【ニュースリリース】

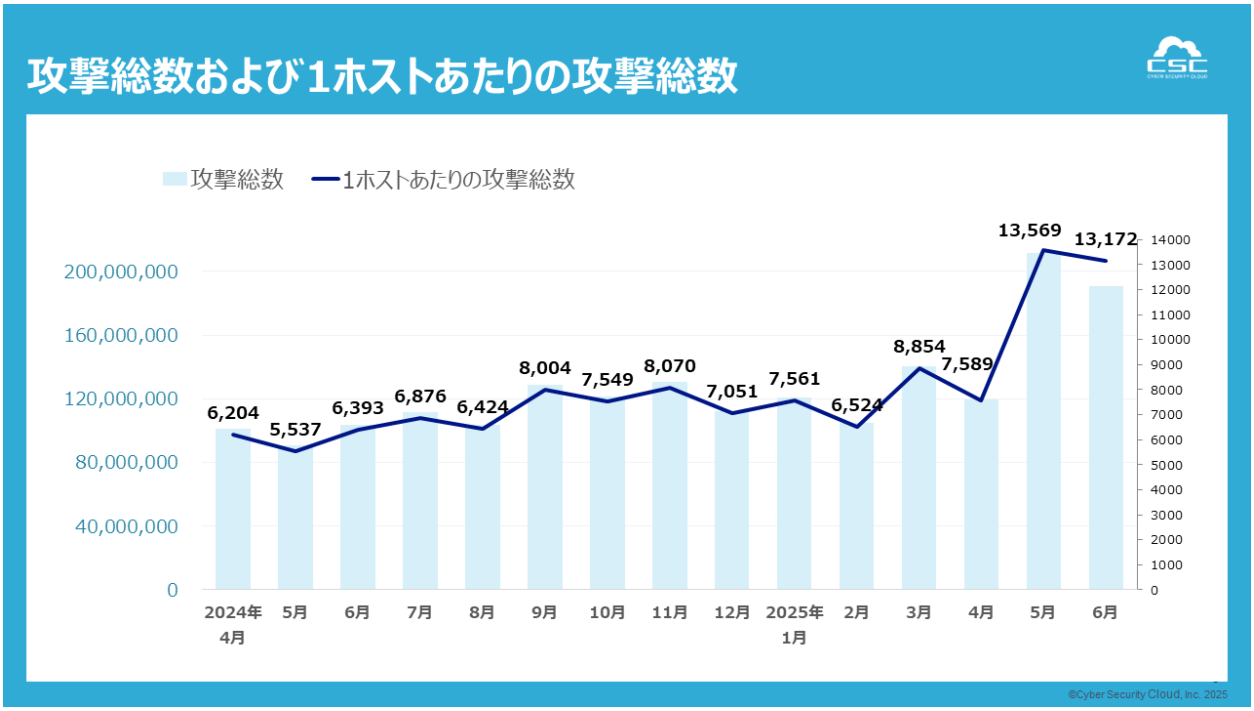
2025 年 8 月 21 日
株式会社サイバーセキュリティクラウド

報道関係者各位

5 月後半に攻撃急増　2Q で 5.26 億件･前年比 78%増を観測
2025 年 4 月～6 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、2025 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。

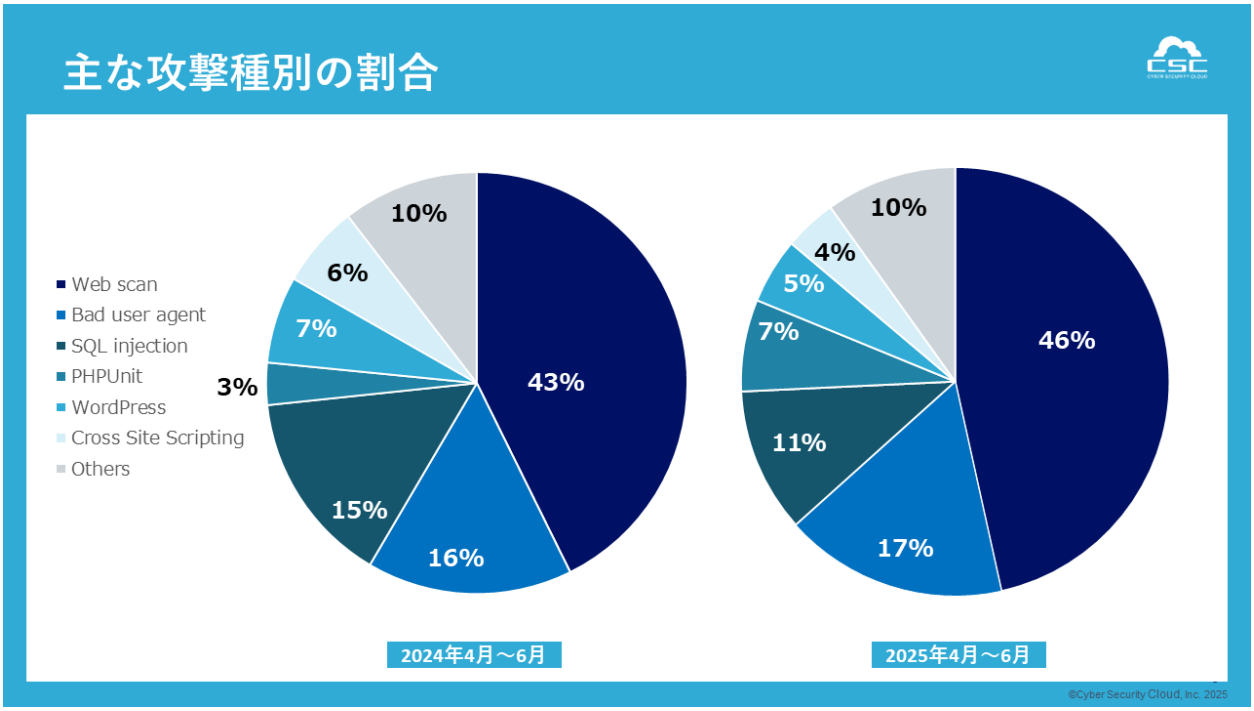
■ 全体概要：3 カ月で 5 億件超の攻撃を検知



2025 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 5 億 2654 万件（約 67 回/秒）にのぼり、前年同期比で 78%増となりました。
さらに、1 ホスト（※1）あたりの攻撃件数は前年同期比で約 2 倍に。

(※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。

■ **攻撃種別の割合**



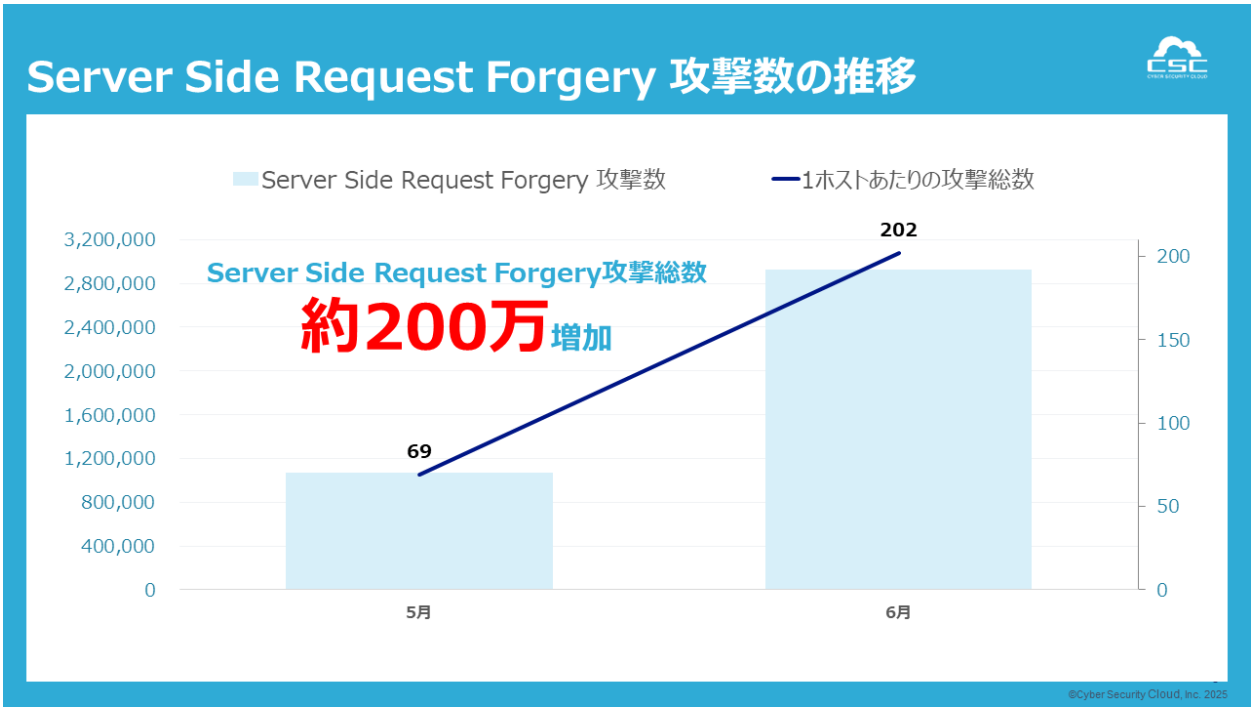
今回の調査期間における主な攻撃種別の傾向を見ると、総攻撃数は増加しましたが、種別構成に大きな変化は見られません。

本レポートでは、SQL インジェクション（SQLi）やクロスサイトスクリプティング（XSS）など、いわゆる「従来型の Web アプリケーション攻撃」が引き続き高頻度で観測されました。これらの攻撃手法は古典的である一方、攻撃の自動化や大規模化が進行しており、検知件数ベースでは過去最高水準に達しています。入力値の検証が不十分な Web アプリケーションや、設定ミス・アクセス制御の不備といった構成上の問題は、セキュリティホールとなるリスクがあり、攻撃の足掛かりとなる可能性があります。

さらに、WordPress や PHPUnit などのオープンソースソフトウェア（OSS）や CMS に内在する既知の脆弱性を狙った攻撃も多数確認されました。これらのソフトウェアは企業・自治体・個人を問わず広く利用されており、「誤った設定不備や脆弱性」が放置されたままになっている Web 資産が、攻撃者の格好の標的となっていると考えられます。

【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

■ **API 時代の新定番：Server Side Request Forgery が約 293 万件と 3 倍に増加。**



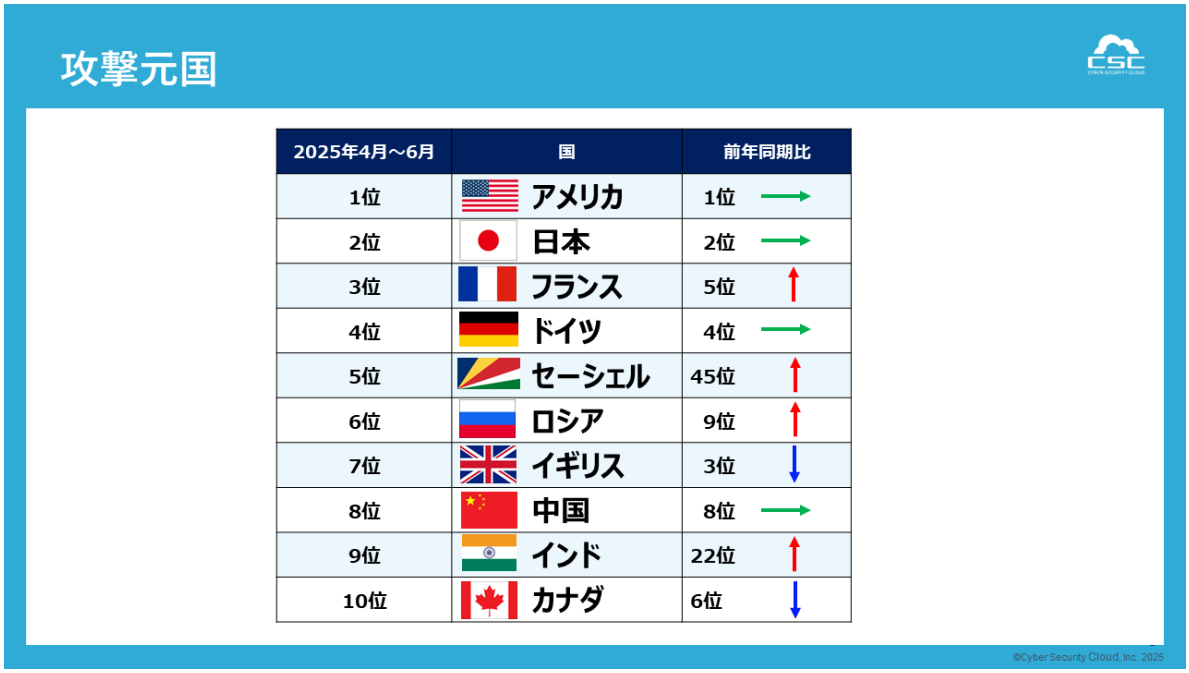
2025 年 6 月の Server Side Request Forgery 検知件数は、前月 5 月から約 200 万件増加しています。Server Side Request Forgery（サーバサイドリクエストフォージェリ）とは、サーバが本来アクセスしてはいけない場所や意図しないリソースへ、攻撃者がリクエストを送らせる攻撃手法です。
API ゲートウェイやクラウド IMDS 経由での内部アクセスが狙われ、境界外から内部資源への踏み台となる危険性が高まっていると考えられます。

Server Side Request Forgery は、件数・構成比ともに顕著な増加傾向を示しており、攻撃は主に API やクラウド連携の経路を狙って行われています。これにより、境界防御を回避して内部資源へ直接攻撃を仕掛けることが可能となる点が大きな脅威です。

対策としては、WAF による Server Side Request Forgery 検知ルールの適用、アウトバウンド通信（egress）の制御、クラウドメタデータサービスの保護が重要です。また、アプリケーション改修前であっても、仮想パッチ（例：WAF ルールによるアクセス遮断や、不正な URL スキームを含むリクエストのブロック）を適用することで、即日リスク軽減を実現することが可能です。

【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

■攻撃元国

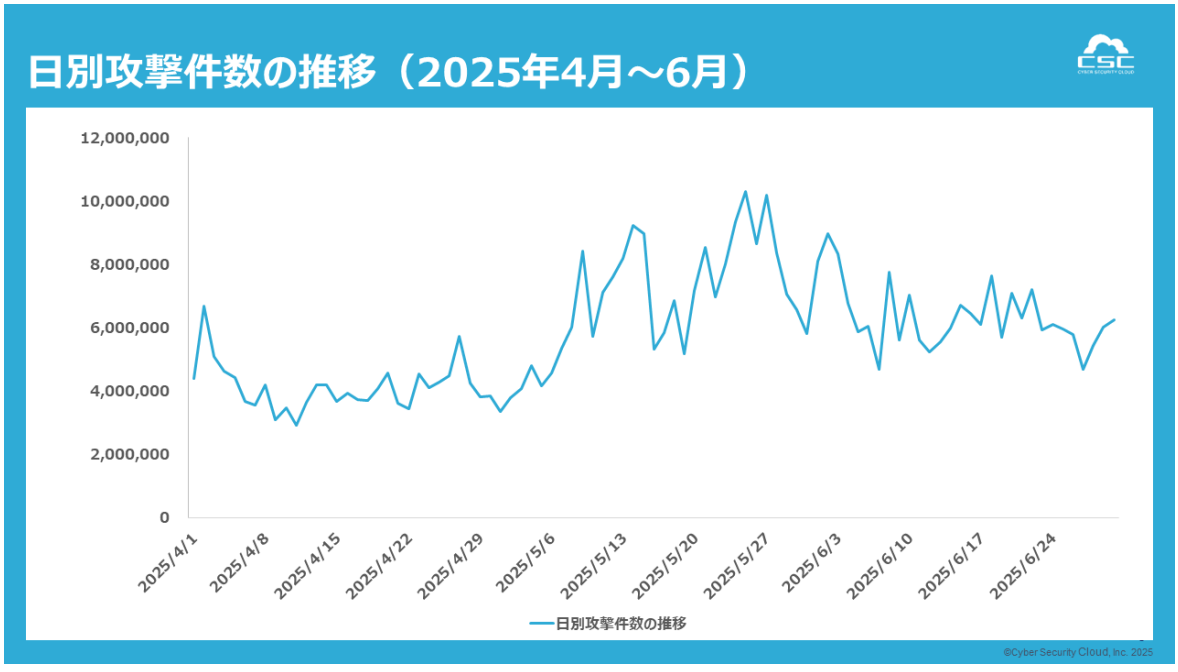


2025年4月～6月	国	前年同期比
1位	アメリカ	1位 →
2位	日本	2位 →
3位	フランス	5位 ↑
4位	ドイツ	4位 →
5位	セーシェル	45位 ↑
6位	ロシア	9位 ↑
7位	イギリス	3位 ↓
8位	中国	8位 →
9位	インド	22位 ↑
10位	カナダ	6位 ↓

検知された攻撃元を国別に 2024 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 位フランス、ドイツと続きました。

上位国についてはさほど変化はありませんが、2024 年 4 月～6 月で 45 位だったセーシェルが、今回の調査で 5 位に順位を大きく上げています。

■最も狙われた日は 5/25（1,029 万件）／5 月後半に連日の“1000 万件級”



【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

2025 年 5 月後半、攻撃トラフィックは一気に加速しました。ピークは 5 月 25 日の 1,029 万件で月間最多を記録し、この日を皮切りに 27 日にも 1,018 万件と“1000 万件級”が立て続けに観測されました。5 月後半全体で平均約 810 万件と前半を大きく上回り、2025 年で最も狙われた期間となりました。
これらの急増は、ボットネットを用いた自動スキャン型攻撃や、分散型サービス妨害（DoS/DDoS）攻撃の前兆である可能性が高いと考えられます。一定の条件を満たした対象に対して短期間に一斉アクセスを試みる動きが見られ、インフラ負荷や情報収集を目的とした行為が推察されます。

■4 月～6 月に攻撃が増加する要因

4 月～6 月は、運用体制・変更イベント・情報露出が同時多発的に重なる構造的にリスクが高い四半期です。当社の観測・分析から、以下の要因が複合的に作用していると考えられます。

長期休暇・連休の影響（監視の薄さ × 攻撃の活発化）

4 月～5 月は各地域で大型連休が重なり、運用監視や初動対応が相対的に手薄になりがちです。偵察（Web スキャン／Bad user UA）から実行段階（SQLi／SSRF 等）への移行が活発化し、5 月後半～6 月初旬にピークが立ちやすい傾向が当社観測でも繰り返し確認されています。

年初～2Q の「新規公開・構成変更」の集中

新年度・新予算の反映に伴い、新規サイトや新機能の公開、インフラ切替が 4 月～6 月に集中。初期設定ミスや既知 CVE の取りこぼしが発生しやすく、当社の検知でも Spring 系／SQLi は月末に強く、Traversal は月初に強いなど、リリース／調整タイミングと親和するパターンが見られます。

脆弱性公開・PoC 露出の時期的偏り

春～初夏はイベントや研究発表が重なり、脆弱性公開直後のスキャン波が発生しやすい季節です。6 月上旬の実行系スパイクはその典型で、一方で個別 CVE（KEV 等）との“同日相関”は強くなく、「露出増 × スキャンの一般化」により横断的に探索が拡散している可能性があります。

CMS／プラグイン／フレームワークの更新タイミング

WordPress や PHPUnit、Spring／Tomcat などエコシステムの更新に伴い、その周辺を狙うスキャンが 4 月～6 月に偏るケースがあります。実データでも PHPUnit／WordPress／SSRF／ServerSideCode 関連の検知が上位に定着しています。

以上を総合すると、4～6 月は「連休による監視の手薄化」「変更イベントの集中」「脆弱性情報の露出増」が重なり、短期間に高強度のスパイクが発生しやすい四半期といえます。対策として、連休前後のハードニング、月末の変更ゲーティング強化、公開直後の追加モニタリングを徹底し、件数だけでなく攻撃率で評価することが重要です。

【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

■ **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 洋司からのコメント**

今回の結果は、2Q に特有の構造的リスクが数値として可視化されたものと受け止めています。5 月後半のスパイクは、連休期の監視体制の薄まり、月末の変更集中、脆弱性情報の露出に、自動化された探索とスキャンの一般化が重なったことが背景にあると考えられます。

また、SSRF の急増は、API やクラウド連携が内部資産への入口となり得るリスクを改めて浮き彫りにしました。あわせて、SQLi や XSS などの従来型攻撃も引き続き高水準で観測されています。

これらを踏まえると、WAF での SSRF 検知適用、アウトバウンド通信管理や IMDS 保護、公開直後の追加モニタリング、月末の変更ガバナンス強化など、運用実態に即した対策の組み合わせが有効と考えます。また、件数だけでなく攻撃率に基づく評価や、ゼロデイ露出時の仮想パッチによる暫定対応から恒久対策への移行を通じて、スパイクの影響低減が期待できます。
当社は、実データに基づく知見の提供と製品機能のアップデートを継続し、安心・安全な Web 運用を支えてまいります。

■**株式会社サイバーセキュリティクラウドについて**

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
「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