2025 年 5 月 12 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai による API セキュリティの影響調査、APAC の API セキュリティインシデント支出は平均約 8,200 万円に上ったことが明らかに

部門間でのギャップとビジビリティの欠如、不適切な優先順位づけなどによって、企業は多額の API セキュリティインシデントコストに直面

※本リリースは 2025 年 5 月 7 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。

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、アジア太平洋(APAC)地域における 2025 年 API セキュリティ影響調査を発表しました。これは、APAC の主要国におけるアプリケーション・プログラミング・インターフェイス（API）のセキュリティインシデントに起因する隠れた脆弱性、財務への影響、運用上の課題を詳細に調査したものです。本調査によると、API の脆弱性についての認識は高まっているものの、APAC 地域全体で経営陣やセキュリティチームからの API のセキュリティに対するコミットメントは十分とは言えず、その結果、API 攻撃による被害は多額に上っている実態が明らかになりました。自社のサイバーセキュリティにおける API セキュリティの優先順位について早急にコンセンサスを固める必要性を浮き彫りにしています。

中国、インド、日本、オーストラリアの IT およびセキュリティの専門家 800 人超を対象にした本調査では、セキュリティ対策が不十分な API が原因となって企業が直面するリスクが増大していることが鮮明になりました。API は現在のデジタルインフラの基盤となるものですが、同地域の組織の 85%は、過去 12 か月間に少なくとも 1 回、API 関連のセキュリティインシデントが発生したと回答しました。財務への影響も懸念され、調査対象となった市場における API セキュリティインシデントの推定平均コストは 58 万米ドル（日本円でおよそ 8,200 万円）以上に達しています。また、多くの企業では未だに自社の API エコシステムや、漏洩のリスクがあるセンシティブデータに関するビジビリティが不足しています。

Akamai Technologies APAC 担当セキュリティテクノロジーおよび戦略担当ディレクターである Reuben Koh は「API は、ミッションクリティカルになり、モバイルバンキングからコネクテッドカーまで、あらゆることの原動力となっています。しかし、当社の調査では、アジア太平洋地域の組織はそのセキュリティの確保に苦戦している実態を示しています。組織にとって、開発からランタイムまで、クリティカルな API の保護を目的とする包括的なセキュリティ戦略を実施するために、API セキュリティインシデントの根本原因、影響、優先度レベルについて社内でコンセンサスに至ることは極めて重要です」と述べています。

APAC 地域に関する調査結果要点：

● **API セキュリティの優先事項においては中国がリードしているが、依然ギャップが残る：**中国の回答者は、「脅威アクターから API を保護する」ことがセキュリティの最大の優先事項であると回答した唯一のグループでした。ただし、コストの認識についてはばらつきが見られ、経営幹部は API インシデントのコストを 375 万元（51 万 7,000 米ドル）と見積もっているのに対し、現場のセキュリティ担当者は 670 万元近く（92 万 5,000 米ドル）と推定しています。

● **内部の分断が鮮明なインド：**インドの経営幹部の 77%は、API インベントリは十分だと主張していますが、それに同意するアプリケーション・セキュリティの専門家は 41%に過ぎません。この分断は、センシティブデータに対する意識にも及んでおり、アプリケーション・セキュリティチームの中で、どの API がセンシティブデータを返すのかを知っていると回答したメンバーは 11%にとどまりました。

● **日本は、業界のリスクにもかかわらず、API リスク軽視の傾向：**日本のエネルギーおよび小売セクター企業の 96%は最近 API インシデントが発生したと回答したにもかかわらず、API セキュリティのサイバーセキュリティ優先度は 4 位にとどまりました。日本のアプリケーション・セキュリティチームは、「取締役および役員会の評判の毀損」をインシデントが生じた場合の最大の被害と考えています。

● **インシデントから最大の打撃を受けているオーストラリアの対応は最も遅い：**オーストラリアでは、インシデント発生率が 95%と最高で、財務への重大な影響（平均 49 万 3,000 豪ドル）が発生しましたが、総合的な API 脆弱性テストを定期的に実施している組織は最も低く、6%でした。

リスクと対応のギャップ：
本調査によって、4 か国全体で認識と現実に大きなギャップがあることを明らかになりました。

● **経営幹部の認識は高いが、運営上のビジビリティは低い：**APAC 地域の役員の 92%は、過去 12 か月間に API インシデントを経験しましたが、どの API にセンシティブデータのリスクがあるのかを特定できた回答者は全体の 37%に過ぎませんでした。

● **テストは依然として一貫性に欠ける：**インシデント発生率が高いにもかかわらず、リアルタイムで API テストを実施しているとした回答者は、中国で 22%、インドで 15%、日本で 11%、オーストラリアで 6%でした。

Koh は「こうしたギャップは、課題がより大きいことを反映しています。組織は、セキュリティを保護できる以上のスピードで API を実装しており、これが攻撃者に付け入る隙を与えています。」「もはや問題は理論上のものではありません。API の悪用は現在実際に起こっており、財務や評判に被害が出ているのです」「経営陣は、セキュリティとアプリケーション・セキュリティの専門家と密接に連携して、このクリティカルなテクノロジーを保護するために適切なツール、プロセス、アラインメントに投資し、こうしたギャップを解消する必要があります」と述べています。

コンプライアンスの警鐘：
本調査によれば、大半の回答者は API セキュリティを自社のコンプライアンスプログラムで考慮しているものの、それを総体的に行っている組織はほとんどありません。実際、API をリスク評価に組み込んでいるのはわずか 41%、報告要件に組み込んでいるのは 40%です。日本はまた、API 関連のコンプライアンス要件の認識にお

いて、同地域の他国に遅れを取っています。回答者の 22%は、API セキュリティを自社のコンプライアンスの取り組みに取り入れていないと述べています。

中国のデータセキュリティ法からオーストラリアの消費者データ権規制まで、コンプライアンスおよびセキュリティの枠組みに API リスクを取り込むことの必要性は急速に高まっています。デジタル事業の中核をつなぐ重要な役割を果たすようになった API のセキュリティ確保には、熟慮したエンド・ツー・エンドのアプローチが必要です。本調査では、APAC 地域の組織は、持続的なレジリエンスの構築を優先すべきであると提言しています。これには、API の完全なインベントリ作成、API のコードが適切であることを確認するための定期的なテスト、「正常」と「異常な」API アクティビティを見分けるためのランタイム検知の実施などが含まれます。

詳細な調査結果と戦略は、調査の全文をダウンロードしてください。

Akamai では API セキュリティについて、デモを交えて製品紹介を行うセミナーやワークショップを開催しています。詳しくはこちらのページをご覧ください。

# # #

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。