

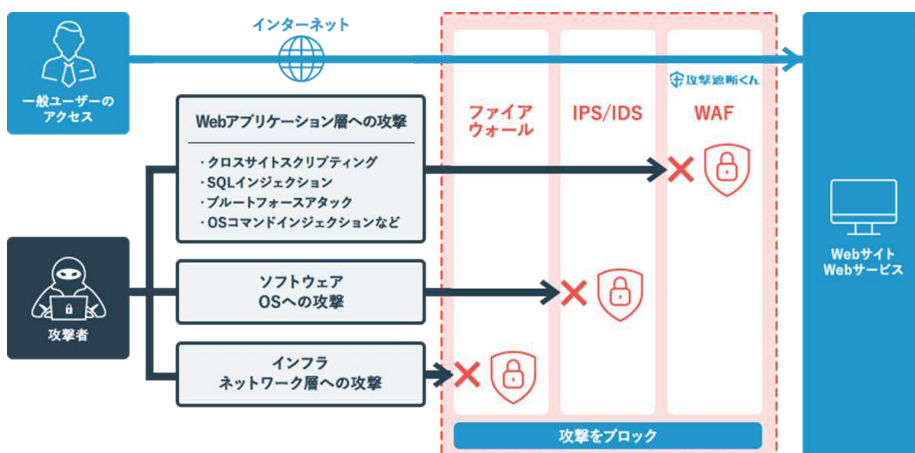
攻撃遮断くん

セキュリティ技術者不要で新たな脅威に瞬時に対応！クラウド型 WAF

Web セキュリティ対策の重要度が増す中、「攻撃遮断くん」は、あらゆる Web システムに導入可能な、独自開発のクラウド型 WAF（Web Application Firewall）サービスです。

WAF は、SQL インジェクションやクロスサイトスクリプティング（XSS）をはじめとした不正侵入による情報漏えいや Web サイト改ざんなどを防ぐファイアウォールです。

WAF は、従来の FW（ファイアウォール）や IDS / IPS では防ぐ事ができない攻撃にも対応します。



Web サービスからの
個人情報への窃取

サービス妨害攻撃による
サービスの停止

Web サイトの
改ざん

Web サービスへの
不正ログイン

対策情報の公開に伴い公知となる
脆弱性の悪用

重大な脅威を WAF で対策 攻撃遮断くん

「攻撃遮断くん」は、クラウド型の WAF（Web Application Firewall）製品です。情報漏えい、Web 改ざん、サーバーダウンを狙った Web サイトや Web サーバーへの攻撃を遮断することにより、Web セキュリティへの脅威から企業とユーザーを守ります。クラウド型のため、保守・運用に一切手間をかけることなく、24 時間 365 日の高セキュリティを実現します。また、業界で唯一の“サイバー保険”を付帯しています。

公開サイトの数が多くて、対策するサイトを決めることが難しい。

すべての公開サイトを対策すると、予算が膨大になるのではと不安。

自社での WAF 運用が難しい。日本語のサポートを受けたいので、海外製品では不安。

あらゆる Web システムに導入可能

クラウド型 WAF 唯一の定額制

国産だからできる 万全のサポート体制

他社の WAF では導入が困難な高トラフィックの Web サービスにも対応する独自開発のクラウド連動型 WAF を提供。

Web サイト数やトラフィック量の増加に関わらず一定額でご利用いただけるプランを提供。

24 時間 365 日の技術サポート体制で個別カスタマイズにも柔軟に対応。

サーバセキュリティタイプ

1. 様々な環境での導入が可能

クラウド型（SaaS）のため、各社様のクラウド環境（IaaS）に対応しております。

2. サービスへの影響なし

通信はクラウド上の攻撃遮断くん監視センターとのログのみとなるため、障害発生時にもお客様側のサービスに影響しません。



サーバーに攻撃遮断くんのエージェントをインストールして、アクセスログ / システムログをクラウド上の監視センターに送ります。クラウド上で攻撃の判定をし、遮断命令を出してサーバーを攻撃から守ります。

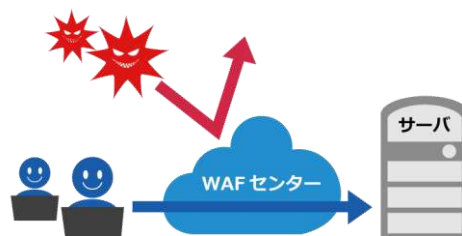
Web / DDoS セキュリティタイプ (WAF + DDoS 対策)

1. ネットワーク構成変更やサーバー停止は不要

担当者様の作業は DNS の切り替えだけ。簡単に導入が可能です。

2. DDoS 対策機能 (DDoS セキュリティタイプ)

WAF では防御できない DoS / DDoS 攻撃を、お客様ネットワークより上位のネットワーク側で検知、軽減します。



SaaS / クラウドの形で提供するタイプ。お客様のシステムに変更を加えることなく、DNS を切り替えるだけで簡単に導入可能です。WAF センターを経由して、正規のアクセスはそのまま通し、不正なアクセスは WAF センターで遮断します。

DDoS セキュリティタイプで、より安全なサーバー環境に！

WAF では防御できない DoS / DDoS 攻撃を、お客様ネットワークより上位のネットワーク側で検知、軽減することにより、サーバーやネットワーク機器、インターネット回線までを含めた防御が可能です。

お客様ネットワークに最適化したポリシー

サービス開始前に防御対象ネットワークのトラフィックを学習、分析します。その結果から防御ポリシーを設定することで、精度の高いクリーニングを実現します。

不正なトラフィックを選択的に遮断

トラフィックのモニタリングを実施し、異常を検知した場合はお客様サーバーやネットワーク宛のすべての通信をアンチ DDoS システムへ引き込みます。そこで通信の精査と不正なトラフィックのクリーニングを実施し、正常な通信だけをお客様サーバーやネットワークへ転送します。

◆ 防御できる DoS / DDoS 攻撃の代表例

- TCP
(Syn flood, Ack flood, Fins flood, Fragments)
- HTTP GET / POST Flood
- HTTP Slow Attack Protection
- ICMP (Unreachable, Echo, Fragments)
- Connection Exhaustion
- Ping of Death
- TCP 不正フラグ

※ セキュリティ上、一部のみ公開しています。