別紙

スマートフォン決済の安全基準等に関する基本的な考え方

はじめに

【本紙の趣旨】

日本国内でも既に一部の事業者がサービス提供を開始しているスマートフォン等を活用したクレジットカード決済において、クレジットカード会員にとって、安心・安全にクレジットカード利用ができる環境を提供することを目的として、スマートフォン決済の安全基準等に関する基本的な考え方をまとめたもの。

【前提となる考え方】

・現在、クレジットカード加盟店に設置される一般的なクレジットカード端末は、ＪＣＣＡが安全基準や運用ルールを取り決めており、「カード会員情報等の保護（※１）」「不正利用の防止」に関する安全措置を具備している。
・スマートフォン等（※４）をクレジットカード端末として使用する場合も、一般的なクレジットカード決済端末と同様、「カード会員情報等の保護」「不正利用の防止」に関する安全措置を最低限具備する必要がある。

上記を踏まえた、「スマートフォン決済アプリケーション」「スマートフォン」「周辺機器」「通信」等において最低限具備すべき内容は以下のとおり。

※１：カード会員情報等
センシティブ認証データ（※２）及び会員データ（※３）を指す。

※２：センシティブ認証データ
クレジットカードに記録されているデータのうち、完全な磁気ストライプデータ、カード検証コード又は値、個人識別番号（PIN）及び暗号化された PIN ブロック。

※３：会員データ
クレジットカードに記録されているデータのうち、センシティブ認証データ以外のデータ。具体的にはカード番号（PAN）、有効期限、カード会員名、サービスコード

※４：スマートフォン等
製造後もアプリケーションやソフトウェアが継続的に更新可能な無線通信機能を有している、汎用 OS コンピューティング・デバイス。具体的にはスマートフォン（iOS、Android、Windows Mobile 等）、タブレット（PAD 系）等。

１．カード会員情報等の保護、不正利用の防止のために必要な基準

■スマートフォン決済アプリケーションについて

○カード会員情報等の漏えい及び不正利用を防止するため、スマートフォンをクレジットカード決済端末として利用する際に使用するアプリケーション（以下、スマートフォン決済アプリケーション）は、以下の要件を満たす必要がある。

・スマートフォン決済アプリケーションにおいて、カード会員情報等を承認処理完了後に保存しないこと。

・スマートフォン決済アプリケーションで、カード会員情報等の外部メモリ（SD メモリ等）への保存が禁止されていること。

・スマートフォン決済アプリケーションで、売上票等にカード番号を表示・出力する場合には、個人を識別する桁が非表示化されること。

・スマートフォン決済アプリケーションの配布は予め定められた安全な方法でのみ実施し、クレジットカード取引の都度、適正なアプリケーションであるかが認証されること。

・スマートフォン決済アプリケーションを遠隔で機能停止または削除が可能であること。

・スマートフォン決済アプリケーションが利用しているデータ領域を他アプリケーションからアクセスを不可とすること。

■スマートフォン等について

○不正なスマートフォン等によるスマートフォン決済の利用を防ぐため、スマートフォン等に対して、以下の要件を満たす必要がある。

・ スマートフォン等が特定できるよう、スマートフォン等を認証する（認証用の識別番号は独自に管理、認証可能な番号を推奨）。

・ 暗号化された会員情報等のデータについて、スマートフォン等での暗号化解除、直接閲覧、編集及び複合等は不可とする。

■周辺機器（カードリーダー、IC カードリーダー、PIN パッド等）について

○「カード会員情報等」の漏えいを防止するため、スマートフォン決済において使用が想定される周辺機器（カードリーダー、ＩＣカードリーダー、ＰＩＮパッド等）については、以下の要件を満たす必要がある。

・カード会員情報等は、周辺機器を通じて読み取ることを必須とし、スマートフォンに直接入力することを禁止する。

・カード会員情報等の読込直後に、カードリーダー（ＩＣカードリーダーを含む）でカード会員情報等のデータを暗号化する。

・カードリーダー（ＩＣカードリーダーを含む）でカード会員情報等は保持しない。

・IC カードリーダーは、EMV4.2 Book2-Security and key Management “11.1 Security Requirements”以上の要件に準拠する。

・PIN パッドは、PCI-PTS 認定要件に準拠する。

■通信について

○カード会員情報等の漏えいを防止するため、スマートフォン等とスマートフォン決済センター、スマートフォン等と周辺機器の間の通信においては、以下の要件を満たす必要がある。

・スマートフォン等とスマートフォン決済センター間、およびスマートフォン等と周辺機器間の通信時はカード会員情報等を暗号化する。

・スマートフォン等とスマートフォン決済センター間、スマートフォン等と周辺機器間の通信路を暗号化する。

２．クレジットカード取引を実現するために必要な基準

○スマートフォン決済においても、通常の決済端末と同様、以下の機能が必要となる。

・スマートフォン等の属性を管理する機能。

・ＩＣチップでの取引においてはＰＩＮ入力、磁気ストライブでの取引においては売上票への署名を可能とする機能。

・売上票を出力する機能。

＜参考＞

【スマートフォン決済サービスにおけるサービス提供者の概念図】