クレジットカード・セキュリティガイドライン【３.0版】
改訂ポイント

【2022年3月】

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

改訂ポイント

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

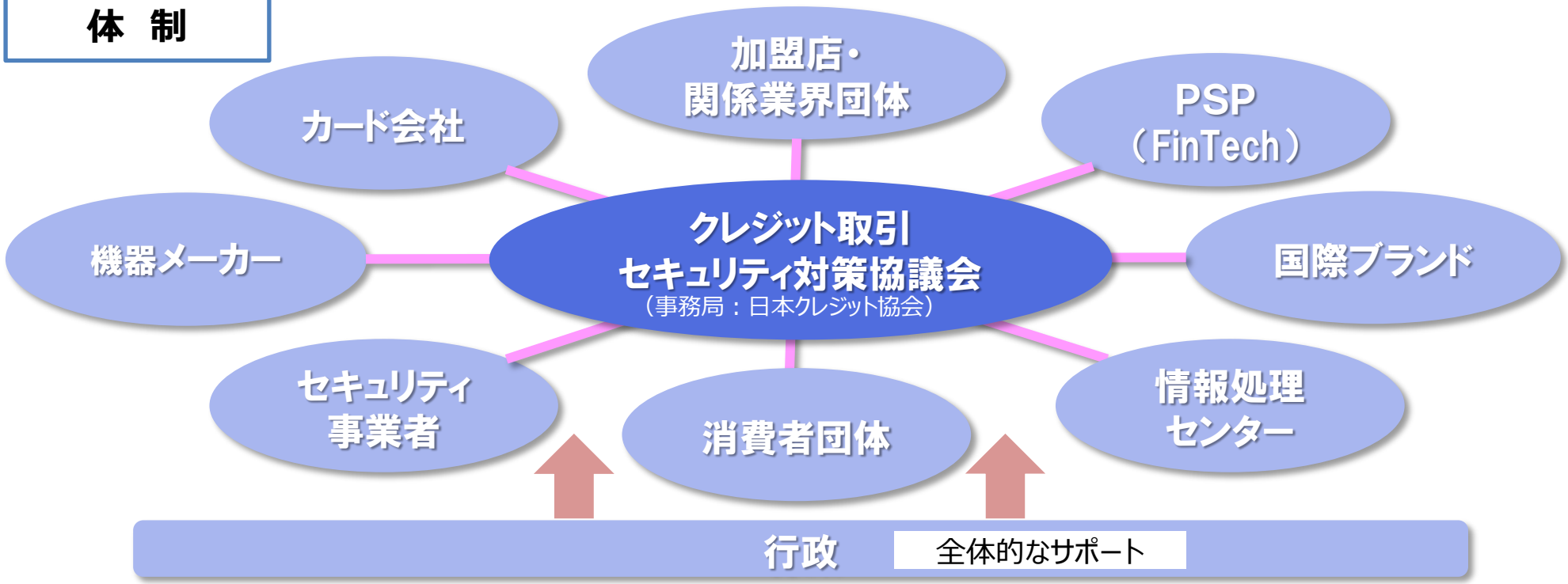
はじめに

はじめに①

クレジット取引セキュリティ対策協議会

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

体　制



はじめに②

協議会　本会議メンバー

【委員】

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

【オブサーバー】

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

2022年3月8日反映

本ガイドラインの基本的な考え方

本ガイドラインの基本的な考え方①

1．本ガイドラインにおけるセキュリティ対策の対象について

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

2．割賦販売法との関係性について

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

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

3．対象となる関係事業者について

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

本ガイドラインの基本的な考え方②

4．ガイドラインの最新性・実効性等について

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

改訂ポイント

〈クレジットカード情報保護対策分野〉

- 割賦販売法第35条の16第1項　第4号から第7号事業者の定義、並びに各事業者が取りうるクレジットカード情報保護対策の明確化。
- EC加盟店の対策

〈不正利用対策分野〉

〈対面取引におけるクレジットカードの不正利用対策〉

- 「サイン」取得の任意化、PINバイパスの廃止、NoCVM（本人確認不要取引）の見直し

〈非対面取引におけるクレジットカードの不正利用対策〉

- EC加盟店の指針対策の見直しと明確化
- EMV 3-Dセキュアの詳細説明
- 不正利用被害拡大防止に向けた新たな施策検討について追記

＜消費者及び事業者等への周知・啓発について（全般）＞

Ⅰ．クレジットカード情報保護対策分野

Ⅰ．クレジットカード情報保護対策分野①

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

◆「４号事業者」：決済代行業者等

○定義

■4号事業者とは、割賦販売法第35条の16第1項第4号に規定される事業者であり、具体的には、アクワイアラーから交付を受けた代金相当額(立替金)を加盟店に交付する事業者を指す。
対象事業者の例としては、以下の通り。
〇決済代行業者(対面取引、非対面取引双方)
〇ECモール事業者(デジタルプラットフォーマーなど)
〇SC,モール等(対面取引)
〇CCT端末先(対面取引)、これらの事業者に限らない。

○【指針対策】

■4号事業者については対面取引、非対面取引のいずれにかかわらずPCI DSSを準拠し、維持・運用する。ただし対面取引を取扱う4号事業者であって、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。

※　詳細は、「セキュリティガイドライン Ⅰ　クレジットカード情報保護対策分野」で説明

Ⅰ．クレジットカード情報保護対策分野②

◆「５号事業者」：QRコード決済事業者等

○定義

■割賦販売法第３５条の１６第１項第５号に規定される事業であり、具体的には、カード会員データ等を別の決済用情報（QRコード、IDなど）に紐付け、当該決済用情報で後払決済を行うことができるサービスを提供している事業者を指す。

対象事業者の例としては、以下の通り。

〇QRコード決済事業者

〇スマートフォン決済事業者

〇ID決済事業者等

〇その他名称の如何に関わらず、カード情報と紐づけた他の決済用番号で決済を行う事業者、これらの事業者に限らない。

○【指針対策】

■5号事業者については、PCI DSSに準拠し、これを維持・運用する。

※　詳細は、「セキュリティガイドラインⅠ　クレジットカード情報保護対策分野」で説明

Ⅰ．クレジットカード情報保護対策分野③

◆「６号事業者」：5号事業者の委託会社

○定義

■割賦販売法第３５条の１６第１項第６号に規定される事業者であり、具体的には、5号事業者からカード会員データの伝送処理保存を委託されている事業者を指す。

対象事業者の例としては、以下の通り

〇第5号事業者からカード情報の管理を受託している事業者

○【指針対策】

■6号事業者については、PCI DSSに準拠し、これを維持・運用する。

※　詳細は、「セキュリティガイドライン Ⅰ　クレジットカード情報保護対策分野」で説明

Ⅰ．クレジットカード情報保護対策分野④

◆「7号事業者」：加盟店向け決済システム提供事業者

〇定義

■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、加盟店が決済代行会社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、決済代行会社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。
〇ECシステム提供会社(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。

〇【指針対策】

■7号事業者については、PCI DSSに準拠し、これを維持・運用する。

※　詳細は、「セキュリティガイドラインⅠ　クレジットカード情報保護対策分野」で説明

Ⅰ．クレジットカード情報保護対策分野⑤

□全ての事業者のセキュリティ対策として、PCI DSS準拠と明確化した。

②PCI DSS準拠

(1)2号事業者で「非保持化」を達成した加盟店を除く、1号事業者から7号事業者についてはPCI DSSに準拠しカード情報の保護を行う。なお、非保持化を達成しても業務の都合等によりPSP等から別途カード情報の還元を受けて保持する場合には「非保持」とはならず、PCI DSSに準拠しなければならない。

(2) 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、自社が対応するべき事項を検証し、準拠する必要がある。

(3)PCI DSSのバージョン変更への対応について
　カード情報を保持する場合の方策であるPCI DSSへの準拠に関しては、今般、現行のバージョンである「Ver3.2.1」から「Ver4.0」へと更新されており、その日本語版が2022年春に公表される予定である。PCI DSSに準拠する各事業者は、PCI SSCのホームページ上で掲載される新バージョンへの移行スケジュールに則り、遺漏なく円滑に対応していくことが必要である。

Ⅰ．クレジットカード情報保護対策分野⑥

割賦販売法の改正により拡充されたクレジットカード番号等取扱業者に対するクレジットカード・セキュリティガイドラインにおけるセキュリティ対策の一覧

			情報保護			
			非保持化			PCI DSS準拠
事業者	事業者の例示		外回り方式		内回り方式（非保持同等/相当）	
1号事業者	イシュア					○
2号事業者	加盟店	EC加盟店	リダイレクト（リンク）型	Java Script（トークン）型		○
		MO/TO	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	○
		対面	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または本協議会が取りまとめたセキュリティ技術要件	○
3号事業者	アクワイアラ					○
4号事業者	決済代行事業者等	対面	一部の事業者においては「セキュリティ対策チェック項目」			○
		非対面				○
5号事業者	QRコード事業者等					○
6号事業者	5号事業者の委託会社					○
7号事業者	加盟店向け決済システム提供事業者					○

Ⅰ．クレジットカード情報保護対策分野⑦

□EC加盟店の対策（セキュリティガイドラインP19抜粋）

最近の漏えい事案では非通過型を採用しているEC加盟店からの漏えいも見られ、2019年末以降、行政（経済産業省、消費者庁）や独立行政法人情報処理推進機構（IPA）によりオープンソースソフトウェアの利用先に対し安全対策を徹底するよう注意喚起がなされている。原因として、EC加盟店では非保持化の達成が目的になっており、行政やIPAの情報などをもとにした、自らのセキュリティ対策の取り組みが不十分な背景があり、基本的なセキュリティ対策が疎かになっていると言える。協議会では、今後は新規契約時に契約主体に対して業界が定める基本的なセキュリティ対策の申告書を提出し、EC加盟店の基本的なセキュリティ対策を確認するなど新たな方策も検討している。

Ⅰ．クレジットカード情報保護対策分野⑧

２．その他留意事項

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

- セキュリティ対策の実施主体者である関係事業者（加盟店、カード会社、決済代行業者等、コード決済事業者等及びその委託会社、加盟店向け決済システム提供事業者等 ）が、カード情報を取り扱う業務を外部委託する場合は、委託者自身が委託先のセキュリティ状況を確認し、責任を持ってPCI DSS準拠等の必要な対策を求める。
- 特に、複数の委託者からカード情報を取り扱う業務を受託する事業者およ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。

（２）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、取引に関係するカード会社及び決済代行業者等は被害の拡大を防ぐために早急に行動を起こす必要がある。具体的には、日本クレジット協会において策定した「クレジットカード情報漏えい時および漏えい懸念時の対応要領」を有事の際の参考にしつつ、二次被害の防止のために必要な措置を講ずることとする。
- また、カード情報の漏えい事案が発生した加盟店等は、被害の拡大を防止するために初動対応として漏えい元（データベース等）のネットワークからの切り離し、カード決済の一時停止等の措置、フォレンジック調査、PCI DSS 準拠等の確認及び再発防止のための適切な措置を講じる。
- 契約元のカード会社（アクワイアラー）等は、漏えい事案が発生した加盟店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、決定することとする。

Ⅰ．クレジットカード情報保護対策分野⑨

附属文書一覧

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

関係文書

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

Ⅰ．クレジットカード情報保護対策分野⑩

補足事項

【注1】カード情報について

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

①**トークナイゼーション**（自社システムの外でクレジットカード番号を不可逆的に別の番号等に置き換え、自社システム内ではクレジットカード番号を特定できないもの）

②**トランケーション**（自社システムの外でクレジットカード番号を、自社システム内では特定できない方法で安全に国際的な第三者機関に認められた桁数を切り落としたもの）

③**無効処理されたクレジットカード番号**

上記にかかわらず、2号業者以外の事業者にはPCIDSS準拠が求められる。

【注2】PCI DSSについて

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

Ⅱ．不正利用対策分野
（A）対面取引におけるクレジットカードの不正利用対策

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策①

２．IC取引時のオペレーションルール

□加盟店によるサイン取得の任意化

- ■ 我が国市場では長年にわたり、本人確認としてサインの果たす役割の重要性に鑑み、カード会員に対してはサインパネルへの自署の徹底を、加盟店に対してはそのサイン照合の徹底について業界を挙げて啓発してきた。
- ■ 割賦販売法による不正利用防止措置の義務化、本ガイドラインに基づくIC化の取組の推進により接触IC取引の実現が進展し、PIN入力による本人確認が一般化している状況にあるものの、オフラインPIN環境に対応していないカードが利用される場合や、非接触IC取引におけるCVMリミット金額を超過する取引の際にサインによる本人確認を行う場合があり、依然、本人確認方法としてサインが残存している。
- ■ 一方で、カード会員自ら決済端末にカードを挿抜する、あるいはかざす決済オペレーションが増加しつつあるなど商慣習の変化があり、また国際ブランドのルールも変更され、サインの取得は加盟店の任意とする動きがあり、世界的には既に、サインが従来果たしてきた本人確認としての有効性が低下している。
- ■ 上記を鑑み、本人確認方法としての「サイン」の取得は2025年3月を目途に加盟店の任意とし、取得しないことを推奨する。なお、「サイン」を取得する場合においてもサインの同一性確認は必須とはしない。

□PINバイパスの廃止

- ■ 現状、IC取引において、カード会員のPIN失念時に「サイン」で救済が可能となるよう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-一方で、サイン任意化により救済措置の意義も低下する
- ■ 上記を鑑み、PINバイパスは2025年3月をもって原則廃止する。

Ⅱ．（A）対面取引におけるクレジットカードの不正利用対策②

２．IC取引時のオペレーションルール

□NoCVM（本人確認不要取引）の見直し

- 店頭でのPIN等による本人確認は、取引の成立を証明する為の基本要件の一つであるが、取引の安全性が確保できる環境であることを前提に、例外的な取引として「本人確認不要取引」を認め、「本人確認不要取引の対象加盟店（業種/売場等）」および「本人確認不要取引の除外商品」を定めてきた。
- 本人確認不要取引は近年諸外国でも急速に普及し、一定金額以下は本人確認を不要とする非接触IC取引の世界的な普及に加えて、今後「サイン」を取得しない取引を推奨することも踏まえ、不正利用防止とカード会員の利便性の両立・カード会員の混乱回避、グローバルな視点の観点から見直しを実施した。
- 本人確認不要取引は、その導入の必要性を十分に勘案したうえで、カード会員の保護並びに不正利用発生の防止に留意するものとし、業界で別途定める「**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**」に基づく適切な対応が図られるように、加盟店に対して十分な説明を行い、理解を求めていく必要がある。
- 同ガイドラインで規定する「本人確認が必要となる業種/売場/商品等」に該当せず、かつ、「本人確認不要取引のCVMリミット金額」の範囲内については、加盟店は本人確認を不要とすることができる
- 本人確認不要取引のCVMリミット金額を変更する。

※ 「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」は日本クレジット協会が定める業界ガイドライン
※ 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

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策③

附属文書一覧①

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

Ⅱ.（A）対面取引におけるクレジットカードの不正利用対策④

附属文書一覧②

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

関係文書

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

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

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策①

□EC加盟店の指針対策の見直しと明確化

（２）EC加盟店

【指針対策】に高リスク商材取扱加盟店、及び不正顕在化加盟店の対策を追記

- 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つの方策の内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。**

●「高リスク商材取扱加盟店」及び「不正顕在化加盟店」のEMV 3-Dセキュア導入推進における内容を追記

１）「高リスク商材取扱加盟店」

○本ガイドラインが掲げる４方策のうち、１方策以上の導入が必要

※EMV 3-Dセキュアへの移行又は導入

２）「不正顕在化加盟店」

○本ガイドラインが掲げる４方策のうち、２方策以上の導入が必要

※EMV 3-Dセキュアへの移行又は導入

○印は必要な措置

※印は求められる措置

※なお、EMV 3-Dセキュアの移行又は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」を参照

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策②

□EMV 3-Dセキュアの詳細説明

①EC加盟店における非対面不正利用対策の具体的方策

●3-Dセキュアとは

■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のこと。

●EMV 3-Dセキュアについて

■EMV 3-Dセキュアでは、各カード会社が、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共に、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セキュアにおいては、クレジットカード登録等、非決済分野での利用が可能であるが、登録カードを利用した不正取引も頻繁に発生していることから、カード登録時にオーソリゼーション処理を行うことを推奨する。

■2022年10月をもって、3-Dセキュア1.0の取扱いが終了するため、EMV 3-Dセキュアへの早期移行が必要となる。
※詳細は「EMV 3-Dセキュア導入ガイド」を参照。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策③

□不正利用被害拡大防止に向けた新たな施策検討について追記

■今後の不正利用防止対策に向けた協議会の活動について

・これまでの取組をしてもなお、非対面不正利用による被害は増加傾向にある。一方、昨今、従来からの加盟店による不正利用防止対策に加え、イシュアーベースやネットワークベース等の不正利用防止の仕組みやサービスが展開され、不正利用防止の効果を上げている。

・また、本ガイドラインでは、個社毎の不正利用対策を基本として推進してきたが、国内の不正利用被害の減少、クレジットカード取引の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も重要となっている。

・このような動向も踏まえ、次年度以降、イシュアーベースやネットワークベース等の不正利用防止の新たな仕組みやサービスの利用状況、効果検証を行うとともに、関係事業者の協調の下、業界として取組める施策を検討し、普及・促進に取組む。

Ⅱ.（B）非対面取引におけるクレジットカードの不正利用対策④

附属文書一覧

No	文書名	目的・概要
1	「2019年版実行計画上の方策導入による不正抑止の好事例の紹介」	カード会社、決済代行会社、加盟店の協力を得て、実行計画に掲げる４つの不正利用防止方策を導入した際の不正抑止効果について好事例集としてとりまとめたもの。
2	「非対面加盟店における不正利用対策の具体的な基準・考え方について」	加盟店のリスクや被害発生の状況等に応じ、実行計画に掲げる４つの不正利用防止方策を導入する際の指針として、具体的な基準・考え方をとりまとめたもの。
3	「EMV 3-Dセキュア導入ガイド」	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毎に必要な情報が分かりやすいように取りまとめたもの。

Ⅲ. 消費者及び事業者等への周知・啓発について

Ⅲ. 消費者及び事業者等への周知・啓発について①

１．消費者への周知・啓発

（１）カード会社（イシュアー）

- 「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署名の任意化」及びPIN入力スキップ機能(以下、「PINバイパス」の廃止)に向けカード会員へ暗証番号の必要性について周知、啓発活動に取組む。
- 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。
- フィッシング被害に遭わないように、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、またフィッシングによる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カード会員に対する周知活動に取組む。
- 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、カード会員に対する周知活動に取組む。
- 静的パスワードから動的パスワードに移行する場合など、新たな本人認証方法を導入する場合は、改めてその必要性などについて、カード会員への周知活動に取組む。

Ⅲ. 消費者及び事業者等への周知・啓発について②

（２）加盟店

(対面取引)

- 対面取引の加盟店においては、「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署名の任意化」、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。
- 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。

(非対面取引)

- 非対面取引においては、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。
- 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。

Ⅲ. 消費者及び事業者等への周知・啓発について③

（３）その他関係事業者等

①国際ブランド

■グローバルな観点から、海外におけるカード情報保護に関するリスクや各種課題、我が国における国際水準のセキュリティ環境の整備の必要性等について、積極的に働きかける。

②業界団体等

- 日本クレジット協会は、カード会社(イシュアー)と連携し、協議会が策定した対面取引における「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署名の任意化」、及び「PINバイパス」の廃止に向けた周知、啓発活動に取組む。日本クレジット協会は、クレジットカード業界全体でIC取引を推進していること、IC取引では本人確認のためPIN入力が必要になることの周知に引き続き取組む。
- 日本クレジット協会は、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、啓発活動に取組む。
- 日本クレジット協会は、カード会社(イシュアー)や関係団体等と連携し、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、また、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、啓発活動に取組む。
- 日本クレジット協会は、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、啓発活動に取組む。

Ⅲ. 消費者及び事業者等への周知・啓発について④

2．事業者等への周知・啓発

（1）カード会社（アクワイアラー・PSP）

- 「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署名の任意化」、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。
- 署名取得の任意化及びPINバイパスの廃止について、加盟店へ周知するとともに、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などの必要な対応を依頼する。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。
- EC決済事業者が加盟店となる際には、カード情報漏えい対策が強く求められるものであり、セキュリティ・チェックリストの活用などの対策を講じる必要性があることをから、その重要性について自社のホームページに掲載することなどにより促進することが求められる。

（2）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、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業界団体等

- 加盟店におけるセキュリティ対策については、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。