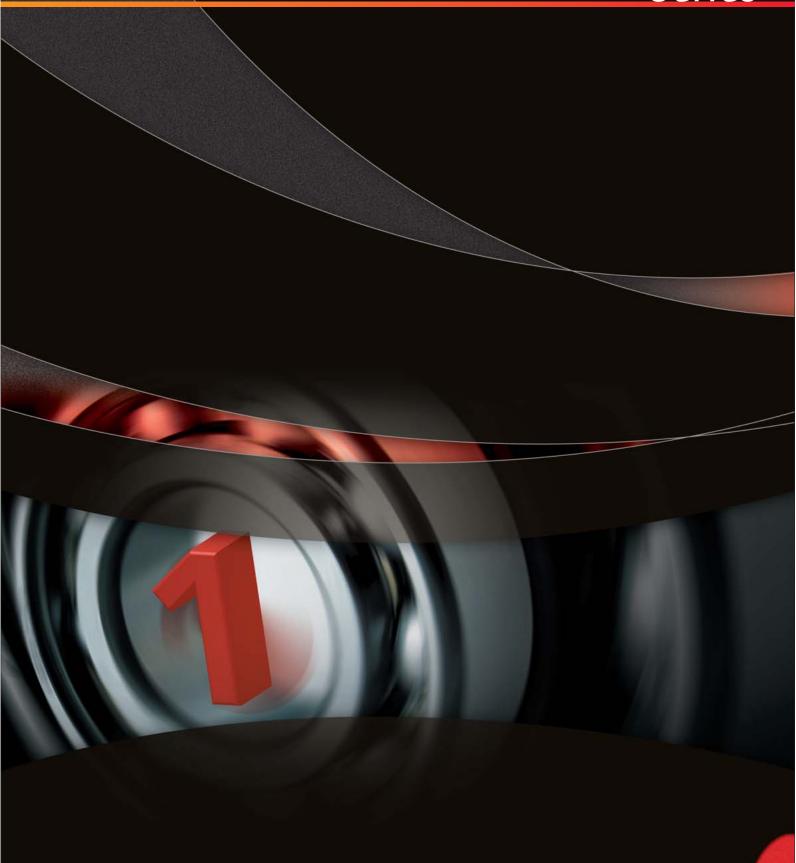
FIRST FOR UTM SECURITY SOLUTIONS.

様々な脅威から情報システムを守る

FORTIGHTE Series





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

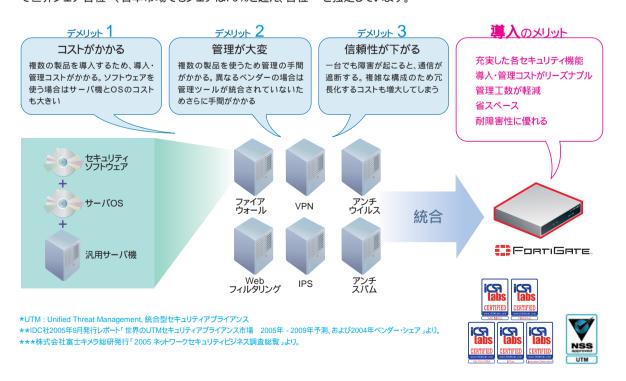
また、2005年4月に施行された個人情報保護法により、多くの企業は個人情報を中心とした重要情報の漏洩やウイルスによる業務停止といった情報セキュリティインシデンド(事件、事故)のリスクが、ますます重大なものとなっています。

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。

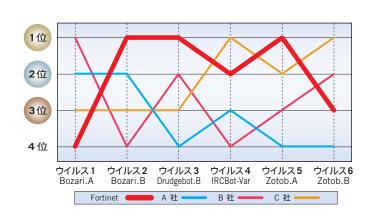
1台で9つのセキュリティ機能を実現

「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。



パターンファイル更新速度 10.1

右のグラフをご覧ください。2005年8月に発表された「MS05-039 - 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 $N_{0.1}$

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

	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	0	0	0	0	0	0
A 社					0	0
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)

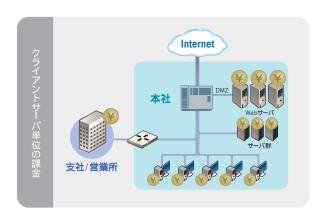
によって「疑わしいファイル」としてパターンファイル更新前に検出できたのも、AV-Test.orgの調査によると国内でよく使われているアンチウイルスベンダー4社中フォーティネットだけでした。

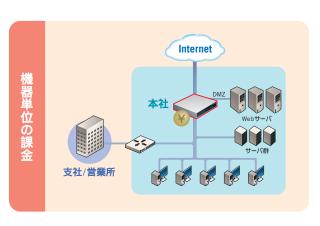
ASICによる高速処理

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。





FortiOS™ 3.0の新機能

「Winny」からの情報漏洩

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っことで、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、侵入自体を防く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



いてかな 解凍エラー XI 解凍できませんでした: 音楽ではないが、現れています。



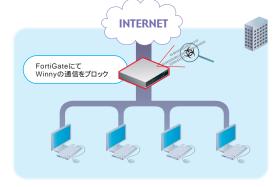
- ①Winny経由で侵入
- 一般的なゲートウェイアンチウイルスは、Eメール/HTTP/FTPのみをチェックしているため、侵入を検知できません
- ②クリックすると偽の表示が! 既にウイルスは発病しています
- ③デスクトップファイルなどを外部へ送信(漏洩) 一般的なゲートウェイアンチウイルスでは防止できません

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「プロック(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。

Automatic Refresh	n Interval 15 second	s • Refresh	Usage	Since: 2006-01-	19 10:49:13 P	Reset Stats
	IM Usage		MSN	Yahoo!	AIM	ICQ
Users						
Current Users	使用中のユーザ		3	0 0		0
Since Last Reset	ユーザー放業計(前回り)	316	12	0	4	
Blocked	プロックしたユーザ数	1	0	0	0	
Chat						
Total Chat Session	ダチャットセッションの業計		62	12 0		0
Total Messages	メッセージの異計		612	243 0		0
File Transfers		A STATE OF THE STA				
Since Last Reset			8	0 0		0
Blocked	ブロックしたファイル転送	の無計	1	0 0		0
Voice Chat						
Since Last Reset			1	0 0		0
Blocked	プロックしたボイスチャッ	homat	0	0	0	0
P21	Usage	BitTorrent	eDonkey	Gnutella	KaZaa	WinNY
P2P Usage						
Total Bytes	バイナ数の要計	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B
Average Bandwidt	カ平均パイト飲砂	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s

赤色の文字は管理画面には表示されません。

STOF

FortiOS™ 3.0の新機能

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。

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





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

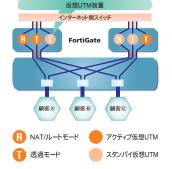
また、レポート分析ツールの「FortiAnalyzer 」と連携させることで、チャットの内容を記録することも できます。日本版企業改革法(J-SOX)に対応するため、社員が送受した電子メールの記録を保存 することが求められるようになってきていますが、FortiOS[™] 3.0とFortiAnalyzer[™]の連携により、 IMについての同様の保存を行うことが可能です。



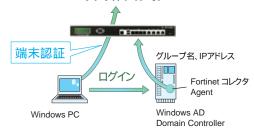
バーチャルドメイン(仮想UTM機能)機能とSSL-VPNの実装 その他の主な最新機能

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。またさもう 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。



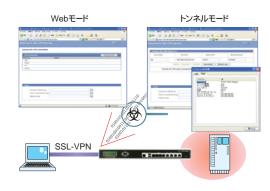
Windowsドメインヘログインしたユーザ端末を自動認証 シングルサインオン



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。プ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 - 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、 雷源を投入するだけで全てが終了します。

5

FortiG	ate™ファミリー		エントリー	-モデル	ミッドレンジモデ			
機能		FGT-50A	FGT-60	WiFi-60A	FGT-100A	FGT-200A	FGT-300A	FGT-400A
インターフェース	10 / 100 イーサネットポート	2	7	7	8	8	4	4
	10 / 100 / 1000 イーサネットポート ギガビット・イーサネットポート(カッパー / ファイバー)		_	<u> </u>		_		
	□□は4、3、4、4数	OEK.	FOIL	FOL	2001/	4001/	400K	4001/
システムパフォーマンス	同時セッション数 新規セッション数 / 秒	25K 2K	50K 2K	50K 2K	200K 4K	400K 4K	10K	400K 10K
	ファイアウォールスループット(Mbps)	50	70	70	100	150	400	450
	168ビット3DESスループット(Mbps) 同時ユーザ数無制限	10	20	20	40	70	120	135
	ポリシー数	200	500	500	1K	2K	5K	5K
	スケジュール数	256	256	256	256	256	256	256
アンチウイルス、スパイウェア、 ワーム検知&駆除 (ICSA認定取得)	HTTP、SMTP、POP3、IMAP、FTP、IM VPNトンネル内のスキャン ウイルスDBの" ブッシュ型 "自動更新							
	感染したメッセージの隔離 ファイルサイズによるプロック	-	-	-	-	オプション	オプション	オプション
ファイアウォール	NAT、PAT、トランスペアレント(ブリッジ)、ルートモード							
(ICSA認定取得)	VLANサポート(802.1q) バーチャル・ドメイン							
	ユーザグループベースの認証							
	H.323 NATトラバーサル プロテクション・プロファイル数	32	32	32	32	32	32	32
VPN (ICSA認定取得)	トンネル数 暗号化方式(DES, 3DES, AES) PPTP, L2TP, VPNクライアント・パススルー ハブ&スポーク・アーキテクチャ IKE認証(X.509) IPSec NATトラパーサル RSA SerurIDのサポート	20	40	40	80	200	1.5K	2K
コンテンツフィルタリング	URLプロック、キーワードブロック、URL除外リスト Javaアブレット、クッキー、ActiveXのブロック FortiGuardウェブフィルタリングのサポート							
P2P / インスタントメッセンジャー (IM)	P2P(Winny含む)の遮断、 帯域制御 IMコントロール							
不正侵入防御(IPS) (ICSA認定取得)	1400種類以上の攻撃の防御 カスタマイズ可能な検知シグニチャリスト 侵入検知/防御用DBの自動更新							
アンチスパム	RBL / ORDBサーバへのリアルタイムクエリ MIMEへッグー・チェック キーワード / フレーズ・フィルタリング IPアドレス・ブラックリスト / 除外リスト							
ロギング / モニタリング	メールによるウイルスや攻撃の通知 Syslog、SNMP							
ハイアベイラビリティ (HA)	アクティブ-アクティブ、アクティブ・バッシブ ステートフル・フェールオーパー(FW&VPN) 機器障害の検知・通知 冗長電源 リンクステータスのモニター	- - - -	-	-	-	-	-	-
ネットワーキング	マルチWANリンクサポート PPPoEクライアント(HA構成を除く) DHCPクライアント/サーバ ポリシーベース・ルーティング ダイナミック・ルーティング(RIP v1 & v2, OSPF)	-						
システム管理	コンソールインターフェース(RS-232) WebUI(HTTP / HTTPS)、複数言語サポート コマンドライン・インターフェース、 FortiManagerによる管理							
管理	複数管理者およびユーザレベル定義 TFTPとWebUlを介した更新および変更 システムソフトウェア・ロールパック							
ユーザ認証	内部データベース RADIUS / LDAP DBのサポート IP / MACアドレス・バインディング RADIUSによるXauthのサポート(IPSec) RSA SerurIDのサポート							
トラフィック管理 FortiGuard [™] サブスクリプシ	ポリシーベースの帯域制御 DiffServの設定 帯域幅保証/最大帯域幅/帯域幅優先割当							



Fortinet

7

ル		ハイエンドモデル								
FGT-500A	FGT-800	FGT-1000A	FGT-3000	FGT-3600	FGT-5001	FGT-5001FA2	FGT-5002FB2	FGT-5020	FGT-5050	FGT-5140
8	4	-	3	1	_	_	_	_	_	-
	— 4C	10 —	- 1C / 2F	 2C / 4F	4/4SFP	4/4SFP	4	8/8SFP	20 / 20 SFP	— 56 / 56 SFP
400K	400K	600K	975K	1M	1M	1M	1M	2M	5M	14M
10K	10K	15K	20K	25K	25K	25K	25K	50K	125K	350K
500 150	1Gbps 200	2Gbps 250	2.25Gbps 530	4Gbps 600	4Gbps 600	16Gbps 600	16Gbps 600	8Gbps 1.2Gbps	20Gbps 3Gbps	56Gbps 8.4Gbps
5K	20K	30K	50K	50K	50K	50K	50K	100K	250K	700K
256	256	256	256	256	256	256	256	256	1280	3584
オプション					_	_	_	_	_	_
		-								
32	32	32	200	200	200	200	200	200	200	200
3K	3K	5K	5K	5K	5K	5K	5K	10K	25K	70K
_	_	-								
										_
									_	-

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。



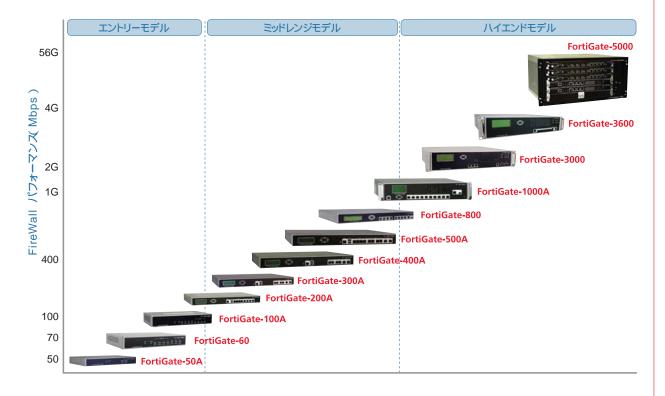
複数のFortiGate™を効率よく管理するには ── FortiManager™

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。



FortiGate™シリーズ ラインアップ



フォーティネットジャパン株式会社

〒107-0052 東京都港区赤坂2-12-10 国際溜池ビル6F TEL: 03-5549-1640 FAX: 03-5549-1641

お問い合わせ: http://www.fortinet.co.jp/contact/

記載された社名、各製品名は各社の登録商標または商標です。記載された内容は、変更する場合がありますのでご了承ください。

お問い合	わせ