2026 年 7 月 17 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：APAC で AI 駆動型コマースブームが ボットや API 攻撃の急増を助長、地域全体の 38%をコマース業が占める

小売企業、旅行・ホスピタリティ業界がデジタル体験のパーソナライズを競うなか、
同地域のボット活動は 63%急増

※本リリースは 2026 年 7 月 16 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、アジア太平洋地域（APAC）で急速に成長するコマース経済が、サイバー犯罪者の格好の標的となっていると発表しました。これは、小売企業、オンライン旅行予約サイト、ホスピタリティ業界が AI を活用したショッピング、予約、顧客体験の利用を加速させていることが背景にあります。Akamai の最新の「インターネットの現状（SOTI）」セキュリティレポート、「エージェント型ストアフロントのセキュリティ確保：コマース業界を狙う攻撃」によれば、APAC のコマース企業を標的とするボットアクティビティは 2025 年に 63%増加し、世界で最も高い増加率となりました。2025 年 7 月から 12 月にかけて、APAC の全業界で観察された AI ボットトラフィック全体の 38%をコマース業界が占めており、この地域での AI を活用したコマースの急速な導入のペースに対応できるセキュリティ戦略の必要性が浮き彫りになっています。

この地域では、小売企業はエージェント型コマースへと舵を切っており、ボットを活用したショッピング体験の高度なパーソナライズ化や、カゴ落ち（カート離脱）を抑制に取り組んでいます。APAC では特にチャットボットの増加も加速しています。ビジネスにおいて、よりパーソナライズされた顧客体験を通じて差別化しようと競い合っているためです。しかし、このことが正当な自動処理と、悪性ボットやスクレイピング、Credential Stuffing、API の悪用などの不正アクセスとを見分けることを難しくしています。

小売企業は依然として主要な標的となっていますが、APAC の旅行およびホスピタリティ業界も他の地域と比較して、より脅威にさらされています。その要因としては、断片化された旅行予約プラットフォーム、デジタルおよびモバイルの高い普及率、ロイヤルティプログラムの人気の高まり、中華圏の春節、日本のゴールデンウィーク、インドのディワリ、年末年始などの地域特有の祝祭日の繁忙期といったことが挙げられます。コマースビジネスが決済、ロイヤルティプログラム、在庫システム、物流および予約プラットフォームなどと連携するのに伴って、API が脅威にさらされるようになっています。APAC では特に旅行業界でこの傾向が顕著で、コマースに対する Web 攻撃の 22%を旅行業界が占め、その攻撃の 25%が API を標的としています。また、APAC のコマースビジネスは、アプリケーションレイヤー DDoS 攻撃の増加にも直面しています。レイヤー7 DDoS 攻撃は 2025 年に 2,600 億件から 3,610 億件へと、39%増加しました。API を標的としたレイヤー7 DDoS 攻撃のうち、小売企業が 51%を占め、次いでホスピタリティ業界（28%）と旅行業界（21%）が続きます。

Akamai の APJ 地域担当 Director of Security Technology and Strategy を務める Reuben Koh は「APAC のコマース業界は、AI に対応した、さらに自動化された未来に向かって急速にシフトしています。ビジネスでは生成 AI チャットボットやその他の AI を活用したサービスを利用して体験をパーソナライズし、フリクションを軽減しています」「しかしながら、チャットボットとのやり取り、予約フロー、ロイヤルティプログラムとの連携が増えるたびに、検知、理解、保護しなくてはならない新たなデジタルサーフェスが生じます。断片化されたプラットフォーム、ロイヤルティプログラムの人気の高まり、繁忙期のトラフィック急増などにより、旅行およびホスピタリティ業界においてリスクが高まっている APAC では、これは特に重要なことです。ビジネスは、顧客に余計な手間をかけさせることなく、大量の正当な自動化されたアクセスの中に隠された悪意ある意図を特定できるリスクベースの防御を、今こそ実装する必要があるのです。」と述べています。

コマース組織が AI と自動化を継続的に導入していくうえで、レジリエンスをセキュリティ機能にとどまらず、ビジネスの重要な取り組みまで拡張することが求められています。これには次のことが含まれます。

- **収益チェーンのマッピング：**決済、ロイヤルティプログラム、チェックアウト、在庫、パートナー連携をサポートする API を継続的に特定し、機微な情報がどこで露出する可能性があるかを把握
- **自動化をリスクベースで管理：**一律に「許可」または「ブロック」を判断するのではなく、正当な自動化と悪性ボットアクティビティを区別できるリスクベースのアプローチを採用
- **ピークトラフィック期間への備え：**主要なショッピングおよび旅行繁忙期に先立って、トラフィックの急増に対するキャパシティを強化し、DDoS 対応計画をテストし、偽の店舗サイトの出現や認証情報の漏えいを監視し、サイバーセキュリティチームと不正防止チームの連携を強化

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。

レポートの全文はこちらでダウンロードいただけます。

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。