2025 年 4 月 23 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：AI により、APAC での Web 攻撃は前年比 73% 増の 510 億件に増加

日本は 63 億件を記録

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、Akamai Technologies, Inc.（NASDAQ：AKAM）は、新しいインターネットの現状（SOTI）に関するレポート「アプリと API セキュリティの現状 2025：AI はデジタル領域をどうシフトさせるか」を公開しました。本レポートによれば、アジア太平洋・日本（APAC）地域では、Web アプリケーション攻撃が前年比で 73% 増加しています。これは、世界的に最も高い増加率であり、人工知能（AI）が急速に普及し利用が広がる中、Web アプリケーションや API のセキュリティ確保の重要性が明らかになりました。

AI による脅威の検出と対応の機能強化により、Web アプリケーションと API のセキュリティ環境が変革しています。一方で AI による新たなセキュリティ課題も発生しています。2024 年には、APAC 地域で 510 億件の Web アプリケーション攻撃が報告されており、2023 年の 290 億件から大幅に増加しています。この急速な伸びは AI アプリケーションの急速な普及と関連しており、アタックサーフェスが拡大し、サイバー攻撃の複雑性が高まっています。

APAC 地域で Web 攻撃や API 攻撃を最も多く受けた国としては、オーストラリア（203 億件）、インド（173 億件）、シンガポール（159 億件）が挙げられ、日本（63 億件）、中国（62 億件）、韓国（49 億件）、ニュージーランド（29 億件）、香港特別行政区（22 億件）が続きます。APAC 全体で最も多く攻撃を受けた業界は金融サービスで、270 億件を超える Web 攻撃を受けており、次いでコマース業界が 180 億件を超える Web 攻撃を受けています。これには、これらの業界が AI などの新しいテクノロジーを迅速に導入していることが関わっています。

APAC における Web 攻撃と API 攻撃の数は、2024 年に世界全体で 3,110 億件あった Web アプリケーション攻撃の数を押し上げており、前年比で 33% 増加しています。今年の調査結果の核心は、AI で駆動するツールをコアプラットフォームに統合するために使用が広がっている API を標的とする脅威です。Akamai は 2023 年 1 月から 2024 年 12 月の間に、世界中で 1,500 億件の API 攻撃を記録しました。これは、攻撃者が認証に関わる脆弱性と攻撃の自動化に適した攻撃ベクトルを悪用したためです。AI ベースの API は、外部からのアクセスが可能であり、認証対策が不十分である場合が多いため、特にリスクが高くなっています。

APAC はレイヤー 7 DDoS 攻撃の第 2 位の標的地域

レポートによれば、同期間中、レイヤー 7（アプリケーションレイヤー）の DDoS 攻撃が 94% 増加して、世界全体で 7 兆件の攻撃に達しており、ハイテク分野が最も影響を受けた業界であることが明らかになっています。月ごとの攻撃数は、2023 年前半の 5,000 億件以上から、2024 年末には 1.1 兆件以上に増加してい

す。HTTP フラッドは、引き続きレイヤー 7 の DDoS 脅威の上位に位置しています。Web アプリと API を標的としていて、重大度が高い状態を維持しています。

この世界的な増加傾向はアジア太平洋・日本地域でも明らかで、同地域ではレイヤー 7 DDoS 攻撃が前年比 66% 増加し、世界で第 2 位の標的地域となっています。24 か月間の数値として最大で、2024 年 12 月には 5,040 億件とピークに達しました。同地域はこの 2 年間で 7.4 兆件の攻撃を受け、各国が受けた攻撃件数は、シンガポールが 4.7 兆件で、インド（1.1 兆件）、韓国（6,070 億件）と続きます。また、このレポートでは、ソーシャル・メディア・チャネルなどのデジタル・メディア・プラットフォーム、およびコマース業界が、APJ で最も影響を受けている分野であることも明らかになりました。

その他の主なグローバル調査結果は次のとおりです。

- コマース企業を標的とした Web 攻撃が 2,300 億件以上発生しており、これが最も影響を受けた業界となっています。攻撃件数はハイテク分野（攻撃数が第 2 位の業界）のほぼ 3 倍に相当します。
- OWASP API Security Top 10 に関連するインシデントは 32% 増加しており、認証や認可の欠陥によって、機微な情報の漏えいや機能の悪用が発生しています。
- MITRE セキュリティフレームワーク関連のセキュリティアラートが 30% 増加しました。これは、攻撃者が自動化や AI などの高度な技術を用いて API を悪用していることが原因です。
- シャドウ API やゾンビ API は特に、ますます複雑化する API エコシステムにおいて脆弱な攻撃ベクトルを発生させています。

Akamai Technologies APJ の Director of Security Technology and Strategy、Reuben Koh は「APAC における Web 攻撃と API 攻撃の急増は、この地域のデジタル化が急速に進んでいるからだけでなく、AI を企業エコシステムに統合することによりサイバーセキュリティを急速に進化させることが至急必要であることを示しています。攻撃者が規模と手法の両方で攻撃を強化している状況を受けて、セキュリティ戦略もそれに応じて適応する必要があります」「この SOTI レポートでは、新たな脅威から組織をより適切に保護する方法として、実践的な緩和戦略についても詳しく説明しています。」と述べています。

将来の攻撃を緩和するためのコンプライアンス要件の強化

Web 攻撃と API 攻撃の急増に対応するため、世界各国の規制当局は、より厳格なサイバーセキュリティコンプライアンス要件とガイドラインを施行しており、APAC 地域の政府も例外ではありません。シンガポールは、規制管理を拡大するためにサイバーセキュリティに関する法案を拡張しました。日本は国内のサイバーセキュリティ戦略や法律の強化を進めており、インドはデジタル個人データ保護法を可決しました。オーストラリアは、機微な情報を処理する API とアプリケーションをより厳格な監督下に置くため、サイバーセキュリティ法 2024 を制定しました。

コンプライアンスの期限が迫っており、規制が強化されているため、組織がセキュリティの改善に後れを取れば、規制上の罰則を受けるだけでなく、評判の低下、データの損失、サービスの停止といったリスクも伴います。Akamai では、シフトレフトのセキュリティアプローチを採用し、API ガバナンスを強化し、進化を続ける脅威を検知し緩和する AI ベースの防御を展開することを推奨しています。

11 年目を迎えた、Akamai のインターネットの現状（SOTI）に関するレポートシリーズでは、グローバルな Web トラフィックの 3 分の 1 以上を処理するネットワークインフラから収集したデータに基づき、サイバーセキュリティと Web パフォーマンスに関する専門的な知見を提供します。

# # #

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。