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2回

社内ネットワーク「分離なし」が4割
外部からの侵入拡大のリスク

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

社内ネットワークを「分けていない」企業が約4割。184名への調査で、このような実態が明らかになりました。ネットワークを分けずにいると、一度でもサイバー攻撃を受けてしまうと、社内全体に一気に被害が広がります。今回は「ネットワークの分離」という考え方と、それを実現する機器の選び方について、ITに詳しくない方でも理解できるように、身近な例を挙げて解説していきます。

衝撃の実態 4割が「分離なし」

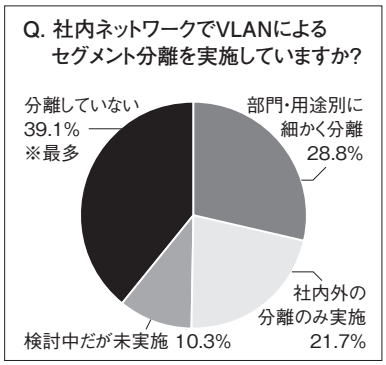
Q：社内ネットワークでVLANによるセグメント分離を実施していますか？

今回のアンケートは、SNS上で情報システム担当者を対象に実施し、184名から回答が寄せられました。注目すべきは、最多回答の「分離していない」が約4割に達したことです。さらに「社内外の分離のみ」という回答も21・7%ありました（図1）。

これは、インターネットの出入口は管理しているものの、社内ネットワークがひとつながりになっている状態を示しています。

「社内は分けなくても大丈夫では？」と思われるかもしれませんが、実は社内ネットワークを分けていないことがサイバー攻撃の被害を最大化させる大きな要因になっています。今回は、その理由と対策を詳説します。

図1　アンケート結果



「ネットワーク分離」の意味を正しく理解する

まずは、会社の中にあるネットワークをイメージします。

各デスクのパソコン、Wi-Fi、プリンター、受付のタブレット、会議室のモニター、防犯カメラなどが、すべて同じ1本の回線でつながっている状態が「フラットネットワーク」です。

これを用途や部門ごとに区画分けするのが「ネットワーク分離」です。その代表例として「VLAN（Virtual LAN）※」などの技術を使って、論理的にネットワークを区切る手法があります。

それは、物理的に別々のケーブルを引くのではなく、1本のケーブルの中を「仮想的な壁」で区切るイメージで、たとえるなら、事務所の大きなワンフロアーを壁で仕切って、部署ごとに部屋分けした状態です。

※ VLAN（Virtual LAN）：1台のスイッチや同一の物理LAN上にある機器を、論理的に複数のネットワーク（仮想LAN）に分割し、同じVLAN内だけL2通信できるようにする仕組み。

図２　具体的な侵入経路の例

ケース１：来客用 Wi-Fi からの侵入

会社を訪れた業者や来客が、社内で提供された Wi-Fi につないだとき、その端末がウイルスに感染していた場合、社内の機器と同じネットワークに接続されている状態では、他の機器へ攻撃が試みられる可能性があります。ネットワークが適切に分離されていれば、来客用の Wi-Fi と社内のネットワークは別々に管理されるため、こうしたリスクを大幅に低減できます。

ケース２：防犯カメラからの侵入

防犯カメラや入退室管理などの IoT 機器は、セキュリティ対策が手薄なものも多く、攻撃者に狙われやすい機器です。これらが社内の業務用ネットワークと同じ回線につながっていると、機器を乗っ取られた際に社内ネットワークへの侵入の足がかりになる可能性があります。セキュリティカメラを踏み台にした企業への侵入事例は国内外で多く報告されています。

ケース３：感染パソコンからの拡大

１台のパソコンがウイルスに感染した場合、社内のネットワークが分かれていなければ、このパソコンから同じネットワーク上の他の端末へ感染が広がる可能性が高まります。特に被害が大きいのが「ランサムウェア」と呼ばれる身代金要求型のウイルスです。社内の多くのファイルが暗号化されて使えなくなり「元に戻してほしければお金を払え」という要求が届きます。復旧には多大な時間とコストがかかり、身代金を払っても確実に回復できる保証はありません。

分ける前（フラットネットワーク）は、誰でも他の部署へ自由に行き来できます。一方、分けた後は、経理・営業・来客用の部屋などにそれぞれが独立しているため許可なく移動ができません。

具体的には、以下のように分けることが一般的です。

・業務用ネットワーク：社員のパソコンや業務システム
・来客、ゲスト用ネットワーク：来客に提供するＷｉ‐Ｆｉ
・ＩｏＴ機器用ネットワーク：防犯カメラ、入退室管理、スマート機器
・サーバー用ネットワーク：重要データが入ったサーバー群

ではなぜ、この「仕切り」をつくることが重要なのでしょうか。

分離していないと被害が全社に広がる

ネットワークを分けていない状態の怖さは、どこか一箇所が攻撃を受けてしまうと、社内全体に被害が広がりやすいことです。

「横展開攻撃」と呼ばれる手口があり、まず攻撃者は比較的ガードが低い場所から侵入し、そこから社内の他のシステムへと次々に移動して感染を広げて、侵入後に社内を「偵察」しながら、重要なサーバーや機密情報を探し当て、最終的に全社のデータを盗んだり暗号化したりします。

この手口が厄介なのは、侵入から被害が出るまでに時間がかかるため、気づいたときには手遅れになっていることが多い点です。具体的な侵入経路の例を見てみましょう（図２）。

ネットワークを分離しておけば、感染が広がる範囲をひとつの区画に限定できます。経理のネットワークが感染しても、営業のネットワークには届きにくくなります。被害を「消火できる範囲」に抑えられるのです。

これを火災でたとえるなら、防火扉のない建物と、防火扉で区画分けされた建物の違いです。防火扉があれば、一部屋が燃えても隣の部屋は守られます。ネットワーク分離は、サイバー攻撃に対する「防火扉」の役割を果たします。

分離を実現する「スイッチ」を知る

では、ネットワーク分離はどうやったら実現するのでしょうか。鍵となるのが「スイッチ」という機器で、社内の複数の機器をつなぐ「ハブ」のような機器です。

社内のパソコンやプリンターをＬＡＮケーブルで挿し込み、それぞれが通信できるようにする装置で、オフィスのいたるところに設置されています。このスイッチには大きく２種類があります。

●レイヤー２スイッチ（Ｌ２スイッチ）：基本的なスイッチ

機器同士をつなぎ同じネットワーク内でデータを転送する、いわ

ば「社内の郵便配達役」です。家庭用のスイッチやハブの多くもこのタイプに近い機能を持ちます。

ＶＬＡＮの設定ができる製品も多くありますが、分けたネットワーク間での通信制御は、基本的にルーターやレイヤー３スイッチで行います。小規模なオフィスやフロアの末端（各デスク周辺）で使うのに適しています。

●レイヤー３スイッチ（Ｌ３スイッチ）：高機能スイッチ

異なるネットワーク間でのデータの行き先を管理する「社内の交通整理役」で、ルーターに近い機能を持ちます。複数のＶＬＡＮを設定したうえで「経理と営業の間は通信させない」「サーバーへはどの部門からもアクセスできるが、来客Ｗｉ‐Ｆｉからはアクセス禁止」という、細かなルール設定ができます。

中規模以上の企業や、複数のＶＬＡＮを詳細に管理したい場合に必要な機器です。一般的に、会社の中心に設置する基幹スイッチにはＬ３スイッチが採用されます。

スイッチを選ぶ際の重要ポイント

スイッチの選択には、以下の重要な確認ポイントがあります。

●ポート数と速度

ポートとは、ＬＡＮケーブルを挿す差し込み口のことです。接続する機器の数より少し多めのポート数を選ぶことが重要です。将来の増設も見込んで余裕を持たせましょう。

速度は「１Ｇｂｐｓ」か「10Ｇｂｐｓ」が主な選択肢です。一般の社員のパソコンをつなぐフロアスイッチは１Ｇｂｐｓで十分ですが、サーバーへの接続や基幹となる中心的なスイッチには10Ｇｂｐｓ対応が推奨されます。

●ＶＬＡＮ機能と管理機能

ネットワーク分離を実現するには、スイッチがＶＬＡＮ機能に対応していることが必須で、そのためには「マネージドスイッチ」と呼ばれる管理機能付きの製品が必要です。つなぐだけで動く安価な「アンマネージドスイッチ」ではＶＬＡＮの設定ができないため、企業向けのマネージド製品を選ぶことが重要です。

●クラウド管理対応

近年、インターネット経由でスイッチをまとめて管理できる「クラウド管理型」の製品が増えています。複数拠点を持つ企業やＩＴ担当者が常駐できない拠点でも、本社から一括管理ができるため、運用の手間が大幅に減ります。

特に《情シス担当者》が少ない中小企業では、このクラウド管理機能が大きなメリットになります。設定変更や障害確認をどこからでも行えるため、夜間や休日の突発対応にも強みを発揮します。

●信頼性と保守サポート

企業向けスイッチを選ぶ際は、製品の保証期間とサポート体制の確認が必須です。故障した際にすぐに代替機が手配できるか、メーカーサポートはいつまで受けられるかを事前に確認してください。

前回でも触れた「保守切れ」を避けるため、サポート期間の長い製品を選ぶことが重要です。

ＰｏＥで配線をシンプルにする

スイッチを選ぶ際、もうひとつ理解しておきたい機能が「ＰｏＥ（Power over Ethernet）」です。

ＰｏＥとは、ネットワークのケーブル１本で、データ通信と電力供給を同時に行う技術です。

通常、Ｗｉ‐Ｆｉのアクセスポイント（無線ＬＡＮ機器）や防犯カメラ、ＩＰ電話などを設置する場合、ＬＡＮケーブルの他に電源コードも必要です。しかしＰｏＥ対応のスイッチを使えば、ＬＡＮケーブル１本で通信と電力の両方を賄えるため、電源コンセントがない場所にも設置できます。

天井や壁の高い位置にＷｉ‐Ｆｉアクセスポイントを設置したいとき、近くにコンセントがなくてもＬＡＮケーブルを引くだけで設置でき、電波の届き具合を考えた最適な場所に設置できます。配線の本数も半分に減り、オフィスの

図３　スイッチ選択の失敗例

スイッチ選びでよくある３つの失敗

実際の現場では、スイッチ選びで同じような失敗が繰り返されています。導入前に知っておくべき代表的なケースを紹介します。

失敗①「安いから」と家庭用製品を選んでしまう

ホームセンターや家電量販店でも売られている安価なスイッチを、オフィスに導入するケースがあります。しかし、こうした製品の多くはアンマネージドスイッチであり、VLANの設定ができません。

また、故障しても保証やサポートが薄く、業務への影響が長引くことがあります。価格の差は数千円から数万円でも、後から企業向け製品に買い替えるコストと手間を考えると、最初から適切な製品を選ぶほうが賢明です。

失敗② 現在の台数だけで選んでしまう

「今は20台しかつながないから24ポートで十分」と考え、ちょうどの台数で購入するケースです。しかし、社員増員や新しい機器の追加により、１～２年後にはポートが足りなくなることは珍しくありません。

追加でスイッチを購入してつなぎ合わせると、管理が煩雑になり、障害時の対応も難しくなります。購入時は「今の1.5倍程度の余裕」を持ったポート数を基準にすることをお勧めします。

失敗③ PoEを後から考えてしまう

スイッチを購入した後に「やはりWi-Fiアクセスポイントを天井に設置したい」「防犯カメラをPoEで給電したい」と気づくケースです。後からPoE対応スイッチに交換しようとすると、機器の買い替えだけではなく設定の移行作業も発生します。

将来的にWi-Fiや防犯カメラの設置を検討しているのであれば、あらかじめPoE対応の製品を選定しておくことで、長期的にはコストの抑制につながります。

見た目もスッキリします。

さらに、ＰｏＥ対応スイッチにＵＰＳ（無停電電源装置）を接続しておくと、停電時でも一定時間、Ｗｉ‐Ｆｉアクセスポイントや防犯カメラに電力を供給し続けられるため、業務継続の観点からも有効なしくみです。

ＰｏＥには、供給できる電力の上限によっていくつかの規格があります。一般的なＷｉ‐Ｆｉアクセスポイントや小型カメラなら「ＰｏＥ＋（30Ｗ）」で対応できますが、高機能なアクセスポイントや一部のカメラには「ＰｏＥ＋＋（60Ｗ～90Ｗ）」が必要な場合もあります。機器の仕様に合わせた規格を選ぶことが重要です。

図3にスイッチ選択の失敗例を示しました。あわせてご確認ください。

「分けること」が守りの第一歩

今回のアンケートでは、約4割の企業で「社内ネットワークを分けていない」という現実が明らかになりました。その一方で、部門・用途別に細かく分離している企業が28・8％存在しており、セキュリティ意識の高い担当者は着実に対策を進めています。

ネットワーク分離の導入に迷ったら、まずは「来客用Ｗｉ‐Ｆｉを社内のネットワークから切り離す」ことから始めてください。

これは、リスク回避効果が最も高く、かつシンプルに実施できる分離です。費用もそれほどかからず、既存のスイッチがＶＬＡＮ対応であれば設定変更だけで実現できるケースもあります。その一歩が踏み出せれば、次は「ＩｏＴ機器を別ネットワークに移す」「部門間の通信を制限する」という流れで段階的に強化できます。

ネットワーク分離は「攻撃を防ぐ」ための対策ではなく「攻撃を受けても被害を最小限に抑える」ための対策です。１００％の防御は難しくても、被害の範囲を限定する「防火扉」を設置することは、すべての企業にとって現実的かつ有効な選択です。