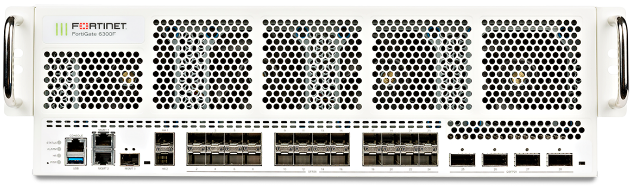
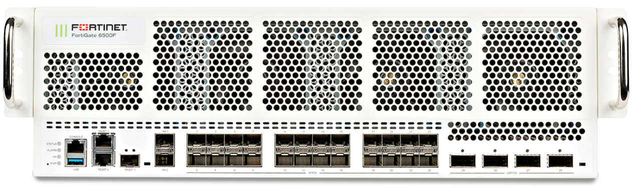
DATA SHEET

# FortiGate 6000F シリーズ

FortiGate 6300F / 6300F-DC、6301F / 6301F-DC、
6500F / 6500F-DC、6501F / 6501F-DC

次世代ファイアウォール
セグメンテーション
IPS
モバイルセキュリティ





FortiGate 6000F 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（NGFW）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、高スループットを実現する FortiGate 6000F シリーズは、エンタープライズのエッジ、ハイブリッドデータセンターコア、および内部セグメントへの配備に理想的です。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。フォーティネットのセキュリティ ドリブン ネットワーキングのアプローチにより、新世代のセキュリティがネットワークへと緊密に統合されます。

### セキュリティ

- ネットワークトラフィック内の数千規模のアプリケーションを特定して詳細に検証し、ポリシーをきめ細かく適用
- 暗号化 / 非暗号化トラフィック両方を、マルウェア、エクスプロイト、不正 Web サイトから保護
- AI 機能を活用した FortiGuard Labs のセキュリティサービスが継続的に提供する最新の脅威インテリジェンスを使用して、既知の攻撃を検知し阻止
- フォーティネット セキュリティ ファブリックと統合された AI ドリブンの FortiSandbox を活用し、未知の巧妙な脅威をプロアクティブにブロック

### 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るイノベーションを支える設計により、超低遅延と業界最高レベルの脅威保護パフォーマンスを実現
- ファイアウォールベンダーとして初の TLS 1.3 ディープインスペクションを提供し、暗号化トラフィックにおいても業界最高レベルのパフォーマンスと保護を実現

### 認定

- 第三者機関のテストによって実証済みのトップクラスのセキュリティ効果とパフォーマンス
- NSS Labs、ICSA、Virus Bulletin、AV Comparatives などの第三者機関によるテストで比類ない高評価を獲得

### ネットワーク機能

- 標準搭載された SD-WAN 機能によるアプリケーション識別型のトラフィックルーティングにより、一貫したアプリケーションパフォーマンスとトップクラスのユーザーエクスペリエンスを実現
- 高度なルーティング機能を内蔵し、大規模な暗号化 IPSec トンネルにおいてもハイパフォーマンスなトラフィック処理が可能

### 管理

- 使いやすく運用効率の高い管理コンソールを提供し、包括的なネットワークの自動化と可視化を実現
- Fabric Management Center（ファブリック管理センター）における一元管理機能を活用する、ゼロタッチプロビジョニングをサポート
- 事前定義済みのコンプライアンスチェックリストによって導入環境を分析し、総体的なセキュリティ状態の向上に役立つベストプラクティスを提示

### セキュリティ ファブリック

- フォーティネットとファブリック レディ パートナーの製品が統合可能になることで、広範なネットワークの可視化、統合的なエンドツーエンドの検知、脅威インテリジェンスの共有、自動修復を実現
- 自動的にネットワークトポロジーを可視化し、IoT デバイスを検知してフォーティネットおよびファブリック レディ パートナー各社の製品における完全な可視化を実現

| モデル | FortiGate 6300F / DC、FortiGate 6301F / DC | FortiGate 6500F / DC、FortiGate 6501F / DC |
|---|---|---|
| ファイアウォール | 239 Gbps | 239 Gbps |
| IPS | 110 Gbps | 170 Gbps |
| NGFW | 90 Gbps | 150 Gbps |
| 脅威保護 | 60 Gbps | 100 Gbps |
| ネットワークインタフェース | 複数の40 / 100 GbE QSFP28、1 / 10 / 25 GbE SFP28、<br>1 / 10 GbE SFP+およびGbE RJ45 | 複数の40 / 100 GbE QSFP28、1 / 10 / 25 GbE SFP28、<br>1 / 10 GbE SFP+およびGbE RJ45 |

詳細は、技術仕様表を参照してください。

# 導入例

## 次世代ファイアウォール（NGFW）

- フォーティネットのセキュリティプロセシングユニット（SPU）を搭載する単一のハイパフォーマンスネットワークセキュリティアプライアンスに脅威保護セキュリティ機能をすべて統合することで、複雑さを軽減し ROI を最大限に向上
- 攻撃対象領域全体でユーザー、デバイス、アプリケーションを完全に可視化すると同時に、企業資産の場所を問わず一貫したセキュリティポリシーを適用
- 有効性、低遅延、そして最適なネットワークパフォーマンスが業界で実証された IPS セキュリティにより、悪用される可能性のあるネットワークの脆弱性から企業を保護
- 業界トップクラスの SSL インスペクションパフォーマンスを活用し、復号されたトラフィックの脅威を自動的にブロックするほか、採用が義務付けられている暗号を使用する最新の TLS 1.3 標準にも対応
- AI ドリブンの FortiGuard Labs のサブスクリプションをはじめ、フォーティネット セキュリティ ファブリックで提供される高度な脅威保護サービスを活用し、新たに発見された巧妙な脅威をリアルタイムでプロアクティブにブロック

## セグメンテーション

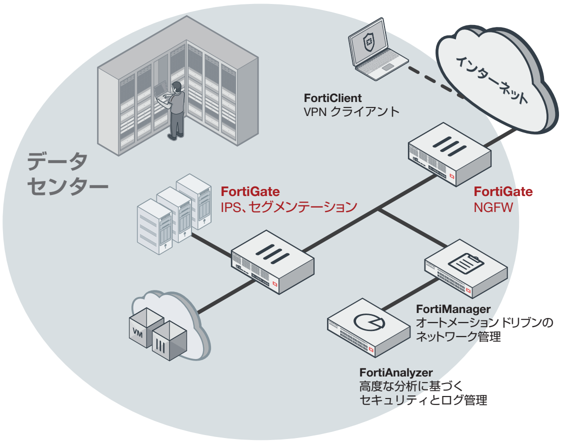
- あらゆるネットワークトポロジーに適応するセグメンテーションにより、支社レベルからデータセンターまで、さらにマルチクラウドへの拡張も可能なエンドツーエンドのセキュリティを提供
- フォーティネット セキュリティ ファブリックを構成するコンポーネントにおけるネットワークの可視性を改善し、セキュリティリスクを低減。フォーティネット セキュリティ ファブリックは、最新のトラストレベルに基づくアクセス許可に適応し、効果と効率に優れたアクセス制御を適用
- フォーティネットの専用 SPU が提供するハイパフォーマンスの L7 インスペクションと修復機能により、縦深防御型のセキュリティを提供すると同時に、保護対象の Mbps あたりの TCO に関して第三者機関による優れた評価を獲得
- クリティカルなビジネスアプリケーションを保護し、ネットワークを再設計することなくあらゆるコンプライアンス要件の達成を支援

## IPS

- 業界で実証された高スループット、低遅延の IPS パフォーマンスを提供する専用設計のセキュリティプロセッサ
- ネットワークレベルで仮想パッチを配備し、悪用される可能性のあるネットワークの脆弱性から企業を保護すると同時に、ネットワークの保護に要する時間を最適化
- ワイヤースピードで詳細なパケットインスペクションを実行し、最新の TLS 1.3 標準で暗号化されたトラフィックをはじめとするネットワークトラフィックにおいて、脅威に対する比類ない可視性を提供
- フォーティネット セキュリティ ファブリックのインテリジェンスサービスが提供する高度な脅威保護機能により、新たに発見された巧妙な攻撃をリアルタイムでプロアクティブにブロック

## 4G、5G、IoT に理想的なモバイルセキュリティ

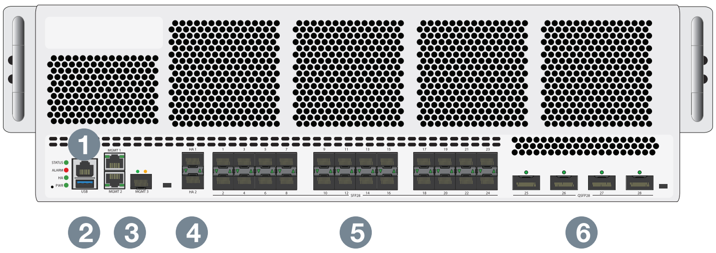
- SPU によって高速処理される、4G SGi LAN および 5G N6 セキュリティ対応のハイパフォーマンス CGNAT / IPv4 / IPv6 トラフィック
- 高度な拡張性を備えたトッププラスのパフォーマンスの IPsec アグリゲーションおよび制御用セキュリティゲートウェイ（SecGW）による RAN アクセスセキュリティ
- GTP-U インスペクションにおける完全な脅威保護と可視化によって実現するユーザープレーンセキュリティ
- SCTP、GTP-U/C および SIP などのユーザーおよびデータプレーントラフィック向けの 4G / 5G セキュリティにより、攻撃に対する保護を提供
- 4G / 5G コアネットワークにおける IoT のシグナリングストーム保護
- 柔軟な導入展開を支援する高速インタフェースを装備

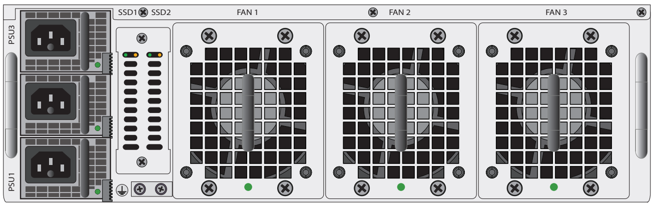


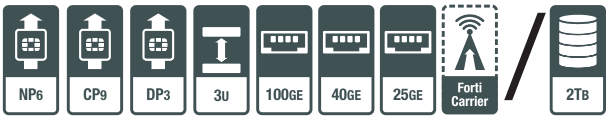

FortiGate 6000Fのデータセンターへの導入例
（NGFW、IPS、インテント ベースト セグメンテーション）

# ハードウェア

## FortiGate 6300F / DC、6301F / DC、6500F / DC、6501F / DC




### インタフェース

1. シリアル管理コンソールインタフェース
2. USB インタフェース
3. 2 x GbE RJ45、1 x 1 / 10 GbE SFP+ 管理インタフェース
4. 2 x 10 GbE SFP+ HA インタフェース
5. 24 x 1 / 10 / 25 GbE SFP28 インタフェース
6. 4 x 40 / 100 GbE QSFP28 インタフェース

### SPU によるアクセラレーション

- フォーティネット独自の SPU プロセッサにより、悪意のあるコンテンツを検出するために必要なマルチギガビットの高速な処理能力を提供します
- 汎用 CPU に依存しているセキュリティテクノロジーでは、危険なパフォーマンスギャップが発生し、今日の多様なコンテンツベース / 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
- SPU プロセッサは、最新の脅威を阻止すること、第三者による厳格な認証要件を満たすこと、ネットワークセキュリティソリューションがネットワークのボトルネックにならないこと、を満たすために必要な優れたパフォーマンスを提供します

### ネットワークプロセッサ

フォーティネットが新たに提供する画期的な SPU である NP6 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、2 マイクロ秒の超低遅延を実現
- VPN 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

フォーティネットが新たに提供する画期的な SPU である CP9 コンテンツプロセッサは、トラフィックのダイレクトフローから独立して動作し、次のような演算処理集約型のセキュリティ機能を高速処理します。

- SPU でシグネチャのマッチングを完全実行する独自の機能により、IPS パフォーマンスを強化
- 業界で使用を義務付けられている最新の暗号化スイート（Cipher Suites）を基盤とする SSL インスペクション機能
- 暗号化 / 復号のオフロード

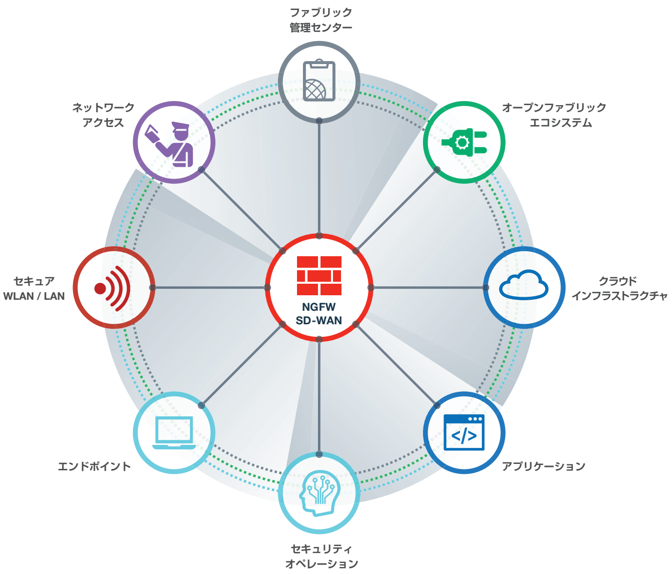
### ディストリビューションプロセッサ

フォーティネット独自の SPU である DP3 ディストリビューションプロセッサは、ハードウェアによる複数のユニットへのトラフィック処理の負荷分散を可能にします。

# フォーティネット セキュリティ ファブリック

## セキュリティ ファブリック

フォーティネット セキュリティ ファブリックは、デジタルイノベーションを実現するサイバーセキュリティプラットフォームです。攻撃対象領域全体の広範な可視化を実現し、リスク管理能力を改善します。セキュリティ ファブリックよってソリューションが 1 つに統合されることで、複数の単機能製品を管理する複雑な作業が軽減すると同時に、ワークフローの自動化によって短時間での効率的なオペレーションが可能となりフォーティネットが展開するエコシステム全体で迅速なレスポンスが実現します。フォーティネット セキュリティ ファブリックは、一元的なファブリック管理センターから次の主要な領域の管理を実現します。




- **セキュリティ ドリブン ネットワーキング:** ネットワークおよびユーザーエクスペリエンスの保護、高速化、統合
- **ゼロトラストネットワークアクセス：** オンネットワークとオフネットワーク両方でユーザーとデバイスをリアルタイムで識別し、保護
- **ダイナミッククラウドセキュリティ：** クラウドインフラストラクチャとアプリケーションを保護し、制御
- **AI（人工知能）ドリブン セキュリティオペレーション：** サイバー脅威の防止、検知、レスポンスを自動化

## FortiOS

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 FortiGate では、フォーティネット独自の FortiOS がその中核として機能しています。FortiOS は直感的なセキュリティオペレーティングシステムで、FortiGate プラットフォーム全体にわたるセキュリティおよびネットワーク機能をすべて一元制御できます。次世代のセキュリティ製品やサービスを単一のプラットフォームに統合する FortiOS は、複雑さやコストの軽減、そしてレスポンスに要する時間の短縮を実現します。

- 一元管理が可能な単一の OS により、デジタル攻撃対象領域を網羅する真の統合セキュリティプラットフォームが実現します。
- 業界最先端の保護機能：NSS Labs の「Recommended（推奨）」評価および VB100 アワード獲得、AV Comparatives および ICSA 認定の優れたセキュリティとパフォーマンスが提供されます。
- 脅威を欺き誘い出すデセプションベースのセキュリティをはじめとする最新技術を活用できます。
- TLS 1.3 の完全サポートに加えて、数千ものアプリケーションの制御、最新のエクスプロイトのブロック、そして数百万規模の URL のリアルタイム評価に基づく Web トラフィックのフィルタリングが可能です。
- AI 活用によるセキュリティ侵害の防止と高度な脅威保護フレームワークの統合により、わずか数分で巧妙な攻撃からの自動的な防御、検知、そして減災を実現します。
- 革新的な SD-WAN 機能、そしてセグメンテーションの自動化による脅威の検知、封じ込め、隔離の機能をフル活用し、ユーザーエクスペリエンスの改善と統一を実現します。
- SPU ハードウェアアクセラレーションを活用し、ネットワークセキュリティのパフォーマンスを強化します。

# サービス

## FortiGuard セキュリティサービス

FortiGuard Labs は、脅威の最新状況に関するリアルタイムの情報を駆使して、フォーティネットのさまざまなソリューション向けに包括的なセキュリティアップデートを提供します。セキュリティに対する脅威の研究者、エンジニア、犯罪科学のスペシャリストで構成されるチームが、脅威の監視を手掛ける世界有数の機関やネットワーク / セキュリティ分野を代表するベンダー、世界各国の捜査機関と協力して、優れたサービスをお届けします。

## FortiCare サポートサービス

FortiCare カスタマーサポートチームは、全てのフォーティネット製品に関する技術サポートをグローバルに提供します。FortiCare は南北アメリカ、ヨーロッパ、中東、アジアの各地域にサポートスタッフを配備しており、あらゆる規模の企業ニーズに最適なサービスを提供します。

詳細は、www.fortinet.com/jp/threat-research および www.fortinet.com/jp/forticare をご覧ください。

# 技術仕様

| | FortiGate 6300F、FortiGate 6300F-DC / FortiGate 6301F、FortiGate 6301F-DC | FortiGate 6500F、FortiGate 6500F-DC / FortiGate 6501F、FortiGate 6501F-DC |
|---|---|---|
| **インタフェースとモジュール** | | |
| 40 / 100 GbE QSFP28 インタフェース | 4 | |
| 1 / 10 / 25 GbE SFP28 インタフェース | 24 | |
| 10 GbE SFP+ インタフェース | 3 | |
| GbE RJ45 管理インタフェース | 2 | |
| USB インタフェース | 1 | |
| シリアル管理コンソールインタフェース | 1 | |
| 内蔵ストレージ | 2 x 1 TB NVMe（6301F および 6501F のみ） | |
| 付属トランシーバ | 2 x SFP+（SR 10 GbE）モジュール | |
| **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 [1] | 110 Gbps | 170 Gbps |
| NGFW スループット [1、2] | 90 Gbps | 150 Gbps |
| 脅威保護スループット [1、3] | 60 Gbps | 100 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） | 239 / 238 / 135 Gbps | 239 / 238 / 135 Gbps |
| ファイアウォールレイテンシ（64 バイト UDP パケット） | 5 μ s | 5 μ s |
| ファイアウォールスループット（パケット / 秒） | 202.5 Mpps | 202.5 Mpps |
| ファイアウォール同時セッション（TCP） | 120 M | 200 M |
| ファイアウォール新規セッション / 秒（TCP） | 2 M | 3 M |
| ファイアウォールポリシー | 200,000 | 200,000 |
| IPSec VPN スループット（512 バイト）[4] | 96 Gbps | 160 Gbps |
| ゲートウェイ間 IPSec VPN トンネル | 16,000 | 16,000 |
| クライアント - ゲートウェイ間 IPSec VPN トンネル | 90,000 | 90,000 |
| SSL-VPN スループット | 9 Gbps | 9 Gbps |
| 同時 SSL-VPN ユーザー（推奨最大値、トンネルモード） | 30,000 | 30,000 |
| SSL インスペクションスループット（IPS、avg. HTTPS）[5] | 66 Gbps | 110 Gbps |
| SSL インスペクション CPS（IPS、avg. HTTPS）[5] | 30,000 | 50,000 |
| SSL インスペクション同時セッション（IPS、avg. HTTPS）[5] | 10 M | 18 M |
| アプリケーション制御スループット（HTTP 64 K）[1] | 150 Gbps | 220 Gbps |
| CAPWAP スループット（1444 バイト UDP パケット） | — | — |
| 仮想 UTM（VDOM：標準 / 最大） | 10 / 500 | |
| FortiSwitch サポート数 | 256 | |
| FortiAP サポート数（合計 / トンネルモード） | — | |
| 高可用性（HA） | ○ | |

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. 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。
2. 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。
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。
4. 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。
5. 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。

| | FortiGate 6300F、FortiGate 6300F-DC / FortiGate 6301F、FortiGate 6301F-DC | FortiGate 6500F、FortiGate 6500F-DC / FortiGate 6501F、FortiGate 6501F-DC |
|---|---|---|
| **ハードウェア仕様** | | |
| 高さ x 幅 x 奥行 | 132 x 437 x 665 mm | 133 x 437 x 694 mm |
| 重量 | 30.7 kg / 31.3 kg | 35.5 kg / 36.1 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（3 RU） | |
| AC 電源 | 100 ～ 240 V AC、50 ～ 60 Hz | |
| AC 最大電流 | 100 V AC / 30 A、240 V AC / 20 A | |
| DC 電源 | -48 ～ -60 V DC | |
| DC 最大電流 | 25 ～ 32 A（x 2） | |
| 消費電力（平均 / 最大） | （977 / 1,217 W）/（977 / 1,237 W） | （1,308 / 1,548 W）/（1,328 / 1,568 W） |
| 放熱 | 4,153 / 4,221 BTU/h | 5,282 / 5,350 BTU/h |
| 冗長電源 | 2 + 1 冗長 / 1 + 1 冗長：ハイライン電源使用の場合、（ホットスワップ対応） | |
| **動作環境と準拠規格・認定** | | |
| 動作温度 | 0 ～ 40 ℃ | |
| 保管温度 | -35 ～ 70 ℃ | |
| 湿度 | 10 ～ 90%（結露しないこと） | |
| 騒音レベル | 57.43 dBA | |
| 動作高度 | 最高 2,250 m | |
| 準拠規格・認定 | FCC Part 15 Class A、RCM、VCCI、CE、UL / cUL、CB | |

# オプションアクセサリー

| アクセサリー名 | 型番 | 説明 |
|---|---|---|
| 100 GbE QSFP28 トランシーバモジュール、4 チャネルパラレルファイバー、ショートレンジ | FG-TRAN-QSFP28-SR4 | 100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots. |
| 100 GbE QSFP28 トランシーバモジュール、4 チャネルパラレルファイバー、ロングレンジ | FG-TRAN-QSFP28-LR4 | 100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots. |
| 40 GbE QSFP+ トランシーバモジュール、ショートレンジ | FG-TRAN-QSFP+SR | 40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots. |
| 40 GbE QSFP+ トランシーバモジュール、ショートレンジ BiDi | FG-TRAN-QSFP+SR-BIDI | 40 GE QSFP+ transceiver module, short range BiDi for all systems with QSFP+ slots. |
| 40 GbE QSFP+ トランシーバモジュール、ロングレンジ | FG-TRAN-QSFP+LR | 40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots. |
| 10 GbE/25 GbE SFP28トランシーバモジュール、ショートレンジ | FG-TRAN-SFP28-SR | 10 GE/25 GE SFP28 transceiver module, short range for all systems with SFP28 slots. |
| 25 GbE SFP28 トランシーバモジュール、ロングレンジ | FG-TRAN-SFP28-LR | 25 GE SFP28 transceiver module, long range for all systems with SFP28 slots. |
| 10 GbE SFP+ トランシーバモジュール、ショートレンジ | FG-TRAN-SFP+SR | 10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots. |
| 10 GbE SFP+ トランシーバモジュール、ロングレンジ | FG-TRAN-SFP+LR | 10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots. |
| 1 GbE SFP LX トランシーバモジュール | FG-TRAN-LX | 1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GbE SFP RJ45 トランシーバモジュール | FG-TRAN-GC | 1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1 GbE SFP SX トランシーバモジュール | FG-TRAN-SX | 1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 10 GBase-ER SFP+ トランシーバモジュール | FS-TRAN-SFP+ER | 10GBase-ER SFP+ transceiver module for FortiSwitch and FortiGate, 1550nm. Single Mode. 40km range for systems with SFP+ slots. |
| AC 電源 | FG-7040E-PS-AC | 1500 W AC power supply module for supported products. |

## 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の保護機能を簡単に最適化できます。

| 個別のサブスクリプションサービス | 360 Protection | Enterprise Protection | Unified Threat Protection | Threat Protection |
|---|---|---|---|---|
| FortiCare | ASE [1] | 24x7 | 24x7 | 24x7 |
| FortiGuard App Control Service | • | • | • | • |
| FortiGuard IPS Service | • | • | • | • |
| FortiGuard Advanced Malware Protection（AMP）— Antivirus、Mobile Malware、Botnet、CDR [2]、Virus Outbreak Protection [2]、FortiSandbox Cloud Service [3] | • | • | • | • |
| FortiGuard Web Filtering Service | • | • | • | |
| FortiGuard Antispam Service | • | • | • | |
| FortiGuard Security Rating Service [2] | • | • | | |
| FortiGuard Industrial Service | • | • | | |
| FortiGuard IoT Detection Service [5] | • | • | | |
| FortiConverter Service | • | • | | |
| IPAM Cloud [5] | • | | | |
| SD-WAN Orchestrator Entitlement [5] | • | | | |
| SD-WAN Cloud Assisted Monitoring [4] | • | | | |
| SD-WAN Overlay Controller VPN Service [4] | • | | | |
| FortiAnalyzer Cloud [4] | • | | | |
| FortiManager Cloud [4] | • | | | |

1. 24x7 とアドバンスサービス テクニカルサポートチケットに対応。2. FortiOS 6.0.0 以降を実行している場合に利用可能。
3. FortiOS 6.0.1 以降を実行している場合に利用可能。4. FortiOS 6.2 以降を実行している場合に利用可能。5. FortiOS 6.4 を実行している場合に利用可能。

FORTINET
フォーティネットジャパン株式会社

〒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

Copyright© 2021 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。