CSC
CYBER SECURITY CLOUD

サイバー攻撃の脅威と
WEBセキュリティの必要性について

2019年1月　株式会社サイバーセキュリティクラウド

2.

近年、WEBサイトへのサイバー攻撃で起こった事故

WEBサイトへのサイバー攻撃による個人情報漏洩は影響も大きく、時には、
記者会見等の対応に発展し株価に影響する場合があり、「会社の信頼損失」に繋がります。

化粧品会社S（2016年12月2日）

・化粧品会社Sの某サイトにて、
外部からの不正アクセスにより顧客情報が流出。

・クレジットカード情報：**5万6,121件**、
個人情報（氏名、電話等）：**42万1,313件**が流出。

・株価は一時、前日比**25.5円下落（0.9％）**し、
親会社の化粧品会社Sが謝罪会見を行った。

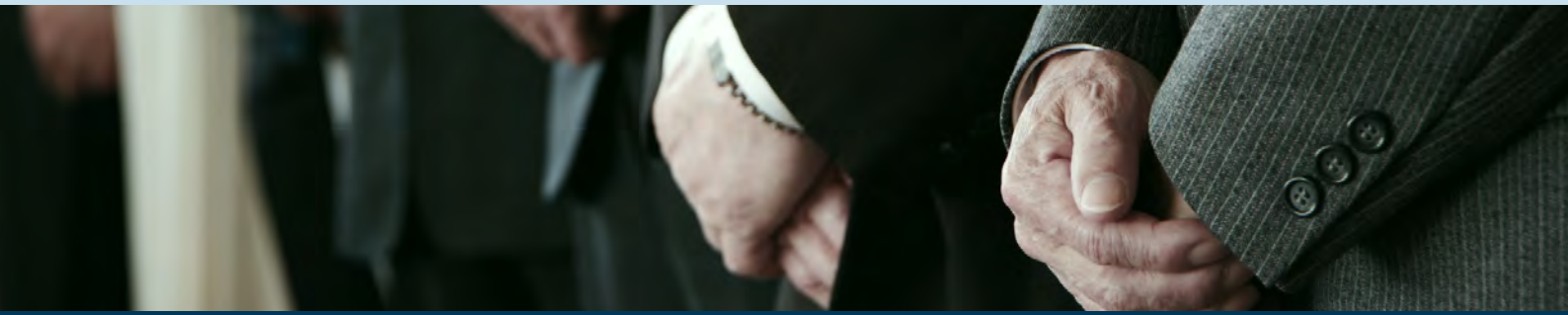
大手通信販売会社S（2016年4月15日）

・大手通信販売会社S子会社にて、
外部からの不正アクセスにより顧客情報が流出。

・クレジットカード情報：**1万3,713件**、
個人情報（氏名、電話等）：**13万1,096件**が流出。

・株価は発覚後、3日続落。一時前日比**13円下落**
（1.8％）し、ホームページ等での謝罪を行った。

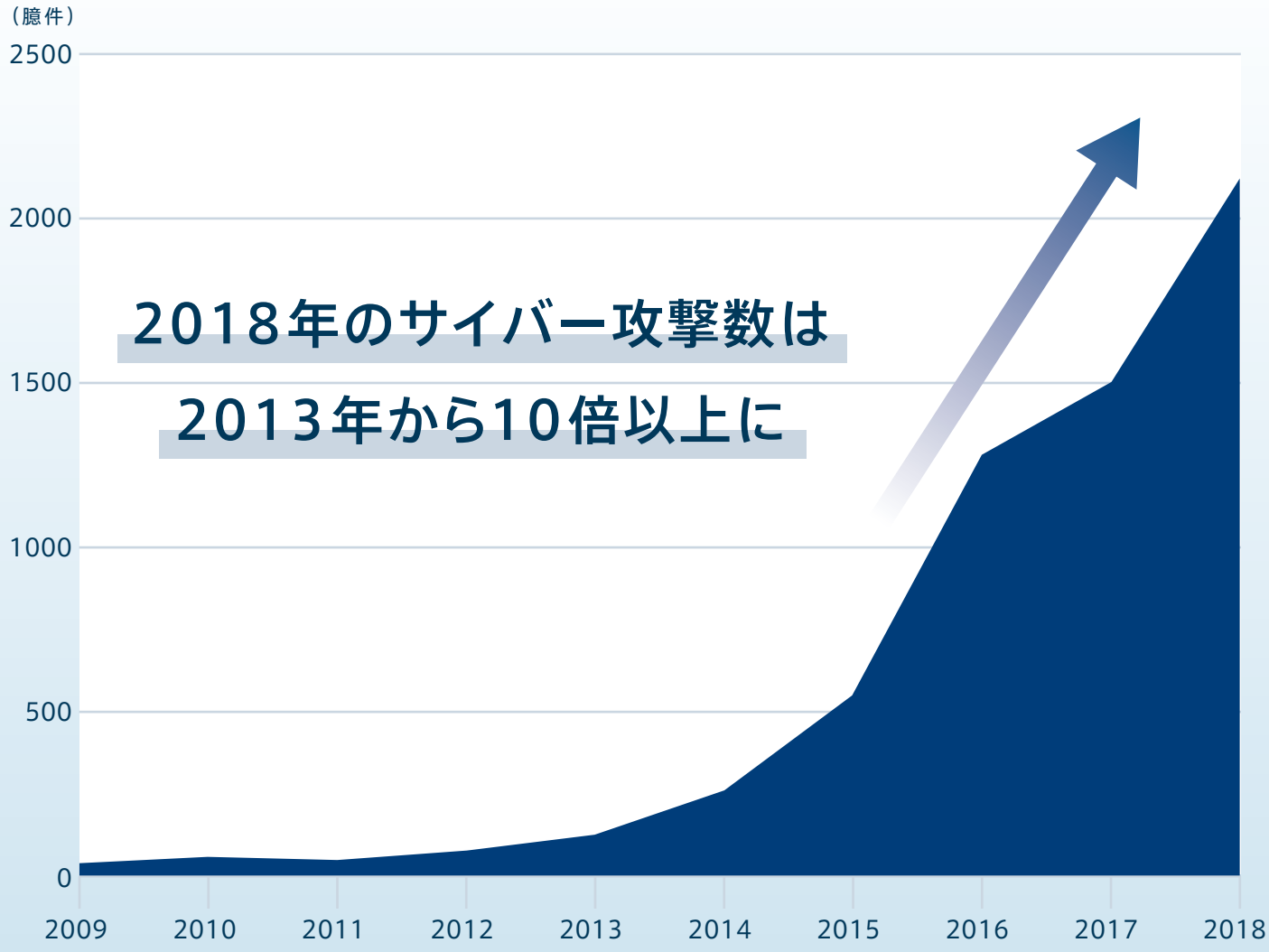
その他の主な被害事例／衣料品メーカーW・観光業H・出版社Kなど



1.

日本国内に向けたサイバー攻撃の推移

サイバー攻撃数は年々増加傾向であり、企業のセキュリティ対策が肝となってきています。



※出典：国立研究開発法人情報通信研究機構（NICT）「NICTER 観測レポート 2018（2019年2月6日公開）」

3.

2019年サイバーセキュリティ10大脅威

10大脅威の内、**3件**がWebに関する脅威となっています。

順 位	内 容
1 位	標的型攻撃による被害
2 位	ビジネスメール詐欺による被害
3 位	ランサムウェアによる被害
4 位	サプライチェーンの弱点を悪用した攻撃の高まり
5 位	内部不正による情報漏えい
6 位	**サービス妨害攻撃によるサービスの停止**
7 位	**インターネットサービスからの個人情報の窃取**
8 位	IoT機器の脆弱性の顕在化
9 位	**脆弱性対策情報の公開に伴う悪用増加**
10 位	不注意による情報漏えい

※出典：情報セキュリティ10大脅威 2019（IPA 独立行政法人情報処理推進機構）

4.

セキュリティ対策の種類と違い

セキュリティ対策に万能はありません。WEBサイトでの事故の原因となる「SQLインジェクション、クロスサイトスクリプティング」等のサイバー攻撃は、一般的に講じられているSSLやファイアウォールだけでは防ぐことはできない為、WAFでの対策が有効です。

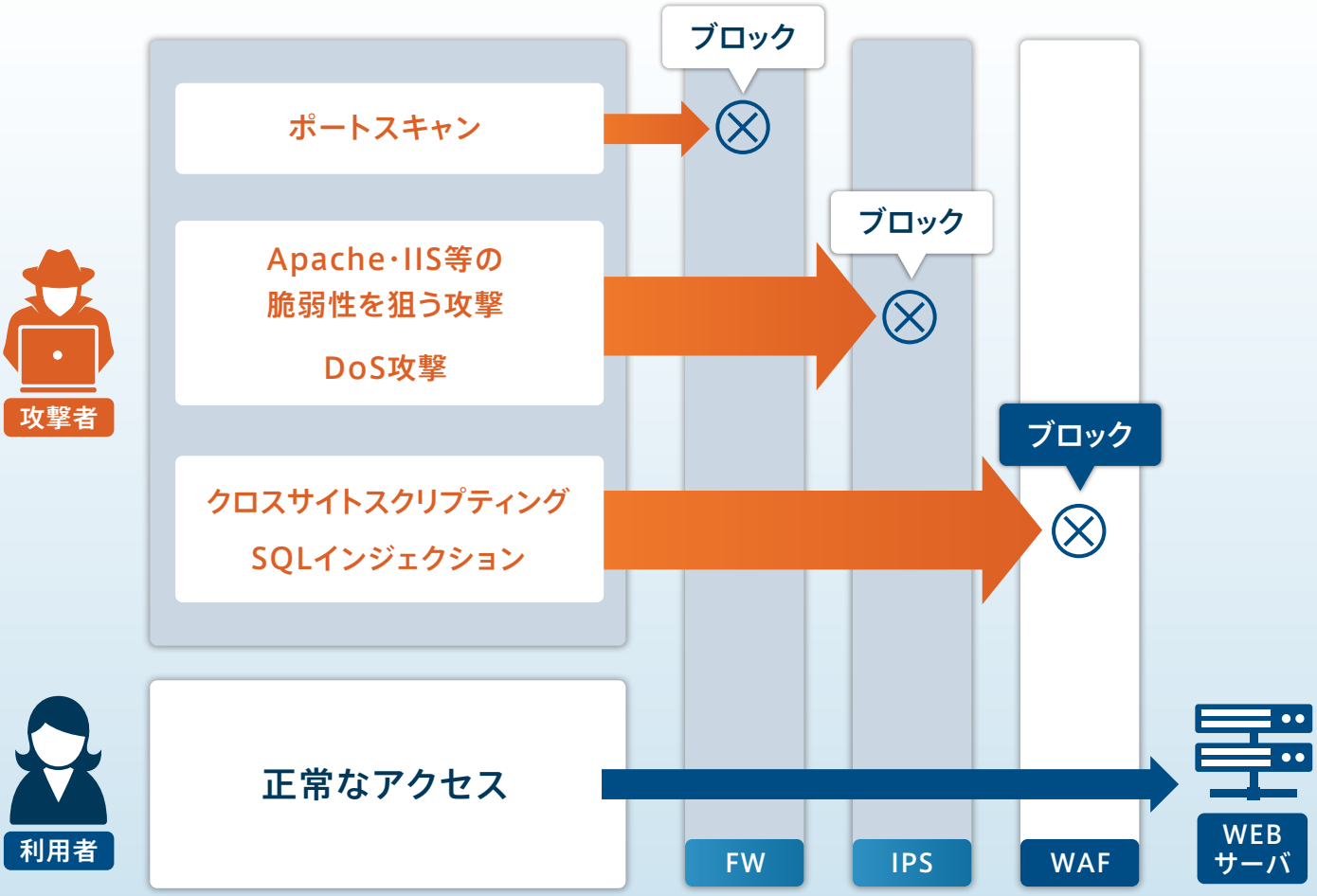
セキュリティの種類	セキュリティの効果
脆弱性診断	Webサイトの脆弱性を見つける。
WAF	**SQLインジェクション、 クロスサイトスクリプティングなどの攻撃を防ぐ。**
IPS	OSの脆弱性を狙う攻撃を防ぐ。
ファイアウォール(FW)	ネットワークのアクセス制御を行う。
ログ監視	ログを収集、監視する。
SSL	メールフォームなどの入力データを暗号化する。

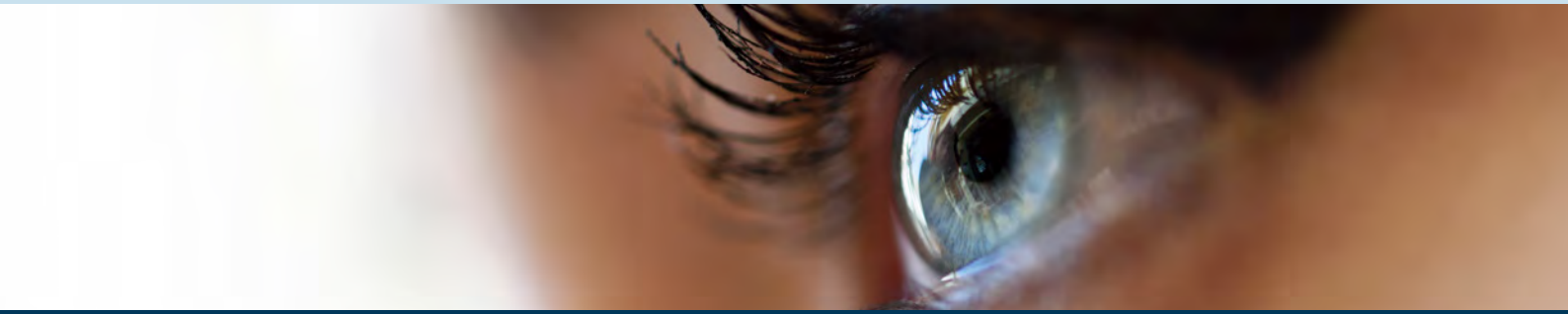
5.

WAF(Web Application Firewall)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。

FWがIPアドレスとポートを防御、IDS／IPSがプラットフォームレイヤを防御、WAFはアプリケーションレイヤを防御することにより、高セキュリティな環境を実現します。



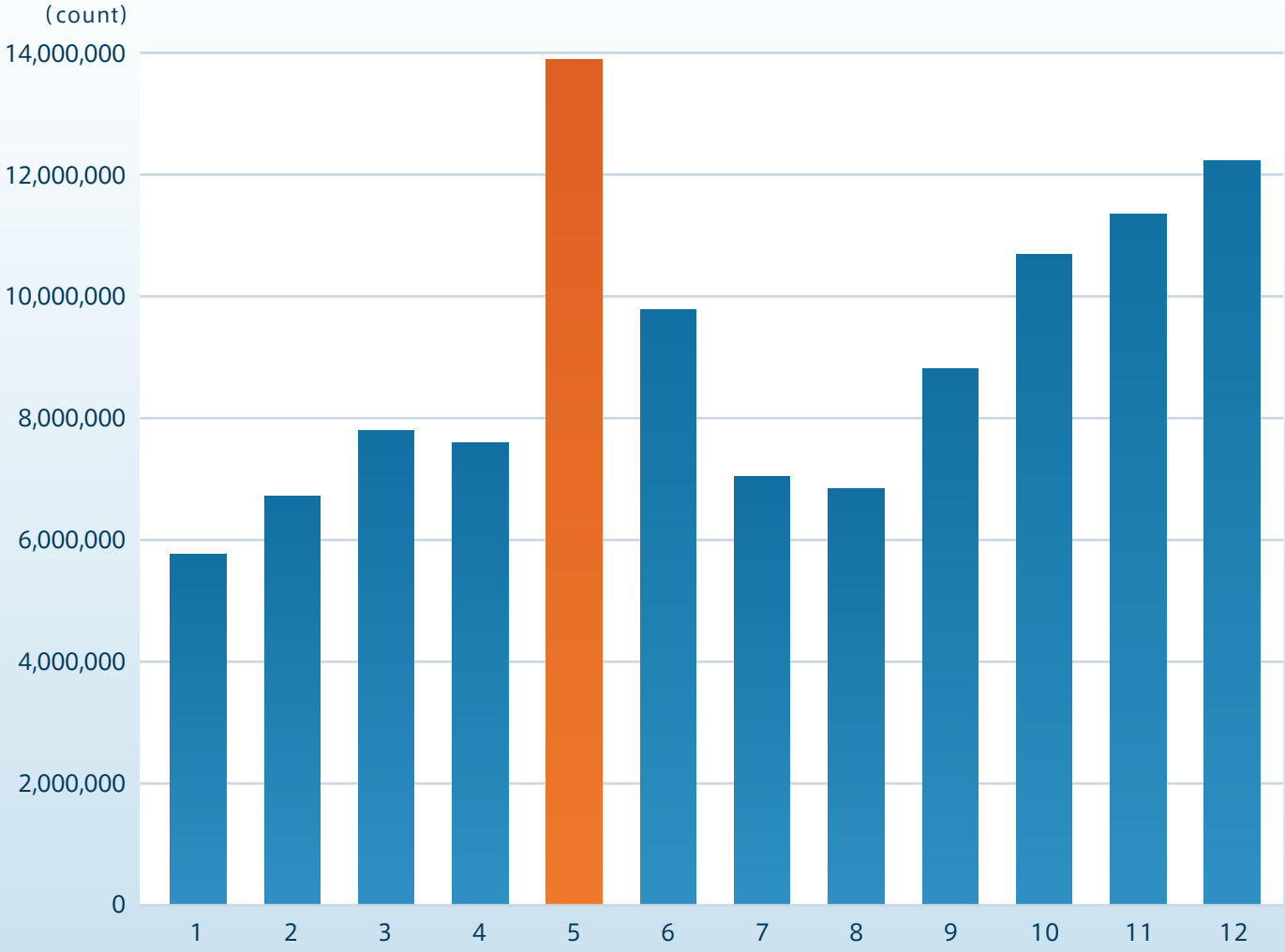


6.

攻撃遮断くんからわかるデータ

2018年の導入企業への攻撃ログ数は合計107,803,890件となりました。月単位で１番多く観測されたのは5月となっております。
また、2018年は後半にかけて月ごとに攻撃数は多く観測されており、今後も攻撃ログ数が増えていくことが予想されます。

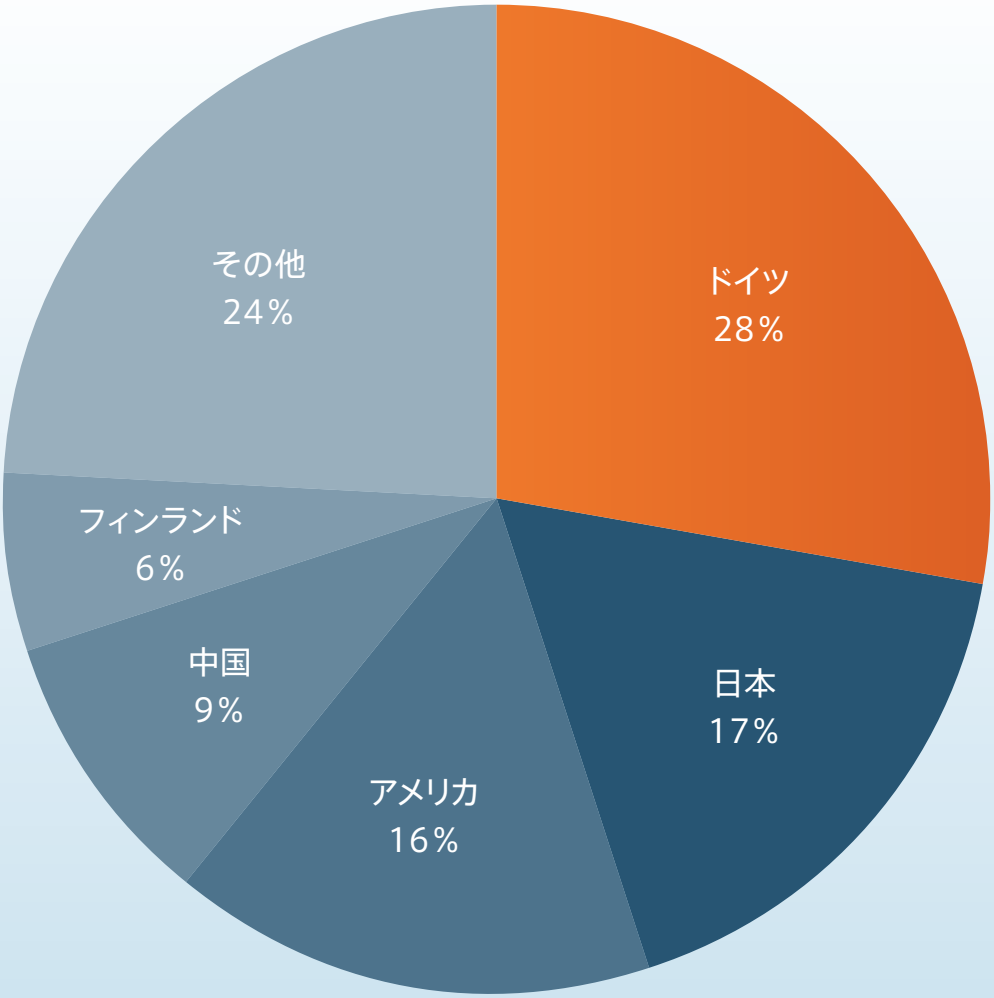
年間攻撃数推移

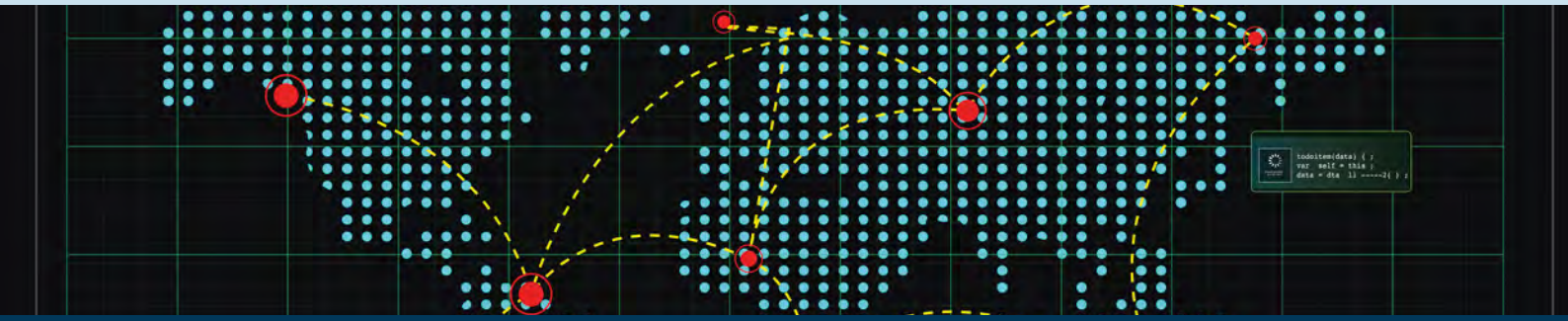


7.

国別での攻撃状況

2018年に検知した攻撃の攻撃元IPアドレスを国別に集計したのが、下記のグラフです。
クラウド型WAF「攻撃遮断くん」導入サービスにおける、攻撃元の国別Top10の1位はドイツとなりました。それぞれの順位とパーセンテージは、1位：ドイツ（28％）、2位：日本（17％）、3位：アメリカ（16％）、4位：中国（9％）、5位：フィンランド（6％）となっております。





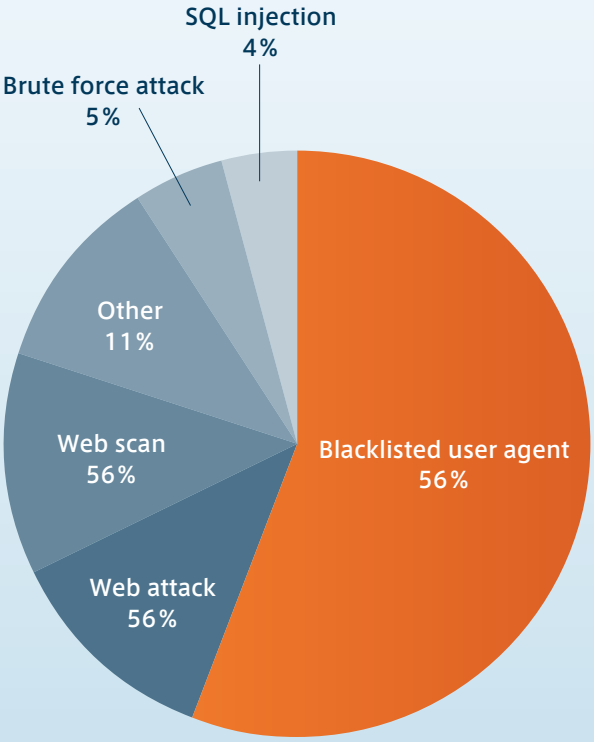
8.

攻撃別の構成比

検知した攻撃種別の構成比を現したグラフです。攻撃全体の56%が「Blacklisted user agent」によるものとなり、突出していることが読み取れます。

Blacklisted user agentについて

全体の約60%を占める「Blacklisted user agent」とは脆弱性スキャンツールを利用したBotによる攻撃を検知したものです。
「Blacklisted user agent」として検知するスキャンツールの１つである「ZmEu」は2012年9月ごろに開発されたツールではありますが、依然攻撃の手段として利用されています。このツールはphpMyAdminの脆弱性をスキャンします。Webサーバの安全を確保するためにも、最新のバージョンへアップデートする必要があります。



Blacklisted user agent
脆弱性スキャンツールを利用したBotによる攻撃です。「ZmEu」「Nikto」「Morfeus」などといったスキャンツールが該当します。

Web attack
DoS攻撃に近いものやOSコマンドインジェクションを行う攻撃です。

Web scan
攻撃の対象を探索・調査する動作や、無作為に行われる単純な攻撃で脆弱性を探す攻撃予兆と見られる方法です。

Brute force attack
暗号解読やパスワードを割り出すために総当たりで攻撃する方法です。

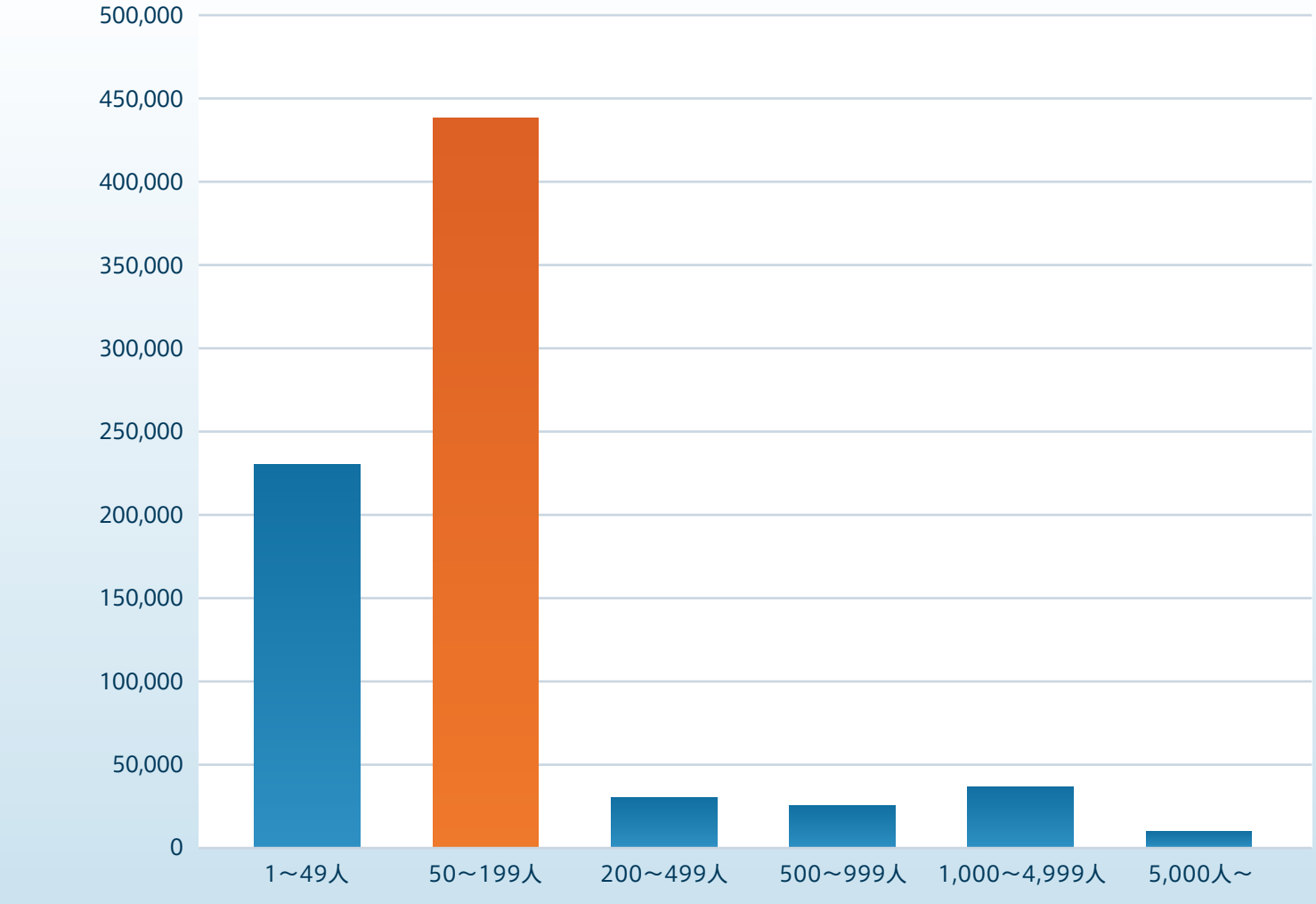
SQL injection
WEBアプリケーションの脆弱性を利用し、アプリケーションが想定してないSQL文を実行させることで、DBを不正に操作する攻撃です。

Other
上記に記載した攻撃手法の他にも、クロスサイトスクリプティングやディレクトリトラバーサルなどの攻撃方法がありますが比較的割合が少なかったものについてはOtherとしています。各種OSやミドルウェアなどの脆弱性を突いた攻撃などや通常、WAFの範囲外とされるものなども含みます。

9.

企業規模別の平均攻撃検知数

グラフは、企業規模で分類した１社あたりの攻撃検知数の平均グラフです。50～199人規模の企業への攻撃がもっとも多く観測されています。1～50人規模の企業や5,000人規模の企業への攻撃も計測されていることから、前述したBlacklisted user agent（脆弱性スキャンツールを用いたBotによる攻撃）をはじめとした様々なサイバー攻撃の脅威に、企業規模に問わずさらされていることがわかります。



10.

クラウド型WAF「攻撃遮断くん」のご案内

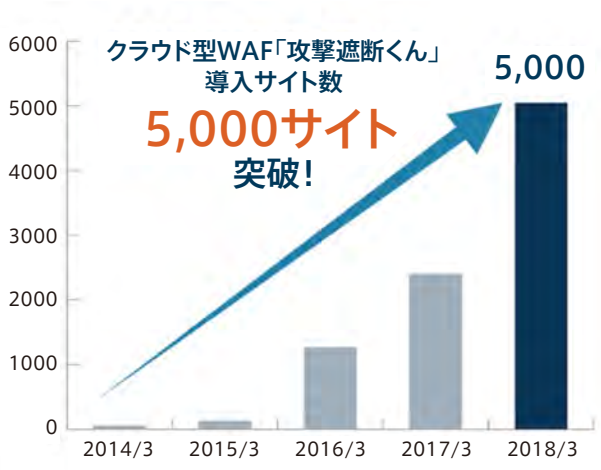
Webサイトへのサイバー攻撃を可視化・遮断するクラウド型WAF／導入社数・導入サイト数 No.1※

国産クラウド型WAF

攻撃遮断くん

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)

11.

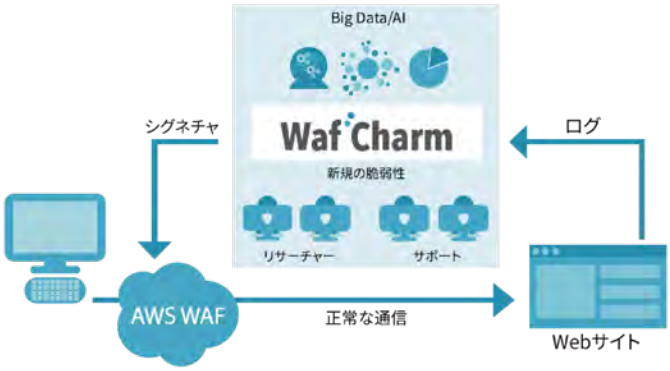
AWS WAF自動運用サービス「WafCharm」のご案内

AWS環境のセキュリティ対策ならWafCharm（ワフチャーム）
世界中のWebに対する攻撃パターンをAIによって学習し、全ての運用を自動化。

AWS WAF自動運用サービス

WafCharm

AIで「AWS WAF」が驚くほど簡単に！



Appendix：世の中の動き

サイバーセキュリティ基本法　【2014年11月】【成立2015年1月15日施行】

・内閣サイバーセキュリティセンター（NISC）設置

・セキュリティマインドを持った企業経営の推進

サイバーセキュリティ経営ガイドライン（経済産業省）　2017年11月16日 Ver.2公開

・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**

・グループ会社やビジネスパートナーやシステム管理の
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**

サイバーセキュリティ経営宣言（経団連）　2018年3月22日 公開

**サイバーセキュリティ対策を投資と位置づけ、
積極的な経営に取り組むことを掲げる。**

お問い合わせ

電話でお問い合せ／03-6416-1579（平日10:00～18:00）

メールでお問い合わせ／sales@cscloud.co.jp

Webからのお問い合わせ／ https://shadan-kun.com/

攻撃遮断くん／ https://www.shadan-kun.com/

WafCharm／ https://www.wafcharm.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
電話番号	03-6416-9996
FAX番号	03-6416-9997
Webサイト	https://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