本レポートの主要な知見

AI ベースの API は、そうでない API に比べて安全性が低い。

人工知能（AI）を利用する API の大部分は外部からアクセス可能で、多くの場合、脆弱な認証メカニズムに依存しています。そのような API を標的とする AI 主導の攻撃が増加しているため、この脆弱性は深刻化しています。

AI は脅威アクターの技術的進歩を促進する。

これには、AI 主導のマルウェア、脆弱性スキャン、AI 統合システムへの攻撃、高度な Web スクレイピング機能などの技術的進化が含まれます。

32%

OWASP API Security Top 10 関連のインシデントの増加率

API セキュリティインシデントが増加している中、Open Worldwide Application Security Project（OWASP）API Security Top 10 の問題により、機微な情報と機能を公開する認証および認可の欠陥が明らかになっています。

30%

MITRE セキュリティフレームワークに関連するセキュリティアラートの増加率

攻撃者は自動化や AI などの高度な手法を使用して API を悪用しています。MITRE フレームワークは、防御側がそのような攻撃を迅速かつ正確に特定するために役立ちます。

33%

グローバルな Web 攻撃の前年比増加率

攻撃の急増は、クラウドサービス、マイクロサービス、AI アプリケーションの急速な普及と直接関係しており、それらによってアタックサーフェスが拡大し、新たなセキュリティ上の課題が生じています。

2,300 億件以上

コマース組織を対象とした Web 攻撃の数

コマース業界は最も影響を受けた業界であり、ハイテク業界（2 番目に多くの攻撃を受けた業界）の 3 倍近くの数の攻撃を受けました。