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

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

カードを提示しない加盟店（すべてのカード会員データ機能を完全に外部委託）

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 2, 8 と 12 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。 PCI DSS 要件 2 と 8 に含まれる事の意図を明確にするために「開始する前に」へ注釈を追加。
2018 年 6 月	3.2.1	1.0	PCI DSS v3.2.1 にあわせて更新。変更の詳細については、「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。 PCI DSS v3.2.1 から要件 6.2 を追加。

目次

開始する前に

SAQ A は、カード会員データの取り扱いはすべて認証済みのサードパーティに外部委託しており、店内にはカード会員データの紙の計算書または領収書だけを保管している加盟店に適用される要件を示すために作成されました。

SAQ A の加盟店は、電子商取引/通信販売（カードを提示しない）加盟店で、カード会員データをシステムまたは店内に電子形式で保管、処理、伝送することはありません。

SAQ A 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。

- あなたの会社はカードを提示しない（電子商取引または通信販売による注文）取引のみを扱っています。
- カード会員データのすべての処理を PCI DSS 認定の第三者サービスプロバイダに全面的に外部委託しています。
- 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。

さらに、電子商取引チャネルでは、

- 消費者のブラウザに配信される支払ページの全ての要素は PCI DSS 認定の第三者サービスプロバイダからのみ直接送信します。

この SAQ は対面式の加盟店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。

注釈：この SAQ はコンピュータシステムの保護に対処する PCI DSS 要件（例えば要件 2 や 6, 8）で、顧客をウェブサイトから第三者にリダイレクトする e コマース加盟店、特にリダイレクトするメカニズムを配置している加盟店の Web サーバに適用されます。すべての業務を完全に委託している（加盟店から第三者へのリダイレクトメカニズムがない）ため、この SAQ の対象となるいかなるシステムも持たないメール/電話オーダー（MOTO）や e コマース加盟店については、これらの要件は“N/A（該当なし）”と判断されます。N/A の報告方法については、次ページ以降のガイダンスを参照してください。

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了させます。
   - 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)
   - セクション 3 (AOC パート 3 & 4) - 検証と準拠証明(AOC)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）*	• 範囲設定に関するガイダンス • 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。評価を始める前に、PCI DSS および他の付属文書をお読みください。

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とおり満たされました。
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 (該当する場合)

会社名:					
QSA リーダーの名前:			役職:		
電話番号:			電子メール:		
会社住所:			市区町村:		
都道府県:		国:		郵便番号	
URL:					

パート 2. 概要

パート 2a. 加盟店のビジネスの種類 (該当するものすべてにチェック)

☐ 小売	☐ 電気通信	☐食料雑貨およびスーパーマーケット
☐ 石油	☐電子商取引	☐通信販売
☐ その他 (具体的に記入してください):		

あなたの会社はどのような種類の支払チャネルを提供していますか？	この SAQ でカバーされている支払チャネルはどれですか？
☐ 通信販売(MO/TO)	☐ 通信販売(MO/TO)
☐ 電子商取引	☐ 電子商取引
☐ カード提示（対面式）	☐ カード提示（対面式）

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

パート 2b. 支払カードビジネスの説明

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

パート 2c. 場所

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

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

パート 2d. ペイメントアプリケーション

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

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

ペイメントアプリケーションの名前	バージョン番号	アプリケーションベンダ	アプリケーションは PA-DSS 登録済みですか載っていますか	PA-DSS 登録の有効期限 (該当する場合)
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	
			☐ はい ☐ いいえ	

パート 2e. 環境の説明

この評価の対象となる環境の概要を説明してください。 *例:* • *カード会員データ環境(CDE)との接続* • *POS デバイス、データベース、Web サーバーなど、CDE 内の重要なシステムコンポーネント、および該当する場合に必要となる他の支払要素*	
あなたの会社は、PCI DSS 環境の範囲に影響するようなネットワークセグメンテーションを使用していますか？ *（ネットワークセグメンテーションについては、PCI DSS の「ネットワークセグメンテ*	☐ はい ☐ いいえ

ーション」セクションを参照してください。）	

パート 2f. サードパーティサービスプロバイダ	
あなたの会社は認定インテグレータとリセラー（QIR）を使用していますか？	☐ 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、カードを提示しない（電子商取引またはメール/電話注文）取引のみを許可している。
☐	すべてのカード会員データのプロセシングは、PCI DSS 検証済みの第三者サービスプロバイダに完全にアウトソースされている。
☐	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。
☐	*電子商取引チャネルに対する追加として:*

	消費者のブラウザに提供されるペイメントページのすべての要素は、PCI DSS 検証済みの第三者サービスプロバイダだけから直接得たものである。

セクション 2:　自己問診 A

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 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 ▪ システム構成およびアカウント設定の調査 ▪ 担当者のインタビュー	☐	☐	☐	☐

脆弱性管理プログラムを維持する

***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		期待されるテスト	回答 *(各質問に対して 1 つ回答を選んで下さい)*			
			Yes	Yes with CCW	No	N/A
6.2	(c) ベンダーが提供する、適用可能なセキュリティパッチをインストールすることで、すべてのシステムコンポーネントとソフトウェアが、既知の脆弱性から保護されていますか?	▪ ポリシーと手順を調べる	☐	☐	☐	☐
	(d) 重要なセキュリティパッチは、リリース後 1 ヶ月以内にインストールされていますか?	▪ ポリシーと手順を調べる ▪ システムコンポーネントを調べる. ▪ インストールされているセキュリティパッチの一覧を、最新のベンダーパッチリストと比較する	☐	☐	☐	☐

強力なアクセス制御手法の導入

***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		期待されるテスト	回答 *(各質問に対して 1 つ回答を選んで下さい)*			
			はい	はい、CCW 付	いいえ	N/A
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	☐	☐	☐	☐

PCI DSS 質問		期待されるテスト	回答 *(各質問に対して 1 つ回答を選んで下さい)*			
			はい	はい、CCW 付	いいえ	N/A
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	☐	☐	☐	☐
8.2	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	☐	☐	☐	☐
8.2.3	(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システム構成設定の調査	☐	☐	☐	☐
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。 ▪ システムコンポーネントの管理に共有および汎用ユーザ ID が使用されていない	▪ ポリシーおよび手順のレビュー ▪ ユーザ ID 一覧の調査 ▪ 担当者のインタビュー	☐	☐	☐	☐

要件 9: カード会員データへの物理アクセスを制限する

PCI DSS 質問		期待されるテスト	回答 *(各質問に対して 1 つ回答を選んで下さい)*			
			はい	はい、CCW 付	いいえ	N/A
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。*	▪ 物理セキュリティメディアの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と手順のレビュー ▪ 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 ▪ メディア廃棄証明ログおよび文書の調査	☐	☐	☐	☐
9.7	媒体の保存およびアクセスに関して、厳格な管理が維持されていますか?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
9.8	(a) ビジネスまたは法律上の理由で不要になった場合、媒体はすべて破棄されていますか?	▪ 定期的なメディアの廃棄ポリシーおよび手順のレビュー	☐	☐	☐	☐
	(c) 破棄は、以下の方法によって行われていますか：					

PCI DSS 質問		期待されるテスト	回答 *(各質問に対して 1 つ回答を選んで下さい)*			
			はい	はい、 CCW 付	いいえ	N/A
9.8.1	(a) ハードコピー資料は、カード会員データを再現できないように、クロスカット裁断、焼却、またはパルプ状に溶解していますか?	▪ 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	☐	☐	☐	☐
	(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	☐	☐	☐	☐

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、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、および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
12.8	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し得るサービスプロバイダを管理するポリシーと手順が以下の通り整備および実施されていますか：					
12.8.1	提供されるサービスの詳細を含むサービスプロバイダのリストが整備されていますか?	▪ ポリシーと手順のレビュー ▪ 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の所有する、または顧客に委託されて保管、処理、伝送する、あるいは顧客のカード会員データ環境の安全に影響を及ぼすような、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同意した、書面での契約が維持されていますか? ***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 ▪ ポリシーと手順のレビュー	☐	☐	☐	☐
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 ▪ ポリシーと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
12.8.4	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 ▪ ポリシーと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 ▪ ポリシーと手順と補足文書のレビュー	☐	☐	☐	☐
12.10.1	(a) システム侵害が発生した場合に実施されるインシデント対応計画が作成されていますか?	▪ インシデント対応計画のレビュー ▪ インシデント対応計画手順のレビュー	☐	☐	☐	☐

付録 A:　　追加の PCI DSS 要件

付録 A1:　　共有ホスティングプロバイダ向けの PCI DSS 追加要件

この付録は加盟店評価では使用されません。

付録 A2:　　カードを取り扱う POS POI 端末の接続に、SSL / 初期の TLS を使用する事業体への PCI DSS 追加要件

この付録は自己問診 A の加盟店評価では使用されません。

付録 A3:　　指定事業体向け追加検証 (DESV)

この付録はペイメントブランドまたはアクワイアラーによって PCI DSS 既存要件の追加検証が必要であると指定された事業体のみに適用されます。

この付録の検証を求められた事業体は、報告のために『DESV 追加報告テンプレートおよび追加準拠証明書』を使用する必要があり、提出手順について該当するペイメントブランドおよび/またはアクワイアラーへ相談する必要があります。

付録 B:　　代替コントロールワークシート

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

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

代替コントロールの使用に関する情報とワークシートの記入方法についてのガイダンスは、PCI DSS 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 A(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を完了し、すべての質問に対して肯定的に答えたため、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ないことを示しました。 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。*
☐	**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、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 3. PCI DSS検証 (続き)	
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. 非準拠状態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	
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	☐	☐	
6	安全なシステムとアプリケーションを開発し、維持する。	☐	☐	
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	☐	☐	
9	カード会員データへの物理アクセスを制限する	☐	☐	
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	☐	☐	

**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