

Net Attest® WAF

Webアプリケーションファイアウォール

ネットアテスト ワフ



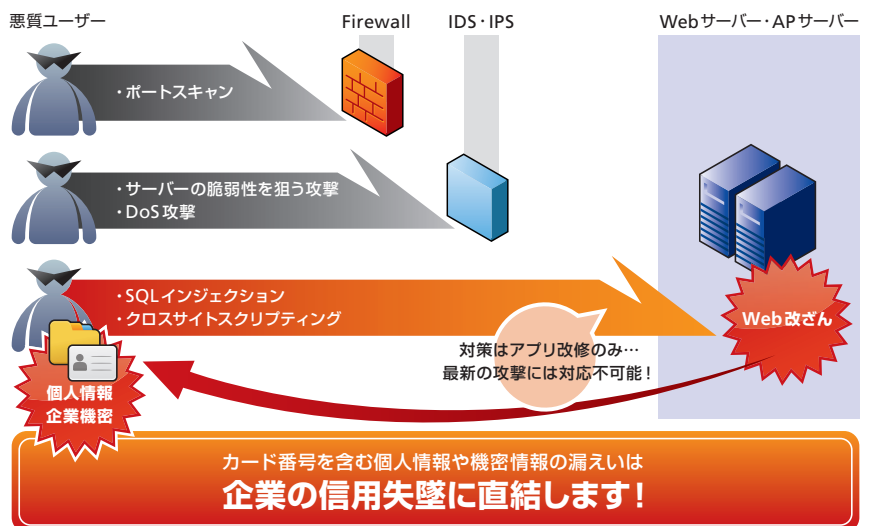
手軽な導入と自動化された運用で Webアプリに高度なセキュリティを提供

- シグネチャと4つのデータチェックでWebアプリケーションへの攻撃を排除
- 自動更新されるシグネチャにより最新の攻撃にも自動的に対応
- わずか4ステップで利用が開始でき、導入がスムーズ
- インライン設置ならネットワーク構成の変更なく導入可能
- シグネチャベースで導入後の運用が容易

Webサーバーを確実に守らなければ、あなたの会社は信頼を失うかもしれません

SQLインジェクションやクロスサイトスクリプティングという攻撃手法をご存じですか？かつては、ネットワークやWebサーバー自体の脆弱性が狙われていましたが、最近では決済処理や個人情報を扱うWebアプリケーションを狙った攻撃が主流になっています。Webアプリケーションを狙う攻撃はHTTP（ポート80）を使用するため、ファイアウォールでは防げません。また個別に開発、カスタマイズされたWebアプリケーションは、IDS・IPSでも守れません。多くのWebアプリケーションで個人情報や商品情報が取り扱われており、Webサイトの改ざんや情報漏洩が発生した場合の被害は深刻です。

■ 従来のセキュリティ技術では防げない脅威が増大



Net'Attest WAFはWeb専用セキュリティ製品です

Webアプリケーションを守るために利用され始めたのが、WAF (Web Application Firewall) と呼ばれる製品です。WAFはHTTPリクエストを中身までチェックすることでWebアプリケーションへの攻撃を検知、防御します。個別開発されたWebアプリケーションを、簡単に攻撃から守ることができる最新のソリューションです。

■ Webアプリケーションを攻撃から保護



クレジットカード業界でも認められたセキュリティ標準を、貴社サイトにも

クレジットカード情報を取り扱うサイトが守るべきセキュリティ指標にPCI DSSがあります。PCI DSSでは守るべきセキュリティの概念だけではなく、具体的な対策が示されています。その中では、Webアプリケーションを保護するために必要な対策としてWAFの導入が求められています。WAFはクレジットカード業界でも有効性を認められたセキュリティ対策なのです。

【PCI DSS (抜粋)】

6-6 すべてのWebに面したアプリケーションは、以下のどちらかの手法を摘要することで、既知の攻撃から防御されなければならない。

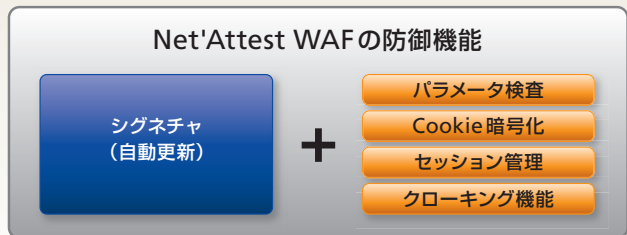
- カスタム・アプリケーション・コードについては、アプリケーションセキュリティに特化した組織に依頼して、定期的な検査を実施し、問題があれば改修する。
- 公開しているWebアプリケーションの手前に、Webアプリケーションファイアウォールをインストールする。

Net'Attest WAF 3つの機能ポイント



シグネチャベースなので 検知精度が高く、最新の攻撃にも自動的に対応

攻撃を検知、防御するために、Net'Attest WAFにはいくつもの防御技術を組み合わせて使用しています。シグネチャ技術を中心に、パラメータ検査やCookie暗号化、セッション管理、クローキング機能などの技術が採用されています。アンチウイルスソフトのように定期的にシグネチャを更新することで、最新の脅威にも自動的に対応可能とし、また、高い検知精度を実現しています。



シグネチャベースなので 面倒なポリシー策定なしで、すぐに使い始められる

WAFはその性質上、導入時の設定が難しい製品が少なくありません。自社専用にカスタマイズしたWebアプリケーションに合わせてポリシーを設定する必要があるからです。しかしNet'Attest WAFならそんな心配は無用。IPアドレスを設定してシグネチャの

自動更新を有効にするだけで、すぐにWebアプリケーションのセキュリティを向上できます。インラインで設置できるので、既存システムのネットワーク構成を変更する必要もありません。



シグネチャベースなので 見直しサイクルも不要で導入後の運用もラクラク

従来のWAF製品では、Webアプリケーションに合わせて個別にホワイトリストを設定する必要がありました。Webサイトに変更が生じるたびに再チューニングが求められるため、運用にはセキュリティとネットワークに深い知識を持つ人材が必要でした。それに対してNet'Attest WAFの運用で必要なのは、自動的に行われるシグネチャの更新を管理するだけ。何度も繰り返されるチューニング作業は不要です。



どのようなサイトにも対応する高い信頼性と柔軟性

高い耐障害性

Net'Attest WAFはコンパクトフラッシュから起動します。故障の原因となりやすいHDDを搭載しないことで、ハードウェア障害の可能性を極力排除しています。また障害発生時には自動的にバイパスされるため、万一のハードウェア故障でもWebサイトを止めることはありません。ミッションクリティカルなサイトやビジネスに直接つながるECサイトの保護にも、安心してご導入いただけます。

SSL通信に対応

現在、オンラインショップや個人情報を取り扱うサイトでは、SSLによる暗号化が広く採用されています。Net'Attest WAFはSSLに対応し、クライアント側のWebブラウザとの間でSSL暗号化処理を行ないます。Webを利用されるお客様には、安全なサイトを安心して使っていただけます。Webサーバー側でSSL暗号化処理を行わなくてよいので、サーバー負荷を軽減し、レスポンスを向上します。

様々なネットワークに対応

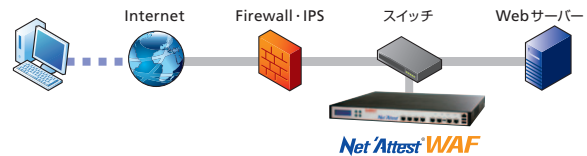
Net'Attest WAFの導入形態は、既存ネットワークに応じて柔軟に対応可能。既存システムのネットワーク構成を変えずに導入できるインライン設置のほか、ネットワーク上に故障ポイントを

増やさないプロキシ構成として組み込むこともできます。またWebサーバーが冗長化されたシステムでは、それぞれのWebサーバーの前段に組み込めばNet'Attest WAFも冗長化できます。

【インライン構成】



【プロキシ構成】



製品仕様



製品写真は参考画像になります。

モデル番号	WAF-ST51A
処理能力*	スループット：100~200Mbps HTTPリクエスト処理数：2,500 (/sec)
ネットワーク インターフェイス	10/100/1000BASE-T (X) 自動認識 & Auto-MDI-X ×3 (LAN1とLAN2、LAN8のみ使用)
筐体形状	EIA19 インチラックマウントタイプ
外形寸法 (W×H×D)	443mm×44mm×457mm
重量	14Kg
電源	90~264V AC、47~63Hz
最大消費電力	174VA
発熱量	593.9BTU/h、149.6kcal、174W
動作環境	温度5~40℃、湿度20~90% RH結露なきこと
適合規格	VCCI Class A、FCC Class A、CE、UL、RoHS

*処理能力は環境により異なります。

※記載の製品名は、各社の商標または登録商標です。

安全に関するご注意

正しく安全にお使いいただくために、ご使用前に必ず「取扱説明書」をお読みください。

Soliton

株式会社ソリトンシステムズ <http://www.soliton.co.jp>

〒160-0022 東京都新宿区新宿 2-4-3

TEL 03-5360-3811 FAX 03-3356-6354 netsales@soliton.co.jp

大阪営業所 06-6821-6777 福岡営業所 092-263-0400

名古屋営業所 052-963-9700 東北営業所 022-716-0766

札幌営業所 011-242-6111