2023 年 6 月 9 日

*Press Release*

アカマイ・テクノロジーズ合同会社

# Akamai 脅威レポート：APJ 地域の金融サービスに対する Web アプリケーションおよび API 攻撃が約 250%増加

## オーストラリアや日本などの金融ハブが攻撃の最大の標的になっていることが明らかに

- **アジア太平洋・日本地域での Web アプリケーションおよび API 攻撃件数は、1 日平均 1,000 万件**
- **2022 年 APJ 地域で最も多く攻撃を受けた業界は金融サービス、コマース、デジタルメディア**

※本リリースは 2023 年 5 月 24 日 (現地時間)シンガポールで発表されたプレスリリースの抄訳版です。

オンラインの力となり、守るクラウドカンパニーの Akamai Technologies, Inc.（NASDAQ：AKAM）は、最新の脅威レポート「インターネットの現状 | セキュリティギャップのすり抜け：組織を狙うアプリケーションおよび API 攻撃の増加」を公開しました。本レポートでは、アジア太平洋・日本（APJ）地域の金融サービス業界がこの地域で最多の攻撃対象となり、Web アプリケーションおよび API 攻撃数が前年比 248% 増という驚異的な勢いで増加していることを明らかにしています。

248% 増という APJ の金融業界に対する Web アプリケーションおよび API 攻撃数の増加率は、約 169%というグローバル全体の増加率をはるかに上回っています。つまり、同地域の金融サービス組織はより頻繁に攻撃対象となっており、攻撃者の規模、頻度、巧妙さが高まる中で深刻なリスクにさらされている実状が浮かび上がります。

「攻撃数が約 250% 増加したという事実は、APJ の金融サービス組織がデジタルトランスフォーメーションと、顧客中心志向のデジタル商品およびサービスに引き続き多額の投資をしていることが関係しています。これは金融サービス組織にとって重大な懸案事項です。デジタル化の普及によって全体的なアタックサーフェスが拡大し、攻撃者がサイバー攻撃を仕掛ける機会が増加しているのです」と、Akamai の Security Technology／Strategy Director（APJ）の Reuben Koh は説明します。

APJ 地域では、直近の 24 カ月で Web アプリケーションおよび API 攻撃が着実に増加しており、1 日に平均 1,000 万件の攻撃が発生しています。Akamai は攻撃件数が 6,000 万件を超える日も複数観測しており、この地域の組織は高頻度の標的型攻撃のリスクに引き続き直面していると言えます。

ローカル・ファイル・インクルージョン（LFI）攻撃は、APJ で最も多用されている攻撃ベクトルです。前年比約 154% 増となり、クロスサイト・スクリプティング（XSS）および SQL インジェクション攻撃を上回る勢いです。LFI

攻撃は、セキュアでないコーディングや Web サーバーに実際に存在する脆弱性を悪用し、コードをリモートで実行するか、ローカルに保存されている機微な情報へのアクセスを試みます。

APJ で LFI 攻撃が増加しているのは、攻撃者がその手法を絶えず進化させ、攻撃の標的を消費者の行動にシフトして、投資に対する最大のリターンを得ようとしているからです。

Akamai のレポートでは、APJ の市場ごとの Web および API 攻撃パターンのトレンドの特徴も明らかにしています。

- 2022 年に APJ で Web アプリケーションおよび API 攻撃を最も多く受けた上位 3 つの業界は、金融サービス（20 億件）、コマース（9 億 8,000 万件）、デジタルメディア（3 億 9,300 万件）でした。
- APJ において重要な金融ハブと認知されているオーストラリアと日本は、金融業界に対する Web アプリケーションおよび API 攻撃の増加率が極めて高く、それぞれ前年比で 259% 増と 1,635% 増を記録しました。
- ただし、オーストラリアでは、2022 年はいくつかのビッグバン級の攻撃とともに Web アプリケーションおよび API 攻撃が長期にわたって一定の割合で増加するパターンだったのに対し、日本では毎月ビッグバン級の攻撃が発生する状況でした。これは、これらの国の特定の業種と組織が頻繁に標的にされたことを示しています。
- 日本のハイテク業界を標的とした攻撃の増加率は、2022 年に前年比 116% 増となりましたが、これは日本が R&D と先進テクノロジーに多額の投資をしていることが主な要因と考えられます。
- インドでは、小売およびコマース業界を標的とした、より長期的で一貫した攻撃キャンペーンが発生しており、2022 年の Web アプリケーションおよび API 攻撃数は前年比約 90% 増となりました。インドでは、多数のオンライン小売企業が存在し、e コマース支出額も増加していることから、この業界は攻撃者にとって利益の出やすい標的と言えます。インドでの金融サービスに対する攻撃件数は、前年比 56% 増を記録しています。
- 2021 年から 2022 年にかけて最も高い攻撃増加率を記録した APJ の上位 3 つの業界は、金融サービス（248%）、製造（162%）、公共部門（139%）でした。

「サイバー犯罪者は、Web アプリケーションおよび API を常に悪用し、新たな攻撃手法を絶えず導入して最大のリターンを得ようとします。APJ の金融、製造、コマース業界はデジタルイノベーションのハブです。だからこそ、攻撃者にとって非常に利益の出やすい標的とされています」と、Koh は述べています。

「脅威の状況は、サーバーサイド・リクエスト・フォージェリー（SSRF）、サーバーサイド・テンプレート・インジェクション（SSTI）、サーバーサイド・コード・インジェクションなどの新たな攻撃ベクトルとともに、リモートコード実行に移行しつつあります。執拗な攻撃に絶えず直面する中、組織は最新の攻撃トレンドとベストプラクティスを常に把握し、自らの緩和戦略を適合させる必要があります」と Koh は結論付けています。

なお、Akamai は API データと行動分析に基づく API 検知および対応プラットフォームを提供する Neosec の買収に関する正式契約を締結したことを発表しました。この買収は、アプリケーションおよび API セキュリティポー

トフォリオを補完するものであり、これにより、Akamai は急速に拡大しつつある API 脅威に対する可視性を大きく高めることができます。

SOTI について詳細な情報は、Akamai セキュリティハブにアクセスするとともに、Twitter で @Akamai_Research をフォローしてください。Akamai の脅威リサーチャーと交流し、貴重な知見を得ることができます。

**Akamai について：**

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。広範に分散したエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com/ja および akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。