2024 年の API セキュリティの影響に関する調査

金融サービス業界

API インシデントは増加しています。金融サービス業界がどのようにしてこの最も重要なセキュリティの課題に対処しているか、そして安全性を維持するために組織ができることをご確認ください。

昨年、金融サービス企業の 88.7% が、自社のデータを処理して顧客やパートナーを重要なサービスに接続する API に対する攻撃を受けました。脅威アクターはますます革新的な手口を使用して、保護が十分でない API からデータにアクセスし、口座残高や取引履歴などの個人情報や財務情報を窃取する可能性があります。

セキュリティチームはその影響を感じ、改善方法を模索しています。ただし、特に API のような別の攻撃ベクトルへの取り組みは、とてつもなく困難に思えるかもしれません。API の設定が誤っていたりビジネスロジックに欠陥があったりすれば、簡単に発見され、悪用される可能性があります。

なぜそう言えるのでしょうか。Akamai は、最高情報セキュリティ責任者（CISO）からアプリケーションセキュリティ（AppSec）のスタッフまで、1,200 人を超える IT およびセキュリティの専門家を対象に、API 関連の脅威に関する経験についての調査を行いました。

ここでは、API セキュリティインシデントの最大の影響は「規制当局からの罰金」や「チーム／部門に対するストレスやプレッシャーの増大」であると答えた金融サービス業界の回答者に調査結果を絞りました。これらの密接に関連し合った影響については、同業界の専門家たちが API インシデントに対応するためのコストを 832,800 ドルとしたことを考えると、容易に理解できます。このコストは、調査対象の全 8 つの業界の平均を 40% 上回り、他のどの業界よりも高額です。

業界の知見を得るには、詳細を「2024 年の API セキュリティの影響に関する調査」でご覧ください。

攻撃が増加する中、可視性は低下している

業界全体の 84% の組織が API セキュリティインシデントを経験していますが、金融サービス組織が標的にされた割合は 88.7% と、平均よりも高い頻度でした。同業界の専門家たちはこの攻撃の原因となっている主な 2 つの脆弱性を特定しました。それは、ネットワークファイアウォールが脅威を検知できないこと（26.5%）と、大規模言語モデル（LLM）などの生成 AI ツールの API 内の脆弱性（23.2%）です。

頻発するインシデントから高度な是正コストや規制上の罰金まで、API の脅威を示す山のような証拠があるにもかかわらず、Akamai の調査結果は多くの金融サービスチームがまだ API セキュリティを最優先事項にしていないことを示唆しています。実際、API セキュリティは、今後 1 年間のサイバーセキュリティの優先順位の中で 9 位（18.5%）でした。

金融業界にとって、真の API アクティビティと悪性の API アクティビティ、または不正な API アクティビティを区別することは依然として難しく、特に API の多くのリスクを可視化しにくくする要因です。同業界の専門家の 73.5% は API の完全なインベントリを有していると回答していますが、API が機密データを返すことを認識しているのは、その内 28.5% だけです。機微な情報には、カード保有者の信用履歴から大手銀行の顧客の財務記録まで、個人を特定できる情報（PII）やデータが含まれます。

88.7% - 過去 12 か月間に API セキュリティインシデントを経験した金融サービス企業の割合

わずか 28.5% - API の完全なインベントリを有する金融サービス企業のうち、機微な情報を返す API を認識している企業の割合

832,800 ドル - 過去 12 か月間に金融サービス企業が経験した API セキュリティインシデントの財務的影響

影響の上位 3 つ

1. セキュリティチームの**ストレスやプレッシャーの増加**
2. 規制当局からの**罰金**
3. 評判と**信頼の喪失**

出典：
Akamai「API セキュリティの影響に関する調査」（2024）

Akamai

金融サービスプロバイダーの部門や子会社が、その会社の中心的な IT チームやセキュリティチームの協力や監視を受けずに導入したシャドウ API で何が起こり得るかを考えてみましょう。その API は次のような状態になっている可能性があります。

- 顧客の取引データを返すように設計されているが、適切な認証管理がなく、設定ミスに対するテストも適切に行われていない
- 新しいバージョンに置き換えられたが、無効化されていないため、インターネットにさらされたままの状態である
- 管理されていない API を検知できない従来のツールに見過ごされる
- 実際の顧客アカウントにアクセスして資産を窃取しようとするサイバー犯罪者によって悪用される

このようなシナリオは単なる仮説ではありません。LexisNexis® Risk Solutions 社の「2023 True Cost of Fraud™ Study（真の詐欺のコストに関する調査）」によると、不正行為による損失の 50% は新規口座開設の不正利用に遡る可能性があり、詐欺グループは大規模に口座を開設するために API を悪用しています。さらに、これらのシナリオには、実際の IT とセキュリティに挙げられた API インシデントの主な原因が反映されています。

API インシデントがコンプライアンス、ビジネスコスト、チームのストレスに与える影響

2024 年 5 月の「Gartner® API Market Guide for API Protection」によると、「現在のデータは、平均的な API 侵害によって漏えいするデータ量は平均的なセキュリティ侵害の少なくとも 10 倍以上であることを示しています」。広く採用されている PCI DSS v4.0 規制に API セキュリティに関する要件が追加されたのも当然なことです。現在のところ、この基準では、企業はリリース前に API コードを検証し、定期的に脆弱性をテストし、API ベースのコンポーネントの安全な使用を確認することが求められています。これは API によって毎日数百万件もの金融取引を円滑化している業界では特に重要です。

規制当局の信頼を失うことにより、監視が強化され、コンプライアンス要件対応に追われ、すでに疲弊しているチームにさらに大きな負担がかかる可能性があります。また、高額な罰金が科せられる可能性もあります。

それを考慮に入れると、金融サービス企業が API の脅威による影響を十分に認識していることは明らかです。今回初めて、調査対象の 3 か国において、過去 12 か月間に経験した API セキュリティインシデントによる推定の財務的影響を、回答者に尋ねました。

	金融サービス業界	すべての業界の平均
米国	832,800 ドル	591,404 ドル
英国	297,189 ポンド	420,103 ポンド
ドイツ	604,405 ユーロ	403,453 ユーロ

Q3.API **セキュリティインシデントを経験したことがある場合、これらのインシデントの合計財務的影響の推定値はどのようなものでしたか？システムの修理、ダウンタイム、法的費用、罰金、その他の関連費用など、関連するすべての費用を含めてください。**

* Gartner、Market Guide for API Protection、2024 年 5 月 29 日。GARTNER は、Gartner, Inc. またはその関連会社の米国およびその他の国における登録商標およびサービスマークであり、同社の許可に基づいて使用しています。All rights reserved.

プロアクティブな API セキュリティでリスクとストレスを軽減

金融サービス企業に対する API 攻撃の範囲、規模、巧妙さ、コストが増大しています。これには、従来の API セキュリティツールやその他の境界防御を回避するために迅速に適応する、生成 AI を利用したボット攻撃が含まれます。業界の多くのセキュリティチームは、これらの脅威を直接経験し、その財務的および人的な影響を感じています。しかし、組織が API の脅威の重要性を理解していても、それに対して何ができるのか、という疑問が残ります。

API とそれらが交換するデータのセキュリティを確保するために今すぐ対策を講じることで、企業は自社の収益を保護し、セキュリティチームの負担を軽減することができます。これらのステップを行うと同時に、高度な API の脅威に関するチームの知識を深め、そのような脅威に対する防御に必要な機能を構築することで、顧客や取締役会からの信頼を維持することができます。

2024 年の API セキュリティの影響に関する調査をダウンロードいただき、レポートの全文で API の可視性と保護に関するベストプラクティスをご確認ください。

貴社の課題や Akamai が提供するサポートついてのご相談

カスタマイズされた Akamai API Security のデモをリクエスト

Akamai は、本書で取り上げた脅威に関連するリスクを組織が軽減するための支援をするよう設計された次のソリューションを提供しています。

- Akamai API Security は、API の探索、リスクポスチャの把握、ふるまい分析を行い、脅威の侵入を阻止します。
- Akamai Account Protector は、ユーザーのふるまいをリアルタイムで監視し、変化するリスクプロファイルに適応することで、新規口座開設の不正を防止します。

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。Akamai のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携して、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現することが可能になります。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X と LinkedIn で Akamai Technologies をフォローしてください。公開日：2025 年 3 月