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

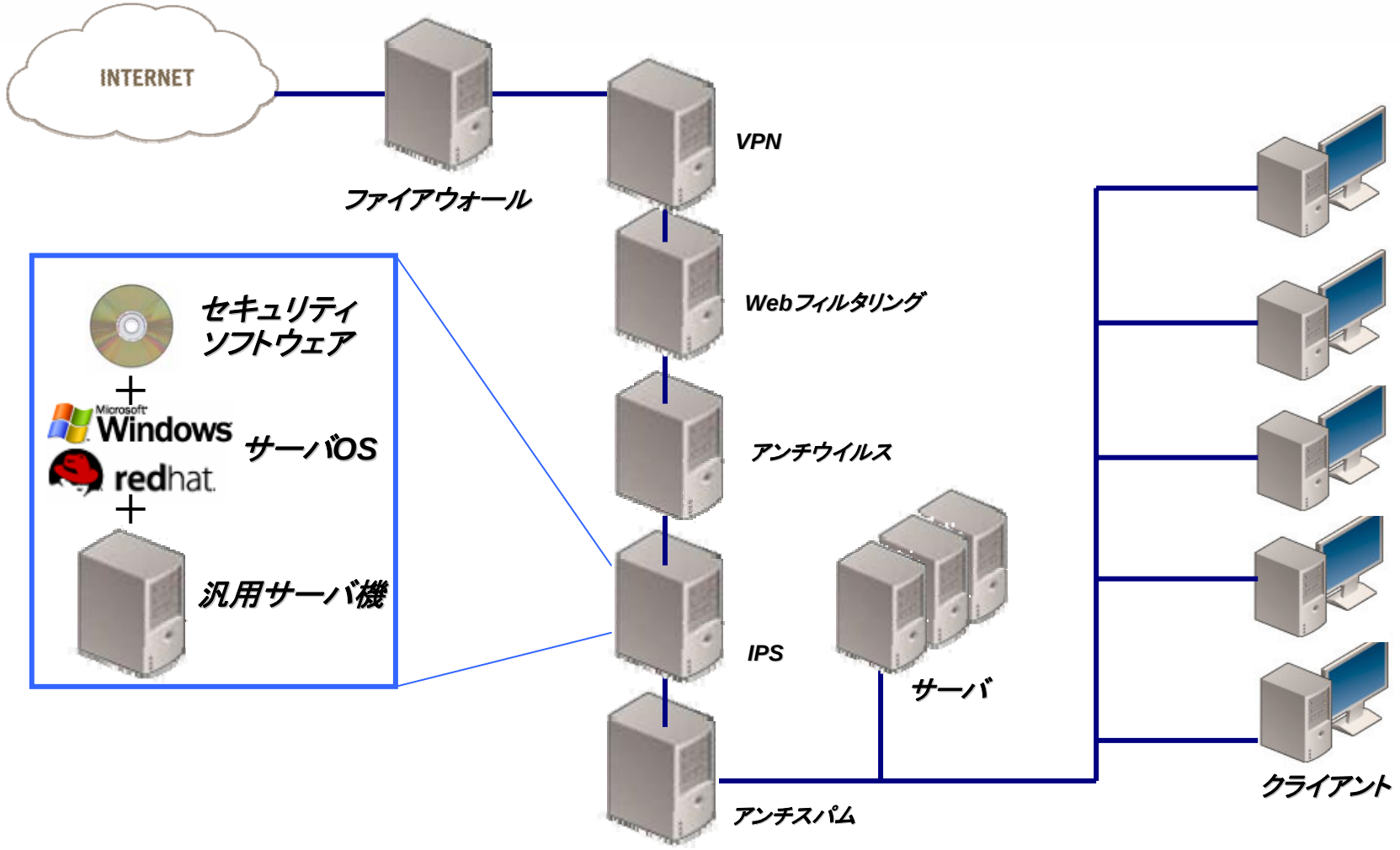
脅威	有効な対策					
	ファイアウォール	IPS	Webアンチウイルス	Webコンテンツフィルタリング	メールアンチウイルス	アンチスパム
スパイウェア		○	○	○		
ボットネット		○	○	○		
トロイの木馬		○	○	○		
フィッシング				○		○
情報漏えい				○		○
マスメール型ウイルス				○	○	○
Web型ウイルス			○	○		
DoS攻撃	○	○				
スパムメール						○
P2Pソフト		○				

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?

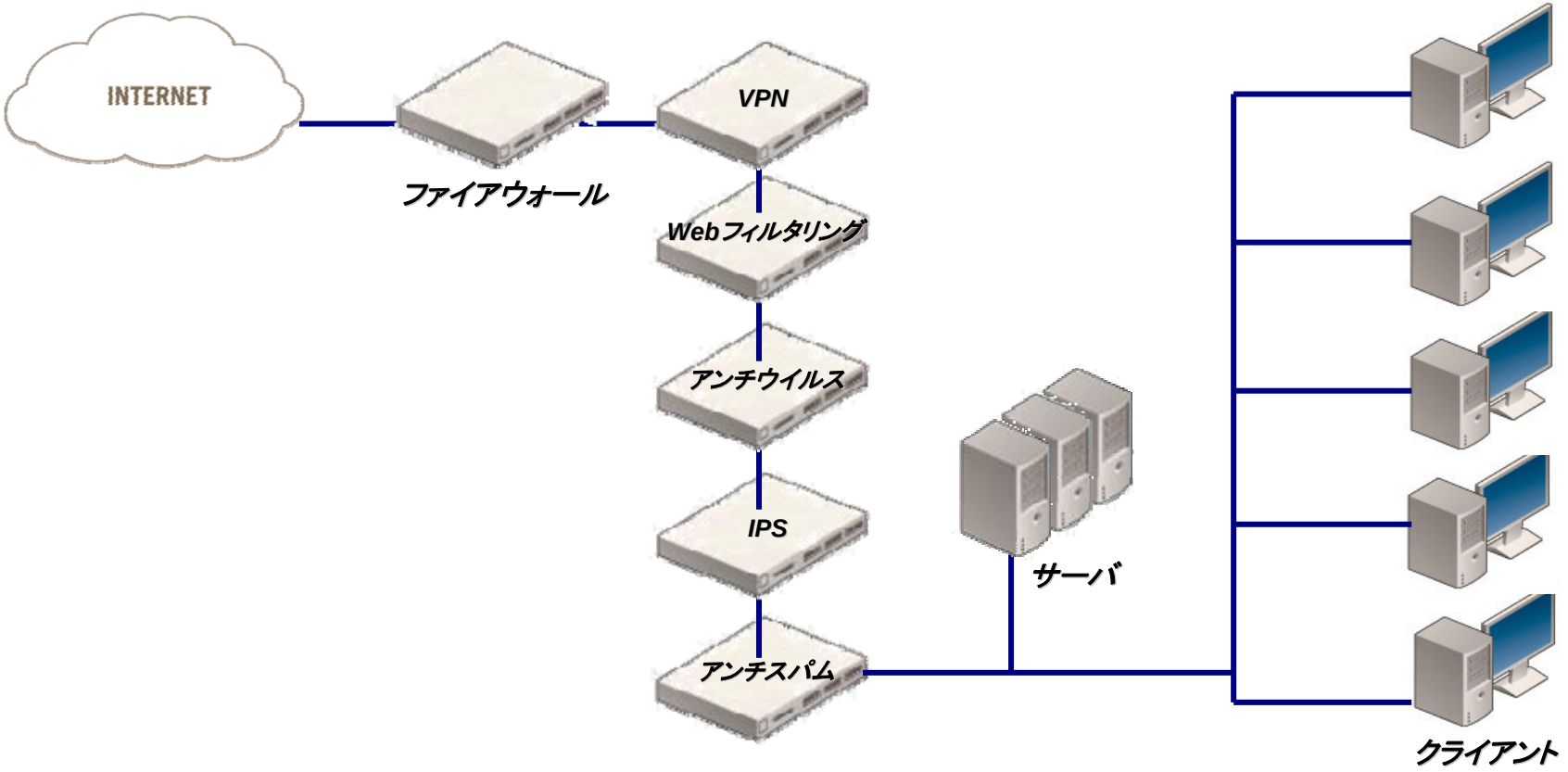
FortiGate以外の方法①
～セキュリティソフトウェアで構築～

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

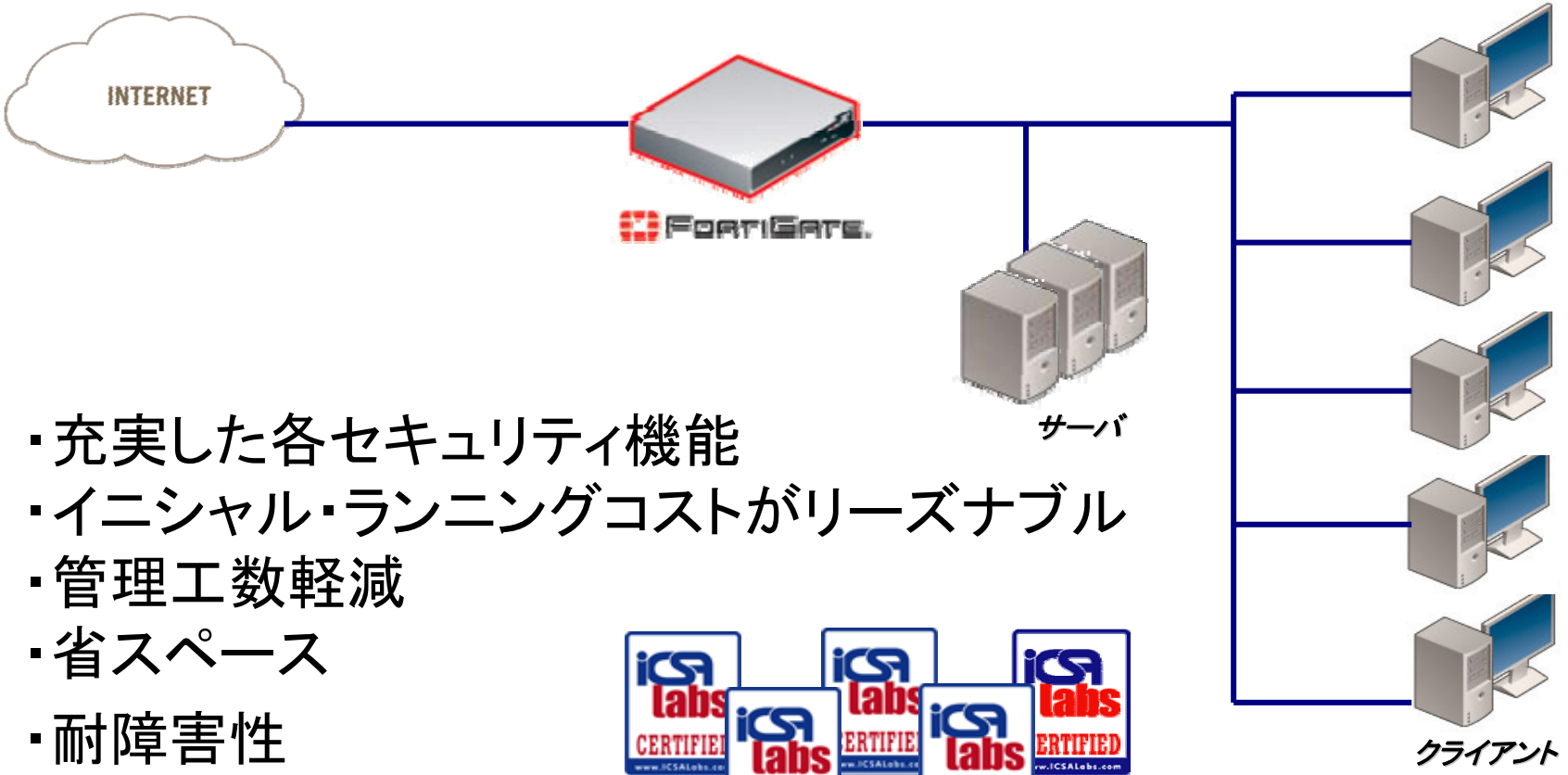


FortiGate以外の方法②
～単機能アプライアンスで構築～

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

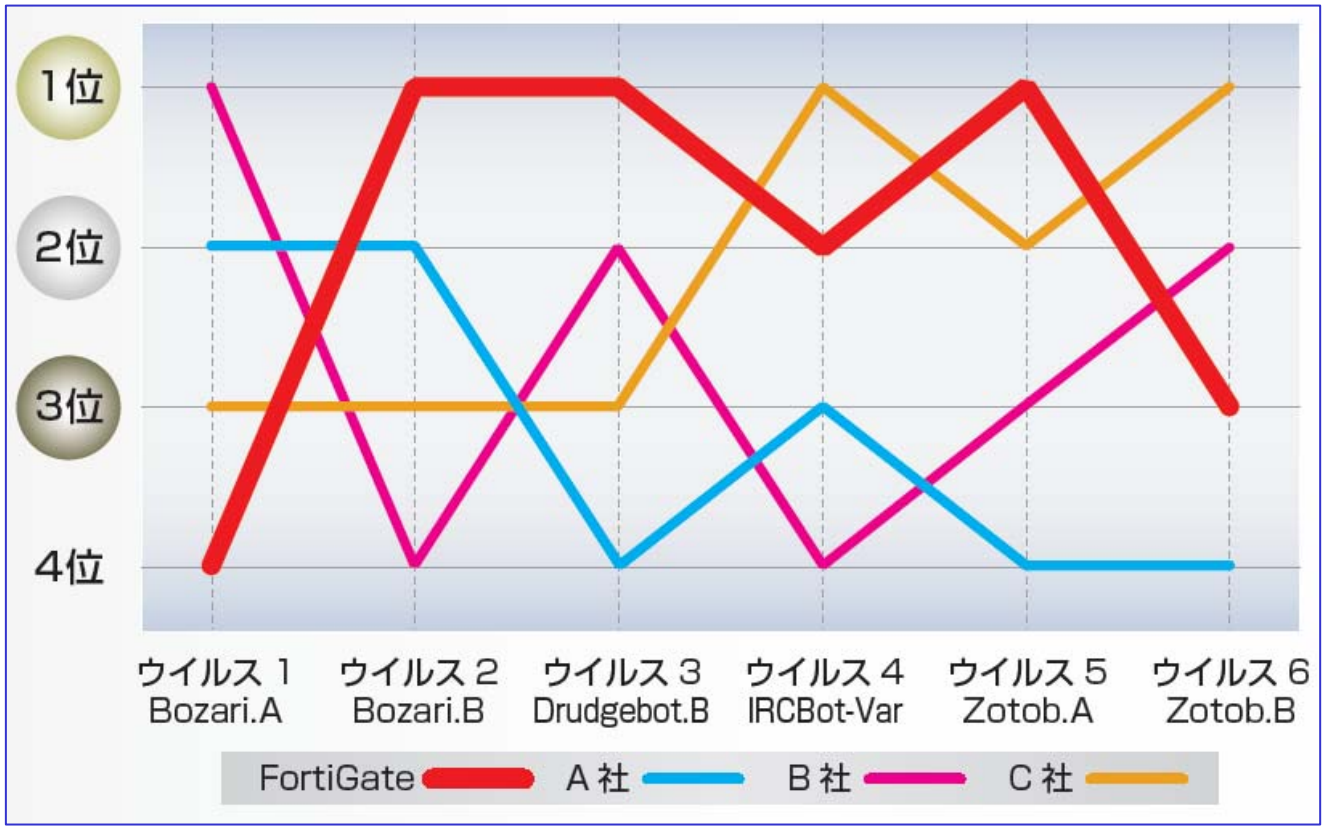


- 充実した各セキュリティ機能
- イニシャル・ランニングコストがリーズナブル
- 管理工数軽減
- 省スペース
- 耐障害性

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)

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)

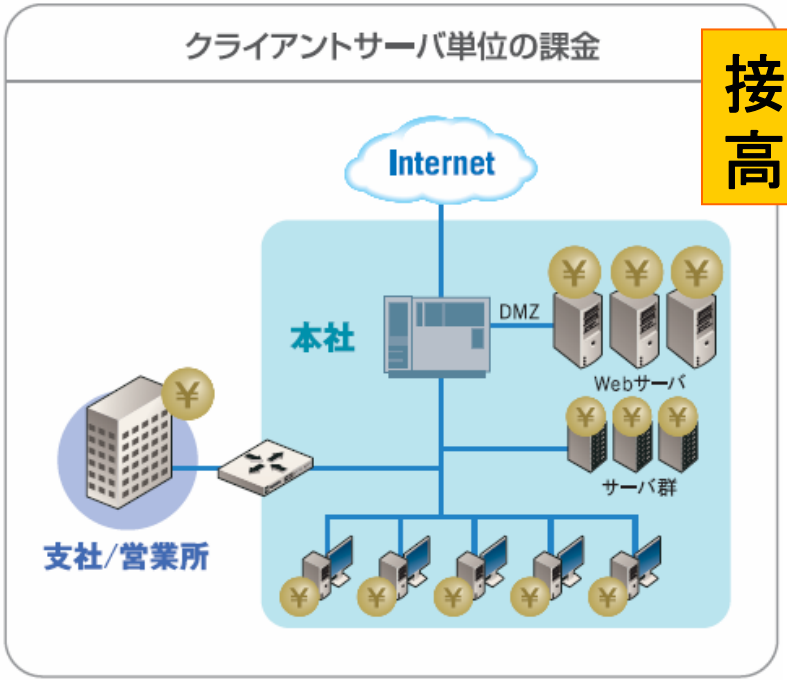
ヒューリスティックにウイルスを検出できたのは、FortiGateだけ！

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。

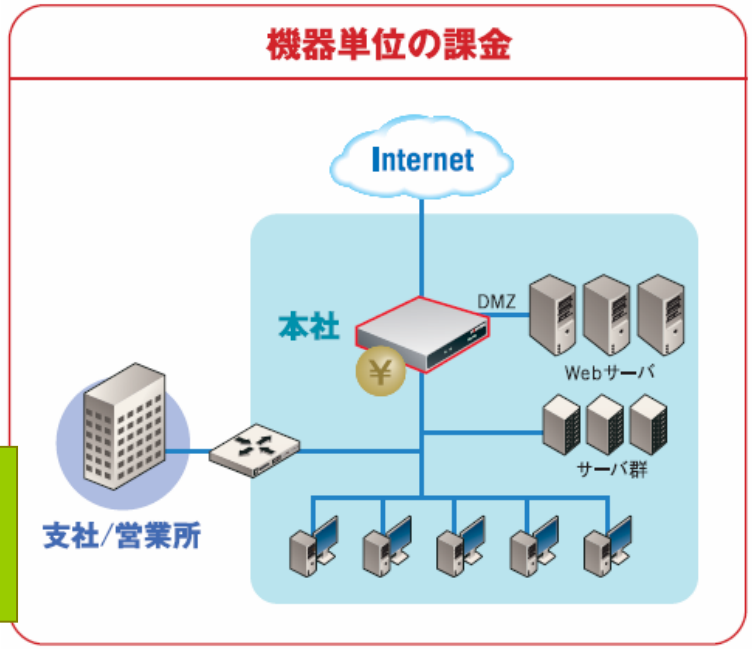
	ウイルス 1 Bozari.A	ウイルス 2 Bozari.B	ウイルス 3 Drudgebot.B	ウイルス 4 IRCBot-Var	ウイルス 5 Zotob.A	ウイルス 6 Zotob.B
FortiGate	○	○	○	○	○	○
A 社					○	○
B 社						
C 社						

※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



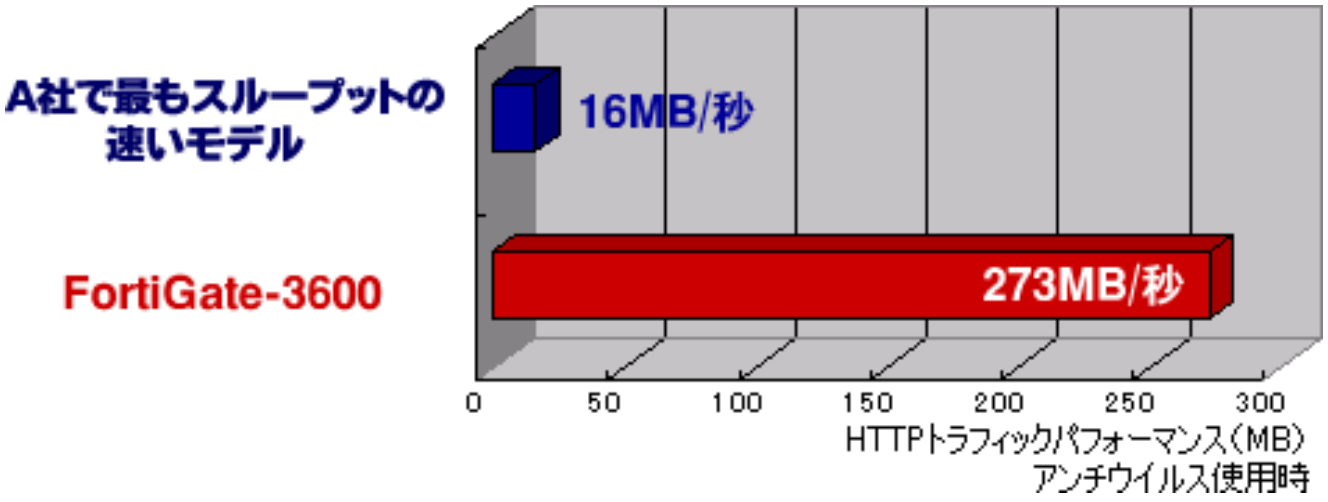
接続機器のカウントが面倒
高額なライセンス



クライアント無制限
手間も無く価格もリーズナブル

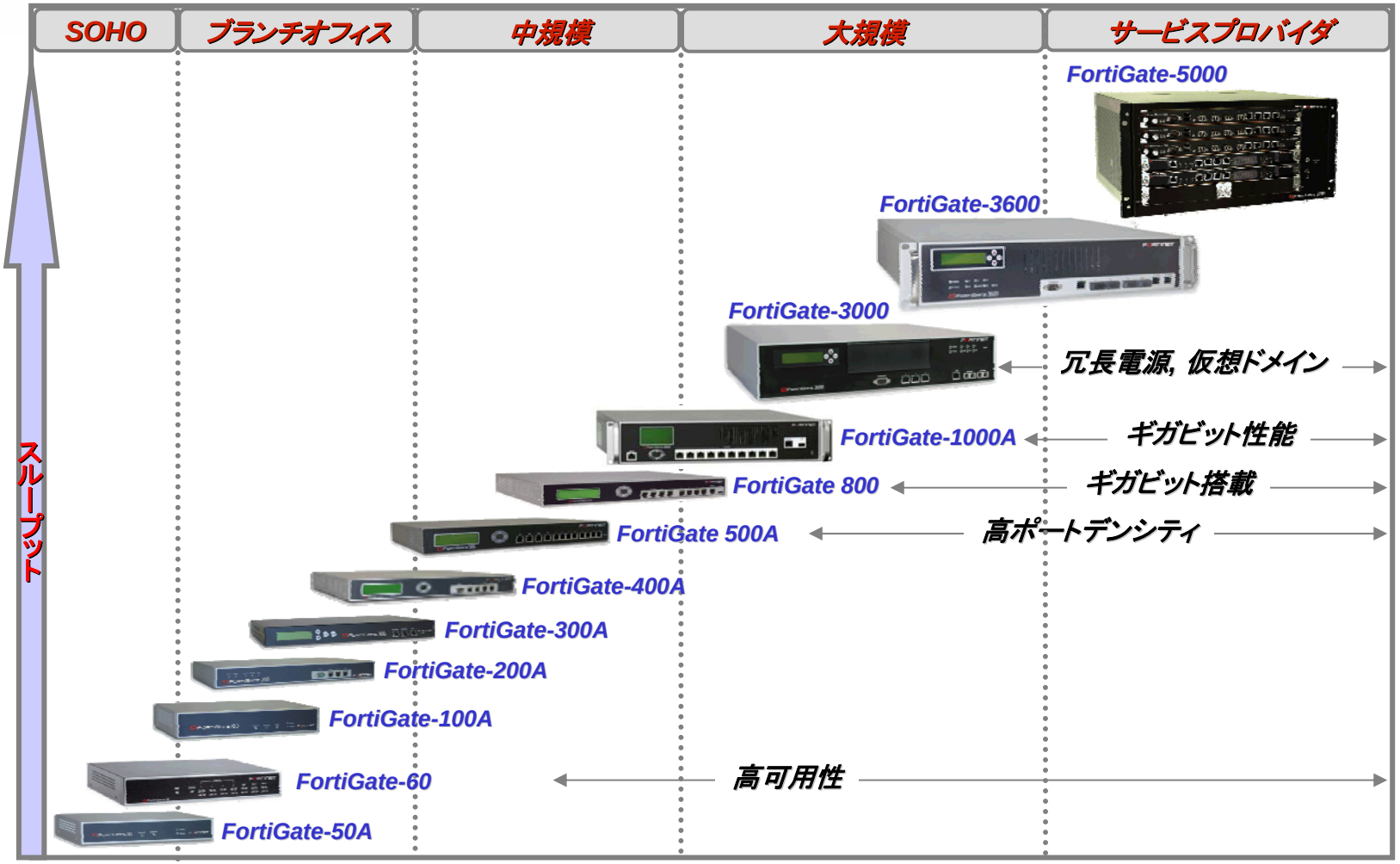
理由その4. ASICによる高速処理

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、驚異的な処理スピードを実現。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）



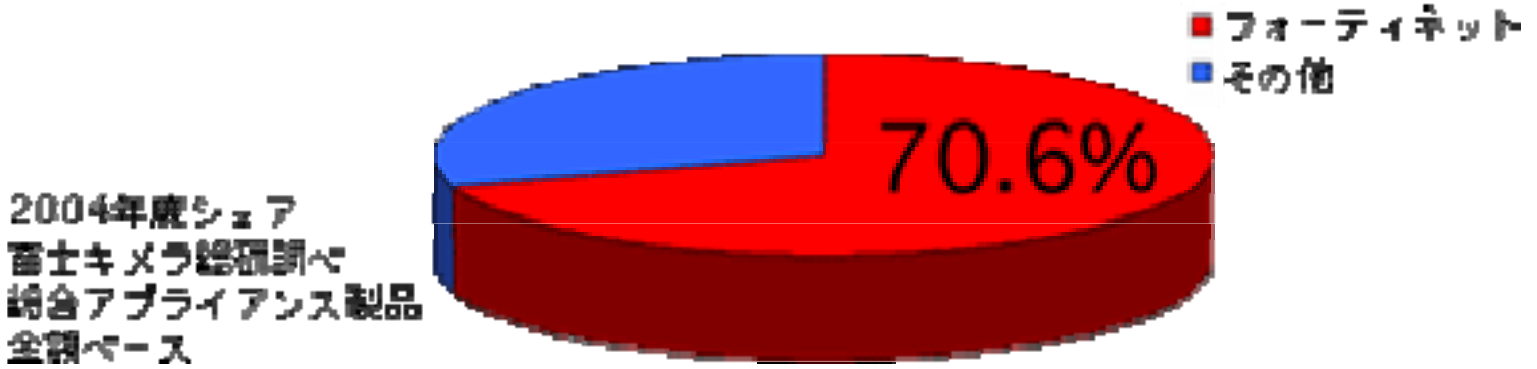
2005年9月現在

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

IDC
Analyze the Future

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

FortiOS3.0による IM/P2Pマネージメント

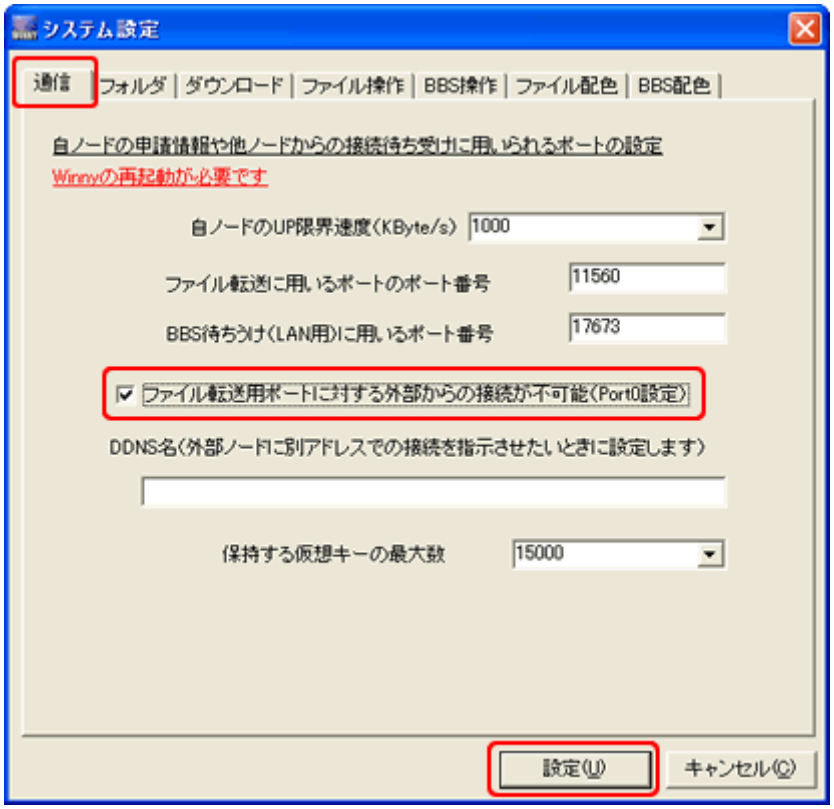
P2Pを止められない環境例

- 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

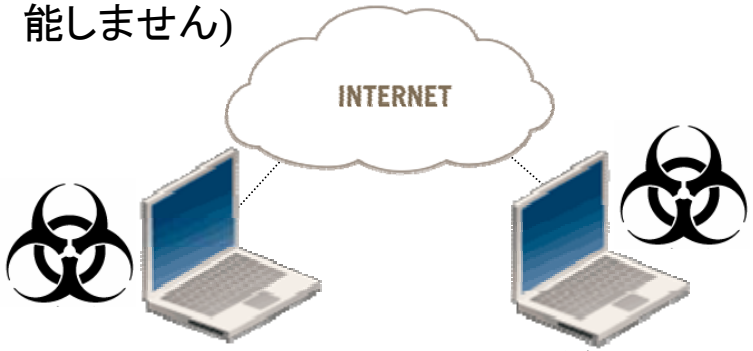


(Winnyの場合)

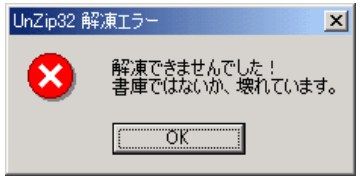
- 任意のポートを使用
- ポートを閉じていても限定的な接続が可能

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～

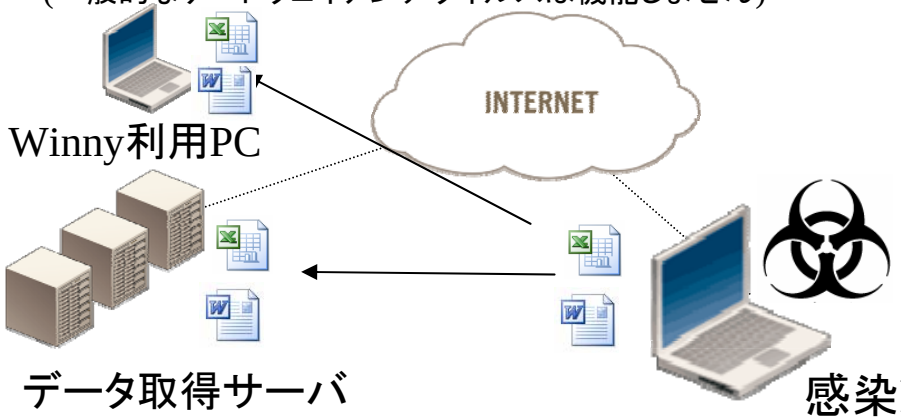
① Winny経由で侵入
(一般的なゲートウェイアンチウイルスは機能しません)



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

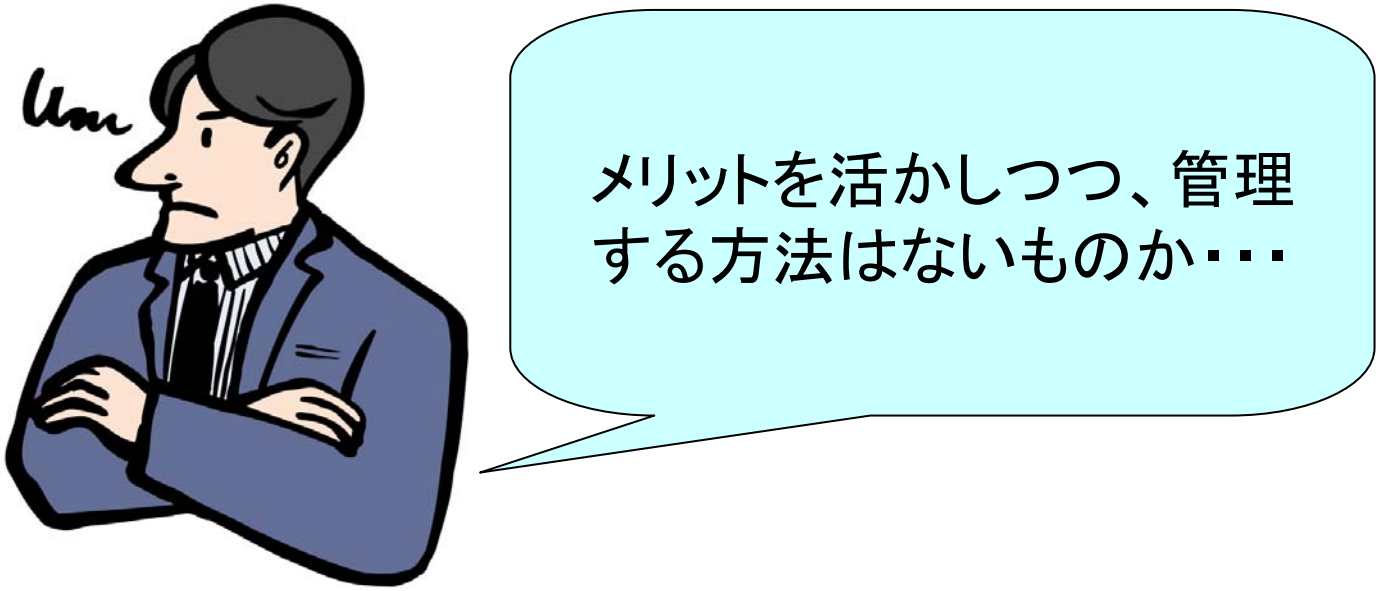
- 生産性低下
- モラル低下
- 情報流出
- ウイルスの新しい侵入経路

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



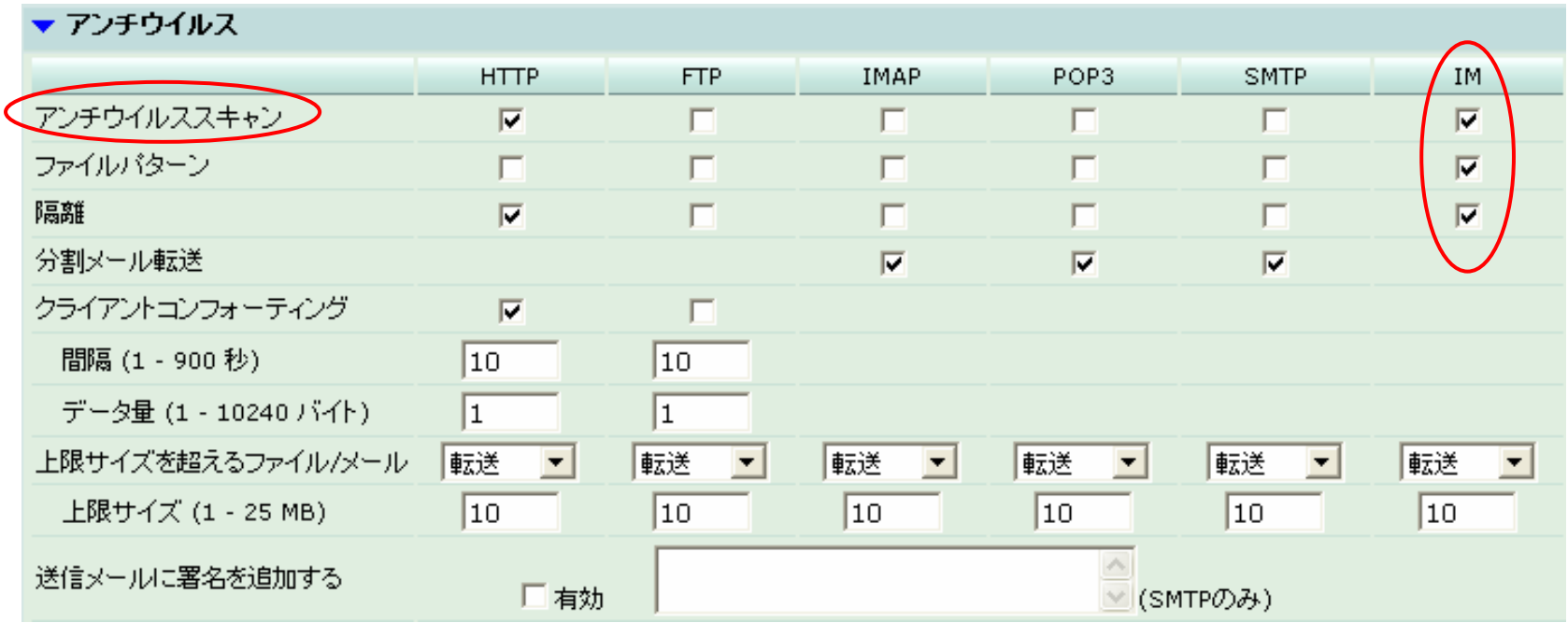
IMに対する新機能

- 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
- ホワイトリスト、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



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

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

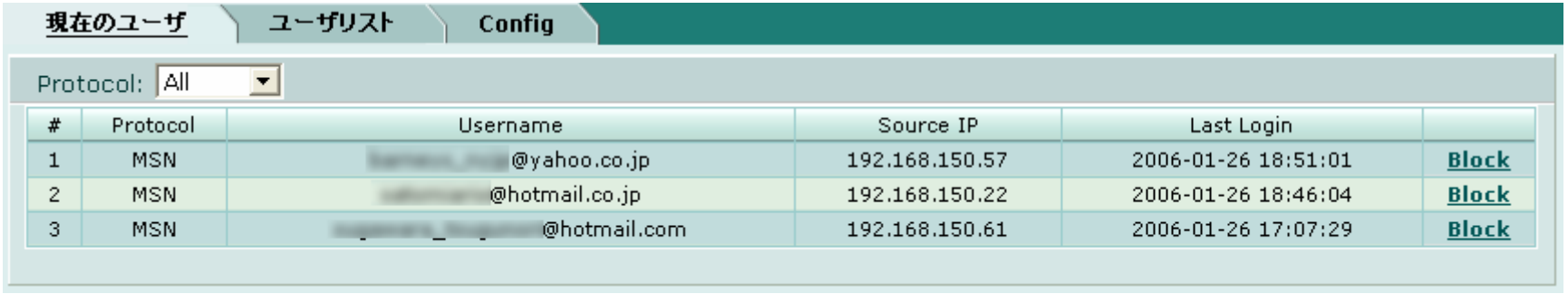
Automatic Refresh Interval 15 seconds　Refresh　Usage Since: 2006-01-19 10:49:13　Reset Stats

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
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

※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



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:

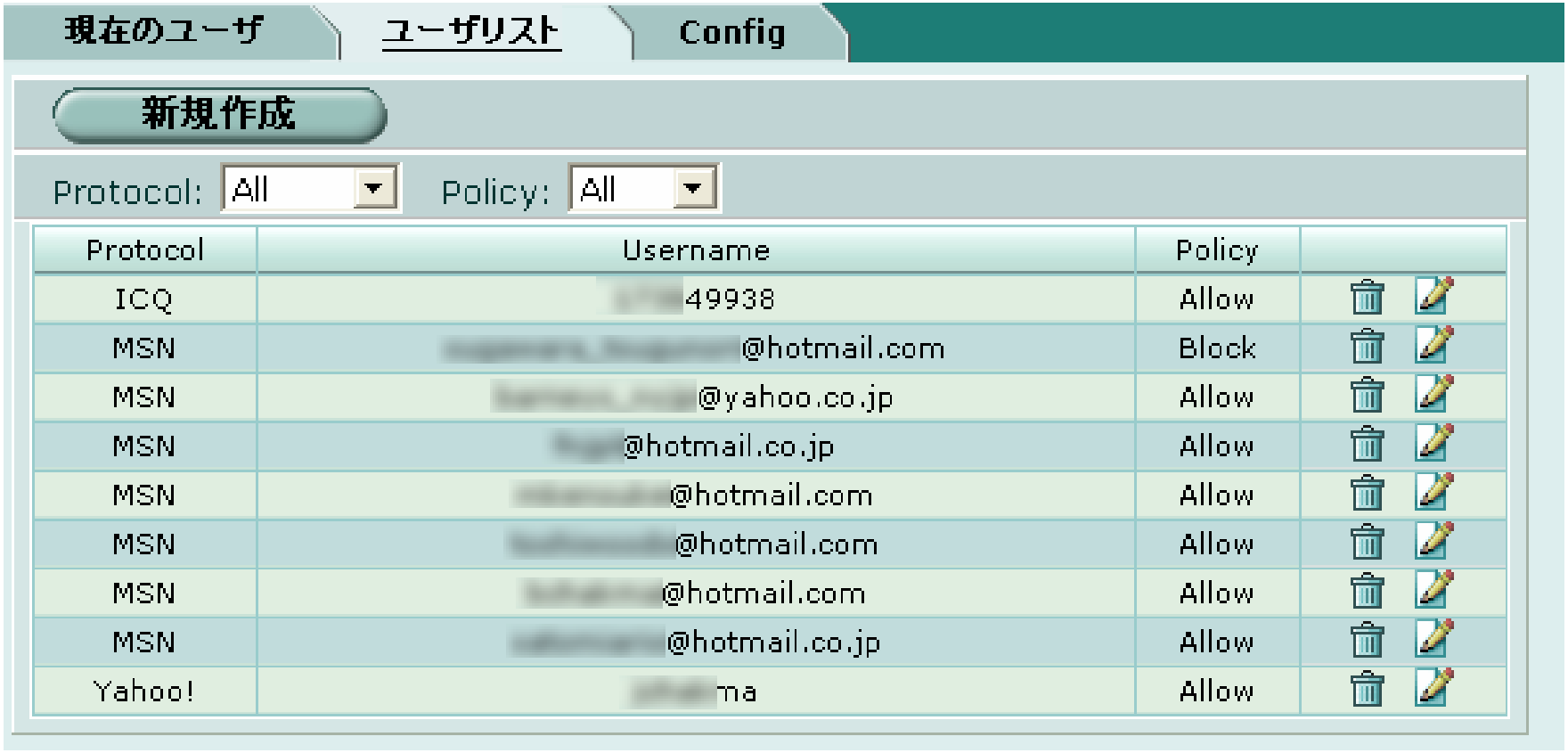
	MSN	Yahoo!	AIM	ICQ
Automatically Allow	◉	◉	◉	◉
Automatically Block	○	○	○	○

List of Temporary Users

Protocol: All

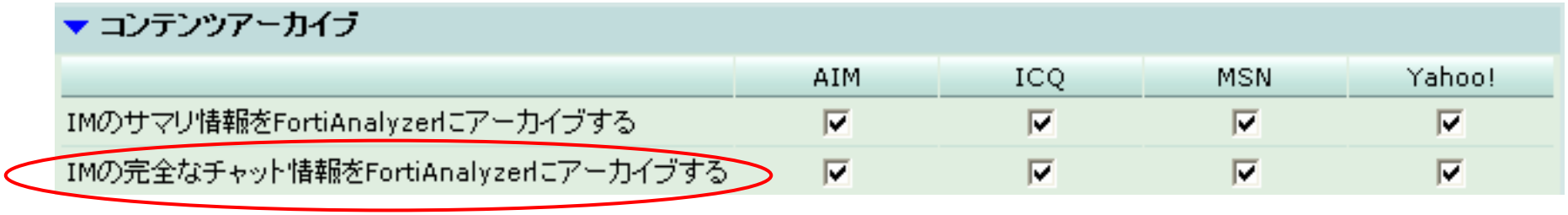
#	Protocol	Username	Policy	
1	Yahoo!	[redacted]kma	Allow	Permanently Allow Permanently Block
2	Yahoo!	[redacted]miya44	Allow	Permanently Allow Permanently Block
3	MSN	[redacted]@hotmail.co.jp	Allow	Permanently Allow Permanently Block
4	MSN	[redacted]@hotmail.com	Allow	Permanently Allow Permanently Block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

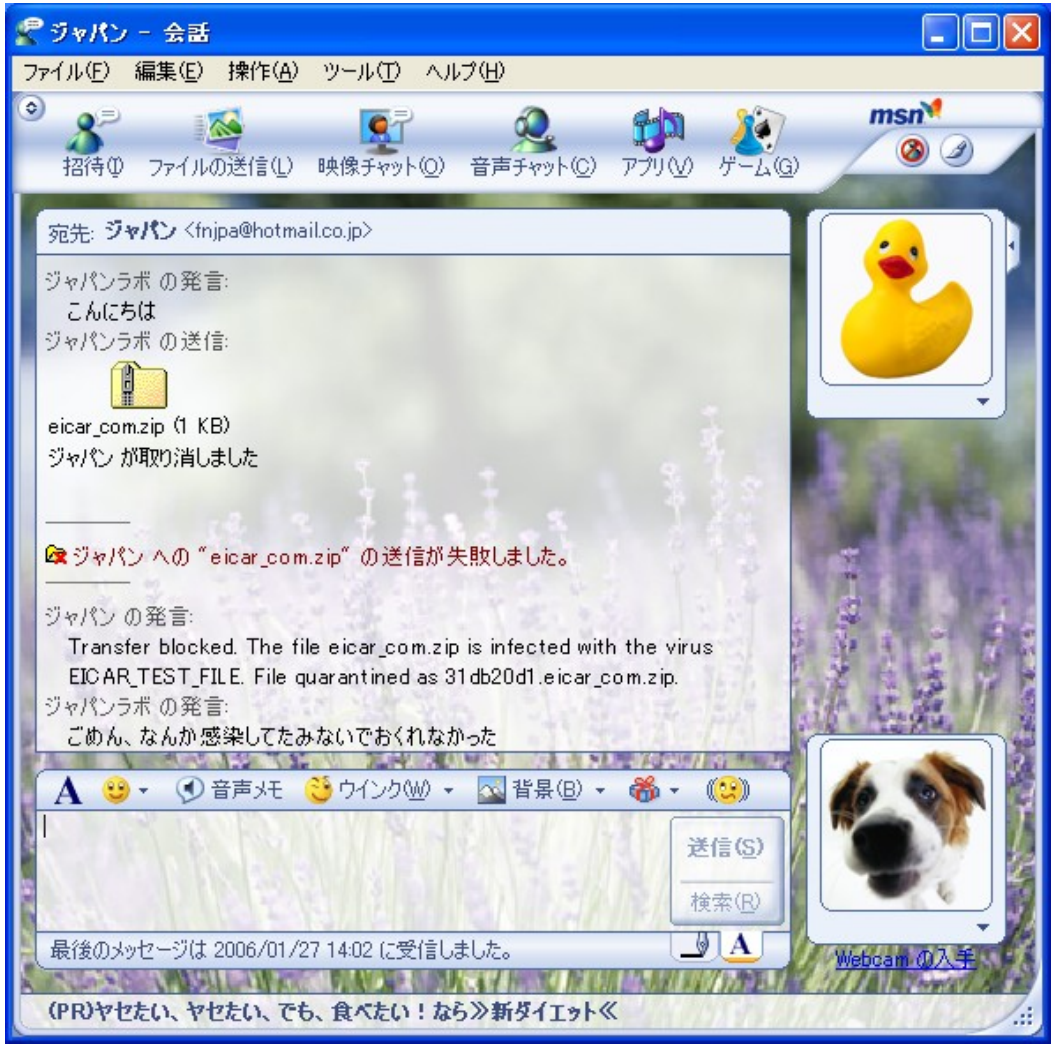


チャット内容のアーカイブが可能

※FortiAnalyzerとの連携機能

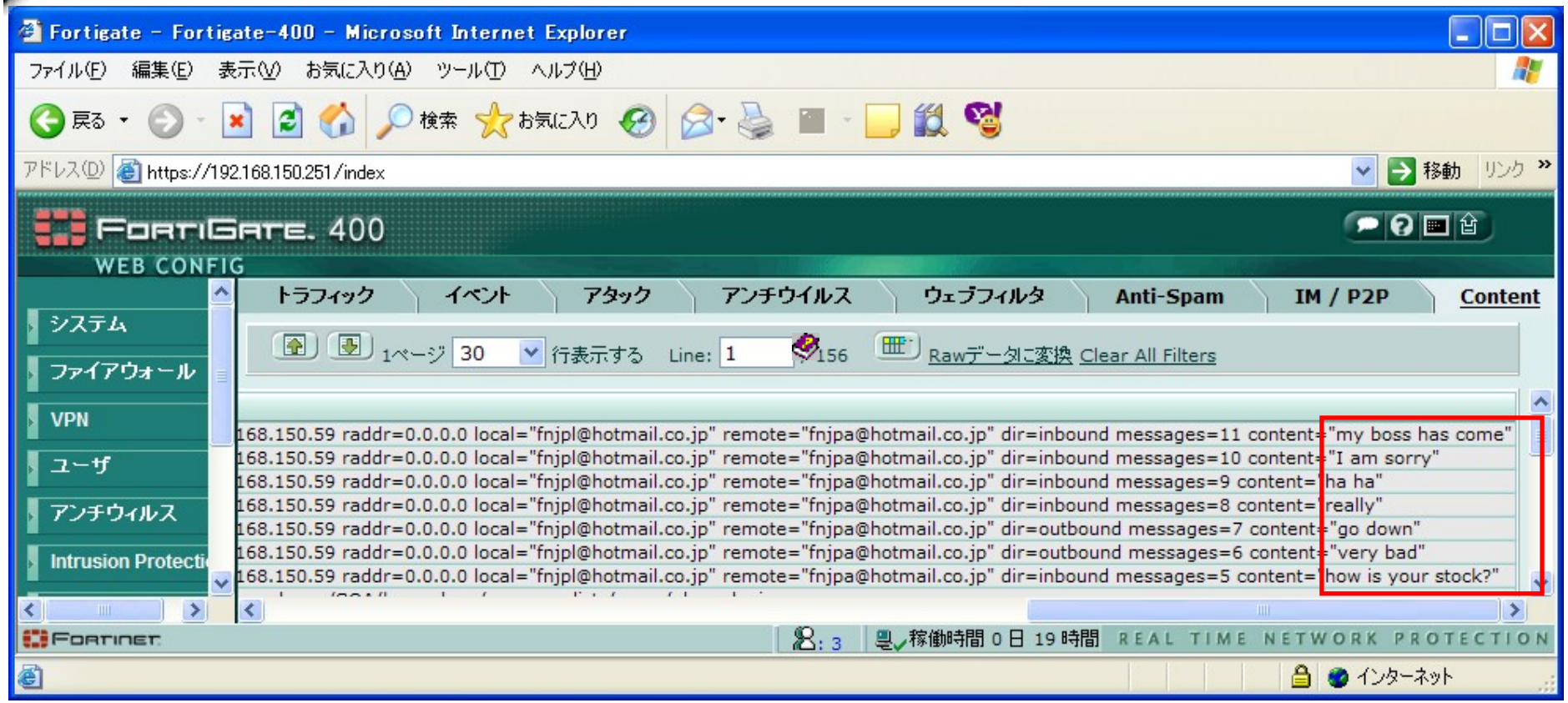


IMのファイル転送をウイルススキャン可能



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™
REAL TIME NETWORK PROTECTION

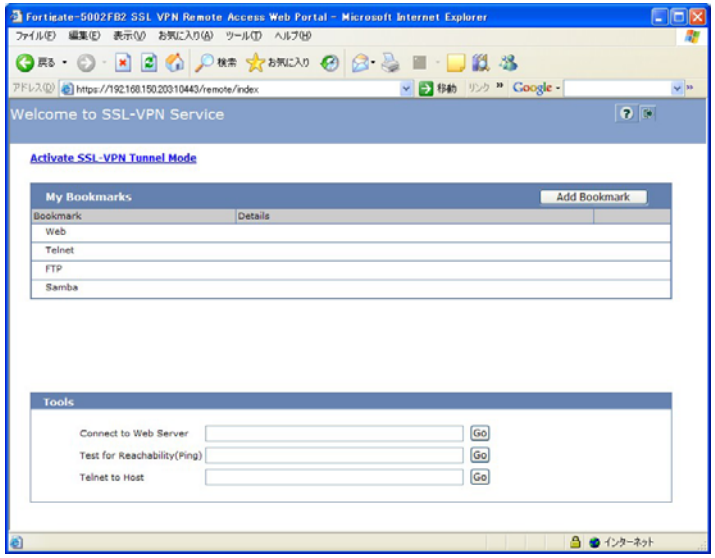
FOS3.0主な新機能

FOS3.0主な新機能

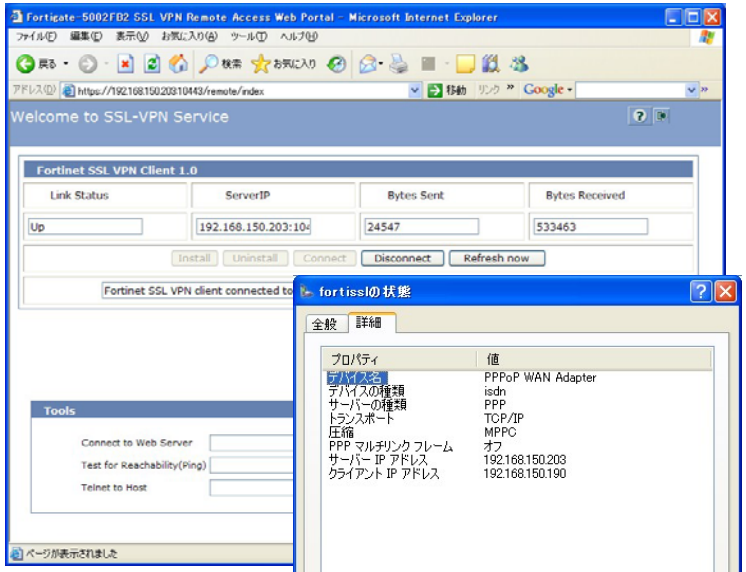
- SSL-VPN
- VDOM拡張
- ADシングルサインオン
- FortiAnalyzer　ブラウザ
- FortiAnalyzer　隔離
- USB Disk

SSL-VPNに対応

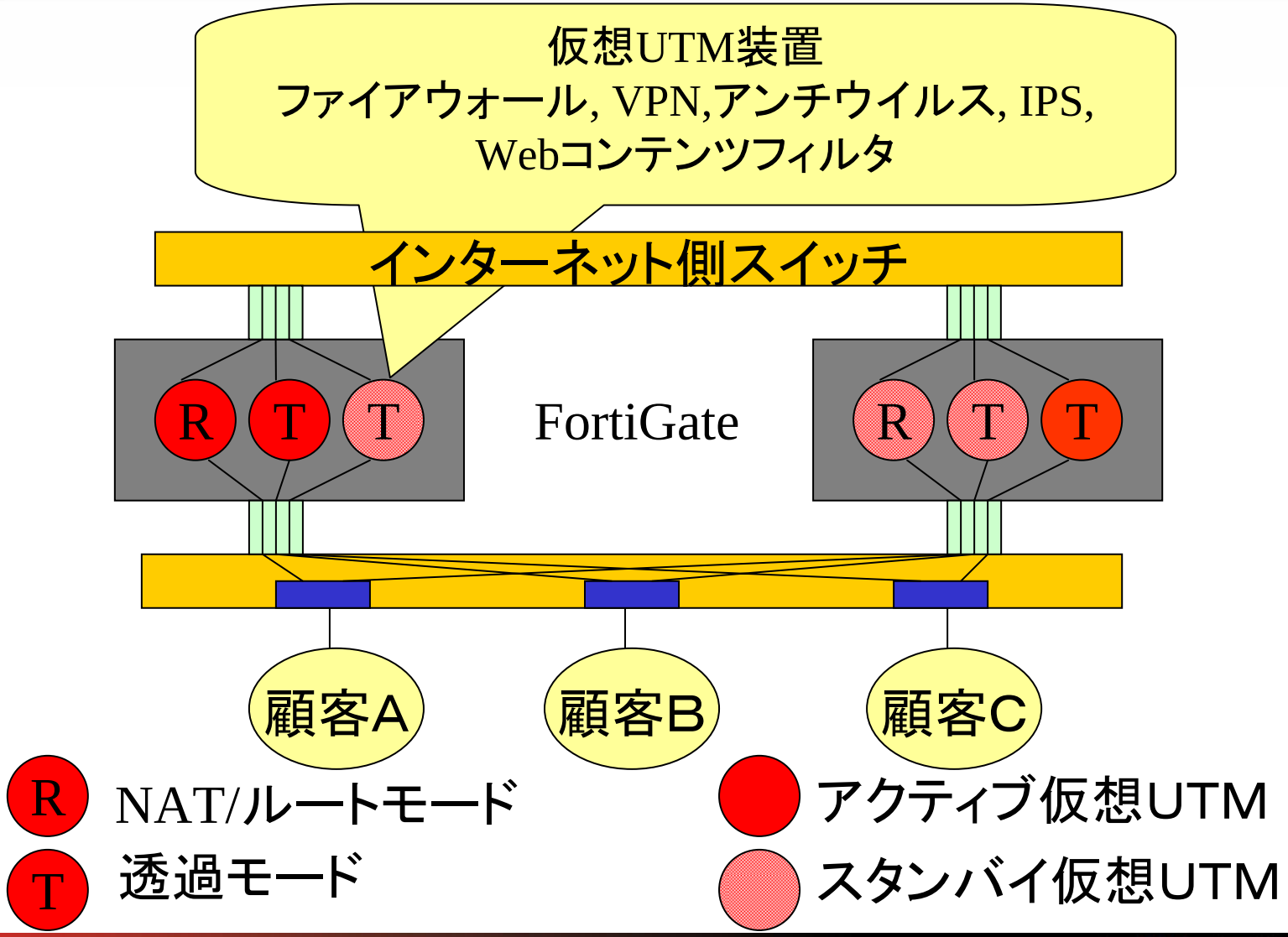
Webモード



トンネルモード

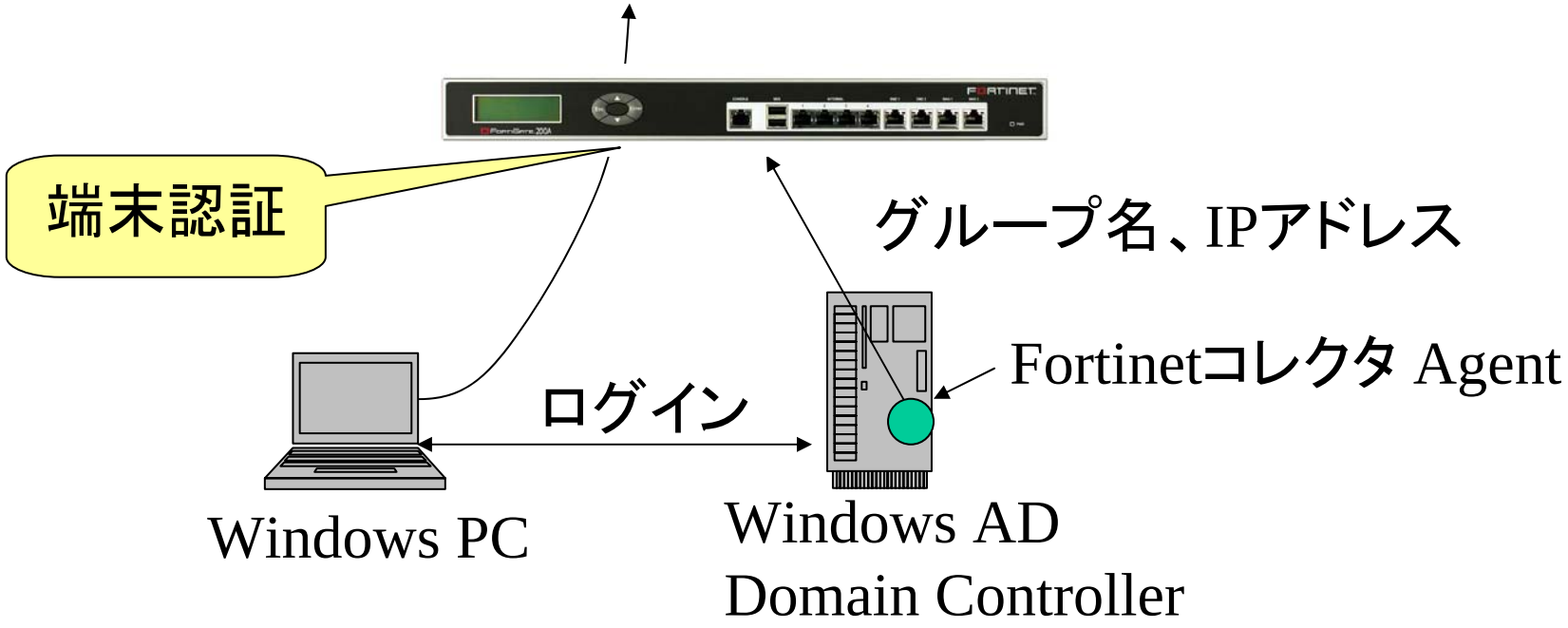


バーチャルドメイン拡張（仮想UTM機能）
～柔軟な設計と有効なリソース活用が実現～

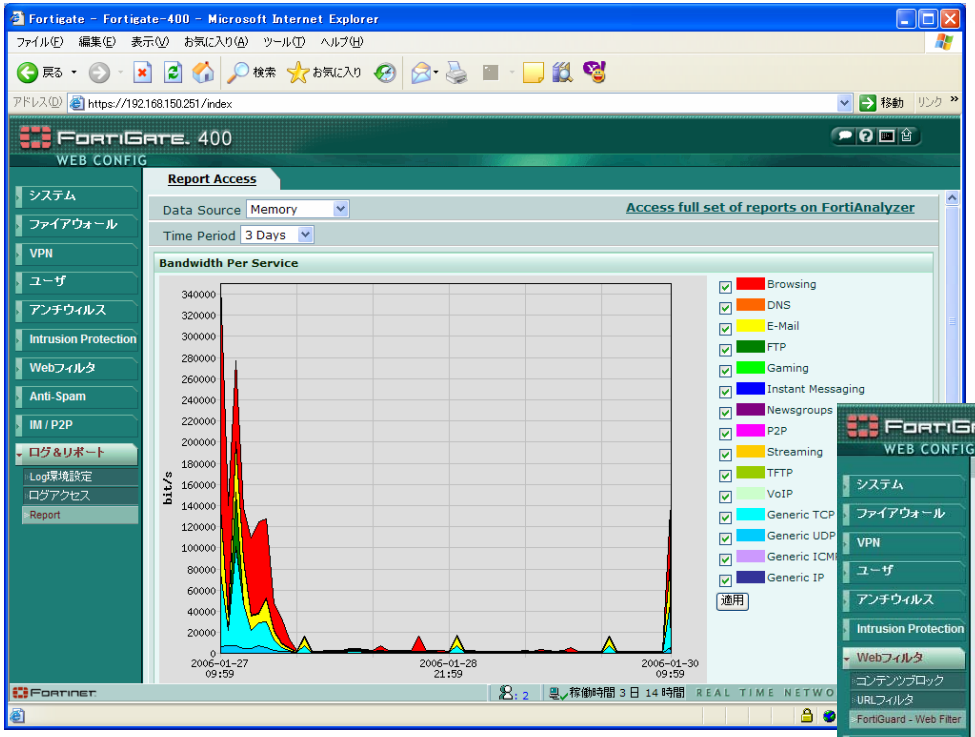


Active Directoryシングルサインオン

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

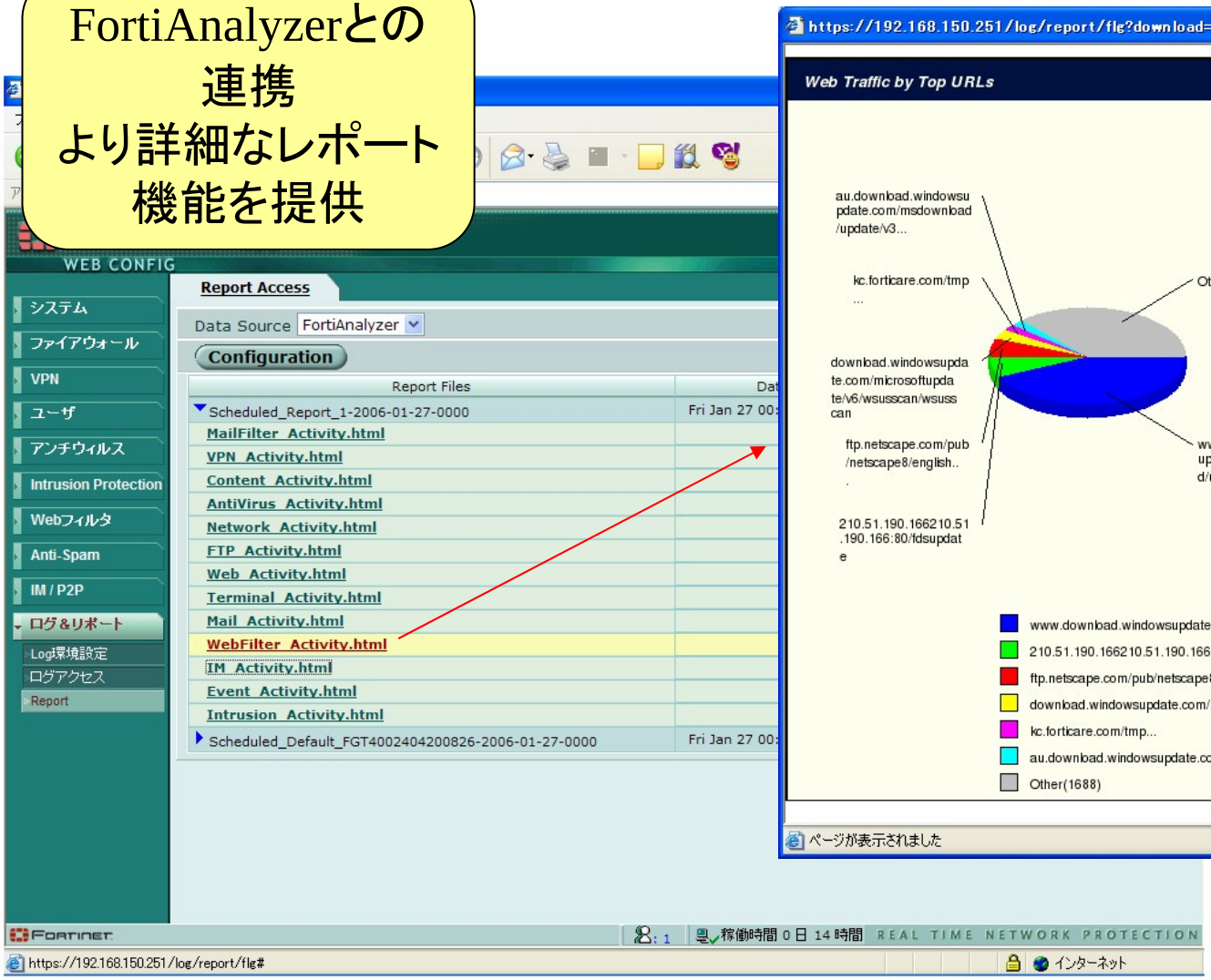


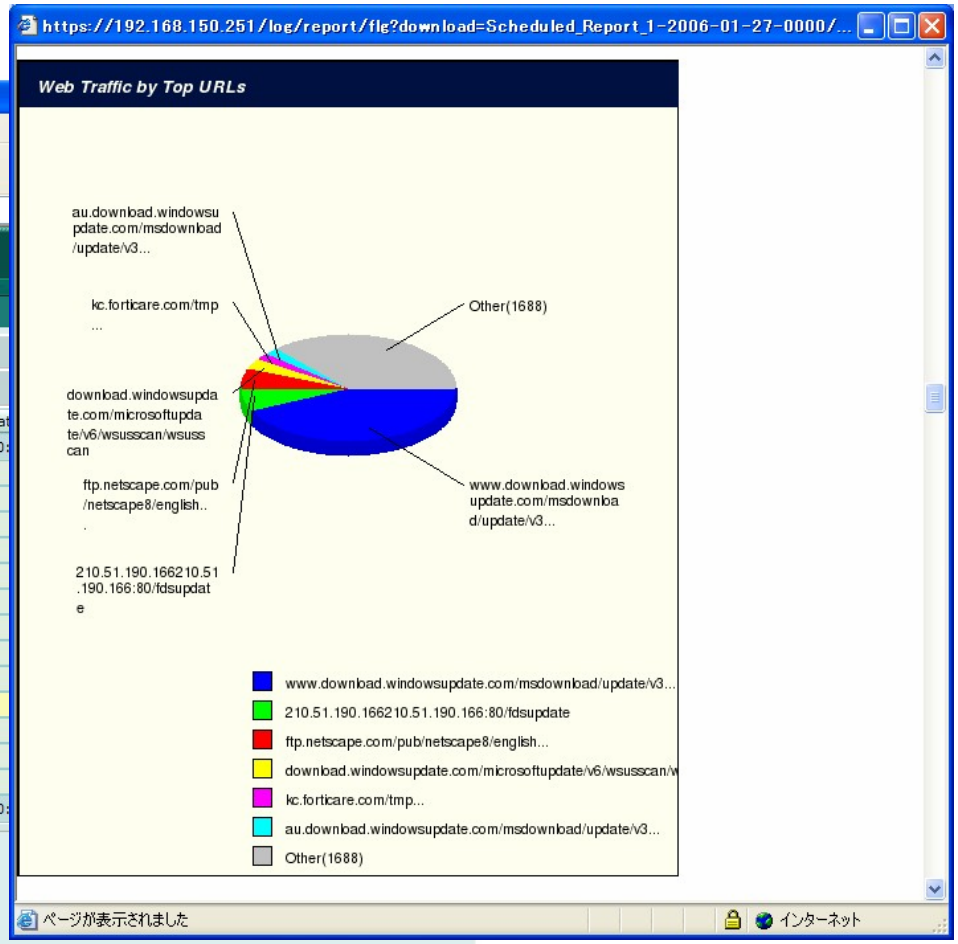
グラフィカルなアプリケーション
カテゴリ毎の統計グラフ

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





FortiAnalyzerとの連携

- コンテンツアーカイブ
- 隔離ファイル保存

Webブラウズサイト、メール内容、IMチャット内容

ディスクレス

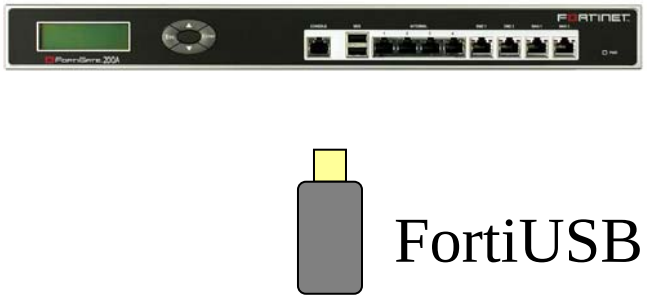
ログ
コンテンツアーカイブ
隔離ファイル

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で簡単にファイアウォール、VPN、アンチウイルス、IPS、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。