2026 年 5 月 25 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai による API セキュリティ調査：
AI 関連の API インシデントが最多、
日本企業では 1 件あたり約 2 億 4,600 万円の損害に

APAC 企業の 81%がインシデントを経験、
AI 連携 API の増加で監視・保護が困難になりリスクが増大

※本リリースは 2026 年 5 月 12 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 は、アジア太平洋地域での AI 導入の増加に伴い、API のセキュリティがどのように影響を受けているか、最新の調査結果で明らかにしました。Akamai の API セキュリティの影響に関する調査（APAC 版）では、過去 12 か月間に、APAC 地域の回答者の 81%が API に関するセキュリティインシデントを経験したことが判明しました。金銭的な被害額も同様に目立っており、インシデント 1 件あたりの平均推定コストは、昨年の調査で示された 58 万米ドルよりも急増し、100 万米ドル（約 1 億 5,500 万円※）を超えています。AI によって、攻撃者が攻撃を開始する方法や規模を拡大する方法が変化する中で、盲点が拡大していることが明らかになっています。（※本リリースにおける円換算は、1 米ドル＝155 円で計算しています。）

本調査は、中国、インド、日本、シンガポールのサイバーセキュリティに関する意思決定者 640 人を対象に実施したものです。回答者の 43%は、最も一般的なインシデントの種類として、アプリケーション、エージェント、大規模言語モデル（LLM）などの AI 技術に関連する API 攻撃を挙げています。この調査結果は、持続的な可視性が欠落していることも示しています。自社の API を完全に把握しており、どの API が機微な情報を返すかを理解していると回答したのはわずか 22%にとどまりました。

これらの結果から、デジタル化への意欲とセキュリティへの備えの間のギャップが拡大していることがわかります。企業が AI 対応サービスを急速に展開するにつれ、API の監視、管理、保護が難しくなり、サービスの中断、データの漏えい、運用コストの増加といったリスクが高まっています。

Akamai Technologies のアジア太平洋および日本地域の Director of Security Technology & Strategy である Reuben Koh は「APAC の組織は、AI の利用を急速に拡大していますが、その成長を支えるセキュリティ基盤の多くは、必要な堅牢性を備えていないのも実情です。AI アプリケーションを強化する API が急増し、それが盲点になれば、技術的な分野を超えるリスクの増大につながります。また、大規模なサービス中断、復旧コストの増加、信頼性の低下を招く恐れもあります。API と AI は連携して動作するため、企業は API セキュリティを、実際に信頼できる AI システムを構築する際の中核的な要素として扱う必要があります」と述べています。

APAC 地域に関する調査結果のポイント：

- **APAC では AI 関連の API 攻撃インシデントが最多：**過去 12 か月間に、AI の技術、アプリ、エージェント、LLM に関連する API に関する攻撃を受けたという回答は 43%にのぼりました。
- **インドおよびシンガポールは最多件数のインシデントを報告：**インドの企業の 93%、シンガポールの企業の 90%が、過去 1 年間に API セキュリティインシデントを経験しました。
- **日本ではインシデント 1 件あたりの平均コストが過去最高を記録：**API に関するセキュリティインシデントの平均被害額は、シンガポールでは平均 133 万米ドルであったのに対し、日本では 159 万米ドル（約 2 億 4,600 万円※）に達しました。
- **セキュリティの成熟度が依然として不均一：**回答者の 72%が、API セキュリティへの注力度が前年より増したと回答していますが、API ソフトウェア開発ライフサイクルと CI／CD パイプライン全体にセキュリティテストが完全に組み込まれていると答えたのはわずか 19%でした。

AI 導入の意欲とセキュリティへの備えの間のギャップが拡大

調査対象の 4 つの市場では、全般的に企業は API セキュリティにさらに注力し、所有権を明確にし、テストを強化しています。しかし、AI が実験から拡張展開に移行するにつれ、それによって得られるメリットを一貫した保護に変換するまでに至っていないのが現状です。インシデントの再発が頻繁に発生するのは、特に追跡とセキュリティ確保が困難な API の中でもよく見られることです。これは、急速に増すシステムの複雑さに対して既存のセキュリティ対策が追いついていない現状を示しています。

この調査では、経営幹部の自信と現場における対応状況との間に乖離があることも明らかになりました。全体的なサンプルでは、経営幹部の回答者の 56%が、脅威に対して十分に準備ができている、または完璧に準備ができていると答えています。これに対し、現場の回答者で同様の回答をした割合は 44%に留まっています。これは、現場の運用よりも上層部の自信が先に立っていることを示しています。こうしたギャップが存在すると、AI 主導のサービスがコアビジネス業務に深く組み込まれるようになった際にリスクが高まる要因となります。

可視性とコンプライアンスの重要性を再認識するための警鐘

APAC の回答者のほとんどは、組織が API を規制コンプライアンス要件の要素としていると回答していますが、実際の制御を実証するために必要な手順を実行しているのは、はるかに少ない割合となっています。

実際、API をリスク評価に組み込んでいるのは 63%、報告要件に組み込んでいるのは 40%です。つまり、多くの企業が、運用上の明確さを裏付けるための取り組みを行うことなく、API コンプライアンスについて大枠で議論している可能性があるのです。

APAC の企業にとって、API の可視性が弱いことは、セキュリティの問題だけではなく、AI コンプライアンスの課題でもあります。どのような API が存在し、機微な情報を公開する API はどれか、またそれらのデータフローがどのように保護されているかが明確に把握できなければ、AI 導入の規模拡大に伴い、企業は監視、報告、および説明責任に対する期待の高まりに応えることが困難になる可能性があります。

この調査は、デジタルサービスや AI アプリケーションに API が深く組み込まれるようになった現在、ライフサイクル全体にわたる強力な可視性、ガバナンス、テストの必要性を強調しています。具体的には、API の検出とインベ

ントリの改善、開発と導入の早い段階でのセキュリティチェックの組み込み、API セキュリティを信頼できる AI の前提条件として取り扱うことが推奨されています。

詳細な調査結果と戦略については、こちらからレポート全文をご覧いただけます。
なお、APAC を含むグローバル全体を対象とした調査レポート（英語版）については、こちらからご参照ください。

###

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。