

媒体名	発行部数	掲載日	掲載面
日経コミュニケーション	32,995	2006年8月1日号	p. 89-91

ファイアウォール ウイルス対策 スパイウェア

ヒット製品の

今と将来



● セキュリティ・アプライアンス ●

単機能型から統合型へ 検疫や暗号メール機能も取り込む

ファイアウォールに代表されるセキュリティ・アプライアンス。最近では、多様化する脅威に備えるためにユーザーは何種類もの装置を利用しなければならず、運用の手間が膨らんでいる。こうした課題の解消に向け、セキュリティ・アプライアンスは各種対策を統合したモデルへと進化し始めている。

ファイアウォール、ウイルス対策ゲートウェイ、インターネットからの不正アクセスを遮断するIPS (intrusion prevention system: 侵入防止システム) など、多くの企業が利用しているセキュリティ・アプライアンス (専用装置)。当初、ソフトウェアとして提供されてきたこれらのセキュリティ対策

ツールは、設置や設定が容易なアプライアンスとして提供されるようになったことで急速に広まった。

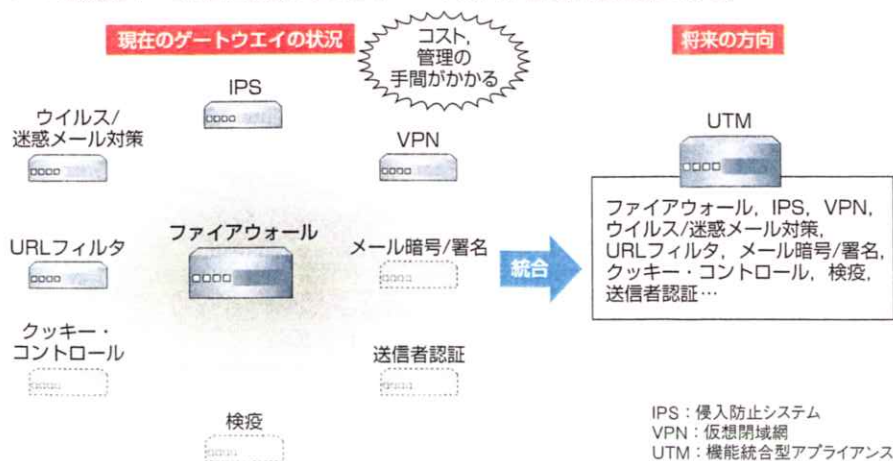
最近ではさらに、新しい種類の脅威に対処するために、さまざまなゲートウェイ装置が登場。ユーザーによる導入も始まっている。例えば迷惑メール・フィルタリング・ゲートウェイ、

フィッシングや不正なプログラムが仕込まれたWebページへのアクセスを防止するURLフィルタリング装置などである。

ただ、こうした装置を個別に導入していくと管理/運用が大変になる。個別に設置作業が必要になるうえ、運用時にはそれぞれの製品ごとに異なる管理コンソールを立ち上げ、監視しなければならない。個別にハードウェアを購入して月額/年額のライセンス料を払うためコストがかさむし、設置スペースの浪費にもつながる。

そこで今、セキュリティ・アプライアンスは、ゲートウェイで必要とされるセキュリティ機能を1台に集約する方向に向かいつつある (図1)。いわゆるUTM (unified threat management) と呼ばれるカテゴリの製品だ。

図1 セキュリティ・アプライアンスは統合の方向へ ゲートウェイとして設置されるアプライアンスの機能をすべて1台に集約することで、コストを抑え、管理作業を軽減できる。



ファイアウォールを核に発展

現在市場に登場しているUTMのほとんどは、従来ファイアウォール・アプライアンスとして提供されてきた装置に、IPS、ウイルス対策、URLフィルタリング、迷惑メール対策、VPN (仮想閉域網) ゲートウェイを搭載し

3分でわかる
コスト・
メリット

単機能製品組み合わせの半額以下

UTMの価格は、ハードウェアのスペック、つまり100Mビット/秒モデル、1Gビット/秒モデルといったスループット値によって変わる。ファイアウォールやIPSなどトラフィックを監視するタイプのアプライアンスと同様の価格体系である。もちろん、高速なモデルほど価格は高い。

基本モデルには、ファイアウォールやIPSなどの機能が標準搭載されていて、これにウイルス対策や迷惑メール対策といったオプションを追加する。これらのオプション価格はハードウェアのモデルに応じて決まっており、ユーザー数は問わない製品が多い。利用ユーザー数に応じて価格が変わるウイルス対策や迷惑メール対策の単機能製品との大きな違いだ。このため、コスト・パフォーマンスでは、「利用人数が増えるほどUTMの方が有利になる」（フォーティネットジャパンの菅原継頭

マーケティングマネージャ）。

単機能製品よりお買い得

1000人程度の企業で導入する場合の価格を考えてみよう。例えばフォーティネットジャパンが1000人規模の企業に推奨する「FortiGate-300A」はスループットが400Mビット/秒で145万円。ウイルス対策オプションを追加すると、合計180万7000円になる。

一方、単機能製品の場合は、ファイアウォールが一般に200万～300万円程度。ウイルス対策アプライアンスは1ユーザー当たり4000円程度必要で、1000ライセンスでは400万円、合計では600万～700万円に達する。こう見るとUTMは単体製品を購入するよりも格安と言える。

気になるのは性能だ。UTMは一つのハードウェアで複数の機能を同時に稼働させるため、単機能のアプライア

ンスよりも性能が劣化しやすい。ベンダーが示すスループットはあくまでも参考値で、使い方やトラフィック次第では実効スループットが参考値を大幅に下回る可能性は否定できない。「メモリーの制限などにより、単機能製品に比べて性能面で見劣りする」（ジュニパーネットワークス技術本部の小澤嘉尚副本部長）。こうした点から、「UTMはあくまでもお試し版」と見ているユーザーやベンダーがいることは確かだ。

ただ、ベンダーによっては豊富なラインアップをそろえているため、ユーザーは用途やトラフィックに合わせて製品を選択できる。ハイエンド製品は単機能アプライアンスと変わらない性能を持つ。また、ユーザーが複数のUTMを導入して負荷分散させることも可能。もちろん、単機能アプライアンスを組み合わせる場合と比べてコスト面でのメリットは薄れるが、それでも運用の手間を削減できる点は魅力である。

表A 国内で販売されている主なUTM製品

製品名	国内ベンダー	特徴
Astaro Security Gateway	ネクスト・イット	送信者認証機能を持つなど多機能
Firebox	ウオッチガード・テクノロジーズ	プロキシ型ファイアウォールのため、細かい制御や検査が可能
FortiGate	フォーティネットジャパン	ウイルス対策機能を一部専用LSIで処理するため高速
NetScreen	ジュニパーネットワークス	小規模からISPでも使える大規模まで広いラインナップを持つ
SonicWALL	ソニックウォール	管理・設定が容易
Symantec Gateway Security	シマンテック	ゼロ脆弱性ベースのシグネチャで、未知の攻撃を防御可能
VPN-1 UTM	チェック・ポイント・ソフトウェア・テクノロジーズ	複数のアプライアンスを一元的に管理できる

たものである。このうち、ウイルス/迷惑メール対策やURLフィルタリングは他社のソフトウェアをベンダーがカスタマイズして搭載するのが一般的だ。

どの製品もWebページによる設定画面か、GUI設定ツールを備えており、それぞれの機能を一元的に設定・管理できる。多くの製品は、ブリッジとし

て働く「トランスパレント・モード」で動作できるので、ネットワークの構成変更も必要ない。

また、機能を1台に集約することで耐障害性を高めやすくなるメリットもある。アプライアンスの数が減るほどハードウェアに起因する障害の確率が下がるからだ。冗長構成も取りやすい。

本文中の付いた用語を解説

IPS=intrusion prevention systemの略。攻撃や侵入といった不正な通信を検知し、それを遮断する機能を持つ。

フィッシング=金融機関などを装い、暗証番号や各種カード番号をだまし取る詐欺。メールで偽サイトに誘導し、情報を入力させるのが一般的な手口。

複数の機能を1台で済ませるため、ハードウェアのコストは安く済む。ソフトウェア部分も、ユーザー数ではなくハードウェアの性能に応じて課金されるのが一般的で、安価な場合が多い(前ページに関連記事)。

機能の統合はまだまだ進む

こうした機能統合型アプライアンスは既に、企業のシステム担当者に受け入れられつつある。「UTMの引き合いは2005年から顕著になり、最近さらに伸びている」(フォーティネットジャパンの菅原継顕マーケティングマネージャ)。

IT関連の調査を行うIDC Japanによれば、2004年の日本におけるUTM製品の出荷額は23億円(図2)。2005年は53億円と倍増している。さらに、2007年には155億円に達し、ファイアウォールの出荷額を上回る予測だ。

とはいえ今のUTMはまだ完成形とは言いきれない。企業を取り巻くセキュリティ事情を考えると、現在のUTMが備える機能では不十分だからだ。

ポットやスパイア型ウイルスに見られるように、脅威は複合化している。こうした脅威に備えるために、ベンダ

ーはUTMにさらに他のセキュリティ機能を統合しようとしている(図3)。今のところベンダーごとに統合の対象は異なっているものの、ベンダー間の競争の苛烈さを考えれば、いずれ各社があらゆるセキュリティ機能を統合して行くのは間違いない。

危険な端末はつながせない

例えば米ソニックウォールは、検疫ネットワーク機能の実装を進めている。ネットワークに接続する前に、ウイルス対策ソフトのパターン・ファイルが最新のものに更新されているか、OSやアプリケーションの最新のセキュリティ・パッチが適用されているかなどパソコンの状態をチェック。危険な状態にある場合はインターネット接続を遮断する。

既にウイルス対策ソフトのパターン・ファイルについてバージョンをチェックする機能は実装済み。今後は、「最新セキュリティ・パッチの適用状況やOSの設定などを確認できるようにする」(ジョン・クーン プロダクト・ライン・マネージャ)。加えて、パソコン側にパーソナル・ファイアウォールを導入し、ウイルスに感染しても外部に

情報を漏らさないように細かな制御を可能にする意向だ。

UTMでメールに署名/暗号化

このほか、各社が実装を急いでいるのが情報漏えい対策。暗号メール、キーワード・フィルタリングといった機能だ。

独アスタローは、情報漏えい防止に向けて暗号メール機能を搭載する。「今年秋ごろ登場するバージョンでは、S/MIMEやPGPで暗号化できるようになる」(日本の代理店であるネクスト・イットの事業統括本部セキュリティ・ソリューション担当 金子英樹本部長)という。

デジタル署名も可能で、フィッシング対策に利用できる。社員は普段使用しているメール・ソフトを使ってメールを送るだけ。UTMがメールを中継する際に送信先を読み取り、その送信先に対して暗号化したり署名を付けるルールになっていれば、UTMに登録された鍵を使って処理を施す。

“社外秘文書”を出口でブロック

ソニックウォールはコンテンツ・フィルタリングに目を付ける。インター

図2 日本国内でのUTM市場予測 右は主なUTM製品。

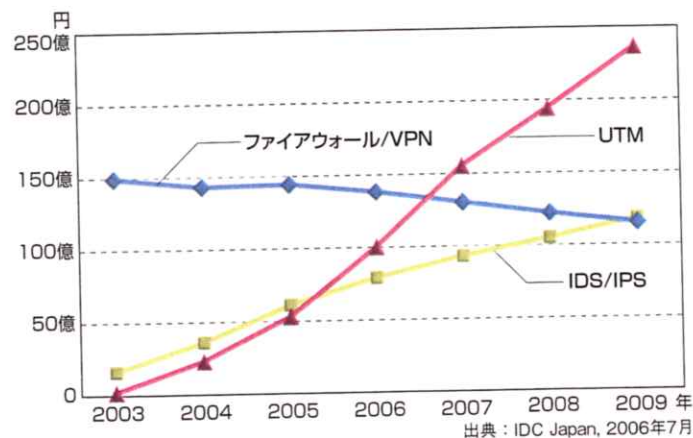
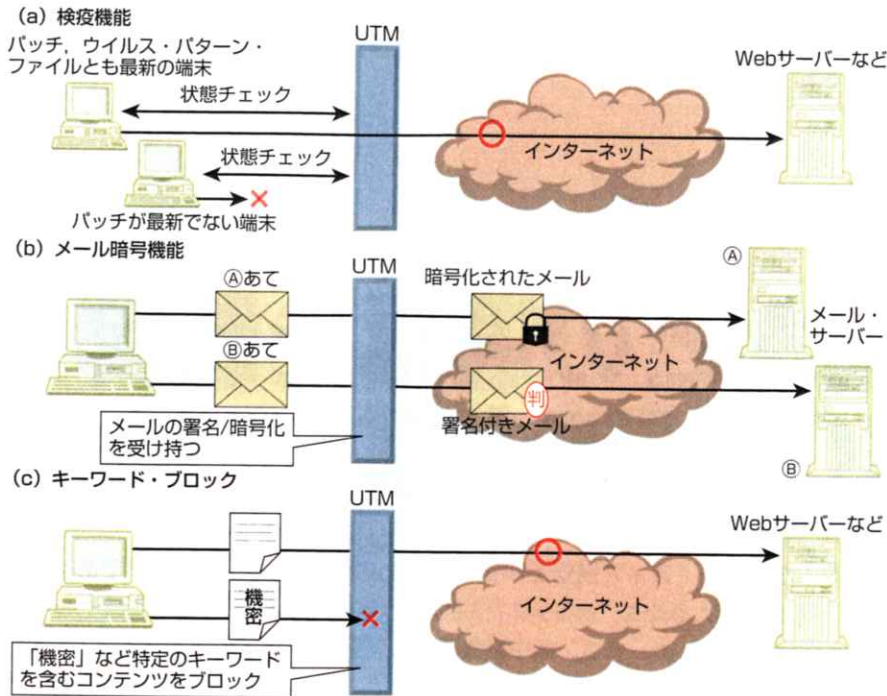


図3 UTMに将来搭載が見込まれる機能の例



ネットに送信されるコンテンツを検査し特定の言葉が入っていれば送信をブロックする仕組みだ。例えば、外部に漏れてはいけないファイル名に必ず「社外秘」のような単語を入れるようにしておけば、この言葉が入ったファイルの流出を食い止められる。

ユーザーごとに帯域を割り当てる

セキュリティ以外の機能強化を図る動きもある。ウォッチガード・テクノロジーズ、ジュニパーネットワークス、ソニックウォール、フォーティネットジャパンなどは、それぞれ、QoS (quality of service) 制御機能を実装済みだ。送信先/送信元IPアドレス、利用するTCP/UDPのポートなどに応じて、パケット送信の優先度を変えられる。

さまざまなトラフィックが混在する場合、業務をストレスなく継続できるようにするには、アプリケーションごとに帯域を割り当てる必要がある。最

近では、デスクトップ・アプリケーションまでがネットワークを前提として動作する。好例が、米グーグルが提供中の表計算ソフト。Webブラウザで利用できる。マイクロソフトのOfficeもこの方向に進む。このため、QoS制御は一層重要度を増す。ソニックウォールのクーン プロダクト・ライン・マネージャは、「誰かが大容量のファイルをダウンロードしている影響で、他の社員がデスクトップ・アプリケーションを利用できなくなる可能性がある。QoS制御は不可欠だ」と主張する。

今後はさらに細かいQoS制御が可能になる。ソニックウォールは「認証サーバーと連携し、ユーザーやアプリケーションごとに細かく制御できるようにしたい」(クーン プロダクト・ライン・マネージャ)という。一刻を争う業務を行っている部署は遅延のないようにするといった制御をかけるわけだ。

(中道 理)

ポット=ユーザーのパソコンに忍び込み、ネットワークから第三者が操作することで悪事を働くプログラム。

スパイ型ウイルス=企業や組織の特定の人にもみ送られるウイルス。上司や知人になりすましたメールに添付されてくるので、ユーザーがウイルス・ファイルを開いてしまう可能性が高く、攻撃が発覚しづらい。

S/MIME=secure MIMEの略。暗号メール技術の一つ。公開鍵暗号基盤(PKI)を使い、メールの暗号化、デジタル署名などを行える。

PGP=pretty good privacyの略。暗号メール技術の一つ。公開鍵暗号方式を利用し、メールの暗号化、デジタル署名などを行える。利用する公開鍵暗号は、公開鍵暗号基盤(PKI)と違って認証局がない。

ポート=ネットワークを介して通信しているプログラムを識別するための番号。IPアドレスを建物の住所とすれば、ポート番号は部屋番号に相当する。0~65535番まで指定できる。1024番までのポートはwell knownポートされており、アプリケーションとの対応付けが決まっている。