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

オンサイト評価 - サービスプロバイダ
準拠証明書

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

サービスプロバイダは、「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の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。サービスプロバイダは、該当する場合、各セクションが関連当事者によって記入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、要求元のペイメントブランドに問い合わせてください。

パート 1. サービスプロバイダと認定セキュリティ評価機関の情報					
パート 1a. サービスプロバイダの組織情報					
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:		郵便番号:	
URL:					

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:		郵便番号:	
URL:					

パート 2. 概要

パート 2a. 評価範囲の検証

PCI DSS 評価範囲に含まれていた提供されたサービス(該当するものすべてを選んでください)

評価したサービスの名前:		
評価したサービスの種類:		
ホスティングプロバイダ: ☐ アプリケーション/ソフトウェア ☐ ハードウェア ☐ インフラ/ネットワーク ☐ 物理空間(ロケーション) ☐ 保存 ☐ Web ☐ セキュリティサービス ☐ 3-D 安全なホスティングプロバイダ ☐ 共有ホスティングプロバイダ: ☐ その他のホスティング(具体的に記入してください):	**管理サービス(具体的に記入してください):** ☐ システムセキュリティサービス ☐ IT サポート ☐ 物理セキュリティ ☐ 端末管理システム ☐ その他のサービス(具体的に記入してください):	**支払の処理:** ☐ POS/カード提示 ☐ インターネット/電子商取引 ☐ MOTO/コールセンター ☐ ATM ☐ その他の処理(具体的に記入してください):
☐ アカウント管理	☐ 不正行為および返金サービス	☐ ペイメントゲートウェイ/スイッチ
☐ バックオフィスサービス	☐ イシュアの処理	☐ プリペイドサービス
☐ 請求管理	☐ ロイヤルティプログラム	☐ 記録管理
☐ 清算と決済	☐ 加盟店のサービス	☐ 税金/政府支払い
☐ ネットワークプロバイダ		
☐ その他(具体的に記入してください):		

__注__: これらのカテゴリは一般的な例としてのみ提供されており、事業所のサービスの説明を制限したり事前指定するものではありません。これらのカテゴリがあなたの会社のサービスに適合しない場合は、"その他" に記入してください。あるカテゴリがあなたの会社のサービスに適格かわからない場合は、該当するペイメントブランドにご確認ください。

パート 2a. 評価範囲の検証 *(続き)*

サービスプロバイダによって提供されているが、PCI DSS 評価範囲に含まれていなかったサービス(当てはまるものをすべて選んでください):

評価しなかったサービスの名前:	

評価しなかったサービスの種類:

ホスティングプロバイダ:	**管理サービス(具体的に記入してください):**	**支払の処理:**
☐ アプリケーション/ソフトウェア	☐ システムセキュリティサービス	☐ POS/カード提示
☐ ハードウェア	☐ IT サポート	☐ インターネット/電子商取引
☐ インフラ/ネットワーク	☐ 物理セキュリティ	☐ MOTO/コールセンター
☐ 物理空間(ロケーション)	☐ 端末管理システム	☐ ATM
☐ 保存	☐ その他のサービス(具体的に記入してください):	☐ その他の処理(具体的に記入してください):
☐ Web		
☐ セキュリティサービス		
☐ 3-D 安全なホスティングプロバイダ		
☐ 共有ホスティングプロバイダ:		
☐ その他のホスティング(具体的に記入してください):		
☐ アカウント管理	☐ 不正行為および返金サービス	☐ ペイメントゲートウェイ/スイッチ
☐ バックオフィスサービス	☐ イシュアの処理	☐ プリペイドサービス
☐ 請求管理	☐ ロイヤルティプログラム	☐ 記録管理
☐ 清算と決済	☐ 加盟店のサービス	☐ 税金/政府支払い
☐ ネットワークプロバイダ		

☐ その他(具体的に記入してください):

選択したサービスが評価に含まれていない理由の短い説明:	

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?	
それ以外で、どのように、またどのような機能で、カード会員データのセキュリティに影響を及ぼしているか、影響を及ぼすことができますか?	

パート 2c. 場所

PCI DSS レビューに含まれている施設の種類（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:	この種類の施設の数	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）
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ 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となる他の支払要素*	
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、検証対象となるサービスの目的で、認定インテグレータまたはリセラ（QIR）と関係がありますか? 「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:	☐ はい ☐ いいえ
あなたの会社は、ここで検証しているサービスの目的で、1 つ以上のサードパーティサービスプロバイダと関係がありますか（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）?	☐ 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:**

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。*

パート 2g. テストした要件の概要

各 PCI DSS 要件に対して、以下から 1 つ選んでください。

- **完全** - その要件およびその下位要件すべてを評価し、ROC で「未テスト」または「該当なし」とマークした下位要件はない。
- **部分的** - その要件の下位要件のうちの 1 つ以上に対し、ROC で「未テスト」または「該当なし」とマークした。
- **なし** - その要件のすべての下位要件に対し、ROC で「未テスト」または「該当なし」とマークした。

「部分的」または「なし」とマークしたすべての要件に対し、以下を含む詳細を「アプローチの正当理由」欄に記入してください。

- ROC で「未テスト」または「該当なし」としてマークした下位要件の詳細
- その下位要件が未テストまたは該当なしである理由

***注:** このAOC の対象となる各サービスに対してそれぞれ 1 つの表に記入してください。このセクションの追加コピーは PCI SSC の Web サイトにあります。*

評価したサービスの名前:	

	評価した要件の詳細			
PCI DSS 要件	**完全**	**部分的**	**なし**	**アプローチの正当理由** （「部分的」と「なし」回答すべてに必要。どの下位要件が未テストまたは該当なしであるかを記入。）
要件 1:	☐	☐	☐	
要件 2:	☐	☐	☐	
要件 3:	☐	☐	☐	
要件 4:	☐	☐	☐	
要件 5:	☐	☐	☐	
要件 6:	☐	☐	☐	
要件 7:	☐	☐	☐	
要件 8:	☐	☐	☐	
要件 9:	☐	☐	☐	
要件 10:	☐	☐	☐	
要件 11:	☐	☐	☐	
要件 12:	☐	☐	☐	
付録 A1:	☐	☐	☐	
付録 A2:	☐	☐	☐	

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?	☐ はい	☐ 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）?	☐ はい	☐ いいえ
テストされなかった要件はありますか?	☐ はい	☐ 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?	☐ はい	☐ 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***)

☐	**準拠:** PCI DSS ROC のすべてのセクションを完了し、すべての質問に対して肯定的に答えたため、全体的な評価が**準拠**になり、*(サービスプロバイダの会社名)*は PCI DSS に完全に準拠していることを示しました。
☐	**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、*(サービスプロバイダの会社名)*は PCI DSS に完全には準拠していないことを示しました。 準拠の**目標期日:** 非準拠の状態でこ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 を完成させる前にペイメントブランドに確認してください。*
☐	**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。 *選択されている場合、次の各項目に記入してください。*

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)

☐	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。
☐	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。
☐	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。
☐	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。
☐	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 認定の認定スキャニングベンダー*(ASV 名)*が完了

パート 3b. サービスプロバイダの証明書	
サービスプロバイダ役員の署名 ↑	*日付:*
サービスプロバイダ役員名:	*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プ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、事業体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号（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 を完成させる前に該当する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	☐	☐	
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	☐	☐	
3	保存されるカード会員データを保護する	☐	☐	
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	☐	☐	
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	☐	☐	
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	☐	☐	
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	☐	☐	
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	☐	☐	
9	カード会員データへの物理アクセスを制限する	☐	☐	
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	☐	☐	
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	☐	☐	
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	☐	☐	
付録 A1	共有ホスティングプロバイダ向けの PCI DSS 追加要件	☐	☐	
付録 A2	SSL/early TLS を使用している事業体向けの PCI DSS 追加要件	☐	☐	