2025 年 6 月 12 日

Press Release

アカマイ・テクノロジーズ合同会社

FS-ISAC と Akamai による脅威レポート、アジア太平洋地域の金融業界を標的とした DDoS 攻撃が前年比 245% 増加

金融業界全体で、信頼性と回復力を脅かす高度で持続的な DDoS 攻撃が増加していることが明らかに

会員主導の金融サービス向けグローバル・サイバー・インテリジェンス共有コミュニティの FS-ISAC と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のグローバルリーダーである Akamai Technologies, Inc（NASDAQ：AKAM）は、グローバルにおける、金融機関を主な標的とした分散型サービス妨害（DDoS）攻撃の急増について詳述した最新レポートを共同で発表しました。

2025 年版の『迷惑行為から戦略的脅威へ：金融業界に対する DDoS 攻撃』によると、昨年、APAC の金融サービス企業は、ボリューム型レイヤー 3 およびレイヤー 4 DDoS 攻撃の標的となった企業の 38% を占め、2023 年の 11% から 245% の大幅な増加を記録しました。脅威アクターは APAC の急速にデジタル化する金融業界にフォーカスしているため、これらの攻撃は、地域における業務の継続性と顧客からの信頼をますます脅かしています。

FS-ISAC（EMEA）の Chief Intelligence Officer 兼 Managing Director である Teresa Walsh 氏は「DDoS 攻撃はますます巧妙化しており、単純なネットワークフラッディングから、サプライチェーン全体にわたる複雑な脆弱性を悪用する標的型の多次元攻撃へと進化しています」「APAC のデジタル化が進む金融システムに影響を与える脅威戦術が進化し続けている中で、私たちは技術的防御を強化し、従業員、ツール、プロセスをシームレスに連携させる必要があります。インフラを強化し、継続的な監視とコラボレーションの文化を育成して、継続性と顧客の信頼を保護することが重要です。」と述べています。

レポートに記載されている地域別の主な調査結果は次のとおりです。

- 2024 年第 4 四半期に発生した継続的な DDoS キャンペーンは、6 か国の 20 以上の機関に影響を与えました。これは、同じ脅威アクターまたはハッカーグループによるものであった可能性があります。
- 個々の攻撃はそれほど大規模ではありませんでしたが、継続的なキャンペーンは長期にわたり、執拗に続きました。これは、以前の APAC では見られなかった傾向です。
- 2024 年第 4 四半期に APAC で発生した前例のない DDoS 攻撃の波は、小売企業、決済処理業者、投資銀行、政府系金融機関など、複数の金融サービス区分を標的としたものでした。
- APAC におけるレイヤー 7（アプリケーションレベル）攻撃は大幅に増加し、金融サービス部門が最も標的とされています。この増加は API での導入が拡大したことによるもので、これにより、攻撃者にとってのアタックサーフェスが拡大しました。

また、アジア太平洋地域を超えた地政学的緊張の高まりや、悪性の意図を持つ脅威アクターがツールにアクセスしやすくなる DDoS 請負プラットフォームの拡散など、複数の要因による攻撃の急増も原因となっています。

Akamai（アジア太平洋・日本）の Director of Security Technology & Strategy の Reuben Koh は「APAC での DDoS 攻撃は、もはや単純な力ずくの攻撃ではなく、脆弱なシステムや公開された API を悪用する高度なマルチベクトルキャンペーンへと進化しています」「金融サービス、コマース、製造など、高い需要を集める主要業界がデジタル化を加速させる中、これらの継続的な攻撃は、運用上のリスクとレピュテーションリスクを増大させています。組織は、今日の脅威の状況で自社を守るために必要なインテリジェンス、スケーラビリティ、アジリティを提供できる、信頼性の高いサイバーセキュリティパートナーと連携する必要があります。」と述べています。

世界的に見られる同様の傾向

APAC での観測結果は、レポートに記載されたグローバルの傾向と一致しています。2024 年に発生したすべてのレイヤー 3 およびレイヤー 4 DDoS 攻撃の 3 分の 1 以上（37%）が金融サービス業界を標的とするものであり、次いでゲーム業界が 20%、製造業が 17% を占めました。これで、金融業界は 2 年連続でこうした攻撃の主な標的となり、2024 年に DDoS 攻撃の急増を経験した唯一の業界でした。

DDoS 攻撃頻度の増加は、イスラエルとハマスの紛争やロシアとウクライナの紛争など、現在進行中の地政学的緊張にも密接に関連しており、このような紛争がイデオロギー的に動機付けられたハクティビズムの急増をもたらしています。また、DDoS 請負グループ、ハクティビスト、および国家支援の攻撃者との間の境界があいまいになるにつれ、アトリビューションも困難になりつつあります。

断片化されたサイバー環境における防御を最新のものへ

『迷惑行為から戦略的脅威へ：金融業界に対する DDoS 攻撃』レポートでは、FS-ISAC と Akamai が開発した DDoS 対策成熟度モデルを採用する金融機関にとってのメリットも強調しています。このモデルは、準備状況をベンチマークし、防御戦略への投資をガイドするために設計されたスケーラブルなフレームワークです。

レポートでは、次のような組織が早急に考慮すべき内容を強調しています。

- リアルタイムのふるまい分析とトラフィックのベースライン化
- 脅威インテリジェンス主導の検知と緩和の自動化
- 継続的なテストと堅牢化による DNS と API のセキュリティ強化
- ハイリスク地域からの攻撃をブロックするジオ IP フィルタリング

『迷惑行為から戦略的脅威へ：金融業界に対する DDoS 攻撃』には、地域別データ、主要なハクティビストグループのプロファイル、およびサイバー衛生のベストプラクティスの概要が含まれています。さらに、このレポートには緩和戦略に関するセクションも用意されています。特に注目すべきは、FS-ISAC と Akamai が共同開発した DDoS 対策成熟度モデルに従うことを推奨している点です。このモデルは、組織が自社の具体的な能力と実践する内容をマッピングすることで、DDoS 攻撃への耐性を評価するために役立ちます。このモデルでは、さまざまな成熟度の段階を概説した構造化されたアプローチが提供されます。

この共同レポートは、FS-ISAC が金融業界のサプライチェーンのセキュリティ向上を目的としたプログラム、Critical Providers Program を 2022 年にスタートした際に、Akamai が設立に参加したことで生まれました。

レポートの全文はこちらからダウンロードできます。

FS-ISAC について

FS-ISAC は、会員主導の非営利組織です。グローバル金融システムにおけるサイバーセキュリティと回復力を強化し、金融機関とその顧客を保護しています。1999 年に設立された同組織のリアルタイム情報共有ネットワークは、会員が有するインテリジェンス、知識、実践を広め、金融業界全体のセキュリティと防御に役立っています。加入する金融企業は、75 か国で 100 兆ドルの資産を保有しています。

# # #

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。