不適正利用対策に関するワーキンググループ（第３回）

令和６年４月15日

【小澤利用環境課課長補佐】　本日は皆様、お忙しい中お集まりいただきましてありがとうございます。不適正利用対策に関するワーキンググループ第３回会合を開催いたします。事務局の小澤でございます。

まず、ウェブ会議の開催上の注意事項について御案内をいたします。

本日、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影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、傍聴者の方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、音声設定は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いております。

次に、構成員の方におかれましては、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、オフにしていただいて、映像もオフにしていただく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い旨を書き込んでいただきまして、座長からの指名に基づいて御発言をいただければと思っております。御発言の際にはマイクをオンにして、映像もオンにした状態で御発言をお願いいたします。発言が終わりましたら、いずれもオフに戻すようにお願いします。接続に不具合があるような場合、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。また、チャット機能で事務局宛てに連絡いただければ対応させていただきますので、よろしくお願いします。

資料の確認ですけれども、本日の資料は、議事次第に載っております資料３－１から３－４を用意しております。

注意事項は以上になります。

では、早速ですが議事のほうに入らせていただきたいと思います。これ以降の議事の進行を大谷主査にお願いしたいと思います。大谷先生、よろしくお願いいたします。

【大谷主査】　大谷でございます。それでは早速、議事に入らせていただきます。

本日はまず、前回までに御議論いただいているSMS対策の方向性について、事務局から説明をいただいた後、意見交換をさせていただければと思います。その後に、携帯電話不正利用防止法に基づいて、本人確認方法の見直し状況について、事務局からまず御説明をいただきます。その後に、警察庁と楽天モバイル株式会社様からの御発表をいただきまして、その後に質疑応答、それから皆様との意見交換をさせていただければと思います。

それでは事務局から、SMS対策の方向性につきまして、御説明をお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございます。それでは、資料３－１　SMSの不適正利用対策の方向性（案）につきまして、御説明をさせていただきます。

前回まで、第１回、第２回において、構成員の皆様に御意見をいただきまして、このページ、SMS対策論点のたたき台に基づいて、御意見をいただいたところでございます。

２ページ目のほうに、前回、特に最後、このたたき台について御意見いただいたところを中心に、各構成員の皆様の御発言のところをまとめさせていただいております。

前半、マルウェア感染端末からのSMS発信対策について、初回から御説明があったわけですけれども、構成員の皆様、特に中原先生ほか皆様から、このマルウェア感染端末／回線の特定、あと利用者への警告／注意喚起、これにつきましては、通信の秘密の取扱いに留意した上で積極的に進めるべきであるという御賛同の御意見をいただいたと思ってございます。

この際、特に中原先生、星先生、鎮目先生から御意見いただいたところで言いますと、この利用者への警告／注意喚起を行う方法については、実効性のある方法を検討するべきであり、その結果、マルウェアの削除でありますとか、対策アプリの導入などの行動変容が実際に実現したかどうか、こちらはしっかりフォローアップをした上で、有効な方法を検討する必要があると御意見をいただいております。

悪意を持ってマルウェアに感染させていくようなパターンとかもあるのではないか、警告についても、SMSを送るなどいろんな方法がある中で、どういう方法がいいのかというところは、フォローアップの中で随時見直していくべきではないかという御意見をいただいたと思っております。

３点目、スミッシングメッセージについて、円滑にユーザーからの申告を受け付けられるようにして、事業者横断で活用できるような環境を整備すべきという御意見です。

これは初回に、ニュージーランドの実例や他の国の御紹介もございました。あとはキャリアの皆様から第２回の御説明がありましたけれども、キャリアのほうで受け付けている申告はもちろんですが、それ以外の事業者横断、特に沢田先生からは、通信事業者以外のなりすまされる側といいますか、SMSを利用する側に対して、こんなメッセージが来ていたよという申告がある可能性もあるため、お互いに横断で活用できるような環境を整備していく必要があるのではないかという御意見をいただきました。

後半、SMS配信者・受信者の不適正利用対策ということで、まず発信元を明確化しまし

ょうという話ですけども、沢田先生から、メッセージが正規のものであると見分けられるよう、SMS発信元の明確化・透明化の取組を進めましょうと御意見がございました。特に、SMS認証を活用するような事業者も巻き込んで、特に、SMSを法人から送るときはこういう番号から送りましょう、みたいなしっかりしたルールを業界の中で策定し事業者同士で運用するというような、自主的な対策も含めて検討する必要があるのではないかという御意見と理解しております。

これと関連しますけれど、２つ目、事業者間の連携に当たってSMSを利用する側の事業者とも連携するべきではないかといった御意見もございました。前回、SMSの配信に関するキャリアや配信事業者様を巻き込んだ事業者連絡会を立ち上げた旨御紹介いたしましたが、それだけでなく、利用する側の事業者とも横断で連携しながら対策を検討すべきという御意見をいただきました。

また前回、警察庁様から御発表いただきましたSMS認証代行につきまして、星先生からも、しっかり対策進めるべきという御意見をいただいたと思います。こちらについても、悪質な事業者がSMSを使うということがないように、これも事業者一丸となって排除していくというところも対策の一つと認識し、御意見を掲載しております。

また、国外におけるSMS不適正利用対策の動向を参考として進めるべきというところについても、仲上先生から、御意見としていただいております。

最後、これまで特に第２回において、各キャリアさんの方で行っている対策について御説明がございましたけれども、まだ利用者の理解が高まっていないと、0005番号やRCSプラスメッセージへの対応についても御説明いただきましたが、これを利用者側が、こういうふうな番号で来るものは安心だとか、こういうものは気をつけなければいけないとか、そういう意味でも、SMSの仕組みそのものが分かりにくいところもございますので、周知啓発をしっかり行うべきではないかと、大谷先生ほかの皆様から御意見をいただいたと思います。

これらを踏まえ、事務局にて、方向性（案）という形でまとめさせていただいたものがこちらになっております。

１つ目が、マルウェア感染端末の特定・警告の推進ということで、通信の秘密の取扱いに留意した上で、マルウェアに感染してしまった端末の利用者の方に警告していくというものです。

これに関連して、ちょうど３月末ですか、NTTドコモさんから、意図せずこういったメ

ッセージを大量に送ってしまっているような方について、注意喚起を行うような取組をこの夏からスタートするという、事前の報道がございました。こういったものもこれに資するかと思いますが、利用者の行動変容を促すような取組をしっかり進めていくということを１つ目に入れております。

２つ目が申告の受付け、先ほどの３つ目で御紹介した、事業者横断で活用するというところを中心に、申告受付けの窓口をしっかりつくるということを入れております。

３つ目、SMS関連事業者による業界ルールの策定ということで、SMS不適正利用対策事業者連絡会を前回立ち上げましたので御報告しましたけれども、これも利用する側の事業者も含めて、発信元を明確化するような、業界ガイドライン、ルールを策定していきましょうというものでございます。

ここの中で、特に利用する側という意味では、SMS認証代行業者のような悪質事業者は、逆に言うと排除していくようなところも含めて、しっかり業界での対策を進めていくということを盛り込んでおります。

最後、SMS対策の周知啓発です。これは、スミッシングの手口はもちろんですけど、それ以外の、事業者で行っている対策、キャリア共通番号0005ですとかRCSのようなもの、あとはそもそもSMSというものがどういうふうに届いてくるのか。キャリアさんとSMS配信事業者さんがいるという話も前回、各社さんから御説明がありましたが、こういったSMSに関する利用者のリテラシー向上に努めて、自主的な防衛を推進することもセットで必要ではないかということで、この４つの方向性にまとめさせていただいております。こちらについて御意見をいただければと思います。

事務局からは以上です。

【大谷主査】　御説明ありがとうございました。

それでは、ただいまの御説明につきまして、質問ですとかコメントございましたらお願いいたします。

沢田構成員、よろしくお願いいたします。

【沢田構成員】　御説明ありがとうございました。対策の方向性に、もちろん異論はございません。いろいろ提案したことを取り上げていただいて感謝しております。ありがとうございます。

方向性の④に関しまして、一点だけ付け加えます。利用者に対する周知啓発ということで、基本的な仕組みも御説明いただくように考えていただいているのはよかったと思いま

す。

もし可能であれば、連絡会のほうで検討いただいているかもしれないのですが、一般消費者といいますか、利用者がSMSに対して、どういう意識を持っているかという意識調査のようなことをやっていただけるとうれしいなと思いました。

ほかの連絡手段がいろいろあるので個人間の連絡にはSMSをそんなに使っていないのではないかという想定の下ですが、送信側の立場で日常的にどの程度利用しているのか、受信側として、フィッシングメールを受け取った経験があるか、その時どういう行動を取ったか、どこかに連絡したかとか、無視したとか引っかかったとか、そういう経験についてお聞きできるといいのではないかと思いました。

以上です。ありがとうございます。

【大谷主査】　貴重な御意見ありがとうございます。①のところで「利用者の行動変容を促し」というふうなことも言っているので、どう変わっていったのかといったことを利用者の意識で見るということも必要なことではないかなと、私も感じております。

この辺りについて、事務局のほうからコメントがありましたらいただきたいと思います。

【小澤利用環境課課長補佐】　ありがとうございます。SMS利用者の意識をしっかりはかるべきと、これはおっしゃるとおりだなと思いました。先ほど大谷先生からも補足がありましたように、行動変容をしっかりフォローアップするということも入れておりましたので、まず現実に、どういうふうに使っていて、どういうふうに不正利用を感じているかとか、そういうところも含めて、何かしら意識調査を行う、これも方向性に盛り込めればと思います。ありがとうございます。

【沢田構成員】　ありがとうございます。

【大谷主査】　ありがとうございました。

ほかに質問ですとか御意見ございますでしょうか。

それでは、中原構成員、お願いいたします。

【中原構成員】　前回発言しそびれたので補足ということなんですけれども、通信の秘密との関係について、前回の事務局資料で、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」の第三次取りまとめを参考としてお示しいただいたものと思います。

その通信の秘密との関係というのは、SMSの被害対策であるところのマルウェア感染端末／回線の特定及び利用者への警告／注意喚起というところでも、同様に問題になると思

いますけれども、サイバー攻撃の場合とでは、通信の秘密と対立する法益が異なるのだと思います。

サイバー攻撃の方の研究会では、インターネットサービスプロバイダーによる電気通信役務の提供の円滑性という、公益に近いものの保護が問題とされていたのに対して、おそらく今回の場合は、直接には当該携帯電話利用者の財産の保護であるとか、あるいは間接的にはマルウェアに感染した端末からSMSが送信される、他の携帯電話利用者の財産の保護というのが問題になってくるのかなと思います。

このことによって通信の秘密との関係でのハードルが上がるということはおそらくないのではないか、むしろ下がるのではないかと思われますけれども、いずれにせよ、こういう状況の相違を念頭に置きながら検討する必要があるのではないかなと思った次第です。

以上です。

【大谷主査】　ありがとうございます。確かに今回、保護法益としての公益の側面のほかに、直接、本当に財産を詐取されたりする方がいるのを防止できるということでは、逆にハードルを下げるという効果があるということ、触れていただきましてありがとうございます。

こちら、事務局のほうで、「通信の秘密の取扱い」と書いていただいていますが、コメントがありましたらお願いします。

【小澤利用環境課課長補佐】　中原先生、ありがとうございます。通信の秘密の取扱いについて、前回サイバー研の第三次の取りまとめの御紹介で、これを参考に整理が可能ではないかということを御説明しましたけども、今回、ドコモさんが実際のサービスのイメージも御発表されていますので、そういったものも参考にして、ほかの通信事業者さんも含めて、しっかり、安心してサービスできるような形で、何らか説明できるような形を準備すべきかなというふうに、御意見を伺って思いました。過去に迷惑メールの対策のほうでもやったことがございますので、こういう方法だったら大丈夫ですよと、何らか事務局のほうでも検討させていただければと思います。ありがとうございます。

【大谷主査】　ありがとうございました。その辺りの整理が、きっと③のところにも活かされるといいなと思っております。

仲上構成員、よろしくお願いします。

【仲上構成員】　お世話になります。日本スマートフォンセキュリティ協会の仲上です。

不適正利用対策の方向性について、案を御提示いただきありがとうございます。こちら

の方向性については、異論なく賛成させていただきたいというふうに思っております。SMSは今後も引き続き認証の重要なポジションを占めていくのかなと思いますので、安全化を図っていくべき内容かと思います。

一点、意見なんですけれども、４番の周知啓発の推進につきまして、スミッシングですとかこういった悪用につきましては、どんどん高度化している状況があるかと思います。

とはいえ、スマートフォン等は、幅広い世代で様々な方がお使いになられているというところで、受け手側のリテラシーに配慮した情報発信ですとか啓発の活動、そういったところについて様々なレベル感でお伝えする必要があるなというふうに思っております。

この点、日本スマートフォンセキュリティ協会でも、引き続きこのような周知啓発等、御協力させていただければと思いますので、御意見として出させていただきました。

以上でございます。

【大谷主査】　貴重な御意見ありがとうございます。また、御協力いただけるということで、スマホ利用者はあらゆる年代層にわたっていますので、その方たちに伝わる形で、ということですね。

何というか、利用者のリテラシーのみに依拠したくはないなと思いつつ、やはり知っていただくべきことは十分に周知したほうがいいと思いますので、ぜひ今後ともよろしくお願いいたします。

事務局サイドで何かコメントがあるようでしたらお願いします。

【小澤利用環境課課長補佐】　仲上先生、ありがとうございます。おっしゃるとおり、利用者への周知広報ですかね、先ほどもリテラシーだけではなくてという話もありましたけど、いろんなところをとらまえてやらなければいけないところがあると思いますので、ぜひ協力させていただいて実施できればなと思います。よろしくお願いします。

【仲上構成員】　よろしくお願いいたします。ありがとうございます。

【大谷主査】　たくさん貴重な意見を寄せていただいておりますけれども、ほかにございますでしょうか。

それでは、一巡まではしておりませんけれども、今日はちょっと重たいテーマが控えておりますので、次に進ませていただきまして、また時間があるときに振り返ってみればと思っております。

それでは、議題の２に入りまして、事務局のほうから、携帯電話不正利用防止法に基づく本人確認方法の見直しの状況につきまして、御説明をお願いしたいと思います。よろし

くお願いいたします。

【小澤利用環境課課長補佐】　ありがとうございます。それでは、３－２の御説明に入りたいと思います。

こちらは、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についてということで、現在の検討状況と、あとは、そもそも、本人確認の議論はここからスタートになりますので、現在どういう制度になっているかというところも含めて御説明をさせていただきます。

こちらは、初回の御説明の中でもございましたけれども、総務省においてはこれまで、特に電話の悪用に基づく詐欺、特殊詐欺対策については、この３つの柱で対策をしてきました。この携帯電話不正利用防止法、犯罪収益移転防止法、こちらがいずれも契約時の本人確認に基づく事前の対策。事後の対策として電話番号の利用停止措置ということで取り組んでまいりました。今回は、この契約時の本人確認の方法についての議論ということになります。

携帯電話不正利用防止法については、概要は初回も御説明しましたけれども、ポイントを再度御説明いたしますと、携帯電話の契約時の本人確認ということになりまして、この携帯電話の中にはいわゆる携帯電話、プリペイド携帯を含めたものだけではなくて、レンタル携帯ですとか、あとこの４月から050アプリ電話という、携帯端末上で050を使って電話できるようなサービス、こちらも携帯電話不正利用防止法の対象に追加されております。

こちらについては、いずれも契約時の本人確認義務、あとは無断譲渡禁止というのもセットでございますけれど、譲渡時の本人確認といったような制度がございます。

また、警察署長からの契約者確認の求めという、犯罪に携帯電話が悪用されましたというのが確認された場合に、警察署から、本人確認を取り直してくださいというような要請ができるような制度がございまして、これに対応しないような場合には役務提供拒否をするというような仕組みがございますので、こういった、いろんなタイミングでの本人確認方法というのを定めている法律になっております。

これと関連して、犯罪収益移転防止法になりますけれども、こちらのほうは、金融機関を中心としていろんな事業者が特定事業者として定められておりまして、こういった事業者について共通して、マネロン対策のために契約時の本人確認をしましょうというような法律になっておりまして、警察庁さんをはじめ、ほかのいろんな業界を所管する省庁との共管法令になっております。こちらについては、通信関係では電話受付代行業、あとは電

話転送サービスが対象になっております。

こちらについても、ちょっと言い方は違うんですけれども、契約時の本人確認を中心とする確認の義務というのがございます。また、犯収法では、疑わしい取引届出とか、独自のルールもございます。

携帯電話不正利用防止法と犯罪収益移転防止法の関係性で言いますと、これまでも本人確認方法を、犯収法の金融機関の本人確認の方法と併せながら検討してきた、本人確認というものの在り方ということで、常に参考とさせていただいているということもあって、触れさせていただいています。

ここからやや細かい話になるのですが、携帯電話不正利用防止法の省令でどのような本人確認方法が認められているかということをこちらに書いております。

一番上に書いてあるのが、一番分かりやすい対面での提示によるもので、特に写真のついているような本人確認書類が分かりやすいと思いますが、こういったものを提示して本人確認する方法がございます。

また、この後、偽変造の話とか警察庁さんの御説明がございますけれども、非対面における方法について、幾つか方法が定められております。細かくあるのですが、一番分かりやすいものが、本人確認書類の写しの送付とありまして、いわゆる免許証の写真を撮って、その本人確認書類に記載の住所に転送不要郵便を送るものであり、写しの送付＋転送不要郵便をもって、本人確認が終了するといったようなルールが規定されています。非対面で一番使われている方法はこちらになっております。

この次に多いのが、最近入った方法ですが、eKYCと呼ばれる方法です。ソフトウエアを通じて本人の容貌の画像を送信し、加えて、写真付本人確認書類の画像、その厚みとか、本人確認書類を45度傾けて写真を撮ってくださいというものもありますが、そういうのも含めて送ることによって、オンラインで完結して本人確認ができるというような仕組みがございます。このeKYCの厚み方式と呼ばれるものが、２番目に多く使われているものになります。

これ以外に、この下に、特定事項伝達型本人限定受取郵便、これは郵便局員が玄関口で本人確認書類を確認するというような方法になります。あとは、電子証明書を付した本人特定事項の送信、こちらが、例えばマイナンバーカードの公的個人認証といった、チップの中に入っているようなものを使って電子証明書を送るというような方法で、何事業者かが使われているものになります。そのほかにも細かくは、住民票の写しの原本を送る方法

とか、eKYCでチップを読む方法とか、多数の方法が定められております。

なお、法人の場合は、登記事項証明書のような法人を証明する書類の提示、または写しの送付＋転送不要郵便に加えて、契約担当者の自然人としての本人確認を行うというようなルールになっております。これも、最終的に自然人までたどれるようにというような趣旨で定められております。

本人確認書類として使えるものについては、この省令の別の条項で、こういったような形で列挙されております。運転免許証、マイナンバーカード、パスポートなど、細かく指定がございまして、この書類については郵便が必要ですとか、そういった種別ごとに分けられて定めがございます。

昨年６月に、デジタル社会の実現に向けた重点計画、こちらが閣議決定をされております。この文章を抜粋しておりますけれども、犯収法、携帯電話不正利用防止法に基づく非対面の本人確認手法は、マイナンバーカードの公的個人認証に原則として一本化し、運転免許証等を送信する方法や、顔写真のない本人確認書類等は廃止する、というふうに書かれております。

特に券面の偽変造が多く、特に非対面の場合は見分けるのが難しいということに起因して、こういった見直しを行いましょうということが位置づけられております。

これを踏まえて、今年度、総務省のほうでも、犯収法の検討状況とかも鑑みながら検討し、事業者にも意見聴取しているものが以下の方向性になります。

分かりやすい条文ごとの表を御覧いただければと思いますが、先ほど申し上げました非対面の場合の、写しの送付＋転送不要郵便を送る方法、あとはeKYCの厚みの方法、こちらのほうは券面の偽変造に弱いということもありまして、廃止する方向で検討したいということで今、対応を進めております。

これ以外の方法については、リスクやコストを見ながら、残す方法で考えておりまして、あと対面のほうは、事業者の準備状況ですとか、リスクとコストも鑑みながら、どういうふうに進めていくか検討しております。

スケジュール感でありますけれども、これはデジタルの重点計画のほうで昨年度定められましたので、先ほど申し上げました検討内容について案をつくって、事業者と調整してきているところであります。

今年度中に省令改正のパブリックコメントを行って、改正内容を決定するというふうに位置づけられておりますので、今回このワーキンググループで議論した内容も踏まえて、

今年度中に省令案のパブコメをできればなというふうに考えております。

また、令和７年、８年、十分な準備期間を確保した上で施行することとなっておりますので、こちらも併せて検討していければと思っております。

私のほうからの説明は以上になります。

【大谷主査】　御説明ありがとうございました。

そういたしましたら、続きまして警察庁の捜査支援分析管理官の道家理事官に御説明をいただきたいと思います。どうぞよろしくお願いいたします。

【道家オブザーバー】　よろしくお願いいたします。

ただいま御紹介いただきました警察庁捜査支援分析管理官付の道家と申します。これまでオブザーバーとして参加しておりました野村管理官が、３月25日付で人事異動になっておりまして、現在空席になっておりますので、僭越ではございますけれども、代わって御説明させていただきます。

本日は、「本人確認書類の偽変造等の実態」というテーマをいただいておりますので、表示の資料に従って御説明させていただきます。

まずは、ワーキングの冒頭に事務局から御説明がありました、特殊詐欺の情勢につきまして補足いたします。

令和６年における特殊詐欺の被害は、この右下の棒グラフですけども、２月末時点で、昨年同期に比べて、認知件数こそ500件以上ということで約20％減っておりますけれども、被害額は1.3億円、プラス２％増加しておりまして、引き続き厳しい情勢が続いております。

特殊詐欺は主として電話を使い、対面せずに相手をだますという点が特徴でありまして、犯人グループにとりましては、足のつかない電話を確保することが非常に重要であるということを、本日の御説明の前提として進めさせていただきます。

犯罪予防の観点からは、特殊詐欺の犯行グループに匿名電話を与えないということが重要でございまして、電話対策につきましては、もうかれこれ20年間にわたりまして、国を挙げて取り組んできました。

こういった様々な対策を積み重ねてもなお特殊詐欺が止まらない背景の一つには、犯人グループが必死になってこれらの対策の隙間を狙って、匿名で通信できる電話を何とか探し出しているという実態がございます。

悪用目的で電話を契約しようとする者を予防的に排除するとともに、犯人を追跡して捜

査するためには、契約時の本人確認が確実に行われることが必要ですけれども、令和５年中に犯行利用されたもので、契約方法まで追跡できた携帯電話を対象に調査分類した結果、半分以上は偽変造された運転免許証によって不正に契約されたことが分かっています。

画面のグラフは代表的な本人確認資料ごとに、偽変造されたものと真正なものとを並べて記載してありますけれども、これを御覧になって、思った以上に真正な運転免許証による契約が多いのではないかと感じる方も多いかもしれませんけれども、若干補足しますと、この中には、本人が契約しているわけではなくて、例えばアルバイトの応募ですとか借金の申込みとか、そういった場面で送信した真正な運転免許証を悪用されてしまって、本人が知らないうちに契約されてしまっているといったケースも相当数含まれております。

なお、明確な統計的資料はないのですけれども、携帯電話の契約の場合には、申込者が身分証を撮影した写真を送信し、携帯電話事業者がSIMやサンキューレターを申込者に送付して、それが到着したことをもって住所確認を行うという方式で不正契約されるケースが最も多く、実際はその送付先には空きアパートが使われているといったことが多いと見ております。

つまり、これは本人確認が終わったから商品を発送しているのではなくて、商品が届いたということをもって、きっとこれは本人だったのだろうというふうに、ある意味事後的な確認が行われているといった部分が、その隙を突かれているのかなと考えております。

また、業者をだますことができるほど精巧な本人確認書類というのは、実は今ではネット注文を通じて簡単に入手することが可能となっております。

例えば、「身分証偽造」といった用語で検索しますと、すぐにこのように、本物と見分けがつかないことを売りとするような販売ページが堂々と出てきております。ところどころ、我が国と異なる漢字が出てくるので、資料の業者の場合には、本拠地が国外にあるのかなと思われます。

他方で、このような偽造身分証をつくっている工場は、しばしば日本国内でも見つかっております。最近報道された例を見ますと、例えば警視庁なんですけども、令和５年12月に大阪府下で検挙した偽造工場では、海外の指示役の指示を受けて、１枚約１万円の、マイナンバーカードを含む各種身分証を販売したとされております。また埼玉県警でも、令和５年９月に川口市内で工場を摘発しております。

これらの偽造では、パソコンとプリンター、またラミネート機などの一般的な事務機器があれば、アパートの部屋でも簡単にできてしまいますので、こういった偽造身分証の流

通を止めるというのは相当難しいというのが実態でございます。

それから、今年３月にも、長崎県下で夫婦２人による偽造工場が検挙されております。この夫婦の役割は、テレグラムで受け取った偽造データを印刷して偽のカードをつくり、それを指定の場所に郵送することだったそうですが、この夫婦とは別に、スミッシングで個人データを得た者、また、そのデータを基に偽造身分証のカードデータを作成した者、それから、夫婦から受け取った偽造カードを使ってSIMを再発行させて詐欺を実行する者に分業されておりまして、結局その黒幕は捕まらないという構造になっております。

携帯電話が一般人の社会活動のハブになっているのと同様に、悪人にとっても犯行の基盤になっていることを考えますと、本人確認が脆弱である現状というのは改善しなければならないと考えております。

また、今のところ一般的ではありませんけれども、契約者本人の容貌の画像情報と、写真付き本人確認書類の厚みなどの画像情報等を一緒に送信させることにより、本人確認を完結できる仕組みも、これを乗り越えられているという事例が確認されております。

詳しい手口までここでは紹介しませんが、こういった画像情報を違法入手する方法は幾らでも考えられますので、もはや本人確認を券面情報のみに頼ってはならないと強く思っております。

それから、携帯電話不正利用防止法の第８条には、詐欺を含め、匿名性の強い指定犯罪に携帯電話が使われたときに、警察署長から携帯電話事業者に要請して、現在の使用者をもう一度確認していただく仕組みがあります。

これは犯罪捜査ではないため、警察が利用者情報を入手する仕組みにはなっておらず、事業者の本人確認に犯人が応じない場合には、以降、犯行利用されないように、事業者において電話利用を停止するというものでありますけれども、これに対して、制度ができたフィーチャーフォンの時代とは異なっておりまして、現在は写真の品質がとてもよいので、他人名義のスマホと一緒に契約時の免許証写真も併せて入手しておけば、その求めがあった場合に、それを送付することによって事業者の確認ができてしまうといった問題が起こり得ます。

この件に関しましては、警察庁が携帯電話事業者に御協力いただきまして取ったアンケートでも、回答いただいた事業者の約半数がこの問題点を認識しているということが分かっております。これも券面情報に頼った本人確認をめぐる問題の一つですので、データ技術を向上するなどして、利便性を落とすことなく、本人確認の確実性を向上する工夫が必

要です。

さらに、海外の記事によりますと、海外ではAI技術を用いまして、手書きのサインまで整えたIDカードの画像を瞬時につくることができるというインターネットサイトが悪用されています。そのうち冗談抜きに、免許証を手に持った人物の画像まで生成できるサービスが出てくるのではないかと懸念しております。

特に電話は、不正契約されて悪人の手に渡ると犯罪ツールになってしまいますので、このようなサービスが日本語対応する前に本人確認の確実性を高めねばならないと、危機感を感じているところでございます。

これまで、電話が重要な社会インフラとして信頼性を積み上げてきた歴史を考えますと、現状ですと「電話に出ると危ない」と言わざるを得ない状況は非常に残念なことだと考えております。

国民が電話を引き続き便利で信頼できる道具として利用できる環境を守るとともに、国民生活の安全を取り戻すため、時代に合った新しい本人確認の実現に向けた検討をお願いして、説明といたします。

私からは以上です。

【大谷主査】　御説明どうもありがとうございました。

それでは次に、楽天モバイルの小田様、御準備よろしいでしょうか。

【楽天モバイル株式会社（小田氏）】　楽天モバイル、小田でございます。この資料３－４に従って、私より御説明させていただきます。

めくっていただいて、２ページ目でございます。「はじめに」ということで、携帯電話不正利用防止法、以降「携帯法」と申し上げますが、本日この法律の施行規則、先ほどまさに出てきた本人確認の部分について、不適正利用の防止やデジタル社会の実現の観点を踏まえた実施方法の導入を御提案させていただきます。

御提案させていただく方法は、犯罪収益移転防止法において、いわゆる依拠の形で、従来より金融業界で実施されている方法です。この実施に際しまして、銀行等では銀行側でセキュリティー認証を実施することで、なりすまし等の不適正利用に取り組んでいるというふうに承知してございます。

先ほど総務省様からもお話があったように、今後、一部の本人確認方法が廃止される方向性となっていることで、多くの国民において利便性が損なわれるのではないかということも想定されることに鑑みまして、不適正利用を増やさない代替的な方法として、今回の

御提案をさせていただきます。

まず、不適正利用の防止の観点についてです。左が、先ほどの警察庁様からの資料と重複する部分がございますが、弊社にてレイアウト等させていただいたものです。

御説明にもありましたように、特殊詐欺の件数、それから被害額、近年再び増加傾向にあるということで、精巧に偽変造された本人確認書類の悪用等、特殊詐欺に使われる手法はますます高度化・複雑化しているという現状もあろうかと理解しております。

また、左下にありますように、特殊詐欺に利用される電話の方法としては、国際電話のほうに今シフトをしているところですけれども、既存の方法についても、ほかの電話の方法についても引き続きしっかり本人確認していく必要があろうと考えております。

その説明が右側でございまして、本人確認の実施、不適正利用を防止・牽制しまして、またサービス全体の安全・安心につながっていくものというふうに理解してございます。

続いて、デジタル社会の実現の観点についてです。左側、行政手続におけるデジタル３原則について御紹介しております。

デジタル庁様の「デジタル社会の実現に向けた重点計画」では、デジタル社会形成のための基本原則として、個々の手続・サービスが一貫してデジタルで完結するという「デジタルファースト」、それから、一度提出した情報は二度提出することを不要にするという「ワンスオンリー」、そして複数の手続・サービスをワンストップで実現するという「コネクテッド・ワンストップ」の３つの原則が掲げられております。

これらデジタル３原則は、行政手続のオンライン化の基本原則として位置づけられているものでございますが、携帯電話は既に社会的なインフラとなっておりまして、ほぼ全ての国民の方々が、携帯法上の本人確認手続に対処する必要がございますことから、国民の利便性を確保する必要性は行政手続同様に高いのではないかと。よって、携帯電話契約においても、デジタル３原則を踏まえた本人確認手続が同様に求められるものというふうに、当社としては考えてございます。

右側は御参考情報でございまして、民間機関による調査によりますと、オンラインで郵送、それから窓口での本人確認手続中に、面倒になって手続そのものを中断したことがありますかという質問に対しまして、「あります」という方々が42%程度ございまして、「覚えていない」という方を抜きますと、ほぼ半数の方がそういった経験をされているということになります。本人確認手続においてデジタルを活用することで、ワンストップでワンスオンリーの手続といったものに対する国民のニーズが高いことがうかがわれるというこ

とで、参考資料として御紹介させていただきます。

続いて、依拠による本人確認方法について御紹介をさせていただきます。

犯収法においては、銀行やクレジットカードといった会社で既に行われた本人確認結果を活用する、いわゆる依拠による本人確認方法が2012年より実施されております。

左側の図に保険会社が例に挙がっておりますが、そういった収納機関が新たに提供しようとするサービスの契約に際しての本人確認におきまして、既に本人確認を実施済みである銀行ですとかクレジットカード会社さん、そういった金融機関の本人確認結果を活用することによる本人確認方法となっております。

携帯法におきましては、このような、他の事業者による本人確認結果を活用する方法は現在認められておりませんが、本人確認手続の重複は社会的に大きなコストがあることから、犯収法だけでなく携帯法においても依拠の制度の必要性はありまして、また、犯収法と携帯法の本人確認内容及び本人確認方法に共通する部分が多々あることもございますので、依拠制度を携帯法においても導入することの許容性はあろうかというふうに考えてございます。

具体的に、どう携帯法に依拠を導入するかという当社案が、このページでございます。

ここまで御説明しました、不適正利用の防止ですとかデジタル社会実現の観点、そして犯収法における依拠による本人確認方法等を踏まえまして、携帯法においても同様に、ほかの事業者が法令に基づき実施した本人確認結果を、新たなサービス提供契約における本人確認に際しても活用する方法の導入を提案させていただきます。

具体的には、左側の図にありますように、携帯電話事業者が新たに提供する携帯のサービスの本人確認に際して、過去に本人確認を実施済みの事業者の本人確認結果を活用するという本人確認方法となります。

過去に本人確認を実施済みの事業者となり得る事業者としましては、まずは犯収法同様に銀行ですとかクレジットカード会社が挙げられます。それに加えまして、本人確認実施済みのほかの携帯事業者といったものも想定されるというふうに考えてございます。

その背景としましては、右側の棒グラフにございますが、銀行口座、それからクレジットカード、携帯電話各サービス、いずれも国民における浸透度が非常に高く、これらはいずれも契約時に本人確認を必要とすることから、本人確認結果を活用する仕組みを導入することで、多くの国民が利便性の向上を享受できるのではないかというふうに考えてございます。

７ページ目が、御参考までに掲げさせていただきましたが、犯収法に基づく依拠手続フローの例でございます。

犯収法における依拠におきましては、本人確認を実施済みの銀行またはクレジットカード会社と、新たにサービスを提供する収納機関とのシステム連携によって実施されておりまして、収納機関から銀行またはクレジット会社に対する支払い方法の申込み時に合わせて、銀行・クレジット会社から、収納機関に本人確認結果を連携するといった仕組みになってございます。この仕組みの中で、銀行やクレジットカード会社さんのほうでは、ワンタイムパスワード等のセキュリティー認証を実施することで、いわゆるなりすまし等の不適正利用の抑止に取り組まれているというふうに理解してございます。

携帯法における依拠手続においても同様に、本人確認結果を実施済みの銀行・クレジットカード会社さんと、新たにサービスを提供する携帯電話事業者とのシステム連携によって、本人確認結果の活用が実施可能というふうに考えております。

また、ここも同様ですが、銀行・クレジットカード会社さんが同様にワンタイムパスワード等のセキュリティー認証を実施することで、なりすまし等の不適正利用抑止にも取り組めるものというふうに考えております。

今度は、本人確認済みの携帯電話事業者における本人確認結果を活用する場合について、当社として検討したものを御紹介させていただきます。

携帯電話事業者間におきましても、事業者間の連携手続として、昨年開始したMNPワンストップの仕組み等がございます。これらも参考にしまして、事業者間でシステム連携することによりまして、MNPや新たに異なる事業者の携帯の回線を契約する際に、他事業者における本人確認結果の活用が可能というふうに考えております。

また、銀行・クレジットカード会社と同様に、本人確認済みの携帯電話事業者においてもワンタイムパスワード等のセキュリティー認証を実施することで、なりすまし等の不適正利用抑止に取り組むことができるというふうに考えております。

この10ページ目は構成員限りとさせていただいておりますが、当社が実施している不適正利用対策に関する概要を参考にお示ししております。

携帯電話業界におきましては、長年不適正利用対策に、警察庁様、総務省様と連携して取り組んでおりますが、後発である当社においても、当社グループのECですとか金融といったサービスの取組事例も参考に、同様に取組を進めているところでございます。

また、次の11ページ目で、不適正利用対策の中でも、先ほど触れましたなりすまし対策

としての、当社はMFAと書いていますが、いわゆる多要素認証としてワンタイムパスワードを導入しておりますので、こちらも御参考までに、こういった仕組みですよということで御紹介させていただきます。

12ページ目です。ここまで専ら個人の方との契約を念頭に御説明しておりましたが、ここでは法人との契約における本人確認についても、３点御提案をさせていただきます。

１点目ですが、先ほど御説明した依拠による本人確認方法を、法人契約における代表者の本人確認に導入するという点でございます。

個人契約と同様に、法人契約においても代表者の本人確認は必要なんですけども、ここにおいても、利便性の向上ですとか社会的コスト削減の観点から、こういった手続の導入が必要と考えております。

２点目、真ん中ですが、貸与契約で既に認められている２回線目における簡略化された本人確認方法を、法人契約にも導入可能ではないかということで考えてございます。

現状、法人契約では、２回線目以降の契約においても、窓口になっている会社の代表者さん、改めて本人確認が都度必要だということになっているところですけれども、一度本人確認が済んでいることから、２回目以降の本人確認を簡略化してもリスクの程度が高いとは言えないのかなというところで、当該本人確認を導入することの許容性はあるというふうに考えてございます。

３点目、右側です。犯収法で認められている登記情報提供サービスの登記情報を用いた方法を、携帯法にも導入するということでございます。

法人の本人確認において、登記情報証明のためには、通常これまで原本の登記事項証明書を出していたのですが、書面でなく電子的に取得した情報を用いる方法も許容いただきたいというふうに考えているところでございます。

13ページ目、スケジュールに関する要望でございます。

今回御提案させていただいた、依拠による本人確認方法、それから法人契約における本人確認方法の見直しにつきまして、本ワーキンググループ等における議論ですとか報告書の取りまとめ等を経て、2024年中に提供開始できることを当社としては要望いたします。

関連しまして、先ほど総務省様から御説明いただいた資料にありました、廃止の方向となっている本人確認方法につきまして、偽変造された本人確認書類が悪用されているという、警察庁様から非常に詳細な資料の御提示もありましたが、そういった実態を鑑みまして、見直しが検討された方向性については当社としても理解しているところでございます。

その上で、具体的な廃止のタイミングとしては令和７年以降というところで、総務省様の資料ではございましたが、その具体的な時期をどこに置くかという決定に際しましては、今回廃止の方向になっている本人確認方法の実施状況の検証あるいはモニタリング等をしていただきまして、今回当社が御提案している方法が仮に導入されれば、この方法も加えてということになりますが、ほかの廃止されない本人確認方法が広く国民に使われているという状況が、実態として実現されたことを十分確認した上で廃止していただくというプロセスを踏んでいただきたいというふうに要望させていただきます。

15ページ目で、本日の御提案のまとめでございます。

まず１点目で、不適正利用の防止、それからデジタル社会実現の観点から、携帯電話契約時の本人確認について、犯収法と同様に、他事業者が実施した本人確認結果を活用する、いわゆる依拠による方法を導入いただきたいということです。

導入いただく際には、犯収法と同様に、ワンタイムパスワード入力等のセキュリティー認証を実施することで、なりすまし等の不適正利用抑止に取り組むということで考えております。

２つ目に、法人契約における本人確認についてということで、依拠による本人確認方法、それから２回目以降の本人確認方法、それからオンライン登記情報の利用の３点の改正を導入いただきたいというポイントでございます。

３つ目はスケジュールです。

１点目、２点目にある本人確認の導入は、今年中に提供開始いただけることを要望いたします。なお、廃止の方向になっている本人確認については、利用実態を検証・モニタリングいただきまして、ほかの方法が広く国民に使われている状況が実現されたことを確認いただいた上で廃止いただくということを、併せて御要望させていただきます。

次ページ以降は、10ページ目で御紹介しました、当社が実施する不適正利用対策の詳細となりまして、構成員の方々限りということにさせていただいておりますので、説明は割愛させていただきます。

当社から御説明は以上です。御清聴ありがとうございました。

【大谷主査】　小田様、どうもありがとうございました。丁寧な御説明をいただきまして、いろいろ御要望もいただいたところでございます。

それでは、資料の番号で言いますと３－２、３－３、そして３－４を含めまして、これから質疑応答、それからコメントをいただく時間にしてまいりたいと思います。どなたか

らでも結構でございます。

辻構成員から挙手いただいております。よろしくお願いいたします。

【辻構成員】　セキュリティーの専門家として、本日の話題は非常に重要かと思いますので、発言をさせていただきます。

まず、セキュリティーの大原則としまして、「確実な安全」と「安全であろう」というのは全く異なるものでございまして、今まではいろんな事情により、「確実な安全」の確保ができない事情があったのだろうなと思います。

本日話題になりました、本人確認の見直し、廃止の検討がなされている内容というのは、従来の運用であったり実情を踏まえての仕組みであったと思いますが、セキュリティーの専門家から言わせると、「安全であろう」に近い仕組みであったということで、それを是正する流れというのは歓迎すべきかなと思っております。

ですので、より確実な本人確認、デジタルの世界での本人確認を行っていくことは、非常に重要な議論になると思っております。

２点目ですが、そういった中で、依拠についてしっかり整理しておくべきかなと思っておりまして、依拠は、どこかで信頼できたことを確認できたからそれを活用することだと思いますが、その確認できている信頼性と確認したい信頼性が――信頼性というか安心・安全性が、一致しているかの再確認は必要かと思います。

私は、マイナンバーのほうの委員もやらせていただいておりましたけれども、NISTという技術の安全をつくる機関があり、そのNISTでSP800-63が定められており、本人認証におけるアシュアランスレベルが定義されております。

ここでは、AALとかIALとかFALという言葉が出てきますが、どういった形で発行されたIDなのか、マイナンバーカードにおいては、IAL３、AAL３と最もレベルが高いもので発行されているんですけれども、それをスマホに移行する際には、それをちゃんと準拠するというか、デライブドする形で安全性を担保する仕組みを設計しました。

同様に、今回話題に挙がっている依拠というものが、どういうレベルの安全性をどういうものに対して適用しようとしているのかのレベル合わせは、しっかり確認が必要かと思いました。依拠することに関しては、それによってより効率的になる、便利になる、安全になるということであれば良いですが、そこのレベル感の確認は今一度しっかりすべきかと思いました。

３点目ですが、今回、犯収法と携帯法の話、２つの法令が出てきておりますけれども、

それぞれのよい点をうまく合わせていくことが必要だと思います。非常に似た場所で使われる法律である以上、２つの整合性という点も考慮していくべきではないかと思いました。

【大谷主査】　専門家ならではの御意見、どうもありがとうございました。特に依拠については、御指摘の点、私も非常に気になっているところでして、これは楽天モバイルの小田様のほうから、何か今のコメントについて補足説明いただけることがありましたらお願いしたいのですが、いかがでしょうか。

【楽天モバイル株式会社（小田氏）】　辻先生、大谷先生、ありがとうございます。

当社としましては、そういう意味では2012年から、犯収法の世界の中では、依拠という仕組みで、事業者間で本人確認結果を使うことが実施できています。

そこで、私のほうで挙げさせていただいたのはワンタイムパスワードだけでしたが、業界としてノウハウがあり、不正対策に取り組んでこられたと理解しております。

そういった意味で、犯収法の世界での本人確認における依拠の実績、ノウハウを、携帯法の世界でも実現できないかと考えておりますので、そういった成功事例といいますか、まさに警察庁様からあった、画像の確認に依存しない、非対面の本人確認方法として、こういった依拠の仕組みができないかと考えているところでございますので、お話のあったアシュアランスレベルのところ等も、おそらく携帯法で改めて検討するに際しても、犯収法の世界でどのように整理しているのかを参照すべきと考えているところでございます。

【大谷主査】　ありがとうございます。ちょっと難しいところがあるかなと思いました。幾つも論点があると思います。

鎮目構成員から、御発言をお願いしたいと思います。

【鎮目構成員】　先ほどの辻先生の御指摘は非常に参考になりまして、関連する話ではございますが、私自身は１人のユーザーとしても、非対面による本人確認というのは非常に利便性が大きいと考えてきましたが、警察庁の御説明や、先ほどの事務局の御説明などを伺いまして、画像による本人認証というのはやはり相当問題が大きいということで、利便性があるとはいえ、今後廃止していくという方向は取らざるを得ないのかなと。その点については賛成でございます。

他方、それに代替する方法として、やはり本人確認の確実性という点では非常に優れていると考えられるのは、マイナンバーカードによる本人確認と思われまして、政府の努力もあってマイナンバーカードが非常に普及した状況などを踏まえますと、もちろん、なぜ画像による本人確認ではもう駄目なのかということを丁寧に説明して納得いただく必要は

あるかと思いますが、そちらに移行していくということは必要なのかなと思います。

ただ他方で、楽天モバイル様のほうから、先ほど依拠による本人確認についても導入すべきという御指摘がございましたが、その辺りは、画像による本人確認を廃止して、ICチップが入った、あるいは電子署名に係る本人確認に専ら移行するということでは、おそらく国民の利便性を損なうという御配慮に基づいていると思うのですが、その辺りはどういった考えに基づいて、依拠による本人確認方法という、先ほど辻先生から、確実性のレベルが同じであることを担保する必要があるという御指摘がございましたが、なぜそれを御提案されるのかを、もし補足があれば御説明いただけると大変助かります。

【大谷主査】　議論を整理していただきましてありがとうございます。

今、鎮目構成員のほうからも依拠についてコメントをいただきましたが、この点につきまして、もう一度小田様のほうからコメントをお願いします。

【楽天モバイル株式会社（小田氏）】　まず、警察庁様からも詳細御説明があったように、画像を人間が目視で確認する本人確認方法は、AI等の現状を踏まえると、今後非常に厳しいだろうと、当社としても理解しているところでございます。

他方で、非対面の携帯電話契約においては、まさに今問題になっている方法が非常に多数、もう９割を軽く超える割合で使用されていると、業界としては理解しております。

そういった中で、マイナンバーカードを使った本人確認方法についても、各社、今急ピッチで検討を進めているところでございますが、医療機関等の実施状況等を鑑みましても、どこかのタイミングで広く使われるというところが、まだ見通せない状況ではあると理解しております。

そういった中で、信頼できる本人確認方法、要は画像確認をしない形の本人確認方法を早急に普及させる必要があるということを我々としても考えまして、そういった中で、依拠という方法であれば、あらかじめ本人確認を金融機関等のしっかりしたものに依拠することで、少なくとも画像を確認するものよりは非常に安全性が高く、また、10年以上業界で取り組んでこられた実績等もあることから、次善の方法として取り得るかと考え、本日御提案させていただいた次第です。

【大谷主査】　繰り返し丁寧な御説明いただきましてありがとうございます。

辻構成員から挙手いただいていますため、御発言をお願いします。

【辻構成員】　小田様に確認ですが、先ほど私が質問した話であったり、その前の質問もそうだと思いますが、依拠される側とする側で、それの基準は統一されているかという

ところが、気になりました。

例えば、過去に銀行口座開設をしました、過去にどこどこで開設をしました、その時確認されている基準は一緒なのかというところがもともとの質問でしたが、そこはお答え可能でしょうか。

【大谷主査】　質問としては、より確実な本人確認方法を使った実績に基づいて、それに依拠するのであれば安全ではないかというコメントではないかなと思うのですが、その辺りを、事実関係を補足していただけると大変ありがたいです。

【楽天モバイル株式会社（小田氏）】　当社の資料７ページにございましたところで、若干省略した部分があるので、その部分も含めて御説明をさせていただきますと、実際には金融機関とのリファレンス申込みの受付けですとか、あるいは本人確認情報を金融機関から収納機関に戻すところに関しまして、例えば銀行の場合は、NTTデータさんが使われているネット口座振替受付けのゲートウェイ等を使用していると確認しております。

こういったプラットフォームを提供している事業者さんのほうでも、当然セキュリティー等を確保した形で提供されていると理解しておりますので、こういった形で、業界として、銀行さんではプラットフォームを提供されているということは確認してございます。

あとは、クレジットカード会社さんにおいても同様に、プラットフォーム事業者さんがいらっしゃると理解しておりますので、そういった会社さんが確認して、こういった依拠等に対応できる金融機関さんと連携しているという仕組みと理解しております。

【辻構成員】　大変細かくて申し訳ないんですけれども、この図では、収納機関Aさんが新たにサービスを提供し、本人確認済みの銀行Bさんがいますが、この収納機関A、銀行B、何とかC、Dとあって、それは業界でそういうルールをつくられており、その業界の中でのルールにおける「本人確認済み」の定義は、ちゃんと一致しているのでしょうか。

【楽天モバイル株式会社（小田氏）】　そのルールというのは、違う銀行でも同じにやっているんですかという質問ですか。

【辻構成員】　そうです。

【楽天モバイル株式会社（小田氏）】　そういった意味では、本人確認をしているということで同一ルールであると認識してございます。

【辻構成員】　厳密な意味でいうと、さきほど話にあがったSP800-63でいうIAL、AALは一致していることになるのでしょうか。

【楽天モバイル株式会社（小田氏）】　そのように認識しております。

【辻構成員】　一致しているもの同士しか信頼し合わないという、ちゃんと業界のルールがあるということですね。

【楽天モバイル株式会社（小田氏）】　そのように理解しております。

【辻構成員】　細かくて申し訳ありません。そこの確認をしたかったということであります。ありがとうございます。

【大谷主査】　どうもありがとうございます。非常に細かい確認ではありましたけれども、重要な確認事項だと思いますので、小田様のほうでも丁寧に御説明いただきましてありがとうございました。

それでは、星構成員、お願いします。

【星構成員】　クレジットカードについて、つい先日も過去最大541億円の不正利用被害があったと報道されていまして、たまたま私のとこにいる中国人留学生が、これに近いテーマを勉強しており、日本ではこのような状況だが、中国でも似たような状況になっているのではないかと聞いたところ、中国は、かつてはかなりひどかったけれども、今、クレジットカードの不正利用については、正式な統計のある国ではないので分からないですが、大分減っているような印象だということでした。

それはなぜかというと、オンラインでの決済、アリペイとウィーチャットペイのいずれかでほぼ固まっていますが、ウィーチャット自体の本人確認がものすごく厳しいと。その前提は、携帯端末の、特にSIMの本人確認が非常に厳しいというものから成り立っていて、それとリンクしているウィーチャットペイ、クレジットカードの使用も、分割払いの場合にはクレジットカードという形になるでしょうけれども、それの利用とリンクしているため、不正利用は非常にしづらくなっているということがあるのではないかというような話を聞きました。ひょっとしたら間違っているかもしれないんですが。

やはりこれは非常に大事な話と思っていまして、先ほど警察庁様の資料の３ページにありましたけれども、いかに身元を偽装できるか、本人確認ができないようにするかというところが、こういったスキームにとってみれば一番根幹といいますか、犯罪者が欲しがるところでして、それに対し、モグラたたきといいますかいたちごっこが続いてきているというところがあるわけですよね。

その中で、携帯電話というのが、画像という意味ではなくて、運転免許証であるとか、そういったようなものと同じような存在になってきていると、携帯電話がもう社会のハブになっているという御説明がございましたけれども、そうしますと、やはり携帯電話の

SIMの身元の確認も、本物の運転免許証と同じレベルでしっかり確保できるようにしておく必要があるのではないか。

逆に、そこがしっかり確認できているということであれば、それと同じレベルで、ほかのサービスの提供というところに関しても、本人確認コストなどの負担軽減、これは業者サイドとしても利用者サイドとしても、同じような形で、一々あちこちで本人確認をしなくて済むという、依拠の形が確認できてくるだろうと思います。

そうしますと、携帯電話側の確認を徹底させるのか、銀行側の確認を徹底させるのかというのはニワトリ卵の話なのかもしれませんが、そこは前提として両方しっかり確認できているということがないと、その確からしさというところで、依拠の場合、１か所破られたら全てが虚偽での認証という形になってしまいかねないという問題はあろうかと思いますので、そこも含めてですね。

あともう一つ申し上げると、携帯音声通信役務だけで本当にいいのかということも含めて、将来的には考えていかないといけない問題があるのではないかなと思った次第です。

それともう一つ、一生懸命取り組んでいらっしゃる業者様を前にして申し訳ないんですけれども、ではかの国で全く問題がないのかというと、やはり蛇の道は蛇という形で、色々な抜け穴みたいなところはあるようですが、内部不正対策といったようなところも含めて、業者様の自主的な対応だけということではなくて、法令レベルでそこも担保するというようなところがないと、なかなか業者様の負担も減らない、利用者サイドの負担も減らないというようなことが起きてしまうのではないのかと思った次第です。

【大谷主査】　具体的な例も挙げていただきまして、大変整理していただいたと思います。

それでは、沢田構成員、お願いします。

【沢田構成員】　事務局から御説明いただきました中に、デジタル重点計画の話がありました。マイナンバーカードの公的個人認証に原則として一本化するという方針は、セキュリティーもさることながら、マイナンバーカードの民間利用促進という文脈だったのかもしれないですが、鎮目先生もおっしゃっていたように、これが正しい方向だと思います。画像を廃止する方向はよいとして、それ以外のものを残すとか、追加的な方法を認めるかの判断基準としては、利便性以外のメリットやデメリット、辻先生がおっしゃっていたような確実性についても議論すべきだと思います。

とはいえ、私自身は技術的なことは素人ですので、参加するに当たって周りのセキュリ

ティーの専門家のお話も伺って意見を聞いてみました。その上で、楽天モバイル様に３点ほど御質問させていただきたいことがございます。技術的なことではないです。

一つは、実施済みの本人確認結果を提供する側、銀行やクレジットカード側のインセンティブは何かということです。犯収法でも、口座振替の登録をするときに、併せて本人確認結果を連携するという、楽天モバイル様の資料でいうと７ページの辺りに書いてあり、さらにオプションサービスとして手数料も徴収されるということでしたので、銀行のほうから見ても必然性があると思えました。

携帯の通信料金の引き落としに使う銀行とかクレジットカードとかでしたら、それと同じことが言えるかもしれないのですが、ほかの携帯会社の行った本人確認結果に依拠することは、MNP等によりお互い様の関係で取り組めるからということでしょうか。他の携帯会社としては、自社がコストをかけて行った本人確認の結果を他社に利用されることをどのように見ているかというのが質問の１点目です。

２点目は、辻先生がおっしゃっていたことと若干通じるかもしれないですが、銀行側の本人確認がどれくらいの精度かということと、結果として駄目だったときの責任分担についてお尋ねしたいです。

数年前ですが、電子決済サービス、何とかペイとかで、なりすましのアカウントが大量に作成されてしまった事件で、その時の本人確認を、電子決済サービス側ではあまりちゃんと行っておらず、銀行に依拠していたという話もあったかと思います。本人確認が十分でない銀行もあったため、結果としてなりすましが起こってしまったと。本人確認書類の画像が流出してしまったという問題も別途ありますが。

本人確認の精度が十分ではなく、結果として不正が発生したときに、例えば被害者への補償など責任をどちらが負うか、当初本人確認をした銀行が負うのか、それとも＋αで本人確認をしなかった携帯会社が負うのかといったようなことは、あらかじめ事業者間で契約しておくのだと思いますが、その辺りをどのように考えられているか、というのが２点目です。

３点目は、個人情報の話です。利用者としては、銀行で口座を開設するときに本人確認のための情報を提供するわけですが、その情報をほかの事業者の本人確認にも利用するということは、もちろん規約で書いておけば目的外にはならないと思いますが、提供先が決まっていればまだよいとして、将来どこかとシステム連携するかもしれない、ということではちょっと不安があるので、まずはどこまでの情報が提供されるのかをお聞きしたいで

す。携帯会社が銀行からもらうのは、本人に間違いないです、という結果だけなのか、それとも、銀行が利用者から本人確認するために取得した生の情報も提供されてしまうのかが３点目の質問です。

楽天モバイルさんの場合は、楽天銀行も楽天カードもあり、そもそもグループで共同利用することになっていると思いますから、あまり問題にならないのかもしれないですが、グループを超えて依拠する場合にはどのように考えたらいいのかというのが３点目の質問です。

【大谷主査】　貴重な御質問ありがとうございます。３点それぞれ違っているのですが、小田様のほうで御回答をお願いします。

【楽天モバイル株式会社（小田氏)】　まず１点目、提供側の、特に携帯電話事業者間の場合のインセンティブはどのように、ということですが、携帯電話業界は長年、いかに消費者の方が円滑にスイッチングをしていただくか、要は通信サービスに関してはやはり携帯を使ってみないと分からない部分、電波の入り等いろいろございますので、それがお客様のニーズに合わなければスムーズに、前の事業者が縛りを設けることなく別の事業者に移行できるということをいかに促進するかということを、事業者としても総務省様と一緒にずっと取り組んできた経緯がございます。

そういった観点を鑑みますと、まさにこういったMNPというのは、消費者の方が次の事業者に移る際に非常に重要なステップになりますので、これに関しては、「お互い様」と言っていただいたのですが、まさにこのお互い様の観点で、消費者の方がよりよいサービスを選んでいただけるようにということで、事業者として大過なく取り組むべきことであろうと、当社としては考えてございます。

１点目は以上でございます。

２点目のなりすまし対策のところですけれども、そもそも本人確認が十分でない事業者さんに依拠するということ自体が事業者として非常にリスクですので、きちんとなりすまし対策等がされた事業者さんとだけやるということが、この依拠を実際に事業者として取り組む場合に非常に重要なことと考えてございます。

また、そういったことに取り組むことによって、ある種、依拠してもらえない金融機関さんにとっても、セキュリティーレベルを上げて消費者の方の利便性を上げるとインセンティブにもなるのかなというふうに考えています。そういった意味でも、依拠をお願いする事業者が、しっかりその金融機関さんの対策等を見極めて、個別にお願いしていくとい

う取組が必要だろうと考えてございます。

それから３点目でございますが、本人確認結果の依拠に際してどういった情報が渡るかというところでございますが、当社のほうで例に挙げさせていただいた、銀行さんから依拠する場合に関しては、本人確認結果のみを連携していると、つまり、依拠している元の銀行さんに、本人確認情報として本人確認の３情報と券面の情報がしっかりありますよということの、「ありました」というフラグだけが渡ると聞いてございます。

また、当社グループ内におきましても、携帯電話と各金融機関はプライバシーポリシーが別になっておりまして、個別にプライバシーポリシーを持って情報も管理してございますので、仮にこういった依拠等を導入して契約者情報のやり取りをする場合には、都度、個別に契約者の方、利用者の方から共有内容等の許諾をいただいて、その範囲でのみ利用するという形を取ろうと考えてございますし、現在もそういった形で実施してございます。

【沢田構成員】　ありがとうございました。分かりました。

【大谷主査】　丁寧な御回答ありがとうございました。

２番目の御質問についての回答で、ちゃんとした本人確認をやっている事業者かどうかの見極めをして、つまり、提供を受けた側で全面的に、もし万が一のことがあったときはリスクを負うというか、被害者への補償も含めて、法的に必要になった場合の責任を負うという考え方でいいのかどうかという確認をお願いします。

あともう一点ですけれども、３つ目の御質問のところで、結果のみのフラグの共有ということなのですが、調査したい個人と、本人確認済の個人が一致することの確認というのはどういう手続で行うのか、簡単に御説明いただけるとありがたいです。

【楽天モバイル株式会社（小田氏）】　１点目につきまして、お客様と実際に契約をいただいているサービス提供者、今挙げている例であればまさに携帯電話事業者が、何らかサービス利用上で問題が生じた場合に、会社として責任を負うべきと考えてございます。

それから２点目のところで、情報の渡し方ですが、具体的には、例えば携帯電話事業者に申込みをする際に、当然ながら携帯電話事業者のほうに氏名ですとか住所、生年月日等の本人確認に関する情報を、先にまず、非対面であれば入力等をされるかと思います。その情報を、今度は金融機関側に渡しまして、それと一致する方が口座の所有者としていらっしゃるかというところを照合しまして、その照合結果が合いましたという場合のみ、本人確認結果として、その本人確認書類があることを含めて連携するということになっておりまして、逆に相違等があれば、携帯電話事業者側で、一致しなかったことをもって改め

て本人確認をお願いするという手続になると考えてございます。

【大谷主査】　大変よく分かりました。ありがとうございました。

それでは山根構成員、お願いいたします。

【山根構成員】　私からは、３点コメントさせていただきます。

１点目が、まず廃止の方向性で検討している携帯法の本人確認の方法についてですが、これについては、今日の警察庁からの御発表などを見ても、やはり本人確認書類の偽造というのは大きな問題になっているかと思いますし、そういった現状を踏まえると、書類の画像を使用する方法であるとか、あるいは写しを使用する方法というのは廃止せざるを得ないと思いますので、方向性については賛成でございます。

２点目について、先ほど来、依拠についていろいろと話が盛り上がっているところではございますが、私はどちらかというと犯収法になじみがあるものでしたので、この会合前までは、こういった依拠の方法は十分に考えられるのではないかと思っていたところです。

金融機関においても、犯収法に基づいて、携帯法と同じような確認方法が規定されており、同レベルの本人確認を行っていることかと思いますので、重ねて携帯事業者の方で確認するというのは、ある意味、リソースを二重に使ってしまっているという面があると思いまして、そういった観点、社会的なリソースであったり利便性という面から、依拠の方法について考えることは十分検討の余地があると思いました。

ただ、今回の会合のお話をいろいろと聞き、どれだけ信頼性を確保するかというところは、やはりまだ検証の余地があると思ったところでございます。

先ほど沢田構成員や大谷主査からの御発言の中でもあったように、実際に問題が起きた場合の補償等について、金融の分野、ペイメントサービスが銀行口座と連携を行うような場合は、先ほど沢田構成員からも言及があったような、ペイメントサービスでの不正利用の事案などを受けて法令の改正が行われ、ペイメント事業者の方で利用者に対する補償の方針などを表示しなければならない、説明しなければならないというような義務も課されているところです。

金融機関とペイメント事業者のどちらが責任を負うかというところは、事業者間の契約によって変わり得るところではありますが、実態としては、ペイメント事業者が責任を負うという形になっているところが多いのではないかと思っている次第です。

そのため、先ほど楽天モバイル様からは、携帯事業者の方が責任を負うべきではないかと御発言がありましたが、現在の実態とも合った方向性なのかと思った次第でございます。

また、楽天モバイル様からは、法人の本人確認の方法についてもいろいろと御提案がありましたが、確かに、例えば登記情報提供サービスを用いた方法は、現状、実際に紙の登記簿謄本の提供を受けなければならないということになっているかと思いますが、登記情報提供サービスを利用することは、信頼性においてもあまり変わるところはないと思いますため、十分検討の余地が、こちらもあるのではないかと思った次第でございます。

以上になります。

【大谷主査】　犯収法の実務などについて、詳しく御解説いただきましてありがとうございました。

中原構成員からも御発言お願いします。

【中原構成員】　警察庁からプレゼンテーションがあった中で、契約者確認の求めがスライド９ページで説明されていて、構成員限りとなっていますが、その左下に挙げられていた事業者アンケートが非常に印象的でした。規制をかいくぐって悪用するという実態が存在すること、そして、携帯電話事業者各社で、問題認識やその対応のスピードが異なることが表れているのではないかと思いました。

一つは、契約者確認という仕組み自体が十分に機能しているのかということは、常に検証していく必要があると思います。携帯電話不正利用防止法第８条に基づいて、警察署長が携帯電話事業者に対して契約者確認を求めた上で、９条に基づいて、携帯電話事業者が契約者確認をする。その具体的な方法としては、この法律の施行規則の13条が定める方法で本人特定事項の確認がなされる。15、16条に基づいて、役務提供契約上の地位を有していることの確認、通話可能端末設備等を所持していることの確認がなされる。これは約款上の対応なんだと思いますが、契約者確認ができなかった場合には、携帯電話事業者によって利用停止措置が取られるという仕組みであると理解しています。

この契約者確認についても、おそらく契約締結時の本人確認に沿ったような見直しが行われていくのだと思いますが、これは不正利用に直接対応していくための最重要な仕組みだと思いますので、その実効性は常に検証することが重要だと思います。

もう一つは、契約者確認について、このアンケートで例示されているような規制のすり抜けについて、個々の携帯電話事業者に周知することはもちろんのこと、携帯電話事業者間で対策について情報を共有したり、対策を共同で練り上げたりといったことが、既に行われているかもしれませんが、推進されるべきだと思います。

同じことが、おそらく契約締結時、あるいは新たな契約を締結するときの本人確認につ

いても言えるわけで、楽天モバイルさんからのプレゼンテーションで、犯収法上の依拠の手続を携帯法でも認めてほしいという御要望がありましたが、他社の本人確認を信頼してよいと。本日いろいろ議論されていましたように、セキュリティー上の諸般の要請が満たされているという場合には、事業者の負担を軽減するために、そのような仕組みを認めるということは、将来的に一定の合理性が見いだされ得るのではないかとは期待されるものと思いますが、特に楽天モバイルさんのスライド９ページにあるように、携帯電話事業者間でのシステム連携で済ませる場合には、やはり業界全体として、本人確認が適切な方法で行われていることが大前提になると思われます。この点でも、携帯電話事業者間でどのような横の連携がされているのかが、今後重要になってくるのではないかなと思いました。

【大谷主査】　ありがとうございます。この点につきましては、事務局からコメントをお願いします。

【小澤利用環境課課長補佐】　まず、契約者確認につきましては、警察庁さんないし警察署との連携でこれまでもやってきたところでありまして、今回も御発表の中で一部、課題認識について御紹介いただきましたが、これについては、先ほど私のほうから説明したデジタル時代の見直しのところに入れられておりませんので、その他リスクとコストのバランスを見た上で、施行以降の効果検証も見ながら、契約者確認の方法の定めについても見直しを図るべきだと思いますので、そこについては検討したいと思います。

【大谷主査】　契約者確認についても改めて検討いただくという方向で整理できればと思います。

星構成員から、音声通信役務だけでいいのかと問題提起もありましたが、この点について、もし事務局のほうで何かコメントがございましたらお願いしたいと思います。

【小澤利用環境課課長補佐】　ありがとうございます。携帯音声通信役務の範囲は省令で定めており、ちょうど昨年、050アプリの悪用が多いということで、昨年夏に改正しましたが、この省令についても警察庁さんと連携して、最新の手口を見ながら見直しを図ってきたところですので、今後もしっかり見直してまいります。

おっしゃるように、そもそも携帯音声だけでいいのかというところも議論があるとは思いますが、そうすると法律全体の在り方をどう考えていくかという論点もあると思いますので、私の一存では申し上げにくいですが、確かに、犯罪の手口、悪用の状況を見ながら、法律の在り方も検討されていくところと思いますので、そちらについても御意見として承ります。

【大谷主査】　確かに、事務局の一存ではなかなか答えにくいことだと思いますが、やはり犯罪の手口というものとの関わりも大きいと思いますので、構成員の皆様におかれては、実態に即し、必要な施策について、いろいろ御提案いただきありがとうございました。

それでは、沢田構成員、お願いします。

【沢田構成員】　先ほどちらっと申し上げました、写真付き本人確認書類を安易にデジタルな状態で送ってしまうことの危険性が、だんだん大きくなってきていると思います。

いろいろなサービスに登録しようとしたときに、本人確認をするので本人確認書類、免許証のコピーを送るように、といったことが行われています。適正に行われているケースが多いとは思うものの、闇バイトに応募してきた人に免許証の情報を送らせるようなケースもあるため、その結果どうなるのか、悪意のある先に送ってしまったらどうにもならないということをもっと周知しなくてはいけない。だとすると、逆に真面目な事業者はそのようなことを行わないといった形になっていかなければ、ユーザーとしては、なかなか区別がつきにくいと思ったところです。携帯法の中に、本人確認書類の写しを一定期間保存しなければならないという規定があると伺いましたが、それ自体リスクの元でもあるように思います。過去、代理店等から情報が流出してしまった、持ち出されてしまったケースもあると聞いておりますので、その辺りのことも、将来的には考えていかなければならないという感想を持ちました。

【大谷主査】　たくさんの論点があり、議論も尽きないところではありますが、この辺りで検討を終了させていただきます。

今日は活発な議論、それから、御提案いただいた楽天モバイル様も、一人一人の質問に丁寧に御回答いただきましてありがとうございました。

警察庁からも、非常にどきどきするような、資料の御説明をいただきましてありがとうございました。

それでは、次回の会合につきまして、事務局から御案内をお願いします。

【小澤利用環境課課長補佐】　次回の会合については、今回の本人確認の見直し議論の続きということになろうかと思いますが、日程については、別途、事務局のほうから御案内します。

【大谷主査】　それでは、以上で不適正利用対策に関するワーキンググループの第３回の会合を終了とさせていただきます。本日は皆様遅くまで、お忙しい中御出席いただきましてありがとうございました。