クレジットカード・セキュリティガイドライン【2.0 版】

＜公表版＞

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

目次

はじめに 5

用語集 6

附属文書、関係文書 11

（１）附属文書一覧 11

（２）関係文書一覧 12

本ガイドラインの基本的な考え方 13

Ⅰ．クレジットカード情報保護対策分野 14

１．各事業者に求められる対策等 14

（１）加盟店 14

❶加盟店に求められる対策 15

❷加盟店における対策概要 16

①非保持化対策 16

１）非対面加盟店における非保持化対策 17

ａ）EC 加盟店の対策 17

＜具体的方策の考え方＞ 17

＜留意事項＞ 17

□EC 加盟店における非保持化導入例 18

❶リダイレクト（リンク）型 18

❷Java Script 型（トークン型） 18

ｂ）メールオーダー・テレフォンオーダー加盟店の対策 19

＜具体的方策の考え方＞ 19

□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 19

❶非保持化　決済用端末を利用した外回り方式 20

❷非保持化　タブレット等の専用端末を利用した外回り方式 20

❸非保持と同等/相当

PCI P2PE 認定ソリューション端末を利用した内回り方式 21

２）対面加盟店における非保持化対策 22

＜具体的方策の考え方＞ 22

＜留意事項＞ 22

□対面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 22

❶・❷非保持化　決済専用端末連動型・ASP/クラウド接続型（外回り方式） 22

❸非保持と同等/相当　ASP クラウド接続型（内回り方式） 23

３）非保持化対策における留意点 24

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 24
ｂ）過去に取り扱ったカード情報の保護対策 25
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 25
②PCI DSS 準拠 25
（２）カード会社（イシュアー・アクワイアラー） 26
（３）決済代行業者等 26
（４）コード決済事業者等 26
（５）その他関係事業者等 26
①国際ブランド 26
②ソリューションベンダー 26
③行政 27
④業界団体等 27
２．その他留意事項 27
（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 27
（２）カード情報漏えい時の対応 27

Ⅱ．不正利用対策分野 28
（A）対面取引におけるクレジットカードの不正利用対策 28
１．各事業者に求められる対策等 28
（１）加盟店 28
①POS システムの IC 対応に係る実現方式例 28
１）決済専用端末（CCT）連動型 28
２）決済サーバー接続型 29
３）ASP/クラウド接続型 30
②クレジットカード決済に POS システムを用いない加盟店等の対応 31
③特定業界向けの IC 対応について 31
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 31
２）オートローディング式自動精算機における IC 対応 32
□加盟店における指針対策の実現方法 32
（２）カード会社（イシュアー・アクワイアラー） 32
（３）その他関係事業者等 33
①国際ブランド 33
②機器メーカー 33
③行政 33
２．IC 取引時のオペレーションルール 33
（１）接触 IC 取引 33
（２）非接触 IC 取引 34
①カード型 35
②モバイル型等 35
３．その他留意事項 36

（1）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
及び PIN バイパスの廃止等の検討開始について 36
（2）POS システムの IC 対応に係る各種ガイドライン等（附属文書） 37

（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 38
1．各事業者に求められる対策等 38
（1）加盟店 38
①加盟店における非対面不正利用対策の具体的方策 39
1）本人認証 39
a）3-D セキュア 39
b）認証アシスト 39
2）券面認証（セキュリティコード） 39
3）属性・行動分析（不正検知システム） 39
4）配送先情報 40
②加盟店における方策導入の指針 41
1）全ての非対面加盟店 41
2）高リスク商材取扱加盟店 41
3）不正顕在化加盟店 42
③大量かつ連続する購入申込への対応 42
（2）カード会社（イシュアー） 42
①EMV 3-D セキュアへの対応 43
②「3-D セキュア 1.0」におけるリスクベース認証 43
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 43
④デバイス認証（生体認証等） 44
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 44
⑥カード会員向け利用確認メール等通知 44
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 44
（3）カード会社（アクワイアラー）及び PSP 44
①EMV 3-D セキュアへの対応 45
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について 45
（4）その他関係事業者等 45
①国際ブランド 45
②行政 46
③業界団体等 46

Ⅲ．消費者及び事業者等への周知・啓発について 47
1．消費者への周知・啓発 47
（1）加盟店 47
（2）カード会社（イシュアー） 47

（3）その他関係事業者等 48
①国際ブランド 48
②業界団体等 48
2．事業者等への周知・啓発 48

履歴 49

はじめに

「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画（以下「実行計画」という）」がその実施期限である 2020 年 3 月末に終了し、クレジットカード取引の関係事業者が実施すべきセキュリティ対策を「クレジットカード・セキュリティガイドライン（以下「本ガイドライン」という）」としてとりまとめてから一年が経過しようとしている。

この間、令和 2 年 6 月には、第 201 回通常国会で「割賦販売法の一部を改正する法律（令和 2 年法律第 64 号）」が成立し、クレジットカード番号等取扱業者が拡充されることとなり、令和 3 年 4 月 1 日付で施行されるところである。今般、新たに追加された事業者である「決済代行業者等」、「コード決済事業者等」は、クレジットカード番号等取扱業者が講ずべき「必要かつ適切な措置」として、PCI DSS への準拠が求められることとなる。また、これら新たな事業者がカード情報の取扱いを委託する場合は、委託者自身が委託先のセキュリティ対策状況を確認し、責任をもって PCI DSS 準拠等の必要な対策を求めなければならない。

また、クレジット取引セキュリティ対策協議会（以下「本協議会」という）を取り巻く外部環境に目を向けると、不正利用被害のほとんどは EC 加盟店での非対面取引において発生し、その被害額は依然として高い水準で推移しているところであり、同被害を減少させるために引き続き実効性のある取組みが求められる状況にある。加えて、キャッシュレス決済全般に視野を広げれば、コード決済サービスにおける不正利用被害事案の発生や、悪意のある第三者が、銀行口座と連携して利用される決済サービスを提供する資金移動業者等を通じて、同口座から不正な出金を行う事案が複数発生したことで、クレジットカードを含むキャッシュレス決済全般の、取引の安全性確保への消費者の関心は一層の高まりを見せているところである。本協議会としても、非対面取引の不正利用対策として、本人認証強化に向けて、EMV 3-D セキュアの導入推進や多面的・重層的な対策の導入の必要性について本ガイドラインに掲載し関係事業者に取組みを求めている。

以上、本ガイドライン策定以降の環境変化を踏まえ、各関係事業者が本ガイドラインに基づくセキュリティ対策を実施し、クレジットカードを利用する消費者が安全・安心に利用できる環境の整備に一層取り組まれることを引き続き期待する。

2021 年 3 月

用語集

本ガイドラインにおける用語の説明は以下のとおり。
（本文中（目次及び用語集内における記載を除く）において、用語集に掲載する用語が初出する箇所に「*」を付している。）

用　語	説　明
3-D セキュア	EC 加盟店における非対面不正利用防止のための本人認証手法の一つ。 利用者がカード会員本人であることを確認する仕組みであり、カード会員に本人のみが知る情報を入力させることなどで、本人認証を行う。
ACS	Access Control Server の略。 3-D セキュアにおいて、カード会社（イシュアー）が加盟店からの本人確認要求に対して、本人であることを確認するためのサーバー。
CCT	Credit Center Terminalの略。 共同利用端末として運営される情報処理センターの信用照会端末。
CVM リミット金額	CVMとは、Cardholder Verification Methodの略。 クレジットカードに対するカード保有者を認証する本人確認方法。カードを提示した者が当該カードを使用する権利を有する者かを検証する。 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。
DUKPT	Derived Unique Key Per Transactionの略。 トランザクションごとにデータの暗号鍵が異なる暗号鍵管理の仕組み。
EMV 3-D セキュア	次期バージョンの 3-D セキュアで、国際ブランドが設置した国際機関 EMVCo よりその仕様が公表されている。 【EMV 3-D セキュア仕様の特徴について】 ①3-D セキュア 1.0 のブラウザベース（PC 利用）に加え、EMV 3-D セキュアではアプリケーションベースも対象となる。これによりスマートフォンのアプリケーションを利用した取引も、3-D セキュアによる認証が活用できるようになる。 ②カード会員のネット接続端末情報や購入時にカード会員が入力した属性等、加盟店から ACS に提供される情報が、3-D セキュア 1.0 に比べ EMV 3-D セキュアでは増加する。これら情報の活用により、リスク判別力の高いモデルの設定が可能になり、パスワード入力を求める取引が格段に少なくなることが期待できる。 注　実行計画においては、「3D セキュア 2.0」と表記されていた。
EMV カーネル	EMVとは、IC取引の基準を策定する国際的な業界団体EMVCoが管理するICカードによる金融取引に関する仕様で、事実上の国際的な基準。 カーネル（Kernel）とは、オペレーティングシステム（OS）の中核となる部分であり、EMVカーネルはEMV仕様に対応したカーネルをいう。IC取引によるクレジット決済処理を行うために必要な処理等を行うためのソフトウェア。

用　語	説　明
EMV 認定	EMVCoが相互運用性の確保のために実施している認定テストのこと。認定はレベル1とレベル2とに階層化されており、レベル1はハードウェア仕様を含めICカードとのインターフェース制御処理の認定を、レベル2はICカードとのアプリケーション処理の認定を行う。
IC 化	IC は Integrated Circuit の略。 クレジットカードにICチップを組み込むこと。構造上ICカードの複製は極めて困難であるとともに、演算機能を利用してオフラインで、偽造カードの検知やカード使用者の本人確認が可能であり、セキュリティ面で磁気カードより格段に優れる。ICチップのインターフェースによって接触型と非接触型に大別される。
IC 対応	加盟店に設置するクレジットカード決済端末にICチップ読取機能を持たせること。
IC 取引	カード情報をICチップに暗号化して格納したICカードを、加盟店に設置されたICチップ読取機能を持ったカード決済端末で処理する取引。
MO・TO 加盟店	メールオーダー・テレフォンオーダー等の EC 加盟店以外の非対面加盟店。
No CVM	本人確認を不要とすること。
PCI DSS	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（VISA、Mastercard、JCB、American Express、Discover）が共同で策定したデータセキュリティの国際基準。 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、12 の要件に基づいて約 400 の要求事項から構成されており、「準拠」とは、このうち該当する要求事項に全て対応できていることをいう。PCI DSS 準拠の検証方法としては、①オンサイトレビュー（認定セキュリティ評価機関（QSA）による訪問審査）又は②自己問診（SAQ、自己評価によって PCI DSS 準拠の度合いを評価し、報告することができるツール）による方法がある。 注　Diners Club は Discover のグループであり、PCI DSS においては Discover の基準を適用している。
PCI PTS	Payment Card Industry PIN Transaction Securityの略。 PCI SSCが定めた、PIN取引を保護するPIN入力装置に関わる国際的なセキュリティ基準。PIN取得時はPCI PTSに準拠した機器の利用が必要となる。機器メーカーがPCI SSCに申請し、個体ごとにその認定を受ける。物理的なキーパッドやタッチスクリーン等、PINを入力して伝送する端末を対象とし、端末の不正開封行為に対する強度（耐タンパー性）や、端末の操作時に発生する信号の保護、PIN伝送時の暗号化等を定める。
PCI P2PE	PCI Point to Point Encryption の略。 カードリーダーデバイスから決済処理ポイントまでカード会員データを安全に伝送処理する仕組みで、PCI SSC に認定されたソリューション。

用　語	説　明
	注　詳細については、附属文書の「【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。
PCI SSC	Payment Card Industry Security Standards Council の略。 国際ブランド（VISA、Mastercard、JCB、American Express、Discover）が共同で設立した PCI セキュリティ基準の開発、管理、教育、認知を担当する、グローバル規模の開かれた協議会。 ※現在、新たに UnionPay International（銀聯国際）がストラテジックメンバーとして参加している。
PIN	Personal Identification Number の略。 カード入会時にカード会社（イシュアー）に登録する暗証番号で、IC取引時にカード会員がIC対応決済端末に入力する数字。
PIN パッド	IC取引に必要なPIN（暗証番号）を入力するためのパッド。
PSP	Payment Service Provider の略。 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決済スキームを提供し、カード情報を処理する事業者をいう。 注　割賦販売法におけるクレジットカード番号等取扱契約締結事業者の登録を行った事業者はカード会社（アクワイアラー）としての対策等も必要となる。
QSA	Qualified Security Assessorの略。 PCI SSC に認定されたセキュリティ評価機関。加盟店やサービス・プロバイダーへのインタビューやドキュメント、サーバー等の訪問審査を正式に行うことができる認定審査機関。
SAQ	Self-Assessment Questionnaireの略。 自己問診。PCI DSS準拠の自己評価を支援することを目的とした検証ツール。
オーソリモニタリング	カード会社がオーソリゼーション情報等により不正利用を検知する仕組み。「不正検知システム」とも呼ばれるが、属性・行動分析ベンダーが提供するサービスとの混同を避ける観点から、本ガイドラインでは「オーソリモニタリング」と表記する。
オフライン PIN	IC 対応決済端末に IC カードが読み込まれ、カード利用時にカード会員が入力した数字と、カードの IC チップ内に記録された PIN とを照合するもの。 一方、IC対応決済端末上での照合ではなく、オンラインネットワークを経由してカード会社（イシュアー）のシステム上で照合するオンラインPINがある。
カード会社（イシュアー・アクワイアラー）	イシュアーはクレジットカード等購入あっせん業者（割賦販売法第 35 条の 16）のこと。 アクワイアラーはクレジットカード番号等取扱契約締結事業者（割賦販売法第 35 条の 17 の 2）のこと。
カード情報	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、

用　語	説　明
	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。 ・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） ・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） ・無効処理されたクレジットカード番号
共通シンボルマーク等	周知活動に活用するために、日本クレジット協会が策定したもので、消費者が IC クレジットカード対応加盟店であることを認識・識別できるよう、IC 対応済みであることを示す「共通シンボルマーク」及び「IC 対応デザイン」のこと。 **「IC 対応」・「暗証番号の認知度向上」共通シンボルマーク** **「IC 対応デザイン」** 注　「共通シンボルマーク」は日本クレジット協会の登録商標（平成 30 年 7 月 27 日登録） 使用方法は「クレジットカードの IC 対応『見える化』等のための共通シンボルマーク・デザインマニュアル」を参照（日本クレジット協会のホームページに掲載）。
決済代行業者等	以下のいずれかの業務を行う決済代行業者（PSP を含む）※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

用　語	説　明
	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。
決済専用端末	CCT（Credit Center Terminal）及びそれと同等以上のセキュリティレベルのものをいう。
コード決済事業者等	以下のいず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。
ソリューションベンダー	非保持化や非保持と同等/相当を実現するためのソリューション（仕組み）を提供するシステム会社等をいう。
非保持化	加盟店におけるカード情報保護対策の一つ。 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。
非保持と同等/相当	POS 内システム又は社内システムを介してカード情報を処理等するが、クレジットカード番号を特定できない状態とし、自社内で復号できない仕組み。 注　詳細については、附属文書の「【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」及び「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。
ブランドテスト	国際ブランドを介した取引に利用する決済システムの導入時に、国際ブランドごとに当該ブランドについて国際的な相互運用性が確保できることを確認するためのテスト。

附属文書、関係文書

本ガイドラインにおけるセキュリティ対策の各方策等については、本協議会が同ガイドラインとは別に策定した附属文書及び本協議会事務局である一般社団法人日本クレジット協会が策定した関係文書の中で詳述しており、本文中において※を付しその参照を促している。

（1）附属文書一覧

文書名	目的・概要
【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。
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。
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・利用等の措置内容をとりまとめたもの。
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。
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。
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。
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。
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。
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、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。

文書名	目的・概要
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。
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。
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。
「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。

（２）関係文書一覧

文書名	目的・概要
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。
「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、日本クレジット協会が策定したもの。

本ガイドラインの基本的な考え方

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」及び「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こととする。

４．対象となるクレジットカードについて

本ガイドラインの対象となるクレジットカードは、世界中で利用され、不正利用のリスクが高い「国際ブランド付きのクレジットカード」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」は、利用できる範囲が限定され不正利用のリスクも低いことから本ガイドラインの対象とはしていないが、不正利用等のリスクに応じたセキュリティ対策を講じることは必要である点に留意が必要である。

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ため、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実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。

Ⅰ．クレジットカード情報保護対策分野

カード情報*の保護は、クレジットカード取引に関わる全ての事業者の責務である。

企業や個人を狙ったマルウェアや標的型攻撃によって個人情報やカード情報の窃取、またそれらの窃取した情報を利用した特殊詐欺等の事件は引き続き発生しており、特にカード情報の不正利用は国内だけに止まらず、国際的にも甚大な被害をもたらしている。これらは、不正を働いている犯罪者の大きな資金源になっているとも言われており、犯罪防止の観点からも関係事業者が責任を持って適切な情報管理を行うことが求められる。

そもそもカード情報を自社で保持していなければ、カード情報を窃取されることがなく、情報漏えいの観点からも有効なセキュリティ対策と考えられる。しかし、カード情報を保持しなくても事業を運営できる事業者と、保持しなければ事業を運営できない事業者があるため、各事業者の実態を踏まえた対策を講じることが重要である。

本ガイドラインにおいて、加盟店には非保持化（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 準拠、カード会社、決済代行業者等及びコード決済事業者等には国際ブランド（VISA、Mastercard、JCB、American Express、Discover）が共同で策定したデータセキュリティの国際基準である PCI DSS*（Payment Card Industry Data Security Standard）の準拠を求めている。

各事業者は、本ガイドラインに基づき自社の業務の実態を踏まえたカード情報保護対策を的確に講じる必要がある。

注　「カード情報」とは、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。
・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）
・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）
・無効処理されたクレジットカード番号

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。

加盟店が非保持化に向けた具体的な取組を進めるにあたっては、対面加盟店と非対面加盟店に分けてアプローチする必要がある。さらに、非対面加盟店のうち、昨今カード情報漏えい事案の発生源となっている EC 加盟店においてはセキュリティ対策を一層強化することが重要である。

特に、EC 加盟店のウェブサイトの脆弱性やウェブサイトの開発・運用段階で管理画面に簡易なログインパスワードを設定する等の不適切なアクセス制御、EC 加盟店の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）の脆弱性等が悪用された漏えい事案が発生している点を踏まえ、委託先に必要な対策を求めるとともに、自社システムの定期的な点検やその結果に基づいて追加的な対策等を講じるなどセキュリティレベルを向上させることが重要である。

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* (ﾒｰﾙｵｰﾀﾞｰ・ ﾃﾚﾌｫﾝｵｰﾀﾞｰ)	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１　非保持と同等/相当を実現した場合でも、事業者の選択により PCI DSS に準拠することを否定しない。

注２　継続課金加盟店において、カード受付時は対面取引を行い、以降は非対面取引を行う場合には、対面加盟店と非対面加盟店双方の対策が必要。

注３　上表は加盟店に求められる対策を示すものであるが、どの対策をとるかは各事業者の選択に委ねられる。

❷加盟店における対策概要

「❶加盟店に求められる対策」の概要は以下の通り。

対策 / 項目	非保持化	非保持と同等/相当	PCI DSS 準拠
概要	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	自社で保有する機器・ネットワーク外でカード番号を特定できない状態とし、自社内で復号できない仕組み（仮に窃取されてもカード情報として不正に利用することは極めて困難となる）	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（PCI DSS）に準拠すること
実現方法	本ガイドラインに記載の非保持化実現方策の導入等	本ガイドラインに記載の非保持と同等/相当実現方策の導入	PCI DSS に定められた要件への対応 （12 のセキュリティ要件への対応、準拠項目に関する QSA*による訪問審査（オンサイトレビュー）又は自己問診（SAQ*）の実施）
各々の特徴	非通過型（EC 加盟店）又は外回り方式（対面加盟店、MO・TO 加盟店）等によりカード情報を一切保持しない	POS 内システム又は自社内システムを介してカード情報を処理等せざるを得ない場合でも、事実上、「非保持化」が可能	カード情報を自社で保有する機器・ネットワークで保持する場合の対策

①非保持化対策

加盟店におけるカード情報保護のための取組として「非保持化」を推進する。

非保持化は PCI DSS 準拠とイコールではないものの、カード情報保護という観点では同等の効果があるものと認められるため、本ガイドラインにおいては、PCI DSS 準拠に並ぶ措置とする。

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「非保持化」に該当する。

なお、以下①～③の状態でカード情報を保存する場合には、「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）

注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。

注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」とはならないが、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 の準拠対象になることに留意する必要がある。

１）非対面加盟店における非保持化対策

非対面加盟店における非保持化は、具体的には、以下の考え方により実現可能である。

ａ）EC 加盟店の対策

PSP を利用する EC 加盟店のカード決済システムにおいては、カード情報が EC 加盟店の機器・ネットワークを通過する「通過型」と、通過しない「非通過型」に大別される。

通過型は、カード情報が EC 加盟店の機器・ネットワークを「通過」して「処理」されるため、EC 加盟店が意図せずにカード情報を「保存」することがある。これらの「通過」し「処理」されたカード情報や「保存」されたカード情報は、外部からの不正アクセスやウイルスの設置、システムの改ざんや機器の脆弱性により、窃取されるリスクが高い。これまで発生している漏えい事故の多数は、この「通過型」の EC 加盟店にて発生したものであった。

一方、非通過型は、カード情報が EC 加盟店ではなく、PSP の機器・ネットワークを「通過」して「処理」され、EC 加盟店はカード情報を「保存」「処理」「通過」することはない。このため、EC 加盟店が非保持化を実現するためには、PSP が提供する非通過型の決済システムを導入することとなる。この場合、EC 加盟店は、PCI DSS 準拠済みの PSP が提供する非通過型の決済サービスを導入しなければならない。

＜具体的方策の考え方＞

ア）PSP を利用する EC 加盟店は、PCI DSS 準拠済みの PSP が提供するカード情報の非通過型（「リダイレクト（リンク）型）」又は「Java Script 型（トークン型）」）等の決済システムを導入する。

イ）「非通過型」を導入しても、業務の都合等により PSP 等から別途カード情報の還元を受けて保持する場合には「非保持」とはならず、PCI DSS に準拠する。

ウ）「通過型」を導入している EC 加盟店はカード情報を保持するため、PCI DSS に準拠する。

※なお、EC 加盟店では「非保持と同等/相当」の対策はない。

＜留意事項＞

・「非通過型」の決済システムを導入した場合でも、EC サイトの開発・運用段階でのセキュリティ対策が不十分であることを原因として不正侵入を許し、カード情報の漏えい事案へと繋がっていることが近時の傾向である。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でカード情報漏えいを防止することが重要である。加えて、コロナ禍の新常態として EC 加盟店での非対面取引が増加傾向にある中、これまで、EC 取扱

高の伸長に伴い不正利用被害も増加してきたことからも、引き続き実効性のある不正利用防止の取組が求められている。

・自社の決済システムが「通過型」「非通過型」のいずれかであることを認識しておらず、カード情報の漏えい事故が発生した後に、「通過型」であることを認識する事例が見られることから、EC 加盟店は自社の決済システムを確認し、「通過型」を導入している場合には、カード情報を保持しない非通過型への移行か、カード情報を保持する必要がある場合は、PCI DSS に準拠しなければならない。

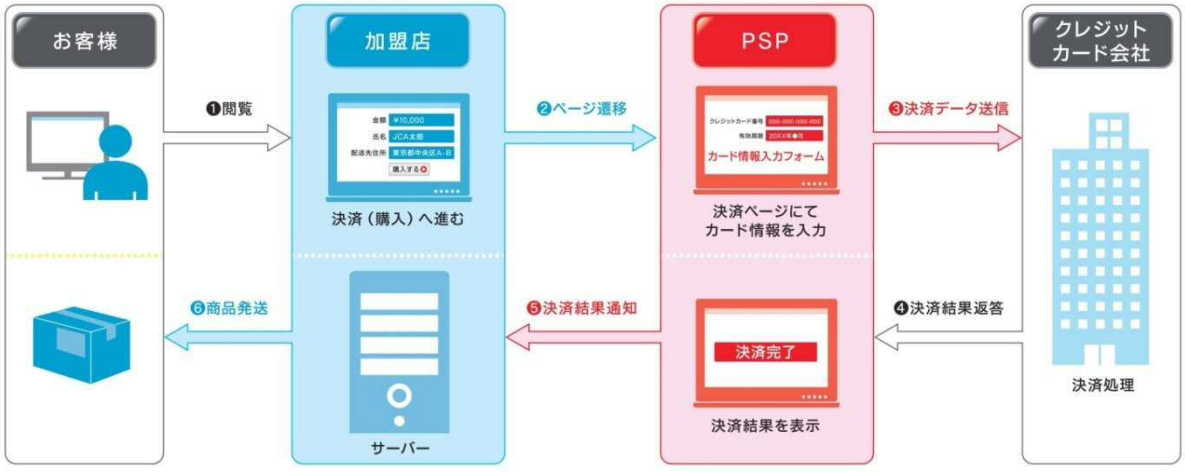
□EC 加盟店における非保持化導入例

方策		概要
非通過型	❶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
	❷Java Script 型（トークン型）	加盟店の決済画面に PSP が提供する Java Script プログラムを組み込んで利用し、決済を行う方式

❶リダイレクト（リンク）型

EC 加盟店においてカード決済処理を行うのではなく、PSP において決済処理する方式。カード情報入力画面は、加盟店サイトの購入画面から PSP が提供する決済画面に遷移させカード決済を行うため、加盟店ではカード情報を保持しない。

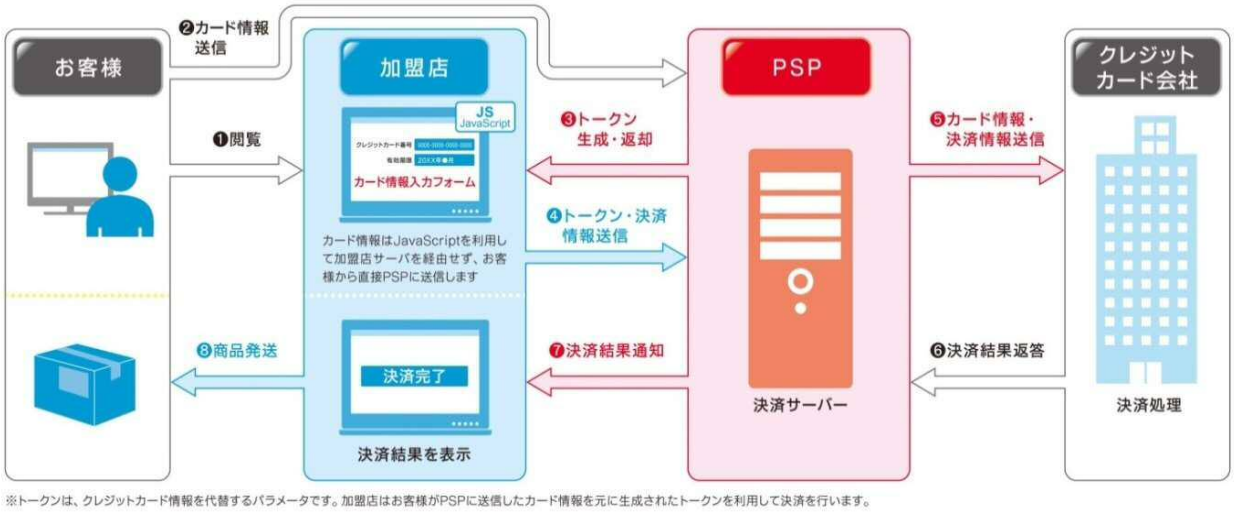
【❶リダイレクト（リンク）型】
（決済画面は PSP のサイトへ遷移する）



❷Java Script 型（トークン型）

EC 加盟店のカード情報入力画面に、PSP が提供する Java Script プログラムを組み込み、それを利用することで決済を行う方式。カード情報は Java Script を利用して加盟店サーバーを経由せず、利用者から直接 PSP に送信するため加盟店ではカード情報を保持しない。

【❷Java 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）



b）メールオーダー・テレフォンオーダー加盟店の対策

＜具体的方策の考え方＞

ア）MO・TO 加盟店が、顧客から電話・FAX・はがき等でカード情報を入手し、MO・TO 加盟店の機器にカード情報を入力して決済を行っている場合には、カード情報を電磁的情報として自社内に「通過」させない外回り方式を導入することにより、非保持化を実現することが可能である。

イ）PCI P2PE*認定ソリューションは、カード会員データを特定できない状態とし、自社内で復号できない仕組みであり、仮に情報を窃取されてもカード情報として不正に利用することは極めて困難であることから、PCI P2PE*認定ソリューションを導入することにより、非保持と同等/相当のセキュリティ措置を実現することが可能である。（この場合には、PCI DSS 準拠までは求めないこととする。）

※MO・TO 加盟店における対策の詳細は、「【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。

□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

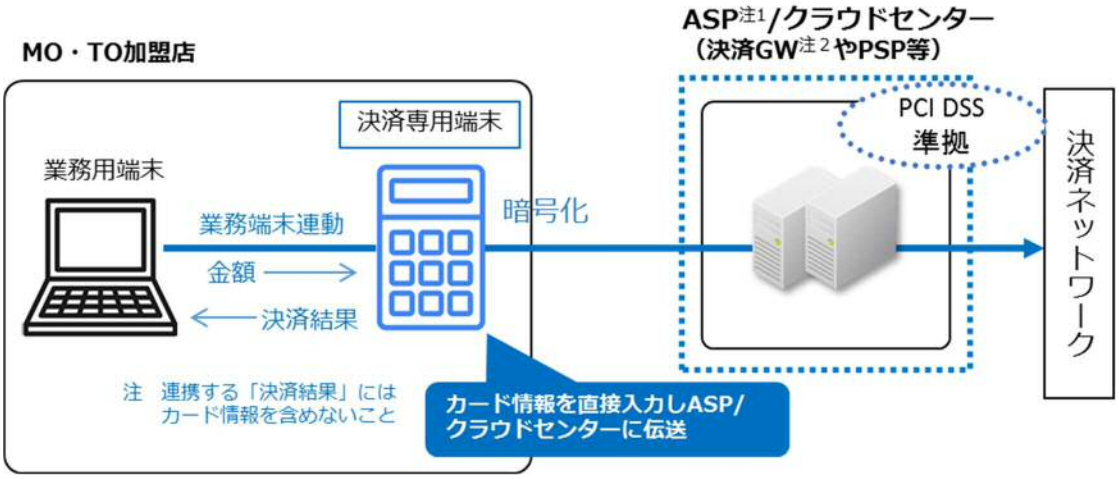
方策		概要
非通過型（外回り方式）	❶非保持化	決済専用端末を利用した外回り方式
	❷非保持化	タブレット端末※を利用した外回り方式
❸非保持と同等/相当（内回り方式）		PCI P2PE 認定ソリューションを導入した内回り方式

※非保持化のためにカード情報の取扱いを委託した PSP から提供される端末の例示

❶非保持化　決済専用端末を利用した外回り方式

PCI DSS に準拠した ASP/クラウドセンターより貸与された、CCT*（Credit Center Terminal）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使用して決済を行う方式である。カード情報を MO/TO 加盟店が自社で保有する機器である業務用端末ではなく決済専用端末に入力することにより、外回りによる非保持化を実現するものである。当該決済専用端末と MO/TO 加盟店の業務用端末との接続を行い、金額を連動させる場合には、業務用端末側の決済結果に、カード情報を含めないこと及び、通信回線はキャリア等の外部の回線を使用することが必要である。

【❶非保持化　決済専用端末を利用した外回り方式】



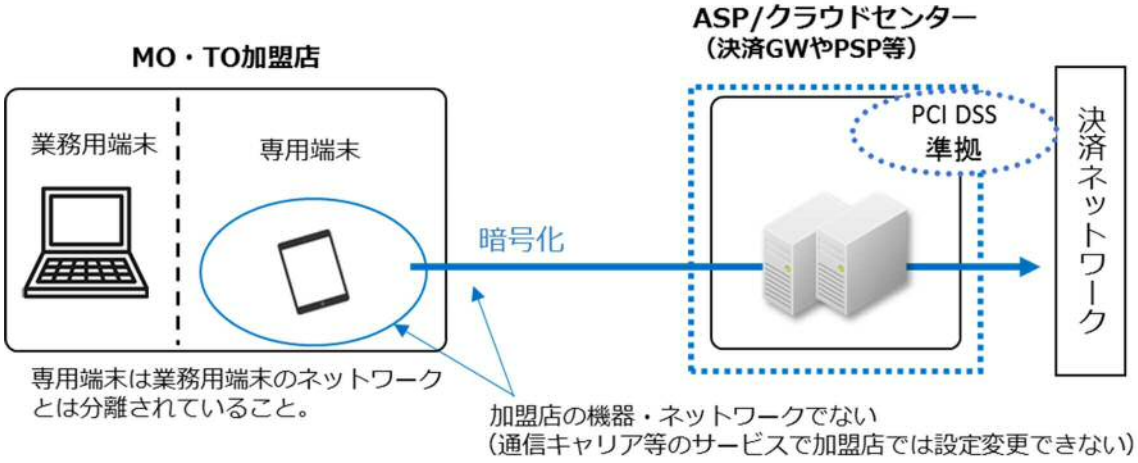
注 1　ASP は Application Service Provider の略

注 2　決済 GW は決済ゲートウェイの略

❷非保持化　タブレット等の専用端末を利用した外回り方式

MO/TO 加盟店のオペレーターが、PSP 等から提供されたタブレット等の専用端末の機器・ネットワークを利用して自社の EC サイトで注文情報を入力する方式。タブレット等の専用端末は業務用端末のネットワークとは分離されていることが条件となる。

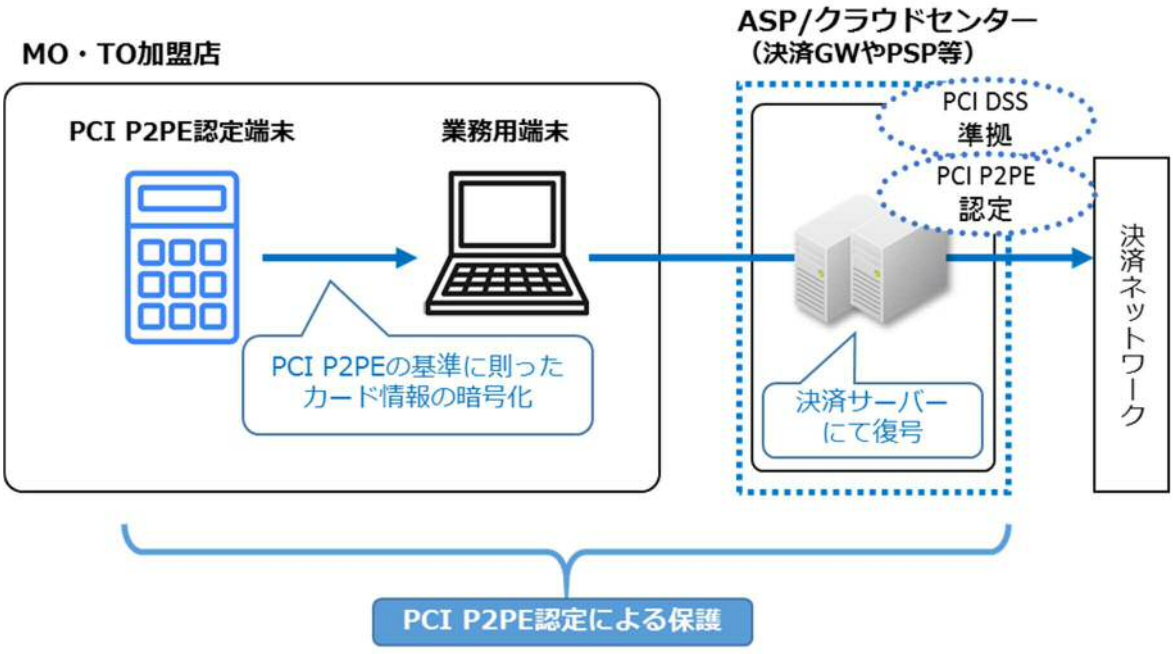
【❷非保持化　タブレット等の専用端末を利用した外回り方式】



❸非保持と同等/相当　PCI P2PE 認定ソリューション端末を利用した内回り方式

「PCI P2PE」は、カード会員データを、カードリーダーデバイスから決済処理ポイントまでの加盟店自社内を DUKPT*（Derived Unique Key Per Transaction の略。トランザクションごとにデータの暗号鍵が異なる暗号鍵管理の仕組み）により安全に伝送処理する方式。
PCI P2PE 認定ソリューション端末の利用により、カード会員データは暗号化され、トランザクションごとに暗号鍵が異なることから、多量なカード会員データを解読することは事実上困難である。このため仮に解読された場合であっても、使用が可能となるカード番号は極めて限定的であるため、不正利用されるリスクは極めて低いことから、非保持と同等/相当の対策となる。

【❸非保持と同等/相当　PCI P2PE 認定ソリューション端末を利用した内回り方式】



２）対面加盟店における非保持化対策

＜具体的方策の考え方＞

ア）POS システムを導入している加盟店では POS の機能と決済の機能を分離し、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」を導入することにより非保持化を実現することが可能である。

イ）カード会員データを特定できない状態とし、自社内で復号できない仕組みとすれば、仮に窃取されてもカード情報として不正に利用することは極めて困難であるため、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※を満たすことにより（「内回り方式」）、非保持と同等/相当のセキュリティ対策を実現することが可能である。（この場合には、PCI DSS 準拠までは求めないこととする。）

※セキュリティ技術要件に適合するセキュリティ基準については「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。

＜留意事項＞

・カード会社や ASP/クラウドセンター等を運営する事業者から、カード情報の還元を受け自社で保有する機器・ネットワークにおいて「保存」「処理」「通過」している場合（決済以外の目的の場合も含む）は、カード情報の保持となるため PCI DSS の準拠が必要。

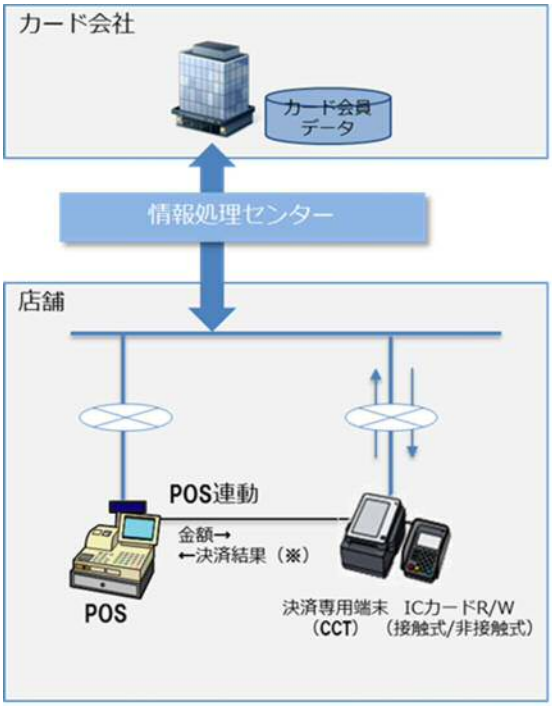
□対面加盟店における非保持化（非保持と同等/相当を含む）導入例

方策		概要
非保持化（外回り方式）	❶非保持化	決済専用端末連動型
	❷非保持化	ASP/クラウド接続型
❸非保持と同等/相当（内回り方式）		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よる内回り方式

❶・❷非保持化　決済専用端末連動型・ASP/クラウド接続型（外回り方式）

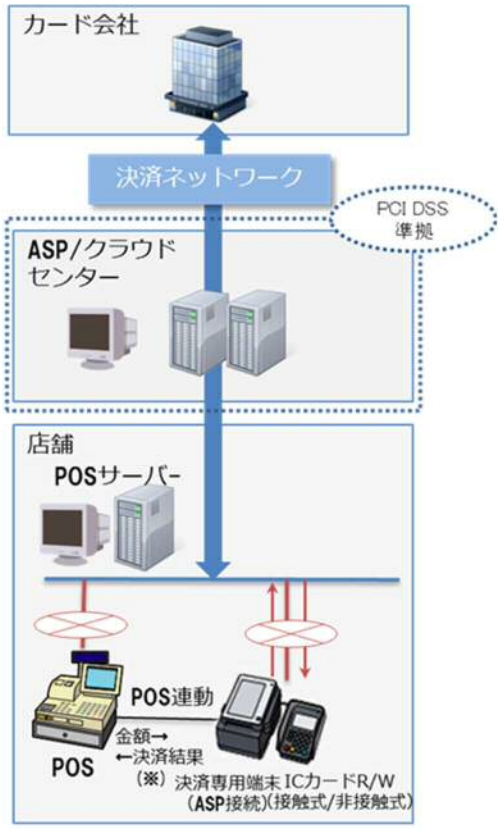
オーソリゼーションやクレジットカードの売上処理を、加盟店あるいはカード会社等が所有する決済専用端末から直接外部の情報処理センター又は ASP/クラウドセンター等に伝送して行う方式である。この方式では、POS に連動する場合「決済結果」にカード情報が含まれないようにする必要がある。両方式とも、決済機能は POS システムの外側となるため、カード情報が POS 端末や POS システムの機器・ネットワークを「保存」「処理」「通過」しないことから、カード情報の非保持化が実現可能である。また、加盟店が POS システムでクレジットカード決済を行わず「IC 対応*した決済専用端末」のみを使用し、カード情報を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となる。

【❶非保持化　決済専用端末連動型】



※POS 連動する「決済結果」にはカード情報を含めないこと

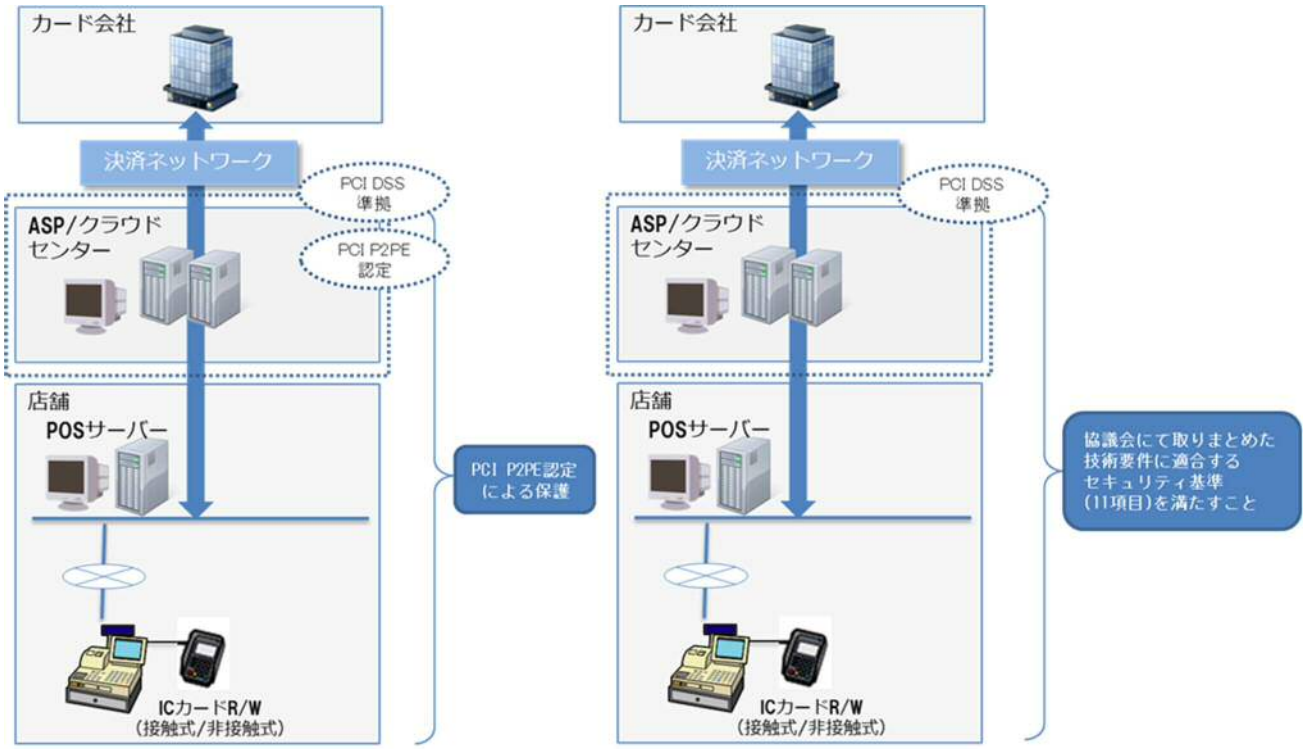
【❷非保持化　ASP/クラウド接続型】



❸非保持と同等/相当　ASP/クラウド接続型（内回り方式）

オーソリゼーションやクレジットカードの売上処理のため、カード情報が決済端末から POS システム又は自社内システムを介して外部の情報処理センター又は ASP 事業者等へ伝送される方式である。この場合、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」するため、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とりまとめた「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。

【❸非保持と同等/相当　ASP/クラウド接続型（内回り方式）】



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

クレジットカードを利用した顧客からの返品や購入金額の訂正等の照会に対し、クレジットカード番号等を用いてカード会社（アクワイアラー）への連絡、確認等を行っていた加盟店については、非保持化を実現した場合、以下のような対応が考えられる。

（非対面加盟店）

非対面加盟店においては、通常 PSP がカード情報を保有しているため、カード情報を非保持化した場合でも、PSP が仲介を行うことで従来通り顧客からの照会等への対応が可能である。

（対面加盟店）

対面加盟店のうち決済専用端末を導入している加盟店においては、クレジットカード番号の一部非表示化が図られており、一部非表示化されたクレジットカード番号に加え、利用日、利用金額、端末番号、伝票番号等により顧客からの照会等への対応が可能である。

一方、決済専用端末導入以外の方法にて非保持化（非保持と同等/相当を含む）を実現した加盟店では、クレジットカード番号以外の取引を特定するための照会キー（伝票番号、取引日時、金額等）により照会を行うこととなるが、これらの照会キーのみでは対象取引を特定できないこともある。また、全ての加盟店とカード会社が一律に、クレジットカード番号を保持していた時と同様の対応を行うことは現状困難であるため、クレジットカード番号を

基本としつつ、加盟店の委託先の PCI DSS に準拠した ASP 事業者から一時的にクレジットカード番号を取り寄せるなど、加盟店、カード会社双方で照会する必要がある。

（非対面・対面加盟店）

非保持化（非保持と同等/相当を含む）を実現した加盟店が顧客照会等の際、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、紙媒体をスキャンした画像データ、電話での通話記録（音声データを含む）を利用する方法や、PCI 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に加盟店がアクセスし、一時的にクレジットカード番号を入手・利用する方法は、非保持化後も認められる。なお、顧客対応については、加盟店の運用実態により異なることから、これらの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、個別に対応を実施することが重要である。

ｂ）過去に取り扱ったカード情報の保護対策

非保持化（非保持と同等/相当を含む）を実現した加盟店において、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非保持化対応完了以前に取り扱った過去のカード情報を画像データ以外のテキスト形式等で電子帳票として保存する場合、本協議会にて定めたセキュリティ対策※を行う必要がある。

※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であり、カード情報の保護方法に関しては、管理責任者のもとで第三者に持ち出されて閲覧されない方法により適切な管理が行われていること。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（非保持と同等/相当を含む）を実現した加盟店であっても、継続的な情報保護に関する従業員教育やウイルス対策、デバイス管理等について情報漏えい防止のための必要なセキュリティ対策が求められる。

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 の要件に基づき約 400 項目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事項が異なることから、自社が対応するべき事項を検証し、準拠する必要がある。

なお、PCI DSS 認定審査機関（QSA）の団体である日本カード情報セキュリティ協議会（以下「JCDSC」という）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDSC ホームページ　https://www.jcdsc.org/）。

（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

■決済代行業者等については、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。

（4）コード決済事業者等

■コード決済事業者等については、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

■非保持化を実現した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。

④業界団体等

■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。

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発生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被害の拡大を防ぐために早急に行動を起こす必要がある。具体的には、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 準拠等の確認及び再発防止のための適切な措置を講じる。

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。

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

対面取引の不正利用対策であるIC取引については、割賦販売法によるセキュリティ対策の義務化により加盟店の決済端末のIC対応が進み、カードのIC化についても本協議会の取組により、ほぼ全ての国内発行カードがIC化されている。このようなIC取引の進展により、対面取引による不正利用被害は減少傾向が続いており、対面取引のクレジットカードの不正利用対策は、現時点においてはIC取引が最も効果的な対策である。

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対応にする。【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対応に係る実現方法を選択する際には、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。

①POSシステムのIC対応に係る実現方式例

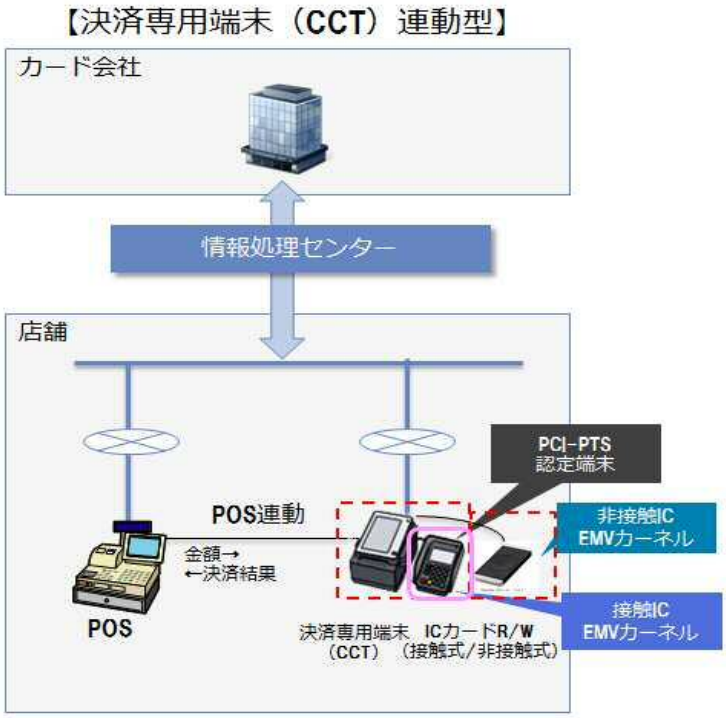
IC対応の実現方式としては、各加盟店の現行システムや店頭オペレーションの特徴を踏まえ、技術面、コスト面から検証・整理を行うと、決済専用端末（CCT）連動型、決済サーバー接続型、ASP/クラウド接続型に大別される。以下に示すIC対応の型別の構成図は、コスト削減を目的としたインターフェースの標準化、ブランド認定/テストの簡素化の観点からの推奨例を示したものである。

※詳細は、「ICカード対応POSガイドライン」を参照。また、カード情報保護の観点からのパターン別構成図は、「Ⅰ．クレジットカード情報保護対策分野」（14頁～15頁）の記載内容を参照。

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である。EMVカーネル*を決済専用端末やPINパッド*等に置くことで、クレジット決済処理をPOSシステムの処理端末と切り離して行うこととなるため、開発・EMV認定*・ブランドテスト*等については決済専用端末側（CCT）で対応すればよく、POSシステム側の対応が不要であることから、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（CCT）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[注]。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対応が必要となる。

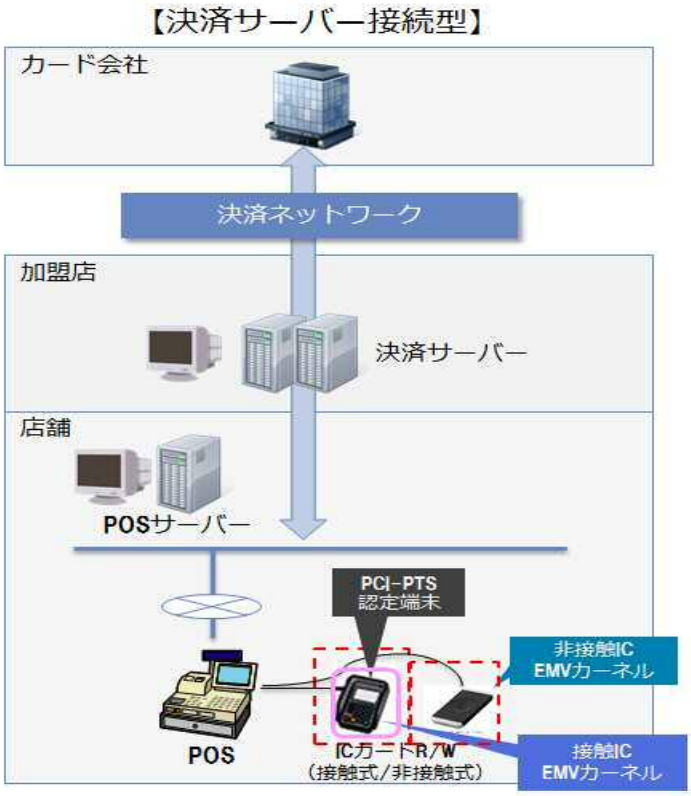
注　非保持化の実現においては、決済専用端末（CCT）よりPOSへ連動する「決済結果」にカード情報を含めないことが前提。



２）決済サーバー接続型

EMV カーネルを PIN パッドに置き、POS システムでクレジットカード決済を行う仕組みである。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、導入による対応の影響が小さい。

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、カード情報が自社で保有する機器・ネットワークを「保存」「処理」「通過」し、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。

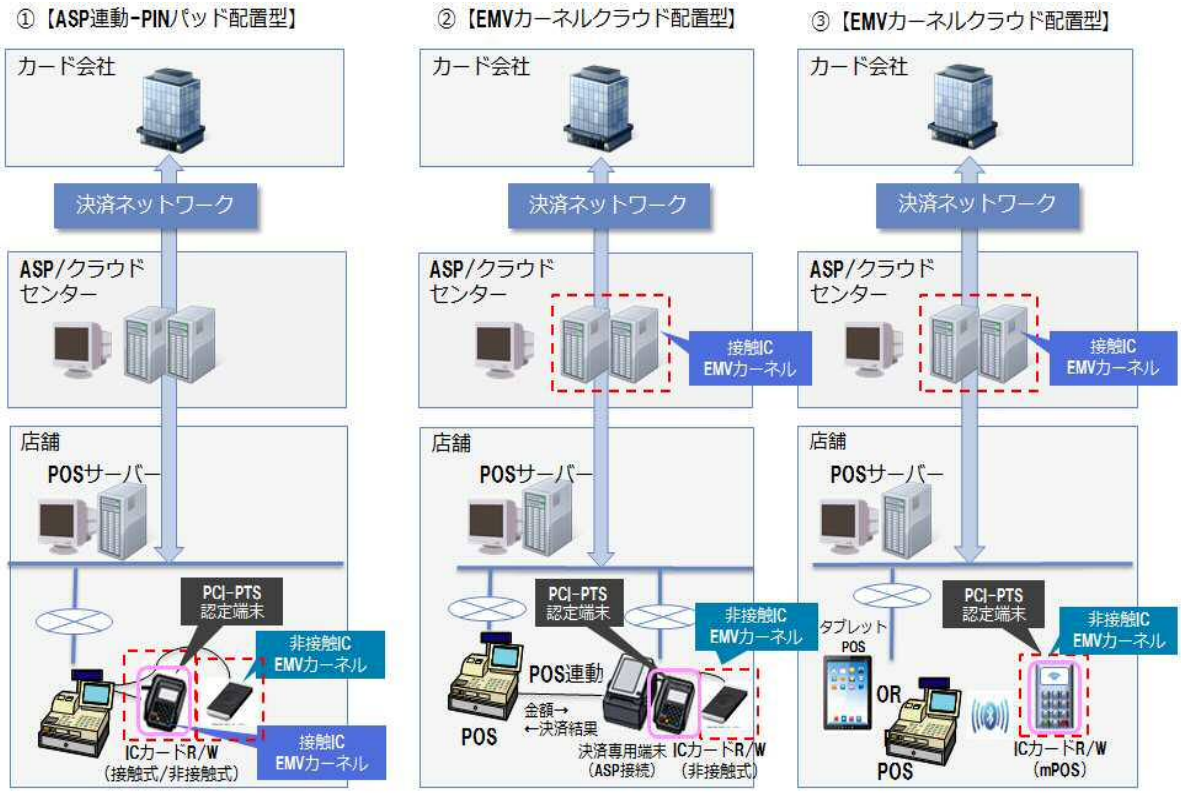


3）ASP/クラウド接続型

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である。基本的には前記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（下記概要図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[注]。下記概要図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とりまとめた「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　非保持化の実現においては POS に連動する「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。



②クレジットカード決済に POS システムを用いない加盟店等の対応

POS システムを導入していない加盟店又は POS システムをクレジットカード決済に用いていない加盟店については、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といったサービス（フルサービス）を行う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、代替コントロール策の導入が必要となる。このため、同様の課題を抱える一部の業界と合わせて対応の指針として「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」をとりまとめており、これらの課題が解決するまでの間は、この指針に基づいて対応することとする。

また、ガソリンスタンドにおけるIC対応については、上記のような業界固有の課題を踏まえ「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」に実現可能な方策をとりまとめており、同指針に基づく対応によりIC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」及び「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、PCI SSC*が定めた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」を参照。

□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 システムでクレジットカード決済を行う加盟店	次の実現方式による 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 システム以外でクレジットカード決済を行う加盟店	IC 対応決済専用端末（CCT）の導入
特定業界の加盟店	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」に基づく実現可能な方策による IC 対応 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」に基づく代替コントロール策による IC 対応

（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、「2. IC 取引時のオペレーションルール（33 頁を参照）」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。

（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
■加盟店における IC 対応に関し、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。

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。

2．IC 取引時のオペレーションルール

カード会社は、IC 取引上の本人確認方法等のオペレーションについては、日本クレジット協会が策定したクレジットカード業界としての IC 取引時のオペレーションルールである、「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」に基づき対応することとする。

加盟店や機器メーカーは、上記クレジットカード業界としての IC 取引時のオペレーションルールに基づき、IC 取引を推進することとする。

同ガイドラインに基づく IC 取引における本人確認方法の大別は以下のとおり。

（1）接触 IC 取引

接触 IC 取引は、決済端末に IC カードを挿入しカード券面上に露出した IC チップの接触端子からカード情報を読み込んで処理を行うものである。

・カード偽造防止のみならず、紛失・盗難カードによる不正利用被害抑制のため、原則 PIN 入力による本人確認を行うこととする。カード利用時にカード会員が入力した PIN の照合方法には、カードの IC チップ内に保存された PIN と照合する「オフライン PIN*」とオンラインネットワークを経由してカード会社（イシュアー）のシステム上で照合する「オンライン PIN」があるが、現状の我が国の決済インフラを考慮すると「オフライン PIN」が最適な本人確認方法である。

・一部の海外発行カードでは、「オフライン PIN」環境では利用を許容しないカードが存在するため、これらのカード利用時の本人確認にも対応できるようサイン記入欄が印字可能な機能やサインパッド等の装備も必須とする。
・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る、決済処理の迅速性が求められる業種業態の加盟店においては、CVM リミット金額[注]*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。ただし、不正利用防止の観点から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、換金性の高い商品を除外する。
・なお、本人確認が不要とされる取引は、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、IC 取引時のオペレーションルールに基づき、全件オンラインオーソリゼーションを必須とする。
・上記の接触 IC 取引オペレーションを実現するため、国内の IC 決済端末には、オフライン PIN 機能と本人確認を不要とする No CVM*機能が装備されていることが必須となる。No CVM を実現させるために採用する具体的な実現方式は、セレクタブルカーネルコンフィグレーション方式とする。同方式は、決済アプリケーションの機能にて取引単位で端末が指定する本人確認方法の切り替えを可能とする EMV カーネルの実装方式であり、EMV 仕様に準拠しつつ、「本人確認要（PIN/サイン）」と「本人確認不要」の両方の取引を一つの装置で実現する方式である。本方式により、原則「オフライン PIN」の考え方に則り、CVM リミット金額以下は本人確認不要取引を認めつつ、CVM リミット金額超では「オフライン PIN」での本人確認が可能となる。

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

（２）非接触 IC 取引

非接触 IC 取引は、決済端末に IC カードをかざす通信により、カード券面の内部に搭載された IC チップ内のカード情報を読み取り処理を行うものである。

・非接触 IC 取引の形態は、「カード型」とスマートフォン等を用いた「モバイル型等（『キーホルダー型』や『ウェアラブル型：リストバンドや時計等の身に着けて使用』）を含む」に分けられる。
・非接触 IC 取引の多くは少額での決済が中心であり、CVM リミット金額以下になること、消費者の利便性を勘案し、CVM リミット金額以下の取引においては、本人確認不要とすることができるものとする。
・CVM リミット金額を超える取引においては、以下のとおりカード会員が提示する媒体に応じて本人確認を行う。

①カード型

・CVM リミット金額超の取引については、非接触 IC 取引から接触 IC 取引に切り替え、オフライン PIN による本人確認を行う。接触 IC 取引への切り替えができないカードの場合には、サインによる本人確認を許容する。

②モバイル型等

・CVM リミット金額超の取引については、Consumer Device CVM (モバイル型等のパスワードや指紋認証等の機能)もしくはサインを用いた本人確認を行う。

このため、日本国内の接触 IC/非接触 IC の処理をする決済端末には、カード型対応のために「No CVM（本人確認不要）機能」「オフライン PIN 機能」及び「サイン機能」また、モバイル型対応のために「No CVM（本人確認不要）機能」「Consumer Device CVM 機能」及び「サイン機能」の装備を必須とする。

IC 取引時のオペレーションルール

□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[注1]）	[接触 IC 取引へ切替え] 原則 オフライン PIN （切替え不可の場合 サインを許容[注2]）	Consumer Device CVM （モバイル PIN/指紋等）もしくはサイン

注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 注２　非接触 IC 取引の「カード型」において、接触 IC 取引への切り替えを許容しないカードが存在するため

※詳細は「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」を参照。

３．その他留意事項

（１）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及び PIN バイパスの廃止等の検討開始について

・我が国クレジットカード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カード券面上の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取組んできた経緯がある。

・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、一般的には PIN 入力により本人確認が行われているが、例えば、海外イシュアーが発行したオフライン PIN 環境に対応しないカードが利用される場面や、今後一層の利用拡大が見込まれる非接触 IC 取引については本ガイドラインにおいても規定しているように、CVM リミット金額を超える取引の際にサインによる本人確認を行う場合があることから、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浸透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では、サインを取得するか否かは加盟店による裁量に委ねられており（任意化）、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は低下している。こういった状況を踏まえ、我が国においても加盟店によるサインの取得を将来的に任意としていくことについて、本協議会として具体的な検討に着手することとする。

・また、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、PIN 入力による本人確認の未実施により不正利用被害を発生させるリスクがあるため、業界としても将来的な PIN バイパスの廃止を検討する必要性を認識していたところである。上述のとおり、本人確認としてのサインの有効性の低下によりその取得を任意とした場合、当該救済措置としての同機能の存在意義も失われることになるため、これを契機に、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。

・これら検討にあたっては、紙の売上票の削減や No CVM（本人確認不要取引）の見直し等の周辺領域の検討と併せて、具体的な方向性を示していくこととする。

・なお、このサイン取得の任意化の適用にあたっては、冒頭で述べた我が国市場におけるこれまでの経緯を踏まえ、そのステークホルダーに与える影響の大きさに鑑み混乱を招かぬよう、カード会員と加盟店への周知、準備と移行のための十分な期間を設定する予定である。

（２）POS システムの IC 対応に係る各種ガイドライン等（附属文書）

POS システムの IC 対応にあたっては、接触 IC 取引を対象とした「IC カード対応 POS ガイドライン」と各種手引き、非接触 IC 取引を対象とした「非接触型 EMV 対応 POS ガイドライン（全体概要編・取引処理編）」がとりまとめられている。

機器メーカー、加盟店及び情報処理センターは、これら各附属文書に留意し、IC 取引実現上の必要な対応を行うこととする。

（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

非対面取引の加盟店には、カタログやテレビを見て、はがきや電話で注文が行われるいわゆるメールオーダー・テレフォンオーダーによる通信販売の MO・TO 加盟店とインターネットを利用して注文が行われる電子商取引の加盟店（EC 加盟店）があるが、不正利用被害のほとんどは、EC 加盟店において発生している。また、同被害額は引続き高水準にあると言える。

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犯罪者により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。

このような不正利用の発生状況等を踏まえ、非対面取引の加盟店、特に EC 加盟店における非対面不正利用被害を極小化するためには、関係事業者において、取引の真正性を確認する的確な対応が求められる。

１．各事業者に求められる対策等

（１）加盟店

■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カード利用の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。本年度協議会の非対面不正対応 WG で行った調査においても、引き続き複数の方策を導入した加盟店において、不正利用の抑止の効果を確認している。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。

①加盟店における非対面不正利用対策の具体的方策

１）本人認証

EC 加盟店における非対面不正利用防止のための本人認証の具体的手法として、3-D セキュア*や認証アシストがある。これらは、カード会員に特定のパスワードや属性情報等を入力させること等で、利用者本人が取引を行っていることを確認するものである。

ａ）3-D セキュア

・利用者がカード会員本人であることを確認する仕組みであり、カード会員以外の利用を防ぐ手段である。カード会員のみが知るパスワード（静的・動的）を利用したパスワード認証や過去の不正利用実績やデバイス情報等を活用したリスク評価によるリスクベース認証があり、国際ブランドが推奨する本人確認手法である。

・海外では 3-D セキュア 1.0 がバージョンアップされた「EMV 3-D セキュア*」の運用が開始されている。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。

・また、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」の解消にも資するものである。

ｂ）認証アシスト

・「認証アシスト」とは、カードのオーソリゼーション電文を用いて、加盟店が特定のカード会員の属性情報をカード会社（イシュアー）に送信し、カード会社（イシュアー）が自社に予め登録している属性情報と照合し、利用者本人が取引を行っていることを確認する手法である。カード会社（イシュアー）が保有するカード会員本人の属性情報を用いた認証方法であるため、カード会員によるパスワード失念等を懸念することなく運用が可能であることが特徴である。

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」を認証することにより真正なカードが利用されていることを確認する手法である。

・「セキュリティコード」による認証は、使用するクレジットカード番号が真正であることをカード会社（イシュアー）が確認できること、セキュリティコード自体がカード会社（イシュアー）及びそのカード会員のカードに 100%普及していること、カード会員が認証で使用する番号を失念する懸念がないこと、既存のオーソリゼーション電文の活用で導入できること等の点で評価されている。

３）属性・行動分析（不正検知システム）

・非対面取引でのカード利用時に、利用者の入力情報（氏名、クレジットカード番号、メールアドレス等）、利用者の利用端末（PC・モバイル等）情報であるデバイス情報、IP アドレス、過去の取引情報、取引頻度等収集した情報の分析に基づいて、取引のリスク評価

（スコアリング等）を行い、不正な利用であるか加盟店側で判定する手法である。なお、日本クレジット協会の非対面不正利用対策検討 WG の報告でも、本方策により加盟店の不正検知精度の向上が確認されている。

・不正利用の手口や傾向は変化するため、「属性・行動分析（不正検知システム）」のツールにおいては、不正利用傾向の分析に基づき構築された不正判定の条件設定を更新・変更する機能を有することが必要である。真正/不正の判別が正当であったか否かについて、カード会社等から提供される不正利用の情報等により確認し、常に条件設定を最新化しておくことが望まれる。

4）配送先情報

・不正利用された注文等の商品の配送先情報を蓄積することで、取引成立後であっても商品等の配送を事前に止めることで不正利用被害を防止する手法である。ただし、規模の小さい加盟店では、他の加盟店で発生した不正事例含めた不正利用に使われた配送先情報の把握が困難であることから、外部のベンダーや企業が提供するサービスを利用することも有効である。現在、大手加盟店が独自のデータベースを運用しているほか、カード会社複数社が共同で運用しているサービスやシステムベンダーが提供するサービスがある。

・「配送先情報」による不正利用対策では、加盟店自らが取引顧客の配送先情報から、不正な取引か否かの判断を行うため、加盟店において不正判断のノウハウを蓄積し、対策実施のための体制構築が必要となる。

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 ・機械的にクレジット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―）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 ・個々の取引を人的対応によって判定するのではなく、上記の条件設定による自動判定が行われることが重要で、更に、即時判定機能を導入すれば、短時間に連続した不正判定が行われる場合でも即時に検知・拒否することが可能
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を利用しないと期待する効果が得られない）

②加盟店における方策導入の指針

加盟店の取り扱う商材や不正利用の被害発生状況等を踏まえ、加盟店のリスクや被害発生の状況等に応じ、以下の考え方にて、前述の非対面不正利用防止の 4 つの方策をベースとした対策を導入する。

１）全ての非対面加盟店

全ての非対面加盟店は、不正利用犯の標的になり得ることから、リスクや被害発生の状況にかかわらず、方策の導入が求められる。全ての非対面加盟店の不正利用防止のための方策としては、加盟店契約に定める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、リスク評価を含めたカード会社（イシュアー）の承認判定を得るためのオーソリゼーション処理が必要である。

さらに、以下の加盟店は、不正利用の発生リスクや被害発生の状況に応じた方策を導入しなければならない。なお、昨今、リスト型攻撃（システムを利用し短時間に大量の購入申込を行う）による不正利用が発生していることから、不正利用が継続的に発生していない加盟店であっても、カード会社（アクワイアラー）から、短期間に不正利用が急増し不正利用防止の対応が必要であることの情報連携を受けた場合は、追加的な方策の導入が必要となる。

２）高リスク商材取扱加盟店

不正利用被害の発生状況からリスクの高い商材として選定した①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット、⑤宿泊予約サービスを主たる商材として取り扱う加盟店には、「高リスク商材取扱加盟店」として、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 方策以上の導入を求める。

なお、ここでいう③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。「44 頁⑤及び 45 頁②参照」

３）不正顕在化加盟店

カード会社（アクワイアラー）等が不正利用被害が多発状況にあると認識する加盟店は「不正顕在化加盟店」として、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 方策以上の導入が必要である。なお、「不正顕在化加盟店」の対象は、カード会社（アクワイアラー）各社が把握する不正利用金額が「3 ヵ月連続 50 万円超」に該当する加盟店とする。

また、4 つの方策のうち 2 方策以上を導入していても不正利用被害が減少せず、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。

＜加盟店分類表＞

1）全ての非対面加盟店 **〇カード取引に対する善管注意義務の履行** **〇オーソリゼーション処理**
2）高リスク商材取扱加盟店 **〇本ガイドラインが掲げる非対面不正利用対策の 4 方策のうち、1 方策以上**
3）不正顕在化加盟店 **〇本ガイドラインが掲げる非対面不正利用対策の 4 方策のうち、2 方策以上**

〇印は求められる措置

③大量かつ連続する購入申込への対応

昨今の EC 加盟店に対するクレジットカードの不正利用は、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という手口が大多数を占めている。このような手口では、真正なカード会員がカード番号等を入力して購入申込を行う場合と比較すると、その申込速度や連続性の点が明らかに異なることから、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。

（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 EMV 3-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。
■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。
■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。

①EMV 3-D セキュアへの対応

3-D セキュアについては、現行の 3-D セキュアからバージョンアップされた「EMV 3-D セキュア」の運用が海外を中心に開始されている。EMV 3-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。

②「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」において、ACS*ベンダーがカード会社（イシュアー）に対し、イシュアー版の属性・行動分析（不正検知システム）である「リスクベース認証」を提供しており、導入したカード会社（イシュアー）において不正利用の抑止効果が認められている。

本機能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。

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推進する。

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。

⑥カード会員向け利用確認メール等通知

「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」は、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。

一方、本通知を導入する場合には、カード会社（イシュアー）は、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

「セキュリティコード」は桁数が少ないため、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。

（3）カード会社（アクワイアラー）及び 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。

「（1）②加盟店における方策導入の指針（41 頁を参照）」

■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問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。
「（1）①加盟店における非対面不正利用対策の具体的方策（39 頁を参照）」
■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。

①EMV 3-D セキュアへの対応

本ガイドラインで掲げる方策の一つである本人認証の 3-D セキュアについては、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について

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。

（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。

Ⅲ．消費者及び事業者等への周知・啓発について

クレジットカード取引のセキュリティ対策を強化することは、消費者の安全・安心な消費生活による快適な環境づくりに資することから、消費者の理解・協力を得つつ推進することが重要である。

こうした観点から、消費者への周知・啓発は様々な機会を捉えて各関係事業者が積極的に行うことが必要であり、日本クレジット協会は行政とともに、加盟店業界団体、消費者団体等と連携の上、クレジットカード情報の保護対策及び不正利用対策に関する消費者及び関係事業者向けの周知・啓発に取組む。カード会社（イシュアー）はカード会員向け、カード会社（アクワイアラー）及び PSP は契約加盟店向けの周知・啓発活動等を強化するものとし、各関係事業者は以下の取組を行う。

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消費者がセキュリティ対策導入済み加盟店を認識・識別できる「見える化」への取組に努める。

■EC 加盟店は、カード会社（アクワイアラー）及び PSP と連携し、本ガイドラインで求められるクレジットカード情報の保護対策及び不正利用対策を講じている場合には、自社 EC サイトのサービス紹介ページや決済画面等のサイトにおいて、本ガイドラインに取組んでいることを表示（自己宣言）し、消費者がセキュリティ対策導入済み加盟店を認識・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）

■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。

■カード会員等に対し、IC 取引では本人確認のため PIN 入力が必要になることから、「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 における不正利用対策の導入・普及には、カードの不正利用対策の必要性やカード利用時に求められる場合のあるセキュリティコードやパスワードの利用方法等、具体的なセキュリティ対策に関するカード会員の理解・協力を得ることが重要であることから、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。

■EC 加盟店における不正利用を防止するためには、本人認証サービス等の方策を取ることが有効であるが、カード会員が複数のインターネットサイトで同一の ID・パスワードを使い回している場合、一つのサイトでカード情報が漏えいすれば、他のサイトに不正ログインされ、登録されているカード情報等が不正利用される可能性があることから、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・啓発を行う。加えて、その他の本人認証の手法を導入する場合も同様である。

■フィッシング被害を防止するためには、カード会員がその手口等を理解し、不審と思われるサイトにはカード情報等の入力を行わないことが重要であることから、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。
■不正利用による被害を防止するためには、カード会員自身がカードの利用明細をチェックし、不正利用の発生に早期に気付くことが重要であることから、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等に関する周知活動を積極的に行う。

（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等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、とりわけ 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 における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等に関する周知活動を積極的に行う。

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。

【履歴】

2020 年 3 月 19 日　　新規制定　1.0 版

2021 年 3 月 10 日　　改定　2.0 版