アプリと API セキュリティの現状 2025

AI はデジタル領域をどうシフトさせるか

企業が AI ベースのアプリケーションに投資し続ける中、新たな脆弱性が生まれています。同時に、脅威アクターは AI を利用してキルチェーン全体を自動化しています。その結果、Web アプリケーションと API に対する攻撃の規模は拡大し、巧妙さが増しています。

攻撃者が AI を利用する 6 つの手口

- **AI 強化型マルウェア**
- **AI ベースの脆弱性スキャン**
- **LLM ベースのアプリケーションに対する攻撃**（プロンプトインジェクション、データポイズニング、ジェイルブレイク手法）
- **高度な Web スクレイピング**
- **自動化された分散型サービス妨害（DDoS）攻撃**
- **Low & Slow（少しずつ時間をかけた）攻撃**

Web 攻撃

33%

グローバルな Web 攻撃の前年比増加率

⚠ 影響

攻撃の急増を後押しする AI

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。

Web 攻撃に関する業界の傾向

2,300 億件以上

Web 攻撃

コマース業界は Web 攻撃の影響を最も受けた業界で、2 番目に多く攻撃を受けたハイテク業界と比べて、攻撃数はほぼ 3 倍に達しました。

API 攻撃

32%

OWASP API Security Top 10 に関連するインシデントの増加率 *

⚠ 影響

AI ベースの API のセキュリティは低下しています

AI を利用する API の大部分は外部からアクセス可能で、API の多くは脆弱な認証メカニズムに依存しています。この脆弱性により、AI 主導の攻撃が増加し、事態をさらに深刻化させています。

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 *

⚠ 影響

MITRE フレームワークは、API を標的とする攻撃者の手法に関する知見を提供するために依然不可欠なものです

攻撃者は自動化と AI を使用して API を悪用するため、MITRE フレームワークによって、防御側がそのような攻撃を迅速かつ正確に特定することができます。

レイヤー 7 DDoS 攻撃数

94%

レイヤー 7 DDoS 攻撃数 Top 10 に関連するインシデントの月間増加率

⚠ 影響

攻撃は巧妙さと強さの両方が増しています

レイヤー 7 DDoS 攻撃は、攻撃者が Web アプリケーションロジックまたは API の特定の脆弱性を悪用する手口を改造したために急増しました。一方で、ボット主導型攻撃のトラフィックパターンが巧妙化し、正当な API の使用を忠実に模倣するようになりました。

レイヤー 7 DDoS 攻撃に関する業界の傾向

7 兆

ハイテク業界を標的としたレイヤー 7 DDoS 攻撃の件数（2023 年 1 月～ 2024 年 12 月）。これにより、ハイテク業界は最も影響を受けた業界となりました。

緩和戦略

- シフトレフトと DevSecOps API セキュリティプランを採用する
- 適応型セキュリティエンジンを使用する
- API テストツールを適用する
- OWASP セキュリティガイドラインを実装する
- 専用の DDoS 防御を開発する
- セキュリティフレームワークを監視する
- レイヤー型ランサムウェア防御を採用する
- AI ベースのファイアウォールおよびボット防御ソリューションを活用する

*30 日間の集計結果

攻撃の傾向に関する包括的な知見を、ぜひレポートでご確認ください。

レポートをダウンロードする

 | 公開日 2025 年 5 月