PCI (Payment Card Industry)
データセキュリティ基準

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

スタンドアロン型 IP 接続 PTS 加盟店端末装置 (POI) 端末を持つ加盟店（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 **3.2.1**

2018 年 6 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 , © 2006-2018 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。不明瞭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 , © 2006-2018 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
N/A	1.0		未使用
N/A	2.0		未使用
2014 年 2 月	3.0		ペイメントプロセッサーに IP 接続される、スタンドアロン型 PTS 認定の加盟店端末装置のみによって、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新しい SAQ。 内容を PCI DSS v3.0 の要件とテスト手順に合わせて改訂。
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。 PCI DSS v3.2 から付録 A2 が追加されました。
2017 年 1 月	3.2	1.1	"SCR"と許可されるシステムの意図を明確にするために「開始する前に」へ注釈を追加。 要件 2.3 の意図に関連して要件 8.3.1 を追加 セグメンテーションが使われる場合のセグメンテーションコントロールを確認するために要件 11.3.4 を追加
2018 年 6 月	3.2.1	1.0	PCI DSS v3.2.1 にあわせて更新。 詳細については、「PCI DSS - PCI DSS バージョン 3.2 から 3.2.1 への変更点のまとめ」を参照してください。

目次

開始する前に

SAQ B-IP は、ペイメントプロセサーに IP 接続される、スタンドアロン型 PTS 認定の加盟店端末装置のみによって、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ました。セキュアカードリーダ(SCR)として分類される POI 装置に対して例外が適用します。すなわち、SCR を使う加盟店はこの SAQ の対象外です。セキュアカードリーダ(SCR)と分類される POI 装置は適用が除外され、この SAQ は SCR を使う加盟店には適切ではありません。

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-IP 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、顧客のペイメントカード情報を取り込むためにペイメントプロセサーに IP 経由で接続されているスタンドアロン型 PTS 承認の加盟店端末装置 (POI) （SCR を除く）のみを使用しています。
- スタンドアロン型 IP 接続 POI 装置は、PCI SSC Web サイトに一覧表示されている通り PTS POI プログラムに対して検証されます（SCR を除く）。
- スタンドアロン型 IP 接続 POI 装置は、環境内の他のシステムには接続されていません（これは、POI 装置を他のすべてのシステムから分離するネットワークセグメンテーションによって実現できます）*1
- カード会員データの唯一の伝送は、PTS 認定 POI 装置からペイメントプロセサーへのものです。
- POI 装置は他の装置（コンピュータ、携帯電話、タブレット等）を介すことなく ペイメントプロセサーに接続されます。
- 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。**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。

*1 この基準は、許可されたシステムが他のタイプのシステムから隔離されている限り（例:ネットワークセグメンテーションを実装により）、2 つ以上の許可されたシステムタイプ（つまり IP 接続 POI 装置）が同じネットワークゾーンに存在するのを、禁止するものではありません。また、この基準は、定義されたシステムタイプが、アクワイアラーやペイメントプロセッサー等のプロセシングを行う第三者にネットワークを介して取引情報を送信できないようにする事を意図したものではありません。

- 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-IP)
- 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、アクワイアラー、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	内容
PCI DSS *（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）*	• 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	• 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
PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）	• 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

SAQ B-IP を完成させる会社の多くは各 PCI DSS 要件への準拠を検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。たとえば、ワイヤレス技術をまったく使用しない会社は、ワイヤレス技術の管理に特化した PCI DSS セクションへの準拠を検証する必要がありません（例えば、要件 1.2.3、2.1.1、4.1.1など）。

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、契約先のアクワイアラー（加盟店銀行）またはペイメントブランドに問い合わせてください。

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)

☐ 小売	☐ 電気通信	☐食料雑貨およびスーパーマーケット
☐ 石油	☐電子商取引	☐ 通信販売
☐ 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？	この SAQ でカバーされている支払チャネルはどれですか？
☐ 通信販売(MO/TO)	☐ 通信販売(MO/TO)
☐ 電子商取引	☐ 電子商取引
☐ カード提示（対面式）	☐ 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でこの 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 2. 概要 (続き)

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 登録済みですか載っていますか	PA-DSS 登録の有効期限 (該当する場合)
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ 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、そ 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	☐ はい

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ーション」セクションを参照してください。）*	☐ いいえ

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？	☐ はい ☐ いいえ

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:	

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、ペイメントプロセサー、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）？	☐ はい ☐ 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-IP 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

☐	加盟店は、消費者のペイメントカード情報を取り入れるために、加盟店のペイメントプロセッサに IP を介して接続されているスタンドアロンの、PTS 承認の加盟店端末装置（SCR を除く）のみを使用している。
☐	IP 接続されたスタンドアロンの加盟店端末装置は、PCI SSC Web サイトのリストに載っている PTS POI プログラムに対して検証されている。（SCR を除く）
☐	IP 接続されたスタンドアロンの加盟店端末装置は、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。（これは、その他のシステムから分離するためのネットワークセグメンテーションによって実現できます）

☐	カード会員データは唯一、PTS 承認の加盟店端末装置によって、ペイメントプロセッサに伝送されている。
☐	加盟店端末装置は、ペイメントプロセッサに接続するために、他のいかなるデバイス（例えば、コンピュータ、携帯電話、タブレットなど）にも依存しない。
☐	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。
☐	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-IP

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:

安全なネットワークとシステムの構築と維持

要件 1: *カード会員データを保護するために、ファイアウォールをインストールして構成を維持する*

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
1.1.2	(a) ワイヤレスネットワークを含め、カード会員データ環境と他のネットワークとの間のすべての接続を文書化した最新のネットワーク図はありますか?	▪ 最新のネットワーク図のレビュー ▪ ネットワーク構成の調査	☐	☐	☐	☐
	(b) 図が最新に保たれていることを確認するプロセスがありますか?	▪ 責任者のインタビュー	☐	☐	☐	☐
1.1.4	(a) 各インターネット接続、および DMZ（demilitarized zone）と内部ネットワークゾーンとの間にファイアウォールが要求され、実装されていますか?	▪ ファイアウォール構成基準のレビュー ▪ 対象範囲内のファイアウォールが確認できるネットワーク構成の観察	☐	☐	☐	☐
	(b) 現在のネットワーク図は、ファイアウォール構成基準と一致していますか?	▪ ファイアウォール構成基準と最新のネットワーク図の比較	☐	☐	☐	☐
1.1.6	(a) ファイアウォール/ルーター構成基準に、業務に必要なサービス、プロトコル、ポートと業務における各々の必要性と承認を含むリストが文書化されていますか?	▪ ファイアウォールおよびルータ構成基準のレビュー	☐	☐	☐	☐

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) 安全でないサービス、プロトコル、およびポートはすべて特定され、それぞれについてセキュリティ機能が文書化され、特定された各サービスで実装されていますか?	▪ ファイアウォールおよびルータ構成基準のレビュー ▪ ファイアウォールおよびルータ構成の調査	☐	☐	☐	☐
1.2	信頼できないネットワークとカード会員データ環境内のすべてのシステム間の接続が、次のように、ファイアウォール/ルーター構成によって制限されていますか? ***注:*** *「信頼できないネットワーク」とは、レビュー対象の事業体に属するネットワーク外のネットワーク、または事業体の制御または管理が及ばないネットワーク（あるいはその両方）のことです。*					
1.2.1	(a) 着信および発信トラフィックが、カード会員データ環境に必要なトラフィックに制限されていますか?	▪ ファイアウォールおよびルータ構成基準のレビュー ▪ ファイアウォールおよびルータ構成の調査	☐	☐	☐	☐
	(b) たとえば明示の「すべてを拒否」、または許可文の後の暗黙の拒否を使用することで、他のすべての着信および発信トラフィックが明確に拒否されていますか?	▪ ファイアウォールおよびルータ構成基準のレビュー ▪ ファイアウォールおよびルータ構成の調査	☐	☐	☐	☐
1.2.3	すべてのワイヤレスネットワークとカード会員データ環境の間に境界ファイアウォールがインストールされており、これらのファイアウォールはワイヤレス環境とカード会員データ環境間のトラフィックを拒否または（業務上必要な場合）承認されたトラフィックのみを許可するように構成されていますか?	▪ ファイアウォールおよびルータ構成基準のレビュー ▪ ファイアウォールおよびルータ構成の調査	☐	☐	☐	☐

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
1.3	インターネットとカード会員データ環境内のすべてのシステムコンポーネント間の、直接的なパブリックアクセスは禁止されていますか?					
1.3.3	アンチスプーフィング対策を実施し、偽の送信元 IP アドレスを検出して、ネットワークに侵入されないようにブロックしていますか? （たとえば、内部アドレスを持つインターネットからのトラフィックをブロックするなど）	▪ ファイアウォールおよびルータ構成の調査	☐	☐	☐	☐
1.3.4	カード会員データ環境からインターネットへの発信トラフィックは明示的に承認されていますか?	▪ ファイアウォールおよびルータ構成の調査	☐	☐	☐	☐
1.3.5	ネットワーク内への接続は確立された接続のみ許可されていますか?	▪ ファイアウォールおよびルータ構成の調査	☐	☐	☐	☐

要件 2:　　システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない

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
2.1	(a) システムをネットワークに導入する前に、ベンダ提供のデフォルト値が必ず変更されていますか? *これは、オペレーティングシステム、セキュリティサービスを提供するソフトウェア、アプリケーション、システムアカウント、POS 端末、ペイメントアプリケーション、簡易ネットワーク管理プロトコル（SNMP）コミュニティ文字列で使用されるがこれらに限定されない、すべてのデフォルトパスワードに適用されます。*	▪ ポリシーおよび手順のレビュー ▪ ベンダ文書の調査 ▪ システム構成およびアカウント設定の観察 ▪ 担当者のインタビュー	☐	☐	☐	☐
	(b) ネットワーク上にシステムをインストールする前に不要なデフォルトアカウントを削除または無効化されましたか?	▪ ポリシーおよび手順のレビュー ▪ ベンダ文書のレビュー ▪ システム構成およびアカウント設定の調査 ▪ 担当者のインタビュー	☐	☐	☐	☐
2.1.1	カード会員データ環境に接続されている、またはカード会員データを伝送するワイヤレス環境について、すべてのベンダのデフォルト値が、以下のように変更されていますか?					
	(a) 暗号鍵がインストール時のデフォルトから変更されていて、鍵の知識を持つ人物が退社または異動するたびに、鍵が変更されていますか?	▪ ポリシーおよび手順のレビュー ▪ ベンダ文書のレビュー ▪ 担当者のインタビュー	☐	☐	☐	☐
	(b) ワイヤレスデバイスのデフォルトの SNMP コミュニティ文字列がインストール時に変更されていますか?	▪ ポリシーおよび手順のレビュー ▪ ベンダ文書のレビュー ▪ 担当者のインタビュー ▪ システム構成の調査	☐	☐	☐	☐

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
2.1.1 (続き)	(c) アクセスポイントのデフォルトのパスワード/パスフレーズがインストール時に変更されていますか?	▪ ポリシーおよび手順のレビュー ▪ 担当者のインタビュー ▪ システム構成の調査	☐	☐	☐	☐
	(d) ワイヤレスデバイスのファームウェアが更新され、ワイヤレスネットワーク経由の認証および伝送用の強力な暗号化をサポートしていますか?	▪ ポリシーおよび手順のレビュー ▪ ベンダ文書のレビュー ▪ システム構成の調査	☐	☐	☐	☐
	(e) その他、セキュリティに関連するワイヤレスベンダのデフォルト値は変更されていますか?(該当する場合)	▪ ポリシーおよび手順のレビュー ▪ ベンダ文書のレビュー ▪ システム構成の調査	☐	☐	☐	☐
2.3	すべての非コンソール管理アクセスは以下のように暗号化されていますか?					
	(a) すべての非コンソール管理アクセスは強力な暗号化技術を使用して暗号化され、管理者パスワードが要求される前に、強力な暗号化方式が実行されていますか?	▪ システムコンポーネントの調査 ▪ システム構成の調査 ▪ 管理者ログオンの観察	☐	☐	☐	☐
	(b) システムサービスおよびパラメータファイルは、Telnet などの安全でないリモートログインコマンドを使用できないように構成されていますか?	▪ システムコンポーネントの調査 ▪ サービスおよびファイルの調査	☐	☐	☐	☐

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
	(c) Web ベース管理インターフェースへの管理者アクセスは、強力な暗号化技術で暗号化されていますか?	▪ システムコンポーネントの調査 ▪ 管理者ログオンの観察	☐	☐	☐	☐
	(d) 使用テクノロジの強力な暗号化が業界のベストプラクティスとベンダの推奨事項に従って導入されていますか?	▪ システムコンポーネントの調査 ▪ ベンダ文書のレビュー ▪ 担当者のインタビュー	☐	☐	☐	☐

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を保護する*

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
3.2	(c) 機密認証データを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?	▪ 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	☐	☐	☐	☐
	(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）は承認後保存されませんか？ *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:*** *通常の取引過程では、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。* • *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。*	▪ データソースとして以下を含む調査 • 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	☐	☐	☐	☐

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?	▪ データソースとして以下を含む調査 • 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	☐	☐	☐	☐
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されませんか?	▪ データソースとして以下を含む調査 • 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	☐	☐	☐	☐
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 の最初の 6 桁と最後の 4 桁より多くを見ることができるようにしていますか? ***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、その要件が優先します。*	▪ 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	☐	☐	☐	☐

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
4.1	(a) オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化技術と安全なプロトコルを使用して保護していますか? ***注:*** *オープンな公共ネットワークの例として、インターネット、802.11 および Bluetooth を含むワイヤレス技術、携帯電話技術、例えば Global System for Mobile communications (GSM)、符号分割多元接続 (CDMA)、および General Packet Radio Service (GPRS) などが挙げられますが、これらに限りません。*	▪ 文書化された基準のレビュー ▪ ポリシーおよび手順のレビュー ▪ CHD が伝送するまたは受領するすべての拠点のレビュー ▪ システム構成の調査	☐	☐	☐	☐
	(b) 信頼できる鍵および/または証明書のみが受け付けられていますか?	▪ 着信および発信伝送の観察 ▪ 鍵および証明書の調査	☐	☐	☐	☐
	(c) 実装されたセキュリティプロトコルは安全な構成のみ使用され、安全でないバージョンまたは構成がサポートされていませんか?	▪ システム構成の調査	☐	☐	☐	☐
	(d) 使用中の暗号化手法（ベンダの推奨事項/ベストプラクティスを確認）は適切な暗号化強度が実装されていますか?	▪ ベンダ文書のレビュー ▪ システム構成の調査	☐	☐	☐	☐
	(e) 使用中の暗号化手法（ベンダの推奨事項/ベストプラクティスを確認）は適切な暗号化強度が実装されていますか? *例えば、ブラウザベースの実装の場合：* • *ブラウザの URL プロトコルとして「HTTPS」が表示される、および* • カード会員データは、URL に「HTTPS」が表示される場合にのみ要求される	▪ システム構成の調査	☐	☐	☐	☐

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
4.1.1	カード会員データを伝送する、またはカード会員データ環境に接続しているワイヤレスネットワークには、業界のベストプラクティスを使用して、認証および伝送用に強力な暗号化が実装されていますか?	▪ 文書化された基準のレビュー ▪ ワイヤレスネットワークのレビュー ▪ システム構成設定の調査	☐	☐	☐	☐
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での送信を防ぐものとなっていますか?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐

脆弱性管理プログラムの維持

要件 6: *安全性の高いシステムとアプリケーションを開発し、保守する*

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
6.1	セキュリティの脆弱性を識別するための以下を含むプロセスが導入されていますか? ▪ 信頼できる外部情報源を使用したセキュリティ脆弱性情報の収集 ▪ すべての「高」リスクと「重大」な脆弱性の識別を含む脆弱性のランク分けの割り当て *注: リスクのランク分けは、業界のベストプラクティスと考えられる影響の程度に基づいている必要があります。たとえば、脆弱性をランク分けする基準は、CVSS ベーススコア、ベンダによる分類、影響を受けるシステムの種類などを含む場合があります。* *脆弱性を評価し、リスクのランクを割り当てる方法は、組織の環境とリスク評価戦略によって異なります。 リスクのランクは、最小限、環境に対する「高リスク」とみなされるすべての脆弱性を特定するものである必要があります。リスクのランク分けに加えて、環境に対する差し迫った脅威をもたらす、重要システムに影響を及ぼす、対処しないと侵害される危険がある場合、脆弱性は「重大」とみなされます。重要システムの例としては、セキュリティシステム、一般公開のデバイスやシステム、データベース、およびカード会員データを保存、処理、送信するシステムなどがあります。*	▪ 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	☐	☐	☐	☐
6.2	(a) すべてのシステムコンポーネントとソフトウェアに、ベンダ提供のセキュリティパッチがインストールされ、既知の脆弱性から保護されていますか?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐

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) 重要なセキュリティパッチが、リリース後 1 カ月以内にインストールされていますか? *注: 要件 6.1 で定義されているリスクのランク分けプロセスに従って、重要なセキュリティパッチを識別する必要があります。*	▪ ポリシーおよび手順のレビュー ▪ システムコンポーネントの調査 ▪ インストール済セキュリティパッチの一覧と最近のベンダパッチの一覧の比較	☐	☐	☐	☐

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? ▪ 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	▪ アクセス制御ポリシー文書の調査 ▪ 担当者ノインタビュー ▪ 管理者のインタビュー ▪ 特権ユーザ ID のレビュー	☐	☐	☐	☐
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?	▪ 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 ID のレビュー	☐	☐	☐	☐

要件 8:　　システムコンポーネントへのアクセスを確認・許可する

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
8.1.5	(a) ベンダがリモートアクセスを通してシステムコンポーネントのアクセス、サポート、管理に使用するアカウントは、必要な期間のみ有効にされており、使用されなくなったら無効にされていますか?	▪ パスワード手順のレビュー ▪ 担当者のインタビュー ▪ プロセスの観察	☐	☐	☐	☐
	(b) ベンダのリモートアクセスアカウントが使用されている間、そのアカウントは監視されていますか?	▪ 担当者のインタビュー ▪ プロセスの観察	☐	☐	☐	☐
8.3	カード会員データ環境への非コンソールの管理者アクセスとすべてのリモートアクセスには、以下の 8.3.1～8.3.2 のように多要素認証が使用されていますか？ ***注:*** *多要素認証では、3 つの認証方法のうち 2 つを認証に使用する必要があります（認証方法については、PCI DSS 要件 8.2 を参照）。1 つの因子を 2 回使用すること（たとえば、2 つの個別パスワードを使用する）は、多要素認証とは見なされません。*					
8.3.1	カード会員データ環境への管理者のアクセス権を持つ担当者によるすべての非コンソールアクセスには多要素認証が組み込まれていますか？	▪ システム構成の調査 ▪ 管理者のカード会員データ環境へのログインの観察	☐	☐	☐	☐
8.3.2	従業員（ユーザと管理者を含む）および第三者（サポートやメンテナンス用のベンダアクセスを含む）によるネットワークへのリモートアクセス（ネットワーク外部からのネットワークレベルアクセス）に 多要素認証が組み込まれていますか?	▪ システム構成の調査 ▪ リモート接続担当者の観察	☐	☐	☐	☐

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
8.5	グループ、共有、または汎用のアカウントとパスワードや他の認証方法を以下のように禁止していますか? ▪ 汎用ユーザ ID およびアカウントが無効化または削除されている ▪ システム管理作業およびその他の重要な機能のための共有ユーザ ID が存在しない、および ▪ システムコンポーネントの管理に共有および汎用ユーザ ID が使用されていない	▪ ポリシーおよび手順のレビュー ▪ ユーザ ID 一覧の調査 ▪ 担当者のインタビュー	☐	☐	☐	☐

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
9.1.2	物理/論理制御を実施することで、誰でもアクセス可能なネットワークジャックへのアクセスを制限していますか? *例えば、公共の場や訪問者がアクセス可能なエリアにあるネットワークジャックは、無効にしておき、ネットワークへのアクセスが明示的に承認されている場合にのみ有効にすることができる。または、アクティブなネットワークジャックがあるエリアでは訪問者に常に同行者をつけるプロセスを実施できる。*	▪ ポリシーおよび手順のレビュー ▪ 担当者のインタビュー ▪ 拠点の観察	☐	☐	☐	☐
9.5	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? *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。*	▪ 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	☐	☐	☐	☐
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?	▪ メディア廃棄のポリシーおよび手順のレビュー	☐	☐	☐	☐
	(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?	▪ 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	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐

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
9.6.3	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?	▪ 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	☐	☐	☐	☐
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?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐
	(c) 破棄は、以下の方法によって行われていますか?					
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?	▪ 担当者のインタビュー ▪ 手順の調査 ▪ プロセスの観察	☐	☐	☐	☐
	(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?	▪ ストレージコンテナのセキュリティの調査	☐	☐	☐	☐
9.9	カードから直接物理的な読み取りを経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? ***注:*** *この要件には、カード（カードのスワイプやディップ）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*					
	(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?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐

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) 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?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
	(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?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
9.9.1	(a) デバイスのリストには以下が含まれていますか? • 装置のメーカと形式 • 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	▪ デバイスの一覧の調査	☐	☐	☐	☐
	(b) リストは正確で最新になっていますか?	▪ デバイスとデバイス設置場所の観察と一覧の比較	☐	☐	☐	☐
	(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?	▪ 担当者のインタビュー	☐	☐	☐	☐
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。*	▪ 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	☐	☐	☐	☐
	(b) 関係者は装置を検査する手順を知っていますか?	▪ 担当者のインタビュー	☐	☐	☐	☐

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
9.9.3	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?					
	(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? • 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	▪ トレーニング資料のレビュー	☐	☐	☐	☐
	(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?	▪ POS 拠点担当者のインタビュー	☐	☐	☐	☐

ネットワークの定期的な監視およびテスト

要件 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*

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
11.2.2	(a) 四半期に一度、外部の脆弱性スキャンが実行されていますか? ***注:*** *四半期に一度の外部の脆弱性スキャンは、PCI（Payment Card Industry）セキュリティ基準審議会（PCI SSC）によって資格を与えられた認定スキャニングベンダ（ASV）によって実行される必要がある。* *スキャンにおける顧客の責任、スキャンの準備などについては、PCI SSC Web サイトで公開されている『ASV プログラムガイド』を参照してください。*	▪ 直近 4 回分の四半期外部脆弱性スキャンの結果のレビュー	☐	☐	☐	☐
	(b) 外部の四半期ごとのスキャンの結果は ASV プログラムガイドの要件を満たしていますか（CVSS スコアで 4.0 を超える脆弱性がない、自動障害がない、など）?	▪ 各外部四半期スキャンと再スキャンの結果のレビュー	☐	☐	☐	☐
	(c) 四半期ごとの外部の脆弱性スキャンは、認定スキャニングベンダ（ASV）によって実行されていますか?	▪ 各外部四半期スキャンと再スキャンの結果のレビュー	☐	☐	☐	☐
11.3.4	セグメンテーションを用いて カード会員データ環境を他のネットワークから分離する場合：					
	(a) すべてのセグメンテーション方法をテストし、それらが運用可能で、効果的であることを確認し、カード会員データ環境内のシステムからすべての適用範囲外のシステムを分離する事を確認する事を定義した侵入テスト手順がありますか?	▪ セグメンテーション制御の調査 ▪ 侵入テスト方法論のレビュー	☐	☐	☐	☐

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) セグメンテーション制御を検証するための侵入テストは、以下の要件を満たしていますか？ • 少なくとも年 1 回、およびセグメント制御/手法を変更した後に実施する • 使用しているすべてのセグメンテーション制御／手法を含む • セグメンテーション手法が運用可能で効果的、カード会員データ環境内のシステムからすべての適用範囲外のシステムが分離されている事を検証する	▪ 最新の侵入テストの結果を調査	☐	☐	☐	☐
	(c) すべてのテストは、認定された内部リソースまたは外部の第三者によって実施されているか？該当する場合は、テスターが組織的に独立した立場であるか？（QSA や ASV である必要はない）	▪ 責任者のインタビュー	☐	☐	☐	☐

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?	▪ 情報セキュリティポリシーのレビュー	☐	☐	☐	☐
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?	▪ 情報セキュリティポリシーのレビュー ▪ 責任者のインタビュー	☐	☐	☐	☐
12.3	重要なテクノロジに関する使用ポリシーを作成し、以下を含むテクノロジの適切な使用方法を定義していますか? ***注:*** *重要なテクノロジの例には、リモートアクセスおよびワイヤレステクノロジ、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*					
12.3.1	テクノロジを使用するために、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?	▪ 使用方法ポリシーのレビュー ▪ 責任者のインタビュー	☐	☐	☐	☐
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?	▪ 使用方法ポリシーのレビュー ▪ 責任者のインタビュー	☐	☐	☐	☐
12.3.5	テクノロジの許容される利用法が要求されていますか?	▪ 使用方法ポリシーのレビュー ▪ 責任者のインタビュー	☐	☐	☐	☐
12.3.9	ベンダおよびビジネスパートナーには必要とする場合にのみリモートアクセステクノロジをアクティブ化し、使用後直ちに非アクティブ化する	▪ 使用方法ポリシーのレビュー ▪ 責任者のインタビュー	☐	☐	☐	☐

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
12.4	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?	▪ 情報セキュリティポリシーおよび手順のレビュー ▪ 責任者のサンプルのインタビュー	☐	☐	☐	☐
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当てていますか?	▪ 情報セキュリティポリシーおよび手順のレビュー	☐	☐	☐	☐
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?	▪ セキュリティ意識向上プログラムのレビュー	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐

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
12.8.2	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。*	▪ 合意契約書の観察 ▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
12.8.3	契約前の適切なデューディリジェンスを含め、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?	▪ 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	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐

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: カードを取り扱う POS POI 端末の接続に、SSL / 初期の TLS を使用する事業体への PCI DSS 追加要件

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
A2.1	*POS POI 端末（加盟店またはカード決済を行う場）においてSSL および/または 初期 TLS を利用している場合：* • デバイスは、SSL / 初期の TLS において既知の脆弱性に影響されないことを確認していますか? *注：この要件は、販売店などの POS POI 端末を持つ事業体に適用することを意図しています。この要件は、POS POI 端末の終端または接続ポイントとして機能するサービスプロバイダーを対象としていません。要件 A2.2 および A2.3 は POS POI サービスプロバイダーに適用されます。*	▪ POS POI デバイスが既知の SSL / 初期の TLS の影響を受けないことを検証した文書（例えば、ベンダ文書、システム/ネットワーク構成の焼成など）のレビュー	☐	☐	☐	☐

付録 A3: 指定事業体向け追加検証 (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体のみに適用されます。この付録の検証を求められた事業体は、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 要件とテスト手順』の「付録 B: 代替コントロール」、「付録 C: 代替コントロールワークシート」および、「代替コントロールワークシート – 完成例」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。	

付録 C:　　適用されない理由についての説明

「N/A」(該当なし)欄を選択した場合、このワークシートで該当要件が自社に適用されない理由を説明してください。

要件	要件が適用されない理由
例:	
3.4	カード会員データが電子的に保存されることはない。

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 B-IP(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-IP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)***：

☐	**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 に完全に準拠していることを示しました。
☐	**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。*
☐	**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。*

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)

☐	PCI DSS 自己問診B-IP、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。
☐	上記で参照されているSAQ およびこの証明書のすべての情報は、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。
☐	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。
☐	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。
☐	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）	
☐	取引承認後にフルトラックデータ[1]、CAV2、CVC2、CID、CVV2 データ、またはPIN データ[2]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]
☐	ASV スキャンはPCI SSC 認定スキャニングベンダ*(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	
1	カード会員データを保護するために、ファイアウォールをインストールして構成を維持する	☐	☐	
2	システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない	☐	☐	
3	保存されるカード会員データを保護する	☐	☐	
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	安全性の高いシステムとアプリケーションを開発し、保守する	☐	☐	
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	☐	☐	
8	システムコンポーネントへのアクセスを識別・認証する	☐	☐	
9	カード会員データへの物理アクセスを制限する	☐	☐	
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	☐	☐	
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	☐	☐	
付録 A2	カードを取り扱う POS POI 端末の接続に、SSL/初期 TLS を使用している事業体向けの追加の PCI DSS 要件	☐	☐	

** 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。

JCDSC Japan Card Data Security Consortium	日本カード情報セキュリティ協議会
Infosec	株式会社インフォセック
NRI SECURE TECHNOLOGIES	NRI セキュアテクノロジーズ株式会社
NTT DATA NTTデータ 先端技術株式会社	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 International Certificate Authority of Management System	国際マネジメントシステム認証機構株式会社
net one	ネットワンシステムズ株式会社
bsi.	BSI グループジャパン株式会社
FUJITSU	富士通株式会社
株式会社ブロードバンドセキュリティ BBSec	株式会社ブロードバンドセキュリティ

【日本語版の更新】

2019 年 2 月　誤字・誤記を訂正。要件の付録 A2.2 を削除。