報道関係者各位

PRESS RELEASE　　2026年4月30日

株式会社サイバーセキュリティクラウド

1秒あたり最大160回の攻撃を観測

インフラ全体を狙う“無差別化”が顕在化

2026年1月～3月
『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

«レポートサマリー»

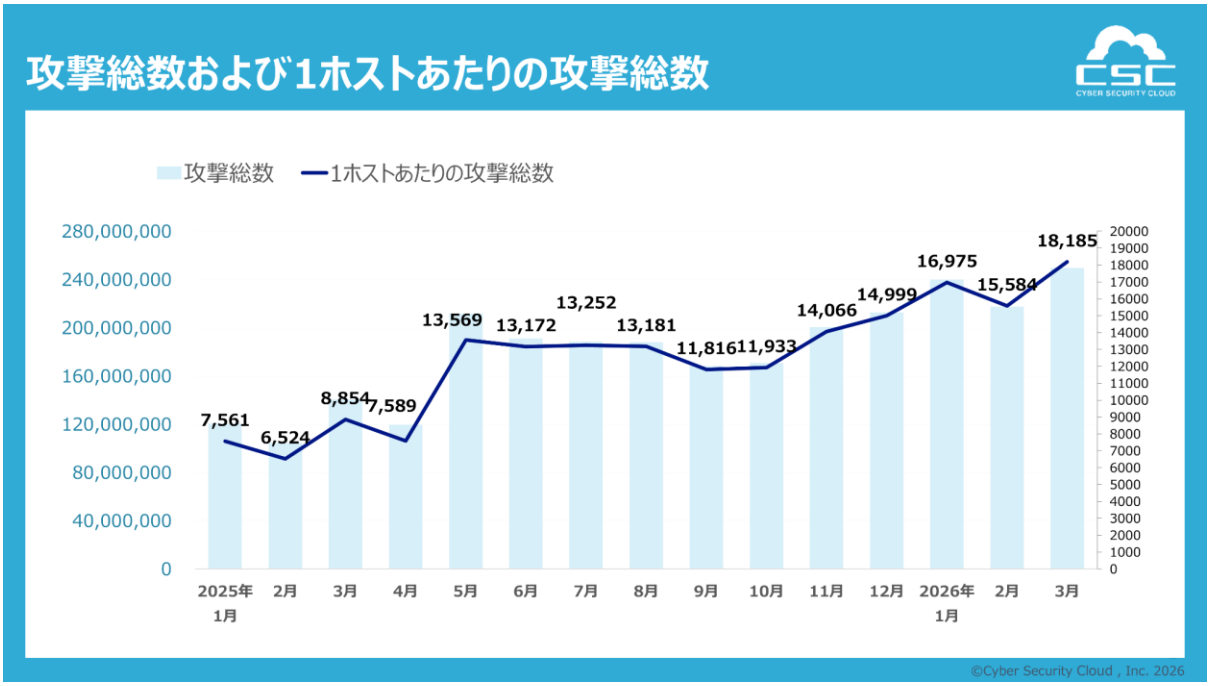
・サイバー攻撃は引き続き高水準で推移、最大で約1,300万件/日の瞬間的急増を観測

・攻撃密度が上昇。1ホストあたりの攻撃件数は前四半期最大約2倍に増加

・複数のデータセンターにまたがる無差別型DDoS攻撃を観測

・短時間・断続的に発生するDDoS攻撃が増加。

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、2026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。

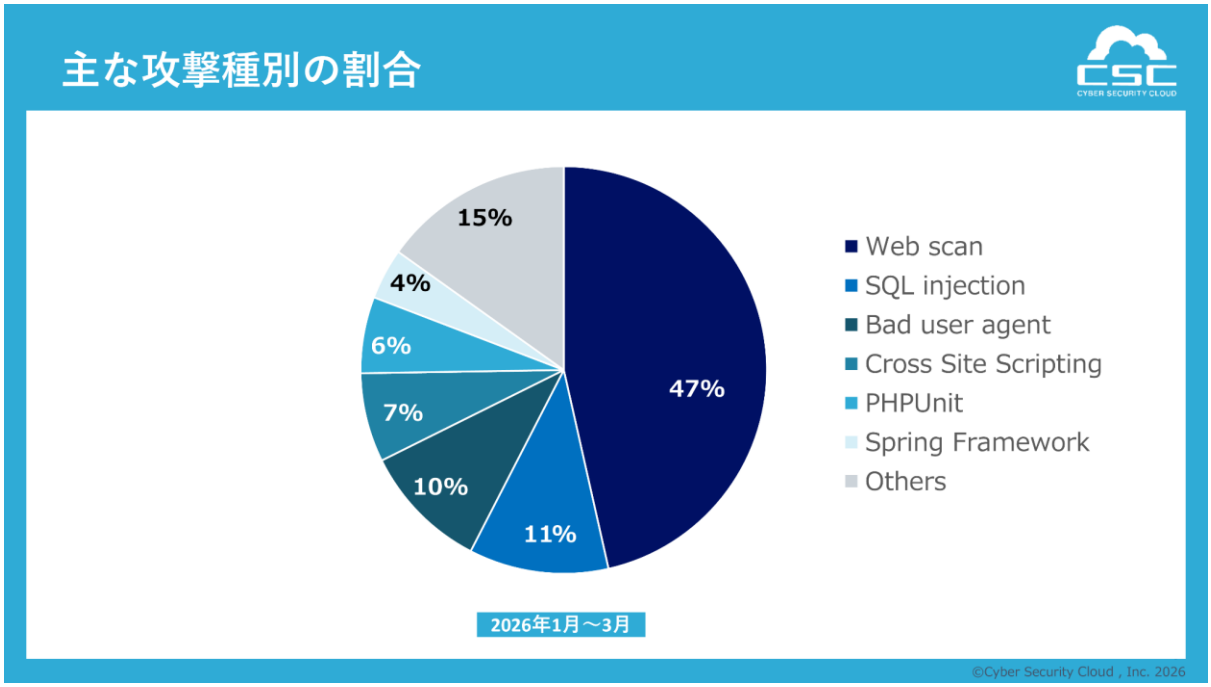
■ 攻撃総数と推移

2026年1月～3月におけるサイバー攻撃の検知数は、累計で約7.1億件にのぼり、1秒あたりに換算すると平均約90回の攻撃が発生している計算となります。攻撃は期間を通じて高水準で推移しており、企業・組織のWebサービスが常時サイバー攻撃に晒されている状況が続いています。

また、1日あたりの攻撃数は平均約785万件で推移し、最小値は約592万件、最大値は約1,393万件を記録しました。最大時は1秒あたり約160回の攻撃に相当し、通常時と比較して短時間で大幅に増加する様子が複数回観測されています。

これらの結果から、サイバー攻撃は常時高水準で発生する状態に加え、短期間で急増するイベント型の攻撃が重なる構造へと変化していることが示唆されます。単純なアクセス量の監視だけでは攻撃の全容を把握することが困難であり、パターン分析を含む多角的な監視体制が求められています。

■ 攻撃種別の構成比と傾向



攻撃種別の構成比を見ると、Web scanが約46%と最も高い割合を占めており、サイバー攻撃の多くが脆弱性の有無を確認するための探索行為であることが分かります。これは、攻撃者が無差別にインターネット上の公開サービスをスキャンし、侵入可能な対象を特定している状況を示しています。

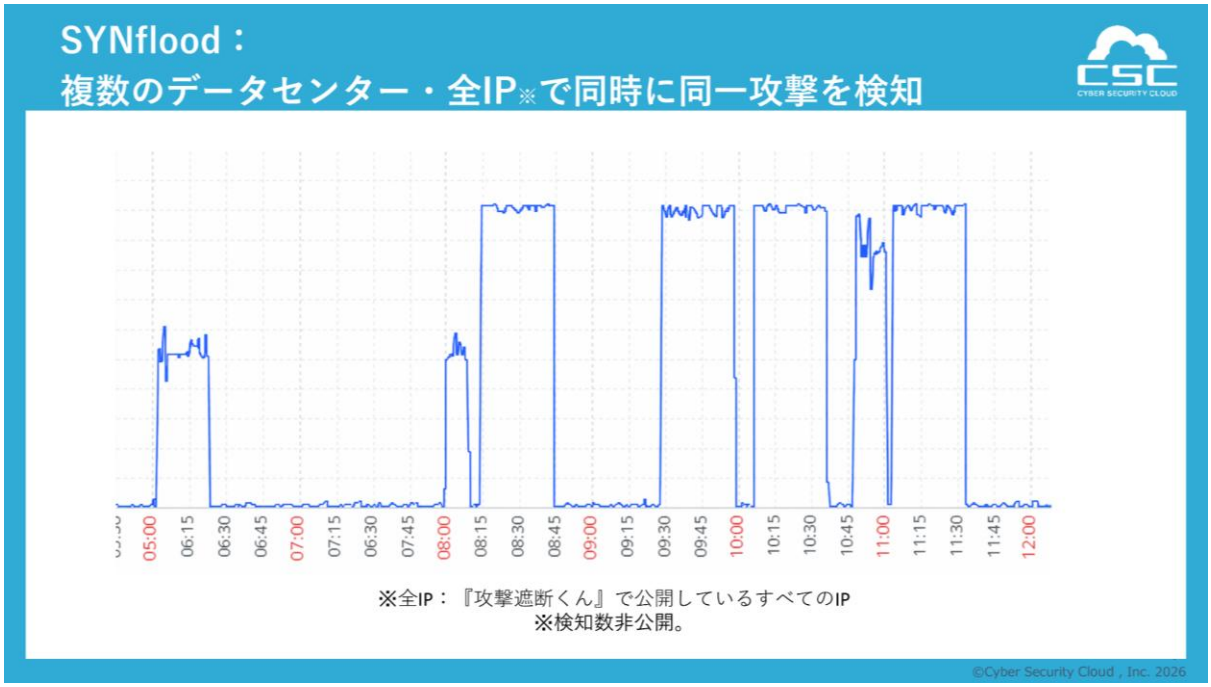
次いで、SQLインジェクションが約11%、不正なUser-Agentを用いたアクセス（Bad User Agent）が約10%を占めており、攻撃の自動化が進んでいることがうかがえます。これらは、スクリプトやボットを利用した機械的な攻撃が広範囲に実行されていることを示唆しています。

また、クロスサイトスクリプティング（XSS）やPHPUnit、Spring Frameworkを狙った攻撃など、特定のソフトウェアやフレームワークの脆弱性を対象とした攻撃も一定割合を占めています。後述するReactやLog4Shellの事例と同様に、OSSや広く利用されているソフトウェアが継続的な攻撃対象となっていることが確認されました。「その他」に分類される攻撃も約15%を占めており、攻撃手法の多様化が進んでいることが分かります。
このように、サイバー攻撃は「探索（スキャン）」「自動化された攻撃」「脆弱性を狙った侵入行為」が組み合わさる形で実行されており、単一の対策ではなく、多層的な防御が求められています。

■ 攻撃傾向の変化（2025年10月～12月との比較）

2026年1月～3月の攻撃動向を前四半期（2025年10月～12月）と比較すると、サイバー攻撃の性質に明確な変化が確認されました。
前四半期においては、Webアプリケーションの脆弱性を狙った攻撃が中心でしたが、今四半期は攻撃の構造そのものが変化しています。

1．攻撃範囲の拡大：無差別型DDoS攻撃の出現



複数のデータセンターに対して同時に攻撃が行われる無差別型のDDoS攻撃が確認されました。これらの攻撃は、特定のWebサービスを狙う従来の手法とは異なり、クラウドインフラのIPレンジ単位で広範囲に対して実行されている可能性があります。

当社の観測では、SYN flood攻撃において特定地域のIPレンジから集中的なトラフィックが確認されており、特にブラジルのIPアドレス帯域を起点とする通信が多数観測されました。これらのトラフィックの送信元は連続する複数のIPアドレスのケースも見られ、単一の端末ではなく、複数のノードまたはネットワークを活用した攻撃である可能性が示唆されます。

こうした特定地域からの集中トラフィックの背景としては、いくつかの要因が考えられます。例えば、比較的低コストで利用可能なクラウドインフラやネットワークリソースの存在、あるいは攻撃に利用されやすいネットワーク環境などが影響している可能性があります。また、攻撃者が特定の地域のインフラを経由することでトラフィックの分散や追跡の困難化を図っている可能性も考えられます。

このような攻撃は、単一の対象を集中的に狙うのではなく、日本国内あるいは世界のデータセンターを無差別に狙っているものと考えられ、特定のアプリケーション・サービスを狙ったターゲット型攻撃とは異なる性質を持っています。

※なお、これらの観測された攻撃元のIPアドレスは、攻撃者の所在を直接示すものではありません。攻撃者は低コストのクラウドインフラや追跡困難なネットワーク環境を意図的に経由する場合があり、利用可能なインフラやネットワーク条件に基づいて選択されている可能性がある点に留意が必要です。

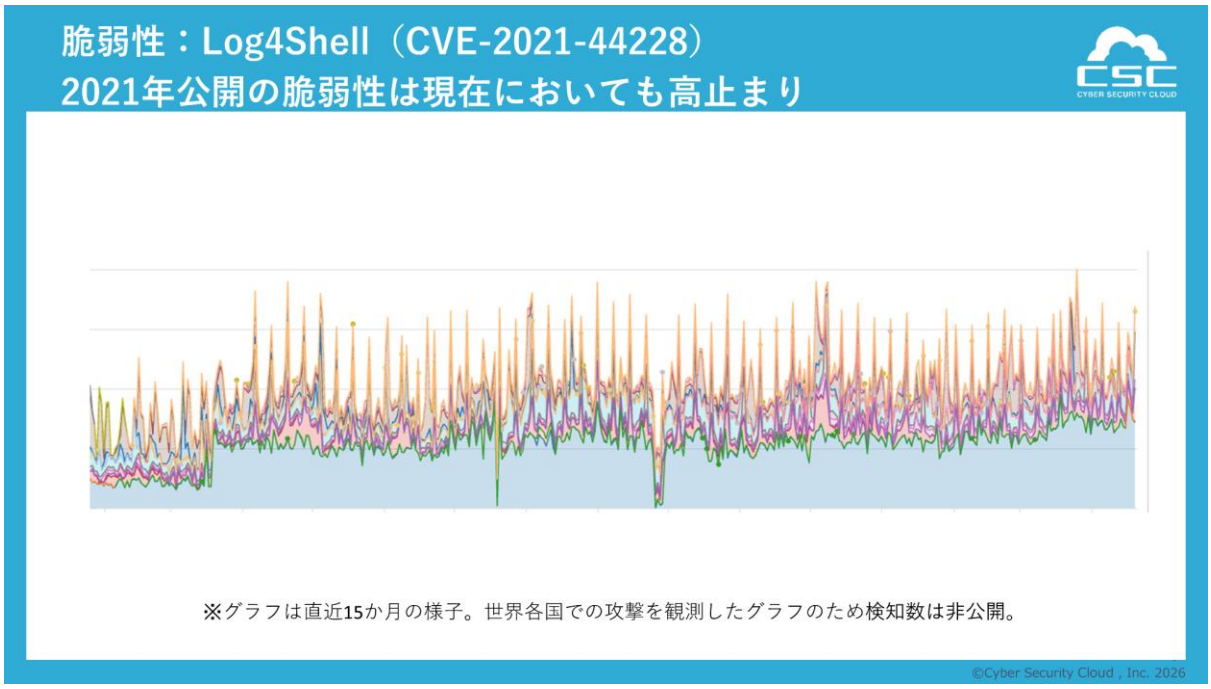
2. 攻撃パターンの変化：短時間・断続型攻撃の増加

数分単位で断続的に攻撃を繰り返す傾向が確認され、短時間での急増が連続的に発生する特徴的なトラフィックパターンが観測されました。

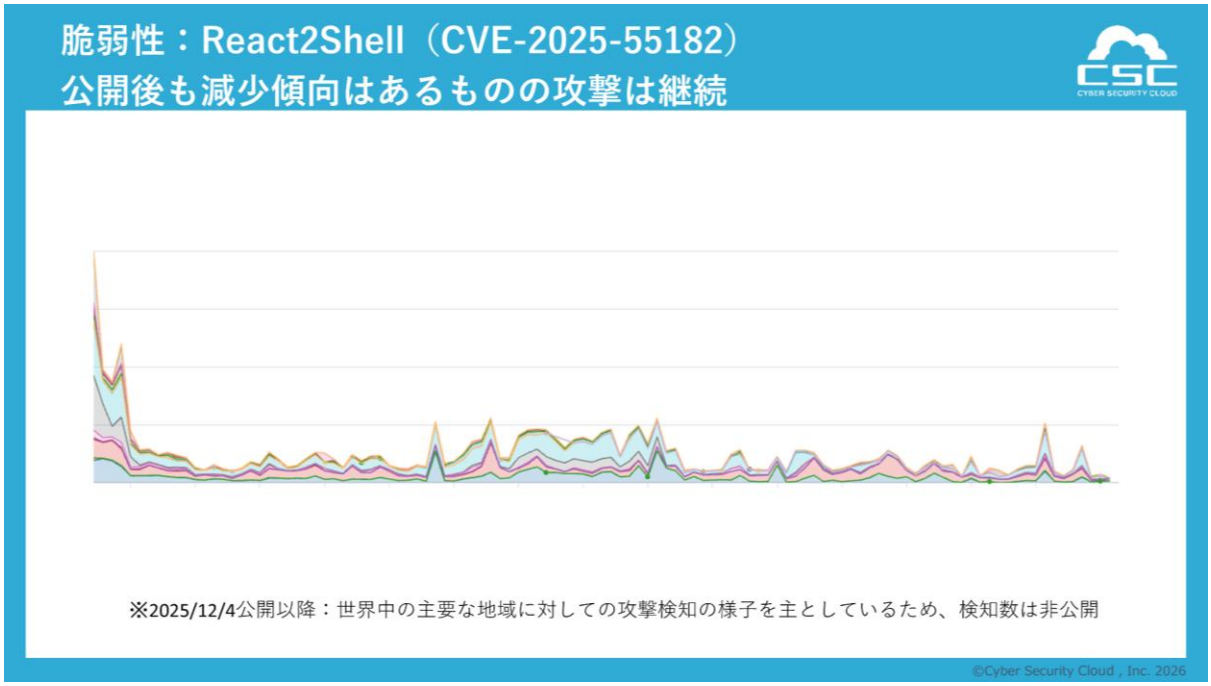
このような攻撃は、従来の長時間にわたり負荷をかけ続ける攻撃とは異なり、防御システムの検知閾値や緩和処理を回避することを目的としている可能性があります。短時間の攻撃を繰り返すことで、システムへの継続的な負荷を維持しつつ、単純なレート制限（リクエスト数制限）を回避することを狙う困難にする新たな手法と考えられます。

また、こうした攻撃パターンは自動化されたツールやボットによって実行されている可能性が高く、攻撃の高度化・効率化が進んでいることを示唆しています。

■ 脆弱性攻撃の状況



過去に公開された脆弱性に対する攻撃は、現在も継続して観測されています。特に、2021年に公開されたLog4Shell（CVE-2021-44228）については、発覚から数年が経過した現在においても攻撃が減少しておらず、依然として主要な攻撃対象となっている状況が確認されました。
掲載している直近15ヶ月の推移グラフからも、一定間隔で増減が繰り返されている様子が確認でき、攻撃が一過性のものではなく、継続的に実行されていることが分かります。未対策のシステムが一定数存在し、攻撃者にとって継続的に狙う余地が残されていることを示唆しています。



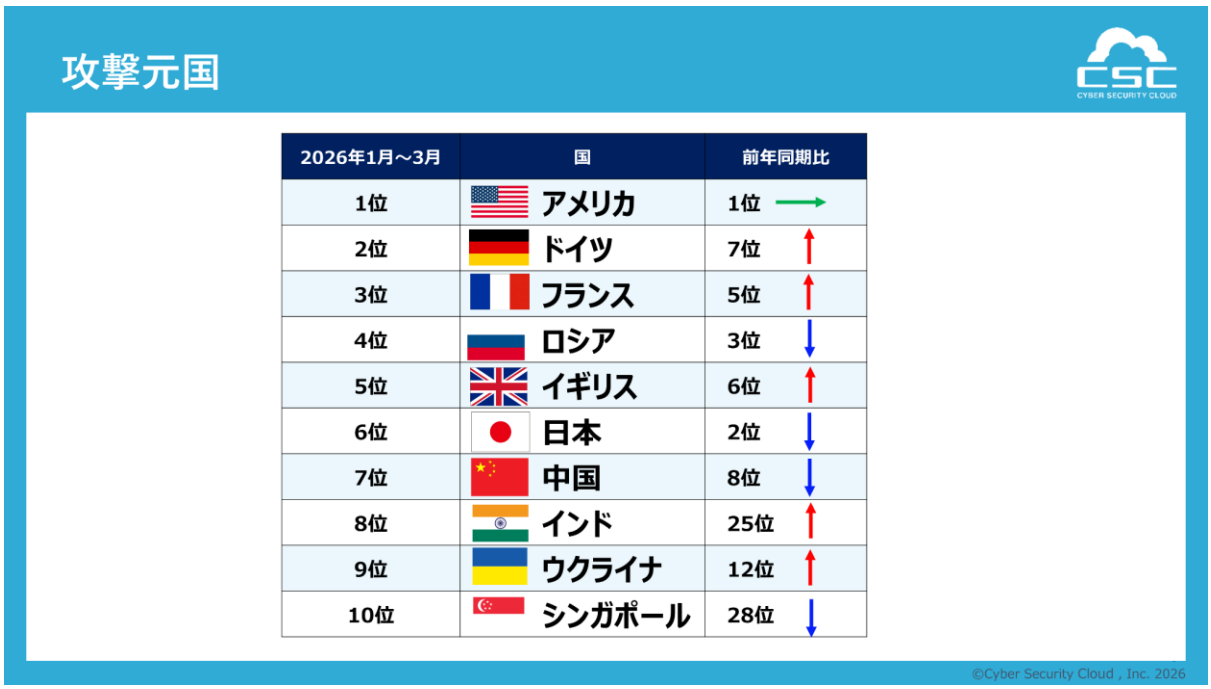
2025年12月4日に公開されたReactに関連する脆弱性については、公開直後から攻撃が急増し、当社の観測環境においても短期間で大きなピークが確認されました。その後は減少傾向にあるものの、一定水準で攻撃が継続している状況が見られます。

このように、近年のサイバー攻撃は、脆弱性公開直後の爆発的な攻撃と、過去の脆弱性に対する長期的・持続的な攻撃が並行して発生する傾向が強まっています。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一方で、対応が遅れたシステムに対しては長期間にわたり攻撃が続く傾向があります。

こうした状況は、脆弱性への対応が十分に行われていないシステムが一定数存在している可能性を示しており、攻撃者にとって継続的に狙う余地があることを意味します。企業・組織においては、脆弱性情報の迅速な把握と初動対応に加え、過去の脆弱性に対する継続的な棚卸しと対策を行うことが重要です。

■ 攻撃元国の傾向

2026年1月～3月における攻撃元国の傾向は以下の通りとなりました。



2026年1月～3月	国	前年同期比
1位	アメリカ	1位 →
2位	ドイツ	7位 ↑
3位	フランス	5位 ↑
4位	ロシア	3位 ↓
5位	イギリス	6位 ↑
6位	日本	2位 ↓
7位	中国	8位 ↓
8位	インド	25位 ↑
9位	ウクライナ	12位 ↑
10位	シンガポール	28位 ↓

前年同期と比較すると、攻撃元の地理的構成には明確な変化が見られました。特に、ドイツ（7位→2位）、フランス（5位→3位）といった欧州地域の順位上昇が顕著であり、これらの地域からのトラフィックの存在感が増しています。

一方、日本は前年の2位から6位へと順位を下げており、相対的に国内トラフィックの比率が低下しています。また、インド（25位→8位）、ウクライナ（12位→9位）、シンガポール（28位→10位）など、これまで上位ではなかった国の順位上昇も確認されました。

このような変化の背景には、特定のIPレンジを集中的に利用した攻撃や、複数地域からのトラフィックが組み合わさる傾向も確認されており、攻撃インフラが分散的かつ動的に利用されていることが示唆されます。

さらに、攻撃元として観測される地域については、インフラコストやネットワーク環境などの要因により、攻撃に利用されやすい地域が存在する可能性も指摘されています。これらは必ずしも攻撃者の所在を示すものではなく、利用可能なリソースや環境条件によって選択されている可能性があります。

※本ランキングは当社WAFで検知されたトラフィックを基に集計したものであり、攻撃者の所在を直接示すものではありません。

■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

今回のレポートからは、サイバー攻撃の対象が広範囲に拡大しつつある明確な兆候が見て取れます。特に、複数のデータセンターを跨いで観測された無差別型のDDoS攻撃は、従来の「特定サービスを狙う攻撃」とは異なり、より広域への影響を意図したものと考えられます。

また、短時間・断続的に攻撃を繰り返す攻撃パターンの増加は、防御側の検知や緩和の仕組みを前提とした攻撃設計へと進化している可能性を示唆しています。攻撃の自動化・効率化が進む中で、従来の対策では対応が難しいケースも増えていくと考えられます。

さらに、Reactのように公開直後から急増する攻撃と、Log4Shellのように長期間継続する攻撃が並行して発生している点は、現在のサイバー攻撃の特徴を端的に示しています。攻撃者が「短期的な機会」と「長期的な未対策領域」の両方を同時に狙っていることを意味します。

こうした状況においては、単発的な対策ではなく、継続的な可視化と運用を前提としたセキュリティ対策が不可欠です。当社は今後も、実際の攻撃データに基づく知見をもとに、より実効性の高いセキュリティ対策の提供に取り組んでまいります。

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