平成 24 年 6 月 29 日

「スマートフォン決済セキュリティガイドライン」の制定について

社団法人日本クレジット協会

社団法人日本クレジット協会は、スマートフォン等を加盟店におけるクレジットカード処理端末として利用するクレジットカード決済の安全な運用を確保するため、標記ガイドラインを別添のとおり策定し、加盟店契約のある協会会員カード会社（以下「アクワイアラー」といいます。）に対し協力を依頼した。

≪ガイドラインの概要≫

アクワイアラーは、加盟店が自ら、又はスマートフォン決済提供事業者のサービスを利用してスマートフォン決済を導入する際に、安全・安心なクレジットカード取引を確保するため、本ガイドラインに定める、次のようなセキュリティ対策を加盟店に求めることとする。

＜セキュリティ対策＞

〇カード情報の保護

カード情報の保護として、「スマートフォン等に関するセキュリティ」「スマートフォン決済アプリケーションに関するセキュリティ」「周辺機器のセキュリティ」「ワイヤレス通信におけるセキュリティ」「加盟店のセキュリティ」等を定めている。

〇運用・管理

スマートフォン決済を導入し運用するにあたって加盟店が行なうべきものとして、「スマートフォン決済の管理」「本人確認・売上処理時の対応」「スマートフォン決済の運用の実効性確保」「スマートフォン決済提供事業者のサービスを利用している加盟店における運用の実効性確保のための留意事項」等を定めている。

≪ガイドライン策定の経緯等≫

近時わが国において、スマートフォン等がその利便性の高さゆえに急速に普及している。そして、スマートフォン等の機動性や低コストなどの特徴に着目し、スマートフォン専用アプリケーションやカードリーダー、プリンター等を組み合わせ、クレジットカード決済端末として使用するスマートフォン決済サービス(以下、「スマートフォン決済」といいます。)が、既に一部実用化されており、今後の普及が見込まれる。

その一方で、このスマートフォン決済が汎用のスマートフォン端末等及び通信ネットワークを用いるため、ぜい弱なセキュリティ環境おいて運用された場合、クレジットカード番号等カード情報の漏えいや不正利用等の事故が発生するなどの消費者トラブルが発生することが危惧された。

そこで、スマートフォン決済において、クレジットカード番号等カード情報が安全かつ適切に取り扱われ、消費者に安全・安心なクレジット取引を提供できるよう、セキュリティの確保について十分な対策を講じる必要性が指摘された。

こうした状況を踏まえ、加盟店がスマートフォン決済を導入する際に、アクワイアラーが加盟店に対して求めるセキュリティ対策の基準を示すものとして、本ガイドラインを策定した。

以上

平成 24 年 6 月 11 日

スマートフォン決済セキュリティガイドライン

社団法人日本クレジット協会

＜目次＞

第１章　本ガイドラインの位置付け

１．目的

本ガイドラインは、加盟店が自ら、又はスマートフォン決済提供事業者のサービスを利用してスマートフォン決済を導入する際に、安全・安心なクレジットカード取引を確保するため、アクワイアラーが加盟店に対して求めるセキュリティ対策の基準を示すものである。

２．対象取引の範囲

本ガイドラインでは、加盟店におけるスマートフォン等を用いた対面取引において、IC チップおよび磁気ストライプからカード情報を読み取り処理する取引を対象とする。

なお、カード番号及び有効期限については、スマートフォン等の本体へのマニュアル入力はできないものとする。

また、電文は対面電文により処理されるものとする。

第２章　用語の定義

本ガイドラインにて使用する用語について、以下の通り定義する。

１．センシティブ認証データ

（１）クレジットカードに記録されているデータのうち、以下のもの。

①完全な磁気ストライプデータや IC チップ上の同等のデータ

②カード検証コード又は値

（２）個人識別番号（PIN)または PIN ブロック。

※「完全な磁気ストライプデータ」とは、磁気ストライプの全トラックデータ。

※「カード検証コード又は値」とは、カードを提示しない取引を検証するために使用される、署名欄若しくはその右側、又はクレジットカードの前面に印字されている 3 桁若しくは 4 桁の数値（CAV2/CVC2/CVV2/CID）。

※「個人識別番号（PIN）」とは、Personal Identification Number の略、暗証番号。

※「PIN ブロック」とは、PIN を伝送用にまとめた単位。

２．カード会員データ

クレジットカードに記録されているデータのうち、以下のもの。

（１）カード番号（PAN）

（２）有効期限

（３）カード会員名

（４）サービスコード

３．カード情報

センシティブ認証データおよびカード会員データの総称。

４．スマートフォン等

汎用モバイル OS を搭載し、アプリケーションやソフトウェアを継続的に更新することが可能な無線通信機能を有している、携帯可能な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、タブレット。

５．スマートフォン決済

スマートフォン等にカードリーダーを装着させ又は無線等により接続してクレジット決済端末として使用する決済のしくみ。

６．スマートフォン決済アプリケーション

スマートフォン決済を実現するためにスマートフォン等の上で動作するアプリケーション。

７．スマートフォン決済センター機能

スマートフォン等とカード会社の間に介在し、売上承認業務及び売上処理業務等の決済処理のうち、暗号化データの複合化、スマートフォン決済アプリケーションの認証など、スマートフォン決済特有の処理を行う機能。

８．スマートフォン決済提供事業者

スマートフォン決済センター機能、スマートフォン決済アプリケーション及びカードリーダーを組み合わせて決済手段を提供もしくは構築する事業者。(加盟店自らが構築している場合を除く。)

９．適切な鍵管理を伴う安全な暗号アルゴリズム及び鍵長

CRYPTREC の調査結果等で推奨されている暗号アルゴリズム及び鍵長。

９．１．CRYPTREC

CRYPTography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。

10．対面取引

会員と加盟店（自動精算機等含む）が対面し、加盟店が直接カード現物を確認できる状態で行う取引。

11．対面電文

取引電文の中に磁気ストライプもしくは IC チップから読み込んだカード情報が含まれている電文。

12．ワイヤレス通信

モバイル回線や無線 LAN 等に代表されるスマートフォン等で利用可能な無線方式。

12．１．モバイル回線

携帯電話キャリアの提供する無線通信サービスの総称。

13．PCI DSS

クレジットカード情報及び取引情報を保護するために 2004 年 12 月、JCB・American Express・Discover・マスターカード・VISA の国際ペイメントブランド 5 社が共同で策定した、クレジットカード業界におけるグローバルセキュリティ基準。

14. PCI-PTS

個人識別番号(PIN）を使用するクレジットカード取引のセキュリティを保証するため、PCI‐SSC が規定した PIN 入力を受け付けるデバイスに適用される国際的なセキュリティ基準。

第３章　セキュリティガイドライン

１．カード情報の保護

１．１．スマートフォン等に関するセキュリティ

アクワイアラーは、スマートフォン決済におけるスマートフォン等の不正な利用を防ぐため、使用するスマートフォン等が特定されるよう、加盟店が以下の要件に対応していることを確認する。

（１）スマートフォン等の認証

・加盟店又はスマートフォン決済提供事業者によるスマートフォン等の認証が行われていること。

・認証の方法は、機器メーカー、通信キャリア等が管理する個体番号等に依存しない、加盟店又はスマートフォン決済提供事業者独自の方法によるものであること。

１．２．スマートフォン決済アプリケーションに関するセキュリティ

アクワイアラーは､不正なスマートフォン決済アプリケーションによる処理を防ぐため、スマートフォン決済アプリケーションについて、加盟店が以下の要件に対応していることを確認する。

（１）カード情報の保護

①データ保存の禁止

・カード情報は、スマートフォン等の本体及び周辺機器並びに外部メモリへ保存しないこと。

ただし、暗号化されたカード情報の、承認処理完了前の一時的なスマートフォン等の本体への保存であって、クレジットカード取引に係る一般的な時間をもとに設定した合理的な制限時間を経過した後の自動的な消去が設定されている場合を除く。

②確実なデータ消去

・一時的に保存されたカード情報の消去は、任意のデータ又はランダムデータによる上書き等、元のデータを復元できないよう確実に消去されること。

③カード番号の非表示

・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（通常、先頭6桁及び末尾4桁以外）が非表示化されること。

（２）不正利用の防止

①スマートフォン決済アプリケーションの安全な配布と認証

・スマートフォン決済アプリケーションは､予め定められた安全な方法でのみ配布され、クレジットカード取引に関する処理の都度、適正であるか認証されること。

②スマートフォン決済アプリケーションの遠隔操作機能の実装

・スマートフォン決済アプリケーションは、遠隔操作による停止または削除が可能な機能を有するものであること。

（３）スマートフォン決済アプリケーションの保護

・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は、予め同アプリケーションが許容しているものを除き、他アプリケーションからはアクセス不可であること。

１．３．周辺機器のセキュリティ

アクワイアラーは、スマートフォン決済に必要な周辺機器におけるセキュリティ確保のため、加盟店が以下の要件に対応していることを確認する。

（１）カードリーダーのセキュリティ

①データ読込時のデータ保護

・データ読込みの直後に、適切な鍵管理を伴う、安全な暗号アルゴリズム及び鍵長を用いた暗号化が行われること。

・カードリーダーのハードウェア自体には、読込データを保存できないこと。

②IC カードリーダーのセキュリティ

・IC カードリーダーは、EMV4.2 Book2-Security and key Management “11.1 Security Requirements”以上の要件を満たしていること。

（２）PIN パッドのセキュリティ

・PIN 入力方式は、PCI-PTS 認定の要件に準拠していること。

１．４．ワイヤレス通信におけるセキュリティ

スマートフォン決済では、スマートフォン等とスマートフォン決済センター機能の間又は周辺機器とスマートフォン等との間におけるワイヤレス通信によるデータ伝送が想定されることから、アクワイアラーは、データの適切な保護のため、加盟店が以下の要件に対応していることを確認する。

（１）スマートフォン等とスマートフォン決済センター機能間のワイヤレス通信

・スマートフォン等とスマートフォン決済センター機能間のデータ伝送においては、以下の対応が図られていること。

①伝送するカード情報のデータ自体の暗号化が行われていること。その方法は、適切な鍵管理を伴う、安全な暗号アルゴリズム及び鍵長を用いたものであること。

②通信路の暗号化が行われていること。その方法は、PCI DSS（要件 4）に準拠していることが望ましい。

③通信プロトコルは、PCI DSS（要件 4）で規定されている認証及び暗号技術が用いられていること。

④Bluetooth を使用する場合、スマートフォン決済に関係ない不特定多数の機器との通信を防ぐ手段が講じられていること。

（２）スマートフォン等と周辺機器間のワイヤレス通信

・カードリーダー（IC カードリーダーを含む）、もしくは PIN パッドで取り込んだデータをスマートフォン等へ送信する場合、又は、スマートフォン等からプリンターに印字データを送信する場合は、送信するカード情報のデータ自体が、適切な鍵管理を伴う、安全な暗号アルゴリズム及び鍵長を用いた方法により暗号化されていること。

・上記に加え、以下の対応が図られていることが望ましい。

①通信路が、PCI DSS（要件 4）で規定されている方法により暗号化されていること。

②通信プロトコルは、PCI DSS（要件 4）で規定されている認証及び暗号技術が用いられていること。

③Bluetooth を使用する場合、スマートフォン決済に関係ない不特定多数の機器との通信を防ぐ手段が講じられていること。

・ただし、上記 2 つの対応は、カード情報が含まれない印字データがプリンターに送信される場合を除く。

１．５．加盟店のセキュリティ

アクワイアラーは、加盟店がスマートフォン決済を行ううえで必要なセキュリティを担保するため、スマートフォン決済センター機能の範囲において PCI DSS に準拠していることを確認する。

なお、加盟店がスマートフォン決済提供事業者のサービスを利用している場合は、当該スマートフォン決済提供事業者の対応を確認する。

２．運用・管理

２．１．スマートフォン決済の管理

アクワイアラーは、スマートフォン決済に関連する不正利用又は不具合等が発生した場合に、速やかに当該端末の特定が可能となるよう、スマートフォン等の管理について、加盟店が以下の要件に対応していることを確認する。

（１）スマートフォン等に関する情報の管理

・加盟店において、スマートフォン等及びスマートフォン決済アプリケーションに係る個体番号並びにスマートフォン決済の利用範囲が把握され、変更等が生じた場合は速やかにアクワイアラーに連絡されること。

・加盟店がスマートフォン決済提供事業者のサービスを利用している場合においても、同様の対応が図られること。

（２）スマートフォン決済の利用範囲

・スマートフォン決済は、アクワイアラーと加盟店において予め定められた業務範囲内での利用に限定されていること。

２．２．本人確認・売上処理時の対応

アクワイアラーは、スマートフォン決済を行う加盟店において、不正利用防止、関係法令の遵守等の観点から、適正な売上処理を実施するため、本人確認及び売上処理時の対応について、加盟店が以下の要件に対応していることを確認する。

（１）本人確認

スマートフォン決済における本人確認について、以下の内容を満たす措置がとられていること。

・IC カードによる売上処理を行った場合の PIN 入力による本人確認。

・磁気ストライプカードによる売上処理を行った場合の、カード会員による売上票への署名取得及びカード裏面の署名と同一である旨の確認。

（２）売上処理時の対応

関係法令を踏まえた必要な措置の確保のため、加盟店において、売上処理完了後、カード会員に対し売上票等が適切に提供されていること。

２．３．スマートフォン決済の運用の実効性確保

アクワイアラーは、加盟店が本ガイドラインに記載した各種安全対策基準等の実効性確保のため、加盟店の社内への十分な周知等が図られていることを確認する。

また、アクワイアラーは、加盟店がスマートフォン決済提供事業者のサービスを利用してスマートフォン決済を導入する場合は、当該スマートフォン決済提供事業者が本ガイドラインに記載した各種安全対策基準等を満たしたサービスを提供できることを自ら確認する。

２．４．スマートフォン決済提供事業者のサービスを利用している加盟店における運用の実効性確保のための留意事項

アクワイアラーは、スマートフォン決済提供事業者のサービスを利用している加盟店において、スマートフォン決済の運用上発生する障害・不具合等のトラブルに関する対応と責任分担等について、当該スマートフォン決済提供事業者と予め取り決めていることを確認する。

①スマートフォン決済提供事業者の行為に起因して発生した加盟店契約違反への対応。
②スマートフォン決済固有のツールの故障又は障害等に起因して売上阻害が発生した場合の代替手段。
③スマートフォン決済に起因して発生したカード情報等の漏洩事故への対応。
④スマートフォン決済に関するツール・ネットワークに関する問合せ又は不具合等への対応
⑤スマートフォン決済に関連する不正利用、情報漏洩等の事故が発生した場合におけるスマートフォン決済アプリケーションの停止。
⑥加盟店との間でスマートフォン決済に係る疑義・紛争等が生じた場合の対応。

以上