

## PCI

データセキュリティ基準(PCIDSS)

自己査定アンケート **B**

および遵守証明書

---

インプリンタまたはスタンドアロン型**CAT**端末のみ。カード会員データの電子保管は行いません。

バージョン **1.1**

2008年2月

## 目次

---

|   |            |
|---|------------|
| <b>PCI データセキュリティ基準(PCIDSS) : 関連文書</b> .....     | <b>iii</b> |
| 開始前に .....                                      | <b>iv</b>  |
| 自己査定アンケートの完了 .....                              | <b>iv</b>  |
| <b>PCI DSS 遵守 – 完了ステップ</b> .....                | <b>iv</b>  |
| <b>遵守証明書、SAQ B</b> .....                        | <b>1</b>   |
| <b>自己査定アンケート B</b> .....                        | <b>6</b>   |
| カード会員データの保護 .....                               | <b>6</b>   |
| 要件 3 : 保管されたカード会員データを保護する。 .....                | 6          |
| 要件 4 : オープンまたはパブリックネットワークのカード会員データの送信を暗号化する .   | 6          |
| 厳しいアクセス規制措置の実装 .....                            | <b>7</b>   |
| 要件 7 : 既知の業務のニーズによりカード会員データへのアクセスを制限する .....    | 7          |
| 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。 .....            | 7          |
| 情報セキュリティ方針の管理 .....                             | <b>8</b>   |
| 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。 ..... | 8          |

## 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の理解の向上の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 <sup>1</sup>                   |
| 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 <sup>1</sup>                   |
| 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 <sup>1</sup>                   |
| 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 <sup>1</sup> |
| 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                 |

<sup>1</sup> 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 B** は、インプリンタまたはスタンドアロン型 **CAT** 端末のみにより、カード会員データを処理する加盟店に適用される要件を示すために作成されたものです。

これらの加盟店は本書、**PCI DSS** 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で **SAQ** 認証タイプ 2 および 3 と定義されています。 **SAQ** 認証タイプ 2 の加盟店は、カード会員データをインプリンタのみにより処理します。 **SAQ** 認証タイプ 3 の加盟店は、カード会員データをスタンドアロン型 **CAT** 端末のみにより処理します。 これらの加盟店のタイプは、電子取引を行っていない（対面式）従来型の、または（非対面式）電子商取引もしくはメール／電話による注文を受ける加盟店のいずれかとなります。 以上の加盟店は、**SAQ B** と関連遵守証明書を完了させ、以下の事項を確認し、遵守を証明する必要があります。

#### 認証タイプ 2：

- あなたの会社はインプリンタのみを使用しています。
- あなたの会社は電話線またはインターネットを介して、カード会員データを送受信しません。
- あなたの会社はカード会員データのカード利用控もしくは領収書のみを保管します。そして
- あなたの会社はカード会員データの電子保管を行いません。

#### 認証タイプ 3：

- あなたの会社はスタンドアロン型 **CAT** 端末（電話線により処理装置に接続）のみを使用しています。
- スタンドアロン型 **CAT** 端末は他のシステムやインターネットに接続されていません。
- あなたの会社はカード会員データのカード利用控もしくは領収書のみを保管します。そして
- あなたの会社はカード会員データを電子保管しません。

アンケートの各セクションでは、**PCI** データセキュリティ基準(**PCIDSS**)の要件に基づき、特定のセキュリティ分野に焦点をあてています。

### **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 B**)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。

## 遵守証明書、SAQ B

### 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 : |  | タイトル :  |  |        |
| 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 : |  | タイトル :               |  |        |
| 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 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 取引処理**

使用しているペイメントアプリケーション(PA) :

ペイメントアプリケーション(PA)バージョン :

## パート2d SAQ B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"/> | A. <input type="checkbox"/>        | 加盟店は、インプリンタを使用してクレジットカード情報をインプリントし、カード会員データを電話線またはインターネットを介して送信しません。  |
|                          | または<br>B. <input type="checkbox"/> | 加盟店はスタンドアロン型CAT端末を使用し、加盟店の周囲の環境でこのCAT端末はインターネットまたはその他のシステムに接続されていません。 |
| <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 B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への完全な遵守が示されました。
- 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 #)は同書にあるイントラ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、使用している決済システムが認証後に機密認証データを保管しないものであることを、ペイメントアプリケーション(PA)会社に確認しました。  |
| <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。   |
| <input type="checkbox"/> | 決済認証後、磁気ストライプ (例えば、追跡)データ <sup>2</sup> 、CAV2、CVC2、CID、またはCVV2データ <sup>3</sup> 、もしくはは暗証番号データ <sup>4</sup> がこの認証中に審査されるいかなるシステムにも保管された形跡はありません。 |

<sup>2</sup> 対面式決済の認証に使用される磁気ストライプ内にエンコードされたデータ。決済認証の後、事業者はいかなる磁気ストライプデータを保持することはありません。追跡データの中で、保持してもよいものは、カード番号、有効期限、氏名のみです。

<sup>3</sup> 署名欄かその右、もしくはクレジットカード表面に印刷されている3桁または4桁の数字は非対面式決済に使用されるもの。

<sup>4</sup> 対面式決済中に、カード会員により入力された暗証番号(PIN)、および/または決済メッセージ中に暗号化されたPINブロック。

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

各要件の適切な「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<br>(遵守状態が「いいえ」である場合) |
|------------|---------------------------------------|--------------------------|--------------------------|--------------------------------|
|            |                                       | はい                       | いいえ                      |                                |
| 3          | 保管されたカード会員データを保護する。                   | <input type="checkbox"/> | <input type="checkbox"/> |                                |
| 4          | オープンまたはパブリックネットワークのカード会員データの送信を暗号化する。 | <input type="checkbox"/> | <input type="checkbox"/> |                                |
| 7          | 既知の業務のニーズによりカード会員データへのアクセスを制限する。      | <input type="checkbox"/> | <input type="checkbox"/> |                                |
| 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 B

完了日：

### カード会員データの保護

要件 3： 保管されたカード会員データを保護する。

| 質問  | 回答： | はい                       | いいえ                      |
|---|-----|--------------------------|--------------------------|
| 3.2 全てのシステムは、機密認証データの保管に関する以下の要件に従っていますか？   |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.1 (カードの裏面、チップ内などにある)磁気ストライプからのトラックのいかなる内容も保管しない。このデータはまた、フルトラック、トラック、トラック 1、トラック 2、磁気ストライプデータと呼ばれます。<br><br>通常業務の決済処理では、磁気ストライプからのデータの中で、カード会員の氏名、カード番号(PAN)、有効期限、およびサービスコードが、保管される必要があることがあります。危険性を最小限に抑えるために、業務に必要なデータ要素のみを保管してください。決して、カード認証コードまたは値、または暗証番号認証値のデータ要素を保存しないでください。 |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.2 非対面式決済を認証するために使用されるカード認証コードまたは値（決済カードの表面または裏面に印刷されている 3 桁もしくは 4 桁の数字）を保管しない。  |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.3 暗証番号(PIN)または暗号化された PIN ブロックを保管しない。  |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3 カード番号が表示される際、隠されていますか？ (最初の 6 桁および最後の 4 桁が表示される最大桁数です。)<br><br>注記：この要件は、カード番号全てを見る必要のある特定のニーズを持つ従業員およびその他の当事者には適用されません。また、カード会員データの表示に関して実施されているより厳格な要件（例えば店頭(POS)受領書など）に優先するものではありません。   |     | <input type="checkbox"/> | <input type="checkbox"/> |

要件 4： オープンまたはパブリックネットワークのカード会員データの送信を暗号化する

|  |  |                          |                          |
|--|--|--------------------------|--------------------------|
| 4.2 実施されている方針、手順、業務は、非暗号化カード番号の電子メールでの送信を防ぐものとなっていますか？ |  | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--|--------------------------|--------------------------|

## 厳しいアクセス規制措置の実装

要件 7: 既知の業務のニーズによりカード会員データへのアクセスを制限する

| 質問   | 回答: | はい                       | いいえ                      |
|--|-----|--------------------------|--------------------------|
|  |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1 コンピューティング資源およびカード会員情報へのアクセスは、このアクセスを必要とする職を持つ個人に制限されていますか? |     | <input type="checkbox"/> | <input type="checkbox"/> |

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?<br>(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) カード会員データを含む、あらゆる種類のメディアの社内、または社外分配に関し、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ことを(特にメディアが個人に配布される場合)確実にするプロセスや手順が適所ありますか?   | <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無効にされていますか?<br>無効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>               |
|--------|---|-----|--------------------------|--------------------------|
| 12.1   | セキュリティ方針が作成、発行、管理、普及され、以下が実行されていますか？  |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 12.1.3 | 少なくとも1年に1回は審査され、環境の変化に伴い、更新されていますか？   |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 12.3   | (a) 重要な従業員が向き合う技術（モデムやワイヤレス）に関する使用方針は、すべての従業員および契約者に対して、これらの技術の正しい用を定義するために作成されていますか？ |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 12.4   | セキュリティ方針および手順は、すべての従業員および契約者に対し明確に情報セキュリティの責任を定義していますか？                               |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 12.5   | 以下の情報セキュリティ管理責任は、個人または団体に課せられるものですか？  |     |                          |                          |
| 12.5.3 | セキュリティに関する事故への対応および上申の手順は、すべての状況をタイムリーかつ効率的に取り扱うように作成、記録、分配されていますか？                   |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 12.6   | 実施されている正式なセキュリティ意識向上プログラムは、すべての従業員にカード会員データのセキュリティの重要性を意識させるものとなっていますか？               |     | <input type="checkbox"/> | <input type="checkbox"/> |
| 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、契約上、以下のものは必要となりますか？                                       |     | <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"/> |
| 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"/> |