各 SAQ (v3.2 版)を適用すべきカード情報取扱い形態の説明

2017.7.1/ JCDSC

各 SAQ の「開始する前に」の部分を抽出したものです。
カード情報の取り扱い形態が詳しく書かれていますから、自社の業務形態に適合する SAQ タイプを検討してください。それでも判断に迷う場合は、アクワイアラーや QSA、コンサルタントに相談してください。

【SAQ A】

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ー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ーに、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ー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ーからのみ、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。

【SAQ A-EP】

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ッ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ッサーに、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、第三者プロバイダーによってホストされている場合、そのプロバイダー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（プロバイダーが共有ホスティングプロバイダーの場合は、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ー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ー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）のみを保管し、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。

【SAQ B】

インプリンターまたはスタンドアロン型ダイヤルアップ端末のみによって、カード会員データを処理する加盟店に適用される要件を示すために、作成されたものです。SAQ B 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、カード会員データをコンピューターシステムに保存しません。

SAQ B 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、インプリンターのみを使用するか、スタンドアロン型ダイヤルアップ端末（電話回線によって処理装置に接続）のみを使用して（あるいはその両方）、顧客のペイメントカード情報を取り込みます。
・スタンドアロン型ダイヤルアップ端末は、環境内のその他のシステムに接続されていません。
・スタンドアロン型ダイヤルアップ端末は、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）を経由して伝送しません。
・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）のみを保管し、これらの書類を電子的に受信することはありません。
・これらの書類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、電子商取引チャネルには適用されません。

【SAQ B-IP】

ペイメントプロセッサーに IP 接続される、スタンドアロン型 PTS 認定の加盟店端末装置のみによって、カード会員データを処理する加盟店に適用される要件を示すために、作成されました。セキュア

カードリーダー(SCR)として分類される POI 装置に対して例外が適用します。すなわち、SCR を使う加盟店はこの SAQ の対象外です。

SAQ B-IP 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、カード会員データをコンピューターシステムに保存しません。

SAQ B-IP 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、顧客のペイメントカード情報を取り込むために、ペイメントプロセッサーに IP 経由で接続されている、スタンドアロン型 PTS 承認の加盟店端末装置 (POI) (SCR を除く)のみを、使用しています。

・スタンドアロン型 IP 接続 POI 装置は、PCI SSC Web サイトに一覧表示されている通り、PTS POI プログラムに対して検証されます(SCR を除く)。

・スタンドアロン型 IP 接続 POI 装置は、環境内の他のシステムには接続されていません(これは、POI 装置を他のすべてのシステムから分離する、ネットワークセグメンテーションによって実現できます)。

・カード会員データの唯一の伝送は、PTS 認定 POI 装置からペイメントプロセッサーへのものです。

・POI 装置は他の装置(コンピューター、携帯電話、タブレット等)を介すことなく、ペイメントプロセッサーに接続されます。

・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。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、電子商取引チャネルには適用されません。

【SAQ C】

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 C の加盟店は、POS(販売時点情報管理)システム、またはインターネットに接続されている、その他のペイメントアプリケーションシステム経由で、カード会員データを処理しますが、カード会員データをコンピューターシステムに保存しません。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)加盟店のいずれかとなります。

SAQ C 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、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、同じデバイス上または同じローカルエリアネットワーク(LAN)上(あるいはその両方)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、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他のすべてのシステムから分離する、ネットワークセグメンテーションによって実現できます)。

・POS 環境の物理的場所は、他の敷地や場所に接続されておらず、LAN は単一場所用です。

・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)のみを保管し、これらの書類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 は電子商取引チャネルには適用されません。

【SAQ C-VT】

インターネットに接続されたパーソナルコンピューター上にある、隔離された仮想端末のみによって、カード会員データを処理する加盟店に適用される要件を示すために、作成されました。

仮想端末は、ペイメントカードトランザクションを承認するアクワイアラー、プロセッサー、または第三者サービスプロバイダーの、Web サイトへの Web ブラウザベースのアクセスです。加盟店は安全に接続された Web ブラウザを使用して、ペイメントカードデータを手動で入力します。物理的端末の場合と異なり、仮想端末はデータをペイメントカードから直接には読み取りません。ペイメントカードトランザクションを手動で入力するため、一般に仮想端末は、取引量の少ない加盟店環境で、物理的端末の代わりに使用されます。

SAQ C-VT 加盟店は、仮想端末のみによってカード会員データを処理し、カード会員データをコンピューターシステムに保存しません。これらの仮想端末は、仮想端末の支払い処理機能をホストする、第三者にアクセスする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取引を承認および/または決済するため、カード会員データを保存、処理、および/または伝送するプロセッサー、アクワイアラー、またはその他の第三者サービスプロバイダーがありえます。

この SAQ オプションはキーボードを介して、一度に 1 つのトランザクションを、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、適用されることを目的としています。SAQ C-VT 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。

SAQ C-VT 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。

・あなたの会社の唯一の支払い処理は、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、仮想端末によって行われます。

・あなたの会社の仮想端末ペイメントソリューションは、PCI DSS を検証済みの第三者サービスプロバイダーによって提供され、ホストされます。

・あなたの会社は、一箇所に隔離され、環境内の他の場所またはシステムに接続されていないコンピューターを介して、PCI DSS に準拠する仮想端末ソリューションにアクセスします（これはコンピューターを他のシステムから隔離するために、ファイアウォールまたはネットワークセグメンテーションによって実現されます）。

・あなたの会社のコンピューターには、カード会員データを保存するソフトウェア（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）がインストールされていません。

・あなたの会社には、カード会員データをキャプチャーまたは保存するためのハードウェアデバイス（カードリーダーなど）は取り付けられていません。

・あなたの会社は、カード会員データを、何らかのチャネル（内部ネットワークまたはインターネットなど）を介して、電子的に受信または伝送しません。

・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。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、電子商取引チャネルには適用されません。

【SAQ P2PE】

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、どのコンピューター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。

・加盟店がカード会員データを保存する場合、保存するのは紙の計算書または領収書のコピーのみであり、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ー提供の 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。

【SAQ D Marchant】

加盟店用 SAQ D は、他の SAQ タイプの基準を満たさない 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、次のようなものがありますが、これらに限定されません。

·カード会員データを、自社の Web サイトで承認する電子商取引加盟店

·カード会員データを、電子形式で保存する加盟店

·カード会員データを、電子形式で保存しないが、他の SAQ タイプの基準を満たさない加盟店

·他の SAQ タイプの基準を満たす環境にあるが、自社の環境に他の PCI DSS 要件が適用されるような加盟店

SAQ D を完成させる会社の多くは、各 PCI DSS 要件への準拠を検証する必要がありますが、特定のビジネスモデルの会社には適用されない要件もあります。特定の要件の除外については、この SAQ のガイダンスを参照してください。

【サービスプロバイダー用 SAQ D ServiceProvider】

ペイメントブランドにより SAQ 対象として定義された、すべてのサービスプロバイダーに適用されます。SAQ D を行う会社の多くは、各 PCI DSS 要件への準拠を検証する必要がありますが、特定のビジネスモデルの会社には適用されない要件もあります。

たとえば、ワイヤレス技術をまったく使用しない会社は、ワイヤレス技術の管理に特化した PCI DSS セクションへの準拠を検証する必要がありません。同様に、カード会員データをいつも電子形式で保存しない会社はカード会員データの安全な保管に関連する要件を検証する必要はありません（要件 3.4 など）。

以上