます。この問題には、ゼロトラスト アーキテクチャーを介したユーザーとアプリケーション間の厳格なセグメンテーションと継続的な監視で対処する必要があります。セグメント化することで、各ユーザーがアクセスできるアプリケーションが細かく制御されると同時に、他のアプリケーションは非表示になるため、ラテラル ムーブメントの影響範囲が大幅に縮小されます。

VPN の脆弱性を悪用する攻撃はますます巧妙化しており、ゼロトラスト フレームワークへの移行の必要性がこれまで以上に高まっています。ゼロトラストは厳格なアクセス制御と継続的な検証を実施することで、不正なラテラル ムーブメントを制限し、拡大するデジタル環境全体のセキュリティを強化します。

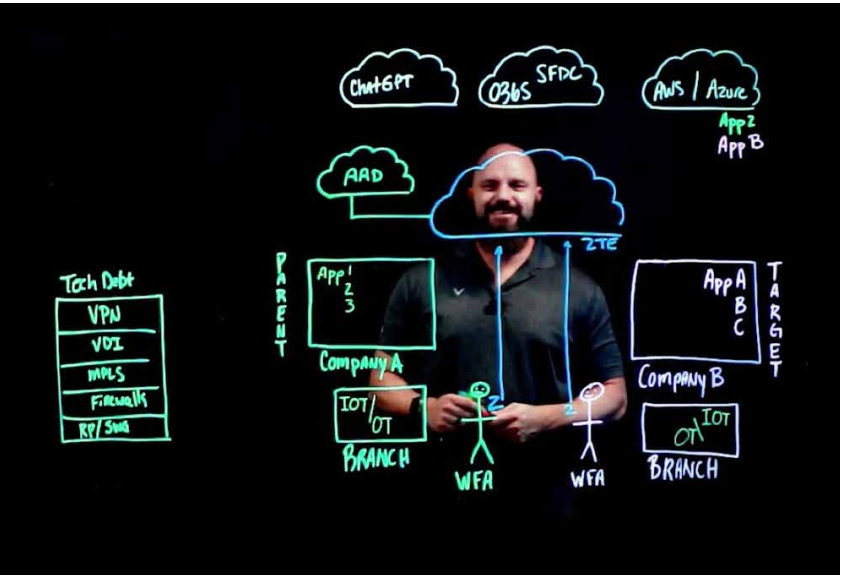
組織が受けたすべての攻撃のうち、脅威が VPN からアクセスを取得した後に水平方向に拡散した割合はどれくらいですか？



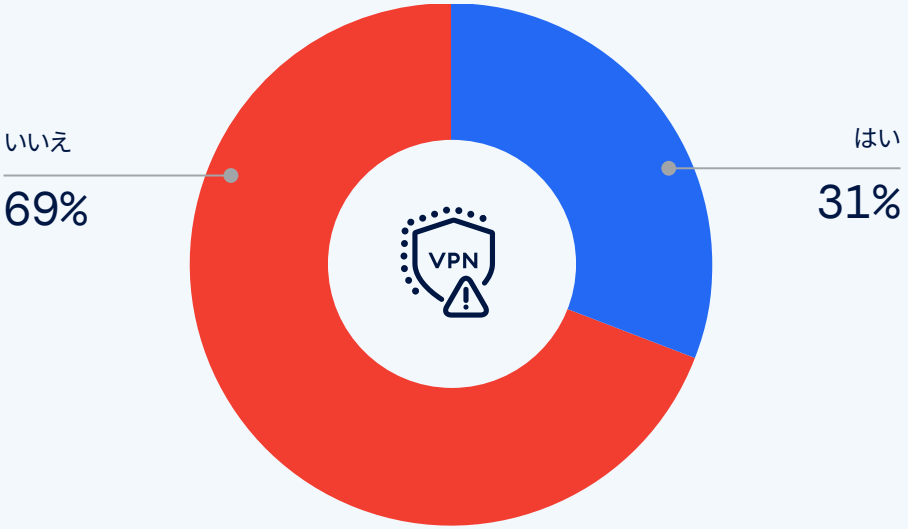
M&A後のVPNのセキュリティに対する懸念

合併と買収 (M&A) が既存の VPN インフラに与える影響を懸念する組織は少なくありません。これは、組織の変化や異なるネットワークの統合が脆弱性を生み出しかねないためです。

回答者の 69% が M&A 後のサイバー攻撃に不安を示していることからも、こうした組織変革に伴うセキュリティ リスクや、M&A 活動によって既存のセキュリティ フレームワークが不安定になり、サイバー脅威にさらされる可能性が高まるといった認識が浸透しつつあることがわかります。



現在のインフラでは、M&A 後に攻撃を受ける可能性があると思いますか？



M&A の移行期間は、脆弱な VPN 技術を段階的に廃止してゼロトラスト フレームワークを導入する絶好の機会となります。ゼロトラスト アーキテクチャーは、ユーザーとアプリケーション間、ワークロード間、拠点間、デバイス (管理対象 / 非管理対象のデバイス、IoT、OT システムなど) 間の環境を包括的にセグメント化することで、セキュリティを強化します。このアプローチでは、すべてのユーザーとデバイスの厳密な検証、包括的なセグメンテーション、最小特権アクセス制御の完全な施行を通じて、移行中および移行後のセキュリティが大幅に強化されます。

組織におけるゼロトラストの導入

加速するゼロトラストの導入

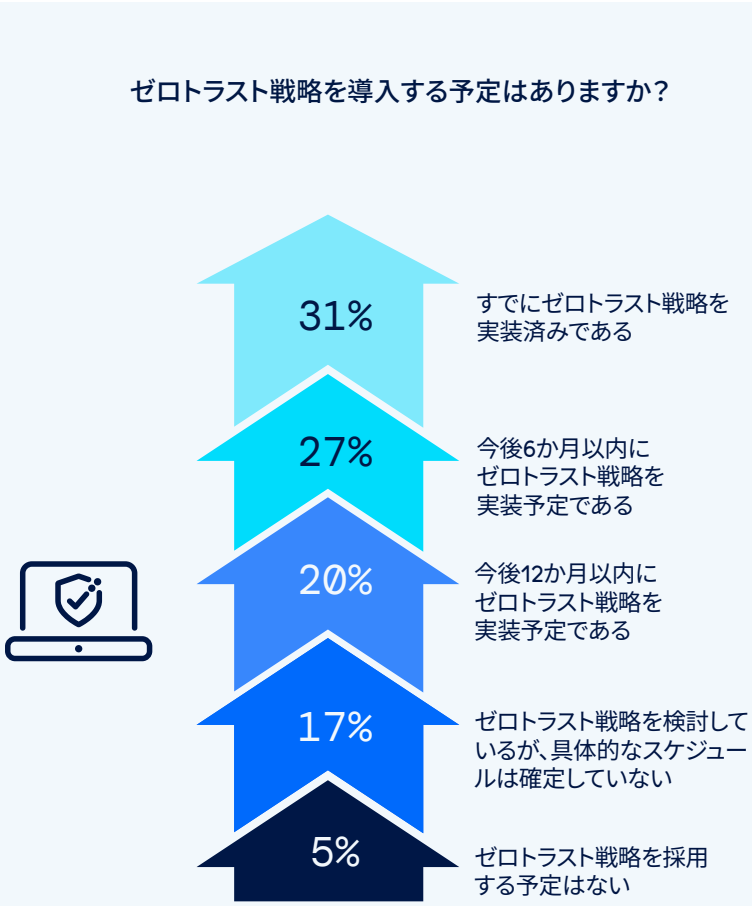
ゼロトラスト セキュリティ フレームワークは、サイバーセキュリティを強化する重要な役割として強く認識され始めていることが今回の調査からも明らかになりました。回答者の 31% がすでにゼロトラストを実装しており (2023 年の 27% から増加)、ネットワーク リソースの保護を強化するための事前予防的な取り組みが拡大しています。

また、今後 6 か月以内にゼロトラスト戦略を実装する予定の組織は 27% (2023 年の 18% から増加)、今後 12 か月以内を予定している組織は 20% となっています。回答者の 4 分の 3 以上 (78%) がゼロトラストの緊急性とメリットを認識しており、ゼロトラストに移行する取り組みを加速させています。

一方で、回答者の 17% は具体的なスケジュールを設定しないままゼロトラスト戦略を検討しており (2023 年の 23% から減少)、この背景には、移行の具体的な計画や開始に踏み切れない事情や潜在的な課題があると考えられます。ゼロトラストを導入する予定がないと回答したのはわずか 5% (2023 年の 8% から減少) で、これはおそらくリソース不足が原因です。

組織規模別の分析によると、調査対象の大規模組織、特に従業員数が 20,000 人を超える組織ではゼロトラスト戦略を導入する可能性が高く、導入も早い傾向にあり、すでに 33% がゼロトラスト戦略を導入しています。対照的に、従業員数 1,000 ～ 5,000 人の小規模組織では導入率が 29% とわずかに低く、限られた規模とリソースがゼロトラスト統合のペースと範囲に影響を与えています。

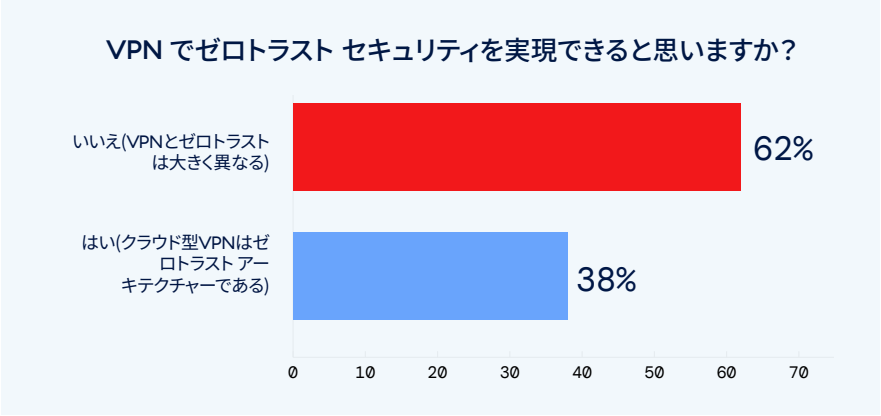
ゼロトラストの導入を決めかねている組織や計画中の組織は、まず現在のセキュリティ態勢とネットワーク アーキテクチャーを評価し、具体的なニーズと潜在的な課題を特定する必要があります。



ゼロトラスト セキュリティを実現できないVPN

調査結果から、VPN とゼロトラスト セキュリティ フレームワークの互換性に関する考え方に大きな隔たりがあることがわかりました。大多数 (62%) が VPN とゼロトラストは相反するものであり、従来の VPN アーキテクチャーはゼロトラスの原則に従っていないと考えています。これに対し、回答者の 38% は VPN、特にクラウドベースの VPN はゼロトラスト アーキテクチャーと互換性があると考えています。

一部の VPN ベンダーは、自社のクラウドベースのソリューションがゼロトラストの原則に準拠していると主張しており、これが誤った認識を生み出した可能性があります。こういった主張を批判的に精査することが重要です。例えば、クラウドで VPN サービスをホストするだけでは、ゼロトラスト属性が自動的に付与されるわけではありません。ゼロトラスト セキュリティには、安全なホスティング環境以上のものが求められます。つまり、境界ベースの防御から、セキュリティが動的かつきめ細かく、コンテキストベースであるモデルへの根本的な移行が不可欠なのです。

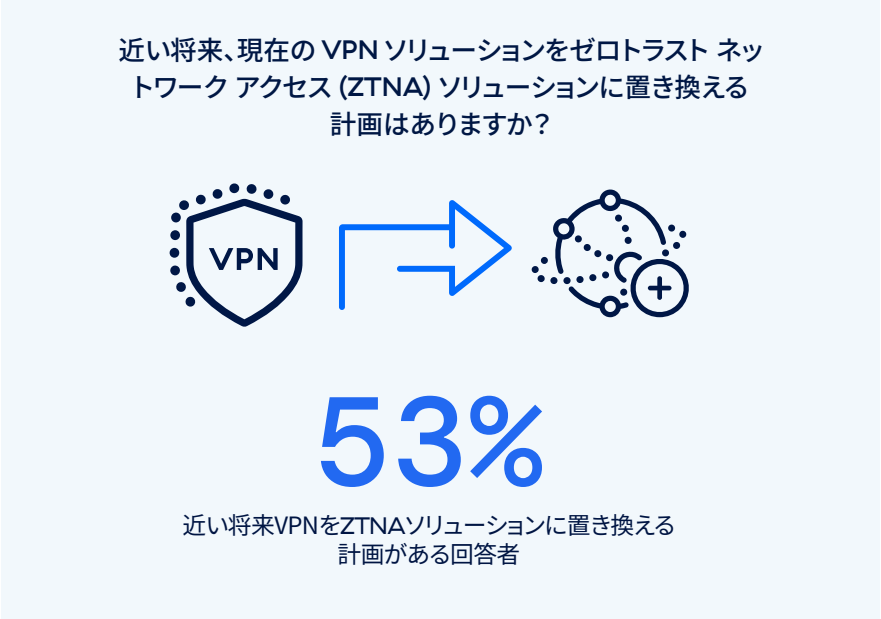


真のゼロトラスト セキュリティはすべてのユーザーとデバイスを継続的に検証して最小特権アクセスを適用し、トラフィックのセグメント化でラテラル ムーブメントを防止します。従来の VPN、そしてクラウドベースの VPN ではこれらの機能を提供できません。重要なのは、ベンダーの宣伝に惑わされることなく、「ゼロトラスト」VPN と主張する VPN が実際にこれらの基本原則を組み込んでいるかを確認することです。

VPNからゼロトラスト ネットワーク アクセスへの移行

ほとんどの組織が戦略的な転換期を迎えており、回答者の 53% が近い将来に既存の VPN ソリューションを ZTNA ソリューションに置き換える予定にしています。ZTNA はユーザーのコンテキスト、場所、デバイスのセキュリティに基づいてポリシーを施行することで、より柔軟で安全なアプローチを提供します。ネットワークの場所に基づいた信頼を前提にはしません。これは、一般的に広範なネットワーク アクセスを許可し、セキュリティ上の脆弱性を生み出す従来の VPN とは対照的です。

移行を成功させるためにも、ZTNA への移行を検討している組織の 53% は包括的なリスク評価を計画し、アクセス ポリシーを更新し、新しいソリューションについてユーザーを教育する必要があります。一方、移行を検討していない 47% の組織も、現在のセキュリティ上の課題を評価し、ZTNA が VPN よりも効果的にこれらの課題に対処できるかどうかを確認することが重要です。

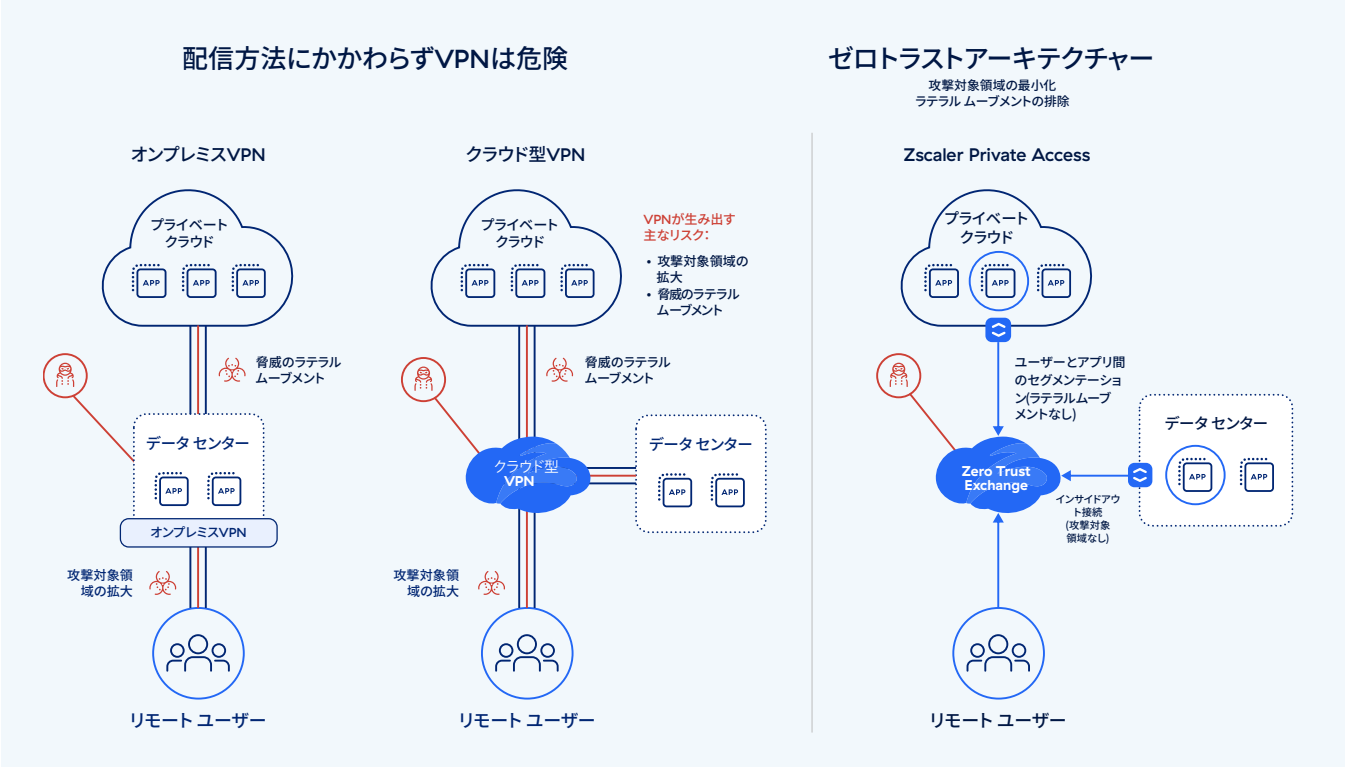


ゼロトラストがVPNよりも安全な理由

アーキテクチャーの観点からも、ゼロトラストと ZTNA は従来の VPN よりも安全です。その主な理由は、すべての接続を本質的に信頼しない堅牢なセキュリティ フレームワークレームにあります。従来の VPN ベースのアーキテクチャーは単一障害点の影響を受けやすく、例えば、VPN またはデバイスが新しい CVE などによって侵害されると、脅威アクターはフラットなネットワークの本質的な信頼を悪用してネットワーク全体にアクセスし、水平移動してデータを盗み、ランサムウェアを展開します。このため、セキュリティ専門家は VPN のセキュリティ リスクへの懸念を強めています。

オンプレミス VPN とクラウド型 VPN には、同様のセキュリティ上の脆弱性が存在します。さらに、VPN では複雑さが生じるだけでなく、ユーザーのプロビジョニング、ルート テーブルの管理、接続のトラブルシューティング、パッチの適用、監視、パフォーマンスの最適化など、不要な負荷や時間のかかる作業も発生します。

ゼロトラスト アーキテクチャーでは、あらゆる接続が信頼されません。ユーザーは基盤となるネットワークではなく、アプリケーションに直接接続されます。発信元に関係なくすべての接続を一度終了させ、7 層のゼロトラスト セキュリティ制御で検証します。ゼロトラスト アーキテクチャーは、ユーザーとアプリケーション間、ワークロード間、拠点間、IoT や OT デバイスを含むデバイス間など、きめ細かなアクセスで環境を包括的にセグメント化します。



主な違いとメリット

攻撃対象領域の大幅な縮小
ゼロトラスト アーキテクチャーは内側から外側への接続を行うことで、重要な資産、アプリケーション、サーバーなどをパブリック インターネットから隠します。VPN やファイアウォールなどの脆弱な資産が不要になるため、攻撃対象領域を大幅に縮小しながら、従業員にハイブリッドな接続を提供できるようになります。対照的に、VPN やファイアウォールをベースとしたアーキテクチャーでは、増加する接続に対応するために攻撃対象領域を拡張する必要があります。

継続的な検証
ゼロトラスト モデルはアクセスを許可する前に、認証情報とセキュリティ態勢に対するセキュリティ検証を継続的に実施します。こうすることで、不正なエンティティーが機密情報やシステムへのアクセスを入手して、維持することがはるかに困難になります。一方、VPN ではアクセスが一度許可されると、ユーザーやデバイスはネットワーク リソースに広範囲にアクセスできるようになります。

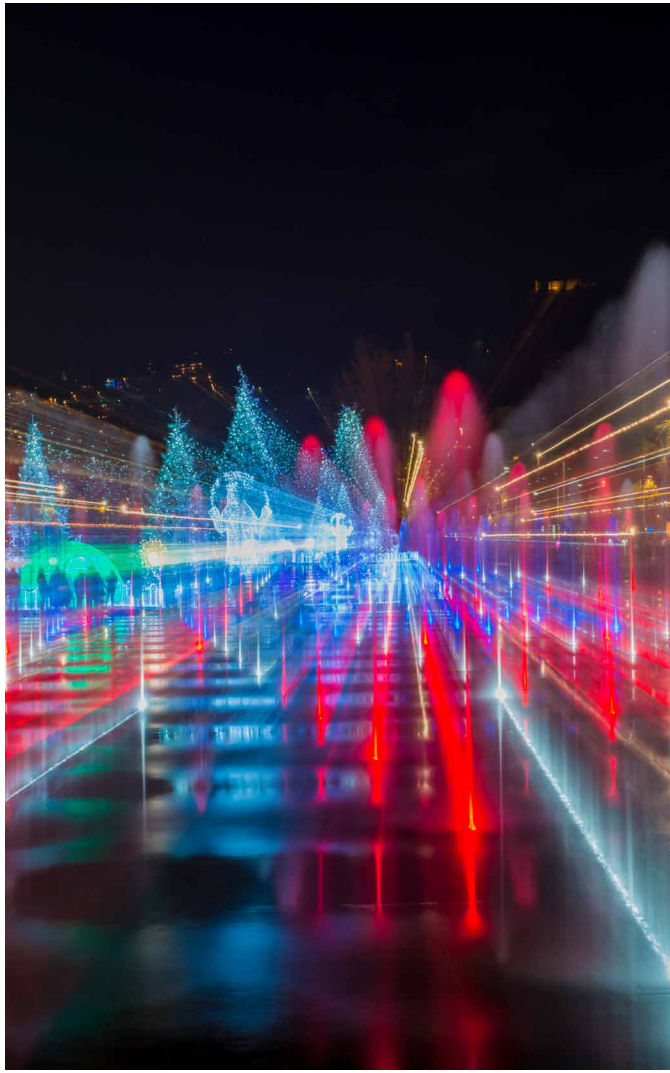
最小特権アクセス
ゼロトラストの原則は、最小特権アクセス ポリシーを施行して、ユーザーやデバイスが必要なリソースのみにアクセスできるようにします。これにより、VPN 設定の一般的な脆弱性である、ネットワーク内の内部脅威やラテラル ムーブメントのリスクが最小限に抑えられます。

きめ細かなアクセスとセグメンテーション
ゼロトラストはネットワーク リソースをユーザーとアプリ間、ワークロード間、デバイス間で個別のセグメントに分割し、潜在的な侵害をより小さな領域に隔離することで、攻撃の影響を大幅に軽減します。ネットワーク環境をセグメント化しようとする組織は少なくありませんが、これは運用上複雑で、コストのかかるプロセスが伴うため、実際には不完全なままになるケースがほとんどです。また、個別に数百ものファイアウォール ルールが必要になり、認証されたユーザーに広範なネットワーク領域が公開されることになります。

現代のハイブリッド ワーカーを強力にサポート
ゼロトラストにより、本社や支店、サードパーティーのパートナーに加えて、リモート ユーザー全体にプライベート アプリケーションへの超高速アクセスを簡単に拡張できます。

ユーザー エクスペリエンスの向上と複雑さの軽減
VPN では、すべてのリモート トラフィックを中央のネットワーク ポイントを経由させてルーティングする必要がありますが、これがパフォーマンスを低下させる主な原因の一つとなっています。ゼロトラストはこうしたプロセスを排除することで、ユーザー エクスペリエンスを向上させます。また、このアーキテクチャーは、IoT や BYOD ポリシーを含む最新のネットワークの拡張要件をより適切に処理するほか、セキュリティ制御を自動化し、ネットワーク全体でのセキュリティ ポリシーの施行を簡素化することで、管理負荷を削減します。

このように、ゼロトラストにはさまざまなアーキテクチャー上のメリットがあり、特に巧妙化および分散化する現代の脅威環境においては、従来の VPN に代わる重要な選択肢となります。サイバーセキュリティ防御の強化を目指す組織は、ゼロトラスト アプローチを採用することで、より堅牢で柔軟な拡張性の高いセキュリティ インフラを実現できます。



2024年以降のVPNに関する予測

1 深刻な VPN の脆弱性とそれを悪用した攻撃が増加する

過去 1 年間に公開された VPN の脆弱性の件数、重大度、規模を考えると、この傾向は今後も続くと考えられます。脅威アクターとセキュリティの研究者は、VPN 製品における重大な脆弱性のリスクが高まっていることを認識しており、積極的に新たな脆弱性を探しています。そのため、今後数か月から数年の間に、CVE がさらに追加される可能性があります。

2 VPN が引き起こす深刻な攻撃が社会の注目を集める

これは最初の予測と密接に関連していますが、VPN の脆弱性が悪用された結果、より多くの大規模組織が侵害を公表するようになると予測されます。その一因となるのが、深刻な影響を与えるセキュリティ侵害の詳細の開示を上場企業に義務付ける SEC の新たな規則ガイドラインです。これまで見てきたように、脅威アクターは VPN の脆弱性が明らかになると、一貫して標的の環境にバックドアを作成し、脆弱性にパッチが適用された後でも、後日それを悪用できるようにします。年が経つにつれて、こうした事例が SEC の公開資料でさらに多く開示され、ニュースで取り上げられると考えられます。

3 AI を活用した VPN サービスの急増により、セキュリティとプライバシーへの懸念が高まる

AI の進化に伴い、AI を活用した VPN ソリューションが市場に並ぶようになると予測されます。ただし、組織はこれらの製品を慎重に評価する必要があります。AI の統合によってパフォーマンスは向上するものの、セキュリティ リスクが増大し、攻撃者が VPN の脆弱性を悪用する機会が増える恐れがあります。さらに、機密情報が漏洩するリスクを高める広範なデータ分析により、プライバシーの懸念も生じます。

4 VPN に対するパスワードスプレー攻撃は今後も増え続ける

攻撃者はパスワードスプレー攻撃を通じて、脆弱なパスワード管理方法やデフォルトの VPN 接続プロファイルを悪用する方法をさらに見つけるようになると考えられます。これらの攻撃では、脅威アクターはログインに成功するまで多くの VPN アカウントで同じパスワードを試し、不正にアクセスしようとします。昨今の深刻な VPN 侵害でもこの手法が効果的に悪用されているため、同様の攻撃が続くと予測されます。

5 組織の支出は VPN からゼロトラスト接続へと移行する

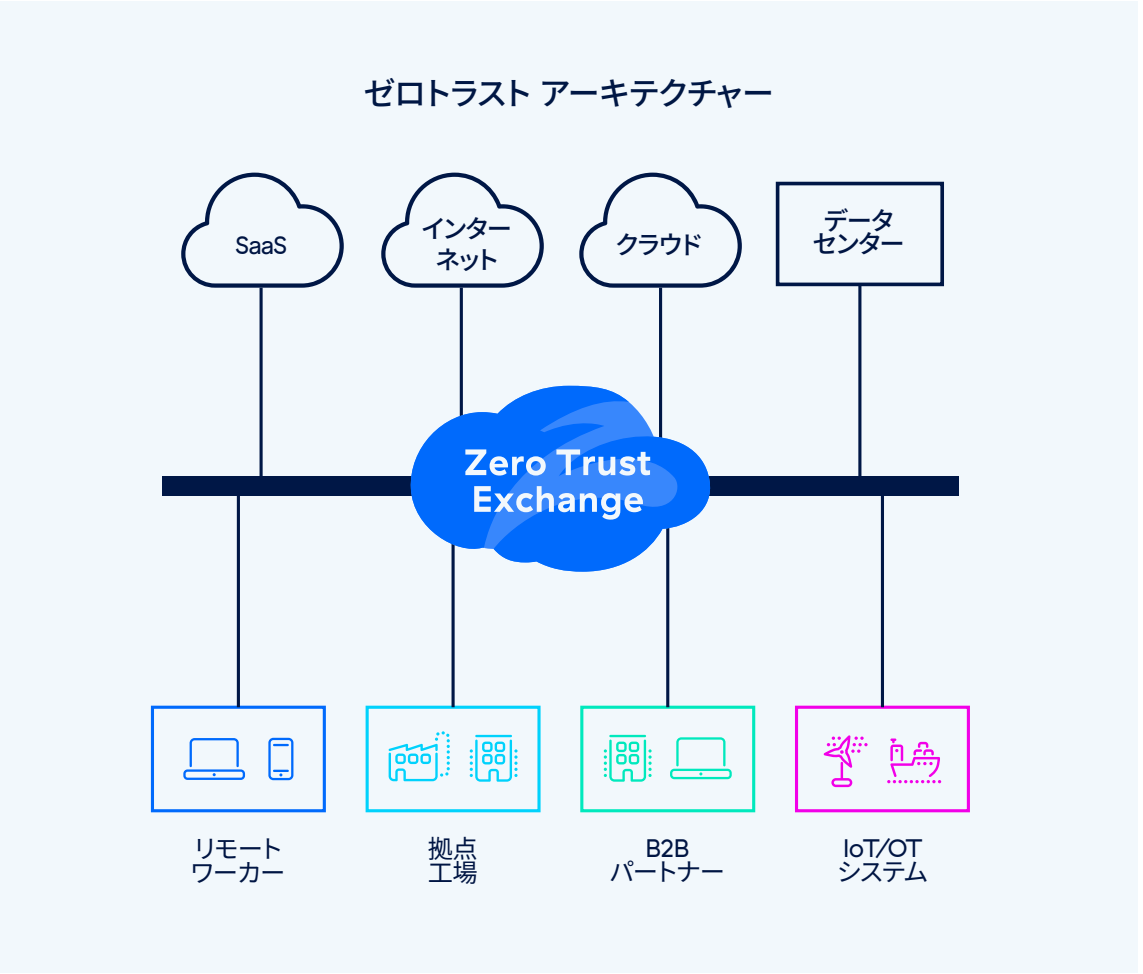
VPN は長年にわたって、リモート接続のために使用されてきましたが、この技術が抱えるセキュリティ上の課題は一貫して増大しており、長期的な支出を正当化することがますます困難になっています。セキュリティと接続のための推奨アーキテクチャーとして、ゼロトラストが重要な立ち位置を担うにつれて、組織はリモート ワーカーのセキュリティを確保するために、ゼロトラスト戦略に予算をかけるようになると予測されます。

Zscalerで脱VPNとゼロトラスト トランスフォーメーションを実現

従来のファイアウォールや VPN は大規模な攻撃対象領域を生み出すため、脅威アクターは簡単に公開されたリソースを見つけ出し、悪用することができます。同時に、ユーザーをネットワークに接続させ、そのネットワークにホストされているアプリケーションすべてにアクセスできるようにするため、攻撃者が機密データにアクセスしやすい環境を生み出します。また、こうした旧式のアプローチを使って、サードパーティーのベンダーや請負業者、代理店に安全にアクセスを提供したり、リソースを共有したりするには、多大な労力と時間が必要になるばかりか、コストや複雑さも増大し、現代のハイブリッド ワーカーに十分なスピードでサービスを提供できません。

世界最大のインライン セキュリティ クラウドである Zscaler Zero Trust Exchange™ プラットフォームは、ネットワーク アクセスを拡張することなく、ユーザー、ワークロード、IoT/OT、B2B パートナーを安全に接続させます。

Zero Trust Exchange の中核の一つである Zscaler Private Access™ (ZPA™) は、Zero Trust Exchange の背後に隠されたプライベート　アプリケーションへの直接アクセスを確保し、攻撃対象領域を最小限に抑え、ユーザーとアプリ間に 1 対 1 のきめ細かなセグメンテーションを提供します。また、ラテラル ムーブメントを排除し、プライベート アプリの保護とインラインのトラフィック検査を提供しながら、ゼロデイ脅威を阻止し、セキュリティ態勢を強化します。クラウド ネイティブ サービスである ZPA は数時間で展開でき、VPN や VDI などの従来のリモート アクセス ツールを置き換えることができます。



ゼロトラスト ネットワーク

ZPA では、プライベート アプリケーションとワークロードへの内側から外側への接続により、きめ細かくセグメント化されたアクセスが可能になります。他にも、AI を活用したユーザーとアプリ間のセグメンテーション (ユーザーのアクセス ポリシーと Application Segment の自動推奨機能付き)、ワークロード間のセグメンテーション、特権リモート アクセス、Private Service Edge、ブラウザー アクセスなど、包括的なアクセス制御サービスが含まれています。

サイバー脅威対策

ZPA は、さまざまな機能を備えた高度なサイバー脅威対策を提供します。この機能には、インライン セキュリティ検査を実行して一般的なアプリ攻撃やゼロデイ脆弱性を阻止するアプリ保護機能やデコイ アプリで攻撃者をおびき寄せ、高度な脅威を簡単に検出するデセプション テクノロジーなどが含まれます。

データ保護

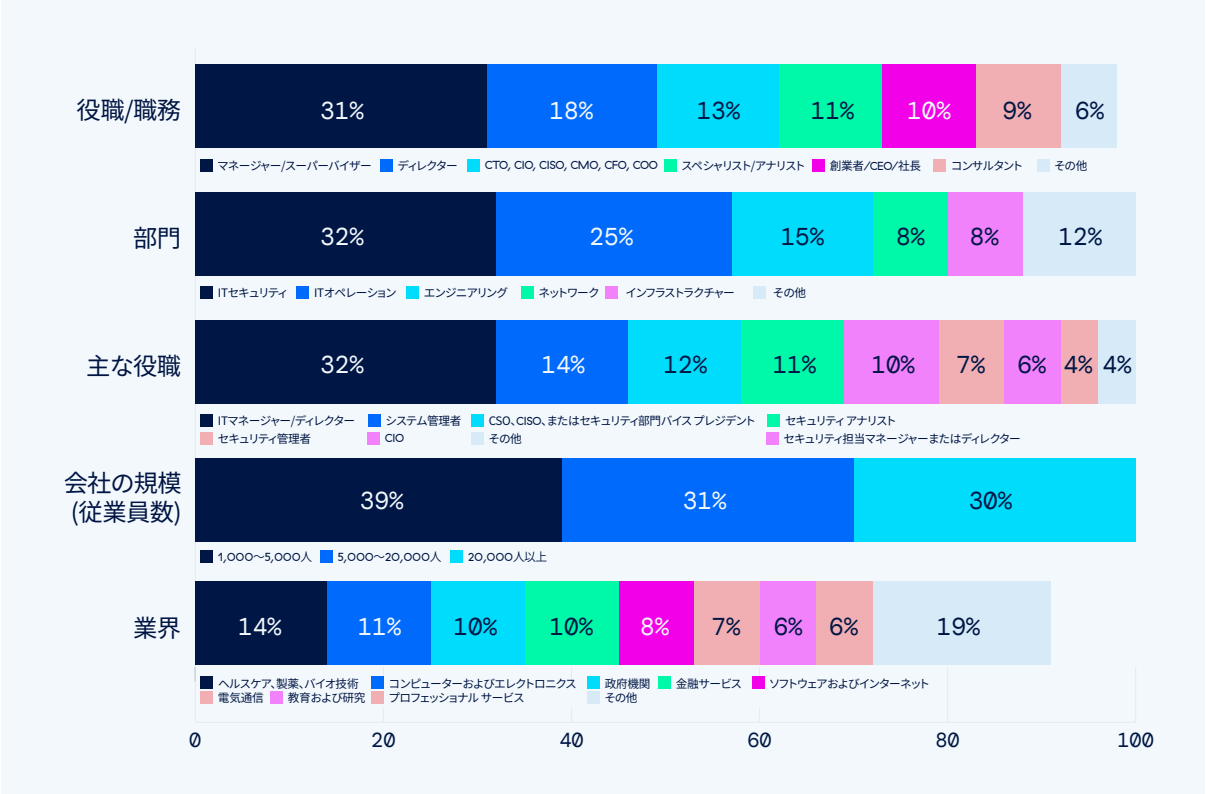
ZPA は、Web 情報漏洩防止 (DLP)、エンドポイント DLP、脆弱なユーザーや BYOD のエンドポイントのデータ漏洩を防ぐブラウザー分離などを活用して包括的なデータ保護を実現し、すべてのチャネルでデータ流出を防止します。

VPNのリスクに対抗するための ベスト プラクティス

- **攻撃対象領域の最小化：**アプリケーションへの直接アクセスを提供し、アプリとユーザーの両方がインターネットから見えなくなるようにすることで、攻撃者がそれらを発見して初期アクセスに悪用することを防止します。
- **初期侵害の防止：**すべてのトラフィックをインラインで検査し、ゼロデイ エクスプロイト、マルウェア、その他の高度な脅威を自動的に阻止します。
- **不正アクセスのブロック:**ワンタイム パスワードやトークン、生体認証、FIDO2 認証情報などの強力な多要素認証 (MFA) を使用して、ユーザーのアクセス要求を検証します。セキュリティ強度の弱い MFA では通常、パスワード リセットの質問が使用されます。
- **最小特権アクセスの施行：**アイデンティティーとコンテキストに基づいてユーザー、トラフィック、システム、アプリケーションへのアクセスを制限し、許可されたユーザーのみが指定のリソースにアクセスできるようにします。MFA が侵害されたり、認証情報が盗まれたりした場合は、追加のセキュリティを提供します。
- **ラテラル ムーブメントの排除：**ユーザーをネットワークではなくアプリに直接接続させることで、潜在的なインシデントの影響範囲を制限し、脅威のラテラル ムーブメントのリスクを軽減します。
- **侵害されたユーザーと内部脅威の検知：**インライン検査と監視を有効にして、ネットワーク、プライベート アプリケーション、データにアクセスする侵害されたユーザーを検知します。
- **情報漏洩の阻止：**攻撃中のデータの持ち出しを阻止するために、転送中データと保存データを検査します。
- **アクティブ ディフェンスの導入：**デコイを活用するデセプション テクノロジーを駆使して脅威ハンティングを毎日実行し、攻撃者をリアルタイムであぶり出します。
- **セキュリティ態勢の確認：**サードパーティーによる定期的なリスク評価やパープル チームの活動を実施して、セキュリティ プログラムのギャップを特定、強化します。サービス プロバイダーやテクノロジー パートナーにも同様の措置を講じ、これらのレポートをセキュリティ部門と共有させることが重要です。

調査方法と回答者の内訳

本レポートは、各組織の VPN のリスクに関連した最新の導入傾向、課題、ギャップ、検討中のソリューションを特定するために、IT およびサイバーセキュリティの専門家 647 人を対象に実施したオンライン調査 (2024 年 4 月実施) の結果に基づいています。回答者は、技術系幹部から IT セキュリティの実務担当者まで、さまざまな業界や規模の組織から選定されています。



Zscalerについて

Zscaler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、www.zscaler.jpをご覧ください。

ThreatLabzについて

ThreatLabzは、Zscalerが誇る世界トップクラスのセキュリティ調査部門であり、Zscalerのプラットフォームを使用する世界中の組織が常に保護された状態にあることを保証する責任を担います。ThreatLabzのメンバーは、マルウェアの調査や振る舞い分析に加え、Zscalerのプラットフォームの高度な脅威対策を実現するための新しいプロトタイプ モジュールの研究開発も進めています。また、定期的に社内のセキュリティ監査を実施して、Zscalerの製品とインフラがセキュリティ コンプライアンス基準を満たしていることを確認します。ThreatLabzは、新たな脅威に関する詳細な分析を定期的にポータル(research.zscaler.jp)で公開しています。

Cybersecurity Insidersについて

Cybersecurity Insiders には、 60 万人以上の IT セキュリティ専門家と世界トップクラスのテクノロジー ベンダーが結集し、 今日の最も重要なサイバーセキュリティの課題に取り組む際のスマートな問題解決とコラボレーションを促進します。

独自のコンテンツの作成とキュレーションに重点を置くことで、最新のサイバーセキュリティの傾向、ソリューション、ベスト プラクティスについてサイバーセキュリティの専門家に有益な情報を提供します。総合的な調査研究や公平な製品レビューから、実用的なeガイド、充実したウェビナー、教育関連記事まで、サイバーセキュリティが抱える複雑な課題に対するエビデンスベースの回答を与えるリソースの提供に努めています。

Cybersecurity Insidersは、競争の激しい市場で存在感を確立させ、需要やブランド認知度、ソート リーダーシップを高められるようサポートします。
詳細をご希望の場合は、info@cybersecurity-insiders.com までお問い合わせいただくか、cybersecurity-insiders.comを参照してください。

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、**www.zscaler.jp** をご覧ください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp