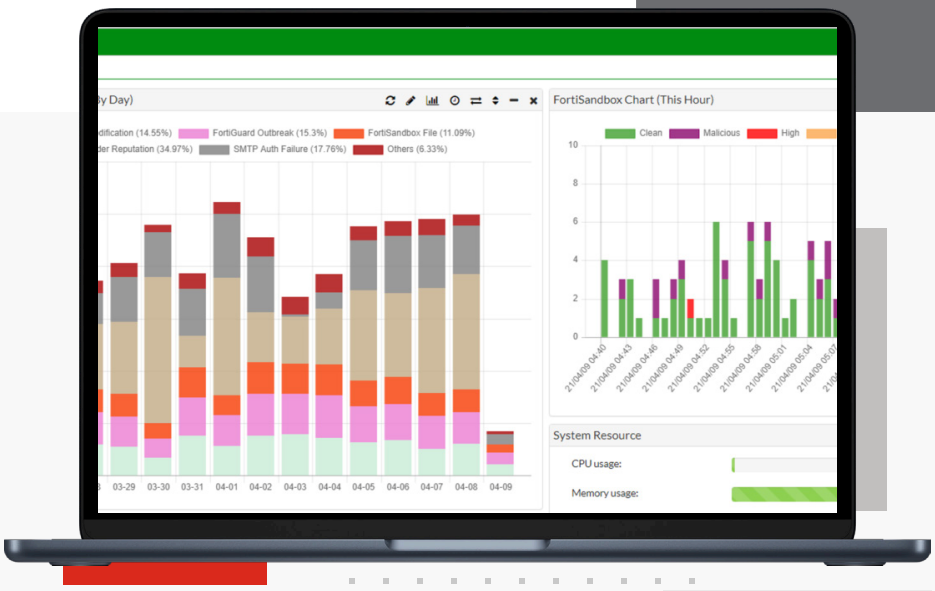
FortiMail で実現する E メールセキュリティ



ハイライト

- E メールを悪用する脅威からの保護
- 実証済みのパフォーマンス
- ファブリック対応の E メールセキュリティ
- FortiGuard Labs の活用

さまざまな導入モデルで利用可能な、強力でスケーラブルな Eメールセキュリティソリューション

第三者機関によって実証済みのクラス最高レベルのパフォーマンスを誇る FortiMail は、E メールを悪用するあらゆる脅威からの高度な多層型の保護を提供します。FortiGuard Labs の脅威インテリジェンスを活用し、フォーティネット セキュリティ ファブリックに統合された FortiMail は、スパム、フィッシング、マルウェア、ゼロデイ脅威、なりすまし、BEC（ビジネスメール詐欺）攻撃などの E メールベースの脅威の防止、検知、レスポンスを支援します。

機能

E メールを悪用する脅威からの保護

強力なアンチスパムおよびアンチマルウェア、さらにそれらを補完するアウトブレイク防止、コンテンツ無害化、サンドボックスによる分析、なりすまし検知などの先進技術により、不要な一斉送信メール、ランサムウェア、ビジネスメール詐欺を防止し、標的型攻撃を回避します。

実証済みのパフォーマンス

フォーティネットは、第三者機関によるテストで FortiMail の有効性を一貫して証明している、数少ないメールセキュリティベンダーの 1 つです。FortiMail は、SE Labs から AAA 評価を獲得し、Virus Bulletin により 99.97% のスパム捕獲率が実証されています。

ファブリック対応の E メールセキュリティ

FortiMail はフォーティネット製品だけでなく、サードパーティ製コンポーネントとも統合することにより、シームレスなセキュリティ ファブリック全体で IOC（Indicators of Compromise：侵害指標）を共有し、プロアクティブなセキュリティ対策を導入できます。さらには、API レベルの統合によって、Microsoft 365 および Google Workspace のメールセキュリティを補完し、高度な保護を実現します。

FortiGuard Labs の活用

FortiMail には、FortiGuard Labs の脅威インテリジェンスおよび、アンチウイルス、ウイルスアウトブレイク防止、アンチスパムといった FortiGuard AI 搭載のセキュリティサービスが活用されています。FortiGuard Labs は、世界中の 60 万ものお客様の環境の可視化を可能にする、最も優れた脅威リサーチチームの 1 つです。

自社での管理を希望するお客様

E メールセキュリティインフラストラクチャの完全制御と管理を求める組織に最適な E メールセキュリティソリューション。

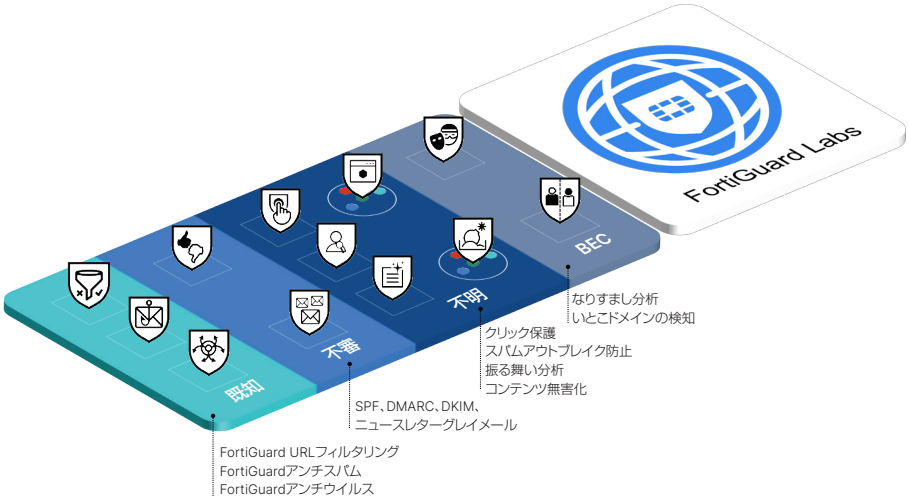
以下の選択が可能：

- スパムサイト
- フィッシングサイト
- スピアフィッシング / ホエールフィッシング
- 不正添付ファイルや URL
- ランサムウェア
- ゼロデイ脅威
- なりすまし
- ビジネスメール詐欺（BEC）

機能

プロアクティブ E メールセキュリティ

FortiMail は、最新の脅威に関する FortiGuard Labs のグローバルな可視性とインテリジェンスを活用することで、E メールが組織にもたらすあらゆるリスクに対応します。



多層型のアンチスパム対策

複数の送信者、プロトコル、コンテンツのインスペクション手法で、スパムやジャンクメールからユーザーを保護します。レピュテーション分析、接続フィルタリング、認証、受信者確認の手法を組み合わせて使用することで、高速かつ正確なメール保護を可能にします。IP、ドメイン、送信者、SPF、DKIM、DMARC、地理による制限などのチェックボックスを選択できます。

最後に、デジタル署名、コンテキストのキーワード、画像分析、本文に含まれる URI に基づく分析、さらには、振る舞い分析やスパムアウトブレイク保護などの高度な技術を活用した分析によって、メッセージの構造と内容が検査されます。これらの技術の連携により、実環境の条件下で 99.97% のスパムを特定し、ブロックします。

強力なアンチマルウェア対策

FortiMail は、シグネチャ、ヒューリスティック、挙動などの複数の静的 / 動的テクノロジーを活用し、ウイルスアウトブレイク防止機能を利用することで、常に進化するさまざまな脅威からの保護を可能にします。

高度な脅威保護

ビジネスメール詐欺や標的型攻撃など、ごく最近猛威を振るう脅威に対抗するために、FortiMail はコンテンツ無害化、サンドボックスによる分析、高度な偽装検知など、さらに強力な防御機能をオプションで追加することができます。

統合型のデータ漏洩防止

データ漏洩防止や E メールの暗号化などの機能を利用することで、機密データが含まれる E メールを確実に保護し、偶発的なデータ漏洩を防ぎます。このような機能により、企業ポリシーや業界規制のコンプライアンスが容易になります。

直感的な操作

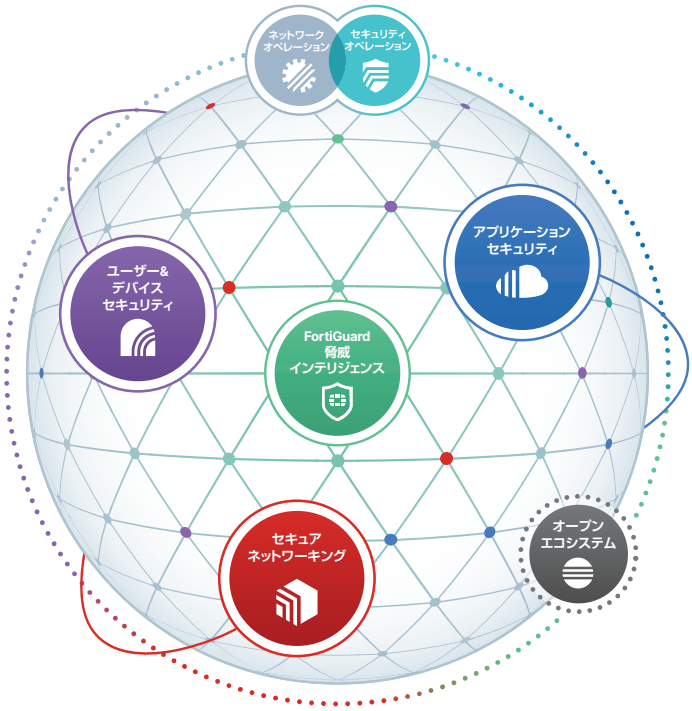
リアルタイムダッシュボード、豊富なレポート、一元管理の隔離、使いやすいエンドユーザーコントロールで、すぐに運用を開始し、価値を実現できます。 直感的なユーザーインタフェースと MTA やメール処理の柔軟な機能を組み合わせることで、E メールトラフィックを完全に可視化し制御できます。

機能

フォーティネット セキュリティ ファブリックとの統合

高度化する脅威やマルチベクトルキャンペーンからの保護を可能にするため、今後は、プラットフォームベースやファブリック対応の E メールセキュリティが主流になります。フォーティネット セキュリティ ファブリックの一部として、IOC（Indicators of Compromise：侵害指標）やその他のテレメトリを共有することで、セキュリティインフラストラクチャ全体のセキュリティが強化されます。

IT チームやセキュリティチームは、点と点をより完全に結び付けて、高度な犯罪者によるマルチベクトル攻撃を特定でき、レスポンスを含む面倒で反復的なワークフローを自動化することで、セキュリティオペレーションチームの負担を軽減できます。



業界で実証済みのトップクラスのパフォーマンス

FortiMail は、第三者機関によるテストで実証済みの優れたパフォーマンスを提供します。

vb VERIFIED SPAM virusbtn.com

99.98%
スパム検知率

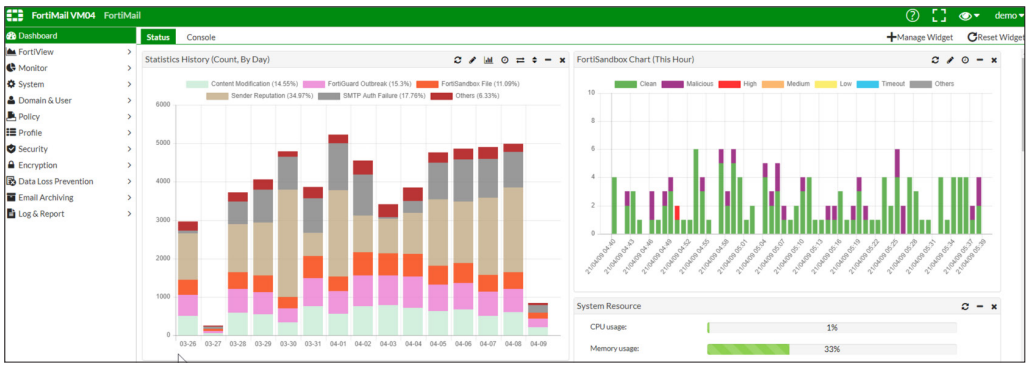
vb 100 VIRUS virusbtn.com

100%
マルウェアの検知

機能

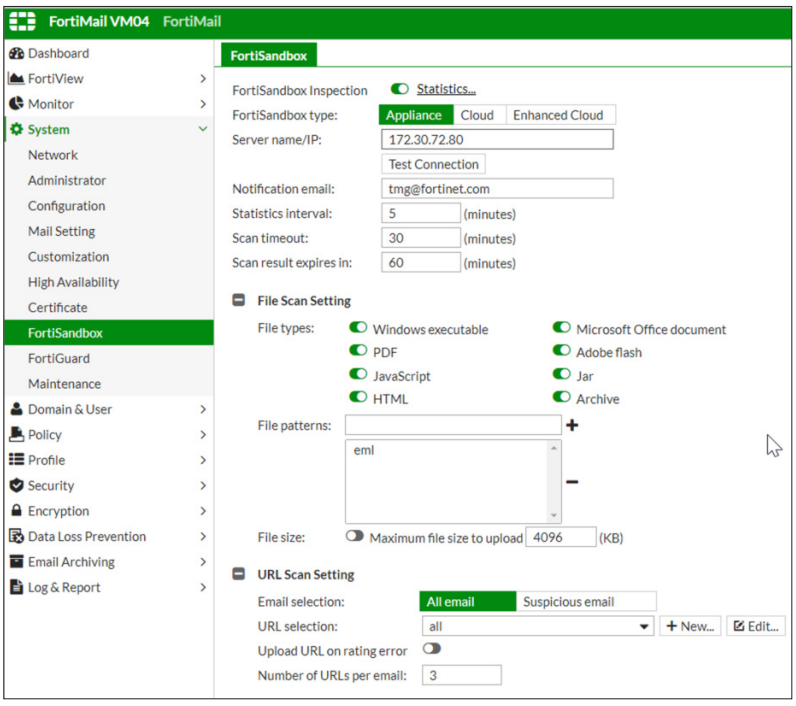
直感的な E メール管理

リアルタイムのダッシュボード、豊富なレポート機能、集中隔離機能、エンドユーザーの制御と MTA および E メール処理のフル機能によって、E メールのトラフィックの完全な可視化と容易な制御が可能になります。



使いやすい構成

使いやすい構成機能により、あらゆる規模の企業やユースケースで、高度なセキュリティ機能であっても簡単に E メールセキュリティをセットアップし、管理することができます。



最適なソリューションの選択

お客様にとってベストな FortiMail ソリューションはどちらですか？

自社での管理を希望するお客様

仮想マシンとアプライアンスを使用し、インフラストラクチャと E メールセキュリティをお客様がすべて管理します。

管理の委託をご希望のお客様

E メール SaaS（Security-as-a-Service）を利用して、E メール脅威の監視とレスポンスのみをお客様が担当し、フォーティネットがインフラストラクチャを管理します。

FortiMail Cloud のデータシートは、こちらをご参照ください。
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/ja_jp/FortiMail-Cloud_DS.pdf

機能

高性能、柔軟な導入

容易な拡張が可能で、1 時間あたり数百万件のメッセージを処理できます。フォーティネットは、あらゆる規模の組織に対し、E メールセキュリティの多様なニーズに対応する幅広い導入モデルと運用モードを提供します。

導入モデル

アプライアンスと仮想マシン

FortiMail アプライアンスと仮想マシンは、オンプレミスやクラウドのユースケースで E メールセキュリティインフラストラクチャを自らが完全に制御し、管理したいと考える組織向けのモデルです。

- オンプレミス環境向けアプライアンス
- 動作する仮想マシン：
  - 主要なハイパーバイザープラットフォーム：
    - VMWare
    - Citrix XenServer
    - Hyper-V
    - KVM
  - 主要なクラウドプラットフォーム：
    - AWS
    - Azure
    - Google Cloud
    - Oracle

FortiMail Cloud

FortiMail Cloud は、オンプレミスとクラウドベースの両方の E メールサービスの保護を可能にするシンプルで使いやすい E メールセキュリティサービスを希望する組織向けのモデルです。

運用モード

ゲートウェイモード

既存の E メールゲートウェイに対してインバウンドおよびアウトバウンドのプロキシメールトランスファーエージェント（MTA）サービスを提供します。シンプルな DNS MX レコード変更機能によって E メールが FortiMail にリダイレクトされて分析された後に、安全な E メールが宛先の E メールサーバーに中継されて配信されます。

Microsoft 365 および Google Workspace API 統合モード

FortiMail を導入することで導入環境が簡素化され、MX レコードの変更は必要なく、ネイティブ Microsoft 365 および Google Workspace API を活用した脅威の検知と配信後のメッセージの回収が可能になります。キーワード、ファイル名、コンテンツタイプに基づく検索パラメータの構築といった、コンプライアンスや独自のビジネス要件に対応した回収のポリシーを柔軟に作成できます。これらの機能が Microsoft および Google のネイティブのセキュリティ機能を補完することで、全体としてのセキュリティを強化し、リスクを軽減できます。

トランスペアレントモード

トランスペアレントモードでは、DNS MX レコードを変更したり、既存のネットワーク構成を変更したりする必要がありません。トランスペアレントモードは、E メールセキュリティサービスを既存の顧客に提供したいと考えるサービスプロバイダーに最適です。FortiMail Cloud ではこのモードを使用できません。

サーバーモード

FortiMail ユニットはスタンドアロンメッセージングサーバーとして動作し、セキュアな POP3、IMAP、および Web メールアクセスを柔軟にサポートする、SMTP メールサーバーのフル機能を提供します。

機能

自社での管理を希望するお客様			
機能	ベースバンドル	Enterprise Advanced Threat Protection バンドル	Cloud メール API サポート付き Enterprise Advanced Threat Protection バンドル
99.97% のスパム検知率	✓	✓	✓
高度な多層型マルウェア検知機能	✓	✓	✓
インバウンド / アウトバウンドのメールフィルタリング	✓	✓	✓
ご利用中の LDAP との統合	✓	✓	✓
セキュアなメッセージ配信（TLS）	✓	✓	✓
メッセージ追跡	✓	✓	✓
VOS（ウイルスアウトブレイク防止サービス）	✓	✓	✓
ID ベース暗号（IBE: Identity Based Encryption）	✓	✓	✓
レポート	✓	✓	✓
メールデータ喪失防止	✓	✓	✓
CDR（コンテンツ無害化）		✓	✓
URL クリック保護		✓	✓
なりすまし分析		✓	✓
クラウドサンドボックス		✓	✓
Microsoft / Google メールボックスのリアルタイムスキャン			✓
Microsoft / Google メールボックスのスケジュールスキャン			✓
新たに発見されたメール脅威の配信後のクローバック			✓

追加のアドオン機能

Email Continuity

FortiMail Cloud の Email Continuity は、組織の E メールサービスで障害が発生した際に、緊急メールボックスサービスを提供することにより、価値ある生産性を保護するように設計されています。

動的画像分析サービス

動的画像分析サービスは、不適切な画像や性的な画像から組織や従業員を保護します。

フォーティネットのソリューションとの統合

FortiAnalyzer
FortiIsolator
FortiSandbox Cloud
FortiSOAR
FortiAnalyzer Cloud
FortiNDR
FortiSIEM

機能概要

システム仕様
多様な導入 / 運用オプション – オンプレミス、パブリック / プライベートクラウドへの導入に対応 – ゲートウェイモード、M365 API モード、トランスペアレントモード、サーバーモード – クラウド管理型サービス
インバウンド / アウトバウンドスキャン
複数の E メールドメインをサポートし、ドメイン別のカスタマイズも可能 – MSSP のマルチテナントをサポートし、自社ブランドによる提供も可能 – 多層型管理
IPv4、IPv6 アドレスのサポート
送信元や宛先に関する IP アドレスのプールを用いた仮想ホスティング
LDAP、RADIUS、POP3、または IMAP による SMTP 認証
LDAP ベースの E メールルーティング
ポリシー（ドメイン）単位の LDAP 属性を用いた、ユーザー単位のスキャン
IP の地理的ロケーションベースのポリシー
サーバーモードの展開と隔離メール管理のための、分かりやすい Web メール画面
メールキュー管理
Web メールと管理画面の多言語対応
SMTP RFC 標準のコンプライアンス
最先端の HTML 5 GUI
第三者機関である SELabs および Virus Bulletin によるテストで実証済み
Microsoft 365、Google Workspace、Amazon AWS、Microsoft Azure などのクラウドサービスとの互換性
DANE（DNS-based Authentication of Named Entities）のサポート
アンチスパム
FortiGuard アンチスパムサービス – 送信者やドメインのレピュテーション – スパムや添付ファイルのシグネチャ – ダイナミックヒューリステックルール – スパムアウトブレイク防止
全カテゴリの FortiGuard URL フィルタリング – スパム、マルウェア、フィッシングメール URL など – アダルトサイトの URL – 新規登録ドメイン
IPv4、IPv6 アドレスと E メールアカウントのグレーリスティング
ローカルセンダーレピュテーション（IPv4、IPv6、エンドポイント ID ベース）
振る舞い分析
サードパーティのスパム URI とリアルタイムブラックリスト（SURBL / RBL）
ニュースレター（グレイメール）および不審なニュースレターの検知
PDF スキャン、イメージ分析
グローバル、ドメインおよびユーザーレベルのブロック / セーフリスト
エンタープライズ向けの送信ドメイン認証技術のサポート – 送信者ポリシーフレームワーク（SPF） – Domain Keys Identified Mail(DKIM) – Domain-Based Message Authentication（DMARC）
柔軟なアクションと通知プロファイル
複数システム / ユーザー毎のセルフサービスによる隔離
標的型攻撃に対する保護
CDR（コンテンツ無害化） – Office / PDF ドキュメントの無害化 （マクロ、アクティブコンテンツ、添付ファイルの削除など） – ハイパーリンクの削除 / URL の書き換えによるメール HTML コンテンツの無害化
ビジネスメール詐欺（BEC） – 複数段階のアンチスプーフィング保護 – なりすまし分析：なりすまし検知の手動 / 自動実行 – なりすました類似ドメイン名の検知
URL のクリックを保護し、URL のリライトとアクセス時の再スキャンを実行
FortiIsolator ブラウザ隔離プラットフォームとの統合によるブラウザベース脅威の無害化

API 統合
Microsoft 365 / Google Workspace メール統合 – 脅威を検知し、配信後のメールを回収 – スケジュールスキャン – リアルタイムスキャン – 内部メールスキャン
コンテンツ検知
FortiGuard アンチウイルスサービス検知 – CPRL シグネチャチェック – ヒューリスティックベースのビヘイビア（振る舞い）検知 – グレイウェア検知
FortiGuard ウイルスアウトブレイク防止サービス – グローバルな脅威インテリジェンスおよびデータ分析
アクティブなコンテンツ検知（PDF および Office 形式ドキュメント）
隔離解除時の脅威の再スキャン実行
カスタムファイルハッシュのチェック
MIME / ファイルタイプの検知
ファイルのフィンガープリントチェックや機密データの検知による包括的なデータ漏えい対策 – 自動 Windows ファイル共有およびマニュアルアップロードによるファイルのフィンガープリントチェック – 医療、財務、個人を特定する情報、不適切な言葉の検知
ビルトイン / 管理者定義によるパスワードリストと、メール本文の単語検知による、アーカイブ、PDF、Office ドキュメントの自動復号
PDF スキャン、イメージ分析
動的画像分析サービス – 不正 / 性的コンテンツの特定とレポート
暗号化
包括的な暗号化サポート – きめ細かい暗号スイート制御とオプションの適用によるサーバー間 TLS – S / MIME – クライアントレスの ID ベース暗号（IBE：Identity Based Encryption）による受信者デスクトップの暗号化 – オプションの Outlook プラグインによる ID ベース暗号（IBE）のトリガー
管理、ログ、レポーティング
ベーシック / アドバンスト管理モード
ドメイン単位のロールベースの管理者アカウント
アクティビティ、構成の変更やインシデントの広範なログとレポート
レポートモジュール内蔵
詳細メッセージ追跡
大規模な導入にも対応する集中隔離機能
FortiAnalyzer を利用したログとレポートの集約
しきい値ベーストラップによる標準 / プライベート MIB を利用した SNMP サポート
iSCSI デバイスを含む、外部またはローカルストレージサーバーのサポート
外部 Syslog サーバーのサポート
構成 / 管理用オープン REST API
高可用性（HA）
あらゆる導入形態で高可用性をサポート – アクティブ - パッシブモード – アクティブ - アクティブ構成同期モード
隔離およびメールキューの同期
デバイス障害の検出および通知
リンクステータス、フェイルオーバー、冗長インタフェースサポート
アドバンスト
外部ストレージの利用も可能な、ポリシーベースのメールアーカイブ – Exchange ジャーナルによるアーカイブに対応
先進の E メールサーバー機能セット – 包括的な Web メールインタフェース – POP3、IMAP メールアクセス – カレンダー機能 – 送信の取り消し
SAML 2.0 SSO / ADFS 統合による Web メールおよび隔離アクセス
サポート
包括的なバンドルサービスによるシンプルなサポートオプション
高度な RMA サポート
プロフェッショナルサービスおよびインストールサポートオプション

技術仕様

	FortiMail 200F	FortiMail 400F	FortiMail 900F
推奨される導入環境			
	小規模の企業、支社、組織	中小規模の組織	中規模から大規模企業、教育機関および政府機関の各部門
ハードウェア仕様			
10 / 100 / 1000 インタフェース（カッパー、RJ45）	4	4	4
SFP GbE インタフェース	—	—	2
SFP+ 10 GbE インタフェース	—	—	—
冗長電源（ホットスワップ対応）	—	—	○
内蔵ストレージ	1 × 1 TB	2 × 1 TB	2 × 2 TB（2 × 2 TB 追加可）
RAID ストレージ管理	—	ソフトウェア：0、1	ハードウェア：0、1、5、10 ホットスペア（ドライブの台数に基づく）
形状	ラックマウント（1 U）	ラックマウント（1 U）	ラックマウント（1 U）
トラステッドプラットフォームモジュール（TPM）	○	○	○
電源	単一	単一（オプションで冗長化可能）	冗長
システム性能			
保護される E メールドメイン数 *	20	70	500
受信者ベースのポリシー数（ドメイン / システム）、送信または受信	60 / 300	400 / 1,500	600 / 2,000
メールボックス数（サーバーモード）	150	400	1,500
アンチスパム、アンチウイルス、認証、コンテンツプロファイル数（ドメイン / システム）	50 / 60	50 / 200	50 / 400
DLP（Data Loss Prevention：情報漏洩対策）	—	○	○
脅威の一元的な隔離機能	—	○	○
Microsoft 365 / Google Workspace API 統合	—	オプション	オプション
パフォーマンス（メッセージ数 / 時：100 KB のメッセージサイズに基づく、キューイングがない場合)			
メールルーティング（時間あたり）**	50,000	250,000	800,000
FortiGuard Antispam + Virus Outbreak（メッセージ / 時）**	40,000	200,000	500,000
FortiGuard Enterprise ATP（メッセージ / 時）**	30,000	150,000	400,000
クラウド API パフォーマンス（メッセージ数 / 時：100 KB のメッセージサイズに基づく、キューイングがない場合)			
メールルーティング（時間あたり）**	18,000	83,000	241,000
FortiGuard Antispam + Virus Outbreak（メッセージ / 時）**	14,000	72,000	170,000
FortiGuard Enterprise ATP（メッセージ / 時）**	12,000	58,000	148,000
サイズ			
高さ × 幅 × 奥行	44 × 438 × 422 mm	44 × 438 × 416 mm	44 × 438 × 701 mm
重量	5.4 kg	11.0 kg	15.00 kg
動作環境			
電源	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz
最大電流	100 V / 3 A、240 V / 1.5 A	100 V / 5 A、240 V / 3 A	100 V / 5 A、240 V / 2.5 A
必要電源（最大）	62 W	113 W	190 W
消費電力（平均）	51 W	77 W	174 W
放熱	245 BTU/h	418 BTU/h	681 BTU/h
エアフロー	前面 ～ 背面	前面 ～ 背面	前面 ～ 背面
湿度	5 ～ 90%（結露しないこと）	5 ～ 90%（結露しないこと）	5 ～ 90%（結露しないこと）
動作温度	0 ～ 40 ºC	0 ～ 40 ºC	0 ～ 40 ºC
保管温度	-20 ～ 70 ºC	-20 ～ 70 ºC	-20 ～ 70 ºC
準拠規格			
	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB、RoHS	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB、BSMI、RoHS	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB、BSMI、RoHS
認定			
	VB Spam、VB100、Common Criteria NDPP、FIPS 140-2	VB Spam、VB100、Common Criteria NDPP、FIPS 140-2	VB Spam、VB100、Common Criteria NDPP、FIPS 140-2

* 保護 E メールドメイン数は、アプライアンス上で構成・管理可能な E メールドメインの総数です。
ドメインアソシエーションを利用することで、割当て先のプライマリドメインと構成を共有する追加のドメインを有効にすることが可能です。
アドバンスド管理ライセンスにより、保護ドメインの上限を 50% 増加させます。

** FortiMail 7.0 で検証済

技術仕様

	FortiMail 2000F	FortiMail 3000F
推奨される導入環境		
	大規模企業、教育機関および政府機関の各部門	最大レベルの規模の大学、企業、ISP、通信キャリア向けのハイエンドアプライアンス
ハードウェア仕様		
10 / 100 / 1000 インタフェース（カッパー、RJ45）	4	4
SFP GbE インタフェース	2	2
SFP+ 10 GbE インタフェース	—	2
冗長電源（ホットスワップ対応）	○	○
内蔵ストレージ	2 × 2 TB SAS（6 × 2 TB 追加可）	2 × 2 TB（10 × 2 TB 追加可）
RAID ストレージ管理	ハードウェア：1、5、10、50 ホットスペア（ドライブの台数に基づく）	ハードウェア：1、5、10、50 ホットスペア（ドライブの台数に基づく）
形状	ラックマウント（2 U）	ラックマウント（2 U）
トラステッドプラットフォームモジュール（TPM）	○	○
電源	冗長	冗長
システム性能		
保護される E メールドメイン数 *	1,000	2,000
受信者ベースのポリシー数（ドメイン / システム）、送信または受信	800 / 3,000	1,500 / 7,500
メールボックス数（サーバーモード）	2,000	3,000
アンチスパム、アンチウイルス、認証、コンテンツプロファイル数（ドメイン / システム）	50 / 400	50 / 600
DLP（Data Loss Prevention：情報漏洩対策）	○	○
脅威の一元的な隔離機能	○	○
Microsoft 365 / Google Workspace API 統合	オプション	オプション
パフォーマンス（メッセージ数 / 時：100 KB のメッセージサイズに基づく、キューイングがない場合)		
メールルーティング（時間あたり）**	1,600,000	3,500,000
FortiGuard Antispam + Virus Outbreak（メッセージ / 時）**	1,100,000	2,600,000
FortiGuard Enterprise ATP（メッセージ / 時）**	800,000	2,100,000
クラウド API パフォーマンス（メッセージ数 / 時：100 KB のメッセージサイズに基づく、キューイングがない場合)		
メールルーティング（時間あたり）**	372,000	705,000
FortiGuard Antispam + Virus Outbreak（メッセージ / 時）**	280,000	560,000
FortiGuard Enterprise ATP（メッセージ / 時）**	233,000	465,000
サイズ		
高さ × 幅 × 奥行	89 × 437 × 647 mm	89 × 437 × 647 mm
重量	14.5 kg	18.2 kg
動作環境		
電源	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz
最大電流	10.0 A / 110 V、3.5 A / 240 V	9.8 A / 110 V、4.9 A / 220 V
必要電源（最大）	219 W	379 W
消費電力（平均）	189 W	348 W
放熱	781 BTU/h	1325 BTU/h
エアフロー	前面 ～ 背面	前面 ～ 背面
湿度	8 ～ 90%（結露しないこと）	8 ～ 90%（結露しないこと）
動作温度	5 ～ 35 ºC	10 ～ 35 ºC
保管温度	-40 ～ 60 ºC	-40 ～ 70 ºC
準拠規格		
	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB、BSMI、RoHS	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB、BSMI、RoHS
認定		
	VB Spam、VB100、Common Criteria NDPP、FIPS 140-2	VBSpam、VB100、NDPP、FIPS 140-2

* 保護 E メールドメイン数は、アプライアンス上で構成・管理可能な E メールドメインの総数です。
ドメインアソシエーションを利用することで、割当て先のプライマリドメインと構成を共有する追加のドメインを有効にすることが可能です。
アドバンスド管理ライセンスにより、保護ドメインの上限を 50% 増加させます。

** FortiMail 7.0 で検証済

技術仕様

FortiMail 仮想アプライアンスの技術仕様	VM01	VM02	VM04	VM08	VM16	VM32
推奨される導入環境 *						
	小規模の企業、支社、組織	中小規模の組織	中～大規模エンタープライズ	大規模エンタープライズ	大規模エンタープライズ	大規模エンタープライズ
技術仕様						
サポートするハイパーバイザー	VMWare ESX / ESXi 6.0 / 6.7 / 7.0 以降、Citrix XenServer v5.6 SP2 / 6.0 以降、Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019、KVM qemu 2.12.1 以降、AWS（Amazon Web Services）、Nutanix AHV **、Microsoft Azure、Google Cloud Platform、Oracle Cloud Infrastructure ***					
仮想 CPU 数（最大）	1	2	4	8	16	32
仮想 NIC 数（最小 / 最大）	1 / 4	1 / 4	1 / 6	1 / 6	1 / 6	1 / 6
仮想マシン用ストレージ容量（最小 / 最大）**	250 GB / 1 TB	250 GB / 2 TB	250 GB / 4 TB	250 GB / 8 TB	250 GB / 12 TB	250 GB / 24 TB
仮想マシン用メモリ（最小 / 最大）	2 GB / 4 GB	2 GB / 8 GB	4 GB / 16 GB	4 GB / 64 GB	4 GB / 128 GB	4 GB / 128 GB
パフォーマンス（メッセージ数 / 時：100 KB のメッセージサイズに基づく、キューイングがない場合)*****						
メールルーティング（時間あたり）**	34,000	67,000	306,000	675,000	875,000	1,200,000
FortiGuard Antispam + Virus Outbreak（メッセージ / 時）**	30,000	54,000	279,000	630,000	817,000	1,100,000
FortiGuard Enterprise ATP（メッセージ / 時）**	26,000	52,000	225,000	585,000	758,000	1,000,000
クラウド API パフォーマンス（メッセージ数 / 時：100 KB のメッセージサイズに基づく、キューイングがない場合)*****						
メールルーティング（時間あたり）**	—	23,000	110,000	295,000	495,000	940,000
FortiGuard Antispam + Virus Outbreak（メッセージ / 時）**	—	18,000	96,000	226,000	383,000	740,000
FortiGuard Enterprise ATP（メッセージ / 時）**	—	16,000	75,000	197,000	311,000	620,000
システム性能						
保護される E メールドメイン数 *****	20	70	500	1,000	1,500	2,000
受信者ベースのポリシー数（ドメイン / システム）、送信または受信	60 / 300	400 / 1,500	800 / 3,000	800 / 3,000	1,500 / 7,500	1,500 / 7,500
メールボックス数（サーバーモード）	150	400	1,500	2,000	3,000	3,000
アンチスパム、アンチウイルス、認証、コンテンツプロファイル数（ドメイン / システム）	50 / 60	50 / 200	50 / 400	50 / 400	50 / 600	50 / 600
DLP（Data Loss Prevention：情報漏洩対策）	—	○	○	○	○	○
脅威の一元的な隔離機能	—	○	○	○	○	○
Microsoft 365 / Google Workspace API 統合	—	オプション	オプション	オプション	オプション	オプション

* ゲートウェイおよびトランスペアレントな導入向けの推奨ユーザー数。サーバーモードでの導入については、メールボックス数（サーバーモード）の項目をご参照ください。適切なモデルの選択が難しい場合は、最大メールフローレートおよび平均メッセージサイズをご確認の上、FortiMail 製品担当者にご相談ください。

** FortiMail 7.0.1 は、Nutanix AHV 20201105.2096 および AOS 5.20.1.1 で検証されています。

*** トランスペアレントモードは、利用可能なネットワーク構成の制約のため、Microsoft HyperV およびクラウドハイパーバイザーでは完全サポートされていません。

**** 初期 VM セットアップで、デフォルトのフォーティネット OVF ファイルをインストールするために 250 GB が必要です。導入後にこのデフォルト OVF ファイルを削除することで、ディスク領域が 50 GB 以下になります。

***** システム構成に依存します。記載の数値は 2 個の Intel Xeon E5-2620 v4（2.10 GHz）を使用する VVMWare 6.0 システムで測定されており、実際の数値は割り当てる CPU コア数に依存します。

****** 保護 E メールドメイン数は、アプライアンス上で構成・管理可能な E メールドメインの総数です。
ドメインアソシエーションを利用することで、割当て先のプライマリドメインと構成を共有する追加のドメインを有効にすることが可能です。
アドバンスド管理ライセンスにより、保護ドメインの上限を 50% 増加させます。

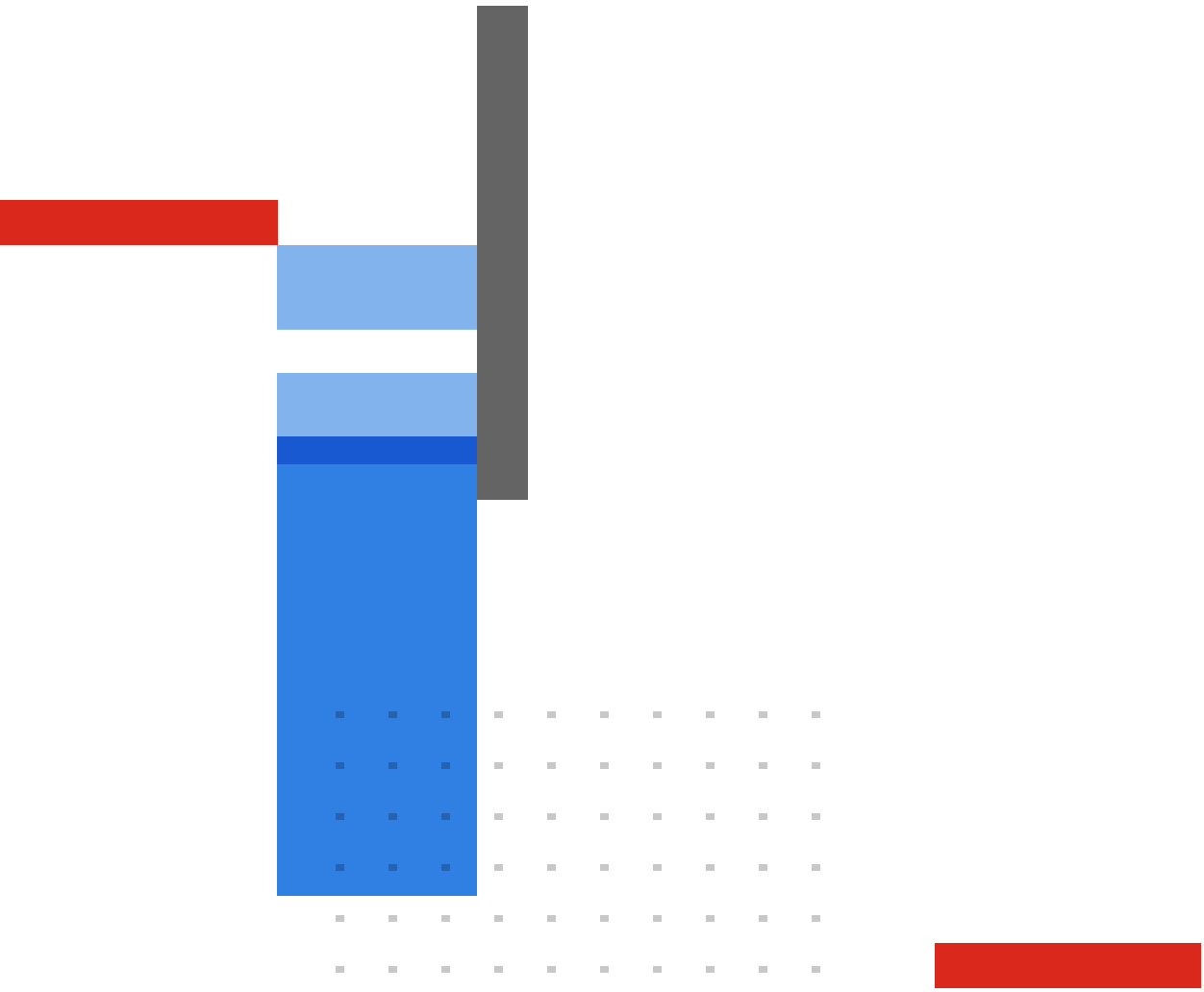
オーダー情報

ご注文については、フォーティネットのアカウントマネージャーにご相談いただくか、詳細については、「注文ガイド」をご参照ください。

FortiMail Product	SKU	Description
FortiMail 200F	FML-200F	Email Security Appliance — 4x GE RJ45 ports, 1 TB storage
FortiMail 400F	FML-400F	Email Security Appliance — 4x GE RJ45 ports, 2 TB storage
FortiMail 900F	FML-900F	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 2000F	FML-2000F	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 3000F	FML-3000F	Email Security Appliance — 4x GE RJ45 ports, 2× 10 GE SFP+ slots, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail VM		
FortiMail VM01	FML-VM01	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 1x vCPU core
FortiMail VM02	FML-VM02	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 2x vCPU cores
FortiMail VM04	FML-VM04	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 4x vCPU cores
FortiMail VM08	FML-VM08	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 8x vCPU cores
FortiMail VM16	FML-VM16	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 16x vCPU cores
FortiMail VM32	FML-VM32	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 32x vCPU cores
Accessories		
Power Supply	SP-FAD700-PS	AC power supply for FML-400E
Power Supply	SP-FML900F-PS	AC power supply for FML-400F and FML-900F
Power Supply	SP-FML2000F-PS	AC power supply for FML-2000F
Power Supply	SP-FML3000F-PS	AC power supply for FML-3000F and FML-3200F
Hard Drive	SP-D2TE	2 TB 3.5" SAS hard drive with tray for FML-2000F, FML-3000F and FML-3200F
Hard Drive	SP-FML900F-HDD	2 TB 3.5" SATA hard drive with tray for FML-900F
Service and Support		
Appliances - Hardware plus 24×7 FortiCare and FortiGuard Base Bundle		
Appliances - Hardware plus 24×7 FortiCare and FortiGuard Enterprise ATP Bundle		
Virtual Machines - 24×7 FortiCare and FortiGuard Base Bundle Contract		
Virtual Machines - 24×7 FortiCare and FortiGuard Enterprise ATP Bundle Contract		
Microsoft 365 and Google Workspace API Integration Service		
Add-on Capabilities		
Dynamic Adult Image Analysis Service		
Email Continuity		
For Service Providers and Enterprises		
Advanced Administration License for MSSPs and Enterprises requiring multi-tenancy and additional features		

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-FML-R58-202401-R1