【ニュースリリース】

2023 年 2 月 21 日
株式会社サイバーセキュリティクラウド

報道関係者各位

1 秒間に 17 回ものサイバー攻撃を検知
2022 年 1 月～12 月の『Web アプリケーションへのサイバー攻撃検知レポート』を発表

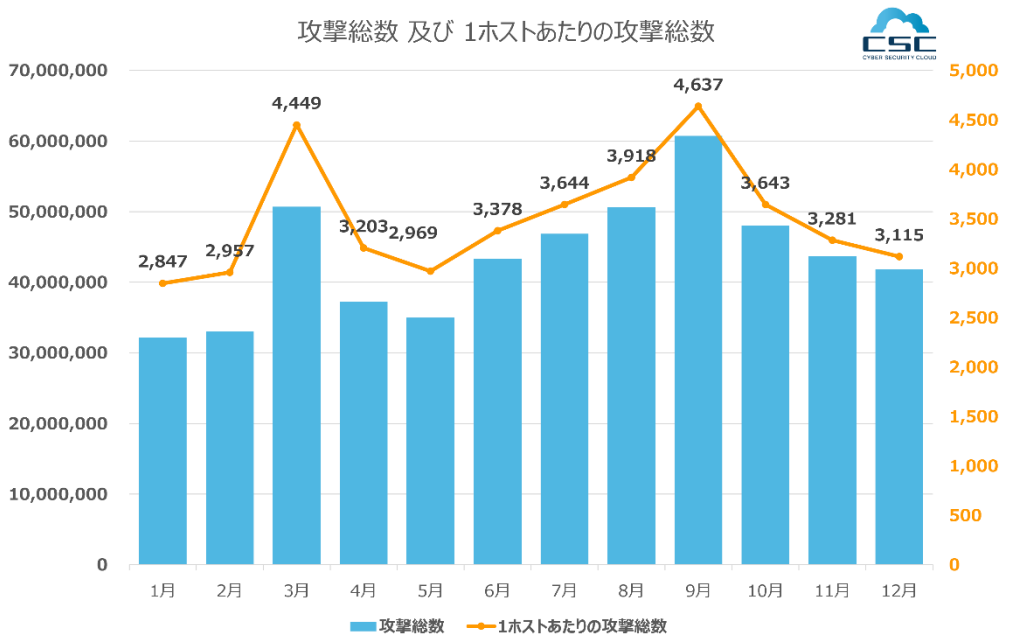
ハッカー対策サービスを展開するグローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池敏弘、以下「当社」）は、2022 年 1 月 1 日～12 月 31 日を対象とした『Web アプリケーションへのサイバー攻撃検知レポート（以下「本レポート」）』を発表します。

本レポートは、当社が提供する Web アプリケーション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』、及びパブリッククラウド WAF の自動運用サービス『WafCharm（ワフチャーム）』で観測したサイバー攻撃ログを集約し、分析・算出しています。

サイバー攻撃は年々大幅な増加傾向にあり、企業としても対策が急務になっています。しかしながら、サイバー攻撃は目に見えないため「身近に感じられない」という問題があります。本レポートはサイバー攻撃の実情を明らかにすることで、より多くの方にサイバーセキュリティ強化の必要性を感じていただくためのものです。

«レポートサマリ»
■ 1 秒間に 17 回もの攻撃を検知。
■ 攻撃元 IP は 1 位がアメリカで 49%、2 位は日本国内からで 20%に。
■ 攻撃種別として最も多かったのは、Web サーバを構成するソフトウェアの脆弱性に対して無差別に行われる単純攻撃の“Web attack”が全体のおよそ 44%。引き続き“SQL injection”も顕在しており増加傾向。

■ 検知総数と推移：1 秒間に 17 回のサイバー攻撃を検知

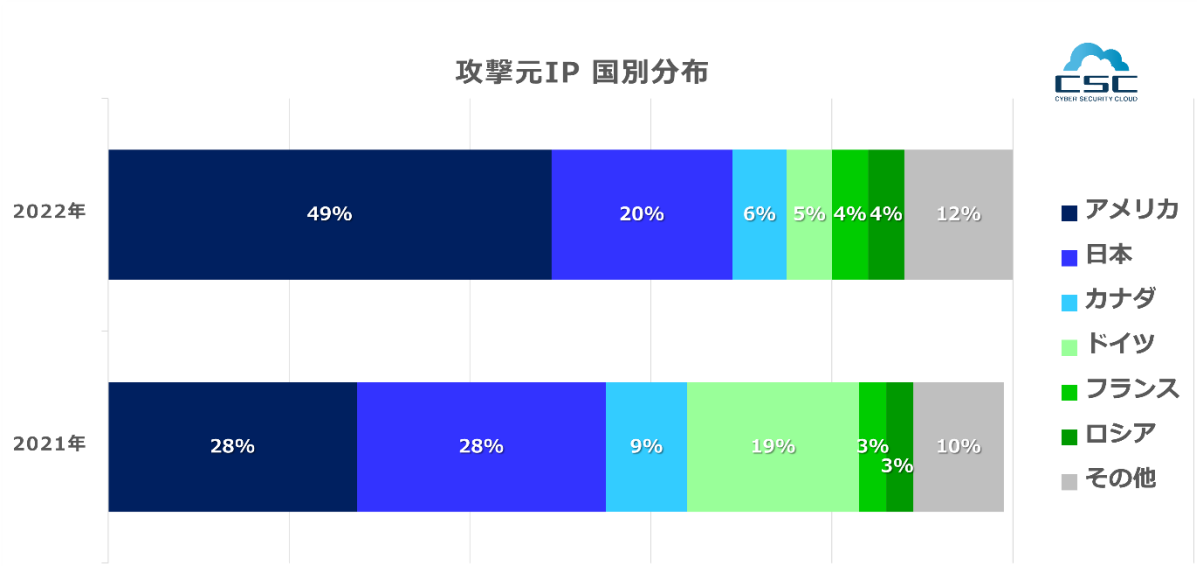


2022 年 1 月 1 日から 12 月 31 日までに、当社で検知した Web アプリケーションへのサイバー攻撃の総数は 523,210,675 件でした。また、1 ホストあたり（※）では 415,463,802 件で、これは 1 秒あたり 17 回ものサイバー攻撃を検知していることとなります。

サイバー攻撃自体は 1 企業を狙ったものではなく、無差別に様々な企業へ仕掛けられていることから、今やサイバー攻撃被害の可能性はどの企業でも有り得ると言えます。

※『攻撃遮断くん』の保護対象ホスト数（Web タイプ：FQDN 数、サーバタイプ：IP 数）と、『WafCharm』の保護対象ホスト数（WebACL）との総数を分母に概算。

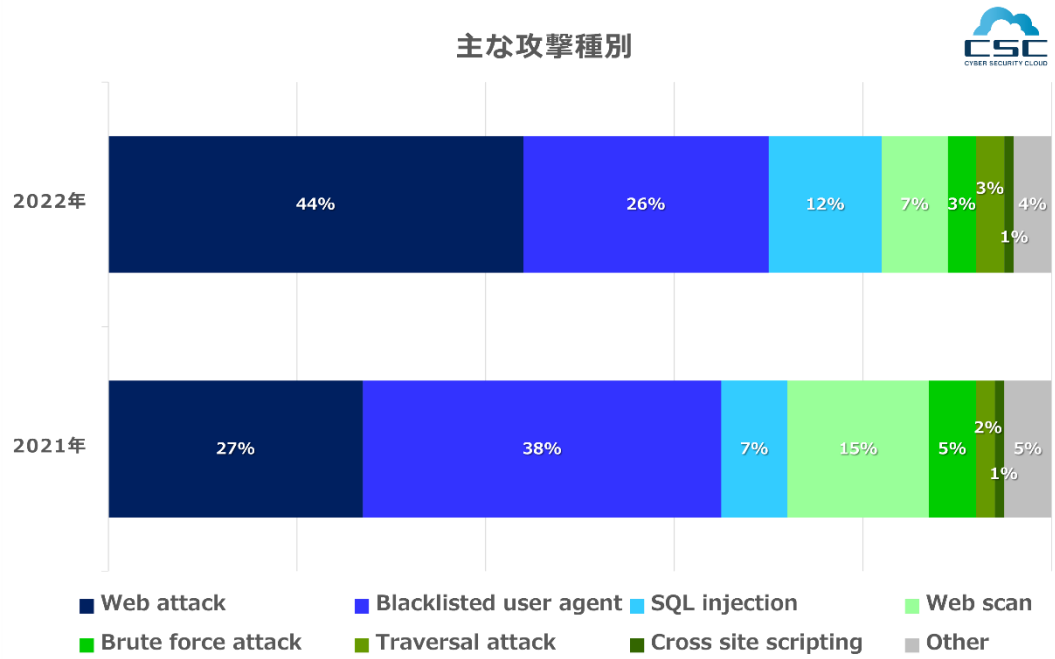
■ 攻撃元 IP は 1 位がアメリカで 49%、攻撃検知のほぼ半分を占める割合に。



当社が検知した Web アプリケーションへのサイバー攻撃について、攻撃元 IP を国別に見ると、2022 年はアメリカからの攻撃が 49%と最も多く、2 位が日本国内からで 20%、3 位がカナダで 6%、次いでドイツ、フランスと続いています。2021 年と比較すると、アメリカからの攻撃が大幅に増えていることがわかります。

しかし以前から、特に大掛かりな組織が標的型攻撃を仕掛ける場合は直接ターゲットにアクセスするのではなく、途中に様々な国のデータセンターなどを幾度も経由し、相手から本当の攻撃発信元の所在地を知られないようにカモフラージュすることも非常に多くはなっています。

■ **攻撃種別では 1 位が 44%で“Web attack”。3 位の“SQL injection”は昨年度より増加。**

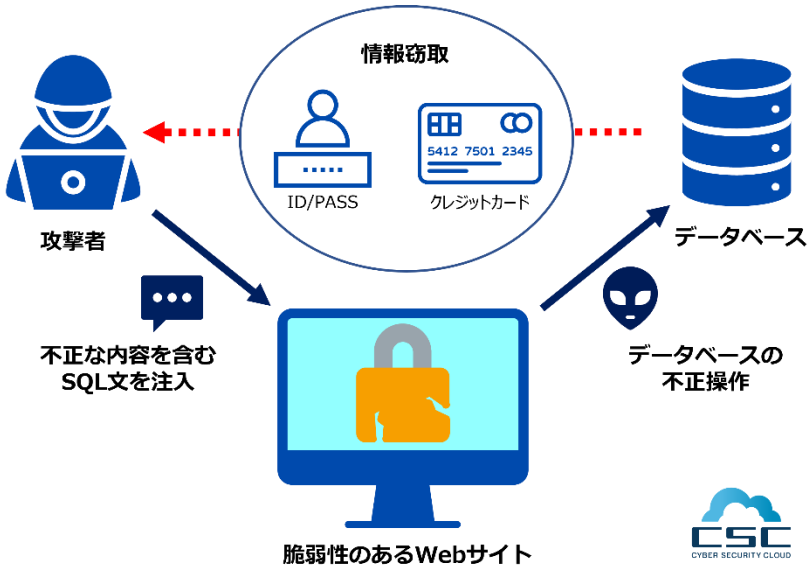


今回の調査期間における主な攻撃種別ごとの攻撃状況を見ると、主だった傾向は 2021 年とさほど大きくは変わっていません。最も多かったのは、Web サーバを構成するソフトウェアの脆弱性に対して無差別に行われる単純攻撃の“Web attack”が全体のおよそ 44%を占め、2021 年より大きく増加しています。

一方、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”は 26%と 2021 年より減少していました。

注目したいのが 3 位に位置する“SQL injection”で、母数は少ないながらも割合として増加しています。この攻撃から不正にデータベースのデータが読み取られたり、データが改竄・削除されたりするので被害は甚大です。2022 年末時点でもまだまだ大きな被害を及ぼしていますので、引き続き注意が必要となります。

■ **増加している SQL インジェクションとは**



SQL インジェクションとは、攻撃者が不正な「SQL 文（データベースの情報を動かす命令文）」を作成し、Web サイトなどの脆弱性（不完全さ・脆さ）を突いて「注入（injection）」することでデータベースを不当に操作する攻撃です。
対策として Web アプリケーションを常に最新のバージョンにすることや、攻撃を無効化が出来る様なエスケープ処理などがありますが、脆弱性そのものをなくすのは困難な場合が多いです。必要に応じて WAF（Web Application Firewall）などを利用して、攻撃を監視・検知・遮断を行うことが大切です。

■ 自社を含むサプライチェーン全体でのサイバーセキュリティ強化が急務
2022 年は世界情勢の影響により、サイバー攻撃が増えるなど、国内外問わずサイバー攻撃の潜在的リスクが急激に高まりました。
代表的なところではサプライチェーン攻撃や BEC（ビジネスメール詐欺）などを始め、ロシアを支持するサイバー攻撃集団「キルネット」が日本国に向けて宣戦布告し、政府・企業の「DDoS 攻撃」被害なども相次いで発生しました。
一方で、サイバーセキュリティに関する法令関係のアップデートとして、2022 年 4 月には改正個人情報保護法が施行され、個人情報漏洩の報告が義務化となりました。また、個人情報保護委員会からの命令違反や虚偽報告などがあった場合の罰金刑が最高で 1 億円以下に大きく引き上げとなり、日本国全体でのサイバーセキュリティ強化の気運は高まり続けています。
2023 年も引き続きサイバー攻撃の増加が考えられ、自社だけの対策強化に留まらず、サプライチェーン全体でのサイバーセキュリティ強化が求められます。そのためにはサプライチェーンを含む自社で必要な対応策を検討し、継続的に管理・運用しながら、定期的な見直しと改善とを続けることが重要となります。
当社では「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」ことを経営理念としています。サイバー攻撃の実情を定期的に集約・分析することで、サイバーセキュリティ強化が急務となる一方で具体的なサイバー攻撃対策方法に悩む、様々な企業のサポートを行っていきます。

■ 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：〒141-0021　東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 階
代表者：代表取締役社長 兼 CEO 小池敏弘
設立：2010 年 8 月
URL：https://www.cscloud.co.jp

サイバーセキュリティクラウドは「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」という経営理念を掲げ、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、及び脆弱性情報収集・管理ツールといったハッカー対策サービスを提供しています。これからも私たちは WAF を中心としたサイバーセキュリティにおけるグローバルリーディングカンパニーの 1 つとして、情報革命の推進に貢献してまいります。

主な展開サービス：
- クラウド型 WAF『攻撃遮断くん』：https://www.shadan-kun.com

- パブリッククラウド WAF の自動運用サービス『WafCharm』：https://www.wafcharm.com
- 改竄検知機能を搭載した『WafCharm for AWS Marketplace』：
https://www.wafcharm.com/jp/aws-mp
- 厳選された AWS WAF 用のルールセット『Cyber Security Cloud Managed Rules for AWS WAF』：
https://aws.amazon.com/marketplace/seller-profile?id=baeac351-6b7c-429d-bb20-7709f11783b2
- 脆弱性情報収集・管理サービス『SIDfm』：https://sid-fm.com

■ 調査概要
・調査対象期間：2022 年 1 月 1 日～2022 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アカウント
・調査方法：『攻撃遮断くん』『WafCharm』で観測したサイバー攻撃ログの分析

■ 報道関係者のお問い合わせ先
株式会社サイバーセキュリティクラウド
経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996
FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp