DATA SHEET

FortiWeb

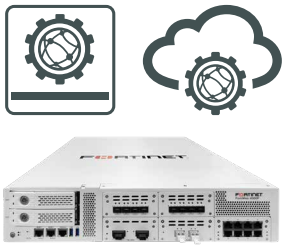
提供形態：

アプライアンス　仮想マシン　SaaS　クラウド　コンテナ

Web アプリケーションと API の保護

FortiWeb 100E、400E、600E、1000E、2000F、3000F、4000F、VM、Container

FortiWeb は、既知や未知のエクスプロイトを標的にする攻撃から Web アプリケーションや API を保護し、法規制のコンプライアンスを支援する、Web アプリケーションファイアウォール（WAF）です。



機械学習を活用して各アプリケーションをモデリングすることで、FortiWeb は既知の脆弱性およびゼロデイ攻撃の脅威からアプリケーションを保護します。高性能の物理アプライアンス、仮想アプライアンス、コンテナをオンサイトまたはパブリッククラウドに導入することで、小規模企業からサービスプロバイダー、キャリア、大企業まで、あらゆる規模のユーザーに対応します。

Web アプリケーション保護

機械学習も活用する、OWASP トップ 10 アプリケーション攻撃に対する多層型の保護により、既知および未知の攻撃からの防御を可能にします。

API の保護

ポジティブおよびネガティブのセキュリティポリシーを自動適用することで、サイバー攻撃者から API を保護します。API セキュリティを CI/CD パイプラインにシームレスに統合します。

ボット減災

高度なボット減災機能により、無害のボットと有害なボットを高精度で区別するで、Web サイト、モバイルアプリケーション、API を自動化された攻撃から保護します。FortiWeb Bot Mitigation は、不要な CAPTCHA やチャレンジでユーザーの生産性を低下させることなく、必要とされる可視性とコントロールを提供します。

ハイライト

- 機械学習を活用することで誤検知を最小限にしつつ脅威を検知してブロック
- 高度なボット減災により、正規のユーザーに影響することなく Web 資産を効果的に保護
- API（モバイルアプリケーションのサポートに使用する API を含む）を保護
- フォーティネット セキュリティ ファブリックとの統合による保護の拡張
- 高度な脅威に関する実用的なインテリジェンスを提供するビジュアル分析ツール
- サードパーティ製品との統合と仮想パッチ

FortiCare Worldwide Support

support.fortinet.com

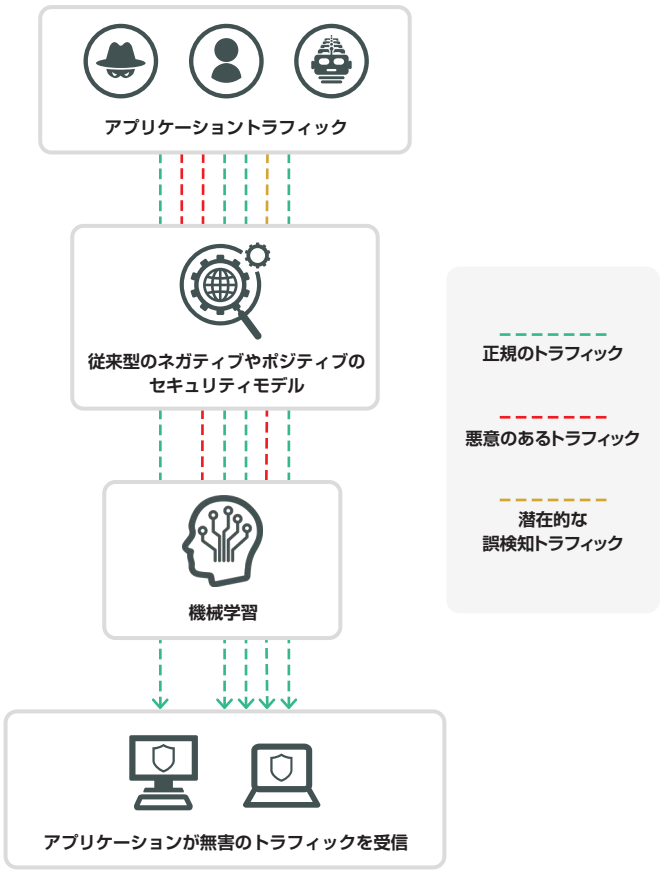
FortiGuard セキュリティサービス

www.fortiguard.com

第三者機関の認定

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

ハイライト



FortiWeb は、従来型のネガティブやポジティブのセキュリティモデル（攻撃シグネチャ、IP アドレスのレピュテーション、プロトコルの検証など）にとどまらない機能を提供し、第 2 レイヤーの機械学習の分析を経ることで、誤検知を最小限にしつつ悪意のある異常を検知してブロックします。

機械学習による検知率の向上と運用の効率化

FortiWeb の多層型アプローチには、高精度の脅威の検知と運用の効率化という 2 つの重要なメリットがあります。

保護対象であるアプリケーションに関連する異常な振る舞いを検知する FortiWeb の機能で未知のエクスプロイトをブロックすることで、アプリケーションを標的にするゼロデイ攻撃からの最大限の保護を実現します。

運用面においては、FortiWeb の機械学習により、誤検知の修正や WAF ルールの手動での調整などの時間のかかる作業から解放されます。FortiWeb のモデルはアプリケーションの進化に合わせて継続的に更新されるため、アプリケーションを更新するたびにルールを手動で更新する必要はありません。時間のかかる WAF ルールの手動での調整や高度な機能のない WAF で発生する誤検知のトラブルシューティングを排除し、本番環境への迅速なコードの取得を可能にします。

ゼロデイ脅威をブロック

包括的 Web アプリケーションセキュリティ

多層型で相関的な先進のアプローチを採用する FortiWeb は、OWASP トップ 10 やその他多くの脅威に対抗する万全のセキュリティを企業向けの Web ベースアプリケーションに提供します。FortiWeb の防御の第 1 レイヤーは、フォーティネットの業界最先端のセキュリティリサーチ部門である FortiGuard Labs のインテリジェンスを使用し、従来型の WAF の検知エンジン（攻撃シグネチャ、IP アドレスレピュテーション、プロトコル検証など）を活用して悪意のあるトラフィックを特定し、ブロックします。FortiWeb の機械学習検知エンジンがさらに、この第 1 レイヤーを通過するトラフィックを検証することで、継続的に更新されるアプリケーションのモデルを使用して悪意のある異常を特定し、ブロックします。

API の保護

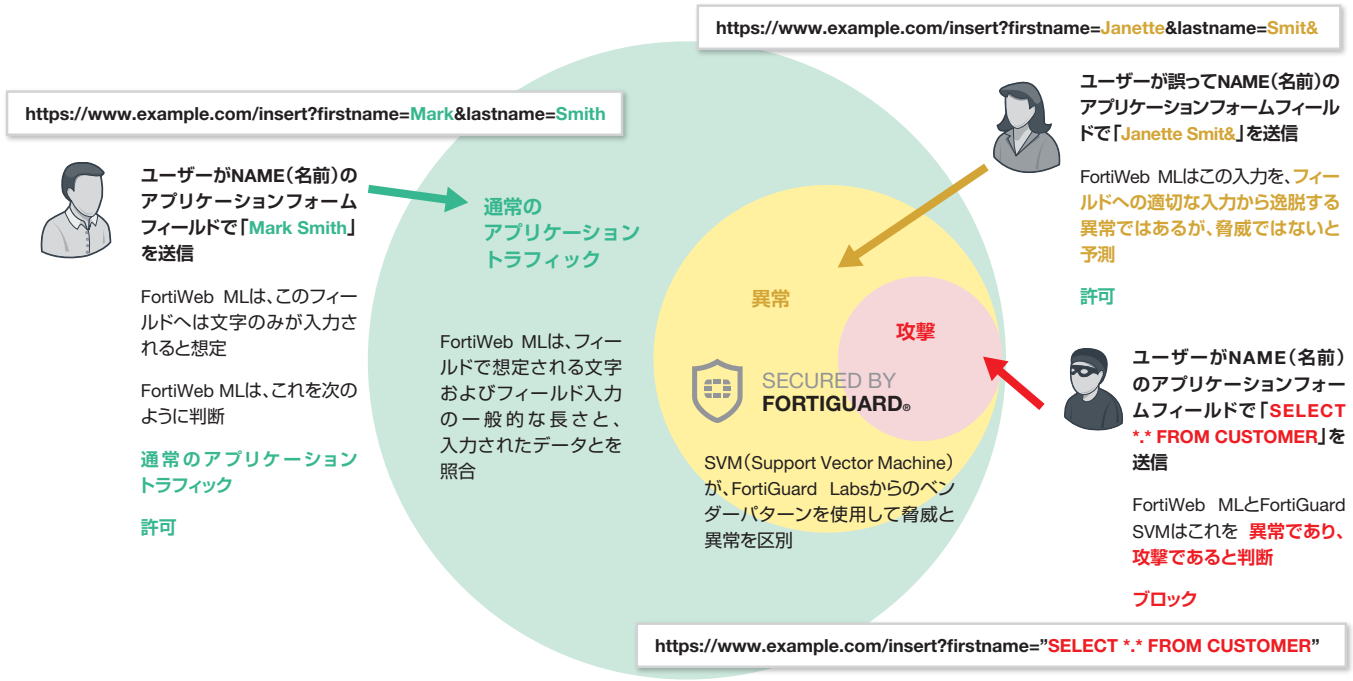
デジタルトランスフォーメーションの推進に伴い、モバイルアプリケーションのバックボーン、B2B の運用の自動化、アプリケーションの管理の効率化を目的とする API の採用が加速しています。しかしながら、そのように急速な採用により、企業が保護しなければならない、外部に公開されるアプリケーションが増加し、攻撃対象領域が拡大しています。フォーティネットの FortiWeb には、API に対する脅威からの保護に役立つツールが提供されています。FortiWeb は、組織のスキーマ仕様（OpenAPI、XML、一般的な JSON をサポート）に基づいて自動生成されるポジティブセキュリティモデルポリシーを設定不要で統合することで、API エクスプロイトからの保護を可能にします。FortiWeb のスキーマ検証を CI/CD パイプラインに統合できるため、API が更新されると、更新されたポジティブセキュリティモデルポリシーが自動生成されます。

ボット減災

FortiWeb は、自動化されたボット、Web スクレイパー、クローラー、データハーベスティング、クレデンシャルスタッフィングなどの自動化された攻撃から、Web 資産、モバイル API、アプリケーション、ユーザー、機密データを保護します。しきい値ベースの検知、ボットディセプションなどのポリシーの機械学習に、無害のボットを高精度で識別する生体認証ベースの検知を組み合わせることで、正規のユーザーへの影響を軽減しつつ、悪意のあるボット攻撃をブロックします。FortiWeb は、高度な追跡手法で、人間、自動化された要求、再犯者を区別し、振る舞いを長期にわたって追跡することにより、ボットと人間を高精度で識別し、必要に応じて CAPTCHA 認証を要求します。FortiWeb のグラフィカル分析ダッシュボードである FortiView を併用することで、攻撃を迅速に識別し、無害のボットや正規のユーザーを区別できます。

ハイライト

FortiWeb の機械学習には、異常の検知と脅威の識別の精度が向上するというメリットがあります。他の WAF ベンダーに広く採用されている、すべての異常を脅威として処理する自動学習検知モデルとは異なり、FortiWeb のこの高精度の検知モデルでは、誤検知がほぼ解消され、他のモデルでは不可能な種類の脅威を捕捉できます。

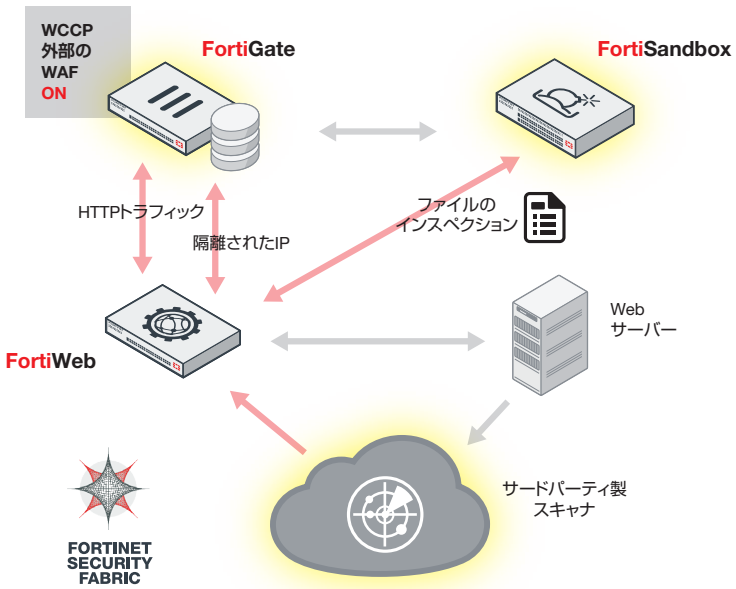


FortiWeb の AI ベースの機械学習はアプリケーション要求を評価し、正常、無害の異常、または脅威である異常のいずれであるかを判断します。

フォーティネット セキュリティ ファブリックやサードパーティのスキャナとの緊密な統合

脅威の状況が進化し、新たに多くの脅威が出現したことを受け、Web ベースのアプリケーションを保護する上で多目的なアプローチが求められています。APT（持続的標的型攻撃）は、攻撃経路が 1 つしかない従来型の攻撃タイプとは異なり、さまざまな攻撃形態をとります。また、単一のデバイスによる保護機能を回避することができます。FortiWeb が FortiGate および FortiSandbox と統合され、脅威情報の同期と共有が実現したことで、基本的な WAF の保護機能が強化され、不審なファイルの徹底したスキャンおよび感染した内部ソースの共有が可能となります。

また FortiWeb は、主要なサードパーティ製脆弱性スキャナ（Acunetix、HP WebInspect、IBM AppScan、Qualys、ImmuniWeb、WhiteHat など）との統合も可能で、アプリケーション環境におけるセキュリティの問題に対応する仮想パッチを動的に提供することができます。スキャナが発見した脆弱性は、FortiWeb によって瞬時に自動でセキュリティルール化され、開発者がコードの脆弱性を解消するまでアプリケーションを保護します。



FortiGate や FortiSandbox などのフォーティネット セキュリティ ファブリックの他の要素との統合によって APT 保護が可能になり、主要サードパーティベンダーとの統合によって脆弱性スキャンが拡張されます。

ハイライト

脅威誤検知の課題を解決

脅威の誤検知はアプリケーションの中断に繋がりかねない深刻な問題であることから、多くの管理者がセキュリティルールを緩和せざるを得ず、結果として Web アプリケーションファイアウォールは、信頼できる脅威回避のプラットフォームではなく単なる監視ツールになってしまっている場合が少なくありません。WAF のインストールはおそらく数分で完了しますが、微調整には数日、場合によっては数週間かかる場合があり、セットアップ後もアプリケーションや環境の変更に伴う検査や調整が必要になることがあります。

FortiWeb の AI ベースの機械学習によって、脅威の見逃しと誤検知どちらの問題も解決され、ホワイトリストの管理や脅威検知ポリシーの微調整といった面倒な作業も必要ありません。すべての異常を無条件にブロックしてしまう他の方法とは異なり、FortiWeb は 2 層構造の機械学習エンジンがほぼ 100% の精度で異常を検知し、その異常が脅威であるかどうかを判断します。ユーザー追跡、セッション追跡、脅威の重み付けなどの他のツールを FortiWeb と組み合わせることで、事実上すべての誤検知のシナリオを排除できます。

高度なグラフィカル分析 / レポーティング

FortiWeb には、FortiView と呼ばれるグラフィカル分析ツールスイートが装備されています。FortiGate などの他のフォーティネット製品と同様に、サーバーの IP 構成、攻撃やトラフィックのログ、攻撃マップ、OWASP トップ 10 攻撃分類、ユーザーの行動などの FortiWeb の主要エレメントを管理者が可視化し、ドリルダウンすることができます。FortiView for FortiWeb によって、管理者は不審な行動をリアルタイムで迅速に特定し、脅威の発生源、一般的な違反、クライアント / デバイスのリスクなどの重要なユースケースに対処することができます。

FortiGuard による強力なセキュリティ

FortiWeb のレイヤーの大半でアプリケーションセキュリティへのアプローチの根幹となっているのは、豊富な実績を誇るフォーティネットの FortiGuard Labs です。FortiGuard サービスは、ご利用の Web アプリケーションに対する保護対策のニーズに応じて 5 つのオプションを選択することができます。FortiWeb IP アドレスレピュテーションサービスは、ボットネット、スパマー、匿名プロキシ、有害なソフトウェアによる感染が確認されているソースなどの既知の攻撃ソースからお客様を保護します。

FortiWeb セキュリティサービスは、アプリケーションレイヤーシグネチャ、機械学習による脅威モデル、悪意のあるロボット、不審な URL パターンおよび Web 脆弱性スキャナのアップデートなど、FortiWeb に特化したサービスを提供します。クレデンシャルスタッフィングディフェンスは、ログイン試行を FortiGuard 作成の侵害された認証情報のリストと照合し、アラートの発信から盗まれたユーザー ID とパスワードを使用する不審なログインのブロックまで、さまざまなアクションを実行できます。FortiWeb Cloud Sandbox サブスクリプションは、FortiWeb とフォーティネットのクラウドサンドボックスサービスとの統合を可能にします。さらに FortiWeb は、トップレベルの評価を得ている FortiGuard のアンチウイルスエンジンを活用し、サーバーやその他のネットワーク構成要素を感染させる可能性のある脅威を検知するため、すべてのファイルアップロードをスキャンします。

仮想マシンとパブリッククラウドのオプション

FortiWeb は、トップレベルの柔軟性を備えており、仮想環境やハイブリッド環境にも対応可能です。FortiWeb の仮想バージョンは、ハードウェアベースのデバイスと同じ機能をすべてサポートし、VMware、Microsoft Hyper-V、Citrix XenServer、Open Source Xen、VirtualBox、KVM、Docker などのプラットフォームに導入できます。FortiWeb は、AWS、Azure、Google Cloud、Oracle Cloud では VM として、AWS、Azure、Google Cloud では WAF-as-a-Service として利用することもできます。詳細は、Fortiweb-Cloud.com を参照してください。

FortiView for FortiWeb

主な機能

導入オプション

- リバースプロキシ
- インラインイントランスペアレント
- 真のトランスペアレントプロキシ
- オフラインスニフィング
- WCCP

Web セキュリティ

- AI ベースの機械学習
- 自動プロファイリング（ホワイトリスト）
- Web サーバーおよびアプリケーションシグネチャ（ブラックリスト）
- IP アドレスのレピュテーション
- IP アドレスのジオロケーション
- HTTP RFC コンプライアンス
- HTTP/2 のネイティブサポート
- OpenAPI 3.0 認証
- WebSocket の保護とシグネチャの適用
- MiTB（Man in the Browser）に対する保護

アプリケーション攻撃に対する保護

- OWASP トップ 10
- クロスサイトスクリプティング
- SQL インジェクション
- クロスサイトリクエストフォージェリ
- セッションハイジャック
- 内蔵脆弱性スキャナ
- サードパーティ製脆弱性スキャナとの統合（仮想パッチ）
- アップロードされたファイルの AV / サンドボックスによるスキャン

セキュリティサービス

- Web サービスシグネチャ
- XML および JSON プロトコル適合性
- マルウェア検知
- 仮想パッチ
- プロトコル検証
- ブルートフォース攻撃に対する保護
- Cookie の署名および暗号化
- 脅威のスコア評価と重み付け
- 構文ベースの SQLi 検知
- HTTP ヘッダーセキュリティ
- エラーメッセージのカスタマイズとエラーコードハンドリング
- オペレーティングシステム侵入シグネチャ
- 既知の脅威およびゼロデイ攻撃に対する保護
- L4 ステートフルネットワークファイアウォール
- DoS 防御
- 複数のセキュリティ要素を活用する先進の相関的保護
- 情報漏洩防止
- Web サイト改ざんに対する保護

アプリケーションデリバリ

- レイヤー 7 サーバーロードバランシング
- URL リライト
- コンテンツのルーティング
- HTTPS / SSL オフロード
- HTTP コンテンツ圧縮
- キャッシング

認証

- アクティブ / パッシブ認証
- サイトパブリシング、SSO
- 二要素認証対応の RSA アクセス
- LDAP、RADIUS、SAML のサポート
- SSL クライアント証明書のサポート
- CAPTCHA と RBE（Real Browser Enforcement）

管理 / レポート

- Web ユーザーインタフェース
- コマンドラインインタフェース
- FortiView グラフィカル分析 / レポートツール
- 複数の FortiWeb デバイスの一元管理
- アクティブ / アクティブ HA クラスタリング
- REST API
- ログ管理 / レポート機能の一元化
- ユーザー / デバイス追跡
- リアルタイム表示ダッシュボード
- ボットダッシュボード
- OWASP トップ 10 攻撃分類
- 地理的 IP 分析
- SNMP、Syslog および E メールのログ管理 / モニタリング
- 完全な RBAC（ロールベースのアクセス制御）対応の管理ドメイン

その他

- IPv6 対応
- HTTP/2 から HTTP 1.1 への変換
- HSM の統合
- シームレスな PKI の統合
- ActiveSync / MAPI アプリケーション、OWA、FTP の添付ファイルのスキャン
- 複数のアクティブなアプライアンス間の同期をサポートする構成同期機能による高可用性
- 導入を簡素化する自動セットアップ機能およびデフォルト構成による設定
- 一般的なアプリケーションとデータベース用のセットアップウィザード
- 一般的な Microsoft アプリケーション（Exchange、SharePoint、OWA など）向けの事前構成
- FortiWeb VM に対する OpenStack のサポート
- Drupal、Wordpress アプリケーション向けの事前定義済みセキュリティポリシー
- WebSocket のサポート

技術仕様



	FortiWeb 100E	FortiWeb 400E	FortiWeb 600E
ハードウェア			
10 / 100 / 1000 インタフェース（RJ45）	4	4 GbE RJ45、4 SFP GbE	4 GbE RJ45（2 バイパス）、4 SFP GbE
10 G BASE-SR SFP+ インタフェース	—	—	—
SSL/TLS プロセシング	ソフトウェア	ソフトウェア	ハードウェア
USB インタフェース	2	2	2
ストレージ	32 GB SSD	480 GB SSD	480 GB SSD
形状	デスクトップ	1 U	1 U
電源	単一	単一	冗長
システム性能			
スループット	50 Mbps	250 Mbps	750 Mbps
レイテンシ	5 ミリ秒未満	5 ミリ秒未満	5 ミリ秒未満
高可用性	アクティブ / パッシブ、アクティブ / アクティブクラスタリング	アクティブ / パッシブ、アクティブ / アクティブクラスタリング	アクティブ / パッシブ、アクティブ / アクティブクラスタリング
アプリケーションライセンス	無制限	無制限	無制限
管理ドメイン（ADOM）	—	32	32
数値はすべて「最大」の性能値であり、システム構成に応じて異なります。			
サイズ			
高さ x 幅 x 奥行	41 × 210 × 133 mm	44 × 438 × 416 mm	44 × 438 × 416 mm
重量	1.1 kg	9.97 kg	9.97 kg
ラックマウント	オプション	○	○
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	110 V / 1.2 A、220 V / 1.2 A	100 V / 5 A、240 V / 3 A	100 V / 5 A、240 V / 3 A
消費電力（平均）	18 W	109 W	109 W
放熱	74 BTU/h	446.3 BTU/h	446.3 BTU/h
動作温度	0 ～ 40 °C	0 ～ 40 °C	0 ～ 40 °C
保管温度	-25 ～ 70 °C	-25 ～ 70 °C	-25 ～ 70 °C
湿度	10 ～ 90%（結露しないこと）	10 ～ 90%（結露しないこと）	10 ～ 90%（結露しないこと）
準拠規格・認定			
準拠規格	FCC Class A Part 15、RCM、VCCI、CE、UL/cUL、CB	FCC Class A Part 15、RCM、VCCI、CE、UL/CB/cUL	FCC Class A Part 15、RCM、VCCI、CE、UL/CB/cUL

技術仕様




	FortiWeb 1000E	FortiWeb 2000F	FortiWeb 3000F	FortiWeb 4000F
ハードウェア				
10 / 100 / 1000 インタフェース（RJ45）	6（4 バイパス）、4x SFP GbE（非バイパス）	4 GbE（4 バイパス）、4 SFP GbE	8 GbE（8 バイパス）	8 GbE（8 バイパス）
10 G BASE-SR SFP+ インタフェース	2	4	10（2 バイパス）	10（2 バイパス）
40 G QSFP	—	—	—	2 バイパス
SSL/TLS プロセシング	ハードウェア	ハードウェア	ハードウェア	ハードウェア
USB インタフェース	2	2	2	2
ストレージ	2 × 1 TB	2 × 480 GB SSD	2 × 960 GB SSD	2 × 960 GB SSD
形状	2 U	2 U	2 U	2 U
電源	ホットスワップ対応冗長電源	ホットスワップ対応冗長電源	ホットスワップ対応冗長電源	ホットスワップ対応冗長電源
システム性能				
スループット	1.3 Gbps	5 Gbps	10 Gbps	70 Gbps
レイテンシ	5 ミリ秒未満	5 ミリ秒未満	5 ミリ秒未満	5 ミリ秒未満
高可用性	アクティブ / パッシブ、アクティブ / アクティブクラスタリング	アクティブ / パッシブ、アクティブ / アクティブクラスタリング	アクティブ / パッシブ、アクティブ / アクティブクラスタリング	アクティブ / パッシブ、アクティブ / アクティブクラスタリング
アプリケーションライセンス	無制限	無制限	無制限	無制限
管理ドメイン（ADOM）	64	96	96	192

数値はすべて「最大」の性能値であり、システム構成に応じて異なります。

サイズ				
高さ x 幅 x 奥行	88 × 430 × 501.20 mm	88 × 438 × 560 mm	88 × 444 × 574 mm	88 × 444 × 574 mm
重量	12.8 kg	15 kg	22.5 kg	22.5 kg
ラックマウント	○（フランジが必要）	○	○	○
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	100 ～ 240 V AC、50 ～ 60 Hz
最大電流	100 V / 5 A、240 V / 3 A	120 V / 6 A、240 V / 3 A	120 V / 2.6 A、240 V / 1.3 A	120 V / 3 A、240 V / 1.5 A
消費電力（平均）	140 W	200 W	200 W	248.5 W
放熱	471 BTU/h	1433 BTU/h	1045.5 BTU/h	1219.8 BTU/h
動作温度	0 ～ 40 ºC	0 ～ 40 ºC	0 ～ 40 ºC	0 ～ 40 ºC
保管温度	-20 ～ 70 ºC	-20 ～ 70 ºC	-20 ～ 70 ºC	-20 ～ 70 ºC
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）	5 ～ 90%（結露しないこと）
準拠規格・認定				
準拠規格	FCC Class A Part 15、RCM、VCCI、CE、UL/CB/cUL	FCC Class A Part 15、RCM、VCCI、CE、UL/CB/cUL	FCC Class A Part 15、RCM、VCCI、CE、UL/CB/cUL	FCC Class A Part 15、RCM、VCCI、CE、UL/CB/cUL

技術仕様

仮想マシン	FortiWeb VM（1 vCPU）	FortiWeb VM（2 vCPU）	FortiWeb VM（4 vCPU）	FortiWeb VM（8 vCPU）
システム性能				
HTTP スループット	25 Mbps	100 Mbps	500 Mbps	3 Gbps
アプリケーションライセンス	無制限	無制限	無制限	無制限
管理ドメイン（ADOM）	4 ～ 64（割り当てられているメモリによって異なります）			
仮想マシン				
サポートするハイパーバイザー	VMware、Microsoft Hyper-V、Citrix XenServer、Open Source Xen、VirtualBox、KVM、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud、Oracle Cloud. サポートするハイパーバイザーのバージョンについては、FortiWeb VM インストールガイドを参照してください。			
仮想 CPU 数（最小 / 最大）	1	2	2 / 4	2 / 8
仮想 NIC 枚数（最小 / 最大）	1 / 10	1 / 10	1 / 10	1 / 10
ストレージ容量（最小 / 最大）	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
メモリ（最小 / 最大）	1,024 MB / 無制限（64-bit の場合）	1,024 MB / 無制限（64-bit の場合）	1,024 MB / 無制限（64-bit の場合）	1,024 MB / 無制限（64-bit の場合）
推奨メモリ	8 GB	8 GB	8 GB	8 GB
高可用性（HA）	○	○	○	○

数値は、ネットワークトラフィックとシステム構成によって異なります。測定条件：Dell PowerEdge R710 サーバー（2 x Intel Xeon E5504 2.0 GHz 4MB Cache）、VMware ESXi 5.5、FortiWeb Virtual Applicance（4 vCPU および 8 vCPU）は 4 GB vRAM、FortiWeb Virtual Applicance（2 vCPU）は 4 GB vRAM

コンテナアプライアンス	FortiWeb VMC01	FortiWeb VMC02	FortiWeb VMC04	FortiWeb VMC08
システム性能				
HTTP スループット（最大）	25 Mbps	100 Mbps	500 Mbps	3 Gbps
アプリケーションライセンス	無制限	無制限	無制限	無制限
管理ドメイン（ADOM）	4 to 64 based on the amount of memory allocated			
仮想アプライアンス				
サポートするコンテナマネージャ	Docker			
仮想 NIC 枚数（最小 / 最大）	1 / 10	1 / 10	1 / 10	1 / 10
ストレージ容量（最小 / 最大）	30 GB / 500 GB	30 GB / 500 GB	30 GB / 500 GB	30 GB / 500 GB
メモリ（最小）	4 GB	4 GB	4 GB	4 GB
推奨メモリ	8 GB	8 GB	8 GB	8 GB
高可用性（HA）	—	—	—	—

スループットおよびその他の基準値は、各バージョンで許容される最大値を掲載しています。数値は、ネットワークトラフィックとシステム構成によって異なります。

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

お問い合わせ