クレジットカード・セキュリティガイドライン【2.0版】
概要版

【2021年3月】

クレジット取引セキュリティ対策協議会
（事務局　一般社団法人日本クレジット協会）

改定ポイント

〈クレジットカード情報保護対策〉

- 割賦販売法の改正により拡充されたクレジットカード番号等取扱業者に対するクレジットカード・セキュリティガイドラインにおけるセキュリティ対策のとりまとめ

〈非対面取引における不正利用対策〉

- 加盟店における非対面不正利用対策の具体的方策にEMV 3-Dセキュアの説明を追記
- イシュアー、アクワイアラー、PSPに求められる対応を追記

改定ポイント① クレジットカード情報保護対策

□割賦販売法の改正により拡充されたクレジットカード番号等取扱業者に対するクレジットカード・セキュリティガイドラインにおけるセキュリティ対策のとりまとめ

◆**「決済代行業者等」** ※シート25参照

○**定義**

以下のいずれかの業務を行う決済代行業者（PSP含む）※1、ECモール 、ECシステム提供会社※2等の事業者の総称。

①特定のアクワイアラーのために加盟店に立替払いをする業務。

②加盟店のためにカード情報をアクワイアラーに提供（当該アクワイアラー以外の者を通じた提供を含む。）する業務。

※1 ここでいう決済代行業者は、インターネット上の取引においてEC加盟店にクレジットカードスキームを提供し、カード情報を処理する事業者であるPSPと、インターネット以外の取引において加盟店にクレジットカードスキームを提供し、カード情報を処理する事業者をいう。

※2 ここでいうECシステム提供会社は、アクワイアラーとの契約有無にかかわらず、決済システムを運営しEC加盟店にサービスとして提供する事業者をいう。ASP/SaaSとしてEC加盟店にサービス提供する形式や、EC加盟店に購入プラットフォームを提供する形式等がある。

◆**「決済代行業者等」** ※シート25参照

○**求められる対策**

・PCI DSSに準拠し、これを維持・運用する。【指針対策】

・非保持化（非保持と同等/相当を含む）の対策を講じている対面取引は、当該対策に加え、リスクに応じた必要なセキュリティ対策を講じるとともに、適切な管理運営を行う。【指針対策】

・加盟店の取組を支援するため、加盟店に対しカード情報保護対策について必要な助言や情報提供等を実施する。なお、カード会社（アクワイアラー）と契約を有する決済代行業者等については、カード会社（アクワイアラー）と連携して対応する。

改定ポイント② クレジットカード情報保護対策

◆**「コード決済事業者等」** ※シート26参照

○**定義**

以下のいずれかの業務を行う事業者。

①カード会員からカード情報の提供を受けてQRコードや決済用のID※等対面取引・非対面取引の決済に用いることができる情報と結び付け、カード会員に当該情報を提供する業務。

②上記①の事業者から委託を受けてカード情報を他の決済情報により特定できる状態で管理する業務。

※ カード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）が事前に登録された際に、カード会員データの代わりにクレジットカード決済が可能となるID又は番号を指す。

○**求められる対策**

・PCI DSSに準拠し、これを維持・運用する。【指針対策】

・また、コード決済事業者等から委託を受けてカード情報を他の決済情報により特定できる状態で管理している事業者についてもPCI DSSに準拠し、これを維持・運用する。【指針対策】

改定ポイント③ 非対面取引における不正利用対策

□加盟店における非対面不正利用対策の具体的方策にEMV 3-Dセキュアの説明を追記

※シート45、46参照

・現在の3-Dセキュア1.0に比較して、カード会員のデバイス情報等に加え、加盟店がカード会員の同意を得て、カード会員及び取引情報をカード会社（イシュアー）に提供することにより、カード会社（イシュアー）がリスク評価（リスクベース認証）を実施することができるようになることから、不正利用の判定の精度が向上する。
・EMV 3-Dセキュアでは、カード会社（イシュアー）によるリスク評価により不正利用の可能性が低いと判断される取引については、カード会員にパスワード入力を求めない対応も可能となる。この低リスクの取引に対してパスワードの入力を求めないことは、利用者のパスワード忘れ等により発生していた「かご落ち」の解消に資するものである。

改定ポイント④ 非対面取引における不正利用対策

□カード会社（イシュアー）に求められる対応を追記 ※シート48、49参照

◆EMV 3-Dセキュアへの対応

・カード会社（イシュアー）は、加盟店がカード会員の同意を取得した上で加盟店から提供を受けるカード会員に関する情報を用いることにより本人認証精度が向上する。3-Dセキュアにおいては、現行のバージョン1.0より精度の向上したEMV 3-Dセキュアを早期に導入する。

◆「3-Dセキュア1.0」におけるリスクベース認証

・3-Dセキュア1.0におけるリスクベース認証は、加盟店から提供される利用者情報や取引情報、デバイス情報等を活用したリスク評価により、不正利用を判別する精度を高めることを目的としたものである。カード会員にパスワード入力を求める取引を最小限にすることも期待できることから導入が求められる。EMV 3-Dセキュアに移行するまでの間、バージョン1.0で対応する場合にはリスクベース認証を導入する。

◆「動的パスワード」への移行と利用登録率の推進

・EMV 3-Dセキュアを導入するまでの間に3-Dセキュア1.0で対応する場合には、「静的（固定）パスワード」から「動的（ワンタイム）パスワード」への移行が求められる。なお、「動的（ワンタイム）パスワード」を活用する場合には、カード会員に対する利用環境の整備を促進する。

◆デバイス認証（生体認証等）

・生体情報による認証は、必ずしもイシュアーがカード会員の生体情報を保有する必要はなく、クレジットカード情報と生体情報をスマートフォン等のデバイスに登録する際に、確実な本人認証が行われていれば、その後の当該デバイスによるクレジットカード利用時において登録された生体情報の認証等も認められる。

◆クレジットカードと連携するコード決済事業者等に対する多面的・重層的な対策の実施

・クレジットカードを、コード決済事業者等が提供する他の決済サービスと連携（紐づけ）する取引は、非対面不正利用によりクレジットカードを連携された場合、反復的に不正にチャージがなされ、また、不正なクレジットカード決済が行われ、高額な不正利用被害が発生する蓋然性がある。このことから、クレジットカードと連携する取引の時点で、イシュアーはオーソリゼーションによるモニタリング、セキュリティコードの照合、3-Dセキュアにおけるパスワード照合及びリスクベース認証等の取引の時点の対策を複数組み合わせることにより、セキュリティ対策を多面的・重層的に講じる必要がある。

改定ポイント⑤ 非対面取引における不正利用対策

□カード会社（アクワイアラー）・PSPに求められる対応を追記 ※シート51参照

◆EMV 3-Dセキュアへの対応
・EMV 3-Dセキュアの導入態勢を早急に整備し、加盟店に対して導入を求める必要がある。

◆クレジットカードと連携する決済サービスを提供する決済事業者等との契約時におけるセキュリティ対策の確認
・コード決済事業者等クレジットカードと連携することにより他の決済手段を提供する事業者と包括加盟店契約等を締結する場合には、当該事業者が一般社団法人キャッシュレス推進協議会がとりまとめた「コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン」や一般社団法人日本資金決済業協会がとりまとめた「銀行口座との連携における不正防止に関するガイドライン」等、関係するガイドラインに準拠するなど、十分な安全対策が講じられていることを確認する必要がある。

概要版

- はじめに
- 本ガイドラインの基本的な考え方
- Ⅰ．クレジットカード情報保護対策分野
- Ⅱ．不正利用対策分野
  - （A）対面取引におけるクレジットカードの不正利用対策
  - （B）非対面取引におけるクレジットカードの不正利用対策
- Ⅲ．消費者及び事業者等への周知・啓発

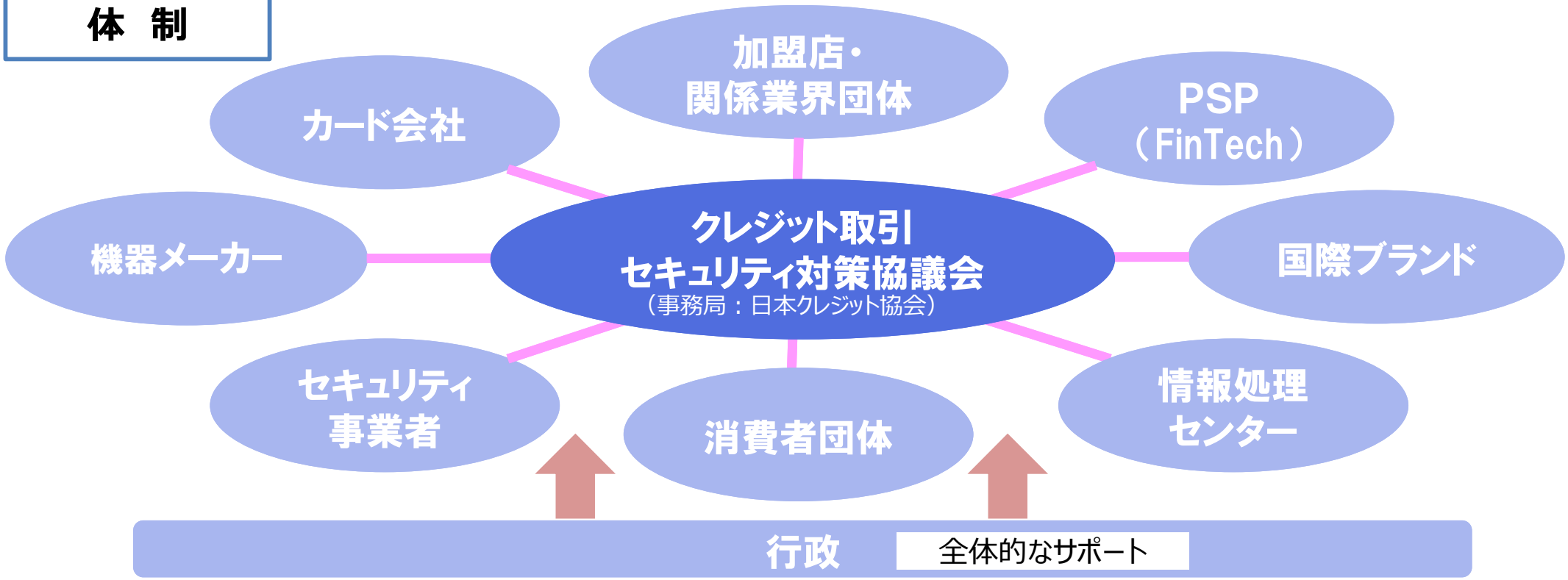
はじめに

はじめに①

クレジット取引セキュリティ対策協議会

- 本協議会は、我が国のクレジットカード取引において、**「国際水準のセキュリティ環境」**を整備することを目的として、クレジット取引に関わる**幅広い事業者及び行政等が参画**して設立された（2015年3月）。
- 本協議会では、「実行計画」（2016年2月～2019年3月）を策定し、セキュリティ対策の推進を図ってきた。
- 実行計画の対応期限経過後の2020年4月からも、関係事業者が実施するセキュリティ対策として「**クレジットカード・セキュリティガイドライン**」を策定（1.0版は2020年3月）し、引き続き安全・安心なクレジットカード利用環境の整備に取組む。

体　制



はじめに②

協議会　本会議メンバー

【委員】

（カード会社）	イオンクレジットサービス、SMBCファイナンスサービス、オリエントコーポレーション、クレディセゾン、ジェーシービー、ジャックス、トヨタファイナンス、三井住友カード、三菱UFJニコス、ユーシーカード、楽天カード
（加盟店）	ジャパネットホールディングス、 JTB、Ｊ.フロントリテイリング、三越伊勢丹ホールディングス、ヤフー、ユニー、ヨドバシカメラ、楽天
（決済代行業者(PSP)）	EC決済協議会
（機器メーカー）	NECプラットフォームズ、オムロンソーシアルソリューションズ
（情報処理センター）	NTTデータ
（セキュリティ事業者）	トレンドマイクロ、P.C.F. FRONTEO
（消費者団体）	全国消費者団体連絡会
（学識経験者）	笠井修・中央大学法科大学院教授（本会議議長）、田中良明・早稲田大学教授

【オブサーバー】

（国際ブランド）	アメリカン・エキスプレス・インターナショナル、ビザ・ワールドワイド・ジャパン、マスターカード・ジャパン、三井住友トラストクラブ[Diners Club] 、UnionPay International Co.,Ltd[銀聯国際]
（団体事務局）	日本チェーンストア協会、日本通信販売協会、日本百貨店協会
（官庁）	経済産業省

本ガイドラインの基本的な考え方

本ガイドラインの基本的な考え方①

１．本ガイドラインにおけるセキュリティ対策の対象について

■ 本ガイドラインでは、「カード情報保護」と「不正利用防止」のため、クレジットカード取引の関係事業者が講ずべきセキュリティ対策を定めるとともに、その対策を有効に機能させるために取組むべき事項を記載している。

２．割賦販売法との関係性について

■ **本ガイドラインは**、「割賦販売法（後払分野）に基づく監督の基本方針」において割賦販売法で義務付けられているカード番号等の適切管理及び不正利用防止措置の**実務上の指針**として位置付けられるものであり、**本ガイドラインに掲げる措置又はそれと同等以上の措置**を講じている場合には、セキュリティ対策に係る法令上の基準となる**「必要かつ適切な措置」**を満たしていると認められる。

■ 本ガイドラインにおいては、同法で規定される措置に該当する部分を**【指針対策】**と記載している。

３．対象となる関係事業者について

■ 現時点ではセキュリティ対策の実施主体者である「加盟店」「カード会社（イシュアー・アクワイアラー）」「決済代行業者等」及び「コード決済事業者等」並びにこれらの事業者が対策を実施するに際し協力等を行う「機器メーカー」「ソリューションベンダー」「情報処理センター」「セキュリティ事業者」「国際ブランド」「業界団体」等のクレジットカード取引に関係する事業者を「関係事業者」としている。今後新たな決済スキームの進展や新たな事業者が登場し、これらのセキュリティ対策の検証が必要な場合には、関係事業者を追加する。

本ガイドラインの基本的な考え方②

４．対象となるクレジットカードについて

■ **国際ブランド付きのクレジットカード**
世界中で利用され、不正利用のリスクが高い。
⇒本ガイドラインでは、「**国際ブランド付きのクレジットカード**」を**対象**としている。

■ **国際ブランドが付いていないクレジットカード**
利用できる範囲が限定され、不正利用リスクが低い。
⇒本ガイドラインでは、対象とはしていないが、リスクに応じたセキュリティ対策が必要となる点に留意する。

５．関係事業者間の情報連携等について

■ 本ガイドラインのセキュリティ対策は、関係事業者間による緊密な連携、協力体制の下で実施されなければ実効性のあるものにはならない。

■ 各関係事業者は、本ガイドラインに基づく対策を講ずる場合には相互に必要なサポートや情報提供を行う体制を構築する必要がある。

６．消費者への情報提供について

■ 本ガイドラインのセキュリティ対策の有効性確保のためには、クレジットカード利用者である消費者自らの取組の実施が必要である。このため、各関係事業者は、消費者の理解及び取組の推進に向けた情報提供、周知活動に取組む必要がある。

本ガイドラインの基本的な考え方③

７．ガイドラインの最新性・実効性等について

- ■ カード情報の漏えい、不正利用の手口は時とともに巧妙化、多様化しており、セキュリティ対策の内容もそれに適したものでなければならない。
- ■ 本ガイドラインにおいても、カード情報漏えい、不正利用被害の発生状況、手口等を検証し、これらの発生防止や被害拡大防止に適した対策を求めていく。

Ⅰ．クレジットカード情報保護対策分野

Ⅰ．クレジットカード情報保護対策分野①

クレジットカード情報保護対策としては、加盟店はカード情報の非保持化（非保持と同等/相当を含む）又はPCI DSSの準拠を、カード会社やPSP等のカード情報を保有し処理等を行う事業者はPCI DSSの準拠が求められる。

１．各事業者に求められる対策等

（１）加盟店

- ■ カード情報を保持しない非保持化（非保持と同等/相当を含む）又はカード情報を保持する場合はPCI DSSに準拠する。【指針対策】
- ■ カード情報の窃取を企図する者の最新の攻撃手口等の情報を踏まえ、対策実施後も不断に自社のセキュリティ対策の改善・強化を図る。

【注1】カード情報について

カード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）及び機密認証データ（カード情報を含む全トラックデータ、CAV2/CVC2/CVV2/CIDいわゆるセキュリティコード、PIN又はPINブロック）をいう。
ただし、カード会員データのうち、クレジットカード番号以外のデータのみであれば「カード情報」ではない。

また、**以下の処理がなされたものはクレジットカード番号とは見做さない。**

①**トークナイゼーション**（自社システムの外でクレジットカード番号を不可逆的に別の番号等に置き換え、自社システム内ではクレジットカード番号を特定できないもの）
②**トランケーション**（自社システムの外でクレジットカード番号を、自社システム内では特定できない方法で安全に国際的な第三者機関に認められた桁数を切り落としたもの）
③**無効処理されたクレジットカード番号**

【注2】PCI DSSについて

Payment Card Industry Data Security Standardの略。
カード情報を取り扱う全ての事業者に対して国際ブランドが共同で策定したデータセキュリティの国際基準。

Ⅰ．クレジットカード情報保護対策分野②

❶加盟店に求められる対策

形 態		指針対策	
		外回り(非通過型) カード情報が自社で保有する機器・ネットワークを「保存」「処理」「通過」しない方式	**内回り(通過型)** カード情報が自社で保有する機器・ネットワークを「保存」「処理」「通過」する方式
非対面加盟店	EC加盟店	非保持化	PCI DSS準拠
	MO・TO加盟店	非保持化	非保持と同等/相当　又は　PCI DSS準拠
対面加盟店		非保持化	非保持と同等/相当　又は　PCI DSS準拠

【注】カード情報の保持とはならない例について

以下①～③の状態で保存する場合には、カード情報の**『保持』とはならない。**

①紙（クレジット取引伝票、カード番号を記したFAX、申込書、メモ等）

②紙媒体をスキャンした画像データ

③電話での通話記録（音声データを含む）

※1　上記①～③以外において**非保持化（非保持と同等/相当を含む）が実現されていることが前提** 。

※2　本ガイドラインにおいて上記①～③の状態でカード情報を保存する場合は「保持」とならないが、PCI DSS準拠を目指す加盟店においては、本ガイドラインの内容にかかわらず、PCI DSSに則って取組むことに留意する 必要がある。

Ⅰ．クレジットカード情報保護対策分野③

①非保持化対策

本ガイドラインで示す加盟店における「非保持化」とは、**自社で保有する機器・ネットワークにおいて「カード情報」を『保存』『処理』『通過』しないことをいう。**また、決済専用端末から直接外部の情報処理センター等に伝送している場合も「非保持」に該当する。

加盟店における対策導入事例（非保持（非保持と同等/相当））

加盟店		方策	概要	方式
非対面加盟店	①EC加盟店	リダイレクト（リンク）型	PSPの決済画面に遷移させカード決済を行う方式（決済画面はPSPのサイトへ遷移する）	外回り方式（非保持/非通過型）
		Java Script型（トークン型）	決済画面にPSPが提供するJava Scriptプログラムを組み込み決済を行う方式（決済画面は加盟店サイトから遷移しない）	外回り方式（非保持/非通過型）
	②MO・TO加盟店	決済専用端末を利用	CCT端末と同等以上のセキュリティレベルの決済専用端末を利用した外回り方式	外回り方式（非保持/非通過型）
		タブレット端末を利用	タブレット端末を利用した外回り方式	外回り方式（非保持/非通過型）
		非保持と同等/相当	PCI P2PE認定ソリューションを導入したカード情報暗号化による内回り方式	内回り方式（非保持と同等/相当）
③対面加盟店		決済専用端末連動型	決済専用端末から直接外部の情報処理センター又はASP事業者等に伝送される外回り方式	外回り方式（非保持/非通過型）
		ASP/クラウド接続型	決済専用端末から直接外部の情報処理センター又はASP/クラウドセンター等に伝送される外回り方式	外回り方式（非保持/非通過型）
		非保持と同等/相当	PCI P2PE認定ソリューションの導入又は本協議会がとりまとめたセキュリティ技術要件に適合するセキュリティ基準を満たしたカード情報の暗号化に対応した内回り方式	内回り方式（非保持と同等/相当）

Ⅰ．クレジットカード情報保護対策分野④

1）非対面加盟店における非保持化対策　a）EC加盟店の対策

・非対面加盟店における非保持化は、不正アクセスによる外部への情報漏えい被害の極小化に有効。

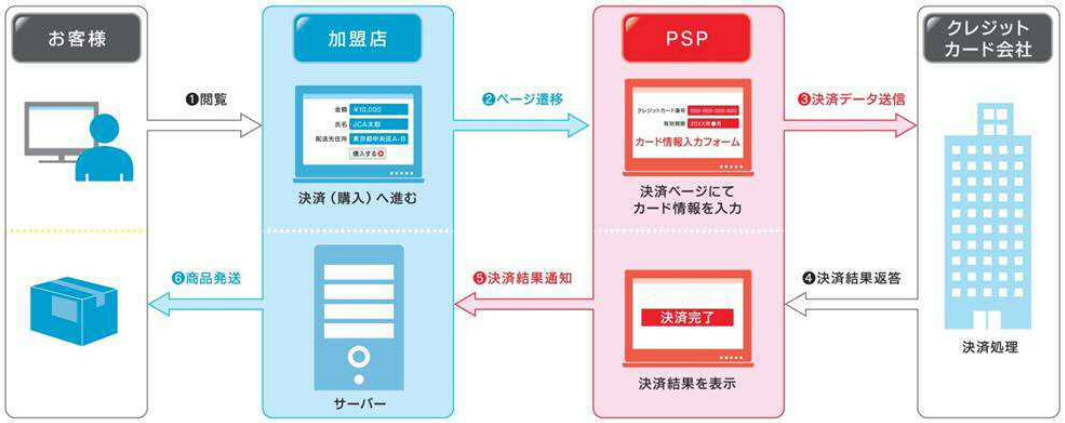
・本ガイドラインにおいて例示する方式により、非保持化の実現が可能である。

■EC加盟店における非保持化 導入例

◆非保持化：非通過型（「リダイレクト（リンク）型」又は「Java Script型（トークン型）」）の決済システムの導入

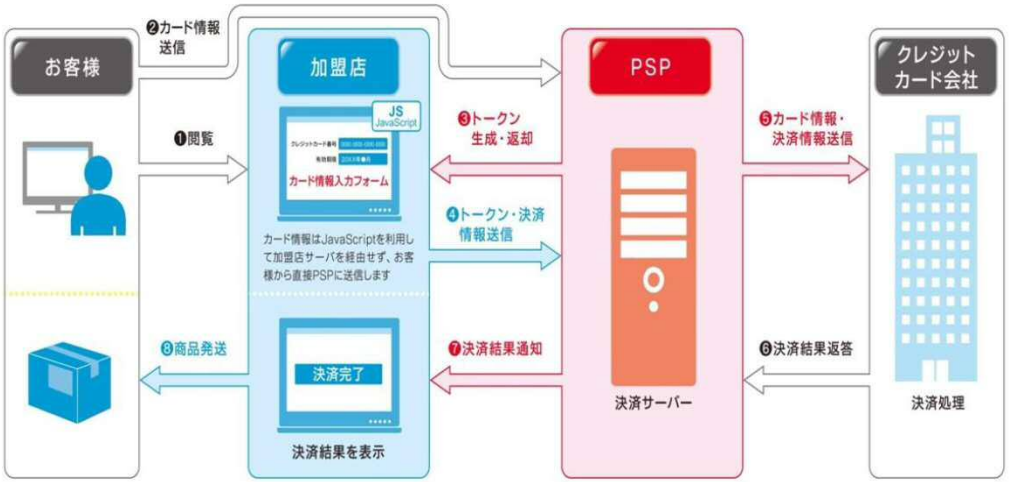
➢リダイレクト（リンク）型

（決済画面はPSPのサイトへ遷移する）



➢Java Script型（トークン型）

（決済画面は加盟店のサイトから遷移しない）



※トークンは、クレジットカード情報を代替するパラメータです。加盟店はお客様がPSPに送信したカード情報を元に生成されたトークンを利用して決済を行います。

ECサイトの開発・運用段階での以下リスクへのセキュリティ対策が不十分であることにより、カード情報漏えい事案が発生している近時の傾向を踏まえ、自社システムの絶え間ない点検と脆弱性対策に万全を期すことが重要

・管理画面へのアクセス制御が適切に行われていないなど、ウェブサイトの開発・運用段階での設定の不備

・ ECサイトの脆弱性や委託先事業者が提供する決済ソリューション（ショッピングカート機能等）の脆弱性等

・ ECサイトの改ざん、偽の決済画面への誘導など不正犯の巧妙化した新たな攻撃手口

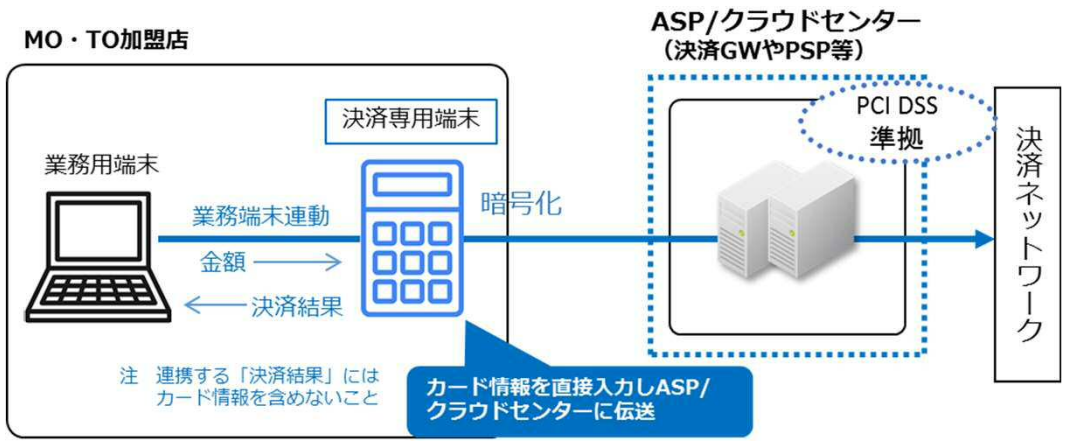
Ⅰ．クレジットカード情報保護対策分野⑤

1）非対面加盟店における非保持化対策　b）MO･TO加盟店の対策

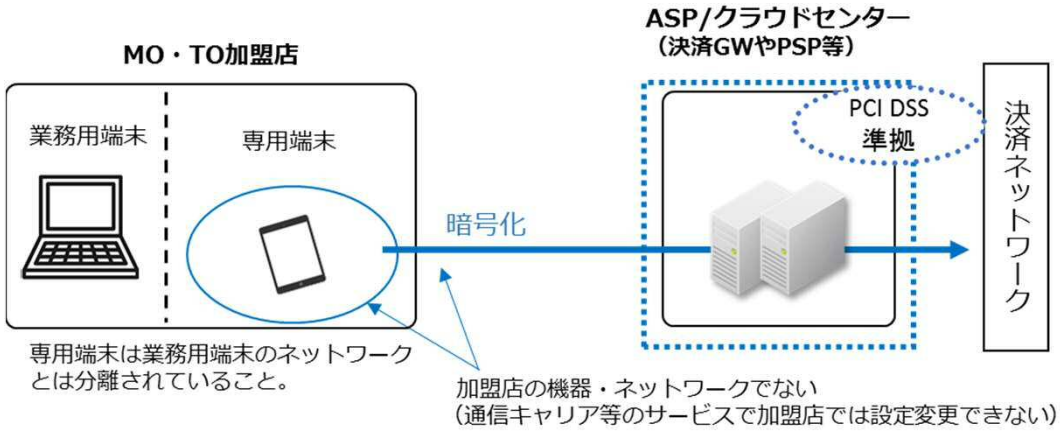
■MO･TO加盟店における非保持化（非保持と同等/相当を含む）導入例

◆非保持化：要件を満たした決済専用端末やタブレット端末を活用した外回り方式の導入

➢決済専用端末を利用した外回り方式

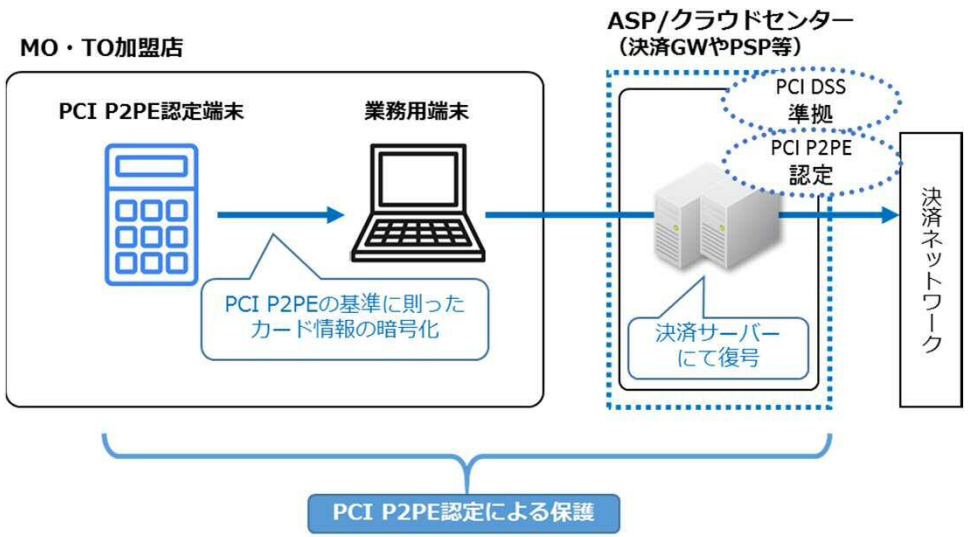


➢タブレット端末を利用した外回り方式



◆非保持と同等/相当：PCI P2PE認定ソリューションの導入

➢PCI P2PE認定端末を利用した内回り方式



※これら非保持化、非保持と同等/相当の詳細については、「【追補版】メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて」を参照

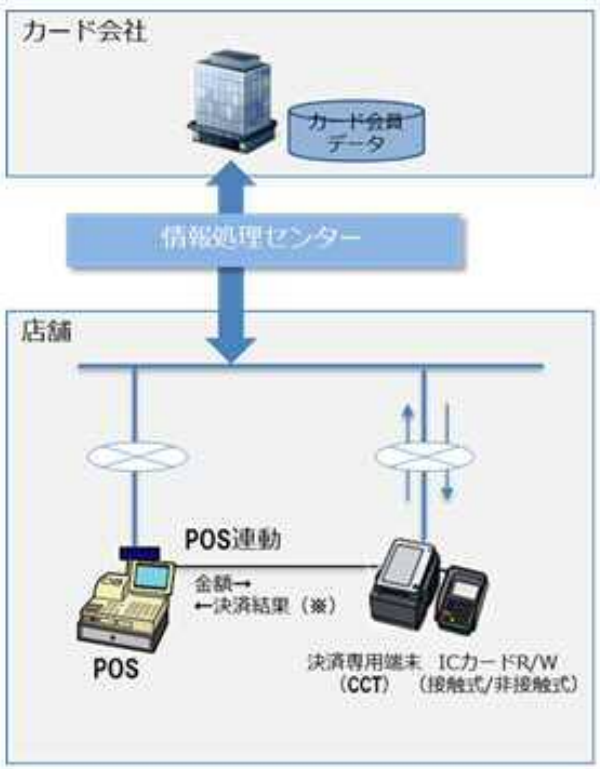
Ⅰ．クレジットカード情報保護対策分野⑥

2）対面加盟店における非保持化対策

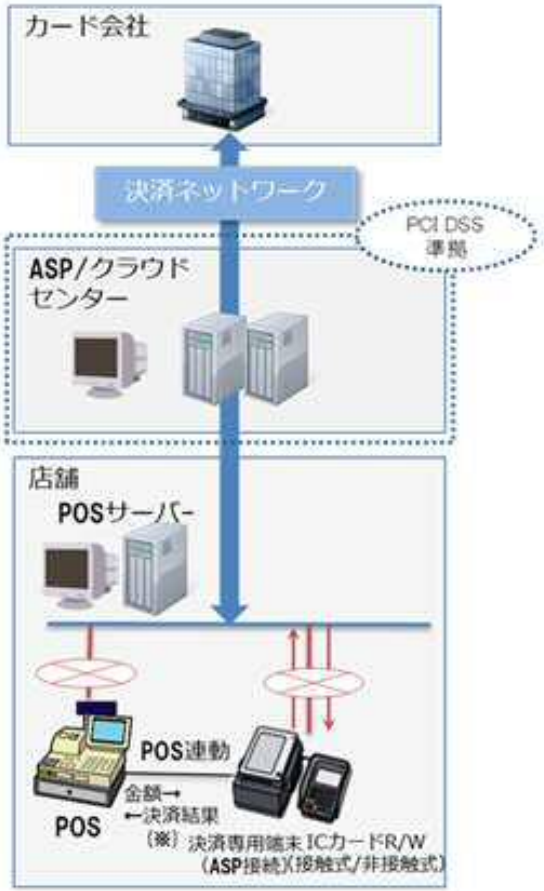
■対面加盟店における非保持化 導入例

◆非保持化：非決済専用端末から直接外部の情報処理センター又はASP/クラウドセンター等に伝送される方式
※POSに連動する決済結果には「カード情報」は含めないことが前提

➢決済専用端末連動型（外回り）



➢ASP/クラウド接続型（外回り）



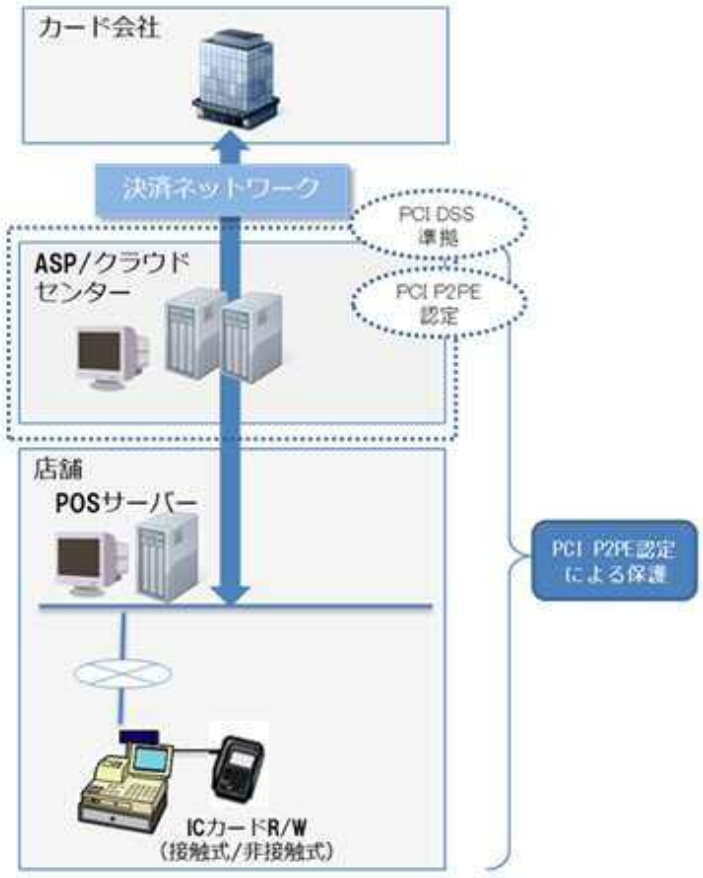
Ⅰ．クレジットカード情報保護対策分野⑦

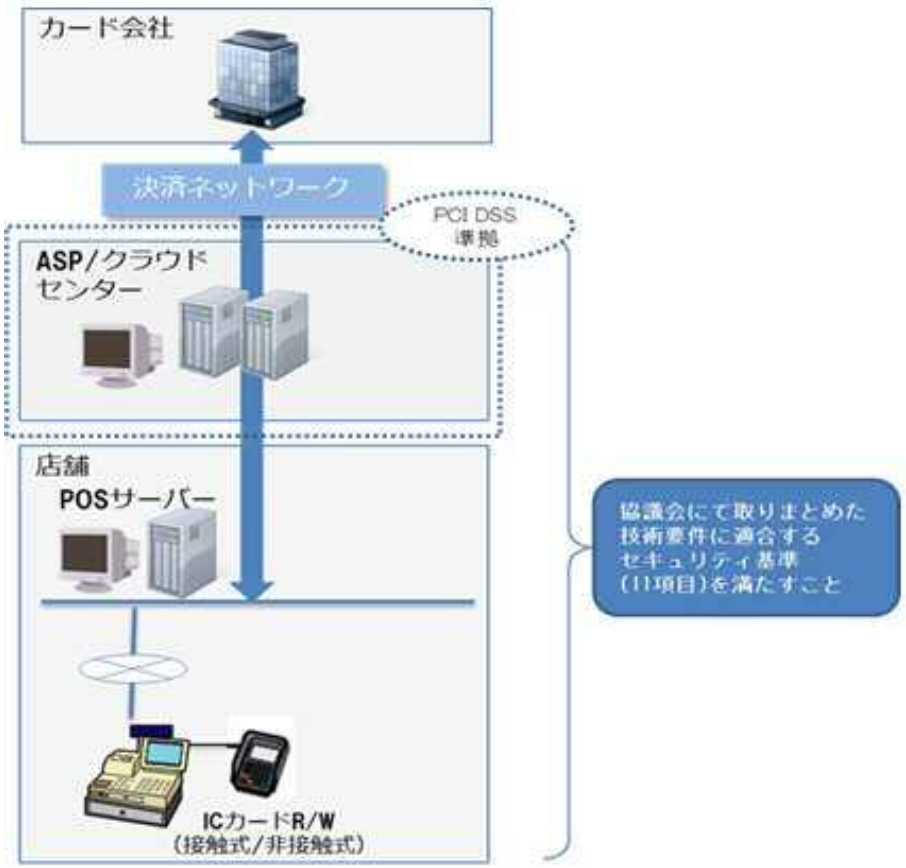
2）対面加盟店における非保持化対策

■対面加盟店における非保持と同等/相当 導入例

◆非保持と同等/相当：PCI P2PE認定ソリューションの導入又は本協議会においてとりまとめた技術要件に適合するセキュリティ基準（11項目）を満たすこと

➢ASP/クラウド接続型（内回り）





※詳細については「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」を参照

Ⅰ．クレジットカード情報保護対策分野⑧

３）非保持化対策における留意点

a）非保持化を実現した加盟店における顧客からの照会等への対応

顧客照会等の際、以下を利用して一時的にクレジットカード番号を入手・利用することが認められる。
①クレジットカード取引に係る紙伝票（加盟店控え、お客様控え）等の紙媒体
②紙媒体をスキャンした画像データ
③電話での通話記録（音声データを含む）
④PCI DSSに準拠したASP事業者が提供するセキュリティ対策が施された環境へのアクセスによる照会
※運用上の課題については各加盟店、カード会社、必要に応じてASP事業者等が連携の上、個別に検討を進めることが重要

b）過去に取り扱ったカード情報の保護対策

過去のカード情報が以下要件を全て満たす場合、当該カード情報をテキスト形式等の電子帳簿として保存していても保持とはならない。
①電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律に基づく管理を求められている
②非保持化対応完了以前に取り扱った過去のカード情報である
③本協議会にて定めたセキュリティ対策※が行われている
※ネットワークを利用しない「スタンドアローン環境」で保管・利用することが必須条件
詳細については、「非保持化実現加盟店における過去のカード情報保護対策」を参照

c）非保持化を実現した加盟店におけるセキュリティ対策

非保持化実現後も以下の情報漏えい防止のための継続的なセキュリティ対策が求められる。
・情報保護に関する従業員教育
・ウイルス対策
・デバイス管理　等

Ⅰ．クレジットカード情報保護対策分野⑨

②PCI DSS準拠

加盟店はカード情報を保持する場合にはPCI DSSに準拠しなければならない。PCI DSSは安全なネットワークの構築や、カード会員データの保護等の12の要件に基づく約400の要求事項から構成されているが、加盟店の業態、システム・ネットワーク構成に応じ要求項目が異なることから、自社が対応するべき事項を検証し、準備する必要がある。

（2）カード会社（イシュアー・アクワイアラー）

- カード会社（イシュアー・アクワイアラー）は、外部からの不正侵入やカード情報の外部への漏えい等といった外的脅威によるリスクを極小化し、かつ予見される様々なリスクに厳格に対処するためPCI DSSに準拠し、これを維持・運用する。このほか、関係法令・ガイドライン等を参照し、リスクに応じた必要なセキュリティ対策を講じるとともに、適切な管理運営を行う。【指針対策】
- カード会社（アクワイアラー）は、契約のある決済代行業者等と連携し、加盟店に対し非保持化（非保持と同等/相当を含む）又はPCI DSS準拠について必要な助言や情報提供等を行う。
- カード会社（イシュアー）は、フィッシングやウイルス感染、ECサイト改ざんによる不正画面への遷移等、カード　会員から直接カード情報等を窃取する手口について、消費者に対する注意喚起及びセキュリティ対策の必要性等の啓発を行う。

（3）決済代行業者等

- 決済代行業者等は、PCI DSSに準拠し、これを維持・運用する。【指針対策】
- 非保持化（非保持と同等/相当を含む）の対策を講じている対面取引は、当該対策に加え、リスクに応じた必要なセキュリティ対策を講じるとともに、適切な管理運営を行う。【指針対策】
- 決済代行業者等は、加盟店の取組を支援するため、加盟店に対しカード情報保護対策について必要な助言や情報提供等を実施する。なお、カード会社（アクワイアラー）と契約を有する決済代行業者等については、カード会社（アクワイアラー）と連携して対応する。

Ⅰ．クレジットカード情報保護対策分野⑩

（4）コード決済事業者等

- コード決済事業者等は、PCI DSSに準拠し、これを維持・運用する。【指針対策】
- また、コード決済事業者等から委託を受けてカード情報を他の決済情報により特定できる状態で管理している事業者についてもPCI DSSに準拠し、これを維持・運用する。【指針対策】

（5）その他関係事業者等

①国際ブランド

- 本ガイドラインに掲げるカード情報保護対策の実現に向け、国際ブランドの各種ルール等との調整を行い、各種課題の解決に向けて関係事業者と協働して取組む。
- グローバルな観点から、海外におけるカード情報保護に関するリスクや各種課題、我が国における国際水準のセキュリティ環境の整備の必要性等について、事業者向けの情報共有・発信に取組む。

②ソリューションベンダー

- 非保持化加盟店に対し決済端末やソリューション等を提供する立場から、本ガイドラインに基づく非保持の状態が維持されるように、各事業者が連携の上、端末やソリューション等の機能・仕様面で情報漏えい防止のための必要なセキュリティ対策を講じる。

③行政

- 割賦販売法に基づく監督等を通じ、カード会社及び加盟店等におけるカード情報の適切な管理のために必要な措置の適確な実施について指導等を行う。また、本ガイドラインに掲げるカード情報保護対策の実施について、事業者向けや消費者向けの情報発信に取組む。

Ⅰ．クレジットカード情報保護対策分野⑩

④業界団体

- 日本クレジット協会は、カード会社（アクワイアラー）と連携し、本ガイドラインに掲げるカード情報保護対策の必要性について加盟店に対する周知活動を徹底するとともに、加盟店の業界団体、消費者団体及び関連団体（一般社団法人キャッシュレス推進協議会、EC決済協議会、一般社団法人Fintech協会）等との連携を強化し、 事業者向けの情報発信に取組む。
- 日本クレジット協会は、行政と連携の上、他の情報セキュリティに係る関係機関との連携・情報共有を図り、クレジット取引に関係する事業者等に対して適時情報発信を行う。
- 政府の情報セキュリティ政策会議において、クレジット分野は、国の重要インフラの一つに指定されており、「重要インフラ情報セキュリティ第4次行動計画」（2020年1月30日付改定）に基づき、官民連携による重要インフラ防護を推進していく。具体的な取組としては、「クレジットCEPTOARにおける情報セキュリティガイドライン」に基づき、重要インフラ事業者における安全基準等の整備・浸透、情報共有体制の強化等を図る。

Ⅰ．クレジットカード情報保護対策分野⑪

２．その他留意事項

（１）カード情報の取扱い業務を外部委託する場合の留意点と受託者における必要な対策

- セキュリティ対策の実施主体者である関係事業者（加盟店、カード会社、決済代行業者等、コード決済事業者等）は、カード情報を取り扱う業務を外部委託する場合は、委託者自身が委託先のセキュリティ状況を確認し、責任を持ってPCI DSS準拠等の必要な対策を求める。
- 特に、複数の委託者からカード情報を取り扱う業務を受託する事業者においては、カード情報が漏えいした場合の影響が大きいため、また、ショッピングカート機能等のシステムを提供する事業者においては、ショッピングカート部分の脆弱性からフィッシング等によりカード情報が漏えいする事案が多発していることから、自社システムにおけるカード情報の保持状況について確認の上、PCI DSS準拠等の必要なカード情報保護対策等を行う。

（２）カード情報漏えい時の対応

- 加盟店からカード情報が漏えいした際は、取引に関係するカード会社及び決済代行業者等は、日本クレジット協会において策定した「クレジットカード情報漏えい時および漏えい懸念時の対応要領」を有事の際の参考にしつつ、二次被害の防止のために必要な措置を講ずることとする。
- また、カード情報の漏えい事案が発生した加盟店は、被害の拡大を防止するために初動対応として漏えい元（データベース等）のネットワークからの切り離し、カード決済の一時停止等の措置、フォレンジック調査、PCI DSS 準拠等の再確認及び再発防止のための適切な措置を講ずる。
- 契約元のカード会社（アクワイアラー）等は、漏えい事案が発生した加盟店のカード決済の再開にあたっては、SAQ等の提出内容や再発防止のための措置等の対応状況を十分に確認した上で、判断する必要がある。なお、PCI DSS準拠等の再発防止のための適切な措置の具体的な内容は、当該加盟店と契約カード会社（アクワイアラー）等で協議の上、決定することとする。

Ⅰ．クレジットカード情報保護対策分野⑫

附属文書一覧

No	文書名	目的・概要
1	【追補版】メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて	メールオーダー・テレフォンオーダー（MO・TO）加盟店における「非保持化（非保持と同等/相当を含む）」の取組を推進するため、具体的な方策例についてとりまとめたもの。
2	対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について	内回り方式を採用する対面加盟店において、「非保持と同等/相当」のセキュリティ確保を実現するため求められる11の想定リスクに対応したセキュリティ対策措置（暗号化、アクセス制限等）をとりまとめたもの。
3	非保持化実現加盟店における過去のカード情報保護対策	電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律に基づき、過去のカード情報を含む電子帳簿について非保持化が困難な場合があることを踏まえ、「スタンドアローン環境」での保管・利用などの措置内容を取りまとめたもの。

Ⅰ．クレジットカード情報保護対策分野⑬

関係文書

No	文書名	目的・概要
1	クレジットカード情報の漏えい時および漏えい懸念時の対応要領	クレジットカード取扱加盟店からクレジットカード情報が漏えいした、又は漏えいの懸念がある場合の、対応ポイントをまとめたもの。

Ⅱ．不正利用対策分野
（A）対面取引におけるクレジットカードの不正利用対策

Ⅱ．（A）対面取引におけるクレジットカードの不正利用対策①

クレジットカード偽造防止等による不正利用対策としては、窃取した情報を用いた偽造ICチップの生成は困難であること等から、IC取引の実現が現状の技術水準では最も効果的な対策であり、カード会社はクレジットカードのIC化、加盟店は決済端末のIC対応が求められる。

１．各事業者に求められる対策等

（１）加盟店

- IC取引を可能とするため設置する決済端末の全てをIC対応する。【指針対策】
- 特に、POSシステムでクレジットカード決済を行う加盟店は、自社のIC対応に係る実現方式を選択する際には、カード会社（アクワイアラー）や機器メーカー等に情報を求める。

□加盟店における指針対策の実現方法

加盟店	指針対策の実現方法
POSシステムで決済を行う	次の3つの実現方式によるPOSシステムでのIC対応 1）決済専用端末（CCT）連動型 2）決済サーバー接続型 3）ASP/クラウド接続型
POSシステム以外で決済を行う	IC対応した決済専用端末（CCT）の導入
特定業界	以下附属文書に基づきIC対応する 1）国内ガソリンスタンドにおけるICクレジットカード取引対応指針 2）オートローディング式自動精算機のIC対応指針と自動精算機の本人確認方法について

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策②

①POSシステムのIC対応に係る実現方式例

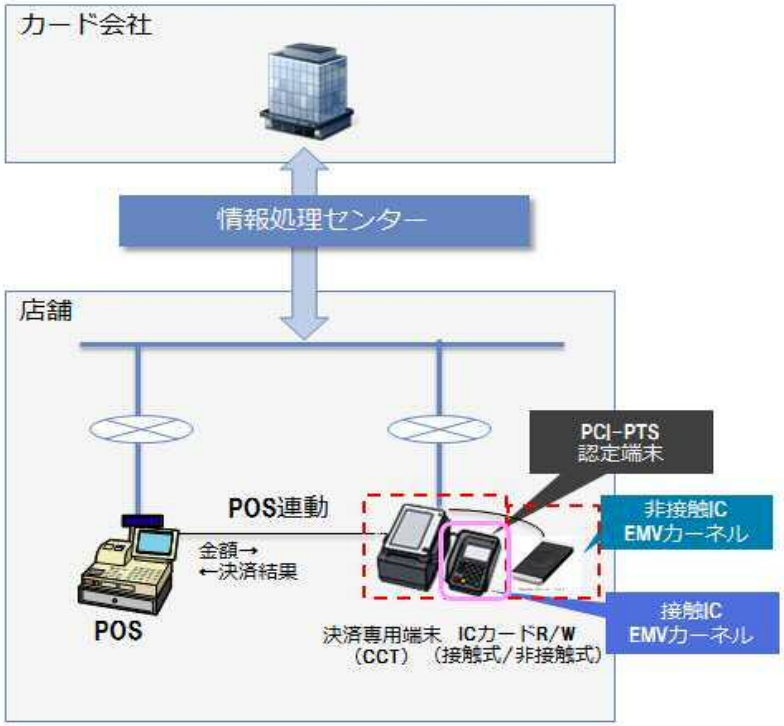
1）決済専用端末（CCT）連動型

◆IC対応した決済専用端末（CCT）とPOSシステムの間で取引金額や決済結果等を連動する仕組み。

- EMVカーネルを決済専用端末やPINパッド等に置くことで、POSシステムの外側となるため、決済専用端末側で開発・EMV認定・ブランドテスト等の対応を行えばよく、POSシステム側で対応する必要がないことから、導入時における対応（開発・EMV認定・ブランドテスト等）の影響が最も小さい。

- また、カード情報がIC対応の決済専用端末から直接カード会社に伝送されるため、加盟店におけるカード情報の非保持化が同時に実現できる。一方で、決済専用端末（CCT）を新たに追加する必要があるため、設置場所の確保等の課題がある。

【決済専用端末（CCT）連動型】



注 非保持化は、決済専用端末（CCT）よりPOSへ連動する「決済結果」にカード情報を含めないことが前提。

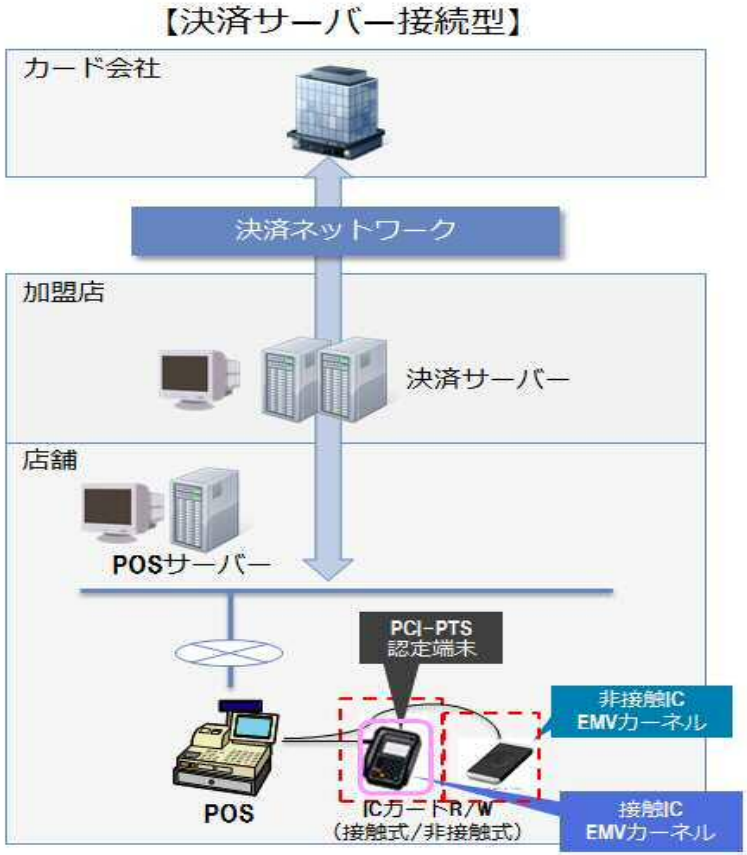
Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策③

①POSシステムのIC対応に係る実現方式例

2）決済サーバー接続型

◆POSシステムで決済を行うが、EMVカーネルがPINパッドにある仕組み。

- EMVカーネルをPOSシステムの外側に置くため、POS本体で開発・EMV認定等を取る必要がなく、ブランドテスト等の対応で済むため、導入時における対応の影響は小さい。
- この場合、カード情報はPOSシステムを通過してカード会社に伝送されるため、カード情報が自社内機器・ネットワークを「保存」、「処理」、「通過」するため、カード情報を保持することになることから、PCI DSS準拠が必要となる。



Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策④

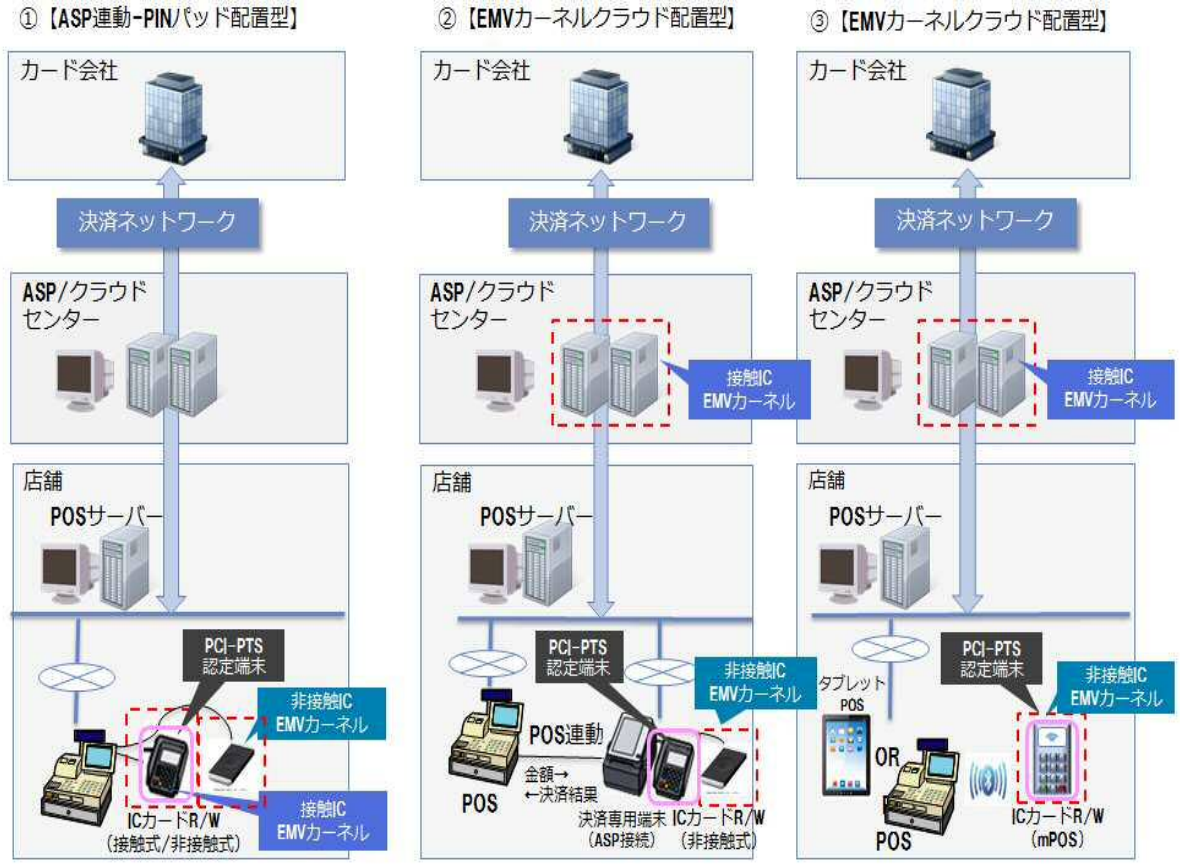
①POSシステムのIC対応に係る実現方式例

3）ASP/クラウド接続型

◆POSシステムと加盟店の外部の事業者（ASP/クラウドセンター）との間で取引金額や決済結果を連動させる仕組み。

- 基本的には2）決済サーバー接続型と同じ構造であるが、ASP/クラウド配置型でのEMV認定・ブランドテストの対応については社外（ASP/クラウドセンター）で行うため、加盟店の個別負担は少ない。この中で、EMVカーネルクラウド配置型のうち決済専用端末をPOSシステムと連動させる場合（右記②）については、カード情報がIC対応の決済専用端末から直接外部のASP/クラウドセンターに伝送されるため、加盟店におけるカード情報の非保持化が同時に実現できる。

- 右記①及び③の場合には、カード情報はPOSシステムを通過するため、加盟店はPCI DSS準拠、又は非保持と同等/相当のセキュリティ措置（PCI P2PE認定ソリューションの導入又は本協議会において取りまとめた「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」に適合するセキュリティ基準（11項目））を満たすことが求められる。



注　非保持化はPOS連動する「決済結果」にカード情報を含めないことが前提。
※上記11項目の詳細については、附属文書「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」を参照のこと。

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策⑤

②IC対応した決済専用端末（CCT）の導入

■ IC対応した決済専用端末（CCT）を導入することで、IC対応を図ることができる。

③特定業界向けのIC対応について

1）ガソリンスタンドにおけるIC対応上の実現可能な方策

■ 日本国内のガソリンスタンドにおいては、利用者が乗車したまま決済するサービス対応を行うフルサービスのガソリンスタンドの場合、総務省消防庁通知の内容に準拠したPIN入力が可能なハンディ端末の開発・導入が必要となる。
■ また、セルフサービスのガソリンスタンドにおいては、現行システム・機器の仕様の制約上、現状では国際基準が求めるPINパッドの設置等が困難であり、代替策の導入が必要となる。（以下、2）オートローディング式自動精算機におけるIC対応を参照）
■ このため、ガソリンスタンドにおける業界固有の課題を踏まえながら、IC対応上の実現可能な方策を示す「国内ガソリンスタンドにおけるICクレジットカード取引対応指針」をとりまとめている。同指針に基づきIC対応することとする。

※詳細は附属文書「国内ガソリンスタンドにおけるICクレジットカード取引対応指針」参照

2）オートローディング式自動精算機におけるIC対応

■ オートローディング式自動精算機に関しては、ICカードリーダーライターとPINパッドが物理的に分離した構造となるため、現状、国際的なセキュリティ基準であるPCI PTSに準拠することが技術的に難しいという課題がある。
■ 一部の業界（例：ガソリンスタンド、鉄道等）では、PCI PTSへの準拠が困難であるオートローディング式によりIC対応を進めることとなったことを受け、「オートローディング式自動精算機のIC対応指針と自動精算機の本人確認方法について」をとりまとめた。当該指針では、オートローディング式の自動精算機をIC対応する場合のPCI PTS未準拠により生じ得るセキュリティリスクに応じた代替コントロール策の内容等、具体的な対応事例を示している。オートローディング式の自動精算機のIC対応については、当面の間、同指針に基づき対応することとする。

※詳細は附属文書「オートローディング式自動精算機のIC対応指針と自動精算機の本人確認方法について」参照

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策⑥

（２）カード会社（イシュアー・アクワイアラー）

- ■ カード会社（イシュアー）は、発行するカードの全てをIC化する。
- ■ カード会社（アクワイアラー）は、自ら所有する決済専用端末のIC対応を行う。
- ■ カード会社（アクワイアラー）は、IC取引時のオペレーションルールに基づく運用がなされるように、加盟店に対して日本クレジット協会策定のガイドライン等について周知を行う。
- ■ カード会社（アクワイアラー）は、契約を有する加盟店に対し、本ガイドラインで整理された各方策について、必要に応じて機器メーカーとも連携して情報を提供する。
- ■ カード会社（アクワイアラー）は、POSシステムの接続インターフェース等の共通化やIC取引オペレーション等を踏まえ作成した「ICカード対応POSガイドライン」及び「非接触EMV対応POSガイドライン」について、機器メーカーや加盟店等への周知を行う。

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策⑦

（３）その他関係事業者等

①国際ブランド

■ IC取引時のオペレーションについて、我が国のクレジットカード業界として制定したルールを推進することに協働して取組む。また、技術の向上や環境の変化等により新たな措置等が必要になった場合は、カード会社（イシュアー・アクワイアラー）と調整を行う。

②機器メーカー

■ 加盟店のIC対応を推進するため、IC対応の必要性及び本ガイドラインで整理された各方策について、カード会社（アクワイアラー）とも連携し、加盟店へ必要な情報を提供する。

■ POSシステムの接続インターフェース等の共通化や国際ブランドテストの簡略化等を活用し、加盟店におけるIC対応POSシステム導入時のコスト低減化に資する技術的解決策の実現に取組む。

■ IC対応端末のコスト低減化や加盟店でのIC対応を円滑に行うために、今後開発・製造するクレジット機能を有するPOSシステムについては、IC対応可能なシステムを標準とする。

③行政

■ 割賦販売法に基づく監督等を通じ、対面加盟店における偽造カードによる不正利用防止のための必要な措置の適確な実施について指導等を行う。

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策⑧

２．IC取引時のオペレーションルール①

□取引形態別（接触IC取引/非接触IC取引）の本人確認方法

◆接触IC取引
・原則、「オフラインPIN」とする。
・CVMリミット金額以下の場合は、本人確認を不要とすることができる。

◆非接触IC取引
・CVMリミット金額以下の場合は、本人確認を不要とすることができる。
・「カード型」におけるCVMリミット金額超過時は**「接触IC取引」**へ切り替え、原則、「オフラインPIN」とする（切替不可の場合サインを許容）。
・「モバイル型等」におけるCVMリミット金額超過時はConsumer Device CVM（モバイルPIN/指紋等）もしくはサインとする。

CVMリミット金額	取引形態		
	接触IC取引	非接触IC取引	
		カード型	モバイル型等
CVMリミット以下	本人確認を「不要」とすることが可能		
CVMリミット超	原則 オフラインPIN （サインを許容※1）	【接触IC取引へ切替】 原則 オフラインPIN （切替不可の場合サインを許容※2）	Consumer Device CVM （モバイルPIN/指紋等） もしくはサイン

※1 接触IC取引において、一部の海外イシュアー発行のカードはオフラインPIN環境での利用が許容されないため
※2 非接触IC取引の「カード型」において、接触IC取引への切替を許容しないカードが存在するため

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策⑨

2. IC取引時のオペレーションルール②

□本人確認不要取引

- CVMリミット金額以下の場合には、カード会員の利便性の観点から本人確認は不要とすることができる。
- 具体的には、本人確認を求めることがクレジットカード取引の阻害要因となり、また、本人確認が不要となることにより決済処理の迅速性が増し、クレジットカード取引の普及に寄与する業種業態の加盟店を対象とする。
- ただし、不正利用のリスクが低い業種売場等であることを前提とし、不正利用防止の観点から換金性の高い商品を除外する。

注　CVMリミット金額とは、カード会社が定める本人確認を不要とする上限額

□本人確認不要取引でのオーソリゼーション要否

- 本人確認不要取引は、紛失・盗難カードによる不正利用のリスクを踏まえたセキュリティ確保の観点から、**全件オンラインオーソリゼーションを必須**とする。

3. その他留意事項

□PINバイパスの廃止に向けた具体的な検討の開始

- 現状、IC取引において、カード会員のPIN失念への一時的な救済措置が可能となるようPIN入力スキップ機能（PINバイパス）の運用が許容されているが、本機能の利用により、PIN入力による本人確認を実施しないことで不正利用被害が発生するリスクがあるため、日本クレジット協会及びカード会社（イシュアー・アクワイアラー）は、本機能の廃止に向けて具体的検討を開始する。

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策⑨

□本人確認としての有効性の低下に伴う、サイン取得を任意とすること等の検討開始について

- 我が国市場では長年にわたり、本人確認としてサインの果たす役割の重要性に鑑み、カード会員に対してはサインパネルへの自署の徹底を、加盟店に対してはそのサイン照合の徹底について業界を挙げて啓発してきた。
- 割賦販売法による不正利用防止措置の義務化、本ガイドラインに基づくIC化の取組の推進により接触IC取引の実現が進展し、PIN入力による本人確認が一般化している状況にあるものの、オフラインPIN環境に対応していないカードが利用される場合や、非接触IC取引におけるCVMリミット金額を超過する取引の際にサインによる本人確認を行う場合があり、依然、本人確認方法としてサインが残存している。
- 一方で、カード会員自ら決済端末にカードを挿抜する、あるいはかざす決済オペレーションが増加しつつあることにより、従来、加盟店がカード会員から一時的にカードを預かりサイン照合を行ってきた商慣習がその変更を迫られている。また、国際ブランドのルールが変更され、サインを取得するか否かは加盟店の裁量に委ねられる任意化の動きがあり、世界的には既に、**サインが従来果たしてきた本人確認としての有効性が低下**している環境変化を踏まえ、**加盟店によるサインの取得を将来的に任意とすることについて、今後、本協議会として具体的な検討に着手する。**
- これら検討に伴い、**前述のPINバイパスの廃止、紙の売上票の削減やNoCVM（本人確認不要取引）の見直し等の周辺領域についても検討し、具体的な方向性を示していく。**
- なお、このサイン取得の任意化の適用にあたっては、そのステークホルダーに与える影響の大きさに鑑み、**カード会員と加盟店への十分な周知のために準備と移行期間を設定する。**

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策⑩

附属文書一覧①

No	文書名	目的・概要
1	国内ガソリンスタンドにおけるICクレジットカード取引対応指針	国内のガソリンスタンドにおける商慣習上の制約を考慮し、2020年3月までのIC対応に向けて、実現可能な代替策をとりまとめたもの。
2	オートローディング式自動精算機のIC対応指針と自動精算機の本人確認方法について	オートローディング式自動精算機の国際的なセキュリティ準拠が技術的に困難なことから、2020年3月までに実現可能な自動精算機のIC対応とそれに伴うセキュリティリスク及び代替コントロール策を示したもの。
3	ICカード対応POSガイドライン	接触IC取引を対象としたPOS加盟店でのIC対応を円滑に進める具体的な方策として策定したもの。
4	ICカード対応POS導入の手引き～全体概要編～	POS導入を計画するシステム企画担当者、売場のPOS運用担当者、POSのシステム・ネットワーク保守管理担当者を対象とし、ICクレジットカードの受入れの為に必要な基礎知識について紹介するもの。
5	ICカード対応POS導入の手引き～取引処理フロー解説編～	加盟店のPOS端末システム企画担当者、POS端末保守運用管理担当者を対象に、EMV仕様書で規定されているICカードとIC対応端末の間、ICカードとカード会社ホストの間で行われる処理内容やそのフローを解説したもの。
6	ICカード対応POS導入の手引き～認定・試験プロセス概要～	加盟店様・POSベンダーを対象に、接触／非接触EMV対応有人型POSの導入・修正において考慮していただきたい要件や認定・試験プロセスを整理したもの。
7	ブランドテスト要否一覧	「ICカード対応POS導入の手引き～認定・試験プロセス概要～」の付属文書であり、同手引きに記載される「シナリオ別ブランドテスト要否一覧」の詳細を記したもの。

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策⑪

附属文書一覧②

No	文書名	目的・概要
8	非接触EMV対応POSガイドライン（全体概要編）	今後の非接触EMV決済の普及、及び接触型と非接触型のPOS端末の同時導入を志向するニーズに応えるために策定したもの。
9	非接触EMV対応POSガイドライン（取引処理編）	主にアクワイアラー、情報処理センターが端末を導入する際の共通仕様に関する項目や、加盟店に設置された際の、接触EMV端末との運用性の整合性及び磁気端末との相違点等について説明しているもの。

関係文書

No	文書名	目的・概要
1	「IC取引における本人確認方法に係るガイドライン」及び「本人確認不要（サインレス／PINレス）取引に係るガイドライン」	IC取引時のオペレーションルールとして、国内加盟店でのIC取引における本人確認方法の業界統一的な考え方を示すとともに、加盟店の円滑なIC対応に資するよう、一般社団法人日本クレジット協会が策定したもの。

Ⅱ．不正利用対策分野
（B）非対面取引におけるクレジットカードの不正利用対策

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策①

非対面不正利用による被害が高水準を維持している背景としては、不正アクセスによるEC加盟店からの情報漏えいやフィッシングメールにより、窃取されたクレジットカード番号が不正利用される手口の発生件数が高止まりしていること、クレジットカード番号の採番の規則性を悪用して推定した大量のクレジットカード番号を特定のEC加盟店において集中的に短期間で使用する手口が依然として継続していること等が考えられる。

１．各事業者に求められる対策等

（１）加盟店

- オーソリゼーション処理の体制整備と加盟店契約上の善良なる管理者の注意をもって不正利用の発生を防止するとともに、リスクや被害状況に応じた非対面不正利用対策を導入する。【指針対策】
- 自社での不審なカード利用の把握に努めるとともに、不正利用の手口は日々巧妙化することから、カード会社における不正利用対策の更なる向上のため、当該情報（不審利用）について契約カード会社（アクワイアラー）やPSPと迅速な情報共有に努める。
- 自社が導入している不正利用対策の課題を検証し、必要に応じて新たな方策の導入等を検討するため、契約カード会社（アクワイアラー）やPSPとの間で迅速な情報共有に努める。
- 加盟店サイトでの大量かつ連続する申込については早期に検知、遮断するなど、加盟店各社サイトにおいて被害の状況等に応じて必要な対策を講じる。

非対面不正利用による被害を防止するための具体的な方策にはそれぞれ特徴があり、加盟店が取り扱う商材や販売手法に応じた有効な方策を講じることが重要である。特に、不正利用が多発している加盟店においては、多面的・重層的な対策を講じることが求められる。不正利用が多発している加盟店は、契約先のカード会社（アクワイアラー）、PSP、セキュリティ事業者等と連携し、自社の業務実態、不正利用の発生リスクに応じて、本ガイドラインが掲げる方策を実施することが求められる。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策②

① 加盟店における非対面不正利用対策の具体的方策

・非対面不正利用による被害を防止するための具体的な方策について、現状における主なものを以下のとおり整理した。

・それぞれの方策には特徴があり、加盟店が取り扱う商材や販売手法に応じた有効な方策を講じることが重要である。

方策		特徴
1）本人認証	a） 3-Dセキュア	• カード会員のみが知るパスワードをカード会社（イシュアー）が照合する本人認証（パスワード認証） • カード会員のデバイス情報等の活用により不正判定を行う本人認証（リスクベース認証） • 比較的容易に導入が可能
	b） 認証アシスト	• 取引時の属性情報とカード会社（イシュアー）の登録属性情報を照合し本人を確認 • カード会員のパスワード失念等の懸念がない
2）券面認証 （セキュリティコード）		• カード券面の「セキュリティコード（数字3～4桁）」を入力し、カードが真正であることを確認 • カード会員の対応が容易 • 加盟店の対応も比較的容易 • カード券面への印字はイシュアー側でほぼ100%対応済み • 機械的にカード番号を生成して攻撃する手口に有効
3）属性・行動分析 （不正検知システム）		• 過去の取引情報等に基づくリスク評価によって不正取引を判定 • 抑止効果維持には継続的な不正利用の条件設定の最適化が必要で、カード会社（アクワイアラー）との継続的な情報連携が重要 • カード会員の負担なし • 不正利用の発生状況に合わせた不正利用の条件設定が可能 • 加盟店が収集した利用者のデバイス情報を活用できる
4）配送先情報		• 不正配送先情報の蓄積によって商品等の配送を事前に停止 • カード会員の負担なし • 多数の取引と一定以上の不正利用被害がある加盟店においては自社構築で一定の効果（上記以外の加盟店は外部サービス利用でないと期待効果得られない）

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策③

② 加盟店における方策導入の指針

・非対面加盟店は、当該加盟店が取り扱う商材や不正利用の被害状況等を踏まえ、非対面不正利用対策の４つの方策をベースとした対策を導入することが求められる。（具体的な指針内容については以下を参照）

１）「全ての非対面加盟店」

【定義】全ての非対面加盟店
【対策】加盟店契約に定める善管注意義務の履行、オーソリゼーション処理

２）「高リスク商材取扱加盟店」

【定義】本ガイドラインで定める５つの商材※１を主たる商材として取り扱う加盟店
【対策】本ガイドラインの掲げる非対面不正利用対策の４つの方策のうち、１方策以上

※１　デジタルコンテンツ（オンラインゲームを含む）、家電、電子マネー、チケット、宿泊予約サービス
ここでいう電子マネーは、コード決済事業者等のその他決済サービス（プリペイド機能等）にクレジッカードを紐づけ、その決済サービスにチャージすることにより利用可能となるものは除く。

３）「不正顕在化加盟店」

【定義】継続的に一定金額を超えた不正利用被害が発生している加盟店※2
【対策】本ガイドラインの掲げる非対面不正利用対策の４つの方策のうち、２方策以上※3

※2　カード会社（アクワイアラ―）各社が把握する不正利用金額が「3ヵ月連続50万円超」に該当する加盟店。
※3　4方策のうち、2方策以上を導入していても不正被害が減少せず、引き続き、「不正顕在化加盟店」と認識される加盟店は、カード会社（アクワイアラー）等より不正利用の発生状況等の情報共有を受け、自社で発生する不正利用防止に対して実効的な方策の導入が必要となる。

③ 大量かつ連続する購入申込への対応

不正に入手した大量のカード情報や採番の規則性を悪用して推定した大量のクレジットカード番号を利用して、コンピューターを用いて自動的に申込む不正利用では、真正なカード会員の購入申込と比べ、申込速度や連続性の点で異なる。加盟店が真正な取引との相違点等により不正な取引を早期に検知し、取引を遮断することが、不正利用防止の有効な対策となる。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策④

（２）カード会社（イシュアー）

- 過去の取引履歴等の様々な情報から、不正取引か否かを判断するオーソリモニタリングの検知精度の向上・強化を図る。
- 「3-Dセキュア」においては、現行のバージョン1.0より、精度の向上したEMV3-Dセキュアを早期に導入する。
- 「EMV 3-Dセキュア」への移行においては「静的（固定）パスワード」からの脱却が求められている。
  なお、「動的（ワンタイム）パスワード」を活用する場合には、カード会員に対しても動的パスワードの利用登録等の環境整備を促進する。併せてオーソリモニタリングやリスクベース認証を用い、多面的・重層的な不正利用対策を講ずる。
- 「EMV3-Dセキュア」に移行するまでの間、バージョン1.0で対応する場合には「リスクベース認証」を導入する。
- 加盟店（オフアス取引の場合はアクワイアラー経由）からの真正利用確認照会に対し、加盟店とイシュアーの情報連携の高度化に取組む。
- 「カード利用時におけるカード会員向け利用確認メール等通知」の導入を促進する。
- 「セキュリティコード」の桁数が少ないことを悪用し、真正な「セキュリティコード」を探り当てるため、数値を変えた多数回連続のオーソリゼーションに対しては当該不正行為を早期に検知し当該取引を停止するとともに、万一真正な数値に合致した以降の不正利用を防ぐことが重要である。

①「EMV 3-Dセキュア」への対応

・EMV3-Dセキュアでは、カード会社（イシュアー）は、加盟店がカード会員の同意を取得した上で加盟店から提供を受けるカード会員に関する情報を用いることにより本人認証の精度が向上する。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策⑤

②「３-Dセキュア1.0」におけるリスクベース認証

・加盟店から提供される利用者情報や取引情報、デバイス情報等を活用したリスク評価により不正利用の判定を行うことで、カード会員にパスワード入力を求める取引を最小限にすることも期待できることから導入が求められる。

③「動的パスワード」への移行とカード会員の利用登録の推進

・3-Dセキュア1.0に動的パスワードを活用しているカード会社からは、その取引において不正利用が抑止されている実績が報告されている。

・EMV 3-Dセキュアを導入するまでの間に3-Dセキュア1.0で対応する場合には、カード情報とともに「静的（固定）パスワード」が窃取された場合、不正利用被害を有効に防ぐことができなくなるため、「静的（固定）パスワード」から「動的（ワンタイム）パスワード」への移行が求められる。さらに、新たな本人確認方法を採用する場合にも、カード会員に対して当該認証方法の理解を促すとともに利用環境の整備を促進する。

・3-Dセキュアの精度向上と普及のためには、カード会員の動的パスワードの利用登録が不可欠であり、早急に環境整備が進むよう促進する。

④デバイス認証（生体認証等）

・国際ブランドでは、EMV 3-Dセキュアの本人認証として「リスクベース認証」や「動的（ワンタイム）パスワード」とともに、「指紋等の生体情報による認証」の活用も推奨している。
生体情報による認証は、必ずしもカード会社（イシュアー）がカード会員の生体情報を保有する必要はない。
クレジットカード情報と生体情報をスマートフォン等のデバイスに登録する際に、確実な本人認証が行われていれば、その後の当該デバイスによるクレジットカード利用時において登録された生体情報の認証等も認められる。

⑤クレジットカードと連携するコード決済事業者等に対する多面的・重層的な対策の実施

・クレジットカードを、コード決済事業者等が提供する他の決済サービスと連携（紐づけ）する取引は、非対面不正利用によりクレジットカードを連携された場合、反復的に不正にチャージがなされ、また不正なクレジットカード決済が行われ、高額な不正利用被害が発生する蓋然性がある。このことからクレジットカードと連携する取引の時点で、カード会社（イシュアー）はオーソリゼーションによるモニタリング、セキュリティコードの照合、3-Dセキュアにおけるパスワード照合及びリスクベース認証等の取引の時点の対策を複数組み合わせることにより、セキュリティ対策を多面的・重層的に講じる必要がある。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策⑥

⑥ カード会員向け利用確認メール等通知

・カード会員がメール等通知内容を確認し、利用覚えがない場合はカード会社（イシュアー）に連絡することにより、早期に不正利用であることの確定とカードの無効手配・処理が可能となるため、有効な不正利用対策となる。

・メール等受信に関するカード会員の同意やメールアドレス等の登録・管理（メールアドレス等の情報の最新化）等の対応が必要となる。

⑦「券面認証（セキュリティコード）」の多数回連続アクセスへの対策

・有効なクレジットカード番号を用いて、「セキュリティコード」のみを入れ替えて連続して購入申込を行う不正利用がある。

・正当なコードに合致した場合、取引が成立してしまうことから、このような購入申込を早期に検知し、当該クレジットカード番号による取引を停止させることが必要となる。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策⑦

（３）カード会社（アクワイアラー）・PSP

- カード会社（アクワイアラー）及びPSPは、加盟店に対して、非対面不正利用対策の具体的な方策の導入について、適切な助言・協力ができるよう体制の整備をするとともに、リスク・被害発生状況に応じた方策導入の確実な実施のため加盟店に対する指導及び状況に応じた適切な提案を行う。
- カード会社（アクワイアラー）は、加盟店に対し、不正利用対策の参考となるよう、非対面不正利用の傾向や事例等の情報及び非対面不正利用対策を導入しないリスクについて情報共有に努める。
- カード会社（アクワイアラー）は、オフアス取引において、加盟店における非対面不正利用対策の更なる向上のため、カード会社（イシュアー）から提供された不正情報についてできるだけ多くの加盟店と迅速な情報共有に努める。各加盟店における不正利用対策の課題の特定とともにその解決を図るため、各加盟店との間で迅速な情報共有に努める。
- PSPは、本ガイドラインに掲げる「本人認証」「券面認証」「属性・行動分析（不正検知システム）」「配送先情報」の各方策を提供できる体制を構築し、契約先の加盟店に対して導入の推進に努める。
- 加盟店からの、真正利用確認照会に対し、情報連携の高度化に取組む。

①「EMV 3-Dセキュア」への対応

・現行の3-Dセキュア1.0より精度の高いバージョンであるEMV 3-Dセキュアの運用が始まっている。EMV 3-Dセキュアであれば、不正利用防止の精度が向上することはもとより、加盟店への普及阻害となっていた「パスワード入力によるかご落ち」といった課題の解決もできることから、カード会社（アクワイアラー）及びPSPは、このEMV 3-Dセキュアの導入態勢を早急に整備し、加盟店に対して導入を求める必要がある。

②クレジットカードと連携する決済サービスを提供する決済事業者等との契約時におけるセキュリティ対策の確認

・カード会社（アクワイアラー）は、コード決済事業者等のクレジットカードと連携することにより他の決済手段を提供する事業者と包括加盟店契約等を締結する場合には、当該事業者が(一社)キャッシュレス推進協議会がとりまとめた「コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン」や(一社)日本資金決済業協会がとりまとめた「銀行口座との連携における不正防止に関するガイドライン」等、関係するガイドラインに準拠するなど、十分な安全対策が講じられていることを確認する必要がある。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策⑧

（４）その他関係事業者等

①国際ブランド

- 我が国における非対面加盟店でのクレジットカード取引実態を踏まえ、各種課題の解決に向けて関係事業者と協働して取り組む。
- 「EMV 3-Dセキュア」に係るステークホルダーへの影響（運用ルール等）及び「EMV 3-Dセキュア」への移行について、情報の提供及び説明を行う。
- 非対面加盟店における不正利用対策の取組を推進するため、海外のカード会社や加盟店における取組事例について情報提供を行うとともに、我が国における国際水準のセキュリティ環境の整備の必要性について、事業者向けの情報発信に取組む。

②行政

- 割賦販売法に基づく監督等を通じ、非対面加盟店における非対面不正利用防止のための必要な措置の適確な実施について指導等を行う。また、本ガイドラインに掲げる非対面不正利用対策の実施について、事業者向けや消費者向けの情報発信に取組む。

③業界団体等

- 日本クレジット協会は、他の業界団体に協力を要請し、不正利用の実態を踏まえ、加盟店において本ガイドラインに掲げるリスクに応じた非対面不正利用対策を導入する必要性及び各方策の有効性等について、事業者向けの周知活動の強化に取組む。
- 日本クレジット協会は、最新の不正利用発生状況を踏まえた「不正顕在化加盟店」の基準や「高リスク商材取扱加盟店」の特定商材の継続的な検討、不正利用被害が継続的に発生する加盟店の不正利用の発生状況の分析・評価、加盟店が取り扱う商材に応じた各方策の有効性の検証や方策の組合せ効果の検証を継続して行う。
- 日本クレジット協会は、不正利用による被害の実態や最新の犯罪手口、不正利用対策に対する取組の成功事例等について、他の情報セキュリティに係る関係機関との連携・情報共有を図り、クレジット取引に関係する事業者等に対して適時情報発信を行う。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策⑦

附属文書一覧

No	文書名	目的・概要
1	「2019年版実行計画上の方策導入による不正抑止の好事例の紹介」	カード会社、決済代行会社、加盟店の協力を得て、実行計画に掲げる４つの不正利用防止方策を導入した際の不正抑止効果について好事例集としてとりまとめたもの（2019年版）。
2	「非対面加盟店における不正利用対策の具体的な基準・考え方について」	加盟店のリスクや被害発生の状況等に応じ、実行計画に掲げる４つの不正利用防止方策を導入する際の指針として、具体的な基準・考え方をとりまとめたもの。

Ⅲ. 消費者及び事業者等への周知・啓発について

Ⅲ. 消費者及び事業者等への周知・啓発について①

１．消費者への周知・啓発

（１）加盟店

- IC対応済み加盟店は、「共通シンボルマーク等」の掲出、あるいは自社独自の「見える化」への取組に努める。
- 本ガイドラインで求められるクレジットカードの情報保護対策及び不正利用対策を講じているEC加盟店は、本ガイドラインに取組んでいることを表示（自己宣言）し、認識・識別できる「見える化」への取組に努める。

（２）カード会社（イシュアー）

- カード会員から直接カード情報等を窃取する手口も存在するため、消費者に対する注意喚起及びセキュリティ対策の必要性等の啓発を行う。
- 「共通シンボルマーク等」を使用しカード会員のPIN認知度向上のため周知活動を行うとともに、PINを認知していないカード会員に対しては、特にPINの重要性やPINの確認方法等について、自社のホームページやカード会員向けの広報媒体を用いて、分かりやすく丁寧に説明する。
- ECの不正利用対策に関する消費者への周知活動に取組む。
- カード会員に対し、ID・パスワードの使い回しの防止等について、周知活動に取組む。
- 従来の静的パスワードから動的パスワードに移行する場合においては、改めてカード会員への周知・啓発が必要である。
- カード会員に対し、フィッシングの手口や防止策等に関する周知活動に取組む。
- 不正利用の早期発見のため、毎月の利用明細の確認の重要性に関する周知活動を積極的に行う。

Ⅲ. 消費者及び事業者等への周知・啓発について②

（３）その他関係事業者等

①国際ブランド

- グローバルな観点から、海外におけるカード情報保護に関するリスクや各種課題、我が国における国際水準のセキュリティ環境の整備の必要性等について、消費者向けの情報共有、発信に取組む。

②業界団体等

- 日本クレジット協会は、フィッシングによるカード情報の漏えいが増加していることから、カード会社（イシュアー）や関係団体と連携し、周知・啓発に適した媒体を活用するなどして、カード会員に対する注意喚起とフィッシングの手口や防止策の情報提供に取組む。
- 日本クレジット協会は、クレジットカード業界全体でIC取引を推進していること、IC取引では本人確認のためPIN入力が必要になることの周知に引き続き取組む。
- 日本クレジット協会及び業界団体等はカードの不正利用対策の必要性やその具体的な方策に関するカード会員の理解・協力を得るために、ECの不正利用対策に関する消費者への周知活動に取組む。
- 日本クレジット協会はカード会社（イシュアー）と連携し、カード会員に対し、ID・パスワードの使い回しの防止等について、周知活動に取組む。
- 日本クレジット協会は、カード会員に対し、毎月の利用明細を確認することの重要性に関する周知活動を積極的に行う。

Ⅲ. 消費者及び事業者等への周知・啓発について③

２．事業者等への周知・啓発

クレジットカード取引における不正を企図する攻撃者の手口は日々巧妙化していくため、加盟店をはじめとするクレジットカード取引関係事業者は最新の手口やセキュリティ技術等に関する情報を常に収集することが求められる。

特に各加盟店におけるセキュリティ対策については、多額の投資や業務の変更等を要することもあり、適切な情報の収集と分析等が必要となるが、個社の取組のみでは限界もある。

こうした事情を踏まえ、行政及び日本クレジット協会は、本ガイドラインの内容を広く周知するとともに、セキュリティ対策について必要な助言や情報提供を行い、その取組を支援していくものとする。