【ニュースリリース】

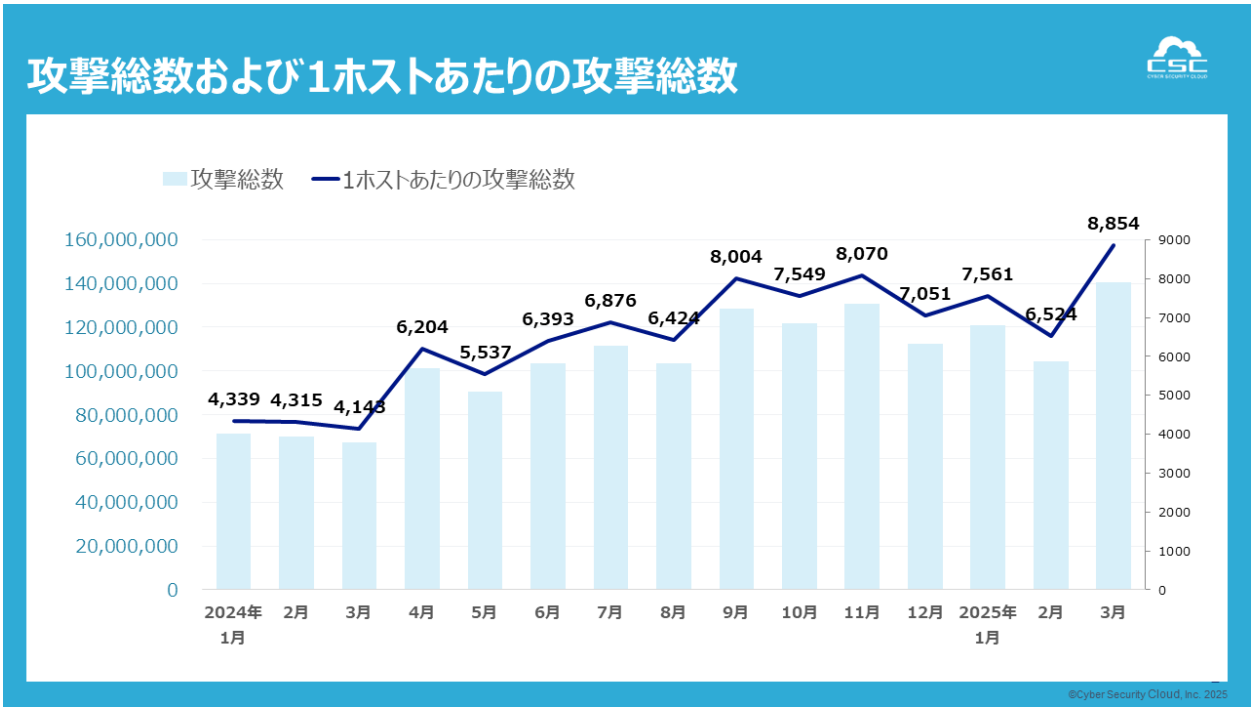
2025 年 5 月 2 日
株式会社サイバーセキュリティクラウド

報道関係者各位

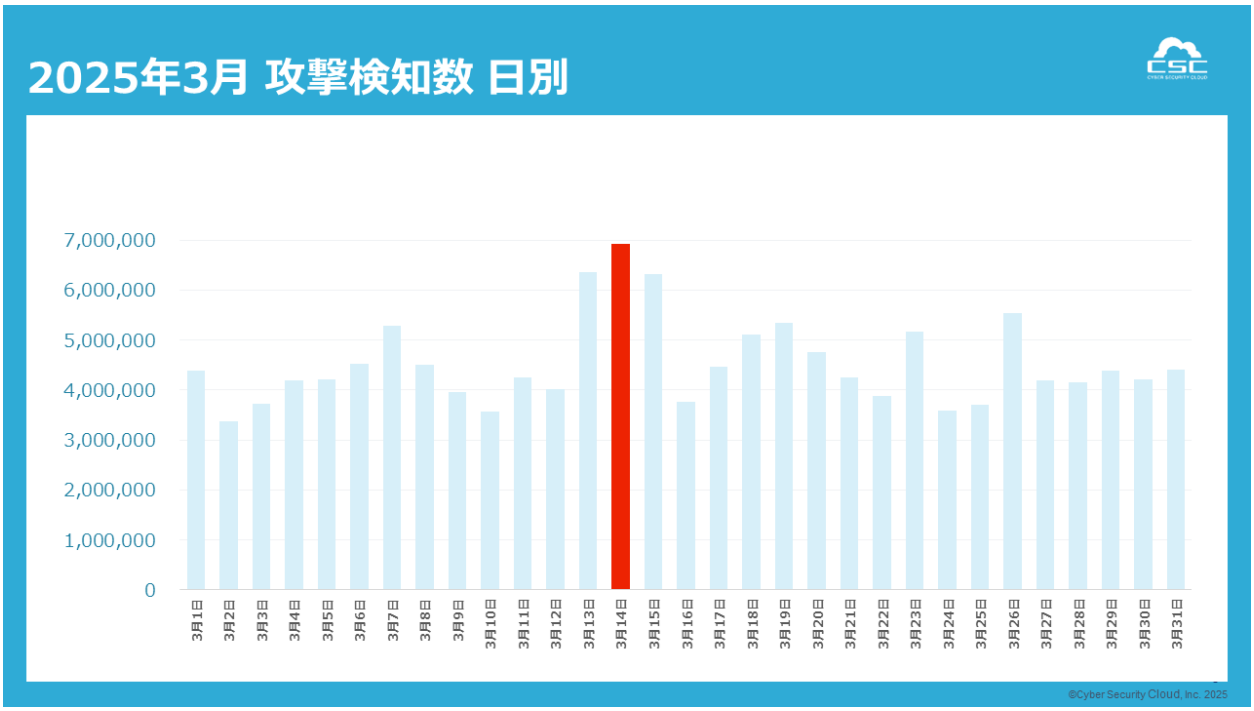
1 日で約 692 万件、1 秒あたり約 80 回のサイバー攻撃を観測
2025 年 1Q で最も狙われた日は“3 月 14 日”
2025 年 1 月～3 月の『Web アプリケーションへのサイバー攻撃検知レポート』を発表

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 1 月 1 日～3 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。

■攻撃総数と推移：3 か月間で 3 億 6,000 万回のサイバー攻撃を検知



2025 年 1 月 1 日~3 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 365,956,552 件でした。また、1 ホスト(※1)あたりでは 47,884 件でした。



また、調査期間中、最も攻撃件数が多かった日は 2025 年 3 月 14 日で、検知件数は 6,922,969 件にのぼりました。これは 1 秒あたりに換算すると約 80 回の攻撃が発生していた計算になります。
なお、前年 2024 年 1 月～3 月における 1 日平均の攻撃件数は約 2,298,029 件であり、3 月 14 日の攻撃件数はこれと比較して約 3 倍に相当する異常なスパイクであったことが明らかになっています。

2025 年 2 月から 3 月にかけて、サイバー攻撃の活動が活発化していました。2 月には、IoT ボットネット「Eleven11bot」を使った DDoS 攻撃が国内外で報告されるなど、ボットネットを利用した大規模攻撃が目立つ期間となっていました。

続く 3 月 10 日には、Web サーバー「Apache Tomcat」の新たな深刻なリモートコード実行（RCE）脆弱性（CVE-2025-24813）が公表されました。この脆弱性は、HTTP の PUT リクエストで不正なセッションファイルを書き込み、細工されたセッション ID で GET アクセスするという二段階の手口で、任意のコードを実行できる危険なものでした。脆弱性の公表直後には PoC（概念実証コード）が公開され、悪用リスクが急速に高まりました。

実際に 3 月 12 日には、ポーランドからこの脆弱性を悪用した初期攻撃が確認され、その後、脆弱性を狙ったスキャンや攻撃が世界中に急速に拡散しました。日本国内の Web サイトにもこの攻撃トラフィックが流入し、防御が不十分なサーバーに対して大量の HTTP リクエスト（PUT/GET 要求）が送信された結果、通常時の約 3 倍に及ぶアクセス増加が観測されています。

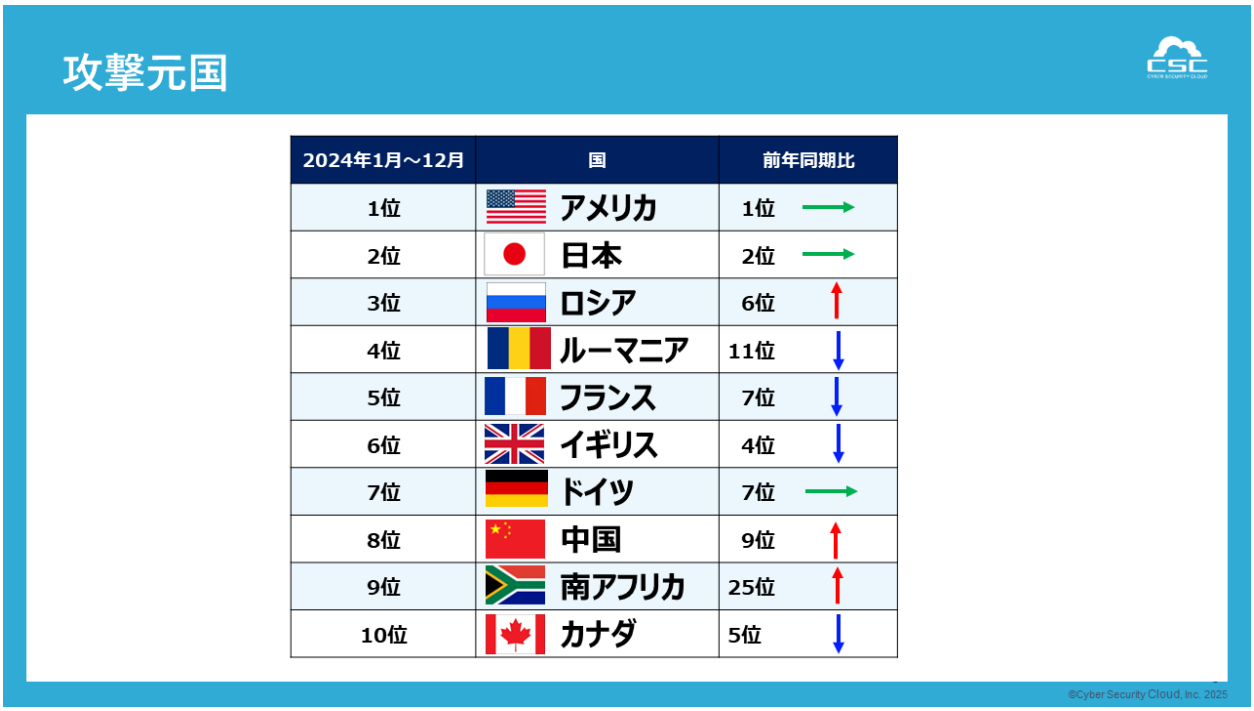
【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド　経営企画部　広報担当：竹谷・川﨑
TEL：03-6416-9996　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp

さらに、3 月 14 日には利用者が多い GitHub Actions である「changed-files」が、サイバー攻撃の被害を受けて一時的に乗っ取られるという、サプライチェーン攻撃が発生しました。この日は、バレンタインデーやホワイトデーといったイベントシーズンに合わせて不正注文の増加が見られるタイミングとも重なっており、複数要因が交錯する中で、特に攻撃件数が集中した可能性が考えられます。

以上のように、2 月から 3 月にかけて、ボットネットを使った攻撃、Apache Tomcat 脆弱性を悪用したキャンペーン、GitHub Actions 関連のインシデントなど、複数の脅威が連続して発生したことが、サイバー攻撃全体の急増につながったと考えられます。

(※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

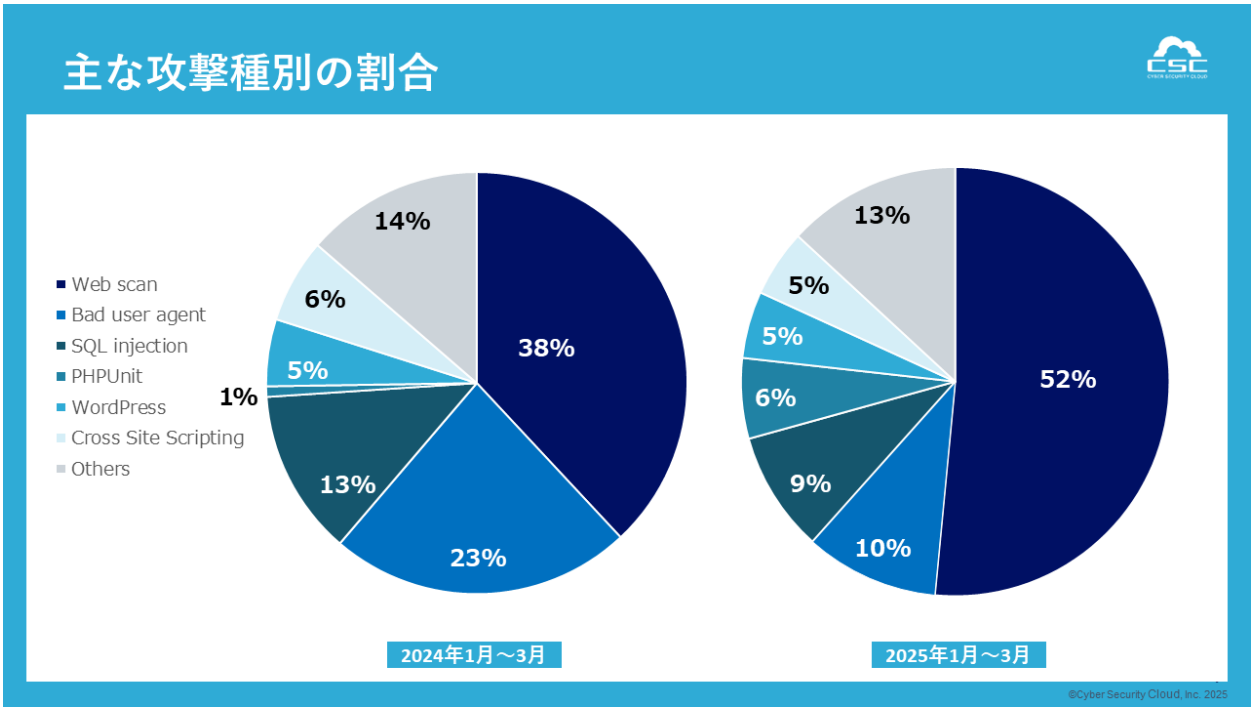


2024年1月～12月	国	前年同期比
1位	アメリカ	1位 →
2位	日本	2位 →
3位	ロシア	6位 ↑
4位	ルーマニア	11位 ↓
5位	フランス	7位 ↓
6位	イギリス	4位 ↓
7位	ドイツ	7位 →
8位	中国	9位 ↑
9位	南アフリカ	25位 ↑
10位	カナダ	5位 ↓

2025 年 Q1 の攻撃元国ランキングでは、例年通りアメリカ・日本・ロシアが上位を占めた一方で、前年同期では 25 位だった「南アフリカ」が 9 位に急浮上したことが確認されました。
また、ルーマニアも 11 位から 4 位にランクアップしており、これまでとは異なる地域からの攻撃が増加傾向にあることがうかがえます。

【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

■主な攻撃種別

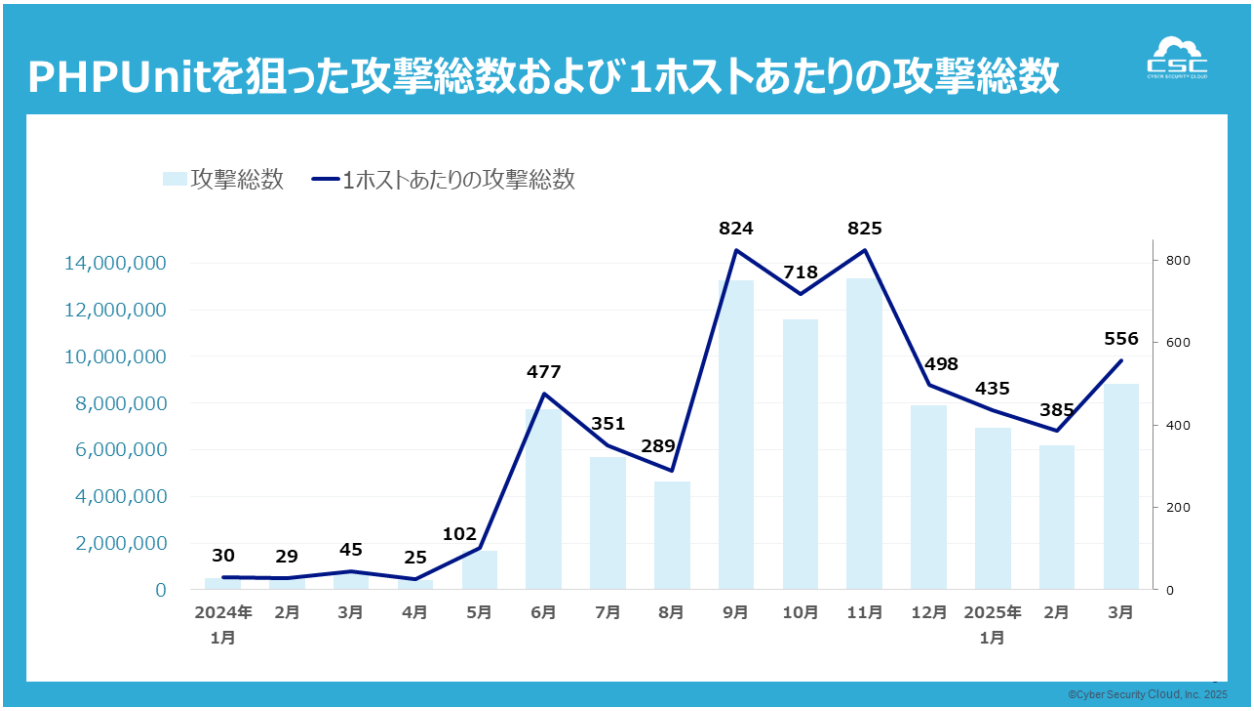


今回の調査期間における主な攻撃種別の攻撃状況を見ると、全体の総数は増加しているものの主だった傾向は 2024 年とさほど大きくは変わっていない状況です。最も多い攻撃種別は、攻撃の対象を探索・調査、また無作為に行われる単純な攻撃で脆弱性を探すなどの「攻撃の予兆」である「Web scan」が 52%を占めています。

この「Web scan」が多く観測されているという事実は、今後の本格的な侵害につながる“下準備”が、すでに多数の組織を対象に進行していることを示しています。Web スキャンは、特定の企業を狙い撃ちにするというよりも、無作為に広範囲なシステムや Web アプリケーションを調査し、既知の脆弱性を探す手法です。また、これらのスキャンはボットネットによる DDoS の標的探しに使われた可能性もあります。スキャンの過程で脆弱性が検出され、それが修正されずに放置されていた場合、攻撃者に悪用されるリスクは飛躍的に高まります。

【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

■「PHPUnit」への攻撃が前年から継続して増加



2023 年まであまり目立っていなかった、PHP アプリケーションのテストフレームワークである「PHPUnit」への攻撃が前年に引き続き増加傾向にあることが判明しました。

「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。

2024 年第 2 四半期に 850 万件超の攻撃増加が観測された後も、2025 年 1 月～3 月にかけてその攻撃数は高水準を維持。

■ **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**

2025 年第一四半期の観測データは、Web アプリケーションを取り巻く脅威の頻度、手口ともに、さらに高度化・複雑化している実態を浮き彫りにしました。

とりわけ、3 月 14 日に記録された 1 日あたり約 692 万件、1 秒あたり約 80 回という異常な攻撃スパイクは、通常時のおよそ 3 倍にあたり、短期間に集中して脆弱性探索や攻撃活動が行われたものと推測されます。

また、攻撃元国ランキングでは、これまで目立った動きのなかった南アフリカが 25 位から 9 位へと急上昇しており、攻撃インフラが特定の地域に依存せず、クラウドサービスや VPN を経由して地理的制約を回避する動きが加速していることがうかがえます。攻撃者は、クラウドサービスや VPN などの技術を活用することで地理的制約を回避し、従来は想定されていなかった国や地域を中継拠点として利用するケースが増加しています。

【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

特にロシアや中国が、アフリカなどのサイバーセキュリティが追いついていない地域で、アメリカやヨーロッパなど他国へサイバー攻撃するための足がかりとしたり、現地でサイバー犯罪者の育成を進めたりするなど、攻撃の隠れ蓑として利用しているという報告もあります。
こうした背景から、いまや「どこからの攻撃か」に加え「攻撃の土台がどう変化しているか」に注視すべき時代になってきています。
さらに、あまり注目されてこなかった PHP のテストフレームワーク「PHPUnit」への継続的な攻撃増加も警鐘を鳴らすべき事象です。本来テスト環境向けのツールが本番環境に残存し、セキュリティ対策の盲点となっているケースが目立ちます。このような“想定外の脆弱性”を狙う攻撃が、今後さらに拡大していくことが懸念されます。

私たちは、日々変化する脅威に迅速に対応できるよう、攻撃傾向の把握と異常兆候の早期検知体制をさらに強化し、企業のセキュリティリスク低減と安心できる Web 運営を支援してまいります。

■株式会社サイバーセキュリティクラウドについて
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