

PCI

データセキュリティ基準(PCIDSS)

自己査定アンケート **C**

および遵守証明書

インターネットに接続するペイメントアプリケーション(**PA**)。

カード会員データの電子的保管は行いません。

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
遵守証明書、SAQ C	2
自己査定アンケート C	7
安全なネットワークの構築と管理.....	7
要件 1: カード会員データを保護するために、ファイアーウォール設定をインストールし、管理する。	7
要件 2: システムパスワードおよびその他セキュリティパラメータは、ベンダーの初期設定をそのまま使用しない。	7
カード会員データの保護.....	8
要件 3: 保管されたカード会員データを保護する。	8
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。	8
脆弱性管理プログラムの管理.....	10
要件 5: 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使用し、更新する。	10
要件 6: 安全なシステムおよびアプリケーションを開発、管理する。	10
厳しいアクセス規制措置の実装	10
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。	10
コンピュータへのアクセスには、個人それぞれ独自の ID を割り当てる。	10
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。	11
定期的なネットワークの監視およびテスト.....	12
要件 10: ネットワーク資源およびカード会員データへのすべてのアクセスをトラックし監視する。	12
要件 11: セキュリティシステムおよび手順を定期的にテストする。	12
情報セキュリティ方針の管理.....	13
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。	13

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の理解の促進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 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 C はカード会員データをインターネット（高速接続、DSL、ケーブルモデムなど）に接続されたペイメントアプリケーション(PA)（例えば POS システムなど）を通じて処理するが、カード会員データをコンピュータシステムに保管し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。このペイメントアプリケーション(PA)は、以下の理由よりインターネットに接続されます。

1. ペイメントアプリケーション(PA)がインターネットに接続されたパーソナルコンピューター上にある、または
2. このペイメントアプリケーション(PA)がカード会員データを送受信するためにインターネットに接続されている

これらの加盟店は **SAQ 認証タイプ 4** と、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定義されています。認証タイプ 4 の加盟店は、カード会員データをインターネットに接続された POS マシンを通じて処理するが、カード会員データをコンピュータシステムに保管せず、(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/電話での注文を受ける加盟店となります。このような加盟店は、**SAQ C** と関連遵守証明書に記入し、以下の事項を確認し、遵守を証明する必要があります。

- あなたのベンダーは、ペイメントアプリケーション(PA)システムおよびインターネット接続を同じデバイス上に持っています。
- ペイメントアプリケーション(PA)/インターネットデバイスは、あなたの周囲で他のシステムには接続されていません。
- あなたのベンダー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有します。そして
- あなたのベンダーはカード会員データを電子保管していません。
- あなたのベンダーのペイメントアプリケーション(PA)ベンダーは、決済システムにリモートサポートを提供する安全な技術を使用しています。

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)**の要件に基づいて、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 C**) を完了させてください。
2. **PCI SSC** 認定スキャンングベンダー(**ASV**)により完全な脆弱性スキャンを行い、**ASV** より安全であるという診断の証拠を取得してください。
3. 遵守証明書をすべて完了させてください。
4. **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 C

提出方法

加盟店は PCI データセキュリティ基準(PCIDSS)の加盟店の遵守状態の宣言として遵守証明書に記入する必要があります。すべての適用セクションに記入し、本書内の「PCI DSS 遵守 – 記入ステップ」の提出インストラクション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)

ベンダー名 :					
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

ベンダー名 :		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

あなたのベンダーは、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ベンダー、航空券予約代理店、ロイヤルティプログラムベンダーなど)と関係を結んでいますか? はい いいえ

いえ

あなたのベンダーには、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"/>	加盟店はペイメントアプリケーション(PA)システムまたはパブリック・ネットワーク接続を同じデバイス上に持っています。
<input type="checkbox"/>	ペイメントアプリケーション(PA)システム/インターネットデバイスは加盟店の周囲で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存しません。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。そして
<input type="checkbox"/>	加盟店のペイメントアプリケーション(PA)ソフトウェアのベンダーは、加盟店のペイメントアプリケーション(PA)システムへのリモートサポートを提供する安全な技術を採用しています。

パート 3 PCI DSS 認証

(completion date)のSAQ Cに述べられた結果に基づいて、(Merchant Company Name)は以下の遵守状態を表明します。(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、PCI SSC認定スキャンベンダーによる脆弱性スキャンで合格であるという診断を受けており、(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おらず、質問のいくつかに対し「いいえ」と答え、その結果、評価は全面的未遵守となった、またはPCI SSC認定スキャンベンダーによる脆弱性スキャンで合格であるという診断を受けていないため、(Merchant Company Name)のPCI DSSへの完全な遵守が示されていません。
 - 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ものもありますので、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C、バージョン(SAQ version #)は、同書にあるインタラクシオ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)ベンダーに確認しました。
<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 ² 、CAV2、CVC2、CID、またはCVV2データ ³ 、もしくは暗証番号データ ⁴ 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。

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： ↑

加盟店ベンダー代表 ↑

² 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、事業者は磁気ストライプデータ全体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。

³ 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。

⁴ 対面式決済中に、カード所有者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ものもありますので、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	
1	カード会員データを保護するために、ファイアウォール設定をインストールし、管理する。	<input type="checkbox"/>	<input type="checkbox"/>	
2	システムパスワードおよびその他セキュリティパラメータは、ベンダーの初期設定をそのまま使用しない。	<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	
5	ウィルス対策ソフトウェアを使用し、定期的に更新する。	<input type="checkbox"/>	<input type="checkbox"/>	
6	安全なシステムおよびアプリケーションを開発、管理する。	<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"/>	
8	コンピュータへのアクセスには、個人それぞれ独自のIDを割り当てる。	<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"/>	
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	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 C

完了日：

安全なネットワークの構築と管理

要件 1: カード会員データを保護するために、ファイアーウォール設定をインストールし、管理する。

質問	回答：	はい	いいえ
1.3 (a) 公的にアクセス可能なサーバーと、カード会員データを保管するシステムコンポーネントの接続が、ワイヤレスネットワークからの接続も含め、ファイアーウォール設定により制限されていますか？		<input type="checkbox"/>	<input type="checkbox"/>
1.4 (a) 外部ネットワークと（例えばデータベース、ログ、トレースファイルなどの）カード会員データを保管するシステムコンポーネントの直接パブリック・アクセスがファイアーウォール設定により禁止されていますか？		<input type="checkbox"/>	<input type="checkbox"/>

要件 2: システムパスワードおよびその他セキュリティパラメータは、ベンダーの初期設定をそのまま使用しない。

質問	回答：	はい	いいえ
2.1 ベンダーの初期設定は常に、ネットワーク上にシステムをインストールする前に変更されていますか？ 例えば、パスワード、簡易ネットワーク管理プロトコル(SNMP)コミュニティストリング、不必要なアカウントの削除などが挙げられます。		<input type="checkbox"/>	<input type="checkbox"/>
2.1.1 ワイヤレス環境初期設定は、ワイヤレスシステム導入前に変更されていますか？ ワイヤレス環境初期設定には、WEP キー、デフォルト SSID、パスワード、SNMP コミュニティストリングを含みますが、これに限定されるものではありません。		<input type="checkbox"/>	<input type="checkbox"/>
(a) SSID のブロードキャストが無効とされていますか？		<input type="checkbox"/>	<input type="checkbox"/>
(b) 暗号化および認証に、WPA が可能な場合、WiFi 保護アクセス (WPA と WPA2) 技術が有効となっていますか？		<input type="checkbox"/>	<input type="checkbox"/>
2.3 ノンコンソール管理的アクセスはすべて暗号化されていますか？ ウェブベースの管理およびその他ノンコンソール管理的アクセスには、SSH、VPN、SSL/TLS(トランスポートレイヤセキュリティ)などの技術を使用してください。		<input type="checkbox"/>	<input type="checkbox"/>

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	すべてのシステムは、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。 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、口座所有者の氏名、カード番号(PAN)、有効期限、およびサービスコードが、保有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 桁が表示されてよい最大桁数です。) 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。

4.1	オープン、パブリック・ネットワーク上での通信の際、カード会員機密データを保護するために、セキュアソケットレイヤー(SSL)/トランスポート・レイヤ・セキュリティ(TLS)およびインターネット・プロトコル・セキュリティ(IPSEC)などの強力な暗号法およびセキュリティ・プロトコルが使用されていますか？ PCI DSS の範囲にあるオープン、パブリック・ネットワークの例には、インターネット、WiFi (IEEE 802.11x)、グローバル・システム・フォー・モバイルコミュニケーション(GSM)、ジェネラル・パケット・ラジオサービス(GPRS)が挙げられます。	<input type="checkbox"/>	<input type="checkbox"/>
-----	--	--------------------------	--------------------------

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？

脆弱性管理プログラムの管理

要件 5: ウィルス対策ソフトウェアまたはプログラムを定期的を使用し、更新する。

質問	回答:	はい	いいえ
5.1 ウィルス対策ソフトウェアは、ウィルスの影響を共通に受けるシステムすべて（特にパーソナルコンピューターおよびサーバー）で稼動していますか？ 注記：ウィルスの影響を共通に受けるシステムには、UNIXベースのオペレーティングシステムまたはメインフレームは含まれません。		<input type="checkbox"/>	<input type="checkbox"/>
5.1.1 ウィルス対策プログラムは、スパイウェアやアドウェアを含む他の形式の不当ソフトウェアを検知、削除し、システムを保護することが可能ですか？		<input type="checkbox"/>	<input type="checkbox"/>
5.2 すべてのウィルス対策装置は最新のもので、積極的に動作しており、スキャンログを作成することができますか？		<input type="checkbox"/>	<input type="checkbox"/>

要件 6: 安全なシステムおよびアプリケーションを開発、管理する。

6.1 (a) すべてのシステムコンポーネントおよびソフトウェアには、ベンダーが提供する最新のセキュリティパッチがありますか？		<input type="checkbox"/>	<input type="checkbox"/>
(b) 関連セキュリティパッチがリリース1ヶ月以内にインストールされていますか？		<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
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"/>

コンピュータへのアクセスには、個人それぞれ独自の **ID** を割り当てる。

8.5.6 リモート管理でベンダーに使用されるアカウントは、必要な時間だけ有効にされていますか？		<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? (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? 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"/>

定期的なネットワークの監視およびテスト

要件 **10** : ネットワーク資源およびカード会員データへのすべてのアクセスをトラックし監視する。

質問	回答 :	はい	いいえ
SAQ C に適用される質問はありません。			

要件 **11** : セキュリティシステムおよび手順を定期的にテストする。

11.1	(a) セキュリティコントロール、制限、ネットワーク接続、制約は、認証していないアクセスの試みを十分に識別し、防ぐよう、毎年テストされていますか？	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 使用中のワイヤレスデバイスをすべて識別するために、少なくとも年 4 回ワイヤレスアナライザが使用されていますか？	<input type="checkbox"/>	<input type="checkbox"/>
11.2	内部および外部ネットワークの脆弱性スキャンが少なくとも年 4 回、および(新しいシステムコンポーネントのインストール、ネットワーク・トポロジーの変更、ファイアウォール規則の変更、製品アップデートなどの) ネットワークへの重要な変更が行われた後、実行されていますか？ 注記 : PCI 認定のスキャンベンダーによる外部脆弱性スキャンを、年 4 回実行する必要があります。 ネットワーク変更後に行われるスキャンは、ベンダー内部のスタッフにより実行されることがあります。	<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：	はい	いいえ
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、更新されること。		<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お定義していますか？		<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"/>