

PCI

データセキュリティ基準(PCIDSS)

自己査定アンケート**A**と遵守証明書

カード会員データの電子保管、処理、通信は行いません。

バージョン**1.1**

2008年2月

目次

PCI データセキュリティ基準(PCIDSS) : 関連文書	ii
開始前に	iii
自己査定アンケートの完了	iii
PCI DSS 遵守 – 完了ステップ	iii
PCI DSS SAQ A、v1.1、遵守証明書 2008年2月	1
自己査定アンケート A	4
厳しいアクセス規制措置の実装	4
要件 9 : カード会員データへの物理的アクセスを制限する。	4
情報セキュリティ方針の管理	4
要件 12 : 従業員と契約者に向けた、情報セキュリティ取り扱いの方針を管理する。	4

PCI データセキュリティ基準(PCIDSS) : 関連文書

以下の文書は、加盟店とサービスプロバイダーのPCIデータセキュリティ基準(PCIDSS)およびPCI DSS SAQの理解を促進するために作成されたものです。

文書	対象
PCIデータセキュリティ基準(PCIDSS)	すべての加盟店とサービスプロバイダー
PCI DSSナビゲート: 基準要件の目的理解	すべての加盟店とサービスプロバイダー
PCIデータセキュリティ基準(PCIDSS): 自己査定ガイドラインとインストラクション	すべての加盟店とサービスプロバイダー
PCIデータセキュリティ基準(PCIDSS): 自己査定アンケートA(PCI DSS SAQ A)と証明書	加盟店 ¹
PCIデータセキュリティ基準(PCIDSS): 自己査定アンケートBと証明書	加盟店 ¹
PCIデータセキュリティ基準(PCIDSS): 自己査定アンケートCと証明書	加盟店 ¹
PCIデータセキュリティ基準(PCIDSS): 自己査定アンケートDと証明書	サービスプロバイダーとすべてのその他加盟店 ¹
PCI DSS用語集、略語、および頭文字語	すべての加盟店とサービスプロバイダー

¹ 適切な自己査定アンケートを決定するには、PCIデータセキュリティ基準: 自己査定ガイドラインとインストラクション、「あなたの会社に最もよく合う SAQ および証明書の選び方」を参照してください。

開始前に

自己査定アンケートの完了

SAQ A は、カード会員データのカード利用控え領収書だけを保管し、その敷地内で電子形式でカード会員データを保管、処理、送受信を行わない加盟店に適用される要件を示すために作成されました。

ここ、および PCI DSS 自己査定ガイドラインとインストラクションで SAQ 認証タイプ 1 と定義されるこれらの加盟店は、その敷地内で電子形式でカード会員データを保管せず、カード会員データを処理、送信しません。このような加盟店は、SAQ A と関連遵守証明を完了させ、以下の事項を確認し、遵守を立証する必要があります。

- あなたの会社は非対面式(電子商取引かメール/電話による注文)商取引のみを扱います。
- あなたの会社は、その敷地内でカード会員データを保管、処理、送受信しませんが、これらの機能の扱いを第三者サービスプロバイダーに委託しています。
- あなたの会社は、第三者サービスプロバイダーのカード会員データの保管、処理、そして/または、送受信が PCI DSS を遵守するものであることを確認しました。
- あなたの会社はカード会員データのカード利用控えもしくは領収書のみを保管し、これらの文書が電子的に受信されることはありません。および
- あなたの会社は電子形式でカード会員データを保管していません。

このオプションは、対面式の POS 環境を持つ加盟店に適用されることはありません。

PCI DSS 遵守 – 完了ステップ

1. 自己査定アンケートインストラクションおよびガイドラインに従って、自己査定アンケート (SAQ A) を完了させてください。
2. 遵守証明書をすべて完了させてください。
3. SAQ および遵守証明書を、その他求められる文書すべてと一緒にアクワイアラに提出してください。

PCI DSS SAQ A、v1.1、遵守証明書

2008年2月

提出方法

加盟店は、PCI データセキュリティ基準(PCIDSS)の遵守状態の宣言として、遵守証明書を完了させる必要があります。すべての適用セクションを完了させ、本書内の「PCI DSS 遵守 - 完了ステップ」にある提出方法を参照してください。

パート1 認定審査機関(QSA)会社情報 (該当する場合)

会社名 :					
QSA 問い合わせ担当者名 :		役職 :			
電話 :		電子メール :			
事業所住所 :					
州/県 :		国 :		郵便番号 :	
URL :					

パート2 加盟店会社情報

会社名 :		データベース管理者 (DBA(S)) :			
問い合わせ担当者名 :		役職 :			
電話 :		電子メール :			
事業所住所 :					
州/県 :		国 :		郵便番号 :	
URL :					

パート 2a 加盟店業種 (適用するものすべてチェックしてください) :

- 小売ベンダー
 電気通信
 食料品店とスーパーマーケット
 石油
 電子商取引
 メール/電話による注文
 その他(具体的に記入してください):

PCI DSS の審査に含まれる施設および所在地をリストしてください。

パート2b 関係

あなたの会社は、1つ以上の第三者サービスプロバイダー(例えば、ゲートウェイ、ウェブホスティング会社、航空券予約代理店、ロイヤルティプログラム会社など)と関係を結んでいますか? はい いいえ

あなたの会社には、1つ以上のアクワイアラとの関係がありますか? はい いいえ

パート2c SAQ Aに該当する加盟店

以下に該当する加盟店は、短縮版自己査定アンケートを完了する必要があります。

<input type="checkbox"/>	§ あなたの会社は、その敷地内でカード会員データを保管、処理、送受信しませんが、これらの機能の扱いを第三者サービスプロバイダーに委託しています。
<input type="checkbox"/>	カード会員データの保管、処理、そして/または送信を取り扱う第三者サービスプロバイダーがPCI DSSを遵守していることを確認しました。
<input type="checkbox"/>	加盟店は電子形式でカード会員データを保管しません。そして
<input type="checkbox"/>	加盟店がカード会員データを保管する場合、そのデータはカード利用控または領収書のコピーであり、電子的に受信することはありません。

パート3 PCI DSS認証

(completion date)付けのSAQ Aの記入結果に基づき、(Merchant Company Name)は以下の遵守状態を証明します。(1つをチェックする)

- 遵守:PCI SAQのすべてのセクションを完了し、そのすべての質問に対し「はい」と答え、その結果、評価は全面的遵守となり、(Merchant Company Name)のPCI DSSへの完全な遵守が証明されました。
- 未遵守 : PCI SAQのすべてのセクションが完了していない、または質問のいくつかに対し「いいえ」と答えた結果、評価は全面的未遵守となり、(Merchant Company Name)のPCI DSSへの完全な遵守が証明されませんでした。
 - 遵守の目標日程
 - 未遵守の状態でのこのフォームを提出する事業者は、本書のパート4にある行動計画を行うことを求められることがあります。カードブランドによってはこのセクションを必要としない場合がありますので、パート4を完了する前にアクワイアラもしくはカードブランドを確認してください。

パート3a 遵守状況の確認

加盟店は以下を確認します。

<input type="checkbox"/>	PCI DSS自己査定アンケートA、バージョン(SAQ version #)は同書にあるインタラククションに従って完了されました。
<input type="checkbox"/>	上述のSAQおよび本証明書にあるすべての情報は、自社の査定の結果を公正に示すものです。
<input type="checkbox"/>	自社はPCI DSSを読み、いかなるときもPCI DSSへの完全な遵守を行う必要があることを認めます。

パート3b 加盟店承認

加盟店役員の署名 ↑	日付 ↑
加盟店役員名 ↑	役職： ↑
加盟店会社代表 ↑	

パート4 未遵守の行動計画

各要件に適切な「遵守状態」を選択してください。要件のいずれかに「いいえ」と回答する場合、要件を遵守する日程および要件を満たす行動の詳細を簡単に説明し、提出する必要があります。カードブランドによってはこのセクションを必要としない場合がありますので、パート4を完了する前にアクワイアラもしくはカードブランドを確認してください。

PCI DSS 要件	要件の詳細	遵守状態(1つを選択してください)		改善日程および行動 (遵守状態が「いいえ」である場合)
		はい	いいえ	
9	カード会員データへの物理的アクセスを制限する。	<input type="checkbox"/>	<input type="checkbox"/>	
12	情報セキュリティを扱う方針を管理する。	<input type="checkbox"/>	<input type="checkbox"/>	

自己査定アンケート A

完了日：

厳しいアクセス規制措置の実装

要件 **9**：カード会員データへの物理的アクセスを制限する。

9.6	カード会員データを含むすべての紙と電子メディアは、物理的に安全ですか？ (このメディアには、コンピュータ、電子メディア、ネットワーク、通信ハードウェア、通信回線、紙の受領書、カード利用控、およびファックスなどが含まれます。)	<input type="checkbox"/>	<input type="checkbox"/>
9.7	(a) 社内、または社外に分配されたカード会員データを含むあらゆる種類のメディアに関し、厳重な管理が行われていますか？	<input type="checkbox"/>	<input type="checkbox"/>
	(b) この管理には、以下が含まれていますか？		
9.7.1	メディアは、部外秘と識別できるように分類されていますか？	<input type="checkbox"/>	<input type="checkbox"/>
9.7.2	メディアは安全な宅配便または正確に追跡できる他の発送方法で送られていますか？	<input type="checkbox"/>	<input type="checkbox"/>
9.8	安全な場所からメディアを動かす前に、管理者の承認を得る(特にメディアが個人に配布される場合)プロセスや手順が実行されていますか？	<input type="checkbox"/>	<input type="checkbox"/>
9.9	カード会員データを含むメディアの保管とアクセシビリティに関し、厳重な管理が行われていますか？	<input type="checkbox"/>	<input type="checkbox"/>
9.10	業務上または法律上に必要でなくなった場合、カード会員データを含むメディアは破棄されていますか？ 破棄の方法は以下のものである必要があります。	<input type="checkbox"/>	<input type="checkbox"/>
9.10.1	ハードコピーの文書は、クロスカットシュレッダーにかけるか、焼却するか、またはパルプにされていますか？	<input type="checkbox"/>	<input type="checkbox"/>

情報セキュリティ方針の管理

要件 **12**：従業員と契約者に向けた、情報セキュリティ取り扱いの方針を管理する。

質問	回答：	<u>はい</u>	<u>いいえ</u>
12.8	カード会員データがサービスプロバイダーと共有される場合、契約により以下が求められていますか？	<input type="checkbox"/>	<input type="checkbox"/>
12.8.1	サービスプロバイダーは PCI DSS 要件を厳守する必要がありますか？	<input type="checkbox"/>	<input type="checkbox"/>

質問	回答 :	<u>はい</u>	<u>いいえ</u>
12.8.2 契約には、サービスプロバイダーはプロバイダーが所有するカード会員データのセキュリティに責任を負うという認識が含まれていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>