

# 時代の要請を受けた消費者保護 ～QRコード決済事業者等のセキュリティ対策～

令和元年10月15日

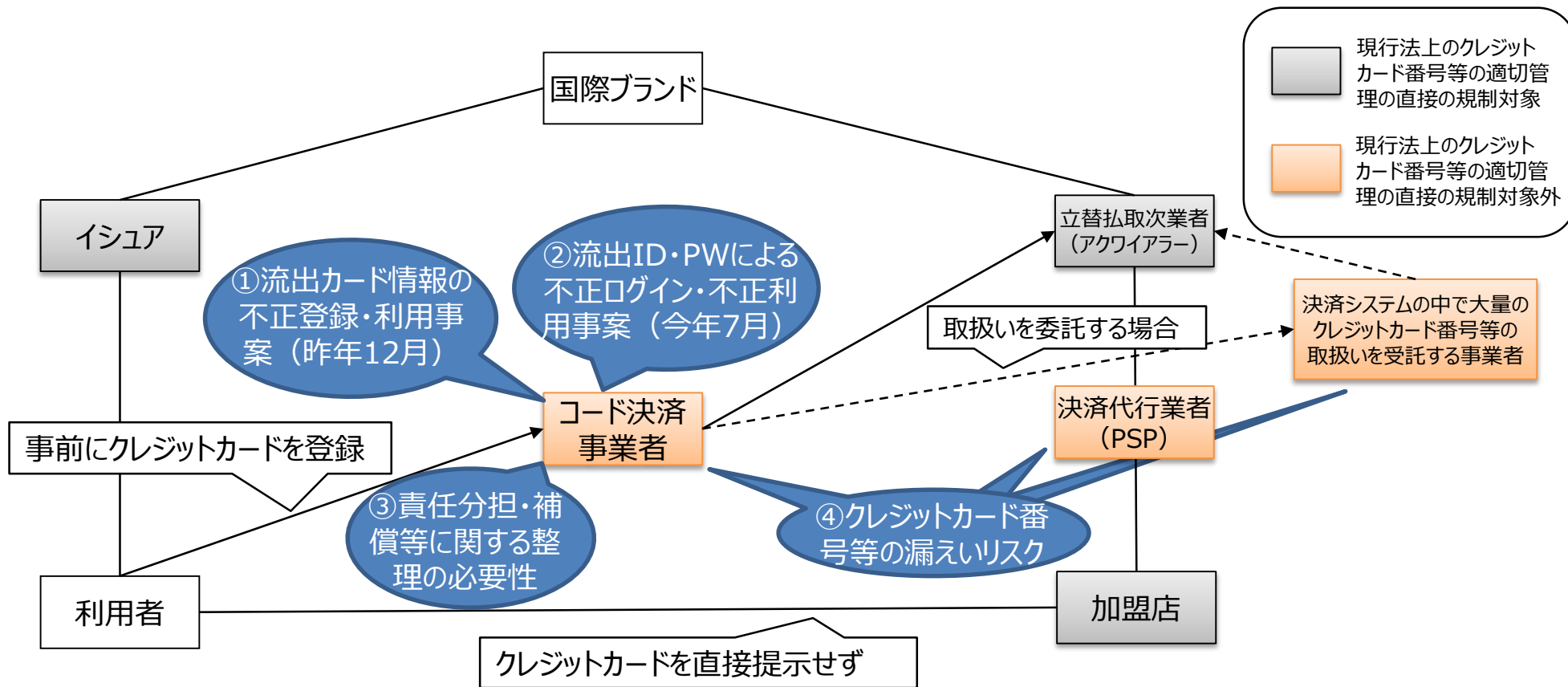
商務・サービスグループ

商取引監督課

# クレジットカード取引を取り巻く環境変化

- ICTの進展に伴い、決済テクノロジーが進化し、コード決済事業者等、新たな決済サービスを提供する事業者が出現している。
- こうした事業者は、利用者の利便性を向上させている一方、昨年12月にクレジットカード不正登録事案が、今年7月に第三者からの不正アクセス被害が発生するなど、新たな問題が生じている。

## コード決済事業者等を取り巻くクレジットカード取引と昨今の不正利用事案等の整理



コード決済事業者等の新たに出現している事業者について、発生している事案やリスクをどのように捉え、対応することが考えられるか。

# 昨今発生している不正事案やリスクに係る検討（1）

①昨年12月、流出カード情報の不正登録・利用事案が発生

## 事案の概要

コード決済サービスにて、**流出したカード情報を元にクレジットカードが登録され、不正利用**される事案が発生。

## 対応

（一社）キャッシュレス推進協議会にて「**コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン**」を策定。その後、同様の事案は発生していない。

## ガイドラインの概要

	コード決済事業者	クレジットカード事業者
アカウント作成時	本人認証	—
クレジットカード登録時	<ul style="list-style-type: none"><li>券面認証（入力回数制限含む）</li><li>3Dセキュア</li><li>属性・行動分析 等</li></ul>	<ul style="list-style-type: none"><li>3Dセキュアの啓発</li><li>オーソリモニタリング</li><li>クレジット名義人への登録通知</li></ul>
決済時	<ul style="list-style-type: none"><li>金額や利用回数等の上限設定</li><li>取引モニタリング</li><li>クレジットカード事業者との情報連携</li></ul>	<ul style="list-style-type: none"><li>不正検知の精度向上・強化</li><li>コード決済事業者との情報連携</li></ul>
決済後	<ul style="list-style-type: none"><li>不正検知の精度向上・強化</li><li>関係事業者との連携による不正利用の被害拡大の防止</li></ul>	<ul style="list-style-type: none"><li>不正検知の精度向上・強化</li><li>関係事業者との連携による不正利用の被害拡大の防止</li></ul>

なお、同協議会では、同時に、QRコード等の仕様の統一化を図るとともに、セキュリティ対策について必須の対策から参考となる対策までを整理した「**コード決済に関する統一技術仕様ガイドライン（CPM／MPM）**」を策定している。

②今年7月、流出ID・PWによる不正ログイン・不正利用事案が発生

## 事案の概要

コード決済サービスにて、流出ID・PWによりアプリ内不正ログインされ、アプリと端末のとの紐付け管理がなされていなかったため、登録されているクレジットカードを用いてチャージを行い、商品が購入される事案が発生。

## 原因

「コード決済に関する統一技術仕様ガイドライン」では、アプリと端末との紐付け管理を求めており、ログインID・PWが流出しても、端末が異なれば決済拒否等が可能だが、こうした**ガイドラインで掲げている措置が必ずしも遵守されていなかった**。

## 対応

経済産業省

- 協議会の全会員に対し、不正対策ガイドラインの趣旨と取組徹底を求める文書を発出。
- 協議会主催の「コード決済普及促進プロジェクト全体会」において、参加会員全員に対し不正対策の実施を強く要請。

キャッシュレス推進協議会

- 「複数システムを連携させた決済サービスにおける不正利用対策に関する検討会」を立ち上げ、システム連携時に決済事業者として注意すべきセキュリティ対策について検討中。

（一社）キャッシュレス推進協議会において、上記の取組を含め、コード決済事業者におけるセキュリティ対策が継続的に進められており、引き続き各種ガイドラインを含め、こうした取組をフォローしていくことが必要であると考えられるのではないかと。

# 昨今発生している不正事案やリスクに係る検討（2）

## ③責任分担・補償等に関する整理の必要性

### 背景

昨今のコード決済サービスにおける不正利用事案の発生を受け、コード決済事業者による安全かつ安心な決済サービスの提供の重要性が改めて認識される中、消費者にとって「安心」な決済サービスであるためには、不正利用が発生した場合に利用者にとどのような責任・補償等があるかを、あらかじめ明確にしておく必要がある。

### 対応

- （一社）キャッシュレス推進協議会において、「コード決済における不正利用に関する責任分担・補償等についての規定事例集（利用者向け利用規約）」を策定・公表。
- コード決済事業者に対し、不正利用における責任分担・補償等の規定を利用規約等に明示的に記載することを求めている。

#### 規定事例集の構成（以下についてそれぞれ参考事例を記載）

本人が利用者登録した場合における不正利用時の責任分担等に関する規定

本人が利用者登録をしていない場合における不正利用時の責任分担等に関する規定

賠償額の上限等

不正利用が行われた場合に備えて補償制度を設けている事例

（一社）キャッシュレス推進協議会において、消費者への適切な情報提供がなされるよう、機動的に対応が進められており、引き続き、こうした取組をフォローしていくことが必要であると考えられるのではないかと。

## ④クレジットカード番号等の漏えいリスク

### クレジットカード番号等の適切管理義務の制定経緯

H20年：イシュー・アクワイアラーを直接の義務主体として措置。  
H28年：加盟店からのカード情報の漏えい拡大を受け、加盟店を直接の義務主体として措置。  
H29年：決済代行業者(PSP)からのカード番号等の漏えい事案が発生（約700,000件）

### 現行法におけるクレジットカード番号等の適切管理義務

条文	主体	クレジットカード番号等の適切管理義務
35条の16	①クレジットカード等購入あつせん業者（イシュー）	直接の義務主体（第1号）
	②立替払取次業者（アクワイアラー）	直接の義務主体（第2号）
	③加盟店	直接の義務主体（第3号）
	④①～③からクレジットカード番号等の取扱いの委託を受けた者	①～③からの指導等を受ける（第3項）(間接的な義務主体)
35条の17の9	⑤クレジットカード番号等取扱契約締結事業者	直接の義務主体

### 新たに出現している事業者等

以下の事業者には、現行法上、必ずしも適切管理義務が課されない。

#### 決済代行業者（PSP）

アクワイアラー・加盟店間の決済データの授受やアクワイアラーと包括加盟店契約等を締結することで加盟店にクレジットカード決済スキームを提供する事業者

#### コード決済事業者（QRコード決済事業者など）

利用者からクレジットカード番号等の提示を受け、これを自社又は他社に委託することでトークンに置換し、トークン（コード）を用いた後払いサービス等を提供する事業者

#### ECメール事業者

利用者からクレジットカード番号等の提示を受け、ECメール内でこれを用いた後払い決済が可能となるようなウォレットサービス等を提供する事業者

#### 決済システムの中で大量のクレジットカード番号等の取扱いを受託する事業者

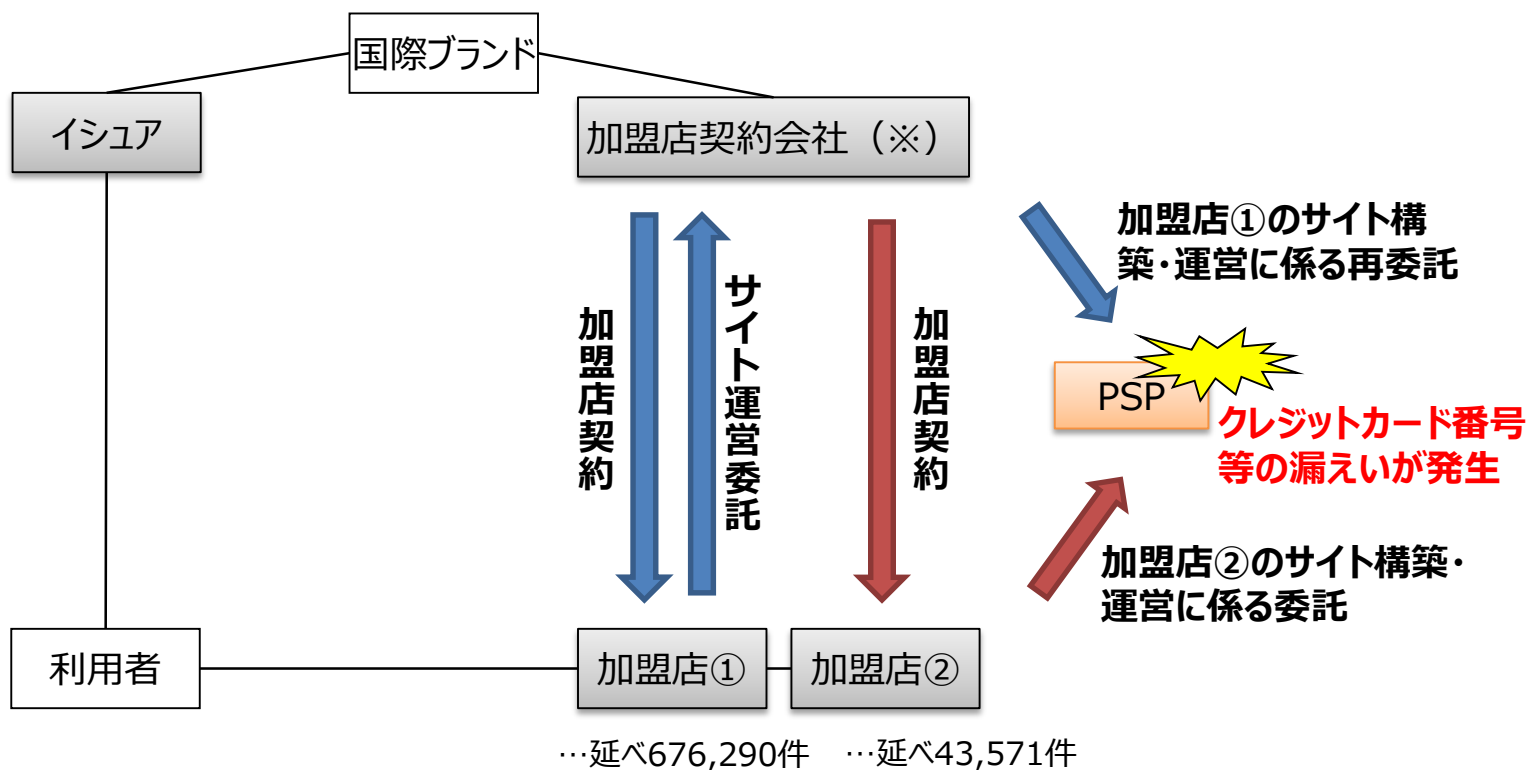
コード決済事業者やECメール事業者等から、クレジットカード番号等の取扱いの委託を受け、クレジットカード番号等を大量に取り扱う事業者

これらの事業者とクレジットカード番号等の適切管理義務との関係をどのように考えるか。

## (参考) PSPにおけるクレジットカード番号等の漏えい事案

- 平成29年3月、Apache Struts2 (※) の脆弱性を悪用した不正アクセスを受け、PSPから延べ約700,000件のクレジットカード番号等が漏えいする事案が発生。

(※) Apache Struts2… Apache Software Foundationが提供するJavaのウェブアプリケーションを作成するためのソフトウェアフレームワーク



**⇒計延べ719,861件の漏えいが発生。**

# クレジットカード番号等の適切な管理に係る検討①

## 現行法におけるクレジットカード番号等の適切管理義務

条文	主体	クレジットカード番号等の適切管理義務
35条の16	①クレジットカード等購入あつせん業者（イシュア）	直接の義務主体（第1項第1号）
	②立替払取次業者（アクワイアラー）	直接の義務主体（第1項第2号）
	③加盟店	直接の義務主体（第1項第3号）
	④①～③からクレジットカード番号等の取扱いの委託を受けた者	①～③から適切管理のための指導等を受ける（第3項） （間接的な義務主体）
35条の17の9	⑤クレジットカード番号等取扱契約締結事業者（※1）	直接の義務主体（35条の17の9）

（※1）アクワイアラーとPSP又はコード決済事業者等のうち、加盟店契約の締結及び解除について最終決定権限を有する者が登録が必要となる。

## 今回の検討課題となる事業者（※2）と現行法におけるクレジットカード番号等の適切管理義務の関係

（※2）決済代行業者（PSP）・コード決済事業者・ECモール事業者・決済システムの中で大量のクレジットカード番号等の取扱いを受託する事業者

### ①②③との関係

これらの事業者は現行法上の①②③の事業者の定義に該当しない。

### ④との関係

決済代行業者（PSP）やコード決済事業者等は、イシュア・立替払取次業者・加盟店等との間でクレジットカード番号等の取扱いの委託契約関係があれば、これらの事業者からクレジットカード番号等の適切管理のための指導等を受けるが（間接的に適切管理の義務がかかる）、当該間接的な義務がかかるかどうかは、専ら当事者間の委託契約関係の有無によることとなる。

（例えば、コード決済事業者の場合、一般的には委託関係はない）

委託契約関係がない場合には指導を受ける等間接的な義務がかからない。

### ⑤との関係

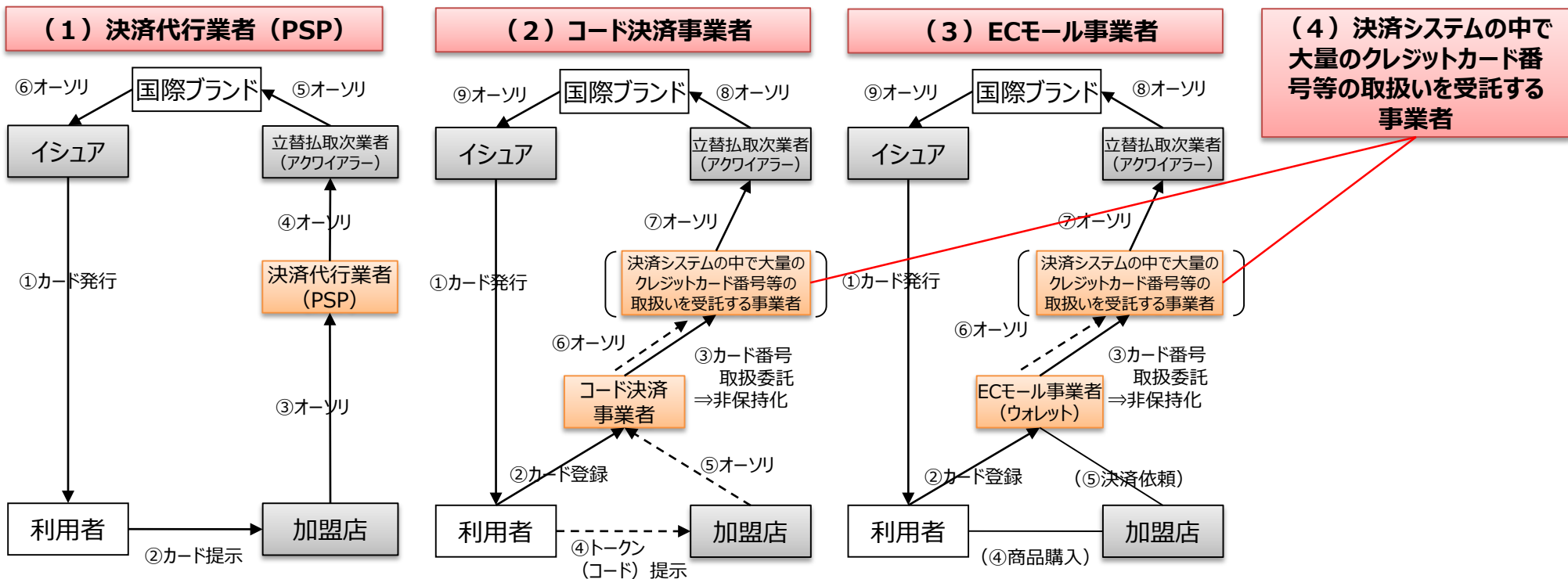
クレジットカード番号等取扱契約締結事業者の登録は、アクワイアラー又は決済代行業者（PSP）・コード決済事業者のうち、加盟店契約を締結する際に最終的な決定権限を有するいずれかの者が登録の義務を負うこととなっており、専らこれら事業者の間の契約関係により、登録の要否が決まる。

決済代行業者（PSP）やコード決済事業者が登録を要しない場合には、クレジットカード番号等取扱契約締結事業者としてクレジットカード番号等の適切管理に係る直接の義務は課されない。

これらの事業者は直接の義務も間接的な義務もかからない場合がある。

# クレジットカード番号等の適切な管理に係る検討②

各主体の提供するサービスとクレジットカード番号等との関係



## 検討のポイント

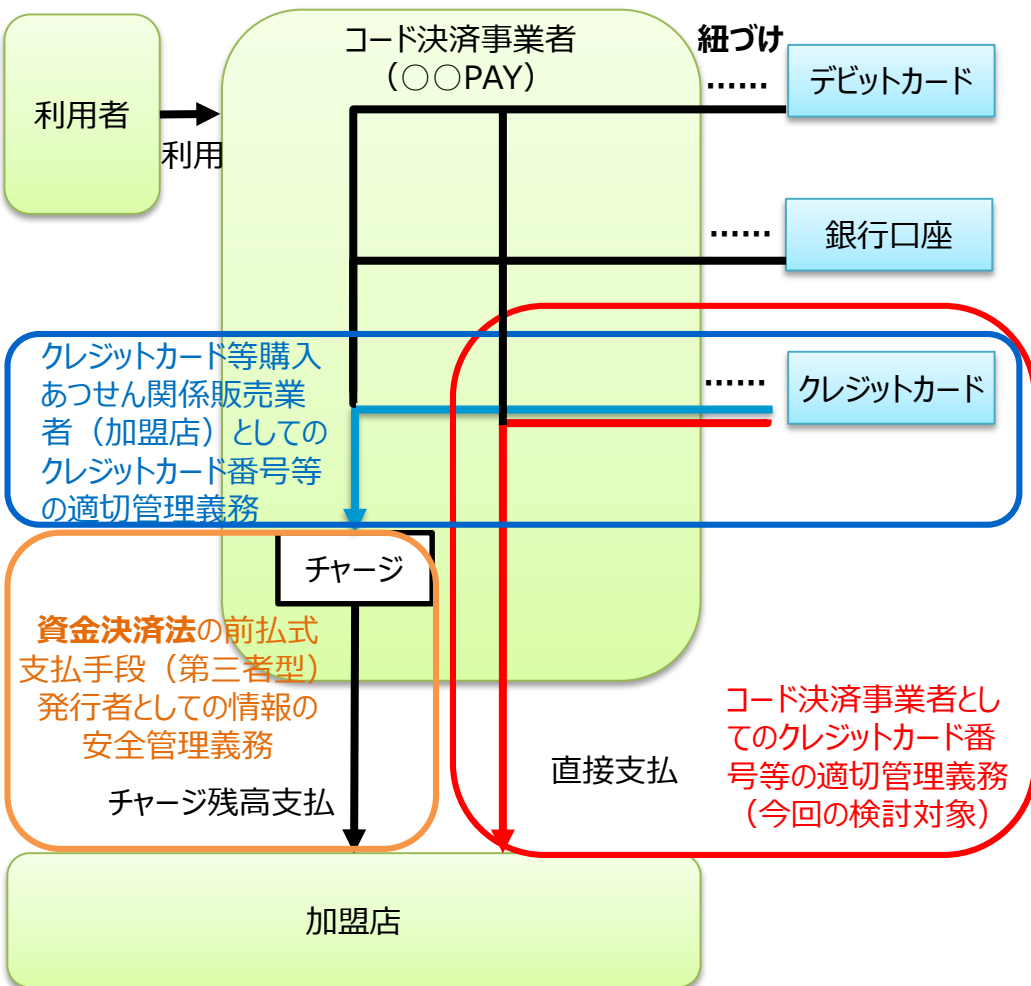
- 大量のクレジットカード番号等を取り扱っており、漏えいすれば、**大規模な情報漏えい事件**につながる**懸念**される。
- PSPにおいて、平成29年に**約700,000件のクレジットカード番号等が流出**する事案が発生。コード決済事業者等においても、同様の事案が発生するリスクを抱えている。
- 前ページの通り、**委託契約関係や登録の有無により、直接の義務も間接的な義務もかからない**場合がある。

➡ (1) 決済代行業者 (PSP) ・ (2) コード決済事業者 ・ (3) ECモール事業者 ・ (4) 決済システムの中で大量のクレジットカード番号等の取扱いを受託する事業者にも、クレジットカード番号等の適切管理義務を課すことについてどのように考えるか。

# (参考) コード決済事業者にかかる義務

例えば、コード決済事業者には、現行法上、クレジットカードによりチャージを行うケースでは、クレジットカード等購入あつせん関係販売業者として、クレジットカード番号等の適切管理義務がかかることに加え、資金決済法上の前払式支払手段（第三者型）発行者として、情報の安全管理義務がかかるなど、事業を営むに当たり、複数の法律の対応が求められる場合がある。  
 (Suicaなどのクレジットカードでチャージができるサービスにおいても同様に、割賦販売法と資金決済法の義務がかかる構造となる)

## コード決済事業者にかかるセキュリティ対策義務



			割賦販売法	資金決済法
コード決済事業者の位置付け			クレジットカード等購入あつせん関係販売業者	前払式支払手段（第三者型）発行者
セキュリティ対策に関する義務	情報管理に係る義務	概要	クレジットカード番号等の適切な管理 <ul style="list-style-type: none"> <li>法第35条の16第1項第3号</li> <li>省令第132条</li> <li>実行計画2019ⅡA</li> </ul>	情報の安全管理 <ul style="list-style-type: none"> <li>法第21条</li> <li>前払府令第44条</li> <li>ガイドラインⅡ-2-3</li> </ul>
		詳細	非保持化又はPCIDSS準拠 <PCIDSS> 国際ブランドが定めたデータセキュリティの国際基準 12の要件に基づく約400の要求事項から構成	<ul style="list-style-type: none"> <li>保存期間を設定・保存場所を限定・速やかに廃棄</li> <li>画面に表示する際は全て表示させない</li> <li>定期的又は随時の内部監査</li> </ul>
	不正利用防止に係る義務	概要	クレジットカード番号等の不正な利用の防止 <ul style="list-style-type: none"> <li>法第35条の17の15</li> <li>省令133条の14</li> <li>実行計画2019ⅡB及びC</li> </ul>	