

AKAMAI ソリューション概要

Akamai による PCI DSS v4.0 準拠

PCI コンプライアンスとは、決済カードのアカウントデータを扱う環境を保護し、セキュリティを確保するために、世界的な一連のセキュリティ要件を遵守することを意味します。カード所有者データをオンラインで処理、伝送、または保存するあらゆる企業は、PCI DSS（Payment Card Industry Data Security Standard）に準拠する責任があります。2004 年に策定されたこの基準は、業界の変化やサイバーセキュリティ脅威の進化に合わせて定期的に更新されています。2022 年 3 月にリリースされた最新の PCI DSS v4.0 には大幅な変更が加えられており、2025 年 3 月までに組織が満たさなければならない 12 の主要な要件が含まれています。

PCI DSS v4.0 に適合するための準備はお済みですか？

PCI 基準に準拠しなくても法律で罰せられることはありませんが、クレジットカード会社はこの基準に準拠しない企業に罰金を科す可能性があります。さらに、カード所有者データのセキュリティを確保できない場合、ブランドはサイバー攻撃に対して脆弱になります。その結果、多額の罰金を伴い顧客の信頼を永久に失うような、壊滅的なデータ漏えいにつながる可能性があります。

そこで、Akamai の出番です。Akamai は、PCI DSS Level 1 のコンプライアンスを維持するだけでなく、組織が PCI DSS v4.0 に準拠するために役立つ業界有数の幅広いセキュリティソリューションを提供します。ソリューションの中には、PCI 監査の範囲を縮小し、認定要件を満たすために費やされる貴重な時間とコストを節約するものまであります。

マルウェア防御を備えた App & API Protector

ログのコンプライアンスを維持し、個人を特定できる情報の漏えい、ゼロデイ攻撃、CVE、その他のエッジベースの攻撃を防止することにより、要件 6.4.2、6.5.3、11.5 を満たすことができます。

「すでに回っている10億以上のマルウェアプログラムに加え、56万もの新しいマルウェアが毎日検知されています」

出典：Getastra | 30+ Malware Statistics You Need to Know In 2023

API Security

API のふるまいとロジックの不正使用の検知と緩和、API アクティビティのログ記録、応答性に優れた自動の API 保護の実装により、コンプライアンス要件 6.2.3、6.2.4、6.3.2、6.4.1、6.4.2、10.2.1、10.5.1、11.3.2 を満たすことができます。

「2024年までに、APIの悪用とそれに関連するデータ漏えいが約2倍に増加します」

出典：Gartner: Top 10 Aspects Software Engineering Leaders Need to Know About APIs（英語版のみ）

メリット



セキュリティチームとコンプライアンスチームのワークフローを効率化



専用に構築された PCI 機能により、監査の負担を軽減



コンプライアンス関連イベントに関する実行可能な PCI アラートを受信し記録



PCI 要件を満たすために、Akamai の総合的なセキュリティ・ソリューション・ポートフォリオによってベンダーを統合

Client-Side Protection & Compliance

Web スキミングや Magecart などのクライアントサイド攻撃は、ブラウザーで実行される悪性のコードインジェクションによってオンライン支払いページから決済カードデータをスキミングし、流出させます。これを防ぐための支援をすることにより、新しい JavaScript セキュリティ要件 6.4.3 および 11.6.1 を満たします。

「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しています」

出典 : From Bad Bots to Malicious Scripts: The Effectiveness of Specialized Defense | 2023 (英語版のみ)

Akamai Guardicore Segmentation

単一のプラットフォーム内で統合された複数のテクノロジーを活用して、規制対象の資産をより効率的にセグメント化し、複数の PCI 要件の遵守を支援します。ネットワークと資産の可視化、分散型ファイアウォール、レイヤー 7 までのポリシー適用、違反の検知と応答を実現します。

「ソフトウェア定義のセグメンテーションにより、プロセスレベルでセグメンテーションポリシーを作成して適用できるようになり、セキュリティ体制と PCI-DSS 技術要件を満たすための能力の両方が大幅に強化されました」

— The Honey Baked Ham Company, Senior Infrastructure Engineer

Akamai を活用して PCI DSS v4.0 のコンプライアンスを促進する方法について詳しくは、弊社のエキスパートチームへお問い合わせください。