2023 年 10 月 5 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai Client-Side Protection & Compliance、組織による PCI DSS v4.0 への準拠を支援する新機能を導入

新機能により、PCI DSS v4.0 への準拠をシンプルに実現し、
最新の JavaScript セキュリティ要件 6.4.3 および 11.6.1 の達成を支援促進

オンラインライフの力となり、守るクラウド企業、Akamai Technologies, Inc.（NASDAQ：AKAM）は、PCI DSS v4.0 の JavaScript セキュリティ要件 6.4.3 および 11.6.1 に準拠するために設計された Client-Side Protection & Compliance 製品の新機能を提供することを発表しました。

Payment Card Industry Data Security Standard（PCI DSS）とは、ペイメントカードデータのセキュリティを促進、強化するとともに、国際的に一貫したデータセキュリティ対策の幅広い導入の推進を目的として開発された基準です。最新版の PCI DSS（バージョン 4.0）は 2022 年にリリースされました。この基準は 2024 年 3 月に発効し、2025 年 3 月に要件が完全に施行されます。これにはいくつかの新しいセキュリティ要件と、現在の脅威やテクノロジーに対処するための最新のガイダンスが含まれています。ペイメントカード情報をオンラインで処理、保存、または送信する組織は、これに準拠する必要があります。

新しい PCI DSS v4.0 の要件 6.4.3 および 11.6.1 では、JavaScript サプライチェーンの脆弱性を悪用して機密性の高いエンドユーザーデータをブラウザー内から盗むクライアントサイドの有害な Web スキミング攻撃を、企業が阻止する必要性について概説しています。このような攻撃（Magecart など）は高度化し、デジタルコマースに影響を与え続けています。新しい標準に準拠するために、組織は Web サイトの決済ページで読み込みおよび実行されているスクリプト、そのスクリプトが実行しているアクション、およびスクリプトが変更されたタイミングを把握できなければなりません。

Akamai の Client-Side Protection & Compliance（旧称 Page Integrity Manager）は、クライアントサイドのアタックサーフェスを広範囲にわたって可視化し、エンドユーザーデータの窃取を防止し、Web サイトを JavaScript ベースの脅威から保護します。悪性のスクリプトのふるまいをリアルタイムで検知し、次のアクションが可能なアラートを受け取ることで、セキュリティチームは有害なアクティビティを迅速に緩和できます。新たに PCI DSS v4.0 準拠に特化した機能を備えた Client-Side Protection & Compliance は、セキュリティチームがコンプライアンスワークフローを合理化し、最新の JavaScript セキュリティ要件を満たすために役立ちます。

PCI DSS v4.0 へのコンプライアンスに特化した重要な機能

- **スクリプトインベントリ管理**（PCI DSS v4.0 要件の 6.4.3 に対応）— 保護された決済ページで読み込まれ実行されるすべての JavaScript のインベントリを提供します。ユーザーは、観測された

スクリプトごとに、正当性を示す文書を簡単に記録できます。このソリューションは、事前に定義された正当な証拠とルールを使用して、可能な限り多くの正当な理由の設定を自動化し、コンプライアンスの作業を大幅に削減します。

- **PCI DSS v4.0 ダッシュボード**（PCI DSS v4.0 要件の 6.4.3 および 11.6.1 の対応）— ワンクリックでコンプライアンスに関する知見を得ることができます。製品内の包括的なダッシュボード上で表示される内容が、直接、要件 6.4.3 および 11.6.1 の各構成要素に対応します。セキュリティチームは、監査プロセスを容易にする単一のビューで、スクリプトの認可とふるまいの整合性を確保し、決済ページの改ざんを防止し、スクリプトインベントリ管理に迅速に対応できます。
- **専用 PCI アラート**（PCI DSS v4.0 要件の 6.4.3 および 11.6.1 に対応）— リアルタイムの緩和のために、PCI 関連イベントに関する即時的かつ次のアクションが可能なアラートを受け取ることができます。これには、データ窃取、不正なスクリプト、設定された決済ページの保護の改ざん、および不正な HTTP ヘッダーの変更の通知が含まれます。アラートは PCI DSS v4.0 ダッシュボードに要約され、監査証拠として記録されます。

Client-Side Protection & Compliance は、CDN に依存しない製品であり、柔軟な展開オプションを備えています。このソリューションは、業界をリードする Akamai の Web アプリケーション・セキュリティ・ポートフォリオの一部であり、Akamai App & API Protector と連携します。企業は、これらの製品をバンドルして、サーバーサイドとクライアントサイドの両方の脅威に対する包括的な保護を実現し、PCI DSS v4.0 で追加された要件を満たすことができます。

Akamai の Application Security Group 担当 Senior Vice President 兼 General Manager である Rupesh Chokshi は「PCI DSS v4.0 への準拠の期限が目前に迫っているなか、Akamai の Client-Side Protection & Compliance は、複雑なコンプライアンスプロセスをシンプル化するために役立ちます。結果として、エンドユーザーのペイメントカードデータが保護されるという安心感を企業に与えます。これらの新機能は、コンプライアンスワークフローを合理化するように設計されており、Web サイトの決済ページで実行される JavaScript をお客様が簡単に管理するために役立ちます。ブラウザー内でエンドユーザーのペイメントカードデータを保護し、セキュリティチームがクライアントサイドのアタックサーフェスを制御できるようにします」と述べています。

オンラインで支払いを受けるあらゆる業界の企業は、来たる PCI DSS V4.0 への準拠期限に向けて準備する必要があります。Forrester の「The State of Application Security, 2023」（2023 年におけるアプリケーションセキュリティの現状）レポート（Forrester のサブスクライバー向けレポート、個別購入も可能）では、金融サービス企業や保険会社が今年導入を予定している主要なテクノロジーとして、クライアントサイドの保護が取り上げられており、「PCI Security Standards Council がクライアントサイドのセキュリティ要件を追加したため、金融サービス企業が PCI DSS に準拠して Magecart、フォームジャッキング、クリプトジャッキングなどの攻撃を阻止するためにクライアントサイドのコード保護を導入することは驚くべきことではありません」と述べられています。

Akamai の Client-Side Protection & Compliance、および一貫したオンライン体験の提供を支援するその他の製品と機能の詳細については、https://www.akamai.com/ja/products をご覧ください。

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。世界中の先進企業が 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、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。

※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しうるものです