経済産業省

（資料１－１）

産業構造審議会割賦販売小委員会の報告書(追補版)について
（クレジットカード取引システムの健全な発展を通じた消費者利益の向上に向けて）

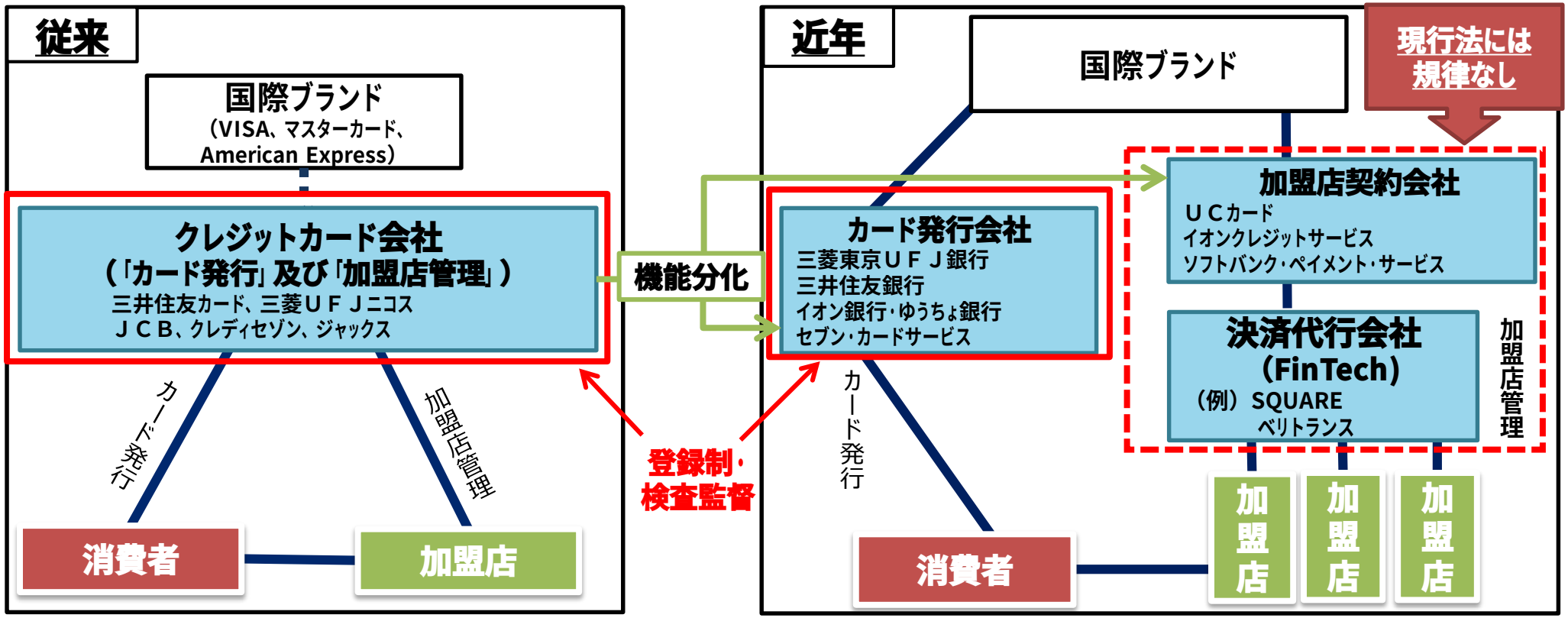
平成２８年６月

商務流通保安グループ

商取引監督課

クレジット取引の構造変化と悪質加盟店対策の必要性

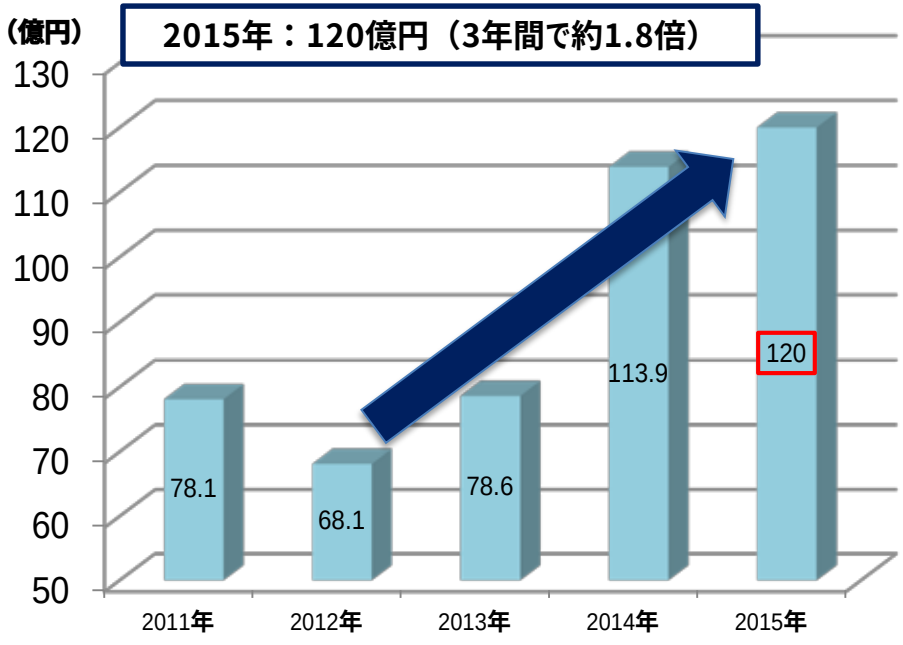
- 「カード発行」と「加盟店管理」に**機能分化**（**加盟店契約専業**の事業者も出現）。
- **IT系の新興企業が決済代行業に参入**し、ネット取引を中心に、**加盟店の裾野を拡大**。
- 一方、決済代行業者の中には、「営業」優先で**「加盟店管理」が不十分**な者も出現。
- **ボーダーレス化**も進み、**悪質加盟店が審査の甘い海外の加盟店契約会社に流れる**傾向。
- こうした状況に対処するため、昨年７月に、**加盟店契約会社の登録制や加盟店管理の義務付け等**を提言する報告書を公表。



クレジット取引の不正使用被害の増加

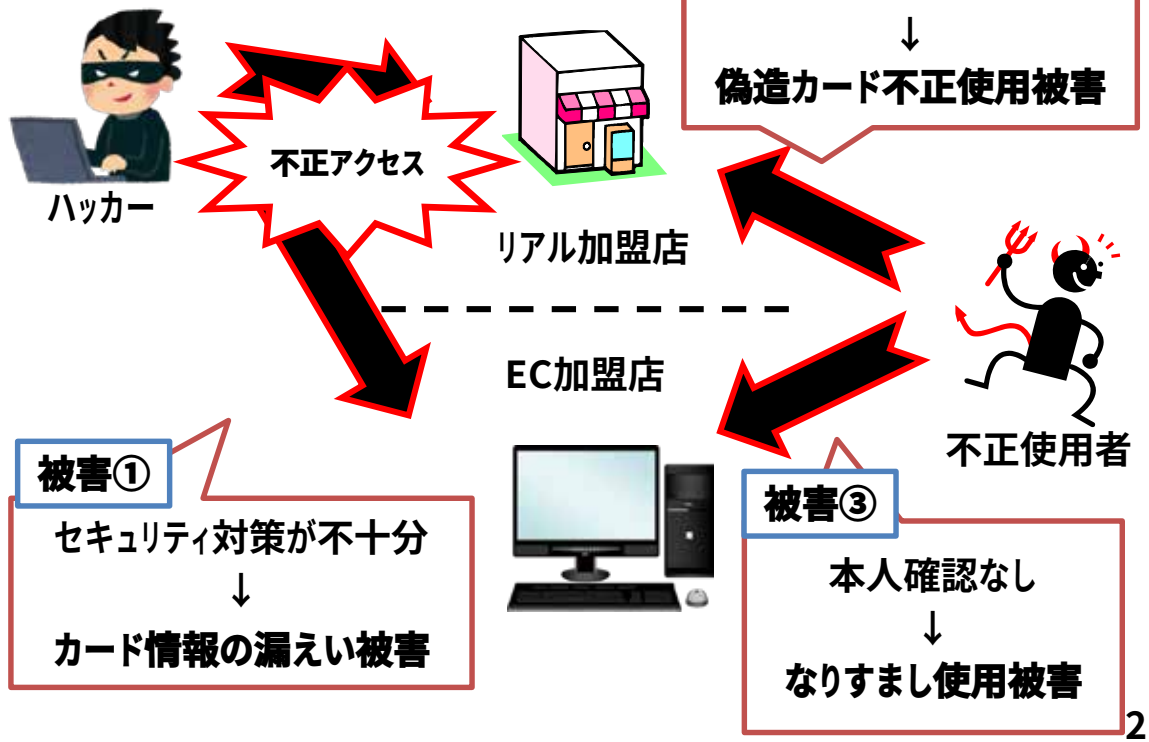
- 昨今、セキュリティ対策が不十分な加盟店を狙った不正アクセスにより、カード情報の漏えいが拡大。※2015年で30件（前年比2.3倍、報告ベース）
- これに伴い、窃取したカード情報を使って、偽造カードや本人になりすました不正使用による被害は増加（2015年で120億円）。
- 不正使用は国境を越えて行われ、換金性の高い商品の購入を通じて、犯罪組織に多額の資金が流出しているとの指摘あり。

クレジット取引の不正使用額の推移



（注）不正使用被害額は、国内発行クレジットカードでの不正使用分で、カード会社が把握している分を集計（海外発行カード分は含まれない。）。
出所：一般社団法人日本クレジット協会「クレジットカード不正使用被害の集計結果について」

クレジット取引での被害イメージ



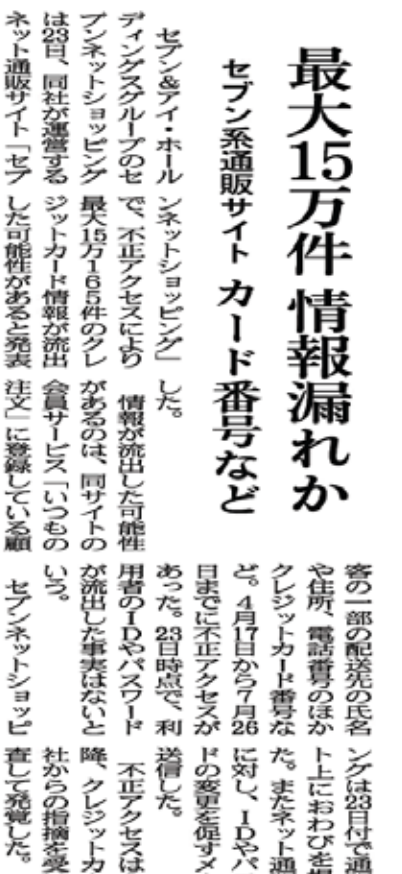
加盟店からのカード情報の漏えい～①ECサイト

- 近年公表された大規模なカード情報漏えい事案（１万件以上のもの）は、全て（４年間で18件）が加盟店からの情報漏えいによるもの。
- カード情報を扱う責任について、加盟店自身に当事者意識が希薄なことが問題と指摘されている。

最近の情報漏えい事例

	件名	公表日	流出原因	カード情報の漏えい件数
1	クーコム（株） （宿泊予約サイト「トクー！」）	平成27年 ７月	外部からの不正アクセスにより、**会員氏名、カード番号、有効期限、セキュリティコード、住所、電話番号、メールアドレスが流出**	可能性のある件数 約２万２千件
2	DL Market （音楽、書籍等のネット販売）	平成27年 ９月	SQLインジェクション*１によって、**会員氏名、カード番号、有効期限、セキュリティコード等が流出**	可能性のある件数 約２万３千件
3	江崎グリコ（株） 「グリコネットショップ」 （菓子・飲料等の通販サイト）	平成28年 ３月	SQLインジェクションによって、**会員氏名、カード番号、有効期限、カード名義、住所、電話番号、メールアドレス等が流出**	可能性のある件数 約４万４千件

＊１　アプリケーションのセキュリティ上の不備を利用し、アプリケーションが想定しないSQL文を実行させることにより、システムを不正に操作する攻撃方法のこと



最大15万件 情報漏れか

セブン系通販サイト カード番号など

セブン&アイ・ホールディングスグループのネットショッピング「セブンネットショッピング」で、不正アクセスにより最大15万165件のクレジットカード情報が流出した可能性があると発表した。23日、同社が運営するネット通販サイト「セブンネットショッピング」は23日付で通販サイト上におわびを掲載し、クレジットカード番号など。4月17日から7月26日までに不正アクセスがあった。23日時点で、利用者のIDやパスワードの変更を促すメールを送信した。

情報が流出した可能性があるのは、同サイトの会員サービス「いつもの注文」に登録している顧客の一部の配送先の氏名や住所、電話番号のほか、不正アクセスは6月以降、クレジットカード会社からの指摘を受け、調査して発覚した。

平成25年10月25日　日経MJ　4面

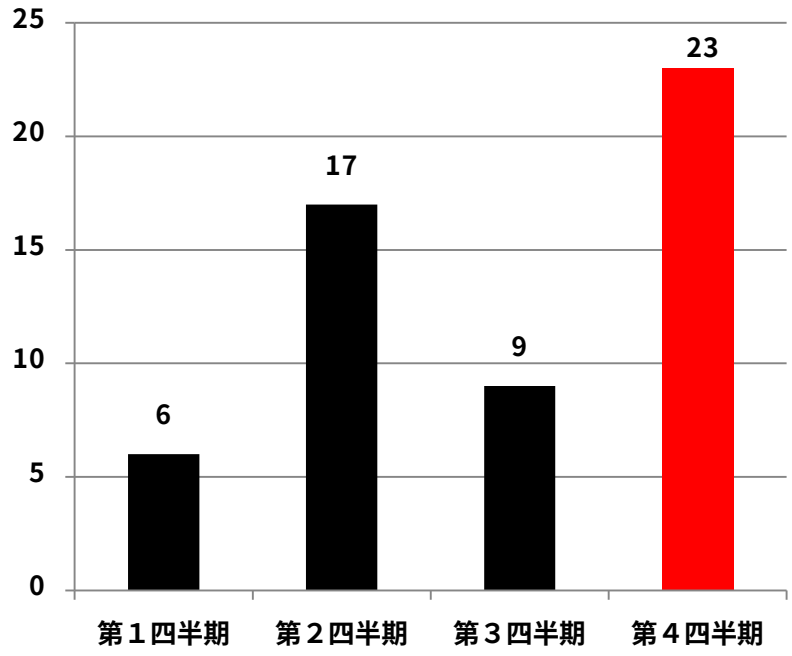
加盟店からのカード情報の漏えい～②POSシステム

- 大手ホテルチェーンの米ハイアット社が、決済処理システムでマルウェアの感染を確認。調査の結果、日本国内の４拠点（パークハイアット東京ほか）を含む54の国・地域／250拠点で感染していたことが判明。国内初のPOSシステムのマルウェア感染による被害。
- これにより、カード会員氏名、カード番号、有効期限、セキュリティコード等が窃取された。
- POSシステムを標的としたマルウェアの検出台数は世界的に増加傾向。日本でも2015年から急増。（2015年検出台数55台、前年比約７倍、米・フィリピンに続き世界第3位）。

最近のPOSマルウェア被害事例

時期	企業名	被害内容
2015年3月	マンダリンオリエンタル	米国とヨーロッパの拠点でマルウェア感染
2015年4月	White Lodging	北米10拠点のレストランやラウンジで約7ヶ月間POSマルウェア感染
2015年10月	Trump Hotel Collection	北米7拠点のレストランやギフトショップで約1年間にわたりPOSマルウェア感染
2015年11月	ヒルトン	複数のグループホテルで約4ヶ月間にわたりPOSマルウェア感染
2015年11月	スターウッド	北米50拠点のレストランやギフトショップで約11ヶ月間にわたりPOSマルウェア被害
2016年1月	ハイアット	日本を含む全世界54ヶ国地域250拠点で約4ヶ月間POSマルウェア感染

2015年POSマルウェア検出台数（日本）



（出典）2016年２月トレンドマイクロ調査

我が国のクレジット決済のＩＣ対応化における現状と課題

○ クレジット決済のIC対応化は、カード偽造防止の唯一無二の対策であり、セキュリティの世界標準であるが、現状、我が国は取組が遅れている。

現状・課題

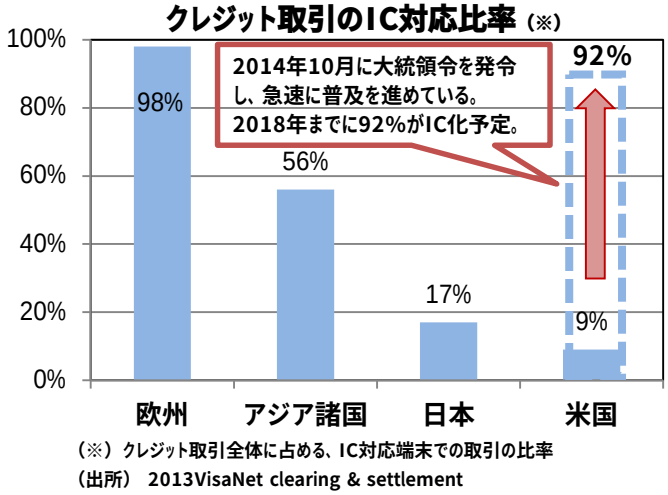
① **訪日外国人の50%**は、クレジットカードを利用。

（出所） 観光庁 訪日外国人の消費動向（平成26年報告書）

② 訪日外国人から見た日本の改善すべき点

セキュリティの高い**ICカード対応の決済環境**を整備すべき：**49％**

（出所） 日本クレジットカード協会によるアンケート調査（平成26年12月）



（※）クレジット取引全体に占める、IC対応端末での取引の比率

（出所） 2013VisaNet clearing & settlement

カードのIC化

◇**偽造カード**は、**磁気カードをコピー**して作られる。ICカードは、**ICチップ内に情報を暗号化**して格納しているので、情報のコピー（**偽造**）**ができない**。

磁気カードの10～200倍の情報を蓄積

端末のIC対応化

◇**磁気ストライプ**決済では、**スキミングの恐れ**があるが、**IC対応**によりカード情報の処理が**暗号化**されるため、**偽造カードの生成・使用が防止**できる。

磁気ストライプ対応端末

百貨店等での対応例

ICカード・パスワードでの本人確認対応の携帯端末をスマートフォンやタブレットと接続し、無料アプリをダウンロードすることで、中小・小規模の加盟店でも、低コストで安全なクレジットカード決済が可能となる。

モバイル端末での対応例

○磁気決済が中心でセキュリティ環境の脆弱な我が国を狙って、国際的な犯罪が集中（セキュリティホール化）する懸念を払拭するため、IC対応を進め、安全・安心な決済環境整備が喫緊の課題。

クレジット取引セキュリティ対策協議会

- 2020年に向け、「**国際水準のセキュリティ環境**」を整備することを目指し、クレジット取引に関わる**幅広い事業者**（カード会社や、加盟店・関係業界団体、国際ブランド、端末機器メーカー、PSP、セキュリティ事業者、情報処理センター等）**及び行政が参画**して設立（2015年3月）。
- **目標**、**各主体の役割**、**当面の重点取組**をとりまとめた「**実行計画**」を策定（2016年2月）。
- **日本クレジット協会**を中心に、**「実行計画」の推進体制を構築**。2020年に向け、実行を推進。

「実行計画」における対策の３本柱

１．カード情報の漏えい対策

◇カード情報を盗らせない

- 加盟店におけるカード情報の「非保持化」
- カード情報を保持する事業者のPCIDSS準拠

２．偽造カードによる不正使用対策

◇偽造カードを使わせない

- クレジットカードの「100%IC化」の実現
- 決済端末の「100%IC対応」の実現

３．ECにおける不正使用対策

◇ネットでなりすましをさせない

- 多面的・重層的な不正使用対策の導入
  （パスワードによる本人認証、セキュリティコード等）

今回の割賦販売小委の報告書取りまとめについて

○平成26年8月、経済産業省は、消費者委員会から、「クレジットカード取引に関する消費者問題についての建議」を受けた。

○ 昨年７月、産業構造審議会割賦販売小委員会において、悪質加盟店排除等に向けた割賦販売法の見直しについて報告書を取りまとめた。

○ クレジットカード取引を巡るセキュリティリスクの増大等を踏まえ、本年４月から同小委を再開し、セキュリティ対策の強化等について改めて審議を行い、５月２６日に報告書（追補版）として取りまとめ。（６月２日に公表）

第１章　平成２７年報告書以降の状況変化と取組の進捗

第２章　クレジットカード取引におけるセキュリティ対策強化について

第３章　改正特商法への割販法における対応について

第４章　FinTechの活用による新たな業態への対応について

１．クレジットカード取引におけるセキュリティ強化

- 加盟店からのカード情報の大型漏洩事件の続発、不正使用被害の増加傾向等、セキュリティリスクの高まる中、「クレジット取引セキュリテイ対策協議会」の実行計画（本年2月）の実効性を確保するため、法制上の措置を講じることが必要。
- クレジット取引のセキュリティ確保のため、消費者の理解と協力が必要。「見える化」を推進し、「マルチステークホルダー・プロセス」でも、消費者とのリスクコミュニケーションを促進。

１．加盟店等へのセキュリティ対策の義務づけ

- **全ての関係事業者**に対し「**リスクに応じた措置**」を義務づけ
  - ①**情報管理**（漏洩対策）：加盟店を含め、カード情報を保有する事業者　※個人情報保護法の特別法的な位置づけ
  - ②**不正使用対策**：加盟店
- 義務履行のための具体的手段については、技術進歩に応じて、多様な手段を許容する「**性能規定**」の考え方を採用。

２．加盟店契約会社等による加盟店調査を通じたセキュリティ強化

- 加盟店契約会社等が、**加盟店調査の一環**として、加盟店における**セキュリティ対策の状況を確認**し、是正指導等の適切な対応を行う。　※クレジット取引のネットワークの「ゲートキーパー」としてスクリーニング・モニタリング機能を果たす。

３．認定割賦販売協会（日本クレジット協会）を中心としたセキュリティ推進体制の構築

- **法定業務**として「セキュリティ対策の推進」を追加。
- 協会の役割として、「**実行計画**」**の実施**を進めるとともに、「性能規定」の下で、**標準的な対策に関する指針**を策定。

２．今般の特定商取引法改正を踏まえた割賦販売法における対応

- 今般の特定商取引法改正を受け、消費者利益保護の観点から必要な対応を行う。

特商法改正の内容	割販法における対応
１．適用対象の見直し（指定権利の拡大）	・特商法で今回新たに追加された権利（社債その他の金銭債権、株式等の社員権）に関し、クレジットに係る消費者被害事例は確認されていないため、**現時点では割販法上は追加しない**。 ・なお、特商法の「役務」の解釈を踏まえ、割販法においても、適切に対応。
２．電話勧誘販売における過量販売への申込みの撤回等の導入	・特商法上、販売契約の申込みの撤回等を行う場合、個別クレジット業者に既払金の返還を求められるよう、**特商法改正と平仄を合わせ、割販法上も申込みの撤回等を導入**。
３．訪問販売等における販売業者等による不実告知等の場合の取消権の伸長等	・**特商法改正案と平仄を合わせ**、割販法上の個別クレジット契約に関する取消権の消滅時効も**１年に伸長**。

３．FinTechによるイノベーション促進のための環境整備

- 割賦販売法では、<u>カード利用時の加盟店等の書面交付義務</u>を規定（項目も詳細で多数）。※書面一括法制定（2000年）以降「書面が原則」で、事前に消費者の個別の承諾があった場合のみ電磁的方法が利用可能。
- モバイル端末を提供するFinTech企業から、<u>カード決済サービスの展開のネック</u>となっているとの指摘あり（FinTech協会等）。
- インターネットの普及等の<u>IT環境変化</u>を踏まえ、消費者保護の観点に留意しつつ、情報提供すべき項目及び情報提供の方法について見直しが必要。

１．提供される情報項目の見直し

- 消費者が、取引のどの段階で、どのような情報が必要か、それをどの主体から提供させるべきかについて、再整理

→**<u>加盟店からの情報提供項目の見直し</u>**

２．情報提供方法の在り方の見直し

- 加盟店等の書面交付義務に関し、現行法の「書面交付を原則、電磁的方法を例外」という考え方を見直し
  （例：消費者がネットを通じて購入の申込みを行う場合）

→「**<u>情報提供義務</u>**」への転換を検討

- その際、高齢者等のネットを利用しない消費者への情報提供が確保されるよう、配慮。

割賦販売法の改正の方向性（案）

１．事業者の登録

- 「**加盟店契約会社**」について**登録制**を導入。
  ※　外国事業者の場合は、国内拠点の設置を要件化。
- 「**決済代行会社（PSP）**」は、**任意登録制**とする。
  ※　加盟店契約会社と同様、加盟店調査ができる体制整備を登録要件に。
- **登録を受けた「決済代行会社」**は、「加盟店契約会社」に代わり、法律に基づく**加盟店管理を代行**することを可能とする。

２．事業者に対する行為規制

（１）**「加盟店契約会社」及び「登録を受けた決済代行会社」**に対し、**加盟店調査を義務づけ**
① 加盟店契約時における基礎的事項の確認（代表者、商材、販売方法等）
② 契約締結後における、悪質加盟店排除のためのモニタリング
③ 加盟店調査の結果に応じた適切な対応（不正を行う加盟店への是正指導や契約の解消）

（２）**加盟店等**に対し、**セキュリティ対策を義務づけ**（リスクベース、性能規定）
① 加盟店や決済代行会社等、カード情報を保有する全ての事業者に情報漏洩対策を義務付け
② 加盟店に対し、不正使用対策（対面は偽造カード、非対面はなりすまし防止）を義務付け

３．行政による監督、処分等

- 報告徴収、立入検査　※セキュリティ対策については勧告や公表制度も検討。
- 行為規制に違反した者に対する、改善命令や登録の取消し
- 改善命令に従わない者に対する罰則