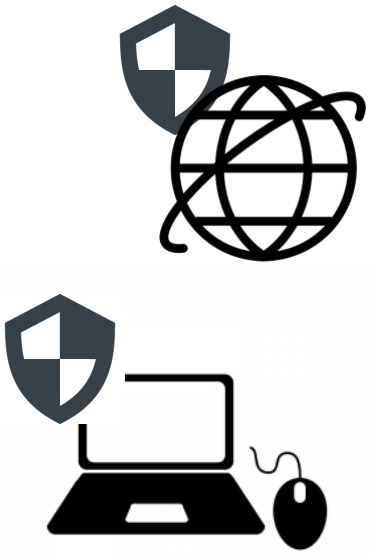
クラウド型 Web Application Firewall
「攻撃遮断くん」ご提案
サービス概要 ver6.1

2019年4月
株式会社サイバーセキュリティクラウド

サイバーセキュリティとは？



サイバーセキュリティは大きく分けて２つ
対策すべきは、手薄な「Webセキュリティ」

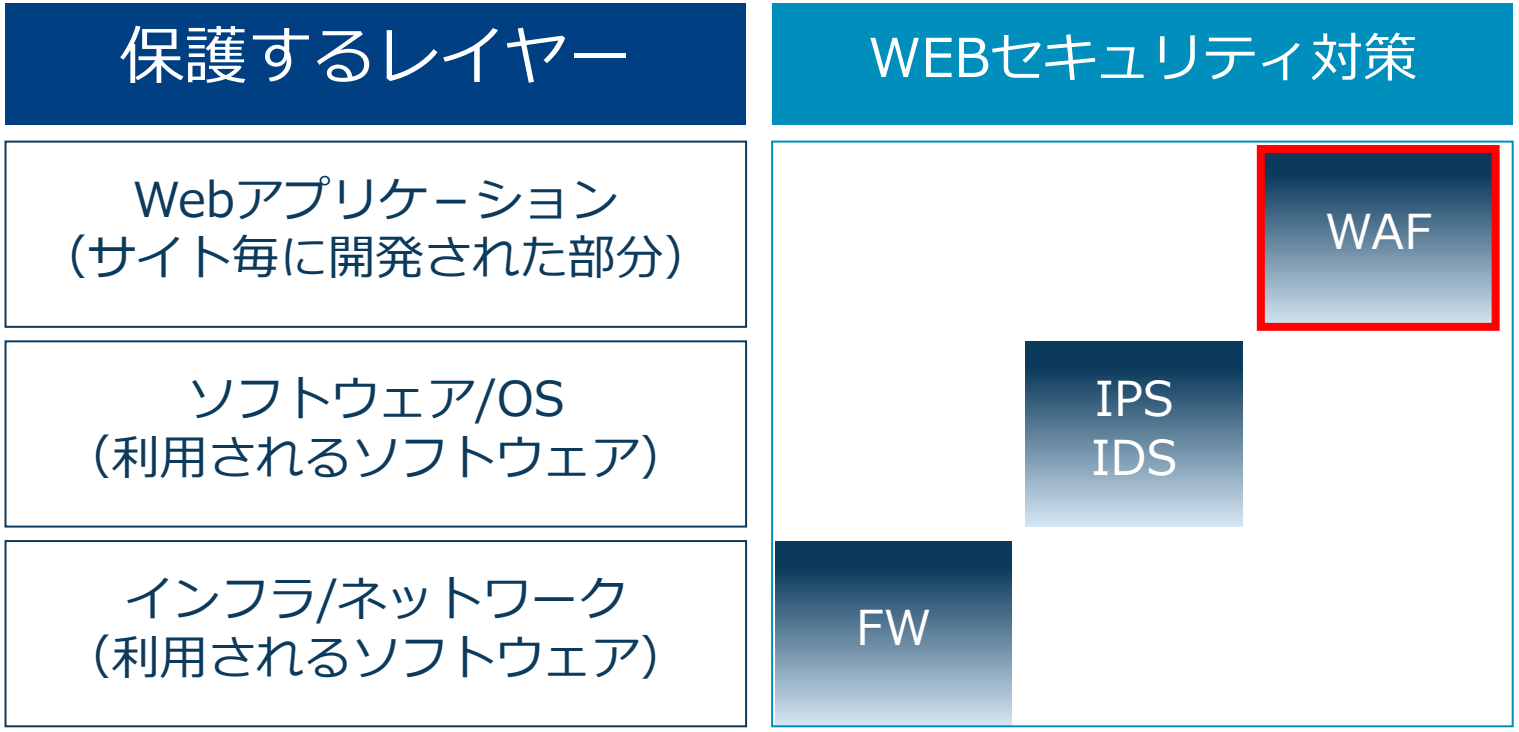
　サイバーセキュリティは大きく２つに分けることができます。ひとつはマルウェアに対してPCや社内ネットワークを守るための**社内セキュリティ。**
もうひとつはソフトウェアの脆弱性やWebアプリケーション層への攻撃から外部公開サーバー守る
Webセキュリティです。

　過去に発生したセキュリティインシデントを紐解いてみると、セキュリティ被害の多くはWeb経由であり、依然として増加傾向にあります。

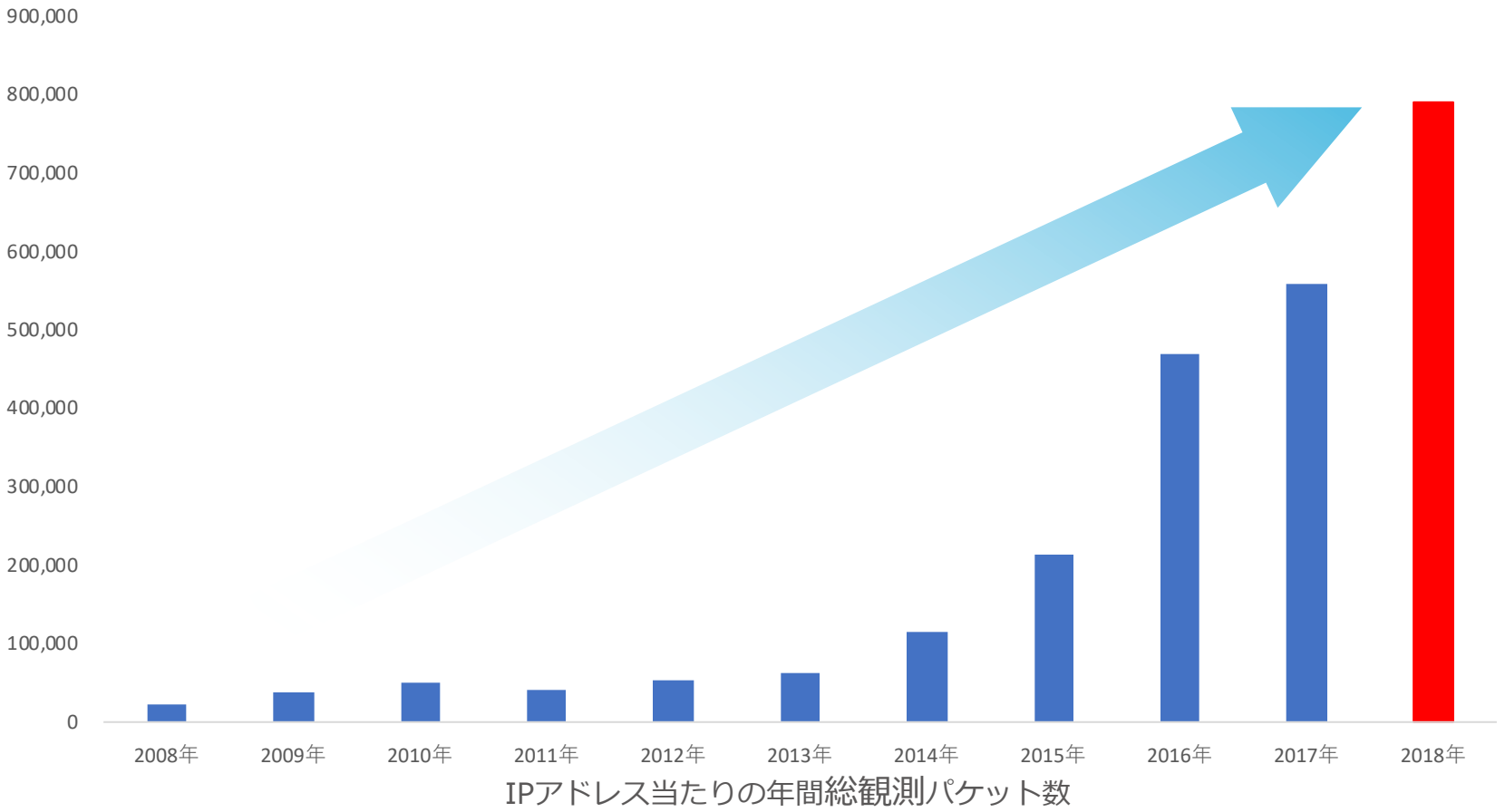
※出典：情報処理推進機構（IPA）「情報セキュリティ10大脅威 2018」

WAFとは？

WAF(Webアプリケーションファイアウォール)とは、
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不正な攻撃から
Webアプリケーションを防御するファイアウォールの事です。



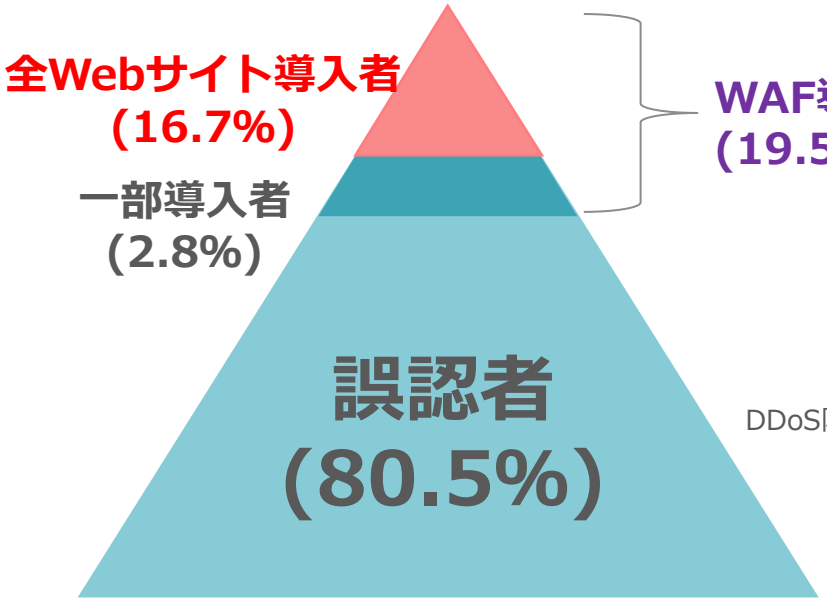
サイバー攻撃の推移

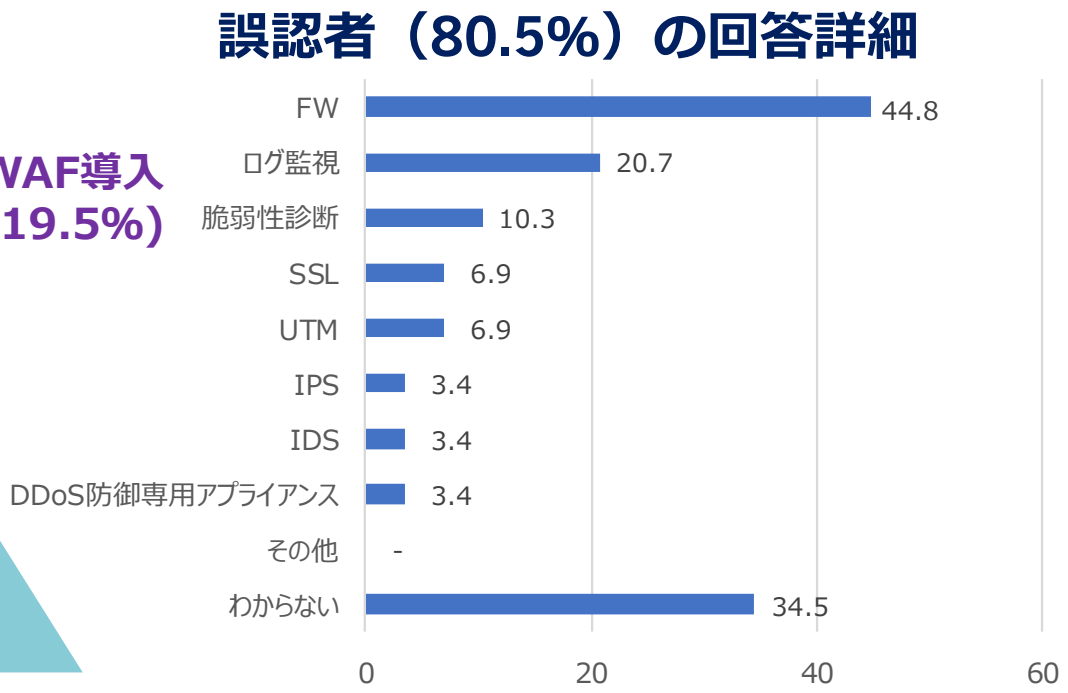


サイバー攻撃は10年間で約35倍に急増

※出典：NICTER観測レポート2017,2018

WEBセキュリティに対しての誤認





経営層の約8割が
「Webサイトのセキュリティは対策済」と誤認。

※出典：株式会社マーケティングアンドアソシエイツ「セキュリティソフト浸透度調査」

市場背景

個人情報漏洩事故の増加

個人情報を保有するWEBが外部からの攻撃を受け，漏洩事故を起こした事例も増えています。
サイバー攻撃による被害は、サービス停止、売上機会の損失、ブランドイメージの棄損に留まらず、予期せぬ二次災害を起こす可能性もあります。

サイバーセキュリティ対策は経営責任に

Webセキュリティ被害の増加にともない、2015年には経済産業省とIPAが『サイバーセキュリティ経営ガイドライン』を策定し、経営者に対してセキュリティ対策を推進するよう求めました。また、2017年11月の改訂では、概要部分に「経営責任や法的責任が問われる可能性がある」といった強い文言が記載されており、経営者へ警鐘を鳴らしています。

- **セキュリティ事故は経営者の経営責任・法的責任**
- **サイバー攻撃を監視・検知する仕組みの構築**
- **ビジネスパートナーや委託先等を含めた、サプライチェーン全体の対策及び状況把握**

攻撃遮断くんとは

「攻撃遮断くん」は、クラウド型のWAF（Web Application Firewall）製品です。

WebサイトやWebサーバへの攻撃を遮断し、情報漏えい、Web改ざん、サーバダウンを狙った攻撃などの脅威から、企業とユーザーを守ります。

クラウド型の為、保守・運用に手間を掛ける事なく、24時間365日の高セキュリティを実現します。

1 **あらゆるWebシステムに導入可能**

2 **サイト数無制限の定額制プランを提供**

3 **自社開発だからできる万全なサポート体制**

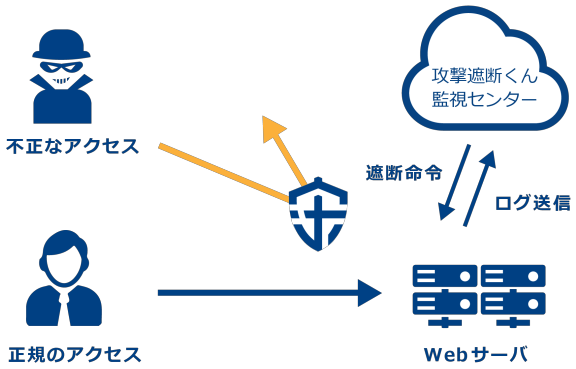
サービスラインナップ

攻撃遮断くんはお客様の環境に応じて、最適なタイプをご用意しています。

エージェント連動型

サーバセキュリティタイプ

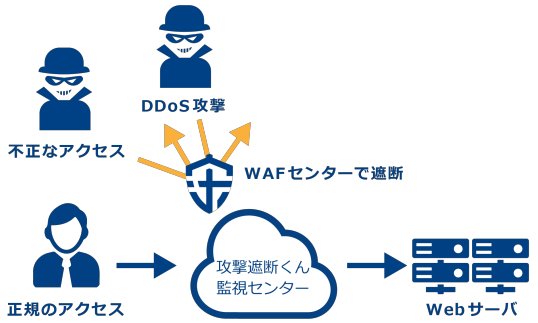
■クラウド（IaaS）含め多様なサーバに対応
■専任のセキュリティエンジニアが不要
■導入時サーバ停止の必要なし
■自動シグネチャ更新
■最新の攻撃に対応



DNS切り替え型

DDoSセキュリティタイプ

■DNSの切り替えのみ
■専任のセキュリティエンジニアが不要
■導入時サーバ停止の必要なし
■自動シグネチャ更新
■Webサイトへのリソース負荷がかからない
■最新の攻撃に対応
■DDoS攻撃にも対応



攻撃遮断くんの選定ポイント

	サーバセキュリティタイプ		DDoSセキュリティタイプ	
プラン名	ベーシックプラン	使い放題プラン	1サイトプラン	入れ放題プラン
プラン選定例	トラフィック量の多いWebサイト 目安：1~20台	トラフィック量が多く、Webサイトが多い 目安：20台以上	トラフィック量の少ないWebサイト	Webサイトが多い
特長	Webサービスを無停止で導入可能。導入後もサービス稼働の影響を最小限で提供。		DNSを切り替えるだけで簡単に導入可能。入れ放題プランは、環境の異なるWebサイト全体（レンタルサーバを利用したWebサイト）も包括し導入可能。	

自社で開発・運用・サポートまで全て一貫して対応

開発・運用・サポートまで、自社で一貫して提供。

お客様の声を、直接開発に反映できる環境があるため、カスタマイズ等の様々なご要望をスムーズに連携しています。

稼働率99.999%※1、解約率約1.1%※2を実現しています。

※1：2019年1月～2019年3月の月間稼働率 = (月間総稼働時間−月間サービス停止時間) ÷ 月間総稼働時間 × 100
※2：2017年1月～2018年12月の月次平均解約率

サポート体制

・24時間365日サポート（電話、メール、管理画面）
・日本人スタッフによる丁寧な対応
・管理画面も全て日本語対応

Q&A対応

・仕様確認
・契約内容確認
・定型的な作業依頼
（証明書更新、FQDN追加等）
・その他Q&A

テクニカルサポート

・導入時の技術サポート
・検知ログに関する質問
・シグネチャカスタマイズ
・その他WAF機能に関する
技術的な質問

緊急時サポート

・お客様Webサービス停止時
・止めてはいけない通信が
何度も止まっている時
・その他緊急を要するサポート

シグネチャの更新について

情報収集

各種情報の収集

公的機関・ベンダー・最新攻撃手法等を収集し、最新の攻撃への対応を目的に活用しております。

スレットインテリジェンスの活用

最新の攻撃兆候・動向を把握を目的に活用しております。

当社運用情報の活用

5,000サイト以上の運用実績から、検出精度の向上を目的に活用しております。

更新

日々収集する情報をもとにシグネチャを更新しています。

定期更新

随時定期的なアップデートを実施いたします。

緊急更新

緊急度の高い脆弱性が公表された場合に実施いたします。

緊急対応の事例

2019年2月21日

Drupal の脆弱性(CVE-2019-6340(SA-CORE-2019-003)) 注意喚起及び、攻撃遮断くんでの対応状況について

2018年8月23日

Apache Struts2 の脆弱性(CVE-2018-11776(S02-057)) 注意喚起及び、攻撃遮断くんでの検知設定完了について

2018年8月23日

Apache Struts2 の脆弱性公開(S02-057/CVE-2018-11776)を確認いたしました。

2018年4月26日

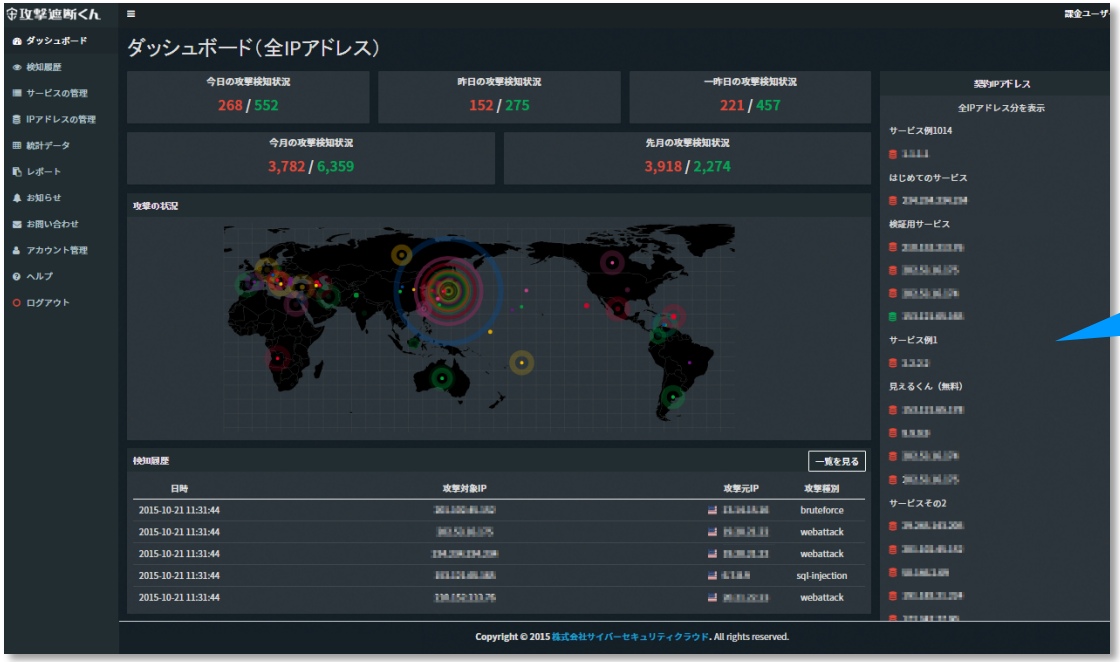
Drupal の脆弱性(SA-CORE-2018-004)を利用した攻撃を、検知できることを確認しました。

2018年4月26日

Drupal の脆弱性公開(SA-CORE-2018-004)を確認いたしました。

管理画面（検知履歴表示）

- 企業アカウントごとに管理画面をご提供
- 1万件の検知履歴をCSVで出力可能
- 全て日本語で対応
- グラフィカルなマップとデータで攻撃状況を可視化



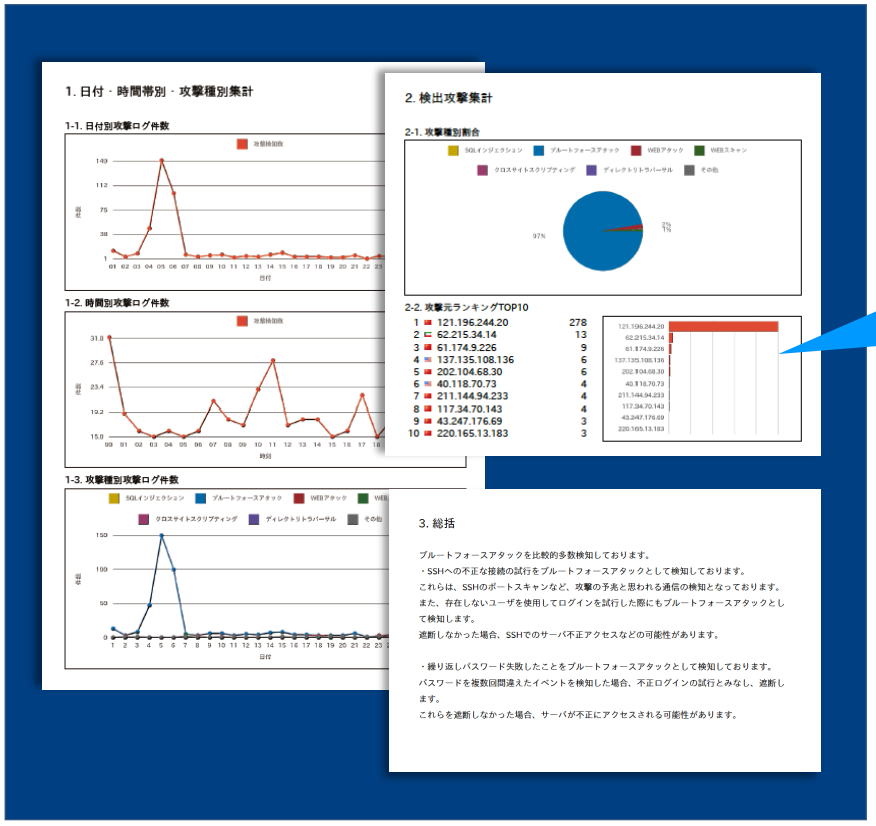
※DDoS攻撃の検知状況は表示されません

攻撃に関する表示内容

- **リアルタイム攻撃情報**
- **攻撃種別**
- **攻撃元IP**
- **攻撃元国の確認**
- **期間毎の攻撃グラフ**

月次レポート

月間の攻撃データに加えてセキュリティエンジニアによる総括などを記載したレポートを毎月ご提供します。攻撃状況を一目で把握でき、共有の簡易化、資料作成の手間を省きます。※一部プランは別途オプションになります。



- 日付別攻撃ログ件数
- 時間別攻撃ログ件数
- 攻撃種別攻撃ログ件数
- 攻撃種別割合
- 攻撃元ランキングTOP10
- 総括
  セキュリティエンジニアによる総括コメントで、自社の攻撃概要を把握可能

月次レポートのご提供内容

	サーバーセキュリティタイプ	DDoSセキュリティタイプ
ベーシックプラン 1サイトプラン	○	－（※1）
使い放題プラン 入れ放題プラン	○	○（※2）

※1：ご要望の場合は別途有償オプション（税抜2万円/月）対応となります
※2：FQDN単位での月次レポートは別途有償オプション対応となります

WAFの攻撃状況に関してのレポートになります。
DDoSセキュリティタイプにおける「DDoS攻撃」のレポートには別途有償オプション（税抜2万円/月）対応となります。

サイバー保険付帯について

「攻撃遮断くん」をご利用中のサービスが、10Gbps以上のDDoS攻撃やゼロデイ攻撃により
損害を受けてしまった場合、費用を最大1,000万円まで補償するサイバー保険を付帯が可能です。

損害賠償	合わせて1,000万円の補償
事故対応特別費用	
喪失利益・営業継続費用	対象外

※WEBセキュリティタイプ・DDoSセキュリティタイプ 1サイト/~500kbpsプランをご契約のお客様は対象外となります。
※※保険付帯には情報提供等の条件があります。

本サイバー保険は、損害保険ジャパン日本興亜株式会社、株式会社フィナンシャル・エージェンシー（以下、FA社)の協力のもと提供しております。

保険契約者　　：株式会社サイバーセキュリティクラウド
被保険者　　：「攻撃遮断くん」ご利用企業様
引受保険会社　　：損害保険ジャパン日本興亜株式会社
取扱代理店　　：株式会社フィナンシャル・エージェンシー

サイバー保険の補償内容

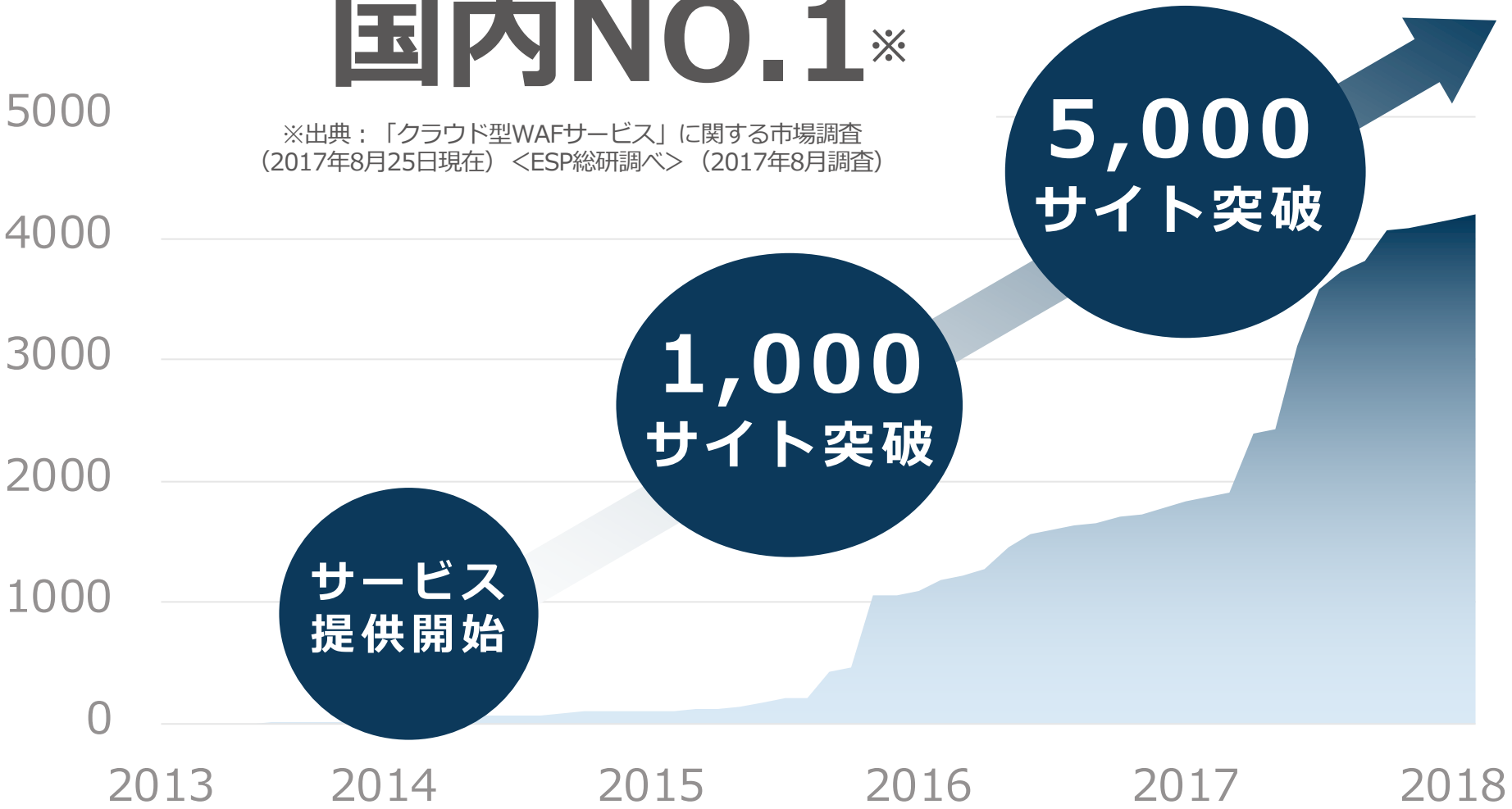
損害賠償
■ 情報漏えいまたはその恐れ ■ ネットワークの所有、使用もしくは管理または情報メディアの提供にあたり生じた偶然な事由

調査・応急対応	復旧	緊急時広報
■ 事故判定 ■ 原因究明・影響範囲調査支援 ■ 被害拡大防止アドバイス など	■ 情報機器修理費用 ■ データ復旧費用	■ 記者会見実施支援 ■ 報道発表資料のチェックや助言 ■ SNS炎上対応支援（公式アカウント対応サポート） ■ WEBモニタリング・緊急通知

コールセンター	信頼回復	コーディネーション
■ コールセンター立ち上げ ■ コールセンター運用 ■ コールセンターのクロージング支援など	■ 再発防止策の実施状況について証明書を発行 ■ 格付機関として結果公表を支援	■ 必要となる各種サポート機能の調整 ■ 法令対応等について協力弁護士事務所を紹介など

導入社数/導入サイト数
国内NO.1※

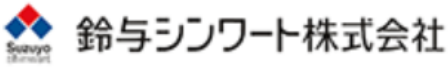
※出典：「クラウド型WAFサービス」に関する市場調査
（2017年8月25日現在）<ESP総研調べ>（2017年8月調査）



攻撃遮断くん導入実績

国内トップクラス 5,000サイト以上の導入実績！
中小から大手まで、あらゆる規模のWebサービスで
「攻撃遮断くん」をご利用いただいています。

パートナー企業一覧 ※一部抜粋



弊社パートナー詳細：https://www.shadan-kun.com/partners/

攻撃遮断くん　簡易料金表

■サーバセキュリティタイプ（エージェント連動型）

プラン名	初期費用（税抜）	月額費用（税抜）
ベーシックプラン（1IP）	200,000円	40,000円
使い放題プラン（サーバ台数無制限）	2,000,000円	800,000円

■DDoSセキュリティタイプ（DNS切り替え型）

プラン名	ピーク時トラフィックの目安	初期費用（税抜）	月額費用（税抜）
1サイトプラン（1FQDN）	～5Mbps	200,000円	60,000円
入れ放題プラン	～100Mbps	380,000円	220,000円
	～200Mbps		380,000円
	～300Mbps	月額料金と同額	480,000円
	～400Mbps		580,000円
	～500Mbps		620,000円
	～1Gbps		720,000円

本資料に記載されている価格は全て税抜です。
詳細なプラン料金は別途営業宛にお問合せください。

お問い合わせ

電話：03-6416-1579（平日10:00～18:00）

メール：sales@cscloud.co.jp

Web：https://shadan-kun.com/

会社名	株式会社サイバーセキュリティクラウド
本社所在地	〒150-0011 東京都渋谷区東3-9-19　VORT恵比寿maxim3階
代表電話	03-6416-9996
FAX番号	03-6416-9997
Webサイト	http://www.cscloud.co.jp
代表取締役	大野 暉
事業内容	Webセキュリティ事業 ・Webセキュリティサービスの開発・運用・保守・販売 ・サイバー攻撃対策コンサルティング