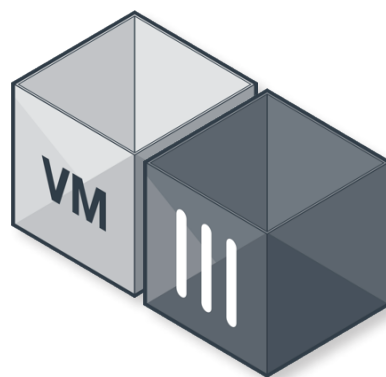


# FortiGate 仮想アプライアンス

仮想環境に最適な統合セキュリティ

フォーティネットは、ソフトウェア制御によるデータセンター向けにエンドツーエンドの包括的なセキュリティエコシステムを提供します。これによって、企業のデータセンター統合におけるあらゆるプロセスを支援し、促進します。



フォーティネットは、物理および仮想両方のアプライアンスを提供し、固有のデータプレーンを保護します。比類のないパフォーマンスとセキュリティ機能を両立することで、サービスレベルの低下やボトルネックを発生させることなく、トップクラスのセキュリティを実現します。そして、比類のないROIを実現しながら、ソフトウェアによって定義される堅牢なセキュリティフレームワークを作り出し、データセンターの統合を推進し企業の成長を支援します。

FortiGate仮想アプライアンスによって、重要なセキュリティ機能を仮想インフラストラクチャに実装し、死角のない万全なセキュリティ対策を実現することができます。また、いつでも必要に応じてセキュリティインフラストラクチャを迅速にプロビジョニングすることが可能です。さらに、フォーティネットの仮想アプライアンスには、従来のハードウェアベースのFortiGateアプライアンスで提供されているすべてのセキュリティおよびネットワーク機能が備えられています。フォーティネットが提供する仮想アプライアンスを導入することにより、ハードウェアおよび仮想アプライアンスを連携させて運用できると同時に、共通の管理プラットフォームから一元管理することも可能になります。

## FortiGate 仮想アプライアンスの特長

FortiGate仮想アプライアンスは、FortiOSオペレーティングシステムが提供するすべてのセキュリティおよびネットワーク機能に対応しており、巧妙化する脅威に対する最新の保護機能を提供します。加えて、次にあげるさまざまなメリットをもたらします。

- 仮想インフラストラクチャの監視におけるセキュリティの可視性を向上
- 迅速な導入を実現
- 単一の管理プラットフォームから仮想アプライアンスおよび物理アプライアンスを一元管理可能
- ユーザー数無制限のシンプルなライセンスモデル
- 多様な仮想/クラウドプラットフォームをサポート
- 幅広いライセンスの選択肢により、あらゆるインフラストラクチャ要件に適応
- VDOM (仮想ドメイン) 対応モデルはマルチテナント環境をサポート



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、16を超えるソリューションに対応しています。上図には、日本で未発売の製品も含まれます。

## プラットフォーム

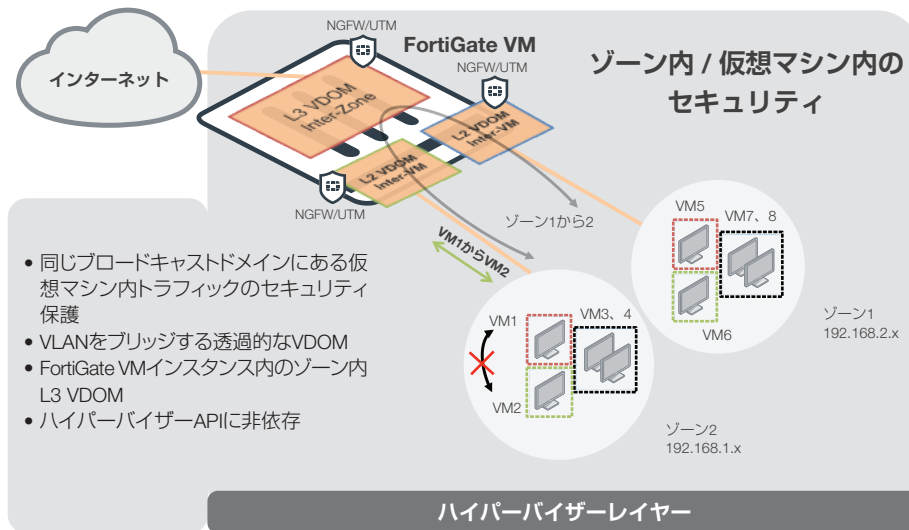
### さまざまなフォームファクタに対応

今日、完全にハードウェアのみ、あるいは仮想環境のみのITインフラストラクチャを利用している企業はほとんど存在せず、セキュリティ戦略においてはハードウェアアプライアンスと仮想アプライアンスの両方を取り入れることが求められています。フォーティネットは、ハードウェアと仮想アプライアンスの両方から構成されるセキュリティソリューションを構築し、企業にとって最適な環境を作り出し、コアからエッジまでの万全なセキュリティを実現すると同時に、仮想化されたインフラストラクチャで可視性を向上し通信の制御を強化します。FortiManagerの仮想および物理アプライアンスによって、ハードウェア、仮想、またはその両方におけるフォーティネットのセキュリティ資産を容易に一元管理および更新できるようになります。

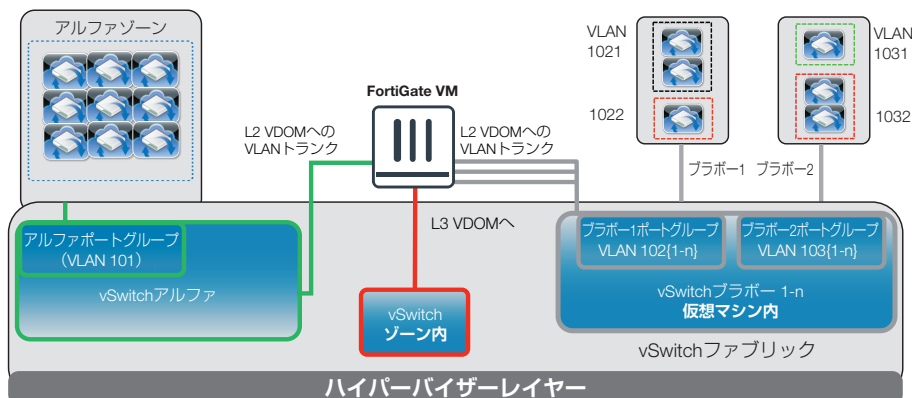
### 多様な脅威に対応するセキュリティ

FortiGateアプライアンスは、高度な機能を備えたFortiOSオペレーティングシステムの活用によって、仮想環境が直面する多様なセキュリティの脅威を効率的に無力化します。セキュリティ防御の最前線としてエッジに導入する場合でも、ゾーン内のセキュリティ対策のために仮想インフラストラクチャ内の深部に導入する場合でも、FortiGateアプライアンスは必要とされるセキュリティを提供し、現在利用可能な最も効果的なセキュリティ機能によって企業のインフラストラクチャを保護します。

## 導入例



ブラボゾーンにおける仮想マシン内のすべてのトラフィックは、L2 VDOMを介して詳細なUTMスキャンが実施される対象となります。ゾーン内トラフィックは、L3 VDOMを介して次世代ファイアウォールおよびUTMの詳細なスキャンが実施される対象となります。アルファゾーンのVMIは、相互に制約のない通信が可能です。

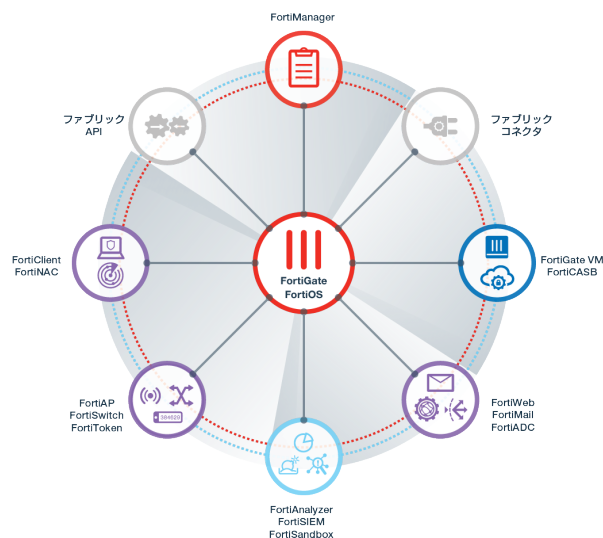


## フォーティネット セキュリティ ファブリック

### セキュリティ ファブリック

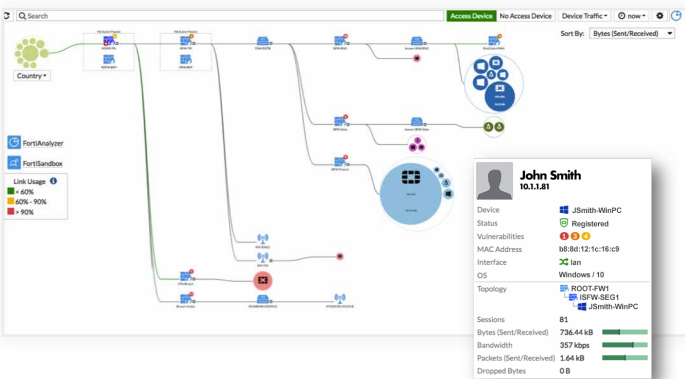
フォーティネット セキュリティ ファブリックは、広範なネットワークの可視化、AIの活用による統合的なセキュリティ侵害の防止、そしてすべてのフォーティネット製品とそのエコシステム環境の運用、オーケストレーション、レスポンスの自動化を実現します。セキュリティ ファブリックにより、ワークロードやデータの増加に合わせたセキュリティの動的な拡張や変更が可能になります。また、ネットワーク上のIoT、デバイス、およびクラウド環境を行き来するデータ、ユーザー、およびアプリケーションをシームレスに追跡して保護します。これらすべての機能は一元管理のもと緊密に統合され、お客様の環境全体に最先端のセキュリティ機能を提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

## Specifications

	FortiGate VM00	FortiGate VM01 / 01v	FortiGate VM02 / 02v	FortiGate VM04 / 04v
<b>技術仕様</b>				
仮想 CPU 数 (最小 / 最大)	1 / 1	1 / 1	1 / 2	1 / 4
メモリ (最小 / 最大)	1 GB / 2 GB *	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB
ストレージ容量 (最小 / 最大)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
制御可能な無線アクセスポイント数 (トンネル / グローバル)	32 / 32	32 / 64	256 / 512	256 / 512
仮想 UTM (VDM : 標準 / 最大) **	2 / 2	10 / 10	10 / 25	10 / 50
ファイアウォールポリシー	10,000	10,000	10,000	10,000
FortiToken サポート数	1,000	1,000	1,000	5,000
FortiClient サポート数	200	2,000	2,000	8,000
ユーザー数無制限ライセンス	○	○	○	○

	FortiGate VM08 / 08v	FortiGate VM16 / 16v	FortiGate VM32 / 32v	FortiGate VMUL / ULv
<b>技術仕様</b>				
仮想 CPU 数 (最小 / 最大)	1 / 8	1 / 16	1 / 32	1 / 無制限
メモリ (最小 / 最大)	1 GB / 12 GB	1 GB / 24 GB	1 GB / 48 GB	1 GB / 無制限
ストレージ容量 (最小 / 最大)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
制御可能な無線アクセスポイント数 (トンネル / グローバル)	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096
仮想 UTM (VDM : 標準 / 最大) **	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
FortiToken サポート数	5,000	5,000	5,000	5,000
FortiClient サポート数	20,000	20,000	20,000	20,000
ユーザー数無制限ライセンス	○	○	○	○

## ネットワークインタフェースのサポートについて

FortiGate VM の各インスタンスで使用可能なネットワークインタフェースの最大数は、FortiGate 5.6.6 および 6.0.3 以降のバージョンでは 18 です。それ以前のバージョンは 10 で、最小数は 1 です。実際に使用可能なネットワークインタフェース数は、クラウドプラットフォームやインスタンスの種類によって異なります。FortiGate では最大 18 のインタフェースをサポートしている場合であっても、インスタンスの最大サポート数を上回る数のインタフェースを追加できない場合があります。

\* FortiOS 5.6 以降で稼働している VM の場合。

\*\* 2018 年第 1 四半期以前の FG-VMxxV シリーズでは VDM (仮想ドメイン) がサポートされていないため適用外。

## ベンダー

## プライベートクラウドプラットフォーム (ハイパーバイザー)

VMware ESXi v5.5、v6.0、v6.5、v6.7

VMware NSX-T v2.3\*

Microsoft Hyper-V Server 2008 R2、2012、2012 R2、2016

Microsoft AzureStack

Citrix Xen XenServer v5.6 sp2、v6.0、v6.2 およびそれ以降

Open source Xen v3.4.3、v4.1 およびそれ以降

Red Hat Enterprise Linux、CentOS 6.4 およびそれ以降向けの KVM qemu 0.12.1、libvirt 0.10.2 およびそれ以降、Ubuntu 16.04 LTS (標準カーネル)

SuSE Linux Enterprise Server 12 SP1 LTSS 向けの KVM qemu 2.3.1

Nutanix AHV (AOS 5.10、Prism Central 5.10) \*\*

Cisco Cloud Services Platform 2100\*\*

\* FortiGate VM 6.0.4 以降で VMware NSX-T をサポート ([https://www.vmware.com/resources/compatibility/search.php?deviceCategory=nsxt&details=1&releases=446&partners=579&page=1&display\\_interval=10&sortColumn=Partner&sortOrder=Asc](https://www.vmware.com/resources/compatibility/search.php?deviceCategory=nsxt&details=1&releases=446&partners=579&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc))

\*\* FortiGate VM 6.0.3 以降で Nutanix AHV and Cisco CSP 2100 をサポート

## ベンダー

## パブリッククラウドプラットフォーム (マーケットプレイス)

Amazon AWS (GovCloud および AWS China を含む)

VMware Cloud on AWS\*

Microsoft Azure (次の Azure リージョンを含む: Government、Germany、China)、AzureStack syndication

Google GCP (Google Cloud Platform)

Oracle OCI

Alibaba Cloud (AliCloud)

サポートする仮想化 / クラウドプラットフォームは、モデルおよび FortiOS のビルドによって異なります。詳細は、該当のリリースノートをご参照ください。FG-VMxxV シリーズをご利用いただくには、FortiOS 5.4.8 以降、5.6.1 以降、6.0.0 が必要です。

\* FortiGate VM 6.0.4 以降で VMware Cloud on AWS をサポート

**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](http://www.fortinet.com/jp/contact)

## お問い合わせ