

不適正利用対策に関するワーキンググループ（第4回）

令和6年5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4回会合を開催いたしたいと思っております。事務局の利用環境課、小澤でございます。よろしくお願いいたします。

定例でございますが、まずウェブ会議の開催上の注意事項を御案内いたします。

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きます。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きますので、音声設定は変更しないようお願いいたします。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させていただいて、映像もオフにさせ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、それを見て、座長から発言者を指名いただくという方式で進めさせていただきたいと思っております。御発言いただく際はマイクをオンにして、映像もできればオンにして御発言をいただきたいと思っております。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お願いいたします。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お願いいたします。また、チャット機能で随時、事務局や主査宛てに連絡をいただければ対応させていただきます。と思っております。

本日の資料は、議事次第と、本編の資料として資料4-1から4-3を御準備しております。

注意事項は以上になります。

また、本日の出欠状況でございますけれども、中原構成員が御欠席となっております。

それでは、これ以降の議事の進行を大谷先生にお願いしたいと思っております。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。

今日が4回目ということで、今日の議事は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に関する関係者ヒアリングということで、デジタルアイデンティティ推進コンソーシアム、それからイオンリテール株式会社、日本通信株式会社からそれぞれ御発表い

ただきまして、その後に、質疑応答ですとか構成員の皆様との意見交換を進めていきたいと思えます。

それでは、早速でございますが、デジタルアイデンティティ推進コンソーシアムの日下理事、よろしくお願いいたします。

【デジタルアイデンティティ推進コンソーシアム（日下氏）】 それでは、早速始めさせていただきます。よろしくお願いいたします。一般社団法人デジタルアイデンティティ推進コンソーシアム、Govtech協会代表理事の日下と申します。よろしくお願いいたします。

本日、私からは、本人確認手法のJPKI一本化を前提とした不正対策と利便性の高い本人確認の実現というテーマで、貴重なお時間いただいております。よろしくお願いいたします。

まず、今日の話の前提になるところで、釈迦に説法かと思いますが、昨年5月にデジタル庁のほうからデジタル社会の実現に向けた重点計画という資料の概要のところにも、本人確認手法のカードへの一本化と記載され、犯罪収益移転防止法、携帯電話不正利用防止法について、公的個人認証に原則一本化していこうというような報道がなされたところは皆様も御承知おきかなという中で、こういったワーキングも行っているかなと認識しております。

今日、少し背景からお話しながら、具体的に、一本化に向けて、今後どういった課題があるかですとか、民間企業にとってもどういったことをしていくと利便性が上がるかについてお話しできればなと思っております。まず、少し背景としてお話しさせていただくと、2015、2016年頃から、厚みを見るタイプの画像解析型の本人確認、いわゆるeKYCというのが主流で広がってきたんですけれども、昨今、マイナンバーカードも含めた偽造身分証、そういったものがどんどん出てきていて、かつ精度が上がってきていると。ネットで検索すると、安心・安全の偽造身分証という、何が安心・安全なのか分からないんですが、そういったものが本当に低コストで作れてしまう時代になっています。

海外を見ると、こういった身分証の発行機関である公的機関に台帳照合を行ったりですとか、照合を行って身分証の真正性を検証するようなインフラが整備されているケースもありますが、日本の場合、これまでよく身分証として使われていた運転免許証については、特にこういう台帳照合を民間企業が行う手だてはないということで、あくまでもオンラインでもオフラインでも、最終的な信頼性のよりどころというのは目視確認になってしまっ

ているというところが大きく課題としてあるのかなと思います。

加えて、まさに直近のニュースの抜粋にはなりますけれども、従来のこの書類の画像＋容貌を使った本人確認手法が限界に来ているんじゃないかという中では、実際には、左側のとおり、事前にビデオ通話をしたときに顔などの写真のデータを記録されてしまって、そのデータを使ってネットバンクの口座開設をされてしまったという70歳の女性の方のニュースが出ていたりですとか、右側は日立製作所さんが二、三年前に出したレポートなのでちょっと古いんですけども、ディープフェイクを用いたeKYCのなりすましが実現できてしまうのかという実証が行われていまして、実証結果としてもディープフェイクを用いて、ビデオチャットですとか、画像解析型のeKYCで他人になりすまることが技術的に容易になってきているという社会に、突入しているのかなと思っております。

今回、オンラインの話だけになっていますけれども、実際には、オンラインの本人確認手法が、今回の話を含め、どんどんJPKIで強化されていくと、次の不正のターゲットというのは、間違いなく対面の本人確認になってくると思っております。こういった中で、実際に、携帯ショップでのいわゆるSIMスワップという事件が数件発生しているというところで、こういったところについても今回、議論できるとよいのかなと考えております。

今回のお話なんですけれども、オンライン本人確認手法についてJPKI一本化を前提にと考えたときに、当然、オンラインの本人確認の強化という話にはなつてこようかと思うんですけれども、ここをJPKIに一本化していく中で、併せて発生してくる課題についても、同時に検討していく、解決していくことで、不正対策を強化しつつも、特定事業者あるいは携帯事業者さんの負担を減らしながら、ユーザーにとって利便性が高い本人確認を実現できるといった社会を実現していけたらいいんじゃないかなと思っております。

大きくは左側を実現していただきたいことと、その背景と書いているんですが、1つは従来、JPKIやマイナンバーカードが普及する前は、本人確認手法の規定がばらばらだった携帯電話不正利用防止法と犯罪収益移転防止法を、今回を機に、できる限りそろえていただけるとよいのかなと考えております。

背景として、最近では事業者がもうグループ企業内で通信事業と金融事業を両方運営しているケースも大分増えてきていると思っております。そういった中で、それぞれの省令がばらばらで規定がそろっていないことで、事業者の対応負担が上がってしまうということが起きているのかなと思います。そういったことも含めて、社会全体の本人確認にかかるコストを下げっていくことによって、コストがかかるから厳格な本人が確認できないといった

環境をなくしていくということも非常に大事なんじゃないかなと思っております。

それを実現していく上での実現に向けた検討案として、今日の論点、大きく3つ御用意してきました。1つはオンライン本人確認手法の原則JPKI一本化に向けてというところで、今、書類の画像+容貌の写真アップロード、いわゆるeKYCの厚み方式の廃止を検討されているかなと思うんですが、廃止のインパクトというのはどういったものなのかというのを少し触れさせていただければと思っています。

2点目が依拠による本人確認の見直しということで、前回のワーキングでも楽天モバイル様から御発表があったかと思うんですが、これまで犯収法のみ適用のあった既に行われた本人確認結果を活用するという部分を携帯法にも適用するというところで、JPKI一本化の後の不正対策強化を実現しつつも、事業者、ユーザーの利便性を考慮した本人確認が実現できるんじゃないかなと思っております。

3つ目が、オンラインの本人確認だけではなくて、まさに同時にこの対面本人確認における真贋判定。まさに昨今、話題になっていますけれども、偽造マイナンバーカード、こういったところの真贋判定を、目視に頼らず、技術的にやっていく仕組みが必要なんじゃないかなと思っております。

1つ目のJPKIへの一本化なんですけれども、既にこのワーキングでは、書類の画像+容貌の写真アップロード、いわゆる携帯法の厚み方式の廃止が検討されているかなと思います。これは実際に犯収法と足並みをそろえようとなると、犯収法の場合はホ方式が廃止になっていくわけなんですけれども、そういった際にインパクトのある事業者の数を、携帯電話事業者、金融事業者だけじゃないんですが、ざっとインターネット上で、従来のeKYCサービスを提供する事業者の導入企業数を推計すると、700社以上に及ぶということが分かってきています。この中の大部分が携帯事業者、金融事業者ですので、JPKIに一本化する、この厚み方式が廃止されると700社の企業に一定の影響が出るかなと思っています。この影響をポジティブにしていくのが、本来、今回の目的かなと思うんですけれども、単にJPKIの一本化だけ、この旧来方式の廃止だけでは、せっかく先行してこのeKYCを導入することで、そのデジタルサービスを便利にしようということで取り組んでいる事業者にとって、むしろ何か数年前にeKYCに取り組んできたこと自体が負の遺産になりかねないというところで、こういった事業者にとっての追加対応への負担ですとか、投資負担が大きくなってしまうと、社会全体で前向きに今回の改正が捉えられないんじゃないかという懸念もありましたので、そういったところについて、しっかりとケアできるような方向で進めら

れるといいんじゃないかなと思っています。

その中で1つ、今、マイナンバーカードについては、マイナンバーカードを使った公的個人認証。これは公的個人認証の制度というのがある中で、プラットフォーム事業者とサービスプロバイダ事業者という事業者が、大臣の認定を取ったうえで、本人確認をする必要があるというのですが、現状は携帯事業者も金融機関さんも、少なくともこの左側、緑のところの、サービスプロバイダ事業者という、大臣認定をプラットフォーム事業者の下で取得をし、その上で公的個人認証を使うということが必須になっています。つまり、特定事業者の皆さんはこの大臣認定も取得する必要があるということで、携帯法、犯収法の準拠だけではなくて、公的個人認証法に準拠した手続も追加で必要になってくるというところは一つあるのかなと思っています。

実際、正確な数字は申し上げられないんですが、現状今、こういったプラットフォーム事業者様、サービスプロバイダ事業者様の公的個人認証サービスは大体、初期費用、月額費用とこのマイナンバーカードを1回使うに当たっての従量課金という3つの構成になっていますが、この月額費用という部分が数十万円、10万円の前半台から、高いところだと50万円の後半台ぐらいまでなるというレンジになっています。従量課金については、今は、J-LISにおいて無料の措置が取られていますが、当初は20円の費用を払う必要があった中で、事業者さんによってはまちまちではありますが、50円から大体150円ぐらいのレンジで各事業者さんが提供をしていると。なので、場合によっては件数とかボリュームによっては従来のeKYCを使っているほうが、eKYCのランニングコストと公的個人認証へのスイッチングコストを考えると低くなる可能性もあるという中で、金融機関さん、携帯事業者が、SP事業者になることが必須であるというところが、今後どうなっていくかという点は課題なのかなと思っています。

2点目です。依拠による本人確認の見直しというところで、JPKIに一本化していく中で、仮に、ハ方式、ホ方式が完全に廃止されていくと、当然、携帯法、犯収法の適用を受ける各事業者様も、先ほどの大臣認定の事業者になる必要があるんですけども、現在はこの依拠の仕組みというのは御存じのとおり、犯収法のみを導入されていて、携帯法には導入されていません。この依拠の本人確認というのを、今回、JPKIに一本化していく中で、他事業者の実施済み本人確認への依拠を、携帯電話不正利用防止法にも導入して、さらには、この両省令の適用事業者間で本人確認結果を利用することを可能にするということができると、利便性が非常に上がるのではないかなと思います。簡単な比較表ではあるんですけ

れども、犯収法については施行規則第13条で規定されていて、依拠の元というのはどこなのかという、基本的には特定事業者、いわゆる銀行ですとか金融機関、クレジットカード会社に限定をされています。分かりやすく言うと何々銀行さんで本人確認済みの結果を、あるクレジットカード会社が使えるというような形になっているので、あくまでもいわゆる金融、特定事業者の範囲内で限定されていて、携帯電話不正利用防止法について規定はありません。なので当然、依拠元もないというところなのですが、今回、JPKIによる本人確認というのは、従来のeKYCですと、各民間事業者が本人確認をしているという事実を担保する、あくまでも民間企業さんが保証することでしかなかったわけなんですけれども、JPKIになると、当然、この大臣認定事業者として署名検証結果ということがデジタル上で記録されます。しかも大臣認定事業者の設備環境内でしか保管ができないという法律まであります。なので、それを前提に考えると、この本人確認結果の依拠元というのは、もしかしたら特定事業者に限定することなく、公的個人認証で本人確認実施済みの事業者、イコール大臣認定のプラットフォーム事業者またはSP事業者というのを依拠元にする形での、依拠による本人確認ということが両省令でできるようになれば、依拠元の本人確認の厳格さをしっかりそろえながら、事業者とユーザーにとって、何度も何度もJPKIの本人確認をしたりする必要がなくなることで、コストが下がったり、利便性が上がったりということができるとは思っていないかなと思っています。

これは実際にJPKIの本人確認はプラットフォーム事業者の環境の中に電子証明書と署名結果、署名データが保管されるというのは法律上、定められていますので、そこを当局が照会をかけにいけば、本人確認結果というのは必ずログが残っているということも保証されるのかなと思っています。

JPKIを前提とした依拠による本人確認で実施するには本人認証が重要というところで、先ほどの依拠のところについてなんですけれども、実際に依拠をやっていく上で課題になってくるのは、本当にその本人確認結果を、その本人が使っているのかということになってくるかなと思います。現在は、犯収法のみで、依拠元が特定事業者に限定されていますが、身元確認については、現状、ほかの特定事業者が犯収法に準拠したホ方式ですとか、そういったものの本人確認を実施したことを信頼している。本人認証、いわゆる間違いなくその本人確認結果をまた同一人物が使っているかということについては、特に細かな規定は技術上は担保されていないと。今後、これを犯収法、携帯法で担保する場合には、公的個人認証で本人確認実施済みの事業者＝大臣認定のプラットフォーム事業者また

SP事業者が依拠元になり、身元確認については、当然、公的個人認証法で担保されたレベルになると。本人認証について、ここが非常に重要だと思っていまして、やっぱりいわゆる本人認証レベル2以上のレベルを保証する必要があるのかなど。逆にここが弱いと、せっかく不正対策をしようと思っても、本人確認済みの結果を第三者に悪用されるリスクがあるんじゃないかなと思っております。この身元確認レベル、本人認証レベルについては、少し技術的な内容もありますので、参考資料で12ページから14ページにかけて記載していますので、また後ほど御覧いただければと思います。

最後になりますが、対面本人確認における身分証の真贋判定をする方法についてです。現状、対面での本人確認については、目視確認または真贋判定機が一部のメーカーで導入されているにすぎないという状況になっています。一方で、この真贋判定機なんですけれども、現状、各メーカーさんに確認をしたところ、真贋判定結果はメーカーは保証していないということになっていますので、判定器で偽物ですよと出ても本当に偽物なのか、あるいは本物ですよと出ても本当に本物なのかという結果は、メーカー側は免責事項になっているという状況もあります。そうした中で、マイナンバーカードに限った話ですけれども、精度の高い偽造身分証の検出を実現するという意味では、河野大臣の発言もありましたが、やはりICチップの読み取りなどの技術的にカードの真正性が表明される仕組みが必要じゃないかなと思うんですが、実際それを実現しようにも、やはり店頭窓口の設備投資ですとかコストの問題が出てくるのかなと思います。大きく実際、実現する方法としては、例えばマイナ保険証のカードリーダーの活用をするですとか、あるいは既存で存在しているユーザーのスマホ端末用のアプリで検証するですとか、いくつか懸念点はあるんですけれども、いくつかの検討方法はあるかなと思います。

参考になりますけれども、実際、J-LIS、地方公共団体情報システム機構さんのほうで、実はJPKI利用者ソフトというアプリが無料で公開されていますので、そういったものを使うと、店頭でマイナンバーカードを提示しつつも、マイナンバーカードのICチップの情報を読み取って、スマホ上に表示されている4情報と、マイナンバーカードの4情報が一致しているかということを確認すれば、無料でこういった検証ができるんじゃないかと思っております。他にもこういったサービスが無料で使えるものもあるかなと思いますので、こういったところを利用することで、対面本人確認の厳格化についても、オペレーションを改善しながらも、コストについては大きくかけずに、実現することもできるんじゃないかなと思います。

私からの発表は以上になります。ありがとうございました。

【大谷主査】 日下理事、どうもありがとうございました。

それでは、続きましてイオンリテール様、井原マネージャーにお願いしたいと思います。御準備いかがでしょうか。

【イオンリテール株式会社（井原氏）】 イオンリテール、井原でございます。それでは、説明させていただければと思います。当社からは、本人確認方法の見直しに関する意見を説明させていただきます。

まず、本日、このような説明機会をいただきまして、誠にありがとうございます。

それでは、2ページのほうに移らせていただきます。説明の前に、イオンモバイル事業部について少し説明させていただきます。当部署は総合小売業のイオンリテールの携帯販売部門でございます。1994年より携帯電話の代理店として事業を開始しておりまして、今年で30年の事業部でございます。事業内容は大手の通信事業者及び一部のMVNOの販売代理店と、2016年2月からMVNOとして、イオンモバイル通信サービスを運営させていただいております。このように、通信事業者でありながら、他の通信事業者の販売代理店も展開しているという非常に珍しい事業展開を行っております。特徴のほうは割愛させていただきます。

3ページを御覧ください。まず、今回の本人確認方法の見直しについて、不適正利用防止の観点から、マイナンバーカードによる公的個人認証を一本化するという方向性は本当に賛同させていただきます。ただし、実施に当たりましては課題も多いと考えておりますので、本日は当社で考えている課題3点について説明させていただきます。

まず、対象範囲について、本人確認手段であるために、原則、非対面ではなく、対面においても同じ時期に開始されるべきであると考えます。2つ目が利用者の課題でございます。非対面の場合、利用者側において、マイナンバーカードを読み取るための環境が必要となりますので、環境を誰が用意するのかということについては検討する必要があるかと思っております。そして、3つ目は事業者課題及び意見でございます。公的個人認証に対応するための開発期間の確保、あと開発投資に必要なコストに対しての御支援をいただけないかということ、あと事業者側が用意するマイナンバーカードを読み取るための環境ルールかと思っております。それらにつきましては、次ページ以降で詳しく説明させていただきます。

まず、対象範囲でございます。先ほども申し上げたとおり、対面についても同じ時期で開始いただくことを希望しております。理由につきましては3点ございます。1つ目は対面

での不正契約のリスク拡大です。対面を抜け穴とした不正契約が増大する可能性があるかなと考えます。特に当社はMVNOでは珍しく対面契約が多いということもありまして、ぜひとも対面も対象としていただければと思います。2つ目はルールが異なることによる混乱でございます。販売チャネルによってルールが異なることで、利用者側の混乱を招く可能性があるかなと思っております。契約手法によって手続が異なることは避けたほうがいいと思われま。より厳格な手順に合わせたほうが、結果的に単純化できるはずと考えます。3つ目でございます。課題が正しく整理されない可能性があるということです。対面も対象とすることで、全ての利用者を対象として検討することとなりますので、中長期的にも、利用者課題及び事業者課題を正しく整理できるのではないかと考えます。

続きまして、5ページを御覧ください。利用者の課題についてでございます。JPKIの一本化の実現に当たりまして、利用者側がマイナンバーカードを読み取るための環境を準備する必要があります。当社は高齢者のお客様の契約割合が非常に高く、お客様の環境というのが最も課題ではないかと考えています。いかに優れた仕組みであっても利用できないようなものでは意味がないと考えますので、利用者の環境については、ぜひとも丁寧に議論いただきますようお願いをいたします。当社で考えている課題や検討案を以下のとおりまとめております。

まず1つですが、読み取りに対応したスマートフォンを用意できない利用者の対応についてでございます。読み取り対応のスマートフォンは限定されておまして、現在、全ての利用者がJPKIによる手続が行える環境ではないかなと思っております。また、もし他人のスマートフォンを利用した場合、セキュリティーの問題があるかと思っております。マイナンバーカードの情報を他人のスマートフォンで読み取ることの危険性をどう考えるかということもあるかなと思っております。2つ目、利用者のリテラシーの問題でございます。公的個人認証の利用に必要となるパスワードについて失念されている可能性が非常に高いかと思っております。失念とかロックされた場合、パスワードリセットの手続が非常に面倒であるために、運用面に課題があると考えておりますので、ぜひこの辺りの見直しも検討いただければと思います。3つ目なんですけれども、その他の環境について、スマートフォンを利用しない手段としては、コンビニのキオスク端末とかATMの利用も可能ではないかと考えています。コンビニのキオスク端末などを利用して、JPKIによる契約手続が実現できれば、幅広い利用者での利用も可能ではないかと考えます。

6ページを御覧ください。事業者課題及び当社からの要望について説明させていただきます

ます。1つはシステム開発の期間の確保でございます。MVNOは様々な企業が参入しております。当社のようにIT企業ではない事業者もございます。そのために必要なシステム開発に対しての要件整理とか設計及び開発の期間については、事業者が置かれている環境によって大きく異なるのかなと思っています。つきましては、そこに当たりまして、多くの事業者の意見をぜひヒアリングいただくとともに、事業者が対応できるための十分な期間を確保いただけないかと思っております。2つ目が開発コストの問題でございます。開発の期間と同じように、内製で開発できる事業者もあれば、外部ベンダーで開発する事業者など、様々かと思っております。JPKIによる本人確認は、現在の本人確認システムとは別に、新たに開発が必要となりまして、多大なコストが必要となる場合も考えられますので、ぜひ開発に関する支援の検討もお願いできないかと思っております。3つ目、公的個人認証の利用料の引下げです。公的個人認証を活用することで、本人確認の厳格化を図ることができまして、現在発生している不適正利用の防止は徹底できるかなと思っています。なので、契約手続だけではなくて、様々な業務においても積極的にJPKIを活用することが望ましいかと思われまます。とはいえ、これは利用料がかかるということですので、ぜひ引下げの検討をお願いできないかということでございます。なお、当社ですけれども、既にJPKIに対応するための要件は整理しておるところで、早ければ本年度中にはリリースできるように準備しているところでございます。

最後、その他としてJPKIの活用についての意見でございます。公的個人認証を利用することで、本人確認の厳格化を図ることができまますので、様々な環境で使っていただくことで、より利用率も上がって、コストも下がるかなと思っていますので、少し意見させていただければと思います。まず、既存利用者の本人確認としての活用でございます。SIMスワップ等のトラブルが今、発生しているということで、SIMカードの再発行時の本人確認とか契約時以外でも、JPKIの活用は有効な手段かと思っています。現在、当社では物理SIMとeSIMについて、個別に再発行に関するルールの見直しを検討しているところでございます。再発行時だけではなくて、各種手続の本人確認手段としてJPKIは非常に有効な手段であると考えておりますし、様々な場面で利用した場合、結果的には利用率も上がりまして、利用料金も下がってくる可能性があるのかなと思っていますので、この辺りも検討いただけないかと思っています。2つ目は、通信事業だけに限った話になりますが、MNPワンストップです。MNPの大きな課題として、他者によるなりすましの問題があるんですけども、携帯電話番号に、利用者の任意で、例えば、マイナンバーカードの情報を紐付

けることが可能になりますと、MNPの手続の際に本人確認と同時に引継ぎをする携帯番号の確認もできますので、簡便にMNPが、結果的にはワンストップが実現できるのではないかなと思います。携帯番号は2段階認証等でも利用されているとおり、本人を確認するための番号なので、マイナンバーカードを紐付けることができれば利便性が高くてかつセキュリティが高い仕組みとなりますので、様々なサービスも利用できるのではないかと考えます。

最後のページは参考でございます。当社の直近の本人確認の書類の状況でございます。まだまだ免許証が圧倒的に多いんですけども、徐々にマイナンバーカードの利用も増えてきていまして、それに伴いまして、マイナンバーカードでの不正も、若干ではありますが、増えてきています。免許証につきまして、偽造等の知見も結構たまっておりまして、対策の手段もあるんですけども、マイナンバーカードにつきましては、まだ免許証ほどの偽造の知見もなければ、対策の手段も少ないということでございます。ただ、今後はさらにマイナンバーカードの利用が拡大するかと思いますので、公的個人認証の本人確認で非常に有効であると考えますので、実現に向けて、ぜひとも丁寧な議論をお願いしたいと思っております。

以上でございます。

【大谷主査】 井原様、どうもありがとうございました。

それでは、続きまして日本通信の福田社長をお願いしたいと思っております。

【日本通信株式会社（福田氏）】 日本通信の福田と申します。本日はよろしくお願いたします。

貴重な機会をいただきまして、まずありがとうございます。当社、日本通信はいわゆるMVNOという事業を世界で最初につくり出した、MVNOのまさにパイオニアとして取り組んできています。

次のページ、お願いします。1ページなんですけど、今現在、こういったラインナップで携帯電話サービスを提供しているという形なんですけど、これはMVNOとして、日本の市場あるいは世界の市場の中で取り組んできた中でいうと、他社は皆さん、ショップをお持ちだったと。それに対して当社はショップを持っていないので、当初からインターネットによる申込みをずっとやってきております。そういった意味で、この本人確認プロセスをいかに効率的にどう行うかというところが、会社としても極めて重要な課題となっており、その課題意識に基づいて、昨年1月5日からマイナンバーカードによる公的個人認証を用

いた本人確認ということも並行して進めてきたところです。その結果について、今の状況については、後ほど数字をもってお示ししたいと思っております。

次のページ、お願いします。これは釈迦に説法になってしまうので割愛しますが、要はマイナンバーカードには、いろいろな活用方法があるということです。健康保険証として使う部分というのが、一番左側の券面情報を見る、いわゆる画像として見ているという使い方だと思いますが、あるいはICチップ内に入っている情報をただ読むというもの。ただ、そこに対して、やはり中にある電子証明書と秘密鍵を使って、これを署名検証するというのに、やはり基本的には一本化していかないとセキュリティー、安全性を保つことは無理だろうと考えております。

次のページ、お願いします。従来、画像アップロードという形で、当社は2010年からずっとこういう形を現在も続けております。一方で、この2番目にありますマイナンバーカードの公的個人認証を使った方法を、昨年1月5日から提供を開始したというところで、そして、今準備しているのがもう1つのデジタルKYCと。デジタル本人確認には2つの方法があり、1つはマイナンバーカードを直接使う方法、もう1つが電子署名法に基づく認定を取得した、いわゆる認定電子証明書を使う方法がございます。デジタル一本化とといったときに、この2つを指していると思いますが、そういった意味で、このめぶくIDというのは、前橋とかほかの地域で使い始めているものですが、今年度は様々な名称で、これが様々な企業とか様々な地域が別の名称のIDとして始まってきますので、こういったことからこのめぶくIDを使った本人確認もしっかりとやっていけるという形を今、準備をしているところでございます。

次のページ、お願いします。これはめぶくIDの御参考です。前橋からスタートしたのですが、今、江別、大村という形でやっていて、今年もさらに広がり、いろいろな企業が別名称で、いわゆる会社名のIDという形で広がりつつあるというものになっております。本来的に言うと、デジタルの本人確認は電子署名法の認定の電子証明書が、いわゆるJ-LISとの連携ができるという形で、もしそれを取ってない場合には、冒頭、日下さんから御説明があったと思いますが、新たに別の認定を取らなきゃいけないですよという形になっております。その2つの方法があるということです。

次のページ、お願いします。先ほどお話しした公的個人認証を使い始めて、昨年1月以降ですけれども、当然、当初、認知がなかったところで、本当に5%ぐらいからスタートしたんですが、直近の1-3月で見ると、ほぼ4割近く、最近の月でいうと、4割を超

えるところに、着実に普及してきていると。これマイナンバーカード自体の普及が広がっていることによって、これが広がっているというところだと思います。

次のページ、お願いします。この辺は参考として、こんな形で、今、御提供していますということなので、御参考までです。

5ページ、6ページ、7ページ、8ページ、ちょっと飛ばしていただいて9ページをお願いします。この部分については、赤枠内構成員限りという形にさせていただいておりますけれども、いわゆる本人確認をしたところから、私どもで分かるのは警察から照会があった件数です。これは照会されたものの、それが実際犯罪になっていたのかどうかというのは、これは我々分かる立場でもないし、分かる必要がある話でもないところでございますが、参考数値として、照会件数というものを取って分析したのになっております。先ほどお話ししたように、直近でいうと4割ぐらいがこの左側の公的個人認証、右側の画像アップロードが6割ぐらいというところに来ているんですが、この1年を通して見ると、まだ徐々にスタートしてきたということで、サンプル数としては統計上、十分な数字を持っていると思いますが、ここから分かる部分でいうと、警察からの照会がそれぞれこのような数字になっていると。もう1つ、そもそも発行して照会する前に、当社として審査したときに、この画像はどう考えても偽造でしょうみたいなことってやっぱりあるんですよね。そういったものとして拒否したものが実はかなり多いです。その2つの部分が、申込みの中からはじかないといけないという数字になっております。この辺のところを公的個人認証の場合と画像アップロードの場合で見たときに、どういう比率になるかという形になると、この上に書いてありますが、約16倍と、正確には15.9倍という形になっておりますけれども、16倍、警察からの問合せが、画像アップロードが大きいと。つまり、公的個人認証でやっている場合というのは、このデジタル的な本人確認をやっている場合というのは極めて低いですよという、これは想定どおりでございますが、そういった形になっているというところですよ。

この辺に基づいて、次のページ、デジタルKYCに一本化すべきでしょうと。いわゆる電子署名による署名検証に一本化すべきと。これは特にめぶくIDとスマートフォンに載っている場合でいうと、対面でも簡単に使えるようになっておりますので、別にカードリーダーを店舗に設置する必要もないという形でできますので、その辺を考えると、効率的かつ低コストで、社会的なコストも低いという形になると思います。それによってマイナンバーカードに格納されている電子証明書を使うという1つの方法、もう1つは電子署名法の

認定証明書を使うと、この2つがいわゆるデジタル的なKYCとして位置づけられておりますので、この部分に一本化をして、今の規定はインターネットでの申込みというところになっておるかと思いますが、この辺を対面も含めて、一気に進めていく必要があるのではないかと考えております。

11ページのところは、要望として、これは現在の携帯電話不正利用防止法に関する部分ですが、自然人に関しては電子署名でできるという形なんですが、法人の担当者に関しては、電子署名の規定がないというところになっておりまして、実は私どもも法人のところに対して、極力デジタル化という形を進めているんですが、この法人担当者の部分は、実はデジタル的な方法が定められていないというところがありますので、この辺は見直しの際に、ぜひとも落とさずをお願いしたいと考えております。

最後のページ、12ページ目になります。まず私ども、これはいわゆるネットワークに入る方々一人一人がしっかりと身分確認をされていて、その上で当人認証制、先ほど日下さんもAAL2という言い方をされておりましたけれども、めぶくIDでAAL3という最高レベルにしておりますが、そういったところも含めて、当人認証もしっかりとしたものを使うというふうに、これは携帯電話関係事業者全てがそこに持っていかないと駄目だろうという部分もあります。そういった形を取って、携帯電話が犯罪に利用されることを阻止するというのを徹底してやっていかないと、今も非難する人たちがすごく多いというところですね。それによって、この部分を強化するというところについては、課題はあるものの、それ以外の方法を残した時点で、やはり犯罪はそちら側に逃げていくという形になるので、そこは一律、一本化するということが極めて重要だろうというふうに思います。デジタル的に電子証明書をしっかりと電子署名する、マイナンバーカードを使う、電子署名法認定電子証明書を使うということで、それをやるべきというのがあります。

それから2点目としては、これは私どもも昨年の1月からスタートして、また当社はeSIMでのサービス提供もしております。そうすると、マイナンバーカードとスマホがある方であると、オンラインで10分ぐらいあれば、MNPをして、本人確認が瞬間的に終わって、かつ、eSIMでサービスインという形で、10分ぐらいあると、他社から当社に乗り換えて、もう使い始めることができるという形で、極めて利便性が非常に高い形になっているというところがあります。そういった意味では、利用者視点でいえば、もちろん不正に使おうとしている方を阻止しながら、ちゃんと正しく使おうとしている圧倒的多くの利用者からすれば、利便性が向上するというものがあります。

もう1つ、これは事業者としては極めて重要なことなのですが、これをやる際に、私もでいうとデジタル的な方式であるとほとんどコストがかかっておりません。もちろん手数料とか、若干はかかっているのですが、極めて小さなコストで実現をしているというところがあります。これは当社でいえば、先ほどデジタルの画像アップロードに関して言えば、それが本物かどうか、様々なノウハウをためて、そこについて、これは偽物の可能性があるんじゃないとか、この辺を警察ともお問合せをしながら、そういった形の対応をずっとしてきております。ここについては人手をかなり介しているということによって、時間的なあるいは労力的なコストというのが非常に大きくなっていると。これをデジタル化して100%確実だという形を取りながら、事業者としては大幅なコスト削減が可能になるということになりますので、この3点の面を考えると、やはりデジタルKYCに一本化していくことが極めて重要だと思います。

以上です。ありがとうございます。

【大谷主査】 福田社長様、どうもありがとうございました。興味深いデータを構成員限りということでも開示していただきました。

それでは、今、御三方から御説明をいただきましたので、質疑応答に移ります。

それでは、辻構成員、お願いいたします。

【辻構成員】 発言をさせていただきます。DIPC及び情報セキュリティ大学院の辻と申します。

今回、JPKIという形でお話が出ていましたけれども、当初よりこちらのワーキングに参加させていただいて、JPKIの活用については何度か触れさせていただきました。それについて、今日、具体的なお話をいただきまして、どうもありがとうございます。その中で、誤解を招かないように、いきなりJPKIと言われても、それが何のことか、分かりづらい方もいらっしゃるかもしれませんが、特に一般の消費者に向かってお話しするとき、JPKIって何ぞやということはちゃんとお話しておく必要があると思います。よく言われるマイナンバーカードの認証は非常に曖昧です。マイナンバーカードはいくつかの機能を持っていて、その中の1つがJPKIになります。特に、マイナンバーカードということもあり、表面に記載されているマイナンバーがどうにかなるのではないかとと思われるかもしれませんが、JPKIがマイナンバーそのものを使って何かをするというわけではありません。もちろん中の情報の一部ではありますが、そういった誤解を招かないためにも、このJPKIの議論をするときには、消費者、利用者に対し、JPKIが何ぞやということを丁寧に説明する必

要があると思っているのが1つ目です。そこは注意が必要と思います。

その上で、マイナンバーカードの普及率がもう8割ぐらいになりましたが、そうすると、次に、普及したマイナンバーカードは何に使うかという議論になります。やはりこの活用はすごく重要であり、活用の方法については、デジタル庁ができる前、総務省の時代からいろいろな仕組みがつくられてきました。そういった中で、今回、本人確認にこれを活用するというのは王道中の王道で、これを携帯法に適用するのはある意味必須なのかと思います。JPKIという言葉のうちPKIとは公開鍵暗号基盤というもので、この基盤を軸につくった仕組みがJPKIということです。これは、単純にICカードの情報を読み取るといったシンプルなものではなく、複雑かつ安全な仕組みにより担保されているものです。ですので、JPKIを使うということとICチップの情報を読み取って何かするという単純な話についても、混同しないようにすべきかと思います。

そういう意味でいうと、最初に日下様よりお話がありました、JPKIを軸にするということとは、本当に、私もそれが一番いいと思いました。なぜかという、先ほどイオンさんから話もありましたし、日本通信さんからも話がありましたけれども、やはり信頼性という点でしっかりとした基盤であるということを活用する。一方で、そこから外れてしまう人をどう救うのかという点について考えるべきというのはそのとおりであり、そこで、犯収法の依拠を活用するという事なんですが、前回もお話しさせていただいて、今日、日下様も御指摘があった認証レベルをしっかりと合わせるということに対して、依拠をJPKIベースにされるという日下様の御提案は非常によい御提案ではないのかと思います。一方で、そういった場合に、やはり、犯収法との整合性という論点がありますので、その犯収法との整合をどう取るのか。携帯法だけでこの犯収法とうまく整合させるのか、場合によっては、警察庁とうまく連携を取る必要があるのかといったことも考慮をする必要があると思います。これが3点目です。

あとイオンリテールさんの発表の中で、JPKIの活用について、現場のいろいろなお話がありましたけれども、やはり、ちゃんと利用者がJPKIを使えるようにすることが非常に重要で、そこをどうしていくのかについては、いろいろ御発言があり、本ワーキンググループのテーマから外れている御提案もあったかと思いますが、そこについてはデジタル庁の管轄のものであったり、総務省さんの管轄のものであるかと思いますが、ぜひ総務省さんからデジタル庁さんに働きかけを行ってもらいたいです。実は昨今、報道でありましたとおり、デジタル庁の各種サービスの進め方というのはいろいろ非公開な面があり、

マイナンバー機能の活用、JPKIの活用について、こういったワーキンググループや総務省さんから、こういった形で使いたい、だからこうしてほしいということをお願いいただくと助かりますと思ったところです。

ということで、4点ほど触れましたけれども、そういったところをぜひこちらのワーキンググループを通じて形にできればと思っております。

【大谷主査】 貴重なコメントをありがとうございました。マイナンバーとマイナンバーカードが区別できていないとか、いろいろ問題があるところですし、JPKIについても正しく理解できているのかというような基本的な問題がありますので、そこを十分に説明していきましようという貴重な提案だったと思います。

それでは、仲上構成員、コメントをお願いします。

【仲上構成員】 日本スマートフォンセキュリティ協会の仲上でございます。

お三方からの発表、それから辻先生のコメントも大変勉強させていただいております。直近でも、個人認証の悪用というところで、SIMスワップによる金融被害等も報道されておりますので、個人確認の強化という観点で、電子証明書それから電子署名、そういったJPKIの利用の推進が求められている状況ということについては、非常に全くそのとおりであると思います。

日下様の発表でお伺いしたいところがあるのですが、マイナンバーカード偽造対策として、P16の中で参考情報としてお示しいただいておりましたユーザーのスマホ端末上のアプリでマイナンバーカードの中の証明書を確認できるという機能を活用してのカードの真正性、真贋判定というところについて、非常に利便性が高いという印象を受けましたけれども、これは使い方によってはアプリケーションの画面そのものを偽造されて、あたかもこのソフトウェアを動かしているかのような見せ方をして、この4情報を一致するというところの目視確認に臨むようなサイバー攻撃者が出てきてもおかしくないと思いますので、このような形で進められるときは、例えば確認者側、携帯電話事業者様の窓口の方がスマートフォンを使って確認することが可能なのか、それは議論が必要かと思っておりますけれども、アプリケーションそのものの偽造対策についても留意する必要があると思った次第でございます。こういったところについて、検討されていることがあれば、ぜひお聞かせいただきたいと思えました。

【大谷主査】 ありがとうございます。

それでは、日下理事から御回答をお願いしてよろしいでしょうか。

【デジタルアイデンティティ推進コンソーシアム（日下氏）】 御質問いただきまして、ありがとうございます。日下です。

ユーザー端末のアプリケーションの画面が偽造されるのではないかという点については、ユーザー端末を使うという話で、必ずいろいろなところで出てくる話かと思います。例えばPaypayさんのQR決済でも、一時、ペイペイと音だけ出して、画面をキャプチャーで見せて、決済をしたふりをするみたいな問題があったと聞いていますけれども、この点については、技術的には解決の方法はいくつもあると思っています。Howの部分ではいろいろあるので、あとはコストであったりとか、運用オペレーションの観点でどういったことが一番普及していくかということは、まだまだ検討の余地があると思います。例えばワクチン接種証明書するときにも、ユーザーの端末に証明書を登載し、ユーザー端末上に掲示されたものを検証するという仕組みは、実はQRを事業者側が読み取ることで検証できます。国際的にはVerifiable Credentialsという仕組みを使っていましたけれども、このような仕組みがあるんですね。しかも、日本では実はもうデジタル庁の下にこれを実施済みであるという観点でいうと、対面におけるスマホ上の証明書を検証する仕組みというのは、国際的にももう規格がまとまってきていますし、実際、日本ではマイナンバーカードと紐付けて、ワクチン接種証明書を発行していますので、そういった観点ではユースケースが既に存在しています。先ほどお示ししたJPKIモバイルですとかそういったものについては、確かに、iOSのストアというか、Appleの場合は、サイドローディング的に端末にほかのネイティブアプリを入れることは難しいんですけども、例えばですが、究極を言えばAndroid端末の場合は、偽造JPKIモバイルアプリをつくり、偽物のマイナンバーカードを読み取ったふりをして、JPKIモバイルと同じような振る舞いで4情報の結果を表示するみたいなことは、スクリーンショットのような簡易的な方法ではなく、より高度にできると思いますけれども、この辺りは、その不正する側のかけるコストとそのコストによって得られる便益とのトレードオフになってきますので、今みたいなことをしようとするとそれなりにコストがかかることになります。あとはいちごっこにはなると思いますが、技術的にはいくつかの方法として、既に対面本人確認によって券面が真正であるかを検証する方法はあると考えております。

【仲上構成員】 ありがとうございます。参考になります。

【大谷主査】 御回答ありがとうございました。沢田構成員、お願いいたします。

【沢田構成員】 どうもありがとうございます。

今日、お話しいただいた事業者さんは、いずれも対面を含めて本人確認の厳格化を非常に希望されていることがよく分かって、印象的でした。それぞれの事業者様が抱える課題も、ある程度、理解できたところでございます。

その上で、3点、コメントさせていただきたいです。事業者さん側の課題として、やはりコストがあるようだということは分かりました。開発コストとか、導入費用とか、オペレーション費用とか。実はかえってコストを下げるのだという話も日本通信様からいただき、コストを下げるためのアプリのお話も御紹介いただいたところではありますが、やはり何らかの支援が、この先、携帯事業者以外にも広げていくとなれば、必要だということもおっしゃるとおりだと思います。それは、まさに辻様がおっしゃったように、デジタル庁で公的個人認証を普及させるための施策をいろいろ打っていると思いますので、そういう支援事業みたいなこともデジタル庁でやっていけば、ぜひ一緒に考えていただければいいのではないかとということが1点です。

2点目も、辻様がおっしゃったことと同意見なのですが、利用者側に関する視点です。JPKIとは何かとか、マイナンバーとマイナンバーカードの区別がついていない、機能が違うことを分かっていないというのは、座長もおっしゃっていましたが、まさに日々感じているところです。私の周りの消費者団体なども、そこはいまだに混乱していますし、誤解もしています。マイナンバーカードを保険証に使うことに関しても、相当まだ抵抗感が強く、かなりの誤解、思い込みもあると感じており、そこへの啓発が必要と思います。イオンリテール様の御発表にありましたように、課題を正しく整理するというのは、利用者に対しても、とても必要なことだと思いました。単純な利便性で、便利になると謳って普及させようとする、全然便利ではない、今までのほうが便利だと反発を受けてしまいます。そうではなく、デジタル化することの意義や重要性をきちんと説明する、保険証に関しては医療レベルを上げるという意味でのデータ利用の必要性とか、今回はその話とは少し違い、安全性を高めるという意味で必要だということを利用者にもちゃんと伝えること、ポイントを配るのではない形で普及を図っていくことが必要だと思います。日下様の御説明の中にありました、IALやAAL等という、本人確認との意味はこの2つから成っていると、そういう基本的なところがもう少し共通言語になる必要があると思いました。

ついでに申し上げますと、どうしてもついていけない高齢者などの利用者がいた場合に、ついていけない人がいるからそれはやらないということではなく、また、別の方法を準備して二本立てでやるということではなくて、できるようにサポートする方向で考えること

が必要だと思います。例えば学生さんに手伝ってもらおうといった形でのサポートが必要ではないかと思いました。

3点目に、ほかのネットサービスでも、本人確認の確実性を上げることは重要と思います。例えばeコマースやSNSのアカウント登録の際の本人確認にも、できれば公的個人認証が低コストで使えるような形で普及していけばよいなと思います。

以上、3点です。ありがとうございます。

【大谷主査】 ありがとうございます。幅広い観点からコメントいただきまして、ありがとうございました。

私が聞きたかったことを教えていただいてもよろしいでしょうか。

日本通信の福田社長に教えていただきたいのですけれども、イオンモバイル様のほうで利用者側のリテラシーとか利用者側のハードウェアとかのところで問題があるので、その環境をどういうふうにつくるのかといったところで問題提起をいただいていたと思うんですが、日本通信様の場合は、利用者様のほうに環境がなかった場合には、やはり従来の方法で対応されているというようなことなんでしょうか。

【日本通信株式会社（福田氏）】 御質問ありがとうございます。お答えさせていただきます。

まず、ここに提示していますのは、今現在、昨年1月からiPhone及びAndroid用に作成しているものになります。これについては、スマートフォンをある程度使っている方からすれば、何の問題もなく手続できています。それ以外の方に関しては、従来型の画像アップロードであるとか、電話対応の後、それを郵送していただくような方法とか、お客様によって様々な方法を取っているというところでございます。

あとはリテラシーのお話でございますが、これは、群馬県の前橋市、人口33万人弱の町でございますが、そのまちづくりに関わって、このめぶくIDをベースにしためぶくpayというサービスを、昨年12月20日からスタートしております。これは、いわゆるQRコード決済としては、全国200いくつあるうちの、最後発の一つです。ただし、唯一ここでしかできてないことがあって、それは前橋市役所のデータベースとデータ連携を取ることで、子育て給付金等を自動的な手続で給付がされるというものです。従来だと申し込んでから2か月ぐらい経ってからやっと銀行口座に入っていたものを、ほぼ1日の中で完了するというような形を取り始めています。これは今、全国で非常に注目いただいている、そういったものをこの部分で、めぶくpayという形、このIDを使ってやっていると。この本人

確認が犯罪収益移転防止法にも対応できているからできていることでもありますし、今、デジタルIDという形でいうと、このデータ連携をしっかりと行政等も含めてできる基盤がこれ1つしかないということもあって、それが特徴になっているというものです。

そのめぶくpayの経験で申しますと、実は80代、90代の方も普通に、結構使われている方がとても多いです。何をしたかという、一つは前橋市役所の最上階のフロアに、五、六人の体制で、ずっと今もいるんですが、そこに来ていただければ手続をちゃんと指導しますよ、ということに取組んでいます。それをしたところ、もちろん全員というわけにはいかないですが、来ていただいた方は確実に使えるようになっていきます。なので、我々もついつい考えてしまいますけれども、お年寄りだと難しいと思っているのですが、そんなこともなくて、実は簡単にできるようになっていることが前提なんです、使い勝手のいいものを丁寧に教えればしっかりとできるということがあります。それを、決済を受ける側のところも、何のシステムもなく、いわゆるおじいちゃん、おばあちゃんが経営している飲食店のようなところでも、お店のQRコードは用意していただきますが、ここで支払うものについては、その金額を確認さえしていただければ決済できるその形で来ていると。したがって、その取組に関しては、もちろん、これは特に行政というか、地方自治体の方と一緒にやっていたら当然のことながら、老若男女全ての方が使えないと困るという前提で動いているため、実はそういったところのサポートをしっかりと提供し続けていると、それほど大きな問題ではないというのが今、この前橋による取組の一つの結果だと思っています。

あとはそこに対して、先ほど、例えばアプリケーションのサイドローディングによる偽のアプリケーションというような御指摘がありましたけれども、これはいわゆるマイナンバーカードを読み取る部分のアプリを偽造するというお話だと思いますが、このめぶくIDの部分でいうと、そもそもその電子証明書がいわゆるスマートフォン、iPhone、Androidの中のHSM（ハードウェアセキュリティモジュール）という、いわゆるハードウェアで守られているところに埋め込んでいますので、そもそもサイドローディングをしても、偽のフェイクのアプリはそれにアクセスしようがない、iOS及びAndroidのOSとしてきちっとプロテクトされているので、その心配は全くないのです。ですから、そもそも心配がありますよということを知るとすごく大変なことで、心配が要らない仕組み、絶対に安全な仕組みをしっかりと御提供するということが、やはりその辺の不安感を取り除き、また、サポートもすごく楽にするという形で、前橋でどこまでいけるかということ徹底し

て取組んでいるので、御参考までに御説明をすることで御回答とさせていただきます。

【大谷主査】 ありがとうございます。ちょうど沢田構成員からいただいた問題点の御指摘についてのよい回答をいただいたと思っております。

鎮目構成員、よろしく願いいたします。

【鎮目構成員】 本日は大変貴重な勉強になる御報告を3名の方からいただきまして、どうもありがとうございました。

日下様から御報告いただいた中で、前回も少し今議論があった依拠による本人確認の見直しというか、JPKIを前提として、依拠による本人確認をするということについて、ある程度、積極的な評価をいただいたかと思えますけれども、日下様が御指摘された本人認証が極めて重要であって、本人認証がしっかりしていない、脆弱である場合には、依拠による本人確認の結果が悪用されるおそれがあるという御指摘ですが、それは技術的なことなのでということさらっと流されたかなとは思うのですけれども、本人認証について、現在の様々な技術的な水準などを踏まえたときに、できる限り悪用を防ぐといった観点からすると、本人認証レベルについて、日下様の資料でいうと14ページのところに参考としていろいろ挙がっているかと思いますが、どのくらいものを要求することが妥当と考えられるか、その点について教えていただきたいということでございます。これを導入する場合は、やはりその辺りをかなり真剣に考えていかないと、依拠の仕組みを通じて、銀行やクレジットカードあるいは他の携帯電話事業者による本人確認結果が悪用されるというたちごっこになりかねないなと思ひまして、質問させていただきました。よろしく願いします。

【大谷主査】 それでは、日下理事からお願いできますか。

【デジタルアイデンティティ推進コンソーシアム（日下氏）】 承知しました。御質問ありがとうございます。

この11ページのほうの右下に示しているとおり、やはり本人認証のレベルが、これは間違いなく、レベル1でいいことはないだろうと。これがレベル2、レベル3なのかということは、14ページでお示ししているところに違いがあるわけですが、やはり、昨今、例えばSNSのアカウントや、いろいろなメッセージングアプリのアカウントなどが、第三者に奪われてしまうという事件が、私の周りも含めて、後を絶たないところかと思ひます。本当に身近な人でもそういった被害にさらされているという状況がある中で、本人認証のレベルという観点からいうと、マイナンバーカードについてはレベル3に位置づけられて

います。耐タンパー性のあるハードウェアの中に鍵が保管されているという仕組みですが、実際にこの耐タンパー性のあるハードウェアということを実現しようと思うと、一般的に皆さんが使っている何々IDでログインするみたいなものというのは、ほぼ全部使えないということになってしまいます。では、どこまでが実現できるのかというと、最近、WebAuthnですとかPasskey含めて多要素認証で対応する事業者のサービスが多くなってきていますけれども、最低でもやはりレベル2以上の本人認証レベルを担保する必要があるんじゃないかなと思います。

あともう1点、一般的に、例えばですけれども、前回、楽天モバイル様がたまたま出られていたので楽天モバイル様の場合楽天IDがあったりですとか、ほかの通信事業者でも何々IDとかを持たれていたりすると思いますけれども、自社のIDが現状、例えば、1人の同一人物が複数のアカウントを持たれている、あるいは複数のアカウントを持てることを許容している場合に、どのIDに対してマイナンバーカードを紐付けるのか。これが、複数のIDを作れて、かつ複数のIDにマイナンバーカードを全部ぶら下げられるとすると、言葉を選ばず言うと、片方のIDを誰かに売るといったことが口座の売却よりも容易にできてしまうので、こういった観点についてもしっかりと検討する必要があると思っております。

以上になります。

【大谷主査】 御回答ありがとうございました。鎮目構成員、よろしいでしょうか。

【鎮目構成員】 ありがとうございます。最後の御指摘も、はっとさせられたというか、大変勉強になりました。

【大谷主査】 それでは、日本通信の福田様、よろしく申し上げます。

【日本通信株式会社（福田氏）】 やはり本人認証レベルが低いということが最大の問題で、身元確認をすることと本人認証をするという2つのことがまぜこぜに論じられています。これらを英語で言うと、identityという話とidentifierという別の話になりますが、それがIDという形で一緒になってしまうことが、一つの不幸の始まりと感じております。

その中で、先ほどいわゆる本人認証レベルでいうと、先ほどめぶくIDというのを紹介しましたが、これは本人認証レベルが3になっております。本人認証レベル3という形にしているために、いわゆる行政のデータベースと直接つなぐことができると。これは、金融庁とともに7、8年前に開発した技術が基になっていまして、インターネットバンキングについては、このレベル3に持っていけないと駄目だろうという議論は昔からあって、これはもう間違いなくそうなってくると思います。現在も、インターネットバンキングにお

いて不正利用が多いというところありますので、そういったお金にまつわる話。それから医療データそのものに関して言うと、やはり極めてセンシティブな情報であるために、これはレベル3じゃないと駄目でしょうという形になっていて、今現在も、いわゆる電子カルテ上の医療データと直接つなぐ取組というのは、このめぶくIDベースで、レベル3のものを使う形で、きちっとプロテクトしながら行うという取組がいろいろなところで進んでおります。

この辺のところはセキュリティー対策なので、あとはバランスの問題になってきて、例えばチャットのようなものというところがどこまで守らないといけないかみたいなのところになってくると思います。ですから、その辺については最低でもレベル2、できればレベル3と、この辺のところは事業者さんとかあるいは分野によって、皆さん非常にお考えなので、どうするかというようになっているんだと思います。ただ、いずれにしても、この身元確認というところをしっかりとやったらオーケーというような感じが何となく思われている部分があって、マイナンバーカードは本人確認をやるための道具なので、それはそれでいいんですけども、本人認証レベルをしっかりと規定して、そのレベルに合わせると。私が知る限り、携帯電話不正利用防止法の金融庁のほうで、その取組については先に取組を進めていらっしゃるので、そこも総務省様のほうで連携をしながら、その辺をきっちりと整理をしていくということが必要だと考えます。

【大谷主査】 ありがとうございます。本人認証レベルについては、重要なポイントを御指摘いただきまして、しかも行政レベルと直接つなぐ際の条件になっているということなんですが、それを制度でどこまで義務づけをしたり、例えば事業者の絞り込みにつなげていくかというのは、なかなか難しいところなのかなとは思っております。

【デジタルアイデンティティ推進コンソーシアム（日下氏）】 今の点、1点よろしいですか、補足で。

【大谷主査】 どうぞ、お願いします。

【デジタルアイデンティティ推進コンソーシアム（日下氏）】 先ほどの行政のといいますと、実は総務省令において、いわゆる地方自治体、行政がある手続を行います。例えば住民票の申請手続を行いますみたいなときに、省令が決まっています、その省令でいうと、マイナンバーカードの電子証明書による署名検証を行う、または電子署名法の認定の証明書を行うという、ここに一本化されているんです。この2つというところに限定をされている。例えば前橋とかほかでやっている部分は、電子署名法の認定証明書を使っているの

で行政手続に使っていいですね、したがって、子育て系の様々な給付金等の処理をそのままできるという形になっています。そういった意味ではこの総務省令が非常に実はすごく重要な重いものであって、この辺のところはやはり本人確認という部分だけではなくて、当人認証も含めた形で、この総務省令のようなものが、これはデジタル庁なのかもしれないですけども、分野横断的にそういったことをされるということが極めて重要で、特に地方自治体については総務省令があるのでそれじゃないと駄目という規定になっているところなんです。

【大谷主査】 ありがとうございます。

それでは、辻構成員、お願いいたします。

【辻構成員】 今の本人確認をどう進めていくかというところで、やはり本日でいくと、レベルの問題だったり出てきておりますけれども、最初、私、JPKIを丁寧に説明していくべきではないか、マイナンバーの違いということをお話しさせていただいたんですが、あとやっぱりこの本人レベルをしっかりと共有してというところも含めてかなと感じました。もともとこういう認証レベルというのは日下様もお話しされていたところでもありますけれども、米国の国立標準技術研究所、いわゆるNISTと言われるところがSP800という認証文書を作っており、これがコンピューターセキュリティーに関わる部分。これは米国ではあるんですけども、結局、米国で採用されるために必要なので世界的にこれを参照することになっていて、その中のデジタル認証に関わるところがチャプター63なんですね。SP800-63と我々は呼ぶんですけども、ここに認証レベルの規定、AAL、IALといったところが仮定されておまして、こういったレベルがあって、そのレベルのどこに該当しているというところを知るだけでなく、そういうものですよというところをやはり利用者であったり使う側にも伝えていく必要があるのかなと。やっぱりJPKIでの認証が難しいのは確かですし、手続も厄介だというのはそのとおりなんですけど、ちゃんと説明していくことが必要なかなと感じました。そういった中で、依拠の話にせよ、ICカードチップ読み取りにせよ、このセキュリティーレベル、認証レベルがどうなっているかを丁寧に説明することが必要なかなと感じました。あと、それをちゃんと皆さんで認識共有しながらお話しすることは必要だろうと思っております。

すみません。あともう1つです。今ちょうど日下様から認証をJPKIベースでとか、要は本人認証をどのように安全にしていくかというところから出てきたんですが、もう1つ私、ちょっと最初にお話しし忘れたんですけども、セキュリティーばかりに目を向けると、

もう1つ忘れてしまうこととしてプライバシーの問題。セキュリティーを守ろうとして、例えば、Aがある情報をもらってBに依拠するというを行うんですけれども、認証をお互い行うときに、こういう情報をやり取りしたりとか、認証のためにこういう情報をやり取りしたり、こういうという言い方をしちゃったんですが、認証のアクションを取るときに、やっぱり何らかの情報のやり取りが発生することになりまして、その情報のやり取りで何をやり取りして、そのやり取りの結果、それが蓄積されるとどうなるのか。結局、名寄せということが可能になって、いろいろサービス、銀行、例えば証券もそうですし、あと普通の民間なんかのサービス、いろいろなサービスを利用して、それで名寄せすることで、ある個人のプロファイルが確定できてしまう、もしくはその人の分析データが可能になるということは、ある意味、プライバシーの侵害につながると懸念されておりまして、ちょうど私、先ほど言いました各メディアさんがちょっとデジタル庁の認証アプリというものに対して懸念を表明される記事を最近書かれていた。それがまさにそれで、デジタル庁が集約的にそういった認証を行ってしまうと、デジタル庁に個人情報が集まってしまうんじゃないかということがちょっと今、問題点です。そういう意味でいうと、デジタルにおけるセキュリティーもすごく重要なんですけれども、同様にやっぱりプライバシーもちゃんと担保されるようなところを言っていないと消費者に受け入れられないということは、最近、私、強く思っていますので、それを忘れないようにしなきゃいけないなということを最初に言い忘れました。

もう1点なんですけれども、大谷様、総務省の小澤様にお聞きたかったのは、かなり今日、重要な論点が出てきて、こういった論点を今後どのように進められるのかなということも少し気になりましたというところを御質問（音声途切れ）。

【大谷主査】 ありがとうございます。辻構成員から、また重要なポイントで、認証レベルのお話と、プライバシーですね。私、名寄せはできない仕組みになっていたと思うんですけれども、ちょっとそこが技術的に分からないので、誰か御説明いただけるとありがたいんですが。あるいは既にメディアなどで取り上げられているということでしたら、後でその関係の記事か何かを教えていただければと思います。

【辻構成員】 すみません。記事については別途、共有するようにいたします。

【大谷主査】 ありがとうございます。名寄せができないような制度として、私も作り込みに参加したつもりでいたので、セキュリティーの強化ということで擦り抜けられている実態があるんだとすると、非常にそれは心配です。お手を挙げていただいているのは

事務局ですね。では小澤さん、よろしくお願いします。

【小澤利用環境課課長補佐】 事務局でございます。

皆様、御意見、御質問、ありがとうございます。ちょっと今、何点か気になったのは、まず、さっき本人認証レベルが行政手続のほうで、総務省令でというお話がありましたが、これは多分、住民基本台帳の話がされているんだらうと。すみません、私も昔取ったきねづかで、自治体にいた頃の記憶で、また別途、確認をいたしますが、なので行政手続一般について総務省令でというところで、しかも本人認証まで総務省令で明文で書かれているかどうかについて、私の認識ではなかったもので、そこは別途確認はいたします。事実上、マイナンバーカードによる認証なりを、例えば住民票をオンラインで申し込むときに求められているという意味では、本人認証レベル3まで満たしているとか、そういったようなことは御指摘のとおりかなと思いましたが、その事実関係だけは別途、確認をしたいと思っております。

先ほど、辻先生からプライバシーの部分でも留意がというので、我々もデジタル庁さんのほうでどのようなアプリケーションをつくっているかというのは認識はしてないんですけども、JPKI一般でいえば、大谷先生がおっしゃるように、JPKIのほうで名寄せするとかいうようなことはないはずでありまして、そこら辺、あとは各SP事業者、PF事業者側のデータをうまくプライバシーの観点で取り扱っていくと。法令に基づいてというところだと思いますので、それぞれのところで作られている個別のアプリケーションが今どうなっているかというのはちょっと今、網羅的に把握しているわけじゃないので、今、お答えはできないんですけども、多分JPKIそのものは名寄せできないようになっているという意味では、大谷先生がおっしゃるとおりだと思っております。

【辻構成員】 そこはちょっと誤解を招く発言をして申し訳ありませんでした。JPKIそのものが、今の仕組みが安全じゃないという、プライバシーに懸念があるということなので、これを使ったいろいろなサービスなり何かをしようとするときにそうならないように注意すべきですねという意味でのコメントでした。

【小澤利用環境課課長補佐】 事務局からは以上です。

【大谷主査】 貴重な御指摘の数々をいただいております、ありがとうございます。議論をまとめる段階ではないんですけども、いろいろ御提言いただいたところでは、やはりeKYCでいろいろ不具合が出ているところは、dKYC、デジタルKYCに統合していくことが必要だということについての共通認識が得られたところであり、またそれに対する事業

者側のコストや利用者側の便宜ということを考えたときに、犯収法であると。それから、犯収法で先に実現していることを、やはりこの現場における本人確認のところでも制度の整合性を取っていくことが利便性につながっていくのではないかという点ですね。あとは、福田社長のお話では法人担当者のところについても御提言をいただいております、そういう制度間の整合性であるとか、より安全性を高めるための取組について、おおむね共感が得られたというところだと思います。また、利用者サイドでも、新しいdKYCについていきづらいついた方に伝えるべきリテラシーに関わる事項であるとか、サポートといったことについても御提言をいただいていたと思います。その際の注意事項で、本人認証のレベルをちゃんと確保することであるとか、プライバシーにも十分気をつけること、それから言葉の使い方の正しさというようなどころも重要だったかと思います。

最近では、マイナンバーカードで、もう、なりすましが生じているといった、ちょっとセンセーショナルな見出しなどで報じられており、マイナンバーカードが駄目なのかといった誤解を呼んでしまうようなところもあり、私は非常に懸念しているところなんですけれども、そうではないんだというか、もう何をどうすればいいのかといったところの情報を共有できるようにしていくことも必要だということは、今日も御提言をいただいております。

コストについては、やはりできるだけ低廉なものにということが必要だと思っておりますが、これについては日下理事のほうからも具体的なコストについての感じを説明していただきましたが、かなりかかるものだなと思っております、これは利用者が増えればだんだん減っていくものだとは思いますが、ほかの方法とかなないのかなというのはちょっと気になっているんですけれども。

どなたからもなければ、日下理事に私からその点、質問してもよろしいでしょうか。コストダウンについていろいろお知恵をいただいたんですけれども、そもそもその従量制の課金というのは今、たまたま無料になっていますけれども、末永く無料というわけにはいかないのではよ。分かる範囲でお願いします。

【デジタルアイデンティティ推進コンソーシアム（日下氏）】 はい、もちろん。もともとは約3年前にデジタル庁のほうから、3年間の無料期間ということで、J-LISに対してプラットフォーム事業者という民間事業者が払うコスト、署名用電子証明書が20円の、利用者が2円と費用を払わなくていいという3年間措置が施されたんですけれども、これが延長に今なっています、まだ無料の期間が続いているという状況です。ただ、これは

あくまでもプラットフォーム事業者とかそういったマイナンバーカード、公的個人認証の法における提供する事業者のある意味、仕入れコストが下がったという話なので、基本的には価格競争になっていけば上代に、つまり利用される金融機関さんですとか携帯事業者様のかかる費用にも転嫁されていく、つまり安くなっていくはずなんですけれども、今の御指摘のとおりで、やっぱりまだまだこれまでの過去3年というのはマイナンバーカードが普及していない状態で値づけ、価格設定を各事業者がされていまして、ここからマイナンバーカードが普及しているという前提で価格設計をしていくと、すごい細かな話ですけれども、各社さんの今後の3年間でひく事業計画の中では、より大きな見込み、件数に対して、じゃあ1件当たりのコストはもっと下げるんじゃないかという試算は今後、起きてくるのではないかなと思っております。

そういった中で、今までは署名用電子証明書の利用だけだったんですけれども、今回の対面の本人確認とかを考えると、利用者用の電子証明書の利用も含めて、民間事業者さんでも積極的に活用していこうという動きも出てきているかなというふうに思いますので、ここは民間企業の企業努力とマイナンバーカードを普及してきたというところの背景から、もっともっと下げていけるんじゃないかなと思っています。

もう1点が先ほども話したとおり、依拠のところを含めて、じゃあ毎回毎回JPKIする必要があるのか、公的個人認証するのかと。一度、公的個人認証していれば、それ以降はもっとさらに乗り合い効果が高まるような廉価な仕組みというものをつくるといったことも検討を進める事業者さんもいらっしゃると思いますので、コストの部分というのはもっと利用者が広がっていけば下がっていくという構造になっていくかなと思います。

以上です。

【大谷主査】 ありがとうございました。

依拠も現実的な仕組みということで、引き続き選択肢の一つとして考えていくというようなことなのではないかなと思いました。

福田社長から挙手いただいておりますが、御発言いただいてよろしいですか。

【日本通信株式会社（福田氏）】 今の事業者のコストの面なんですが、当社のように、両側、いわゆるeKYCもやっているし、デジタルKYCも使ってやっていますという側面からすると、圧倒的にコストで見ると、デジタルKYCのほうがはるかに安いです。なので、事業者にとっては、新たな負担というよりはむしろコスト削減になるので、しかも回収期間も極めて短期間で回収できるものだと思いますので、コストの面というのは、むしろ下

がりますよというふうに捉えていただいたほうが、そこは別にゼロではないんだけど、今までのやり方よりはるかに安く。これはちょっと考えていただければ、人手がかかっていないので当然安くなっているわけで、そこに一定の費用が若干そこにJPKI、公的個人認証の費用が有償化されたとしても、はるかにコストが低いということは、私どもの両側をやっている事業者としての経験値として御報告させていただきたいと思います。

【大谷主査】 日本通信様、ありがとうございます。

コストの関係ではイオンモバイル様のほうからも御提言いただいています、もちろんオペレーションが開始されると、非常にコストダウンにつながる仕組みだというのは、今の福田社長の御説明にもありましたけれども、仕組みを導入して開発するところまでは、かなりハードルが高い事業者さんもあるのではないかなというように、十分な時間の猶予が欲しいという御意見もあったんですが。多大な開発コストというのは、事業者によっても異なるころだと思いますが、期間とかは大体どのくらいが必要なんだろうかな。もし差し支えなければ。

すみません。ちょっと今、山根さんから手が挙がっていたんですが、ちょっと先に井原さんから御回答いただいて、その後、山根さんにおつなぎします。

【イオンリテール株式会社（井原氏）】 イオンリテールの井原です。

私への質問ということで、すみません、当社もまだ今ちょうど要件の整理が終わったところで、今から実は開発を進めさせていただきまして、期間がどれぐらいかかるかというのは、当社は今から検討なんですけれども、説明させていただいたところ、我々はもう既に開発を進めさせていただいておりますが、MVNOは大小、様々ございますので、当然、利益的なところも企業によって大きく異なるかなと思っています。なので、これが初期投資として相当費用がかかるということであれば、事業者自体がそのコストを捻出することができないということも出てくるかなと思いますので、そういった意味で、様々な事業者があるということと、当然、自社でエンジニアがいる会社とそうでない会社ではまたコストも相当変わってくるかなということがございますが、その辺りは様々な事業者の声もぜひヒアリングいただければなと思っています。

【大谷主査】 いえいえ、どうもありがとうございます。

多分、事務局のほうで、事業者の声を拾っていただけることと考えております。

それでは、お待たせしました。山根構成員、お願いいたします。

【山根構成員】 まず今日の話について、DIPCさんの発表、非常に勉強になりました。

本人確認に関する社会的なコストの削減などを踏まえると、やはり他の事業者のほうに確認あるいは自社が過去に行った本人確認に依拠するという方法も、十分に検討に値するのではないかなと思っておりまして、あとは今日、特にお話にもあったとおり、本人認証のレベルをどう確保していくのかというところが、特に課題になってくるのかなと考えております。これはちょっと感想めいたコメントになります。

もう一点、DIPCさんとイオンリテールさんのほうから、対面での本人確認についてもJPKIを使った方法について一本化していくのがいいんじゃないかという御示唆があったかなと思ひまして、デジタル重点計画では、非対面の取決めについて見直しの方向が示されていたかなと思うんですけれども、確かに非対面の方法について、本人の認証のレベルが上がったということになると、対面の方法において不正が増加するのではないかという御指摘は確かにごもっともかなと思ひまして、対面の方法についても、少なくとも中長期的な方向性としては、JPKIを使った方法に原則として一本化していくということが望ましいのではないかなと思った次第でございます。その時期については、非対面の場合と同時期に実現できるのか、そうしていった場合に、現状だとやはりまだまだ対面で運転免許証の提示をして本人確認を行うといった方法もかなり多いかと思ひますので、実際の実務へのインパクトがどれぐらいあるのか、といったところも含めて検討していく必要があるのかなと思ひました次第でございます。

私からの発言は以上になります。

【大谷主査】 ありがとうございます。対面の確認の際にも確かに問題提起いただいたところで、重要な御指摘をありがとうございます。

先ほどユーザーのアプリを使って検証をすることができるというようなことですので、やり方はいくらでもあると思うんですけれども、実際にそれに統一するとかということになりますと、相当の準備期間とかも必要になるんだと思ひますので、そこも含めて本会の取りまとめの中でも触れていけるように、事務局にお願いしていきたいと思ひます。

それでは、ほかに御意見、御質問がある方は挙手いただけますか。一通り御発言いただいたようですね。

それでは、多分、細かなところになりますと議論はなかなか尽きないテーマでもありますが、お時間の関係もございまして、この辺りで討議を一旦終了させていただきたいと思ひます。今日もプレゼンテーションをしてくださった3事業者の皆様、それから構成員の皆様、多岐にわたる論点につきまして、活発な御議論をいただきまして、ありが

とうございました。

それでは、次回の会合についての御案内を事務局からお願いできますか。

【小澤利用環境課課長補佐】 事務局でございます。

皆様からいただいたところは、事務局としても受け止めて、検討してまいります。

次回、会合の予定については、今、調整中でありますので、別途、事務局のほうから御案内をいたしたいと思っております。よろしく申し上げます。

以上です。

【大谷主査】 ありがとうございます。

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4回会合を終了させていただきます。本日は皆様、お忙しい中、ありがとうございました。