資料３

クレジットカード番号等の漏えい防止の強化

令和４年９月13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漏えい対策の全体像

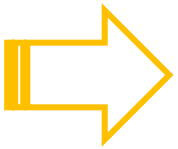
クレジットカード番号等の漏えい対策の位置づけ

- 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漏えい対策は、クレジットカード決済システムの信頼性を確保するため、同システムに携わるすべての事業者による責務であり、クレジットカード番号等の不正利用の未然防止に直接寄与するもの。今回の議論は、特にサイバー攻撃により、事業者からクレジットカード番号等が漏えいするものを焦点とする。

事業者からの漏えい
（サイバー攻撃による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
漏えい防止対策

消費者からの漏えい
（フィッシング）



クレジットカード番号等の
不正利用対策

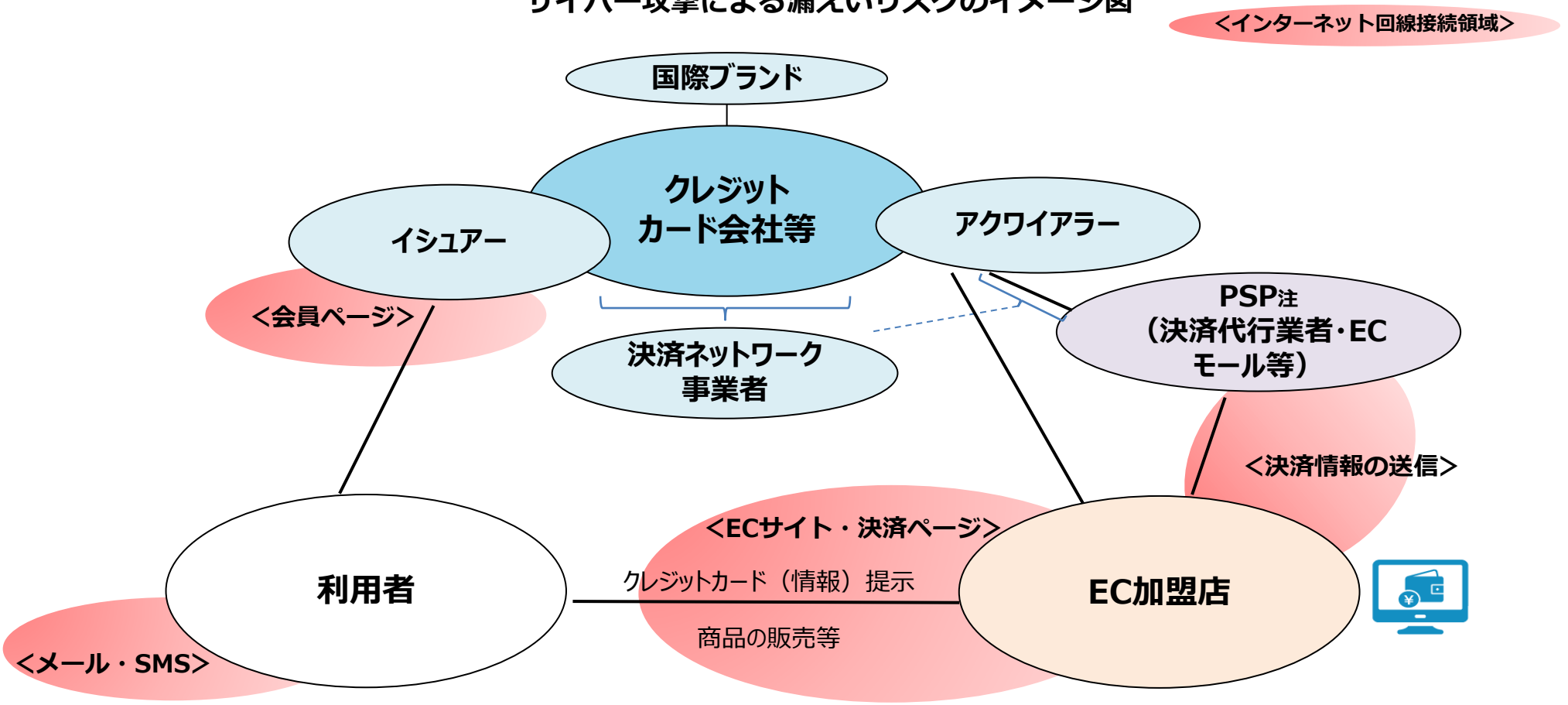
クレジットカード番号等の有効性確認による割り出し
（クレジットマスター）

クレジットの安全・安心な利用
に関する周知・犯罪抑止

クレジットカード番号等の漏えいリスク

- 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。

クレジットカード番号等の適切管理義務等について（概要）

● これまで割賦販売法では、クレジットカード番号等の漏えい対策として、クレジットカード番号等の適切な管理の義務、加盟店調査等の義務を措置。

1．**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・平成28年改正・令和２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**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。
- 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取扱いを委託した者**に対して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**を講じなければならない。

■クレジットカード番号等取扱業者　　数字は法第35条の16第１項各号を示す

平成20年：カード会社からカード番号等が相次いで漏えい
⇒1号　イシュアー（包括信用購入あっせん業者）・３号　アクワイアラー（立替払取次業者）
平成28年：加盟店での漏えい・不正利用被害の増加
⇒2号　加盟店
令和２年：決済代行業者の役割の増大
⇒４号　決済代行業者・７号　加盟店向け決済システム提供事業者
スマートフォン決済等の新たな後払い決済サービス提供主体の登場
⇒５号　利用者向け決済サービス・６号　利用者向け決済サービス委託先

2．**加盟店調査等の義務**（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）

（参考）クレジットカード番号等の適切管理義務の主体者

クレジットカード番号等取扱事業者	対象事業者	セキュリティ対策	違反に対する措置等
1号　・・・ イシュアー 「クレジットカード等購入あっせん業者」（二月払含む）	・クレジットカード会社等	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査等
2号　・・・ 加盟店　（旧法３号） 「クレジットカード等購入あっせん関係販売業者」 「クレジットカード等購入あっせん関係役務提供事業者」		**非保持化** または、PCI DSS準拠	報告徴収・立入検査 (改善命令・罰金なし)
3号　・・・ アクワイアラー　（旧法２号） 「立替払取次業者」	・クレジットカード会社等	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査等
4号　・・・決済代行業者等 「立替払取次業者（３号）のために、加盟店に対して、立替金の交付を行う事業者」	・決済代行業者（ネット取引、対面取引双方） ・EC モール事業者	**PCI DSS準拠 同等以上** ※対面は、非保持可	改善命令・罰金 報告徴収・立入検査
5号　・・・利用者向け決済サービス提供事業者 「利用者から提供を受けたクレジットカード番号等を用いて、次回以降、当該クレジットカード番号等を入力することなく、商品購入等を行うことができるサービスを提供する事業者」	・QR コード決済事業者 ・スマートフォン決済事業者 ・ID 決済事業者等 その他名称の如何にかかわらず、クレジットカード情報と紐づけた他の決済用番号で決済を行う事業者	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査
6号　・・・利用者向け決済サービス委託先 「第５号の事業者が提供する決済サービスについてクレジットカード番号等の管理を受託する事業者」	・第5号事業者からクレジットカード情報の管理を受託している事業者	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査
7号　・・・加盟店向け決済システム提供事業者 「後払い決済において、立替払取次業者にクレジットカード番号等を提供する事業者」（２号に対し提供）	・決済代行業者（ネット取引、リアル取引双方） ・EC システム提供会社 ASP/SaaS として EC 事業者にサービス提供する事業者、EC 事業者に購入プラットフォームを提供する事業者	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査

（参考）クレジットカード会社のセキュリティに関する主な関係法令（法令・ガイドライン等）

- クレジットカード会社のセキュリティへの対応は、クレジットカード番号等の観点から、主に割賦販売法・個人情報保護法、重要インフラの観点からサイバーセキュリティ基本法によって、規律されている。

法令	割賦販売法 ・クレジットカード番号等の適切な管理 ・クレジットカード番号等の不正な利用の防止	個人情報の保護に関する法律 ・個人情報の不正利用や不適切な取扱いを防ぐため、個人情報を取り扱う事業者が遵守すべき義務等	サイバーセキュリティ基本法 ・サイバーセキュリティに関する施策の基本理念の策定 ・重要インフラ事業者の努力義務に関する規定等
方針等	割賦販売法（後払分野）における監督の基本方針	個人情報の保護に関する基本方針	サイバーセキュリティ戦略
	信用購入あっせん業者等に対する検査基本方針及び検査基本計画		重要インフラのサイバーセキュリティに係る第4次行動計画
ガイドライン	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） 割賦販売法におけるセキュリティ規定、実務上の指針	個人情報の保護に関する法律についてのガイドライン（通則編）等 対個人情報取扱事業者 信用分野における個人情報保護に関するガイドライン 対与信事業者	クレジットCEPTOARにおける情報セキュリティガイドライン

（参考）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

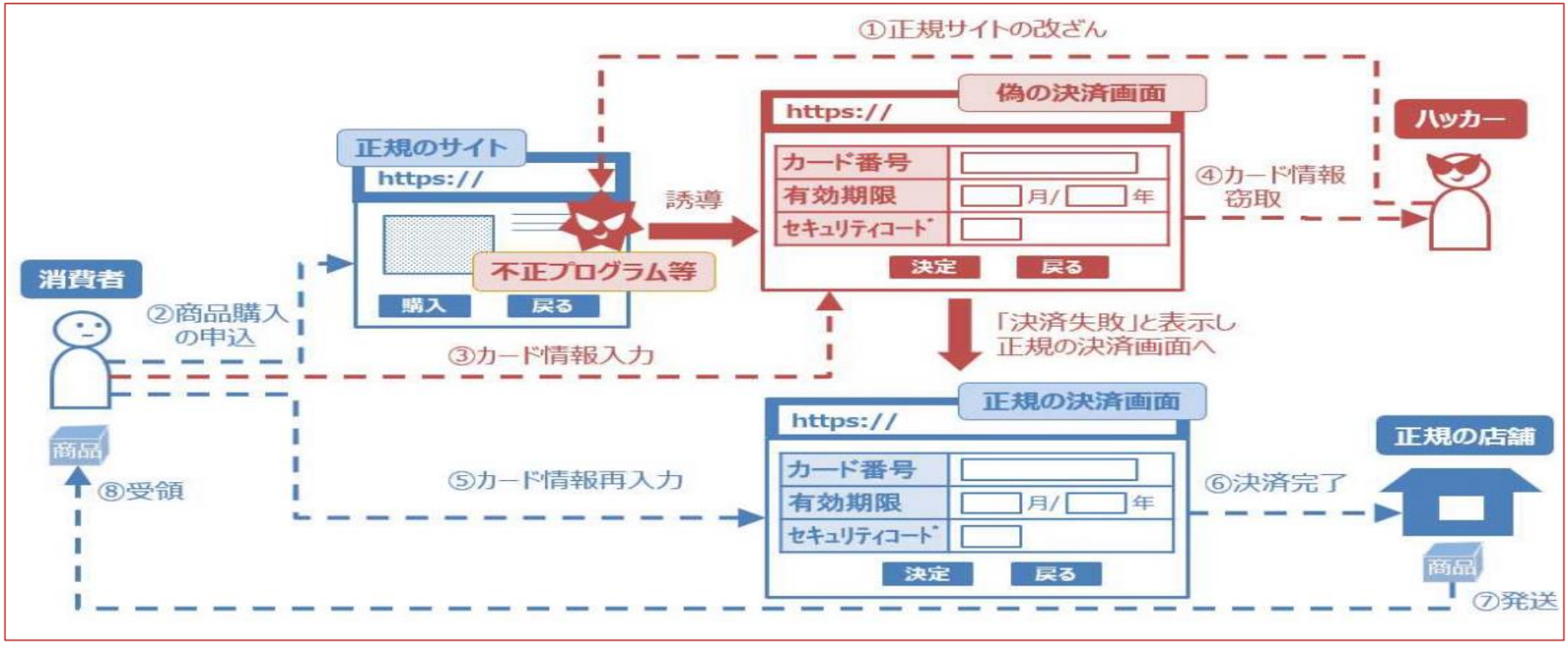
クレジットカード会社等　クレジットカード加盟店　利用者　PSP等

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

２．EC加盟店（2号業者）での漏えい対策

（１）EC加盟店での漏えい（概要）

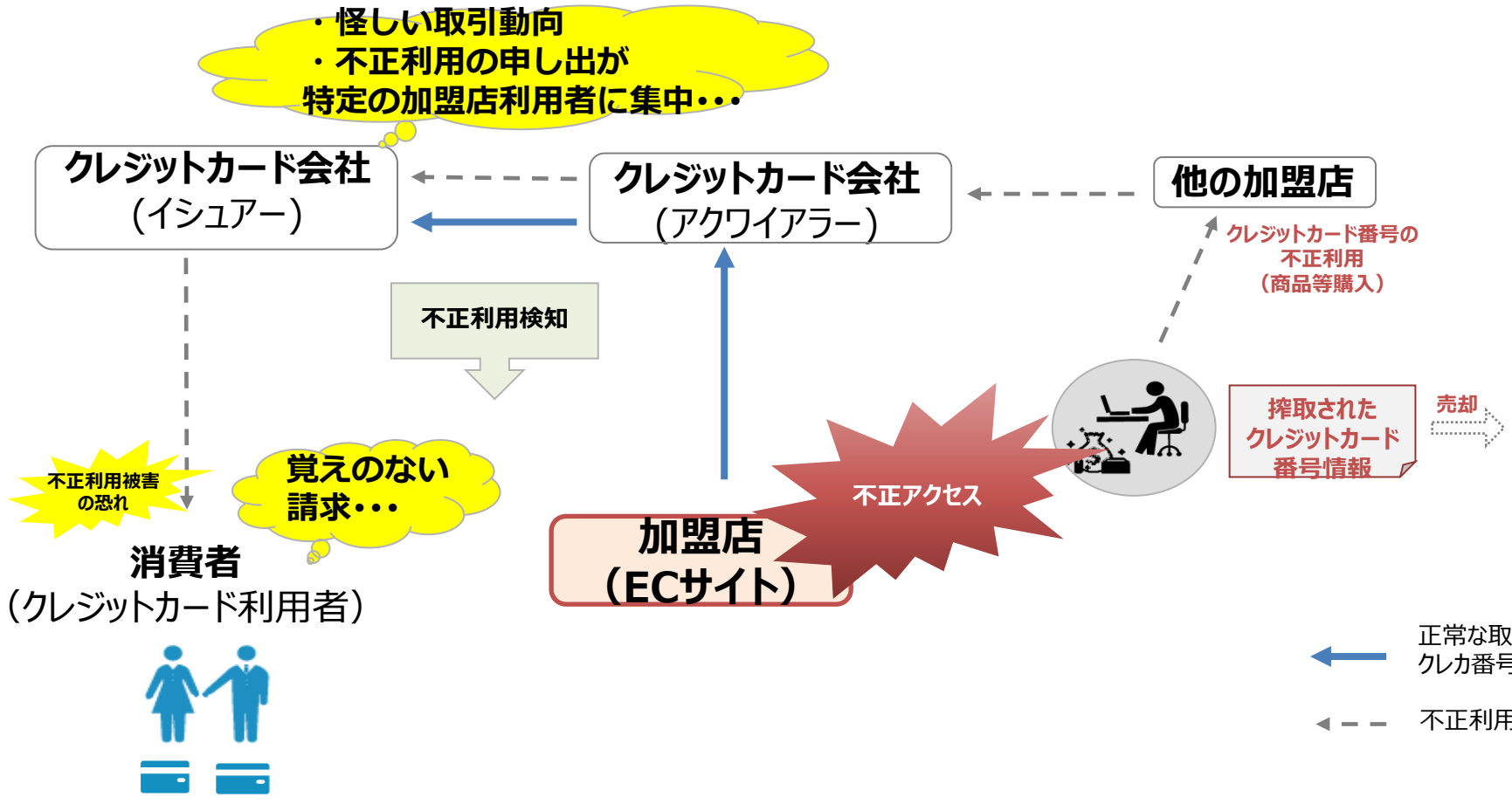
- 特にオープンソースにより構築され、自社（委託先含む）で適切なアップデートを行わないなど、十分なセキュリティ対策を講じていないECサイトの脆弱性を狙った不正アクセス等による漏えい事案が増加。クレジットカード番号等を保持していなくとも、**ECサイト自体が改ざんされることで、不正ファイルの設置や偽の決済サイトへの誘導でクレジットカード番号等が流出。**
- 当省でも加盟店に対する注意喚起を実施(令和元年12月）。IPAとも連携。
- しかしながら、**ECサイトでのサイバー攻撃によるクレジットカード番号漏えい事案は増加**（約２割増（うちオープンソース関連は、約４割増加））。



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）EC加盟店での漏えい（発覚経緯）

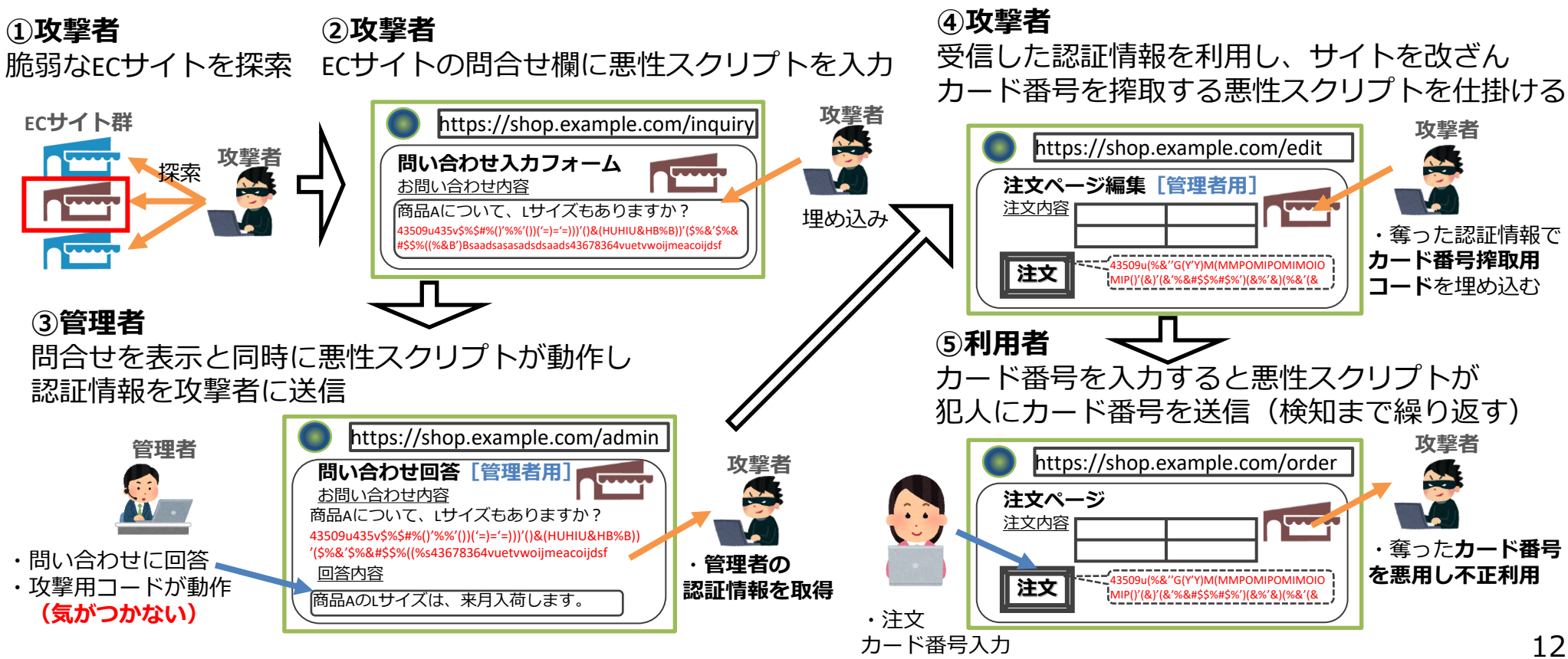
- EC加盟店での漏えいの発覚経緯は、カード会社（イシュアー）によることが主。利用者からの連絡で発覚することもあるが、加盟店自らで早期に不正アクセスを検知できているものはほとんどない。
- 結果として、過去の漏えい事案では、不正アクセスによる漏えいの発生から漏えいの検知までの期間が３か月以上かかるものが約７割以上。数日から数年間に渡るものもある。



（１）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



（２）「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、PCI DSSの準拠か非保持化※の実施を求めてきたところ、**多くのECサイトは非保持化を選択。**

※非保持化：自社で保有する機器・ネットワークで非処理・非保存・非通過の３要件をすべて満たした状態

- 非保持化により、**１事案あたりの漏えい件数は減少**したが、非保持化には不正アクセス自体を防止する効果はないため、**漏えい事案は増加傾向。**

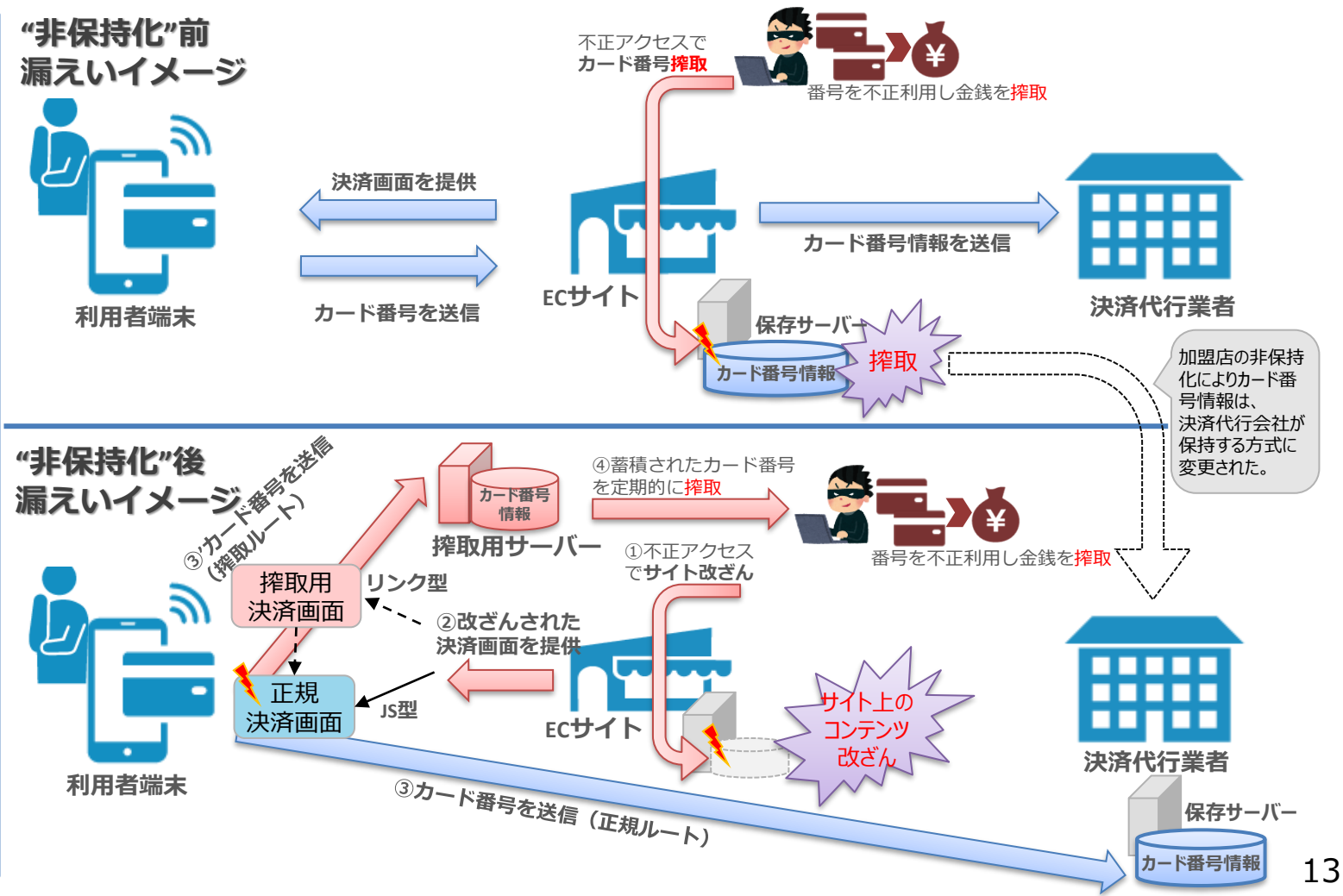
“非保持化”を実現する決済処理方式は「リンク型」と「JS型」の２種類が存在

・「リンク型」改ざん遷移例

②決済画面
（ECサイト：リンク先を改ざん）
↓
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：送信処理を改ざん）
↓
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）



（２）「非保持化」と更なる漏えい対策の必要性

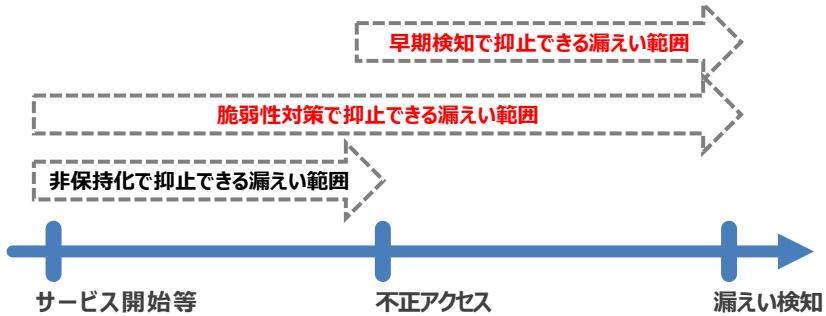
- 昨今の漏えい事案を踏まえると、不正アクセス防止のため、まずは**ECサイトの脆弱性対策**等が必要。
- また、不正アクセスから**漏えい検知までの期間が長期化**し、被害（漏えい件数）が拡大する事例が多いことから、EC加盟店による**漏えい（改ざん検知）の早期検知**が必要ではないか。
- 更に、クロスサイトスクリプティングによる被害拡大防止の観点からは、**ECサイト表示中の外部との通信制限**（CSP※）等も有効ではなか。

※CSP：Contents Security Policy　クロスサイトスクリプティングを防止するブラウザの標準機能。
管理者権限のダッシュやカード番号の外部送信を抑止できる可能性あり。(**EC加盟店のサイト毎の設定が必要**)

必要と考えられる観点	観点に対する対策例
保持しているクレカ番号等の漏えい防止（被害の極小化）	・非保持化
不正アクセスの防止	・サイトの脆弱性対策 ・各種ツールの導入・運用 (IPSやWAF、ウィルス対策ソフトの導入・運用等)
不正アクセス発生後の被害拡大の防止	・不正アクセス時の早期検知（改ざんの定期確認等） ・サイト通信制限（CSP）等による多段階防御

考えられる３つの対策

抑止できる被害の範囲（漏えい防止範囲）



（３）ECサイト構築の現状（ECサイトへの不正アクセスの要因）

- 一般的に、ECサイトでの個人データ等の漏えいの直接的な原因には、 ECサイトの脆弱性に対する不正アクセスが多くを占めるほか、管理者権限へのアクセス制限の不備がある。
- これらの発生理由としては、ECサイト運営事業者の理解不足や委託先任せの姿勢といったリテラシーのほか、技術的ノウハウの不足が事業者から回答されている。

不正アクセスの直接的な原因

SQL インジェクション脆弱性	決済画面の改ざんを引き起こす脆弱性	EC サイトの管理者画面へのアクセス制限不備	その他	分からない
31% （22 社）	37% （26 社）	15% （11 社）	13% （9社）	4% （3社）

不正アクセスの発生理由についての自社の認識

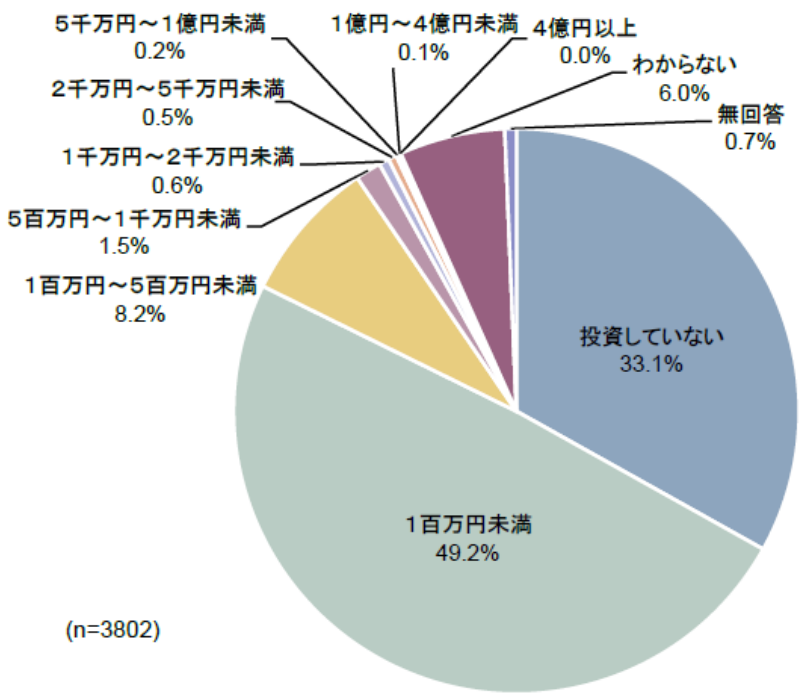
		該当する	該当しない	無回答
①	脆弱性についての理解不足	66% （47 社）	32% （23 社）	1社
②	委託先任せの姿勢	59% （42 社）	39% （28 社）	1社
③	技術的ノウハウの不足	59% （42 社）	39% （28 社）	1社
④	リスク意識の欠如	44% （31 社）	55% （39 社）	1社
⑤	予算・人的リソースの不足	44% （31 社）	55% （39 社）	1社

出典： ECサイトへの不正アクセスに関する実態調査　（令和４年３月個人情報保護委員会）

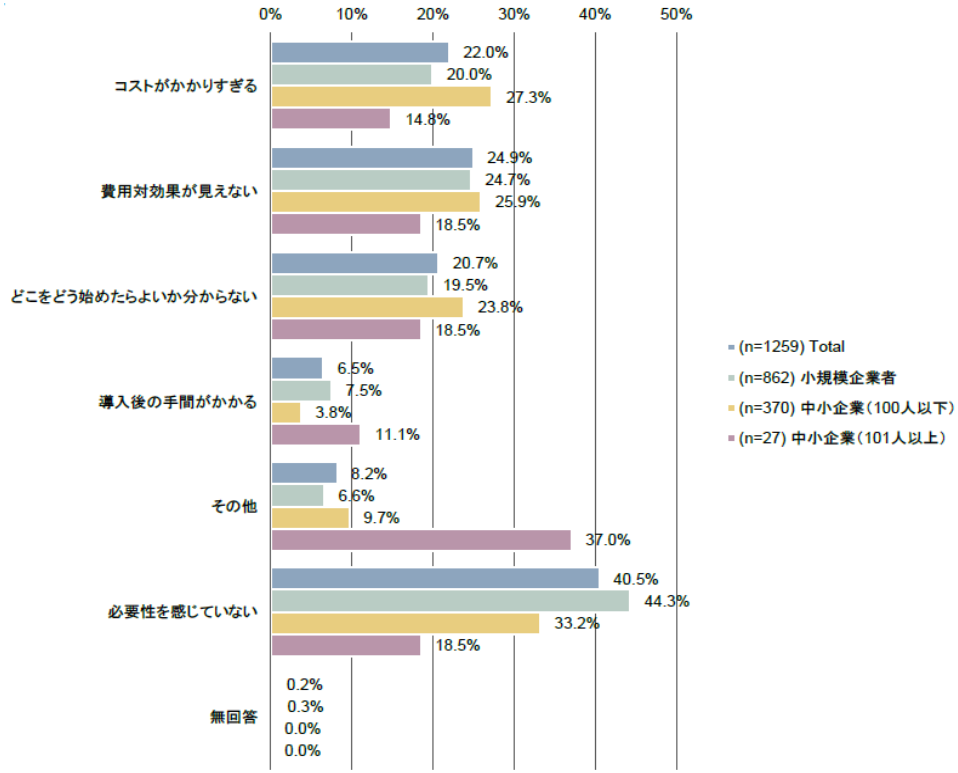
（３）ECサイト構築の現状（中小企業での情報セキュリティ投資）

- 特に中小企業では、情報セキュリティ投資を行っていないと回答している事業者が３割以上。対策の必要性を感じていない等、自ら投資のモチベーションがわきづらいことが窺われる。
- クレジットカード決済を扱う場合には、より高いセキュリティ意識が求められるべきであるが、実際に漏えいが起きるまでは、自分ごととして捉えきれていないことが想定される。

直近過去3期の情報セキュリティ対策投資額



情報セキュリティ対策投資を行わなかった理由（企業規模別）



出典： 2021年度中小企業における情報セキュリティ対策に関する実態調査　（IPA）

（３）ECサイト構築の現状（サイバー攻撃を受けたECサイトの対応）

- サイバー攻撃により、個人データが漏えいしたECサイトのうち一部のサイトには、一定程度の行動変容が見られる。

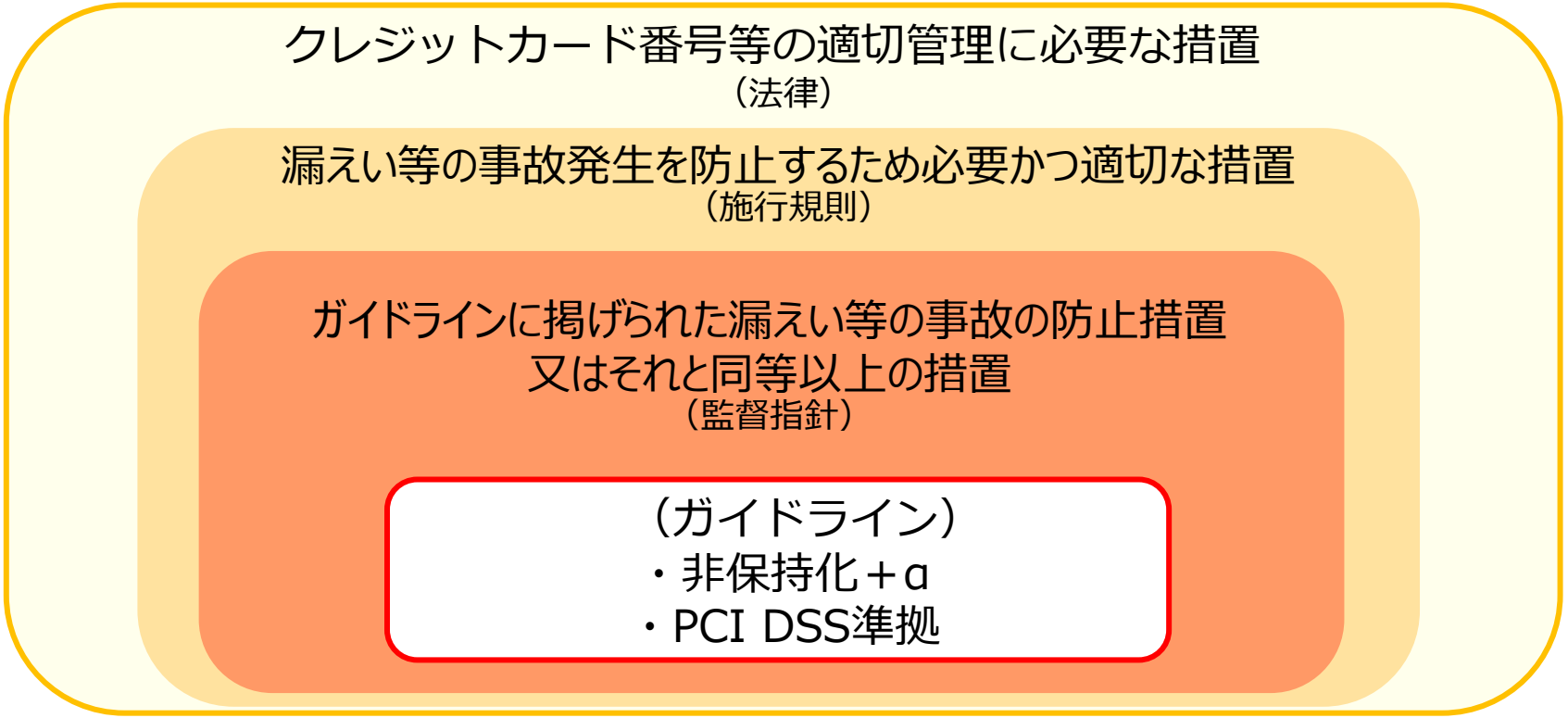
＜漏えい前の対応＞
・ECサイト公開前にECサイト脆弱性診断を実施していなかった（ほぼ全サイト）。
・ECサイト運用中に、脆弱性問題への対応を放置してしまったサイトもある。
・漏えい時のフォレンジック調査に必要となるログやバックアップデータの保存期間が十分でなかったサイトもある。
・インシデントの予兆を感じていたサイトもある。
・外部委託しているECサイトの運用・保守契約がセキュリティの観点から機能していないサイトもある。

＜漏えい後の対応＞
・ASPショッピングカート型やショッピングモール型に移行（70%程度のサイト）。
・WAFやサイト改ざん検知ツールを導入・運用したサイトもある。
・管理者画面へのアクセス制御の強化、二段階認証や二要素認証を導入。
・サイバー保険に加入または加入を検討中。

出典：2022年度EC加盟店サイトセキュリティガイドライン検討委員会　第１回事務局資料（IPA）から抜粋

（４）対策①：EC加盟店での適切管理

- 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。



（４）対策②：アクワイラー等によるEC加盟店への加盟店管理

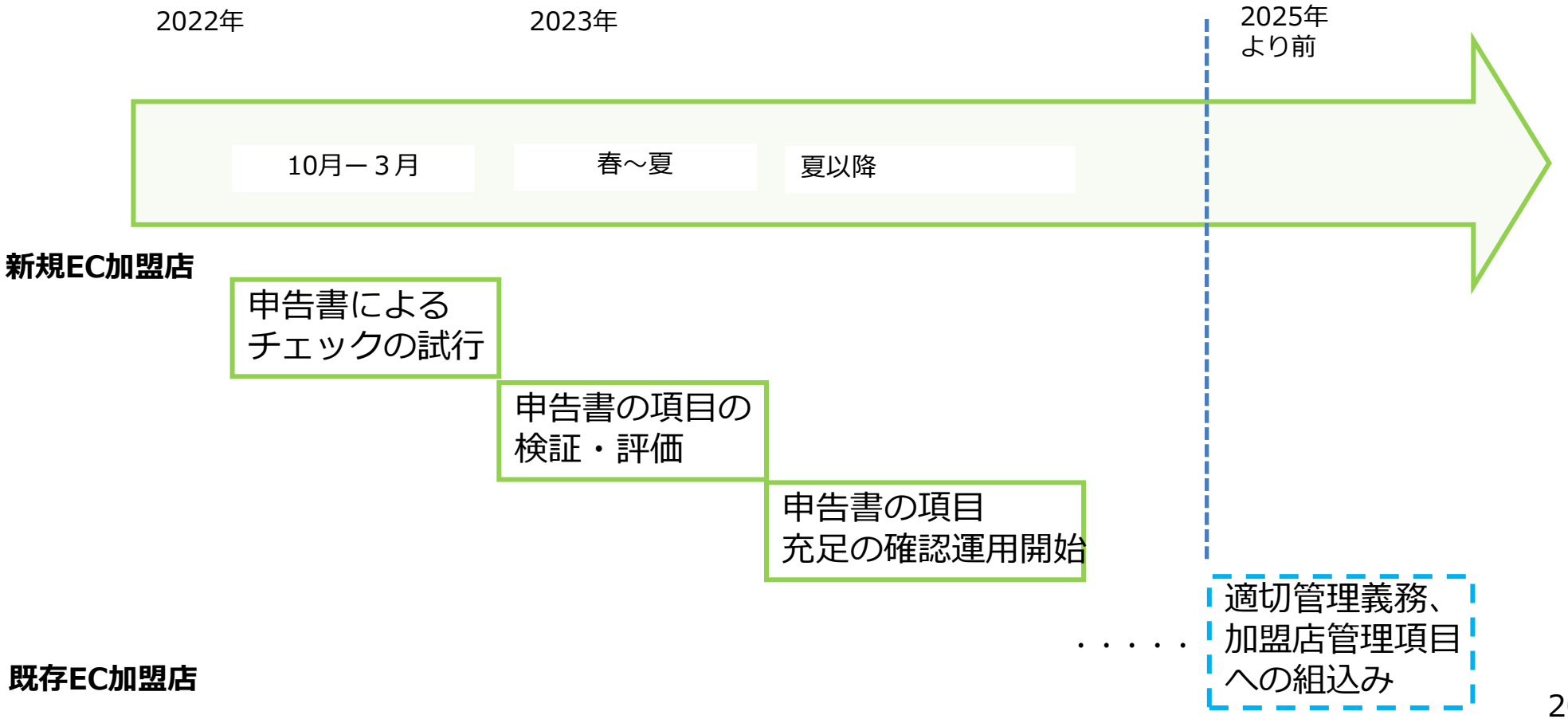
- これまで、アクワイアラー等は加盟店調査の一環として、EC加盟店との加盟店契約締結時に、いわゆるクレジットカード番号等の「非保持化」又は「PCIDSS」の実施状況を確認し、「非保持化」の方針を確認すれば、それ以上の管理状況は問うていなかった。
- 現在、クレジット取引セキュリティ対策協議会（協議会）において、ECサイトの脆弱性対策を念頭に置いた議論がなされており、アクワイアラー・PSP等が新規にEC加盟店との加盟店契約する前に、セキュリティ・チェックリストによる対策の実施状況の申告を求め、その内容を確認する取組の試行の運用を2022年10月から開始することとしている。
- 試行の結果、効果検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

（４）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。



（参考）ECサイトセキュリティ対策促進事業（令和３年度補正）

- 中小企業者等が運営するECサイトについて、システムベンダー等との契約・運営保守状況や脆弱性に関する調査を実施（IPA）。
- サイト運営事業者が特に陥りやすいセキュリティの誤解や対策を明らかにし、ECサイト構築時・運営時に留意すべき事項をまとめたガイドラインやモデル契約の策定・普及を予定。

①実際に被害を受けた企業へのヒアリング
- 被害の原因、事業への影響、被害後の対応、教訓等を把握

②ECサイト関係ベンダーへのヒアリング
- 各ベンダーのセキュリティ対策状況、保守契約のメニュー等を確認

③中小企業の自社構築ECサイトの脆弱性診断
- 募集対象は、自社でECサイトを構築・運用している中小企業
- 診断対象は、事業規模、構築方式、使用パッケージ、業種等を勘案し選定
- 脆弱性診断、ヒアリングによりECサイトのセキュリティ対策状況を確認・把握

来春を目処

ECサイト向けセキュリティ対策ガイドラインの作成
- ①～③の成果を元にガイドラインを策定、普及

ご議論いただきたい事項（EC加盟店での漏えい対策）

２－１：EC加盟店での漏えい対策
総論：昨今のEC加盟店での漏えいを念頭におき、EC加盟店における漏えい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
（１）加盟店の義務履行の担保の在り方
これまで、EC加盟店に対しては、クレジットカード番号等に固有の適切管理として、非保持化、または 保持する場合のPCI DSSの準拠の可否を中心に法的に確認を求めてきたところ。
①今後、EC加盟店に対し、クレジットカード番号等を適切に管理すべき内容として、従前の非保持化対策に加え、その前提となるECサイト自体の脆弱性対策について求めていくこととなるが、これらをEC加盟店の適切管理義務としていくことについて、どのような観点に留意すべきか。

②今後、EC加盟店に対し、不正アクセスの早期検知等についても求めていくことについて考えられるがどうか。

③これまで、加盟店の適切管理義務については、基本的にはアクワイアラー等による加盟店管理の手法によることとし、加盟店に対して改善命令の対象としてこなかった。また、EC加盟店でのセキュリティ対応状況について利用者や市場の目に触れることはほとんどなかった。セキュリティ投資の必要性を感じない EC加盟店もいるなか、EC加盟店おける漏えい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効果的か。

２．アクワイアラー側での対応
（１）アクワイアラー等によるEC加盟店への加盟店管理による対策
まずはアクワイアラー等によるEC加盟店に対する加盟店管理（セキュリティ基準）の強化によるアプローチが考えられるところ。
①クレジットカード番号等の適切管理義務として、クレジットカード番号等に固有の適切管理として、保持・非保持の有無／ PCIDSSの準拠の可否だけでなく、非保持化している場合には、その前提となるECサイト自体の脆弱性対策についても、加盟店管理義務の対象としていくことについて、どう考えるか。ECサイトの脆弱性対策を念頭においた加盟店調査項目の追加以外に必要な観点や方策もあるか。不正アクセスの早期検知状況の確認も求められるか。

② ECサイトの脆弱性対策等について、アクワイアラー等が継続的に加盟店を管理していくうえで、アクワイアラー等によるEC加盟店に対する加盟店管理をどのように実効的に実施していくべきか。

（参考）関連義務の法体系

（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）

1．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・平成28年改正・令和２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　クレジットカード番号等の漏えい、滅失、毀損その他のクレジットカード番号等の管理に係る**事故（以下「漏えい等の事故」という。）の発生を防止するため必要かつ適切な措置を講ずること**。【事故の防止措置】⇒PCI DSS準拠または同等以上の措置

二　クレジットカード番号等取扱業者において**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、直ちに当該事故の状況を把握し、当該事故の拡大を防止する**とともに当該事故の状況に応じて**速やかに、その原因を究明するために必要な調査（当該事故に係るクレジットカード番号等の特定を含む。）**を行うこと。【事故発生時の状況把握・原因究明等】⇒フォレンジック調査（カード番号等の特定含む）

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）

四　クレジットカード番号等取扱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、当該クレジットカード番号等取扱業者は**類似の漏えい等の事故の再発防止のために必要な措置を講ずること**。【再発防止】⇒再発防止策の実施

五　クレジットカード番号等をクレジットカード等購入あつせんに係る**取引の健全な発達を阻害**し、又は**利用者若しくは購入者等の利益の保護に欠ける方法により取り扱わないこと**。【利用者等の利益保護】 ⇒クレジットカード番号等の不適切な取扱いの禁止

（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）

1．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・平成28年改正・令和２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は、次の各号のいずれかに該当する者**をいう。

一　クレジットカード等購入あつせん業者 【イシュアー】

二　包括信用購入あつせん又は二月払購入あつせん（以下この項及び第三十五条の十七の二において「クレジットカード等購入あつせん」という。）に係る販売の方法により商品若しくは権利を販売する販売業者（以下「クレジットカード等購入あつせん関係販売業者」という。）又はクレジットカード等購入あつせんに係る提供の方法により役務を提供する役務提供事業者（以下「クレジットカード等購入あつせん関係役務提供事業者」という。）【加盟店】

三　特定のクレジットカード等購入あつせん業者のために、自己の名をもつて特定の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にクレジットカード等購入あつせんに係る購入の方法により購入された商品若しくは権利の代金又は受領される役務の対価に相当する額の交付（当該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以外の者を通じた当該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への交付を含む。次号において同じ。）をすることを業とする者（同号において「立替払取次業者」という。）【アクワイアラー】

四　特定の立替払取次業者のために、自己の名をもつて特定の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にクレジットカード等購入あつせんに係る購入の方法により購入された商品若しくは権利の代金又は受領される役務の対価に相当する額の交付をすることを業とする者 【決済代行業者等】

五　利用者からクレジットカード番号等の提供を受けて、当該クレジットカード番号等を決済用情報（当該クレジットカード番号等以外の番号、記号その他の情報であつて、当該利用者がそれを提示し又は通知して、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ができるものをいう。以下この項において同じ。）と結び付け、当該決済用情報を当該利用者に提供することを業とする者 【QRコード決済事業者等】

六　前号に掲げる者から委託（二以上の段階にわたる委託を含む。）を受け、クレジットカード番号等をその結び付けられた決済用情報により特定することができる状態で管理することを業とする者 【５号事業者の委託会社等】

七　第三号から前号までに掲げる者のほか、大量のクレジットカード番号等を取り扱う者として経済産業省令で定める者 【加盟店向け決済システム提供事業者等】

（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）

1．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・平成28年改正・令和２年改正

＜監督指針＞【すべての取扱業者における事故の防止措置】

- **法令においてはセキュリティ確保に不可欠な機能のみを定め**、その実現手段及び方法については、各事業者の創意工夫に基づく多様な手法に対してオープンなものとする**「性能規定」の考え**の下、クレジットカード番号等取扱業者に、**必要かつ適切な措置を講ずること**を求めている。この「必要かつ適切な措置」については、**最新の技術動向等を踏まえて毎年見直しが行われる「クレジットカード・セキュリティガイドライン」（以下「ガイドライン」という。）に掲げられる措置が実務上の指針**となるものであり、**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「必要かつ適切な措置」が講じられているものと認められる。**

＜クレジットカード・セキュリティガイドライン＞ 非対面関連

クレジットカード番号等取扱事業者	対象事業者	セキュリティ対策
１号　カード発行会社（イシュアー）	・クレジットカード会社等	**PCI DSS準拠**
２号　加盟店		**非保持** または、PCI DSS準拠
３号　アクワイアラー	・クレジットカード会社等	**PCI DSS準拠**
４号　決済代行業者等	・決済代行業者（ネット取引） ・EC モール事業者（デジタルプラットフォーマーなど）	**PCI DSS準拠**
５号　QRコード決済事業者等	・QR コード決済事業者 ・スマートフォン決済事業者 ・ID 決済事業者等 その他名称の如何にかかわらず、クレジットカード情報と紐づけた他の決済用番号で決済を行う事業者	**PCI DSS準拠**
６号　利用者向け決済サービス委託先	・第5号事業者からクレジットカード情報の管理を受託している事業者	**PCI DSS準拠**
７号　加盟店向け決済システム提供事業者	・決済代行業者（ネット取引） ・EC システム提供会社（ASP/SaaSとしてEC事業者にサービス提供する事業者、EC事業者に購入プラットフォームを提供する事業者等）、これらに限られない。 カード会員データの伝送処理保存を行っている事業者、決済代行業者又はアクワイアラー決済モジュールを提供している事業者も含まれる	**PCI DSS準拠**

（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）

1．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・平成28年改正・令和２年改正

＜監督指針＞【取扱業者（加盟店除く）の体制整備】
クレジットカード番号等取扱業者は、以下の点に留意してクレジットカード番号等を適切に管理する体制を整備しなければならない。
（１）クレジットカード番号等の管理を行う**責任部署及び責任者を定めている**こと。
（２）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。
（３）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漏えい等の事故の防止措置又はそれと同等以上の措置を講ずる**ことを定め、これらの措置を講じていること。また、**毎年のガイドラインの見直し等を踏まえて、自社の漏えい等の事故の防止措置について見直す**こととしていること。
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て必要かつ適切な漏えい等の事故の防止措置を定め、当該措置を実施していること。
（４）クレジットカード番号等の漏えい等の事故が発生し、又は発生したおそれがある場合の**対応部署を定め、直ちに事故の状況を把握し、当該事故の発生状況に応じた事故の拡大防止措置を実施する体制を整備**していること。また、**事故の対象となるクレジットカード番号等を速やかに特定し、事故の原因を究明するための調査を速やかに実施するための体制を整備**していること。クレジットカード決済システムからの漏えい等の事故の発生、又はそのおそれがある場合には、**デジタルフォレンジック調査等の調査を実施する体制を整備している**こと。
（５）クレジットカード等購入あっせん業者は、自社が利用者等に付与したクレジットカード番号等の漏えい等の事故が発生し、又は発生したおそれがある場合に、当該利用者以外の者による不正利用を防止するため、**不正利用検知モニタリングの実施やクレジットカード番号等の差し替え等の必要な措置を実施する体制を整備している**こと。
（６）クレジットカード番号等の漏えい等の事故が発生し、又は発生したおそれがある場合に、**類似の漏えい等の事故を再発防止するための措置を検討し、実施する体制を整備している**こと。
（７）クレジットカード番号等の漏えい等の事故が発生し、又は発生したおそれがある場合に**関係機関、関係事業者への連絡体制を整備**し、**事故発生時に迅速かつ適切な対応を実施するよう役職員に周知している**こと。

（８）クレジットカード番号等の取扱いを委託する場合、**委託先との契約に**当該委託先が実施するべきクレジットカード番号等の管理措置の内容、クレジットカード番号等の漏えい等の事故が発生し、又は発生したおそれがある場合の**事故の状況把握及び自社への報告、事故の拡大防止、原因究明調査及び再発防止措置を実施することを定めている**こと。また、**これらの措置を適切に実施できないと認められた場合には、契約内容を変更することや契約を解除することを定めている**こと。
（９）クレジットカード番号等の取扱いを**委託する場合、当該委託先の監督の基準や手続を定め、日常業務の運営において実践している**こと。
（１０）**委託先において**クレジットカード番号等の漏えい等の事故が発生し、又は発生したおそれがある場合の**対応部署を明確化し、事故の状況把握及び自社への報告、事故の拡大防止、原因究明調査及び再発防止措置等の実施を指導する体制を整備している**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）

１．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・平成28年改正・令和２年改正

＜監督指針＞【加盟店における必要な措置】
（１）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漏えい等の事故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漏えい等の事故の防止措置を実施していること。
（２）（略）
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。

（参考）加盟店調査等の義務について（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**

- 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、前掲省令第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（加盟店において漏えい等の事故が発生した場合の調査）（施行規則第１３３条の８第４号）

加盟店からの連絡・その他の方法によって知った事項からみて、**加盟店による漏えい等の事故が発生し、又は発生した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 当該漏えい等の事故に関し、加盟店が行った原因究明等の調査（省令第１３２条第２号に基づき加盟店が実施する調査）の結果
② 当該加盟店がカード番号等の適切管理について、法令の要求水準に適合した措置を適切に講ずるように指導をするために必要な事項
③ 当該加盟店が類似の漏えい等の事故の再発防止策を講ずるように指導をす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。

・加盟店におけるカード番号等の適切管理措置等が前掲**省令第１３２条の基準に適合していない場合、合理的な期間内に当該基準に適合した措置を講じるよう指導。**
・加盟店において、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、**類似の漏えい等の事故の再発防止のために必要な措置を講じるよう指導。**
・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）加盟店調査等の義務について（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（割販法省令第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．**加盟店調査等の義務**（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、割販法省令第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）割販法省令第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、割販法省令第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、割販法省令第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、割販法省令第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、割販法省令第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、**割販法省令第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）加盟店調査等の義務について（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**

＜クレジットカード・セキュリティガイドライン＞　推奨事項

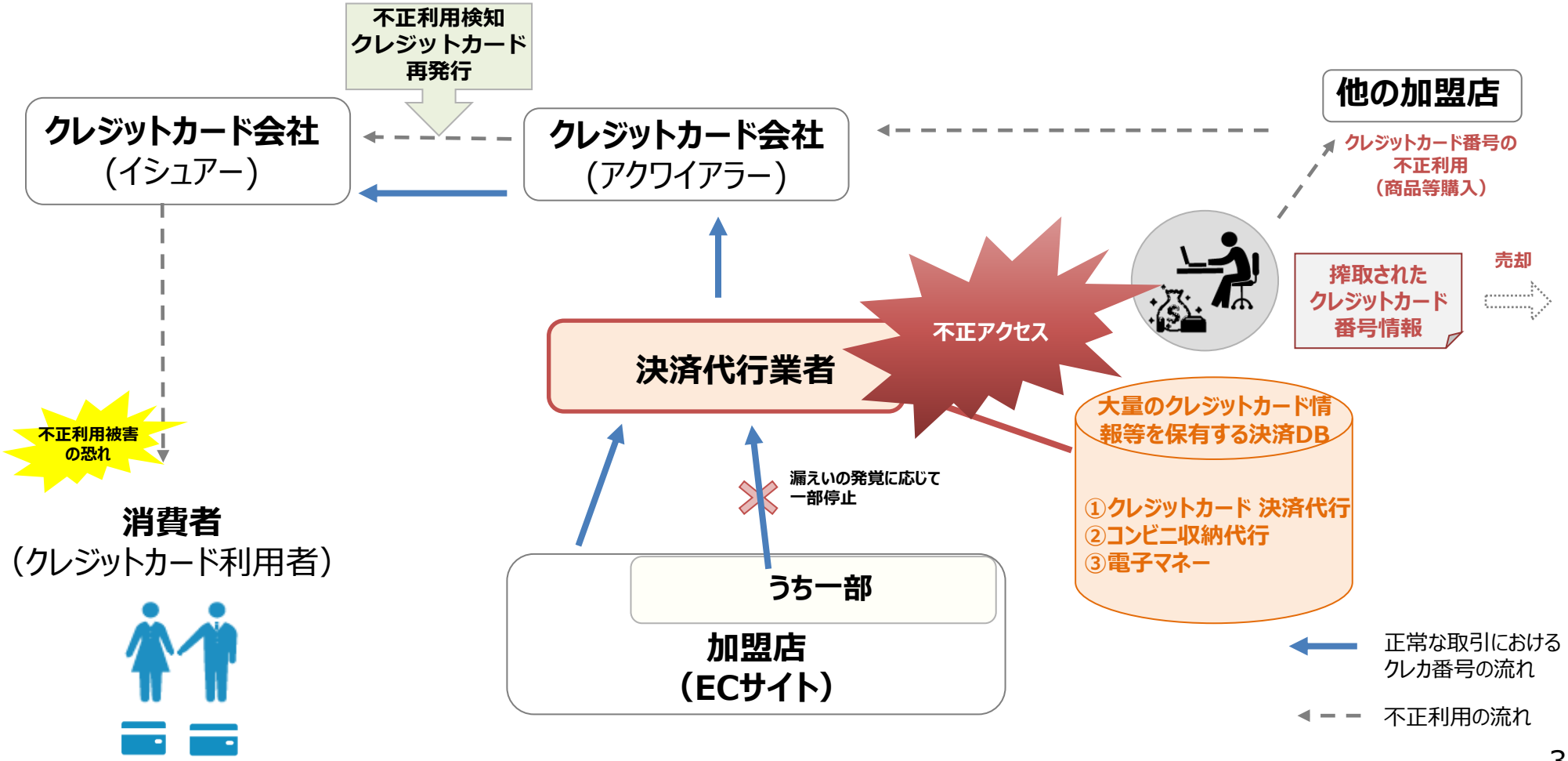
○3 号事業者：カード会社(アクワイアラー)
アクワイアラー（3号事業者）は、契約のある決済代行業者等と連携し、対面/**非対面加盟店に対し非保持化（非保持と同等/相当を含む）又はPCI DSS準拠及び、その他セキュリティ対策について必要な助言や情報提供等を行う。**また、EC加盟店に対して、**基本的なセキュリティ対策を4号事業者と共に確認していく。**

○4 号事業者：決済代行業者等
決済代行業者等は、加盟店の取組を支援するため、加盟店に対しカード情報保護対策について**必要な助言や情報提供を実施**する。なお、カード会社（アクワイアラー）と契約を有する決済代行業者等については、カード会社（アクワイアラー）と連携して対応する。特に、EC 加盟店に対して、**基本的なセキュリティ対策をカード会社（アクワイアラー）と共に確認していく。**

３-1．PSP（４号･7号業者）での漏えい対策

（１）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。



（２）PSPにおける適切管理義務

- 決済代行等を業とするPSPは、個別のEC加盟店の非保持化の進展により、クレジットカード番号等が蓄積されていくことから、セキュリティ対策の要請は更に強まるところ。
- 一方、アクワイアラー等から契約先として管理される対象ではなく、現状はクレジットカード番号等の適切管理義務が事後規制として課されている（改善命令のみ対象）。

個別事案：クレジットカード番号等取扱業者に対する行政処分（令和４年６月30日）

・事業者：株式会社メタップスペイメント

・クレジットカード番号等取扱業者（４号・７号業者）として、クレジットカード番号等の適切管理義務（法第35条の16第1項）に違反し、改善命令。

（違反事実）

①PCI DSSを準拠するための措置が講じられていない

- クレジットカード決済システム内にコンビニ決済に係る加盟店向けアプリが移設された事実を監査機関に伝えなかった。
- 脆弱性診断・ネットワーク脆弱性スキャンの報告書を改ざんし、監査機関に提示又は提出。
- これらの改ざんについて、経営陣に報告がなく、内部監査機能も働かなかった。
- 同社の別サービスのクレジットカード決済システムではPCI DSSを準拠していない。

②基本的なセキュリティ対策が実施されていない

- 不正アクセスの検知・防御対策の不備、データベースの未分離、自社システムのアプリケーションやネットワークの脆弱性診断の不適切な実施、検出された脆弱性への未対応等。

③クレジットカード番号等の適切な管理のための必要な措置を講じていない

- 関係役職員での適確な情報共有や記録なし。発生したアラートの全件を確認しない。サイバー攻撃を検知した際の原因究明の不実施。

（参考）他のキャッシュレス関連法で求められているセキュリティレベル

- 第三者型前払式支払手段発行者や資金移動業者に対しては、資金決済法における情報の安全管理義務として、システムリスク管理態勢やサイバーセキュリティ管理態勢が求められており、登録時にチェックされている。

資金決済法（前払式支払手段発行者）

法令　・前払式支払手段の発行の業務に係る情報の漏えい等の防止その他の当該情報の安全管理のために必要な措置を講じる義務（法第21条。情報の安全管理につき前払式支払手段に関する内閣府令第43条、第44条）
・前払式支払手段の発行の業務の一部を委託した場合における委託先に対する指導その他の当該業務の適正かつ確実な遂行を確保するために必要な措置を講じる義務（資金決済法第21条の２）

ガイドライン等　第三分冊（５　前払式支払手段発行者関係）（抜粋）　**※資金移動業者においてもほぼ同内容。**

Ⅱ－３－１ システム管理

Ⅱ－３－１－１ 主な着眼点

（１）システムリスクに対する認識等、（２）システムリスク管理態勢、（３）システムリスク評価、（４）情報セキュリティ管理

（５）サイバーセキュリティ管理

① サイバーセキュリティについて、経営陣は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

② サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。

・サイバー攻撃に対する監視体制等

③ サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。

・入口対策（例えば、ファイアウォール、WAF の設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入 等）

・内部対策（例えば、特権 ID・パスワードの適切な管理、不要な ID の削除、特定コマンドの実行監視、本番システム（サーバー間）のセキュア化（パケットフィルタや通信の暗号化）、開発環境（テスト環境を含む。）と本番システム環境のネットワークの分離、利用目的に応じたネットワークセグメント分離 等）

・出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断 等）

④ サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。

・攻撃元の IP アドレスの特定と遮断等

⑤ システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。

⑥ サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

⑦ インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。 また、内外の環境変化や事故・事件の発生状況を踏まえ、定期的かつ適時にリスクを認識・評価し、必要に応じて、認証方式の見直しを行っているか。

・可変式パスワード、生体認証、電子証明書等実効的な要素を組み合わせた多要素認証などの、固定式の ID・パスワードのみに頼らない認証方式等

⑧ インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような業務に応じた不正防止策を講じているか。

・不正な IP アドレスからの通信の遮断等

⑨ サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。

⑩ サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

（６）システム企画・開発・運用管理

（７）システム監査

（８）外部委託管理

（９）コンティンジェンシープラン

③ コンティンジェンシープランの策定に当たっては、災害による緊急事態を想定するだけではなく、前払式支払手段発行者の内部又は外部に起因するシステム障害等も想定しているか。また、以下のようなリスクを想定した十分なリスクシナリオとなっているか。

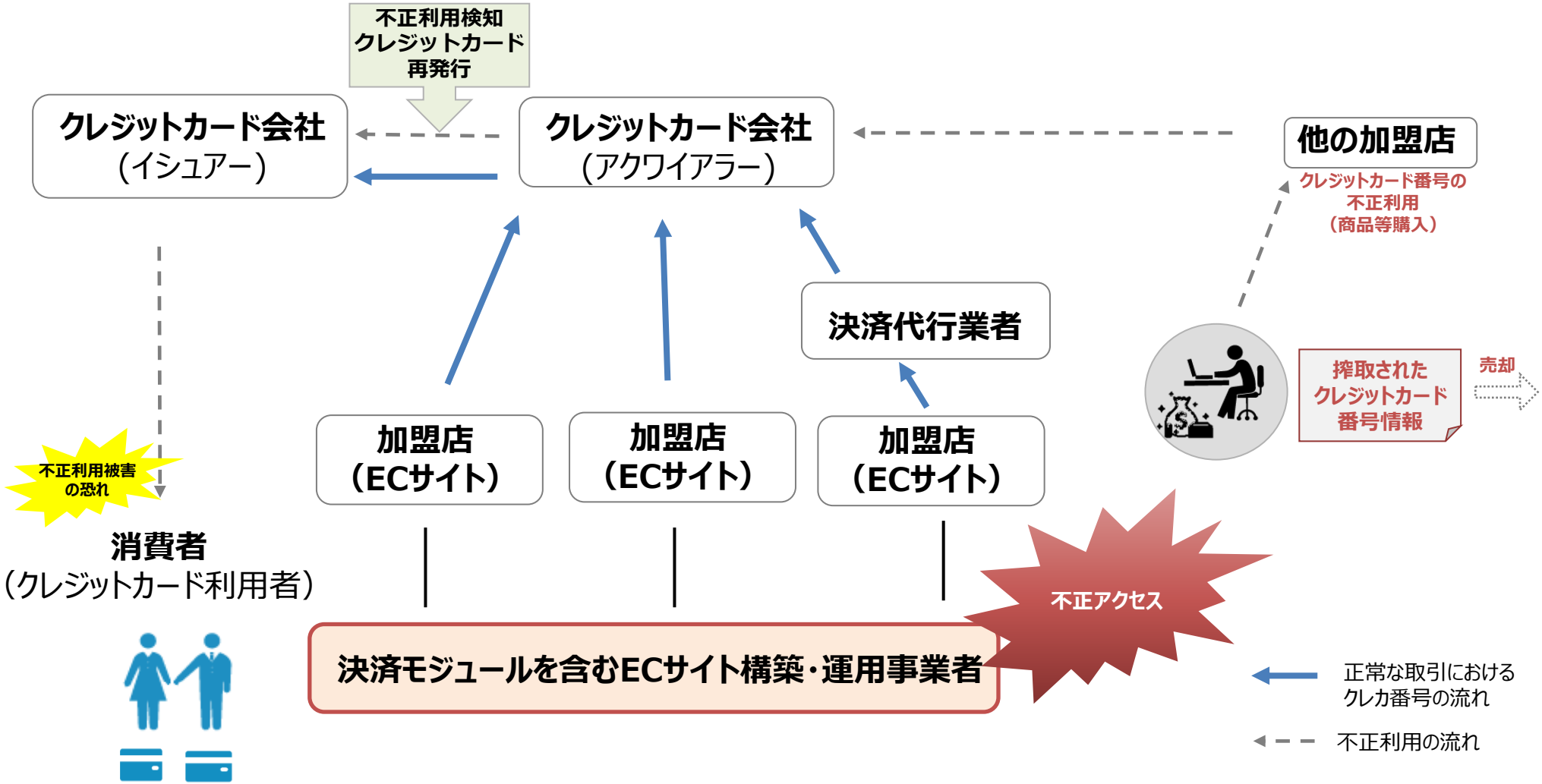
・サイバー攻撃等

（１０）障害発生時等の対応

3-2. 加盟店向け決済システム提供事業者（７号業者）での漏えい対策

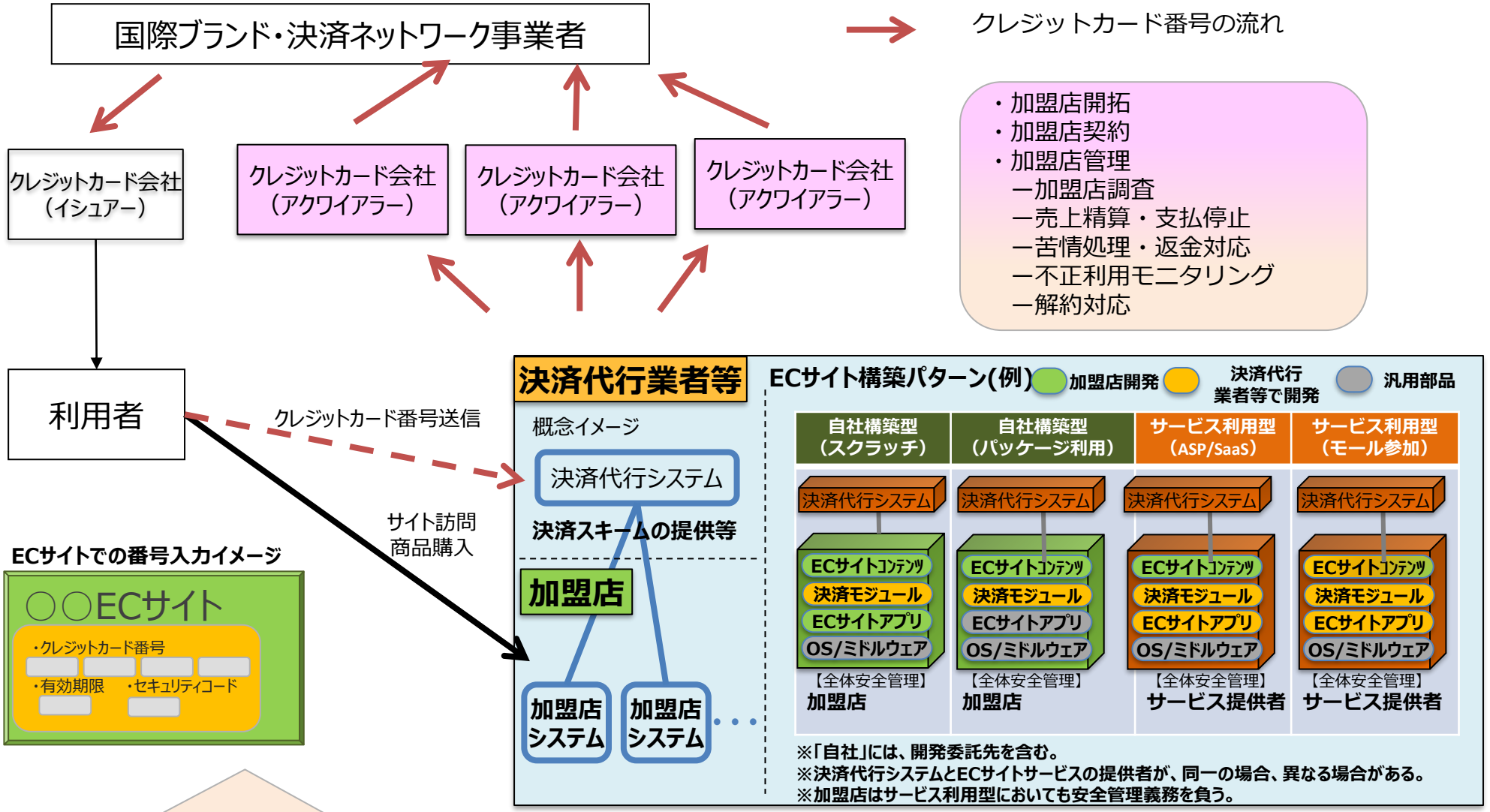
（１）ECシステム提供者での漏えい（概要）

- EC加盟店での漏えいは、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加盟店は約９事業者）。



（１）EC加盟店構築をめぐる多様なプレーヤーの出現

- EC加盟店では、決済スキームだけでなく構築そのものも多様なパターンが出現。



画面の一部分が、リンクまたはサイトへのプログラムの組み込みにより、決済代行と繋がっており
クレジットカード番号は決済代行システムに直接送信される

（２）加盟店向け決済システム提供事業者の該当性

- EC加盟店向けに、決済モジュールを含むECサイトを構築・運用をするサービスプロバイダーなどでは、自らのシステム内ではクレジットカード番号を保持していない（プログラムの提供のみである）場合は適切管理義務の対象ではない、加盟店の委託先である場合は適切管理義務があってもそのレベルは加盟店と同等レベルでよいと誤認されているケースも散見されるところ。
- 加盟店向け決済システム提供業者に該当するものとして、「クレジットカード番号等を取り扱う」意義について、監督指針で明確化することを検討。

＜法第35条の16第１項＞
七　第三号から前号までに掲げる者のほか、**大量のクレジットカード番号等を取り扱う者として**経済産業省令で定める者

＜施行規則第132条の２＞
（大量のクレジットカード番号等を取り扱う者）
第百三十二条の二　法第三十五条の十六第一項第七号の経済産業省令で定める者は、特定の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のために、**クレジットカード番号等を特定の立替払取次業者に提供**（当該立替払取次業者以外の者を通じた当該立替払取次業者への提供を含む。）**することを業とする者**とする。

＜監督指針での明確化を検討しているポイント＞
・法第35条の16第１項第７号に規定する「取り扱う」とは、必ずしもクレジットカード番号等を物理的に取り扱うことのみを対象としているものではなく、他社が提供するサービスやシステムを利用することにより間接的にクレジットカード番号等を取り扱うことも含んでいるといえるのではないか。
・施行規則第１３２条の２に規定する「提供」の範囲とは、加盟店の利用者が、クレジットカード番号等を、ECシステム提供者のネットワークを介さず、自身のＰＣ等に表示される加盟店の決済画面から決済代行業者に対して直接伝送し、さらに当該決済代行業者が立替払取次業者にクレジットカード番号等を提供するスキームであったとしても、ECシステム提供者のサービスにより立替払取次業者に対してクレジットカード番号等を提供できているのであれば、「当該立替払取次業者以外の者（決済代行業者）を通じた立替払取次業者への提供」を行っているといえるのではないか。

ご議論いただきたい事項

３－１.PSPにおける漏えい対策
総論：昨今のPSP（決済代行業者）での漏えいやその役割を念頭におき、PSPおける漏えい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。

PSPに対しては、クレジットカード番号等の適切な管理として、PCI DSSの準拠のみならず、漏えい防止に必要な措置を求めてきたところ。しかしながら、PCI DSS準拠に向けては対応するものの、基本的なセキュリティ対策や業務運営体制について軽視する事業者も存在。
①クレジットカード番号等の適切管理義務として、クレジットカード番号等に固有の管理の前提である基本的なセキュリティ対策や業務運営体制の措置を講ずることについて、監督上の観点として明示してはどうか。

②今般の漏えい事案を踏まえ、PSPのセキュリティレベルを担保するためには、どのようなアプローチが有効か。アクワイアラー等がPSPに対し、調査・指導できる権限を持てるようにすべきか、またはその役割の重要性に鑑み、業について国が事前に監督すべきか。

３－２.加盟店向け決済システム提供事業者における漏えい対策

昨今では、EC加盟店のサイトや決済スキームの構築をめぐり、多様なプレーヤーがいるところ。
①自社のシステムではクレジットカード番号等を扱っていない等により、「加盟店向け決済システム提供事業者」であると認識していない事業者に対し、加盟店向け決済システム提供業者に該当することについて、どのように周知していくか。