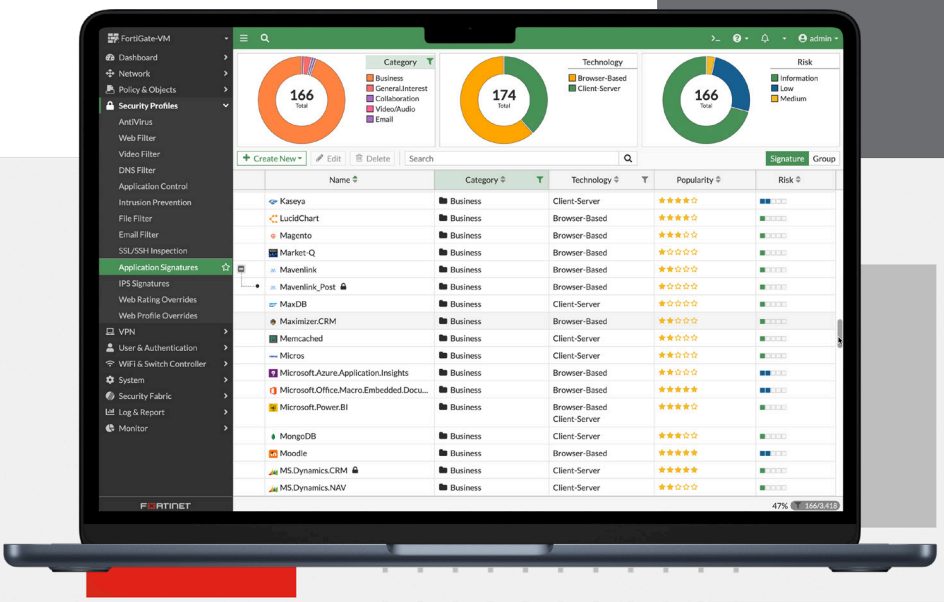
FortiGate-VM on Microsoft Azure



ハイライト

- パフォーマンスのボトルネックになることなく、アプリケーションワークロードへの安全な接続を実現
- セキュリティを低下させることなく、クラウドのスピードでの移行が可能
- 運用の負担を増加することなく、クラウド保護をシームレスに拡張
- 柔軟な消費モデルにより、ビジネス成果に影響することなく、クラウドトランスフォーメーションを安全に実現

AI を活用した高度な脅威保護による アダプティブマルチクラウドセキュリティ

フォーティネットの FortiGate-VM on Microsoft Azure 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。

FortiGate-VM は、ネットワークセキュリティのさまざまな脅威からの保護を可能にします。FortiOS オペレーティングシステムと同じセキュリティとネットワークのサービスをパブリッククラウド、プライベートクラウド、通信事業者向けクラウド（VNF）でも利用でき、共通の運用モデルをハイブリッドクラウド、マルチクラウド、サービスプロバイダーの環境で利用できるため、セキュリティチームのトレーニングの負担が軽減されます。

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、ZTNA の統合など、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。

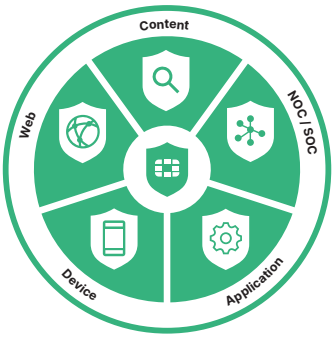
- ドリルダウンとトポロジのインタラクティブビューで、リアルタイムにステータスを表示
- ワンクリックで改善を実行する機能により、脅威と悪用からの保護を正確かつ迅速に実現
- 独自の脅威スコアシステムで重み付けされた脅威をユーザーに相関させ、優先度を提示

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

FortiGuard AI 活用セキュリティ

FortiGuard の豊富なセキュリティサービスは、FortiGuard Labs のセキュリティ脅威のリサーチャー、エンジニア、フォレンジックのスペシャリストが設計した、AI を活用した協調型の保護を使用することで、脅威からのリアルタイムの保護を可能にします。

Web セキュリティ

URL、DNS（ドメインネームシステム）、ビデオの高度なフィルタリングをクラウドから提供することで、フィッシングやその他の Web 経由の攻撃の完全防御を実現しつつ、コンプライアンスの達成を支援します。

さらには、動的インライン CASB（クラウドアクセスセキュリティブローカー）サービスが、ビジネス SaaS データの保護を強力に支援し、インライン ZTNA トラフィックインスペクションと ZTNA ポスチャチェック、アプリケーションへのセッション単位のアクセス制御を提供します。FortiClient ファブリックエージェントと統合することで、リモートやモバイルのユーザーまで保護が拡張されます。

コンテンツセキュリティ

高度なコンテンツセキュリティテクノロジーにより、既知および未知の脅威やファイルベースの攻撃戦術のリアルタイムの検知と防御を可能にします。CPRL（Compact Pattern Recognition Language）、アンチウイルス、インラインサンドボックス、ラテラルムーブメント保護などの機能が加わることで、ランサムウェア、マルウェア、認証情報ベース攻撃からの保護など、完全なソリューションが実現します。

デバイスセキュリティ

高度なセキュリティテクノロジーを、IT、IoT、OT（オペレーショナルテクノロジー）デバイスの監視と脆弱性やデバイスベースの攻撃戦術からの保護を前提に最適化することで、ほぼリアルタイムの検証済み IPS インテリジェンスによる既知およびゼロデイの脅威の検知とブロックを可能にし、ICS / OT / SCADA プロトコルの細部に至る可視性と制御を実現し、自動検知、セグメンテーション、パターン識別ベースのポリシーを提供します。

SOC / NOC 向けの先進ツール

NGFW に搭載される NOC / SOC 管理の先進ツールを利用することで、シンプルかつ迅速なアクティベーションが可能になります。

SOCaaS（SOC-as-a-Service）

Tier1 ハンティングと自動化、ログロケーション、24 時間 365 日の SOC アナリストエキスパートに加えて、管理対象のファイアウォールとエンドポイントの機能とアラートのトリアージを提供します。

ファブリックレーティングセキュリティのベストプラクティス

サプライチェーンの仮想パッチに加えて、最新のリスクや脆弱性のデータも利用することで、迅速なビジネスの意思決定とデータ侵害時の修復を可能にします。

あらゆるエッジに対して規模を問わず保護

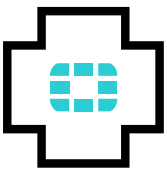
高度仮想セキュリティプロセッシングユニット（vSPU）

仮想ファイアウォールをソフトウェア制御によるデータセンターやマルチクラウド環境の仮想化環境を保護する目的で一般的に使用する理由は、最も低コストかつ最もポータブルで、クラウドからクラウドへと簡単に移動できるといった長所があるためです。また、ほとんどの仮想ファイアウォールの欠点は、物理ファイアウォールに比べてネットワークスループットが大幅に低下するために、ネットワーク全体でボトルネックが発生し、ビジネスの俊敏性とパフォーマンスが低下することです。

vSPU（高度仮想セキュリティプロセッシングユニット）を搭載する FortiGate VM（FortiGate 仮想ファイアウォール）は、このようなスループットの課題を解消し、プライベートクラウドやパブリッククラウドで最高のパフォーマンスを実現します。FortiGate VM を使用することで、あらゆるアプリケーションの安全な移行とクラウドでの高可用性大規模 VPN（仮想プライベートネットワーク）などのさまざまなユースケースのサポートが可能になります。

FortiGate VM は、業界をリードする多くの機能により、仮想 NGFW の採用にあたってのコストパフォーマンスの課題を解消します。

- FortiGate VM vSPU は、パケット処理の一部をユーザー空間にオフロードしつつ、オペレーティングシステムの内部でカーネルバイパスソリューションを使用することで、パフォーマンスを向上させる独自のテクノロジーです。vSPU を有効にすることで、FortiGate-VM の UDP ファイアウォールルールの 3 倍以上のスループットの向上が可能になります。
- 最新の QuickAssist アダプターで動作する Intel QuickAssist テクノロジー（Intel QAT）のサポートにより、サイト間 IPSec VPN 経由のトラフィック処理のアクセラレーションが実現します。QAT を有効にすることで、パケットフレームサイズによって異なるものの、FortiGate VM の 2 ～ 3 倍のスループットの向上が可能になります。



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。フォーティネットのライフサイクルポートフォリオは、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。運用サービスは、デバイスレベルの FortiCare Elite サービスを高い SLA で提供することで、お客様の運用や可用性のニーズに対応します。さらには、カスタマイズされたアカウントレベルのサービスにより、迅速なインシデント解決とプロアクティブケアを提供し、フォーティネットの導入環境のセキュリティとパフォーマンスを最大限に向上させます。

導入例

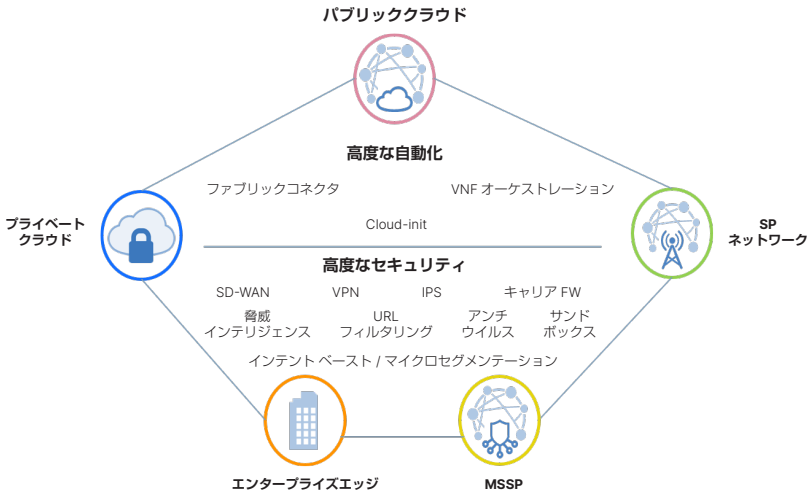
次世代ファイアウォール（NGFW）

- 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化を使用して、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

VPN ゲートウェイ

- VGW から VPC 間の FortiGate VPN
- ハイブリットクラウドのサイト間 IPsec VPN
- リモートアクセス VPN

包括的な可視性を確保し、一貫した制御を適用



Azure との統合

FortiOS には最新のオートスケール機能が組み込まれており、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。

Azure ロードバランシングと 2 つの FortiGate-VM を使用することにより、中断を最小限に抑えながら、最も効果的なシステムとアプリケーションのアップタイムを実現するため、容易で一貫性のある展開を保証するように設計されています。

FortiOS は Azure Traffic Manager と連携し、拡張性を確保するとともに、低遅延の顧客向けローカルアクセスを提供します。

ライセンス

FortiGate-VM for Microsoft Azure 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 Microsoft Azure インスタンスを使用できます。

Azure Government、Azure Germany、Azure China などの Azure リージョンに FortiGate-VM を導入でき、FortiGate-VM は、Azure Stack もサポートしています（BYOL のみ）。

技術仕様

FortiGate-VM は、Intel および AMD ベースの x64 プロセッサを活用した複数のインスタンスファミリーに加え、Ampere® Altra® Arm ベースのプロセッサを活用した ARM64 インスタンスファミリーをサポートしています。

サポートされているインスタンスファミリーの全リストは、「Azure Administration Guide: Instance type Support」を参照してください。

以下は、BYOL ライセンスタイプの x64（Standard DSv2 および Dsv3）インスタンスファミリーのパフォーマンスを示しています。

技術仕様

	VM-01/01V/01S	VM-02/02V/02S			VM-04/04V/04S			
システム要件								
仮想 CPU 数（最小 / 最大）	1 / 1	1 / 2			1 / 4			
技術仕様								
仮想 NIC 枚数（最小 / 最大）[1]	1 / 24	1 / 24			1 / 24			
仮想ドメイン：VDOM（標準 / 最大）[2]	10 / 10	10 / 25			10 / 50			
ファイアウォールポリシー	10,000	10,000			200,000			
システム性能		高速ネットワーク オフ		高速ネットワーク オン		高速ネットワーク オフ		高速ネットワーク オン	
測定するインスタンス		DS2_v2（2vCPU）				D4s_v3（4vCPU）			
Azure 想定帯域幅 [3]		1,500 Mbps				2,000 Mbps			
		スタンドアロン	IPsec	スタンドアロン	IPsec	スタンドアロン	IPsec	スタンドアロン	IPsec
ファイアウォールスループット（UDP パケット）（Mbps）- 1280 バイト		1,200	1,300	1,600	1,600	1,350	1,250	2,150	1,800
ファイアウォールスループット（UDP パケット）（Mbps）- 512 バイト		500	550	1,600	1,250	560	500	2,140	1,200
ファイアウォールスループット（UDP パケット）（Mbps）- 64 バイト		80	80	750	250	80	80	1,000	230
ファイアウォール新規セッション / 秒（TCP）		6,000	—	4,500	—	6,000	—	4,600	—
HTTP スループット（アプリケーションプロファイル使用時）（Mbps）- 64 K サイズ [6]		690	—	1,530	—	1,310	—	2,000	—
HTTP スループット（IPS プロファイル使用時）（Mbps）- 44 K サイズ [4]		720	—	1,510	—	1,300	—	2,000	—
HTTP スループット（IPS プロファイル使用時）（Mbps）- 1 M サイズ [4]		700	—	1,540	—	1,310	—	2,000	—
NGFW スループット（Mbps）[7]		560	—	600	—	710	—	810	—
脅威保護スループット（Mbps）[8]		560	—	590	—	700	—	800	—
SSL インスペクションスループット（Mbps）[5]		560	—	1,080	—	850	—	1,670	—

サイジングガイドについては、www.fortinet.com/jp 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。

注：数値はすべて「最大」の性能値であり、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。
PAYG は最大 32 vCPU インスタンスをサポートします。

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。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、最新のデータシートを参照してください。

FOS v7.0.1 を実行し、FortiGate-VM BYOL インスタンスを使用した場合の性能指標です。

1. 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、Microsoft Azure 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。現在のテストバージョンは FortiOS 7.2.3。
2. 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。VDOM の購入については、オーダー情報を参照してください。
3. Microsoft Azure の帯域幅に関する最新情報は、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general に記載されています。
4. IPS パフォーマンスは、IPS プロファイルを有効にして 44 K および 1 M のパケットサイズで HTTP スループットを使用して測定されます。
5. TLS ECDHE RSA - AES 256 GCM SHA384（2K）を使用しています。
6. アプリケーション制御パフォーマンスは、64 K 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。
7. NGFW パフォーマンスは、IPS およびアプリケーション制御が有効な状態と、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。
8. 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が有効な状態と、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。

技術仕様

	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 / 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
仮想ドメイン：VDOM（標準 / 最大）[2]	10 / 500				10 / 500				10 / 500				10 / 500
ファイアウォールポリシー	200,000				200,000				200,000				200,000
システム性能	高速ネットワークオフ		高速ネットワークオン		高速ネットワークオフ		高速ネットワークオン		高速ネットワークオフ		高速ネットワークオン		
測定するインスタンス	D8s_v3（8vCPU）				D16s_v3（16vCPU）				D32s_v3（32vCPU）				
Azure 想定帯域幅 [3]	4,000 Mbps				8,000 Mbps				16,000 Mbps				
	スタンドアロン	IPsec	スタンドアロン	IPsec	スタンドアロン	IPsec	スタンドアロン	IPsec	スタンドアロン	IPsec	スタンドアロン	IPsec	
ファイアウォールスループット（UDP パケット）（Mbps）- 1280 バイト	1,550	1,450	4,100	4,000	1,840	1,780	8,000	7,200	1,900	1,780	16,500	7,600	
ファイアウォールスループット（UDP パケット）（Mbps）- 512 バイト	720	600	4,000	2,500	800	720	8,000	3,600	820	720	14,500	3,800	
ファイアウォールスループット（UDP パケット）（Mbps）- 64 バイト	100	90	1,800	500	120	120	3,750	700	125	120	1,950	750	
ファイアウォール新規セッション / 秒（TCP）	7,800	—	6,600	—	12,500	—	19,000	—	15,500	—	19,000	—	
HTTP スループット（アプリケーションプロファイル使用時）（Mbps）- 64 K サイズ [6]	1,320	—	4,080	—	1,470	—	8,160	—	1,750	—	16,290	—	
HTTP スループット（IPS プロファイル使用時）（Mbps）- 44 K サイズ [4]	1,300	—	4,070	—	1,410	—	8,180	—	1,700	—	16,290	—	
HTTP スループット（IPS プロファイル使用時）（Mbps）- 1 M サイズ [4]	1,360	—	4,090	—	1,500	—	8,170	—	1,780	—	16,280	—	
NGFW スループット（Mbps）[7]	1,020	—	1,560	—	1,100	—	2,950	—	1,240	—	5,000	—	
脅威保護スループット（Mbps）[8]	1,000	—	1,550	—	1,100	—	2,900	—	1,240	—	4,900	—	
SSL インスペクションスループット（Mbps）[5]	890	—	2,310	—	1,050	—	6,000	—	1,230	—	8,100	—	

サイジングガイドについては、www.fortinet.com/jp 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。

注：数値はすべて「最大」の性能値であり、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。
PAYG は最大 32 vCPU インスタンスをサポートします。

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。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、最新のデータシートを参照してください。

FOS v7.0.1 を実行し、FortiGate-VM BYOL インスタンスを使用した場合の性能指標です。

1. 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、Microsoft Azure 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。現在のテストバージョンは FortiOS 7.2.3。
2. 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。VDOM の購入については、オーダー情報を参照してください。
3. Microsoft Azure の帯域幅に関する最新情報は、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general に記載されています。
4. IPS パフォーマンスは、IPS プロファイルを有効にして 44 K および 1 M のパケットサイズで HTTP スループットを使用して測定されます。
5. TLS ECDHE RSA - AES 256 GCM SHA384（2K）を使用しています。
6. アプリケーション制御パフォーマンスは、64 K 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。
7. NGFW パフォーマンスは、IPS およびアプリケーション制御が有効な状態と、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。
8. 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が有効な状態と、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。

オーダー情報

以下をBYOLスキームで購入できます。PAYG / オンデマンドサブスクリプションの場合、さまざまなインスタンス / VMタイプをマーケットプレイスで選択できます。BYOL は、PAYG / オンデマンドサブスクリプションとは異なり、マーケットプレイスに記載されている製品で利用できる時間単位の永続ライセンスです。

Product	Description
FortiGate-VM01	FortiGate-VM 'virtual appliance'. 1x vCPU core. No VDOM by default for FG-VM01V model.
FortiGate-VM02	FortiGate-VM 'virtual appliance'. 2x vCPU cores. No VDOM by default for FG-VM02V model.
FortiGate-VM04	FortiGate-VM 'virtual appliance'. 4x vCPU cores. No VDOM by default for FG-VM04V model.
FortiGate-VM08	FortiGate-VM 'virtual appliance'. 8x vCPU cores. No VDOM by default for FG-VM08V model.
FortiGate-VM16	FortiGate-VM 'virtual appliance'. 16x vCPU cores. No VDOM by default for FG-VM016V model.
FortiGate-VM32	FortiGate-VM 'virtual appliance'. 32x vCPU cores. No VDOM by default for FG-VM032V model.
FortiGate-VMUL	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores. No VDOM by default for FG-VMULV model.
Optional Accessories/Spares	**Description**
Virtual Domain License Add 5	Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 15	Upgrade license for adding 15 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 25	Upgrade license for adding 25 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 50	Upgrade license for adding 50 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 240	Upgrade license for adding 240 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.

VDOM は、vCPU モデルごとのサポートしている VDOM の最大数まで積み重ね方式で構成できます。仕様の「仮想 UTM（VDOM：最大）」を参照してください。

以下は、年間サブスクリプションのライセンススキームを採用しています。

Product	Description
FortiGate-VM01-S	Subscriptions license for FortiGate-VM (1 vCPU core)
FortiGate-VM02-S	Subscriptions license for FortiGate-VM (2 vCPU cores)
FortiGate-VM04-S	Subscriptions license for FortiGate-VM (4 vCPU cores)
FortiGate-VM08-S	Subscriptions license for FortiGate-VM (8 vCPU cores)
FortiGate-VM16-S	Subscriptions license for FortiGate-VM (16 vCPU cores)
FortiGate-VM32-S	Subscriptions license for FortiGate-VM (32 vCPU cores)
FortiGate-VMUL-S	Subscriptions license for FortiGate-VM (Unlimited vCPU cores)

FortiOS 6.2.3 以降と 6.4.0 以降は、FortiGate-VM S シリーズをサポートしています。FortiGate-VM S シリーズには、いずれの vCPU レベルでも RAM の制限はありません。
FortiManager 6.2.3 以降と 6.4.0 以降は、FortiGate-VM S シリーズデバイスの管理をサポートしています。

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
セキュリティサービス	FortiGuard IPS Service	•	•	•	•
	FortiGuard Anti-Malware Protection（AMP）— Antivirus、Mobile Malware、Botnet、CDR、Virus Outbreak Protection、FortiSandbox Cloud Service	•	•	•	•
	FortiGuard Web Security — URL and web content、Video [2] and Secure DNS Filtering	•	•	•	
	FortiGuard Anti-Spam		•	•	
	FortiGuard IoT Detection Service [1]	•	•		
	FortiGuard Industrial Security Service	•	•		
	FortiCloud AI-based Inline Sandbox Service [3]	•			
NOC サービス	FortiGate Cloud（SMB Logging + Cloud Management）	•			
	FortiGuard Security Fabric Rating & Compliance Monitoring Service	•	•		
	FortiConverter Service	•	•		
	FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
SOC サービス	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
ハードウェア / ソフトウェアサポート	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
基本サービス	FortiGuard Application Control	FortiCare サブスクリプションに含まれています。			
	FortiCloud ZTNA Inline CASB Service [3]				
	Internet Service（SaaS）DB Updates				
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS（v4 / v6）Service				

1. FortiOS 6.4 以降を実行している場合に利用可能。 2. FortiOS 7.0 以降を実行している場合に利用可能。 3. FortiOS 7.2 以降を実行している場合に利用可能。

FortiGuard バンドル

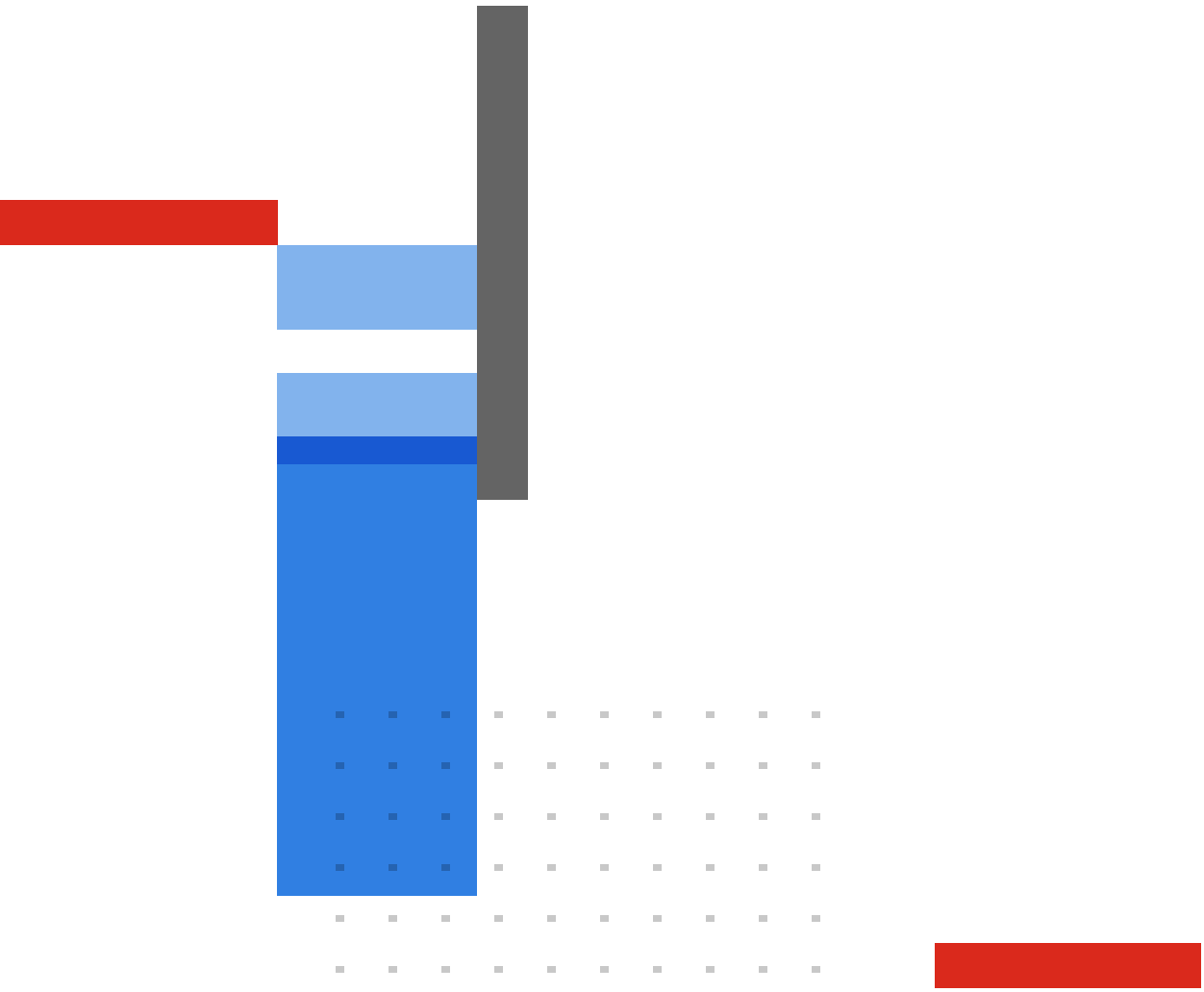
FortiGuard Labs は、FortiGate ファイアウォールプラットフォームと併せてご利用いただける、多数のセキュリティインテリジェンスサービスを提供しています。最適な Protection をお選びいただくことで、FortiGate の保護機能を容易に最適化できます。

FortiCare Elite

FortiCare Elite サービスは、SLA（サービスレベルアグリーメント）の強化と迅速な問題解決を支援します。この高度なサポートサービスでは、専任のサポートチームが任命され、エキスパートで構成されるテクニカルチームがチケットを処理することで、解決を効率化します。このオプションは、18 ヵ月の EoE（Extended End-of-Engineering-Support）も提供することで、さらなる柔軟性を提供し、新しい FortiCare Elite Portal へのアクセスも可能にします。この直感的なポータルを利用することで、デバイスやセキュリティの状態を 1 つの統一ビューで参照できます。

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

DS-FG-VM-AZU-R28-202304-R1