【ニュースリリース】

2021 年 2 月 3 日

報道関係者各位

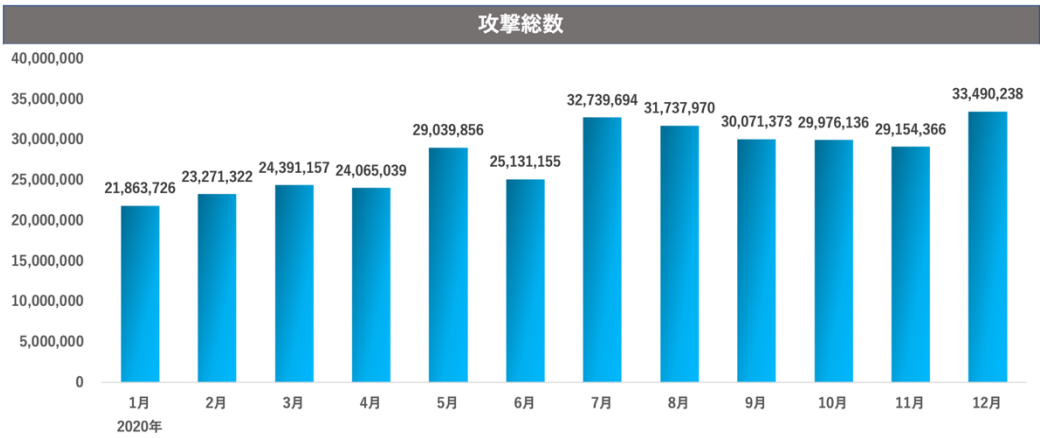
# サイバーセキュリティクラウド、「サイバー攻撃検知レポート 2020」を発表
## ～コロナ禍の 2020 年は過去 3 年間で最多の攻撃を検知～

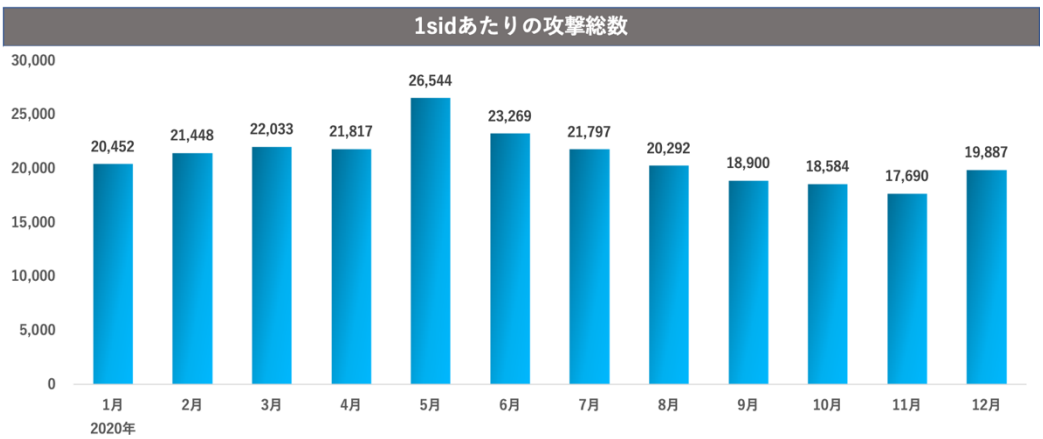
株式会社サイバーセキュリティクラウド（本社：東京都渋谷区、代表取締役社長　兼　CTO：渡辺洋司、以下「当社」）は、2020 年（2020 年 1 月 1 日～12 月 31 日）を対象とした、サイバー攻撃検知レポートを発表いたします。なお、本データは当社が提供する、Web サイトへのサイバー攻撃を可視化・遮断するクラウド型 WAF の「攻撃遮断くん」、AWS WAF、Azure WAF の自動運用サービス「WafCharm（ワフチャーム）」で観測した攻撃ログを集約し、分析・算出しています。

## ■調査概要

・調査対象期間：2020 年 1 月 1 日～2020 年 12 月 31 日
・調査対象：「攻撃遮断くん」、「WafCharm」をご利用中のユーザーアカウント
・調査方法：「攻撃遮断くん」、「WafCharm」で観測した攻撃ログの分析

## ■2020 年のサイバー攻撃検知状況



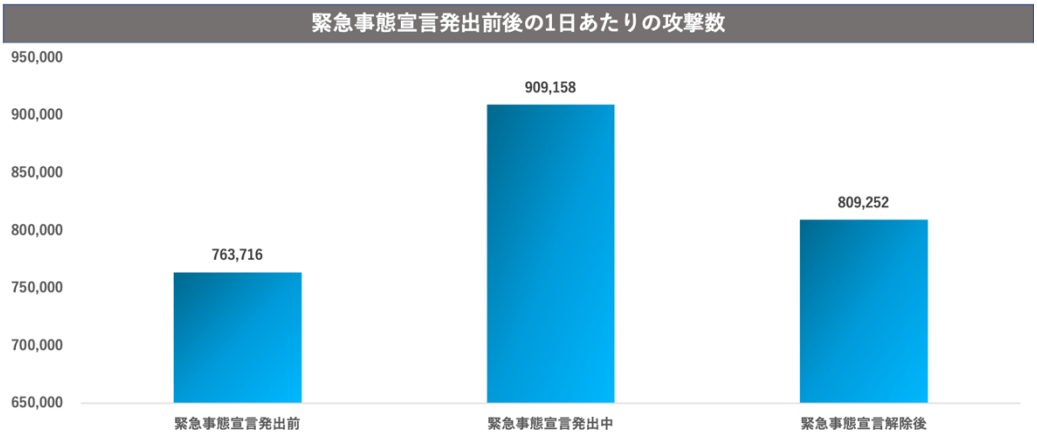



2020 年 1 月から 12 月の間に検知したサイバー攻撃の検知数は 334,932,032 件でした。これは 1 年間の間、約 10 秒に 1 回のペースで攻撃を検知していたことになります。

さらに 1sid（sid=Security Identifier：ネットワークのユーザアカウントやグループなどを一意に識別するセキュリティ識別子）あたりでは、平均 21,059 件/月の攻撃を検知。2019 年と比較すると約 10%増加しており、過去 3 年間で最多の検知数となりました。中でも 5 月が最も多くのサイバー攻撃を検知しており、新型コロナによって多くの企業がテレワーク等のニューノーマルな働き方にシフトし、オンラインでの対応が増えたことなどが影響したと考えられます。

また 2020 年 1 月から 6 月の上半期を見ると、1sid あたり平均 22,593 件／月の攻撃を検知。対して 7 月から 12 月の下半期は、1sid あたり平均 19,525 件／月と約 13.5%減少しました。企業の夏季休暇を含む 7 月・8 月は比較的多くの攻撃を検知したものの、その後は減少傾向が続きました。

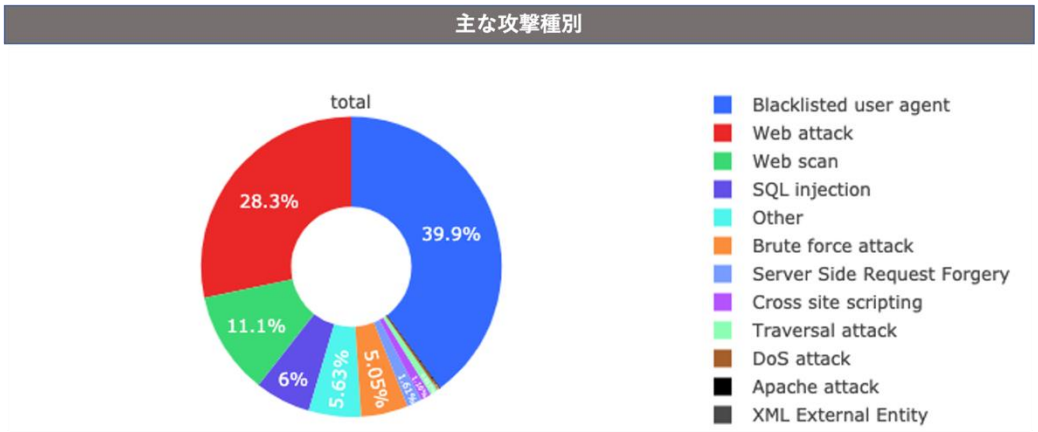
## ―新型コロナ発生による緊急事態宣言の前後で検知状況に変化




さらに攻撃の多かった上半期における攻撃数のデータにおいて、新型コロナウイルスの感染拡大による緊急事態宣言の発出前後で 1 日あたりの平均攻撃数を比較した結果、4 月 7 日～5 月 25 日の緊急事態宣言期間中においては 1 日あたり 909,158 件の攻撃を検知し、宣言発出前である 1 月 1 日～4 月 6 日間の 1 日あたりの平均攻撃数に対し 19%以上多い結果となりました。また緊急事態宣言が解除された 5 月 26 日から 6 月 30 日の 1 日あたりの平均攻撃数は、809,252 件と減少したものの、宣言発出前と比べると 6%程度増加しました。

新型コロナの感染拡大が懸念されている中、再び緊急事態宣言が発出されており、前回同様に発出期間中は攻撃数が増加している可能性も考えられるため、改めてサイバー攻撃への警戒を強める必要があります。

## ■攻撃種別ごとの検知数と攻撃動向



今回の調査期間における、主な攻撃種別の攻撃状況を見ると、脆弱性スキャンツールなどを利用した Bot による攻撃である「Blacklisted user agent」が全体の 39.9%を占め、次いで Web サーバーを構成するソフトウェアの脆弱性に対する攻撃である「Web attack」が 28.3%、攻撃の対象を探索・調査したり、無作為に行われる単純な攻撃で脆弱性を探す方法である「Web scan」が 11.1%と続きました。

### ―新型コロナ禍において「Web attack」が急増

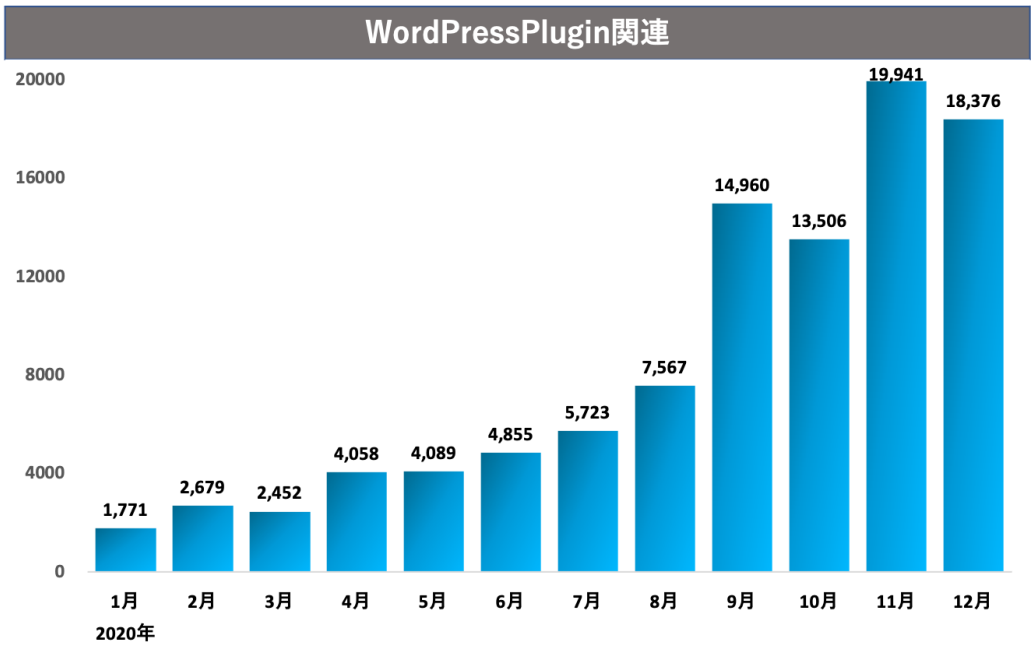
2020 年の攻撃種別ごとの攻撃件数と 2019 年の同時期のものを比較すると、攻撃種別の上位 3 項目について、「Blacklisted user agent」は約 1.6 倍、「Web scan」は約 1.4 倍程度の増加率であったことに対して、「Web attack」は約 2.5 倍増加。さらに 2020 年 1 月 1 日から 1 月 31 日において「Web attack」が攻撃全体に占める割合は 18%程度であったのに対し、5 月 1 日～30 日の間では 29.8%にまで増加しており、新型コロナの感染拡大とともに、「Web attack」の脅威が高まったことが判明しました。

### ―攻撃方法が多様化

本調査期間における攻撃種別ごとの攻撃検知結果と 2019 年の同時期のものを比較し、各攻撃が全体に対して占める割合を比べたところ、「Web attack」をのぞいて、「Blacklisted user agent」や「Web scan」、「SQL injection」、「Brute force attack」など、攻撃数の上位にある攻撃方法が占める割合が減少しています。2020 年に入り、攻撃の方法が「Web attack」に集中している可能性の他に、攻撃手法の幅が広がり、多様化している可能性が考えられます。

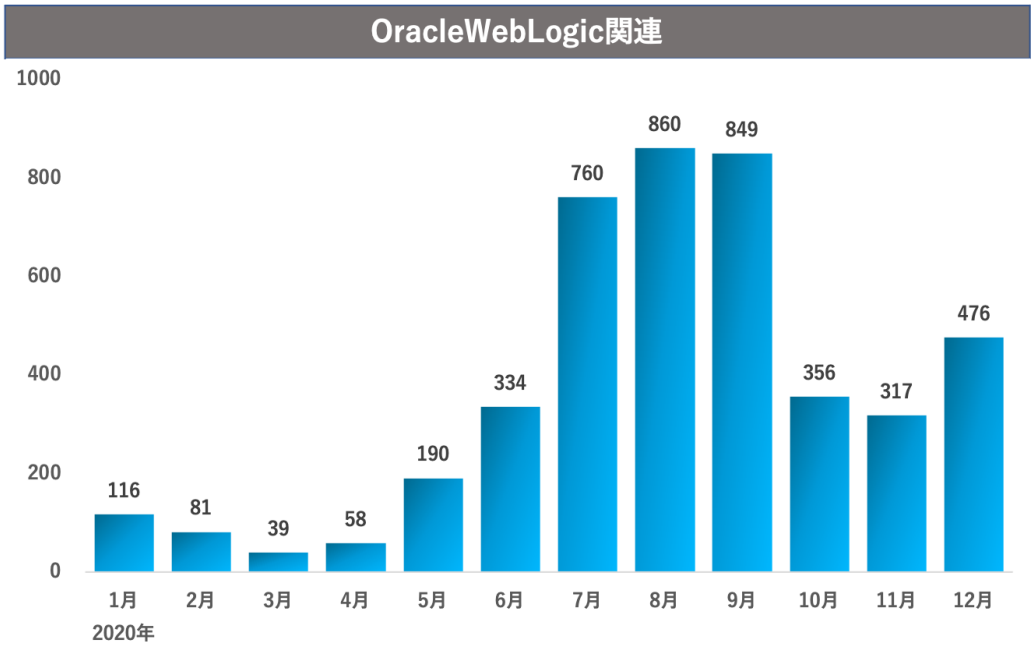
## ■主な脆弱性に関する攻撃状況

### ―「WordPress Plugin」の脆弱性を狙った攻撃



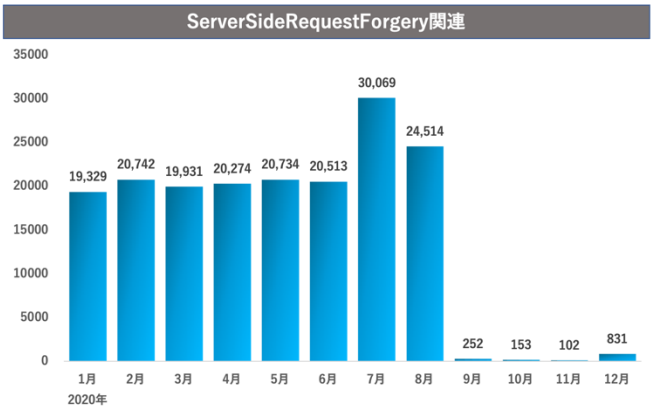
WordPress の機能を拡張するためのツールである「WordPress Plugin」の脆弱性を狙った攻撃が、9 月中旬から大幅に増加し、その後一旦減少したものの、11 月に向かうにつれ再び増加しました。これは同時期に WordPress 用 Plugin「File Manager」の脆弱性が見つかっており、この脆弱性を標的にした攻撃が増加した可能性が高いと考えられます。

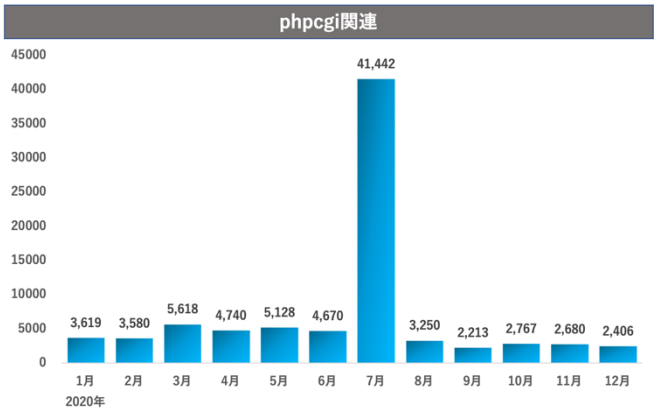
### ―「Oracle WebLogic」の脆弱性を狙った攻撃

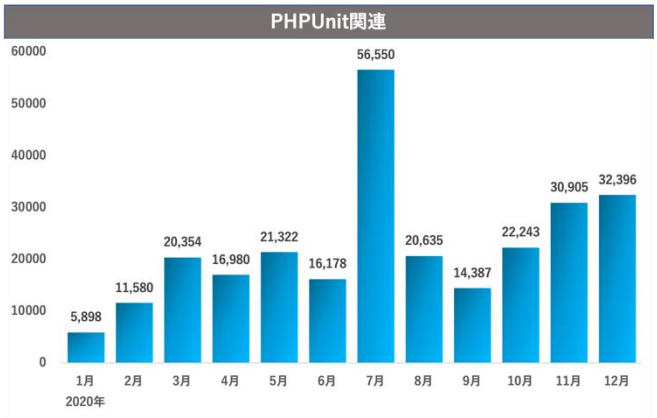


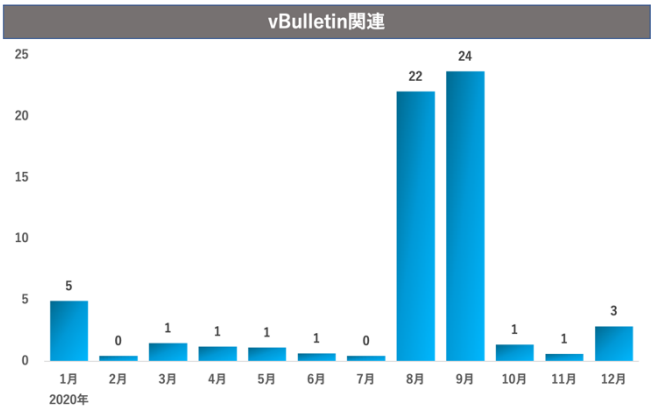

Oracle 社が提供するアプリケーションサーバである「Oracle WebLogic」の脆弱性を狙った攻撃が 5 月以降徐々に増加しており、一旦減少したものの 12 月 14 日には年内最高値を計測いたしました。「Oracle WebLogic」の脆弱性が 10 月に公表されていることから、公表前まで脆弱性を標的にしたアクセスが増加していた可能性が高いと考えられます。

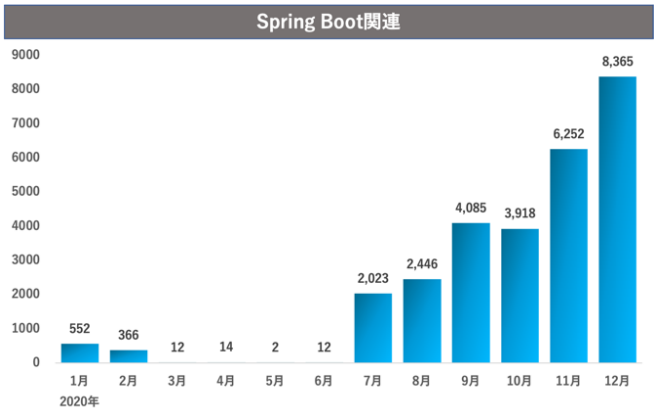
### ―その他の脆弱性を狙った攻撃






「ServerSideRequestForgery」は、外部から到達できない領域にあるサーバーなどに対して、バグを悪用することでリクエストを送る攻撃手法で、一般的には対策を施そうとするとサーバーの機能を阻害してしまうなど、攻撃手法の中でも対策が難しい攻撃とされ、7 月から 8 月にかけて急激に増加しその後大幅に減少しました。またプログラム言語の PHP を実行ファイル形式で動作させる「php cgi」や PHP での単体テストを行うフレームワークである「PHPUnit」の脆弱性を狙った攻撃が 7 月に突出して増加しました。またフォーラムサイト構築ソフトである「vBulletin」の脆弱性に対する攻撃は 8 月後半から 9 月にかけて急激に増加し、さらに Java フレームワークである「Spring Boot」に対する攻撃が 7 月半ばから徐々に増加しております。

**■サイバーセキュリティクラウド 代表取締役社長 兼 CTO 渡辺洋司のコメント**

新型コロナの影響によって人々の生活様式が大きく変化した 2020 年において、国内のサイバーセキュリティ事案を振り返ってみると、9 月に問題が表面化したドコモ口座の不正利用事案や、11 月に発覚したカプコンにおける最大 35 万件にも及ぶ顧客情報流出事案などが話題になりました。中でもカプコンのケースは、コロナ禍で需要が高まるオンラインゲームサービスをターゲットにした攻撃であり、同様にこうした状況下で需要拡大が見込まれるサービスでは十分な警戒が必要と言えます。

また 2020 年は、過去 3 年間の調査において最多の攻撃数を検知し、中でも上半期は特に多くの攻撃を検知しました。緊急事態宣言の発出前後で攻撃数に変化も見られ、新型コロナによる働き方の変化の影響も見られました。

このように多数の攻撃が検知された中、公表に至った事例は一部のみで、他にも多くの企業が発覚にすら至っていない可能性も考えられます。新型コロナ禍においてサイバー攻撃は増加、多様化しており、さらに改正個人情報保護法の成立によって個人情報漏洩に対する企業の責任も重くなるため、企業規模を問わず Web サイトを保有する組織は、一度自社のサイバーセキュリティ対策が十分かを見直すことも必要です。

**【クラウド型 WAF「攻撃遮断くん」について】**

https://www.shadan-kun.com/

クラウド型 WAF「攻撃遮断くん」は、Web サイト・Web サーバへのサイバー攻撃を可視化・遮断する Web セキュリティサービスです。ディープラーニング（深層学習）を用いた攻撃検知 AI エンジン「Cyneural」を活用し、一般的な攻撃の検知はもちろん、未知の攻撃の発見、誤検知の発見を高速に行うとともに、世界有数の脅威インテリジェンスチーム「Cyhorus」により、最新の脅威にもいち早く対応します。導入社数・サイト数で国内 1 位※1 を獲得し、企業規模を問わずご利用いただいています。

**【「WafCharm（ワフチャーム）」について】**

https://www.wafcharm.com/

「WafCharm」は導入ユーザ数で国内 No.1※2 の、パブリッククラウドで提供されている WAF を“AI”と“ビックデータ”によって自動運用することが可能なサービスです。AWS と Microsoft Azure の 2 大プラットフォームに提供しております。
機械学習を用いて最適な WAF ルールを自動運用する AI エンジン「WRAO（ラオ）※3」（特許番号：特許第 6375047 号）を搭載しており、累計導入サイト数・導入社数国内 No.1※1 の実績を持つクラウド型 WAF「攻撃遮断くん」で培った累計 1.7 兆件以上のビックデータを活用し、お客様毎に最適なルールを自動で適用します。サイバー脅威情報監視チーム「Cyhorus」により最新の脅威にもいち早く対応します。また、国内有数のシグネチャカスタマイズのノウハウをもった、開発エンジニアによるサポート※4 も合わせて提供しています。

**【株式会社サイバーセキュリティクラウドについて】**

会社名：株式会社サイバーセキュリティクラウド
所在地：〒150-0011　東京都渋谷区東 3-9-19 VORT 恵比寿 maxim3 階
代表者：代表取締役社長　兼　CTO　渡辺　洋司
設立　：2010 年 8 月
URL　：https://www.cscloud.co.jp/
「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」という理念を掲げ、サイバーセキュリティクラウドでは、世界有数のサイバー脅威インテリジェンスと AI 技術を活用した、Web アプリケーションのセキュリティサービスを全世界に向けてサブスクリプションで提供しています。また、クラウド市場世界シェア 47.8%※5 を持つ AWS において、世界で 7 社目と

なる AWS WAF マネージドルールセラーにも認定されております。
これからも私たちは、リーディングカンパニーとして、世界中の人々が安心安全に利用できるサイバー空間を創造するためのサービス開発を行い、情報革命の推進に貢献してまいります。

※1 出典:「クラウド型 WAF サービス」に関する市場調査(2019 年 5 月～2019 年 6 月 調査)＜ESP 総研 調べ＞
※2 出典: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 AWS WAF classic のみに対応
※4 一部プランのみ対象となります
※5 出典:Gartner(August 2020)・・・Worldwide Iaas Public Cloud Services Market Share, 2018-2019

**＜本件のお問い合わせ＞**

■サービスに関するお問い合わせ先
株式会社サイバーセキュリティクラウド
マーケティング部 PR・マーケティングチーム
電話:03-6416-9996 FAX:03-6416-9997
E-mail:pr@cscloud.co.jp

■報道関係お問い合わせ先
サイバーセキュリティクラウド PR 事務局(スキュー内)
担当:北出
TEL:03-6450-5457 Mail:csc@skewinc.co.jp