【ニュースリリース】

2024年3月29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

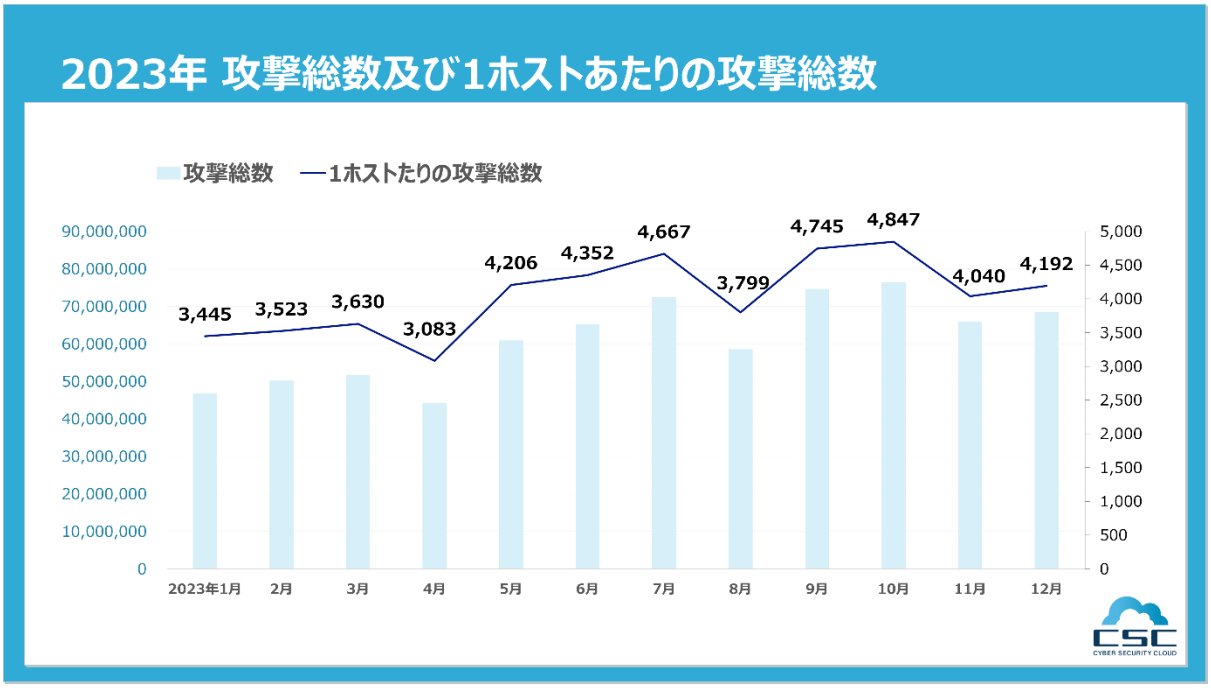
1秒間に23回ものサイバー攻撃を検知
2023年1月～12月の『Webアプリケーションへのサイバー攻撃検知レポート』を発表

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、2023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。

«レポートサマリー»

・1秒間に23回のサイバー攻撃を検知
・WordPressを狙った攻撃が増加

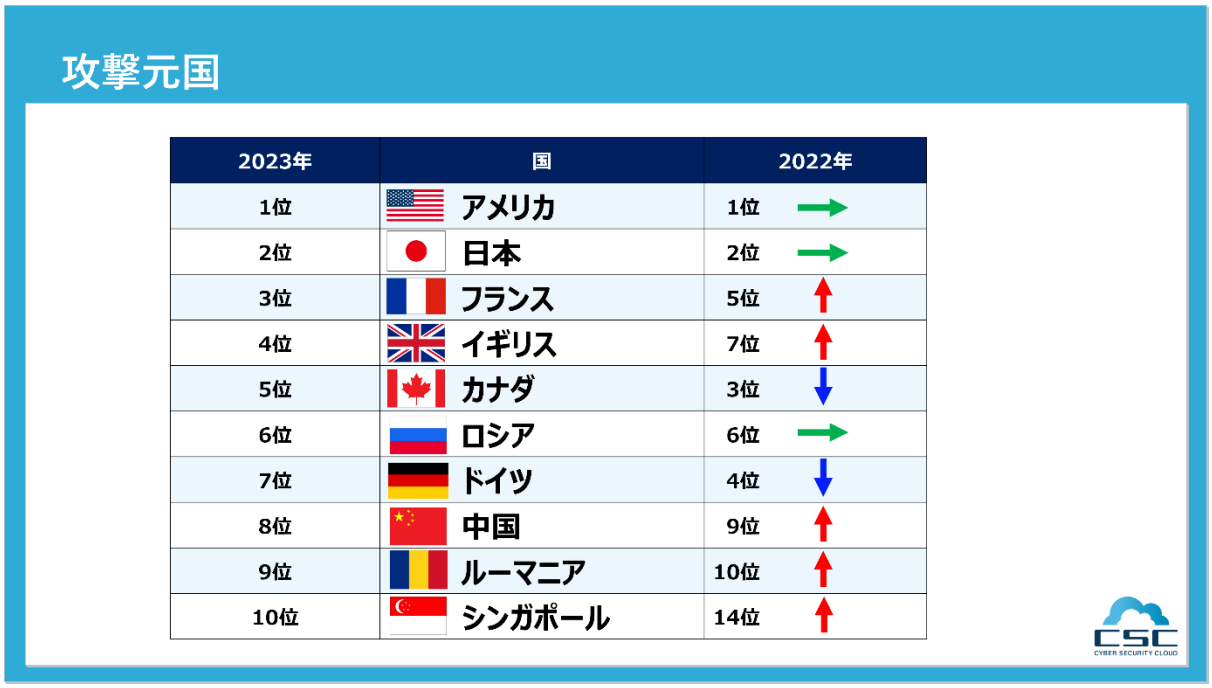
■ 攻撃総数と推移：1秒間に23回のサイバー攻撃を検知



2023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735,508,279件でした。これは、1秒間に23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48,527件の攻撃が行われ、この攻撃回数は過去3年間の記録（2020年約4.3万件、2021年約4.2万件、2022年約4.2万件）を大幅に上回り、過去最高の数値となっています。

※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。

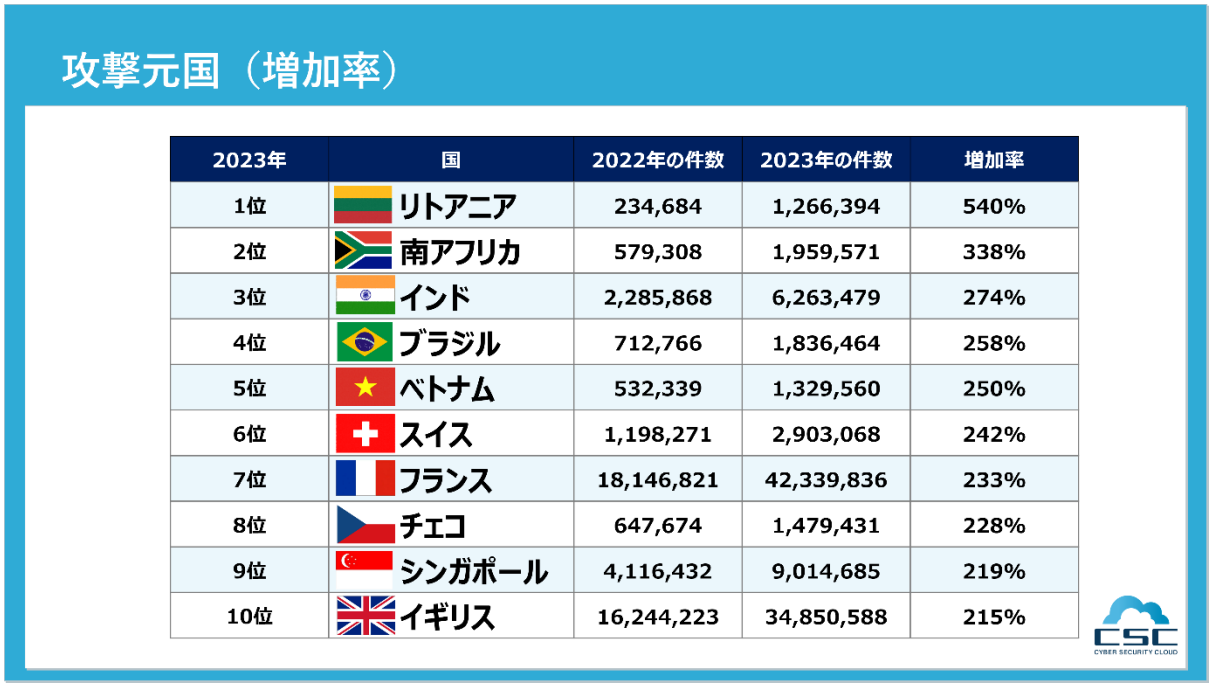
■ **攻撃元国**



2023年	国	2022年
1位	アメリカ	1位 →
2位	日本	2位 →
3位	フランス	5位 ↑
4位	イギリス	7位 ↑
5位	カナダ	3位 ↓
6位	ロシア	6位 →
7位	ドイツ	4位 ↓
8位	中国	9位 ↑
9位	ルーマニア	10位 ↑
10位	シンガポール	14位 ↑

検知された攻撃元を国別に2022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位フランス、イギリス、カナダと続いていました。
上位国についてはさほど変化はありませんが、前年14位だったシンガポールが10位にランクインしています。

■ **攻撃元国（増加率）**



2023年	国	2022年の件数	2023年の件数	増加率
1位	リトアニア	234,684	1,266,394	540%
2位	南アフリカ	579,308	1,959,571	338%
3位	インド	2,285,868	6,263,479	274%
4位	ブラジル	712,766	1,836,464	258%
5位	ベトナム	532,339	1,329,560	250%
6位	スイス	1,198,271	2,903,068	242%
7位	フランス	18,146,821	42,339,836	233%
8位	チェコ	647,674	1,479,431	228%
9位	シンガポール	4,116,432	9,014,685	219%
10位	イギリス	16,244,223	34,850,588	215%

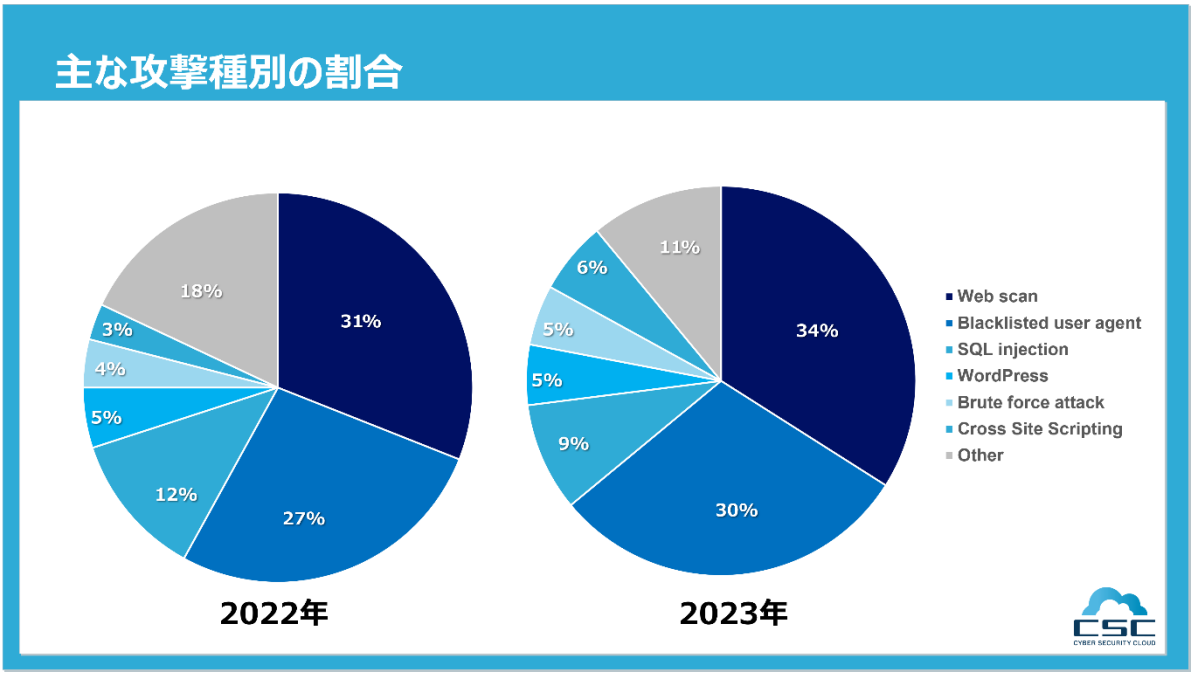
さらに、昨年に比べて攻撃数が増加している国のランキングでは、リトアニアが1位、南アフリカが2位、インドが3位、ブラジルが4位、ベトナムが5位となりました。サイバーセキュリティアドバイザリー※2の報告によると、連邦捜査局（FBI）、国家安全保障局（NSA）、米国サイバー司令部、および複数の国際機関は、ロシアの国家支援型サイバー攻撃グループが世界中で悪意ある活動を展開するためにUbiquiti EdgeRouters

【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

（エッジルーター）を使用していることを公表しました。これらの攻撃者は、侵害されたルーターを介して認証情報を収集し、ネットワークトラフィックを制御し、フィッシング詐欺用のページやツールを設置していることが明らかにされています。
いずれにしても、増加率の高い国はハッカー集団などからサイバー攻撃を受けたと報道される国が多く、中継地点として利用されている可能性や、ルーターが侵害されることにより、攻撃の踏み台として利用された結果、増加している可能性も考えられます。
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。

※2 出典：Russian cyber actors use compromised routers to Facilitate Cyber Operations . JOINT CYBERSECURITY ADVISORY. (2024, February 27). https://www.ic3.gov/Media/News/2024/240227.pdf

■ 攻撃種別：CMS※3を狙った攻撃が増加

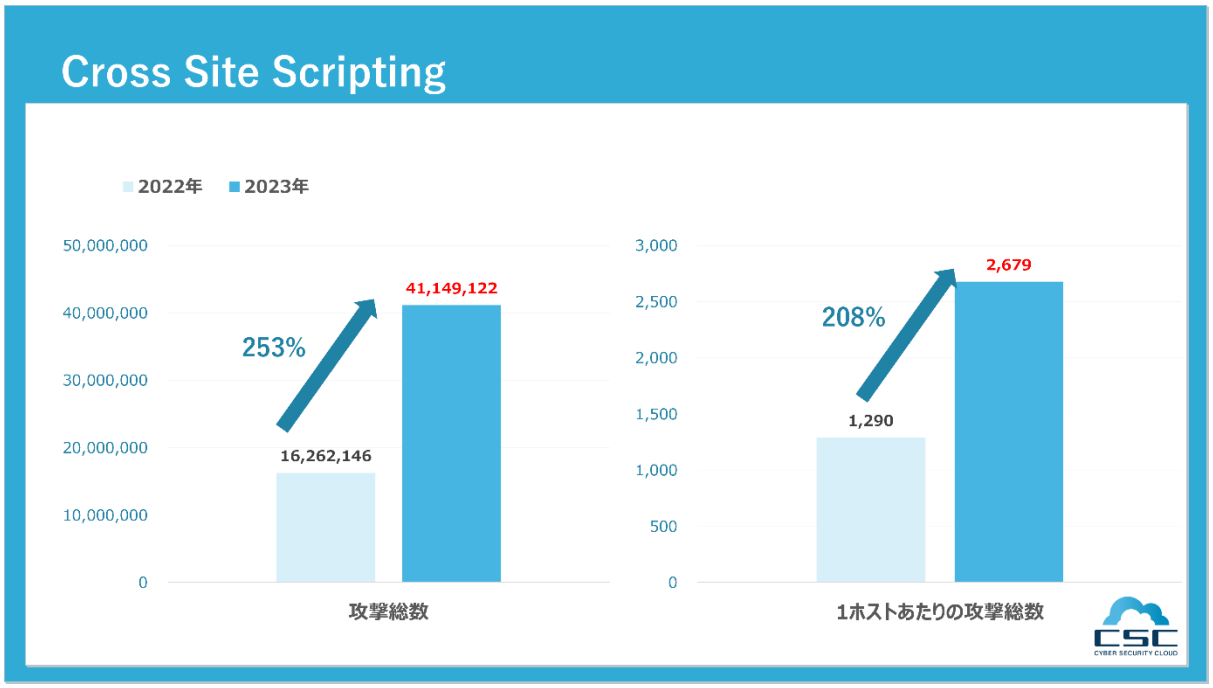


今回の調査期間における主な攻撃種別の攻撃状況を見ると、全体の総数は増加しているものの主だった傾向は2022年とさほど大きくは変わっていない状況です。最も多かったのは、攻撃の対象を探索・調査、また無作為に行われる単純な攻撃で脆弱性を探すなどの「攻撃の予兆」である「Web scan」が34%占め、続いて脆弱性スキャンツールなどを利用したBotによる攻撃である「Blacklisted user agent」が全体の30%を占めています。
なお、2023年第3四半期の調査レポートまでは、WordPressやMovable Typeなど約66種の攻撃を「Web attack」という表記で使用していましたが、本レポートからはより詳細な攻撃種類に分けて記載しています。

※3 CMSはコンテンツ・マネジメント・システムの略で、Webサイトの専門知識がなくとも更新や新規ページ制作ができるツールです。

【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

■ **Cross Site Scripting（クロスサイトスクリプティング）**

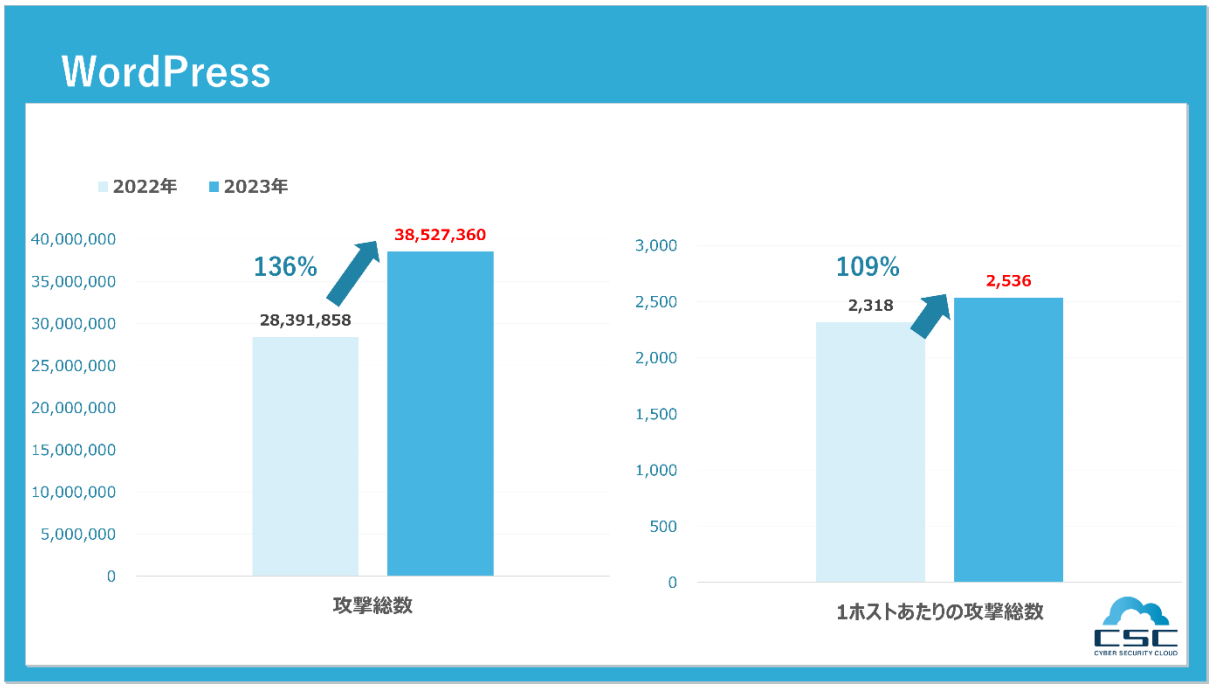


クロスサイトスクリプティング（XSS）とは、Webサイトの脆弱性を利用し、記述言語であるHTMLに悪質のあるスクリプトを埋め込む攻撃です。ユーザーの入力内容をもとにWebページを生成するサイトは、クロスサイトスクリプティングの攻撃対象になり得ます。例えば、Facebook、TwitterのようなWebアプリケーションや、アンケートサイトでの回答結果、サイト内検索での検索ワード、ブログや掲示板の記事やコメントなどです。サイトに設置されたフォームに攻撃者が用意したコードが埋め込まれた場合、ユーザーがそのフォームで情報を入力・送信するタイミングで、入力した情報に加えCookie情報や個人IDなども攻撃者に送られます。これにより攻撃者は、被害者のSNSアカウントを乗っ取ったり、被害者の権限で社内システムに侵入したりできます。

2022年1月～12月とで比較すると、2023年1月～12月のクロスサイトスクリプティングの攻撃総数は16,262,146件から41,149,122件とおよそ253%に増加していることが分かりました。1ホストあたりでは、1,290件から2,679件と前年比でおよそ208%に増加していました。

【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

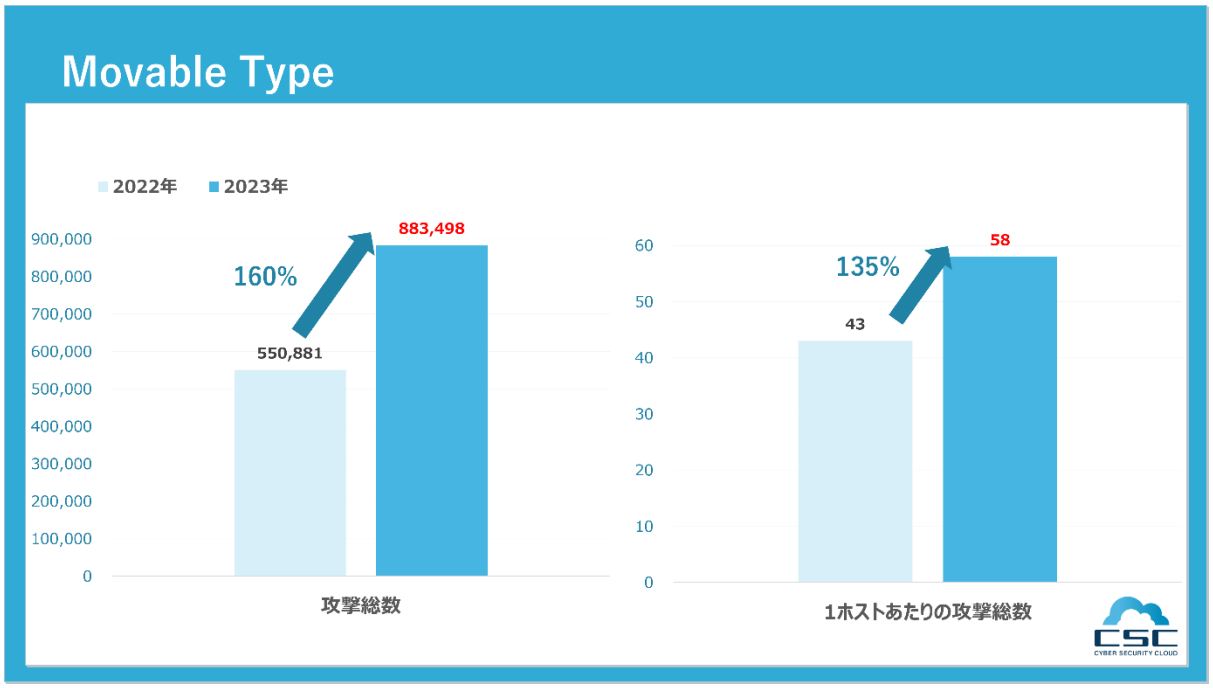
■WordPress（ワードプレス）



WordPress（ワードプレス）はPHPというプログラミング言語で作られているCMS（コンテンツ・マネジメント・システム）の一種で、ブログやWebサイトを簡単に作る事ができます。W3Techsの調査結果によると、WordPressはインターネット上の全Webサイト（独自コードで開発されたCMSも含む）の42%を占め、市場シェアは62%に達しています。

ユーザー数が多いことから、脆弱性が報告された場合に狙われるリスクが高い傾向にあります。またその使いやすさから、Webアプリやセキュリティの知識がなくても、Webサイトの運営が可能です。その結果、WordPressを狙った攻撃が頻発していると考えられます。

■Movable Type（ムーバブルタイプ）



【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

Movable Type（ムーバブルタイプ）はWordPressと並ぶ、代表的なCMSの一つとして知られています。当社が以前公開した「サイバー攻撃検知レポート2021」では、2021年10月20日に明らかにされたMovable
TypeのXMLRPC APIに存在する、リモートからの悪用が可能な脆弱性（CVE-2021-20837）への注意を呼びかけました。その後、2022年との比較で攻撃数が増加していることが確認され、2023年10月にはMovable Typeにおける新たな脆弱性として、クロスサイトスクリプティングの問題が公表されました。

■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

2023年には、総攻撃数が735,508,279件に達し、これは1秒あたり約23回の攻撃を受けていることを意味します。昨年、CMSを狙った攻撃の増加が顕著でした。この背景には、CMSが導入しやすく利用者も多いことが挙げられます。CMSを利用しているサイトを攻撃することは、単一のWebサイトを狙うよりも効率的であり、成功した場合、広範囲のユーザーに影響を及ぼす可能性があります。

このため、Webサイト運営者は、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が重要です。セキュリティ設定は一度行えば終わりではなく、常に警戒を怠らず更新を行う必要があるプロセスです。適切なセキュリティ対策を実施することで、攻撃者からWebサイトを保護し、ユーザーの信頼を保つことが可能になります。

■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/

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。

【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