【ニュースリリース】

2024 年　7 月　24 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

2024 年第 2 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」と「OpenSSH の脆弱性（CVE-2024-6387）に影響する製品」を発表

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 2 四半期(2024 年 4 月 1 日～6 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。また、脆弱性情報収集・管理ツール『SIDfm（エスアイディーエフエム）』の監視対象製品が OpenSSH の脆弱性（CVE-2024-6387）に関しての影響を受けるかについて調査した結果を合わせて公開します。

«レポートサマリー»

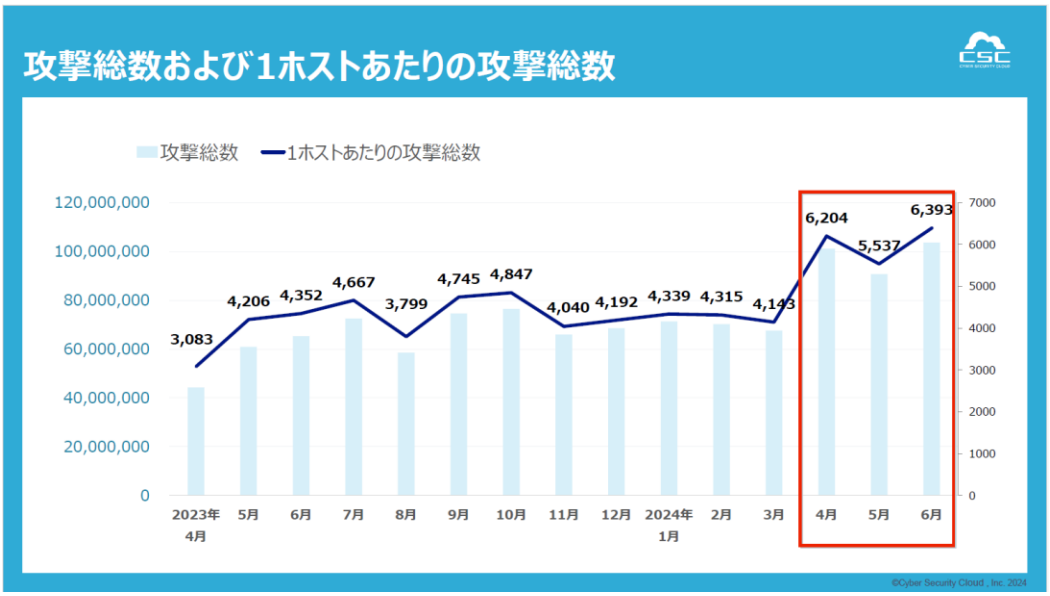
・1 日に約 320 万回のサイバー攻撃を検知

・SQL インジェクションが昨対比で 3200 万件増加

・PHPUnit の脆弱性を狙った攻撃が昨対比で 850 万件増加

・OpenSSH の脆弱性（CVE-2024-6387）の影響を受ける製品一覧の公開

■ **攻撃総数と推移：1 日に約 320 万回のサイバー攻撃を検知**



2024 年 4 月 1 日～6 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 295,539,852 件でした。これは、1 日に約 320 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 18,134 件でした。また、検知された攻撃数は前年同期比で+173%増加しており、ランサムウェアをはじめとするサイバー攻撃が増加の一途をたどっていることが明らかです。

(※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。

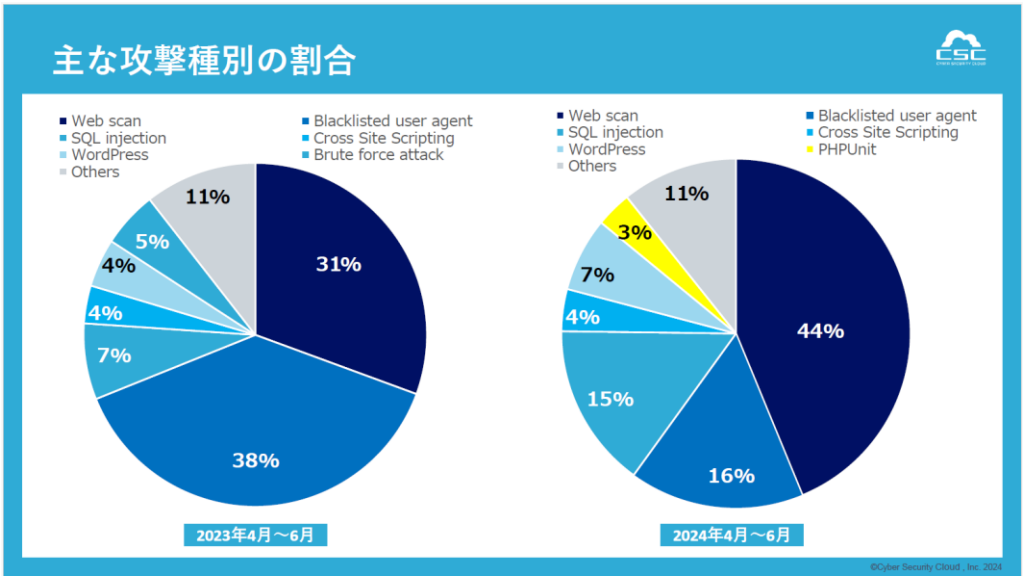
■**攻撃元国**

2024年4月～6月	国	前年同期比
1位	アメリカ	2位 ↑
2位	日本	1位 ↓
3位	イギリス	5位 ↑
4位	ドイツ	7位 ↑
5位	フランス	3位 ↓
6位	カナダ	6位 →
7位	シンガポール	8位 ↑
8位	中国	9位 ↑
9位	ロシア	4位 ↓
10位	インドネシア	41位 ↑

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

検知された攻撃元を国別に 2023 年同期比でみると、攻撃件数の上位は 1 位アメリカ、2 位日本、3 位イギリス、ドイツ、フランスと続いていました。
上位国についてはさほど変化はありませんが、2023 年 4 月～6 月で 41 位だったインドネシアが 10 位にランクインしています。

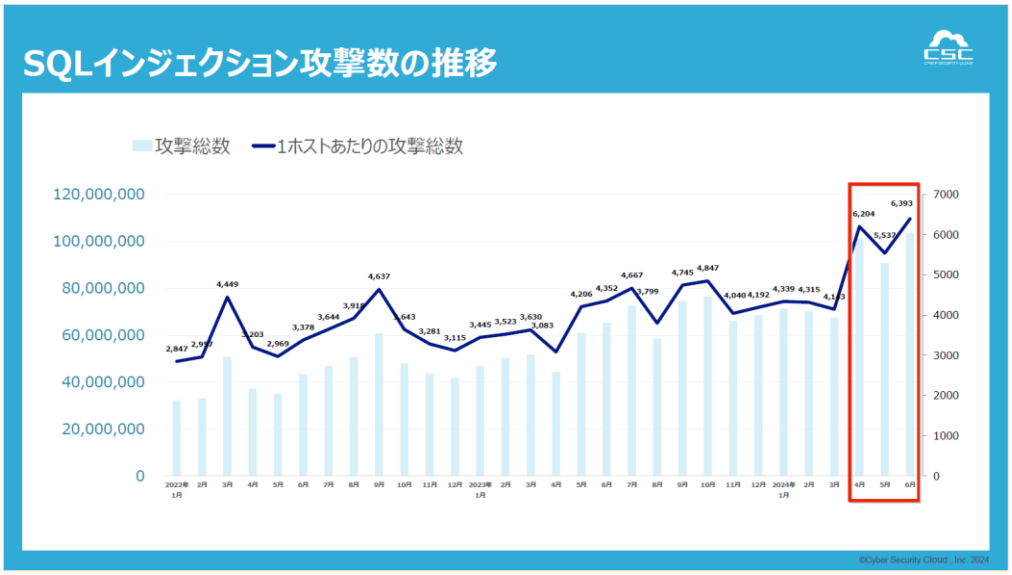
■主な攻撃種別



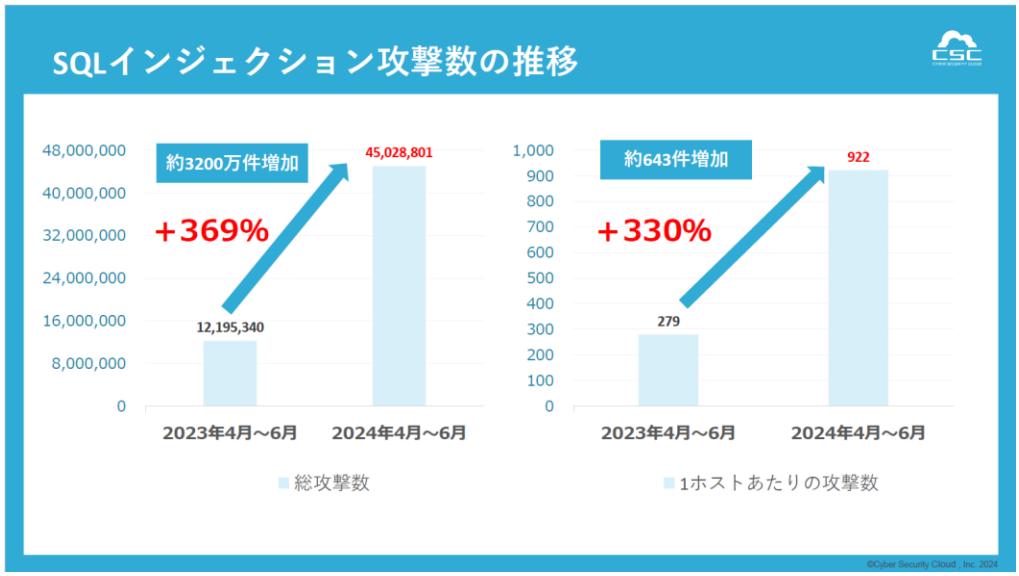
今回の調査期間における主な攻撃種別の攻撃状況を見ると、全体の総数は増加しているものの主だった傾向は 2023 年とさほど大きくは変わっていない状況です。最も多い攻撃種別は、攻撃の対象を探索・調査、また無作為に行われる単純な攻撃で脆弱性を探すなどの「攻撃の予兆」である「Web scan」が 44%を占めています。続いて脆弱性スキャンツールなどを利用した Bot による攻撃である「Blacklisted user agent」が全体の 16%を占めています。また、これまでランク外であった PHP のテストフレームワークである「PHPUnit」を狙った攻撃が増加していることが確認されました。

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

■2023 年 4 月～6 月と比較して SQL インジェクションが約 3200 万件増加



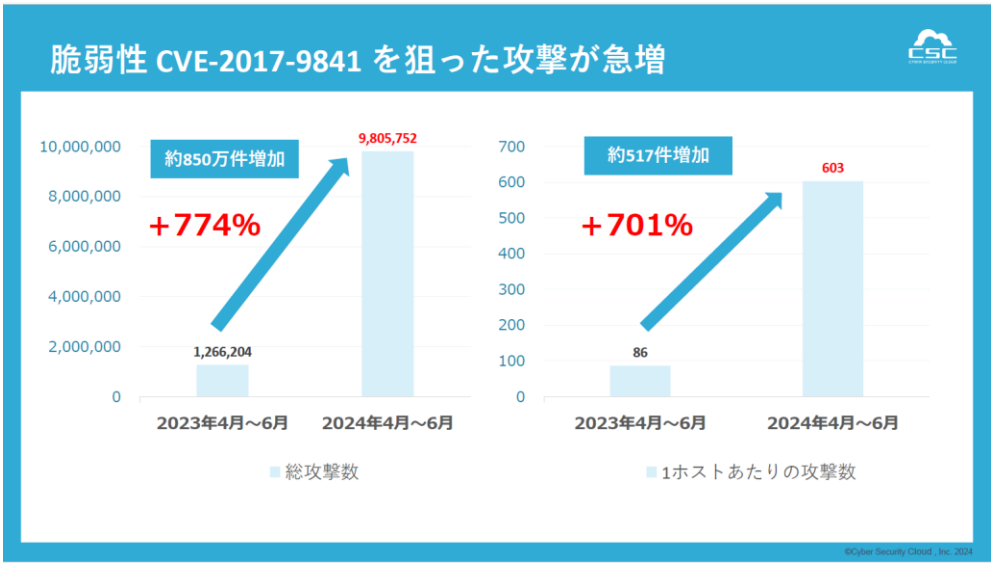
SQL インジェクションとは、外部からの入力を元に SQL 文を動的に作成するサイトやアプリケーションで、意図しない外部入力により悪意のある SQL 文を注入されることによって、不正にデータベースのデータが読み取られたり、データが改ざんまたは削除されたりする攻撃のことです。SQL インジェクションの脆弱性が悪用されると、外部からデータベースを操作され、その結果、データベースに記録されたデータの閲覧や盗難、変更、消去などが行われる可能性があります。2022 年 1 月からの動向を見ると、SQL インジェクション攻撃の検知数が増加傾向にあることが確認できます。特に、検知数は一貫して右肩上がりで増加しており、直近 3 ヶ月ではその増加が顕著に現れています。



2023 年 4 月～6 月と比較すると、総攻撃数で約 3200 万件もの攻撃件数増加が確認できました。

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

■2023 年４月～６月と比較して PHPUnit を狙った攻撃（CVE-2017-9841）が約 850 万件で 7 倍に増加



CVE-2017-9841 は、PHP の単体テストフレームワークである PHPUnit の特定バージョンに存在する脆弱性です。

PHPUnit の脆弱性を利用されると、攻撃者はリモートから任意の PHP コードを実行することができます。これにより、攻撃者は PHP コード経由で、サーバー上で広範囲の活動を行うことができる、危険な脆弱性です。

2023 年 4 月～6 月と比較すると、検知件数が約 850 万件増加しています。2017 年に公表された少し古い脆弱性であっても、攻撃者が依然として悪用を狙っていることが伺えます。

■OpenSSH の脆弱性（CVE-2024-6387）に影響する製品一覧を公開

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

regreSSHion と名付けられた OpenSSH の脆弱性（CVE-2024-6387）が一般公開されたことに伴い、7 月 2 日(火)に SIDfm においても脆弱性情報を登録・公開しました。これは OpenSSH サーバーの SIGALARM シグナルハンドラにおいて競合状態を引き起こすことが原因である脆弱性であり、この脆弱性を利用された場合、遠隔からシステムの制御を奪われる可能性があるものです。
OpenSSH サーバーは、機器の遠隔管理を行うにあたって広く使用されており、サーバーの他にもネットワークインフラを構成するファイアウォールやルータなどにおいても組み込まれた形で使用されており、この脆弱性の影響が懸念されています。

▼SIDfm の監視対象製品への影響一覧

https://sid-fm.com/blog/archive/entry/20240705.html

この度公開する一覧は、すでにアドバイザリが公開されているベンダーのみとなっております。今後ベンダーがアドバイザリ情報を公開・更新することによって、一覧の情報は追加・更新される可能性があります。最新情報は SIDfm ブログにて随時更新いたします。

■株式会社サイバーセキュリティクラウド 代表取締役 CTO 渡辺洋司コメント

2024 年第 2 四半期の「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」を発表しました。本レポートが示すデータは、テクノロジーの進化に伴い、サイバー脅威も高度化している現状を反映しています。特に SQL インジェクション攻撃や PHPUnit の脆弱性攻撃が増加していることは、企業にとって重大なセキュリティリスクとなります。

2024 年 4 月 1 日から 6 月 30 日までの間に、当社は 1 日に平均約 320 万件のサイバー攻撃を検知しています。特に、SQL インジェクション攻撃が昨対比で 3200 万件増加し、PHPUnit の脆弱性を狙った攻撃が 850 万件増加している点は、迅速かつ効果的な対策を講じる必要性があると考えています。

当社では、最新の技術を駆使してセキュリティソリューションの更新と強化を継続的に行っています。攻撃手法が日々進化する中で、我々もそれに対応して進化し続けることが求められています。Web サイト運営者にとって、セキュリティの最新動向や脅威に関する情報を継続的に収集し、適切な対策を施すことは極めて重要です。セキュリティ設定は一度行ったら終わりではなく、常に警戒し続け、更新を行うプロセスが必要です。適切なセキュリティ対策を実施することで、Web サイトを攻撃者から保護し、ユーザーの信頼を維持することが可能になります。

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

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