

# FortiGate / FortiWiFi 40F シリーズ

FortiGate 40F、40F-3G4G、FortiWiFi 40F、40F-3G4G



## ハイライト

**Gartner® Magic Quadrant:** ネットワーク・ファイアウォールと SD-WAN の両部門で、リーダーの 1 社に位置付け

**セキュリティドリブン ネットワーキング:** FortiOS による ネットワーキングとセキュリティのコンバージェンスにより実現

**比類ないパフォーマンス:** フォーティネットの特許取得済み SoC プロセッサにより実現

**エンタープライズセキュリティ:** AI / ML を活用した統合 FortiGuard サービスにより実現

**運用の簡素化:** ネットワーキングとセキュリティの一元管理、自動化、詳細分析、自己修復により実現

## 次世代ファイアウォールと SD-WAN のコンバージェンス

FortiGate FortiWiFi 40F シリーズは、ファイアウォール、SD-WAN、セキュリティが 1 つに統合された、分散する企業拠点におけるセキュリティ ドリブン ネットワークの構築やあらゆる規模の WAN アーキテクチャのトランスフォーメーションに最適なアプライアンスです。

FortiOS オペレーティングシステムを搭載する FortiGate FortiWiFi 40F シリーズは、ネットワーキングとセキュリティのコンバージェンスを業界で初めて実現しました。このコンバージェンスにより、今日の動的なデジタルインフラストラクチャの効率的な保護が可能になります。

フォーティネット セキュリティ ファブリック プラットフォームの中核である FortiGate 次世代ファイアウォール (NGFW) は、FortiGuard AI 活用セキュリティサービスとのシームレスな連携により、リアルタイムかつ協調型で自動化されたエンドツーエンドの脅威保護をあらゆるユースケースに提供します。

FortiGate FortiWiFi 40F シリーズは、特許取得済みの SD-WAN ベースの ASIC を採用して構築されており、従来の CPU を圧倒する比類なきパフォーマンスを、コストと消費電力を低減しつつ実現します。専用設計と内蔵マルチコアプロセッサにより、ネットワーキングとセキュリティ機能のコンバージェンスがさらに加速し、支社 / 拠点における安全な接続とユーザーエクスペリエンスが最適化されます。

IPS	NGFW	脅威保護	インタフェース
1 Gbps	800 Mbps	600 Mbps	複数の GbE RJ45   WiFi モデル

Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hills, Tom Lintemuth, 19 December 2022.  
 Gartner, Magic Quadrant for SD-WAN, Jonathan Forest, Naresh Singh, Andrew Lerner, Karen Brown, 27 September 2023.  
 Gartnerは、Gartnerリサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高のレーティング又はその他の評価を得たベンダーのみを選択するようにテクノロジーユーザーに勧告するものではありません。Gartnerリサーチの発行物は、Gartnerリサーチの見解を表したものであり、事実を表現したものではありません。Gartnerは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の責任を負うものではありません。GARTNERおよびMagic Quadrantは、Gartner Inc.または関連会社の米国およびその他の国における登録商標およびサービスマークであり、同社の許可に基づいて使用されています。All rights reserved.



提供形態



アプライアンス



仮想マシン



ホスティング



クラウド



コンテナ

## 場所を問わず動作する FortiOS

### FortiOS：フォーティネットの高度なオペレーティングシステム

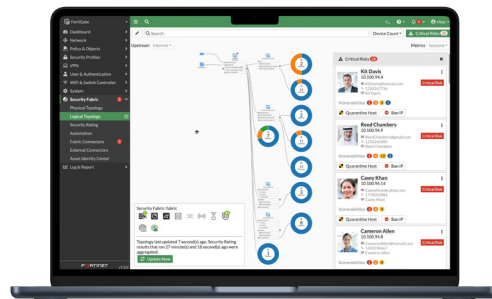
FortiOS は、フォーティネット セキュリティ ファブリックにおけるハイパフォーマンスのネットワークとセキュリティのコンバージェンスを可能にします。あらゆる場所に導入できるため、ネットワーク、エンドポイント、マルチクラウドのいずれの環境でも一貫性あるコンテキストウェアなセキュリティポスチャーが実現します。

FortiOS は、物理デバイス、仮想デバイス、コンテナ、またはクラウドサービスのあらゆる FortiGate の導入環境に対応します。このユニバーサル導入モデルにより、多数のテクノロジーやユースケースが、有機的に構築されたトップクラスの機能、統一されたオペレーティングシステム、圧倒的なスケーラビリティに統合されます。このソリューションを導入することで、パフォーマンスや保護を低下させることなく、あらゆるエッジの保護、運用の簡素化、ビジネスの遂行が可能になります。

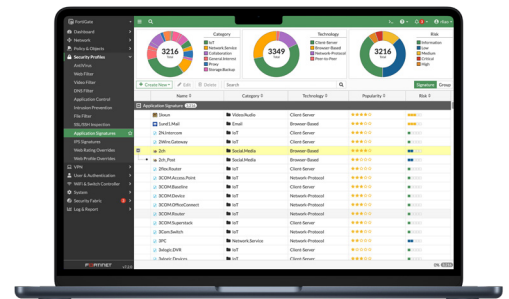
FortiOS は、AI / ML を活用した高度なサービス、インラインの高度なサンドボックス検知、統合 ZTNA の適用など、フォーティネット セキュリティ ファブリックの能力の飛躍的な拡大を可能にし、ハードウェア、ソフトウェア、そして SASE による SaaS (Software-as-a-Service) といったハイブリッド導入環境モデルでの保護を実現します。

FortiOS では、可視性と制御を拡張し、セキュリティポリシーの一貫した展開と適用を確実に実現し、大規模ネットワークでの一元管理を可能にする、以下の機能を提供します。

- ドリルダウンとトポロジのインタラクティブビューアで、リアルタイムにステータスを表示
- ワンクリックで改善を実行する機能により、脅威と悪用からの保護を正確かつ迅速に実現
- 独自の脅威スコアシステムで重み付けされた脅威をユーザーに相関させ、調査を優先付け



直感的で使いやすいビューにより、  
ネットワークやエンドポイントの脆弱性を表示



FortiOS アプリケーションシグネチャによる  
可視化

### FortiConverter サービス

FortiConverter サービスは、従来型のさまざまなファイアウォールから FortiGate 次世代ファイアウォールへの迅速かつ容易な移行を支援します。このサービスは、高度な方法論と自動化されたプロセスによるベストプラクティスの採用により、エラーや冗長性を排除します。最新の FortiOS テクノロジーに移行することで、企業はネットワーク保護を加速させることができます。



## FortiGuard サービス

### ネットワーク / ファイルセキュリティ

ネットワークベースやファイルベースの脅威からの保護を提供します。このサービスを構成する侵入防止システム (IPS) は、AI / ML モデルを使用してディープパケット / SSL インスペクションを実行することで、不正コンテンツを検知してブロックし、新たな脆弱性が見つかった場合は仮想パッチを適用します。アンチマルウェアサービスも提供することで、既知および未知のファイルベースの脅威からの保護を可能にします。アンチマルウェアサービスは、アンチウイルスとファイルサンドボックスの両方による多層型保護を提供し、FortiGuard Labs の脅威インテリジェンスによってリアルタイムでサービスが強化されます。アプリケーション制御は、セキュリティコンプライアンスを強化し、リアルタイムのアプリケーション可視性を提供します。

### Web / DNS セキュリティ

DNS ベースの脅威、不正 URL (E メールも含む)、ボットネット / コマンド & コントロール通信などの Web ベースの脅威からの保護を提供します。DNS フィルタリングは、DNS トラフィックを完全に可視化しつつ、高リスクのドメインをブロックし、DNS トンネリング、DNS 侵入、C2 サーバー、ドメイン生成アルゴリズム (DGA) からの保護を可能にします。URL フィルタリングは、3 億以上の URL のデータベースを活用して、不正サイトやペイロードへのリンクを特定し、ブロックします。IP レピュテーションサービスとアンチボットネットサービスは、ボットネット通信を防止し、既知のソースからの DDoS 攻撃をブロックします。

### SaaS / データセキュリティ

FortiGuard サービスは、アプリケーションの利用やデータセキュリティ全般の多くのセキュリティのケースに対応します。ネットワーク DLP (データ漏洩防止) 機能が構成されているため、ネットワークを移動するデータの可視性、管理、保護 (データの持ち出しのブロックを含む) が保証され、コンプライアンスとプライバシーの実装も簡素化されます。さらには、フォーティネットのインライン CASB (クラウドアクセスセキュリティブローカー) サービスを利用することで、管理者が特定の SaaS アプリケーションのユーザーアクティビティに適切なポリシーアクションを適用したり、特定のドメインに属するユーザーだけに特定のアプリケーションへのアクセスを許可したりすることもできます。インフラストラクチャを継続的に評価し、構成が効果的かつ安全に動作していることを検証し、業務に影響する可能性のあるリスクや脆弱性を知らせる、攻撃対象領域管理も含まれています。IoT デバイスもサービスの対象に含まれているため、IoT 検知と IoT 脆弱性関連の両方が可能になります。

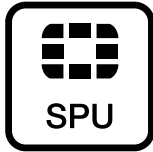
### ゼロデイ脅威保護

ゼロデイ脅威保護は、フォーティネットの AI ベースのインラインマルウェア保護が組み込まれた、最も高度なサンドボックスサービスです。未知のファイルをリアルタイムで分析してブロックすることで、ゼロデイ脅威と高度な脅威からの 1 秒以下の保護をすべての NGFW で実現します。このサービスは、MITRE ATT&CK® マトリクスの内蔵により、迅速な調査を可能にします。このサービスが目指しているのは、未知の脅威をブロックしつつ、インシデントレスポンスの作業を合理化し、セキュリティオーバーヘッドを軽減し、包括的な防御を実現することです。

### OT セキュリティ

OT 検知、OT 脆弱性の相関付け、仮想パッチ、OT シグネチャ、業界に特化したプロトコルデコーダを提供し、OT 環境とデバイスの包括的で堅牢な防御を可能にします。

## あらゆるエッジに対して規模を問わず保護



### SPU (セキュリティプロセッシングユニット) を搭載

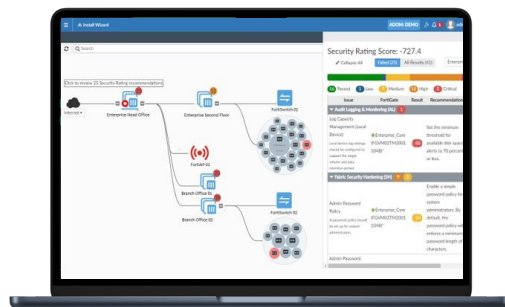
従来型のファイアウォールは、市販のハードウェアや汎用 CPU に依存しているため、危険なパフォーマンスギャップが発生し、今日のコンテンツベース / 接続ベースの脅威から企業を保護することはできません。フォーティネット独自の SPU プロセッサは、最大 520 Gbps の処理能力を提供することで、新たな脅威の検知と不正コンテンツのブロックを可能にしつつ、ネットワークセキュリティソリューションがパフォーマンスボトルネックにならないようにします。

### ASIC の優位性



### セキュア SD-WAN ASIC SOC4

- RISC アーキテクチャのシステム CPU とフォーティネット独自の SPU (Security Processing Unit) であるコンテンツ / ネットワークプロセッサを統合し、比類ないパフォーマンスを実現
- 業界最速のアプリケーションの識別とステアリングによって業務効率を向上
- IPsec VPN の高速化により、インターネットへの直接アクセスにおいてトップクラスのユーザーエクスペリエンスを提供
- クラス最高レベルの NGFW セキュリティと詳細で高パフォーマンスの SSL インспекションの理想的な組み合わせを実現
- セキュリティをアクセスレイヤーまで拡張するとともに、スイッチとアクセスポイントの接続の統合と高速化によって SD ブランチ実現に向けたトランスフォーメーションを可能に



FortiManager によるネットワークセキュリティ態勢の直感的なビューと、明確で実用的なインテリジェンス

### ネットワークとセキュリティのスケラブルで一元的な管理

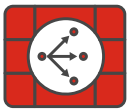
フォーティネットの一元管理ソリューションである FortiManager は、FortiGate、FortiSwitch、FortiAP などのデバイスを含むフォーティネット セキュリティ ファブリックの統合管理を可能にします。多様な環境のネットワークとセキュリティの機能の監視を簡素化し、自動化することで、ハイブリッドメッシュファイアウォールの導入にあたっての基本コンポーネントとしての役割を果たします。

## ユースケース



### 境界保護

- 送受信トラフィックを定義済みセキュリティポリシーに基づいてインスペクションして制御
- FortiGuard AI 活用セキュリティサービスと NGFW のネイティブ統合により、Web、コンテンツ、デバイスをプロアクティブに保護し、ランサムウェアや高度なサイバー攻撃からネットワークを保護
- リアルタイム SSL インスペクション (TLS 1.3 を含む) が、攻撃対象領域のユーザー、デバイス、アプリケーションの完全な可視性を実現
- フォーティネットの特許取得済み SPU (セキュリティプロセッシングユニット) と、セキュリティおよびネットワークテクノロジーのコンバージェンスにより、優れたパフォーマンス、保護、エネルギー効率を提供



### セキュア SD-WAN

- FortiGate は、SD-WAN、WAN 最適化、セキュリティの統合と単一の FortiOS オペレーティングシステムからの統一された管理を可能にすることで、トップクラスの WAN エッジを実現
- 特許取得済みの SD-WAN ベースの ASIC を採用して構築された FortiGate は、アプリケーションを高速で識別することで、アプリケーションアクセスでの遅延を回避し、あらゆる拠点のオーバーレイパフォーマンスを高速化
- クラウドから提供される SD-WAN とセキュリティサービスエッジ (SSE) が統合された包括的な SASE ソリューションにより、場所に縛られない働き方を強力に支援
- 自動化、詳細分析、自己修復により、あらゆる規模の運用を効率化

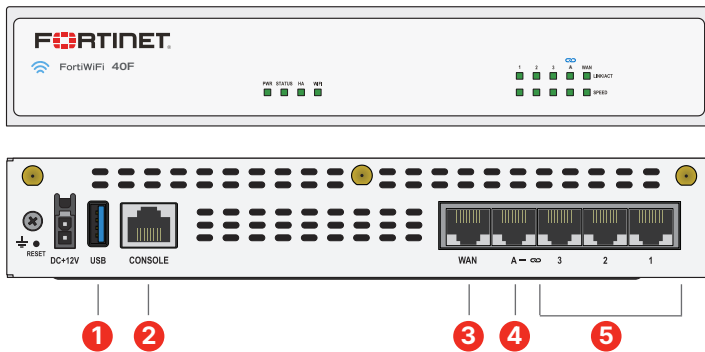


### 支社 / 拠点の保護

- フォーティネット セキュリティ ファブリックの単一プラットフォームにより、FortiGate NGFW が IoT デバイスを自動的に検出して保護できるため、拠点への迅速な導入を実現
- FortiGate は、FortiSwitch の Ethernet スイッチや FortiAP のアクセスポイントとの完全統合により、拠点の WAN、LAN、WLAN へのセキュリティの容易な拡張を可能にすることで、統一された保護と信頼性の高い接続を実現
- FortiGate とフォーティネット製品は、FortiManager とのシームレスな連携により、一元化された可視性を IT チームに提供し、拠点の管理を簡素化
- FortiGate の HA サポートにより、継続的なネットワーク保護が保証され、ハードウェア障害やネットワーク中断の発生時のダウンタイムが最小化

## ハードウェア

### FortiGate / FortiWiFi 40F シリーズ



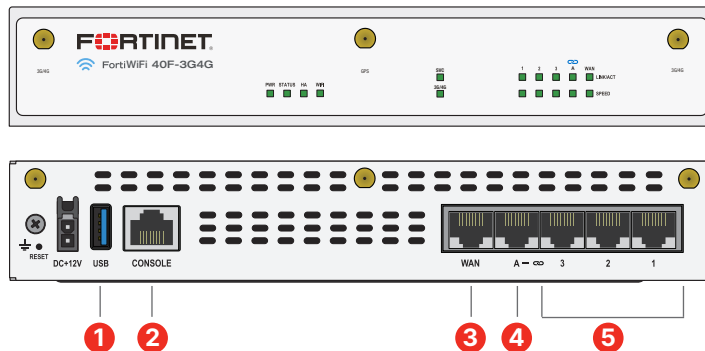
### インタフェース

1. 1 × USB ポート
2. 1 × 管理コンソールポート
3. 1 × GbE RJ45 WAN ポート
4. 1 × GbE RJ45 FortiLink ポート
5. 3 × GbE RJ45 Ethernet ポート

### ハードウェアの特長



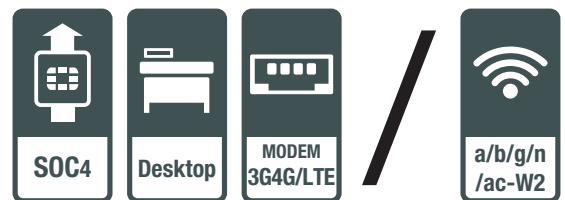
### FortiGate / FortiWiFi 40F-3G4G



### インタフェース

1. 1 × USB ポート
2. 1 × 管理コンソールポート
3. 1 × GbE RJ45 WAN ポート
4. 1 × GbE RJ45 FortiLink ポート
5. 3 × GbE RJ45 Ethernet ポート

### ハードウェアの特長



### コンパクトで信頼性の高いフォームファクター

小規模環境に理想的なコンパクトなデザインのフォームファクターは、デスクトップでの設置や壁掛けにも容易に対応可能です。小型軽量化されたデザインでありながら、高い信頼性の証である優れた平均故障間隔（MTBF）を実現しており、ネットワーク障害の発生を最小限に抑えることができます。

### アクセスレイヤーセキュリティ

FortiLink プロトコルにより、FortiSwitch を NGFW の論理拡張として FortiGate に統合し、セキュリティとネットワークアクセスの垂直統合を実現します。FortiLink が有効なこれらのインタフェースは、必要に応じて通常のポートとして再構成することが可能です。

## 技術仕様

	FortiGate 40F	FortiWiFi 40F	FortiGate 40F-3G4G	FortiWiFi 40F-3G4G
インタフェースとモジュール				
ハードウェアアクセラレーション対応 GbE RJ45 WAN / DMZ ポート	1	1	1	1
ハードウェアアクセラレーション対応 GbE RJ45 内蔵ポート	3	3	3	3
ハードウェアアクセラレーション対応 GbE RJ45 FortiLink ポート (デフォルト)	1	1	1	1
ハードウェアアクセラレーション対応 GbE RJ45 PoE / + ポート	—	—	—	—
セルラーモデム	—	—	3G4G LTE	3G4G LTE
無線インタフェース	—	シングルラジオ (2.4 GHz / 5 GHz)、802.11/a/b/g/n/ac-W2	—	シングルラジオ (2.4 GHz / 5 GHz)、802.11/a/b/g/n/ac-W2
アンテナポート (SMA)	—	3	3	6
USB ポート	1	1	1	1
RJ45 シリアル管理コンソールポート	1	1	1	1
SIM スロット (Nano SIM)	—	—	2	2
オンボードストレージ	—	—	—	—
付属トランシーバ	非同梱	非同梱	非同梱	非同梱
システム性能 — エンタープライズトラフィック混合				
IPS スループット <sup>2</sup>			1 Gbps	
NGFW スループット <sup>2, 4</sup>			800 Mbps	
脅威保護スループット <sup>2, 5</sup>			600 Mbps	
システム性能				
IPv4 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	
ファイアウォールレイテンシ (64 バイト UDP パケット)			2.97 $\mu$ s	
ファイアウォールスループット (パケット / 秒)			7.5 Mpps	
ファイアウォール同時セッション (TCP)			700,000	
ファイアウォール新規セッション / 秒 (TCP)			35,000	
ファイアウォールポリシー			5,000	
IPSec VPN スループット (512 バイト) <sup>1</sup>			4.4 Gbps	
ゲートウェイ間 IPSec VPN トンネル			200	
クライアント - ゲートウェイ間 IPSec VPN トンネル			250	
SSL-VPN スループット			490 Mbps	
同時 SSL-VPN ユーザー (推奨最大値、トンネルモード)			200	
SSL インスペクションスループット (IPS、avg. HTTPS) <sup>3</sup>			310 Mbps	
SSL インスペクション CPS (IPS、avg. HTTPS) <sup>3</sup>			320	
SSL インスペクション同時セッション (IPS、avg. HTTPS) <sup>3</sup>			55,000	
アプリケーション制御スループット (HTTP 64 K) <sup>2</sup>			990 Mbps	
CAPWAP スループット (HTTP 64K)			3.5 Gbps	
仮想 UTM (VDM: 標準 / 最大)			10 / 10	
FortiSwitch サポート数			8	
FortiAP サポート数 (合計 / トンネルモード)			16 / 8	
FortiToken サポート数			500	
高可用性 (HA)	アクティブ / アクティブ、アクティブ / パッシブ、クラスタリング			

注：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。

<sup>1</sup> 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。

<sup>2</sup> IPS (エンタープライズトラフィック混合)、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。

<sup>3</sup> 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。

<sup>4</sup> 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。

<sup>5</sup> 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。





## 技術仕様

	FortiGate 40F	FortiWiFi 40F	FortiGate 40F-3G4G	FortiWiFi 40F-3G4G
<b>サイズ / 電源</b>				
高さ × 幅 × 奥行	38.5 × 216 × 160 mm		40.5 × 216 × 160 mm	
重量	1 kg		1 kg	
形状 (EIA 規格およびその他の 19 インチラック適合)	デスクトップ		デスクトップ	
定格入力	12 Vdc, 3 A		12 Vdc, 3 A	
電源	100 ~ 240 V AC, 50 ~ 60 Hz (外部 DC 電源)		100 ~ 240 V AC, 50 ~ 60 Hz (外部 DC 電源)	
最大電流	100 V AC / 0.2 A, 240 V AC / 0.1 A		100 V AC / 0.3 A, 240 V AC / 0.2 A	
消費電力 (平均 / 最大)	7.74 W / 9.46 W	14.6 W / 16.6 W	15.8 W / 18.6 W	18.6 W / 19.8 W
放熱	52.55 BTU/h	56.64 BTU/h	63.5 BTU/h	67.6 BTU/h
<b>動作環境 / 準拠規格・認定</b>				
動作温度	0 ~ 40 °C			
保管温度	-35 ~ 70 °C			
湿度	10 ~ 90% (結露しないこと)			
騒音レベル	0 dBA (ファンレス)			
動作高度	最高 2,250 m			
準拠規格・認定	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
認定	USGv6 / IPv6			
<b>ラジオ仕様</b>				
マルチユーザ MIMO (MU-MIMO)	—	3 × 3	—	3 × 3
最大 Wi-Fi 速度	—	5 GHz の場合 1,300 Mbps, 2.4 GHz の場合 450 Mbps	—	5 GHz の場合 1,300 Mbps, 2.4 GHz の場合 450 Mbps
最大送信電力	—	20 dBm	—	20 dBm
アンテナゲイン	—	5 GHz の場合 3.5 dBi, 2.4 GHz の場合 5 dBi	—	5 GHz の場合 3.5 dBi, 2.4 GHz の場合 5 dBi
<b>3G4G モデム</b>				
最大送信電力	—		—	20 dBm
地域	—		—	全地域対応
モデムモデル	—		—	Sierra Wireless EM7565 (2 SIM スロット、アクティブ / パッシブ)
LTE カテゴリー	—		—	CAT-12
LTE バンド	—		—	B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B18, B19, B20, B26, B28, B29, B30, B32, B41, B42, B43, B46, B48, B66
UMTS / HSPA+	—		—	B1, B2, B4, B5, B6, B8, B9, B19
WCDMA	—		—	—
CDMA 1xRTT / EV-DO Rev A	—		—	—
GSM / GPRS / EDGE	—		—	—
モジュール認証	—		—	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
ダイバーシティ	—		—	○
MIMO	—		—	○
GNSS バイアス	—		—	○



## サブスクリプション

サービスカテゴリ	提供サービス	アラカルト	バンドル		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard セキュリティサービス	IPS — IPS、Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP) — AV、Botnet Domains、Mobile Malware、Virus Outbreak Protection、Content Disarm and Reconstruct <sup>3</sup> 、AI-based Heuristic AV、FortiGate Cloud Sandbox	•	•	•	•
	URL、DNS and Video Filtering — URL、DNS and Video <sup>3</sup> Filtering、Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention <sup>3</sup>	•	•		
	Data Loss Prevention (DLP) <sup>1</sup>	•	•		
	Attack Surface Security — IoT Device Detection、IoT Vulnerability Correlation and Virtual Patching、Security Rating、Outbreak Check	•	•		
	OT Security — OT Device Detection、OT vulnerability correlation and Virtual Patching、OT Application Control and IPS <sup>1</sup>	•			
	Application Control		FortiCare サブスクリプションに含まれています。		
Inline CASB <sup>3</sup>		FortiCare サブスクリプションに含まれています。			
SD-WAN / SASE サービス	SD-WAN Underlay Bandwidth and Quality Monitoring	•			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth) <sup>2</sup>	•			
NOC / SOC サービス	FortiConverter Service for one time configuration conversion	•	•		
	Managed FortiGate Service — available 24×7、with Fortinet NOC experts performing device setup、network、and policy change management	•			
	FortiGate Cloud — Management、Analysis、One Year Log Retention	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
ハードウェア / ソフトウェアサポート	FortiGuard SOCaas — 24×7 cloud-based managed log monitoring、incident triage、SOC escalation service	•			
	FortiCare Essentials <sup>2</sup>	•			
	FortiCare Premium	•	•	•	•
FortiCare Elite	FortiCare Elite	•			
	Device/OS Detection、GeoIPs、Trusted CA Certificates、Internet Services and Botnet IPs、DDNS (v4/v6)、Local Protection、PSIRT Check、Anti-Phishing		FortiCare サブスクリプションに含まれています。		

1. FortiOS 7.4.1を実行している場合に利用可能

2. デスクトップモデルのみ

3. FortiOS 7.4.4以降の場合、FortiGate / FortiWiFi 40F、60E、60F、80E、90Eシリーズでは利用不能



### FortiGuard バンドル

FortiGuard Labs は、FortiGate ファイアウォールプラットフォームと併せてご利用いただける、多数のセキュリティインテリジェンスサービスを提供しています。最適な Protection をお選びいただくことで、FortiGate の保護機能を容易に最適化できます。



### FortiCare サービス

フォーティネットは、FortiCare サービスを通じて、フォーティネット セキュリティ ファブリック ソリューションの最適化を支援します。フォーティネットの包括的なライフサイクルサポートは、設計、導入、運用、最適化、進化を支援するサービスを提供します。その1つである FortiCare Elite サービスは、SLA(サービスレベルアグリーメント)の強化と、専任のサポートチームによる迅速な問題解決を提供します。このアドバンスドサポートオプションには、18 ヶ月の EoE (Extended End-of-Engineering-Support) が含まれているため、柔軟な対応が可能になります。直感的な FortiCare Elite ポータルにアクセスして、統一されたビューでデバイスやセキュリティの状態を理解することで、運用効率を合理化し、フォーティネットの導入環境のパフォーマンスを最大限に向上させることができます。



## オーダー情報

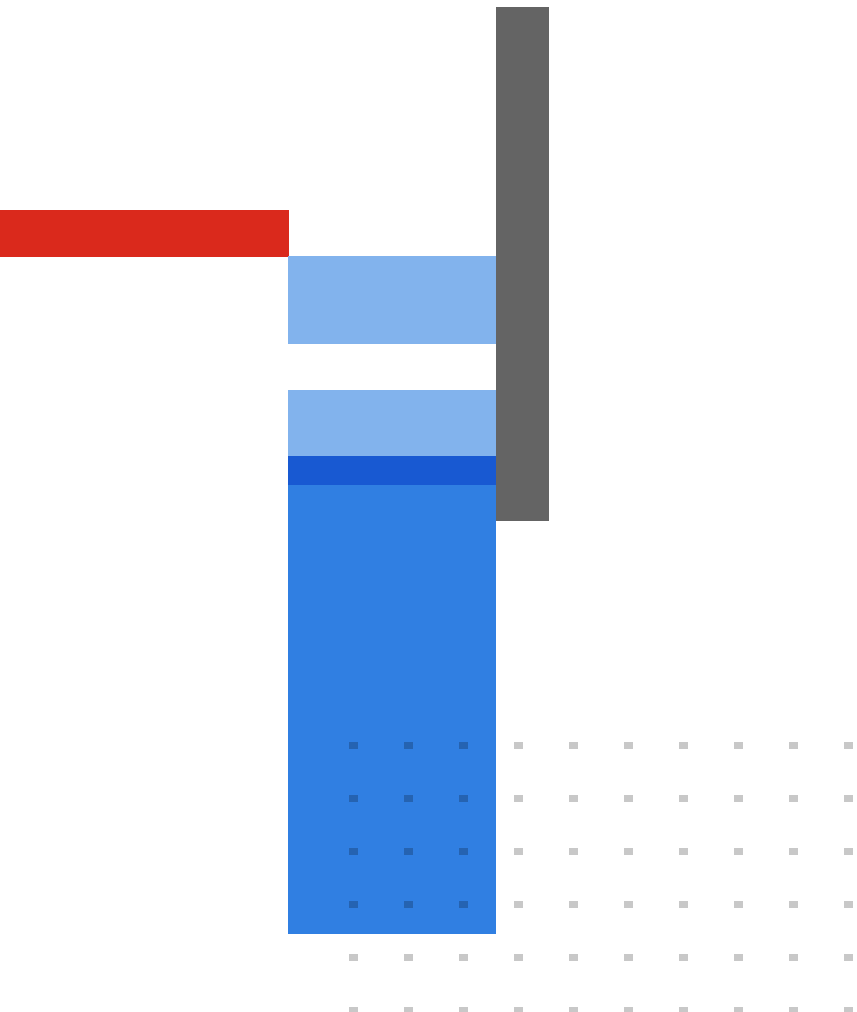
Product	SKU	Description
<b>FortiGate 40F</b>	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports).
<b>FortiWiFi 40F</b>	FWF-40F-[RC]	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2).
<b>FortiGate 40F-3G4G</b>	FG-40F-3G4G	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, external SMA WWAN antennas included.
<b>FortiWiFi 40F-3G4G</b>	FWF-40F-3G4G-[RC]	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, Wireless (802.11a/b/g/n/ac-W2), external SMA WWAN and wireless antennas included.
Optional Accessories		
<b>Rack Mount Tray</b>	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
<b>AC Power Adaptor</b>	SP-FG-40F-PA-10(-XX)	Pack of 10 AC power adaptors for FG/FWF-40F, come with interchangeable power plugs. (XX=various countries code).
<b>Wall Mount Kits</b>	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass.

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y



## フォーティネット CSR ポリシー

フォーティネットは、サイバーセキュリティを通じてあらゆるお客様の進歩と持続可能性を推進し、人権を尊重する倫理的な方法でビジネスを遂行し、常に信頼できるデジタル世界を実現することをお約束します。お客様には、フォーティネットの製品およびサービスを使用して、違法な検閲、監視、拘留、または過剰な武力行使などの人権の侵害または乱用に関与したり、何らかの形で支援したりしないことをフォーティネットに表明し、保証していただくこととなります。フォーティネット製品の利用にあたっては、[フォーティネットの EULA](#)（エンドユーザー使用許諾契約）を遵守し、EULA に違反すると疑われる場合は、[フォーティネット不正告発規定](#)に概要が記載されている手順で報告する必要があります。



**FORTINET**

フォーティネットジャパン合同会社

〒106-0032

東京都港区六本木 7-7-7 Tri-Seven Roppongi 9 階

[www.fortinet.com/jp/contact](http://www.fortinet.com/jp/contact)

お問い合わせ