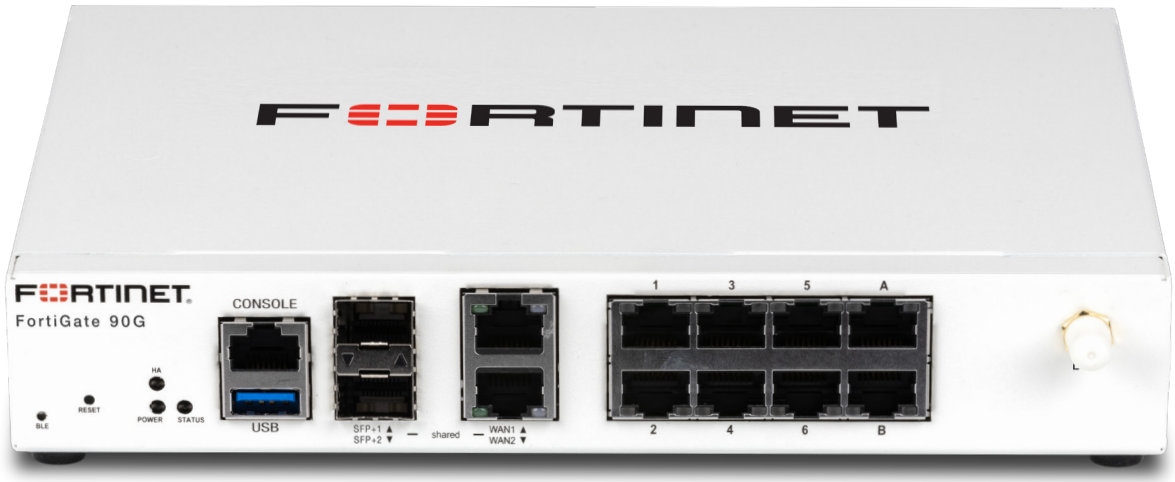
FortiGate 90G シリーズ

FortiGate 90G、FortiGate 91G



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

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 ASIC と FortiOS オペレーティングシステムにより実現

エンタープライズクラスの保護：FortiGuard AI 活用セキュリティ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、ワークフローの自動化、詳細分析、自己修復により実現

SD-WAN と無線コントローラ：すべての FortiGate アプライアンスに追加費用なしで搭載

豊富なポートフォリオ：あらゆるビジネスの予算とニーズに対応

次世代ファイアウォールと SD-WAN のコンバージェンス

FortiGate 90G シリーズは、ファイアウォール、SD-WAN、セキュリティが 1 つのアプライアンスに統合された、分散する企業拠点におけるセキュア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ソリューションです。

FortiOS オペレーティングシステムを搭載する FortiGate 90G 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かつ最適な保護が可能になります。

FortiGate NGFW は、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基盤として、FortiGuard AI 活用セキュリティサービスとシームレスに連携し、協調型で自動化されたエンドツーエンドの脅威防御をリアルタイムで実現します。

FortiGate 90G シリーズは、特許取得済み SD-WAN ベースの ASIC の搭載により、従来の CPU を凌駕する比類ないパフォーマンスを低コストかつ低消費電力で実現します。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が最適化され、堅牢なユーザーエクスペリエンスが実現します。

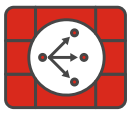
IPS	NGFW	脅威保護	インタフェース
4.5 Gbps	2.5 Gbps	2.2 Gbps	複数の GbE RJ45、10 GbE RJ45、SFP+ 共有メディアポート | 内蔵ストレージモデル

Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hils, Tom Lintemuth, 19 December 2022.
Gartner, Magic Quadrant for SD-WAN, Jonathan Forest, Karen Brown, Nauman Raja, 30 September 2024.

ユースケース

境界保護

- FortiGuard AI 活用セキュリティサービスのネイティブ統合により、不正トラフィックからネットワークを保護し、ファイルベースの脅威からの保護、Web ベースの攻撃のブロック、アプリケーションとデータの保護を支援
- 定義されたセキュリティポリシーに基づき、送受信トラフィックをインスペクションして制御
- リアルタイム SSL インスペクション（TLS 1.3 を含む）を実行し、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 と、セキュリティおよびネットワーキング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 の最適化、セキュリティ、統合管理を単一の FortiOS オペレーティングシステムで統合することで、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 を搭載する FortiGate で高速のアプリケーションの識別を可能にすることで、アプリケーションアクセスの遅延を回避し、あらゆる場所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）を統合することで、包括的な SASE ソリューションでハイブリッドワークを強力に支援
- 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 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 やフォーティネット製品と FortiManager のシームレスな連携により、IT チームの可視性が一元化され、拠点における管理を簡素化
- FortiGate HA サポートにより、継続的なネットワーク保護を可能にし、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を最小化

ユニバーサル ZTNA

あらゆる場所のユーザーによるあらゆる場所でホスティングされるアプリケーションへのアクセスを制御することで、アクセスポリシーの統一された適用を実現します。

- アプリケーションへのアクセスを許可する前に、広範な認証、チェック、ポリシーの適用を常に実行
- FortiClient によるエージェントベースのアクセス、またはゲストや BYOD 向けのプロキシポータル経由のエージェントレスアクセスが可能

FortiGuard AI 活用セキュリティサービス

FortiGuard AI 活用セキュリティサービスは、フォーティネットの多層型防御の一部として、FortiGate NGFW やその他の製品に密接に統合されています。FortiGuard Labs の最新の脅威インテリジェンスを活用するこれらのサービスは、ゼロデイ攻撃や AI を活用する高度な攻撃などの最新の攻撃ベクトルや脅威から組織を保護します。

ネットワーク / ファイルセキュリティ

ネットワーク / ファイルセキュリティサービスは、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。フォーティネットの業界をリードする侵入防止システム（IPS）は、18,000 以上のシグネチャと AI / ML モデルのディープパケット / SSL インスペクションを使用することで、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。アンチマルウェアは、既知および未知の両方のファイルベースの脅威から防御し、アンチウイルスとサンドボックスを組み合わせた多層型のセキュリティを実現します。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改善し、アプリケーションと使用状況のリアルタイムの可視性を提供します。

Web / DNS セキュリティ

Web / DNS セキュリティサービスは、DNS ベースの攻撃、不正 URL（E メール内の URL も含む）、ボットネット通信からの保護を提供します。DNS フィルタリングは、DNS ベースのあらゆる攻撃をブロックし、URL フィルタリングは、3 億以上の URL のデータベースを使用して不正リンクを特定し、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、ボットネット活動や DDoS 攻撃から保護します。FortiGuard Labs の毎週 5 億以上の不正 / フィッシング / スパム URL のブロックと毎分 32,000 のボットネットのコマンド & コントロールの試行をブロックしている実績は、フォーティネットが提供する堅牢な保護を証明するものです。

SaaS / データセキュリティ

SaaS / データセキュリティサービスは、アプリケーションの使用とデータ保護に対する重要なセキュリティニーズに対応します。このサービスのデータ漏洩防止により、ネットワーク、クラウド、ユーザーの間を移動するデータの可視化、管理、保護（持ち出しの阻止）が可能になります。フォーティネットのインラインクラウドアクセスセキュリティブローカーサービスは、移動データ、保存データ、クラウド内のデータを保護することで、コンプライアンス標準を適用し、アカウント、ユーザー、クラウドアプリの使用状況を管理します。また、インフラストラクチャを評価し、構成を検証し、IoT デバイスの検知や脆弱性の相関などのリスクや脆弱性を明らかにします。

ゼロデイ脅威保護

ゼロデイ脅威保護は、AI を活用したインラインマルウェア保護により、ファイルの内容を分析して未知のマルウェアをリアルタイムで特定してブロックすることで、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® マトリクスの統合により、迅速な調査を可能にします。FortiGate NGFW に統合されたこのサービスは、未知の脅威をブロックし、インシデントレスポンスを合理化し、セキュリティオーバーヘッドを軽減することで、包括的な防御が実現します。

OT セキュリティ

統合型の OT セキュリティ機能は、1,000 以上の仮想パッチ、1,100 以上の OT アプリケーション、3,300 以上のプロトコルルールを活用して、OT インフラストラクチャを標的にする脅威を検知し、脆弱性の相関付けを実行し、仮想パッチを適用し、業界に特化したプロトコルデコーダを利用して OT 環境とデバイスの堅牢な防御を可能にします。

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リアルタイムネットワークセキュリティオペレーティングシステム

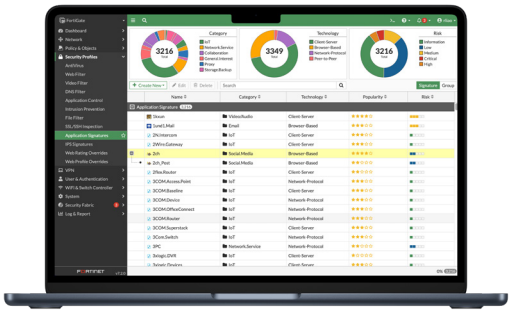
FortiOS は、フォーティネット セキュリティ ファブリック プラットフォームの基盤となるオペレーティングシステムとして、デジタル攻撃対象領域全体でのセキュリティポリシーの適用を可能にし、包括的なビューを提供します。FortiOS は、ネットワーク、クラウドベース、ハイブリッド、または IT / OT / IoT のコンバージェンスの管理と保護の統一フレームワークを提供し、AI を活用した一貫性ある統合型の保護を今日のハイブリッド環境で実現することで、フォーティネット製品のシームレスで効率的な相互運用を可能にします。

従来のポイントソリューションとは異なり、フォーティネットは、サイバーセキュリティの包括的アプローチを採用することで、複雑さの軽減、セキュリティサイロの排除、運用の効率化を可能にします。FortiOS は、セキュリティ機能を単一のプラットフォームに統合することで、管理を簡素化し、コストを削減し、全体的なセキュリティ態勢を強化します。FortiGate と FortiOS の連携により、インテリジェントで適応型の保護が実現するため、複雑さの軽減、セキュリティサイロの解消、ユーザーエクスペリエンスの最適化が可能になります。

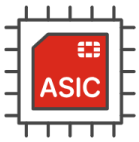
FortiOS は、生成 AI の統合により、ネットワークトラフィックや脅威インテリジェンスを分析する能力を強化し、逸脱や異常を効果的に検知し、修復についての精度の高い推奨事項を提示することで、セキュリティを侵害することなく、パフォーマンスへの影響を最小化します。

FortiOS の最新情報をご覧ください。https://www.fortinet.com/jp/products/fortigate/fortios

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



ネットワークパフォーマンス、セキュリティ、
システムステータスの包括的なビュー



フォーティネットの ASIC：
比類ないセキュリティ、圧倒的なパフォーマンス

専用設計の SPU を活用

従来型のファイアウォールは、市販の汎用 CPU に依存しているため、危険なセキュリティギャップが存在し、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。フォーティネットのカスタム SPU によって、速度、規模、効率性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が大幅に改善され、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 SPU は、最大 520 Gbps の保護スループットを提供することで、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。

フォーティネットの ASIC はエネルギー効率を考慮して設計されているため、消費電力を削減し、TCO が改善されます。業界をリードするスループットを提供し、多くのトラフィックを処理し、セキュリティインスペクションを高速で実行し、待ち時間を短縮して迅速なパケット処理を可能にし、ネットワークの遅延を最小化します。

フォーティネットの SPU は、ゼロトラスト、SSL、IPS、VXLAN などの多くのセキュリティ機能を統合して設計されているため、競合他社がソフトウェアに実装していたこれらの機能のパフォーマンスが大幅に向上します。

セキュア SD-WAN ASIC SP5

- 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 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 セキュリティと高パフォーマンスのディープ SSL インスペク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

一元管理によりセキュリティと効率性を効率化

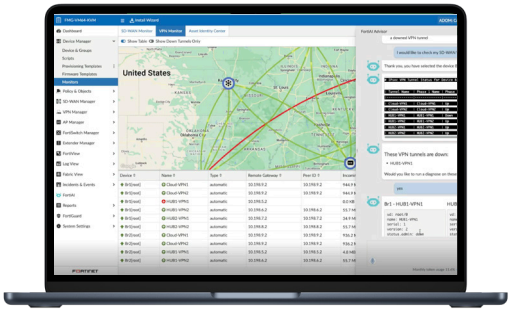
フォーティネットは、セキュリティインフラストラクチャの一元管理、可視化、自動化をあらゆる規模の企業に提供します。

FortiManager：分散型のエンタープライズに対応するスケーラブルな一元管理

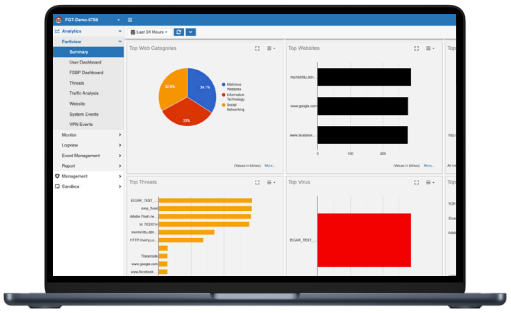
FortiManager は、フォーティネット セキュリティ ファブリックの一元管理を可能にする、FortiAI を搭載するソリューションです。ハイブリッド環境の FortiGate、FortiGate VM、クラウドセキュリティ、SD-WAN、SD ブランチ、FortiSASE、ZTNA のマスプロビジョニングとポリシー管理を合理化します。さらには、管理対象インフラストラクチャ全体をリアルタイムで監視し、ネットワークオペレーションワークフローを自動化します。FortiAI の GenAI を活用することで、計画から導入の段階での構成やプロビジョニング、運用の段階でのトラブルシューティングとメンテナンスがさらに強化され、フォーティネット セキュリティ ファブリックの可能性が最大化し、運用効率が大幅に向上します。

FortiGate Cloud：中小規模企業向けの簡素化された管理

FortiGate Cloud は、フォーティネットの FortiGate NGFW の管理、セキュリティ分析、レポートを簡素化することでデバイスの効率的な管理とサイバーリスクの低減を支援する SaaS サービスです。ゼロタッチプロビジョニングにより、FortiGate と FortiAP、FortiSwitch、FortiExtender などのダウンストリームの接続デバイスの初期導入、セットアップ、継続的な管理を簡素化します。トラフィック分析とセキュリティ脅威のリアルタイムと履歴のどちらでも可視化することで、リスクの低減とセキュリティ態勢の強化を実現します。クラウドに保存されたさまざまな脅威、Web トラフィック、システムイベントを最長で 1 年間表示し、事前定義済のレポートを提供することで、コンプライアンスに対応し、実用的なインテリジェンスを提供します。



FortiManager の GenAI は、構成やポリシーのスクリプトの生成、問題のトラブルシューティング、推奨されるアクションの実行などのネットワークの管理を容易にします。



FortiGate Cloud は、エンドツーエンドの可視性、ログ、レポートの機能を SMB に提供する、直感的な操作が可能な管理 / 分析ソリューションです。

FortiConverter サービス

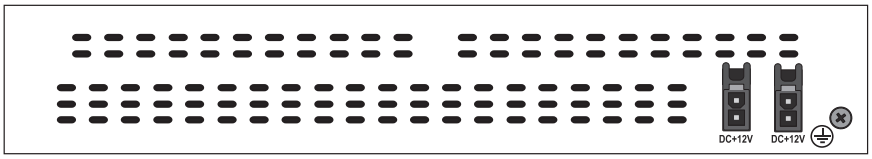
FortiGate NGFW への容易な移行

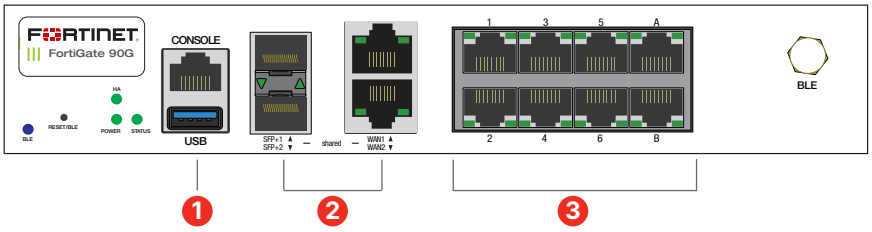
FortiConverter サービスは、従来型のさまざまなファイアウォールから FortiGate NGFW への迅速かつ容易な移行を支援します。このサービスは、高度な方法論と自動化されたプロセスによるベストプラクティスの採用により、エラーや冗長性を排除します。最新の FortiOS テクノロジーに移行することで、企業はネットワーク保護を加速させることができます。

ハードウェア

FortiGate 90G / 91G

SP5 DESKTOP 120GB





インタフェース

1. 1 × RJ45 管理コンソールポート / 1 × USB 管理ポート
2. 2 × 10 / 5 / 2.5 / GbE RJ45 または 10 GbE / GbE SFP+ / SFP 共有メディアポート
3. 8 × GbE RJ45 ポート

ハードウェアの特長

トラステッドプラットフォームモジュール（TPM）

FortiGate 90G シリーズは、暗号鍵の生成、保存、認証を実行して物理ネットワークアプライアンスを堅牢化する専用モジュールを搭載しています。ハードウェアベースのセキュリティメカニズムが、悪意のあるソフトウェアやフィッシング攻撃からお客様を保護します。

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 FortiGate 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。

技術仕様

	FortiGate 90G	FortiGate 91G
インタフェースとモジュール		
10 / 5 / 2.5 / GbE RJ45 または 10 GbE / GbE SFP+ / SFP 共有メディアポート	2	2
GbE RJ45 内蔵ポート	8	8
無線インタフェース	—	—
USB ポート	1	1
RJ45 管理コンソールポート	1	1
内蔵ストレージ	—	1 × 120 GB SSD
トラステッドプラットフォームモジュール（TPM）	✓	✓
Bluetooth Low Energy（BLE）	✓	✓
署名付きファームウェア ハードウェアスイッチ	—	—
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 [2]	4.5 Gbps	
NGFW スループット [2、4]	2.5 Gbps	
脅威保護スループット [2、5]	2.2 Gbps	
システム性能		
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）	28 / 28 / 27.9 Gbps	
ファイアウォールレイテンシ（64 バイト UDP パケット）	3.23 µs	
ファイアウォールスループット（パケット / 秒）	41.85 Mpps	
ファイアウォール同時セッション（TCP）	3 M	
ファイアウォール新規セッション / 秒（TCP）	124,000	
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）[1]	25 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	2,500	
SSL-VPN スループット [6]	1.4 Gbps	
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）[3]	2.6 Gbps	
SSL インスペクション CPS（IPS、avg. HTTPS）[3]	1,400	
SSL インスペクション同時セッション（IPS、avg. HTTPS）[3]	300,000	
アプリケーション制御スループット（HTTP 64 K）[2]	6.7 Gbps	
CAPWAP スループット（HTTP 64K）	23.6 Gbps	
仮想 UTM（VDOM：標準 / 最大）	10 / 10	
FortiSwitch サポート数	24	
FortiAP サポート数（合計 / トンネルモード）	128 / 64	
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	

	FortiGate 90G	FortiGate 91G
サイズ		
高さ × 幅 × 奥行	42 × 216 × 178 mm	
重量	1.12 kg	
形状	デスクトップ	
動作環境 / 準拠規格・認定		
定格入力	12 V DC、3 A（冗長電源）	
電源（オプションで冗長化可能）	100 ～ 240 V AC、50 ～ 60 Hz（2 × 外部 DC 電源）（1 つのアダプター同梱）	
電源効率指標	80 Plus 規格に準拠	
電源（オプションで冗長化可能）	100 ～ 240 V AC、50 ～ 60 Hz（2 × 外部 DC 電源）（1 つのアダプター同梱）	
最大電流	115 V AC / 0.4 A、230 V AC / 0.2 A	
消費電力（平均 / 最大）	19.9 W / 20.53 W	22.4 W / 23.5 W
放熱	70.0 BTU/h	80.1 BTU/h
動作温度	0 ～ 40 °C	
保管温度	-35 °C ～ 70 °C	
湿度	10 ～ 90%（結露しないこと）	
騒音レベル	21.73 dBA	
動作高度	最高 3,048 m	
準拠規格・認定	FCC、ICES、CE、RCM、VCCI、BSMI、UL/cUL、CB	
認定	USGv6 / IPv6	

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。

[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（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。

[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] SSL VPN は、7.0.12 から 7.0.15 のみサポートしています。

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 [3]、AI-based Heurestic AV、FortiGate Cloud Sandbox	•	•	•	•
	URL、DNS and Video Filtering — URL、DNS and Video [3] Filtering、Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	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 [1]	•			
	Application Control		FortiCare サブスクリプションに含まれています。		
	Inline CASB [3]		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) [2]	•			
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	•			
	FortiGuard SOCaaS — 24×7 cloud-based managed log monitoring、incident triage、SOC escalation service	•			
ハードウェア / ソフトウェアサポート	FortiCare Essentials [2]	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
基本サービス	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

FortiGate 向け FortiGuard AI 活用セキュリティバンドル

FortiGuard AI 活用セキュリティバンドルは、既知や未知の攻撃、ゼロデイ攻撃、新たに登場する AI ベースの脅威からの保護を支援することを目標に厳選されたセキュリティサービスで構成されています。これらのサービスは、不正コンテンツによる侵害を防止し、Web ベースの脅威から保護し、IT / OT / IoT 環境のデバイスを保護し、アプリケーション、ユーザー、データの安全性を保証するように設計されています。すべてのバンドルに、24 時間 365 日のサポートを提供する FortiCare Premium が付属しており、重大な問題については 1 時間、それ以外の問題については翌営業日のレスポンスが提供されます。

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。このアドバンストサポートオプションには、18 ヵ月の EoE（Extended End-of-Engineering-Support）が含まれており、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。

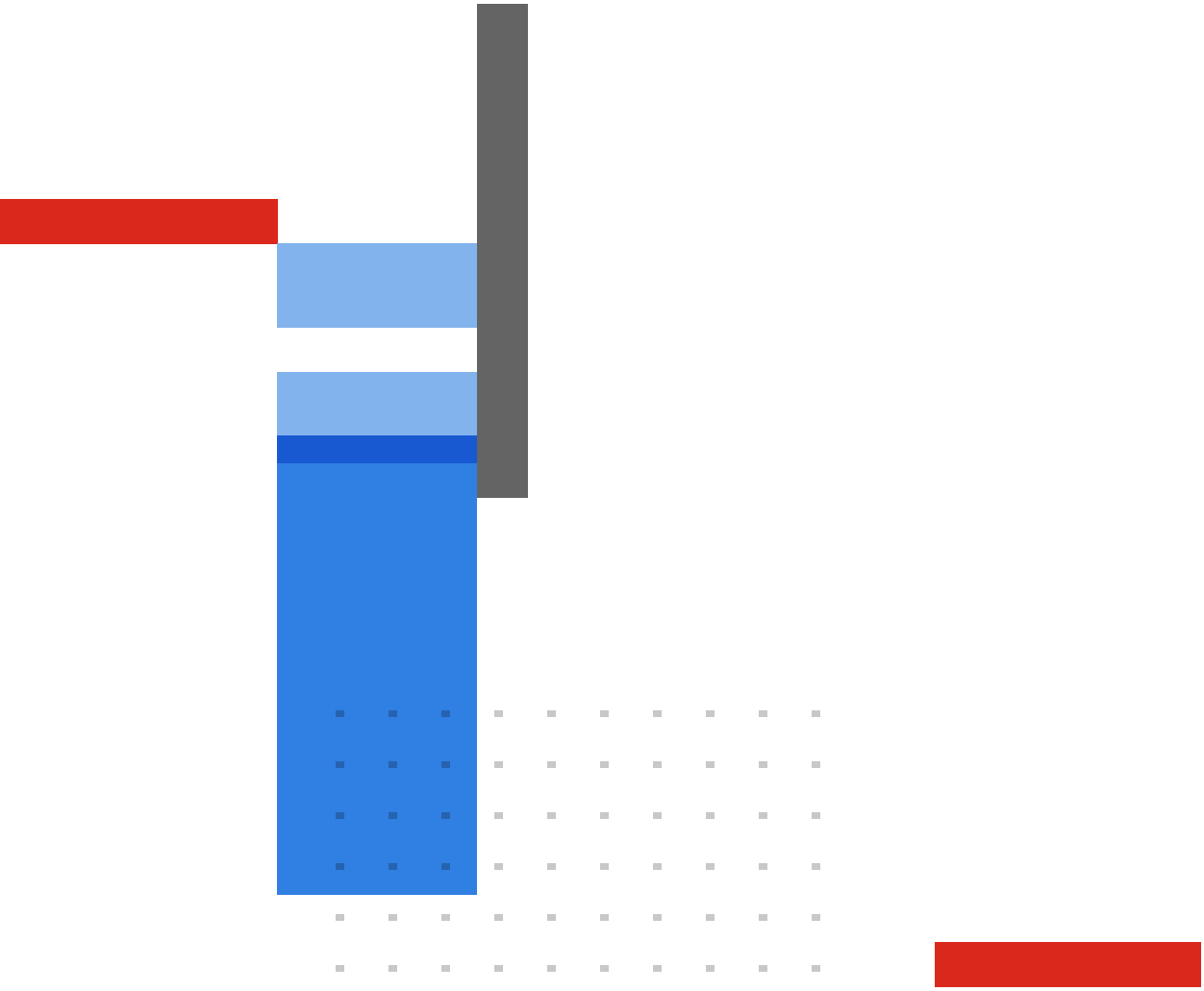
オーダー情報

Product	SKU	Description
FortiGate 90G	FG-90G	8x GE RJ45 ports, 2× 10GE RJ45/SFP+ shared media WAN ports.
FortiGate 91G	FG-91G	8x GE RJ45 ports, 2× 10GE RJ45/SFP+ shared media WAN ports with 120GB SSD.
Optional Accessories		
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, FG/FWF 60F/61F, FG-80E/81E, FG-80F/81F, and FG-90G/91G.
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F, FG-90G/91G and FG/FWF-80F series.
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E, F, and G series desktop models.
Mounting Ear Bracket	SP-EAR-FG90G-10	Mounting Ear brackets for FG-90/91G 10 pairs pack.
Transceivers		
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10 GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver Module, (connects to FN-TRAN-SFP+BD27, ordered separately)	FN-TRAN-SFP+BD33	10 GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
Cables		
10 GE SFP+ Passive Direct Attach Cable, 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable, 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable, 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.

詳細は、「オーダーガイド」をご参照ください。https://www.fortinet.com/resources/ordering-guides

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になります。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。



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

お問い合わせ

DS-FG-90G-R09-202412-R1