API セキュリティの影響に関する調査 2024

API インシデントが貴社と貴社のチームに与える影響

Akamai

Akamai の「インターネットの現状（SOTI）」レポートの関連出版物

目次

エグゼクティブサマリー

今年で 3 年目となる「API セキュリティの影響に関する調査」（旧称「API セキュリティの断絶レポート」）は、米国、英国、ドイツ（2024 年から参加）のリーダーと現場の担当者 1,207 人の調査に基づいて、API 保護の現状を探究しています。この調査では、企業が API セキュリティイベント（頻度、原因、影響）をどのように体験しているか、またセキュリティ部門が攻撃ベクトルとしての API にどのように対応しているかについて検証します。

全体像を把握するために、以下のバランスの取れた対象に調査を実施しました。

500 人未満から 1,000 人以上の規模の組織に所属する、最高情報セキュリティ責任者（CISO）、最高情報責任者（CIO）、最高技術責任者（CTO）、シニアセキュリティ担当者、アプリケーションセキュリティ（AppSec）チームメンバー

8 つの業界：金融サービス、小売／ E コマース、ヘルスケア、政府／公共部門、製造、エネルギー／公益事業、（2024 年から追加）自動車および保険

はじめに

API は、広く蔓延し被害をもたらしているというデータが存在するにもかかわらず、新しく出現しつつある攻撃ベクトルと見なされることがよくあります。次の統計を見てください。

- Akamai の最近の「インターネットの現状（SOTI）」レポートによれば、2023 年 1 月から 2024 年 6 月にかけて 1,080 億件の API 攻撃が記録されています。
- 2024 年 5 月の「Gartner® Market Guide for API Protection」によれば、「現在のデータは、平均的な API 不正使用が平均的なセキュリティ侵害の 10 倍以上のデータ漏えいにつながることを示唆しています *」。
- 攻撃も増加しています。SOTI では、Web アプリケーションおよび API 攻撃の合計が 2023 年第 1 四半期から 2024 年第 1 四半期の間に 49% 増加したと報告されています。

多くの API は保護が十分でないため、サイバー犯罪者にとって魅力的でコスト効果に優れた攻撃ベクトルとなっています。

このような増加は驚くことではありません。API は、水面下でデジタルイニシアチブを推進するほぼすべてのテクノロジー間の通信を促進し、データを交換しています。たとえば、生成 AI ツール、顧客対応アプリ、クラウドサービスなどのテクノロジーです。しかし、多くの API は保護が十分ではありません。認証なしの設計や設定ミス、あるいは完全に忘れられている場合もあります。このため、サイバー犯罪者にとって魅力的でコスト効果に優れた攻撃ベクトルとなっています。必要なのは脆弱な API を 1 つ見つけるだけです。**たったそれだけで**、その API が呼び出されたときに返す全てのデータに直接アクセスできるようになり、それは何千件ものレコードである場合もあります。

大局的には、当社の調査によって明らかになったのは、API セキュリティはまだ包括的なセキュリティ戦略の主要な要素になっていないということです。組織の多くは API 脅威を新しいものとして扱っていますが、攻撃データや当社の調査で明らかになった金銭的影響やチームへのストレスは、これらの脅威が数を増やし、しばしば成功していることを示しています。当社の 2024 年の調査結果は、API セキュリティインシデントが、皆様の同業者やその組織にどのような影響を与えているかを垣間見る機会を提供しています。このデータを、お客様のチームが API 保護を適切に評価し、必要に応じて改善するための体制を整えるのに役立てていただければ幸いです。

大局的な発見事項：API インシデントはビジネスに影響し、チームにストレスを与える

当社の 2024 年の調査結果は、API が増加を続ける攻撃ベクトルであり、チームにとって相当なセキュリティ上の課題を生み出していることを示しました。回答者は以下の点について驚くべき一致を示しました。

- API セキュリティインシデントが 3 年連続で増加している
- API 関連のインシデントに対応して回復するために、平均 50 万ドル以上を費やしている（米国の経営幹部の回答者によると金銭的影響の平均額は 94 万 3,162 米ドル）
- API インシデントによる人的損害を感じており、チームへのストレスや評判悪化の影響（特にこの圧力を増幅する社内精査）は、インシデント修復のコストより上位に挙げられている

回答者は、自社の API インベントリの完全性についてさまざまな見解を示しました。このばらつきは役職別に分類するとさらに顕著でした（11 ページ参照）。驚くべきことに、完全な API インベントリを有し、どの API が機微な情報を返すかを把握している企業の割合は、すでに低かった 2023 年の 40% から 2024 年にはわずか 27% にまで減少しました。

回答者は、API を保護するために利用している従来のツールがリスクを完全にはカバーしていないことも示しました。これらのツール、たとえば Web アプリケーションファイアウォール（WAF）、API ゲートウェイ、ネットワークファイアウォールなどは、攻撃成功の原因として槍玉に上がることがよくあります（原因の完全なリストは 17 ページ、WAF と WAAP に関する注は 12 ページを参照）。

また、今回の調査結果から、API セキュリティ戦略に注目すべき根拠があるにもかかわらず、なぜ高い優先順位が与えられていないのかについて、いくつかの理由を推測することができます。一つの大きな要因は、保護が必要な API の数、場所、リスク属性について、主要なセキュリティ役職間で認識が一致していないことです。これは、おそらく API の可視性が悪く、信頼できる唯一の情報源が存在しないためだと考えられます。

また、API 攻撃の原因について、セキュリティリーダーと現場の間で合意が得られていないことも判明しました。さて原因は、使用しているツール、開発時のコーダーのミス、生成 AI イノベーションの抜け穴に対する攻撃のうちどれでしょうか？答えは誰に話を聞くかによって変わります。

もちろん、API セキュリティが戦略的にあまり重要視されないもう一つの理由は、チームがすでに差し迫った他の脅威に対応するのに手一杯であり、それらの脅威に予算、チームの注意力、労力の大半が奪われている可能性が高いためです。結果を詳しく見てみましょう。

セキュリティ専門家は API インシデントによる人的損害を感じており、チームに対するストレスと評判低下の影響がインシデント修正のコストより上位に挙げられています。

API セキュリティの影響に関する調査 — 2024
主な調査結果のスナップショット

84% 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回答者の割合

過去 12 か月間の API インシデントに対応するための平均コスト：

米国	英国	ドイツ
$591,404	£420,103	€ 403,453

低い可視性
完全な API インベントリを備え、どの API が機微な情報を返すかを把握している企業はわずか 27%（2023 年の 40% から低下）

高いストレス
API インシデントの最も大きな影響 *CISO*：シニアリーダーや取締役会からの部門への評判が低下
CIO：チームや部門に対するストレスやプレッシャーの増加

テスト不足
API の開発から本番までの間に、API のテストをリアルタイムで行っている回答者は 13%、毎日テストしている回答者は 18% しかいませんでした。

API セキュリティインシデントの財務コストは、チームやリーダーへの影響を悪化させます。高額な被害をもたらすセキュリティ侵害は精査の対象となり、取締役会のような影響力のあるステークホルダーに対して、チームが仕事を上手くこなしていないように見える可能性があります。これはストレスになります。実際、参加者は地域を問わず、API セキュリティインシデントの最大の影響として、チームに対するストレスを挙げています。

API セキュリティの現状

過去 3 年間に、API セキュリティインシデントを報告している組織の数は増加を続け、2024 年には 84% に達しています（以下を参照）。これらの API 攻撃は組織にどのような影響を与えるでしょうか？リスクを軽減するために、組織は何をしているのか、または、まだしていないのでしょうか？当社の調査結果を、これらの質問に対する回答として構成しました。

API 攻撃は組織とそのセキュリティチームに大きな影響があるか？

簡単に答えるなら、「はい」です。API セキュリティインシデントの金銭的影響に関するデータを収集したのは今年が初めてです。この影響はかなりの額になることが判明し、過去 12 か月間に API インシデントを経験した 84% の組織の API インシデント修復のための平均コスト（システム修理、ダウンタイム、法的手数料、罰金、その他の関連費用を含む）は次のとおりです。

- 米国：**$591,404**
- 英国：**£420,103**
- ドイツ：**€ 403,453**

一部の役職はコストをはるかに高く見積もっており、特に米国の経営幹部の回答者は、94 万 3,162 ドルと報告しています。これは米国の回答者全員の平均を 60% 近く上回っています。

過去 12 か月間に API セキュリティインシデントを経験しましたか？

年	合計	米国	英国	ドイツ
2022	76%	75%	77%	—
2023	78%	85%	69%	—
2024	84%	83%	83%	84%

正確な数字が何であれ、API セキュリティインシデントの財務コストは人的影響を悪化させます。高額な被害をもたらすセキュリティ侵害は精査の対象となり、取締役会のような影響力のあるステークホルダーに対して、チームが仕事を上手くこなしていないように見える可能性があります。これはストレスになります。実際、参加者たちは地域を問わず、API セキュリティインシデントの最大の影響として「ストレス」（特にチームにかかるストレス）を挙げました。次いで「シニアリーダーや取締役会からの部門への評判の低下」が続き、3 番目に「修復コスト」が挙げられました。とりわけ、士気に最も影響を与える社内への影響は再度出現し、影響の下位 3 つをほぼ同率で独占しています（以下参照）。

結果は業界別に分類しても同様でした。「API 侵害後のチームに対するストレスやプレッシャーの増加」は、調査した 8 つの業界のうち 4 つで影響の 1 位に挙げられています（9 ページのサイドバーを参照）。これには金融サービスも含まれており、金融サービスは全業種の中で金銭的影響が最も大きく、83 万 2,801 米ドルを報告しています。

API セキュリティインシデントの主な影響

1. チームや部門のストレスやプレッシャーの増加 – **27.0%**
2. シニアリーダーや取締役会からの部門への評判が低下 – **26.6%**
3. 問題解決のためにコストが発生 – **25.8%**
4. 規制当局からの罰金 – **25.4%**
5. 顧客の善意の喪失とアカウントの解約 – **25.0%**
6. 生産性の低下 – **24.1%**
7. 信頼と評判の低下 – **23.8%**
8. 従業員の善意の喪失 – **23.8%**
9. 事業部門によるチームや部門への社内精査の増加につながった – **23.5%**

回答の元になった質問：*API* セキュリティインシデントがビジネスにもたらしたコストや影響が何かあれば、それは何ですか？
（*3* つまで選択可）、 *n = 1,207*

API インシデントの影響についての IT およびセキュリティリーダーの回答から（各回答者は最大 3 つまで選択可能でした）、API 攻撃の金銭的コストと人的コストの関係も明確に浮かび上がりました。地域や役職を問わず全般的に合意が見られた一つの領域は、API セキュリティインシデントの最大の影響はスタッフに対する影響であるということでした。

- CISO から報告された上位 2 つの影響（「シニアリーダーや取締役会からの部門への評判が低下」と「顧客の善意の喪失とアカウントの解約」）は、人的影響と金銭的影響がともに 31% で完全な同率となりました。
- 同様に、CIO から報告された上位 2 つの影響は、「チームや部門に対するストレスやプレッシャーの増加」と「修復コスト」で、ともに 34% で同率でした。

これらの結果は、CISO と CIO にとって納得できるものです。彼らが率いるチームが、劣悪な労働環境を生み出し、予算を大幅に超過させ、顧客を怒らせるようなセキュリティインシデントに繰り返し見舞われたらどうなるでしょうか？リーダーたちは、優秀な人材が去っていくことや、部門の評判が急落することを望んでいません。それに加えて、修復コストや顧客離れなどの金銭的圧力が加わると、CISO と CIO にかかるストレスは著しく高まります。実際に「顧客の善意の喪失とアカウントの解約」は、保険業界と自動車業界の両方の回答者によって、API セキュリティインシデントの影響の 1 位に挙げられました（業界ごとの詳細な調査結果については、次のページのサイドバーを参照）。

残りの役職の 1 位の回答は次のとおりです。

- CTO、30%、「従業員の善意の喪失」
- シニアセキュリティ担当者、27%、「シニアリーダーや取締役会からの部門への評判が低下」
- AppSec チーム、31%、「チームや部門に対するストレスやプレッシャーの増加につながった」

業界別 API セキュリティインシデントの主な影響	
自動車	顧客の善意の喪失とアカウントの解約 – **33%**
エネルギー／公益事業	シニアリーダーや取締役会からの部門への評判が低下 – **36%**
金融サービス	同率：チームや部門へのストレスやプレッシャーの増加につながった + 規制に基づく罰金 - どちらも **29%**
政府／公共部門	チームや部門へのストレスやプレッシャーの増加につながった - **29%**
ヘルスケア	同率：信頼と評判の低下 + 生産性の低下 – どちらも **29%**
保険	顧客の善意の喪失とアカウントの解約 – **28%**
製造	チームや部門へのストレスやプレッシャーの増加につながった - **34%**
小売／ E コマース	チームや部門へのストレスやプレッシャーの増加につながった - **29%**

回答の元になった質問：*API* セキュリティインシデントがビジネスにもたらしたコストや影響が何かあれば、それは何ですか？
（*3* つまで選択可）、 *n = 1,207*

API と潜在的なリスクに対する十分な可視性があるか？

いいえ。実際には悪化しています。今年、完全な API インベントリを有し、かつどの API が機微な情報を交換しているかを把握している参加者の割合は、すでに低い 2023 年の 40% から 2024 年にはわずか 27% にまで低下しました（もし、多くの組織は完全なインベントリを作成しようとしているが、すべての API を特定し、各 API 内のアクティビティを把握するためのツールが欠けていると考えるならば、この調査結果には良い面があるかもしれません）。

完全な API インベントリを有し、かつどの API が機微な情報を交換しているかを把握している参加者の割合は、**すでに低い 2023 年の 40% から 2024 年にはわずか 27% にまで低下**しました。

API インベントリの現状と意識、全回答者

	2024	2023
はい。そしてどの API が機微な情報を返すのかを**把握している**	27%	40%
はい。しかしどの API が機微な情報を返すのかを**把握していない**	43%	32%
API の部分的なインベントリがあり、どの API が機微な情報を返すのかを**把握している**	23%	24%
API の部分的なインベントリがあるが、どの API が機微な情報を返すのかを**把握していない**	6%	4%
いいえ。インベントリは**一切ない**	1%	—

回答の元になった質問：貴社に *API* の完全なインベントリはありますか？
また、どの *API* が機微な情報を返すのか把握していますか？（*5* つの選択肢から選択）、 *n = 1,207*

調査対象となった 3 か国 8 業界のリーダーたちの回答を見ると、CIO は CISO に比べ、自社に完全な API インベントリがあると考えている傾向が大幅に高くなっています。実務レベルでは、シニアセキュリティ担当者も AppSec チームメンバーも、すべての API が把握されているという平均的な CIO の見解におおむね一致しています。

しかし、どの API が呼び出されたときに機微な情報を返すかを知っているかどうかについて、5 つの役職の平均的回答を比べるとどうなるでしょうか？この回答は重要です。これらの呼び出しの多くは悪意のあるソースから発信され、よくある API の脆弱性を悪用しようとしているからです。

攻撃者がデータアクセスの標的にする 4 種の未管理 API

1. **シャドウ API**（文書化されていない API）は、組織内の公式の監視チャネルの外に存在し、稼働しています。
2. **不正な API** は、システムやネットワークにセキュリティリスクをもたらす不正な API や悪性の API です。
3. **ゾンビ API** には、新しいバージョンの API や完全に別の API に置き換えられた後も稼働したままになっている API が含まれます。
4. **非推奨の API** は、API が変更されたために使用を推奨されなくなった API です。

これらの調査結果は、API リスクに対する可視性について興味深い論点を提供しています。CISO と CTO の大部分は、完全なインベントリはあるがどの API が機微な情報を返すかを**知らない**（この知識を「機微な情報の知識」と呼ぶことにします）、または部分的なインベントリがあり機微な情報の**知識もある**と回答しました。

CIO の大半は API の完全なインベントリがあると報告しており、それらの CIO のうち 42.9% は機微な情報の完全な知識もあると回答しています。36.3% は、その知識はないと回答しています。シニアセキュリティ担当者は CIO と一致していましたが（75% が完全なインベントリを報告）、機微な情報の知識に関しては**逆の結果**になりました。シニアセキュリティ担当者の 32.5% は機微な情報の知識があると回答し、42.5% はないと回答しました。

最後に、すべての回答者の中で最も現場に近い AppSec のスタッフメンバーが、5 つの役職すべての中で単独で最大の多数派を占めました。ほぼ半数が機微な情報の知識のない完全なインベントリを報告しました。残りの半数はおおむね次の 2 つに分かれました。

- 完全なインベントリと機微な情報の完全な知識
- 部分的なインベントリとそれらの API の機微な情報の完全な知識

インベントリの測定は、API カウントの単一の情報源ができるほど十分に標準化されていないことが分かります。このような変動性を考慮すると、完全なインベントリがあ企業の多くは、機微な情報の完全な知識が**ない**可能性があります。機微な情報を返す API を把握することは、常に非常に重要です。しかし、部分的なインベントリは最も危険である可能性があります。なぜなら、シャドウ API、不正な API、ゾンビ API、非推奨の API は標的にされやすく、保護が不十分で、通常は従来のセキュリティツールから漏れてしまうからです。

API インベントリの現状と意識、役職別

	CISO	CIO	CTO	シニアセキュリティ担当者	AppSec
完全なインベントリがあり、どの API が機微な情報を返すのかを**把握している**	17.2%	42.9%	16.5%	32.5%	26.4%
完全なインベントリがあるが、どの API が機微な情報を返すのかを**把握していない**	41.4%	36.3%	34.8%	42.5%	47.4%
API の部分的なインベントリがあり、どの API が機微な情報を返すのかを**把握している**	32.5%	15.4%	39.9%	18.3%	20.4%
API の部分的なインベントリがあるが、どの API が機微な情報を返すのかを**把握していない**	8.3%	5.5%	8.2%	5.8%	5.2%

回答の元になった質問：貴社に *API* の完全なインベントリはありますか？また、どの *API* が機微な情報を返すのか把握していますか？
（*5* つの選択肢から選択）、*n = 1,207*

未管理の API が無秩序に増殖し、従来のセキュリティツールでは把握が難しいことが判明している現在、これらの調査結果は、API 攻撃ベクトルが攻撃者にとって魅力的に見える共通のセキュリティギャップを明らかにしています。

もちろん、未管理の API は、少なくとも 5 つは存在する、セキュリティチームが確認して評価する必要がある API 属性の 1 つにすぎません。これらの API 属性は次のとおりです。

- パッチが適用されていない**既知の脆弱性を持つ API**
- **管理されていないか忘れられている API**（シャドウ、不正、ゾンビ、非推奨）
- **外部への露出のある API**（資格情報、キー、制御外の変数など）
- **演算子エラーのある API**（インフラとサービスのセキュリティ設定ミス）
- 攻撃者が特定し悪用できる**未発見の脆弱性やバグを含む API**

少なくとも、API インベントリと API の脆弱性に対する可視性に関する役職間の回答の幅は以下のことを示唆しています。

- 企業は依然として、API（特に高リスクの未管理 API）の探索とセキュリティの確保に特化して設計されていないセキュリティ製品を利用しています。
- セキュリティ部門は、確認と評価が必要な API のリスク属性をまだ定義しておらず、また、API の探索とインベントリ作成の戦略について、多岐にわたる事業部門、開発チーム、ベンダーの間で合意を形成できていません。

このような断絶に対処することは、すべての API のセキュリティを確保するための強力な機能への投資を効果的に主張するための第一歩となるでしょう（18 ページの「API セキュリティ体制の成熟に近付く方法」を参照）。現状では、API セキュリティの予算を獲得するために必要な焦点と主張が整っていないことが多いため、API や Web アプリの防御だけでなく、組織全体のセキュリティ体制を向上させるようなイニシアチブを優先し、資金を調達することが難しくなっています。

連携による強化：WAAP + API 固有の保護

複数の攻撃ベクトルからの脅威を迅速に特定し、緩和するために設計された Web アプリケーションと API の保護（WAAP）は、従来の WAF の保護機能を拡張します。**API セキュリティソリューションが連携して機能することで、ファイアウォールを超えて保護を拡張し、可能な限り最強の防御を実現します。**

API は悪用や侵害のリスクを軽減するのに十分な頻度でテストされているか？

いいえ、十分な頻度ではありません。外部公開されている API で、設定ミスがあるもの、認証制御が不十分なもの、コーディングエラーが埋め込まれているもの、あるいはその他の予防可能なリスクを抱えているものは、まさに攻撃者が探し求めているものです。そして攻撃者はそれらを見つけることがますます上手くなっています。

そのため、開発チームが包括的なテストを行わずにこのような API を本番環境に送り出すたびに、意図せずセキュリティチームの将来の作業負荷の種を植え付けていることになります（その作業負荷は間違いなく緊急性が高く、今回の調査結果で明らかになったストレスの一因となっています）。

予防可能なリスクと書いた点に注意してください。

API を本番環境にリリースする前に、自動化を手段として開発段階でテストを頻繁かつ効率的に実施することは、組織全体、開発チーム、セキュリティチームにとって大きなメリットとなります。そしてそのメリットは、未知の脆弱性に対する不安を軽減し、本番環境で発見されると修正がはるかに困難で高コストとなるようなエラーを防げるという点で、即座に効果を実感できます。

ところが、調査結果によれば、これまでのところテストの普及は思うように進んでいません。頻繁な（リアルタイムおよび毎日）API テストを実施している回答者の割合は、本番環境を含む API ライフサイクル全体で昨年から低下しました。

- 2023 年には、米国と英国の回答者の 18% がリアルタイムでテストしたと回答しています。同じ調査対象グループで、**2024 年にその数字は 13% に低下**しました。
- 2023 年には、米国と英国の回答者の 37% が少なくとも 1 日 1 回はテストを実施したと回答しています。**2024 年には、この頻度でテストした回答者はわずか 13%** でした。ただしドイツの回答者は、26% が 1 日 1 回テストしています。

API を本番環境にリリースする前に、自動化を手段として開発段階でテストを頻繁かつ効率的に実施することは、組織全体、開発チーム、セキュリティチームにとって大きなメリットとなります。

週 1 回の API テストは、地域を問わず参加者の間で最も一般的ですが、50% に達した地域はありませんでした。さらに API テストの頻度は、**リアルタイム**から**まったく実施しない**まで、地域を問わず幅が非常に大きくなっています。注目すべきは、「API のセキュリティをテストするのは本番環境にリリースする前だけ」と回答した回答者がわずか 6% である点です。理想的には、チームは API ライフサイクル全体を通した継続的なテストに移行するべきです。

API を継続的にテストするとはどういう意味か？

API の脆弱性は、ライフサイクルのどの段階でも発生する可能性があります。開発中のコーディングエラーから、ユーザーが API とのやり取りを開始してから明らかになるセキュリティギャップまで多岐にわたります。そのため、理想的には、開発中に API テストを実行し（シフトレフト）、本番環境でも継続的にテストを実行するべきです（シフトライト）。

開発中の API テストの例：

- 悪性トラフィックをシミュレートする自動テストを実行する
- 確立されたガバナンスポリシーに照らして、API 仕様を検査する
- オンデマンドで、または CI ／ CD パイプラインの一環として API をテストする

本番環境での API テストの例：

- API トラフィックを継続的に監視し、トラフィックのメタデータを評価する
- 自動分析により、既存の API の変更を特定する
- 問題をリアルタイムで検出し、攻撃者が気付く前に修正する

お使いの API セキュリティプロトコルはコンプライアンス義務を満たしていますか？

多くのデータ保護規制において、API と直接言及されることはないものの、API が動作するアプリケーションやインフラ全体のセキュリティ確保が要件として明確に定められています。コンプライアンス要件は常に進化しており、米国プライバシー権利法（現在法案段階）や EU サイバーレジリエンス法など、API に影響を及ぼす新たな規制が追加で制定される予定です。

現時点で API セキュリティに直接的な影響を与えている規制やフレームワークには次のようなものがあります。

- PCI DSS（現在 v4.0.1）
- 一般データ保護規則（GDPR）
- デジタル・オペレーショナル・レジリエンス法（DORA）
- Health Insurance Portability and Accountability Act（医療保険の携行性と責任に関する法律、HIPAA）
- Network and Information Security（NIS2）Directive（ネットワークおよび情報セキュリティ指令）

API セキュリティは注目を集めているものの後回しにされたまま

API への攻撃は、多額の損失や罰金、顧客の信頼の喪失、スタッフのストレス増大、そして取締役会での信用失墜など、深刻な影響をもたらします。それにもかかわらず、チームが断固とした対策に踏み切れないのはなぜでしょうか？以下の質問への回答がその理解に役立ちます。

企業のさまざまな役職は API セキュリティをどのように優先付けているか？

参加者に今後 12 か月間のサイバーセキュリティの主な優先事項を特定してもらい、広範なリストから 3 つまで選択できるようにしました（サイドバーを参照）。上位 6 つの優先事項の差はわずか 2% であり、下位 6 つの差はわずか 1% です。これは地域や業界を超えて優先事項が類似していること、そしてチームはしばしばこれらすべてに同時に対処することを余儀なくされていることを示唆しています。

しかし、一部の業界では、API に関するランキングの違いが異なる状況を示しています。たとえば、エネルギー／公益事業では、API セキュリティを優先事項とする回答の割合が 13.2% と他の業界すべてに比べて最も低く、全参加者の平均 18% を下回っています。同時に、エネルギー／公益事業は API セキュリティインシデントの報告率が 91% と 8 つの業界の中で最も高く、全体の平均 84% を上回っています。これは何を示唆しているのでしょうか？すなわち、API セキュリティの優先順位の低さと高い攻撃率です。

今後 12 か月間の最優先セキュリティ事項

1. **生成** AI を利用した攻撃に対する防御 – 21.2%
2. ランサムウェアに対する防御 – 20.5%
3. 従業員ユーザー向けの認証のセキュリティの確保 - 19.7%
4. 開発者の機密情報の管理とセキュリティの確保 – 19.6%
5. エンドポイントのセキュリティの確保 – 19.2%
6. クラウド・セキュリティ・ソリューション – 19.1%
7. 特権 IT アクセスのセキュリティの確保 – 18.6%
8. データ損失の防止 – 18.6%
9. 攻撃者からの API のセキュリティの確保 – 17.9%
10. アプリケーションのセキュリティの確保 – 17.7%
11. セキュリティ情報およびイベント管理 – 17.6%
12. インシデント対応および管理 – 17.6%

回答の元になった質問：今後 *12* か月間の貴社のサイバーセキュリティの主な優先事項は何ですか？（*3* つまで選択してください）、 *n = 1,207*

回答を役職別に分析することで、より示唆に富むデータが浮かび上がりました。

- CISO は、生成 AI を利用した攻撃と API 保護をそれぞれ **25.5%** および **24.8%** と最も重要な優先事項として挙げました。
- AppSec スタッフは CISO と一致しており、生成 AI を利用した攻撃を **22.5%** と最優先事項に挙げています。
- CIO と CTO はどちらも特権アクセスを重視し、CTO はインシデント対応も同率で挙げています。
- シニアセキュリティ担当者だけがランサムウェアを最優先事項と評価しました。

これらの違いから次のような疑問が浮かびます。IT セキュリティ組織のさまざまな層が、異なるプレイブックに基づいて動いているように見えるのはなぜでしょうか？トップのセキュリティリーダーと現場の従業員の見解が、生成 AI を利用した攻撃において、API とそのリスクが重要な役割を果たしているという点で一致している一方で、他の役職はそうではないのはなぜでしょうか？

おそらく、CISO が、自社の事業部門が需要に応えるために 生成 AI を活用したアプリなどのイノベーションを急いで展開しているのを見ている一方で、AppSec チームメンバーも同じ状況を見ているからです。機微な情報に関わる AI コンポーネント（大規模言語モデル（LLM）など）の脆弱性に関して未知の範囲を把握しているのは**彼ら**だけです。さらにこのチームは、攻撃者が 生成 AI を攻撃手法に組み込んでいる多くの警告サインを最前席で見ています。

しかし、一番の理由は最もシンプルです。特に大企業では、トップダウンとボトムアップのコミュニケーションがあまり行われないため、上層部の優先事項とチームが日々処理**しなければならない**事項との間に食い違いが生じます。

最後に、回答者のサイバーセキュリティの最優先事項と、彼らが挙げた API セキュリティインシデントの原因を比較してみましょう。17 ページに示されているように、回答者が挙げた原因の上位 3 つは、API 問題を捕捉できなかった従来のアプリケーション・セキュリティ・ツールを指しています。この比較は、API 探索およびテストソリューションが、API セキュリティだけでなく、他のほとんどすべてのセキュリティの最優先事項をどのように強化できるかについての議論を始める良い機会になるでしょう。

言い換えれば、適切な API セキュリティツールは API を保護できるだけでなく、データ、クラウド、アプリケーションなどの分野のセキュリティも向上させることができるのであれば、API セキュリティはステークホルダーにとっても孤立したニッチな分野には見えなくなります。全体像について話すことで、API を優先事項リストの上位に引き上げる承認を得られやすくなります。

適切な API セキュリティツールは API を保護できるだけでなく、データ、クラウド、アプリケーションなどの分野のセキュリティも向上させることができるのであれば、API セキュリティはステークホルダーにとっても孤立したニッチな分野には見えなくなります。

API セキュリティインシデントに関する認識の不一致は、信頼できる唯一の情報源がないことを示唆しているか？

ここまで経営幹部と現場スタッフの間で全体的なセキュリティ優先事項における差異を強調してきましたが、その差異は API の脅威に特有の問題においても依然として存在しています。たとえば、CIO は API 攻撃の認知に関して AppSec チームと一致しています（各役職の約 88% がインシデントを経験したと報告）。一方、CISO、CTO、シニアセキュリティ担当者はどれも約 8% 低く、約 80% がインシデントを経験したと報告しました。

API セキュリティインシデントの原因として最上位に挙げられたものは役職によって異なり、ほとんどの CISO やシニアセキュリティ担当者は API ゲートウェイが問題を捕捉できなかったことを原因としている一方で、他の 3 つの役職はそれぞれ異なる原因を挙げました。

- CISO：API ゲートウェイによって捕捉されなかった – **26.8%**
- CIO：意図しないインターネットへの公開 – **28.6%**
- CTO：WAF によって捕捉されなかった – **25.9%**
- シニアセキュリティ担当者：API ゲートウェイによって捕捉されなかった – **23.3%**
- AppSec チーム：API の設定ミス – **23.2%**

API セキュリティインシデントの主な原因、すべての回答者

1. API が意図せずインターネットに公開された - 21.8%
2. Web アプリケーションファイアウォールによって捕捉されなかった – 21.8%
3. API ゲートウェイによって捕捉されなかった – 20.2%
4. 生成 AI ツール／テクノロジー内の API（LLM など）– 20.0%
5. API の設定ミス – 19.9%
6. ネットワークファイアウォールによって捕捉されなかった – 19.6%
7. 既知のテクノロジーツール／サービス（Microsoft など）– 19.2%)
8. API コーディングエラーによる脆弱性 – 19.1%
9. 未管理 API（休眠 API やゾンビ API など）– 18.9%
10. API 認証制御の欠如 – 18.8%
11. 認証の脆弱性 – 18.7%
12. インターネットからダウンロードしたソフトウェアソリューション – 17.6%
13. ミッドティア・ソフトウェア・ソリューション（Slack など）– 16.3%

回答の元になった質問：貴社が経験した *API* セキュリティインシデントの原因は何だと思いますか？（*3* つまで選択可）、*n = 1,207*

報告された API セキュリティインシデントのコストも、上層部と現場で一致していないことを示しています。ただし、役職**と**地域別にデータを分析すると、自然とサンプルサイズが小さくなることに注意してください。それでも、これらのサブセット間の差異は注目に値します。特に米国では、CIO と CTO がインシデントのコストを約 100 万ドルと報告したのに対し、CISO は約 73 万 7,000 ドルと報告しました。一方、シニアセキュリティ担当者と AppSec スタッフは、それぞれ約 37 万 5,000 ドル、44 万 4,000 ドルと報告しています。

英国では役職別のサブセット間でおおむねコストが一致していましたが、AppSec チームメンバーが最高額の 74 万 9,000 ポンド、CISO が最低額の 19 万ポンドと報告しています（中間の役職では 37 万 4,000 ポンドから 22 万 2,000 ポンドの範囲でした）。ドイツのコスト報告の格差は英国と似ており、見積もりの最高額は最低ランクの現場スタッフの 34 万 5,000 ユーロで、最低額は最高ランクの CISO の 19 万 7,000 ユーロでした（米国とは逆の結果です）。地域や役職を問わず全般的に合意が見られた一つの領域は、API セキュリティインシデントの最大の影響はスタッフに対する影響であるということでした（7 ページの影響を参照）。

API セキュリティ体制の成熟に近付く方法

前述のように、今回の調査結果は、組織の異なる階層にいるセキュリティチームのメンバーが API セキュリティを同じ視点で捉えているわけではないことを、明確に示しています。しかし、逆の側面もあります。基盤となる共通点があることも明らかです。コスト（金銭的および人的）を理解しており、これまで利用してきたツールが十分ではないことを認識しています。

API セキュリティが組織に与える影響は非常に大きいため、次のステップとしてできるのは、何を基盤にするか、何を変更するかを決定し、API のセキュリティを確保することが収益にどのように貢献できるかをリーダーに示すことです。CISO から AppSec チームまで、セキュリティ部門内で API セキュリティの優先順位をどう位置付けるかについて合意を得ることは、良い出発点です。その次に、経営陣と現場の AppSec チームメンバー、さらにはその中間の管理層との間でオープンなコミュニケーションを促進することが挙げられます。

実行可能なステップ

今回の調査を締めくくるにあたり、セキュリティチームが API セキュリティ戦略を開始し構築し、成熟した API 保護に近付くために活用できる一連の段階的なステップをまとめました。

1 API の探索と可視性から始める

自社の API 資産全体の完全なインベントリを作成するためには、API と API がサポートするマイクロサービスを探索する自動化アプローチを備えたツールを探します。カバレッジの広さが重要です。なぜなら未管理の API（10 ページのサイドバーを参照）は攻撃者の第一の標的となるからです。

2 テストに投資する

API が正しくコーディングされ、意図した機能を実行できるかどうかを簡単にテストできる API セキュリティソリューションを選択します。理想的には、テストはデプロイ前に実施するべきですが、すでに本番環境にあるすべての API についても、トラフィックと潜在的な脆弱性のリアルタイム分析によってテストすることが重要です。

3 API の完全な文書化を実施する

API 環境全体を監査し、設定ミスのある API やその他のエラーを特定することは不可欠です。また、すべての API について、それらが機微な情報を含んでいるか、適切なセキュリティ制御が不足していないかを適切に文書化できる監査機能が必要です。これはまた、暗黙的または明示的に API セキュリティが関係するコンプライアンス要件への準備にも役立ちます（14 ページ参照）。

4 ランタイム検知を利用する

API セキュリティソリューションに自動化ランタイム検知機能があれば、通常の API アクティビティと異常な API アクティビティを区別することができます。このようにして API インタラクションを監視することで、脅威を示すふるまいをリアルタイムで検知し、対処することができます。

5 不審なふるまいに対応する

API セキュリティソリューションを既存のセキュリティスタック（WAF や WAAP など）と統合することで、高リスクのふるまいを特定し、不審なトラフィックが重要なリソースにアクセスする前にブロックできるようになります。

6 脅威を調査し、追跡する

最も成熟した API セキュリティ段階では、過去の脅威データに対してフォレンジック分析を実施し、アラートが脅威を正確に特定したかどうか、また、高度なツールとヒューマンインテリジェンスを組み合わせて事前対応型の脅威ハンティングを可能にするパターンが出現したかどうかを確認します。

結論

今年のレポートでは、セキュリティ（この場合は API セキュリティ）が単に脅威リストやツールの問題ではなく、人が深く関わっていることが明確に示されました。

今回の調査では、セキュリティチームが過度の負担を抱えており、チームの仕事にまったく新しい攻撃ベクトルを追加するという考えが、とても困難に感じられるかもしれないことが確認されています。しかし、API の増殖が緩むことはなく、API のセキュリティを確保するための対策を講じることは、他の優先度の高い分野にも大きな波及効果をもたらします。たとえば、生成 AI の脆弱性（LLM とデータを交換する API を保護）やクラウドセキュリティ（移行するワークロードに含まれるすべての API のリスクを軽減）などです。

API セキュリティに積極的に取り組むことは、ビジネスを保護するだけでなく、この重要な攻撃ベクトルに対する見解において、セキュリティチームが同僚、経営陣、そして取締役員の間で、高い信用と信頼を得られるようになると、私たちは強く信じています。この取り組みには、チームのストレスレベルを軽減できるという大きなメリットがあります。今回の調査によれば、API セキュリティのインシデントとそれに伴う厳しい監視や信用の喪失は、従業員と顧客の双方に大きく影響を与えることが示されています。

今から対策を始めることで、コンプライアンス計画策定や報告の負担を事前に軽減できるだけでなく、規制違反による罰金を未然に防ぐことも可能になります。始めてみませんか？

- 成熟した API セキュリティ体制に向けて次のステップを検討する準備ができましたら、当社のホワイトペーパー「API セキュリティの基礎」からスタートすることをお勧めします。
- お客様が抱えている課題や、Akamai がどのようにお手伝いできるかについてご相談されたい場合は、カスタマイズされた Akamai API Security デモを簡単にお申し込みいただけます。

API セキュリティの影響に関する調査について

2024 年 API セキュリティの影響に関する調査は、2023 年 6 月 12 日から 2024 年 7 月 7 日にかけて、Opinion Matters によって実施されました。同社のチームは、合計 1,207 人の回答者を対象に調査を実施しました。回答者の企業の所在地の内訳は、英国 404 人、米国 402 人、ドイツ 401 人です。回答者の 3 分の 1 は CIO または CISO、3 分の 1 はシニアセキュリティ担当者、3 分の 1 は、アプリケーション・セキュリティ・チームのメンバーです。回答者は、従業員数 500 人未満から 1,000 人以上の企業に所属しており、自動車、金融サービス、小売／ E コマース、ヘルスケア、保険、政府／公共部門、製造、エネルギー／公益事業という 8 つの主要産業から選ばれています。

Opinion Matters は、Market Research Society（MRS）の会員を採用し、同協会の行動規範および ESOMAR の原則を厳守しています。Opinion Matters は、British Polling Council のメンバーでもあります。

クレジット

Lead writer
Annie Brunholzl

Managing editor
John Natale

Research director
Mitch Mayne

Copy editor
Randi Kravitz

販促資料
Barney Beal

マーケティング・出版
Georgina Morales Hampe

校閲およびテーマ別寄稿者
Pam Cobb
Jim Lubinskas
Kimberly Gomez
Stas Neyman

インターネットの現状／セキュリティ

高い評価を受けている Akamai の「インターネットの現状／セキュリティ」レポートのバックナンバーおよび今後のリリースについては、**akamai.com/soti** をご覧ください。

Akamai の脅威リサーチ

akamai.com/security-research では、最新の脅威インテリジェンス分析、セキュリティレポート、サイバーセキュリティリサーチを通じ、常に最新情報を把握できます。

Akamai API Security

Akamai は、API の開発から本番運用まで、ライフサイクル全体を保護します。API の探索から、セキュリティ体制の管理、ランタイム保護、API セキュリティテストまで、必要な機能を完備しています。その詳細をご紹介します。 **https://www.akamai.com/products/api-security**