キーマンズネット

第 8 回：VPN が侵入口になっているのに、なぜ情シスはそれを使い続けるのか？

VPN の脆弱性を突いた攻撃が相次ぎ、侵入経路として悪用される事例が増えている。それでも多くの企業が VPN をやめられないでいる。コストや移行の複雑さをどう乗り越えるか、ZTNA だけに頼らない現実的な選択肢も含めて 2 本の記事で整理する。

守りきれない VPN、放置か脱却か？　セキュリティ対策の実態調査【2025 年版】

リモートアクセスのために「VPN」が企業で広く使われている。だが、VPN はランサムウェア攻撃で最も狙われる入口でもある。企業の現場では VPN のセキュリティをどの程度固めているのか、「脱 VPN」の動向についても探った。

業種や従業員規模を問わず、あらゆる企業がサイバー攻撃の標的となり得る現在、特に対応を緩めてはいけないのが「VPN」「EDR」「クラウド」の 3 領域だ。VPN は攻撃の侵入口として、EDR は侵入後の異常検知手段として、クラウドは情報資産の中枢として、それぞれ防御の要となっている。

本稿では、2025 年 6 月 18 日〜7 月 11 日にかけて実施したアンケート（回答数：216 件）の結果を基に、これら 3 領域における企業のセキュリティ対策の実態を明らかにする。近ごろアタックサーフェスとなっている VPN に焦点を当て、「脱 VPN」に向けた取り組みの現状についても詳しく解説する。

大企業 44.4%、中小企業 37.8%が「セキュリティ被害に遭った」

まず、自社がサイバー攻撃を受けた経験の有無について尋ねたところ、「攻撃を受けたことはない」が 41.7%、その一方で、「攻撃を受けたことはあるが、自社が標的だったかは不明」（16.7%）、「自社を明確に狙った攻撃があった」（12.5%）との回答も一定数見られ、合計すると約 3 割（29.2%）の企業が何らかの形で攻撃を受けた経験があると答えた（図 1）。

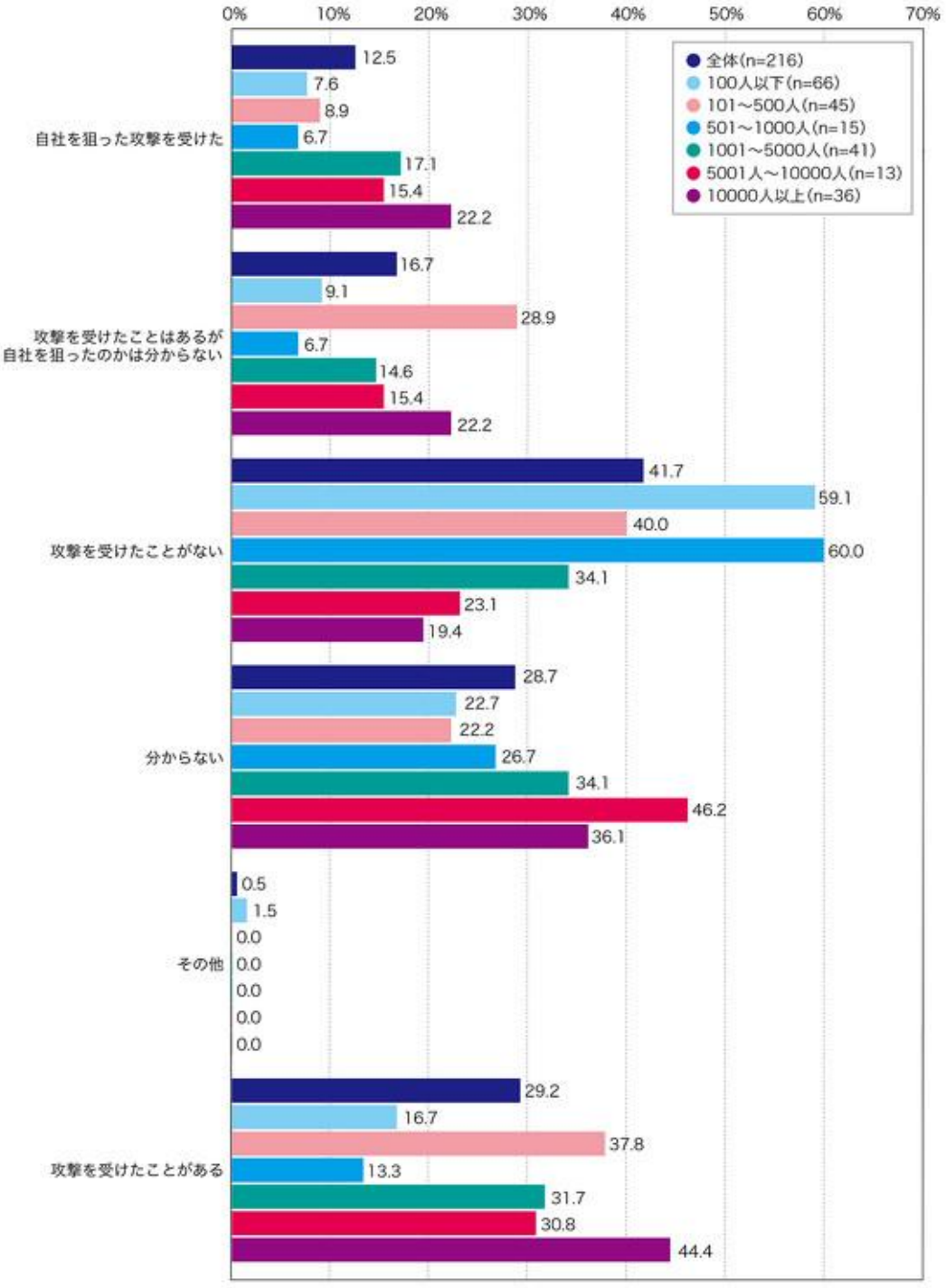


図 1　自社を狙ったサイバー攻撃を受けたことがあるか（従業員規模別）

この結果を企業規模別に分析すると、従業員 1 万人以上の大企業では 44.4%が攻撃経験ありと回答しており、高い水準を示した。また、101 人～500 人規模の中堅・中小企業においても 37.8%が攻撃を受けたと回答した。

さらに、攻撃を受けた企業のうち、過半数が「特に被害はなかった」とする一方で、一定割合が実被害を報告している点にも注目したい。「情報漏えい」（15.6%）、「マルウェア感染」（14.1%）、「システム停止」（14.1%）といったインシデントが複数挙がっており、特に「ランサムウェアによるデータ暗号化」（12.5%）や「業務停止」（9.4%）など、事業継続に影響する深刻なケースも見受けられた（図 2）。

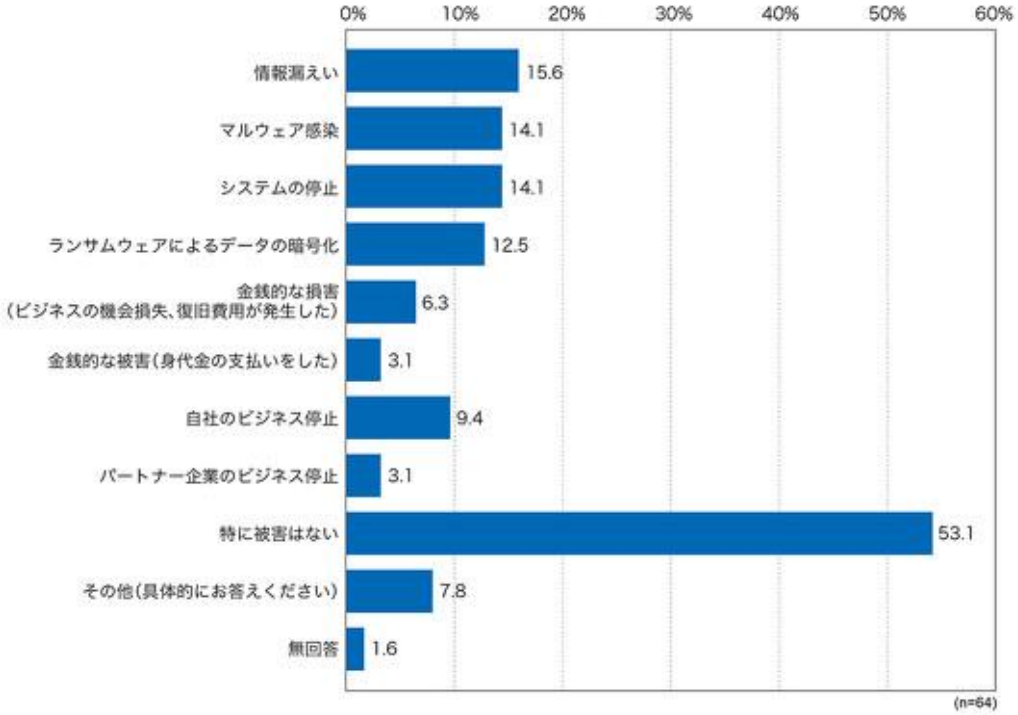


図 2　サイバー攻撃によって発生した被害

悩める「脱 VPN」、企業の対応に温度差　VPN セキュリティの実態

ランサムウェアの被害事例として、2024 年 6 月に発生した KADOKAWA およびドワンゴへの攻撃は記憶に新しい。IPA（情報処理推進機構）が発表した「情報セキュリティ 10 大脅威 2025（組織向け）」においても、「ランサム攻撃による被害」は 10 年連続で上位にランク入りしており、依然として企業にとって脅威であることに変わりはない。

2025 年 3 月に警察庁サイバー警察局が公表したレポートによれば、ランサムウェアの主な侵入経路として最も多かったのが VPN 機器だった。こうした実情を受けて、従来の VPN に依存しないアクセス環境、いわゆる「脱 VPN」への関心が高まりつつある。

本調査では、勤務先における VPN の運用状況と脱 VPN への取り組み状況、検討している VPN の代替ソリューションについても尋ねた。

従業員に VPN を「提供していない」が 42.1%と最多であったものの、「SSL VPN を提供している」（36.1%）、「IPsec VPN を提供している」（15.3%）となった（図 3）。

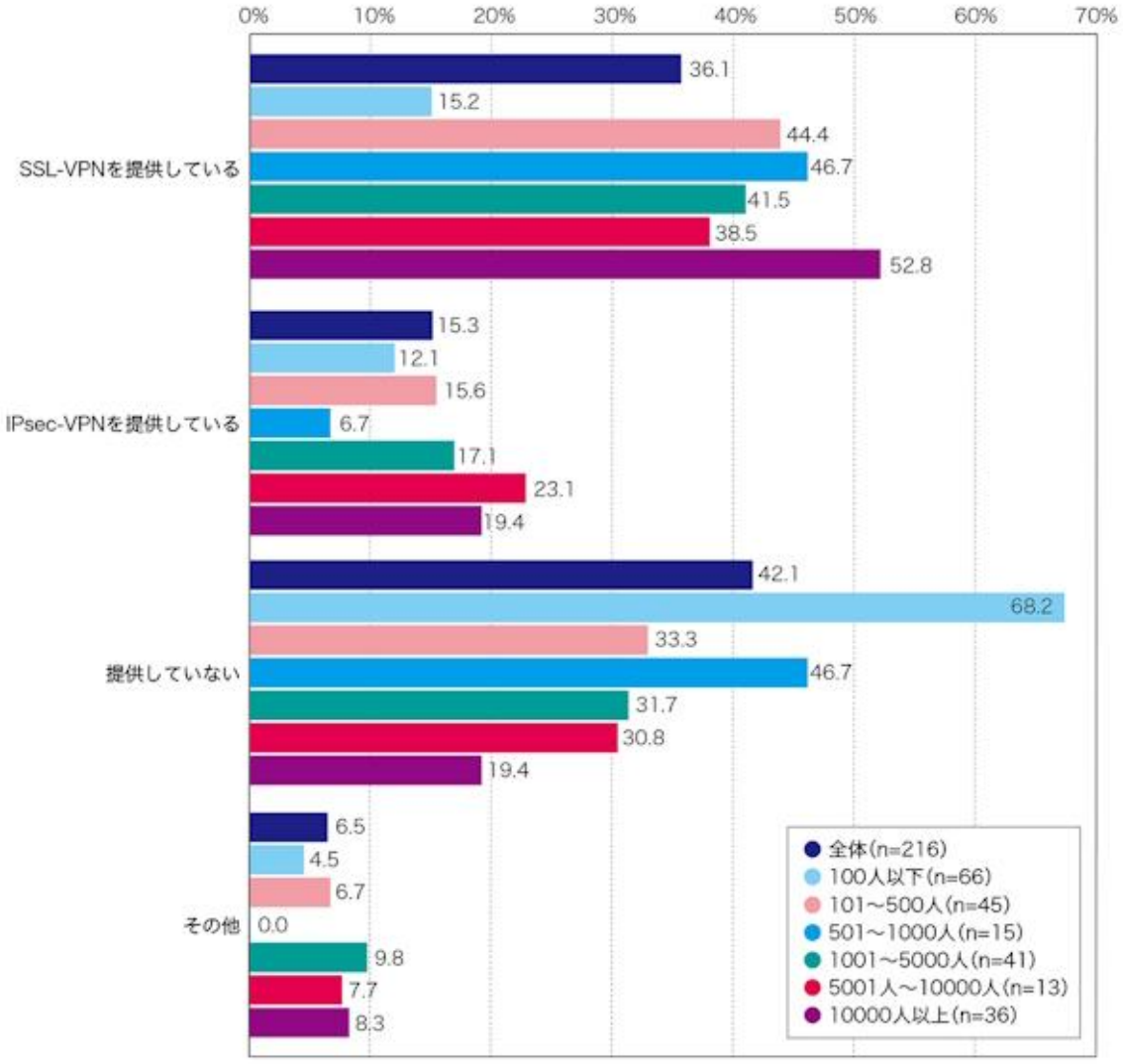


図 3　従業員向けの VPN の提供状況（従業員規模別）

一方で、VPN のセキュリティ対策には明確なばらつきが見られた。「最小権限の原則を適用している」（72.0%）、「シングルサインオンを導入済み」（53.6%）といった基本的な取り組みは一定程度浸透しているものの、より実践的かつ継続的な対策である「月 1 回以上の脆弱（ぜいじゃく）性スキャン」（33.6%）や「VPN ログの定期的な分析」（28.8%）の実施率は依然として低水準にとどまっている（図 4）。

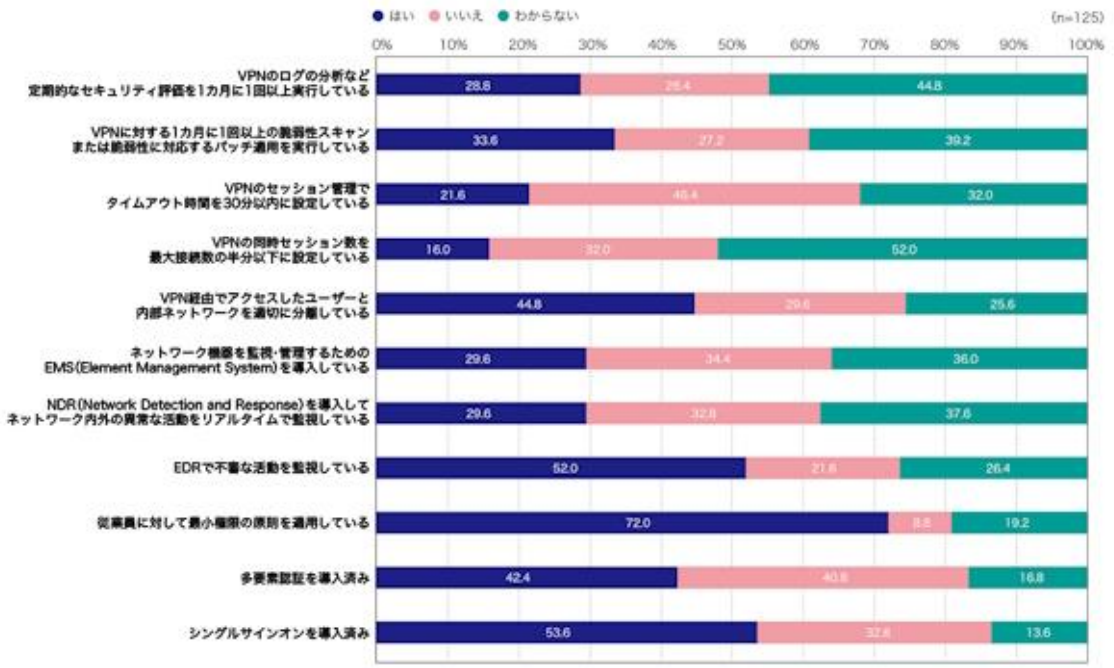


図 4　セキュリティに関する VPN の運用状況

また、侵入後の不審な動きを検知する EDR（Endpoint Detection and Response：52.0%）や、ネットワーク全体を対象とする NDR（Network Detection and Response：29.6%）の導入状況については、企業規模によって大きな差が見られた。大企業では一定の水準に達している一方で、中堅・中小企業では導入が進んでおらず、セキュリティ体制の二極化が進んでいるようだ。

VPN のセキュリティリスクや運用負荷の高さを背景に、「脱 VPN」を視野に入れた動きが広がりつつある。今回の調査でも、約 4 分の 1 の企業が VPN からの移行を検討中と回答しており（図 5）、移行を「現実的な選択肢」と捉える企業が一定数存在していることが分かった。

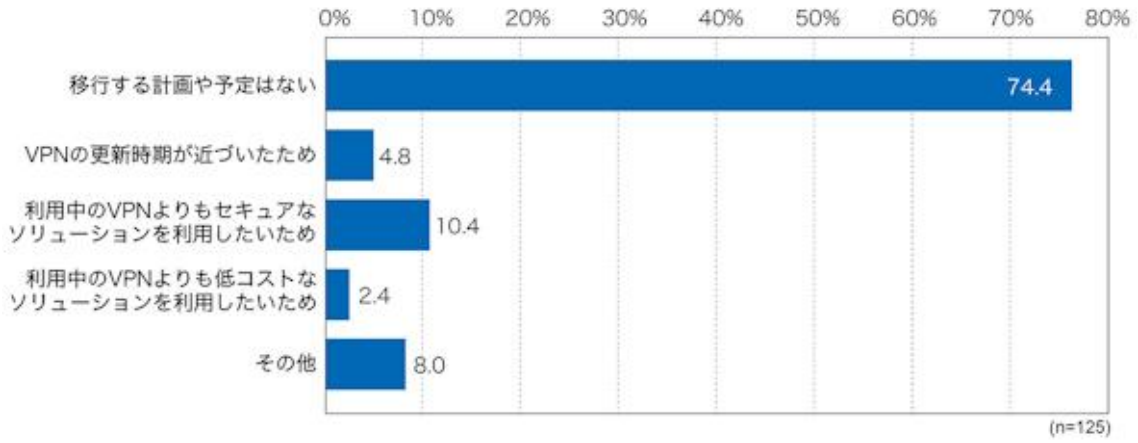


図 5　VPN から別のソリューションに移行する計画とその理由

代替手段として挙げられたのは、「ZTNA」（Zero Trust Network Access）および「SASE」（Secure Access Service Edge）がいずれも 31.3%で並び、注目度の高さがうかがえる（図 6）。

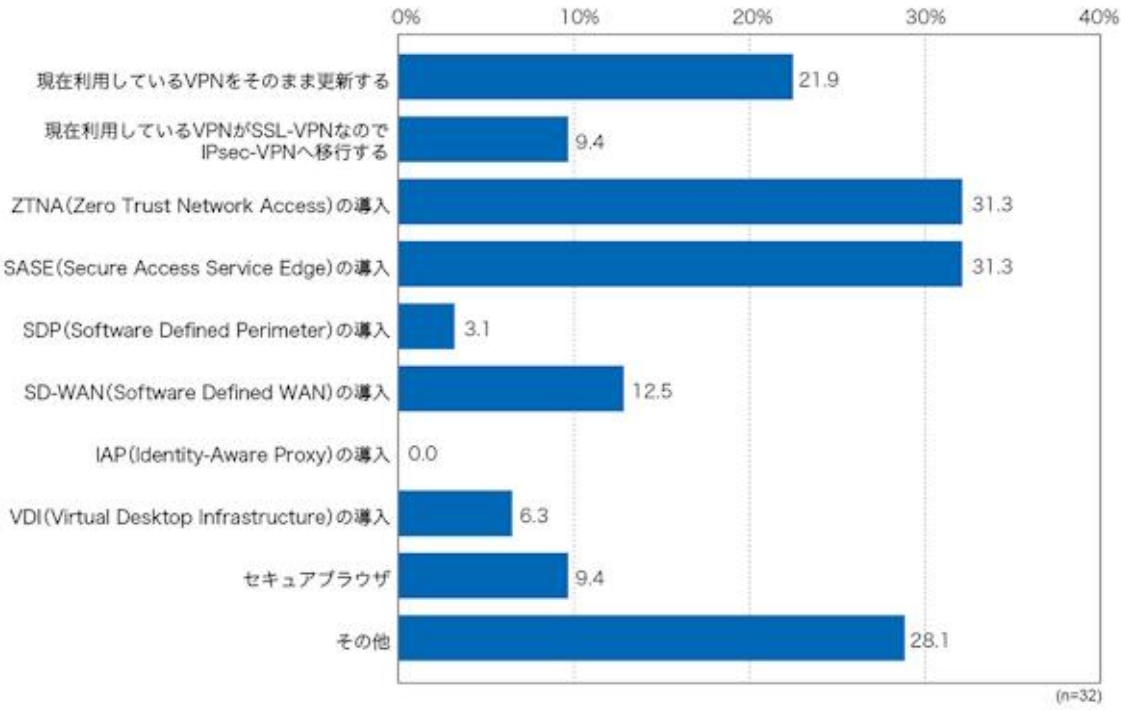


図 6　VPN から移行、併用するソリューション

これらのソリューションは、ユーザーごとの厳密なアクセス制御に加え、クラウド環境におけるセキュリティ管理の一元化に強みを持ち、ゼロトラストを実現するための中核技術として導入が進みつつある。

導入検討時に企業が重視する観点としては、「セキュリティの強度」「管理・運用コストの低さ」「従業員の利便性・負担の軽さ」が上位を占めた（図 7）。これは、単に堅牢（けんろう）なセキュリティを求めるだけでなく、現場での業務効率や運用の持続可能性にも配慮している企業の姿勢を反映している。

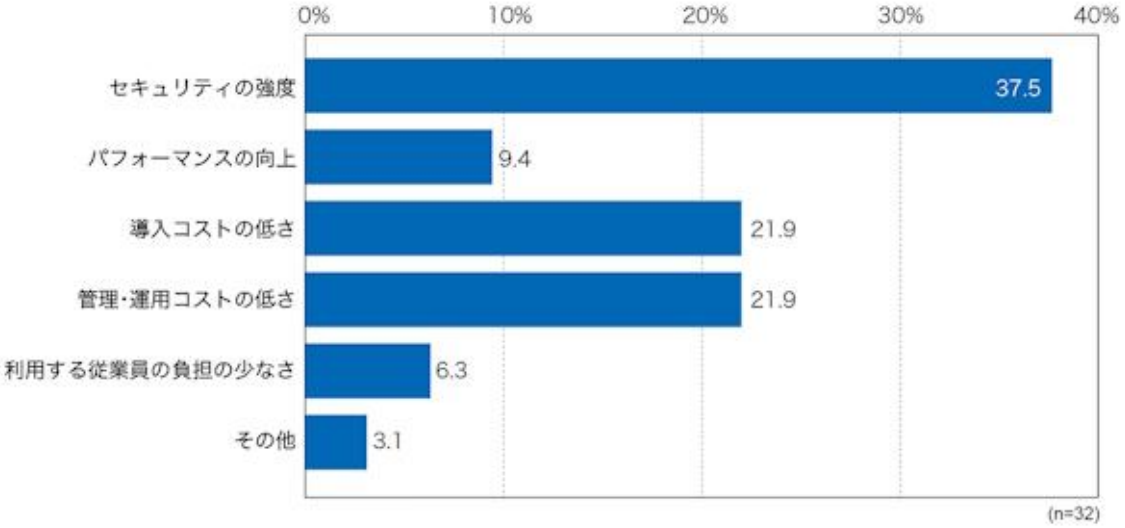


図 7　VPN から別ソリューション移行する際に重視する点

VPN から ZTNA へ移行するには何をしなければならないのか

しかしながら、ZTNA の導入は決して容易ではない。多くの企業が直面するのが、導入プロセスの煩雑さと初期コストの高さだ。ZTNA の構築には複数フェーズを要し、PoC（概念実証）から本番稼働まで半年以上を要するケースも少なくない。次章では、ZTNA 導入に向けたステップを具体的に解説する。

ZTNA ソリューションは購入してインストールして終わるというものではない。ベンダーによって多少異なるが、7 つ程度のフェーズを経る必要がある。

（1）現状分析と要件定義

現状の VPN 環境をまず調べる必要がある。ユーザー数や帯域の利用状況、ユーザーが利用しているアプリケーション、認証基盤などを洗い出して、ZTNA の利用時に必要になる条件を調べる。ZTNA 導入の目的やリスク分析もこのフェーズで固めておく。

（2）ZTNA ソリューションの選定

（1）の現状分析や要件定義に従って選定しながら PoC を実施する。利用規模が大きい場合には PoC 環境の構築にも時間と費用がかかる。

（3）ZTNA アーキテクチャの設計

ネットワーク構成やアクセスポリシー、認証フローだけでなく、ログ管理や監視についても設計しなければならない。IDaaS や MDM（モバイルデバイス管理）、SIEM（Security Information and Event Management）を導入済みであれば、これらとの連携方法も設計する。ユーザーごとの権限についてもここで定める。最後に VPN から ZTNA への段階的な移行計画を策定しながら、DR や BCP の視点も入れていく。

（4）環境構築と設定

（3）のアーキテクチャに従って、具体的なアクセス制御ポリシーを作成して適用する。アクセス制御ではゲートウェイの設定が中心になる。ゲートウェイがユーザーとアプリケーションやリソースの中継点になるため、ここでアクセス要求を検証するからだ。クラウドとオンプレミスの両方に対応させる場合は、環境構築がさらに複雑になる。次にユーザーデバイスに ZTNA クライアントの役割を果たすエージェントを配布してインストールする。

（5）テスト

設計通りのアクセス制御が実現できているか、パフォーマンスに問題がないかどうかのテストが必要だ。次に脆弱性診断とペネトレーションテストのスケジュールを作って実行していく。

（6）ユーザー教育と運用の準備

トラブルシューティングとセキュリティガイドラインについて従業員に強調する。従業員は必ず入れ替わるため、ポリシー変更手順の教育も必要だ。障害対応の他、サイバー攻撃などによる緊急時対応についてマニュアルを配布する。サポート体制もこのフェーズで固めていく。

（7）移行と本番稼働

一部のユーザーから ZTNA へ切り替えていき、その都度、問題をつぶしていく。VPN を全廃する場合でも ZTNA との並行運用期間が必要だ。その後、パフォーマンスチューニングはもちろん、不適切なセキュリティポリシーがないかどうかを監視して、サイバー攻撃に備える。

これらのフェーズを全て終えるには、最短でも数カ月、長ければ 1 年近くかかるケースも少なくない。費用面も小規模導入で数百万円、大規模では数千万円規模の投資が必要となる。

中堅・中小企業にも広がるリスク、RaaS の拡大が背景に

警察庁の報告によれば、2024 年におけるランサムウェア被害の報告件数（222 件）のうち、大企業では減少傾向が見られた一方で、中小企業では前年比 37%増という顕著な増加が確認された。

この背景には、ランサムウェアを「サービス」として提供する RaaS（Ransomware as a Service）の拡大がある。RaaS の普及により、かつては高度な技術を要した攻撃が、現在では低スキルの攻撃者でも容易に実行可能となり、セキュリティ対策が手薄な企業が新たな標的となりやすい構図が生まれている。

サイバー攻撃は、対象を選ばず、「規模の小さな企業だから狙われない」という過信は通用しない時代に突入している。特に中堅・中小企業では、限られたセキュリティ予算や人材の中で、いかに効率的かつ効果的にリスクを管理するかが大きな課題だ。

サイバー攻撃者は、そうした"脆弱な隙"を的確に突いてくる。だからこそ、最新の脅威動向を定期的に把握し、自社の状況に照らして優先度を見極めながら段階的に対策を講じていくアプローチが不可欠だ。

今後は、防御の強化と運用効率を両立するソリューション選定や、人的リソースに依存しすぎない自動化・可視化の取り組みも、持続可能なセキュリティ対策の鍵を握るだろう。

初出：2025 年 7 月 17 日
執筆者：キーマンズネット編集部
URL：https://kn.itmedia.co.jp/kn/articles/2507/17/news044.html

VPN はもう限界：コストを抑えた「脱 VPN」対策 ZTNA や SASE 以外の選択肢とは

ランサムウェア被害を受けた日本企業の過半数で VPN に原因があった。コストが比較的低く、より安全な「脱 VPN」の方法を企業の規模別に解説する。

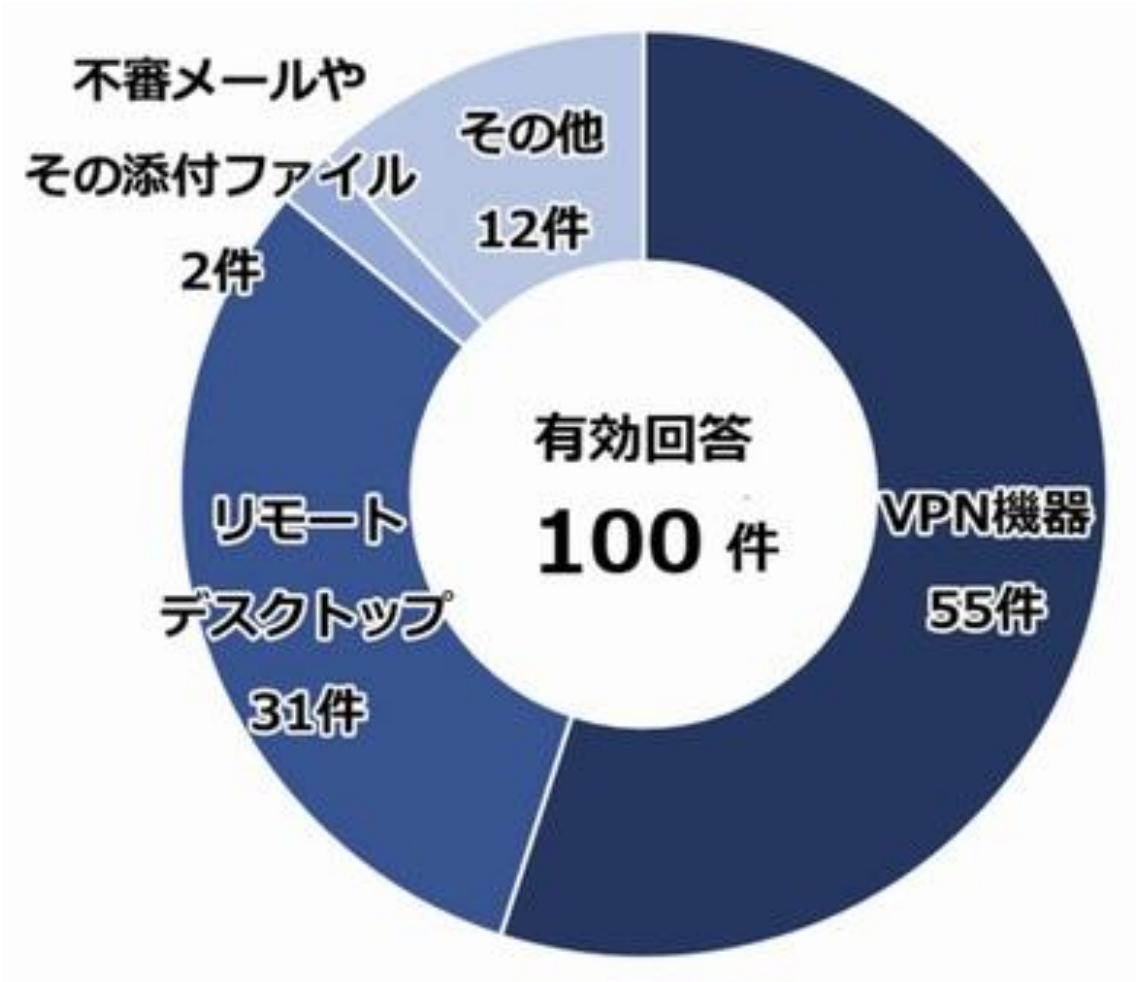
今日のビジネス環境において、テレワークの普及は加速の一途をたどっている。それに伴い、企業ネットワークへ外部からアクセスする手段として標準的だった VPN（Virtual Private Network）の課題が顕在化して、代替ソリューションを探す「脱 VPN」への関心が高まっている。

本稿では、ゼロトラストネットワークアクセス（ZTNA）や SASE（Secure Access Service Edge）といった新たな選択肢が注目される中で、企業が直面する VPN の具体的な課題と、脱 VPN の最適なソリューションを選定するためのポイントを紹介しよう。

VPN はどれほど危険か

テレワークの普及やクラウドの利用が進むにつれて、VPN について安全性の問題や運用の手間が目立つ。

大きく報道された大阪急性期・総合医療センターやつるぎ町立半田病院の事例では、VPN のゲートウェイに侵入の形跡が発見された。警察庁が公開した「サイバー空間をめぐる脅威の情勢等」では、ランサムウェア感染の経路の 55%が VPN 機器だと報告されており、VPN の脆弱性が企業や組織の事業継続に大きなリスクをもたらしている。



ランサムウェア被害の感染経路は、もはや添付ファイルではなく「VPN 機器」が大半を占める（警察庁「サイバー空間をめぐる脅威の情勢等」）

このような VPN の危機について、比較的中立的な機関や組織はどのような対策を推奨しているのだろうか。

情報処理推進機構（IPA）は、ZTNA（Zero Trust Network Access）の導入を推奨している。ZTNA は、これまで VPN が担ってきたリモートアクセスの役割を、より細やかな認証・認可のポリシーを用いて代替する仕組みであり、ネットワーク全体ではなく、アプリケーションやサービス単位でアクセスを制御することを目的としている＊。

＊ゼロトラスト移行のすすめ（IPA）　https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002ko3-att/000099778.pdf?utm_source=chatgpt.com

ZTNA 以外の方法はあるのか

かもめエンジニアリングの潮村剛氏

IPA は ZTNA の一要素ともいえる IAP（Identity-Aware Proxy）の導入も推奨している。IAP はアプリケーション単位でのアクセス制御に特化しており、外部ネットワークからのアクセス時にユーザーID や端末の状態に応じて認証・認可を行うため、脱 VPN の有力な選択肢となる（ZTNA と IAP の相違点については本文末の囲み記事を参照）。

脱 VPN を進める際、ZTNA はサイバー攻撃に対する強力な防御策として有効だ。だが、導入のハードルは決して低くない。従業員数が 1000 人以上の企業では、導入費用が数千万円に達し、導入後の運用コストも従業員 1 人当たり数万円かかる。また、ZTNA は複数のサービスで構成されているため、導入・運用するサービスの数によってコストに 2〜3 倍の幅が生じることもある。

コストを抑えて脱 VPN に特化した対策を考えるのであれば、IAP の導入が第一の候補になるだろう。

脱 VPN、取るべき対策は？　企業規模別で分かれる課題と打ち手

脱 VPN を検討する際、導入コストを抑えつつ効果的な対策を求めるなら、IAP の導入が有力な選択肢となる。

そこで IAP 寄りの導入が可能なソリューションを提供するかもめエンジニアリングの取締役の潮村剛氏に導入時の課題やコスト感について話を伺った。

潮村氏はまず「現状を理解しつつ、変えなければならないことは理解していても、ベンダーに（ZTNA や）SASE の見積もりを取ったところで、コスト感が合わず立ち止まってしまう」と指摘する。

潮村氏によると、同業他社がセキュリティインシデントに見舞われた場合、経営層から情報システム部門が自社の状況を問われるケースが増えており、従来の VPN では対応しきれない状況が確実に生まれている。こうした課題に直面した企業は、ZTNA や SASE といったより先進的なゼロトラストソリューションへの移行を検討する段階に移っている。

VPN からの脱却を検討する企業の状況は、規模によって大きく二分されると潮村氏は指摘する。

（1）従業員数 100 人未満の中堅・中小企業の場合

これまでセキュリティ対策に無関心だった企業も、業界で起きたインシデントやセキュリティ情報に触れて、「対策は必要らしいが、何をすれば良いか分からない」と悩むケースが多い。ZTNA のような最新セ

キュリティソリューションは「自分たちには縁遠い」と感じる傾向が強く、担当者が情報を収集したとしても、社内で予算や理解を得るのが難しい。

経営層が同業他社の被害を聞きつけて自社の状況を問い詰める、といった突発的な要因が導入の動機になることが多い。「セキュリティ対策はコストがかかるが売り上げには直結しないため、経営層は被害が顕在化しない限り導入を渋る」と潮村氏は語り、「もし被害に遭えば甚大な事態になる」というリスクを、前出の警察庁の資料などを引用しながら具体的に伝えることが重要だと言う。

（2）従業員数 100 人以上の企業の場合

何らかのセキュリティ対策を導入済みにもかかわらず、VPN の部分が手付かずで残っているケースが多い。ZTNA や SASE、SD-WAN といったソリューションを横並びにして詳細な比較表を作成し、どの製品を導入すべきなのか深く悩む傾向にある。しかし、各ソリューションは他のセキュリティソリューションと重なる部分を内包しているため、単純な比較は困難だ。

また、「機能が多い海外ベンダーの高性能製品を選定して見積もりを取るととんでもなく高額になる」ことが頻発し、導入計画が頓挫するケースが多いという。高額な SASE 製品を導入したものの、2 年程度で「そこまでの機能は不要だったのではないか」と見直しに入る企業もある。大手企業が最も懸念するのは、「本当にちゃんと動くのか」「自社の運用担当者の手間がどれだけ増減するか」、そして何より「従業員の手間がどれだけ変わらないか」が非常に重要だという。従業員の業務負荷増大は、導入の大きな障壁になるためだ。

脱 VPN に何を望むのか

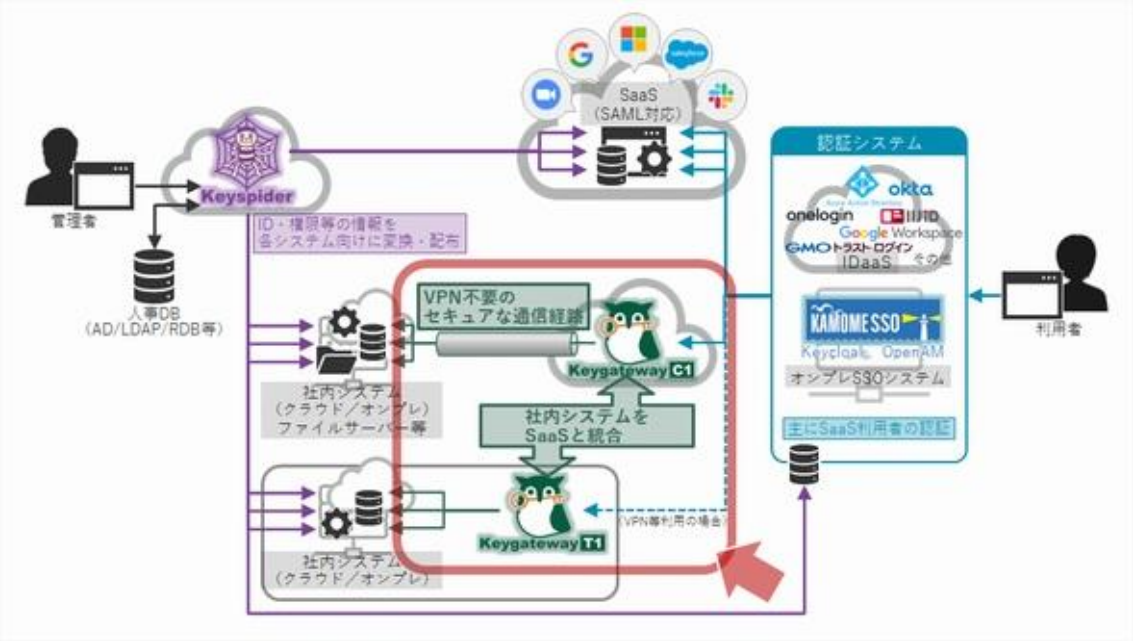
脱 VPN について扱ったキーマンズネットの読者調査（2025 年 6〜7 月に実施）では、「セキュリティの強度」「導入コスト」「管理・運用コストの低さ」が脱 VPN において重視されていることが分かった。潮村氏の指摘も踏まえ、選定ポイントを具体的に見ていこう。

セキュリティの強度と運用負荷の低減

ZTNA ソリューション、特に代理認証機能の導入は、従業員自身による ID・パスワードの管理を不要にする。つまり、パスワード漏えいリスクが大幅に低減する。これは情報システム部門のパスワード再発行業務などの負担がゼロに近くなるという大きなメリットがある。「セキュリティ強化と運用負荷軽減の両方をアピールできる」点で非常に有効だ。

導入コストと運用コスト

初期導入費用は接続対象のシステムの数や代理認証の必要性に応じて変わる。潮村氏によれば、かもめエンジニアリングのソリューション「Keygateway」では、一般的なケースとして、Web アプリケーション 5〜10 システムに代理認証機能を含めて接続する場合、「200〜500 万円の初期費用がかかる」という。利用料はサブスクリプション形式で、ユーザー単位での課金だ。基本的な料金は 1 ユーザー当たり月額 500 円で、1000 ユーザー以上の大規模な導入ではボリュームディスカウントが適用される。運用コストの課金体系が自社にとってふさわしいものなのかは事前に確認が必要だろう。



かもめエンジニアリングが提供するソリューション「Keygateway」の概要（提供：かもめエンジニアリング）

企業が実行しなければならない作業は

導入決定から平常運用までの期間は対象とするシステムの数によって大きく異なる。かもめエンジニアリングのソリューションの場合は、5〜10 システム程度であれば、「2〜3 カ月で完了するケースが多い」という。

最も時間がかかるのは、ベンダー側の作業ではなく、「どのシステムを保護対象とするか」というユーザー企業側の意思決定プロセスだ。情報システム部門の担当者が少ない企業では、シャドーIT などの把握しきれていないシステムが多数存在し、それらをどこまでカバーするか、カバーした場合の運用負担をどうするか、といった点が課題となる。その一方で導入後の日常的な運用負荷については、「通常利用シーンではほとんどかからない」と潮村氏は述べ、「ユーザーは使っていることを意識しない」状態が理想だとしている。

成功事例から学ぶ導入のヒント

潮村氏は同社のソリューションが成功した事例として、以下の 2 つを挙げた。

（1）国内大手の基礎資材供給企業（従業員数 1 万人規模）の事例

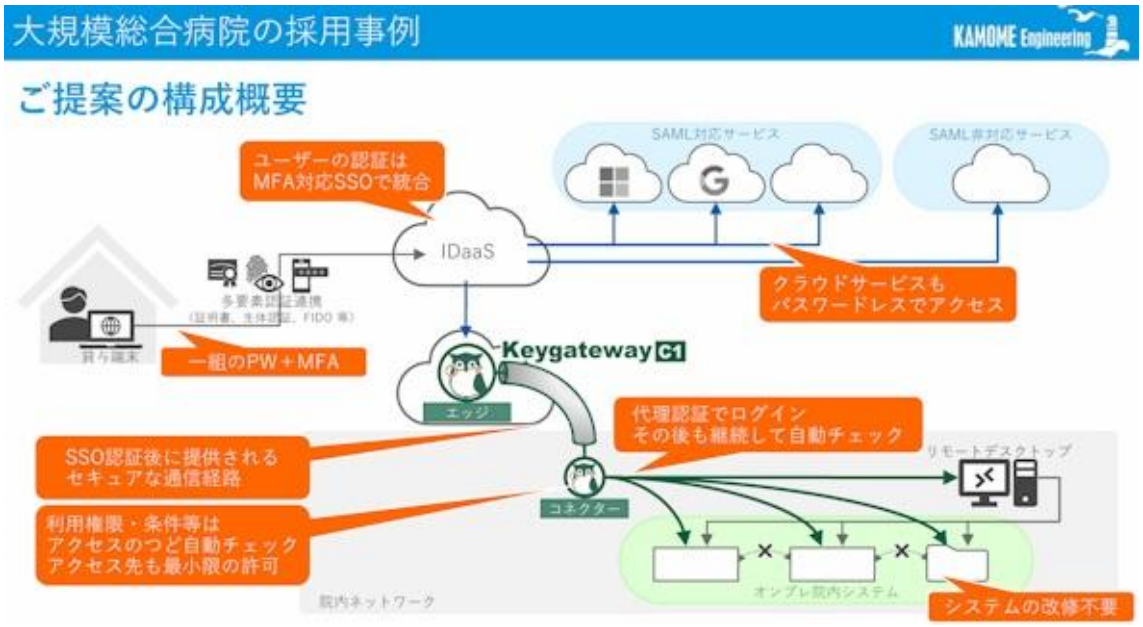
大手ベンダーによる製品と比較した後、3 カ月間の PoC（概念実証）を実施した結果、かもめエンジニアリングのソリューションが選定された。

選定の要因は「構造のシンプルさ」（情報システム部門にとって理解しやすくトラブル時の特定が容易）、「体感速度の速さ」（利用者が従来の 2 倍速いと感じた）、「コストパフォーマンス」だった。情報システム部門から導入を開始して、徐々に事業部や本社全体、関連会社へと対象が拡大していく理想的な広がり方を見せたという。

（2）都道府県別の中核となる総合医療センター（従業員数百人単位の病院）の事例

地域の基幹病院として遠隔医療で画像診断などを実施していたところ、VPN のアクセスログに侵入の形跡があり、急きょ VPN を遮断しなければならない事態に直面した。これにより遠隔医療だけでなく、約 30〜40 社のベンダーによる病院のシステムメンテナンスも滞り、業務が停止寸前となったという。

緊急性の高い状況の中、3〜4 カ月という短期間で導入が完了した。導入後、医師や業者からは「以前よりも楽になった」「速い」といった声が聞かれ、情報システム部門の評価も向上したという。特に病院では機微情報に相当する個人情報を扱うため、セキュリティ意識が非常に高く、多要素認証が義務付けられる医療ガイドラインにも対応できる同社のシングルサインオン（SSO）が有効に機能したという。



導入したシステム構成図（提供：かもめエンジニアリング）

これらの事例から、「ぼんやりとした漠然とした不安」ではなく、「具体的な課題を掘り下げて困っている企業」がソリューション導入に至る傾向が強いことが示唆されるとした。

脱 VPN を検討する企業への提言

最後に、潮村氏から VPN からの脱却を検討する企業へのアドバイスがある。

潮村氏はまず、「最も大事なポイントはさまざまな商材を扱う複数のベンダーに相談することだ」と述べる。一社だけでは、そのベンダーが売りたい製品に偏った情報しか得られない可能性があるため、複数社の意見を聞き、多角的な視点から製品の長所と短所を比較検討することが重要だという。

そして、「自社がどこまでできるのか、どこまでやりたいのか、予算はどうか、利用者の IT リテラシーはどのくらいかといった点を総合的に勘案し、最適なソリューションを見極めるしかない」とも指摘する。その上で、「一気に全てを移行するのは現実的ではない。まずは『どこから着手するか』を決めて段階的に進めるのが良いだろう」と述べる。

VPN から ZTNA（IAP）への移行期にある現在、多種多様なソリューションが存在し、選定は非常に困難を極める。企業は、自身の課題を明確にし、信頼できるパートナーと共に多角的な情報収集を行うことで、最適な脱 VPN 戦略を策定していく必要があるだろう。

ZTNA と IAP は何が違うのか

ZTNA と IAP はどちらも VPN を使ったネットワーク境界型アクセスの弱点を補う技術だ。ではどこが違うのだろうか。

ZTNA と IAP の共通点は 3 つある。第 1 にどちらも VPN のように（社内）ネットワーク全体へ接続するための暗号化されたトンネルを作り出す方式とは異なり、不要なリスクを減らすためにアクセスを最小限に限定することを目指している。第 2 に認証・認可を重視して、ユーザーやデバイスのコンテキスト（場所、デバイスの健全性）を考慮できることだ。第 3 にアプリケーション単位でアクセスを制御でき、攻撃対象の露出を減らすことが可能だ。

相違点は 6 つある。目的、対応プロトコル（アプリケーション）、アクセス制御の粒度と持続性、ネットワーク露出、運用とポリシー管理、セキュリティ保証の強さだ。目的で見ると、IAP はアプリケーションやサービスへのアクセスをアイデンティティーとコンテキストで制御するプロキシ（ゲートウェイ）と言える。ZTNA はセキュアなアクセスモデル全体を包括しており、IAP よりも広い。IAP は HTTP や HTTPS などを中心に扱い、SSH や RDP に対応するものもある。ZTNA はどのようなプロトコルにも対応できる。IAP の粒度は「誰が」「どのアプリケーションを」「どのデバイス／コンテキストで」というもので、アクセス要求ごとに認証・認可する。ZTNA はさらに広く、アクセス中であってもコンテキストが変化したら制御を見直したり、あるデバイスの健全性が低下したらアクセスを打ち切ったりできる。

つまり、HTTP／HTTPS ベースのアクセスに限られており、厳格なデバイス管理が必要でなければ IAP で目的を十分に達成することが可能だ。

初出：2025 年 9 月 24 日
執筆者：宮田健（キーマンズネット）
URL：https://kn.itmedia.co.jp/kn/articles/2509/24/news043.html