最新の API セキュリティの影響に関する調査では、サイバーセキュリティのさまざまな分野で役職に就く 800 人以上の回答者による回答を収集し、アジア太平洋（APAC）地域の 4 大経済国（中国、インド、日本、オーストラリア）における API セキュリティの現状を評価します。この調査は、過去 3 年間にわたるセキュリティ対策の取り組みにおいての API の位置づけについてセキュリティプロフェッショナルに意見を求めた Noname Security（現在は Akamai Technologies の一員）による年次調査を基盤としています。一貫してわかったのは、API の脆弱性に対する意識が高まっているにもかかわらず、CISO と CIO の両者が増え続ける優先課題への対応に追われているため、上級管理職からの API セキュリティへの取り組みが遅れているということです。

2024 年の **API セキュリティの影響に関する調査**では、これまで対象としていた米国および英国の組織に加え、新たにドイツを調査範囲に含めました。調査の結果、以下のことが明らかになりました。

- API セキュリティインシデントは 3 年連続で増加している。
- このようなインシデントに対応するコストの推定値は平均 50 万ドルを超えている（IT およびセキュリティのリーダーによると、100 万ドル近く）。
- ほとんどの回答者は、これらのインシデントがセキュリティチームに与えるストレスや評判への悪影響を認識している。

API セキュリティインシデントとは

インシデントには、API の悪用、API への攻撃、API を標的としたデータ漏えい、そして攻撃者による API の侵害を試みる行為全般が含まれます。

この調査の回答者は、経営幹部（CISO、CIO、最高技術責任者）、シニアセキュリティ担当者、および以下の 8 つの業界の企業に所属する AppSec チームメンバーで構成されています。

- 自動車
- 保険
- 金融サービス
- 政府／公共部門
- 小売／Eコマース
- 製造業
- ヘルスケア
- エネルギー／公益事業

この調査結果から、API のセキュリティプラクティスや優先順位に関する次のような貴重な知見が明らかになりました。

- API セキュリティインシデントの原因
- サイバーセキュリティの全体的な優先事項
- API セキュリティインシデントに関連するコスト（罰金や修正費用など）
- API セキュリティインシデントがセキュリティチームに与える影響
- API のインベントリ管理とテストの実施状況
- 機微な情報を返す API の把握
- 規制コンプライアンスの取り組みにおける API セキュリティの現状