2013年7月10日

PCI DSSセキュリティフォーラム 2013

ＰＣＩＤＳＳ導入は どこまで進んでいるか

一般社団法人 金融財政事情研究会

月 刊「消 費 者 信 用」

編 集 長 浅 見 淳

割賦販売法改正のポイント

2009年12月1日施行
2010年12月17日完全施行

個別クレジット

✓個別クレジットに登録制導入行政の権限強化

✓個別＆特商法の場合は与信契約の書面交付義務

✓個別＆特商法の場合は加盟店調査義務

✓個別＆特商法の場合は、従前の抗弁権の接続に加えて、クレジット契約のクーリングオフ、過量販売時の契約解除、加盟店に不正勧誘販売行為があった場合の契約取消の民事ルールを新設し、被害者救済を可能に（過量販売、不正勧誘の場合は与信契約の禁止規定も）

✓適合性原則（購入者の知識、経験等）

包括クレジット

✓割賦定義の見直し

✓指定商品・役務制廃止へ

✓返済可能見込額調査義務と過剰与信防止義務

✓個人信用情報の利用・登録義務

✓認定割賦協会設立

✓加盟店情報の提供義務

✓業務運営の適正化

✓カード情報の安全管理義務（加盟店・委託先の監督・指導も）

割賦販売法の改正とセキュリティ

第三章の四　クレジットカード番号等の適切な管理等

（クレジットカード番号等の適切な管理）
第三十五条の十六　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。）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（クレジットカード等購入あつせん業者が、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、滅失又はき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。
＜2項以下略＞

（改善命令）
第三十五条の十七　経済産業大臣は、クレジットカード等購入あつせん業者又は立替払取次業者が講ずる前条第一項、第三項又は第四項に規定する措置がそれぞれ同条第一項、第三項又は第四項に規定する基準に適合していないと認めるときは、その必要の限度において、当該クレジットカード等購入あつせん業者又は当該立替払取次業者に対し、当該措置に係る業務の方法の変更その他必要な措置をとるべきことを命ずることができる。

カード番号等の安全管理

個人情報保護法では、氏名等の個人情報と結びついている場合は、クレジットカード番号等も保護対象。
クレジットカード番号等単体の場合は、通常は「個人情報」にすら該当しないため、個人情報保護法で充分保護されない場合も存在する。

改正割販法35条の16

クレジットカード等購入あっせん業者
（イシュアー）＜1項に規定＞

包括信用購入あっせん業者

二月払購入あっせん業者
（マンスリー）＜2項に定義＞

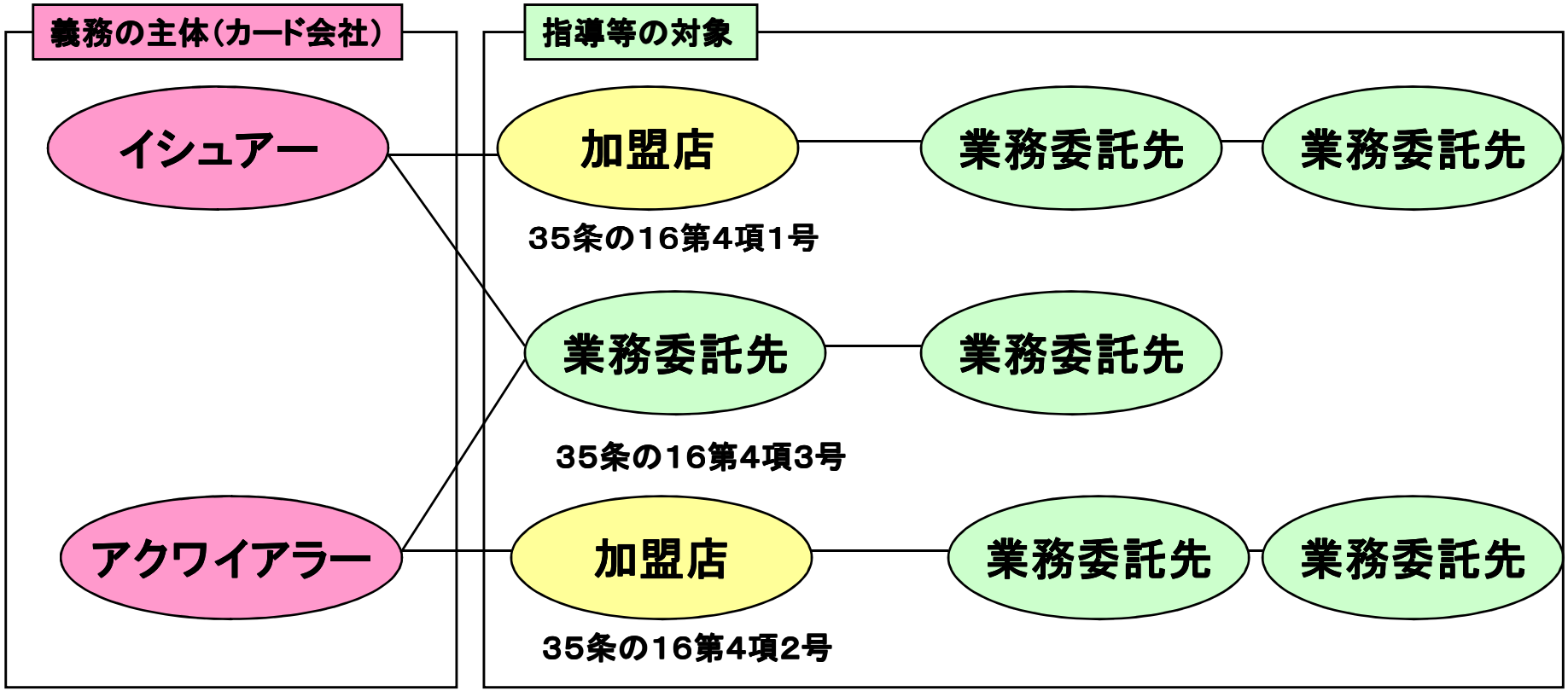
立替払い取次業者
（アクワイアラー） ＜3項に規定＞

経済産業省令で定める基準に従い

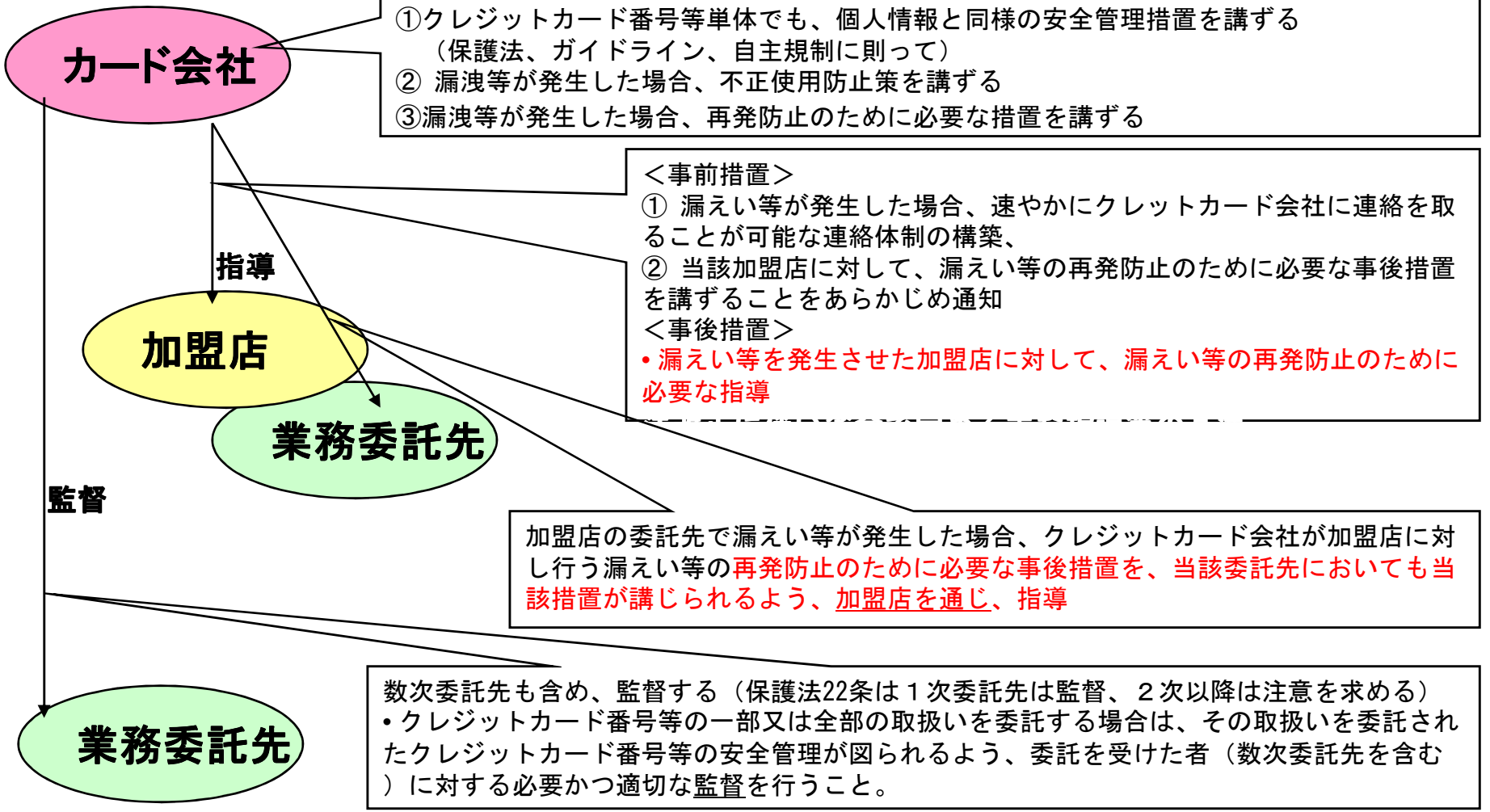
クレジットカード番号等の漏えい、滅失又は棄損の防止その他のクレジットカード番号等の適切な管理のために必要な措置を講じなければならない＜１項、３項に規定＞

クレジットカード番号等保有業者等の適切な管理が図られるよう、経済産業省令で定める基準に従い、クレジットカード番号等保有業者に対する必要な指導その他の措置を講じなければならない。
＜４項に規定＞

安全管理義務の対象範囲



カード会社の義務の詳細（省令）

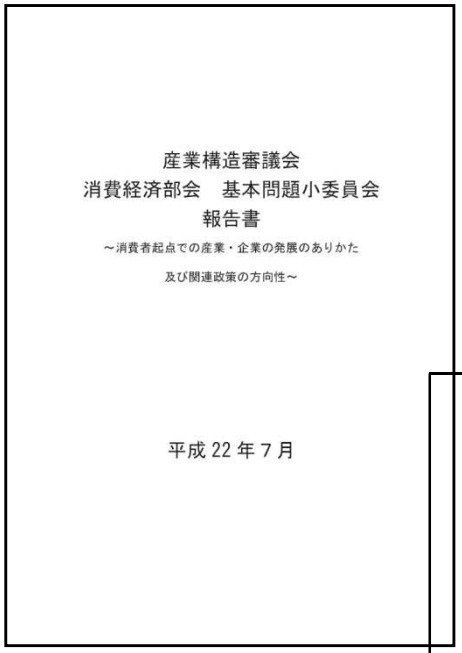


METI「将来像を考える会」

- 09年秋、経済産業省の声かけで、主要カード会社のトップが協議
- 新しい事業戦略を考える趣旨だったが・・・
- 数回の会合を行った後、セキュリティに関する問題などをクレジット協会のインフラ部会に投げる

WG1：本人認証と海外アクワイアラーにおけるトラブル
WG2：現金化
WG3：PCIDSS
WG4：ICカード化

ポスト割販法の行政課題は安全・安心


産業構造審議会
消費経済部会　基本問題小委員会
報告書
～消費者起点での産業・企業の発展のありかた
及び関連政策の方向性～

平成 22 年 7 月

最近の消費者ニーズを踏まえ、消費者を起点にした関係者の取組の方向性を提示できないか。

＜企業の取組と政策の方向性＞

1．製品の安全・安心と使いやすさ

2．快適で便利な消費環境

（3）安全・安心で便利なキャッシュレス決済

→悪質加盟店対策等の安全・安心を確保する取組、ｲﾝﾀｰﾈｯﾄ決済や多機能携帯等を用いた新たな決済方法に対するｾｷｭﾘﾃｨ向上のための取組、電子ﾏﾈｰの利便性向上のための端末や仕様の共通化を含めた検討などを実施

3．買い物と地域コミュニティ

②キャッシュレス決済の利便性・懸念点

反面、取引データや個人情報が流出・改竄される恐れがある、非対面取引で消費者が被害にあう恐れがある等の懸念点もある

③安全・安心を確保するための取組

・消費者に対し、適切な与信管理を行っていく
・加盟店管理を徹底すること（現金化業者、決済代行業者）
・消費者教育

④セキュリティを向上させるための取組

・クレジットカード情報の漏洩防止のための体制整備（PCIDSS）
・ネット取引における本人確認の更なる強化(3Dセキュア）
・ICカード対応

セキュリティ強化の両面作戦

カード情報

加盟店のカード決済システム

カード情報流出

成りすまし

PCIDSS

3Dセキュア

カード情報

３Ｄセキュアについては、２０１２年４月２日に「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」を制定

2010年9月を巡る攻防

対加盟店（アクワイアラー）

・ビザが08年11月13日に、PCIDSS遵守の義務化に向けたグローバルフレームワークを発表。年間取扱件数がレベル1加盟店とレベル2加盟店について、アクワイアラーに09年9月までに、加盟店がオーソリゼーション後にセンシティブデータを保管していないことを確認、報告する義務を課す。

・さらに、レベル1加盟店について、アクワイアラーはレベル1加盟店がPCIDSSに完全準拠した証明書を10年9月までに提出する義務を課した。

・報告・提出がなかった場合は、アクワイアラーに対し「罰金が科せられることもある」ことを示唆。

対カード会社

・ビザは11年に、新たな業態区分を設定。ビザネットにダイレクトに接続しているカード会社を「VNP」（ビザ・ネット・プロセッサー）と定義し、このうち、他のカード会社の受託業務を行っている会社を「メンバーVNP」とし、10年9月までの完全準拠を求めた。メンバーVNPに該当するのは、三井住友カード、三菱UFJニコス、ユーシーカード、クレディセゾンの4社。

・VNPではあるが、メンバーVNPに該当しない企業はメンバーアクワイアラーVNPと位置づけ、11年9月を期限に、遵守証明書の取得を義務づけた。このメンバーアクワイアラーVNPに属するのが、イオンクレジット、セディナ、トヨタファイナンスなど6社。

PCIDSSのナショナルプラン

日本クレジット協会は12年5月31日に、「日本におけるクレジットカード情報管理強化に向けた実行計画」を公表

対　象	形　態	基　準	レベル	PCIDSS準拠対応	対応期限
決済代行事業者	形態問わずすべて	すべて	—	PCIDSS準拠	13年3月
加盟店	非対面・ネット	4ブランドにより決定	A	センシティブ情報非保持	12年9月
				PCIDSS準拠	13年3月
	対面・POS			センシティブ情報非保持	13年3月
				PCIDSS準拠	18年3月
	非対面・ネット	レベルA以外	B	センシティブ情報非保持	12年9月
				PCIDSS準拠またはクレジットカード情報非保持	13年3月
	対面・POS	100万件以上、レベルA以外		センシティブ情報非保持	13年3月
				PCIDSS準拠またはクレジットカード情報非保持	18年3月
	対面・POS	100万件未満	C	クレジットカード情報非保持	18年3月
	対面・スタンドアローン	すべて	—	クレジットカード情報非保持	13年3月
クレジットカード会社	アクワイアリングまたはプロセッシング	すべて	A	PCIDSS準拠	18年3月
	イシュイングのみ	100万件以上	B	PCIDSS準拠	18年3月
		100万件未満	C	他社クレジットカード情報非保持	18年3月

(注)　①基準における件数は決済代行事業者と加盟店は、いずれかのブランドにおける年間のカード取引件数、カード会社は発行枚数、
②レベルAは各国際ブランドの基準に基づく。ビザ、マスターカードは年間カード取引件数が600万件以上、JCBは100万件、アメックスは250万件以上。

経済産業省のこれからの政策課題

- 平成 24 年度商取引適正化･製品安全に係る事業（クレジット産業の健全な発展及び安全利用等に向けた調査研究）《報告書》
- 12年12月に「クレジットカードの利用拡大と安全利用に向けた研究会（座長山本豊京大教授）を立ち上げ
- 第１章：クレジットカード利用機会の拡大
- 第２章：クレジットカードの安全利用の確保
- 行政課題の可能性あるものを包括的に整理

第１章：利用機会の拡大

- 地方部における拡大：端末の費用負担。「買い物弱者」対策としての振興。高齢化対応
- 公共分野（税・上下水道）、教育（国公立・私立高校、学習塾等）など、カード決済比率の低い分野での利用拡大
- 自治体のシステム基盤の共通化、標準化
- 電子マネー、デビットカードを含めたキャッシュレス化（決済インフラの共有化）
- 消費者教育

第2章：安全利用の確保

- 問題の背景

①不正利用が、偽造カードによる対面取引からカード番号盗用による非対面取引にシフト

②スマホ端末の導入によって、カード決済を提供できる主体が個人を含めて広がる

③電子商取引の拡大が国際取引や決済代行業者の介在する取引の拡大にもつながり、悪質加盟店による消費者トラブルを招来

④電子商取引特有の消費者トラブルが増加

2-（１）情報セキュリティ対策①

（ア）情報セキュリティ対策に係る現状

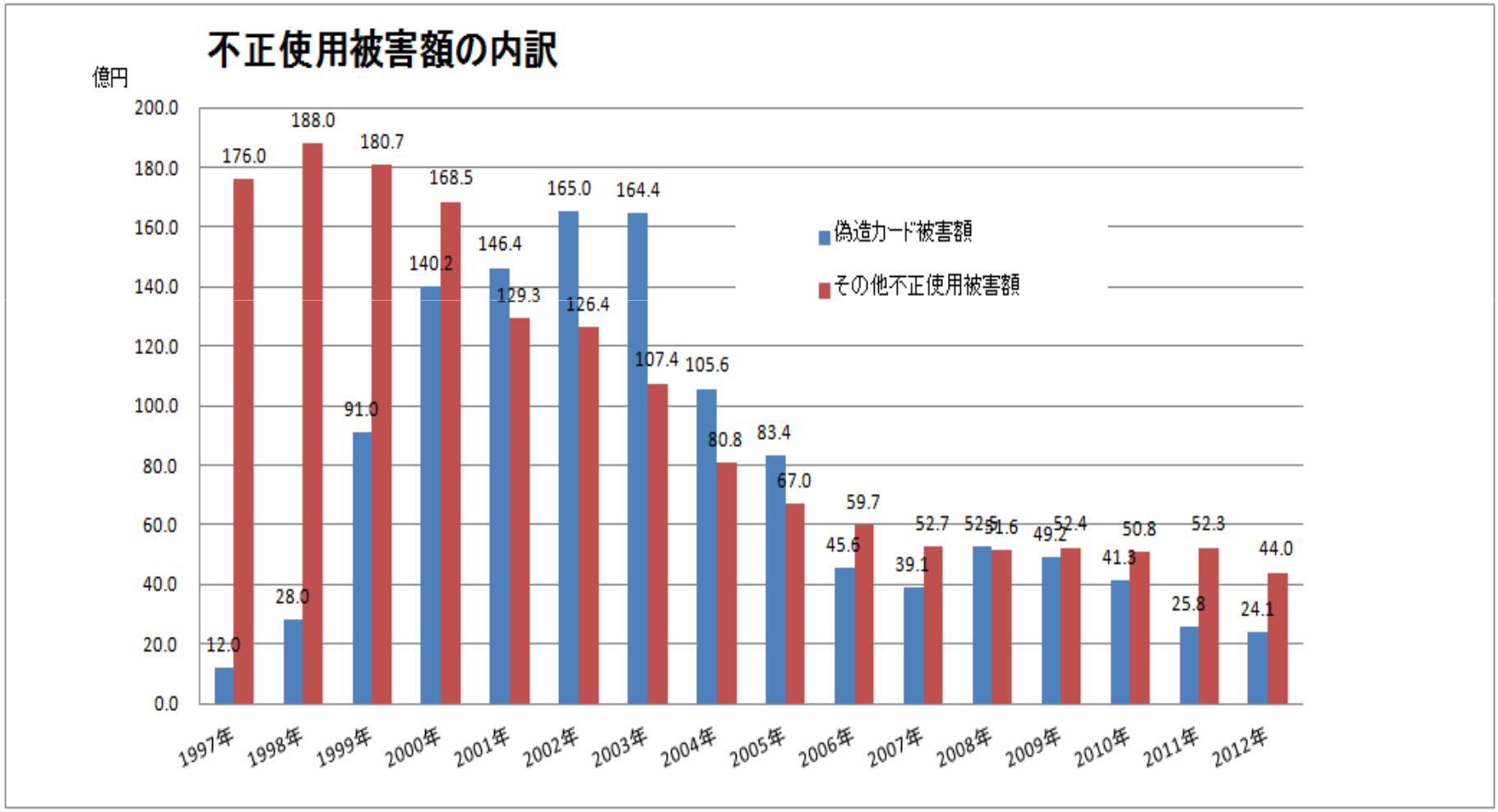
(a) クレジットカード不正使用の状況

クレジットカードの不正使用による被害額は、平成 12 年の308.7 億円をピークに平成13 年の刑法及び関税法の改正と取締当局による積極的な対応などもあり、平成23年には78.1 億円、平成24 年は上半期で31.6 億円まで減少している。

不正使用被害額の内訳を見ると、「偽造・変造カード被害額」はIC カードの普及等に伴い減少傾向にあるが、「その他不正使用被害額」は50 億円前後で高止まりしている。

この「その他不正使用」は、かつては紛失・盗難カードの悪用が大部分を占めていたが、現在は加盟店等から漏洩したクレジットカード番号や有効期限等を不正に利用する「番号盗用」がその多くの部分を占めている。

不正使用被害額の内訳


不正使用被害額の内訳
億円
200.0
180.0
160.0
140.0
120.0
100.0
80.0
60.0
40.0
20.0
0.0
偽造カード被害額
その他不正使用被害額
176.0
188.0
180.7
168.5
165.0
164.4
140.2
146.4
129.3
126.4
107.4
105.6
91.0
80.8
83.4
67.0
59.7
45.6
52.7
39.1
52.4
49.2
50.8
41.3
52.3
25.8
44.0
24.1
12.0
28.0
1997年
1998年
1999年
2000年
2001年
2002年
2003年
2004年
2005年
2006年
2007年
2008年
2009年
2010年
2011年
2012年

2-（１）情報セキュリティ対策②

(b) 情報セキュリティ対策の現状

業界として導入を進めている情報セキュリティ手段としては、(1)IC カードの推進、(2)3D セキュアの推進、(3)PCI DSS の導入推進があげられる。

セキュリティ対策	目的	対象取引	概要
PCI DSS	カード情報漏洩への対策	対面取引／非対面取引全般	○加盟店、決済代行業者、及びクレジットカード会社において、クレジットカード会員データを安全に取り扱うことを目的として作成された国際的なセキュリティ基準。 ○ＪＣＡが実行計画を策定し、業界全体として対応を進めている。 ○導入の障害となっているのは対応のための費用。特に加盟店に費用負担が生じることが、導入推進を難しくしている。

2-（１）情報セキュリティ対策③

(d) 情報セキュリティ対策の普及を阻害している要因

業界として取組みが進められている情報セキュリティ手段（IC カード、3D セキュア、PCI DSS）には普及に向けた課題がある。

まず、導入のために費用や労力がかかることがあげられる。セキュリティ対策は売上増に直結する投資ではないため、加盟店は導入に対して消極的になりがちであり、実店舗や主要なインターネットモールにおいて3D セキュアやPCI DSS への対応が進まない一因となっている。また、クレジットカード会社（アクワイアラ）にとって加盟店は顧客であるため、両者の力関係から、セキュリティ対策の導入を強力に推進するのは難しいという事情もある。また、セキュリティ対策の導入による不正利用防止の効果が明らかではないために、クレジットカード会社や加盟店がセキュリティ対策導入のためにどの程度の費用をかけてもよいか判断しにくいという点もあげられる

2-（１）情報セキュリティ対策④

（イ）情報セキュリティ対策の向上に向けた課題
（b）業界として取り組むべき情報セキュリティ対策
②関連当事者に対する働きかけ

b) 加盟店

ハード面での情報セキュリティ強化だけでなく、加盟店向けの情報セキュリティ教育のようなソフト面でのアプローチも重視していく必要がある。例えば、情報管理の面で問題を起こした加盟店に対し、加盟店契約を継続するためにはJCAの運営する「個人情報取扱主任者認定制度」での講座の受講や資格の取得を求めることなどが考えられる。また、クレジットカード会社各社で、または業界全体で、加盟店のための教育プログラムを作っていくことも検討の対象となる。

(c) 制度面での対応の必要性

① 加盟店での情報セキュリティ手段導入に関する行政のサポート

我が国では加盟店が複数のクレジットカード会社（アクワイアラ）と加盟店契約を結んでいることが多く（マルチアクワイアリング）、このような環境下では加盟店に対するクレジットカード会社の立場が相対的に弱いため、加盟店向けの情報セキュリティ対策の導入にあたってクレジットカード会社が強力な推進を行うことが難しい状況となっている。

そのため、加盟店での情報セキュリティ対策については、行政によって制度面での対応がなされることによって、クレジットカード会社が推進を図りやすくなるという意見があった。

2-（１）情報セキュリティ対策⑤

③ クレジットカード会社以外の主体によるカード情報の適切な管理に向けた措置

現状では、割賦販売法によりクレジットカード番号等の適切な管理についてクレジットカード会社（イシュア及びアクワイアラ）に対する義務付けはあるものの、販売業者や決済代行業者に対する直接の規制はなく、カード会社に対して必要な指導その他の措置を講じる義務を課すという間接的なものにとどまっている。また、その指導・措置の内容は、漏洩などの事故が発生した場合の状況把握や再発防止のための指導にすぎない。しかしながら、現実にはクレジットカード会社以外にもクレジットカード情報を電算処理において大量に扱う事業者は存在している。特に、電子商取引においてはクレジットカード取引の処理において決済代行業者や決済処理を代行する情報処理業者（サードパーティプロセッサ）の果たす役割が大きくなっているという現状がある。これらの事業者が取り扱うクレジットカード情報は大量であり、情報漏洩のリスクも大きなものとなっている。

このような現状を鑑みて、クレジットカード会社以外の主体のうち大量のクレジットカード情報を取り扱う者（決済代行業者、サードパーティプロセッサ、規模の大きい販売業者など）については、クレジットカード情報の管理が適切に行われるよう、効率性、有効性の要素を考慮しつつ実現可能な方策を検討する必要性があると考えられる。

経済産業省の認識

Q:クレジットカードに関しては、業界がガイドライン等を設けて、3Dセキュアや PCIDSSを推進しているが、その進捗状況をどうみているか。

A:経済産業省　取引監督課長　苗村公嗣氏

本人認証やカード情報の安全管理を強化する方法はいろいろあると思うが、3Dセキュアや PCIDSSの導入は、その有効な手段の一つであり、その推進に向け、業界が自主的に行動指針を策定し、連携しあっていくことは、非常に望ましいことだと受け止めている。

とはいえ、なかには独自のセキュリティシステムを構築している事業者もいるとか、システムなどの投資に相応のコストがかかるなどの理由により、その推進が容易でないこともよく理解している。日本の実情をふまえながら、行政も一緒になって粘り強く取り組んでいく必要があると思う。行政としても、いろいろな機会を利用し、本人認証やカード情報の安全管理体制を強化する必要性を訴えていきたい。また、実際にシステムの脆弱性に起因する事故が生じた場合には、当該事業者おいて適切な対策が講じられるよう、指導監督を行っていく場面もあるだろう。

キャッシュレス社会の進展

自民党選挙公約　J-ファイル2013　総合政策集

290 経済活動におけるキャッシュレス化の推進

IT技術の高度化、サービスの多様化の中で、世界的に経済社会のキャッシュレス化（クレジットカード、デビットカード、電子マネー等の利用）が急速に進展する中で、わが国も、キャッシュレスに対応するためのインフラの整備、利用環境の標準化等により、消費・販売分野における利便性や透明性の向上に努めるとともに、本分野でのグローバルスタンダード化に取り組みます。

その際、比較的対応力が弱い分野に着目し、高齢者を含めた消費者の利便の向上、地方の中小小売業の販売事務の効率化を促し、消費社会全体の健全な発展・拡大を目指します。

ICT成長戦略会議　ICTコトづくり検討会議

報告書（13年6月28日）

5.4. ICTコトづくりの社会実装に向けた仕組みの確立

ICT コトづくりの推進に伴い、モノ・サービスの提供の在り方に変革が生じることが予測される。変革に柔軟に対応するためには、新サービスに対応したネットワーク上での新たな決済システムの開発・確立、モノづくりのネットワーク機能の強化、地域における高度な生産技術とICT の連携等、社会性のある取組が必要となる。こうした取組を実証プロジェクトとして、地域において集中的に実施することが期待される。

５月９日のある構成員の提言
「非現金決済やPOSデータの連携等、情報の流れを活発化させる方策を特区を使って実証実験」

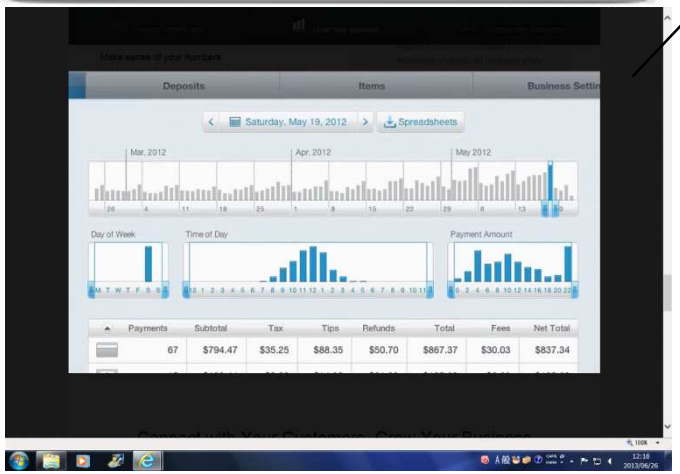
シンクライアント型マルチ端末の動き

- 2012年7月10日、三菱UFJニコスが、JR東日本メカトロニクスと共同開発した「J-Mups」（Joint Multi Payment System）の設置開始
- 2013年2月、iPhone(iPod touch)を端末として活用できる「Poke Pos for J-Mups」開発
- JCBがTMN（トランザクション・メディア・ネットワークス）の「シンクライアント型電子マネー決済システム」の加盟店への導入を開始。TMNへの出資も（SMCC、DNPも出資。2013年3月にはUCも出資、導入）
- トッパン・フォームズの子会社TFペイメントサービスがクラウド型決済プラットフォームサービス「Thincacloud（シンカクラウド）」を展開
- データセンターをPCIDSSに準拠し、カード情報を保護

スマホの決済端末化の商品群

- 「Square（スクエア）」
  （Twitter創業者のジャック・
  ドーシーが09年に開発）
- 三菱UFJニコスが「ペイメント・
  マイスター」を開始（１０年９月）
- 楽天が１２年１２月に「楽天スマートペイ」開始
- ソフトバンクがPayPalと合弁で「PayPal Here」を本格的に推進（１３年３月）
- 三井住友カードがスクエア、クレディセゾンがｺｲﾆｰと提携
- 中小小売店、個人事業主が各社のターゲット
- スマホにはカード情報を残さず、データセンターに吸い上げる。
  データセンターはPCIDSS準拠で高セキュリティ化

Squareレジ（アプリ）の機能



iPadで商品を登録する

・[編集]をタップして、商品のセットアップモードに。
・プラス記号のアイコンをタップし、[商品を登録する]をタップし、商品の写真、名前、カテゴリ、価格、最小単位を登録。税金の[オン]と[オフ]を切り替えて、消費税の設定を行う。
その他、ディスカウントを設定したり、商品カテゴリを設定し管理することも可能。
※オンラインの「Squareデータ」でも商品ライブラリのカスタマイズを行うことが可能。サーバーに保存されたデータはSquareレジアプリと同期される

インタラクティブ分析ツール

・オンラインのSquareデータにログイン
・取引量の推移（上）、曜日ごとの取引履歴（中段左）、時間帯ごとの取引履歴（同中）、支払額ごとの取引履歴（中段右）、カードや現金などの取引種別、売上額、手数料といった取引履歴の内訳（棒グラフ下）が表示される。
　＜その他の機能＞
支払履歴・振込履歴のダウンロード、カスタムレポート作成等

スクエアのアプリの、スマホ、タブレットをPOS端末化する機能が、中小小売店に支持される可能性がある。

PCIDSSを巡る今後の環境変化

- 国際ブランドのプレッシャーを回避するための行動計画だが、いずれ「やるといった責任」が問われる
- 行政は引き続き、カード情報保護を最重要課題と位置付けている
- ICTの進歩により、シンクライアント型端末、スマホのカード決済端末化（POS端末化）といった新しい決済モデルが続々と登場。むしろ、中小小売店における決済を中心に、PCIDSSに準拠したセキュアな環境におかれたカード情報が増えていく
- カード情報を自前で保管管理する、大規模・中規模の実店舗における安全性が問われる