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

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

支払処理に第三者 Web サイトを使用することで部分的に外部委託している電子商取引加盟店

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
N/A	1.0		未使用
N/A	2.0		未使用
2014 年 2 月	3.0		カード会員データを受け取らないが支払取引の安全性および消費者のカード会員データを承認するページの完全性に影響を及ぼすような Web サイトを持つ電子商取引加盟店に適用される要件を対象とする新しい SAQ です。 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		要件 11.3 のエラーを修正するため更新。
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」としての参照を削除し、要件 11.3 の PCI DSS v2 報告書オプションを削除するよう更新。
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 1, 5, 6, 7, 8, 10,11 と付録 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。
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 A-EP は、カード会員データを受け取らないが支払取引の安全性および消費者のカード会員データを承認するページの完全性に影響を及ぼすような Web サイトを持つ電子商取引加盟店に適用される要件を対象とするために開発されました。

SAQ A-EP 加盟店は、電子商取引の支払チャネルを PCI DSS 認定の第三者に部分的に外部委託している電子商取引加盟店で、システムや店内ではカード会員データを電子的に保存、処理、伝送することはありません。

SAQ A-EP 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：

- あなたの会社は電子商取引のみを扱っています。
- 支払ページを除くカード会員データのすべての処理を PCI DSS 認定の第三者支払プロセサーに全面的に外部委託しています。
- あなたの会社の電子商取引 Web サイトはカード会員データを受信しませんが、消費者または消費者のカード会員データが PCI DSS 認定の第三者支払プロセサーにリダイレクトされる方法を制御します。
- 加盟店の Web サイトが第三者プロバイダによってホストされている場合、そのプロバイダが該当するすべての PCI DSS 要件を満たすことが検証されます（プロバイダが共有ホスティングプロバイダの場合は PCI DSS の付録 A を含む）。
- 消費者のブラウザに表示される支払ページのそれぞれの要素は加盟店の Web サイトまたは PCI DSS 準拠のサービスプロバイダからのものとします。
- あなたの会社は、システムまたは敷地内でカード会員データを電子的に保管、処理、伝送することなく、これらの機能を第三者に全面的に委託しています。
- あなたの会社は、第三者サービスプロバイダのカード会員データの保管、処理、伝送処理が、PCI DSS に準拠するものであることを確認しました。**また**
- あなたの会社にあるカード会員データの全ては紙（例えば計算書または領収書）でのみ保管され、これらの書類を電子的に受信することはありません。

この SAQ は電子商取引チャネルにのみ適用されます。

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。

***注:** この SAQ の目的において、「カード会員データ環境」を指す PCI DSS 要件は、加盟店のウェブサイトに適用されます。これは加盟店のウェブサイト自身がカード会員データを受け取らないとしても、ペイメントカードデータを伝送する方法について加盟店のウェブサイトが直接影響を与えるためです。*

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 A-EP)
   - 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

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

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:			
都道府県:		国:		郵便番号:	
URL:					

パート 2. 概要エグゼクティブサマリ

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 2b. 支払カードビジネスの説明

カード会員データをどのように、またどのような理由で保存、処理、伝送していますか？	

パート 2c.場所

PCI DSS レビューに含まれている施設の種類（例えば、小売店、事業所、データセンター、コールセンターなど）と場所の概要を挙げてください。

施設の種類	該当する施設の数	施設の拠点 (市区町村、国)
例: 小売店	*3*	*米国マサチューセッツ州ボストン*

パート 2d. ペイメントアプリケーション

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

対象組織が使用するペイメントアプリケーションについて次の情報を記入してください:

ペイメントアプリケーションの名前	バージョン番号	アプリケーションベンダ	アプリケーションは PA-DSS 登録済みですか	PA-DSS 登録の有効期限(該当する場合)
			☐ 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、Web サーバーなど、CDE 内の重要なシステムコンポーネント、および該当する場合に必要となる他の支払要素*	
あなたの会社は、PCI DSS 環境の範囲に影響するようなネットワークセグメンテーションを使用していますか？	☐ はい

（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 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、電子商取引トランザクションのみを許可している。
☐	すべてのカード会員データの処理は、ペイメントページを除き、PCI DSS 検証済みの第三者ペイメントプロセッサに完全にアウトソースされている。
☐	加盟店の電子商取引 Web サイトはカード会員データを受信しないが、消費者、またはそのカード会員データがPCI DSS検証済みの第三者ペイメントプロセッサにどうリダイレクトされるかを制御している。
☐	加盟店の Web サイトが第三者プロバイダによってホストされている場合、プロバイダは該当するすべての PCI DSS 要件に対して検証されている。(例えば、プロバイダが共有ホスティングプロバイダであれば、PCI DSS 付録 A を含む。)

☐	消費者のブラウザに提供されるペイメントページの各要素は、加盟店の Web サイトまたは PCI DSS 準拠サービスプロバイダによって生成される。
☐	加盟店は、加盟店システムまたは環境上のいかなるカード会員データも、電子的に保存、処理、伝送しないが、これらすべての機能の処理は完全に第三者に依存している。
☐	カード会員データの保存、処理、伝送を扱っている第三者の全てが、PCI DSS 準拠であることを確認している。
☐	加盟店は、すべてのカード会員データを紙面で保持し、これらの文書は電子的に受信されていない。

セクション 2:　自己問診 A-EP

注 : 以下の質問は、『PCI DSS 要件とテスト手順』文書内で定義された 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:　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	確立され実装されたファイアウォールおよびルーター構成基準には、以下が含まれていますか :					
1.1.1	すべてのネットワーク接続およびファイアウォール/ルーター構成への変更を承認およびテストする正式なプロセスがありますか?	▪ 文書化されたプロセスのレビュー ▪ 担当者のインタビュー ▪ ネットワーク構成の調査	☐	☐	☐	☐
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	☐	☐	☐	☐
1.1.3	(a) システムとネットワーク内でのカード会員データのフローを示す最新図がありますか?	▪ 最新のデータフロー図のレビュー ▪ 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?	▪ 担当者のインタビュー	☐	☐	☐	☐
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のファイアウォールが必要で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	☐	☐	☐	☐

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) 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、ポートを文書化したリストが含まれていますか?	▪ ファイアウォールおよびルータ構成基準のレビュー	☐	☐	☐	☐
	(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	☐	☐	☐	☐
1.1.7	(a) ファイアウォール/ルーター構成基準で、ファイアウォールおよびルーターのルールセットを少なくとも 6 カ月ごとにレビューするように要求していますか?	▪ ファイアウォールおよびルータ構成基準のレビュー	☐	☐	☐	☐
	(b) ファイアウォールおよびルーターのルールセットは少なくとも 6 カ月ごとにレビューされていますか?	▪ ファイアウォールレビューの記録の調査	☐	☐	☐	☐
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?	▪ 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
	(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	☐	☐	☐	☐
1.2.2	ルーター構成ファイルが不正アクセスから安全に保護されており、同期化されていますか–たとえば、実行（アクティブ）構成が起動構成（マシンの再起動時に使用）に一致していますか?	▪ ファイアウォールおよびルータ構成基準のレビュー ▪ ルータ構成ファイ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	☐	☐	☐	☐
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：					
1.3.1	DMZ は、誰でもアクセス可能な承認済みのサービス、プロトコル、ポートを提供するシステムコンポーネントにのみ着信トラフィックを制限するように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調査	☐	☐	☐	☐
1.3.2	着信インターネットトラフィックを DMZ 内の IP アドレスに制限していますか?	▪ ファイアウォールおよびルータ構成基準の調査	☐	☐	☐	☐
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基準の調査	☐	☐	☐	☐

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
1.3.4	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基準の調査	☐	☐	☐	☐
1.3.5	ネットワーク内へは、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基準の調査	☐	☐	☐	☐
1.3.7	(a) インターネットへのプライベート IP アドレスとルート情報の開示を防ぐ方法は実施されていますか? ***注:*** *IP アドレスを開示しない方法には、以下のものが含まれますが、これらに限定されません:* • *ネットワークアドレス変換 (NAT)* • *カード会員データを保持するサーバをプロキシサーバ/ファイアウォールの背後に配置する* • *登録されたアドレス指定を使用するプライベートネットワークのルートアドバタイズを削除するか、フィルタリングする。* • *登録されたアドレスの代わりに RFC 1918 アドレス空間を内部で使用する。*	▪ ファイアウォールおよびルータ構成基準の調査	☐	☐	☐	☐
	(b) プライベート IP アドレスとルート情報の外部の事業体への開示は承認されていませんか?	▪ ファイアウォールおよびルータ構成基準の調査 ▪ 担当者のインタビュー	☐	☐	☐	☐
1.4	(a) インターネットに直接接続するすべてのモバイルデバイスまたは従業員所有のデバイス（あるいはその両方）で、ネットワークの外側ではインターネットに接続され、またネットワークへのアクセスにも使用されるものに（従業員が使用するラップトップなど）、パーソナルファイアウォールソフトウェアがインストールされて、アクティブになっていますか?	▪ ポリシーおよび構成基準のレビュー ▪ モバイルおよび/または従業員所有デバイスの調査	☐	☐	☐	☐

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
	(b) パーソナルファイアウォールソフトウェアが所定の構成に設定され、アクティブに実行されており、モバイルデバイスや従業員所有のデバイスのユーザによって変更できないようになっていますか?	▪ ポリシーおよび構成基準のレビュー ▪ モバイルおよび/または従業員所有デバイスの調査	☐	☐	☐	☐
1.5	ファイアウォールを管理するためのセキュリティポリシーと操作手順は以下の要件を満たしていますか： ▪ 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	▪ 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	☐	☐	☐	☐

要件 2:　　システムパスワードおよび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		想定されるテスト	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、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 ▪ システム構成及びアカウント設定の調査 ▪ 担当者のインタビュー	☐	☐	☐	☐
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? *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）、Center for Internet Security（CIS）が含まれますが、これらに限定されません。*	▪ 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	☐	☐	☐	☐
	(b) システム構成基準が、新たな脆弱性の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?	▪ ポリシーおよび手順のレビュー ▪ 担当者のインタビュー	☐	☐	☐	☐
	(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?	▪ ポリシーおよび手順のレビュー ▪ 担当者のインタビュー	☐	☐	☐	☐

PCI DSS 質問		想定されるテスト	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 (続き)	(d) システム構成基準に以下がすべて含まれていますか： • 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安全性の高いサービス、プロトコル、デーモンなどのみを有効にしているか? • 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るか? • システムセキュリティのパラメータが、悪用を防ぐために設定されているか? • 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るか?	▪ システム構成基準のレビュー	☐	☐	☐	☐
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、DNS は別々のサーバに実装する必要があるなど。*	▪ システム構成の調査	☐	☐	☐	☐
	(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?	▪ システム構成の調査	☐	☐	☐	☐
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）?	▪ 構成基準のレビュー ▪ システム構成の調査	☐	☐	☐	☐

PCI DSS 質問		想定されるテスト	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) 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?	▪ 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	☐	☐	☐	☐
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?	▪ 構成基準のレビュー ▪ 構成設定の調査	☐	☐	☐	☐
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?	▪ 担当者のインタビュー	☐	☐	☐	☐
	(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?	▪ システム構成基準のレビュー	☐	☐	☐	☐
	(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?	▪ 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	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐
	(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?	▪ 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	☐	☐	☐	☐
	(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?	▪ 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	☐	☐	☐	☐

PCI DSS 質問		想定されるテスト	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
2.3	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	☐	☐	☐	☐
	(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?	▪ 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：					
3.2.2	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 ブロックを承認保存していませんか?	▪ 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	☐	☐	☐	☐

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
4.2	(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	☐	☐	☐	☐
4.3	カード会員データの伝送を暗号化するための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? ▪ 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	▪ 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	☐	☐	☐	☐

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?	▪ システム構成の調査	☐	☐	☐	☐
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?	▪ ベンダ文書のレビュー ▪ システム構成の調査	☐	☐	☐	☐
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？	▪ 担当者のインタビュー	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐
	(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?	▪ 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	☐	☐	☐	☐
	(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?	▪ ウイルス対策構成の調査 ▪ ログ保管プロセスのレビュー	☐	☐	☐	☐

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
5.3	すべてのウイルス対策メカニズムが ▪ 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? ***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。*	▪ 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	☐	☐	☐	☐
5.4	システムを保護するためのセキュリティポリシーと操作手順は以下の要件を満たしていますか? ▪ 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	▪ 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	☐	☐	☐	☐

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	☐	☐	☐	☐

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?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
	(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	☐	☐	☐	☐
6.4.5	(a) セキュリティパッチやソフトウェアの変更の実装に関連する変更管理手順が文書化されていますか? • 影響の文書化 • 適切な権限を持つ関係者による文書化された変更管理の承認 • 変更がシステムのセキュリティに悪影響を与えていないことを確認するための機能テスト • 回復手順	▪ 変更管理プロセスおよび手順のレビュー	☐	☐	☐	☐
	(b) すべての変更に対して以下が実行されていますか?					
6.4.5.1	影響の文書化	▪ 変更管理文書の変更の追跡 ▪ 変更管理文書の調査	☐	☐	☐	☐
6.4.5.2	適切な権限を持つ関係者による文書化された変更承認。	▪ 変更管理文書の変更の追跡 ▪ 変更管理文書の調査	☐	☐	☐	☐
6.4.5.3	(a) 変更がシステムのセキュリティに悪影響を与えていないことを確認するための機能テスト。	▪ 変更管理文書の変更の追跡 ▪ 変更管理文書の調査	☐	☐	☐	☐
	(b) カスタムコード変更の更新について、本番環境に導入される前の PCI DSS 要件 6.5 への準拠テスト	▪ 変更管理文書の変更の追跡 ▪ 変更管理文書の調査	☐	☐	☐	☐

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
6.4.5.4	回復手順	▪ 変更管理文書の変更の追跡 ▪ 変更管理文書の調査	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐
6.5	(a) ソフトウェア開発プロセスで一般的なコーディングの脆弱性は対処されていますか?	▪ ソフトウェア開発ポリシーおよび手順のレビュー	☐	☐	☐	☐
	(b) 開発者は、一般的コード化脆弱性を回避する方法を含めた安全なコーディング技法のトレーニングを受けており、メモリ内で機密データを取扱う方法を理解していますか?	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ トレーニング記録の調査	☐	☐	☐	☐
	(c) アプリケーションは、最小限以下の脆弱性からアプリケーションを保護する、安全なコーディングガイドラインに基づいて開発されていますか?					
6.5.1	インジェクションの不具合、特に SQL インジェクションがコーディング技法によって対処されていますか? ***注:*** *OS コマンドインジェクション、LDAP および Xpath のインジェクションの不具合、その他のインジェクションの不具合も考慮します。*	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
6.5.2	バッファオーバーフローの脆弱性がコーディング技法によって対処されていますか?	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
6.5.4	安全でない通信がコーディング技法で対処されていますか?	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 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
6.5.5	不適切なエラー処理がコーディング技法で対処されていますか?	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
6.5.6	脆弱性特定プロセス（PCI DSS 要件 6.1 で定義）で特定された、すべての「高」脆弱性がコーディング技法で対処されていますか?	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
Web アプリケーションおよびアプリケーションインターフェイス（内部または外部）の場合、以下の追加の脆弱性からアプリケーションを保護するための安全なコーディングガイドラインに基づいてアプリケーションが開発されていますか?						
6.5.7	クロスサイトスクリプティング（XSS）の脆弱性がコーディング技法によって対処されていますか?	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
6.5.8	不適切なアクセス制御（安全でないオブジェクトの直接参照、URL アクセス制限の失敗、ディレクトリトラバーサル、機能へのユーザアクセス制限の失敗など）がコーディング技法によって対処されていますか？	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
6.5.9	クロスサイトリクエスト偽造（CSRF）はコーディング技法で対処されていますか?	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
6.5.10	不完全な認証管理とセッション管理はコーディング技法によって対処されていますか?	▪ ソフトウェア開発ポリシーおよび手順の調査 ▪ 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
6.6	一般公開されている Web アプリケーションは、常時、新しい脅威と脆弱性に対処され、以下のいずれかの手法によって既知の攻撃から保護される必要があります。 ▪ 一般公開されている Web アプリケーションは、アプリケーションのセキュリティ脆弱性を手動/自動で評価するツールまたは手法によって、以下のようにレビューされる。 – 少なくとも年に一度実施する – 何らかの変更を加えた後 – アプリケーションのセキュリティを専門とする組織によって – 少なくとも要件 6.5 のすべての脆弱性が評価内に含まれている – 脆弱性がすべて修正されている – 修正後、アプリケーションが再評価されている *注: この評価は、要件 11.2 で実施する脆弱性スキャンとは異なります。* - または - ▪ Web ベースの攻撃を検知および回避するために、一般公開されている Web アプリケーションの手前に、Web アプリケーションファイアウォールをインストールしている。 – Web ベースの攻撃を検知および回避するために、一般公開されている Web アプリケーションの手前に、Web アプリケーションファイアウォールをインストールしている – アクティブに実行されており、最新状態である（該当する場合） – 監査ログを生成する – Web ベースの攻撃をブロックするか、アラートを生成し即時調査されるよう構成されている	▪ 文書化されたプロセスのレビュー ▪ 担当者のインタビュー ▪ アプリケーションセキュリティ評価の記録の調査 ▪ システム構成設定の調査	☐	☐	☐	☐

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
6.7	セキュアシステムとアプリケーションを開発・保守するためのセキュリティポリシーと操作手順は以下を満たしていますか? ▪ 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	▪ 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	☐	☐	☐	☐

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 ▪ 担当者のインタビュー ▪ 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	☐	☐	☐	☐
7.1.4	適切な権限を持つ関係者による承認を必要としており、その承認は文書化され、必須の特権を明記していますか?	▪ ユーザ ID のレビュー ▪ 文書化された承認の比較 ▪ 割り当て済の特権と文書化された承認の比較	☐	☐	☐	☐

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の ID が割り当てられていますか?	▪ パスワード手順のレビュー ▪ 担当者のインタビュー	☐	☐	☐	☐
8.1.2	ユーザ ID が、（指定された権限を含み）承認されたとおりの実装となるように、ユーザ ID、資格情報、およびその他の識別子オブジェクトの追加、削除、変更は管理されていますか?	▪ パスワード手順のレビュー ▪ 特権および通常ユーザ ID および承認に関わる調査 ▪ システム設定の観察	☐	☐	☐	☐
8.1.3	契約終了したユーザのアクセスは直ちに無効化または削除されていますか?	▪ パスワード手順のレビュー ▪ 不要なユーザアカウントの調査 ▪ 現在のアクセスリストのレビュー ▪ 物理認証デバイスの返却の観察	☐	☐	☐	☐
8.1.4	90 日以内に非アクティブなアカウントは削除または無効化されますか?	▪ パスワード手順のレビュー ▪ ユーザアカウントの観察	☐	☐	☐	☐
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	☐	☐	☐	☐

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
8.1.6	(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?	▪ パスワード手順のレビュー ▪ システム構成設定の調査	☐	☐	☐	☐
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?	▪ パスワード手順のレビュー ▪ システム構成設定の調査	☐	☐	☐	☐
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?	▪ パスワード手順のレビュー ▪ システム構成設定の調査	☐	☐	☐	☐
8.2	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? ▪ 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）	▪ パスワード手順のレビュー ▪ 認証プロセスの観察	☐	☐	☐	☐
8.2.1	(a) すべてのシステムコンポーネントで強力な暗号化を使用して、送信と保存中に認証情報（パスワード/パスフレーズなど）をすべて読み取り不能としていますか?	▪ パスワード手順のレビュー ▪ ベンダ文書のレビュー ▪ システム構成設定の調査 ▪ パスワードファイルの観察 ▪ データ伝送の観察	☐	☐	☐	☐
8.2.2	パスワードリセットの実施、新しいトークンの準備、新しいキーの生成など、認証情報を変更する前に、ユーザの身元を確認していますか?	▪ 認証手順のレビュー ▪ 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
8.2.3	(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なように設定されていますか? • 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 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	▪ 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	☐	☐	☐	☐
8.2.4	(a) 少なくとも 90 日ごとにユーザパスワードが変更されていますか?	▪ パスワード手順のレビュー ▪ システム構成設定の調査	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐
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、初回使用後、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?	▪ 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	☐	☐	☐	☐
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?	▪ システム構成の調査 ▪ CDE への管理者のロギングの観察	☐	☐	☐	☐

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
8.3.2	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	☐	☐	☐	☐
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?	▪ 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	☐	☐	☐	☐
	(b) 認証手順とポリシーに以下が含まれていますか? • 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	▪ 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	☐	☐	☐	☐
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	☐	☐	☐	☐

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
8.6	他の認証メカニズムが使用されている場合（物理または論理セキュリティトークン、スマートカード、証明書など）、そのメカニズムの使用は次のように割り当てられていますか? ▪ 認証メカニズムは、個々のアカウントに割り当てなければならず、複数アカウントで共有することはできない ▪ 物理/論理制御により、意図されたアカウントのみがアクセスできるようにする必要がある	▪ ポリシーおよび手順のレビュー ▪ 担当者のインタビュー ▪ システム構成設定および/または物理制御の調査	☐	☐	☐	☐
8.8	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? ▪ 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	▪ 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	☐	☐	☐	☐

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?	▪ 物理アクセス制御の観察 ▪ 担当者の観察	☐	☐	☐	☐
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	☐	☐	☐	☐
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	☐	☐	☐	☐

PCI DSS 質問		必要なテスト	回答 *(各質問に対して 1 つ回答を選んでください)*			
			はい	はい、CCW 付	いいえ	N/A
9.8	(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	☐	☐	☐	☐

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
10.1	(a) システムコンポーネントに対する監査証跡が有効になっていてアクティブですか?	▪ プロセスの観察 ▪ システム管理者のインタビュー	☐	☐	☐	☐
	(b) システムコンポーネントへのアクセスが各ユーザにリンクされていますか?	▪ プロセスの観察 ▪ システム管理者のインタビュー	☐	☐	☐	☐
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	▪ 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	☐	☐	☐	☐
10.2.3	すべての監査証跡へのアクセス	▪ 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	☐	☐	☐	☐
10.2.4	無効な論理アクセス試行	▪ 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	☐	☐	☐	☐
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もつアカウントの変更、追加、削除のすべて	▪ 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	☐	☐	☐	☐
10.2.6	監査ログの初期化、停止、一時停止	▪ 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	☐	☐	☐	☐

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
10.2.7	システムレベルオブジェクトの作成および削除	▪ 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	☐	☐	☐	☐
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	▪ 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	☐	☐	☐	☐
10.3.2	イベントの種類	▪ 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	☐	☐	☐	☐
10.3.3	日付と時刻	▪ 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	☐	☐	☐	☐
10.3.4	成功または失敗を示す情報	▪ 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	☐	☐	☐	☐
10.3.5	イベントの発生元	▪ 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	☐	☐	☐	☐
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	▪ 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	☐	☐	☐	☐

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
10.4	すべての重要なシステムクロックおよび時間は時刻同期技術を使用して同期されており、技術は最新に保たれていますか? **注:** ネットワークタイムプロトコル（NTP）は、時刻同期技術の一例です。	▪ 時刻設定基準およびプロセスのレビュー	☐	☐	☐	☐
10.4.1	重要なシステムには以下のプロセスが実装されており、正しい、一貫性のある時刻となっていますか?					
	(a) 指定した中央タイムサーバのみが、外部ソースから時刻信号を受信し、外部ソースからの時刻信号は国際原子時または UTC に基づいていますか?	▪ 時刻構成基準およびプロセスのレビュー ▪ 時刻関連システムパラメータの調査	☐	☐	☐	☐
	(b) 複数のタイムサーバがある場合、それらのタイムサーバが正確な時刻を保つためにお互いに通信し合っていますか?	▪ 時刻構成基準およびプロセスのレビュー ▪ 時刻関連システムパラメータの調査	☐	☐	☐	☐
	(c) システムは時刻情報を指定した中央タイムサーバからのみ受信していますか?	▪ 時刻構成基準およびプロセスのレビュー ▪ 時刻関連システムパラメータの調査	☐	☐	☐	☐
10.4.2	時刻データは以下のように保護されていますか? (a) 時刻データへのアクセスは、業務上時刻データへアクセスする必要のある担当者のみに制限されていますか?	▪ システム構成および時刻同期設定の調査	☐	☐	☐	☐
	(b) 重要なシステムの時刻設定の変更は、ログに記録され、監視され、レビューされていますか?	▪ システム構成および時刻同期設定とログの調査	☐	☐	☐	☐

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
10.4.3	時刻設定は業界で認知された時刻ソースから受信されていますか?（これは悪意のある個人が変更するのを防ぐためです。） （内部タイムサーバの不正使用を防ぐために）これらの更新を対称鍵で暗号化し、時刻更新が提供されるクライアントマシンの IP アドレスを指定するアクセス制御リストを作成することもできます。	▪ システム構成の調査	☐	☐	☐	☐
10.5	監査証跡は、変更できないようにセキュリティで保護されていますか?					
10.5.1	監査証跡の表示は、業務上の必要性を持つ人物のみに制限されていますか?	▪ システム管理者のインタビュー ▪ システム構成およびパーミッションの調査	☐	☐	☐	☐
10.5.2	アクセス制御メカニズム、物理的な分離、ネットワークの分離などによって、現在の監査証跡ファイルが不正な変更から保護されていますか?	▪ システム管理者のインタビュー ▪ システム構成およびパーミッションの調査	☐	☐	☐	☐
10.5.3	監査証跡ファイルは、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップされていますか?	▪ システム管理者のインタビュー ▪ システム構成およびパーミッションの調査	☐	☐	☐	☐
10.5.4	外部に公開されているテクノロジ（ワイヤレス、ファイアウォール、DNS、メールなど）のログが安全な一元管理される内部ログサーバまたは媒体に書き込まれていますか?	▪ システム管理者のインタビュー ▪ システム構成およびパーミッションの調査	☐	☐	☐	☐
10.5.5	ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにしていますか（ただし、新しいデータの追加は警告を発生させない）?	▪ 設定、監視対象ファイル、および監視活動の結果の調査	☐	☐	☐	☐

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
10.6	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? ***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。*					
10.6.1	(b) 手動またはログツールを用いて、以下のログとセキュリティイベントは少なくとも毎日レビューされていますか? • 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	▪ 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	☐	☐	☐	☐
10.6.2	(b) すべての他のシステムコンポーネントのログは（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されていますか?	▪ 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	☐	☐	☐	☐
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していますか?	▪ 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	☐	☐	☐	☐

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
10.7	(b) 監査ログは少なくとも 1 年間保持されていますか?	▪ セキュリティポリシーおよび手順のレビュー ▪ 担当者のインタビュー ▪ 監査ログの調査	☐	☐	☐	☐
	(c) 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?	▪ 担当者のインタビュー ▪ プロセスの観察	☐	☐	☐	☐

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	☐	☐	☐	☐
11.2.3	(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。*	▪ 変更管理文書とスキャン報告書の調査と関連付け	☐	☐	☐	☐
	(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? • 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	▪ スキャンレポートのレビュー	☐	☐	☐	☐

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
	(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?	▪ 担当者のインタビュー	☐	☐	☐	☐
11.3	ペネトレーションテスト方法には以下が含まれていますか? ▪ 業界承認のペネトレーションテスト方法（NIST SP800-115 など）に基づいている ▪ CDE 境界と重要システム全体を対象とした対応 ▪ ネットワークの内部と外部からのテスト ▪ セグメンテーションと範囲減少制御の有効性テスト ▪ アプリケーション層のペネトレーションテストは、少なくとも要件 6.5 に記載されている脆弱性を含める必要がある ▪ ネットワーク層のペネトレーションテストには、ネットワーク機能とオペレーティングシステムをサポートするコンポーネントを含める必要がある ▪ 過去 12 カ月にあった脅威と脆弱性のレビューと考慮 ▪ ペネトレーションテスト結果と修正実施結果の保持を指定	▪ ペネトレーションテスト手法の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
11.3.1	(a) 外部ペネトレーションテストが少なくとも年に一度および大幅なインフラストラクチャまたは環境の変更（オペレーティングシステムのアップグレード、環境へのサブネットワークの追加、環境への Web サーバの追加など）後に定義されている方法に従って実行されていますか?	▪ 実施対象範囲の調査 ▪ 直近の外部ペネトレーションテストの結果の調査	☐	☐	☐	☐

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
	(b) テスト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?	▪ 責任者のインタビュー	☐	☐	☐	☐
11.3.3	ペネトレーションテストで検出された悪用可能な脆弱性が修正され、テストが繰り返されて修正が確認されましたか?	▪ ペネトレーションテスト結果の調査	☐	☐	☐	☐
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？	▪ 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	☐	☐	☐	☐
	(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? • 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	▪ 直近のペネトレーションテストの結果の調査	☐	☐	☐	☐
	(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、テスター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）	▪ 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
11.4	(a) 侵入を検出/防止するための侵入検出/侵入防止技法をネットワークに組み込んで、すべてのトラフィックを監視していますか? • カード会員データ環境の境界、および • カード会員データ環境の重要なポイント	▪ システム構成の調査 ▪ ネットワーク図の調査	☐	☐	☐	☐
	(b) 侵入検出/侵入防止技法が侵害の疑いを関係者に警告するように設定されていますか?	▪ システム構成の調査 ▪ 責任者のインタビュー	☐	☐	☐	☐
	(c) すべての侵入検知および防止エンジン、ベースライン、シグネチャは最新状態に保たれていますか?	▪ IDS/IPS 構成の調査 ▪ ベンダ文書の調査	☐	☐	☐	☐
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。* • *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* • *事業体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）*	▪ 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	☐	☐	☐	☐

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
11.5 (続き)	(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:*** *変更検知の目的において、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。*	▪ 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	☐	☐	☐	☐
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?	▪ システム構成設定の調査	☐	☐	☐	☐

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	☐	☐	☐	☐
12.4	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?					

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
12.8.1	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	☐	☐	☐	☐
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	☐	☐	☐	☐

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?	▪ 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	☐	☐	☐	☐
	(b) 計画は、最低限、以下に対応していますか?					
	• 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	▪ インシデント対応計画手順のレビュー	☐	☐	☐	☐
	• 具体的なインシデント対応手順	▪ インシデント対応計画手順のレビュー	☐	☐	☐	☐
	• ビジネスの復旧および継続手順	▪ インシデント対応計画手順のレビュー	☐	☐	☐	☐
	• データバックアッププロセス	▪ インシデント対応計画手順のレビュー	☐	☐	☐	☐
	• 侵害の報告に関する法的要件の分析	▪ インシデント対応計画手順のレビュー	☐	☐	☐	☐
	• 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	▪ インシデント対応計画手順のレビュー	☐	☐	☐	☐
	• 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	▪ 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 を使用する事業体の追加 PCI DSS 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」にチェックが付けられている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 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.　特定されたリスク	元のコントロールがないことで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 A-EP(セクション2)に記載した結果に基づいています。

上記に記載されたSAQ A-EP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 A-EP、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）
		YES	NO	
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	☐	☐	
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	☐	☐	
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	☐	☐	
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	☐	☐	
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