

FortiGate-VM on Amazon Web Services

次世代ファイアウォール
VPN ゲートウェイ



フォーティネットの FortiGate-VM on AWS は、あらゆる規模の組織向けに次世代ファイアウォール機能を提供します。次世代ファイアウォールやVPNゲートウェイとして展開可能な最適な柔軟性も備えています。ハイパフォーマンス、セキュリティの有効性、詳細な可視性により、巧妙なサイバー脅威からお客様を保護します。

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、未知と既知の攻撃を検知し阻止
- AWS GuardDuty 脅威検知サービスがインシデント対応を自動化し、脅威インテリジェンスを提供

パフォーマンス

- 専用設計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
- 第三者機関によるテストで比類ない高評価を獲得
- AWS セキュリティコンピテンシーパートナー

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 (VDM) とシームレスに統合可能な先進のネットワーク機能を提供し、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 (BYOL のみ VDM をサポート)
- 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
- AWS ヘルスチェックを使用した高可用性を実現する設計

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
- 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、総合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
- セキュリティ対策をお使いの EC2 にマッピングし、スケールアップ/ダウン

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



FortiManager



FortiAnalyzer



FortiSandbox



FortiAuthenticator



FortiSIEM



FortiWeb



FortiMail

フォーティネットの包括的なセキュリティ仮想アプライアンスのラインナップは、AWS に対応しています

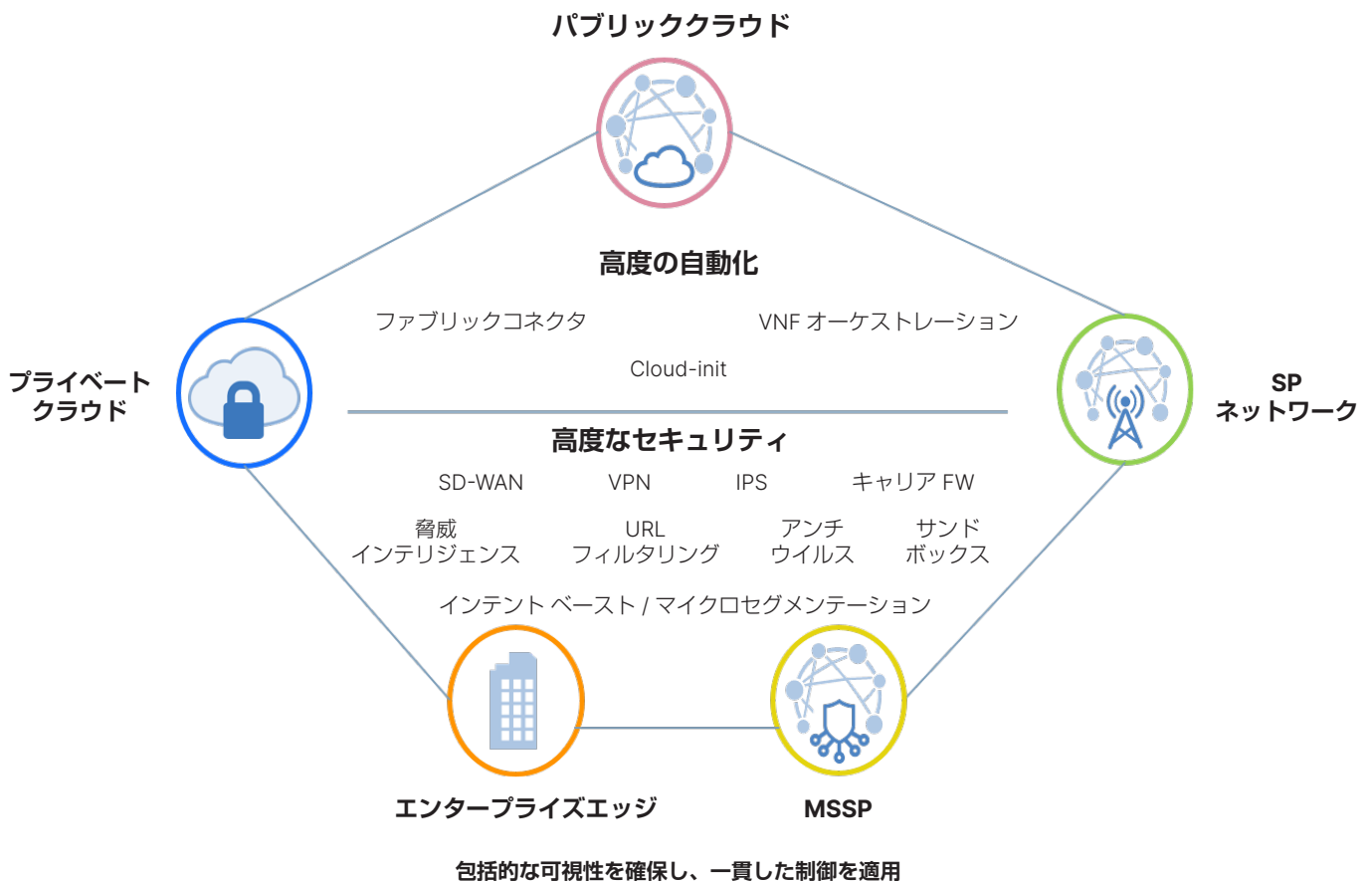
導入例

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спек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

VPNゲートウェイ

- ご利用中の AWS VPC へ、および AWS VPC からの SSL / IPSec VPN 接続に FortiGate ファイアウォールを使用
- VGW から VPC 間の FortiGate VPN
- ハイブリッドクラウドのサイト間 IPsec VPN
- リモートアクセス VPN



AWS との統合

- フォーティネットは、最新の AWS Auto Scaling 機能と FortiGate CloudFormation テンプレートの構成をクラウドセキュリティ ファブリックに組み込み、クラウドワークロードのリソース需要に合わせたセキュリティの自動化を実現しています。
- AWS GuardDuty が検知した新たな脅威に対する保護に要する時間を、悪意のある IP / DNS アドレスを動的な FortiGate のポリシーに自動反映させるネイティブの AWS スクリプトを配備することで短縮します。
- AWS ネイティブロードバランサーによりサービスの復元力を提供します。

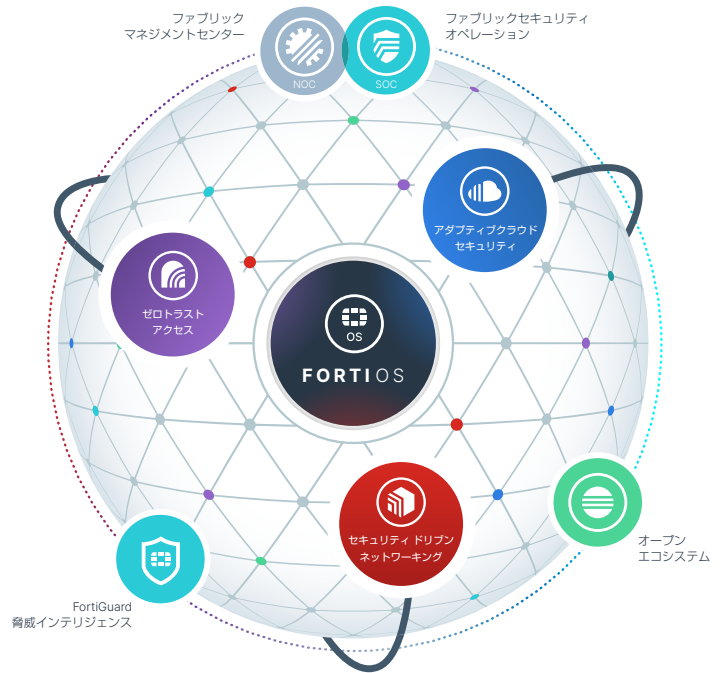
フォーティネット セキュリティ ファブリック

セキュリティ ファブリック

FortiOS を搭載し、業界最高レベルの性能を誇るサイバーセキュリティプラットフォームに、拡大するデジタル攻撃対象領域の保護を前提に設計されたエコシステムが加わることで、完全に自動化された自己修復型ネットワークセキュリティが実現します。

- **Broad (幅広い)**: エッジ、クラウド、エンドポイント、ユーザーを含むデジタル攻撃対象領域でネットワークとセキュリティのコンバージェンスを可能にすることで、協調型の検知と適用を実現
- **Integrated (統合化)**: 異なるテクノロジー、場所、導入オプションを統合し、最も広範なエコシステムを活用して、統一されたセキュリティ、オペレーション、パフォーマンスを実現
- **Automated (自動化)**: クラウドのスケラビリティと高度な AI を活用したコンテキスト対応の自己修復型ネットワーク / セキュリティ態勢により、ユーザーとアプリケーションを連携させた保護をほぼリアルタイムかつ自動的に提供

フォーティネット セキュリティ ファブリックは、ハイブリッドインフラストラクチャの保護と簡素化を可能にし、あらゆる規模の組織のデジタルイノベーションを支援します。



FortiOS オペレーティングシステム

フォーティネットの業界をリードするオペレーティングシステムである 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高性能ネットワークとセキュリティのコンバージェンスを可能にし、ネットワークエンドポイントとクラウドで一貫したコンテキスト対応セキュリティ態勢を実現します。組織的に構築されたトップクラスの機能と統一されたアプローチにより、パフォーマンスや保護に妥協を強いられることなくビジネスを遂行できるようになり、シームレスなスケラビリティのサポートと革新的なテクノロジーの容易な利用が可能になります。

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 サービス

フォーティネットはお客様の支援に全力で取り組んでいます。FortiCare サービスは、毎年数千社の組織に利用されており、セキュリティ ファブリックソリューションを最大限に有効活用する一助となっています。1,000 人以上のエキスパートが在籍し、テクノロジーの迅速な実装の支援、高度で信頼できるサポート、フォーティネット導入環境のセキュリティとパフォーマンスを最大化するためのプロアクティブなサービスを提供します。



ライセンス

FortiGate-VM for AWSは、オンデマンドのPAYG(Pay-As-You-Go)モデルやBYOL(Bring-Your-Own-License)モデルにより、さまざまなプライベート/パブリッククラウド環境を幅広い導入方法でサポートします。

オンデマンドライセンスは、非常に柔軟なオプションであり、新しい導入環境と必要に応じて成長する環境のいずれにも適しています。幅広いインスタンスタイプがサポートされるため、あらゆるユースケースにも対応できます。このライセンスでは、UTPバンドルでFortiOSが提供されます。

BYOLモデルは、既存のプライベートクラウド環境をパブリッククラウド環境へと移行するユースケースに最適です。既存のライセンスを使用する場合には、追加コストのみでAWSインスタンスを使用できます。

技術仕様

FortiGate-VMは、AWS GovCloudとAWS Chinaを含むすべての地域で購入いただけます。

BYOLライセンスのシステム要件は次のとおりです。

	VM-01/01V/01S	VM-02/02V/02S	VM-04/04V/04S	VM-08/08V/08S	VM-16/16V/16S	VM-32/32V/32S	VM-UL/ULV/ULS
システム要件							
仮想 CPU 数 (最小 / 最大)	1 / 1	1 / 2	1 / 4	1 / 8	1 / 16	1 / 32	1 / 無制限
技術仕様							
仮想 NIC 枚数 (最小 / 最大) ¹	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24
仮想 UTM (VDOM: 標準 / 最大) ²	10 / 10	10 / 25	10 / 50	10 / 500	10 / 500	10 / 500	10 / 500
ファイアウォールポリシー	10,000	10,000	200,000	200,000	200,000	200,000	200,000
システム性能							
		ENA Driver ○	ENA Driver ○	ENA Driver ○	ENA Driver ○	ENA Driver ○	ENA Driver ○
測定するインスタンス		C5n.large	C5n.xlarge	C5n.2xlarge	C5n.4xlarge	C5n.9xlarge	
AWS 帯域幅 ³		最大 25 Gbps	最大 25 Gbps	最大 25 Gbps	最大 25 Gbps	50 Gbps	
ファイアウォールスループット (UDP パケット) (Mbps)		6,200	20,000	21,000	22,500	39,000	
ファイアウォール新規セッション / 秒 (TCP)		92,000	210,000	225,000	300,000	330,000	
IPS スループット (Mbps) ⁴		9,000	13,000	13,150	16,850	27,000	
IPS HTTP 1M (Mbps) ⁴		9,000	13,150	13,200	16,950	27,500	
SSL インспекションスループット (Mbps) ⁵		645	1,365	2,900	6,220	14,005	
アプリケーション制御スループット (Mbps) ⁶		8,400	13,200	13,300	17,000	27,400	
NGFW スループット ⁷		1,100	2,100	4,000	4,850	7,700	
脅威保護スループット ⁸		950	1,800	3,750	4,500	7,670	
IPSec VPN スループット (SHA2-256) (1518 バイト UDP)		1,600	1,960	3,300	3,400	16,500	

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。実際の性能は、ネットワークとシステム構成によって異なります。なお、これらの指標は、内部で実施するテストにより製品性能が向上しているため、定期的に更新されます。また資料のバージョンにより、性能値の相違が指摘される場合があるため、必ず最新のデータシートを参照してください。
VM-32の性能指標: FortiOS 6.4.4を実行し、FortiGate-VM BYOL 32 CPUライセンスを使用した場合。
その他の性能指標: FortiOS v6.2.1を実行し、FortiGate-VM BYOL インスタンスを使用した場合。SSL インспекション値は、FortiOS v6.4.2を実行した場合。

- 6.4.0以降を実行している場合。実際に使用可能なネットワークインタフェース数は、AWS インスタンスの種類やサイズによって異なり、少ない場合があります。
- FG-VMxxV および FG-VMxxS シリーズでは VDOM (仮想ドメイン) が標準で付属しな

いため、追加購入が必要です。別途 VDOM 追加永久ライセンスを適用することで追加できます。

- AWS 帯域幅に関する最新情報は、<https://aws.amazon.com/ec2/instance-types/> をご参照ください。
- IPS パフォーマンスは、エンタープライズトラフィック混合および 1M バイト HTML ファイルを用いて測定されています。
- TLS ECDHE RSA - AES 256 GCM SHA384 (2K) を使用しています。
- アプリケーション制御パフォーマンスは、64K バイト HTML ファイルのトラフィックを用いて測定されています。
- NGFW パフォーマンスは、IPS およびアプリケーション制御有効、エンタープライズトラフィック混合の状態のトラフィックを用いて測定されています。
- 脅威保護パフォーマンスは、IPS、アプリケーション制御、およびマルウェア保護有効、エンタープライズトラフィック混合の状態のトラフィックを用いて測定されています。



サイジングガイドについては、www.fortinet.com で公開されているサイジングドキュメントを参照してください。

バンドル



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	Advanced Threat Protection
FortiCare	ASE ¹	24×7	24×7	24×7
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 and Video ⁶ Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service ²	•	•	•	
FortiGuard IoT Detection Service ⁵	•	•		
FortiGuard Industrial Service	•	•		
FortiConverter Service	•	•		
SD-WAN Orchestrator Entitlement ⁵	•			
SD-WAN Cloud Assisted Monitoring ⁴	•			
SD-WAN Overlay Controller VPN Service ⁴	•			
Fortinet SOCaaS	•			
FortiAnalyzer Cloud ⁴	•			
FortiManager Cloud ⁴	•			

1. 24×7 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。6. FortiOS 7.0 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