資料２

クレジットカード番号等不正利用対策の強化

令和４年10月11日

経済産業省　商務・サービスグループ

商取引監督課

目次

１．クレジットカード番号等の不正利用対策の全体像

クレジットカード番号セキュリティ対策の３つの方向性

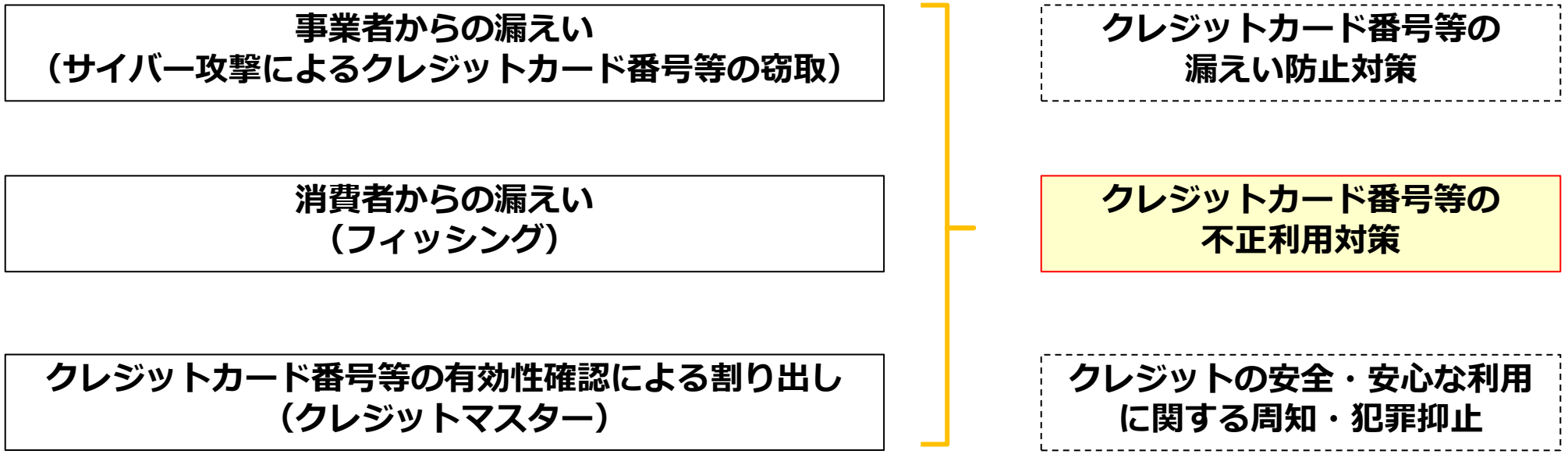
クレジットカード加盟店会社等　利用者　PSP等

目的意識	これまでの取組	今後の方向性
クレジットカード番号を安全に管理する（漏えい防止）		
▌クレジット決済に関与するプレイヤーは、クレジットカード番号を取り扱う上でシステム等の安全性を確保する	✓ 割賦販売法に基づく対応 （クレジットカード番号等の適切管理規定） － PCI DSS準拠相当 － 非保持化	✓ さらなる制度的措置の検討 －クレジットカード・セキュリティガイドラインでのアップデート ✓ 加盟店やPSP等のECサイト、システムの脆弱性対策の強化
クレジットカード番号を不正利用させない（不正利用防止）		
▌決済を承認する際には本人認証を行い、なりすましをさせない	✓ 割賦販売法に基づく対応 － 対面取引におけるIC決済の推進 － 非対面取引における本人認証の導入 （セキュリティコード・静的パスワード等における認証）	✓ 特に非対面取引における本人認証の原則化 ✓ 本人認証方法の高度化 生体認証・ワンタイムパスワード等といった強力な本人認証方法を推進 ⇒EMV-3Dセキュアの普及
▌決済取引をモニタリングし、不正利用を検知する	✓ クレジットカード会社等における個社での不正検知の取組 ✓ 明細、利用履歴の確認（クレジットカード会社等における明細通知・利用者における確認）	✓ 共同システムの構築・新しい技術や方法に基づく不正利用検知のイノベーション ✓ 明細による確認強化（リアルタイム通知等、利用者へのアラート機能の充実）
クレジットの安全・安心な利用に関する周知・犯罪の抑止		
▌利用者は、悪意を持った第三者からのフィッシング被害に遭わないよう対策を行う	✓ フィッシング対策協議会や日本クレジット協会等における周知啓発	✓ フィッシング対策に向けた多層的な取組（送信ドメイン認証（DMARC）等） ✓ 周知啓発の強化 ✓ 事業者と行政機関等における連携強化
▌漏えい防止・不正利用防止で行き届かない部分については、執行で対応	✓ 割賦販売法第49条の２（クレジットカード番号等の不正利用・取得）／不正アクセス禁止法等に基づく執行対応	✓ 経済産業省と警察庁（サイバー警察局等）との連携強化

（資料）クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）（第30回産構審割販小委（令和４年６月）

クレジットカード番号等の不正利用対策の位置づけ

- クレジットカード番号等の不正利用は、クレジットカード決済網の事業者からの漏えい、フィッシング、クレジットマスター等による手法が原因と考えられている。
- サイバー攻撃や利用者へのオンラインツールでの接触の増加、機械学習の進展により、どの手法も、従前より高度化してきていると考えられる。
- クレジットカード番号等の不正利用対策は、クレジットカード決済システムの信頼性確保だけでなく、社会犯罪に資金が流入することを抑止するもの。



クレジットカード番号等の不正利用防止義務について（概要）

- これまでの割賦販売法では、以下の改正により、クレジットカード番号等の不正利用防止について措置してきたところ。

1．加盟店のクレジットカード番号等の不正な利用の防止（法第35条の17の15）：平成28年改正

- **加盟店**は、クレジットカード番号等の**不正利用を防止**するために必要な措置を講じなければならない。

※改善命令はない。

2．加盟店の調査等（法第35条の17の8）：平成28年改正

- クレジットカード番号等取扱契約締結事業者は、**取扱契約の締結に先立つ加盟申込店に対する調査**である**加盟店調査**（悪質加盟店の排除、クレジットカード番号等の漏えい防止、不正利用の防止の措置状況）をし、調査結果等を踏まえ、**基準※に適合しない／適合しないおそれがある場合は契約を締結してはならない。**
- クレジットカード番号等取扱契約締結事業者は、**取扱契約を締結した加盟店に対する定期的または必要に応じた調査**である**加盟店調査**をし、調査結果等を踏まえ、**基準に適合しない／適合しないおそれがある場合は契約の解除又は必要な措置（指導、指導に従わない／基準への適合が見込まれない場合は契約の解除）**を講じなければならない。
- クレジットカード番号等取扱契約締結事業者は、加盟店調査を記録・保存しなければならない。

※基準：クレジットカード番号等の漏えい防止（施行規則132条・133条2項から６項）・不正利用防止措置（施行規則133条の14各号）

3．クレジットカード番号等の適切な管理（法第35条の16）：平成20年改正

- クレジットカード番号等取扱業者は、**クレジットカード番号等の漏えい防止措置等適切な管理のために必要な措置**※を講じなければならない。

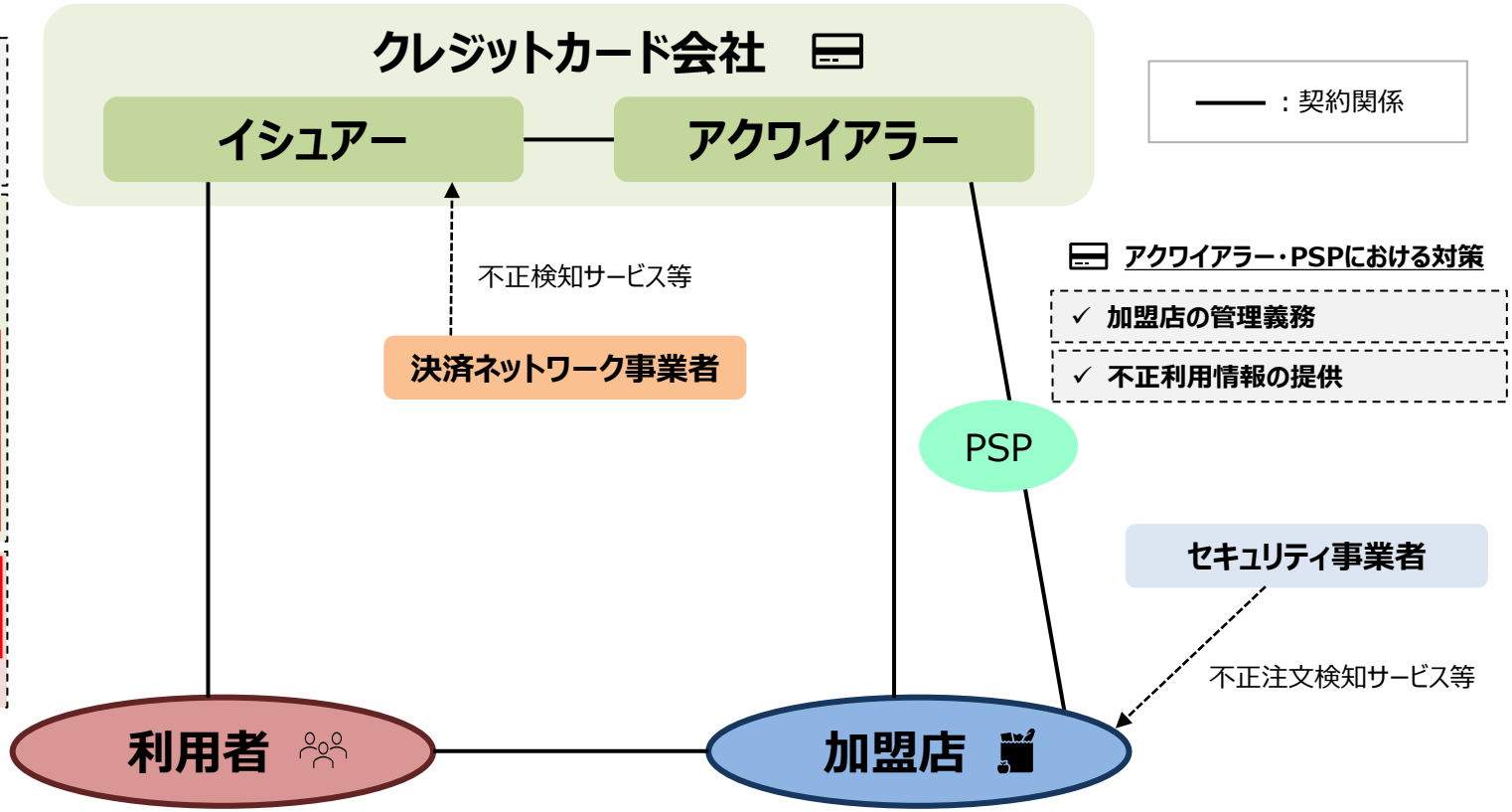
※措置：漏えい事故発生時または発生のおそれがあるときは、イシュアーは利用者以外の者による加盟店での購入（不正利用）を防止する措置を講ずること

4．クレジットカード番号等の不正取得（法第49条の２第２項）：平成20年改正

- 不正な手段（人への欺罔、不正アクセス等）によるクレジットカード番号等の取得行為の禁止。罰則の対象。

クレジットカード決済に関係するプレイヤーの不正利用防止対策の全体イメージ

- 各プレーヤーの連携の下、各種多面的・重層的な不正利用防止対策が実施されてきたところ。



イシュアーにおける対策

- ✓ **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する手法
- ✓ **本人認証**

  認証アシスト
  - 取引時の属性情報とイシュアーの登録属性情報を照合し本人を確認する手法

  3-Dセキュア
  - 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ともに、リスク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手法
  - EMV 3-Dセキュアを推奨
- ✓ **オンラインモニタリング（不正検知システム等）**
  - カードの利用状況を常時モニタリング
- ✓ **オーソリゼーション処理**

アクワイアラー・PSPにおける対策

- ✓ **加盟店の管理義務**
- ✓ **不正利用情報の提供**

利用者における対策

- ✓ **本人認証**

  3-Dセキュア（再掲）
- ✓ **利用明細・利用通知の確認**

加盟店における対策

- ✓ **券面認証（セキュリティコード）**（再掲）
- ✓ **配送先情報**
  - 不正配送先情報の蓄積等によって商品等の配送を事前に停止する手法
- ✓ **本人認証**

  認証アシスト、3-Dセキュア（再掲）
- ✓ **属性・行動分析**（不正検知システム）
  - 過去の取引情報、EC加盟店が収集した利用者のデバイス情報等に基づく取引のリスク評価によって不正取引を判定する手法（目検含む）
- ✓ **オーソリゼーション処理**（再掲）

※赤字はクレジットカード・セキュリティガイドラインにおけるいわゆる４方策
※赤枠は今後の重点強化項目

クレジットカード番号等の不正利用防止義務について（経緯）

- クレジットカード番号等の不正利用の防止は、利用者と対面している加盟店を対象とし、とりわけ偽造カードによる不正利用の根絶のため、店舗での決済端末「100%IC対応」の実現に向け、対面加盟店での不正利用防止に寄与。

過去の不正利用防止義務に係る法改正の背景

＜平成２０年改正＞

3．クレジットカード番号等の適切な管理（法第35条の16）

4．クレジットカード番号等の不正取得（法第49条の２第２項）

- クレジットカード会社等の従業員、退職者によるクレジットカード番号等の漏えい、不正取得が多発。

＜平成２８年改正＞

1．加盟店のクレジットカード番号等の不正な利用の防止（法第35条の17の15）

2．加盟店の調査等（法第35条の17の8）

- 偽造カードや本人になりすました不正利用被害の増加
- 加盟店でのクレジットカード端末のIC化対応
  ⇒2020年の東京オリンピック・パラリンピックに向けて、インバウンド需要の取り込み
- オフアス取引の増加による加盟店管理の限界

現在の非対面加盟店での不正利用防止義務について（具体的基準）

- 非対面取引での加盟店の不正利用防止は、①利用者によるものであるかの適切な確認等の②その他の不正利用を防止するために必要かつ適切な措置を講ずることとされ、不正利用リスクに応じた多面的・重層的な対策を求めている。

すべてのEC加盟店

・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
・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

・すべてのEC加盟店に求める事項
・４つの方策のうち1方策以上の導入

※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 EC 加盟店

不正顕在化加盟店

・すべてのEC加盟店に求める事項
・４つの方策のうち2方策以上の導入

※ カード会社（アクワイアラー）等が不正利用被害が多発している状況にあると認識するEC加盟店。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」に該当するもの。

＜４つの方策＞
・本人認証（3-Dセキュアまたは認証アシスト）
・券面認証（セキュリティコード）
・属性・行動分析（不正検知システム）
・配送先情報

（資料）クレジットカード・セキュリティガイドライン【3.0 版】（クレジットセキュリティ対策協議会）を元に事務局作成

（参考）現在の非対面加盟店における４つの方策

- 本人認証手法である旧3-Dセキュア(旧3DS)の導入をはかったが普及せず、他の３つの代替方策も併せて規定。

		取引の真正性の責任主体
①券面認証 （セキュリティコード）	● 個別決済の際に、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する手法	**イシュアー**
②本人認証	● **3-Dセキュア** ✓ 個別決済の際に、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ともに、リスク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手法 ✓ EMV 3-Dセキュア（EMV-3DS）を推奨	**イシュアー**
	● **認証アシスト** ✓ 個別決済の際に、取引時に入力された属性情報（氏名等）とカード会社（イシュアー）に事前に登録した属性情報（氏名等）を照合し、本人を確認する手法	**EC加盟店**
③属性・行動分析 （不正検知システム）	● 過去の取引情報、EC加盟店が収集した利用者のデバイス情報等に基づく取引のリスク評価によって、不正取引を判定する手法（目検での確認も含む広い概念）	**EC加盟店**
④配送先情報	● 個別決済後に、過去に不正利用された配送先情報の蓄積・照合によって、商品等の配送を事前に停止する手法	**EC加盟店**

（資料）クレジットカード・セキュリティガイドライン【3.0 版】（クレジットセキュリティ対策協議会）を元に事務局作成

（参考）３Dセキュアの普及に向けた業界・行政の取組

- 業界では、本人認証の普及に向けて、2000年代後半より、導入に向けたガイドラインを策定する等、旧3DSの導入を推進。かご落ちリスクが懸念され、普及に至らなかった。
- 平成28年割賦販売法改正で、 加盟店に対する不正利用防止措置の実施、アクワイアラー等による加盟店への不正利用防止措置の指導等を義務付け。

2007年　売上高上位100社に対して、旧3DSの導入を推進
　JCIA(日本クレジット産業協会、現JCA)：インターネット商取引におけるクレジットカード決済に係る本人確認強化によるなりすまし防止対策のための行動計画
2010年　新規加盟店の旧3DS導入のガイドライン策定
　JCA(日本クレジット協会)とJCCA(日本クレジットカード協会)：新規ｲﾝﾀｰﾈｯﾄ加盟店･･･新規インターネット加盟店におけるクレジットカード決済に係る本人認証導入による不正使用防止のためのガイドライン(※１)
2012年　加盟店に旧3DS、その他の効力のある認証方式を求めるガイドラインの策定
　JCA：インターネット上での取引時における本人なりすましによる不正使用防止のためのガイドライン（※２）
2016年　不正使用対策の方策として、旧3DSの効果と課題。**EMV-3DS**の情報収集と早期導入を検討
　クレジット取引セキュリティ対策協議会：実行計画２０１６(※３)

2016年　**割賦販売法**を**改正**し、**加盟店の不正利用防止措置** (旧3DSも対策の選択肢)、
　アクワイアラー等による加盟店への不正利用防止措置の指導等を義務化
2017年　2016年10月の**EMV-3DS**の仕様公開及び情報収集と導入への課題・必要な対応を検討
　クレジット取引セキュリティ対策協議会：実行計画２０１７（※３）
2021年　イシュアーへ**EMV-3DSの早期導入**、アクワイアラー等へ**EMV-3DS**の導入体制の早急な整備と**加盟店への導入の推進**を要請
　クレジット取引セキュリティ対策協議会：ガイドライン２．０版（※３）
2022年　PSPへEMV-3DS等の**導入の推進**、イシュアーへ**ワンタイムパスワードへの移行**等を要望
　クレジット取引セキュリティ対策協議会：ガイドライン３．０版（※３）
　EMV-3DSの新規導入及び旧3DSからの移行する事業者向けの共通**導入ガイドラインを策定**
　クレジット取引セキュリティ対策協議会：ＥＭＶ ３-Ｄセキュア導入ガイド（※３）

（資料）　※１　日本クレジット協会：「新規インターネット加盟店におけるクレジットカード決済に係る 本人認証導入による不正使用防止のためのガイドライン」の制定について
　https://www.j-credit.or.jp/download/101215_news.pdf
※２　日本クレジット協会：「インターネット上での取引時における本人なりすましによる不正使用防止のためのガイドライン」の制定について
　https://www.j-credit.or.jp/download/120402_news.pdf
※３　日本クレジット協会：クレジット取引セキュリティ対策協議会資料 https://www.j-credit.or.jp/security/document/index.html

（参考）加盟店のクレジットカード番号等の不正な利用の防止（法体系）

1．加盟店のクレジットカード番号等の不正な利用の防止：平成28年改正

＜法第３５条の１７の１５＞

・クレジットカード等購入あつせん関係販売業者又はクレジットカード等購入あつせん関係役務提供事業者は、経済産業省令で定める基準に従い、利用者によるクレジットカード番号等の**不正な利用を防止するために必要な措置を講じなければならない。**

＜施行規則第１３３条の１４＞

・法第３５条の１７の１５の経済産業省令で定める基準は、次のとおりとする。

一　クレジットカード番号等の通知を受けたとき、**当該通知がクレジットカード等購入あつせん業者から当該クレジットカード番号等の交付又は付与を受けた利用者によるものであるかの適切な確認その他の不正利用を防止するために必要かつ適切な措置を講ずる**こと。

二　加盟店において不正利用されたときは、**その発生状況を踏まえ、類似の不正利用を防止するために必要な措置を講ずる**こと。

＜監督指針＞

加盟店におけるクレジットカード番号等の適切な管理等

　加盟店は、以下の点に留意してクレジットカード番号等の適切な管理及び不正利用を防止するための措置を講じなければならない。なお、マンスリークリア専用のクレジットカード番号等も本項目の対象となることに留意すること。

（２）ガイドラインの対象となるクレジットカード番号等については、**ガイドラインに掲げられた不正利用の防止措置又はそれと同等以上の措置を講じている**こと。ガイドラインの対象ではないクレジットカード番号等については、不正利用のリスク等に応じた必要かつ適切な不正利用の防止措置を講じていること。

（３）クレジットカード番号等の管理者を限定する等、自社の役職員によるクレジットカード番号等の不正な取扱いを防止するための措置を講じていること。

＜クレジットカード・セキュリティガイドライン＞

■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つの方策のうち 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。

（参考）加盟店の調査等（法体系）

2．加盟店の調査等（法第35条の17の8）：平成28年改正

- クレジットカード番号等取扱契約締結事業者は、**（１）取扱契約の締結に先立つ加盟申込店に対する調査**である**加盟店調査**（悪質加盟店の排除、クレジットカード番号等の漏えい防止、不正利用の防止の措置状況）をし、調査結果等を踏まえ、**基準※に適合しない／適合しないおそれがある場合は契約を締結してはならない。**　※基準：クレジットカード番号等の漏えい防止（施行規則132条・133条2項から６項）・不正利用防止措置（施行規則133条の14各号）
- クレジットカード番号等取扱契約締結事業者は、**取扱契約を締結した加盟店に対する（２）定期的または（３）必要に応じた調査**である**加盟店調査**をし、調査結果等を踏まえ、**基準に適合しない／適合しないおそれがある場合は契約の解除又は必要な措置（指導、指導に従わない／基準への適合が見込まれない場合は契約の解除）**を講じなければならない。
- クレジットカード番号等取扱契約締結事業者は、加盟店調査を記録・保存しなければならない。

＜施行規則第１３３条の５～第１３３条の９＞

■（１）初期調査（省令第１３３条の５第３号、第１３３条の６第４項）

クレジットカード番号等取扱契約締結事業者は、加盟申込店が講じようとするクレジットカード番号等の適切な管理のための措置等について、省令第１３２条において求められている基準に適合しているかを調査しなければならない。

■（２）定期調査（省令第１３３条の７、第１３３条の５第３号）

クレジットカード番号等取扱契約締結事業者は、加盟店におけるクレジットカード番号等の適切な管理のための措置や加盟店における漏えい等の事故の発生状況を含むクレジットカード番号等の適切な管理等を図るために必要かつ適切な事項について、**適切な頻度※で定期的に調査しなければならない。**

※加盟店において行われる取引の種類、漏えい等の事故、**不正利用**、利用者からの苦情の発生状況**に応じたリスク判断に基づき実施頻度**を定める。

■（３）随時調査（加盟店における不正利用防止措置に支障がある場合の調査）（施行規則第１３３条の８第５号）

イシュアーからの連絡その他の方法によって知った事項に基づき、加盟店における不正利用の発生状況その他の事情からみて、**当該加盟店による不正利用の防止に支障を生じ、又は生ずるおそれがあると認められる場合、以下の事項を調査しなければならない。**

①当該不正利用の内容

②加盟店が当該不正利用の防止を図るために講ずる省令第133条の14第１号の規定による措置（本人によるカード利用であるかの適切な確認等）の実施状況

③省令第133条の9第1号及び第3号に掲げる措置（省令第133条の14第1号に規定する基準に適合した本人によるカード利用であるかの適切な確認等の不正利用防止措置及び類似の不正利用の発生防止のために必要な措置を講じるよう指導すること）を適切に講ずるために必要な事項

■加盟店調査の結果に基づく必要な措置（施行規則第１３３条の９）

クレジットカード番号等取扱契約締結事業者は次に掲げる措置を講じなければならない。

・加盟店において不正利用の発生が多発等しているときは、類似の不正利用の再発防止のために必要な措置を講じるように指導。

・加盟店が**上記の指導に従わない又は法定の基準を満たすことが見込まれないときは、当該加盟店とのクレジットカード番号等取扱契約を解除。**

（参考）加盟店の調査等（法体系）

2．加盟店調査等の義務（法第35条の17の8）：平成28年改正

＜監督指針＞

１．加盟店調査及び措置に係る社内体制の整備

（１）加盟店の調査及び措置に関する**責任部署を社内規則等に明確に定めている**こと。また、加盟店調査の調査事項に応じた適切な調査方法（省令第１３３条の６第１項ただし書きに基づく調査の省略等及び代替を含む。）及び措置の方法を社内規則等に定め、日常業務の運営において実践していること。

（２）**加盟店が講じるべき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基準を明確に定め、これに基づき加盟店の措置の実施状況等を確認する体制**となっていること。この際、**加盟店がガイドラインの対象となるクレジットカード番号等を取り扱う場合には、ガイドラインに掲げられた措置又はそれと同等以上の措置を当該基準**としていること。

（３）購入者等からクレジットカード等購入あっせん業者に申出のあった加盟店に対する苦情を当該クレジットカード等購入あっせん業者から受ける体制を整備していること。

（４）購入者等からの苦情について、苦情の内容及び重要性に則した合理的な苦情の類型化の基準を社内規則等に定め、類型化した苦情を加盟店調査の担当部署や加盟店営業部署等の関係部署との間で共有するとともに、重要案件については、経営陣に対して報告をしていること。

（５）**加盟店契約件数に応じ、加盟店管理を適切に行うことができるシステムや組織等の体制を整備**していること。

（６）加盟店の苦情、**漏えい等の事故又は不正利用**の発生状況を踏まえ、**加盟店情報交換制度に登録された情報又はそれと同等の情報を必要に応じて確認する体制を整備している**こと。また、それらの情報を必要に応じて、加盟店調査、苦情処理及び営業等の関係部署への共有を行う体制を整備していること。

（参考）加盟店調査等の義務について（法体系）

２．加盟店の調査等（法第35条の17の8）：平成28年改正

＜監督指針＞

２．加盟店調査及び措置

（１）加盟店契約の締結に先立って行う調査（以下「初期調査」という。）について、加盟店の属性、取引の種類等の基本的な事項（以下「基本的事項」という。）及び商品、権利又は役務に関する事項（以下「取扱商材」という。）の調査の結果等からみて、省令第１３３条の６第１項第１号に基づき調査の一部を省略等する場合、あらかじめその基準及び当該基準を満たした場合に実施する調査方法（省略を含む。）を定め、当該方法により実施していること。

（２）省令第１３３条の６第１項第２号に基づき、同条第７項に基づく調査の代替調査を行う場合、あらかじめ当該代替調査の方法を定め、当該方法により実施していること。

（３）初期調査の結果、加盟店契約を締結しない場合の基準を社内規則等に定め、当該基準を踏まえて加盟店契約を締結していること。

（４）加盟店契約締結後の定期的な調査(以下「定期調査」という。)のうち、省令第１３３条の７第２項に定める調査については、当該調査の前、最後に実施した定期調査等により確認した当該加盟店が実施する措置の基準の適合状況等を踏まえ**実施頻度を定めて運用**していること。

（５）定期調査のうち、省令第１３３条の７第３項に定める調査については、自社で把握する加盟店に対する購入者等の利益の保護に欠ける行為に係る苦情の発生状況を踏まえ、実施頻度及び調査方法を定めて運用していること。

（６）定期調査のうち、省令第１３３条の７第４項に定める調査については**、自社で把握する加盟店の漏えい等の事故又は不正利用の発生状況に鑑み、漏えい等の事故又は不正利用の防止措置の実施状況、取引の種類及び取扱商材に関する情報等を踏まえた危険性の程度を判断し、実施頻度及び調査方法を定めて運用**していること。

（７）割販法第３５条の１７の８第３項に基づいて必要に応じて行う調査（以下「随時調査」という。）のうち、省令第１３３条の８第１号に定める事項の調査については、基本的事項又は取扱商材に変更があった場合に加盟店がクレジットカード番号等取扱契約締結事業者に報告する旨を加盟店契約に規定する方法その他の適切な方法により、基本的事項又は取扱商材の変更を把握するための措置を講じていること。

（８）随時調査のうち、**省令第１３３条の８第２号から第６号までに定める事項の調査については、調査を実施する基準を定め、当該基準に応じて実施**していること。

（９）定期調査及び随時調査の結果等を踏まえ、加盟店に対して講ずる指導等の措置の実施基準、措置の内容及び手法を定め、運用していること。また、加盟店契約の解除に関して、その実施要件を定めていること。

なお、**定期調査及び随時調査等により、加盟店がガイドラインの対象となるクレジットカード番号等について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ないことを確認した場合には、合理的な期間内に当該措置の実施を指導し、当該指導に従った措置が実施されているかについて確認**すること。

（１０）加盟店調査の記録事項、保存方法、保存期間等の必要事項を明確に定め、日常業務において実践していること。

（１１）認定割賦販売協会会員については、自主規制規則に基づき加盟店情報交換制度へ情報を適切に登録していること。

（参考）クレジットカード番号等の適切管理義務について（法体系）

3．クレジットカード番号等の適切な管理（法第35条の16）：平成20年改正

＜法第35条の16第１項＞

- **クレジットカード番号等取扱業者**（次の各号のいずれかに該当する者をいう。以下同じ。）は、**経済産業省令で定める基準**に従い、**その取り扱うクレジットカード番号等**（包括信用購入あつせん業者又は二月払購入あつせんを業とする者（以下「クレジットカード等購入あつせん業者」という。）が、その業務上利用者に付与する第二条第三項第一号の番号、記号その他の符号をいう。以下同じ。）**の漏えい、滅失又は毀損の防止その他のクレジットカード番号等の適切な管理のために必要な措置を講じなければならない。**

※なお、**クレジットカード番号等の取扱いを委託した場合には、委託者**に対し、クレジットカード番号等の適切な管理のために**必要な指導その他の措置**を講ずることも求められている（同条第３項）。

＜施行規則第132条＞

・法第三十五条の十六第一項の経済産業省令で定める基準は、次のとおりとする。

一・二　（略）

三　クレジットカード番号等取扱業者又はクレジットカード番号等取扱受託業者において漏えい等の事故が発生し、又は発生したおそれがあるときは、当該事故に係るクレジットカード番号等を利用者に付与した**クレジットカード等購入あつせん業者は当該利用者以外の者が当該クレジットカード番号等を通知して特定の販売業者から商品若しくは権利を購入し、又は特定の役務提供事業者から役務の提供を受けることを防止するために必要な措置を講ずる**こと。【事故によるイシュアーの不正利用防止】⇒不正利用のモニタリングの強化、リスク状況に応じた措置（カード交換等）

（参考）クレジットカード番号等の不正取得（法体系）

４．クレジットカード番号等の不正取得（法第49条の２）：平成20年改正

＜法第49条の２＞

・クレジットカード番号等取扱業者若しくはクレジットカード番号等取扱受託業者又はこれらの役員若しくは職員若しくはこれらの職にあつた者が、その業務に関して知り得たクレジットカード番号等を自己若しくは第三者の不正な利益を図る目的で、提供し、又は盗用したときは、三年以下の懲役又は五十万円以下の罰金に処する。

２　人を欺いてクレジットカード番号等を提供させた者も、前項と同様とする。クレジットカード番号等を次の各号のいずれかに掲げる方法で取得した者も、同様とする。

一　クレジットカード番号等が記載され、又は記録された人の管理に係る書面又は記録媒体の記載又は記録について、その承諾を得ずにその複製を作成すること。

二　不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。）を行うこと。

３　正当な理由がないのに、有償で、クレジットカード番号等を提供し、又はその提供を受けた者も、第一項と同様とする。正当な理由がないのに、有償で提供する目的で、クレジットカード番号等を保管した者も、同様とする。

４　前三項の規定は、刑法その他の罰則の適用を妨げない。

２．クレジットカード決済システムの不正利用対策

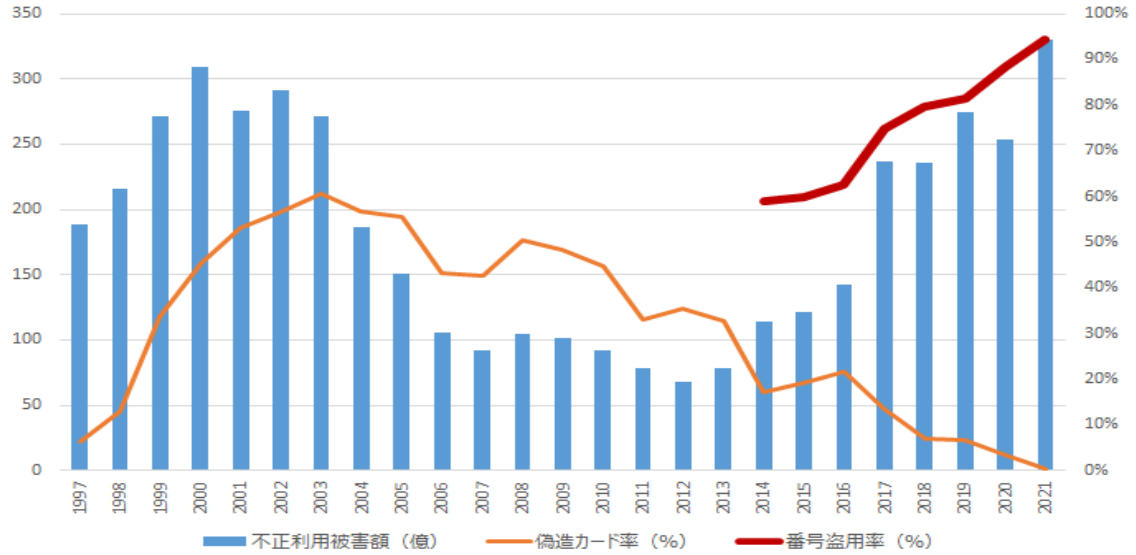
非対面取引における不正利用被害の実態（サイバー上でのなりすまし）

- 昨今の不正利用被害の実態は、非対面取引がほとんど。実態として、セキュリティコードによる券面認証での対策をしているEC加盟店も多くなったが、ECサイト上ではクレジットカード番号とともに漏えいすることにより、不正利用を防ぐことが限界となりつつある。

  ※クレジットカード番号等に紐付くEC加盟店のアカウントの乗っ取り（なりすまし）による不正利用も生じている。

- 特に、換金性があり転売されやすい商品や配送を伴わない商品は、不正利用の標的となりやすい。その時々の人気商品により、不正利用される商品も変化。昨今では、人気のスポーツブランドの衣料品の不正利用が増加傾向。また、価格帯として低価格な商品での不正利用も増えている。

不正利用被害額の推移（1997年～2021年）



（資料）日本クレジット協会
「クレジットカード不正利用被害額の発生状況」を基に作成

（１）利用者の適切な確認による対策

非対面取引における不正利用防止対策の課題①（非対面取引）

- これまで、クレジットカード決済の不正利用対策は、**取引の真正性**を確認するため、真正な利用者が真正なクレジットカードを保持していることを前提に、個別決済時に、真正なクレジットカードの保持を証明するものを示すことが中心となっていた。
- しかしながら、クレジットカード番号等の漏えい等により、セキュリティコードなどのクレジットカードの券面情報や固定パスワードがインターネット上で流通し得る現在、非対面取引では、容易に利用者のなりすましが可能。
- **非対面取引において、**法の求める**「利用者であるかの適切な確認」の実施**を原則求める必要があるのではないか。

●加盟店の不正利用防止措置の基準＜施行規則第１３３条の１４＞
一　クレジットカード番号等の通知を受けたとき、**当該通知がクレジットカード等購入あつせん業者から当該クレジットカード番号等の交付又は付与を受けた利用者によるものであるかの適切な確認その他の不正利用を防止するために必要かつ適切な措置を講ずる**こと。

利用者であるかの適切な確認の原則化

※以下、現状のガイドラインですべての加盟店に最低限求められる対応

	①利用者であるかの適切な確認	②その他必要な防止措置
対面取引	IC化対応 ー確認できるための端末設備の設置 ーPIN入力	ー
非対面取引	ー	・オーソリゼーション処理のための体制整備 ・善管注意義務

非対面取引における不正利用防止対策の課題②（対象となるEC加盟店の範囲）

- 割賦販売法のセキュリティ上の実務指針であるガイドラインでは、リスクの高いEC加盟店に対しては任意で求めていたものの、すべてのEC加盟店に対しては、オーソリゼーション処理（各イシュアーによる有効性確認）を基本の方策として求めているものの、「利用者の適切な確認」に該当する対策は必須とはなってはいない。
- EC取引の決済時に「利用者の適切な確認」が必ずしも行われていない状況は、クレジットカード決済システムの信頼性を毀損するものであるとともに、犯罪組織への資金供与につながるものであることから、国の制度として一定の対策を求めるべきではないか。
- なお、国際ブランドのルールでは、EMV-3DSによる利用者の確認が推奨されている。

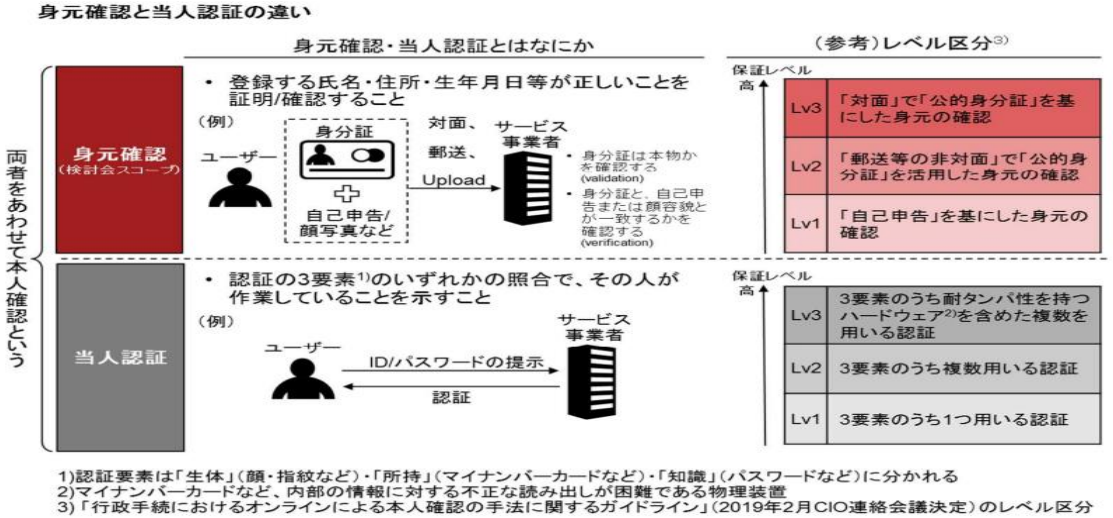
	これまでの対策の課題
すべてのEC加盟店	○オーソリゼーションの体制整備以外対応していないEC加盟店の許容 ○各イシュアーによるオーソリゼーション処理依存の不十分性 ーオーソリゼーションは、各イシュアーによる有効性の確認であり、不正検知に特化したものではないため、単体での方策としては不十分
高リスク商材取扱加盟店	○高リスク商材の指定の限界
不正顕在化加盟店	○４方策のうち１つまたは２方策の追加を選べる任意性 ーセキュリティコード、固定PWの漏えいによる方策の有効性の限界。 ー属性・行動分析でのレベルのばらつき。 ー任意の選択により、利用者の本人認証の方策は選択されない場合も。

「利用者であるかの適切な確認」等の防止措置①（基本的な対策）

- 非対面取引における不正利用防止措置として、「利用者であるかの適切な確認」の手法については検討が必要。非対面では利用者を間接的にしか把握できないため、知識・所有・生体の要素を組み合わせた本人の「認証」が基本と考えられる。
- 併せて、加盟店・カード会社の保有する顧客の属性情報の活用による不正判定技術の向上により、これらの取組で不正利用を防ぐことも有効。
- EMV-3DS（**個別決済及びアカウント登録時に**、取引の不正利用のリスクに応じて、**利用者本人のみが知るワンタイムパスワード・生体認証を通じて**、イシュアーに通知されたクレジットカード番号等の真正性を確認できる場合）は、これらの機能を含む手法であり、現時点におけるEC加盟店の基本的な不正利用対策として、すべてのEC加盟店でEMV-3DSによる「利用者であるかの適切な確認」を実施するべきではないか。

「認証」の一般的な構成要素
知識（記憶）、所有、生体の３要素。
（NIST（米国国立標準技術研究所）、デジタル行政手続ガイドライン）

<当人認証>
ある行為の「実行主体」と、当該主体が主張する「身元識別情報」との同一性を検証することによって、「実行主体」が身元識別情報にあらかじめ関連付けられた人物（あるいは装置）であることの信用を確立するプロセスのこと。認証情報の確認方法により、以下の二つに大別する。
(1) 単要素認証
単一の認証情報によって、利用者本人であることを確認する当人認証方法。
※例えば、ID と紐付けて、パスワード（≒本人だけが記憶している情報）、所有物、指紋、虹彩といった生体情報等のいずれかを用いる方法がある。
(2) 多要素認証
記憶、所有物、生体情報の各要素のうち、複数の認証情報を組み合わせることで、利用者本人であることを確認する当人認証方法。
※例えば、パスワード（≒本人だけが記憶している情報）とワンタイムパスワード（ワンタイムパスワードを発行できるスマートフォンを所有していることを確認する。）を組み合わせる方法がある。



（出典）行政手続におけるオンラインによる本人確認の手法に関するガイドライン（2019年２月）
（資料）オンラインサービスにおける身元確認手法の整理に関する検討報告書（経済産業省・令和２年４月）

「利用者であるかの適切な確認」等の防止措置②（アカウントの紐付けの場合）

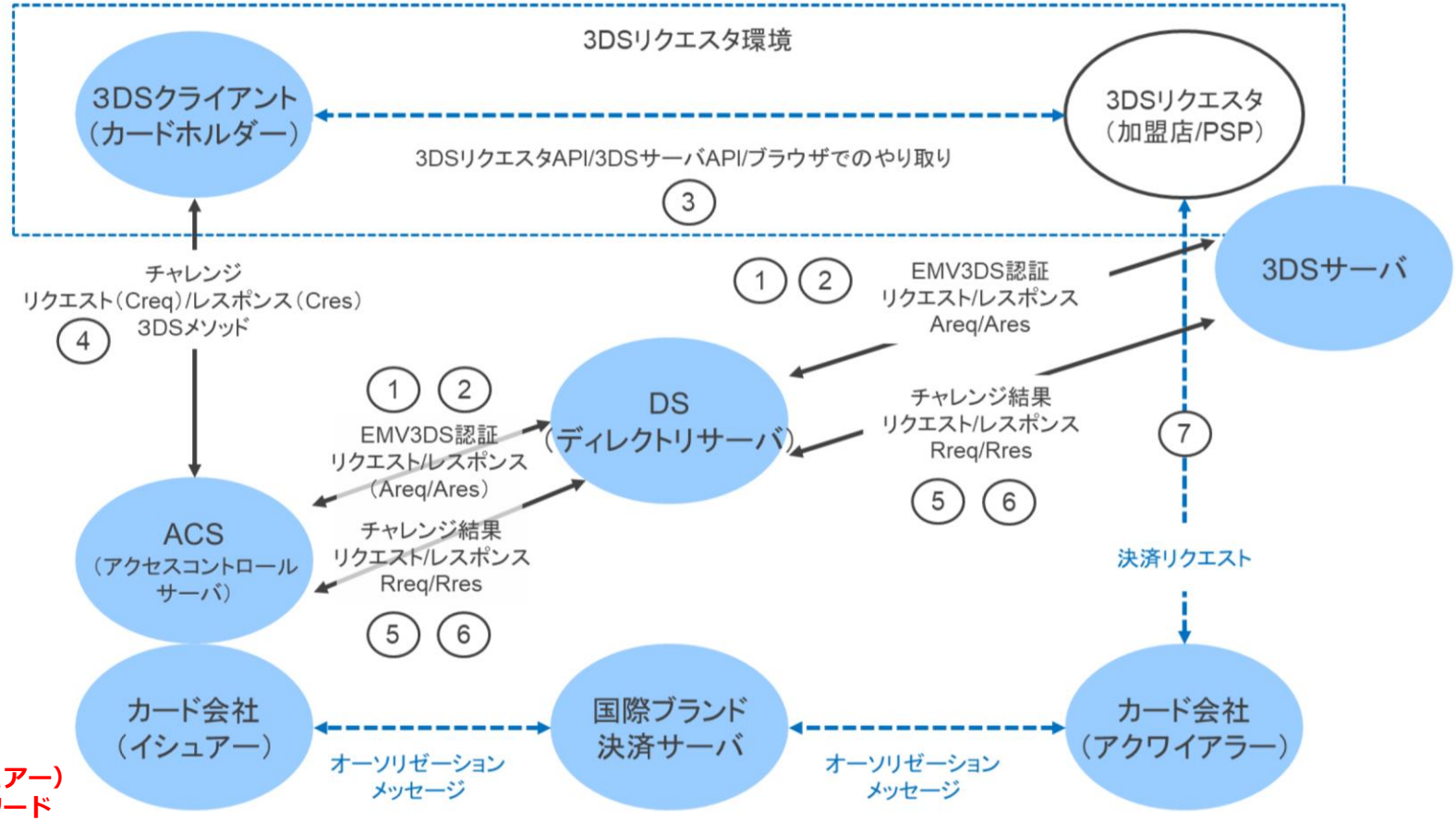
- EC加盟店やECモールは、自社顧客の属性や取引行動に関する情報を直接収集できることから、これらの情報を分析し、取引の適正性を判断する属性・行動分析や配送先住所の突合など、EC加盟店、ECモール等の不正取引による被害防止のための措置をEMV-3DSによる「利用者であるかの適切な確認」と組み合わせて実施することも求められる。
- また、キャッシュレスサービスやECモールのアカウントと紐付けられたクレジットカード決済が普及している状況下では、クレジットカード番号等のアカウントへの紐付時及び決済時のなりすまし対策も必要ではないか。

＜クレジットカード番号等をアカウントに紐付ける場合における認証の実施＞

- ◆ ECモール等では利用者の利便性を図るため、会員登録・初回購入時等に、クレジットカード番号等をECモール等のアカウントに紐付けることで、決済ごとのクレジットカード番号等の入力を省略する仕組みが普及している。
- ◆ クレジットカード番号等のアカウントへの紐付時のEMV-3DSによる認証の実施や商品購入・決済時のアカウントのなりすまし対策の実施が求められる。

EMV-3DSの仕組み

- EMV-3DSは、あらかじめカード会社（イシュアー）に設定した方法によりパスワードを入力することにより、カード利用者本人かの判断を行うもの。
- EC加盟店からイシュアーに、利用者のデバイス・行動・属性情報等が提供。イシュアーでのルール設定によるスコアリング・リスク判定を踏まえ、取引の拒絶／チャレンジ（パスワードの要求）／取引認証（パスワード不要）を判断。



要：事前設定
（利用者→イシュアー）
・ワンタイムパスワード
・生体認証

（資料）ＥＭＶ ３-Ｄセキュア導入ガイド1.1版 図９（2022年９月）

（参考）EMV 3-Dセキュア（旧３-Dセキュアとの比較）

- EMV 3-Dセキュア（EMV-3DS）は、従来の旧３-Dセキュア（旧3DS）の更新版。リスクベースの認証のほか、ワンタイムパスワードの標準化によるセキュリティ強化及び利用者の入力負荷の軽減、スマホアプリ対応による対象取引の拡大や加盟店からイシュアー（ACS）への提供情報の拡大が可能となった。

旧３DSとEMV-3DSの比較

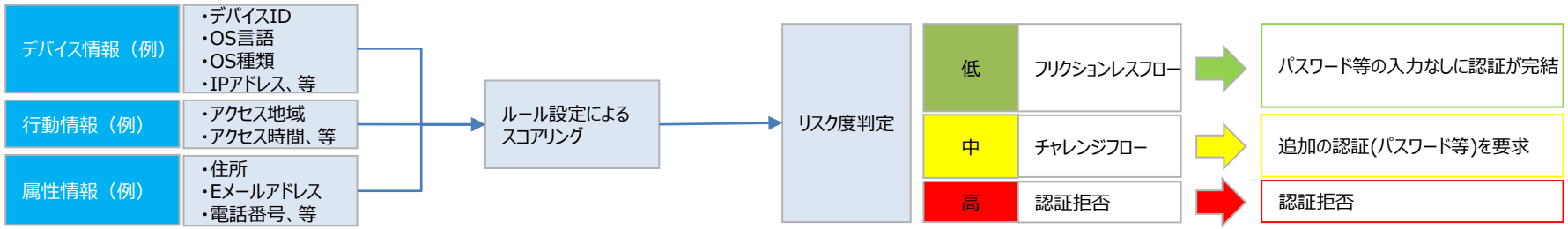
旧３DS（2022年10月サービス終了）

- 全取引にパスワードを毎回入力
- **固定パスワード**で一律認証
- ブラウザ取引のみ

EMV-3DS			
特長	内容	メリット	
		会員	加盟店
パスワード入力負荷を低減	・原則リスクベース認証※のみとなり、会員へのパスワード要求が不要（フリクションレス）	入力負担軽減	取引離脱リスクの減少（カゴ落ちリスクの減少）
ワンタイムパスワード等による本人認証	・中リスク判定時のみワンタイムパスワードなどによる追加認証を実施	パスワード漏えいによる不正リスクの軽減	会員のパスワード忘れによる機会損失の軽減
スマホアプリへの対応	・ブラウザに加え、スマートフォンやタブレットのアプリ内決済に対応	利便性向上	認証ツールの拡大

[参考]
リスクベース認証
ネット通販で使用されるパソコンやスマートフォンにおける機器やネットワークの情報から不正利用を判定する手法。
認証（スコアリング）によるリスク度判定によって、認証処理が異なる。

出典：クレジット取引セキュリティ対策協議会
「ＥＭＶ ３-Dセキュア導入ガイド」



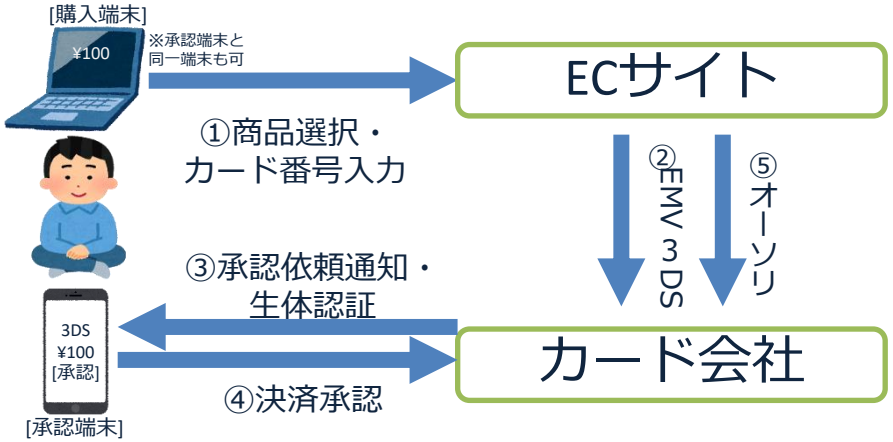
（参考）生体認証等によるEMV 3-Dセキュアの利用者負担の軽減

- EMV-3DSでは、スマホアプリ等での生体認証等も可能。（一部イシュアーで対応）
- ワンタイムパスワードに比べ、リアルタイムなフィッシング等での不正利用への耐性も強く、パスワードの転記等も不要となるため、使い勝手の向上と利用者負担の軽減が可能。

概要

一部のカード発行事業者において、EMV-3DSのOut of Band Authentication(OOBA)やDecoupled Authenticationの仕様を利用しスマートフォンアプリでのEMV-3DSの本人認証（取引の承認）が可能である。スマホ自体やスマホアプリの起動に生体認証を利用することで、実質的に**デバイス認証**と**生体認証**による本人認証となる。
承認時は、通知を起点にアプリを起動することで購入時と異なる通信チャネルとなり、フィッシング等を介した不正利用への耐性も強く、**利用者負担を軽減しつつ、セキュリティを向上が図られる**。購入端末と承認端末を分けることも可能。

処理フローイメージ



画面イメージ [購入端末]

[承認端末]

（参考）EUにおける強力な顧客認証①

- EUでは、決済サービス指令（PSD2）でカード会社に対し強力な顧客認証（SCA）を義務化し（2019年９月）、複数要素の認証を求めた。一方、個別取引のリスク度合い、金額、取引形態により例外も。EMV-3DSも対象で、2022年春までに多くの加盟国が導入済。

SCA(Strong Customer Authentication)

- 不正利用の削減を目的とし、全ての電子決済取引では3つの方法の内、少なくとも2つの認証をしなければならない。
  1. **知識：**
     PINなど、そのユーザのみが取引前から知っているもの
  2. **所有：**
     トークンやワンタイムパスワードなどにより認証される端末・アプリなど、取引開始後にそのユーザのみが所有しているもの
  3. **固有性：**
     生体認証(例：指紋認識)など、ユーザの一部

（参考）不正利用率の閾値

Transaction value band	PSP Fraud Rate
≤€100	13 bps / 0.13%
€100 ≤ €250	6 bps / 0.06%
€250 ≤ €500	1 bps / 0.01%

SCA準拠の例外条件

- **The Transaction Risk Analysis (TRA) exemption**
  - PSPがトランザクションモニタリングによりリスクが低いと判断したもの
  - 直近９０日内に、取引決済額に応じた不正取引の閾値（左下図）を越えない場合
- **The trusted beneficiaries exemption**
  - 支払者が決済事業者を通じて事前に作成または確認した「信頼できる加盟店のリスト」に、支払先が登録されているケース
- **The low value transaction exemption**
  - 以下両方の条件を満たす場合
    - 単価が€30未満
    - 前回利用者がSCAを適用して以来の累計5回までの取引または累積合計€100未満の取引
- **Secure corporate payments**
  - 一般消費者が利用できない決済システムにおける法人同士での取引（例：企業間の購買（B2B）取引、バーチャルカードでの宿泊代金管理システム）
- **Recurring Transactions**
  - リカーリング取引（カード登録型の継続的な取引）

（資料）令和４年度商取引・サービス環境の適正化に係る事業調査事業（NTTデータ経営研究所）

（参考）EUにおける強力な顧客認証②

- EUの強力な顧客認証（SCA）で認められている知識・所有・固有性の要素は以下のとおり。

	要素
知識	固定パスワード
	PIN
	知識ベースのチャレンジ問題
	パスフレーズ
	記憶されたスワイプパス

	要素
固有性	指紋スキャン
	音声認識
	静脈認識
	手や顔の形状
	網膜・虹彩スキャン
	キーストローク
	心拍数やユーザーを特定する体の動き
	デバイスを持つ角度

	要素
所有	ワンタイムパスワード（OTP）により証明されているデバイスの所有
	デバイスによって生成された署名によって証明されるデバイスの所有権
	外部機器から読み取ったQRコードにより証明されるカードまたは機器
	デバイスバインディングによって証明される所有権を持つアプリまたはブラウザ
	カードリーダーによって証明されるカード
	動的セキュリティコードによって証明されるカードの所有

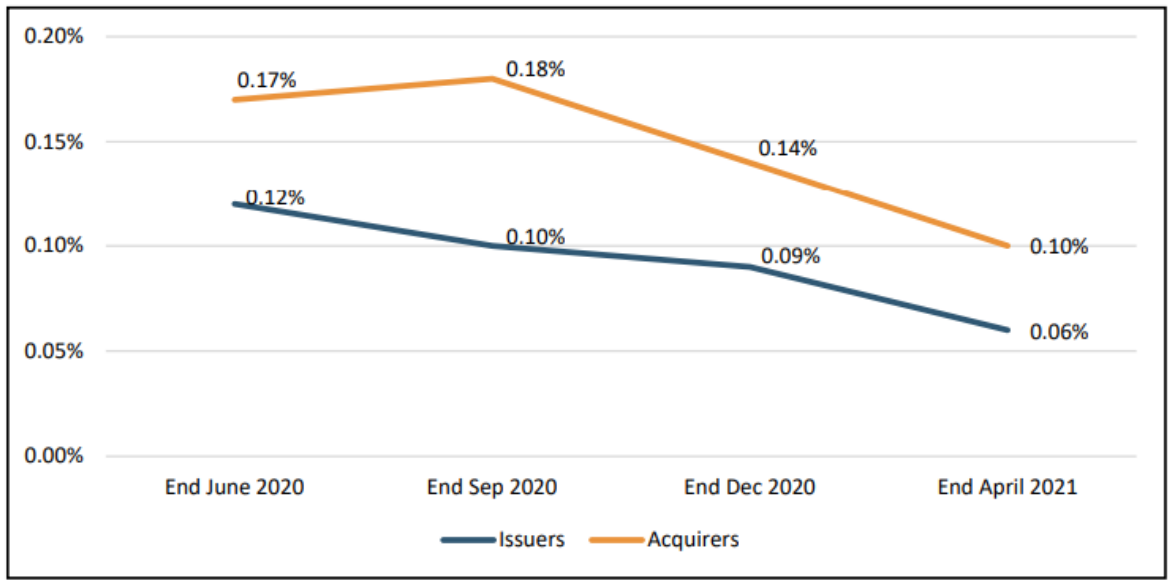
（資料）令和４年度商取引・サービス環境の適正化に係る事業調査事業（NTTデータ経営研究所）

（参考）EUでのEMV-3DSの普及

- EUから指令を受けた各加盟国で導入され、EUでのSCA（事実上EMV-3DSがほとんど）の普及は、利用者で約９割（EMV-3DSの会員登録を設定しないと取引が進めなくなる）、EC加盟店でほぼ全て。
- 不正利用の割合も半分近く削減（取引件数ベース）。

EUにおけるSCA状況(2021年4月段階)

Figure 7: Fraud rates across Member States based on average percentage rate* of the value of fraudulent transactions reported by issuers and acquirers**



*The EBA used the average percentage rate of the value of fraudulent transactions, since it provides a better overview of the situation at EU level and also because of the lack of particular outliers distorting the data.
** Data for Norway, Belgium and Poland is not covered in the fraud rate of acquiring PSPs, and data for Poland is not covered in the fraud rates for issuing PSPs. There are no acquiring PSPs authorised in Norway. The data quality received from acquiring PSPs in Belgium did not allow for meaningful interpretation. PSPs in Poland provided data only for the reporting period in April 2021.

- EU全域でのイシュアーベースで把握した不正利用の平均割合は、2020年７月から2021年４月の間で約50%減少。

  平均値：0.17%➡0.10%
- なお、アクワイアラーベースで把握した不正利用割合の平均割合は、約40%減少。

  平均値：0.12%➡0.06%

出典：EBA「EBA Report EBA/REP/2021/16」

（資料）令和４年度商取引・サービス環境の適正化に係る事業調査事業（NTTデータ経営研究所）

（参考）米国でのEMV-3DSの普及

- 米国では、EMV-3DSによるライアビリティシフトは2019年・2020年から適用。グローバルな大手PSPを中心に、EC加盟店に一定程度普及していると言われている。
- 連邦政府の納税徴収金融機関（カード会社）は、セキュリティの担保を求められ、国際ブランドのルール遵守の一環として、事実上、EMV-3DSに準拠している。

米国財務省・財政局によるTFM(財務省財務マニュアル)の概要

- **TFM**
  財務省財務マニュアル(TFM)は、米国財務省の公式ドキュメントであり、連邦政府の財務管理に関する方針・手続き・指示をまとめたもの。
- **TFMの主旨**
  政府の財務健全性と業務効率性を促進することを目的としている。
- **TFMのChapter7000とは**
  連邦機関が、クレジットまたはデビットカードを介して債務を回収する際に連邦機関が従わなければならない各種要件を示したもの。
- 連邦法やネットワーク規則(例：国際ブランド等の定めるルール)との兼ね合い
  連邦機関は、自ら承認したクレジットまたはデビットカード取引を管理する規則または規制(総称「ネットワーク規則」)に準拠し、拘束されなければならない。ネットワーク規則が連邦法および/または本章の条項と矛盾する場合、連邦法および/または本章の条項がネットワーク規則よりも優先される。

出典：米国財政サービス局「TFM→VOLUME1→PART5→7000」

（追補）不正利用発生時の利用者負担

- カード会員規約等では、利用者の届出から60日前までに不正に取得されたカード情報の使用による損害については、イシュアーが利用者の経済的負担としないようにする運用が主。
- 結果、不正利用を防止できず、イシュアーが加盟店に立て替えた代金の売上げは取り消され、その金銭負担は、基本的には加盟店が負うこととなる。

不正利用に関連するカード会員規約の規定(典型例)

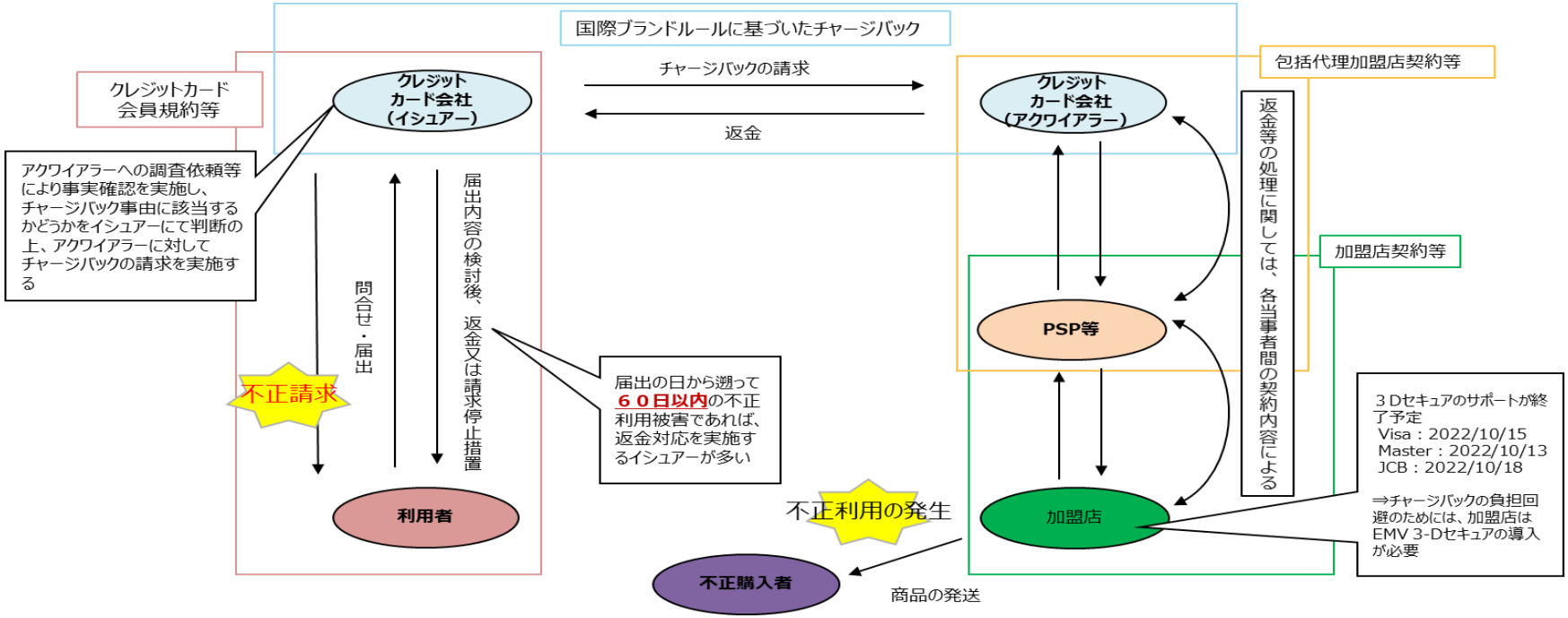
① カード情報が不正取得された場合等※1における、会員のイシュアに対する届出及び警察署への連絡が必要
② **当該連絡より60日前※2まで遡り**、その間において使用された損害について、会員の故意又は重過失が存在しない場合等に限り、会員の負担としない
※１ 規約上、カード情報の不正取得について明示していない場合もある
※２ 当該連絡日を含め、61日とする場合もある
→上記60日の期間外において発生した不正利用被害の補てん等に関しては、明文の規定なし

不正利用に関連する加盟店規約の規定（典型例）

① 信用販売を行うにあたっての、セキュリティ・ガイドライン（同規約上、「実行計画」とされる場合もある。）に掲げられた加盟店での措置又はそれと同等の措置を講じる義務
② 不正利用発生時における再発防止のための調査協力義務
③ 不正利用発生時における再発防止に関する計画の策定及び実施
④ ①に記載の義務に違反して、信用販売を行った場合における、カード会社の加盟店に対する立替払契約の取消等、支払拒絶又は返金請求が可能

（追補）国際ブランドルールでのライアビリティシフト

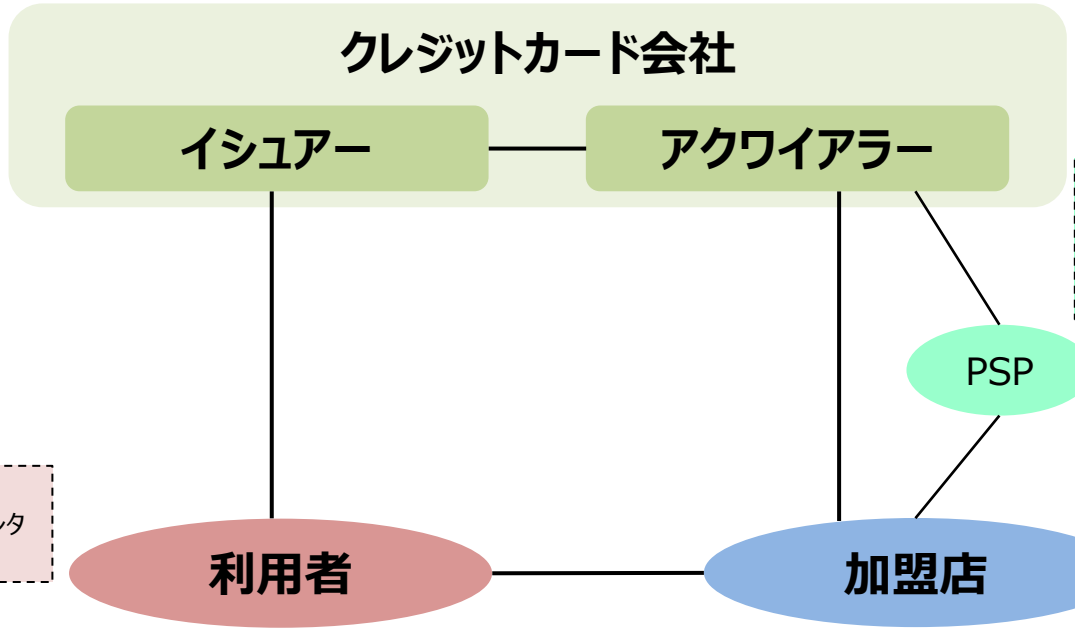
- 国際ブランドでは、不正利用時のチャージバックの際のライアビリティシフトのルール（個別の取引を認証する旧３DS／EMV-3DSを導入しない加盟店に対して、不正利用発生時のチャージバックの負担を、イシュアーでなく加盟店側負担にする仕組み）を従前より適用。
- なお、旧３DS自体は、国際ブランドにより、2000年代後半より推奨されてきたものの、かご落ちリスクへの不安等により、国内ではあまり普及しなかった。日本では、2022年10月、旧３DSのサービスが使用停止となり、旧３DSではライアビリティシフトが適用されなくなることから、EMV-3DSへの切り替えが順次行われている。



EMV-3DS導入に向けた環境整備

- 非対面取引での不正利用を防ぐため、「利用者であるかの適切な確認」には、まずはEMV-3DSの導入が現実的な選択肢と考えられる。EMV-3DSの導入には、カード会社（イシュアー）、EC加盟店、利用者の３者の準備が必要。
- また、すべてのEC加盟店がEMV-3DSを導入できるよう、クレカ決済機能を提供するPSP（ECモール等）の仕組みなくしてEMV-3DSを導入できないEC加盟店に対しては、当該PSPはEMV-3DSへの接続サービスを提供することが必要となる。

イシュアー
- EMV-3DSの導入
- 会員のパスワード利用の徹底（固定パスワードの廃止：ワンタイムパスワードの設定）
- リスクベース判定の向上
- 本人認証サービスの安定的な提供



PSP（ECモール等）
- クレカ決済機能を提供するECモール等で、EC加盟店に対するEMV-3DSの提供

利用者
- 本人認証の登録、会員のパスワード設定（ワンタイムパスワード／生体認証）

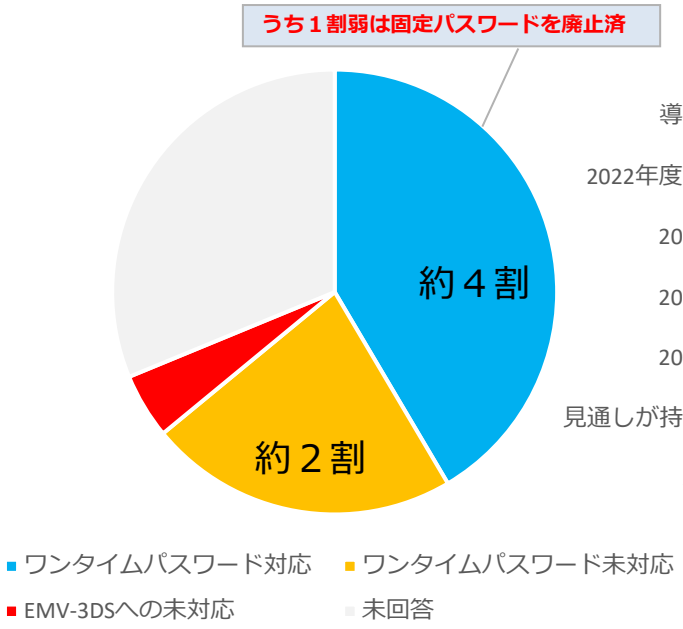
（例）利用者の作業イメージ
・クレジットカード番号等でマイページアカウントの作成
・マイページにて本人認証登録
・本人認証の設定を固定パスワードからワンタイムパスワードに変更
・ワンタイム用のアプリケーションの導入(SMS等の場合不要)

EC加盟店
- EMV-3DSの導入

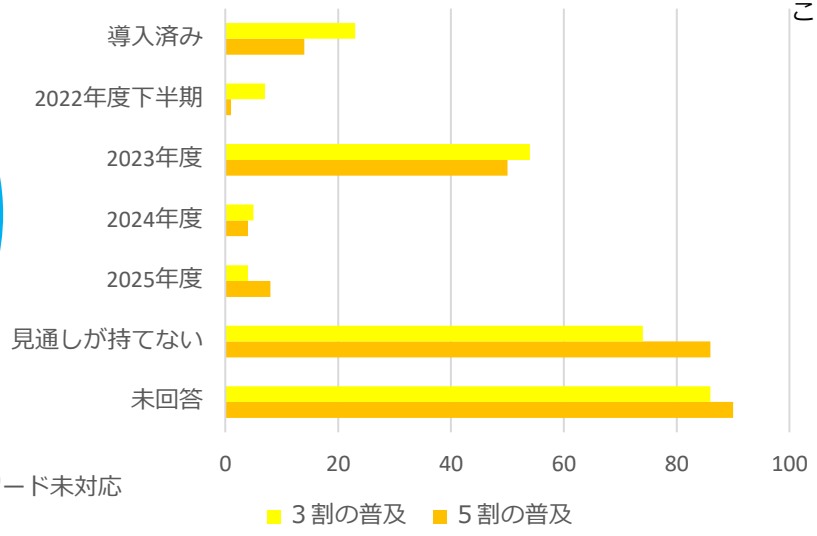
EMV-3DS導入に向けた対応状況（イシュアー、利用者）

- EMV-3DS自体の導入は、回答事業者のうち約９割のイシュアーが対応済み、うち約６割強はワンタイムパスワードに対応済み。（イシュアーの任意回答ベース）
- ワンタイムパスワードについて、3割の利用者が設定済みのイシュアは、回答事業者のうち１割強、５割の利用者が設定済みのイシュアーは、回答事業者のうち１割弱。（イシュアーの任意回答ベース）
- 利用者のワンタイムパスワードへの移行は、８割以上の利用者にとって許容可能な様相。

＜国内イシュアーでのEMV-3DS対応状況＞

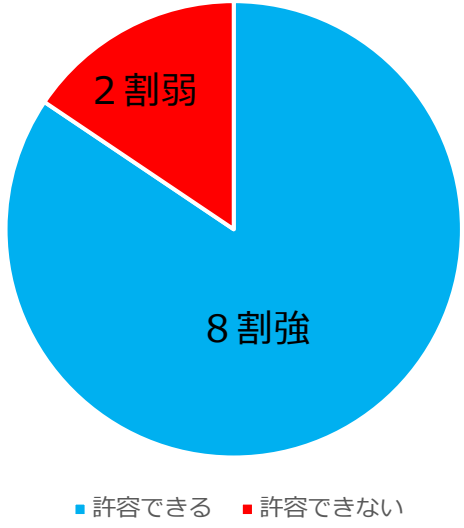


＜利用者のワンタイムパスワード設定状況＞（普及の想定含む）



＜利用者のワンタイムパスワードへの許容度＞

問：不正利用防止の観点から、クレジットカード会社が取引にリスクがあると判断した場合に、本人認証（パスワード入力やSMS・メールでのワンタイムパスワードの入力等）を求められることは許容できますか。

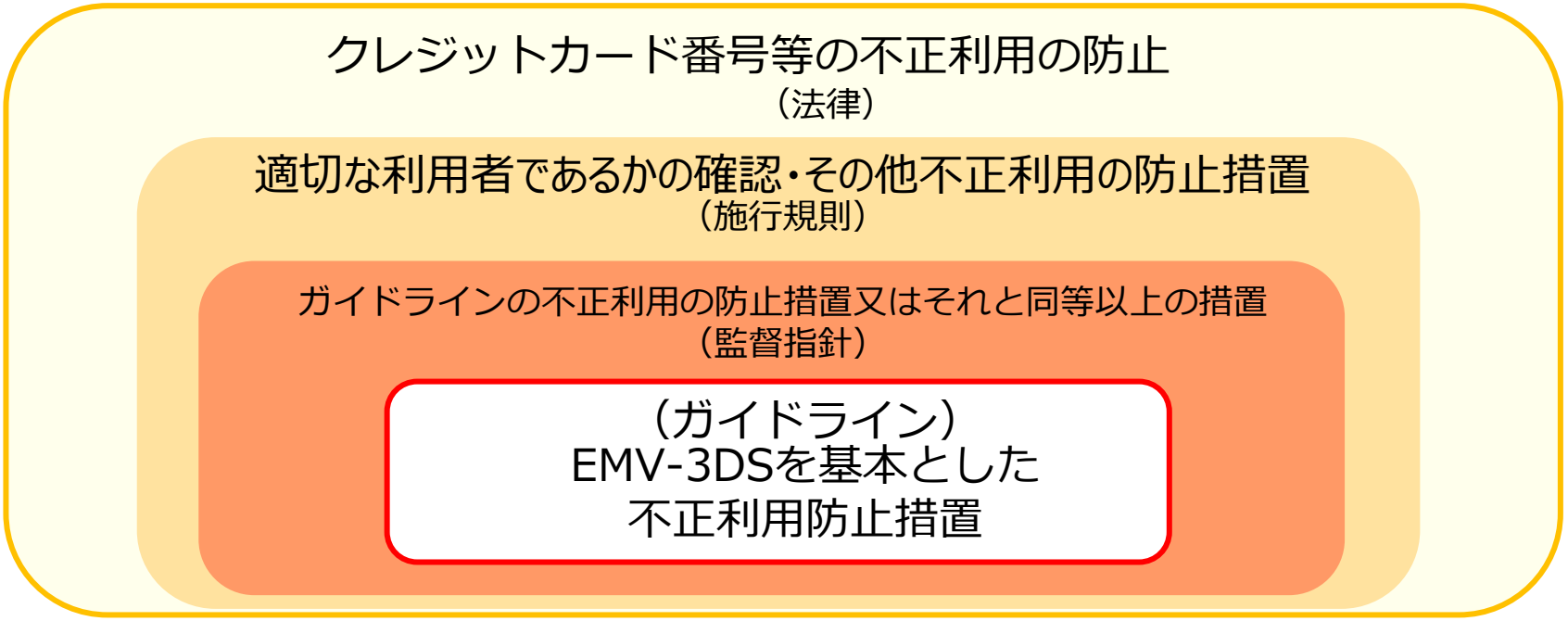


（2022年９月時点で事務局で把握しているもの）

「クレジットカード利用に関するアンケート」（2022年9月下旬：回答者数：1117人）

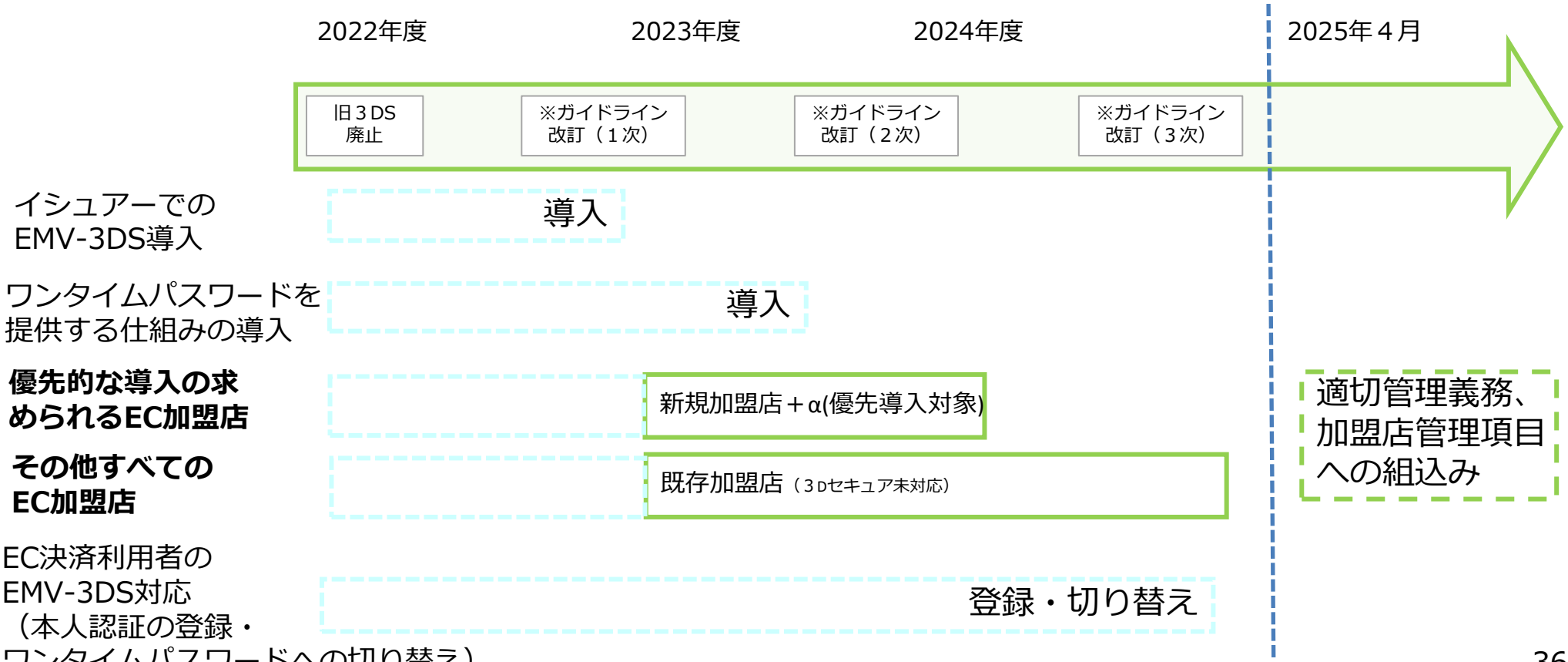
EC加盟店での不正利用防止／アクワイアラー等による加盟店管理

- 今後、EC加盟店にクレジットカード番号等の不正利用防止として、「利用者であるかの適切な確認」として、基本的には、個別の決済ごとに、利用者本人しか知らない情報や本人に固有の情報から、真正なカード利用者本人であると認証して、本人認証を高度化していくことが必要。
- また、アクワイアラー等による加盟店管理においても、EC加盟店が利用者であることの適切な確認のための体制整備・運用ができているか確認し、指導していくことが必要。



不正利用防止義務の引上げに向けて

- 将来的に、不正利用防止の対策基準の引上げ、またアクワイアラー等による加盟店管理における調査事項として、法的義務に引き上げていくことが考えられる。
- クレジットカード・セキュリティガイドライン（クレジット取引セキュリティ対策協議会）を改訂する際には、法的義務の引上げに向け、段階的な導入に向けた指針を示すことが期待される。まずはイシュアーでの導入完備が求められ、順次EC加盟店での導入が必要。



（参考）インターネット・バンキングでのワンタイムパスワードの普及

- わが国のインターネットバンキングでも、IDや認証情報の漏えい・搾取といったセキュリティリスクから、取引の認証方式として、ワンタイムパスワードを推進。
- 銀行におけるインターネットバンキングで送金を利用するには、利用者側はワンタイムパスワードを求められることとなる。

※各年３月末の数字。

年月	手法	ポイント	個人向け可変パスワード導入済金融機関（%）※
2006年 ７月	検討会 報告書	スパイウェアやフィッシングサイト等におけるIDや認証情報の漏えい・搾取を踏まえ、インターネットバンキングにおける認証方式について、個々の認証方式が、各種犯罪手口に対してどの程度の強度を有するか検証したうえで選択すべき、と提示。	
2007年 １月	主要行等向けの総合的な監督指針	セキュリティの確保として、本人認証について、取引のリスクに見合った適切な認証方式を選択しているか、の項目を追加。	15.3%
2012年 １月	全銀協 申し合わせ	可変式パスワードや電子証明書といった固定式のID/パスワードのみに頼らない認証方法の導入を図り、セキュリティ対策の一層の向上に努めるものとする。	37.4%
2012年 ２月	主要行等向けの総合的な監督指針	セキュリティの確保として、可変式パスワードなどの固定式のID/パスワードのみに頼らない認証方式の導入を図ることを例示。	
2013年			94.7%
2021年			99.7%

（２）不正利用情報の共有化

不正利用情報の共有化の必要性

- クレジットカードの不正利用防止にあたり、クレジットカード決済システム全体での不正検知能力の向上に向けて、個社で実施していた不正検知システムを共同化していくことが有効との考えがある。
- 現在、各イシュアーでオンラインモニタリングがされているが、各イシュアーの持つ不正利用情報を共有化し、不正検知精度を向上させることは効果的と考えられる。
- クレジットカード決済網の当事者間において、不正利用に関する情報を即座に共有・集積することで、より高度な不正検知を実現する取組みが進められていくことが必要。
- ①イシュアーから利用者への個別取引の利用明細のリアルタイム通知による利用者の不正利用の即座の把握、②個社を超えた不正利用情報の共有による各イシュアーでの不正検知の精度向上・不正利用への即座の防御が考えられる。

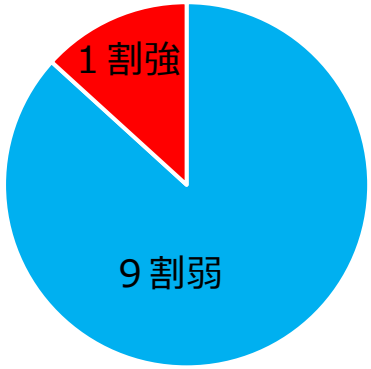
手法	共有する者	共有データ
①利用明細の通知のリアルタイム化	イシュアー・利用者間	個別取引の利用明細
②不正利用情報の共有	案①イシュアー間 案②イシュアー間 案③PSPをハブとした加盟店間	各社で、不正利用／不正利用のおそれありとした取引

個別取引の利用明細のリアルタイム通知

- 後日の支払請求となる利用明細（通常月次）を確認している利用者は９割弱。オンライン通知により、2割弱の利用者の確認頻度が増えており、不正利用による利用者被害を生まないためにも、引き続き、利用明細の確認の周知が必要。
- イシュアーのスマホアプリ等により、個別決済時の利用明細のリアルタイム通知を導入することで、不正利用を即座に気づきやすくすることも可能（フィッシング対策として、通知において、カード番号の入力を求めない、URLを貼らない等の工夫は必要）。イシュアーでの利用時の通知の導入状況は回答事業者のうち５割弱の事業者が導入済みで、そのうち９割弱の事業者でリアルタイムに通知が行われる。
（事業者の任意回答ベース）
- イシュアーでの更なる導入とともに、利用者への周知が求められるのではないか。

＜利用明細の確認状況＞

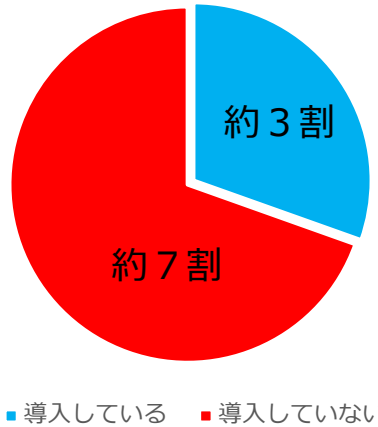
問：クレジットカード利用の後日、支払請求が確定となる利用明細が送付されますが、利用明細を確認していますか 。



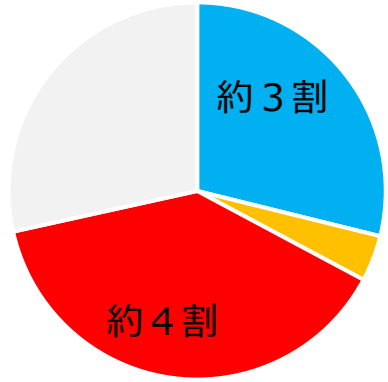
「クレジットカード利用に関するアンケート」（2022年9月下旬：回答者数：1117人）

＜リアルタイム通知アプリの導入状況＞

問：クレジットカードでの取引決済時に、リアルタイムで利用者に通知するスマホアプリを導入していますか 。



＜イシュアーでの利用者に対する個別決済時の通知状況＞



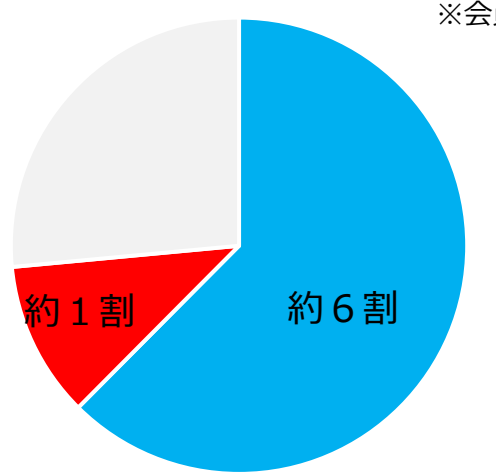
（2022年９月時点で事務局で把握しているもの）

不正利用情報の共有化に向けたイシュアーの動き

- イシュアーでは日々不正検知のオンラインモニタリングを実施。昨今では、ルールベースによる検知だけでなく、機械学習により不正利用のトレンドに合わせた不正検知を実施するイシュアーも存在。不正利用に係る情報を多く共有・集積、活用することで、不正検知の精度が向上することが期待される。
- 実際に不正を検知し、利用を止めているイシュアーにおいては、他社と不正利用にかかる情報を共有したい意向があり。一方、各イシュアー間を超えた個人情報の共有は、個人情報保護法に留意する必要がある。

<イシュアーでの不正利用情報の共有化に向けた自社の不正利用情報の提供の意向>

※会員からの同意が得られた場合

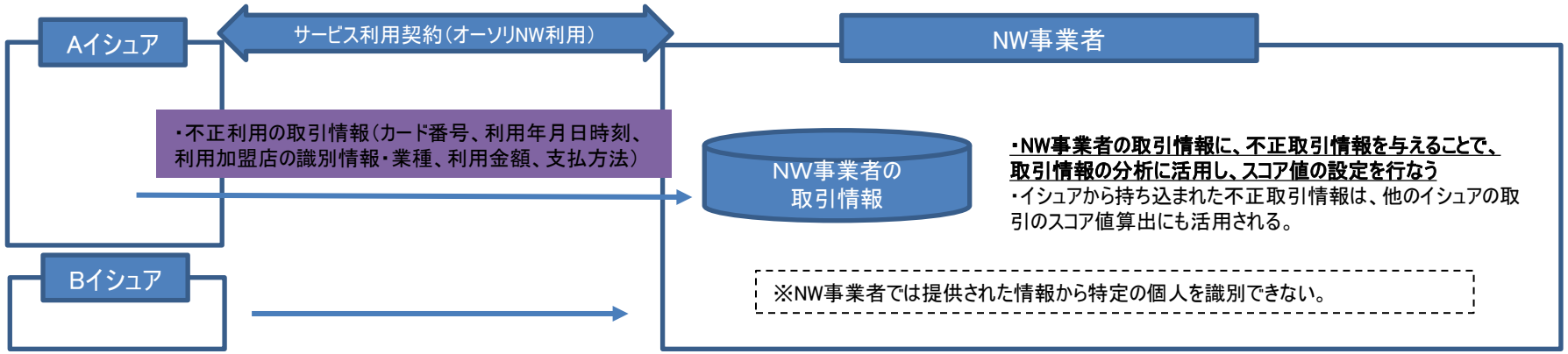


（2022年９月時点で事務局で把握しているもの）

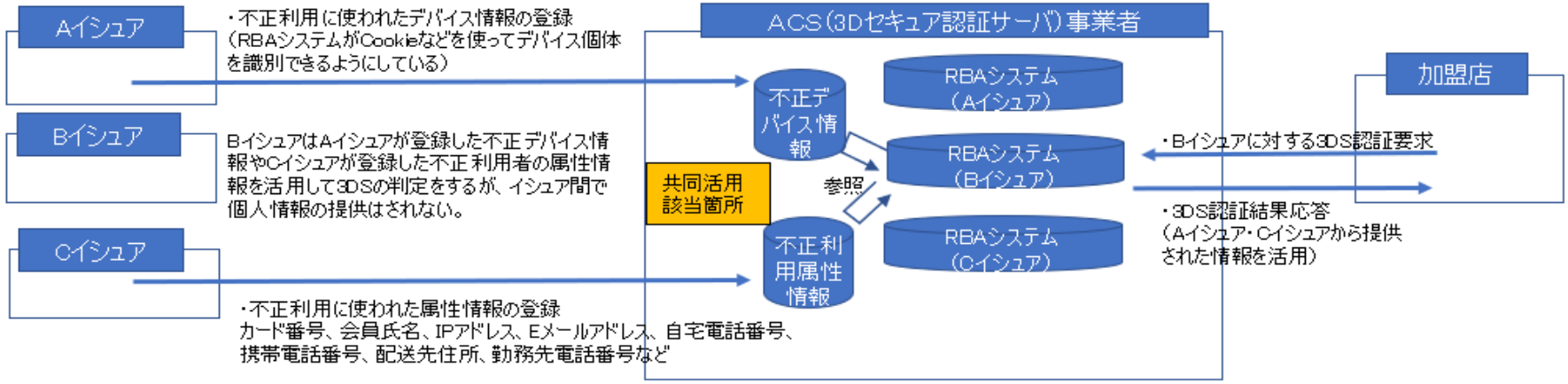
不正利用情報の共有化に向けたスキームの検討

- 現在、業界において、既存のオーソリゼーション網を活かしたオーソリゼーション中の不正利用情報の共有のほか、 EMV-3DSの過程でACSに集積される不正利用データを活かした本人認証中の不正利用情報の共有が検討されている。

案①既存のオーソリネットワークを活かした共同利用（イシュアー間）



案②EMV-3DSのリスクベース認証（ACS）でのイシュアー間の共同利用（イシュアー間）



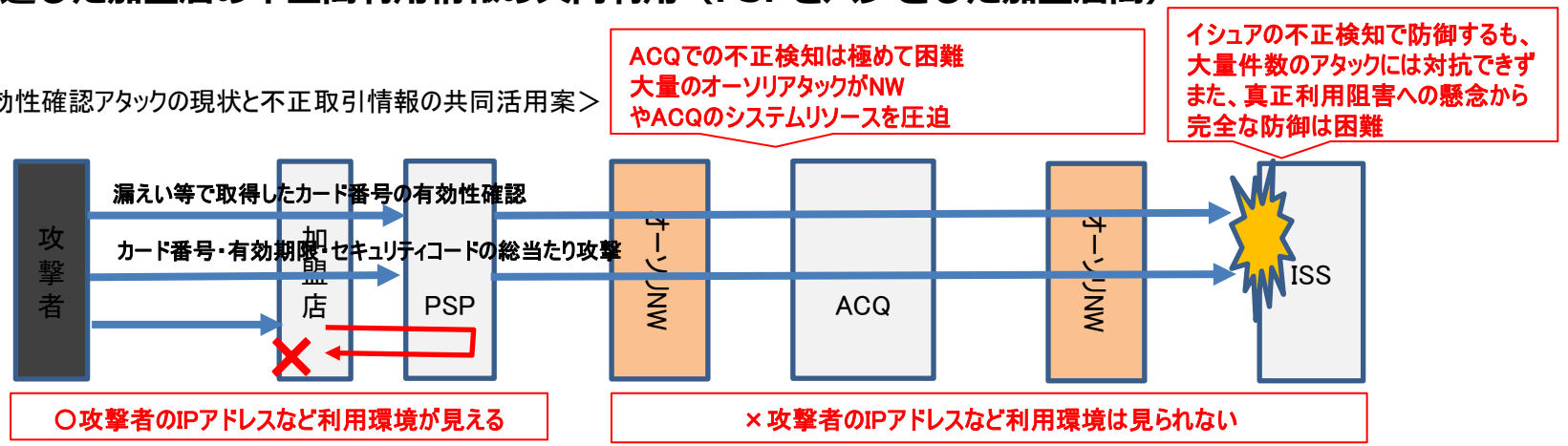
不正利用情報の共有化に向けたスキームの検討

- また、EC加盟店の実質ハブとなっているPSPで、各EC加盟店の不正利用動向を検知する不正利用防止も、クレジットマスター対策に有効ではないかと検討されている。

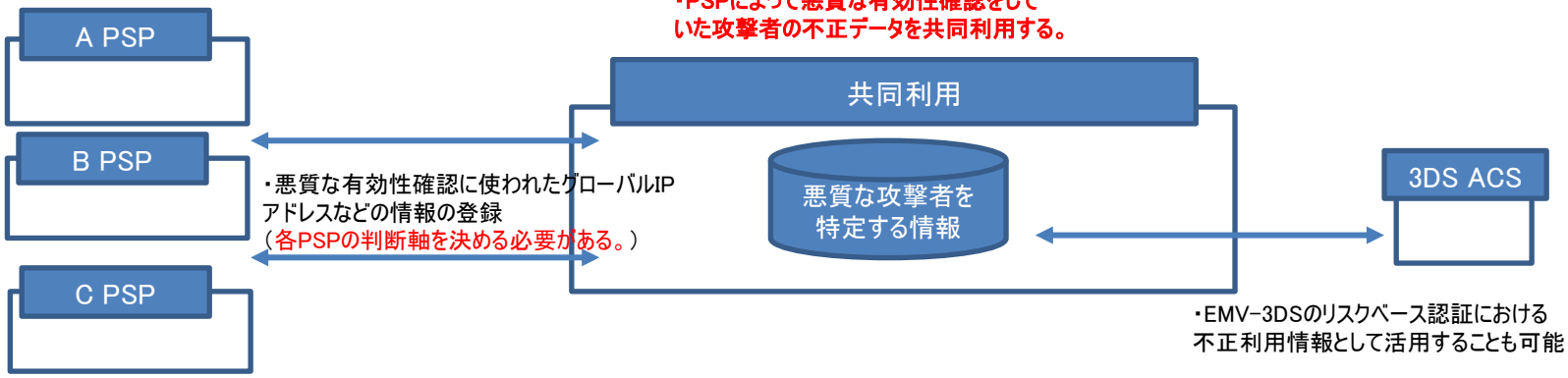
案③PSPを通じた加盟店の不正間利用情報の共同利用（PSPをハブとした加盟店間）

イメージ図

＜クレマス/有効性確認アタックの現状と不正取引情報の共同活用案＞



IPアドレス等を活用した悪質な有効性確認に該当する攻撃者のトランザクションの検知及び停止（PSP）



ご議論いただきたい事項

EC加盟店での不正利用防止対策
総論：昨今のクレジットカードの不正利用を念頭におき、不正利用対策の実効性を確保するためには、どのようなアプローチが有効か。

（１）加盟店側での対応
これまで、EC加盟店に対しては、リスクの高いEC加盟店にのみ、本人認証の対策を任意で求めてきたところ。
①今後、EC加盟店における不正利用防止措置として、「利用者であることの適切な確認」として、個別取引時にカイシュアーによるカード利用者本人の確認を求めていくにあたり、その手法として、利用者本人しか知らない情報により、本人を認証する手法に高度化させてはどうか。

②当面の対応としては、まずは原則すべてのEC加盟店での取引について、EMV-3DSによる確認をどのように進めていくべきか。一方、リスクや取引規模が大きい加盟店においては、EMV-3DSだけで十分だろうか。キャッシュレス決済の基盤として、クレジットカード番号１６桁の以外の入力方法による決済（例：EC加盟店でのアカウントがクレジットカード番号等と紐付いている場合）の場合には、不正利用対策はどのようにあるべきか。

③不正利用防止義務して、EMV-3DSを導入していく場合、いつまでに、どのように導入していくことが効果的か（時期、優先的な導入が求められるEC加盟店、実効的な手法、未登録会員への対応等）。

（２）PSP（ECモール等）での対応
①EC加盟店にクレジットカード決済機能を提供しているPSPやECモール等は、EC加盟店がEMV-3DSを導入できるよう自ら措置していくことが必要ではないか。

（３）イシュアー側での対応
これまで、イシュアーには、個別決済に伴う不正利用防止として、基本的には任意の取組が求められてきたところ。
①「利用者であることの適切な確認」は、イシュアーでなければ難しいところ、確認主体はイシュアーとして責任を有するという形でよいか。
②EMV-3DSのリスクベース認証の精度をあげていくには、どうしていくべきか。
③EMV-3DSはリスクベースであるところ、イシュアーでの不正利用防止対策の効果を事後的に確認していくべきか、どのように確認していくべきか。