

Akamai 脅威レポート：2023 年を振り返り、今後の展望を明かす

オンラインライフの力となり、守るクラウド企業の [Akamai Technologies, Inc.](#) (NASDAQ : AKAM) は、2023 年に発刊した「SOTI インターネットの現状」レポートの中から注目すべきサイバー攻撃の傾向を取り上げて 1 つのレポートにまとめた「[インターネットの現状 | 年間レビュー](#)」を発表しました。本レポートでは、Akamai の Security Intelligence Group (SIG) に属するライターやデータサイエンティストたちがそれぞれの視点から今年の攻撃動向の変化や進化を解説するとともに、今後の展望を明らかにしています。

エグゼクティブサマリー

- Akamai が発見した、高度な隠ぺい工作を用いる Web スキミング攻撃の驚くべき新手口とは？
- ランサムウェアや Web 攻撃の標的となるヘルスケア業界の IoMT（医療の Internet of Things）と医療サービスにアクセスするための API
- JSON Web Token (JWT) による API 認証に潜んでいる脆弱性と大きな脅威
- Outlook バイパスの脆弱性パッチをめぐるセキュリティ研究者の試行錯誤
- アジア太平洋および日本 (APJ) 地域において、金融サービスは最も Web アプリケーションおよび API 攻撃の標的となり、2023 年 6 月のレポート以降、金融サービスへの攻撃は 45 億件に
- 2022 年 1 月から 2023 年 10 月の APJ において攻撃を受けた上位 3 つの業界は、金融サービス、コマース、ソーシャルメディア
- 現在の地政学的状況から、EMEA は DDoS 攻撃の地域シフトの標的になっており、中でも金融サービスへの攻撃が際立っている
- DDoS 攻撃の変化の一つで、DNS に対する攻撃が飛躍的に増加しており、その大半は正規のものとの判別が難しいクエリー攻撃である

2023 年の状況を一言で表すと、「転換 (pivot)」です。攻撃者はセキュリティ対策を回避するために戦術を転換し、新たなアタックサーフェスやまだ侵害されていないターゲットを探し、あらゆる規模や業界の組織に大きな損害を与えました。その一方で、セキュリティの防御側でも、攻撃を緩和し、組織の保護を改善するために、手直しを加えながら新たな方法を学び続けています。

DDoS や API 攻撃は 2024 年に引き続き蔓延することが予想されます。DDoS は、より大規模なボットネット群を構築し、新たな手法を開発するために絶えず活動し、国家からの影響力を受けることで拡大していくでしょう。API は DX の推進とともに実装が急速に進む一方で、アタックサーフェスの拡大と脆弱性の増加、シャドー API、ゾンビ API、API の悪用を招きます。また、攻撃の進化と複雑化によって、経験あるサイバーセキュリティの専門家の不足が世界中で課題になるでしょう。



Akamai では、蔓延している脅威や新たに登場するセキュリティリスクに警鐘を鳴らし続けます。2024 年には、SOTI レポートが 10 周年を迎えます。セキュリティ専門家の知見を共有することで、皆さまのセキュリティ設計の一助となれるよう、これからも引き続きレポートを改善していきます。

Akamai Technologies 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。世界中のトップ企業が 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、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。広範に分散した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 のクラウドコンピューティング、セキュリティ、コンテンツ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、[X](#) (旧 Twitter) と [LinkedIn](#) で Akamai Technologies をフォローしてください。

※Akamai と Akamai ロゴは、Akamai Technologies Inc.の商標または登録商標です

※その他、記載されている会社名ならびに組織名、ロゴ、サービス名は、各社の商標または登録商標です

※本プレスリリースの内容は、個別の事例に基づくものであり、個々の状況により変動するものです