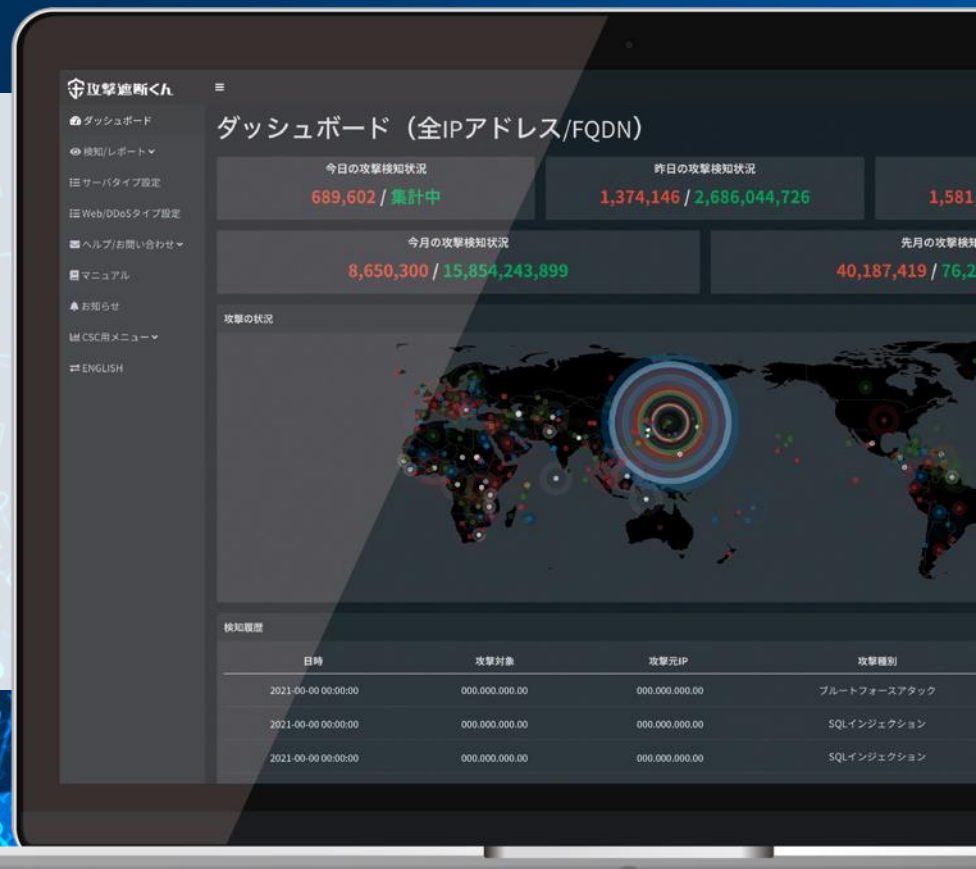


クラウド型 WAF (Web Application Firewall)

守 攻撃遮断くん

サービス紹介資料

ver. 9.4



株式会社サイバーセキュリティクラウド

本資料に記載された情報は株式会社サイバーセキュリティクラウド（以下CSC）が信頼できると判断した情報源を元にCSCが作成したものです。その内容および情報の正確性、完全性等について、何ら保証を行っておらず、また、いかなる責任を持つものではありません。本資料に記載された内容は、資料作成時点において作成されたものであり、予告なく変更する場合があります。本資料はお客様限りで配布するものであり、CSCの許可なく、本資料をお客様以外の第三者に提示し、閲覧させ、また、複製、配布、譲渡することは強く禁じられています。本文およびデータ等の著作権を含む知的所有権はCSCに帰属し、事前にCSCの書面による承諾を得ることなく、本資料に修正・加工することは強く禁じられています。

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**。

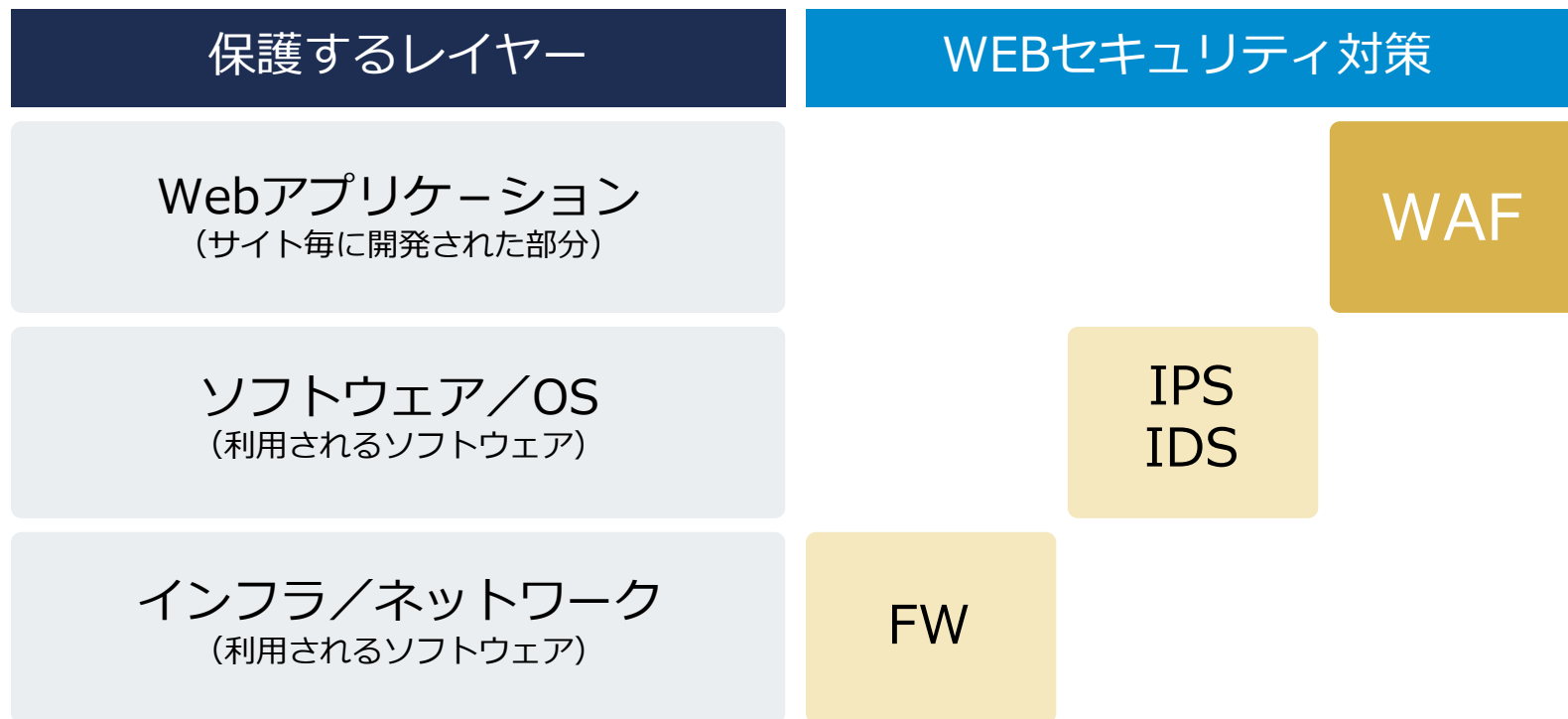
もうひとつはソフトウェアの脆弱性やWebアプリケーション層への攻撃から
外部公開サーバを守る**Webセキュリティ**です。

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？

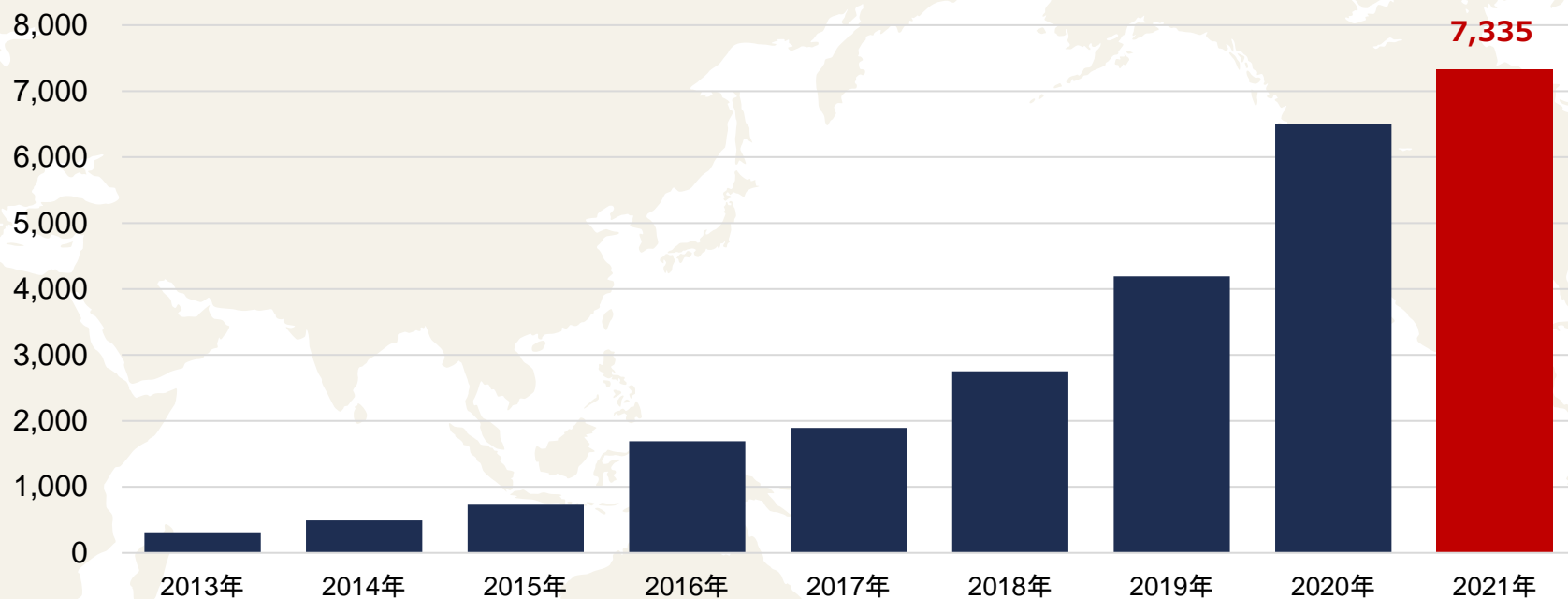
WAF（Webアプリケーションファイアウォール）とは、従来のFW（ファイアウォール）やIDS／IPSでは防ぐ事ができない不正な攻撃からWebアプリケーションを防御するファイアウォールの事です。



サイバー攻撃の推移

警察庁が観測しているサイバー攻撃の兆候

(件/日・IPアドレス)



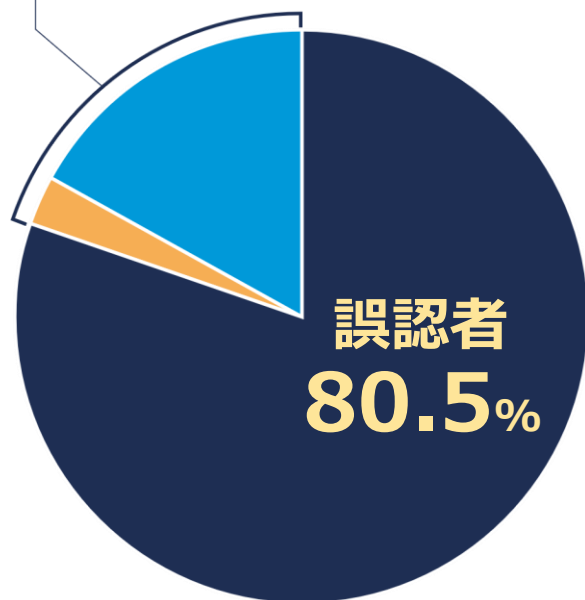
過去9年間で約24倍に急増

※出典：警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」、警察庁「平成29年中におけるサイバー空間をめぐる脅威の情勢等について」の「サイバー空間における脆弱性探索行為などの観測状況」より作成

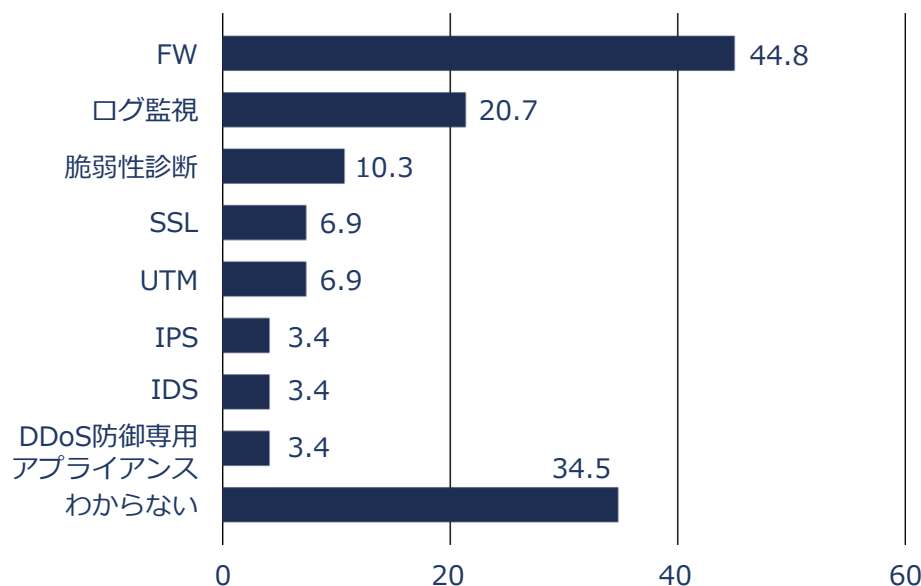
Webセキュリティに対しての誤認

WAF導入 **19.5%**

- 全Webサイト導入者 (16.7%)
- 一部導入者 (2.8%)



誤認者 (80.5%) の回答詳細



※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」。

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。

市場背景

個人情報漏洩事故の増加

個人情報保有する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

「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

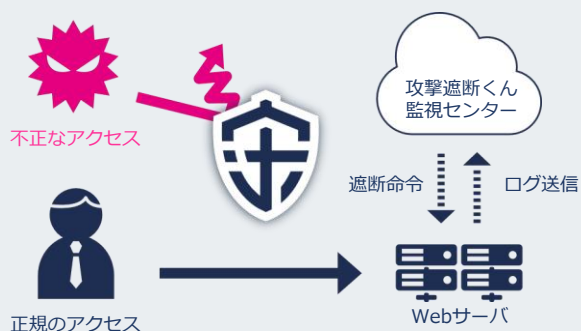
③ 自社開発だからできる**万全なサポート体制**

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

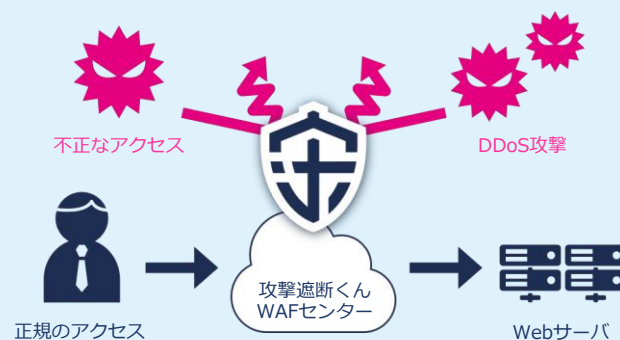
サーバセキュリティタイプ



- クラウド（IaaS）含め多様なサーバに対応
- 障害ポイントの切り分けが容易

DNS切り替え型

WEB/DDoSセキュリティタイプ



- DNSの切り替えのみ
- Webサイトへのリソース負荷がかからない
- DDoS攻撃にも対応

共通

- 専任のセキュリティエンジニアが不要
- 最新の攻撃に対応
- 自動シグネチャ更新

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		WEB/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	Webサイト 入れ放題プラン
プラン 選定例	トラフィック量の多いWebサーバ 【目安】1~20台	トラフィック量が多く、Webサーバが多い 【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 **0.97%**^{※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：MRRチャーンレートの2022年1月～2022年12月の平均値。MRRチャーンレートとは、当月失ったMRRを先月末時点のMRRで除すことで計算される解約率。

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
- 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・動向の把握を目的にグローバル機関から収集し活用しています。

当社運用情報の活用

20,000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。

過去実績

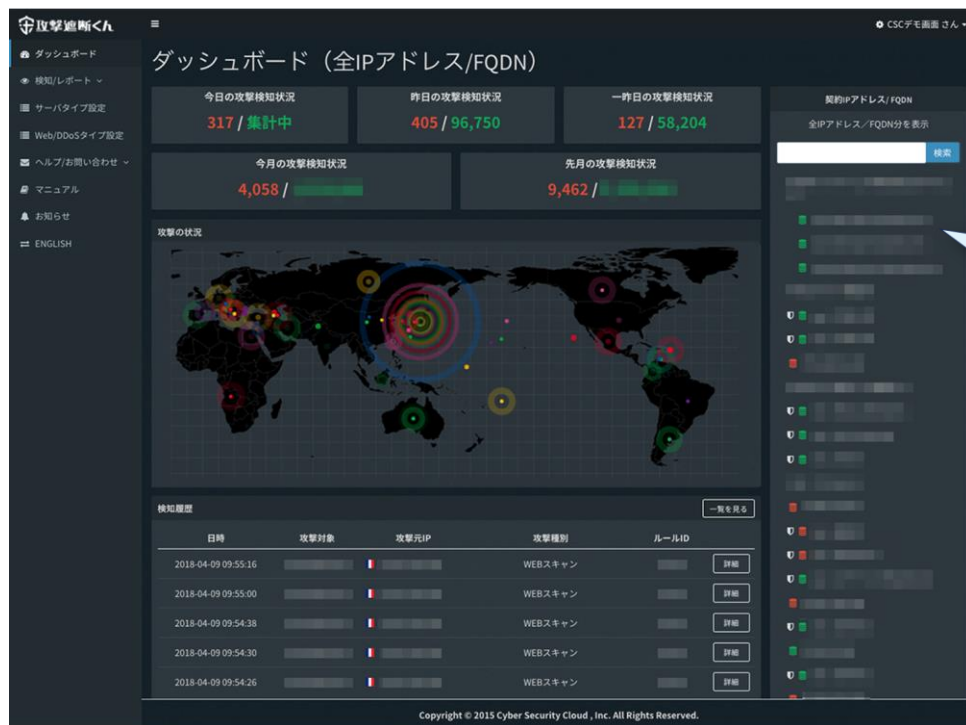
- 2021年12月10日
Apache Log4jの脆弱性
(CVE-2021-44228)
- 2019年2月21日
Drupalの脆弱性
(CVE-2019-6340 (SA-CORE-2019-003))



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

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

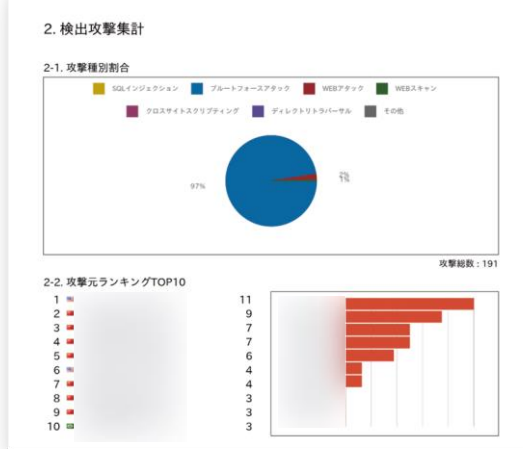
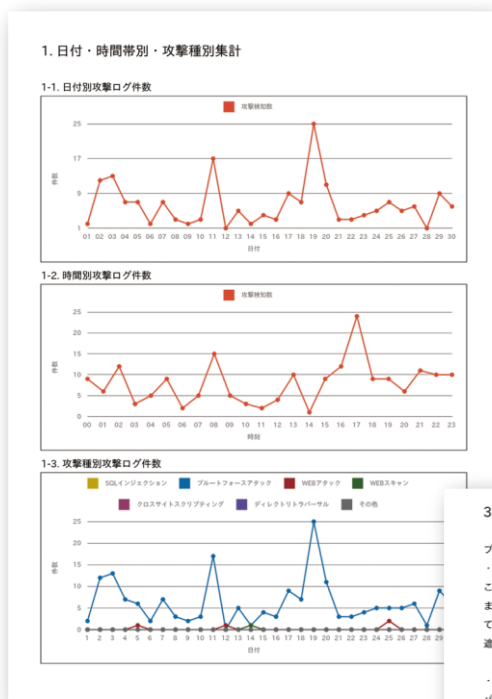
期間毎の攻撃グラフ

※DDoS攻撃の検知状況は表示されません。

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。



3. 総括

ブルートフォースアタックを比較的多数検知しております。
 ・SSHへの不正な接続の試行をブルートフォースアタックとして検知しております。
 これらは、SSHのポートスキャンなど、攻撃の予兆と思われる通信の検知となっております。
 また、存在しないユーザを使用してログインを試行した際にもブルートフォースアタックとして検知します。
 遮断しなかった場合、SSHでのサーバ不正アクセスなどの可能性があります。

・繰り返しパスワード失敗したことをブルートフォースアタックとして検知しております。
 パスワードを複数回間違えたイベントを検知した場合、不正ログインの試行とみなし、遮断します。
 これらを遮断しなかった場合、サーバが不正にアクセスされる可能性があります。

- 日付別攻撃ログ件数
- 時間帯別攻撃ログ件数
- 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

レポートの ご提供	サーバセキュリティタイプ		WEB/DDoSセキュリティタイプ	
	ベーシック プラン	使い放題プラン	1サイトプラン	Webサイト 入れ放題プラン
	○	○	× ※1	○ ※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の攻撃状況に関するレポートになります。

GeoIP制限機能 / IP制限機能

GeoIP制限機能

概要

国別の拒否/許可設定が可能です。

設定例

- ① 日本からのアクセスのみ許可したい場合
- ② 中国/米国からのアクセスを拒否したいが、Googleのbotからのアクセスは許可したい場合

IP制限機能

概要

IPアドレス別に拒否/許可設定が可能です。

設定例

- ① 複数のIPアドレスからの不正なアクセスが多い。これらをブラックリストとして登録したい場合
- ② example.comは、企業A/企業B様向けのEラーニングWEBサービス。そのため、企業Aと企業B様のIPアドレスのみ許可した上で、WAF機能を利用したい場合

対応プラン

(2022年6月時点)

- Webセキュリティタイプ : Webサイト入れ放題プラン
- DDoSセキュリティタイプ : Webサイト入れ放題プラン

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
- 引受保険会社 : 損害保険ジャパン株式会社
- 被保険者 : 「攻撃遮断くん」ご利用企業様
- 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

- 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

復旧

- 情報機器修理費用
- データ復旧費用

緊急時広報

- 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

- 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

信頼回復

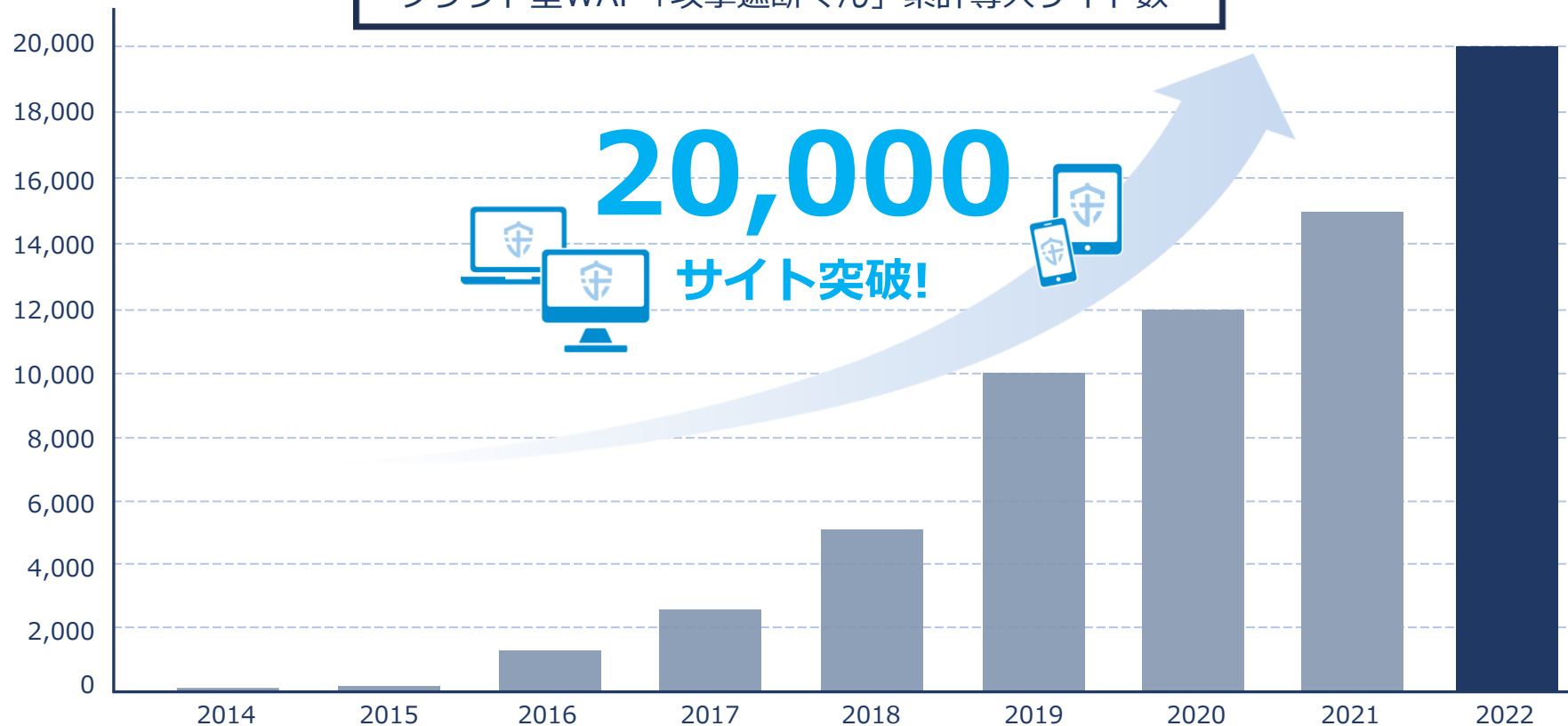
- 再発防止策の実施状況について
証明書を発行
- 格付機関として結果公表を支援

コーディネーション

- 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

導入サイト推移

クラウド型WAF「攻撃遮断くん」累計導入サイト数



導入社数／導入サイト数国内NO.1[※]

※ 出典：日本マーケティングリサーチ機構調べ 調査概要：2021年10月期_指定テーマ領域における競合調査

攻撃遮断くん導入実績

国内トップクラス20,000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。

金融・保険

SBI証券

あなたのまちの
筑邦銀行

全国信用金庫厚生年金基金

SOMPOリスクマネジメント

SOLXYZ
株式会社ソルクシーズ

エース証券

インターネット

PERSOL
パーソル プロセス&テクノロジー

FANCOM!

Inter Factory

UNITED

せんたく便
Cleaning & Laundry

A Solutions

交通

ANA

建設

子どもたちに誇れるしごとを。
SHIMIZU CORPORATION
清水建設

小売

PARCO

多慶屋

メーカー

Pioneer

キョクヨー

Vitabrid C¹²

その他

代々木ゼミナール

AEON PET

SB Human Capital

PASONA
JOBHUB

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①

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	IP数	初期費用（税抜）	月額費用（税抜）
ベーシックプラン	1～3 IP	200,000円	40,000円/IP
	4 IP以上	200,000円	1～3IP 40,000円/IP 4IP以降 10,000円/IP
使い放題プラン サーバ台数無制限 (最低利用期間6ヶ月)	-	2,000,000円	800,000円

下記のいずれかに該当する場合は、別途お問い合わせください。

■ベーシックプラン

- IP数が20IP以上の場合
- 中間機器に導入する場合
- リクエスト数が秒間200リクエストを超過する場合

■使い放題プラン

- リクエスト数が秒間4,000リクエストを超過する場合

攻撃遮断くん 簡易料金表②

WEB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)	～500kbps	200,000円/サイト※	10,000円
	～2Mbps		30,000円
	～5Mbps		50,000円
	～10Mbps		100,000円
Webサイト 入れ放題プラン (最低利用期間6ヶ月)	～100Mbps	340,000円	180,000円
	～200Mbps	月額料金と同額	340,000円
	～300Mbps		450,000円
	～400Mbps		550,000円
	～500Mbps		600,000円
	～1Gbps		700,000円

※ 1サイトプランは、サイト数ごとに初期費用がかかります。

※ GeoIP制限機能／IP制限機能はWebサイト入れ放題プランのみ対応しています。(2022年6月時点)

攻撃遮断くん 簡易料金表③

DDoSセキュリティタイプ (DNS切り替え型・DDoS攻撃対策機能付きWAF)

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)	～500kbps	200,000円/サイト※	15,000円
	～2Mbps		40,000円
	～5Mbps		60,000円
	～10Mbps		120,000円
Webサイト 入れ放題プラン (最低利用期間6ヶ月)	～100Mbps	450,000円	250,000円
	～200Mbps	月額料金と同額	450,000円
	～300Mbps		600,000円
	～400Mbps		700,000円
	～500Mbps		800,000円
	～1Gbps		1,000,000円

※ 1サイトプランは、サイト数ごとに初期費用がかかります。

※ GeoIP制限機能／IP制限機能はWebサイト入れ放題プランのみ対応しています。(2022年6月時点)

サイバーセキュリティクラウドの提供サービス

自社で開発したSaaS型セキュリティサービスを全世界に提供しています。

クラウド型WAF

パブリッククラウド WAF
自動運用サービス

aws marketplace

脆弱性情報
収集・管理ツール

AWS WAF / Azure WAF / Google Cloud Armor



Waf Charm

AWS WAF
Managed Rules

SIDfm



国内シェア

No.1^{※1}

AWS WAF 自動運用サービス
導入ユーザ数

国内
No.1^{※2}

導入ユーザ数

90カ国以上
3,000^{※3}
ユーザー以上

脆弱性情報配信サービスシェア
脆弱性情報提供実績
脆弱性オリジナルコンテンツ数
3部門国内

No.1^{※4}

※1 日本マーケティングリサーチ機構調べ 調査概要：2021年10月期_実績調査
※2 日本マーケティングリサーチ機構調べ 調査概要：2020年7月期_実績調査

※3 2022年10月時点
※4 日本マーケティングリサーチ機構調べ 調査概要：2021年8月期_実績調査

お問い合わせ

☎ **03-6416-1579** (平日10:00~18:00)

✉ **mkt@cscloud.co.jp**

💻 **<https://shadan-kun.com/>**



COMPANY

会社名	株式会社サイバーセキュリティクラウド	
代表電話	03-6416-9996	
FAX番号	03-6416-9997	
Webサイト	https://www.cscloud.co.jp	
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



世界中の人々が安心安全に使える
サイバー空間を創造する