不適正利用対策に関するワーキンググループ（第10回）

令和７年６月６日

【田中利用環境課課長補佐】　定刻となりましたので、不適正利用対策に関するワーキンググループ第10回会合を開催いたします。

事務局を務めております、総務省利用環境課課長補佐の田中でございます。

事務局からのウェブ会議による開催上の注意事項については、投影しているとおりでございます。

本日の資料は本体資料として議事次第と資料10－１を用意しております。

では早速ですけれども、議事に入りたいと思います。議事進行は大谷先生にお願いしております。大谷先生、よろしくお願いいたします。

【大谷主査】　それでは、早速議事に入らせていただきたいと思います。進め方といたしましては、まず事務局、それから警察庁から御説明をいただきまして、その後に皆様との意見交換を行わせていただきたいと思います。

それでは、事務局、よろしくお願いいたします。

【田中利用環境課課長補佐】　ありがとうございます。事務局です。

これまでICTサービスの利用環境をめぐる諸問題として、特殊詐欺、闇バイト対策と携帯電話の本人確認のルールということで、４月以降、３回に分けて御議論いただいてきたところでございます。本日は６月６日のところでございますけれども、論点整理を予定しております。今後、本日の議論を踏まえまして、７月３日の親会へ報告をしていく予定でございます。

２ページ目でございますけれども、大きな２つ柱のうちの１つの特殊詐欺、闇バイト対策についてでございます。資料についてはこれまでのワーキンググループで御紹介した内容を再掲しているところも含むんですけれども、それぞれの論点についてオレンジの枠で考え方（案）というものをつけております。

まず、課題１と課題２の部分です。こちらについては昨年の特殊詐欺、SNS型投資ロマンス詐欺の被害額が過去最悪となっているような状況の中で、特に特殊詐欺においては国際電話発で固定電話着の電話が多用されているという話と、またそのほかの技能手段として携帯電話SMSメッセージなどが使用されているというようなことがございまして、こちらを踏まえてどういった対策が取り得るのかについて御議論いただいております。

５月９日に事業者からも御発表いただいたところです。その中では、固定向けの国際電話を休止する民間のサービスであります国際電話不取扱いセンターにおける申込みが急増していることを踏まえて、その体制の強化ですとか申込みの円滑化をどのようにしていくかというところについて御発表いただいたところです。また、携帯電話SMSメッセージにつきましても、迷惑電話のブロックサービスですとかメッセージのブロックを含めたフィルタリングなどを含めた各種詐欺対策のサービスについて、事業者において実施されているとの御発表をいただいたところです。

こちらについて、総務省においては６月上旬に迷惑電話の相談窓口を設置予定でございまして、この窓口と不取扱いセンターの連携をしながら官民連携を行い、早期解消することに貢献する予定でございます。また、事業者に発表いただきましたサービスについては、利用者の方にもよく知ってもらい、また、さらに使いやすくしていただくよう、周知ですとか低廉化の取組が必要になってくるところだと思っておりまして、事業者において周知に限らず低廉化についても一層の取組を推進して、実施していくこととしてはどうかという形で記載させていただいております。

課題３については、５月９日に発表したところでございますけれども、実在する電話番号を表示する偽装手口に関する課題についてですけれども、こちらは通信事業者と連携をして効果的な対策を今検討しているところで、できるところから実施しているところでございます。こちらについては引き続きの注意喚起とともに、移り変わっていく手口について引き続き検討を行ってはどうかとしてございます。

また、課題４につきましては、５月９日に発表したとおりのところもございますけれども、海外電話番号による詐欺電話については、簡単にアプリで取得可能なところ、関連する注意喚起を推進していくこと、また、引き続き実態把握を行ってはどうかと思っているところです。

大きな２つ柱の２つ目の携帯電話の本人確認のルールについてです。こちらは課題１から６がございました。課題１から３については５月16日にお示ししたところがございますけれども、課題１についてはSIMの不正転売について分かりやすい周知啓発を強化するとともに、事業者の取組を一層推進していってはどうかというところです。

課題２については、法人の代理権ないし在籍確認の部分ですけれども、必要な書類を求めるなど所要の規定見直しを行っていくこととしてはどうかとしております。

３つ目のところは、他社の本人確認結果の依拠については、まずは現在行っている議論

を踏まえた上で検討を進めてはどうかとしてございます。

課題４以降については、５月16日に御発表いただいた内容を概要として記載しておりますけれども、その上でそれぞれの構成員から、また発表者からの御意見を御紹介するとともに、考え方について示しております。５月16日の概要については時間の関係上から説明を割愛させていただきますので、構成員の御意見から御説明させていただきます。追加回線の本人確認についてですけれども、現状のID・パスワードの簡易な確認のみでは不安なので、当人認証の取組を向上させるべく、デジタル庁のガイドラインなども参考にしてはどうかという御意見を沢田構成員からいただいております。

２点目ですけれども、現在許容されている簡便な確認方法では足りないという状況が生じてきているということと、AppleWatchなどのデバイス追加の際に有意な悪用リスクがあるのかどうか確認するべきというような、中原構成の御意見をいただいております。

また、３つ目の部分ですけれども、追加回線の本人確認の際にはJPKIの活用などの事業者の取組も活用していくことが考えられるのではないかという御意見をいただいております。

今回の御意見と前回の御議論を踏まえまして、考え方（案）を示しております。読み上げていきますけれども、簡易な本人確認手法では一定の利便性が認められる一方で、現にそのような手法が犯罪の起点となっている点を踏まえれば、当人認証性を向上させるべく、デジタル庁のガイドラインなども参考に厳格化に向けた規定の見直しが必要ではないか。その際には、犯罪実態を踏まえて全ての改正に等しくルール適用するかどうかについても検討するべきではないかとさせていただいております。

次ですけれども、上限契約台数についてです。構成員からの御意見としまして、ID・パスワードを軸に本人確認を厳格に管理することができれば、契約台数の上限という考え方が不要になるのではないかというような御意見を辻構成員からいただいております。

２点目のところでは、複数台契約のニーズは様々に想定されるので、定型的な悪用リスクは想定できないので、常識的な範囲内で台数制限を予防的に設けるという現在の自主的な取組を継続しながら、状況を注視してはどうかという御意見を中原構成員からいただいております。

３点目ですけれども、沢田構成員から、事業者の取組として例えば使用用途を聞いた上で、その使用用途が申告内容と異なる利用をしている場合については解除するなどのことも考えられるのではないかというような御意見をいただきました。

こちらを踏まえまして、考え方のところですけれども、契約台数の上限については一部利用者からの複数台契約のニーズはあるものの、不自然に多数の契約が行われるケースもあり得る。業界ルールで示されている原則５台を超えての例外的な契約について、使用用途の事前の確認をする事業者がいることも踏まえ、事業者における自主的な取組を一層強化するべきではないか。その上で今後、業界ルールの適用状況について検証を行い、さらなる自主的な取組を促進するとともに、必要に応じて犯罪との因果関係を踏まえながら何らかのルール化について検討するべきではないかとしております。

６のデータSIMの本人確認についてです。こちらは発表内容の抜粋なので割愛させていただきまして、次、構成員、発表者からの御意見の部分です。総論としまして、データSIMについて悪用の実態が相当程度確認される以上、悪用リスクはあると言うべきであって、本人確認の義務づけの対象とするのが原則ではないか。その際には例外を設けることについて検討するべきということで、SMS機能がついていないものやIoT機器等に利用されるものを除外するべきかということについては悪用リスクの評価の問題であり、悪用リスクが低かったり、技術的にコントロール可能であったりということは除外してもよいと思うという御意見を中原構成員からいただきました。

また、仲上構成員からは、様々なサービスの利用において携帯電話の番号というのが本人確認するためのトラストアンカーになっているので、SIMの通話機能ですとかSMS機能のありなしによってこのトラストアンカーとしての役割は変わってくるのではないかという御意見をいただいております。

対象SIMのところですけれども、沢田構成員から、SMSつきのデータSIMについては厳格な本人確認が必要ということで合意の方向だと考えているけれども、例外のところをどのようにするのかというのは精緻な議論が必要ではないかという御意見をいただいております。

その１個下の鎮目構成員ですけれども、SMSなしのSIMついてどの程度悪用実態があるのか、現時点でどれぐらいあるのかも併せて厳格化を考える必要があると。特にネット経由で訪日前に購入されるケースも多いので、義務化というのは相当大がかりな変更になるので慎重な検討が必要という御意見をいただいております。

仲上構成員からSMSなしのデータSIMについて、トラストアンカーについての役割を考えたときに犯罪を抑制する効果を期待できるのか、それとも捜査の精度を高めていく効果が期待できるのか、疑問であるというようなコメントをいただいております。

最終ページに移ります。利用用途の訪日外国人向けプリペイドの部分ですけれども、こちらについては詐欺事件に利用されているものがあるのか要検証という御意見を山根構成員からいただきました。これについて、補足説明を警察庁からいただく予定です。また、４月22日に発表した事例においてもこのプリペイドだったのかという御意見をいただいたので、こちらも補足の発表をいただく予定です。

３ポツ目ですけれども、自販機での販売については抜け穴にもなり得るのではないかというような御意見を鎮目構成員からいただいています。

また、４点目ですけれども、プリペイドSIMを除外するべきかについて、原則、本人確認自体は必要であろうと。一方で現実的困難性の問題もあるので、検討するべきはその方法の緩和であって、貸与時の本人確認の規律を参考にするということも含めて、引き続き検討が必要ではないかという御意見を中原構成員からいただいております。

本人確認の実効性の部分でございますけれども、こちらについてはパスポートによる本人確認を判断するのが店舗スタッフであることから、実効性の確保は難しいのではないかという事業者からの御発言があったところですけれども、こちらについて星構成員からパスポートが偽造かどうかに関わらず記録自体を残すということが、偽造パスポートの出どころ調査につながるなど捜査の進展に資するのではないかというような御意見をいただいております。こちらについても警察庁から本日、補足説明をいただける予定です。

以上の議論を踏まえまして、一番下に考え方（案）として記載させていただいております。データSIMについては悪用の実態が確認されたことを踏まえて、一部の事業者で既に行っている本人確認の取組を確実に行うという観点から、義務化について検討するべきではないか。ただし、義務化の検討に当たっては貸与時の本人確認の規律も参考に、対象SIMですとか利用用途、例えば訪日外国人やIoT機器などに関して利便性、不正利用のバランスの観点から利用実態や実効性に配慮した規定とするべきではないかというように考え方を記載させていただきました。

事務局からは以上でございます。

【大谷主査】　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、警察庁の方からも御説明をいただきたいと思います。資料で８ページのところで、構成員からいただいていた御質問について御回答を用意していただいておりますので、よろしくお願いいたします。

【警察庁（根本）】　警察庁の根本でございます。３点、補足の説明をさせていただき

ます。

まず１点目、山根構成員から御指摘をいただいております、SMSつき訪日外国人向けのプリペイドSIMで、詐欺事件に利用されていたりするものはあるのか要検証という御指摘をいただいております。こちらについてまず、お答えをいたします。前回御説明をさせていただいたSNS型投資ロマンス詐欺に係る被疑事件に使用されたSMSつきデータSIMの一部が、訪日外国人向けのプリペイドSIMでありました。前回、資料９－２で説明をしている資料となります。再度簡単に説明をさせていただきますと、SIM種別の特定に至ったのが244件、そのうち185件はSMSつきデータSIMでありました。さらに185件のうち本人確認がなされていたのは75件で、そのほとんどが訪日外国人向けプリペイド型SIMでありました。

２点目が、沢田構成員から御指摘をいただいております、警察庁の４月22日発表の事例２の、架空の契約者情報で契約をしたSMSなしデータSIMを使用した事件では、プリペイドで短期滞在の観光客が犯罪に加担していたというケースなのか確認が必要であるという御指摘をいただいております。こちらについてお答えをいたしますが、御指摘の事件で使用されたSMSなしデータSIMはプリペイドではありませんでした。また、当該SIMはインターネット上において訪日外国人に限らず広く販売されているものであります。

続いて３点目、星構成員からの御指摘について追加の説明をさせていただきます。例えばホテル宿泊の際に必ずパスポートの提示を求められている。パスポートが偽造かどうかに関わらず、記録自体を残すことは偽造パスポートの出どころの調査にもつながるなど、捜査に資するものではないかという御指摘をいただいております。こちらについては一概には言えないところもありますが、御指摘のとおり、偽造パスポートの使用記録を調査することによって被疑者の行動を追跡する手がかりとなる可能性もあると考えております。また、この偽造パスポートが複数の事件に共通して使われていた場合には、その利用状況を分析することによって事件間の関連性を解明できる可能性もあるものと考えております。

私からの追加説明は以上となります。

【大谷主査】　御説明、ありがとうございました。

それでは、御質問いただいていた山根構成員、それから沢田構成員、それから星構成員に御確認させていただければと思っております。山根構成員、今の御回答でいかがでしょうか。

【山根構成員】　ありがとうございます。追加の質問等は特になくて、訪日外国人向けのプリペイドSIMも犯罪利用されているということなので、訪日外国人向けのものだから

ということでこのSMS機能つきのものを対象外にするというのは慎重にやらないといけない、本人確認義務の対象にしていくべきということになるかと思いました。

【大谷主査】　ありがとうございます。プリペイドSIMで短期間なのでというということで、事件に使われにくいのではないかという声も当初ありましたが、犯罪実態もあるということですので、実際に訪日外国人の方が犯罪に関与したかどうかは分かりませんけれども、そのような形で手に入るものは本人確認を行ったほうがいいという御意見だと受け止めました。

それでは、沢田構成員からはチャット欄にコメントをいただいております。「御回答ありがとうございます。いろいろ入手経路があることがよく分かりました」ということで、ネット経由で誰でも入手できるような形で、SMS機能がないデータ通信SIMを使用していた事例もあったということですね。様々なところに犯罪実態があるということです。

それでは次に、訪日外国人のホテル宿泊の際にパスポートの提示をいただいていて、例えば偽造のパスポートでもということなんですが、星構成員、いかがでしょうか。

【星構成員】　ありがとうございます。素人考えの質問に対して丁寧にお答えいただきまして、ありがとうございます。ですから、ともかく偽造のものであっても提示してもらっているということで分かることがあり得るということであれば、確かに事業者さんに対して一定の御負担をいただくことになってしまうわけですけれども、何のために本人確認をするのかということであれば、不正利用を抑止するということに加えて、不正利用されてしまった、犯罪ツールとして使われてしまった場合の追跡可能性の把握ということからすると、私自身はそれなりに意味のあることなのではないかと思った次第でございます。ありがとうございました。

【大谷主査】　ありがとうございました。

警察庁におかれましても、改めて、質問への御回答をいただきまして、ありがとうございました。

それでは、事務局から用意していただいた説明、それから今のやり取りを踏まえまして、全体の討議に移りたいと思います。委員の皆様からの御質問、御意見、特にテーマは絞らずに、全体について行いたいと思います。

それでは、チャット欄に沢田構成員から御記入いただいておりますので、代読をさせていただきたいと思います。

「方針案のお取りまとめ、大変お疲れさまです。特殊詐欺、闇バイト等の対策（課題１、

２）については、総務省の相談窓口が開設され、通信事業者さんとしても、国際電話不取扱センターの積滞解消やホームページの改修を含む体制整備をしていただけるとのこと、ありがとうございます。通信事業者さんにさらなる御負担をおかけするのは心苦しいですが、利用者としては、費用がかかることがネックとなって、せっかくの各社の詐欺対策サービス利用を控えるということにならないよう、基本的な対策部分はできるだけお安く（できれば無料かつデフォルト設定に）していただけると助かります。高機能の対策には開発コストもかかっていると思いますので、有料オプションで問題ないと思います。

次に、課題３、４の注意喚起は本当に重要ですが、手口の解明や実態把握はそれ以上に重要で、消費者庁や国民生活センターとも連携・協力し、トラブル事例を集めて分析する省庁横断の仕組みをつくっていただきたいです。」

貴重なコメント、ありがとうございました。

それでは、辻構成員、よろしくお願いいたします。

【辻構成員】　よろしくお願いします。ありがとうございます。今回、このワーキング、４回目になりますけれども、短期間でこれだけの幾つもの課題を皆様でうまく整理できてきたのかと思っております。本当にありがとうございますといったところですけれども、私が思いますのは、最近はいろいろ犯罪も巧妙化してきて、利用者の利便性よりも安全性の確保にどうしても倒さなければいけない状況になりつつあって、その中で本人確認等を厳密化するというのはもうしようがないことなのかと思っている次第です。そういった中で今回の取りまとめについては大枠、全体の方向性、このような形でいいのではないかと私は思っております。

幾つかコメントさせていただきますと、課題１、２につきまして、国際電話不取扱いセンターにつきまして、私は存在を知らなかったんですという話しを前回もさせていただいたんですけれども、単なるプロモーションに限らずもう少し、プロモーションしか方法はないのかもしれないんですけ

れども、みんなに知っていただく方法、もしくは例えばキャリアさんと連携して、安全にしたいというのを最初からお望みのユーザーさんには最初からもう国際電話は使わないといったオプションを用意するとか、そういったことも必要なのではないのかと。あとは、官民連携によって低廉化するというのはぜひ推し進めていただきたいと思っております。

あと、４番の追加回線の整理というところも非常によい形でまとめていただいたと思っているんですけれども、そこに当人認証性を向上させる云々という記載があったんですが、

その内容と課題１の新規の部分の当人認証のレベル感はぜひ合わせていただきたいと思っております。

コメントとしては以上になるんですけれども、デジタル庁さんが本人確認のガイドラインを今用意されている中で、そういったものともしっかり整合を取って、ぜひ本人確認といったところを進めていただく、あとはキャリアさんとの連携をうまく、各キャリアさんにお願いするのではなくて連携して進めていただくということをお願いできればと思っております。以上です。

【大谷主査】　貴重のコメントをありがとうございました。デフォルトでどこまでできるのだろうかということは結構真剣に追求しなければいけないなと思いながらお話を聞かせていただきました。

【辻構成員】　私もそう思っております。よろしくお願いします。

【大谷主査】　ありがとうございます。

次に、山根構成員、よろしくお願いします。

【山根構成員】　まず、事務局におかれましては短期間で論点整理、考え方の案をまとめていただいて、ありがとうございます。基本的な方向性については私も賛成しているところでございます。これまでの会合の中であまり実質的なコメントができていなかった部分もありますので、全般的に、少し長くなるかもしれないんですけれども、コメントさせていただきたいと思います。

まず、特殊詐欺、闇バイト等の対策関連なんですけれども、こちらについてはなかなか特効薬的な対策がない中で、犯罪手口であったりとかユーザーが取り得る対策、あるいは自分が特殊詐欺、闇バイトに加担してしまった場合のリスクについて周知啓発をしていくということに頼らざるを得ない部分があるかと思います。そういう意味では、ここに書かれているとおり注意喚起であったり周知の活動を進めていくという方向性については、賛成いたします。また、特に犯罪の手口の傾向は状況によってどんどん変わってくると思いますので、そういった犯罪手口の傾向について官民、あるいは民民で適切に情報連携して、状況に応じた周知啓発の活動を引き続き行っていただくというのがいいと思っております。

続いて携帯電話の本人確認ルールですけれども、まず課題の１から３の部分については、前回会合の段階でも基本的な方向性については認識共有が得られているところだと思いまして、私もまとめていただいた方向性に賛成でございます。個別の論点について少しコメントさせていただくと、法人の代理権の確認については、これは利用者目線で予測可能性

を高めるというところを主眼にしていて、現状として担当者の代理権確認のルールが明確でないということで、何か不正利用が広がっているというような状況ではないと理解しておりますので、そういう意味では、具体的に規定を見直すに当たっては確認の際に用いることができる書類を明確化していくということをしつつ、犯収法では担当者が法人のために行為を行っていることが明らかである場合には書類の確認までは要しないというような建てつけになっておりますので、そういった形で柔軟な対応の余地を残しておくということも考えられるのではないかと思っております。

続きまして、課題４点目の追加回線の本人確認についてなんですけれども、こちらは２回線目以降の回線契約が容易になっていることが犯罪利用に寄与をしているところがあると思いますので、確認方法を厳格化していかざるを得ないと思いますし、そのやり方として本人認証のレベルを上げる方向で検討していくというところも賛成いたします。当人認証の保証レベルをレベル２以上の方法を求めていくというようなところが基本線になっていくのではないかと思っております。

全ての回線契約について同じルールを適用すべきかどうかというところにつきましては、契約形態ごとの犯罪利用実態で不正利用のリスクの程度に応じて検討すべきということにはなるかと思うんですけれども、現状ID・パスワードによる確認だけでやっていたところについて多要素認証を導入するということであれば、利用者利便への影響はそこまで大きくないというような評価もあり得るかと思いまして、そういったリスクの程度と利用者利便への影響とのバランスを考慮しての検討をしていくべきではないかと思います。

こういった法令レベルでのルールの設定の話に加えて、事業者の取組としてリスクに応じた確認方法を実施するということも考えられるのではないかと思っております。次の論点にも関係してくることなんですけれども、例えば契約の数が多いと不正利用のリスクが高まるというような評価ができると思っておりまして、リスクの程度の判断要素は契約数に限られないとは思いますけれども、リスクが高いと判断できるような場合には通常の本人確認方法と同様の方法で実施するという形で、リスクに応じた対応をするという取組が行われるのが望ましいのではないかと思っております。

上限契約台数についてはなかなか法令レベルで定量的な基準をいきなり設定するのは難しいかと思いますので、自主的な取組としてやっていくべきだと思っております。先ほど申し上げたとおり、契約台数が多くなると不正利用があった場合の影響の程度も大きくなり得るという意味では、契約台数が多くなるほどリスクが高いという評価もできるかと思

いますので、そういった場合には、SIMの不正転売の取組の中でも定期的な本人確認の取組ということで、契約後の対応についても挙げられていますが、契約台数が多い場合には契約後の顧客管理の段階でその点を考慮した取組を行っていくということも考えられるのではないかと思います。

最後、データSIMについてなんですけれども、犯罪利用の実態を踏まえますと、本人確認義務を課すという方向性については賛成でして、その上で対象範囲をどうするかというのが一番の論点だと思います。こちらも基本的には犯罪の実態を踏まえたリスクの程度と、顧客の利便や事業者への影響というところを考慮して判断することにはなるかと思います。SMS機能なしのデータSIMに関しては、犯罪利用された場合のリスクの程度や使われ方というところもSMS機能つきのものとは異なってくると思いますし、これまでの会合における事業者様の発表を聞くに、利用者利便であったりとか事業者の活動への影響が相応にありそうだと思いますので、少し慎重な検討が必要になる部分ではないかと思っております。

警察庁様からの発表では、犯行時の通信に利用されたりとか、一定の犯罪利用の実態はあるということだったんですけれども、定量的な実態まではつかみ切れてないというのが現状かと思いますので、そういったところも加味して当面は実態把握に努めつつ、まずは事業者の自主的な取組を促進していくという方向もあり得るのではないかと思っております。長くなりましたが、私からのコメントは以上になります。

【大谷主査】　非常に丁寧なコメントをいただきまして、ありがとうございました。また、全体にわたって御意見をいただくことができまして、ありがとうございました。先ほどから本人確認のところ、データSIMのところの本人確認で、いろいろ犯罪実態はSMS機能ありなしどちらもあるというようなことでありましたけれども、確かに山根構成員がおっしゃるようにリスクの程度には軽重があるところもありまして、今御指摘いただいたようなリスクベースでの対応を検討していくことが必要なのではないかと受け止めさせていただきました。

次に、中原構成員から御発言いただきたいと思います。

【中原構成員】　事務局にお示しいただいた方向性につきましてはいずれも賛成でありますけれども、補足的にコメントさせていただきたいと思います。

前回の検討会に寄せたコメントでも申し上げましたように、論点４から６の携帯電話の本人確認のルールについては、悪用されるリスクが定型的に存在するということが確認されるか、確認される場合には、一定のものについては例外が認められないかが問題となる

と理解しております。追加回線であるとかデータSIMについては基本的に悪用されるリスクが確認されるということなので、規制強化の方向を原則としつつ、過剰な規制にならないように例外を認めていくと。他方、多数台契約のほうは、いろいろなニーズがあって、現状悪用されるリスクを定型的に見いだすことはできないので、一律な規制強化は控えつつ、過少な規制にならないように、怪しいものがないか注視していくということなのではないかと思います。

やや気になっていますのは、基本的には本人確認は必要だけれども、例外的に不要とする、あるいは緩和するといったときの例外の根拠です。これは、特に論点６のデータSIMについて問題となることだと思いますけれども、SMSなしのデータSIMであるとかIoT機器向けのデータSIMというのは、それぞれの機能、用途に照らして悪用されるリスク自体が低いために例外となり得るということなのだと思います。それに対してプリペイドSIMというのは、プリペイドであるということだけからは悪用されるリスクが低いと言うことはできない。その意味で本人確認は本来必要なんだけれども、訪日外国人のような現実の利用者層を考えると、厳格な本人確認は現実的でないと。

そういう意味での現実的な困難性に照らした緩和だというふうに位置づけるべきであって、その意味では悪用されるリスク自体が低いものとは区別して、つまり悪用リスクはあるんだけれどもそれでも緩和すべきかという、言わば一段低い問題として考えるべきなのかと思います。

以上は雑駁な整理に過ぎませんけれども、いずれにせよデータSIMについては特にですけれども、様々なものがあり得るだけに、ルール化に向けた具体的な検討の際には一定の交通整理が必要になってくると思いました。

それからあともう１点ですが、論点１のSIMの不正転売、あるいは前々回に取り上げられた闇バイトに関連して、周知啓発の強化について追加的なコメントをさせていただきますと、現状、事業者の店頭掲示では、あなたがやっていることは違法行為であって犯罪に当たりますよと、判明すれば警察に通報しますよという警告、あるいは逆に警察に相談してはどうですかという勧告がメインであるようですけれども、こうした刑事上の事柄だけでなくて民事上の事柄についても、もっと警告・勧告してもよいのかもしれないと思いました。

４月のNTTドコモのヒアリング資料では、携帯電話契約を締結した場合、闇バイトであっても支払い義務が契約者にあること、契約を取り消すことができないことを警告する店

頭掲示が紹介されていたと思います。ただ、こうした契約上の事柄だけでなくて、不法行為、民事の損害賠償責任の問題もあり得ます。詐欺被害者は自己の損害の賠償を詐欺の首謀者に対して請求する、これはもちろん論理的に可能なわけですけれども、詐欺の首謀者は行方をくらましてしまっていて、現実に請求することは難しい。そういった場合に詐欺に使われる手段を提供することによって作業を容易にした者に対して、損害賠償請求をするということも十分に考えられまして、現に預貯金口座の提供の事例では口座提供者の損害賠償責任を認める下級審裁判例が幾つか出ているようであります。

SIMの不正転売、携帯電話の無断譲渡の事例では、闇バイトとして素人が加担してしまう。もちろんそうした人たちに重い責任を課すべきなのかということは問題となり得るにせよ、闇バイトがこれだけ社会問題化し、これだけメディアでも報じられている中では、知らなかった、あるいは軽い気持ちでやってしまったというような言い訳は、民事の損害賠償請求でもなかなか通用しない。つまり、過失が認められてしまう。そうすると、自分が闇バイトで得た報酬よりもはるかに多額の責任を背負うことになってしまうというわけで、そういった経済的に多大な不利益があり得るというような情報は、もしかすると刑事責任と同等の、あるいはそれ以上の抑止力として働くのかもしれないと思った次第です。もちろん現状、最高裁判決があったりするわけではないんですけれども、今後必ず本格的に出てくるのではないかという問題でありまして、闇バイトがなかなか後を絶たないということになった場合に、こういった民事上の不利益についての啓発をしていくことも重要なのではないかと思いました。長くなりましたけれども、以上です。

【大谷主査】　中原構成員、どうもありがとうございます。御欠席の間も丁寧なコメントをお寄せいただきましたので、全体の議論の整理に非常に役立てさせていただいたことに御礼申し上げたいと思います。特に今データSIMの種類別に本人確認の事務をどれだけ求めるかといったことについてもよく整理していただきましたので、最終報告にはぜひ取り込みたい御指摘ではなかったかと思っております。また、闇バイト問題につきましても、何らかの経済的な利益を目的として、犯罪とは知りつつ手を染めるというような人に対しては、経済的な不利益を強調するという啓発の仕方もあり得るということで、いい御示唆をいただきました。

それでは、次に沢田構成員、読ませていただきます。

「本人確認のルールに関しては、１から３の論点に加え、４の追加回線についてお示しいただいた考え方（案）に異議ありません。５の上限契約台数についても異議ありません。

業界ルール強化後も同様の犯罪が発生してしまった場合には、お書きいただいている通り因果関係、つまりどこに穴が開いていたのかをしっかり分析・検証する必要があると思います（全ての論点に当てはまる話ですが)。

６番のデータSIMの本人確認については、警察庁から追加の情報をいただき、ありがとうございます。原則義務化とし、対象や用途に応じて例外を考えていくという考え方に異議ありません。その上でのコメントですが、SMS機能がないもののうち、IoT機器向けは例外扱いで問題なさそうに見えます。それ以外はまだ実際に発生している犯罪との因果関係が明らかになっていないようですが、だからといって今後もリスクがないとはもちろん言えず、匿名性を確保できる通信手段が他になくなっていけば、犯罪者はこれを使おうとするのかもしれません。なので油断はできないと思う一方で、SMS機能のないデータSIMを現在誰がどう入手して何に利用しているのか、本人確認を強化した場合の利用者への影響等について十分な判断材料が揃っているとは言えない段階ですので、本人確認の強化についてはまずは慎重に現状維持とし、今後の犯罪発生状況によって再度精緻に検討するということでもいいのではないかと思います。」

丁寧なコメントをありがとうございました。おおむねこれまで構成員から寄せられた議論の方向性と同じように受け止めております。

ありがとうございます。仲上厚生委員から挙手いただきました。御発言をお願いいたします。

【仲上構成員】　これまで議論の中でいろいろと発言させていただいた内容を含めて、事務局のほうには丁寧に取りまとめていただいているところと、あと前回質問になっていたところについて警察庁のほうからコメントをいただいて、非常に参考になる情報をいただけたかと思います。今回事務局でまとめていただいている内容、方向性については非常にそのとおりだと思っておりますので、この方向で取りまとめを進めていただければと思う次第です。以上でございます。

【大谷主査】　ありがとうございます。賛同意見ということで受け止めさせていただきました。これまでのワーキンググループでも、いい発言をたくさんしていただいて、ありがとうございました。

鎮目構成員からも、ありがとうございます。御発言、よろしくお願いいたします。

【鎮目構成員】　事務局におかれまして、大変丁寧に、今回は取りまとめ案をつくっていただき、ありがとうございます。私も全体の方向性については全て賛成でございます。

とりたてて指摘させていただきたいことはあまりないのですが、携帯電話の本人確認については基本的には強化していく方向で、どこまで例外を認めるかという辺りが今後の課題ということは非常によく理解できました。

先ほど中原構成員が御指摘くださった、本人確認を例外的に緩和する根拠をどこに見いだすのか、すなわち、悪用リスクが低いのか、それとも規制自体に現実的に限界があるという、そういう違いに基づいて例外を認める範囲を決めていけばいいのではないかという御指摘に、全く賛成でございます。あとは、闇バイトに関しては、方向性は賛成ですが、新しい様々なテクニック、犯罪に用いる方法が出てくるところ、スプーフィングというのが非常気がかりに思っているところではありますが、この辺りについては今回の取りまとめでも今後の課題として挙げられていたかと思いますので、引き続きこういった新しい手口に弾力的に対応できるような検討をお願いできればと思います。

【大谷主査】　ありがとうございます。おっしゃるようにスプーフィング、連日報道されていて、おおむね一定の手口が国民全般に共有されてきて、同じ手口に引っかかる人はなくなっていくのかなと思いつつ、そうするとまた新しいものが出てくるので、弾力的な運用ができるような仕組みというのも、要するに事業者の自主規制などに頼りつつということだと思いますが、そういう自主的な取組の役割の大きさも含めて、今回のワーキンググループで再確認できた事柄かと思っております。

また手を挙げて、星構成員からも、ありがとうございます。御発言、よろしくお願いします。

【星構成員】　どうもありがとうございます。私自身も特にとりたてて新しいコメントがあるというわけではないんですけれども、最後の会だということもあるので一言述べさせていただきたいと思います。

これはどこかの段階でもお話しさせていただきましたけれども、こういったような一つの犯罪の形として犯罪者の側が身元をいかに隠せるか、偽ることができるかということの要請といいますか、そちらへの需要というのは非常に大きなものがあって、それが携帯電話の普及とともにいろいろこれまでも050電話を潰してみたりとかいろいろな、ある意味いたちごっこなところがあったのかもしれませんけれども、どこかで対策をとれば別のところに流れていってしまうという、先ほど沢田構成員からの御指摘にもありましたように、そういったようなことは続いていくんだろうとは思うんです。けれども、さはさりながら現実的な問題として先ほどから縷々、中原構成員をはじめ皆様方、御指摘のように、現実

的な可能性というところ、事業者の負担の問題、実効性の問題であるとか、あるいは不適正利用されるリスクとのバランスの中で考えていく中で、今回、事務局に大変な御尽力をいただいてお取りまとめいただいた案、私といたしましても現時点で非常に必要十分な対策を受けているのかとは思います。

そうだとしますと、それをいかに展開していくかというところで、これは闇バイト関連の周知徹底というところも含めてですけれども、事業者その他の関係者との間での今後の調整ということが非常に重要になっていくのかと思います。ぜひとも、社会インフラを提供される事業者の方としての責務として一定の御負担について御理解をいただきたいし、また利用者の側としても本人確認が厳格になっていくということの意味合い、本人確認に関しては諸外国ではあまりないのではないかというような話もある一方で、マイナンバーカードが日本にもできましたけれども、そういったものとひもづけをしなければ携帯電話が買えないといった国もあったりして、様々な中で日本としては当面こういうやり方をやっていくんだということを、訪日の方も含めて御理解をいただいていく必要があるかと思います。

その中で枠組みとして何か反対するというわけではないんですけれども、海外電話の関係については今の状況ではもうやむを得ないところはあるかと思いますけれども、喫緊の課題でもありますので、ぜひ最大限ストレッチをして早急な対応をいただきたいということだけ、最後コメントさせていただければと思います。私からは以上になります。ありがとうございます。

【大谷主査】　星構成員からもコメントいただきまして、ありがとうございました。本当に御指摘のとおりでして、訪日外国人が利用されているデーSIMについてはなかなか本人確認をやろうとしてもその実効性が分からないという、それを理由にして、リスクは決して小さくないわけですけれども、利便性にも配慮しつつ、またサービスを提供する事業者にとってのサービス提供の可能性といったことにも一定の配慮をしつつ、何らかの結論に、例外ルールを決めるときの範囲をより明確にしていくことになろうかと思いますが、貴重な御意見をいただきまして、ありがとうございました。

それでは、全員何らかの形で御発言いただきまして、ありがとうございます。まだ、時間がありますので、ありますのでというかそれほどないんですね。すみません、今日は16時までというおおむねのお約束でスタートさせていただいたので、既に残された時間が限られておりますが、御発言を希望される方、いらっしゃいますでしょうか。大丈夫な感じ

でございますね。

そうしますと、今回が確かに最後のワーキンググループの会合でございまして、この辺りで討議につきましては一区切りさせていただければと思っております。活発な御議論、そして貴重な御意見を多数いただきまして、ありがとうございました。今日も非常にたくさんの御意見をいただきましたので、ぜひ皆様方の御意見というのは、今回の規制強化に当たってのコメントもありますし、また今後を見据えての課題についての御指摘もあったと思いますので、これらを報告書形式で取りまとめる際にできるだけ事務局には取り込んでいただければと考えております。

全体の方向性についてはおおむね賛同意見をいただいているということでございますので、実際の報告書の文案につきましてはまた皆様に御覧いただくとしても、最終的な取りまとめについ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でしょうか。

特に御異議もないようですので、ありがとうございます。それでは、事務局に原案をつくっていただきまして、その原案を皆様に展開しつつ、私のほうで取りまとめをさせていただきたいと思います。その上で、親会であるICTサービス利用環境の整備に関する研究会に御報告をさせていただきます。ありがとうございました。

それでは、事務局から連絡事項をお願いいたします。

【田中利用環境課課長補佐】　本ワーキンググループは本日で一区切りとなります。本当に先生方には御議論いただきまして、本当にありがとうございました。親会であるICTサービス利用環境の整備に関する研究会の開催については、別途事務局から御案内いたします。以上です。

【大谷主査】　ありがとうございました。進行にも御協力いただきまして、ありがとうございます。

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の第10回会合を終了させていただきます。本日まで皆様、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。