The serialization title

情報システム担当が選ぶネットワークインフラ

第7回 「ゼロトラスト」8割が初耳の実態

株式会社ピーエスアイ
管理部広報担当
内藤 純一
URL https://www.psi.co.jp
E-mail support@psi.co.jp

「ゼロトラスト」とは、特定の製品やサービス名ではなくすべてのアクセスを信用せず、社内外を問わず検証する考え方です。ただし、中小企業の現場では、まだ十分に浸透していない実態があり、今回の当社アンケートでは「初めて聞いた」が77.6%と大多数を占め、「理解しており導入検討中」は6.6%にとどまりました。今回は、中小企業が押さえるべき基本とネットワーク視点での実践方法を整理します。

「ゼロトラスト」の認知度と本来の意味

「自社のゼロトラストセキュリティの概念について、理解度はどの程度だと思いますか?」

今回のアンケートは、SNS上でIT担当者を中心に、76名から回答が寄せられました（図1）。

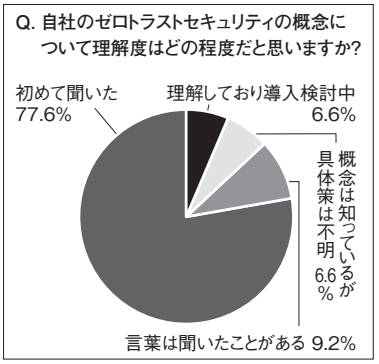
最も多かったのは「初めて聞いた」の77・6%でした。つまり、回答者の約8割が「ゼロトラスト」という概念に、まだ触れてもいないということになります。

一方で「理解しており導入検討中」と答えた企業は6.6%にとどまりました。「概念は知っているが具体策は不明」の6.6%、「言葉は聞いたことがある」の9.2%を合わせても、具体的な導入検討に進んでいる企業はまだ少数派であることがわかります。

この結果は、ゼロトラストという言葉がセキュリティ業界で頻繁に使われるようになった一方で、中小企業の現場にはまだ十分に届いていない実態を示しています。

なお、今回の調査はSNS上で実施した76名へのアンケートであるため、回答者の企業規模や業種には一定の偏りがある可能性があります。ただし「現場ではあまり浸透していないがゼロトラストは重要で、これから理解が進むテーマである」という傾向を示す材料にはなります。

図1 アンケート結果（回答数76票）



●信頼を見直すための設計思想

ゼロトラストが難しく見える理由のひとつは、説明される範囲が広いことです。「ID管理／端末管理／クラウド認証／ネットワーク制御／ログ監視／EDR※1／SASE※2」など、関連する言葉が一度に出てくることもあり、その結果「大企業が高価なしくみをまとめて導入するもの」という印象を持たれています。

しかし、ゼロトラストの本質はもっとシンプルで「社内だから安全」「VPNで入っているから信

頼できる」「一度認証したから後は自由に使える」という前提を置かず、その都度、利用者、通信先、端末、アクセス権限を確認する考え方です。つまり、製品やサービス名ではなく、信頼の置き方を見直すための設計思想なのです。

「ゼロトラスト」はなぜわかりにくいのか

●入った後も確認し続ける

その理由は「ゼロ」という言葉の強さにあり、直訳すると「何も信頼しない」となり、すべてを遮断する極端なセキュリティのように感じるかもしれませんが、実際は業務を止めるための考え方ではなく「必要な人が／必要な端末で／必要な業務システムへ／必要な範囲だけ」安全にアクセスできるようにするための考え方です。

例えば、会社の建物に入るシーンで考察すると、従来の考え方は「社員証を見せて入口を通れば建物内では比較的自由に動ける」という発想です。

これに対して、ゼロトラストでは「玄関だけではなく各部屋に入るときにも、その人が本当に入っていいのか」を確認します。また、同じ社員でも「経理資料の部屋／設計図面の部屋／来客用エリア」など、入れる範囲が異なります。

ネットワークでも同じです。従来は「社内ネットワークにいる端末は比較的安全」と考えられ、外から内へ入る境界にファイアウォールを置き、社内はある程度信頼するという構造が一般的でした。しかし現在は、この前提が成り立ちにくくなっています。

社員は、オフィスだけではなく自宅や外出先からクラウドサービスを利用します。業務端末だけではなく、スマートフォンやタブレット、ＩｏＴ機器もネットワークにつながります。

Microsoft365やGoogle Workspaceのようなクラウドサービスを使う場合、重要な業務データは社内サーバーではなくインターネット上にあり、会社の中と外を単純に分けることが難しいのです。

また、攻撃者の侵入経路も変化しており、境界のファイアウォールを正面から突破するだけではなく「フィッシングによってＩＤとパスワードを盗む／ＶＰＮ機器の脆弱性を突く／マルウェアに感染した端末から社内へ広がる」といった手口が使われます。一度内部侵入されるとフラットなネットワークでは、横方向に移動しやすく被害拡大のリスクが高まります。

よって、ゼロトラストでは「一度入れたら信頼」ではなく「入った後も確認し続ける」ことを重視します。ただし、何でも疑って止めるという意味ではなく、業務に必要な通信は通し、不要な通信や不自然な通信は制限する。これを現実的に行うために、ＩＤ、端末、ネットワーク、ログを組み合わせて判断します。

境界防御の限界とネットワーク再構築

●建物内に区画と入退室管理を

本連載でもお伝えしていますがネットワークはセキュリティの土台で、スイッチや無線ＬＡＮ、ＵＴＭ（統合脅威管理）、拠点間接続、監視のいずれも、単独では完結しません。ゼロトラストとは、これらをひとつの考え方でつなぎ直すテーマだと捉えてください。

従来の境界防御は変わらず重要であり、インターネットとの入口にファイアウォールやＵＴＭを置き、不審な通信を遮断することが必須です。しかし、それだけでは十分とはいえません。

なぜなら、業務の入口がファイアウォールだけではなくなり、クラウドサービスやリモートアクセス、スマートフォン、取引先連携など、利用者が業務システムへ到達する経路は複数です。

例えば、社員のＩＤとパスワードが盗まれたとします。すると攻撃者は、正規の利用者になりすましてクラウドサービスへログインを試みます。この場合、通信そのものは正規のログイン処理に見え単純な境界防御だけでは見抜きにくく、そこで必要なのが、多要素

※1 EDR（Endpoint Detection and Response）：PC・サーバ・スマホなどエンドポイントでの検知と対応を行うセキュリティ製品やしくみ
※2 SASE（Secure Access Service Edge）：ネットワーク機能とセキュリティ機能をクラウド上で一体提供するしくみ

認証や条件付きアクセスです。

いつもと違う場所からのログインや未管理端末からのアクセス、深夜の大量ダウンロードなどを検知し、追加認証や遮断を行います。

また、社内端末がマルウェアに感染した場合も同様です。感染端末が社内ネットワーク内で自由に他のサーバーや端末へアクセスできる構成では、被害が広がりやすくなります。

これを防ぐには、部門や用途ごとにネットワークを分けるVLAN（仮想LAN）設計、端末間通信の制限、サーバーへのアクセス制御が必要です。第2回で扱ったスイッチングやVLANは、ゼロトラストの土台です。

無線LANも同じで、来客用Wi-Fi、業務用Wi-Fi、IoT機器用ネットワークを分離せずに運用していると、どこかひとつの弱点が社内全体のリスクにつながります。

ゼロトラストの視点では「つながること」だけではなく「つながった後にどこまで行けるか」を設計することが重要です。

つまり、境界防御の限界は「境界防御が不要になる」という意味ではなく、入口の防御に加えて、内部でも信頼を分け、アクセスを絞り、通信を見えるようにする必要があるということです。外側の壁だけで守るのではなく「建物の中にも区画と入退室管理を設けること」が、ゼロトラストの感覚に近いといえます。

「ゼロトラスト」の実装アプローチ

●組み合わせと整理の視点

では、ネットワーク視点ではゼロトラストをどのように実装していけばいいのでしょうか。難しい言葉を並べる前に、まずレイヤーごとに整理するとわかりやすくなります（図1）。

そして、これらの制御を支えるのがIDと端末の確認です。多要素認証、端末証明書、MDM※4、EDRなどを組み合わせることで「正しい利用者か」「管理された端末か」「危険な状態ではないか」を判断しやすくなります。ネットワークだけで完結するのではなく、IDと端末の情報をネットワーク制御に反映することが、ゼロトラストらしい実装です。

さらに欠かせないのが、監視とログです。第6回で扱った可視化の考え方は、ゼロトラストと直結します。アクセスを絞っても、実

図1　ゼロトラストのレイヤーごとの実装アプローチ

■ L2（データリンク層）の観点

端末がどのネットワークに接続できるかを制御します。具体的には、VLANによる分離、無線LANのSSID（サービスセット識別子）分離、ポート単位の制御などです。業務端末、来客端末、監視カメラ、複合機、IoT機器を同じネットワークに置かないことが基本になります。

すべてを細かく分ける必要はありませんが、少なくとも「業務用」「来客用」「IoT用」「サーバー用」程度に分離するだけでも、横展開のリスクを下げやすくなります。

■ L3・L4（ネットワーク層・トランスポート層）の観点

IPアドレスやポート番号をもとに、どの通信を許可するかを制御します。

例えば、営業部門の端末から経理サーバーへ直接アクセスできないようにする、監視カメラからインターネットへの不要な通信を制限する、拠点間VPNで通す通信を必要な範囲に絞る、といった制御です。

ゼロトラストでは、通信を「通すか止めるか」ではなく「誰が、どの端末で、どのサービスへ、どの範囲でアクセスするか」をできるだけ細かく考えます。

■ L7（アプリケーション層）の観点

アプリケーションやクラウドサービス単位での制御が重要になります。単に443番ポートのHTTPS※3を許可するだけでは、業務用のクラウドサービスや個人利用のストレージも、危険なWebサイトへの通信も同じように見えてしまいます。

次世代ファイアウォールやSASE、クラウドプロキシなどを活用すると、アプリケーションの種類やユーザー属性に応じて制御できる場合があります。

※3 HTTPS（HyperText Transfer Protocol Secure）インターネット上でデータを安全に送受信するためのプロトコル
※4 MDM（Mobile device management）：携帯端末管理

際にどの通信が起きているかを見ていなければ、ルールが効いているのか、抜け道がないのかを確認できません。認証ログ、通信ログ、端末ログを組み合わせ、普段と違う動きに気づけるようにすることが重要です。

ここで注意したいのは「ゼロトラスト製品をひとつ入れれば完成する」と考えないことです。ゼロトラストは製品の名前ではなく、複数の技術を組み合わせて信頼を確認し続ける設計思想です。

既存のスイッチ、無線LAN、ファイアウォール、VPN、クラウド認証を、どう組み合わせて整理するのかが、ネットワークベンダー視点の第一歩になります。

小さく始める「ゼロトラスト」の道筋

中小企業がゼロトラストに取り組む際に、最初から完璧を目指す必要はありません。現在の環境を棚卸しして、リスクの高いところから段階的に見直すのが現実的です。ゼロトラストは一度に完成させるものではなく、以下のステップ1〜4を参考にしてください。

【ステップ1】
資産と通信の見える化

どの拠点にどのような機器があり、誰がどのクラウドサービスを使い、どのサーバーにアクセスしているのかを把握します。ここがわからないままでは、最小権限もアクセス制御も設計できません。まずは重要なサーバー、インターネット出口、無線LAN、VPN接続から確認するだけでも十分です。

【ステップ2】
IDの強化

特にクラウドサービスやVPN、管理者アカウントには多要素認証を優先して導入すべきです。全社員・全システムを一気に変える必要はありません。まずは漏えい時の影響が大きいアカウントから始めることで、効果を得やすくなります。退職者アカウントの削除、共有IDの廃止、権限の棚卸しも地味ですが重要な対策です。

【ステップ3】
ネットワークの分離

業務用、来客用、IoT用、管理用のネットワークを分け、必要な通信だけを許可します。特に複合機、監視カメラ、入退室管理などは、長期間使われる一方で管理が後回しになりやすい機器です。これらを業務端末と同じネットワークに置き続けることは、リスクを広げる要因になります。

【ステップ4】
監視と改善

アクセス制御を入れた後も、ログを見て、不要な通信が残っていないか、業務に必要な通信を止めていないかを確認します。ゼロトラストは「厳しくする」だけではなく「業務に必要な通信を安全に通す」ための取り組みです。そのためには、設定して終わりではなく、運用しながら調整する姿勢が欠かせません。

今回のアンケートでは「ゼロトラストを初めて聞いた」が77・6％を占め、ゼロトラストがまだ中小企業の現場に十分浸透していない実態が明らかになりました。だからといって「自社は遅れている」と考えるのではなく、自社のネットワークを見直すきっかけとして捉えることが大切です。

ゼロトラストは、大企業だけの特別な対策ではありません。中小企業にとっても「ネットワークを分ける／IDを強くする／端末を確認／ログの監視」といった基本動作の積み重ねとして始められます。大切なのは、言葉に振り回されることではなく、自社のどこに信頼しすぎている部分があるのかを見つけることです。

「社内だから安全」ではなく「必要なアクセスだけを安全に許可する」この発想への切り替えが、これからのネットワークインフラには求められています。

ゼロトラストへの移行は、最新技術を導入するためだけのものではありません。会社の情報資産を守り、働き方の変化に耐えられるネットワークへ整えていくための現実的な設計の見直しなのです。