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

自己問診 (Self-Assessment Questionnaire) P2PE および準拠証明書

PCI リストにある P2PE ソリューションハードウェア支払端末のみを使用する加盟店（カード会員データを電子形式で保存しない）

PCI DSS バージョン 3.2.1

2018 年 6 月

この文書について

この文書（「公式日本語訳」）は、https://www.pcisecuritystandards.org/document_library , © 2006-2018 PCI Security Standards Council, LLC (「審議会」)で入手可能な SAQ と記される文書の公式の日本語訳です。この公式日本語訳は、JCDSC（「団体」）の承認と支援により情報提供のみを目的として、審議会と団体間の契約に基づいて提供されるものです。この翻訳に関して、本文書に記述された仕様を実装する権利は認められません。そのような権利は、https://www.pcisecuritystandards.org/document_library で入手可能な使用許諾契約書の条項に同意することによってのみ確保されます。本文書の英語版は、https://www.pcisecuritystandards.org/document_library で入手できるもので、本文書の完全版であるとみなされます。不明瞭な点および日本語訳と英語版における不一致については英語版が優先され、日本語訳はいかなる目的であっても依拠することはできません。審議会も団体も、本文書に含まれるいかなる誤りや不明瞭さにも責任を負いません。

About this document

This document (the “Official Japanese Translation") is the official Japanese language translation of the document described as SAQ, available at https://www.pcisecuritystandards.org/document_library , © 2006-2018 PCI Security Standards Council, LLC (the “Council”). This Official Japanese Translation is provided with the approval and support of JCDSC (“the Company”), as an informational service only, under agreement between the Council and the Company. No rights to implement the specification(s) described in this document are granted in connection with this translation; such rights may only be secured by agreeing to the terms of the license agreement available at https://www.pcisecuritystandards.org/document_library . The English text version of this document is available at https://www.pcisecuritystandards.org/document_library and shall for all purposes be regarded as the definitive version of this document. To the extent of any ambiguities or inconsistencies between this version and such English text version of this document, the English text version shall control, and accordingly, this version shall not be relied upon for any purpose whatsoever. Neither the Council nor the Company assume any responsibility for any errors or ambiguities contained herein.

文書の変更

日付	PCI DSS バージョン	SAQ 版	説明
N/A	1.0		未使用
2012 年 5 月	2.0		PCI SSC にリストされている検証済み P2PE ソリューションの一部としてハードウェア端末のみを使用する加盟店用の SAQ P2PE-HW を作成します。 この SAQ は PCI DSS v2.0 用です。
2014 年 2 月	3.0		内容を PCI DSS v3.0 の要件とテスト手順に合わせて改訂し、追加の回答オプションを組み込む。
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。 加盟店によって使用される、HW/HW または HW/ハイブリッド P2PE ソリューションとして方式のいずれかがあるため、SAQ のタイトルから HW を削除した。
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」の参考を削除するため更新した。
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 P2PE ソリューションと P2PE 説明書 (PIM)の実装にカバーされている PCI DSS 要件 3.3.と 4.2 を削除。
2017 年 1 月	3.2	1.1	2016 年 4 月更新版にて削除された要件の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

加盟店の SAQ P2PE 対象基準

SAQ P2PE は、検証され PCI に登録された P2PE（ポイントツーポイント暗号化）ソリューションに含まれるハードウェア支払端末のみを介して、カード会員データを処理する加盟店へ適用される要件に対応するために作成されました。
SAQ P2PE加盟店は、どのコンピュータシステムの平文のカード会員データへもアクセスできず、ハードウェア支払端末を介して PCI SSC 認定の P2PE ソリューションからアカウントデータを入力することだけができます。SAQ P2PEの加盟店は、従来型（カードを提示する）加盟店、または通信販売（カードを提示しない）加盟店のいずれかです。例えば、通信販売加盟店が紙面か電話で受け取ったカード会員データを、検証済み P2PE ハードウェア装置のみに直接入力する場合は SAQ P2PE の対象となるでしょう。
SAQ P2PE 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。

- 全ての支払プロセスは PCI SSC によって承認され登録された、検証済み PCI P2PE ソリューションを介して行われます。
- アカウントデータの保存、処理、または伝送をする加盟店の環境内にある唯一のシステムは、検証済みで PCI のリストに掲載されている P2PE ソリューションと共に使用することを承認された、加盟店端末装置（POI）デバイスです。
- それ以外の方法でカード会員データを電子的に送受信は行いません。
- 既存の環境に電子的なカード会員データは保存していません。
- あなたの会社が保持するカード会員データは、すべて紙に印刷されたものです。(たとえば印刷された伝票や領収書など)。これらの書類は電子的に受領したものではありません。また
- あなたの会社は、P2PE ソリューションプロバイダ提供の *P2PE* 説明書 *(PIM)* に記載されているすべてのコントロールを実装しています。

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。

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 を識別します - 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』を参照してください。
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. PIM の全要素を実装したことを確認してください。
4. 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。
5. 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 P2PE)
    - 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）

6. SAQ および準拠証明書を、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 の主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 C 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　☐ 食料雑貨店およびスーパーマーケット

☐ 石油　☐ 通信販売(MOTO)　☐ その他 (具体的に記入してください):

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

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

パート 2. 概要 (続き)

パート 2b. 支払カードビジネスの説明

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

パート 2c. 場所

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

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

パート 2d. P2PE ソリューション

あなたの組織で使用している検証済み PCI P2PE ソリューションに関する情報を以下に提供してください。

P2PE ソリューションプロバイダ名	
P2PE ソリューション名	
PCI SSC リファレンス番号	
加盟店が使用する、リスト記載の P2PE 加盟店端末装置（PTS デバイス依存）：	

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ーション」セクションを参照してください。）*	☐ はい ☐ 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	
☐	すべてのペイメントプロセスは PCI SSC によって承認され、リストに載っている検証済み PCI P2PE ソリューションを介している。
☐	加盟店環境内にある、アカウントデータを保存、処理、伝送するシステムは、PCI のリストに載っている検証済み P2PE ソリューションとともに使用することが承認された加盟店端末装置のみである。
☐	加盟店はカード会員データを電子的に受信、伝送しない。
☐	加盟店は、加盟店環境内に、電子カード会員データの従来のストレージが存在しないことを確認している。
☐	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。
☐	加盟店は、P2PE ソリューションプロバイダによって提供された P2PE 説明書（PIM）のすべての制御を実装している。

セクション 2: 自己問診 P2PE

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。この SAQ P2PE では PCI DSS 要件のサブセットのみが提供されているため、これらの質問の番号付けは連続しない場合があります。*

自己問診の完了日:

カード会員データの保護

要件 3: *保存されるカード会員データを保護する*

注: *要件 3 は SAQ P2PE 加盟店が保持するプライマリアカウント番号（PAN）を含むアカウントデータの紙の記録（例えば、レシート、印刷されたレポートなど）のみに適用されます。*

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
3.1	データの保存と廃棄に関するポリシーと手順、およびプロセスは以下のとおり実装されていますか:					
	(a) 保存するデータ量と保存期間が、法律上、規制上、業務上必要な範囲に限定されていますか?	• データ保管および削除ポリシーと手順のレビュー ▪ 担当者のインタビュー	☐	☐	☐	☐
	(b) 法律上、規制上、または業務上、不要になったカード会員データを安全に削除するプロセスが定義され、実施されていますか?	• ポリシーおよび手順のレビュー • 担当者のインタビュー ▪ 削除メカニズムの調査	☐	☐	☐	☐
	(c) カード会員データの特定のデータ保存要件がありますか? *例えば、カード会員データは、X の期間、Y という業務上の理由で保存する必要がある。*	• ポリシーおよび手順のレビュー • 担当者のインタビュー • 保存要件の調査	☐	☐	☐	☐
	(d) 定義された保存要件を超えるカード会員データを特定して安全に廃棄する四半期ごとのプロセスがありますか?	• ポリシーおよび手順のレビュー • 担当者のインタビュー • 削除プロセスの観察	☐	☐	☐	☐

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
	(e) 保存されたカード会員データがすべて、データ保存ポリシーで定義された要件を満たしていますか?	▪ ファイルおよびシステム記録の調査	☐	☐	☐	☐
ガイダンス: *アカウントデータを含む紙媒体（レシート、紙媒体の報告書など）を保存している加盟店が、業務上、法律上、規則上の理由で必要な場合に限って保存しており、必要がなくなった際に破棄しているのであれば、要件 3.1 に対して「Yes」をチェックするものとします。* *加盟店がアカウントデータを含むいかなる紙媒体を保存および印刷していなければ、「N/A」の列にチェックを記入し、ワークシートの付録 C にある「適用されない理由についての説明」を完成させる必要があります。*						
3.2.2	すべての紙媒体の保管について、カード検証コードまたは値（3 桁または 4 桁のクレジットカードの表面または裏面に印字された番号）が承認後に保管されていませんか？	▪ 紙媒体データの調査	☐	☐	☐	☐
ガイダンス: *取引が行われている間、セキュリティコードを書き留めている加盟店において、取引完了直後に、（例えばシュレッダー等で）その紙媒体を安全に破棄しているか、もしくは、紙媒体が保存される前に、（例えば、マーカ等でブラックアウトする等で）コードを見えなくしている場合は、要件 3.2.2 に対して「Yes」にチェックを記入するものとします。* *クレジットカードに印刷されている 3 桁もしくは 4 桁のセキュリティコードを加盟店が要求しなければ、「N/A」の列にチェックを記入し、ワークシートの Appendix C にある「適用されない理由についての説明」を完成させる必要があります。*						
3.7	保存されているカード会員データ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	☐	☐	☐	☐
ガイダンス: *加盟店はアカウントデータの用紙を保管しているケースにおいて、加盟店が要件 3.1、要件 3.2.2、要件 3.3 に対して適切なポリシーと手順を持ち合わせている場合は、要件 3.7 は「Yes」にチェックを記入するものとします。* *このガイダンスは、継続的なカード会員データの安全な保存を管理するために次のセキュリティポリシーと操作手順を担当者が認識し、確認する際に役立てるものとします。*						

強力なアクセス制御手法の導入

要件 9:　　カード会員データへの物理アクセスを制限する

注: *プライマリアカウント番号（PAN）を含むアカウントデータのある紙の記録（例えば、レシート、印刷されたレポートなど）を保有する SAQ P2PE 加盟店のみに要件 9.5 および 9.8 が適用されます。*

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
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	☐	☐	☐	☐
9.8	(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?	▪ 定期的なメディア廃棄ポリシーと手順のレビュー ▪ 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?	▪ 定期的なメディア廃棄ポリシーと手順のレビュー ▪ ストレージコンテナのセキュリティの調査	☐	☐	☐	☐

ガイダンス: *加盟店がアカウントデータを含む紙媒体を安全に保存しているケース、例えば、施錠した引き出し、キャビネット、または金庫に格納し、ビジネスの目的上必要がなくなった際に破棄しているのであれば、要件 9.5 および 9.8 の「Yes」をチェックするものとします。*

加盟店はアカウントデータ含む紙媒体を保存していない場合は、「N/A」の列にチェックを記入し、ワークシートの付録 C にある「適用されない理由についての説明」を完成させる必要があります。

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
9.9	カードから直接物理的な読み取りを経由してペイメントカードデータをキャプチャするデバイスが改ざんおよび不正置換から保護されていますか? ***注:*** *この要件には、カード（カードのスワイプやディップ）によるトランザクションに使用されるカード読み取り装置も含まれる。この要件は、コンピュータのキーボードや POS のキーパッドのような手動キー入力コンポーネントには適用されません*					
	(a) ポリシーと手順はデバイスの一覧の維持を要求していますか?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
	(b) ポリシーと手順はデバイスを定期的に検査して改ざんや不正置換がないか調べることを要求していますか?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
	(c) ポリシーと手順は関係者にトレーニングを行い、怪しい行動を識別し、POS デバイスの改ざんや不正置換を報告できるようにすることを要求していますか?	▪ ポリシーおよび手順のレビュー	☐	☐	☐	☐
9.9.1	(b) デバイスのリストには以下が含まれていますか? • 装置のメーカと形式 • 装置の場所（例えば、装置が設置されている拠点や施設の住所） • 装置の連番や他の一意な識別番号	▪ デバイスの一覧の調査	☐	☐	☐	☐
	(c) リストは正確で最新になっていますか?	▪ デバイスとデバイス設置場所の観察と一覧の比較	☐	☐	☐	☐
	(d) 装置が追加、移動、廃棄された場合に装置のリストが更新されていますか?	▪ 担当者のインタビュー	☐	☐	☐	☐

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
9.9.2	(a) 改ざん（カードスキマーの取り付けなど）や不正置換（連番など装置の特性を調べて偽の装置に差し替えられていないことを確認する）を検出するために定期的に装置の表面を次のように検査していますか? ***注:*** *装置が改ざんされたり不正置換された兆候の例としては、予期していない付着物やケーブルが装置に差し込まれている、セキュリティラベルが無くなっていたり、変更されている、ケースが壊れていたり、色が変わっている、あるいは連番その他の外部マーキングが変更されているなどがあります。*	▪ 担当者のインタビュー ▪ 検査プロセスの観察と定義済プロセスとの比較	☐	☐	☐	☐
	(b) 関係者は装置を検査する手順を知っていますか?	▪ 担当者のインタビュー	☐	☐	☐	☐
9.9.3	関係者は装置の改ざんや不正置換の試みを認識できるようにトレーニングを受けていますか?					
	(a) POS のある場所の関係者用トレーニング資料には、以下のトレーニングが含まれていますか? • 第三者の修理・保守関係者を名乗っている者に POS 装置へのアクセスを許可する前に、身元を確認する • 検証なしで装置を設置、交換、返品しない • 装置の周辺での怪しい行動（知らない人が装置のプラグを抜いたり装置を開けたりする）に注意する • 怪しい行動や POS 装置が改ざんや不正置換された形跡がある場合には適切な関係者（マネージャーやセキュリティ関係者など）に報告する	▪ トレーニング資料のレビュー	☐	☐	☐	☐
	(b) POS 拠点の関係者はトレーニングを受けており、装置の改ざんや不正置換を検出し、報告する手順を知っていますか?	▪ POS 拠点担当者のインタビュー	☐	☐	☐	☐

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
ガイダンス: *加盟店が要件 9.9.1 から要件 9.9.3 に対する適切なポリシーと手順を整備し、デバイスの最新のリストを維持し、デバイスの定期的な調査を行い、さらにデバイスの改ざんや置換を検出するには何を探せばよいかについて従業員を訓練している場合は、要件 9.9 に対し「Yes」をチェックするものとします。。*						
9.10	保存されているカード会員データへの物理アクセスを制限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調査 ▪ 担当者のインタビュー	☐	☐	☐	☐
ガイダンス: *自身の環境に該当する要件 9.5、9.8、9.9 に対する適切なポリシーと手順を加盟店が保持している場合、要件 9.10 の「Yes」をチェックするものとします。このガイダンスは、次のセキュリティポリシーと文書化された有効な手順を認識し、遵守していることを担当者に確認する際に役立てるものとします。*						

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 は、加盟店が従業員向けの情報セキュリティポリシーをもつ必要があることを規定していますが、これらのポリシーは、加盟店業務の規模や複雑さに基づく必要性に応じて、単純または複雑になっても構いません。ポリシー文書は、支払い端末、カード会員データを含む紙文書などを保護する責任を認識するように、すべての担当者に提供されている必要があります。加盟店に従業員がいない場合、加盟店は店舗内のセキュリティに対する責任を理解し、それを認識することが期待されます。

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	☐	☐	☐	☐
ガイダンス: *加盟店の運営規模および複雑性が考慮されたセキュリティポリシを加盟店が保持している場合、またそのポリシーが年 1 回レビューされ、必要に応じて更新されている場合は、要件 12.1 に対して「Yes」と記入するものとします。例えば、ポリシーは、P2PE 取扱説明書（PIM）に沿って、決済デバイスや店舗をいかに保護するか、緊急時に誰に連絡をするかを網羅している、簡潔なドキュメントになりえます。*						
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	☐	☐	☐	☐
ガイダンス: *加盟店の運営規模および複雑性に応じて、すべての担当者に対して基本的なセキュリティに関する責任をセキュリティポリシーに定義している場合、要件 12.4 を「Yes」と回答するものとします。例えば、管理者/所有者に期待される責任や従業員に期待される責任のように、セキュリティに対する責任は、従業員の職位による基本的な責任に応じて定義することができます。*						
12.5	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	☐	☐	☐	☐
ガイダンス: *要件 12.9 に対し、インシデントレスポンスおよびエスカレーション計画の責任者を指定している場合、要件 12.5.3 を「Yes」と回答するものとします。*						

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
12.6	(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	☐	☐	☐	☐
ガイダンス: *加盟店の運営規模および複雑性を考慮した適切なセキュリティ啓発プログラムを保有している場合、要件 12.6 を「Yes」と回答するものとします。例えば、オフィス内の掲示物や全従業員に対して定期的に送信されるメールでも、簡潔なセキュリティ啓発プログラムとなりえます。啓発プログラムのメッセージの例として、ドアや保管庫の施錠方法、決済端末が改ざんされたかどうかの見分け方、およびハードウェア決済端末の修理に来た担当者が正当な人物かの見極め方など、すべての従業員が従うべきセキュリティ上のヒントの記述が含まれます。*						
12.8	カード会員データを共有するか、カード会員データのセキュリティに影響を与えるサービスプロバイダを管理するポリシーと手順が以下の通り整備および実施されていますか?					
12.8.1	提供されるサービスの詳細を含むサービスプロバイダのリストが整備されていますか?	▪ ポリシーおよび手順のレビュー ▪ プロセスの観察 ▪ サービスプロバイダの一覧のレビュー	☐	☐	☐	☐
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 ▪ ポリシーと手順のレビュー	☐	☐	☐	☐

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
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	☐	☐	☐	☐
ガイダンス: *カード会員データをともに共有するサービスプロバイダーのリストおよび同意を加盟店は保持している場合、要件 12.8 は「Yes」と回答することとします。例えば、アカウントデータを含む紙媒体の文書保持企業をを加盟店が利用している場合、要件 12.8 に対し「Yes」と回答するものとします。*						
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	☐	☐	☐	☐
ガイダンス: *加盟店の運営規模および複雑性に応じて、緊急時に使用されるインシデント対応およびエスカレーション計画を加盟店が保持している場合、要件 12.10 を「Yes」と回答するものとします。例えば、バックオフィスに掲示される様々な状況の出来事が発生した際に誰に連絡すべきかをリスト化した簡潔なドキュメントで、正確性を年 1 回確認するレビューを行っているような計画であってもよいし、バックアップの「ホットサイト」施設と徹底した毎年のテストを含む、完全なインシデント対応計画に拡張することもできます。*						

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

この付録は SAQ P2PE 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I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 P2PE(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 P2PE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 P2PE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解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 P2PE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。*ペイメントブランドによっては、このセクションを必要としないこともあるため、パート 4 を完了する前にアクワイアラ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:** 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 P2PE、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 および本証明書のすべての情報は、自社の評価の結果を公正に示すものです。
☐	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。

パート 3a. 状態の確認（続き）	
☐	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。
☐	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どのシステムでも見つかりませんでした。[3]

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. ISA の確認（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、事業体は磁気ストライプデータ全体を保持することはできません。保持できる追跡データの要素は、アカウント番号、有効期限、名前のみです。

[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、署名欄またはその右側、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 桁の数値。

[3] カード提示の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の日付と、要件を満たすために講じるアクションの簡単な説明を記入する必要があります

ペイメントブランドによっては、このセクションを必要としないこともあるため、パート 4 を完了する前にアクワイアラまたはペイメントブランドに確認してください。

PCI DSS 要件*	要件の説明	PCI DSS 要件への準拠 (1 つ選んでください)		修正日とアクション (“いいえ” が選択されている要件すべて)
		はい	いいえ	
3	保存されるカード会員データを保護する	☐	☐	
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

【日本語版の更新】

2019 年 2 月　誤字･誤記を訂正。