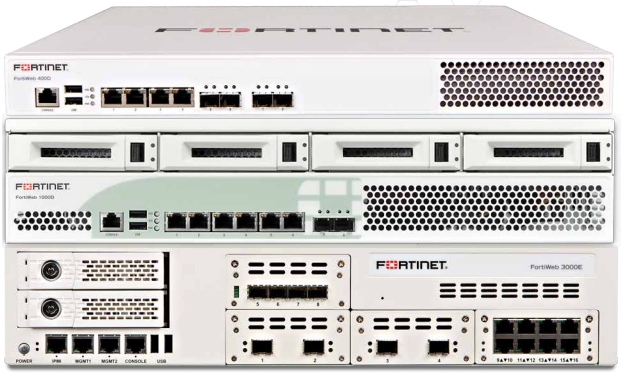
FortiWeb

FortiWeb 400D、600D、1000E、2000E、3000E、3010E、4000E、VM

FortiWeb は、既知 / 未知両方の脆弱性に対するエクスプロイトの攻撃から、ホスティングされている Web アプリケーションを保護する WAF（Web アプリケーションファイアウォール）です。多層型の相関的な検知メソッドを活用することで、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。



アクセラレーションとパフォーマンス

マルチコアプロセッサとハードウェアベースの SSL ツールの組み合わせにより、超高速の保護された WAF スループットを提供します。

アプリケーションの保護

クロスサイトスクリプティングや SQL インジェクションをはじめとする OWASP トップ 10 の攻撃からアプリケーションを保護します。

検知機能の強化

先進の検知ツール群を内蔵し、利用状況の監視、ユーザーセションの追跡、不審なコマンドの解析を実行することで巧妙な攻撃も検知します。

ハイライト

- 最大20 Gbpsのスループットによるハイパフォーマンス
- 相関的な多層型脅威スキャン機能
- ユーザーのスコア評価とセッション追跡
- FortiGateおよびFortiSandboxとの統合による容易な導入と保護機能の強化
- 脆弱性スキャナ機能
- ボットネットに対する保護を実現するトランスペアレントなユーザー検証

FortiCare Worldwide Support

support.fortinet.com

FortiGuard Security Services

www.fortiguard.com

第三者機関の認定

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

ハイライト

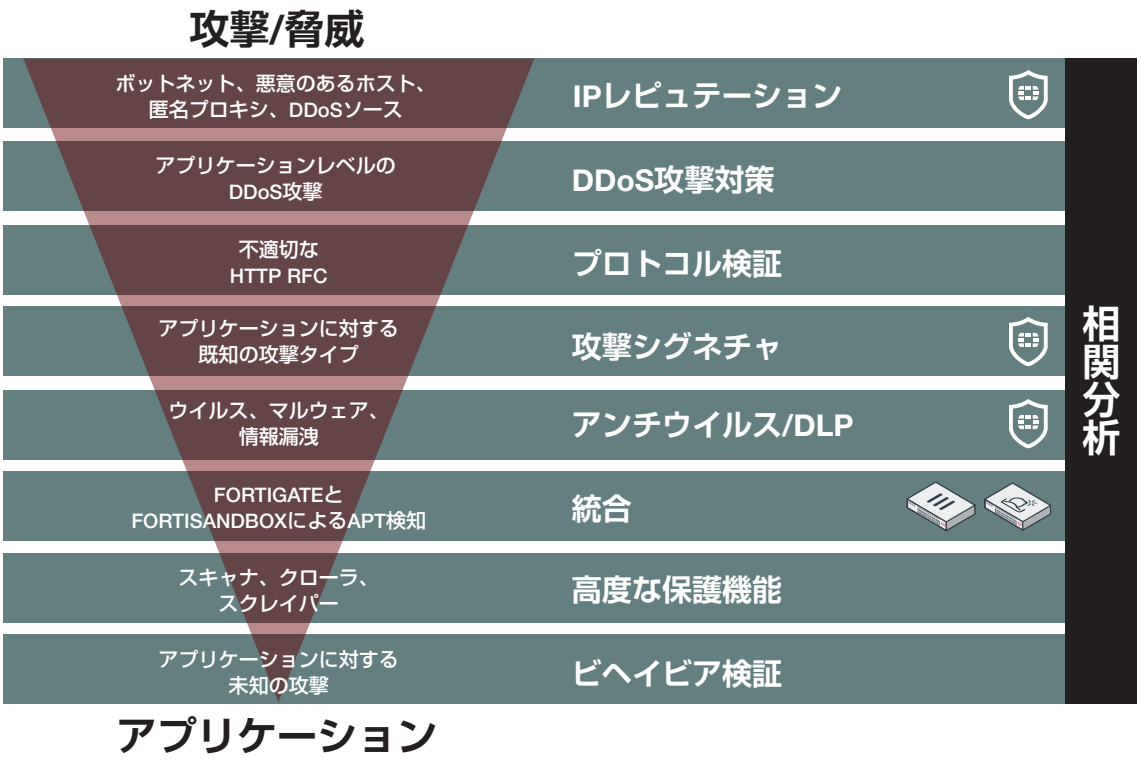
インターネットに接続している Web アプリケーションは、クロスサイトスクリプティング、SQL インジェクション、レイヤー 7 Denial of Service（DoS）などの攻撃にさらされています。企業内の Web アプリケーションの場合、ネットワークのペリメータにおける防御対策によって保護されていると考える企業の内部ネットワークに攻撃者がアクセス可能になれば、いとも簡単に侵害を受けてしまいます。通常最大の弱点となるのはカスタムコードで、その理由は企業の開発チームが新しいタイプの攻撃すべてを熟知することは不可能であるためです。しかしながら、商用コードの脆弱性はさらに深刻です。コードのパッチやセキュリティ修正が提供されても、多くの企業はそれらをすぐに適用するためのリソースを抱えていないのです。また、すべてのパッチを適用し、社内のシステム保護を担当する大勢の開発者を抱えていたとしても、ゼロデイ攻撃の脅威によって企業は無防備な状態に陥る可能性があり、その対応策は攻撃を受けた後に講じるしかありません。

総合的な Web アプリケーションセキュリティを実現する FortiWeb

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外部 / 内部向けの Web ベースアプリケーションに提供します。IP レピュテーションサービスによって、ボットネットやその他の悪意のあるソースが被害を及ぼす前にそれらを自動的に検知し遮断することができます。DoS 攻撃の検知と保護機能は、レイヤー 7 DoS 攻撃によるオーバーロードからアプリケーションを安全に保護します。FortiWeb は、HTTP RFC 準拠を厳格に検証し、リクエストが操作されたものでないことをチェックします。リクエストは FortiWeb のシグネチャに対するチェックが実行され、無害であることを確認するために既知の攻撃タイプであるかどうか比較検証されます。添付ファイルやコードは、すべて FortiWeb に内蔵されたアンチウイルスおよびアンチマルウェアサービスで検疫が行われます。FortiWeb の自動学習型ビヘイビア検知エンジンは、既知の攻撃を検知するテストを通過したすべてのリクエストを再検査します。ユーザーが設定した、または自動設定されたパラメータに適合しないリクエストは、すべてブロックされます。そして最後に、FortiWeb は異なるセキュリティレイヤーの複数のイベントが相関する箇所で相関エンジンによる分析を実行し、より正確な判断を行ってもっとも巧妙な攻撃に対する保護対策を支援します。このような複数のセキュリティ対策の組み合わせによって、シグネチャファイルベースのシステムでは検知できないゼロデイ攻撃の脅威を含む Web アプリケーションへのあらゆる攻撃に対するほぼ 100% の保護が実現します。

脆弱性スキャナ機能

FortiWeb は、追加の費用なしですべてのアプライアンスに Web アプリケーション脆弱性スキャナを搭載している唯一の製品で、PCI DSS のコンプライアンスを支援します。FortiWeb の脆弱性スキャナは、アプリケーションのあらゆる要素の詳細なスキャンを実行し、アプリケーションの潜在的な弱点を徹底的に検証します。FortiGuard Labs が提供する定期的なアップデートによって、脆弱性スキャナは常に最新状態に保たれます。



ハイライト

FortiGate および FortiSandbox 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。

FortiWeb は、先進の脅威検知プラットフォーム、FortiSandbox との統合が可能な数あるフォーティネット製品のひとつです。FortiSandbox との統合により、脅威に関する情報を共有し、サンドボックス環境で検知された脅威をブロックするように構成することができます。Web サーバーにアップロードされたファイルを FortiSandbox および FortiSandbox Cloud に送信して分析することも可能です。悪意のあるファイルが特定されると瞬時にアラートが送信され、以後類似のファイルは速やかにブロックされます。

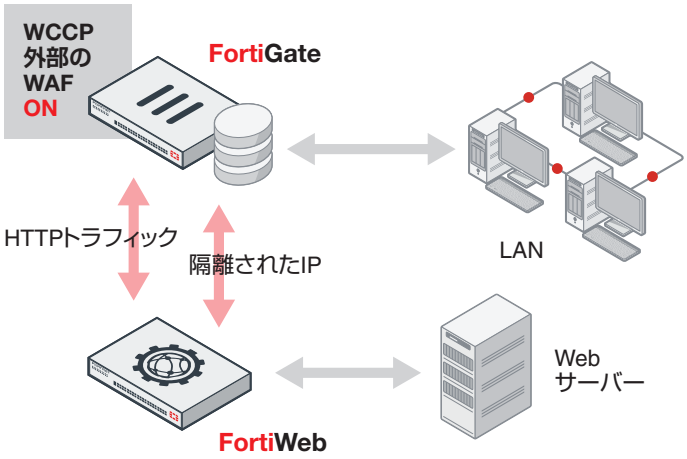
FortiGate との統合により、FortiGate ファイアウォールで検出・確保された隔離 IP アドレスの共有が可能になりました。FortiWeb は、FortiGate による定期的ポーリングを通じて、常に最新の感染した（または感染が疑われる）内部ソースリストを保有しており、感染したデバイスから送信されたトラフィックによる被害の拡大を防止します。

さらに、FortiGate ユーザーはフォーティネット製品ベースのネットワークに FortiWeb を容易に導入することができます。WCCP プロトコルを使用すれば、ルータや DNS サービスを手動で設定することなく、HTTP トラフィックが FortiWeb の検査を受けるように FortiGate を設定できます。ユーザーは、カスタムルールを設定して包括的で詳細な転送ポリシーを変更することで、特定のトラフィックをルーティングできます。

ユーザーのスコア評価とセッション追跡機能を搭載した高度な誤検知対策ツール

Web アプリケーションファイアウォールが適切に設定されていない場合、誤検知が発生して問題を引き起こす可能性があります。WAF の導入は数分で完了することもありますが、誤検知を最小限に抑えるためのチューニングには数日から数週間かかることがあります。さらに、アプリケーションや環境の変更に合わせて定期的な調整も必要です。FortiWeb には、アラートチューニング、ホワイトリスト、例外の自動学習、相関に基づいた脅威検知、SQL ベースのインジェクション攻撃を検証する高度な構文分析など、この問題を解決するための先進的なツールが数多く搭載されています。

FortiWeb は、ユーザーのスコア評価機能とセッション追跡機能を採用した唯一の WAF で、フォーティネットの誤検知対策ツールをさらに強化します。管理者は、FortiWeb の任意の WAF 保護機能に脅威レベルを追加して、トリガーしきい値を設定することができます。これにより、ユーザセッション全体で複数イベントの違反スコアを超過したユーザーに対しブロック、報告、または監視が可能になります。これほど高水準のカスタマイズや高度な相関分析が WAF で可能になったのは初めてのことで、管理者が設定した重要度レベルに応じて誤検知の件数は大幅に減少します。



FortiWeb が FotiGate とシームレスに統合することで、HTTP トラフィックの検査および隔離された IP 情報の共有が可能になります。

FortiWeb によるユーザーのトラッキング

FortiWeb は、Web アプリケーションへの認証を行うユーザーを監視すると同時に、認証後のユーザーのアクティビティをすべて追跡します。トラフィックおよび攻撃のログはすべてユーザー名と関連付けられているため、ユーザーレベルでルールの適用およびフォレンジック分析が可能です。

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 3 つのオプションを選択することができます。FortiWeb IP 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、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。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。

ハイライト

仮想パッチ

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 IBM QRadar、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 によって自動で瞬時に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。

超高速の SSL オフロード

FortiWeb ではハードウェアによる高速な SSL オフロード機能が提供され、大半のモデルは数万の Web トランザクションを処理することが可能です。ASIC ベースのチップセットを活用するほぼリアルタイムの復号と暗号化により、FortiWeb はセキュアなアプリケーションを標的とする脅威を容易に検知できます。

アプリケーションデリバリと認証

FortiWeb は、先進のレイヤー 7 ロードバランシングおよび認証オフロードサービスを提供します。FortiWeb の優れたアプリケーション識別型レイヤー 7 ロードバランシング機能により、複数のサーバー上にアプリケーションを容易に拡張することができると同時に、SSL オフロードと組み合わせることでセキュアなアプリケーショントラフィックの負荷分散が可能です。HTTP コンテンツ圧縮機能を搭載する FortiWeb は、コンテンツリッチなアプリケーションに対応するために帯域幅の利用率とユーザーへの応答時間を改善することができます。認証オフロード機能は、LDAP、NTLM、Kerberos、RADIUS、さらに RADIUS や RSA SecureID 対応の二要素認証など、数多くの認証サービスとの統合が可能です。このような認証サービスを利用することで、Web サイトの容易なパブリッシングが可能になると同時に、Outlook Web Access や SharePoint などの Microsoft アプリケーションをはじめとするあらゆる Web アプリケーションで Single Sign On（SSO）を利用できます。また FortiWeb は、よく利用するコンテンツをキャッシュすることでアプリケーションの応答時間を改善し、同じ情報が必要な時に毎回リクエストする場合に比べ短時間でユーザーにサービスを提供することができます。

仮想マシンと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、主要なハイパーバイザ（VMware、Microsoft Hyper-V、Citrix XenServer、Open Source Xen、KVM）のいずれとも連携が可能です。FortiWeb は、Amazon Web Services および Microsoft Azure にも対応しています。

管理 / レポーティング機能の一元化

FortiWeb は、複数のアプライアンスの管理、そしてお客様のアプリケーションを標的とする攻撃に対して有効な洞察を得るために必要なツールを提供します。フォーティネットが提供する、VMware ベースの一元管理ユーティリティを使用して、単一の管理コンソールから複数の FortiWeb ゲートウェイの構成と管理を行うことができます。ネットワーク全体に渡る攻撃の集約ビューが必要な場合には、フォーティネットのレポートアプライアンスである FortiAnalyzer と FortiWeb を容易に統合し、複数の FortiWeb デバイスのログおよびレポートの統合と一元化が可能です。

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

- 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 レピュテーション
- IP 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

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）

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
- 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 および RADIUS のサポート
- SSL クライアント証明書のサポート

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
- 複数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
- 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
- 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
- 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 400D	FortiWeb 600D	FortiWeb 1000E
ハードウェア			
10 / 100 / 1000インタフェース（RJ-45）	4 GbE RJ45、4 SFP GbE	4 GbE RJ45（2 バイパス）、 4 SFP GbE	6（4 バイパス）、 4x SFP GbE（非バイパス）
10 G BASE-SR SFP+インタフェース	0	0	2
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
内蔵ストレージ	240 GB SSD	240 GB SSD	2 x 2 TB
形状	1 U	1 U	2 U
電源	単一	冗長	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	100 Mbps	250 Mbps	1.3 Gbps
レイテンシ	ミリ秒未満	ミリ秒未満	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	64
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（mm）	44 x 438 x 416	44 x 438 x 416	88 x 430 x 501.20
重量	9.97 kg	9.97 kg	12.8 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
電流（最大）	100 V / 5A、240 V / 3A	100 V / 5A、240 V / 3A	100 V / 5A、240 V / 3A
消費電力（平均）	109 W	109 W	140 W
放熱	446.3 BTU/h	446.3 BTU/h	471 BTU/h
動作温度	0 ～ 40 ℃	0 ～ 40 ℃	0 ～ 40 ℃
保管温度	-25 ～ 70 ℃	-25 ～ 70 ℃	-20 ～ 70 ℃
湿度	10 ～ 90%（結露しないこと）	10 ～ 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, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL

FortiWeb 400D

FortiWeb 600D

FortiWeb 1000E

技術仕様

	FortiWeb 2000E	FortiWeb 3000E	FortiWeb 3010E	FortiWeb 4000E
ハードウェア				
10 / 100 / 1000インタフェース（RJ-45）	4 バイパス、 4 SFP GbE（非バイパス）	8 バイパス、 4 SFP GbE（非バイパス）	8 バイパス、 4 SFP GbE（非バイパス）	8 バイパス、 4 SFP GbE（非バイパス）
10 G BASE-SR SFP+インタフェース	2	4	4（2 バイパス）	4（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
内蔵ストレージ	2 x 1 TB	2 x 2 TB	2 x 2 TB	2 x 2 TB
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	2.5 Gbps	5 Gbps	5 Gbps	20 Gbps
レイテンシ	ミリ秒未満	ミリ秒未満	ミリ秒未満	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	64	64	64
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（mm）	88 x 438 x 530	88 x 444 x 574	88 x 444 x 574	88 x 444 x 574
重量	15 kg	22.5 kg	22.5 kg	22.5 kg
ラックマウント	○	○	○	○
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
電流（最大）	120 V / 6 A、240 V / 3 A	120 V / 2.6 A、240 V / 1.3 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）	200 W	200 W	200 W	248.5 W
放熱	1433 BTU/h	1045.5 BTU/h	1045.5 BTU/h	1219.8 BTU/h
動作温度	0 ～ 40 ℃	0 ～ 40 ℃	0 ～ 40 ℃	0 ～ 40 ℃
保管温度	-25 ～ 70 ℃	-25 ～ 70 ℃	-25 ～ 70 ℃	-25 ～ 70 ℃
湿度	5 ～ 95%（結露しないこと）	5 ～ 95%（結露しないこと）	5 ～ 95%（結露しないこと）	5 ～ 95%（結露しないこと）
準拠規格・認定				
準拠規格	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL

FortiWeb 2000E

FortiWeb 3000E

FortiWeb 3010E

FortiWeb 4000E

技術仕様

	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	2 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、KVM、Amazon Web Services（AWS）、Microsoft Azure 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 / 4（10 VMware ESX）	1 / 4（10 VMware ESX）	1 / 4（10 VMware ESX）	1 / 4（10 VMware ESX）
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）	1,024 MB / 無制限（64-bit）	1,024 MB / 無制限（64-bit）	1,024 MB / 無制限（64-bit）
推奨メモリ	4 GB	4 GB	4 GB	4 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

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 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ