【ニュースリリース】

2025 年 2 月 10 日
株式会社サイバーセキュリティクラウド

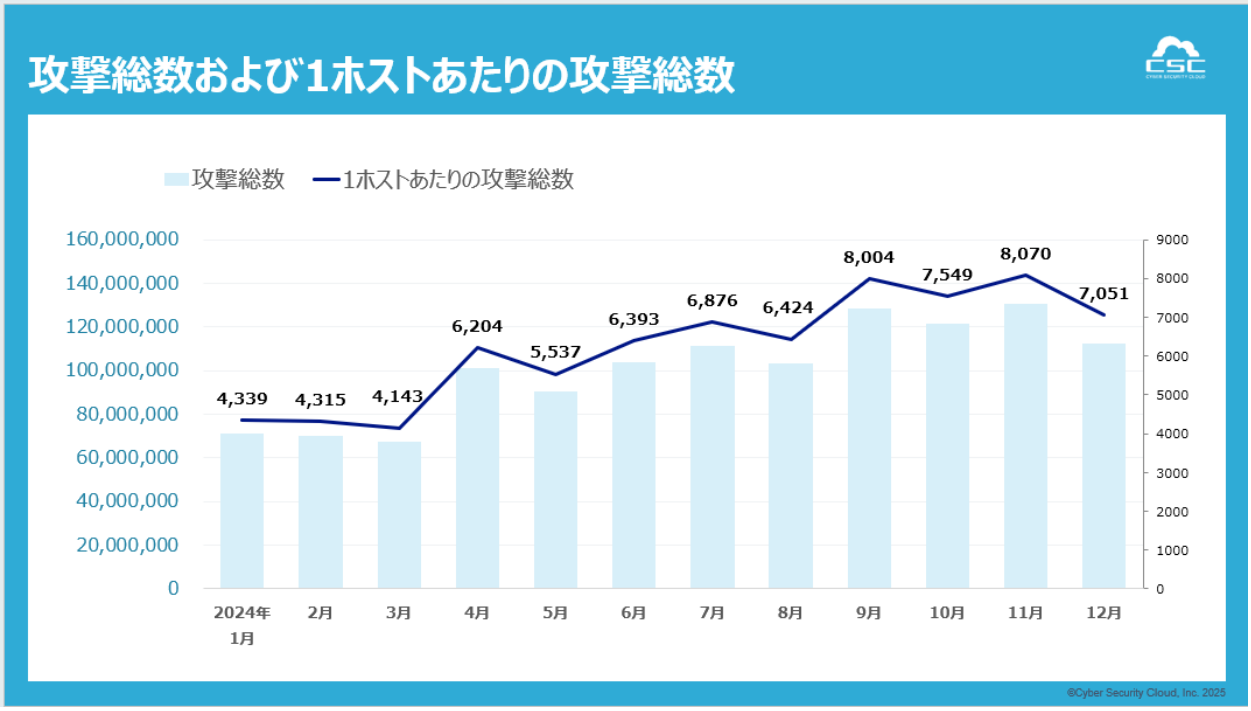
報道関係者各位

1 日に約 330 万回ものサイバー攻撃を検知
攻撃総数は前年比 154%に増加し過去最高を記録
2024 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

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 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）』『CSC AWS WAF Managed Rules』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。

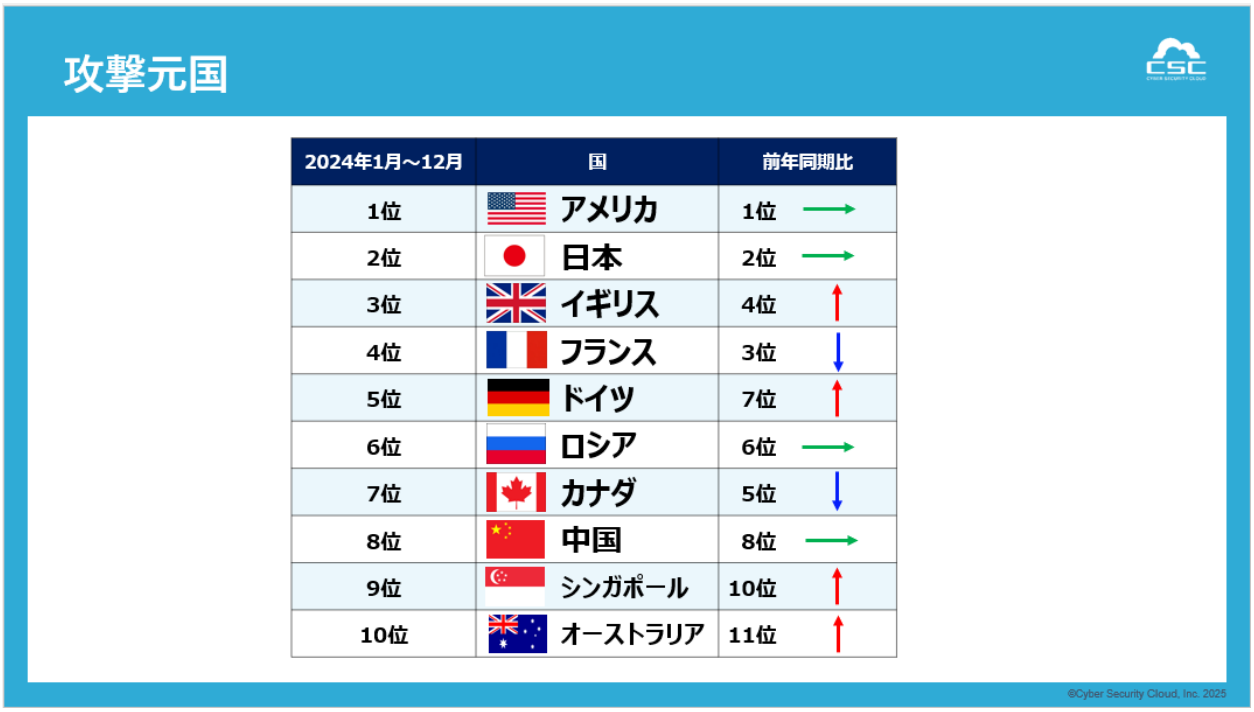
«レポートサマリー»
・1 日に約 330 万回のサイバー攻撃を検知
・SQL インジェクションを狙った攻撃数が約 1 億 4 千万件増加
・PHPUnit を狙った攻撃数が約 6,000 万件増加

■ 攻撃総数と推移：1 日に約 330 万回のサイバー攻撃を検知



2024 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攻撃数は 1,212,511,259 件でした。これは、1 日に約 330 万回の攻撃を受けている計算になります。また、1 ホスト（※1）あたりでは 1 年間に 74,905 件の攻撃が行われ、この攻撃回数は前年比で 154%に増加し、過去最高の数値となっています。（2020 年約 4.3 万件、2021 年約 4.2 万件、2022 年約 4.2 万件、2023 年約 4.8 万件）
（※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

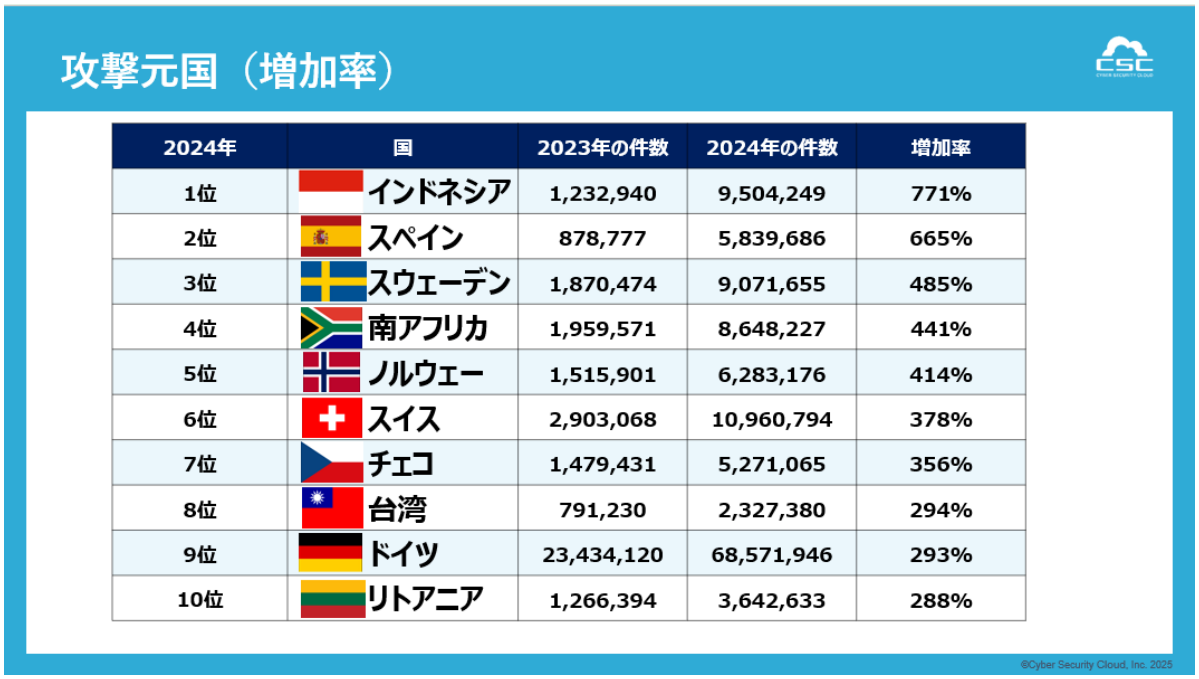


2024年1月～12月	国	前年同期比
1位	アメリカ	1位 →
2位	日本	2位 →
3位	イギリス	4位 ↑
4位	フランス	3位 ↓
5位	ドイツ	7位 ↑
6位	ロシア	6位 →
7位	カナダ	5位 ↓
8位	中国	8位 →
9位	シンガポール	10位 ↑
10位	オーストラリア	11位 ↑

検知された攻撃元を国別に 2023 年比較でみると、攻撃件数の上位は 1 位アメリカ、2 位日本、3 位イギリス、フランス、ドイツと続いていました。
前年 11 位だったオーストラリアが 10 位にランクインするなどの変動はあったものの、上位国の顔ぶれに大きな変化はありませんでした。

【報道関係者各位の問い合わせ先】
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　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

■攻撃元国（増加率）



2024年	国	2023年の件数	2024年の件数	増加率
1位	インドネシア	1,232,940	9,504,249	771%
2位	スペイン	878,777	5,839,686	665%
3位	スウェーデン	1,870,474	9,071,655	485%
4位	南アフリカ	1,959,571	8,648,227	441%
5位	ノルウェー	1,515,901	6,283,176	414%
6位	スイス	2,903,068	10,960,794	378%
7位	チェコ	1,479,431	5,271,065	356%
8位	台湾	791,230	2,327,380	294%
9位	ドイツ	23,434,120	68,571,946	293%
10位	リトアニア	1,266,394	3,642,633	288%

さらに、攻撃元の国別増加率のランキングが上記になります。2024 年は、世界各国で大規模な選挙が実施される中、分散型サービス妨害攻撃（DDoS 攻撃）をはじめとするサイバー攻撃が頻発しました。インドネシアの大統領選挙、台湾の総統選挙、EU の欧州議会選挙などの重要な政治イベントが実施された国が、上記の表の増加率ランキングの多くを占めています。

独立行政法人情報処理推進機構（IPA）で発表された「情報セキュリティ 10 大脅威 2025」（※2）の調査によると、分散型サービス妨害攻撃（DDoS 攻撃）や、地政学的リスクに起因するサイバー攻撃が TOP10 にランクインしました。

DDoS 攻撃は、Web サイトやアプリのサービス停止を狙う攻撃です。攻撃側のコストは比較的低い一方で、重要インフラや企業の業務継続性に重大な影響を及ぼす可能性があります。
2024 年の年末に観測された DDoS 攻撃の増加は、世界規模のボットネット活動と関連している可能性があり、多くの国で攻撃の頻度が高まったことが確認されています。

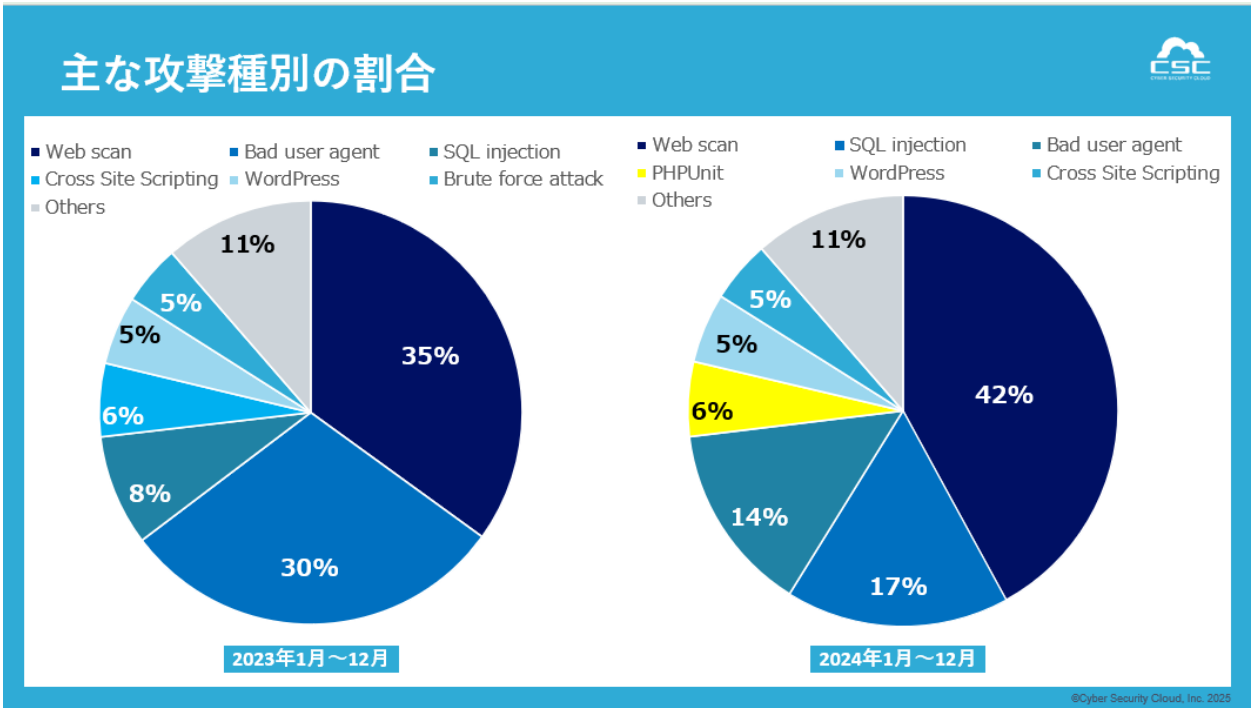
また、攻撃の発信元として特定の国が急激に増加している要因として、地政学的リスクの高まりとそれに伴うハッカー集団の活動の活発化が挙げられます。選挙・国際紛争・経済制裁などの局面で、国内外のハッカー集団による攻撃が増えやすく、特に DDoS 攻撃や情報操作を目的としたサイバー攻撃が頻発する傾向にあります。

【報道関係者各位の問い合わせ先】
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　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

日本でも、衆議院選挙の期間中に政党ホームページが DDoS 攻撃を受けたことが報告され、選挙期間中は特にサイバー攻撃に気をつける必要があると言えます。

なお、本レポートで特定された攻撃元の国は、攻撃者がサーバーを中継点として利用するケースも考えられるため、攻撃の発信源を確定的に示すものではありません。

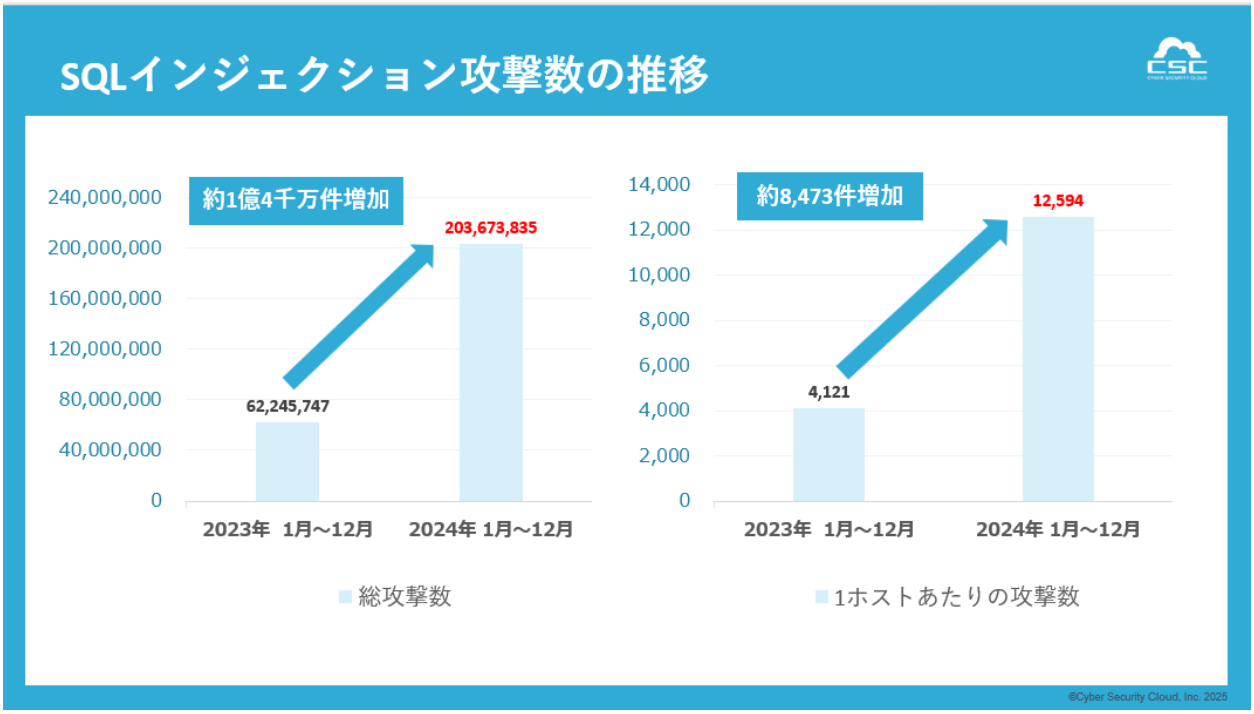
■ 主な攻撃種別



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 42%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 17%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、2024 年第 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。

【報道関係者各位の問い合わせ先】
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　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

■ **2023 年度と比較して SQL インジェクションを狙った攻撃数が約 1 億 4 千万件増加**



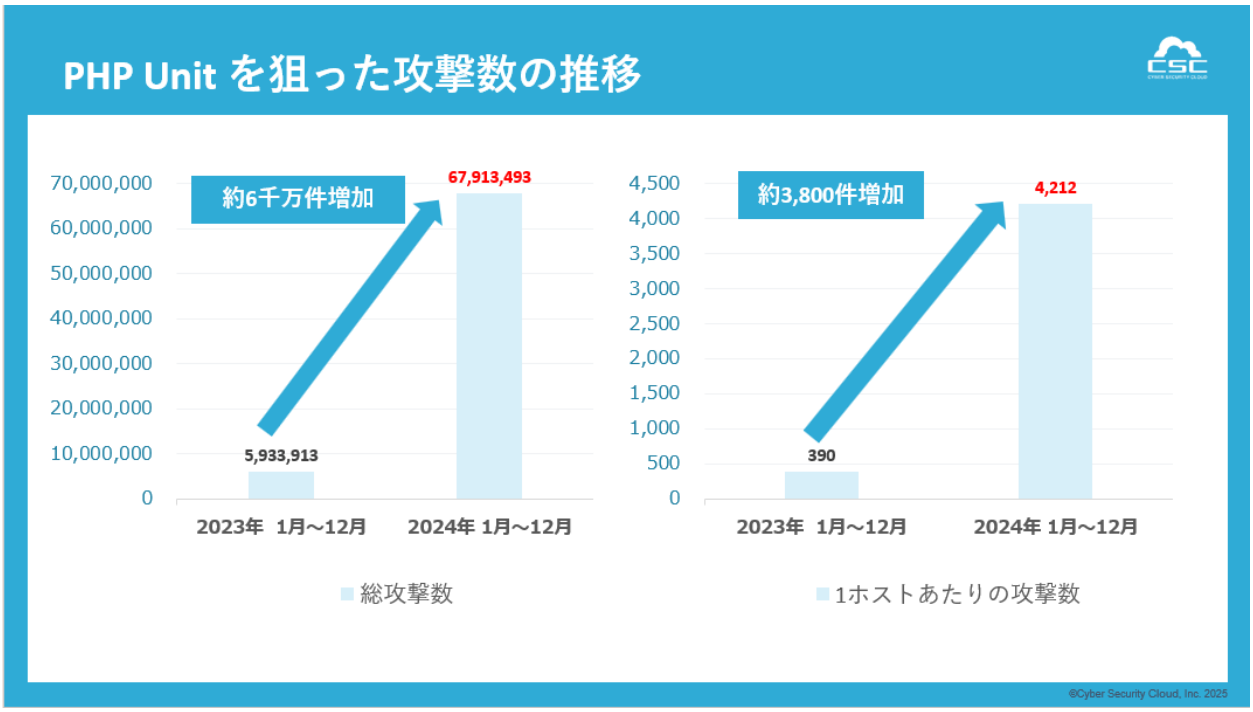
SQL インジェクションとは、外部からの入力を元に SQL 文を動的に生成するサイトやアプリケーションにおいて、意図しない外部入力によって悪意のある SQL 文を注入され、不正にデータベースのデータが閲覧、改ざん、削除される攻撃のことです。この脆弱性が悪用されると、攻撃者にデータベース操作を許してしまい、保存されているデータの閲覧や盗難、改変、削除といった被害が発生する恐れがあります。

2024 年には、エンドポイント管理ツールを提供する企業が攻撃の標的となった事例がありました。このソリューションは企業の IT 資産管理やエンドポイントデバイスの統合管理を支援するものですが、未修正の脆弱性や不適切な設定が実際に悪用され、管理権限の奪取やマルウェア感染が発生した事例が確認されています。そのため、適切な対策を講じない場合、同様のリスクにさらされる可能性があります。

また、ゼロデイ脆弱性の発見や既存の脆弱性を悪用した攻撃の継続が懸念されており、さらなる被害拡大が予想されます。利用者は、セキュリティアップデートを速やかに適用し、ベンダーの指示に従って不要な機能を無効化するなど、万全のセキュリティ対策を講じる必要があります。

【報道関係者各位の問い合わせ先】
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　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

■ **2023 年度と比較して PHPUnit を狙った攻撃数が約 6 千万件増加**



PHPUnit とは、 PHP プログラミング言語用の単体テストを行うためのフレームワークです。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 1 月～12 月と比較すると、検知件数が約 6 千万件増加しています。

■ **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**
この度発表された『Web アプリケーションへのサイバー攻撃検知レポート』は、私たちが直面しているサイバー攻撃の現状を浮き彫りにしています。2024 年 1 年間で、1 日に約 330 万回もの攻撃を検知したというデータは、Web アプリケーションを標的とした攻撃の深刻さと増加傾向を改めて示しています。前年比 154%増加という事実は、サイバー攻撃が進化し、規模を拡大していることを強調しています。

また、エンドポイント管理ツールを狙った攻撃が注目される中、企業が使用するソリューションの脆弱性を標的とした攻撃が増加している点も見逃せません。これらの攻撃は、単なるデータ流出にとどまらず、組織の運用停止やブランドへのダメージを引き起こす可能性があります。

私たちは、このような脅威に対処するため、定期的なセキュリティパッチの適用や、WAF（Web アプリケーションファイアウォール）を含む多層的な防御体制の構築を強く推奨します。

【報道関係者各位の問い合わせ先】
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　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

また、組織内でのセキュリティ意識の向上や、攻撃手法の変化に迅速に対応できる体制の整備が求められます。これからも当社は、最前線のセキュリティソリューションを提供し、お客様の安全な IT 環境の実現を支援してまいります。

（※）独立行政法人情報処理推進機構（IPA）の「情報セキュリティ 10 大脅威 2025」：
https://www.ipa.go.jp/security/10threats/10threats2025.html

■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。

【報道関係者各位の問い合わせ先】
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　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp