2026 年 6 月 1 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：
金融サイバー攻撃の標的、アジア太平洋地域の銀行が世界最多に

2025 年の金融サービスを狙ったアプリケーションレイヤーDDoS 攻撃は APAC が世界全体の 52%を占める

※本リリースは 2026 年 5 月 22 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。

Akamai（NASDAQ：AKAM）は、最新の脅威レポート「*AI* を活用したボットネットと *API* 可視性のギャップ：金融サービス業界の攻撃トレンドに関するインターネットセキュリティの現状」を公開しました。アジア太平洋地域（APAC）の金融機関では、デジタルバンキング、リアルタイム決済、および API 連携によるサービスが急増する一方で、多くの組織ではセキュリティ対策が追いつかず、アタックサーフェスが拡大しているため、世界的なサイバー攻撃の割合が増加しています。レポートによると、2025 年に金融サービスに対する全世界のレイヤー7DDoS 攻撃のうち、APAC が 52%を占めており、4 年連続で最もアプリケーションレイヤー攻撃の標的にされた地域となっています。このことは、拡大するデジタル環境のセキュリティ確保が組織にとって急務であることを示しています。

DDoS 攻撃は、オンラインバンキングのポータル、決済 API、および顧客が利用するアプリケーションを正規のアクセスを装ったトラフィックで過負荷状態にするように設計されています。そのため、従来のネットワークフラッド DDoS よりも攻撃の識別と阻止がはるかに困難です。APAC の金融業では、銀行とフィンテック企業が最も被害を受けており、レイヤー7 DDoS 攻撃のそれぞれ 44%と 38%を占めました。一方で、レイヤー3/4 DDoS では銀行が同地域の 92%を占めました。

問題は、攻撃の量だけでなく、標的になっている環境の複雑さにもあります。その国で普及しているリアルタイム決済システムやモバイル・バンキング・プラットフォーム、フィンテックのエコシステム、様々な顧客向けサービスの展開により、銀行やフィンテック企業が保護すべきエンドポイントの数は増加しています。さらに、競争圧力や AI を活用したコーディングツールなどにより、新しいサービスが実装されるスピードは加速しています。

しかし、多くの組織は、自社が依存している API を完全に把握できていません。APAC の金融サービス業界の IT およびセキュリティリーダーの 77%は、自社の API 資産の全体像を把握していると考えていますが、どの API が機密データを返しているかまで把握しているのはわずか 27%に留まっています。世界全体では、金融サービス組織の 96%が過去 12 か月間に少なくとも 1 件の API セキュリティインシデントを報告しており、これはあらゆる業界の中で最も高い割合です。不正なアクティビティと正当なトラフィックを区別することが困難になっている現在、このような状況は深刻な盲点を拡大させています。Akamai は、2025 年後半に高度なボットアクティビティが 147%急増したことを確認しました。AI を悪用したボットネットは、ブラウザーの挙動を模倣し、従来型の防御策を回避する能力が向上しています。

Akamai の Security Technology and Strategy APAC 担当 Director である Reuben Koh は「APAC の銀行およびフィンテック企業は、世界で最も急速に変化するデジタル金融環境の中心に位置しています。新しい決済サービス、モバイルバンキング機能、フィンテックの統合、AI を活用したワークフローが登場するたびに、攻撃者に狙われる新たな依存関係が生まれています」「多くの銀行は、パッチ適用や安全な統合が困難なレガシーシステムの上に、新しいデジタルサービスのセキュリティも確保しようとしています。どのような API が存在し、どの API が機密データを露出させているか、またそれらが本来どのように動作するべきかを把握していない機関は、すでに高いリスクに晒されているといえます」と述べています。

金融機関にとっての、教訓は明らかです。単にコンプライアンス要件を満たすだけではなく、セキュリティを運用上のレジリエンスにおける最優先事項へと進化させる必要があるということです。これには、アプリケーションレイヤー DDoS、ネットワークフラッド、API の悪用に対する防御の強化、機密データの露出や異常なふるまいを特定できる API セキュリティツールへの投資、マシンスピードで応答可能な AI 搭載の防御策の実装などが含まれます。

また、このレポートでは、マイクロセグメンテーションを導入している組織は、重要なアプリケーションを隔離して内部に侵入した攻撃者の水平展開を制限することで、インシデントへの対応にかかる時間が 33%向上したことも明らかにしています。これは、中断が 1 分長引くたびに評判、規制、財務上の損失につながる可能性がある環境では大きなアドバンテージとなります。

今年で 12 年目を迎える Akamai の「インターネットの現状 - セキュリティレポート」では、世界の Web トラフィックの大部分を処理する Akamai のサイバーセキュリティ保護インフラで観測された攻撃データを取り上げています。

本レポートの監修を務めた Akamai の Advisory CISO である Steve Winterfeld は「サイバー犯罪者やハクティビストは、単に迷惑を及ぼすだけの攻撃からハクティビズムとサイバー犯罪の両方を含む持続型の包囲攻撃へと DDoS を拡大し続けており、金融サービス業界はその標的にされています。さらに、観測データからは、AI が従来のセキュリティリスクを軽減するどころか、リスクを急激に増幅させているため、API が狙われるケースがますます増えていることが明らかになりました。金融サービス業界向けに詳述するセキュリティ戦略とベストプラクティスを活用して、自社のセキュリティ対策の一助としていただければと思います」と述べています。

レポートの全文はこちらでお読みください。

Akamai について

Akamai は、オンラインビジネスの力となり、守るサイバーセキュリティおよびクラウドコンピューティング企業です。当社の市場をリードするセキュリティソリューション、優れた脅威インテリジェンス、グローバル運用チームによって、あらゆる場所でエンタープライズデータとアプリケーションを保護する多層防御を利用いただけます。Akamai のフルスタック・クラウド・コンピューティング・ソリューションは、世界で最も分散化されたプラットフォームで高いパフォーマンスとコストを実現しています。多くのグローバル企業が、ビジネスの成長に必要な業界最高レベルの信頼性、拡張性、専門知識を提供できる Akamai に信頼を寄せています。詳細については、akamai.com および akamai.com/blog をご覧いただくか、X や LinkedIn で Akamai Technologies をフォローしてください。

※AkamaiとAkamai ロゴは、Akamai Technologies Inc.の商標または登録商標です
※その他、記載されている会社名ならびに組織名、ロゴ、サービス名は、各社の商標または登録商標です
※本プレスリリースの内容は、個別の事例に基づくものであり、個々の状況により変動しうるものです