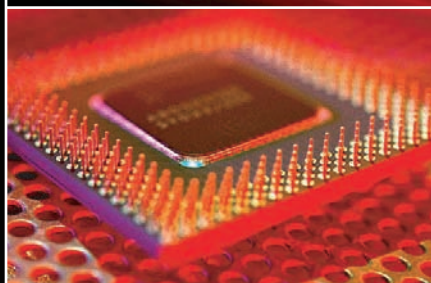


FORTIGATE™ 1000A

ADVANCED REAL-TIME DATA SECURITY SOLUTIONS



POWERFUL, INTELLIGENT & STATE OF THE ART

フォーティネットはセキュリティ分野におけるリーダー

FortiGate™ シリーズのマルチ・スロット (脅威) 対応・セキュリティ・システムは、ASIC ベースの専用アプライアンス製品です。マルチギガビットのスピードにまで拡張可能な包括的ネットワークプロテクションを提供します。フォーティネットのコンプライト・コンテンツ・プロテクション&再構成テクノロジーは、業界初のハードウェア化されたコンテンツ・インスペクション・エンジンを採用しました。ASIC ベースでネットワークベースのセキュリティ製品としては、現在、業界最先端を進んでいます。

FortiGate-1000A セキュリティシステムは、大規模企業から求められる厳しい要求に対応するため、ギガビットスループットと優れた信頼性を実現した高性能ソリューションです。FortiGate-1000AFA2 は、小パケットの処理能力を高める FortiAccel™ テクノロジーをオプションとして利用するためのポートを 2 基備えています。どの FortiGate-1000A 製品も、既存のネットワークに容易に導入できます。さらに、アンチウイルスとコンテンツフィルタリングだけを利用することも、すべてのセキュリティ機能を活かし、完全なネットワーク保護ソリューションとして利用することもできます。高可用性 (HA) 運用とホットスワップ対応の冗長電源により、ミッションクリティカルなアプリケーションの連続動作を実現します。FortiGate-1000A は、FortiGuard™ ネットワークを通じて自動的に更新されます。これにより、最新のウイルス/ワーム/トロイの木馬などの脅威から防御します。FortiGuard サブスクリプションサービスを利用すれば、24 時間 365 日休むことなく更新を受け取ることができます。

複数の脅威に対応し、コスト効率の高いセキュリティを提供する FortiGate-1000A システム

統合型ネットワークベースのアプリケーションセキュリティ

- ・アンチウイルス (アンチスパイウェア含む)
- ・IPS (不正侵入検知・防御)
- ・Web コンテンツフィルタリング
- ・アンチスパム
- ・ステートフルファイアウォール/帯域制御

柔軟な VPN 機能

- ・IPSec VPN
- ・SSL VPN
- ・L2TP, PPTP

新しい技術や脅威への対応

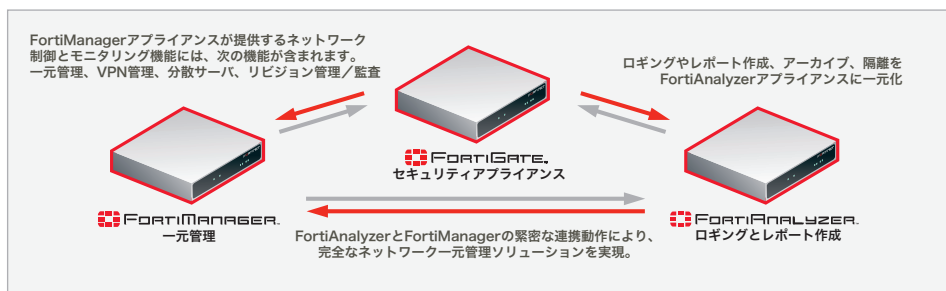
- ・VoIP
- ・IM (インスタントメッセージ)、P2P
- ・フィッシング
- ・複合型脅威

各セキュリティ機能のサブスクリプションはクライアントライセンス無制限なので、総所有コスト (TCO) を低減できます。

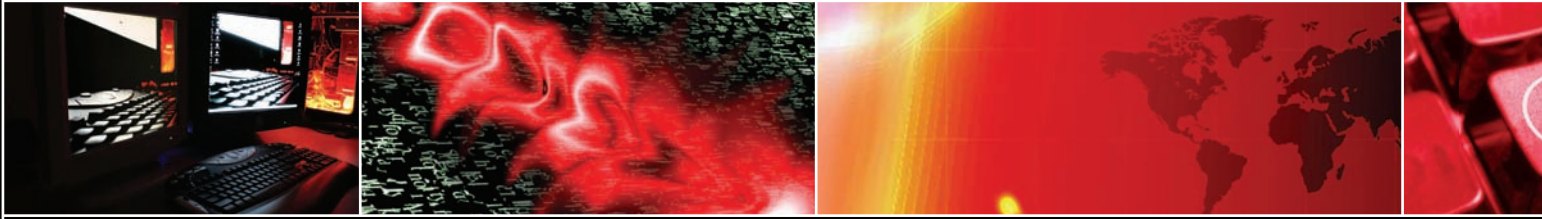


高度なセキュリティソリューション

FortiGate-1000A/FA2 システムは、強固なセキュリティプラットフォームで、重要な各種セキュリティ機能を提供します。信頼性や有用性、迅速な導入、低運用コスト、そして特に、既知と未知とのかかわらず、変則的な脅威に対しても、優れた検知率を達成しました。FortiGate セキュリティシステムのサブスクリプションサービスを利用すれば、プロアクティブにリアルタイムで脅威を検知できます。フォーティネットは、価値や性能、機能のどの面においても、最高のサービスを提供します。



FORTIGATE™ 1000A



POWERFUL

ステートフルファイアウォールから、アンチウイルス (アンチスパイウェア含む)、IPS (不正侵入防御)、IPSec、SSLVPN、アンチスパム、Web コンテンツフィルタリング、FortiGuard サブスクリプションサービスまで、すべての機能を 1 つのセキュリティソリューションに搭載しました。

INTELLIGENT

プロアクティブにネットワークベースの脅威をリアルタイムに検知できます。ウイルスやワーム、トロイの木馬、スパイウェアなどの悪質なコンテンツをはじめ、最新の攻撃を検知して不正侵入を阻止します。

SOPHISTICATED

フォーティネットのダイナミックスレット (脅威) 防御システムは、業界で初めて統合型の脅威相関性分析エンジンを採用しました。このシステムには、ステートフルインスペクション、シグニチャマッチング、ディープ・パケット・インスペクション、ヒューリスティック、プロトコル・アノマリ・チェック、フルコンテツ再構成、アクティビティ・インスペクションなどが組み込まれています。

どの FortiGate プラットフォームでも、ポリシーベースの Web UI や一元管理向けの FortiManager™ を介して容易に管理できます。FortiManager は、1 台のコンソールで数百台の FortiGate 機器の設定変更やポリシー変更を管理できます。このような一元管理により、すべての FortiGate プラットフォームに対して確実にポリシーが適用されていることを保証します。FortiAnalyzer™ は、ロギング機能の一元化を実現しました。一元管理されているすべての FortiGate プラットフォームからログを収集して分析します。FortiManager と FortiAnalyzer の連携により、完全なネットワーク管理のための統一アーキテクチャを実現しました。

セキュリティサービスの自動更新

FortiGate セキュリティシステムには、最新の脅威にする予防効果があります。FortiGuard サブスクリプションサービスをオプションとして追加すると、フォーティネットが新たな脅威を検知してから数分以内にシグニチャの自動更新が可能です。

FortiGate サブスクリプションサービスは、フォーティネットのグローバルな FortiGuard Distribution Network (FDN) を通じて提供されます。FDN は日本を含む世界 10 か所に冗長化構成の高速センターを配置して、ノンストップで稼働させています。シグニチャや検知エンジンの重要な更新は、以下に示すように、ネットワーク環境に応じて最も適した方法で入手できます。

- ・自動更新 (プッシュ型)。FDN ネットワークからフォーティネット製品へ通知し、自動的に更新します。
- ・定期更新 (プル型)。指定したスケジュールで更新します。
- ・即時更新 (手動更新)。手動で更新します。

FortiGuard Web コンテンツフィルタリングやアンチスパムなどのセキュリティ・フィルタリングサービスは、閲覧が許可されていない Web サイトやスパムメールからネットワークやユーザを保護するためのソリューションです。日本語化されたわかりやすい GUI を採用しているため、Web コンテンツフィルタリングもアンチスパムサービスも、非常に簡単に設定できます。数分で高度なセキュリティポリシーを作成することも可能です。フォーティネットの豊富なナレッジベースが利用できるため、業務に無関係なサイトや有害なサイトにアクセスできないようにしたり、迷惑な E メールを速やかに除去したりすることができます。



主要機能	特長
業界で実証済みの複数脅威対応セキュリティアーキテクチャ	統合型アプリケーションセキュリティで、複合型脅威やワーム、ウイルス、トロイの木馬、スパイウェア、フィッシングなどから保護
アンチウイルスと IPS のシグニチャを自動更新	24 時間 356 日の体制で最新の脅威に対応
ネットワークベースの ASIC アプライアンスで、導入と管理を簡易化	ギガビットパフォーマンスにより、ファイアウォールがネットワークのボトルネックになることを回避
VPN (IPSec、SSL) コンテンツのインスペクション	VPN を通じてウイルス感染の拡大や脆弱性の悪用を阻止
導入と管理のコストを低減	セキュリティゾーンやバーチャルドメインにより、複数の顧客や内部のネットワーク群を単一プラットフォームで容易に管理可能
H.323、SIP、IM、P2P などの新しい技術に対応	柔軟な OS で、IM や P2P ソフトウェア、VOIP アプリケーションを細かく制御可能
詳細なロギングとレポート作成のためのツールを提供	FortiAnalyzer と FortiManager アプライアンスは、広範囲にわたるレポート、イベント相関分析、単一コンソールによる管理を提供
柔軟かつスケーラブルな設計	どのようなネットワーク環境 (HA、NAT、Route、トランスペアレント (bridge)) にも対応
RIP、OSPF、BGP4 など、動的ルーティングプロトコルを幅広くサポート	分散型のネットワーク設計にも容易に対応



AUTOMATED

プロテクションの多層化と自動化。リアルタイムで 6000 種以上の脅威に対応します。最新の攻撃に対しても、社内リソースに被害が及ぶ前に阻止します。

EASY TO USE

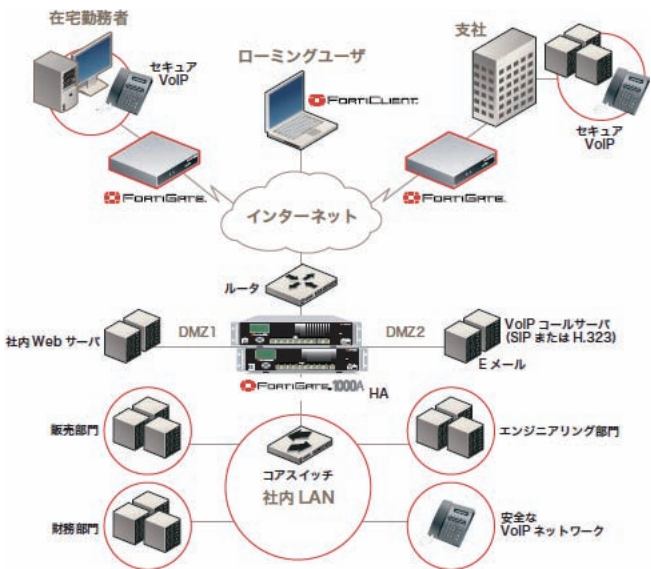
ICSA 認定を受けた各種セキュリティ機能を専用のアプライアンスに組み込みました。インストールも管理も容易です。

AFFORDABLE

FortiGuard セキュリティ・サブスクリプションサービスは、クライアントライセンス無制限です。他社のセキュリティ製品に比べ、運用コストを大幅に削減できます。

STATE OF THE ART

FortiGate のコスト効率の高いソリューションは、業界で評価されている優れた包括的セキュリティサービスです。現在、ネットワークを狙った最新のウイルスや複合型脅威への対策として最適です。



強力なセキュリティ

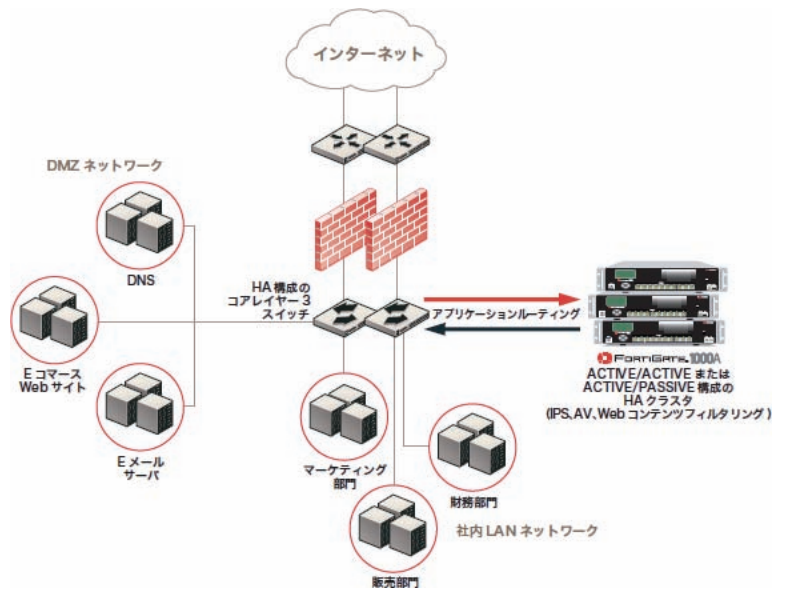
将来想定される攻撃から企業を効果的に保護するには、包括的なセキュリティ戦略が必要です。ネットワークのエッジとコアで、ネットワークベースの防御機能を多層化する必要があります。FortiGate-1000A は、複合型脅威に対抗するために複数のセキュリティソリューションを統合した高性能アプライアンスです。統合されたアンチウイルスとアンチスパイウェアエンジンは、Eメールをはじめ、HTTP や FTP でダウンロードしたファイルに悪意のコンテンツがないかを検査します。ダイナミック IPS は、アプリケーションの脆弱性を狙う攻撃を検知して侵入を阻止します。アンチスパムフィルタリングは、迷惑メールの侵入を阻止します。包括的 Web コンテンツフィルタリングは、有害で悪質なインターネットサイトへのアクセスを阻止します。ステートフルファイアウォールは、防御の最前線に配置します。

柔軟な設計

FortiGate-1000A システムは、柔軟なアーキテクチャで設計されているので、IM や P2P、VoIP アプリケーションといった新しい技術はもちろん、スパイウェアやフィッシング、ファームウェアといった脅威にも、迅速に対応できます。

FortiGate-1000A の運用モードには、NAT や Route、トランスパレント (透過型) があります。目的に応じて、柔軟な選択ができるので、ほとんどのネットワークに対応できます。FortiGate-1000A のコアネットワーク機能には、高可用性 (HA) のほかに、RIP や OSPF、BGP などの動的ルーティングプロトコルのサポートもあります。最大限のネットワーク可用性を要求する複雑なフルメッシュネットワーク環境にも対応できます。

運用コストを削減するため、FortiGate-1000A アプライアンスは、セキュリティゾーンとバーチャルドメインをサポートします。管理が容易な単一プラットフォーム上で、複数の内部ネットワークや外部の顧客の安全を確保します。





モデム 10/100/1000Base-T ポート(銅線) コンソール用ポートと USBポート



ホットスワップ可能な 冗長電源

システム仕様

インターフェース	FGT-1000A	VPN	FGT-1000A	ネットワーク	FGT-1000A
10/100/1000Base-Tポート(銅線)	10	PPTP、L2TP、IPSec	Yes	マルチWANリンクのサポート	Yes
FortiAccel SFPポート	2*	専用トンネル数	5000	DHCPクライアント/サーバ/リレー	Yes
モデムポート	1	暗号化(DES、3DES、AES)	Yes	ゾーン間のルーティング	Yes**
USBポート	1	SSL	Yes**	ポリシーベースのルーティング	Yes
コンソール用ポート	1	SHA-1またはMD5を用いた認証	Yes	VLANタギング(802.1q)	Yes
システム性能		PPTP、L2TP、VPNクライアントパ ススルー	Yes	システム管理	
同時セッション数	60万	ハブ&スポークVPNアーキテクチャ	Yes	コンソール用インターフェース (RS-232)	Yes
新規セッション数/秒	1万5000	IKE証明書による認証(X.509)	Yes	WebUI (HTTPS)、コマンドライン インターフェース	Yes
ファイアウォールスルーット(Gbps)	2	IPSec NATトランパサル	Yes	多言語サポート	Yes
168ビット3DESスルーット(Mbps)	250	Aggressiveモード	Yes	SSH	Yes
無制限の同時ユーザ	Yes	リプレイ保護	Yes	FortiManager™システム	Yes
ポリシー	3万	デッドピア検知	Yes	管理	
スケジュール	256	VPNトンネルモニター	Yes	役割ベースの管理	Yes
ウイルス/スパイウェア/ワーム/ トロイの木馬への対策		アンチスパム		マルチ管理者、マルチ・ユーザレベル	Yes
HTTP、SMTP、POP3、IMAP、FTP、 IM、暗号化VPNトンネルのスキャン	Yes	RBL/ORDBSサポート	Yes	TFTPとWebUI経由での更新と変更	Yes
感染メッセージの隔離	Yes	FortiGuardアンチスパムをサポート MIMEヘッダのチェック	Yes	ユーザ認証	
ファイルのサイズと拡張子によるブ ロック/除外	Yes	キーワード/フレーズによるフィル タリング	Yes	内部データベース	Yes
IMでのファイル転送のスキャン	Yes**	IPアドレスのブラックリスト/除外 リスト	Yes	外部のLDAP/RADIUSデータベース のサポート	Yes
不正侵入の動的阻止		ロギング/モニタリング		RSA SecureID	Yes
プロトコルノマリ検知	Yes	リモートSyslog/WELFサーバへのロ グ出力	Yes	IPSec VPN用にXauth over RADIUSをサポート	Yes
包括的な攻撃シグニチャ	Yes	SNMP	Yes	IP/MACアドレスバインディング	Yes
カスタマイズ可能な検知シグニチャ	Yes	グラフィカル表示によるリアルタイ ムおよび時系列モニタリング	Yes	Windows Active Directory	Yes**
P2Pブロッキング	Yes	ウイルスや攻撃をEメールで通知	Yes	トラフィック管理	
ファイアウォールのモード		FortiAnalyzerをサポート	Yes	DiffServサポート	Yes
NAT、PAT、トランスベアレント(透 過型)、Routeの各種モード	Yes	リアルタイムに機器をモニターする ためのWebダッシュボード	Yes	ポリシーベースの帯域制御	Yes
ポリシーベースのNAT	Yes	高可用性(HA)		帯域幅の下限/上限/優先権の設定	Yes
バーチャルドメイン	10(TP)、2(NAT)	クラスタリング	Yes	動的ルーティング	
セキュリティアゾーン	Yes	Active/ActiveとActive/Passive HA	Yes	RIP v1、v2	Yes
ユーザ/グループに基づく認証	Yes	ステータフル・フェイルオーバー (FW、VPN)	Yes	BGP4	Yes**
カスタマイズ可能な保護プロフィール	200	機器故障の検知と通知	Yes	OSPF	Yes
H.323、SIPアプリケーションレイ ヤゲートウェイ	Yes	冗長電源(ホットスワップ可能)	Yes	静的ルーティング	Yes
コンテンツフィルタリング				IMのアクセス制御	
URL/キーワード/フレーズによる ブロック				AOL-IM	Yes
URL除外リスト	Yes			Yahoo	Yes
Javaアプレット、クッキー、Active Xのブロック	Yes			MSN	Yes
FortiGuard Webコンテンツフィル タリングをサポート	Yes			ICQ	Yes
リアルタイム自動更新	Yes				

* FGT-1000AFA2で利用可能
** FortiOS-3.0で利用可能

FortiGuardサブスクリプションサービス

サービスの内容

- ・自動更新。高速データベースサーバを冗長化構成として世界各地に設置しました。
- ・ウイルスの侵入阻止。6万種類以上のウイルスが登録されたFortiGuardデータベースから作成した完全なワイルドリストにより、4500以上の活動中のウイルスに対応しました。
- ・リアルタイムのシグニチャ・アップデートで6000種類以上の脅威に対応しました。
- ・サイトの分類。Webサイトを56のカテゴリに分けて、Webコンテンツフィルタリングの精度を向上させました。
- ・ドメインとページの評価。Webコンテンツフィルタリングの対象として評価したドメインは2600万件以上、Webページは20億件以上に達しました。

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/>