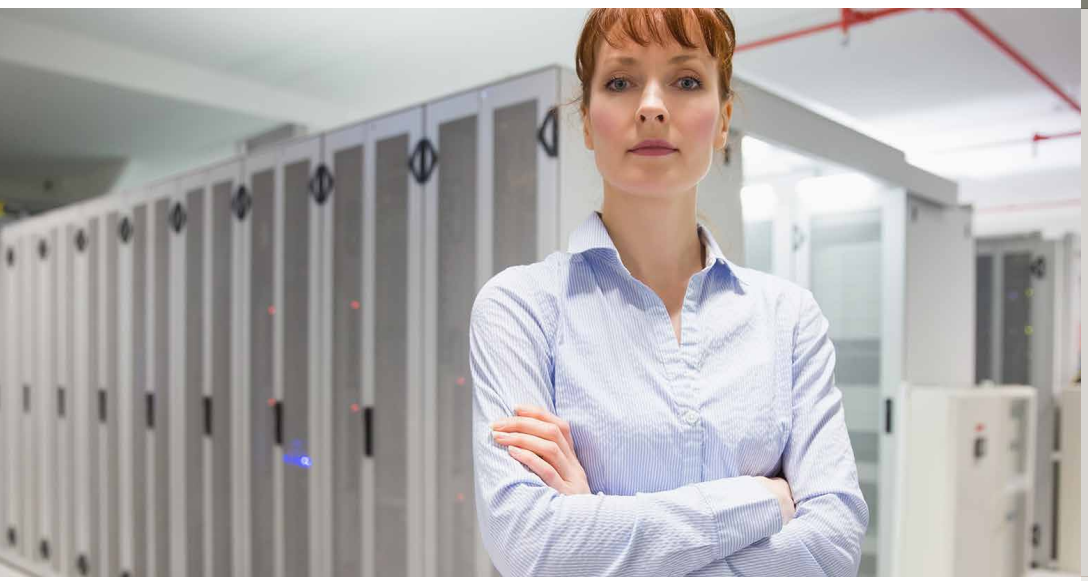
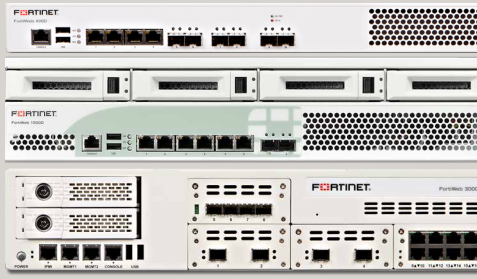
DATA SHEET



FortiWeb
Web アプリケーションファイアウォール



FortiWeb

FortiWeb 1000D

Web アプリケーションファイアウォール

攻撃の標的になりやすい Web アプリケーション

PCI DSS（Payment Card Industry Data Security Standards）のコンプライアンスは、大半の企業が Web アプリケーションファイアウォール（WAF）を展開する主な理由となっていますが、保護されていない Web アプリケーションはレベルの低いハッカーでさえも容易に侵入できるエントリーポイントとなることを多くの企業が認識しています。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

業界最高レベルの Web アプリケーションファイアウォールのパフォーマンス

- 脆弱性スキャナ機能
- レイヤー 7 のサーバーロードバランシング機能
- ビヘイビアベースの攻撃検知
- FortiGuard の IP レピュテーション、攻撃シグネチャ、FortiSandbox Cloud、アンチウイルスサービス
- 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 との統合による容易な導入配備
- FortiGate が隔離した IP アドレスのポーリング
- FortiSandbox との統合による APT 検知
- 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
- 導入後すぐに利用可能な自動化された攻撃からの保護機能
- ネットワークおよびアプリケーションレイヤーに対する DoS 攻撃からの保護機能
- 認証、サイトパブリシング、SSO

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

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。

技術仕様

	FortiWeb 1000D
ハードウェア	
10 / 100 / 1000 インタフェース（RJ-45）	6（4 バイパス）、2x SFP GbE（非バイパス）
10 G BASE-SR SFP+ インタフェース	0
USB インタフェース	2
内蔵ストレージ	2 x 2 TB
形状	2 U
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 Gbps
レイテンシ	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
アプリケーションライセンス	無制限
管理ドメイン（ADOM）	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 368
重量	12.5 kg
ラックマウント	○（フランジが必要）
動作環境	
AC 電源	100 - 240 V AC、50 – 60 Hz
電流（最大）	100 V / 5 A、240 V / 3 A
消費電力（平均）	115 W
放熱	471 BTU/h
動作温度	0 ～ 40 ℃
保管温度	-25 ～ 70 ℃
湿度	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

FortiWeb 1000D

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