クライアント側の保護を考える

JavaScript は強力なユーザー体験を提供するために不可欠ですが、一方で、クライアント側の脅威やエンドユーザーデータの窃取に対して、Web サイトが脆弱になってしまいます。

Web スキミングや Magecart、フォームジャッキング攻撃は、罰金や信頼の失墜、収益損失など、ブランドにとって悪い結果をもたらすおそれがあります。

感染はどこから始まるか

ファーストパーティの脆弱性の悪用

セキュリティの誤設定、フレームワークの脆弱性など

サードパーティのサプライチェーン攻撃

許可されたサードパーティプロバイダーを介した悪性コードの挿入

Web スキミング攻撃でエンドユーザーのデータを盗む手口

エンドユーザーがオンラインで閲覧

Web アプリケーション

エンドユーザーがチェックアウトページに**機密情報**を入力

データを**悪性スクリプト**の挿入によってスキミング

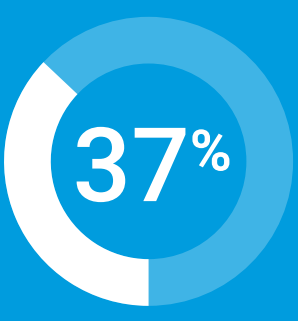
不正アクセスを受けた JavaScript

攻撃者が制御するドメインによって**収集・窃取**されたデータ

サードパーティの JavaScript によって、ブランドが脆弱に

サードパーティ製の JavaScript を使用する Web サイトの割合

小売およびコマース [1]



金融サービス [2]

あらゆる規模の企業に脅威が迫る

大手オンライン小売企業の 81% が、2022 年に自社が不審なスクリプトのふるまいの標的にされたと報告 [3]

壊滅的な影響

445 万米ドル	2023 年の世界全体におけるデータ漏えいに伴うコスト総額の平均 [4]
948 万米ドル	2023 年の米国におけるデータ漏えいに伴うコスト総額の平均 [4]

PCI コンプライアンスにクライアント側のセキュリティが必須に

Security Standards Council

ペイメントカードのデータを処理する組織は、罰則を回避するために、新しい **PCI DSS v4.0 JavaScript セキュリティ要件に 2025 年までに**準拠しなければなりません [5]

要件 6.4.3

要件 11.6.1

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance は、JavaScript の脅威から守り、PCI DSS v4.0 ワークフローを合理化し、エンドユーザーのデータの安全を守ります。JavaScript の脆弱性を可視化し、スクリプトのふるまいを分析して、有害で悪性のスクリプトアクティビティを検知します。また、セキュリティチームがクライアント側の攻撃を迅速に緩和し、防御できるように、実用的なアラートを提供します。

詳細については、製品ページをご覧いただくか、Akamai の営業担当にお問い合わせください。

1. コマース業界における脅威トレンドの分析 | Akamai SOTI 2023
2. イノベーションに潜む高いリスク：金融サービス業界の攻撃トレンド | Akamai SOTI 2023
3. 悪性ボットから悪性スクリプトまで：特別な防御の有効性 | 2023
4. IBM 2023 年のデータ漏えいのコストに関するレポート | 2023
5. PCI DSS v4.0 | 2022

©2023 Akamai Technologies | サポート | | 公開日 2023 年 12 月