2023 年 8 月 24 日

*Press Release*

アカマイ・テクノロジーズ合同会社

# API セキュリティ調査：ほとんどの企業で API のリスクを課題視しながら、API に特化した攻撃で優先すべき対策との認識にギャップが生じていることが明らかに

※本リリースは 2023 年 7 月 18 日 (現地時間)マサチューセッツ州ケンブリッジで発表されたプレスリリースの抄訳版です。

オンラインの力となり、守るクラウドカンパニー、Akamai Technologies, Inc.（NASDAQ：AKAM）は、API セキュリティに関する調査結果を新たに発表しました。本調査では、事業者のアプリケーションセキュリティに関与する立場の人達が何をアプリケーション・プログラミング・インターフェース（API）関連の最も重要なセキュリティリスクと見なしているのかについて調査しています。

「2023 SANS Survey on API Security」（2023 年 SANS API セキュリティ調査）では、API セキュリティ・テスト・ツールを導入している回答者の割合は 50%未満であり、API ディスカバリーツールを導入している回答者の割合はさらに少ない（29%）ことが判明しました。また、レポートによると、DDoS 対策サービスや負荷分散サービスに含まれる API セキュリティコントロールは「十分に活用されていない」とされており、この機能を利用している回答者の割合はわずか 29%でした。

Akamai は SANS Institute と協力して 2023 年第 1 四半期にこの調査を実施し、API セキュリティリスクへの対処に関するエンタープライズの意識、準備状況、将来的な計画について調査しました。主に事業者のアプリケーションセキュリティに関与する、または関与予定のある立場の世界中の 231 人の回答者が調査に参加しました。

モダンなアプリケーションは、ますます API を利用するようになり、ビジネスプロセスに対応して、効率的にビジネスパートナーや顧客が企業と協力できるようにするために必要なコミュニケーションにビジネスプロセスを組み込んでいます。「セキュリティギャップのすり抜け」と題した Akamai の最新の「インターネットの現状（SOTI）」レポートでは、2022 年はアプリケーション攻撃と API 攻撃の記録が塗り替えられた年とされています。

今回の調査では以下のことがわかりました。

- 62%の回答者は、API リスク緩和の一環として Web アプリケーションファイアウォールを利用しています。
- 57.1%の回答者は、API インベントリの精度が 25-75%であると回答しています。
- ほとんどの回答者は、OWASP（Open Web Application Security Project）Application Security Top10 リストと OWASP API Top10 リストについて言及し、アプリケーションと API のリスクを定義するための基礎として MITRE ATT&CK Framework を取り上げています。OWASP API Top10 の上位は、API の実装に特有の脆弱性を悪用した攻撃が占めています。

- それにも関わらず、API セキュリティに関する懸念事項の第 1 位はフィッシング（38.3%）、第 2 位はパッチの見落とし（24%）であり、脆弱なアプリケーション／API の悪用（12%）、過失による機微な情報の開示（9.1%）はそれに続く位置にあげられています。本レポートの結論では「利用中の API の発見と（API ごとに異なる）脆弱性の評価を最上位にする必要がある」と述べています。
- 76%の調査参加者は、開発者に対してアプリケーションセキュリティに関するトレーニングを実施していると回答しています。

Akamai Application Security 部門の Senior Vice President 兼 General Manager である Rupesh Chokshi は「この新たな調査は、2023 年以降も重要なセキュリティ上の問題であり続けるトピックに対する、産業界の見方を示しています。調査の結果、脆弱な API が攻撃に最もよく利用されるアクセスのポイントとなっていることを踏まえ、企業は多くの API がどこでどのように稼働しているかにもっと注目する必要があることが分かりました」と、述べています。

SANS の Director of Emerging Security Trends である John Pescatore 氏は「この調査の重要なポイントは、強力な(API)認証、API アセットのインベントリおよび脆弱性の管理、（API の）変更管理などのセキュリティ健全性コントロールによって、API（特有の）セキュリティに関する課題に対処する必要があるということです。API 中心の攻撃に対処するための防止と検知を強化する必要があり、その上でインフラサービス（CDN やサービス妨害フィルタリングなど）を活用する必要があります」と、語りました。

**Akamai について：**

Akamai はオンラインライフの力となり、守っています。世界の先進企業が Akamai を選び、安全なデジタル体験を構築して提供することで、Akamai は、毎日、世界中の人々の生活、仕事、娯楽をサポートしています。超分散型のエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のセキュリティ、コンピューティング、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、Twitter と LinkedIn で Akamai Technologies をフォローしてください。