2026 年 11 月 2 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 におけるログイン試行の 3 回に 1 回以上は高リスクまたは重大リスク

デジタル詐欺の手口がますます巧妙化、金融サービス業界が APAC で最も標的とされている実態が明らかに

※本リリースは 2026 年 10 月 30 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。

- **APAC の高リスクログイン試行は 3 回に 1 回以上：**アジア太平洋地域におけるログイン試行の 36.4%（3 回に 1 回以上）が高リスクまたは重大リスクと判定されました。
- **AI と自動化による手口の高度化：**攻撃者が長期的な認証情報の窃取から即時の金銭的詐欺（オンライン詐欺がフィッシングを逆転）へとシフトするなど、サイバー犯罪に構造的な変化をもたらしています。
- **金融サービス業界が主要な標的に：**金融サービスが APAC における攻撃活動の 12.5%を占め、AI や自動化を活用した巧妙な攻撃手法が確認されています。

Akamai の新たな調査結果によると、アジア太平洋（APAC）地域全体で Akamai が観測したログイン試行のうち、3 回に 1 回以上（36.4%）が高リスクまたは重大リスクとして判定され、世界平均の 26.6%を上回りました。これは、ラテンアメリカ（37.8%）に次いで世界で 2 番目に高い割合で、北米（23.6%）や EMEA（23.7%）を上回っています。サイバー犯罪者が、企業を日々支えるログインサイトを標的とするケースが増加している中、より強力なアイデンティティ保護の必要性が浮き彫りになっています。

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、「AI 駆動型デジタル詐欺：2026 年詐欺と不正行為レポート」では、サイバー犯罪者がアカウント不正利用の主要な侵入口としてログインの段階をどのように悪用しているかを明らかにしています。世界的に見ると、アカウント検証リクエストは、高リスクまたは重大リスクに分類されるログインアクティビティの 40%を占めており、Credential Stuffing 攻撃（パスワードリスト型攻撃）を開始する前にアカウントの検証を試みた可能性を示しています。これらのリスク分類は、攻撃の成功を示すものではなく、悪性の可能性があるアクティビティを示すものです。

また、本レポートでは、AI や自動化が、従来の境界防御を上回るほど巧妙な手口で不正を可能にし、サイバー犯罪の構造的な変化をもたらしていることを明らかにしています。

- **詐欺がフィッシングを上回る：**世界的なオンライン詐欺の検知件数は前年比で 320 万件から 640 万件へと倍増し、2026 年第 1 四半期には初めて従来のフィッシング件数を上回りました。これは、攻撃者が長期的な認証情報の窃取よりも、即時の金銭的詐欺を優先したためです。

- **攻撃の持続期間が半減：**フィッシングキャンペーンの平均活動期間は、2025 年第 4 四半期の 48.3 日から 2026 年第 2 四半期にはわずか 22 日に短縮され、セキュリティチームが脅威を検知して無効化するための猶予が大幅に短縮されていることがわかります。

金融サービスが APAC で最も標的とされる業界として浮上

金融サービスは APAC における主要な標的として浮上し、銀行（6.4%）とフィンテック（6.1%）を合わせると、観測された攻撃活動の 12.5%を占めました。同地域で観測された主な脅威は、マルウェア、高度な持続型脅威、ランサムウェア、ボットネットです。

また、Akamai の脅威インテリジェンスは、現代の攻撃者がどのようにして総当たり攻撃の自動化と標的型ステルスを組み合わせているかを浮き彫りにしています。2026 年 7 月、研究者らは、APAC の大手金融機関を標的とした、以下の二重の手口による同時攻撃を追跡しました。

- **大規模な偵察行為：**7 日間にわたり 42,000 件の自動リクエストが集中的に送られ、再利用またはその後の乗っ取りを目的として、認証情報データベースを大量に検証するように設計されていた。
- **Low & Slow アカウントの作成：**しきい値に引っかからない程度の通信でレートコントロールを回避し、合成 ID またはマネーロンダリング用口座を確立するために、わずか 164 件のリクエストを精密に設計して送信する試み。

サイバー犯罪者はまた、地域の行動様式に合わせて詐欺の手口をカスタマイズしています。東南アジアでは、研究者らが、旅行関連の検索を利用してユーザーを現地のギャンブルプラットフォームに誘導するキャンペーンに関連する 2,157 件の URL を分析しました。これらのキャンペーンは、暗号資産（仮想通貨）投資家、金融機関、消費者向けブランド、およびコマースビジネスを標的とし、認証情報の窃取、決済詐欺、アカウントの乗っ取りを目的としていました。

Reuben Koh（APJ 地域担当 Director of Security Technology and Strategy）は「詐欺師たちは、人目につかないよう、巧妙に身を隠す術を向上させています。一見すると通常のログイン、新しいアカウント作成、または少額決済であっても、実際にはより大規模な攻撃の一部である可能性があります。AI や自動化により、これらのスキームのスケーリングや巧妙な潜伏が容易になっています。企業にとっての課題は、疑わしい活動が、単体では必ずしも疑わしく見えないという点にあります。組織は、カスタマージャーニー全体にわたって点と点を繋ぎ、不正な意図を早期に特定すると同時に、正当な顧客がシームレスに取引を継続できるようにする必要があります」と述べています。

デジタル詐欺に対する防御の強化

進化する不正手口に対抗するために、Akamai は組織が従来の事後対応型の防御から脱却し、登録や認証から決済まで、アカウントのライフサイクル全体にわたって、意図をベースとしたふるまい検知を採用することを推奨しています。

ボット管理を強化することで、組織は、検知を回避するように設計された小規模攻撃を含め、自動化されたアカウント作成、Credential Stuffing、不正な取引を特定できるようになります。また、組織は、個々のフィッシング

サイトにとどまらず、組織的なキャンペーンにつながる可能性のある共有インフラやふるまいパターンを特定することを目指すべきです。

サイバーセキュリティ、不正防止、ビジネスの各チーム間の緊密な連携も同様に重要です。カスタマージャーニーのさまざまな段階において脅威インテリジェンスを結び付けることで、組織は新たに浮上するリスクを早期に検知し、潜在的な財務損失を軽減し、正当なユーザーの経験を損なうことなく顧客の信頼を守ることができます。

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。

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 では、AI・クラウド・セキュリティの最新トピックや最新情報を 3 分で解説するポッドキャスト「Akamai Tech Insight」を配信しています。ぜひあわせてお聴きください。
URL：https://x.gd/G0bb1m

※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