不適正利用対策に関するワーキンググループ（第６回）

令和６年６月20日

【小澤利用環境課課長補佐】　定刻になりましたので、「不適正利用対策に関するワーキンググループ」第６回会合を開催いたします。事務局の小澤でございます。

事務局よりウェブ会議開催上の注意事項について御案内をさせていただきます。本日の会合の傍聴者につきましては、ウェブ会議システムによる音声及び資料投映のみでの傍聴とさせていただいております。事務局において傍聴者は発言ができない設定とさせていただいておりますので、音声設定を変更しないようにお願いいたします。また、本日の会合につきましては、記録のために録画をさせていただきます。

構成員の皆様におかれましては、ハウリングや雑音混入防止のため、発言時以外はマイクをミュートにしていただいて、映像もオフにしていただきますようお願いいたします。御発言を希望される際は、事前にチャット欄に発言した旨を書き込んでいただきまして、それを見て主査から発言を御指名いただくという方式で進めさせていただければと思います。御発言をする際にはマイクをオンにして、できれば映像もオンにして御発言いただければと思います。御発言が終わりましたら、いずれもオフに戻していただくようにお願いします。接続に不具合がある場合は、速やかに再接続を試していただくようにお願いいたします。その他、チャット機能等で随時事務局や主査宛てに連絡を頂ければ対応をさせていただきます。

それでは、これ以降の議事進行は、大谷主査にお願いしたいと思います

【大谷主査】　本日は、まず事務局から御説明いただきまして、その後に質疑応答、そして意見交換をさせていただければと思います。

それでは、事務局、お願いいたします。

【小澤利用環境課課長補佐】　資料６－１「携帯電話不正利用防止法に基づく本人確認の見直しの方向性（案）」について御説明をさせていただければと思います。

第５回ワーキンググループにおきまして、構成員から各条文ごとの論点につきまして御意見を頂いたところです。

１つ目、「対面における電子的な確認方法」の在り方についてです。マイナンバーカードに係る機能のスマートフォンへの搭載というものが、法改正によって来年の春に施行される見込みで、特に辻先生からアメリカの技術的な状況なども御紹介いただき、こういっ

た新しいものの活用もぜひ進めるべきだという御意見を頂きました。

また、対面におけるICチップの読み取りによる確認方法の導入については、単にICチップを読み取ることを要件とするのではなく、ICチップに格納された本人特定事項、氏名、住所、生年月日を券面情報と照合するなど、セキュアなICチップの中の情報をしっかり確認する方法にすべきであるという御意見を頂きました。

２つ目、「非電子的な確認方法の在り方」について、何らかのやむを得ない理由でICチップ付きの本人確認書類を所持できないような場合に、代替手段として非電子的な確認方法を認めることが考えられるのではないかと各先生からご意見を頂きました。

特に非電子的確認方法は、あくまで例外的な確認方法としてやむを得ない場合に限り補充的に利用できるという位置づけにすべきという御意見を頂いたと思っております。

また、その非電子的確認方法の具体的な方法の検討に当たっては、電子的な確認方法と比較してこの悪用のリスクが高くならないように、継続的な検証を行う必要があるという御意見を頂きました。これを留意していきたいと思います。

３つ目、「他の事業者への依拠の在り方」について、皆様から、他の事業者への依拠の検討に当たっては、当該事業者における身元確認レベルが一定以上であることを確認できた場合に限り依拠を行うこととすべきではないか、例えば、公的個人認証で確認済みであることを確認できたような場合に依拠を行うということにすべきでないかという御意見を賜りました。

このような動きを踏まえ、携帯電話不正利用防止法の本人確認方法の見直しの方向性（案）ということで１枚にまとめさせていただいております。参考資料として「国民を詐欺から守るための総合対策　概要」をつけておりますが、こちらにも一部盛り込まれたものがございますので、そちらを参照いただきつつ、この方向性（案）を見ていただければと思っております。

１番目１つめ、「①自然人の本人確認方法」について、非対面における券面を確認する方法、具体的には、写しの送付、本人確認書類の写真を撮って送って郵便を送る方式と、eKYC厚みの方式、この２つを廃止しましょうと。

２つ目、対面における電子的な確認方法の義務化は、今回、「国民を詐欺から守るための総合対策」の本文にも盛り込まれ、参考資料の３ページと５ページのところに記載がありますが、対面における電子的な確認方法、ICチップの読み取り等を求めるということを盛り込んでおります。これは、特定事項伝達型本人限定受取郵便という、非対面でありな

がら疑似的に対面の確認をする、玄関口などで本人確認書類の提示を受ける仕組みですけれども、こちらについても併せてICチップの読み取りなどの電子的確認方法を求めるということで、「含む」と書かせていただいております。

３つ目、カード代替電磁的記録です。マイナンバーカード機能のスマートフォンへの搭載の部分です。こちらの活用についても新たに確認方法として導入すべきであると入れております。

４つ目、例外的な確認方法としての非電子的な確認方法の存置について、具体的な方法は犯収法や他法令、他業界との調整もありますことから記載してませんが、盛り込ませていただいております。

２番目、「②法人の本人確認方法」であります。各社から御提案いただきました犯収法で認められた登記情報提供サービスとの連携による確認方法の導入、また、法人の契約担当者、法令上で言うと代表者等の本人確認における電子証明書の導入、こちらも盛り込みたいと思っております。

３番目、「③過去の確認結果への依拠」については、先ほども身元確認レベルが一定以上であることを確認した場合ということがございましたので、公的個人認証で本人確認を実施済みの事業者に対する依拠を導入できないかということを盛り込んでおります。その際、併せて当人認証レベルをしっかり確保すべきであるという御意見がございましたので、多要素認証等の認証レベル、第４回の資料で、身元確認レベル、当人認証レベルが、もともとアメリカの基準を取り込んで、行政手続におけるオンラインの本人確認の手法に関するガイドラインの中でも明示されている、レベル２以上を求めるべきという御意見がございましたので盛り込んでおります。

また、継続的顧客管理による確認記録の更新は、他人の確認結果の依拠というよりは、２回線目契約などを想定していますが、住所変更などを行ったときに確認記録に反映する仕組みが携帯法に今ありませんので、こちらのほうを入れまして、継続的顧客管理をしっかり最新化しているような場合に、過去の情報に依拠できるように改正をできればと思っております。

「④その他の見直し事項」の１つ目は、携帯電話不正利用防止法特有の譲渡時の本人確認、貸与時、レンタルの本人確認においても①から③と同様の見直しをします。

２つ目、電子的確認方法における確認記録への保存の在り方の見直しについて、プライバシーの保護や新たな不正利用のリスクへの対策という観点で、券面情報の写真の写しと

かが転々流通してしまうとよくないので券面を確認する方法を見直すという流れもありますので、券面の画像情報なども確認記録に保存しないようにするといった見直しをできればと思っております。

３つ目、これも携帯法の特有の話で、警察からの求めに基づく契約者確認という、犯罪に使われた携帯電話の本人確認を取り直す制度の確認方法の見直しも図っていきたいと思っております。

４つ目、事業者からのニーズが多いところで、犯罪収益移転防止法との整合性をしっかり確保した上で検討していきましょうということが盛り込まれております。

以上、十分な準備期間を確保した上で省令改正の施行時期を決定していくということにしておりますので、具体的な施行時期やパブリックコメントの時期などは決めておりませんが、犯収法や他業界、他業種との調整状況も鑑みた上で、十分に準備期間を確保して施行時期を決定できればと考えております。

また、この議論の過程で、その他の留意事項についても各構成員から御意見を賜りましたので、留意事項としてまとめております。

１つ目、「デジタルデバイド等への対応」につきまして、デジタル技術の活用が難しい高齢者等の利用者への対応や、災害時、通信障害時の対応としても、別の方法を準備するのではなく、デジタル化した方法に対応できるよう、サポートが必要ではないかという御提案がございましたので、既存のデジタル推進委員や地域におけるデジタル活用のスマートフォン教室といった各種取組がございますので、また、通信事業者様でそういった地域活動をされているところもあると思いますので、そういったところと連携しながら留意していきたいと思っております。

２つ目、「本人確認の意義に係る周知広報」は、携帯電話不正利用防止法の目的や契約時の本人確認の意義・重要性について、特に利用者に対して説明を行う周知広報をしっかり進めるべきという御意見を頂きました。

参考で、携帯電話不正利用防止法の目的規定を引用しましたが、携帯音声通信事業者による契約者の管理体制の整備の促進及び携帯音声通信役務の不正な利用の防止を図るということで、特に不正な利用の防止、犯罪対策です。特殊詐欺や犯罪に使われる携帯電話を防止することが主目的というところをしっかり広報していきたいと考えて盛り込ませていただいております。

後はこれまでの論点の引用、参考情報となっております。

事務局からの説明は以上でございます。

【大谷主査】　ただいまの資料や、かなり報道もされていましたけれども、参考資料の犯罪対策閣僚会議の決定事項の関係も含めまして、質問、質疑、それから意見交換を進めてまいりたいと思います。沢田構成員、よろしくお願いいたします。

【沢田構成員】　おまとめいただきありがとうございました。

見直しの方向性につきましては、異論のないところでございます。４点ほどコメントをさせていただきたいと思います。

１点目は、３ページ、留意事項「デジタルデバイド等への対応」ということで、過去の私の発言を取り入れていただいたと理解しております。ありがとうございます。補足をさせていただきたいのですが、高齢者と災害時で、それぞれ留意すべきことは違うと思います。高齢者などデジタルデバイドに関しましては、デジタルに対応できるようにサポートするというのは御説明いただいたとおりと思います。通信障害のときは、通信しなくてもローカルでできる方法を用意する。大災害で停電が起こったようなときには、読み取り機に非常用のバッテリーを入れておくなどでカバーすべきで、アナログな方法を残すということではないのかなと思いました。

２点目も同じページで、周知広報について、犯罪対策閣僚会議の報道への反応を見て、まだ随分誤解がある、マイナンバーカードへの抵抗感とか、アレルギー反応みたいなものが出てきているように見えました。普及させたいためのごり押しではないかといった声もあり、メディアの取り上げ方にもかなり責任があると思いますが、目的と必要性をきちんと説明していくことが重要と思いました。

３点目、その意味でも、保証レベルについて表にしていただいたのはありがたく、これをかみ砕いて利用者への啓発にも使うべきではないかと思いました。ただ、身元確認レベルは、レベル３でもICチップを読むとまでは言っていないのでしょうか。今後改定される予定などがあるのであれば教えていただきたいです。

４点目、利用者に対して、犯罪対策ということをもう少しかみ砕いて説明する必要があると思います。今までの対面での券面確認やeKYCの厚み方式では偽造を見破れないということをきちんと利用者に対しても言ったほうが良いと思います。

それと、公的個人認証が現時点で最善の選択肢だと、そこは一致されていると思いますが、必ずしもそれ一択ではなくて、合理的な理由があればほかの方法も使えるということ、どんな場合にどこまで認めるかというのは今後の検討かと思いますが、マイナンバーカー

ドをどうしても持つのは嫌だという場合は、自分のスマホに電磁的な記録を入れてもらえれば良いとか、選択肢を提示できるといいのかなと。段階をつけてかもしれませんが、そういう感想を持ちました。

以上４点です。ありがとうございました。

【大谷主査】　沢田構成員、ありがとうございました。本人確認の保証レベルのレベル３については御質問で、事務局の御回答を要するということでよろしいですか。

【沢田構成員】　もし御存じでしたらということで。

【小澤利用環境課課長補佐】　ありがとうございます。本人確認の保証レベルといって、身元確認レベルは、もともとの本人確認書類がどういう性格か、それの偽造がないかという意味で、当人認証レベルは、ICチップなりデジタルの確認としてセキュアな耐タンパー性のあるハードウエアを読みますということですので。今、辻先生がもしかしたら補足してくださるかもしれないです。

【辻構成員】　補足させていただきます。ICカードというのは、当人認証レベルに書いてある耐タンパー性のあるハードウェアのことを言います。重要なのは、ICカードと例えばパスワード、ICカードと何か複数の認証要素による認証、つまり多要素認証で、一般的にはカードのような物理的なもの、もしくはパスワードやPIN番号のようなもの、もしくは生体認証のようなものと、全然異なる性質の要素による認証を組み合わせなければいけない。そういう意味で言うと、暗証番号や生体認証とICカードという物理的なものを組み合わせるのがこの多要素認証ということになっていまして、かつ耐タンパー性のあるハードウェアというのは、ICカードの中に重要な証明書とか鍵を入れておくんですけれども、これは実は取り出すことができないようになっています。我々が使っているスマートフォンやPCは、完全に分解して専用のレーザーを当てたり分析機器を使うと中にある情報を読み取ることができるのです。それはかなり難しいんですけれども、中にある情報が漏れないようにする技術要件が決まっておりまして、これが耐タンパー性です。なので、ICチップは単なるICチップではなくて、外部から何をしても基本的には中を見られない仕様を満たしていることを言って、これがスマートフォンの中に、ICチップとは別にセキュアエレメントという形で入っております。これはこの中の情報を取り出すことができないような、暗号モジュールのようなものが最近のスマートフォンに入っていて、それかICカードなど耐タンパー性のあるハードウェアに重要な情報を保存することが要件になっています。

【沢田構成員】　ありがとうございます。なかなかかみ砕いても難しいということが分

かりました。

【辻構成員】　そうですね、かみ砕いても難しい。こちらに書いてある基準は、米国の標準を作る団体NISTが出しているもので、世界的にこれを参照しているというものです。SP800-63ですね。

【大谷主査】　ありがとうございました。取りまとめのときには、恐らくそのNISTのSP800-63であるとか、耐タンパー性のあるハードウェアに相当するものとしてスマホの中のセキュアエレメントとか、あとはICカードが相当するということを脚注のような形で付け加えていただけますと、理解しやすくなるのではないかと思いますので、事務局にお願いできればと思います。

山根構成員から、よろしくお願いいたします。

【山根構成員】　まず、事務局においては、見直しの方向性（案）のお取りまとめをありがとうございます。見直しの方向性につきましては、特に異論ないといいますか、賛同するところでございます。

１点コメントをさせていただくと、事務局の説明の中でもあった話ではあるんですけれども、この本人確認の方法の見直しを行うということになると、事業者においても相応の負担がかかってくるかなとは思いますので、この準備期間については、事業者の意見も踏まえて、十分な準備期間を確保した上でやっていく必要があるのかなと思っているところでございます。

また、同じような観点から、犯収法との整合性の確保というところも携帯法と犯収法とでその見直しの内容であったりとか、あるいは見直しの時期について変わってきてしまう、違ってきてしまうということになると、そこの対応の負荷というのも余計にかかってしまう部分があるかと思いますので、その辺りの配慮も必要なのではないかなと思っているところでございます。

以上になります。

【大谷主査】　貴重なコメントをありがとうございました。十分な準備期間ということで、ただ、できるだけ早く安全なセキュアな本人確認方法で運用がしっかりできるようにということ、当然のことかなと思っております。ありがとうございます。

私からも一言よろしいでしょうか。

資料の２ページのところの「自然人の本人確認方法」で、例外的な確認方法としての非電子的な確認方法の具体的なその確認方法については、どれをということは明記しないと

いうことではありますけれども、ある程度セキュアなレベルといったものをどこにするのかといったことについては、注記があったほうがより方向性が分かりやすいのかなと思っております。今までの非電子的な確認方法を全て認めるということなのか、あるいは特にセキュアなものに絞り込むのかということもあると思いますので、この点、ある程度クリアに書いていただいたほうがいいのかなと思っております。

星先生、よろしくお願いいたします。

【星構成員】　お取りまとめいただきまして、本当に事務局におかれましてはありがとうございました。また、大谷先生もお疲れさまでございます。

私からも言わずもがなの話ではあるんですけれども、先ほど沢田構成員からもお話がございましたように、その券面による確認ですよね。これは今まで普通にやってきたところなわけですけれども、それがいかにリスキーなことになってきているのかということについて、まだ世間のほうでの理解というのが得られていない中で、それであああいう報道が出ると、結局マイナンバーの普及のほうなんだろう、政府の都合なんだろうみたいな見られ方がされてしまうというところはあるのかなと。要するに、結局犯罪者というのは、身元をいかに分からないようにするツールを入れるかというところで腐心、苦心しているわけで、それが最終的には、いつまでたってもなくならない特殊詐欺であるとか、トクリュウ型の新しい犯罪とか、そういったものにつながっているのだということを、総務省さんの検討会でどこまでそういう犯罪関係のことを書けるかというのはあるのかもしれませんけれども、普通に真面目に生活している人たちにとって跳ね返ってくる話なんだというところは伝わるようにしておかないと、少なくともレクを受けたメディアの方がそういった報道をしていただく形にしないと、ハレーションばかり大きくなってしまうと懸念するところではありました。

あと、今後検討すべき論点、代表者等の本人確認というところで、法人についても、いろいろな人にペーパーカンパニーをつくらせて、そこで飛ばしの携帯電話をつくるやり方も随分増えてきているので、この代表者の本人確認というところも、確かに任意団体や大学の中での組織をつくった場合、なかなか銀行の口座を作れないとか、昔に比べると厳しくなって不便だなと思うことも正直あることはあるんですけれども、残念ながらいつまでたってもなくならない特殊詐欺対策のための１つの大きな柱なのだというところを何とか伝わるような形にしていただけるといいのかなと思った次第です。

もう一つ、その依拠というのを使う中で、いろいろなところでセキュリティレベルを合

わせていかないと、どうしても水は低きに流れる、穴ができているところに行って、結局怪しいものが依拠という形でいつまでも続くみたいなことが万が一にでもできてしまったら、かえってリスキーな話にもなってしまうかと思いますので、そこは犯収法との整合、すり合わせということも含めて、ぜひ御対応をお願いできればと思った次第です。

【大谷主査】　星構成員、ありがとうございました。沢田構成員から頂いている貴重な指摘に加えて、さらに意見を加えていただきまして、ありがとうございます。

確かに、犯罪対策閣僚会議の決定の中に、肝腎のその周知のところがうまく記述されていないというか、たまたまその資料がそうなっているだけかもしれないんですけれども、そこのところは、ぜひメディアの取上げ方も、自分の身を守るために必要なもので、単に便利になるとかそういうものではないんだという周知をしてほしいと私も切に思っているところです。

それでは、中原構成員、よろしくお願いいたします。

【中原構成員】　事務局におかれましては、お取りまとめをしていただきまして、ありがとうございます。

「自然人の本人確認方法」について、非電子的な確認方法を存置するのが現状では必要であるということ、ただ、それはあくまで例外的、補充的なものとして位置づけていく必要があるということについて、私も全く異論のないところでありまして、デジタルだから安心だとは言えないんだろうけれども、非電子的なその方法の危険性が高まっている中では、原則デジタルという方向に向かう必要があると思っています。

今回、３ページに加えていただいたこと、「デジタルデバイド等への対応」、これについては高齢者に関する事柄と災害時に関する事柄で分けて考える必要があるというご意見は、そのとおりだと思います。高齢者の方については、非電子的な方法の存置というよりは、デジタルの方法を利用することへの支援という形でケアをしていくということ、もちろんさらに例外というのは出てき得るにせよ、これは第一に据えるべきだと考えています。

ただ、その原則例外というのは、位置づけを省令の条文上どういうふうにするのかという立法技術の問題があるのだろうと思います。このワーキンググループでも、それから閣僚会議の決定でも、対面におけるICチップの読み取り等の方法を義務づけるという話が他方であって、義務づけるという場合には、それ以外の方法を削除するということでよいのだろうと思いますけれども、非対面の場合に電子的な方法を原則とする、非電子的な方法は例外とするというのは、現状では本人確認の方法を羅列しているだけであり、どのよう

な場合に例外に当たるのかということを定式化するためには、いろいろな要素を考慮して考えていかなければいけないのではないかと思います。

今回のワーキンググループの報告書では、原則例外というような形で提示するというところまでは踏み込まなくて、単に「例外的な確認方法としての非電子的な確認方法の存置」という形にとどめると理解していますけれども、今後、非対面の場合について、幾つかある本人確認方法に優劣をつけるのか、優劣をつけるとすればどういった形で例外性を定式化するか、優劣をつけないとすればどういった形で電子的な方法に誘導していくのかといったことは、考えていくべき課題なのではないかなと思います。

犯収法とのすり合わせという話はありましたけれども、原則例外というのは、それ自体としてなかなか難しい問題を含んでいるのかなと思います。いずれも前回の議論の中で多かれ少なかれ含まれていた事柄だと思いますけれども、改めて指摘させていただく次第です。

【大谷主査】　中原先生、ありがとうございました。ちょうど立法技術という御指摘も頂いたところですので、これまでに頂いた御意見などについて、後ほど事務局からリアクションいただくときに、その点についても触れていただければと思っております。

すみません、仲上構成員からチャットを頂いているのですが、音声デバイスが不調とのことで、コメントを私のほうで読み上げさせていただきます。「日本スマートフォンセキュリティ協会では、キャリアの皆様から御意見を承っております。その中で、今回の対面、非対面における確認方法の変更については、導入すべきステップ、段階をお示しいただき、対応すべき内容やレベル感を明確にしていただきたいという御意見がありました。今後の検討課題かと思いますが」ということです。

貴重な御意見をありがとうございます。これはキャリアの皆様からの御意見ということですね。今後に向けての進め方ということで、先ほど山根構成員から頂戴したコメントにも通ずるところがあるのではないかと思いますので、今後とも、事務局のほうでは積極的に事業者の方ともコミュニケーションを取っていただいていますので、その点をぜひクリアできるところはクリアにしながら進めていくということかと思います。ありがとうございました。

では、ここまでのところを一旦事務局で引き取って整理していただいて、その中でまた御意見とかが出るかもしれないのですが、中間取りまとめにも通ずるところですので、そのまま中間取りまとめの御説明に入っていただければと思います。

【小澤利用環境課課長補佐】　各先生から御意見を頂きまして、ありがとうございます。

まず、デジタルデバイド関係の、特に高齢者の対応と障害時の対応は分かれるというのはおっしゃるとおりでしたので、そこを留意しつつ、大規模な災害の場合、省令の特例措置を設けて、そういう本人確認ができないような場合、一旦猶予して後から本人確認を取り直すことを一時的に認めるケースもあり、能登地震のときも適用しております。大規模な場合はもちろん、一時的に通信が使えないような場合について、事業者側でデジタルで使えるような対応をしてもらうというのもおっしゃるとおりだと思いましたので、施行に当たっては留意をしていきたいと思っております。

山根先生からも、事業者の負担や準備期間の確保についてご意見頂きまして、そこはしっかり留意をして、十分な準備期間を確保するというところを、事業者の意見も聞きながら進めていきたいと思っています。

星先生から、券面の偽変造が増えている中でこういうデジタルの方法を求めていくという背景事情をしっかり周知しないと受け入れてもらえないということは、おっしゃるとおりだと思っていまして、実際、第３回のワーキンググループで、警察庁捜査支援分析管理官様から御紹介いただいた内容について、結構注目いただきまして、お問合せいただくこともありますし、また、デジタル庁からもそういった偽変造の状況について発信されたり、少しずつ御理解いただけるよう進んできているかと思いますが、しっかり制度改正施行に当たっては、準備期間の間は特に周知広報をしていくことが重要かと思っております。

中原先生から、非電子的な方法をどう求めていくのか、対面、非対面の話もあり、既にある非デジタルなものの主要な２つを廃止、残る住民票の写しの原本を送る方式は残すということで、そこが最後残るものかと今のところ考えております。条文上、どういうふうに位置づけるかは、しっかり検討していきたいと思います。

仲上先生からは、その導入すべきステップで、施行時期、準備期間をどうするのかというところですけれども、その条文内容も含めて、しっかり事業者様の準備が整うように進めていきたいと思っております。

また追加の御意見がございましたら頂ければと思います。

引き続いて、資料６－２の御説明をしたいと思います。

今回でワーキンググループは一旦一区切りするということで、「不適正利用対策に関するWG中間取りまとめ（案）」を作らせていただきました。今回、不適正利用対策に関するワーキンググループの議論は、今年の２月からいろいろと進めてまいりまして、最初、親

会の研究会のほうから指示いただいた論点として、３つございました。本人確認の見直しはまさに今議論してきたところで、SMSの話は前半に議論をさせていただいたところ、利用停止スキームは、現在、電気通信番号政策委員会の下で、犯罪対策のワーキンググループが立ち上がっており、こちらのほうで特殊詐欺、犯罪に悪用される電話番号の対策というところを制度的対応も含めて検討をされると伺っておりますので、そちらのほうの検討に合流するということを考えております。

これまで第６回まで議論を重ねてまいりまして、第３回の前半までSMSの話、３回の後半から今回まで本人確認の話を中心に議論をしてまいりました。少しおさらいをさせていただきつつ、特にSMSの話で進捗もございましたので、紹介できればと思います。

初回でマクニカ様から御紹介いただいた資料を引用させていただいていますけれども、SMSの配信は非常に増えて、いろいろな用途で使われるようになってきています。それに伴って、コロナ禍で巣籠もり需要が増えたりいろいろな背景があると思いますけれども、フィッシング詐欺の被害は、クレジットカード番号盗用被害額でかなり増えていまして、これのうちの幾らかはSMS、スミッシングによるものが含まれているだろうと考えております。

SMSの対策に関しては、特に受信者側で分かりにくいところがありますが、携帯電話端末から送られてくるもの、配信事業者経由で法人のプロモーションやSMS認証の形で送られてくるもの、海外の通信事業者から送られてくるようなものがあり、それぞれについて発信元の表示や特性が異なることが、課題、問題意識としてありました。

事務局から初回に仮説として御説明しましたが、各社のヒアリングでも国内携帯電話端末でマルウェアに感染したものからのスミッシングメッセージが大部分を占めているということで、本人の意図に反してSMSが送られてしまうので、これをまず対策しなければならないと考えております。

また、海外でのスミッシング対策の事例として、スミッシングの申告窓口を設けて対応されているということが御紹介されました。こういったものも進めるべきではないかと。日本でも各社それぞれ申告受付をされていて、総務省運用の迷惑メール相談センターでも試行的にSMSの申告を受けてみたところ、それなりに申告が来始めておりますので、ニーズはあるのかなと思っております。

第２回で御説明いただきましたが、各社、SMS数のフィルタリングや端末からの対応を導入いただいておりまして、楽天モバイル様も今年７月から迷惑SMS拒否設定の提供開始

予定とのこと、SMS対策が進んできていると期待しております。

また、各社協調したRCS、プラスメッセージの取組や、キャリア共通番号0005など、周知広報が進んでないというご意見もございましたので、しっかり周知広報していくべきだと考えております。

事業者間の横連携、縦連携をしっかり進めていく観点で、SMS不適正利用対策事業者連絡会を立ち上げ、定期的に情報交換をする場を設けております。

これと関係して、フィッシング対策協議会でも事業者間でスミッシング対策の意見交換のワークショップを何度も開催され、今年６月、フィッシング対策ガイドライン2024年度版が公開されています。引用させていただき、フィッシング対策の要件があり、このうちSMSも柱立てして、事業者側の対策が進むように周知広報・共通認識をつくるための取組をされております。こういったような取組と連携してスミッシング対策をしっかり進めていければと思っております。

おさらいで「マルウェア感染端末からのSMS発信対策」と「SMS配信者・受信者の不適正利用対策」に関する御意見、SMSの不適正利用対策の方向性（案）をまとめてございます。

改めて御紹介しますと、「①マルウェア感染端末の特定・警告の推進」、「②スミッシングメッセージの申告受付の推進」、「③SMS関連事業者による業界ルールの策定」、これは正規のメッセージがしっかり正規のものと分かる形で配信されるよう効果的な対策をということ、さらに「④迷惑SMS対策に係る周知啓発の推進」の４つの事項が盛り込まれております。犯罪対策閣僚会議でまとめられた総合対策でも、SMS不適正利用対策が盛り込まれており、このワーキンググループの議論がまさにインプットされていると思っております。

ここまでがSMS対策の話であります。

後半は、携帯電話不適正利用防止法の本人確認の見直しの議論でございます。前半に詳しくご説明したので、概略にさせていただきますが、同法に基づく本人確認義務があり、いろいろな方法が省令で定められております。利用できる本人確認書類もその方法に応じて各種規定されております。

昨年６月のデジタル重点計画に基づいて、非対面の本人確認方法の見直しから先行して特に事業者さんと議論を進めてまいりまして、こういう見直し方針にしていきましょうというものが第３回で事務局から御説明した内容になります。

先ほど中原先生から御提案いただいたところに関連しますが、非対面については、eKYCの厚み方式（ハ方式）と、写し＋転送不要郵便等（ヘ方式）の２つを廃止しますという方

針を発表しております。この２つは、いずれも券面の画像を目で見て確認する方法で、残りのICチップを読み取るeKYC、電子証明書、公的個人認証、特定事項伝達型本人限定受取郵便、先ほど言いましたように疑似対面の方法としてICチップを読み取る方法を求めることにしておりますので、原本＋転送不要郵便が非電子的な方法として残る１つかと思っております。対面の提示は、第３回では検討中でしたが、今回の取りまとめで方針を決定していくことになろうかと思っております。

スケジュールとしては、昨年のデジタル重点計画で示されておりますけれども、今年度中に省令案についてパブリックコメントを行うことが決められております。

「自然人の本人確認方法」や「法人の本人確認方法」、「他の事業者への依拠」、「その他の論点」について御意見を頂きまして、条文ごとに想定される論点を記載させていただいております。こちらについても、省令改正案を作成していく際にしっかり留意していきたいと思っております。

留意事項として「デジタルデバイド等への対応」や「本人確認の意義に係る周知広報」、券面への偽変造のリスクの周知広報も併せて入れるのかと思っております。

事務局からの説明は以上になります。よろしくお願いします。

【大谷主査】　立派な中間取りまとめ（案）の御説明もしていただきまして、ありがとうございました。それでは、資料６－１、６－２を含めまして、御意見、御質問等を頂ければと思いますが、いかがでございますか。

それでは、沢田構成員、お願いいたします。

【沢田構成員】　御説明をありがとうございます。

スミッシング対策につきましてもまとめていただき、アップデートもいただきまして、ありがとうございます。方向性にもちろん異論はございません。

関係する事業者さんの間でやれることをいろいろやっていただいていると理解をいたしました。特に13ページにつけていただいたフィッシング対策ガイドラインにスミッシング対策もしっかり入れ込んでいただいたたというのは、本当にありがたいことですし、利用者にも啓発しなければいけないと思いますので、その啓発の資料としても使えるのではないかなと思いました。

その上で、１つは、当初少しだけ議論になっていたかなと思うのですが、スミッシング対策と通信の秘密との関係も含めて、現在は制度的対応が必要なことというのは当面ないということでいいのか。

もう１点は、利用者への啓発ということで、マルウェア感染をしている端末を持っている人に教えてあげるという話があり、感染していることは、通常は気づかないという前提でお話しいただいていますけれども、気づくケースはないのでしょうか。

例えば、自分が感染していろいろな人に変なSMSを送ってしまっていたら、送った相手から、あなたの番号から変なメッセージが来たよと教えてもらうこともあるのではないかと思うのですが、そういうときに、もしかして自分の端末が勝手に暴走しているのではないかと思った人は、どこへ相談すればいいのでしょうか。契約しているキャリアなのか、端末メーカーなのか、よく分からないユーザーもいるかなと思いまして、そういう窓口があるのかどうかというのが質問の２点目です。

もう１点だけ、そういう問題意識も含めてなのですが、そういう経験があるかとか、そのときにどうしたかとか、どれだけ理解できているかといったユーザーサイドへの意識調査を、１度やってみていただいてもいいのかなというのはコメントです。

以上です。ありがとうございました。

【大谷主査】　御質問とコメントを頂きまして、ありがとうございます。スミッシング対策の通秘との関係、そして利用者が自分の端末が感染していると気づくケースというのは実際にあるのかというのと、その暴走していることに気づいた場合にどこに相談するのがいいのかという点についてですけれども、確かにまとめにもそういったことについてある程度記載されていてもいいのかなという気がしておりますので、先々、このまとめに書いていただくという前提で、事務局から御回答いただければと思います。よろしくお願いいたします。

【小澤利用環境課課長補佐】　沢田先生、ありがとうございます。

まず１つ目、マルウェア感染端末の特定・警告の中の通信の秘密は、過去のIoTや類似事例と同様の整理ができるという御説明までしたが、おっしゃるとおり、ほかの事業者との横展開をしていくに当たって、例えば迷惑メールではDMARCという送信ドメイン認証技術について通信の秘密の整理はこうなっているという資料をお出ししており、事業者様からそういったものがあったほうがやりやすいとか、利用者の理解が得られやすいということであれば作るべきだと思いますので、取りまとめに追記したいと思っております。

２つ目、本人が気づくケースは多分いろいろあって、送られた側から、あなたは感染している、何か勝手に送られていると教えられるケースもあれば、料金が高額になっていて、おかしいと気づくケースもあるのではないかと思います。

そういった場合の窓口という話ですけれども、まず第１は、そういった料金の問題もあると思いますので、まずは契約しているキャリアのほうに御相談されるのが一番かなとは思っており、おっしゃるとおり、周知広報はしっかりやらなければいけないだろうなと。現に被害に遭ったような場合に、取りまとめに明示的に書かれてはいないので、そこも留意して書けるところを書きたいと思います。

あと、利用者のニーズ調査ができないかという御意見を頂きまして、キャリアや関連事業者で既にやっているものがあるか、例えば迷惑メール対策では、総務省も事業者ヒアリング、アンケートをやってきているんですけれども、SMSに特化して豊富にあるわけではないので、事業者の状況も聞きながら必要に応じてやるべきだなと思いましたので、そこも留意したいと思います。ありがとうございます。

【沢田構成員】　ありがとうございました。よく分かりました。

【大谷主査】　沢田構成員から有益な御提案も頂き、今後につながる重要なポイントだったと思います。鎮目構成員、よろしくお願いいたします。

【鎮目構成員】　SMSの不適正利用対策におけるマルウェア感染端末の特定・警告の推進について、通信の秘密の取扱いに留意した上でという点でございますが、同感でございまして、従来取られてきた考え方を再確認した上で、どのような意味で通信の秘密を不当に損なうことがないように配慮することが可能なのかということを、取りまとめにおいてもある程度示して、具体的に示していただいたほうがよろしいのではないかということがまず１点です。

２点目として、不適正利用対策としての本人確認で、今回のお取りまとめで、対面における本人確認ついては、方向性としては、ICチップの利用を原則として、それ以外の方法については、例外的、補充的なものとしていくという点については賛成でございます。

ただ、先ほども諸先生方から御指摘がありましたけれども、ここ数日の報道などを聞いていると、利用者の方に負担感を感じさせるという面が少なからずあるということは実感いたしまして、むしろそのICチップを利用して本人確認ができるというのは利用者にとっては利便性も高くなる側面もあるようですので、詐欺防止が喫緊の課題だということについて十分説明をするとともに、この新たに導入していく仕組みというのはどのようなものなのか、どういう点で利用者にとってもメリットがあるのかということについて、先ほども広報の重要性ということが御議論になっていましたが、理解を十分に得る、そういう努力を今後していただければと思います。

【大谷主査】　鎮目構成員、ありがとうございました。確かに利便性もあるなというのはおっしゃるとおりだったと思います。また、通秘との関係ですけれども、第２回研究会で整理された内容を１枚くらい入れるというのも可能ではないかと思いますので、事務局のほうで御検討いただければと思います。

場つなぎにお話をしますと、別の会合で、電気通信番号の不正利用対策ということで、本人確認の重要性などが検討されているところですが、そこで事業者の方にヒアリングをしますと、利用者にとって負担感のあるその本人確認手続、例えばその証明書を持って来てくださいというようなことですとか、それについての御理解を得るのが難しいので、ぜひその周知をしてほしいという、逆にこちら事業者に求めたいと思っていたようなことについて、事業者側からも公的な広報でその必要性について周知してほしいというようなコメントが出ていたということもお伝えしておきたいと思います。そういう意味で、ある程度負担感のあることであっても、必要なものだということが理解されるということが必要かと思っている次第です。

本日も活発な御議論、それから貴重な御意見の数々をありがとうございました。このワーキンググループは、２月から始めまして全部で６回、特に今月は２回にわたりまして実施させていただきましたが、本日で一旦一区切りとさせていただければと思います。

構成員の皆様から本日もたくさん貴重な意見を頂きましたので、これらの取りまとめを進めてまいりたいと思いますが、事務局で作成していただいた本日の資料６－１、６－２、について、本日頂いた御意見を加えたものを取りまとめ、親会であるICTサービス利用環境の整備に関する研究会への中間取りまとめ報告資料とさせていただきたいと思います。皆様の御意見をうまく取り入れているかどうかという御確認をぜひとも皆様にもお願いしたいと思っておりまして、その確認は事務局からメールをさせていただくような形で対応させていただければと思います。

また、字句の修正や取りまとめの体裁、皆様の御意見が漏れなく反映されているかどうかの確認などの作業につきましては、主査である私に御一任いただければと思いますが、いかがでございますか。

（「異議なし」の声あり）

【大谷主査】　ありがとうございます。異議ないとのコメントを頂きましたので、皆様に一旦その資料の修正版を送った後で、この確認を経た上で最終的な取りまとめを御一任いただくことにさせていただきます。

また、親会であるICTサービス利用環境の整備に関する研究会への御報告、開催日、親会でどのような御意見を頂いたかというようなことにつきましても、事務局からも皆様に御報告が行くような形で今後も進めさせていただきたいと思います。

それでは、事務局からの御連絡事項に移りたいと思います。

【小澤利用環境課課長補佐】　大谷先生、各構成員の皆様方、ありがとうございました。

先ほど大谷主査からお話しいただきましたとおり、本ワーキンググループは本日で一区切りとなりますけれども、親会のICTサービスの利用環境整備に関する研究会、こちらの開催、こちらへの報告日時等につきましては、別途調整をした上で事務局から御案内をさせていただければと思っております。

事務局からの説明は以上です。

【大谷主査】　それでは、以上をもちまして「不適正利用対策に関するワーキンググループ」第６回会合を閉会させていただきます。

本日は、皆様、お忙しい中、御出席いただきまして誠にありがとうございました。