



FortiOS 3.0の新機能のご紹介

フォーティネットジャパン株式会社

2006年2月時点での情報です。予告無く仕様変更になる可能性がございます。予めご了承ください。



企業をとりまく様々な脅威

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		○				

すでにファイアウォールとアンチウイルスだけでは
万全ではありません。

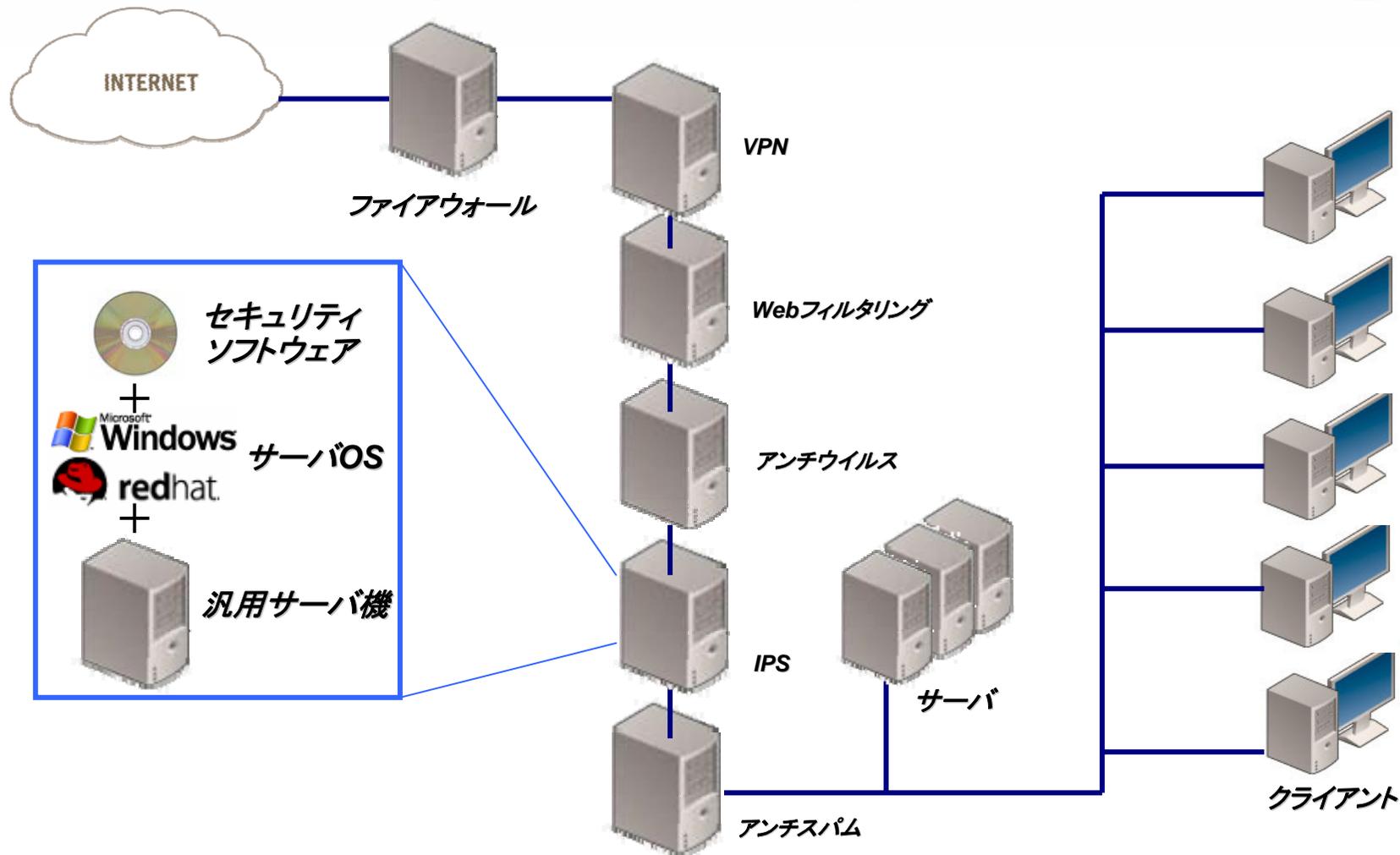
Why Fortinet?

FORTINET

Stateful Firewall • Antivirus • Spyware Protection • Intrusion Prevention • IPSec Virtual Private Network • Web Content Filtering • Antispam • Bandwidth Shaping

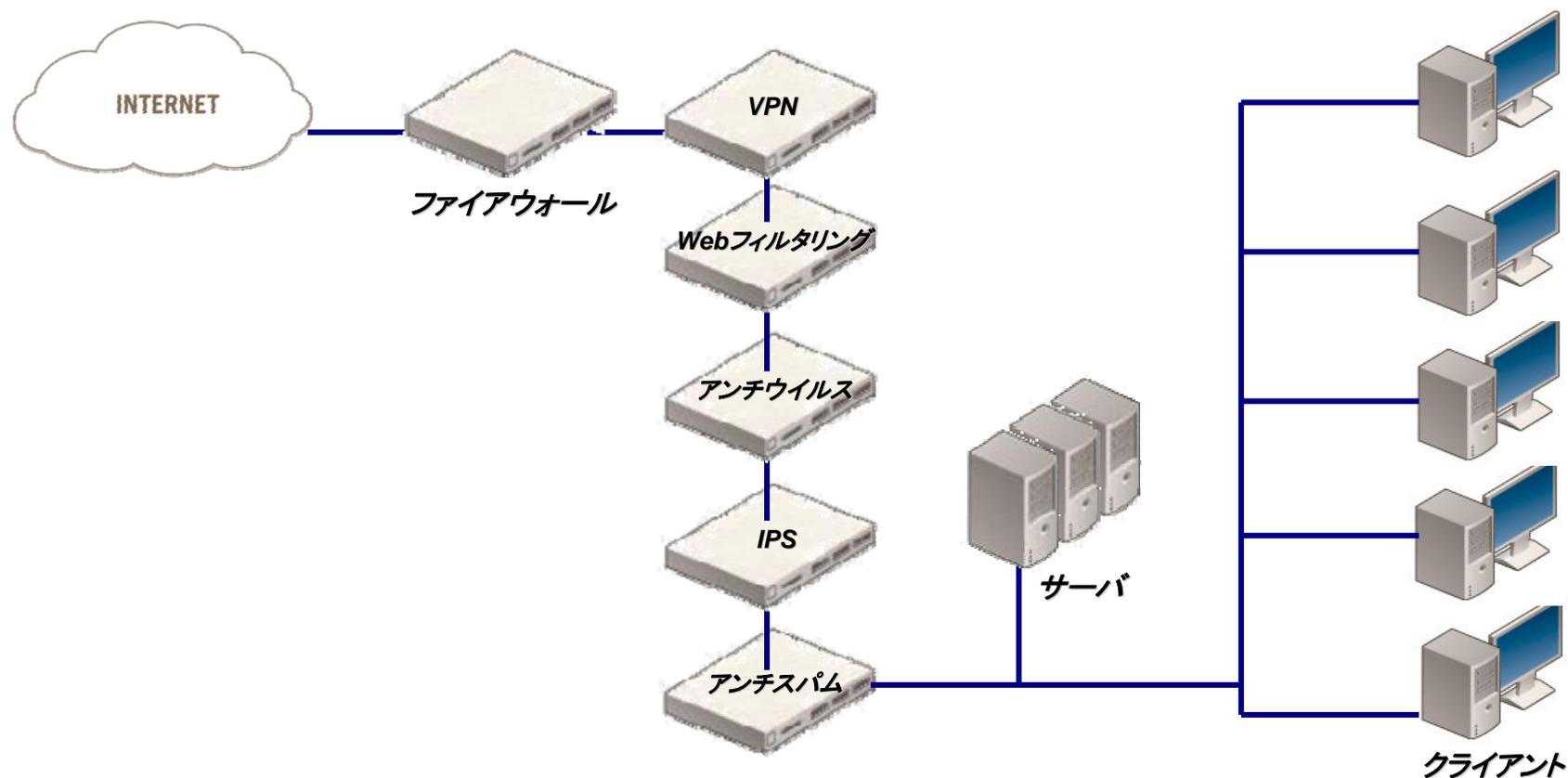
FortiGate以外の方法① ～セキュリティソフトウェアで構築～

サーバ機、サーバOS、セキュリティソフトウェアがすべて自由に選択可能

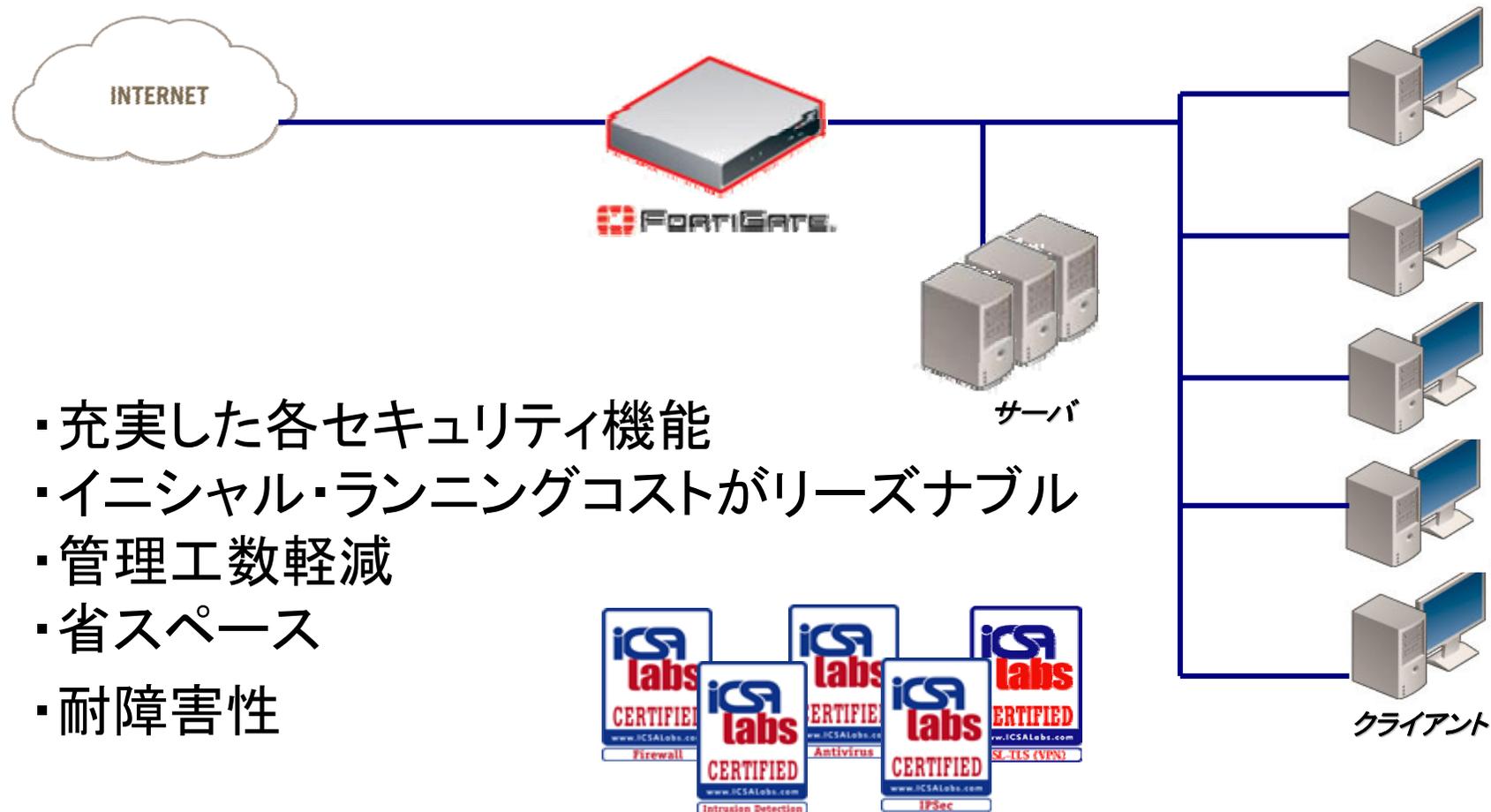


FortiGate以外の方法② ～単機能アプライアンスで構築～

セキュリティ機能ごとにアプライアンスを選択可能



理由その1. 一台で6つの主要な ゲートウェイセキュリティ機能を実現



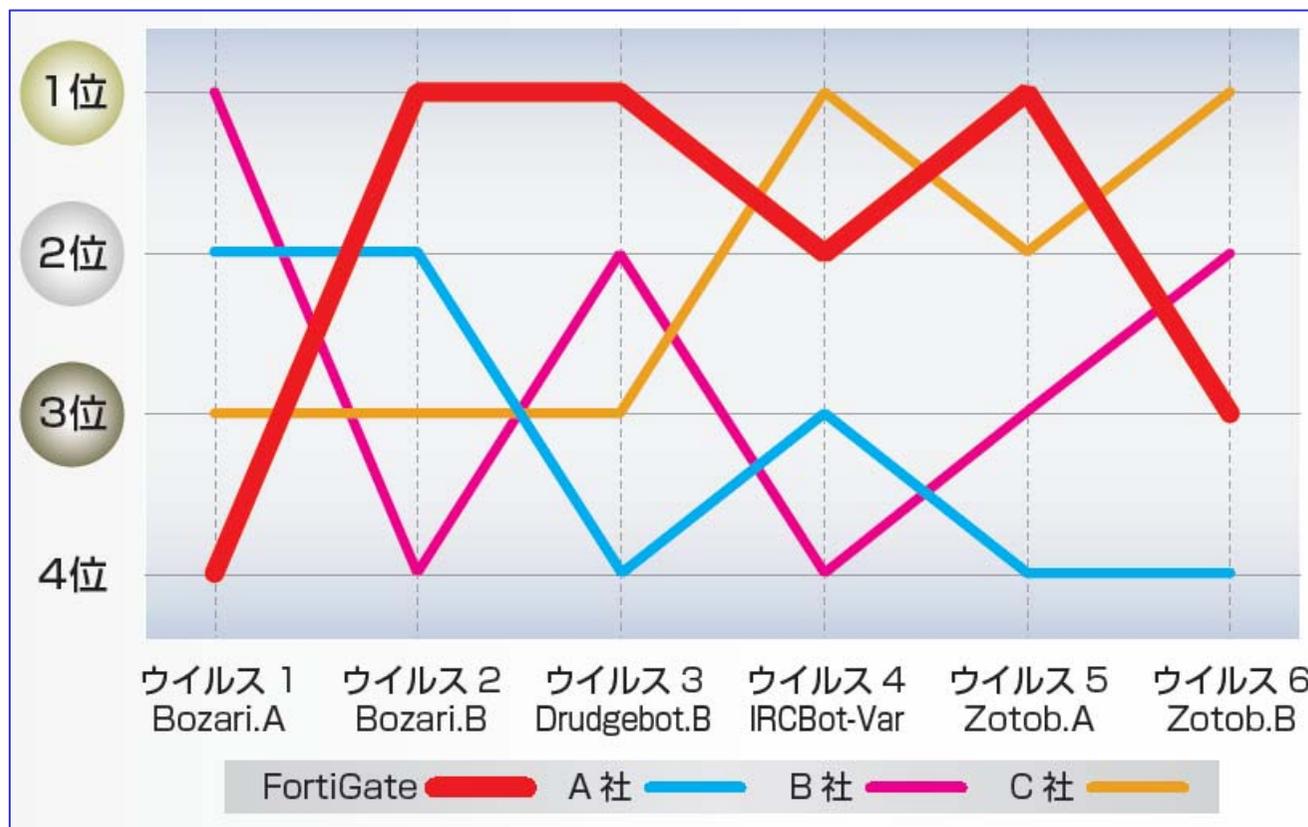
FORTINET

Stateful Firewall • Antivirus • Spyware Protection • Intrusion Prevention • IPSec Virtual Private Network • Web Content Filtering • Antispam • Bandwidth Shaping

理由その2.新しい脅威への優れた対応スピード (パターンファイル編)

パターンファイルの更新の早さの比較

次のグラフは、日本国内において代表的なアンチウイルスベンダー4社が、2005年8月に発表されたMS05-039の脆弱性を利用する6種類のウイルスに対して、パターンファイルを更新した時間を調査し、更新した時間が早かったベンダー順にグラフ化したものです。



※グラフは、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)

FORTINET

理由その2.新しい脅威への優れた対応スピード (ゼロデイアタック対応編)

ヒューリスティックにウイルスを検出できたのは、FortiGateだけ！

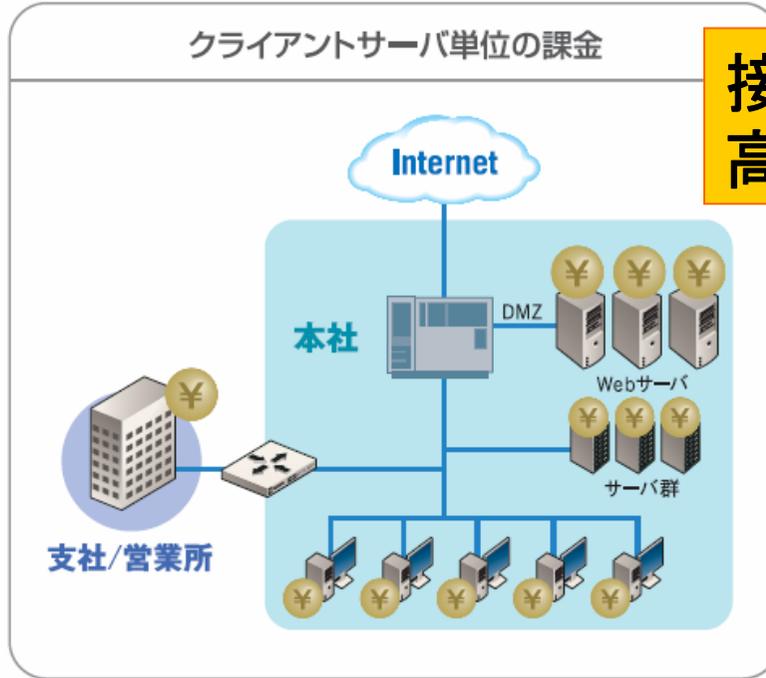
6種類のウイルスに対して、ヒューリスティックにウイルスを検出できたかどうかを表したものです。FortiGateのみが、全てのウイルスをヒューリスティックに検出することができました。つまり、パターンファイルの更新前にウイルスを、疑わしいファイルとして発見できたのです。

	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
FortiGate	○	○	○	○	○	○
A社					○	○
B社						
C社						

※グラフは、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)

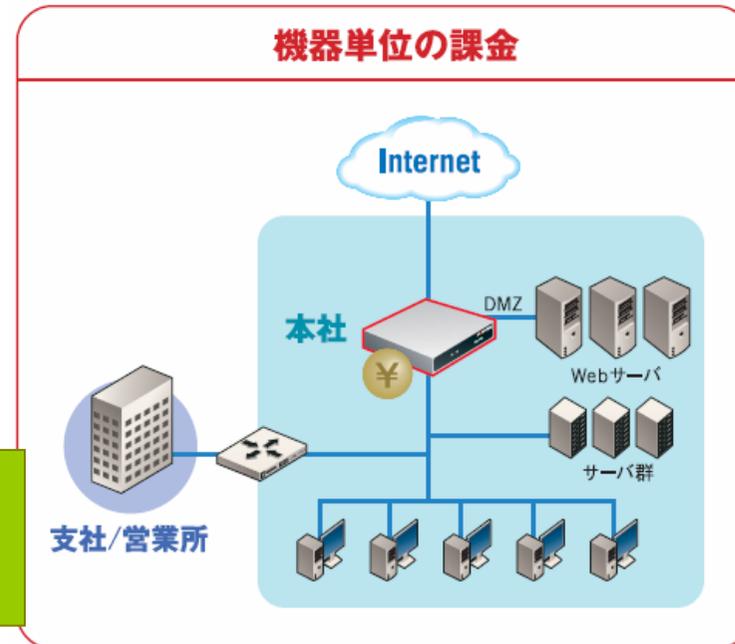
理由その3.クライアントライセンス無制限

クライアントサーバ単位の課金



接続機器のカウン트가面倒
高額なライセンス

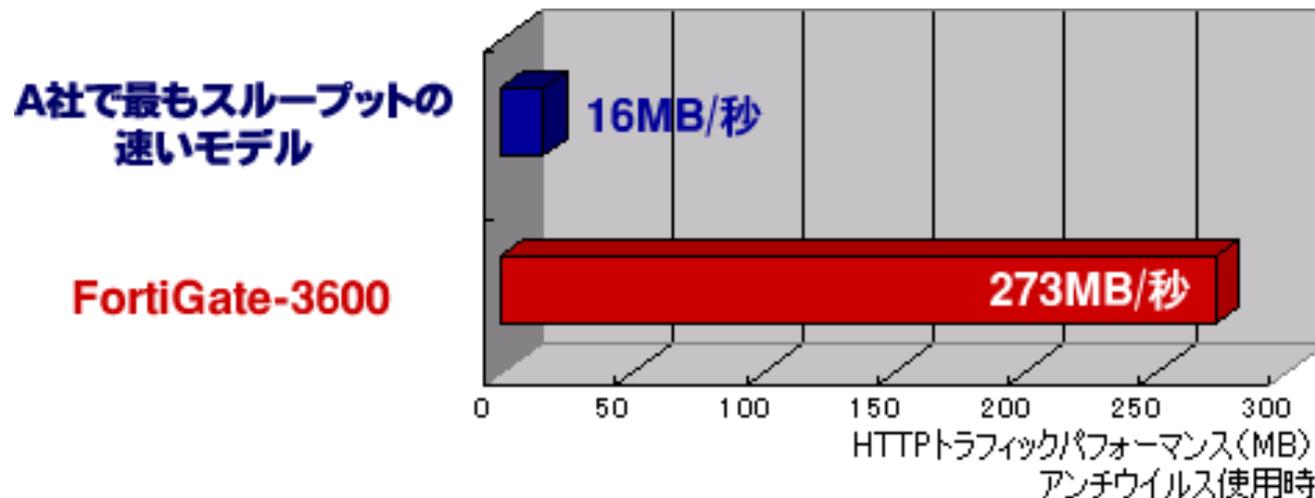
機器単位の課金



クライアント無制限
手間も無く価格もリーズナブル

理由その4. ASICによる高速処理

アンチウイルス処理のために独自開発した専用ASICと専用OSによって、驚異的な処理速度を実現。ネットワークのパフォーマンスを損なうことなく、リアルタイムにアプリケーション層サービス(ウイルスやコンテンツフィルタリング)を提供します。(下グラフ: 自社調べ 2005年)



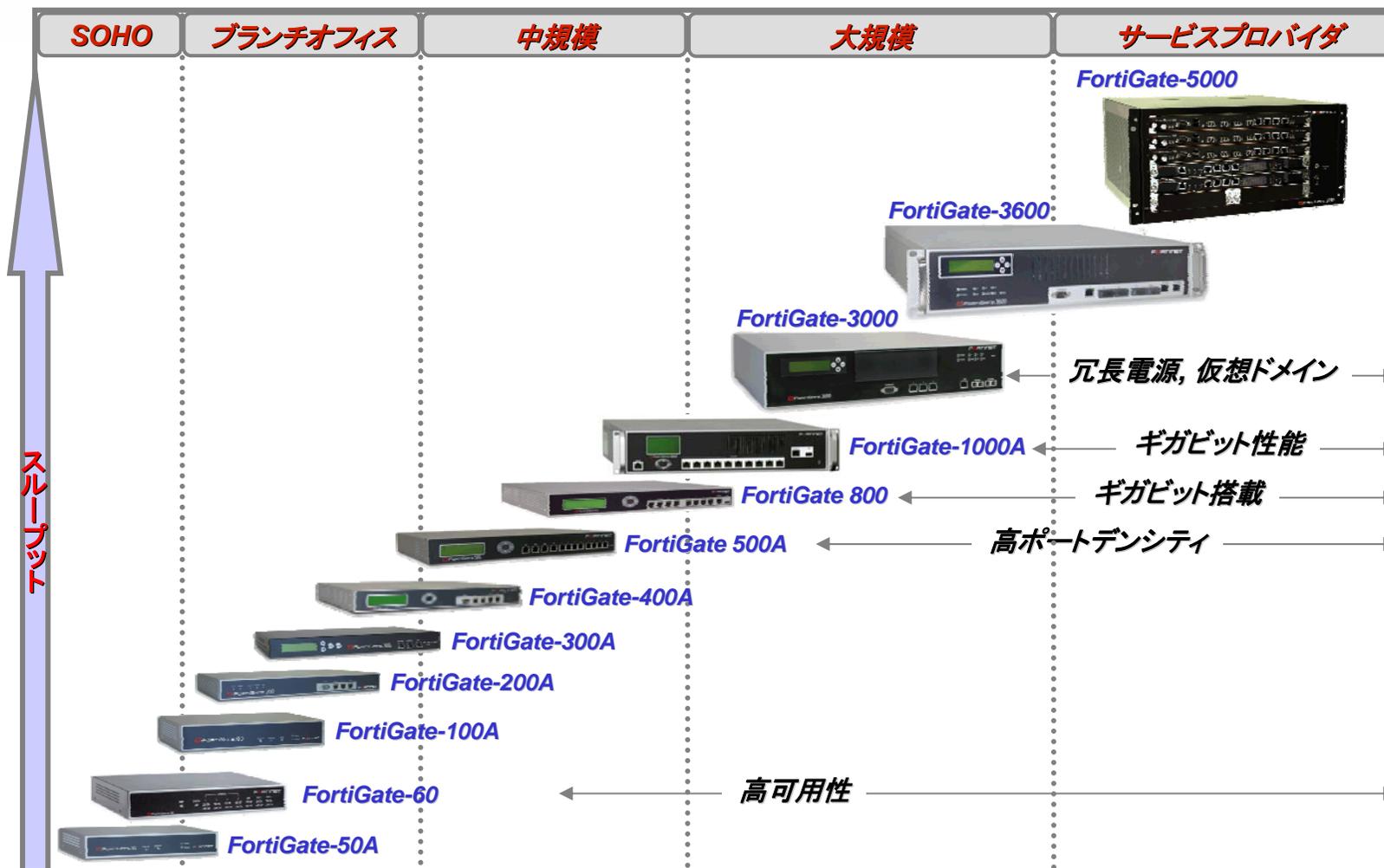
2005年9月現在

Footnote

FORTINET

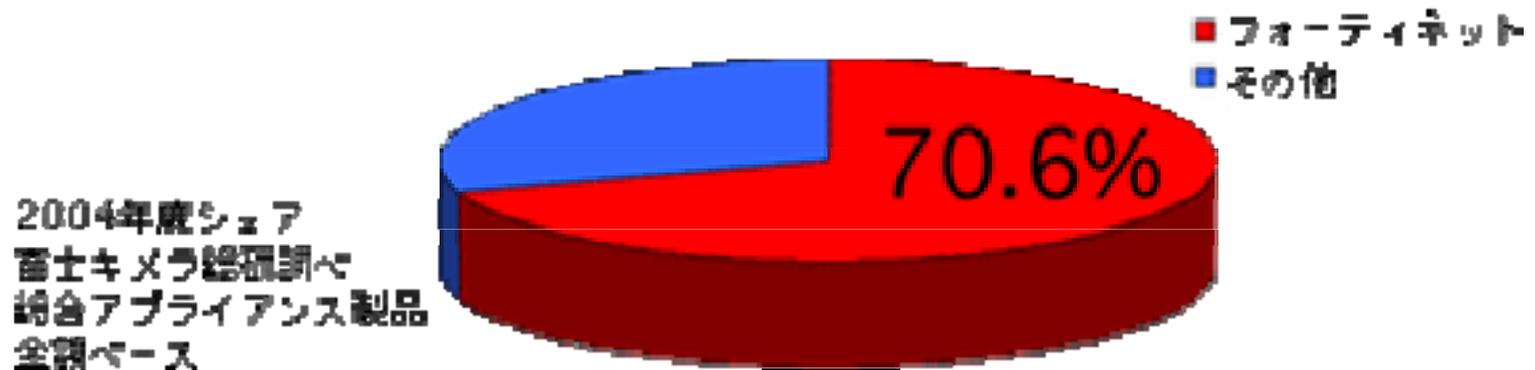
Stateful Firewall • Antivirus • Spyware Protection • Intrusion Prevention • IPSec Virtual Private Network • Web Content Filtering • Antispam • Bandwidth Shaping

理由その5.SOHOからプロバイダまで対応する 豊富なラインナップ



統合アプライアンス市場でのポジション

統合アプライアンス製品市場で国内シェアにおいてNo.1を獲得



<http://www.fortinet.co.jp/news/news.html>

- 2005年9月、市場調査会社IDC社が発表したレポート「Unified Threat Managementセキュリティ製品市場」において、フォーティネットが新しいカテゴリーである“UTM”セキュリティアプライアンス市場において市場シェア2年連続で第一位を獲得



<http://www.fortinet.co.jp/news/pr/2004/pr093004.html>
http://www.idc.com/getdoc.jsp?containerId=pr2004_09_10_182902

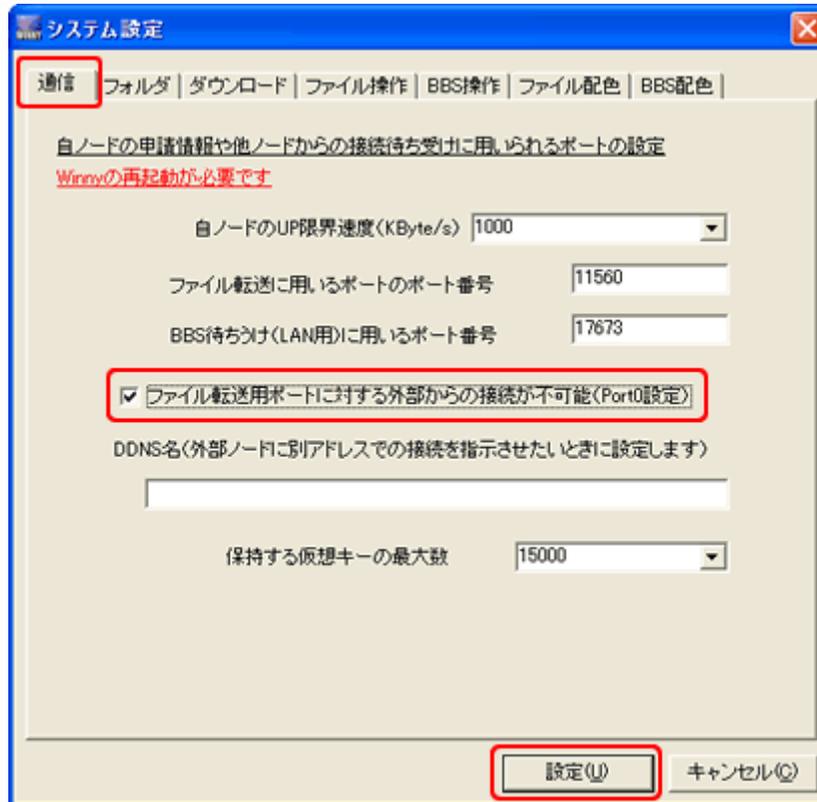
FORTINET

P2Pを止められない環境例

- 公衆無線LAN(喫茶店など)
 - インターネットマンション
 - ホテル内LAN
 - 航空機、列車内無線LAN
 - 大学構内(研究で利用)
- など

ただし帯域制御は可能な場合も

P2Pを簡単に止められない理由



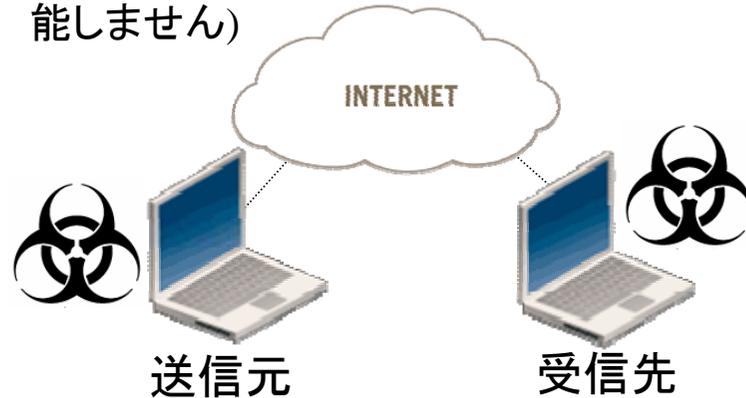
(Winnyの場合)

- 任意のポートを使用
- ポートを閉じていても限定的な接続が可能

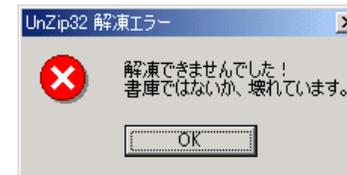
Winny経由の情報漏えい

～Winnyを悪用するウイルスAntinnyの基本的動作～

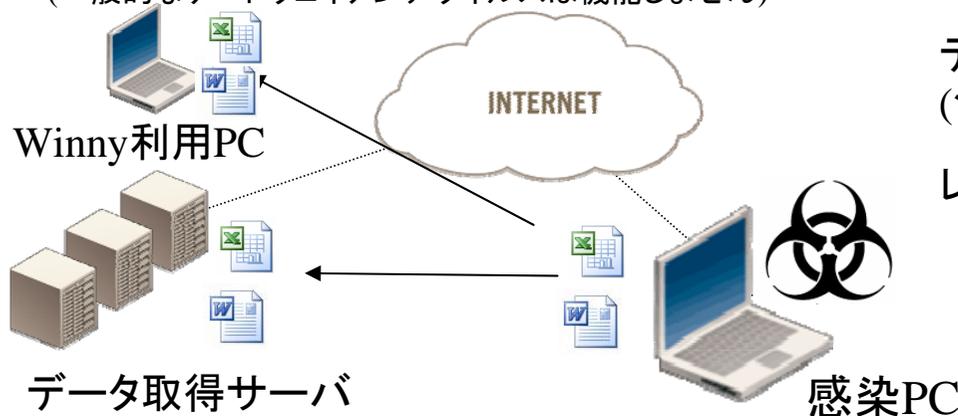
- ① Winny経由で侵入
(一般的なゲートウェイアンチウイルスは機能しません)



- ② クリックすると偽の表示が。
(既にウイルスは発病)



- ③ デスクトップファイルなどを外部送信
(一般的なゲートウェイアンチウイルスは機能しません)



デスクトップのスクリーンショットやファイルを送信
(ショートカットの場合は本体を探して送信)

レジストリから、ログイン名、ドメイン名を取得、送信

P2Pに対する新機能

- アプリケーション毎にブロック、許可、レート制限
- Overview(データサイズ累計、平均使用帯域)閲覧

日本固有のP2Pソフト”Winny”に
1stリリースより対応致しました！

2006/2現在:BitTorrent, eDonkey, Gnutella, KaZaa, Skype, Winnyに対応
※アプリケーション毎に制御機能が異なります。

企業にとってのIMとは？

便利な使用方法

- メールと電話の間を埋める
コミュニケーションツールとして有効
- 片手間コミュニケーション
- 通信費の節約
- 簡易テレビ会議システムとして
- 会議中の人と連絡などに便利
- 自宅で勤務中の連絡ツールとして

ネガティブ面

- 生産性低下
- モラル低下
- 情報流出
- ウイルスの新しい侵入経路

IMに対するIT管理者の迷い

- セキュリティ面の危険性があるから全面禁止
- or
- 仕事でも使えるからすべて許可



メリットを活かしつつ、管理
する方法はないものか...

IMに対する新機能

- ファイル転送のウイルスチェック
- アプリケーション毎にログイン・ファイル転送・オーディオのブロック
- Overview(使用中や累計のユーザ数、メッセージ数など)閲覧
- IM使用中ユーザのID確認
- 過去のIM使用者のID確認
- ホワイitelist、ブラックリスト
- チャット内容のアーカイブ

2006/2現在:AOL,ICQ,MSN,Yahoo!に対応

画面紹介

IM経由のウイルスチェックが可能

▼ アンチウイルス	HTTP	FTP	IMAP	POP3	SMTP	IM
アンチウイルススキャン	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ファイルパターン	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
隔離	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
分割メール転送			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
クライアントコンフォーティング	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
間隔 (1 - 900 秒)	<input type="text" value="10"/>	<input type="text" value="10"/>				
データ量 (1 - 10240 バイト)	<input type="text" value="1"/>	<input type="text" value="1"/>				
上限サイズを超えるファイル/メール	<input type="text" value="転送"/>	<input type="text" value="転送"/>	<input type="text" value="転送"/>	<input type="text" value="転送"/>	<input type="text" value="転送"/>	<input type="text" value="転送"/>
上限サイズ (1 - 25 MB)	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="10"/>	<input type="text" value="10"/>
送信メールに署名を追加する	<input type="checkbox"/> 有効	<input type="text" value=""/> (SMTPのみ)				

IM/P2Pのアプリケーション毎の管理が可能

アプリケーション毎にログイン、ファイル転送、オーディオブロックの設定が可能

IM / P2P						
	<input checked="" type="checkbox"/>					
ログインのブロック	<input type="checkbox"/>					
ファイル転送のブロック	<input type="checkbox"/>					
オーディオのブロック	<input type="checkbox"/>					
非標準ポートの監視	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
P2P						
	BitTorrent	eDonkey	Gnutella	KaZaa	Skype	WinNY
アクション	レート制限	レート制限	レート制限	ブロック	ブロック	ブロック
制限値(キロバイト/秒)	32	32	32	0		0

アプリケーション毎に許可、レート制限、ブロックなどの設定が可能

IM/P2PのOverviewを閲覧可能

Overview		プロトコル					
Automatic Refresh Interval		15 seconds	Refresh		Usage Since: 2006-01-19 10:49:13		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	ユーザー数累計(前回クリアの後)	316	12	0	4		
Blocked	ブロックしたユーザ数	1	0	0	0		
Chat							
Total Chat Sessions	チャットセッションの累計	62	12	0	0		
Total Messages	メッセージの累計	612	243	0	0		
File Transfers							
Since Last Reset	ファイル転送の累計(前回クリアの後)	8	0	0	0		
Blocked	ブロックしたファイル転送の累計	1	0	0	0		
Voice Chat							
Since Last Reset	ボイスチャットの累計(前回クリアの後)	1	0	0	0		
Blocked	ブロックしたボイスチャットの累計	0	0	0	0		
P2P Usage		BitTorrent	eDonkey	Gnutella	KaZaa	WinNY	
P2P Usage							
Total Bytes	バイト数の累計	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B
Average Bandwidth	平均バイト数/秒	0.00 B/s	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。

IM使用中のユーザを閲覧可能

現在のユーザ ユーザリスト Config

Protocol: All

#	Protocol	Username	Source IP	Last Login	
1	MSN	[redacted]@yahoo.co.jp	192.168.150.57	2006-01-26 18:51:01	Block
2	MSN	[redacted]@hotmail.co.jp	192.168.150.22	2006-01-26 18:46:04	Block
3	MSN	[redacted]@hotmail.com	192.168.150.61	2006-01-26 17:07:29	Block

過去のIM使用者の閲覧可能

現在のユーザ ユーザリスト **Config**

User Policy

When unknown IM users connect through the FortiGate, the following action should be taken:

	MSN	Yahoo!	AIM	ICQ
Automatically Allow	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Automatically Block	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

List of Temporary Users Protocol:

#	Protocol	Username	Policy	
1	Yahoo!	████kma	Allow	Permanently Allow Permanently Block
2	Yahoo!	████miya44	Allow	Permanently Allow Permanently Block
3	MSN	████@hotmail.co.jp	Allow	Permanently Allow Permanently Block
4	MSN	████@hotmail.com	Allow	Permanently Allow Permanently Block
5	MSN	████@hotmail.co.jp	Allow	Permanently Allow Permanently Block
6	MSN	████@yahoo.co.jp	Allow	Permanently Allow Permanently Block
7	MSN	████@hotmail.com	Allow	Permanently Allow Permanently Block
8	MSN	████@ruby.plala.or.jp	Allow	Permanently Allow Permanently Block
9	MSN	████@fortinet.com	Allow	Permanently Allow Permanently Block

ホワイトリスト、ブラックリストが作成可能

現在のユーザ ユーザリスト Config

新規作成

Protocol: All Policy: All

Protocol	Username	Policy	
ICQ	49938	Allow	 
MSN	@hotmail.com	Block	 
MSN	@yahoo.co.jp	Allow	 
MSN	@hotmail.co.jp	Allow	 
MSN	@hotmail.com	Allow	 
MSN	@hotmail.com	Allow	 
MSN	@hotmail.com	Allow	 
MSN	@hotmail.co.jp	Allow	 
Yahoo!	ma	Allow	 

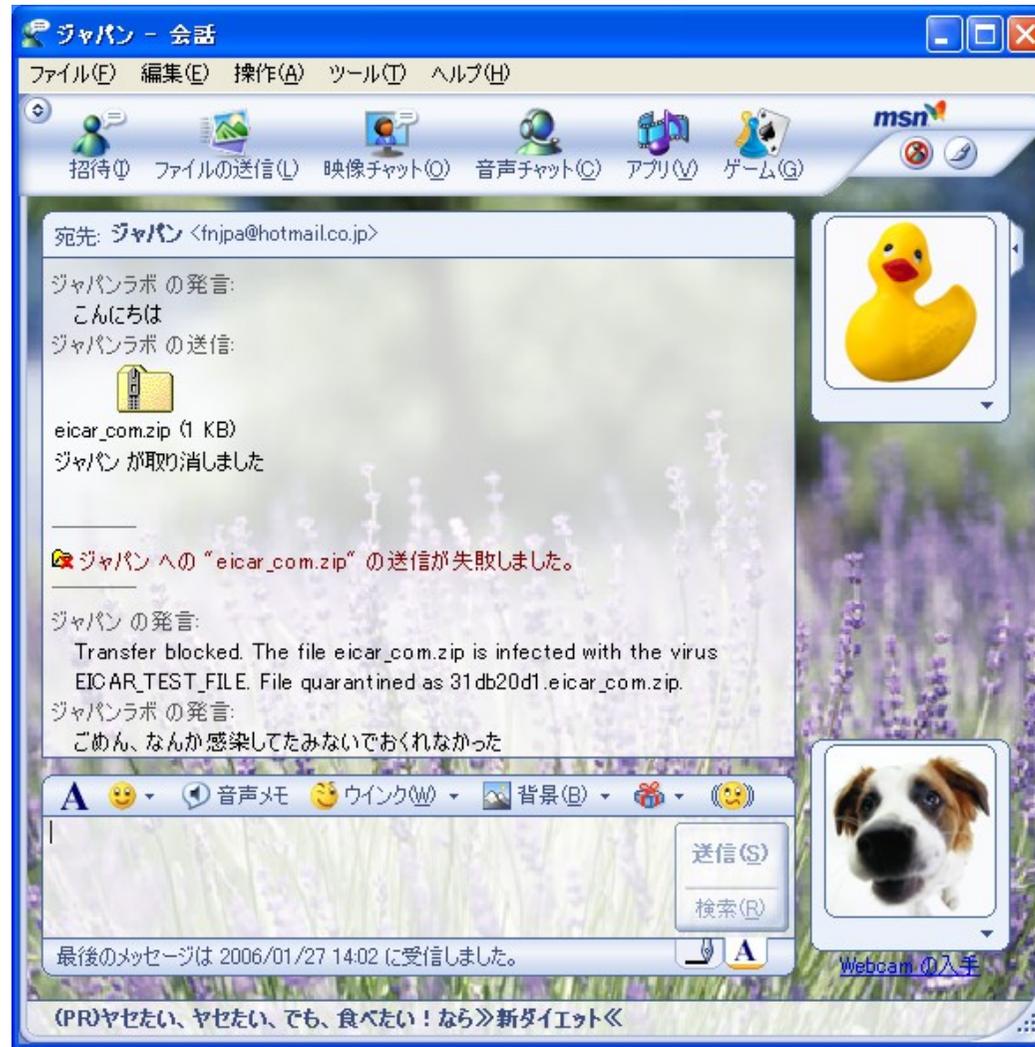
チャット内容のアーカイブが可能

※FortiAnalyzerとの連携機能

▼ コンテンツアーカイブ

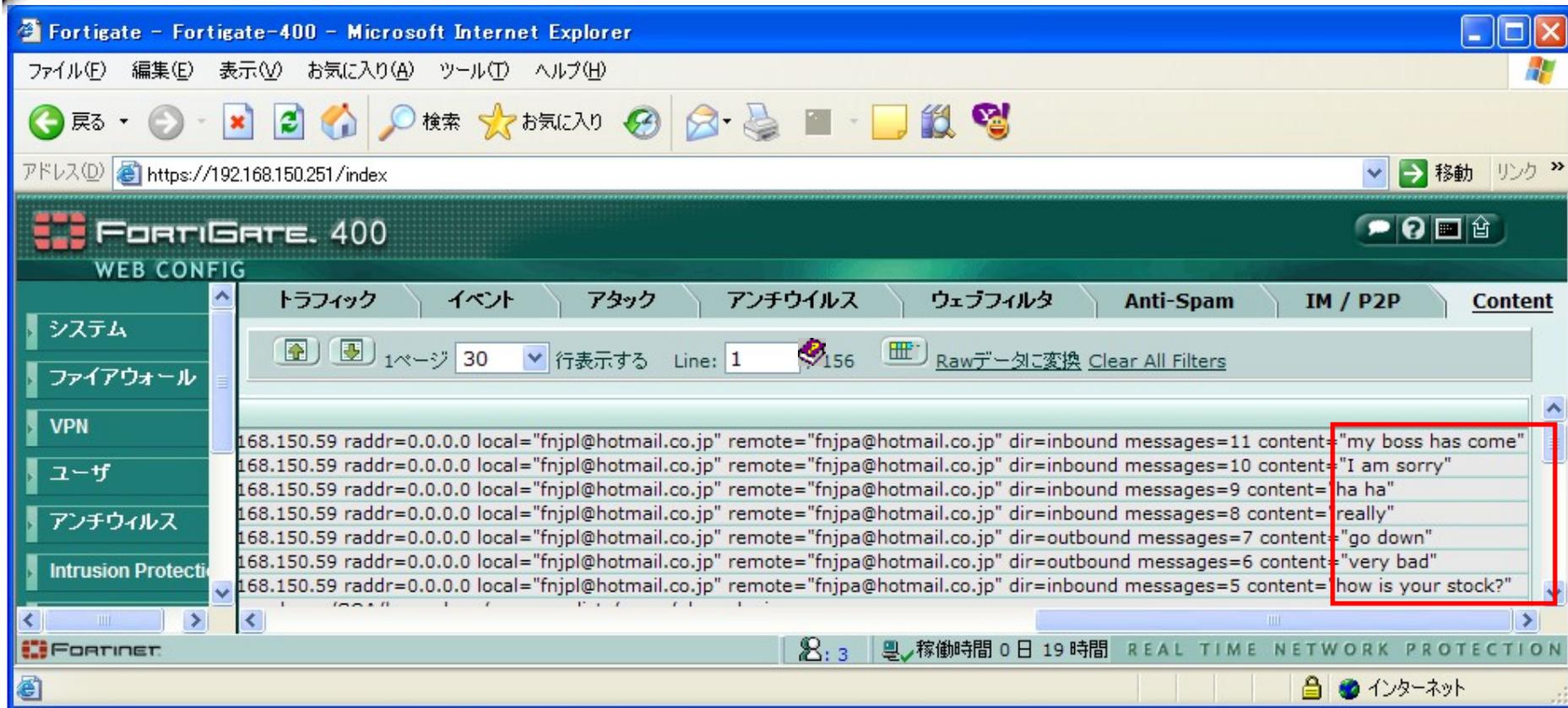
	AIM	ICQ	MSN	Yahoo!
IMのサマリ情報をFortiAnalyzerにアーカイブする	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IMの完全なチャット情報をFortiAnalyzerにアーカイブする	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

IMのファイル転送をウイルススキャン可能



IMのメッセージのアーカイブが可能

※FortiAnalyzerとの連携機能



アーカイブの主な理由:個人情報保護法に伴う内部機密情報漏洩
日本版SOX法などへのコンプライアンス(法令順守/内部統制)対応
過度の業務外利用の抑止力として

FORTINET

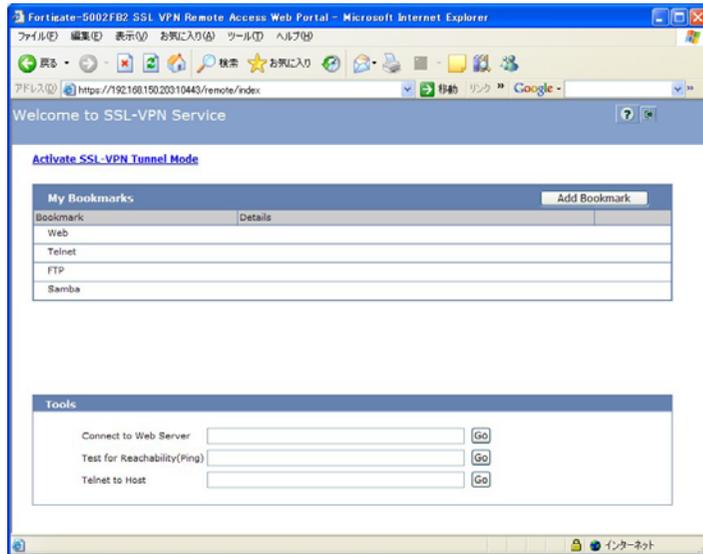
Stateful Firewall • Antivirus • Spyware Protection • Intrusion Prevention • IPSec Virtual Private Network • Web Content Filtering • Antispam • Bandwidth Shaping

FOS3.0主な新機能

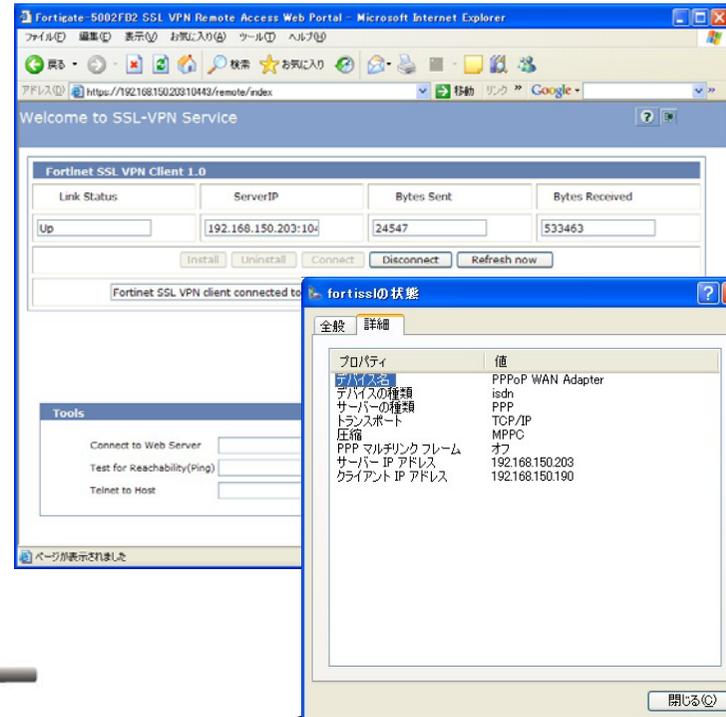
- SSL-VPN
- VDOM拡張
- ADシングルサインオン
- FortiAnalyzer ブラウザ
- FortiAnalyzer 隔離
- USB Disk

SSL-VPNに対応

Webモード

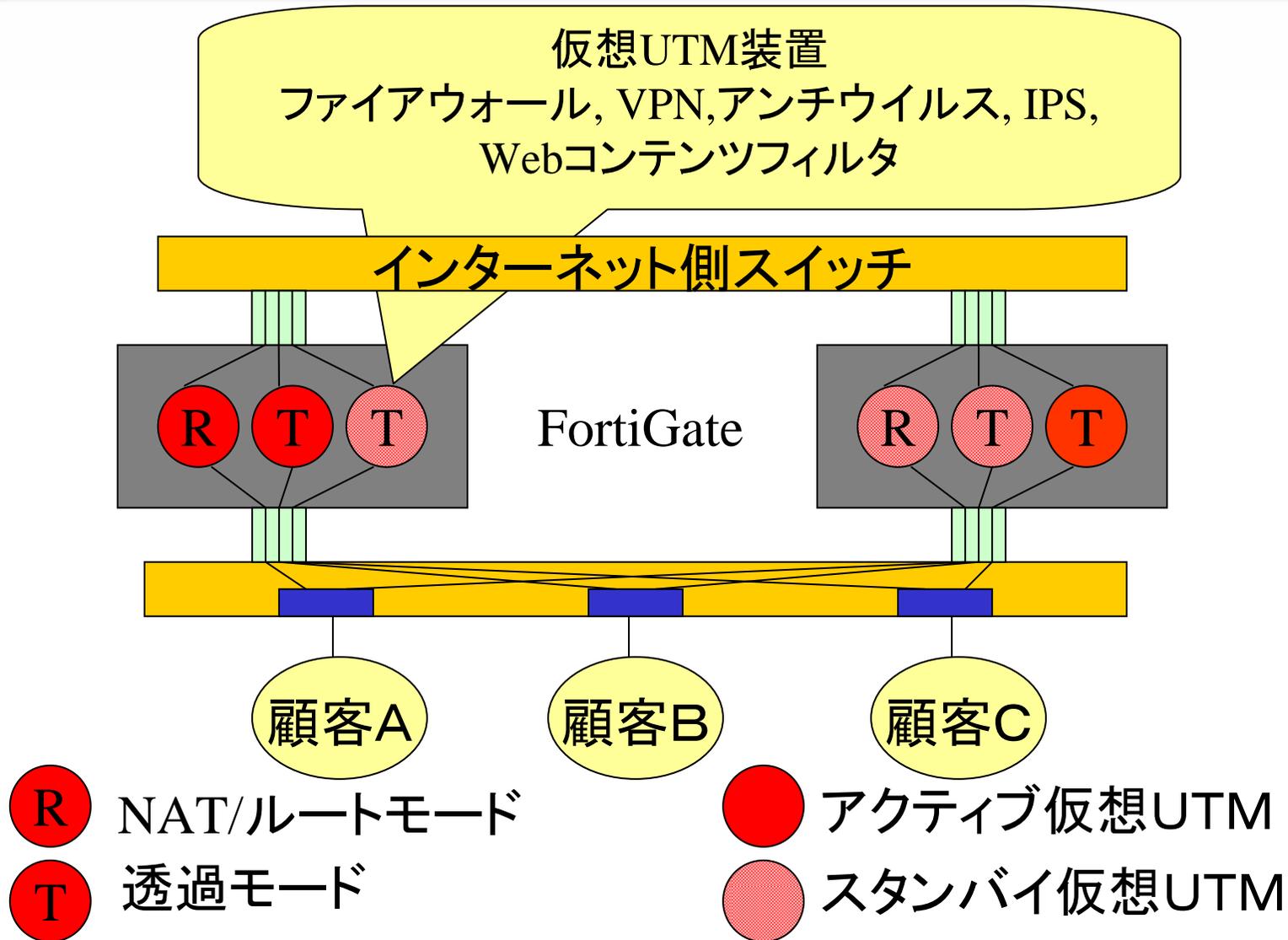


トンネルモード



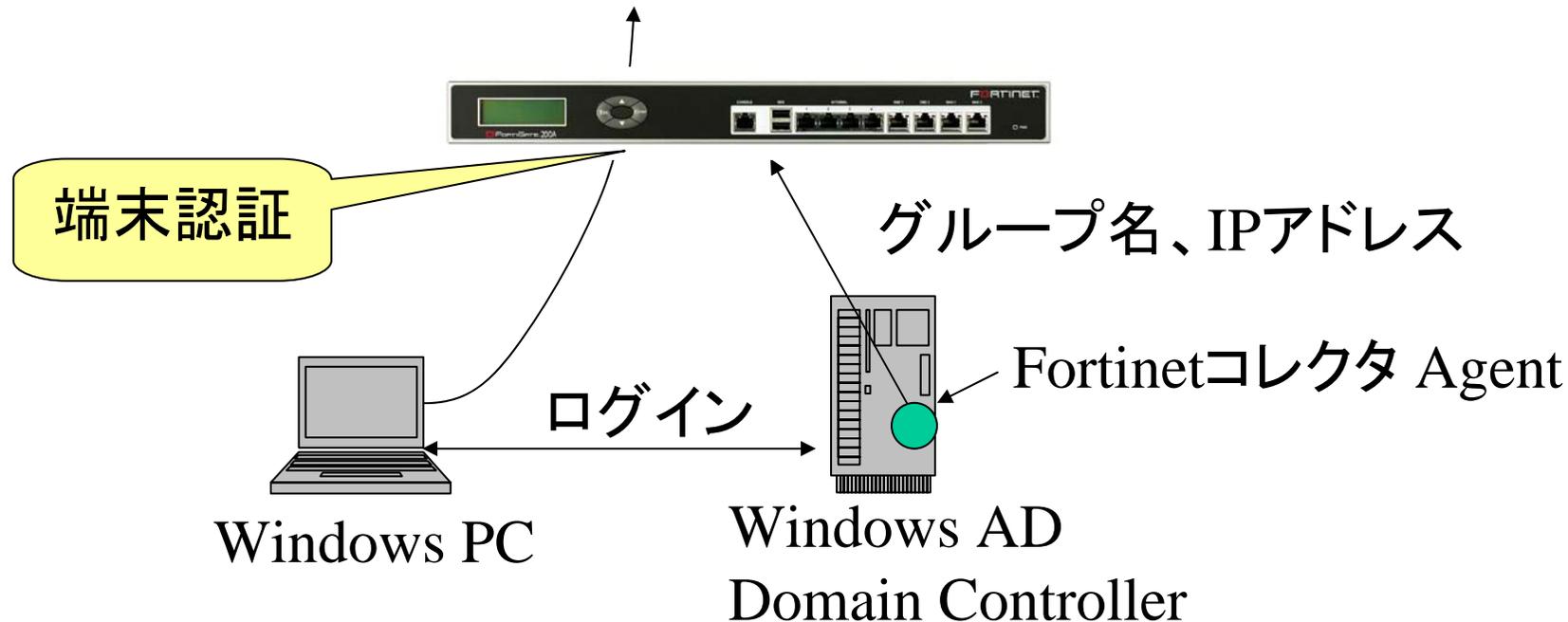
FORTINET

バーチャルドメイン拡張(仮想UTM機能) ~柔軟な設計と有効なリソース活用が実現~

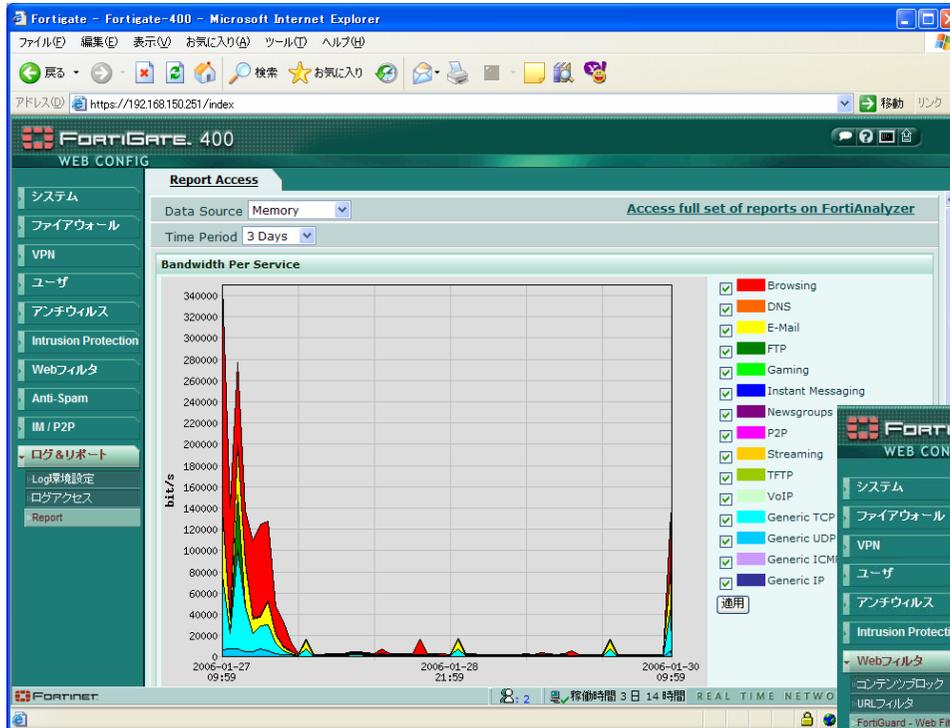


Active Directoryシングルサインオン

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



より詳細なレポート機能を実現



グラフィカルなアプリケーション
カテゴリ毎の統計グラフ

The screenshot shows the FortiGate 400 Web Config interface with the 'Report' window open. A 3D pie chart is displayed, showing the distribution of categories. Below the chart is a table with columns: カテゴリ (Category), 許可 (Allow), ブロック (Block), Logged, and Overridden. The table lists various categories and their corresponding counts.

カテゴリ	許可	ブロック	Logged	Overridden
違法性/犯罪性が高い	34	0	34	
カルト/オカルト	23	0	23	
ハッキング/不正アクセス	1	0	1	
違法・脱法行為/犯罪情報	7	0	7	
サイト翻訳	3	0	3	
コンテンツブロック	6106	0	6007	
アダルト商品/サービス	899	0	899	
おしらせ/ノード	14	0	14	
ポルノ	74	0	68	
広告	5041	0	4966	
ウェブチャット	78	0	60	
生産性低下	6165	0	6085	
オンラインローカー/株取引	1175	0	1172	
フリーウェアダウンロード	386	0	349	
ゲーム	399	0	397	
インスタントメッセージ	464	0	430	
ニュースグループ/伝言板	3470	0	3466	

Webコンテンツフィルタ結果を表示

FortiAnalyzerとの連携

FortiAnalyzerとの
連携
より詳細なレポート
機能を提供

The screenshot displays the FortiAnalyzer web interface. On the left, a sidebar menu includes 'システム', 'ファイアウォール', 'VPN', 'ユーザ', 'アンチウイルス', 'Intrusion Protection', 'Webフィルタ', 'Anti-Spam', 'IM / P2P', 'ログ&レポート', 'Log環境設定', 'ログアクセス', and 'Report'. The main area is titled 'WEB CONFIG' and shows 'Report Access' configuration with 'Data Source' set to 'FortiAnalyzer'. A table lists report files, with 'WebFilter Activity.html' highlighted in yellow. A red arrow points from this file to a pie chart titled 'Web Traffic by Top URLs' in a separate browser window. The pie chart shows the following data:

URL	Percentage
www.download.windowsupdate.com/msdownload/update/v3...	~45%
210.51.190.166210.51.190.166:80/fdsupdate	~15%
ftp.netscape.com/pub/netscape8/english..	~10%
download.windowsupdate.com/microsoftupdate/v6/wsusscan/w	~5%
kc.forticare.com/tmp...	~5%
au.download.windowsupdate.com/msdownload/update/v3...	~5%
Other(1688)	~15%

FortiAnalyzerとの連携

- コンテンツアーカイブ
- 隔離ファイル保存

Webブラウザサイト、メール内容、IMチャット内容

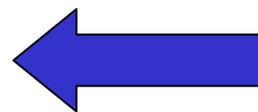


ディスクレス

ログ
コンテンツアーカイブ
隔離ファイル



RAID 5



レポート表示
アーカイブ内容表示

USBディスクへのバックアップ・リストア

- FortiUSBへの設定バックアップ、リストア
- FortiUSBからのファームウェア、設定復旧



FortiUSB

FortiUSBで簡単にファイアウォール、VPN、アンチウイルス、IP S、Webコンテンツフィルタ等全UTM機能を簡単に復旧

ありがとうございました。