クレジットカード・セキュリティガイドライン【1.0 版】

＜公表版＞

2020/03

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

「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）」では、我が国のクレジットカード取引において、「国際水準のセキュリティ環境」を整備するために、2016 年 2 月に、クレジットカード取引の関係事業者が取組むべき具体的なセキュリティ対策とその実施期限を 2020 年 3 月末と定めた「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）」を策定し、毎年度改訂を行いながら、その推進に精力的に取組んできた。

この間、2016 年 10 月には割賦販売法が改正され、カード会社（イシュアー・アクワイアラー）*に加え加盟店に対してセキュリティ対策が義務付けられ、2018 年 6 月から施行されている。実行計画は同法に規定するセキュリティ対策に係る措置の実務上の指針となっており、実行計画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、同法で求める「必要かつ適切な措置」が講じられていると認められることとしている。

実行計画の推進及び割賦販売法改正は、多くの関係事業者のセキュリティに対する意識変革をもたらし、我が国のクレジットカード取引におけるセキュリティ対策の取組は大きく前進した。

このように、各関係事業者によるセキュリティ対策が進展する一方、クレジットカードの不正利用等の手口も多様化・巧妙化しており、クレジットカードの不正利用被害額は未だに増加傾向にある。

健全なクレジットカード取引が確保される環境を整備するためには、実行計画の実施期限である 2020 年 3 月以降においても不正利用の発生状況等に応じたセキュリティ対策の継続的な検討や実施は必須であるところ、今般、クレジットカード取引の関係事業者が実施する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）」として取りまとめた。

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、安全・安心なクレジットカード利用環境が整備されることを期待する。

2020 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 加盟店におけるなりすまし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等で、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	Delivered Unique Key Per Transactionの略。 暗号化のためのプロトコルであり、トランザクションごとに異なる暗号鍵による暗号化処理を行う仕組み。
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。
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共に、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など、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、および認知を担当する、グローバル規模の開かれた協議会。
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、クレジット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、サーバーなど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（改正割賦販売法第 35 条の 17 の 2）のこと。
カード情報	クレジットカード会員データ（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、クレジット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。
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するが、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、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。

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）」「PSP*（Payment Service Provider）」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」「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。また、決済場面では、コード等が用いられ、その決済代金が国際ブランド付きのクレジットカードで請求されるコード決済サービスにおいては、クレジットカード紐付け時におけるクレジットカード会社（イシュアー）及びコード決済事業者における本人確認等のセキュリティ対策が重要となる点にも留意する必要がある。

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。

７．ガイドラインの最新性・実効性等について

カード情報の漏えい、不正利用の手口は時とともに巧妙化、多様化しており、セキュリティ対策の内容もそれに適したものでなければならない。

本ガイドラインにおいても、カード情報の漏えい、不正利用被害の発生状況、手口等を検証し、これらの発生防止や被害拡大防止に適した対策を求めていくこととする。

Ⅰ．クレジットカード情報保護対策分野

カード情報[注]*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。

カード情報保護対策について具体的には、カード情報を保持しない非保持化*や、カード情報を取り扱う場合は、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）への準拠の取組がある。PCI DSS の準拠においては、事業者が PCI DSS の内容を正しく理解し効率的に対応する必要がある。

本ガイドラインにおいて加盟店は非保持化（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、カード会社及び PSP は PCI DSS 準拠が求められる。

各事業者は、本ガイドラインに基づき自社の実態を踏まえたカード情報保護に向けた適切な対策を講じる必要がある。

注　「カード情報」とは、クレジットカード会員データ（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、クレジット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たアプローチをする必要がある。さらに、非対面加盟店のうち、昨今カード情報漏えい事案が発生している 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簡易なログインパスワードを設定しているなどの管理画面への不十分なアクセス制御等のウェブサイトの開発・運用段階での設定の不備、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、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	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せざるを得ないが、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	カード情報を自社内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 準拠に並ぶ措置として整理する。

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」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（通話データを含む）

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 に則って取組む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」するカード情報や「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は、この「通過型」の EC 加盟店にて発生したものが多数であった。

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セキュリティ措置としては、非通過型の導入がある。ただし、この場合、非通過型の決済サービスを提供する PSP が PCI DSS 準拠済みであることが前提である。

＜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 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保持にあたるため、PCI DSS に準拠する。

＜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な場合には、カード情報が漏えいするリスクが残るため、EC サイトの脆弱性対策を行うことが重要である。

・既存の EC 加盟店においては、自社サイトにカード情報を含む決済情報等のログが蓄積されるなどのシステム的問題点を認知できていないケースもあることから、不要なシステムログ等の有無を確認し、有る場合は速やかに消去を行う。

・「通過型」か「非通過型」の認識がなく、カード情報の漏えい事故が発覚してから、「通過型」を導入していたことを認識した事例もあることから、自社の決済システムを確認し、「通過型」であれば、カード情報を保持しない非通過型へ移行するか、カード情報を保持する場合は、PCI DSS 準拠が必要である。

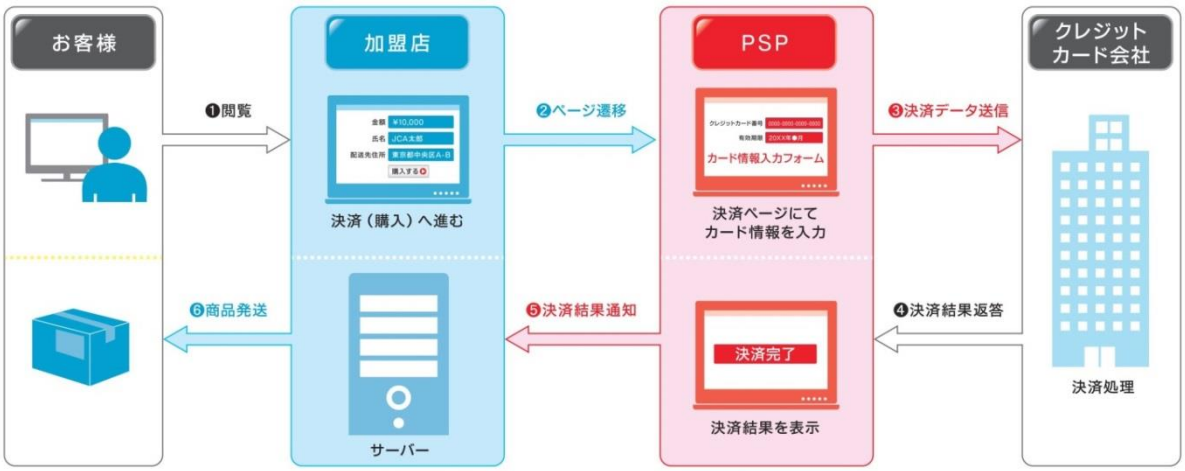
□EC 加盟店における非保持化導入例

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み決済を行う方式

❶リダイレクト（リンク）型

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。クレジット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。

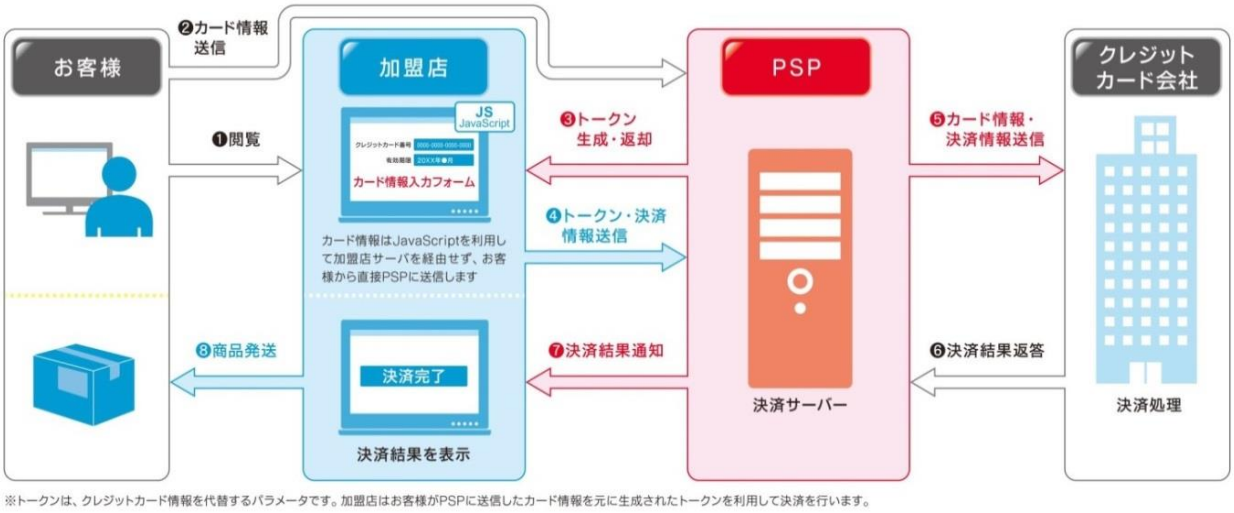
【❶リダイレクト（リンク）型】
（決済画面は PSP のサイトへ遷移する）



❷Java Script 型（トークン型）

加盟店のクレジット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、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）「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（以下「MO・TO 加盟店」という）」においては、顧客から電話・FAX・はがき等でカード情報を入手し、MO・TO 加盟店の機器においてカード情報を入力し決済を行うため、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となる。

イ）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となる。（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。

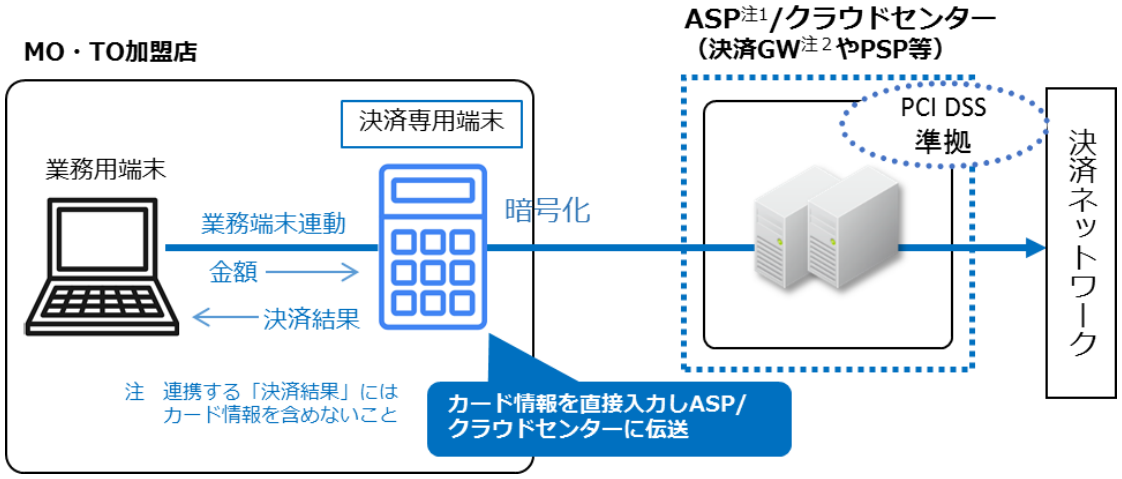
□MO・TO 加盟店における非保持化（非保持と同等/相当含む）導入例

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

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。当該決済専用端末と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も業務用端末側の決済結果には、カード情報を含めないこと。また、通信回線はキャリア等の外部の回線を使用する。

【❶非保持化　決済専用端末を利用した外回り方式】



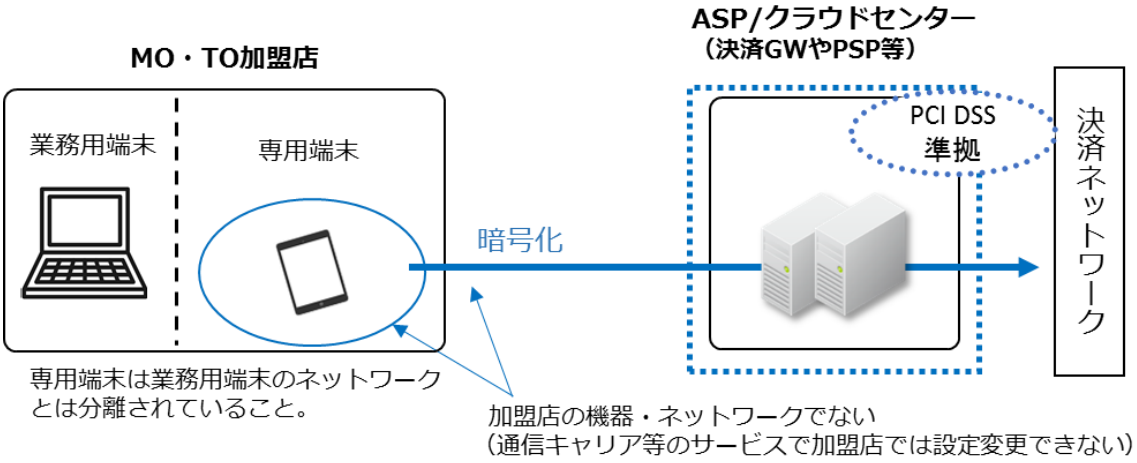
注 1　ASP は Application Service Provider の略

注 2　決済 GW は決済ゲートウェイの略

❷非保持化　タブレット端末を利用した外回り方式

加盟店のオペレーターが PSP 等の加盟店以外から提供されたタブレット端末等の機器・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。

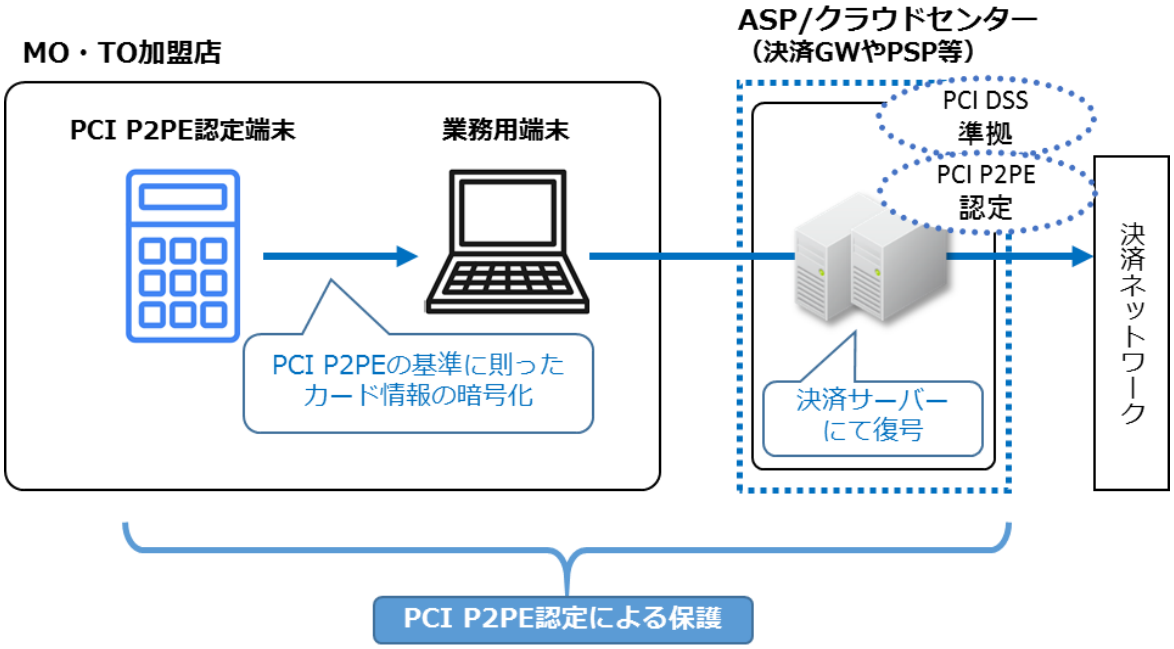
【❷非保持化　タブレット端末を利用した外回り方式】



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*（Delivered 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毎回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を利用することにより、仮に漏えいしても、カード会員データが暗号化されているうえに、トランザクションごとに暗号鍵がそれぞれ異なり、解読方法もそれぞれ異なるため、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。このため解読された場合でも当該カード番号だけが使用可能なため、漏えいした場合でも不正利用されるリスクは極めて小さくなることから、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できる。

イ）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を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できる。（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。

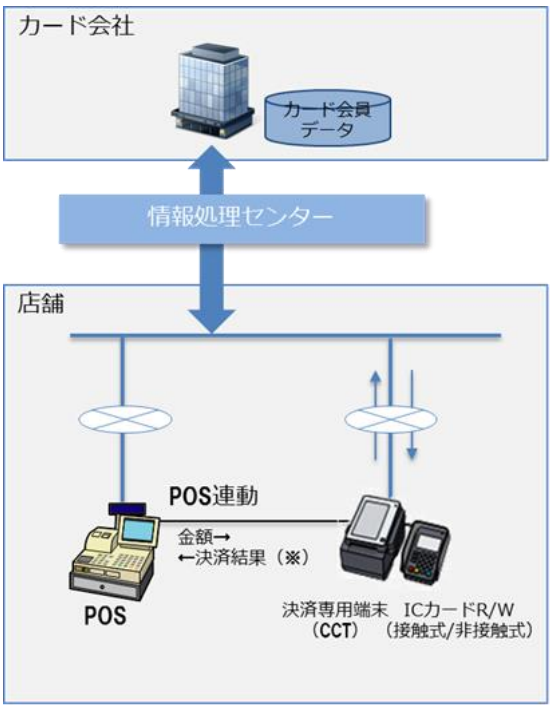
□対面加盟店における非保持化（非保持と同等/相当を含む）導入例

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）

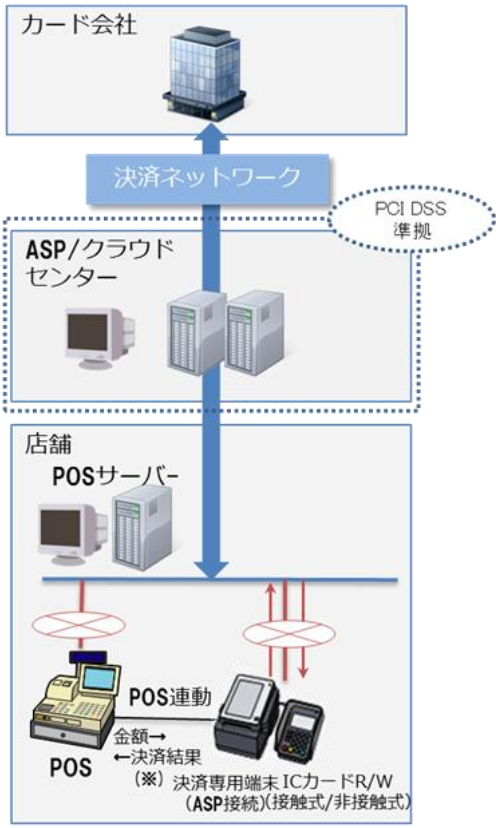
オーソリゼーションやクレジットカードの売上処理を、加盟店あるいはカード会社等が所有する決済専用端末から直接外部の情報処理センター又は ASP/クラウドセンター等に伝送して行う方式である。両方式とも、決済機能は POS システムの外側となるため、カード情報が POS 端末や POS システムの機器・ネットワークを「保存」「処理」「通過」しないことから、カード情報の非保持化が実現できる。なお、POS システムでクレジットカード決済を行わず「IC 対応*した決済専用端末」のみを使用し、カード情報を直接外部の情報処理センター等に伝送している加盟店も非保持となる。

【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

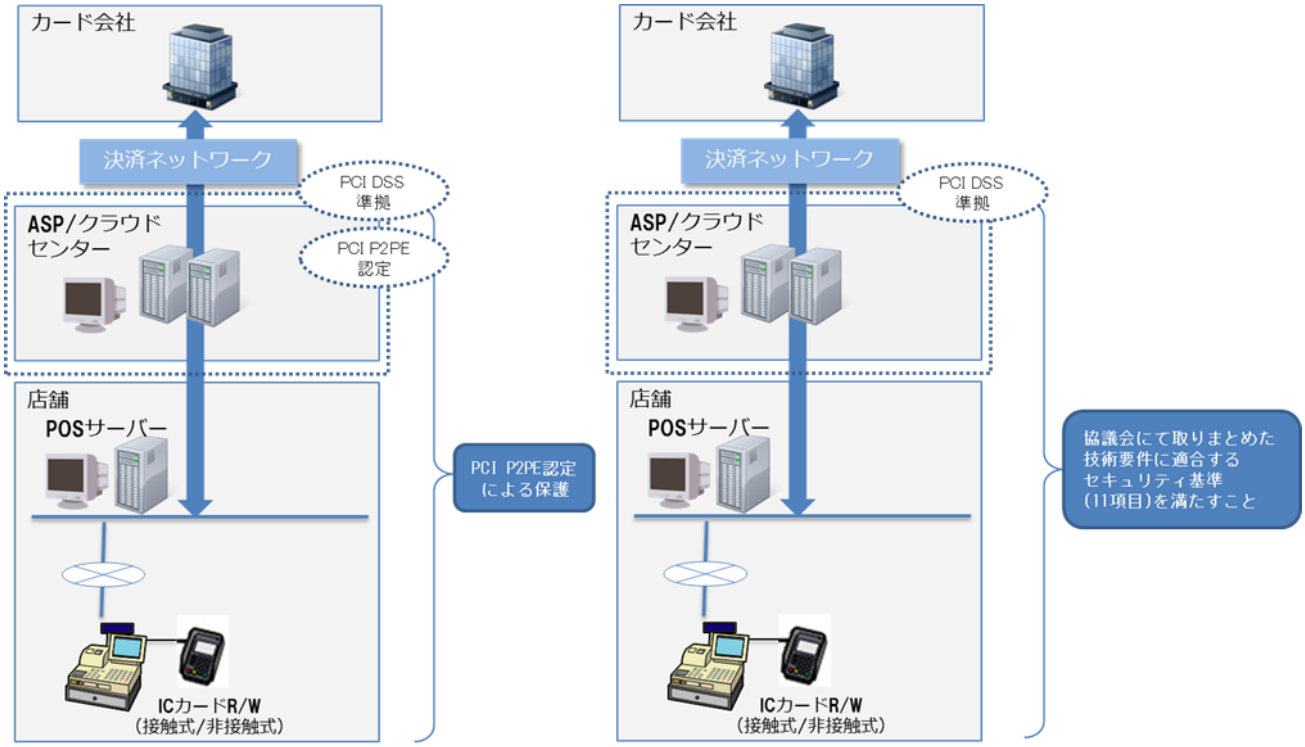
【❷非保持化　ASP/クラウド接続型】



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取りまとめた「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」に適合するセキュリティ基準（11 項目））を満たすことが求められる。

【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

非保持化実現前は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加盟店とカード会社間で対応してきたが、非保持化を実現した場合の対応としては、次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）を実現した加盟店における照会等対応では、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）はあるものの、クレジットカード番号以外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・カード会社が一律、同レ

ベル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て加盟店、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）実現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（通話データを含む）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、各加盟店の運用実態は異なり、顧客対応についても一律的な対応とすることは困難であることから、運用上の課題については各加盟店、カード会社、必要に応じて ASP 事業者等が連携の上、個別に検討を進めることが重要である。

ｂ）過去に取り扱ったカード情報の保護対策

非保持化実現加盟店において、電子帳簿保存法に基づく管理が求められ、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。

注　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

加盟店がカード情報を保有する場合には PCI DSS に準拠することが求められる。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。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、準拠においては自社に求められる事項を検証する必要がある。

なお、PCI DSS 準拠の取組をサポートするため、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）が本協議会と協力して、各種資料の提供や相談窓口を設置している。（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）

■カード情報を取り扱うカード会社は、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、PSP 等と連携の上、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 準拠を推進するとともに、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。また、PCI DSS 準拠を完了していない PSP がある場合には可及的速やかに準拠するよう指導を行う。

■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など、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。

（3）PSP

■カード情報を取り扱う PSP については、PCI DSS に準拠し、これを維持・運用する。

■カード会社（アクワイアラー）と協力して、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行い、その取組を支援する。

（4）その他関係事業者等

①国際ブランド

■本ガイドラインに掲げるカード情報保護対策の実現に向け、国際ブランドの各種ルール等との調整を行い、各種課題の解決に向けて関係事業者と協働して取組む。

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

②ソリューションベンダー

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

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」（2018 年 7 月 25 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

関係事業者は、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。

また、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又は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は、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に被害の拡大を防ぐために、取引に関係するカード会社及び PSP は早急にリスク回避に向けた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及び PCI DSS 準拠等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、契約カード会社（アクワイアラー）等は、加盟店からの 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）等で協議の上で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

我が国のクレジットカード取引は磁気情報での取引が大半を占めてきたことから、犯罪組織等にその情報が窃取され、偽造カードによる不正利用被害が後を絶たず、喫緊の課題としてIC取引*の推進に取組んできた。海外に目を向ければ、大手加盟店のPOSシステムがウイルスに感染し、そこで決済したカード情報を含む顧客情報が大量に窃取されるという事案が頻発したことを受けて、特に最大の偽造カード被害国であった米国では偽造カードによる不正利用対策としてIC対応が急速に進められた。欧州等では既にほぼ100%がIC取引となっており、磁気情報による取引の継続は、我が国クレジットカード取引のセキュリティ対策が脆弱であるとの印象を与え、安全・安心を求める訪日外国人の需要の取込を阻害する要因にもなりかねない。

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

１．各事業者に求められる対策等

（１）加盟店

■IC取引を可能とするため設置する決済端末の全てをIC対応する。【指針対策】
■特に、POSシステムでクレジットカード決済を行う加盟店は、自社のIC対応に係る実現方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。

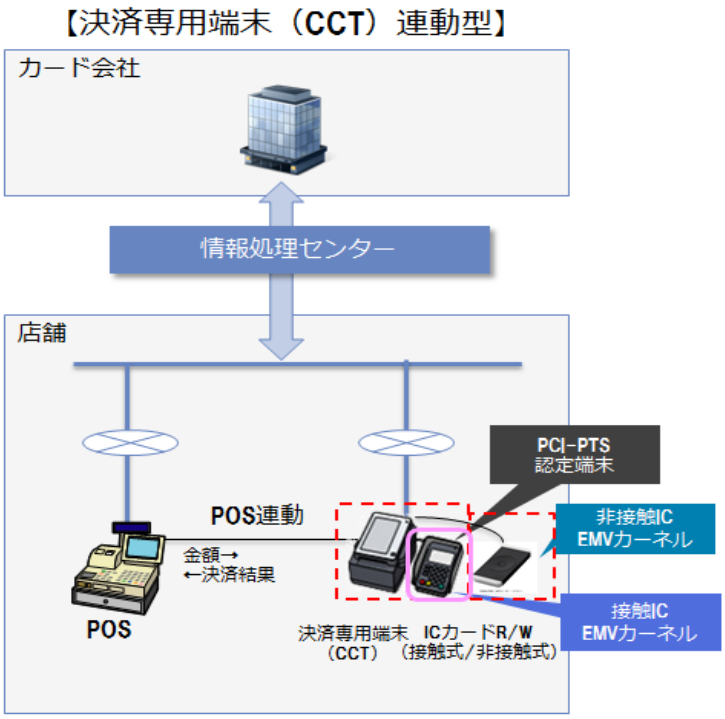
※詳細は、「ICカード対応POSガイドライン」を参照、また、カード情報保護の観点からのパターン別構成図は、「Ⅰ．クレジットカード情報保護対策分野」（11頁～12頁）の記載内容を参照。

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、POSシステムの外側となるため、決済専用端末側で開発・EMV認定*・ブランドテスト*等の対応を行えばよく、POSシステム側で対応する必要がないことから、導入時における対応（開発・EMV認定・ブランドテスト等）の影響が最も小さい。また、カード情報がIC対応の決済専用端末から直接カー

ド会社に伝送されるため、加盟店におけるカード情報の非保持化が同時に実現できる[注]。一方で、決済専用端末を新たに追加する必要があるため、設置場所の確保等の課題がある。

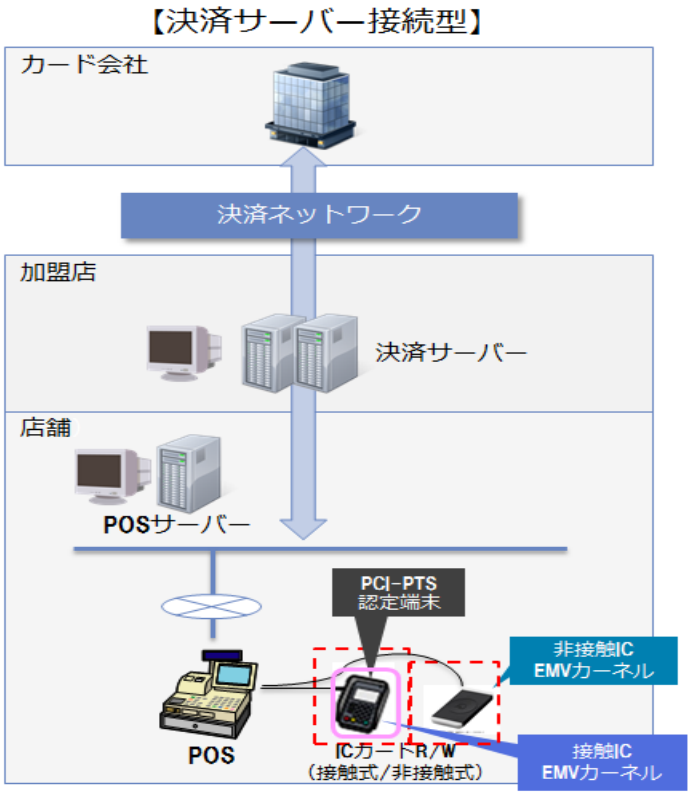
注　非保持化の実現においては、決済専用端末（CCT）より POS へ連動する「決済結果」にカード情報を含めないことが前提。



２）決済サーバー接続型

POS システムでクレジットカード決済を行うが、EMV カーネルが PIN パッドにある仕組みである。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、導入時における対応の影響は小さい。

この場合、カード情報は POS システムを通過してカード会社に伝送されるため、カード情報が自社で保有する機器・ネットワークを「保存」「処理」「通過」するため、カード情報を保持することになることから、PCI DSS 準拠が必要となる。

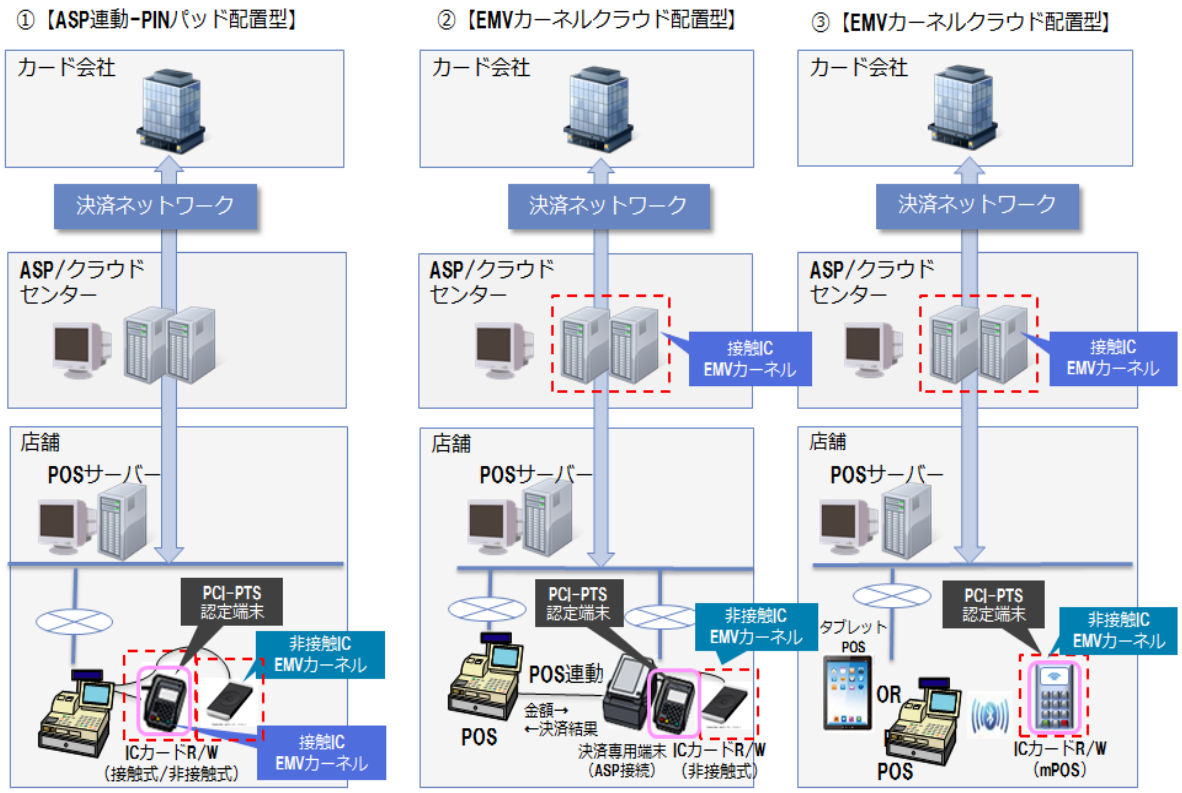


3）ASP/クラウド接続型

POS システムと加盟店の外部の事業者（ASP）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。基本的には上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）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取りまとめた「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」に適合するセキュリティ基準（11 項目））を満たすことが求められる。

注　非保持化の実現においては POS 連動する「決済結果」にカード情報を含めないことが前提。

※上記 11 項目の詳細については、附属文書「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」を参照。



②IC 対応した決済専用端末（CCT）の導入

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

③特定業界向けの IC 対応について

1）ガソリンスタンドにおける IC 対応上の実現可能な方策

日本国内のガソリンスタンドにおいては、利用者が乗車したまま決済するといったサービス対応を行うフルサービスのガソリンスタンドの場合、総務省消防庁通知の内容に準拠したPIN入力が可能なハンディ端末の開発・導入が必要となる。

また、セルフサービスのガソリンスタンドにおいては、現行システム・機器の仕様の制約上、現状では国際基準が求めるPINパッドの設置等が困難であり、代替コントロール策の導入が必要となる（以下、2）オートローディング式自動精算機におけるIC対応参照）。

このため、ガソリンスタンドにおける業界固有の課題を踏まえながら、IC対応上の実現可能な方策を示す「国内ガソリンスタンドにおけるICクレジットカード取引対応指針」を取りまとめている。同指針に基づき対応することでIC対応することとする。

※詳細は附属文書「国内ガソリンスタンドにおけるICクレジットカード取引対応指針」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」を取りまとめた。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
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（30 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の IC 対応を促進させるため、本ガイドラインで整理された各方策について加盟店の理解を促す活動を行うとともに、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、カード会社と調整を行う。

②機器メーカー

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

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

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

③行政

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

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に基づき対応することとする。

※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。

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を参考にし、IC 取引を推進することとする。

なお、本人確認不要加盟店は、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、接触 IC 取引・非接触 IC 取引ともに全件オンラインオーソリゼーションを必須とする。

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

・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、当該カードでのサインによる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の装備も必須とする。
・CVM リミット金額[注]*以下の場合には、カード会員の利便性と不正利用防止の両立から本人確認は不要とする。具体的には、本人確認を求めることがクレジットカード取引の阻害要因となり、また、本人確認が不要となることにより決済処理の迅速性が増し、クレジットカード取引の普及に寄与する業種業態の加盟店を対象とする。ただし、不正利用のリスクが低い業種売場等であることを前提とし、不正利用防止の観点から換金性の高い商品を除外する。
・また、現在、IC 取引において、カード会員の PIN 失念への一時的な救済措置が可能となるよう PIN 入力スキップ機能（PIN バイパス）の運用が許容されているが、本機能の利用により PIN 入力による本人確認を実施しないことで不正利用被害が発生するリスクがあることや、海外カード会社発行のカードには本機能を許容しないものも存在し利用阻害が発生することを踏まえ、日本クレジット協会及びカード会社は、本機能の将来的な廃止に向けて検討することとしている。
・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 取引の形態は、「カード型」と「モバイル型等（「キーホルダー型」「ウェアラブル型」）を含む」に分けられる。
・非接触 IC 取引の多くは CVM リミット金額以下になることが想定されるため、消費者の利便性も勘案し、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。
・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。

◆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。

・「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	不要		
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 取引への切替えを許容しないカードが存在するため

３．その他留意事項

（１）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）」が取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通信販売の加盟店（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なりすましによるものである。また、その被害額は近年増加傾向にあり、2018 年度においても高水準にある。

近年、なりすましによる不正利用被害が急増した背景としては、漏えいしたクレジットカード番号の不正利用に加え、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加盟店において集中的に短期間で使用する手口が急増したこと、加えて不正利用の巧妙化により真正利用との判別が困難になるといった要因等が考えられる。

このような不正利用の発生状況等を踏まえ、非対面加盟店、特に EC 加盟店におけるなりすましによる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、犯罪組織や悪意のある第三者による不正な取引を検知・停止する取組を一層強化し、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なりすまし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。

■自社の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、契約先のカード会社（アクワイアラー）や PSP との間で迅速な情報共有に努める。

■加盟店サイトでの大量かつ連続する申込については早期に検知、遮断するなど、加盟店各社サイトにおいて被害の状況等に応じて必要な対策を講じることに努める。

なりすましによる不正利用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。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ていくことが有効である。日本クレジット協会の調査においても複数の方策を導入した加盟店において、不正抑止の効果を確認することができたことから、加盟店は、契約先のカード会社、PSP、セキュリティ事業者等と連携し、本ガイドラインが掲げる以下の 4 つの方策の中からリスクの状況に応じて導入することを基本とした不正利用対策を確実に実施していくことが求められる。

①加盟店におけるなりすまし不正利用対策の具体的方策

１）本人認証

EC 加盟店におけるなりすまし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

・「3-D セキュア」とは、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等（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等があり、国際ブランドが推奨する本人確認手法である。

・加盟店が「3-D セキュア」を導入した場合、本人確認が要求される全取引に対してパスワード確認が実施されることになるが、パスワード未登録の際のカード会員の利用阻害を避けるためにパスワード入力を省略した結果、なりすましによる不正利用被害が発生している。このため、3-D セキュア導入加盟店において本人認証が要求される対象取引全てに実施されることが必要である。

・カード会社（イシュアー）とカード会員のみが認知している情報による照合は、その情報が漏えいしない限り有効であるが、カード会員によるパスワードの使い回しやパスワードの漏えいにより、その効果が発揮できない状況も発生している。

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、カード会員の属性情報を送信し、カード会社に予め登録され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。本人の属性情報を用いるため、カード会員のパスワード失念などの懸念がないのが特徴である。

・一方、「認証アシスト」を導入する場合、加盟店は当該サービスを利用するカード会社との間で直接契約が必要であり（国内のカード会社のみが対象）、利用者全てのカードが対象とならない可能性がある。

・「3-D セキュア」と同様、カード情報とともに当該属性情報が漏えいした場合には不正利用被害発生のリスクが生じることとなる。

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。

・「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。

・クレジットカード番号とともに「セキュリティコード」が窃取されることにより、券面認証を突破される被害が一部確認されているが、こうしたことがなければ、一定の不正利用防止効果が確認されている。

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、利用者の入力情報（氏名、クレジットカード番号、e 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、加盟店が収集できる情報に基づいて取引のリスク評価（ス

コアリング等）を行い、不正な取引であるか加盟店側で判定する手法である。特に、利用者のデバイス情報は、通常のオーソリゼーションの過程においてはカード会社で取得できない情報であるため、これを活用することで不正検知精度の向上が期待できる。

・不正取引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。

・また、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により重要である。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になる。

4）配送先情報

・不正利用された注文等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、その情報の蓄積には時間がかかることから、新規に取組を始めて直ちに効果が発揮されることは困難であるため、外部の実績があるサービスの利用等が有効である。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存在する。

・「配送先情報」による不正利用対策では、送付先の不自然さ等から、不正な取引か否かの判断を行うことも必要となるため、加盟店においては不正判断ノウハウの蓄積や体制構築も必要となる。

方策		特徴
1）本人認証	a）3-D セキュア	・国際ブランドが推奨する利用者がカード会員本人であることを確認する仕組み ・カード会員のみが知るパスワード等（静的・動的）やその他の情報（デバイス情報等）を用いて本人認証を行う ・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の登録属性情報を照合し本人を確認 ・カード会員のパスワード失念等の懸念がない
2）券面認証 （セキュリティコード）		・カード券面の「セキュリティコード（数字 3～4 桁）」を入力し、カードが真正であることを確認 ・カード会員の対応が容易 ・加盟店の対応も比較的容易 ・カード券面への印字はイシュアー側でほぼ 100%対応済み ・機械的にカード番号を生成して攻撃する手口に有効

3）属性・行動分析 （不正検知システム）	・過去の取引情報等に基づくリスク評価によって不正取引を判定 ・抑止効果維持には継続的なルールのチューニングが必要で、カード会社との継続的な情報連携が重要 ・カード会員の負担なし ・発生状況に合わせたルール設定可能 ・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利用で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、前述のなりすまし不正利用防止の 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において、不正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。そ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、カード会社が不正利用のリスクを評価するためのオーソリゼーション処理の体制整備を図ることである。この上で、以下の加盟店については、リスクや被害発生の状況に応じた方策の導入を求める。なお、昨今の不正犯の手口として、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）が発生しており、継続的（連月）ではなくとも単発的（単月）で高額な不正被害が発生する加盟店に対して、カード会社（アクワイアラー）は早急に追加的な方策を導入する必要があると判断する場合があり、当該加盟店には方策の導入を含めた不正利用防止策の実施を求める。

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なりすまし不正利用対策の 4 つの方策のうち、1 方策以上の導入を求める。

なお、宿泊予約サービスは、2020 年度より追加となり、当該商材を主たる商材として取り扱う加盟店については、2020 年 9 月末日までにその対応の完了を求める。

３）不正顕在化加盟店

不正利用被害が多発状況にあるとカード会社（アクワイアラー）等が認識する加盟店は「不正顕在化加盟店」として、本ガイドラインの掲げるなりすまし不正利用対策の 4 つの方策のうち、2 方策以上の導入を求める。なお、「不正顕在化加盟店」となる条件については、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」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、不正利用防止についての追加的な方策の導入等のため継続的な検討が求められる。

＜加盟店分類表＞

1）全ての非対面加盟店 ○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
2）高リスク商材取扱加盟店 ○本ガイドラインが掲げるなりすまし不正利用対策の 4 方策のうち、1 方策以上
3）不正顕在化加盟店 ○本ガイドラインが掲げるなりすまし不正利用対策の 4 方策のうち、2 方策以上

○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、コンピューターを用いて自動的に申込ませる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、加盟店においてこれらの相違点等から不正な取引を早期に検知し取引を遮断することは、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・強化に努める。

■「3-D セキュア」において、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」の導入を検討する。

■「3-D セキュア」の利用拡大のため、カード会員の利用登録率の向上を図るとともに、「動的（ワンタイム）パスワード」の導入を促進する。

■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、真正利用確認照会件数の増加を想定

した対応体制を整備する。
■「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た多数回連続アクセスに対して早期に検知し、当該取引を不成立とする対策が必要である。

①「3-D セキュア」におけるリスクベース認証

「3-D セキュア」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）において不正利用抑止効果が認められている。

本機能は過去の不正実績とデバイス情報等を活用したリスク評価モデルにより、不正利用の判別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推奨される。

②「3-D セキュア」の利用登録率向上の施策推進

・「3-D セキュア」は、カード会員が「静的（固定）パスワード」を失念した場合の販売機会の損失の懸念もあるため、カード会員へのパスワードの管理に関する周知活動が重要である。
・利用登録率向上の施策推進にあたっては、カード情報とともに「静的（固定）パスワード」が窃取されたことによる不正利用被害が発生している状況を踏まえると、「リスクベース認証」や「動的（ワンタイム）パスワード」、「指紋等の生体情報によるデバイス認証」の導入をともに行うことが有効策となり得る。
・「リスクベース認証」「動的（ワンタイム）パスワード」や「指紋等の生体情報によるデバイス認証」の利用は国際ブランドも推奨しており、特に「リスクベース認証」「動的（ワンタイム）パスワード」については国内においても既に複数のカード会社（イシュアー）に採用されている。今後、新たに「動的（ワンタイム）パスワード」を採用するカード会社（イシュアー）の増加等により、パスワードの漏えいに起因する不正利用対策の強化やパスワード失念による販売機会損失の回避が図られることが期待される。
・次期バージョンである「EMV 3-D セキュア*」においては、カード会社（イシュアー）は加盟店がカード会員の同意を得た後に提供するカード会員に関する情報を用いたリスクベース認証が可能となる。また、ログイン認証等の他認証方式もサポート可能なことから、静的（固定）パスワードからの脱却が図れる。

③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）が必要となる等の課題について考慮する必要がある。

④「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、早期に検知し、当該取引を不成立とさせることが重要となる。

（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、なりすまし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（37 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、なりすまし不正利用の傾向や事例等の情報及びなりすまし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、加盟店におけるなりすまし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加盟店におけるなりすまし不正利用対策の具体的方策（34 頁を参照）」

（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なりすまし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なりすまし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なりすまし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、時として消費者の利便性に影響を及ぼすことも事実であることから、推進にあたっては消費者の理解・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、行政は、日本クレジット協会とともに、加盟店業界団体、消費者団体等と連携の上、クレジットカードの情報保護対策及び不正利用対策に関する消費者及び事業者向けの周知・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「見える化」への取組に努めることとする。

■EC 加盟店は、カード会社及び 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の情報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など、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、特に丁寧に対応していくこととする。

■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は、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。

■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に関する周知活動を積極的に行う。

（3）カード会社（アクワイアラー）

■契約を有する IC 対応済み加盟店に「見える化」の取組及び「共通シンボルマーク等」を周知し、掲出等を依頼する。また、IC 対応済み加盟店において独自の「見える化」の取組が行えるよう、日本クレジット協会のホームページに掲載されている「共通シンボルマーク等」をダウンロードにより活用できることを周知する。

■EC 加盟店の「見える化」への取組を支援する。

（4）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、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の業界団体、消費者団体等との連携を強化し、消費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、2016 年改正割賦販売法の国会附帯決議を踏まえ、加盟店のクレジットカード取引におけるセキュリティ対策を「見える化」する方策の検討を行い「共通シンボルマーク等」をとりまとめた。消費者が IC クレジットカード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」、「IC 対応デザイン」（以下「共通シンボルマーク等」）を策定し、周知活動に使用している。

■日本クレジット協会は、消費者に対し、IC 取引の安全性及び IC 対応の「見える化」の方策である「共通シンボルマーク等」を周知するとともに、PIN 認知度の更なる向上のための周知に引き続き取組む。

■日本クレジット協会は、クレジットカード業界全体で IC 取引を推進していること、IC 取引では本人確認のため PIN 入力が必要になることの周知に引き続き取組む。

■日本クレジット協会及び業界団体等はカードの不正利用対策の必要性やその具体的な方策に関するカード会員の理解・協力を得るために、EC の不正利用対策に関する消費者への周知活動に取組むこととする。

■日本クレジット協会はカード会社（イシュアー）と連携し、カード会員に対し、ID・パスワードの使い回しの防止等について、周知活動に取組む。

■日本クレジット協会は、カード会員に対し、毎月の利用明細を確認することの重要性に関する周知活動を積極的に行う。

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。

参考

（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取りまとめたもの。
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	電子帳簿保存法に基づき、過去のカード情報を含む電子帳簿について非保持化が困難な場合があることを踏まえ、「スタンドアローン環境」での保管・利用などの措置内容を取りまとめたもの。
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	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～	加盟店様・POS ベンダーを対象に、接触／非接触 EMV 対応有人型 POS の導入・修正において考慮していただきたい要件や認定・試験プロセスを整理したもの。
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・考え方を取りまとめたもの。

（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。

【履歴】

2020 年 3 月 19 日　　新規制定　1.0 版