クレジットカード・セキュリティガイドライン【5.0版】
改訂ポイント

【2024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.構成の変更

- 関係事業者ごとに講じるべき具体的な対策等を記載

2.2025年3月末までの、原則、全てのEC加盟店のEMV 3-Dセキュアの導入に向けて

- イシュアーにおける目標設定やアクワイアラー・PSPにおけるEC加盟店への導入優先順位の考え方を記載

3.EC加盟店におけるカード情報保護対策及び不正利用対策

- カード情報保護対策
  EC加盟店における基本的セキュリティ対策の考え方を記載し、セキュリティ・チェックリストによる不断なセキュリティ対策の改善・強化を示した

- 不正利用対策
  決済前・決済時・決済後のそれぞれの場面ごとに対策を導入するという対策の全体像を示した

1.構成の変更

1.構成の変更

□関係事業者ごとに講じるべき具体的な対策等を記載

■必要なセキュリティ対策を自ら適切に講じられる内容とすることを目的に事業者別の構成に変更

・過去最多の不正利用被害額を更新している状況において、不正利用被害を減少させるためには、改めて、各関係事業者自らが適切なセキュリティ対策を不断に講じることが重要である。

・しかしながら、特にクレジットカードのEC等非対面決済においては様々な事業者が関係しており、割賦販売法やカードビジネスの実務に精通していない場合においても、自身がどの事業者に該当し、必要なセキュリティ対策を自ら適切に講じられるよう、理解しやすい内容に見直しを行った。

・従前の【4.0版】の内容を基に、対象事業者ごとに、対面取引と非対面取引別に、各事業者が講じるべきカード情報保護対策、不正利用対策、周知・啓発等に関して、対策を具体的に記載。

・なお、指針対策の実装方法や仕様については、ガイドライン本文に基本的な考え方や概要を記載。【4.0版】に記載の「POSのIC対応の具体的方法」、「IC取引時のオペレーションルール」、「非保持化の実現方法」、「非対面取引不正利用対策の4方策の内容」等、詳細な内容については関係する附属文書に移し、誘導する記載とするとともに、関係する附属文書がないものは新規に作成した。

2.2025年3月末までの、原則、全てのEC加盟店のEMV 3-Dセキュアの導入に向けて

□カード会社（イシュアー）

□加盟店（EC加盟店）

□カード会社（アクワイアラー）

□PSP

2.2025年3月末までの、原則、全てのEC加盟店のEMV 3-Dセキュアの導入に向けて

□カード会社（イシュアー）＜ガイドライン P20～21＞

■目標設定の考え方

・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図る

・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
➡ 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

・リスクベース認証の精度向上に継続的に取組む

・「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
➡ 2025年3月末時点でEMV 3-Dセキュア登録会員ベースで100%の移行率を目指す

2.2025年3月末までの、原則、全てのEC加盟店のEMV 3-Dセキュアの導入に向けて

□加盟店（EC加盟店）＜ガイドライン P34～35＞

■導入の考え方

・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

・「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

・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、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

2.2025年3月末までの、原則、全てのEC加盟店のEMV 3-Dセキュアの導入に向けて

□カード会社（アクワイアラー）＜ガイドライン P46＞

□PSP＜ガイドライン P50～51＞

■EC加盟店への導入優先順位の考え方

・**「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る

✓ 「不正顕在化加盟店」に対して、**<u>即時の導入着手</u>**を働きかける

✓それ以外の加盟店に対して、以下の優先順位を参考にEMV 3-Dセキュアの導入計画を策定し**<u>早期にEMV 3-Dセキュアの導入に着手</u>**するよう働きかける

【優先順位】

（1）「不正顕在化加盟店」ではないが不正が発生しているEC加盟店

（2）「高リスク商材取扱加盟店」

（3）上記以外の加盟店

✓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**<u>導入することを説明した上で契約</u>**する

3. EC加盟店におけるカード情報保護対策及び不正利用対策

□加盟店（EC加盟店）

□カード会社（アクワイアラー）

□PSP

3.EC加盟店におけるカード情報保護対策及び不正利用対策

□加盟店（EC加盟店） ＜ガイドライン P29、31＞

□アクワイアラー＜ガイドライン P45＞

□PSP ＜ガイドライン P49～50＞

■カード情報保護対策

✓セキュリティ・チェックリストによる不断なセキュリティ対策の改善・強化

・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やカード情報や会員のログインアカウント窃取を企図する者の最新の攻撃手口等の情報を踏まえ、常にセキュリティ対策を講じる必要がある。

・EC加盟店は、新規加盟店契約の申込み前に、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。

・アクワイアラーやPSPは、「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を行う。

3.EC加盟店におけるカード情報保護対策及び不正利用対策

□加盟店（EC加盟店）、カード会社（アクワイアラー）及びPSP ＜ガイドライン P57～58＞

■不正利用対策

✓決済の場面（決済前・決済時・決済後）を考慮した場面ごとの対策導入の運用の検討

・非対面不正利用対策として、4つの方策（①本人認証（EMV 3-Dセキュア、認証アシスト）、②券面認証（セキュリティコード）、③属性・行動分析、④配送先情報）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、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「線の考え方」である全体像を示した。

・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。

3.EC加盟店におけるカード情報保護対策及び不正利用対策

□加盟店（EC加盟店）、カード会社（アクワイアラー）及びPSP ＜ガイドライン P57～58＞

■不正利用対策

今後の不正利用対策の考え方(「線」の考え方)

（参考1）新規策定附属文書

今年度は、非対面取引分野（EC加盟店）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。

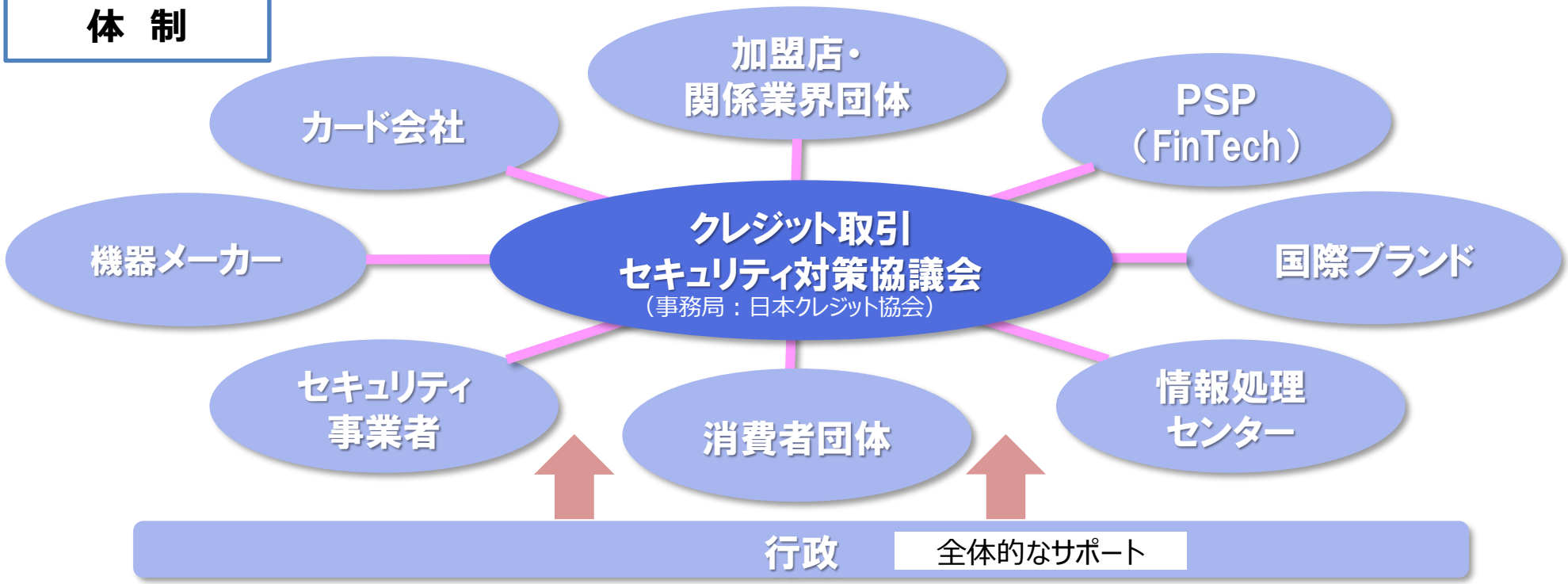
	附属文書名	概要
1	EC加盟店における非保持化対応ソリューションについて【附属文書18】	EC加盟店における「非保持化」の取組を推進するための実現方法等について取りまとめたもの。
2	属性・行動分析のポリシー文書【附属文書19】	「属性・行動分析（不正検知システム）」の導入検討及び導入済み加盟店の継続的な運用の見直し、サービス提供事業者と加盟店の間の体制整備等の方針を定めたもの。
3	EC加盟店における基本的なセキュリティ対策　導入ガイド【附属文書20】	EC加盟店やその他非対面取引加盟店においてセキュリティ意識の向上と講じるべき対策についての理解を深め、情報漏えい及び不正利用対策に資するよ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。
4	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。

（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）	イオンフィナンシャルサービス(株)、(株)オリエントコーポレーション、(株)クレディセゾン、(株)ジェーシービー、(株)ジャックス、トヨタファイナンス(株)、三井住友カード(株)、三菱UFJニコス(株)、ユーシーカード(株)、楽天カード(株)
（加盟店）	(株)ジャパネットホールディングス、(株)JTB、Ｊ.フロントリテイリング(株)、(株)三越伊勢丹ホールディングス、ユニー(株)、(株)ヨドバシカメラ、LINEヤフー(株)、楽天グループ(株)
（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(株)、オムロンソーシアルソリューションズ(株)
（情報処理センター）	(株)NTTデータ
（セキュリティ事業者）	Secure・Pro(株)、トレンドマイクロ(株)
（消費者団体）	（一社）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）

【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,Inc.、ビザ・ワールドワイド・ジャパン(株)、マスターカード・ジャパン(株)、三井住友トラストクラブ(株)[Diners Club] 、銀聯国際有限公司
（団体事務局）	日本チェーンストア協会、（公社）日本通信販売協会、（一社）日本百貨店協会
（官庁）	経済産業省

2024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

■ 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、対面取引と非対面取引別に、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

■ 「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。

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」「コード決済事業者等の委託先」「加盟店向け決済システム提供事業者」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」「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

■ 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。

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

■ 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。