The serialization title

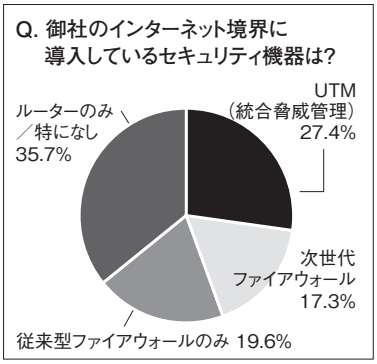
情報システム担当が選ぶネットワークインフラ

第4回 境界防御、4割が未整備の実態

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

弊社がX（旧Twitter）で実施したアンケート（791票）で、インターネット境界に「ルーターのみ／特になし」と回答した企業が35.7%と最多で、約4割の中小企業が実質的な境界防御を持たない実態が浮き彫りとなっています。本稿では、OSI※1レイヤー構造から境界防御のしくみを整理し、UTM※2・次世代ファイアウォールの機能と選定の落とし穴、中小企業に適した導入・運用基準を解説します。

図1 アンケート結果（回答数791票）



4割がインターネットの境界防御なし

●無施錠の玄関状態

インターネットの入口を守る境界防御について企業がどのような対策を講じているのか、アンケート結果を詳しく読み解くと「UTM（統合脅威管理）が27・4%」「次世代ファイアウォールが17・3%」と、高度なセキュリティ機器の導入が進んでいる企業が存在する一方で、最も多かった回答は「ルーターのみ／特になしが35・7%」となっており、この結果は約4割の中小企業では、事実上インターネットの脅威に対して十分な防御が行われていない状態にあることを示しています。

また、この傾向は規模が小さくなるほど顕著で、日々の業務に追われる中で十分な対策に手が回っていない現状が伺えます。

現場でよく耳にするのが「各パソコンにウイルス対策ソフトを入れているから大丈夫だろう」という声ですが、これは、例えるなら「建物の玄関の鍵を開けっ放しにしたままで、各部屋のドアにだけ鍵をかけている」状態です。

攻撃者にとって、無施錠の玄関から建物内に侵入することは極めて容易であり、一旦内部に入り込まれてしまえば、被害が拡大するリスクが大幅に高まります。入口での防御が欠けているだけで、内部全体のセキュリティリスクは飛躍的に高まるのです。

また「従来型ファイアウォールのみ」と回答した企業も19・6%で、後述しますが、従来型ファイアウォールは静的なルールに基づく通信制限しか行えず、複雑化・巧妙化する現代のサイバー攻撃を防ぐには十分とはいえません。

これらを合わせると、半数以上の企業が現代の脅威レベルに見合わない装備でインターネットに接続していることになります。

IPA（情報処理推進機構）などの調査でも、中小企業の約半数がランサムウェアに対する備えが不十分であるという実態が浮き彫

※1 OSI (Open System Interconnection)：デジタル環境の構築方法を定める基本的な概念。
※2 UTM（Unified Threat Management 統合脅威管理）：コンピュータウイルスやハッキングなどの脅威からネットワークを保護する手法。

りになっています。攻撃者にとって最も狙いやすく、侵入の足がかりにされるのが「入口（境界）」なのです。

これは「意図的に対策をしていないのではなく、日々の業務に追われ高度化する脅威に対策が追いついていない企業が多い」というのが実情です。裏を返せば、境界部分の防御を適切に講じるだけで、企業のセキュリティレベルは大きく向上します。

ルーターだけでは会社を守れない

●中身が危険か判断できない

ルーターの本来の役割は、異なるネットワーク間でパケットを中継することにあります。

IPアドレスとルーティングテーブルに基づき、届いた手紙（データ）を宛先へと効率よく転送する「郵便局の仕分け」のような役割に特化しており、手紙の中身が危険なものかどうかを判断する機能は持たず、通信の道案内をするのが目的であり、安全性を検査するための装置ではありません。

一方で、現代のサイバー攻撃は単純な不正アクセスではなく「通信の中身（コンテンツ）」を巧妙に偽装して侵入を試みます（図2）。

さらに昨今、インターネット通信の大半が、HTTPのセキュアバージョンHTTPSによって暗号化通信されており、そのままでは中身を確認できず「通信先が正規であっても、中身が危険なケース」を素通りさせてしまいます。

暗号化技術はプライバシー保護のために不可欠ですが、同時にサイバー攻撃者にとっても悪意ある通信を隠すための絶好の隠れ蓑となっているのが現実です。

図2　現代のサイバー攻撃の例

■ 改ざんされた正規のWebサイトを閲覧しただけでマルウェアに感染する「ドライブバイダウンロード」攻撃

■ 本物そっくりのフィッシングURLを経由してマルウェアを配布する手口

これらの攻撃は、通信先自体は正規のサーバーや、一見すると問題のないURLであるため、ルーターのしくみでは異常を検知できません。郵便局員が宛先だけを見て手紙を届けるように、ルーターは危険なデータであっても宛先が合っていれば社内に通してしまいます。

2024年にも、VPN機器やルーターの既知の脆弱性（未適用パッチ）を突かれ、ランサムウェアに感染した日本企業の被害事例が相次ぎました。境界での厳密な検査が行われていなければ、最終的な防御はPC上のEDR※3などのエンドポイント対策に委ねられ、負荷とリスクが一点に集中してしまいます。

境界、ネットワーク内部、エンドポイントの3層でそれぞれ脅威を食い止める「多層防御」の観点からも、入口での高度な検査は絶対に欠かせない要素なのです。

現代に必要な「境界防御」とは

●境界防御機器が担う主な機能群

境界防御を具体的に理解するためには、ネットワークの通信階層を示す「OSIレイヤー（階層）構造」の概念が役立ちます。

インターネット上のあらゆる通信は、物理的な信号からアプリケーションの表示まで、複数の階層を経て処理されています。ちなみに、従来型ファイアウォールが守備範囲としているのは、主に、

- **L3（ネットワーク層）**：IPアドレスに基づく通信の許可・拒否を行う
- **L4（トランスポート層）**：ポート番号（例えば、Web通信の80番や443番など）による制御を行う

この2つですが、あくまでも「外装のチェック」に過ぎません。差出人と宛先、そして荷物の大まかな種類（Webかメールかなど）を見ているだけで、箱の中に何が入っているかは全く確認していない状態です。

これに対して「次世代ファイアウォール（NGFW）」や「UTM」は、L7（アプリケーション層）まで深く踏み込んで通信を制御します。つまり「手紙の中身（通信内容）まで開封」して、アプリケーションの識別やコンテンツの安全性を検査するのです。

例えば、ポート443番（HTTPS）の通信であっても、それ

※3 EDR：コンピュータシステムのエンドポイント（PC、サーバー、スマートフォンなどの末端機器）において脅威を継続的に監視し、対応するサイバーセキュリティ技術

図３　境界防御機器が担う主な機能群

- **IPS（侵入防止システム）**：既知の攻撃パターンをシグネチャと照合してリアルタイムに検知・遮断する。
- **アンチウイルス**：ダウンロードされるファイルを検査する。
- **Web フィルタリング**：危険なサイトや業務に無関係なサイトへのアクセスを制限する。
- **アプリケーション制御**：特定の SNS や個人用クラウドストレージの利用だけを制限することが可能。
- **SSL/TLS インスペクション**：暗号化された通信を機器内で一度復号し、中身の安全性を検査したうえで再度暗号化して届ける機能で、現代の脅威に対抗するための要となる。ただし、適切な証明書管理と運用設計が前提となる点に注意が必要。

が業務に必要なＷｅｂサイトの閲覧なのか、危険なマルウェアのダウンロードなのかを識別し、後者であれば即座に遮断します。

こうした高度な境界防御機器が担う主な機能群には、図３のようなものがあります。

これらの機能は単体で動くのではなく「組み合わせ」によって初めて強固な多層防御が成立します。今、境界防御の概念は「通信を通すか止めるか」という単純な門番ではなく「どのレベルで、どの通信を安全とみなして許可するか」を総合的に判断する高度な検疫システムへと転換しています。

なお、目指す防御の方向性は同じですが、ＵＴＭはこれらの機能をオールインワンで提供する統合型であり、ＮＧＦＷはＬ７制御に特化しつつ必要に応じてオプションで機能を拡張していくといった違いがあります。

安価なＵＴＭに潜む落とし穴

●カタログ値を鵜呑みにしない

境界防御の重要性を認識し「とりあえずＵＴＭを入れているから安心」と考える中小企業には、大きな落とし穴が存在します。

それが、カタログ値と実効性能の乖離（いわゆる性能差）の問題と運用放置のリスクです。コストばかりを優先して選定した結果、実務に耐えられない事態に直面するケースが後を絶ちません。

安価なＵＴＭを導入した際に、カタログ値の「最大１Ｇｂｐｓ対応」を鵜呑みにするのは危険で、多くの場合、その数値はセキュリティ機能をすべてオフにした「単なるファイアウォール機能のみ」を動作させた理論値です。

自動車でいえば、エアコンやオーディオなどの装備をすべて外して、直線コースを走ったときの最高時速のようなものであり、実際の業務環境を反映していません。

前述したＩＰＳ、アンチウイルス、そしてＳＳＬ／ＴＬＳインスペクションなどの機能をすべて有効にすると、機器の処理負荷は急激に跳ね上がります。

特に、ＳＳＬ／ＴＬＳ通信の検査は、パケットを受信するたびに「復号→内容解析→再暗号化」という重い３ステップの処理が毎回必要になり、その結果、カタログ上は１Ｇｂｐｓ対応の機器であっても、実環境で全機能を有効にすると実効スループットが数百Ｍｂｐｓ以下にまで激減するケースが頻発します。

こうして通信速度が極端に遅くなると、業務への支障を避けるために「重いセキュリティ機能をオフにする」という悪循環が生じ、何のためのセキュリティ機器の導入かがわからなくなります。

また、ＵＴＭの各種機能はサブスクリプション（定期契約）型で提供されることが多く、ライセンスの更新切れを放置した結果、機能が停止し、ただの箱と化している危険な運用スタイルも見受けられます。安く買って放置することが最も危険な選択であり、それを避ける適切な選定と運用には、

- 実効スループット
- 全機能有効時の性能
- ライセンス管理

この３点を必ず確認してください。

境界防御の適切な選び方とは

中小企業における境界防御機器の選定と運用はいかにすべきなのか。前述の落とし穴を回避して自社に最適な機器を導入するためには、いくつかの重要な選定基準と運用プロセスの順守が必須です。

●選定の基本原則

それは「自社の通信量と利用実態を正確に把握すること」です。単純にオフィスの人数だけで機器の規模を決めるのは危険で、同時接続するユーザー数に加えて、クラウドサービス（SaaS）の利用状況や大容量データの送受信頻度、Web会議の実施頻度などを総合的に考慮する必要があります。

●機器のカタログスペック比較

すべてのセキュリティ機能（IPS、アンチウイルス、SSL／TLSインスペクション等）を常時有効にした状態での実効スループットを基準に、サイジング（機器の規模選定）を行わなければなりません。

さらに、ネットワークの通信量は業務のデジタル化に伴い年々増加する傾向にあるため、導入時の通信量ギリギリの性能を選ぶのではなく、将来を見越して20～30％以上の余裕（バッファ）を持たせたモデルを選択することが大切です。ギリギリの性能で導入してしまうと、わずか1～2年で機器の買い替えを迫られることになりかねません。

●数年間のトータルコスト

確認すべきは「総所有コスト（TCO）の観点」であり、機器の初期導入コスト（ハードウェア費用）だけではなく、各種セキュリティ機能を利用するための年間サブスクリプション費用、および障害時の保守サポート費用を合算し、3～5年間のトータルコストで比較検討することが重要です。

●ライセンスの更新管理

実はこれが非常に重要で、更新手続きを忘れてしまうとセキュリティ機能が即座に停止し、ネットワークが十分に防御されない状態に陥ってしまいます。

●運用のしやすさ

これも機器選びの大きなポイントです。ログの可視化、危険な通信を検知した際のアラート通知、そしてリモート環境からでも設定変更が可能なリモート管理機能が備わっているかを確認します。

また、自社のIT担当者の技術力や人員体制に見合わない複雑すぎる機器を導入してしまうと、適切な設定やチューニングが行われず「運用放置」の状態に陥るリスクが高まります。

もし、自社での運用管理が難しい場合は、MSP（マネージドサービスプロバイダー）や、システムインテグレーターへ監視・運用を委託するという選択肢も積極的に検討すべきです。

●段階的な導入

初日からすべての機能を適用すると、正常な業務通信まで遮断してしまうトラブルが発生する可能性もあります。

まず、UTMの基本機能（アンチウイルス・Webフィルタリング）を有効化して通信傾向を把握し、その後、アプリケーション制御などの高度なNGFW機能へとステップアップしていく進め方が、業務影響を最小限に抑えつつセキュリティを着実に強化できる確実な方法です。

機器の信頼性を評価する際は、情報セキュリティに特化したNSS Labsなど第三者評価機関のテスト結果や、業界での導入実績も判断基準として参照してください。

【まとめ】

「4割の企業がルーターのみ、あるいは特に対策をしていない」今回のアンケート結果が示す現実は、日本の中小企業が抱えるサイバーセキュリティ上の深刻な課題を浮き彫りにしています。

もはや境界防御は単なるIT投資ではなく、事業継続（BCP）と社会的信用を守るための「経営課題」として捉えるべき段階に達しています。

現在「ルーターのみ」の環境の企業は、今すぐ実態を確認し対策に乗り出す必要があります。自社の通信量と業務要件を把握したうえで、段階的にUTMやNGFWを導入し、適切な機能を有効化していくことが求められます。

境界防御を軸に多層防御体制を整えることが、高度化する脅威環境に対抗するための極めて有効な現実解のひとつです。