ネットワールドの保守サービス

TEC-World（ヘルプデスク & FAQ）

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://tec-world.networld.co.jp/login

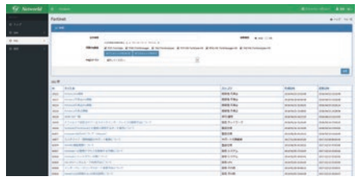
対応内容

● 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、対応策などの助言

● 充実の FAQ

TEC-World FAQ の記載内容は、当社サポート対応の中で出てきた内容を掲載しております。



● 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、祝祭日および年末年始など、弊社休業日を除く> ② 365 日 24 時間< 4 時間駆けつけ目標>
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 ～ 17：00 *

＊祝日および年末年始など、弊社休業日を除く

● 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け付け
・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
（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け付け
・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らせていただきます）
・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らせていただきます）

製品導入サービス

お客様のシステムをスムーズに構築するため、製品を熟知したスタッフによる導入サービスをご用意しています。

- 新規導入 / リプレース
- 設定変更
- バージョンアップ
- ネットワーク設計
- トレーニング
- 構築時 QA サポート

ファイア・ウォル子で検索‼

https://www.networld.co.jp/solution/fortinet_manga/

株式会社ネットワールド https://www.networld.co.jp/
お問い合わせ ✉ forti-info@networld.co.jp

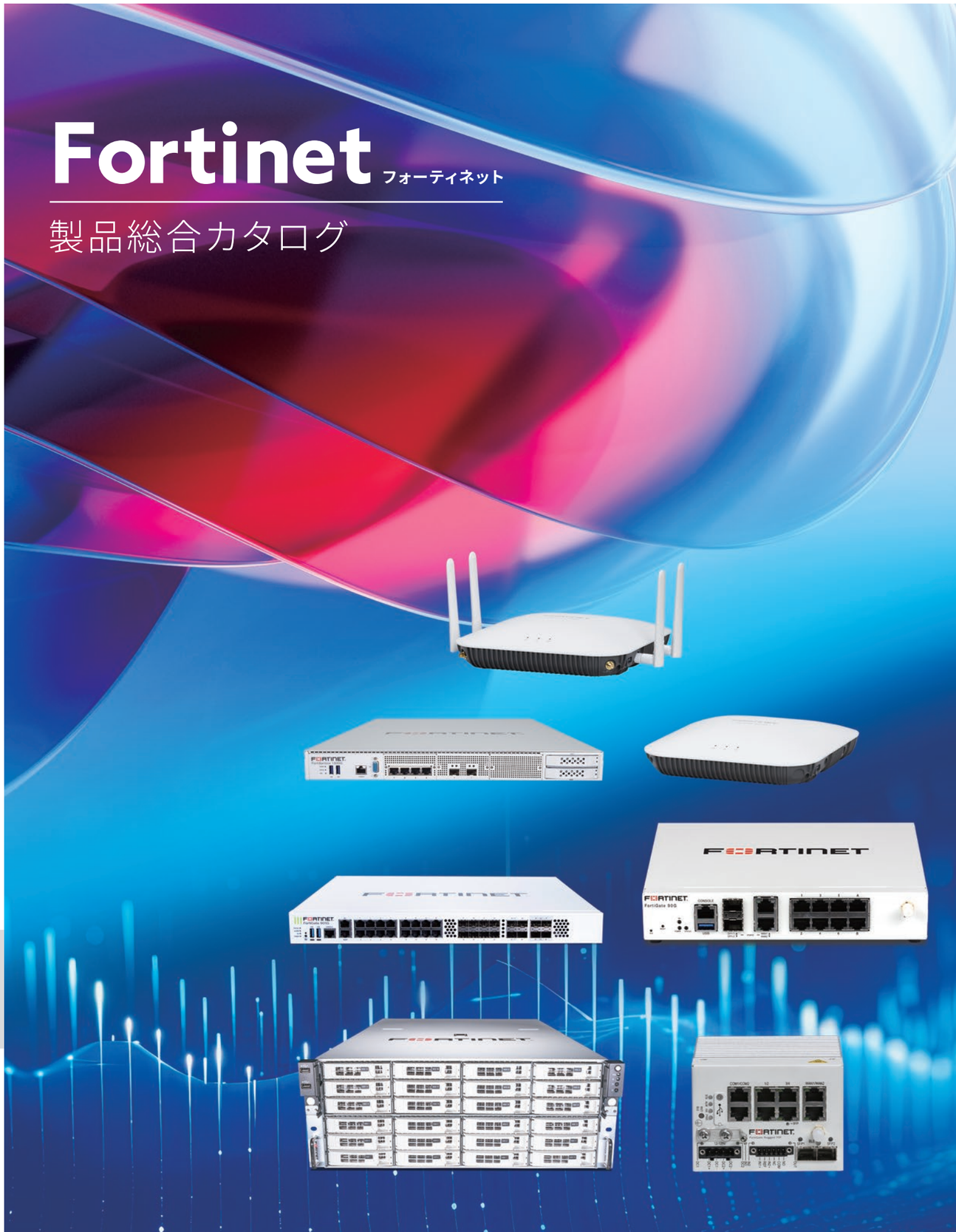
本　　社	〒101-0051 東京都千代田区神田神保町 2 -11-15 住友商事神保町ビル	TEL：03-5210-5020, 5031, 5095
関 西 支 店	〒530-0001 大阪市北区梅田 3-3-20 明治安田生命大阪梅田ビル 24F	TEL：06-7777-4174
中 部 支 店	〒450-0003 名古屋市中村区名駅南 1-17-23 ニッタビル 10F	TEL：052-588-7611
九 州 支 店	〒812-0013 福岡市博多区博多駅東 2-6-1 九勧筑紫通ビル 3F	TEL：092-461-7815

FORTINET

NETWORLD

Fortinet フォーティネット

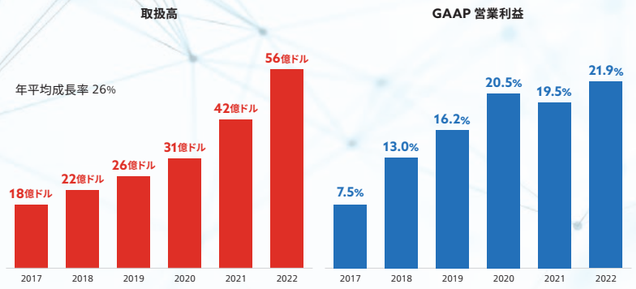
製品総合カタログ



フォーティネットについて

フォーティネットは、もっとも革新的でトップレベルのパフォーマンスを実現するネットワーク セキュリティファブリックを提供し、お客様の IT インフラストラクチャを簡素化するとともに安全に保護することをミッションとしています。
フォーティネットは、ネットワークセキュリティと SD-WAN、ネットワークスイッチや無線アクセス、ネットワークアクセス制御、認証、パブリック / プライベートクラウドのセキュリティ、エンドポイントセキュリティを提供すると同時に、通信事業者、データセンター、エンタープライズ、そして分散型オフィスに幅広く対応する AI ドリブンの高度な脅威保護ソリューションをグローバルに提供するリーディングベンダーです。

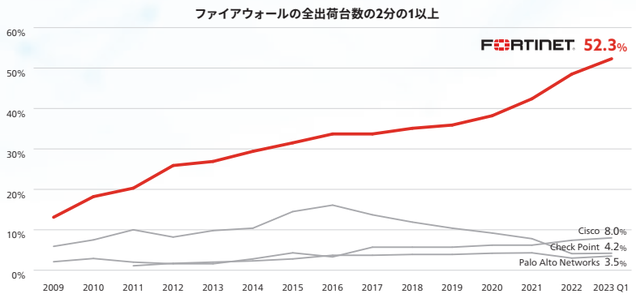
堅牢かつ圧倒的な成長力を誇るネットワークセキュリティ企業



出荷台数 No.1 のネットワークセキュリティソリューション

FW/UTM アプライアンスの
総出荷台数の 50% 近くを占める

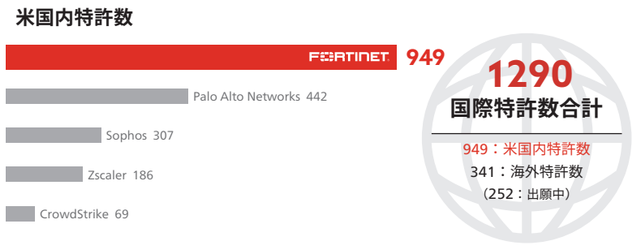
出典：IDC Quarterly Security Appliance Tracker 2023 Q1
（ファイアウォール / UTM アプライアンスの出荷台数に基づく）



No.1 のネットワークセキュリティイノベーター

競合ネットワークセキュリティ企業の
3倍に達する特許を取得

出典：米国特許商標局（2023 年 9 月 30 日現在）



会社情報

設立：2000年11月
最初の製品出荷：2002年5月
NASDAQ 上場：2009年11月
NASDAQ: FTNT（銘柄名）

本社：カリフォルニア州サニーベール

地域別の従業員数（2023 年 9 月 30 日現在）

北米 / 南米		欧州 / 中東 / アフリカ	
アメリカ	3,862	フランス	522
カナダ	2,588	イギリス	456
上記以外	998	上記以外	2,432
日本 / アジア太平洋地域			
インド	743		
日本	633		
上記以外	1,384	**合計**	13,618

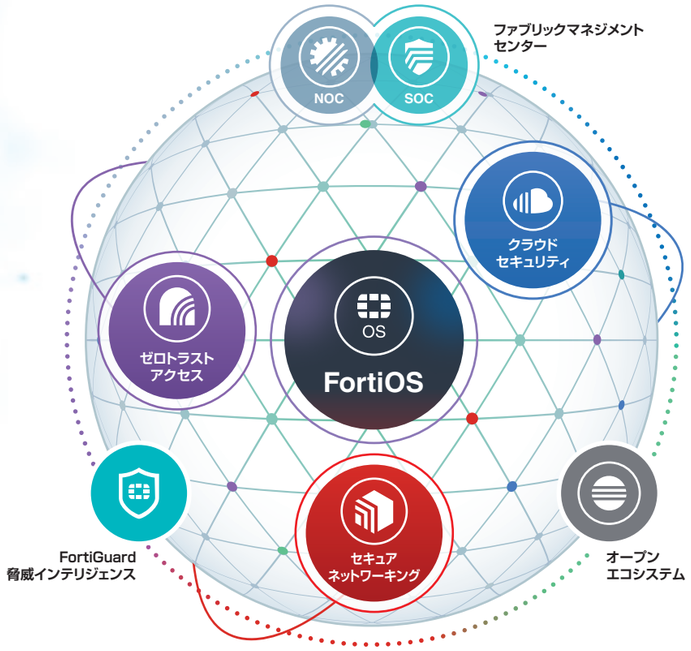
出荷実績：11,400,000台以上

顧客数：705,000社以上

SD-WAN 導入顧客数：21,000社以上

フォーティネット セキュリティファブリック

フォーティネットは、進化する IT インフラに対する動的な適応と保護を実現する、初のオープンなセキュリティアプローチである「 フォーティネット セキュリティファブリック 」を提供し、ネットワークセキュリティの未来を再び切り拓いていきます。



Broad 幅広い
デジタル攻撃対象領域全体の広範な
可視化によるリスク管理能力の改善

Integrated 統合化
複数のポイント製品をサポートする
複雑さを軽減する統合ソリューション

Automated 自動化
ワークフローの自動化による
オペレーションとレスポンスの迅速化

あらゆる攻撃対象領域を包括的に保護

ゼロトラスト アクセス
- ZTNA エージェント
- 認証
- 多要素認証 / トークン
- SASE

セキュア ネットワーキング
- ネットワーク ファイアウォール
- SD-WAN
- SD ブランチ
- Web プロキシ
- Wi-Fi
- ネットワーク スイッチ
- 5G / LTE
- ネットワーク アクセス制御

クラウド セキュリティ
- クラウド ファイアウォール
- マルチクラウド向け SD-WAN
- WAF
- E メール セキュリティ
- ADC / GSLB
- アンチ DDOS
- CASB

ネットワーク オペレーション
- ネットワーク管理
- ネットワーク オーケストレーション
- ネットワーク監視
- クラウド管理
- デジタル エクスペリエンス
- 監視

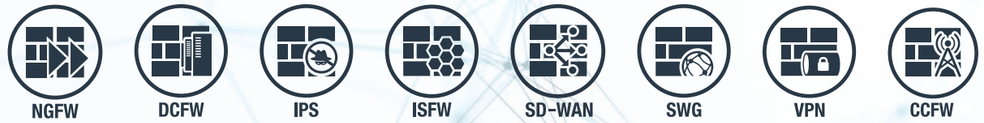
セキュリティ オペレーション
- エンドポイント保護
- EDR、XDR、MDR
- UEBA
- サンドボックス
- ディセプション
- 分析
- SIEM
- SOAR

オープン エコシステム
- ファブリック コネクタ
- ファブリック API
- ファブリック DevOps
- 広範な エコシステム

490 を超える
オープン ファブリック
エコシステム
インテグレーション

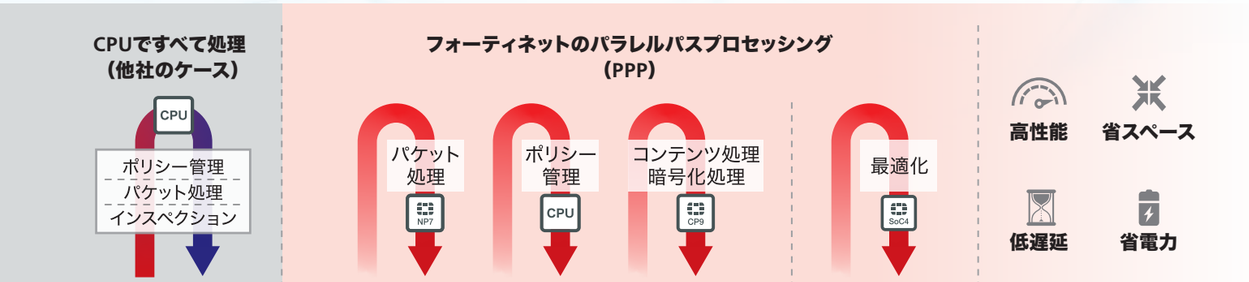
FortiOS のメリット

FortiOS はフォーティネット セキュリティファブリックの基盤となるセキュリティオペレーティングシステムで、多数のテクノロジーとユースケースを簡素化された単一のポリシーおよび管理フレームワークに統合します。FortiOS によって、攻撃対象領域全体にわたる優れた保護機能、詳細な可視化と制御、複雑さの低減、効率的な運用管理が可能になります。



FortiGate だけが実現可能な高いパフォーマンス

フォーティネット独自のセキュリティプロセッサによって、フォーティネットのソリューションのパフォーマンス、拡張性およびバリューが飛躍的に向上するとともに、ユーザーエクスペリエンスの品質が改善され、スペースおよび電力の要件が大幅に削減されます。フォーティネットの次世代ファイアウォール（NGFW）アプライアンスは、独自のセキュリティプロセッサと、トラフィックに最適化するパラレルパスプロセッシングがもたらす比類のない性能のメリットを得られます。



FortiGuard Labs 業界をリードする脅威インテリジェンス

FortiGuard Labs は、2002 年に設立されたサイバーセキュリティの脅威インテリジェンスを提供するフォーティネットの調査研究組織です。新たなグローバルセキュリティリスクに対抗するため、世界中の法執行機関、政府機関、そして世界中の提携セキュリティベンダー各社と連携しています。FortiGuard Labs は、次の 3 つの主要カテゴリにおいて、フォーティネット セキュリティファブリックのリアルタイム脅威インテリジェンスと革新的な防御戦術やツールを提供しています。

信頼性の高い AI / ML

実用的なローカル学習と AI / ML モデルを大規模クラウドドリブンデータレイクで強力に組み合わせることで、未知の脅威を迅速に阻止します。

リアルタイムの脅威インテリジェンス

FortiGuard Labs の独自の研究と外部とのコラボレーションに基づく継続的なセキュリティアップデートにより、プロアクティブなセキュリティ態勢を実現します。

脅威ハンティングとアウトブレイクアラート

アラート、分析 / 検知、アウトブレイクを含む防止 / 修復ツールにより、迅速な修復を可能にします。

グローバルなリーダーシップとコラボレーション：

CYBER THREAT ALLIANCE / WORLD ECONOMIC FORUM / INTERPOL / NCI AGENCY

フォーティネットのオープンなエコシステム

2023年10月5日現在
注：セキュリティファブリック エコシステムを代表する一部のパートナーのロゴを記載しています。

FortiCare

FortiCare のカスタマーサポートチームは、フォーティネットの全製品に対してテクニカルサポートをグローバルに提供します。南北アメリカ、ヨーロッパ、中東、アジア地域でサポートを提供し、あらゆる規模の企業のニーズにお応えします。

サービス / サポートのご紹介

Enterprise Protection は、高度なサポート、リアルタイムのネットワーク管理、そしてさまざまなセキュリティ / 運用サービスを組み合わせた、新しいサポート / サービスパッケージです。

プロフェッショナルサービス

プレミアム RMA

FortiCare
- 24 時間対応の FortiCare
  - 高度なサポートエンゲージメントレベル

FortiGuard
- Enterprise Protection の全機能を包含

運用サービス
- クラウド分析 / 管理
- SD-WAN 関連サービス
- FortiConverter

トレーニングおよび認定プログラム

フォーティネットは、Training Advancement Agenda（TAA）と Training Institute プログラムを通じて、2026 年までに100 万人にトレーニングを提供します。受賞歴のあるフォーティネットの Training Institute は、その卓越したサイバーセキュリティトレーニングによって、多数の組織から高く評価されています。

NSE 認定プログラム

ネットワークセキュリティエキスパート（NSE）認定プログラムには、講習形式と自習形式の広範なコースのほか、複雑なサイバーセキュリティの概念の習熟度を確認する、実用的かつ実践的な演習が含まれています。117 カ所の認定トレーニングセンターを通じて、150 以上の国と地域で技術トレーニングが実施されています。

トレーニング / 教育プログラム

Training Institute のパートナーシップでは、より多くの方にフォーティネットの認定プログラムをご利用いただけます。Academic Partner Program は、98 の国と地域の教育機関と連携しています。また、Education Outreach Program では、女性、マイノリティ、退役軍人、その他の過小評価されているグループなど、多様な人材にご参加いただけるよう努めています。

1,400,000 以上
認定証発行数

617
教育機関パートナー
（98 の国と地域）

46
教育支援および退役軍人
プログラムのパートナー

FortiGate 主要モデル仕様一覧

物理アプライアンス

	FortiGate 40F	FortiGate 60F	FortiGate 90G	FortiGate 120G	FortiGate 200F	FortiGate 400F	FortiGate 600F	FortiGate 900G
Pv4 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）	5 / 5 / 5 Gbps	10 / 10 / 6 Gbps	28 / 28 / 27.9 Gbps	39 / 39 / 28 Gbps	27 / 27 / 11 Gbps	79.5 / 78.5 / 70 Gbps	139 / 137.5 / 70 Gbps	164 / 163 /153 Gbps
IPSec VPN スループット（512 バイトパケット）[1]	4.4 Gbps	6.5 Gbps	25 Gbps	35 Gbps	13 Gbps	55 Gbps	55 Gbps	55 Gbps
IPS スループット（エンタープライズトラフィック混合）[2]	1 Gbps	1.4 Gbps	4.5 Gbps	5.3 Gbps	5 Gbps	12 Gbps	14 Gbps	26 Gbps
NGFW スループット（エンタープライズトラフィック混合）[2, 4]	800 Mbps	1 Gbps	2.5 Gbps	3.1 Gbps	3.5 Gbps	10 Gbps	11.5 Gbps	22 Gbps
脅威保護スループット（エンタープライズトラフィック混合）[2, 5]	600 Mbps	700 Mbps	2.2 Gbps	2.8 Gbps	3 Gbps	9 Gbps	10.5 Gbps	20 Gbps
ファイアウォールレイテンシ	2.97 µ sec	3.3 µ sec	3.23 µ sec	3.17 µ sec	4.78 µ sec	4.19 µ sec / 2.5 µ sec [8]	4.12 µ sec	3.78 µ sec / 2.5 µ sec [8]
ファイアウォール同時セッション	700,000	700,000	1.5 M	3 M	3 M	7.8 M	8 M	16 M
ファイアウォール新規セッション / 秒	35,000	35,000	124,000	140,000	280,000	500,000	550,000	720,000
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	10,000
ゲートウェイ間 IPSec VPN トンネル	200	200	200	2,000	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	2,500	16,000	16,000	50,000	50,000	10,000
SSL VPN スループット	490 Mbps	900 Mbps	1.4 Gbps	1.5 Gbps	2 Gbps	3.6 Gbps [9]	4.3 Gbps [9]	10 Gbps [9]
同時 SSL-VPN ユーザー（推奨最大値、トンネルモード）	200	200	200	500	500	5,000	10,000	10,000
SSL インスペクションスループット（IPS、avg. HTTPS）[3]	310 Mbps	630 Mbps	2.6 Gbps	3 Gbps	4 Gbps	8 Gbps	9 Gbps	16.7 Gbps
アプリケーション制御スループット（HTTP 64 K）[2]	990 Mbps	1.8 Gbps	6.7 Gbps	6.7 Gbps	13 Gbps	28 Gbps	32 Gbps	74.8 Gbps
FortiAP サポート数（合計 / トンネルモード）	16 / 8	64 / 32	96 / 48	128 / 64	256 / 128	512 / 256	1,024 / 512	1,024 / 512
FortiSwitch サポート数	8	16	24	32	64	72	96	96
FortiToken サポート数	500	500	500	5,000	5,000	5,000	5,000	5,000
仮想 UTM（VDOM: 標準 / 最大）	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10
インタフェース	5 x GE RJ45	10 x GE RJ45	8 x GE RJ45、2 x 10 GE RJ45/SFP+（選択使用）	4 x 10 GE SFP+、18 x GE RJ45、8 x GE SFP	4 x 10 GE SFP+、18 x GE RJ45、8 x GE SFP	8 x 10 GE SFP+、18 x GE RJ45、8 x GE SFP	4 x 25 GE SFP28、4 x 10 GE SFP+、18 x GE RJ45	4 x 25 GE SFP28、4 x 10 GE SFP+、1 x 2.5 GE RJ45、8 x GE SFP、17 x GE RJ45
ストレージ	—	—	120 GB（91G）	480 GB（121F）	480 GB（201F）	960 GB（401F）	480 GB（601F）	960 GB（901G）
電源	単一 AC 電源	単一 AC 電源	単一 AC 電源 二重入力	二重 AC 電源	二重 AC 電源	二重 AC 電源	二重 AC 電源	二重 AC 電源
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）	ラックマウント（1 RU）

	FortiGate 1000F	FortiGate 1800F	FortiGate 2600F	FortiGate 3200F	FortiGate 3500F	FortiGate 3700F	FortiGate 4200F	FortiGate 4800F
Pv4 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）	198 / 196 / 134 Gbps	198 / 197 / 140 Gbps	198 / 196 / 120 Gbps	387 / 385 178.5 Gbps	595 / 590 / 420 Gbps	589 / 589 / 420 Gbps	800 / 788 / 400 Gbps	3.1 / 3.1 / 0.93 Tbps
IPSec VPN スループット（512 バイトパケット）[1]	55 Gbps	55 Gbps	55 Gbps	105 Gbps	165 Gbps	160 Gbps	210 Gbps	800 Gbps
IPS スループット（エンタープライズトラフィック混合）[2]	19 Gbps	22 Gbps	24 Gbps	63 Gbps	72 Gbps	86 Gbps	52 Gbps	87 Gbps
NGFW スループット（エンタープライズトラフィック混合）[2, 4]	15 Gbps	17 Gbps	19 Gbps	47 Gbps	65 Gbps	80 Gbps	47 Gbps	77 Gbps
脅威保護スループット（エンタープライズトラフィック混合）[2, 5]	13 Gbps	15 Gbps	17 Gbps	45 Gbps	63 Gbps	75 Gbps	45 Gbps [6]	75 Gbps
ファイアウォールレイテンシ	3.45 µ sec	3.22 µ sec	3.41 µ sec	3.42 µ sec	2.98 µ sec	3.56 µ sec / 1.45 µ sec [8]	3.02 µ sec	3.6 µ sec
ファイアウォール同時セッション	7.5 M	12 M / 40 M [7]	24 M / 40 M [7]	70 M	140 M / 348 M [7]	140 M	210 M / 450 M [7]	280 M / 1.8 B [7]
ファイアウォール新規セッション / 秒	650,000	750,000 / 2M [7]	1 M / 2 M [7]	800,000	1 M / 5 M [7]	930,000	1 M / 7 M [7]	915,000 / 25 M [7]
ファイアウォールポリシー	100,000	100,000	100,000	200,000	200,000	200,000	200,000	400,000
ゲートウェイ間 IPSec VPN トンネル	20,000	20,000	20,000	40,000	40,000	40,000	40,000	40,000
クライアント - ゲートウェイ間 IPSec VPN トンネル	100,000	100,000	100,000	200,000	200,000	200,000	200,000	200,000
SSL VPN スループット	5.3 Gbps [9]	11 Gbps	16 Gbps	11 Gbps	16 Gbps [9]	16 Gbps [9]	16 Gbps	18 Gbps
同時 SSL-VPN ユーザー（推奨最大値、トンネルモード）	10,000	10,000	30,000	30,000	30,000	30,000	30,000	30,000
SSL インスペクションスループット（IPS、avg. HTTPS）[3]	10 Gbps	12 Gbps	20 Gbps	29 Gbps	63 Gbps	55 Gbps	50 Gbps	63 Gbps
アプリケーション制御スループット（HTTP 64 K）[2]	44 Gbps	34 Gbps	64 Gbps	109 Gbps	135 Gbps	190 Gbps	135 Gbps	180 Gbps
FortiAP サポート数（合計 / トンネルモード）	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	8,192 / 4,096	8,192 / 4,096
FortiSwitch サポート数	196	196	196	300	300	300	300	300
FortiToken サポート数	20,000	20,000	20,000	20,000	20,000	20,000	20,000	20,000
仮想 UTM（VDOM: 標準 / 最大）	10 / 250	10 / 250	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500
インタフェース	2 x 100 GE QSFP28、8 x 25 GE SFP28、16 x 10 GE SFP+、8 x 10 GE RJ45、1 × 2.5 GE RJ45、1 x GE RJ45	4 x 40 GE QSFP+、12 x 25 GE SFP28、2 x 10 GE SFP+、8 x GE SFP、18 x GE RJ45	4 x 100 GE QSFP28/40 GE QSFP+、16 x 25 GE SFP28、16 x 10 GE RJ45、2 x 10 GE SFP+、2 x GE RJ45	4 x 400 GE QSFP-DD、12 x 50 GE SFP56、4 x 25 GE SFP28、2 x 10 GE RJ45	6 x 100 GE QSFP28/40 GE QSFP+、32 x 25 GE SFP28、2 x GE RJ45	4 x 400 GE QSFP-DD、4 x ULL 25 GE SFP28、20 x 50 GE SFP56、2 x 10 GE RJ45	8 x 100 GE QSFP28/40 GE QSFP+、18 x 25 GE SFP28、2 x GE RJ45	8 x 400 GE、12 x 200 GE QSFP56、12 x 50 GE SFP56、2 x 10 GE RJ45
ストレージ	960 GB（1001F）	2 TB（1801F）	2 TB（2601F）	2 TB（3201F）	4 TB（3501F）	4 TB（3701F）	4 TB（4201F）	4 TB（4801F）
電源	二重電源	二重電源	二重電源	二重電源	二重電源	二重電源	二重電源	四重電源
形状	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（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（4 RU）

仮想アプライアンス

	FortiGate-VM01/01V		FortiGate-VM02/02V		FortiGate-VM04/04V		FortiGate-VM08/08V		FortiGate-VM16/16V		FortiGate-VM32/32V		FortiGate-VMUL/ULV	
技術仕様														
仮想 CPU 数（最小 / 最大）	1 / 1		1 / 2		1 / 4		1 / 8		1 / 16		1 / 32		1 / 無制限	
メモリ容量（最小 / 制限無し）	2 GB		2 GB		2 GB		2 GB		2 GB		2 GB		2 GB	
ネットワークインタフェース数（最小 / 最大）[1]	1 / 10		1 / 10		1 / 10		1 / 10		1 / 10		1 / 10		1 / 10	
ストレージ容量（最小 / 最大）	32 GB / 2 TB		32 GB / 2 TB		32 GB / 2 TB		32 GB / 2 TB		32 GB / 2 TB		32 GB / 2 TB		32 GB / 2 TB	
制御可能な無線アクセスポイント数（トンネル / グローバル）	32 / 64		512 / 1,024		512 / 1,024		1,024 / 4,096		1,024 / 4,096		1,024 / 4,096		1,024 / 4,096	
仮想ドメイン（標準 / 最大）[2]	10 / 10		10 / 25		10 / 50		10 / 500		10 / 500		10 / 500		10 / 500	
ファイアウォールポリシー	10,000		10,000		10,000		200,000		200,000		200,000		200,000	
最大クライアント数	2,000		2,000		8,000		20,000		20,000		20,000		20,000	
ユーザー数無制限ライセンス	○		○		○		○		○		○		○	
パフォーマンス（vSPU-off/on）	off	on	off	on	off	on	off	on	off	on	off	on	off	on
ファイアウォール スループット（UDP パケット 1518 バイト）	12.9 Gbps	vSPU非対応	17 Gbps	32 Gbps	25 Gbps	56 Gbps	44 Gbps	105 Gbps	50 Gbps	110 Gbps	79 Gbps	117 Gbps	–	–
ファイアウォール スループット（UDP パケット 512 バイト）	6 Gbps		7 Gbps	11.2 Gbps	10.8 Gbps	19.7 Gbps	14 Gbps	36.7 Gbps	15.5 Gbps	37.5 Gbps	40.7 Gbps	39.8 Gbps	–	–
ファイアウォール スループット（UDP パケット 64 バイト）	1 Gbps		1.1 Gbps	1.7 Gbps	2 Gbps	2.9 Gbps	3 Gbps	5.3 Gbps	3.2 Gbps	6 Gbps	4.3 Gbps	6.4 Gbps	–	–
ファイアウォール新規セッション / 秒（TCP）	106 K		151 K	104 K	123 K	155 K	392 K	323 K	673 K	524 K	914 K	620 K	–	–
ファイアウォール最大セッション	1.5 M		3.5 M	1.7 M	6 M	3 M	13 M	6.5 M	27 M	14 M	55.5 M	29 M	–	–
IPsec VPN UDP スループット（AES256GCM、1360 バイト）	0.5 Gbps		1 Gbps	12 Gbps	2.1 Gbps	22.5 Gbps	4 Gbps	37.5 Gbps	5.2 Gbps	39.7 Gbps	7.2 Gbps	45.6 Gbps	–	–
SSL VPN スループット	1.5 Gbps		1.6 Gbps	使用不可	3.9 Gbps	使用不可	8.1 Gbps	使用不可	8.6 Gbps	使用不可	9.7 Gbps	使用不可	–	使用不可
IPS スループット [3]	0.8 Gbps		1.7 Gbps	2 Gbps	3.3 Gbps	3.6 Gbps	5.9 Gbps	6.1 Gbps	10.1 Gbps	12.1 Gbps	15.4 Gbps	16.1 Gbps	–	–
IPS HTTP 1M	1.1 Gbps		1.9 Gbps	2.4 Gbps	3.5 Gbps	4.5 Gbps	6.8 Gbps	8.9 Gbps	11.6 Gbps	16.4 Gbps	17.5 Gbps	21 Gbps	–	–
アプリケーション制御スループット [4]	1.4 Gbps		2.3 Gbps	3.4 Gbps	5.3 Gbps	7.1 Gbps	9.1 Gbps	11.3 Gbps	17.3 Gbps	19.5 Gbps	25.6 Gbps	26.5 Gbps	–	–
NGFW スループット [5]	0.7 Gbps		1.3 Gbps	1.4 Gbps	2.6 Gbps	2.8 Gbps	4.2 Gbps	5.2 Gbps	8.5 Gbps	10.1 Gbps	12.6 Gbps	13.6 Gbps	–	–
脅威防御スループット [6]	0.4 Gbps		0.9 Gbps	1.1 Gbps	1.8 Gbps	1.9 Gbps	3.4 Gbps	3.5 Gbps	6.3 Gbps	7 Gbps	10.5 Gbps	11 Gbps	–	–

■ 物理アプライアンスについて

代表的なモデルを掲載しています。全モデルはホームページをご覧ください。数値はすべて「最大」の性能値であり、システム構成に応じて異なります。

1. IPSec VPN パフォーマンスは、AES256-SHA256 を使用して測定されています。
2. IPS、アプリケーション制御、NGFW および脅威保護スループットは、ログ機能が有効な状態で測定されています。
3. SSL インスペクションパフォーマンスは、複数の異なる暗号スイートを使用した HTTPS セッションの平均値を記載しています。
4. NGFW パフォーマンスは、ファイアウォール、IPS およびアプリケーション制御が有効な状態で測定されています。
5. 脅威保護パフォーマンスは、ファイアウォール、IPS、アプリケーション制御、およびマルウェアに対する保護が有効な状態で測定されています。
6. 計測条件に URL filter も含みます。
7. Hyperscale ライセンス利用時の数値になります。
8. 特定の低遅延ポートの組み合わせを用いた場合となります。
9. RSA2048bit 証明書利用時のパフォーマンスとなります。

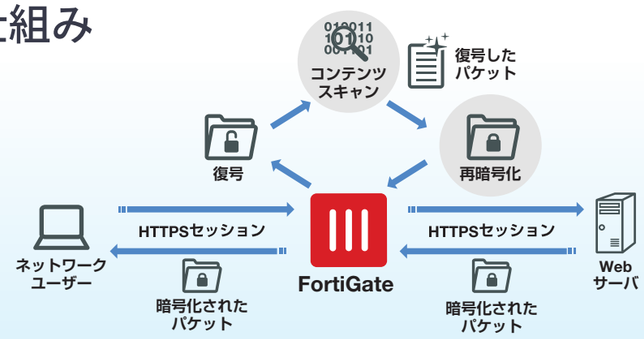
■ 仮想アプライアンスについて

VMware ESXi 環境での情報を掲載しています。他のプラットフォーム、パブリッククラウドの情報はそれぞれデータシートをご覧ください。
数値はすべて「最大」の性能値であり、システム構成に応じて異なります。

1. 計測はDELL R740 (CPU Intel Xeon Platinum 8268 @ 2.9 GHz、96 コア、IntelX710 ネットワークアダプタ SR-IOV有効) 上で行われています。
2. FG-VMxxVおよびFG-VMxxSシリーズにVDOMライセンスは付属しません。必要に応じて別途ご用意ください。
3. IPSスループットは1M byte httpとEnterprise Traffic Mixで測定されています。
4. アプリケーション制御スループットは64 Kbyte HTTPトラフィックで計測されています。
5. NGFWスループットはIPSとアプリケーション制御を有効にして計測されています。
6. 脅威防御スループットはIPSとアプリケーション制御とマルウェア防御を有効にして計測されています。

SSL インスペクションの仕組み

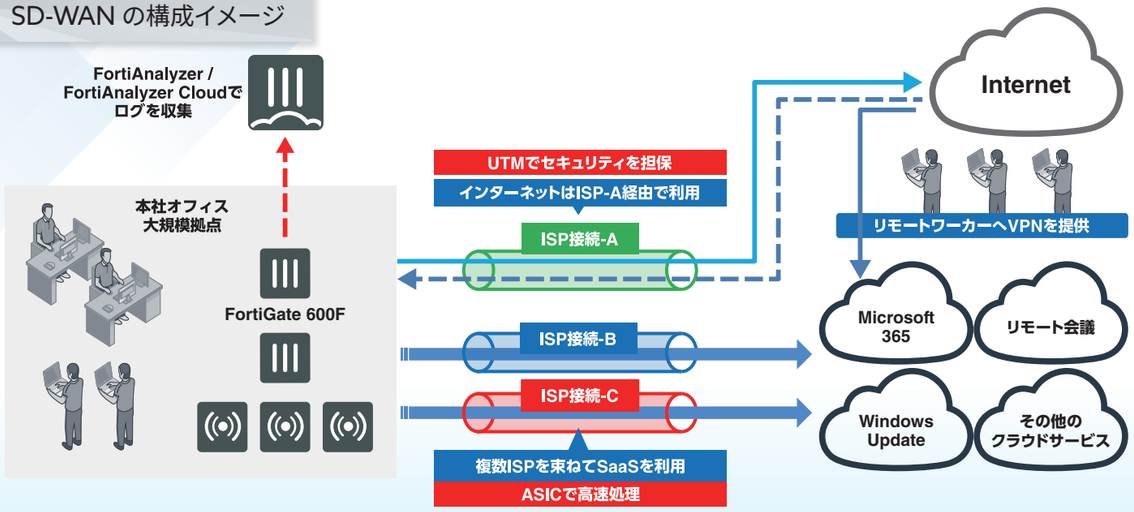
暗号化された通信を FortiGate で復号して、セキュリティ検査を実施した上で、再び暗号化します。SSL インスペクションを行うには、事前にエンドポイントに FortiGate の証明書をインストールする必要があります。インストール方法は手動もしくは Active Directory による自動配布が可能です。



アプリケーションのパフォーマンス向上と安全性を両立する セキュア SD-WAN ソリューション

ビジネスに不可欠なクラウドベースのアプリケーションやツールの使用が増加し続けるにつれて、複数の支店や拠点を抱える分散型の組織は、パフォーマンスが制限された WAN（広域ネットワーク）から SD-WAN（ソフトウェア定義型広域ネットワーク）アーキテクチャに切り替えています。
フォーティネットのセキュア SD-WAN ソリューションは、ベストオブブリードの次世代ファイアウォールセキュリティ、SD-WAN、高度なルーティング機能、および WAN の最適化機能で構成されており、これらの製品においてセキュリティドリブンのネットワーク WAN エッジ変革を実現します。

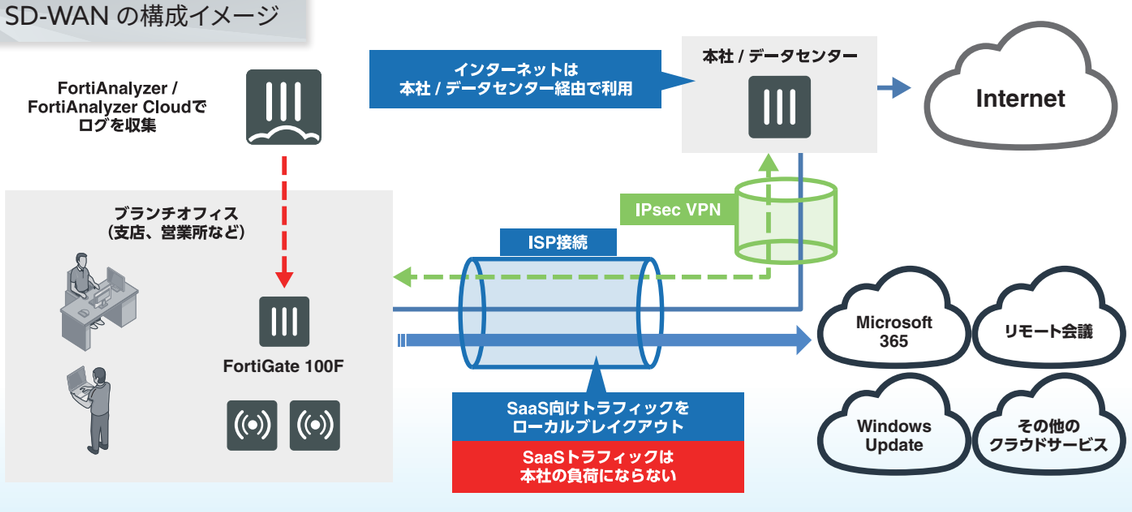
エンタープライズ向け SD-WAN の構成イメージ



名前	送信元	宛先
Microsoft_Outbound01	Intenal_Networks	Microsoft-Microsoft.Update Microsoft-Office365 Microsoft-Outlook Microsoft-Web
Remote_presense_Outbound02	Intenal_Networks	Cisco-Webex LogMeIn-GoTo.Suite Microsoft-Skype_Teams Zoom.us-Zoom.Meeting

常に最新に保たれる IPアドレス&ポートリスト

ブランチ向け SD-WAN の構成イメージ



名前	送信元	宛先
Microsoft_Outbound01	Intenal_Networks	Microsoft-Microsoft.Update Microsoft-Office365 Microsoft-Outlook Microsoft-Web
Remote_presense_Outbound02	Intenal_Networks	Cisco-Webex LogMeIn-GoTo.Suite Microsoft-Skype_Teams Zoom.us-Zoom.Meeting

常に最新に保たれる IPアドレス&ポートリスト

ソリューションのポイント

1 複数の ISP 回線（インターネット、WAN）を効率よく使い分けることができ、冗長性も確保しやすくなってコスト効果の高いネットワーク運用を実現！

2 FortiGate に搭載している SD-WAN ASIC（専用プロセッサ）の高速処理でスループットを維持し、いつでも快適なリモート会議の実施や体感パフォーマンスを向上！

3 リモートワーカーへの VPN 提供、FortiGate Cloud による管理 / バックアップなどより使いやすく、運用管理の質も向上！

ソリューションのポイント

1 拠点からのインターネット利用は、本社やデータセンターを経由させてセキュリティをしっかり確保！

2 信頼できるクラウドサービスやリモート会議の利用はローカルブレイクアウトで拠点から直接アクセスして、本社やデータセンターの UTM の負担を軽減！

3 FortiGate に搭載している SD-WAN ASIC でスループットの心配はなし。FortiGate Cloud を使ってゼロタッチプロビジョニングで拠点側の負担も削減！

セキュア SD-WAN ソリューションの中核となる代表的な FortiGate モデル

エントリーレベル
FortiGate 60F

FortiGate 60F シリーズは、省スペースでファンレス設計のデスクトップ型セキュリティ /SD-WAN ソリューションです。独自の SOC（System-on-a-Chip）プロセッサの高速処理、業界最先端のセキュア SD-WAN によって、サイバー脅威からの保護を可能にします。

ミッドレンジ
FortiGate 120G

FortiGate 120G シリーズは、分散した事業拠点を持つ中規模から大規模の企業向けに、次世代ファイアウォールと SD-WAN 機能を組み合わせて提供します。最新の ASIC を搭載した SP5 でビジネスクリティカルアプリケーションに最適な高性能を発揮し、トップクラスのセキュリティを提供します。

ミッドレンジ
FortiGate 600F

FortiGate 600F シリーズは、中規模から大規模の企業向けに次世代ファイアウォール機能を提供します。キャンパスや大規模企業の支社への展開に適しており、独自の SOC（System-on-a-Chip）プロセッサによる高速処理、そしてアプリケーションセントリックで拡張性の優れたセキュアな SD-WAN ソリューションを提供します。

ハイエンド
FortiGate 1800F

FortiGate 1800F シリーズは、大規模エンタープライズやサービスプロバイダー向けに高性能の次世代ファイアウォール機能を提供します。複数の高速インタフェースを高密度実装して高スループットを実現しており、エンタープライズエッジ、ハイブリッド / ハイパースケールのデータセンターコア、および内部セグメントへの配備に適しています。

ハイエンド
FortiGate 2600F

FortiGate 2600F シリーズは、大規模エンタープライズ、サービスプロバイダーのデータセンターコアや社内セグメントで高性能な脅威保護と SSL インスペクションを提供します。複数の高速かつ高密度のインタフェースを備えており、優れたセキュリティの効率性と高スループットによって、安定したセキュアネットワーク接続を実現します。

ハイエンド
FortiGate 3500F

FortiGate 3500F シリーズは、大規模エンタープライズやサービスプロバイダー向けに高性能の次世代ファイアウォール機能を提供します。複数の高速インタフェースを高密度実装することで高スループットを実現しており、業界最先端の IPS、SSL インスペクション、高度な脅威保護機能を活用し、最適なネットワークパフォーマンスを実現します。

ハイエンド
FortiGate 4200F

FortiGate 4200F シリーズは、高速のネットワーキング、強化された拡張性、そして最適化されたパフォーマンスを提供します。エンタープライズやサービスプロバイダーは、トップクラスの IPS、SSL インスペクション、そして脅威保護機能で、あらゆる脅威のリスクを管理することができます。

仮想アプライアンス
FortiGate VM

FortiGate 仮想アプライアンスは、FortiOS オペレーティングシステムが提供するすべてのセキュリティおよびネットワーキング機能に対応しており、巧妙化する脅威に対する最新の保護機能を提供します。

各モデルのスペック比較

	FortiGate 60F	FortiGate 120G	FortiGate 600F	FortiGate 1800F	FortiGate 2600F	FortiGate 3500F	FortiGate 4200F
Pv4 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）	10 / 10 / 6 Gbps	39 / 39 / 28 Gbps	139 / 137.5 / 70 Gbps	198 / 197 / 140 Gbps	198 / 196 /120 Gbps	595 / 590 / 420 Gbps	800 / 788 / 400 Gbps
IPSec VPN スループット（512 バイトパケット）[1]	6.5 Gbps	35 Gbps	55 Gbps	55 Gbps	55 Gbps	165 Gbps	210 Gbps
脅威保護スループット（エンタープライズトラフィック混合）[2, 3]	700 Mbps	2.8 Gbps	10.5 Gbps	9.1 Gbps	17 Gbps	63 Gbps	45 Gbps
SSL VPN スループット	900 Mbps	1.5 Gbps	4.3 Gbps	11 Gbps	16 Gbps	16 Gbps	16 Gbps
インタフェース	10 x GE RJ45	4 x 10 GE SFP+、18 x GE RJ45、8 x GE SFP	4 x 25 GE SFP28、4 x 10 GE SFP+、18 x GE RJ45	4 x 40 GE QSFP+、12 x 25 GE SFP28、2 x 10 GE SFP+、8 x GE SFP、18 x GE RJ45	4 x 100 GE QSFP28/40 GE QSFP+、16 x 25 GE SFP28、16 x 10 GE RJ45、2 x 10 GE SFP+、2 x GE RJ45	6 x 100 GE QSFP28/40 GE QSFP+、32 x 25 GE SFP28、2 x GE RJ45	8 x 100 GE QSFP28/40 GE QSFP+、18 x 25 GE SFP28、2 x GE RJ45

1. IPSec VPN パフォーマンスは、AES256-SHA256 を使用して測定されています。
2. IPS、アプリケーション制御、NGFW および脅威保護スループットは、ログ機能が有効な状態で測定されています。
3. 脅威保護パフォーマンスは、ファイアウォール、IPS、アプリケーション制御、およびマルウェアに対する保護が有効な状態で測定されています。

SD-WAN のサイジングの考え方

機種	人数（UTM あり）	人数（UTM なし）
FortiGate 60F	50	200
FortiGate 120G	100	500
FortiGate 600F	1,000	5,000
FortiGate 1800F/2600F	2,000	10,000
FortiGate 3500F/4200F	10,000 ～	10,000 ～

* 上記はあくまでも目安です。使用する機能で条件は変わります。

より使いやすくするお勧め製品

FortiManager

FortiManager は、複数の FortiGate を効率良く管理する統合管理・監視アプライアンスです。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、SD-WAN オーケストレーター機能を備えています。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。

FortiGate Cloud
クラウドベースの管理ソリューション
P32 へ

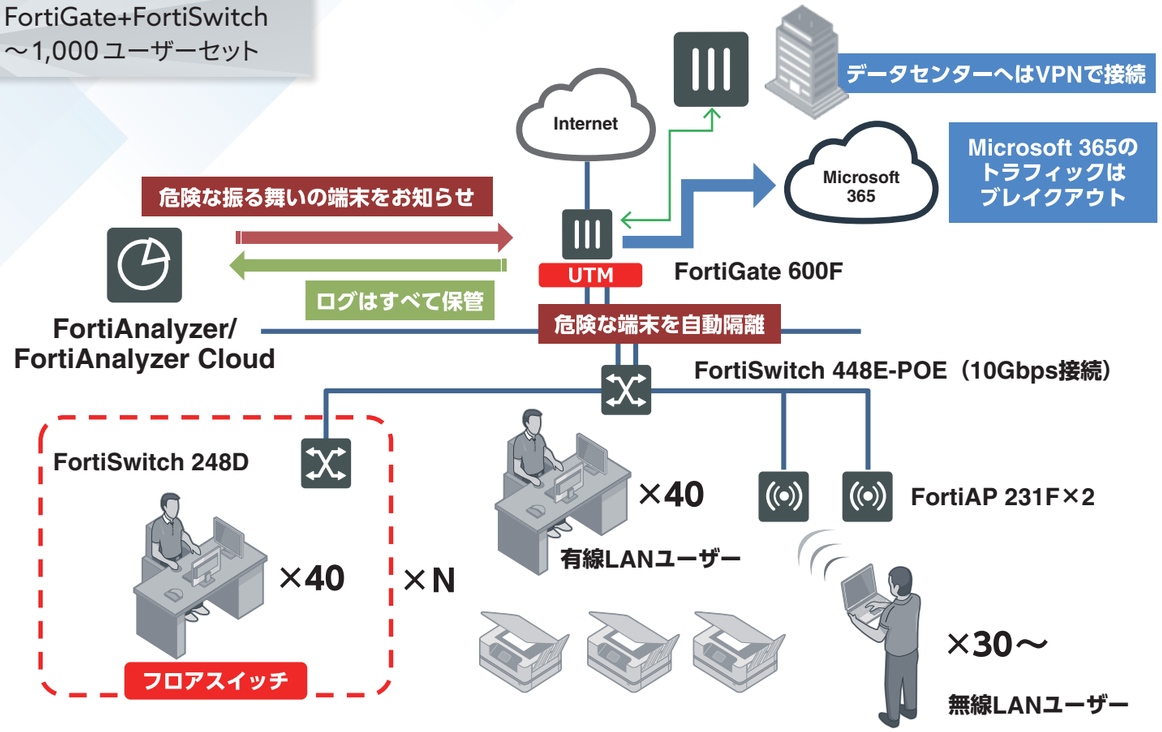
FortiSandbox
プロアクティブな脅威検出を実現
P31 へ

FortiMail
FortiGate のメールセキュリティを強化
P30 へ

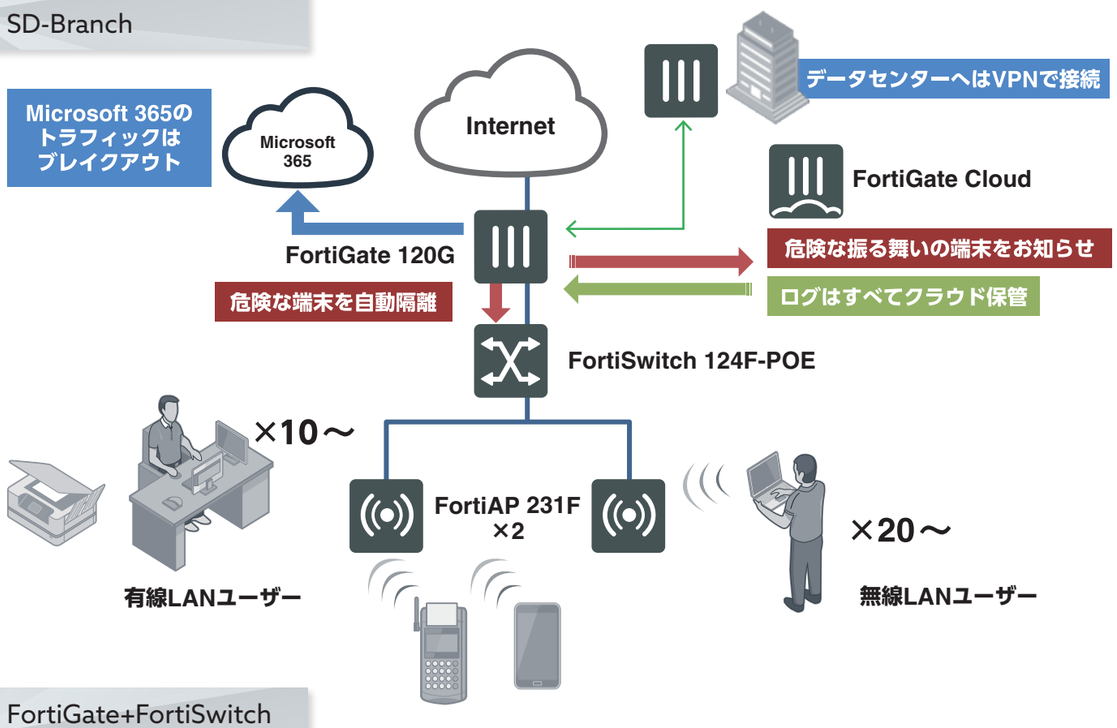
拠点ネットワーク（エッジ）をより安全にするセキュア SD-Branch ソリューション

リモートとローカルの両方のユーザーが、クラウドや SaaS（Security-as-a-Service）アプリケーションを利用するためにインターネットに直接アクセスするようになったことで、WAN やアクセスエッジがこれまで以上に複雑化しています。さらに、支社ネットワークに接続される IoT デバイスによって、攻撃者に悪用される恐れのある脆弱性が新たに加わることになります。
フォーティネットのセキュア SD-Branch ソリューションは、セキュリティとネットワークアクセスを融合させて、フォーティネット セキュリティファブリックのメリットをより多くの拠点にも提供します。

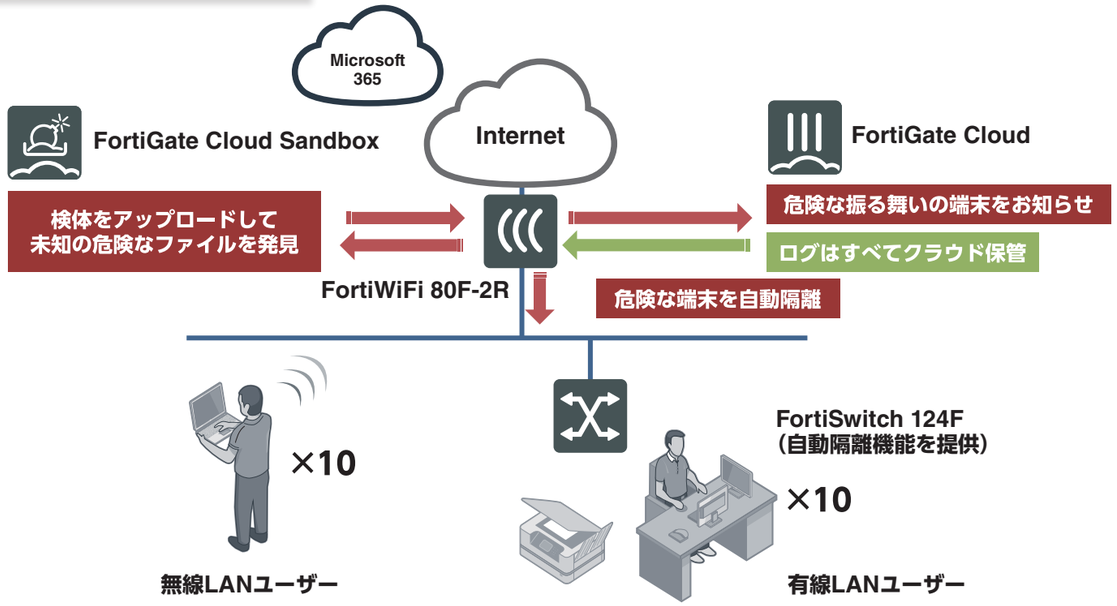
FortiGate+FortiSwitch ～1,000 ユーザーセット



FortiGate+FortiSwitch SD-Branch



FortiGate+FortiSwitch SOHOソリューション



ソリューションのポイント

1 エンタープライズ規模では、UTM を中核として有線 / 無線インフラを提供し、スイッチやアクセスポイントを追加すれば規模を自由に拡張。外部クラウドサービスへの対応も万全！

2 小規模向けでは、コストパフォーマンスに優れた FortiWiFi で有線 / 無線インフラをまとめて提供。FortiGate Cloud Sandbox で未知の脅威にも対応！

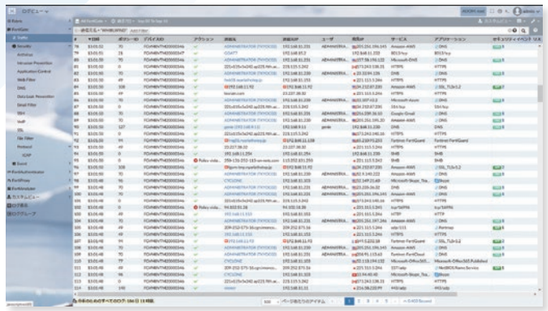
3 端末間の通信も含めてログはすべてクラウドに保存し、怪しい動きの端末は自動隔離するなどセキュリティ面も強化！

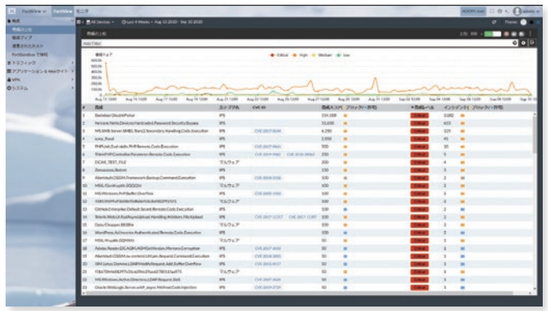
セキュア SD-Branch ソリューションを支える代表的な FortiGate モデル

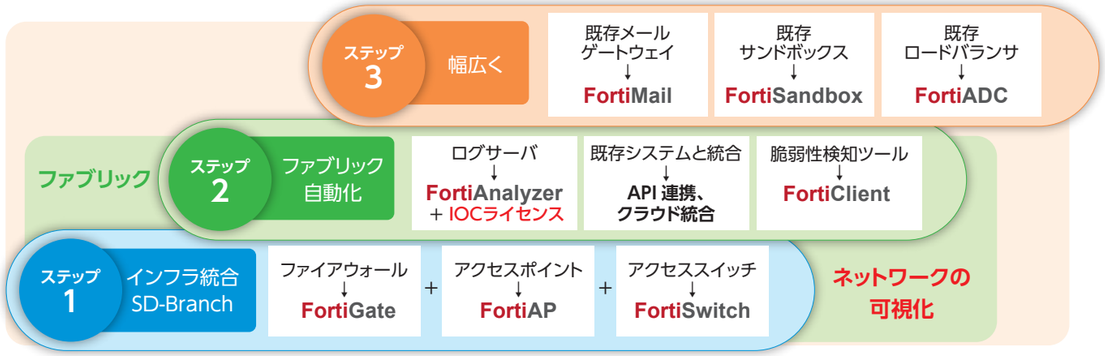
P10へ

FortiAnalyzer

FortiAnalyzer は、オーケストレーション、オートメーション、レスポンスの一元化によって、攻撃対象領域全体のリスクを軽減し、組織全体のセキュリティを強化します。
フォーティネット セキュリティファブリックに FortiAnalyzer を統合することで、攻撃対象領域の拡大につながった新しいテクノロジーの分析や監視の複雑さが軽減され、エンドツーエンドの可視性によって脅威の特定と排除が容易になります。







	FAZ-150G	FAZ-300G	FAZ-810G	FAZ-1000F	FAZ-3000G	FAZ-3510G	FAZ-3700G	FAZ-VM-BASE to FAZ-VM-GB2000
ログ処理 GB/ 日	25	100	200	660	3,000	5,000	8,300	1 ～ +2,000
分析用持続レート（ログ / 秒）	500	2,000	4,000	20,000	42,000	60,000	100,000	–
コレクタ用持続レート（ログ / 秒）	750	3,000	6,000	30,000	60,000	90,000	150,000	–
最大デバイス数	50	180	800	2,000	4,000	10,000	10,000	–
インタフェース	2 × GE RJ45	4 × GE RJ45	4 × GE RJ45 2 × GE SFP	2 × GE RJ45 2 × 10 GE SFP+	2 × GE RJ45 2 × 25 GE SFP28	2 × 10 GE RJ45 2 × 25 GE SFP28	2 × 10 GE RJ45 2 × 25 GE SFP28	1 / 4 (vNIC Min / Max)
ストレージ	4 TB (2 × 2 TB)	8 TB (2 × 4 TB)	16 TB (4 × 4 TB)	32 TB (8 × 4 TB)	64 TB (16 × 4 TB)	96 TB (24 × 4 TB) + 7.68 TB (2 × 3.84 TB)	240 TB (60 × 4 TB) 3.5 HDD + 19.2 TB (6 × 3.2 TB) NVMe SSD	500 GB ～ +100 TB
RAID ストレージ管理	RAID0、1	RAID0、1	RAID0、1、1s、5、5s、10	RAID0、1、1s、5、5s、6、6s、10、50、60	RAID0、1、1s、5、5s、6、6s、10、50、60	RAID0、1、1s、5、5s、6、6s、10、50、60	RAID0、1、1s、5、5s、6、6s、10、50、60	–
FortiAnalyzer Cloud	–	–	–	–	–	–	–	–

SD-Branch 活用時の対応機器数

機種	対応 FortiSwitch 数	対応 AP 数（トンネルモード）
FortiGate 60F	24	32
FortiGate 120G	32	64
FortiGate 600F	96	512
FortiGate 1800F/2600F	196	2048
FortiGate 3000F/3500F/3700F	300	2048

* 上記はあくまでも目安です。使用する機能で条件は変わります。

より使いやすくするお勧め製品

FortiAP

FortiAP は、無線 LAN コントローラ機能を備えた FortiGate/FortiWiFi で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、包括的で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 431F/FortiAP 433F は Wi-Fi 6（IEEE802.11ax）対応です。

	FortiAP 431F	FortiAP 433F	FortiAP 231F	FortiAP 234F
設置環境	屋内	屋内	屋内	高耐久性 屋内 / 屋外
ハードウェア				
ラジオ数	3 + 1（BLE）	3 + 1（BLE）	3 + 1（BLE）	3 + 1（BLE）
アンテナ数	5（内蔵）+ 1（内蔵 / BLE）	5（外部、RP-SMA）+ 1（内蔵 / BLE）	3（デュアルバンド / 内蔵 / Wi-Fi）+ 1（BLE / ZigBee）	2（デュアルバンド / Wi-Fi）+1（デュアルバンドスキャン）+1（シングルバンド 2.4 GHz BLE / ZigBee）
Radio 1（対応する周波数帯と無線技術）	対応する周波数帯：2.4 GHz チャンネル幅：4 × 4 20 / 40 MHz 変調：BPSK、QPSK、QAM64、QAM256、QAM1024 MIMO チェーン：4 × 4 サービス		対応する周波数帯：2.4 GHz チャンネル幅：20 / 40 MHz 変調：BPSK、QPSK、64 / 256 / 1024 QAM MIMO チェーン：2 × 2 サービス	対応する周波数帯：2.4 GHz チャンネル幅：20 / 40 MHz 変調：BPSK、QPSK、64 / 256 / 1024 QAM MIMO チェーン：2 × 2 サービス
Radio 2（対応する周波数帯と無線技術）	対応する周波数帯：5.0 GHz チャンネル幅：4 × 4 20 / 40 / 80 MHz、2 × 2 160 MHz 連続したチャネル 変調：BPSK、QPSK、QAM64、QAM256、QAM1024 MIMO チェーン：4 × 4 サービス		対応する周波数帯：5.0 GHz チャンネル幅：20 / 40 / 80 MHz 変調：BPSK、QPSK、64 / 256 / 1024 QAM MIMO チェーン：2 × 2 サービス	対応する周波数帯：5.0 GHz チャンネル幅：20 / 40 / 80MHz 変調：BPSK、QPSK、64 / 256 / 1024 QAM MIMO チェーン：2 × 2 サービス
Radio 3（対応する周波数帯と無線技術）	対応する周波数帯：2.4 / 5.0 GHz MIMO チェーン：1 × 1 周波数スキャン		対応する周波数帯：2.4 / 5.0 GHz MIMO チェーン：1 × 1 周波数スキャン	対応する周波数帯：2.4 / 5.0 GHz MIMO チェーン：1 × 1 周波数スキャン
最大データレート	Radio 1：最大 1,147 Mbps Radio 2：最大 2,402 Mbps Radio 3：スキャンのみ	Radio 1：最大 1,147 Mbps Radio 2：最大 2,402 Mbps Radio 3：スキャンのみ	Radio 1：最大 574 Mbps Radio 2：最大 1,201 Mbps Radio 3：スキャンのみ	Radio 1：最大 574 Mbps Radio 2：最大 1,200 Mbps Radio 3：周波数スキャンのみ
Bluetooth Low Energy 無線	6 dBm の最大送信電力での Bluetooth スキャニング および iBeacon アドバタイズメント		10 dBm の最大送信電力での Bluetooth スキャニング および iBeacon アドバタイズメント	10 dBm の最大送信電力での Bluetooth スキャニング および iBeacon アドバタイズメント
インタフェース	1 x 100 / 1000 / 2500 Base-T RJ45、1 x 10 / 100 / 1000 Base-T RJ45、1 x Type A USB、1 x RS-232 RJ45 シリアル管理インタフェース		2 x 10 / 100 / 1000 Base-T RJ45、1 x Type 2.0 USB、1 x RS-232 RJ45 シリアル管理インタフェース	2 x 10 / 100 / 1000 Base-T RJ45、1 x RS-232 RJ45 シリアル管理インタフェース
PoE（Power over Ethernet）	・802.3at PoE 標準仕様 ・1 ポート（802.3at 供給の電源）または 2 ポート（802.3af 供給の電源）- 完全システム機能 + USB サポート ・1 ポートを 802.3af に接続 - USB サポートなし、省電力 R1/R2 17dBm（送信電力）の 2 × 2 モードで動作		・802.3at PoE 標準仕様 ・1 ポート（802.3at 供給の電源）- 完全システム機能 +USB サポート ・1 ポートを 802.3af に接続 - USB サポートなし	・802.3at PoE 標準仕様（パッシブ PoE インジェクター付属） ・1 ポート（802.3at 供給の電源）または 2 ポート（802.3af 供給の電源）- 完全システム機能 ・1 ポートを 802.3af に接続 - USB サポートなし、省電力 R1/R2 17dBm（送信電力）の 2 × 2 モードで動作
同時 SSID	ラジオあたり最大 8（バックグラウンドスキャンが有効の場合 7）		ラジオあたり最大 8（バックグラウンドスキャンが有効の場合 7）	ラジオあたり最大 8（バックグラウンドスキャンが有効の場合 7）
最大送信電力（Conducted 規定）	Radio 1：2.4 GHz：24 dBm / 251 mW（4 チェーン混合時）* Radio 2：5 GHz：23 dBm / 200 mW（4 チェーン混合時）* Radio 3：–		Radio 1：2.4 GHz：23 dBm / 200 mW（2 チェーン混合時）* Radio 2：5 GHz：22 dBm / 158 mW（2 チェーン混合時）* Radio 3：—	Radio 1：2.4 GHz：27 dBm / 500 mW：（2 チェーン混合時）* Radio 2：5 GHz：25.5 dBm / 354 mW（2 チェーン混合時）* Radio 3：—
ラジオあたりのクライアント数	Radio 1 および Radio 2：最大 512	Radio 1 および Radio 2：最大 512	Radio 1 および Radio 2：最大 512	Radio 1 および Radio2：最大 512

* 実際の送信電力は、技術基準適合証明に記載された値となります。

セキュア SD-Branch ソリューションを支える FortiSwitch のラインナップ

FortiSwitch 108F

FortiSwitch 148F

エントリーレベル

FortiSwitch 100 シリーズ

- 8 ～ 48 ポート x GE インタフェース、PoE+ 対応
- デスクトップ～ワイヤリングクローゼットスイッチ
- 2 x GE SFP（FS108F）/4 x 10 GE SFP+（FSW124F、148F）アップリンクポート

FortiSwitch 224E

FortiSwitch 248E

ミッドレンジ

FortiSwitch 200 シリーズ

- 24 ～ 48 ポート x GE インタフェース、PoE+ 対応
- 標準的なワイヤリングクローゼットスイッチ
- 4 x GE SFP アップリンクポート

FortiSwitch 448E

FortiSwitch 548D

プレミアム

FortiSwitch 400/500 シリーズ

【400 シリーズ】エンタープライズスイッチ

- 24 ～ 48 ポート x GE インタフェース、PoE+ 対応
- 大規模ワイヤリングクローゼットまたは高スループット向け
- 4 x 10 GE SFP アップリンクポート

【500 シリーズ】アグリゲーションスイッチ

- 4 ～ 48 ポート x GE インタフェース、PoE+ 対応
- 大規模ワイヤリングクローゼットまたは高スループット向け
- 4 x 10 GE + 2 x 40 GE SFP アップリンクポート

FortiSwitch 1048E

FortiSwitch 3032E

データセンター

FortiSwitch 1000/2000/3000 シリーズ

- 1 RU で GE/10 GE/100 GE インタフェースを利用可能
- 40 GE/100 GE のアップリンクをサポート
- FortiLink を利用して FortiGate を管理でき、セキュリティファブリックを構成可能
- 1 台の FortiGate に最大 300 台のスイッチをスタック接続可能（機種によって異なります）
- ホットスワップ対応の冗長電源
- ストアアンドフォワードおよびカットスルー両方の転送モードでワイヤスピードのスイッチングをサポート

各モデルのスペック比較

FortiSwitch 100 シリーズ	108F	108F-PoE/ 108F-FPoE	124F	124F-PoE/ 124F-FPoE	148F	148F-PoE/ 148F-FPoE
ポート数	8 x GE RJ45 2 x GE SFP (PoE 受電可能)	8 x GE RJ45 2 x GE SFP	24 x GE RJ45 4 x GE SFP	24 x GE RJ45 4 x 10 GE SFP+	48 x GE RJ45 4 x 10 GE SFP+	48 x GE RJ45 4 x 10 GE SFP+
PoE ポート数	N/A	4/8（802.3af/at）	N/A	12/24（802.3af/at）	N/A	24/48（802.3af/at）
PoE 容量（シャーシ）	N/A	65W/130W	N/A	185W/370W	N/A	370W/740W
筐体サイズ	デスクトップ	デスクトップ	デスクトップ	1 RU	1 RU	1 RU
スイッチ容量	20 Gbps	20 Gbps	128 Gbps	128 Gbps	128 Gbps	176 Gbps

FortiSwitch 200 シリーズ	224D-FPoE	224E	224E-PoE	248D	248E-PoE/248E-FPoE
ポート数	24 x GE RJ45 4 x GE SFP	24 x GE RJ45 4 x GE SFP	24 x GE RJ45 4 x GE SFP	48 x GE RJ45 4 x GE SFP	48 x GE RJ45 4 x GE SFP
PoE ポート数	24（802.3af/802.3at）	N/A	12（802.3af/802.3at）	–	24/48（802.3af/802.3at）
PoE 容量（シャーシ）	370 W	N/A	180 W	N/A	370 W/740 W
筐体サイズ	1 RU	1 RU	1 RU	1 RU	1 RU
スイッチ容量	56 Gbps	56 Gbps	56 Gbps	104 Gbps	104 Gbps

FortiSwitch 400 シリーズ	424D	424D-PoE/ 424D-FPoE	448D	448D-PoE/ 448D-FPoE	424E-FIBER
ポート数	24 x GE RJ45 2 x 10 GE SFP+*1	24 x GE RJ45 2 x 10 GE SFP+*1	48 x GE RJ45 4 x 10 GE SFP+*1	48 x GE RJ45 4 x 10 GE SFP+*1	24 x GE SFP 4 x 10 GE SFP+*1
PoE ポート数	–	24（802.3af/at）	–	48（802.3af/at）	N/A
PoE 容量（シャーシ）	N/A	185 W/370 W	N/A	370 W/740 W	N/A
筐体サイズ	1 RU	1 RU	1 RU	1 RU	1 RU
スイッチ容量	88 Gbps	88 Gbps	176 Gbps	176 Gbps	128 Gbps

FortiSwitch 400 シリーズ	M426E-FPoE	424E	424E-PoE/ 424E-FPoE	448E	448E-PoE/ 448E-FPoE
ポート数	16 x GE RJ45 8 x 2.5 GE RJ45 2 x 5 GE RJ45 4 x 10 GE SFP+*1	24 x GE RJ45 4 x 10 GE SFP+*1	24 x GE RJ45 4 x 10 GE SFP+*1	48 x GE RJ45 4 x 10 GE SFP+*1	48 x GE RJ45 4 x 10 GE SFP+*1
PoE ポート数	24（16x 802.3af/at, 8x 802.3af/at/UPoE）	–	24（802.3af/at）	–	48（802.3af/at）
PoE 容量（シャーシ）	420 W	N/A	250 W/421 W	–	421 W/772 W
筐体サイズ	1 RU	1 RU	1 RU	1 RU	1 RU
スイッチ容量	172 Gbps	128 Gbps	128 Gbps	176 Gbps	176 Gbps

FortiSwitch 500 シリーズ	524D	524D-FPoE	548D	548D-FPoE
ポート数	24 x GE RJ45 4 x 10 GE SFP+*1 2 x 40 GE QSFP*2	24 x GE RJ45 4 x 10 GE SFP+*1 2 x 40 GE QSFP*2	48 x GE RJ45 4 x 10 GE SFP+*1 2 x 40 GE QSFP*2	48 x GE RJ45 4 x 10 GE SFP+*1 2 x 40 GE QSFP*2
PoE ポート数	N/A	24（802.3af/at）	N/A	48（802.3af/at）
PoE 容量（シャーシ）	N/A	400 W	N/A	750 W
筐体サイズ	1 RU	1 RU	1 RU	1 RU
スイッチ容量	288 Gbps	288 Gbps	336 Gbps	336 Gbps

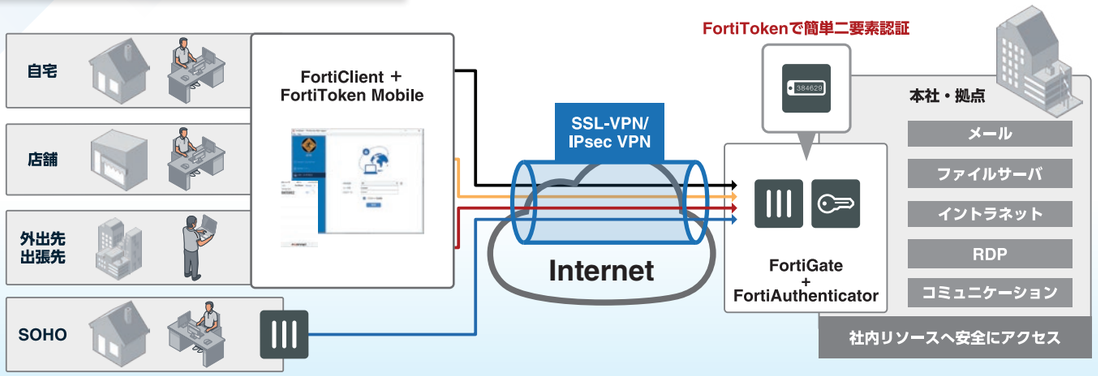
FortiSwitch 1000/2000/3000 シリーズ（コア / データセンタースイッチ）	1024E	T1024E	1048E	2048F	3032E
ポート数	24 x 10 GE SFP+ 2 x 100 GE QSFP28	24 x GE/MGIG/10 GE 2 x 100 GE QSFP28	48 x GE/10 GE SFP/SFP+ 6 x 40 GE QSFP+ または 4 x 100 GE QSFP28	48 x 25 GE SFP28 2 x 10 GE SFP+ 8 x 100 GE QSFP28	332 x 100 GE QSFP28
筐体サイズ	1 RU	1 RU	1 RU	1 RU	1 RU
スイッチ容量	880 Gbps	880 Gbps	1760 Gbps	4000 Gbps	6400 Gbps

*1：SFP+ インタフェースは 1GE SFP インタフェースと互換性があります。
*2：40 GE インタフェースは 4 x 10 GE にスプリット可能です。

テレワークを維持・促進するための セキュアなリモートアクセスソリューション

事業の継続と従業員の安全の両方を確実に達成するためには、テレワークを実践する従業員を支援する環境作りが不可欠です。フォーティネットは、従業員のテレワークを支援する統合ソリューションを提供します。
FortiGate は、IPsec VPN（仮想プライベートネットワーク）を標準でサポートしており、従業員はリモート環境から安全に企業ネットワークへ接続できます。FortiClient が提供するエンドポイント保護、さらに FortiAuthenticator による MFA（多要素認証）を活用することで、企業組織は従業員のテレワークを支援すると同時に事業オペレーションを継続させることが可能になります。

どこからでも安全にリモートアクセス



ワンタイムパスワードを簡単運用

ソリューションのポイント

1 社外のさまざまな拠点、場所ですぐに VPN 接続を利用でき、FortiAuthenticator や FortiToken による認証処理で安全性も確保！

2 ワンタイムパスワードをその都度手入力する必要がなく、誰でも簡単に、安全なリモートアクセスを利用可能！

FortiAuthenticator

FortiAuthenticator は、ユーザーのアイデンティティ管理とシングルサインオン機能を提供する認証ソリューションです。セキュアな Fortinet Single Sign-On（FSSO）認証システムを基盤としており、既存の Active Directory や LDAP 認証システムと統合することで、ユーザーの生産性を低下させたりネットワーク管理者の作業負荷を高めることなく、企業においてユーザーのアイデンティティベースの確実なセキュリティを実現します。FortiAuthenticator は、フォーティネット製品で保護されている企業ネットワークへのアクセスを許可するゲートキーパーとして機能し、ユーザーの識別やサードパーティ製システムからのアクセス許可の照会を実行するほか、このような情報を FortiGate デバイスと交信してアンデンティティベースのポリシー実施に活用することができます。

- セキュアな二要素 /OTP 認証と FortiToken/FortiToken Mobile の完全サポート
- FortiToken 410 などの FIDO2 トークンによる FIDO2 認証をサポート
- RADIUS、LDAP および SAML 認証、OAuth に対応
- 企業の VPN 導入における証明書の管理機能
- IEEE802.1X に対応し、無線 / 有線ネットワークのセキュリティを確保
- SAML SP/IdP Web SSO

仮想アプライアンス	FortiAuthenticator VM Base	FortiAuthenticator VM-100-UG	FortiAuthenticator VM-1000-UG	FortiAuthenticator VM-10000-UG	FortiAuthenticator VM-100000-UG
Capacity					
ローカルユーザー数	100	+100	+1,000	+10,000	+100,000
リモートユーザー数	100	+100	+1,000	+10,000	+100,000
FortiToken サポート数	200	+200	+2,000	+20,000	+200,000
NAS デバイス	33	+33	+333	+3,333	+33,333
ユーザーグループ	10	+10	+100	+1,000	+10,000
CA 証明書サポート数	5	+5	+50	+500	+500
クライアント証明書サポート数	100	+100	+ 1,000	+10,000	+100,000

FortiTrust

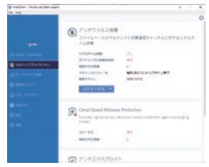
FortiTrust Identity は、クラウドベースの認証プロキシサービスです。多要素認証を含むユーザー認証の集中管理を提供します。

- 可用性の高いマネージドクラウドサービス
- FortiToken Mobile プッシュや配布をサポート
- FortiGate を含む Fortinet 製品の認証インフラとして機能

FortiToken/ FortiToken Mobile

二要素認証に欠かせない
ワンタイムパスワード製品

P24へ



FortiClient

セキュアなアクセスを支える
リモートアクセスクライアント

P22へ

FortiToken 410

FIDO2 認証に用いることができる認証器

P24へ

FortiClient EMS

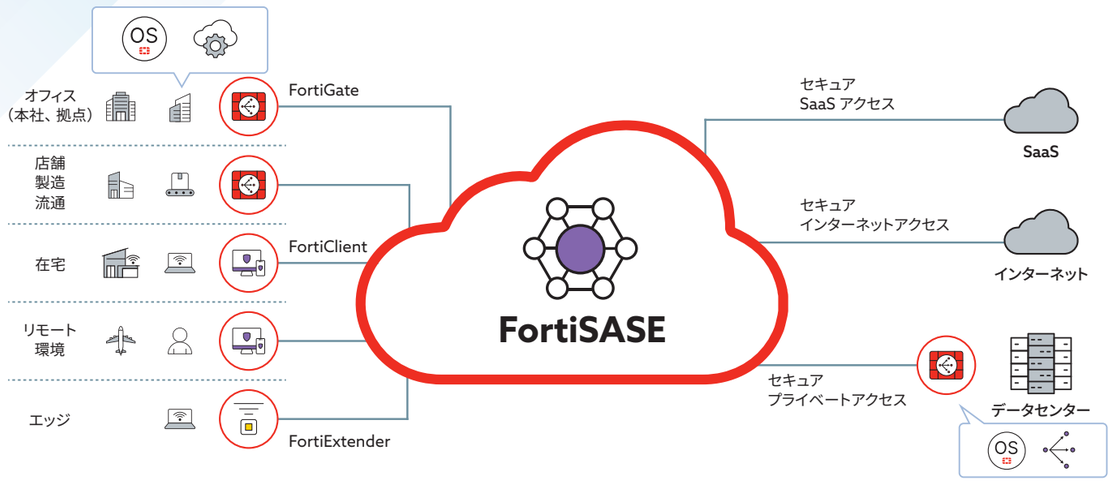
FortiGate へのゼロトラストネットワークアクセスの提供、各種エンドポイントの一元管理ソリューション

P23へ

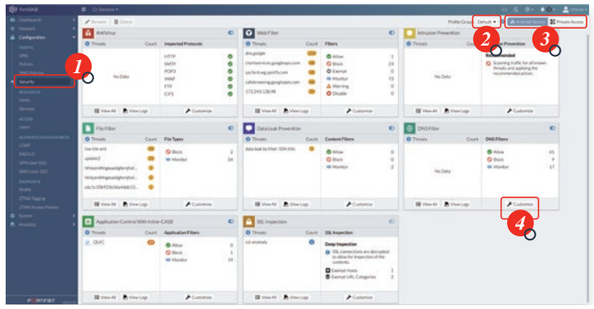
いつでもどこでも安全なネットワーク利用を実現するシングルベンダーのSASEソリューション

FortiSASE は、一貫性のあるセキュリティ体制をあらゆるユーザーに提供し、セキュリティポリシーの管理も簡素化します。シングルベンダーによる SASE ソリューションは、SWG（セキュア Web ゲートウェイ）、ユニバーサル ZTNA、CASB、FWaaS、セキュア SD-WAN の統合など、ネットワーキングとセキュリティのすべての機能を提供し、1 つのコンソール画面でシンプルに管理できます。

一貫性のある OS と AI/ 機械学習を活用したセキュリティ



シングルコンソールで運用管理はシンプル



1. FortiOS のセキュリティをシングルペインで簡素化
2. デフォルトのプロファイルを用いて素早い展開と利用開始が可能
3. Web とプライベートアプリケーションの区別を表示
4. セキュリティプロファイルはカスタマイズ可能

ソリューションのポイント

1. 既存のネットワーク資産（FortiGate）を有効活用。導入済みの FortiGate を使って、セキュア SD-WAN と ZTNA の両方を実現
2. 優先的な課題から環境整備が可能。必要なところから段階的な導入～移行することで、リスクとコストを抑制

FortiSASE の構成要素

基盤となるフォーティネット独自の技術・サービス

- FortiOS P4へ
- FortiGuard AI活用 セキュリティサービス P4へ
- クラウドベースの管理 P34へ

ネットワーク

- SD-WAN P8へ
- アプリケーションの可視化と制御 P32へ

クライアント、エッジ

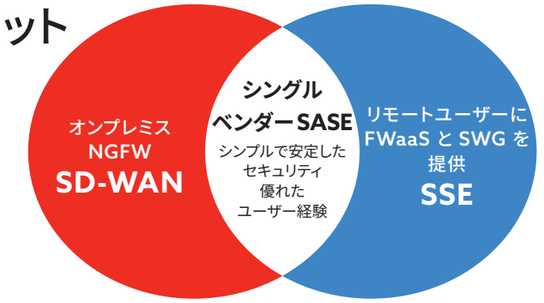
- FortiGate SD-WAN P10へ
- FortiClient ユニファイドエージェント P22へ
- FortiExtender

セキュリティ

- SWG（セキュア Web ゲートウェイ） P25へ
- FWaaS（ファイアウォール as a Service）
- ユニバーサル ZTNA（ゼロトラストネットワークアクセス） P22へ
- インライン/API デュアルモードCASB（クラウドアプリケーションサービスブローカー）

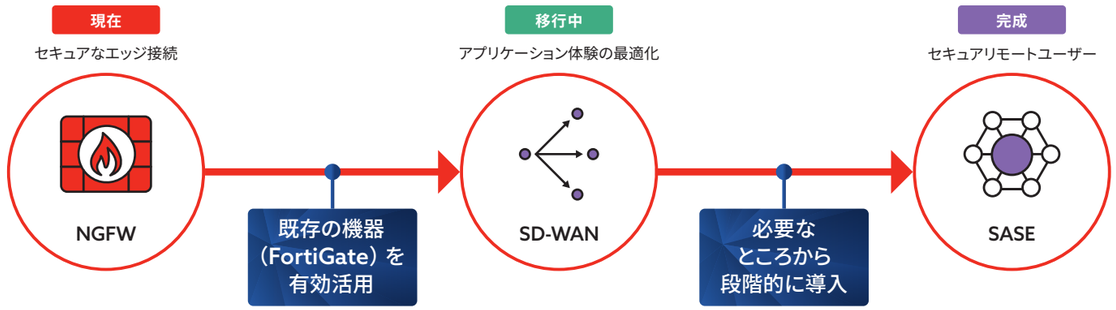
シングルベンダー SASE のメリット

- オンプレミスとリモートユーザーのネットワークを融合
- リスクポスチャの改善とセキュリティギャップの削減
- 複数の製品を排除してシンプルさを実現
- シングルエージェントによる効率的な運用
- 製品とベンダーの削減によるコストの削減



ネットワーキング SD-WAN ＋ セキュアサービスエッジ SSE

既存の環境から SASE へ段階的に移行



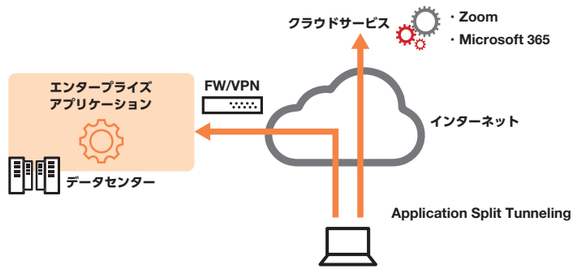
FortiClient

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。Work From Anywhere を実現するためにセキュアな認証を使用したリモートアクセスだけではなく、アプリケーションにより接続を使い分けるアプリケーションブレイクアウト、クライアント自身を保護するサンドボックス対応を含むアンチマルウェア、アプリケーションファイアウォール、USB 制御、URL フィルタリング機能を提供します。

- 実行中のアプリケーションやファームウェアのバージョンなど、デバイスのステータスをセキュリティファブリックに報告
- 疑わしいファイルをファブリックサンドボックスに送信
- アプリケーション制御、USB 制御、URL フィルタリング、ファームウェアアップグレードポリシーの適用
- マルウェアからの保護
- アプリケーションファイアウォールサービスを提供
- デバイスを VPN（SSL もしくは IPsec）または ZTNA トンネル経由でセキュリティファブリックに安全に接続

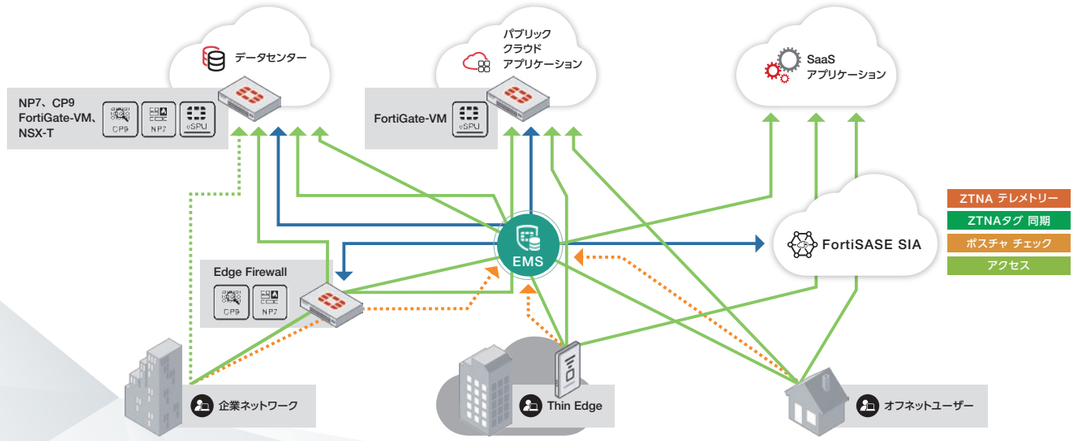
Application Split Tunneling

Application Split Tunneling によって、Windows Update やリモート会議、信頼できる SaaS への接続を VPN を介さずに行えます。これによって VPN 接続先の FortiGate のリソース節約や通信回線（帯域）の効率化が可能です。



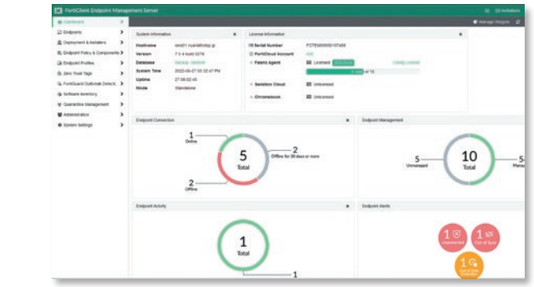
FortiClient ZTNA

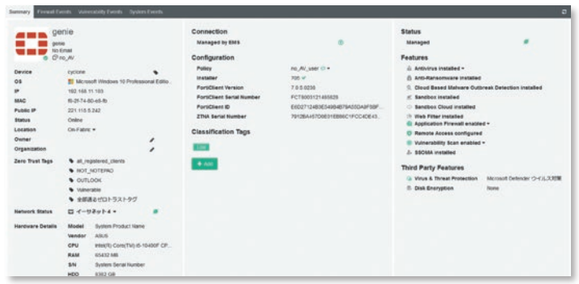
FortiClient ZTNA（Zero Trust Network Access）は、これまでの VPN のような L3 ベースの接続ではなく、アプリケーションのセッションごとにそれぞれリソースがある拠点の FortiGate、もしくはクラウドサービスへ認証と端末のコンディションチェックを行った上でシームレスに接続します。



FortiClient EMS

FortiClient EMS（Enerprise Management Server）は、Windows、Mac、Linux、Chrome、iOS および Android のエンドポイントに対するインストール / アンインストール、アップグレードポリシーの適用など一元管理機能を提供します。ソフトウェアのインベントリ管理によるインストールされたソフトウェアアプリケーションおよびライセンス管理の可視化、Active Directory との統合、FortiClient の一元配備などが利用できます。また、リアルタイムでエンドポイントのステータスが表示されるので、エンドポイントの最新アクティビティやセキュリティイベントを常に把握でき、脆弱性のあるエンドポイントを容易に特定できる脆弱性ダッシュボードもあります。

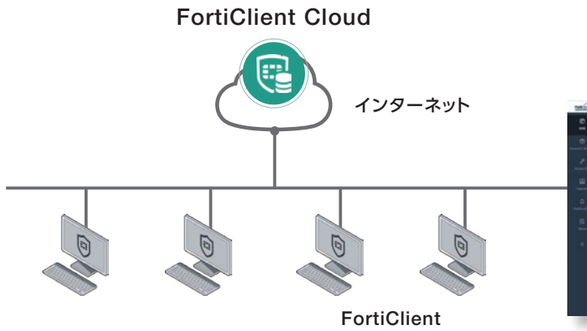


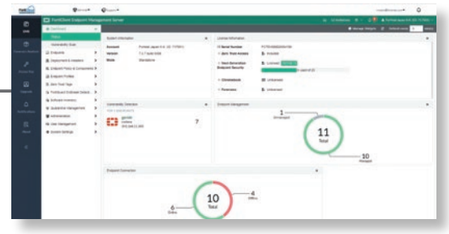


FortiClient Cloud

FortiClient Cloud は、FortiClient EMS と同等の機能をクラウドサービスとして提供します。

- FortiClient の集中管理
- クライアント上のアプリケーション情報管理（ソフトウェアインベントリ）
- クライアントの脆弱性管理 - 各クライアントへのアプリケーションパッチ配信
- コンプライアンス管理
- エンドポイントポリシー / エンドポイントプロファイル管理
- クライアント隔離（Quarantine）





FortiToken/FortiToken Mobile

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。モバイルデバイス向けの「FortiToken Mobile」もあります。

FortiToken 210

- OATH TOTP 準拠
- 大型で見やすい LCD ディスプレイ
- 長寿命リチウム電池
- 不正開封防止 / 不正開封明示機能付き
- CD 付属（シード買い切りモデル、オフライン対応）
- オプションあり

FortiToken 310

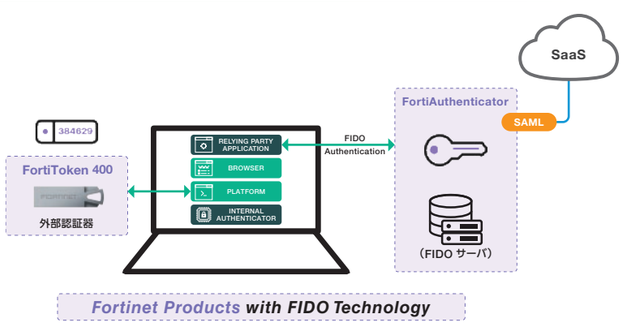
- FIPS140-2 Level 3 認定
- Windows、Linux および MacOS をサポート
- Microsoft CAPI および PKCS#11 API をサポート
- NIST FIPS CAVP 承認済のオンボード RSA、AES、DES / 3DES、SHA-1、SHA-256 アルゴリズム
- 不正開封明示機能付のハードウェア USB トークン
- さまざまな PKI インフラストラクチャと容易に統合可能

FortiToken 410

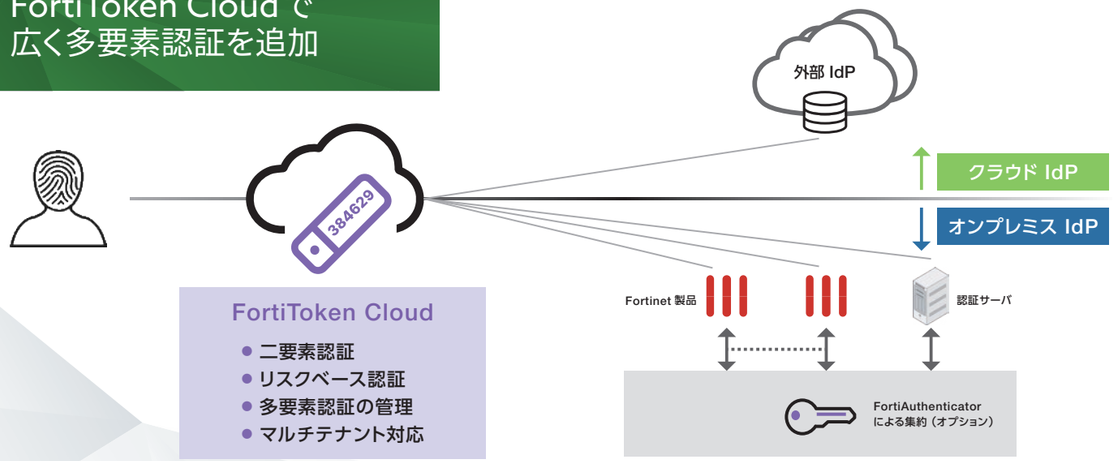
- FIDO U2F、FIDO2 対応
- HOTP 対応
- FortiAuthenticator と組み合わせることでパスワードレス認証を提供
- SSL-VPN や Web 認証に対応
- パスワードに関連するサポートコストを削減

FortiToken 400 による パスワードレス認証

- パスワードを使うことを狙う攻撃から解放
  - パスワードを紛失しない
  - パスワードを忘れない
  - ブルートフォースに耐えうる
- 他のサイトに盗み出されることがない
- ドライバーのインストールも開発も不要
- パスワードに関連するサポートコストを削減



FortiToken Cloud で 広く多要素認証を追加



FortiWeb

FortiWeb は、既知 / 未知両方の脆弱性に対するエクスプロイトの攻撃から、ホスティングされている Web アプリケーションを保護する WAF（Web アプリケーションファイアウォール）です。AI を活用した多層型の相関的な検知メソッドを活用することで、既知およびゼロデイ脆弱性の脅威からアプリケーションを保護します。

FortiWeb 4000F

VM/ コンテナ環境

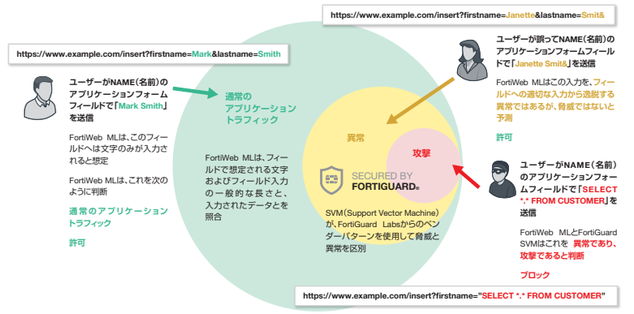
FortiWeb Cloud

総合的な Web アプリケーション セキュリティを実現

FortiWeb の多層型で相関付けに基づく脅威検知のアプローチは、アプリケーションの脆弱性を標的にする既知および未知のゼロデイ脆弱性の脅威からの保護を提供します。

FortiGuard Labs を活用した 2 層構造の機械学習

FortiWeb の AI ベースの機械学習はアプリケーション要求を評価し、正常、無害の異常、または脅威である異常のいずれであるかを判断します。



	FortiWeb 400E	FortiWeb 600E	FortiWeb 1000E	FortiWeb 2000F	FortiWeb 3000F	FortiWeb 4000F
システム性能						
スループット	250 Mbps	750 Mbps	1.3 Gbps	5 Gbps	10 Gbps	70 Gbps
レイテンシ	5 ms 以下					
高可用性	アクティブ / パッシブ、アクティブ / アクティブクラスタリング					
SSL/TLS 処理	ソフトウェア	ソフトウェア	ハードウェア	ハードウェア	ハードウェア	ハードウェア
電源	シングル	デュアル	デュアル / 交換可	デュアル / 交換可	デュアル / 交換可	デュアル / 交換可
アプリケーションライセンス	無制限					
管理ドメイン	32	32	64	96	96	192

FortiWeb VM	VM01	VM02	VM04	VM08	VM16
FortiWeb VMC ※コンテナマネージャーは Docker をサポートします	VMC01	VMC02	VMC04	VMC08	–
HTTP スループット	25 Mbps	100 Mbps	500 Mbps	3 Gbps	6 Gbps
推奨メモリ	8 GB	8 GB	16 GB	32 GB	64 GB
アプリケーションライセンス	無制限				
管理ドメイン	4 ～ 64（割り当てられているメモリによって異なります）				

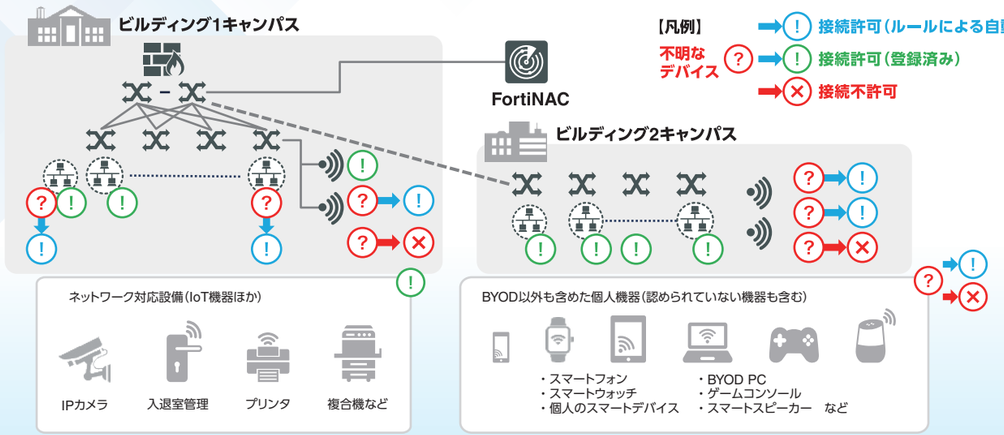
FortiWeb Cloud	
サポートするクラウド	AWS Marketplace、Microsoft Azure、Google Cloud、Oracle Cloud Infrastructure
ライセンス形態	従量課金

* 数値はすべて「最大」の性能値であり、システム構成に応じて異なります。

あらゆるデバイス・ユーザーを可視化する IoT/OT 向けソリューション

IoT環境の可視化

FortiNACで既知 / 未知のデバイス、
IoTデバイスをすべて可視化し通信を制御

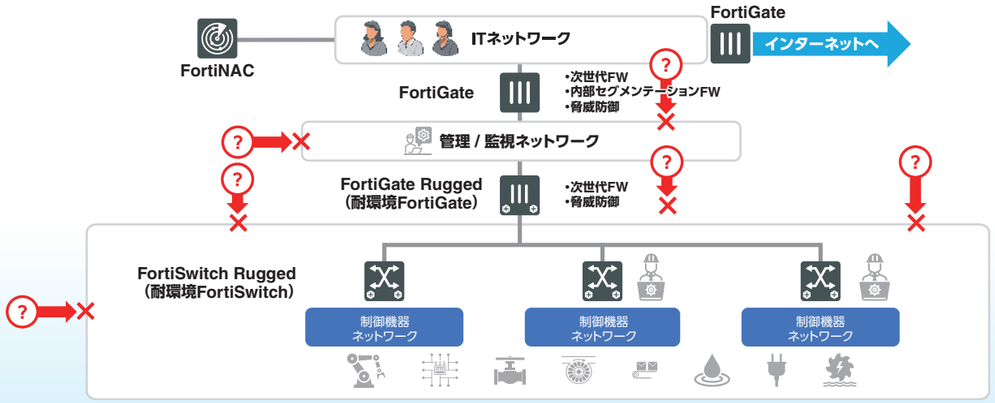


ポイント

- エージェントレス&非侵襲
- マルチベンダーのインフラに対応
- すべてのデバイスを可視化可能
- 未知のデバイスも検知可能
- 管理者が接続をコントロール可能
- 接続事前テンプレートで設定や運用が容易
- デバイス種別による自動仕分けが可能

OT環境の可視化

FortiNACで製造現場などOT環境を
可視化して登録外ノード / 通信を排除

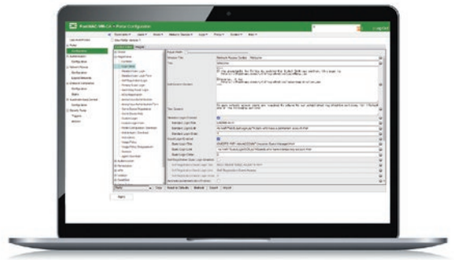


ポイント

- エージェントレスで運用
- 耐環境製品をラインナップ
- すべてのデバイスを可視化可能
- 未知のデバイスをすべて排除
- 未知の通信をすべて排除
（通信のホワイトリスト運用）
- FortiGate でセグメンテーションを実現

FortiNAC

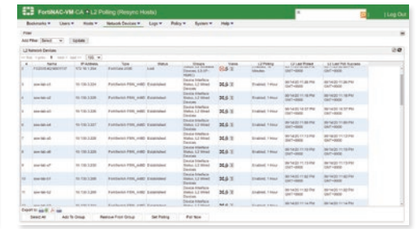
FortiNAC は、ネットワークに接続するあらゆるデバイスの可視化、制御、そしてイベント対応の自動化によってセキュリティファブリックの拡張を可能にする、フォーティネットのネットワークアクセス制御ソリューションです。FortiNAC によって、IoT に対する脅威からの保護が実現し、サードパーティデバイスへのアクセス制御の拡張、さまざまなネットワーキングデバイスへの自動レスポンスのオーケストレーションが可能になります。



- ネットワークスキャンによるデバイスの検知、分類
- ネットワーク上のあらゆるデバイスのインベントリを作成
- ネットワーク上のすべてのエンドポイントのリスクを評価
- 広範なサードパーティのネットワークデバイスをサポート
- 多数のエンドポイント、ユーザー、ゲストの初期登録プロセスを自動化
- ネットワークアクセスの動的な制御を適用し、ネットワークセグメンテーションを実現
- 隔離に要する時間を数日から数秒へと短縮

仮想アプライアンス					
ネットワークサイズ	推奨利用環境	仮想サーバ	vCPU**	メモリ	ディスク
ネットワークで最大2,000 ポート *	小規模環境	FortiNAC Control and Application VM	4	16 GB	100 GB
ネットワークで最大15,000 ポート *	中規模環境	FortiNAC Control and Application VM	6	32 GB	100 GB
ネットワークで最大25,000 ポート *	大規模環境	FortiNAC Control and Application VM	14	96 GB	100 GB
無制限	大規模環境	FortiNAC Manager VM	4	12 GB	100 GB

* ネットワークの「ポート数」は、エッジスイッチのポート数、無線 LAN アクセスによる最大同時接続数の総計です。
FortiNAC では、アプライアンスの性能はデバイス数ではなく総ポート数をベースにします。
**vCPU 欄の値はガイドラインであり、個別の環境によって異なります。



FortiNAC ライセンス種別

BASE

OT、IoT など
ドメインコンピュータの検出と制御

（BASEに含まれるすべてのオプションについては以下を参照）

PLUS

BASE 機能＋ユーザーの可視性 / 制御、キャプティブポータル、より深いエンドポイントコンプライアンス

- 802.1x EAP（EAP-TLS、PEAP、LEAP、TTLS、MD5、GTC）
- 負荷の軽いNACエージェント（dissolvable、Passive、Persistent）
- Windows、OSX、Linuxのエンドポイントコンプライアンス
- BYOD、コントラクター、ゲスト向けのキャプティブポータル
- FAZ、SIEM、Syslog、またはAPIへのアウトバウンドセキュリティイベント
- NAC for VPN（Cisco ASAおよびFortiGate）

PRO

PLUS 機能＋セキュリティイベントへの応答

- IPS / SIEM / Tenable/Qualysからトリガーイベントを受信する
- ユーザーやデバイスの種類、時刻、場所に基づく分離と通知のオプション
- 侵入の痕跡を使用してホストをすぐに分離する

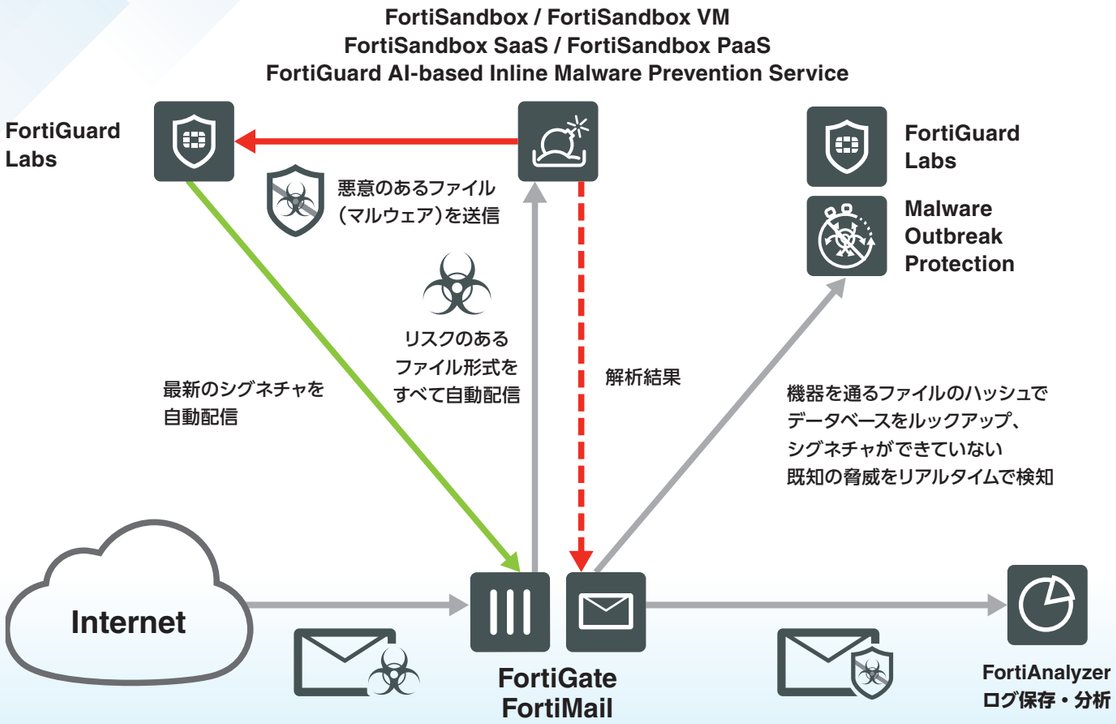
■ 基本機能

●動的エンドポイントデータベースと LDAP ユーザーディレクトリ統合を作成するネットワークインベントリの検出
●エンドポイントの分類、不正端末検出

- MDM統合：AirWatch、FortiEMS、Google Workspace、JAMF、MaaS360、Microsoft Intune、Mobile Iron、Nozomi、Citrix Endpoint Management
- デバイスプロファイル：アクティブ（NMAP）、DHCP fingerprint、FortiGate連携、FortiGuard IoTサービス、HTTP / HTTPS、IP範囲、場所、Netflow、ONVIF、Perl、SNMP、SSH、TCPポート、Telnet、UDPポート、ベンダーOUI、WinRM、およびWindowsプロファイル（WMI）
- Fortinetシングルサインオン
- NAC制御
- 不正なデバイスの検出と封じ込め
- ネットワークアクセスポリシー自動セグメンテーション（プロファイルとVLAN割り当て）
- SwitchとAPを制御する基本的なRADIUS MAB&PROXY
- Rest APIを使用したFortiGate自動化ステッチ
- API入力/出力

標的型攻撃へ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当たり、『重要』として定義された「サンドボックス装置の導入」は、一般企業でも標的型攻撃への有効な対策として導入されています。フォーティネットのサンドボックス製品である FortiSandbox は、検知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。



ソリューションのポイント

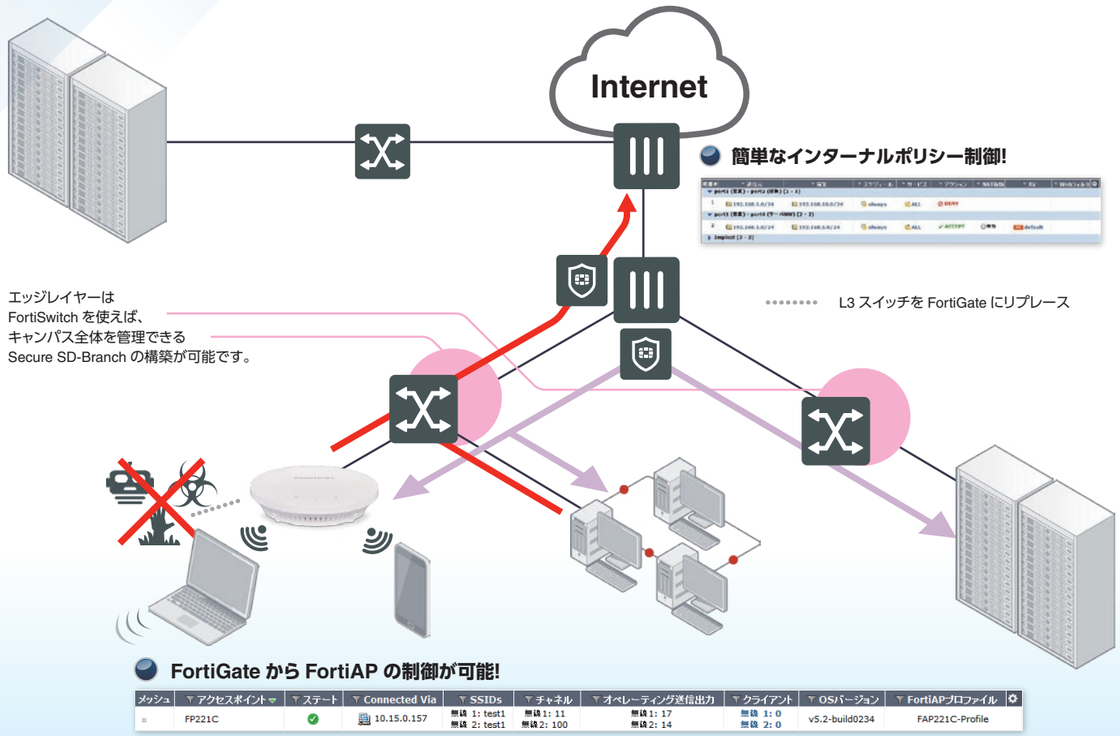
1 ファイルハッシュ値を問い合わせることで FortiGuard で危険と判断されたファイルをリアルタイムに検知

2 検知したマルウェアは FortiGuard Labs に自動送信され、FortiGate/FortiMail と連携し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 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、標的型攻撃への最適化されたディフェンスを提供！

内部セグメンテーション・ファイアウォールとして FortiGate を活用

内部セグメンテーション・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いました。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 にリプレイスすることで、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。



ソリューションのポイント

1 内部セグメンテーション・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イス！

3 FortiAP との組み合わせで、無線通信も FortiGate で制御可能！

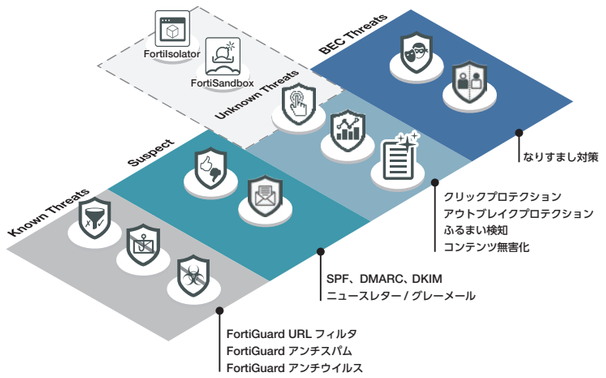
FortiMail/FortiMail Cloud

E メールは現代のビジネスには不可欠ですが、技術的な攻撃だけではなく、ソーシャルエンジニアリングや騙りによって人をだます攻撃にも用いられることが多いツールとなっています。標的として狙われている場合、また無差別な攻撃者からの攻撃の場合でも巧妙化が進み、複数のベクトルを持った攻撃活動が発生するようになっています。多層攻撃への防御、そして E メールという攻撃ベクトルへ対応するために、FortiMail や FortiMail Cloud は極めて有効なソリューションです。

FortiMail/FortiMail Cloudが提供する高度なマルチレイヤーセキュリティ

- 既知の脅威
- 疑わしい脅威
- 未知の脅威 / ゼロデイ
- なりすましの試み
- ビジネスメール詐欺

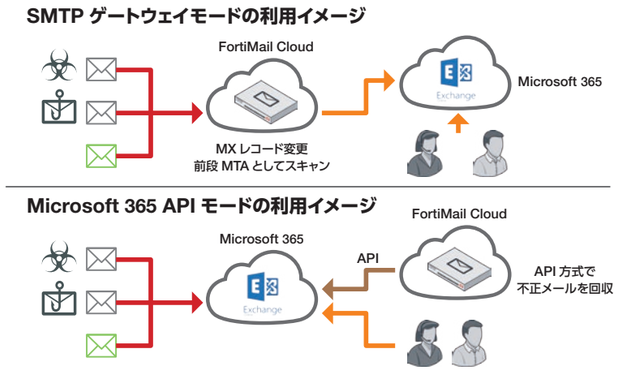
FortiMail コンテンツベースのメール防御
FortiMail 添付ファイルベースのメールからの脅威防御
FortiMail URL ベースのメール脅威防御
FortiMail ビジネスメール詐欺の防止
Microsoft 365 との連携［ゲートウェイモード］



FortiMail Cloudの動作モード

SMTP ゲートウェイモード：
FortiMail をメールの入り口とすることで防御を提供

Microsoft 365 API モード：
Microsoft 365のメールサービスへ API 経由でアクセスし、メールの安全を確認できるまでユーザーへ見せないことで防御を提供



選択可能なライセンスと提供機能

FortiMail Cloud：ゲートウェイ
基本的なアンチスパム、アンチマルウェアの機能を提供

FortiMail Cloud：ゲートウェイプレミアム
上記「ゲートウェイ」に加えて、情報漏えい対策、ID ベース暗号化（IBE）、コンテンツ無害化、なりすまし分析、URL クリック保護、クラウドサンドボックスが利用可能

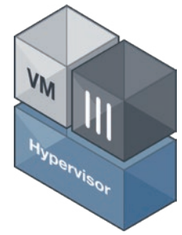
FortiMail Cloud：Microsoft 365 API サポート付ゲートウェイプレミアム
上記「ゲートウェイプレミアム」の機能を、Microsoft 365 のメールボックスに対して提供

FortiMail

FortiMail は、ボリュームベースで標的型サイバー攻撃を阻止する、トップクラスのセキュア E メールゲートウェイです。エンタープライズ環境の常に変化する攻撃対象を保護し、機密データの漏えいを食い止め、コンプライアンスの維持を支援します。高性能の物理アプライアンスと仮想アプライアンスをオンサイトまたはパブリッククラウドに導入することで、小規模企業からキャリア、サービスプロバイダー、大企業まで、あらゆる規模のユーザーに対応します。


FortiMail 900F


FortiMail 3000F



FortiMail VM

	FML-200F	FML-400F	FML-900F	FML-2000F	FML-3000F
メール転送能力 *（メッセージ / 毎時）	50,000	250,000	800,000	1,600,000	3,500,000
Enterprise ATP 利用時メール転送能力 *（メッセージ / 毎時）	30,000	150,000	400,000	800,000	2,100,000
最大管理ドメイン数	20	100	800	1,000	2,000
ストレージ容量（機種により増設可能）	1 x 1 TB	2 x 1 TB	2 x 2 TB（最大 8 TB）	2 x 2 TB（最大 12 TB）	2 x 2 TB（最大 20 TB）

*100KB のメッセージサイズ、キューイングなしの場合の数値。

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 1500G

FortiSandbox VM

	FortiSandbox 500G	FortiSandbox 1500G	FortiSandbox 3000F
VM 数	2 + 12 追加可能	2 + 26 追加可能	8 + 64 追加可能
サンドボックスのプリフィルター処理（ファイル数 / 時）※1	20,000	80,000	160,000
VM のサンドボックス処理（ファイル数 / 時）	500	1,000	1,600
実環境の処理効率（ファイル数 / 時）※2	10,000	32,000	68,000
スニファースループット	500 Mbps	4 Gbps	9.6 Gbps

* 数値はすべて「最大」の性能値であり、利用環境およびシステム構成に応じて異なります。
※1 FortiSandbox では、FortiGuard インテリジェンスを利用してプリフィルタリングを実行します。
※2 プリフィルターおよび動的分析が連続的に実行される場合は、実環境の Web および電子メールのトラフィックに基づいて算出されます。

FortiGate Cloud Sandbox

FortiGate Cloud で Sandbox 機能を提供します。AMP ライセンスを持つ FortiGate から検体をアップロードして利用できます。

FortiSandbox Cloud

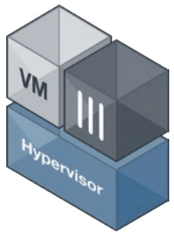
ハードウェアアプライアンスと同等の FortiSandbox を Fortinet がクラウドサービスとして提供します。必要な VM 数をサブスクリプションで利用できます。

FortiADC

FortiADC（アプリケーションデリバリコントローラ）は、エンタープライズにおけるアプリケーションデリバリの可用性、ユーザーエクスペリエンス、拡張性を最適化し、エンタープライズ環境のもっとも要件の厳しいアプリケーションにおいても、高速かつ安全でインテリジェントなアクセラレーションと負荷分散を可能にします。
エントリーレベルのハードウェアアプライアンスから最新のクラウド環境への導入が可能な高度な VM オプションまで、幅広い提供形態と製品ラインナップがあります。FortiADC VM は、VMware、Microsoft Hyper-V、Citrix XenServer、Open Source Xen、KVM、Oracle Cloud をサポートします。

FortiADC 300F

FortiADC 1200F



FortiADC VM

	FortiADC 120F	FortiADC 220F	FortiADC 300F	FortiADC 400F	FortiADC 1200F	FortiADC 2200F	FortiADC 4200F	FortiADC 5000F
L4/L7 スループット	3 Gbps / 2.2 Gbps	5 Gbps / 4 Gbps	8 Gbps	15 Gbps / 12 Gbps	40 Gbps / 30 Gbps	60 Gbps / 35 Gbps	100 Gbps / 80 Gbps	250 Gbps / 220 Gbps
L4 CPS	80,000	160,000	300,000	400,000	1,000,000	1,200,000	1,800,000	4 M
L4 HTTP RPS	230,000	500,000	1M	1.5 M	3 M	4 M	5 M	18 M
最大 L4 同時接続数	4.5 M	6 M	12 M	12 M	36 M	72 M	144 M	160 M
SSL バルク暗号化スループット	500 Mbps	1.2 Gbps	3 Gbps	6 Gbps	20 Gbps	25 Gbps	50 Gbps	120 Gbps
圧縮スループット	1.3 Gbps	2 Gbps	6 Gbps	10 Gbps	20 Gbps	22 Gbps	45 Gbps	150 Gbps
SSL アクセラレーションテクノロジー	ソフトウェア	ソフトウェア	ソフトウェア	ASIC	ASIC	ASIC	ASIC	ASIC
メモリ	8 GB	8 GB	16 GB	32 GB	32 GB	64 GB	128 GB	384 GB
仮想ドメイン（VDOM）	10	10	10	20	45	60	90	90
内蔵ストレージ	64 GB SSD	120 GB SSD	128 GB SSD	120 GB SSD	240 GB SSD	240 GB SSD	480 GB SSD	3.74 TB SSD
冗長電源	–	–	–	オプションで対応	○	○	○	○
形状	1 RU	1 RU	1 RU	1 RU	1 RU	1 RU	2 RU	2 RU

FortiGate Cloud

FortiGate Cloud は、フォーティネットのファイアウォールやアクセスポイント製品を網羅する幅広い管理機能とサービスを提供するクラウドベースの SaaS アプリケーションです。ゼロタッチ展開、構成の管理、レポートおよび分析、ゼロデイ攻撃の脅威保護を実現するサンドボックス、さらにビッグデータを分析してすでにクライアントデバイスに存在している脅威を特定する IOC（Indicators of Compromise：侵害指標）サービスを提供します。
FortiGate Cloud のアカウントを登録すると、FortiGate など各機器からログデータを自動的に転送し、FortiGate Cloud 上でログを保存、管理、解析します。

FortiEDR

FortiEDR は、マルウェアによる攻撃の侵入前からエンドポイントを保護し、データの侵害と不正使用をリアルタイムかつ自動的に阻止します。また、マルウェアが侵入した場合も継続して被害を抑えるための機能を提供します。コンテキストベースのインシデント対応プレイブックに基づいて、インシデントのタイプと攻撃対象ホストごとにインシデントの調査と対応をカスタマイズおよび自動化できるため、セキュリティ対応の最適化が可能になります。

脅威侵入前 / 侵入後、リアルタイムで脅威をブロックするソリューション

準備 → 検知 → 分析 → 封込 → 根絶 → 復旧

脆弱性管理　侵入前（EPP）　EPP

発見&予測

予防的なリスク低減

- 不正なデバイスと IoT の発見
- 脆弱性
- リスクベースのポリシーにより攻撃対象の低減
- 仮想パッチ

保護

実行前の保護

- カーネルレベル
- 機械学習とシグネチャレス
- アプリケーション通信制御

EDR　侵入後（EDR）

検知

リアルタイムな脅威検知

- アラート / 監視疲弊無し
- マルウェア分類の提供
- IOC の表示
- 完全な攻撃チェーンの提供

無効化

情報漏えい / 消失の阻止

- リアルタイムの感染後ブロッキング
- アウトバウンド通信のブロック
- 情報流出からの保護
- 情報の改ざんやランサムウェア暗号化の防止

対応と調査

攻撃の完全な可視化

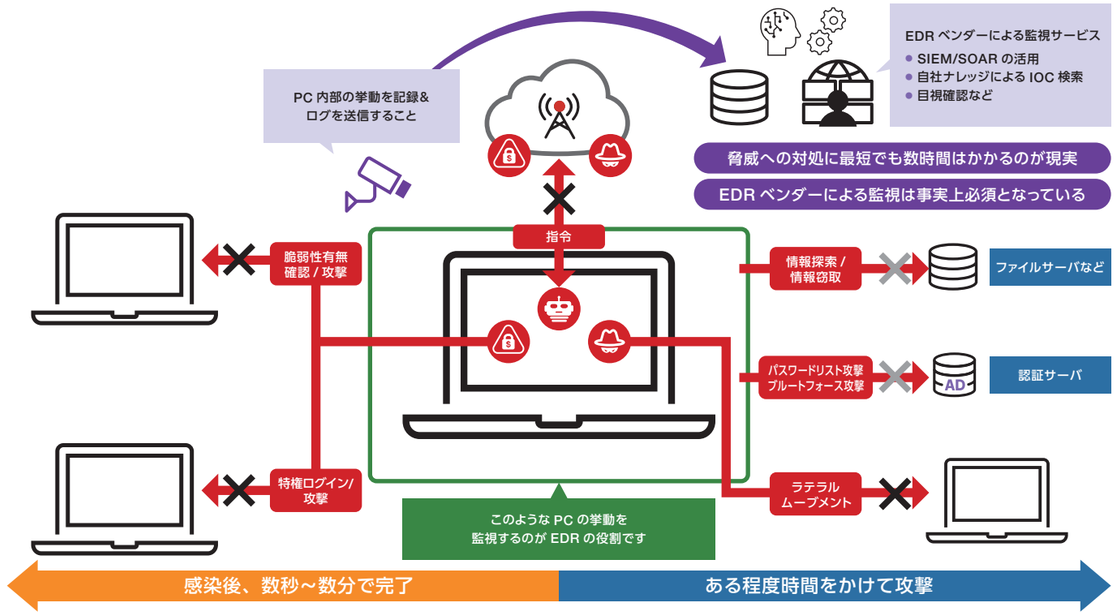
- カスタマイズ可能なインシデント対応プレイブック
- インシデント発生から認知までの時間の除去
- 柔軟な脅威ハンティングの実施

修復とロールバック

回復

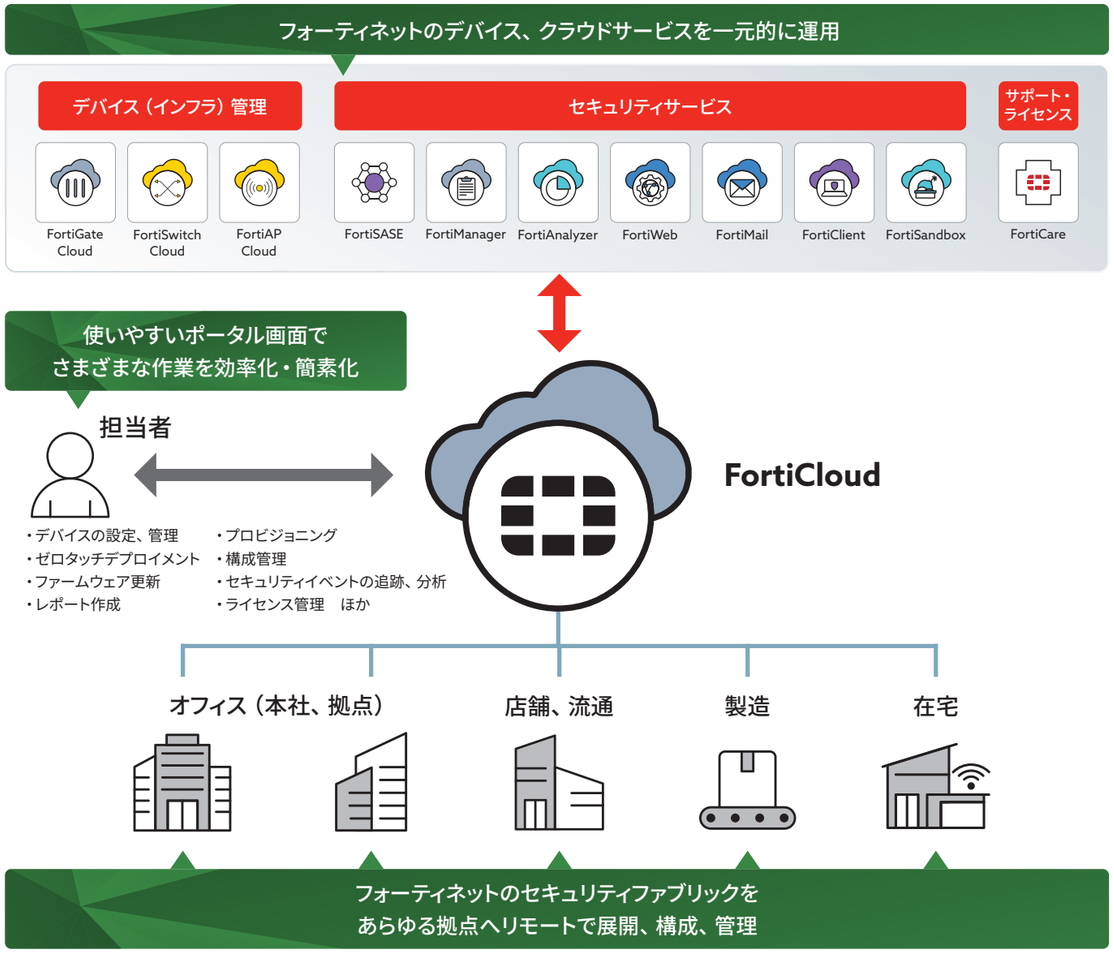
- 悪意のある変更からのロールバック
- 不正ファイルの削除
- 永続的なクリーンアップ
- 再イメージ / 再構築作業の排除
- 事業継続性の確保

EDR には「リアルタイムブロック」と「モニタリング」が求められる



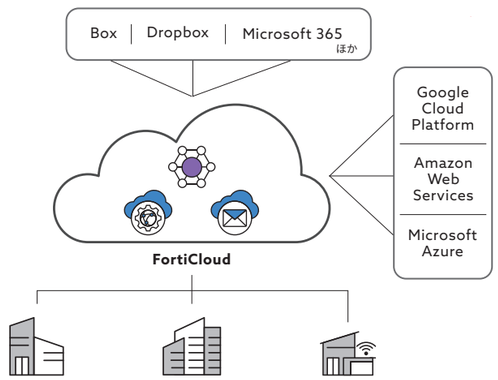
FortiCloud

FortiCloud は、フォーティネットの機器とセキュリティサービスの運用管理を集約し、業務の効率化や簡素化を促進するクラウドベースのセキュリティ・管理プラットフォームです。フォーティネットのセキュリティファブリックを構成するさまざまな機器とサービスを、オンプレミスかクラウドかを問わず、使いやすいポータル画面から一括して扱えます。また、FortiCare へのアクセスも統合されるので、ライセンス管理も可能です。



マルチクラウド環境の安全性を向上

FortiCloud 製品は、FortiMail や FortiWeb、FortiSASE などの多方面のセキュリティサービスを提供しています。フォーティネットのセキュリティファブリックをクラウド環境まで拡張し、緊密に連携・統合することによって、安全なネットワークとアプリケーション利用を実現します。
Microsoft 365 や Salesforce などクラウドで提供されているアプリケーションや外部サービスを安全に利用するための環境整備にも役立ちます。



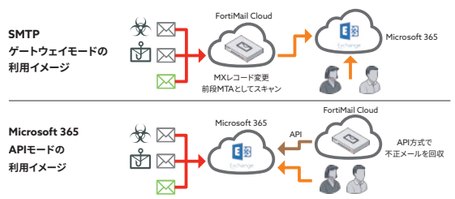
セキュリティファブリックを支える各機能をクラウドで管理

FortiManager Cloud

複数の FortiGate の一元管理が可能で、SD-WAN オーケストレーター機能を備えています。テンプレートやウィザードにより管理者の作業を大幅に軽減し、仮想管理機能（ADOM）によって MSSP 事業者などでは管理機能をユーザーに提供できます。

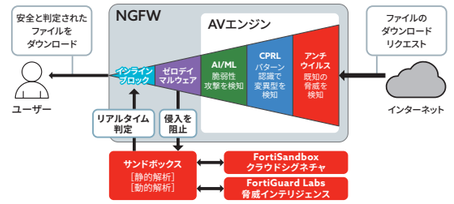
FortiAnalyzer Cloud

オーケストレーション、オートメーション、レスポンスの一元化によって、組織全体のセキュリティを強化します。攻撃対象領域の拡大につながる新しいテクノロジーの分析や監視の複雑さを軽減し、エンドツーエンドの可視性によって脅威の特定と排除を容易にします。



FortiMail Cloud

E メール経由のサイバー攻撃を阻止するセキュア E メールゲートウェイです。フィッシング、ランサムウェア、ゼロデイ脅威、なりすまし、ビジネスメール侵害（BEC）攻撃などの脅威に対する防御、検知、対策を提供。小規模企業からキャリア、サービスプロバイダー、大企業まで、あらゆる規模のユーザーに対応します。

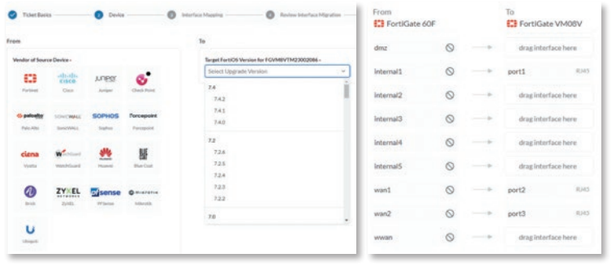


FortiSandbox Cloud

プロアクティブな脅威検出と対策機能を提供し、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します。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。

FortiConverter Service

FortiConverter Service は、他ベンダーの機器や FortiGate の他モデル / 他バージョンから、お客様が運用する FortiGate のモデル / バージョンへ設定を変換するサービスです。クラウドポータルから既存のファイアウォール構成をアップロードし、変換された結果をダウンロードするだけで移行が完了します。



Inline SandBox（インラインマルウェア防止サービス）

FortiGuard AI ベースのインラインマルウェア防止サービスは、FortiGate NGFW 向けの追加サービスです。ダウンロードされたファイルを一度止めた状態で、検体に対する静的 / 動的分析、ヒューリスティック分析、行動分析を行い、AI/ 機械学習を使用して不明の脅威やゼロデイ攻撃から組織を秒単位で保護します。

※ エンタープライズバンドルには含まれています。