特別企画 伊藤忠テクノサイエンス／フォーティネットジャパン

複雑化が進む脅威から企業を守る「FortiGateシリーズ」
～1台で高度な機能を実現した統合セキュリティ・アプライアンス～

Winnyをはじめとした P2P ソフトによる情報漏えいや、PCやサーバに侵入して遠隔操作で攻撃を行うボットネット、詐欺を目的としたフィッシングなど、複雑化が進む脅威から企業を守るためには、高度なセキュリティ機能が必要である。これまでは、専用ツールを導入してきたが、最近では、1台に主要なセキュリティ機能を搭載して複数の脅威から攻撃を防ぐ統合セキュリティ・アプライアンス（UTM）が主流になりつつある。この成長著しいUTM市場において、マーケットリーダーの地位を固めつつあるのが米国フォーティネット社である。ここでは、同社の代表的なUTM「FortiGateシリーズ」について紹介する。

企業を取り巻く脅威とその対策

2001年9月に発生したNimdaワームは、当時のインターネット上で猛威を振るい、24時間で200万台以上のPCが感染するなど、全世界に大きな被害を与えた。Nimdaは、マイクロソフト社のWindowsシリーズのOSを搭載したPCに感染して、同社の複数のソフトウェアを介して様々な手段で感染するように設計されていたことから、本格的な「複合型の脅威」として注目された。

Nimdaが発生して5年が経過した現在でも、企業を取り巻く脅威は増え続けている。悪意を持って他人のPCのデータやプログラムを盗み見たり、改ざん・破壊などを行うクラッキングや、メールやWWW、インスタントメッセージング（IM）等で侵入してくるウイルス、トロイの木馬などによる被害は依然として増えている。また最近では、ウイルスなどを利用してPCやサーバに侵入して遠隔操作で攻撃を行うボットネットや、暗証番号やクレジットカード番号などを搾取するフィッシング詐欺、WinnyやShareなどのP2Pソフトウェアを利用した情報漏えい、ゾンビPCによるスパムやDos攻撃などによる被害が頻発している。このような脅威は、多様化および複雑化が進んでいることから、1つの脅威に1つの単一機能製品では対応できなくなっている（図1参照）。

脅威	有効な対策					
	ファイアウォール	IPS	Webアンチウイルス	Webコンテンツフィルタリング	メールアンチウイルス	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				○		○
マスメール型ウイルス				○	○	○
Web型ウイルス			○	○		
DoS攻撃	○	○				
スパムメール						○
P2Pソフト		○				

図1　企業を取り巻く脅威とその対策

これまで多くの企業では、様々な脅威への対策として、専用サーバやアプライアンスをLANとインターネットの間にゲートウェイとして設置して、ウイルスやスパム、フィッシング、ボットネットなどの脅威に対応したセキュリティツールをゲートウェイ製品として積み上げてきた。しかし、このような対策を続けてきた結果、次のようなデメリットが生じている。1つが「コストがかかる」こと。複数の製品を導入するために、導入・管理コストがかかってしまい、ソフトウェアの場合でもサーバとOSのコストがかかってしまう。次に「管理が大変」なこと。複数の製品を使うため管理に手間がかかってしまい、さらに異なるベンダーの製品の場合は、管理ツールも異なるので余計に手間がかかってしまう。そして「信頼性が下がる」こと。1台に障害が起こると通信が遮断されてしまう場合があり、冗長化するとネットワーク構成が複雑になり、コストが増大してしまう。

このような問題を解決する製品と

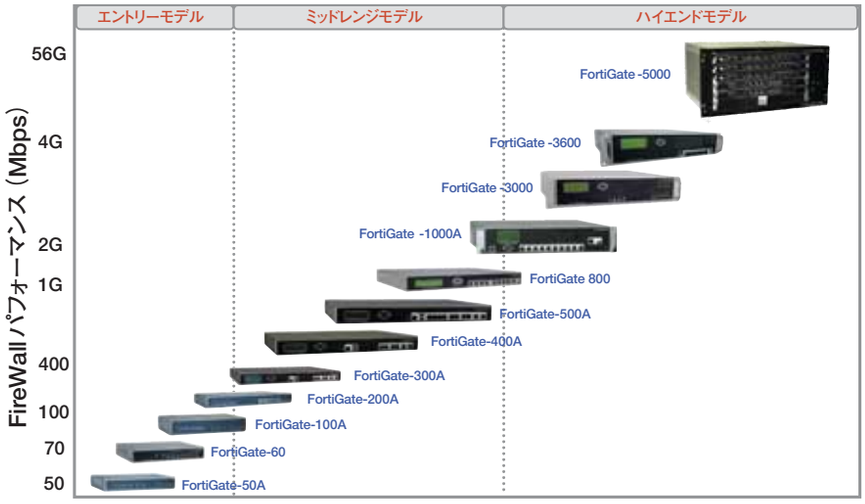


図２　FortiGateシリーズのラインアップ

して注目されているのが、統合型のセキュリティゲートウェイである。これは、複数のセキュリティ機能を単一のハードウェアプラットフォームに統一・統合し、提供することで、複合型の脅威から企業を守る統合セキュリティ・アプライアンスである。これらの製品は「UTM（Unified Threat Management：統合脅威管理）装置」とも言われており、その代表的な製品がフォーティネット社の「FortiGateシリーズ」である。

驚異的な処理スピードを誇る「FortiGateシリーズ」

米国カリフォルニア州サニーベールに本社を置くフォーティネット社は、複合型の脅威に対応したASICベースのセキュリティ・アプライアンスを提供するリーディングベンダーである。同社のFortiGateシリーズは、ファイアウォール、VPN、アンチウイルス（アンチスパイウェア含む）、アンチスパム、Webコンテンツフィルタリング、IPS（侵入検知・防御）を１台で実現する統合セキュリティ・アプライアンスである。

FortiGateの第一の特長は、安定性やパフォーマンスをチューニングした堅牢で拡張性が高い専用OS「FortiOS」上に主要なセキュリティ機能を搭載していること。そして、これまでソフトウェアと汎用CPUで行っていたウイルススキャンやWebフィルタリングなどの処理を、専用ASIC「FortiASIC」によりハードウェアで処理できるようにしたことである。

このFortiOSとFortiASICにより、驚異的な処理スピードを実現し、複数のセキュリティ機能を搭載していても処理能力が低下することがなく、アンチウイルスやコンテンツフィルタリングもリアルタイムで行うことができるようになった。

新たな脅威への迅速な対応と導入・運用コストの低減を実現

図２は、FortiGateの製品ラインアップである。小規模の企業でも大きな負担が無く導入が可能。大規模企業の場合は、メインゲートウェイにはハイエンドモデル、支社・支店間にはミドルレンジモデルを用意するなど、同様の管理操作性で一貫したセキュリティ対策が可能である。

このFortiGateの優位性として、次のようなことがあげられる。

◆クライアントライセンスは無制限

セキュリティ製品の多くは、ユーザーごと（クライアントサーバ単位）にライセンス料金を支払う体制を採用しているが、FortiGateは、アプライアンスごと（機器単位）の料金

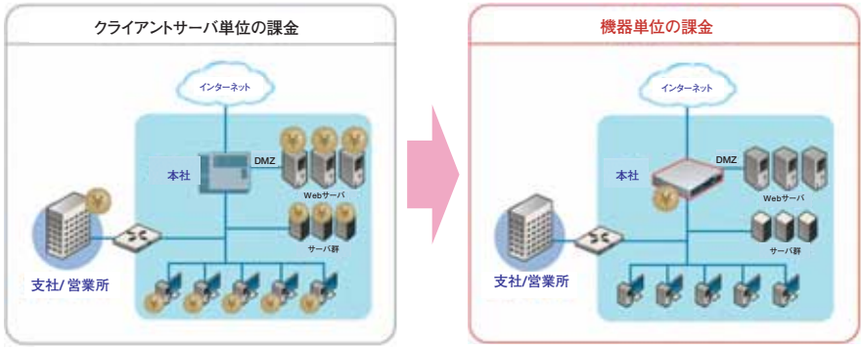


図３　ユーザー単位からアプライアンス単位の料金体系へ

体系を採用している（図３参照）。従来のクライアントサーバ単位での課金では、ユーザーごとにライセンスコストが発生してしまい莫大なライセンス管理の手間とコストが生じてしまうが、FortiGateが採用している機器単位の課金なら、イニシャルコストやランニングコストを低く抑えられるようになる。

◆わかりやすいインタフェースで運用管理の負荷を軽減

FortiGateには、統合セキュリティ・アプライアンスならではの機能として、複数のセキュリティ機能の設定を１つのプロファイル上で行える「プロテクションプロファイル」がある。プロファイルを開くと、アンチウイルスやWebフィルタリング、Webカテゴリフィルタリング、スパムフィルタリング、IPS、コンテンツアーカイブ、IM/P2P/など各機能の設定が並んでおり、これらの設定を横断的にまとめて1つのプロファイルにする。そして、ファイアウォールのポリシー設定で、LANからインターネットへのトラフィックに対してこのプロファイルを適用させる。このプロテクションプロファイルを活用することで、運用管理の負荷を大幅に軽減できる。

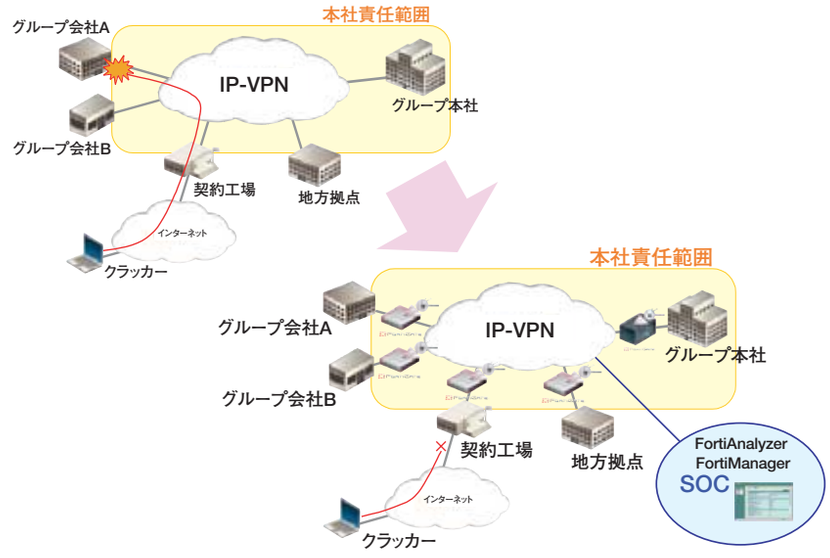
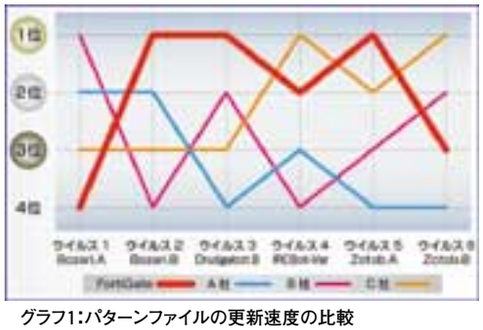


図５　IP-VPN環境での脅威と解決策

◆新たな脅威への迅速な対応

図４のグラフ１は、2005年８月に発表された「MS05-039-Windowsのプラグ アンド プレイに関する脆弱性」を利用する6種類のウイルスに対して、ドイツの第三者機関「AV-Test.org」の調査をもとに、日本国内でよく使われているアンチウイルスベンダー4社のパターンファイルの更新速度を比較したものである。FortiGateのパターンファイル更新は、他社の製品と比べて迅速に対応していることが確認できる。

またFortiGateは、定義ファイルと比較することでウイルスを検出するのではなく、プログラムコードの動きを見てウイルスを検出する技術「ヒューリスティック（heuristic）」により、高精度にウイルスを検出することが可能である。図４のグラフ２は、上のグラフ１と同様に2005年８月にAV-Test.orgが調査したもので、前記の６種類のウイルスに対して、ヒューリスティックにウイルスを検出できたかどうかを表している。その結果、FortiGateだけが、全てのウイルスを「疑わしいファイル」としてパターンファイル更新前に検出することができた。



グラフ1:パターンファイルの更新速度の比較

	ウイルス1 Bozori.A	ウイルス2 Bozori.B	ウイルス3 Drulgabot.B	ウイルス4 RCBot.Var	ウイルス5 Zotob.A	ウイルス6 Zotob.B
FortiGate	○	○	○	○	○	○
A社					○	○
B社						
C社						

グラフ2:未知のウイルスへの対応速度の比較

図４　新しい脅威への対応スピードの比較

IP-VPN環境での脅威と解決策

FortiGateの活用例として、フォーティネット社では次のような対策を提案している。例えば、IP-VPN

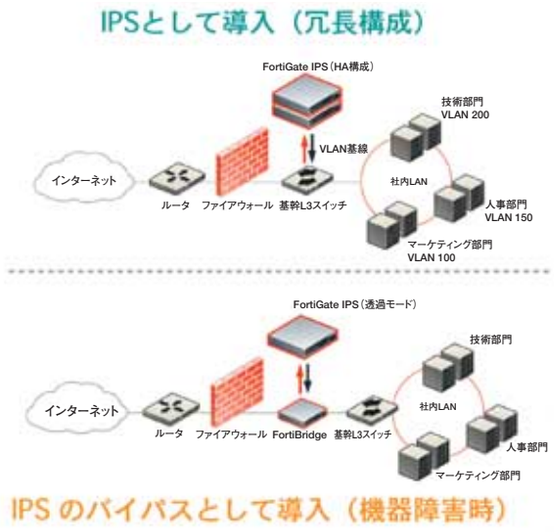


図６　IPSとしてのFortiGate導入例

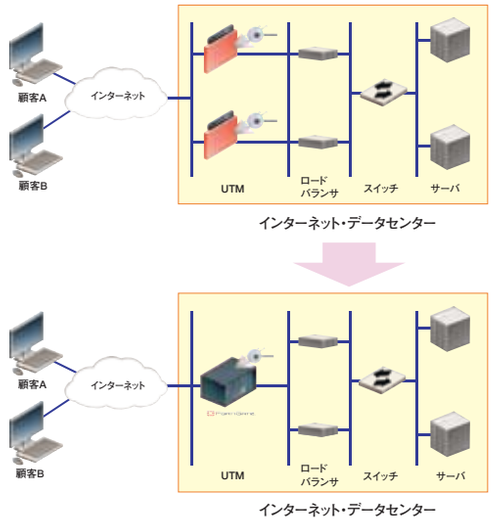


図７　FortiGate-5000による集約

環境での脅威とその解決策について。IP-VPNに接続しているグループ会社Aに対して、IP-VPNの範囲外（欧米やアジア等の国外）からDos攻撃を受けた場合。これまでは、Dos攻撃が責任範囲外から侵入していたため、効果的な対策を打てなかった。しかし、FortiGateを導入してウイルスチェックとIPSを実施。そして責任範囲内のセキュリティ対策の運用管理をSOC（Security Operation Center）で行うことで、責任範囲外からの攻撃を防ぐことができるようになる（図５参照）。

また、FortiGateをIPSとして導入する場合は、既存のファイアウォールと併用してトラフィック経路の中に配置して、受信／送信パケットの中を調べて悪意のあるものや不正に構成されたものが紛れ込むのを防止する。FortiGateは、ハイアベイラビリティ（HA：高可用性）構成をとることで、ネットワーク資源を効率的に活用できるようになる。さらに、フェイルオープン（故障時に通信を継続する機能）を付加するオプション「FortiBridge」を使用することで、ネットワークにおけるIPSのバイパスを実現することができる（図６参照）。

最上位モデル「FortiGate-5000」を活用して投資回収期間を短縮化

昨今、アンチウイルスやファイアウォール、IPSなどのセキュリティサービスを、効率良く、しかも対費用対効果の高い方法で提供できることとから、FortiGateを導入するMSSP（マネージド・セキュリティ・サービスプロバイダー）が増えている。例えば、FortiGateの最上位モデルである「FortiGtae-5000シリーズ」と、統合管理ツール「FortiManager」、ロギングとレポーティング製品「FortiAnalyzer」を組み合わせることで、1台のコンソールで何千台ものFortiGateを構成し、システムを容易に管理できるようになる。またFortiGateは、セキュリティゾーンやバーチャル・ドメインなどの機能をサポートするので、高度なセキュリティポリシーを部門／顧客ごとにきめ細かく設定することが可能である。

このようなITC（In The Cloud）型のセキュア・ホスティングを行うことで、投資回収期間の短縮化を図れることから、フォーティネット社では、中・大規模企業やインターネット・データセンターに対しても、FortiGate-5000の導入を提案している（図７参照）。

●お問い合わせ先●
伊藤忠テクノサイエンス㈱
テレコム事業企画室
TEL：03-6203-5231
E-mail：telbizmarcom@ctc-g.co.jp
CTCグループForinet社取扱代理店
CTC エスピー㈱ 営業推進部
TEL：03-3419-9672
E-mail：sp-admin@ctc-g.co.jp
フォーティネットジャパン㈱
TEL：03-5549-1640