


ホワイトペーパー

# PCI DSS 4.0へのコンプライアンスを維持するための戦略的アプローチ



# 本文

- 3 概要
  - 4 PCI DSSコンプライアンスの課題
  - 5 高度なサイバー脅威に後れを取らないための対策
  - 6 解決策：PCI DSS 4.0への新たなアプローチ
  - 7 Cloudflareが支援できる主な分野
  - 8 まとめ
- 

## 概要

クレジットカード、デビットカード、プリペイドカードによる決済を処理する企業はすべて、ペイメントカード業界データセキュリティ基準 (PCI DSS) に準拠しなければなりません。基準の適用対象には小規模な商店、小売業者からeコマース (EC) Web サイト、銀行、大手企業まで含まれます。しかし、クラウドとハイブリッドワークへの移行が進む中、PCI DSS 4.0が発表されて基準が進化し、効率的なコンプライアンスが難しくなっています。

デジタル技術で最新化する今日の世界では、コンプライアンスのプロセスを拡張可能な方法で合理化し、企業のデジタルモダナイゼーションに対応して動的に変化する規制状況に適応していく必要があります。



# 現代企業におけるPCI DSSコンプライアンスの課題

PCI DSSへのコンプライアンスは必須で、違反すれば罰金、訴訟、政府による調査の対象となります。しかし、この規制の対象である金融機関、EC事業者、その他がコンプライアンスを確保するにあたってクリアすべき課題がいくつかあります。

また、クラウドコンピューティングやリモートワークへの依存度が高まり、ITチームがデジタル環境のコントロールを喪失しており、それらの課題を解決するプロセスが一層複雑化しています。



**時間とリソースの割り振り:**企業の53%は、プライバシー保護技術者が不足していてコンプライアンスが困難だと回答しています。<sup>1</sup>



**多様な環境でのデータセキュリティ:**クラウドコンピューティングやモバイル決済が普及し、多様で制御が不十分な場合が多い環境でコンプライアンスを保証することがますます難しくなっています。



**技術スタック統合の複雑さ:**暗号化やファイアウォール設定など、コンプライアンス基準への準拠に必要な技術の統合と保守は複雑であることが多く、レガシーシステムを抱えていたり、デジタルトランスフォーメーションを進めていたりする場合はより複雑になります。



**監査:**ITチームはコンプライアンスを保証するため、すべてのインフラとシステムについて最新の監査記録を残さなければなりません。



**ベンダーコンプライアンス:**サードパーティサービスプロバイダーやベンダーのPCI DSS準拠を保証しなければならないことが、課題の解決を一層複雑にしています。



# PCI DSS 4.0で高度なサイバー脅威に後れを取らないよう対策

2022年3月31日に発表されたPCI DSS 4.0は2024年3月31日付で発効し、追加要件は2025年3月31日に発効します。PCI DSS 4.0は以下を目的としています：<sup>2</sup>

## 1. ペイメントカード業界のセキュリティニーズを継続的に充足

- 認証要件の強化：カード会員データ環境 (CDE) へのすべてのアクセスについて、認証 (特に多要素認証) を強化します。パスワード要件も厳しくなり、最低必要文字数が8から12へ増えます。
- 暗号化要件の強化：PCI DSS 4.0では、カード会員データの保存と伝送に「強力な」暗号化技術 (既知の不正利用に対して脆弱性のないTLSなど) を使用するよう義務付けています。
- ECとフィッシング対策の新規要件で絶え間ない脅威に対抗：PCI DSS 4.0では、クライアントサイドセキュリティとフィッシングやソーシャルエンジニアリングからの防御に関する要件が追加されています。

## 2. 継続的プロセスとしてセキュリティを推進

- リスクの分析と管理を一層重視：脆弱性を即座に特定して修正するための継続的なリスク分析・管理プロセスを実装するよう奨励しています。
- 説明責任とガバナンスを強調：PCI DSS 4.0では、セキュリティ制御を維持する上でカード会員データのガバナンスと説明責任が重要であることを強調しています。
- セキュリティ要件の実装と充足の詳細ガイダンス：PCI DSS 4.0は、基準の意図とタイムフレームを明確化しています。

## 3. さまざまな手法が使えるよう柔軟性を付加

- 新技術の統合：PCI DSS 4.0は、クラウドやモバイル決済システムといった新技術のセキュリティについても定めています。
- セキュリティ目標の達成方法に柔軟性：「カスタマイズしたアプローチ」が認められ、要件を満たす手法の範囲が広がりました。また、ターゲットリスク分析に基づくアクション実行の頻度決定についても、より柔軟になっています。

## 4. 検証手法を強化

- 継続的な監視とテスト：新基準では、年次のコンプライアンス検証からセキュリティとコンプライアンスの継続的監視へ切り換えるよう奨励しています。
- コンプライアンスの評価と準拠証明の整合性を強化：コンプライアンスに関する自己評価アンケートやレポートの情報を、コンプライアンス準拠証明書の項目に沿ったものにしていきます。



# 解決策：CloudflareのコネクティビティクラウドでPCI要件への新たなアプローチを実現

IT・セキュリティチームは、現行のセキュリティや技術スタックと容易に統合し、自社のインフラストラクチャやPCI DSSが進化しても対応できるシンプルかつプログラム可能な方法で、PCI DSSの要件を満たす必要があります。

多くのレガシーソリューションや個別セキュリティソリューションを寄せ集めるアプローチでは駄目なのです。必要なのは、企業が自社IT環境のコントロールを回復し、PCI DSSを含めさまざまなコンプライアンス要件を満たせるように設計された、クラウドネイティブのセキュリティサービスとネットワークサービスの統合プラットフォームです。このような統合プラットフォームは、コネクティビティクラウドと呼ばれます。

## Cloudflareのコネクティビティクラウドが提供するのは：

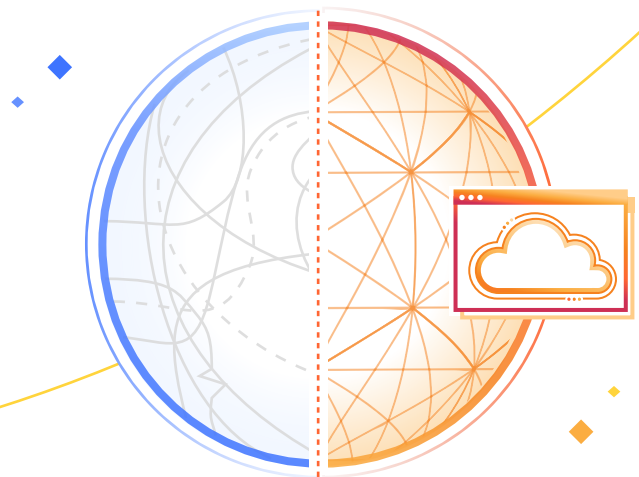
- データコンプライアンスのために設計されたプラットフォーム
- 統合ポリシーエンジン
- 妥協のないデータ主権尊重
- 監査に対応したレポート

ITチームはCloudflareを使って、単一のコントロールプレーンで制御を有効化し、一貫性のある制御を全セッションに適用することができます。

監査のために、Cloudflareのエッジからお好みのSIEMやクラウドへログを直接送信することもできます。また、Cloudflareなら大量のインターネットトラフィックの可視化が可能で、新たな脅威を自動識別して防御することができます。

Cloudflare自体がPCI DSSに準拠し、v4.0の要件をネイティブにサポートしています。例えば、PCI DSS 4.0で重視される多要素認証も、Cloudflareなら簡単に適用できます。さらに、Cloudflareは最新の暗号化規格もサポートし、その作成にもよく貢献しており、機密情報の暗号化に関するPCI DSS 4.0の要件をお客様が満たせるよう支援しています。

PCI DSSの要件とCloudflareコネクティビティクラウドの機能を、次ページで簡単にマッピングしていますのでご覧ください。



# CloudflareがPCI DSS要件の 充足に役立つ主な分野\*

PCI DSSの要件	Cloudflareの機能
1. ネットワークセキュリティ制御を実装し、保守（以前は「ファイアウォールを実装し、保守」）	Cloudflareはネットワーク、アプリケーション、クラウドデプロイメントを悪性ネットワークトラフィックから保護します。Cloudflareは日々数千億件の脅威を分析して得た脅威インテリジェンスに基づいて、Web経由の脅威（OWASPトップ10やゼロデー攻撃など）からWebサイトやWebアプリを保護します。Cloudflareのセキュリティプラットフォームはクラウドネイティブで、数分でデプロイでき、ユーザーは世界的なポリシー変更を数秒でロールアウトすることができます。
2. 全システムコンポーネントにセキュアな設定を適用	Cloudflareの背後にあるユーザー、デバイス、アプリケーションを強力に暗号化し、Web上の潜在攻撃者からマスキングします。ユーザーはCloudflareのAPI Shieldでシークエンスを識別し、APIトランザクション関連のポリシーを適用することにより、API脆弱性の悪用に対する保護を実現できます。
3. 保存データを暗号化などのデータ保護手段によって保護	Cloudflareは保存された個人特定情報（PII）を識別でき、カード会員ログの保管期間に関する要件を満たします。
4. オープンなパブリックネットワークすべてにおいて、カード会員データを暗号化	Cloudflareのグローバルネットワーク経由で送られるトラフィックは、この要件で指定された暗号化規格に準拠しており、Cloudflareはユーザーが特定に必要なPIIの伝送をブロックできます。
5. すべてのシステムとネットワークを悪性ソフトウェアから保護	Cloudflareは毎秒5500万件のHTTPリクエストを処理しており、実際にある最新の攻撃について比類なく広い視野を持っています。Cloudflareは、アンチウィルス、クラウドメールセキュリティ、リモートブラウザ分離などのマルウェア対策保護機能一式をユーザーに提供します。
6. セキュアなシステムとソフトウェアを開発し、保守	Cloudflareは、ユーザーによるセキュリティ違反やSaaSアプリ内で検出された設定ミスのランキングと加重を行えます。Cloudflareのセキュリティサービスを使えば、すべての公開Webアプリケーションを既知の攻撃や不正利用から保護できます。
7. カード会員データへのアクセスを「知る必要がある」人に限定	Cloudflareは、ユーザーの居場所やデータの保存場所を問わず、最小特権の原則に基づくきめ細かなアクセス制御を適用できます。
8. ユーザーを識別し、システムコンポーネントへのアクセスを認証	Cloudflareはそのグローバルネットワークを経由するあらゆるトラフィックに、IDベースのポリシーとセキュリティポスチャチェック（多要素認証の有無確認など）を適用できます。
10. システムコンポーネントとカード会員データへのアクセスをすべてログ化し、監視	Cloudflareは、そのプラットフォーム上にある全製品についてきめ細かな監査ログを提供し、主要なSIEMと統合します。
11. システムとネットワークのセキュリティを定期的にテスト	Cloudflareは、主要製品すべてについて詳細ログを提供するほか、限定アクセスポリシーのテストと侵入検知サービスの機能も提供します。

\*Cloudflareは、PCI DSS 4.0の要件中、物理的セキュリティと組織構造に関する要件9と要件12の準拠支援は行いません。

## まとめ: CloudflareをPCIコンプライアンス要件の充足にお役立てください

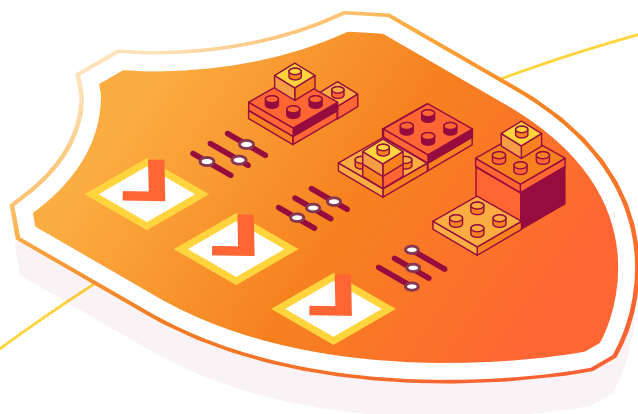
CloudflareはPCI DSSに準拠し、お客様自身がインフラの形態にかかわらずコンプライアンス要件を満たせるように支援します。

実際、Cloudflareの利用によってデータ漏洩の可能性を65%低減し<sup>3</sup>、サイバー保険の年換算保険料を24%削減し<sup>4</sup>、システムやプロセスの管理に費やす時間を59%削減<sup>4</sup>することができます。

“

「当社の法人顧客は、細かく指定したコンプライアンス基準にStaxが従うことを契約で義務付けています。そこで、ゼロトラストのようなセキュリティ制御を適用したわけですが、Cloudflareはまさに当社が必要としていたことをきっちりやってくれました。当社のエンドポイントを保護し、セキュリティをロックダウン型にしたのです。」<sup>5</sup>

Troy Ridgewell氏  
[Stax、セキュリティ責任者](#)



Cloudflareの[データコンプライアンスソリューション](#)に関する情報を今すぐご覧ください。利用開始を[当社の専門担当者](#)にご相談ください。



## 参考文献

1. <https://www.isaca.org/about-us/newsroom/press-releases/2023/privacy-staff-shortages-continue-amid-increasing-demand-for-these-roles>
2. <https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf>
3. IBM Cost of Breach 2022 report
4. 2023 Cloudflare TechValidate Survey of Cloudflare App Service Customers
5. <https://www.cloudflare.com/case-studies/stax>



© 2024 Cloudflare Inc. All rights reserved.  
Cloudflareロゴは、Cloudflareの商標です。その他、  
記載されている企業名、製品名は、各社の商標または  
登録商標である場合があります。

[enterprise@cloudflare.com](mailto:enterprise@cloudflare.com) | [cloudflare.com/ja-jp](https://cloudflare.com/ja-jp)

REV: BDES-5776.2024APR09