第30回　産業構造審議会　商務流通情報分科会　割賦販売小委員会　議事録

日時：令和４年６月２日（木）16時00分～18時00分

場所：オンライン開催（Ｔｅａｍｓ）

○刀禰商取引監督課長　　ただいまから、経済産業省産業構造審議会割賦販売小委員会を開催いたします。御多忙のところを御出席賜りまして、委員の先生方におかれましては誠にありがとうございます。

私は、経済産業省で事務局を務めます商取引監督課長の刀禰でございます。今日はどうぞよろしくお願いいたします。

本日はオンラインでの開催となります。通信負荷軽減の観点から委員の方々におかれましては、御発言いただくときだけマイクをオンにしていただければと思います。カメラについては常時オンでよろしくお願いいたします。また、本日はＹｏｕＴｕｂｅでの同時中継となっております。

開会に当たりまして、まず新しく御着任いただいた委員のお二方を御紹介いたします。５月31日付で、公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会の長谷川ゆかり委員及びＢＳＩグループジャパン株式会社認証事業本部金融セクター部長・森竹由美子委員、お二方に本日御着任いただいております。

本日は、定足数を超える委員の皆様に御出席をいただいておりますことを報告いたします。

次に、配付資料の確認をさせていただきます。事前に事務局から資料を送付させていただいておりますけれども、不足があります場合にはＴｅａｍｓのメッセージ欄に御記載いただければと思います。また、御発言がある場合にはＴｅａｍｓのメッセージ欄にその旨を御記入いただきますよう、よろしくお願いいたします。御発言に当たりましては岩原委員長、もしくは事務局のほうから御指名をさせていただきます。

本日の議事の運営に関してでございますけれども、議事については原則公開とし、議事録につきましては事後に公表とさせていただきたいと思います。

続きまして、今回は２年ぶりの委員会の開催ということでございます。先ほど御紹介しましたお二方、新しい委員にも御着任いただいております。つきましては、改めまして各委員から１分程度で自己紹介をお願いできればと思っております。順番につきましては五十音順でお願いしたいと思います。

それでは、まず池本委員のほうからお願いできますでしょうか。よろしくお願いします。

○池本委員　　池本でございます。よろしくお願いします。

本日は、特に悪質商法などで利用されるクレジット決済によって、トラブルが高額化するといった辺りの情報をいろいろ相談事例などで、あるいは弁護団などで見聞きしているところがあります。安心・安全なカード決済となるために、言わばキャッシュレス決済の中の最も先頭を走るルールとして、さらに高めていただきたいということで、いろいろ発言させていただきたいと思います。よろしくお願いします。

○刀禰商取引監督課長　　ありがとうございます。

続きまして、岩下委員、よろしくお願いいたします。

○岩下委員　　京都大学公共政策大学院の岩下と申します。

私は現在の職務に就く前に日本銀行のほうで、最終職はＦｉｎＴｅｃｈセンター長というのを務めておりましたが、金融機関の様々な新しいビジネスの展開や、そこにおける安全対策等について技術的、制度的、あるいは経済学的な観点からの分析を行ってまいりました。

私がクレジットカードのセキュリティの問題等に関与してかれこれ30年になりますが、現状はいっかな改善していないというか、むしろますます悪化していることを大変憂いております。

私自身、30年前から、インターネットでクレジットカードを使うときのＳＥＴという規格が当時ありましたが、それをＳＥＰＰとＳＴＴからつくるというのがサンフランシスコで開かれた会議であったのですけれども、そういうものの策定にも参画しております。その意味では、残念ながらＳＥＴはその後はやらなくて今は３-Ｄセキュアなどになっていますけれども、いずれにせよ、そういう努力を関係者がしてきたにもかかわらず、なかなか事態は改善しないことが大きな問題だと思っております。

私自身は政府の暗号技術検討会などに参加しつつ、情報技術の観点からどのように安全な決済が可能かということ。そしてクレジットカードビジネスが何やらへんてこりんな規制に日本はなっているのですけれども、世界的な標準に基づいた形での、きちんとした技術的なセキュリティの対策が取られることが非常に大事であることを常々感じておりますので、そういう観点からコメントさせていただきたいと思っております。どうぞよろしくお願いいたします。

○刀禰商取引監督課長　　ありがとうございます。

続きまして、岩原委員長、よろしくお願いいたします。

○岩原委員長　　委員長を拝命しております早稲田大学法学部・岩原でございます。

私の専門は会社法、金融法でございまして、金融法の中でも決済を主に研究してまいりましたので、その一環として割賦販売法についても勉強させていただいております。

令和２年の改正のときには皆様の御意見がなかなか分かれまして、取りまとめるのに苦労いたしましたけれども、今回はまた非常に難しいセキュリティの問題で課題は重いのでありますが、皆様の御協力をいただきまして岩下さんに怒られないような、今よりは少しでもよりよい制度改正としたいと思いますので、皆様の御協力をよろしくお願い申し上げます。

○刀禰商取引監督課長　　ありがとうございます。

続きまして、沢田委員、お願いいたします。

○沢田委員　　一般社団法人ＥＣネットワークの理事をしております沢田と申します。よろしくお願いいたします。

ＥＣネットワークのＥＣはＥｌｅｃｔｒｏｎｉｃ　Ｃｏｍｍｅｒｃｅの略でございまして、私どもＥコマースのトラブル相談を受けている組織です。消費者も事業者も安心して参加できるＥＣ市場を目指して活動しております。セキュリティは以前から大変重要な課題であることとともに、現在は消費者にとっても、事業者にとっても喫緊の課題となっていると思いますので、今回改めてテーマに取り上げていただき感謝申し上げます。どうぞよろしくお願いいたします。

○刀禰商取引監督課長　　よろしくお願いいいたします。

続きまして、田中委員、よろしくお願いいたします。

○田中委員　　野村総合研究所の田中です。

私、野村総研の中ではコンサルティング事業本部というところに所属しておりまして、その中でクレジットカード会社ですとか、その他キャッシュレス関連企業の事業拡大に伴うコンサルティングですとか、あるいは新たにこの分野に参入したいという企業の事業参入の戦略を考えるようなコンサルティングなどを主にやっております。あるいは、政府や自治体等でのキャッシュレスを推進する政策の御支援といったことをさせていただいております。よろしくお願いいたします。

○刀禰商取引監督課長　　よろしくお願いいたします。

続きまして、二村委員、よろしくお願いいたします。

○二村委員　　ありがとうございます。弁護士の二村でございます。

私、割販小委に参加しましたのは平成28年改正に関わるもの以降でございますが、業務としては弁護士登録をしてからほぼ一貫してクレジットカード、クレジットの分野をやっております。そこが自分の業務の大半を占めるというぐらいの形です。ですから、先ほどＳＥＴの話が出ましたが、非常に懐かしい、普及しなかった大変残念な規格であったと記憶しておりますが、そういう中で主としてクレジットカード会社、事業者側の情報のほうが私には多く入っている点では池本先生とは対極をなす部分があるかと思いますが、決して消費者の利益をないがしろにしていいという立場ではなく、どのようにして最大公約数的に消費者の利益を図れるか、よい制度をつくれるかという観点から御意見を申し上げたいと思っております。よろしくお願いいたします。

○刀禰商取引監督課長　　ありがとうございます。

続きまして、長谷川委員、よろしくお願いいたします。

○長谷川委員　　公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会の長谷川と申します。協会の名前はとても長いのでＮＡＣＳと省略しまして、ナックスと称しています。

私はふだん、行政の消費生活センターの相談員として勤務をしております。法律の専門家ではないので、ふだんの相談業務を通して感じたことをお伝えさせていただきたいと思っております。このような委員を務めさせていただきますのは初めてですので、どうぞよろしくお願いいたします。

○刀禰商取引監督課長　　よろしくお願いいたします。

続きまして、藤原委員、御発言可能でございますでしょうか。通信の調整中かと思うのですけれども、藤原委員、御発言可能でしたらお願いできますと幸いです。

○藤原委員　　藤原でございますが、申し訳ありませんでした。

最初から聞いていなかったのですけれども、第三者としてこれまでクレジット、あるいは最近キャッシュレスの研究会等に参加させていただいておりますので、そこで得た知見を基に、また今日の議論にも出てくると思いますけれども、デジタルということで情報が統一化され、国際化される時代でございますので、それを背景にクレジットの安全と執行の完全性を目指して議論をできればいいと思います。

申し遅れましたけれども、私、専門は行政法でございまして、その中でも特に情報の関係の法律を勉強しております。ここで皆様方と一緒に深く勉強させていただきたいと思い

ます。どうぞよろしくお願い申し上げます。

○刀禰商取引監督課長　　ありがとうございます。

それでは、最後に森竹委員、よろしくお願いいたします。

○森竹委員　　ＢＳＩグループジャパン株式会社の森竹と申します。今回から小委員会のメンバーとして参加させていただきます。どうぞよろしくお願いいたします。

私はＢＳＩグループジャパンで認証事業本部金融セクター部の部長を担当しています。主にＱＳＡとしてＰＣＩＤＳＳの準拠評価を実施しております。また前職では、金融システムを含めまして情報システムに対するセキュリティ実装というところと、あとはセキュリティのマネジメントという辺りも従事しておりました。どちらかといいますと、私は現場からの視点となる傾向が多いかもしれませんけれども、皆様と連携して、この小委員会の目的を達成するために御貢献できればと考えております。どうぞよろしくお願いいたします。

○刀禰商取引監督課長　　よろしくお願いいたします。

以上、各委員の皆様に御挨拶いただきまして、どうもありがとうございました。

それでは、これより先の議事進行は岩原委員長にお願いしたいと思います。どうぞよろしくお願いいたします。

○岩原委員長　　それでは、議事に入りたいと思います。

お手元の議事次第にございますように、本日の議題は「割賦販売法の令和２年改正後の主な動向と課題」でございます。事務局より資料の説明をお願いいたします。

○刀禰商取引監督課長　　事務局の商取引監督課でございます。

まず資料２―１を御覧ください。

１ページ目、目次でございます。本日は割賦販売法、２年前の改正以降の動向、執行状況について御説明いたします。また次には、２.クレジットカード事業者を巡る様々な政策課題についても御説明いたします。そして最後に、今後の検討課題ということで、本日はサイバーセキュリティ等への対応を中心に御審議いただければと思っております。

続きまして、２ページ目でございます。早速、割販法の執行状況ということであります。

右下にページ番号を振っております。３ページ目でありますが、前回２年前の令和２年改正でございます。当時におきましては、まず１つには新しい与信審査制度の導入をやっております。ＡＩやビッグデータといった新しいイノベーションを活用しながら、与信審査制度をより合理的なものにしていくことについて当時検討を行っていただき、新たな認

定・登録の制度をつくっていただきました。

他方で２つ目のポツに書いておりますけれども、クレジットカード番号の情報漏えいリスクというのは年々広がっております。こうした中でクレジットカード事業者に関わっているプレイヤーが非常に多様化している。こういう状況に鑑みまして、割賦販売法の適用対象を拡大したということになっております。こういった各種の措置を当時させていただいたところでございます。

４ページ目でございます。ちょうどそれから１年後の昨年４月から、この改正法につきましては施行をいたしました。施行から１年経過いたしまして、まず新たな認定・登録制度については事業者からの申請がございまして、こちらに対する厳正な審査を行い、既に３件登録や認定を行ったところでございます。

今後は、これら事業者に対しては、重要なことは合理的なＡＩ等を使った与信管理制度が適切にうまくいっているかどうか、また、各社においてＰＤＣＡをしっかり回し改善が図られているか、また、消費者保護の観点から問題が起こっていないかどうか、こういったことを確認していく必要がございます。今後各社から提出される定期報告書を当省で確認をし、延滞率等の確認を実施し、必要な場合は検査等の監督を行っていくことで考えてございます。今既に３社でございますが、今後またこういった申請についても数社から予定が見込まれているということでございます。

続きまして、５ページ目でございます。こちらのほうは監督上の行政処分を行った主立った事例を掲載しております。特にこの１年におきましては、加盟店管理を行い、そして様々な決済事業を、キャッシュレスを利用拡大させていく、こういった取りまとめを行っていくアクワイアラーにおいて不適切な事案、悪質な事案というものが少なからず見られております。こういった事業者に対して検査を行うことはもとより、必要に応じて業務改善命令、さらには登録の取消しに至った事案もございます。

特に特徴として考えられるのは、消費者問題として昔から苦情が多い情報商材をはじめといたしまして、占いやあるいは風営的なサービスも含めた様々な事業について消費者との関係でトラブルが起きた時、これに対する苦情処理がしっかりできるような体制になっているか。これらについて本来的にはアクワイアラー自身が管理責任を最終的に果たしていく必要があるのですけれども、こういったところについて十分でない事例などが見受けられます。これらの事業者に対しては厳正な体制を取っているところでございます。

６ページ目でございます。とはいえ、実際私どもが割販法に基づきまして監督を実施し

ていく上で、実務上の苦労もございます。これはあくまで一例として記載しておりますけれども、事業者が最近は分業化する中で、国を超えて国際的なつながりの中でビジネスを行っているものも当然増えてきております。

国内におけるアクワイアラーと、海外のＰＳＰ、決済代行業者がつながるような事業ビジネスも最近見受けられます。こういったところにおいて国内の加盟店を管理する責任を負うアクワイアラーは登録が必要なわけでありますけれども、この登録を実質的に行っていないところで無登録業者が見られる。あるいは国内の加盟店管理を行うべき事業者と海外の代行業者との間で、加盟店管理に関する責任関係が明確でない問題があったりしているところでございます。

こういった事業者に対しては、我々が一つ一つ各社にアプローチをして確認を行っているところでございますが、なかなか民間の中で十分に法律の遵守、コンプライアンスの意識が十分でなく、実際に登録が必要だということは、むしろ行政のほうからアプローチがあって気づくような事案もございますので､その意味でこうした事業者に対する注意喚起、指導徹底というものはしていかなければいけないと考えているところでございます。

続きまして、12ページ目に移ります。今度は割販法以外の関係法令との関係で、対応していかなければいけないものについても御紹介申し上げます。

13ページ目でありますが、これは簡単な絵で整理をしております。御覧のとおりクレジットカード事業者は、今や社会インフラということでございます。

したがって、割販法に基づいて様々な規律を求めているわけでありますけれども、当然消費者保護、個人情報保護、サイバーセキュリティといった必要な社会課題に対しても、割販法以外の関係法令との関係で適切に対応していかなければいけないというのが現状でございます。

具体例を幾つか御紹介申し上げます。

次の14ページ目であります。１つは、成年年齢引下げへの対応ということであります。各委員御案内のとおり、今年４月に改正民法が施行されました。成年年齢が20歳から18歳に引き下げられまして、若い人たちにとっては新成年の新しい権利が拡大したということでもございます。クレジットカードについても従前は親の同意を得て契約することが必要であったものが、もう大人として親の同意を得ることなく契約することができる時代に入ったわけです。

他方で18歳といいますと、まだ高校生の方もいらっしゃいますし、社会経験についても

まだまだ十分でないという背景もございます。その意味で悪質な勧誘を受ける、あるいは多重債務を防いでいく観点からは、丁寧に新しい新成年の消費者に対応していく必要があるということであります。

経産省におきましては、まず１つは教育ということで対応しておりますけれども、日本クレジット協会においても様々な教材を作成し、学校への無料配布や、あるいは中学、高校への講師の派遣なども行っております。さらに経済産業省としては新しく学習塾等でも、そういった情報提供の場を広げていくことで取組を強化しています。

２つ目、真ん中、広報・啓発につきましては経産省の消費者相談室も含めまして、関係省庁の様々なチャンネルを通じて、何かあればいつでもホットラインへということで、御相談を受けるような形で対応しているところであります。

そして最後、一番下の関係業界への働きかけということで、何よりクレジットカードを提供していく事業者自身が過剰与信の防止に向けたさらなる自主的な取組を促すということでありますし、また当省といたしまして検査や監督を今年度重点的に強化していくということで、予定をしているところでございます。

次の課題でございますが、17ページ目を御覧ください。今度は個人情報保護への対応ということで、こちらも同じく４月から改正法の施行がされております。大変重要な情報について個人の権利を守るということで、大事な課題になってきております。

２つ目のポツに書いておりますように、クレジットカード番号は財産情報でございますので、１件でも漏えいしたら報告の対象ということで、個人情報保護委員会への報告を義務づけております。既に４月から施行されておりますが、様々な漏えいのきっかけがありますけれども、多くの漏えい事案の報告を受けているような状況でございます。

２つ目は越境移転への情報提供ということでございまして、海外に情報を移転する場合の対応についても新たな本人への説明責任等を課している状況でございます。

続きまして、19ページ目を御覧ください。今度はサイバーセキュリティへの対応ということで、後ほど本日の主題になってまいりますけれども、サイバーセキュリティについても現在、足下で政府全体の行動計画の改定が進行中でございます。

様々新たに求めていくことがありますが、特に１つ重要なことは右下の表に書いておりますように経営者自身がリスクマネジメント、セキュリティマネジメントをしっかりやっていく。体制を整えるということで、ＣＩＳＯなどしっかり経営陣に、そういった責任を担うポストを用意し、その人の下で体制を整えていくことも今後必要になっていくという

ことでございます。

さらに20ページ目でございますが、その延長で今後はさらに経済安全保障への対応ということで、重要インフラを担うクレジットカード決済事業のシステムについて、安全・安心な事業者から提供されているかどうか、システムの提供ベンダーや部品機器も含めた確認を取るということでございます。本件につきましては非常に重要なインフラに重点的に対象を絞って対応していくというのが今後の方針でございます。

それから、21ページ目でございます。今度はマネー・ローンダリング対策ということで、金融機関と同様にクレジットカード業についてもＦＡＴＦによる審査対象になっております。既に犯収法に基づく管理もこれまで行ってきておりますけれども、不正な取引を防いでいくことから継続的な顧客管理を強化していくことで、ガイドラインを改正するなどの対応を今取っております。

続きまして、22ページ目でございます。今度は今後の検討課題ということでございます。

23ページ目を御覧ください。現在皆様御案内のとおりＥＣ取引、それからキャッシュレス決済は右肩上がりの急成長を遂げておりまして、ちょうど昨日経産省から発表しておりますけれども、キャッシュレス決済についても、日本におきましてはついに３割を超えて32.5％に至っております。また、その中においてクレジットカードは引き続き約９割、大部分を占めるということでございます。

次の24ページ目を御覧ください。その一方でサイバー攻撃、それから消費者を狙ったフィッシング被害、サイバー上での犯罪も増加傾向というような状況でございます。

25ページ目を御覧ください。こういった背景の下で、結果といたしましてクレジットカードの不正利用被害額、これはＪＣＡ（日本クレジット協会）が毎年公表しているものでありますが、今年３月末に公表した昨年2021年のデータについては再び300億円を突破し、過去最高ということになっております。

経済産業省といたしましても、言わば非常事態だというような認識の下で、これまで以上に徹底的なセキュリティ対策を講じていく必要があると認識しております。

具体的な事例ということで、幾つか御紹介しております。

26ページ目でございます。こちらについては加盟店、特にオンライン上のＥＣ加盟店から漏えいする場合でございます。様々な背景、原因がありますけれども、特に目立つのはホームページやサイトを立ち上げたときに構築したソフトウェアを日々アップデートしていないことで、例えば２、３年前に構築したバージョンでずっと放置されていることで結

果的に古いバージョンになっていて、こういったアップデートされていないところに対して攻撃が仕掛けられることが最近見受けられます。

また27ページ目でございますが、他方でＥＣシステム提供会社ということで、加盟店の代わりにクラウド上でまとめてシステムを提供する会社も当然出てきております。こういった企業においてはより一段､二段高いセキュリティ対策を講じているわけでありますが、こういったところに対しても巧妙な攻撃が仕掛けられる。またこういった事業者においても、オープンソースなどを活用したソフトウェアにおいてアップデートを実は怠っているところがあったりして、結果的にこういったところが狙われますと加盟店一つ一つが狙われる以上に、ボリュームとしてどばっと情報が外へ出てしまうような大きなリスクを抱えております。

28ページ目であります。１つは決済代行業者ということで、これはアクワイアラーと加盟店の間に入って決済を代行する業者でありますけれども、こちらについても多くの情報漏えい事案があります。今年につきましても早速、年明けにメタップスペイメント社という決済代行業者から、当該企業発表では最大約46万件に達する可能性のある情報漏えい事案も起きておりまして、こういった決済代行業者に対する対応も重要になってきているかと思います。

もう１つ最後に、29ページ目でありますが、フィッシング被害ということでございまして、最後は消費者を直接狙ったメールやショートメッセージ、ＳＮＳなどを介して情報を窃取する、誤って誘導されて消費者が情報を入力してしまうような攻撃が昨今増えていることも確かでございます。

31ページ目であります｡このような被害に対応していくためにはクレジットカード業界、様々なプレイヤーが関わっておりますが、多様なプレイヤーが全体として総合的な対策を強化していく必要があるということであります。加えて左下の絵で申し上げますとカード会社と加盟店のみならず、これを結ぶＰＳＰ（決済代行業者）やＥＣシステム提供会社などの新しい、言わばサードパーティーのようなプレイヤーも含めて対策を強化していかなければいけないというような認識でございます。

32ページ目につきましては割販法による対応ということで、これまでもクレジットカード番号の取扱いから始まり、適切な安全管理措置を求める適用対象事業者を拡大するような、順次制度的な措置をやってきているところでもございます。

また、34ページ目でございます。クレジットカードのセキュリティガイドラインという

ことで、専門的、実務的なガイドライン、これは業界が必ず準拠しなければいけない指針でございますが、こういった技術的な要件をしっかり示して対策を取っているところでもございます。既に加盟店においては、クレジットカード情報の非保持化を促す、それから各プレイヤーにおきましては、国際的なデータセキュリティ基準でありますＰＣＩＤＳＳの準拠を求める、こういったこともやってきているところでございます。

しかしながら、35ページ目でございますが、結果として今300億円を超える被害を受けることを考えますと、これまで以上の対策を講じていかなければいけないのではないかというのが私ども事務局の考えでございます。つきましては、もちろん今日この後委員の先生方に御審議いただいて中身もきちんと踏まえた上で、より詳細な対応について検討してまいりたいと思っております。検討に当たりましては産構審の小委員会とは別に、経済産業省におきましてセキュリティに関する専門家の方々によります検討会を別途立ち上げまして、そこで年末に向けて検討を深め、その見解については改めて本小委員会に御報告させていただこうと思っている次第でございます。

最後、こういった方向を考えていく上で、資料２―２というのを用意しております。経済産業省のほうでまとめております対策の方向性でございます。

６ページ目を御覧ください。今後の対応策ということで将来に向かってやっていくという話で申し上げますと、大きく３つの方針で考えております。１つは、クレジットカードシステム全体のセキュリティ対策を底上げしていくということ。２つ目、黄色の部分で書いておりますが、仮に情報が漏えいした場合であっても、そういった情報が実際犯罪者に使われないように防いでいく。あるいは２次被害、３次被害を防いでいくような対応。最後には、取締りや消費者の方々も含めた自衛をしっかり徹底していく。こういう３本の方向性で考えたいと思っております。

紫の右上の部分にございますけれども、セキュリティにつきましてはＰＣＩＤＳＳ、国際基準が２年後には次の4.0の新しいバージョンに更新しなければいけませんので、こちらへの対応を促します。もう１つは加盟店、ＰＳＰにおけるＥＣサイトの更新に関わる脆弱性点検を徹底させたいと思っております。

それから真ん中でございますが、不正利用を防止していくことから本人確認の徹底ということでＥＭＶ３-Ｄセキュア、これも国際的なセキュリティ対策が求められているものでありますけれども、本人確認の徹底ということでワンタイムパスワード、あるいは生体認証等を組み合わせた、なりすまし防止のための対策を集中的に取り組んでいきたいと思

っております。またカード業界自身が共同して、不正利用防止システムを構築することについても促していきたいと思います。

最後、右下でございますが、経産省自身もＪＣＡ等、各業界とも連携いたしまして、捜査当局、治安当局である警察庁におきましては４月からサイバー警察局が立ち上がっておりますけれども、こういった関係機関との連携を強化して消費者の皆様への周知はもとより、犯罪の取締りに向けた対応をしっかり取っていきたいと考えているところでございます。

すみません、説明のほうは駆け足になりました。

最後、資料２―３を御覧ください。改めまして、本日御議論いただきたい事項でございます。

下の黄色で囲っているところでございますが、１つはセキュリティ対策ということで、クレジットカード番号等の適切な管理について求めるなど、これまで一定程度対策してきたところでございますけれども、今後どのような方向での対策が求められるか、どのような観点を強化すべきかについて御意見を頂戴したいと思います。

もう１つ､後半ではその他執行の強化ということでフィンテックの興隆等もありまして、クレジットカード決済はカード会社と加盟店間で多様な事業者や影響の大きい事業者が参加しております。業界がこのように複雑化していく中で、どのように実効的な監督を行っていくか。これらについても委員の皆様から御意見を賜れればと思っております。

事務局から説明は以上でございます。よろしくお願いいたします。

○岩原委員長　　どうもありがとうございました。

それでは、意見交換に入りたいと存じます。まずは御議論いただきたい事項の１つ目として、セキュリティ対策について委員の皆様から御質問や御意見をいただければと存じます。お一人５分以内を目安に御発言いただければ幸いです。また御発言の際は、Ｔｅａｍｓのメッセージ欄に発言希望等のメッセージを入れていただきたいと思います。私のほうから指名をさせていただきます。いかがでしょうか、沢田委員。

○沢田委員　　ありがとうございます。すみません、私のＴｅａｍｓのアプリにメッセージ機能が出てこないものですから、挙手させていただきました。

セキュリティ対策についてコメントさせてください。２本柱で、漏えいと不正利用対策が挙がっていると思います。私は不正利用対策の方に着目して発言いたします。

クレジットカードという切り口で見た場合、カード番号さえ悪用されなければ良いと思

いそうですが、加盟店の側から見ると、クレジットカード以外の決済手段も多数取り扱っています。もしカードで対策が行き届いて不正がしにくくなった場合には、他の決済手段に不正が流れていくのではないかという危惧を持っており、実際に後払い決済の悪用という事例も発生しているところです。カード決済だけきれいになっても駄目で、決済手段全体として考えなければいけないのではないかと思います。

その観点で２点、１点目は不正者が次にどこを狙ってくるか。その行動を予測するためには不正者のことを知らなければいけない。何よりも犯罪ですから法執行が必要です。警察やＪＣ３との連携をぜひ進めて、不正者を捕まえることも検討課題として挙げていただきたいと思います。そのためには不正者の特定につながるあらゆる情報を集約する必要があり、決済サービス事業者が有するものに加え、加盟店や物流業者のところにも断片的にですが不正者につながるいろいろな情報があるはずなので、それらを集約するための仕掛けをお考えいただきたいというのが１点です。

２点目ですが、法執行の目的に限らず、民間同士で情報共有することも十分考えられると思います。その場合、法執行についてもですが、個人情報保護法との関係を整理することが不可欠と思います。資料２―２の32ページあたりに書かれているように、不正検知の精度を向上させていくためには共同システムのようなものが有効と思います。33ページのマネロン対策のように法定化して、きちんとした形にできれば万全と思いますが、その前段階でもいろいろできることがあります。まずは顧客情報や個々の取引情報を不正検知に利用することに関し、誰がどのように利用目的などを本人に通知または公表するか、不正検知システムに第三者提供する場合には、どのタイミングで誰が本人の同意を得るかということを明確にする必要があると思います。不正検知の一環で外部データの活用が挙げられていましたが、現状そこに少し不安があるなと思っております。

もう一点、23ページにリスクベース認証に利用される情報のことが書かれています。具体的にはデバイスの情報、行動情報、属性情報などです。リスク度を判定するためには本人の情報を使わざるを得ないと思いますが、もしそのうち不正なケースだけを取り出して情報共有する場合には、それはカード会員の個人データではなく犯罪者の個人データに当たる。つまり本人同意の規律の外にあるという整理でいいのかどうか、そういったことを実態を踏まえて、個人情報保護委員会に解釈を示していただく必要があるのではないかというのが問題意識の２点目です。

以上でございます。

○岩原委員長　　ただいまの御意見についてでも結構ですし、他の点についてでも結構です。――池本委員、どうぞお願いします。

○池本委員　　池本でございます。

先ほど御報告いただいた中で、不正利用の前提となるカード番号情報の漏えい防止の観点で発言したいと思います。セキュリティ対策をいろいろ工夫しても、それをまた破る事業者が、不正利用が出てくるという問題もあるのですが、そもそもカード番号の非保持化対策とか、ＰＣＩＤＳＳ対策がちゃんとできている割合が今どのくらいになっているのか。あるいは、それをしているけれども破られて、さらにセキュリティのレベルを上げなければいけないのか。その辺りの具体的なデータも教えていただきたいところなのですが、どちらかというと、これは私の受け止めとしては、きちんと対策を取っていない加盟店などで、不正アクセスによってまとめて情報が取られている。それがあちこちへ流されて、不正利用になっていくということではないかと受け止めています。

だとすると、セキュリティのレベルを上げていく議論もさらに追求していただきたいのですが、むしろ加盟店にきちんと守らせるためのルールづくりです。経済産業省が直接全国の数百万ある加盟店に行政処分をすることは不可能なわけで、たしかアクワイアラーが加盟店に対する調査を行う、きちんとやっていなければ加盟店契約の解除も含めた、加盟店の調査・管理の中で実効性を確保するというルールだったと思います。

ただ、言わばお客さんに対してどこまでできるかという問題が出てくるのですが、私はその中でセキュリティ対策を講じていないがために情報漏えいになった場合は、その責任を加盟店がちゃんと負担するのだというところのルールをもっと見える化していただく必要があるのではないかと考えます。

というのは、弁護士のところへの相談、あるいは消費生活センターへの相談などで情報を聞いているところでは、カード会社は不正利用の問題については相変わらずカードの紛失・盗難における60日ルール。警察へ届けて60日以内のものは保険でカバーするけれども、それ以降は御本人の負担ですよと。基本的に、これを形式的に当てはめてしまっているケースを複数聞いています。もともと物理的なカードを持っている人が紛失したり、盗難にあったり、ある意味では気づくきっかけがある場合の対処の問題ですが、どこかでハッキングされたというのは、全く関係がないところである日情報が漏えいされ、ある日不正利用が始まる。しかも今は利用明細書も、あるいは銀行の口座もみんな電子化して、オンラインで自分で見なさいとなっているので、３か月も４か月も遅れて気づく人が増えている

ということを相談員などからも聞きます。

むしろハッキングによって取られて不正利用されるというのは、出発点で消費者には落ち度はないわけですから、セキュリティ対策を講じていない加盟店が責任を負うという、このルールをきちんと見える化して、そこをルールとして明確化する。そうして初めて加盟店は自分が損失負担するわけにいかないから、ルールを守る対策が必要なのだということの動機づけになるのではないかと考えます。ぜひその辺りも含めたセキュリティ対策の実効性確保の方策も、検討していただきたいと思います。

あと最後ですがＥＣモールとか、ＱＲコード決済業者とか、あるいは加盟店から委託を受けて決済処理をするところになると、アクワイアラーが監督する立場にないものと、アクワイアラーと加盟店関係があるものと違いが出てくると思います。その辺りが、誰が責任を持って監視していくのかということをルールの中でもっと見える化していただく必要があるのかなと考えます。

以上です。

○池原委員長　　岩下委員、どうぞ。

○岩下委員　　岩下でございます。コメントを述べさせていただきます。

今回の議論というのは大変ホットなトピックであって、かつ資料２―１の25ページにあるとおり、クレジットカードの不正利用被害といっても94.4％はカードそのものではなくてカード番号ですので、クレジットカード番号の不正利用被害額と言うべきなのだと思うのですが、それが実に330億を超えているという。この点からまず議論を出発するべきだと思います。

ＥＣ事業者さん、あるいはカードホルダーである一般の消費者個人の方々、それぞれの事情というのもよく分かるのですけれども、しかもここ数年、2017年以降ずっと200億超えですよね。かつて1990年代とかにかなり増えて幾つか波がありますが、私、そういうときに対策を講じる側におりましたのでいろいろ議論させていただいたわけです。

そのときにすごく思ったのは、もう既にクレジットカード番号を盗用する犯罪産業になっているわけです。毎年毎年300億からの売上げが上がるわけですから、犯罪者にとっては、もうこれをやるのがビジネスになってしまっているわけです。ということは犯罪者集団に対して、毎年毎年300億の資金を一般の消費者が負担する費用によって供出しているようなものであります。組織的な犯罪に対して、これを撲滅しなくてはいけないという社会の正義という観点からすると、こういうことがまかり通っているのは大変嘆かわしいことだ

と私は思います。

なぜこれがまかり通ってしまっているのかということなのですけれども、似たような事件で、例えば2003年、2004年ぐらいに大きな問題となった偽造キャッシュカード事件というのが、これは銀行のキャッシュカードの問題としてありました。あるいは比較的最近ですと2017年、2018年ぐらいでしょうか。セブンペイ問題とか、ドコモ口座問題とかです。そういう問題がいろいろ発生して耳目を騒がせたわけであります。

ただ、これらの犯罪による被害額というのは、たかだかというと怒られてしまいますが、2003年とか2004年の偽造カード被害は10億円に達しない程度でございました。ドコモ口座や、あるいはセブンペイ事件における被害額というのも多分１億に達しないくらいの規模なので、世の中を騒がしている割には被害の金額は少ない。かたがた、毎年300億の被害が出ていることに対してなぜ騒がれないかというと、犬が人をかんだ的な話になってしまっているところもあるのですが、これに対して消費者が何ら痛痒を感じないというとちょっと言葉が過ぎると思いますけれども、実際に不正被害に遭った人は、事情によっては個人負担を求められるようなケースも起こり得るという意味で、そこに注意しなくてはいけないところがあるわけですが、基本的には保険でカバーされているので、クレジットカードの不正利用があっても、クレジットカード会社が取引自体をなかったことにしますみたいなことで、個人の消費者にとっては事実上負担はないわけです。

結果として何が起こるかというと、個人の消費者のクレジットカード番号のハンドリングが極めて甘い。普通のプレーンなメールや、プレーンなWebベースのＥＣサイトに対して、そのままＣＶＶまでそっくり入れて、はい、どうぞとやるようなケースというのが多数見受けられます。個人がそういうことをやっていること自体、こういう被害が生まれていて、それが個人の被害ではなくて保険会社からの支払いになるわけです。実は通してみればクレジットカードの決済費用の中にかかっている、多分１％ぐらいの保険料が結果として割り当てられているわけです。言ってみればクレジットカードで買い物をする人はみんな１％ぐらいの費用を持って、その費用が犯罪者集団に献金されるみたいな、そういう仕組みになってしまっているわけです。これを何とかしないといけない。

３-Ｄセキュアの話が途中で時々出てきましたけれども、今のＥＣサイトは余りにセキュリティが甘過ぎるし、それに対して消費者も唯々諾々とプレーンなクレジットカード番号を入れてしまうという問題があるわけで、そこの構造を抜本的に変えていかないといけないというのは、知っている人はみんな分かっているわけです。

ところが、実際にはなかなかできない。クレジットカード決済をしたい人たちはとにかく番号が欲しいので、番号をどんどん入れてくださいという形で、全然セキュリティが担保されないような仕組みで使っているケースが非常に多い。この状況がある限りは、もちろんフィッシング等で個人が盗まれてしまうケースもあるでしょうけれども、複数のプレーンなデータで決済できてしまう構造自体がそもそもおかしいのであって、我々は何のためにクレジットカードにＩＣカードを入れて、ＥＭＶの規格をつくり、その中にＲＳＡ署名のための秘密鍵を格納しているかを考えると、何とも情けない状況になっています。この状況を何とか抜本的に変えていただきたいというのが､私が一番申し上げたいことです。

これに関連して、例えば先ほど挙げた偽造カードの問題については、その後ずっと金融庁で偽造カード犯罪等の被害額の対応。どういう手口で、どういう解決がなされたかというのを業態別に全部開示しています。

ところが、クレジットカードの不正被害については何かぼーんとクレジット協会さんが被害総額を出すだけで、中身が全然分からないのです。もちろんオンラインとか、国内・国外ぐらいの差はあるのですけれども、それ以上のことは全然分からないし、どんなカード会社が、どんな決済代行会社がやっているのか。今みたいな複雑化した仕組みの中で原因究明をしながら、その改善を図っていくことは非常に大事なので、そういったマクロの情報をきちんと出していただいて、どこに手を打てばいいのかをきちんと考えていくことが必要だと思います。

私からは以上です。

○岩原委員長　　ありがとうございました。

田中委員、お願いいたします。

○田中委員　　私からは、先ほど資料２―２で大きく３分類で対策をされているというお話がありましたので、それぞれに沿ってコメントさせていただければと思います。

まず漏えい対策のところなのですけれども、１つは、特に中小なのかなと思いますが、ＥＣサイトでパッケージの仕組みなどを使ってセキュリティ対応が取られていない。そういうところから抜けていますねというお話で、例えばクレジットカード・セキュリティガイドラインなどでも対策を講じるところで、加盟店になるときにセキュリティ対策を申告してもらうみたいなお話が上がっているように認識していますけれども、それで十分なのかというところは懸念があるかなと思っています。そもそもセキュリティに対する認識が低い方々に自己申告でチェックしろといっても、そこで十分な対策が取られるとは、なか

なか期待できないのではないかと思っております。そうすると、そこに対してアクワイアラーなり、ＰＳＰなりがもう少しきちんとチェックをすることが、どうしても必要になってくるのではないかと思いますというのが１点。

その上で、漏えいしても不正に使えないような対策みたいなことを、もう少しきちんと取っていくべきではないかと思っております。今もう一部のカード会社で提供されていると思いますが、ＥＣやリカーリングの取引などで、セキュリティコードやカード番号16桁そのものをワンタイムで使っていくような形で、サービスの提供をするようなものが実質的には実現しているところで､そういうものをＥＣサイトに登録する場合､あるいは電気、ガス、水道みたいなところに登録するときに、そういうものを使って、たとえ漏えいしたとしても、ほかの場所では使えないみたいな構造をきちっとつくっていくことをしたほうが、結果的に対策にとしては有効なのではないかという気がしています。

もう１つ、ちょっと後で森竹委員のお話もぜひお伺いしたいですけれども、先ほど池本先生からは、対策がちゃんとできていないところから漏れているのが多いのではないかというお話がありましたが、一方で先ほど事務局から御説明があったＰＳＰの事例などは、当然ＰＣＩＤＳＳが取れているところから漏れている。ＰＣＩＤＳＳの認定のところでＱＳＡがチェックしているときに、企業と会計監査する監査法人との関係に似ていて、監査とかチェックをしなければいけないわけですけれども、そのための費用はチェックする相手からいただいているという構造があるので、そうするとＱＳＡのモラルと言うとちょっと失礼なのかもしれませんけれども、ビジネスの態度によっては、甘い判断が出てきたりということがあるのではないかという懸念がちょっとしています。そういったところも含めてきちんと対応していく、チェックしていくみたいなことが必要なのかなと感じております。

２番目の不正利用防止とされているところは、特にフィッシングにどう対応していくかというところで、事務局の御説明でもいろいろな周知をされているところなのですけれども、これに関して言うと岩下先生のお話にありましたけれども、どのぐらい本当に消費者が認識していて、気をつけているのかというところを、きちんとチェックしていかないといけないのではないかと思っています。

相手､不正をする側のフィッシングメールも年々巧妙になってきていて､私の周りでも、ついうっかり引っかかってしまったという人がいるぐらい、もうぱっと見て判断するのはなかなか難しい状況まで来ていると思いますが、その上で消費者の方々がちゃんとそうい

うことがあると判断するには、見分けるにはどうしたらいいかをちゃんと認識していただく必要があって、それが本当に浸透しているのかというところを確認していかないといけないのかなと思っています。

あと不正利用の対策というところで、これはもうＥＭＶ３-Ｄセキュアをきちんと入れていくことになると思っておりますが、大きな変更点として、リスクベースでの対応になっていくところが目玉としてあると思うのです。リスクベースを運用するのは、要は個々のカード会社に委ねられることになりますと、リスクの判断のレベルみたいなものが、当然イシュアーによって違ってくるみたいなことが懸念としては起こり得るのかなと思っておりまして、そうすると弱いところが狙われるみたいなことになりかねないので、そういう意味でも業界で連携して情報共有するみたいなところを、きちんとやっていく必要があるのではないかと思っております。

私からは以上になります。

○岩原委員長　　どうもありがとうございました。

次に、二村委員、お願いいたします。

○二村委員　　ありがとうございます。

私の発言は田中委員ともちょっと重なる部分がございますが､まず今回セキュリティで、データセキュリティと不正利用対策というところを取り上げていただいたことに関しては、非常に重要なポイントかと思っております。データセキュリティ自体は300億を超える不正利用が起きて、何と特殊詐欺の年間の被害金額より多いわけです。警察があれだけ動いている特殊詐欺より多いのに、こんなにのほほんとしていいのかということがまず当然出てきますから、それは相当力を入れてやらないといけない。それをやるに当たっては、データセキュリティと不正利用対策という２本柱が必要だということは明らかだと思います。ただ、この２つはどう動くかということが全く違うものだと思っております。

まずデータセキュリティなのですが、これに関しては不正利用対策だけでなくて、ちょっと大げさに言うと経済安全保障的な観点。つまりデータ改ざん等が行われないようにということも含めて、対策を取っていかないといけない。キャッシュレスが３割を超え、４割を目指していきますと言っているときに、なおかつ、それが個人に一番近いネットワークでデータセキュリティが確保されないことになると、言わばそこがウイークリンクになって、国民経済に対してマイナスインパクトが大きい状態が生まれてしまうことが懸念されますから、ただ単に不正利用対策でデータセキュリティですというだけでない視点で、

もう少し発信していただいたほうがよろしかろうと思っております。

その上で、では何をやるのだということに関して言うと、もう既にルールベースでもはっきりしているはずなのです。ＰＣＩＤＳＳをやりますということをセキュリティガイドラインでは言っていて、それを皆さん守りますと言っているはずです。ＰＣＩＤＳＳ自体はその時々にアップデートしていって技術水準等を追っかけているもののはずですから、これを皆さんがちゃんとやっていれば、こんなに抜かれることは少なくとも事業者サイドから起きないはずなのです。

なおかつ、クレジットカードというのはカード番号という生のものを流通させてしまっていますから、それをワンスで使うようなＩＤに変えないで、そのまま番号を送ってしまっているので、盗み出すポイントがいっぱいあるわけです。ポイントがいっぱいあって、しかも個人の方もいるから、セキュリティをどうやって守ろうとしても難しいのだけれども、少なくとも事業者サイドはＰＣＩＤＳＳがあるはずなのに、なぜこれができていないのですかというところを問わないといけない。

その要素の１つは、申し訳ない、テストなり検証という機能が弱いのではなかろうか。そこのところをどう改善していくかという目線を持たないと、データセキュリティに関しては、ルールを幾らいじっても変わらんのではないかということを危惧しております。

そういう意味では、認証機関の果たしていただく役割。森竹さんのところのお役目が非常に大きいだろうというのと同時に、うまくいった事例、悪かった事例というものの共有化などによって、自己改善機能を各事業者が発揮できるようにしていく。その仲立ちを行政なりがやっていく。あるいはクレジット協会なり、業界団体がやっていくという思考が必要ではないかなと思っております。

２点目、不正利用対策ということですが、不正利用に関して言うと、今回カード情報が不正利用ですということでフォーカスされているのですが、この構造はもう前から変わっていないわけです。

なぜ起きるかと言ってしまえば、これは単純な話で、低い水準から始めてしまったからです。リアルなカードに関しては低い水準であったけれども、その時々でセキュリティ対策をちょこちょこ入れていったのだけれども、残念ながらＳＥＴも失敗して、最初はもう平文でカード番号を流しますなんていう。とんでもないところから始めてしまったわけです。低いところでできる事業者さん。特にマーチャントサイドにとっては、それでいいじゃないか、不利益ないじゃないかということで動いてしまったものだから、今３-Dセキュ

アを入れるのにこれだけ苦労してしまっています。３-Ｄセキュアを入れるのに苦労しているがゆえに、それこそＥＭＶ３-Ｄセキュアではなくて、1.0すら全く普及していない。この状態でやりましょうといっても、加盟店さんは負担が気になりますからそうはやりたくないわけです。ここは恐らくルールの中できちっとこれをやれというのを入れていかないと、もう動かないだろうと思っています。

ただ、そのときも、ではどうやってやるのか、誰の負担でやるのかというところを詰めないと、やれと言ったところでそっぽを向いてしまうということが危惧されていて、ここはもう法律で義務づけるしかないだろうと思っております。

さらにその部分に関連してですけれども、ＥＭＶ３-Ｄセキュアなどで購入者情報。沢田さんが先ほど御指摘になっていましたが、不正利用した者の情報なのか、購入者情報なのか。そういうものをカード会社側にも流通させることによって、あるいは各カード会社で不正利用情報を共同利用することによってという構想があるわけですが、これを実現しようとしても、個人情報保護法の壁が高くてずっとできていないわけです。そういう意味では情報交流のために必要な法整備もやっていただくことが必要ではないかと、このように思っております。

○岩原委員長　　森竹委員、お願いいたします。

○森竹委員　　私のほうも今後の方向性というところでは、この３つの視点というのはすごくいい考えだと考えております。

まず１つ目の漏えい防止というところなのですが、現状クレジットカード情報、決済するというシステムが多数ございますので、やはりＰＣＩＤＳＳ等の準拠をしていく、ガイドラインに従っていくという対応が必要かと思っております。

ただ、昨今のカード情報が漏えいするところでとても残念に思うのは、ＰＣＩＤＳＳを準拠していたにもかかわらず漏えいしていますというところについてなのですけれども、そこについての原因が、例えば不正アクセスがありましたということは公開情報として掲載されているのですけれども、そもそも論の、それが本当にＰＣＩＤＳＳの準拠評価のスコープに入っていたのかどうか。そこのスコープ決めのところが私は一番重要だと思っているので、漏えいしたところが準拠範囲にもし入っていたのだとすれば、もしかしたらサンプリングの課題だったかもしれないですし、あと検証の深さだったかもしれない。そもそもそこがスコープにちゃんと入っているか。一番最初のＰＣＩＤＳＳの準拠範囲決めのスタートがどうだったかというところがすごく気になっておりますので、漏えい事案が出

た場合には公開するのが難しい事情も十分分かってはいるのですけれども、そういった情報もあると、それを基にほかの会社さんも自分たちが対策を打つべきこととか、予防措置といったこともできるのではないかなと考えております。

２点目なのですけれども、やはり漏えいは起きてしまう。もちろん防止しなければいけないですけれども、その被害をいかに防ぐか、不正利用を防止していくというところで、３-Dセキュアといったところの浸透がますます必要であると私も考えております。

あとほかの委員の皆様からもお話がございましたが、消費者の皆様がインターネットでいろいろ個人情報を含めてクレジットカード情報を入力する際に、セキュアなＨＴＴＰの通信かどうか。そういったところに気づけるかということも重要かと思いますので、ますます消費者の皆様が理解できるような、すごく分かりやすいようなアプローチも必要かなと思っております。

私からは以上となります。

○岩原委員長　　藤原委員、お願いします。

○藤原委員　　ありがとうございます。ほかの委員の方々の御発言と重なる部分もありますけれども、お許しください。

まず、もはやクレジットカード、あるいはクレジットシステムは社会インフラである。いわゆるマルチステークホルダーをもって語らなければならないわけで、まさしく国際ブランドには国際ブランド的なことをやっていただくことから始まり、第三者認証機関もあるでしょうし、さらに言えば消費者には消費者契約ということで、多様なプレイヤーの役割の整理もここに書いてあるとおりです。

では現状については、例えばクレジット協会のセキュリティガイドラインの第３版で新たにやるべきことが、２版からこういうことが変わりますという。対象等変わっておりますけれども、そこに既に問題は表れているわけで、全て徹底するというと、まさしく多様な業者の全てがついてこられないということで協会も非常に苦労しておられるのでしょうけれども、それを何とか打破しなければならない。

今のが前提で、そうしますと何がいいのかといいますと、私の思うに皆さんと重複しないように言うと、１つは座長の御専門であるところでよく言われるコーポレートガバナンス・コードとスチュワードシップ・コードですけれども、ソフトローとハードロー、ある程度組合せでいくしかないのかなと。つまりこうやってくださいと、できないのなら説明してくださいという手法もある程度考えてもいいのかなと。一般論ですけれども、そうい

うこともあり得るのかなと思っております。

もう１つは情報の世界ですけれども、技術でできることは技術でというのが鉄則ですので、例えば今いろいろなセキュリティの手法が出ています。しかしながら、キャッシュレスの世界の新たなプレイヤーなどを見ていると、結構細かなセキュリティ対策はモバイルであるがゆえにやっていて結構進んでいたりしますので、それもちゃんと学習する必要があるのかなと。

なぜかというと、そもそも以前より16桁の番号と有効期限と、さらにセキュリティコードと組み合わせてやっていくという日本的な手法。クレジットの世界の手法が本当にどこまで機能しているのか、どこまで必要なのかという議論は事故、事件が起きるたびに言われてきたわけで、先ほどワンタイムパスワードのお話も出ましたけれども、この辺りも技術でできることは、新たな技術として見直したほうがいいのかなという気がいたします。これが２つ目です。

あとデータセキュリティ等の問題が出ましたけれども、この辺りに関しては逆に、まずは一般的に公表したデータでは取りにくいと思いますが、協会とか、先ほど申し上げたようなスタークホルダーのところに情報は蓄積しているはずなので、そこを正確に取って分析するところから、もうやっておられるのかもしれませんけれども始めたほうがいいし、あるいは業界側も、ＭＥＴＩに対して情報を出し惜しみすることによって結局跳ね返ってきて、あとコストがかかるという話になると思いますので、その辺りの情報共有は積極的に進めていただいたほうがいいと思います。

あとは皆様方がおっしゃったとおりですので、私が申し上げたかったのは以上のようなことでございます。

○岩原委員長　　どうもありがとうございました。

各委員から一応御発言いただいたようですが、ほかに特に御発言ございませんでしょうか。長谷川委員、何か御発言ございますでしょうか。

○長谷川委員　　長谷川です。

私は消費生活センターで相談員をしておりますので、消費者の方から御相談を受けているのですけれども、消費者の方はネットリテラシーはとても低いという傾向にあります。例えばネットでぽちっとして申込みはできても、解約ができない。それでトラブルになっているという方はとても多いです。

今はインターネット通販の詐欺サイトですとか、フィッシングメールがとても多くなっ

ておりまして、ＳＮＳなどの広告から飛んだサイトですとか、商品名で検索して出てきたサイト。詐欺サイトがとても多くなっているのですけれども、クレジットカード番号を入力させるようなサイトが最近はあります。商品が届かないですとか、メールをしても返信がないということで御相談が入るのですけれども、そのようなサイトは個人情報ですとかカード番号を収集して、不正利用などに使われている可能性が高いのかなと思います。

あとフィッシングメールですけれども、私もＮＡＣＳの活動でグループメールを使っていまして、それはＮＡＣＳのホームページで公開されているのですが、そのメールアドレスにはカード会社ですとか、通販モール、あと銀行などを騙ったフィッシングメールがとても多く入ってきます。内容を読みますと不正なアクセスがありましたですとか、消費者を焦らせるような内容になっていまして、本物と同じようなロゴを使っていますので、消費者が間違えて入力してもしようがないかなというような巧みなものが最近は出ています。

フィッシングメールからＵＲＬにアクセスして、ＩＤやパスワードを入力して、カード番号などを不正に取られてしまうというケースですが、入力した消費者の方はフィッシングメールだと気づいていないので、不正利用されて大分たってから気づくというケースが多いです。

先ほど池本先生がおっしゃっていたように、今はカードの利用明細も紙ではなくオンラインで、自分でカード会社のサイトにアクセスするですとか、アプリにアクセスしないと見られない状況ですので、カード明細を確認していない消費者というのはとても多くなっています。気づいたときにはもうカード会社の補償できる期間を過ぎてしまっていて、補償が受けられないというケースが多々あります。

カード会社から請求金額が確定しましたというメールが届きますけれども、そこには合計金額などが記載されている事業者さんもありますし、記載されていない事業者さんもありますので、金額だけでも書いてあると自分が使ったよりも多いなということで、気づく可能性もあるのではないかと思っています。

あとＥＣサイトなどで、購入者の名義とクレジットカードの名義が違っていても利用できるサイトがありますので、どのような仕組みができるのか分からないですけれども、購入者名義とクレジットカードの名義が異なる場合は利用できないなどの対策ができればよいかなと思います。

あとは消費者教育も必要だと思いますので、安易にクレジットカード番号をサイトに入力しないですとか、カードの明細は頻繁に見ましょうというような啓発が必要だと思いま

す。

以上です。

○岩原委員長　　各委員から御発言いただきましたが、なお御指摘いただくことがあれば追加していただきたいと思いますが、いかがでしょうか。――よろしいですか。

特に追加の御発言がないようでございましたら、次のテーマに移りたいと思います。御議論いただきたい事項の２つ目といたしまして、その他執行の強化について、委員の皆様から御質問や御意見があればいただきたいと思います。お一人３分以内を目安に御発言いただければと思います。どうぞよろしくお願いします。いかがでしょうか。――池本委員、よろしくお願いします。

○池本委員　　ありがとうございます。

執行の問題としては、平成28年改正で入ったアクワイアラーの加盟店調査義務に関連して２点申し上げたいと思います。

国際ブランドを経由して、イシュアーとアクワイアラーの役割分担がある。そういう中で実効性ある加盟店調査を、あるいは苦情処理をするためにイシュアーについては苦情の伝達義務、アクワイアラーについては加盟店調査義務という形で非常に具体的に記述した点は、様々なキャッシュレス決済の中では一番進んでいるものだと思います。

ただ、海外アクワイアラー、あるいは海外決済代行業者経由で日本国内の加盟店がつながっているところは、無登録業者排除の問題は事務局の資料にも出ていましたが、現場で弁護団、あるいは消費生活センターの相談事例なども聞いてみると、これはまだまだたくさんあります。法律上は罰則で対処することしかなくて、先ほどの話では個別にアプローチして注意喚起をするという。結局指導ベースのことで、罰則対象の違法な業者に行政処分をするのは屋上屋を重ねるというのか、種類が違うのかもしれませんが、やはりもっとルールを明確化して、執行の手段として加えていく必要があるのではないか。金融商品取引の分野などでは無登録業者に対して行政庁がさらに排除するというルールがあるやに聞いていますし、海外アクワイアラーに関しては、国際ブランドを通じて排除に向けた是正の指導をしてもらうことが当時議論されたのですが、それがどの程度実行されているのか、あるいはできていないのかという辺りは、さらに整理していただく必要があると思います。

もう１点は、マンスリークリア取引についてアクワイアラーは、それも加盟店調査の対象になっていますが、イシュアーについては従来の包括信用購入あっせん業者にとどまっている。相談現場の話、あるいは弁護団の話からも、クレジット会社の中でもきちんと自

主的なルールに沿って２か月を超えるものに準拠して苦情の伝達処理をしておられるところと、ほとんどやっていただけていない事業者の色分けが随分大きくなっていることを複数聞いております。そういった辺りは、場合によっては国民生活センターなりを通じて実態把握した情報を共有して、もっとルールを明確化していただきたい。施行から間もなく12月には５年になります。その辺りの実施状況を見て、場合によってはイシュアーについての法的な義務が必要なのかどうか。そういう議論も必要な時期に来ているのではないかと思います。

以上、２点です。

○岩原委員長　　岩下委員、お願いします。

○岩下委員　　つい最近、世間の耳目を騒がせた山口県阿武町の誤送金事件がございました。あの事件で何が明らかになったかというと、それを使ってしまった個人の人はともかくとして、日本国内には決済代行業者なる人たちがいて、その人たちを経由すれば4,000万円なるお金を、あっという間に海外の実質的な違法性のある、非常にグレーなサイトに送金してしまうことができると白日の下にさらされたわけです。同じ手法はマネー・ローンダリングであるとか、様々なことに明らかに利用可能なのであって、こういう仕組みが現在存在していることは、もちろんその部分については銀行からの送金によってなのだと思いますけれども、そこから先については決済代行業者というのが、例えばクレジットカードやデビットカードの決済であったという話を聞きますので、そういう意味において現在のクレジットカードの仕組みというのは、基本的にクレジットカード会社、主としてアクワイアラーを担う人が加盟店について信用度であるとか、不正な行為をしていないことをきちんとチェックして、その人たちにクレジットカードという業務を担わせる。本当はそういうものが一番オリジン、基礎にあったのだと思います。

しかし､今や決済代行業者を通してしまえば､そこから先の事業者が何をやっていても、決済代行業者の判断によって担われることになってしまいますので、実質的にクレジットカード会社の加盟店の管理というものが全く行き届かないことになってしまうわけで、逆に言うと、そういう管理が行き届かないことが嫌だというのであれば、そもそも決済代行業者を経由した決済などを認めないことが本来の筋だと私は思いますが、そのようにはなっていないわけです。

そういう意味で非常に複雑化した仕組みの中で、どうやって全体の健全性を保つか。決済代行業者自体は、たしか金融庁の登録になっていると思いますけれども、そういうこと

も含めて全体としての枠組みをチェックして、違法なこと、あるいはそれに類すること、マネー・ローンダリング等の問題の発生をどうやって防ぐかということについてしっかり考える仕組みというものは､多分省庁をまたいだ形で対応が必要になるだろうと思います。その意味で現在のクレジットカードを、かつての百貨店会というところの延長線として業界を指導している枠組み自体がもう古いのであって、新しい仕組みに行政の仕組みのほうが対応できていないのは明らかであって、それを変えていくことが直ちに必要であろうと思います。

私からは以上です。

○岩原委員長　　二村委員、お願いします。

○二村委員　　ありがとうございます。

特に私は、海外アクワイアラー問題について一言申し上げたいと思います。海外アクワイアラーについては平成28年改正の当委員会での審議のときにも、どうやって登録を受けていないものであるかを見破るのかという話が出て、その際に私からは各マーチャントにどの業者と加盟店契約を締結しているかを、特に通信販売については、特商法の中で表示義務の１項目として課せばよろしいのではないかと。そうすればどこと契約しているかを登録事業者と突合することによって、無登録業者と契約しているかどうかがすぐ分かる状態がつくれるのではないかということを申し上げましたが、残念ながらマーチャントにとっての負担が大き過ぎるのではないかという御意見もいただき、その案は通らなかった。その時点から、もうこれは予想された状態だと私は思っております。

ですから改めて１つは、加盟店がどこと加盟店契約を結んでいるかという単純な一言だけでも表示をする。もう１つは、加盟店に登録事業者との契約の確認を義務づけることがよろしいのではないか。行政が幾らやれと言ったって分からなければやりようがない、動けない。知るということがまず第一で、知るためには当事者間の契約の中身を外からじっと見たって分かるわけがないので、表示をさせるしかない。もう単純明快だと思っています。

○岩原委員長　　田中委員、お願いします。

○田中委員　　私からは今の皆様のお話ともつながるところであるのですけれども、先ほども申し上げましたが中小のＥＣサイトであったり、あるいは消費者であったりといった人たちに、自主的にガイドラインを調べたりとか、あるいは不正に対してどういう対策が取れるかを知るように動いてもらうことを期待すること自体が、そもそもナンセンスでは

ないかと思っています。

今いろいろな周知・広報も含め対策を打たれていて、そこにものすごいリソースがかかっていることに関しては非常に頭が下がる思いであるのですけれども、周知・広報するのであれば、さらに先ほど学校にパンフレットを配るみたいな話もありましたが、配るだけでは読まないですよね。配った上でちゃんと授業の中で扱っていただくみたいなところまで踏み込むですとか、今の二村先生の加盟店側に表示を義務づけるにしても、そんなことを加盟店は知り得ない、知らないと思いますので、義務づけていることをちゃんとアクワイアラーなり、ＰＳＰなりに確認させることを、アクワイアラー、ＰＳＰにも義務づけるというところでセットでやっていかないと、なかなか実効性のあるものにならないのではないかと思います。

その上で、では実際に消費者としてフィッシング対策をどうしたらよいかみたいなところは、どのぐらい本当に消費者の方が認識しているのか、あるいは加盟店の人たちが守らなければいけないガイドラインを、どのぐらいちゃんと認識しているのか、みたいなところを、追跡的に調査していくみたいなことをきちんとやって、いろいろな施策がどのぐらいちゃんと実効性が出ているのかというところを評価しながらやっていく取組が必要なのではないかと思います。

○岩原委員長　　ほかに御意見ございませんでしょうか。沢田委員。

○沢田委員　　ありがとうございます。先生方がおっしゃること、そのとおりと思いながら伺っておりました。

岩下先生がおっしゃった省庁をまたがっての検討でないと無理ではないかというのは、私も全くそう思います。先ほど申し上げたこととも関係するのですが、クレジットカード決済だけ取り出して規制して監督してというのが余り現実的ではなくなっている。海外事業者のことを考えても、やはり決済全体の健全性を保つためにどこがウイークポイントになっているか関係者が共通認識を持つ必要があると思うので、クレジットカードだけを取り出してというのは、ちょっと無理があるなと思います。

今までのクレジットカードでのやり方は、アクワイアラーとＰＳＰの加盟店調査にかなり依拠していて、その方法をほかの決済手段にも広げようという話もあったかと思いますが、限界に来ているところもあるように思い、何か答えがあるわけではなくて恐縮ですが、少し別の形を考えないといけないのかなと思ったりしております。

二村先生がおっしゃった表示義務を課すという件も、確かに加盟店の負担が大きいとい

うことで以前は自分も反対したように思いますが、もし本当に登録していない決済代行会社を通じた取引でものすごく悪いことが起こっているとしたら、そういう方策も考えなければいけないかなと思いつつあります。ただ、現実に今どのくらいのインパクトか分からないので、全体の中でそこに注力すべきかどうかはまだ判断できないかなと思っております。

ＥＣ加盟店の立場からしますと、意外と決めてくれれば言うことを聞くというか、漏えい対策はコストになるのでいろいろな受け止め方があると思いますが、不正利用対策に関しては、やらないと代金が返ってこないという形で自分が損をすることになりますので、インセンティブは結構働くのではないかと思います。

確かに最初はすごくゆるゆるのところから始まったかもしれないですが、前々回改正で課された非保持・非通過化はかなり浸透しているように思います。最初はセキュリティコードもなしで決済が通っていたところも、だんだんと改善されてきていますので、行政的な、法律による方向づけはそこそこ有効なのではないかと思います。

すみません、話が戻ってしまいましたけれども、以上です。

○岩原委員長　　長谷川委員、お願いします。

○長谷川委員　　ありがとうございます。

恐らく海外の決済代行会社ですとか、登録していない決済代行業者が関わっているかと思うのですけれども､サクラサイトですとか､情報商材の被害がとても多くなっています。返金を求めて消費者センターがあっせん交渉することがあるのですけれども、大体決済代行業者さんとお話しすることが多いです。その先の加盟店であるサクラサイトですとか、情報商材事業者の実態は不明で交渉の場には出てこないことが多いです。あっせん途中でやり取りをしている決済代行業者も変わったりするので、複数の業者が間に入っているかと思われます。

消費者センターとしては返金してもらうのが第一ですので、どのような事業者さんが間に入っているのかという関連性を聞いたことはないですけれども、恐らく無登録の決済代行業者などが入っているかと思いますので、そういうところが関わらないような対策をしていただければと思います。

以上です。

○岩原委員長　　藤原委員、お願いします。

○藤原委員　　一言だけ申し上げます。執行ですけれども、これは本論から外れますが先

ほど田中委員からお話のあった、いつ誰にやれば実効的かというものは他の分野でも議論していまして、例えば携帯を持つ、持たない。携帯の危険性などというのは御父兄が来る入学式、卒業式といったときこそがチャンスだと言われていますし、こういう事業者を集めるのだったら、事業者の横のネットワークの大会であるとか、あるいは税務が関連しているときに言うとか、そういうお話があるわけです。

それは本筋からそれますので執行一般のことを申し上げますと、海外ブランドとか、あるいは詐欺案件等の執行となりますと、従来の我が国の行政執行というのは、ある意味で言うと行政指導ベースでやってきたところがありますので、経産省が行政指導ベースでやってできるところと、まさしくサイバーセキュリティ基本法に出てくるように、各省庁の連携でやらないと無理なところと両方ありますので、これまで連携がなかなかできなかった部分については、まさしく社会インフラだ、重要インフラだという観点から積極的に働きかける。御苦労ですけれども、働きかけていただくのが一番いいのかなという気がします。

あと行政指導ベースのところは、いわゆる情報の活用です。公表でありますとか、そういう政策をどう組み合わせていくのかという話で、より実効性のある方向に持っていくしかないのかなという感じがしております。

以上です。

○岩原委員長　　森竹委員、お願いします。

○森竹委員　　私のほうはまた先ほどの話とつながってしまうのですけれども、今回御提示いただいております資料２―２のところで関係行政機関、サイバーセキュリティ対策関係の連携強化の２ページ。58ページ、59ページなのですけれども、今回赤字の部分で強化と記述のあるところについての情報が今後より一層公開されて取組強化がなされていくのかなと､大変期待しておりますというところでコメントとさせていただきたいと思います。

○岩原委員長　　各委員からそれぞれ御指摘いただきましたが、追加しての御意見等ございましたら、どうぞいただきたい。池本委員、お願いします。

○池本委員　　まず１つは、先ほど割販法平成28年改正の施行日を平成29年12月１日と申し上げたのですが、これは特定商取引法の施行日でして、割販法はその翌年、平成30年６月１日施行だったと思います。ここは訂正させてください。

したがって、現在ちょうど４年で、あと１年で５年になるというところです。

そしてセキュリティの話と、悪質加盟店排除の両方について一言申し上げたいのです。

まずセキュリティのほうについては、そもそも不正利用が発覚して問題が手がかりとして分かるということと、それから加盟店の側が自分のところで不正利用されて漏えいしたようだと申告するという２つのルートがあり得るとは思うのですが、現実にはどちらがどのぐらいを占めるのか。恐らく不正利用の問題が出てきて調べていくことになるのではないと思うのですが、そういった内訳というのは把握できておられるのかどうか。

そして、どうもこれは情報漏えいから不正利用があったようだというときに、どこの加盟店なり、あるいは別のサイトなり、どこから漏えいしたのかという漏えい元の特定はきちんとできているのか。それ自体が不明で終わるケースがどのぐらいあるのか。そして漏えい元が分かっているものについて、先ほど来お話のあります現在の水準のセキュリティ対策を講じていたけれども破られた割合と、そもそも実行できていなかったのがどのくらいなのかということを、厳密ではないかもしれないですけれどもある程度の割合を示していただいて、それによってどの辺りから重点的に取り組んでいく必要があるのかというところを、見ていく必要があるのではないかと思います。これは事務局、あるいは業界団体に対してのお願いです。

もう１点は悪質加盟店排除のところですが、そもそも無登録業者を通じた決済だというものが､事業者数ベースでいってどのくらい申告ないし情報として把握しておられるのか。その中で警告することによって排除､あるいは是正されているものがどのくらいあるのか、ないのか。具体的なデータをお伺いしたいと思います。

それと先ほど来複数の委員から指摘のあったプリペイドとか、資金移動とか、決済代行とか、ほかの手段は加盟店の管理という制度がきちんとできていない分野があるために、カード会社の資金の送金先が加盟店そのものではなくて、そこの間に別の決済業者が入っているために、その先とのつながりが見えないというケース。その辺りもクレジットカード会社として、どのぐらいこういう問題があるというように把握しておられるのか。具体的な事実。把握できているところ、できていないところを含めた事実関係をもう少し示していただいて、どこが重点施策かというところを議論できたらよいのではないかと思います。

以上です。

○岩原委員長　　池本委員から、ただいま事務局側への御質問をいただきましたので、事務局側から何か。

○刀禰商取引監督課長　　経済産業省でございます。

幾つか御質問いただいておりますけれども、まず不正利用額の状況でありますが、実は正確なフィッシング被害由来、消費者の方々が直接狙われてフィッシング被害が出ているものと、加盟店や決済代行業者などカードサービスを提供する側から情報漏えいが起きて出ていく場合の情報分析については、精緻なデータについてまだ十分業界全体として分析ができているわけではございません。むしろ今池本委員からお話があったように、我々といたしましても、業界に対しては、こういった内訳の分析を改めてカード会社、各社からの協力を得ながらやっていただきたいと思って、今対応を進めているところでございます。

ただ、数字的なことは申し上げにくいのですけれども、昔からあったのはサイバー攻撃を受けて情報漏えいが起きてしまうことがＥＣ決済が拡大する中で多かったのですが、ここ数年の急激な伸びについて申し上げれば、やはりフィッシング被害によるものが相当多いだろうと言われております。消費者がうっかり情報を誘導されて入力して出ていってしまうようなケースも相当増えてきておりまして、ここ２、３年での動向は大変多いということになっております。

したがって、こういったところについては途中森竹委員からもお話がありましたが、サイバー警察局など関係部局とも連携して進めていかなければいけないと思っております。

２つ目は、それに関連してということで申し上げますと沢田委員からもお話がありましたが、キャッシュレス全体でも取組が必要だというような御意見でございます。まさに御指摘のとおりだと思います。

とはいえ、今足下でいきますと、キャッシュレスの中でもクレジットカードが大半でございます。約９割がクレジットカードというキャッシュレスに占める比率からいたしましても、不正利用額も当然実際に出てきている金額の大宗は、やはりクレジットカード由来というところがございます。

ただ、他方で金融庁のほうで所管されているような前払いの世界でも、キャッシュレスの拡大に伴って不正利用が増えてきていることも、傾向としてはおっしゃるとおりであります。具体的に最近ニュースなどになっているメルカリ、メルペイも、多くのフィッシング被害を受けているといったことで今話題になっておりますが、したがって、こういったところについてはよく関係省庁が情報連携、共有をしながら、さらなる対策を取っていかなければならないと思っております。

最後３点目でありますが、悪質な無登録の業者に対する警告や対応ということでございますが、当然多くの事業者さんは真面目に登録されているわけでございます。これは二村

委員からも御指摘があったと思いますが、当然関係業者の大半は真面目にしっかり手続きを取って事業を行っておられるわけですが、少数とはいえ、ごく一部にいろいろな事例が出てくるということでございます。

具体的な社数等については、今こういった無登録業者、我々が見つけていって、実際に個社に対して個々にアプローチをしていくような形でございます。昨年一年間を見ましても本省が対応している案件でも数社、こういった事例は幾つかございました。そういったものについては、その都度対応していっているということでございます。

途中長谷川委員からもお話がありましたように消費生活センターからも、そういったいろいろなルートを通じて情報が入ってまいりますので、端緒をよく有効に生かして対応していきたいと思っております。

事務局からの回答は以上でございます。

○岩原委員長　　ほかに皆様から、さらに追加の御意見をいただけることはございますでしょうか。よろしいですか。――岩下委員、お願いします。

○岩下委員　　先ほど申し上げたことでもあるのですけれども、もう一度申し上げておきますと、この種の犯罪の、かつてクレジットカードのカードそのものをどこかで使った情報を取って、それを別のカードに偽造して使うみたいな犯罪の場合は、どこで盗まれたかみたいな話をカード会社がかなり詳細にフォローしていましたが、今のカード番号になってしまうとカード会社は全くフォローできないはずなので、原因を追求するのはなかなか難しいと思うのです。

多分今考えるべき対策というのはクレジットカードそのもの、オンラインの利用方法を何がしか今よりも、言葉は悪いですけれども使いにくくするというか、少なくとも消費者が安易にどうせ何をやっても保証されるのだと思って、どんどんデータを入れてしまうようではない状況をつくり出すことが非常に大事で、消費者にダメージがなければそれでいいのかというと、消費者にダメージがなくても犯罪者に手取りがあれば、犯罪者が収益を上げてしまえば再びまた狙われて結果として消費者の被害が拡大してしまうので、それを何とか防ぐために消費者のほうの行動を変えていただけるような、そういう対策をしっかり講じていくことが非常に大事だと私は思います。

消費者は弱いので何の義務も課さないということではなくて、消費者自身も当然重要なステークホルダーなわけですから、消費者が何をしなければいけないのかについての厳しい、単なる教育というよりも、もし仮に不注意があっても自分自身が損害を被るような形

になっていないからこそ、ほかのものはあんなに騒がれるのにクレジットカードだけは騒がれない。不思議な状態がつくられていて、それがどんどん被害の拡大につながっているという問題は何とかするべきだと思います。

私からは以上です。

○岩原委員長　　ほかに何か御指摘いただくことはございませんか。――特にないようでございましたら、ちょっと事務局のほうから補足をお願いいたします。

○刀禰商取引監督課長　　ありがとうございます。

それでは、今日は各委員におかれましては多くの貴重な御意見をいただきまして、誠にどうもありがとうございました。一つ一つに全て回答できるわけではございませんが、各委員から重要な御指摘をいただいておりますので、事務局のほうから幾つか補足をさせていただきます。

まず最初のセキュリティに関しての対応でございます。沢田委員からは、不正利用防止の対策をしっかりすべきという話がございました。特に不正犯罪者、どこからアプローチされているか、特定なども必要ではないかということで、警察、ＪＣ３との連携の話もありました。

資料２―２の58ページに書いておりますが、これは森竹委員からもお話があったとおりでございますけれども、サイバー警察局とも連携をしっかり取っております。

特にポイントは、これまではカード会社自身が被害届は各警察署に出しているのですけれども、途中多くの委員から御指摘があったようにカード会社自身が保険を掛けていたりとか、情報漏えいが発生してしまった加盟店や、あるいはＰＳＰ等に最終的に損害賠償を求めれば補償を受けられることもありまして、なかなか全ての案件、サイバー攻撃について被害届を出している状態ではございません。

これは逆に捜査する側の立場に立ちますと、どういう情報であれ、裏の世界ではいろいろな情報が、一つ一つの点が線や面になっているということでございますので、これまで被害届を出すまでに至っていなかった攻撃の情報だとか、インシデントの情報についても、積極的にサイバー警察局や治安当局との連携に努めていかないといけないと思っておりまして、そういった情報連携の在り方についてはよく国側のほうで連携して、整理をしていきたいと考えております。

それから池本委員からは、ＰＳＰやアクワイアラーに対する管理責任をしっかり位置づけていくべきだというお話がございました。実際今スライド29ページに書いておりますよ

うに、今でも法律や、それからガイドラインに基づきまして加盟店調査というものをしっかり行わせているところでございますけれども､実効性ならしめるような対策をもう一度、もう二段取っていくためには何ができるか。この辺りについては、引き続き別途用意させていただきますセキュリティ関係の専門の有識者検討会のほうでも検討を進めたいと思いますし、また業界自身もセキュリティ対策協議会のほうで対応していきたいと思っております。

それから岩下委員からも多くの御指摘をいただいたところでございますが、最後にもお話がありましたように消費者へのアプローチが大事ということでございます。

実際ＥＭＶ３-Ｄセキュアについてはスライド39に書いておりますように、これを相当普及しなければいけない。特に我々は、これは一日でも早く普及したいと思っていますけれども、どれだけ日本全国に展開できるかということでいきますと、経産省としても2025年にはキャッシュレス比率をさらに４割まで引き上げていこうとうたっている中では、併せてセキュリティを高める方策を集中的に、これからの期間で打って対応していかなければいけないと思っております。

その際、次の40ページ目のスライドに書いておりますけれども、仮に加盟店側からいたしますと､いわゆるチャージバック制度の問題を抱えておりますので、ＥＭＶ３-Ｄセキュアを導入しなければ最終的に損害賠償を受ける、セキュリティの免責事由にはならないような事態に今後なってきますので、そういったところをしっかり促していく。消費者側に対してはフィッシング対策協議会などと連携して、まさに一つ一つの情報を入力することに対する注意喚起、こういったところについては消費者庁さんも含めて、どのような連携をしていくかについて検討を深めていきたいと考えております。

それから二村委員からも多くの御指摘がございましたが、特に経済安全保障の観点という話もございました。特にどの国と名指しでするわけではございませんが、フィッシング被害、サイバー攻撃を仕掛けている国との関係では国際的に対応していくことも必要でございます。こういったところに対しては、やはり警察当局との連携も強めたいと思っておりますし、併せて途中お話があったように事業者自身がペネトレーションテストだとか、自ら検証テストをやる、いわゆるセキュリティ監査をしっかり引き締めていくことが何より大事だと思います。そして申し上げたように経営陣にもセキュリティ担当の役員を置いて、その下で対応していくというガバナンスをしっかり促していかなければいけないと思っておりますので、こういったところについても今後セキュリティ対策ガイドラインの中

で、リクワイアメントをより強い意味の方向で検討しなければいけないのかなと、改めて認識したところでございます。

それから森竹委員からは、ＰＣＩＤＳＳの設定については、事業者によってはそもそもスコープ決めとか、あるいは取得過程においていろいろな問題も実はあるのではないかという話もございました。こういったところについては実際に起こってしまったインシデントに対して、しっかり我々が行政として検証し、再発防止を促すという形で、しっかり原因究明をしていきたいと思っております。特にＰＳＰやＥＣシステム提供会社といった新しいプレイヤーについては、まさに２年前の割販法の改正におきまして報告徴収命令等の必要な行政の権限を我々に与えていただきましたので、むしろこれをしっかり行使して、対応していきたいと考えております。

それから藤原委員からも、情報の共有ということがございました。これは何人かの先生方からもお話のあった個人情報との関係も問題になってまいります。ここについては個人情報保護委員会との関係も含めて、不正情報の共有の仕方について有効的にやっていくのか、ここについても今後事業者側もシステムの共同化を検討していく中で、併せて行政側で環境を整備していく観点からも検討を深めたいと思っております。

それから長谷川委員からも消費者保護の立場からフィッシング被害という話がございましたが、繰り返しになりますが59ページに書いておりますように、フィッシング被害に関わる周知・啓発というものについてＪＣＡ（日本クレジット協会）とか、フィッシング対策協議会といった、まさに官民の連携でしっかりやって、消費者に対する効果的な周知というものに取り組んでいきたいと思っております。

それから後半でございます。セキュリティ以外についても様々な御意見をいただきました。ありがとうございます。

二村委員からはマンスリークリアについても、また池本委員からも御指摘ございましたが、４年以上経過する中で改めて検証が必要ではないかという話もございましたが、こちらも今後の在り方についてよく検証させていただきたいと思っております。

それから多くの委員の方々に御指摘いただきましたアクワイアラーの、いわゆる無登録の悪質な業者に対する取締りなり、実効性、エンフォースメントの強化ということでございます。こちらについてもまだまだ我々は実態を十分に、全貌が把握できているわけではありません。むしろ一つ一つの事案についてその都度対応するような、個別撃破するような対応を強いられているのですが、おっしゃっていただいたように制度的に改めてこうい

ったところに対するアプローチはどうするのか。特商法との関係性だとか、それからアクワイアラー、ＰＳＰがむしろ管理責任をしっかり強化すべきではないかという御意見もありましたので、こういったところもよくよく我々としては踏まえて監督の強化ということで、しっかり取り組んでいきたいと思っております。

最後に、先ほど池本委員から御質問いただいたところでございますが、まだまだ犯罪なり不正利用がどこからどういう形で揺らいできているか。まさに業界全体としても、十分な分析が精緻にできているわけでないことは確かでございます。こういったところができなければ、当然打ち手が効果的にできないわけでございますので、しっかりとしたエビデンス、データの検証というものも今後しっかり対応したいと思っております。

そして最後、決済代行業者につきましては岩下委員をはじめとして各委員からもお話がありましたが、キャッシュレス全体に関わる、言わば金融におけるプラットフォーマー的な存在で、昔は裏方であったものが、むしろ今はメインのプレイヤーになりつつあるのではないかという直感も、私自身は持っているところでございます。言わばプラットフォーマー的な人たちに対するやり方は、なかなか正直申し上げましてよく慎重に検討もしなければいけないかと思いますし、金融庁も含めて省庁連携して対応しなければいけない、検討も深めなければいけないと思っておりますので、こういった論点についても、今後経産省のほうで別途用意させていただきます有識者検討会の重要なイシューとして、検討を深めていきたいと思っております。

経産省のほうからの回答は以上でございます。

○岩原委員長　　どうもありがとうございました。

お時間の関係もございますので、ここで本日の議論を区切らせていただきたいと思います。皆様、大変活発な御意見をいただきまして、ありがとうございました。いずれの御意見も非常にポイントを突いた重要なものであり、また多様な御意見をいただきましたので、事務局のほうでよく整理して、今後の審議の方向を検討させていただきたいと思います。

私としては、最初に岩下委員が御指摘になりましたように、300億もの金をブラック社会に投げ込んでいること自体が非常に大きい問題でありまして、また同時に決済のシステム全体のコストを上げていることになっているわけですから、こういうことが起きないように制度全体で見て、そういうことを最小化していくための仕組みをどうやって考えたらいいかということを、考えたいと思います。その中には先ほど情報共有で出ました個人情報保護法との関係とか、あるいは決済代行業者のような関与者が出ておりますので、省庁連

携その他、全体としての決済の中の１つであるクレジットカードのシステムの、セキュリティに関してのコストを最小化できるような仕組みを皆様と考えていきたいと思いますので、どうかよろしくお願い申し上げます。

それでは、最後に事務局から事務連絡等についてお願いいたします。

○刀禰商取引監督課長　　本日は委員の先生方におかれましては活発な御議論をいただきまして、誠にありがとうございました。

本日の議事録に関しましては後ほど事務局で作成の上、各委員の皆様に個別に御確認をいただいた後、経済産業省のＷｅｂサイトで公表する予定としております。

また次回の委員会は、今回の議論にもありましたように年明けを目途に皆様に御報告できるよう、鋭意検討を深めていきたいと考えております。引き続き、どうぞよろしくお願いいたします。

○岩原委員長　　それでは、以上をもちまして本日の審議は全て終了いたしました。本日はお忙しいところを熱心に御審議いただき、誠にありがとうございました。

――了――