2024 年の API セキュリティの影響に関する調査

政府機関

API インシデントは増加しています。政府機関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。

世界中の政府機関は、API 優先時代におけるデジタルサービスのセキュリティ確保に対する圧力にさらされています。2024 年には、公共部門組織の 86.1% が API セキュリティインシデントを報告しました。これは、前年の 76.8% から大きく増加しています。この増加により、公共部門は業界全体の平均（84%）を上回り、課題の規模が拡大していることを浮き彫りにしています。一般データ保護規則（GDPR）の要件を満たすことから、マルチクラウドシステム全体でデータの常駐を実施し、セキュリティ上の脅威に対処することまで、政府系機関は可視性の向上、ガバナンスの強化、および組み込みの回復力に対する普遍的なニーズに直面しています。

政府機関の API セキュリティインシデントの真のコスト

政府機関は、デジタルサービスの実現、機関間のデータ共有の促進、インフラの最新化のために API を採用するようになっています。しかし、この傾向は、脅威アクターが悪用したいと考えるような新たな脆弱性を数多く生み出しています。不十分な認証メカニズム、API の設定ミス、重要なリスク指標の認識不足により、政府機関は API セキュリティ侵害の影響を特に受けやすくなっています。このようなインシデントの影響は、データ窃盗にとどまらず、業務の継続性、規制の遵守、公共の信頼にリスクをもたらすなど、広範囲に及びます。

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からアプリケーションセキュリティのスタッフまで、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。

政府機関への調査をまとめた結果がこちらです。回答によると、API セキュリティインシデントの主な影響は次のとおりです。

- 「チームや部門のストレスやプレッシャーの増加」（28.5%）
- 「シニアリーダーや取締役会からの部門への評判が低下」（27.2%）
- 「規制当局からの罰金」（25.2%）

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 717,500 米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 21.3% 上回っています。

業界特有の知見を得るには、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。

攻撃が増加するにつれ、可視性に関する懸念も増大

API セキュリティインシデントの主な原因を挙げるよう求められたとき、同業界の専門家たちは 2 つの主要な脆弱性を特定しました。

- API 認証制御の欠如（25.2%）
- API のセキュリティ保護に使用される従来のツール（25.2%）

Akamai の調査は、API の脅威による高額の修復コストや信頼の低下など、深刻な影響を指摘していますが、政府機関チームの多くが API セキュリティを最優先事項として位置づけていないことを明確に示しています。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 6 位（17.9%）でした。

政府機関の 86.1% が、2024 年に API セキュリティインシデントを経験したと報告しています。これは 2023 年の 76.8% から大幅に増加しています

米国の政府組織における API セキュリティ侵害の平均的な経済的コストは 717,500 ドルであり、全産業の平均額である 591,404 ドルを上回っています

政府機関の 66.9% が API インベントリを保有している一方、機微な情報を取り扱う API を完全に把握しているのは 18.5% に過ぎず、重要な情報がリスクにさらされています

影響の上位 3 つ

1. セキュリティチームのストレスとプレッシャーの増加
2. 指導者や取締役会におけるチームの評判の低下
3. コンプライアンス違反による罰金

出典：
2024 年の API セキュリティの影響に関する調査

政府機関の場合、API 攻撃のコストは、財務的影響および人的影響を含めて急激に増加しています。セキュリティ侵害により、リーダーシップレベルで信頼が失われると、監視の強化、業務の中断、コンプライアンス要件の遵守に苦労しているチームの作業負荷が増える可能性があります。

Akamai

民間企業と同様に、政府機関も、API のアクティビティが本物か悪性かを区別することは困難です。これは、API の脆弱性がどこにあるのかを正確に可視化できていないことが一因です。同業界の専門家の 66.9% 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 が機微な情報を返すことを認識しているのは、その内の 18.5% だけです。機微な情報には、国民識別番号、生体認証データ、連絡先情報など、個人を特定できる情報（PII）が含まれます。

政府組織の省庁や補助機関が、その組織の中心的な 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認証されていない API を導入した場合、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。

- 適切な認可管理を行わずに市民の個人データや財務データにアクセスできるように設計されており、機密情報が漏えいする可能性がある
- 新しいバージョンに置き換えられたが、適切に廃止されていないため、古いエンドポイントが悪用される可能性がある
- 中央の IT チームとセキュリティチームが見えない範囲で運用し、従来の監視ツールとコンプライアンスチェックを回避している
- 攻撃者によって政府システムに不正アクセスされ、データ漏えい、アイデンティティの盗難、金融詐欺などの問題が生じるおそれがある

これは単なる仮定ではありません。米国政府機関のサイバーセキュリティの現状は、大きな課題となっています。Cybernews Business Digital Index によれば、多くの政府系機関や省庁は、堅牢なセキュリティポスチャを維持することに苦労しています。4 割近く（38.8%）がセキュリティ評価において「重大なリスクがある」という評価を受けており、75% がデータ漏えいを経験しています。

これらの統計は、政府機関のセキュリティチームが直面している、ミッション目標、レガシーシステム、進化する脅威のバランスを取りながら、独自の制約や監視の下で運用する必要があるという複雑な現実を反映しています。特に API セキュリティの分野では、こうした課題が深刻化しているため、政府機関は、特定の要件を理解し、政府環境に合わせたソリューションを提供できるパートナーを必要としています。

API インシデントが信頼性、費用、チームのストレスに与える影響

API 攻撃の頻度とコストを考慮すると、API のセキュリティ保護が世界中の政府機関の優先事項となっていることは当然です。米国では、General Services Administration が管理する Data.gov イニシアチブが、一貫性、セキュリティ、相互運用性を向上させるために、連邦政府機関全体の API を標準化しています。EU と英国のオープン・データ・フレームワークから、アジア太平洋地域と中東地域のデジタル変革イニシアチブまで、世界中で同様の取り組みが行われています。政府機関は、安全でシームレスなデータ交換を実現するために標準化された API を採用しています。

これらの取り組みの多くは、EU の GDPR、オーストラリアの Notifiable Data Breaches スキーム、日本のマイナンバー法などの地域の規制に沿っています。共通の標準とフレームワークを施行することにより、各国の政府機関は、サードパーティの統合や不正アクセスによるリスクを軽減しながら、データ交換のセキュリティ確保に取り組んでいます。

	政府機関	すべての業界の平均
米国	$717,500.50	$591,404.01
英国	£378,140.69	£420,103.18
ドイツ	€296,975.79	€403,453.26

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。**

政府機関が API の脅威の結果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。

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。先に述べたように、上位 2 つの回答は「チームや部門のストレスやプレッシャーの増加」、「シニアリーダーや取締役会からの部門への評判が低下」でした。

これらの影響は、長期的に残ります。セキュリティ侵害は信頼を損ない、将来の資金供給や国民の信頼を脆弱にするおそれがあります。同時に、すでに負担の大きい機関における生産性の低下によって、職員は疲労を抱え、エンゲージメントが低下する可能性があります。

しかし、この圧力は一部の地域に限定されたものではありません。このレポートは特定の市場を対象としてはいますが、アジア太平洋地域、ラテンアメリカなどの公的機関がデジタルインフラのセキュリティを確保し、コンプライアンス基準を満たし、進化する脅威から機微な情報を保護するという同様の課題に直面しているため、API セキュリティは世界中の公共機関にとって重要な問題となっています。

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

政府機関に対する API 攻撃の範囲、規模、巧妙さ、費用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、組織は収益と機微な情報を保護し、セキュリティチームの負担を軽減すると同時に、取締役会や政府関係者からの信頼を維持できます。これらの対策には、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

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