フォーティネットのアンチウイルス・ソリューション

ソリューションブリーフ

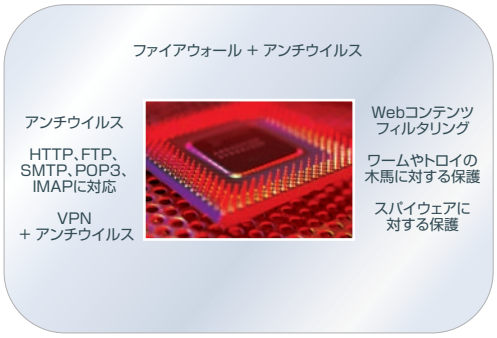
ASICベースのアンチウイルス・プロテクション

ANTIVIRUS ACCELERATED

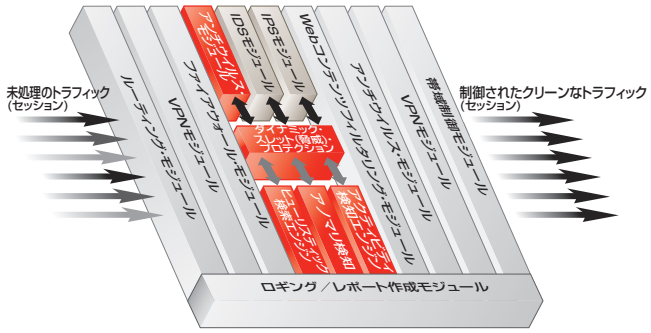
複合型脅威などさまざまな脅威に対するセキュリティプロテクション

フォーティネットのセキュリティ製品ファミリは、完全に統合化された包括的ソリューションです。複合型の脅威や、不正侵入、ウイルス、トロイの木馬、ワーム、スパイウェア、グレーウェア、アドウェア、DoS攻撃など、さまざまな攻撃や悪質な行為を検知して除去します。ASICで高速化されたハードウェアによるネットワークベースのプラットフォームを採用し、一連の高性能なダイナミック・スレット(脅威)・プロテクション・エンジンを組み合わせました。これにより、フォーティネットは、TCOを削減しながら、最高レベルのマルチ・スレット(脅威)対応セキュリティと業界最高のパフォーマンスを提供します。これらのセキュリティ・エンジンは、定評のあるFortiOS™で実行しますが、個別に利用することもすべてをまとめて利用することもできます。IT管理者が、まさに求めていた包括的なセキュリティ・ソリューションです。

フォーティネットのASICベースのマルチ・スレット(脅威)対応セキュリティ・ソリューションは、リアルタイムパフォーマンスを提供します。



最先端のFortiGateシステムがサポートするセキュリティ機能



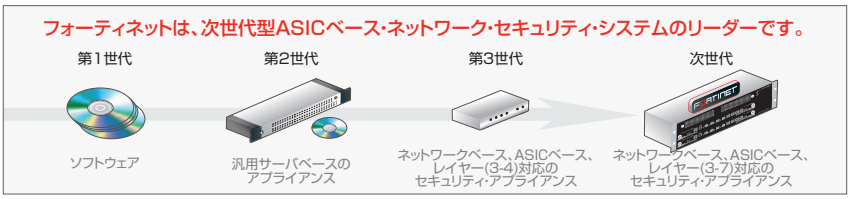
FortiOSマルチスレット(脅威)セキュリティプロテクションシステム

ソリューション

フォーティネットの最先端のアンチウイルス技術は、シグニチャ検知エンジンとヒューリスティック検知エンジンを組み合わせることにより、デスクトップコンピュータやネットワークゲートウェイへのさまざまな攻撃に対する多層的なリアルタイム保護を実現します。総合的なFortiASICプロセッサに、フォーティネットが特許出願中の技術CPRL(Content Pattern Recognition Language)を組み合わせることで、ウイルススキャンとアノーマリ検知を高速化し、驚くほど高いシステムパフォーマンスを実現しています。FortiClient™ソフトウェアを利用して、ノートパソコンや、デスクトップパソコン、アプリケーションサーバのセキュリティレベルを高めることも可能です。

ICSA labs CERTIFIED www.ICSALabs.com Antivirus

Network Computing Editor's Choice



Feb 2005 100% VIRUS BULLETIN www.virusbtn.com

FORTINET MULTI-THREAT SECURITY SOLUTIONS

マルチギガビットまで対応可能なスケーラビリティ

主要機能

- 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するアンチウイルス・プロテクション
- ASICベースのハードウェア設計
- アンチウイルス・シグニチャの自動更新
- SMTP、POP3、IMAP、FTP、HTTPに対応
- VPN(IPSec、SSL)コンテンツに対応
- 双方向コンテンツ・フィルタリング
- 圧縮形式ファイルに対応(tar、gzip、rar、lzh、iha、cab、arj、zip)
- FortiClient統合セキュリティ・ソフトウェア
- 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
- トロイの木馬、ワーム、スパイウェア、グレーウェアに対する保護

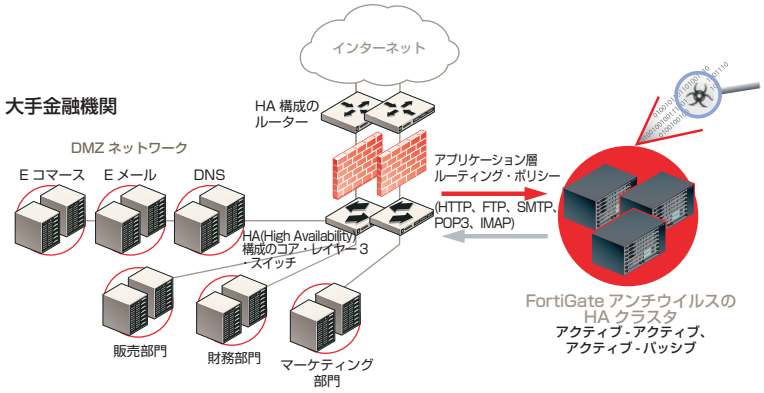
特長

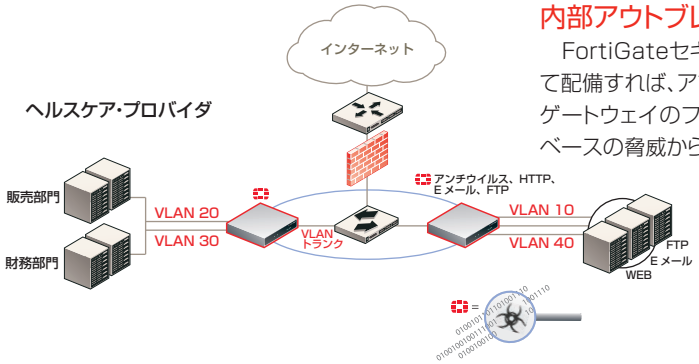
- どのような規模のネットワークにも対応できるFortiGateシステム
- 業界最高のパフォーマンス
- 新型のゼロデイ・アタックに対する保護
- 包括的なマルチプロトコル・アンチウイルス・プロテクション
- VPNトンネル内のウイルス・プロテクション
- 外部からの攻撃だけでなく内部の攻撃に対する保護
- 圧縮ファイルに潜む悪質なコンテンツの検知
- 最先端のアンチウイルス・プロテクションをクライアントとサーバにも提供
- セキュリティポリシーを常に更新して、管理や運用コストを削減
- さまざまな構成形態のネットワークに柔軟かつ容易に配備可能
- 包括的セキュリティ保護

フォーティネットのアンチウイルス・ソリューション

MSSP(マネージド・セキュリティ・サービスプロバイダ)コア・ネットワーク・セキュリティ

大規模企業やサービスプロバイダのコアに配備することにより、Eメール、Web、FTPなどのトラフィックに紛れてネットワークに不正侵入しようとするウイルスを防止します。ポリシーベースのルーティング／コンテンツ・スイッチングを活用することにより、マルチギガビットのスケーラビリティを実現します。問題のあるトラフィックをFortiGateセキュリティ・アプライアンスに送って、さらに高度なスキャニングを実施します。この配備構成は、インライン配備としても十分機能します。



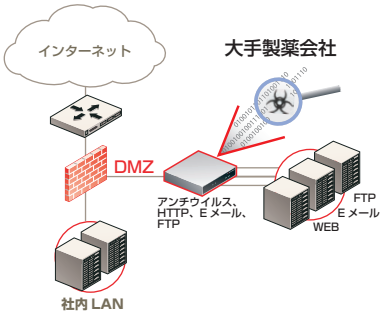


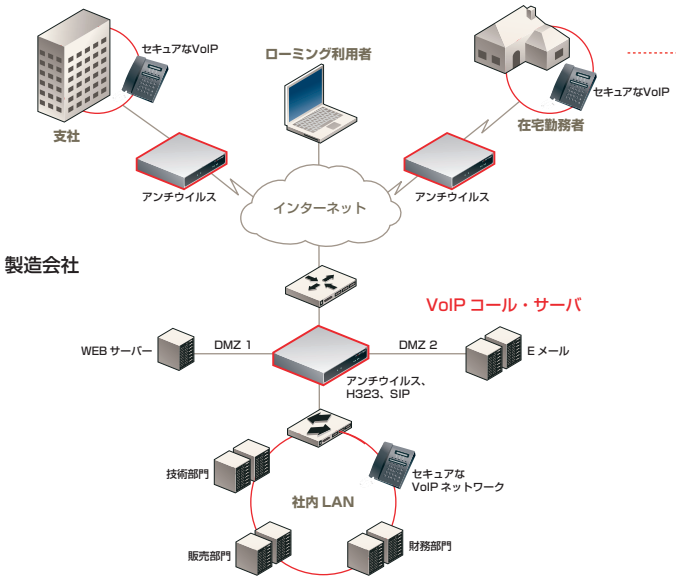
内部アウトブレークの防止

FortiGateセキュリティシステムは、多層セキュリティ設計の一環として配備すれば、アプリケーション層の攻撃に対する保護を強化できます。ゲートウェイのファイアウォールをすり抜けるおそれのあるコンテンツベースの脅威からも保護できます。

DMZ保護

既存のファイアウォールで保護されていないDMZ区域でインターネットにさらされているWebサーバ、FTPサーバ、Eメールサーバを保護するために配備します。フォーティネットの最先端のアンチウイルス技術は、ウイルススキャンのオーバーヘッドによりサーバの性能を悪化させずに、従来のサーバソフトウェアの数分の1のコストで、ウイルス感染を検知して防止します。





エッジ・プロテクション

ネットワーク・セキュリティ・ゲートウェイとして配備します。1台のFortiGateセキュリティシステムで、社内ネットワークと複数のDMZ区域を、ウイルスなどのコンテンツベースの攻撃から保護できます。フォーティネットのセキュリティゾーン機能とバーチャル・ドメイン機能は、複数のネットワークを保護する必要がある大規模企業のTCO削減に役立ちます。

FortiGuard配信ネットワーク

フォーティネットは、ネットワークを攻撃する現在9万件を超えるウイルスのデータベースの中から4500種以上のアクティブなウイルスを抽出したWildListに基づいてウイルス対策を強化しました。フォーティネットは、世界50ヵ所に重複配備された高速データベースサーバ経由で、シグニチャのリアルタイム自動更新も行なっています。成長する世界経済や常に変化するセキュリティ情勢の要求に応えるため、フォーティネットは、ワールドワイドかつ一級のサービス配信ネットワークの実現に尽力します。

業界で定評のあるアンチウイルス専門技術

フォーティネットのアンチウイルス調査チームは、チーフ・アンチウイルス・サイエンティストのJoe Wellsが率いています。Joe Wellsは、世界最大のアンチウイルス調査連携プロジェクトWildListの創始者です。

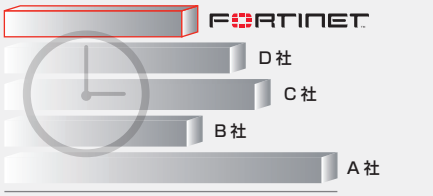
グローバル・ウイルス調査チーム

フォーティネットのアンチウイルス・セキュリティサービスは、フォーティネットのセキュリティ専門家のグローバルチームが、年中無休の24時間体制で、作成、更新、管理を担当しています。新型の攻撃が企業の社内リソースに被害を与えたりエンドユーザのコンピュータに感染したりしないように、事前に確実に検知し防止します。フォーティネットのアンチウイルス・シグニチャは、業界最速で自動的に更新できます。

- **自動更新** – シグニチャやヒューリスティック・エンジンを自動的に更新して、新種のウイルスやスパイウェアの侵入を防止します
- **業界をリードするスレット(脅威)レスポンスタイム** – フォーティネットは、より早くシグニチャを更新し、新型攻撃を防止します
- **脅威に対する予防型のライブラリ** – WildListで報告された脅威、OSやアプリケーションで発見された数千件の既知の脆弱性から保護します。
- **年中無休の24時間体制で世界全体をカバー** – 世界12ヵ国50ヵ所以上にサーバを分散配備しています。
- **アプライアンス単位のライセンス体系(クライアント無制限)** – 従来のユーザ単位のライセンス体系に比べ、サブスクリプション費用を大幅に低減できます。

どこよりも早く市場に投入

フォーティネットは、競合他社のどこよりも早く FortiGuard アンチウイルスを投入して、Sober ウイルスの新亜種 W32/Sober.M-mm に対応しました。



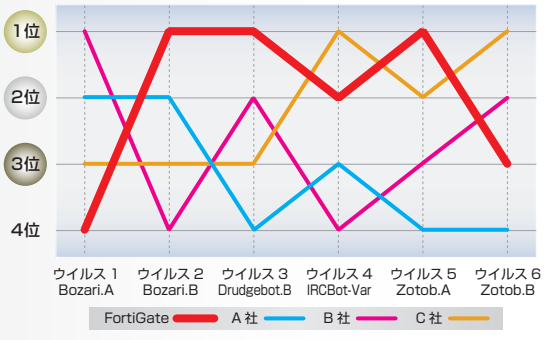
出典：www.avtest.org

既知・未知のウイルスへの対応力

- **世界各地の専門家が、迅速にパターンファイルを更新!**
  世界各地のネットワークの専門家を集めた世界的ネットワーク『Threat Response Team』が、ウイルスサンプルを収集・分析し、ウイルスパターンファイルを迅速に開発。24時間体制でパターンファイルをアップデートし、最新のウイルス、ワーム、トロイの木馬、スパイウェアなどの脅威から守ります。
- **独自OS「FotiOS」が、新たなゼロデイ・アタックの脅威を阻止!**
  パターンファイルとして更新されていない、新たなゼロデイ・アタックへの脅威には、独自OS「FotiOS」のヒューリスティック技術を使い、ビヘイビアベースの分析で高いレベルで阻止します。

パターンファイルの更新の早さの比較

右のグラフは、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。



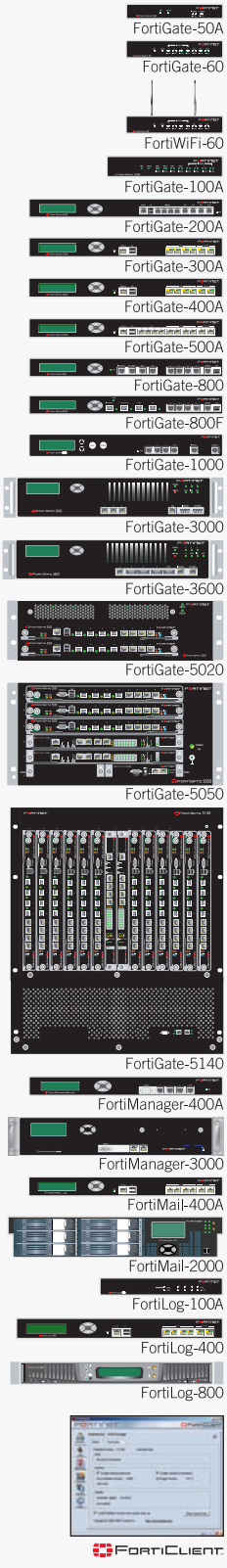
ヒューリスティックにウイルスを検出できたのは FortiGate だけ

右の表は、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						

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™
REAL TIME NETWORK PROTECTION

顧客満足

「フォーティネットのプラットフォームを使用して、わが社は管理サービスの標準化に成功しました。おかげで、今はセキュリティ・オプションを強化して、より迅速に、より低価格でサービスを顧客に提供することができるようになりました。しかも、複数ベンダーのソフトウェアを使用していたときより、利益率の高いサービスや機能を提供することもできるようになりました」

- BAI Security(BAIセキュリティ社)
  Michael Bruck, President(マイケル・ブラック社長)

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/