

FortiManagerアプライアンス

Fortinetセキュリティ ネットワークの集中管理

企業のセキュリティ インフラをコントロール (展開、監視、制御)

FortiManager集中管理アプライアンスは、フォーティネット製品で構成されたセキュリティ インフラを効果的に管理するために必要となる重要なツールを提供します。数台から数千台に及ぶ新しいデバイス/エージェントの展開や、アップデートの配布、あるいは管理対象となる装置全域へのセキュリティ ポリシーのインストールなどのいずれにおいても、FortiManagerアプライアンスは管理コストとオーバーヘッドを大幅に削減します。FortiManagerアプライアンスは、作業時間を節約する様々な機能として、機器の検出、グループ管理、設備の監査、複雑なメッシュおよびスター型VPN環境の管理、その他様々な機能を備えています。さらにログインおよびレポート機能を集約したFortiAnalyzerアプライアンスを補完的に追加することで、FortiManagerアプライアンスは高度な性能を備えた包括的な集中管理ソリューションとなります。

各ドメインを徹底管理

FortiManagerアプライアンスは、管理可能なフォーティネット機器/エージェントの規模として数千台まで対応できます。そうした様々な環境により柔軟に対応できるよう、2種類の管理モードが選択できます。1つは、すべての装置を集中的に管理するもので、FortiManagerユーザ インタフェースから設定します。もう1つは、分散ネットワークを構成し、各管理者がそれぞれの定義に基づいて機器/エージェント セットを管理できるようにするものです。機器/エージェントをグループ分けし、それぞれに対して管理者を割り当てることで、管理ドメイン(ADOM)に関するFortiManagerのコンセプトになります。完全な集中管理と分散管理のどちらのモデルを選択しても、また設定するADOMが1つであろうと100個であろうと、FortiManagerアプライアンスはフォーティネット製の装置を常に効果的かつ効率的に管理することができます。

フォーティネットの 統合管理ソリューション

FortiManagerアプライアンスは、フォーティネット セキュリティ インフラを統制管理するためのセキュアなWebベース インフラを提供します。他にも、FortiGate、FortiMailの各アプライアンスやFortiClientエンドポイントセキュリティ エージェントに対する集中ポリシー ベース プロビジョニング、設定、アップデート管理も行います。また、リアルタイム モニタリング機能が搭載されているため、可視性が向上します。

集中管理ソリューションを完成させるため、FortiManagerはFortiAnalyzerアプライアンスとシームレスに統合します。これらのアプライアンスによって、導入環境内で発見されたセキュリティ イベントの詳細な検出、分析、優先順位付け、レポートが可能になります。FortiManagerとFortiAnalyzerのシステム全体で、包括的なエンタープライズ クラスの管理ソリューションが構成されます。

| 機能 | メリット | |
|------------------------|---|---|
| グローバルとエレメンタルの2つの管理モード | 集中管理のほかに、一部またはすべての管理タスクをローカルで実行する分散管理も可能 |  FortiManager-200D |
| グローバル オブジェクト データベース | 組織全域にわたって共通設定を容易に再利用 |  FortiManager-400C |
| アプライアンス ベースの集中管理 | サードパーティ製のオペレーティング システムやハードウェア機器が不要となり、集中管理ソリューションにともなう展開と保守を簡素化 |  FortiManager-1000C |
| 機器の自動プロビジョニング/集中ポリシー設定 | FortiGateまたはFortiClient新規導入の展開コストを削減し、管理している資産すべてのポリシー設定を維持 |  FortiManager-3000C |
| 役割ベースの管理 | 大規模組織で重要な要件となっている分散管理が可能 |  FortiManager-5001A |
| ポリシー/機器の監査 | コンプライアンス遵守の証明と、必要なセキュリティ ポリシーからの逸脱のすべてを追跡可能 | |
| WebポータルSDK | JSONベースのAPIでMSSPがユーザに管理用Webポータルを提供することができます。 | |
| XML API | 多くのデバイスのプロビジョニングと設定の自動化と統合管理が可能 | |

仮想管理 (ADOM)

主任管理者は、他の管理者が監視と管理を行うための機器グループを設定できます。

- 管理者は機器の仕様を地理的なロケーションや事業部門に合わせて設定を維持することができます。
- 複数の仮想UTM (VDOM) が設定されているいくつかのFortiGateユニットを、複数の管理ドメイン間で割り振ることができます。
- 管理ユーザがログインしても、その管理者に対して設定されている機器や仮想UTM (VDOM) 以外は表示されません。
- 主任管理者は、すべての管理ドメインとそのドメイン内にある機器を表示および管理することができます。

グローバル オブジェクト データベース

様々な装置の設定詳細を保存する、FortiManagerの集中レポジトリです。

- 機器の設定テンプレートを作成することで、新しいフォーティネット アプライアンスの設定が迅速に行えます。
- 管理対象の装置グループ間で同様の設定を再利用できます。

Webポータル SDK

単一の管理プラットフォームで複数のテナント アプリケーションを扱えるよう設計されています。

- JSONベースのAPIでMSSPがユーザに管理用Webポータルを提供することができます。
- ネットワーク セキュリティ管理をある程度コントロールする必要がある場合に適した管理Webポータルです。
- SSL-VPNユーザ リストやWebコンテンツ フィルタリングの設定を制御できます。
- 設定後、ユニットや仮想UTM (VDOM) に対するファイアウォール ポリシーも表示できます。

ローカルにホスティングされたセキュリティ コンテンツ

セキュリティ コンテンツをローカルにホスティングすることで、管理者はセキュリティ コンテンツ アップデートの制御が容易になり、またレーティング データベースの応答時間を短縮することができます。

以下に対するサポートが含まれます。

- アンチウイルス定義アップデート
- 不正侵入防御アップデート
- 脆弱性とコンプライアンス管理アップデート
- Webコンテンツ フィルタリング (選択したシステム)
- アンチスパム (選択したシステム)

グローバルとエレメンタルの2つの管理モード

運用モードを選択することで、各組織の管理モデルに適応します。

グローバル管理システム (GMS) モード

- 複数の機器を単一の設定で管理する場合に使用します。
- どのインストール環境も同一のポリシー、グループ、VPNの設定を保持します。
- すべての機器に設定が強制的に反映されます。

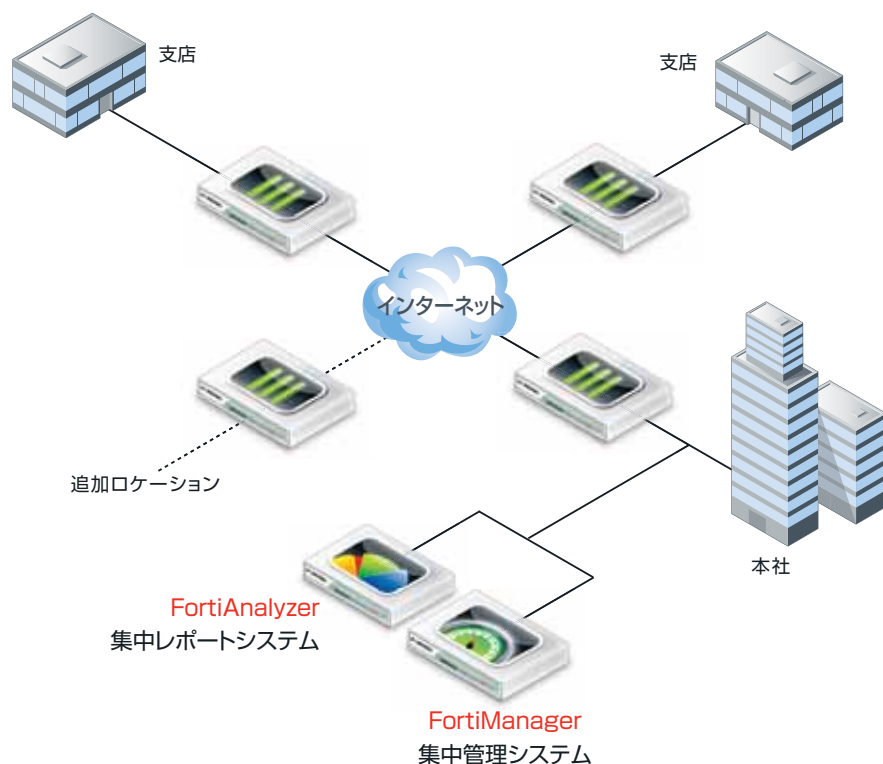
エレメント管理システム (EMS)

- 管理者は複数のデバイスに対して複数の設定で管理できます。
- 各インストール環境において、ファイアウォール ポリシーやユーザ グループ、VPNなどの設定について固有または特定の設定が保持されます。

XML API

XML APIは、自動化のためのWebサービスインターフェースです。

- プロビジョニングの統合ができます。
- Webサービスインターフェースを通して、FortiGateの設定を管理できます。
- FortiManagerのデータベースから情報取得し、FortiOS CLIスクリプトを生成し、FortiGateの設定変更ができます。



| 技術仕様 | FortiManager-200D | FortiManager-400C | FortiManager-1000C | FortiManager-3000C | FortiManager-5001A |
|----------------------|--|--|--|--|--------------------|
| インタフェースとモジュール | | | | | |
| GbE SFP インタフェース | – | – | – | 2 | – |
| 10/100/1000 インタフェース | 4 | 4 | 4 | 4 | 2 |
| 管理コンソールインタフェース | RJ-45 | RJ-45 | DB-9 | DB-9 | DB-9 |
| 液晶パネル | – | – | ○ | ○ | – |
| 内蔵ストレージ | 1 TB | 1 TB | 2 TB | 4 TB | 80 GB |
| システム性能 | | | | | |
| ライセンス承諾ネットワーク機器数* | 30 | 300 | 800 | 5,000 | 4,000 |
| 仮想管理 (ADOM) | 30 | 300 | 800 | 5,000 | 4,000 |
| 管理Webポータル数 | – | – | 800 | 5,000 | 4,000 |
| Webポータルユーザ数 | – | – | 800 | 5,000 | 4,000 |
| 高可用性(HA) | ○ | ○ | ○ | ○ | ○ |
| グローバルポリシー | ○ | ○ | ○ | ○ | ○ |
| ハードウェア仕様 | | | | | |
| 高さ | 4.5 cm | 4.4 cm | 4.3 cm | 8.9 cm | 3.0 cm |
| 幅 | 43.3 cm | 43.5 cm | 43.4 cm | 44.5 cm | 35.5 cm |
| 奥行 | 35.2 cm | 36.4 cm | 62.71 cm | 73.7 cm | 31.0 cm |
| 重量 | 6.08 kg | 6.7 kg | 11 kg | 28.6 kg | 3.63 kg |
| 形状 | ラックマウント (1 RU) | ラックマウント (1 RU) | ラックマウント (1 RU) | ラックマウント (2 RU) | ATCA ブレード |
| AC電源 | 100 - 240 VAC、 50 - 60 Hz | 100 - 240 VAC、 50 - 60 Hz、4.0 A(最大) | 100 - 240 VAC、 50 - 60 Hz、7.0 A(最大) | 100 - 240 VAC、 50 - 60 Hz、9.0 A(最大) | シャーシからDC電源供給 |
| 消費電力(平均) | 60 W | 100 W | 189 W | 200 W | 148 W |
| 冗長電源(ホットスワップ対応) | – | – | – | ○ | ○(シャーシに内蔵) |
| 動作環境 | | | | | |
| 動作温度 | 0 ~ 40°C | | | | |
| 保管温度 | -25 ~ 70 °C | | | | |
| 湿度 | 5 ~ 95% (結露しないこと) | | | | |
| 準拠規格・認定 | | | | | |
| 準拠規格 | FCC Part 15 Class A、UL/CB/CUL、CE、C Tick、VCCI | | | | |

* ライセンス承諾ネットワーク機器の定義は次の通りです。
VDOM (仮想UTM) モードをイネーブルしていない1台のFortiGateユニット
または FortiGateユニットを複数VDOMモードで実行している場合1つのVDOM
または 1台のサードパーティ製Syslog互換機器

| FortiManager仮想 アプライアンス | FMG-VM-Base | FMG-VM-10-UG*1 | FMG-VM-100-UG*1 | FMG-VM-1000-UG*1 | FMG-VM-5000-UG*1 | FMG-VM-U-UG*1 |
|------------------------|---|----------------|-----------------|------------------|------------------|---------------|
| 技術仕様 | | | | | | |
| ライセンス承諾ネットワーク機器数*2 *3 | 10 | +10 | +100 | +1,000 | +5,000 | 無制限*3 |
| 仮想管理 (ADOM) | 10 | +10 | +100 | +1,000 | +5,000 | 無制限*3 |
| 管理Webポータル数 | 10 | +10 | +100 | +1,000 | +5,000 | 無制限*3 |
| Webポータルユーザ数 | 10 | +10 | +100 | +1,000 | +5,000 | 無制限*3 |
| 仮想環境 | | | | | | |
| ハイパーバイザ | VMware ESXi / ESX v3.5, v4.0, v4.1, v5.0 | | | | | |
| 仮想CPU数 | 無制限 | | | | | |
| メモリ(最小/最大) | 1,024MB / 4,096 MB(32-Bitの場合)、1,024 MB / 無制限(64-Bitの場合) | | | | | |
| ストレージ容量(最小/最大) | 80 GB / 2 TB | | | | | |
| 仮想NIC枚数(最小/最大) | 1 / 4 | | | | | |
| 高可用性(HA) | ○ | | | | | |

*1 追加ライセンスです。FMG-VM-Baseと同時にご契約ください。

*2 仮想UTM (VDOM) 毎に1ライセンスとしてカウントされます。

*3 現在のソフトウェア上の制限はデバイス、仮想管理 (ADOM)、管理Webポータル数、Webポータルユーザ数、それぞれ10,000です。

管理機能の実行

- 機器およびエンドポイント エージェントを個別または論理グループとして管理します。
- 新しい機器を自動的に検出します。
- VPNを作成、展開、監視します。
- 分散管理機能により、他のユーザにコントロールを任せることができます。
- コンプライアンスを遵守できるように監査設定を変更します。

アップデートの管理

- 機器アップデートをスケジュール設定することで、フォーティネット製品で構成されたセキュリティ インフラの継続的な保守を簡素化します。

監視、分析、レポート機能

- 重要なセキュリティおよびネットワーク統計にアクセスします。
- FortiAnalyzerアプライアンスと組み合わせることで、データマイニングやグラフィカルなレポート機能を追加できます。

サポート対象の機器およびエージェント

- FortiGate 複合脅威セキュリティ アプライアンス
- FortiClient エンドポイント セキュリティ ソフトウェア
- FortiMail メッセージング セキュリティ アプライアンス
- FortiAnalyzer 分析&レポート アプライアンス
- FortiSwitch セキュリティ アプライアンス

FortiManager Feature

| | アドオン | | ローカルホスト セキュリティコンテンツ | | | | | その他の機能 | |
|---------------------------------------|-----------|------------|---------------------|-----|-------|------------|--------|--------|------------------------------|
| | グローバルポリシー | WebポータルSDK | アンチウイルス | IPS | 脆弱性管理 | Webフィルタリング | アンチスパム | シェルフ管理 | クローズドネットワークモード (VMアクティベーション) |
| FortiManager-200D | ○ | — | ○ | ○ | ○ | ○ | ○ | — | — |
| FortiManager-400C | ○ | — | ○ | ○ | ○ | ○ | ○ | — | — |
| FortiManager-1000C | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| FortiManager-3000C | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| FortiManager-5001A | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| FortiManager-VM Base (4.0 MR3) | ○ | ○ | ○ | ○ | ○ | — | — | — | — |
| FortiManager-VM Base + FMG-VM-10-UG | ○ | ○ | ○ | ○ | ○ | — | — | — | — |
| FortiManager-VM Base + FMG-VM-100-UG | ○ | ○ | ○ | ○ | ○ | — | — | — | — |
| FortiManager-VM Base + FMG-VM-1000-UG | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| FortiManager-VM Base + FMG-VM-5000-UG | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| FortiManager-VM Base + FMG-VM-U-UG | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

FortiCareサポートサービス: 全てのフォーティネット製品においてグローバルサポートを提供するサービスです。FortiCareサポートによりフォーティネット製品を最適にご利用いただくことが可能になります。サポートプランには、Technical Assistant Center (TAC)を通じて、製品サポート(ソフトウェア、ハードウェア)を当社の1次代理店様にご提供します。また、万一のハードウェア不良時に備え、センドバック方式によるハードウェアRMA交換サービス(良品、後出し)を含む平日の9時間サポートから、オプションとして、プレミアムサポート、プレミアムRMA交換サービス、プロフェッショナルサービス等もご提供いたします。 *FortiCareサポートサービスは、当社の1次代理店様経由でご提供させていただきます。

FortiGuardサブスクリプションサービス: フォーティネット製品に対して、動的な自動セキュリティアップデート配信を提供するサービスです。フォーティネットのグローバルセキュリティ研究チームが開発するこれらのセキュリティアップデートにより、巧妙な脅威に対する最新のプロテクションが確保できます。サブスクリプションには、アンチウイルス、不正侵入検知/防御Webコンテンツフィルタリング、アンチスパム、脆弱性/コンプライアンス管理、アプリケーション制御、Webアプリケーションファイアウォール、データベースセキュリティサービスなどが含まれます。

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 7-18-18

住友不動産六本木通ビル 8階

TEL:03-6434-8531/8533

www.fortinet.co.jp

お問い合わせ