

ネットワークの保守サービス

TEC-World (ヘルプデスクサービス)

ヘルプデスク専用の Web サイトからインシデント制にて技術的なお問い合わせを行うことが可能です。

<https://hds.networld.co.jp>

- 対応内容
- Web によるテクニカルサポート

ブラウザベースの当社ヘルプデスクシステム「TEC-World」により下記内容をサポートいたします。

- ・セットアップ方法の確認
- ・操作、設定方法に関する技術上の助言
- ・障害についての回避策、対応策等の助言

- 最新版ファームウェア (修正パッチ / モジュール) へのアップグレード



有償保守サービス

センドバック保守	平日 9:00 ~ 17:00 ※
先出しセンドバック保守	平日 9:00 ~ 17:00、翌営業日対応※
オンサイト保守	① 平日 9:00 ~ 17:00、翌営業日対応※ ② 平日 9:00 ~ 17:00、4 時間対応目標※ ③ 24 時間 365 日、4 時間対応目標
ヘルプデスクサポート (ソフトウェアサポート)	平日 10:00 ~ 12:00、13:00 ~ 17:30 ※

※祝祭日および年末年始など、弊社休業日除く

- 先出しセンドバック保守
 - ・ 一次切り分け後の障害コールの受付
 - ・ 代替品の郵送による交換
 - ・ 代替交換品は、メーカー出荷時の状態にて発送します。設置およびインストール作業は、お客様にてお願いいたします。
- オンサイト保守
 - ・ 一次切り分け後の障害コールの受付
 - ・ オンサイトでの障害機交換作業、設置および Config file のリストア作業 (リストア作業は、お客様が設定データを保管されている場合に限りさせていただきます)
 - ・ 代替交換作業後の動作確認 (動作確認は保守対象機器の範囲に限りさせていただきます)

株式会社ネットワークド <http://www.networld.co.jp/>

お問い合わせ forti-info@networld.co.jp

本社 〒101-0051 東京都千代田区神田神保町2-11-15 住友商事神保町ビル TEL:03-5210-5080
関西支店 〒530-0001 大阪市北区梅田3-3-20 明治安田生命大阪梅田ビル 24F TEL:06-7664-5400
中部支店 〒451-6008 名古屋市中区牛島町6-1 名古屋ルーセントタワー 8F TEL:052-588-7611
九州支店 〒812-0013 福岡市博多区博多駅東2-6-1 九勤筑紫通ビル 3F TEL:092-461-7815

*記載されている会社名および製品名、ロゴは各社の商標または登録商標です。 2015年06月

FORTINET

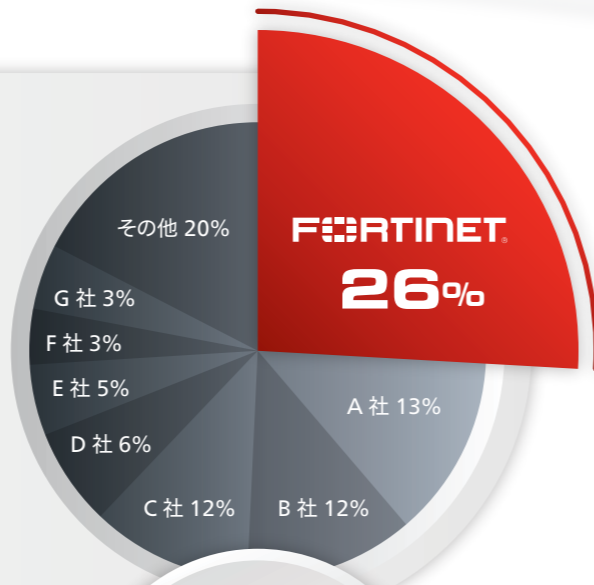
Networld

Fortinet 製品総合カタログ

フォーティネット



革新的なプラットフォームでシンプルかつ確実にビジネスを守る



※出典: IDC's Worldwide Quarterly Security Appliance Tracker - 2014 Q4 (出荷台数)

標的型攻撃をはじめとする種々のセキュリティ脅威がもたらす被害の規模拡大。スマートデバイスの普及やワークスタイルの多様化に伴う無線トラフィックの増加。そして、企業や行政の施策に伴う新たなセキュリティ要件への対応。

ネットワークセキュリティをめぐる状況は、依然として大きな変化の中にあります。

多くの企業にとって、重要な資産となった多様な情報を保護し、安全に業務を継続できる環境を維持することは社会的責任の1つです。一方で、より高い投資対効果を実現すべく、コストや運用管理性、パフォーマンスにも注意を払う必要があります。

変化するビジネス環境、セキュリティ状況に迅速に対応し、求められる多層的な防御をシンプルかつ確実に実現するために。

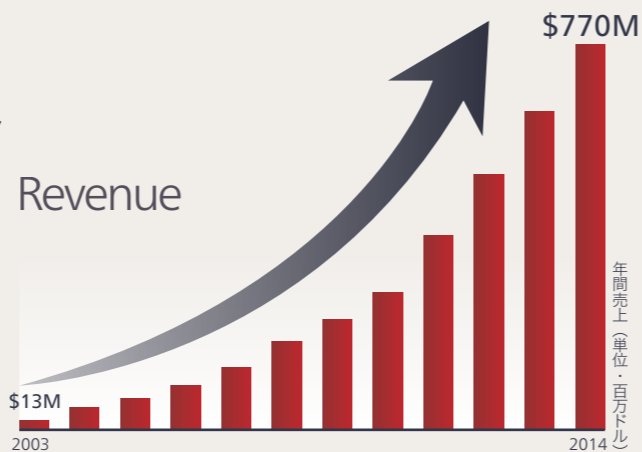
フォーティネットは、ネットワークセキュリティの領域にとどまらず、エンドポイントからアプリケーションなどの境界や大規模エンタープライズのセキュリティまで、幅広い製品ラインアップでお客様のビジネスを守ります。



※バーチャルアプライアンス版もラインアップしています。

セキュリティ市場で成長を続けるフォーティネット

フォーティネットは、通信事業者、データセンター、エンタープライズ、分散型オフィスに幅広く対応する次世代ファイアウォールや UTM (統合脅威管理) をはじめとする、優れたネットワークセキュリティアプライアンスをグローバルに提供しています。自社開発の独自 ASIC (専用プロセッサ)、ハードウェア、ソフトウェア、管理機能、そしてセキュリティ対策の研究において革新を続けており、市場において他社を圧倒する優れたパフォーマンスの製品を常に提供しています。



導入から運用支援まで充実した体制を誇るネットワーク

ネットワークは、フォーティネット製品の正規ディストリビューターとして「Advanced CSP (Advanced Certified Service Partner)」の認定を受けており、高い技術力とサポート力で顧客の課題解決を支援します。フォーティネット製品に関する技術情報やサポート情報を幅広く公開し、専用の Web サイトから問い合わせができるヘルプデスクサービスも提供しています。また、マンガ形式の利用事例紹介といったユニークな取り組みなど、情報発信とユーザー支援を積極的に展開しているのもポイントです。
 →サポートサービスについては、裏表紙をご覧ください。
 →マンガ形式のソリューション紹介はこちら
<http://www.networkworld.co.jp/fortinet/manga/>



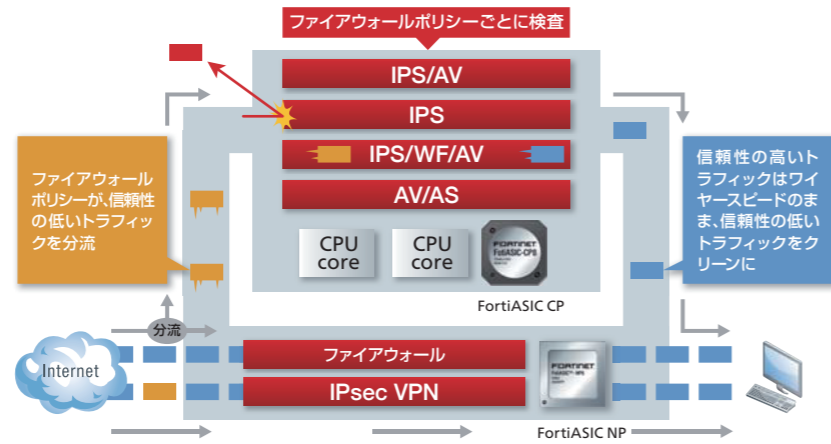
FortiGate UTM シェア No.1 の理由

ファイアウォール中心の対策から次のステージへ
FortiGate は、巧妙化するセキュリティ脅威への対策と TCO 削減を両立します。

高速

世界最速の驚異的な性能

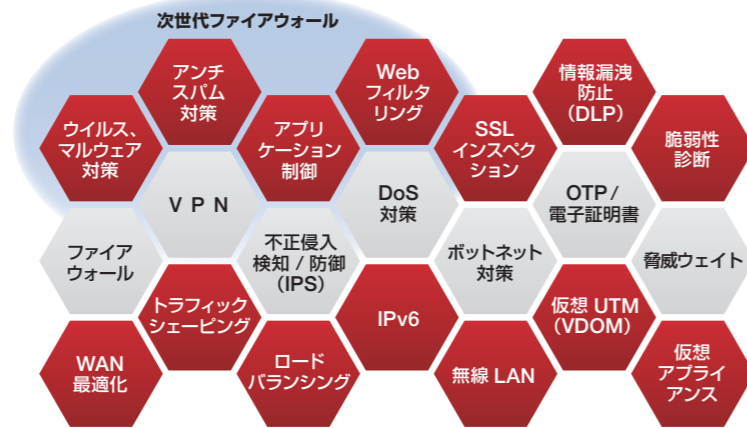
セキュリティアプライアンスのパフォーマンスはその心臓部であるプロセッサによって決まります。FortiGate は、独自に開発した専用プロセッサ FortiASIC を搭載。他社を凌駕する圧倒的なパフォーマンスを実現しています。一般的な UTM は、汎用プロセッサを採用しているために当然、性能に限界があります。フラッグシップモデルである FortiGate-5000 シリーズのファイアウォール スループットは世界最速の 1.12Tbps という驚異的なパフォーマンスを達成しています。



多機能

フルラインの多彩な機能

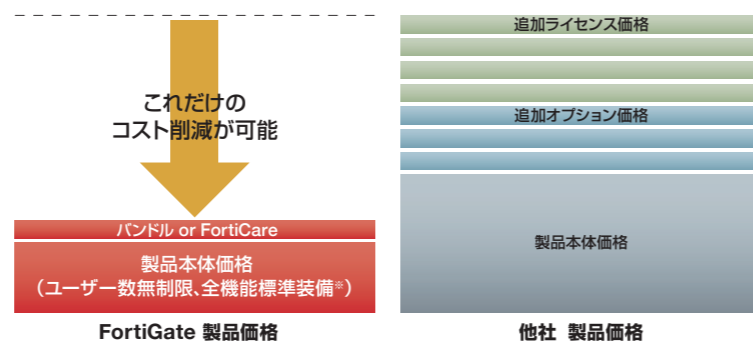
FortiGate は、ウイルス / マルウェア対策、スパムメール対策、アプリケーション可視化と制御、Web フィルタリングから無線 LAN コントローラや仮想 UTM まで、フルラインのセキュリティ機能とネットワーク機能をすべて 1 台の製品に統合しています。ハードウェアソフトウェア、サービスすべてを自社開発・提供し、操作性に優れた日本語 GUI で導入も管理も容易。また、シンプルな価格体系によって導入後に利用する機能を順次増やすことができます。



安価

圧倒的なコストパフォーマンス

他社製品の多くは、ユーザー数をもとにしたライセンス体系としているため、ユーザー数の増加とともにコストが大きく増加します。しかし、FortiGate ならそんな心配も不要です。アプライアンス単位のライセンスによって、価格体系もとてもシンプル。ユーザー数無制限ライセンスで、圧倒的なコストパフォーマンスを実現しています。
※一部オプション機能があります。



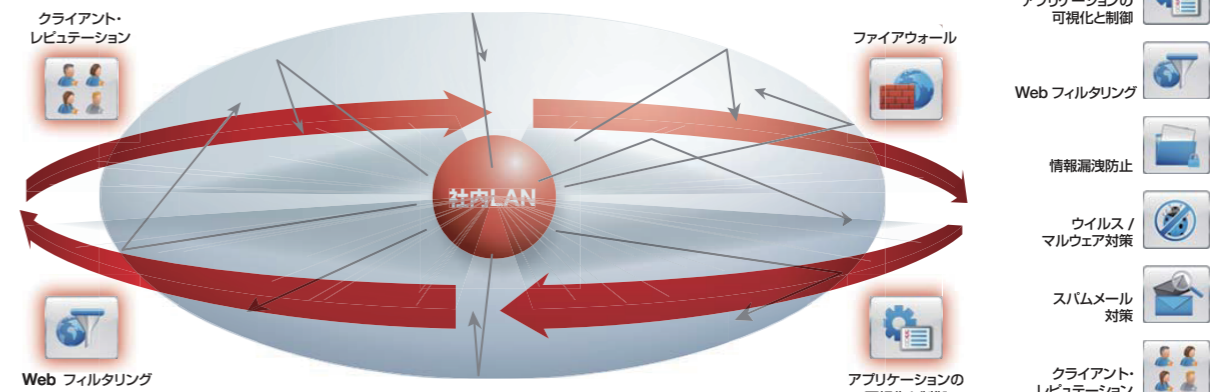
刻一刻と変化し増加の一途をたどる 外部からの脅威への防御は強固でしょうか？

インターネットを介した企業ネットワークへの攻撃はますます巧妙化するばかりです。なかでも近年増加しているのが、特定の企業や団体を狙った標的型攻撃。この攻撃の多くはウイルスや悪意のあるファイルなどを添付したメールが使用され、脅威を秘めたスパムメールは増加の一途をたどっています。FortiGate は、このような企業ネットワークへのインバウンド攻撃を、ファイアウォールや不正侵入検知 / 防御、ウイルス / マルウェア対策、スパムメール対策をはじめとする複合的かつ先進のセキュリティ機能で防御します。



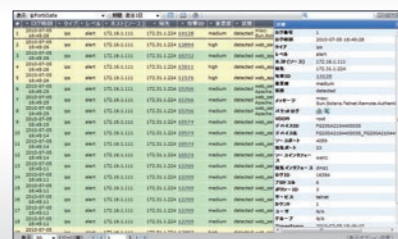
標的型攻撃に備えるためには 内部から外部へ情報を出さない防御も重要です

次々と新種の脅威が出現する現在、外部からの脅威に備えるインバウンド防御だけでは完璧とは言えません。「内部から外部へ」というアウトバウンド防御も併せて導入することが重要です。FortiGate は、このアウトバウンド防御においても多層的なセキュリティ機能を提供します。危険を秘めた Web サイトへのアクセスをあらかじめ防止したり、もしもウイルスが侵入した場合も情報漏洩を阻止することが可能です。



自動アップデートで最新の脅威に対抗「不正侵入検知 / 防御 (IPS)」

社内ネットワークに侵入しようとする脅威に対して最新の防御機能を提供します。8,200[※]以上のシグネチャによる IPS ライブラリを用意。自動アップデートによって、最新の脅威に対抗する強固な防御を可能にします。
※ 2014 年 5 月現在



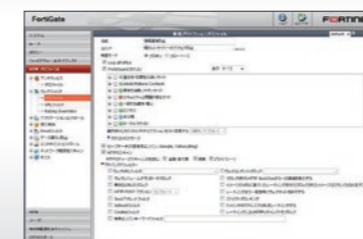
ネットワーク内に潜伏中の脅威を発見する「脅威ウェイト」

クライアントごとに通信やアプリケーションの利用状況を分析。その「振る舞い」を評価し、スコア化することで脅威の状況をランキング形式でレポート。マルウェアを潜伏中に発見することで、情報の漏洩を未然に防ぎます。



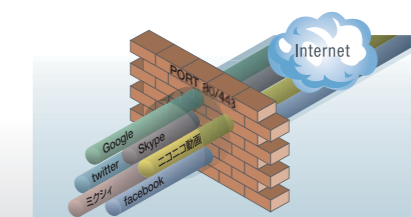
アクセスを制御して情報漏洩を防止する「Web フィルタリング」

脅威を秘める未承認の Web サイトへのアクセスを遮断します。全世界 2 億 5,000 万[※]以上の URL を、6 グループ・79 カテゴリーに分類し、カテゴリーごとにアクセスを制御。未分類の URL へのアクセスを遮断することで、情報漏洩を防止できます。
※ 2014 年 5 月現在



3,200[※]種以上のアプリケーションに対応する「アプリケーションの可視化と制御」

ユーザー認証と組み合わせ、ユーザーごとのアプリケーションの使用状況を可視化して制御し、また、アプリケーションごとに帯域幅も制御できます。ミクシィやニコニコ動画など、日本発のアプリケーションのほか、Skype、YouTube など全世界の 3,200[※]種以上のアプリケーションの制御を日本語 GUI の管理画面で行えます。
※ 2014 年 5 月現在



FortiGate/FortiWiFi

FortiGate/FortiWiFi は、豊富な機能と高い性能を兼ね備え、優れたコストパフォーマンスを実現している統合型ネットワークセキュリティソリューションです。
 自社開発のハードウェアとソフトウェア、専用プロセッサの搭載など数々の特長を活かして、高度化、多様化するネットワーク上の脅威に漏れなく対応。小規模から大規模まで、幅広いニーズに対応する豊富なモデルをラインアップしています。
 また、世界 6 カ所のセキュリティ研究センターが 24 時間 365 日の運用体制でセキュリティ脅威の変化を常に把握。最新のシグニチャ配信、ポータルサイトを通じたセキュリティ専門家の情報発信など、安心を保つ取り組みを提供しています。

ローエンドモデル



ミッドレンジモデル



ハイエンドモデル



バーチャルアプライアンス

FortiGate-VM00 / VM01 / VM02 / VM04 / VM08

FortiGate/FortiWiFi 主な仕様

	FortiWiFi-30D FortiGate-30D	FortiWiFi-60D FortiGate-60D	FortiWiFi-90D FortiGate-90D	FortiGate-100D	FortiGate-200D	FortiGate-300D	FortiGate-500D
ファイアウォールスループット (1518 / 512 / 64 バイト UDP パケット)	800 / 800 Mbps	1.5 / 1.5 / 1.5 Gbps	3.5 / 3.5 / 3.5 Gbps	2,500 / 1,000 / 200 Mbps	3 / 3 / 3 Gbps	8 / 8 / 8 Gbps	16 / 16 / 16 Gbps
ファイアウォールレイテンシ	8 μs	4 μs	4 μs	37 μs	2 μs	3 μs	3 μs
ファイアウォール同時セッション	200,000	500,000	2 M	3M	1.4 M	6 M	6 M
ファイアウォール新規セッション / 秒	3,500	4,000	4,000	22,000	77,000	200,000	280,000
ファイアウォールポリシー	5,000	5,000	5,000	10,000	10,000	10,000	10,000
IPSec VPN スループット	350 Mbps	1 Gbps	1 Gbps	450 Mbps	1.3 Gbps	7 Gbps	14 Gbps
ゲートウェイ間 IPSec VPN トンネル	20	200	200	2,000	2,000	2,000	2,000
クライアント-ゲートウェイ間 IPSec VPN トンネル	250	500	1,000	5,000	5,000	10,000	10,000
SSL VPN スループット	25 Mbps	30 Mbps	35 Mbps	300 Mbps	400 Mbps	350 Mbps	400 Mbps
同時 SSL VPN ユーザー (推奨)	80	100	200	300	300	500	500
IPS スループット	150 Mbps	200 Mbps	275 Mbps	950 Mbps	1.7 Gbps	2.8 Gbps	4.7 Gbps
アンチウイルススループット (プロキシベース / フローベース)	30 / 40 Mbps	35 / 50 Mbps	35 / 65 Mbps	300 / 650 Mbps	600/1,100 Mbps	1.4 / 2.5 Gbps	1.7 / 3.4 Gbps
FortiAP サポート数 (合計 / トンネルモード)	—	10 / 5	32 / 16	64 / 32	64 / 32	512 / 256	512 / 256
FortiToken サポート数	20	100	100	1,000	1,000	1,000	1,000
FortiClient サポート数	10	200	200	2,000	2,000	600	2,000
仮想 UTM (VDM: 標準 / 最大)	—	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10
インタフェース	5 x GbE	10 x GbE	16 x GbE	2 x GbE/SFP 共有、 18 x GbE、2 x HA	2 x GbE SFP、 18 x GbE	4 x GbE SFP、 6 x GbE	8 x GbE SFP、 10 x GbE
無線インタフェース	IEEE 802.11 a/b/g/n (FortiWiFi)	IEEE 802.11 a/b/g/n (FortiWiFi)	IEEE 802.11 a/b/g/n (FortiWiFi)	—	—	—	—
ストレージ	—	—	32 GB	32 GB	64 GB	120 GB	120 GB
冗長電源 (ホットスワップ対応)	—	—	—	—	—	—	—
形状	デスクトップ	デスクトップ	デスクトップ	ラックマウント (1 RU)	ラックマウント (1 RU)	ラックマウント (1 RU)	ラックマウント (1 RU)

	FortiGate-800C	FortiGate-1000D	FortiGate-1500D	FortiGate-3240C	FortiGate-3600C	FortiGate-3700D	FortiGate-3950B
ファイアウォールスループット (1518 / 512 / 64 バイト UDP パケット)	20 / 20 / 20 Gbps	52 / 52 / 33 Gbps	80 / 80 / 55 Gbps	40 / 40 / 40 Gbps	60 / 60 / 60 Gbps	160 / 160 / 110 Gbps	20 - 120 / 20 - 120 / 20 - 120 Gbps
ファイアウォールレイテンシ	6 μs	3 μs	3 μs	4 μs	4 μs	2 μs	4 μs
ファイアウォール同時セッション	7 M	11 M	12 M	10 M	28 M	50 M	20 M
ファイアウォール新規セッション / 秒	190,000	240,000	250,000	200,000	235,000	300,000	250,000
ファイアウォールポリシー	10,000	100,000	100,000	100,000	100,000	100,000	100,000
IPSec VPN スループット	8 Gbps	30 Gbps	50 Gbps	17 Gbps	25 Gbps	100 Gbps	8 - 50.5 Gbps
ゲートウェイ間 IPSec VPN トンネル	2,000	20,000	10,000	10,000	10,000	40,000	10,000
クライアント-ゲートウェイ間 IPSec VPN トンネル	50,000	50,000	50,000	64,000	64,000	64,000	64,000
SSL VPN スループット	1.3 Gbps	3.6 Gbps	4 Gbps	3.4 Gbps	5.3 Gbps	10 Gbps	1.2 Gbps
同時 SSL VPN ユーザー (推奨)	10,000	10,000	10,000	30,000	30,000	30,000	25,000
IPS スループット	6 Gbps	8 Gbps	11 Gbps	8 Gbps	14 Gbps	23 Gbps	5 - 20 Gbps
アンチウイルススループット (プロキシベース / フローベース)	1.7 / 3.1 Gbps	3.5 / 5.5 Gbps	4.3 / 13 Gbps	2.6 / 9 Gbps	5.8 / 18 Gbps	7.5 / 18 Gbps	4 / 5 - 15 Gbps
FortiAP サポート数 (合計 / トンネルモード)	1,024 / 512	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024
FortiToken サポート数	1,000	5,000	5,000	5,000	5,000	5,000	5,000
FortiClient サポート数	2,000	8,000	8,000	8,000	8,000	8,000	20,000
仮想 UTM (VDM: 標準 / 最大)	10 / 10	10 / 250	10 / 250	10 / 500	10 / 500	10 / 500	10 / 500
インタフェース	2 x 10 GbE SFP+, 8 x GbE/SFP 共有、 14 x GbE、 2 x ハイ/ビス ペア	2 x 10 GbE SFP+, 16 x GbE SFP、 18 x GbE	8 x 10 GbE SFP+/ GbE、 16 x GbE SFP、 18 x GbE	12 x 10 GbE SFP+, 10 x GbE SFP、 2 x GbE	12 x 10 GbE SFP+, 16 x GbE SFP、 2 x GbE	4 x 40 GbE QSFP+, 20 x 10 GbE SFP+/ GbE SFP 共有、 8 x 10 GbE SFP+、 2 x GbE	2 - 12 x 10 GbE SFP+、 2 - 102 x GbE、 4 - 104 x GbE SFP
ストレージ	60 GB	120 GB	240 GB	64 GB	128 GB	960 GB	256 GB
冗長電源 (ホットスワップ対応)	オプション	○	○	○	○	○	○
形状	ラックマウント (1 RU)	ラックマウント (2 RU)	ラックマウント (2 RU)	ラックマウント (2 RU)	ラックマウント (3 RU)	ラックマウント (3 RU)	ラックマウント (3 RU)

	FortiGate-VM00	FortiGate-VM01	FortiGate-VM02	FortiGate-VM04	FortiGate-VM08
仮想 CPU (最小 / 最大)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
仮想 NIC 枚数 (最小 / 最大)	2 / 10	2 / 10	2 / 10	2 / 10	2 / 10
メモリ (最小 / 最大)	1 GB / 1 GB	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB	1 GB / 12 GB
ストレージ容量 (最小 / 最大)	30 GB / 2 TB	30 GB / 2 TB	30 GB / 2 TB	30 GB / 2 TB	30 GB / 2 TB

無線LANアクセスポイント ●●

FortiAP

FortiAP は、無線 LAN コントローラ機能を備えた FortiGate/FortiWiFi によって一元的に管理できる無線 LAN アクセスポイントです。統合脅威管理 (UTM) 機能を活用した、包括的に統合されたセキュリティ ソリューションを実現します。



FortiAP-221B



FortiAP-221C



FortiAP-320C

集中レポートシステム ●●

FortiAnalyzer

FortiAnalyzer は、フォーティネット製品をはじめとする syslog 互換の機器からログデータをセキュアに収集します。ユーザーはカスタマイズが容易な総合レポートセットを用いて、さまざまなログを閲覧するとともに、それらのデータマイニングを通じてセキュリティのスタンスを判断することが可能です。



FortiAnalyzer-200D



FortiAnalyzer-1000D



FortiAnalyzer-300D



FortiAnalyzer-3000E

FortiAnalyzerの主な機能

- セキュリティログ分析 ... トラフィックログ・Web フィルタログ、ウイルス検知ログなどさまざまなログを取得可能
- グラフィカルレポート ... 300 種類以上のレポートテンプレートを用意
- コンテンツアーカイビング / データマイニング
- ネットワーク分析
- 悪意のあるファイルの隔離
- 脆弱性評価

● バーチャルアプライアンス

FAZ-VM-BASE / GB1 / GB5 / GB25 / GB100

集中セキュリティ管理 ●●

FortiManager

FortiManager は、複数の FortiGate を効率よく管理するための統合管理・監視アプライアンスです。また、FortiGate ばかりでなく、FortiMail や他のアプライアンスを含めた効率的な一元管理が可能で、導入や設定、監視、保守に関する管理者の作業を大幅に軽減できます。さらに仮想管理機能 (ADOM) をサポートしており、MSSP 事業者などでは管理機能をユーザーに提供できます。



FortiManager-200D



FortiManager-4000E



FortiManager-300D

FortiManagerの主な機能

- 集中管理 ... すべての FortiGate、FortiAnalyzer、FortiClient を一元管理
- 数千台規模のデバイスを操作の容易なユーザーインターフェースで操作
- FortiAnalyzer と統合されたコンソール画面からすべての管理機能を起動可能、ポリシープロビジョニング、およびエスカレーション通知機能などのアラート管理、設定変更および監査制御、VPN マネージャ、配信サーバによる集中的な更新

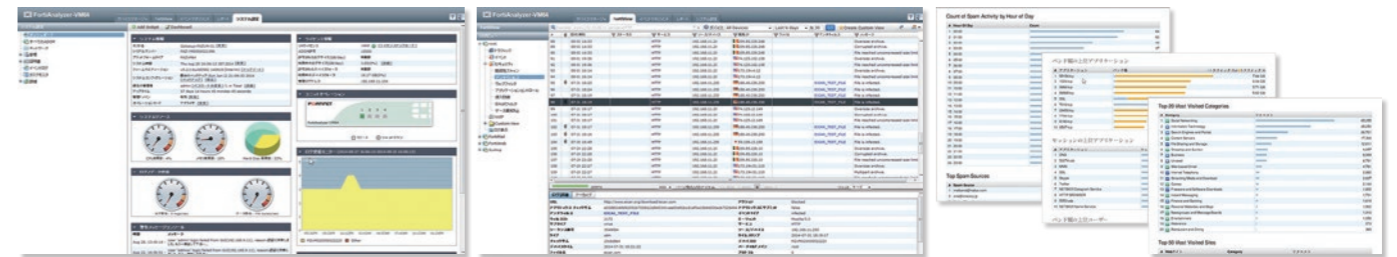
● バーチャルアプライアンス

FortiManager-VM-BASE / 10-UG / 100-UG / 1000-UG / 5000-UG / U-UG

FortiAP 主な仕様

	FortiAP-221B	FortiAP-221C	FortiAP-320C
設置環境 (屋内 / 屋外)	屋内	屋内	屋内およびプレナム
ラジオ数	2	2	2
アンテナ数	4 (内蔵)	4 (内蔵)	6 (内蔵)
Tx/Rx 空間ストリーム (802.11n モード)	2 x 2 MIMO 2 空間ストリーム – 300 Mbps/ ラジオ (合計 600 Mbps)	2 x 2 MIMO 2 空間ストリーム – Radio 1 – 300 Mbps、Radio 2 – 867 Mbps (合計 1,167 Mbps)	3 x 3 MIMO 3 空間ストリーム – Radio 1 – 450 Mbps、Radio 2 – 1,300 Mbps (合計 1,750 Mbps)
同時 SSID	16 (14: クライアントアクセス、2: モニタリング)	16 (14: クライアントアクセス、2: モニタリング)	16 (15: クライアントアクセス、1: モニタリング)
最大送信電力	17 dBm (10 mW/MHz 以下)	20 dBm (10 mW/MHz 以下)	21 dBm (10 mW/MHz 以下)
インタフェース	1 x GbE	1 x GbE	2 x GbE
Power over Ethernet (PoE)	802.3af (15.4W)	802.3af (12.9W)	802.3af (12.9W) をサポートする 2つの冗長 PoE 給電インタフェース

FortiAnalyzer 運用管理画面 / 主な仕様



	FortiAnalyzer-200D	FortiAnalyzer-300D	FortiAnalyzer-1000D	FortiAnalyzer-3000E	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
ログ処理 GB / 日	5 GB	15 GB	25 GB	250 GB	1 GB	+1 GB	+5 GB	+25 GB	+100 GB
セッション数 / 日	18 M	55 M	85 M	850 M	3.5 M	3.5 M	18 M	85 M	360 M
最大ログレート (ログ / 秒: スタンドアロンモード)	350	625	1,000	50,000	—	—	—	—	—
仮想管理 (ADOM) サポート数	150	200	2,000	4,000	—	—	—	—	—
インタフェース	4 x GbE	4 x GbE	6 x GbE、2 x GbE SFP	4 x GbE、2 x GbE SFP	—	—	—	—	—
ストレージ	1 x 1 TB	2 x 2 TB	4 x 2 TB	8 x 2 TB (最大 16 TB)	200 GB	200 GB	1 TB	8 TB	16 TB
RAID ストレージ管理	—	RAID 1	RAID 0、1、5、6、10	RAID 0、1、5、6、10、50、60	—	—	—	—	—

FortiManager 運用管理画面 / 主な仕様



	FortiManager-200D	FortiManager-300D	FortiManager-4000E	FortiManager-VM-BASE	FortiManager-VM-10-UG	FortiManager-VM-100-UG	FortiManager-VM-1000-UG	FortiManager-VM-5000-UG	FortiManager-VM-U-UG
ライセンス承諾ネットワーク 機器数	30	300	4,000	10	+10	+100	+1,000	+5,000	無制限 [®]
仮想管理 (ADOM) サポート数	30	300	4,000	10	+10	+100	+1,000	+5,000	無制限 [®]
管理 Web ポータル数	—	—	4,000	10	+10	+100	+1,000	+5,000	無制限 [®]
Web ポータルユーザー数	—	—	4,000	10	+10	+100	+1,000	+5,000	無制限 [®]
ログ処理 GB / 日	2	2	10	1	2	5	10	25	50
ローカルホスト セキュリティコンテンツ	AV、IPS、VM、WF、AS	AV、IPS、VM、WF、AS	AV、IPS、VM、WF、AS	AV、IPS、VM	AV、IPS、VM	AV、IPS、VM	AV、IPS、VM、WF、AS	AV、IPS、VM、WF、AS	AV、IPS、VM、WF、AS
インタフェース	4 x GbE	4 x GbE	4 x GbE、2 x GbE SFP	—	—	1 / 4 (仮想 NIC 枚数: 最小 / 最大)	—	—	—
ストレージ	1 x 1 TB	2 x 2 TB	8 x 2 TB	—	—	80 GB / 16 TB (最小 / 最大)	—	—	—

※ハードウェア上の制限は 10,000 です。

統合セキュアメールアプライアンス ●●

FortiMail

FortiMail は、FortiGate のメールセキュリティ機能を拡張し、高機能化したメールアプライアンスです。独自 OS をベースにした高速処理が可能で、高機能なアンチスパム / アンチウイルス、コンテンツフィルター、暗号化、アーカイブ、Web メール、カレンダー機能を搭載しています。



FortiMail-200D



FortiMail-1000D



FortiMail-400C



FortiMail-3000D

● パーチャルアプライアンス

FortiMail-VM01 / VM02 / VM04 / VM08

多層型サンドボックス ●●

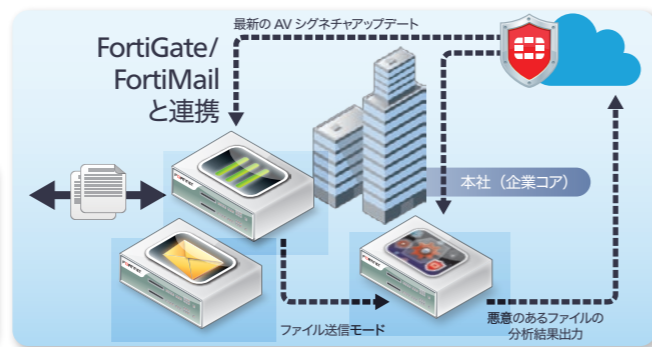
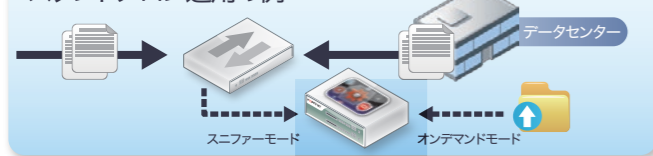
FortiSandbox

FortiSandbox は、プロアクティブな脅威検出と対策機能を提供するとともに、脅威の本質を把握することで実効性の高い対策を可能にする、堅牢で導入の容易な統合ソリューションです。独自の二重構造のサンドボックスを基盤とし、セキュアな仮想ランタイム環境で未知の脅威を事前に発見。未知の脅威に対する対策、脅威の高度な可視化、そして総合的なレポート機能を提供します。



FortiSandbox-1000D
FortiSandbox-3000D

スタンドアロン運用の例



アプリケーションデリバリーコントローラ ●●

FortiADC

FortiADC は、シンプルなサーバロード バランシングからエンタープライズ レベルのグローバル規模のトラフィック分散管理まで、ほぼすべての Web ベースアプリケーションのニーズに対応可能なアプライアンス製品です。



FortiADC-100E



FortiADC-600E



FortiADC-300E



FortiADC-1000E



FortiADC-400E

FortiMail 主な仕様

	FortiMail-200D	FortiMail-400C	FortiMail-1000D	FortiMail-3000D	FortiMail-VM01	FortiMail-VM02	FortiMail-VM04	FortiMail-VM08
メールトランザクション数	76 K	150 K	680 K	1.5 M	76 K	150 K	680 K	1.5 M
アンチスパム + アンチウイルス	58 K	120 K	500 K	1.3 M	58 K	120 K	500 K	1.3 M
管理ドメイン数	50	500	1,000	3,000	50	500	1,000	3,000
メールボックス数 (サーバ モード)	200	1,000	1,500	3,000	200	1,000	1,500	3,000
インタフェース	4 x GbE	4 x GbE	6 x GbE、 2 x GbE SFP	4 x GbE、 2 x GbE SFP	—	—	—	—
ストレージ	1 x 1 TB	2 x 1 TB	2 x 2 TB	2 x 2 TB (最大 12 TB)	50 GB - 1 TB	50 GB - 2 TB	50 GB - 4 TB	50 GB - 8 TB

FortiSandbox 主な仕様

	FortiSandbox-1000D	FortiSandbox-3000D
VM のサンドボックス処理 (ファイル数 / 時)	160	560
AV スキャン処理 (ファイル数 / 時)	6,000	15,000
VM 数	8	28

FortiADC 主な仕様

	FortiADC-100E	FortiADC-300E	FortiADC-400E	FortiADC-600E	FortiADC-1000E
L4 スループット	1.0 Gbps	4.8 Gbps	8.0 Gbps	13.0 Gbps	18.0 Gbps
L7 TPS	19,000	200,000	220,000	280,000	450,000
SSL TPS (2048 キー)	1,000	6,000	24,000	33,000	46,000
メモリ	2 GB	2 GB	2 GB	4 GB	4 GB
ネットワークインタフェース	4 x GbE RJ45 インタフェース	6 x GbE RJ45 インタフェース	8 x GbE RJ45 インタフェース	2 x 10 GbE SFP+ インタフェース、 8 x GbE インタフェース	2 x 10 GbE SFP+ インタフェース、 8 x GbE インタフェース
ストレージ	16 GB SSD	120 GB SSD	120 GB SSD	120 GB SSD	120 GB SSD
管理プロトコル	HTTPS、SSH、CLI、 Direct Console DB9 CLI、 SNMP	HTTPS、SSH、CLI、 Direct Console DB9 CLI、 SNMP	HTTPS、SSH、CLI、 Direct Console DB9 CLI、 SNMP	HTTPS、SSH、CLI、 Direct Console DB9 CLI、 SNMP	HTTPS、SSH、CLI、 Direct Console DB9 CLI、 SNMP

ロードバランサ パーチャルアプライアンス ●●

Equalizer OnDemand



Equalizer OnDemand は、VMware 上でソフトウェアとして動作するパーチャルアプライアンスです。ハードウェアアプライアンスに比べ、低コストで柔軟性のある環境構築を可能とします。

	主な仕様
L4 スループット	1 Gbps
L7 TPS	100,000
SSL TPS (2048 キー)	5,000
最大クラスタ (仮想 IP) 数	無制限ライセンス
仮想 IP あたりのサーバ数	512
対応するハイパーバイザ	VMware ESX / ESXi 4.1 またはそれ以上
システム要件	1 GB RAM、ハードディスク 1 GB の空き容量

ワンタイムパスワード (OTP) トークン ●●

FortiToken

FortiToken は、二要素認証ソリューションを実現する、使いやすさを追求したワンタイムパスワード (OTP) トークンです。セキュリティ管理者は、ユーザーがどこからネットワークへアクセスしても、強化されたセキュリティを提供でき、静的なパスワードなどの単一要素の認証が抱えるセキュリティ侵害のリスクを軽減できます。



エンドポイントセキュリティ ●●

FortiClient

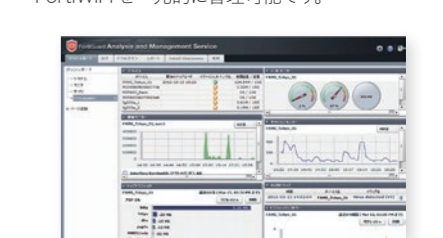
FortiClient は、デスクトップ PC、ノート PC、タブレット、スマートフォンのあらゆるデバイスに対応し、ローカル、リモート、オフィス、モバイルのあらゆる環境で FortiGate と統合して運用できるセキュリティソリューションです。エンドポイント管理の負荷を抑制し、ユーザーとゲストはいつでもどこでも安全に業務を行えます。



クラウド型セキュリティ/ログ管理サービス ●●

FortiCloud

運用管理ソリューションを SaaS 形式で提供するクラウドサービスです。トラフィック分析データ、ウイルス情報や攻撃パターン、FortiGate/FortiWiFi のリソースをリアルタイムに監視、把握できます。また、設定情報の履歴管理、ファームウェアの管理・更新機能などがあり、複数の FortiGate/FortiWiFi を一元的に管理可能です。



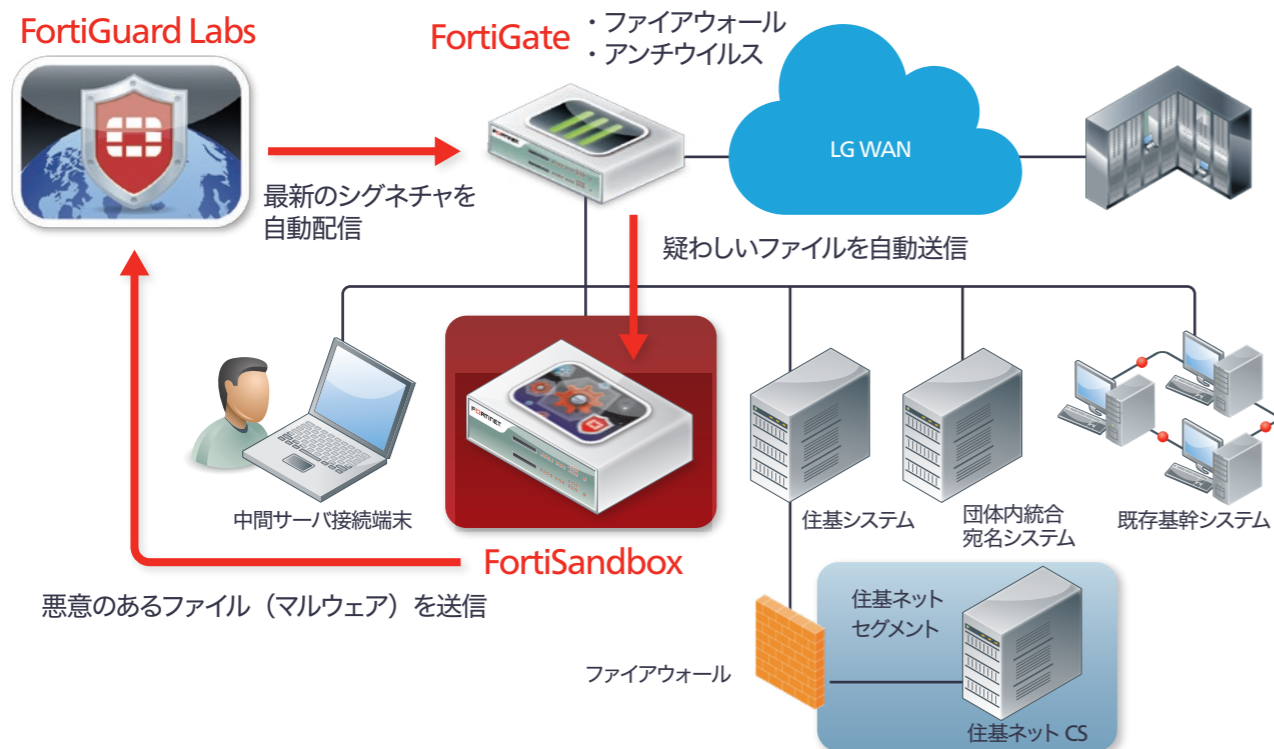
「マイナンバー制度」のセキュリティ対策を FortiSandbox と FortiGate の連携で実現

地方公共団体におけるマイナンバー制度の運用にあたり、所轄官庁の共用ネットワークから中間サーバへの接続におけるセキュリティ対策が示されています。「共用環境（庁内 LAN 接続あり）」の場合、「サンドボックス装置の導入」が『重要』として定義されています。専用環境や共用環境（庁内 LAN 接続なし）の場合でも、サンドボックスの導入は『推奨』とされています。

フォーティネットのサンドボックス製品である FortiSandbox は、検出したゼロデイマルウェアを FortiGuard Labs に自動送信して解析し、新しいシグネチャを生成して迅速に FortiGate へ配信します。これにより、管理者の運用負荷を大きく軽減しながら、セキュリティ強度を大きく高めることが可能となります。

FortiGuard Labs と FortiGate の連携によって防御力は常に強化され、疑わしいファイル判定も最小限で済みます。

1



ここがポイント

- 1 高精度なプレフィルタでゼロデイ脅威を効率的に検出し、脅威の検出までの時間を短縮することが可能!
- 2 検出したマルウェアは FortiGuard Labs に自動送信され、新しいシグネチャの迅速な配信によって攻撃のブロックまで自動化!
- 3 標的型攻撃の侵入経路となる各種プロトコルをシームレスな運用で保護し、初期導入コスト、運用コストも抑制!
- 4 アンチウイルス、アプリケーション制御、Web フィルタリング、アンチスパム、侵入検知など複数のセキュリティ技術と連携し、最適化されたディフェンスを提供!

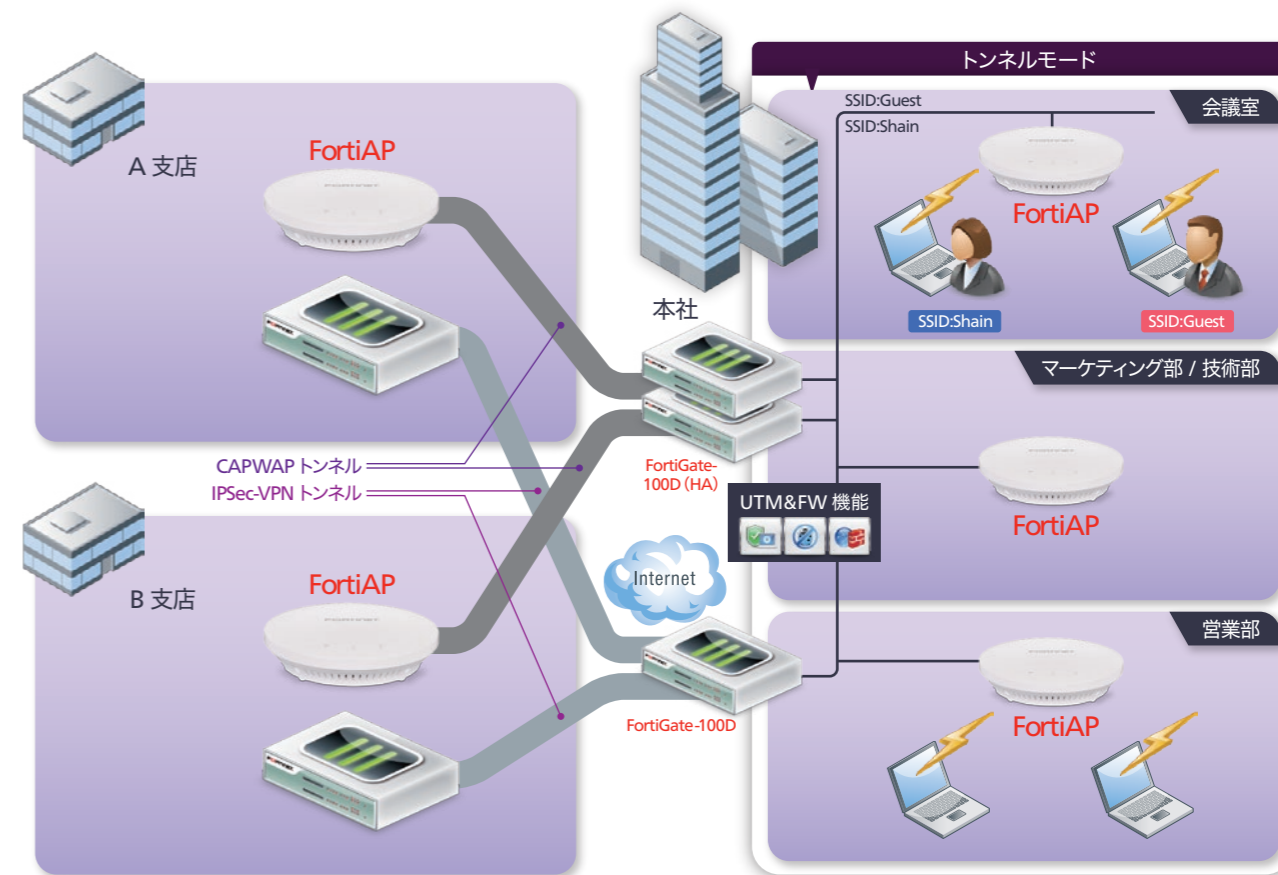
高セキュリティで安定した無線 LAN を FortiGate+FortiAP で実現

会議室にノート PC を持ち込んでミーティングを行うといった光景も当たり前になり、無線 LAN インフラの安定性・接続性は重要になっています。また、無線 LAN 環境のセキュリティ強化も大きな課題です。

フォーティネットの無線 LAN アクセスポイント FortiAP は、FortiGate に備わる無線 LAN コントローラ機能と連携し、安全かつ快適な無線 LAN アクセスを実現します。FortiGate はファイアウォールやアンチウイルス、IPS（不正侵入防止システム）などセキュリティ機能を網羅的に備えており、これらの機能を無線 LAN 端末のトラフィックにも適用することで、パケットをクリーンな状態にした上で社内 LAN に流すことができます。

また、FortiGate では、個々の SSID ごとに異なるセキュリティポリシーを割り当てることが可能で、商談やセミナーなどお客様向けの無線 LAN サービスの展開にも役立ちます。

2



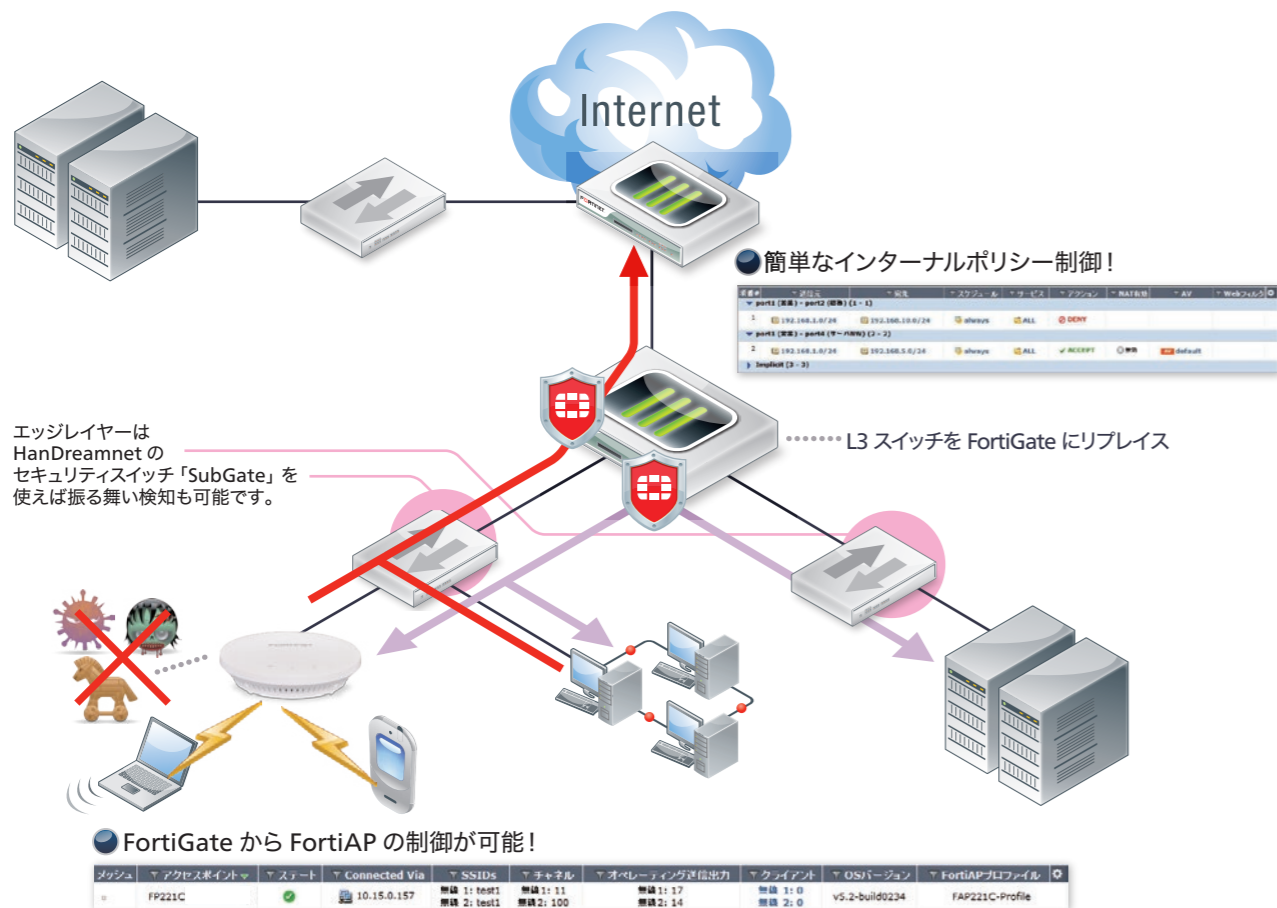
ここがポイント

- 1 最大 50 ユーザー同時接続でも快適に無線 LAN を利用できる環境を実現!
- 2 FortiGate の UTM 機能を適用することで、安全な無線 LAN アクセスを実現!
- 3 FortiGate に標準装備されている無線 LAN コントローラ機能を活かし、低コストで構築!

内部ネットワーク・ファイアウォールとして FortiGate を活用

内部ネットワーク・ファイアウォールとは、企業の L3 スイッチ部分で使用するファイアウォールを指します。これまでファイアウォールはインターネットとのゲートウェイとして使用されてきました。しかし近年ではノート PC やスマートフォンなどモバイルデバイスの普及に伴い、無線を通して社内のネットワークにアクセスする通信に対しては無防備になりがちです。

L3 スイッチを FortiGate にリプレースすることで、社内のセグメントをまたいだ通信に対してきめ細かなポリシー制御やアンチウイルスなどの UTM 機能による強固なセキュリティを簡単に適用できます。さらに FortiAP を組み合わせれば、無線通信に対しても FortiGate のセキュリティ機能を適用可能です。



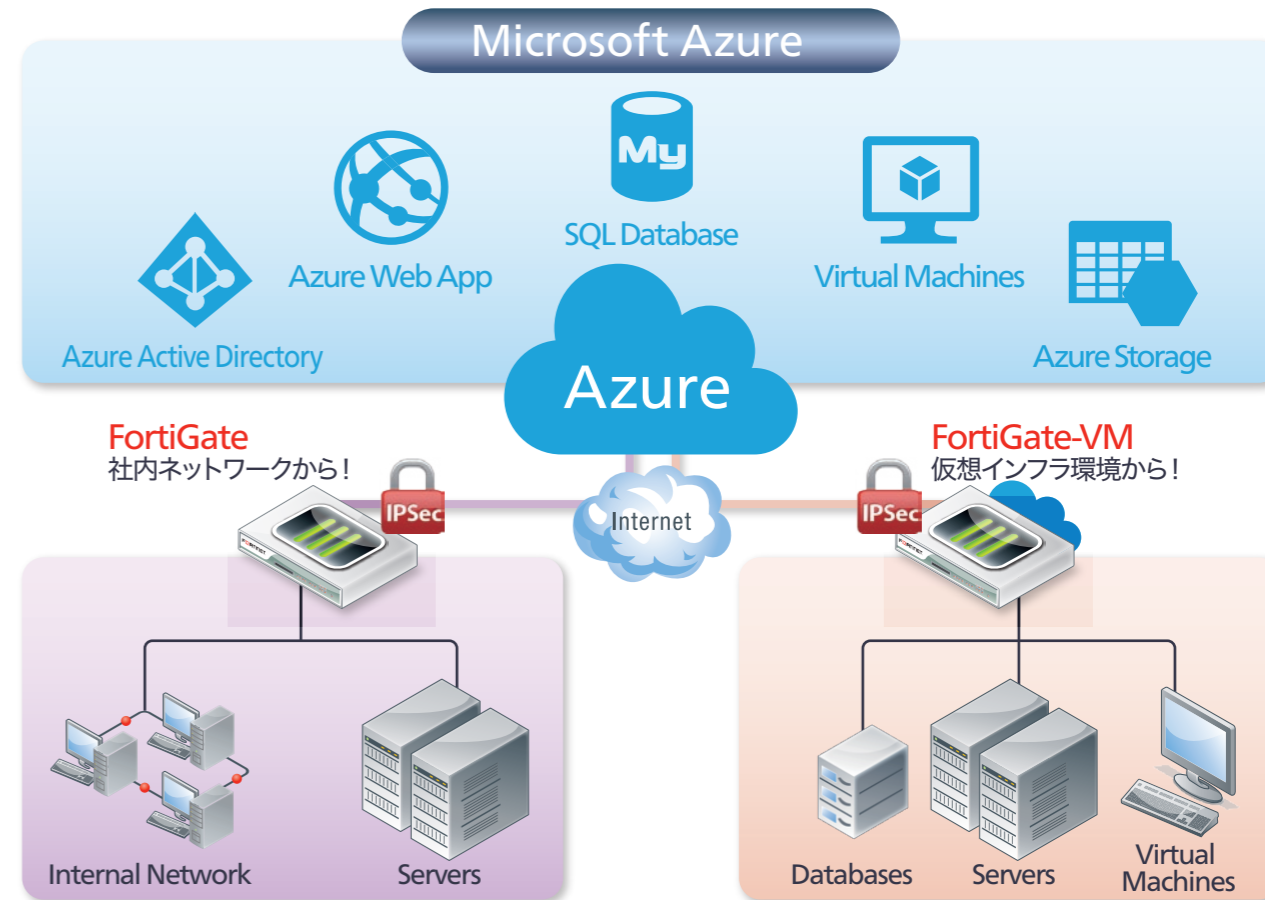
ここがポイント

- 1 内部ネットワーク・ファイアウォールで社内のネットワークに対しても強固なネットワークセキュリティを!
- 2 コマンドラインの煩雑な ACL 制御も、GUI で簡単なインターナルポリシー制御へリプレース!
- 3 FortiAP との組み合わせで、無線通信も FortiGate で制御可能!

VPN による Microsoft Azure へのセキュアアクセス

FortiGate は、マイクロソフトのクラウドプラットフォームである Microsoft Azure へのセキュアなアクセスをサポートしています。クラウドへの情報（データ）移管、インフラ拡張が進む近年、FortiGate が提供する IPsec VPN を利用すれば、社内ネットワークから Microsoft Azure が提供するデータベース、ストレージなどの各種サービスへシームレスかつセキュアにアクセスすることができます。

また、FortiGate パーチャラプライアンスの FortiGate-VM から接続すれば、仮想インフラ環境と Microsoft Azure の間でセキュアなコネクティビティを確立することも可能です。



ここがポイント

- 1 社内ネットワーク & 仮想化インフラ環境 ⇄ Microsoft Azure 間のセキュアなアクセスを提供!
- 2 ファイアウォールを利用して、ユーザー、端末、サービスごとに Microsoft Azure へのアクセスを制御!
- 3 UTM 機能を利用して、社内ネットワークから Microsoft Azure へのウイルスの攻撃、蔓延を防ぐ!

FortiGate-Microsoft Azure 間の IPsec VPN 設定手順を公開中!!
「FortiGate Azure VPN」で検索!!