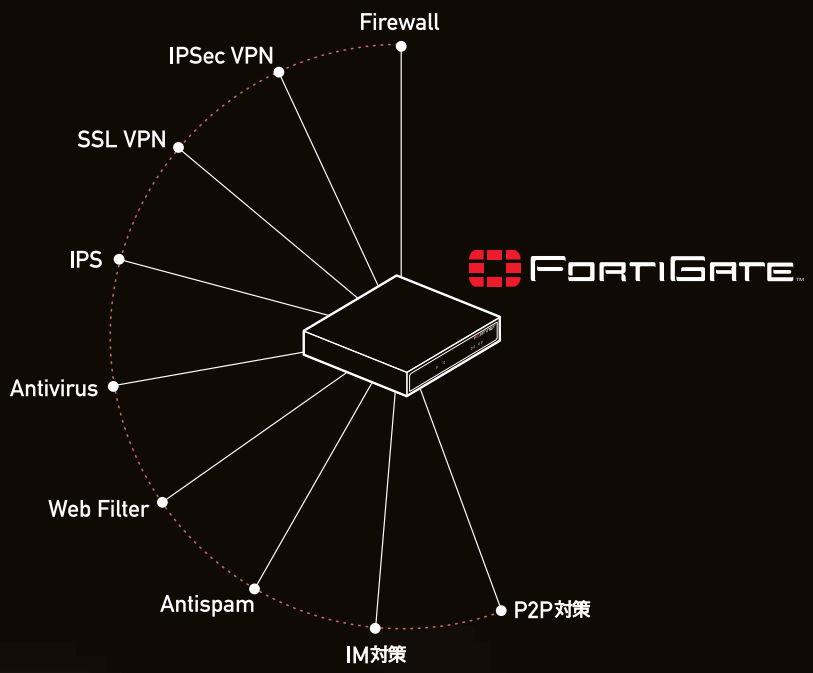
FIRST FOR UTM SECURITY SOLUTIONS.

ゲートウェイで求められる9つのセキュリティ機能が“全部入り”。

FortiGate™ Series



FORTINET™
REAL TIME NETWORK PROTECTION

UTMアプライアンスはFortiGate™

巧妙さを増す多面的な攻撃

メールを利用して企業内のユーザーにトロイの木馬型ウイルスを送り付ける攻撃や、閲覧したWebサイトから企業ネットワークにスパイウェアを侵入させる攻撃、サーバのアプリケーションの脆弱性を突く攻撃など、企業のセキュリティを脅かす攻撃は、シンプルなものからより複雑なものへと、日々巧妙さを増しています。このような多面的な攻撃を、ファイアウォールだけですべてを防止することは不可能です。

情報漏洩対策もますます重要に

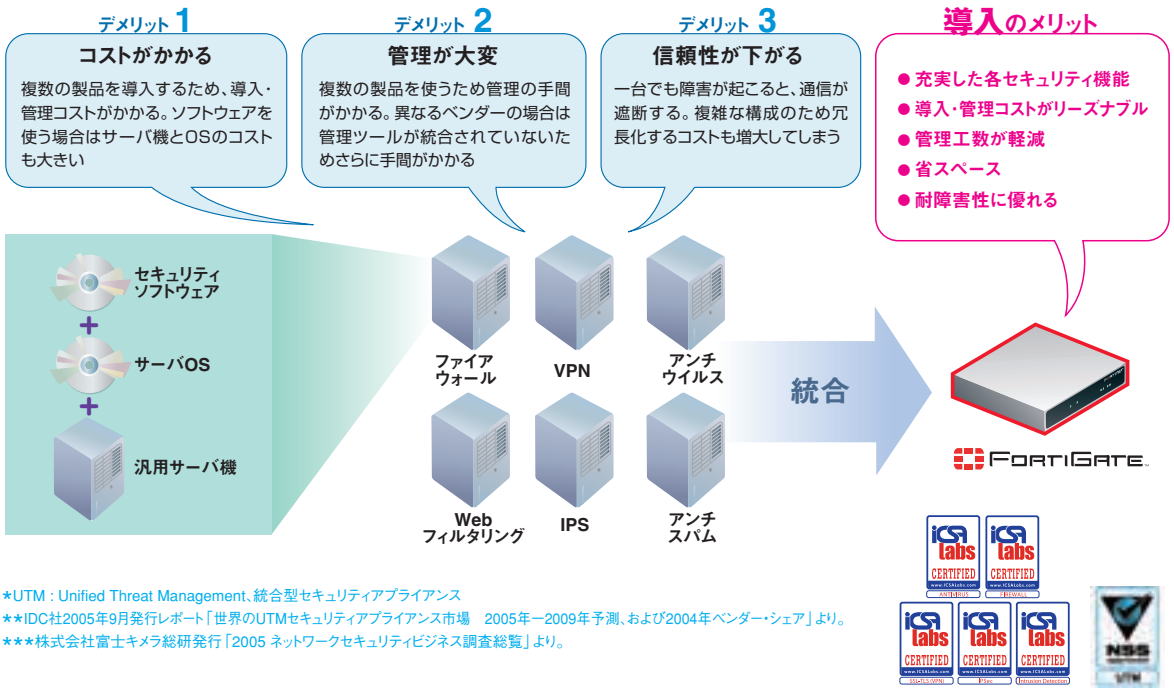
また、2005年4月に施行された個人情報保護法により、多くの企業は個人情報を中心とした重要情報の漏洩やウイルスによる業務停止といった情報セキュリティインシデント（事件、事故）のリスクが、ますます重大なものとなっています。

多様化する脅威に優れたコストパフォーマンスで対抗するFortiGate™

このような多面的な攻撃からネットワークを守るため、外部からの不正侵入を検知するIDS製品や、メールで感染するウイルスの拡散を防御するゲートウェイレベルでのウイルス対策製品、さらにはスパムメール対策製品などの導入が次々に必要となってきました。しかし、これらの機能を単体（専用アプライアンスやソフトウェア）で別々に導入していくことは、機器自体のコスト、そして、ネットワーク構成の変更や管理などのプロセスに掛かるコストの面から、企業に大きな負担を強いることになってしまいます。この問題を解決するために登場したのが、「UTMアプライアンス*」であるFortiGate™シリーズです。FortiGate™シリーズはファイアウォールをベースに複数のセキュリティ機能を統合しており、複合的、多面的な脅威に対抗することが可能であるばかりか、1つのインタフェースで全ての機能を制御できるため、管理コストも低減させることができます。

1台で9つのセキュリティ機能を実現

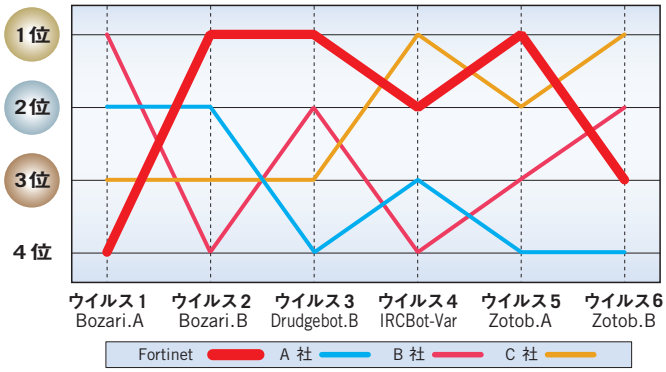
「FortiGate™シリーズ」は、企業のインターネットゲートウェイに必要な9つのセキュリティ機能〔ファイアウォール、IPsec-VPN、SSL-VPN、アンチウイルス（アンチスパイウェア含む）、P2P（Peer to Peer）ファイル型交換ソフト（以下P2Pソフト）対策、インスタントメッセンジャー対策、Webコンテンツフィルタリング、IPS、アンチスパム〕を一台で実現するUTMとして、2年連続で世界シェア首位**、日本市場でもシェアは70%を超え、首位***を独走しています。



*UTM : Unified Threat Management、統合型セキュリティアプライアンス
**IDC社2005年9月発行レポート「世界のUTMセキュリティアプライアンス市場　2005年ー2009年予測、および2004年ベンダー・シェア」より。
***株式会社富士キメラ総研発行「2005 ネットワークセキュリティビジネス調査総覧」より。

パターンファイル更新速度 No.1

右のグラフをご覧ください。2005年8月に発表された「MS05-039ー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」の調査を元に、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更新速度を比較したものです。FortiGateのパターンファイル更新が、他社と比較して、いかに迅速かご理解いただけるでしょう。



未知のウイルスへの対応速度 No.1

未知のウイルスには、「ヒューリスティック（heuristic）」テクノロジで対応します。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・コードの動き自体を見て、ウイルスを検出する技術です。上記の全6種類のウイルスを、ヒューリスティックによって「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できたのも、AV-Test.orgの調査によると国内でよく使われているアンチウイルスベンダー4社中フォーティネットだけでした。

	ウイルス 1 Bozari.A	ウイルス 2 Bozari.B	ウイルス 3 Drudgebot.B	ウイルス 4 IRCBot-Var	ウイルス 5 Zotob.A	ウイルス 6 Zotob.B
Fortinet	○	○	○	○	○	○
A 社					○	○
B 社						
C 社						

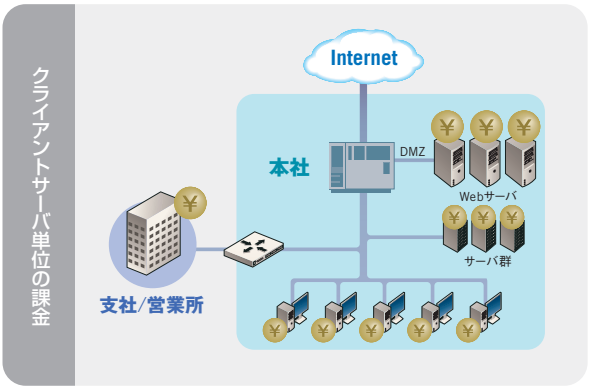
ドイツの第三者機関「AV-Test.org」による調査データを元に作成。（調査月:2005年8月）

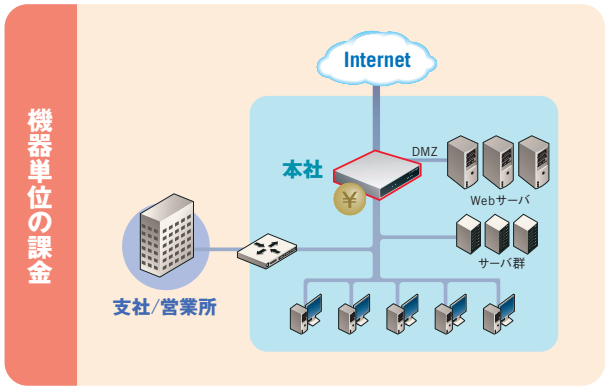
ASICによる高速処理

FortiGate™は、アンチウイルスなどスキャニングの高速処理のために、独自開発した専用ASIC「FortiASIC™」と専用OS「FortiOS™」を搭載しています。このため、ネットワークのパフォーマンスを損なわずに、アンチウイルスやコンテンツフィルタリングを、リアルタイム行うことができます。

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、ユーザーごとにライセンス料金を支払う料金体系をとっています。そのような料金体系では、機器の導入コストばかりか、ユーザーが多ければ莫大なライセンスコストがかかり、ライセンス管理の手間とコストもかかります。FortiGateは、ユーザー単位ではなくアプライアンス単位の料金体系を採用していますので、イニシャルコストもランニングコストも低く抑えることができます。





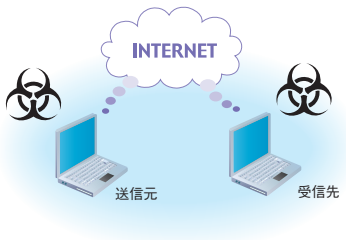
STOP! 「Winny」からの情報漏洩

FortiOS™ 3.0の新機能 1

終わらない「Winny」からの情報漏洩

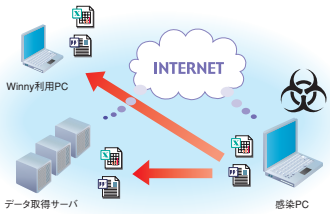
WinnyなどのP2Pソフトを利用し、不特定多数の個人間で直接情報のやり取りを行なっている社員や取引先のPCがウイルスに侵されてしまうことで、顧客情報や機密情報が流出する事件は、増加の一途をたどっています。これらの事件を起こしているWinnyをターゲットとしたウイルス「Antinny」は、一般的なゲートウェイアンチウイルスでは感染行動をブロックできないため、侵入自体を防ぐことは難しいようです。
また、一般企業が業務でWinnyを利用する必要はほとんどないため、Winny自体の通信を止めてしまえば、Winnyから情報漏洩することはなくなります。しかしWinnyは、任意のポート（実際に通信される出入口）を利用できるだけでなく、仮にポートが閉じていても限定的に接続できる機能があるため、一般的なファイアウォールやルータを使って止めることは困難です。

Winny利用型ウイルス：Antinnyの基本的動作



❶Winny経由で侵入
一般的なゲートウェイアンチウイルスは、Eメール/HTTP/FTPのみをチェックしているため、侵入を検知できません

❷クリックすると偽の表示が！
既にウイルスは発病しています

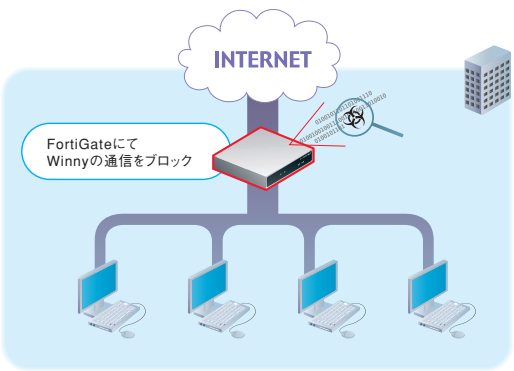


❸デスクトップファイルなどを外部へ送信（漏洩）
一般的なゲートウェイアンチウイルスでは防止できません

FortiGate™ ができること

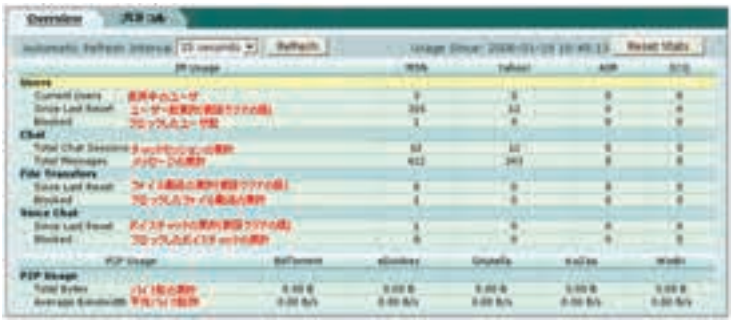
「Winny」による通信を遮断

FortiGate™の最新版ファームウェアFortiOS™ 3.0では、Winnyによる通信を「ブロック（遮断）」することや、「レート制限（帯域制御）」することができます。「遮断」に設定した場合は、たとえPCにWinnyがインストールされていても使用できなくなります。Winnyの通信を根本的に遮断してしまえば、Winnyを通じて大切な情報が漏洩する事を防止できます。



他のP2Pソフトについても遮断やレート制限が可能

FortiOS™ 3.0は、P2Pソフトに対応するセキュリティ機能を大幅に強化しました。日本独自のWinnyの他、世界的に使われているGnutellaやKaZaa、Skype、BitTorrent、eDonkeyなど、P2Pソフトごとに通信のブロックや許可、レート制限などを設定できます。また、それぞれのP2Pソフトが通信したデータの累計や、平均使用帯域などのレポートが行えることも特徴です。



※赤色の文字は管理画面には表示されません。

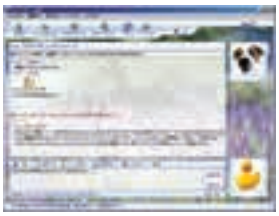
STOP!

FortiOS™ 3.0の新機能 2

インスタントメッセンジャーからの情報漏洩とウイルス流出

インスタントメッセンジャーの普及と新たな脅威

インターネットに接続している相手と、リアルタイムにチャットやファイル転送などが行える「インスタントメッセンジャー（IM）」が、ブロードバンドの普及とともに幅広く使われるようになってきました。会議中や在宅勤務中の相手との連絡ツールとして、また簡易テレビ会議システムとしても利用することができ、通信コストの節約にもなるため、業務に利用している会社も増えています。大手ポータルサイト各社も、サービスの一貫として自社ブランドのIMクライアントを無償配布しており、今後もますます普及するものと思われます。しかし、IMがウイルスの新しい侵入経路や情報漏洩の経路となる危険があることをご存知でしょうか。IMは上記のようなメリットを業務にもたらすため、セキュリティ面が不安だからと言ってトラフィックを遮断して、IMを全面使用禁止にしてしまうのはもったいない話です。

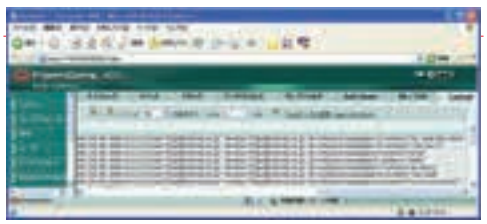


FortiOS™ 3.0でインスタントメッセンジャーを安全に使用

FortiOS™ 3.0は、IMでのファイル送受信時に、ウイルスを検索し、ウイルスを検知した場合にはファイルごと隔離する機能を持っていますので、安心してIMを業務に利用することができます。また、アプリケーションごとにログイン・ファイル転送や音声通信を個別にをブロックすることや、IMを利用しているユーザーの数や累計、メッセージ数を確認することもできます。対応しているIMは、Yahoo! Messenger、MSN Messenger、AOL Instant Messenger、そしてICQです。

インスタントメッセンジャーのアーカイブにも対応

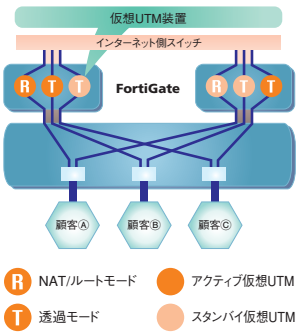
また、レポート分析ツールの「FortiAnalyzer™」と連携させることで、チャットの内容を記録することもできます。日本版企業改革法（J-SOX）に対応するため、社員が送受した電子メールの記録を保存することが求められるようになってきていますが、FortiOS™ 3.0とFortiAnalyzer™の連携により、IMについての同様の保存を行うことが可能です。



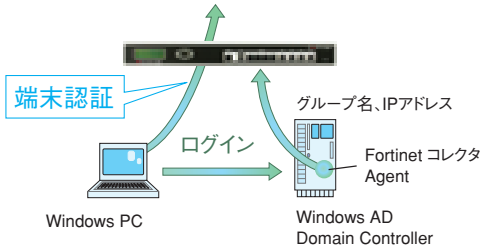
バーチャルドメイン（仮想UTM機能）機能とSSL-VPNの実装　その他の主な最新機能

バーチャルドメイン（仮想UTM機能）機能

FortiOS™ 3.0では、1台のFortiGate™上で仮想的に複数のUTM機能を実行するできるようなバーチャルドメイン機能を拡張しました。これは、大規模サイトやISPのお客様を対象とした機能で、NAT（Network Address Translation）/ルートモードと透過モードの二つの動作モードを混在させることができます。またもう一台のFortiGate™を利用すれば、仮想UTMをHA（ハイ・アベイラビリティ）構成とすることも可能です。



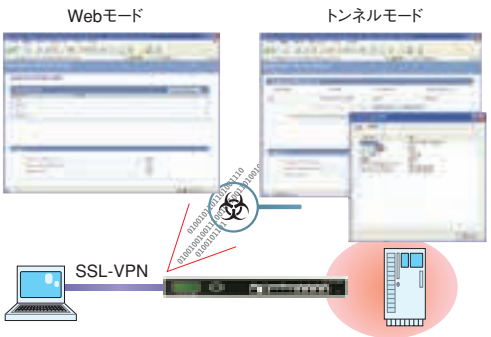
Windowsドメインへログインしたユーザ端末を自動認証
シングルサインオン



WindowsのActive Directoryを利用したユーザー端末のシングルサインオン機能も実装しています。この機能を使えば、Windows ドメインへ一度ログインした端末はその後は自動認証され、FortiGate™での認証を省略することができるようになります。

SSL-VPN

SSL-VPN機能も新しく実装されました。ブラウザに標準装備されているSSL（HTTPS）機能を利用して、社内のWebアプリケーション・サーバーなどにアクセスする「Webモード」と、すべてのプロトコルを暗号化する「トンネルモード」の2つのモードを用意しています。



電源ONだけで設定を復旧ーFortiUSB

FortiGate™の背部にあるUSB（Universal Serial Bus）端子に専用メモリ「FortiUSB」を接続するだけで、ファイアウォールやVPN、IPSなどのFortiGate™の全UTM機能（コンフィグ）と、ファームウェアを、簡単にバックアップすることができます。作業ミスなどで設定を復旧（リストア）したい場合でも、FortiUSBを差し込んで、電源を投入するだけで全てが終了します。

STOP! 内部攻撃による被害

FortiGate-224B 1

FortiGate-224B™

統合ネットワーク アクセス エッジ セキュリティ

「Nimda」「CodeRed」「MS Blast」……。企業ネットワークに内部からの攻撃で深刻なダメージを与えてきたネットワーク型ウイルスは、2003年のMS Blastで表面化し、大きな問題をもたらしました。またボットと呼ばれるタイプのワームは、いったん内部に入り込むと、周りのPCを攻撃したり、スパムを大量に送信し、内部に対しても攻撃や感染活動を行います。

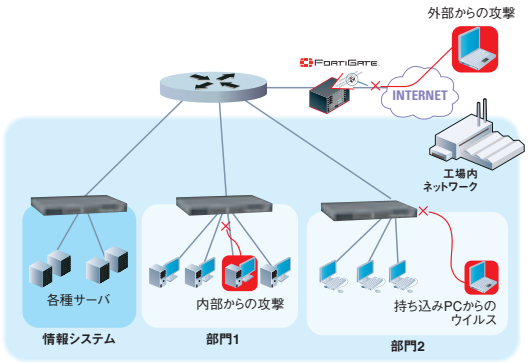
これらの被害の一因は、社外から持ち込まれたノートPC。社外のインターネット接続でワームに感染してきた社員が、そのままPCを社内LANに接続することで、社内全体に被害が拡大したケースが数多く報告されています。また、ビジネス・パートナーや業者などが持ち込んだPCなど、全く管理が行き届いていないPCに対しては、より注意を払わねばなりません。

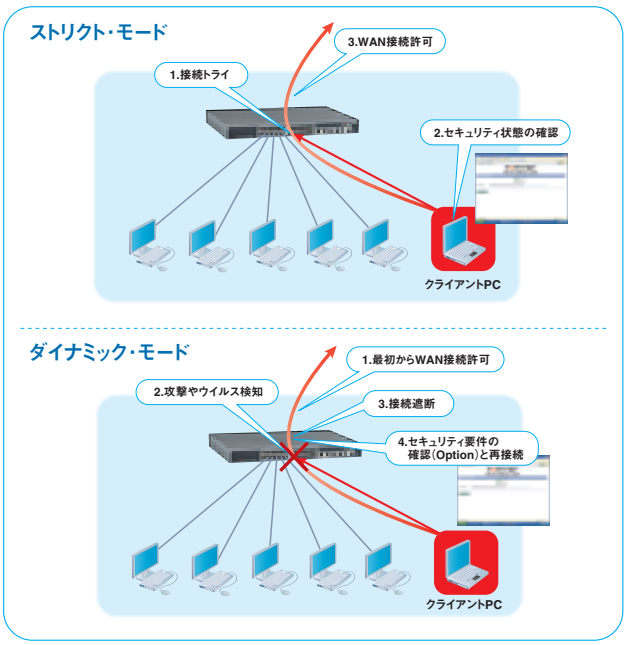
このような問題の対策として注目されているのが、検疫ネットワークです。PCを社内LANに接続しようとした際、コンプライアンスを検査する仕組みです。問題がなければ社内LANへの接続を許可しますが、セキュリティの問題があれば対策を施さない限り社内のネットワークに接続させません。このため、外部から持ち込まれたPCや、出先で感染したPCから社内LANを守ることができるのです。

FortiGate-224B™ ができること

スイッチングと検疫／アクセスコントロール機能を搭載
3つの機能が融合された内部セキュリティの為の新シリーズ

インターネットだけが危険であり、社内ネットワーク内がクリーンであると言う前提は崩れつつあります。ゲートウェイをすり抜けて侵入するウイルスへの対処や、ネットワークのセキュリティを保持するため、セキュリティ要件を満たしたユーザーのみアクセスを許可できるシステムの確立の必要性が高まっています。
FortiGate-224Bは、外部からの脅威だけでなく、ネットワーク内部の脅威に対抗するためにスイッチ機能とアクセスコントロール機能をUTMに融合させた製品です。ファイアウォールやアンチウイルス、WebフィルタリングなどFortiGate特徴であるきめ細かい機能を、24のポートそれぞれに割り当てることができます。





2つのオペレーション モード
（アクセス・レイヤ・ポート・コントロール）

FortiGate-224Bは、オペレーション モードをポートごとに設定可能です。接続時に必ずポリシーが適用される「ストリクト・モード」と、違反を行ったクライアントを即座に隔離する「ダイナミック・モード」の2種類を用意しており、24ポートそれぞれに、異なったポリシーを設定できます。ストリクト・モードでは、ポートに接続した時点でポリシーを満たしていないクライアントを自動的に隔離します。ダイナミック・モードでは、接続時にポリシーを満たしているかどうかの確認は行いませんが、ウイルスやワームの拡散を試みようとしたクライアントは瞬時に切断し、他のポートに被害が拡散することを防ぐことができます。

FortiGate-224Bは、ファイアウォールやVPN（IPSec/SSL-VPN）、アンチウイルス、不正侵入検知・防御、Webコンテンツ・フィルタリング、アンチスパイウェア、アンチスパムといったFortiGateの全ての機能を含んでいます。

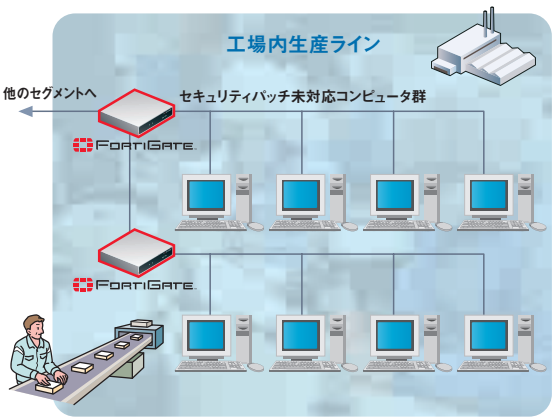
工場のFAシステムや小売店のPOSシステムはほとんど無防備です

セキュリティ対策が必要なのは、企業の基幹システムだけではありません。
「Windows Embedded」など、クライアントでのセキュリティ対策ソフトでは対応できない特殊なOSが利用される組込みシステムのセキュリティが大きな問題になりつつあります。
作り込みのアプリケーションの動作保証の問題から、サポート期間を終了したOSを使い続けざるを得なかったり、OSにセキュリティパッチを当てることができないケースもあり、FA機器やPOSシステム、医療機器などの組込みシステムにウイルス感染があった場合は、深刻な被害が想定されます。

例えば、

1）工場のFAシステムで

これまでは、工場LAN内の感染を止める効果的なソリューションがなく、工場内ネットワークに持ち込まれたノートPCから侵入した、たった1つのウイルスが工場全体をダウンさせ、企業存続の危機をも引き起こしかねない状態におかれていました。FAシステムの構成機器には最新のセキュリティパッチが適用されていないことも多く、瞬時に生産ラインの停止にまで追い込まれる可能性すらあったのです。FAシステムの脆弱性の問題は、生産停止や事後対応に要する莫大なコストなどを考えると、早急に対応をとる必要があります。この問題を解消するのが、内部UTMとしての使用に適したFortiGate-224Bです。



[FortiGate-224B]

- ポート間のスキャンにより、攻撃やウイルスを防御
- ポート毎のセキュリティスキャンポリシーの設定可能
- サポート終了済みやパッチ未対応のOS、またウイルス対策やパーソナルファイアウォールを未使用の端末の接続を拒否

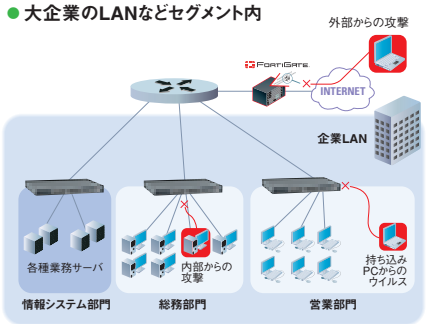
2）小売店のPOSレジで

POSシステムやATMなどの業務用端末は、Windows Embeddedなどの特殊なOSの採用が進むとともに、店舗システムのネットワーク化が進み、パソコンやサーバと同じレベルのウイルス対策やアタック防止策をとることが急務となっています。しかし、この分野での対策はまだまだ十分とは言えないのが現状です。POSは在庫管理や企業情報システムなどの重要な情報を持つシステムとネットワークで接続されているケースが多く、売上データや顧客データの改竄や盗聴などが行われてしまうと、企業活動に大きなダメージを与えます。しかし、ファイアウォールやアンチウイルスなど多くの単機能ソリューションを組み合わせることで包括的セキュリティソリューションを構築しようとしても、複雑かつ高価なものとなってしまい、維持するのはとても大変です。この状況に対するソリューションが、FortiGate-224Bです。

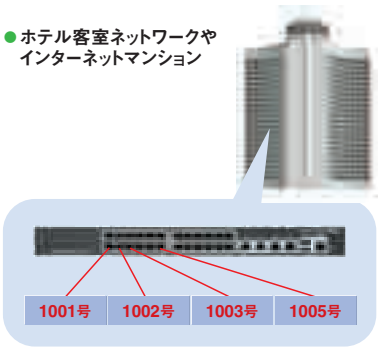
3）その他

内部セキュリティを検討すべき環境には主に下記の3つなどがあげられます。

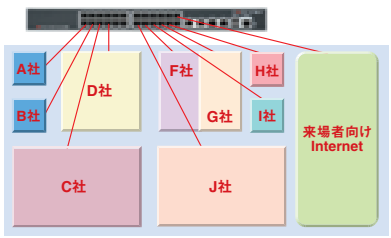
● 大企業のLANなどセグメント内



● ホテル客室ネットワークやインターネットマンション



● イベント会場ネットワーク



大企業LANでは、脅威の影響を受ける範囲を限定するため、各部門毎でのゲートウェイセキュリティが求められます。ホテル客室ネットワークやイベント会場ネットワークでは、セキュリティレベルの異なる不特定多数のクライアントが接続されるため、アクセスコントロールは必須です。FortiGate-224Bは、脅威を持ち込んだPCをリアルタイムで特定し、接続を拒否できる、UTMとアクセスコントロールと融合させた「統合ネットワーク アクセス エッジ セキュリティ製品」です。

ログの分析とレポーティングには — FortiAnalyzer™

複数のFortiGate™のログやイベントデータを安全に収集し、そのデータの分析を行うハードウェア製品です。高度なレポート機能とネットワーク利用状況の管理機能、コンプライアンス（法規制遵守）サポート機能などを搭載しています。ネットワーク管理者はネットワークの利用状況やセキュリティに関する情報を総合的に把握できるため、サービスプロバイダなど大規模システムを構築されているお客様には必かせないツールと言えます。FortiOS™ 3.0を搭載したFortiGate™と連携させることで、閲覧したWebサイトやメール・IMチャットの内容などを記録したり、隔離ファイルの内容を保存したり、それらについて詳細なレポートを作成することもできます。

FortiAnalyzer™ファミリー

複数のFortiGate™を効率よく管理するには — FortiManager™

FortiManager™システムは、中規模から大規模の企業やサービスプロバイダが、複数のFortiGate™を簡単効率よく管理したり、監視したりするための統合ツールです。
FortiManager™は、FortiGate™が提供する包括的なセキュリティサービスの導入や設定／監視／保守に必要とされる管理者の作業を最小限にし、リモートに置かれた複数のFortiGateによる統一されたセキュリティポリシーの確立を容易にするとともに、保守運用管理の負荷を大幅に軽減することができます。

FortiManager™ファミリー

FortiGate™シリーズ ラインアップ

SOHOからプロバイダまで対応する豊富なラインナップ

FORTINET™
フォーティネットジャパン株式会社
〒107-6223
東京都港区赤坂9丁目7番1号 ミッドタウン・タワー23階
TEL : 03-6434-8533　FAX : 03-6434-8532
お問い合わせ：http://www.fortinet.co.jp/contact/

お問い合わせ
株式会社ジーサウスシステムズ
GSouth systems
〒810-0004 福岡市中央区渡辺通3丁目6-15 NMF天神南ビル 3階
TEL 092-715-7400 (代表)　FAX 092-715-7401
http://www.gsouth.co.jp/ E-mail:gs-info@gsouth.co.jp

2008年5月