

Payment Card Industry (PCI) データセキュリティ基準

オンサイト評価の準拠証明書 – 加盟店

バージョン 3.2

2016年4月

ご利用条件への同意

全ての目的において、PCIのSSCサイトに記載された英文テキストがこの文書の正式版とみなされるものとし、このテキストと英文テキスト間に曖昧さや矛盾がある場合は、英文テキストが優先されるものとします。

セクション 1: 評価情報

提出に関する指示

加盟店は「PCI データセキュリティ基準 (PCI DSS) 要件およびセキュリティ評価手順」の自己問診結果を表明するものとしてこの準拠証明書記入を完了する必要があります。この文書のすべてのセクションの記入を完了してください。加盟店は、該当する場合、各セクションが関連当事者によってされることを確認する責任を負います。レポートおよび提出手順については、アクワイアラー (加盟店銀行) またはペイメントブランドにお問い合わせください。

パート 1. 加盟店と認定セキュリティ評価機関の会社情報

パート 1a. 加盟店の会社情報

会社名:		DBA (商号):	
担当者名:		役職:	
電話番号:		電子メール:	
会社住所:		市区町村:	
都道府県:		国:	
URL:		郵便番号:	

パート 1b. 認定セキュリティ評価機関の会社情報 (該当する場合)

会社名:			
QSA リーダーの名前:		役職:	
電話番号:		電子メール:	
会社住所:		市区町村:	
都道府県:		国:	
URL:		郵便番号:	

パート 2. 概要

パート 2a. 加盟店のビジネスの種類 (該当するものすべてにチェック)

- 小売 情報通信 食料雑貨およびスーパーマーケット
 石油 電子商取引 通信販売 (MOTO)
 その他 (記入してください):

あなたの会社はどのような種類の支払チャネルを提供していますか?

- 通信販 (MOTO)
 電子商取引
 カード提示 (対面式)

この評価でカバーされている支払チャネルはどれですか?

- 通信販売 (MOTO)
 電子商取引
 カード提示 (対面式)

注: あなたの会社の支払チャネルまたは処理でこの評価でカバーされていないものがある場合は、それら他のチャネルの検証についてアクワイアラーまたはペイメントブランドに相談してください。

パート 2b. 支払カードビジネスの説明

カード会員データをどのように、またどのような機能で、保存、処理、伝送していますか？

パート 2c. 場所

PCI DSS レビューに含まれている施設の種類の種類(小売店、事業所、データセンター、コールセンターなど)と場所の概要を挙げてください。

施設の種類の種類	この種類の施設の数の数	施設の場所(市区町村、国)
例: 小売店	3	米国マサチューセッツ州ボストン

パート 2d. ペイメントアプリケーション

会社で一つまたは複数のペイメントアプリケーションが使用されていますか？ はい いいえ

あなたの会社が使用するペイメントアプリケーションについての次の情報を記入してください。

ペイメントアプリケーションの名前	バージョン番号	アプリケーションベンダ	アプリケーションは PA-DSS に記載されているものですか？	PA-DSS 検証の有効期限(該当する場合)
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	

パート 2e. 環境の説明

この評価の対象となる環境の概要を説明しています。

例:

- カード会員データ環境(CDE)との接続
- POS 装置、データベース、Web サーバなど、カード会員データ環境内の重要なコンポーネント、および該当する場合に必要な他の支払要素

あなたの会社は、PCI DSS 環境の範囲に影響するようなネットワークセグメンテーションを使用していますか？(ネットワークセグメンテーションについては、PCI DSS の「ネットワークセグメンテーション」セクションを参照してください。)

はい いいえ

パート 2f. 第三者サービスプロバイダ

あなたの会社は認定インテグレータまたはリセラ(QIR)を利用していますか?

はい いいえ

「はい」と答えた場合:

QIR の会社名:

QIR の個人名:

QIR によって提供されるサービスの説明:

あなたの会社は、第三者サービスプロバイダ(認定インテグレータまたはリセラ(QIR)、ゲートウェイ、ペイメントプロセサー、ペイメントサービスプロバイダ(PSP)、Web ホスティング業者、航空券予約業者、ポイントサービス業者など)とカード会員データを共有していますか?

はい いいえ

「はい」と答えた場合:

サービスプロバイダ名:

提供されるサービスの説明:

サービスプロバイダ名:	提供されるサービスの説明:

注: 要件 12.8 は、このリスト上のすべての事業体に適用されます。

セクション 2: 準拠に関するレポート

本準拠証明書は、添付の準拠に関するレポート(ROC) に文書化されているオンサイト評価の結果を反映するものです。

本準拠証明書と ROC に文書化されている自己問診の完了日:	
ROC の要件を満たすために代替コントロールは使用されましたか?	<input type="checkbox"/> はい <input type="checkbox"/> いいえ
ROC の要件に不適用として特定されたものがありますか(N/A)?	<input type="checkbox"/> はい <input type="checkbox"/> いいえ
テストされなかった要件はありますか?	<input type="checkbox"/> はい <input type="checkbox"/> いいえ
ROC の要件で、法的制限により満たすことができなかったものがありますか?	<input type="checkbox"/> はい <input type="checkbox"/> いいえ

セクション 3: 検証と証明の詳細

パート 3. PCI DSS 検証

この AOC は ROC の日付(ROC 完了日)に記載された結果を基にしています。

前述の ROC に記載された結果を基に、パート 3b-3d で指定された署名者は、本書のパート 2 に記載されている事業体について以下の準拠状態を証明します。(1 つ選んでください)

<input type="checkbox"/>	<p>準拠: PCI DSS ROC の必ずしもすべてのセクションを完了していない、またはすべての質問に対して肯定的に答えため、全体的な評価が準拠になり、(加盟店名)は PCI DSS に完全に準拠していることを示しました。</p>						
<input type="checkbox"/>	<p>非準拠: PCI DSS ROC のすべてのセクションを完了していないか、一部の質問に対して肯定的に答えられていないため、全体的な評価が非準拠になり、(加盟店名)は PCI DSS に完全には準拠していないことを示しました。</p> <p>準拠の目標期日:</p> <p>非準拠の状態でのフォームを提出する事業体は、本書のパート 4 にあるアクションプランを完了しなければならない場合があります。パート 4 を完成させる前にアクワイアラーまたはペイメントブランドに確認してください。</p>						
<input type="checkbox"/>	<p>準拠、法的例外付き: 法的制限のために要件を満たすことができないため、1 つ以上の要件に "未対応" と答えられています。このオプションには、アクワイアラーまたはペイメントブランドからの追加レビューが必要です。</p> <p>選択されている場合、次の各項目に記入してください。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">影響を受けた要件</th> <th style="width: 50%;">法的制限により要件を満たすことができなかった理由の詳細</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> </tbody> </table>	影響を受けた要件	法的制限により要件を満たすことができなかった理由の詳細				
影響を受けた要件	法的制限により要件を満たすことができなかった理由の詳細						

パート 3a. 状態の確認

署名者が以下を確認します。

(該当する項目すべてにチェック)

<input type="checkbox"/>	ROC は、「PCI DSS 要件およびセキュリティ評価手順」バージョン (バージョン番号) の指示に従って完了されました。
<input type="checkbox"/>	上記で参照されている ROC およびこの証明書のすべての情報は、評価の結果をすべての重要な点において公平に表しています。
<input type="checkbox"/>	当社は、自社のペイメントアプリケーションベンダに、自社のペイメントシステムでは承認後の機密認証データが保存されないことを確認しました。
<input type="checkbox"/>	私は PCI DSS を読み、当社の環境に適用される範囲において、常に PCI DSS への完全な準拠を維持する必要があることを認識しています。
<input type="checkbox"/>	当社の環境が変化した場合、私は新しい環境を再評価し、該当する追加の PCI DSS 要件を導入する必要があることを認識しています。

パート 3a. 状態の確認 (続き)

- 取引承認後にフルトラックデータ¹、CAV2、CVC2、CID、または CVV2 データ²、または PIN データ³が保存されているという証拠は、この評価でレビューされたすべてのシステムで見つかりませんでした。
- ASV スキャンは PCI SSC 認定の認定スキャンベンダ (ASV 名) が完了

パート 3b. 加盟店の証明書

加盟店役員の署名 ↑

日付:

加盟店役員名:

役職:

パート 3c. 認定セキュリティ評価機関 (QSA) の確認 (該当する場合)

この評価に QSA が関与しているか、支援している場合、実施した役割を説明してください。

QSA 企業の正式に認定された責任者の署名 ↑

日付:

正式に認定された責任者の名前:

QSA の会社:

パート 3d. 内部セキュリティ評価機関 (ISA) の関与 (該当する場合)

この評価に ISA が関与しているか、支援している場合、その ISA の担当者を記入し、実施した役割を説明してください。

¹ カードを提示する取引中に、承認のために使用される磁気ストライブのエンコードされたデータまたはチップ内の同等のデータ。取引承認の後、事業者はフルトラックデータ全体を保持してはいけません。保持できるトラックデータの要素は、プライマリアカウント番 (PAN)、有効期限、カード会員名のみです。

² カードを提示しない取引を検証するために使用される、署名欄またはペイメントカードの前面に印字されている 3 桁または 4 桁の値。

³ カードを提示する取引中に、カード会員によって入力される個人識別番号、または取引メッセージ内に存在する暗号化された PIN ブロック、あるいはその両方。

パート 4. 非準拠要件に対するアクションプラン

要件ごとに該当する“PCI DSS 要件への準拠状態”を選択してください。要件に対して“いいえ”を選択した場合は、会社が要件に準拠する予定である日付と、要件を満たすために講じられるアクションの簡単な説明を記入する必要があります。

パート 4 を完成させる前にアクワイアラーまたはペイメントブランドに確認してください。

PCI DSS 要件	要件の説明	PCI DSS 要件への準拠 (1 つ選んでください)		修正日とアクション (“いいえ”が選択されている要件すべて)
		はい	いいえ	
1	カード会員データを保護するために、ファイアウォールをインストールして構成を維持する	<input type="checkbox"/>	<input type="checkbox"/>	
2	システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない	<input type="checkbox"/>	<input type="checkbox"/>	
3	保存されるカード会員データを保護する	<input type="checkbox"/>	<input type="checkbox"/>	
4	オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	<input type="checkbox"/>	<input type="checkbox"/>	
5	すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する	<input type="checkbox"/>	<input type="checkbox"/>	
6	安全性の高いシステムとアプリケーションを開発し、保守する	<input type="checkbox"/>	<input type="checkbox"/>	
7	カード会員データへのアクセスを、業務上必要な範囲内に制限する	<input type="checkbox"/>	<input type="checkbox"/>	
8	システムコンポーネントへのアクセスを識別・認証する	<input type="checkbox"/>	<input type="checkbox"/>	
9	カード会員データへの物理アクセスを制限する	<input type="checkbox"/>	<input type="checkbox"/>	
10	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	<input type="checkbox"/>	<input type="checkbox"/>	
11	セキュリティシステムおよびプロセスを定期的にテストする	<input type="checkbox"/>	<input type="checkbox"/>	
12	すべての担当者の情報セキュリティポリシーを整備する	<input type="checkbox"/>	<input type="checkbox"/>	
付録 A2	SSL/early TLS を使用している事業者向けの PCI DSS 追加要件	<input type="checkbox"/>	<input type="checkbox"/>	

