2024 年の API セキュリティの影響に関する調査

保険業界

API インシデントは増加しています。保険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。

自動車事故からビジネス機器の損傷まで、災害に見舞われた保険契約者は、デジタルサービスを利用して保険金を請求し、保険会社から支援を受けます。こうしたサービスを支える保険会社の API は、保険契約者のライフストーリーとなる機密情報をデータという形で処理します。

顧客の信頼が最優先される業界において、保険会社は増大するセキュリティ上の課題に直面しています。それは、API の脆弱性です。

Akamai が実施した包括的な調査によると、保険業界の専門家の 76.7% は過去 12 か月以内に API に関するセキュリティインシデントが発生したことを報告しています。財務的な影響は甚大で、保険会社は米国だけでこうしたインシデントに対応するために平均 625,634 ドルを費やしています。

しかし、おそらく最も懸念されるのはビジネスへの影響です。API インシデントの次に保険会社が懸念しているのは、「顧客の信用の喪失や顧客離れ」（28%）です。顧客が保険会社を容易に変更できる競争の激しい市場では、評判の低下は、即時にかかるコストを上回り、長期的な影響をもたらす可能性があります。

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。

攻撃が増加する一方で、可視性は依然として重要な課題に

API 攻撃による金銭的被害は保険会社にとって大きなものであり、米国におけるコスト（625,634 ドル）は、各業界共通の平均コスト（591,404 ドル）を上回っています。こうしたインシデントの原因とは何でしょうか？

保険業界のセキュリティチームによると、主な原因は次のとおりです。

1. 休眠 API や「ゾンビ」API などの管理されていない API（22%）
2. 意図しない形でインターネットに露出している API（21.3%）
3. API セキュリティを保護するために使用されている従来のツールが脅威を発見できていない（20%）
4. 認可の脆弱性（19.3%）
5. API の設定ミス（18.7%）

多くの組織は API 攻撃の原因を認識していますが、リスクの重要な指標である API の応答性（呼び出されたときに機微な情報を返す機能）を可視化できていません。保険会社の 56.7% は、自社の API の完全なインベントリを把握していると答えていますが（全業界平均の 69.7% を下回る割合）、機微な情報を返す API を把握していると答えたのは 20.7% にとどまります。

この可視性のギャップは、規制の厳しい個人データや財務データを処理する業界において、コンプライアンスとセキュリティに重大な影響を及ぼします。

76.7% の保険会社： 過去 12 か月間に API インシデントを経験

わずか 20.7% の保険会社： API の完全なインベントリを把握している保険会社のうち、機微な情報を返す API を把握している割合

625,634 ドル： 過去 12 か月間に米国の保険会社が経験した **API セキュリティインシデントの財務的な影響**

影響の上位 3 つ

1. **顧客の信用の喪失や顧客離れ（28%）**
2. **経営陣における部門の評判の低下（25.3%）**
3. **問題解決にかかるコスト（24.7%）**

出典：
Akamai、「API セキュリティの影響に関する調査」（2024）

Akamai

私たちは、API の保護を困難にするいくつかのトレンドを確認しています。

- **継続的な API スプロール**：あらゆるデジタルイニシアチブにおいて、API が増加し、常に進化しているため、正確なインベントリを維持することが困難になっています。
- **一貫性のない基準**：多くの保険会社では、安全な設計のための統一されたプレイブックに従うことなく、事業部門ごとに複数の開発チームがサイロ化し、業務を行なっています。
- **目に見えないリスク**：API は機密性の高い保険契約者データを送信しますが、ほとんどの組織は機微な情報を返す具体的な API を特定できません。

セキュリティチームの適切な監督なしで、特定の部門が独断で API を展開した場合、何が起こり得るかを考えてみましょう。こうした API は、適切な制御なしでレコードを共有するように構築されているか、システムのアップグレード後にアクティブなまま放置される可能性があり、機密性の高い顧客データの潜在的な流出ポイントになります。

API インシデントがコンプライアンス、顧客の信頼、チームのストレスに与える影響

保険会社が API の脅威がもたらす財務的な結果を十分に認識していることは明らかです。今回の調査では、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コストについて、回答者に尋ねました。

	保険業界	すべての業界の平均
米国	$625,633.70	$591,404.01
英国	£493,000.50	£420,103.18
ドイツ	€ 373,918.72	€ 403,453.26

財務的な影響は大きいものの、調査参加者から明確に聞かれたのは、コストには収益の懸念と評判の懸念が複合的に反映されるということでした。これまでに経験した API セキュリティインシデントの最大の影響を挙げるように求めると、回答は次のような分布になりました。

- 28% が「顧客の信用の喪失や顧客離れ」と回答
- 25.3% が「経営陣および取締役会におけるチームの評判の低下」と回答
- 24.7% が「問題解決にかかるコスト」と回答

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

保険会社に対する API 攻撃の範囲、規模、巧妙さ、コストなどは拡大しています。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と同時に、取締役会や顧客からの信頼を維持できます。これらのステップには、高度な API の脅威に関するチームの知識と、それらに対する防御に必要な機能を構築することが含まれます。

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** : 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** : 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

Akamai Security 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 5 月