第31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５年２月２日（木）10時00分～12時00分

場所：オンライン開催（Ｔｅａｍｓ）

○刀禰商取引監督課長　　ただいまから第31回産業構造審議会商務流通分科会割賦販売小委員会を開催いたします。

御多忙のところ御出席賜りまして、誠にありがとうございます。

本日は、オンラインでの開催となります。通信負荷の軽減の観点から、御発言いただくときのみ、マイク、必要に応じてカメラをオンにしていただければと思います。また、ＹｏｕＴｕｂｅでの同時中継となっております。

本日は、御欠席の方はおらず、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。

また、議題１の関係者といたしまして、日本クレジット協会及びクレジット取引セキュリティ対策協議会にオブザーバーとして参加いただいております。

次に、配付資料の確認をさせていただきます。事前に事務局から各委員の皆様に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ください。

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記入していただきますようよろしくお願いいたします。岩原委員長、もしくは事務局から適宜指名をさせていただくことといたします。

議事の運営に関しましては、議事については原則公開とし、本日の配付資料及び議事録につきましては、事後に公表とさせていただきます。

次に、新しく今回御着任いただきました委員の御紹介をいたします。本年１月11日付で、中央大学国際情報学部教授・石井夏生利委員及び神戸大学法学部研究科・法学部教授の中川丈久委員、お二方に御着任いただいております。今回御着任いただきましたお二方の委員より、それぞれ１分程度で自己紹介をお願いできればと思います。

それでは、最初に、石井委員からよろしくお願いいたします。

○石井委員　　よろしくお願いいたします。中央大学国際情報学部の石井と申します。

本日から割賦販売小委員会に参加させていただくこととなりました。どうぞよろしくお願い申し上げます。

私の専門分野は、プライバシーや個人情報保護法を中心とします情報法の領域となります。特に個人情報保護法関係ですと、政府の政策課題の至るところで登場する法律と思っておりまして、割賦販売法の領域に関しましては、クレジットカード番号等の適切な管理の規定などがまさにそれに関係するところかと思います。ふだんは個人情報保護法本体の視点から論点を見ていくことが多いわけですが、こちらの検討会では割賦販売法の全体の仕組みからいろいろな論点について議論に参加してまいりたいと考えております。どうぞよろしくお願いいたします。

○刀禰商取引監督課長　　ありがとうございました。どうぞよろしくお願いいたします。

それでは、続きまして、中川委員、どうぞよろしくお願いいたします。

○中川委員　　中川でございます。神戸大学で行政法を担当しております。

行政法が専門ですので、かなり広い範囲の法律のうち、行政的な規制があるもの全般を普段から見ておりまして、割賦販売法につきましてもその観点から、これまでもちらちらと見ることもあったのですが、何しろ非常に複雑なといいますか、業界構造が外部からはなかなかよく分からないところでしたので、これまでそんなにやってきたわけではないのです。後で御報告がございますが、昨年、セキュリティの検討会に参加させていただきました。その中で、行政法的な問題だけではなくて、先ほど申し上げた産業構造であるとか、これまでのいろいろな改正の経緯等を御教授いただきまして、ますます関心を持っているところでございます。引き続きまして、皆様のいろいろな御知見をいただきながら、私自身も勉強を進めていきたいと考えております。どうぞよろしくお願いいたします。

○刀禰商取引監督課長　　中川委員、どうもありがとうございました。どうぞよろしくお願いいたします。

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　　岩原でございます。よろしくお願いします。

それでは、議事に入りたいと存じます。本日の議題はお手元の議事次第のとおりでございます。

１がクレジットカード決済システムのセキュリティ対策強化検討会報告書について。事務局より御説明をお願いいたします。

○刀禰商取引監督課長　　それでは、事務局の経済産業省商取引監督課から御説明申し上げます。

まず、資料２を御覧ください。パワーポイントの１枚でポイントを記載しております。

この検討会の設置でございますが、先ほど中川委員から御説明がありましたが、中川委員に座長を務めていただく形で、専門的、技術的な観点から、より深掘りした検討を昨年来、半年間かけて検討いただいたものでございます。そして先月、１月に検討会でこの報告書がまとまったということでございます。

今回この報告書につきましては、いよいよこれから我々行政、それから今日オブザーバーで参加している業界、協議会など、クレジットカード決済に関わる各プレーヤーがしっかりこの対策を実行に移していく段階に入ってまいります。その実行に当たっては、まだまだ詳細な設計、様々な工夫、また引き続き検討課題になっているものもございます。こういったものを取り組んでいくに当たりまして、改めて今日、産構審の割販小委員会の委員の皆様に御意見をいただきまして、そういった御意見も参考にしながら、次の実行に移していきたいと思っておりますので、今日の御審議のほど、どうぞよろしくお願いしたいと思います。

さて、この検討会でございますが、ちょうど半年前、昨年６月、前回の割販小委員会を開催した際に、こういったクレジットカードの不正利用が増加している対応に対して、しっかり対応を取っていくという観点から設置をしていくということを決めた次第でございます。

2021年のクレジットカード不正利用額は300億円を突破して、過去最悪に上る数字に至っております。もとよりカード決済のセキュリティ対策強化は、長年行政、そして業界挙げて、官民連携で取り組んで、対策を積み上げてきたところではありますが、サイバー攻撃の巧妙化、また最近は消費者自身を狙ったフィッシング詐欺なども横行しておりまして、セキュリティをめぐる対策というのはますます高度化している状況であります。したがって、従来の取組に加えて、さらに対策を追加、強化していくという観点から、今回の検討会だと思ってございます。

また、一つの目安として、行政としては2025年にキャッシュレスの達成割合を現状の３割からさらに４割に引き上げていくという目標を持っておりますが、こういった目標を達成していく上でも、安全・安心なクレジットカード決済システムの環境を整えることが必須であります。したがって、当面、まずは2025年に向けて対策をしっかり講じていくという観点から、今回の対策を取りまとめた次第でございます。

それでは、ポイントを幾つか申し上げます。今回の対策は大きく３つの枠組みになって

おります。

１つ目の柱が漏えい防止。何よりカード番号の情報漏えいを防ぐということであります。

２つ目の柱、枠組みは不正利用防止ということで、カード情報が完全に漏れないようにすることもなかなか難しい状況の中で、仮に漏れた場合に、そういった漏えい情報が犯罪者によって不正利用されないように、二次被害を防いでいくための対策を講じる。こういった本人認証を徹底する不正利用防止が２つ目の柱になっております。

３つ目は、何より消費者の皆様にこういった対策についての理解をいただきながら、さらなる対応の周知を図る。それから、サイバー警察局はじめ、関係当局とも連携しながら犯罪を抑止していくというのが３つ目の柱になっております。

１つ目の漏えい防止でございます。左側画面にありますけれども、まず、今回の取組、対策を積み上げていく、強化していく観点でターゲット、重点的に考えているのは、１つはやはりＥＣ加盟店への対応であります。ＥＣ加盟店においても、カード会社、アクワイアラー等の下で安全管理措置を講じるという対策も、これまで数年間積み上げてきているところであります。例えば、いわゆる非保持化の対策というのを2010年代後半以降強化してまいりました。しかし、この従来の取組だけではカード情報の漏えいは防げない、そもそもサイバー攻撃に対して非常に脆弱性が高まっているというような状況もあります。その原因は、やはりＥＣサイトそのものに欠陥がある、あるいはソフトウエアなど、日頃のアップデート、運用管理を怠っていて、サイバー攻撃を招いてしまうような状況になってしまっているというような背景もございます。したがって、従前のカード情報を保存しない、保持しないという非保持化の取組のみならず、それに加えてＥＣサイト自体の脆弱性対策をしっかり取り組んでもらうということを、今回あえて明示的に必須化ということにしたいと考えております。ターゲットイヤーとしては2025年度から正式に法律上の義務がかかる形にしていこうということで、これから２年かけて順次、正式な義務化に向けた取組の準備を進めていくということで考えております。

また、この取組は、当然加盟店の管理責任、加盟店調査の責任を割販法に基づいて法律上の責任を負うカード会社等アクワイアラーの取組とも一体でございます。ＥＣ加盟店、アクワイアラー等が一体的に取り組んでいくことが何より大事になってまいります。下のＥＣ加盟店の次にアクワイアラー等と書いておりますけれども、アクワイアラー等においては、加盟店管理の従来の取組の中でさらに強化をしていくという観点から、ＥＣ加盟店におけるチェックリストを、まずはＥＣ加盟店でしっかり自己点検をし、そして管理責任

を負うアクワイアラーがそれをダブルチェックしていくというような仕組みを導入しようと考えております。既にこういったチェックリストを、どのようなものをまずひな形として作って、実際運用を始めるかということについては、今年度から既に試行的に始めているところでありますけれども、そういった試行の取組の状況などをしっかり検証し、2025年の本格的な法律の義務づけに対応した運用に何とか間に合わせていきたいと考えています。

また、今回の対策は全体として大きく２段構えになっております。2025年に向けて、まず足元しっかり取り組まなければいけない当面の対策というのが１つ目になってまいりますけれども、もう一つ、中長期的に、継続的に検討していく課題というのも今回の報告書に盛り込んでおります。座長をお務めいただきました中川委員のお言葉をお借りすれば、２段階ロケットということになってまいりますけれども、２段階目のロケットについては、継続的検討事項ということで、三角括弧で記載してございます。

例えば、ＥＣ加盟店での対応ということになってまいりますと、より実効性を上げていくという観点から、国の関与の在り方についても、引き続き議論、論点があろうかと思います。例えば、場合によっては、こういった安全管理措置が不十分な加盟店に対して、将来、処分まで規定していくのかどうか。今回そこについては結論を出しておりませんけれども、今後の運用状況などを踏まえて、引き続き、こういった更なる措置についての要否を検討していくことになろうかと思っております。

続きまして、(2)決済代行業者、いわゆるＰＳＰでございます。こちらについても昨年の６月の割販小委員会でこの検討会を設置するに当たりまして、当時大きなインシデント事案がございました。中堅の決済代行業者において40万件を超えるカード情報漏えいが起きたという事案が当時発生してございまして、こういった事案も考えますと、さらなる監督上の措置、規律の強化についても今回の検討会においても取り扱ったところでございます。ただ、この半年間の検討会においては、具体的な措置というところまで結論には至っておりません。むしろ、引き続き、まだまだ決済代行業者、ＰＳＰ、多様なプレーヤー、また大中小、その規模に応じて業態も違ってきているということでありますので、引き続き、行政のほうでは実態把握に努めて、そういった実態状況を踏まえた課題の整理、そしてさらなる対応といったところで継続的に検討させていただきたいと考えているところでございます。

それから、(3)は、いわゆるイシュアー、カード会社等ということでございますが、こ

れはもう既に取り組んでいる話、いわゆる国際的なセキュリティ基準、ＰＣＩ　ＤＳＳバージョン4.0への準拠が既に開始されており、これは既に2024年の３月末という期限が控えておりますので、これを着実に実行していくということが何より大切になってまいります。

また、継続的な課題ということで検討会において議論があった一つの例としては、やはりこういったセキュリティ対策を強化していること、あるいはそのセキュリティ対策が万全かどうかといったことについても、消費者の方々が分かりやすく、また市場によってそういった評価がされるように、対策の見える化をより工夫していくべきではないかというような御意見もございました。

消費者行政のほうでは、特商法等でこういった表示義務などの取組も先行して事例がございます。クレジットカード決済システムに係るセキュリティにおいて、こういった表示の在り方についても、一つのアイデアとして検討会でも示されたところでございます。対応についてどうしていくかということについては、引き続き継続的な課題として取り扱っていければと考えているところでございます。

それから、(4)漏えい時のインシデント対応の強化ということであります。やはり何よりこのサイバー攻撃、それからフィッシング詐欺などを通じてカード情報漏えいが起きて、そして不正利用になったというようなことが起きたときに、当然これを早く検知して、不正利用を止めて、原因を分析し再発防止を講じていくということを速やかにやることが何より大事であります。

しかし、他方で、情報漏えいという形で被害を被るのは消費者の皆様、あるいはこういったサイバー攻撃がほかの事案に及んでくるということで、早く業界全体で共有していくということも必要になってまいります。したがって、サイバーインシデント時の対応の在り方、初動対応については、より早期化、迅速化していかなければいけないと思っております。これについては、ＪＣＡ、日本クレジット協会が定める業界のマニュアルの改定に今後しっかり反映していきたいと思います。またその際、政府全体でもこういったサイバー攻撃対応に関する初動対応、それから情報公開、公表についての手引、ガイダンスの検討が今進んでおります。例えば最近ですと、病院がサイバー攻撃にさらされるという話もあります。また、同じ金融業界では、インターネットバンキング等、ほかの事案でもそういった事例もございます。したがって、こういったサイバー攻撃が日常茶飯事的に今起きているような状況を考えますと、横断的にこういったガイダンスを整えていく必要がある

ということで、別途検討が進んでおります。こういった取組についてもしっかりカード業界の取組に盛り込んでいきたいと考えているところでございます。

また、日本クレジット協会そのものもこういった対策の取組を業界の中で主導していく役割が期待されますので、こういったセキュリティの対応状況、それから、サイバー攻撃に対する傾向だとか調査分析、こういった機能についても体制の強化に引き続き取り組んでいきたいと考えているところでございます。

続きまして、右肩、Ⅱ．不正利用防止であります。これは何らかの形でＥＣ加盟店など、あるいはＰＳＰ等がサイバー攻撃にさらされて、それをきっかけにカード情報が漏えいする、あるいは消費者自身がフィッシング詐欺に遭って、誤ってカード情報を外に漏らしてしまうということ、あるいは、クレジットマスター攻撃のように、ＡＩなどを活用しながら犯罪者がランダムにカード情報を打ち込んで攻撃してくる。このような第三者、犯罪者によるなりすましの利用ということが当然出てくるわけでありまして、ここに対する不正利用防止が大きな２つ目の柱になってまいります。

ここにおいては、特に対策を取っていくのがカード会社であるイシュアーと、決済のフロントとなる、消費者との関係では取引の前線になるＥＣ加盟店、この両者における一体的な取組が今後必要になってまいります。その際強化をしていかなければいけないと思っておりますのが本人認証であります。いわゆるクレジットカードに記載されている４情報だけでは、こういった不正利用を防止することができないという事案になってきております。

また、従来は、高リスク商材など一部の加盟店での取引についてはさらなる本人認証なども含めて、対策の強化を促してきているところでありますけれども、こういった不正利用はもう高リスク商材にとどまらず、様々な取引においても不正利用は生じているという現状に鑑みますと、これは全ての取引を対象に、こういった本人認証を取り入れていくという形にしなければならないということであります。こちらについても2025年からしっかり法律上の義務がかかる形にしていくということが今回の報告書のポイントでございます。そして、2024年度末に向けて、これから２年間かけて業界を挙げて対応準備を整えていくということになってまいります。

その際、イシュアー・ＥＣ加盟店の欄の２つ目のポツに書いてありますが、これも国際的なブランドが推奨する本人認証手法であるＥＭＶ３ＤＳを原則全ての加盟店に導入するということがポイントになってきます。こちらについては、今後、クレジット取引セキュ

リティ対策協議会が毎年度末に改定していますガイドラインのところにしっかり反映して、対策を促していくということになってまいります。

他方で、カード会社であるイシュアーにおいても、ＥＭＶ３ＤＳの導入を有効かつ実効ならしめるための取組をやっていくというのが表裏一体、セットでございます。いわゆるリスクベース認証をしっかり整えるということであります。全てのあらゆる取引に本人認証を課すということは、当然、取引の過度な負担を加盟店、消費者自身が抱えることになりますし、逆に言えば、全ての取引にそういったチェックをかけることがかえって、リスクの高い取引を検知し、それを止めるということを妨げてしまうということもありますので、したがって、そこはカード会社自身がしっかり日頃の行動特性分析、それから商品のリスク性、また販売店等の状況など、様々な情報をしっかり分析して、リスクの高い取引については、しっかり本人認証を課すというようなリスクベース認証を組み合わせる形にしていかなければなりません。これについては、今後カード会社がしっかり準備を整えていくということになってまいります。

それから、こういった不正利用防止は業界横断の課題になっていることも確かでございます。(2)に書いておりますように、カード会社であるイシュアー間での不正利用の情報の共有に向けた枠組みの検討というものも、もう既に一部の主要会社を中心に検討が始まりつつあるところでありますけれども、こういった取組についてもさらに前進させていくべく、国もしっかり連携を取りながら、官民連携の取組を進めていきたいと考えております。

最後、右下、Ⅲ．でありますが、犯罪抑止・広報周知であります。(1)フィッシング対策に関しては、まさに今消費者に直接働きかけるフィッシング詐欺メール、あるいは偽サイトに誘導するフィッシングサイトなど、様々な手法で消費者が狙われている状況にあります。こういった偽サイト、それから偽メールに消費者が騙されないで済むためにも、カード会社自身がしっかり自分たちの電子メールのドメインの管理をし、偽サイトをテイクダウンするとか、フィッシングメールとカード会社が流す自分たちの正規のメールとの識別、また偽メールが消費者に届かないようにするための仕掛けをしっかり整えていく必要があると思っています。その点で、ＤＭＡＲＣという取組が今産業界に対して推奨されているものであります。また、昨年の年末、12月に政府全体で閣議決定されました「世界一安全な日本」創造戦略」の中でも、このフィッシング対策の強化、またＤＭＡＲＣの導入がうたわれているところでございます。

既に今日、参考資料５でお配りしておりますけれども、昨日、フィッシング対策の強化について、経済産業省からＪＣＡを通じてカード会社各社等に対しての取組の要請をしているところでございます。

最後、資料の右下のところでありますけれども、サイバー警察局との連携ということで、こちらについても犯罪の摘発につなげていく。先ほど左側の部分で初動対応の迅速化ということをうたいましたが、これは最後は犯罪の摘発につなげていくという部分と一気通貫でありまして、こちらについては経済産業省が警察庁サイバー警察局など、関係機関の協力を得ながら、取組の具体的な手順を今検討しているところでございます。こちらについても業界マニュアル等に反映させていくべく、今後取り組みたいと考えているところであります。

そして、消費者の方々への周知ということについても、今後、日本クレジット協会、カード業界、そして国、関係機関が一体となって、消費者の皆様、特に先ほど申し上げた本人認証、ＥＭＶ３ＤＳの導入に当たっては、リスクの高い取引という形で判定された場合は、カード情報に加えて、ワンタイムパスワードや生体認証なども加えて求められるというような仕組みに変わり得るということについても周知をしていかなければいけません。また、日頃から、毎月の利用明細、日々の利用明細について確認いただくということについても、改めて理解をお願いするような形に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。

以上が全体の枠組みの説明でございます。残り、資料３の報告書本文について、少しだけお加えをさせていただければと思っております。

例えば資料の10ページ目でございますけれども、ＥＣサイト、ＥＣ加盟店への対応ということにつきましては、先ほど監督の強化というものが中長期的な課題となっているということも申し上げました。今回は、当面の対応というのはあえて四角の枠で囲っておりまして、その下に＜更なる制度的措置の必要性の検討＞ということが書いてありますけれども、加盟店の対応についてのさらなる措置、あるいは将来的な表示、見える化みたいなものについても、これはあくまでも例でございますけれども、将来的な検討課題として残されたものとなっているところでございます。

それから、次の11ページ目においては、アクワイアラー側の対応ということも記載しておりますけれども、当然実行に当たっては、数多くのＥＣ加盟店を抱えているのがアクワイアラーの現状でございますので、実際の実施状況の調査とか管理、こういった業務負担

についての留意も必要ではないかといったことも、これまでの検討会で御意見があったところでございます。

したがって、12ページ目においても、四角囲いしております国の監督の在り方、あるいは、その下に書いてあります＜更なる制度的措置の必要性の検討＞についても、どのような管理手法でやっていくのがいいのか、この辺りについてはやはり実効性の問題をしっかり留意しながら検討を深めていかなければいけないと考えております。

それから、13ページ目、右上については、これも先ほど例として申し上げましたが、ＰＳＰ、決済代行業者の登録化を図るのかどうか。これの要否については継続的な課題ということで、残された論点となりました。こちらについては、繰り返しになりますが、実態把握、それから課題の整理について、まずは努めていきたいと考えてございます。

続きまして、今度は19ページ目でございますけれども、消費者の皆様との関係でも、やはりカード情報の漏えいが起きたときの利用者の方々への早期の個別通知や公表の在り方というものも、検討会でも相当多くの御意見が出たところでございます。こちらの取組については、繰り返しになりますが、日本クレジット協会において今後対応していくことになりますけれども、現状よりもさらに迅速化が図られるように、工夫に取り組んでいきたいと考えているところでございます。

続きまして、今度は22ページでございますけれども、今回の対策の柱ということで、一部報道においても相当取り上げられているＥＭＶ３ＤＳ、本人認証の導入ということであります。こちらについては検討会においても様々な御意見がございました。特にＥＣ加盟店の方々からの御意見も含めますと、やはり公平、平等の観点から、原則全ての加盟店で導入していくということで、一部の方だけに偏った導入にならないようにというような話があったことも確かでございます。したがって今回、基本的には原則全ての導入ということを促しているところであります。

ただ、他方で、24ページ目に入りますけれども、とはいえ、このＥＭＶ３ＤＳの導入を今後図っていく一方で、従前から様々な不正利用防止措置、本人認証とは違う形の手法の措置というものも大手のＥＣモール等を中心に取り組まれてきていることも現状としては確かでございます。また、従来、国においては、高リスク商材等に限った重点的な対策でありましたけれども、属性・行動分析なども促してきてございます。こういった取組については、決して、今後必要ではないとか、むしろ無効になるということではなくて、様々な対策を組み合わせながら、総合的に対応を取っていくというのが何より大事であります。

ＥＭＶ３ＤＳそのものも完全にこれで全てリスクを下げられるわけでもありません。したがって、従前の不正利用防止措置も組み合わせる形での対応ということは、引き続き今後の取組において留意していかなければならないだろうと思っております。

そして、他方で、ＥＭＶ３ＤＳと同等の性能やファンクションを果たす本人認証の工夫も今後、業界の自主的な知恵や最新の技術、知見なども組み入れながら開発されていく、導入されていくことも今後想定されます。したがって、25ページ目の対応④に書かれておりますけれども、ＥＭＶ３ＤＳの導入を原則全てという形でしつつも、他方で、ＥＭＶ３ＤＳ以外の本人認証の在り方についても、いいものはどんどん取り入れていく、オルタナティブとして許容していくということも併せて講じなければいけないだろうと思っています。ただ、こちらのところでは、やはり相当技術的に、あるいは専門的に、代替策についての検証、またそれを取り入れていくことの妥当性の検証も大変大事だろうと思っております。したがって、これらについては、まさにこれまで専門的なガイドラインをつくってきたセキュリティ対策協議会を中心に、様々なプレーヤーの意見も集約しながら、詳細化を図っていくということを中心的に検討していかなければいけないと思います。また、国側のほうも、こういった業界の動静などもしっかり情報を把握して提供しながら取り組んでいきたいと考えております。

最後でございますが、32ページ目でございます。「おわりに」ということで、これは終わりの文ということで書いております。業界全体、また国全体も含めて改めて認識しなければいけないのは、この３パラグラフ目の最後に書いておりますけれども、セキュリティ対策に終わりはないということであります。不断にセキュリティ対策を講じていく、２～３年前の対策は２～３年たつと陳腐化していくというのがこの世界であります。したがって、今回2025年に向けて対応を取ってまいりますが、毎年度しっかり取組を検討して、不断に取組をアップデートしていくということを続けていかなければいけないと思います。

また、こういった取組については、カード業界が様々なプレーヤー、マルチステークホルダーによって成り立っているということでありますので、そういったプレーヤーによって業界全体で底上げをしていく取組、先ほど申し上げた協議会に多くのプレーヤーが参画して、全体の知恵を持ち寄って取組を促していくということもしていかなければならないと考えております。多面的な、重層的な取組をしっかり取り組んでいくということから、引き続き行政としてもこういった取組を推進し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、説明が時間を超過しておりますけれども、事務局からはまず以上でございます。御審議のほど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思います。ただいまの事務局からの説明について、委員の皆様から順に、御質問や御意見があればいただければと存じます。お１人５分以内を目安に御発言いただきたいと存じます。名前順で指名をさせていただきます。検討会の座長を務めていただいた中川委員には、最後に御発言いただきたいと思います。

それではまず、石井委員、御発言をお願いいたします。

○石井委員　　中央大学国際情報学部の石井です。

報告書についての御説明をいただきましてありがとうございました。今回、参加が初めてとなりますので、今御説明いただいた報告書の内容を正しく理解できているかどうか、やや心もとないところもありますが、理解に誤り等ありましたら御指摘いただければと思います。大きく３点ほどコメントをさせていただきます。

まず第１は、クレジットカード決済に関わる事業者の実態に応じた責任範囲を検討していく必要性が出ていると思いました。本来はアクワイアラーが加盟店管理を行う立場であるかと思いますが、ＰＳＰが実質的、実務的な加盟店管理を行っている現状があるという記載も報告書の中であったところです。とはいえ、ＰＳＰの種類が複数あって実態が分かりにくいといった記載も御説明の中にあります。クレジットカード決済において鍵となるプレーヤーには相応の責任を負っていただくのが制度上の考え方としては妥当ではないかと考えておりますので、ＰＳＰの実態管理や実態把握はもちろんのこと、事前規制としてのＰＳＰの登録制や、アクワイアラーとＰＳＰによる加盟店管理の役割分担の検証など、取り組むべき課題がいろいろあるのだなということを認識した次第です。

２点目は、透明性の担保という観点です。クレジットカード決済の構造は非常に複雑で、一般消費者には理解しにくい仕組みになっていると思います。クレジットカード決済を行ったとしても、自分が使ったカード決済に係る情報がどのように流れているかも非常に分かりにくい。一般消費者が直接接するＥＣ加盟店のサイトがふだん講じているセキュリティ対策も見えにくく、かつ、セキュリティ対策を受けたときに、どこからどのような報告をいつ受けられるのかも見えていない状況かと思います。このようなことからしますと、ＥＣサイト上では、ふだんから講じているセキュリティ対策を分かりやすく説明していただくということは必須だと思いますし、問題が生じたときの対応についても明らかにして

おくことが求められるのではないかと思いました。

また、情報漏えいが起きたときの透明性も非常に重要性が高いと思います。現状では、イシュアーとクレジットカード会社の調整が必要なので、フォレンジック調査を待って公表されるという御説明になっていたかと思いますが、方針が決まるまで情報を明らかにしないというのは、利用者にとって、利用停止の手続をした日の60日前から補償の対象ということを前提に考えますと、２次被害が仮に生じていたとしても放置される期間は生じてしまうということではないかと思います。そうしますと、報告書において利用者目線で対応を行うと述べていただいているスタンスにはそぐわない結果が生じてしまうかもしれない。

クレジットカード会社に問合せが殺到する恐れがあるともありましたが、これは実際どの程度の現実的なリスクとして顕在化しているのかも正しく把握しておくことが必要かと思います。

個人情報保護法上も、不正に利用されることにより財産的被害が生じる恐れがある個人データの漏えいなどは報告対象事態に該当するという規定がありまして、個人情報保護委員会への報告や本人への通知を求めている。本人への通知を求める趣旨としては２次被害を防ぐという趣旨がありますので、こうした趣旨からしても、本人に待たせることで被害が拡大しないような措置は当然必要になってくるのではないか。最低でも本人通知、本人への連絡が遅れてしまうことで被害が拡大したとすれば、それは補償してあげたほうがいいのではないかと思っております。

３点目は、不正利用防止ですが、こちらは御説明にありましたとおり、全ての加盟店に対して本人認証の仕組みを求め、他方でリスクベースの評価を行うという御方針については賛同いたします。

この関係で、26ページですか、不正利用情報の共有化についての記述があるところですが、こちらは確かに個人データの第三者提供という問題が出てくるとは思います。他方で、不正利用情報を共有化することには正当な理由もありますので、個人データだから共有が妨げられてしまうという結果にはならないよう、むしろ不正利用情報については積極的に共有化できるといった整理が必要だと考えております。

私からは差し当たり以上です。ありがとうございます。

○岩原委員長　　どうもありがとうございました。

それでは、次に池本委員、お願いします。

○池本委員　　池本でございます。

私はセキュリティの検討会にも参加させていただきましたので、本当に多岐にわたる新しい技術や対応で、カード加盟店も、イシュアー、アクワイアラーも、それぞれの関係者がたくさんの課題があるということを確認することができました。それはしっかりと実施していただきたいわけですが、今後の法制度の課題について、２点に絞って発言したいと思います。

まず第１点は、先ほどの石井委員の第１の論点とも共通するのですが、報告書でいいますと13ページから14ページに２か所ほど、ＰＳＰの登録制、事前のセキュリティ体制のチェックということが指摘されています。その必要性、重要性について少し補足して意見を述べます。

これは、現行法でいいますと、カード加盟店はセキュリティ対策の義務が定められ、それの履行確保は、カード番号取扱契約締結事業者、つまり主としてアクワイアラーが調査、指導監督するという位置づけになっております。ただ、現代はアクワイアラーとカード加盟店が直接つながるケースよりも、決済代行業者とか、ＥＣモール運営事業者とか、ＱＲコード決済業者とか、そういう様々な業者が中間に介在しているために、アクワイアラーが直接加盟店を調査、指導するという関係が薄くなっている。間接的なつながりでしかないという問題があります。しかも、今の決済代行、あるいはＥＣモール、ＱＲコードの決済業者などは、セキュリティの義務はありますが、アクワイアラーが指導監督するという関係は、必ずしも経済的にもないし、規定の上でも明確でないために、セキュリティ対策を実質的に担保する監督者が明確でないということになっているのではないか。その意味で、これらの中間の関係業者について、登録制度によって行政庁が事前に審査する仕組み、あるいは定期的にチェックするという仕組みが必要なのだろうと思います。その場合、中間業者自身のセキュリティ対策はもちろんですが、カード加盟店に対するセキュリティ対策の調査指導などの体制も項目に加えていただく必要があると思います。

先ほどカード加盟店に対する行政的な監視ということも課題となっておりますし、行政庁としては大変だと思うのですが、そこは多少人的体制を拡大してでも、今のキャッシュレス決済の安心・安全を確保することが大事だと思います。

ただ、留意点として、行政庁が審査するからアクワイアラーの指導監督の役割が弱くなってもよいということになっては、これは本末転倒です。やはりクレジットシステムが安心・安全なシステムとして確保される責任は、何よりもシステムを展開するイシュアー、

アクワイアラーが連携して責任を果たす。この点は十分に強調しておく必要があると思います。

２点目は、報告書でいいますと32ページ、「おわりに」のところであります。第３段落の辺りに、インシデントが発生した場合に当事者間、特に利用者との関係で公正な負担となるよう留意することも必要であるという指摘があります。私はこれは非常に重要な課題だと考えます。というのが、クレジット決済システムのセキュリティ対策、関係事業者の誰がどう責任を分担するのかというのは、行政的な義務だけではなくて、不十分な対応のために情報漏えいとか不正利用の被害が発生したときに、誰がその損害を、どういう割合で負担するのかということを明確化する必要があると思います。ただ、これは事業者間の負担割合の話ですので、きちんと議論していただくのですが、割販法そのもので直接関与することではないのかもしれませんが、非常に重要な課題です。特に最近の、今回の議論にもありますが、カード加盟店だけではない、イシュアーによって本人認証制度を強化するとか、不正利用の監視体制だとか、不正利用についてもいろいろな当事者の役割があるということが明らかになりました。だとすると、その部分についてもきちんとしたルールを定めておく必要があるというところです。その場合に、従来のクレジットカードの紛失、盗難を想定したカード保険のルールだけでなくて、カードは手元にあるのだけれども、どこかで漏えい、不正利用されたという場合も、消費者とカード業界との間の責任分担の在り方。例えば預金者保護法の考え方を参考にするとか、ここはきちんと公正なルールはどうあるべきかという消費者法の観点をきちんと踏まえたルールを議論する必要があるのではないかと思います。

以上です。

○岩原委員長　　岩下委員、お願いします。

○岩下委員　　京都大学の岩下でございます。意見を述べさせていただきます。

私は、今回議題にのぼっているセキュリティ検討会のメンバーではございません。検討に参加しておりませんので、この報告書及び取りまとめ資料を拝見した上でのコメントを述べさせていただきます。

一つの大きなイシューとしては、これまで基本的にクレジットカードのセキュリティ対策というのは、各業者が関連する、これまでも議論になった複数の事業者が複雑に絡み合ってクレジットカードというサービスのインフラストラクチャーを提供しているわけですので、その方々、それぞれ事業者が適切な対応をしてくださるということを当然に期待し

て、それを担保するために、業界内の自主規制、あるいは様々な認証制度、ＰＣＩ　ＤＳＳであるとか、ＩＳＭＳ、あるいはプライバシーマークであるとか、そういうものを活用して、一種ソフトロー的な形で対応をお願いしてきたという実態があるかと思います。これに対して登録制というお話がありましたが、より行政庁が直接的に関与するハードロー的な対応が必要ではないのかというイシューについての一つの論点があると思います。

この点について、この報告書では、とりわけＰＳＰ、決済代行業者等に関する規定が今後の継続的な検討事項になってございます。この点については私は大いに不満であります。なぜかというと、この審議を議論したときにまさに問題となったのは、メタップスペイメント――先ほど事務局はあえて名前を隠しましたが、これは個社名をぜひ出すべきだと思います。メタップスペイメントという会社が、ＰＣＩ　ＤＳＳ、ＩＳＭＳ、プライバシーマークを取っているといいながら、実際にその規定に沿った形でのセキュリティ対策を講じずに、しかも、警告が出ても、わざわざそれをリセットする形で、それに対する適切な対応を取らずに、46万件のクレジットカード情報を漏えいさせてしまったという大変深刻な事例が１年ほど前に発生しました。この事件を踏まえてこの検討が行われたわけです。その半年後には行政庁による行政処分まで行われました。にもかかわらずＰＳＰについては今後の継続的な検討にするという結論にしていくのは、この対応としてやや適切ではないのではないかと私は考えますので、この点についてはきちんとした枠組みをつくっていくことがぜひ必要である。なんとなれば、ソフトローだけで自主的に対応してくれないという反例が実際出てしまったわけですから、適切な対応を担保していくことがぜひ必要です。その意味では、引き続き皆さん御協力をお願いしますということでは、現在100億円単位で発生している犯罪の対策にはならないだろうと私は思います。この問題を解決するためには、やはりきちんとした行政庁の対応であるとか、監督、検査がぜひ必要です。

国際的に見ますと、クレジットカードというのはそもそも銀行のビジネスでありまして、銀行に対する監督の中でクレジットカードのビジネスも監督されているというのが世界的な常識です。日本だけ、クレジットカードビジネスと銀行ビジネスが分離され、異なる官庁によって監督されています。そういう特例を日本が設けている以上、そこについてしっかり日本の対応官庁が監督責任を果たすべきです。

もう一つは、今回、例えば将来的なセキュリティ対策の改善というお話がありました。この種の議論を行うときには、決定的に重要なのは、技術的な検討が必要だということです。技術的というのは、情報セキュリティーリスクに関する検討が必要だということで、

この点については、情報セキュリティの専門家、こういう分野についてきちんと専門に研究している研究者、学者が大勢おりますので、そういう方々の知見をぜひ利用するべきだと思います。業界の方々の自主的なルールに基づいて、ゆるゆるのチェック体制にする、ゆるゆるの実態にするということになるようでしたら、こういう制度を入れる必要はございません。そういう意味では、きちんとした外部の目で本当に有効な対策がきちんと取られているかということを検証し、それが利用者にも分かるようにする仕組みがぜひ必要だと考えます。

私からの意見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。

それでは、次に沢田委員、お願いします。

○沢田委員　　ＥＣネットワーク・沢田でございます。ありがとうございます。

論点はたくさんあるのですけれども、２点に絞って申し上げます。

まず１点目ですが、今回の報告書をＥＣ加盟店から見るとどう見えるかという点について申し上げます。これはやはり実質的な法的義務の拡大と見えます。今の割販法の枠組みですと、アクワイアラーによる加盟店管理を通じてという間接的な規定でありますし、今すぐではなくて時間的な猶予はあると理解はしているものの、法的義務の実質的な拡大という方向性は間違いがないのだろう。具体的な義務の内容と程度につきましては、クレジットカード・セキュリティ対策協議会のガイドラインによるということになると思いますので、そのガイドラインについてはぜひ今後パブリックコメント、意見募集をしていただきたいというのが１点です。

２点目ですが、この報告書は、細かいところはガイドラインに委ね、報告書自体は大きな方向性を示したものと理解しております。だとしても、やや結論を急ぎ過ぎの部分もあるのかなという印象を受けております。具体的には、不正利用対策、24ページの具体的な措置の対応の②の辺りです。原則全ての加盟店でＥＭＶ３ＤＳの導入を求めるということであります。

ソフトローというお話もありましたが、2015年改正で実行計画が実務上の指針になってから、先ほど事務局からも御説明がありましたが、ＥＣ加盟店は結構真面目に実行計画に示された４方策を実施していると思います。４方策とは何かというところは、参考資料３の19ページから20ページ辺りに記載いただいています。

その次の21ページでは、利用者であるかの適切な確認を原則求めると書かれているので

すが、これはＥＣ加盟店からすると、やっていますということです。なぜならば、不正利用で被害を受けるのはイシュアーではない。そのリスクは加盟店が負うのだとずっと言われ続けてきましたし、対面取引ではＩＣカードのような効果的な対策をイシュアー側で用意してくれたのですが、非対面ではそれに当たる効果的な対策が用意されていなかったので、そのリスクを加盟店が負っていた。やらないと自分が損をするという状態だったので、ＥＣ加盟店としてはそれなりにやってきたということです。

今回、ＥＭＶ３ＤＳという夢のソリューションをイシュアーが提供するから、さあ、使え、使わなければ加盟店契約させない、となっていくようにも読めるのですが、そこはまだいろいろ御検討中というところもあると思います。

申し上げたかったのは、ＥＣ加盟店は、サイバー攻撃もそうですけれども、不正利用についても被害者ですということです。被害がどこでどのように発生しているのかの実態をよく見ていただきたい。参考資料４に「世界一安全な日本」創造戦略についても御紹介いただいていますが、そこでも「被害実態を踏まえた有効な対策が必要」と書かれているかと思います。

もう少し具体的にお話させていただくと、一くくりにＥＣ加盟店となっていますが、この目的の下で、ざっくり３つのグループに分けることができると思っています。

グループ１が、属性・行動分析に代表される独自の不正検知が効果を上げていて、被害が抑えられているグループ。典型的には大手プラットフォームが実施する不正検知によって、そこに出店している加盟店が守られているという場面だと思います。グループ２は、外部サービスも使っているし、配送先の情報を見るなどいろいろ不正検知しているけれども、それでも被害に遭って困っているというグループです。よりよい対策があればぜひ使いたいと思っていると思います。グループ３が、効果のある対策ができていないところです。できているか、できていないかというのは不正利用被害の発生率で客観的に分かるはずなので、どの加盟店がグループ３に当たるか見分けるのはそれほど難しくないと思います。

今申し上げた中のグループ１は、既に不正利用抑止の目的は達成している、つまり割販法に定められた性能を満たしているので、新たに義務化をする必要はないと思われます。グループ２、やっているけれどもまだ十分ではないというところは、ＥＭＶ３ＤＳの効果が高いということが分かれば当然自主的に導入すると思います。なので、義務化の必要はないと思います。性能を既に満たしている当事者に義務を課すというのは公平でも平等でもない。本当に対策が必要なのはグループ３で、例えば何をしていいか分からないＥＣ加盟店に対して

はＥＭＶ３ＤＳを強くお勧めすることに意味はあると思います。行政がお勧めしていいのかという問題は別途あるものの、お勧めすることには意味がある。

ただ、その前に、何をしていいか分からないというところだけではないので、実態調査が必要と思います。４方策のうちのどの対策を取っているか、それがどうして効果がないのかを分析しないまま、ＥＭＶ３ＤＳがベストなソリューションだと決めてしまうのは少し飛躍があるのかなと思います。

グループ１と２、ある程度やっているところであっても、もちろんそれ以上の対策を常に求めています。ＥＭＶ３ＤＳを既に導入しているところも何社もあると思います。その結果、コストはどうだったか、効果はどうだったか、安定性はどうか、使い勝手はどうかといったようなことも、既に実績が出ているわけですから、きちんと聞き取って、課題も含めて今後の施策に反映させていくべきだと思います。この検討会には、加盟店として通信販売協会さんはいらっしゃいましたけれども、ＥＣに特化した加盟店はメンバーにいらっしゃらなかったと思います。ＥＣ事業者に対するヒアリングも特になかったようで、ＥＣ加盟店の実情があまり反映されていないと思いました。そこは今後、ガイドラインに反映していただくことを期待したいです。この議論をＥＣ加盟店は多分99％知らないのではないかと思いますので、パブコメを通じて、こういった議論がされているということの周知を図っていくことも重要かなと思います。

とりあえずは２点申し上げました。ありがとうございます。

○岩原委員長　　どうもありがとうございます。

それでは、次に田中委員、お願いいたします。

○田中委員　　野村総合研究所の田中でございます。よろしくお願いいたします。

私からは、最初に幾つか教えていただきたい点があります。そのあと、加盟店回りの話と、ＥＭＶ３ＤＳに関連して意見を述べさせていただこうと思います。

最初に確認したい点ですけれども、３ＤＳについて、昨年の10月の段階で、既存の３ＤＳから、ＥＭＶ３ＤＳに順次置き換えていっていると認識しています。新規に導入している先などからは、検討会のほうでのプレゼンでも大分効果が出ているという話もあったのかなと思いますが、まだ３か月ぐらいというところではあるのですけれども、この10月を挟んで、３ＤＳ導入に関連して、全体感として何か影響が出ているのかどうか、経産省側か、クレジット協会さんか、お分かりになる方がいれば、教えていただきたい。

あと、加盟店について、今チェックリストの試行が始まっているところだと思います。

こちらもまだ始まったばかりだというところは理解していますが、アクワイアラー側、加盟店側も結構負荷がある気がしておりまして、現状、始めてみたところでどういう状況かというところをお伺いしたい。

それはそれとして、報告の中身について意見を述べさせていただきますと、まず加盟店のところなのですけれども、まさに今チェックリストを始めていただいていたり、ガイドラインをつくって周知したりということになっていると思いますが、周知するといっても、方法は難しいと思います。アクワイアラー、あるいはＰＳＰなどから連絡せざるを得ないと思いますし、業界団体のホームページに掲示しても、多分誰も見に来ないと思いますので、具体的にどうやって周知させていくのかというところはきちんと考えていただきたいと思います。

一方で、対策をつくって継続的に更新していっても、本当に加盟店側がそれをフォローできるのかというところのほうが課題であると思います。これはジャストアイデアでしかありませんが、例えば飲食店などですと、食品衛生責任者を置かなければいけないというようなことが定められていると思いますけれども、ＥＣに関してもかなりそれに近いような状況に来ているのではないか。要はＥＣセキュリティ責任者のような人を置いてもらうということを明確化していくみたいなことがそろそろ必要なのではないかというような気がしております。それはセキュリティの専門家である必要はおそらくなくて、まさに行政とか業界団体が出すガイドラインをきちんとフォローして、書いてあることを理解して、それに従った対応ができるというぐらいの人でいいのではないかと思うのですけれども、そういう人をきちんと置かない限りは、自前のＥＣはやるべきではないのではないか。置けない場合は、ＰＣＩ　ＤＳＳ等のセキュリティ対策がきちんととられているＥＣモールに入ってくださいというような方向性もそろそろ検討しないといけない時期になっているのではないかという気が、この議論などを見ながら思ったところです。もちろん当面はＥＭＶ３ＤＳなどの導入状況と効果を見ながら、必要性などは考えるべきと思いますが、一つの意見として述べさせていただきました。

それから、ＥＭＶ３ＤＳについてですけれども、期限を切ってということではありますが、それに対する懸念があります。期限について、対応できないところが出てくる事が想定されますが、対応ができない人がいるから延長する、ということはないように、きちんと期限までに導入が徹底されるようにしていただきたいと思います。

あと、先ほど沢田委員もおっしゃったと思いますが、３ＤＳだけで今の400億円近い不

正が完全になくなるとは考えられないと思っております。資料２にも触れてありましたが、トークナイゼーションなど、漏えいしても使えないような、ワンタイムの番号を使うといったアプローチも恐らくすぐ必要になってくるだろうと感じております。なので、今回３ＤＳを導入したことで、それだけやればいいのでしょうというようなムードにはならないように、業界の関係者の方々には意識していただきたいと思います。

３ＤＳについても、リスクベースの認証のところは、やはりカード会社ごとのノウハウであったり技量の差が出る部分だと思っております。なので、ここはきちんと各社ごとに、チャレンジに回している比率とか、拒否した比率とか、フリーで通したけれども、実際にはどのぐらい不正が出たか、チャレンジしたけれども不正がどのぐらい出たかというところを丁寧に検証していただきたいと思います。それをもって、その先にある不正情報の共有のところで、では、どういう情報を共有すべきか、という議論にもつながっていくと思いますので、なるべく丁寧に数字を共有していただければと思います。

私からは以上です。

○岩原委員長　　どうもありがとうございました。

それでは、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。私は、この検討会に参加しておりましたので、この内容自体についてはもろ手を挙げて賛成というところでございますが、検討会でも申し上げたことですけれども、幾つか注意すべき点というか、こういう視点もあるのだぞというところを申し上げたいと思います。

まず１つは、不正利用対策ということで、主として、これは消費者とか利用者の安心・安全という観点が重視されているということは否めないかと思います。ただ一方で、不正利用が行われるということは、犯罪行為が行われ、犯罪者に利得を得させているというものである。このような状態を放置していいはずがないというのが一つ。

もう一つは、不正利用というのは結局カード会員とは違う人が使えてしまうということです。御承知のように、クレジットカードの発行契約を締結したときには、取引時確認を行いなさいと犯収法上義務づけられ、本人特定事項を確認するということをやっているわけですが、それをやっても別の人が使えてしまうという環境が放置されていたら、マネロンを防ぐという観点からも、非常に意味が薄くなってしまう。そういう意味では、不正利用対策というのは、一面でマネロンの観点というのも出てくるはずなのです。

これらの観点抜きに、被害が出る出ないという議論だけをやってしまうと、例えば先ほ

ど沢田さんからＥＣ加盟店のところに損失が行くのですという話になるわけですけれども、それでは、実際に不正利用による被害が顕在化したらそれはＥＣ加盟店のところに行くかもしれません。でも、多くのＥＣ加盟店はそもそも不正利用が起きない。だとすると、対策のコストと被害が発生する危険性とを両てんびんにかけた場合、どう選択するかという、その経済合理性の話だけになってしまう。この話は決して経済合理性だけで語ってはいけない世界の話である。セキュリティも含めて、そういう観点でいうと、被害が顕在化した場合と、その対策コストを見比べてどうこうではなくて、防ぐということが大前提に来るべき話であるということを確認すべきだと思っております。

その観点から、ＥＭＶ３ＤＳの導入が実質義務化ではないかという沢田委員の御指摘などもありましたけれども、これは今やるしかない、当面できる、しかも、かご落ち等の危険性なども考慮して、なるべく商取引に悪影響を与えない、利用阻害を発生させない手法として今考えられるいい方法ということで選び取られているわけですから、タイムリーになるべく迅速にこれを進めていくべきだろうと思っております。

その上で、先ほど田中委員からも御指摘がありましたけれども、今後を考えていった場合に、ＥＭＶ３ＤＳだけで足りるというものではありません。そういう観点からすると、トークナイゼーションですとか、いろいろ今後活用できる技術も多面的に見ていくべきだろうと思っております。これらを進めていく上で、一律のルールベースで画一的に処理をしますということになると、ＥＣ加盟店さんも多い、ＰＳＰも多い、そしてトランザクションの件数も多いということになりますから、これはかなりな労力、負担ということになってきて、結果としてビジネスを阻害するという側面も出てくるかと思います。効果的、効率的な対策を取るというところでいくと、やはりリスクベースというものを大前提に置くしかない。

そのリスクベースというときに、リスクのアセスメントが実は今、情報が十分でない。特にＥＣ加盟店さんなどを含めて見ていったときに、リスクアセスメントの情報が十分でないということになりますので、当面取る対策の中でどんどん情報を集積し、リスクアセスメントのための基礎を固めていくというのがまず先にやらなければいけないことだろうと思っております。そのために行政の役割というのは非常に重要だと思っております。

もう一点、今回クレジットカードという分野について、ここまでの対策を入れましょうという話になったわけですが、ＥＣでの決済というのはほかにいろいろツールが出てきております。これらのツール、クレジットカードのほうはセキュリティ対策を入れた、不正

利用対策を入れた。では、ほかのところはどうなのだという話になっていって、弱いところが狙われるという関係が出てきますから、やはり今回取りまとめた知見というのは、経済産業省、あるいはクレジットカードという分野だけでなくて、他の隣接業界の方にも参考にしていただき、あるいは金融庁その他においても活用していただくということを積極的に進めるべきでないかと思っております。ありがとうございました。

○岩原委員長　　どうもありがとうございました。

それでは、次に長谷川委員、お願いいたします。

○長谷川委員　　ＮＡＣＳの長谷川でございます。

私はこのセキュリティ検討会のメンバーでした。この検討会を通じて、各事業者さんの対策などは議論されましたので、ぜひ実施していただきたいと思います。私は、消費者側の視点から意見を申し上げたいと思います。

カード情報の漏えい事案があったときですけれども、消費者としては、先ほどどなたかがおっしゃっていたように、クレジットカードの仕組みというのはとても複雑で、どのようになっているかが分からないので、自分の被害が今後どうなるかというのは不安になります。流出したという事実とともに、今後どのような対策を消費者が取っていけばいいかということを適切に伝えていただければと思います。

消費者センターではクレジットカードの不正利用の相談を時々受けますけれども、消費者としては、一旦クレジットの請求を止めてほしいと伝えていますが、最近は家族の利用かもしれないということで、調査はしますけれども請求は止めませんというカード会社さんもありました。消費者としては予定外の出費で支払えないですとか、今後返金されるか不安という方もいますので、不正利用という申出があった場合には、調査期間中は請求を保留していただきたいと思います。

また、消費者センターでは消費者の啓発を行っていますが、クレジットカードの明細を小まめに確認するとか、安易にカード番号を入力しない、不審な点があったらすぐにカード会社さんに連絡するなど、啓発活動を行っていきたいと思います。ただ、このような情報が伝わらない消費者の方もいますので、そういう方に対してはどのように啓発をしていったらいいかということは課題だと思っております。

以上です。ありがとうございます。

○岩原委員長　　どうもありがとうございました。

それでは、次に森竹委員、お願いいたします。

○森竹委員　　ＢＳＩの森竹です。

私は、カード会社様、サービスプロバイダー様へのＰＣＩ　ＤＳＳ準拠評価をする立場となりますが、本委員会と検討会にも参加させていただきまして、クレジットカード業界に関わる様々な組織や団体の状況や、対策検討の機会をいただきましたこと、大変感謝しております。今回の報告書内容につきましては、私も検討会参加メンバーとして、ぜひ実行に向けて進めていただきたいと考えております。

現状の課題改善に向けた３つの取組方針はとても重要だと考えておりまして、現状対応の運用継続の確実化と、やはり範囲の明確化、また新たに取り組まなければならないことをいかに実行していくかというところの計画策定、プライオリティーづけ、またその実行確認や効果測定がすごく重要だと考えております。

また、具体的措置に関わることといたしましては、報告書の11ページ、14ページに関わることについて意見を述べさせていただきたいと思います。

最初に、ＥＣ加盟店においては、非保持化が進みまして、外部サービスを組み合わせて顧客に提供することが増えている状況かと思いますけれども、安心・安全に消費者に利用していただくためには、その組み合わせたサービスを含めた総合的なセキュリティ対策の実施状況を評価していくことが重要だと考えております。また、その評価結果と漏えい事案の発生原因との関係を分析していただきたいとも考えております。

それから、ＰＣＩ　ＤＳＳ準拠評価をする立場としましては、本委員会や検討会の情報を踏まえたセキュリティ対策が強化された新バージョンへの対応促進に向けて取り組んでいきたいと考えております。また、法令チェックサービスに昨年後半から関わってきたということもございまして、事案の発生傾向から今回の検討結果の対応を確実に実行していくということが非常に重要だということを実感しております。

例えば、発生事案の中には、ＥＣ加盟店様のほうがレンタルサーバーを利用され、ほかの外部サービスも利用され、アプリケーションは別ベンダーさんに実施していただいている。そういった運用をしながらのサービス提供をしていらっしゃる。このようなときに漏えい事案が発生したときには、漏えい事案を分析するには情報を取得するということが必要になってくるのですけれども、組合せしたことによって、契約内容とかそういったところによりまして、タイムリーな情報を収集することが難しいというようなケースもございます。

最後なのですけれども、漏えい対策、不正防止、利用者の本人認証の強化、発生事案の

タイムリーな連絡、責任範囲の明確化、状況に応じた、策定した計画のプライオリティーの見直しなども含めて、このような業界横断の措置機関の連携により、総合的に実行、運用していくことが、この実行を成功させるところのキーになるのではないかと考えております。

私からは以上となります。ありがとうございました。

○岩原委員長　　どうもありがとうございました。

それでは、最後に、検討会の座長をお務めいただきました中川委員より御発言をお願いしたいと思います。

○中川委員　　中川です。

今回の検討会においては、私、取りまとめに関わりまして、２つほど大きな気づきといいますか、あるいは業界に対するメッセージがあったのかなと思います。

１つは、Ｅコマースに関わるということはかなり危険なことだという認識が関係者にあまりないということです。物理的な店舗、たとえばパン屋さんを開くとか、美容室を開く。これはいろいろ法規制があって大変ではあるのですけれども、それに比べるとＥコマースのほうは比較的楽といいますか、少しネットのことが分かっていれば誰でもできるという気安さ、手軽さがすごく強調されいて、それでここまで広がってきたと思うのです。しかし、そこに非常に大きな落とし穴があったかなと思うわけです。ＥＣ加盟店だけではなくて、そこに関与してくるＰＳＰの皆さんもそうだと思うのですけれども、ネットないしプログラムのテクニックさえあれば、何とかなるというところがあって、そこの意識転換を図らないとセキュリティの改善はできないというところが一つ大きな気づきだったと思います。

先ほど沢田委員でしたか、ＥＣ加盟店それぞれに工夫しているので、ＥＭＶ３ＤＳを原則として一律にせよというのは厳し過ぎるのではないかという御指摘はございましたけれども、そこのところの意識がこれで十分なのかという指摘をしているつもりでいます。

それから、田中委員から御提案のあった、ジャストアイデアということでありましたけれども、ＥＣセキュリティ責任者を置いてはどうかというのは、なるほどと思いながら伺いました。そのぐらいの体制は組んでいただかないと、Ｅコマースのとても危険な世界をわたっていけないと思います。資料２でいくと左側になりますか、漏えい防止のＥＣ加盟店にどのような義務を設けるのかというところの一つのヒントとして、そのような対話ができる人、リテラシーが最低限ある人というのは必ず置いていただくということはあり得

べきだと思いました。

もう一点ですが、そうであるがゆえに、現在の割販法の仕組みであるアクワイアラーがいわばゲートキーパーとして規制するという仕組み、これは基本的には対面でのクレジットカードの世界での安全、セキュリティの確保の方法であったわけですけれども、やはりＥコマースになると、これが、いろいろな意味でうまく機能しないということです。アクワイアラーに対する過重負担、あるいはそもそもできないことを求めることになるかもしれないという意味で、大きく法規制の在り方全体を考え直していく必要があるのではないか。その一環として、ＰＳＰに対してどのような役割を果たしていただくよう規制していくかという問題も出てくる。そうすると、ＰＳＰだから何か義務づければいいという単純な話ではなくて、その範囲というか実態もよく分からないところもありますので、そういった意味で法制上の考え直しは、継続的検討事項になっておりますけれども、これはすぐにやらなければいけない継続的検討事項だと思っております。

今回、全体をすぐにやる項目と継続的検討事項の２つの項目に分けました。課長から２段ロケットという言葉を先ほど言っていただきました。２段目の継続的検討事項というのは、いつかやるのではなくて、これはすぐにやらなければいけない。ただ、法制を見直すという話がほとんどで、場合によっては根本的に変えなければいけないという覚悟が必要ですので、準備に時間がかかる。その意味で継続的という言葉を使っているわけであります。先ほど岩下委員でしたか、メタップスの深刻さに対して継続的課題というのは少し遅いのではないか、あるいはソフトローに委ねているのではないかということでございましたが、まさに深刻であるがために、あるいは対応の仕方がなかなか現在の法制度はうまくいかないということから、時間がかかるけれども、これはやらなければいけないということで、それが継続的検討事項の趣旨であると理解しております。

最後に、感想です。二村委員がおっしゃったマネロンの関係は非常に重要で、今回検討会ではこれ自体は議論の項目にしなかったのですけれども、資料２の右側のⅢの(2)警察等との連携というところで少し話題になりました。これは犯収法ですから警察庁の所管ではあるのですけれども、その辺りについて、経産省から知見を出して、犯収法をもう少し有効に機能させる、もっと効果的にする方法の知恵がないかという形での協議ができないかというような話は検討会でしたところであります。

私からは以上です。

○岩原委員長　　どうもありがとうございました。

それでは、ただいま各委員からいただきました御指摘や御質問につきまして、事務局及び、業界に係る事項については業界からお答えをいただきたいと思います。

まず、田中委員の御質問に対しまして、クレジット取引セキュリティ対策協議会から回答していただければと思います。よろしくお願いします。

○島貫オブザーバー（クレジット取引セキュリティ対策協議会）　議長、ありがとうございます。こちらの声は聞こえておりますでしょうか。

○岩原委員長　聞こえております。

○島貫オブザーバー（クレジット取引セキュリティ対策協議会）　クレジット取引セキュリティ対策協議会の三菱ＵＦＪニコスの島貫でございます。私から、田中委員からの御質問に対して回答させていただきます。

御質問は２つあったと認識しております。まずは、ＥＭＶ３ＤＳの現在の状況だと認識しておりますが、委員御指摘のように、昨年10月に前バージョンの1.0がサンセットになりまして、現行のＥＭＶ３ＤＳに移行になりました。業界全体としては、今まで導入いただいていた加盟店様がスムーズに移行できるということを最重要、最優先ということで対策しておりまして、おおむねこの10月の切替えにはうまくできているというところでございます。いよいよこれから新規の加盟店様にどんどん導入していくというフェーズに入りまして、業界全体としてそういうかじを切ったところでございます。したがいまして、不正利用被害額の防止というところに具体的にどれだけ寄与しているかというところについては、まだ被害額防止の上乗せにはなっていないというのが実態でございまして、そこはこれからといったところでございます。

２つ目の御質問は、現在協議会で実施しておりますＥＣ加盟店のサイトの脆弱性の確認といったところの試行についての進捗状況ということだと思います。こちらは現在アクワイアラー様、ＰＳＰ様、それから包括加盟店代理契約を担っていらっしゃる事業者様、約250社以上にこの試行に参加いただくように声かけをこちらからいたしました。試行自体は新規の加盟契約時に脆弱性を確認するというような内容でございまして、これ自体はおおむね順調に推移しております。今後はこの脆弱性にプラスしてセキュリティ対策を加盟店様に紹介して、これを取り入れていただくという試行をもう一段高度化いたしまして、さらに試行を継続し、セキュリティ対策の実効性を挙げていきたいというようなことで今取り組んでいるところでございます。

私からの回答は以上でございますが、回答になっておりますでしょうか。

○田中委員　　ありがとうございます。ぜひこれからも推進していっていただければと思います。

○島貫オブザーバー（クレジット取引セキュリティ対策協議会）　　ありがとうございました。

○岩原委員長　　ほかの各委員からの御指摘等について、何か事務局からございますでしょうか。

○刀禰商取引監督課長　　委員長、ありがとうございます。では、事務局の経済産業省から回答させていただければと思います。

まず、各委員から活発に御意見をいただきまして、誠にありがとうございました。冒頭申し上げましたように、この報告書の取組はこれから着実に、速やかに実行していくということが大事であります。ただし、具体的な詳細のところ、まだまだ決まっていない部分もありますので、そういった取組を設計していくに当たって、まず今日は皆様からいただいた意見を参考にさせていただきながら、実行にしっかり反映していきたいと考えております。

全ての御意見に対してコメントということはちょっと差し控えたいと思いますけれども、主立ったところだけ事務局のほうから回答させていただきたいと思います。

まず、中身で申し上げますと、１つ目の柱であるカード情報漏えい防止の左側の枠組みの話で申し上げますと、一部の委員からは、やはり事業者の実態に応じた対策ということの大事さをご指摘いただきました。そういった実態というところになっていくと、今のカード業界は大変複雑ではありますけれども、とりわけ決済代行業者、ＰＳＰの存在感、プレゼンスというのが高まってきている。また、こういった取組については、やはり従来の業界自主的なソフトローだけではなくて、やはりより踏み込んだハードロー的な対応も必要ではないかという話もありました。また、検討会座長を務めていただいた中川委員からは２段階ロケットといっても速やかにやっていく中長期的な課題だということの改めての念押しもございますので、なるべく早く、しっかり実態把握と課題整理に努めて、次の本格的な検討に進めていきたいと思っているところでございます。

あわせて、この業界、様々なプレーヤーが入ってきているという意味では、やはりＥＣ加盟店が実際に活用する対策の中に、外部のベンダー、外部サービスの提供なども最近はどんどん増えてきております。ただ、ここにもやはり様々な品質の違いがございますので、そういった面も踏まえながら総合的に対応していくという形で、このＥＣ加盟店における

安全管理措置、セキュリティ対策というのもしっかり見ていかなければいけないと思っているところでございます。

また、あわせて、左下の漏えい時のインシデント対応の強化ということ、特にこれは消費者の方々との関係でも多くの委員から御意見をいただいたところだと思います。やはり見える化を図っていくこと、それから消費者に対する迅速な情報提供につなげていくということ、もとより、既に個人情報保護法の下でＥＣ加盟店も個人情報保護法に基づく義務を負っていて、インシデント発生時においては報告をしなければいけないとか、様々な一般的義務も負っております。また、今後、割販法のセキュリティーガイドラインに基づいて、ＥＣサイトそのものの自己点検、静寂制対策をしっかりやっていってもらうということでもあるわけでありますけれども、さらに様々な対策を積み上げていくということも引き続き考えなければいけないと思います。その中で、あくまで一例ということではあるかと思いますけれども、セキュリティ責任者を置くなどの様々なアイデアもいただきましたので、こういったところも今後参考にさせていただければと思っております。

また、業界全体でこういった取組をシェアしながら強化していくという観点からは、今日オブザーバーで参加している日本クレジット協会において、サイバー攻撃の対応の被害事例の傾向分析の知見をしっかりと集積して、業界全体で分析能力、それに対する対応をしっかり取っていけるような体制をさらに強化していければと思ってございます。

それから、２つ目の不正利用防止、２本目の柱でありますけれども、ＥＭＶ３ＤＳをまず今後の対策の基本的な柱として今後原則導入していくということであるわけでありますが、またその一方で、これも複数の委員からお話があったように、ＥＭＶ３ＤＳ一本足打法ではない。もちろんこれは対策の、ある種、テストの点数でいけば、100点満点中の60点、優、良、可の可は取れるか分からないけれども、だからといって70点、80点を達成しているわけでもない。そのように私はむしろ理解しておりまして、70点、80点、100点と対策を積み上げていくためには、ＥＭＶ３ＤＳ以外にも様々な手法などを組み合わせながら取り組んでいく。さらには、一部の委員からもお話があったような、トークナイゼーションなど、将来的に考えられる最新の技術知見だとか技術をしっかり取り入れていく、こういう不断の取組も大事なのだろうと思います。

他方で、やはり現実問題、こういった業態は、益々複雑化しており、またこの取組については現場レベルでいろいろ工夫をしながら取り組まれていることもあります。実際にＥＣモールなどにおいては、昨年の秋には一部のＥＣモール、ＥＣ加盟店にも検討会に参加

いただいて、実際にＥＭＶ３ＤＳを先行して導入された方々のヒアリングも実施したところでありますけれども、他方で、そういったＥＭＶ３ＤＳと同等の機能を果たし得る、いわばオルタナティブとなっていくような手法などについても、今後提案されてくるものがあれば、そういったものの中味をしっかり検証して、このガイドラインの中で運用にしっかり許容していくような工夫も引き続き継続的にしなければならないのかなと思っております。

ただ、その際、あくまでもクレジットのセキュリティ協議会は、そもそも2015年に創設以来、まさにマルチステークホルダー、様々なプレーヤーがしっかりそれぞれの立場での利害も踏まえながら調整していく、そういった場としてつくってきました。したがって、先ほどあったような例外的な措置についても、そういった場を通じて事業者の声をなるべく広く聞いていくということが大事だと思いますし、ＥＣモールなど、従来以上に様々なプレーヤーの意見を聞いていく範囲をより広げていくとか、そういった工夫もしていかなければいけないのかなと思っています。

他方で、ＥＣ加盟店への周知の仕方ということについては、パブリックコメントというような御意見もありました。また一方で、アクワイアラー自身の責任として、加盟店としっかりそういったコミュニケーションを取っていくということも本来的に求められるのではないかと思っております。硬い話になってしまうのですけれども、クレジットカード・セキュリティガイドラインそのものは、国の機関というよりは、協議会そのもので策定されているものですから、行政がパブリックコメントを行うというような形は、プロセス的にはなかなかなじまない世界ではあるのです。とはいえ、広くＥＣ加盟店の意見を聞くべきではないか、あるいは様々な工夫をされているＥＣモールの意見を聞くべきではないかというような御趣旨については、しっかり協議会での取組などに、今後も聞いていくプロセスとか、関係者を入れていくとかといったところで工夫をしていければと思っているところでございます。

最後の３つ目の柱、消費者啓発ということについても、これも様々な関係機関の御協力を得ながらやっていかなければいけないところでありますが、行政自身も、例えば政府広報など、業界と連携した大きなキャンペーンなどを今後展開していかなければいけないかなということも思っておりますので、引き続き消費者関係機関とも連携をして取組をさせていただければと思っています。

最後、全体を通してということでありますけれども、この取組はあくまでもクレジット

カード決済、ＥＣ決済というところでの取組でありましたが、当然、キャッシュレスとして、ＥＣ決済の手法は、クレジットカード以外にも、デビットカードや前払いの何とかペイといったようなツールも様々あります。したがって、こういったところについては、今般の検討会に、金融庁にオブザーバーで参加していただいておりましたけれども、引き続き経産省と金融庁が連携して、キャッシュレス全体、また、中川委員のお話でいけば、ＥＣ全体の取組にしっかり反映させていくということで、行政機関の連携を進めていければと思っているところでございます。

ちょっとお答えになっていない部分もあるかと思いますけれども、まず、経産省、事務局からの回答とさせていただきます。

○岩原委員長　　どうもありがとうございました。

それでは、日本クレジット協会からも御発言いただければと思います。よろしくお願いします。

○河野オブザーバー（日本クレジット協会）　　議長、ありがとうございます。日本クレジット協会・河野でございます。

本日御議論を聞いておりまして、まず、クレジット業界、またはクレジット業界関係の取組としてお示しいただきました事項につきましては、今後しっかりと取り組んでまいりたいと考えてございます。また、クレジットカード業界、クレジット業界につきましては、日頃の業務においても、消費者の皆様、また関係事業者の皆様からの御指摘については真摯に受け止めて取り組んでまいっておりますし、今後も引き続き取り組んでまいりたいと考えております。

また、御承知のとおりでございますけれども、本日の委員の皆様からの御意見または御報告にもありましたとおり、昨今、クレジットカード決済については、非常に多くのプレーヤーの皆様が参画して、現在の決済スキームを構築してございます。そのために、一定の業界だけがセキュリティに取り組めばこの不正が防げるというものではなくて、全ての各プレーヤーそれぞれに必要な対策を講じることで、このセキュリティのレベルが底上げしていくということが必要なのだろうと私どもも思っております。

その観点では、先ほどもお話がございましたけれども、私ども日本クレジット協会は、マルチステークホルダープロセスによる施策の取りまとめを行うクレジット取引セキュリティ対策協議会の事務局という側面と、業の振興及び自主規制団体であるクレジット業界の団体として、関係する皆様と共に、引き続き、実務運用の実効性の観点も踏まえながら

も、施策に取り組んでまいりたいと思っておりますので、関係各位の皆様の御協力も賜ればと思っております。

私からは以上です。

○岩原委員長　　どうもありがとうございました。

それでは、引き続き、クレジット取引セキュリティ対策協議会からも全般的な点について御発言いただければと思います。よろしくお願いします。

○島貫オブザーバー（クレジット取引セキュリティ対策協議会）　　議長、ありがとうございます。引き続き、クレジット取引セキュリティ対策協議会から一言コメントさせていただきます。

本日は、大変活発な御議論ありがとうございました。協議会といたしましては、今回の検討会の報告書に記載されております対策につきましては、来年度４月からは、外部の専門家の知見をいただきながら、具体的なセキュリティ対策に落とし込んで、これを実施していくフェーズに入るという予定でございます。まずは効果測定を並行して行いながら、トライアル、試行という形態で実施する方針でございます。ただ、本日の御議論でもありましたように、一つ一つの対策についての効果は限定的な部分もございます。したがいまして、複合的に様々な対策を組み合わせて実施し、実効性を上げていくというスタンスでトライアルしていきたいと思っております。これに当たりましては、御指摘のように、加盟店様を含め、多くのプレーヤーの皆様からの御意見を真摯に受け止めながら実施してまいりたいと思いますので、引き続きよろしくお願いいたします。ありがとうございました。

○岩原委員長　　どうもありがとうございました。

最後に、私から一言御発言させていただきたいと思います。

各委員の皆様には、大変闊達な御意見を賜り、かつ非常に鋭い御指摘をいろいろ賜ったと承知しております。この不正利用の問題は非常に深刻な問題であります。さらには、単に被害が生じているというだけではなくて、その被害が反社会的な形で利用されるという社会全体にとって脅威であって、単に損益のバランスから対策を考えるのではなくて、社会的な側面からもきちんとした対策を実行する義務があるという御指摘は非常に大事な御指摘だと私は思っております。

そのような観点から、例えばＰＳＰにつきまして、現在のようなソフトロー的な対応ではなく、登録制を採用するなど、ハードローのほうでもきちんと行政的な対応も必要だという御指摘を岩下委員などからいただいたところであります。ＰＳＰに登録制ということ

になりますと、ＰＳＰは決済代行業者でもありますので、金融庁の所管でもあります。そういうことを考えると、省庁間を超えた、まさに横断的な対応を今後検討していく必要があると思います。

一方で、登録制にすればそれできちんと実効的にセキュリティ対策を推進していけるかというと、現在の役所の体制などを考えるとやはり限界があるということも実際で、本当に実効的にセキュリティ対策がなされていくようにするためにはどうしたらいいか、いろいろ工夫する必要がある。そういう点では、先ほどのセキュリティ対策の責任者をそれぞれのところ、例えばＥＣ加盟店などでも設けていただくというようないろいろな工夫をしていく必要があるという御指摘も大変貴重な御指摘だったと思います。

そして、二村委員の御指摘は非常に鋭いと思います。実は私、今日、金融機関に対するマネーロンダリング規制について講演することになっていまして、明日は法務省と商業登記を使ったマネーロンダリング対策の政策を検討することになっています。例のＦＡＴＦの日本に対する審査には非常に厳しいことが書かれておりまして、特に金融機関以外の当事者に関わるところについて、きちんとした対策の意識がまずないし、何よりも制度の実効性が図られていないということが指摘されています。こういう形の不正利用によって生じた利益が闇の世界に流れていくということをぜひ防がないと、国際的にも非常に批判にさらされることになるわけで、そういうことを十分考えて対策を取っていっていただければと思います。

本当に今日は熱心な御議論をありがとうございました。

それでは、最後に自由討議といたしまして、クレジットカード決済システムのセキュリティ以外の、割販法や関係業界に係る全般的な御質問や御意見があれば、自由にいただきたいと思います。

御発言の際は、Ｔｅａｍｓのメッセージ欄に発言希望のメッセージをいただきたいと思います。私から指名させていただきます。

さっき私の指摘で１つ忘れたことがありまして、池本委員から御指摘いただきましたが、こういう不正利用が起きたときの損害について、当事者間でどのような責任分担になるかということのルールが整備される必要がある。これも非常に重要な御指摘だと思っておりまして、そういう点も今後検討していただき、そういう私法上のルールが整備されることによって、行政庁が直接いろいろやらなくても、私的なエンフォースメントによってルールが守られていくということも大事だと思っております。私の意見が多くなって恐縮です

が、それでは、自由討議について御意見いただきたいと思います。

池本委員、お願いします。

○池本委員　　池本でございます。発言の機会をいただきありがとうございます。手短に申し上げます。

キャッシュレス決済、特にクレジット決済の課題を広く見ていくと、もちろんこのセキュリティの問題も大きいのですが、消費生活相談の現場、あるいは被害救済に取り組む弁護士の現場の問題意識としては、悪質なサイト業者が無登録の決済代行業者を経由して、海外アクワイアラー経由でクレジット決済をしている。本当に犯罪的なものがいまだに横行しているという問題が１つ。

それから、そういった悪質サイト業者の取引について、イシュアーに対して消費者から苦情の申出をしても、これはあくまで一部のイシュアーなのですが、マンスリークリアは苦情の適切処理の法的な義務はないということを公言して、ほとんど対応してくれないということが少なくありません。ＰＩＯ―ＮＥＴで消費生活センターに寄せられる相談件数、マンスリークリアの相談が2021年度は12万7,000件ですが、その中でも、今申し上げた２つの特徴を有しているものというのはかなりの割合のものを占めていると思います。こういった点は、ぜひ国民生活センターにＰＩＯ―ＮＥＴ情報の分析を含めた報告をしてもらって実態把握をしていただきたい。

その上で、先ほどの２つの論点でいいますと、今回、セキュリティ対策の確保のために決済代行業者の登録制が議論されておりますが、そのときに、セキュリティの対応についての実態を押さえるだけではなくて、加盟店の不適正取引についての調査措置の実行も加えていただくことが必要ではないか。これが１点です。

そして、２点目のマンスリークリアについては、平成28年法改正のときの国会附帯決議でも、まずはマンスリークリアについては、業界の自主規制を促していく。そして、その自主規制の効果を経産省において実態把握した上で、必要に応じて法的義務の必要性の検討も必要だということが指摘されているわけです。ですから、こういった辺りも今後の検討課題としてぜひ位置づけていただきたいと思います。

以上です。

○岩原委員長　　ありがとうございました。

それでは、次に二村委員、お願いします。

○二村委員　　ありがとうございます。先ほど委員長からも御指摘がありましたが、私、

まず一つは、隣接決済サービスとの関係でイコールフィッティングを追求するということをやはり今後も検討すべきだということを申し上げたいと思います。もう一つは国際ブランドとの関係です。

まず１点目、いわゆる横断化法制ということで一時検討しておりましたが、その後、少し中断しております。しかしながら、クレジットカードのサービスだけでなくて、その課題というのは同じようなサービスを提供しているところで同じように生まれてくる。それらについてばらばらの規制をしている、あるいは凸凹の状態を放置していくというのは、やはり効率的でもないし効果的でもない。ということを考えていきますと、どのような形でイコールフィッティングを図っていくかということについて真剣な検討を進めるべきだろう。

ただ、さすがにもう60年もの歴史をクレジットカードというか、信用購入あっせんが持ってしまっているという状態が維持されていますので、即座に何かができるとか、あるいは全部金融庁に持っていけばそれで足りるとかという話ではもちろんないだろうと思っております。少し課題を整理して検討していくということをじっくりと腰を据えてやるべきだろうと思っております。これが１点目。

２点目。特にクレジットカードがそうですけれども、基本的な取引の構造あるいは形態は、国際ブランドのルールによってつくられている。利害調整もその中で行われるというのが基本的な構造です。ここを外してルールメイクをしていっても非効率になるだけです。国際ブランドがどのように動いているか、どのようなルールを持っているか、どのようなサービスを提供しているかということについて十分に把握しないままドメスティックなルールを決めていくということでは、やはり限界があるだろうと思っております。その観点で、国際ブランドと定期的な十分な意見交換、情報共有を進めていくのが第一歩。第二歩は、国際ブランドに対するレギュレーションというものをどのように考えるか、こういう辺りを検討すべきだろうと思っております。ありがとうございます。

○岩原委員長　　ありがとうございました。

それでは、次に沢田委員、お願いします。

○沢田委員　　ありがとうございます。委員長のおまとめと今の先生方のお話も伺いまして、セキュリティ対策を含めた決済サービスの今後の在り方というのは、本当に包括的に考えなければいけない問題だと私も思います。同様に、Ｅコマースの今後の在り方も真面目に考える必要があります。簡単に決済ができるということも含めて、Ｅコマースの発展

が世の中の役に立つという前提で、手軽な点も許容する形で促進されてきたのは、二十数年前の経産省の政策方針でもありました。それによってクレジットカードの流通量拡大も進んできたものと思います。ただ、それが見直しの時期に来ているというのも事実と思いますので、包括的にいろいろなことを議論する必要があるということは全く同感でございます。

ちょっとそれとは違う話を１点だけさせていただきたいのですが、参考資料の工程表の中にフィッシングサイトの取締りの話が出てくるのですが、先ほど二村委員から御指摘があったとおり、フィッシングだけでなく、クレジットカード番号の不正利用も犯罪です。割賦販売法49条の２で罰則が科されているので、これをちゃんと執行していただきたいというのが行政に対する要望の一つです。

警察との連携の話も御紹介いただきましたけれども、不正利用者を取り締まるという観点がちょっと欠けているようにも思いました。実行役は闇バイトで集められた普通の人かもしれないですけれども、その背後には、御指摘があったように反社組織があるかもしれません。自分たちが被害を防げればいいということではなく、ちゃんと捕まえないといけない。捕まえることによって、カード不正利用をしても経済的な利益もないどころか逮捕されるという状態をつくらないといけないと思っております。そのため、ＥＣ事業者と警察との間で情報共有の試みを始めようとしています。なぜならＥＣ加盟店は不正利用で狙われる立場なので、実行役の情報を持っているわけです。属性・行動分析をすることによって情報がたまっています。配送先住所も持っています。この枠組みを進めるにあたり、経産省もぜひ入っていただきたい。不正利用の実態がお分かりいただけると思います。それが１点。

もう一つは、石井委員におっしゃっていただいて大変心強く思ったのですが、そういう情報を共有するということは不正抑止に有効である半面、組織をまたがった個人データの共有だということ。それ以前に、属性・行動分析をするために個人データを使うということを利用目的として明示する必要もありますし、それも含めて、個人情報保護法との関係、個人情報でなかったとしても、利用者のデータであれば、改正電気通信事業法の外部送信規律も課されることになりましたので、そういった他の法律との関係をぜひ整理していただきたいというのが行政への要望です。

以上です。ありがとうございます。

○岩原委員長　　ありがとうございます。先ほどのＦＡＴＦの日本に対する審査では、日

本の司法当局の起訴が非常に消極的だと厳しく指摘されています。今の御意見はもっともだと思って伺いました。

それでは、次に岩下委員、お願いします。

○岩下委員　　岩下でございます。クイックに御発言させていただきます。

今、何人かの委員から、この種の対応に対する国際的な情報共有であるとか、情報が必要だという議論があったように思います。私がこの話に以前から関係しておりますのは、ＩＳＯのＴＣ68という委員会の国内の事務局長をしばらくやっていたためです。実はこれは世界的な銀行の集まりなのですが、海外では銀行がクレジットカードを発行していますので、ＩＳＯの国際会議でもクレジットカードの話ばかりしていました。国内のクレジットカード業界がそういうサークルと切れていて、国際ブランドを経由してしか情報が入ってこないのであれば残念です。国内のクレジットカード業界の方々にもそういう部分に直接触れていただくという意味では、こういう国際会議に参加していただくのが良いのではないかと思います。

もう一つ、クレジットカードでは番号が単独で機能してしまっているのでいろいろな犯罪が起こりがちです。最近の様々なＥＣ決済のツールにおいては、番号だけで動くものは存在しません。それらは、きちんとシステム的に連動して、動的な認証を行っていますので、クレジットカードのような巨額の犯罪被害は発生していません。また、インターネットバンキングのように提供者が利用環境をある程度限定できる状態で認証の仕組みを入れているのも同様です。そういう意味で、やはりクレジットカードは非常に犯罪が起きやすい構造が広まってしまったということを踏まえて、今後の規制体系、あるいは監督当局の技術面も含めての要員の体制整備をぜひ検討していただきたいと思います。

私からは以上です。

○岩原委員長　　どうもありがとうございました。よろしゅうございますか、ほかの皆様。

特に御意見がないようでございましたが、ただいまの御質問や御意見に対し、事務局から何か補足があれば承りたいと思いますが、いかがでしょうか。

○刀禰商取引監督課長　　委員長、ありがとうございます。事務局からは特に意見はございません。各委員の皆様、意見をいただきまして、どうもありがとうございます。

○岩原委員長　　それでは、もう時間になっておりますので、ここで本日の議論を区切りたいと存じます。本日は闊達な御議論をいただき、誠にありがとうございました。

今日出ました各委員の御指摘等を踏まえて、ぜひ事務局のほうで今後施策を進め、また

立法が必要な問題等については、そちらのほうの検討を進めていただきたいと思います。

それでは、事務局より事務連絡等についてお願いいたしたいと思いします。

○刀禰商取引監督課長　　岩原委員長、議事進行いただきまして、どうもありがとうございました。また、各委員の皆様におかれましては、本日活発な御意見を頂戴いたしまして、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、事務局におきまして作成の上、各委員の皆様に御確認いただいた後、当省のウェブサイトにおいて公表する予定でございます。

また、今後につきましては、本日いただきました御意見を踏まえまして、改めて事務局において整理させていただき、岩原委員長にも御相談をさせていただいて、来年度の次の運営に反映させていきたいと考えているところでございます。

再び開催ということになりましたら、事前に事務局より適宜日程調整をさせていただければと思っております。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、お忙しいところ熱心に御議論いただき、誠にありがとうございました。

――了――