

# Gateway AntiVirus (ウイルス対策) Intrusion Prevention Service (不正侵入検知・防御)

スパイウェアやその他の悪意のあるアクティビティをリアルタイムで阻止

Gateway AntiVirus/Intrusion Prevention Service (Gateway AV/IPS) は、アプライアンス用のシグネチャベースのセキュリティ機能です。ファイアウォールによる既知のスパイウェア、マルウェア、アプリケーション攻撃、UTM(統合脅威管理)においてリアルタイムの保護を提供します。

- » ゼロデイ保護を強化、スパイウェアやネットワーク経路での脅威からの保護
- » HTTP、FTP、SMTP、POP3 などの標準的なプロトコルをサポート
- » 既知の攻撃をシグネチャベースのセキュリティ対策で防御
- » 感染添付ファイルをロックし、デスクトップでの実行を防止
- » シグネチャの自動更新により常に最新の保護状態を維持
- » ブロックサイトリストがスパイウェア配布サイトへのアクセスを予防

## ゼロデイ保護を強化

インテリジェントレイヤードアーキテクチャは、先進のアプリケーションプロキシテクノロジーを通じて、多くのウイルス、トロイの木馬、スパイウェアの侵入、バッファオーバーフロー、その他の攻撃を積極的にブロックしています。

## 効率的なシグネチャの更新

シグネチャデータベースは、WildList ウィルスや zoo ウィルスを含む何千ものウィルスシグネチャで構成され、広範囲にカバーします。

侵入防止 (IPS) コンポーネントは、効率的に設計された実績のある商用シグネチャセットを採用し、継続的に更新されネットワークは常に最新の保護を受けます。

## 既知の攻撃源をブロック

特定の IP アドレスからの攻撃が認識されると、それ以降の同一 IP アドレスからの攻撃はダイナミックにブロックされます。

ブロックしないシステムをホワイトリストとして設定し、信頼するアプリケーションや送信先に継続的にアクセスして効率的な業務を継続することが可能です。

## スパイウェア対策のサポート

ブロックサイトリストは絶えず更新され、スパイウェアからネットワークを保護します。マルチレイヤーのアンチスパイウェア、「ドライブバイスパイウェア」ホストに接続しようとするスパイウェアのアクセスをブロックします。

## すべての主要トラフィックプロトコルを入口でスキャン

HTTP、FTP、SMTP、POP3 トラフィックをスキャンし、マルウェアと関連付けられる種類のファイルをゲートウェイでブロックします。脅威はネットワークへ浸入し、デスクトップやサーバーのセキュリティを無効にする前に阻止されるため、攻撃後にクリーンアップを行うための費用は管理者の時間を節約できます。

## 感染添付ファイルをロック

ネットワークの種類、ユーザー / グループ、プロトコル、重要度に基づいて、疑わしいトラフィックを許可、ブロック、ロックすることができます。

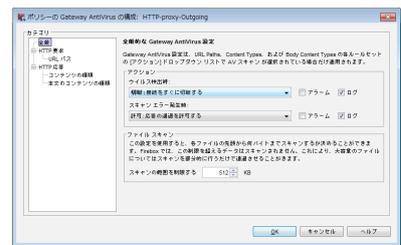
疑わしいと認識されたすべての添付ファイルをロックすることにより、悪意のあるペイロードのデスクトップ上での実行を防ぎます。確実に効果的な保護を提供するために ZIP、TAR、GZIP など多様な圧縮エンコードファイルをスキャンします。

## 隔離機能

AV エンジンによって捕捉されたメールを隔離し、IT 管理者がどのメールがウイルスに感染しているか調べることが可能。これにより、安全にファイルのウイルス除去を行い、業務遂行に関するリスクを軽減します。



IPS 設定画面



Gateway AntiVirus 設定画面

Gateway AntiVirus/IPS powered by 

ウォッチガード・テクノロジー・ジャパン株式会社



〒106-0041 東京都港区麻布台 1-11-9 CR 神谷町ビル 5 階 TEL:03.5797.7205 FAX:03.5797.7207

Web: <https://www.watchguard.co.jp>