The serialization title

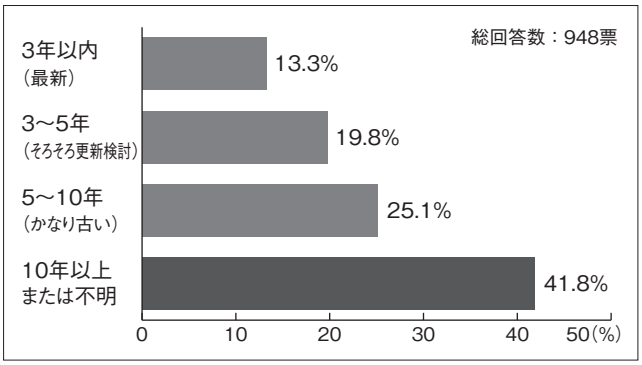
情報システム担当が選ぶネットワークインフラ

第1回 基幹ネットワーク機器の4割超が10年以上運用の実態

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

948名の情報システム担当者へのアンケートで明らかになった衝撃の調査結果があります。それは、4割超の企業が10年以上前のネットワーク機器を使い続け、3社に2社が古い環境で現在も業務を行っているという事実です。普段は意識しない「見えないインフラ」に潜む3つのリスク。なぜ更新は後回しにされ、それにどう対処すべきなのか。本連載では中小企業のネットワーク刷新への道筋を示します。

図1 基幹ネットワーク機器の運用年数



衝撃の調査結果 機器の4割超が10年以上運用

●質問

「貴社のネットワーク機器（スイッチ・ルーター等）はどのくらいの頻度で交換しますか？」

本連載の開始にあたり、弊社がSNS上で右記の質問（アンケート調査）を、情報システム担当者を対象に実施したところ948名から回答が寄せられました。

その内容は、中小企業が抱える深刻な実態を浮き彫りにするものでした（図1）。

実に、4割を超える企業が10年以上前のネットワーク機器を使い続けている、あるいは運用年数すら把握していないという結果が得られました。

さらに、5年以上の機器を含めると全体の66・9％、つまり3社に2社が、古い環境で日々の業務を行っていることになります。

ちなみに、ネットワーク機器とは、会社のパソコンやプリンター、インターネットをつなぐ装置のことで、具体的には「スイッチ」（社内の機器同士をつなぐ装置）や「ルーター」（インターネットと社内をつなぐ装置）を指しています。

それらは普段、事務所の天井裏やサーバールームの片隅に設置されており、目に触れることはほとんどありません。

そして、これは単に「古い機器を使っている」という問題ではなく、企業のセキュリティ、業務効率に加えて、万が一の際の事業継続に直結する重大なリスクが静かに進行し、確実に蓄積されていることを示しています。

なぜ「更新」は「後回し」にされるのか

●失敗＝業務停止のプレッシャー

ネットワーク機器は、企業のIT環境の中で最も「見えにくい」存在です。例えば、パソコンの場合は毎日使っていて、故障すれば仕事になりません。

しかし、スイッチやルーターは天井裏やサーバールームで静かに動き続けているため、普段は存在すら意識されないうえに、調子よく動いている限り「問題ない」と判断されてしまうのです。

それは、建物の配管のようなものです。水道管が古くなっていても水が出ていれば気にしませんが、ある日突然破裂ともなれば、建物全体で水が使えなくなります。ネットワーク機器も同じです。「インターネットが遅い、接続が不安定」といった問題が起きても「Wi-Fiが悪い、パソコンが古い」と考えがちで、ネットワーク機器に問題があるとは思わないケースが多いのです。

さらに、中小企業ならではの事情として予算面の制約があり、効果が可視化されにくい設備投資は、新システム導入や人材採用に比べて優先順位が下がり「まだ使用可能なものをあえて入れ替える必要があるのか」という心理から、経営判断のハードルが高くなります。

ネットワーク機器の更新は、その効果がトラブルの発生を抑制するなど比較的地味なものであるために「経営者への説明が難しい」との声も多く聞かれます。

専門知識の不足も深刻で、中小企業では情報システム部門の人員が1～2名、あるいは総務が兼任のケースも多く、ネットワークの専門家がいない環境では「何年で更新すべきか」「どの製品を選べばよいか」の判断ができず、結果、現状維持を選択してしまいます。

入れ替え作業の煩雑さも無視できません。特に少人数部門では、普段の業務をこなしながらの大掛かりな入れ替えプロジェクトとなり大きな負担になります。

業務を止めない機器交換作業は専門的な技術と念密な計画が必要で「失敗＝会社全体の業務停止」というプレッシャーが、前述の現状維持を選択させます。

こうした理由から「壊れていないから大丈夫」「あと1～2年は使える」と判断されて、更新が先送りされ続けます。そして、気づいたときには10年以上が経過している状況に陥るのです。

古い機器が招く「3つのリスク」

10年前のネットワーク機器を使い続ける危険性を、具体的に大きな「3つのリスク」として、解説します。

〔リスク1〕

速度不足でビジネスチャンスを逃す

10年前と現在では、インターネットの使い方が全く違います。

2016年頃までは、多くの企業が社内サーバーにファイルを保存しメールも社内で管理していましたが、現在は違います（図2）。

当時は充分だった通信速度も今では全く足りず、以下のような問題が発生しています。

- クラウドにファイルをアップロードするのに数分かかる
- オンライン会議中に映像が止まる
- 朝、パソコンを起動するとネットワークが遅い
- 複数人が同時に作業すると極端に遅くなる

貴社はどうでしょうか。これらは単なる不便ではありません。

例えば、営業担当が顧客とのオ

図2　変化しているインターネットの使い方

クラウドサービスの利用：Microsoft365、Google Workspace、会計ソフトなど、常にインターネット経由で使うサービスが増加している

オンライン会議の日常化：Zoomや Teamsでの会議が毎日のように行われている

防犯カメラのネット接続：映像をインターネット経由で確認できるカメラが増えている

さまざまな機器のネット接続：照明や入退室管理など、さまざまな機器がインターネットを経由して動いている

ンライン商談中に映像が停止すれば、信頼を損なうおそれがあります。また、経理担当がクラウド会計ソフトへのデータ入力に時間を要する場合、残業の増加を招きます。

こうした小さなストレスの積み重ねが、社員の不満や生産性の低下を招いているのです。

ネットワークの遅さによる業務の遅れで、従業員1人あたり年間20時間以上の損失が出ているとの試算もあります。社員数50名であれば、年間1千時間、時給3千円で計算すれば、年間３００万円のコストです。

この「見えないコスト」は、経営判断において見落とされがちですが、実は無視できない金額です。

〔リスク2〕

セキュリティの大幅な低下

ネットワーク機器も、パソコンと同じようにプログラム（ファームウェア）で動いています。そして、定期的にセキュリティの欠陥（脆弱性）が見つかり、修正プログラムが配布されます。

しかし、メーカーのサポート期間は通常5～7年です。10年前の機器は既に修正プログラムが提供されない「サポート終了」状態にあります。つまり、新しい欠陥が見つかっても直せないのです。

例えるなら、古い家の鍵が壊れているにもかかわらず、鍵メーカーが廃業していて修理できない状態です。泥棒は、その家が無防備であることを知り、狙ってきます。

実際、２０２３年から２０２４年にかけて、国内でも古いルーターの欠陥を狙ったサイバー攻撃が複数報告されています。攻撃者は、最新の修正プログラムが出ていない古い機器をインターネット上で探し出し、欠陥を突いて侵入します。そこから、会社全体のシステムに攻撃を広げるのです。

特に危険なのは、ネットワーク機器が「会社とインターネットをつなぐ入口」にあることです。ここが突破されれば、どのような高価なセキュリティソフトを入れていても、裏口から侵入されたようなものです。

さらに、古い機器には現代のセキュリティに必要な機能がありません。

- **暗号化通信の処理**：安全な通信を処理する能力が足りません
- **不正な通信の検知**：怪しい通信を見つける機能がありません
- **細かなアクセス制限**：誰がどこにアクセスできるかを細かく管理できません
- **記録の保存**：攻撃を受けた時の調査に必要な記録が残せません

つまり、古いネットワーク機器を使い続けること＝セキュリティの穴を放置することなのです。

〔リスク3〕

突然の故障で業務が完全停止

機械は必ず壊れます。問題は、10年以上前の機器は壊れた際に同じものが手に入らないことです。

既に製造が終了した機器は、メーカーに問い合わせても「販売終了」「在庫なし」という答えしか返ってきません。中古を探すこともできますが、それも古い機械なので、またすぐに故障するリスクがあります。

新しい機種に交換しようとしても設定方法が全く違うため一から設定し直す必要があるうえに、復旧までに数日から数週間かかり、その間は会社の業務が完全に止まることもあります。また、緊急対応では技術者の確保も難しく、費用も通常の数倍に膨らみます。

事例：製造工場のネットワーク機器が突然故障し、生産ラインが3日間停止。代替機器を探して設定し直すのに1週間かかり、結果、数千万円の損失となる。さらに納期が遅れたことで顧客の信用を失い、その後の注文にも影響が出た。

後から「計画的に交換していれば損失は完全に防げた」と悔やんでも遅いのです。このような事例は、実際に発生しています。

特に中小企業では、予備機器の用意もなく、1台が壊れると全社の業務が止まる構造になっています。これは、企業にとって最も避けるべきリスクのひとつです。

ネットワークはセキュリティの土台

●ゼロトラスト

最近、サイバーセキュリティ対策として「UTM」（総合的なセキュリティ機器）や「次世代ファイアウォール」（高度な防御壁）の導入が注目されています。これらは重要な施策ですが、基盤となるネットワークが老朽化している場合、その効果は大きく制限されるという点は見落とされがちです。

例えるなら、高性能な防犯カメラと頑丈な金庫を導入しても、建物自体の老朽化で壁に穴が開いていれば意味がありません。ネットワークはこの建物に相当し、それがしっかりしていないと、どのような防犯設備も役に立ちません。

セキュリティの世界には「ゼロトラスト」という新しい考え方があります。これは、従来の会社の中にいれば安全という考えを捨てて「社内でも常に確認と監視を怠るな」という概念です。

その実現には、図3に挙げたしくみが必要です。

図３　ゼロトラスト実現のしくみ

●ネットワークの分離

「部門ごと」「用途ごと」にネットワークを分けることで、もしどこか一箇所に侵入されたとしても、他には広がらないようにします。例えば、経理部門、営業部門、来客用のWi-Fiを別々に分けておけば、来客用から侵入されても経理のデータは守られます。しかし、古い機器ではこうした細かい分離ができません。

●通信の監視

「どのパソコンがどこと通信しているか」「怪しいデータ送信はないか」を常に監視します。深夜に大量のデータが外部に送られていれば、ウイルス感染の兆候かもしれません。しかし、古い機器には監視機能がなかったり、機能を使うと通信速度が極端に遅くなってしまいます。

●細かなアクセス管理

「誰が」「どの端末で」「どこに」アクセスできるかを細かく管理することで、不正アクセスや持ち込みパソコンからの感染拡大を防ぎます。しかし、10年前の機器にはこうした機能がありません。

つまり、ネットワーク機器を新しくしないと、本当の意味でのセキュリティは強化できないのです。高価なセキュリティ製品を導入する前に、まずネットワークの土台が健全なのかを確認することが重要です。

壊れる前に交換する機器の交換計画の作成

では、どうすればいいのでしょうか。答えは「壊れてから慌てる」のではなく「壊れる前に計画的に交換する」習慣をつけることです。

ネットワーク機器にも、自動車の部品と同じように「交換時期の目安」があります。一般的な目安は以下のとおりです。

・ルーター・セキュリティ機器　5年
・基幹スイッチ（重要な機器）　5～7年
・フロアスイッチ（各階の機器）　7～10年
・無線LAN機器　3～5年

無線LANの交換時期が短いのは、Wi-Fi規格の進化が速いためです。現在は「Wi-Fi 6」が主流ですが、数年後には「Wi-Fi 7」が普及します。

一方、有線の機器は規格が安定しており、やや長めの期間使用しても問題ありません。これを踏まえ、段階的に交換する計画を立てることが現実的です。ちなみに、一度に全部を交換する必要はありません。

以下で、その流れ（第1～3段階）を解説します。

〔第1段階〕入口のセキュリティ機器を最優先する（最重要）

まずインターネットとの接続口にあるルーターなどの機器を交換します。ここを守ることが最も重要で費用対効果も高い投資です。

比較的少ない予算（数十万円～100万円程度）で、最大のリスクを減らせます。最新機器は従来の数倍の速度で、セキュリティ機能を使っても速度が落ちません。

〔第2段階〕

会社全体を支える中心機器

全フロアを支える中心的な基幹スイッチなどの機器を新しくします。ここで部門ごとにネットワークを分ける設定をすることで、万が一の侵入時にも被害を最小限に抑えられます。また、高速通信に対応した機器にすることで、将来のデータ量増加にも対応できます。投資は数百万円程度になりますが、会社全体の速度とセキュリティが大きく向上します。

〔第3段階〕

各フロアの機器と無線ＬＡＮ

社員に近い部分の機器を交換し、快適性とセキュリティを両立させます。最新のＷｉ－Ｆｉ機器への交換で、在宅勤務との併用時代に必要な速度も確保できます。

また、電源供給機能のある機器にすることで、ＩＰ電話や防犯カメラへの電源も一緒に供給できるため、配線が簡単になります。

この3段階を1～2年かけて順番に実施することで、予算を分散でき、業務への影響も最小限に抑えられます。各段階で得た経験を次に活かすことで、より良い構成を実現できます。

経営者を説得する「3つのポイント」

担当者の最大の課題は「経営者にネットワーク機器交換の必要性を理解してもらうこと」です。以下の3つの視点で説明すると効果的であり、これは経営者も知っておく必要があります。

〔ポイント1〕

もし止まったらいくら損するか

「業務が1日止まったら、いくらの損失になりますか?」を具体的に示します。売上の機会損失、従業員の給料、お客様からの信頼など、これらを金額にすると数百万円から数千万円になることも珍しくありません。

例えば、従業員50名、平均日給2万円であれば、1日の人件費が１００万円。これに売上の機会損失を足せば、数日止まるだけで交換費用を超える損失が出ます。

〔ポイント2〕

計画的交換と緊急対応のコスト比較

計画的に交換する場合と、壊れてから慌てて対応する場合のコストを比較します。計画的なら通常価格で機器を買い、夜間や休日に作業できます。一方、緊急対応では高い代替機、休日・深夜の割増人件費、業務停止の損失が加わります。合計では3～5倍のコストになることもあります。

自動車で例えれば、定期点検とエンジンが壊れてからの修理の違いです。

〔ポイント3〕

社員の働きやすさと人材確保

快適なＩＴ環境は、社員の満足度や生産性に直結します。さらに、優秀な人材の採用にも影響します。「ＩＴが古い会社」は、特に若い世代から敬遠されます。

応募者が「この会社のＩＴは時代遅れだ」と感じれば、採用で不利になります。ネットワークへの投資は人材戦略の一部です。

「見えない設備」を「重要な資産」に

ネットワークは、会社のすべての活動を支える血管のようなものですが、その重要性は止まってから気づくことが多いのです。

冒頭のアンケート結果が示す通り、多くの中小企業が古いネットワーク環境で綱渡りを続けています。しかし、これは「仕方ない」ことではありません。正しい知識と計画があれば、限られた予算の中でも安全で快適なネットワーク環境は実現できます。

さて本連載では、全8回にわたり、各種の技術や選び方、段階的な刷新計画まで、中小企業に必要な知識をわかりやすく解説していきます。

「見えない設備」を「会社を支える重要な資産」として認識し直す、その一助となれば幸いです。