AKAMAI ソリューション概要

# Akamai による PCI DSS コンプライアンスに備える金融機関の支援

PCI DSS v4.0 では、ペイメントカード業界のセキュリティ基準が 2004 年以降で最も大幅に変更されるため、金融機関はコンプライアンスを維持するために迅速に対応する必要があります。PCI Security Standards Council によって確立されたこの包括的なフレームワークは、カード所有者データを保護するための厳格な対策を義務付けています。Akamai のソリューションは、高度なセキュリティ機能、継続的な監視、堅牢な侵入テストを通じて、金融機関がこれらの進化する要件に対応できるよう支援します。Akamai のツールは、コンプライアンスを合理化し、顧客情報を保護し、PCI の期限である 2025 年 3 月までに機関が準備できるよう支援することを目的に設計されています。

## 統一されたコンプライアンス：単一のプロバイダーで PCI DSS を簡略化

金融機関の場合、PCI DSS コンプライアンスには、従業員トレーニングや企業ポリシーだけでなく、要件の大部分を満たすための高度なセキュリティソフトウェアが必要です。これらの要件は包括的なものであるため、多くの場合、複数のプロバイダーと連携する必要があります。ファイアウォールを必要とする要件もあれば、アイデンティティ管理に関する要件もあります。総合的なテクノロジーを備えた単一のプロバイダーを見つけることができれば、金融機関は監査プロセスをシンプル化するだけでなく、顧客の財務情報のセキュリティを強化することができます。より広範なセキュリティ戦略の一環としてこれらの要件に対応する堅牢なサイバーセキュリティソリューションを採用することは、長期的なコスト削減と複雑さの軽減につながります。Akamai のソリューションポートフォリオは、既存および今後の PCI DSS 要件に対して包括的に対応し、金融機関にシームレスな体験を提供します。

## 対象範囲に関する課題への対処

PCI DSS 要件を満たすことを目指している金融機関にとっての大きな課題は、対象範囲の問題です。PCI によって「対象範囲」と見なされるアプリケーションやネットワーク環境は複合的であり、さまざまな種類のインフラ、テクノロジー、および場所に渡ります。金融機関がインフラにも SaaS ベースのアプリケーションにもクラウドを活用するようになると、そのようなオンプレミスとオンデマンドサービスのハイブリッド環境がさらに複雑さを増します。e コマース事業をオートスケールしている金融機関などでは、特定のワークロードの場所を常に把握することは特に困難です。

対象範囲の課題に対処するために、金融機関は内部ファイアウォール、VLAN、およびアクセス制御リストに着目しました。しかし、これらのレガシーアプリケーションはハイブリッド環境に対応するのに苦戦することが多く、セキュリティギャップを残したまま、複雑さ、ダウンタイム、運用オーバーヘッドが増大します。

### 利点

- **セキュリティとコンプライアンスのワークフローを合理化**
- **専用の PCI 機能で監査の負担を軽減**
- **実用的な PCI コンプライアンスアラートを受信し、ログに記録**
- **機微な財務データの保護**
- **運用効率の向上とコンプライアンスコストの削減**

Akamai Guardicore Segmentation は、カード所有者データ環境（CDE）とその境界を可視化します。これはコンプライアンスプロセスにおける重要なステップです。この可視性により、金融機関は PCI DSS の複数の要件を満たし、ネットワークを包括的に監視することができます。以下に例を示します。

- 要件 1.2.3 は、組織にネットワークの図を保持することを求めています。Akamai Guardicore Segmentation ダッシュボードには CDE と他のネットワーク間のすべてのつながりが表示されるため、金融機関はこの要件を満たすことができます。
- 要件 1.2.4 は、システムとネットワーク間でアカウントデータがどのように移動するかを示すデータフロー図を保持することを組織に求めています。Akamai Guardicore Segmentation のダッシュボードは、必要な接続を表示することで、金融機関がこの要件を検証するのに役立ちます。

## 制御に関する課題への対処

- 要件 1.2.5 では、許可されているすべてのサービス、プロトコル、ポートを識別、承認し、業務上の明確な正当性を確保する必要があることが規定されています。Akamai Guardicore Segmentation は普遍的に適用されるポリシーを実行し、許可されているプロトコルやサービスと許可されていないプロトコルやサービスを見極めることで、金融機関がこの要件を満たすのを支援します。

## クライアントサイドの保護に関する課題への対応

ペイメント・カード・データを受け取る金融機関は、自社の環境に対する責任を負うだけではありません。現代の Web 開発では JavaScript を使用することでイノベーションと一貫性がもたらされていますが、ペイメントカードを処理する組織に課題も生じています。JavaScript はクライアントサイドでの実行が分散化されており、サードパーティに依存しているため、金融機関が監視および管理するのは非常に困難です。攻撃者はこの盲点を悪用し、クライアントサイドで Web サイトに有害なコードを挿入して機微な情報を窃取します。この種の攻撃（Web スキミング、フォームジャッキング、Magecart など）の人気が高まっていることに伴い、クライアントサイドの保護とスクリプトの監視に関する新たな要件が生まれています。

PCI DSS v4.0 では、金融機関は公開されている Web サイトのペイメントページで実行されるすべての JavaScript を追跡し、一覧表を作成し、正当化する必要があります。要件 6.4.3 により、すべてのスクリプトのふるまいの整合性と認可を確保し、これらのスクリプトの一覧表を作成して、個々の必要性を書面で正当化しなければならなくなります。さらに、要件 11.6.1 に基づき、金融機関はペイメントページで行われた不正な変更を検知し、それに対応する必要があります。消費者のブラウザーによって HTTP ヘッダーやペイメントページのコンテンツに対する侵害、変更、追加、削除が行われた兆候などがあった場合、権限のある担当者に変更が通知されなければなりません。

> Akamai Guardicore Segmentation により、レガシーファイアウォールのアップグレードにコストや時間をかけることなく、アタックサーフェスを大幅に削減できました。
>
> **– Dave Wigley 氏、**
> **Daiwa Capital 社、CISO Markets Europe**

## 要約すると、PCI DSS v4.0 は金融機関に次のことを要求しています。

- ペイメントページで実行されるすべてのスクリプトの一覧表を保持し、正当性を維持する
- すべてのスクリプトが承認され、意図したアクションを実行するようにする
- ペイメントページにおける不正なスクリプト変更、保護の改ざん、データ窃取に対処するための検知、アラート、応答メカニズムを確立する

Akamai Client-Side Protection & Compliance は、金融機関が PCI DSS v4.0 の要件 6.4.3 および 11.6.1 を満たすための幅広いサポートを提供します。ペイメントページ上のスクリプトを自動的に追跡して一覧表を作成し、それらの完全性と認可を強化します。セキュリティチームは、事前定義された正当性と自動化されたルールを使用して、ペイメントページで実行されているスクリプトの目的を簡単に正当化できます。このソリューションには、HTTP ヘッダーやペイメントページの保護状態に対する変化を監視する機能もあり、ページの改ざんも防ぐことができます。包括的なダッシュボードと専用の PCI アラートにより、コンプライアンス関連のイベントに迅速に対応し、監査証拠を提供することが容易になります。

## 攻撃からの保護

カード所有者データの保護は PCI DSS の中核的な原則ですが、Web アプリケーションや API が幅広く使用される中、こうしたものが攻撃者のエントリーポイントになる可能性があります。PCI DSS に準拠するために、金融機関はマルウェア、ゼロデイ攻撃、その他のデータ漏えいにつながる可能性のある攻撃からの強力な保護を必要としています。

マルウェア保護モジュールを備えた Akamai App & API Protector は、マルウェアがネットワーク内部に侵入して拡散を開始する前にネットワークのエッジでファイルをスキャンすることで、金融機関をペイメントカード情報のデータ漏えいから保護するのに役立ちます。ペイメント・カード・データを狙う攻撃者が悪用しようとする新たな脆弱性が、API によってもたらされる可能性があります。多くの金融機関は、API のセキュリティが確保されていることを証明するどころか、すべての API を把握することさえできません。カード所有者データを受信または送信する API はすべて PCI DSS の適用範囲内にあります。つまり、金融機関は API の開発と認証を監視し、これらの API を保護する必要があります。

Akamai API Security は、環境全体で API の継続的な探索を自動化します。API と既存のドキュメントを比較して、セキュリティチーム、開発者チーム、API チームに誤設定や脆弱性について通知し、API とエンドポイントにリスクスコアを割り当てます。このようにして継続的に自動化を行うことにより、API 資産の最終更新時に脆弱性の評価が行われるようになります。

## 結論

PCI DSS 制御を実施することの最終的な目的はカード所有者のデータを保護することであり、ひいては顧客と自社を保護することですが、金融機関は依然として監査官を納得させる必要があります。単一のプロバイダーを利用することは、そのための明確なメリットとなります。ネットワークのリアルタイムビューと履歴ビューの両方を使用することで、監査の多くの側面をより迅速かつ容易に満たすことができます。さらに、業界でリーダーシップを発揮している単一のプロバイダーと協力し、更にはそのプロバイダーが PCI DSS の要件を満たすことに成功した顧客を擁している場合は、実施を円滑化し、監査を迅速化し、コンプライアンスを維持するための継続的な支援を得ることができます。Akamai の包括的な可視化と統合ソリューションは、金融機関がコンプライアンスへの取り組みを合理化し、進化する脅威に対する防御を強化するのに役立ちます。

**詳細については、akamai.com または Akamai の営業担当チームにお問い合わせください。**