産業構造審議会 商務流通情報分科会 割賦販売小委員会 第14回 議事録

日時：平成28年4月4日（月曜日） 15時00分～17時30分

場所：経済産業省別館3階312会議室

○山本委員長　　皆様、こんにちは。定刻になりましたので、ただいまから産業構造審議会商務流通情報分科会割賦販売小委員会の第14回を開催いたします。

皆様方におかれましては、お久しぶりでございます。ご多忙中のところご出席いただきまして、まことにありがとうございます。

議事に進みます前に、オブザーバーの追加、変更、今回の委員、オブザーバーの出欠状況確認、今回からペーパーレス化の取り組みを実施することにつきまして、事務局から説明をお願いいたします。

○坂本商取引監督課長　　商取引監督課・坂本でございます。皆様、本日はお忙しい中ご参集いただきまして､まことにありがとうございます｡どうぞよろしくお願いいたします。

まず、前回からのオブザーバーの追加、変更についてご連絡させていただきます。今回からＥＣ決済協議会の会長選出企業であるＧＭＯペイメントゲートウェイ株式会社より吉岡様にご出席いただいております。どうぞよろしくお願いいたします。なお、沖田様におかれましては、これまでの議論との継続性という観点から、引き続きご参加いただいておりますので、改めてよろしくお願いいたします。また、消費者庁取引対策課からは、昨年の人事異動に伴いまして桜町課長にご出席いただいております。よろしくお願いします。

次に、委員、オブザーバーの出欠状況についてご連絡いたします。本日は渡辺委員がご欠席ということで、委員、専門委員合わせまして12人中11名ご参加いただいております。ありがとうございます。

最後に、事務の効率化、高度化を図るためのペーパーレス化について、政府全体の方針ということを踏まえまして、大変恐縮ながら、今回の本委員会よりペーパーレスで実施させていただければと思っております。委員、オブザーバーの皆様におかれましては、机にお配りしておりますiPadの電源を入れていただきますと、資料のフォルダが一覧で出てくるかと思いますので、ご確認いただいて、今後、議事進行に応じましてそれぞれの関連資料をクリックして開いていただく形でご利用いただければと思います｡もしiPadの使い方、動作確認等についてご不明な点がございましたら、事務局のほうで係の者が待機しており

ますので、合図を送っていただければサポートに入ります。議事の途中でも結構ですので、お知らせいただければと思います。どうぞよろしくお願いいたします。

大変恐縮ながら、きょうは住田商務流通保安審議官と商務流通担当の松本大臣官房審議官が国会対応の関係で少しおくれての参加になります。ご了承いただければと思います。松本審議官については４時前ごろには到着予定、住田商保審については４時半ごろの到着予定となっておりますので、途中からで大変恐縮ですが、よろしくお願いします。

また、そのときに改めてご挨拶をさせていただきたいと思いますが、事務局より、今回の割賦販売小委員会の再開につきましては、前回、昨年７月にまとめていただきました報告書を基本としながら、これを法改正につなげるべく準備を進めているところでございます。その後、昨年７月以降の特にクレジット取引にかかわるセキュリティの状況変化、あるいは今国会に提出されております特定商取引法改正案も踏まえまして、改めて昨年７月の報告書に追加的に載せるべき事項があるのかどうかという観点から、今回改めてご審議をお願いしたいという趣旨でございます。どうぞよろしくお願いいたします。

○山本委員長　　どうもありがとうございました。

それでは、本日の議題でございます。資料１にお示ししておりますように、クレジットカード取引におけるセキュリティ強化となってございます。

最初に、議事次第に従いまして、５つのテーマにつきまして順次プレゼンテーションをいただいてまいりたいと思います。まず、資料２、産業・金融・ＩＴ融合に関する研究会、いわゆるFinTech研究会でのご議論につきまして、経済産業政策局産業資金課の福本課長からご説明をお願いいたします。よろしくお願いいたします。

○福本経済産業政策局産業資金課長　　産業資金課・福本でございます。遅参いたしまして申しわけございません。それでは、資料２に基づきましてご説明させていただきます。

FinTechについてということで、我々は、こちらでの議論も踏まえまして、全体的な金融とテクノロジーの融合について議論しているところでございます。

ページおめくりいただきまして、産業・金融・ＩＴ融合に関する研究会というのを昨年から集中的に開催いたしました。

次のページをごらんいただきまして、この研究会自身は、FinTechは新しい分野でもあるということで、まずどんな課題があるのかということもなかなかみえにくい部分があったので、かなり大きなテーマでもってさまざまな方にご参加いただいて開始いたしました。

次のページをごらんいただきまして、３ページ目でございます。今まで10回研究会をや

ってございますけれども、テーマを変え、参加者もさまざまな立場の方にご参加いただいて、今までここに挙げられております延べ80名の方にご参加いただいております。その中には、こちらの審議会に加わっていただいております方々にもご参加いただいております。

４ページ目は、細かいので詳細に入りませんけれども、これまでの研究会で議論されたことという全体像が書いてございます。上のほうには、FinTechと呼ばれているものがＢｔｏＢの分野、ＢｔｏＣの分野、あるいは保険といった分野でどういうことが起きているのかということ。下のほうは、それも踏まえた上でどういう課題があるのか。業特有の課題でありますとか、全体に通じる情報システムの課題といったものが議論されております。

そういった議論を受けまして、今FinTechで起きていることはこういうことではないかというのを我々なりにまとめたのが５ページ目以降でございます。５ページ目は非常に簡単にFinTechの定義から入っておりますが、その下の部分でございます。金融のＩＴ活用というのが昔からいわれていたけれども、今、なぜ改めていわれているのかという部分について、大きく２つのことがいわれております。

１つは、従来型の金融に対する不信、不満といいますか、まだニーズが満たされていない部分がある点。右側のところでは、圧倒的にＩＴ技術が進展して、コストが劇的に下がった。スタートアップして企業を起こしていく、開発するコストが下がった。それからまた、今までインフラのないところにもみんなスマートフォンで通じるようになった点。この２点を大きな流れとして捉えております。

６ページ目は、いわゆるFinTechといわれている分野にどういう分野があるかということでございます。

７ページ目が今時点でのまとめでございます。今世界で起きていることということでまとめておりますけれども、上のほうは全世界でこういうことが起きているということでございまして、下のほう日の丸が書いてありますのは、その中でもとりわけ日本の文脈ではこういう点が重要だろうということでございます。上のほうはよくいわれていることでございますが、左側、金融を供給、提供する側のほうでいきますと、プレーヤーの形が大きく変わってきているということ。それから、既存の金融機関は今まで積み重ねてきたシステムでありますとか人、設備といったものが逆に不利になってきているのではないかという問題意識がございます。

あるいは右側、ユーザーのほうでございますけれども、こちらでご議論いただいております決済、クレジットカードといった分野を初めとしまして、さまざまなＢｔｏＢ、ＢｔｏＣ

での影響が出てきているということでございます。

日本の文脈として、我々の中で重要だろうというところにつきましては、下の４つに大きくまとめてございます。上から申し上げますと、まず中小企業の経営を高度化していく。生産性を高めていく。資金調達を円滑化していくという面があろうかと存じます。それから、金融機能、インフラ、これまで投資してきたインフラをどのように高めていくのか。競争力をどう上げていくのかという点でございます。それから、全体的な新陳代謝、新しいものを生み出す存在としてのFinTech産業をどのように高めているのか。それから、家計の資産形成ということで、貯蓄から投資への流れを大きく加速する動きではないかという点でございます。

８ページ目は、こちらの審議会でこれからご議論いただく部分と関連いたしますけれども、FinTech時代の課題と対応について大きく左側と右側の２つに分けてございます。

左側の緑の部分につきましては、まず今まで店頭にあったデータがデジタル化されてくる。あるいはデジタル化されているいろいろなソーシャルメディアなどに載っているデータを活用して、活用可能な状態になるということがございます。その中にはキャッシュレス化の動きでありますとか、クレジットカードにおけるデータを標準化するといった話、あるいは金融ＥＤＩも――これは金融庁と一緒に議論しておりますけれども、インフラとしての整備があろうかと思います。そういうデータが整ったところで、そのデータが行政なり民間のところで使えるようになるためには、プロセス全体が変わっていく必要があろうということで、とりわけ金融機関、金融サービスというのは規制でありますとか制度と直結する部分がございますので、このあたりを進めていくというのが左下でございます。

右側のところはFinTechイノベーションに対応する環境整備といたしまして、特に上の部分はこちらでご議論いただく部分とも関連すると思います。イノベーションを促していくための今までと少し違う新しい観点での規制なり制度の枠組みの仕方があろうかと思います。恐らく割販法でご議論いただくのも、その先駆けといいますか１つのケースとして、その他の金融の規制でありますとか枠組みにも影響を及ぼしていくといいますか、参考になっていくのではないかと考えております。

それから、右下のところはFinTechのビジネスを応援するということだけではなくて、アメリカ、アジア等では、どちらかというとFinTechはベンチャー企業が担い手であるということでございますが、世界的には従来型の金融機関でありますとかベンチャーから大きくなって、むしろ本格的に金融サービスを提供しているところが主役になってきている面も

あります。そういう意味では、日本においてもさまざまなプレーヤーの方、今までの金融サービスを提供している方も含めて、この機能を高めていくことが課題になってこようかと存じます。具体的政策については、まさにこちらでのご議論も受けながら、引き続き検討してまいりたいと考えております。

それ以降は参考でございますので、最後の11ページ目だけごらんいただきます。先ほど少し申し上げましたＩＴ、あるいはデータを使っていくためのインフラという面につきましては、さまざまな入り口といいますか接点がございます。今まではそれぞれ別個に考えられてきたものが、実はデータをつなげることで大きく価値を生み出す可能性があるのではないかということでマッピングしているところでございます。

早口でございましたけれども、私からは以上でございます。

○山本委員長　　どうもありがとうございました。

引き続きまして、クレジット取引セキュリティ対策協議会の実行計画につきまして、事務局と日本クレジット協会理事、当小委員会の専門委員でもあられます與口理事からご説明をお願いいたします。まず、事務局から。

○坂本商取引監督課長　　ありがとうございます。資料３をごらんいただければと思います。こちらは経済産業省と日本クレジット協会連盟の資料ということで準備させていただいております。前半、事務局から最近のクレジットカード取引のセキュリティに関する背景になりますけれども、直近の状況をご紹介させていただいて、後半、セキュリティ協議会の事務局であられたクレジット協会の與口理事に、先々月、２月23日にまとめられた実行計画の中身についてご紹介のバトンタッチをしたいと思います。

まず、めくっていただきまして１ページ目でございます。これは釈迦に説法かもしれませんが、クレジットカードの取引高は一貫して順調に拡大しているということで、青いグラフがクレジットカードの利用額、赤い棒がネット取引の金額となります。こうやって並べてみていただきますと、ネット取引の拡大に伴いまして、それに牽引されるような形でクレジットカード取引が伸びているということで、民間の最終消費支出の16％まで来ています。他方で、青いボックスの参考というところで書かせていただいていますように、諸外国に比べますと、日本のカード利用率16％というのは、まだまだ伸びる余地が大きいだろう、発展段階にあるのではないかということです。

次の２ページ目をみていただきますと、一昨年、日本再興戦略2014になりますが、2020年のオリンピックイヤーに向けてキャッシュレスの推進を図るための１つの大きな大前提

として、クレジットカードを消費者が安全に利用できる環境整備が再興戦略の中にも位置づけられていて、安全利用できる環境がますますクレジットカードの利用を伸ばすのに必要だということが政府の方針として示されているということでございます。

これを受けて同年12月には、キャッシュレス化に向けた方策の中に、具体的に悪質加盟店の排除ですとかクレジットカード番号の管理、あるいはＩＣ対応などのセキュリティ強化が関係省庁合同のとりまとめの中でも明記されております。さらに、昨年の再興戦略の中では、同じように安全利用できる環境整備ということで、クレジットカードのＩＣ化の推進といったことが引き続き明確に掲げられているということでございます。

次、めくっていただきまして３ページでございます。訪日外国人は着々と増加していまして、右下のグラフにありますように、訪日外国人数も2020年2,000万人という目標だったのを早くも昨年段階でそれに近いところまで到達しており、それに伴う消費額も非常に急速に伸びている中で、先ほどご紹介したように、もともと諸外国では日本以上に自国でのカード利用率が高く、訪日外国人の50％は観光で日本にやって来てクレジットカードを利用している。

こういった方々は日本のカード利用環境についてどんな意識をもっておられるかという、これは日本クレジットカード協会のアンケート調査を引っ張っていますけれども、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。逆にいうと、磁気ストライプで読み取られている環境について、改善すべき事項だと回答いただいている方が49％ぐらいいるということでございます。インバウンド事業をしっかり取り込んでいくためにも、加盟店におけるセキュリティの向上が喫緊の課題になっているのではないかということでございます。

４ページをごらんいただきますと、後ほどサイバーセキュリティセンター内閣参事官からもご紹介いただきますが、政府全体で取り組んでおりますサイバーセキュリティ対策の中でもセキュリティ基本法に基づきまして、クレジット分野というものが電力やガス、金融と並びまして、特に重点的にサイバーセキュリティ対策に取り組むべき重要インフラということで、13分野の１つに指定されているものでございます。情報システムが障害に至った場合、国民生活に多大な影響を及ぼす重要インフラということで指定を受けております。

左下にございますように、重要インフラに関する行動計画の中で、サービスの持続的な提供を行うことが重要インフラの防護の目的ということで、ＩＴ障害を減らすことに加え

て、障害発生時の迅速な復旧という２段構えで大きな目的、目標が掲げられているということでございます。こちらは後ほどまたプレゼンの中で詳しくご紹介いただく予定にしております。

５ページでございます。クレジットカード取引の不正使用被害が最近どのようになってきているかというので、左下のグラフをみていただきますと、2012年以降、ここ３年ばかりクレジットの不正使用額が大幅に伸びている。３年で約1.8倍ということです。では、どういった仕組みで不正使用につながっているのかというのをお示ししているのが右側のポンチ絵でございます。

まず、対面の加盟店、あるいはネット等の非対面の加盟店に対してハッカーが――国際的に活動しているものが多いといわれていますけれども、不正なアタックをかけるということで、加盟店の中に蓄積されたカード番号等を抜き取っていくというのが第１段階でございます。

抜き取られたカード情報が今度は右側に来て不正使用する人に渡りまして、対面加盟店については､先ほどの磁気でつくられる偽造カードで不正使用するということになります。ネット取引であれば、カード番号があればお買い物できてしまうところも多いですので、本人になりすまして不正使用が行われるという形で実際の不正使用が起こっていくという２段階の仕組みになっております。

ちょうど先月末に発表された2015年の数字が年間120億ということで､こちらはクレジット協会の統計でございますが､カード会社が把握して負担している部分だけで120億。これについてはカード会社の負担ということで、直接消費者の負担にはなっていない金額について取り出した数字でございますが、上の箱の３つ目にございますように、カード会社が負担しているからいいではないかということではなくて、国境を越えて国際的な犯罪組織に犯罪資金として渡っているだろうという指摘もございますので、そういった観点からも深刻な状況だろうと考えております。

６ページをみていただきますと、最近の大規模情報漏えいにつきましては、全て加盟店からの情報漏えいになっております。１万件以上のものだけに絞って４年間で18件。そもそも情報漏えいの事案もふえていますし、大規模なものだけをとってみても全て加盟店からということで、これにつきましては前回、昨年までのこちらの小委員会でもご議論いただいていたかと思いますけれども、加盟店の中には、カード情報を取り扱っていることについての当事者意識が必ずしもしっかりしていない希薄なところもあるのではないかとい

うご指摘もございます。

直近の例でいいますと、一番下にありますように、先月、江崎グリコの通販サイトからも４万件に及ぶカード情報を含む個人情報が漏えいしたということで、大きく報道されているところでございます。

７ページでございます。２年半前になりますけれども、アメリカの大手スーパーで大規模漏えい事件、日本と桁が違うのですが、4,000万件のカード情報が漏れるという、これが大きな社会問題となり、後ほど出てきますけれども、ＩＣ対応を中心とするセキュリティ対策に大きくかじが切られた１つのきっかけになった事件でございます。漏えいの規模が大きいということもありますし、経営の責任も問われ、最終的にはＣＥＯも退任に追い込まれたという事案になっております。

次の８ページでございます。先ほど６ページでご紹介したのは、主にＥＣ加盟店を狙った不正アタックでございましたが、直近にみられますのがＰＯＳ加盟店を狙ったマルウエアの感染件数が非常にふえてきているということでございます。

昨年のマルウエア検出台数（日本）というグラフをお示ししておりますけれども、2015年、第４四半期に向けて急増していることに加えまして、その前の2014年８件に対して2015年55件ということで、約７倍感染件数が急増しているということでございます。これに加えて、ことしに入ってアメリカのホテルチェーンのハイアット社がマルウエア感染で実際の情報漏えいが発表された事件、記憶に新しいかと思います。その中で、日本国内でＰＯＳ加盟店からマルウエアの攻撃による情報漏えいが実際確認されたということでは、国内初の実被害が生じたということもあわせてお示ししているところでございます。感染件数がふえていることに加えて、実際の被害も出たということでございます。

私からの最後、９ページです。特に偽造カードの不正使用対策ということで、国際標準になっておりますＩＣ対応につきまして、左下のグラフをみていただきますと、これは2013年の数字でございますが、国際比較しますと、ある意味、日本とアメリカがＩＣ対応の後進国でございました。こういった中、世界全体の不正使用の約半分がアメリカで発生していたということでございますが、その後、先ほどのターゲット社の情報漏えい事件が社会的に大きく取り上げられ、ここにございますように2014年、翌年10月にはクレジット決済のＩＣ対応化について大統領令が発令されて、アメリカでのＩＣ対応の取り組みも一気に進むことになってきております。後ほど日本クレジットカード協会様から詳細ご報告いただきますけれども、2013年の日本よりもアメリカがおくれていたという状況は既に逆転

されておりまして、ここ２年ほどでアメリカも92％ぐらいに到達するだろうという予測が示されているところでございます。

少し小さくなって恐縮ですが、右側のグラフでお示ししていますのは、ちょうど10年ほど前に欧州でＩＣ対応が進んだときに、１つの例としてイギリスで発行されたカードの不正利用がどの国で起こっているかということを時系列で追ったものです。このときＩＣ対応の進んだ国からＩＣ対応のおくれた国に不正利用のリスクが実際シフトしたということを１つの過去の教訓としてお示ししているところでございます。あわせて考えますと、アメリカで急速にＩＣ対応が進む中、偽造カードということで考えますと、いよいよ日本がセキュリティホール化して、もともと国際的な不正利用の犯罪組織はボーダレスに活動しているものですので、国境を越えて不正使用の被害リスクは日本に流入してくるのではないかと非常に危機意識をもっているということでございます。

10ページ以降、こういった危機意識を共有しながら、国際水準のセキュリティ環境の整備を目指してちょうど１年間議論してきていただきました協議会の実行計画を與口理事からご紹介いただければと思います。

○與口専門委員　　10ページ目をおあけいただければと思います。2020年に向けて国際水準のセキュリティ環境を整備するという目的に対しまして、下のほうにございますようなクレジット取引に関する多くの方々に幅広くお集まりいただき、行政にも全面的なサポートをいただいて、この２月に実行計画をとりまとめたところでございます。

メンバーにつきましては、お手元の11ページ目に協議会のメンバー、それからワーキンググループをそれぞれ設置してテーマごとに取り組んでおりますけれども、より多くの方々にご参加いただきながら取り組ませていただいたということで、12ページ目にワーキグのメンバーなども掲載させていただいております。

13ページ目以降、実行計画の中身に入らせていただきます。実行計画における対策の３本柱ということで、今回３つのテーマに基づいて実行計画をとりまとめております。

１点目がカード情報の漏えい対策ということで、右側に書いてありますけれども、カード情報をそもそも盗らせない。カード情報の流出をいかに防ぐかというのがテーマでございます。２つ目が偽造カードによる不正使用対策ということで、こちらは偽造カードを作り難くする。その上で使わせないことを目指していくということでございます。３番目のＥＣにおける不正使用対策というのは、ネットでのなりすましを防止して不正使用させないというのを目的として取り組んでいくことになります。

14ページ目で、１つ目のテーマであるカード情報の漏えい防止について記述させていただいております。先ほど来出ておりますように、ＥＣにおける加盟店から情報漏えいが非常に多発しているということ。それから、攻撃の手口がグローバル化、巧妙化しているという点。それから、残念ながら一部の加盟店に当事者意識が必ずしも醸成されていないという３つを現状課題と捉えて、目標というところで対策を書かせていただいております。

対策としては、１つは、加盟店さんにおきましては、原則カード情報をおもちいただかない非保持化というものを目指していこうと考えております。カード情報をそもそも保有していなければ漏えいも起きませんし、アタックを受けることもないという意味から、できる限りカード情報をもたないでいただけないだろうかということで、カード情報の非保持化を１つ目に置いております。

２つ目が、カード情報を取り扱う事業者と書いております。主にカード会社、あるいはＰＳＰはカードでビジネスを行っておりますので、カード情報を取り扱わざるを得ない人たちについては、セキュリティに関する国際基準、安全対策基準でありますPCI DSSに準拠していただこうと。一部加盟店についても、どうしてもカード情報を保有せざるを得ないという加盟店の方については、同様にPCI DSSに準拠していただこうと考えているところでございます。

下のほうに各主体の役割というのがございます。今回の実行計画は、それぞれの事業の主体者がセキュリティ対策に取り組むことによって、全体としてセキュリティを醸成しようということを考えておりますので、それぞれ主体の役割を実行計画の中に盛り込んでおります。

１つ目のカード会社・ＰＳＰについては、先ほど申しましたPCI DSSの準拠なのですが、これを2018年３月までにという期限を切らせていただいております。

それから、隣の加盟店でございます。先ほど申しました非保持化、またはどうしてももたなければいけなければPCI DSS準拠になりますけれども、こちらについてはＥＣ加盟店、ネットの加盟店については2018年３月まで。既に血が流れておりますので早急な対応を求めるということで、こちらのようになっております。対面加盟店については、対応についてコスト、労力が非常にかかることもあって、2020年３月までという期間に設定させていただいているところでございます。

それから、行政でございます。我々、業界団体、行政を含めてのエリアになるのですが、１つ目のところは、カード情報の適切な管理義務を拡大するという方向でＰＳＰさん、あ

るいは加盟店さん等についてもカード情報の適切な管理を割販法等で義務づけてはどうかという話でございます。

続きまして、15ページ目はPCI DSSの内容を少し書いてあるところでございますので、割愛させていただきます。

次、16ページで２つ目のテーマでございます。偽造カードによる不正使用防止というところになります。先ほどご説明があったとおり、海外におけるＩＣカード化が進む中で日本がセキュリティホール化することを防ぐためにどうするかということで、ＩＣカード化にいかに取り組むかということなのですが、目標のところにございますように2020年までにカード発行のＩＣ化と、それを受け入れる加盟店さんの決済端末の双方のＩＣ化対応100％を目指す、あるいはそれに向けて取り組んでいくということにさせていただいております。

下のほうに主体の役割がございます。カード会社さんについては、クレジットカードのＩＣ化100％を2020年３月までに向けて取り組んでいくことになっております。

それから、真ん中の加盟店さんについては、ＰＯＳ等の決済システムのＩＣ化完了を2020年３月までに目指す。

下のほうに国際ブランドさんとＰＯＳ機器メーカーさんが出ておりますけれども、これにつきましては、例えば国際ブランドさんの場合については、認証プロセスの効率化となっております。これはＩＣを適切に管理するという観点から、ブランドさんの認証を受けねばならないところがあるのですが、これに関しては時間とコストがどうしてもかかりますので、こういったものを少しでも効率化することによって、コストの低減化、あるいは労力の低減化が図れないかという取り組みでございます。

また、ＰＯＳ機器メーカーさんについては、ＰＯＳシステムのＩＣ化対応を、例えば接続の部分についても標準化するということが行われれば、その分コストも下げられるだろうということで書かせていただいているところでございます。

それから、右側の行政でございます。先行的に取り組む加盟店のみえる化というのは、ＩＣカード化を達成したところについては、例えばＩＣ対応加盟店というようなステッカーをお店に張るとか、取り組んでいただいた方についてのみえる化を考えてはどうかということ。

それから、ＩＣ未対応の加盟店さんについて、そこでもし不正使用が起きた場合の損害賠償ルールをどのように考えるかということについての明確化にも取り組んではどうか。

あるいは、必要に応じて実効性確保の観点から、割販法におけるさらなる措置も検討してはどうか。さらに、中小加盟店さんについては、何らかの支援策がとれないかどうかということでございます。

続きまして、17ページ目は、ＩＣ端末等についての記述でございますので、後ほどご確認いただければと思います。

18ページが３つ目のテーマでございます。ネットのなりすまし等による不正使用の防止でございます。これも先ほども説明あったとおり、ＥＣにおける不正使用の多発でカード番号、有効期限のみで決済が行われているＥＣのお店がまだたくさん存在するということに対して、１つは、2020年に向けてＥＣにおける不正使用被害の最小化を目指しつつ、具体的には2018年３月までにＥＣ加盟店において多面的・重層的な不正使用対策を導入していきたいと考えているところでございます。

多面的・重層的な不正使用対策ということで、その下に４つほど例示しております。本人認証、セキュリティコード、属性・行動分析、配送先情報、こういったもろもろのものを組み合わせながらいかに防ぐかということについては、それぞれの加盟店の特性に応じた組み合わせを考えていくことになります。

各主体の役割ですけれども、先ほど申しましたように、加盟店さんについては2018年３月までにこういった不正使用対策を多面的・重層的に行っていただく。

それから、カード会社、ＰＳＰは、例えば３Ｄセキュアについてパスワードの登録がそもそもされていないと使えませんので、こういったものの促進。

行政につきましては、外部専門機関との連携で情報を発信し、どういうセキュリティがとれるのかということを常にご理解いただけるような情報発信をしていくということでございます。

最後になりますけれども、一番後ろ19ページ目でございます。今後の活動方針と体制について。協議会につきましては、具体的な検討、推進を行っていくわけですけれども、今回、報告書をとりまとめたことでこの協議会の活動が終わるわけではございませんで、継続的に検討を進める事項はございますし、さらに推進していく過程の中で何らかの問題が生じれば、それも議論していくということで、協議会は引き続き議論を継続することになっております。

また、上の四角の一番最後のところですけれども、当協会でセキュリティ対策に係る専門部署を設置して進捗管理等を行いながらやっていくことになります。この４月１日から

セキュリティ対策推進センターという専門の部署を当協会の事務局内に設置させていただいて、専門の人員を配置し、取り組んでいくという体制をとらせていただいているところでございます。

少々長くなりましたけれども、以上でございます。

○山本委員長　　どうもありがとうございました。

続きまして、重要インフラとしてのサイバーセキュリティ対策につきまして、内閣サイバーセキュリティセンターの三角参事官からご説明をお願いいたします。

○三角　　内閣サイバーセキュリティセンターの三角と申します。よろしくお願いします。資料４に基づきまして、クレジット関係のサイバーセキュリティが政府全体の政策の中でどう位置づけられているかということを簡単にご紹介させていただきます。

１枚目、これは歴史でありまして、2000年ぐらいから政府全体となってセキュリティ対策をやってきております。政府自身の対策とともに重要インフラとして、当時、電力とかそういうものからスタートしているのですけれども、その辺の対策を進めてきているところです。

体制は２ページ目でございます。現在、内閣の中に特別組織という位置づけでサイバーセキュリティ戦略本部、これは官房長官が本部長をしていまして、そこでいろいろな施策をやっています。左のほうにクレジットとありますけれども、重要インフラ所管省庁、各所管省庁を通じまして対策を進めていくという形をとっております。

次のページです。先ほどからデータなどお示しされていますように、サイバーセキュリティの問題は、攻撃の問題とか去年の年金機構の事件もございましたけれども、世の中でどんどん警戒が高まっているところでありまして、問題が深刻化しているという状況でございます。

このような問題を国としてどう進めているかというのが４ページ目でございます。一昨年11月にサイバーセキュリティ基本法が成立しまして、その中で関係者、例えば国や地方公共団体、重要インフラ事業者はどういう責務があって、国はどういった政策を進めるべきかといった内容が書かれています。ここにありますように重要社会基盤事業者、これが重要な事業者なのですけれども、クレジットというのは、この内数として位置づけているわけでございます。

５ページ目でございます。重要社会基盤事業者、私ども普通には重要インフラといっていますけれども、そこは国民生活及び経済活動の基盤であって、機能が停止し、または低

下した場合に国民生活、経済活動に多大な影響を及ぼすおそれがあるもの。その中で重要社会基盤事業者の責務としましては、サービスを安定的かつ適切に提供するため、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国などが実施するサイバーセキュリティに関する施策に協力するように努めるものとする。

一方で国は逆さまで、必要な取り組み、サイバーセキュリティを行わなければいけないということで、これが下にありますように14条、国は、重要社会基盤事業者におけるサイバーセキュリティに関し、基準の策定、演習、訓練、情報の共有、その他自主的な取り組みの促進、その他必要な施策を講ずるものとするということになっております。重要インフラ事業者は、サイバーセキュリティ戦略本部の中で決めているのですけれども、クレジットというのは2014年からその対象として入ってきているところでございます。

それから、次の６ページ、サイバーセキュリティ戦略です。これは国の施策をきちんと計画的に中期的なタームを見据えて、セキュリティ対策を進めていくということになっています。これは法律に基づきまして閣議決定することになっておりまして、昨年９月４日、閣議決定したものが現在のサイバーセキュリティ戦略でございます。

その中で柱が幾つか立っているのですけれども、真ん中の緑色のところ、国民が安全で安心して暮らせる社会の実現。この中に重要インフラ事業者の取り組みがありまして、防護対象範囲の継続的見直しとか情報共有の活性化とかいろいろあるのですけれども、ポイントは、機能保証という考え方を出しているのです。これはアメリカの軍隊ですと任務保証、安全保証にかわって任務保証と書いているのですけれども、民間の場合は機能保証と呼んでいて、まさに本来、全うしなければいけない責任というかサービスをしっかりとやっていくために、その目的のためにサイバーセキュリティを考える。

しばしばサイバーセキュリティが主役のような、やらなければいけないという形でいきなり来るわけですけれども、それは意味が逆転していまして、本来は、国であり事業者がみずからやらなければいけないというのが法律上、ビジネス上、責務とか目的がありまして、そこを達成するためにやらないといけないことになっているわけです。そういった考え方でセキュリティについても事業者について考えていくという考え方になっております。

そこの関連部分をスライド７、８に書き抜いていますけれども、国民の個人情報や財産を初め実生活に影響を及ぼす事例が頻繁に発生している。重要インフラ、政府の機能、サービスは、それ自体が国民生活、経済社会を支える基盤となっており、支障が生じると国民の安全・安心に直接的かつ重大な影響が生じる可能性がある。したがって、業務の責任

者――これは任務責任者ともいいますけれども――とシステム責任者が業務を実施するに当たって、例えばＩＴを使っていたりいろいろな設備を使っていると思います。そういったシステム責任者とともに機能やサービスを全うするという観点からリスクを分析する。あくまでも大事なことは、業務の責任者が中心となって考えないといけないということ。協議をして、残存リスクの情報も添えて経営層に対して提供して、そして総合的な判断をする。

リスク分析ですから、リスクの低減をするという策をとることもありますし、リスクを移転する、保険とかに移すという話もありますし、そもそも策をとらないというか新しいことをやらないという話、それから受容するということで、そこはリスクと認識した上でほかのことでカバーしていくとか、いろいろな方法がある。そういうことを考えていくということでございます。

その上で８ページ。重要インフラを守るための取り組みとして、官民が一丸となって重点的に防護していくことが必要である。業法によってサービスの維持及び安全確保に係る水準が求められているものについては､安全基準について不断の見直しを行っていくこと。そして、私ども内閣サイバーセキュリティセンターと所管省庁がより緊密に連携して積極的な情報収集などに取り組んでいくということを書いています。まさに業法によって求められているサービスを達成するために必要なセキュリティを考えていくという考え方を出しているわけでございます。

このほか、重要インフラそのものについては、具体的な政策としてどのようにやるかということについて中期的な行動計画をつくっています。この中で分野の設定をしていて、クレジットについて2014年、先ほど申しましたように対象となったわけでございますが、安全基準の整備とその浸透、それから攻撃情報とか脆弱性情報や中央情報、そういった情報共有体制の強化、そして障害対応体制の強化ということで業界横断的な演習を行っていく。

それから、この行動計画につきましては、来年度で現在の期間が終わりますので、その先を見据えて、さらにロードマップを先日、３月31日にサイバーセキュリティ戦略本部で決定したところでございます。真ん中にありますように、機能保証の考え方に立脚して、みずからの経営責任を全うする観点から、セキュリティの経営資源投入を推進していく。それから、情報共有の活性化をしていく。法令に基づく義務的な報告、または補完的な報告の着実な実施、安全基準や報告事項の基準等の見直し、それから監査とか、こういった

ことによって着実に進めていくべきとなっています。

以上のようなことを政策の中にはいろいろと位置づけているのですけれども、これがクレジット分野においてどのようになるかということを申しますと11ページであります。まず大事なことは、管理すべきサービスの明確化ではないか。要するに、業務を全うするためにセキュリティがあるわけですけれども、どこまでを対象とするかということを、今の業務を達成するに当たって、今の範囲で十分かどうかと常に不断の見直しが必要になっていくだろうということ。

それから、防護目的・対象の明確化。防護の目的の明確化、何から何をどのように守るのかということをはっきりさせなければいけない。それから、守り切れない場合は、どのようにプライオリティづけしていくのかということです。

それから、要求事項の明確化。業務に関連する法令、規制等の要求事項は何なのか。それから、法令には明示されていないけれども、業務に不可欠な要求事項は何なのか。そして業務のルール、PCI DSSとかいろいろあると思いますけれども、そういったものや組織が必要と判断するものは何なのか。こういった要求事項を明確化していく。

そして、何よりも大事なのが、これらはリソースの投入が伴いますし、組織としてトップのコミットメントが重要になっていく。どのような方針で取り組んでいくのか。組織ごと、業界全体としてどのように取り組んでいくのかということが重要になっていくわけでございます。

法律でもありますけれども、いろいろな情報管理ということだと思うのですが、重要インフラにつきましては、先ほど申しましたサービスの提供の継続が重要ですので、現行の行動計画の中でもＩＴの機能不全等によりオーソリゼーションの遅延、停止、不正使用等を行わないこととか、そういった幾つかの維持すべき目的を定められて、そこを着実にしていく。こういったことは今後またこういった場でご議論されていって、どこまでどのように守っていくのかということを決めて、それをまた私どものほうで全体として反映していくという形かと思っております。

あと、12ページと13ページは、いろいろな言葉が飛び交っていますので、ちょっと簡単に参考資料としてつけただけでございます。今は時間の関係でご説明いたしませんけれども、そういった形でセキュリティを進めていくのかなと思っております。

以上でございます。

○山本委員長　　どうもありがとうございました。

続きまして、クレジット分野におけるサイバー攻撃の現状につきまして、Payment Card Forensicsの大河内フォレンジック・シニアコンサルタントからご説明をお願いいたします。

○大河内　　Payment Card Forensics・大河内と申します。よろしくお願いいたします。

今までの流れの中で、我々はクレジットカード業界における漏えいがあった際にフォレンジック調査を行う会社の１社でございまして、2011年から活動しております。その中の統計も踏まえて、いろいろお話しさせていただければと思っております。よろしくお願いいたします。アジェンダとしては、簡単に弊社のご説明と制度のご説明をさせていただいて、本題に入らせていただければと思っております。

３ページ目に弊社の会社案内が入っておりまして、我々、PCI SSCという、これはクレジットカード業界団体から認定フォレンジック機関、ＰＦＩ（PCI Forensic Investigator）という資格をいただいた上で調査をやっております。

では、この資格は何ですかといわれますと、５ページ目に概要説明が書いてあります。全てのカード会社がブランド各社の要請により加盟店（対面・非対面を含む）及びサービスプロバイダなどでクレジットカード情報の漏えいが起こった際に、フォレンジック調査というものを義務づけております。この制度は国際ブランド主体で行われておりましたが、2011年３月からPCI SSCに移管されました。その為、この制度の施行により、フォレンジック調査後には調査報告書を５大ブランド（VISA、Master、JCB、American Express、Discover)に対して共通に提出することができます。また、フォレンジック調査会社というのは、インシデントの原因追求とか解決を行うこと、または法的に証跡に対する責任をもつ企業を指しております。

今回の本題、６ページ目になります。非対面取引における犯罪サイクルを議題にさせていただこうと思っております。

７ページ目、初めにというところで、今までのいろいろお話があった中で、我々としても実際同じことを思っていると。その中で非対面取引では、2011年から不正犯罪が毎年平均20件ぐらいあったのではないかと思うのですけれども、去年から大分多くなっている。日本自体がセキュリティホール化しているのではないかということを懸念しております。

もう１つが、2020年のオリンピックに向けて、インバウンドの取り組みやFinTechなどを背景にビジネスは加速しているのですけれども、一方でクレジットカードセキュリティの対策が後回しになっていると捉えられるところもありまして、今後も増加するのではないかと懸念しております。

また、不正犯罪自体が組織化されているのではないかと考えておりまして、犯罪サイクルがあるということを考えております。

次のページ、実際に我々が調査をして、2011年からどのぐらいの件数が今起こっているのかというのを表にしております。2011年が件、2012年が件、2013年が件、2014年が件、我々のほうで調査をやらせていただいている件数のですけれども、2015年に関しては件やらせていただいております。ことしに関しては、先ほど新聞記事もありましたけれども、それも踏まえて、現在調査中も含めて件あります。本日も２、３社フォレンジック調査に入ってほしいという話が出ているので、今後も増加してくるのではないかと考えております。

実際、現時点のものと昨年１年間のカード番号の漏えい件数を、重複を除かないでざっと全部の件数を調べたところ、昨年で万件以上漏えいしていた。ことしに関しては、１月から３月の時点で万件の漏えいが我々の調査でわかっております。なので、今後もこれがふえ続けていくと、やはり今までの戦略のお話もうまく行かないのではないかというところもありまして、いろいろお話をさせていただいております。

10ページ目になります。実際、犯罪サイクルというものがあると我々は考えております。まず、不正アクセスが行われて、各加盟店に対してどこが弱いのかというのを情報収集する部隊がいるのではないかと考えております。その情報収集したものを実際のハッカーに売るという行為を行って、実際にハッカーが、例えばＳＱＬインジェクション機種などの既知の脆弱性を利用してカード番号をとってくる。その取ってきたカード番号に関して、「なりすまし」をする部隊との売買行為が行われて、実際に買い物を行って、その後にそれを売り子というか商品をいただくような人たち、今、警察で捕まっているのがありますけれども、そういった者たちが不正配送先で捕まえられていて、その一連の流れの中で最後に我々のような調査会社がフォレンジック調査に入る。調査会社が調査に入ることによって、クレジットカードの取引を加盟店が一時とめるわけですから、そうすると犯罪組織も加盟店のほうで調査に入っているというのがわかり、次の加盟店を狙いに行くのではないかと我々は考えております。

それを言葉にしたのが次のページに書いてある犯罪サイクルについてです。非対面取引での不正犯罪では、インターネット加盟店に対する不正アクセスは無差別に起こっているということがなかなか加盟店さんに伝わっていないのが現状です。その次に、クレジットカード番号の盗用（漏えい）が発生します。次に、盗用情報を利用するなりすましによっ

て不正購入が行われます。その不正購入した商品が犯罪組織だったり貧困の国の方に渡ってお金にかえられたり、もしくは反社会勢力の活動資金源になっているのではないかとも考えられます。

実際、クレジットカード番号の盗用（漏えい）については12ページ目からお話しさせていただきます。

ここに我々がやったフォレンジック調査の統計があるのですけれども、ＡがＳＱＬインジェクションを起点にされて漏えいしている。基本的にＳＱＬインジェクションが起因だったり、バックドアプログラムの設置が非常に多いのではないかと思います。その辺のところを14ページ目に記載させていただいております。

１ついえるのは、漏えいするＥＣサイトやサービスプロバイダ（加盟店と決済代行会社の間にいるサービスを行う企業）でも漏えいがあるのですけれども、そのどちらに関しても攻撃手法は同じだと我々は考えております。漏えい事案の中で一番多いのはＳＱＬインジェクションです。これは過去年からずっといわれているものなのですけれども、なかなか対策が進められていないのではないかと思っております。

もう１つがバックドアプログラム。足跡がつかないようにバックドアプログラムというものをアップロードされて、バックドアプログラム経由でカード会員データを不正取得するという事例がここ数ヶ月間で非常に目立っておりますので、バックドアプログラムというのも非常に危険が高いのではないかと思います。

最後は既知の脆弱性を利用した攻撃手法です。実は我々が調査する際に加盟店でログを残していない企業が多いので、非常に解明するのが難しい事もあり、既知の脆弱性を利用されているケースもあったりします。

最後のページ、今まではＥＣ加盟店が狙われている事案が非常に多かったのですが、2014年あたりからサービスプロバイダといわれているＥＣ加盟店の情報を決済代行会社のかわりに預かって決済代行会社に伝送したり、もしくはカード会社に伝送するようなサービスをしている会社からの漏えいが非常にふえていると我々は感じております。その中には、例えばホスティング事業者も考えられますし、そういったところも非常に多いのではないかと思っています。その為、サービスプロバイダに対しても注意喚起が必要なのではないかと思っております。

実際、今、実行計画の中にあるペイメントサービスプロバイダ以外にもPCI DSSの規格を利用してセキュリティ強度を高くしないといけないリスクのある企業さんはたくさんいる

のではないかと考えております。

最後に総括ということで、今までセキュリティにはいろいろな規格があるのですけれども､PCI DSS以上にセキュリティ事故をもとにしてつくっている規格が世の中になかなかないのではないかと考えております。きちんとした形でPCI DSSを用いれば、多面的・重層的に対策ができるものだと考えております。

早足でいろいろ解説させていただきましたけれども、以上になります。

○山本委員長　　どうもありがとうございました。

それでは、資料の説明としては最後になりますけれども、ＩＣ化に関する諸外国調査結果につきまして、日本クレジットカード協会の星野事務局長からご説明をお願いいたします。

○星野　　日本クレジットカード協会の星野でございます。

当協会は、昭和59年に発足いたしました銀行系のカード会社の団体でございまして、今現在、会員会社数117社でございます。昨年３月に、先ほど日本クレジット協会の與口様からご説明いただきましたクレジット取引セキュリティ対策協議会が発足したこと、また事務局の坂本課長からご説明があったとおり、諸外国におけるＩＣ化が急速に進展しているといった動行を踏まえまして、当協会では昨年度、ＩＣ化に関する諸外国調査を実施いたしました。本日はその調査結果についてご報告させていただきたいと思っております。

ただ、時間も限られておりますので、本日は調査結果の中でも特に重要なポイントとなります資料６の目次に２点お示ししております日本への偽造カード不正被害の流入リスクと諸外国の決済端末ＩＣ化の推進要因についてご説明させていただきたいと思います。

それでは、ページをおめくりいただきまして２ページ、初めにをごらんいただけますでしょうか。こちらでは調査の目的と調査対象国、そして調査方法についてお示ししております。調査目的につきましては左にお示ししていますが、公知情報にとどまらない実態情報の収集を幅広く行うということで、ＩＣ化の遅延に伴う偽造カード被害の流入リスクをみきわめること。２点目として、日本の商慣習・インフラ環境を踏まえたＩＣ化の推進方法の考察を行いまして、実現方法の検討につなげることを目的としておりました。

調査対象国は左下にお示しのＩＣ化が既に完了している主要６ヵ国に、今現在ＩＣ化を推進しておりますアメリカと韓国を加えました計８ヵ国としております。

また、右側に調査方法につきましてお示ししておりますが、公知情報等の情報収集に加えまして、今回は諸外国の専門家等へのヒアリング並びに米国への現地視察を実施してお

ります。

それでは、ページをおめくりいただけますでしょうか。３ページ目となります。まず、日本への偽造カード不正被害の流入リスクでございます。こちらは今回の調査結果の過程で立てた仮説をお示ししております。まず、クレジットカード先進国の中で残されたＩＣ化後進国でありますアメリカや韓国のＩＣ化の進展に伴いまして、そのリスクの高まりは否定できないとの仮説でございますけれども、こちらの仮説の根拠をその下に３点お示ししております。

まず、左側の棒グラフでございますけれども、先ほど坂本課長に丁寧にご説明いただきましたので簡単にご紹介させていただきます。海外で不正使用されたイギリス発行のカード、またはカード情報でございまして、国別にその数値をお示ししております。ヨーロッパ諸国のＩＣ化の進展に伴いまして、国別の順位が大きく変動していることがおわかりいただけると思います。

矢印でお示ししておりますが、特にＩＣ化未対応国のアメリカにおきましては、偽造カード被害が急増しておりまして、その下にアメリカの偽造カード被害額をお示ししております。直近４年間で倍増しておりまして、昨年、2015年36億ドルという被害額につきましては、全世界の５割近い数字でございまして、現状アメリカが世界最大の偽造カード被害大国となっている状況でございます。こちらは教訓ということで先ほどお話しございましたとおり、もともと最初からアメリカが被害大国であったわけでなく、他国からのリスクが流入して今に至っているということがおわかりいただけると思います。

その右に、アメリカと韓国のＩＣ化推進状況をお示ししております。両国ともに大規模な情報漏えい事案の発生が起因となりまして、現在、国家レベルでＩＣ化を推進しております。アメリカでは決済環境のセキュリティ強化を推進しております団体が2015年、昨年の目標となりますけれども、定量数値、定量目標を掲げて推進しておりました。中でもChip-on-Chipの取引シェアの目標につきましては29％と設定されておりますが、その前年、2014年の実績がわずか0.12％でございましたので、かなりのスピードでＩＣ化対応を進めていることがおわかりいただけると思います。

また、韓国におきましても、昨年７月以降、法制化によりまして加盟店に新規に設置される端末についてはＩＣ化が義務づけられるなど、ＩＣ化の推進が本格化している状況でございます。

それに加えまして、画面の右側にお示しの日本の偽造カード不正被害のトレンドにおき

ましても、偽造カードの被害額につきましては加盟店の視点でみますと近年増加しておりまして、これは海外イシュアーの偽造カードによる不正被害が国内で増加傾向にあるということでございます。

このような背景を踏まえますと、日本への偽造カード不正被害の流入リスクの評価につきましては、アメリカのＩＣ化動向が大きな鍵を握ると考えまして、昨年10月にアメリカへの現地視察を実施し、実態把握に努めてまいりました。

その結果につきましては、次のページ以降でご説明させていただきたいと思います。４ページをごらんいただけますでしょうか。お示ししております米国のＩＣ化推進タイムラインでございますけれども、アメリカの業界横断組織の議長と意見交換した際に説明を受けた資料でございます。アメリカでは、このロードマップに基づきましてイシュアー、アクワイアラー、加盟店等が2017年10月までにＩＣ化の完了を目指すとしております。ただし、こちらはあくまで目標でございますので、各ステークホルダーの推進の実態はどういう状況なのか、特に大型加盟店の対応状況を中心に視察した結果を次のページにとりまとめております。

５ページ目をごらんいただけますでしょうか。現地の視察結果に基づきまして、加盟店を大型、中型、小型の３つに分類いたしまして、ＩＣ化の状況を整理しております。

まず、アメリカ全土の消費額の23％を占めております大型加盟店15社の状況としましては、非対面加盟店の２社を除いた13社中12社が既にＩＣ化の対応が完了しております。12社全店舗でＩＣ化が完了しているかどうかまでは確認できておりませんけれども、おおむねＩＣ化対応にはめどがついている状況でございます。

また、ピラミッドの底辺を形成しております小型加盟店におきましても、端末を置きかえるタイミングでのＩＣ化対応が進捗しておりまして、順調に進行する見通しでございます。

中段の中型加盟店におきましては、現在、ソフトウエア提供の対応が追いついていないことから、進捗は芳しくない状況でございましたけれども、業界団体からはことし、2016年中にキャッチアップが図れる見通しであるというお話を伺いました。アメリカでは日本と違いまして、加盟店ごとにソフトウエアがカスタマーされておりませんので、供給者側でソリューションの用意ができれば、あとは時間の問題と捉えていらっしゃいました。

このように偽造カード不正被害大国であるアメリカにおきましてＩＣ化が進展している状況を踏まえますと、犯罪者が次にターゲットにするエリアのみきわめが重要になってま

いります。

次の６ページ目をごらんいただけますでしょうか。左側にお示ししています世界地図でございますけれども、こちらは近年、クレジットセキュリティの標準化団体となりつつありますＥＭＶＣｏが公表している世界における接触ＩＣの普及状況でございます。６つのエリアごとにカードと取引比率のＩＣ化率の数字をお示ししておりますが、犯罪集団のターゲットエリアのシフトの考え方もあわせて右側にお示ししております。

アメリカのＩＣ化の進展状況を踏まえますと、先ほど申し上げたとおり、ＩＣ化の未対応国に不正被害が流れてくる過去の事実から、Chip-on-Chipの取引比率がアメリカに次いで低いアジア太平洋エリアにシフトしてくる可能性が高いと考えておりまして、万一、日本の対応がおくれれば、日本に不正被害が流入してくるリスクは否定できないと当協会としては結論づけいたしまして、大変大きな危機感をもっている状況でございます。

それでは、画面をおめくりください。続きまして、２点目の報告テーマでございますけれども、諸外国の決済端末ＩＣ化の推進要因に関する調査結果でございます。

諸外国における推進要因につきましては、各国それぞれ異なりましたけれども、６つの推進要因に分類いたしまして、採用国数を表の右側にお示ししております。諸外国におきましては太枠で囲っておりますが、２番目の行政／業界の取り組み、次の３番目のライアビリティシフトがおおむね共通した推進要因となっておりました。

３番目のライアビリティシフトにつきましては、ぽつ２つ目に記載しておりますけれども、諸外国におきまして、アクワイアラーと加盟店との契約において、不正被害の費用負担を加盟店に転嫁する契約となっておりますので、加盟店は偽造カード不正被害の最終的なリスク負担者となり、みずから決済端末のＩＣ化を推進する要因となっております。

日本は、諸外国と商慣習の違い等もございますので、これら全てが同様に推進要因になるとは考えておりませんけれども、先ほど日本クレジット協会様からご説明いただいたとおり、クレジット取引セキュリティ対策協議会の実行計画を各主体者が着実に進めていくことが日本においては大変重要な要素になってくるだろうと考えております。

最後のページには、ご参考としまして、アメリカのトップリテーラー15社のＩＣ化状況をまとめておりますので、こちらは後ほどご確認いただければと思います。

駆け足となりましたが、説明は以上となります。

○山本委員長　　どうもありがとうございました。以上、５つの報告をしていただきました。ここまでが前半部分ということで、後半は討議に移らせていただきたいと思います松

本大臣官房審議官がおみえでございますので、ここで、松本審議官より一言ご挨拶を申し上げます。よろしくお願いします。

○松本大臣官房審議官　　おくれてまいりまして失礼いたしました。経済産業省の審議官をしております松本でございます。本日はお忙しい中、委員の皆様方、オブザーバーの皆様方におかれましては、ご出席いただきましてまことにありがとうございます。また、プレゼンターの方々にもご協力いただきまして、まことにありがとうございます。

2020年に向けてインバウンド事業に確実に取り組むためには、キャッシュレス化の推進と、その大前提となる安全・安心なクレジットカード利用環境を実現することは、日本再興戦略にも掲げられた重要な課題でございます。

昨年７月にとりまとめていただきました報告書におきましては、アクワイアラーやＰＳＰの割賦販売上の位置づけ、悪質加盟店排除のための加盟店調査の位置づけ、カード番号等の保護に関する措置の強化等についてご提言いただいたところでございます。これを１日も早く法改正につなげるべく準備を進めているところでございますが、クレジット取引のセキュリティ対策のニーズの高まりなど、その後の状況変化も含め、さらなる対応の必要性について改めてご審議いただくため、今般、委員会を再開させていただくことといたしました。

昨年６月の日本年金機構における個人情報漏えい事故等を受け、サイバーセキュリティ対策が政府全体として喫緊の課題となる中、重要インフラと指定されておりますクレジット分野についても、さらなるセキュリティ強化が求められております。特にカード決済端末のＩＣ対応化については、先ほどご紹介ありましたように米国でも急速に進展しておりまして、これ以上日本の対策がおくれることは、日本のセキュリティホール化につながるものであるという強い危機意識をもっているところでございます。

こうした中、本年２月にクレジット取引セキュリティ対策協議会が策定した実行計画に基づきまして、幅広い関係事業者が連携して自主的に取り組みを推進していただくことが先決ではございますが、2020年までに確実に国際水準のセキュリティ環境を実現するためには、法的な枠組みによる実効性確保といったことも必要ではないかと考えてございます。

セキュリティに関する議論に当たっては、クレジットカード取引の国際性、あとステークホルダーの対応性とネットワーク性、こういった観点にもご配慮いただきたいと考えております。

また、話は変わりますが、金融や決済の分野でのイノベーションを牽引するFinTechの健

全な発展を促す観点から、昨年の報告書でもご提言いただきましたＰＳＰに対する任意登録制の導入等に対する期待も高まってございます。

また、次回の議題となりますが、今国会に提出されております特定商取引法の改正案を踏まえた対応等についてもご議論いただいて、必要な改正事項につきまして報告書に追記する形でおまとめいただきたいと考えております。

最後に、委員の皆様、またオブザーバーの皆様におかれましては、クレジットカードの信頼性確保に向けまして活発なご議論をお願いしたいと存じます。本日を含めて３回のご議論になりますが、よろしくお願い申し上げます。

○山本委員長　　どうもありがとうございました。ただいまの審議官のご挨拶にもありましたように、前半のプレゼンテーションとしては、最初のFinTech関係のプレゼンテーションが企図されております今回の割販法改正、FinTech企業によるイノベーション、それからFinTechにおける利用者の安心･安全の確保というインプリケーションをお示しするものでありましたし、それ以降の４つのプレゼンテーションにつきましては、クレジット取引のセキュリティ対策に関して、これからご討議いただく内容をご理解いただくための背景事情について説明いただいたということになります。

そこでこれから、後半の討議に入らせていただきます。最初に、事務局から論点の提示をお願いいたします。

○坂本商取引監督課長　　ありがとうございます。資料７に沿いまして、事務局として考える論点をご紹介させていただきます。資料７に関しましては、iPadでみていただいても結構ですし、念のため紙でもご用意させていただいております。あわせまして、昨年７月におとりまとめいただきました報告書につきましても閲覧用ということで、そちらも紙で配付させていただいておりますので、適宜ご参照いただければと思います。

昨年７月の報告書におきまして、セキュリティに関しては法令等の制度整備による対応のみならず、セキュリティ協議会の検討結果を踏まえて、我が国におけるセキュリティ対策強化に向けた取り組みが進められることを強く期待するというご提言をいただいておりまして、それを受けた形で２月にまとめられたセキュリティ協議会実行計画については、先ほどクレジット協会からご紹介いただいたとおりでございます。

一方で、先ほど内閣官房セキュリティセンターからもご紹介いただいたように、政府全体としてサイバーセキュリティ対策強化の必要性が認識されているところでございまして、その中でも重要インフラの１つということで、クレジット分野でもさらなるセキュリティ

対策が求められているということでございます。先ほど日本クレジットカード協会からもございましたように、クレジット取引の国際性ということを考えますと、国際環境の動きが非常に重要になってくる中でアメリカの動きが非常に早いということで、セキュリティホール化の懸念が切実な切迫したリスクと認識されているところでございます。実際、先ほどご紹介したようにＰＯＳシステムを狙った感染件数も急増してきている。前年比約７倍ということで実際の被害も生じているような足もとの状況について受けとめて、今回改めて議論をお願いしたいということでございます。

実行計画に基づきまして、関係事業者の自主的な取り組みを基本とするということでございますが、その実効性を確保するために法律で手当てすべきものとして、大きく３つほど挙げさせていただいております。

１つ目が、先ほどサービスプロバイダという話もございましたが、加盟店も含めて加盟店等という形でくくらせていただいております。加盟店等におけるセキュリティ対策の強化ということで、まず平成20年に改正された現行の割販法におきましては、イシュアー及びアクワイアラーについてのみ番号等の情報管理が義務づけられているところでございまして、７月の報告書では、その他のカード番号を保有する加盟店等については番号等の情報管理を努力義務ということでご提言いただいております。

一方で、先ほど来、各プレゼンテーションの中でもお示しいただいているようなクレジット取引のセキュリティにかかわる最近の動きを踏まえまして、クレジットカード取引システム全体の信頼性を確保するに当たって、これらの措置で十分かどうか。また、情報保護に関するほかの法律、例えば個人情報保護法などの保護法益、あるいは保護法益から導かれる具体的な措置内容などとの関係についても改めてご確認いただければと思っております。

なお、内閣官房からもご紹介いただいたサイバーセキュリティ基本法に基づきます重要インフラの行動計画の中でも、先ほど機能保証というお話しがございましたが、クレジット分野についてはキャッシュレスの決済サービスを持続的に安全・安心に提供いただくことが大きな目標になってきます。その中で情報の機密性、情報をしっかり管理することと同じように、不正使用に対する対策。不正使用が横行すれば、機能不全といいますか、カード会社が負担するにしても、それは何らかの形でカードシステム全体の高コスト化にもつながっておりますので、そういったことも含めて効率的なカードサービスの持続的な提供という観点からも、不正使用の部分もあわせて改めてご検討いただければと思っており

ます。

まず、番号等の情報管理につきましては、先ほどのセキュリティホール化の懸念等も踏まえて努力義務にとどまらず、例えば違反に対して一定の制裁措置が規定されるという意味で法的な義務――通常の義務ということでございますが――を課すことの是非についても改めてご検討いただければと思っております。

一方で、この点につきましては、ご案内のとおりクレジットカード加盟店というのは数も非常に多く、全国でも数百万といわれておりますし、業種や規模、実態についても非常に多様であるということですので、義務について検討いただく際には、その主体、義務の対象範囲、義務違反に対する措置ということにつきましては、加盟店側の実行可能性という意味でも、負担などの観点でも過度な対応にならないようなご配慮もぜひお願いしたいと思います。

一方で、番号等の情報管理につきましては、個人情報保護法について昨年秋、改正個人情報保護法が制定されておりまして、念のためでございますが、こちらの改正によって、これまであった5,000人以上という裾切りが外れておりまして、個人情報を取り扱う全ての事業者について法的な義務づけということで、個人情報保護法においては、指導助言、あるいは勧告命令、この勧告命令に違反した場合には罰則という形で法的な拘束力のある措置が入れられているところでございます。

なお、個人情報保護法にカード番号単体で適用があるかどうかというところについては、今まだ調整中、未定でございますので、そこはそういう前提でご議論いただければと思いますが、個人情報保護法の動きもみながら、カード番号についての手当てが必要になってきているかと思います。

あわせて３ページでございます。不正使用対策ということにつきましては、前回７月の報告書では義務づけ等は見送り、まずは協議会での公的な取り組みを推進する。他方で、対応できない事項が生じた場合には、必要に応じて制度的な措置の要否について検討するという形でまとめていただいております。

この不正使用に関しては、もともと情報漏えいに起因するということでございますので、情報漏えいがきっちり防止されれば、不正使用そのものの根本原因も抑止されるということでございますが、先ほどフォレンジック機関からもご紹介いただいたように、現実には完全な情報漏えいの防止はなかなか難しい。むしろ情報漏えいという意味では増加が見込まれるということ。あるいは日本国内で一生懸命情報漏えい対策をしても海外で漏えいし

て、それが日本で不正使用されることも十分あり得るということですので、クレジット取引の機能不全を防止するという意味、取引全体のシステムの信頼性を確保するという意味で、不正使用対策の必要性についてもご検討が必要ではないかということでございます。ただし、この点についても、先ほどのようなステークホルダーの多様性というところもご配慮いただく必要があるだろうと思っております。

(2)といたしましては、カード会社、アクワイアラーと今回任意という形ですけれどもＰＳＰについて登録をご提言いただいております。去年のご議論の中では、悪質加盟店の排除ということが主眼で加盟店調査義務の導入をご提言いただいておりますけれども、悪質加盟店の排除と同様に、カード取引システムの信頼性を確保するという観点から、加盟店でのセキュリティ体制の確保に関しましても、あわせて加盟店調査の中で行っていただくということについて、その要否についてご検討いただければと思っております。

最後、３点目(3)でございます。現行の割販法の中で認定割賦販売協会ということで、日本クレジット協会が認定を受けて、いわゆる自主規制機関ということで法律上も位置づけられております。法令の遵守ですとか法令に基づく処分の遵守、あるいは苦情処理体制の整備といったことが認定割賦販売協会の法定業務となっております。

日本クレジット協会に関しましては、これまでもセキュリティ協議会の事務局ということで議論を牽引していただきましたし、今後、実行段階でも、先ほどご紹介あったような専門部署を立ち上げて、いよいよ関係事業者に働きかけを行うなど、実行体制の軸ということでやっていただいておりますけれども、法律上もセキュリティ対策推進を認定割賦販売協会の業務としてしっかり位置づけることで、安定的な体制を組んでいただくことが必要ではないかという観点を３つお示しさせていただいておりますので、どうぞよろしくお願いいたします。

○山本委員長　　どうもありがとうございました。

それでは、委員の皆様からご発言をいただきたいと思います。ご質問、ご意見がおありの方は、挙手をお願いいたします。では、池本委員、どうぞ。

○池本委員　　池本でございます。ご説明ありがとうございます。技術的な部分と業界の実態部分でよくわからないところがあるので、何点か質問させていただきます。

資料３の５ページで、2015年の不正使用額が120億円、これをカード会社が負担している状態になっているという説明で、金額に非常に驚いたところですが、その金額を件数に置き直すとどのぐらいの数なのか。後のほうでフォレンジック社の方から2015年15万件とい

う、これがその数字なのか、これはあくまで一部なのか。そこがわからなかったことと、その関係で、カード会社が不正使用額を負担するというご説明があったのですが、カード保険で負担になっているのではないかとこれまで理解していたので、そこの確認をお願いします。これがまず第１点です。

それから、同じ資料３の14ページ、加盟店のカード情報の非保持化、またはPCI DSS準拠というご説明をいただいた中で、できるだけ非保持化、要するにもたない形で対応し、保有せざるを得ない場合にはPCI DSS準拠をお願いするというご説明がありました。どうしてももたなければいけない場合というのは、例えば毎月自動決済しなければいけないとか、どういう場面がそうなのか。要するに、あるべき体制になっていたときに非保持化、もたないでやっていけるのが何割ぐらいで、どうしてももつのがどのぐらい残るというのは、何か加盟店の実態との関係でイメージがつくれるものなのかどうか。これはむしろカード協会の方にお伺いしないといけないのだろうと思います。

それから、同じ資料の16ページ、ＩＣ対応加盟店。全体のご説明の中でＩＣ対応がまだ17％しかないというのは本当に驚きで、カードがＩＣ化されているから安心だと思ったらとんでもない話だというのがきょうのお話でわかりました。それを働きかけていくいわゆるアクワイアラー、これまでイシュアー、アクワイアラー全体を含めたカード会社が国内で何社というイメージで議論してきたのですが、加盟店に働きかけをしていただくアクワイアラーというのは、実態としてどのぐらいの数いらっしゃって、どのように動かれているのか、アクワイアラーの事業者数がおわかりかどうかというところです。

なぜそれをお伺いするかというと、ＰＯＳシステムでＩＣ化がなかなか進まないところを加盟店に対して働きかけをしていかなければいけないと思うのですが、その働きかけの主体がどのくらいなのかというところについてお伺いしたいからです。

とりあえず以上、お願いします。

○山本委員長　　池本委員から３点ご質問が出されたと思います。これについては、まず事務局からお答えいただいて、さらに業務の実態に詳しい方からご説明いただくのが適切な場合には、また別途お願いしたいと思います。まず、事務局から。

○坂本商取引監督課長　　ありがとうございます。資料３の５ページの不正使用の金額についてご質問いただきました。済みません、後ほど與口理事から補足していただければと思いますが、件数では把握されていないと認識しております。あくまでもカード会社が把握して負担をした。この負担の中には、おっしゃるように保険でカバーされているものも

あれば、いわゆる自家保険というかカード会社がみずから負担している部分もあるということです。先ほど、フォレンジックの大河内様からご紹介のあった15万件というのは、あくまでも漏えいされたカード情報の数ですので、情報漏えいに起因はするものの、それが結果不正使用に積み上がっていった金額という関係でございます。

あと、アクワイアラーについては何社ぐらいあるかということでございますが、今はイシュアーの登録制しかございませんので、イシュアーとして登録されているのが約260。そのうち200程度がアクワイアリングも行っている。外側のアクワイアラー専業者という意味では、今のところ我々が把握しているのは10社程度かなと。ただ、海外のアクワイアラーで国内の加盟店を相手にするところも昨年の報告書の中では登録制の範囲に入っているかと思います。そこはまだ十分補足し切れていない部分があるかと思っています。

○山本委員長　　では、まだお答えいただいていない部分と、今事務局からお答えいただいたことについてもご補足等ありましたら、與口専門委員からお願いいたします。

○與口専門委員　　少なくともカード犯罪の件と最後のアクワイアラーの件は、そのとおりですということです。

もう１つの、いわゆるPCI DSS準拠の話でございますけれども、加盟店さんでカード情報の非保持化ができない、要はカード情報をもたざるを得ない加盟店さんということなのですが、ある種、概念上といったら大変失礼な言い方なのですけれども、大手の加盟店さんでＰＯＳを使っていらっしゃる方が、今カード情報をカード決済だけではなくて、後々、赤伝処理をしたり入金確認をしたり、いろいろなところでカード情報を使っていらっしゃる加盟店さんもいたりする。あるいは販促などに使うケースもあるようでございますので、そういうところでカード情報を有効に活用していて、単純に決済だけなのでそれを離すわけにはいかないところが発言としてあるというだけでして、どのくらいあるかとか、どのくらいの方々が非保持化に切りかえていただけるかというところも実はわかっておりません。

ただ、どうしてもそういうことで使わざるを得ないというのであれば、基本的にはPCI DSSによって守ってもらわなければいけないのだという意味でご説明申し上げましたので、もしかしたら、みんながみんな非保持に切りかえていただけるかもしれないということですので、具体的にどれぐらいの方々が切りかえられないといっているということではないので、あくまでもそういうことも想定して考えているとご理解いただければと思います。

○山本委員長　　どうもありがとうございました。それでは、さらにご発言を伺いたいと

思います。きょうは、先ほど事務局が説明しました資料７がワーキングペーパーでありまして、そこで挙げられております論点が(1)、(2)、(3)とございます。そして、(1)にあります割販法の保護法益の確認、他法との保護法益との関係、これは個人情報保護法との関係の整理ということでありまして、全体にかかわる問題かと思います。昨年７月の報告書から仕切り直しをしている部分も若干あります。きょうはそのあたりを十分にご議論、ご討議いただきたいと思っております。

まず、全体に関わる保護法益の関係性につきまして、藤原委員からご発言いただけますでしょうか。よろしくお願いします。

○藤原委員　　藤原です。

今、山本委員長おっしゃったように、昨年の報告書の20ページから21ページあたりで、カード番号単体が個人識別符号に当たる場合と当たらない場合とを場合分けして議論しているわけです。２つありまして、１つは、まず識別符号は、先ほど坂本課長からご説明のありましたように、まだいろいろな状況で固まり切っていないことですので、その話はひとまず置いておいていいと思うのです。基本のところは、この会合できょう議論するのは、20年改正で当初、実現を意図していたところの法益ですよね。つまり実体的な規律の内容を今度新しくなった改正個人情報保護法に全て委ねて実現できるのかどうかというところの精査であろうかと思うのです。

つまり、一般法と個別法の関係は多分出てくると思いますので、一般法としての個人情報保護法、そして現時点でこの状況におけるキャッシュレス社会の中で割販法がどういう役割を果たさなければいけないか。それを背景にして、まずは割販法でできることをしっかり考えて、何ができて、何ができないのかを詰めて整理してみるのがいいと思うのです。ですから、この方向は私も賛成で、個人情報保護法に委ねて全てが実現できるかどうかというのは、識別符号の問題にかかわらず、いま一度精査しておいていただきたいというのが１つのお願いであり、総論です。

それから、２つ目ですけれども、先ほど中小企業などの話も出てきたのですけれども、確かに5,000人という壁はなくなったのですが、実は、我が国の法制はＥＵ対応にするということでやってきたのですけれども、昨年12月15日のＥＵの個人情報保護規則の最終合意をみると、やはり最後はぎりぎりで従業員250人とか、データ処理の形態といった論点でかなり中小企業に配慮しているのです。

そういうこともありますから、経産省でガイドラインができて、それが今度個人情報保

護委員会のガイドラインにつながっていくのであろう思いますけれども、そこでは、一般的な事業者、オールジャパンの事業者に対するガイドライン、例えば中小企業社に対する配慮も一般的に書かれると思うのです。ただ、その場合、総論と関係しまして、恐らくクレジットにはクレジット業界にふさわしい負担の軽減の仕方が多分出てくると思うのです。組織とか処理の問題とか、オールジャパンというよりは、クレジットにはクレジットにふさわしい負担の軽減の仕方も出てくるので、そういう意味でも個別に精査したほうがいいと思います。

それから、３つ目ですけれども、例えば非保持化に関しては、今度のＥＵの規則でもプライバシーの場合デフォルトとはっきり書いてあるのですけれども、要するに技術でできることは技術でやってしまったほうが早いというお話があります。これも恐らくだんだん世界標準になっていくと思います。これは負担という意味でも、與口委員がおっしゃった非保持化と非常に共通するところがあると思いますので、やはりそういうことを考えると、技術もクレジットのところとオールジャパンの話とでは同じ中小といっても違ってくる。そのように微妙に状況、守るべき法益が違ってくると思いますので、この際、一般法に対する個別法としての割販法で何ができるかというのをきっちり整理するという方向は、これでよろしいのではないかと思います。

まず最初に、方向性のことについて申し上げました。

○山本委員長　　どうもありがとうございました。そうしましたら、今の点もそうですが、これに限らず、ほかの委員の皆様のご意見をさらに伺いたいと思います。いかがでしょうか。では、まず沢田委員からお願いします。

○沢田委員　　いろいろな最新情報を頂戴いたしまして、頭の中も整理できました。ありがとうございます。

方向性ですけれども、資料７の２ページにありますこれらの措置で十分といえるかという問いかけに対してなのですが、一般論として、私自身はこれまでの小委員会でも申し上げてきたとおり、消費者の自己責任マターを事業者に転嫁するような規制強化は基本的に反対、非常に抵抗があるところなのですが、セキュリティのような安全に関する規制というのは、ちょっと別かなと思っていまして、消費者がいくら自助努力をしようと思っても、どうしようもないところがある。みえないし、判断もできないし、選べないということで、これに関してはある程度公権力の発動といいますか、ちょっと大げさですけれども、特に番号情報管理については、それも仕方ない部分があるのかなという気がしております。

藤原先生からＥＵのデータ保護規則のご紹介がありましたが、中小企業に配慮して足切りを設けるかどうかの問題と、もう１つ定義の問題があります。個人情報保護法ではクレジットカード番号が適用対象になるかどうかはまだ議論中という話ですし、この話はアンタッチャブルというか、何かいうと電話がかかってきてしまうのでやめておきます。

ただ、グローバル性という意味でいえば、インバウンドだけではなくて、日本にいながらにして海外に向けて物を販売したりサービスを提供したりという越境ＥＣは、いまや日常的といいますか、ますます増えていってもらわなければいけないと思います。ＥＵからみると日本は基準を満たしていないのでデータを移転すること自体違法なのかも知れませんが､実態として海外の特にＥＵの消費者の情報をお預かりする事態も出てくるわけです。定義としては、ＥＵデータ保護規則でもＩＳＯの規格でも、クレジットカード番号は単体で普通に個人情報という扱いになっているのではないかと思いますので、万が一、日本の事業者がＥＵの消費者のクレジットカード番号その他の情報を扱っていて漏えいしてしまったときには、ＥＵから非常に大きな制裁金が課されるのではないかということも考えに入れておいたほうがいいのではないかという問題意識です。

どの程度の制裁金かというのは、売上高等によっていろいろなのだと思いますが、日本の加盟店がいま一つ危機感を感じていないという点に関しては、もう少しグローバルという観点からも、加盟店に対する情報提供というか啓発が必要と思いました。漏えい事件もありましたダウンロード販売とか宿泊予約に関しては、物販よりも簡単に海外の消費者が利用し、情報を預かってしまう可能性も高いと思います。ＥＵの制度が常に正しいと申し上げているわけではないのですが、海外との並びという意味でも、少し強めの措置として制裁のような形も考えていいのではないかという気がしております。

済みません、長くなりましたが以上です。

○山本委員長　　どうもありがとうございました。それでは、與口委員からもお願いいたします。

○與口専門委員　　まず、個人情報保護法との関係の中で一言お話しさせていただければと思います。藤原先生がおっしゃったように、割販法の中でどのようにやっていったらいいのかというのを整理することについては、特段の反対があるわけではないのですけれども、今、個人情報保護委員会との間で我々もいろいろと話をさせていただいていて、個人情報保護委員会さんの考え方のベースの中に、今もおっしゃったような、ＥＵのパーソナルデータの中に、いわゆるクレジットカードのような決済用のさまざまなツールが含まれ

るということで、今回、個人情報保護の個人識別符号の中にクレジットカードを指定してはどうかという話があるのは事実です。

ただ、一方でＥＵの規制が日本の法制と同じなのかというと全然違っていると認識していて、私どもは別に個人のプライバシー保護に反対するつもりはさらさらないのですが、今の個人情報保護法の建てつけでＥＵと同じだからというのは、ＥＵと規制が同じなのかというと、そこが違っていますので、イコールではないところで、我々のクレジットカードだけが個人情報の識別符号だといわれて入れられることについては反対ということで明確にお伝えし、調整させていただいているということだけは申し上げさせていただきたいと思います。

その上で違うテーマなのですが、１つ目は、資料７(1)の②不正使用対策のところです。既に資料の中で過度な対応とならないように配慮も必要だとお書きいただいているので、ほぼ同じことだと思うのですけれども、前回の議論の中でも不正使用対策については、法規制になかなかなじまない部分もあるというお話がありました。その中で加盟店に対して何らかの義務づけを行うとしても、不正使用対策についていうと、加盟店さんのリスクというか状況に応じた何らかの対策がちゃんと許容されるような規定の仕方にしていくべきではないかと考えているというのが１点です。

それから、(2)アクワイアラー及び登録ＰＳＰを通じた加盟店のセキュリティ対策の強化というところです。これについては、先ほどご説明いたしましたセキュリティ対策協議会の実行計画も、さまざまな加盟店さんに対してどのようにやっていこうか、アプローチしていこうかということをそれぞれの加盟店さんの実態も踏まえて検討して、これから推進していこうと考えているところです。

今回のご提案も、いわゆる加盟店さんのセキュリティ状況を確認すること自体が目的というよりは、安全性をいかに確保するかということが目的だと思っておりますので、カード業界としても、ある種同じ目的に向かってより効果的な対応を行うために、加盟店の規模ですとか不正使用被害額の発生状況、そういうものを勘案しながら、優先順位をもって取り組む必要もあるのではないかと考えております。そういう意味では、こういった確認をするということについて、時期ですとか方法ですとか対象範囲についても十分検討させていただければと思っております。

それから、こういった番号管理体制とか不正使用体制の整備については、基本的には加盟店さんに課される義務と理解させていただくと、この業界としてアクワイアラーが加盟

店さんの体制整備について確認させていただくことによって、その調査の結果、例えば調査したにもかかわらず流出が起きてしまったといったときに、アクワイアラーに確認義務的なものの責任が課されることがないように、その点は懸念しているところなので、十分検討していきたいと思っているところでございます。

○山本委員長　　どうもありがとうございました。さらにご意見を伺いたいと思いますが、いかがでしょうか。ご質問でも結構でございます。では、二村委員、お願いします。

○二村委員　　ありがとうございます。まず第一に、前回は保護法がどうなるかによって、場合によっては保護法、保護法に入らない場合には努力義務ということなのですけれども、今回の論点整理の中では、割賦販売法の中である程度義務として位置づけていったらどうかというような方向性で再度整理していただいている。基本的には、その方向性がとるべき道かなと考えております。

それは幾つかポイントがありまして、１つは、保護法で追求しているのは、どちらかというとプライバシーであるとか名誉であるとか人格権に直結するような部分が非常にウエートが高い。そうしますと、もともと個人情報、個人データが第三者の間を転々流通することを本来的には予定していないはずなのです。それに対してクレジットカード番号というのは、支払いの中で使われていくものですから、加盟店を経由し、アクワイアラーを経由し、場合によってはそこにＰＳＰやサービスプロバイダが入ってきて、さらにそれがブランドを経由してイシュアーに回ってくる。ネットワークの中でぐるっと回っていく形になるわけです。そうすると、いろいろなところを転々としていくという性質をもってしまっていますので、保護法の規律ときれいにかみ合っているかという疑問が残らなくはない。

その一方で、クレジットカードのミッションという点でいきますと、まさしく正常な利用については迅速的確に認める。その一方で不正な利用は可能な限り排除するという点に置かれているはずですから、その部分はただ単にカード番号の安全管理というだけでは尽くせないものが出てきてしまう。

例えば、今ぱっとネットで調べましたけれども、クレジット番号生成のサイトなどというのは今でも普通にあるわけです。そうすると、個人を識別しない状態の単なるクレジットカード番号と有効期限、さらに最近のはセキュリティコードまで全部くっつけてふるふるで出しますといっているサイトをみつけてしまいましたけれども、そんなものもあるということになりますと、個人情報保護かというと、生存する個人とは無関係な単なる宙に浮いている番号となっていて、やはりここもちょっとずれてくるだろう。そういう観点で

みていったときに、カード情報として保護を図り、正当な利用は認めつつ、不正な利用は可能な限り排除するためにどのような規制体系が有用かという観点でみていったほうがよろしいのだろうと思っております。

その上で、そうはいいつつも加盟店数が非常に多いとか、中小規模の事業者がいるとか、もろもろの特殊性がある中で、ただ義務をかぶせればいいというものでもない。これは逆に実効性を欠き、法律に対する信頼性を失っていくことになりかねませんから、どうやったら実効性があるところで切り出せるのか。リスクに応じたアプローチが重要だろうと思っております。

それから、中身を法律に逐一書くということに関しては、前回のときも申し上げましたが、それはかえってかいくぐる道を教えてしまうという効果をもちかねませんから、基本的な基準を示した上で、あとは各事業者の創意工夫の中で目的を達成していくことが重要なのではないかと思っております。

済みません、ちょっと長くなりました。

○山本委員長　　ありがとうございました。それでは、大谷委員からご発言をお願いいたします。

○大谷委員　　私からは、消費者という立場で幾つか意見を述べさせていただきたいと思います。

今回、セキュリティ対策の強化ということで、強化していただく方向性については、消費者としても賛成させていただきたいと思っております。ただ、ただ強化すればいいということだけではありませんので、やはり強化していただいた上で、それを利用していくのは消費者でありますから、消費者に対しての情報提供や教育といった面をあわせて十分にしていただくことが大切なのではないかと思っております。

それと、加盟店のセキュリティ対策強化の点なのですけれども、情報番号の管理や不正使用対策の義務というところで対象義務となる主体の範囲だとか、違反の場合の措置については慎重な検討がといわれておりますが、消費者の立場からいうと、範囲を狭めるのは、使う側にとっては余り望ましくないと思っております。ただ、ＩＣ化の進捗状況だとか被害の実態をみきわめていただいた上で、やはり慎重な検討は必要なのかなと思っています。

以上です。

○山本委員長　　どうもありがとうございました。ほかにご意見。それでは、まず小塚委員にお願いいたします。

○小塚委員　　ありがとうございます。最初に、私の好奇心から１つ質問がありまして、その後でまじめな意見を申し上げます。

質問というのは、大河内さんに対してなのですけれども、フォレンジックの話が５大ブランドには共通に適用になっているというお話があったのですが、最近日本では急速に銀聯カードの利用が高まっている。同カードのこういう方面の対応はどうなっているのでしょうかというのが、私の興味関心からのご質問です。

○大河内　　我々のほうで今調査に入っている中で、銀聯の漏えいも１桁台ありまして、そういった場合には、どこかのアクワイアラーが一緒にひもづいてやっていらっしゃったりしますので、漏えい事案によって、銀聯カードがどこから連携をとらないといけないかという話になっています。そこは日本だと基本的にはＶＭＪがイニシアチブをとって動いているのが現状でございます。

○小塚委員　　わかりました。ありがとうございます。

それでは、まじめな意見をいわせていただきます。資料７から申し上げていくのがよいと思うのですが、加盟店等に一定の義務を課すこともアクワイアラーや登録ＰＳＰに加盟店調査義務という形でこれを入れ込んでいくことも反対する趣旨ではありませんが、その場合に、結局何をしたら対策を適切にとっていることになるのかということが示されないと、かえって混乱が大きくなるのではないかということです。

特に加盟店の方は、安全対策をとっていますかといわれて、では自分は何をしたらいいのか、わからない方が相当いるのではないか。そのあたりで、資料７の最後でご提案いただいている認定協会の業務、そこでのいわば業界でのスタンダードの開発が重要だと思いますし、それを確認していったり推奨していくという形の義務づけでないと、恐らく現実的ではないだろうと思います。そのことがまず１つです。

それから、２つ目に、きょうご発言にあった中で、池本先生のおっしゃったことと私は若干違う感覚をもっていまして、今申し上げたこととも関連するのですが、恐らくこういう問題に理想型というか､最後こうしたらいいという形はないのではないかと思うのです。つまり、番号を保持するのも保持しないのも、それは要するにリスク管理のあり方であって、どちらがよいということではない。保持しないほうがリスク管理のコストが安い場合もあれば、保持するほうがリスク管理のコストが安い場合もあって、それは保持しようとしている人の体制やら希望やら専門知識によることだと思いますので、さまざまな状況を総合判断した上で、それぞれの場合に最適なリスク管理の仕方があるということではない

か。ですから、唯一絶対必ずこうしなさいという答えがある性質のものではないのではないか。

負担というお話も同じことだと思いまして、不正使用によって、回収できない金額がアクワイアラーに発生する。それを保険という形でリスク転嫁することも転嫁しないことも、それはその事業者の立場に応じた最適なリスク管理の仕方があるということではないか。内閣サイバーセキュリティセンターからのプレゼンの中でご指摘のありました機能保持という考え方は、要するにそういうことではないかと私は考えました。

○山本委員長　　そうしましたら、丸山委員、お願いいたします。

○丸山委員　　では、丸山から意見を述べさせていただければと思います。

基本的にご提案いただいている方向で検討していくことが重要ではないかという印象をもちました。まず、番号と情報管理に関してでございますけれども、検討課題として出していただいておりますように、努力義務にとどまらない義務ということも考えていいのではないか。特にカード情報を保持するような主体は、先ほどのプレゼンの中では加盟店に限らずサービスプロバイダみたいなお話も出てきましたので、そのときに主体をどのように設定するのかというところも意識しながら、情報を保持する主体について効果的な対策がとれればいいのではないかと思いました。

ただ、その場合に、義務違反として一定の制裁が考えられることになるのですけれども、どういったところまで定める必要があるのかというのは、まさにどこまでやればよい方向性を促進できるかということとの兼ね合いだと思います。いきなり罰金罰則にいかなくても、一定の行政的な命令、指導のレベルということも考えられますし、後のほうで出てきた不正使用対策義務とかアクワイアラーとかが果たす役割との兼ね合いも出てくるのではないかと思いますので、全体としてどういった像が描けるのかというところに定めるべき義務とか制裁の内容が反映されるような関係にあるのではないかと思いました。

それとの関係で、先ほどもちょっと指摘されました加盟店がどのようなセキュリティ対策をとっているのかをアクワイアラーに調査させてはどうかという点に関してなのですけれども、やはりこれもどういったところに結びついていくのかというのをある程度明らかにする必要があるのではないかと思いました。

先ほどのプレゼンの中に出てきたようなアクワイアラーと加盟店が契約するときに一定のリスク転嫁みたいなことを行った諸外国の例も多いという話が出ていて、それが日本とマッチングするかどうかはわからないという話にはなっていたのですけれども、ある意味

クレジット業界全体として、そういう方向性で契約をつくっていくのもあり得るということになれば、その前提としてセキュリティの状態を調査することも必要になってくると考えます。そういったところとの兼ね合いを考えていく必要があるのではないかという印象をもちました。

以上です。

○山本委員長　　ほかに。では、小塚委員が思い出されたということで、そちらから短くお願いします。

○小塚委員　　先ほど申し上げようとしたことを思い出しました。

最後に申し上げたかったのは、こういう問題の場合、消費者の利益とはどういうことなのかという点を、特に消費者側といわれる方々と一緒にもう一度考えたいということです。つまり、セキュリティ対策をとれないところはカードを使うことができません、加盟店でなくなっていきますということになっていくと、ある意味でいうとカードの利用できる範囲が非常に狭くなっていく。それが消費者にとって望ましい世界なのかということも含めて、消費者の利益とは何だったのだろうというのをもう一度考えてみる必要があるということです。

○山本委員長　　それでは、関連する発言であれば二村委員。

○二村委員　　先ほど丸山先生から、アクワイアラーの調査というところでご発言があったものですから、それに関連して一言だけ。

現実問題として、加盟店のセキュリティ状況の調査というのは、特にシステムを大規模に展開している加盟店さんの場合には、カード会社にとっては不可能に近いことになりかねない。ですから、どういう調査、どのレベルを求めるのかということについては、相当慎重な判断をしなければできない義務を課してしまって、結局、画餅に帰すということになりかねないと思いましたので、その点を一言。

○山本委員長　　では、岩崎委員、お願いします。

○岩崎委員　　先ほどの資料で、個人支出に占めるクレジットカードショッピングの割合が２割近くということで、徐々にふえているのですが、諸外国に比べてまだまだ低いという話が出たかと思います。

クレジットカードに対する消費者の一番の不安は、やはりセキュリティだと思うのです。使いたくない最大の要因がセキュリティだということを踏まえますと、これからキャッシュレス社会に向けて進むためにセキュリティ対策は必須だと思うのです。その一方で、例

えば番号等情報管理で加盟店に過度な負担をかけると、今度は加盟店のほうがクレジットカードの取り扱いを躊躇することになってしまい、そうしますとやはりキャッシュレス社会の進展が止まってしまい、小塚委員がおっしゃったように、消費者の利益にとってどうなのかということになります。この２つのジレンマがありますので、今回の議論ではどうやってバランスをとっていくかがすごく大切かと思います。

以上です。

○山本委員長　　どうもありがとうございました。ほかに。では、沢田委員、お願いいたします。

○沢田委員　　ありがとうございます。たびたび済みません。

先ほどの自分の発言と矛盾するようなことを申し上げます。長くなり過ぎてしまったので途中で切ったのですが、基本的な考え方としては法規制もやむを得ないと申し上げました。ただ、実際に何を法律に書くのかというところになると、やはり皆さんおっしゃっていたように大変難しいものがあると思います。適切な対応を求めるとした時の適切な対応が何なのかわからなければ、もちろん加盟店も適切な対応をとれないでしょうし、適切な対応をとっているかどうかアクワイアラーさんも判断できないでしょうということです。

協議会の実効計画にありましたPCI DSSが全てかというと、それを法律に書くというのは非常に違和感があって、技術中立性の観点からどうかと思いますし、これ以外でもちゃんとやっているといえる対策はあるのかもしれないと考えます。

そこで急に弱気なことを言うのですが、妥協案といいますか、それにかわる手段として、例えば、PCI DSSをもっているならもっているという、もっていないならいないという、PCI DSSはないけれどもＩＳＭＳをとっているとか、それを表示義務の形で加盟店に協力してもらうことはできないのかというご提案です。

前回議論されていたアクワイアラーやＰＳＰの情報を特商法の表示義務に入れるということと比べると、負担の点では同じですけれども、有効性に関してはこっちのほうがまだ筋がいいという気がします。消費者がそれをみて何かを判断することは余り期待できないのは同じですが、今回の対策について加盟店に認識していただくためには、割賦販売法は加盟店は自分に関係する法律だと思っていないですから、特商法で検討するほうが現実的かと思ったりしております。オプションの１つとしてお考えいただければ。

済みません、長いのですけれども、もう１つ。不正使用対策のほうは、法律にするのは、さらに難しいと思っています。まだちょっと情報が足りないという印象があります。カー

ドを使用する場面での話ですが、対面に関してはＩＣ化を進めてというのはおっしゃるとおりで、消費者側としても利便性の観点から、一々サインしなければいけないのはとても嫌なので、これはどんどん進めてくださいと思います。

非対面に関しては、消費者はパスワードとか余計なものを聞かれないほうが楽です。もちろん自分のクレジットカード番号でなりすまし注文されてしまうのは嫌ですが、なりすましだときちんと主張できれば、カード会社か加盟店のどちらかが負担を負っていて、消費者には請求が来ない。なので、ここでは消費者の事情よりも聞かなければいけないのは加盟店の考え方だと思うのです。

実態として、どういうベストプラクティスがあるのかとか、不正使用でチャージバックされた経験のある加盟店が、その経験に基づいてどんな措置をとっているかとか、自分でアナログに電話をかけてみるという方法もあるでしょうし、モールなどプラットフォームが提供する不正カードの検知対策が非常に功を奏しているかもしれません。もう少し加盟店側のそういう事情なり実態がわからないと、どうすべきかというところがまだちょっとみえてこないのかなという気がいたしました。

済みません、長くなりました。

○山本委員長　　どうもありがとうございました。ほかに。池本委員、お願いいたします。

○池本委員　　何人かの方の意見をお伺いしている中で、義務化は中身がはっきりしないから難しいのではないかという意見が複数あったので、それに対して意見を述べたいと思います。

１年前の審議のときには、加盟店に義務といったって何をどうすればいいかわからないから努力義務ぐらいにしましょうというような議論で終わったと思います。この間、セキュリティ対策協議会でも非常に中身の濃い議論をしていただいて、対面の加盟店はどういう選択肢があるのか、あるいはＥＣの場合はどうか、アクワイアラーは一体何をするのかというようなことをかなりきめ細かに議論なさって、2020年３月までには100％にもっていこうとか、2018年までには何をしようという、具体的な実行計画をおつくりになっているわけですよね。その意味では、なすべきことというのがかなりみえてきた段階ではないかと思うのです。

先ほど資料のご説明のときには、これはすごい、かなり先がみえてきているのかなと。ただ、そうはいっても、加盟店といってもさまざまな分野でたくさんあるから、それを自主的にやってくださいといったってそうはいかない。そうすると、一定の義務づけをし、

だからといってすべてカード非保持にせよとかということを申し上げているわけではなくて、今ある選択肢の中で、最終的に安全なセキュリティの水準をどの辺に置くかというのは、恐らく法律で条文の中に書き込むことではなくて、政省令なりガイドラインなりに落として、時期によってまた見直してということが必要な分野だろうと思うのです。

それとともに、アクワイアラー、ＰＳＰについてのセキュリティ対策の義務化に対しても消極意見が複数あったのですが、やはりカード決済システムの最終的な運営者はカード会社ですから、加盟店に対する働きかけをしていただくのはカード会社です。実行計画の中でこういうことをやろうというのが出てきた、なにもこの線引きがちょっとでもおくれたら処分するという意味ではないはずです。あくまでも一定の幅のあることとして申し上げているのです。やはり今、カード会社で加盟店に対して、あるいは消費者に対する啓発も含めて、全体としてこの実行計画をどう実現していくのかと考えていく。中身は柔軟な配慮が必要だけれども、加盟店に対しても一定の義務を課すという規定を明示して、それを社会の中でもアナウンスするとともに、きめ細かに働きかけていく。カード会社についてもそういう義務を置いて、先ほどお伺いしたように200社あるのだとすれば、本当に全部足並みがそろうのかどうか。昨年のマンスリークリアカードの議論のときにもカード会社によって対応がばらばらですという話があったと思うのです。

だから、今回も最低限の線引きをして方向づけて実行計画もおつくりになったのだとすれば、それを後押しするような形で義務化することが必要ではないかと考えております。

以上です。

○山本委員長　　どうもありがとうございました。ほかにご発言はございますでしょうか。尾島委員、お願いいたします。

○尾島委員　　キャッシュレス社会を目指すということですので、加盟店もどんどんふえていかなければいけないということが前提だと思うのですけれども、資料にもありましたとおり、直近では46兆円で消費全体の約16％を占めると。これが多いかどうかというのはまた問題があると思うのですけれども、加盟店になっているところでも恐らく現金取引を一部しながら、カード取引もしながらという形での16％だろうと思います。

よく考えてみますと、さっきの小塚先生とかのご意見にもありましたけれども、確かに加盟店というのはカードシステムに不可欠なプレーヤーではあるのですが、加盟店をやっていく上でカードは不可欠ではないという問題があります。もちろん加盟店はいろいろあるので、そのレベルによってどういう対応ができるかというのは変わってくると思うので

すけれども、いろいろな義務を課すことによって、自分はカードをもう取り扱わないということになってしまうと、キャッシュレス社会を目指しているということと逆行することにもなるので、その点についての配慮はどうしても必要になってくるのではないかと思いました。

イシュアー、アクワイアラー、あるいはＰＳＰなどは、当然カードにかかわる事業しかしないのですけれども、加盟店というのは、基本的にサービスとか販売を提供するのであって、カードは単なる決済手段ですので、離脱ということが十分あり得るのではないかと考えた次第です。

以上です。

○山本委員長　　どうもありがとうございます。ほかにご発言ございますか。鈴木委員、お願いします。

○鈴木委員　　セキュリティ対策の強化というのは、全般的には大いに賛成です。一方で、日本の消費者の場合、利便性については非常に関心が高いのですけれども、安心・安全に対して、特にカードについては少し認識が甘いところがあるのではないかと感じることがあります。

先ほどみえる化という言葉が出ましたけれども、カードを安全に使うためにはどうしたらいいか。例えばこのような対策をしているお店だったら安心ですというみえる化をする、消費者も意識を高めるというように、事業者側と消費者側の双方で対策をしていくことが必要ではないかと思っています。

○山本委員長　　それでは、オブザーバーの沖田様、よろしくお願いします。

○沖田オブザーバー　　オブザーバーの立場から失礼いたします。

冒頭の池本先生からのご質問に戻ってしまうのですけれども、非保持化を進めていく中で、保有しないといけないのはどういうシチュエーションなのかというところで、例えば継続課金においては必要かというお話があったかと思うのですけれども、こちらは多少知見がありますので、お話しさせていただきます。

かつては必要とされていることが非常に多うございました。一方で、今は多くのＰＳＰのほうでカード番号をもたなくても継続課金できるサービスを提供しているのが実態ではないかというところです。そういう意味では、先ほどのご発言にもありましたけれども、

テクノロジー、特にきょうもありましたフィンテックの企業がそういったものを解決していけると強く感じております。事実、フィンテックの代表企業であります日本のベリトランスですとか米国のストライプというのは、そういう機能を標準でもっております。そういう意味では、先ほどもありましたけれども、セキュリティとコスト、それから利便性というのは両立していかないといけないと思うのですが、これはまさにFinTechの企業が両立していくべきものですし、事実、そういった部分はFinTech企業がかなり進んでいるのかなと感じております。

その上で１点ご質問させていただきたいのですけれども、資料３の14ページ、クレジット取引セキュリティ対策協議会において、カード番号の非保持というところ。実行計画の非保持のエンドデートを2018年３月、それから2020年３月と具体的に置いているのはすばらしいことではないかと。特にカード会社とＰＳＰは、先ほどの大河内さんのお話も考えると、もう少し早いほうがいいのかなと思う一方で、ＥＣ加盟店も同時期、2018年３月までにしたというのは非常に画期的な検討案ではないかと。

その上で、資料７の問いかけでもありますが、それで十分なのかという観点では、これは正しく実行できるのかに尽きると感じております。そういう意味でご質問がございまして、これはＰＳＰを代表しているＧＭＯペイメントさんがいいと思うのですけれども、現在の非保持化はどのぐらい進んでいるのかというところです。これは加盟店ベース、金額ベースでどうなのか。

私個人の理解では、少なくとも半年前の段階では、通過型の非保持というのはかなり進んでいると思うのですけれども、今回、保有型も通過型も認められない。認められるのは原則的にリンク型とトークナイゼーション型だとすると、現状、日本ではかなり少ないのではないかと思っておりまして、ＥＣ決済協議会で実際そういった現状の非保有化率が業界全体としてどのくらいか把握されていれば。もし把握されていないようであれば個社でも構いませんので、いただけると非常にありがたい。2018年３月はもう２年先ですので、決して簡単ではないと思っているのですけれども、これが現実的か否かというのをぜひ教えていただけるとありがたいと思っております。

○山本委員長　　それでは、どなたへのご質問ですか。資料ということではクレジット協会向けのご質問ということでよろしいですか。

○沖田オブザーバー　　クレジット協会さんとＧＭＯペイメントさん両方にお聞きできるとありがたいかなと。

○山本委員長　　そうですか。では、まず與口委員から可能な範囲でお願いします。

○與口専門委員　　済みません、大変恐縮ですけれども、そのような形の数値はもっておりませんので、協会としては把握していないというお答えになります。

○山本委員長　　そうしましたら、吉岡様、お願いいたします。

○吉岡オブザーバー　　吉岡でございます。

ＥＣ決済協議会のほうでも、残念ながら非保持化の比率等々の数字は現状もっていない状態です。申しわけありません。

○山本委員長　　そうしましたら、多分まだご発言がおありかと思いますが、時間的にはぎりぎりになってしまいました。本日は、大変貴重かつ多様なご意見をお述べいただきまして、本当に感謝申し上げます。

本日の論点ペーパーの問いかけは、全て「検討する必要はないか」となっておりまして、皆様のご意見、方向性としては検討する必要があるかもしれないけれども、その中身については相当多様であったかと思います。検討する必要ということでは支持するご意見が大宗を占めたのではないか。沢田委員などは最初物すごく積極派で、途中ちょっと修正されましたけれども、総体としては検討する必要は大いに認められるということではなかったかと思いますので、きょうのご意見を踏まえて、さらに事務局のほうで整理して進めていただきたいと思います。

先ほど申しましたけれども、もともと昨年７月の報告書も割販法の上乗せあるべしということで議論していましたが、無登録ＰＳＰと加盟店等については特段の措置を講ずる必要性は低いと。それから、不正使用対策について、法令上の義務づけ等の措置は見送りとなっていたところが、今回は、それらにつき検討する必要があるというのは、この間の推移、あるいは世の中のこの問題についてのセンシティビティが高まったことを踏まえまして、仕切り直しということになります。したがいまして、今後、きょうの議論を踏まえてまたペーパーをお示しすることになると思いますので、その際はご審議の方をよろしくお願いいたしたいと思います。

それから、議論を伺っていまして、(2)加盟店調査義務と(1)加盟店等への義務づけとは論理的に関係があるような感じもいたしましたが、そこはどうなのでしょうか。つまり、加盟店に義務がかかっていないのにアクワイアラーに調査しろということが可能なのかという問題もあるように思います。その辺も含めてさらに整理をお示しいただければと思います。

ということで、大変残念ですけれども、時間がまいりました。最後に、きょうは国会等の用務でおくれておられました住田商務流通保安審議官がおみえでございますので、審議官から一言ご挨拶を申し上げます。よろしくお願いいたします。

○住田商務流通保安審議官　　ありがとうございます。おくれてまいりまして、大変恐縮でございます。商務流通保安審議官の住田でございます。

きょうの議論、大変白熱した議論でございまして、私もこの問題は我が国の国民全体にとって極めて大事な問題だと思っておりまして、しっかりとした仕掛けをつくっていきたいと思うわけでございます。

一方で、先ほど鈴木委員からご指摘ございましたように、日本の国民というのは、なぜか安全・安心の認識が非常に甘いところがあって、特にクレジットカードについてはそうなのかもしれませんが、なかなか切迫感がないのですが、きょうのご説明にもあったと思いますけれども、まさにアメリカが大きく変化する中で、我が国がセキュリティホールになってはいけない。

その一方で2020年にはオリンピックがあったり、4,000万人の観光客を受け入れるのだということがある中で、そうしたことになってしまいますと、これは誰が困るって日本人みんなが困るし、経済界も困るし、クレジットカード業界も困ることになりますから、決してそんなことのないように考えなければいけない。

一方で、きょうのご議論にもありましたように、どうも１つの答えになるものではないようだということで、これは皆さんのご議論の中から非常に鮮明に出てくるわけでございまして、かといって加盟店がそんなことをするのは大変だからやめようとかという問題でもない。できる力のある人と、そんな余力、資力のない人とで対応が違うのではないか、これも当然あるわけであります。

こういう状況の中での制度というのは非常に難しいことは間違いないのですが、きょうのFinTechのご説明にもあったと思いますけれども、FinTechの時代というのは、いろいろなイノベーティブなことができる時代なのではないかと我々は思っていまして、これまでの任意登録制みたいな議論自体がそうなのですが、イノベーティブな世界に対しては制度もイノベーティブにやっていこうというのが正直な気持ちでございます。

そういう意味からいうと、きょうのご議論を踏まえれば、どうも複数の道を用意するということがすごく大事なのではないか。規制、ある種の義務化をするにしても、義務の内容は何なのですか、ある種抽象的なことはいえても、それを具体的にはこういうやり方、

こういうやり方、こういうやり方があるのですというのを、どのレベルかわかりませんが、示していくことによって、いろいろな方が、では自分はこれでやってみよう、自分はこっちだと、まさにそれぞれのリスクのとり方という問題とも関係するわけです。そんな仕掛けを皆様の英知をいただきながらつくっていければ、カードの世界でセキュリティ後進国だと思われていた日本が急に前へ出るということも実現できるのではないかと思います。

きょうも関係省庁いろいろな形で来ていただきましたので、関係省庁も一丸となって、また、きょうお集まりの委員の方々、あるいは産業界の方々の意見もよくお聞かせいただきながら、より適切な方向性をまとめさせていただきたいと思います。きょうはどうもありがとうございました。

○山本委員長　　どうもありがとうございました。

それでは、次回以降の予定について事務局からご案内をお願いいたします。

○坂本商取引監督課長　　ありがとうございました。次回は、ちょっと間が短くて恐縮ですが、今月21日木曜日10時から、本日は２時間半いただきましたが、今度は２時間でお願いしております。

21日の議事に関しましては、事務局から昨年７月の報告書でいただきました幾つかの宿題の進捗状況をご報告させていただきますこと、あと３点議題をお願いしたいと思っております。１点が、きょうも消費者庁からご出席いただいていますけれども、特定商取引法改正法案を踏まえて、割販法で対応する必要があるかどうかの幾つかの改正事項についてのご検討。もう１つは、FinTechによるイノベーション促進のための対応。そして、本日いろいろいただいたご意見を事務局で整理させていただいて、セキュリティに関してはもう一度、引き続き議論いただければと思っておりますので、どうぞよろしくお願いいたします。

○山本委員長　　それでは、これをもちまして割賦販売小委員会の第14回を閉会いたします。本日はどうもありがとうございました。

――了――