経済産業省

安全・安心

参考資料３

第１回～第6回クレジットカード決済システムの
セキュリティ対策強化検討会資料より引用

クレジットカード決済システムの
セキュリティ対策強化検討会
（関連資料）

2023年２月２日

経済産業省　商務・サービスグループ

商取引監督課

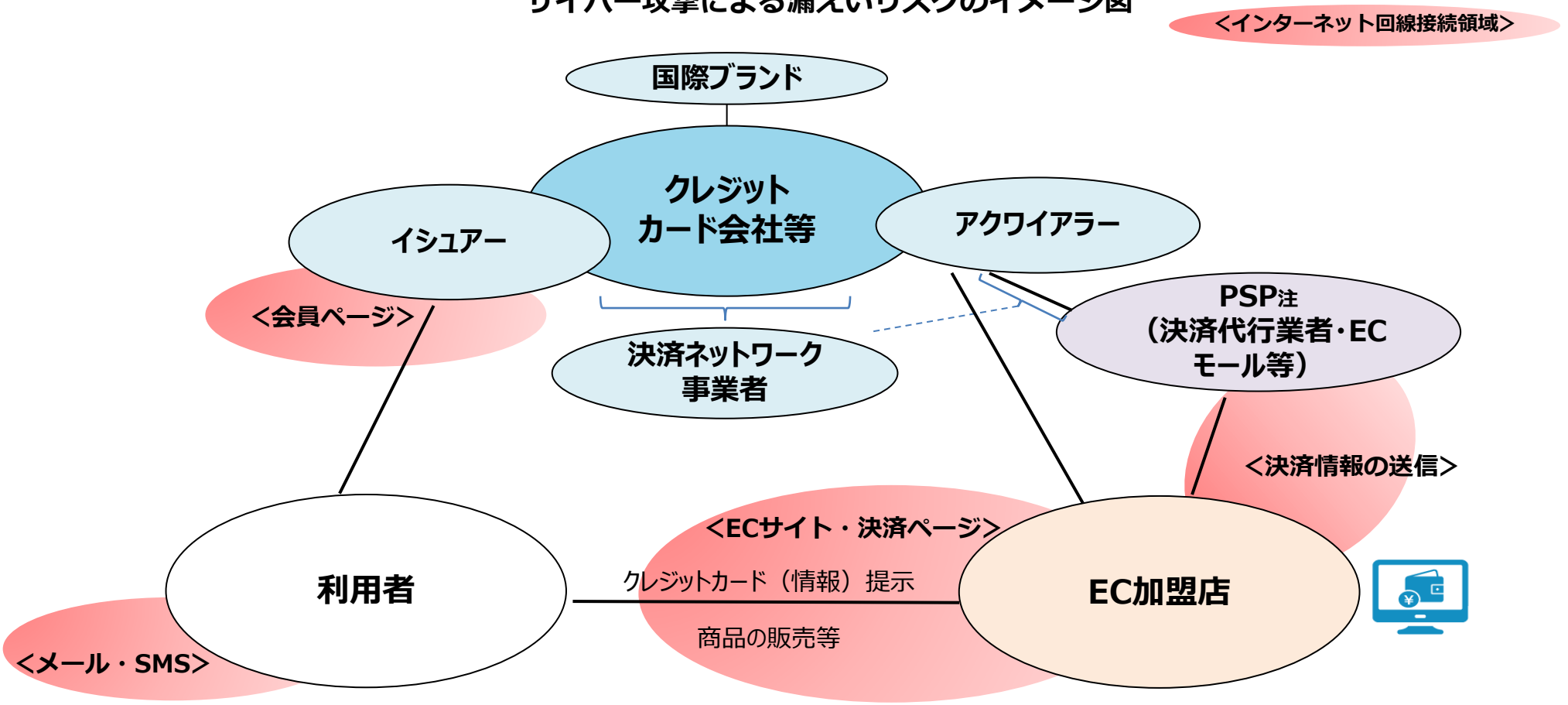
Ⅰ．漏えい防止（クレジットカード番号等の適切管理の強化）

1．クレジットカード番号等の漏えいリスク

2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会 資料３より引用

- クレジットカード決済システムは、多数の事業者のネットワークによって成立。クレジットカード番号を直接保持（保存・処理・通過）しているプレイヤーだけでなく、インターネットを介してクレジット決済を可能にするネットワークの接続を持つプレイヤーにも常にサイバー攻撃のリスクが存在。

サイバー攻撃による漏えいリスクのイメージ図

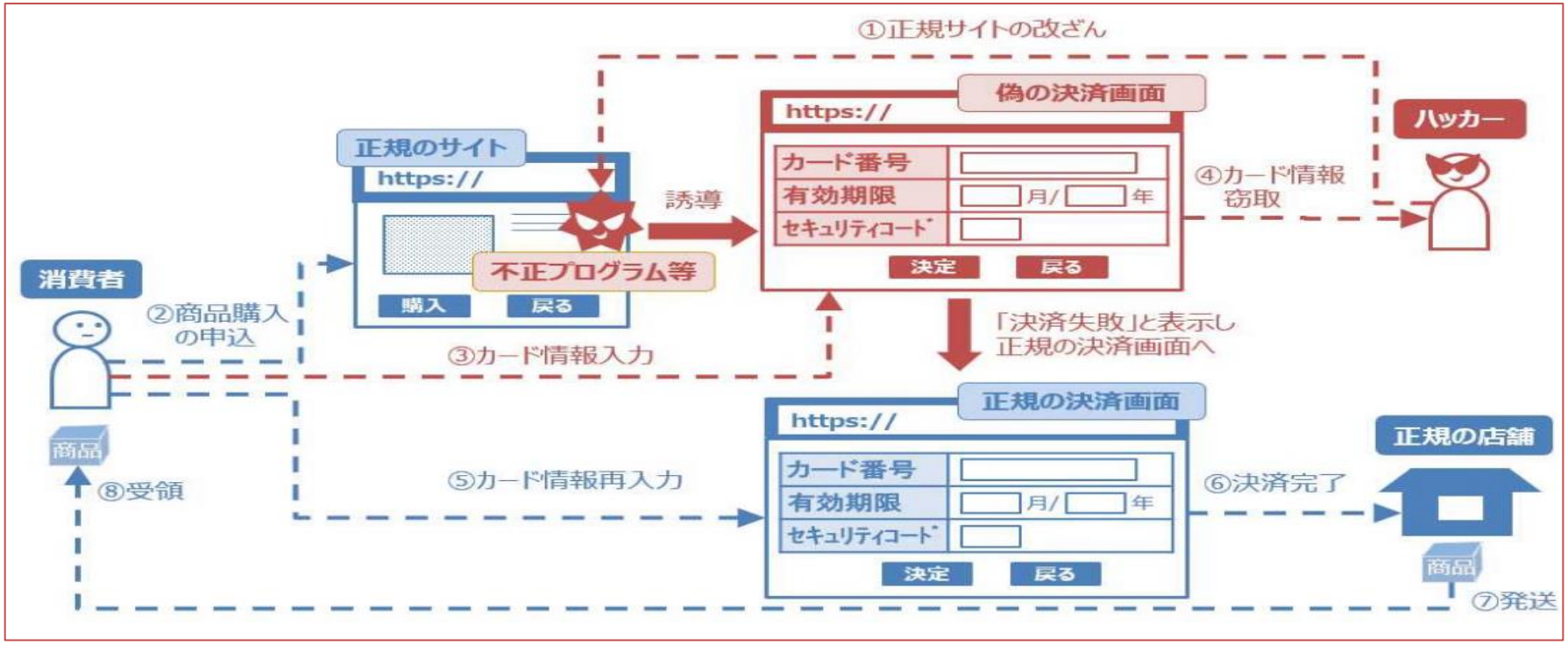


注：本資料では、PSPをその機能面から「インターネット上の取引において EC 加盟店にクレジットカード決済スキームを提供 し、カード情報を処理する事業者」とする。

1．漏えい事案①： EC加盟店での漏えい（概要）

2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会 資料３より引用

- 特にオープンソースにより構築され、自社（委託先含む）で適切なアップデートを行わないなど、十分なセキュリティ対策を講じていないECサイトの脆弱性を狙った不正アクセス等による漏えい事案が増加。クレジットカード番号等を保持していなくとも、**ECサイト自体が改ざんされることで、不正ファイルの設置や偽の決済サイトへの誘導でクレジットカード番号等が流出。**
- 当省でも加盟店に対する注意喚起を実施(令和元年12月）。IPAとも連携。
- しかしながら、**ECサイトでのサイバー攻撃によるクレジットカード番号漏えい事案は増加**（約２割増（うちオープンソース関連は、約４割増加）。

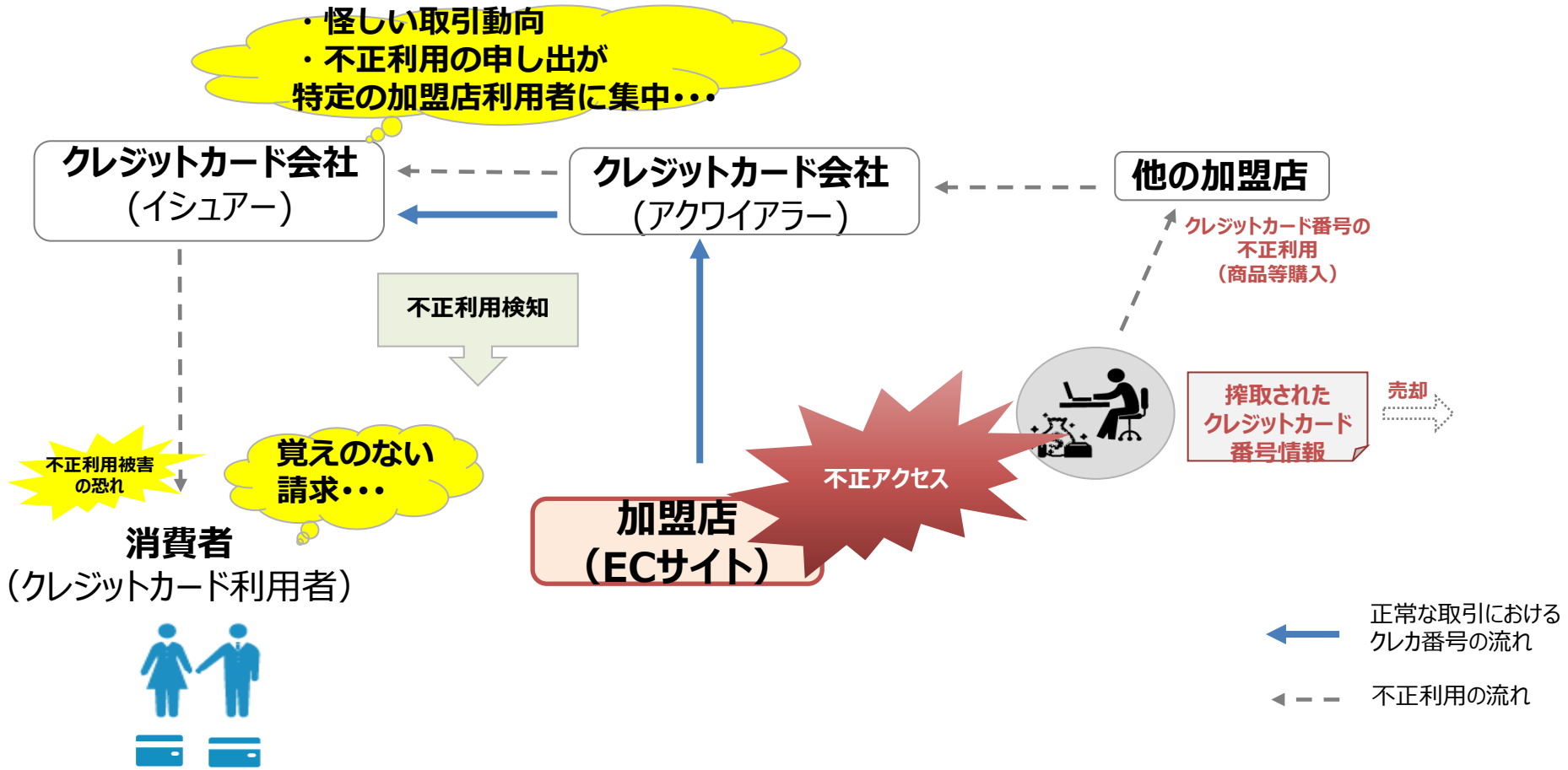


消費者庁・経済産業省「インターネットショップでのクレジットカード番号の漏えい・不正利用に注意しましょう」（令和２年２月13日）
https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/pdf/consumer_policy_cms104_200218_01.pdf

1．漏えい事案①： EC加盟店での漏えい（発覚経緯）

2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会資料３より引用

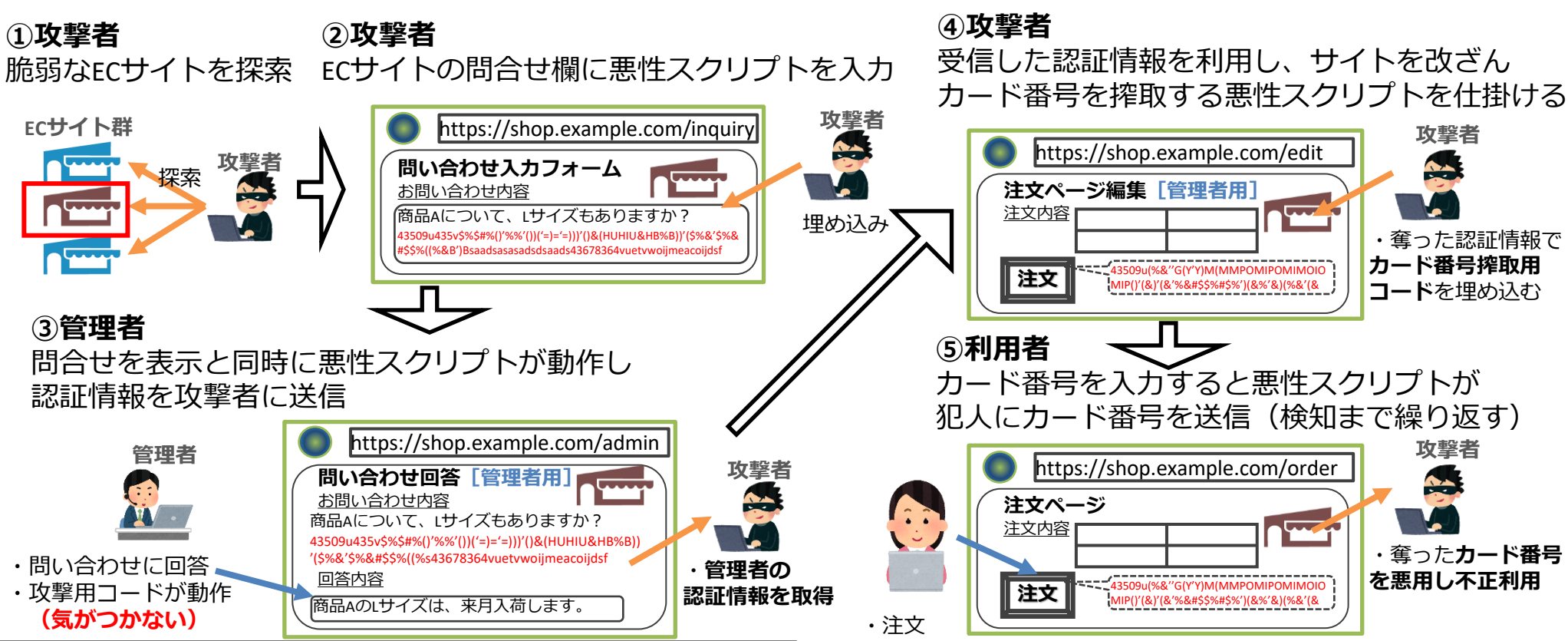
- EC加盟店での漏えいの発覚経緯は、カード会社（イシュアー）によることが主。利用者からの連絡で発覚することもあるが、加盟店自らで早期に不正アクセスを検知できているものはほとんどない。
- 結果として、過去の漏えい事案では、不正アクセスによる漏えいの発生から漏えいの検知までの期間が３か月以上かかるものが約７割以上。数日から数年間に渡るものもある。



1．漏えい事案①： EC加盟店での漏えい（サイバー攻撃手法）

- 昨今のEC加盟店での漏えいは主として既知のサイバー攻撃による。その多くが、外部のインターネットと接続している問合せフォームや注文サイト等へのクロスサイトスクリプティングにより、ECサイトを改ざんし、データを搾取するもの。
- 特に利用者の多いECパッケージでは、攻撃側に脆弱性を熟知されており、攻撃側にとって、より効率的に攻撃できることから、攻撃の対象となりやすい。

EC加盟店へのサイバー攻撃のイメージ



2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会　資料３より引用

1．漏えい事案①：「非保持化」と更なる漏えい対策の必要性

- 平成28年法改正以降、**ほぼ全てのECサイト**が、クレカ番号等の**非保持化を選択。**
- 非保持化により、漏えい時の**被害は小規模化**したがと想定されるが、**漏えい事案は増加傾向。**
- **非保持化だけでは漏えい対策は不十分**との認識がなく、サイトの脆弱性対策等が喫緊の課題。

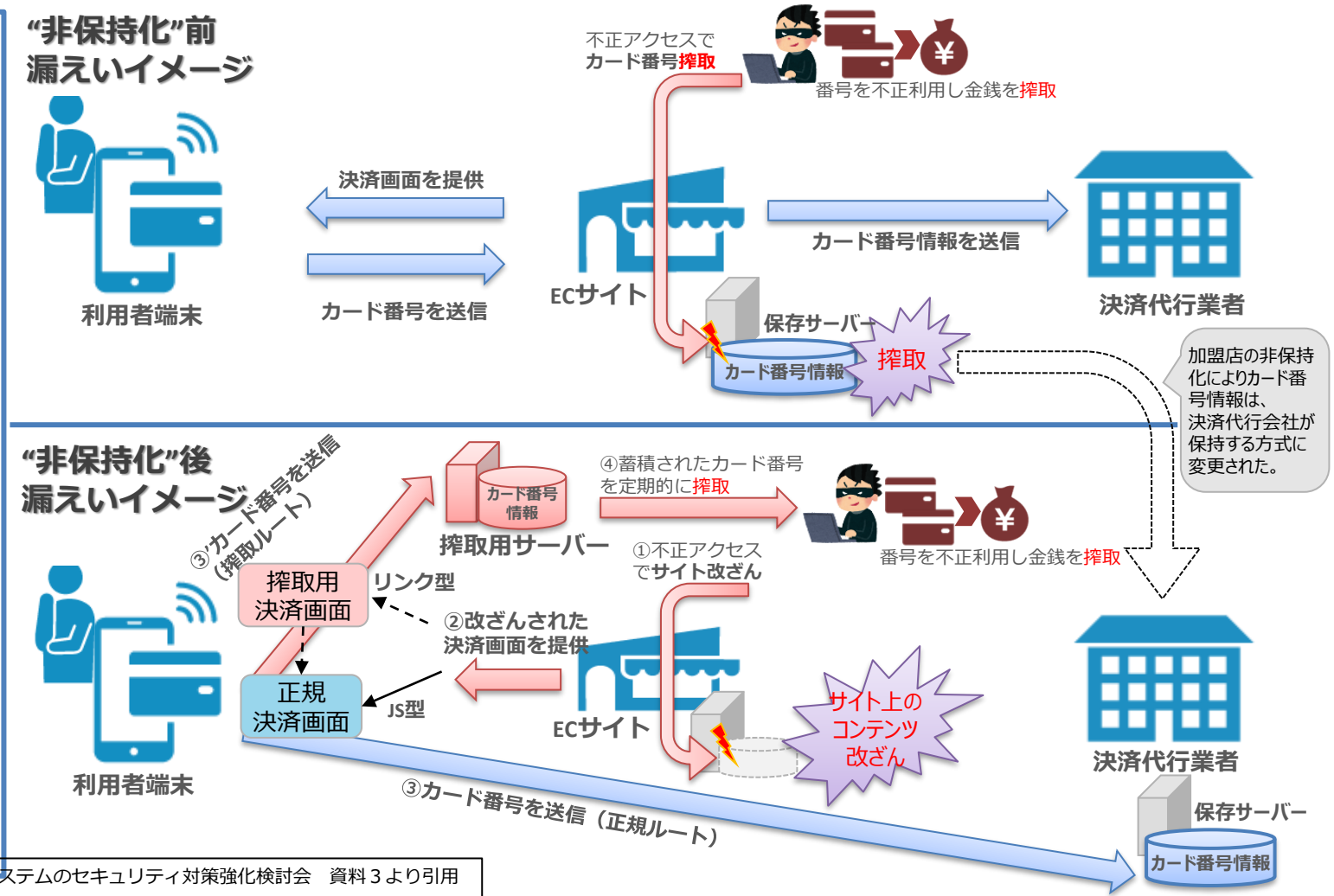
“非保持化”を実現する決済処理方式は「リンク型」と「JS型」の２種類が存在

・「リンク型」改ざん遷移例

②決済画面
（ECサイト：リンク先が改ざん）
↓
③’カード番号入力画面
（搾取用決済画面）
③’搾取用サーバにカード番号送信
↓
③カード番号入力画面
（正規決済画面
（決済代行業者提供））
③ 決済代行サーバにカード番号送信
↓
②決済完了画面
（ECサイト）

「JavaScript(JS)型」改ざん遷移例

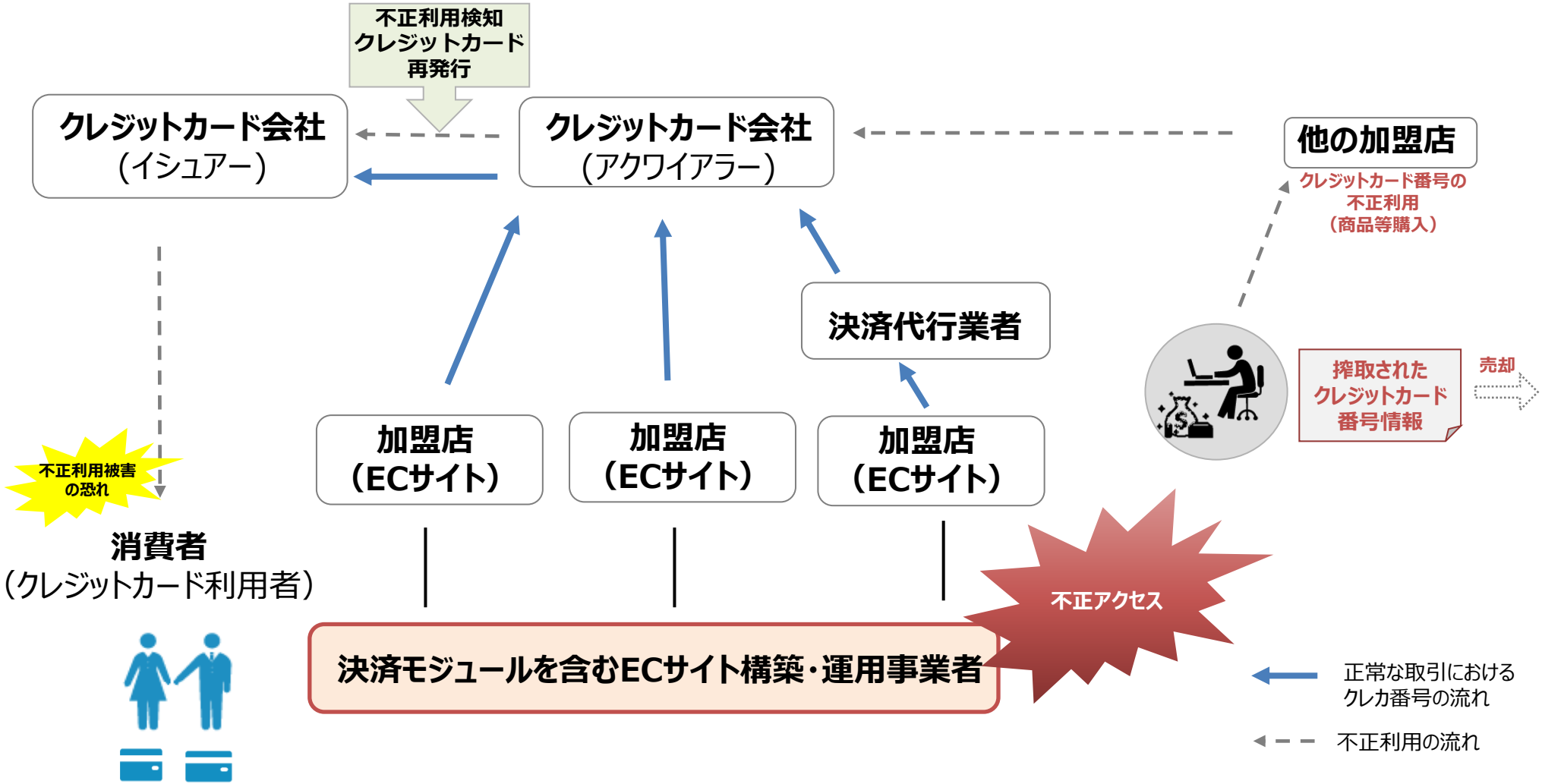
②決済画面
（ECサイト：送信処理が改ざん）
↓
③カード番号入力画面
（正規・搾取用決済画面）
③’搾取用サーバにカード番号送信
③ 決済代行サーバにカード番号送信
↓
②決済完了画面
（ECサイト）



2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会　資料３より引用

1．漏えい事案②：EC決済システム提供者での漏えい（概要）

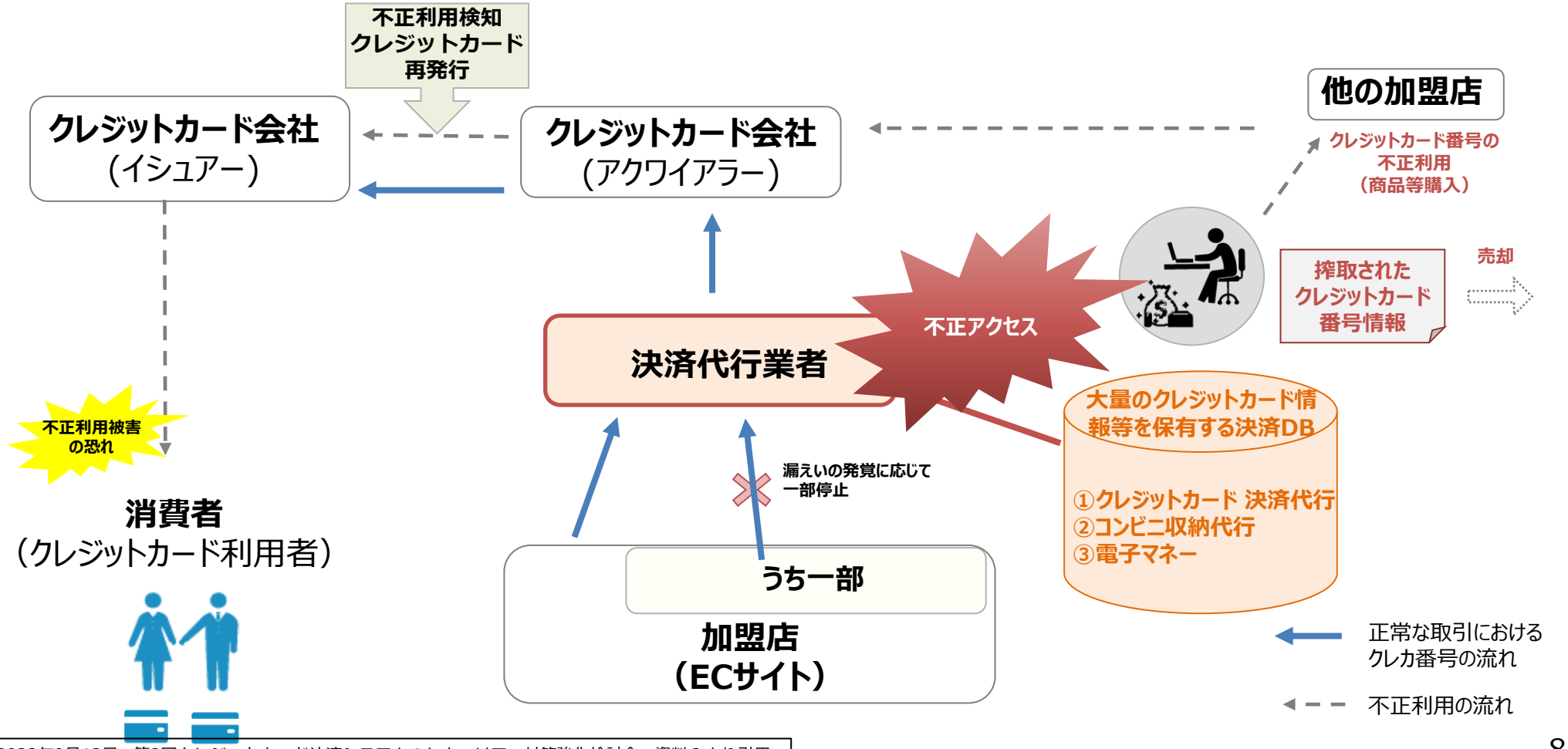
- ECサイトでの漏えいは、決済モジュールを含むECサイトを構築・運用する事業者のサーバーへの不正アクセスを起因とするものも発生。この場合、**一事案であっても、漏えいの規模が広くなる**（関連するECサイトは約９事業者）。



2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会　資料３より引用

1．漏えい事案③：PSP（決済代行業者）での漏えい（概要）

- クレジットカードの決済代行業者の**大量の情報を保有するデータベース**（約46万件のクレジットカード番号等を含むトークン方式クレジットカード決済情報データベース、約240万件のクレジットカード番号等が含まれる決済情報データベース）**への外部からの不正アクセス**により、同社が運営する複数の決済サービスにおいて、決済情報の大規模な漏えいが発生。令和２年法改正後、初めての事案。

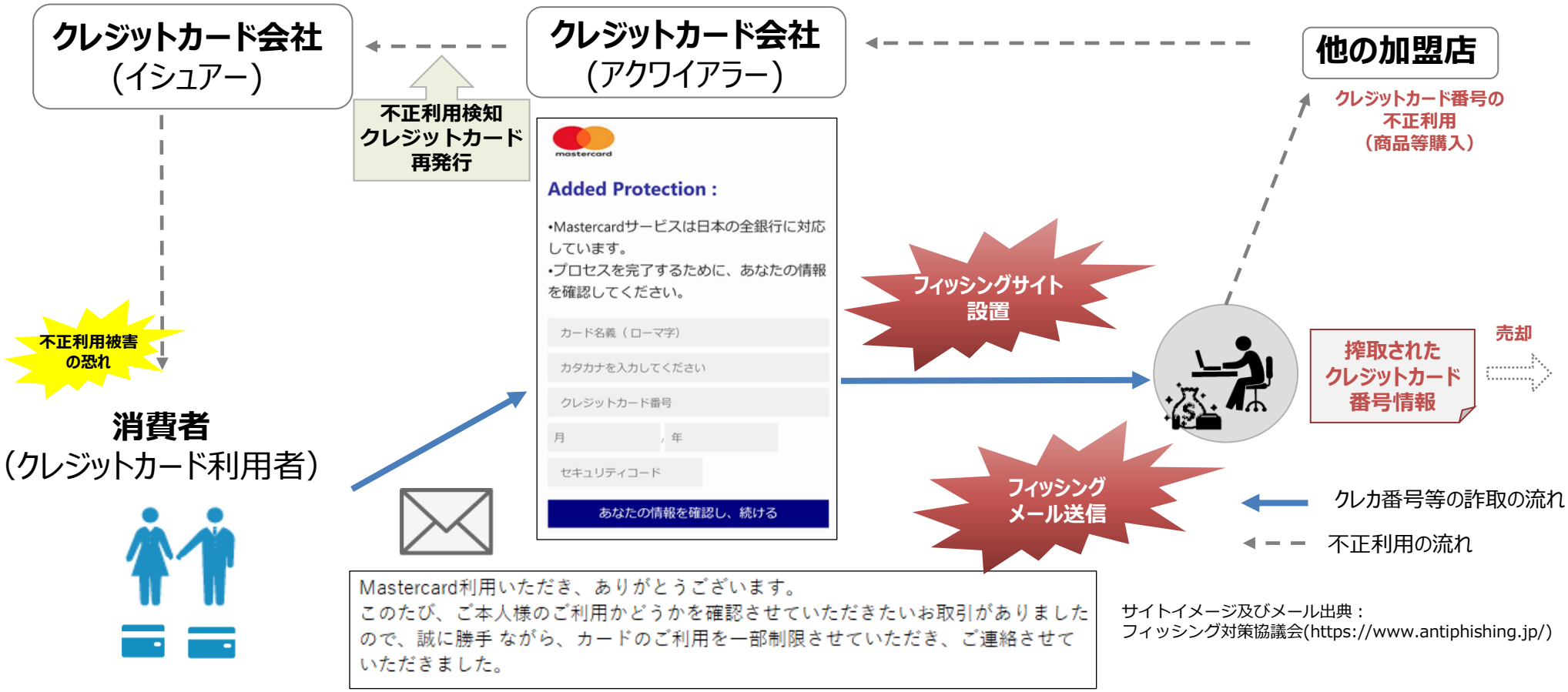


2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会　資料３より引用

1．漏えい事案④：消費者（フィッシング被害）

2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会 資料6より引用

- サイバー攻撃によるクレジットカード番号盗用以外にも、**消費者自身が偽サイトにクレジットカード番号やID・パスワード等を入力する**フィッシングによるクレジットカード番号等の漏えい事案も存在。

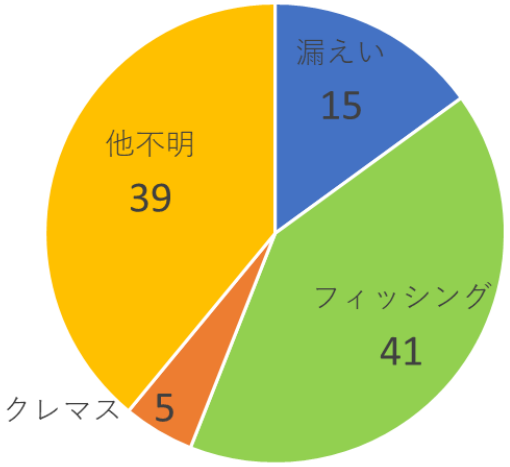


サイトイメージ及びメール出典：
フィッシング対策協議会(https://www.antiphishing.jp/)

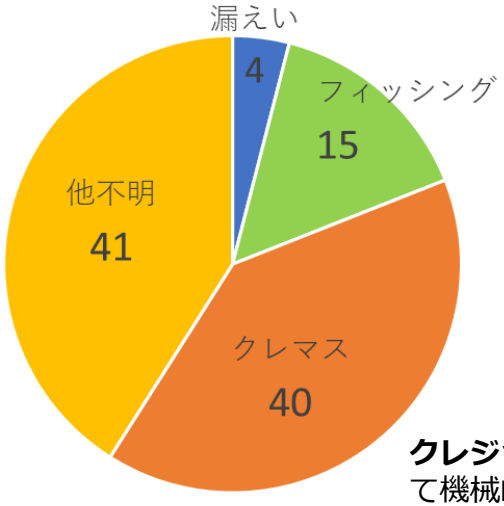
2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会 資料２（JCA提出資料）より引用

番号盗用の不正手口（加盟店からの漏えい、クレジットマスター、フィッシング）の割合【クレジットカード会社２社のサンプル調査】

【A社】



【B社】



クレジットマスター・・・規則性を悪用して機械的に生成した多量のカード番号等の有効性をECサイトを介して確認し、有効なカード情報を不正利用する手口

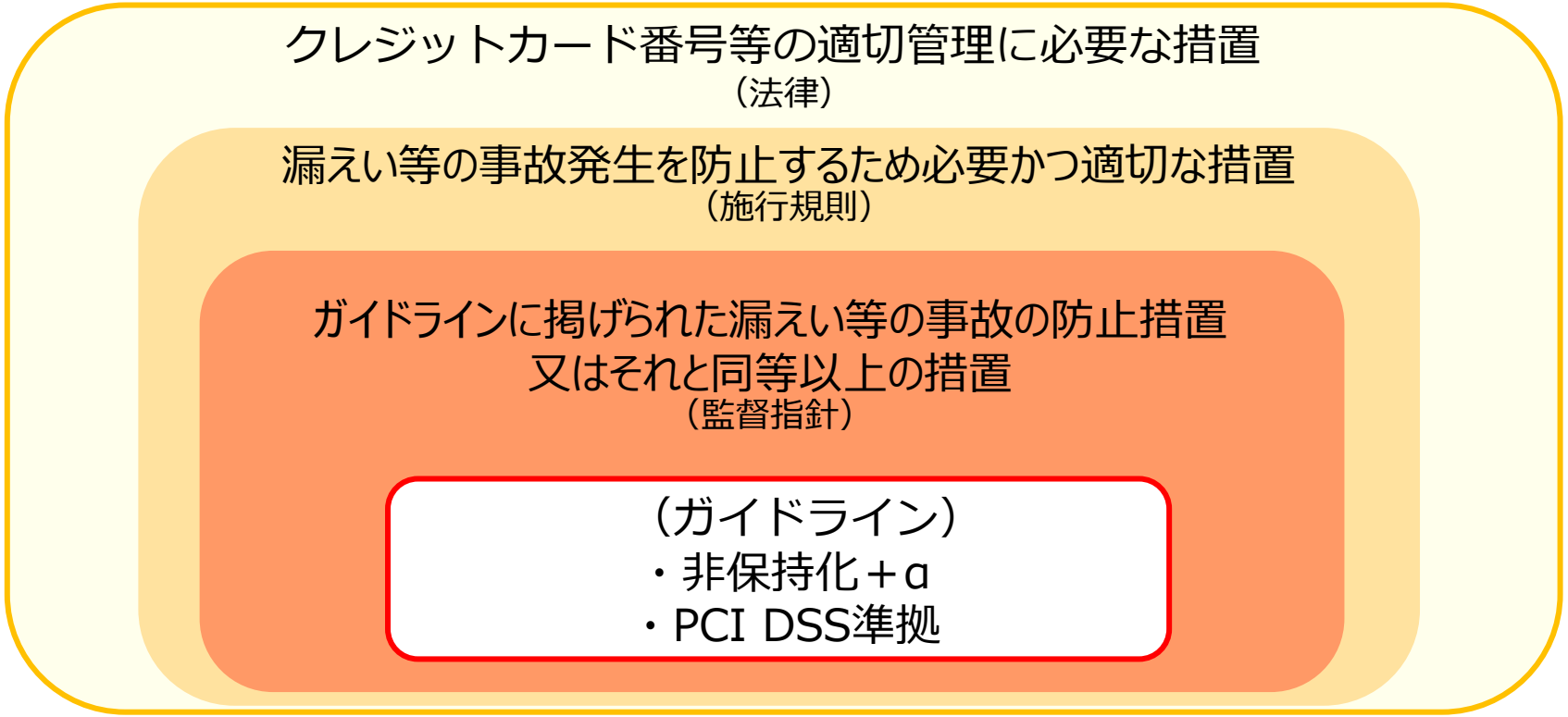
※A社は2021年暦年、B社は2021年度で集計した割合

利用者や加盟店へのヒアリング等により番号盗用の不正手口別の割合を把握できている2社に対して、当協会がヒアリングによるサンプル調査（件数ベース）を実施。

2．対策①：EC加盟店での適切管理

2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会　資料３より引用

- これまで、EC加盟店に求めるクレジットカード番号等の適切管理は、クレジットカード番号等に固有の適切管理として、クレジットカード情報を保持する場合はPCI DSSの準拠、保持しない場合は「非保持化」をPCI DSS準拠に並ぶ措置としてきた。
- しかしながら、今後は、EC加盟店において、漏えい等の事故を防止する必要な措置として、「非保持化」の対策だけでは不十分なものとして、クレジットカード番号等に固有のセキュリティ対策ではないものの、大前提として、まずはECサイト自体の脆弱性対策を講ずることを求めていくことが考えられる。



2．対策②：アクワイラー等によるEC加盟店への加盟店管理

2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会　資料３より引用

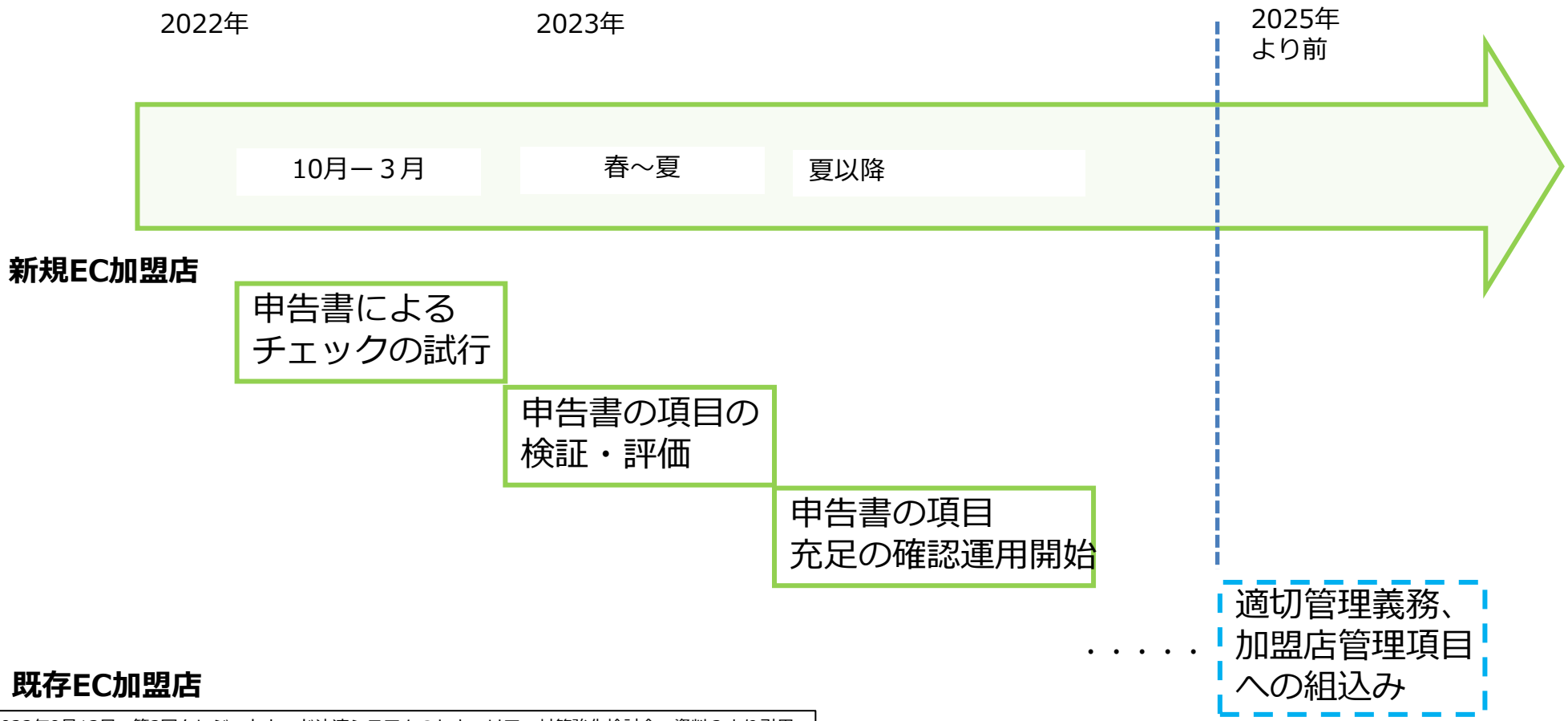
- これまで、アクワイアラー等は加盟店調査の一環として、EC加盟店との加盟店契約締結時に、いわゆるクレジットカード番号等の「非保持化」又は「PCIDSS」の実施状況を確認し、「非保持化」の方針を確認すれば、それ以上の管理状況は問うていなかった。
- 現在、クレジット取引セキュリティ対策協議会（協議会）において、ECサイトの脆弱性対策を念頭に置いた議論がなされており、アクワイアラー・PSP等が新規にEC加盟店との加盟店契約する前に、セキュリティ・チェックリストによる対策の実施状況の申告を求め、その内容を確認する取組の試行の運用を2022年10月から開始することとしている。
- 試行の結果、効果検証・評価を行った上で、本取組を継続し、その結果、EC加盟店のセキュリティ水準の引上げられることが期待されている。

セキュリティ・チェックリストに基づく対策措置状況申告書の観点

①システム上の設定の不備への対策
②脆弱性対策
③マルウェア対策及びウイルス対策

2．対策②：クレジットカード番号等の適切管理義務の引上げに向けて

- 協議会での取組の結果も踏まえ、行政としても、将来的に、これらを、EC加盟店自体のクレジットカード番号等の適切管理として適切管理義務のセキュリティ水準の引上げ、またアクワイアラー等による加盟店管理として加盟店調査対象事項の対象の拡大として、法的義務に引き上げていくことが考えられる。



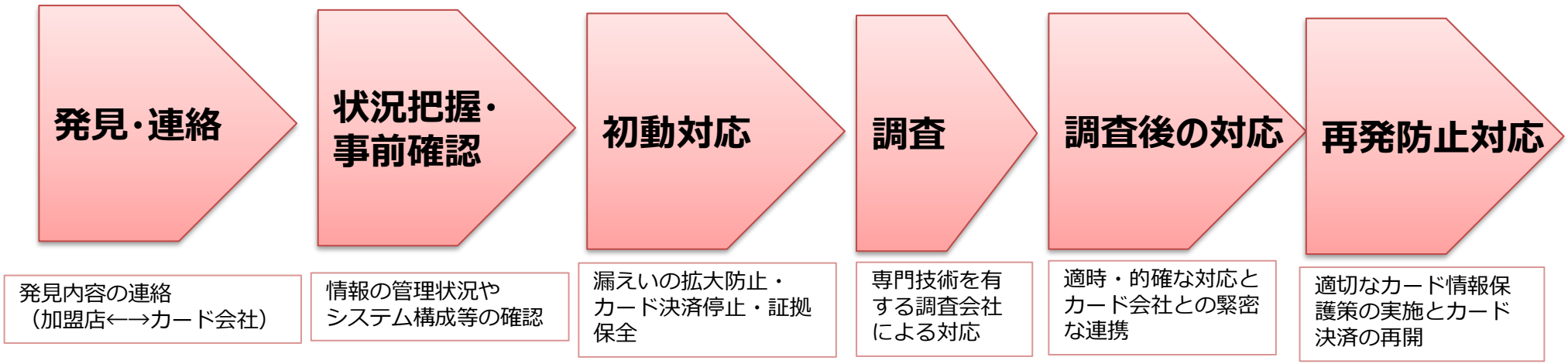
2022年9月13日　第2回クレジットカード決済システムのセキュリティ対策強化検討会　資料３より引用

3．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

- 「クレジットカード・セキュリティガイドライン」の関連文書として、加盟店向けに、クレジットカード情報が漏えい（懸念含む）した際の対応ポイントを、日本クレジット協会で策定。
- 情報漏えいの被害を最小限に抑え、顧客を保護するため、状況把握等と関係団体への報告が求められている。

概要

基本的な対応の流れは、以下の通り



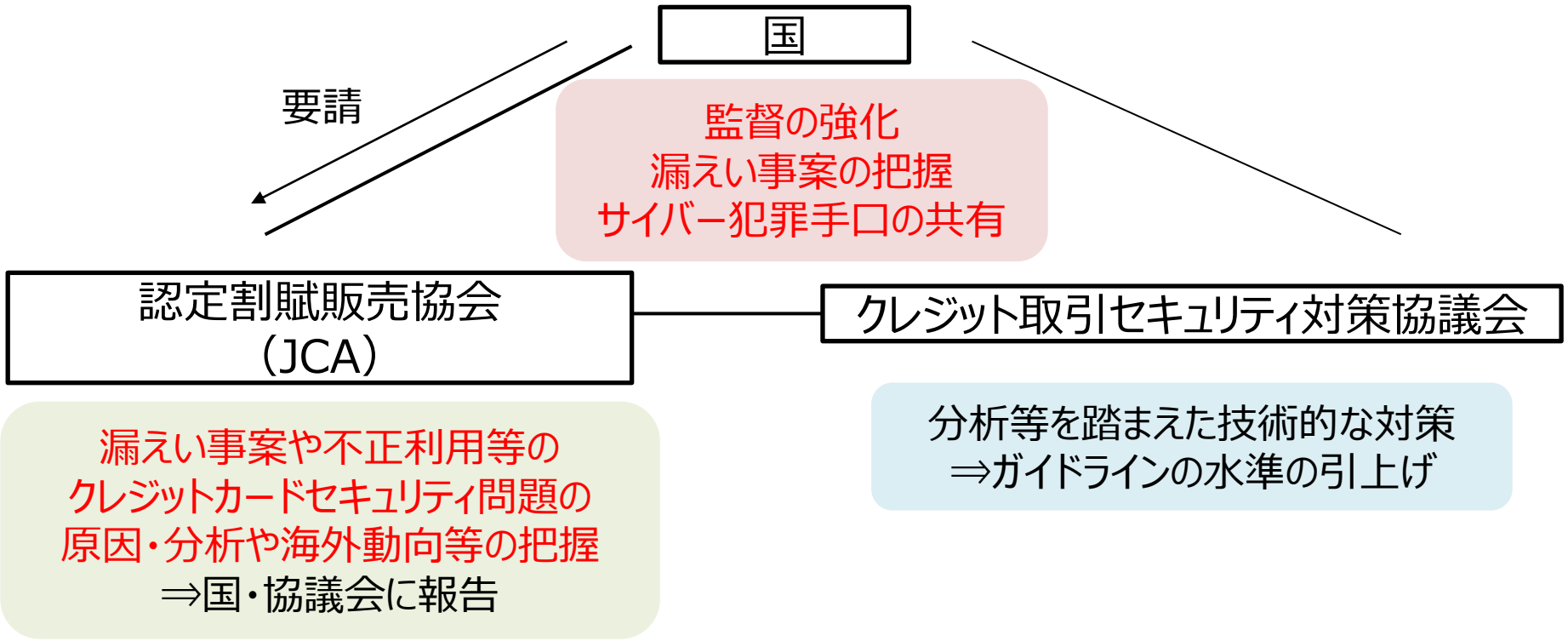
初動対応として、**「個人情報保護委員会等への報告（速報）」**について、
調査後の対応として、**「個人情報保護委員会等への報告（追完）」**や**「警察への被害届出」**について、対応することが記載されている。

これらは、付録の「対応チェックシート」にも記載され、対応漏れの防止が図られている。

2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料6より引用

４．クレジットカード業界のセキュリティ対策に関する体制強化に向けて

- 業界として、次の漏えいや不正利用を防止するため、国としても監督を強化するほか、業界内でクレジットカード番号等の漏えい事案や不正利用の原因・分析を把握するための仕組み、これを踏まえたクレジットカード業界内への周知や再発防止の対策強化をはかっていくことが考えられる。

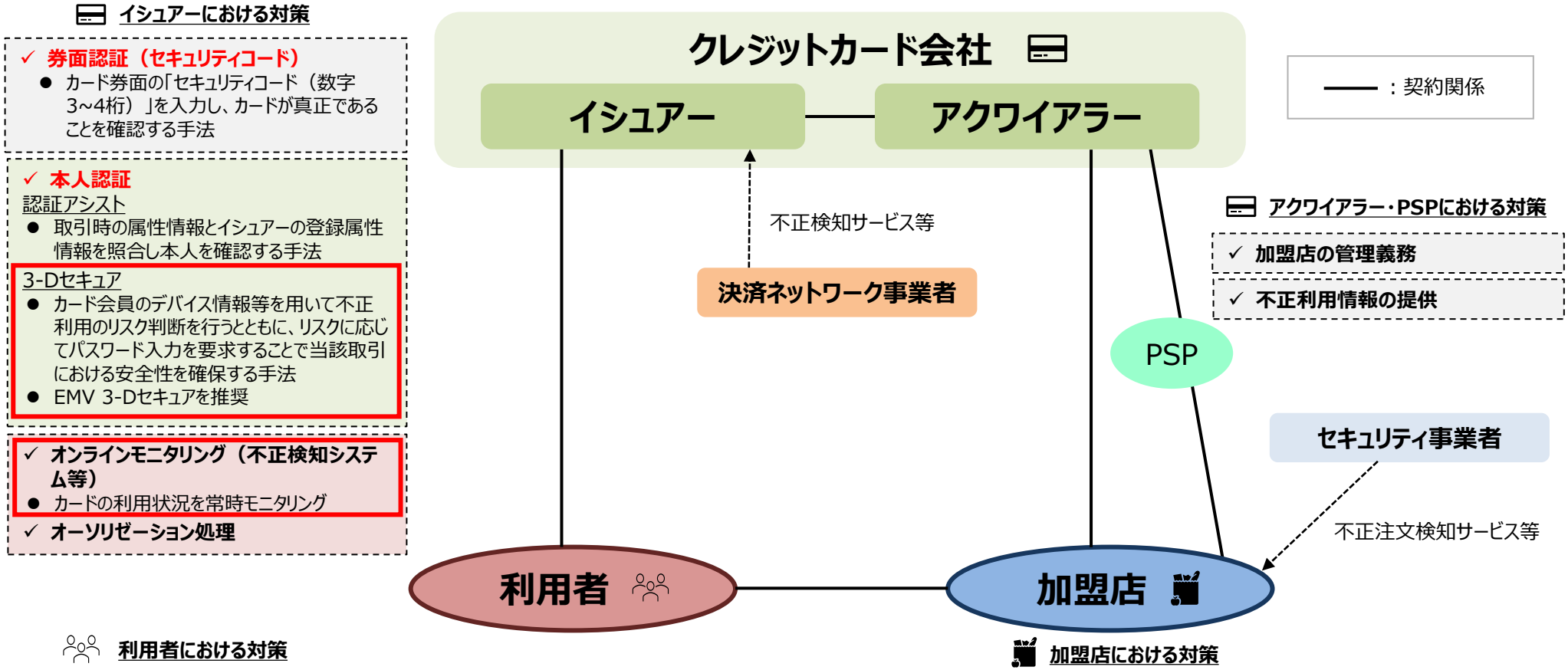


2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料6より引用

Ⅱ.クレジットカード番号等不正利用対策の強化

1．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。



※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

2022年10月11日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料2より引用

１．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

2022年10月11日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料2より引用

2．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

2022年10月11日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料2より引用

（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**

2022年10月11日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料2より引用

２．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

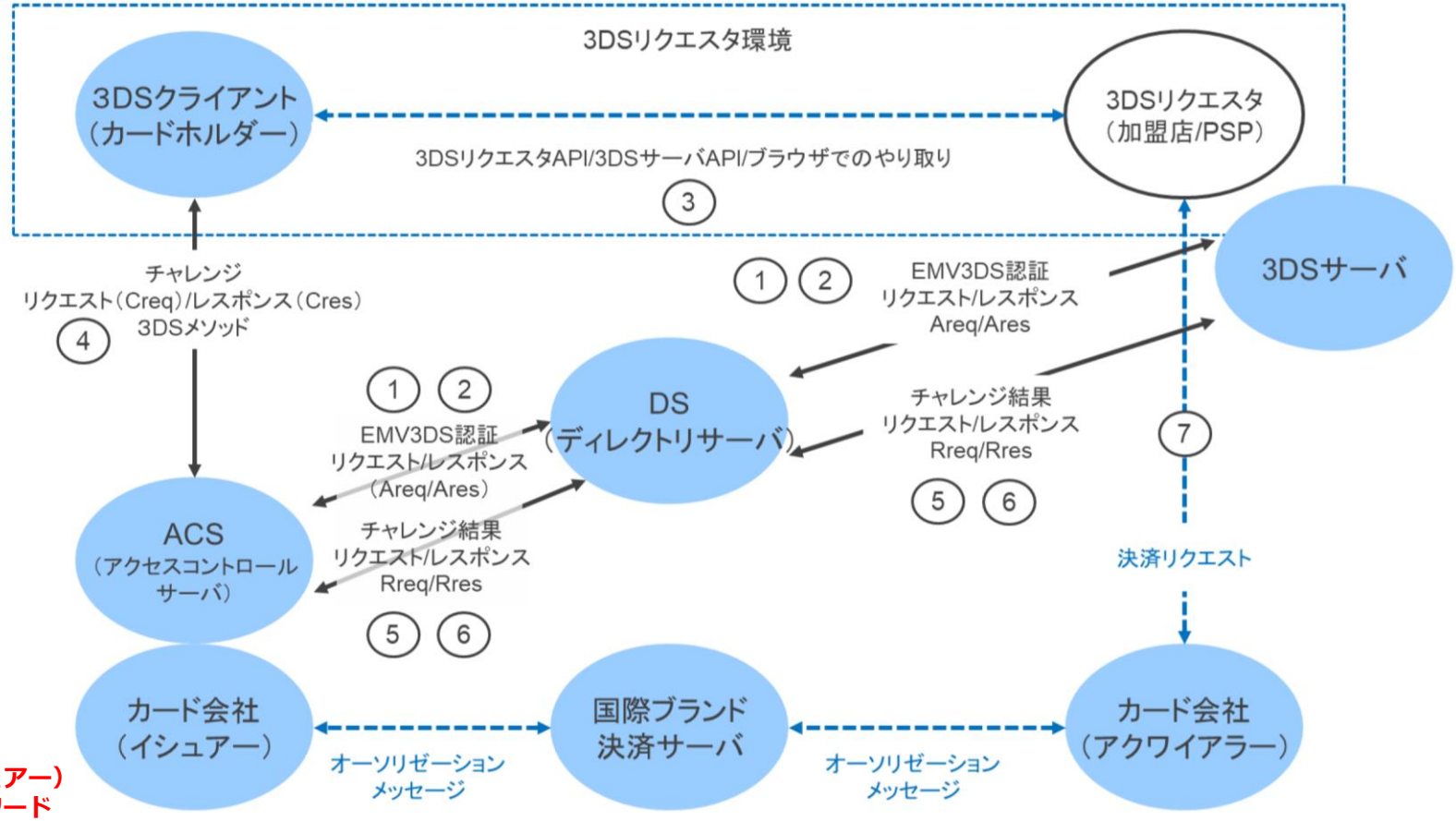
	①利用者であるかの適切な確認	②その他必要な防止措置
対面取引	IC化対応 ー確認できるための端末設備の設置 ーPIN入力	ー
非対面取引	ー	・オーソリゼーション処理のための体制整備 ・善管注意義務

2022年10月11日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料2より引用

（参考）EMV-3DSの仕組み

2022年10月11日　第3回クレジットカード決済システムのセキュリティ対策強化検討会 資料2より引用

- 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）

2022年10月11日　第3回クレジットカード決済システムのセキュリティ対策強化検討会 資料2より引用

- 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。

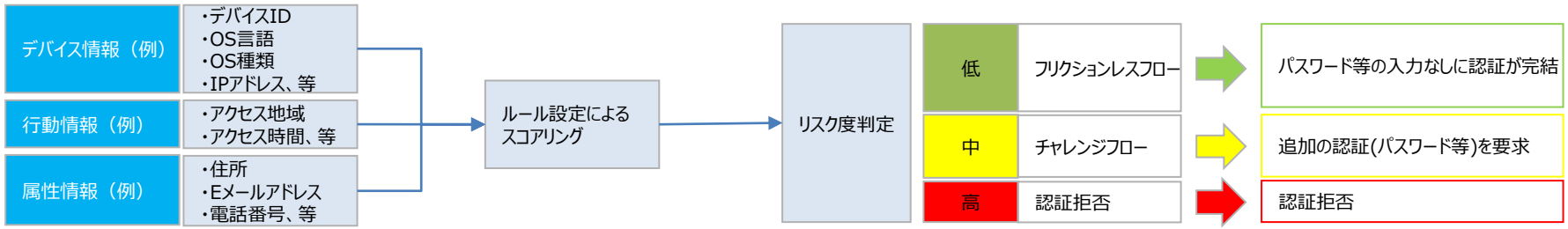
旧３DSとEMV-3DSの比較

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」



3．不正利用情報の共有化の必要性

2022年10月11日　第3回クレジットカード決済システムのセキュリティ対策強化検討会 資料2より引用

- 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。

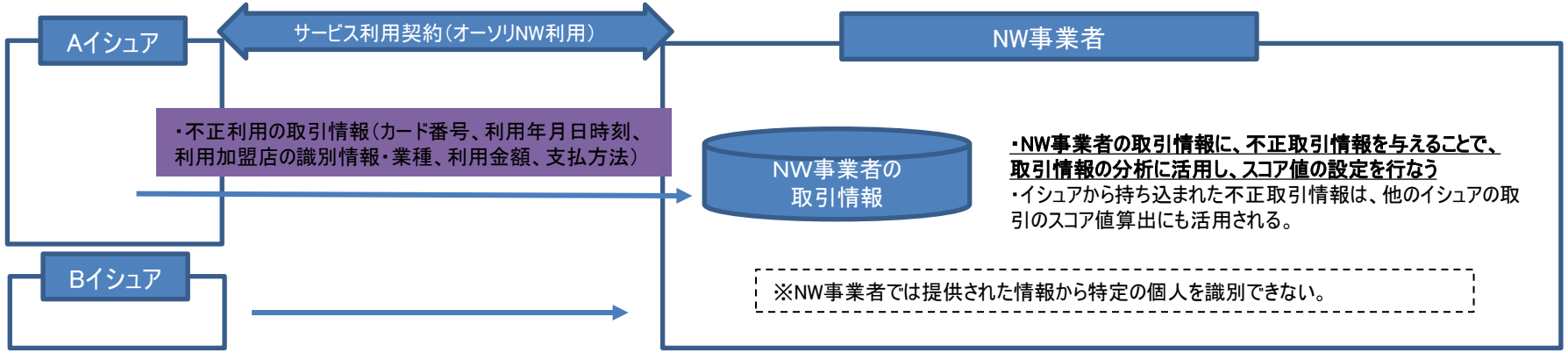
手法	共有する者	共有データ
①利用明細の通知のリアルタイム化	イシュアー・利用者間	個別取引の利用明細
②不正利用情報の共有	案①イシュアー間 案②イシュアー間 案③PSPをハブとした加盟店間	各社で、不正利用／不正利用のおそれありとした取引

3．不正利用情報の共有化に向けたスキームの検討

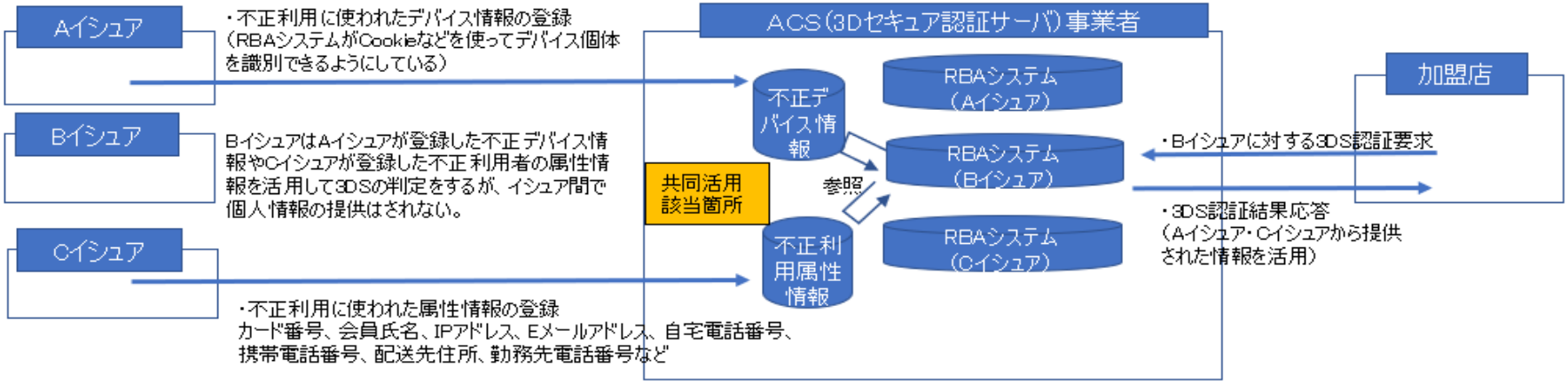
2022年10月11日　第3回クレジットカード決済システムのセキュリティ対策強化検討会 資料2より引用

- 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）



3．不正利用情報の共有化に向けたスキームの検討

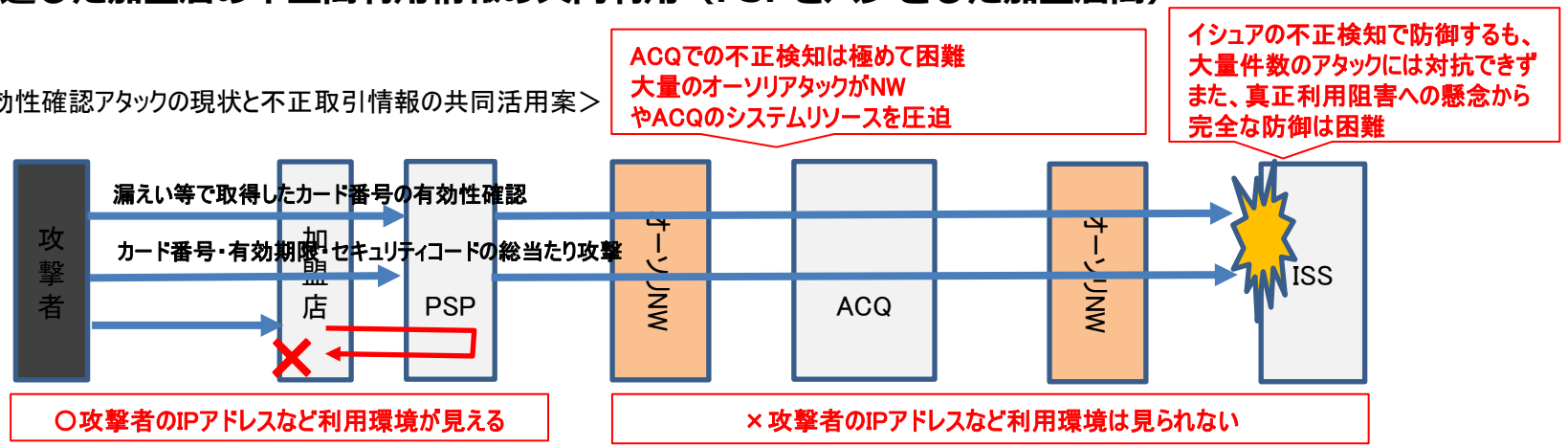
2022年10月11日　第3回クレジットカード決済システムのセキュリティ対策強化検討会 資料2より引用

- 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。

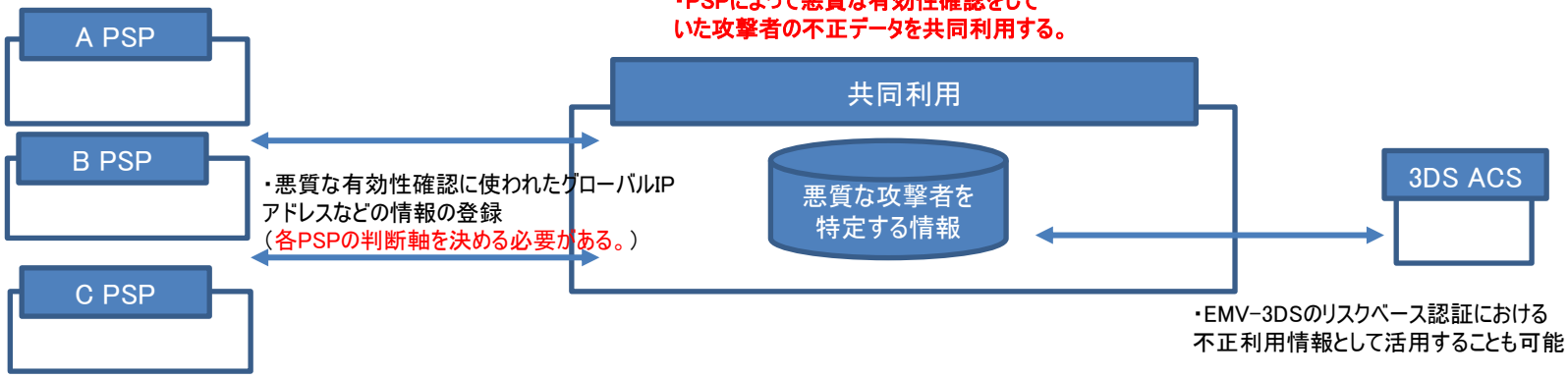
案③PSPを通じた加盟店の不正間利用情報の共同利用（PSPをハブとした加盟店間）

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）

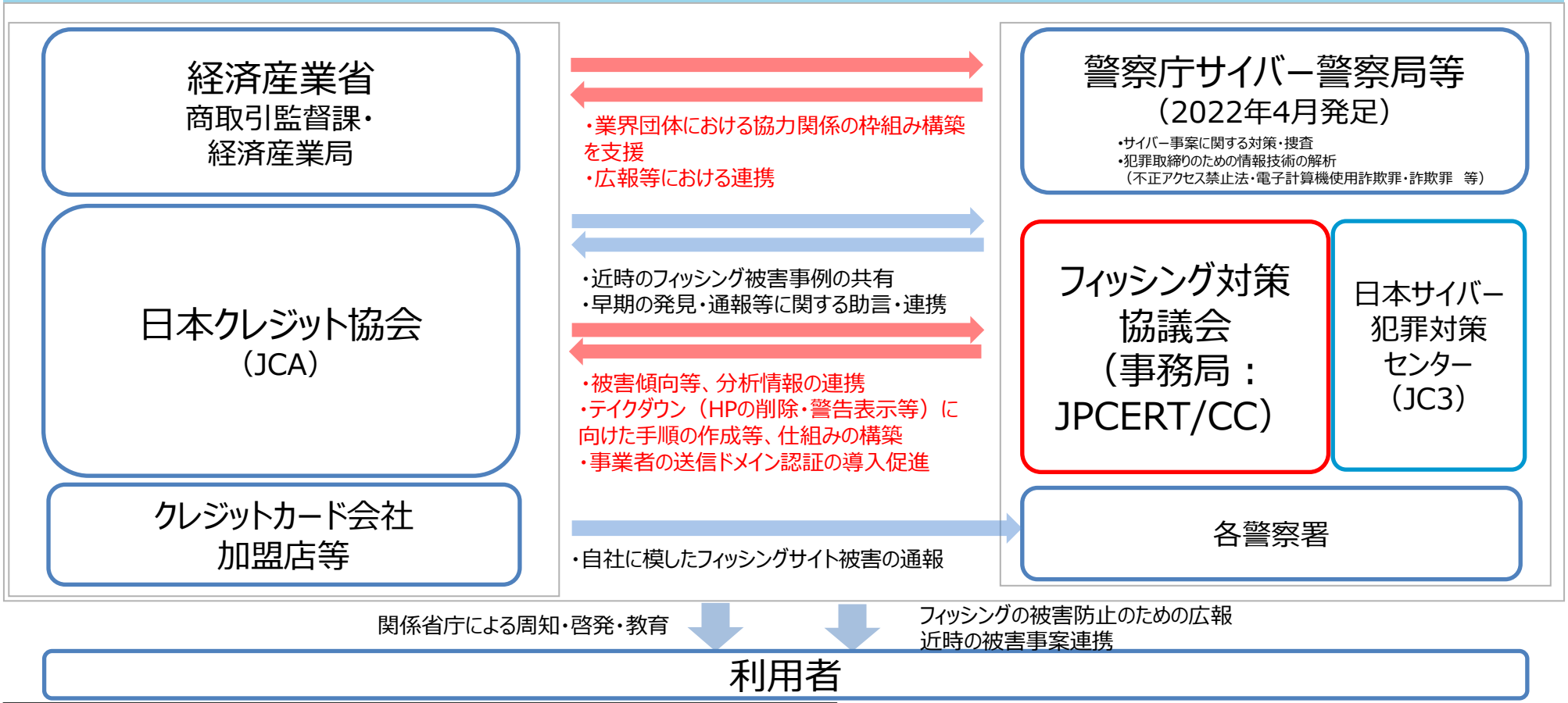


Ⅲ.クレジットの安全・安心な利用に関する周知・犯罪の抑止等

1．関係行政機関・団体との連携強化（フィッシング対策関係）

赤枠・・・取組を強化している主体
赤矢印・赤字・・・新たな取組案
青矢印・黒字・・・これまでの取組

- 従来より、クレジットカード会社等はフィッシングサイトを作成されるなどの被害を認識すると、関係行政機関・団体への報告・相談を行うとともに、所管の警察署にも通報を行ってきた。
- 一方、昨今のEC決済の伸長に伴い、フィッシング報告件数・それに伴う被害が急増。
- 今後は、より効果的な情報連携のため関係省庁間・業界団体間での連携強化のほか、事業者自身の送信ドメイン認証（DMARC）促進等や消費者啓発・広報を行っていくことも考えられる。



2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料6より引用

１．フィッシング対策の強化に向けて

2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料6より引用

- フィッシング技術が巧妙化し、クレジットカード情報を取得しようとするサイトが大半を占めるなか、クレジットカード情報を保護するため、利用者への注意喚起による利用者の対応だけでなく、サイトを持つ事業者自らも対応することが必要。
- クレジットカード業界全体をあげて、まずは、クレジットカード会社をかたるフィッシングサイトのテイクダウンやクレジットカード会社のドメイン管理等による未然防止による多面的・重層的な自衛が必要ではないか。

	これまでの対策	考えられる対策（案）
JCA	利用者への注意喚起	
イシュアー	利用者への注意喚起	●フィッシングサイトの監視 ・フィッシングサイトの検知・テイクダウン ●消費者の誤認防止 ・送信ドメイン認証技術（DMARC等）の導入、ドメインの適切な管理 ・カード情報を入力させるＵＲＬを貼らない
ＥＣ加盟店		●フィッシングサイトの監視 ・フィッシングサイトの検知・テイクダウン ●消費者の誤認防止 ・送信ドメイン認証技術（DMARC等）の導入、ドメインの適切な管理 ・カード情報を入力させるＵＲＬを貼らない
利用者	自発的な注意	●リテラシー ・正規のURLのお気に入り登録やアプリからログインする ・フィッシング対策を講じているカード発行会社、ＥＣ加盟店を選択 ・個人情報の漏えい事案の多発に伴い、自分の情報が既に漏えいしているかもしれない意識をもつ ・フィッシングメールがあること・被害の状況を認知する ・正規メールの見分け方・見分けることの困難さを理解する ●設定 ・メールフィルターの設定

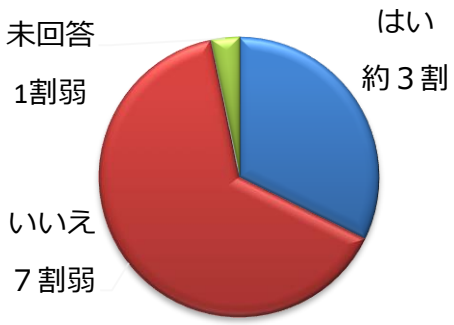
（参考）クレジットカード会社のDMARC等の対策への取組状況

2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料6より引用

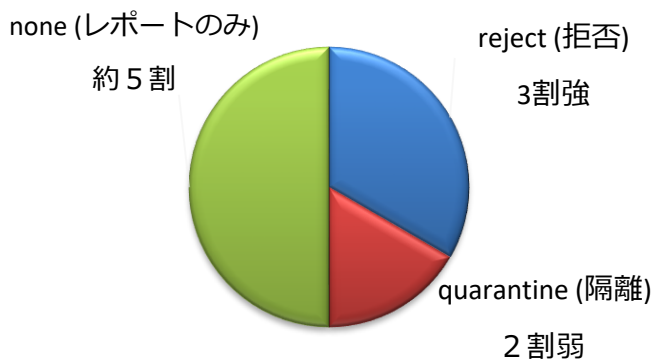
- 主要なクレジットカード会社※の約３割がDMARCを導入。
  うち、受信者に効果のある正式運用(DMARC Policy Enforcement)は、約半数。
  ※事務局で把握している30社程度のイシュアー
- フィッシングメールや偽サイトを確認した場合、約半数が、テイクダウンや関係機関に連絡。

主要なクレジットカード会社での取組状況

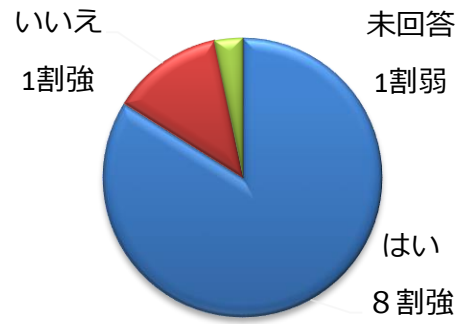
<全てのドメインでのDMARC導入>



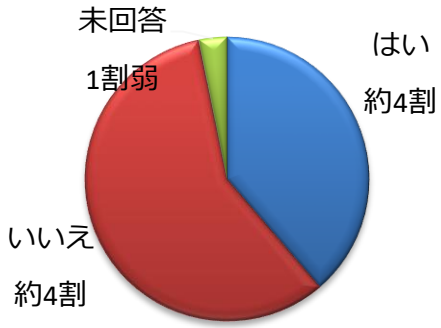
<全てのドメインでのDMARC導入事業者におけるポリシー設定>
※複数回答あり



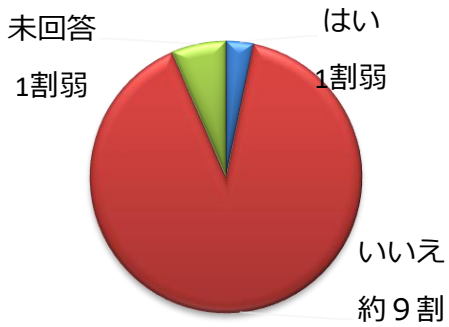
<SPF (Sender Policy Framework)の導入>



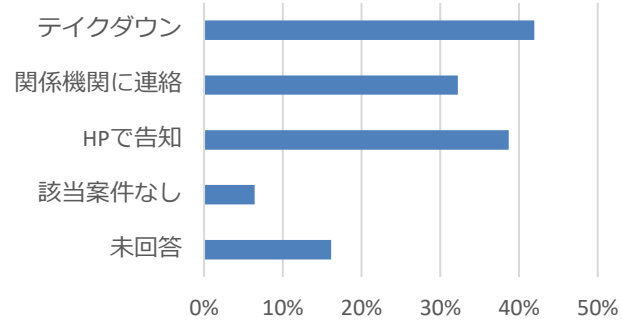
< DKIM(DomainKeys Identified Mail) の導入>



< BIMI の導入>



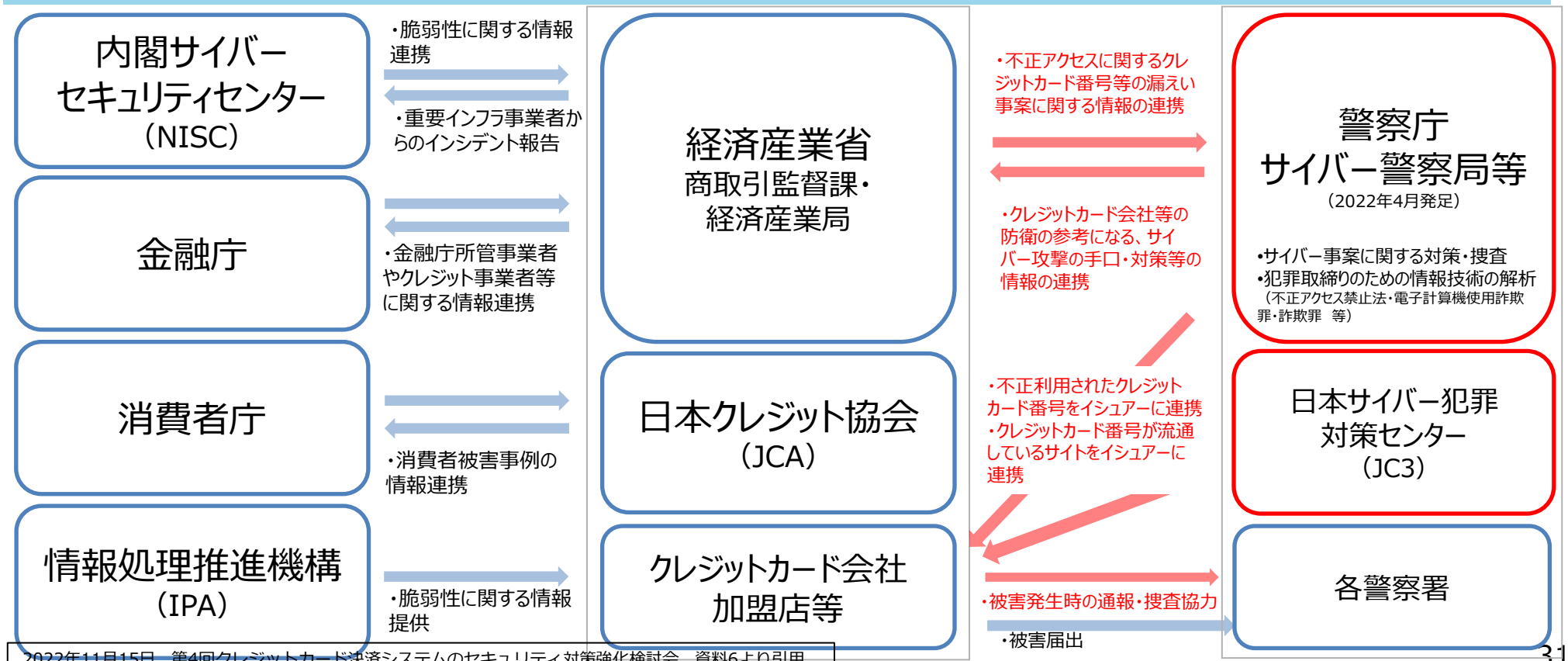
< フィッシングメールや偽サイトを見つけた場合の対応>
※複数回答あり



2．犯罪抑止に向けた関係行政機関等との連携強化（サイバー犯罪）

赤枠・・・取組を強化している主体
赤矢印・赤字・・・新たな取組案
青矢印・黒字・・・これまでの取組

- 従来より、クレジットカード会社等はサイバー攻撃によるインシデント時に関係行政機関・団体への報告・相談を行うとともに、所管の警察署にも通報を行ってきた。
- 一方、昨今は、サイバー攻撃によるクレジットカード番号等の漏えいや不正利用等のサイバー犯罪が急増。
- 今後は、更に犯罪防止に資するべく、より詳細かつ実効的な情報共有を行うため、関係省庁・業界団体間での連携強化の構築も、対策として考えられる。



2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料6より引用

2．クレジットカード決済に関する罰則について（概要）

2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会 資料6より引用

- 偽造クレジットカードによる被害が拡大する中、平成１３年、刑法に支払用カード電磁的記録に関する罪（第１８章の２）を追加。
- カード番号の不正使用被害が相次いだことを踏まえ、平成２０年、割賦販売法にクレジットカード番号等の不正取得、提供、盗用等に係る罰則規定を新設（第４９条の２）。

1. スキミング等による偽造カードの作成・使用

・支払用カード電磁的記録不正作出・同供用（刑法第１６３条の２）

（背景）クレジットカード等の普及に伴い、カード偽造が社会問題化

2. クレジットカード番号等の窃取

・クレジットカード番号等の不正取得・提供（割賦販売法第４９条の２）

（背景）カード会社の従業員等からのクレジットカード番号等の漏えい事件や不正利用事案の発生

・不正アクセス行為の禁止（不正アクセス禁止法第３条・１１条）

※カード番号等窃取のための会員サイトへの不正ログイン等

・他人の識別符号を不正に取得する行為、識別符号の入力を不正に要求する行為の禁止（不正アクセス禁止法第４条・１２条）

3．クレジットマスター

・偽計業務妨害（刑法第２３３条）等

4．窃取したクレジットカード番号等の使用（不正利用）

・ECサイト等：電子計算機使用詐欺（刑法第２４６条の２）、私電磁的記録不正作出・同供用（第１６１条の２第１項、第３項）＋窃盗（第２３５条）
・リアル店舗　：詐欺（第２４６条）、私電磁的記録不正作出・同供用（第１６１条の２第１項、第３項）＋窃盗（第２３５条）

3．安全･安心な利用に向けた利用者への周知

- 不正利用を防止するため、利用明細の確認やEMV 3-Dセキュアの認証用パスワードの設定、クレジットカード番号等の漏えいを防止するため、利用者側でのフィッシング対策について周知。

消費者への周知事項の骨子

※下線は今後新たに呼びかけていくもの

□ 前提

- ➢ 個人情報等の漏えい実態

□ 不正利用被害の防止対策

- ➢ 利用明細･利用通知の確認
- ➢ EMV 3-Dセキュアの認証用パスワードの設定

□ 漏えい防止対策

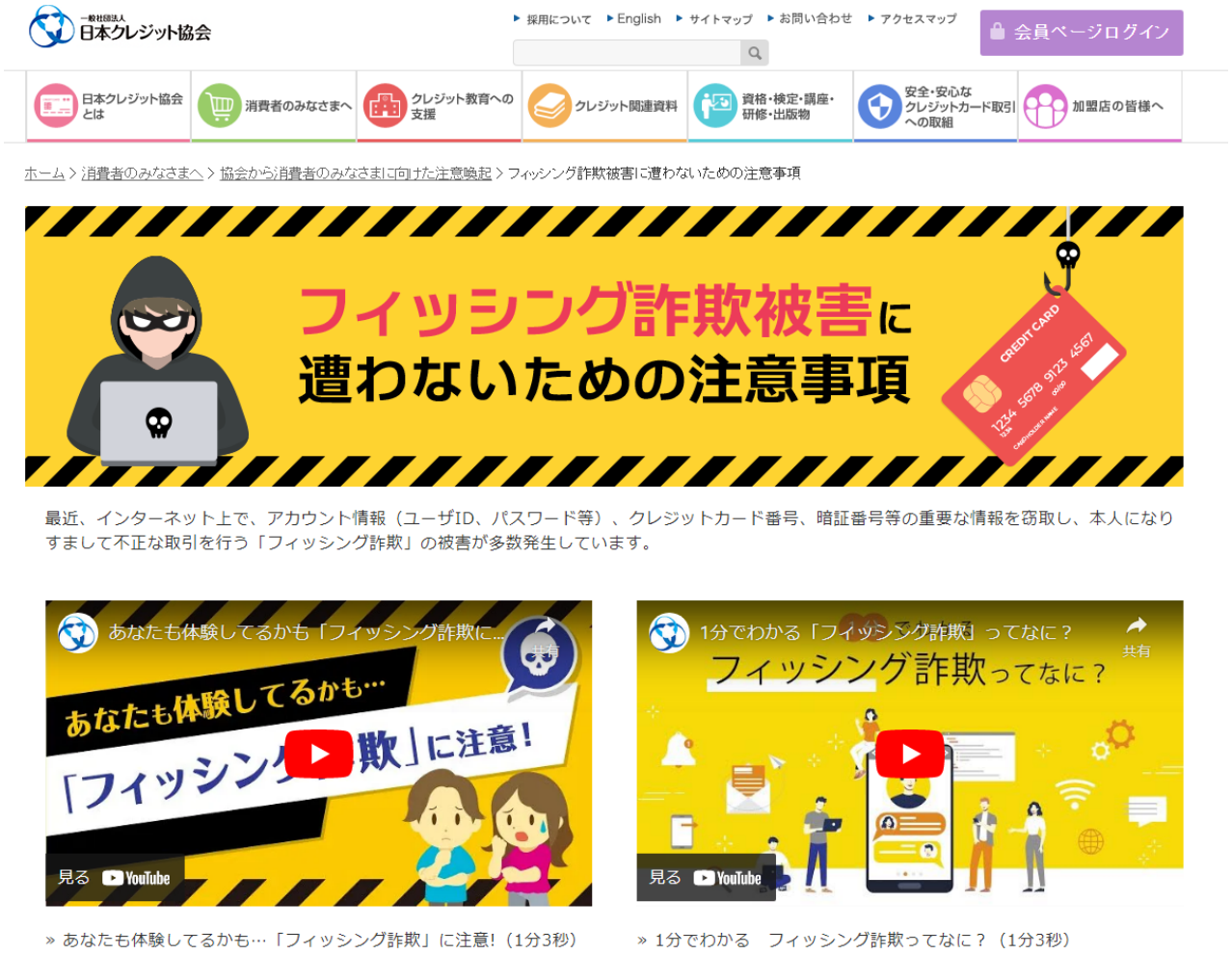
- ➢ 利用者側でのフィッシング対策
  - ー迷惑メールフィルターの設定
  - ー正規メールとフィッシングメールの見分け方を理解
  - ーフィッシングメール、偽サイトを発見した場合の対応（協議会への報告等）
  - ー送信認証技術（DMARC等）、フィルタリング等の対策を取っている事業者の選択

2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料6より引用

2022年11月15日　第4回クレジットカード決済システムのセキュリティ対策強化検討会　資料6より引用

（参考）JCAの利用者向け広報活動

- JCAでは、ウェブサイトにて利用者への注意を呼びかける動画等を公開。



日本クレジット協会「フィッシング詐欺被害に遭わないための注意事項」
https://www.j-credit.or.jp/customer/attention/attention_02.html