

クレジットカード・セキュリティガイドライン【4.0版】 改訂ポイント

【2023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

1. 不正利用対策分野（非対面取引）

- 不正利用被害拡大防止に向けたEMV 3-Dセキュア導入
- 3-Dセキュア1.0終了に伴う記載の変更
- 不正利用被害拡大防止に向けた今後の取組みについて記載

2. 消費者及び事業者等への周知・啓発

- 消費者への周知啓発
 - EMV 3-Dセキュアの登録および静的（固定）パスワード以外の認証方法への登録・移行
- 事業者等への周知啓発
 - （対加盟店）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

1. 不正利用対策分野

非対面取引におけるクレジットカードの不正利用対策

1.非対面取引におけるクレジットカードの不正利用対策①

□不正利用被害拡大防止に向けたEMV 3-Dセキュア導入

■ EC加盟店におけるEMV 3-Dセキュア導入

- ・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。
- ・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EMV 3-Dセキュア導入計画を作成し、それを実行することが強く望まれる。

※割賦販売法の規定を踏まえ、加盟店が、クレジットカード番号等の通知を受けた際、当該通知がイシューア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（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ことを確認しうるのはイシューアのため、その判断はイシューアが行う）ために必要な措置（EMV 3-Dセキュアの導入）を講じるもの。

※EMV 3-Dセキュアによる認証の対象となる「クレジットカード取引」は、以下を想定。なお、EMV 3-Dセキュアによる認証の運用方法については今後検討し、改めて整理することとする。

- ①クレジットカード番号での決済時
- ②加盟店等のアカウントへのクレジットカード番号の紐づけ（有効性チェックのみ含む）時

1.非対面取引におけるクレジットカードの不正利用対策②

(1) カード会社（イシューア）

■ EMV 3-Dセキュア導入及びリスクベース認証（※1）精度向上

- ・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及びリスクベース認証の精度向上を図る。

■ 自社カード会員のEMV 3-Dセキュア登録及び静的（固定）パスワード以外の認証方法への登録・移行

- ・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う。
- ・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、2025年3月末までに自社カード会員が「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。

（※1）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データを活用して本人の利用であるかどうかの認証を行う仕組み。

1.非対面取引におけるクレジットカードの不正利用対策③

(2) EC加盟店

■ EMV 3-Dセキュアの導入

● 全てのEC加盟店

- ・2025年3月末までにEMV 3-Dセキュアの導入を計画的に進める。
- ・カード会社（イシューア）におけるリスクベース認証の精度向上のため、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、カード会社（イシューア）に提供するデータ項目の設定等の体制を整える。

● 高リスク商材取扱加盟店

- ・2025年3月末までにEMV 3-Dセキュアの導入を計画的に進める。
- ・更なる不正対策強化が必要な場合には、アクワイアラーの要請に応じ、カード会社（イシューア）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。

● 不正顕在化加盟店

- ・既に不正利用が発生し被害が生じていることから、EMV 3-Dセキュアを早期に導入する。
- ・更なる不正対策強化が必要な場合には、アクワイアラーの要請に応じ、カード会社（イシューア）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。

1.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

(3) カード会社（アクワイアラー）及びPSP

■ EC加盟店におけるEMV 3-Dセキュア導入に向けたサポート

- ・2025年3月末までに、原則、全てのEC加盟店がEMV 3-Dセキュアの導入を計画的に進められるようサポートを行うなど必要な対策を講じる。
- ・不正顕在化加盟店に対して、早期にEMV 3-Dセキュアを導入するよう働きかける。
- ・カード会社（イシューアー）におけるリスクベース認証の精度向上のため、EC加盟店の取扱商材や不正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（イシューアー）により多く提供できるよう、提供する情報を適宜見直す等、EC加盟店におけるデータ項目の設定をサポートする。
- ・EMV 3-Dセキュアの安定稼働のための対応に継続的に取り組む。

1.非対面取引におけるクレジットカードの不正利用対策⑤

□3-Dセキュア1.0終了に伴う記載の変更

■ EC加盟店における非対面不正利用対策の具体的方策（4方策）

・「3-Dセキュア1.0」が2022年10月をもって取扱い終了となったことから、そのバージョンアップしたスキームである「EMV 3-Dセキュア」に表記を改めた。

方策		
1) 本人認証	a) 3-Dセキュア EMV 3-Dセキュア b) 認証アシスト	3) 属性・行動分析 (不正検知システム)
2) 券面認証(セキュリティコード)		4) 配送先情報

※3-Dセキュア1.0を導入していた「高リスク商材取扱加盟店」及び「不正顕在化加盟店」は、EMV 3-Dセキュアへの切り替え、または他の方策の実施がなされていないと、不正利用被害対策を講じていると認められないこととなる。

【参考】

●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

●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

1.非対面取引におけるクレジットカードの不正利用対策⑥

□不正利用拡大防止に向けた今後の取組について記載

■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

- 不正利用被害減少、クレジットカード取引の信頼性の確保の観点から、関係事業者が連携し、業界全体で取り組むことが重要。
- 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、関係事業者が協力して課題解決に向けて取り組み、適切な環境整備を行う必要がある。
- そのため、クレジットカード取引の安定性・信頼性を確保しつつ、不正利用被害の極小化に資するEMV 3-Dセキュアの実効的かつ現実的な運用方法の検討に各関係事業者の協調の下、取り組むこととする。
- また、不正発生状況やリスクに応じた多面的・重層的な不正対策への取組みとして、EMV 3-Dセキュア以外の他の不正対策も併せた実効的かつ現実的な対策の検討に取り組むこととする。

2. 消費者及び事業者等への周知・啓発

2. 消費者及び事業者等への周知・啓発

消費者への周知啓発（イシューア）

■ EMV 3-Dセキュアの登録および静的（固定）パスワード以外の認証方法への登録・移行

- ・自社カード会員における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カード会員への周知啓発を行う。

事業者等への周知啓発（アクワイアラー・PSP）

■（対加盟店）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

- ・2025年3月末までに、原則、全てのEC加盟店においてEMV 3-Dセキュアの導入が求められる旨、加盟店に対して周知する。

(参考1) 新規策定附属文書

今年度は、情報保護分野及び対面取引分野において、実務における必要性を考慮し、下記の附属文書を新規策定した。

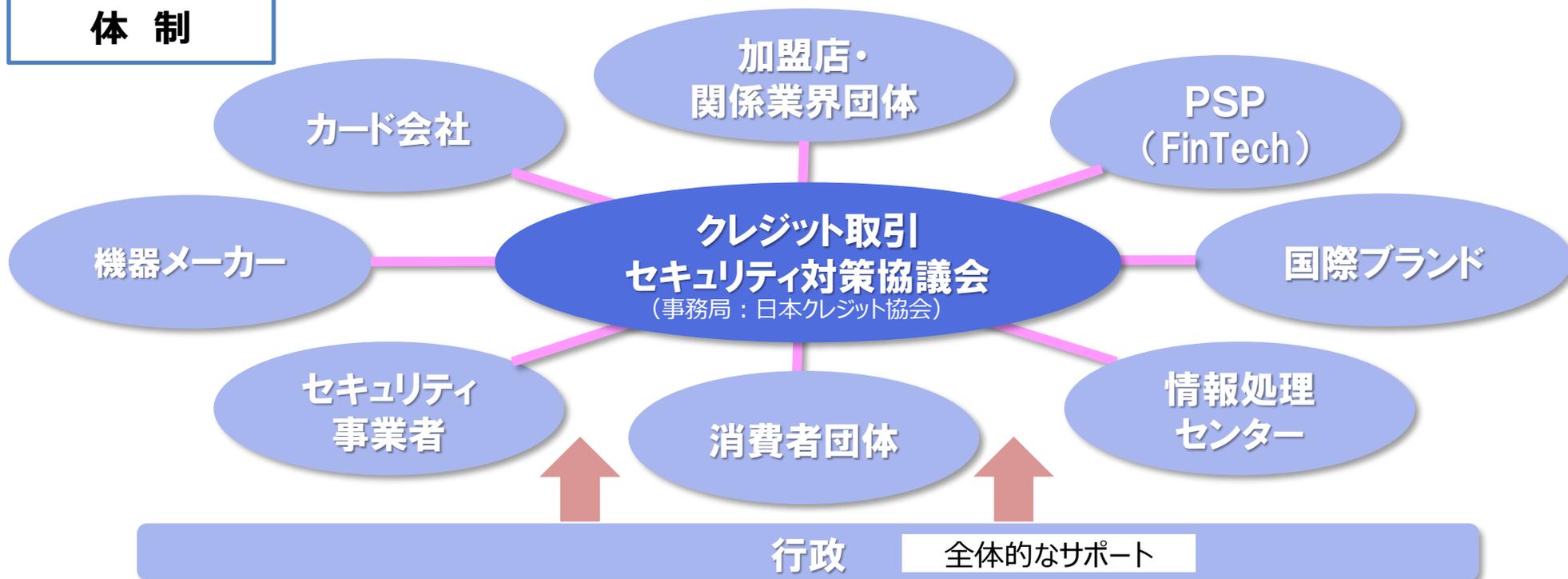
	附属文書名	概要
1	「クレジットカード売上票の作成・保管に関するガイドライン」【附属文書16】	「サイン」を取得しない加盟店の運用変更が円滑に進むことや運用の統一を目指し、クレジットカード取引における売上票の作成・保管に関しての運用を取りまとめたもの。
2	「スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策の技術要件について」【附属文書 17】	スマートフォンやタブレット等の汎用デバイスを用いた決済及び、スマホアプリ等のSDKを利用する決済について、「非保持化（非保持と同等/相当を含む）」の取組を推進するため、具体的な方策例について取りまとめたもの。

(参考2) クレジット取引セキュリティ対策協議会とは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り組む。

体制



(参考3) クレジット取引セキュリティ対策協議会とは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・早稲田大学名誉教授

【オブザーバー】

- (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

2023年3月14日時点

(参考4) 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な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（イシューア・アクワイアラー）」「決済代行業者等」「QR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。

(参考4) 本ガイドラインの基本的な考え方②

4. 対象となるクレジットカードについて

- 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て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。

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、周知活動に取り組む必要がある。