SAQによるPCI DSS準拠

SAQ（自己問診 = Self Assessment Questionnaire）は、
自己調査によって準拠を証明する方法

1. 内部・外部N/Wスキャン検査を四半期ごとに実施し、対応の必要がある脆弱性がない・または解決済である結果レポート1年分をそろえます。

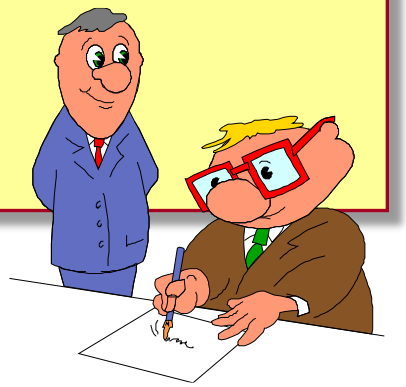
※システム環境により、内部・外部ペネトレーションテストや、アプリケーションぜい弱性検査も求められます。

2. 所定のSAQに指定されている、PCI DSS要件のすべての項目に対応済であることを確認して記入し、内容責任について事業者の役員が署名します。

※業務内容により適合するSAQタイプは異なります。次のページの資料を参照ください。

3. 契約先のアクワイアラーまたはカードブランドによる、所定の手続きに添って提出します。

※決済件数の取扱いレベルにより、必ず提出する場合と、
要求されたら提出する場合があります。ブランドやカード会社により
ガイドラインが異なりますので、契約先へお問合せください。



※SAQには、支援したQSAや ISA（Internal Security Assessor＝PCI DSSの社内審査資格者）**がある場合、署名する欄があります。**

QSAの支援・署名は必須ではありません。受理はアクワイアラー判断です。

どのタイプのSAQを使えばよいか（1）

加盟店の業態により、使用するSAQにはいろいろなタイプがあります。

PCI SSCのサイトから「SAQの説明書とガイドライン」の日本語版をダウンロードして、どのタイプのSAQを使用すべきか、検討しましょう。サービスプロバイダーは1種類のみです。

タイプ A すべてのアカウントデータ機能をPCI DSSに準拠した検証済みサードパーティに完全に委託する、カード非提示型加盟店（Eコマースまたは通信販売／電話注文）。加盟店のシステムまたは施設でアカウントデータを電子的に保存、処理、または伝送しない。対面チャネルには適用されない。サービスプロバイダーには適用されない。

タイプ A-EP 決済処理をPCI DSSに準拠した検証済みサードパーティに部分的に委託し、それ自体はアカウントデータを受領しないが、決済取引のセキュリティおよび／または消費者アカウントデータを受領するページの整合性に影響を与えるウェブサイトを持つEコマース加盟店。加盟店のシステムまたは施設でアカウントデータを電子的に保存、処理、または伝送しない。Eコマースチャネルにのみ適用される。サービスプロバイダーには適用されない。

タイプ B 以下のみを使用する加盟店：電子アカウントデータ保存しないインプリンタ、および／または
電子アカウントデータを保存しないスタンドアロン型ダイヤルアップ端末。 Eコマースチャネルには適用されない。
サービスプロバイダーには適用されない。

タイプ B-IP ペイメントプロセッサーにIP接続された、スタンドアロン型のPCIリストに掲載された認可済みPTS（PINトランザクションセキュリティ）POI（加盟店端末装置）デバイスのみを使用する加盟店。電子アカウントデータは保存しない。
Eコマースチャネルには適用されない。サービスプロバイダーには適用されない。

タイプ C インターネット接続された決済アプリケーションシステムを持つ加盟店。電子アカウントデータは保存しない。
Eコマースチャネルには適用されない。サービスプロバイダーには適用されない。

どのタイプのSAQを使えばよいか（2）

タイプ C-VT 孤立したコンピューティングデバイスと安全に接続されたウェブブラウザを使用して、PCI DSSに準拠した検証済みサードパーティの仮想決済端末ソリューションに、キーボードで一度に1件の取引について決済アカウントデータを手入力する加盟店。電子アカウントデータは保存しない。 Eコマースチャネルには適用されない。サービスプロバイダーには適用されない。。

タイプ P2PE 検証済みでPCIリストに掲載されたポイントツーポイント暗号化（P2PE）ソリューションのみを利用する加盟店。平分アカウントデータにアクセスできず、電子アカウントデータを保存しない。 Eコマースチャネルには適用されない。サービスプロバイダーには適用されない。

タイプ SPoC PCI SCC検証済みSPoCソリューションリストに掲載された、セキュアカードリーダーを備える商用オフザシェルフのモバイルデバイス（例：スマートフォン、タブレット等）を使用する加盟店。平分アカウントデータにアクセスできず、電子アカウントデータを保存しない。無人カード提示型、通信販売／電話注文（MOTO）、Eコマースチャネルには適用されない。
サービスプロバイダーには適用されない。

タイプ D（加盟店用） D：上記のタイプの説明に含まれていないすべての加盟店。 サービスプロバイダーには適用されない。

タイプ D（サービスプロバイダー用） ペイメントブランドによってSAQ実施対象と定義されるすべてのサービスプロバイダー。
※ブランドごとのルールにより、SAQでの準拠を認めず、QSA審査が求められる場合があります。