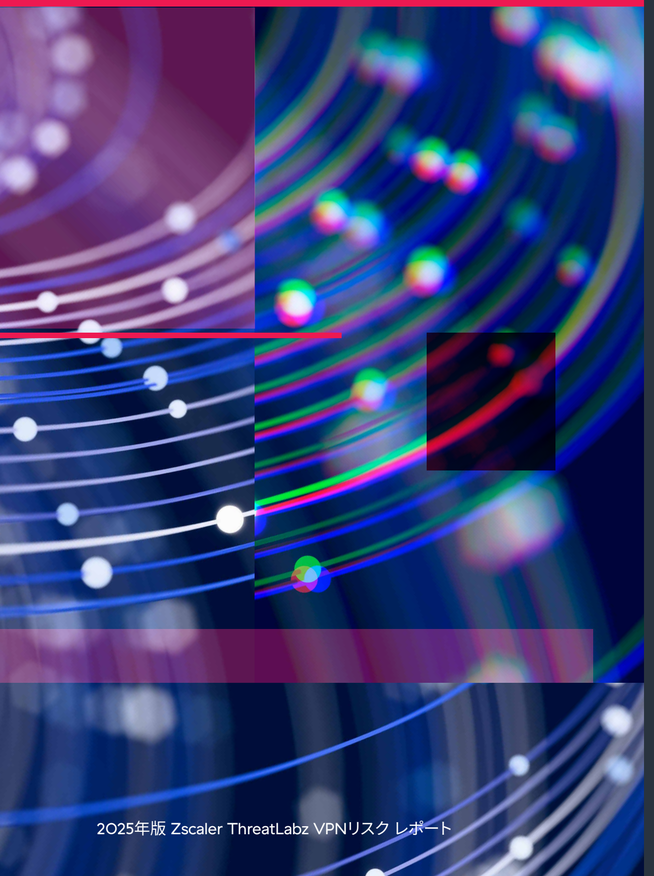
Cybersecurity INSIDERS

2025 年版 Zscaler ThreatLabz VPN リスク レポート

目次



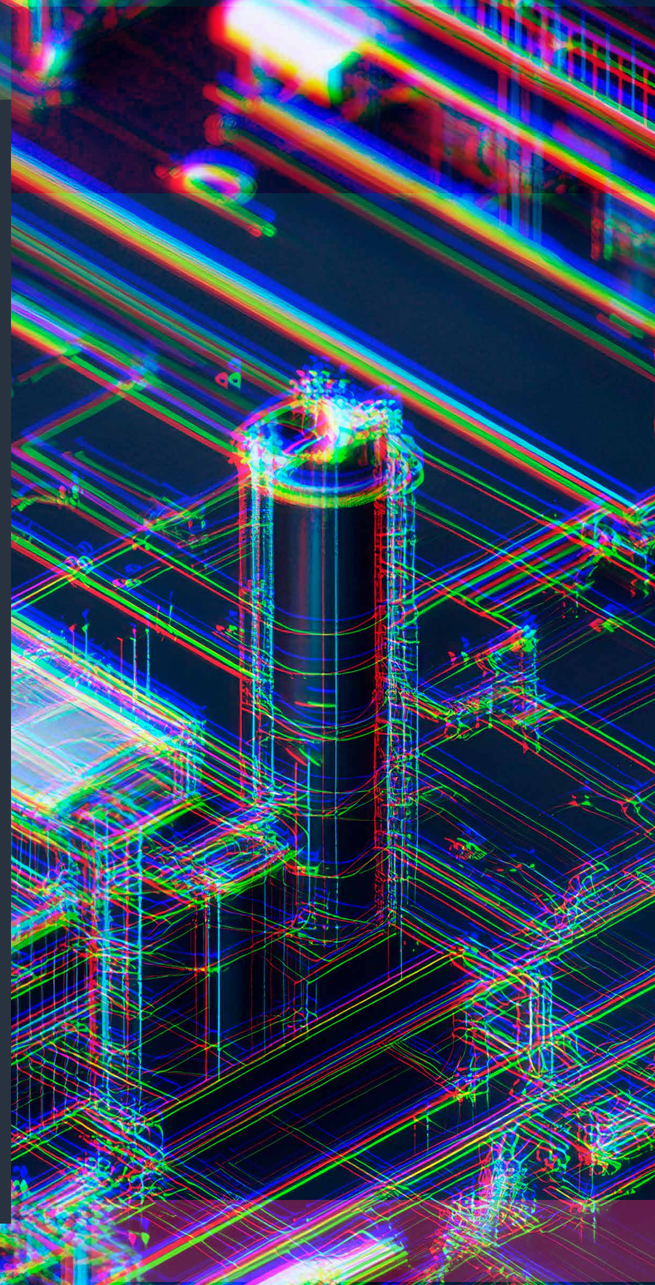
本書の要旨

2025年版 Zscaler ThreatLabz VPNリスク レポートでは、仮想プライベート ネットワーク(VPN)のリスクがどのように進化しているかを分析するとともに、未来に対応できるセキュリティを実現するために、ゼロトラスト アーキテクチャーへの迅速な移行が必要である理由を解説します。かつてはリモート アクセスの柱として重宝されたVPNですが、今ではサイバー攻撃の主なターゲットとなっており、その役割は不可欠なツールから深刻なセキュリティリスクへと変化しています。このレポートは、600人以上のITやセキュリティの専門家から得た洞察を基に、サイバーセキュリティが重要な転換点を迎えている現状を明らかにします。調査対象となった組織の半数以上が過去1年間にVPNの脆弱性を悪用した攻撃を受けており、現代のハイブリッド ワーク環境に対応できる新たなセキュリティ対策の実装が喫緊の課題となっています。

2025年には、従来のVPNに対する不満を背景に、繰り返し発生するVPNの脆弱性への対応はもはや現実的ではないと考える組織が圧倒的多数を占めるようになりました。この状況が、きめ細かなアクセス制御を提供し、セキュリティ リスクを大幅に軽減するゼロトラスト モデルの導入を加速させています。注目すべき点として、81%の組織が2026年までにゼロトラスト戦略を導入し、そのうち65%が同時期にVPNを完全廃止する計画を立てています。また、接続の遅延や頻繁な切断、複雑な認証プロセスといった運用上の課題がこれらの取り組みをさらに後押ししており、シームレスで安全なアクセスを提供するゼロトラスト ソリューションへの移行が急速に進んでいます。

これらの変化はすべて、AIによって高度化した脅威環境の中で起こっています。AIを悪用したサイバー攻撃の台頭は、VPNのセキュリティにこれまで以上の影響を与える恐れがあります。攻撃者は、パブリック インターネット上でVPNの脆弱性をスキャンするプロセスを自動化するために、AIをますます利用するようになると予測されます。巧妙なパスワード スプレー攻撃やエクスプロイトの迅速な開発などの戦術により、攻撃者はVPNの認証情報をより大規模に侵害できるようになります。攻撃チェーンの次の段階でもAIを悪用した回避技術が使われ、VPN経由の侵入の検出が一層困難になり、被害が拡大する可能性があります。このようなAIを悪用した脅威が増大するにつれて、VPNのリスクも高まり続けています。そのため、多くの組織が予防的なセキュリティ対策を導入し、ゼロトラスト ソリューションへの移行を加速させる動きを強めています。

こうした変化を踏まえ、ThreatLabzのレポートは、VPNが必要不可欠なツールからリスクへと変わりつつある現状を解説するとともに、組織がこの転換に対応するための実用的な洞察を提供します。



主な
調査結果

1. VPN の旧式化が加速：

今後 1 年以内に VPN サービスから移行する予定の組織は 65% にも上り、この割合は 2024 年から 23% 増加しています。こうした傾向の背景には、VPN が現代の組織が求めるセキュリティやコンプライアンスの要件を満たせず、実際はリスクを悪化させる一因となっているという現状があります。

2. VPN を悪用したサイバー攻撃とランサムウェアの懸念が深刻化：

過去 1 年間で VPN の脆弱性に起因するサイバー攻撃が急増し、56% の企業が被害を報告しています。これは以前の数値と比べて大幅な増加であり、92% の回答者が未修正の VPN の脆弱性からランサムウェア攻撃が発生する可能性を懸念しています。脆弱性への迅速な対応に苦戦している組織は、強力なセキュリティ対策を導入し、重大なセキュリティ ギャップを解消しながら、VPN が悪用されるリスクを軽減する必要があります。

3. エンドユーザーの不満がセキュリティ戦略の見直しを加速：

VPN の遅い接続スピードや複雑で手間のかかる認証プロセスなどに対するエンドユーザーの不満が、既存のセキュリティ戦略を見直すきっかけとなっています。こうした不満を解消するために、多くの組織が途切れることなく安全なアクセスを提供し、VPN 特有の煩わしさを解消できるゼロトラスト アーキテクチャーへの移行を加速させています。

4. 概念から現実へと転換した VPN からゼロトラストへの移行：

81% の組織が次年度中にゼロトラスト フレームワークの導入を進める予定であり、セキュリティ戦略において大きな転換期を迎えています。ゼロトラストはもはや理論的な理想ではなく、VPN に代わる現実的な解決策として認識されるようになっており、変化の激しい IT 環境でセキュリティを強化するための必須の選択肢となりつつあります。

VPN のリスク：組織の 81% が 2026 年までにゼロトラストに移行する理由

VPNはリモート アクセスを提供する目的で設計されましたが、時代とともに攻撃者の手法も変化しています。VPNの脆弱性はすぐに修正できない場合が多く、またその仕組み上、暗黙の信頼モデルに基づいてネットワークへのフルアクセスを許可するため、現在ではランサムウェア攻撃、認証情報の窃取、サイバー スパイ活動の入口となっています。調査によると、**VPNを利用する組織の最大の課題はセキュリティの脆弱性(回答者の54%)**となっており、攻撃者が未修正の欠陥を日常的に悪用したり、保護を回避してネットワークに侵入したりするなどのリスクが顕在化しています。

サードパーティーによるVPNアクセスでは、リスクがさらに顕著になります。攻撃者がサードパーティーの認証情報を悪用し、検出を回避しながらネットワークを侵害するケースが増えているため、**93%もの回答者が外部からのVPN接続によって生じるバックドアの脆弱性に懸念を抱いています。**VPNは初期アクセスの原因となるだけではなく、侵害の被害を拡大させるという問題もあります。ネットワーク内の移動を防ぐためにきめ細かなポリシーを施行するゼロトラスト ソリューションとは異なり、VPNは広範なアクセスを提供するため、攻撃者による水平方向への移動や権限昇格を容易にしてしまいます。**実際、回答者の71%がラテラルムーブメントを最大の懸念事項とみなしており、**この種の移動は侵害の範囲と影響をはるかに悪化させると考えています。

これらの課題に加え、パフォーマンスの低下、複雑な認証、頻繁な切断といった日常的な問題も、VPNからゼロトラスト モデルへ移行する明確な理由となっています。2025年版 VPNリスク レポートは、ITやサイバーセキュリティの専門家632人の洞察に基づいています。2025年におけるVPNの利用状況やリスク、課題を明らかにするとともに、組織がサイバーセキュリティ態勢やセキュア リモート アクセス対策を向上させるためのベスト プラクティスを提供する目的で作成されました。

このレポートの調査結果は、従来のVPNを廃止して最新のクラウド型ゼロトラスト アーキテクチャーを導入する理由をデータに基づいて深堀りしたものであり、ITやセキュリティのリーダーがより効果的な意思決定を行うのに役立ちます。暗黙の信頼から継続的な検証への移行は、もはや選択肢の一つではありません。現代の分散型組織を保護し、ITの複雑さを軽減しながら、シームレスなユーザー エクスペリエンスを確保するために不可欠な取り組みとなっています。

VPN のセキュリティに関する懸念

VPN の旧式化：セキュリティ リスクとユーザーの不満

現在もリモート アクセスにVPNを使用している組織では、セキュリティ ギャップ、運用上の非効率性、エンドユーザーの不満などの問題が深刻化しており、アクセス セキュリティにVPNはもはや適していないという認識が広まっています。

最大の課題として回答者の54%がセキュリティおよびコンプライアンスのリスクを挙げています。特に、ランサムウェア、権限昇格、ラテラル ムーブメントによる攻撃などに対するVPNの深刻な脆弱性が組織の課題として浮き彫りになっています。攻撃者はVPNを格好の標的とみなしているため、脆弱性はすぐに修正される必要がありますが、高度な脅威に気づく前に対処するのは簡単ではありません。

また、ユーザーの不満は高まり続けており、回答者の51%がVPNのパフォーマンスの低下(接続の低下、接続の中断、煩雑な認証プロトコルなど)が生産性を妨げていると認識しています。VPNは依然として運用負担を伴う技術であり、その理由として回答者の41%が管理の難しさ、37%が継続的な保守にかかる高額な費用を挙げています。これらの結果からも、VPNがいかに貴重なリソースやIT予算を浪費し、反復的なトラブルシューティング作業にIT部門の時間を費やしているかがわかります。

従来のアプローチからゼロトラストへの移行

VPNの脆弱性がいかに深刻であるかを再認識させる侵害が発生しました。2025年1月、中国のサイバー スパイ グループが、Ivanti Pulse Secure VPNに存在するゼロデイ脆弱性を悪用し、組織のネットワーク全体に不正アクセスしました。この攻撃は、ここ数か月で発生したVPNを標的とした攻撃の一例であり、従来のアクセス モデルではインフラを十分に保護できない理由を浮き彫りにしています。

このようにVPNにはさまざまな問題があるため、従来のVPNベンダーの多くが、クラウド型の仮想マシンを「ゼロトラスト ソリューション」として提供し始めてい

VPN からの移行はビジネス上の必須事項です。組織は、アイデンティティーに基づいた最小特権アクセスときめ細かなセグメンテーションを提供する真のゼロトラスト フレームワークに移行する必要があります。これらのクラウド型アーキテクチャーは、水平方向の攻撃対象領域の削減、ユーザー エクスペリエンスの向上、IT の複雑さの軽減を可能にします。VPN では、この 3 つのメリットを同レベルで実現できません。

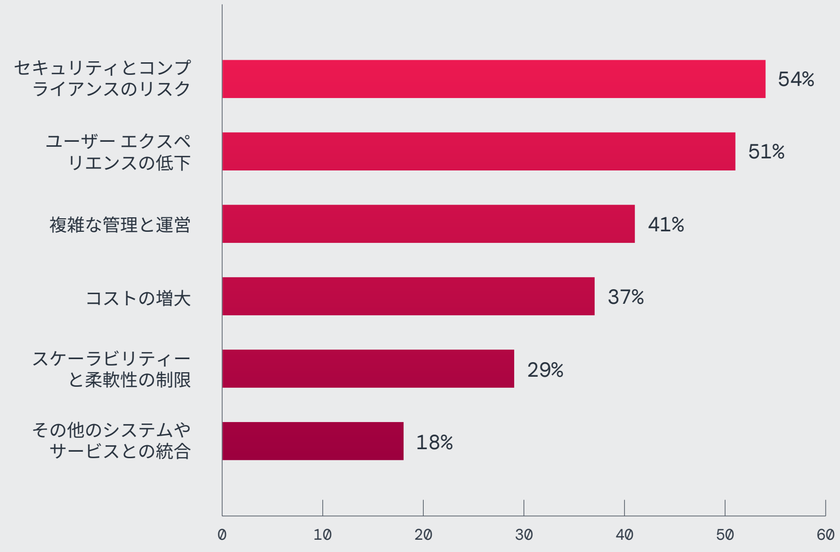


図 1： VPN ソリューションの最大の課題

ます。しかし、クラウド型VPNサービスも、アーキテクチャーの本質的な部分はこれまでと変わりません。つまり、パブリックIPアドレスを持つインターネット接続サービスであり、侵害されるリスクが依然として存在するということです。最近では、ある大手セキュリティベンダーがホストする2万以上のパブリックVPN IPアドレスをスキャンしようとする攻撃の試みが急増しました。過去のケースを踏まえると、この種のスキャン活動は攻撃者が標的のVPNシステムの脆弱性、特にまだ公開されていない脆弱性を悪用する準備を進めている可能性を示唆しています。言い換えれば、システムにアクセスできるということは、侵害もできるということです。クラウドベースのVPNはその基本的な設計により、いかに効果的に宣伝されていても、真のゼロトラスト原則を達成することはできません。

ランサムウェアと VPN：最悪の事態を招く深刻なリスク

ランサムウェア グループは依然としてVPNの脆弱性に狙いを定めており、組織がセキュリティ パッチを適用する前にゼロデイの欠陥と既知の弱点の両方を悪用しています。VPNは広く普及しているうえ、従来のネットワーク信頼モデルを採用しているため、攻撃者にとって「簡単に利益を得られる手段」となっています。

回答者の92%が、未修正のVPNの脆弱性からランサムウェア攻撃が発生する可能性を懸念しており、より堅牢な保護メカニズムの必要性が浮き彫りになっています。このデータは、VPNが最新のサイバー リスクを軽減するための信頼できるツールではなく、むしろリスクを増大させる存在とみなされるようになった理由を強調しています。

これらの懸念が現実のものであることは、数々の実例によって証明されています。たとえば、2023年1月、Citrix NetScalerのパッチ未適用の脆弱性(CVE-2023-4966)が悪用され、米国の複数の医療機関がランサムウェア攻撃の被害に遭いました。攻撃者はこの脆弱性を悪用して病院のシステムに侵入し、業務の妨害や患者データのロックを行ったため、病院側は必要な緊急医療対応を別の施設に送らざるを得なくなりました。これはすべて、脆弱性が迅速に修正されなかったことが原因です。このインシデントからも明らかなように、パッチが適用されていないVPNは広範なリスクをもたらします。攻撃者は修正が適用される前に脆弱性を悪用するために、公開されたシステムを定期的にスキャンしており、組織を侵害、業務の中断、財務損失などのリスクにさらしています。

組織は、無限に続くパッチ適用から脱却し、進化し続ける脅威に対応するための予防的な防御戦略を採用する必要があります。ゼロトラスト フレームワークは、アイデンティティーに基づいたアクセス制御と継続的な検証に焦点を当て、脆弱性にパッチが適用されていない場合でも、ランサムウェアのリスクを大幅に軽減します。さらに、自動化された検出システムと動的なポリシーにより、潜在的な侵害を封じ込め、攻撃者のラテラル ムーブメントや権限昇格を防止します。

未修正の脆弱性が原因でランサムウェアの標的になることをどの程度懸念していますか？

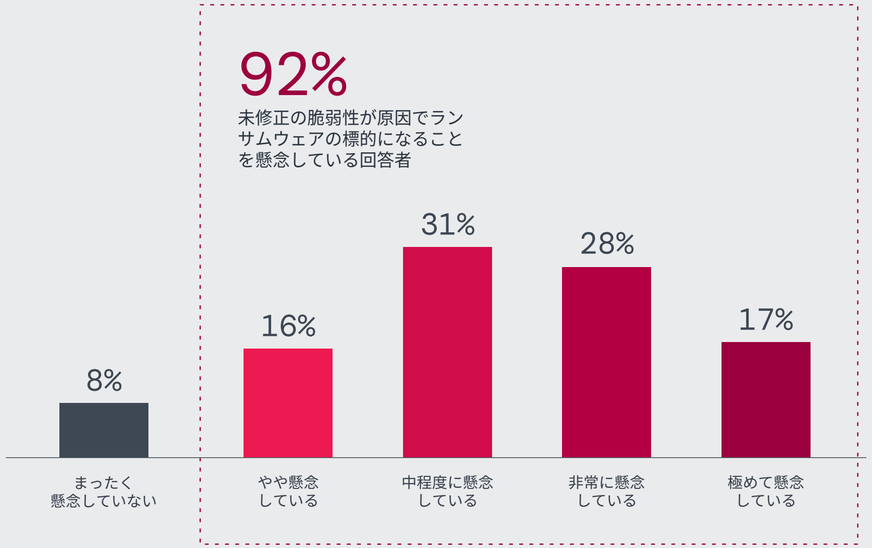


図 2： ランサムウェア攻撃に関する懸念

VPN とラテラル　ムーブメント：侵害の影響範囲の拡大

VPNは、ランサムウェアやその他の脅威による初期侵入だけでなく、危険な攻撃手法であるラテラル ムーブメントも可能にする要因です。攻撃者は、VPNが提供する広範なアクセスを悪用して権限を昇格させ、標的のネットワーク内部に深く侵入し、壊滅的な被害を引き起こします。

回答者の71%がこのリスクに一定の懸念を示し、そのうち32%が高い懸念を示しています。こうした懸念が生じるのも無理はありません。なぜなら、広範なネットワーク アクセスを許可するVPNは、攻撃者が検出を回避しながら移動し、権限を昇格させてネットワーク内部に侵入し、機密データを盗み出すという状況を作り出してしまうからです。

2024年9月、攻撃者がIvanti Cloud Service Appliance (CSA)の複数のゼロデイ脆弱性(特にCVE-2024-8963とCVE-2024-8190)を悪用し、いくつかの組織を侵害したことが、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)とFBIによって確認されました。攻撃者は管理制御を回避しながら、任意のコマンドを実行して認証情報を収集し、Webシェルを埋め込むことで、ネットワーク全体のラテラル ムーブメントを可能にしました。IvantiのVPNに関するセキュリティ インシデントは以前から発生していましたが、今回の新たな攻撃は、パッチ適用や設計の見直しだけでは、ネットワークベースのリモートアクセス モデルが抱える根本的なセキュリティ欠陥を解消できないことを浮き彫りにしました。

VPN が侵害された場合、攻撃者がネットワーク上を水平方向に移動することをどの程度懸念していますか?

89% 攻撃者によるラテラルムーブメントを懸念している回答者

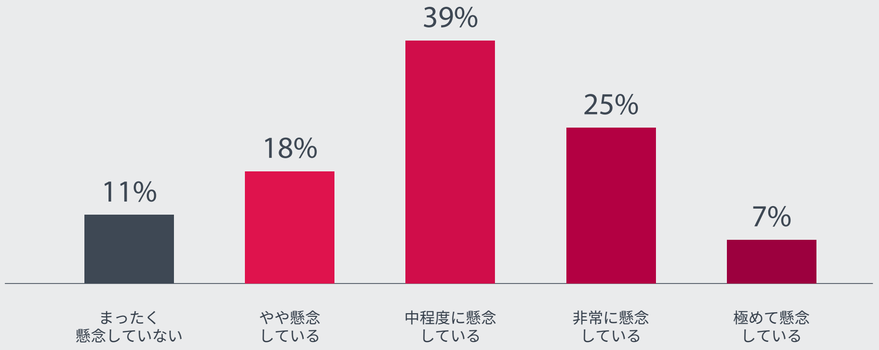


図 3： VPN が侵害された場合のネットワーク上のラテラル　ムーブメントに関する組織の懸念

これらのリスクを軽減するには、VPN アクセスから、厳密なセグメンテーションを備えたゼロトラスト ネットワーク アクセス (ZTNA) に移行する必要があります。ユーザーに広範なネットワーク アクセスを許可する VPN とは異なり、ZTNA はアイデンティティーとコンテキストに基づいたアプリケーションレベルのアクセスを提供し、ユーザーが必要なリソースにのみアクセスできるようにします。このアプローチにより、攻撃者が初期アクセスに成功した場合でもラテラル ムーブメントが阻止され、攻撃対象領域と侵害の潜在的な影響範囲が大幅に減少します。さらに、ネットワークのマイクロセグメンテーションを実装することで、重要なシステムを分離し、侵害された資産と安全な資産との間の不正なやり取りを防ぎ、セキュリティを強化します。

2020 年から 2025 年に確認された VPN のCVE：増加する重大度の高い脆弱性

セキュリティ上の欠陥がまったくないソフトウェアは存在しないため、脆弱性から完全に免れることは現実的ではありません。しかしVPNの脆弱性の場合、特にゼロデイ脅威は、深刻な被害をもたらす可能性が高くなっています。これは、攻撃者がその脆弱性の影響を受けるVPNインフラを簡単に特定し、パッチがリリースまたは適用される前に悪用できるためです。コミュニティー全体の連携を促進するという点で、CVEの報告は非常に価値があります。脆弱性に関する情報を共有することで、ベンダーと顧客は確立されたベスト プラクティスに従い、タイムリーな更新と開示を通じてサイバー ハイジーンを向上させることができます。CVEが発見された経緯やそこに含まれる情報は、サイバー脅威が時間とともにどのように進化しているかのパターンと傾向も明らかにします。

Zscaler ThreatLabzは、MITRE CVE Programによって報告された2020年から2025年のVPNに関する共通脆弱性識別子(CVE) 411件を分析したところ、この5年間でVPNの脆弱性が緩やかながらも顕著に増加していることを確認しました。これらの脆弱性には、Webベースの管理インターフェイスの悪用から、コマンド インジェクションや入力検証の脆弱性、暗号化の失敗、DoS/DDoS攻撃など、幅広いVPNの欠陥が含まれています。VPNの脆弱性は最近も多数報告されており、その多くが社会の注目を集める大規模なセキュリティ侵害を引き起こしています。

これらの多くは重大な脆弱性です。たとえば、2024年にはNISTが報告した83件のVPNの脆弱性のうち、60%がCVSSで「重要(High)」または「緊急(Critical)」に分類されました。VPNの脆弱性に関して最も多く報告されたのが、リモート コード実行(RCE)の脆弱性でした。これは、攻撃者が任意のコマンドを実行し、システムを侵害できる可能性のある脆弱性です。過去1年間に報告されたVPNの脆弱性の大部分は決して軽視できるものではなく、攻撃者が比較的容易に悪用できる脆弱性をユーザーにさらしていました。さらに、これらの脆弱性の多くはゼロデイ エクスプロイトとして利用されていました。2025年初頭のCVEの件数はまだ少ないものの、CVE-2025-0282とCVE-2025-0283の2つのゼロデイ エクスプロイトを含む、重大な脆弱性がすでに特定されています。

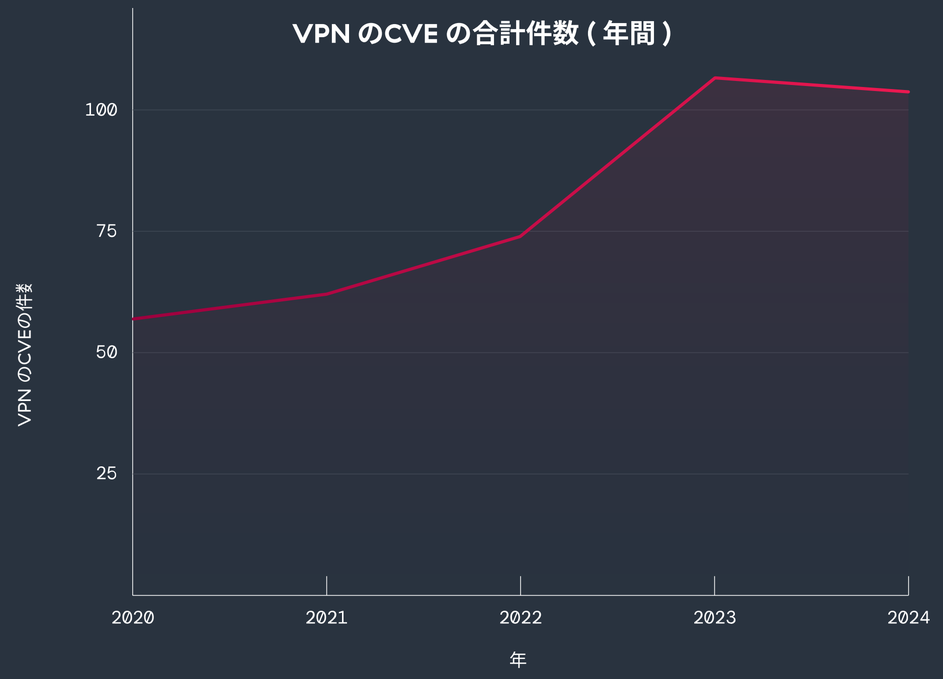


図 4： 2020 年から 2024 年に報告された各年の VPN のCVE の合計件数

1. RCEが引き続き最大の脅威に

- **調査結果：**RCEの脆弱性は、過去4年にわたり常に上位に挙がり、2024年だけでも32件に上りました。さらに、2025年のデータを含めると累計149件に達しており、最も頻繁に発生する重大な脆弱性となっています。
- **推奨事項：**RCEの脆弱性が悪用されると、攻撃者はVPNデバイス上で任意のコマンドを実行できるようになり、システム全体の侵害につながる恐れがあります。これに対処するためにも、組織は脆弱なシステムへの即時のパッチ適用と適切な保護対策を最優先する必要があります。

2. 権限昇格が着実に増加

- **調査結果：**権限昇格の脆弱性は近年着実に増加しており(66.7%)、2024年には20件が報告され、ピークに達しています。
- **推奨事項：**攻撃者がVPNの欠陥を悪用して権限を昇格させ、システムの管理制御を取得するケースが増えています。組織は、安全なシステムの構成を確保し、特権アクセスを厳格に制限する必要があります。

3. サービス拒否(DoS)の脆弱性が200%も増加

- **調査結果：**DoS関連の脆弱性は、2020年に報告された9件から2024年には約3倍の27件にまで増加しました。2025年のこれまでのデータを含めると、全体で85件となり、近年で2番目に多い種類となっています。
- **推奨事項：**DoS攻撃は巧妙化しており、業務を中断させるための主な標的としてVPNシステムが狙われています。これらのリスクを軽減するには、レート制限やトラフィック シェーピングなどの技術を導入する必要があります。

4. 機密データの漏洩は少ないながらも依然として深刻な問題

- **調査結果：**機密データの漏洩に関連する脆弱性は合計41件と比較的少ないものの、その影響は深刻であり、認証情報、暗号化キー、ユーザー データなどの重要な情報が不正に公開される可能性があります。
- **推奨事項：**機密データの漏洩は、特に組織の機密性とコンプライアンスに深刻な損害を与えます。情報漏洩を検出して防止するために、堅牢な暗号化、安全なコーディング手法、トラフィックの常時監視を導入する必要があります。

5. 認証バイパスの脆弱性が着実に増加

- **調査結果：**認証バイパスのインシデントは発生件数が比較的少ないものの、一定の頻度で報告されています。2020年には4件、2023年のピーク時には6件、2024年には再び4件が確認されており、累計では30件に達しています。
- **推奨事項：**攻撃者は、多要素認証(MFA)やログインの仕組みの欠陥を悪用してユーザーになりすまします。組織はMFAの構成を強化し、異常なログイン アクティビティーを積極的に監視する必要があります。

主な傾向：VPN の脆弱性が引き起こす攻撃の種類

これらの脆弱性が悪用された場合の潜在的な被害を把握するために、ThreatLabz は、リモート コード実行 (RCE)、権限昇格、情報漏洩、サービス拒否 (DoS)、認証バイパスの 5 つの攻撃カテゴリーで VPN の脆弱性を評価しました。なお、一部のカテゴリーは、異なるものの密接に関連する種類の攻撃を包括的にまとめています。たとえば、認証バイパスには 2 要素認証または多要素認証 (MFA) を回避する可能性のある攻撃と、その他の基本的な認証手段を回避する攻撃が含まれます。特に RCE の脆弱性は重大であるため、あらゆる組織が優先度の高い問題として対処する必要があります。

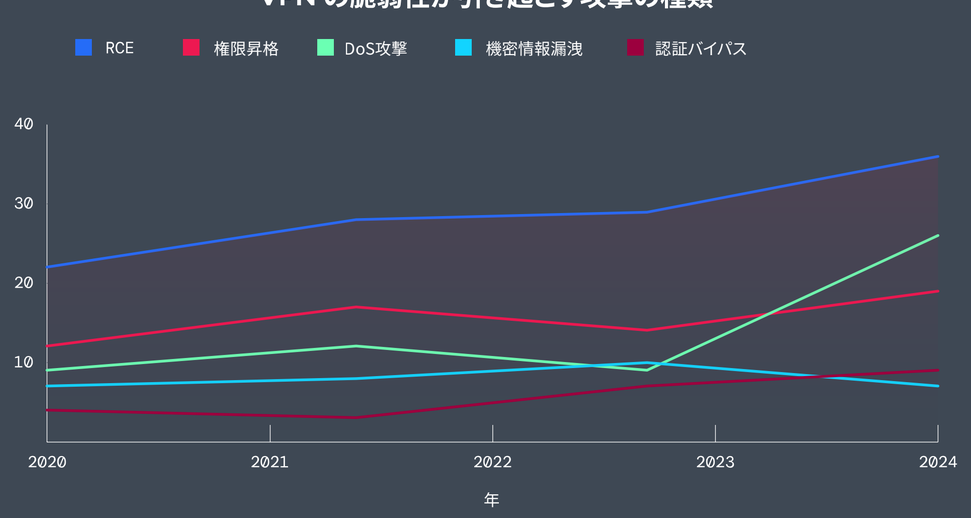


図 5： 2020 年から 2024 年までに VPN の脆弱性が引き起こした攻撃の種類 (RCE、権限昇格、DoS 攻撃、機密情報漏洩、認証バイパス)

主な傾向：
VPN の重大な脆弱性

ThreatLabz は毎年、VPN の脆弱性が引き起こす攻撃の種類だけでなく、その深刻度も分析しています。**全体として、CVSS スコアが高く、「重要 (High)」または「緊急 (Critical)」に分類された脆弱性は、2020 年から 2024 年にかけて 38.9% 増加しました。**特に、2024 年に報告された脆弱性の 66.3% が「重要 (High)」または「緊急 (Critical)」に分類されており、パッチが適用される前にこれらの脆弱性が悪用されると、深刻な被害につながる恐れがあります。さらに、ThreatLabz は、CVE データに記録されているさまざまな種類の脆弱性の重大な傾向も分析しました。進化する VPN の脅威から組織を保護するためにも、これらの傾向を正確に理解しておくことが重要です。

CVSS で「重要 (High)」または「緊急 (Critical)」に分類された VPN の脆弱性の件数

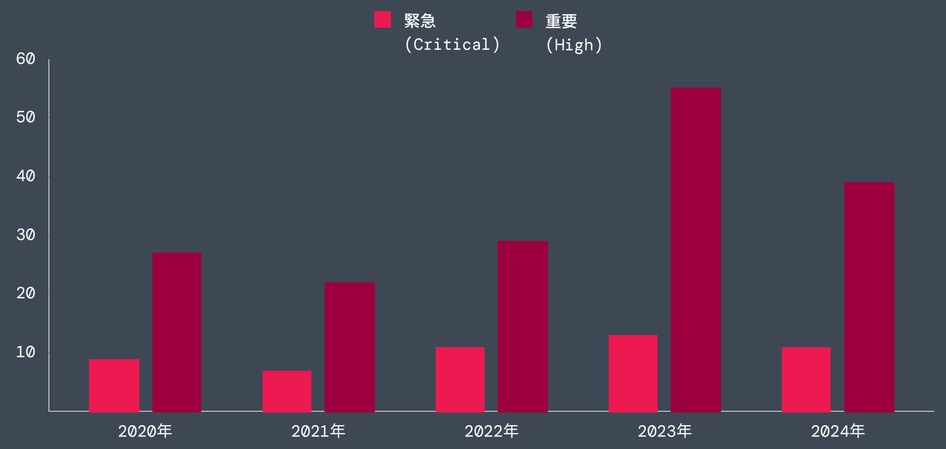


図 6： 2020 年から 2024 年の間に、CVSS スコアが高く「重要 (High)」または「緊急 (Critical)」に分類された VPN の脆弱性の件数

1. Web ベースの管理インターフェイスの悪用の増加

- **傾向：**コマンド インジェクションと入力検証の脆弱性は一貫して増加しています。これは、攻撃者が管理者とエンドユーザーの両方の視点から管理ポータルに注目するようになっているためです。これらのインターフェイスはその設計上、インターネットに公開されているため、攻撃者に悪用されやすい傾向があります。
- **深刻化：**これらの脆弱性は 2020 年から 2021 年にも確認されていましたが、2022 年以降に急激に増加しています。このような管理インターフェイスは、特にセキュリティ コーディングの慣行が不十分なため、攻撃者にとってアクセスしやすい格好の標的となっています。

2. 認証と MFA の広範なバイパス

- **傾向：**MFA バイパス、セッション ハイジャック、不適切なセッション管理など、特に認証方法を標的とした攻撃が着実に増加しています。
- **深刻化：**初期 (2020 年から 2021 年) は主に単純な認証バイパスでしたが、2023 年から 2025 年にかけては MFA の弱点を突いた、より高度で自動化された永続的な攻撃へと進化しています。これは、攻撃者がより強固なセキュリティ対策を弱体化させることを目的としています。

3. ローカル権限昇格の悪用の増加

- **傾向：**ローカル権限昇格の脆弱性はますます一般的になっており、深刻化しています。
- **深刻化：**2020 年から 2021 年においては、軽微な設定ミスなどの単純な問題が原因で発生していました。しかし、2024 年から 2025 年にかけて、攻撃者は DLL ハイジャックなどの高度な手法を採用して、システム内でより高い権限を取得するようになっています。

4. DoS/DDoS 攻撃の巧妙化

- **傾向：**DoS 攻撃は、リソースを枯渇させる基本的な攻撃手法 (2020 年から 2021 年) から高度な DDoS 増幅の手法 (2024 年から 2025 年) へと進化を遂げました。
- **深刻化：**攻撃者は、不正パケットを用いた単純な妨害手法から、より巧妙な増幅攻撃へと移行しており、業務の中断を最大化することを目的とした攻撃がさらに高度化していることが明らかになっています。

5. 継続的かつ深刻化する暗号化の問題

- **傾向：**証明書の不適切な検証、キーの漏洩、不十分な TLS 検証など、暗号化の実装に起因する問題が顕著に増加しています。
- **深刻化：**暗号化に関連する脆弱性は 2022 年頃から著しく急増し、2024 年から 2025 年には深刻な欠陥がピークに達しました。攻撃者がこれらの弱点を悪用して VPN の機密性を侵害する戦略に注力していることが浮き彫りになっています。

VPN のセキュリティに関する懸念（続き）

セグメンテーションの実装における課題

ラテラル ムーブメントのリスクを軽減するために、多くの組織がセグメンテーションを活用して攻撃の拡散を制限しようとしています。セグメンテーションは、攻撃対象領域を削減するための重要な防御メカニズムですが、その実装は簡単ではありません。

この調査ではこうした課題が明確に浮き彫りになっており、組織の51%が構成の複雑さに直面している、または今後直面する可能性があると回答しています。また、39%が専門知識やリソースの不足を課題として挙げ、24%がパフォーマンスのボトルネックに直面していると回答しています。従来のネットワーク アーキテクチャーでは、現代のIT環境に求められるきめ細かなアクセス制御をサポートできないことはこれらのデータからも明らかです。

2023年に発生したMGM Resortsへのランサムウェア攻撃では、セグメンテーションの課題が攻撃の範囲と影響を拡大しました。攻撃者はソーシャル エンジニアリングを通じて初期アクセスを確保しましたが、水平方向に移動できたのはセグメンテーションが不十分だったためです。この侵害により、ホテルの運営、ATM、カジノのゲーム システムが中断し、同社は推定1億ドルの損害を被りました。これは、不十分なセグメンテーションによって攻撃者が重要なシステム間を移動できる環境が作られ、初期侵入による影響が拡大してしまった事例の一つです。

これらの課題に対処するには、アイデンティティーに基づいたクラウドベースのセグメンテーション モデルを実装し、ポリシー施行を合理化しながら、手動の作業負荷を軽減する必要があります。複雑なファイアウォール ルールと VLAN の構成に依存する従来のネットワーク セグメンテーションとは異なり、ゼロトラスト アプローチは、ユーザー アイデンティティー、デバイス ポスチャー、リアルタイムのリスク評価に基づいてネットワークを動的にセグメント化します。この仕組みにより、承認されたユーザーのみに決められたアプリケーションへのアクセスが許可されるのと同時に、より広範なネットワーク セキュリティが確保されます。

セグメンテーションを実装する際、どのような問題に直面しましたか？または直面すると予想されますか？

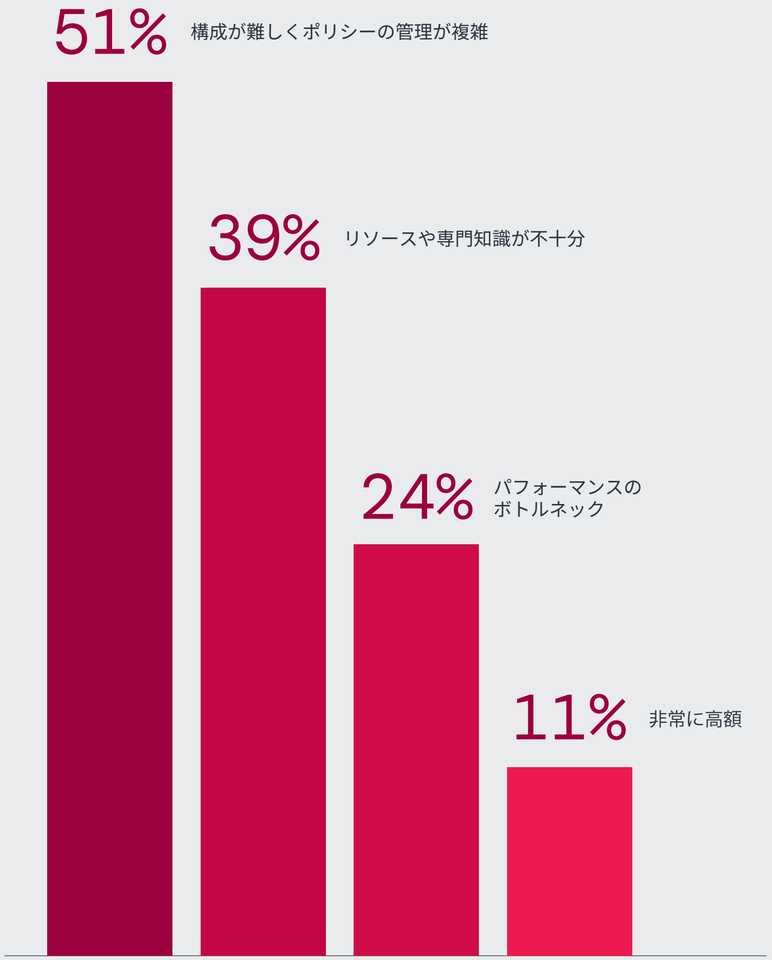


図 7： セグメンテーションを実装する際に組織が直面する主な課題

M&A におけるサイバーセキュリティ リスクを高める VPN

日々のセキュリティ上の課題に加えて、合併と買収 (M&A) などの大規模な IT の移行は、さらなるリスクをもたらし、攻撃対象領域を拡大します。これらの移行には、異なるネットワーク、アプリケーション、アイデンティティーの統合が含まれるため、意図せず脆弱性を継承したり、システムを誤って設定したり、セキュリティ管理が脆弱になったりする可能性があります。

回答者の約 3 分の 2 (64%) が M&A 後のサイバー脅威に懸念を示しており、IT 統合中に生じるセキュリティ ギャップを認識しています。

最近の例としては、2023 年に発生した Capita のデータ侵害が挙げられます。この事例では、組織買収後に攻撃者がセキュリティの弱点を突き、機密情報に不正アクセスしました。このインシデントの主な原因は、合併した組織間でのセキュリティ ポリシーの不整合にあり、その結果、攻撃者が新たに統合されたネットワークを水平方向に移動できるようになりました。この侵害からもわかるように、一貫性のないセキュリティ制御、VPN を使用した従来型アクセス、セグメント化されていない環境は、特に M&A 活動期間中にサイバー攻撃を助長する状況を作り出します。

M&A の最中にこれらのリスクを軽減するには、サイバーセキュリティのデュー デリジェンスを優先するとともに、最小特権アクセスを適用し、セグメンテーションを実装する必要があります。VPN アクセス モデルとは異なり、ゼロトラストは、IT 環境が統合されても広範なアクセス権限を継承しないようにし、ラテラル ムーブメントや権限昇格のリスクを効果的に軽減します。VPN と境界ベースの防御から、すべてのリクエストを検証するアイデンティティーに基づいたアクセス制御に移行することで、従来の IT 環境と新たに統合された IT 環境の両方を保護できます。

M&A 後にサイバーセキュリティ攻撃に対して脆弱になることを懸念していますか?

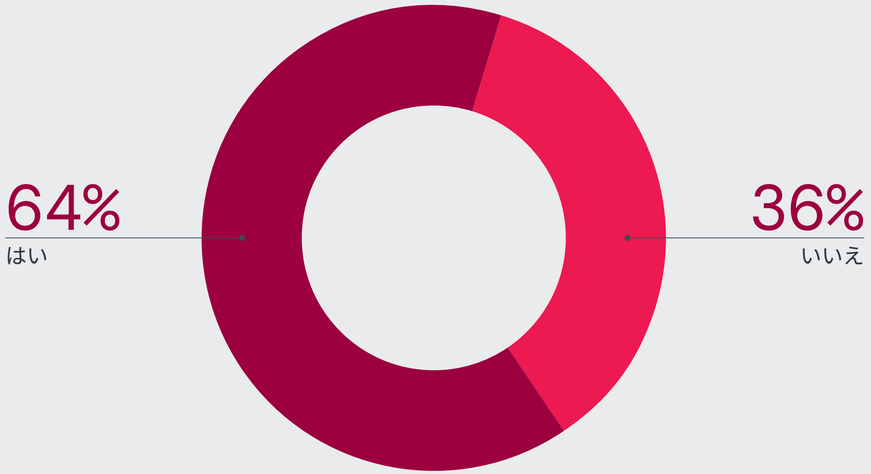


図 8： M&A 後のサイバー攻撃に対する組織の懸念

サードパーティーによる VPN アクセス：バックドアの脆弱性

サードパーティーによる VPN アクセスは、攻撃者にとって最も脆弱な侵入口の一つとなっています。従来の VPN では、認証が完了するとネットワーク全体への広範なアクセスが付与される設計となっており、その権限は外部のベンダーやパートナーにまで拡張されます。しかし、この過剰なアクセスは攻撃者が悪用できる死角を生み出します。攻撃者は、盗んだ認証情報や脆弱なパスワード、設定ミス、パッチが適用されていない脆弱性を悪用して信頼された接続を乗っ取ります。回答者の 93% がバックドアの脆弱性に深刻な懸念を抱いており、信頼ベースの静的なアクセス モデルに依存する組織にとってサードパーティーによるアクセスは、まさに時限爆弾のようなリスクとなっています。

この懸念が現実のものであることを裏付ける事例があります。2024 年 8 月、Enterprise Financial Group (EFG) は、約 2 万人の顧客の個人情報が流出する大規模なデータ侵害に見舞われました。この侵害は、EFG のネットワークにアクセスできるサードパーティーが使用していた VPN の脆弱性に端を発しており、攻撃者はこれを悪用してネットワークに侵入し、機密情報にアクセスしました。サードパーティーに VPN 経由でのアクセスを許可すると、深刻なセキュリティ ギャップが生まれ、企業ネットワークへの侵入経路となる可能性があります。

組織は、サードパーティーによる VPN アクセスを監査し、時間制限付きアクセス、エンドツーエンドのトラフィック検査 (デバイスとアプリケーション間)、適応型の認証など、より厳格なポリシー制御を行うことから始める必要があります。ゼロトラスト モデルに移行すれば、アプリケーションごとのアクセスを適用でき、外部パートナーには必要最小限のアクセスのみ許可されます。さらに、継続的な監視とリスクベースのポリシーにより、サードパーティーの脆弱性を大幅に軽減できます。

サードパーティーによる VPN アクセスがネットワークへの侵入経路となる可能性について、どの程度懸念していますか?

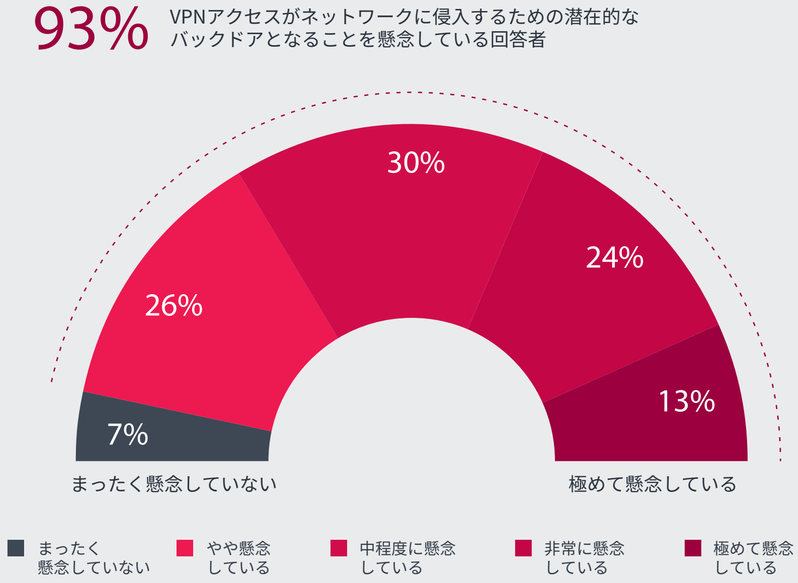


図 9: サイバー攻撃を助長するサードパーティーによる VPN アクセスに関する組織の懸念

従来の保護対策の課題とギャップ

プライベート アプリケーションを危険にさらす従来のツール

ランサムウェア、認証情報の窃取、APIの悪用など、巧妙化するWebベースの脅威からプライベート アプリケーションを保護することは、現代の組織にとって極めて重要な優先事項です。しかし、多くの組織が最新の脅威に対抗するための機能が十分備わっていない旧式のツールを引き続き使用しています。

調査によると、Web攻撃に対する防御は依然として、ファイアウォール(84%)、Webアプリケーション ファイアウォール(WAF、58%)、VPN (43%)が大多数を占めています。一方、攻撃者はパッチが適用されていないデバイス、不適切な構成、境界ベースのセキュリティモデルに内在する弱点などを悪用して、これらの防御ツールをすり抜けるようになってきています。つまり、従来の防御では最新の脅威環境に効果的に対処できなくなっているということです。

最近の侵害は、このような境界型防御の欠点を浮き彫りにしています。2024年8月、Salt Typhoonと呼ばれる中国のハッカー グループは、パッチが適用されていないネットワーク デバイスやルーターの脆弱性を悪用し、AT&TやVerizonなどの米国の大手通信会社に侵入しました。この攻撃は、100万人以上のユーザーの機密性の高いメタデータを侵害し、ファイアウォールやVPNなどの従来のセキュリティ対策を巧妙に回避できることを実証しました。

プライベート アプリケーションを効果的に保護するには、旧式の境界型防御から脱却し、ゼロトラスト アクセス モデルを採用することが最も実用的な選択肢です。ゼロトラスト アーキテクチャーは、ネットワークベースのセキュリティを排除し、厳密に施行されるきめ細かな最小特権アクセスのポリシーに従ってユーザーをアプリケーションに直接接続させます。ファイアウォールや VPN とは異なり、ゼロトラスト アーキテクチャーでは、きめ細かな最小特権アクセスを適用しながらアプリケーションへの直接接続が適用されるため、不正アクセスの試みを確実にブロックできます。さらに、ラテラル ムーブメント、セッション ハイジャック、認証情報の窃取など、従来の境界型防御を回避するための一般的な攻撃手法も阻止できます。

Web ベースの攻撃からプライベート アプリケーションを保護するために、どのような製品を使用していますか?

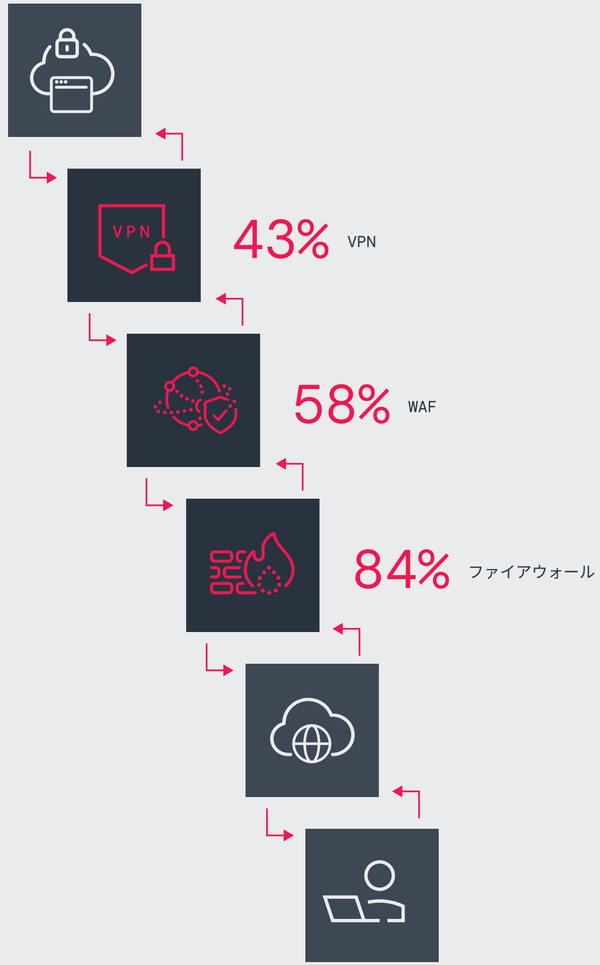


図 10: 組織が Web ベースの脅威からプライベート アプリケーションを保護するために使用しているセキュリティ製品

VPN 環境での NAC の使用：限定的な保護

注目すべきことに、調査対象となった組織の 54% がプライベート リソースへの VPN アクセスを保護するために NAC を使用していると回答しています。しかし、NAC を導入しても VPN の脆弱性に関連する侵害や悪用を防ぐことはできません。つまり、NAC ではネットワークベースの信頼モデルに内在する根本的なリスクに対処できないということです。

NAC ソリューションは、デバイス ポスチャー チェック、認証、ネットワーク セグメンテーションを行います。しかし、VPN が抱える広範なアクセス権限、ラテラル ムーブメントのリスク、暗黙の信頼といった根本的なセキュリティ問題には対応できません。

最近の侵害は、NAC を実装しても VPN の脆弱性が依然として重大な弱点であることを示しています。2023 年 11 月、米国エネルギー省は、VPN の認証情報漏洩に関する大規模なセキュリティ インシデントを確認しました。この事例では、攻撃者がアクセス制御を回避し、機密性の高い内部システムに侵入しました。このインシデントは、攻撃者が盗んだ認証情報やパッチが適用されていない脆弱性、セッション ハイジャックのいずれかを通じて、VPN の弱点を直接悪用する手口を浮き彫りにしています。さらに、基盤となる信頼モデルが根本的に変わらない限り、NAC による防御は限定的なものであることを如実に示しています。

VPN とプライベート リソース間に NAC (ネットワーク アクセス制御) を使用していますか?

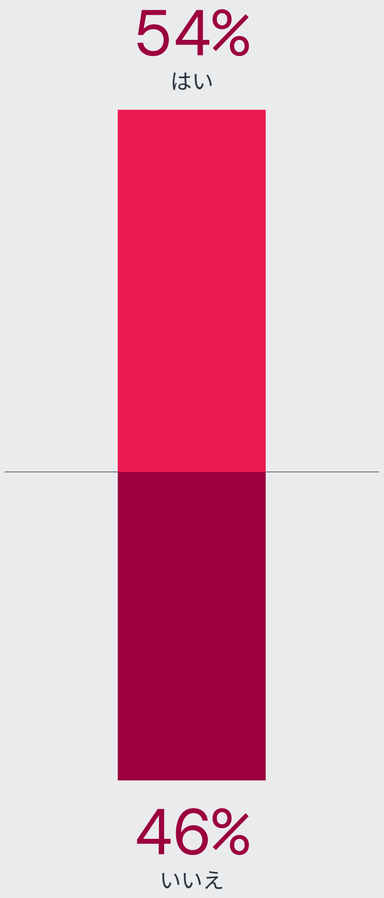


図 11： VPN とプライベート リソース間で NAC を使用している組織の割合

NAC と従来の VPN アーキテクチャーの限界を克服するには、ゼロトラスト セキュリティ モデルを採用する必要があります。ゼロトラストは、アイデンティティー、デバイス ポスチャー、コンテキストに基づいて継続的に検証されるポリシーの下で、ユーザーに特定のアプリケーションへの直接接続を許可することで、無制限のネットワーク アクセスを排除します。そして、不正アクセスをブロックし、ラテラル ムーブメントを封じ込め、権限昇格やデータの持ち出しを阻止します。

VPN のユーザー　エクスペリエンスと管理の課題

VPN のパフォーマンスの問題：ユーザーの不満と IT 部門の過負荷

VPN は単なるセキュリティ上の問題にとどまらず、ユーザーの不満の主な原因にもなっています。エンドユーザーの間では、VPN のパフォーマンスに対する不満が高まっており、この問題が生産性の低下を招くとともに、IT 部門の負担をさらに増大させています。

ユーザーの不満の中で最も多いのは、接続スピードの遅さ (23%) に関するものです。これは、在宅環境でクラウド アプリケーションにアクセスする際に発生する遅延や輻輳、低いパフォーマンスといった VPN の課題を裏付けています。さらに、認証の問題も大きな課題となっています。回答者の 20%が複雑なログイン プロセスを挙げており、17%が認証の問題が原因でアプリケーションにアクセスできない点に不満を感じています。

これらのパフォーマンスに関する問題は、日常業務に混乱を引き起こし、生産性を低下させます。また、IT ヘルプ デスクは頻繁に発生するトラブルシューティング作業に追われており、これがボトルネックとなって解決時間を遅らせています。この問題は、リモート ワークやハイブリッド ワークの環境が複雑化するにつれ、さらに深刻化しています。

VPN からゼロトラスト ネットワーク アクセス (ZTNA) に移行すると、帯域幅の輻輳が解消されます。さらに、アプリケーションへの遅延のない安全な直接接続が可能になり、エンドユーザーのエクスペリエンスが大幅に向上します。VPN の場合、すべてのトラフィックを中央のゲートウェイ経由でルーティングするため、パフォーマンスのボトルネックが生まれます。一方、ZTNA はパフォーマンスを低下させることなく、アプリケーションへの安全な直接接続を可能にします。アイデンティティーに基づいたアクセス制御、継続的な検証、クラウド型のセキュリティを採用することで、VPN に対する一般的な不満を解消できるだけでなく、従業員の生産性を向上させながら、柔軟性に欠ける VPN フレームワークのトラブルシューティングとサポートによる IT 部門の負荷も軽減できます。

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？

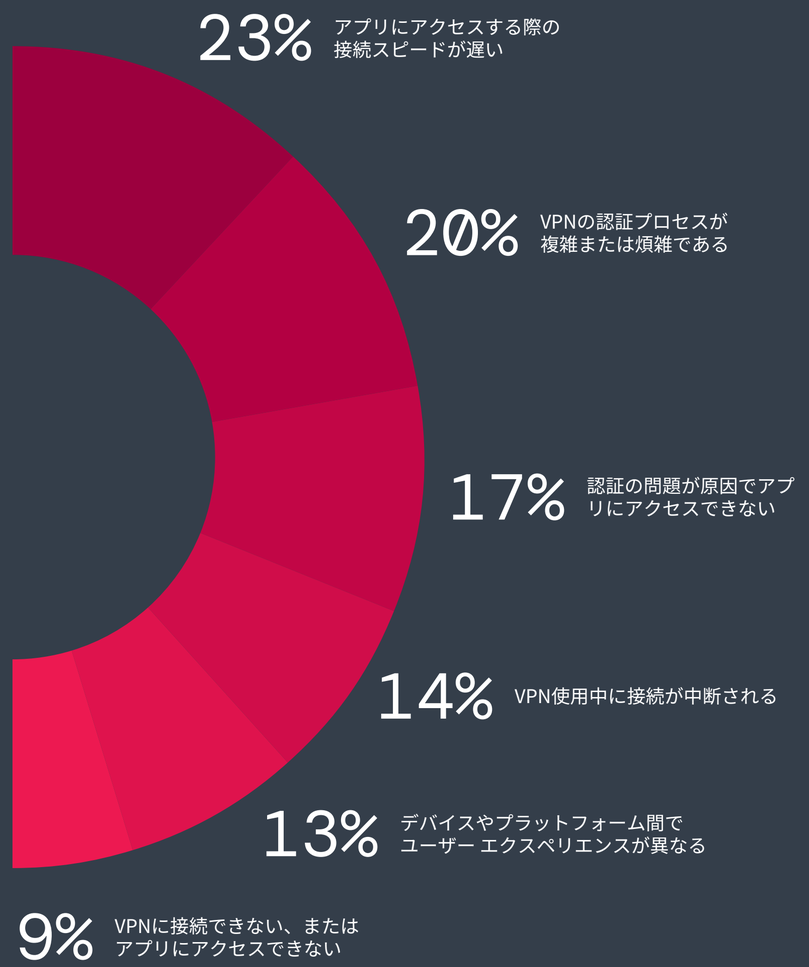


図 12： VPN ユーザーの間で最も一般的な不満

VPN の管理：IT 部門の負担増大と脆弱性の顕在化

VPNは、恒常的なセキュリティの脆弱性、リソース負担の大きい保守要件、現代のクラウド重視の組織環境のニーズに合わなくなった古いアクセス モデルにより、IT部門にとって大きな負担となっています。IT部門の最大の懸念となっているのが、セキュリティ インシデントにつながるセキュリティ ギャップ(52%)です。これは、認証情報の窃取、パッチが適用されていないソフトウェアの悪用、VPNアクセスを悪用したラテラル ムーブメントなどに関連した継続的なリスクをもたらします。これらのリスクは、VPNが欠点の多いアクセス ソリューションとして認識される要因となっています。

VPNは財政面および運用面でIT部門に大きな負荷をかけており、回答者の41%が維持管理に関連する過剰なリソース コストを問題として挙げています。古いインフラを保護するためには、パッチ適用、トラブルシューティング、ログの監視を絶え間なく繰り返す必要があります。その結果、担当部門はこれらの作業に追われ、より価値の高い業務に集中できなくなっています。

その他に、VPNがきめ細かなアクセス制御を適用できないことも重大な欠点として挙げられています(35%)。VPNは、アイデンティティーに基づいて特定のアプリケーションへのアクセスを許可するのではなく、無制限のネットワーク接続を広範に提供するため、内部脅威のリスクが高まり、攻撃者によるラテラル ムーブメントの可能性が大幅に増加します。また、26%がVPN コンセントレーターなどのデバイス管理に伴う運用負荷を挙げており、リモート接続を維持するためのハードウェア アプライアンス、ネットワーク トンネル、アクセス ゲートウェイの保守がいかに複雑であるかが浮き彫りになっています。クラウドネイティブ アプリやリモート ワークが主流となった現代では、こうした複雑さはもはや受け入れられないものとなっており、より俊敏でスケーラブルなソリューションが求められています。

IT およびセキュリティ部門は VPN の管理においてどのような問題やリスクに直面していますか？

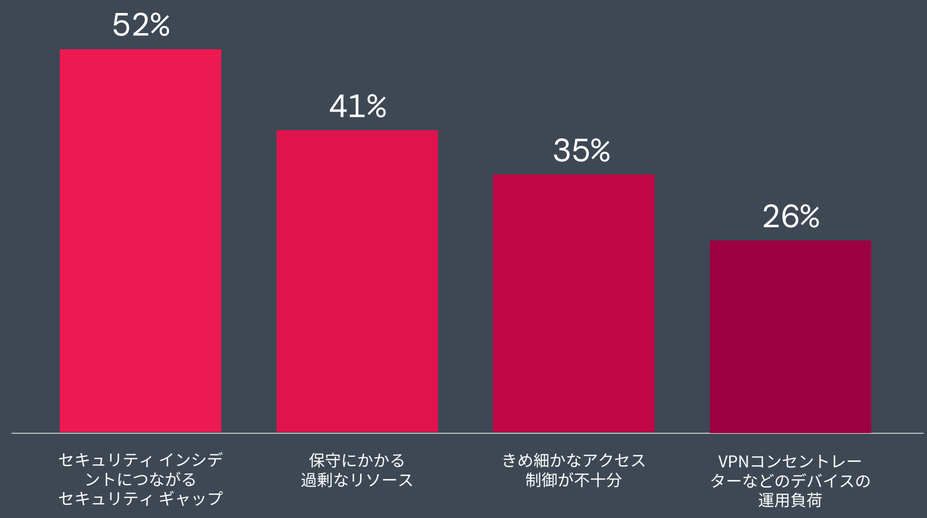


図 13： VPN の管理において IT およびセキュリティ部門が直面している問題やリスク

これらの課題に対処するには、ネットワークベースの VPN アクセスから、クラウド型のゼロトラスト モデルに移行する必要があります。ゼロトラストを採用することで暗黙の信頼が排除され、攻撃対象領域の削減と IT 業務の効率化が可能になります。さらに、VPN 関連の運用負荷の削減、アクセス管理の簡素化、大規模なセキュリティ リスクの最小化も実現します。IT 部門は定期的な保守業務の負担から解放されるため、予防的なセキュリティ対策に集中しながら、より迅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るようになります。

課題と負担を生み出す VPN の管理

VPN インフラの管理は、IT 部門の大きな負担となっています。特に、信頼性、パフォーマンス、保守に関連する管理負荷が主な懸念事項として挙げられています。なかでも、VPN 接続の安定性の問題は深刻であり、回答者の 54%がこれを指摘しています。IT 部門は VPN の安定稼働を維持するのに苦労しており、頻発する接続障害が生産性の低下やセキュリティ リスクの増加、従業員のストレスを招いています。

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も大きな課題 (50%) です。特にクラウドファーストの環境では、VPN が遅延、切断、不安定な接続スピードを引き起こすことが多いため、この課題は深刻です。さらに、47% の IT プロフェッショナルが、頻繁なパッチ適用の必要性とリソースの費用を主な阻害要因として挙げており、恒常的な脆弱性の軽減と古いシステムの維持が運用上の大きな課題となっていることがわかります。

このような課題が原因で、複数の大規模な侵害が発生しています。2023 年 12 月から 2024 年初頭にかけて、複数の政府機関が VPN 関連の攻撃の標的となりました。広く知られた脆弱性へのパッチ適用の遅れから、攻撃者は古い VPN ソフトウェアを悪用し、不正なネットワーク アクセスを成功させました。この事例は、専任の IT 部門を持つ組織であっても、事後対応型のパッチ適用では不十分であることを示すものであり、不完全な VPN の防御が重要な業界を新たな脅威にさらしてしまうことを証明しています。

VPN インフラは、接続のトラブルシューティング、セキュリティ パッチの適用、パフォーマンスの最適化に大量の IT リソースを消費します。そのため、組織は VPN ベースのアクセスが長期的に適切なソリューションであるのかどうかを再評価する必要があります。VPN コンセントレーターおよびファイアウォールや NAC などのネットワーク アプライアンスからクラウドネイティブ アーキテクチャーにリプレースすることで、IT 部門はインフラのボトルネックを解消し、パッチ適用のサイクルを短縮するとともに、接続障害に対する手動のトラブルシューティングを排除できます。

ポリシーに基づく最小特権アクセスにより、ユーザーは許可されたアプリケーションにのみ接続され、複雑なファイアウォール ルールやネットワーク セグメンテーション ポリシーの管理負荷も軽減されます。クラウド型のゼロトラスト モデルに移行することで、VPN 関連のボトルネックを解消しながら、シームレスかつポリシーに基づいたアプリケーション アクセスを確保できます。ネットワーク インフラの管理、ソフトウェアへのパッチ適用、複雑な拡張作業などは大幅に削減されます。

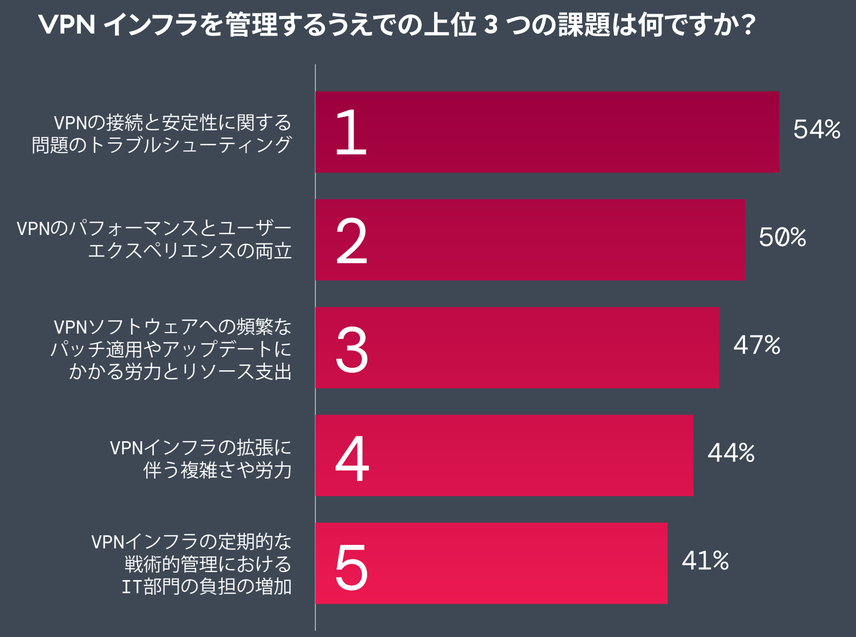


図 14： VPN インフラを管理する IT 部門の主な課題

過度に広範な VPN のアクセス制御：重大なセキュリティ ギャップ

多くのVPNのセキュリティ リスクの根本原因は、そのアクセス モデルにあります。現在も大多数の組織が、アプリケーションごとに厳格なアクセスを提供するのではなく、広範なネットワーク アクセスを許可し、暗黙の信頼モデルを採用しています。そのため、重要なシステムが危険にさらされています。

調査の結果、組織の52%が現在も静的なネットワーク ファイアウォール ルール(28%)や認証済みユーザーのオープン アクセス(24%)など、古いアクセス モデルを使用していることが明らかになりました。これらの古い制御により、攻撃者は検出されることなくネットワークを横断し、権限を昇格させられるようになります。そして、アクセスに成功すると、簡単に重要なデータを盗み出すことができます。

最近のインシデントは、このような広範なアクセスの危険性を露呈しています。2024年初頭、Global Affairs Canada (GAC)は、従業員がオタワ本社にアクセスするために使用していたVPNが侵害されるという重大なセキュリティ侵害を経験しました。攻撃者はVPNの脆弱性を悪用し、不正にネットワークへのアクセスを得て、機密情報を漏洩させた可能性があります。この事例は、無制限の過剰な権限を持つネットワーク アクセスが、攻撃者にとってラテラル ムーブメントやさらなる侵入を容易にする理想的な環境を作り出すことを証明しました。

これらのリスクを軽減するには、暗黙の信頼を排除し、アイデンティティーに基づいたきめ細かなアクセス制御を行う必要があります。広範なネットワークベースのアクセス モデルから直接的なアプリケーションレベルのセグメンテーションに移行することで、ユーザーは自分のロールに必要な特定のリソースにしかアクセスできなくなるため、攻撃対象領域が大幅に削減し、ラテラル ムーブメントを防止できます。

VPN ユーザーのアプリケーションへのアクセスをどのように定義していますか？

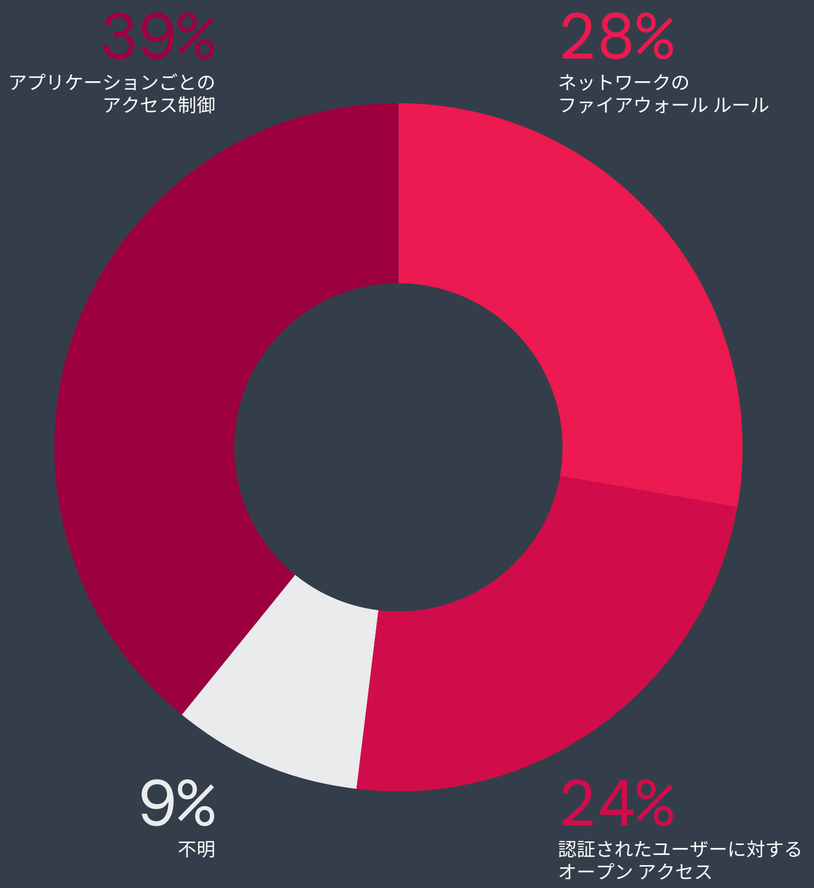


図 15: 組織が VPN ユーザーのアプリケーションへのアクセスを定義する方法

VPN のリプレース：安全なアクセスへの移行

セキュリティの脆弱性の増大、ユーザー エクスペリエンスの課題、VPN の保守の高負荷により、組織は ZTNA などの安全なアクセスを提供する最新技術への移行を加速させています。この変化からも、もはや VPN ではセキュリティや運用に関する最新の要件を満たせないという認識が広がっていることがわかります。

この勢いを裏付けるように、回答者の 65% が VPN から移行中、または来年中に移行する予定と回答しています。

VPN からの脱却が進むなか、組織が優先すべきは、広範なネットワーク接続ではなく、アプリケーションレベルのきめ細かなアクセスを適用するクラウド型のセキュリティ モデルの採用です。ZTNA は、ユーザーを企業ネットワークに直接接続させず、アイデンティティーとセキュリティ態勢に基づいて必要なリソースにのみアクセスできる仕組みを提供することで、VPN に伴うリスクを解消します。このアプローチにより、セキュリティの強化、業務の簡素化、ユーザーエクスペリエンスの向上が実現します。そのため、VPN からの移行は現代の組織にとって緊急かつ必須の取り組みとなっています。

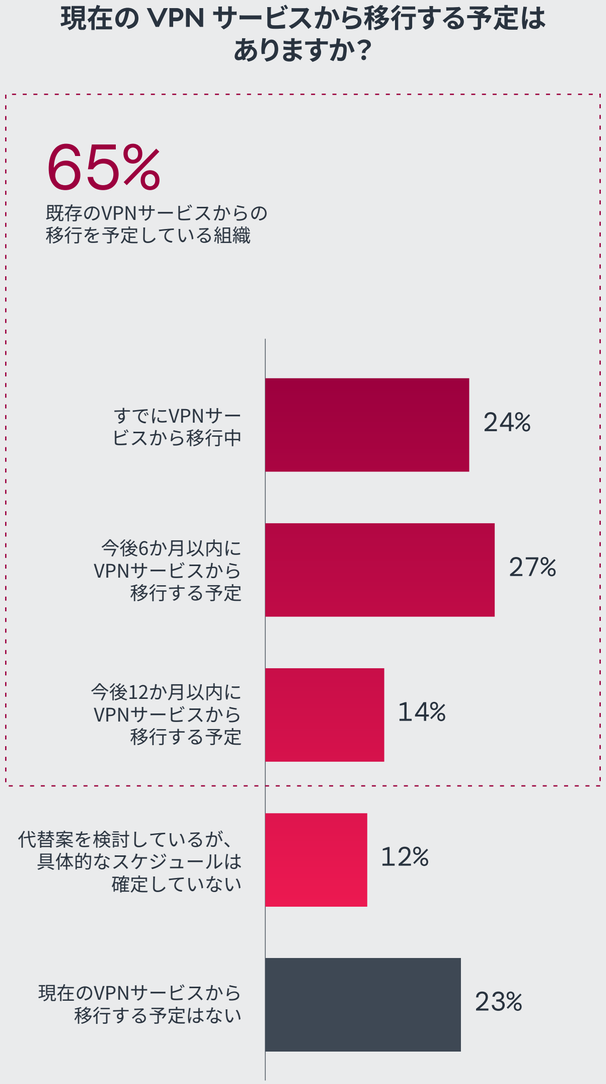


図 16： 既存の VPN サービスから移行する組織の計画

ゼロトラストの導入

VPN からゼロトラストへの移行がさらに加速

VPN から脱却する傾向が強まるにつれ、大多数の組織がゼロトラスト アーキテクチャーに移行して、きめ細かなアクセス制御を実装し、攻撃対象領域を減らし、ユーザーの生産性を向上させています。このパラダイム シフトの勢いは調査結果にも表れており、今後 1 年以内にゼロトラストを導入する予定の組織は 81%にも上り、そのうち、35% がすでにゼロトラスト ソリューションを導入中であり、24% が 6 か月以内に導入、22%が翌年の導入を予定しています。この結果からも、VPN などの従来のアクセス技術をリプレースするうえで、ゼロトラストが業界を牽引する戦略となっていることは明らかです。

ゼロトラストの導入を成功させるには、セキュリティ部門と事業運営部門の連携が必要です。組織はリスク評価を行うことで、リモート アクセス、サードパーティー統合、重要なアプリケーションなど、最も脆弱なアクセス ポイントを特定し、それに応じてゼロトラストの導入を優先する必要があります。ポリシーの施行に自動化を活用すれば、管理負荷を削減しながら移行を加速できます。

ゼロトラスト戦略を採用するためにどのような計画を立てていますか?

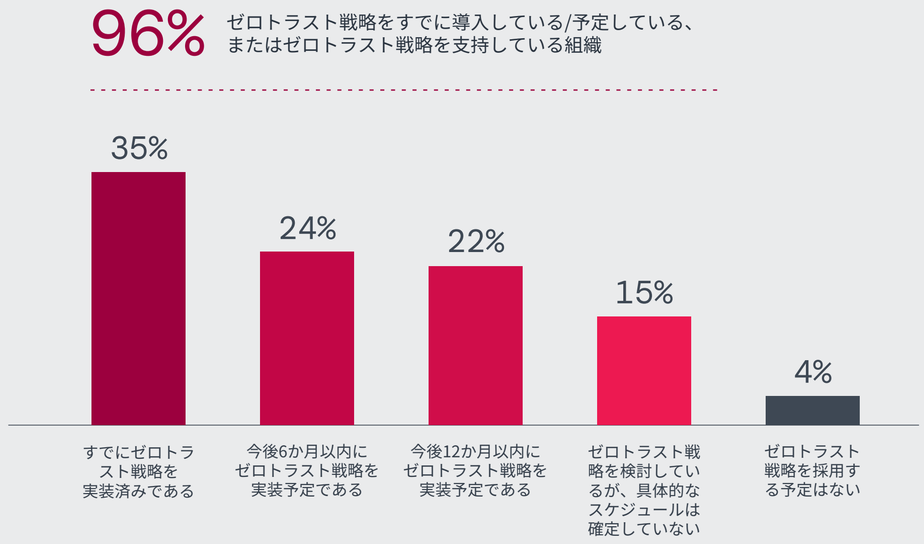


図 17: ゼロトラスト戦略を実装する組織の計画

ゼロトラストの優先事項：導入を後押しするリモート ワーク

従来のVPNからの脱却は、注目すべき大きな変革です。組織はゼロトラスト アーキテクチャーに移行することで、セキュリティ ギャップに対処し、IT業務を合理化しながら、分散したリモート ワーカーのニーズを満たそうとしています。この戦略的な転換は、ゼロトラストがVPNリスクを軽減し、セキュリティ管理を簡素化する最新のソリューションとして注目されていることを意味します。

調査の結果、リモートで作業する従業員の保護がこの変革を後押しした主な理由であることがわかり、組織の37%がリモート ワーク、28%がハイブリッド ワークのセキュリティを最優先事項として挙げています。この結果は、アプリケーションごとの直接接続を提供するセキュリティ モデルが普及している現在の傾向と一致しています。このモデルでは、従来のVPN設定で必要とされる複数のポイント製品が不要になるため、複雑さを最小限に抑えられます。

ゼロトラスト フレームワークを実装すると、セキュリティが強化されるだけでなく、他のセキュリティ ソリューションを管理する運用上の負担も軽減されます。セキュリティ ポリシーと制御を一つの統合システムに集約することで、組織は管理負荷を削減し、より効率的に運用を進められるようになります。たとえば、1回のスキャンで複数のポリシー アクションを実行するゼロトラスト プラットフォームでは、さまざまなソリューションを統合する必要がなくなるため、堅牢なセキュリティを確保しながら、ユーザー エクスペリエンスを簡素化できます。

ゼロトラスト アーキテクチャーでリモート ワークやハイブリッド ワークを効果的に保護するには、複雑さを最小限に抑えるセキュリティ対策の統合に注力する必要があります。統一されたゼロトラスト プラットフォームを実装することで、さまざまなセキュリティ機能を統合できるため、複数のポイント製品が不要になり、管理が簡素化されます。このアプローチにより、セキュリティと運用効率が向上し、IT 部門は複雑なセキュリティ ツールの管理ではなく、戦略的な取り組みに集中できるようになります。

ゼロトラスト ソリューションを導入する主なユース ケースは何ですか？

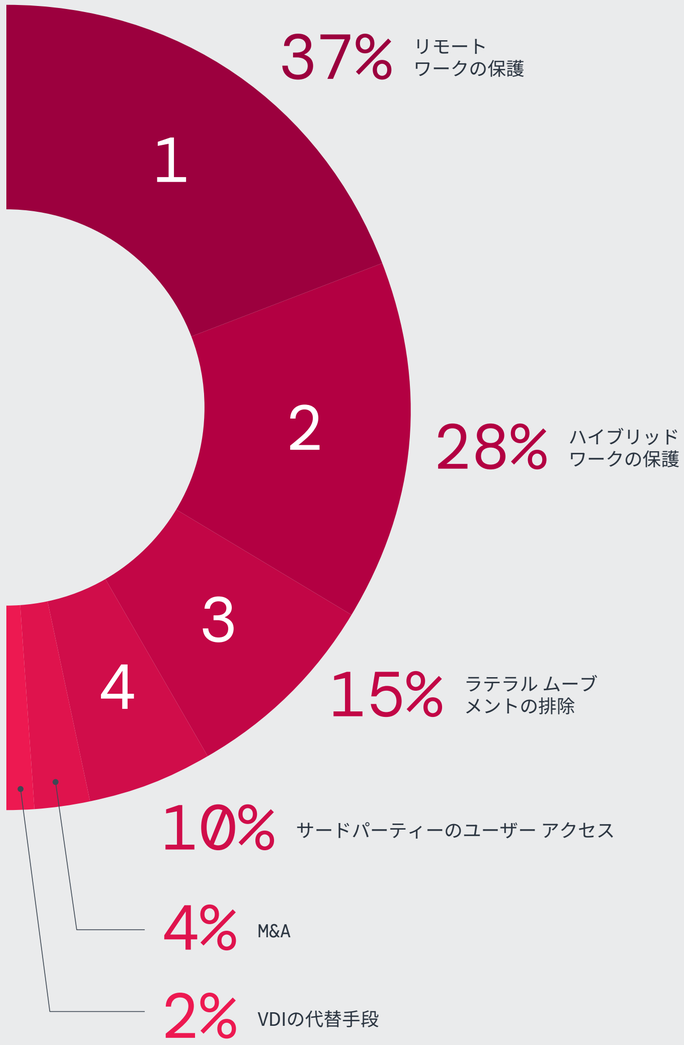


図 18： 組織におけるゼロトラスト ソリューションの主なユース ケース

VPN からゼロトラストに移行する主なメリット

ゼロトラスト ソリューションの導入は、組織のセキュリティを変革します。特に、管理の簡素化、パフォーマンスとスケーラビリティーの向上、攻撃対象領域の大幅な削減、リソース効率の向上など、安全なアクセスにとどまらない広範なメリットをもたらします。VPNモデルからゼロトラストへの移行は、単なるツールのアップグレードではなく、リモート アクセス戦略全体を長期的な視点で強化するものです。

回答者の大多数(76%)が、セキュリティとコンプライアンスの向上を主なメリットと考えています。この結果は、暗黙的なネットワーク アクセスをゼロトラストにリプレースすることで、ランサムウェア、認証情報の窃取、ラテラル ムーブメントのリスクを軽減できることを強調しています。

さらに、64%が管理の簡素化、スケーラビリティー、ユーザー エクスペリエンスの向上を主なメリットとして挙げています。これは、ゼロトラストによって、VPNコンセントレーターの管理や定期的なパッチ適用、アクセスのトラブルシューティングといった運用上の負担が大幅に軽減されるためです。

回答者の半数近く(45%)が、VPNからゼロトラスト ソリューションへの移行は完全なゼロトラスト アーキテクチャー導入に向けた重要な一歩と考えています。

さらに34%が、ゼロトラストの優れたスケーラビリティーと柔軟性を挙げており、リモート ワーカーやハイブリッド ワーカーを保護するためのより効果的なソリューションと捉えています。その他のゼロトラストの価値として、エンドユーザー エクスペリエンスの向上(32%)、ITシステムとセキュリティ システム間のシームレスな統合(28%)、リソースの節約による運用コストの削減(18%)などのメリットが挙げられました。これらのメリットを総合すると、組織が従来のVPNを急速に廃止し、ゼロトラストを優先する理由がわかります。

ManpowerGroupは、人材ソリューションの世界的なリーダー企業であり、現在はゼロトラストを活用してアクセスを保護しています。膨大な数のリモート ワーカーをサポートするという課題に直面した同社は、従来のVPNインフラから脱却し、Zscalerのゼロトラスト ソリューションの導入を決定しました。同社はわずか18日間で3万人以上のユーザーに安全なアプリケーションへのアクセスを拡張し、中断のない事業継続性を達成しながら、ヘルプ デスクのチケットを97%も削減しました。この導入事例は、ゼロトラスト アーキテクチャーが短期間で拡張でき、運用を簡潔化しながら、生産性とセキュリティも向上させることを証明しています。

VPN ソリューションからゼロトラスト ソリューションに移行した場合、以前の VPN ソリューションと比べてどのようなメリットがあると思いますか?

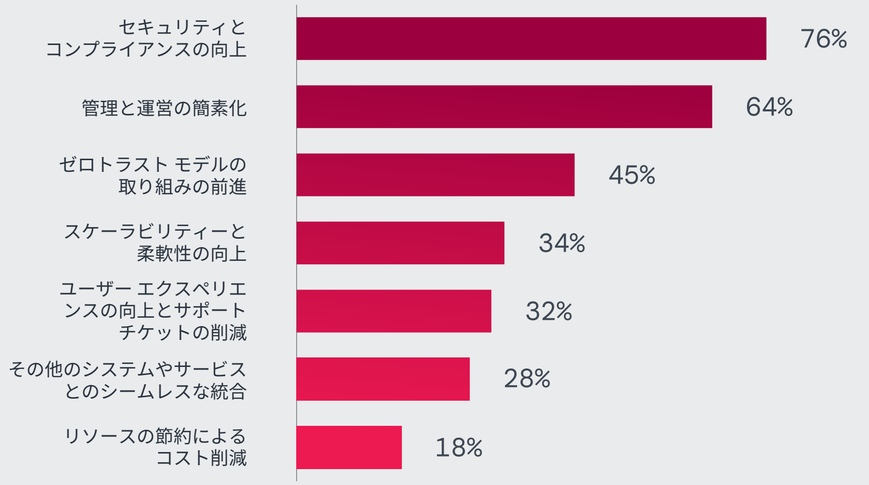


図 19: 以前の VPN ソリューションと比較したゼロトラスト ソリューションの主なメリット

ゼロトラストの導入は、VPN に基づくネットワーク アクセスを廃止し、アプリケーション単位での直接接続に切り替えるといった戦略的な変更から始めることが重要です。こうした取り組みにより、ラテラル ムーブメントのリスクを抑えることができます。組織は、リモートやサードパーティーのユーザー接続の保護といった重要なユース ケースから既存のアクセス方法を見直し、その後、ゼロトラストを IT エコシステム全体に展開していくことができます。また、単一のポリシー セットでアクセス ポリシーを自動化し、アイデンティティーベースのセキュリティを統合することで、ゼロトラスト管理をさらに簡素化しながら、分散したシステム間でのスケーラビリティーを実現できます。これらのインテリジェントなフレームワークにより、IT 部門は俊敏性や効率性を犠牲にすることなく、リアルタイムのセキュリティ制御を維持できるようになります。

VPN のリスクに関する 2025 年の予測

今後も発生し続けるVPNの重大な脆弱性

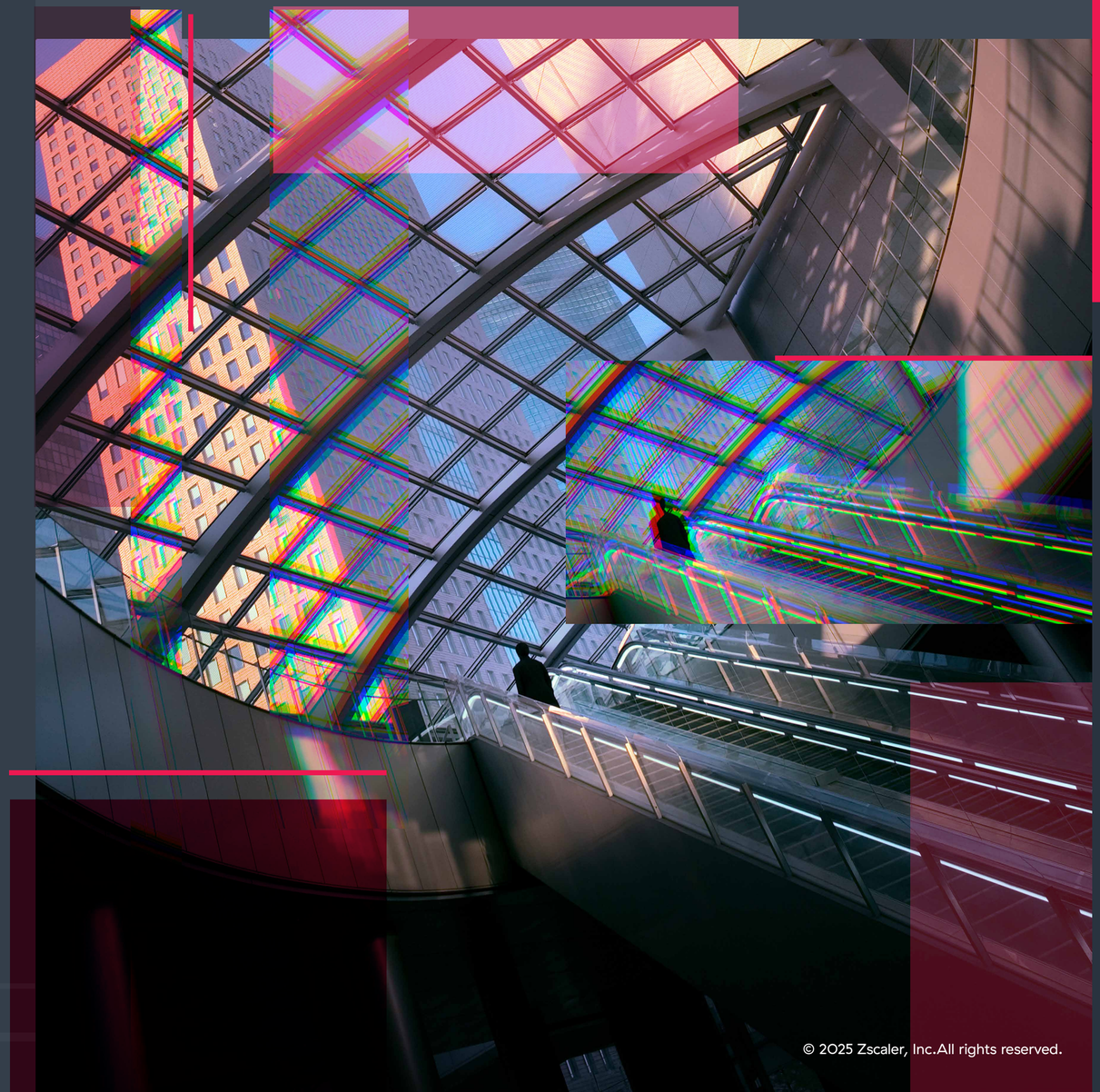
VPNの悪用は近年増加していますが、2025年にはその勢いがさらに増すと予測されます。VPNは組織のネットワークをインターネットにさらすため、脆弱性の特定と悪用が容易であり、攻撃者の格好の標的となっています。組織が適切なタイミングでVPNの脆弱性を修正できずにいるなか、攻撃者は2025年1月に発生したIvanti Pulse Secureの侵害など、新たに発見された深刻な脆弱性を次々と悪用し続けています。セキュリティ研究者や攻撃者は、VPNインフラを積極的に調査しているため、重大なCVEの開示が今後も続く可能性が高いとみられます。

ランサムウェア グループによるVPNの悪用の激化

回答者の92%が、パッチ適用されていないVPNの脆弱性に懸念を示しています。ランサムウェアの攻撃者は、初期アクセスを確保する主な手口としてVPNの既知のゼロデイ脆弱性を引き続き悪用すると考えられます。Ransomware as a Service (RaaS)グループは、修正されていない脆弱性を持つ公開されたVPNを定期的にスキャンし、IT部門が対応する前にランサムウェアを展開します。2025年1月に発生した米国の医療機関を標的としたランサムウェア キャンペーンでは、VPNのセキュリティ ギャップが攻撃者に重要なシステムへの直接的な侵入を許してしまうことが証明されました。このような攻撃が自動化されるにつれて、ゼロトラスト セキュリティに移行する必要性はさらに緊急性を増すと予測されます。

より破壊的な攻撃につながるVPN経由のラテラル ムーブメント

攻撃者はVPNが提供する広範なアクセスを悪用し、ラテラル ムーブメント、権限昇格、データ窃取を実行します。これは、攻撃者や国家支援型アクターが用いる最も効果的な手口にあたります。組織の71%がこのリスクを懸念しているなか、その解決策として頻繁に浮上するのがネットワーク セグメンテーションです。しかし、実装プロセスは複雑で、多くの組織が効果的に管理するスキルを持つ人材を十分に確保できていません。その結果、セグメンテーション プロジェクトの完了に数か月かかったり、プロジェクトが完全に停止したりする事態が発生しています。これらの課題を軽減するには、ゼロトラスト セグメンテーションを導入する必要があります。このアプローチはアプリケーションへの厳格な最小特権アクセスを適用し、従来のネットワーク セグメンテーションに伴う運用負担を軽減しながら、ラテラル ムーブメントの経路を効果的に排除します。



引き続き主な脅威ベクトルとなるサードパーティーによるVPNアクセス

回答者の93%がサードパーティーのVPNの脆弱性に懸念を表明しており、攻撃者は今後も脆弱な外部のアクセス ポイントを標的にすると予測されます。盗まれたサードパーティーの認証情報やVPNアクセスの設定ミスは、攻撃者がネットワークに侵入する主な経路となっています。2024年に発生したEnterprise Financial Group (EFG)の侵害では、攻撃者がサードパーティーのVPN接続を悪用して組織の環境に侵入しました。多くの組織ではサードパーティーのアクセス権限が可視化されていないため、セキュリティ ポリシーの施行が困難になっています。組織はゼロトラスト フレームワークに移行して、すべての外部接続に厳格な最小特権アクセスを適用し、継続的な検証を行うことで、これらのリスクを軽減する必要があります。

AIによるVPNの悪用の増加

AIを悪用したサイバー攻撃の台頭は、VPNのセキュリティにこれまで以上の影響を与える恐れがあります。攻撃者はAIを悪用して、偵察の自動化、巧妙なパスワード スプレー攻撃、迅速なエクスプロイト開発を実行し、VPNの認証情報を大規模に侵害するようになります。さらに、AIを悪用した回避技術により、重大な被害が発生する前にVPN経由の侵入を検出することがますます困難になります。一方で、AIを活用したVPNセキュリティ ソリューション自体が予期せぬセキュリティ ギャップを生み出し、新たな攻撃ベクトルを提供するリスクもあります。AIによる脅威が拡大するにつれて、組織は継続的なアイデンティティー検証やゼロトラスト アクセス制御などの予防的なセキュリティ対策を採用する必要があります。

社会の注目を集めるVPN関連の大規模な侵害

2024年に相次いだ大規模な侵害を背景に、組織はVPN関連のサイバー インシデントの開示をさらに強く求められるようになると考えられます。サイバーセキュリティ リスクの透明性を義務付ける新しいSEC規制により、VPNを悪用された組織は、規制当局による監視の強化、評判の低下、さらには潜在的な罰金に直面する可能性があります。VPNが依然として攻撃の主な侵入口として悪用されている状況を受け、組織は従来のアクセス モデルを見直さざるを得なくなり、ゼロトラスト セキュリティへの移行がさらに進むと予測されます。

VPNの利用の減少に伴うゼロトラストへの投資拡大

組織の65%がすでにVPNから移行しているか、1年以内の移行を予定しているという調査結果が示すように、ゼロトラスト セキュリティへの投資は増加し続けており、リモート アクセス環境が根本的に変わろうとしています。規制要件やサイバー保険の義務化により、組織はVPNからの脱却を余儀なくされています。これは、従来のソリューションではセキュリティ、スケーラビリティー、コンプライアンスの要件を満たせないためです。ゼロトラストの導入は、サイバー リスクを軽減するだけでなく、VPNコンセントレーター、ネットワーク アプライアンス、継続的なパッチ適用サイクルを維持するための高額なコストも排除するため、VPNはますます旧式のソリューションとみなされるようになり、業界全体でゼロトラスト セキュリティ モデルへの移行が加速すると考えられます。

これらの予測は、ゼロトラストの導入を遅らせるとVPNの脆弱性を悪用した攻撃から組織を十分に保護できないという共通の認識が広がっていることを示しています。将来の安全なアクセスを実現する鍵は、事後対応型のパッチ適用ではなく、事前予防型のリスク軽減にあります。今こそVPNから脱却する時です。

安全なアクセスを実現するための ベスト プラクティス

VPN のリスクの軽減とゼロトラスト セキュリティの強化

1. **ネットワークベースのアクセスを排除して攻撃対象領域を最小化**
   VPNとネットワークベースのアクセスを段階的に廃止し、アプリケーションごとの直接接続を採用することで、攻撃者がアクセス ポイントの脆弱性を悪用して、ネットワークに不正に侵入するリスクを防ぎます。調査結果によると、組織の54%がVPNの最大の課題としてセキュリティ リスクを挙げており、VPNとファイアウォールベースのセキュリティ モデルを廃止する必要性が高まっています。

2. **インラインの脅威対策で初期侵入を阻止**
   暗号化されたトラフィックと暗号化されていないトラフィックをすべて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、ランサムウェア ペイロードがユーザーに到達する前にブロックします。組織の92%がVPNの脆弱性を狙ったランサムウェアを懸念しているとおり、リアルタイムのトラフィック検査とポリシーベースのブロックは非常に重要です。クラウドネイティブのセキュリティ モデルにより、オンプレミスのファイアウォールが不要になり、攻撃対象領域が削減されます。

3. **認証とアイデンティティーでセキュリティを強化**
   FIDO2認証情報や生体認証、ハードウェア トークンなど、フィッシングに強い多要素認証(MFA)を実装し、ユーザー アクセスを検証します。SMSベースのMFAやプッシュ通知など、攻撃者が頻繁に回避する従来の認証方法は避けることが重要です。1回限りの認証に頼るのではなく、アイデンティティーベースのセキュリティを継続的な検証と統合します。

4. **ZTNAによるコンテキストベースの最小特権アクセスを適用**
   広範なVPNアクセスからゼロトラスト ネットワーク アクセス(ZTNA)に移行すれば、ユーザーはネットワークではなく、許可されたアプリケーションにのみ接続されるようになります。アイデンティティー、デバイス ポスチャー、リアルタイムのリスク分析に基づくきめ細かなジャストインタイム(JIT)のアクセス制御により、ユーザーは必要なときに必要なものにだけアクセスを許可されます。

5. **ゼロトラスト セグメンテーションでラテラル ムーブメントを排除**
   ネットワークではなくアプリケーションにユーザーを直接接続させることで、攻撃者が初期アクセスを得た場合でもシステム間の移動が防止されます。ゼロトラスト セグメンテーションとアイデンティティー対応型のマイクロセグメンテーションにより、ユーザーが侵害された場合でも、攻撃者は他のリソースに移動したり権限を昇格させたりすることはできません。ZTNAは、ラテラル ムーブメントの主な要因であるVPNトンネルを排除します。

6. **アイデンティティーに基づいた制御でサードパーティーなどの外部アクセスを保護**
   サードパーティー、ベンダー、請負業者に対して最小特権アクセスを施行し、厳格なセッション制御、デバイスの正常性チェック、継続的な監視を行います。サードパーティーのVPNアクセスをZTNAにリプレースすることで、ベンダーの認証情報が侵害された際のリスクを大幅に低減できるため、サードパーティーのVPNリスクを懸念する組織の93%にとって大きなメリットとなります。

7. **統合されたゼロトラスト ポリシーでデータ保護を強化**
インラインの情報漏洩防止(DLP)とクラウド アクセス セキュリティ ブローカー(CASB)による制御を展開し、不正なデータの移動をリアルタイムで検査、暗号化、防止します。ゼロトラスト セキュリティ フレームワークでは、SaaSアプリケーションやクラウド環境でも、すべてのユーザー トラフィックが確実に検査および制御されるようにします。

8. **AIを活用したセキュリティと継続的な監視を展開**
AIによるリアルタイム分析、デセプション テクノロジー、行動検出の自動化を活用することで、脅威が深刻化する前に阻止します。ZTNAは、リアルタイムのリスク スコアリングを提供し、侵害されたアカウントが機密性の高いアプリケーションにアクセスできないようにします。日々の予防的な脅威ハンティングとリスクベースのアクセス制御により、侵害の影響を大幅に軽減します。

9. **セキュリティ態勢を継続的に評価して適応**
自動化されたリスク評価、侵入テスト、敵対者シミュレーションを行い、ゼロトラスト セキュリティ ポリシーを動的に調整します。大規模な侵害は、セキュリティの設定ミスや不十分なポリシー施行が原因で発生します。ヒューマン エラーを減らすには、自動化を通じて適応性の高いポリシーを施行することが重要です。

10. **VPNインフラを排除し、セキュリティ ポリシーの施行を自動化**
クラウド型のゼロトラスト モデルを採用することで、VPNコンセントレーター、ファイアウォール ルールの管理、手動のアクセス制御リストが不要になります。ZTNAは、コンプライアンスの変更、規制の更新、進化するサイバー脅威にリアルタイムで適応する動的なセキュリティ ポリシーを、手動の構成やハードウェアなしで実現します。

これらのベスト プラクティスを実装することで、組織は回復力の高いゼロトラスト セキュリティ フレームワークを構築し、VPN に関連するセキュリティ リスクを排除できます。また、継続的な検証、最小特権アクセス、予防的な脅威軽減も可能になります。

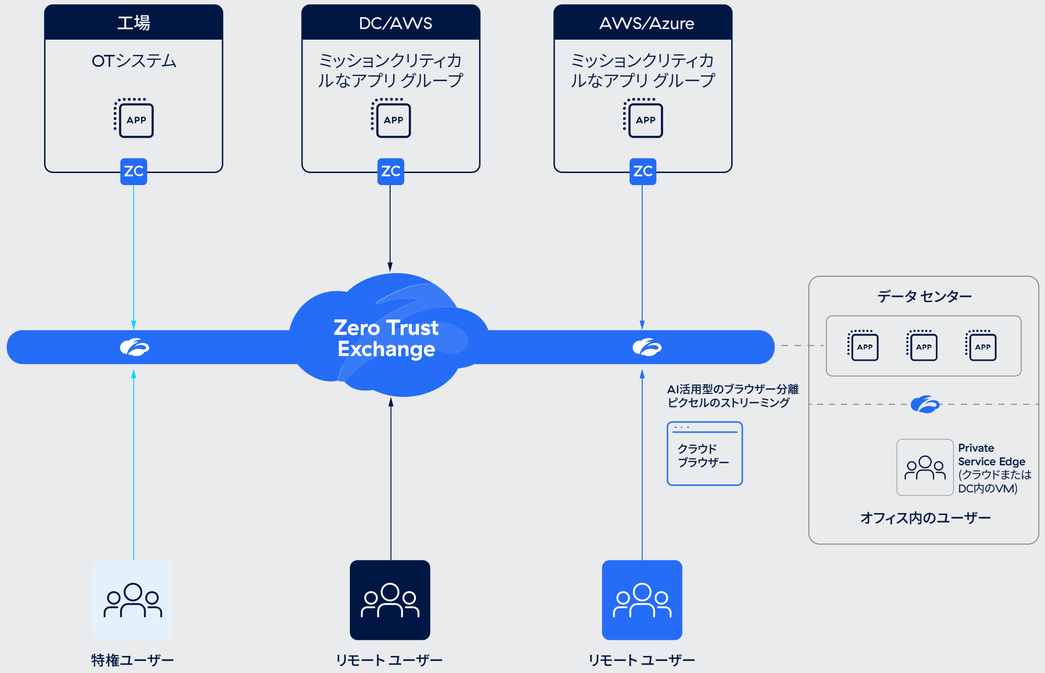
Zscaler が提供する
安全なユーザー　アクセス

従来のVPNとファイアウォールは、ユーザーをネットワーク上に直接配置するため、組織の攻撃対象領域を大幅に拡大します。この広範なアクセスにより、攻撃者は脆弱性を悪用して侵入し、環境内で水平方向に移動することが容易になります。脅威が常に進化し、ハイブリッド ワークが標準になるなかで、こうした旧式の技術への依存は深刻なセキュリティ リスクを招くため、より安全な適応型ソリューションが求められます。

Zscaler Private Access™ (ZPA)は、VPNなどの従来のリモート アクセス ソリューションに代わる安全でスケーラブルなクラウド ネイティブ ソリューションです。ZPAは、プライベート アプリケーションへの直接接続を提供することで、すべてのユーザーのゼロトラスト アクセスを実現します。攻撃対象領域を最小化するために、アプリケーションはZscaler Zero Trust Exchange™プラットフォームの背後に隠されます。このアプローチでは、AIを活用したユーザーとアプリケーション間のセグメンテーションによってラテラルムーブメントを排除するとともに、統合型のトラフィック検査やアプリケーションとデータの保護機能で高度な脅威から組織を守ります。

ZPAは数時間で展開でき、従来のVPNやリモート アクセス ツールから包括的なゼロトラスト プラットフォームに移行できます。世界最大のセキュリティ クラウドを活用することで、世界中のあらゆる場所のユーザーに高速で信頼性が高く低遅延の接続を提供します。このクラウド ネイティブ アーキテクチャーは、柔軟なスケーラビリティーを確保し、さまざまな地域に分散したハイブリッド ワーカーのニーズをシームレスにサポートします。

ZPAを使用すると、安全にクラウドファーストのハイブリッド ワーク モデルを導入できます。ZPAはリソースを不正アクセスから保護し、ユーザーの生産性を向上させ、組織が将来に向けて安全に拡張できるようIT運用を簡素化します。



Zscaler Private Access（ZPA）の主なメリット

攻撃対象領域の最小化によるランサムウェア攻撃からの保護

VPNの脆弱性は、ランサムウェア攻撃や認証情報の窃取につながるセキュリティ上の弱点を生み出します。ZPAは、すべてのアプリケーションをZero Trust Exchangeの背後に隠し、ユーザーに許可されたアプリケーションのみへのゼロトラストの直接接続を提供することで、このリスクを排除します。また、サードパーティー ベンダーや請負業者などの許可されていないユーザーがアプリケーションを見つけて水平方向に移動するのを防ぐことで、ランサムウェア攻撃から効果的に保護します。この仕組みにより、プライベート アプリだけでなく、VoIPやクライアント サーバー アプリのようなネットワークに接続されたアプリケーションなど、あらゆる種類のアプリケーションへのセキュア リモート アクセスが可能になります。さらに、ZPAは、包括的な事業継続性ソリューションを提供することで、業務の中断を最小限に抑え、組織が厳格なコンプライアンス要件を順守できるよう支援します。

脅威のラテラル ムーブメントの排除

ZPAは、ユーザーを特定のアプリケーションに直接接続させることで最小特権アクセスを施行し、ネットワーク内の他のアプリケーションへのアクセスを防止します。これにより、ユーザーとアプリケーション間のアクセスと適用されたポリシーに関する視覚的なインサイトが得られ、可視性と制御が向上します。ZPAのAIを活用したセグメンテーションは、アプリ セグメントとポリシーの推奨を自動的に生成し、セグメンテーションの実装を簡素化しながら、スケーラビリティーと堅牢なセキュリティを確保します。

きめ細かな可視化と分析

ZPAは、アプリケーションの使用状況、ユーザーの行動、アクセス パターンを詳細かつリアルタイムで可視化します。IT部門はこのデータを使用することで、潜在的な脅威の監視や監査、迅速な特定を行い、全体的なセキュリティ態勢を強化できます。また、規制順守の徹底にも役立ちます。

クライアントレス アクセスによるサードパーティーの脆弱性の軽減

ZPAのクライアントレス アクセス機能は、請負業者やパートナーがクライアントを必要とせずに任意のブラウザーを介してアプリケーションに安全に接続できるようにすることで、サードパーティーのアクセスを簡素化します。組織のネットワークから管理対象外デバイスを分離し、機密情報を保護するとともに、Google Chrome Enterprise Browserと統合してBYODのセキュリティを強化します。この最新のアプローチにより、コストを削減し、サードパーティーのアクセスに関連するリスクを最小限に抑え、従来のVDI管理への依存を解消します。

プライベート アプリの侵害の防止

ZPAは、ユーザーとプライベート アプリ間のすべてのトラフィックに対してインライン検査を実行することで、プライベート アプリの侵害と情報漏洩のリスクを最小限に抑えます。堅牢な情報漏洩防止機能により、機密情報の安全性を確保しながら、不正アクセスをブロックします。ZPAは、アプリケーションをパブリック インターネットから隠し、ゼロトラストの原則に基づいてユーザーとアプリ間の安全な接続を確保するため、攻撃対象領域の削減、ラテラル ムーブメントの防止、侵害からの保護が可能になり、全体的なセキュリティが大幅に強化されます。

ポリシー管理の簡素化と導入の迅速化

ZPAは、リモート アクセスの導入、ポリシー管理、ユーザーとアプリ間のセグメンテーションを簡素化することで、IT運用を合理化します。以前は時間を要していたユーザーのオンボーディング、パッチ適用、アップグレードなどの業務も数分で完了できるようになり、IT部門の負担が大幅に削減されます。一元管理と自動化されたポリシー推奨機能を備えたZPAにより、IT部門は業務効率を向上させ、運用を簡素化するとともに、日常業務ではなく戦略的な取り組みに集中できるようになります。

デバイス ポスチャーに基づいたアクセス制御

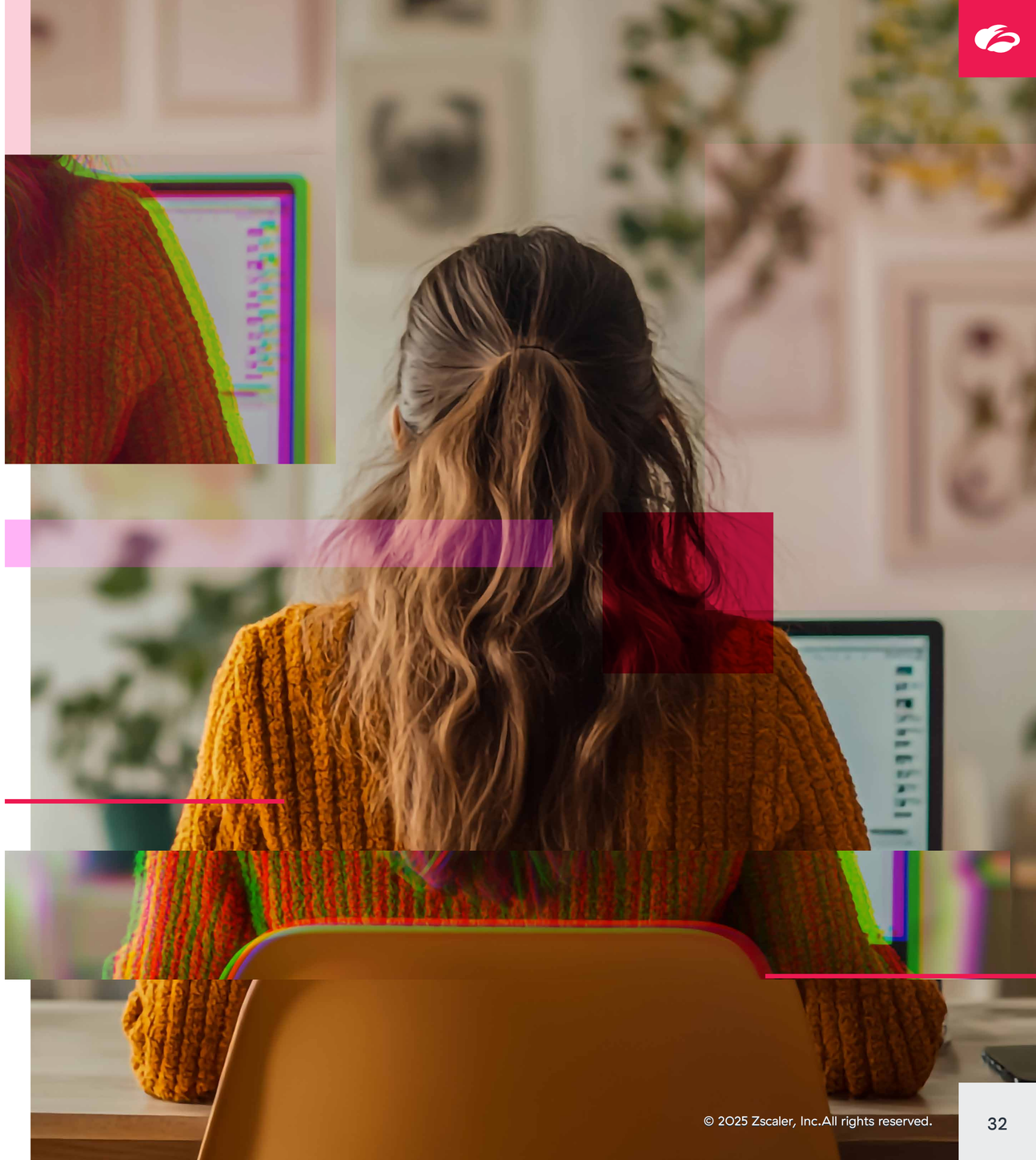
ZPAは、エンドポイント ポスチャー評価ツールと統合し、アクセスを許可する前にユーザー デバイスのセキュリティ態勢を確認します。これにより、準拠したデバイスのみが接続できるようになり、管理対象外デバイスや侵害されたデバイスに起因するリスクが軽減されます。

優れたユーザー エクスペリエンスの実現

ZPAは、業務に不可欠なアプリケーションへの高速でシームレス、かつ安全な接続を提供することで、最適なユーザー エクスペリエンスを確保します。中央集中型のデータ センターを介してトラフィックをバックホールするVPNとは異なり、ZPAはZero Trust Exchange経由でユーザーとアプリケーションを直接接続させるため、遅延が大幅に短縮され、ユーザーの場所がオンサイト、リモート、外出先のどこであってもアプリケーションのパフォーマンスが向上します。ZPAは、複数のログインとクライアントベースのソフトウェアの使用を最小限に抑えることで、アクセスを簡素化し、生産性を向上させます。さらに、ZPAの予防的な監視機能により、問題解決が効率化され、すべてのユーザーに中断のない高品質のアクセスが提供されます。

総所有コストの削減

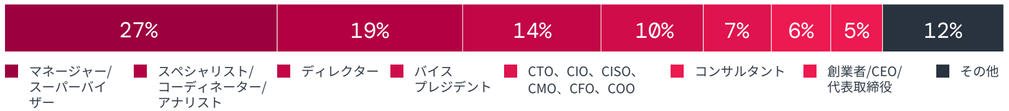
ZPAを導入することで、VPNやファイアウォール、NAC、VPNコンセントレーターなどの複数のポイント製品が不要になるため、総所有コストを大幅に削減できます。ZPAはクラウドネイティブのゼロトラスト アーキテクチャー上に構築されており、ハードウェアのサポート、保守、修理、更新に関連するインフラ コストを排除します。管理の簡素化とポリシー施行の自動化により、運用負荷が削減され、IT部門は時間とリソースを節約しながら、セキュリティとスケーラビリティーを向上させることができます。



調査方法と
回答者の内訳

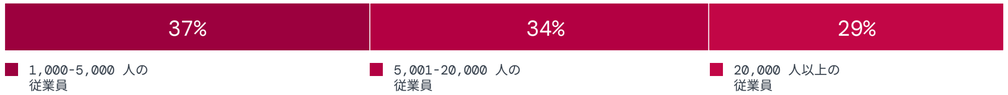
本レポートは、VPN のセキュリティ リスク、組織のアクセスの傾向、ゼロトラスト アーキテクチャーの導入状況を特定するために、2025 年初頭に IT およびサイバーセキュリティの専門家 632 人を対象に行われた調査の結果を基に作成されています。回答者には、さまざまな業界の経営幹部、IT セキュリティ担当者、ネットワーク インフラのリーダーが含まれます。本レポートの調査結果は、VPN の利用の減少とゼロトラストへの移行に関するデータに基づく洞察を提供し、アクセス セキュリティ戦略の近代化を目指す組織に重要な視点を提案します。

役職/職務

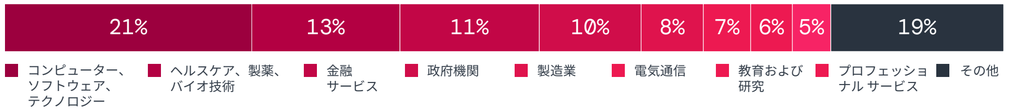


部門

会社の規模(従業員数)



業界



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.com/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 – サイバーセキュリティに関する信頼性の高いデータドリブンのインサイトを提供

Cybersecurity Insiders は、データに基づいた分析と第三者による検証を提供し、サイバーセキュリティのリーダーがデータドリブンかつ戦略的な意思決定を行えるよう後押しします。10 年以上にわたる研究と、60 万人を超える世界中のサイバーセキュリティ専門家のネットワークを基盤に、進化し続ける脅威への対応、新しい技術の評価、そして将来を見据えた戦略立案を支援する実用的な情報を提供しています。

当社は、サイバーセキュリティ ベンダーが研究結果を活用して、有意義な成果を達成できるよう支援します。市場レポートやウェビナーなどの強力な方法を通じて、信頼性、認知度、そして顧客との信頼関係を築きます。提供する内容は、ベスト プラクティスを紹介する CISO 向けガイド、ソリューションを検証する製品レビュー、購入者に役立つハウツー記事、ブランド評価を高める受賞実績まで多岐にわたります。

独自の配信方法とコンテンツを組み合わせることで、競争が激しいサイバーセキュリティ市場でも、ブランドが信頼を得て知名度を上げ、需要を創出できるようサポートします。

詳細はこちら：cybersecurity-insiders.com

Holger Schulze
Cybersecurity Insiders
CEO兼創設者

zscaler™ | Zero Trust Everywhere

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**