



Payment Card Industry (PCI)
データセキュリティ基準
**自己問診 (Self-Assessment
Questionnaire) C および準拠証明書**

ペイメントアプリケーションシステムがインターネットに接続されている加盟店（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 3.2.1

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 , © 2006-2017 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 , © 2006-2017 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	他の SAQ にあわせてバージョン採番を更新。
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 から要件 8, 9, 付録 A2 が追加されました。
2017 年 1 月	3.2	1.1	2016 年 4 月更新版の要件明確化のために改訂。 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 8.1.6 および 11.3.4 のチェックボックスを修正。
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

文書の変更	i
開始する前に	iv
PCI DSS 自己評価の記入方法	iv
自己問診 (SAQ) について.....	v
必要なテスト	v
自己問診の記入方法	vi
特定の要件が適用されない場合	vi
法的例外	vi
セクション 1: 評価の情報.....	1
セクション 2: 自己問診 C.....	5
安全なネットワークとシステムの構築と維持	5
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.....	5
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.....	7
カード会員データの保護.....	13
要件 3: 保存されるカード会員データを保護する.....	13
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.....	15
脆弱性管理プログラムの維持.....	17
要件 5: すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する.....	17
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.....	19
強力なアクセス制御手法の導入.....	21
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	21
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.....	22
要件 9: カード会員データへの物理アクセスを制限する	26
ネットワークの定期的な監視およびテスト	31
要件 10: ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する.....	31
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	34
情報セキュリティポリシーの維持	40
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	40
付録 A: 追加の PCI DSS 要件.....	44

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.....	44
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.....	44
付録 A3:	指定事業者向け追加検証 (DESV).....	45
付録 B:	代替コントロールワークシート	46
付録 C:	適用されない理由についての説明.....	47
セクション 3:	検証と証明の詳細	48

開始する前に

SAQ C は、ペイメントアプリケーションシステム（POS システムなど）がインターネットに接続されている（DSL、ケーブルモデムなどを經由）加盟店に適用される要件を示すために作成されました。

SAQ C の加盟店は、POS（販売時点情報管理）システムまたはインターネットに接続されているその他のペイメントアプリケーションシステム経由でカード会員データを処理しますが、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。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）加盟店のいずれかとなります。

SAQ C 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。

- あなたの会社には、ペイメントアプリケーションシステムとインターネット接続が、同じデバイス上または同じローカルエリアネットワーク（LAN）上（あるいはその両方）にあります。
- ペイメントアプリケーションシステム/インターネットデバイスは、環境内の他のシステムには接続されていません（これは、ペイメントアプリケーションシステム/インターネットデバイス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。
- POS 環境の物理場所は他の敷地や場所に接続されておらず、LAN は単一場所用です。
- 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。
 - 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 C)
 - 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。

*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（つまり決済アプリケーションシステム）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等のプロセッ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。

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 <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

SAQ C 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（要件 **1.2.3**、**2.1.1**、**4.1.1** など）。要件 **11.1**（承認されていないワイヤレスアクセスポイントを識別するプロセスの使用）は、ワイヤレス技術がネットワーク内で使用されていない場合でも回答する必要があります。プロセスは知らないうちに追加された可能性がある不正デバイスを検出するためです。

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)

- 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？

- 通信販売 (MO/TO)
- 電子商取引
- 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？

- 通信販売 (MO/TO)
- 電子商取引
- 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。

施設の種類の種類	該当する施設の数の数	施設の拠点(市区町村、国)
例: 小売店 Retail outlets	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な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

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。)	<input type="checkbox"/> 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？	<input type="checkbox"/> はい <input type="checkbox"/> 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) ?	<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 C 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、同じデバイスまたは同じローカルエリアネットワーク (LAN) 上で、ペイメントアプリケーションシステムおよびインターネット接続を所有している。
<input type="checkbox"/>	ペイメントアプリケーションシステム/インターネットデバイスは、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。
<input type="checkbox"/>	POS 環境の物理的な拠点は、その他の環境または拠点に接続されておらず、LAN は 1 つの拠点に対してのみ存在する。
<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 C

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
1.2 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を、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?	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(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?	<ul style="list-style-type: none"> 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 	<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
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？	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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？					
1.3.4	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？	<ul style="list-style-type: none"> ファイアウォールおよびルータ構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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？	<ul style="list-style-type: none"> ファイアウォールおよびルータ構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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? <i>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、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。</i>	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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?	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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?	<ul style="list-style-type: none"> 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 	<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
(c) アクセスポイントのデフォルトのパスワード/パスワードフレーズがインストール時に変更されていますか?	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 担当者のインタビュー システム構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(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?	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(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)	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2 (a) すべてのシステムコンポーネントについて構成基準が作成され、業界で認知されたシステム強化基準と一致していますか? <i>業界で認知されたシステム強化基準のソースには、SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS) が含まれますが、これらに限定されません。</i>	<ul style="list-style-type: none"> システム構成基準のレビュー 業界で認知された強化基準のレビュー 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"/>
(b) システム構成基準が、新たな脆弱性問題が見つかったときに、要件 6.1 で定義されているように更新されていますか?	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) 新しいシステムを構成する際に、システム構成基準が適用されていますか?	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 担当者のインタビュー 	<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
(d) システム構成基準に以下がすべて含まれていますか？ <ul style="list-style-type: none"> すべてのベンダ提供デフォルト値を変更し、不要なデフォルトアカウントを削除しているか？ 同じサーバに異なったセキュリティレベルを必要とする機能が共存しないように、1つのサーバには、主要機能を1つだけ実装しているか？ システムの機能に必要なサービス、プロトコル、デーモンなどのみを有効にしていますか？ 安全でないと見なされている必要なサービス、プロトコル、またはデーモンに追加のセキュリティ機能を実装していますか？ システムのセキュリティパラメータが、悪用を防ぐように構成されていますか？ スクリプト、ドライバ、機能、サブシステム、ファイルシステム、不要な Web サーバなど、不要な機能をすべて削除していますか？ 	<ul style="list-style-type: none"> システム構成基準のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1 (a) 同じサーバに異なったセキュリティレベルを必要とする機能が共存しないように、1つのサーバには、主要機能を1つだけ実装していますか？ 例えば、Web サーバ、データベースサーバ、および DNS は別々のサーバに実装する必要がある。	<ul style="list-style-type: none"> システム構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) 仮想化技術が使用されている場合は、1つの仮想システムコンポーネントまたはデバイスには、主要機能が1つだけ実装されていますか？	<ul style="list-style-type: none"> システム構成の調査 	<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
2.2.2	(a) システムの機能に必要なサービス、プロトコル、デーモンなどのみが、有効になっていますか（デバイスの特定機能を実行するのに直接必要でないサービスおよびプロトコルが無効になっている）？	<ul style="list-style-type: none"> 構成基準のレビュー システム構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 有効になっているが安全でないサービス、デーモン、プロトコルを特定し、それぞれ文書化された構成基準に従って正当化されていることを確認しましたか？	<ul style="list-style-type: none"> 構成基準のレビュー 担当者のインタビュー 構成設定の調査 有効なサービスと文書化された正当性の比較 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	安全でないとみなされている必要なサービス、プロトコル、またはデーモンに追加のセキュリティ機能は実装されていますか？	<ul style="list-style-type: none"> 構成基準のレビュー 構成設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	(a) システムコンポーネントを構成するシステム管理者または担当者（あるいはその両方）は、それらのコンポーネントの一般的なセキュリティパラメータ設定に関する知識がありますか？	<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"/>
	(b) システム構成基準に一般的なシステムセキュリティパラメータ設定が含まれていますか？	<ul style="list-style-type: none"> システム構成基準のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) セキュリティパラメータは、システムコンポーネントに適切に設定されていますか？	<ul style="list-style-type: none"> システムコンポーネントの調査 セキュリティパラメータ設定の調査 設定とシステム構成基準の比較 	<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	
2.2.5	(a) スクリプト、ドライバ、機能、サブシステム、ファイルシステム、不要な Web サーバなど、不要な機能がすべて削除されていますか?	<ul style="list-style-type: none"> システムコンポーネントのセキュリティパラメータの調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 有効な機能が文書化され、安全な構成がサポートされていますか?	<ul style="list-style-type: none"> 文書のレビュー システムコンポーネントのセキュリティパラメータの調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) システムコンポーネントには文書化された機能のみがありますか?	<ul style="list-style-type: none"> 文書のレビュー システムコンポーネントのセキュリティパラメータの調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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?	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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?	<ul style="list-style-type: none"> システムコンポーネントの調査 管理者ログオンの観察 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) 使用テクノロジー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?	<ul style="list-style-type: none"> 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 	<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
2.5	ベンダデフォルトおよび他のセキュリティパラメータの管理に関するセキュリティポリシーと操作手順が以下の要件を満たしていますか？ <ul style="list-style-type: none"> ▪ 文書化されている ▪ 使用されている ▪ 影響を受ける関係者全員に知られている 	<ul style="list-style-type: none"> ▪ セキュリティポリシーおよび運用手順のレビュー ▪ 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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	<p>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?</p> <p>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。</p> <p>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。</p> <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 <p>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。</p>	<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	<p>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？</p> <p>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。</p>	<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
<p>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?</p> <p><i>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。</i></p>	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(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?</p>	<ul style="list-style-type: none"> 着信および発信伝送の観察 鍵および証明書の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(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?</p>	<ul style="list-style-type: none"> システム構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(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?</p>	<ul style="list-style-type: none"> ベンダ文書のレビュー システム構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(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?</p> <p><i>例えば、ブラウザベースの実装の場合：</i></p> <ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> システム構成の調査 	<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
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？	<ul style="list-style-type: none"> ▪ 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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"/>

脆弱性管理プログラムの維持

要件 5: すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する

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
5.1	悪意のあるソフトウェアの影響を受けやすいすべてのシステムにウイルス対策ソフトウェアが導入されていますか?	<ul style="list-style-type: none"> システム構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	ウイルス対策プログラムは、すべての既知のタイプの悪意のあるソフトウェア（ウイルス、トロイの木馬、ワーム、スパイウェア、アドウェア、ルートキットなど）に対して検知、駆除、保護が可能ですか?	<ul style="list-style-type: none"> ベンダ文書のレビュー システム構成の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	悪意あるソフトウェアの影響を受けにくいとみなされるこれらのシステムが継続して影響を受けないかどうかを確認するために、進化するマルウェアの脅威を特定し評価するための定期的な評価が実施されていますか?	<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"/>
5.2	すべてのウイルス対策メカニズムが以下のように維持されていますか?					
	(a) ウイルス対策ソフトウェアと定義が最新に保たれていますか?	<ul style="list-style-type: none"> ポリシーと手順の調査 マスターインストールを含むウイルス対策構成の調査 システムコンポーネントの調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 自動更新と定期スキャンは有効になっており、実行されていますか?	<ul style="list-style-type: none"> マスターインストールを含むウイルス対策構成の調査 システムコンポーネントの調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) すべてのウイルス対策メカニズムが監査ログを生成し、ログが PCI DSS 要件 10.7 に従って保持されていますか?	<ul style="list-style-type: none"> ウイルス対策構成の調査 ログ保管プロセスのレビュー 	<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
5.3	<p>すべてのウイルス対策メカニズムが</p> <ul style="list-style-type: none"> アクティブに実行されていますか? ユーザが無効にしたり、変更できないようになっていますか? <p>注: ウイルス対策ソリューションは、ケースバイケースで経営管理者により許可されたことを前提に、正当な技術上のニーズがある場合に限り、一時的に無効にすることができます。特定の目的でウイルス対策保護を無効にする必要がある場合、正式な許可を得る必要があります。ウイルス対策保護が無効になっている間、追加のセキュリティ手段が必要になる場合があります。</p>	<ul style="list-style-type: none"> ウイルス対策構成の調査 システムコンポーネントの調査 プロセスの観察 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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
<p>6.1</p> <p>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?</p> <ul style="list-style-type: none"> 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 <p>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。</p> <p>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。</p>	<ul style="list-style-type: none"> 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"/>

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
6.2	(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?	<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) 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。	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.6	大幅な変更の際は、すべての該当する PCI DSS 要件が全ての新しいまたは変更されたシステムやネットワークに実装され、必要に応じて文書が更新されていますか?	<ul style="list-style-type: none"> 変更管理文書の変更の追跡 変更管理文書の調査 担当者のインタビュー 影響のあるシステムまたはネットワークの観察 	<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 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	すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対してユーザー管理コントロールに関するポリシーと手順が定義されて実施されていますか?					
8.1.1	システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザに一意的 ID が割り当てられていますか?	<ul style="list-style-type: none"> パスワード手順のレビュー 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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?	<ul style="list-style-type: none"> 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"/>
8.1.6	(a) 最大 6 回の試行後にユーザ ID をロックアウトすることで、アクセス試行の繰り返しが制限されていますか?	<ul style="list-style-type: none"> パスワード手順のレビュー システム構成設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.7	ユーザアカウントがロックアウトされた場合のロックアウト期間は最低 30 分間、または管理者がユーザ ID を有効にするまでに設定されていますか?	<ul style="list-style-type: none"> パスワード手順のレビュー システム構成設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.8	セッションが 15 分を超えてアイドル状態の場合、端末またはセッションを再有効化するためにユーザに再認証（パスワードの再入力など）が要求されますか?	<ul style="list-style-type: none"> パスワード手順のレビュー システム構成設定の調査 	<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
8.2	<p>一意の ID の割り当てに加え、以下の 1 つ以上の方法を使用してすべてのユーザが認証されていますか?</p> <ul style="list-style-type: none"> ▪ ユーザが知っていること (パスワードやパスフレーズなど) ▪ トークンデバイスやスマートカードなど、ユーザが所有しているもの ▪ ユーザ自身を示すもの (生体認証など) 	<ul style="list-style-type: none"> ▪ パスワード手順のレビュー ▪ 認証プロセスの観察 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.3	<p>(a) ユーザーパスワードパラメータは、パスワード/パスフレーズが以下を満たすことが必要のように設定されていますか?</p> <ul style="list-style-type: none"> • パスワードに 7 文字以上が含まれる • 数字と英文字の両方を含む <p>あるいは、上記のパラメータに等しい複雑さと強度を持つパスワード/パスフレーズ</p>	パスワードパラメータを検証するためのシステム構成設定の調査	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.4	少なくとも 90 日ごとにユーザパスワードが変更されますか?	<ul style="list-style-type: none"> ▪ パスワード手順のレビュー ▪ システム構成設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.5	(a) ユーザが新しいパスワード/パスフレーズを設定する際、最後に使用した 4 つのパスワード/パスフレーズと異なるものを設定しなければなりませんか?	<ul style="list-style-type: none"> ▪ パスワード手順のレビュー ▪ システムコンポーネントのサンプル ▪ システム構成設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.6	初回およびリセット時のパスワード/パスフレーズがユーザごとに一意の値に設定され、初回使用后、直ちにそのパスワードを変更するよう要求していますか?	<ul style="list-style-type: none"> ▪ パスワード手順のレビュー ▪ システム構成設定の調査 ▪ セキュリティ担当者の観察 	<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
8.3	<p>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？</p> <p>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。</p>					
8.3.1	カード会員データ環境への管理者権限を持つ担当者の非コンソールアクセスに多要素認証が組み込まれていますか？	<ul style="list-style-type: none"> システム構成の調査 CDE への管理者のログインの観察 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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？	<ul style="list-style-type: none"> システム構成の調査 リモート接続担当者の観察 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.4	(a) 認証手順およびポリシーが文書化されて、すべてのユーザに伝達されていますか？	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 配布方法のレビュー 担当者のインタビュー ユーザのインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 認証手順とポリシーに以下が含まれていますか？	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー ユーザに提供される文書のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> 強力な認証情報を選択するためのガイダンス ユーザが自分の認証情報を保護する方法についてのガイダンス 前に使用していたパスワードを再使用しないという指示 パスワードが侵害された疑いがある場合にはパスワードを変更するという指示 					

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
<p>8.5</p> <p>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?</p> <ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>8.8</p> <p>識別と認証に関するセキュリティポリシーと操作手順が以下の要件を満たしていますか?</p> <ul style="list-style-type: none"> ▪ 文書化されている ▪ 使用されている ▪ 影響を受ける関係者全員に知られている 	<ul style="list-style-type: none"> ▪ セキュリティポリシーおよび運用手順の調査 ▪ 担当者のインタビュー 	<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
9.1	カード会員データ環境内のシステムへの物理アクセスを制限および監視するために、適切な施設入館管理が実施されていますか?	<ul style="list-style-type: none"> 物理アクセス制御の観察 担当者の観察 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.1	(a) ビデオカメラやアクセス管理メカニズム（あるいは両方）を用いて、機密エリアへの個々の物理アクセスを監視していますか? 注: 「機密エリア」とは、データセンタ、サーバールーム、またはカード会員データを保存するシステムが設置されているエリアのことです。これには、小売店のレジなど、POS 端末のみが存在する一般公開エリアは含まれません。	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 物理監視メカニズムの観察 セキュリティ機能の観察 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ビデオカメラやアクセス管理メカニズム（あるいは両方）が、改ざんまたは無効化から守られていますか?	<ul style="list-style-type: none"> プロセスの観察 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ビデオカメラやアクセス管理メカニズム（あるいは両方）から収集したデータをレビューして、他の監視事項と相互に関連付けていますか?	<ul style="list-style-type: none"> ポリシーおよび手順のレビュー 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"/>
	(d) ビデオカメラやアクセス管理メカニズム（あるいは両方）から収集したデータは、法律によって別途定められていない限り、少なくとも 3 カ月間保管していますか?	<ul style="list-style-type: none"> データ保管プロセスのレビュー データ保管の観察 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"/>

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ます。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。	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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。	<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? (b) 管理には、以下の内容が含まれていますか?	<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"/>
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"/>

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
9.7	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？					
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"> 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	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？ <i>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</i>					
	(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"/>

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
9.9.1 (a) デバイスのリストには以下が含まれていますか? <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"/>
(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"/>

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? <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"/>

ネットワークの定期的な監視およびテスト

要件 10: ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

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	
10.2	すべてのシステムコンポーネントに、以下のイベントを再現するための自動監査証跡が実装されていますか?					
10.2.2	ルート権限または管理権限を持つ個人によって行われたすべてのアクション	<ul style="list-style-type: none"> ■ 担当者のインタビュー ■ 監査ログの観察 ■ 監査ログ設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.4	無効な論理アクセス試行	<ul style="list-style-type: none"> ■ 担当者のインタビュー ■ 監査ログの観察 ■ 監査ログ設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.5	識別と認証メカニズムの使用および変更（新しいアカウントの作成、特権の昇格を含むがこれらに限定されない）、およびルートまたは管理者権限を有するアカウントの変更、追加、削除?	<ul style="list-style-type: none"> ■ 担当者のインタビュー ■ 監査ログの観察 ■ 監査ログ設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3	すべてのシステムコンポーネントについて、イベントごとに、以下の監査証跡エントリが記録されていますか?					
10.3.1	ユーザ識別	<ul style="list-style-type: none"> ■ 担当者のインタビュー ■ 監査ログの観察 ■ 監査ログ設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.2	イベントの種類	<ul style="list-style-type: none"> ■ 担当者のインタビュー ■ 監査ログの観察 ■ 監査ログ設定の調査 	<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
10.3.3	日付と時刻	<ul style="list-style-type: none"> ▪ 担当者のインタビュー ▪ 監査ログの観察 ▪ 監査ログ設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.4	成功または失敗を示す情報	<ul style="list-style-type: none"> ▪ 担当者のインタビュー ▪ 監査ログの観察 ▪ 監査ログ設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.5	イベントの発生元	<ul style="list-style-type: none"> ▪ 担当者のインタビュー ▪ 監査ログの観察 ▪ 監査ログ設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.6	影響を受けるデータ、システムコンポーネント、またはリソースの ID または名前	<ul style="list-style-type: none"> ▪ 担当者のインタビュー ▪ 監査ログの観察 ▪ 監査ログ設定の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6	<p>すべてのシステムコンポーネントのログとセキュリティイベントを調べ、異常や怪しい活動を特定していますか？</p> <p>注: 要件 10.6 に準拠するために、ログの収集、解析、および警告ツールを使用することができます。</p>					

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
10.6.1	(b) 手動またはログツールを用いて、以下を少なくとも毎日一度レビューするポリシーと手順が定義されていますか? <ul style="list-style-type: none"> すべてのセキュリティイベント CHD や SAD を保存、処理、または送信する、または CHD や SAD のセキュリティに影響を及ぼす可能性のあるすべてのシステムコンポーネントのログ すべての重要なシステムコンポーネントのログ すべてのサーバとセキュリティ機能を実行するシステムコンポーネント（ファイアウォール、侵入検出システム/侵入防止システム（IDS/IPS）、認証サーバ、電子商取引リダイレクションサーバなど）のログ 	<ul style="list-style-type: none"> セキュリティポリシーおよび手順のレビュー プロセスの観察 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.2	(b) すべての他のシステムコンポーネントのログを（手動またはログツールを用いて）会社のポリシーとリスク管理戦略に基づき定期的にレビューするためのポリシーと手順が定義されていますか?	<ul style="list-style-type: none"> セキュリティポリシーおよび手順のレビュー リスク評価文書のレビュー 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.3	(b) レビュープロセスで特定された例外と異常をフォローアップするためのポリシーと手順が定義されていますか?	<ul style="list-style-type: none"> セキュリティポリシーおよび手順のレビュー プロセスの観察 担当者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.7	(c) 監査ログは少なくとも1年間保持されていますか?	<ul style="list-style-type: none"> 担当者のインタビュー 監査ログの調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) 解析用に、少なくとも過去3カ月分のログが即座に利用可能な状態ですか?	<ul style="list-style-type: none"> 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"/>

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
<p>11.1 (a) 四半期ごとに、承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントを両方検出し、識別するためのプロセスが実装されていますか?</p> <p>注: プロセスで使用される方法には、ワイヤレスネットワークのスキャン、システムコンポーネントおよびインフラストラクチャの論理的/物理的な検査、ネットワークアクセス制御 (NAC)、ワイヤレス IDS/IPS が含まれますがこれらに限定されません。</p> <p>いずれの方法を使用する場合も、不正なデバイスを検出および識別できる機能を十分に備えている必要があります。</p>	<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"/>
<p>(b) その方法により、少なくとも以下を含む不正なワイヤレスアクセスポイントを検出および識別できますか?</p> <ul style="list-style-type: none"> システムコンポーネントに挿入された WLAN カード ワイヤレスアクセスポイントを作成するためにシステムコンポーネントに (USB などで) 接続したポータブルやモバイルデバイス、および ネットワークポートまたはネットワークデバイスに接続されたワイヤレスデバイス 	<ul style="list-style-type: none"> 手法の評価 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(c) 承認されている無線アクセスポイントと承認されていない無線アクセスポイントの識別に無線スキャンを利用する場合、無線スキャンを少なくとも四半期ごとにすべてのシステムコンポーネントおよび施設に対して、実施していますか?</p>	<ul style="list-style-type: none"> 最近のワイヤレススキャンからの出力結果の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(d) 自動監視 (ワイヤレス IDS/IPS や NAC など) が使用されている場合は、監視は担当者への警告が生成されるように構成されていますか?</p>	<ul style="list-style-type: none"> 構成設定の調査 	<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
11.1.1	文書化されている業務上の理由を含めて、承認されている無線アクセスポイントのインベントリを維持していますか?	<ul style="list-style-type: none"> インベントリ記録の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1.2	(a) インシデント対応計画に、不正なワイヤレスデバイスが検出された場合の対応が含まれていますか?	<ul style="list-style-type: none"> インシデント対応計画（要件 12.10 参照）の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 承認されていないワイヤレスアクセスポイントが見つかった場合の対処が行われていますか?	<ul style="list-style-type: none"> 責任者のインタビュー 最近のワイヤレススキャンおよび関連する対応の検査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2	<p>脆弱性スキャンを、少なくとも四半期に一度、およびネットワークでの大幅な変更後（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の変更、ファイアウォール規則の変更、製品のアップグレードなど）に、以下のように実施していますか?</p> <p>注: 四半期ごとのスキャンプロセスの複数のスキャンレポートをまとめて、すべてのシステムがスキャンされ、該当するすべての脆弱性に対処されたことを示すことができます。</p> <p>未修正の脆弱性が対処中であることを確認するために、追加の文書が要求される場合があります。評価者が 1) 最新のスキャン結果が合格スキャンであったこと、2) 事業体で四半期に一度のスキャンを要求するポリシーと手順が文書化されていること、および 3) スキャン結果で判明した脆弱性が再スキャンにおいて示されているとおりに修正されたことを確認した場合、初回の PCI DSS 準拠のために、四半期に一度のスキャンに 4 回合格することは要求されません。初回 PCI DSS レビュー以降は毎年、四半期ごとのスキャンに 4 回合格しなければなりません。</p>					

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	
11.2.1	(a) 内部の脆弱性スキャンは四半期ごとに実行されていますか?	■ スキャンレポートのレビュー	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) 四半期ごとの内部脆弱性スキャンのプロセスに、PCI DSS 要件 6.1 で定義されているすべての「高」脆弱性が解消されるまで、再スキャンを実施することが含まれていますか?	■ スキャンレポートのレビュー	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) 四半期ごとの内部スキャンが認定された内部リソースまたは認定された外部の第三者によって実行されていますか? また、該当する場合はテスターは組織的に独立した立場 (QSA または ASV である必要はない) にありますか?	■ 担当者のインタビュー	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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	<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
11.2.3 (a) 大幅な変更後、内部と外部のスキャンを実行していますか? 注: スキャンは有資格者が実施する必要があります。	<ul style="list-style-type: none"> 変更管理文書とスキャン報告書の調査と関連付け 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) スキャンプロセスには、以下の状態になるまで再スキャンの実行が含まれますか? <ul style="list-style-type: none"> 外部スキャンの場合、CVSS スコアで 4.0 以上の脆弱性がないこと 内部スキャンの場合、合格結果が取得されること、または PCI DSS 要件 6.1 で定義されたすべての「高リスク」脆弱性が解消されていること 	<ul style="list-style-type: none"> スキャンレポートのレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) スキャンが認定された内部リソースまたは認定された外部の第三者によって実行されていますか? また、該当する場合はテスターは組織的に独立した立場 (QSA または ASV である必要はない) にありますか?	<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"/>
11.3.4 CDE を他のネットワークから分離するためにセグメンテーションが使用されましたか?					
(a) すべてのセグメンテーション方法が効果的かつ運用可能で、カード会員データ環境内のシステムから PCIDSS 準拠範囲外のシステムを分離しているかを確認するための、ペネトレーションテスト手順を定義していますか?	<ul style="list-style-type: none"> セグメンテーション制御の調査 ペネトレーションテスト手法のレビュー 	<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
(b) ペネトレーションテストで、セグメンテーションコントロールが以下を満たしていることが確認できましたか？ <ul style="list-style-type: none"> 少なくとも年1回およびセグメンテーション制御/方法に何らかの変更を加えた後に実施されていますか？ 使用されているすべてのセグメンテーション制御/方法を対象とする セグメンテーション方法が運用可能で効果的であり、対象範囲内システムから対象範囲外システムを分離する 	<ul style="list-style-type: none"> 直近のペネトレーションテストの結果の調査 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) 認定された内部リソースまたは認定された外部の第三者によりテストが実施され、該当する場合は、テストの組織的な独立性が存在していますか？（QSA や ASV である必要はありません）	<ul style="list-style-type: none"> 責任者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5 (a) 変更検出メカニズム（ファイル整合性監視ツールなど）を導入して重要なシステムファイル、構成ファイル、またはコンテンツファイルの不正な変更（変更、追加および削除を含む）を担当者に警告していますか？ 監視する必要があるファイルの例は次のとおりです。 <ul style="list-style-type: none"> システム実行可能ファイル アプリケーション実行可能ファイル 構成およびパラメータファイル 一元的に保存されている、履歴またはアーカイブされた、ログおよび監査ファイル 事業者が指定した追加の重要ファイル（例えば、リスク評価その他の方法などで） 	<ul style="list-style-type: none"> システム設定および監視ファイルの観察 システム構成設定の調査 	<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) 変更検出メカニズムは重要なシステムファイル、構成ファイル、またはコンテンツファイルの不正な変更を警告し、重要なファイルの比較を少なくとも週に一度実行するように構成されていますか？ 注: 変更検出の目的において、通常重要なファイルは定期的に変更されないため、これらのファイルの変更は、システムの侵害や侵害のリスクの可能性を指し示します。ファイル整合性監視製品などの変更検出メカニズムは通常、関連するオペレーティングシステム用の重要なファイルがあらかじめ設定されています。カスタムアプリケーションなどのその他の重要なファイルは、事業体（加盟店、またはサービスプロバイダ）によって評価および定義されている必要があります。	<ul style="list-style-type: none"> システム設定および監視ファイルの観察 監視活動からの結果のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
11.5.1	変更検出ソリューションによって生成された警告に対応するプロセスを実装していますか？	<ul style="list-style-type: none"> システム構成設定の調査 	<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?	■ 情報セキュリティポリシーのレビュー	<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?	■ 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	<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?	■ 使用方法ポリシーのレビュー ■ 責任者のインタビュー	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.2	テクノロジーの使用に対する認証	■ 使用方法ポリシーのレビュー ■ 責任者のインタビュー	<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?	■ 使用方法ポリシーのレビュー ■ 責任者のインタビュー	<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?	■ 使用方法ポリシーのレビュー ■ 責任者のインタビュー	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.6	テクノロジーの許容されるネットワーク上の場所	■ 使用方法ポリシーのレビュー ■ 責任者のインタビュー	<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
12.3.8	非アクティブ状態が特定の期間続いた後のリモートアクセステクノロジーのセッションの自動切断	<ul style="list-style-type: none"> 使用方法ポリシーのレビュー 責任者のインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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ーをアクティブ化し、使用后直ちに非アクティブ化する	<ul style="list-style-type: none"> 使用方法ポリシーのレビュー 責任者のインタビュー 	<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？	<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 責任者のサンプルのインタビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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"/>

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	<p>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？</p> <p><i>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。</i></p>	<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"/>
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"/>

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	
12.10.1	(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"/>
	(b) 計画は、最低限、以下に対応していますか?					
	<ul style="list-style-type: none"> • ペイメントブランドへの通知を最低限含む、侵害が発生した場合の役割、責任、および伝達と連絡に関する戦略 	<ul style="list-style-type: none"> ▪ 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"/>
	<ul style="list-style-type: none"> • 具体的なインシデント対応手順 	<ul style="list-style-type: none"> ▪ 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"/>
	<ul style="list-style-type: none"> • ビジネスの復旧および継続手順 	<ul style="list-style-type: none"> ▪ 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"/>
	<ul style="list-style-type: none"> • データバックアッププロセス 	<ul style="list-style-type: none"> ▪ 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"/>
	<ul style="list-style-type: none"> • 侵害の報告に関する法的要件の分析 	<ul style="list-style-type: none"> ▪ 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"/>
	<ul style="list-style-type: none"> • すべての重要なシステムコンポーネントを対象とした対応 	<ul style="list-style-type: none"> ▪ 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"/>
	<ul style="list-style-type: none"> • ペイメントブランドによるインシデント対応手順の参照または包含 	<ul style="list-style-type: none"> ▪ 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: カードを取り扱う POS POI 端末の接続に、SSL / 初期の TLS を使用する事業者への PCI DSS 追加要件

PCI DSS 質問	必要なテスト	回答 (各質問に対して一つ回答を選んでください)			
		はい	はい、 CCW 付	いいえ	N/A
<p>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:</p> <ul style="list-style-type: none"> デバイスが、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? <p>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 端末の端末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せん。</p>	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS 質問	必要なテスト	回答 (各質問に対して一つ回答を選んでください)			
		はい	はい、 CCW 付	いいえ	N/A
<p>A2.2 SSL および/または 初期の TLS (A2.1 で許可されているもの以外) を使用しているすべての実装において、以下を含む正式なリスク低減策および移行計画書がありますか？</p> <ul style="list-style-type: none"> どのようなデータが伝送されるか、SSL/ 初期の TLS を使用および/またはサポートするシステムの種類および数、環境の種類を含む使用方法の説明 リスク評価結果およびリスク低減コントロール SSL / 初期の TLS に関連する新規脆弱性の監視プロセスの説明 新規環境に SSL / 初期の TLS が実装されていないことを確認するために実装されている変更コントロールプロセスの説明 2018 年 6 月 30 日より後でない移行完了日を含む移行プロジェクト計画の概要 	<ul style="list-style-type: none"> 文書化されたリスク低減策および移行計画のレビュー 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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。	

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 C(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 C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 に完全に準拠していることを示しました。						
<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の記入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"><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 C、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)

- 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、事業者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	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	
5	すべてのシステムをマルウェアから保護し、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更新する	<input type="checkbox"/>	<input type="checkbox"/>	
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	<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"/>	
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	<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"/>	
10	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	<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	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"/>	
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者向けの追加の PCI DSS 要件	<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