DATA SHEET

FortiGate 3100D

FortiGate 3100D、3100D-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 3100D シリーズは、インターネットまたはクラウドエッジに柔軟に導入でき、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コアや社内セグメントにおいて、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る FortiGate 3100D シリーズは、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。

高度なセキュリティ

- 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、未知と既知の攻撃を検知し阻止

優れたパフォーマンス

- 専用のセキュリティプロセッサ（SPU）テクノロジーにより、業界最高レベルの脅威保護パフォーマンスと超低遅延を実現
- SSL 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
- 第三者機関の NSS Labs から比類ない高評価を獲得

ネットワーク機能

- 高度なレイヤー 7 セキュリティおよび仮想ドメイン（VDOM）とシームレスに統合可能な先進のネットワーキング機能を提供し、幅広い導入展開の柔軟性、マルチテナントのサポート、リソースの効果的な利用を実現
- 高密度実装された高速インタフェースの柔軟な組み合わせにより、データセンターや WAN の導入展開に理想的な TCO を実現

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
- セキュリティ ファブリックの一元管理機能により、ゼロタッチ統合を可能に
- 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

ファイアウォール	IPS	NGFW	脅威保護	インタフェース
80 Gbps	22 Gbps	18 Gbps	13 Gbps	複数の10 GbE SFP+ | 複数の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）

- 脅威保護セキュリティ機能を単一の高性能ネットワークセキュリティアプライアンスに集約し、複雑さを軽減
- ポートやプロトコルを越えてネットワークトラフィックのアプリケーションを実際に検査する強力な侵入防止機能によって脅威を特定し、阻止
- 業界で義務付けられている暗号を使用して、業界最高クラスの SSL インスペクションパフォーマンスを提供し ROI を最大化
- 新たに発見された巧妙な攻撃を、リアルタイムの高度な脅威保護によってプロアクティブにブロック

セグメンテーション

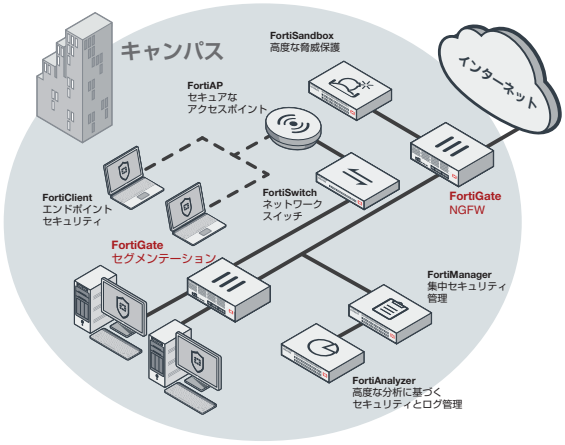
- インテント ベースト セグメンテーションにより、堅牢なセキュリティフレームワークの構築、プロアクティブなリスクの軽減、コストや複雑性の削減が可能
- セキュリティ ファブリックとのシームレスな統合でサードパーティ製ソリューションの活用や継続的な信頼性（トラスト）の評価が可能となり、巧妙な攻撃を阻止
- クリティカルなビジネスアプリケーションを保護し、ネットワークを再設計することなくあらゆるコンプライアンスの実装を支援

IPS

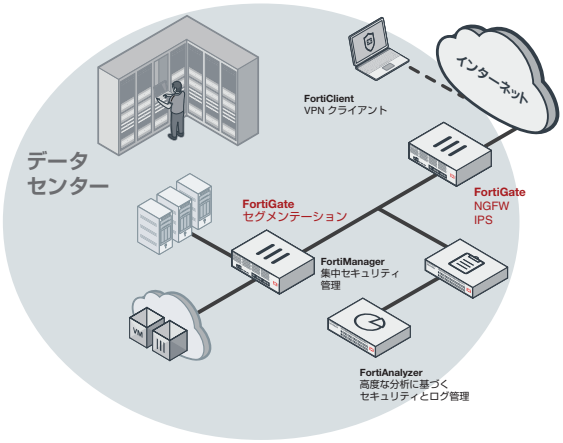
- パッチの適用が困難な IoT、ICS、SCADA などのシステムに対しても、未修正の脆弱性に対するコスト効率に優れた減災が可能
- 機密データを保護し、PCI、HIPPA、PII、GDPR などの幅広い法規制のコンプライアンスを実現
- 未知の脅威からの保護を可能にする、複数の検査エンジン、脅威インテリジェンスフィード、高度な脅威保護のオプションを用意
- ハイパフォーマンスの SSL インスペクションを活用する、クラストップレベルの不正侵入防止機能

4G、5G、IoT に理想的なモバイルセキュリティ

- 複数の SPU による SGi LAN セキュリティにより、ハイパフォーマンスの CGNAT が実現し IPv4 / IPv6 トラフィックを高速処理
- 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、Diameter、GTP-C、SIP をはじめとする幅広いプロトコルのインスペクションを実行し、攻撃に対する保護を実現するシグナリングセキュリティ
- 柔軟な導入展開を支援する高速インタフェースを装備



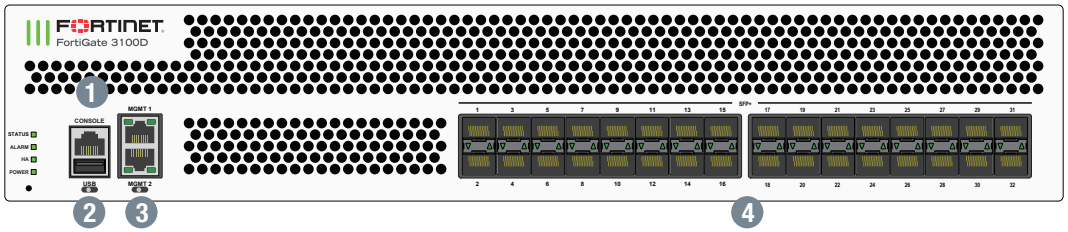
FortiGate 3100D の大規模なキャンパスへの導入例（NGFW、インテント ベースト セグメンテーション）

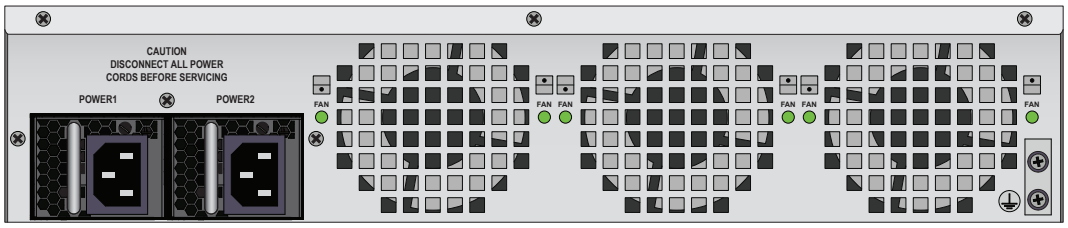


FortiGate 3100Dのデータセンターへの導入例（IPS / NGFW、インテント ベースト セグメンテーション）

ハードウェア

FortiGate 3100D / 3100D-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（クライアント）
3. 2 x GbE R45 管理インタフェース
4. 32 x 10 GbE SFP+ / GbE SFP 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、最新の脅威を阻止し、第三者による厳格な認証要件を満たし、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ることがないようにする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 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、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

SPU CP8 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、高速な暗号処理および次のコンテンツ検査サービスを提供します。

- シグネチャベースのコンテンツ検査アクセラレーション
- 暗号化 / 復号のオフロード

10 GbE の高速接続

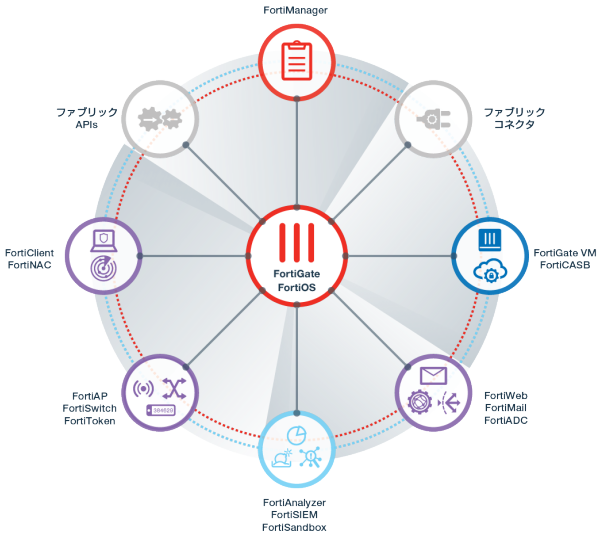
データネットワークのコアにおけるネットワークセキュリティのセグメント化では、高速での接続が不可欠です。FortiGate 3100D は、市場でトップレベルの 10 GbE インタフェースの高密度実装を実現しており、デバイスを追加することなくブリッジ接続ができ、シンプルなネットワークデザインが可能です。

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

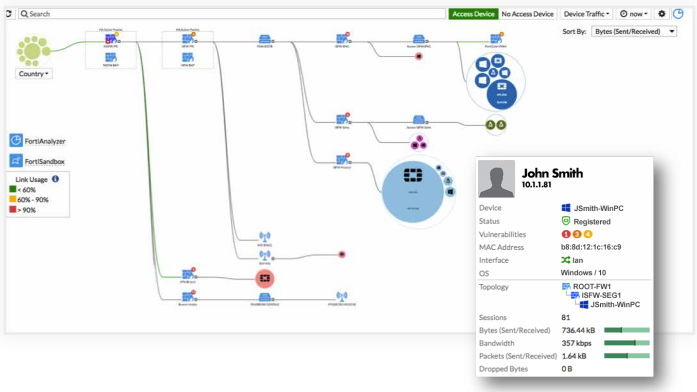
フォーティネット セキュリティ ファブリックは、広範なネットワークの可視化、AI の活用による統合的なセキュリティ侵害の防止、そしてすべてのフォーティネット製品とそのエコシステム環境の運用、オーケストレーション、レスポンスの自動化を実現します。セキュリティ ファブリックにより、ワークロードやデータの増加に合わせたセキュリティの動的な拡張や変更が可能になります。また、ネットワーク上の IoT、デバイス、およびクラウド環境を行き来するデータ、ユーザー、およびアプリケーションをシームレスに追跡して保護します。これらすべての機能は一元管理のもと緊密に統合され、お客様の環境全体に最先端のセキュリティ機能を提供し、複雑さを大幅に軽減します。

セキュリティ ファブリックの基盤となる FortiGate は、他のフォーティネットのセキュリティ製品やソリューション、そしてファブリック・レディ パートナーソリューションとの緊密な統合による詳細な可視化と制御を実現し、セキュリティをさらに拡張します。



FortiOS

直感的な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。複雑さの軽減、運用経費の削減、応答時間の短縮を可能にする次世代セキュリティプラットフォームが実現します。



- 真の統合セキュリティプラットフォームにより、すべての FortiGate プラットフォームのあらゆるセキュリティおよびネットワークサービスが 1 つの OS で一元制御できます。
- 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といった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。
- インテント ベースト セグメンテーションや、ルーティング、スイッチング、SD-WAN など多様なネットワーキング機能を提供し、企業のあらゆるニーズに対応します。
- SPU ハードウェアアクセラレーションを活用して、セキュリティ性能を強化します。

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 3100D / 3100D-DC
インタフェースとモジュール	
10 GbE SFP+ / GbE SFP インタフェース	32
GbE RJ45 管理インタフェース	2
USB インタフェース（A 端子 / B 端子）	1 / 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	1x 480 GB SSD
付属トランシーバ	2 x SFP+（SR 10 GbE）
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]	22 Gbps
NGFW スループット [1, 2]	18 Gbps
脅威保護スループット [1, 3]	13 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）	80 / 80 / 50 Gbps
IPv6 ファイアウォールスループット （1518 / 512 / 86 バイト UDP パケット）	80 / 80 / 50 Gbps
ファイアウォールレイテンシ （64 バイト UDP パケット）	3 μ s
ファイアウォールスループット（パケット / 秒）	75 M pps
ファイアウォール同時セッション（TCP）	50 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	200,000
IPSec VPN スループット （512 バイト UDP パケット）[4]	50 Gbps
ゲートウェイ間 IPSec VPN トンネル	40,000
クライアント - ゲートウェイ間 IPSec VPN トンネル	200,000
SSL-VPN スループット	8 Gbps
同時 SSL-VPN ユーザー （推奨最大値、トンネルモード）	30,000
SSL インスペクションスループット （IPS、avg. HTTPS）[5]	16 Gbps
SSL インスペクション CPS （IPS、avg. HTTPS）[5]	10,000
SSL インスペクション同時セッション （IPS、avg. HTTPS）[5]	3.5 M
アプリケーション制御スループット （HTTP 64 K）[1]	40 Gbps
CAPWAP クリアテキストスループット （1444 バイト UDP パケット）	22 Gbps
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）	4,096 / 1,024
FortiToken サポート数	20,000
FortiClient サポート数	50,000
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 3100D / 3100D-DC
ハードウェア仕様	
高さ x 幅 x 奥行	88 x 442 x 555 mm
重量	17.1 kg
形状	ラックマウント（2 RU）
AC 電源	100 ～ 240 V AC、50 ～ 60 Hz
DC 電源（FortiGate 3100D-DC）	40.5 ～ 57 V DC
消費電力（平均 / 最大）	337 W / 520 W
放熱	1,775 BTU/h
冗長電源	○ （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	50 dBA
動作高度	最高 2,250 m
準拠規格	FCC Part 15 Class A、C-Tick、 VCCI、CE、UL/cUL、CB
認定	ICSA Labs 認定：ファイアウォール、 IPSec、IPS、アンチウイルス、 SSL VPN、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. 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。

技術仕様

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	UTM 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	•	•		
FortiCASB SaaS-only Service	•	•		
FortiConverter Service	•			
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。

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