



PCI (Payment Card Industry)

データセキュリティ基準

自己問診(Self-Assessment Questionnaire) B および準拠証明書

インタプリタまたはスタンドアロン型ダイアルアップ端末のみを使用する加盟店（カード会員データを電子形式で保存しない）

PCI DSS バージョン 3.2 用

改訂1.1版

2017年1月

この文書について

この文書（「公式日本語訳」）は、https://www.pcisecuritystandards.org/document_library , © 2006-2017 PCI Security Standards Council, LLC（「審議会」）で入手可能な SAQ と記される文書の公式の日本語訳です。この公式日本語訳は、JCDSC（「団体」）の承認と支援により情報提供のみを目的として、審議会と団体間の契約に基づいて提供されるものです。この翻訳に関して、本文書に記述された仕様を実装する権利は認められません。そのような権利は、https://www.pcisecuritystandards.org/document_library で入手可能な使用許諾契約書の条項に同意することによってのみ確保されます。本文書の英語版は、https://www.pcisecuritystandards.org/document_library で入手できるもので、本文書の完全版であるとみなされます。不明な点および日本語訳と英語版における不一致については英語版が優先され、日本語訳はいかなる目的であっても依拠することはできません。審議会も団体も、本文書に含まれるいかなる誤りや不明瞭さにも責任を負いません。

About this document

This document (the "Official Japanese Translation") is the official Japanese language translation of the document described as SAQ, available at https://www.pcisecuritystandards.org/document_library , © 2006-2017 PCI Security Standards Council, LLC (the "Council"). This Official Japanese Translation is provided with the approval and support of JCDSC ("the Company"), as an informational service only, under agreement between the Council and the Company. No rights to implement the specification(s) described in this document are granted in connection with this translation; such rights may only be secured by agreeing to the terms of the license agreement available at https://www.pcisecuritystandards.org/document_library . The English text version of this document is available at https://www.pcisecuritystandards.org/document_library and shall for all purposes be regarded as the definitive version of this document. To the extent of any ambiguities or inconsistencies between this version and such English text version of this document, the English text version shall control, and accordingly, this version shall not be relied upon for any purpose whatsoever. Neither the Council nor the Company assume any responsibility for any errors or ambiguities contained herein.

文書の変更

日付	PCI DSS バージョン	SAQ 版	説明
2008 年 10 月	1.2		内容を新しい PCI DSS v1.2 にあわせて改訂、および元の v1.1 以降に加えられた若干の変更を追加。
2010 年 10 月	2.0		内容を新しい PCI DSS v2.0 要件とテスト手順にあわせて改訂。
2014 年 2 月	3.0		内容を新しい PCI DSS v3.0 要件とテスト手順にあわせて改訂。
2015 年 4 月	3.1		PCI DSS v3.1 にあわせて更新。詳細については、『PCI DSS – PCI DSS バージョン 3.0 から 3.1 への変更点のまとめ』を参照してください。
2015 年 7 月	3.1	1.1	2015 年 6 月 30 日までの「ベストプラクティス」に対する参考情報を削除するために更新。
2016 年 4 月	3.2	1.0	PCI DSS v3.2 にあわせて更新。詳細については、『PCI DSS – PCI DSS バージョン 3.1 から 3.2 への変更点のまとめ』を参照してください。
2017 年 1 月	3.2	1.1	他の SAQ に合わせてバージョンナンバーを改訂。

目次

文書の変更	i
開始する前に	iii
PCI DSS 自己評価の記入方法.....	iii
自己問診 (SAQ) について.....	iv
必要なテスト	iv
自己問診の記入方法	v
特定の要件が適用されない場合	v
法的例外	v
セクション 1: 評価の情報.....	1
セクション 2: 自己問診 B.....	4
カード会員データの保護.....	4
要件 3: 保存されるカード会員データの保護	4
要件 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	6
強力なアクセス制御手法の導入	7
要件 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	7
要件 9: カード会員データへの物理アクセスを制限する	8
情報セキュリティポリシーの維持	12
要件 12: すべての担当者の情報セキュリティに対応するポリシーを維持する	12
付録 A: 追加の PCI DSS 要件.....	15
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	15
付録 A2: SSL / 初期の TLS を使用している事業者向けの PCI DSS 追加要件.....	15
付録 A3: 指定事業者向け追加検証 (DESV).....	15
付録 B: 代替コントロールワークシート	16
付録 C: 適用されない理由についての説明.....	17
セクション 3: 検証と証明の詳細	18

開始する前に

SAQ B は、インプリンタまたはスタンドアロン型ダイアルアップ端末のみによって、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。SAQ B の加盟店は、従来型（カードを提示する）加盟店、または通信販売（カードを提示しない）加盟店のいずれかで、カード会員データをコンピュータシステムに保存しません。

SAQ B の加盟店は、この支払チャネルに関して以下を確認します。

- あなたの会社は、インプリンタのみを使用するか、スタンドアロン型ダイアルアップ端末（電話回線によって処理装置に接続）のみを使用して（あるいはその両方）、顧客のペイメントカード情報を取り込みます。
- スタンドアロン型ダイアルアップ端末は環境内のその他のシステムに接続されていません。
- スタンドアロン型ダイアルアップ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、カード会員データをネットワーク（内部ネットワークまたはインターネット）を経由して伝送しません。
- あなたの会社にあるカード会員データの全ては紙（例えば計算書または領収書）でのみ保管され、これらの書類を電子的に受信することはありません。
- これらの書類を電子的に受信することはありません。また
- あなたの会社は、カード会員データを電子形式で保存しません。

この SAQ は電子商取引チャネルには適用されません。

この短いバージョンの SAQ には、前述の適用基準で定義されているように、特定のタイプの小規模加盟店の環境に適用される質問が含まれています。あなたの環境に適用される PCI DSS 要件があり、この SAQ で扱われていない場合、この SAQ はあなたの環境に適していないということです。また、PCI DSS 準拠のため、適用できる PCI DSS 要件すべてに準拠する必要があります。

PCI DSS 自己評価の記入方法

1. あなたの環境に適用される SAQ を見つけます - PCI SSC ウェブサイトにある『PCI DSS: 自己問診のガイドラインと手引き』をご覧ください。
2. あなたの環境が適切に範囲設定され、(パート 2g の準拠証明書の定義どおりに)使用する SAQ の適用基準を満たしていることを確認します。
3. 適用される PCI DSS 要件への準拠状況について、あなたの環境を評価します。
4. この文書のすべてのセクションを完成させます。
 - セクション 1 (AOC パート 1 & 2) - 評価の説明と概要
 - セクション 2 - PCI DSS 自己問診 (SAQ B)
 - セクション 3 (AOC パート 3 & 4) - 検証と準拠証明の詳細および非準拠要件に対するアクションプラン（該当する場合）
5. SAQ および準拠証明書(AOC)を ASV スキャンレポート等、他の必須文書とともに、アクワイアラ一、ペイメントブランドまたは他の要求者に提出します。

自己問診 (SAQ) について

この自己問診の「PCI DSS 質問」欄にある質問は、PCI DSS の要件に基づくものです。

PCI DSS 要件と自己問診の記入方法に関するガイダンスを提供するその他のリソースが評価プロセスを支援するために用意されています。これらのリソースの概要を以下に示します。

文書	説明
PCI DSS <i>(PCI データセキュリティ基準の要件とセキュリティ評価手順)</i>	<ul style="list-style-type: none"> • 範囲設定のガイダンス • すべての PCI DSS の趣旨に関するガイダンス • テスト手順の詳細 • 代替コントロールに関するガイダンス
SAQ 説明およびガイドライン文書	<ul style="list-style-type: none"> • すべての SAQ とその適格性基準についての情報 • どの SAQ があなたの組織に適しているかを判断する方法
<i>PCI DSS と PA-DSS の用語集 (用語、略語、および頭字語)</i>	<ul style="list-style-type: none"> • PCI DSS と自己問診で使用されている用語の説明と定義

これらのリソースおよび他のリソースは PCI SSC ウェブサイト (www.pcisecuritystandards.org) でご覧いただけます。評価を開始する前に PCI DSS および付属文書を読むことを推奨します。

必要なテスト

「必要なテスト」欄では、PCI DSS に記載されているテスト手順に基づくもので、要件が満たされていることを確認するために実施すべきテストの種類に関する概要を説明しています。各要件のテスト手順の詳細説明は PCI DSS に記載されています。

自己問診の記入方法

各質問に対し、その要件に関するあなたの会社の準拠状態を示す回答の選択肢が与えられています。各質問に対して回答を一つだけ選択してください。

各回答の意味を次の表に説明します。

回答	説明
はい	必要なテストが実施され、要件の全要素が記載されている通り満たされました。
はい、CCW 付 (代替コントロール ワークシート)	必要なテストが実施され、代替コントロールの助けを借りて要件が満たされました。 この欄の回答にはすべて、SAQ の付録 B の代替コントロールワークシート (CCW) への記入が必要です。 代替コントロールの使用に関する情報とワークシートの記入方法についてのガイダンスは、PCI DSS に記載されています。
いいえ	要件の要素の全部または一部が満たされていないか、導入中、あるいは確立したかを知るためにさらにテストが必要です。
N/A (該当なし)	この要件は会社の環境に該当しません (「特定の要件が適用されない場合」を参照)。 この欄に回答した場合はすべて、SAQ 付録 C の説明が必要です。

特定の要件が適用されない場合

要件があなたの会社の環境に該当しない場合、その要件に対して「N/A」オプションを選択し、「N/A」を選択した各項目について付録の「適用されない理由についての説明」ワークシートに説明を入力します。

法的例外

あなたの会社が法的制限を受けており、PCI DSS の要件を満たすことができない場合は、その要件の「いいえ」の欄にチェックマークを付け、該当する証明書をパート 3 に記入してください。

セクション 1: 評価情報

提出に関する指示

この文書は、PCI データセキュリティ基準 (PCI DSS) の要件およびセキュリティ評価手順による加盟店の評価結果を表明するものとして完成されねばなりません。この文書のすべてのセクションの記入が必要です。加盟店は、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、アクワイアラー (加盟店銀行) またはペイメントブランドにお問い合わせください。

パート 1. 加盟店と認定セキュリティ評価機関の情報

パート 1a. 加盟店の組織情報

会社名:		DBA (商号):			
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 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. 加盟店のビジネスの種類 (該当するものすべてにチェック)

- | | | |
|--|--------------------------------|---|
| <input type="checkbox"/> 小売 | <input type="checkbox"/> 電気通信 | <input type="checkbox"/> 食料雑貨およびスーパーマーケット |
| <input type="checkbox"/> 石油 | <input type="checkbox"/> 電子商取引 | <input type="checkbox"/> 通信販売 |
| <input type="checkbox"/> その他 (具体的に記入してください): | | |

あなたの会社はどのような種類の支払チャネルを提供していますか？

- | |
|---------------------------------------|
| <input type="checkbox"/> 通信販売 (MO/TO) |
| <input type="checkbox"/> 電子商取引 |
| <input type="checkbox"/> カード提示 (対面式) |

この SAQ でカバーされている支払チャネルはどれですか？

- | |
|---------------------------------------|
| <input type="checkbox"/> 通信販売 (MO/TO) |
| <input type="checkbox"/> 電子商取引 |
| <input type="checkbox"/> カード提示 (対面式) |

注: あなたの会社の支払チャネルまたは処理がこの SAQ でカバーされていないものがある場合は、それら他のチャネルの検証についてアクワイアラーまたはペイメントブランドに相談してください。

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、またどのような理由で保存、処理、伝送していますか？

パート 2c. 場所

PCI DSS レビューに含まれている施設の種類（例えば、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	該当する施設の数	施設の拠点 (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

対象組織は一つまたは複数のペイメントアプリケーションを使用していますか？ はい いいえ

対象組織が使用するペイメントアプリケーションについて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 登録済みですか	PA-DSS 登録の有効期限 (該当する場合)
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	
			<input type="checkbox"/> はい <input type="checkbox"/> いいえ	
			<input type="checkbox"/> はい <input type="checkbox"/> 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ください。

例:

- カード会員データ環境(CDE)との接続
- POS デバイス、データベース、Web サーバーなど、CDE 内の重要なシステムコンポーネント、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

はい
 いいえ

ーション」セクションを参照してください。)

パート 2f. サードパーティサービスプロバイダ

あなたの会社は認定インテグレータとリセラー (QIR) を使用していますか？ 使用している場合： QIR 会社の名前： QIR 個人名： QIR から提供されたサービスの説明：	<input type="checkbox"/> はい <input type="checkbox"/> いいえ
あなたの会社は、1 つ以上のサードパーティサービスプロバイダとカード会員データを共有していますか（例えば、認定インテグレータとリセラー (QIR)、ゲートウェイ、ペイメントプロセッサ、ペイメントサービスプロバイダ (PSP)、Web 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代理店など）？	<input type="checkbox"/> はい <input type="checkbox"/> 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. SAQ B 記入の適格性

このペイメントチャネルが下記に該当することから、加盟店は本自己問診 (SAQ) 簡略版への記入の適格性を証明します。:

<input type="checkbox"/>	加盟店は、消費者のペイメントカード情報をインプリントするために、インプリントマシンのみを使用し、電話回線またはインターネットを経由して伝送していない。; または、 加盟店は、スタンドアロンのダイヤルアウトターミナル (電話回線を介してあなたのプロセッサに接続されている) のみを使用し、スタンドアロンのダイヤルアウトターミナルは、インターネットや加盟店環境内にある他のいかなるシステムにも接続されていない。
<input type="checkbox"/>	加盟店は、ネットワーク (内部ネットワークまたはインターネット) 経由でカード会員データを伝送していない。
<input type="checkbox"/>	加盟店は、電子形式でカード会員データを保存していない。
<input type="checkbox"/>	加盟店がカード会員データを保存する場合、そのようなデータは紙のレポートまたは紙の受領書のコピーのみであり、電子的に受信されていない。

セクション 2: 自己問診 B

注: 以下の質問は、『PCI DSS 要件とセキュリティ評価手順』に定義されているとおり、PCI DSS 要件とテスト手順に従って採番されています。

自己問診の完了日:

カード会員データの保護

要件 3: 保存されるカード会員データの保護

PCI DSS 質問	必要なテスト	回答 (各質問に対して1つ回答を選んでください)				
		はい	はい、 CCW 付	いいえ	N/A	
3.2	(c) 機密認証データは認証プロセスが完了次第削除または復元不可能にしていますか?	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー システム構成の調査 削除プロセスの調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) すべてのシステムが、(暗号化されている場合も) 承認後のセンシティブ認証データの非保持に関する以下の要件に準拠していますか:					
3.2.1	承認後にフルトラックの内容(カード裏面の磁気ストライプ、チップ上に含まれる同等のデータ、または他の場所から)が保存されていませんか? このデータは、フルトラック、トラック、トラック1、トラック2、および磁気ストライプデータとも呼ばれます。 注: 通常取引過程では、磁気ストライプからの以下のデータ要素を保存する必要が生じる場合があります。 <ul style="list-style-type: none"> カード会員名 プライマリアカウント番号(PAN) 有効期限、および サービスコード リスクを最小限に抑えるため、取引に必要なデータ要素のみを保存します。	<ul style="list-style-type: none"> データソースとして以下を含む調査 <ul style="list-style-type: none"> 受入トランザクションデータ すべてのログ 履歴ファイル トレースファイル データベーススキーマ データベースコンテンツ 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 質問	必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
		はい	はい、 CCW 付	いいえ	N/A
3.2.2 カード検証コードまたは値（ペイメントカードの前面または裏面に印字された3桁または4桁の数字）は承認後保存されませんか？	<ul style="list-style-type: none"> ▪ データソースとして以下を含む調査 <ul style="list-style-type: none"> • 受入トランザクションデータ • すべてのログ • 履歴ファイル • トレースファイル • データベーススキーマ • データベースコンテンツ 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3 個人識別番号（PIN）または暗号化されたPINブロックを承認後保存していませんか？	<ul style="list-style-type: none"> ▪ データソースとして以下を含む調査 <ul style="list-style-type: none"> • 受入トランザクションデータ • すべてのログ • 履歴ファイル • トレースファイル • データベーススキーマ • データベースコンテンツ 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3 表示時にPANをマスクして（最初の6桁と最後の4桁が最大表示桁数）、業務上の正当な必要性がある関係者だけがPAN全体を見ることができるようにしていますか？ <i>注: カード会員データの表示（法律上、またはペイメントカードブランドによるPOSレシート要件など）に関するこれより厳しい要件がある場合は、その要件より優先されることはありません。</i>	<ul style="list-style-type: none"> ▪ ポリシーおよび手順のレビュー ▪ PAN全桁を表示するアクセスが必要な役割のレビュー ▪ システム構成の調査 ▪ PANの表示の観察 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

要件 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

PCI DSS 質問		必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
			はい	はい、 CCW 付	いいえ	N/A
4.2	(b) 実施されているポリシーは、保護されていない PAN のエンドユーザメッセージングテクノロジーでの送信を防ぐものとなっていますか？	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

強力なアクセス制御手法の導入

要件 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

PCI DSS 質問		必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
			はい	はい、 CCW 付	いいえ	N/A
7.1	システムコンポーネントとカード会員データへのアクセスは、次のように業務上必要な人に限定されていますか？					
7.1.2	特権ユーザー ID へのアクセスが次のように制限されていますか？ <ul style="list-style-type: none"> ▪ 職務の実行に必要な最小限の特権に制限されている ▪ そのアクセス権を特に必要とする役割にのみ割り当てられる 	<ul style="list-style-type: none"> ▪ アクセス制御ポリシー文書の調査 ▪ 担当者のインタビュー ▪ 管理者のインタビュー ▪ 特権ユーザー ID のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	アクセス権の付与は、個人の職種と職務に基づいていますか？	<ul style="list-style-type: none"> ▪ アクセス制御ポリシー文書の調査 ▪ 管理者のインタビュー ▪ ユーザー ID のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

要件 9: カード会員データへの物理アクセスを制限する

PCI DSS 質問		必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
			はい	はい、 CCW 付	いいえ	N/A
9.5	<p>媒体（コンピュータ、リムーバブル電子メディア、紙の受領書、紙のレポート、FAX など）はすべて物理的にセキュリティ保護されていますか？</p> <p>要件 9 において「媒体」とは、カード会員データを含むすべての紙および電子媒体のことです。</p>	<ul style="list-style-type: none"> メディアの物理的な安全に関するポリシーおよび手順のレビュー 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6	(a) あらゆる種類の媒体の、内部または外部の配布に関して、厳格な管理が行われていますか？	<ul style="list-style-type: none"> メディア廃棄のポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 管理には、以下の内容が含まれていますか？					
9.6.1	媒体は、機密であることが分かるように分類されていますか？	<ul style="list-style-type: none"> メディア分類のポリシーおよび手順のレビュー セキュリティ担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.2	媒体は、安全な配達業者または正確な追跡が可能なその他の配送方法によって送付されていますか？	<ul style="list-style-type: none"> 担当者のインタビュー メディア配布追跡ログおよび文書の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	媒体を移動する前（特に媒体を個人に配布する場合）に管理者の承認を得ていますか？	<ul style="list-style-type: none"> 担当者のインタビュー メディア配布追跡ログおよび文書の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	媒体の保存およびアクセスに関して、厳格な管理が維持されていますか？	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8	(a) ビジネスまたは法律上の理由で不要になった場合、媒体はすべて破棄されていますか？	<ul style="list-style-type: none"> 定期的なメディアの廃棄ポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) 破棄は、以下の方法によって行われていますか？					

PCI DSS 質問		必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
			はい	はい、 CCW 付	いいえ	N/A
9.8.1	(a) ハードコピー資料は、カード会員データを再現できないように、クロスカット裁断、焼却、またはパルプ状に溶解していますか？	<ul style="list-style-type: none"> 定期的なメディアの廃棄ポリシーおよび手順のレビュー 担当者のインタビュー プロセスの観察 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 破棄する情報を含む材料の保存に使用されているストレージコンテナは、中身にアクセスできないようにセキュリティ保護されていますか？	<ul style="list-style-type: none"> 定期的なメディアの廃棄ポリシーおよび手順のレビュー ストレージコンテナのセキュリティの調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9	<p>カードから直接物理的な読み取りを經由してペイメントカードデータをキャプチャするデバイスが改ざんおよび不正置換から保護されていますか？</p> <p>注: この要件には、カード（カードのスイープやディップ）によるトランザクションに使用されるカード読み取り装置も含まれる。この要件は、コンピュータのキーボードやPOSのキーパッドのような手動キー入力コンポーネントには適用されません</p>					
	(a) ポリシーと手順はデバイスの一覧の維持を要求していますか？	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ポリシーと手順はデバイスを定期的に検査して改ざんや不正置換がないか調べることを要求していますか？	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ポリシーと手順は関係者にトレーニングを行い、怪しい行動を識別し、POS デバイスの改ざんや不正置換を報告できるようにすることを要求していますか？	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.1	<p>(a) デバイスのリストには以下が含まれていますか？</p> <ul style="list-style-type: none"> 装置のメーカーと形式 装置の場所（例えば、装置が設置されている拠点や施設の住所） 装置の連番や他の一意な識別番号 	<ul style="list-style-type: none"> デバイスの一覧の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 質問	必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
		はい	はい、 CCW 付	いいえ	N/A
(b) リストは正確で最新になっていますか?	<ul style="list-style-type: none"> デバイスとデバイス設置場所の観察と一覧の比較 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) 装置が追加、移動、廃棄された場合に装置のリストが更新されていますか?	<ul style="list-style-type: none"> 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.2 (a) 改ざん（カードスキマーの取り付けなど）や不正置換（連番など装置の特性を調べて偽の装置に差し替えられていないことを確認する）を検出するために定期的に装置の表面を次のように検査していますか？ 注: 装置が改ざんされたり不正置換された兆候の例としては、予期していない付着物やケーブルが装置に差し込まれている、セキュリティラベルが無くなっていたり、変更されている、ケースが壊れていたり、色が変わっている、あるいは連番その他の外部マーキングが変更されているなどがあります。	<ul style="list-style-type: none"> 担当者のインタビュー 検査プロセスの観察と定義済プロセスとの比較 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) 関係者は装置を検査する手順を知っていますか?	<ul style="list-style-type: none"> 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.3 関係者は装置の改ざんや不正置換の試みを認識できるようにトレーニングを受けていますか?					

PCI DSS 質問	必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
		はい	はい、 CCW 付	いいえ	N/A
(a) POS のある場所の関係者用トレーニング資料には、以下のトレーニングが含まれていますか？ <ul style="list-style-type: none"> • 第三者の修理・保守関係者を名乗っている者に POS 装置へのアクセスを許可する前に、身元を確認する • 検証なしで装置を設置、交換、返品しない • 装置の周辺での怪しい行動（知らない人が装置のプラグを抜いたり装置を開けたりする）に注意する • 怪しい行動や POS 装置が改ざんや不正置換された形跡がある場合には適切な関係者（マネージャーやセキュリティ関係者など）に報告する 	<ul style="list-style-type: none"> ▪ トレーニング資料のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) POS 拠点の関係者はトレーニングを受けており、装置の改ざんや不正置換を検出し、報告する手順を知っていますか？	<ul style="list-style-type: none"> ▪ POS 拠点担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

情報セキュリティポリシーの維持

要件 12: すべての担当者の情報セキュリティに対応するポリシーを維持する

注: 要件 12 において、「担当者」とはフルタイムおよびパートタイムの従業員、一時的な従業員や担当者、事業体の敷地内に「常駐」しているか、またはカード会員データ環境にアクセスできる請負業者やコンサルタントのことです。

PCI DSS 質問	必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
		はい	はい、 CCW 付	いいえ	N/A
12.1	すべての関係する担当者に対してセキュリティポリシーが確立、公開、維持、および周知されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.1.1	少なくとも年に一度レビューし、環境が変更された場合に更新していますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3	重要なテクノロジーに関する使用ポリシーを作成し、以下を含むテクノロジーの適切な使用方法を定義していますか？ <i>注: 重要なテクノロジーの例には、リモートアクセスおよびワイヤレステクノロジー、ノートパソコン、タブレット、リムーバブル電子媒体、電子メールの使用、インターネットの使用がありますが、これらに限定されません</i>				
12.3.1	テクノロジーを使用するために、権限を持つ関係者による明示的な承認が要求されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.3	このようなすべてのデバイスおよびアクセスできる担当者のリストは用意されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	テクノロジーの許容される利用法が要求されていますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.4	すべての担当者に対して、情報セキュリティ上の責任をセキュリティポリシーと手順に明確に定義していますか？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 質問		必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
			はい	はい、 CCW 付	いいえ	N/A
12.5	(b) 個人またはチームに以下の情報セキュリティ管理責任が正式に割り当てられていますか?					
12.5.3	セキュリティインシデントの対応およびエスカレーション手順を制定、文書化、および周知して、あらゆる状況をタイムリーかつ効果的に処理する責任を割り当てていますか?	<ul style="list-style-type: none"> 情報セキュリティポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.6	(a) 正式なセキュリティに関する認識を高めるプログラムを実施して、すべての担当者がカード会員データセキュリティの重要性を認識するようにしていますか?	<ul style="list-style-type: none"> セキュリティ意識向上プログラムのレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8	カード会員データを共有するか、カード会員データのセキュリティに影響を与えるサービスプロバイダを管理するポリシーと手順が以下の通り整備および実施されていますか?					
12.8.1	提供されるサービスの詳細を含むサービスプロバイダのリストが整備されていますか?	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー プロセスの観察 サービスプロバイダの一覧のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.2	サービスプロバイダが自社で所有する、または顧客より委託を受けて保管、処理、伝送するカード会員データ環境の安全に影響を及ぼすような内容を含むカード会員データのセキュリティに対して責任を負うことについて、同意を得て、契約書を取り交わしていますか? 注: 同意の正確な言葉づかいは、両当事者間の同意事項、提供サービスの詳細、各当事者に割り当てられた責任によって異なります。同意には、この要件に記載されているのとまったく同じ言葉づかいを含める必要はありません。	<ul style="list-style-type: none"> 合意契約書の観察 ポリシーおよび手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.3	契約前の適切なデューデリジェンスを含め、サービスプロバイダとの契約に関するプロセスが確立されていますか?	<ul style="list-style-type: none"> プロセスの観察 ポリシーおよび手順と補足文書のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 質問		必要なテスト	回答 (各質問に対して1つ回答を選んでください)			
			はい	はい、 CCW 付	いいえ	N/A
12.8.4	少なくとも年1回サービスプロバイダのPCI DSS 準拠ステータスを監視するプログラムが維持されていますか？	<ul style="list-style-type: none"> プロセスの観察 ポリシーおよび手順と補足文書のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	各サービスプロバイダに対して、どのPCI DSS 要件がサービスプロバイダによって管理され、どの要件が対象の事業体により管理されるかについての情報が維持されていますか？	<ul style="list-style-type: none"> プロセスの観察 ポリシーおよび手順と補足文書のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.1	(a) システム違反が発生した場合に実施されるインシデント対応計画が作成されていますか？	<ul style="list-style-type: none"> インシデント対応計画のレビュー インシデント対応計画手順のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

付録 A: 追加の PCI DSS 要件

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

この付録は加盟店評価では使用されません。

付録 A2: SSL / 初期の TLS を使用している事業者向けの PCI DSS 追加要件

この付録は SAQ B 加盟店評価では使用されません。

付録 A3: 指定事業者向け追加検証 (DESV)

この付録はペイメントブランドまたはアクワイアラーによって PCI DSS 既存要件の追加検証が必要であると指定された事業者のみに適用されます。この付録の検証を求められた事業者は、報告のために『DESV 追加報告テンプレートおよび追加準拠証明書』を使用する必要があり、提出手順について該当するペイメントブランドおよび/またはアクワイアラーへ相談する必要があります。

付録 B: 代替コントロールワークシート

このワークシートを使用して、「はい、CCW 付」と回答した要件について代替コントロールを定義します。

注: 準拠を実現するために代替コントロールの使用を検討できるのは、リスク分析を実施済みで、正当なテクノロジーまたはビジネス上の制約がある企業のみです。

代替コントロールの使用に関する情報とワークシートの記入方法についてのガイダンスは、PCI DSS の付録 B、C を参照してください。

要件番号と定義:

	必要な情報	説明
1. 制約	元の要件への準拠を不可能にする制約を列挙する。	
2. 目的	元のコントロールの目的を定義し、代替コントロールによって満たされる目的を特定する。	
3. 特定されるリスク	元のコントロールの不足によって生じる追加リスクを特定する。	
4. 代替コントロールの定義	代替コントロールを定義し、元のコントロールの目的および追加リスク（ある場合）にどのように対応するかを説明する。	
5. 代替コントロールの検証	代替コントロールの検証およびテスト方法を定義する。	
6. 維持	代替コントロールを維持するために実施するプロセスおよび管理を定義する。	

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、(SAQ完了日)付のSAQ A-EP(セクション2)に記載した結果に基づいています。

上記に記載されたSAQ Bの結果を基に、パート3b-3dで識別された署名者（該当する場合は、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）：

<input type="checkbox"/>	準拠: PCI SAQ のすべてのセクションの記入を完了し、すべての質問に対する回答が肯定的であったため、全体的な評価が準拠になり、(加盟店名)は PCI DSS に完全には準拠していないことが示されました。						
<input type="checkbox"/>	非準拠: PCI SAQ のすべてのセクションの記入を完了しなかったか、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、(加盟店名)は PCI DSS に完全には準拠していることを示しませんでした。 準拠の目標期日: 非準拠の状態での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に記入する前にアクワイアラーまたはペイメントブランドに確認してください。						
<input type="checkbox"/>	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「いいえ」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。 <table border="1" data-bbox="289 1115 1409 1276"><thead><tr><th>影響を受けた要件</th><th>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</th></tr></thead><tbody><tr><td> </td><td> </td></tr><tr><td> </td><td> </td></tr></tbody></table>	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				
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を選んでください)

<input type="checkbox"/>	PCI DSS 自己問診D、バージョン(SAQバージョン)を、同書の指示に従って完了しました。
<input type="checkbox"/>	上記で参照されている SAQ およびこの証明書すべての情報は、評価の結果をすべての重要な点において公正に表しています。
<input type="checkbox"/>	私は、当社のペイメントアプリケーションベンダに、当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。
<input type="checkbox"/>	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。
<input type="checkbox"/>	私は、当社の環境が変化した場合に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)

- | | |
|--------------------------|--|
| <input type="checkbox"/> | 取引承認後にフルトラックデータ ¹ 、CAV2、CVC2、CID、CVV2 データ ² 、または PIN データ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。 ³ |
| <input type="checkbox"/> | ASV スキャンは PCI SSC 認定スキニングベンダ (ASV Name) が実施しています。 |

パート 3b. 加盟店の証明書

加盟店役員の署名 [↑]	日付:
加盟店役員名:	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 会社の正当な権限を有する役員の署名 [↑]	日付:
正当な権限を有する役員の名前:	QSA の会社:

パート 3d. 内部セキュリティ評価者 (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、ISA 個人の識別と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することはできません。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 に記入する前にアクワイアラーまたは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	
3	保存されるカード会員データを保護する	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	
9	カード会員データへの物理アクセスを制限する	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	

* ここで示した PCI DSS 要件は SAQ のセクション 2 を参照



翻訳協力会社

この翻訳文書は、日本カード情報セキュリティ協議会、以下の QSA 各社、およびユーザ部会各社により作成されました。

	日本カード情報セキュリティ協議会
	株式会社インフォセック
	NRI セキュアテクノロジーズ株式会社
	NTT データ先端技術株式会社
	国際マネジメントシステム認証機構株式会社
	ネットワンシステムズ株式会社
	BSI グループジャパン株式会社
	富士通株式会社
	株式会社ブロードバンドセキュリティ