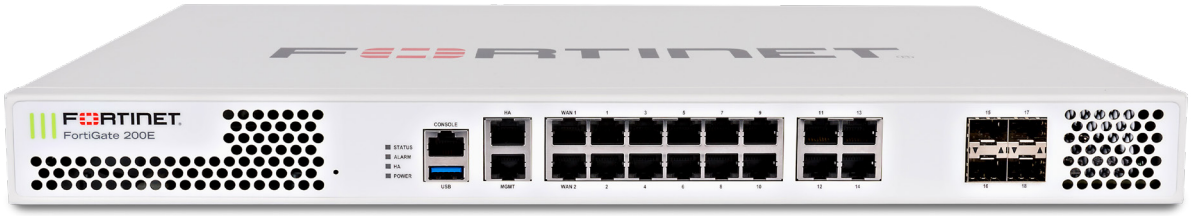
FortiGate 200E シリーズ

FortiGate 200E、201E



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

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 200E シリーズ次世代ファイアウォールは、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 200E 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。

ユニバーサル ZTNA は、アプリケーションへのユーザーアクセスの自動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 インスペクションにより、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
2.2 Gbps	1.8 Gbps	1.2 Gbps	複数の GbE RJ45、GbE SFP

Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hils, 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助言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。

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キング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ア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とユースケースを簡素化された単一のポリシーおよび管理フレームワークに統合することができます。有機的に構築されたトップクラスの機能に統一されたオペレーティングシステムと圧倒的なスケーラビリティが加わることで、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

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ユースケースに対応します。データ漏洩防止（DLP）で構成されているため、ネットワーク、クラウド、ユーザーのデータの可視性、管理、保護（データの持ち出しのブロックを含む）を可能にしつつ、コンプライアンスとプライバシーの実装の簡素化を実現します。別サービスであるインラインクラウドアクセスセキュリティブローカー（CASB）は、移動データ、保存データ、クラウド内のデータを保護します。このサービスは、主要コンプライアンス標準を適用し、アカウント、ユーザー、クラウドアプリケーション使用状況を管理します。お客様の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機能も含まれています。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 脆弱性相関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

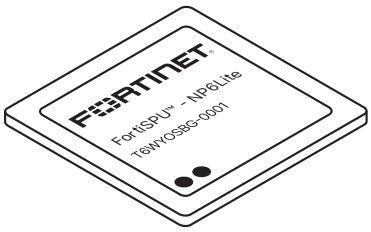
OT 検知、OT 脆弱性の相関付け、仮想パッチ、OT シグネチャ、業界に特化したプロトコルデコーダを提供し、OT 環境とデバイスの包括的で堅牢な防御を可能にします。

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

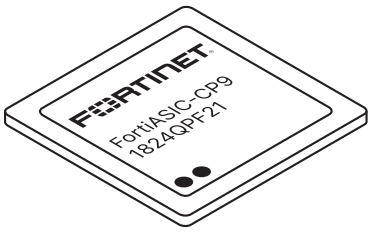
従来型のファイアウォールは、市販のハードウェアや汎用 CPU に依存しているため、危険なパフォーマンスギャップが発生し、今日のコンテンツベース / 接続ベースの脅威から企業を保護することはできません。フォーティネット独自の SPU プロセッサは、最大 520 Gbps の処理能力を提供することで、新たな脅威の検知と不正コンテンツのブロックを可能にしつつ、ネットワークセキュリティソリューションがパフォーマンスボトルネックにならないようにします。

ASIC の優位性

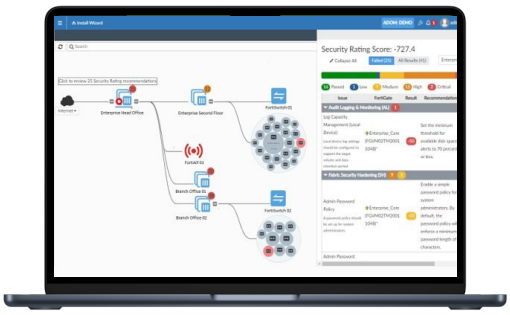


ネットワークプロセッサ 6Lite（NP6Lite）
SPU NP6Lite ネットワークプロセッサは、インラインで動作し、ファイアウォールおよび VPN の各機能と次の優れた性能を発揮します。

- すべてのパケットサイズにおけるワイヤスピードに近いファイアウォールパフォーマンス
- VPN 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（CP9）
フォーティネット独自の第 9 世代 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、高速な検査を提供します。



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

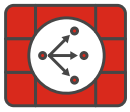
ネットワークとセキュリティのスケーラブルで一元的な管理

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

次世代ファイアウォール（NGFW）

- FortiGuard Labs の AI を活用した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、Work From Anywhere（場所に縛られない働き方）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

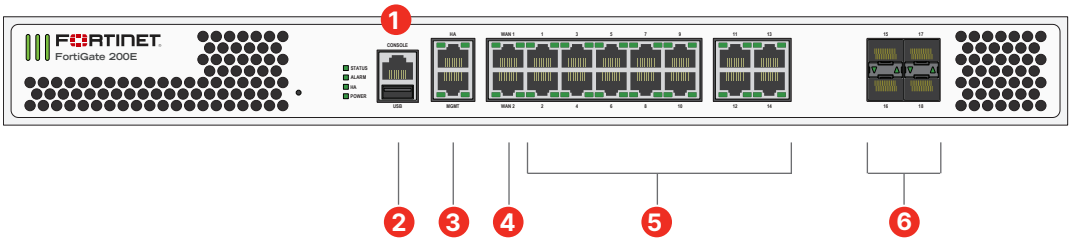
- あらゆる場所のユーザーによるあらゆる場所でホスティングされるアプリケーションへのアクセスを制御することで、アクセスポリシーの統一された適用を実現
- アプリケーションへのアクセスを許可する前に、広範な認証、チェック、ポリシーの適用を常に実行
- FortiClient によるエージェントベースのアクセス、またはゲストや BYOD 向けのプロキシポータル経由のエージェントレスアクセスが可能

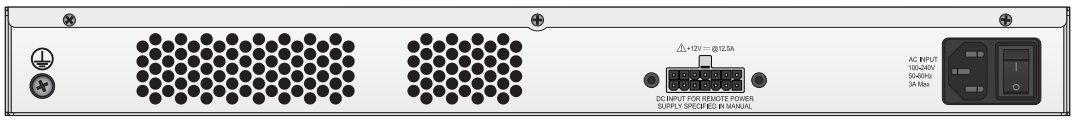
セグメンテーション

- 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

ハードウェア

FortiGate 200E シリーズ





インタフェース

1. 1 × 管理コンソールポート
2. 1 × USB ポート
3. 2 × GbE RJ45 管理 / HA ポート
4. 2 × GbE RJ45 WAN ポート
5. 14 × GbE RJ45 ポート
6. 4 × GbE SFP ポート

ハードウェアの特長

技術仕様

	FortiGate 200E	FortiGate 201E
ハードウェア仕様		
GbE RJ45 WAN インタフェース	2	
GbE RJ45 管理 / HA ポート	2	
GbE RJ45 ポート	14	
GbE SFP ポート	4	
USB ポート	1	
RJ45 管理コンソールポート	1	
ストレージ	—	1 × 480 GB SSD
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]	2.2 Gbps	
NGFW スループット [2、4]	1.8 Gbps	
脅威保護スループット [2、5]	1.2 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）	20 / 20 / 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 µs	
ファイアウォールスループット（パケット / 秒）	13.5 Mpps	
ファイアウォール同時セッション（TCP）	2 M	
ファイアウォール新規セッション / 秒（TCP）	135,000	
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]	7.2 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	10,000	
SSL-VPN スループット	900 Mbps	
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]	820 Mbps	
SSL インスペクション CPS（IPS、avg. HTTPS）[3]	1,000	
SSL インスペクション同時セッション（IPS、avg. HTTPS）[3]	240,000	
アプリケーション制御スループット（HTTP 64 K）[2]	3.5 Gbps	
CAPWAP スループット（1444 バイト UDP パケット）	1.5 Gbps	
仮想 UTM（VDOM：標準 / 最大）	10 / 10	
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 200E	FortiGate 201E
サイズ / 電源		
高さ × 幅 × 奥行	44.45 × 432 × 301 mm	
重量	5.4 kg	5.5 kg
形状	1 RU（EIA 規格およびその他の 19 インチラック適合）	
電源入力	100 ～ 240 V AC、50 ～ 60 Hz	
最大電流	110 V / 3 A、220 V / 0.42 A	
消費電力（平均 / 最大）	70.98 W / 109.9 W	
放熱	374.9 BTU/h	
冗長電源（ホットスワップ対応）	—	
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	10 ～ 90%（結露しないこと）	
騒音レベル	31.1 dBA	
エアフロー	側面 ～ 背面	
動作高度	最高 2,250 m	
準拠規格・認定	FCC Part 15B、Class A、CE、RCM、VCCI、UL/cUL、CB、BSMI	
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。

オーダー情報

Product	SKU	Description
FortiGate 200E	FG-200E	18x GE RJ45 (including 2x WAN ports, 1x Mgmt port, 1x HA port, 14x switch ports), 4x GE SFP slots. SPU NP6Lite and CP9 hardware accelerated.
FortiGate 201E	FG-201E	18x GE RJ45 (including 2x WAN ports, 1x Mgmt port, 1x HA port, 14x switch ports), 4x GE SFP slots, SPU NP6Lite and CP9 hardware accelerated, 480 GB onboard SSD storage.
Optional Accessories		
1 GE SFP LX transceiver module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
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.

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 Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus、Mobile Malware、Botnet、CDR、Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL、DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection、OT Vulnerability correlation、Virtual Patching、OT Signature / Protocol Decoders) [1]	•			
	Application Control		FortiCare サブスクリプションに含まれています。		
	CASB SaaS Control		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 Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC / SOC サービス	FortiGuard Attack Surface Security Service (IoT Detection、IoT Vulnerability Correlation、Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
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	Internet Service (SaaS) DB Updates	FortiCare サブスクリプションに含まれています。			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

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

FortiGuard バンドル

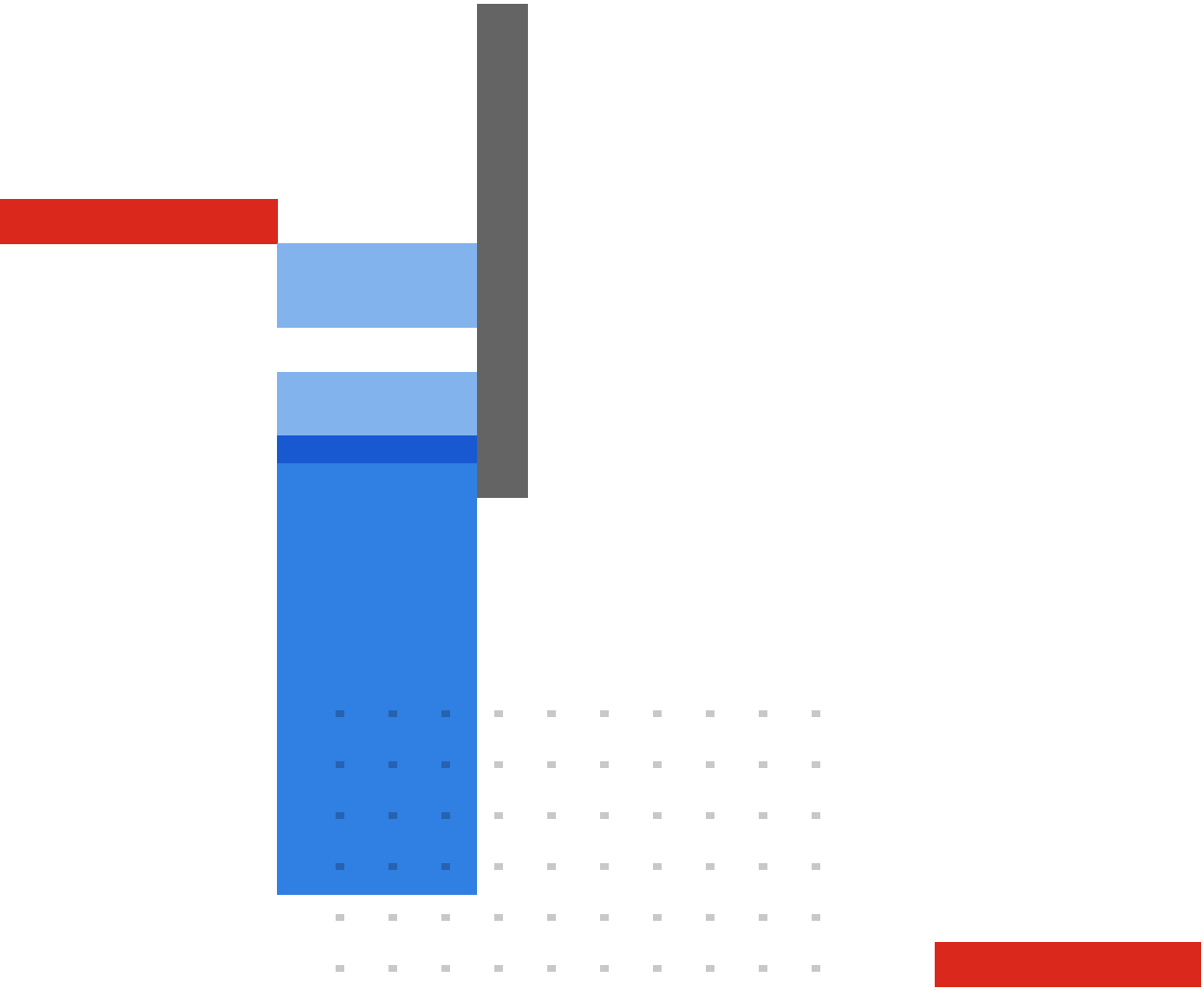
FortiGuard Labs は、FortiGate ファイアウォールプラットフォームと併せてご利用いただける、多数のセキュリティインテリジェンスサービスを提供しています。最適な Protection をお選びいただくことで、FortiGate の保護機能を容易に最適化できます。

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。

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

販売代理店
図研ネットウエイブ株式会社
本社 〒222-8505 神奈川県横浜市港北区新横浜3-1-1
TEL : 045-470-5303 FAX : 045-473-1782
中日本営業所 〒460-0003 愛知県名古屋市中区錦2-4-15 ORE錦二丁目ビル6
TEL : 052-218-5415
西日本支店 〒530-0002 大阪市北区曽根崎新地1-4-20 桜橋IMビル8F
TEL : 06-6450-0860
MAIL : ft-info@znw.co.jp URL : https://www.znw.co.jp

DS-FG-200E-R33-202403-R1