ネットワークマガジン
NETWORK MAGAZINE

ソリューション提案

こんなに使える統合型セキュリティゲートウェイ

企業のITシステムを襲う
さまざまなセキュリティの脅威に対抗するソリューションとして
最近注目を集めているのが統合型セキュリティゲートウェイである。
本誌ではフォーティネットの「FortiGate」シリーズを例に
統合型セキュリティゲートウェイの真の実力に迫る。

積み上げ型はもう限界！

インターネットからのさまざまな脅威を防ぐための手段として、ファイアウォールやVPNだけではなく、アンチウイルス、IDS・IDP、Webフィルタリング、アンチスパムなどの機能を搭載した統合型のセキュリティゲートウェイが注目を集めている。

文●編集部

増えるセキュリティの脅威 個別の対応が必要か？

ブロードバンド・常時接続を前提としたセキュリティ侵害は増え続けている。もとよりインターネット経由でのクラッキングやWebサイトの改ざん、メールやWWW、IM等でやってくるウイルスやトロイの木馬などは、古くから企業のインターネット利用を脅かし続けている。さらに最近では金儲けを目的としたフィッシング詐欺やP2Pアプリケーションでの情報漏えい、あるいはゾンビPCを使ったスパムやDDoS攻撃なども増えている状態だ。

このように脅威は多様化しているため、当然それに対応したセキュリティ対策が必要になる（図1）。従来からインターネットからの攻撃に対抗するためのセキュリティ対策としては、専用のサーバやアプライアンスをLANとインターネットの間の境界にゲートウェイとして設置するのが一般的だ。

もっとも一般的なのは、すでに国内でも90パーセント以上の普及率を誇るファイアウォールであろう。また、現在はLANに入る前にウイルスの侵入を食い止めるウイルススキャンゲートウェイの導入も多い。さらに、最近はそれだけではなく、スパム、フィッシング、DDoS攻撃、ボットネット、データベース攻撃など、さまざまな脅威に応じたセキュリティ装置がゲートウェイ製品として提供されている。

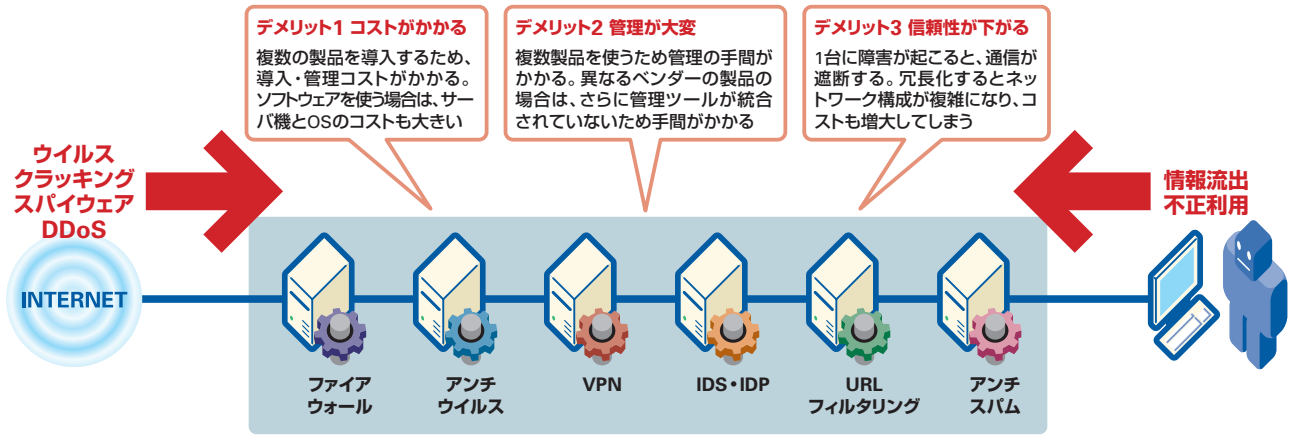
このように脅威が増え、対策が多様化しているという現在のゲートウェイの状況は、ちょうど国際空港での入出国チェックと似ている。国際空港ではテロやハイジャック、あるいは伝染病や麻薬の持ち込みなどさまざまな脅威がある。そのため、本人やパスポート、手荷物などあらゆるものを調べなければ

図1●さまざまな脅威に対するセキュリティ対策

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				●		●
メール型ウイルス				●	●	●
Web型ウイルス			●	●		
DoS攻撃	●	●				
スパム						●
P2Pソフト		●				

すでにファイアウォールだけでは不十分で、さまざまな対策を講じなければならない

図2●積み上げ型ゲートウェイのデメリット



複数のゲートウェイ製品を導入するとコストもかかり、管理の手間も大きくなる。また、ネットワーク構成も複雑になってしまう

ならない。その手段も検査官によるパスポートやビザのチェックのほか、麻薬犬などによる持ち物検査、スキャナによる手荷物や預けものチェック、人体センサーによる感染症の検査など多様化している。

ゲートウェイ積み上げ型のデメリット

しかし、こうした形でゲートウェイ型のセキュリティ製品を積み上げていくと、いくつものデメリットが生じてしまう（図2）。

まずコストがかかってしまうことが、最大のデメリットである。確かにインターネットが普及し始めた当時は、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十分であった。しかし、その後アンチウイルスのソフトを導入し、ファイアウォールで防げない攻撃を検知・遮断するためにIDSを導入することになる。さらに安全な拠点間接続のためにVPNゲートウェイを入れ、スパムを防ぐためにアンチスパム製品を導入。その他にも従業員のWebサイトでの利用制限を行なうためには、Webフィルタリングが必要になる。

こうして積み上げていくと、製品の数は多くなり、導入や管理に膨大なコストがかかってしまうことがわかる。

機能の重複もコスト効果を下げる要因だ。たとえば、アンチウイルスやIDS・IDPのいずれもトロイの木馬を検出する機能があるし、スパム対策を行なえばフィッシングを防ぐことにもなる。もちろん異なるベンダーで機能が重複すれば精度も高くなるという指摘もあるが、投資額を考えれば必ずしも有効とはいえない。

また、このように多くの製品をまとめて使うとなると、管理も容易ではない。セキュリティ機器やソフトはそれぞれ機能が異なり、管理ツールもそれぞれ独自のものを用いている。もちろん昨今ではマルチベンダーの場合も多い。こうなると操作を覚えるまでに時間がかかり、ライセンス等の管理も面倒になってしまう。

信頼性という点でも問題がある。図2のように数珠つなぎの構成だと複数の機器のうち、1台でも障害が起こったら、ネットワーク自体が断絶してしまうからだ。もちろん、複数の台数で冗長化するという方法もあるが、この場合はネットワークが複雑な構成になってしまうことが多い。

統合型セキュリティゲートウェイとは？

こうした中、さまざまなセキュリティ機能をまとめて併せ持つ「統合型セキュリティゲートウェイ」が注目を集めている。統合型とは、文字通り複数のセキュリティ機能を1台のアプライアンスで提供することを意味する。これらの製品を市場調査会社のIDCでは、「UTM（Unified Threat Management・統合脅威管理）と呼ばれるジャンルに分類している。

これまでもVPNが統合されたファイアウォールなどは製品として存在していた。しかし、今回紹介する統合型セキュリティゲートウェイは、アンチウイルス、IDS・IDP、Webフィルタリング、アンチスパム、といった機能まで併せ持つものだ。あらゆるセキュリティの脅威を水際で防ぐための「幕の内弁当的な」製品といえる。

★

以下、統合型セキュリティゲートウェイの機能と使い勝手について見ていきたい。各機能の概要や製品選定のポイント、設定の手順などを理解し、導入に活かしてほしい。

機能とメリットを検討

統合型セキュリティゲートウェイには、さまざまな脅威に対抗する機能が搭載されている。ここでは基本機能を紹介し、さらに導入によってどのようなメリットが得られるのかを検討してみよう。

統合型セキュリティゲートウェイの機能

統合型セキュリティゲートウェイの定義は「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・統合する製品」(IDC)とされている。内部的にはファイアウォールやVPNをはじめ、複数の機能を実現するモジュールが連携して動作している(図3)。

では、実際の製品にはいったいどんな機能が搭載されているのだろうか? 搭載されている、主要なセキュリティ機能・技術をおさらいしておこう。

●ファイアウォール

ユーザーが定義したセキュリティポリシーに則って、必要な通信を通過させ、不要な通信を遮断するというアクセス制御を行なう。主にインターネットからのクラッキングからサイトを防御する。一般的にはパケットのヘッダを精査することで、IPアドレスとTCP/UDPのポートで通過の可否を決める「パケットフィルタリング」を指す。最近ではヘッダではなく、アプリケーションデータを直接精査する方式も用いられる。

●アンチウイルス

ユーザーが望まない処理を勝手に行なう不正プログラム(ウイルスやワーム、トロイの木馬)を検出する機能。ウイルスやワームのコードが登録されているパターンファイルとパケットの中身を照合することで、検出と駆除を行なう。最近では、パターンファイルを使わず、プログラムの挙動を元にウイルスかどうかを判断する「ヒューリスティック分析」という手法もとられる。

●VPN(IPsec/SSL)

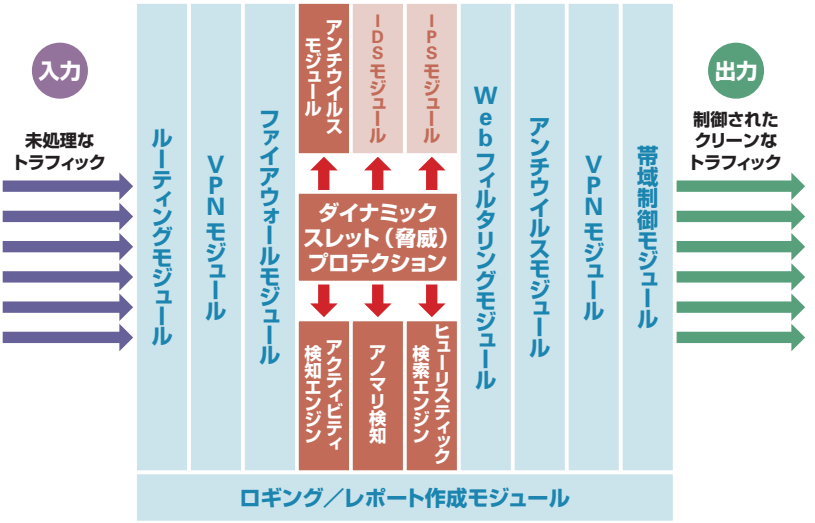
公衆ネットワーク上に仮想の専用線を構築する技術やそのネットワーク。LAN内のパケットを別のパケットで包んで、インターネットや通信事業者のネットワークで伝送する「トンネリング」という技術がベースとなっている。

これらはIPsecやSSLといったプロトコルが利用され、各拠点に設置されたVPNゲートウェイ間で安全なトンネルを張ることで実現される。また、インターネット上での盗聴や改ざん、なりすましを前提としたパケットの暗号化、改ざん検知、あるいは接続先認証などのセキュリティ機能も持っている。

●IDS/IDP

IDS(Intrusion Detection System)は不正侵入検知システムと訳されており、

図3●統合型セキュリティゲートウェイの中身



入力されたトラフィックがファイアウォールやVPN、アンチウイルスなど複数のモジュールで処理され、クリーンなトラフィックとしてユーザーに届く

不正アクセスを管理者に通知するシステム。不正アクセスの手口を登録した「シグネチャ」と呼ばれるデータベースを元に、不正アクセスを検出する。ファイアウォールでは管理者が事前にポリシーを設定する必要があるが、IDSではシグネチャがあるため不要。また通常ファイアウォールで開放されている80番（HTTP）や25番（POP3）などのポートを経由する不正アクセスも検知できるのが特徴だ。その他、正常な通信状態を登録しておき、一定のしきい値を越えたときに警告を発する「アノマリ型」という方法もある。

なお、検知のみのIDSに遮断の機能を加えたのが、IDP（Intrusion Detection & Prevention）である。

●Webフィルタリング

LAN内のユーザーを対象に、URLでWebページのダウンロードを制限する機能。従業員の生産性向上や青少年にふさわしくない内容のWebサイトの閲覧制限などを目的とする。

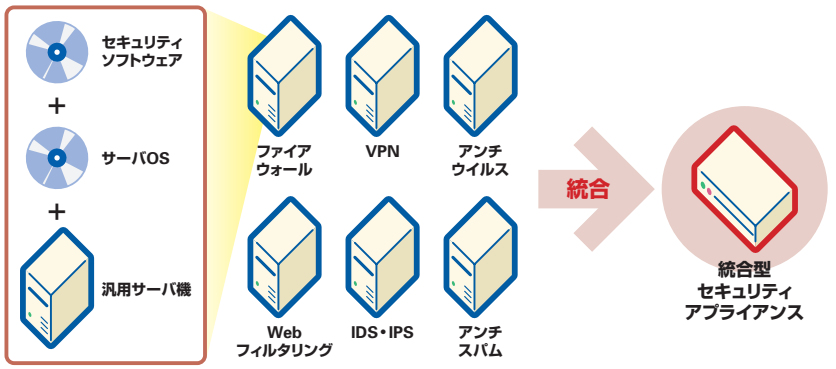
フィルタリングを実現するために、Webページがポルノ、暴力、薬物、自殺、ギャンブル、就職活動、出会い系などのジャンルで分類されてデータベースに登録されている。そしてユーザーからブラウザなどからURLが指定された段階で、このオンラインデータベースに接続の可否を問い合わせる。

URLではなく、実際のページをリアルタイムに読み込んでページのダウンロードの可否を決定する方法は「コンテンツフィルタリング」と呼ばれる。

●アンチスパム

ユーザーが配信を望まない迷惑メール（スパム）を受信前に振り分けたり、除去する機能。SMTPのレベルで不正なメールサーバの中継を拒否する方法と、メールの本文を読み込んでスパムらしさを学習し、振り分ける方法の大きく2つがある。スパム経由で配信されるウイルスやフィッシング詐欺のメールなども、結果的に防ぐことが可能だ。

図4●統合のメリット



複数必要だったサーバが1台に統合されるため、コストや管理の手間は大幅に軽減される

このほか、フィッシングやスパイウェア、DDoS攻撃、ボット、P2Pなどの脅威を防ぐ専用装置やソフトウェアもあるが、上記の技術の拡張で防いでしまうことも多い。

統合型セキュリティゲートウェイは、これらの機能を5つから6つ併せ持つ単一の機器と考えてもらいたい。具体的な製品としては、フォーティネットの「FortiGateシリーズ」が挙げられる。

統合型セキュリティゲートウェイのメリットとデメリット

さて、複数台あったサーバやアプライアンスが1台にまとまるということで、統合型セキュリティゲートウェイの導入メリットはかなり明確である。

まずは導入・管理コストは大幅に低減される。確かに単機能のアプライアンスに比べれば価格は高いだろう。しかし、ハードウェアプラットフォームが共通なので、6つの機能があるから価格が6倍ということにはならない。しかも、通常は必要な機能だけライセンスを購入すればよいので、不要な機能に対してお金を払う必要はない（図4）。

また、管理の手間も低減される。複数の機能が1つのコンソールで管理できるのは非常に大きなメリットだ。導入する機器が1台で済むため、ネットワーク構成もシンプルになり、省スペースも実現できる。信頼性に関しても、障害時に機器を1台交換すれば済むし、必要であれば冗長構成を採ればよい。

逆にデメリットとしては、専用機やソフトウェアに比べて、機能面がやや落ちるという点だ。フォーティネットのマーケティングマネージャである菅原継顕氏も「すべての機能で他の専用機やソフトウェアに絶対勝てますとはいいません。ですが、すべて最高の機能を求めているお客様より、弊社の製品を見てこれで十分というお客様のほうがとても多い」と語っている。

確かに同社のFortiGateシリーズでは、大手のウイルススキャンソフトに比べて、検出できるウイルスの数が少ないのも事実だ。しかし、歴史のあるウイルススキャンソフトはパターンファイルの検証にも時間がかかり、結果としてリリースが遅くなることも多い。これに対して、FortiGateのシグネチャやパターンファイルなどの更新は、これらのウイルススキャンベンダーに比べて圧倒的に速いという。

製品選びと実際の設定

**製品の概要とメリットがわかったところで、次は実際に製品に触れてみよう。
今回はSOHO向けの製品であるフォーティネットの「FortiGate-100A」を試用してみた。
使いやすさと複数の機能の連携に特に注目してもらいたい。**

6つの機能を統合した「FortiGateシリーズ」

まずはフォーティネットの「FortiGateシリーズ」について紹介しよう。フォーティネットはネットスクリーンの創設者でもあるケン・ジー（Ken Xie）氏が設立した企業で、同社のFortiGateシリーズは統合型セキュリティゲートウェイのはしりとして知られている。

FortiGateは安定性やパフォーマンスをチューニングした「FortiOS」と呼ばれるOS上に、自社開発したファイアウォール、VPN、アンチウイルス、Webフィルタリング、アンチスパムなどが搭載されている。さらに、FortiGateシリーズで画期的だったのは、今まで汎用CPUとソフトウェアで行な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世界で初めてASICで実現したという点だ。ASIC化したことで、処理能力は既存の100倍近くに向上したと説明されており、高速なブロードバンド環境でも十分実用に耐えうるようになったのである。

現在、FortiGateシリーズはSOHO向けの50A/60/100A、中小企業向けの200A/300A、大企業向けの400A/800、通信事業者向けの3000/3600/5000シリーズまで幅広いラインナップで展開されている。ただ、FortiOS＋ASICというプラットフォームは基本的に同一で、ログ管理用のHDDを搭載するモデルも用意されている。今回はこのうちSOHO向けの「FortiGate-100A」を試用してみた（写真1・2）。

写真1・2●FortiGate-100A

4つのLANポートのほか、デュアルISP構成をとるためのWANポート、DMZポートがそれぞれ2つずつ付いている

ゲートウェイの導入に際して注意すべきこと

FortiGateを初めとするこうした統合型セキュリティゲートウェイを導入するにあたって、まず決めなければならないのが、利用する機能だ。

多くの製品は、あらかじめ複数の機能が入っており、標準機能以外はライセンスを購入することで機能がアクティブになる。FortiGateの場合、ファイアウォールとVPNが標準搭載でアンチウイルスとIDS・IDP、Webフィルタリング、アンチスパムはそれぞれオプションを購入する必要がある（図5）。

もちろん、アンチウイルス、IDS・IDP、Webフィルタリング、アンチスパムなどの機能は単に動作しているだけでは、意味がない。固定的に設定を施すファイ

図5●ライセンス形態

	ファイアウォール／VPNは標準装備	オプション アンチウイルス アンチスパム Webフィルタリング 不正侵入防御（IPS）	保守
初年度	必要	オプション	購入の必要なし
次年度以降	購入の必要なし	オプション	必要

標準搭載のファイアウォールとVPN以外は、オプションとして「サブスクリプション」する

アウォールとVPNを除けば、新しい脅威に対抗するためのデータベースの更新が必要になるからだ。たとえばアンチウイルスであればパターンファイル、IDS・IDPであればシグネチャと呼ばれるもので、インターネット経由で更新できなければならない。こうしたデータベースの更新サービスは「サブスクリプション（購読）」と呼ばれており、通常はオプションのライセンスに含まれる。また、このオプションは1年ごとに更新されるため、1年間経ったら再度更新手続きを取る必要がある。

さらに保守サービスは製品に1年分が付属し、次年度以降別途購入というパターンになることが多い。

膨大な設定項目を日本語GUIで扱える

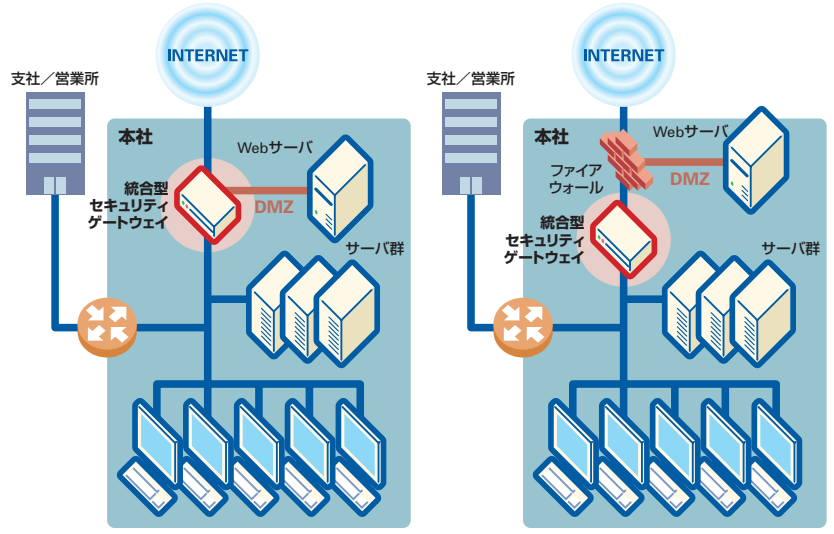
また実際の導入にあたっては既存のファイアウォール／NATルータと併存させるのか、否かを注意しておきたい（図6）。統合型セキュリティゲートウェイの多くはPPPoEやNATなどブロードバンドルータとしての機能も持っている。しかし、最近ではADSLモデムもルータの機能を持っているため、どちらかをオフにする必要があるのだ。FortiGateは「NAT/ルート」モードのほか「トランスペアレント」というブリッジモードがあるため、既存のファイアウォールに追加する形態でも利用できる。

さっそくFortiGate-100Aの設定を見てみよう。初期状態ではDHCPサーバが動作していないので、設定するコンピュータでは、まず固定でIPアドレス（192.168.1.2など）を割り当て、次にLANポートにケーブルを差し込む。その後、PCのWebブラウザから設定ページのIPアドレスを入力するとツールが起動する。初期状態では、表示言語が英語になっているのでまずは左側のメニューで「system」－「config」で「options」のタブを開く。「Web Administration」で「Language」を「Japanese」にし、「Apply」ボタンを押すと、表示がすべて日本語になる。

トップページはステータスの表示ページとなっており、各種警告や攻撃情報、接続やシステムのリソース使用状態がまとめて表示される（画面1）。右上には5つのボタンが並び、このうちの「イージーセットアップウィザード」を起動すると文字通りウィザード形式で、初期設定がすべて行なえる。管理者はパスワードやPPPoEでのブロードバンド接続、DHCPサーバ、アンチウイルスの強度などを選択するだけだ。

設定ツールの左側には、「システム」「ルータ」「ファイアウォール」「VPN」、「IPS」、「アンチウイルス」、「Webフィルタ」、「スパムフィルタ」「ログ&レポート」などのボタンが並んでおり、個別の設定はここから行なう。左のメニューを押すと、サブメニューが表示される。それを開くとメニューによっては右側

図6●統合セキュリティゲートウェイの導入



既存のファイアウォール・ルータと同居指せる場合には、トランスペアレントモードで利用すればよい

画面1●トップページでは、システムや接続の状態、警告などを一元管理できる

に複数のタブが登場する。

複数の機能が搭載されているだけあって、全設定を展開すると非常に膨大な項目になる。ポリシーを登録しなければならないファイアウォールや接続先やセキュリティ設定を行なう必要があるVPN、閲覧制限するジャンルを選択するWebフィルタリングなどは特に設定項目が多い。逆にアンチウイルスやIDS・IDPなどはパターンファイルやシグネチャの中身を確認する程度で、特別な設定はない（画面2）。

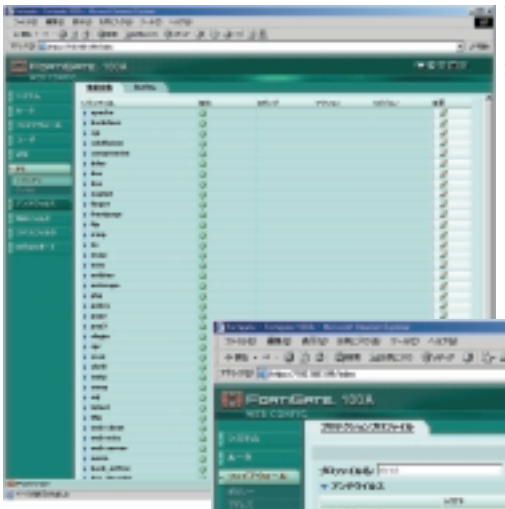
複数のセキュリティ機能にまたがるプロテクションプロファイル

統合型セキュリティゲートウェイならではの機能として注目したいのは、「ファイアウォール」の「プロテクションプロファイル」という設定だ。これは複数のセキュリティ機能の設定を1つのプロファイルにまとめる機能である。プロファイルを開くと、「アンチウイルス」、「Webフィルタリング」、「Webカテゴリフィルタリング」、「Webカタログフィルタリング」、「Spamフィルタリング」、「IPS」「コンテンツアーカイブ」など各機能の設定が並んでいる（画面3）。

たとえば「アンチウイルス」では、どのプロトコルを対象とするか、ファイルサイズのしきい値を超えた場合どうするかなどが指定できる。「Webカテゴリフィルタリング」ではカテゴリブロックを有効にするか、また有効にするのであれば「違法性・犯罪性の高いサイト」や「非生産的になりそうなサイト」などいずれのカテゴリをブロックするか、など詳細な設定が行なえる。このように各セキュリティ機能の設定を横断的にまとめて1つのプロファイルにするのだ。

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などに対して、このプロファイルを適用する。使いこなすと、「12時から13時まで特定のユーザーについてのみ業界動向を流すニュースサイトだけ閲覧可能にする」といった細かいアクセス制御が行なえる。

画面2・3● FortiGateの設定



画面2●IDS・IDPのシグネチャを一覧し、それぞれ有効・無効を決められる

画面3●複数のセキュリティ機能の設定をまとめたプロテクションプロファイル

お問い合わせ先