2024 年の API セキュリティの影響に関する調査

医療業界

API インシデントは増加しています。医療業界が API セキュリティの課題にどのように対処しているか、そして進化する脅威から防御するために何ができるかをご確認ください。

患者とメンバーの信頼が最優先される業界において、医療機関は、あるセキュリティ上の課題の増大に直面しています。それが、API の脆弱性です。

電子カルテ、遠隔診療、接続された医療機器は、サイバー犯罪者の格好の標的となっています。また、保護されていない API を介してアクセスされた保護対象医療情報（PHI）は、「医療保険の相互運用性と説明責任に関する法律（HIPAA）」違反、患者のプライバシーの侵害、そして信頼の失墜につながり、その信頼回復には何年もかかる可能性があります。

これは非常に大きな課題です。Akamai の包括的な調査では、過去 1 年間に医療の専門家の 84.7% が API セキュリティインシデントを確認したと回答しました。これはすべての業種の平均の 84% をわずかに上回る数字です。

ただし、最も懸念されるのは、信頼に与える影響であると考えられます。医療機関の回答者は、API インシデント後の最大の懸念事項の 1 つとして、「信頼と評判の低下」（28.7%）を報告しています。患者が受診する医療機関を容易に変更できる現状では、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、可視性に関する懸念も増大

API 攻撃による金銭的損害は甚大で、医療機関はこれらのインシデントに対処するために平均で 510,600 ドルを費やしています。

こうしたリスクにもかかわらず、データでは、懸念事項の優先順位においてギャップがあることが明らかになっています。医療機関に、今後 12 か月間のサイバーセキュリティの優先事項について尋ねたところ、「脅威アクターからの API を保護」は 12 の選択肢のうち 11 位（16.7%）でした。代わりに、「システムにアクセスするスタッフの認証の保護」（24.7%）と「開発者の秘密の管理」（22.7%）に重点を置いています。

医療機関が正当な API アクティビティと悪性の API アクティビティを区別することは、依然として困難です。同業者の 65% が API の完全なインベントリを有していると報告している一方で、機微な情報を処理する API を特定できるのはこのうちのわずか 24% です。これは 2023 年の 40% から低下し、懸念すべき数字です。医療分野では、データプライバシーの重要性は法的義務にまで及ぶため、可視性におけるこうしたギャップは大きなリスクを生み出します。

中央 IT チームやセキュリティチームの適切な監督なしに臨床部門によって展開された API に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。

- HIPAA に準拠した適切な制御を使用せずに患者レコードを共有するように構築されている
- システムのアップグレード後もアクティブ状態のままになっており、未知のアクセスポイントが存在する
- 管理されていない API を検出するように設計されていない、従来のセキュリティツールでは検知できない
- 攻撃者から悪用され、保護対象医療情報にアクセスされる
- 認証済みのパートナーから悪用され、意図しないユースケースでエンドポイントが使用される

84.7% の医療機関が過去 12 か月間に API インシデントを経験

65% の医療機関が API の完全なインベントリを有しているが、どの API が機微な情報を返すのか把握しているのはこの内わずか 24%

510,600 ドル - 過去 12 か月間に医療機関が経験した 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. **信頼と評判の低下**（28.7%）
2. **生産性の低下**（28.7%）
3. **社内精査の増加**（27.3%）

出典：
Akamai「API セキュリティの影響に関する調査」（2024）

Akamai

このようなシナリオは単なる仮説ではありません。医療データの漏えい件数が過去最高を記録し、1 回のデータ漏えいの被害額が平均で 488 万ドル[1] に達する中、API の脆弱性は、コンプライアンスやセキュリティのリスクを高める要因として注目されています。さらに、これらのシナリオには、同業者が挙げた 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® Market Guide for API Protection[2] では、「現在のデータは、平均的な API 侵害によるデータ漏えいの被害額が平均的なセキュリティ侵害の 10 倍以上であることを示している」と説明しています。

HIPAA コンプライアンスにおいて、API セキュリティの重要性が増してきたため、その対策に焦点を当てることは当然と言えるでしょう。HIPAA では API について明示的に言及していませんが、従業員の役割に基づいて PHI へのアクセスを制限する必要があります。これには、患者データを送信する API の認証とアクセス制御が必要です。医療機関と医療保険企業、およびその規制当局は、自組織の API だけでなく、パートナーやサプライヤーの API を介してどのようなタイプのデータが受送信されているかを把握する必要があります。これは、医療セクターのサードパーティリスクを管理するためのもう 1 つの課題となります。

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。こうしたことを考慮に入れると、医療機関が API の脅威による経済的な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コストについて、回答者に尋ねました。

	医療業界	すべての業種の平均
米国	510,600 ドル	591,404 ドル
英国	363,885 ポンド	420,103 ポンド
ドイツ	643,884 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。**

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、費用以上の負担があるということでした。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られたとき、挙げられたのは費用ではありませんでした。前述のように、回答者は「信頼と評判の喪失」（28.7%）と「生産性の低下」（28.7%）を強調しました。このような結果は長期的な影響をもたらします。患者からの信頼が失墜すると、将来の収益が損なわれるおそれがあります。一方、すでにストレスを抱える医療機関のスタッフの生産性が低下すると、疲労が増大して離職者が増える可能性があります。

[1] IBM データ漏えいのコストに関するレポート（2024 年）
[2] 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

医療機関に対する 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 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。当社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 および LinkedIn で Akamai Technologies をフォローしてください。公開日：2025 年 3 月。