

# FORTINET®

## 総合カタログ

時代は統合セキュリティへ



# ますます多様化・複雑化する脅威、増加するばかりのコスト……。ネットワークセキュリティで悩むのなら、フォーティネットこそが最良の選択です。

フォーティネットは、いまやネットワークセキュリティの主役であるUTM(統合脅威管理)のパイオニアであり、リーディング企業です。

世界はもちろん、日本においてもUTM市場シェアNo.1を誇り、すでに全世界で10万社以上に導入されています。

その製品群もUTMの代名詞であるFortiGateに加えて、

効率のよい管理をサポートするFortiAnalyzerやFortiManager、

各領域に特化してより強固な防御を可能にする FortiMail、FortiWebなど大きく広がり、

社内ばかりでなくモバイル環境、さらにはクラウド環境にも柔軟に対応する

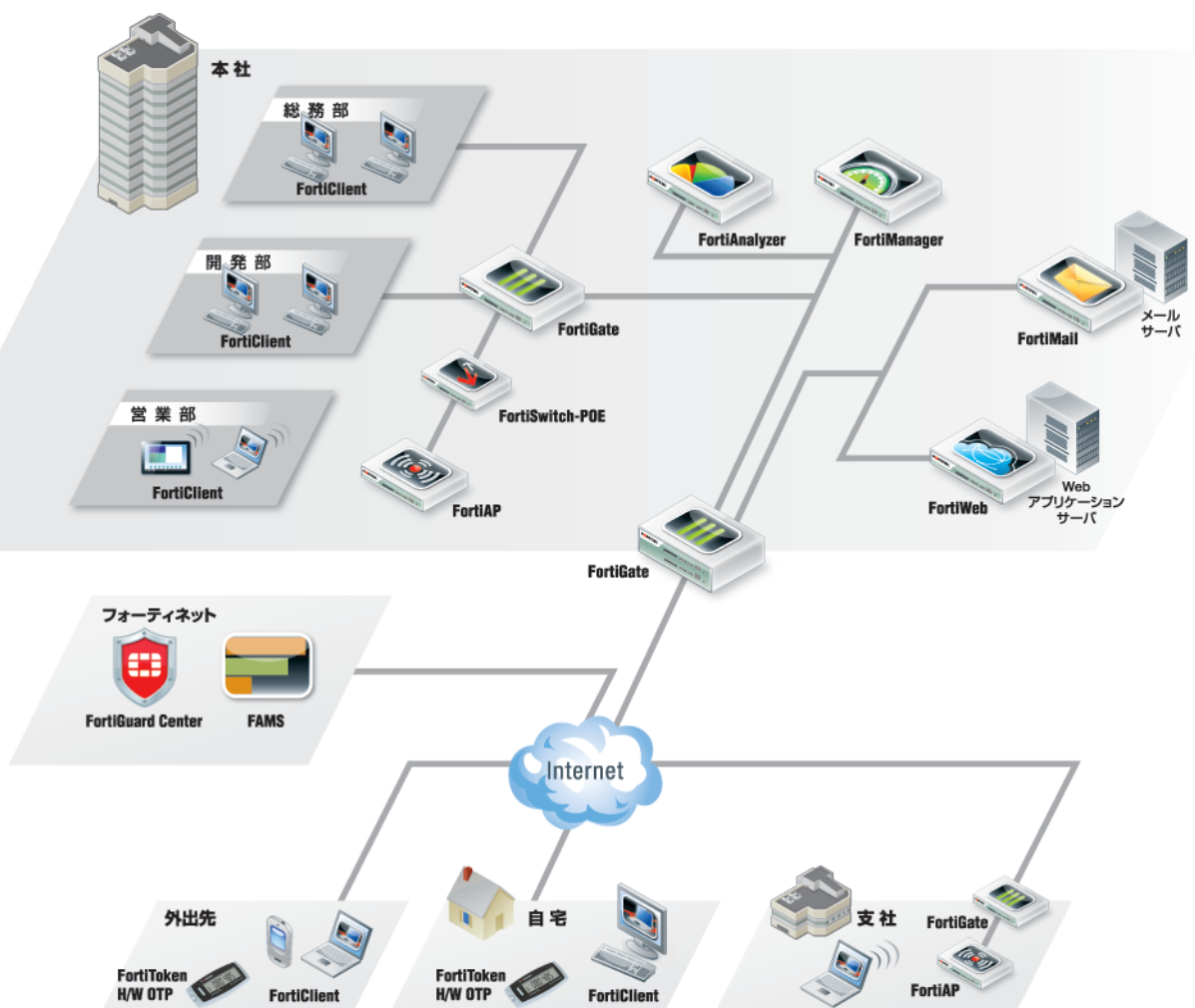
先進のセキュリティソリューションを提供しています。

ますます多様化・複雑化するネットワークへの脅威。さらに増大の一途をたどるセキュリティコスト。

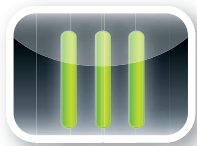
支店やリモートオフィスといった拠点から、大規模企業、さらにはサービスプロバイダまで、

ネットワークセキュリティで悩むならば、その答えは必ずフォーティネットにあります。

## ■フォーティネット製品の構成イメージ



フォーティネットは、SOHOから大企業、さらにデータセンターやMSSP事業者まで、それぞれのネットワーク規模に応じた製品を幅広くラインアップしています。また、モバイルからクラウドまで最新のネットワーク環境に対応。お客様の規模や環境に合わせて最適な製品を導入できます。



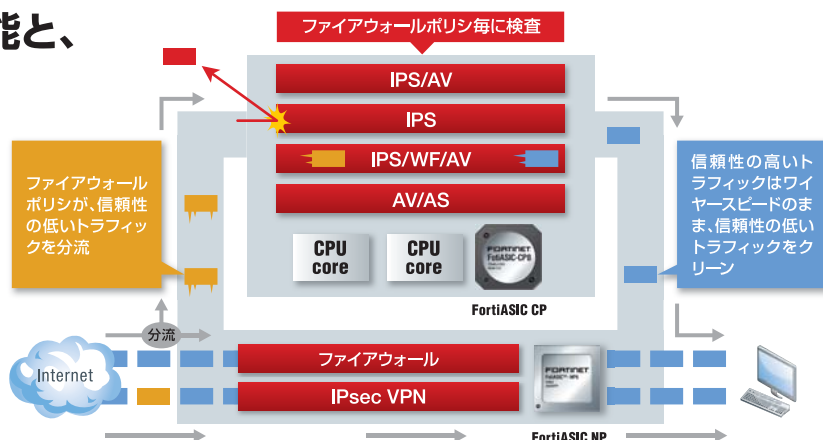
# FortiGate

ますます高度化・巧妙化する脅威。増大するばかりのセキュリティ・コスト。  
世界で、そして日本で市場シェアNo.1のFortiGateが、企業ネットワークが直面する課題を速やかに解決します。

## 高速

### 世界最速の驚異的な性能と、

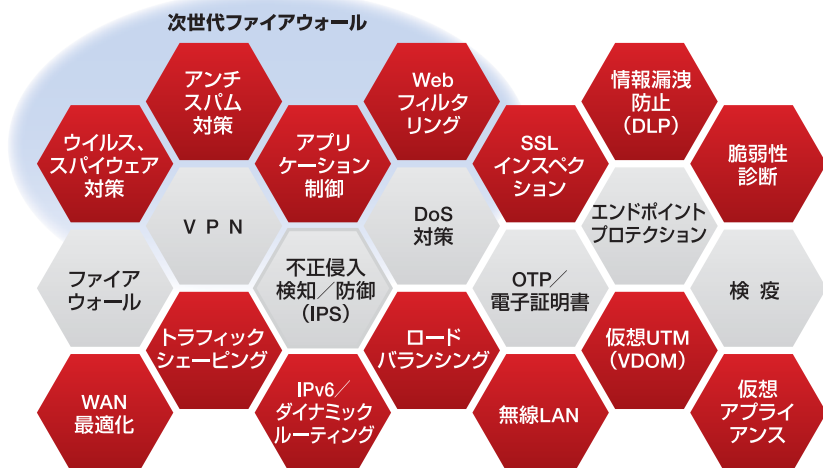
UTMのパフォーマンスはその心臓部であるプロセッサによって決まります。FortiGateは、独自に開発した専用プロセッサFortiASICを搭載。他社を凌駕する圧倒的なパフォーマンスを実現しています。一般的なUTMは、汎用プロセッサを採用しているために当然、性能に限界があります。フラッグシップモデルであるFortiGate-5000シリーズのファイアウォールスループットは世界最速の480Gbps。同時セッション数は1億3,200万という驚異的なパフォーマンスを達成しています。



## 多機能

### フルラインの多彩な機能を、

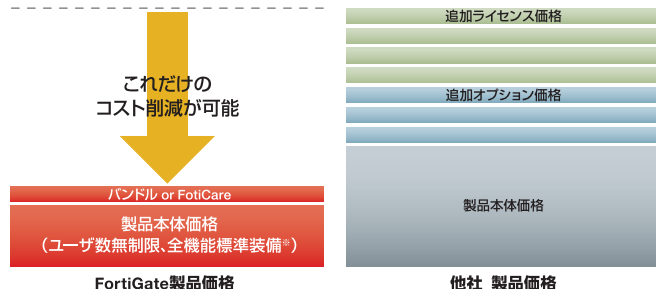
FortiGateは、ウイルス/スパイウェア対策、スパム対策、アプリケーション可視化と制御、Webフィルタリングから無線LANコントローラや仮想UTMまで、フルラインのセキュリティ機能とネットワーク機能をすべて1台の製品に統合しています。ハードウェア、ソフトウェア、サービスすべてを自社開発・提供し、操作性に優れた日本語GUIで導入も管理も容易。また、シンプルな価格体系によって導入後に利用する機能を順次増やすことができます。



## 安価

### 圧倒的なコストパフォーマンスで。

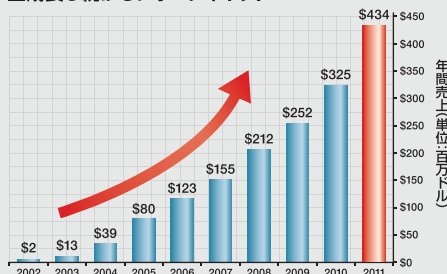
他社製品の多くは、ユーザ数をもとにしたライセンス体系としているため、ユーザ数の増加とともにコストが大きく増加します。しかし、FortiGateならそんな心配も不要です。アプライアンス単位のライセンスによって、価格体系もとてもシンプル。ユーザ数無制限ライセンスで、圧倒的なコストパフォーマンスを実現しています。  
※一部オプション機能があります。



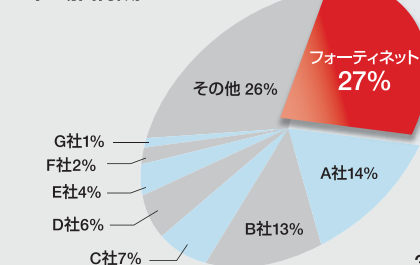
フォーティネットは、  
UTMのリーディング企業として  
世界市場で成長を続け、  
世界および日本で  
UTM市場シェアNo.1\*を獲得しています。

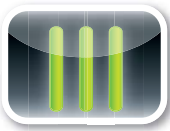
※出典: IDC Worldwide Quarterly Security Appliance Tracker - 2011 Q4

■成長し続けるフォーティネット



■2011年 日本UTM市場シェア\* (工場出荷額)





# FortiGate



ファイアウォール



不正侵入検知/防御



ウイルス/マルウェア対策



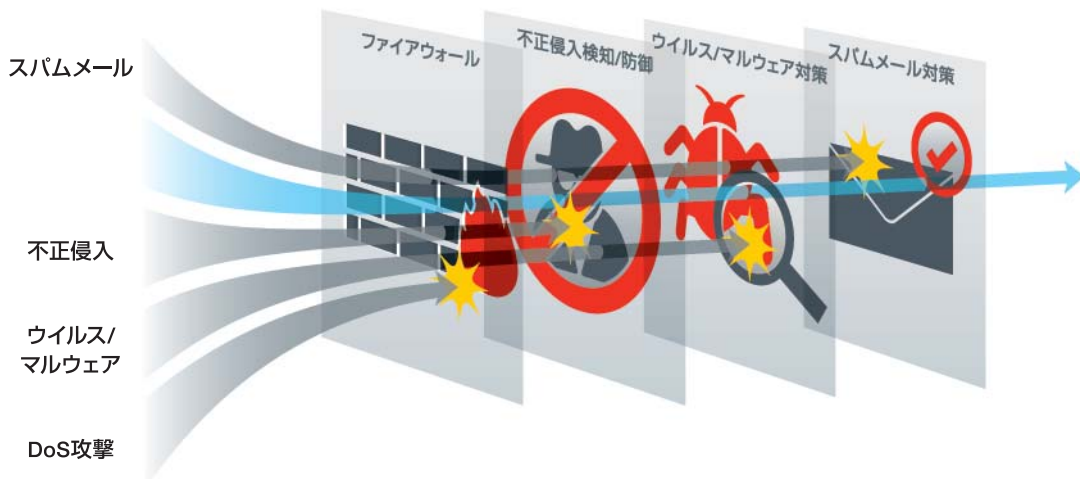
スパムメール対策



SSLインスペクション

## 刻一刻と変化し増加の一途をたどる 外部からの脅威への防御は強固でしょうか？

インターネットを介した企業ネットワークへの攻撃はますます巧妙化するばかりです。なかでも近年増加しているのが、特定の企業や団体を狙った標的型攻撃。この攻撃の多くはウイルスや悪意のあるファイルなどを添付したメールが使用され、脅威を秘めたスパムメールは増加の一途をたどっています。FortiGateは、このような企業ネットワークへのインバウンド攻撃を、ファイアウォールや不正侵入検知/防御、ウイルス/スパイウェア対策、スパムメール対策をはじめとする複合的かつ先進のセキュリティ機能で防御します。



### 1 ファイアウォール

DoS攻撃など外部からの脅威に対して強固な防御を提供。独自開発の専用プロセッサFortiASICによって高速のスループットを実現しています。

### 3 ウイルス/マルウェア対策

最新のウイルス/マルウェアに対抗するリアルタイムのアップデート機能により、常に最高レベルの防御を提供します。

### 5 SSLインスペクション機能

暗号化通信の拡大とともに、SSLの利点を逆にとった脅威が増加しています。FortiGateは、プロキシとして動作し、セキュアプロトコルにおいても最新のチェック機能を提供し、より安全な通信をサポートします。

### 2 不正侵入検知/防御

膨大な侵入防御システム(IPS)シグネチャを備えたIPSライブラリによる包括的な防御機能を提供。自動アップデートによって最新の脅威に対抗します。

### 4 スпамメール対策

多数のアンチスパムフィルタを装備し、大量のスパムメールをユーザや管理者の手を煩わせることなく除去します。

## 自動アップデートで最新の脅威を防御 不正侵入検知/防御(IPS)

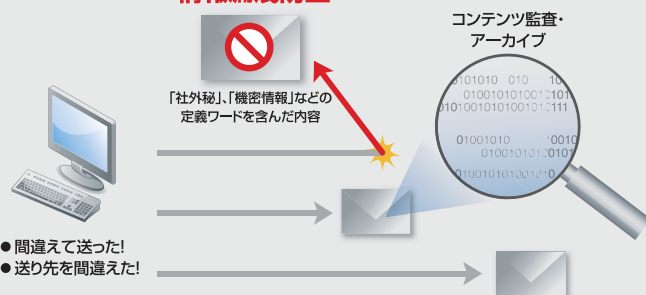
社内ネットワークに侵入しようとする脅威に対して最新の防御機能を提供します。7,100\*以上のシグネチャによるIPSライブラリを用意。自動アップデートによって、最新の脅威に対抗する強固な防御を可能にします。 ※2012年5月現在

Serial	Time	Src	Dest	Out	Protocol	App	Signature	Severity	Action
1	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
2	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
3	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
4	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
5	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
6	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
7	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
8	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
9	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
10	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
11	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
12	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
13	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
14	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
15	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
16	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
17	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
18	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
19	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked
20	18:43:28	172.16.1.111	172.31.1.224	18120	high	detected	sun_00	medium	blocked

## うっかりミスによる情報流出を防ぐ 情報漏洩防止(DLP)

「機密情報をメールに書いてしまった」「社外秘の文書を添付してしまった」などのうっかりミスによる情報流出を防止するのがFortiGateの情報漏洩防止(DLP)機能です。あらかじめ定義しておいた機密情報の特徴をもとに、検知した通信をブロックし、監査のためにアーカイブできます。

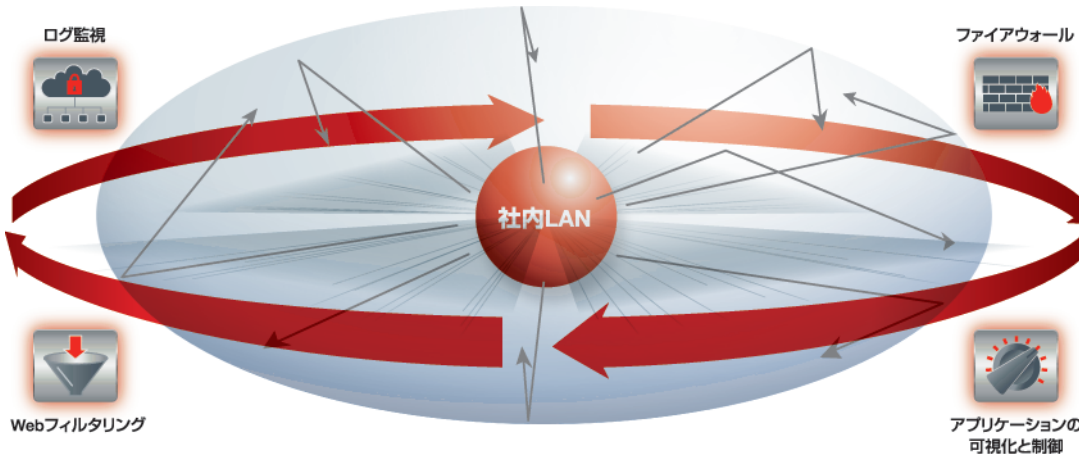
### 情報漏洩防止



## 標的型攻撃に備えるためには 内部から外部へ情報を出さない防御も重要です。

次々と新種の脅威が出現する現在、外部からの脅威に備えるインバウンド防御だけでは完璧とは言い切れません。「内部から外部へ」というアウトバウンド防御も併せて導入することが重要です。

FortiGateは、このアウトバウンド防御においても多層的なセキュリティ機能を提供します。危険を秘めたWebサイトへのアクセスをあらかじめ防止したり、もしもウイルスが侵入した場合も情報漏洩を阻止することが可能です。



- ファイアウォール 
- アプリケーションの可視化と制御 
- Webフィルタリング 
- 情報漏洩防止 
- ウイルス/マルウェア対策 
- スパムメール対策 

### 1 ファイアウォール

社内ユーザから外部ネットワークへの、HTTP(S) プロトコル以外の通信を遮断します。

### 2 アプリケーションの可視化と制御

HTTP(S) を利用するアプリケーションの使用状況を可視化し制御します。ユーザ認証と組み合わせ、ユーザごと制御することもできます。

### 3 Webフィルタリング

安全が確認されたWebサイトのみにアクセスを許可することで、情報漏洩を未然に防ぎます。

### 4 ログ監視

社外へのアクセスを遮断した通信のログを調査し、ウイルス/マルウェアに感染したPC/サーバを早期発見します。

### 5 情報漏洩防止

うっかりミスによる情報流出を防止します。あらかじめ定義しておいた機密情報の特徴をもとに、検知した通信をブロックし、監査のためにアーカイブできます。

### 5 内部UTM

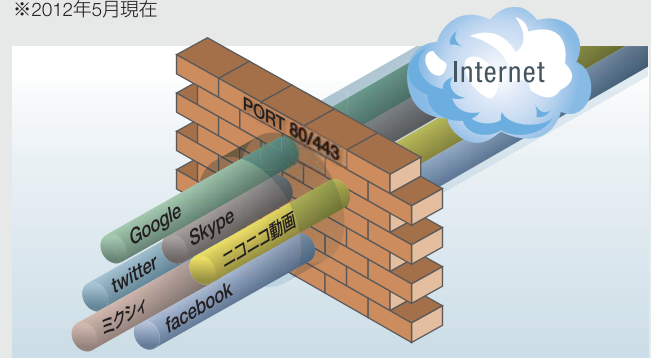
内部UTMを設置することにより、万が一ウイルス/マルウェアに感染した場合でも社内への拡大を防ぎます。また、重要な情報を扱う社内セグメントを強固に守ります。

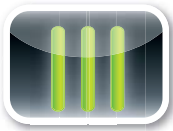
## アクセスを制御して情報漏洩を防止 Webフィルタリング

脅威を秘める未承認のWebサイトへのアクセスを遮断します。全世界1億2,000万\*以上のURL(8,700万\*以上のWebサイト)を、6グループ・79カテゴリーに分類し、カテゴリーごとにアクセスを制御。未分類のURLへのアクセスを遮断することで、情報漏洩を防止できます。 ※2012年5月現在

## 2,100\*種以上のアプリケーションに対応 アプリケーションの可視化と制御

ユーザ認証と組み合わせ、ユーザごとのアプリケーションの使用状況を可視化して制御し、また、アプリケーションごとに帯域幅も制御できます。ミクシィやニコニコ動画など、日本発のアプリケーションのほか、Skype、YouTubeなど全世界の2,100\*種以上のアプリケーションの制御を日本語GUIの管理画面で行えます。 ※2012年5月現在





# FortiGate



ファイアウォール



VPN



ワンタイムパスワード



WAN最適化



トラフィックシェーピング



無線LANコントローラ

## 忘れていませんか？ モバイルアクセスにも、社内ネットワークと同様のセキュリティが必要です。

スマートデバイスが急速に広がるいま、モバイル環境におけるセキュリティ対策も企業ネットワークにとって重大な課題です。FortiGateなら、無線ネットワーク環境においても先進のUTM機能を利用できます。また、スマートデバイスを社内で使用する場合も、UTM機能をフルに利用した無線ネットワークアクセスが可能になります。



### 1 VPN環境

FortiGateはIPSec/SSL VPN、PPTP、L2TPなどをサポートし、セキュアなVPN環境を容易に構築できます。

### 2 WAN最適化

非効率なプロトコル (CIFS、FTP、MAPI、HTTP/HTTPS、TCP) を使用するアプリケーションを圧縮することでWAN、VPNにおけるトラフィックを高速化します。

### 3 トラフィックシェーピング

WANのトラフィックの帯域幅を制御して、重要なトラフィックを優先することができます。

### 4 2要素認証によるアクセス

FortiGateは、OTP認証サーバを搭載。ワンタイムパスワードトークン、FortiTokenと連携させることで、2要素認証によるセキュアなアクセスが可能になります。またクライアント証明書による認証も可能です。

### 5 無線LAN

FortiGateは無線LANコントローラを搭載。無線環境からのトラフィックのゲートウェイとなることで、インターネットからのアクセス時と同様にUTM機能をフルに利用した無線ネットワークアクセスが可能になります。

### 6 エンドポイントセキュリティ

エンドポイントセキュリティソリューション、FortiClientによって、ノートPCなどモバイル環境の端末にも強固なセキュリティ機能を提供します。

## セキュアな無線LAN環境を素早く導入 FortiAP

セキュリティ機能を備えたシン無線LANアクセスポイントがFortiAP。FortiGateが搭載する無線LANコントローラ機能と連携し、セキュアな無線ネットワークを実現します。IEEE802.11nに準拠し、2.4GHzと5GHzの周波数帯におけるセキュリティ機能とWiFi端末からのアクセス機能を同時に実現します。



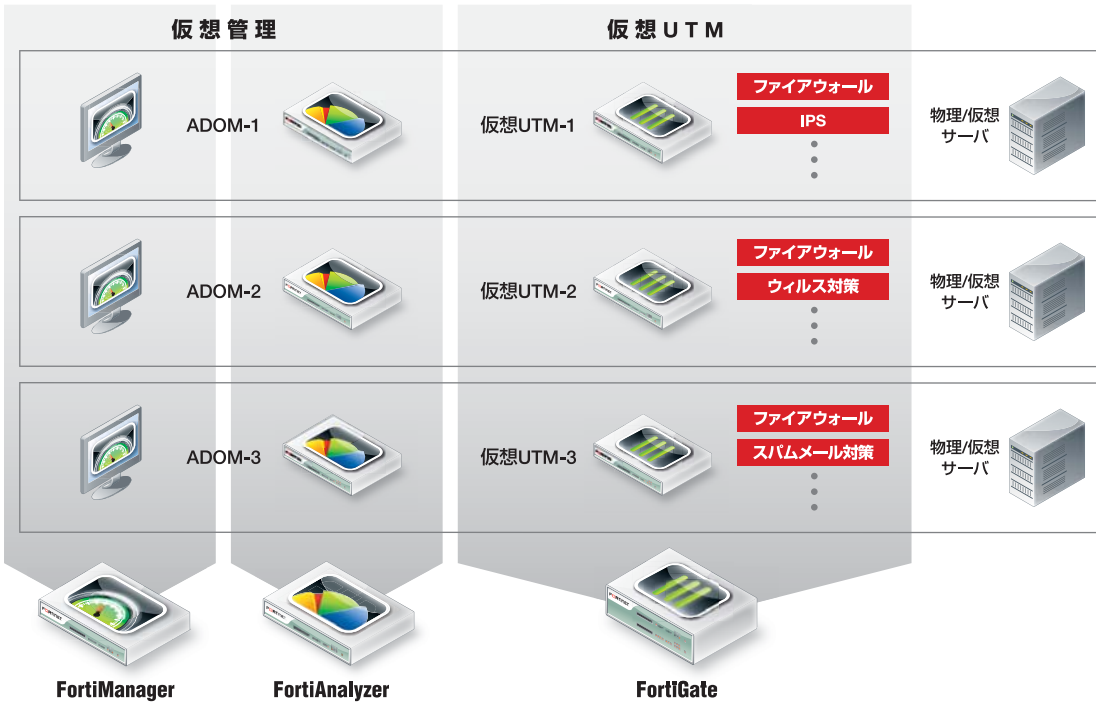
## フレキシブルなVPN環境を可能に FortiClient

FortiClientは、ノートPCやタブレット端末、スマートフォンなどに対応したエンドポイントセキュリティソリューション。FortiGateと連携することで、VPN環境を容易に構築できます。IPSec/SSL VPNトンネルモードをサポート。また、ワンタイムパスワード機能、WANの高速化、ウイルス対策、スパムメール対策機能などを提供します。



# クラウド環境でも統合的なセキュリティを実現する 2つの仮想化ソリューション。

FortiGateは、大規模なクラウド環境にも対応する高度かつ統合的な2つの仮想化ソリューションを提供します。  
たとえば、クラウド型サービスを提供するデータセンターにおいて、「仮想UTM」機能によって、物理的に独立している複数の  
ファイアウォールやUTMを1台のFortiGateアプライアンスへの統合を実現。さらに、FortiGateの機能を仮想環境に統合し  
たソフトウェアソリューション「仮想アプライアンス」を提供。MSSP事業者や大規模ユーザに対して、クラウドにおける先進  
のセキュリティ環境をサポートします。



- ファイアウォール
- VPN
- ワンタイムパスワード
- WAN最適化
- トラフィックシェーピング
- 不正侵入検知/防御
- ウイルス/マルウェア対策
- スパムメール対策
- SSLインスペクション
- Webフィルタリング
- 情報漏洩防止

## 1 仮想UTM機能

1台のFortiGateを複数の仮想FortiGateとして利用できる「仮想UTM (VDOM)」機能を提供。一元的な管理のもと、各ユーザ企業や部門ごとに独立した機能、ポリシーの設定や運用が可能になります。

## 2 仮想管理機能

さらにFortiManagerやFortiAnalyzerなどの管理アプライアンスの仮想化も可能。仮想管理機能 (ADOM) で、ユーザごとに個別の管理サービスを提供できます。

## ハードウェアにまったく依存せずにクラウド環境の仮想インフラをサポート

FortiGateが誇る最新のUTM機能を、仮想環境に統合したソフトウェアソリューションが「仮想アプライアンス」です。VMwareのハイパーバイザー上で稼働し、VMカーネル上で動作するバーチャルスイッチを経由してゾーン間のセキュリティを実現。ハードウェアに依存することなく、大規模クラウドにおけるセキュリティインフラを効率よく柔軟に構築できます。さらに、FortiManagerやFortiAnalyzer、FortiMail、FortiWebなどの仮想アプライアンスも提供しており、フォーティネットのすべてのセキュリティ製品をVMware上で実装できます。



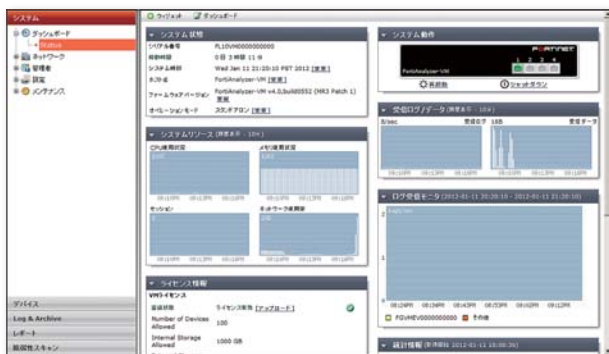


# FortiAnalyzer

## ネットワークを可視化し、ログの集中管理と分析、グラフィカルなレポート機能を提供。

FortiAnalyzerは、FortiGate、FortiMail、FortiWebなどのネットワークおよびセキュリティに関するログの収集・管理、分析、レポート作成のためのアプリケーションです。ログの集中管理からネットワークの可視化、脆弱性のスキャンまで多彩な機能を1台に搭載。また、仮想管理機能(ADOM)をサポートしており、効率的かつ柔軟な管理が可能です。

### 日本語化された管理画面



### 脆弱性スキャン機能によってサーバなどの状況の評価

スキャン機能によって、サーバなどの脆弱性の検知と管理が可能。定期的に検査するなどのスケジューリングも可能で、サーバなどのセキュリティ状況を自動的に確認・評価できます。

### 検知した脅威をキャプチャで自動的に保存

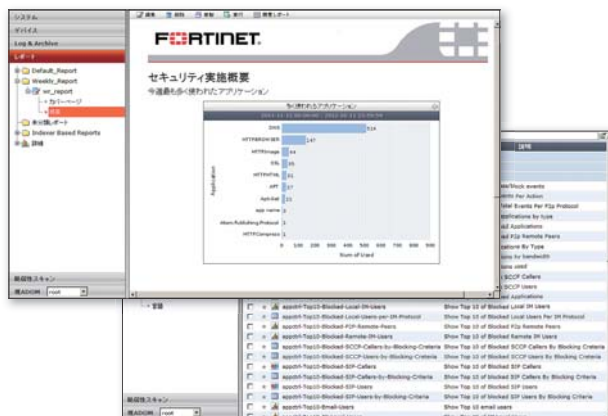
不正侵入検知(IPS)機能によってネットワークへの攻撃を検知した場合、そのパケットをキャプチャして自動的に保存します。また、FortiGateが検知した感染ファイルやウイルスをFortiAnalyzer上に隔離し、一元的に管理できます。

### MSSP管理者の作業を効率化する仮想管理機能(ADOM)

仮想管理機能(ADOM)によって、統合的な管理を実現しながら各ユーザの担当者に一定の権限を委譲することが可能。MSSP管理者の負荷を大幅に削減し、かつ柔軟な管理を実現します。

### 詳細なログを収集・分析して、わかりやすいレポートを作成

ネットワーク上のトラフィック、イベント、インシデントなどのログを保存・分析。その内容をグラフィカルなレポートによって明快地提示します。レポートは300種のテンプレートを揃えているほか、カスタマイズも容易です。



# FAMS

## FortiGateの統合管理をクラウド型サービスで提供し、アプリケーション単位のライセンス体系でコストも削減。

FortiGuardログ分析・管理サービス(FAMS)は、ログの収集・管理、分析、レポート作成、さらには複数のFortiGateの一元管理など、FortiAnalyzerやFortiManagerで提供する運用管理機能をクラウド型サービスで提供するソリューションです。最新の運用管理を効率よく低コストで実現できます。

### クラウド

リアルタイムモニタリング

レポート作成

コストメリット

ログの分析

デバイスの一括管理

FOSの自動アップデート

設定情報のバックアップ

日本語対応

メールのアーカイブ

定期的な機能拡張





# FortiManager

## 複数のアプライアンスを1つのコンソールで集中管理し、管理業務の負荷を大幅に軽減。

FortiManagerは、複数のFortiGateを効率よく管理するための統合管理・監視アプライアンスです。また、FortiGateばかりでなく、FortiMailなどのアプライアンスを含めた効率的な一元管理が可能で、導入や設定、監視、保守に関する管理者の作業を大幅に軽減できます。さらに仮想管理機能(ADOM)をサポートしており、MSSP事業者などでは管理機能をユーザに提供できます。

### 日本語化された管理画面



### 数千台のFortiGateをリモートから一元管理

数千台ものFortiGateを配置した大規模ネットワークでもリモートによる一元管理が可能。FortiGateごとにシグネチャやセキュリティポリシー設定の状況、更新履歴などを画面上で検証でき、ファームウェアやシグネチャの集中的な更新を実行できます。

### MSSP管理者の作業を効率化する仮想管理機能(ADOM)

仮想管理機能(ADOM)によって、統合的な管理を実現しながら各ユーザの担当者に一定の権限を委譲することが可能。MSSP管理者の負荷を大幅に削減し、かつ柔軟な管理を実現します。

### 複数のFortiGateのステータスを1つのコンソールに統合

FortiGateの状態を、単体あるいはグループごとに1つのコンソールで表示。CPUやメモリ使用量など、ステータスおよびイベントのリアルタイムなモニタリングによってシステム障害や攻撃を検出し、速やかな対応を支援します。

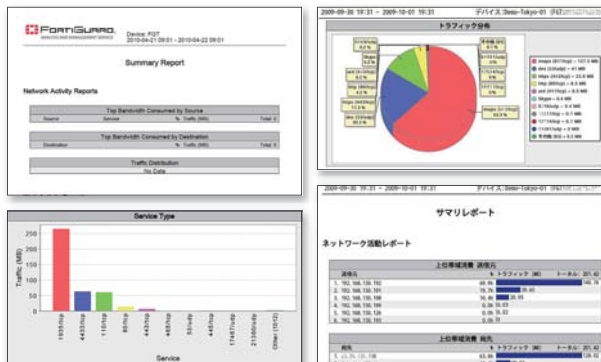


### 最新かつ多様な運用管理機能をクラウド型サービスで提供

ログの収集・分析、グラフィカルなレポート作成、脆弱性スキャン、多様なアプライアンスの一括管理など、FortiGateの統合管理に必要な多様な機能をクラウド型サービスで提供します。また、設定情報のバックアップ機能をサポート。FortiGateをリプレースする場合など、バックアップ情報を利用することで再設定の手間も省け、導入や管理を効率化できます。

### 小規模なネットワークでも低コストで導入可能

アプライアンス単位のライセンス体系によって、卓越したコストパフォーマンスを実現。小規模なネットワークでもFortiGateの最新の統合管理機能を導入できます。

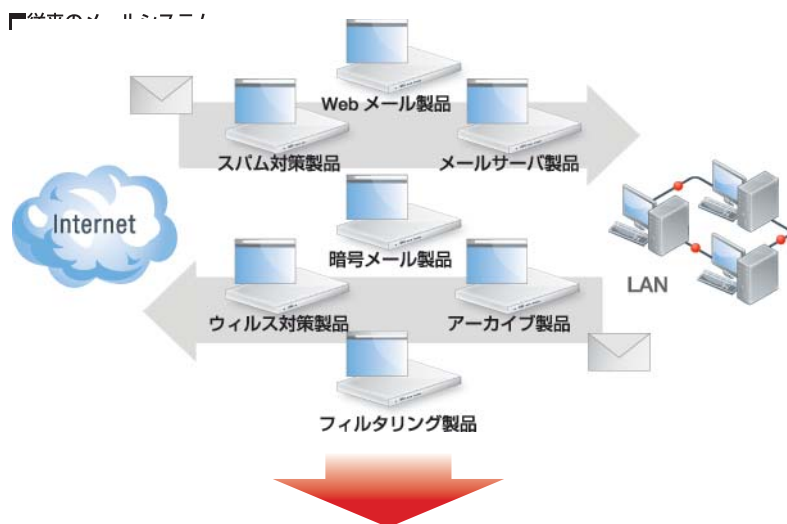




# FortiMail

## スパム対策、ウイルス対策からメールサーバまで、 先進かつ多様な機能を統合したセキュアメールアプライアンス。

FortiMailは、フォーティネットならではの卓越した統合セキュアメールアプライアンスです。FortiGateで蓄積してきた最新のセキュリティ機能に加えて、メールサーバをはじめ多様なメールセキュリティ機能を1台のアプライアンスに統合。3つの動作モードによって、クラウドをはじめお客様それぞれのネットワークに合わせて最適な環境を提供します。また、日本語によるGUIによって管理も容易。仮想アプライアンスでの提供も可能です。ユーザ数無制限のライセンスで、大規模システムでも圧倒的なコストパフォーマンスを実現します。



### 多様なセキュリティ&メール機能を統合して効率よく管理

スパム対策、ウイルス対策、フィルタリングから暗号メール、Webメール、アーカイブ、メールサーバまで、多様な機能を1台のアプライアンスで提供。強固かつ最新のセキュリティを実現するとともに、統合された管理画面で効率よくメールシステムを運用できます。

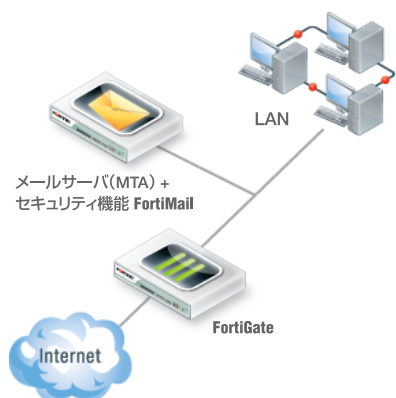
■総合セキュアメールアプライアンス



### すべての機能を1台で提供

#### サーバモード

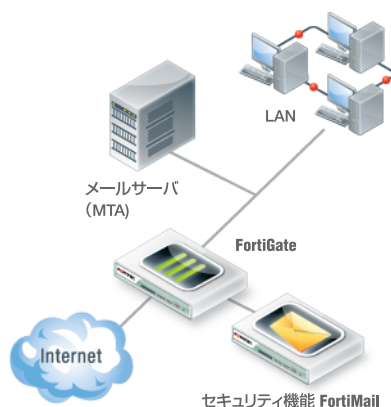
メールセキュリティからメールサーバまですべての機能を1台のアプライアンスで提供し、効率的な統合管理を実現します。また、マルチドメイン対応によって、情報配信用メールサーバなども単一のアプライアンスに統合できます。



### セキュリティ機能を低コストで導入

#### ゲートウェイモード

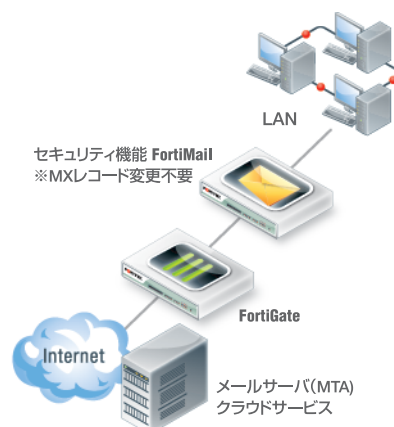
スパム対策、ウイルス対策、フィルタリングなどセキュリティ機能のみを導入できます。ユーザ数無制限ライセンスで、先進のセキュリティ環境を低コストで実現。また、暗号メールやWebメールなどの機能を導入することも可能です。



### メールネットワークの設定変更不要

#### トランスペアレントモード

DNSのMXレコードを変更することなしに、スパム対策、ウイルス対策、フィルタリング、暗号メールなどの機能を導入できます。クラウド型のメールサービスなど、社内にメールサーバがある場合でも、独自のセキュリティ環境を柔軟に構築可能です。

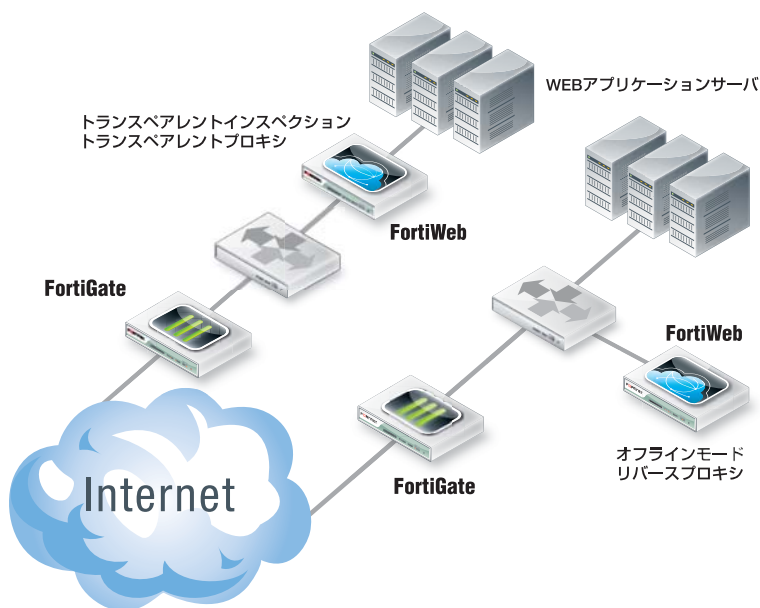




# FortiWeb

## Webアプリケーションの脆弱性を診断し、Webビジネスに忍び寄る最新の脅威をトータルに防御。

FortiWebは、通常のファイアウォールでは防げないWebアプリケーションに対する攻撃からWebサイトを防御するセキュリティプライアンスです。WAF(Webアプリケーションファイアウォール)/XMLファイアウォールによる防御に加え、脆弱性の診断、Webページの改ざんを検知した際の自動復旧機能、入力フォームの自動学習機能や、クレジットカード番号漏洩検知とブロック機能を搭載。また、クレジットカード業界における国際標準、PCI DSS 6.6にも準拠しています。



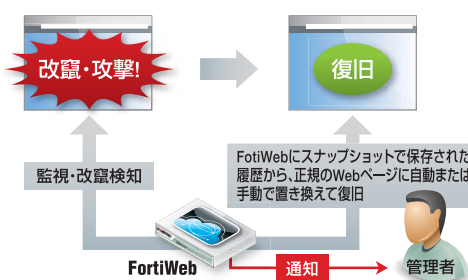
### WAF/XMLファイアウォールでWebアプリケーションへの攻撃を阻止

シグネチャおよびパターンのマッチング、パラメータ検証、しきい値に基づく制限、フロー制御などによって、Webアプリケーションへの攻撃を阻止。また、XML IPS (侵入防御システム)、WSDL検証、XML表現の制限などにより、XMLベースのWebサービスについても防御します。



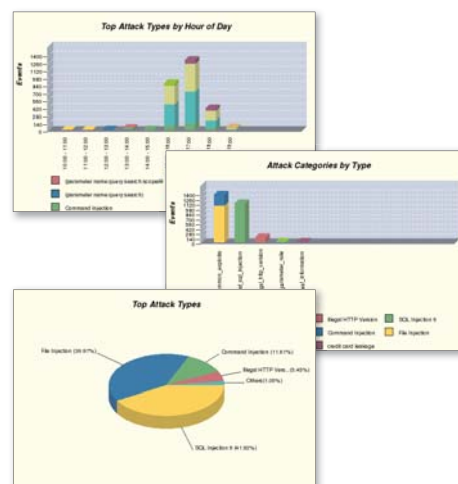
### 不正アクセスなどによる改ざんを検知し、自動で修復

近年、Webサイトを改ざんし、不正Webサイトへ誘導したり不正プログラムに感染させるガンブラーウイルスなどによる攻撃が増加しています。FortiWebは、こうしたWebサイトの改ざんを検知し、自動で迅速に復旧する機能を提供し、被害を最小限に止めます。



### 充実したアラートログとレポートで管理も容易

アラートログの振り分けを簡単にできるなど、わかりやすいアラート画面によって効率的に管理できます。また、数十種類の標準レポートを装備しており、イベントやトラフィックの分析も容易。管理や監査などの目的に応じて最適なレポートを作成できます。



### 脆弱性を定期的に診断し、Webビジネスのリスクを軽減

Webアプリケーションの脆弱性やWebサーバに対するネットワークの脆弱性を定期的に診断。SQLインジェクションやクロスサイトスクリプティングなどに対する脆弱性を検出し、セキュリティの強化をサポートします。

# FortiGuard Center

フォーティネットでは、世界6カ所にセキュリティ研究センターを設置し、日々変化する脅威を世界規模で監視。世界中で発生するあらゆる脅威に対する情報を一元管理し、セキュリティのエキスパートたちがその対策のための研究と開発に日夜取り組んでいます。24時間365日の運用体制で検知した脅威は、フォーティネットのFortiGuardディストリビューションネットワークを通じて、最新のシグネチャとしてお客様のフォーティネット製品に迅速に配信されます。

シグネチャ更新頻度

- アンチスパム:10分ごと
- Webフィルタリング:30分ごと
- アンチウイルス:6時間ごと
- 不正侵入検知/防御:数日ごと
- アプリケーション制御:数日ごと



## 全世界をカバーするFortiGuardディストリビューションネットワーク

- |              |            |                             |
|--------------|------------|-----------------------------|
| ウイルス対策       | Webフィルタリング | アプリケーションの可視化と制御             |
| 不正侵入検知       | スパムメール対策   | 脆弱性診断と管理(VCM)               |
| データベースセキュリティ | Webセキュリティ  | FortiGuardログ分析・管理サービス(FAMS) |

### 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用意しています。

※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

Copyright© 2012 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、およびFortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。