DATA SHEET

# FortiOS 6.2

フォーティネットのセキュリティ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 ファブリックを実現し、セキュリティ ドリブン ネットワーキングを確実に達成可能にするフォーティネット独自の直感的なオペレーティングシステムです。FortiOS 6.2 はフォーティネットの最新セキュリティオペレーティングシステムで、セキュリティ ファブリック全体の基盤となって IoT（モノのインターネット）からクラウドまでを網羅する攻撃対象領域の縮小と管理、高度な脅威の防止、ネットワークセキュリティの簡素化を支援します。


### ネットワークの可視化

マルチクラウドや支社を網羅する完全な可視化が達成されると同時に、SD-WAN、ネイティブのクラウドや仮想コネクタ、インテント ベースト セグメンテーションが実現します。

### AI を活用する統合型セキュリティ侵害防止

最先端の高度なテクノロジーと AI を活用した統合型セキュリティインテリジェンスを組み合わせることで、セキュリティ ファブリック全体における迅速な脅威の阻止および不正侵入や犯罪者の活動の検知が可能です。

### 運用、オーケストレーション、レスポンスの自動化

脅威に対するレスポンスの迅速なオーケストレーション、ワークフローや監査、コンプライアンスの自動化により、複雑さの軽減とコストの削減が可能です。

### ハイライト： 新機能

- タスク分割をサポートする仮想ドメイン
- セキュリティ ファブリックによる製品統合の拡張
- 新しいSDNと脅威インテリジェンスフィード用コネクタ
- SD-WANルール定義およびVPNセットアップの強化
- パブリッククラウドのサポート拡大
- トリガーおよびアクションの追加
- フローベースのセキュリティプロファイル改善
- MACアドレスオブジェクト
- トポロジーマップにおけるリスクビューの統合
- FortiSandbox Cloudのリージョン選択
- ポリシー設定および可視化機能のアップグレード

# 概要

## FortiOS 6.2 のご紹介

ビジネス運用モデルからサービスデリバリの方法までのあらゆる要素のデジタルトランスフォーメーションの推進に伴い、モバイルコンピューティング、IoT、マルチクラウドネットワークなどのテクノロジーを採用して、ビジネスの俊敏性、自動化、拡張性の実現に取り組む企業が増えています。デジタルによる組織間の連携がますます緊密になり続ける今日、セキュリティトランスフォーメーションの要件がこれまで以上に厳しくなり、アプリケーション、デバイス、クラウドネットワークにセキュリティを統合して、そのような複雑な環境に存在するビジネスデータを保護することが不可欠となっています。

FortiOS 6.2 は、何百もの新たな機能を採用し、デジタルビジネスに要求される包括的なネットワークの可視化と統合脅威インテリジェンスを提供し、自動的なインシデント対応を可能にします。

FortiOS 6.2 によって提供されるフォーティネット セキュリティ ファブリックは、スケーラブルで相互接続されたセキュリティと高可用性、実用的な脅威インテリジェンス、およびオープンな API 標準規格をすべて実現することで最大限の柔軟性と統合性を提供し、最も要件の厳しいエンタープライズ環境の保護にも対応するよう設計された、インテリジェントなフレームワークです。

フォーティネットのセキュリティテクノロジーは、第三者機関によって、その優れたセキュリティ効果とパフォーマンスが認定されています。フォーティネット セキュリティ ファブリックは、エンドポイントからクラウドまでの物理環境および仮想環境で必要とされる広範な保護を、強力かつ自動化された方法で提供することで、従来の単機能製品やプラットフォームでは解決できなかったセキュリティギャップを解消します。

## FortiOS 6.2 の詳細

FortiOS は、セキュリティを強化した専用オペレーティングシステムで、FortiGate のソフトウェアの基盤となっています。直感的なオペレーティングシステムを利用することで、ネットワーク全体のすべての FortiGate のセキュリティおよびネットワークのあらゆる機能を一元制御可能になります。FortiOS は豊富なセキュリティ機能を備えており、あらゆる規模の組織がそれぞれの環境に最適なセキュリティゲートウェイ設定を展開できます。要件の変化に合わせて、中断やコストを最小限に抑えつつ、機能や設定を変更できます。

<table>
<tr><td rowspan="2">構成</td><td rowspan="2">ログおよび<br>レポート</td><td rowspan="2">診断</td><td rowspan="2">監視</td><td rowspan="2">運用</td><td>システム<br>統合</td><td colspan="2">管理とプロビジョニングの<br>一元化</td><td>クラウドと<br>SDN の<br>統合</td></tr>
<tr><td colspan="2">可視性</td><td colspan="2">自動化</td></tr>
<tr><td>ポリシー<br>オブジェクト</td><td>デバイスの識別</td><td>SSL<br>インスペクション</td><td>アクション</td><td>ポリシーと<br>制御</td><td colspan="2">AAA</td><td colspan="2">コンプライアンスと<br>セキュリティレーティング</td></tr>
<tr><td>アンチマルウェア</td><td>IPS および DoS</td><td>アプリケーション<br>制御</td><td>Web<br>フィルタリング</td><td rowspan="2">セキュリティ</td><td rowspan="2">高度な脅威<br>保護<br>（ATP）</td><td rowspan="2">脆弱性評価</td><td rowspan="2">IOC の検知</td></tr>
<tr><td>ファイアウォール</td><td>VPN</td><td>DLP</td><td>メール<br>フィルタリング</td></tr>
<tr><td>SD-WAN</td><td>明示的プロキシ</td><td>IPv6</td><td>高可用性</td><td rowspan="2">ネットワーキング</td><td rowspan="2">無線 LAN<br>コントローラ</td><td rowspan="2">スイッチ<br>コントローラ</td><td rowspan="2">WAN<br>インタフェース<br>マネージャ</td></tr>
<tr><td>ルーティング / NAT</td><td>L2 / スイッチング</td><td>オフライン<br>インスペクション</td><td>基幹ネットワーク<br>サービス</td></tr>
<tr><td>物理<br>アプライアンス<br>（SPU 搭載）</td><td>仮想システム</td><td>ハイパーバイザー</td><td>クラウド</td><td>サポートする<br>プラットフォーム</td><td colspan="4">セキュリティ ファブリック</td></tr>
</table>

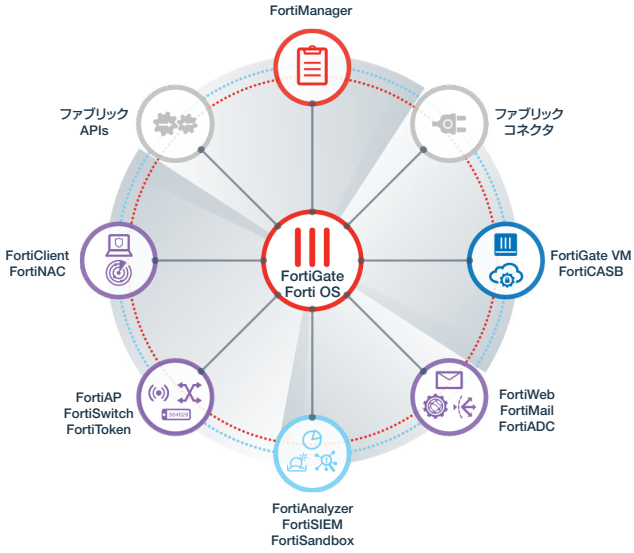
# ハイライト

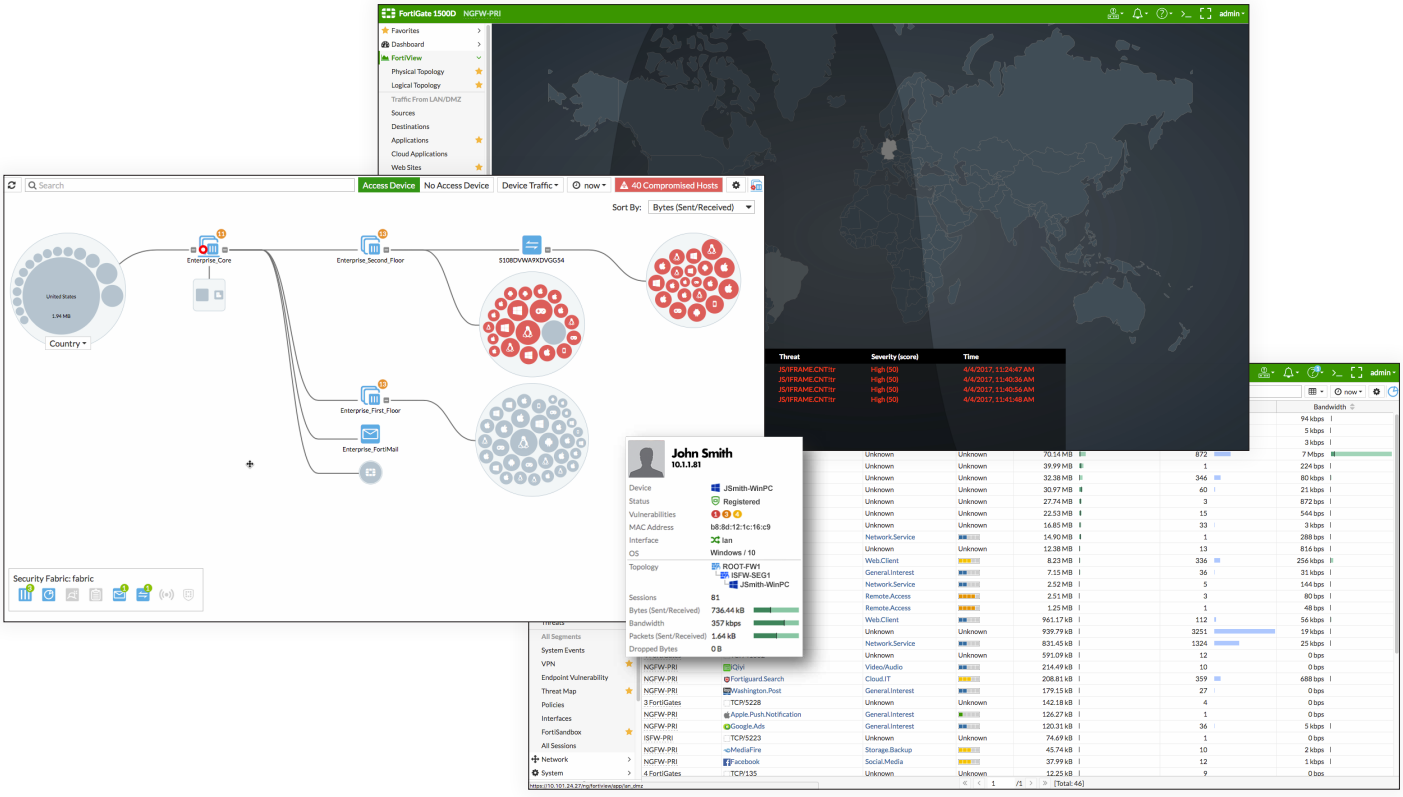
## セキュリティ ファブリック

### FortiGateとの統合

セキュリティ ファブリックでは、ワークロードやデータの追加に合わせた拡張や変更が可能であると同時に、ネットワーク上の IoT、スマートデバイス、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できます。

次世代ファイアウォール FortiGate をセキュリティ ファブリックの中心に展開し、他の FortiGate やフォーティネット製品とファブリック対応ソリューションを緊密に統合して可視化と制御を可能にすることで、セキュリティがさらに強化されます。



FortiView、トポロジー、脅威マップ

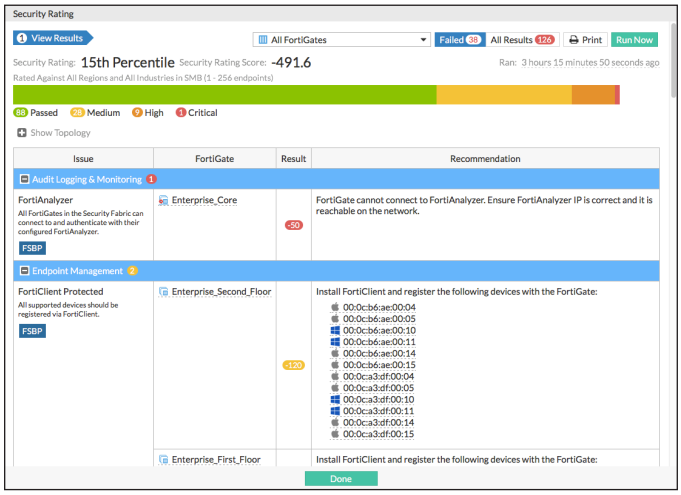
### 可視性

FortiOS 6.2のFortiViewでは、ネットワークトラフィックをあらゆる角度から可視化できます。ワンクリックで、送信元、送信先、アプリケーション、脅威、インタフェース、デバイス、ポリシー、および国別にトラフィックを表示できます。包括的なテーブルビューの他に、国やトポロジーのマップ、ボリュームベースのバブルチャートなどのグラフィカルな可視化により、問題を迅速かつ直感的に特定できます。

# ハイライト

### セキュリティレーティング

セキュリティ ファブリックの監査は、セキュリティ ファブリックの導入環境を分析して潜在的な脆弱性を特定し、ネットワーク全体のセキュリティとパフォーマンスの向上につながるベストプラクティスを提示する機能です。さらに、監査時のネットワークの合否数に基づいて決定されるセキュリティ ファブリックのスコアをチェックすることで、ネットワークのセキュリティを継続的に強化できます。



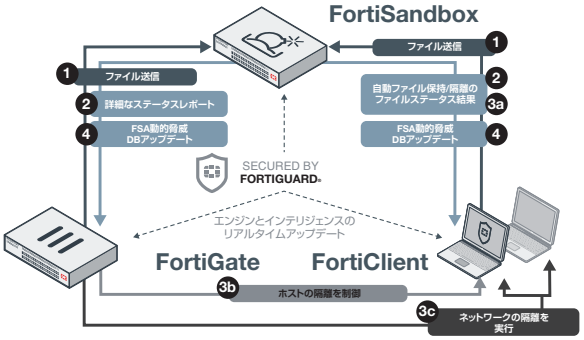


### 自動化

ステッチは、管理者が定義する新しい自動化ワークフローであり、if/then ステートメントを使用して、FortiOS によるプログラミング方式の自動レスポンスを可能にします。ステッチもセキュリティ ファブリックの一部であるため、セキュリティ ファブリック内の任意のデバイスにステッチを設定できます。

### 高度な脅威保護（ATP）

今日最先端の統合および自動化を実現するフォーティネットの ATP（高度な脅威保護）ソリューションは、FortiGate、FortiSandbox、FortiMail、FortiClient、および FortiWeb をはじめとする ATP フレームワークによって提供されます。これらの製品は容易に連携できるため、一般的な攻撃経路すべてにわたってクローズドループの保護が提供されます。




**クエリ**

1. 分析用にファイルを送信
2. それぞれの分析結果を受信

**修復**

- 3a ホストで自動的にファイルを隔離（結果が出るまでファイルを保持するオプションあり）
- 3b 管理者が手動でホストを隔離
- 3c ファイアウォールを使用して手動で送信元IPを隔離

**保護**

4. ゲートウェイとホストに対してプロアクティブな動的脅威DBアップデートを実行

| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| システム統合 | ▪ 標準ベースのモニタリング出力：SNMP Netflow / Sflow および Syslog の外部（サードパーティ）SNMP およびログ管理システムに対するサポート<br>▪ **機能向上：**フォーティネット製品とテクノロジーアライアンスによるセキュリティ ファブリックの統合 | ▪ 詳細なログと出力からさらなる洞察を得られるので、正確かつ迅速にインシデントや問題を識別して解決できます。<br>▪ 組織の既存のシステムを再利用して、TCO を削減してプロセスを合理化できます。 |
| 管理とプロビジョニングの一元化 | ▪ API と CLI スクリプトによるフォーティネット / サードパーティの自動化およびポータルサービスのサポート<br>▪ クラウドベースのプロビジョニングソリューションを含む迅速な導入機能<br>▪ 複雑な統合に対応する開発者コミュニティプラットフォームおよびプロフェッショナルサービスのオプション | ▪ 包括的な API と CLI コマンドにより、豊富な機能を提供するサービスを実現します。<br>▪ 迅速な包括的導入オプションにより、時間とコストの削減を可能にします。<br>▪ Fortinet Developer Network（FNDN）が、大規模サービスプロバイダーおよびエンタープライズによる実装 / カスタマイズ / 統合に関する情報の共有を促進します。 |
| クラウドと SDN の統合 | ▪ **機能向上：**クラウドおよび SDN コネクタを使用したマルチクラウドのサポート：AWS、Microsoft Azure、GCP、OCI、AliCloud、VMware ESXi、NSX、OpenStack、Cisco ACI、Nuage Virtualized Service Platform<br>▪ **新機能：**プライベート / パブリッククラウドプラットフォーム用 Kubernetes コネクタ | ▪ 堅牢で包括的な SDN との統合機能により、アジリティを損ねることなく確実にクラウドソリューションを実装できます。 |

# ハイライト

| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| 可視性 | ▪ リアルタイム / 過去の脅威ステータスとネットワーク使用状況を、包括的なコンテキスト情報とともに表示するドリルダウンビューアーとトポロジービューアー<br>▪ 集約データビューでダウンストリームの FortiGate をリモートで制御可能<br>▪ **新機能：**トポロジーマップにおけるリスクビューの統合 | ▪ リストの送信元 / 送信先に対して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します。<br>▪ 独自の脅威スコアシステムで重み付けされた脅威を特定ユーザーに相関させ、調査を優先付けします。<br>▪ ファブリック全体ビューでは、単一セキュリティエンティティにとどまらない広範な可視化が可能であるため、問題を迅速に特定して解決できます。 |
| 自動化 | ▪ **機能向上：**定義されたトリガーに基づいてセキュリティ ファブリックで適切なアクションを実行する、ウィザードベースの自動化ワークフロー<br>▪ EMS 経由の FortiClient、または FortiSwitch / FortiAP 経由の接続を使用した、感染ホストの自動隔離 | ▪ 侵害リスクを軽減し、人手によるセキュリティプロセスを自動化することで、予算の削減や人材不足の問題を解決できます。 |
| AAA（認証、認可、アカウンティング） | ▪ FortiAuthenticator および多様な外部 ID 管理システムのユーザー認証プロセス用インタフェース<br>▪ 多様なシングルサインオンの ID 取得方法（Windows AD、ターミナルサーバー、アクセスポータル、メールサーバーを含む）<br>▪ 物理およびモバイルの両方のトークンを管理する組み込みトークンサーバーを、VPN アクセスや FortiGate の管理など、FortiOS の多様な認証のニーズに対応するために使用可能 | ▪ FortiOS は広範な AAA サービスと統合し、ユーザーアクセスの制御をさまざまなエントリーポイントから推進し、これによってユーザーの操作を簡素化しながらセキュリティを強化できます。<br>▪ ユーザーおよび管理者のアクセス向けの二要素認証を、コストを抑えて簡単に導入できます。 |
| コンプライアンスとセキュリティ レーティング | ▪ 事前定義済みの PCI コンプライアンスチェックリストを使用する定期的なシステム構成チェック<br>▪ **機能向上：**タグに基づく動的なユーザーグループのセキュリティ状態チェックによるエンドポイントへのポリシー適用<br>▪ **機能向上：**ファブリック全体の FortiGate および FortiAnalyzer のセキュリティ構成とクライアント脆弱性ステータスのチェック<br>▪ **機能向上：**セキュリティレーティングランキングのピアに対するベンチマーク<br>▪ **新機能：**セキュリティレーティングの傾向履歴 | ▪ コンプライアンスの監査を自動化することにより、管理リソースを開放します。<br>▪ ゲートウェイ保護との一貫性のあるクライアントのセキュリティプロファイルを簡単に配布してアップデートすることにより、モバイルユーザーに対するセキュリティの実施を簡素化します。<br>▪ ファブリック内の設定や接続デバイスのステータスと状態をすばやく確認し、大きなリスクになる可能性があるギャップを特定します。 |
| 高度な脅威保護（ATP） | ▪ ローカルファイルの隔離（ストレージ付きモデルの場合）<br>▪ IP レピュテーション DB を使用するアンチボット保護がボットと C&C サーバーの通信を切断<br>▪ 外部のフォーティネットファイル分析ソリューション（FortiSandbox）から、動的な修正（不正ファイルのチェックサムと URL）DB のアップデートと詳細な分析レポートを受信 | ▪ 業界で実証された実績ある AV リサーチサービスによってサポートされます。<br>▪ モバイルユーザーや支社も対象範囲に含む堅牢な ATP フレームワークを採用できます。これにより、暗号化ファイルを含む多様な経路からのファイルを評価し、従来の防御をバイパスする可能性のある高度な攻撃を検知して阻止します。 |
| 脆弱性評価 | ▪ 脆弱性の高いクライアントの詳細を提示するエンドポイント脆弱性ビュー | ▪ ファブリック内の脆弱性が存在するホストを容易に特定します。 |
| IOC 検知 | ▪ IOC サービスの統合により、FortiAnalyzer の IOC 検知データを FortiView やトポロジーマップに表示 | ▪ 管理者が疑いのあるホストを容易に特定し、迅速または自動での隔離が可能になります。 |
| 無線 LAN コントローラ | ▪ 室内、屋外、およびリモートモデルを含むフォーティネットの広範な AP フォームファクター向けに統合された無線 LAN コントローラ（ライセンスやコンポーネントの追加料金は不要）<br>▪ 不正 AP からの保護、無線セキュリティ、監視、およびレポート作成などのエンタープライズクラスの無線 LAN 管理機能<br>▪ WAVE2 AP での 802.3az のサポート<br>▪ **新機能：**WiFi ロケーションマップ | ▪ FortiGate コンソールに統合された無線 LAN コントローラが、利便性と TCO 削減のメリットを提供する真の一元管理を実現します。 |
| スイッチコントローラ | ▪ フォーティネット製アクセススイッチ向けの統合スイッチコントローラ（追加のライセンスやコンポーネントは不要）<br>▪ GUI 構成サポートの強化 | ▪ アクセスレベルのセキュリティの拡張によって、ターミナル間の脅威の阻止と保護を実現します。 |
| WAN インタフェース マネージャ | ▪ USB ポートまたは FortiExtender（日本未発売）を介する 3G / 4G モデムのサポート | ▪ WAN 向けに 3G / 4G 接続の使用や追加を可能にするとともに、アクセス制御を維持してこれらのリンクの使用を定義できます。 |

# ハイライト

## 運用

FortiOS では、幅広い操作ツールが提供されているため、セキュリティとネットワークの問題を効率的に特定し、対応できます。自動化によってセキュリティ運用を最適化することで、問題解決の速度と精度がさらに向上します。

| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| 構成 | ▪ 多様な構成ツール：クライアントソフトウェア、WebUI、CLI<br>▪ 直感的で使いやすい最先端の GUI とウィザード<br>▪ ログビューアー、FortiView、ポリシーテーブルなどの間でのワンクリック操作によるアクセスとアクション<br>▪ インテリジェントなオブジェクトパネルによるポリシーのセットアップと編集<br>▪ インテント ベースト セグメンテーションのアセットのタグ付け | ▪ 管理者は独自の FortiExplorer 構成ツールを使用して、携帯電話やタブレットなどから構成に迅速にアクセスできます。<br>▪ VPN ウィザードにより、一般的なモバイルクライアントや他のベンダーの VPN ゲートウェイへのセットアップが容易になります。<br>▪ 便利なワンクリックのアクセスとアクションにより、管理者は素早く正確に手続きを進めることができるので、脅威の減災や問題解決を迅速に実行できます。 |
| ログおよびレポート | ▪ コンプライアンス、監査、および診断に不可欠な詳細なログと、導入後すぐに利用可能なレポート<br>▪ FortiAnalyzer と FortiCloud へのリアルタイムのログ記録<br>▪ CEF（共通イベント形式）のサポート<br>▪ セキュリティ ファブリック内のロギングの統合 | ▪ 送信元デバイスの詳細、強力な監査証跡を含む詳細なコンテキスト情報を提供します。<br>▪ GUI レポートエディターにより、レポートを詳細にカスタマイズできます。<br>▪ ログのホリスティック管理によって構成が簡素化され、すべての FortiGate の重要な情報を一元的に収集して分析に利用できるようになります。インテリジェンスのギャップが解消されます。 |
| 診断 | ▪ 診断用 CLI コマンド、セッショントレーサー、およびパケットキャプチャによるハードウェア、システム、およびネットワークのトラブルシューティング<br>▪ CLI のハードウェアテストスイート<br>▪ ポリシーとルーティングの GUI トレーサー | ▪ 包括的な診断ツールが、迅速に問題を減災したり異常状態を調査したりする上で役立ちます。 |
| 監視 | ▪ リアルタイム監視<br>▪ NOC ダッシュボード<br>▪ FortiExplorer アプリによる iOS プッシュ通知 | ▪ ダッシュボードの NOC ビューで、ミッションクリティカルな情報を常に表示できます。インタラクティブなドリルダウンウィジェットを利用することで、調査が行き詰まることなく迅速かつスムーズに分析を実行できます。 |

## ポリシーと制御

FortiGate がネットワークに提供する重要なポリシー実施ポイントでは、ネットワークトラフィックを制御してセキュリティテクノロジーを適用できます。FortiOS により、きめ細かなセキュリティ制御を含む統合ポリシーを設定できます。各セキュリティサービスは類似する制御パラダイムにより管理され、統合ポリシーに容易にプラグインできます。直感的なドラッグアンドドロップ操作でポリシーを容易に作成でき、ワンクリック操作のショートカットを使用してより迅速にエンドポイントを隔離したりポリシーを編集したりできます。

| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| ポリシーオブジェクト | ▪ GeoIP および FQDN で定義されたアドレスオブジェクトによる動的 IP / IP 範囲のインテリジェントな追跡<br>▪ インターネットサービス DB：ポリシーの設定、ルーティング、およびリンクのロードバランシング構成に使用可能な重要情報を一般的なクラウドアプリケーションに提供する DB を、動的にアップデート<br>▪ **新機能：** ファブリックコネクタ経由の動的なアドレスオブジェクト | ▪ 動的できめ細かな今日のネットワーク要件に対応する包括的なオブジェクトタイプを提供します。 |
| デバイスの識別 | ▪ ネットワーク上のさまざまなタイプのデバイスの識別<br>▪ **新機能：** MAC アドレスオブジェクト | ▪ 私物デバイスの識別により、今日の BYOD 環境に重要なセキュリティ機能を追加できるように企業を支援します。 |
| SSL インスペクション | ▪ SSL 暗号化トラフィックに含まれる AV や DLP などのさまざまなセキュリティ実装を効果的に評価<br>▪ コンテンツプロセッサによる高性能 SSL インスペクション<br>▪ 定評あるサイトのデータベースによる除外機能 | ▪ パフォーマンスに大きな影響を与えることなく、暗号化されたトラフィックに隠されている脅威を識別してブロックします。 |
| アクション | ▪ 送信元のオブジェクト、IP、ユーザー、および / またはデバイスの組み合わせを使用するセキュリティポリシーの実装<br>▪ ユーザーアクティビティが許可されない場合の通知を詳細にカスタマイズ<br>▪ ユーザー / 攻撃者の自動または手動の隔離<br>▪ 登録された FortiClient にホストの隔離を指示 | ▪ 追加の識別された要素やアクティブなユーザー通知を使用して、ポリシーを柔軟にセットアップします。これにより、効果的なネットワークセキュリティの実装が支援され、堅牢な隔離機能が脅威の減災に役立ちます。 |

# ハイライト

## セキュリティ

FortiGuard Labs は、フォーティネットソリューションからの業界をリードするセキュリティサービスと脅威のインテリジェンスを提供します。FortiOS は FortiGate プラットフォーム向けの広範な FortiGuard サービスを管理します。対象サービスには、アプリケーション制御、侵入防止、Web フィルタリング、アンチウイルス、高度な脅威保護、SSL インスペクション、およびモバイルセキュリティを含みます。サービスライセンスは、個別に、またはコスト効果の高いバンドルで利用できるので、導入の柔軟性を最大限に高めることができます。

### 業界をリードするセキュリティ効果

フォーティネットのソリューションは、NSS Labs（IPS およびアプリケーション制御）、Virus Bulletin（マルウェア対策比較テストの VB100）、および AV Comparatives による業界テストで、業界をリードするセキュリティ効果があることが継続的に実証されています。

- 次世代ファイアウォール（NGFW）として、ほぼ満点の 99.47% のセキュリティ効果の高評価を受け、「Recommended（推奨）」に認定（2017 年の NSS Labs による FortiGate 600D / 3200D の NGFW テスト）
- ブリーチ（情報セキュリティ侵害）防御システムとして、99% を超える高い総合評価を受け、「Recommended（推奨）」に認定（2017 年の NSS による FortiGate および FortiSandbox のブリーチ（情報セキュリティ侵害）防御システムテスト）
- データセンターセキュリティゲートウェイとして 97.87%、セキュリティ効果は 97.97% の高評価を受け、「Recommended（推奨）」に認定（2017 年の NSS による FortiGate 3000D / 7060E のデータセンターセキュリティゲートウェイテスト）
- 次世代 IPS として、99.71% のセキュリティ効果の高評価を受け、「Recommended（推奨）」に認定（2017 年の NSS 次世代 IPS テストにおける FortiGate 600D の評価）
- ICSA 認定のネットワークファイアウォール、ネットワーク IPS、IPsec、SSL-TLS VPN、アンチウイルス

| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| アンチマルウェア | ▪ フローベースおよびプロキシベースの AV オプションとして、保護機能やパフォーマンスを選択可能<br>▪ IP レピュテーション DB を使用するアンチボット保護がボットと C&C サーバーの通信を切断<br>▪ 外部のフォーティネットファイル分析ソリューション（FortiSandbox）から、動的な修正（不正ファイルのチェックサムと URL）DB のアップデートと詳細な分析レポートを受信<br>▪ プロアクティブな保護レイヤーである Virus Outbreak Protection Service の追加により、リアルタイムの FortiGuard チェックサムデータベースを利用して脅威を比較、検知し、新たなマルウェアもブロック<br>▪ コンテンツ無害化（CDR）により、ユーザーにエクスプロイト可能なコンテンツが到達する前に除去 | ▪ 業界で実証された実績ある AV リサーチサービスによってサポートされます。<br>▪ モバイルユーザーや支社も対象範囲に含む堅牢な ATP フレームワークを採用できます。これにより、暗号化ファイルを含む多様な経路からのファイルを評価し、従来の防御をバイパスする可能性のある高度な攻撃を検知して阻止します。 |
| IPS および DoS | ▪ ゼロデイ攻撃の脅威保護と効果的な IPS の実装の研究に支えられた、通常のシグネチャとレートベースのシグネチャ<br>▪ DoS に対する統合保護機能による、異常なトラフィックの挙動からの防御<br>▪ IPS シグネチャ向けの CVE の参照 | ▪ 卓越したカバレッジとコスト / パフォーマンスに対して NSS の「Recommended（推奨）」評価を獲得した、実証済みの高品質な保護を実現します。<br>▪ コンテキストの可視性などの完全な IPS と NGIPS の機能により、エンタープライズのニーズに対応します。<br>▪ スニファーモードなどの多様なネットワーク導入要件をサポートし、一部のモデルではアクティブバイパス機能を持つ FortiBridge または内蔵バイパス機能を持つポートとの互換性を提供します。 |
| アプリケーション制御 | ▪ ネットワーク使用状況を可視化しながら、アプリケーションに基づいてトラフィックの異常を検知し、アクションを実行<br>▪ SalesForce、Google Docs、Dropbox などの一般的なクラウドアプリケーションにおけるきめ細かな制御 | ▪ デスクトップおよびモバイルのアプリケーションの両方を含む広いカバレッジを対象として、ネットワークアクセスポリシーの管理を強化します。<br>▪ パブリッククラウドサービスを利用するエンタープライズが増加する中、より詳細なアプリケーションのインスペクションを適用して制御と可視性を向上します。 |
| Web フィルタリング | ▪ クオータ、ユーザーオーバーライド、透過的セーフサーチ、サーチエンジンのキーワードのログ管理を含む、エンタープライズクラスの URL フィルタリングソリューションを提供<br>▪ 広いカバレッジで 70 言語以上の URL レーティングを提供し、リダイレクト先（キャッシュおよび変換）サイトを識別 | ▪ 統合アプリケーション制御および IPS による多層型のアンチプロキシ回避機能により、Web の使用状況に対する隙のない制御機能の実装が可能です。 |

# ハイライト

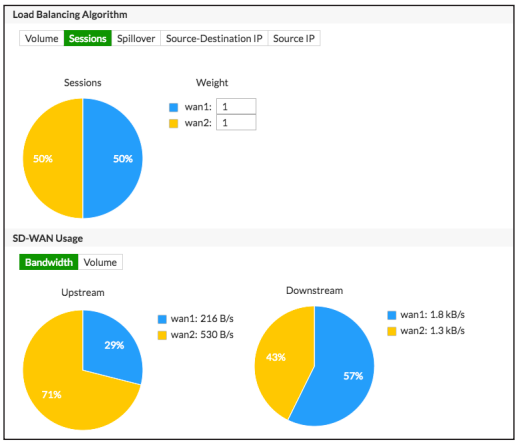
| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| ファイアウォール | ▪ SPU を搭載するアプライアンスによる高性能ファイアウォール<br>▪ 独自のセクションまたはグローバルビューのオプションを含む、使いやすいポリシー管理<br>▪ NGFW ポリシーベースモード | ▪ 優れた費用対効果をもたらす、業界トップレベルのファイアウォールアプライアンスです。 |
| VPN | ▪ さまざまなタイプの VPN セットアップに対応する包括的なエンタープライズクラスの機能<br>▪ 改善された SSL および IPsec VPN のウィザード<br>▪ **機能向上：**フルメッシュ、ハブ & スポークトポロジーをサポートするクラウド活用型オーバーレイコントローラ VPN（ADVPN オプションが必要） | ▪ FortiGate の比類ない VPN パフォーマンスによって、カスタムセキュリティプロセッサ（SPU）を活用してネットワークトラフィックの暗号化と復号を加速することで、複数のネットワークおよびホストの間で安全な通信を確立してデータの機密性を保持します。 |
| DLP | ▪ ネットワークトラフィックを監視し、ファイル形式とコンテンツの定義に対してマッチングを実行し、ネットワーク外への機密情報の漏えいを防止<br>▪ FortiExplorer のウォーターマーキングツールにより、DLP 向けにドキュメントのマーキングを適用 | ▪ TCO を抑えて、機密情報がネットワーク外に送信されないように防止します。 |
| メールフィルタリング | ▪ 誤検知率の低い効果的な多層型スパムフィルター | ▪ 小規模組織および支社向けとして、追加システムへの投資を必要とせずにコスト効率の高いアンチスパムソリューションを提供します。 |

## ネットワーキング

FortiOS を使用することで、FortiGate 上の一貫性のある単一のネイティブ OS でネットワークとセキュリティを管理できます。FortiOS は、広範なルーティング、NAT、スイッチ、Wi-Fi、WAN、ロードバランシング、および高可用性を含むさまざまなネットワーク機能を提供します。これにより FortiGate は、ネットワーク機能とセキュリティ機能の統合を目指す組織向けの選択肢として高い評価を受けています。

### SD-WAN

FortiGate SD-WAN は、次世代の WAN とセキュリティの機能を単一のマルチパス WAN エッジソリューションに統合します。セキュア SD-WAN によって、エッジアプリケーションの認識が可能になると同時に、内蔵された WAN パスコントローラ自動化機能が優れたアプリケーションパフォーマンスを保証します。NGFW の統合によって、インターネットへの容易な直接アクセスが可能となるため、複雑さを軽減するとともに強固なセキュリティ対策を維持できます。




| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| ルーティング / NAT | ▪ 包括的なルーティングプロトコルと NAT のサポート<br>▪ ICAP と WCCP のサポートによるトラフィックのリダイレクト | ▪ 通信事業者やエンタープライズにおけるネットワークの耐障害性要件に対応する広範なルーティング機能を提供します。 |
| L2 / スイッチング | ▪ インタフェースからのソフトウェアスイッチの作成および VLAN スイッチのエミュレーション<br>▪ 複数のインタフェースによる SPAN ポートとポートアグリゲーションのサポート<br>▪ 802.1x やキャプティブポータルなどのインタフェースでのアクセス制御モードの実装<br>▪ Wi-Fi および WAN インタフェースの包括的な構成オプション<br>▪ VXLAN のサポート<br>▪ EMAC VLAN サポート | ▪ 柔軟なインタフェース構成により、組織のネットワーク要件に適した多様なセットアップオプションを採用でき、さらにアクセスセキュリティのオプションを利用できます。 |
| オフラインインスペクション | ▪ スニファーモードにより、ネットワークアクティビティの脅威と使用状況の監視をオフラインで実行 | ▪ 既存の重要なネットワークにインラインでセキュリティソリューションを導入することがまだ適切ではない状況においては、オフラインモードで柔軟に対応できます。 |

# ハイライト

| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| SD-WAN | ▪ インテリジェント WAN パス制御により、アプリケーションおよびユーザー / ユーザーグループに基づいて WAN リンク間でトラフィックをダイレクト<br>▪ レイテンシ、ジッター、パケットロスなどのアプリケーショントランザクションを測定し、自動フェイルオーバーの内蔵によって優先パスを判断することで、ビジネスクリティカルアプリケーションの最適なアプリケーションパフォーマンスを実現<br>▪ **機能向上：**QoS、トラフィックシェーピング、およびポリシールーティングを帯域幅管理に使用<br>▪ **機能向上：**WAN リンクで IPsec VPN を可能にし、業界トップクラスの VPN パフォーマンスとトンネルの拡張性を実現<br>▪ **機能向上：**クラウド活用型 VPN オーバーレイコントローラ<br>▪ ピアツーピアおよびリモートユーザーの WAN 最適化とバイトキャッシングのテクノロジー | ▪ 幅広いアプリケーション可視性と先頭パケット分類による効率的な SD-WAN を実現します。<br>▪ NGFW と SD-WAN を同一アプライアンスに統合することで、TCO と複雑さのさらなる削減を可能にします。<br>▪ WAN パスコントローラの自動化により、優れたアプリケーションパフォーマンスを持続します。<br>▪ 業界トップクラスの IPsec VPN パフォーマンスを提供します。<br>▪ SD-WAN エッジのゼロタッチ展開が可能です。 |
| 高可用性 | ▪ 単一構成で複数の高可用性ソリューションの統合を実現し、業界標準の VRRP と多様な独自ソリューションをサポート | ▪ 柔軟な高可用性機能により、ネットワーク環境と SLA の要件に基づいて最適なソリューションを選択できます。 |
| IPv6 | ▪ ルーティング、NAT、セキュリティポリシーなどの包括的な IPv6 サポート | ▪ 既存のネットワークや重要ネットワークへの導入において柔軟な運用モードのオプションが選択可能で、ネットワーク変更の必要性を低減します。 |
| 明示的プロキシ | ▪ 1 つまたは複数のインタフェースでの IPv4 / IPv6 トラフィックの HTTP / HTTPS、FTP over HTTP、または SOCKS の明示的プロキシ<br>▪ トランスペアレント Web プロキシ | ▪ エンタープライズクラスの統合された明示的 Web プロキシにより、HTTP および HTTPS のプロキシを提供し、UTM のセキュリティとユーザー識別のメリットが追加されます。 |
| 基幹ネットワークサービス | ▪ DHCP、DNS サーバー、NTP サーバーなどの豊富なネットワークサービス | ▪ 導入後すぐに使用可能な組み込みの機能により、必要なネットワークサービスの内部ターミナルへの迅速な提供や、他のネットワークデバイスの統合も可能です。 |

## サポートするプラットフォーム

### パフォーマンス


FortiGate アプライアンスが実現するパフォーマンスは、次世代ファイアウォールの最大 5 倍、他のベンダーが提供する同等価格帯プラットフォームにおけるファイアウォールの 10 倍に達します。FortiGate の高いパフォーマンスは、FortiOS の最適経路プロセッシング（Parallel Path Processing）に基づきます。これは、パフォーマンス、最適化されたセキュリティエンジン、カスタムで開発されたネットワーク、およびコンテンツプロセッサを活用するアーキテクチャです。

### 比類のない導入の柔軟性

ポリシー ドリブンのネットワークセグメント化戦略に基づいて、フォーティネットソリューションを使用してネットワーク内外を保護します。多様な FortiGate プラットフォームを使用し、内部ネットワークセグメント、ネットワークの境界、分散するサイト、パブリッククラウド、プライベートクラウド、およびデータセンターを保護する FortiOS の柔軟性を活かすことにより、セグメントを最適化したファイアウォールを容易に導入でき、それぞれの導入モードに合わせて機能とパフォーマンスを適切に組み合わせることができます。

| 機能 | ハイライト | フォーティネットの優位性 |
|---|---|---|
| 物理アプライアンス（SPU 搭載） | ▪ アクセラレーションコンポーネント（SPU）やマルチコアプロセッサをはじめとする独自のハードウェアアーキテクチャとの統合 | ▪ ソフトウェアおよびハードウェアの優れた統合機能がハードウェアコンポーネントの最適な利用を実現し、費用対効果を最大限に向上させます。 |
| 仮想システム | ▪ 仮想ドメイン（VDOM）：仮想 FortiOS コンポーネントを単一の仮想または物理アプライアンス上の複数の論理システムに配置<br>▪ グローバルセキュリティプロファイル<br>▪ **新機能：**タスク分割をサポートする仮想ドメイン | ▪ MSSP や大規模組織は、マルチテナント環境向けに FortiOS の個別インスタンスを実行したり、さまざまなセキュリティゲートウェイを統合して TCO を削減したりできます。 |
| ハイパーバイザー | ▪ VMware vSphere、Citrix、およびオープンソースの Xen、KVM、および MS Hyper-V を含む一般的なハイパーバイザープラットフォームのサポート | ▪ 物理および仮想のアプライアンス間における一貫性のある管理と機能により、管理コストを削減して導入を簡素化します。 |
| クラウド | ▪ **機能向上：**パブリッククラウドサービスのサポート：Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP、Oracle Cloud Infrastructure（OCI）、AliCloud | ▪ 物理およびクラウドのプラットフォーム間における一貫性のある管理と機能により、管理コストを削減して導入を簡素化します。 |

# 技術仕様

## セキュリティ ファブリック

### システム統合

SNMP システムモニタリング：
- SNMP v1 および v2c をサポート
- SNMP v3 の実装は、クエリ、トラップ、認証、およびプライバシーのサポートを含みます。
- SNMP トラップがログディスクが満杯の場合や検知されたウイルスなどのイベントのアラートを通知

トラフィックモニタリング：
- sFlow バージョン 5, Netflow V9.0 および IPFIX

外部ログ管理：
- Syslog
- RFC 3195 に基づく信頼性の高い syslog（RAW プロファイル）
- WebTrends WELF との互換

テクノロジーエコシステムはファイアウォール / ネットワークリスク管理、SDN / 仮想化、セキュリティ情報 / イベント管理（SIEM）、システム統合、テストとトレーニング、および無線の各市場をリードするパートナーを包含します。

FortiSandbox、FortiSandbox Cloud、FortiMail、FortiMail Cloud、FortiCache、および FortiWeb とのネイティブ統合

セキュリティ ファブリックのロギング
- FortiAnalyzer 構成へのロギングを FortiGates 間で同期
- FortiAnalyzer とのデータ交換（トポロジーやデバイスのアセットタグなどの情報）

### 管理とプロビジョニングの一元化

一元管理サポート：FortiManager、FortiCloud ホストサービス、Web サービス API

迅速な導入展開：インストールウィザード、USB 自動インストール、ローカルおよびリモート環境でのスクリプト実行

### クラウドと SDN の統合

Openstack、VMWare NSX、Kubernetes、Nuage Virtualized Services Platform、Cisco ACI インフラストラクチャとの統合

### 可視性

ユーザー、デバイス、ネットワーク、およびセキュリティに関連するアクティビティ向けのインタラクティブでグラフィカルな可視化ツール（FortiView）：
-「送信元」、「送信先」、「インタフェース」、「アプリケーション」、「脅威」などの異なる視点を使用して現在および過去のステータスを表示する多様な GUI コンソール
- 脅威 / VPN マップ
- データ表示オプション：テーブル、バブルチャート、または世界地図（該当する場合）
- ファイル解析 / サンドボックス結果ビュー（FortiSandbox の統合が必要）
- エンドポイント脆弱性ビュー（FortiClient の統合が必要）
- FortiView の [All Sessions（全てのセッション）] コンソールでのセッション表示の高速化
- FortiView およびログテーブル内でのパブリック IP アドレスの WHOIS ルックアップ

物理 / 論理トポロジービューによる表示：
- セキュリティファブリックネットワーク内のホストの場所
- ホストの隔離、IP 制限、アクセス詳細コンテキスト情報へのワンクリックアクセス
- セキュリティファブリックエンティティ間の接続
- リンク使用などの SD-WAN 関連情報

セキュリティ ファブリック内のダウンストリームの FortiGate による集約データビュー
- FortiView、トポロジー、モニターに表示

### 自動化

シンプルな if-then セットアップを使用して、セキュリティ ファブリック内に自動化を定義：
- トリガー：IOC 検知、システムステータス、構成変更、FortiAnalyzer イベントハンドラーおよびスケジュール
- アクション：CLI スクリプト、パブリッククラウドの機能、通知、API コール / Web フック

FortiAP や FortiSwitch、または EMS 経由の FortiClient により、リモートホストをアクセスレイヤーで自動的に隔離

### AAA（認証、認可、アカウンティング）

サポートするローカルユーザーデータベースおよびリモートユーザー認証サービス：LDAP、Radius および TACACS+、二要素認証

シングルサインオン：Windows AD、Microsoft Exchange Server、Novell eDirectory、FortiClient、Citrix およびターミナルサーバーエージェント、Radius（アカウンティングメッセージ）、POP3 / POP3S、ユーザーアクセス（802.1x、キャプティブポータル）による認証との統合

PKI および証明書：X.509 証明書、SCEP サポート、署名要求（CSR）作成、証明書の失効前自動更新、OCSP サポート

物理、SMS およびソフトウェア OTP（ワンタイムパスワード）トークンのプロビジョニングを行う統合トークンサーバー

### コンプライアンスとセキュリティレーティング

一連のシステム構成のコンプライアンスチェックとログ結果を定期的またはオンデマンドで実行

セキュリティ ファブリックの評価：ファブリック内のコンポーネントがベストプラクティスと照合されて監査されるため、ユーザーが一部のアイテムに修復手順を容易に適用可能

クライアントソフトウェア経由でネットワークデバイスのコンプライアンスを管理：
- セキュリティ状態のチェック：デバイスの種類 / グループ、ユーザー / ユーザーグループ、場所（IP）などに応じて、クライアントソフトウェアのインストールと任意の設定を適用
- 脆弱性レベルのしきい値に達したクライアントを隔離

### 高度な脅威保護（ATP）

外部のクラウドベースまたはオンプレミスのファイル分析（OS 非依存のサンドボックス）に統合：
- ファイル送信（タイプ選択オプションあり）
- ファイル分析レポートの受信
- ファイル分析システム（ファイルのチェックサムと不正 URL の DB）からの動的なシグネチャアップデートの受信

ドメイン名、Web フィルタリング URL、IP アドレス、マルウェアハッシュに関する外部のブロックリストのサポート

### 脆弱性の評価

脆弱性が存在するホストとその脆弱性のリストをテレメトリ経由で FortiClient を使って表示

### IOC 検知

感染したホストのリストを FortiAnalyzer から提供される情報を使って表示

### 無線 LAN コントローラ

ローカルあるいはリモートのシンアクセスポイントやスイッチ（一部モデル）の設定のプロビジョニングと管理

SSID および VLAN 用のアクセスと認証メソッドを設定。統合された、あるいは外部のキャプティブポータル、802.1x、事前共有キーをサポート

WPA Personal の複数の PSK

無線 LAN のセキュリティ：不正なアクセスポイントの停止、無線 LAN IDS、フィッシング SSID の監視および停止

WiFi のトラブルシューティングツールおよびロケーションマップ

サポートする無線 LAN トポロジー：高速ローミング、AP 負荷分散、無線 LAN メッシュおよびブリッジ

無線 LAN コントローラ間のフェイルオーバーの制御

### スイッチコントローラ

フォーティネット製スイッチ（FortSwitch）を CAPWAP に類似する通信によって管理することで、アクセス制御とセキュリティを有線デバイスに拡張

隔離された VLAN のプロビジョニング

PoE、VLAN の割り当てなどの多様なスイッチポート機能を GUI から構成可能

### WAN インタフェースマネージャ

USB 3G / 4G 無線 WAN モデムをサポート

## 操作

### 構成

管理用アクセス：Web ブラウザ経由の HTTPS、SSH、telnet、コンソール

FortiExplorer：
- iOS プラットフォームの管理クライアント
- USB 接続の使用による利便性
- モバイル通知を（自動化機能の一部として）提供

機能ストア：GUI コンポーネント表示の切り替え

タグを作成することで（複数の管理者が定義するカテゴリに基づく）、ネットワークオブジェクト、インタフェース、デバイスを分離し、分類

GUIによる構成：
-「ワンクリック」アクセスにより、管理者が素早く手続きを進めることが可能
- 動的なオブジェクトセレクターと予測型の検索クエリ

サポートする管理用Web UI言語：英語、スペイン語、フランス語、ポルトガル語、日本語、簡体字中国語、繁体字中国語、韓国語

### ログおよびレポート

サポートするログ用設備：ローカルメモリおよびストレージ（利用可能な場合）、複数のsyslogサーバー、FortiAnalyzer、WebTrendsサーバー、FortiCloudホステッドサービス

TCPオプション（RFC 3195）を使用した信頼性の高いロギング

FortiAnalyzerを利用するログの暗号化とログの整合性

ログのバッチアップロードのスケジュール化、リアルタイムのロギング

詳細なトラフィックログ： フォワードされたトラフィック、侵害されたセッション、ローカルトラフィック、無効なパケット

総合的なイベントログ：システムおよび管理者のアクティビティ監査、ルーティングおよびネットワーク、VPN、ユーザー認証、無線関連イベント

トラフィックログの要約オプション

# 技術仕様

CEF（共通イベント形式）でログをsyslogサーバーに送信

IPおよびサービスポート名の解決オプション

### 診断

診断用CLIコマンド、セッショントレーサー、およびパケットキャプチャによるハードウェア、システム、およびネットワークのトラブルシューティング

ポリシーとルーティングのGUIトレーサー

パケットフローのCLIトレーサー

CLIのハードウェアテストスイート

### 監視

グラフィカルモニター：リアルタイムのシステム、ネットワークサービス、およびユーザーに関するステータスビューアー

ダッシュボード：ウィジェットとレイアウトのカスタマイズが可能

## ポリシーと制御

### ポリシーオブジェクト

ポリシーオブジェクト:事前定義済、独自作成、オブジェクトのグループ化、タグ付け、色分け

アドレスオブジェクト：サブネット、IP、IPレンジ、GeoIP（地域）、FQDN

インターネットサービス DB：ポリシーのセットアップ、ルーティング、およびリンクのロードバランシング構成に使用可能な重要情報を一般的なクラウドアプリケーションに提供する DB を動的にアップデート

### デバイスの識別

デバイスの識別：デバイスおよび OS のフィンガープリント、自動分類、インベントリ管理

MAC認証の実施とバイパスのサポート

### SSL インスペクション

IPS、アプリケーション制御、アンチウイルス、WebフィルタリングおよびDLP向けのSSL暗号化されたトラフィックの検査オプション

SSl MITMミラーリング

SSLインスペクション方式のオプション：SSL証明書インスペクションまたはSSLディープインスペクション

サイトレピュテーションDB、Webカテゴリ、および / またはポリシーアドレスによるSSLインスペクションの除外

### アクション

ユーザー通知:ブロックサイトおよび添付ファイル向けのカスタマイズ可能な代替メッセージ

Webブラウザのトップバナーの挿入（フォーティネットバー）：アプリケーション制御の違反、エンドポイント制御の実施、Web閲覧クオータなどを表示

ユーザーの隔離：
- 手動で永続またはカスタマイズ可能な期間を割り当て
- 違反IPSシグネチャのトリガーにより自動的に割り当て

## セキュリティ

### アンチマルウェア

グローバルIPレピュテーションデータベースを活用するボットネットサーバーのIPブロック

ウイルス対策データベースタイプの選択（一部のモデル）

VOR（Virus Outbreak Protection：ウイルスアウトブレイク防止）データベースのクエリ：AVシグネチャ公開前に新たに検知された脅威のリアルタイムチェックサムDBを使用

CDR（Content Disarm and Reconstruction：コンテンツ無害化）オプション：
- AVエンジンが、ユーザーに渡される前にすべてのアクティブコンテンツをリアルタイムで削除
- オリジナルファイルをさらなる分析、隔離、または破棄の目的でサンドボックスに転送

フローベースまたはプロキシベースのAVオプション：
- 一般的なWeb、メール、およびFTPプロトコルのサポート
- SSLインスペクションによる暗号化トラフィックのスキャン

メール添付のWindows実行ファイルをウイルスとして処理するオプション

ファイルの隔離（ローカルストレージが必要）

### IPS および DoS

IPSエンジン：7,000以上の最新シグネチャ、プロトコルアノマリ型検知、レートベース検知、カスタムシグネチャ、マニュアルまたは自動のプル / プッシュ式シグネチャアップデート、脅威エンサイクロペディアの統合

IPSアクション：有効期限付きのデフォルト、監視、ブロック、リセットまたは隔離（攻撃者のIP、攻撃者のIPおよび被害者のIP、侵入インタフェース）

フィルターベースの選択：深刻度、標的、OS、アプリケーション、プロトコル

パケットのログ記録オプション

指定したIPSシグネチャからのIP除外

IPv4およびIPv6のTCP Synフラッド、TCP / UDP / SCTPポートスキャン、ICMPスィープ、TCP / UDP / SCTP / ICMPセッションフラッド（送信元 / 送信先）に対するしきい値設定が可能なレートベースDOS検知（一部モデルを除く）

IDSスニファーモード

バイパスインタフェース（一部モデル）およびFortiBridgeを使用するアクティブバイパス機能

### アプリケーション制御

18 カテゴリにおよぶ数千規模のアプリケーションを検知：ビジネス、クラウド、IT、コラボレーション、E メール、ゲーム、一般向けアプリケーション、モバイル、ネットワークサービス、P2P、プロキシ、リモートアクセス、ソーシャルメディア、ストレージ / バックアップ、アップデート、ビデオ / オーディオ、VoIP、Web チャット、産業アプリケーション

独自のアプリケーションシグネチャをサポート

HTTP / 2 プロトコルを使用するトラフィックの検知をサポートし、QUIC トラフィックをブロックできるため、ブラウザは自動的に HTTP / 2 + TLS 1.2 へフォールバック可能

フィルターベースのオーバーライド：挙動、カテゴリ、評判、テクノロジー、リスク、ベンダー、プロトコルによる

アクション：許可、ブロック、セッションのリセット（CLI のみ）、監視のみ

SSH インスペクション

SalesForce、Google Docs、Dropbox などの一般的なクラウドアプリケーションでのきめ細かなアプリケーション制御

### Web フィルタリング

サポートする Web フィルタリング検査モード：プロキシベース、フローベース、および DNS

独自に定義した URL、Web コンテンツおよび MIME ヘッダーによる Web フィルタリング

クラウドベースのリアルタイム分類データベースによる動的 Web フィルタリング：
- 78 のカテゴリに評価分類された、70 の言語の 2 億 5 千件以上の URL データベース

セーフサーチの適用：クエリに対して透過的にセーフサーチパラメータを挿入。Google、Yahoo!、Bing および Yandex、教育機関向けに定義可能な YouTube フィルターをサポート

プロキシ回避の禁止：プロキシサイトのカテゴリのブロック、ドメインおよび IP アドレスによる URL 評価、キャッシュおよび翻訳サイトからのリダイレクトのブロック、プロキシ回避アプリケーションのブロック（アプリケーション制御）、プロキシビヘイビアのブロック（IPS）

Web フィルタリングのローカルカテゴリおよびカテゴリ評価リストの上書き

Web フィルタリングプロファイルの上書き：管理者が特定のユーザー / ユーザーグループ / IP に対して異なるプロファイルを一時的に割り当て可能

複数の外部ブラックリストをサポート

Google コーポレートアカウントへのアクセスのみに制限

プロキシベースのWebフィルタリングのその他の機能：
- Javaアプレット、ActiveX、および/またはクッキーのフィルタリング
- HTTP POST攻撃のブロック
- 検索キーワードのログ記録
- URL別の画像評価
- 評価に基づくHTTPリダイレクトのブロック
- プライバシー保護の目的で、特定のカテゴリの暗号化された接続をスキャン対象から除外
- カテゴリ別のWebブラウジングクォータ設定

### ファイアウォール

動作モード：NAT / ルートおよびトランスペアレント（ブリッジ）

スケジュール：ワンタイム、繰り返し

セッションヘルパーおよび ALG：DCE / RPC、DNS-TCP、DNS-UDP、FTP、H.245 I、H.245 0、H.323、MGCP、MMS、PMAP、PPTP、RAS、RSH、SIP、TFTP、TNS（Oracle）

VoIP トラフィックのサポート：SIP / H.323 / SCCP NAT トラバーサル、RTP ピンホーリング

サポートするプロトコル：SCTP、TCP、UDP、ICMP、IP

ユーザー / デバイス別のポリシー

ポリシー管理：セクション別 / グローバルのポリシー管理ビュー

NGFW ポリシーモード：アプリケーションおよび URL をオブジェクトとして使用してポリシーをセットアップ

### VPN

カスタマイズ可能な SSL VPN ポータル：カラーのテーマ、レイアウト、ブックマーク、接続ツール、クライアントダウンロード

サポートする SSL VPN アドレス体系：ユーザーグループに関連付けられた複数のカスタム SSL VPN ログインが可能（URL パス、デザイン）

シングルサインオンブックマーク：以前のログインまたは事前定義された認証情報を再利用し、リソースへアクセス可能

パーソナルブックマークの管理：管理者がリモートクライアントのブックマークを参照および維持可能

SSL ポータルの同時ユーザー数制限

ユーザー別のワンタイムログインオプション：同じユーザー名を使用する同時ログインを禁止

SSL VPN Web モード:Web ブラウザのみを装備するシンリモートクライアント向け。次のアプリケーションをサポート：HTTP / HTTPS Proxy、FTP、Telnet、SMB / CIFS、SSH、VNC、RDP、Citrix

SSL VPN トンネルモード：幅広いクライアント / サーバーアプリケーションを実行するリモートコンピュータ向け。SSL VPN クライアントは MAC OSX、Linux、Windows Vista および 64-bit の Windows オペレーティングシステムをサポート

# 技術仕様

SSL VPN ポートフォワーディングモード：ユーザーのコンピュータのローカルポートで接続を待受けする Java アプレットを使用。Java アプレットがクライアントアプリケーションからデータを受信すると、ポートフォワードモジュールがデータを暗号化して SSL VPN デバイスに送信し、続いてアプリケーションサーバーにトラフィックをフォワードします。

SSLトンネルモードの接続前のホスト整合性チェックおよび OS チェック（Windows ターミナル向け）

ポータル毎の MAC ホストチェック

SSL VPN セッション終了直前のキャッシュクリアオプション

クライアントコンピュータのデスクトップ環境から SSL VPN セッションを分離する仮想デスクトップオプション

IPsec VPN：
- サポートするリモートピア：IPsec 準拠ダイヤルアップクライアント、静的 IP / ダイナミック DNS のピア
- 認証メソッド：証明書、事前共有キー
- IPsec フェーズ 1 モード：アグレッシブモードおよびメイン（ID 保護）モード
- ピア受入れオプション：すべての ID、特定の ID、ダイヤルアップユーザーグループの ID
- IKEv1、IKEv2（RFC 4306）をサポート
- IKE モードの構成をサポート（サーバーまたはクライアントとして）、DHCP over IPsec
- フェーズ 1 / フェーズ 2 プロポーザル暗号化：DES、3DES、AES128、AES192、AES256
- フェーズ 1 / フェーズ 2 プロポーザル認証：MD5、SHA1、SHA256、SHA384、SHA512
- サポートするフェーズ 1 / フェーズ 2 Diffie-Hellman Group 番号：1、2、5、14
- クライアントまたはサーバーモードで XAuth をサポート
- ダイヤルアップユーザー向け XAuth：サーバータイプオプション（PAP、CHAP、Auto）、NAT トラバーサルオプション
- IKE 暗号キー有効期限、NAT トラバーサルのキープアライブ頻度を設定可能
- デッドピアディテクション（DPD）
- リプレイ検知
- フェーズ 2 SA 向けの AutoKey キープアライブ

一般的なサードパーティ製デバイスによる終端を構成する IPsec 構成ウィザード

クラウド活用型オーバーレイ コントローラー VPN：容易な構成
- ハブ & スポーク VPN
- メッシュ VPN（ADVPN オプションが必要）

IPsec VPN 導入モード：ゲートウェイツーゲートウェイ、ハブ & スポーク、フルメッシュ、冗長トンネル、トランスペアレントモードにおける VPN 終端

IPsec VPN 構成オプション：ルートベースまたはポリシーベース

VPN モニタリング：IPsec および SSL VPN 接続の詳細表示と管理が可能

サポートするその他の VPN：L2TP クライアント（一部のモデル）およびサーバーモード、L2TP over IPsec、PPTP、GRE over IPEC

### DLP

サポートする Web フィルタリング検査モード：プロキシベース、フローベースおよび DNS

DLP メッセージフィルター：
- サポートするプロトコル：HTTP-POST、SMTP、POP3、IMAP、MAPI、NNTP
- アクション：ログ記録のみ、ブロック、ユーザー / IP / インタフェースの隔離
- 事前定義済フィルター：クレジットカード番号、ソーシャルセキュリティ ID 番号

DLP ファイルフィルター：
- サポートするプロトコル：HTTP-POST、HTTP=-GET、SMTP、POP3、IMAP、MAPI、FTP、NNTP
- フィルターオプション：サイズ、ファイルタイプ、ウォーターマーク、コンテンツ、暗号化の有無

DLP ウォーターマーキング：FortiGate を通過し、ウォーターマーク内に隠された企業識別子（テキスト文字列）および重要度レベル（クリティカル、プライベートおよび警告）を含んでいるファイルのフィルタリングが可能。Windows および Linux 向けの無償ウォーターマーキングツールをサポート

DLP フィンガープリンティング：捕捉されたファイルからチェックサムフィンガープリントを生成し、フィンガープリントデータベースと比較

DLP アーカイビング：E メール、FTP、IM、NNTP および Web トラフィックのコンテンツすべてを記録

### メールフィルタリング

メールプロトコルのサポート：IMAP（S）、POP3（S）、および SMTP（S）

アンチスパム DB のクエリ：IP アドレスチェック、URL チェック、メールのチェックサム

ローカルのスパムフィルタリング：HELO DNS ルックアップ、返信メールの DNS チェック、およびブラックリスト / ホワイトリスト

## ネットワーク機能

### ルーティング / NAT

静的ルーティングおよびポリシーベースのルーティング

動的ルーティングプロトコル：RIPv1 および v2、OSPF v2 および v3、ISIS、BGP4

コンテンツのルーティング：WCCP および ICAP

NAT 構成：ポリシーベース別および中央の NAT テーブル

サポートする NAT：NAT64、NAT46、静的 NAT、動的 NAT、PAT、フルコーン NAT、STUN

マルチキャストトラフィック：スパースモードおよびデンスモード、PIM 対応

### L2 / スイッチング

レイヤー 2 のインタフェースモード：ポート集約、ループバック、VLAN（802.1Q およびトランキング）、仮想ハードウェア、ソフトウェアおよび VLAN スイッチ

VXLAN のサポート：
- interVTEP（VXLAN トンネルエンドポイント）
- 複数のリモート IP（IPv4 ユニキャスト、IPv6 ユニキャスト、IPv4 マルチキャスト、または IPv6 マルチキャスト）をサポート

EMAC-VLAN サポート：複数のレイヤー 2 アドレス（または Ethernet MAC アドレス）の単一物理インタフェースへの追加が可能

仮想ワイヤペア
- 同一ネットワークセグメントの指定された 2 つのインタフェース間でのみトラフィックを処理
- トレンスペアレントおよび NAT / ルートの両モードで使用可能
- ワイルドカードによる VLAN のセットアップを実装するオプション

### オフラインインスペクション

スニファーモード：専用のインタフェースで、そのインタフェースに入るすべての受信トラフィックをスニファーが処理

オフラインのセキュリティインスペクション：AV、Webフィルタリング、アプリケーション制御、IPS、およびアンチスパム

### SD WAN

WANロードバランシング（重み付け）のアルゴリズム：ボリューム、セッション、送信元-送信先IP、送信元IP、およびスピルオーバーによる

SLAのためのWANリンクのチェック：
- PingまたはHTTPプローブ
- レイテンシ、ジッター、パケットロスなどのモニタリング基準
- チェック間隔、障害、フェイルバックのしきい値を構成可能
- クラウドベースのSD-WAN帯域幅監視サービス

以下の要素で定義したルールによるマルチパスインテリジェンス：
- 送信元アドレスやユーザーグループ
- 送信先アドレスや指定したアプリケーション(3,000以上のアプリケーションから選択可能)
- 特定のリンク品質基準やSLAの定義を使用したパス選択

ポリシーまたはアプリケーション別のトラフィックシェーピングおよびQoS：共有ポリシーによるシェーピング、Per-IPシェーピング、最大 / 保証帯域幅、IP毎の最大同時接続、トラフィックの優先付け、Type of Service（TOS）、Differentiated Services（DiffServ）、およびVPNサポート用のForward Error Correction（FEC）

分類されたトラフィック別にインタフェース帯域幅の割合を定義することでトラフィックシェーピングプロファイルを設定し、インタフェースにバインドするオプション

トラフィックシェーピングポリシー：送信元、送信先、サービス、アプリケーション、アプリケーションカテゴリ、および / またはURLカテゴリに基づいて一致するポリシーによるトラフィックシェーピングプロファイルの割り当て

DSCPのサポート：
- SD-WANルールのDSCP一致
- 特定されたアプリケーションに基づく、転送パケットのDSCPタグ設定

インラインおよびアウトオブパス型のWAN最適化トポロジー、ピアツーピアおよびリモートクライアントをサポート

トランスペアレントモードオプション:パケットの本来の送信元アドレスを維持するため、サーバーはクライアントから直接トラフィックを受信しているように見えます。

WAN最適化技術：プロトコル最適化およびバイトキャッシング

サポートするWAN最適化プロトコル：CIFS、FTP、HTTP、HTTPS、MAPI、TCP

セキュアなトンネリングオプション：AES-128bit-CBC SSLを使用して、WAN最適化トンネルのトラフィックを暗号化

トンネル共有オプション：複数のWAN最適化セッション間で同じトンネルを共有

Webキャッシング:帯域幅使用量、サーバーの負荷およびユーザーが認識するレイテンシを低減することで、Webアプリケーションおよびwebサーバーの処理を高速化するオブジェクトキャッシング機能を提供。HTTP 1.0およびHTTP 1.1のWebサイトのキャッシングをサポート

WebキャッシングによるSSLオフロード：
- フルモード：HTTPSトラフィックの暗号化と復号の両方を実行
- ハーフモード：暗号化または復号のいずれかのみを実行

URLパターンによって特定のWebサイトをWebキャッシング対象から除外するオプションを選択可能

高度なWebキャッシング構成とオプションをサポート：
- 常時再確認、キャッシュするオブジェクトの最大サイズ、否定応答持続時間、フレッシュファクター、最大/最小/デフォルト TTL、プロキシFQDN、最大HTTPリクエスト/メッセージサイズ、無視オプション、キャッシュの有効期限切れオブジェクト、再確認されたprama-no-cache

WAN最適化およびWebキャッシュの監視

### 明示的プロキシ

明示的WebプロキシとFTPプロキシ：1つ以上のインタフェースでFTP、HTTPおよびHTTPSプロキシを実行

プロキシ自動構成（PAC）：明示的Webプロキシユーザー向けに自動的にプロキシを構成

プロキシチェーン：Webプロキシセッションを別のプロキシサーバーにリダイレクトするWebプロキシフォワーディング

Webプロキシフォワーディングサーバーの監視とヘルスチェック

IPリフレクト機能

# 技術仕様

プロキシフォワーディングおよびプロキシチェーンの負荷分散

明示的Webプロキシ認証：IPベース認証およびセッション毎認証

トランスペアレントWebプロキシ

### IPv6

IPv6のサポート：IPv6経由の管理、IPv6ルーティングプロトコル、IPv6トンネリング、IPv6トラフィック向けファイアウォールとUTM、NAT46、NAT64、IPv6 IPsec VPN

IPv6 SD-WANサポート：Ping6リンクモニター、IPv6送信元 / 送信先オブジェクト

### 高可用性

高可用性モード：アクティブ / アクティブ、アクティブ / パッシブ、仮想クラスタ、VRRP、FortiGate 5000シリーズのクラスタリング

冗長ハートビートインタフェース

HA用予約済管理インタフェース

フェイルオーバー：
- ポート、ローカルおよびリモートのリンクモニタリング
- ステートフルフェイルオーバー
- 1秒未満の即時フェイルオーバー
- 障害検知の通知

導入オプション：
- リンクアグリゲーションによるHA
- フルメッシュ接続によるHA
- 地理的な分散によるHA

スタンドアロンのセッション同期

### 基幹ネットワークサービス

DHCP、NTP、DNSサーバー、DNSプロキシ内蔵

FortiGuard NTP、DDNS、およびDNSサービス

## サポートするプラットフォーム

### 物理アプライアンス（SPU 搭載）

SPUコンポーネントとの統合によりトラフィック処理を加速

### 仮想システム

仮想システム（FortiOS仮想ドメイン）は、単体のFortiGateユニットを分割して、個別に機能し独立して管理可能な複数の仮想インスタンスまたはFortiOSを作成します。

「アクティブセッション」とログディスククオータの上限 / 保証など、構成可能な仮想システムリソースの制限と管理

VDOMの動作モード：NAT / ルートまたはトランスペアレント

タスク分割をサポートする仮想ドメイン：管理およびデータパス用に仮想ドメインを分離

### ハイパーバイザー

VMware vSphere、Citrix、およびオープンソースのXen、KVM、およびMS Hyper-Vを含む一般的なハイパーバイザープラットフォームのサポート

### クラウド

Amazon AWS：自動スケーリング、ELBによるネイティブHA、AZをまたぐHA、GuardDutyとの統合； IAM、トポロジーおよびCVEの統合

Microsoft Azure：自動スケーリング、ネイティブHA（Azure LB）、Azure Security Centerとの統合
Azure Stack：アクティブ - パッシブHA

Google Cloud Plaform：自動スケーリング、ゾーン間をまたぐHA

Oracle Cloud Infrastructure：ネイティブおよび準仮想化モード、IAMの統合

AliCloud：自動スケーリング、ネイティブHA

## その他

### その他

Webアプリケーションファイアウォール：
- シグネチャベース、URL制限、およびHTTPメソッドのポリシー

サーバーのロードバランシング：複数のバックエンドサーバー全体でトラフィックを分散
- 静的（フェイルオーバー）、ラウンドロビン、重み付けを含む複数の手法に基づく、またはラウンドトリップタイム、接続数に基づく
- HTTP、HTTPS、IMAPS、POP3S、SMTPS、SSL 、あるいは汎用TCP / UDPまたはIPプロトコルをサポート
- セッションパーシステンスは、SSLセッションIDまたは挿入されたHTTP Cookieに基づいてサポート

注：FortiOS 6.2 GAの機能を紹介しており、一部の機能はすべてのモデルに該当しない場合があります。機能の提供状況については、docs.fortinet.com でソフトウェア機能一覧をご覧ください。

# リソース

| リソース | URL |
|---|---|
| FortiOS — Fortinet Docs Lobrary（フォーティネットドキュメントライブラリ） | https://docs.fortinet.com/product/fortigate/6.2 |
| フォーティネットのナレッジベース | http://kb.fortinet.com/ |

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.co.jp/contact

お問い合わせ