AKAMAI チェックリスト

Akamai Client-Side Protection & Compliance を使用した PCI DSS v4.0 JavaScript セキュリティチェックリスト

Payment Card Industry Data Security Standard（PCI DSS）とは、オンラインで処理されるペイメントカードのデータセキュリティを確保し、世界中で一貫したデータセキュリティ対策を広く採用するよう促進するために開発された、グローバルセキュリティ基準です。最も重要なセキュリティ基準の 1 つであり、ペイメントカードのデータをオンラインで処理するすべての組織で準拠が義務付けられています。

PCI DSS の最新バージョン（英語版のみ）はバージョン 4.0 で、2025 年に発効します。これには、12 の中核的なデータセキュリティ要件が含まれ、新しく進化を続けるサイバーセキュリティの脅威に対処するためのガイダンスが付属しています。PCI DSS v4.0 に追加された 2 つの主要要件である 6.4.3 と 11.6.1 は、JavaScript のセキュリティと、ブラウザー内からエンドユーザーの機密情報を盗むクライアントサイドの Web スキミング攻撃に対する保護に、対応しています。このような攻撃は、ここ数年で数を増しており、手法が巧妙化していることで検知がますます難しくなっています。被害を受けた組織は、多額の罰金、ブランドの評判への損害、収益の損失、顧客からの信頼の低下など、壊滅的な影響を受ける可能性があります。

新しい PCI DSS v4.0 スクリプトのセキュリティ要件と、Client-Side Protection & Compliance がどう役立つかについて、チェックリストをご覧ください。

PCI DSS v4.0 要件	Client-Side Protection & Compliance がどう役立つか
要件 6.4.3 — 一般向けに公開されている Web アプリケーションが攻撃から保護されている ☑ ブラウザーで読み込まれ実行されている各スクリプトが認証されていることを確認する方法が実装されている ☑ ブラウザーで読み込まれ実行されている各スクリプトの完全性を保証するための方法が実装されている ☑ ブラウザーで読み込まれ実行されている各スクリプトがなぜ必要なのかの正当な根拠を示す文書とともに、すべてのスクリプトのインベントリが維持されている	**ワンクリックで認証** ☑ Web サイトの決済ページで実行を許可するスクリプトを、ツール内で直接簡単に管理 **整合性を最優先** ☑ ふるまいテクノロジーが、ブラウザーで実行される各スクリプトを分析し、悪性のアクティビティやデータ窃取を検知して警告 **すべてのスクリプトを自動的に追跡し、インベントリ化** ☑ 事前定義された正当な根拠と自動化されたルールにより、ブラウザーに読み込まれ実行される各スクリプトの目的を簡単に正当化

Akamai

PCI DSS v4.0 要件	Client-Side Protection & Compliance がどう役立つか

要件 11.6.1 ― 決済ページに承認されていない変更が加えられた場合、その変更を検知し、しかるべき対応を実施する

変更および改ざん検知メカニズムが以下のように配備されている：

- ☑ 消費者のブラウザーが受信した HTTP ヘッダーおよび決済ページのコンテンツに対する不正な変更（侵害、変更、追加、削除の指標を含む）を担当者にアラートを通知する
- ☑ メカニズムが、受信した HTTP ヘッダーと決済ページを評価するように設定されている

この**メカニズムは**、少なくとも 7 日に 1 回、または定期的（要件 12.3.1 に規定されるすべての要素に従って実施される、エンティティのターゲットリスク分析で定義された頻度）にて実施されるものとします。

決済ページを保護

- ☑ 決済ページに対する悪性の改ざんを監視、分析、緩和することで、エンドユーザーの貴重なデータの安全性を確保

即座に実行可能なアラートにより、不正な変更をリアルタイムで調査

- ☑ 即時検知により、セキュリティチームは決済ページの HTTP ヘッダーの不正な変更や修正に迅速に対応可能

常時稼働防御で保護

- ☑ 24 時間体制の保護により、決済ページでのユーザーとのやり取りを保護

Akamai Client-Side Protection & Compliance は、JavaScript の脅威に対する堅牢な保護を提供し、クライアントサイドのアタックサーフェスを可視化することで、ブラウザー内の機微な情報を保護します。PCI DSS v4.0 専用に構築された機能は、セキュリティおよびコンプライアンスチームが PCI DSS v4.0 監査プロセスを合理化する支援を行い、またスクリプトのセキュリティ要件 6.4.3 および 11.6.1 を満たすための専用ワークフローを提供します。

Akamai Client-Side Protection & Compliance には柔軟な導入オプションが備えてあるため、Akamai Connected Cloud を有効にする必要はありません。

これらの機能が、PCI DSS v4.0 への準拠にどのように役立つかについては、**こちら**をご覧ください。