ネットワーク・セキュリティの潮流（第4回）

ネットワークセキュリティで注目されるUTMとは

2021.01.20

ネットワークセキュリティ分野のキーワードに「UTM」（Unified Threat Management：統合脅威管理）というものがある。UTMとはこれまで個別に提供されていた複数のセキュリティ機能を包括的に対処するサービスで、ビジネスシーンにおける情報セキュリティ対策の仕組みとして注目を集めている。

UTMはファイアウオールの機能をベースに複数のセキュリティ機能がまとめられ、従来型セキュリティ対策の問題解決を行うものだ。現在、セキュリティベンダーをはじめとするIT関連企業から各種の製品・サービスが提供されている。導入に際しては、自社にとって必要な性能が確保されているのはもちろん、サポートの内容、導入・運用コストなどを踏まえた検討が求められる。

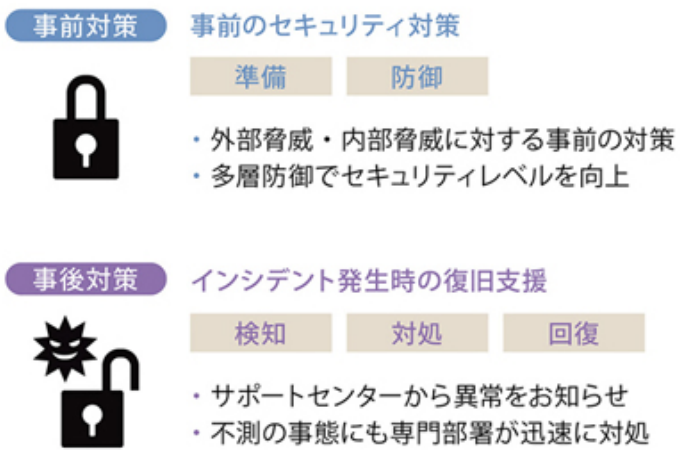
米フォーティネット社の「FortiGate」はトップレベルのシェアを誇るUTM製品で、世界各国の大企業や大学、政府機関で導入されている。ほかにもジュニパーネットワークス社、チェック・ポイント・ソフトウェア・テクノロジーズ社といった大手企業が市場をけん引している印象だ。

NTT西日本では「セキュリティおまかせプラン プライム」（※）においてUTM機能を提供している。ファイアウオール機能やアンチウイルス機能をはじめ、悪意のある第三者が情報を盗み出そうとする詐欺行為を防止するアンチフィッシング機能、有害なサイトへのアクセスを禁止させるURLフィルタリング機能、内部に侵入したウイルスによる外部へのアクセスを制御するIPS（Intrusion Prevention System：侵入防止システム）などが組み込まれる。ネットワーク上のさまざまな脅威に対処する機能が提供され、個別に対策を行った場合に比べて導入が簡単なのが最大の特徴だ。

導入後の管理の部分でもUTMにはメリットがある。個々のパソコンで対策を講じるには台数に応じた人手と手間が必要だが、UTMはゲートウェイで一元的に管理するため、担当者の負担軽減が期待できる。また、絶え間なく行う必要があるネットワークの監視やファームウエア、ウイルスソフトの更新作業も一元化され、社員がそれぞれの端末で行う必要がない。「うっかり」「忙しくて」といった人的ミスの発生が予防できるのも魅力だ。

専任の担当者を置けない事業規模の企業がUTMを導入する場合には、サポートもポイントとなる。NTT西日本のセキュリティおまかせプラン プライムの場合は、ネットワークの入り口と出口対策に加えて、24時間365日の通信監視がある。万が一の異常発生時には電話やメールで連絡が入り、問題解決をサポートする。オプション対応になるが、やむを得ない事態におけるOS初期化やパソコン環境の復旧が必要な際には、お客さまオフィスを訪問して業務復旧を支援する。

【セキュリティおまかせプラン プライムの特徴】



高度化する攻撃方法

そもそもこうしたセキュリティ対策を、サポートが充実した外部業者にある程度まかせたほうがよいとされる理由は、昨今のサイバー攻撃の絶え間ない高度化に他ならない。

企業における情報セキュリティ対策の歴史は、パソコンが本格的にビジネスで使われるようになった1990年代に遡る。当初の対策は、保存されたデータのパスワード管理などが中心だった。その後、LANよって複数のパソコンがネットワークでつながり、インターネットへの接続が一般化するとともに、外部からの侵入・攻撃という新たな脅威への対策が必要となった。

具体的には、ネットワークの入り口（ゲートウェイ）に壁（ファイアウオール）をつくって不正アクセスを防ぐ手段、およびパソコンに侵入するウイルスへの対処手段（アンチウイルスソフト）などが導入され、一般的な対策として普及した。

新たな脅威がはびこる要因は、インターネット利用の増加と多様化だ。メールの送受信、サイトの閲覧に加えて、最近は業務連絡の効率アップを目的に多様なインターネット上でのサービス活用の機会が増えた。インターネットおよびLANで用いられるTCP/IPという共通の通信方式は便利な半面、常に外部への窓が開いた状態に相当する。

情報を盗み出そうとする者にとって、インターネットに接続した状態のパソコンは侵入口として格好のターゲットとなる。サイトを閲覧しただけで感染するウイルスやIM（Instant
Messenger）経由の侵入など、従来想定されなかった攻撃方法が次々と繰り出されるようになったのだ。

担当者が確保できず対策が後手に

これらを防御するにはパソコンをネットワークから切り離すしかない。実際に個人情報を扱うパソコンは単独で使用している企業もあるが、業務効率・スペース・予算などの観点から使い分けが難しく、共用しているケースが一般的だ。

ファイアウオールで不審な通信を遮断できても、通信記録確認や障害対策は行わなくてはならない。担当者が不在の場合は迅速に対応できない。アンチウイルスソフトは頻繁に更新しなくてはならず、きちんと運用するには管理者の存在が求められる。

加えて、セキュリティ対策として多くの装置やソフトを導入するにはコスト負担も大きい。セキュリティの強化によってパソコンの動作が遅くなるなど使い勝手に影響が出る点も無視できない。人員やコスト、使いやすさなどによる制約を理由に対策を行わずに問題が生じれば、責任を問われるだけではなく社会的な信用も大きく損なわれてしまう。

製品・サービス＋人でより強固なセキュリティ環境に

セキュリティ対策の担い手として注目を集めるUTMだが、導入に当たっては注意点もある。まずUTMは“万能薬ではない”のを認識しておくべきだ。UTMの管理はゲートウェイで行われるため、人的対策として社員に対するセキュリティ教育などを並行して実施することが欠かせない。

例えば社員が持ち込んだUSBメモリーによるウイルス感染防止策や、USBメモリーやスマートフォンによる情報持ち出し規制などを用意しなければ、セキュリティ対策は不十分だ。「UTMを導入するだけで大丈夫」などといったセールストークを受けても決してうのみにしてはいけない。

また、ゲートウェイは文字通り社内システムの入り口なので、そこでトラブルが発生した場合、最悪すべての通信不全となる可能性がある。トラブル発生時にどのようなサポートを受けられるのか、代替手段の確保を含めて十分チェックしておきたい。

UTMは設置するだけで完結する装置ではなく、適切なアップデートが不可欠だ。そのためには、導入後にも費用が発生し続けることを覚悟したい。UTMを運用するには監視と更新が必要で、運用コストが相応にかかってくると認識しておいたほうがよいだろう。

現在のオフィス環境で、完璧なセキュリティ対策というものは残念ながら存在しない。UTM導入をはじめとする包括的な対策を検討し、さらにセキュリティに対する意識を一時的ではなく常に高く保ち続ける姿勢が大切だ。

いうまでもなく企業のシステムには重要な情報が保管されており、流出は決して許されない。企業にとって大切な財産でもある情報をいかにして守っていけばいいのか。業種や規模を問わず、すべてのビジネスユーザーが「待ったなし」で対策を進めるべき局面を迎えている。

※本サービスは、ネットワーク上の脅威に対するリスクを低減させるものであり、ネットワーク上の脅威そのものを完全に取り除くものではない
※掲載している情報は、記事執筆時点のものです