クレジットカード・セキュリティガイドライン【5.0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

第１章　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 2020 年 3 月にとりまとめて以降、4 回目の改訂となる。

我が国では、政府の政策としてキャッシュレス化を推進し、2025 年 6 月までにキャッシュレス決済比率 40%を目指す目標を打ち立てている。2022 年現在、我が国のキャッシュレス決済比率は 36.0%に増加しており、多様なキャッシュレス決済がある中で、クレジットカード決済は依然として圧倒的なウェイト（84.5%）を占めている。一方、クレジットカード情報の盗用による非対面不正利用の被害は依然として高い水準で推移している。このような状況は、非保持化を達成した EC 加盟店の設定の不備や既知の脆弱性を悪用した悪意のある第三者の不正アクセスによるクレジットカード情報の窃取、大量かつ連続する不正アタックによるクレジットカード番号の有効性確認、フィッシングによるクレジットカード情報の窃取等により不正に取得されたクレジットカード情報や静的（固定）パスワードが、コード決済や EC 加盟店で悪用されているものと考えられる。

このようなクレジットカード情報の窃取や不正利用を防止するため、EC 加盟店におけるカード情報保護対策及び本人認証を強化するための取組が求められる状況にある。加えて、キャッシュレス化の進展に伴い、カードレスやモバイルの利用が拡大しており、新たな決済の仕組みに応じた取引ルールの見直しや、消費者に対するフィッシングへの注意喚起、クレジットの安全・安心な利用に関する周知・啓発等の円滑な取組も必要となっている。

本協議会としてはこれまでも、非対面取引の情報保護対策としての基本的なセキュリティ対策の強化、不正利用対策としての本人認証の強化に向けて、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を本ガイドラインに掲載し、関係事業者に取組を求めてきたところであるが、上述のような状況を踏まえ、実効性あるセキュリティ対策を検討し、今般、クレジットカード・セキュリティガイドライン【5.0 版】として取りまとめたものである。

各関係事業者がクレジットカード決済環境の変化を踏まえ、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組まれることを引き続き期待する。

なお、本ガイドラインでは各事業者ごとに講じる対策をまとめているが、その対策は「カード情報保護対策」「不正利用対策」「周知・啓発」であり、それぞれの対策等の基本的な考え方はこの後に記載する。

2024 年 3 月

１－１　クレジットカード情報保護対策

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る個人情報やカード情報の窃取、さらには EC サイトの脆弱性やフィッシングによるカード利用者からの窃取、そしてそれらの窃取したカード情報を利用した不正利用は国内に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。

カード情報の漏えいは主に加盟店において発生していることから、カード情報を加盟店で保持しないことが有効なセキュリティ対策と考えられてきたが、最近の漏えい事故の傾向として、EC 加盟店においては非保持化を実施していたとしてもカード情報が窃取されている。このため、EC 加盟店については、カード情報の保持又は非保持にかかわらず、自社システムの定期的な点検を行い、この点検結果に基づき、必要があれば追加的な対策を導入するなどの適切な対策を講じることが求められる。

本ガイドラインにおいては、割賦販売法第 35 条の 16 第 1 項第 2 号に該当する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、さらに EC 加盟店に対しては、新規加盟店契約の申込みの際に、セキュリティ対策の実施状況の申告（試行）を求めている。また、同条同項第 1 号及び第 3 号から第 7 号に該当する事業者には、PCI DSS の準拠を求めている。

１－２　不正利用対策

１－２－１　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及び本協議会の取組により、加盟店の決済端末の IC 対応、カードの IC 化が普及、定着し、偽造カードによる不正利用被害は減少傾向が続いている。このことから、現時点においても対面取引の不正利用対策としては IC 取引が最も効果的な対策である。

１－２－２　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、インターネットを利用して注文する電子商取引の加盟店（EC 加盟店）と、カタログやテレビを見て、はがきや電話で注文す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（MO・TO 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おり、被害額は近年増加し続けている。日本クレジット協会の調査によると、2022 年のクレジットカード不正利用被害額は約 436 億円にのぼり、そのうちの約 9 割を番号盗用による被害が占めている。また、2023 年の不正利用被害額についても 1 月から 9 月の被害額が約 400 億円にのぼり、2022 年の被害額を上回ることは確実な状況にある。

非対面不正利用による被害が増加傾向にある背景としては、EC 加盟店からの情報漏えいや、フィッシングによるカード会員からのクレジットカード番号や静的（固定）パスワード等の窃取、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による不正利用が依然として発生しているためである。

このような不正利用の発生状況等を踏まえ、EC 加盟店の不正利用対策として、後述のとおり EC 加盟店が取扱う商材や不正利用の被害発生状況等から不正利用発生のリスクに応じて、非対面不正利用対策の 4 つの方策をベースとした複数の対策を導入することとしてきたが、EC 加盟店における非対面不正利用被害が増加している現状を踏まえ、2025 年 3 月末までに、原則、全ての EC 加盟店に EMV 3-D セキュアの導入を求めることとしている。割賦販売法第 35 条の 17 の 15 及び同施行規則第 133 条の 14 の規定も踏まえ、加盟店が、クレジットカード番号等の通知を受けた際、当該通知がイシュアーから当該クレジットカード番号等の交付等を受けた利用者によるものであるかの適切な確認をするための措置として、EMV 3-D セキュアの導入を求めるものである。

また、カード会社（イシュアー）によるカード会員の EMV 3-D セキュアの登録率の向上や動的（ワンタイム）パスワード等への移行が実施されないと不正利用の的確な防止、ひいては不正利用被害額の減少を実現することは困難であるため、加盟店による EMV 3-D セキュアの導入のみではなく、クレジットカード取引関係事業者それぞれが実施すべき対策があるところ、各事業者は、2025 年 3 月末までに、関係事業者と連携し、主体的に導入計画を作成し、それを実行することが強く望まれる。

なお、非対面不正利用対策として、4 つの方策をベースとした複数の対策を導入することを指針としてきたが、加盟店の業種や業態、取扱商品、不正利用の実態等により、効果的な不正利用対策が異なっており、複数の方策を導入したとしても実効的な抑止効果が得られにくいケースも散見されたことから、今後は、より抑止効果を高めるために、カード決済の場面（決済前・決済時・決済後）を考慮して、それぞれの場面ごとに対策を導入する取組が重要である。

第２章　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。

用　語	説　明
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。
EMV 3-D セキュア	オンラインショッピング時にクレジットカード番号等の情報の盗用による不正利用を防ぎ、安全にクレジットカード決済を行うために国際ブランドが推奨する本人認証サービス。 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、各カード会社（イシュアー）が、カード会員のデバイス情報等を用いて不正利用のリスク判断を行うとともに、必要に応じてパスワード入力を要求することで当該取引における安全性を確保する。 【EMV 3-D セキュア仕様の特徴について】 ①リスクベース認証で判定されたリスク度合いに応じて、認証処理は下記の通りフローが異なる。 ・低：フリクションレスフローとしてパスワード等の入力なしに認証が完結する。 ・中：チャレンジフローとして会員に対して追加の認証（パスワード等）を要求する。 ・高：認証拒否 ②ブラウザ（PC）を利用した取引に加え、スマートフォンやタブレットによるアプリケーションを利用した取引にも活用できる。 ③クレジットカード登録等、非決済分野での利用が可能。 詳細は、「EMV 3-D セキュア導入ガイド【附属文書 14】」参照。
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	Mail Orderの略語の「MO」とTelephone Orderの略語の「TO」を合わせた用語であるメールオーダー・テレフォンオーダー等のEC加盟店以外の非対面取引加盟店。
PCI DSS	Payment Card Industry Data Security Standard の略。 カード情報を取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。

用　語	説　明
	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。 ※　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。 ※　詳細は、「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【附属文書1】」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、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。
PIN バイパス	PIN（暗証番号）不知の一時的な救済措置として、カード会員に認められている PIN スキップ機能であり、「PIN」の代替として「サイン」による本人確認を行うものをいう。2025 年 3 月までに廃止する予定。
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。 ※　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 PSP 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セキュリティ評価機関。

用　語	説　明
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。
SDK	Software Development Kitの略。 スマートフォンのアプリ等のソフトウェアの開発にあたり、必要なプログラムや文書、サンプルコードなどをパッケージ化したもの。
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）	イシュアーと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 第 1 項第 1 号）のことをいう。 アクワイアラーとは、クレジットカード番号等取扱業者（割賦販売法第 35 条の 16 第 1 項）の 3 号事業者又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）をいう。
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、有効期限で構成されるデータをいう。
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、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。カード仕様の一部を構成する機密認証データは、PCI DSS によりそれ単体での保持も認められていない。 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 上記にかかわらず、2 号事業者以外の事業者には PCI DSS 準拠が求められる。
共通シンボルマーク等	周知活動に活用するために、一般社団法人日本クレジット協会（以下「日本クレジット協会」という。）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。

用　語	説　明
	「IC 対応」・「暗証番号の認知度向上」　　「IC 対応デザイン」 共通シンボルマーク   ※　「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）。
クレジットマスター	クレジットカード番号等の採番の規則性を悪用し、機械的にクレジットカード番号を生成すること。
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。
接触 IC 取引	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をいう。
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。
非接触 IC 取引	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。 ※　詳細については、「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【附属文書 1】」及び「対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】」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。
リスクベース認証	利用者が決済に使用するデバイスの設定情報や利用者から提供される個人情報等の様々なデータを活用して本人の利用であるかを確認し認証をする仕組み。

［カード情報保護対策の対象事業者の定義］

対象事業者	定義
1号事業者	割賦販売法第35条の16第1項第1号に規定されるクレジットカード等購入あっせん業者であり、具体的にはカード発行会社（イシュアー）を指す。
2号事業者	割賦販売法第35条の16第1項第2号に規定されるクレジットカード等購入あっせん関係販売業者又はクレジットカード等購入あっせん関係役務提供事業者であり、具体的には加盟店を指す。
3号事業者	割賦販売法第35条の16第1項第3号に規定される立替払取次業者であり、具体的にはアクワイアラーを指す。
4号事業者	割賦販売法第35条の16第1項第4号に規定されるアクワイアラー（3号事業者）のために、加盟店（2号事業者）にカード決済の代金相当額を交付（立替払い）する事業者を指す。 対象事業者の例としては、以下の通り。 ○決済代行業者（包括代理加盟事業者） ○EC モール事業者（デジタルプラットフォーマー等） ○SC、百貨店（消化仕入れを除く）、ショッピングモール等 ○商店街組合（包括代理加盟事業者）
5号事業者	割賦販売法第35条の16第1項第5号に規定されるカード情報を別の決済用情報と結び付け、当該決済用情報で後払い決済を提供する事業者であり、具体的にはコード決済事業者等を指す。 対象事業者の例としては、以下の通り。 ○QR コード決済事業者 ○スマートフォン決済事業者 ○ID 決済事業者等
6号事業者	割賦販売法第35条の16第1項第6号に規定されるコード決済事業者等（5号事業者）からの委託により、決済用情報に結びつけたカード情報を特定可能な状態で管理する事業者であり、具体的にはコード決済事業者等のカード情報管理業務受託事業者を指す。
7号事業者	割賦販売法第35条の16第1項第7号及び割賦販売法施行規則第132条の2に規定される事業者であり、具体的には加盟店が決済代行業者又はアクワイアラーにカード会員データを提供するために、クレジットカード決済機能を有するシステム及びそのサービスを提供する事業者を指す。この事業者には、カード会員データの伝送処理保存を行っている事業者、決済代行業者又はアクワイアラーに接続できる決済モジュールを提供している事業者も含まれる。 対象事業者の例としては、以下の通り。 ○EC システム提供会社（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。 ASP/SaaS として EC 事業者にサービス提供する事業者、EC 事業者に購入プラットフォームを提供する事業者）、これらに限らない。

第３章　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、本協議会が策定した以下の附属文書及び本協議会事務局である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いる。

３－１　附属文書一覧

文書名	目的・概要
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【附属文書 1】	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）」のため、具体的な方策例について取りまとめたもの。
対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】	対面取引加盟店における「非保持化（非保持と同等/相当を含む）の実現方法及び具体的な技術要件について取りまとめたもの。
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【附属文書 3】	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取りまとめたもの。
国内ガソリンスタンドにおけるクレジットカード取引対応指針【附属文書 4】	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、当面の対応として、実現可能な代替策を取りまとめたもの。
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【附属文書 5】	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、当面の対応として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【附属文書 6】	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～【附属文書 7】	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～【附属文書 8】	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～【附属文書 9】	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。
ブランドテスト要否一覧【附属文書 10】	「IC カード対応 POS 導入の手引き～認定・試験プロセス概要～」の附属文書であり、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）【附属文書 11】	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）【附属文書 12】	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。
不正利用対策 4 方策の具体的な基準・考え方について【附属文書 13】	加盟店のリスクや被害発生の状況等に応じ、セキュリティガイドラインに掲げる 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・考え方を取りまとめたもの。
EMV 3-D セキュア導入ガイド【附属文書 14】	EMV 3-D セキュアの導入促進を目的として、概要やシステム要件等、各ステークホルダーに必要な情報が分かりやすいように取りまとめたもの。
クレジット取引における本人確認方法に係るガイドライン【附属文書 15】	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、2023 年度より協議会の附属文書として移管されたもの。
クレジットカード売上票の作成・保管に関するガイドライン【附属文書 16】	「サイン」を取得しない加盟店の運用変更が円滑に進むことや運用の統一を目指し、クレジットカード取引における売上票の作成・保管に関しての運用を取りまとめたもの。
スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策等ついて【附属文書 17】	スマートフォンやタブレット等の汎用デバイスを用いた決済及びスマホアプリ等の SDK を利用する決済について、「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取りまとめたもの。
EC 加盟店における非保持化対応ソリューションについて【附属文書 18】	EC 加盟店における「非保持化」の取組を推進するための実現方法等について取りまとめたもの。
属性・行動分析のポリシー文書【附属文書 19】	「属性・行動分析（不正検知システム）」の導入検討及び導入済み加盟店の継続的な運用の見直し、サービス提供事業者と加盟店の間の体制整備等の方針を定めたもの。
EC 加盟店における基本的なセキュリティ対策　導入ガイド【附属文書 20】	EC 加盟店やその他非対面取引加盟店においてセキュリティ意識の向上と講じるべき対策についての理解を深め、情報漏えい及び不正利用対策に資するようセキュリティガイドラインには定めていない対策について解説したもの。 本文書の概要を図表も加えて説明した「セキュリティ・チェックリスト」【附属文書 21】も参照すること。
セキュリティ・チェックリスト【附属文書 21】	EC 加盟店のセキュリティ意識の向上と、基本的なセキュリティ対策の強化、これによるカード会員データの漏えい及び不正利用の防止を目的に、EC 加盟店におけるセキュリティ対策義務及び EC 加盟店における基本的な対策について、図表も用いて具体的に取りまとめたもの。

３－２　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及び漏えい懸念時の対応要領【関係文書 1】	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。

第４章　本ガイドラインの基本的な考え方

４－１　本ガイドラインにおけるセキュリティ対策の対象

本ガイドラインでは、クレジットカード取引の関係事業者ごとに、対面取引と非対面取引別に「カード情報保護」と「不正利用防止」のために講じる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。

なお、対面取引と非対面取引とは以下の定義による。

取引形態	定義
対面取引	会員から提示を受けたカードのカード情報を端末機によりカード情報を読取り、当該カード情報をアクワイアラーに提供する取引
非対面取引	インターネット、電話等の会員からカードの提示を受けない方法によりカード情報の通知を受け、アクワイアラーに提供する取引
EC 加盟店	インターネットによりカード情報の通知を受ける加盟店
メールオーダー・テレフォンオーダー加盟店（MO・TO 加盟店）	電話・FAX・はがき等によりカード情報の通知を受ける加盟店

４－２　割賦販売法との関係性

「割賦販売法（後払分野）に基づく監督の基本方針」において、本ガイドラインに掲げられる措置が割賦販売法で義務付けられているクレジットカード番号等の漏えい等の事故及び不正利用を防止するための措置の実務上の指針として位置付けられている。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適切に講じている場合には、クレジットカード番号等の漏えい等の事故及び不正利用を防止する措置として、割賦販売法に規定する「必要かつ適切な措置」が講じられていると認められるとされており、本ガイドラインにおいては、【指針対策】としてこれらの措置を記載している。

なお、割賦販売法においては、【指針対策】が実務指針となっている漏えい等の事故及び不正利用を防止するための措置のみならず、実施するべき措置が義務付けられていることに留意すること。

４－３　対象となる関係事業者

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（イシューアー・アクワイアラー)」「決済代行業者等（4 号事業者)」「コード決済事業者等（5 号事業者)」「コード決済事業者等の委託会社（6 号事業者)」「加盟店向け決済システム提供事業者（7 号事業者)」及び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」並びに「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。

４－４　対象となるクレジットカード

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が必要である。

４－５　関係事業者間の情報連携等

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じ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。

４－６　消費者への情報提供

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及び周知活動に取組む必要がある。

第５章　各事業者が講じる対策等

５－１　カード会社（イシュアー）

５－１－１　対面取引・非対面取引共通

５－１－１－１　カード情報保護対策

①カード会社（イシュアー）の指針対策（１号事業者）

【指針対策】
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。

a. PCI DSS 準拠

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 の要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、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委託者管理

カード情報を取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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③加盟店におけるカード情報漏えい時の対応

加盟店等からカード情報が漏えいした際は、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及び漏えい懸念時の対応要領【関係文書 1】」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じる。

５－１－２　対面取引

５－１－２－１　不正利用対策

①発行カードの IC 化

発行するカードの全てを IC 化する。

②IC 取引時のオペレーションルール

IC 取引の円滑な運用に資するため、「接触 IC 取引」及び「非接触 IC 取引」の本人確認方法を IC 取引時のオペレーションルールとして、下表のとおり定めている。

ただし、本人確認不要取引を行うにあたっては、カード会員の保護及び不正利用発生の防止に留意しなければならない。

［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」へ切り替える。ただし切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。

・「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）又はサインとする。

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）又はサイン

（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 取引への切替えを許容しないカードが存在するため

また、「クレジットカード利用時の本人確認としての売上伝票へのサイン取得の任意化」及び「PIN バイパス（PIN 入力スキップ機能）の廃止」については、2025 年 3 月までの移行を進める。

なお、詳細は「クレジット取引における本人確認方法に係るガイドライン【附属文書 15】」を、自動精算機については「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【附属文書 5】」を参照すること。

５－１－３　非対面取引

５－１－３－１　不正利用対策

①EMV 3-D セキュア

a.導入及び登録推進等

EMV 3-D セキュアを導入し、継続的に安定稼働のための対応をするとともに、自社カード会員に対して EMV 3-D セキュアの登録を強く推進するための取組を行い、2025 年 3 月末時点で EC 利用会員ベースで 80%の登録率を目指す。また、カード会員の登録の有無にかかわらず、オーソリモニタリングやリスクベース認証を用いた不正利用対策を講じる。

なお、後述の「b.リスクベース認証（RBA）の精度向上」及び「c.動的（ワンタイム）パスワード等への移行及び登録推進」も含めて「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照すること。

b.リスクベース認証（RBA）の精度向上

自社カード会員取引のリスク度合いを適切に判定するために、データ処理能力の向上や認証精度の分析及びルール設定等の最適化を行い、リスクベース認証の精度向上に継続的に取組むことが求められる。

c.動的（ワンタイム）パスワード等への移行及び登録推進

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、不正利用被害の蓋然性が高くなることから、カード会社（イシュアー）は EMV 3-D セキュアのチャレンジフローにおける追加認証方法として、「動的（ワンタイム）パスワード等」の「静的（固定）パスワード」以外の認証方法への移行環境を整え、自社カード会員が「動的（ワンタイム）パスワード等」の「静的（固定）パスワード」以外の認証方法へ登録・移行するよう取組むことが求められる。具体的には、2025 年 3 月末時点で EMV 3-D セキュア登録会員ベースで 100%の移行率を目指し、取組む。

また、自社カード会員における「静的（固定）パスワード」以外の認証方法への登録・移行を促進するためのカード会員への周知・啓発を行う。

②オーソリモニタリング

a.精度向上

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。

b.クレジットマスター対策

不正に入手した大量のカード会員データや採番の規則性を悪用し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決済等を行おうとする手口が依然として発生していることから、このようなクレジットカード決済を早期に検知し、当該クレジットカード番号による取引を停止させる対策を講じることが必要となる。

③カード会員に対するカード利用時の通知の導入及び登録推進

「カード会員に対するカード利用時の通知」とは、カード会員に対してメールやアプリ等により、カード利用時にその利用内容を通知することで、カード会員がカードを利用した事実を確認できるものである。当該通知によりカード会員が利用覚

えのない取引を発見し、カード会社（イシュアー）に連絡することで、不正利用を認知し、より早くカードの無効手配・処理が可能となる。このように有効な不正利用対策であることから、カード会社（イシュアー）は導入及びカード会員への登録を促進することが必要となる。

④真正利用照会対応

非対面取引加盟店からの真正利用確認照会（オフアス取引の場合はアクワイアラー経由の照会）に応じるべく情報連携強化に取組む。

⑤コード決済等連携時の対策

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、なりすまし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や決済利用により、高額な不正利用被害が発生する蓋然性がある。

このため、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 EMV 3-D セキュアによる認証や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等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。

５－１－４　周知・啓発

①発行カードの IC 化

a. PIN

・認知度向上

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、引き続き PIN の認知度向上のための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、PIN の重要性や PIN の確認方法等について、分かりやすく丁寧に説明する。

また、PIN 不知による利用阻害を生じさせないよう、カード会員に速やかに PIN を通知するよう努める。

・サイン取得の任意化及び PIN バイパスの廃止

IC 取引において 2025 年 3 月までに移行を目指すこととされている「サイン取得の任意化」及び「PIN バイパスの廃止」に向けたカード会員への周知・啓発に取組む。

②情報管理リテラシー向上

a. フィッシング対策

カード会員に対して、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の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、具体的な事例等の紹介を交えて注意喚起をするとともに、所持する電子機器のセキュリティ対策の必要性等について周知・啓発する。

b. なりすまし対策

EC 取引における不正利用対策の実効性確保のために、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、ID・パスワードの使い回しの危険性等について、カード会員に対して周知・啓発する。

c. 利用明細確認の励行

カード会員が利用覚えのない取引を発見し、カード会社（イシュアー）に連絡することで、不正利用を認知し、より早くカードの無効手配・処理を行うことにより不正利用被害を防止するために、利用明細を確認することの重要性について周知・啓発する。

５－２　加盟店

５－２－１　対面取引

５－２－１－１　カード情報保護対策

①対面取引加盟店の指針対策（２号事業者）

【指針対策】
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。

a. 非保持化

ⅰ.非保持化の定義

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、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「非保持化」に該当する。

対面取引では、決済端末の IC 対応とともに外回りによる非保持化が進展している。

なお、以下ｱ.～ｳ.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。

ｱ.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）
ｲ.紙媒体をスキャンした画像データ
ｳ.電話での通話記録（音声データを含む）

（注 1）上記ｱ.～ｳ.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ｱ.～ｳ.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 準拠対象になることに留意する必要がある。

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。

なお、具体的な非保持化の実現方法については、「対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】」を参照すること。

また、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 の準拠が必要となることに留意する。

ⅱ.非保持と同等/相当（内回り方式）の要件

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取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。

なお、具体的な非保持と同等/相当の実現方法については、「対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】」を参照すること。

［対面取引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）	ｱ.非保持化	決済専用端末連動型
	ｲ.非保持化	ASP/クラウド接続型
ｳ.非保持と同等/相当 （内回り方式）		PCI P2PE 認定ソリューション又は PCI MPoC 認定ソリューションの導入あるいは本協議会が取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

ⅲ.非保持化を実現した加盟店の留意点

非保持化を実現した加盟店においては、①顧客からの照会への対応と、②過去に取扱ったカード情報の保護対策について留意する。

なお、具体的な対応等は、①顧客からの照会への対応については、「対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】」を、②過去に取扱ったカード情報の保護対策については、「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【附属文書 3】」を参照すること。

b. PCI DSS 準拠

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

要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、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委託者管理

カード情報を取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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③カード情報漏えい時の対応

カード情報が漏えいした際は、速やかに契約するカード会社（アクワイアラー）又は PSP に連絡するとともに、契約するカード会社（アクワイアラー）又は PSP の要請にしたがって、被害の拡大を防止するための初動対応として、漏えい元（データベース又は決済端末等）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。

また、カード決済の再開にあたっては、加盟店は契約するカード会社（アクワイアラー）又は PSP と 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について協議し、SAQ 等の提出や再発防止のための措置等の対応状況を十分に講じた上で、契約するカード会社（アクワイアラー）の判断を求める。

５－２－１－２　不正利用対策

①対面取引加盟店の指針対策

【指針対策】
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。

a. 決済端末機の IC 対応

ⅰ. 決済専用端末（CCT）

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。

ⅱ. POS

IC 対応の実現方法としては、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。

なお、IC 対応の実現方法は、「IC カード対応 POS ガイドライン【附属文書 6】」及び「非接触 EMV 対応 POS ガイドライン【附属文書 12】」を参照すること。

ⅲ.特定業界

・石油元売

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（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【附属文書 5】」を取りまとめており、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。

なお、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クレジットカード取引対応指針【附属文書 4】」に実現可能な方策を取りまとめており、この指針に基づいて IC 対応する。

・オートローディング式自動精算機

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【附属文書 5】」を取りまとめた。この指針では、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、この指針に基づいて対応する。

②IC 取引時のオペレーションルール

IC 取引の円滑な運用に資するため、「接触 IC 取引」及び「非接触 IC 取引」の本人確認方法を IC 取引時のオペレーションルールとして、下表のとおり定めている。

ただし、本人確認不要取引を行うにあたっては、カード会員の保護及び不正利用発生の防止に留意しなければならない。

［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」へ切り替える。ただし切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。

・「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）又はサインとする。

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）又はサイン

（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 取引への切替えを許容しないカードが存在するため

また、「クレジットカード利用時の本人確認としての売上伝票へのサイン取得の任意化」及び「PIN バイパス（PIN 入力スキップ機能）の廃止」については、2025 年 3 月までの移行を進める。

なお、詳細は「クレジット取引における本人確認方法に係るガイドライン【附属文書 15】」を、自動精算機については「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【附属文書 5】」を参照すること。

③情報共有要請

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。

５－２－１－３　周知・啓発

①決済端末機の IC 対応

a. PIN

・認知度向上

PIN 不知のカード利用者に対しては、PIN 確認のためにカード会社（イシュア

ー）への案内に協力する。

・サイン取得の任意化及び PIN バイパスの廃止

対面取引加盟店においては、「５－２－１－２　不正利用対策　②IC 取引時のオペレーションルール」に記述のとおり、「サイン取得の任意化」及び「PIN バイパスの廃止」について、円滑な移行に向けたカード利用者への案内に協力する。

なお、クレジットカード取引の売上票（カード会社控え等）は「サイン」取得の前提で取引時に作成され、保管されている運用が一般的であるが、「サイン」を取得しない加盟店の取引においては紙伝票印刷や保管業務の削減等、運用の合理化を図ることが可能となる。運用検討にあたっては、「クレジットカード売上票の作成・保管に関するガイドライン【附属文書 16】」を参照すること。

５－２－２　非対面取引（EC 加盟店）

５－２－２－１　カード情報保護対策

①EC 加盟店の指針対策（２号事業者）

【指針対策】
カード情報を保持しない非保持化、又はカード情報を保持する場合は PCI DSS に準拠する。

a. 非保持化

ⅰ.非保持化の定義

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。

カード情報に含まれる「機密認証データ」の保持は認められない。

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、以下ｱ.～ｳ.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。

ｱ.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）
ｲ.紙媒体をスキャンした画像データ
ｳ.電話での通話記録（音声データを含む）

（注 1）上記ｱ.～ｳ.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ｱ.～ｳ.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 準拠対象になることに留意する必要がある。

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侵入、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。過去に発生した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。EC 加盟店は、PCI DSS 準拠済みの PSP が提供する非通過型（「リダイレクト（リンク）型」又は「JavaScript 型（トークン型）」）等の決済システムを導入して非保持化を実現する必要がある。

しかし、最近の傾向では、「非通過型」により非保持化を達成した EC 加盟店における漏えい事故が主流となっている。これは、脆弱性対策、ウイルス対策、管理者権限の管理、デバイス管理等の基本的なセキュリティ対策を実施していない EC 加盟店に対して外部からの既知の脆弱性の悪用やウイルスの侵入によりシステムの改ざんが行われ、カード情報が不正に窃取される漏えい事故が頻発しているからである。これらの基本的なセキュリティ対策は、カード情報の保持又は非保持であるかにかかわらず、EC 加盟店が実施すべきものである。

このため、EC 加盟店は、新規加盟店契約申し込み前に、自ら「セキュリティ・チェックリスト【附属文書 21】」記載の対策を実施し、その状況をアクワイアラーや PSP に申告、アクワイアラーや PSP は EC 加盟店からの申告を受けた上で加盟店契約を締結することが求められる。（試行）

上記の EC 加盟店によるセキュリティ対策の実施については、2025 年 4 月から、新規のみならず全ての EC 加盟店に対して求めることとしている。（※）

その他にも、PSP との協働による悪質な有効性確認及びクレジットマスターへの対策、加盟店及び消費者のログイン画面に対するセキュリティ対策等、EC 加盟店が実施すべき対策の検討が必要である。

なお、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 加盟店は、PCI DSS 準拠済みの PSP が提供する非通過型（「リダイレクト（リンク）型」又は「JavaScript 型（トークン型）」）等の決済システムを導入して非保持化を実現することができる。

なお、具体的な非保持化実現方法は、「EC 加盟店における非保持化対応ソリューションについて【附属文書 18】」を参照すること。

また、カード会社や PSP 等から、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 の準拠が必要となることに留意する。

［EC 加盟店における非保持化導入例］

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

（※）「クレジットカード決済システムのセキュリティ対策強化検討会報告書」（2023 年 1 月 20 日）において、EC 加盟店の漏えい対策の強化のための当面の対応として、EC 加盟店のシステム、EC サイト自体の脆弱性対策（システム上の設定の不備への対策（PW 管理等）、脆弱性診断・対策、ウイルス対策等）の基本的なセキュリティ対策を必須とすることを 2024 年度末までに本ガイドラインに追記することが求められている。

ⅱ.非保持化を実現した加盟店の留意点

非保持化を実現した加盟店においては、①顧客からの照会への対応と、②過去に取扱ったカード情報の保護対策について留意する。

なお、具体的な対応等は、①顧客からの照会への対応については、「EC 加盟店における非保持化対応ソリューションについて【附属文書 18】」を、②過去に取扱ったカード情報の保護対策については、「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【附属文書 3】」を参照すること。

b. PCI DSS 準拠

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 の要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、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基本的なセキュリティ対策

非対面取引加盟店のうち EC 加盟店では、EC サイトの脆弱性対策、ウイルス対

策、管理者権限の管理、デバイス管理等の基本的なセキュリティ対策の不備を原因としたカード情報の漏えい事案の発生、大量かつ連続する不正アタックや悪質な有効性確認及びフィッシングによるカード情報や会員のログインアカウントなどの不正窃取も見受けられる。これらの対策はカード情報の保持又は非保持にかかわらず必要なものであることから、EC 加盟店は、新規加盟店契約申し込み前に、自ら「セキュリティ・チェックリスト【附属文書 21】」記載の対策を実施し、その状況をアクワイアラーや PSP に申告、アクワイアラーや PSP は EC 加盟店からの申告を受けた上で加盟店契約を締結することが求められる。(試行)

上記の EC 加盟店によるセキュリティ対策の実施については、2025 年 4 月から、新規のみならず全ての EC 加盟店に対して求めることとしている。(※)

その他、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、不断に自社のセキュリティ対策の改善・強化を図る。

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会員データ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決済等を行おうとする手口が依然として発生している。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決済等を行おうとする場合と比較すると、その速度や連続性の点が明らかに異なることから、EC 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など、加盟店各社サイトにおいても被害の状況に応じて必要な対策を構築することが必要となる。

(※)「クレジットカード決済システムのセキュリティ対策強化検討会報告書」(2023 年 1 月 20 日)において、EC 加盟店の漏えい対策の強化のための当面の対応として、EC 加盟店のシステム、EC サイト自体の脆弱性対策(システム上の設定の不備への対策(PW 管理等)、脆弱性診断・対策、ウイルス対策等)の基本的なセキュリティ対策を必須とすることを 2024 年度末までに本ガイドラインに追記することが求められている。

③委託者管理

カード情報を取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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

④カード情報漏えい時の対応

カード情報が漏えいした際は、速やかに契約するカード会社(アクワイアラー)又は PSP に連絡するとともに、契約するカード会社(アクワイアラー)又は PSP の要請にしたがって、被害の拡大を防止するための初動対応として、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。

また、カード決済の再開にあたっては、契約するカード会社（アクワイアラー）又は PSP と 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について協議し、SAQ 等の提出や再発防止のための措置等の対応状況を十分に講じた上で、契約するカード会社（アクワイアラー）の判断を求める。

５－２－２－２　不正利用対策

①EC 加盟店の指針対策

【指針対策】
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。
上記に加え、後述する「高リスク商材取扱加盟店」は、本ガイドラインが掲げる 4 つの方策のうち 1 方策以上、「不正顕在化加盟店」は 2 方策以上の導入が必要となる。

a. 方策導入の考え方

EC 加盟店は、リスクや被害発生の状況に関わらず、不正利用防止のための方策として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。加えて、EC 加盟店の取扱う商材や不正利用の被害発生状況等のリスクに応じて、後述の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。

また、商材としては、換金性があり転売されやすい商品が不正利用の標的となることから、このような商材を取扱う EC 加盟店においては、カード会社（アクワイアラー）や PSP と協力し、商材に合わせた適切な不正利用対策を講じることが必要となる。

b. 4 方策

指針対策に記載の非対面不正利用対策の 4 つの方策は、以下のとおり。

方策		特徴
ｱ.本人認証	a）EMV 3-D セキュア	・カード会員のデバイス情報等を用いて不正利用のリスク判断を行うとともに、必要に応じてパスワード入力を要求することで当該取引における安全性を確保する
	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
ｲ.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 ・EC 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 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

ｳ.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 ・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 ・EC 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、条件設定による自動判定が行われることが重要で、さらに、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 ・「属性・行動分析（不正検知システム）」の導入検討及び導入済み加盟店の継続的な運用の見直しについては、サービス提供事業者と加盟店の間の体制整備等の方針を定めた「属性・行動分析のポリシー文書【附属文書 19】」を参照すること
ｴ.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 ・多数の取引と一定以上の不正利用被害がある EC 加盟店においては自社構築によるデータベースでも一定の効果があるがそれ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

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、EC 加盟店が取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必要である。特に、不正利用が多発している EC 加盟店においては、多面的・重層的な対策を講じる必要がある。

なお、EC 加盟店における不正利用対策の具体的方策については、「不正利用対策 4 方策の具体的な基準・考え方について【附属文書 13】」を参照すること。

さらに、以下のⅰ.ⅱ.の EC 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。加えて、リスト型攻撃（システムを利用し短時間に大量の決済等を行うこと）による不正利用が引続き発生していることから、不正利用が継続的には発生していない EC 加盟店であっても、カード会社（アクワイアラー）や PSP 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。

ⅰ.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扱う EC 加盟店は、「高リスク商材取扱加盟店」として、本ガイドラインにおいて掲げる非対面不正利用対策の 4 つの

方策のうち、1 方策以上を導入する必要がある。なお、ここでいう③電子マネーとは、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。

ⅱ.不正顕在化加盟店

カード会社（アクワイアラー）や PSP が、不正利用被害が多発している状況にあると認識する EC 加盟店を「不正顕在化加盟店」としている。「不正顕在化加盟店」は、本ガイドラインにおいて掲げる非対面不正利用対策の 4 つの方策のうち、2 方策以上を導入する必要がある。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 EC 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 EC 加盟店は、カード会社（アクワイアラー）や PSP から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実効的な方策を追加で導入する必要がある。

なお、ⅰ.ⅱ.に該当する EC 加盟店であっても、4 つの方策と同等以上の性能を満たしている方策であれば、4 つの方策以外の導入も認められるものとする。ただし、その方策が 4 つの方策と同等以上の性能であることの説明が求められる可能性がある点に留意する必要がある。

［非対面取引加盟店が導入する不正利用対策］

<table>
<tr><th>全ての非対面取引加盟店</th></tr>
<tr><td>◎カード取引に対する善管注意義務の履行
◎オーソリゼーション処理
○EMV 3-D セキュア導入計画の策定及び早期の導入着手
<table><tr><th>ⅰ.高リスク商材取扱加盟店</th></tr><tr><td>◎本ガイドラインに掲げる非対面不正利用対策の 4 方策のうち、
1 方策以上
○EMV 3-D セキュア導入計画の策定及び早期の導入着手</td></tr><tr><th>ⅱ.不正顕在化加盟店</th></tr><tr><td>◎本ガイドラインに掲げる非対面不正利用対策の 4 方策のうち、
2 方策以上
○EMV 3-D セキュア即時導入着手</td></tr></table></td></tr>
</table>

◎印は「指針対策」

なお、EMV 3-D セキュアの導入における詳細については、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照すること。

②EMV 3-D セキュア

a. 計画的導入

2025 年 3 月末までに、原則、全ての EC 加盟店に EMV 3-D セキュアの導入が求められることから、EMV 3-D セキュアの導入計画を策定し早期に EMV 3-D セキュアの導入に着手することが求められる。

また、「不正顕在化加盟店」は既に不正利用が発生し被害が生じている加盟店であることから、即時に EMV 3-D セキュアの導入に着手することが求められる。

b. リスクベース認証の精度向上のための対応

カード会社（イシュアー）におけるリスクベース認証の精度向上のため、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照し、カード会社（アクワイアラー）や PSP 等と連携しながら、自社の取扱商材や不正発生状況等の実態を踏まえ、カード会員のデバイス情報等の情報をカード会社（イシュアー）により多く提供できるよう、また提供する情報を適宜見直せるよう、データ項目の設定等の体制を整えることが求められる。加えて、前述の「高リスク商材取扱加盟店」や「不正顕在化加盟店」等において更なる不正利用対策強化が必要な場合には、カード会社（アクワイアラー）や PSP の要請に応じ、カード会社（イシュアー）の認証精度向上に資するデータ項目の設定を行うことが求められる。

③情報共有

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。

また、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）や不正利用対策に有効な情報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。

５－２－２－３　周知・啓発

①情報管理リテラシー向上

a. フィッシング対策

消費者がフィッシング詐欺に遭わないように、フィッシングの手口や自社の名を騙る詐欺サイト等に対する注意喚起を行う。

b. なりすまし対策

EC 取引においては、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、ID・パスワードの使い回しの危険性等について、注意喚起を行う。

５－２－３　非対面取引（MO・TO 加盟店）

５－２－３－１　　カード情報保護対策

①MO・TO 加盟店の指針対策（２号事業者）

【指針対策】
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。

a. 非保持化

ⅰ.非保持化の定義

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。

カード情報に含まれる「機密認証データ」の保持は認められない。

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、以下ｱ.～ｳ.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。

ｱ.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）

ｲ.紙媒体をスキャンした画像データ

ｳ.電話での通話記録（音声データを含む）

（注 1）上記ｱ.～ｳ.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ｱ.～ｳ.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準拠対象になることに留意する必要がある。

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。

なお、具体的な実現方法は、「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【附属文書1】」を参照すること。

また、カード会社等から、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の準拠が必要となることに留意する。

ⅱ.非保持と同等/相当（内回り方式）の要件

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。

なお、具体的な実現方法は、「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【附属文書1】」を参照すること。

［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）	ｱ.非保持化	決済専用端末を利用した外回り方式
	ｲ.非保持化	タブレット端末（※）を利用した外回り方式
ｳ.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

ⅲ.非保持化を実現した加盟店の留意点

非保持化を実現した加盟店においては、①顧客からの照会への対応と、②過去に取扱ったカード情報の保護対策について留意する。

なお、具体的な対応等は、①顧客からの照会への対応については、「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【附属文書１】」を、②過去に取扱ったカード情報の保護対策については、「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【附属文書 3】」を参照すること。

b. PCI DSS 準拠

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 の要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、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委託者管理

カード情報を取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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③カード情報漏えい時の対応

カード情報が漏えいした際は、速やかに契約するカード会社（アクワイアラー）又は PSP に連絡するとともに、契約するカード会社（アクワイアラー）又は PSP

の要請にしたがって、被害の拡大を防止するための初動対応として、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。

カード決済の再開にあたっては、契約するカード会社（アクワイアラー）又はPSP と 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について協議し、SAQ 等の提出や再発防止のための措置等の対応状況を十分に講じた上で、契約するカード会社（アクワイアラー）の判断を求める。

５－２－３－２　不正利用対策

①MO・TO 加盟店の指針対策

【指針対策】
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。
上記に加え、後述する「高リスク商材取扱加盟店」は、本ガイドラインが掲げる 4 つの方策のうち 1 方策以上、「不正顕在化加盟店」は 2 方策以上の導入が必要となる。

a. 方策導入の考え方

非対面取引加盟店は、リスクや被害発生の状況に関わらず、不正利用防止のための方策として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。加えて、非対面取引加盟店の取扱う商材や不正利用の被害発生状況等のリスクに応じて、後述の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。

また、商材としては、換金性があり転売されやすい商品が不正利用の標的となることから、このような商材を取扱う非対面取引加盟店においては、カード会社（アクワイアラー）や PSP と協力し、商材に合わせた適切な不正利用対策を講じることが必要となる。

b. 4 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はそれぞれ特徴があり、非対面取引加盟店が取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必要である。特に、不正利用が多発している非対面取引加盟店においては、多面的・重層的な対策を講じる必要がある。

なお、非対面取引加盟店における不正利用対策の具体的方策については、「不正利用対策 4 方策の具体的な基準・考え方について【附属文書 13】」を参照すること。

また、以下のⅰ.ⅱ.の非対面取引加盟店は、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。加えて、不正利用が継続的には発生していない非対面取引加盟店であっても、カード会社（アクワイアラー）や

PSP 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。

ⅰ.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扱う非対面取引加盟店は、「高リスク商材取扱加盟店」として、本ガイドラインにおいて掲げる非対面不正利用対策の 4 つの方策のうち、1 方策以上を導入する必要がある。なお、ここでいう③電子マネーとは、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。

ⅱ.不正顕在化加盟店

カード会社（アクワイアラー）や PSP が、不正利用被害が多発している状況にあると認識する非対面取引加盟店を「不正顕在化加盟店」としている。「不正顕在化加盟店」は、本ガイドラインにおいて掲げる非対面不正利用対策の 4 つの方策のうち、2 方策以上を導入する必要がある。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」に該当する非対面取引加盟店とする。

なお、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」と認識される非対面取引加盟店は、カード会社（アクワイアラー）や PSP から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実効的な方策を追加で導入する必要がある。

なお、ⅰ.ⅱ.に該当する非対面取引加盟店であっても、4 つの方策と同等以上の性能を満たしている方策であれば、4 つの方策以外の導入も認められるものとする。ただし、その方策が 4 つの方策と同等以上の性能であることの説明が求められる可能性がある点に留意する必要がある。

②情報共有

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。

また、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）や不正利用対策に有効な情報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。

５－２－４　加盟店のカード情報保護対策及び不正利用対策の概要

①カード情報保護対策

形態		【指針対策】			
		非保持化			PCI DSS 準拠
		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 （非保持と同等/相当）	
対面取引加盟店		決済専用端末利用型	ASP/クラウド接続型	PCI P2PE 認定ソリューション PCI MPoC ソリューション 協議会が取りまとめたセキュリティ要件	○
非対面取引加盟店	EC 加盟店	リダイレクト型（リンク）型	JavaScript（トークン）型		○
	MO・TO 加盟店	決済専用端末利用型	タブレット端末利用型	PCI P2PE 認定ソリューション	○

（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、対面取引加盟店と非対面取引加盟店双方の対策が必要となる。

（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、どの対策を採るかは各事業者の選択に委ねられる。

[「①カード情報保護対策」の概要]

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（対面取引加盟店、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

②対面取引加盟店における不正利用対策

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 ｱ. 決済専用端末（CCT）連動型 ｲ. 決済サーバー接続型 ｳ. 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	ｱ.「国内ガソリンスタンドにおける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【附属文書 4】 ｲ.「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【附属文書 5】

③非対面取引加盟店における不正利用対策

全ての非対面取引加盟店

◎カード取引に対する善管注意義務の履行
◎オーソリゼーション処理
○EMV 3-D セキュア導入計画の策定及び早期の導入着手

ⅰ.高リスク商材取扱加盟店
◎本ガイドラインに掲げる非対面不正利用対策の 4 方策のうち、1 方策以上 ○EMV 3-D セキュア導入計画の策定及び早期の導入着手
ⅱ.不正顕在化加盟店
◎本ガイドラインに掲げる非対面不正利用対策の 4 方策のうち、2 方策以上 ○EMV 3-D セキュア即時導入着手

◎印は「指針対策」

なお、EMV 3-D セキュアの導入における詳細については、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照すること。

［非対面不正利用対策の 4 方策］

方策		特徴
ｱ.本人認証	**a）EMV 3-D セキュア**	・カード会員のデバイス情報等を用いて不正利用のリスク判断を行うとともに、必要に応じてパスワード入力を要求することで当該取引における安全性を確保する
	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

ｲ.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 ・EC 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 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
ｳ.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 ・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 ・EC 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、条件設定による自動判定が行われることが重要で、さらに、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 ・「属性・行動分析（不正検知システム）」の導入検討及び導入済み加盟店の継続的な運用の見直しについては、サービス提供事業者と加盟店の間の体制整備等の方針を定めた「属性・行動分析のポリシー文書【附属文書 19】」を参照すること
ｴ.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 ・多数の取引と一定以上の不正利用被害がある EC 加盟店においては自社構築によるデータベースでも一定の効果があるがそれ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

５－３　カード会社（アクワイアラー）

５－３－１　対面取引・非対面取引共通

５－３－１－１　カード情報保護対策

①カード会社（アクワイアラー）の指針対策（３号事業者）

【指針対策】
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。

a. PCI DSS 準拠

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 の要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、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委託者管理

カード情報を取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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③加盟店におけるカード情報漏えい時の対応

加盟店等からカード情報が漏えいした際は、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及び漏えい懸念時の対応要領【関係文書 1】」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じる。

また、漏えい事案が発生した加盟店等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、当該加盟店等と契約カード会社（アクワイアラー）等で協議の上、決定する。

５－３－２　対面取引

５－３－２－１　カード情報保護対策

①加盟店サポート

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 準拠及びその他セキュリティ対策について必要な助言や情報提供等を行う。

５－３－２－２　不正利用対策

①決済端末機の IC 対応

契約を有する加盟店の決済専用端末の IC 対応を行う。

②加盟店サポート

a. ガイドラインの周知及びベンダーとの連携

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。

また、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【附属文書 6】」及び「非接触 EMV 対応 POS ガイドライン【附属文書 12】」について、機器メーカーや加盟店等への周知を行う。

b. IC 取引時のオペレーションルール

IC 取引の円滑な運用に資するため、「接触 IC 取引」及び「非接触 IC 取引」の本人確認方法を IC 取引時のオペレーションルールとして、下表のとおり定めている。

このため、「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、加盟店に対してガイドライン等について周知を行う。

ただし、本人確認不要取引を行うにあたっては、カード会員の保護及び不正利用発生の防止に留意しなければならない。

なお、詳細は「クレジット取引における本人確認方法に係るガイドライン【附属文書 15】」を、自動精算機については「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【附属文書 5】」を参照すること。

[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」へ切り替える。ただし切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。

・「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）又はサインとする。

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） 又はサイン

（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 取引への切替えを許容しないカードが存在するため

５－３－２－３　周知・啓発

①決済端末機の IC 対応

a. PIN

・認知度向上

加盟店と調整の上、必要に応じて加盟店契約内容の改定やカード利用者の PIN 認知度向上のための周知・啓発への協力を依頼する。

・サイン取得の任意化及び PIN バイパスの廃止

IC 取引において 2025 年 3 月までに移行を目指すこととされている「サイン取得の任意化」及び「PIN バイパスの廃止」を実現させることを目的に、加盟店に対し本件を周知することとする。なお、「サイン取得の任意化」及び「PIN バイパスの廃止」の詳細は「クレジット取引における本人確認方法に係るガイドライン【附属文書 15】」を参照すること。

また、「サイン取得の任意化」及び「PIN バイパスの廃止」について、加盟店の売り場へ周知するとともに、加盟店の個別事情を考慮した上で、モバイル端末の導入の検討や売り場オペレーション変更の検討等の必要な対応を依頼する。

なお、クレジットカード取引の売上票（カード会社控え等）は「サイン」取得の前提で取引時に作成され、保管されている運用が一般的であるが、「サイン」を取得しない加盟店の取引においては紙伝票印刷や保管業務の削減等、運用の合理化を図ることが可能となる。運用検討にあたっては、「クレジットカード売上票の作成・保管に関するガイドライン【附属文書 16】」を参照すること。

５－３－３　非対面取引

５－３－３－１　カード情報保護対策

①基本的なセキュリティ対策

a.「セキュリティ・チェックリスト」による確認

EC 加盟店は、新規加盟店契約申し込み前に、自ら「セキュリティ・チェックリスト【附属文書 21】」記載の対策を実施し、その状況をアクワイアラーや PSP に申告、アクワイアラーや PSP は EC 加盟店からの申告を受けた上で加盟店契約を締結することが求められる。（試行）

上記の EC 加盟店によるセキュリティ対策の実施については、2025 年 4 月から、新規のみならず全ての EC 加盟店に対して求めることとしている。（※）

よって、「セキュリティ・チェックリスト」に記載されているセキュリティ対策を実施する必要性の周知も合わせて行う。

（※）「クレジットカード決済システムのセキュリティ対策強化検討会報告書」（2023 年 1 月 20 日）において、EC 加盟店の漏えい対策の強化のための当面の対応として、EC 加盟店のシステム、EC サイト自体の脆弱性対策（システム上の設定の不備への対策（PW 管理等）、脆弱性診断・対策、ウイルス対策等）の基本的なセキュリティ対策を必須とすることを 2024 年度末までに本ガイドラインに追記することが求められている。

②加盟店サポート

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、その他のセキュリティ対策等の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行う。

５－３－３－２　不正利用対策

①加盟店サポート

a. EMV 3-Dセキュア

・計画的導入

「EMV 3-Dセキュア導入ガイド【附属文書14】」を活用し、2025年3月末までに、原則、全てのEC加盟店がEMV 3-Dセキュアを導入するよう働きかけを行う。その際、不正利用被害額の早期削減を実現するため、「不正顕在化加盟店」の即時の導入着手等「加盟店における EMV 3-D セキュアの導入推進ロードマップ」（2023年11月30日）に従って導入計画の策定及び導入を行うよう働きかけを行う。

また、EC加盟店と新規に加盟店契約する際は、2025年3月末までにEMV 3-Dセキュアを導入することを説明した上で契約する。

・AReq設定項目の充実

カード会社（イシュアー）におけるリスクベース認証の精度向上のため、「EMV 3-Dセキュア導入ガイド【附属文書14】」を参照し、EC加盟店の取扱商材や不正利用発生状況等の実態を踏まえ、EC 加盟店がカード会員のデバイス情報等の情報をカード会社（イシュアー）により多く提供できるよう、提供する情報を適宜見直すなど、EC加盟店におけるデータ項目の設定をサポートする。

・システムの安定稼働

EMV 3-Dセキュアの安定稼働のための対応に継続的に取組む。

b. 情報提供

・方策導入基準

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、非対面取引加盟店が取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必要である。特に、不正利用が多発している非対面取引加盟店においては、多面的・重層的な対策を講じる必要がある。

このため、非対面取引加盟店に対して、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・協力を行うための体制の整備をするとともに、非対面取引加盟店がリスク・被害発生状況に応じた方策を確実に導入するための指導及び状況に応じた適切な提案を行う。

なお、非対面取引加盟店における不正利用対策の具体的方策については、「不正利用対策4方策の具体的な基準・考え方について【附属文書13】」を参照すること。

また、この4方策のうち「属性・行動分析（不正検知システム）」の情報提供については、サービス提供事業者と加盟店の間の継続的な運用の見直し及び体制整備等の方針を定めた「属性・行動分析のポリシー文書【附属文書19】」を参照すること。

・事例紹介及び情報共有

非対面取引加盟店に対し、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。

また、非対面取引加盟店が自社での不正利用対策として属性・行動分析（不正検知システム）を有効に活用するためには、多くの不正取引の情報が必要であり、さらに不審なカード利用の把握や不正利用の手口等の情報を最新化するためにも、カード会社（イシュアー）で発生した不正取引の情報についても把握し、できるだけ多くの非対面取引加盟店と迅速な情報共有に努め、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。

・真正利用照会対応

非対面取引加盟店からの真正利用確認照会への対応に取組む。

②コード決済ガイドライン等の準拠の確認

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、当該事業者は一般社団法人キャッシュレス推進協議会が取りまとめた「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取りまとめた「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。

５－４　決済代行業者等・PSP

５－４－１　対面取引

５－４－１－１　カード情報保護対策

①決済代行業者等の指針対策（４号事業者）

【指針対策】
PCI DSS に準拠し、維持・運用する。
ただし、対面取引を取扱う事業者であって、カード会員データを自社で保有せず、保存・処理・通過を自社以外の業者で行っており、立替払いのみを行っている事業者については当協議会が定める資料「セキュリティ対策チェック項目」に基づき対策を実施し、これを維持・運用する方策も認められる。

a. PCI DSS 準拠

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 の要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加して

いる団体である、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委託者管理

カード情報を取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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③加盟店サポート

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）と契約を有する場合は、カード会社（アクワイアラー）と連携して対応する。

④加盟店におけるカード情報漏えい時の対応

加盟店等からカード情報が漏えいした際は、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及び漏えい懸念時の対応要領【関係文書 1】」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じる。

また、カード情報が漏えいした際は、速やかに契約するカード会社（アクワイアラー）に連絡するとともに、契約するカード会社（アクワイアラー）の要請にしたがって、被害の拡大を防止するための初動対応として、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。

なお、漏えい事案が発生した加盟店等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、当該加盟店等と契約するカード会社（アクワイアラー）等で協議の上、決定する。

５－４－１－２　不正利用対策

①決済端末機の IC 対応

契約を有する加盟店の決済専用端末の IC 対応を行う。

５－４－１－３　周知・啓発

①決済端末機の IC 対応

a. PIN

・認知度向上

加盟店と調整の上、必要に応じて加盟店契約内容の改定やカード利用者の PIN

認知度向上のための周知・啓発への協力を依頼する。

・サイン取得の任意化及び PIN バイパスの廃止

IC 取引において 2025 年 3 月までに移行を目指すこととされている「サイン取得の任意化」及び「PIN バイパスの廃止」を実現させることを目的に、加盟店や加盟店の売り場に対し本件を周知するとともに、加盟店の個別事情を考慮した上で、モバイル端末の導入の検討や売り場オペレーション変更の検討等の必要な対応を依頼する。なお、「サイン取得の任意化」及び「PIN バイパスの廃止」の詳細は「クレジット取引における本人確認方法に係るガイドライン【附属文書 15】」を参照すること。

５－４－２　非対面取引

５－４－２－１　カード情報保護対策

①決済代行業者等の指針対策（４号事業者）

【指針対策】 PCI DSS に準拠し、維持・運用する。

a. PCI DSS 準拠

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 の要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、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委託者管理

カード情報を取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扱う業務を受託する事業者及び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、カード情報が漏えいした場合の影響が大きく、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③基本的なセキュリティ対策

a.「セキュリティ・チェックリスト」による確認

EC 加盟店は、新規加盟店契約申し込み前に、自ら「セキュリティ・チェック

リスト【附属文書 21】」記載の対策を実施し、その状況をアクワイアラーや PSP に申告、アクワイアラーや PSP は EC 加盟店からの申告を受けた上で加盟店契約を締結することが求められる。（試行）

上記の EC 加盟店によるセキュリティ対策の実施については、2025 年 4 月から、新規のみならず全ての EC 加盟店に対して求めることとしている。（※）

よって、「セキュリティ・チェックリスト」に記載されているセキュリティ対策を実施する必要性の周知も合わせて行う。

（※）「クレジットカード決済システムのセキュリティ対策強化検討会報告書」（2023 年 1 月 20 日）において、EC 加盟店の漏えい対策の強化のための当面の対応として、EC 加盟店のシステム、EC サイト自体の脆弱性対策（システム上の設定の不備への対策（PW 管理等）、脆弱性診断・対策、ウイルス対策等）の基本的なセキュリティ対策を必須とすることを 2024 年度末までに本ガイドラインに追記することが求められている。

④加盟店サポート

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）と契約を有する場合は、カード会社（アクワイアラー）と連携して対応する。

⑤加盟店におけるカード情報漏えい時の対応

加盟店等からカード情報が漏えいした際は、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及び漏えい懸念時の対応要領【関係文書 1】」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じる。

また、カード情報が漏えいした際は、速やかに契約するカード会社（アクワイアラー）に連絡するとともに、契約するカード会社（アクワイアラー）の要請にしたがって、被害の拡大を防止するための初動対応として、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。

なお、漏えい事案が発生した加盟店等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、当該加盟店等と契約するカード会社（アクワイアラー）等で協議の上、決定する。

５－４－２－２　不正利用対策

①加盟店サポート

a. EMV 3-D セキュア

・計画的導入

「EMV 3-D セキュア導入ガイド【附属文書 14】」を活用し、2025 年 3 月末までに、原則、全ての EC 加盟店が EMV 3-D セキュアを導入するよう働きかけを行う。その際、不正利用被害額の早期削減を実現するため、「不正顕在化加盟店」の即時の導入着手等「加盟店における EMV 3-D セキュアの導入推進ロードマッ

プ」（2023 年 11 月 30 日）に従って導入計画の策定及び導入を行うよう働きかけを行う。

また、EC 加盟店と新規に加盟店契約する際は、2025 年 3 月末までに EMV 3-D セキュアを導入することを説明した上で契約する。

・AReq 設定項目の充実

カード会社（イシュアー）におけるリスクベース認証の精度向上のため、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照し、EC 加盟店の取扱商材や不正利用発生状況等の実態を踏まえ、EC 加盟店がカード会員のデバイス情報等の情報をカード会社（イシュアー）により多く提供できるよう、提供する情報を適宜見直すなど、EC 加盟店におけるデータ項目の設定をサポートする。

・システムの安定稼働

EMV 3-D セキュアの安定稼働のための対応に継続的に取組む。

b. 情報提供

・方策導入基準

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、非対面取引加盟店が取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必要である。特に、不正利用が多発している非対面取引加盟店においては、多面的・重層的な対策を講じる必要がある。

このため、非対面取引加盟店に対して、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・協力を行うための体制の整備をするとともに、非対面取引加盟店がリスク・被害発生状況に応じた方策を確実に導入するための指導及び状況に応じた適切な提案を行う。

なお、非対面取引加盟店における不正利用対策の具体的方策については、「不正利用対策 4 方策の具体的な基準・考え方について【附属文書 13】」を参照すること。

また、この 4 方策のうち「属性・行動分析（不正検知システム）」の情報提供については、サービス提供事業者と加盟店の間の継続的な運用の見直し及び体制整備等の方針を定めた「属性・行動分析のポリシー文書【附属文書 19】」を参照すること。

・事例紹介及び情報共有

非対面取引加盟店に対し、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。

また、非対面取引加盟店が自社での不正利用対策として属性・行動分析（不正検知システム）を有効に活用するためには、多くの不正取引の情報が必要であり、さらに不審なカード利用の把握や不正利用の手口等の情報を最新化するためにも、カード会社（イシュアー）で発生した不正取引の情報についても把握し、できるだけ多くの非対面取引加盟店と迅速な情報共有に努め、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。

・真正利用照会対応

非対面取引加盟店からの真正利用確認照会への対応に取組む。

c.4 方策提供のための体制整備

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、契約先の非対面取引加盟店における導入の推進に努める。

なお、非対面取引加盟店における不正利用対策の具体的方策については、「不正利用対策 4 方策の具体的な基準・考え方について【附属文書 13】」を参照すること。

５－５　コード決済事業者等

５－５－１　対面取引・非対面取引共通

５－５－１－１　カード情報保護対策

①コード決済事業者等の指針対策（５号事業者）

【指針対策】
PCI DSS に準拠し、これを維持・運用する。

a.PCI DSS 準拠

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 の要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、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コード決済ガイドライン等の遵守

カード会社（アクワイアラー）には、以下の対策が求められていることに留意する。

「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、当該事業者は一般社団法人キャッシュレス推進協議会が取りまとめた『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取りまとめた『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。」

③委託者管理

カード情報を取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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

５－６　コード決済事業者等の委託先及び EC システム提供会社等

５－６－１　対面取引・非対面取引共通

５－６－１－１　カード情報保護対策

①コード決済事業者等の委託先及び EC システム提供会社等の指針対策（６号事業者及び７号事業者）

【指針対策】 PCI DSS に準拠し、これを維持・運用する。

a. PCI DSS 準拠

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 の要件から構成されているが、各事業者の業態、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、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0 基準書およびサポート文書」（「Ver4.0」の概要）や移行スケジュールは、PCI SSC（PCI Security Standards Council）のホームページ（https://www.pcisecuritystandards.org/lang/ja-ja/）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、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委託者管理

カード情報を取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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③加盟店サポート（EC システム提供会社等のみ）

加盟店の取組を支援するため、本ガイドラインに基づき、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。

５－７　その他の関係事業者等の具体的な対策

５－７－１　国際ブランド

①各事業者サポート

以下のサポートを行う。

・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。
・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。
・我が国における非対面取引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。
・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最新の情報提供に努め、我が国における国際水準のセキュリティ環境の整備について、関係事業者に対し積極的に働きかける。

②周知・啓発

以下の周知・啓発を行う。

・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・発信に取組むとともに、海外におけるカード情報保護に関する最新の情報提供に努める。
・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 セキュアの導入について、情報提供及び説明を行うとともに EMV 3-D セキュアの安定稼働のための対応に継続的に取組む。
・非対面取引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 EC 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等について、事業者向けの情報発信に取組む。

５－７－２　ソリューションベンダー

①各事業者サポート

以下のサポートを行う。

・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。

５－７－３　機器メーカー

①各事業者サポート

以下のサポートを行う。

・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。

・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【附属文書 6】」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）【附属文書 11・12】」が取りまとめられていることから、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。

②周知・啓発

以下の周知・啓発を行う。

・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。

５－７－４　行政

①各事業者サポート

以下のサポートを行う。

・関係事業者のセキュリティ対策の実施状況、カード情報の漏えい及び不正利用の被害状況等を把握するとともに、本協議会におけるセキュリティ対策の検討に必要な情報提供、助言を行う。

・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、対面取引加盟店における偽造カードによる不正利用防止、非対面取引加盟店における非対面不正利用防止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。

②周知・啓発

以下の周知・啓発を行う。

・本ガイドラインに掲げるカード情報保護対策及び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。

・消費者に対し EMV 3-D セキュア利用の必要性、静的（固定）パスワード以外の認証方法による安全性の確保等についての周知・啓発に取組む。また、フィッシング対策として、カード会社等がカード情報等の入力を求めるメールや SMS を送ることはないこと、不審なメールや SMS のリンク先にカード情報等を送信しないこと、不正利用被害の自衛として利用履歴や利用明細を確認することなどについて周知・啓発を行う。

５－７－５　業界団体

①各事業者サポート

以下のサポートを行う。

・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、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。

・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、「重要インフラのサイバーセキュリティに係る行動計画」（2022 年 6 月 17 日付策定）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。

・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 EC 加盟店の不正利用の発生状況の分析・評価、加盟店が取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。

②周知・啓発

以下の周知・啓発を行う。

・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及び不正利用対策の必要性、各方策の有効性等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、消費者団体及び関係団体（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。

・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、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宜情報発信を行う。

・消費者であるカード会員が利用覚えのない取引を発見し、カード会社（イシュアー）に連絡することで、不正利用を認知し、より早くカードの無効手配・処理を行うことにより不正利用被害を防止するために、利用明細を確認することの重要性について周知・啓発に取組む。

・カード会社（イシュアー）と連携し、2025 年 3 月までに移行を目指すこととされている対面取引における「サイン取得の任意化」及び「PIN バイパスの廃止」に向けた周知・啓発に取組む。

・引き続き 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・啓発に取組む。

・カード会社（イシュアー）や行政等と連携し、消費者であるカード会員に対し EMV 3-D セキュアの登録及び静的（固定）パスワード以外の認証方法への登録・移行を促進するための周知・啓発に取組む。

・カード会社（イシュアー）や行政、フィッシング対策協議会等の関係団体等と連携し、消費者であるカード会員がフィッシングによる不正利用被害に遭わないために、フィッシングの手口や不審と思われるサイトにはカード情報等の入力は行わないなどの注意事項等について周知・啓発に取組む。

・引き続きカード会社（イシュアー）と連携し、ID・パスワードの使い回しの危険性等について周知・啓発に取組む。

第６章　2025 年 4 月以降の EC 加盟店の情報保護対策及び不正利用対策

６－１　カード情報保護対策

クレジットカード取引に関わる全てのステークホルダーは、本ガイドラインに基づき、各々に求められるカード情報保護対策を講じている。

EC 加盟店においては、2018 年 6 月の割賦販売法改正により、カード情報保護対策が義務化され、PCI DSS 準拠、若しくは非保持化（同等/相当を含む）を実現した。

しかしながら、カード情報窃取の手口の変化、巧妙化もあり、一層のカード情報保護対策の強化が喫緊の課題となっている。

このような状況を踏まえ、現在、EC 加盟店に対して、新規の加盟店契約に際し、EC 加盟店自らカード情報保護対策を実施した上で、その実施状況をアクワイアラーに申告することを求めるとともに、申告内容を基に EC 加盟店のカード情報保護対策の実施状況をアクワイアラーが確認することを試行している。

今後は、この取組の対象を拡大することが求められる。

６－２　不正利用対策

本ガイドラインでは、不正利用被害防止のため 2025 年 3 月末までに、原則、全ての EC 加盟店に EMV 3-D セキュアの導入を求めることに加えて、カード会社（イシュアー）は「静的（固定）パスワード」から「動的（ワンタイム）パスワード等」への移行に取組んでいる。

導入や移行の浸透により不正利用被害の抑制が期待できるが、昨今の巧妙化するフィッシング等の不正手口の増加により、EMV 3-D セキュアだけで全ての被害を防止できるわけではない。

さらに、これまでの不正利用対策は 4 つの方策をベースとした複数の対策を導入することを指針としてきたが、加盟店の業種や業態、取扱商品、不正利用の実態等により、効果的な不正利用対策が異なっており、複数の方策を導入したとしても実効的な抑止効果が得られにくいケースも散見された。

ついては、カード決済の場面（決済前・決済時・決済後）を考慮して、それぞれの場面ごとに対策を導入するという、点ではなく線として考える指針の策定が求められる。

加盟店による EMV 3-D セキュア導入のみではなく、クレジットカード決済の関係事業者それぞれが実施すべき、これから目指すべき不正利用対策の全体像は以下のとおり。

［今後の不正利用対策の考え方（線の考え方）］

EMV 3-D セキュアを不正利用対策の軸とし、クレジットマスターやフィッシング被害を抑止する「カード決済前」の対策や商品の配送が伴う場合の「カード決済後」の対策も加え、不正利用対策をより実効的なものとするため、今後、詳細運用を検討する。

第７章　その他関係事項

７－１　消費者及び事業者等への周知・啓発

クレジットカード取引のセキュリティ対策に関する消費者及び事業者への周知・啓発については、カード会社（イシュアー・アクワイアラー）、PSP、加盟店、国際ブランド、業界団体等の各関係事業者は、それぞれの立場で様々な機会を捉えて積極的かつ継続的に行うことが必要である。

７－１－１　消費者への周知・啓発

消費者への周知・啓発では、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が、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ものとなることから、消費者におけるクレジットカード取引におけるセキュリティ対策への理解と協力が得られるよう取組むことが重要である。

今後は、これまで取組んできた消費者への周知・啓発に加え、新たな決済ルールや仕組みに応じた取引ルールの見直しと、それにともなう消費者への周知・啓発といった円滑な移行への取組も重要である。特に、2025年3月末までに、原則、全てのEC加盟店にEMV 3-Dセキュアの導入を求めていくにあたっては、加盟店への周知と併せて消費者であるカード会員の理解・協力を得るための周知・啓発への取組が強く求められる。

また、昨今では、フィッシング等を起因とするカード会員からのクレジットカード情報窃取等によるクレジットカードの不正利用被害も増加しており、カード会社をはじめとする関係事業者においてはDMARCその他のフィッシング対策を講じているものの、事業者における対策だけでは限界もあることから、消費者であるカード会員自らがフィッシングの被害に遭わないための取組が強く求められるところである。

７－１－２　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、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。

また、行政及び日本クレジット協会は、関係事業者に対して、本ガイドラインの内容を広く周知し、セキュリティ対策について必要な助言や情報提供を行うなどにより、事業者の取組を支援することが必要である。

７－２　今後の不正利用防止対策に向けた協議会の活動

不正利用被害の減少、クレジットカード取引の安定性・信頼性の確保の観点からは、関係事業者が連携し、業界全体で取組むことが重要である。

特に、2025年3月末までに、原則、全てのEC加盟店にEMV 3-Dセキュアの導入を求めていくにあたっては、EMV 3-Dセキュアの運用環境についての課題や、今後のトランザクション量の増加が及ぼす影響を踏まえ、EMV 3-Dセキュア導入後のクレジットカー

ド取引が安定的に稼働し、その効果が適切に発揮されるよう、カード会社（イシュアー・アクワイアラー）、PSP、EC 加盟店、国際ブランド等の関係事業者が協力して課題解決に向けて取組み、適切な環境整備を行う必要がある。

また、不正発生状況やリスクに応じた多面的・重層的な不正利用対策への取組として、EMV 3-D セキュア以外の他の不正利用対策も併せた実効的かつ現実的な対策の検討に取組むこととする。

【履歴】

2020 年 3 月 19 日	新規制定	1.0 版
2021 年 3 月 10 日	改訂	2.0 版
2022 年 3 月 8 日	改訂	3.0 版
2023 年 3 月 14 日	改訂	4.0 版
2024 年 3 月 14 日	改訂	5.0 版