UTMアプライアンス

中小企業に必須のセキュリティ商材

1つの筐体にファイアウォール/VPN等のさまざまなセキュリティ機能を集約したUTMアプライアンスが注目されている。コストと管理の手間が省けることから、中小企業への導入が急速に進んでいる。

文◎藤田 健(本誌)

「もはやファイアウォールとアンチウィルスだけではネットワークの脅威からは守れなくなっている」――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はこう語る。

企業を取り巻くネットワークの脅威は増加の一途を辿っており、脅威の種類もウィルスやワーム、スパイウェア、フィッシング、DoS攻撃(Denial of Service attack:サービス不能攻撃)等、多岐にわたる。これらの脅威はますます巧妙化・複合化しており、従来のパケットフィルタリングベースのファイアウォールだけでは防御し切れなくなっている。**図表1**にそれを示した。

これらの脅威に対して各企業はどのように対処しているのだろうか。

大企業の場合は、各機能に特化したアプライアンスを組み合わせて導入するケースが一般的だ。この場合、設定や運用・管理が複雑になるうえ、トータルコストもかかるという課題があるが、情報システム部門の人材が豊富で、セキュリティに対するコストも十分かけられる大企業では大きな負担にはならない。

しかし、中小企業ではそうはいかない。資金面でも人材面でも十分なセキュリティ対策は実施できないのだ。

また、複数の販売代理店によると「それ以前の問題として、セキュリティ対策の必要性に関する意識が希薄」という。このため、PCにアンチウィルスソフトをインストールしてお終いという企業がかなり多い。「中小企業の経営者層は、PBX/ビジネスホンのように、導入すれば通信コストの削減効果がはっきりと分かるシステムへの関心は高いが、コスト削減効果につながるわけではないセキュリティ製品の導入に関しては腰が重い」と語っている。

だが、その状況も少しずつ変わりつつある。中小企業の中には、大企業の下請け業務を生業としているところが多い。このため、大企業からユーザー等のデータを預かっている。折りしも企業の情報漏えい事件が相次いで発生し、社会問題になっている。必然的に、大企業側からセキュリティ対策を要求されるようになっているのだ。

とはいえ、前述のように、資金と人材の両面で不安を抱える中小企業では、なかなか対策に踏み切れなかった。

図表1　企業を取り巻く脅威と有効な対策

脅威	有効な対策					
	ファイアウォール	IPS	Webアンチウィルス	Webコンテンツフィルタリング	メールアンチウィルス	アンチスパム
スパイウェア		○	○	○		
ボットネット		○	○	○		
トロイの木馬		○	○	○		
フィッシング				○		○
情報漏えい				○		○
マスメール型ウィルス				○	○	○
Web型ウィルス			○	○		
DoS攻撃	○	○				
スパムメール						○
ピアツーピアソフト		○				

＊すでにファイアウォールとアンチウィルスだけでは万全ではない状況　　出典:フォーティネットジャパン

UTM市場は急成長

そうしたなか、ファイアウォール、VPN、アンチウィルス、不正侵入検知/防御(IDS/IPS)、Webコンテンツフィルタリング、アンチスパム等の複数のセキュリティ機能を1つの筐体に統合した装置が登場した。「UTMアプライアンス」だ。

UTMとはUnified Threat Managementの略であり、統合脅威管理の意味だ。米国の調査会社