
# ペイメントカード業界（PCI）
# データセキュリティ基準
# 自己問診

---

## 手順およびガイドライン

バージョン **3.2.1**

2018 年 6 月

# 文書更新履歴

| 日付 | バージョン | 説明 |
|---|---|---|
| 2008 年 10 月 1 日 | 1.2 | 内容を新しい PCI DSS v1.2 に合わせて改訂、およびオリジナルの v1.1 以降に加えられた若干の変更を追加。 |
| 2010 年 10 月 28 日 | 2.0 | 新しい PCI DSS v2.0 に合わせて内容を改訂、および SAQ 環境タイプと適格性規準を明確化。<br>Web ベースの仮想端末の加盟店向けに SAQ C-VT を追加。 |
| 2012 年 6 月 | 2.1 | 検証済みおよび PCI SSC リストの PCI ポイントツーポイント暗号化（P2PE）ソリューションに含まれるハードウェア支払端末でのみカード会員データを処理する加盟店向けに SAQ P2PE-HW を追加。<br>この文書は PCI DSS バージョン 2.0 で使用するためのものです。 |
| 2015 年 4 月 | 3.1 | 内容を PCI DSS v3.1 に合わせて改訂（SAQ A-EP および B-IP の追加を含む）、および既存の SAQ の適格性規準を明確化。 |
| 2016 年 5 月 | 3.2 | PCI DSS v3.2 に合わせて改訂し、既存の SAQ の適格性規準を明確化するために更新。 |
| 2018 年 6 月 | 3.2.1 | PCI DSS v3.2.1 に合わせて改訂するための小規模な更新。 |

*免責事項：本文書の英語版は、PCISSC ウェブサイト上で利用可能になっており、全ての目的において、これらの文書の正規版と見做される。本記述と英語版記述との間に曖昧もしくは不一致がある限りにおいては該当部分に相当する英語版が優先される。*

# 目次

**文書更新履歴** ..... **i**

**この文書について** ..... **1**

**PCI DSS の自己問診：すべてがどのように整合するか** ..... **2**

**SAQ 概要** ..... **3**

**PCI DSS が重要な理由** ..... **4**

準拠とセキュリティの違いを理解する ..... 6

PCI DSS 準拠のための全般的なヒントと戦略 ..... 6

**組織に最適な SAQ および証明書の選択** ..... **10**

SAQ A – 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外部委託 ..... 12

SAQ A-EP – 部分的に外部委託 ペイメント処理にサードパーティの Web サイトを使用している電子商取引の加盟店 ..... 13

SAQ B – インプリントのみの加盟店、またはスタンドアローンのダイヤルアウト端末のみの加盟店。カード会員データを電子形式で保存しない ..... 14

SAQ B-IP – スタンドアローンの IP 接続されている PTS 加盟店端末装置（POI）を使用している加盟店、カード会員データを電子形式で保存しない ..... 15

SAQ C-VT – Web ベースの仮想端末の加盟店、カード会員データを電子形式で保存しない ..... 16

SAQ C – 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 ..... 18

SAQ P2PE – PCI SSC リストの P2PE ソリューションでハードウェア決済端末のみを 使用している加盟店、カード会員データを電子形式で保存しない ..... 19

加盟店向け SAQ D – SAQ の適用対象となるその他すべての加盟店 ..... 20

サービスプロバイダ向け SAQ D – SAQ の適用対象となるサービスプロバイダ ..... 20

**自分の環境に最も適している SAQ はどれか** ..... **21**

# この文書について

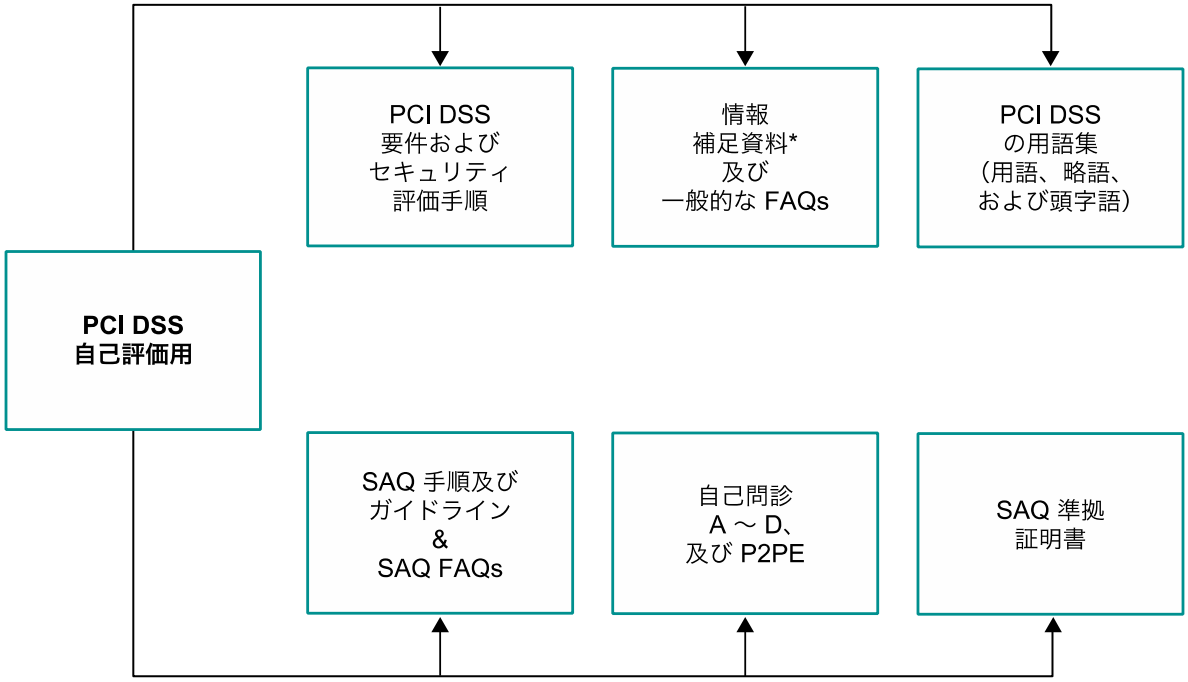
この文書は、加盟店およびサービスプロバイダが PCI データセキュリティ基準（PCI DSS）自己問診（SAQ：SelfAssessment Questionnaire）を理解する助けとなるように作成されました。このガイドラインと手引きに関する文書全体に目を通して、PCI DSS が組織にとって重要な理由、PCI DSS 準拠の検証を促進するために組織で使用できる戦略、および短いバージョンの SAQ のいずれかを完了する資格が組織にあるかどうかを理解してください。

## PCI DSS の自己問診：すべてがどのように整合するか

PCI DSS およびそのサポート文書は、カード会員データの安全な処理を確実にするための共通の業界ツールのセットです。基準は、セキュリティインシデントの防止、検出、対応を含め、堅牢なセキュリティプロセスを開発するための実用的なフレームワークです。セキュリティ侵害のリスクを少なくし、侵害が発生した場合の影響を軽減するには、カード会員データを保存、処理、または伝送するすべての事業体が準拠することが重要です。

次の図に、組織による PCI DSS 準拠および自己問診に役立つツールを示します。

これらの文書およびその他の関連文書は www.pcisecuritystandards.org に用意されています。




*注意：情報補足資料は補足情報とガイダンスのみを提供するものであり、PCI DSS の要件に取って代わるものではありません。

* 注：情報補足資料は補足情報とガイダンスのみを提供するものであり、PCI DSS の要件に取って代わるものではありません。

## SAQ 概要

*PCI DSS の自己問診*（SAQ）は、加盟店とサービスプロバイダによる PCI DSS 準拠の自己評価を支援することを目的とした検証ツールです。PCI DSS SAQ には、さまざまなシナリオに対応するための複数のバージョンがあります。この文書は、組織が最適な SAQ を判断するのを手助けするために作成されました。

PCI DSS SAQ は、それぞれのアクワイアラーまたはペイメントブランドによって PCI DSS の準拠に関するレポート（ROC）の提出が要求されない加盟店およびサービスプロバイダ向けの検証ツールです。PCI DSS 検証要件の詳細については、アクワイアラーまたはペイメントブランドにお問い合わせください。

PCI DSS SAQ は以下のコンポーネントで構成されます。

1. さまざまな環境に応じて、PCI DSS 要件に相互に関連する問診：この文書の「組織に最適な SAQ および証明書の選択」を参照してください。このセクションには、PCI DSS のテスト手順に基づく「期待されるテスト」の列も含まれます。
2. 準拠証明書：証明書には、適切な SAQ を完了する資格があることの宣言と、その後の PCI DSS 自己問診の結果が含まれます。

## PCI DSS が重要な理由

PCI セキュリティ基準審議会のメンバー（American Express、Discover、JCB、MasterCard、Visa）は、アカウントデータの侵害事例を継続的に監視しています。これらの侵害の監視は、非常に小規模な加盟店から非常に大規模な加盟店およびサービスプロバイダまで、あらゆる組織を対象とします。

ペイメントカードデータのセキュリティ違反およびそれに続く侵害は、影響を受ける組織に次のような広範にわたる影響を及ぼします。

1. 監督機関への通知要件
2. 評判の損失
3. 顧客の損失
4. 金銭的な責任の可能性（規制に関する料金と罰金など）
5. 訴訟

セキュリティ侵害のフォレンジック分析では PCI DSS コントロールが対応している共通のセキュリティ弱点が示されました。これは多くの場合、侵害の発生時に PCI DSS コントロールが行われていなかったか、不十分であったために悪用されました。PCI DSS は、セキュリティ侵害の可能性および侵害が発生した場合の影響を最小限に抑えることを目的に設計され、そのための詳細な要件が含まれています。

共通の PCI DSS コントロールの失敗に含まれる例を以下に示します（ただし、これらに限定されません）。

- 承認後のトラックデータなどの機密認証データ（SAD）の保存（要件 3.2）。侵害を受けた多くの事業体はシステムにこのデータが保存されていることに気付いていませんでした。
- POS システムが適切にインストールされていないことによる不適切なアクセス制御。これにより、ハッカーは POS ベンダ用のパスを経由して侵入します（要件 7.1、7.2、8.2、8.3）。
- システムのインストール時に既定のシステム設定とパスワードが変更されていない（要件 2.1）。
- システムのインストール時に不要なサービスや安全でないサービスが削除または修正されていない（要件 2.2.2 および 2.2.3）。
- SQL インジェクションやその他の脆弱性の原因となる不適切にコーディングされた Web アプリケーション。これにより、Web サイトから直接カード会員データを保存するデータベースにアクセスできます（要件 6.5）。
- セキュリティパッチが適用および更新されていない（要件 6.1）。
- ログの不足（要件 10）。
- （ログレビュー、侵入検出/防止、四半期に一度の脆弱性スキャン、変更検知メカニズムによる）監視の不足（要件 10.6、11.2、11.4、11.5）
- 不適切な範囲決定。たとえば、有効性が検証されていない不十分なネットワークセグメンテーションにより、ネットワークの一部が PCI DSS の範囲から除外されます。これによって、カード会員データ環境が、PCI DSS に従って保護されていないネットワークのその他の部分の弱点（

保護されていない無線アクセスポイント、従業員の電子メールや Web ブラウズによる脆弱性など）に無意識のうちにさらされることになります（要件 1.2、1.3、1.4）。

## 準拠とセキュリティの違いを理解する

準拠することと安全であることの違いを認識することが重要です。ある時点で PCI DSS に準拠していても、環境の変化を防ぐことはできません。適切なコントロールが実装されていない場合、セキュリティに影響を与える可能性があります。したがって、PCI DSS コントロールが、日常業務（BAU）アクティビティの一部として全体的なセキュリティ戦略で定義されているとおりに適切に実装され続けるようにする必要があります。これにより、組織のセキュリティコントロールの有効性を継続的に監視し、PCI DSS 評価の間で PCI DSS 準拠環境を維持できます。PCI DSS を BAU アクティビティに組み込む方法の例は、PCI DSS の「PCI DSS を日常業務プロセスに実装するためのベストプラクティス」セクションに記載されています。

また、PCI DSS セキュリティ要件はペイメントカードデータの保護を目的としており、組織には PCI DSS の範囲外となる保護が必要な他の機密データや資産がある場合があります。したがって、適切に維持されていれば、PCI DSS 準拠は確かに全体的なセキュリティに寄与しますが、堅牢な組織全体のセキュリティプログラムに取って代わるものと見なすべきではありません。

## PCI DSS 準拠のための全般的なヒントと戦略

以下は、PCI DSS 準拠作業を開始するにあたっての全般的なヒントと戦略です。これらのヒントは、必要のないカード会員データの保存を除外し、必要なデータを定義済みで管理されている集中エリアに分離するのに役立ちます。また、PCI DSS 準拠の検証作業の範囲を限定することができます。たとえば、必要のないデータを除外したり、必要なデータを定義済みの管理されているエリアに分離することで、カード会員データを保存、処理、伝送しない、またはそれらを行うシステムに接続しないシステムとネットワークを自己評価の範囲から除外することができます。

1. **機密認証データ（磁気ストライプの全内容やチップ内の同等のデータ、カード検証コードと値、PIN ブロックを含む）**

   承認後に***このデータを保存していないこと***を確認します。

2. **POS ベンダにシステムのセキュリティについて問い合わせます。次の質問を推奨します。**

   a. POS システムの一部であるシステムとデータベースで既定の設定およびパスワードは変更されていますか？

   b. POS システムにリモートアクセスしますか？その場合、安全なリモートアクセス方法を使用していて、共通または既定のパスワードを使用していないなど、我が社の POS システムに他者がアクセスできないようにするための適切な管理が実装されていますか？我が社の POS デバイスにどのぐらいの頻度でリモートアクセスしますか、またその理由は何ですか？POS にリモートアクセスする権限を持っているのは誰ですか？

   c. 不要なサービスと安全でないサービスはすべて、POS システムの一部であるシステムとデータベースから削除されていますか？

   d. POS ソフトウェアはペイメントアプリケーションデータセキュリティ基準（PA-DSS）に対して検証されていますか（PCI SSC の検証済みペイメントアプリケーションのリストを参照）？

   e. POS ソフトウェアは機密認証データ（トラックデータ）または PIN ブロックを保存しますか？その場合、この保存は禁止されているため、いつ削除を手伝ってくれますか？

f. POS ソフトウェアはプライマリアカウント番号（PAN）を保存しますか？もしそうなら、このストレージを保護する必要があります。POS はこのデータをどのように保護していますか？

g. 前述の禁止されているデータが保存されていないことを確認したいので、アプリケーションが書き込むファイルの一覧と各ファイルの内容の概要を文書化してもらえますか？

h. POS ソフトウェアはすべてのユーザーに複雑で固有のパスワードを要求していますか？

i. 共通または既定のパスワードを我が社のシステムおよびサポート対象の他の加盟店システムに使用していないことを確信できますか？

j. POS システムの一部であるシステムとデータベースはすべて、適用可能なすべてのセキュリティ更新によってパッチされていますか？

k. POS システムの一部であるシステムとデータベースではログ機能がオンになっていますか？

l. 以前のバージョンの POS ソフトウェアが機密認証データを保存していた場合、この機能は POS ソフトウェアへの最新の更新中に削除されましたか？このデータを削除するために安全なワイプユーティリティが使用されましたか？

**3. カード会員データ — 必要ない場合は、保存してはいけません。**

a. ペイメントブランドのルールでは、個人アカウント番号（PAN）、有効期限、カード会員名、サービスコードの保存が許可されています。

b. このデータを保存するすべての理由と場所のインベントリを作成します。データが重要なビジネス目的を果たさない場合は、削除を検討します。

c. そのデータの保存とサポートするビジネスプロセスが以下に値するかどうかを考えます。

i. データが侵害されるリスク。

ii. そのデータを保護するために適用する必要がある追加の PCI DSS コントロール。

iii. 長期的に PCI DSS への準拠を維持するための継続的な保守作業。

**4. カード会員データ — 必要ない場合は、集約して分離します。**

データ保存を定義済みの環境に集約し、適切なネットワークセグメンテーションを使用してデータを分離することで、PCI DSS 評価の範囲を限定できます。たとえば、カード会員データと同じマシンまたはネットワークセグメント上で従業員がインターネットをブラウズし、電子メールを受信する場合は、カード会員データを（ルーターまたはファイアウォールを介した）独自のマシンまたはネットワークセグメントにセグメント化（分離）することを検討します。カード会員データを効果的に分離できれば、すべてのマシンを含めるのではなく、分離された部分のみに PCI DSS 作業を集中させることができる可能性があります。

**5. 代替コントロール**

組織がある PCI DSS 要件の技術的仕様を満たすことができないが、関連するリスクは十分に軽減されている場合、ほとんどの要件で代替コントロールを検討することができます。組織が PCI DSS で指定されている管理を正確に実装していないが、代替コントロールの PCI DSS 定義を満たすその他の管理が実装されている（PCI DSS 付録 B の「代替コントロール」および www.pcisecuritystandards.org にある『*PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）*』文書を参照）場合、組織では以下を行う必要があります。

a. PCI DSS 付録 B に記載されている代替コントロールの手順に従います。

b. 代替コントロールの支援によって満たされるすべての要件について、"はい（CCW）" 列にチェックを付けて SAQ の質問に回答します。

c. SAQ の付録 B の代替コントロールワークシートを完成させて、各代替コントロールを文書化します。

> 代替コントロールによって満たされる要件ごとに、代替コントロールワークシートを完成させる必要があります。

d. アクワイアラーまたはペイメントブランドからの指示に従って、すべての完成した代替コントロールワークシートを、完成した SAQ や準拠証明書とともに提出します。

**6. 専門家による支援とトレーニング**

a. セキュリティの専門家に自己問診の支援を依頼する場合、認定セキュリティ評価機関（QSA）へのお問い合わせを検討することをお勧めします。QSA は PCI SSC によるトレーニングを受け、PCI DSS 評価を実施しており、PCI SSC Web サイトに掲載されています。

b. PCI SSC Web サイトは、次のような追加リソースの主要なソースです。

- *PCI DSS の用語集（用語、略語、および頭字語）*
- よくある質問（FAQ）
- ウェビナー
- 情報補足資料およびガイドライン
- SAQ フォームと準拠証明書

***注：****情報補足資料は、PCI DSS を補完し、PCI DSS 要件を満たすための追加の考慮事項および推奨事項を示します。また、PCI DSS またはその要件を変更したり、排除したり、取って代わったりするものはありません。*

c. PCI SSC は組織の人員の意識を高めるのに役立つトレーニングプログラムも多数提供しています。たとえば、PCI 意識向上トレーニング、PCI プロフェッショナル（PCIP）プログラム、内部セキュリティ評価者（ISA）プログラムなどがあります。

   詳細については、www.pcisecuritystandards.org を参照してください。

d. ペイメント関連のトレーニングプログラムおよびリソースは、ペイメントブランドや加盟店アクワイアラーからも入手できる場合があります。

## 組織に最適な SAQ および証明書の選択

すべての加盟店とサービスプロバイダは常に、環境に該当する PCI DSS に準拠する必要があります。SAQ にはいくつかの種類があります。次の表に簡単な説明が記載されています。詳細については以降のページで説明します。この表を使用してどの SAQ が組織に適用されるかを判断し、詳細説明を確認して、その SAQ のすべての要件を満たすようにしてください。

***SAQ D を除くすべての SAQ に関する注意：*** これらの SAQ には、関連する SAQ 適格性規準で定義されている特定の種類の加盟店環境に適用される質問が含まれています。指定された SAQ でカバーされていない環境に該当する PCI DSS 要件がある場合、この SAQ が環境に適していないことを示している可能性があります。また、PCI DSS に準拠するには、すべての該当する PCI DSS 要件に準拠する必要があります。

| SAQ | 説明 |
|---|---|
| **A** | すべてのカード会員データ機能を PCI DSS 準拠のサードパーティサービスプロバイダに完全に委託しているカード非提示加盟店（電子商取引またはメール/電話注文）で、加盟店のシステムまたは施設でカード会員データの電子保管、処理、または送信を実行していない加盟店。<br>*対面式のチャネルには適用されません。* |
| **A-EP** | PCI DSS 検証済みで、カード会員データを直接受け取っていないがペイメントトランザクションのセキュリティに影響を与える可能性のある Web サイトを保有しているサードパーティに、すべてのペイメント処理を委託している、電子商取引加盟店。加盟店のシステムまたは施設内で、カード会員データの電子的な保存、処理、送信はできません。<br>*電子商取引のチャネルにのみ適用されます。* |
| **B** | 以下のみを使用している加盟店：<br>▪ カード会員データを電子的に保存していないインプリントマシン、および/または<br>▪ カード会員データを電子的に保存していない、スタンドアローンのダイヤルアウト端末<br>*電子商取引のチャネルには適用されません。* |
| **B-IP** | ペイメントプロセサーと IP 接続されているスタンドアローンの PTS<br>認定の決済端末のみを使用し、カード会員データを電子的に保存していない加盟店。<br>*電子商取引のチャネルには適用されません。* |

| SAQ | 説明 |
|---|---|
| **C-VT** | PCI DSS<br>検証済みサードパーティのサービスプロバイダが提供・ホストしているインターネットベースの<br>仮想支払端末ソリューションに、キーボードから一度に 1 つの取引を手動で入力する加盟店。カー<br>ド会員データは電子的に保存していません。<br>*電子商取引のチャネルには適用されません。* |
| **C** | インターネットに接続されたペイメントアプリケーションシステムを有し、カード会員データを電子的に保存していない加盟店。<br>*電子商取引のチャネルには適用されません。* |
| **P2PE** | 検証済みで、カード会員データを電子的に保存せず、PCI SSC にリストされたポイントツーポイント暗号化（P2PE）ソリューションに含まれ、これによって管理されるハードウェア決済端末のみを使用する加盟店。<br>*電子商取引のチャネルには適用されません。* |
| **D** | ***加盟店向け SAQ D：*** 上記の SAQ タイプの説明には含まれていない、すべての加盟店。 |
| | ***サービスプロバイダ向け SAQ D：*** ペイメントブランドによって SAQ の実施が定義されているすべてのサービスプロバイダ。 |

## SAQ A – 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外部委託

*SAQ A は、カード会員データ機能を検証済みの第三者に完全に委託していて、紙の計算書または領収書でのみカード会員データを保持している加盟店に適用される要件に対応するために作成されました。*

SAQ A の加盟店は、電子商取引またはメール/電話注文（カードを提示しない）の加盟店であり、システムまたは施設内でカード会員データを電子形式で保存、処理、または送信することはありません。

SAQ A の加盟店は、このペイメントチャネルについて以下の適格性規準を満たしていることを確認します。

- あなたの会社はカードを提示しない（電子商取引またはメール/電話注文）取引のみを扱います。
- カード会員データのすべての処理は、PCI DSS 検証済みのサードパーティのサービスプロバイダに完全に外部委託されています。
- あなたの会社は、システムまたは施設内でカード会員データを電子的に保存、処理、送信しませんが、これらすべての機能の扱いは第三者に完全に依拠しています。
- あなたの会社は、カード会員データの保存、処理、送信を扱うすべての第三者が PCI DSS に準拠していることを確認しました。**また**
- あなたの会社が保持するカード会員データは紙媒体（印刷された計算書や領収書など）であり、これらの文書を電子的に受信することはありません。

*さらに、電子商取引のチャネルの場合は*

- 消費者のブラウザに表示されるすべての支払いページのすべての要素が、PCI DSS で検証されたサードパーティのサービスプロバイダを作成元とし、そこから直接提供されています。

***この SAQ は対面式のチャネルには適用されません。***

*チャートに従って SAQ タイプを選択するには、21 ページの「自分の環境に最も適している SAQ はどれか？」を参照してください。*

## SAQ A-EP – 部分的に外部委託 ペイメント処理にサードパーティの Web サイトを使用している電子商取引の加盟店

*SAQ A-EP は、カード会員データを受信しないものの、ペイメントトランザクションのセキュリティや、消費者のカード会員データを受信するページの完全性に影響を与える Web サイトを持つ、電子商取引加盟店に適用される要件に対応するために作成されました。*

SAQ A-EP の加盟店は、電子商取引のペイメントチャネルを PCI DSS 検証済みの第三者に部分的に委託しており、システムまたは施設内でカード会員データを電子的に保存、処理、送信しない電子商取引加盟店です。

SAQ A-EP の加盟店は、このペイメントチャネルについて以下の適格性規準を満たしていることを確認します。

- あなたの会社は電子商取引のみを扱います。
- 支払いページを除くカード会員データのすべての処理は、PCI DSS 検証済みのサードパーティのペイメントプロセサーに完全に外部委託されています。
- あなたの電子商取引 Web サイトは、カード会員データを受信しませんが、消費者またはカード会員データを PCI DSS 検証済みのサードパーティのペイメントプロセサーにリダイレクトする方法を制御しています。
- 加盟店の Web サイトがサードパーティの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、すべての該当する PCI DSS 要件（PCI DSS 付録 A プロバイダが共有ホスティングプロバイダの場合など）に対して検証されています。
- 消費者のブラウザに表示される支払いページの各要素は、加盟店の Web サイトか PCI DSS 準拠のサービスプロバイダを作成元としています。
- あなたの会社は、システムまたは施設内でカード会員データを電子的に保存、処理、送信しませんが、これらすべての機能の扱いは第三者に完全に依拠しています。
- あなたの会社は、カード会員データの保存、処理、送信を扱うすべての第三者が PCI DSS に準拠していることを確認しました。**また**
- あなたの会社が保持するカード会員データは紙媒体（印刷された計算書や領収書など）であり、これらの文書を電子的に受信することはありません。

***この SAQ は電子商取引のチャネルにのみ適用されます。***

***注：SAQ A-EP では、"カード会員データ環境" に言及している PCI DSS 要件が加盟店の Web サイトに適用されます。これは、Web サイト自体がカード会員データを受信しない場合であっても、加盟店の Web サイトがペイメントカードデータが送信される方法に直接影響するためです。***

***チャートに従って SAQ タイプを選択するには、21 ページの「自分の環境に最も適している SAQ はどれか？」を参照してください。***

## SAQ B – インプリントのみの加盟店、またはスタンドアローンのダイヤルアウト端末のみの加盟店。カード会員データを電子形式で保存しない

*SAQ B は、インプリントマシンまたはスタンドアローンのダイヤルアウト端末のみによって、カード会員データを処理する加盟店に適用される要件に対応するために作成されました。*

SAQ B の加盟店は、実店舗（カードを提示する）またはメール/電話注文（カードを提示しない）の加盟店のいずれかとなり、コンピュータシステムにカード会員データを保存しません。SAQ B の加盟店は、このペイメントチャネルについて以下の適格性規準を満たしていることを確認します。

- あなたの会社は、インプリントマシンおよび/またはスタンドアローンのダイヤルアウト端末（電話回線を介してプロセサーに接続）のみを使用して、顧客のペイメントカード情報を取得します。
- スタンドアローンのダイヤルアウト端末は環境内の他のシステムには接続されていません。
- スタンドアローンのダイヤルアウト端末はインターネットに接続されていません。
- あなたの会社は、カード会員データをネットワーク（内部ネットワークまたはインターネット）経由で送信しません。
- あなたの会社が保持するカード会員データは紙媒体（印刷された計算書や領収書など）であり、これらの文書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 は電子商取引のチャネルには適用されません。***

*チャートに従って SAQ タイプを選択するには、21 ページの「自分の環境に最も適している SAQ はどれか？」を参照してください。*

## SAQ B-IP – スタンドアローンの IP 接続されている PTS 加盟店端末装置（POI）を使用している加盟店、カード会員データを電子形式で保存しない

*SAQ B-IP は、ペイメントプロセサーとの IP 接続を持つスタンドアローンの PTS 認可の加盟店端末装置（POI）デバイスを介してのみカード会員データを処理する加盟店に適用される要件に対応するために作成されました。*

SAQ B-IP の加盟店は、実店舗（カードを提示する）またはメール/電話注文（カードを提示しない）の加盟店のいずれかとなり、コンピュータシステムにカード会員データを保存しません。

SAQ B-IP の加盟店は、このペイメントチャネルについて以下の適格性規準を満たしていることを確認します。

- あなたの会社は、ペイメントプロセサーへの IP 接続を持つスタンドアローンの PTS 認可の加盟店端末装置（POI）デバイス（SCR を除く）のみを使用して、顧客のペイメントカード情報を取得します。
- スタンドアローンの IP 接続されている POI デバイスは、PCI SSC Web サイトに記載されている PTS POI プログラムに対して検証されています（SCR を除く）。
- スタンドアローンの IP 接続されている POI デバイスは、環境内の他のシステムに接続されていません（これは、ネットワークセグメンテーションで POI デバイスをその他のシステムから隔離することで実現できます）。
- カード会員データの送信は、PTS 認可の POI デバイスからペイメントプロセサーへの送信のみです。
- POI デバイスは、ペイメントプロセサーへの接続について他のデバイス（コンピュータ、携帯電話、タブレットなど）に依拠しません。
- あなたの会社が保持するカード会員データは紙媒体（印刷された計算書や領収書など）であり、これらの文書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 は電子商取引のチャネルには適用されません。***

*チャートに従って SAQ タイプを選択するには、21 ページの「自分の環境に最も適している SAQ はどれか？」を参照してください。*

## SAQ C-VT – Web ベースの仮想端末の加盟店、カード会員データを電子形式で保存しない

*SAQ C-VT は、インターネットに接続されたパソコン上の隔離された仮想支払端末によってのみ、カード会員データを処理する加盟店に適用される要件に対応するために作成されました。*

仮想支払端末は、ペイメントカードトランザクションを承認するためのアクワイアラー、プロセサー、サードパーティのサービスプロバイダ Web サイトへの Web ブラウザベースのアクセスであり、加盟店は安全に接続された Web ブラウザからペイメントカードデータを手動で入力します。物理端末とは異なり、仮想支払端末はペイメントカードからデータを直接読み取ることはありません。ペイメントカードトランザクションは手動で入力されます。

SAQ C-VT 加盟店は、仮想支払端末を介してのみカード会員データを処理し、コンピュータシステムにカード会員データを保存しません。これらの仮想端末は、仮想端末ペイメント処理機能をホストする第三者にアクセスするため、インターネットに接続されています。この第三者は、加盟店の仮想端末ペイメントトランザクションを承認および/または決済するためにカード会員データを保存、処理、送信するプロセサー、アクワイアラー、またはその他のサードパーティのサービスプロバイダとなります。

この SAQ オプションは、一度に 1 つの取引をキーボードからインターネットベースの仮想端末ソリューションに手動で入力する加盟店にのみ適用するためのものです。SAQ C-VT の加盟店は、実店舗（カードを提示する）またはメール/電話注文（カードを提示しない）の加盟店となります。

SAQ C-VT の加盟店は、このペイメントチャネルについて以下の適格性規準を満たしていることを確認します。

- あなたの会社のペイメント処理は、インターネットに接続された Web ブラウザによってアクセスされる仮想支払端末を介してのみ行われます。
- あなたの会社の仮想支払端末ソリューションは、PCI DSS 検証済みサードパーティのサービスプロバイダによって提供およびホストされています。
- あなたの会社は、1 つの場所に隔離されたコンピュータから PCI DSS 準拠の仮想支払端末ソリューションにアクセスし、環境内の他の場所またはシステムに接続されていません（これは、ファイアウォールやネットワークセグメンテーションでコンピュータをその他のシステムから分離することで実現できます）。
- あなたの会社のコンピュータには、カード会員データを保存するようなソフトウェアがインストールされていません（バッチ処理またはストアアンドフォワード用のソフトウェアなどが存在しない）。
- あなたの会社のコンピュータには、カード会員データを取得または保存するのに使用されるハードウェアデバイスが接続されていません（カードリーダーなどが接続されていない）。
- あなたの会社は、いかなるチャネル（内部ネットワークやインターネットなど）でもカード会員データを電子的に受信または送信しません。
- あなたの会社が保持するカード会員データは紙媒体（印刷された計算書や領収書など）であり、これらの文書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** は電子商取引のチャネルには適用されません。*

*チャートに従って SAQ タイプを選択するには、21 ページの「自分の環境に最も適している SAQ はどれか？」を参照してください。*

## SAQ C – 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

*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経由）加盟店に適用される要件に対応するために作成されました。*

SAQ C の加盟店は、インターネットに接続されている POS システムやその他のペイメントアプリケーションシステムを介してカード会員データを処理するが、カード会員データをコンピュータシステムに保存しない、実店舗（カードを提示する）またはメール/電話注文（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、このペイメントチャネルについて以下の適格性規準を満たしていることを確認します。

- あなたの会社では、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および/またはローカルエリアネットワーク（LAN）上にあります。
- 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、ネットワークセグメンテーションで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その他すべてのシステムから隔離することで実現できます）。
- POS 環境の物理的な場所は他の施設または場所に接続されておらず、LAN は単一の店舗用にのみ用意されています。
- あなたの会社が保持するカード会員データは紙媒体（印刷された計算書や領収書など）であり、これらの文書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 は電子商取引のチャネルには適用されません。***

*チャートに従って SAQ タイプを選択するには、21 ページの「自分の環境に最も適している SAQ はどれか？」を参照してください。*

## SAQ P2PE – PCI SSC リストの P2PE ソリューションでハードウェア決済端末のみを使用している加盟店、カード会員データを電子形式で保存しない

*SAQ P2PE は、検証済みおよびPCI SSC リストのポイントツーポイント暗号化（P2PE）ソリューションに含まれる決済端末でのみカード会員データを処理する加盟店に適用される要件に対応するために作成されました。*

SAQ P2PE の加盟店は、コンピュータシステム上の平文のアカウントデータにアクセスせず、PCI SSC 認可の P2PE ソリューションからハードウェア決済端末を介してのみアカウントデータを入力します。SAQ P2PE の加盟店は、実店舗（カードを提示する）またはメール/電話注文（カードを提示しない）の加盟店のいずれかとなります。たとえば、メール/電話注文の加盟店は、カード会員データを紙または電話で受信し、直接 P2PE 検証済みハードウェアデバイスのみに入力する場合に、SAQ P2PE の対象となります。

SAQ P2PE の加盟店は、このペイメントチャネルについて以下の適格性規準を満たしていることを確認します。

- すべてのペイメント処理は、PCI SSC によって認可およびリスト化された検証済み PCI P2PE ソリューションで行われます。
- アカウントデータを保存、処理、送信する加盟店環境のシステムは、検証済みおよび PCI リストの P2PE ソリューションでの使用が承認された加盟店端末装置（POI）デバイスのみです。
- あなたの会社は、いかなる方法でもカード会員データを電子的に受信または送信しません。
- 環境内に電子的なカード会員データのレガシーストレージはありません。
- あなたの会社が保持するカード会員データは紙媒体（印刷された計算書や領収書など）であり、これらの文書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、P2PE ソリューションプロバイダによって提供されている *P2PE 説明書（PIM）* のすべてのコントロールを実装しています。

***この SAQ は電子商取引のチャネルには適用されません。***

*チャートに従って SAQ タイプを選択するには、21 ページの「自分の環境に最も適している SAQ はどれか？」を参照してください。*

## 加盟店向け SAQ D – SAQ の適用対象となるその他すべての加盟店

*加盟店向け SAQ D は、その他の SAQ タイプの基準を満たしていない SAQ 対象加盟店に適用されます。*

SAQ D を使用する加盟店環境の例には以下が含まれます（ただし、これらに限定されません）。

- Web サイトでカード会員データを受信する電子商取引の加盟店
- カード会員データを電子的に保存している加盟店
- カード会員データを電子的に保存していないが、別の SAQ タイプの基準を満たしていない加盟店
- 別の SAQ タイプの基準を満たしているが、追加の PCI DSS 要件が適用される環境の加盟店

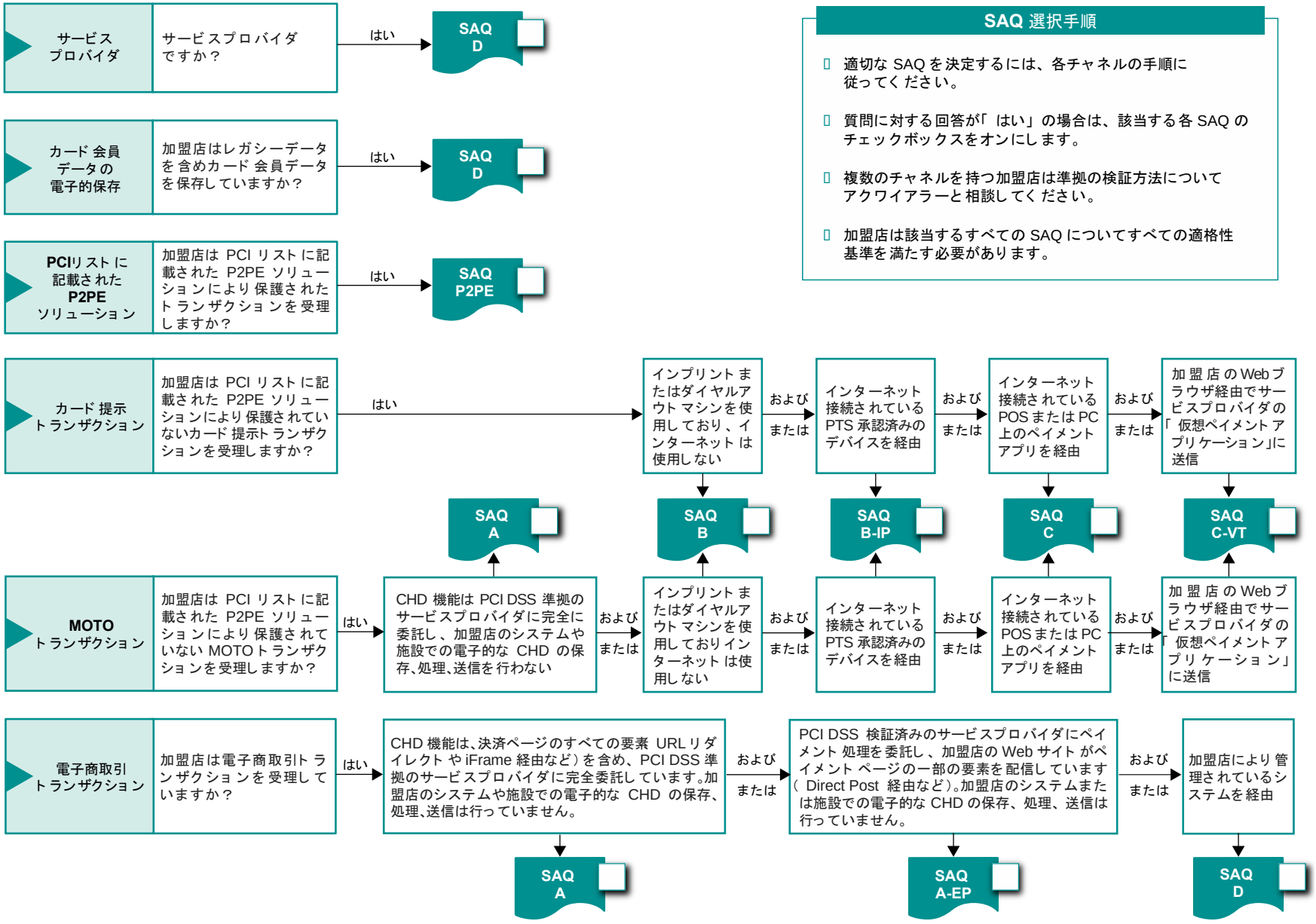
## サービスプロバイダ向け SAQ D – SAQ の適用対象となるサービスプロバイダ

*サービスプロバイダ向け SAQ D は、ペイメントブランドによって SAQ 対象として定義されているすべてのサービスプロバイダに適用されます。*

***加盟店向け SAQ D およびサービスプロバイダ向け SAQ D に関する注意：*** SAQ D を完了している多くの組織がすべての PCI DSS 要件の準拠を検証する必要がありますが、ビジネスモデルが非常に特殊な一部の組織では一部の要件が適用されない場合があります。たとえば、まったく無線テクノロジを使用していない会社は、無線テクノロジの管理に固有の PCI DSS のセクションの準拠を検証することは期待されていません。その他の特定の要件の除外については、各 SAQ D の特定のガイダンスを参照してください。

*チャートに従って SAQ タイプを選択するには、21 ページの「自分の環境に最も適している SAQ はどれか？」を参照してください。*

# 自分の環境に最も適している SAQ はどれか




## SAQ 選択手順

- 適切な SAQ を決定するには、各チャネルの手順に従ってください。
- 質問に対する回答が「はい」の場合は、該当する各 SAQ のチェックボックスをオンにします。
- 複数のチャネルを持つ加盟店は準拠の検証方法についてアクワイアラーと相談してください。
- 加盟店は該当するすべての SAQ についてすべての適格性基準を満たす必要があります。