

報道関係者各位

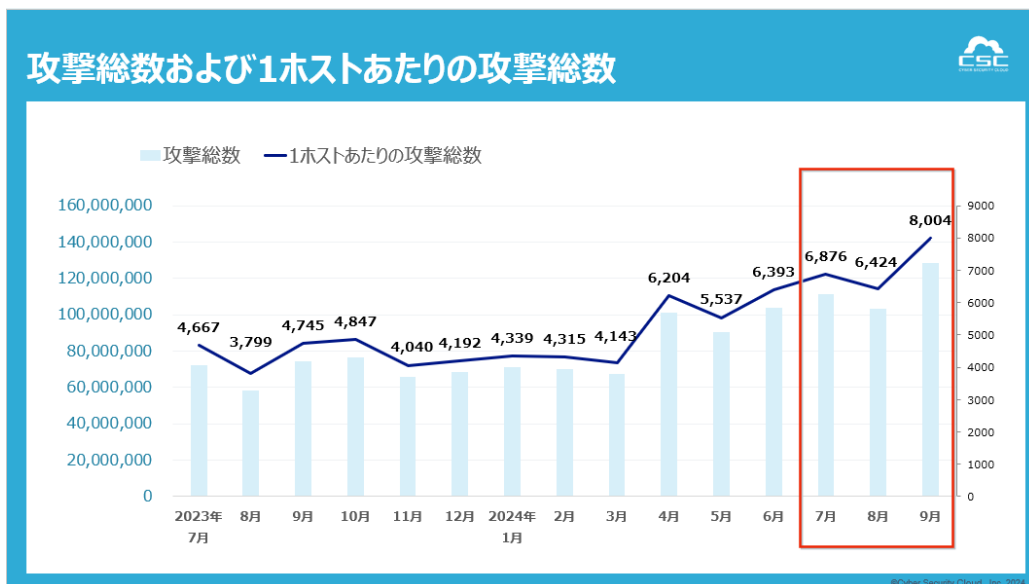
**2024年第3四半期「Webアプリケーションを狙ったサイバー攻撃検知レポート」を発表
～個人情報とクレジットカード情報の流出件数で最も多かった業界は食品・飲料製造業～**

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、2024年第3四半期(2024年7月1日～9月30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。

「レポートサマリー」

- ・1日に約370万回のサイバー攻撃を検知
- ・SQLインジェクションが約6,400万件増加
- ・2024年、個人情報とクレジットカード情報の流出件数で最も多かった業界は食品・飲料製造業

■ 攻撃総数と推移：1日に約370万回のサイバー攻撃を検知



2024年7月1日～9月30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攻撃数は343,495,810件でした。これは、1日に約370万回の攻撃を受けている計算になります。1ホスト(※1)あたりでは21,304件でした。

(※1)『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。

■ 攻撃元国

攻撃元国



2024年7月～9月	国	前年同期比
1位	 アメリカ	1位 →
2位	 日本	2位 →
3位	 イギリス	4位 ↓
4位	 フランス	3位 ↑
5位	 オーストラリア	8位 ↑
6位	 ロシア	7位 ↑
7位	 カナダ	6位 ↓
8位	 中国	9位 ↑
9位	 ドイツ	5位 ↓
10位	 ブルガリア	14位 ↑

©Cyber Security Cloud, Inc. 2024

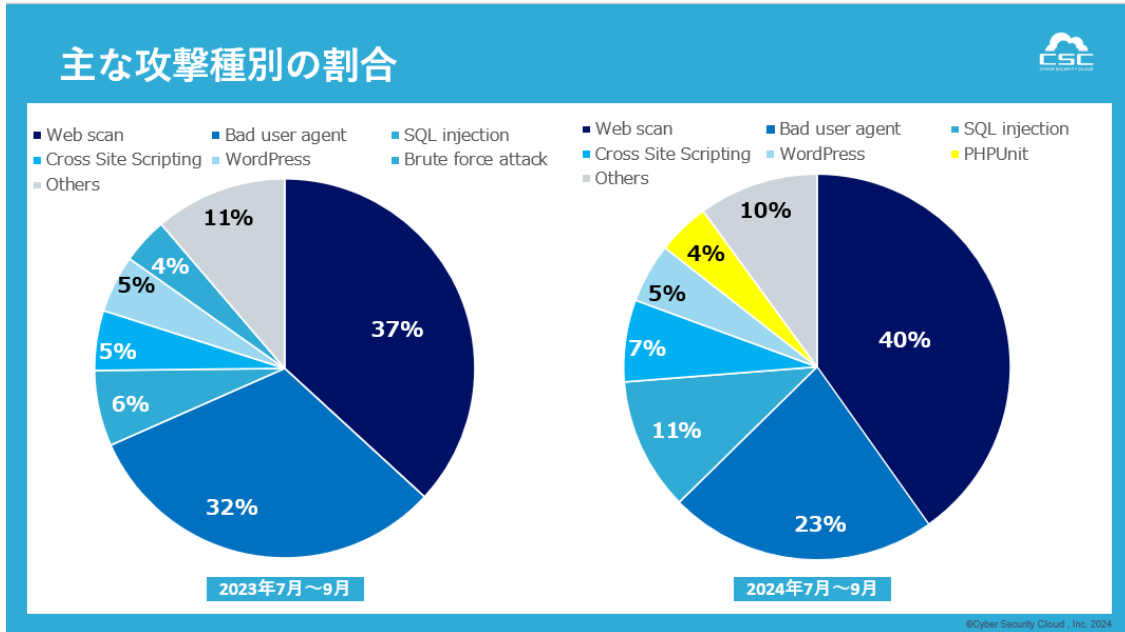
検知された攻撃元を国別に2023年同期比で見ると、攻撃件数の上位は1位アメリカ、2位日本、3位イギリス、フランス、オーストラリアと続いていました。

上位国についてはさほど変化はありませんが、2024年7月～9月で14位だったブルガリアが10位にランクインしています。

【本件に関するお問い合わせ】

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・川崎
 TEL：03-6416-9996 携帯：080-4583-2871(川崎携帯) FAX：03-6416-9997
 E-Mail：pr@cscloud.co.jp

■ 主な攻撃種別

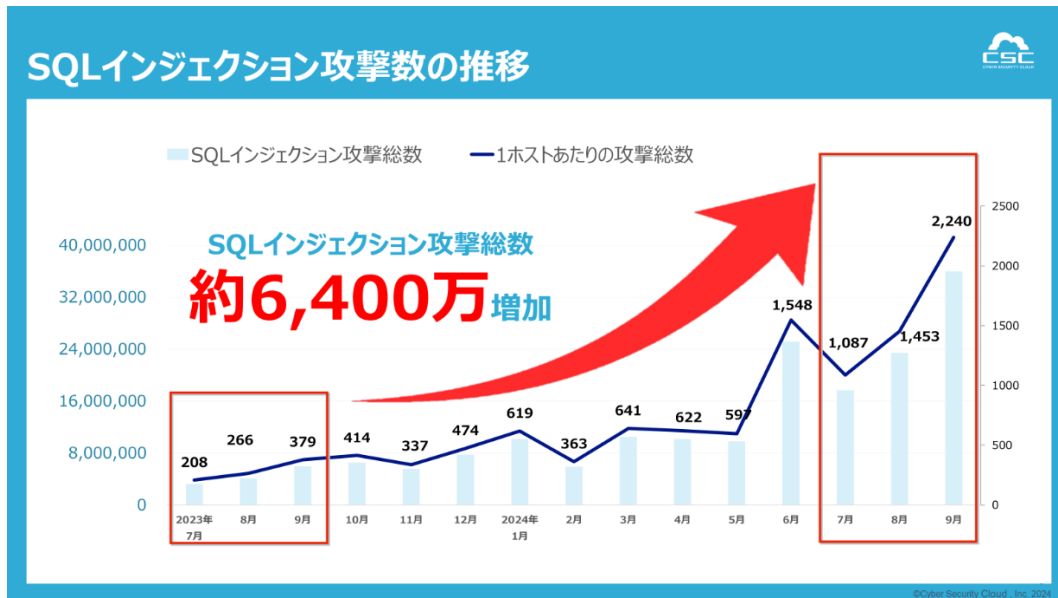


今回の調査期間における主な攻撃種別の攻撃状況を見ると、全体の総数は増加しているものの主だった傾向は2023年とさほど大きくは変わっていない状況です。最も多い攻撃種別は、攻撃の対象を探索・調査、また無作為に行われる単純な攻撃で脆弱性を探すなどの「攻撃の予兆」である「Web scan」が40%を占めています。続いて脆弱性スキャンツールなどを利用した Bot による攻撃である「Bad user agent」が全体の23%を占めています。また、これまで注目されていなかった PHP のテストフレームワーク「PHPUnit」を狙った攻撃も、第2四半期に850万件増加した後、引き続き増加していることが確認されました。

【本件に関するお問い合わせ】

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・川崎
 TEL：03-6416-9996 携帯：080-4583-2871(川崎携帯) FAX：03-6416-9997
 E-Mail：pr@cscloud.co.jp

■ 2023年7月～9月と比較してSQLインジェクションが約6,400万件増加



SQL インジェクションとは、外部からの入力を元に SQL 文を動的に作成するサイトやアプリケーションで、意図しない外部入力により悪意のある SQL 文を注入されることによって、不正にデータベースのデータが読み取られたり、データが改ざんまたは削除されたりする攻撃のことです。SQL インジェクションの脆弱性が悪用されると、外部からデータベースを操作され、その結果、データベースに記録されたデータの閲覧や盗難、変更、消去などが行われる可能性があります。2023年1月からの動向を見ると、SQL インジェクション攻撃の検知数が増加傾向にあることが確認できます。特に、検知数は一貫して右肩上がりが増加しており、直近3ヶ月ではその増加が顕著に現れています。

【本件に関するお問い合わせ】

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・川崎
 TEL：03-6416-9996 携帯：080-4583-2871(川崎携帯) FAX：03-6416-9997
 E-Mail：pr@cscloud.co.jp

■ 2024年のクレジットカード情報を伴う個人情報流出（10月11日時点）

※本データは 2024 年に企業から公表されたクレジットカード情報を伴う個人情報流出の事例を示していますが、流出自体は 2020 年末から 2021 年前半に仕掛けられた改ざんが原因となっているケースなども含まれています。

業種	件数	個人情報流出件数	クレジットカード流出件数
食品・飲料製造業	6件	178,319	117,460
飲食業	2件	107,959	69,365
卸売業	2件	69,781	33,641
小売業	4件	67,677	35,612
美容機器製造業	1件	65,520	4,748
IT・通信業	1件	21,398	1,432
農業	1件	14,933	5,069
アパレル製造業	2件	7,020	4,948
スポーツ業	1件	2,726	2,726

※流出の可能性も件数に含む。 サイバーセキュリティクラウド調べ（2024年10月11日時点）
©Cyber Security Cloud, Inc. 2024

2024年1月から10月11日時点までに、食品・飲料製造業が他の業種と比較して、被害件数が多いことが明らかになりました。これは、自社でオンラインストアなどのECサイトを運営し、クレジットカード情報を含む大量の顧客個人情報を取り扱っていることが背景にあり、攻撃のターゲットにされやすいと考えられます。

続いて飲食業、卸売業が流出件数が多く、特に飲食業ではクレジットカードの流出件数が目立っています。いずれも自社で運営しているオンラインストアでの流出が要因となり、クレジットカード情報を扱う機会が増えているため、被害が大きくなっていると考えられます。

また、すでに一部のシステムが侵害されている可能性も考慮に入れ、定期的な監視や検査を怠らないことが重要です。使用していないと思っている古いサーバやシステムにおいても、脆弱性を放置せず、バージョンアップやパッチ適用を忘れないように注意が必要です。たとえば、過去に報告されたPHPUnitの脆弱性が依然として狙われているケースが報告されており、こうした古い脆弱性が攻撃されるリスクが存在します。

【本件に関するお問い合わせ】

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・川崎
 TEL：03-6416-9996 携帯:080-4583-2871(川崎携帯)FAX：03-6416-9997
 E-Mail：pr@cscloud.co.jp

流出の規模や件数は業種によって異なりますが、業種を問わず情報流出が起きていることから、パッチ適用や脆弱性診断が求められます。特に、クレジットカード情報を取り扱う企業は、PCI DSS（クレジットカード業界のデータセキュリティ基準）準拠の確認を徹底し、顧客情報の保護を強化することが重要です。

■代表取締役 CTO 渡辺洋司からのコメント

2024年第3四半期のサイバー攻撃検知レポートでは、Webアプリケーションに対する攻撃が依然として高水準で発生しており、1日あたり約370万回という非常に多くの攻撃が観測されました。これは、デジタル化が進む社会において、サイバー攻撃が日常的な脅威であることを改めて浮き彫りにしています。

特に、SQLインジェクションの攻撃件数が昨年同時期と比較して大幅に増加している点は深刻です。SQLインジェクションは、データベースの不正操作やデータの流出につながるリスクが高いため、企業はこの脅威に対して徹底したセキュリティ対策を講じる必要があります。

注目すべきは、攻撃手法の高度化とターゲットの多様化です。特に、PHPUnitのようなフレームワークの古い脆弱性を狙った攻撃が増加しており、過去の脆弱性を放置しないことが何より重要です。システム管理者は、常に最新のセキュリティパッチを適用し、脆弱性診断や定期的な監視を行うことが求められています。

当社では、クラウド型WAF『攻撃遮断くん』や『WafCharm』を通じて、Webアプリケーションへの攻撃をリアルタイムで可視化・遮断するだけでなく、脆弱性情報収集・管理ツール『SIDfm』を活用し、顧客の安全性を強化するソリューションを提供しております。今後も、サイバーセキュリティの最前線でお客様を守るため、技術力の向上とサービスの充実に努め、さらに高度なセキュリティ対策を推進してまいります。

■株式会社サイバーセキュリティクラウドについて

住所：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>

「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」をミッションに掲げ、世界有数のサイバー脅威インテリジェンスを駆使したWebアプリケーションのセキュリティサービスを軸に、脆弱性情報収集・管理ツールやクラウド環境のフルマネージドセキュリティサービスを提供している日本発のセキュリティメーカーです。私たちはサイバーセキュリティにおけるグローバルカンパニーの1つとして、サイバーセキュリティに関する社会課題を解決し、社会への付加価値提供に貢献してまいります。

【本件に関するお問い合わせ】

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・川崎

TEL：03-6416-9996 携帯:080-4583-2871(川崎携帯)FAX：03-6416-9997

E-Mail：pr@cscloud.co.jp