

---

# FortiGateのセキュリティ機能のご紹介

---

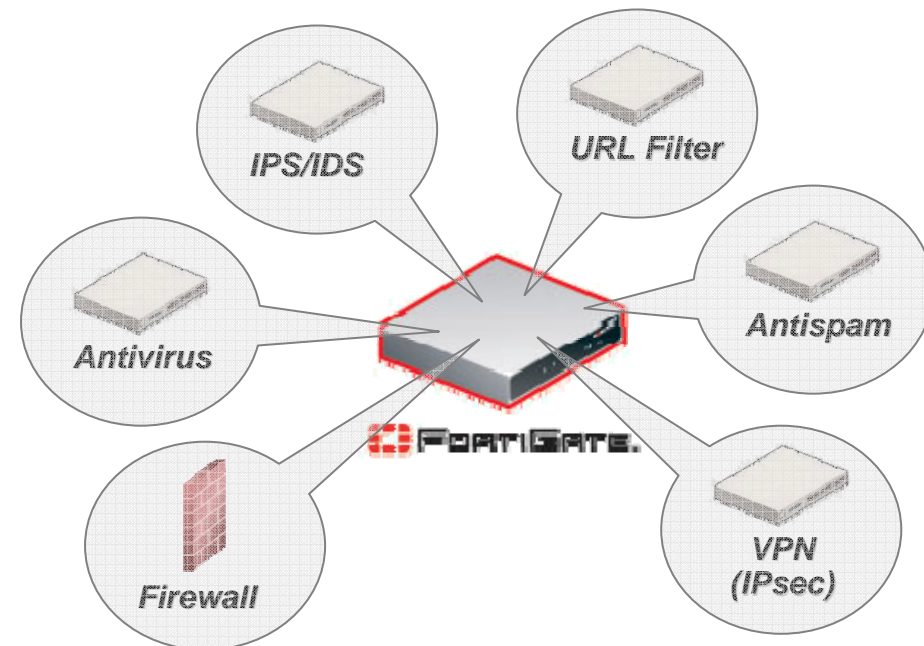
フォーティネットジャパン株式会社

# FortiGateとは？

## - 統合脅威管理システム

セキュリティ機能:

- ファイアウォール (ICSA Certified)
- アンチウイルス (ICSA Certified)
- IPS / IDS (ICSA & NSS Certified)
- VPN (ICSA Certified)
- Webコンテンツフィルタリング
- アンチスパム
- IM/P2P制御





---

# Webコンテンツフィルタリング

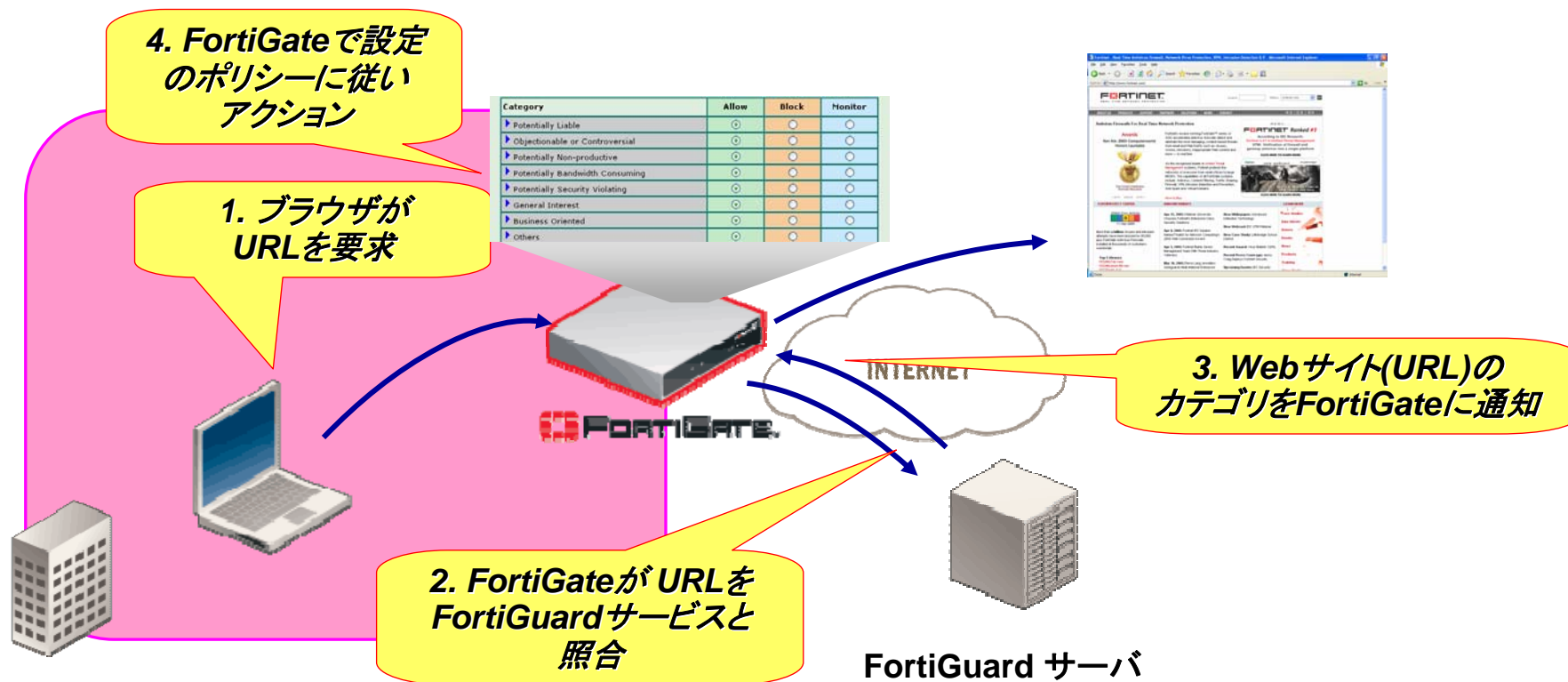
---

## Webコンテンツフィルタはなぜ必要？

1. 掲示板やWebメールからの情報漏洩
2. フィッシングなどの詐欺サイト
3. 私的利用による生産性の低下
4. セキュリティ上危険なサイトへのアクセス
5. 不適切なサイトへのアクセス

Web利用にともなう、これらの弊害を防止します

# FortiGuard Webフィルタリング概要



# FortiGuard Webフィルタリング管理画面

The screenshot displays the FortiGuard Web Filtering Management Interface. The interface includes a sidebar with navigation options and a main table of categories. The table has columns for 'Category', 'Allow', 'Block', 'Log', and 'Override'. Annotations highlight specific parts of the interface:

- カテゴリグループ**: A red circle highlights the first three categories: '違法性/犯罪性が高い', '論議を呼ぶ/物議を醸す', and '生産性を落とす'.
- アクション**: A red circle highlights the '許可', 'ブロック', 'ログ', and 'オーバーライドを許可' columns.
- カテゴリ**: A red circle highlights the 'カテゴリ' column.

カテゴリ	許可	ブロック	ログ	オーバーライドを許可
▶ 違法性/犯罪性が高い	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 論議を呼ぶ/物議を醸す	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ 生産性を落とす	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
広告	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
オンラインブローカー/株取引	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
フリーウェアダウンロード	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
ゲーム	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Webメール	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
ウェブチャット	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
インスタントメッセージ	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
ニュースグループ/伝言板	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
電子ポストカード	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 帯域を消費する	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ セキュリティ上危険	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ 一般的な趣味・関心	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ ビジネス関連	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ その他	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
レーティングなし	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
ローカルカテゴリ	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

# カテゴリー一覧

カテゴリグループ(8カテゴリグループ)	カテゴリ(76カテゴリ)
違法性／犯罪性が高い(12カテゴリ)	ドラッグ、カルト／オカルト、ハッキング／不正アクセス、違法・脱法行為／犯罪情報、人種差別、暴力、大麻、民間伝承／伝説、プロキシサーバ回避、サイト翻訳、フィッシング、盗作／盗用／剽竊
論議を呼ぶ／物議を醸す(14カテゴリ)	中絶、アダルト商品／サービス、権利擁護団体、ギャンブル、反政府行動／テロ／過激派、わいせつ／ヌード、ポルノ、悪趣味／下品／侮辱、兵器、性教育、アルコール、タバコ、下着／水着、狩りと戦争ゲーム
生産性を落とす(9カテゴリ)	広告、オンラインブローカー／株取引、フリーウェアダウンロード、ゲーム、Webメール、ウェブチャット、インスタントメッセージ、ニュースグループ／伝言板、電子ポストカード
帯域を消費する(5カテゴリ)	P2Pのファイル共有、個人ファイルストレージ、マルチメディアのダウンロード、インターネットラジオ／テレビ、IP電話
セキュリティ上危険(2カテゴリ)	ウイルス感染する、スパイウェア感染する
一般的な趣味・関心(24カテゴリ)	アートと娯楽、文化施設、教育、金融／バンキングサービス、ゲイ／レズビアン／バイセクシュアル、健康、求人情報、薬剤／サプリメント、ニュースとメディア、個人広告／出会い系、政党／政治団体／政治家、リファレンスサイト(辞書／地図等)、宗教、サーチエンジン／ポータルサイト、ショッピング／オークション、社会団体／職業団体／慈善団体、社会とライフスタイル、スポーツ、旅行、車、児童教育、不動産、レストラン／飲食、個人サイト
ビジネス関連(5カテゴリ)	ビジネスと経済、情報セキュリティ／コンピュータセキュリティ、政府機関と法的組織、IT、軍隊
その他(5カテゴリ)	サーバが動的に生成するURL、その他、Webホスティング、安全サイト、コンテンツサーバー

7 ユーザーグループ毎にアクセス許可やブロックを設定可能 **FORTINET**

# その他の機能

- キーワードによるブロック
- ウェブコンテンツブロック(しきい値)
- ウェブコンテンツ除外
- ウェブURLフィルタ
- ActiveX/Cookie/Javaアプレットフィルタ
- ウェブレジュームダウンロードブロック
- イメージのURLに基づいたレイティングを行う
- クラシフィケーションによるブロック

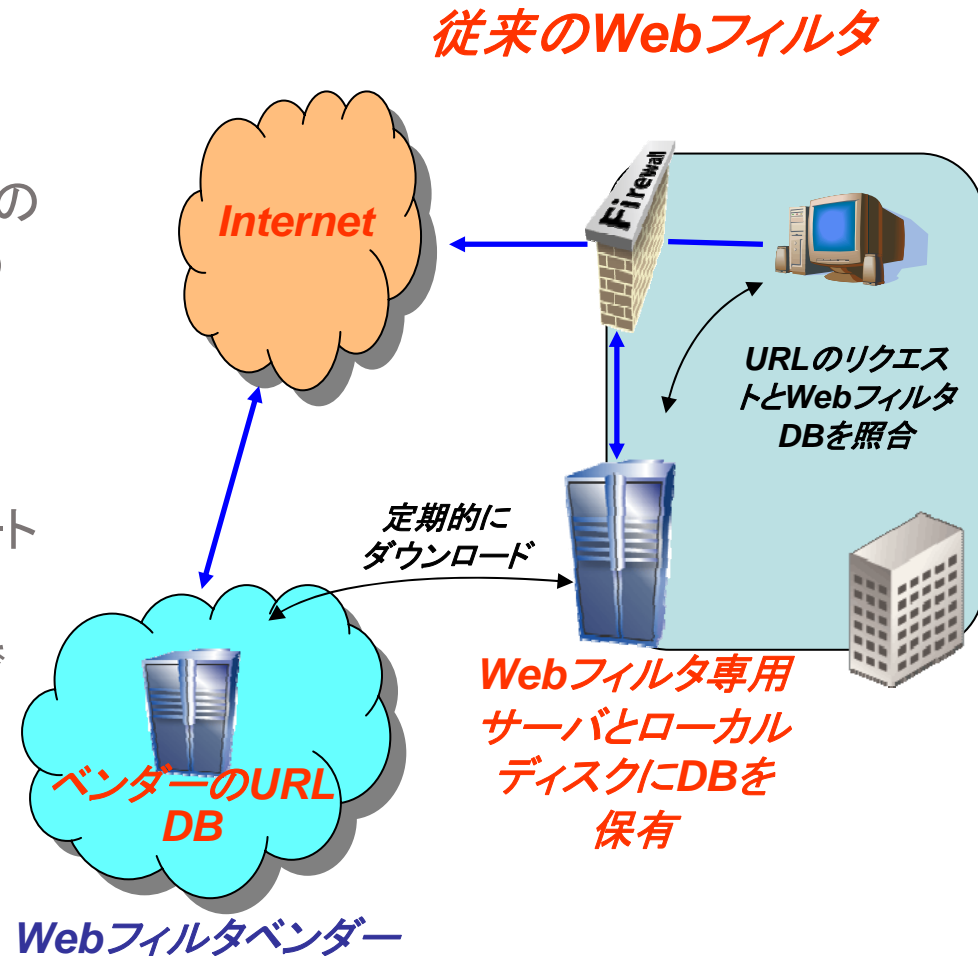
クラシフィケーション	許可	ブロック	ログ	オーバーライドを許可
キャッシュされたコンテンツ	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
マルチメディアサーチ	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
イメージサーチ	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
オーディオサーチ	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
ビデオサーチ	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
スパム URL	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

## FortiGuard Webコンテンツフィルタリングの特徴

- 業界最高レベルのURL評価情報データベース  
-4000万ドメイン以上 20億Webページ以上
- 費用対効果の優れたアプライアンス単位のサブスクリプションサービス
- 毎日更新されるURLデータベース
- CIPA準拠(学校、図書館、政府機関、あらゆる規模の企業の要求に適合)
- 容易なセットアップ、FortiGateセキュリティ・システムと完全に統合
- マルチ言語サポート(日本語含む)
- ピアツーピア接続、フィッシング詐欺、スパイウェアWebサイトへのアクセスをブロック
- 詳細でリアルタイムのWeb利用レポートとロギング
- 時刻によるスケジューリングと帯域制御

# 一般的なソフトウェアベースのURLフィルタとの比較

- 専用サーバを必要とする
- Proxyとの連携が必須の為、設置の自由度が低く、ネットワーク構成の変更が伴う場合も
- キーワードフィルタができないものが多い(パフォーマンスの問題)
- 数メガのDBを定期的にアップデートする必要がある
- リアルタイムに最新のDBを利用できない
- アカウント毎の課金で高価

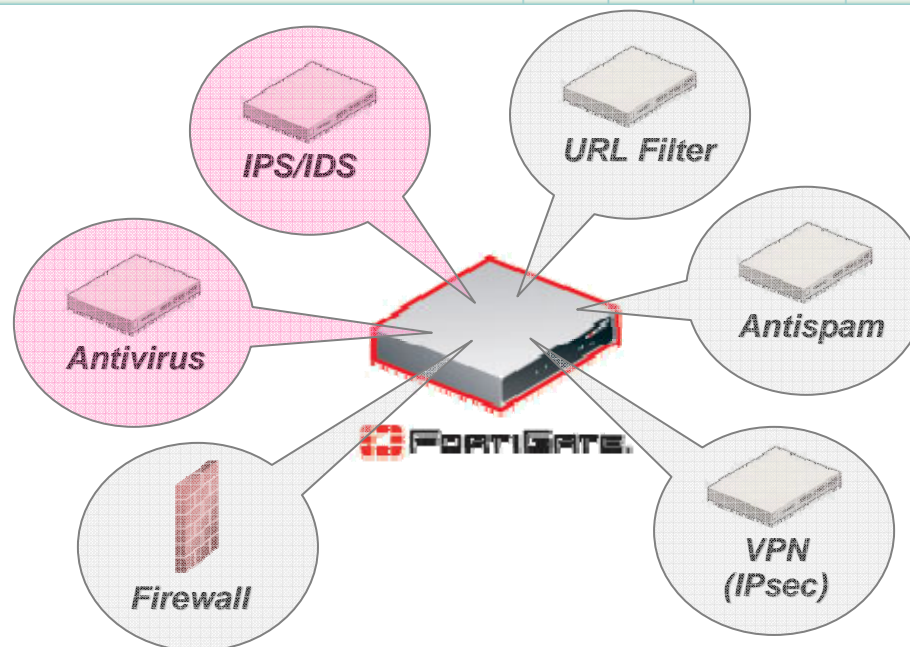


# 統合型のアドバンテージ

Webセキュリティを考えた場合・・・

- HTTPトラフィックのアンチウイルスも必須
- HTTPトラフィックからの攻撃を防ぐ必要がある

eFiction.SQL.Injection.A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	2,279	
eFiction.SQL.Injection.B	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	2,279	



**FORTINET**



---

# アンチウイルス

---

# ウイルス対策基本動作

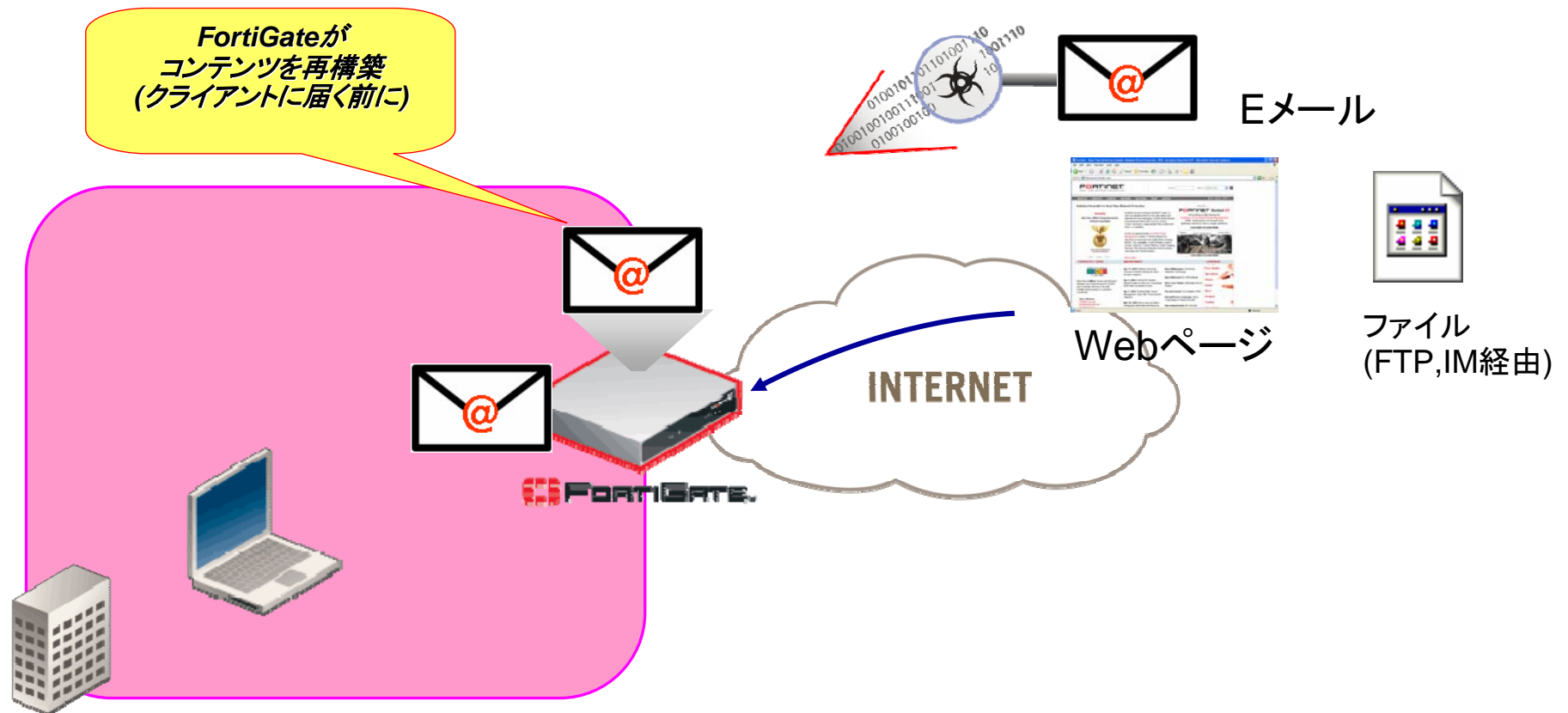
ウイルス対策で重要な「エンジン」と「パターンファイル」とは・・・

ウイルスを犯人に例えると・・・

- エンジンは”警察官”  
新しい仕組みのウイルスに対応する為、エンジンもアップデートが必要
- パターンファイルは”指名手配書”  
ベンダーによって更新スピードに差がある。  
常に最新にしておく必要がある
- ヒューリスティックは”カンによる職務質問”  
※ベンダーの技術に差が出る



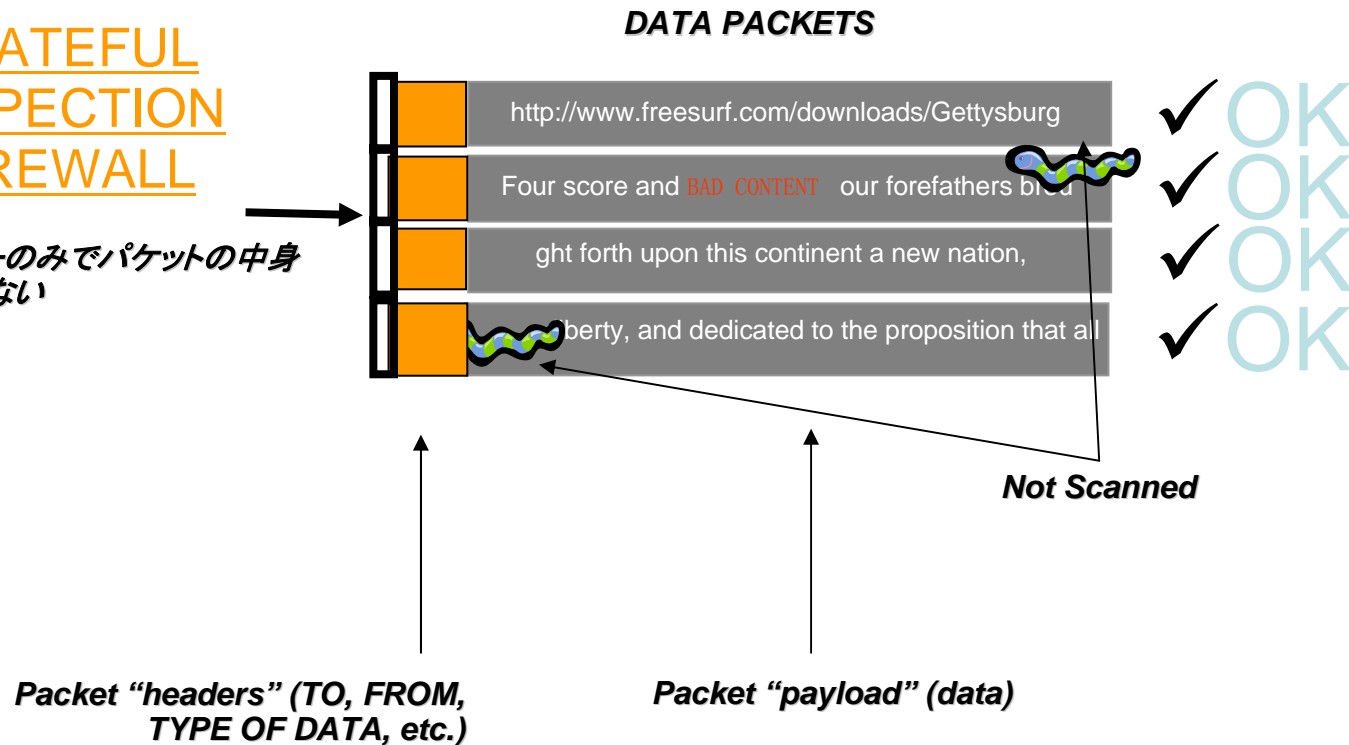
# FortiGuard アンチウイルス概要



# コンテンツベースの脅威には無力な ステートフルインスペクション

## STATEFUL INSPECTION FIREWALL

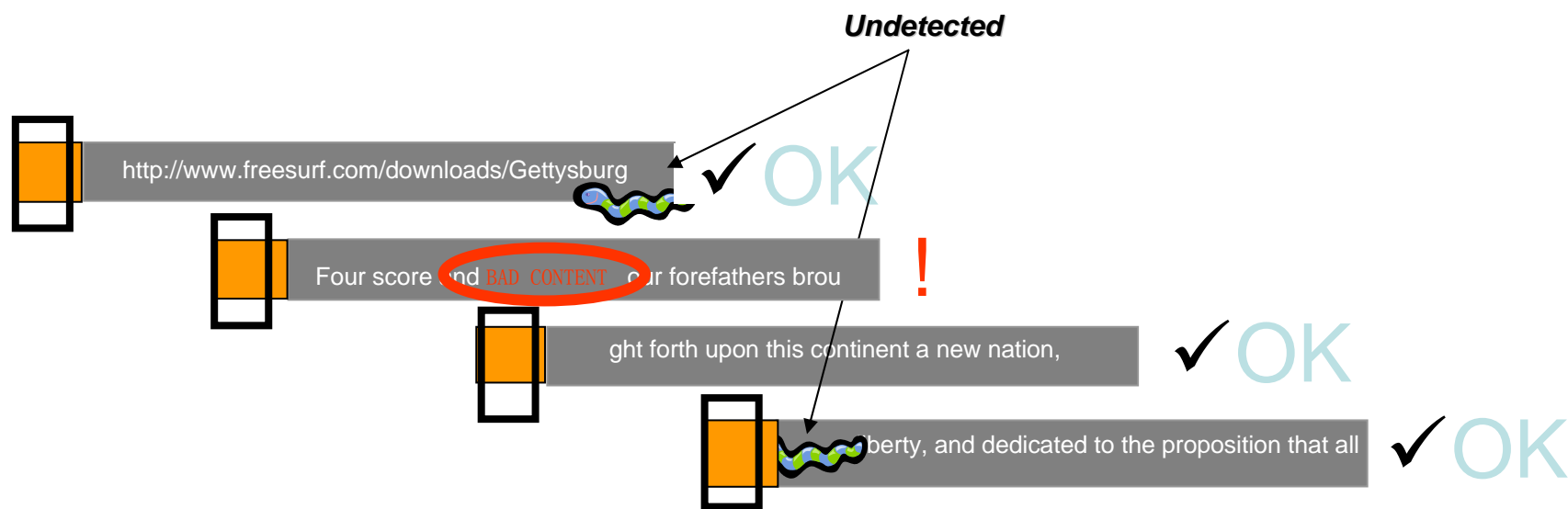
ヘッダーのみでパケットの中身  
は調べない



# ディープパケットインスペクション ～パケット分割されたコンテンツはチェックできない～

## DEEP PACKET INSPECTION

パケットの中身は確認するが、複数にフラグメント化されたパケットに対しては確認する事が出来ない。



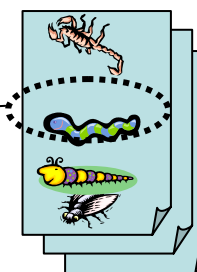
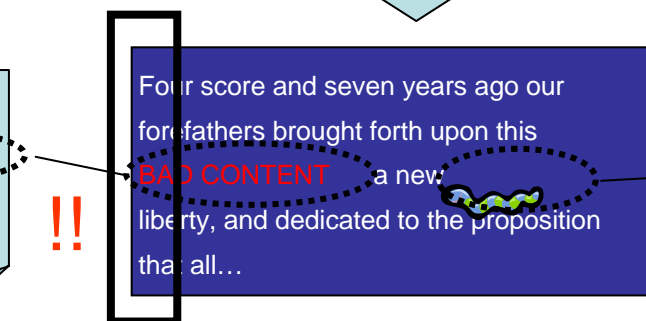
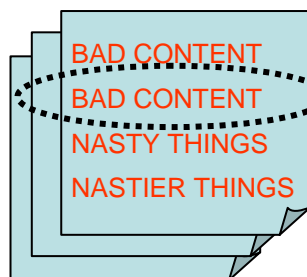
# コンプリートコンテンツインスペクション

## COMPLETE CONTENT PROTECTION

### 1. フラグメント化されたパケットを再構築



許可しないコンテンツ



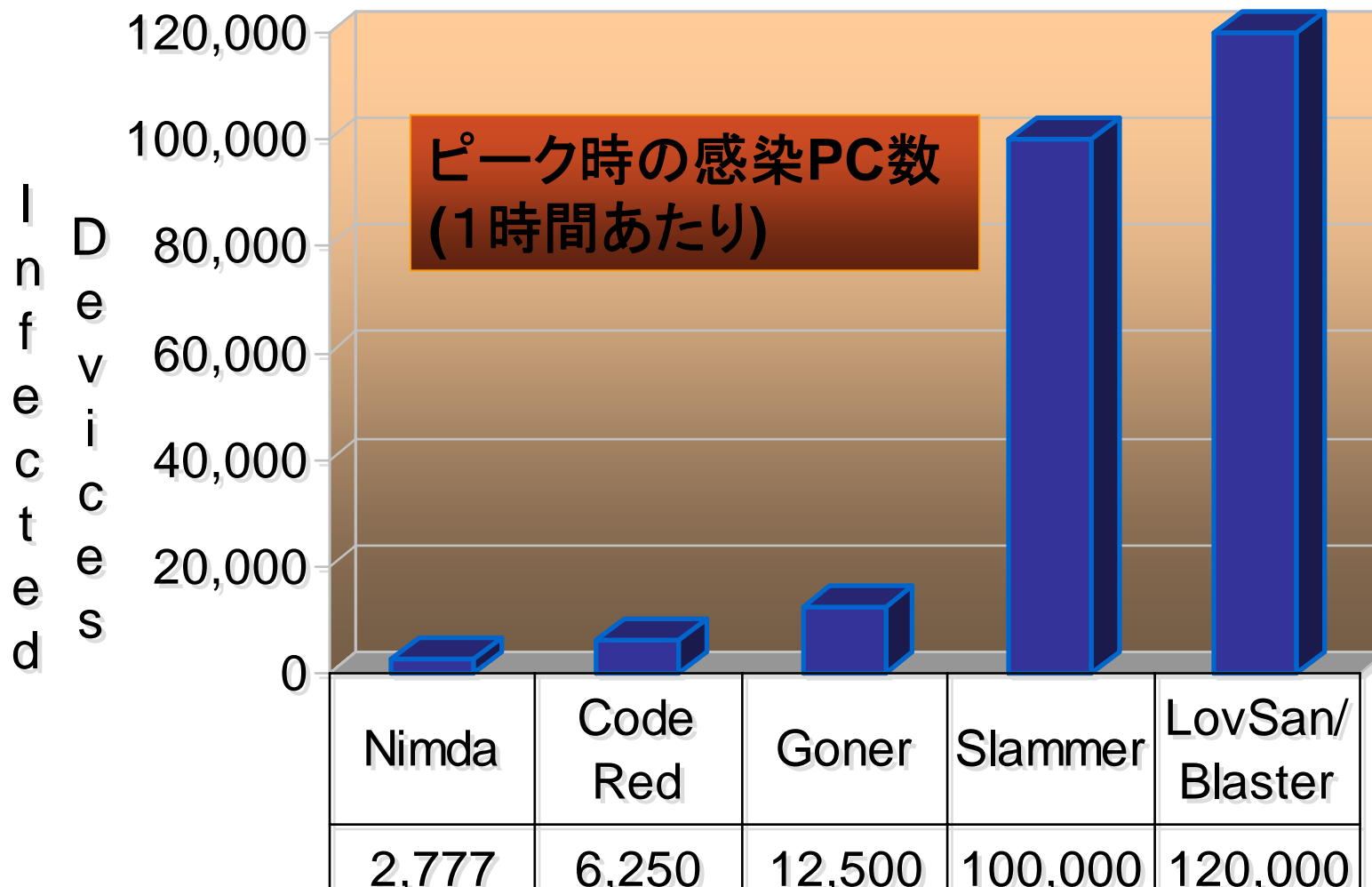
攻撃サイン

### 2. 再構築したファイルをチェック

FortiGateはこの方式を採用

FORTINET™

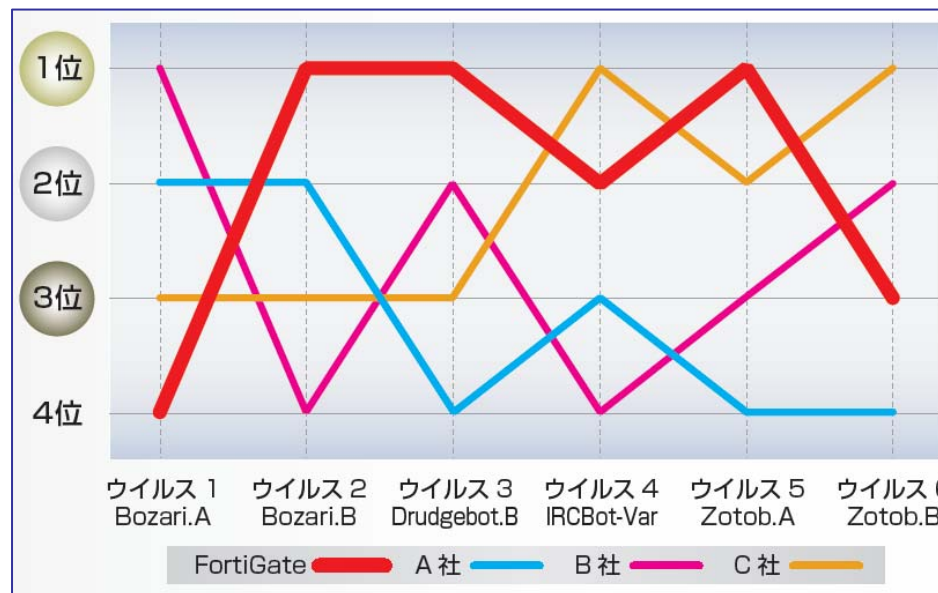
# 爆発的な感染スピード



# 新しい脅威への迅速な対応が必須

## 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。



## FortiGateはヒューリスティックで高精度にウイルスを検出

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)

# 一般的なアンチウイルス専用ソフトウェアとの比較

- Proxyとの連携やメールの転送が必要な為、ネットワークの再構築が必要
- ラインナップや対応OSが多数の為、パターンファイル更新が遅い場合がある
- クライアントベースの課金で高額
- OSの脆弱性と、セキュリティパッチとセキュリティソフトウェアの整合性を管理する必要がある
- 多機能な汎用CPUと汎用OSで、単機能ソフトウェアを動かす為無駄が多く低速である場合が多い
- 限られたプロトコルのみサポート(IMのファイル転送は未対応)

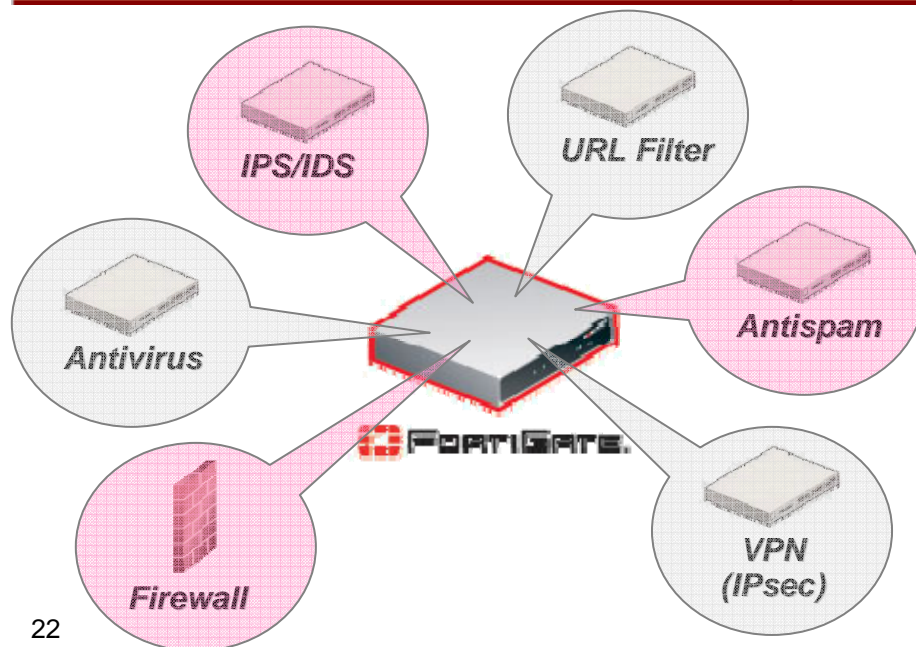
# FortiGuard アンチウイルスの特徴

- アンチウイルス・シグニチャの自動更新(プッシュ配信対応)
- SMTP、POP3、IMAP、FTP、HTTP、IMに対応
- VPN(IPSec、SSL)コンテンツに対応
- 双方向に対しスキャン可能
- 数千台規模のFortiGateシステムの管理とレポート作成が一元的に可能
- Transparent、NAT、Routeの3モード


# 統合型のアドバンテージ

ウイルス対策だけでは、ウイルスによる被害は防げません

AVで防げないウイルスによる被害	ウイルスタイプ	有効なソリューション
脆弱性のあるWebサーバにネットワークベースの攻撃で感染	ネットワーク型ウイルス	IPS
脆弱性のあるPCにネットワークベースの攻撃で侵入	ネットワーク型ウイルス	IPS/FW
感染後ボット化し、感染PCをスパムや攻撃の加害者に	ボット系ウイルス	アンチスパム/IPS/FW
WinnyなどのP2P通信からウイルス侵入および暴露ウイルスによる情報漏えい	Antinnyなど	IPS
Webサーバを作成し情報漏えい	山田オルタナティブなど	FW



ウイルスによる被害を防止するには統合型がもっとも効果的なソリューションです



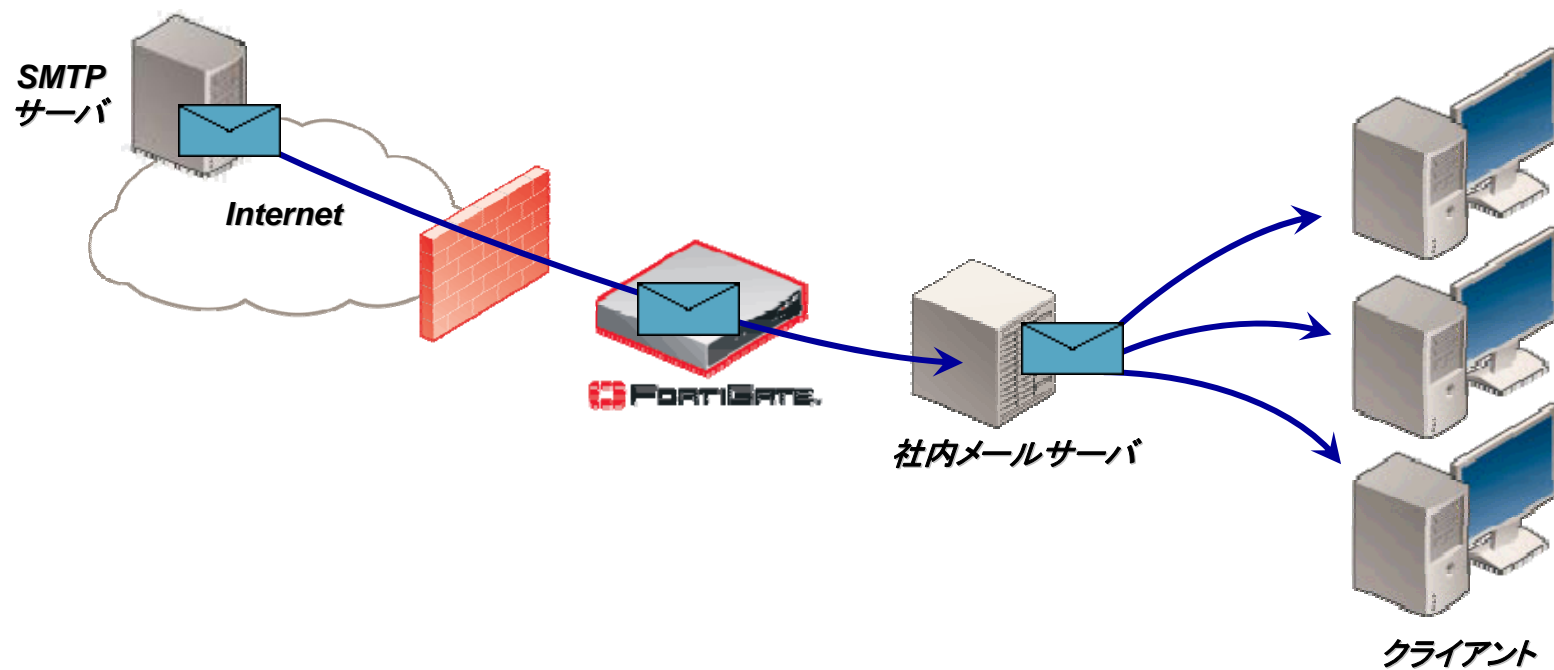
---

# スパム対策

---

---

# アンチスパム基本動作



# FortiGuard アンチスパム

## FortiGateスパムフィルタ

- IPアドレスチェック
- URLチェック
- チェックサムチェック
- IPアドレスBWLチェック
- リバースDNSルックアップ
- メールアドレスBWLチェック
- 返信メールDNSチェック
- 禁止ワードチェック

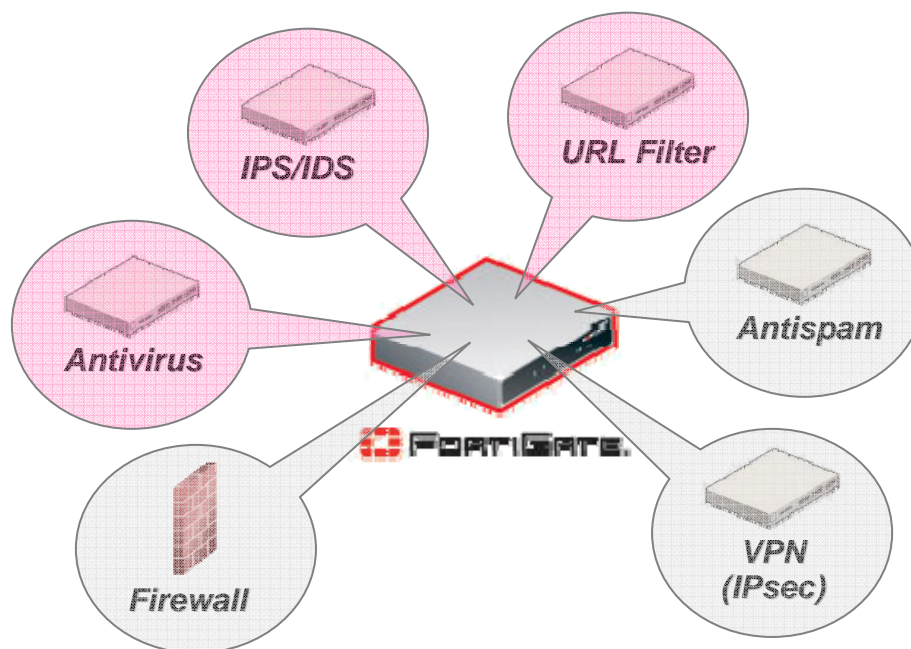
スパムアクション: タグ付与、破棄(SMTPのみ)

# SPAM専用機との比較

- サーバモードのみでトランスペアレントモードがない為、ネットワークの変更が必要
- ラインナップが少ない
- 専用機にもかかわらず検知率が低いものが多い

# 統合型のアドバンテージ

- フィッシングなどの詐欺サイトへのリンクをブロック可能(Webフィルタリング機能)
- メールからのウイルスをブロック可能(アンチウイルス機能)
- メールサーバーへの攻撃を防御可能(IPS)



# 参考:FortiMailとは？

## メール用スパム&ウイルス対策アプライアンス

- ベイジアンやヒューリスティックなどフィルターがより充実
- トランスペアレントに加え、ゲートウェイモード、メールサーバモード、感染メールの隔離
- Webメール機能
- ユーザ毎にフィルターの設定が可能
- メールアーカイブ
- IPS、Webフィルタ、FW、VPN機能は非搭載





---

# ファイアウォール／VPN

---

---

# FW/VPNの特長

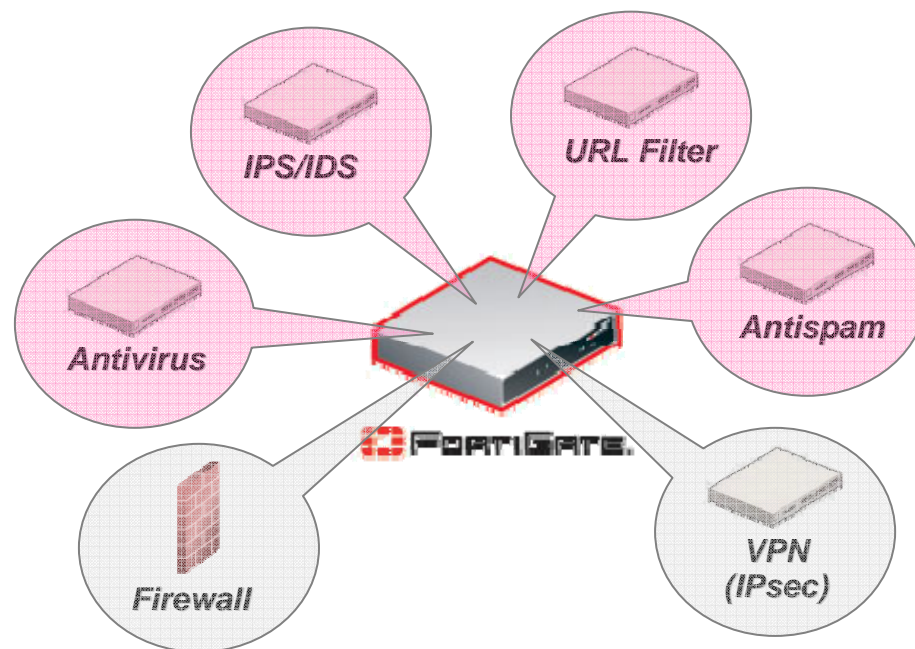
- ACICベースの高速なハードウェアと専用のセキュアなOS
- アプリケーションレベル(L3-7)のセキュリティにも対応
- IMおよびP2Pプロトコルまでサポートを拡大
- IPSec VPN、SSL VPN機能を標準装備
- バーチャルドメイン機能により仮想UTMが作成可能
- FortiManager/FortiAnalyzerによる集中管理&レポートニングに対応
- FortiAnalyzerにより詳細なログ／レポート作成
- RIP、OSPF、BPGなどのダイナミックルーティングプロトコル対応
- SOHOからマルチギガビットまで対応可能な各種製品モデルを用意し、スケーラブルなパフォーマンスを実現

# FW/VPN専用機との比較

- ASICでない場合、パフォーマンスが十分でない場合がある
- 汎用OS場合の場合、脆弱性が多い場合がある
- コンテンツベースの脅威に無力(L3-4のみ対応)
- SSL VPNは別アプライアンスの場合が多い

# 統合型のアドバンテージ

- コンテンツベース(L3-7)の脅威に対応
- FWで防げない攻撃に対応(IPS機能)





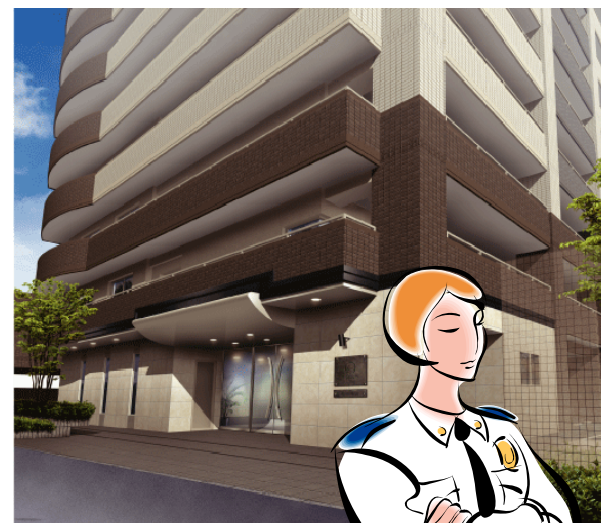
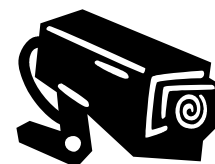
IPS



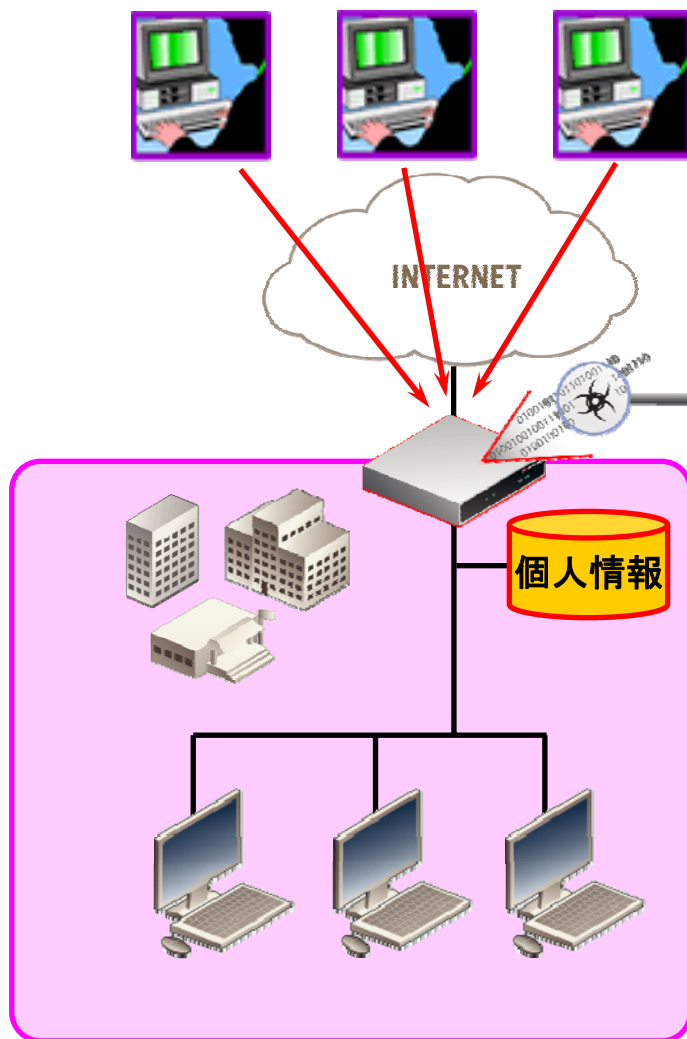
# IPSはなぜ必要

ビルの警備に例えると・・・

- ファイアウォール(ドア):不正な通信を遮断
- IDP(監視カメラ):正常な通信に見せかけた通信を検知
- IPS(ガードマン):正常な通信に見せかけた通信を検知と遮断



# 基本動作



外部からの侵入者

View predefined signatures with severity: <=> All アクション All Go

シグニチャ名	有効	ロギング	アクション	Severity	リビジョン
▶ DoS	●	●			
▶ SCADA	●	●			
▶ VoIP	●	●			
▶ applications	●	●			
▶ backdoor	●	●			
▶ database	●	●			
▶ email	●	●			
▼ file_transfer	●	●			
WFTPD.Pro.MLST.Buffer.Overflow	☑	☑	Pass	Low	2,233
HP-UX.FTP.Server.Directory.Listing.A	☑	☑	Pass	Medium	2,300
HP-UX.FTP.Server.Directory.Listing.B	☑	☑	Pass	Medium	2,300
SolarWinds.TFTP.Server.Directory.Traversal	☑	☑	Pass	Low	2,229
moxftp.Banner.Parsing.Buffer.Overflow	☑	☑	Pass	High	2,229
WS_FTPD.CWD.Stack.Overflow	☑	☑	Pass	High	2,308
Wzdfpd.SITE.Arbitrary.Command.Execution.A	☑	☑	Pass	Low	2,247
FutureSoft.TFTP.Directory.Traversal.A	☑	☑	Pass	High	2,231
FutureSoft.TFTP.filename.Buffer.Overflow	☑	☑	Pass	High	2,231
FutureSoft.TFTP.transfer-mode.Buffer.Overflow	☑	☑	Pass	High	2,231
Gzip.FTP.Get.Buffer.Overflow	☑	☑	Pass	High	2,228

FWでは防ぐことのできない  
侵入を防御

# シグネチャー一覧

View predefined signatures with severity: <= All アクション = All Go

シグニチャ名	有効	ロギング	アクション	Severity	リビジョン	
▶ DoS	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
▶ SCADA	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
▶ VoIP	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
▶ applications	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
▶ backdoor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
▶ database	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
▶ email	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
▼ file_transfer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
WFTPD.Pro.MLST.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	2.233	
HP-UX.FTP.Server.Directory.Listing.A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	2.300	
HP-UX.FTP.Server.Directory.Listing.B	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	2.300	
SolarWinds.TFTP.Server.Directory.Traversal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	2.229	
moxftp.Banner.Parsing.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	2.229	
WS_FTPD.CWD.Stack.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	2.308	
Wzdftpd.SITE.Arbitrary.Command.Execution.A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	2.247	
FutureSoft.TFTP.Directory.Traversal.A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	2.231	
FutureSoft.TFTP.filename.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	2.231	
FutureSoft.TFTP.transfer-mode.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	2.231	
Gzip.FTP.Get.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	2.228	

# FortiGuard IPSサービスの特徴

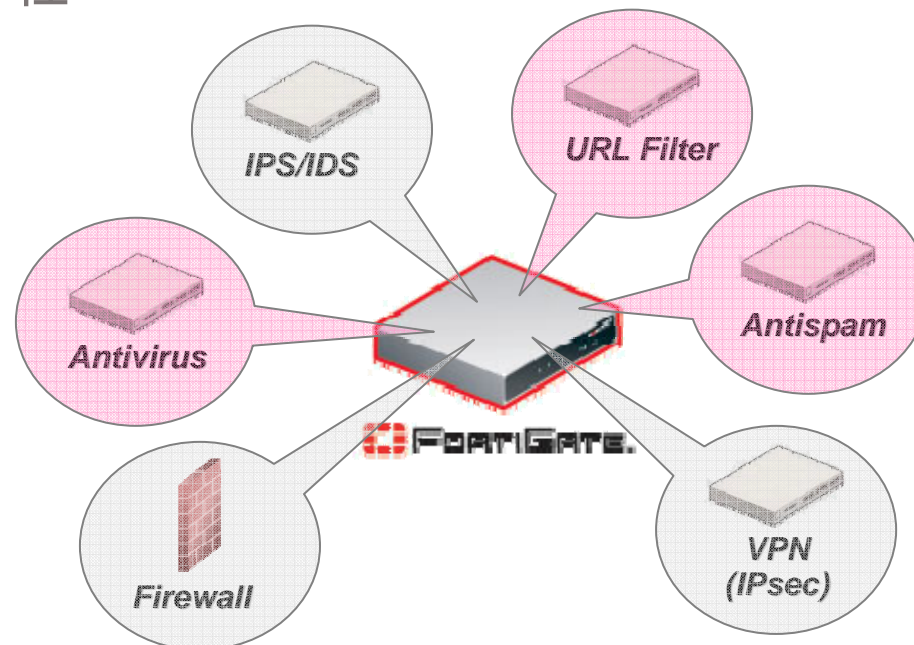
- IPSシグネチャの自動更新
- ユーザ定義可能なカスタムIPSシグネチャ
- VPN (IPSecおよびSSL) コンテンツの検閲
- 双方向のIPSコンテンツ・フィルタリング
- シグネチャ・エンジンおよびプロトコル異常(アノマリ)検知エンジン
- 詳細なロギングとレポート作成
- 50種類以上のプロトコルとアプリケーションをサポート
- ネットワーク設計を変更することなくシームレスに導入可能

# IDS専用機との比較

- 高額な価格設定
- プッシュ型のシグネチャアップデート機能がない為、シグネチャ更新のタイムラグが大きい
- コンテンツベースの攻撃は未対応
- 限られたラインナップ(大企業向けがメイン)
- HA構成対応はハイエンドモデルのみ

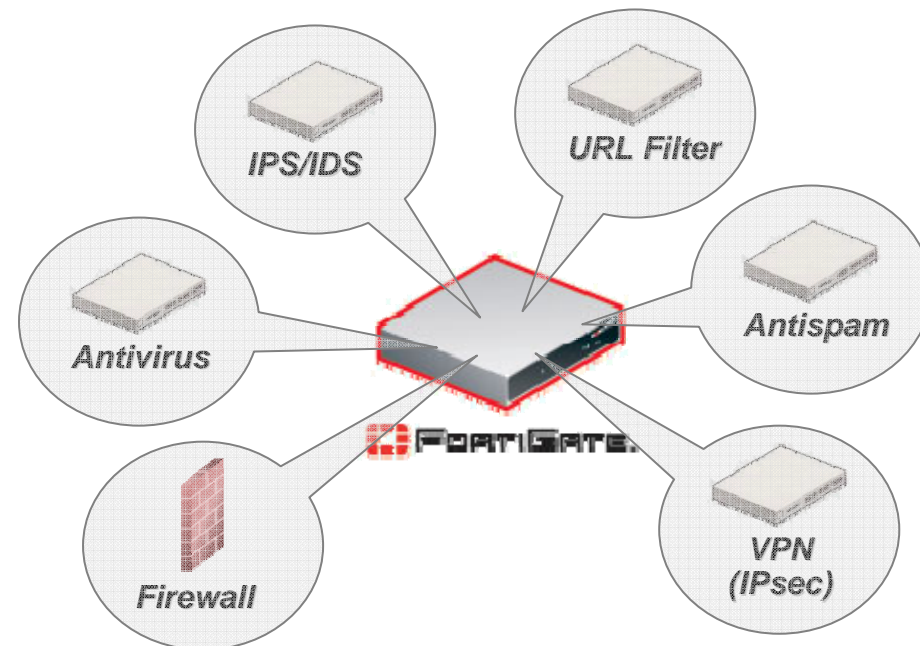
# 総合型のメリット

- アプリケーションレベルの脅威も防御可能
- 幅広いラインナップ  
エントリーモデルは部署間IPSとしても効果的
- 容易な操作性



## セキュリティ機能:

- ファイアウォール (ICSA Certified)
- アンチウイルス (ICSA Certified)
- IPS / IDS (ICSA & NSS Certified)
- VPN (ICSA Certified)
- Webコンテンツフィルタリング
- アンチスパム
- IM/P2P制御



# ありがとうございました。