報道関係者各位

PRESS RELEASE

2026 年 2 月 26 日

株式会社サイバーセキュリティクラウド

1 日に約 554 万回、1 秒あたり約 64 回のサイバー攻撃を検知
～特定脆弱性を狙う集中型攻撃や公開直後の脆弱性悪用が顕在化～
2025 年『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～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»

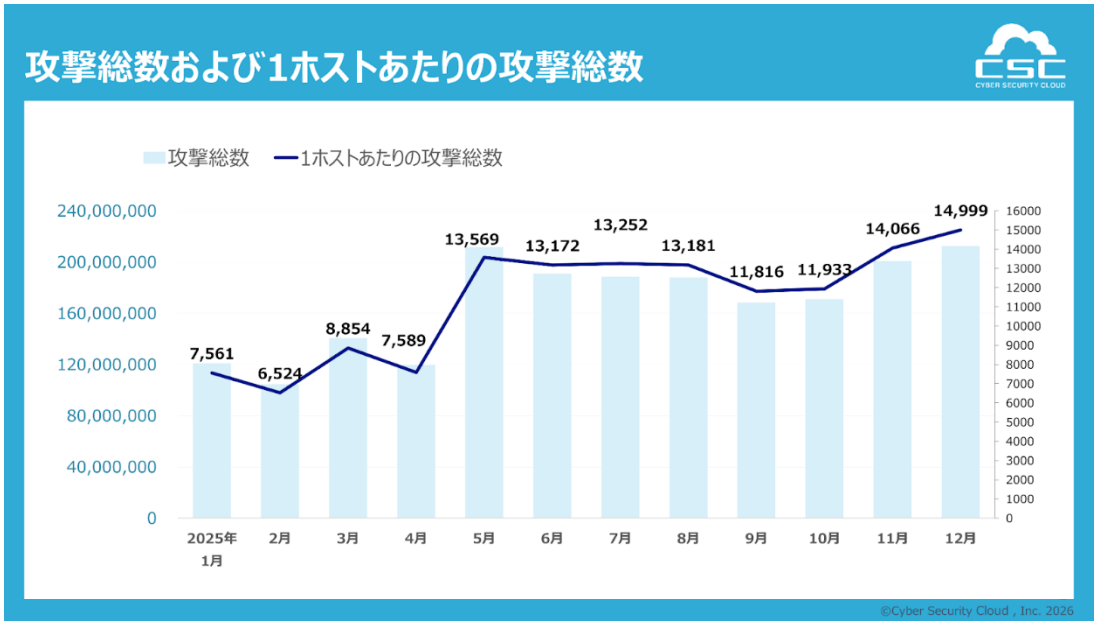
・2025 年の年間攻撃総数は **2,021,376,349 件（約 20.2 億件）**

・1 日あたり**約 554 万回**、1 秒あたり**約 64 回**のサイバー攻撃を検知

・特定脆弱性を狙うリクエスト傾向を複数回観測

・世界的に利用されるライブラリの脆弱性公開直後に攻撃増加を確認

■ 攻撃総数と推移：年間約 20.2 億件、1 秒あたり約 64 回の攻撃



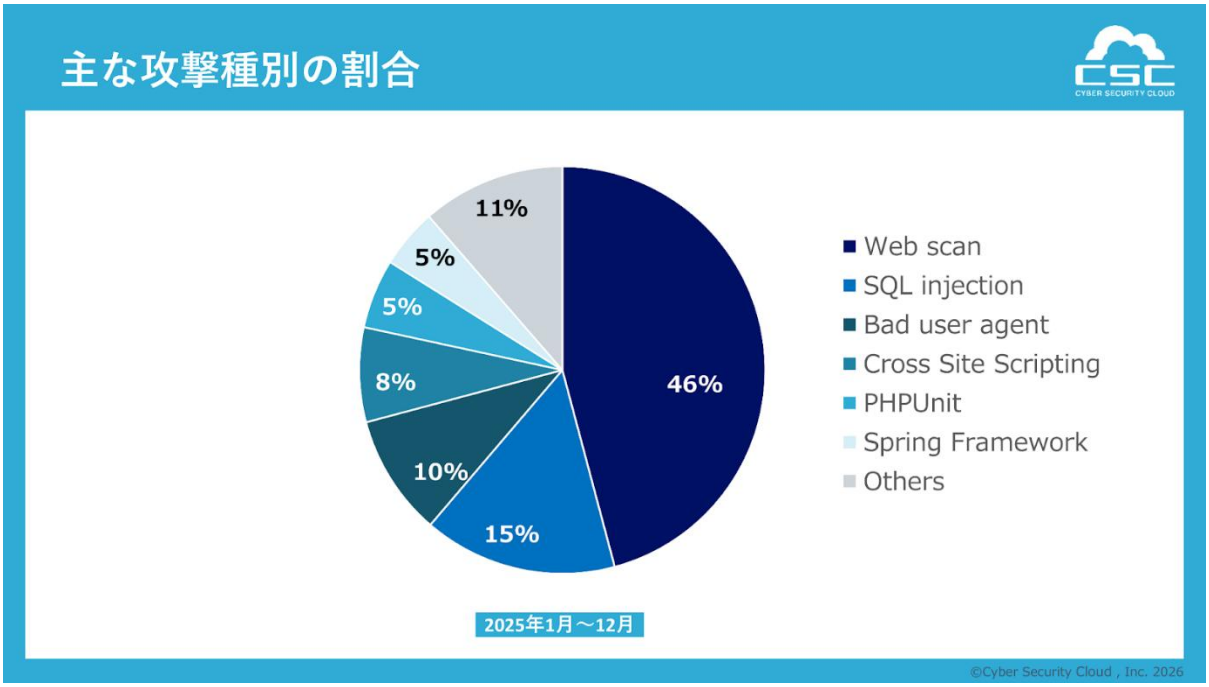
2025 年に検知した Web アプリケーションへのサイバー攻撃総数は **2,021,376,349 件（約 20.2 億件）**にのぼりました。これは 1 日あたり**約 5,538,017 回（約 554 万回）**、**1 秒あたり約 64 回** の攻撃が発生している計算になります。

また、1 ホスト（※1）あたりでは 1 年間に 136,516 件の攻撃が確認されました。。この攻撃回数は前年比で約 182%に増加しており、過去最高の水準となっています。（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、2024 年：約 7.5 万件、2025 年：約 13.6 万件）

攻撃は一過性の増加にとどまらず、継続的に高水準を維持しており、Web アプリケーションを取り巻く脅威環境は依然として厳しい状況にあります。攻撃は業種や企業規模を問わず観測されており、Web サービスを公開するすべての企業・組織にとって、常時対策が求められる状況です。

（※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。

■ 攻撃種別の構成比と傾向

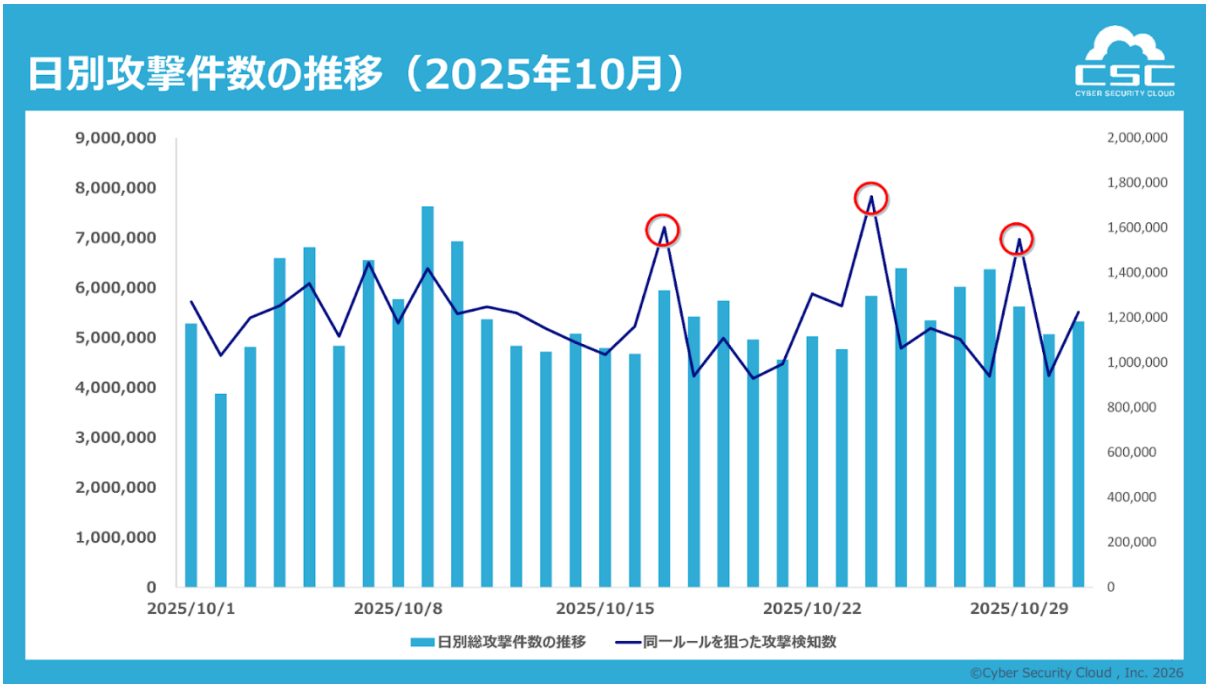


攻撃種別では、依然として Web スキャン（脆弱性探索行為）が最多を占めました。攻撃者は自動化ツールを用いて広範囲に探索を行い、公開された Web アプリケーションの弱点を探索し続けています。SQL インジェクションやディレクトリトラバーサルなどに関連する検知も一定数

確認されました。ただし、これらの検知には探索段階のリクエストも含まれており、実際の侵害行為と明確に区別できるものではありません。
無差別に広く探す動きと、特定の脆弱性に狙いを定める動きが併存していて、攻撃の効率化・自動化が進んでいる状況です。攻撃の効率化や自動化は、引き続き進行している状況です。

■ 2025 年 10 月～12 月に顕在化した攻撃傾向

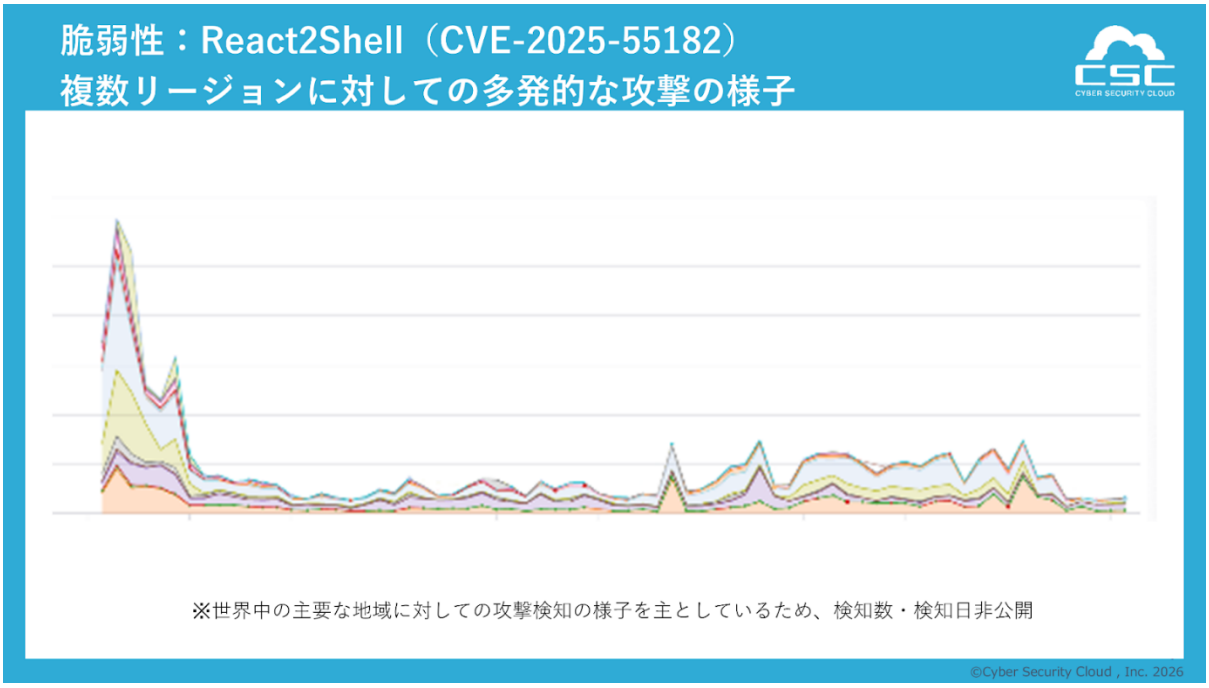
1. 特定の脆弱性を集中的に狙うリクエスト傾向の確認



2025 年 10 月～12 月には、特定の脆弱性に対して短時間に大量のリクエストが集中するリクエストの傾向が複数回観測されました。
特に 10 月には、日別総攻撃件数がおおむね 500 万件前後で推移する中、特定日において単一ルールを対象とした検知数が急増する事象が確認されました。
中旬および下旬には、同一ルールへの検知が通常水準を大きく上回る形で増加し、短時間に集中的なアクセスが発生している様子が見られました。これらは日次総数の増減とは異なる動きを示しており、広範囲を探索するスキャン型攻撃というよりも、特定の脆弱性を狙った集中的な試行であった可能性が考えられます。
12 月下旬には、日本時間未明の時間帯において、単一ルールに対し 1 時間あたり約 5 万件規模の攻撃が数時間継続。当日の検知数は約 40 万件規模に達しました。

これらの挙動は、広範囲に脆弱性を探索する従来型のスキャンとは様相が異なります。攻撃の背景や実行主体を特定するものではありませんが、特定の脆弱性を標的とした集中的な攻撃活動の可能性が示唆されます。

2. 主要ライブラリの脆弱性公開と連動する攻撃増加



2025 年 12 月には、世界的に広く利用されている JavaScript ライブラリ「React(リアクト)」に関連する重大な脆弱性情報が公開されました。

公開後、当社の観測環境においても当該脆弱性を狙う挙動が増加。攻撃は特定地域に限定されず、世界中の主要な地域に対して同時多発的に試行されました。脆弱性情報の公開直後から攻撃が活発化する傾向は年々強まっています。特に利用者の多い OSS や主要ライブラリは、公開直後から広範なスキャン対象となる傾向があり、迅速な情報把握と対策適用の重要性が、改めて示された事例といえます。

■ **攻撃元国の傾向**

攻撃発信元 IP を国別に分類したところ、米国が最多を占め、次いで日本、欧州諸国、アジア地域が続きました。

特に 2025 年は、インドが前年の 20 位から 8 位へと大きく順位を上げた点が特徴的です。

攻撃発信元 IP は必ずしも攻撃者の所在を示すものではありませんが、近年はボットネットやマルウェア感染端末を悪用した分散型攻撃が一般化していることが各種調査でも指摘されています。当社のクラウド型 WAF サービス『攻撃遮断くん』および『WafCharm』において観測された順位変動とあわせて考えると、感染端末の一部が踏み台やボットネットの一部として利用されている可能性も考えられます。

■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 洋司からのコメント

2025 年は、攻撃総数が高水準で推移する中、特定脆弱性を狙う集中型攻撃や、公開直後の脆弱性情報を即座に悪用する動きが顕在化しました。

これは、攻撃者が単に無差別に探索を行う段階から、技術動向や公開情報を踏まえて“効率的に狙いを定める”段階へ移行していることを示唆しています。攻撃の自動化・分業化が進み、インターネット全体が常時スキャンされ続ける環境となっています。

特に大規模 OSS や主要ライブラリの脆弱性は公開直後から世界規模で攻撃対象となります。企業には迅速な脆弱性把握と防御体制の継続的な最適化が不可欠です。

サイバー攻撃は一部の企業だけの問題ではなく、デジタル社会全体が直面する構造的な課題です。当社は今後も脅威インテリジェンスを活用した防御の高度化・自動化を推進し、安心してデジタルサービスを提供できる環境づくりに貢献してまいります。

株式会社サイバーセキュリティクラウド（https://www.cscloud.co.jp）
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
「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：川﨑
TEL：03-6416-9996　Mobile：080-4583-2871（川﨑）
FAX：03-6416-9997　E-Mail：pr@cscloud.co.jp