

# PCIデータセキュリティ基準(PCIDSS)

## 自己診断票

---

### インストラクションとガイドライン

バージョン**1.1**

2008年2月

## 目次

---

目次 .....	i
本書について .....	1
PCI データセキュリティ基準(PCIDSS)自己診断：文書の関連性 .....	2
PCI データセキュリティ基準(PCIDSS)：関連文書 .....	3
自己診断票（SAQ）概要 .....	4
PCI DSS の遵守がなぜ重要なのですか？ .....	5
遵守認証の準備の一般的な注意と戦略 .....	7
あなたの会社に最もよく適する自己診断票（SAQ）および診断の選択 .....	11
自己診断票（SAQ）認証タイプ 1/自己診断票（SAQ） A：カード実物を介さず、すべてのカード会員データ機能が外部委託されている .....	11
自己診断票（SAQ）認証タイプ 2/自己診断票（SAQ） B：カード会員データを電子保管しないインプリントの加盟店のみ。 .....	13
自己診断票（SAQ）認証タイプ 3/自己診断票（SAQ） B：カード会員データを電子保管しないスタンドアロン型ダイアルアウト端末加盟店。 .....	13
自己診断票（SAQ）認証タイプ 4/自己診断票（SAQ） C：インターネットに接続されたペイメントアプリケーション(PA)システムの加盟店 .....	14
自己診断票（SAQ）認証タイプ 5/自己診断票（SAQ） D：自己診断票（SAQ）を記入する必要があるとカードブランドに定義されるその他すべての加盟店およびサービスプロバイダー ...	15
自己診断票（SAQ）の記入インストラクション .....	17
自己診断票（SAQ）インストラクションおよびガイドライン  自社の認証タイプはどれ？ .....	18

---

## 本書について

---

本書は、加盟店およびサービスプロバイダーの PCI データセキュリティ基準(PCIDSS)の理解を促進するために作成されました。このインストラクションおよびガイドラインをご覧ください、PCI DSS があなたの会社にとってなぜ重要となるのか、遵守認証を促進するためにどのような戦略を使用できるか、短縮版自己診断票 (SAQ) を記入する必要があるか理解してください。次のセクションは、PCI DSS 自己診断票 (SAQ) について知る必要がある事柄の概要です。

- PCI データセキュリティ基準(PCIDSS)自己診断：文書の関連性
- PCI データセキュリティ基準(PCIDSS)：関連文書
- 自己診断票 (SAQ) 概要
- PCI DSS の遵守がなぜ重要なのですか？
- 一般的な注意と戦略
- あなたの会社に最もよく適する自己診断票 (SAQ) および診断の選択
- 特定要件の除外ガイダンス
- 診断票記入方法

## PCI データセキュリティ基準(PCIDSS)自己診断：文書の関連性

PCI データセキュリティ基準(PCIDSS)および補足文書は、機密情報の安全な扱いの徹底を促進するための産業のツールおよび基準です。この基準では、セキュリティ関連の事故の防止、検知、対応を含む、強固なカードデータセキュリティプロセスを開発する実用的な方法を提供します。セキュリティ侵害の危険性を削減するため、また侵害が発生した場合その影響を軽減するためには、カード会員データの保管、処理、送受信を行う全ての企業が遵守することが重要となります。下のチャートは、PCIDSS 遵守および自己診断を促進するための実施されているツールの概要です。

これらの、またその他の関連文書は [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) でご覧いただけます。

	PCI データセキュリティ基準(PCIDSS)	
PCI DSS 自己診断	PCI DSS 関連文書	PCI DSS セキュリティ診断手順
自己診断票 A から D	PCI DSS ナビゲート：基準要件の目的理解	
遵守証明書	PCI DSS 用語集、略語、および頭文字語	

## 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 自己診断票 (S A Q) 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): 自己診断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): 自己診断票 A(PCI DSS 自己診断票 (S A Q) A)と証明書	加盟店 <sup>1</sup>
PCI データセキュリティ基準(PCIDSS): 自己診断票 B と証明書	加盟店 <sup>1</sup>
PCI データセキュリティ基準(PCIDSS): 自己診断票 C と証明書	加盟店 <sup>1</sup>
PCI データセキュリティ基準(PCIDSS): 自己診断票 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 データセキュリティ基準(PCIDSS)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> 適切な自己診断票を決定するには、PCI データセキュリティ基準：自己診断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自己診断票 (S A Q) および証明書の選び方」を参照してください。

## 自己診断票（SAQ）概要

---

PCI データセキュリティ基準(PCIDSS)自己診断票は、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)の遵守の自己診断を支援する認証ツールです。あなたのシナリオに応じた、多くのバージョンの PCI DSS 自己診断票（SAQ）があります。本文書は、会社がどの自己診断票（SAQ）が最も適しているか決定する手助けをするものです。

PCI DSS 自己診断票（SAQ）は、PCI DSS セキュリティ診断手順を通じて、オンサイトレビューを実行することを求められていない加盟店とサービスプロバイダーのための認証ツールであり、アクワイアラまたはカードブランドにより必要とされることがあります。PCI DSS 認証の要件についての詳細は、アクワイアラまたはカードブランドにお尋ねください。

PCI DSS 自己診断票（SAQ）は以下の要素からなるものです。

1. サービスプロバイダーおよび加盟店に適切な PCI DSS 要件と相互関連のある質問。本書の「あなたの会社に最もよく適する自己診断票（SAQ）および診断の選択」をご覧ください。
2. 遵守証明：適切な自己診断を実行する必要がある、および実行したという証明。

## PCI DSS の遵守がなぜ重要なのですか？

---

PCI セキュリティスタンダードカウンシル(PCISSC)のメンバー(アメリカンエクスプレス、ディスカバー、JCB インターナショナル、マスターカード、ビザ・インク)は、カードデータのセキュリティ侵害を継続的に監視します。これらのセキュリティ侵害は、小規模から大規模まで、あらゆる加盟店およびサービスプロバイダー会社が対象とされます。

セキュリティ違反およびそれに続くクレジットカードデータのセキュリティ侵害は、会社以下のような広範囲にわたる影響を与えます。

1. 規制による申告の要求
2. 信頼の損失
3. 顧客の損失
4. 潜在的な経済的負担 (例えば、規制およびその他手数料と罰金)
5. 起訴

セキュリティ侵害事後調査では、PCI DSS により発表されていたよくあるセキュリティ上の弱点が、セキュリティ侵害が発生した際に会社内で存在していたことがわかりました。PCI DSS は、セキュリティ侵害の発生と、発生した場合の影響を最小限に抑えるために、詳細にわたる要件を含めています。

セキュリティ侵害後の調査では、一貫して以下のような PCI DSS 違反がよく発見されます。

磁気ストライプデータの保管(要件 3.2)について、セキュリティ侵害を受けた企業が使用しているシステムがこのデータを保管していることに気づいていなかったこと。

加盟店の POS システムが正しくインストールされていない不十分なアクセス管理が、ハッカーによる POS ベンダーをターゲットとした攻撃を受ける。(要件 7.1、7.2、8.2、8.3)

システム設定時にデフォルトシステム設定およびパスワードが変更されていない。(要件 2.1)

システム設定時に不必要な脆弱なサービスが是正されていない。(要件 2.2.2)

ウェブサイトから、カード会員データを保管するデータベースへ直接アクセスすることを許可する SQL インジェクションおよびその他脆弱性をもたらすウェブアプリケーション。(要件 6.5)

セキュリティパッチの欠陥および期限切れ。(要件 6.1)

ロギングの欠如。(要件 10)

(ログの点検、侵入検知/防止、3 ヶ月ごとの脆弱性スキャン、ファイル完全性監視システムによる)監視の欠如。(要件 10.6、11.2、11.4、11.5)

ネットワークがセグメンテーションされていないことで、ネットワーク内の他のエリアの脆弱性により(例えば、ワイヤレスアクセスポイント、従業員の電子メール、ウェブブラウザからの)カード会員データへのアクセスが容易に行われる。(要件 1.3 および 1.4)

## 遵守認証の準備の一般的な注意と戦略

---

PCI DSS 遵守認証を開始するための一般的な注意と戦略は以下のとおりです。これらの注意は、あなたが必要としないデータを削除し、定義済みの集中管理エリアに必要なデータを隔離する手助けをし、PCI DSS 遵守認証の努力の範囲を制限することができます。例えば、必要のないデータを削除し、そして/またはそのデータを定義済管理エリアに隔離することで、自己診断の範囲からカード会員データを保管、処理、送受信しないこれらのシステムとネットワークを削除することができます。

1. 機密認証データ(磁気ストライプ、カード認証コードおよび値、PIN(暗証番号)ブロック)
  - a. 決してこれらのデータを保管しないこと。
  - b. お使いのソフトウェア製品とバージョンがこれらのデータを保管するかどうかわからない場合、POS ベンダーにお問い合わせください。あるいは、機密認証がシステムのいずれかの場所に保管、ログ、キャプチャーされているかどうか決定できる認定セキュリティ担当者を雇用することをお考えください。
2. 加盟店の方は POS ベンダーに、システムのセキュリティについてお問い合わせください。その際、以下の事柄を尋ねることが推奨されます。
  - a. POS ソフトウェアは磁気ストライプデータ(トラックデータ)または PIN(暗証番号)ブロックを保管していますか？ これを保管することは禁止されています。ただちに削除するためにはどうすればいいですか？
  - b. 上述の禁止されたデータが保管されていないことを確認するために、アプリケーションにより作成されたファイルのリストを、各ファイルの内容の概要とともに、文書化していますか？
  - c. 認証されていないアクセスからシステムを保護するために、POS システムにファイアウォールがインストールされていますか？
  - d. システムのアクセスには、複雑で独自のパスワードが必要とされていますか？ 自社に対する共通またはデフォルトのパスワードが、サポートしている他の加盟店システムと同じものを使用していないことを確認できますか？
  - e. POS システムの一部となるシステムおよびデータベースのデフォルト設定およびパスワードは、変更されていますか？
  - f. POS システムの一部となる、不必要および安全でないサービスはすべてシステムおよび

データベースより削除されていますか？

g. 自社の POS システムにリモートアクセスを行っていますか？ この場合、自社の POS システムに他者がアクセスするのを防止するために、安全なリモートアクセス方法を使用する、共通またはデフォルトのパスワードを使用しないなどの適切な管理を実行していますか？ どの程度頻繁に POS デバイスにリモートアクセスしていますか？またどうしてですか？ 自社の POS にリモートアクセスする権限を与えられている人は誰ですか？

h. POS システムの一部であるシステムおよびデータベースはすべて、適切なセキュリティ上のアップデートが行われていますか？

i. ロギング性能は、POS システムの一部であるシステムおよびデータベースに調整されていますか？

j. 自社の POS ソフトウェアの以前のバージョンがトラックデータを保管していた場合、POS ソフトウェアの最新のアップデート中にこの機能は削除されていますか？ セキュア・ワイプ・ユーティリティが、このデータを削除するために使用されていましたか？

3. カード会員データー必要ないものは保管しないこと!
  - a. カードブランドの規則がカード番号(PAN)、有効期限、カード会員名とサービスコードの保管を許可している。
  - b. このデータを保管する理由と場所をすべて一覧すること。このデータが重要な業務上の目的のためでない場合、削除することを検討してください。
  - c. このデータの保管とサポートする業務プロセスが以下の価値があるかどうか検討してください。
    - i. データセキュリティ侵害のリスク。
    - ii. データを保護するために適用する必要がある追加の PCI DSS への対策。
    - iii. PCI DSS への遵守を徹底するための長期にわたる継続的な管理対策。
4. カード会員データー必要がないものは、整理し、隔離してください。
  - a. データ保管を定義環境に整理し、正しいネットワークセグメントの使用を通して、データを隔離することで、PCI DSS 診断の範囲を制限することができます。例えば、あなたの従業員がカード会員データと同じ機器またはネットワークのセグメント内でインターネットをブラウザし、電子メールを受信している場合、カード会員データを独自の機器またはネットワークのセグメントに(ルーターまたはファイアウォールで)セグメント化(隔離)することを検討してください。カード会員データを効率的に隔離することができる場合、PCI DSS への対策を機器すべてではなく、隔離された部分に焦点をあてて行うことができます。
5. 代替コントロール方法の検討(自己診断票(SAQ) Dのみに適用)
  - a. PCI DSS 要件の技術仕様を満たすことができないが、関連リスクを十分に軽減した場合、多くの要件には代替コントロール方法を検討することができます。あなたの会社が PCI DSS に規定されている正確な管理をもっていないが、PCI DSS の代替コントロール方法の定義を満たす他の管理手段が実施されている場合([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)にある自己診断票(SAQ) Dの付属書および PCI DSS 用語集、略語、および頭文字語の文書をご覧ください)、あなたの会社は以下の事柄を行う必要があります。
    - i. 自己診断票(SAQ)の代替コントロールのカラムに、要件を満たすために使用する各代替コントロール手段を記入してください。
    - ii. 付属書の「代替コントロール手段」を再読し、代替コントロールワークシートを記入して代替コントロールの使用を文書化してください。
  - a) 各要件の代替コントロールに対し、代替コントロールワークシートを記入してください。

iii. アクワイアラまたはカードブランドからのインストラクションに従い、記入済みの代替コントロールワークシートと、記入済みの自己診断票（SAQ）および／または診断を一緒に提出してください。

6. 専門家による支援

a. 自己診断票（SAQ）の遵守と記入にあたり、セキュリティ専門家のガイダンスを求めることが奨励されます。セキュリティ専門家の選択は自由ですが、PCI SSC の認定セキュリティ診断者(QSAs)のリストに含まれている専門家は PCI SSC による研修を受けている QSA と認定されていることにご注意ください。このリストは、[https://www.pcisecuritystandards.org/resources/qualified\\_security\\_assessors.htm](https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm) から入手できます。

## あなたの会社に最もよく適する自己診断票（SAQ）および診断の選択

カードブランドの規則に従って、すべての加盟店およびサービスプロバイダーが PCI データセキュリティ基準(PCIDSS)を完全に遵守することを求められています。 自己診断票（SAQ）認証カテゴリーは 5 つあり、これらは下の表で簡潔に示されており、以下の段落で詳しく説明されています。 どの自己診断票（SAQ）があなたの会社に適用されるか正しく判断を行うために、以下の表をご利用ください。 また、詳しい説明を読み、その自己診断票（SAQ）の要件をすべて満たすかどうか確認してください。

自己診断票（SAQ）認証タイプ	説明	自己診断票（SAQ）
1	非対面式(電子商取引かメール／電話による注文の)加盟店で、すべてのカード会員データ機能が外部に委託されている。 これは対面式の加盟店に適用されることはありません。	A
2	カード会員データの電子的保管のない、インプリントのみの加盟店。	B
3	カード会員データの電子的保管のない、スタンドアロン型端末の加盟店。	B
4	カード会員データの電子的保管のない、POS システムがインターネットに接続されていない加盟店。	C
5	(以上の自己診断票（SAQ） A-C への説明に含まれていない) すべての他の加盟店、およびカードブランドに自己診断票（SAQ）を完了する必要がある定義されるすべてのサービスプロバイダー	D

自己診断票（SAQ）認証タイプ 1 / 自己診断票（SAQ） A : カード実物を介さず、すべてのカード会員データ機能が外部委託されている

自己診断票（SAQ） A は、業務上、カード会員データのカード利用控か領収書だけを保有し、電子形式でカード会員データを保存、処理、送信しない加盟店に適切な要件を扱うために開発さ	認証タイプの選択の図式ガイドには、12 ページの「自己診断票（SAQ） インストラクシ
--	---

<p>れました。</p>	<p>ョンおよびガイドライン 自社の認証タイプはどれ？」をご覧ください。</p>
<p>認証タイプ 1 の加盟店はカード会員データを電子形式で保管せず、カード会員データを施設内で処理または送受信せず、自己診断票（SAQ） A と関連遵守証明を記入し遵守を有効とし、以下を確認する必要があります。</p>	

- あなたの会社は非対面式カード(電子商取引かメール/電話による注文)取引のみを扱います。
- あなたの会社は、その業務でカード会員データを保存、処理、送信しませんが、これらの機能の扱いに第三者サービスプロバイダーに頼っています。
- 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もしくは領収書のみを保有し、これらのドキュメント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のカード会員データを保存していません。

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。

自己診断票（SAQ）認証タイプ 2 / 自己診断票（SAQ） B：カード会員データを電子保管しないインプリントの加盟店のみ。

<p>自己診断票（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。</p>	<p>認証タイプの選択の図式ガイドには、12 ページの「自己診断票（SAQ） インストラクションおよびガイドライン 自社の認証タイプはどれ？」をご覧ください。</p>
<p>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でのみ処理し、自己診断票（SAQ） B と関連遵守証明を記入することで遵守を有効とし、以下を確認する必要があります。</p>	

- あなたの会社は顧客のクレジットカード情報の取得に、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信しません。
- あなたの会社はレシートのカード利用控のみを保管します。
- あなたの会社は電子形式でカード会員データを保管しません。

自己診断票（SAQ）認証タイプ 3 / 自己診断票（SAQ） B：カード会員データを電子保管しないスタンドアロン型ダイアルアウト端末加盟店。

自己診断票（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。

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、(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。 認証タイプ 3 の加盟店は、自己診断票（SAQ） B と関連遵守証明書に記入し、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 端末はあなたの周囲で他のシステムに接続されていません。
- スタンドアロン型 CAT 端末は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有します。そして
- あなたの会社は電子形式でカード会員データを保管しません。

自己診断票（SAQ）認証タイプ 4 / 自己診断票（SAQ） C : インターネットに接続されたペイメントアプリケーション(PA)システムの加盟店

自己診断票（SAQ） C は、そのペイメントアプリケーション(PA)システム (例えば、POS またはショッピングカートシステム)が以下のいずれかの理由により(高速接続、DSL、ケーブルモデムなどの)インターネットに接続されている、加盟店に適用される要件を示すために作成されました。

1. ペイメントアプリケーション(PA)システムが(例えば、電子メールまたはウェブブラウザなどのために)インターネットに接続する、パソコン上にある。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。

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。 認証タイプ 4 の加盟店は、自己診断票（SAQ） C と関連遵守証明書に記入し、以下の事項を確認し、遵守を立証する必要があります。

<ul style="list-style-type: none"> <li>● あなたの会社は、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。</li> <li>● 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。</li> <li>● 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有します。そして</li> <li>● あなたの会社はカード会員データを電子形式で保管しません。</li> <li>● あなたの会社のペイメントアプリケーション(PA)会社は、ペイメントシステムにリモートサポートを提供する安全</li> </ul>	<p>認証タイプの選択の図式ガイドには、12 ページの「自己診断票（SAQ）インストラクションおよびガイドライン 自社の認証タイプはどれ？」をご覧ください。</p>
---	--

な技術を使用しています。	
--------------	--

自己診断票（SAQ）認証タイプ 5 / 自己診断票（SAQ） D : 自己診断票（SAQ）を記入する必要があるとカードブランドに定義されるその他すべての加盟店およびサービスプロバイダー

自己診断票（SAQ） D は、カードブランドにより自己診断票（SAQ）を記入する必要があると定義されるすべてのサービスプロバイダーと、上記の認証タイプ 1-4 に当てはまらない加盟店に適用する要件を示すために、作成されています。

認証タイプ 5 の加盟店は、自己診断票（SAQ） D と関連遵守証明書に記入し、以下の事項を確認し、遵守を立証する必要があります。

自己診断票（SAQ） D を完了する会社の多くは各 PCI DSS 要件の遵守を立証する必要がありますが、特定のビジネスモデルの会社には適用されない要件もあります。例えば、潜在的にワイヤレステクノロジーを使用しない会社は、ワイヤレステクノロジーに特有の PCI DSS のセクションの遵守を立証することを求められません。ワイヤレステクノロジーおよび他の特定の要件の除外についての情報は、以下のガイダンスをご覧ください。

#### 特定要件除外のガイダンス

PCI DSS の遵守を有効とするために自己診断票（SAQ） D への回答を求められている場合、以下の例外が検討されることがあります。(これらの要件があなたの環境に適用されない場合、N/A と記すこともできます。)

- ワイヤレスに特有の質問は、あなたのネットワークのどこかにワイヤレスが存在する場合にのみ回答される必要があるものです(要件 1.3.8、2.1.1、4.1.1)。あなたのネットワークにワイヤレスが存在しない場合でも、アナライザが加盟店の知らないところで追加された不正または非認定デバイスを検出するため、要件 11.1(ワイヤレスアナライザの使用)は回答する必要があることにご注意ください。
- カスタムアプリケーションおよびコード(要件 6.3-6.5)は、あなたの会社が独自のカスタムウェブアプリケーションを作成している場合のみ回答する必要があります。

- データセンターに特有の質問(要件 9.1-9.4)は、専用データセンターまたはサーバールームが存在する場合のみ回答する必要があります。 専用のデータセンターとは、PCI SSC によると、IT 基盤(アプリケーションサーバー、データベースサーバー、ウェブサーバー、および/またはネットワークデバイス)を中心に収容し、その主な目的がカード会員データの保管、プロセス、送信である、物理的に安全な部屋または構造であると定義されています。「データセンター」は、サーバールーム、ネットワークオペレーションセンター(NOC)、ISP またはホスティングプロバイダーのコロケーション施設と同意語であることがあります。

## 自己診断票（SAQ）の記入インストラクション

---

1. ここにあるガイドラインを使用し、あなたの会社に適切な自己診断票（SAQ）はどれか決定してください。
2. PCI DSS ナビゲート：基準要件の目的理解を使用して、要件があなたの会社にどのように、またなぜ相当するのか理解してください。
3. PCI DSS との遵守を有効とするツールとして、適切な自己診断票を使用してください。
4. PCI DSS 遵守完了ステップの適切な自己診断票内のインストラクションに従ってください。また、必要な書類をあなたのアクワイアラまたはカードブランドに適宜、提出してください。

## 自己診断票（SAQ） インストラクションおよびガイドライン 自社の認証タイプはどれ？

認証タイプ 1 :	認証タイプ 2 :	認証タイプ 3 :	認証タイプ 4 :	認証タイプ 5 :
CNP、すべてのカード会員データ (CHD) 機能は外部に委託されている。	インプリントのみ。 電子形式での CHD 保管はしない。	スタンドアロン型 CAT 端末のみ。 電子形式での CHD 保管はしない。	インターネットに接続された POS またはペイメントシステム。 電子形式での CHD 保管はしない。	カードブランドにより自己診断票（SAQ）の必要があると定義されるすべての他の加盟店およびすべてのサービスプロバイダー。
CNP のみ 施設内に CHD はなく、すべて外部に委託されている。 第 3 当事者は PCI DSS	インプリンタのみ。 電話またはインターネットを通じた CHD なし。 紙のみが保管されている。 CHD を電子形式で保管は	スタンドアロン型 CAT 端末のみ。 端末は他のいずれかのシステムに接続されていない。 端末はインターネットに接続	POS またはペイメントシステムとインターネットが同じデバイス上にある。 端末は他のいずれかのシステムに接続されて	

<p>に遵守している。</p> <p>紙のみが保管されている。</p> <p><b>CHD</b> を電子形式で保管はしない。</p>	<p>しない。</p>	<p>されていない。</p> <p>紙のみが保管されている。</p> <p><b>CHD</b> を電子形式で保管はしない。</p>	<p>いない。</p> <p>紙のみが保管されている。</p> <p><b>CHD</b> を電子形式で保管はしない。</p> <p><b>POS</b> ベンダーは安全面でのサポートを提供している。</p>	
<p>これが本当に自社の加盟店タイプですか？</p>	<p>これが本当に自社の加盟店タイプですか？</p>	<p>これが本当に自社の加盟店タイプですか？</p>	<p>これが本当に自社の加盟店タイプですか？</p>	
<p>自己診断票 (SAQ) A および証明 (質問 11 個)</p>	<p>自己診断票 (SAQ) B および証明 (質問 21 個)</p>	<p>自己診断票 (SAQ) B および証明 (質問 21 個)</p>	<p>自己診断票 (SAQ) B および証明 (質問 38 個)</p>	<p>自己診断票 (SAQ) B および証明 (質問 226 個)</p>
		<p>PCI DSS のナビゲート</p>		