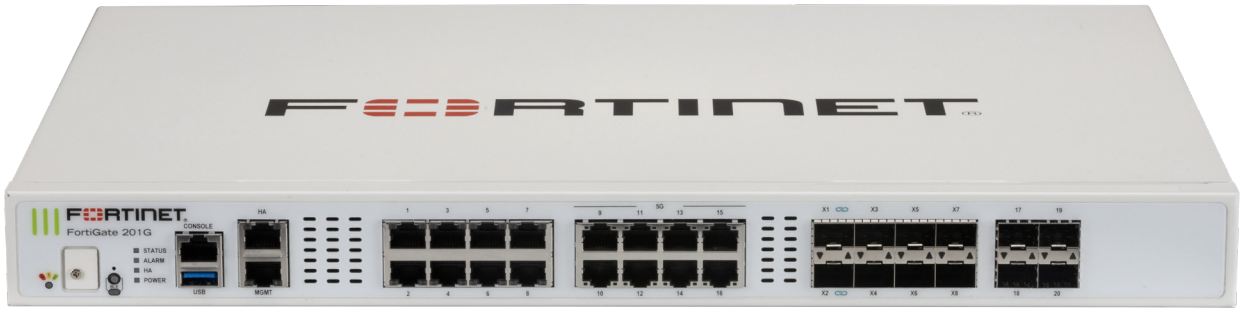
FortiGate 200G シリーズ



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

セキュアネットワーキング：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

最先端の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 SPU / vSPU 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

細部に至る可視性：アプリケーション、ユーザー、デバイスを従来のファイアウォールでは提供できないレベルまで可視化

AI（人工知能）/ ML（機械学習）を活用したセキュリティと詳細な可視化

FortiGate 200G シリーズ次世代ファイアウォール（NGFW）は、AI を活用したセキュリティと機械学習の組み合わせにより、あらゆる規模の脅威保護を実現します。ネットワークを細部まで可視化することで、脅威に発展する前に、アプリケーション、ユーザー、デバイスの状態を把握できるようにします。

FortiGate 200G シリーズは、豊富な AI / ML セキュリティ機能セットを統合セキュリティ ファブリック プラットフォームにまで拡張することで、広範かつ詳細で自動化されたセキュアネットワーキングを実現します。Web、コンテンツ、デバイスのセキュリティを含む高度なエッジ保護により、ネットワークのエンドツーエンドの保護を可能にし、ネットワークセグメンテーションとセキュア SD-WAN でハイブリッド IT ネットワークの複雑さとリスクを軽減します。セキュリティ ファブリックは、ハイブリッドメッシュファイアウォールアーキテクチャを含む、環境全体にわたりシームレスに拡張され、すべてのネットワークセグメントで一貫したポリシーの適用と脅威保護を確保します。

ユニバーサル ZTNA（ゼロトラストネットワークアクセス）は、アプリケーションへのユーザーアクセスの自動的な制御と検証を容易にし、検証されたユーザーのみにアクセスを提供することで、脅威のラテラルムーブメントを低減します。超高速の脅威保護と SSL インスペクションが、パフォーマンスに影響することなく、エッジの可視化と保護を可能にします。

IPS	NGFW	脅威保護	インタフェース
9 Gbps	7 Gbps	6 Gbps	複数の GbE RJ45、5 GbE RJ45、10 GbE SFP+ ポート、GbE SFP ポート

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

次世代ファイアウォール（NGFW）

- FortiGuard Labs の AI を活用するセキュリティサービススイートと NGFW のネイティブ統合により、Web、コンテンツ、デバイスを保護し、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）テクノロジーにより、業界をリードするハイパフォーマンス保護を提供

セキュア SD-WAN

- FortiGate WAN エッジでは、1 つの OS を採用し、セキュリティと管理のフレームワークとシステムを統一することで、WAN のトランスフォーメーションと保護を実現
- 高品質のユーザーエクスペリエンスと効果的なセキュリティ態勢を、ハイブリッドワークモデル、SD ブランチ、クラウドファースト WAN のユースケースで実現
- 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

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
- 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

セグメンテーション

- 動的セグメンテーションが、あらゆるネットワークトポロジに適応し、支社からデータセンター、さらにはマルチクラウド環境までの真のエンドツーエンドセキュリティを提供
- 超スケーラブル、低遅延、VXLAN セグメンテーションにより、レイヤ 4 ファイアウォールルールで物理ドメインと仮想ドメインをブリッジ
- FortiGuard セキュリティサービスによる高度な協調型の保護で既知、ゼロデイ、未知の攻撃を検知して防止することで、ネットワークでのラテラルムーブメントを防止

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のブロックという実績は、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® マトリクスも統合により、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

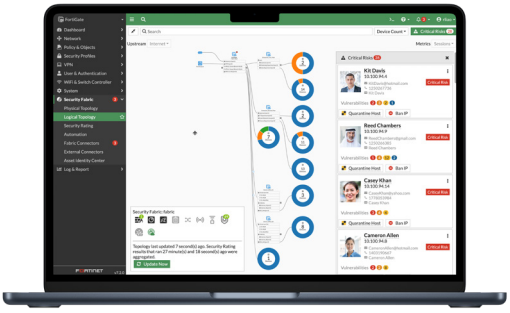
FortiOS：フォーティネットのリアルタイムネットワークセキュリティオペレーティングシステム

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。

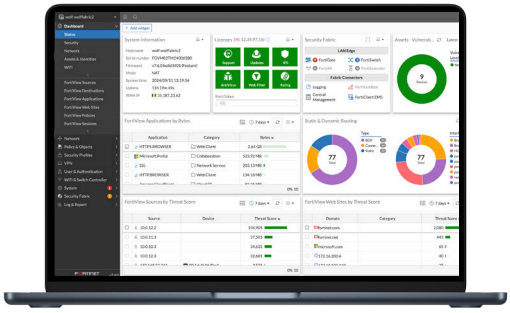
従来のポイントソリューションとは異なり、フォーティネットは、サイバーセキュリティの包括的アプローチを採用することで、複雑さの軽減、セキュリティサイロの排除、運用の効率化を可能にします。FortiOS は、セキュリティ機能を単一のプラットフォームに統合することで、管理を簡素化し、コストを削減し、全体的なセキュリティ態勢を強化します。FortiGate と FortiOS の連携により、インテリジェントで適応型の保護が実現するため、複雑さの軽減、セキュリティサイロの解消、ユーザーエクスペリエンスの最適化が可能になります。

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。

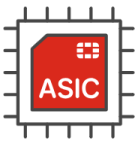
FortiOS の最新情報を、https://www.fortinet.com/jp/products/fortigate/fortios でご覧ください。



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て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、待ち時間を短縮することで迅速なパケット処理が可能になり、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。

ネットワークプロセッサ NP7Lite

フォーティネットが新たに提供する画期的な SPU である NP7Lite ネットワークプロセッサは、FortiOS の各機能と連携し、次の優れた性能を発揮します。

- IPv4 / IPv6、SCTP、およびマルチキャストのトラフィックにおいて優れたファイアウォールパフォーマンスを発揮し、超低遅延を実現
- VPN、CAPWAP、および IP トンネルのアクセラレーション
- アノマリベースの不正侵入検知 / 防御、チェックサムオフロード、およびパケットデフラグ
- トラフィックシェーピングおよびプライオリティキューイング

コンテンツプロセッサ CP10

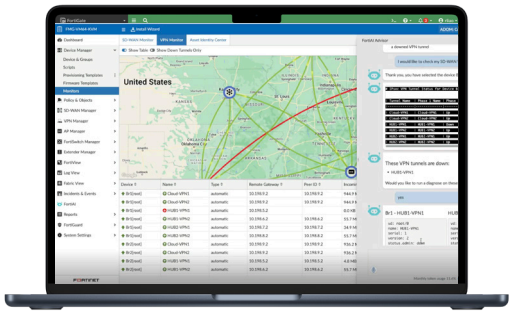
コンテンツプロセッサは、セキュリティ機能において大量のリソースを必要とする処理をオフロードするコプロセッサとして機能します。フォーティネットの第 10 世代コンテンツプロセッサである CP10 は、大量のリソースを必要とする SSL（TLS 1.3 を含む）の復号とセキュリティの機能を高速化しつつ、以下を実現します。

- パターンマッチングの高速化とリアルタイムトラフィックの高速インスペクションによりアプリケーションを識別
- IPS プレスキャン / プレマッチ、シグネチャ相関付けのオフロード、高速アンチウイルス処理

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。



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。

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 テクノロジーにより、ネットワーク保護が加速します。

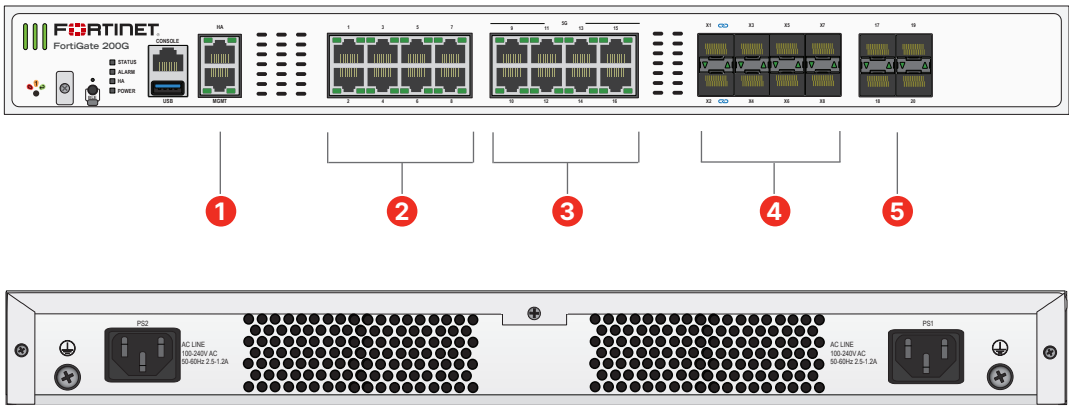
FortiCare サービス

エキスパートによるサービス

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。

ハードウェア

FortiGate 200G シリーズ



インタフェース

1. 2 × GbE RJ45 管理 / HA ポート
2. 8 × GbE RJ45 ポート
3. 8 × 5 / 2.5 / GbE RJ45 ポート
4. 8 × 10 GbE SFP+ / SFP FortiLink ポート
5. 4 × GbE SFP ポート

ハードウェアの特長

NP7Lite (SP5) | CP10 | TPM | 1RU | DUAL AC | 10/5/GE | 480GB

トラステッドプラットフォームモジュール（TPM）

FortiGate 200G 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。

電源冗長化ユニットのサポート

ミッションクリティカルなネットワークの運用には電源の冗長化が不可欠です。FortiGate 200G シリーズは、内蔵型の電源冗長化ユニット（ホットスワップ非対応）を採用しています。

アクセスレイヤーセキュリティ

FortiLink プロトコルにより、FortiSwitch をファイアウォールの論理拡張として 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。

署名付きファームウェア ハードウェアスイッチ

署名付きファームウェアスイッチは、物理セキュリティスイッチです。デフォルトでは、最高のセキュリティレベルに設定されています。最高のセキュリティレベルでは、正しく検証された FortiOS ファームウェアのみが FortiGate にロードされます。この機能により、FortiGate にセキュリティの物理レイヤーが追加され、侵害に対する重要な抑止力として機能し、侵害のリスクを低減します。

技術仕様

	FortiGate 200G	FortiGate 201G
インタフェースとモジュール		
GbE RJ45 ポート	8	
GbE RJ45 管理 / HA ポート	1 / 1	
5 / 2.5/ GbE RJ45 ポート	8	
GbE SFP ポート	4	
10 / GbE SFP/+ FortiLink ポート（デフォルト）	8	
USB ポート	1	
管理コンソールポート	1	
内蔵ストレージ	—	1 × 480 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	✓	
付属トランシーバ	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 [2]	9 Gbps	
NGFW スループット [2、4]	7 Gbps	
脅威保護スループット [2、5]	6 Gbps	
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）	39 / 39 / 26.5 Gbps	
IPv6 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）	39 / 39 / 26.5 Gbps	
ファイアウォールレイテンシ（64 バイト UDP パケット）	4.36 µs	
ファイアウォールスループット（パケット / 秒）	39.75 Mpps	
ファイアウォール同時セッション（TCP）	11 M	
ファイアウォール新規セッション / 秒（TCP）	400,000	
ファイアウォールポリシー	10,000	
IPSec VPN スループット（512 バイト）[1]	36 Gbps	
ゲートウェイ間 IPSec VPN トンネル	2,000	
クライアント - ゲートウェイ間 IPSec VPN トンネル	16,000	
SSL-VPN スループット [6]	3 Gbps	
同時 SSL-VPN ユーザー（推奨最大値、トンネルモード）	500	
SSL インスペクションスループット（IPS、avg. HTTPS）[3]	7 Gbps	
SSL インスペクション CPS（IPS、avg. HTTPS）[3]	7,100	
SSL インスペクション同時セッション（IPS、avg. HTTPS）[3]	900,000	
アプリケーション制御スループット（HTTP 64 K）[2]	27.8 Gbps	
CAPWAP スループット（HTTP 64K）	37.5 Gbps	
仮想 UTM（VDOM：標準 / 最大）	10 / 25	
FortiSwitch サポート数	64	
FortiAP サポート数（合計 / トンネルモード）	256 / 128	
FortiToken サポート数	5,000	
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 200G	FortiGate 201G
サイズ / 電源		
高さ × 幅 × 奥行	44.45 × 432 × 380 mm	
重量	6.4 kg	6.5 kg
形状（EIA 規格およびその他の 19 インチラック適合）	ラックマウント（1 RU）	
AC 消費電力（平均 / 最大）	145 W / 175 W	145 W / 176 W
AC 電源入力	100 ～ 240 V AC、50 ～ 60Hz	
AC 最大電流	100 V AC / 2 A、240 V AC / 1.2 A	
放熱	597.12 BTU/h	600.54 BTU/h
電源効率指標	80 Plus 規格に準拠	
冗長電源	✓ デフォルト：1+1 冗長　スワップ非対応 デュアル AC 電源	
動作環境 / 準拠規格・認定		
動作温度	0 ～ 40 °C	
保管温度	-35 °C ～ 70 °C	
湿度	5 ～ 90%（結露しないこと）	
騒音レベル	LPA 48 dBA / LWA 55 dBA	
エアフロー	側面、前面～背面	
動作高度	最高 3048 m	
準拠規格・認定	FCC Part 15 Class A、RCM、VCCI、CE、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] RSA-2048 証明書を使用しています。

サブスクリプション

			バンドル		
サービスカテゴリ	提供サービス	アラカルト	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, and One Year Log Retention	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiGuard SOCaaS—24×7 cloud-based managed log monitoring, incident triage, and 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。

FortiGuard 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。

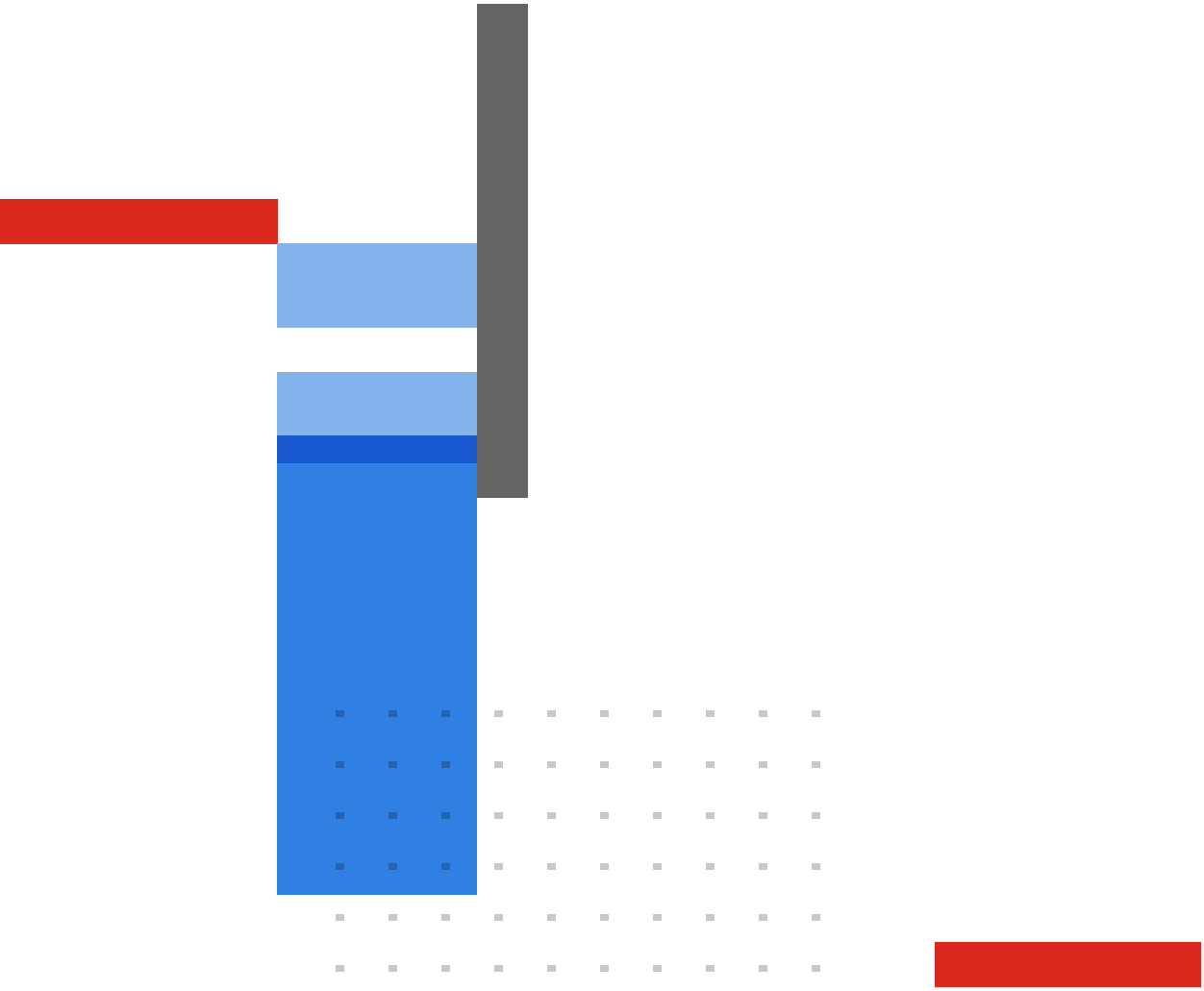
オーダー情報

Product	SKU	Description
FortiGate 200G	FG-200G	10x GE RJ45 (including 1x MGMT port, 1x HA port, 8x switch ports), 4x GE SFP slots, 8× 5GE RJ45, 8× 10GE SFP+ slots, NP7Lite and CP10 hardware accelerated.
FortiGate 201G	FG-201G	10x GE RJ45 (including 1x MGMT port, 1x HA port, 8x switch ports), 4x GE SFP slots, 8× 5GE RJ45, 8× 10GE SFP+ slots, NP7Lite and CP10 hardware accelerated, 480GB onboard SSD storage.
Transceivers		
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, 80km Extreme Long Range	FN-TRAN-SFP+ZR	10GE SFP+ transceiver module, 80km extreme long range, for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10GE 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	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
25 GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range, compatible with 10 GE SFP/SFP+ slots.
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.

関連するオーダーガイドについては、https://www.fortinet.com/resources/ordering-guides をご覧ください。

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-200G-R06-202504-R1