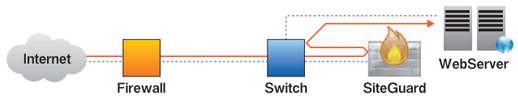
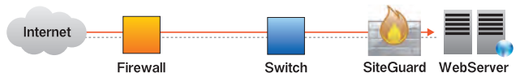
設置構成例

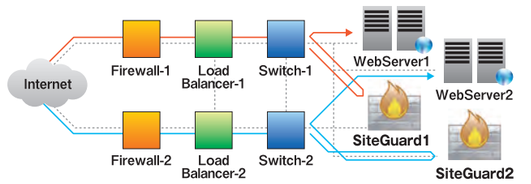
プロキシ構成(シングル)



インライン構成



プロキシ構成(冗長)



導入事例紹介

「SiteGuard」は、金融機関をはじめとする極めてクリティカルなシステムから、数十万サイトを運用する大規模ホスティングシステムまで、業種や規模を問わず、幅広い環境の企業・団体に導入されています。

- 建設・不動産
- 製造（食品、医療、電気機器、精密機器）
- 情報通信（キャリア、SI、ASP、ホスティング、データセンター）
- 金融業・保険（都銀、地銀、証券、生保、損保、ネット決済代行）
- 教育（大学、自治体教育センター）
- 公共（地方公共団体、研究機関、外郭団体）
- サービス（人材、広告代理、メディア、コンサルティング、エンターテイメント）他

ユーザの声

信頼できるシグネチャを採用したソフトウェア型の「SiteGuard」が防御を行うということで、必要以上のアプリケーションのチェックを軽減。アプリケーションの開発、改修のコスト及び工数の削減が実現できた。手間を煩わせない導入と運用が最大の魅力。（ネット通販業）

「SiteGuard」は他製品に比べ導入コストを抑えることができた。またウェブサイトに合わせてルールを設定する必要がなく、構築・運用が用意であることもユーザにはうれしい。（自治体）

選定のポイントは『ソフトウェア』・『国産』・『シンプル』。海外製品が多いなか、国産製品である「SiteGuard」は品質、サポートの面で安心。また、ソフトウェアであるため障害時の切り分け運用も可能。そして何よりも信頼できる高精度なシグネチャの実装により、シンプルな運用が可能。（金融グループ）

推奨動作環境

対応 OS	Red Hat Enterprise Linux 5/6/7 CentOS 5/6/7 Scientific Linux 6 ※各 32/64bit (x86_64) に対応。 ※対応 OS であれば、仮想環境 OS やクラウド上でも利用可能。
CPU	Intel Pentium互換CPU（クアッドコア以上を推奨）
メモリ	4GB以上を推奨
ハードディスク	空きが 20GB以上（ログの保存期間等による）
ネットワークインターフェース	TCP/IP 接続、100BaseT以上

機能一覧

防御機能	トラステッド・シグネチャ検査（ブラックリスト）
	トラステッド・シグネチャ更新（自動、手動）
	カスタム・シグネチャ検査（ブラックリスト、ホワイトリスト、しきい値）
	セッション管理（URL遷移検査、フォーム変数検査、CSRF防御）
	Cookie保護（暗号化、secure属性設定、シグネチャ検査）
	応答ヘッダ追加・削除
	URLデコードエラー検出
	DoS・ブルートフォース防御
	パラメータ数制限
管理機能	攻撃検知時の処理設定（ブロック、モニタリング、フィルタ）
	クライアントへ警告ページ送信・内容編集
	管理者へメール通知・内容編集
	ウェブ管理インターフェース（日本語、英語）
	複数インスタンス一元管理
	ロギング（syslog、ローカル）
	メールサマリレポート
	統計グラフ
	ログ解析レポート　※オプション

開発・販売元　株式会社ジェイピー・セキュア
〒212-0013 神奈川県川崎市幸区堀川町66-2 興和川崎西口ビル2F
TEL:044-201-4036　FAX:044-201-4037
E-Mail sales@jp-secure.com　URL http://www.jp-secure.com/

1505V130-3000

www.jp-secure.com

販売店

JP-Secure

SITEGUARD

トラステッド・シグネチャ搭載 | 純国産ウェブアプリケーションファイアウォール

ウェブサイトをいかに守るか？

企業の看板ともなったウェブサイト。管理者は日々発生する様々な脅威からウェブサイトを守らなければなりません。ウェブサイトの脆弱性を悪用する攻撃によって、改ざんや情報流出、閲覧者のウイルス感染、サービス運用の停止などが発生する危険性があります。さらには、被害者という側面だけでなく、自身の関知しないところで攻撃者の踏み台にされることで、結果として犯罪に加担してしまうケースもあります。管理者は、直接的な損害だけでなく、企業としての信用失墜など間接的な被害の影響も考慮して対策を講じなければなりません。

ビジネスからプライベートまで、必要不可欠なコミュニケーションツールとなったインターネット。そこに存在する様々な脅威は、日々形を変えながら私たちのインターネットアクセスを脅かしています。特に、多くの個人情報や機密情報を保有していたり、あるいは遅延や停止が許されない企業やECサイトの運営者にとって、ウェブアプリケーションをいかに安全に運用するかは、重要な課題となっています。ウェブアプリケーションへの攻撃を防ぐ最高のソリューションとして、いまウェブアプリケーションファイアウォールが求められています。

トラステッド・シグネチャ搭載の「SiteGuard」で、そのウェブにワンランク上の安心を。

「SiteGuard」は、日本のインターネット文化を熟知したスタッフによって開発された、純国産のウェブアプリケーションファイアウォール（WAF）です。

「SiteGuard」は、業界に先駆けて、トラステッド・シグネチャ（高品質・高性能なチューニング済み定義ファイル）を搭載したWAFであり、この技術・品質は多くの導入済みユーザによって実証されています。

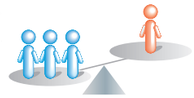
SITEGUARD
トラステッド・シグネチャ搭載
純国産ウェブアプリケーションファイアウォール

業界初のトラステッド・シグネチャを標準搭載

「SiteGuard」は、チューニングされた、高速で高品質のトラステッド・シグネチャを標準搭載。この国内屈指のセキュリティ・プロフェッショナルが提供するブラックリストは、第三者によるテスト結果においてもその優秀性を高く評価されています。

柔軟かつシンプルに、スムーズスタート&ラクラク運用

「SiteGuard」はポリシー策定することなく導入でき、トラステッド・シグネチャの自動更新により導入・運用負荷を大幅削減。また、ソフトウェアならではのネットワーク構成への柔軟な対応も可能です。

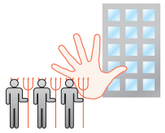


made in japan 完全国産の安心感

日本のウェブ文化を熟知した完全国産製品「SiteGuard」は、管理画面、マニュアル、サポート等の日本語対応はもちろんのこと、ユーザの安心感と満足感を倍増させます。

最高の防御機能

「SiteGuard」の最大の武器である「トラステッド・シグネチャ」。最新の攻撃に対応すべく、シグネチャは自動更新で、常にセキュアに保たれます。ユーザ独自の防御ルールやホワイトリストを作成するカスタマイズ機能も充実。Cookie保護やセッション管理、ブルートフォース防御など、シグネチャ検査以外の防御機能も豊富に搭載しています。



WAFの命、トラステッド・シグネチャは自動更新

新たな攻撃・脅威が発覚
- Site Guard → トラステッド・シグネチャの自動更新で対応
- 他WAF製品 → 攻撃を分析 → ポリシー作成 → テスト → 運用

ホーム画面

検出ログの一覧

検出ログの詳細

幅広い脅威に対応

ウェブアプリケーションの脆弱性を悪用する様々な脅威に対応し、安全なウェブサイトを実現します。

- SQLインジェクション
- クロスサイトスクリプティング
- クロスサイトリクエストフォージェリ（CSRF）
- ディレクトリトラバーサル
- OSコマンドインジェクション
- HTTPヘッダインジェクション
- フォースブラウジング
- ブルートフォース（ログインアタック等）
- クリックジャッキング

等

システムとの高い親和性

ソフトウェアの特性を生かし、システム環境に合わせて様々なネットワーク構成で導入可。プラットフォームも汎用サーバーから仮想環境、クラウドサービス上など、幅広い環境でご利用いただけます。リソース次第で性能を向上できるため、サイトの成長に合わせて拡張性も確保できます。

運用構成イメージ