クレジットカード・セキュリティガイドライン【6.0版】
改訂ポイント

【2025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）

主な改訂のポイント －指針対策の追加と変更－

1.EC加盟店におけるカード情報保護対策への指針対策の追加

- EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施

2.EC加盟店における不正利用対策への指針対策の追加

- EMV 3-Dセキュアの導入
- 適切な不正ログイン対策の実施

3.不正顕在化加盟店・高リスク商材取扱加盟店における指針対策の変更

- 不正顕在化加盟店における不正利用対策の指針対策の変更

4.MO・TO取引取扱加盟店における指針対策の変更

- MO・TO取引を取り扱う加盟店における不正利用対策の指針対策の変更

5.その他

- 指針対策の追加・変更に伴う関係事業者におけるEC加盟店へのサポート等について
- 対面取引加盟店における「サイン取得による本人確認」・「PINバイパスの廃止」について

1.EC加盟店におけるカード情報保護対策への指針対策の追加

● 指針対策追加の背景

- ✓ カード情報保護対策は、「カード情報を加盟店で保持しない対策（非保持化）」を中心とした対策にて短期間に大量のカード情報を窃取される事案については一定の効果があった
- ✓ しかしながら、上記の通りの効果があるものの、環境設定の不備等により、カード情報漏えい事案が発生
- ✓ 原因としては、EC加盟店のシステムやWebサイトのウイルス対策、管理者の権限の管理、デバイス管理等の「脆弱性対策」の不備により、外部からの不正アクセスやウイルス感染、システムの改ざん等により、カード情報等の窃取がされたものである

● 指針対策

□加盟店（EC加盟店） <ガイドラインP34～36>

現指針対策（継続）

✓ **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**

追加指針対策

■ **EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施**

1.EC加盟店におけるカード情報保護対策への指針対策の追加

（1）EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施

□加盟店（EC加盟店） ＜ガイドラインP34～36＞

①目的

✓ EC加盟店のシステム(※1)及びWebサイト(※2)におけるウイルス対策、管理者の権限の管理、デバイス管理等の脆弱性対策の不備を原因としたカード情報漏えいの防止

※1：Webサイト＊2のセキュリティ対策等を含め管理者権限を有するシステム
※2：商品・サービス・金額等を掲載し、消費者が閲覧するWebサイト

②具体的な対応内容

✓ 指針対策は、以下のすべての対策を講じる

導入する「脆弱性対策」
①システム管理画面のアクセス制限と管理者のID/パスワード管理
②データディレクトリの露見に伴う設定不備への対策
③Webアプリケーションの脆弱性対策
④マルウェア対策としてのウイルス対策ソフトの導入、運用
⑤悪質な有効性確認、クレジットマスターへの対策

➢ 詳細は、「EC加盟店におけるセキュリティ対策導入ガイド【附属文書20】（以下「セキュリティ対策導入ガイド【附属文書20】」という。）」の「別紙a_EC加盟店におけるセキュリティ対策一覧（以下「セキュリティ対策一覧」という）_「1.脆弱性対策」を参照

✓ ECシステムやWebサイトの構築・運用を外部委託する場合は、当該委託先に対して、EC加盟店が行うべき「脆弱性対策」を理解した上で構築・運用を行うことを求める

1.EC加盟店におけるカード情報保護対策への指針対策の追加

（1）EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施

□カード会社（アクワイアラー） ＜ガイドラインP50＞ **/** **□PSP** ＜ガイドラインP56＞

①具体的な対応内容

✓ EC加盟店における「脆弱性対策」の導入・運用サポートの実施

- カード会社（アクワイアラー）とPSPは連携し、EC加盟店における指針対策の実施について、必要な助言や情報提供、サポート等を行う。

  ➢「セキュリティ対策　導入ガイド【附属文書20】」_「セキュリティ対策一覧」_「1.脆弱性対策」を活用

□ECシステム提供会社等 ＜ガイドラインP62＞ **/** **□ソリューションベンダー** ＜ガイドラインP62＞

①具体的な対応内容

✓ EC加盟店へのシステム等の提供及びサポートの実施

- 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の各指針対策の内容を理解した上で、EC加盟店に対して「対策が具備されたECシステムの構築やソリューション・サービス等の提供」とその維持・管理等を行うとともに、対策に必要な助言や情報提供等を行う。

2.EC加盟店における不正利用対策への指針対策の追加

● 指針対策追加の背景

- ✓ 不正利用被害額は、2023年には541億円、内93%がEC加盟店における「なりすまし」の不正利用
- ✓ この不正利用は、クレジットマスターにより生成したカード番号やカード情報漏えい及びフィッシングにより窃取したカード情報、アカウント（ID）・パスワード、属性情報等を使用して、カード決済時のカード不正利用のほか、カード決済前の場面では不正なアカウント登録や本人になりすまして不正ログインをする手口により行われている
- ✓ また、不正利用被害額の上位加盟店においては、約7割が「ログイン」必須としていることから、不正ログイン防止のために「カード決済前」の対策が重要
- ✓ さらに、不正利用がされる「カード決済時」、商品の配送・転売がされる「カード決済後」の対策と共に「カード取引の流れ」に沿って、各場面を考慮した適切な対策導入が必要（「線の考え方」に基づく対策導入）
- ✓ 「線の考え方」に基づき、カード決済前の「不正ログイン対策の実施」とカード決済時の「EMV 3-Dセキュアの導入」を軸に適切な対策導入により不正利用被害防止の実効性を高める

［線の考え方の概念図］

2.EC加盟店における不正利用対策への指針対策の追加

● 指針対策

□加盟店（EC加盟店）　<ガイドラインP36～39>

現指針対策（継続）

- ✓ オーソリゼーション処理の体制整備
- ✓ 加盟店契約上の善良なる管理者の注意義務の履行

追加指針対策

- ■ EMV 3-Dセキュアの導入
- ■ 適切な不正ログイン対策の実施

2.EC加盟店における不正利用対策への指針対策の追加

（1）EMV 3-Dセキュアの導入

□加盟店（EC加盟店）　＜ガイドラインP38＞

①目的

✓ カード会社（イシュアー）による本人確認が適切に行われるための措置として、EMV 3-Dセキュアの導入

- 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「なりすまし」による不正利用のリスク判断を行うとともに、必要に応じて「動的（ワンタイム）パスワードの入力」等を要求することで当該取引における安全性を確保する。

②具体的な対応内容

✓ EMV 3-Dセキュアを導入した上で、原則として決済の都度、EMV 3-Dセキュアによる認証の実施

- EC加盟店がEMV 3-Dセキュア以外に講じる不正利用対策やその抑止効果を前提に、アカウント等へのカード番号の登録時にEMV 3-Dセキュアによる認証を行う運用や加盟店のリスク判断によりEMV 3-Dセキュアによる認証を行う運用も認められる。
  - ➢ 詳細は「EMV 3-Dセキュア導入ガイド【附属文書14】」を参照

✓ リスクベース認証（RBA）の精度向上

- カード会社（イシュアー）におけるリスクベース認証（RBA)の精度向上のため、自社の取扱商品や不正利用の被害状況等の実態を踏まえ、カード会社（イシュアー）に、より多くの情報提供（AReq設定項目※）や提供する情報を適宜見直せるよう、体制を整え情報提供することが求められる。

※AReq設定項目：EMV 3-Dセキュアの電文上に設定するカード会員を認証する為の利用者が決済に使用しているデバイス等の情報

2.EC加盟店における不正利用対策への指針対策の追加

（1）EMV 3-Dセキュアの導入

□カード会社（イシュアー）　<ガイドラインP23～24>

①具体的な対応内容

- ✓ 自社カード会員の「EMV 3-Dセキュアの導入」及び登録情報の最新化
  - 自社カード会員のEMV 3-Dセキュアの登録を行うと共に、EC加盟店における円滑な取引等がされるよう「動的（ワンタイム）パスワードの入力」等の周知・啓発及び携帯電話番号やメールアドレス等の登録情報が常に最新化されるよう対応を行う。
- ✓ リスクベース認証（RBA）の精度向上
  - 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常に行い、精度向上を継続的に行う。
- ✓ システムの安定稼働
  - EMV 3-Dセキュアの安定稼働のために関係事業者と連携し継続的に取り組む。

2.EC加盟店における不正利用対策への指針対策の追加

（1）EMV 3-Dセキュアの導入

□**カード会社（アクワイアラー）** <ガイドラインP51～52> / □**PSP** <ガイドラインP58>

①具体的な対応内容

✓導入・運用サポート

- カード会社（アクワイアラー）とPSPは連携し、EC加盟店が適切に導入及び運用をするためのサポートを行う。
  ➢「EMV 3-Dセキュア導入ガイド【附属文書14】」を参照

✓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（RBA)の精度向上のため、EC加盟店の取扱商品や不正利用発生状況等の実態を踏まえ、カード会社（イシュアー）に、より多くの情報提供や提供する情報の適宜見直すなど、EC加盟店のデータ項目（AReq設定項目）の設定等をサポートする。

✓システムの安定稼働

- EMV 3-Dセキュアの安定稼働のために関係事業者と連携し継続的に取り組む。

2.EC加盟店における不正利用対策への指針対策の追加

（2）適切な不正ログイン対策の実施

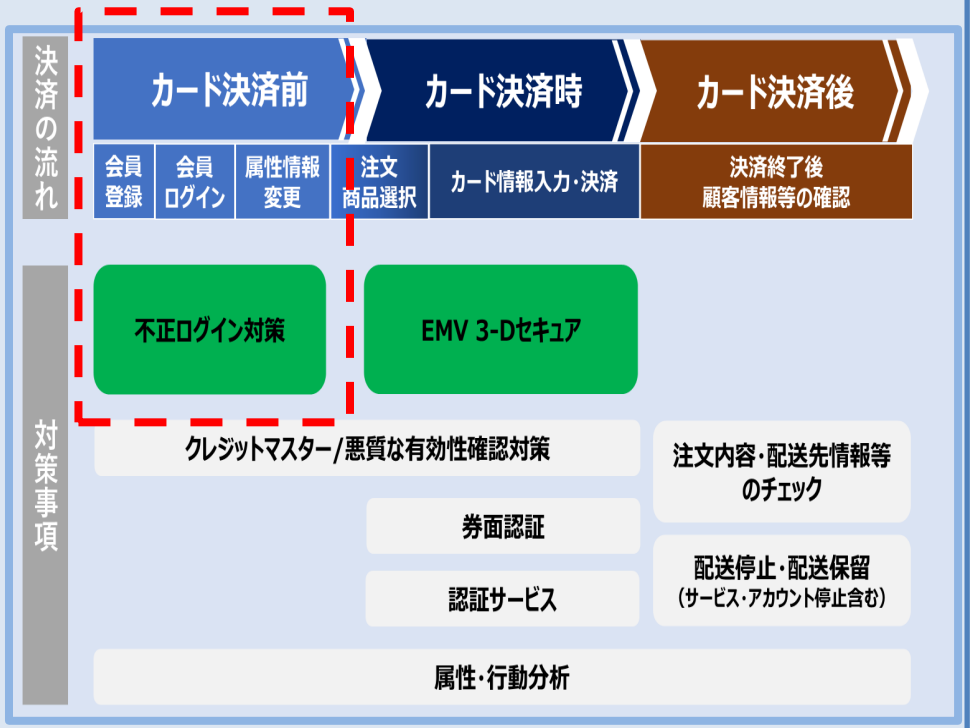
□加盟店（EC加盟店）　<ガイドラインP39～40>

①目的

✓ Webサイトへの「カード決済前」の各場面に応じた適切な対策の導入による不正ログインの防止

- 取扱商品やスキーム等により、不正利用の手口が異なることから、その手口による不正利用の発生リスクに応じて、「カード決済前」の「会員登録」「会員ログイン」「属性情報変更」のそれぞれの場面に応じた適切な対策を導入する。

対策が必要な場面	不正手口	不正内容
会員登録	不正アカウント作成	EC加盟店において、窃取した属性情報・カード情報等を利用し、不正なアカウントの登録を行う
会員ログイン・属性情報変更	アカウント乗っ取り	窃取した正規のアカウント等のログイン情報等を使用し、不正ログインを行う



2.EC加盟店における不正利用対策への指針対策の追加

（2）適切な不正ログイン対策の実施

□**加盟店（EC加盟店）**　<ガイドラインP39～41>

②具体的な対応内容

✓ カード決済前の「会員登録」「会員ログイン」「属性情報変更」の各場面を考慮した適切な対策を１つ以上導入

- EC加盟店の取扱商品・スキーム等から、「不正アカウント作成」「アカウント乗っ取り」の手口による不正利用リスクに応じて、カード決済前の「会員登録」「会員ログイン」「属性情報変更」のそれぞれの場面を考慮した適切な対策※1を１つ以上導入する。
- 効果的な対策導入の観点から、下表①～⑦の対策を優先的に導入を推奨。

※1：「セキュリティ対策導入ガイド【附属文書20】_「セキュリティ対策一覧」_3.不正ログイン対策（決済前の対策）」記載の対策

対策項目	対策が有効な場面　（○：有効対策）		
	会員登録	会員ログイン	属性情報変更
①不審なIP アドレスからのアクセス制限	○	○	○
②2段階認証又は多要素認証（2要素認証）による本人確認	—	○	○
③会員登録時の個人情報確認（氏名・住所・電話番号・メールアドレス等）	○	○	—
④ログイン試行回数の制限強化（アカウント/パスワードクラッキングの対応）、スロットリング	—	○	—
⑤会員ログイン時/属性情報変更時のメールやSMS 通知	—	○	○
⑥属性・行動分析	○	○	○
⑦デバイスフィンガープリント	○	○	○
⑧その他の対策（「EC加盟店におけるセキュリティ対策一覧_3. 不正ログイン対策（決済前の対策）」記載の対策）			

2.EC加盟店における不正利用対策への指針対策の追加

（2）適切な不正ログイン対策の実施

□**カード会社（アクワイアラー）**＜ガイドラインP52＞　**/**　□**PSP**　＜ガイドラインP58～59＞

①導入運用サポート

- ✓ カード会社（アクワイアラー）とPSPは連携し、EC加盟店が適切な対策導入及び運用を行うためのサポート
  - ➢「セキュリティ対策導入ガイド【附属文書20】」_「セキュリティ対策一覧」_3.不正ログイン対策（決済前の対策）」を活用

3.不正顕在化加盟店・高リスク商材取扱加盟店における指針対策の変更

● 指針対策変更の背景

✓ 加盟店の取扱商品、スキーム等により「不正アカウント作成」や「アカウント乗っ取り」等の手口が異なり、これまでの４方策では実効的な抑止効果が得られにくくなっていることから、不正顕在化加盟店は「線の考え方」に基づく不正利用対策を追加導入する指針対策に変更

✓ 高リスク商材取扱加盟店の指針対策は、4方策を見直し、他の商材と比べ不正利用の発生リスクが高い商材※1を「相対的にリスクの高い商材」としてリスクベースによる適切な対応※2に変更

※1：日本クレジット協会　インフラ整備部会調査 「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」
※2：「セキュリティ対策導入ガイド【附属文書20】_第３部 その他の留意事項_２．特定の商材における対策」参照

● 指針対策

□加盟店（EC加盟店）　<ガイドラインP39～40>

変更後の指針対策

■ 不正顕在化加盟店は、類似の不正利用の発生を防止するために、不正利用の発生状況等に応じて、本ガイドラインが掲げる不正利用対策から適切な対策の追加導入

参考：変更前指針対策（終了）

✓ 「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方策以上を導入

3.不正顕在化加盟店・高リスク商材取扱加盟店における指針対策の変更

（1）不正顕在化加盟店における不正利用対策の指針対策の変更

□加盟店（EC加盟店） <ガイドラインP39～40>

①目的

✓ 連続して不正利用被害が発生していることから、不正利用の発生状況から、その発生原因や手口に対応した適切な対策の導入等により、類似の不正利用の発生（再発）の防止

- 不正顕在化加盟店の定義は、これまでと同様、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」に該当する加盟店。

②具体的な対応内容

✓ 不正利用の被害状況や手口に応じた「適切な対策の追加導入」、若しくは「対策の強化」の実施

- 「適切な対策の追加導入」：「セキュリティ対策導入ガイド【附属文書20】」の「セキュリティ対策一覧」_4.不正利用対策（決済前・決済時・決済後）記載の対策から適切な対策を追加導入。
- 「対策の強化」：EMV 3-Dセキュアや属性・行動分析を導入している場合において、リスク判定や不正判定レベルの分析に基づき、リスク判定項目の追加・変更や不正判定レベルのチューニングによる精度向上。

□カード会社（アクワイアラー） <ガイドラインP52～53> / **□PSP** <ガイドラインP59～60>

①導入運用サポート

✓ カード会社（アクワイアラー）とPSPは連携し、不正顕在化加盟店が「適切な対策の追加導入」、若しくは「対策の強化」を行うためのサポートを行う

4.MO･TO取引取扱加盟店における指針対策の変更

（1）MO･TO取引を取り扱う加盟店における不正利用対策の指針対策の変更

●指針対策変更の背景

✓ EC取引併用の事業者も多く、MO･TO取引の取扱に関しては、４方策の指針対策を見直し、リスクベースによる適切な対策の導入に変更

● 指針対策

□加盟店（MO･TO取引取扱加盟店） ＜ガイドラインP43～45＞

変更後指針対策
✓ **オーソリゼーション処理の体制整備**
✓ **加盟店契約上の善良なる管理者の注意義務の履行**
✓ **リスクや被害状況に応じた非対面不正利用対策の導入**

参考：変更前指針対策
✓ オーソリゼーション処理の体制整備
✓ 加盟店契約上の善良なる管理者の注意義務の履行
✓ リスクや被害状況に応じた非対面不正利用対策の導入
✓ 「高リスク商材取扱加盟店」は、4つの方策のうち1方策以上、「不正顕在化加盟店」は2方策以上を導入

5.その他

（1）指針対策の追加・変更に伴う関係事業者おけるEC加盟店へのサポート等について

● 目的

✓ 関係事業者それぞれが、EC加盟店のカード情報保護対策・不正利用対策の内容を理解した上で、システムの構築・提供・維持・管理の実施やEC加盟店への必要な助言、情報提供等のサポートを行うことにより、EC加盟店のカード情報保護対策と不正利用の防止対策の適切な実施

●具体的な対応内容 ［再掲］

□カード会社（アクワイアラー） <ガイドラインP50～52> / **□PSP** <ガイドラインP56～59>

①加盟店サポート

✓ アクワイアラーとPSPは連携し、EC加盟店が講じるカード情報保護対策及び不正利用対策の指針対策を理解の上、加盟店に対し必要な助言や情報提供、サポート等の実施

➢「セキュリティ対策導入ガイド【附属文書20】」_「セキュリティ対策一覧」_3.不正ログイン対策（決済前の対策）」を活用

□ECシステム提供会社等 <ガイドラインP62> / **□ソリューションベンダー** <ガイドラインP62>

①加盟店へのシステム等の提供及びサポート

✓ 加盟店におけるカード情報保護対策及び不正利用対策の各指針対策の内容を理解した上で、加盟店に対して「対策が具備されたソリューション及びシステム構築等のサービスの提供とその維持・管理・運用等」を行うとともに、対策に必要な助言や情報提供等の実施

5.その他

（2）対面取引加盟店における「サイン取得による本人確認」・「PINバイパスの廃止」について

● 背景

- ✓ 対面取引おける本人確認方法は、紛失・盗難カードによる不正利用防止の為、「PINの入力」としている
- ✓ 既に各国際ブランドにおいても、「サインの取得」は、本人確認としての有効性が認められておらず、加盟店の業務上の必要性に応じて実施するもの（任意化）とされている
- ✓ このことより、2022年より、「カード取引において本人確認としてのサインの取得を行わない運用の推奨」及び「2025年4月以降、PINの入力が必要になる」旨の周知・啓発活動を開始
- ✓ また、PINバイパスについても、紛失・盗難カードによる不正利用の防止及びPIN失念時の救済措置としてのPINバイパス時の「サインの取得」も本人確認効果を有さないことから、2025年3月を対応期限としてPINバイパスを廃止することとし、2022年より、クレジット業界全体で周知・啓発活動を実施してきた

● 具体的な対応内容

□加盟店（対面加盟店）　<ガイドラインP31～32>

①サイン取得による本人確認

- ✓ 本人確認としての「サインの取得」を行わない運用とすることを推奨、本人確認として「PINの入力」が必要
  - ・ 加盟店のオペレーション上必要な場合に「サインの取得」を妨げるものではないが、本人確認として効果を有していないことに留意

②PINバイパスの廃止

- ✓ 「PINバイパスの廃止」は、加盟店における運用面での停止又は決済端末の当該機能の停止により対応

（参考1）附属文書の主な改訂

✓ 今年度は、指針対策に関連する附属文書等の統合・整備及び一部一般公開化を行った。

改訂有無	附属文書番号	別紙	文書名	該当指針対策						一般公開（○：JCA一般HP掲載）
				カード情報保護		不正利用対策				
				非保持化	脆弱性	IC化	EMV3DS	不正ﾛｸﾞｲﾝ	不正顕在化	
	附属文書1		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 1.4版	○						
	附属文書2		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 1.4版	○						
	附属文書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 初版	○						
	附属文書4		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 1.4版			○				
●	附属文書5		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 1.7版			○				
●	附属文書6		ICカード対応POSガイドライン（第Ⅰ部　取引処理編）1.0版			○				
●	附属文書7		ICカード対応POSガイドライン（第Ⅱ部　接続運用編）1.0版			○				
●	附属文書8		ICカード対応POSガイドライン（第Ⅲ部　非接触EMV Kernel処理）1.0版			○				
●	附属文書9		ICカード対応POS導入の手引き　～認定・試験プロセス概要～ 1.7版			○				
●	附属文書10		ブランドテスト要否一覧 1.7版			○				
●	附属文書11		ICカード対応POS導入の手引き　～全体概要編～ 1.0版			○				
	附属文書12		ICカード対応POS導入の手引き　～取引処理フロー解説編～ 1.7版			○				
✖	附属文書13		廃版（旧不正利用対策4方策の具体的な基準・考え方について（2024年改訂版））	4方策の終了により廃止（一部、附属文書20に統合）						

改訂有無　●：改訂あり　✕：廃止資料

（参考1）附属文書の主な改訂

改訂有無	附属文書番号	別紙	文書名	該当指針対策						一般公開（○：JCA一般HP掲載）
				カード情報保護		不正利用対策				
				非保持化	脆弱性	IC化	EMV3DS	不正ﾛｸﾞｲﾝ	不正顕在化	
●	附属文書14		EMV 3-Dセキュア導入ガイド 2.0版				○		○	○
●			【EMV 3-Dセキュア】統合版_AReq設定項目及び3RIの仕様・ユースケース（公表版）				○		○	○
●			EMV 3-Dセキュア導入ガイドに関するFAQ 2025年3月版				○		○	○
●	附属文書15		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 1.2版			○				○
●	附属文書16		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 1.1版			○				
	附属文書17		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について 2.0版		○			○	○	
	附属文書18		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 1.0版	○						
●	附属文書19		属性・行動分析ガイダンス 1.1版 （公開版は、附属文書20の文中に記載）				○	○	○	
●	附属文書20		EC加盟店におけるセキュリティ対策　導入ガイド 2.0版		○		○	○	○	○
●		別紙ａ	EC加盟店におけるセキュリティ対策一覧 1.0版		○		○	○	○	○
●		別紙ｂ	EC加盟店におけるセキュリティ対策　導入ガイド　補足資料		○			○		○
●		別紙ｃ	ECサイトのセキュリティ対策実施状況申告書（例）1.0版		○		○	○		○
✖	附属文書21		廃版（旧ｾｷｭﾘﾃｨ・ﾁｪｯｸﾘｽﾄ 第3版　附属文書20別紙ｂへ統合）	附属文書20別紙ｃに統合						

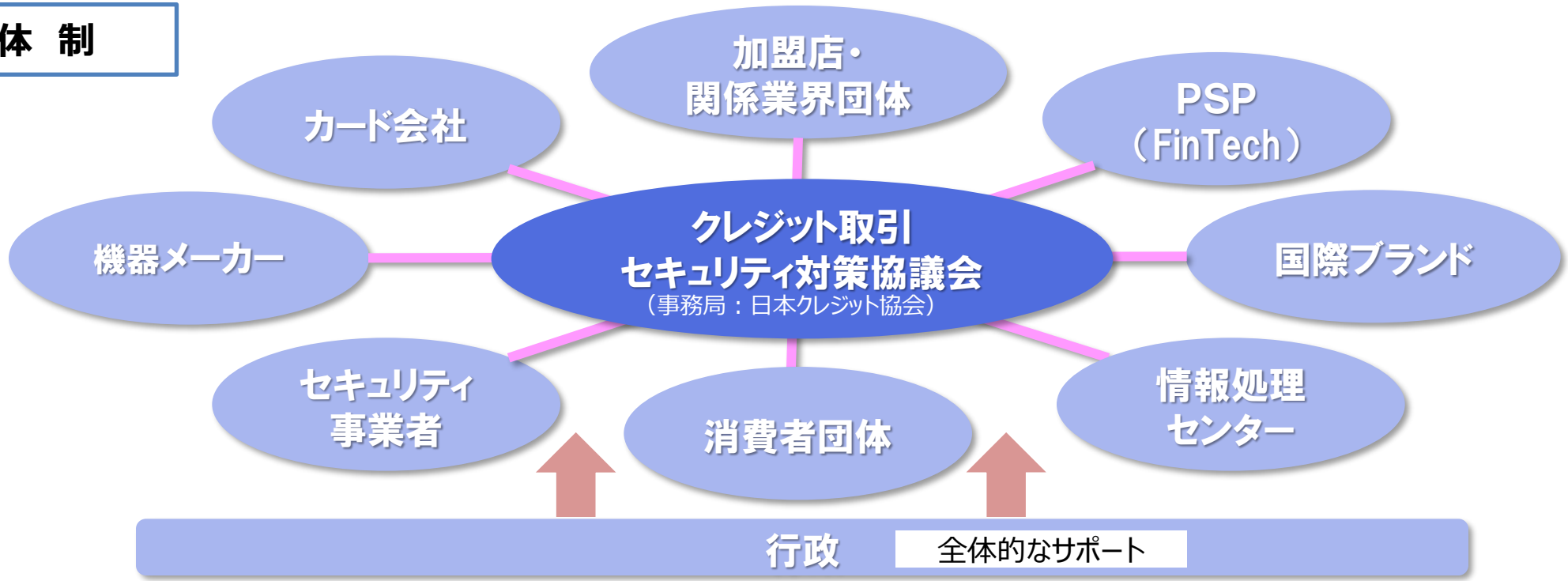
改訂有無　●：改訂あり　✕：廃止資料

（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2）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）	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

2025年３月４日現在

（参考3）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」が講じられているとみなされており、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】としてこれらの措置として記載している。

■ 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。

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3）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。