不適正利用対策に関するワーキンググループ（第７回）

令和７年４月21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７回会合を開催いたします。

本ワーキンググループの事務局を務めます総務省総合通信基盤局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、投映で割愛させていただきまして、開催上の注意事項に沿って、本日、進めさせていただければと思います。

本日の資料は、資料７－１から７－７まで準備しております。また、本日は山根構成員が御欠席、星構成員が冒頭のみ御参加、中原構成員が遅れる御予定と聞いております。

では、早速、議事に入りたいと思います。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、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。

本日の進め方ですけれども、まず、事務局から御説明をいただきまして、その後、警察庁、その後はNTTドコモ様、KDDI様、ソフトバンク様、楽天モバイル様、テレコムサービス協会様、個社から発表いただいた後に、皆様との意見交換を進めたいと思います。

それでは事務局から、よろしくお願いいたします。

【田中利用環境課課長補佐】　本日は、ICTサービスの利用環境をめぐる諸問題について、特に不適正利用対策をめぐる環境変化と新たな対策について、御説明させていただきます。

１ページ目らは１月22日の親会の資料を再掲しております。

これまで、犯罪に悪用される情報通信ツールの多様化に応じまして、総務省においては、本人確認や利用停止などを中心とした対策を講じてきました。一方で、ツールの悪用と対策がいたちごっこになっているということが繰り返されてきていたと思います。

１月22日の親会の時点では、闇バイト犯罪をはじめとして、携帯電話番号の悪用のみならず、SNSアプリや海外電話番号を悪用した被害が増加してきていたところです。

こうした多種多様な形態で不正行為が行われていること、より総括的な対策が求められるようになってきたということを踏まえまして、１月22日の親会では、具体的な課題を７つ取り上げまして、こちらの表にございます１から７について、また、追加での課題が必要ということであれば、不適正WGで集中して御議論いただくということになっておりまし

た。

その後、新たな環境変化が２点ほどございました。

１点目が、特殊詐欺、SNS型投資・ロマンス詐欺の被害の増加です。昨年度の被害額は2,000億円ということで、過去最悪の水準となっております。また、特殊詐欺においては、左下にございますように国際電話発、また固定電話着の悪用が多いことですとか、その右にございますように、そのほかの欺罔手段として、携帯電話、SMS、メッセージなどが悪用されているということが分かってまいりました。これらの甚大な被害への対策として、自民党調査会では、金融関係・通信関係への提言を２月に取りまとめております。この中には、（１）、データ通信SIMの契約時における本人確認の義務づけですとか、（２）から（４）にございます固定電話の国際電話サービスの詐欺への対策、また、詐欺電話・詐欺SMS・詐欺メールへの対策、また、（６）にございますような通信履歴の保存の義務づけに関する対策が盛り込まれております。こちらが環境変化の１点目でございます。

環境変化の２点目でございますけれども、犯罪行為の巧妙化、高度化に伴う犯罪の増加です。本年の２月下旬頃ですけれども、３名の中高生が、不正に入手した大量のIDとパスワードを組み合わせて、楽天モバイル社に対して生成AIを悪用して自作したプログラムを用いて不正アクセスを行い、多数の回線契約を行ったというような不正が発覚しております。その後、同様の手口による不正契約ですとか、当該不正契約をした通信回線を用いた新たな犯罪も判明しているところでございます。少年たちは、楽天モバイル社の契約の上限数が多く、また、追加契約に本人確認が必要ないということを狙ったと供述しております。また、SMSつきデータSIMを悪用した犯罪については本件以外にも発生しているということで、後ほど警察庁から発表をいただく予定です。

こうした２点の環境変化を受けまして、⑧⑨⑩⑪の部分について、論点を追加して御議論いただければと考えております。⑧が特殊詐欺対策として、先ほどの固定・携帯、SMS・メールに関する対策でございまして、⑨から⑪が不正契約への対策でございます。

①から⑪とありますけれども、論点を再構成しまして、携帯電話の本人確認のルールについては本日扱いまして、特殊詐欺、闇バイト対策を次回に取り扱いたいと考えております。

今後の検討スケジュールですけれども、右側のほうを御覧いただきまして、当面の活動として、携帯電話の本人確認のルール、闇バイト、特殊詐欺対策、その後幾つか予備日を設けておりまして、６月中旬頃の中間整理を目指して議論を進めていきたいと思っており

ます。

また、その内容については、左側にありますように親会にフィードバックをして、最後７月に取りまとめを目指していきます。

ここから各論を１つずつ説明してまいります。携帯電話の本人確認のルールとして６点ほど挙げております。

１つ目はSIMの不正転売でございます。現行法令上、携帯電話事業者に無断で携帯電話端末設備等を譲渡する場合、携帯電話不正利用防止法に抵触いたします。最近、青少年などに対して、携帯電話端末設備等を高額で買い取るという触れ込みで、犯罪者自身の代わりに契約させるというようなアルバイトが横行しております。バイト応募者は、各携帯ショップに対してそれぞれ契約を割賦で行うので、譲渡した後、契約の分割金を払い続ける必要があり、負債が残るような形になります。また、バイト応募者が、犯罪者に端末を譲渡または転売した場合、詐欺ツールに使用される可能性というのも指摘されているところです。事業者の取組としまして、不適正利用対策として、ふるまいチェックによる慎重な審査ですとか、事業者を含めた関係者での情報共有、また、利用者への啓発ということで重要事項を説明していただいたり、様々な取組をしていただいているところですけれども、ここの論点にありますような記載も含めて、転売の防止に向けてどのような効果的な対策が考えられるかというところを御議論いただければと思っております。

次は、法人の代理権ないし在籍確認の観点です。現行法令上、法人が新規契約をする場合は、法人自身の本人確認として、登記事項証明の提示に加えまして、来店する担当者の本人確認が義務づけられているところです。一方で、来店する担当者と法人の関係性を担保するようなもの、代理権があるかどうかということについての要件は定められておりません。事業者においては自主的な確認を実施しておりまして、例えば委任状ですとか名刺を求めたり、様々な書類を求めるような形になっておりますけれども、利用者からは分かりづらいという指摘がございます。こういったことを踏まえまして、利用者視点に立って、どのような方策が求められるべきか、例えば分かりやすさや整合性の観点から要件を明確化するべきか、その際にはどのような書類を認めるべきかということについて御議論いただければと思います。

３点目ですけれども、こちらは他社の本人確認結果への依拠でございます。こちらは昨年６月までのワーキンググループでも御議論いただいたところですけれども、一部について引き続き検討課題になっていたところでございます。今般、金融機関及び携帯電話事業

者への本人確認結果に依拠するスキームについて提案がございました。特に携帯電話事業者への依拠については、事業者からも具体的なニーズが認められているところでございます。一方で、他社への本人確認結果に依拠するというところは、そもそも近時、ID/PASSによる本人確認が可能な契約形態を突いた不正契約が行われていることも踏まえて、依拠を認める是非をどう考えるかという点ですとか、少なくとも携帯事業者への依拠については、まさに本人レベルの、保証レベルを上げる取組がまさに行われている段階であるということについてどのように考えるか。また、金融機関への依拠については、金融機関側からのニーズですとか、運用の実現可能性として、間にどういう方に入っていただくのかといったところをしっかり議論していく必要があると考えておりまして、ここに記載の論点などを含めて御議論いただければと思います。

次は、追加回線の本人確認です。現行法令上、音声SIMに関して２回線目以降の追加契約をする場合は、本人確認書類を提示する方式に加えまして、ID/PASSによる簡易な本人確認方式が認められているところでございます。事業者の取組として、本人確認書類の提示を２回線目以降の契約でも自主的に求めているところでございますけれども、昨今の犯罪行為の高度化に伴いまして、このID/PASS方式で本人確認をしたものについて、不正契約が行われる事例が報告されております。ですので、現行法令上のID/PASSのみによる本人認証の認証レベルが十分に高いのかという論点ですとか、また、音声SIMつきAppleWatchについてもID/PASSが認められているんですけれども、様々なサービスがある中どのように考えるのか、ここに記載の論点も含めて御議論いただければと思っております。

５点目ですけれども、上限契約台数です。こちらは現行法令上、上限契約に対する台数制限はございません。一方で自主ルールでは、音声SIMについては５台、データSIMないしAppleWatchについては特段ルールがないというところでございます。一度不正契約がなされた場合に、犯罪被害が広がった事例があると報告されております。こちらについて、本人確認が適切になされない場合に大量不正契約につながる可能性も踏まえて、何らか制度的な担保を行うべきかなどについて御議論いただければと考えております。

６点目ですけれども、データSIMでございます。データSIMでも、SMSつき・SMSなしのものがございます。現行法令上、義務づけがなされていないような形となっておりますが、一部の事業者においては、自主的な取組として、音声SIMと同等の方式で本人確認がなされているところでございます。警察庁の調査、後ほどございますけれども、データSIMを

悪用した犯罪事例などが複数報告されております。特にSMSつきデータSIMについては、詐欺を行う際に、SNSなどのアカウントをつくるための２段階認証に使用されているケースがあるということを伺っております。こうしたことを踏まえまして、データSIMについてどのような対策を講じていけばいいかというところで、犯罪実態ですとか訪日外国人の利用実態、また、先ほど申しましたSMSつき・なしの部分も含めて、ここに記載の論点も含めて御議論いただければと思っております。

事務局からは以上でございます。

【大谷主査】　御説明ありがとうございました。続きまして、警察庁の方から御説明をお願いいたします。

【警察庁(根本)】　データSIMの悪用実態について、資料に沿って説明をさせていただきます。

まず、悪用事例の１つ目として、ニュース等でも多く取り上げられております、大手モバイルキャリアを舞台としたSIMの不正発行事案について紹介をいたします。

被疑者は、SIM発行時の本人確認を一部省略できるサービスを狙い、そのサービスの正規利用者アカウントへ不正ログインをした上で、容易にeSIMを発行し、第三者へそれを売却していたものであります。

音声SIMの所持や金融系サービスの契約有無に応じて、過去の本人確認情報に変更がないことを前提にSIM発行をすることができていたというものであります。

不正アクセスというハードルはあるものの、ID・パスワードのみの簡易な認証であり、非対面で、本人確認手続きの一部を省略してSIMが発行できるという手軽さから狙われたものであります。

この事例のポイントとしては大きく２つあり、まず１点目が、不正に入手したアカウントの本来の所有者が音声SIMを所持している、または金融サービスにおける本人確認が済んでいる場合には、SIM契約時に改めて新規契約時と同等の本人確認が行われていなかったということ。

２点目には、アカウントにはID・パスワードのみでログインでき、SIM契約時にも追加認証等が行われていなかったということが挙げられます。

被疑者らは、他人のID・パスワードの組を30億件ほど所有しており、事業者においては、ID・パスワードは漏れているという前提でセキュリティーを意識したサービス設計が必要不可欠であると言えることでしょう。契約時における都度の本人確認や、追加の認証のい

ずれかでも行われていれば、被害を防ぐことができたのではないかと考えております。

実際に不正に取得されたSIMについては、秘匿性の高いSNSで販売されており、それを購入した別の被疑者がチケット詐欺を行っていたことも確認されております。

続いて、悪用事例の２つ目として、SMSつきデータSIMの契約時の本人確認がなされていなかった事例について、紹介をいたします。

この事例は、オンラインフリーマーケットサイト上で行われた、他人名義のクレジットカードの現金化事件であります。架空出品役のアカウントにひもづく電話番号は、本人確認を行っていない事業者にて販売されたSMSつきデータSIMであり、番号利用者の特定には至っておりません。代理決済役のみ別件で身元が判明し、検挙しております。

こちらのスライドの図に記載しておりますとおり、この事案では、指示役、架空出品役、代理決済役の３者が登場し、指示役を頂点として、他人名義のクレジットカードの不正利用が行われております。

まず、指示役は架空出品役に対し、フリマサイト上で架空出品するように指示を行い、代理決済役には他人名義のクレジットカードを用いて、架空出品された商品を購入するよう指示しております。架空出品役、代理決済役はそれぞれフリマサイトのアカウントを利用しています。アカウントにひもづくSIMに関して照会を行った結果、当該SIMは、本人確認を行っていない事業者によって販売されたSMSつきデータSIMであり、身元の特定には至らなかったものであります。

悪用事例の３つ目は、データSIMの契約時に本人確認がなされなかった事例であります。

他人名義のクレジットカード利用時において、架空の契約者情報で契約をした、SMS機能がないデータSIMを使用していた事件となります。

被疑者は、飲食店予約サイトにて、他人名義のクレジットカードを用いて金券を購入し、同金券を利用し、複数の店舗にて飲食を行っています。ほかにも、ホテルの予約、宿泊においてもクレジットカードの不正利用を行ったものであります。

被疑者は、このクレジットカードの不正利用を行う際に、SMS機能がないデータSIMを用いた通信を行っていましたが、照会の結果、契約時の本人確認は行われておらず、架空の契約者情報が登録されていることが判明しております。

悪用事例の４つ目は、契約時の本人確認が不十分だった事例で、ある不正送金未遂事件から発覚した、銀行口座の不正売買に関する事件となります。

スライドの図に沿って事件の概要を説明いたします。被害者Aのインターネットバンキ

ングアカウントが乗っ取られ、A口座からB口座へ不正送金する手続がなされましたが、B口座については既に凍結されており、着金には至らなかったというものであります。

不正送金に使われたB口座は、口座の持ち主から、SNSを通じて知り合った被疑者Zへ譲渡されていたことが判明しております。被疑者ZのSNSアカウントに関する差押え結果により、同アカウントにひもづく電話番号はSIM１とSIM２の２つであることが判明しております。２つのSIMに対して照会を行った結果、SIM２に関しては少なくとも４事業者を経ており、照会途中の事業者と連絡がつかない状況であり、また、SIM１については、被疑者Zと別名義の被疑者Bの名義で契約をされていたことが判明しております。

SIM１の販売事業者からは、契約は全てインターネット上で完結できるため、他人の身分証を用いて契約をされても当社では分からない、インターネットで契約の申込みを受けた際のログやIPアドレス等は残存しておらず、提出は不可能である、との回答があったほか、被疑者Bからは、SNSを通じて知り合った人物から事業の話を持ちかけられ、預金口座情報や本人確認書類の画像を送ったことがあるとの供述が得られております。

悪意者Fが、被疑者Bに成り済ましてSIM１を契約していたことが推認されております。結果として、同一人物または同一のグループ等に思料される被疑者Z、悪意者Fについては特定に至っておりません。

続いて、契約時の本人確認が決め手となって検挙に至った事例についても紹介をいたします。この事例は、ゲームアカウント売買サイトへの不正アクセス事件となります。図に沿って、事件概要について御説明をいたします。

不正アクセス者Zは、ゲームアカウント売買サイト上において、取引に関するやり取りの中で、正規利用者Aをフィッシングサイトへ誘導し、正規利用者AのID・パスワードを窃取しております。さらに、窃取した正規利用者AのID・パスワードを悪用して、Aのアカウントへ不正ログインを行い、アカウント内に保有されていた売上金等を窃取しております。

このZが使用していたアカウントにひもづく電話番号を照会するとYが浮上し、事情を聴取するとSMS認証代行を行っていたことが判明しております。この事例では、契約時の本人確認が決め手となり、SMS認証代行者Yを検挙しております。

次のスライドは、これまで紹介した事例等も含め、データSIMの悪用の際に見られる傾向をまとめた概要図となります。

悪用されたデータSIMについて照会を行うと、実際に消費者へ販売を行った事業者にたどり着くまでに、幾つもの事業者を経由している場合があります。こういったケースにお

いて、本人確認を行うのは実際に消費者へ販売を行う事業者であり、ここでは、本人確認をしていないケース、偽造または第三者の本人確認資料で本人確認されていたケース、つまりは本人確認が甘かったケースであります。さらに、１人に対して大量のSIMを販売していたケースを確認しております。

このような、厳格な本人確認がなされずに契約されたSMSつきデータSIMは、決済サービスやSNSアカウントを作成する際のSMS認証に使われ、そのアカウントが特殊詐欺をはじめとする各種犯罪に悪用されている傾向が見られております。

また、SMSがないデータ通信SIMについては、クレジットカードの不正利用時や不正アクセス行為時の通信に悪用されている傾向が見られております。

このように、１つでも本人確認が厳格でない事業者が存在していると、悪意者によって狙われ、追跡が困難になることに加え、複数の事業者に対して照会をかけなければいけないことから、照会の長期化にもなり、結果的に被疑者の隠匿につながってしまうものと考えております。

本日は、データSIMの悪用事例について紹介をいたしました。既に、MNO４社をはじめMVNO事業者にて自主的な本人確認の取組を推進いただいているところではありますが、本日紹介した事例等からも、セキュリティーの常として、本人確認の甘いところが狙われているところが見えております。

今後、音声SIMの契約時本人確認がマイナンバーカード等のICチップ読み取り方式に義務化された場合、ますます本人確認義務のないデータSIMの悪用に移行していくものと考えております。そうなってしまう前の手だてとして、法規制をすべきであるものと考えております。

警察としましては、引き続きこうした犯罪の捜査、被疑者の検挙を進めてまいりますが、その中でも重要な事後追跡性の確保のため、本人確認の強化についてぜひ御検討いただければ幸いであります。

私からの説明は以上となります。本日は貴重なお時間をいただきまして、ありがとうございました。

【大谷主査】　根本様、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、御質問がある方は、チャット欄などを御活用いただければと思います。よろしくお願いいたします。

【辻構成員】　昨年のワーキングでは大変お世話になりました。情報セキュリティ大学

院大学の辻と申します。これだけ問題が発生していると認識しているんですけれども、やはりポイントとしては、本人確認をそろそろもう少しちゃんとすべきではないかというところです。

２つ、厳密な本人確認を電子的に行うべきではないかということと、今回の諸問題、個別にコメントをさせていただくこともできるんですけれども、やはりポイントとしては、定期的に行うことも必要になってくる。例えば１年に１回とか、定期的にそういったことを行う必要があるんじゃないかと思っております。

前もお話しさせていただいているとおり、マイナンバーカードの機能をスマートフォンに搭載する検討会も出させていただいているんですけれども、そこでは本人確認のレベルについて、かなり厳密に精緻に議論をさせていただいております。これはNIST、米国立標準技術研究所のSP800-63に、身元確認レベルIALと当人認証保証レベルAALというものがあって、これを適切にレベル合わせして認証していかなければ本人確認は意味がないということで、もちろん、本日出てきました諸問題は、運用や啓蒙で対応できる部分はもちろんあると思うんですけれども、結果すごく手間がかかることであって、そこを補う形で電子的かつ厳密な方法をうまく組み合わせていくことが必要なのではないか。

そういった観点において、マイナンバーの活用、スマホ搭載自体も既にAndroidでは先行しておりますけれども、今年iPhoneに関しても搭載されて、両方が利用できることになりますので、例えばそういった連携も含めて検討していく必要があるのではないかなと思っております。

最初の資料についてもコメントしてよろしいでしょうか。

【大谷主査】　今は、警察庁様のプレゼンに対する質疑の時間とし、また、議論については時間を設けたいと思っておりますので、コメントは後ほどお願いします。

【辻構成員】　分かりました。後ほど質問させていただければと思います。

【大谷主査】　貴重なコメントありがとうございました。

ほかにいらっしゃいますでしょうか。

私が１点、６ページで、自然人に大量にデータ通信SIMを発行しているという、この「大量」というのは大体どのぐらいの枚数のことをおっしゃっているのか、教えていただけるとありがたいです。

【警察庁（根本）】　大量に発行されているについては、正確な数はありませんが、1,000とかそういったオーダーの程度で大量に発行されているものと把握をしております。

【大谷主査】　ありがとうございます。自然人に対して1,000オーダーということですね。

かなりクリアな御説明をいただいておりますので、また後ほど、何か出てきましたら、その関連で御質問を承ることにしたいと思います。

では、続きまして、事業者様からお願いしたいと思います。ドコモ様から、各８分ずつ、御説明をいただければと思います。よろしくお願いいたします。

【NTTドコモ（大橋）】　NTTドコモの大橋でございます。それでは、資料７－３に基づきまして、当社の御説明を差し上げます。

１ページ目、まず、基本的な考えでございます。当社は、公共性の高い携帯電話サービスを提供する事業者として、様々な法律の規律を遵守しております。特に迷惑SMS・メール対策、並びに携帯電話の本人確認については厳格な運用を行っておりまして、特殊詐欺の防止、不正利用の対策に取り組んでいるところでございます。

昨今の特殊詐欺の状況から、不正利用対策に有効な規律の見直しというのは実施すべきと考えておりますが、一部、利用者の利便性とのトレードオフとなる部分もございますので、関係者の意見を十分に踏まえた上で検討いただければと考えております。

当社におきましては、規律を厳格に守っておりまして、加えて、業界団体の自主基準を踏まえて自主的なルールを定めて運用しておりまして、規律の見直しを行った場合でも大きな影響は想定をしていないところでございます。

なお、規律の見直しに当たりましては、システムの開発などを要するケースがございますので、十分な移行期間の確保をお願いしたいと考えております。

以下、各論点について御説明申し上げます。

まず、SIMの不正転売でございます。SIMの不正転売については、見た目上は正当な申込みの要件が揃っておりますので、店頭で発見して抑止することが非常に難しい状況になってございます。

それを踏まえまして、基本的には周知の啓発、並びに不正転売を難しくする仕組みの導入の双方の対策の検討が必要と考えております。

周知啓発につきましては、次のページでお示ししているような形で、当社において注意喚起を行っておりますが、業界団体や関係省庁も連携した取組が必要と考えております。

転売を難しくする仕組みとしましては、与信時の強化が考え得るかと思っております。こちらにおいては、最近実施した事例を例示させていただいているところでございます。

続きまして、法人の代理権に関するものでございます。当社においては、委任状において来店者が代理権を有することの確認、又は名刺もしくは社員証により来店者の在籍確認を実施しているところであります。

法人営業においては、基本的に営業担当者が会社の事業所を訪問して手続を行いますので、不正契約の可能性はそれほど高くないと考えております。従いまして、来店者に求められる書類が分かりづらいといった問題も、基本的に発生はしないと思っております。

一方で、営業担当がついていないお客様については、ドコモショップなど店頭での対応となりますので、この部分について一定統一することは考え得るかと思っております。

続いて３点目でございます。他社の本人確認結果への依拠になります。

当社においては、依拠による本人確認は現状実施しておりません。また、当社において、本人確認においては、先ほども言及がございましたが、NISTのガイドラインを参考に、身元確認、本人認証において独自ガイドラインの策定をしております。また、その後もフィッシング被害の発生状況などに応じて、各手続において対応レベルを常に見直しをしているところであります。

こちらが、最近の取組事例を掲げたものとなってございます。

それを踏まえて、他社の本人確認結果への依拠につきましては、依拠先の本人確認、並びに契約者の同一性確認が適切に行われていない場合には、成り済ましのリスクが非常に想定されますので、慎重な検討が必要であると考えております。

そのため、依拠先における適切な本人確認や本人確認記録の最新化の担保や、依拠元における適切な本人同一性確認について、適切な方法が実現可能か十分に検討した上で、依拠を実施するかを決めていく必要があると考えております。

参考までに後ろに記載しておりますが、本人確認は身元確認と当人認証とフェデレーションという３つの要素から成立しておりまして、デジタル庁の本人確認ガイドライン検討の会議において取りまとめの案が示されているところでございます。こちらはまだ確定したものではありませんが、基本的にこちらに則った形でレベルなどを定めていくことが望ましいと考えております。

続いて４点目、追加確認の本人確認でございます。

当社においては、追加回線においても１回線目と同様の本人確認を実施しております。一部例外として、AppleWatchに代表されるようなウェアラブルデバイスをウェブサイトにおいて手続する場合において、ID・パスワード等による本人確認を行っているところでご

ざいます。これらのケースにおいては、厳格な本人確認を行うことが、ウェアラブルデバイスの付け外しの都度必要になるなど、お客様利便性に影響がある可能性もありますので、例外を考えるのも一つの案かと思っております。

その場合においても、当人認証のレベルをより明確に定めた上で、さらに不正契約の発生のモニタリングなどを実施する前提とすることが考え得るかと考えております。

５点目でございます。上限契約の台数でございます。

当社はTCAの実施基準に則りまして、個人名義における音声SIMの上限契約台数を５台と定めております。また、それを準用しまして、データSIM並びに先ほどのウェアラブルデバイスについても上限台数を定めているところでございます。

これらの上限台数のルール化を行う場合には、TCAの自主基準を踏まえたルールとすることが考え得るかと思っております。

自主基準を拡充したり厳しくすることも考え得るものでありますが、あくまでこれは業界団体の自主基準でありますので、制度的担保とはならない可能性がございます。それを踏まえてルールを考える必要があると考えております。

また、ルール化を行う場合、例えば世帯主が家族全員分を契約者となって契約しているケースにおいて、契約ができなくなるケースも一定発生し得ることから、十分な移行期間をお願いしたいと考えております。

６点目でございます。データSIMの本人確認でございます。

当社では現状、TCAの実施基準に則り、音声契約と同一の本人確認を実施しているところでございます。データSIMは現状、本人確認義務の対象外でありますが、これを用いて固定IP電話の転送役務などを使った詐欺も十分考え得るところでありますので、規律の強化は一定の効果が見込まれると考えております。

仮に実施する場合には、MVNOなど関係事業者の意見も踏まえて、システム対応の期間なども踏まえた検討が必要と考えているところでございます。

また、データSIMにつきましては、IoTの利用や訪日外国人が一時的に利用するケースなど、利用用途が多岐に渡りますので、利便性と犯罪の悪用可能性とのバランスを考慮しながら検討いただくことが必要であると考えております。

最後に、SMS機能がついているかどうかによって区別する必要は、特にないと考えているところでございます。

当社からの説明は以上でございます。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。コンパクト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、次にKDDI様から御説明お願いしたいと思います。

【KDDI（山本）】　KDDIの山本です。それでは、資料７－４で説明させていただきます。

本日の御説明事項、６点ございますが、一つ一つ御説明してまいります。

スライドの２を御覧ください。まず、SIMの不正転売に対する取組事例でございます。

こちらは、新規契約締結の際に、お客様に対して周知活動を継続して実施しております。

左側にお示ししておりますのが、店頭のポップでございます。特に、他人あるいは第三者に無断で貸す、これは転売と書いてありますけれども、実際には売るというよりも勝手に使わせてしまう、こういったものが犯罪によく巻き込まれる、学生さんが巻き込まれるようなことを防ぐためにも、周知活動をしっかりと徹底してまいりたいと考えております。

続きまして、スライドの３をお願いします。こちらは法人の代理権でございます。犯罪等の情勢を踏まえつつ、厳格な審査に加えて、適切な追加的確認書類について、引き続き検討してまいりたいと考えております。

絵でお示ししたのは、左側は法人としての確認、いわゆる登記簿謄本、それから印鑑証明書など、それから真ん中が来店者としての本人確認、マイナンバーカード、運転免許証など、こちらは現行法令、不正利用防止法等で求められている対応に加えて、一番右側、こちらは法人と来店者との関係性を結びつけるものとして、名刺ですとかあるいは社員証といったものを、自主的な取組として加えているところでございます。

続きまして、スライドの４を御覧ください。こちらは、他社の本人確認結果への依拠にでございます。

携帯電話の本人確認というのは、これは強化が行われる状況、保証レベルを上げるべきだという議論をされているところでございます。こちらはワーキンググループの報告書にもある通りです。左が、オンライン、非対面ですね、それから右側は対面、これは店頭でございますが、いずれも本人確認の強化が求められるところでございます。

こういった状況におきましては、他の事業者への依拠を認めることは、現時点では適当ではないというふうに考えております。まずは現状の方向性を踏まえて、本人確認強化の取組というのを実施すべきであると考えております。

続きまして、スライドの５、お願いいたします。これは追加回線の本人確認でございます。

追加回線につきましては、現行の簡易な方式、これを残しつつ、ID・パスワードだけでは十分とは言えませんので、それ以外の方法を実施する必要があると考えております。

表に書いてありますのは、こちらもワーキンググループの報告書で引用されているところでございますが、こういった認証レベルも踏まえながら、特に多要素認証などの適切な確認が求められると考えております。

続きまして、スライドの６を御覧ください。こちらは上限契約台数についてでございます。

上限契約台数については、一定の制限は必要と考えます。これは先ほどドコモさんからもお話がありましたとおり、弊社も音声SIMについては５台というふうにしております。

一方で、新たなサービス提供の妨げとならないように、犯罪等の情勢を踏まえて、例外措置等の検討が必要になると考えております。

こちらはお示ししている例でございますが、例えばお子様向けの見守りGPS端末、あるいはIoTといった、いわゆる通話ではない、通話先が限定しているサービスなど、特にデータ通信のサービスなどは、不正利用のリスクが少ないと考えられますので、例外措置とすべきではないかと考えております。

同じような議論になりますが、続いてスライドの７、これはデータSIMの本人確認でございます。データ通信利用が増えている情勢を踏まえまして、規制の在り方というのは、ニーズと実際の犯罪事例と、リスク対策のバランスで検討していただきたいと考えます。

左側の例は、訪日外国人向けでございます。真ん中は先ほどと同じIoT、あるいは右側は急なリモート会議とか、様々なニーズが想定されます。特に契約期間が一定期間に設定されるような訪日外国人向けサービス、その他通信先が限定的なサービス、先ほども申し上げましたIoTなど、こういったSMSが使えないサービスなどは、例外措置とすべきではないかと考えております。

弊社からの御説明は以上になります。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。コンパクトな御説明ありがとうございます。

それでは、続きましてソフトバンク様、お願いします。

【ソフトバンク（山田）】　ソフトバンクの山田です。それでは、資料７－５に沿って御説明いたします。

まず、当社の基本的な考えでございますけれども、やはり特殊詐欺等の各種犯罪に関しましては、事業者としても重大な社会問題と認識しておりますので、こちらにつきまして

はしっかり対応していきたいと思っております。

その際に、不適正利用の防止に向けての対策ですけれども、もちろん携帯電話契約時の本人確認の強化というのも、当然大事なことだと思いますけれども、先日の犯罪対策閣僚会議でも示されたとおり、このような形で、利用者であるとかSNS事業者を含む、各方面からの対策が必要と考えております。

当社に関しましても、契約時の本人確認に関する関係法令や業界自主ルールの遵守というのはもちろんやっているところではあるんですけれども、それ以外にも、利用者のリテラシー向上に向けた各種取組ということで、こういった様々な活動は継続的に実施したいと考えております。

これから携帯電話の本人確認のルールの管理について、当社の考えを御説明いたします。

まず、不正利用防止法等、業界の自主ルールでございますけれども、こちらは不適正利用の防止、具体的には契約の匿名性の排除であるとか事後追跡性の確保のために、手口に合わせて、民民の契約において足りない部分を補完してきた認識でございます。

例えば、法令や業界自主ルールで定められている事例として、犯罪利用の可能性のある回線の停止、こちらは現在でも、警察署長からの求めがあり、契約者確認が取れない場合には、事業者として回線を止めることができますけれども、このような話。

あと、今でも、数は少なくなりましたが販売しておりますプリペイド携帯、こちらも販売当初は、もともとプリペイドというのが前払いなものですから、与信の観点からすると、事業者からすると別に本人確認というのは必要性はなかった。ただ、やはりそれが様々な犯罪利用にも使われるということで、与信の観点で問題がないとしても、しっかりと契約者の確認が必要だよねということで法令ができたという理解でおります。

３つ目は、データ回線における本人確認ということで、こちらは先ほどドコモ様のほうから御説明がありましたとおり、TCAではデータ回線について音声と同等の契約者確認をするということになっていますけれども、こちらも、かつてクレジットカードのみで本人確認を行ってデータ回線の開通を行っていたのが、様々な犯罪につながったといったところから、そのようなものが設けられた認識でおります。

したがいまして、事業者は、法令によらずとも、もともと与信の観点から、本人確認というのは行う必要があるというのが前提にございます。一方で、犯罪の手口というのが様々変遷し、多様化したりということもございますので、私どもとしましては、ルールを設けるということは、必要性がある場合にはそれは入れるべきかなと思うんですけれども、

基本的には業界自主ルールでの対応というのを基本として、法令による規律というのは最小限にすべきではないかと考えております。

このような考え方にのっとりまして、個別の論点について御説明させていただきますと、まず、１つ目のSIMの不正転売につきましては、やはり第一に、SIMの無断譲渡というのが現状でも不正利用防止法に反する行為であるということの周知徹底も、改めて必要かと考えております。

加えまして、総務省様の資料にあるような、犯罪利用可能性のある利用者の情報交換といったものも対策案の一つと考えますけれども、このような場合には、警察庁様からの提供情報の正確性の確保であるとか、または、それを正とした場合の対応ですね、その時に、事業者側としては当然ながら免責されると、そういった手だてが必要ではないかと考えております。

次に、法人の代理権、法人の本人確認ですけれども、こちらも結局のところ、各事業者が法人との関係性を確認しているというのは、やはり与信の観点から必要なため入れているものであり、そのような意味で一定の対策というのは講じられているのではないかと考えております。

したがいまして、私どもとしてはこの辺り、法令での要件追加というのは不要と考えますし、各事業者において必要書類が異なるという点も、これは与信に関する各社の考え方によるところでございますので、法令等での統一化というところまでを図る必要はないのではないかなと考えております。

次に、他社への本人確認結果の依拠でございますけれども、こちらは仮に依拠を許容するということであれば、本ワーキンググループの報告書にも以下のような記載がございますので、仮にそのような検討をする場合には、やはり依拠先としては公的個人認証を行っている事業者に限定するというのが、検討の前提になるのかなと考えております。

一枚めくりまして、次に追加回線についてでございますけれども、追加回線の本人確認につきましては、２回線目以降の回線契約時の本人確認について、要件が１回線目と異なっているというのは、やはり利便性であるとか、そういった観点から一定の合理性があるのではないかと考えております。

ただ一方で、今次の犯罪事案として、ID・パスの詐取による不正契約事案というのが実際に発生している以上は、ID・パスのみに頼るのではなくて、既存回線でのログインの必須化であるとか、ワンタイムパスワードによる認証を取り入れる等、当人認証制を高める

という取組が必要なのかなと考えております。

続きまして、上限契約台数ですけれども、こちらにつきましては、まず第一にやはり本人確認の徹底、SIMの無断譲渡が違法であることの周知徹底、また、前ページにもありますとおり、２回線目以降の本人確認における当人認証制の強化というのが、まず第一に必要なのではないかなと考えております。

その上で、上限契約台数につきましては、我々としては、利用者の多様な利用用途に鑑みて、過度な制約を設けることはふさわしくないというのが基本的な考えでございます。

業界自主ルールのほか、各社が与信の観点から一定の制限を設けているというような実情を考慮しますと、現行以上の追加的な規律や、法令等による制度的な担保までは不要なのではないかなというふうに考えております。

最後にデータSIMでございますけれども、こちらにつきましては、当社は業界自主ルールの下、音声SIMと同等の本人確認を実施しており、今後もこの取組を継続してまいりたいと考えております。

弊社からの説明は以上です。ありがとうございました。

【大谷主査】　どうもありがとうございました。

それでは、続きまして、楽天モバイル様から御説明をいただきたいと思います。

【楽天モバイル（小田）】　楽天モバイル、小田でございます。楽天モバイルからの説明をさせていただきます。

資料７－６に従って御説明をさせていただきます。３ページ目でございます。

まず、SIMの不正転売についてでございます。当社におきましては、多く各社様とも被る部分はありますが、取組しておりますので御紹介させていただきます。

まず、重要事項説明書において、不正転売等を含む禁止行為について御説明しております。こういうものが法的に問題になります、あるいはルールとしてまずいですよというところを御説明しております。

その上で、その店頭契約に際しまして、スタッフとお客様とで、こういったポイントを含む重要事項説明書を読み合わせをしまして、お客様に個別確認でチェックをいただきまして、最終的にお客様に署名をしていただくということで、お客様の意識づけを行っております。

その上で、これも他社様にもございましたが、SIMの送付時には外装に啓発のシールを貼りまして、受領後に第三者に転送するですとか転売する行為等は犯罪になりますよとい

うことを、利用者に対して啓発しているという取組を行っております。

次のページをお願いします。法人の代理権についてでございます。

当社におきましても、法人に関しまして、契約受付する際には通常の法的に定められた法人の確認書類に加えまして、担当者の代理権の有無を確認するという取組をしておりまして、具体的にはこの③番に記載しております、担当者の方がその会社に所属していると確認できる名刺、あるいは社員証、健康保険証、または在籍を証明する何らかの書類ということで、いずれかを示していただくということで実際の運用を行ってございます。

次お願いします。３番目の、他社の本人確認結果への依拠でございます。

この１月に開催されました親会で、総務省様から公表された資料の中にありました内容を踏まえまして、継続的顧客管理、いわゆる犯収法で行われているものですけれども、こういった継続的顧客管理と多要素認証、具体的にはSMS認証ですとか利用者証明書、電子証明書等があるかと思うんですけど、そういったものによりまして身元確認、それから当人認証の保証レベルを担保できると考えてございます。

こういった過去の本人確認結果への依拠につきましては、金融機関への依拠、それから携帯電話事業者への依拠、いずれにつきましても、この継続的顧客管理、それから多要素認証等の取組によって、身元確認及び当人認証の保証レベルを担保しまして、それと併せて消費者の方々の利便も向上が見込まれるということで、ぜひ早期に実現いただきたいというふうに当社は考えてございます。

これは親会の資料の転用でございます。

次、４番の、追加回線の本人確認でございます。追加回線の本人確認においては、現行法令に基づく対応に加えまして、当社におきましては不正事案が発生したこともございますので、先ほど警察庁の方からも、追加認証を行うことでこの事案は防げたんじゃないかといったコメントもありましたけれども、そういった反省から、多要素認証等を追加実施する等によって当人認証レベルを高めるということが必要であると考えております。

つきましては、当社は現在どうしているかというところなんですけども、今までやっていた既契約者の本人確認情報に変更がないことを前提に、法令で定めている楽天のID・パスワードの認証、それから本人確認情報の再提示に加えまして、既に契約した番号へのSMSに通知するということ、それからワンタイムパスワード認証を実施することで、さらなる不正抑止を行います。

それから、これも他社様からもありましたけれども、AppleWatchのファミリー共有とい

うサービスを提供しておりまして、このサービスにおきましても、音声SIMと同様にということで、申込みされた方が当社の既契約者である場合には、ID・パスワード認証、それから本人確認情報の提示に加えまして、端末のカメラを使いました所持確認ということで、本人確認を実施してございます。

上限契約台数についてでございます。８ページ目です。

そういう意味では、契約台数の上限を設定するということでなく、先ほどから申し上げている多要素認証等によりまして、当人認証をしっかりしていく、強化していくことで不正契約自体を抑止するという取組がまずは重要だろうと、当社はそのように考えてございます。

データSIMでございます。９ページ目でございます。

当社が提供するデータSIMの取組について御紹介させていただきます。当社が提供するデータSIMについては、SMSつきのみを提供しておるんですけれども、これにつきましては、楽天カードという当社グループの金融機関が発行するクレジットカード、これをお持ちの方のみが契約できるという仕組みにしてございます。この方々の信用履歴を活用することで、犯収法に準ずる本人確認の実施ということで取り組んでございます。

データSIMにおける追加回線につきましては、先ほどとも重複しますけれども、既契約回線へのSMS通知ですとか、ワンタイムパスワード認証等を実施してございます。

今後のデータSIMの利活用について、３点目に述べさせていただいております。データSIMにつきましては、現状、訪日の外国人の方々に加えまして、様々な利用者ニーズに応えているものというふうに考えてございます。また、IoT機器での活用等、イノベーションを通じた日本の国際競争力強化にも、今後も引き続き貢献し得るものというふうに考えてございます。よって、これらの機会損失を招くことがないよう、御配慮いただきたく考えております。

弊社からの御説明は以上でございます。

【大谷主査】　御説明ありがとうございました。

それでは、続きまして、テレコムサービス協会のMVNO委員会から御説明をお願いしたいと思います。

【MVNO委員会（井原）】　MVNO委員会、井原でございます。それでは、資料７－７に基づきまして、MVNO委員会としての意見、及び個社の取組について説明させていただきます。

なお、MVNOは個社単位での取組内容が様々であるため、個社の取組については、一部

MVNOの取組となっております。

それでは、２ページを御覧ください。まず、SIMの不正転売でございます。

皆様からもあったとおり、申込み手続の段階で不正転売かどうかということを検知することは極めて困難だと考えます。そのため、広く周知・啓発していくことが重要かと考えております。

なお、個社の対応としまして、SIMカードの配送時に、無断譲渡の違法性についての説明書面を同封するなど、契約者への理解促進を図っているMVNOもあり、実際この書面の結果、契約者より問合せをいただくことで、不正譲渡を事前に防ぐなどの効果を上げている場合もございます。

３ページを御覧ください。法人代理権についてでございます。

MVNO委員会では毎月、消費者問題分科会を開催しておりまして、個人の契約に関する各種課題については議論しているところですが、法人契約に関する課題については、まだまだ議論できていない状況でございます。

つきましては、犯罪実態や各種ニーズを踏まえて御検討いただき、見直しとなる場合には十分な準備期間を確保いただければと考えます。

なお、個社の取組としまして、一部の事業者では、法人担当者の名刺や社員証等の提示により、社員であるかの確認を実施してございます。

４ページを御覧ください。依拠についてでございます。

他社の本人確認の結果への依拠については、メリットと不正契約等の諸課題を踏まえた慎重な議論を必要と考えております。

なお、過去、MVNO委員会内で依拠に関するアンケートを実施しましたが、現状、取組を実施もしくは検討している事業者はございませんでした。

５ページを御覧ください。追加回線についてです。

個人契約においては、利便性の観点から省令上の簡易な方法を維持しつつ、ID・パス入力時の多要素認証等により、当人認証レベルを高めていく必要があるものと考えます。

また、MVNO委員会内で追加回線に関するアンケートを実施させていただいて、11社より回答いただきました。回答いただいた11社は、２回線目以降の契約についても、１回線目と同様の本人確認手続を実施しております。

続きまして、６ページを御覧ください。上限契約台数でございます。

IoT等での利用拡大など、今後モバイル通信サービスは多様化することが想定されると

ころから、契約台数の上限規制は、イノベーションの阻害が強く懸念されているところでございます。現行のとおり、自主的な業界ルール等を踏まえた、各事業者における不正利用対策の考え方に委ねたほうがよいのではないかと考えております。

なお、上限台数についても、MVNO委員会でアンケートを実施しました。結果は、事業者ごとに上限数というのは異なっておりまして、２回線から10回線が上限となっておりました。

最後、７ページを御覧ください。データSIMの本人確認についてです。

MVNO委員会として、いわゆるデータSIMについて、不正利用等の実態は現状把握できていない状況でございます。また、データSIMは、IoT機器や訪日外国人向けのプリペイドSIMなどにも利用されており、本人確認を義務づける場合は利便性を大きく損なうこととなるため、本人確認を義務づけるべきではなく、自主ルールによる本人確認の徹底が望ましいのではないかと考えております。

なお、MVNO委員会では、業界の自主的な取組としまして、SMSつきデータSIMについて音声サービスと同様の本人確認手続を推進しており、本年３月末時点で24社が実施しております。

また、SMS機能なしのデータ専用SIMについても、８社が音声と同様の本人確認手続を実施している状況でございます。

MVNO委員会からの説明は以上でございます。

【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、ただいまの各事業者様からの御説明につきまして、質問等を受け付けたいと思います。チャット欄に、希望者は書き込みをお願いいたします。御質問などいかがでしょうか。

では、仲上構成員、よろしくお願いいたします。

【仲上構成員】　日本スマートフォンセキュリティ協会技術部会の仲上と申します。本日は各社、丁寧な御説明をいただきましてありがとうございました。

質問させていただきたいところは、訪日外国人向けのサービス提供の際に、通常のSIMサービスと、日本の国内でもデータSIMの販売をされているかと思うんですけれども、訪日外国人向けのサービスで差がある部分というのはあるのでしょうかというところと、実際に本人確認をやるとしたら、訪日外国人の方なので当然パスポートはお持ちかと思うんですけど、パスポートの認証になるということですと、例えば空港等で見かけるような自

動販売機でのSIMの販売等は難しくなるようなことが起こるのでしょうか。

この２点について、各社お聞かせいただければと思いました。

【大谷主査】　御質問ありがとうございます。

それでは、今の点について、各社から御回答をいただければと思います。

それでは、ドコモ様から順番にお願いします。

【NTTドコモ（大橋）】　NTTドコモでございます。当社においては訪日外国人向けのサービスを現状提供しておりませんので、いただいた質問に対しては、提供していないがお答えになるかと思います。

【KDDI（山本）】　KDDI、山本です。弊社の場合はpovo2.0という、povoというサービスで訪日外国人向けサービスを提供しております。これはデータ専用でございます。

こちらは上限最大90日間で契約期間を限定しているという形で、不正な利用につながらないように歯止めをかけております。

【大谷主査】　そうしますと今のお答えは、本人確認は特にしないでいらっしゃるということですね。

【KDDI（山本）】　そのとおりでございます。

【大谷主査】　ありがとうございます。

【ソフトバンク（山田）】　ソフトバンクの山田です。まず、当社の場合なんですけれども、訪日外国人向けのサービスとしては卸が中心になっておりますので、基本的に卸先の本人確認方法に委ねているというのが一つございます。

あと、細々と直接私どもがお客様に提供するものもあることはあるんですけれども、そちらにつきましては、まさに３点一致の本人確認を行って販売しております。

したがいまして、外国の方ですと、今の法令だと、たしか日本の居住地というか、ホテル住所とかでも可能というような形になっているかと思うんですけども、そのような形で本人確認を実施して、契約を締結しているという状況でございます。

【楽天モバイル（小田）】　楽天モバイルでございます。弊社におきましては、サービスとしては訪日外国人の方に特化したサービスは特段提供してございません。

一方で、特に中長期で滞在される方が、弊社の店頭で契約の御希望をいただくことがございまして、そういった場合には音声SIMを、本人確認実施の上で契約いただいております。

【MVNO委員会（井原）】　MVNO委員会、井原でございます。まず、訪日外国人向けのサ

ービスと通常のサービスの差なんですけども、一般的にはプリペイドで、訪日外国人の方向けにはプリペイドのサービスになるかと思いますので、これが通常のポストペイドと大きく違うところです。

あと、SIMの購入と契約手続とは別でして、SIMカード自体はプリペイドなのでまず購入ができて、利用する前に契約手続を行うということになりますので、購入者と利用者も異なる場合があるというところが、通常のSIMとは大きく違うところかと思っております。

あと、本人確認のところにつきましては、これは個社ごとに対応が異なるかと思いますので一般的になるんですけども、基本的には本人確認というのは行っていないかと思います。短期の利用ということが前提になりますので本人確認は行っていないのですが、もしこれ、本人確認を行う場合、そもそもどの時間帯で本人確認手続を行うかということにも影響してくるかと思います。日本に来られてすぐ御利用される場合でも、夜に着かれる場合、当然その審査等ができませんので、すぐ御利用いただけないとか、あとは来日前、実際に自国でアクティベートして来られるということも実際可能になってくるかと思いますが、その場合でも様々な手続方法が――様々といいますか、契約方法が様々かと思いますので、現状はこのような課題があるのではないかなと考えております。

【大谷主査】　個社別にいろいろあるところを、うまくまとめて御説明ありがとうございました。

【仲上構成員】　ありがとうございます。各社、使用的なところでの制約ですとか、そういったところで危険なところを回避しながら、利便性は確保しながら提供されているというところで理解いたしました。ありがとうございます。

【大谷主査】　ありがとうございます。

それでは、沢田構成員は質問ではなくコメントということですが、よろしくお願いいたします。

【沢田構成員】　ありがとうございます。丁寧な御説明、皆様ありがとうございました。

感想ですけれども、普通の個人ユーザーの視点で、本人確認、特に身元確認に関しまして、３、４、５、６に共通する、総論的なコメントをさせていただきたいと思いました。その中で質問もあります。

事業者さんの御説明の中で、消費者の利便性、ユーザーの利便性ということが何度か出てまいりました。普通の個人ユーザーは、携帯の契約とかデータ通信の契約とかをそんなに頻繁にするわけではないので、それほど気にしてくれなくてもいいかなというのが個人

的な感想です。マイナンバーカードとか証明書を搭載したスマホで身元確認してくれるのであれば、ユーザーとしても別にそんなに面倒くさくない、ストレスなく手続できるので、大いに活用していただいたほうがよいと思っています。

もちろん、マイナンバーカードをまだ持っていない方への配慮というのは必要かもしれません。現状では代替手段も用意せざるを得ないかもしれないとは思いつつ、基本的にはマイナンバーカード、公的個人認証で良いと思っています。

質問は、全員の事業者さんにということじゃなくても、特に御意見をお持ちの事業者さんでよいのですが、厳密にし過ぎた場合、公的個人認証にこだわった場合に、持っていない人への配慮を別にすると、どんなふうにユーザーの利便性が下がると危惧されるのか、もしお答えをお持ちの方がいらっしゃればお聞きしたいというのが１点目です。

今の質問は利便性の観点ですが、２点目は安心感という観点でして、ユーザーとしても、これだけ犯罪が出回っていることを考えると、ちゃんと本人確認してくれたほうが不安がないです。あまり簡単に通ってしまうと、なりすましも簡単にされるような気がするので、厳密にしていただいたほうがユーザーとしても安心するのではないかというのが２点目です。これは質問ではなくてコメントです。

以上２点、ありがとうございました。

【大谷主査】　ありがとうございます。利用者目線ということで御質問いただきました。

厳密に本人確認をした場合に利便性が損なわれるというのは、どのような形で利便性が損なわれるのかということについて危惧されているのか、お答えのある事業者からということなのですが、まず、ドコモ様からも利用者の利便性への御配慮が必要だという御説明があったかと思いますので、大橋さん、いかがでしょうか。

【NTTドコモ（大橋）】　ドコモでございます。当社においては、AppleWatchなどのウェアラブルデバイスは、AppleWatchにかかわらずほかの種類の物をつけることも一応可能となっていまして、１台当たりで課金されますので、腕につけるものが１台とすると、付け外しのことを考えると利便性に影響があるかもしれないと思います。

他方で、セルフィー型eKYCのケースですと、やはり何度も本人確認を行うのは煩雑かもしれませんが、JPKIのケースにおいては厳密な手続を毎回行うのもさほど利用者の負担にならないのではないかと思いますので、そのバランスを見ながら決めていただければ良いかと思っております。

【大谷主査】　ありがとうございました。

ほかの事業者様も、いかがでしょうか。

【ソフトバンク（山田）】　ソフトバンクの山田です。ありがとうございます。利便性という観点ですと、恐らく今回の場合、主に非対面、オンラインでの契約のことがほとんどだと思います。

対面で２回線目を契約するという場合には、そこでもう一回、基本的には本人確認の書類を出してもらいますのでこのようなものはなくて、恐らくネットを通じてもう１回線といったときに、先ほどドコモ様からありましたとおり、従来のeKYC等だといろいろとアップロードしたりとかということで、確かにそれは私も手間じゃないかなと思っています。

やはり様々なネット上でのショッピング等を含めて、契約というのがID・パス等、あとはワンタイムパスワード等で契約できるというのが結構一般的になっている中で、携帯についても追加回線をそれと同等で契約できたほうが、我々としては、お客様にとっても利便性というのはあるのかなというふうに思っているところではあります。

ただ一方で、特殊詐欺の部分というところは、当然ながらいろいろと問題になっているというところもございますので、その手口に照らしてみて、必要な手だてというのを業界で統一的にということであれば、そこは議論する余地というのは当然あると思いますし、そこには我々としてもしっかりと参画して、対応していきたいなというふうに考えております。

【楽天モバイル（小田）】　弊社からも、利用者の利便性の観点と、もう一つ競争の促進といいますか、業界全体の競争を促進することで、最終的に利用者にもメリットがあるというところの２点で御説明させていただきます。

１点目、まさに今ソフトバンクの山田さんからありましたように、利用者御自身、ふだん、今の本人確認のやり方で結構手間があるというところでございます。実際、画像をアップロードするという、現行の非対面でメインになっているやり方ですと、当社のほうでアクセスログ等を確認しましても、やはり一定の方、全てではないにしても、やはりふだん契約等をやり慣れていない方、それからデジタルのリテラシーが必ずしも得意じゃない方はちょっとためらってしまって、そこで結果的に、契約をやるのは別日にしようとか、やめてしまおうということが起こっていると見て取ってございます。

そういった意味で、今後JPKIの方法がメインになっていくとしても、そういったバリアを下げていく努力というのは、業界としてもしっかりやっていきたいなというふうに考えてございます。

２点目につきまして、スイッチング促進の観点ですと、JPKIで本人確認することで、同じ事業者を使い続ける分には機種変を繰り返していけばいいんですけれども、他事業者に移るというときには、再度本人確認が当然必要でして、ここをいかに簡易にしていくかというところは、スイッチング促進の観点が必要であると考えておりますし、逆に事業者間の競争が促進されることで、最終的に、料金それからサービスの面で消費者にメリットがあることでございますので、そういった観点でも、より簡易な本人確認方法の普及ということは必要ではないかなと。それがひいては利用者の利益につながっていくのかと考えてございます。

【MVNO委員会（井原）】　利便性の観点のところなんですけれども、スマートフォンを利用して本人確認を行う場合って、生体認証も活用できますので、生体認証を活用して、またJPKI等で本人確認ができますので、非常に安心な環境が間違いなく構築できるのか考えております。

一方で、この環境に関しては利用者が準備する必要がありまして、生体認証とかICの読み取りがまだできないスマートフォンもございますので、若干高価なスマートフォンを用意する必要があったりして、全員が御利用できる環境があるかというとまだまだそこには至っていないので、そのような問題は現状でも存在するのと考えております。

【KDDI（山本）】　ほとんど、もう出尽くしてしまっているので、繰り返しに近いところでございます。JPKIというのは、本人確認の方向性としてはそのとおりだと思います。

ただ、やはり実際は、これはJPKIだけではなくて、ICチップつきの本人確認書類を必要とする本人確認も含めてですけれども、お客様自身まだ十分そこについていけない方もいらっしゃるということもありますので、政府の周知も含めて、しっかりとそういった認証というものが普通に行われるようになるような、社会全体としての取組とセットで進めていただければと思います。

【大谷主査】　たくさん御回答いただきましてありがとうございました。

それで、沢田様、今の御回答で、利便性について御期待した回答があったということで大丈夫でしょうか。

【沢田構成員】　大体感じが分かりました。御丁寧に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。

それでは、鎮目構成員から御質問を承りたいと思います。

【鎮目構成員】　時間もあるかと思いますので簡単に。本日はどうも各社様、ありがと

うございました。

先ほど、データ専用SIMについての、訪日外国人についてどうかという御質問がありまして、私もその点が実は気になっていたのですが、もう１点はIoT機器の件なんですけれど、ドコモ様やソフトバンク様からは、データSIMについても現状、音声契約と同一方法で本人確認を実施されているというお話があったかと存じますけれど、これはIoT機器についても全く同じような対応を取っているのかということが、まず疑問としてございます。

IoT機器については、恐らくネットワークのカメラとかを想定しているのかなと思いますが、あと、このIoT機器向けに契約されたSIMというのは、これはeSIMではなくて物理的なデータSIMカードの場合、こちらは他の用途には流用はできないことになっているのかということを教えていただければと思います。

【大谷主査】　最初の御質問は、これはドコモ様でしたね。２つ目もよかったら一緒に答えていただけるとありがたいです。

【NTTドコモ（大橋）】　ドコモの大橋でございます。鎮目先生、御質問ありがとうございます。

まず、IoTにつきましては、個人、法人共に、音声と同様の本人確認を当社においては実施をしているところでございます。訪日外国人についてはサービス提供しておりませんので、先ほど御説明したとおりになります。

IoTで発行されたSIMが他の用途に利用できないか、については一概にそうとは言えないのですが、多くのケースにおいては流用できないことが多いかと思っております。特に法人向けの場合には、接続されるシステムを、インターネットではなくて閉域で直接つなぎに行く用途が非常に多いです。そのほうが外部からの攻撃を受けない観点で堅牢性がありますので、そうした場合には他の用途に流用することはできないとなります。

他方で、個人の方がIoTに通信を使う場合には、普通のインターネット接続とISPを使って通信をすることが一般的と思いますので、その場合にはスマートフォン等に接続をして、正しくAPNの設定などを行えば通信はできるのではないかと考えております。

【大谷主査】　鎮目構成員、質問への回答はよろしいですか。

【鎮目構成員】　ありがとうございます。どの範囲で本人確認をデータ専用SIMについて課すことが正当化されるのかということを考える上で、貴重な情報をいただくことができました。どうもありがとうございました。

【ソフトバンク（山田）】　すみません、ソフトバンクの山田です。当社もデータSIMを

やっていますというふうに書いていることについて、ちょっとコメントさせていただければと思いますが、よろしいでしょうか。

【大谷主査】　お願いします。

【ソフトバンク（山田）】　鎮目先生、御質問ありがとうございます。

まず、当社は、IoT向けは一部、本人確認を除外しているものが正直ございます。それは、ドコモ様の御説明からもございましたけれども、通信先が特定のセンターに限定されていてほかに流用できないであるとか、もしくは端末と完全に一体型になっているような形で、いずれにせよ一般的なデータ通信に流用できないものというのは、そこまでの必要性はないだろうということで本人確認を行っておりません。

なので逆に、外してほかに流用できる可能性があるというものは、基本的には本人確認を行っているというような形になっており、弊社の12ページの資料だと、丸くデータSIMでも本人確認を行っていますというふうに書いているんですけれども、一応そのような形で、一般的なインターネットが可能となるようなデータSIMについては、全て本人確認を行っているというふうに解釈いただければと思っております。

【鎮目構成員】　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。

それでは、ヒアリングを踏まえて全体の討議に入りたいと思いますけれども、皆様からコメントなどもいただきたいと思います。

中原構成員からは、これはコメントで大丈夫でしょうか。

【中原構成員】　全体についてのコメントです。論点が６つありましたけれど、それぞれについて雑駁な感想を述べさせていただきますと、まず、論点１の不正SIMの転売、バイトの応募者は、無断譲渡の違法性というのは、各事業者からかなり説明はされているものと思いますけれども、こういう無断譲渡の違法性の認識以前に、そもそもこれが闇バイトであるとか、犯罪に自分が巻き込まれているという認識自体が不足しているのではないかと思われます。

したがって、利用者への周知・啓発の強化は重要であるというのはもちろんですが、無断譲渡が違法ですよと、アルバイトも「業として」に当たる可能性があって罰せられる可能性がありますよということだけではなくて、闇バイトとしてこういうものがあって、無断譲渡するとこのように犯罪に使われる可能性があるし、それだけでなくて自分自身も経済的な不利益を被る可能性があってというような、想定されるストーリーを示すこと、そ

れから、万が一闇バイトに応募してしまっているとしても後戻りができると、そのための相談先なども具体的に示してあげるというのが理想なのではないかと思います。

もちろん、これを事業者だけでやるということではなくて、警察との連携などが必要になってくるのだと思いますけれども、全体としてそういう方向性を目指すべきなのではないかと思いました。

論点２の代理権ですけれども、「代理権」とあるものの、ここでの問題の所在というのは、民法上の法律行為の代理権の確保というよりは、法人の名をかたって不正な契約をするということの防止にあるのだと思います。

より具体的に言うと、来店者が当該法人のために携帯電話の契約を締結する権限があるか否かということよりも、その来店者が当該法人の関係者であるということの確認が本質なのではないかと思います。

したがって、民法的な意味での委任状、これを要求する事業者もあったようでありますけれども、これはもちろん契約の有効な締結のためには必要ですが、ここではそれよりも、その来店者が当該法人に在籍しているという事実を示す書類が決定的に重要なのではないか思いました。具体的な書類としては色々なものがあると思いますが、今申し上げたような問題の所在は確認しておくべきなのかなと思いました。

それから論点３について、この依拠の問題は、前期からの引き続きの検討課題であり、重要だと思いますけど、他の論点との対比でいうとやや異質というか、つまり規制を緩めていこうという方向での議論なので、位置づけとしては別建てで、検討の順番としては、不正への対応について十分に議論した上で、余裕がある限りにおいて検討するという位置づけがよいのではないかなと思いました。

それから、論点４から論点６について、これらをまとめてですけれども、２つありまして、１つは現状認識の問題でありまして、追加回線にせよ上限契約台数にせよデータSIMにせよ、一方で、先ほど沢田構成員のコメントにもあったところですが、２回線目以降の契約にも本人確認の書類の提示が要求されることでどれだけ利便性が阻害されるのか、契約台数の制限がどれだけ利便性が阻害されるのかといったようなこと、要するに、この文脈での「利便性の確保」がどれだけ切実なことなのかについての検証が必要であるように、私も思いました。

他方で、２回線目以降も簡単に契約できてしまう、あるいは無制限に何台でも契約できてしまうことがどれだけ犯罪に寄与しているかということについても、利用実態、複数回

線、多数台契約、データSIMとか、それぞれ具体的にどういうふうに使われているのかという利用実態があると思いますが、そのことを踏まえた検証が必要であるように思いました。過小な規制も過剰な規制も両方よくないことであると思いますので、こういう基礎的な現状認識をしっかりさせる必要があるように思いました。

それからもう一つ、規制の在り方で、今回お話を伺っていて、事業者の方々の中には、事業者の自主性に委ねるべきだという意見が多く出ていました。確かに、事業者としてはたくさん契約すればよいというわけではなくて、「与信」という言葉を使われていましたけど、その観点からおのずと制約が働いていくのだと思います。ただ、その結果が不正の抑止という観点から望ましいレベルと一致するのかどうかというのは、慎重に検討する必要があるんじゃないかと思います。

それから、当人認証の強化で十分であるというような御意見もたくさん出ていたと思います。確かに、物理的に契約を制限するというよりは、それぞれの契約が慎重にされるということであれば問題ないとも思いますが、ただ問題は、そういう当人認証の強化によって本当に十分な効果が生じるのかということでありまして、それぞれの論点に即して、丁寧にやはり検証する必要があるんじゃないかなと思いました。長くなりましたが以上です。

【大谷主査】　きめ細かくコメントをいただきましてありがとうございました。

続きまして、辻構成員からコメントをいただきたいと思います。

【辻構成員】　先ほどはタイミングを間違えてしまいまして申し訳ございませんでした。１番から６番について、改めてコメントさせていただきます。

特に警察庁からの発表を聞いて衝撃を受けたのは、最近、闇バイトということは非常に話題になっておりますけれども、思ったよりも不正というものが多いんだなということに驚かされております。

私は法律家でもないし業界団体でもないのですが、セキュリティーの専門家という立場において、やはりセキュリティーというのは弱いところが狙われると。どこか弱いところがあれば、そこから水が漏れるかのように狙われるというのがセキュリティーの弱点なんですけれども、もう一つ重要なところは、利便性とセキュリティーはバランスであるというところで、皆さんもよく存じ上げているかと思うんですが、今回感じたことはと利便性と言っていられない部分もあるなと思っておりまして、もちろん、先ほど中原先生がおっしゃった過剰規制、過小規制という言葉もあるかと思うんですけども、その過剰・過小という中で、ちょっと規制側にもう少し力を入れないと安全性の確保はだんだん難しくなっ

てくるんじゃないか。

昨年のこのワーキングをやっていたときに比べて状況は大分悪化しているというのは、あくまで私の所感ではあるんですけれども、本人確認の厳密化、厳密化は入り口だけでなく、それの定期的なチェックのようなものを行う必要が、やっぱりこれから出てくるのではないかと思います。

そういう意味でいうと、依拠という言葉もそうなんですが、レベルを合わせるということNISTのIALとAALのも含めまして、本人確認とは何ぞやというところを改めて定義する。

あと、先ほど業界団体ですとかそういう話もありましたけれども、業界団体ですと、その団体外の方が何かをしてしまうリスクもあるというところも考慮すると、やはりある程度は法律なりでしっかりしていく必要があるのではないかと思っております。

順番に１番からコメントさせていただきますと、SIMの不正転売に関しましても、これももう入り口だけでなく定期的な確認で、これは実際やろうと思うといろんな方法があると思うのですが、例えばJPKIを軸にしたものであれば、２クリックぐらいで確認って定期的にやれると思うんですよね。そういったことで転売されていないかというようなことを確認するような仕組みが必要になってくるんじゃないか。

ただ、実際それができるかどうかというのは、各キャリアさんであったり業界団体さんに検討はしていただく必要があると思うんですけれども、例えばキャリアさんで使われているID自体を、認証レベルをちゃんと確保したIDで発行し、それに基づいて本人確認を定期的に走らせるということでもいいと思うんですけども、そういったことが必要になってくるんじゃないかなと。これはあくまで、仕組みとしてやろうと思ったときに、そういうことがあり得るんじゃないかと思いました。

２番の法人に関してなんですけど、実は私、常々、小規模の法人をやっておりました関係で、ショップに行きますと「名刺を出してください」と言われるんですが、結局名刺なんて幾らでも不正に作ることができます。

先ほど中原先生が、「法人に属していること」ということなんですけども、なかなか現実的な在籍証明って難しいと思っていまして、もちろん大手の企業さんのようにしっかり運用されている企業さんはいらっしゃると思うのですが、むしろ中小零細の数というのはよっぽど多くて、そこを確実にというとなかなか難しいと思うんです。

そういう意味で言いますと、今、デジタル庁さんですかね、GビズIDというのが進められていまして、GビズIDプライムを使うと各種電子申請が利用できる進められているので

すが、あれもJPKIベースの認証がされていないと利用できない。例えばそういったIDでオンラインで連携すれば証明になるというような電子的な手法の導入も、２番に関して、法人に関しては検討すべきではないのかなと思いました。

あと、依拠に関しては、皆様おっしゃっているとおり、JPKIをベースにというところ以外はなかなか厳しいのかなと思っております。

追加回線に関してなんですけど、私、あるキャリアさんで６回線目を契約しようとして、そもそもその業界ルールがあるということを知らずに、駄目ですと言われた経緯があるんですけれども、なぜ５回線以上は駄目なのかみたいなところの明確な説明を受けなかったんです。

そこは、説明は業界団体としても必要だろうなと感じましたし、逆に言うと、本人確認であったり、私が先ほど言った定期的な確認をちゃんとやるのであれば、回線数の制限はむしろ要らなくなるのではないかなと思っております。次にある上限もそうですね。

あと、データSIMの本人確認なんですけれども、警察庁さんのお話にありましたとおり、やはりアクセス元が特定できなくなるというところが致命的かなと思っておりまして、皆様覚えていらっしゃるかどうか分からないのですが、2010年に無線LANが結構自由に利用できて、それでアクセス元が特定できなくなるという事件、尖閣諸島中国漁船衝突映像流出事件というのがございました。

あの時に一気に、漫画喫茶等の無線LANを認証なしでは使えなくなるという条例だったり、そういったものが導入されたんですけれども、昨今、観光向けにオープンにされる無線LANも増えてきたのですが、やはりアクセス元が誰かと証明できなくなるというのは、犯罪という観点から、なかなか厳しくなってくるのかなと思っておりまして、過去、無線LANで起きたことと同様に、データSIMについてもそういったアクセス元が何かあったときに特定できる仕組みというのは残すべきではないのかなと思っている次第です。

【大谷主査】　丁寧なコメントありがとうございました。

沢田構成員から手が挙がっております。

【沢田構成員】　ありがとうございます。改めて、各論のほうで少しだけコメントさせていただければと思います。

論点の１に関して、違法だよとは各社言っていただいているのですけれども、それだけでは足りない気もしています。中原先生はかなり優しい目線でおっしゃっていましたが、もうちょっと厳しくというか、もしもあなたが契約した端末か携帯番号が犯罪に利用され、

実行犯が不明だった場合には、あなたが捜査対象になってしまうかも、ということを、もう少しストレートに言ったほうが刺さるのではないかと思いました。

それと、事務局資料の10ページ目、犯罪利用の可能性がある利用者について警察と情報交換するというのも、施策の一つとして挙げられていたかと思いますが、犯罪利用の可能性があるかどうかをどうやって判断するかによっては、利用者に対する権利侵害になってしまわないか、何をもって犯罪に利用される可能性があると判断するのかという点を詰めておく必要があるのではないか、情報交換は既に始まっているのかもしれないですが、気になりました。

論点３の依拠に関しては、もしも認める場合には、やはりレベルを合わせる必要があるというのと、これも利用者のリテラシーとも関係しますが、個人情報絡みの話です。依拠するというのは情報を共有するのとは多分全然違う話だと思いますが、ユーザーから見ると、依拠先が、自分の身元情報を、これから契約しようとしている通信事業者に提供していると思ってしまったりする可能性はないのかが気になったところです。きちんと説明すればよいことですが、「ここに依拠しています」というのをユーザーにどう説明されるのか、整理をする必要があるかなと思いました。基本的には依拠しないで良いのではないかと思っています。

それから、４と５、先ほど中原先生が指摘されたのと同じ話で、どこにニーズがあるのか、個人がそんなにたくさん契約するニーズというのはあまりないのではないかと基本的には思っています。仕事用と個人用と分けるのは分かるし、家族の分をまとめて契約するのは分かるのですが、それ以外にどんなニーズがあるのかによって、例えば５回線を上限にするか、追加契約のときに毎回本人確認すべきかが変わってくると思っておりましたところ、今、辻様が６回線目を契約しようとされたということなので、ニーズはあると理解しました。どんなニーズかというのをもし教えていただけると。

【辻構成員】　全然大したことじゃないんですけど、私自身が２回線を個人で持っておりまして、プラス、家族の分は私の名義で契約したほうが連携しやすいかなということで、家族も、子供３人プラス妻プラス親の分ということで契約しようと思ったら数が超えてしまったということでした。

【沢田構成員】　事業者さんは、そういうケースがどのぐらいあるかを御存じかと思うので、もしお分かりになれば教えていただければと思いました。

【大谷主査】　ありがとうございます。

事業者の方からは、多分、御家族５人で済まないケースというのが結構あったりするのかもしれませんので、追加で情報提供をいただければありがたいと思っておりますが、残り時間が少なくなってきておりますので、後ほど追加で教えていただくことをお願いしたいと思います。

【仲上構成員】　日本スマートフォンセキュリティ協会技術部会の仲上でございます。

コメントになりますけれども、論点１のところについては、しっかりと啓発活動をやっていくべきところでありますし、日本スマートフォンセキュリティ協会の中でも、中高生に対して、スマホをセキュリティーの観点から安全に利用していくような取組、啓発活動を行っておりますので、こういったところでもぜひ、警察等と連携させていただきながら、実態をもって御説明できるような取組ができればと思っております。

あと、先ほども話題になっておりましたけれども、論点５の上限契約台数につきましては、特にデータSIMのところについては、個人でも個人事業主とか半分事業者のような動きをしているところが、IoTセンサーとしてデータSIMを複数台活用するケース等もあるかなと思いますので、がちがちに５台というわけではなくて、そういった特殊なユースケースに対応できるような契約の内容になっていると非常にありがたいなと思う次第でございます。

あと、論点６のところの訪日外国人の方の事例につきましては、なかなか利便性と実際の本人確認といったところの難しさについては、様々事業者の方から御意見いただいたところかと思います。

こういったところについては、ある程度ガイドラインというか、短期間的な利用にとどめるなどのルールを設けて、レベル感を合わせていくといった取組が重要なのではないかと思った次第でございます。

【大谷主査】　貴重なコメントありがとうございました。

【鎮目構成員】　データSIMの悪用については、警察庁様から、こういう手口が出てきていて、データSIMについても本人確認等を厳格化しないと犯罪抑止の点で不十分であるという、そういう御説明があったかと存じますが、他方で、MVNO委員会様の御意見の中だったと思いますけれど、SMSのないデータ専用SIMについては、不正利用の実態について把握をしていないという御指摘もあったかと存じます。

これは警察庁様に伺うのがいいかなと思うんですけれど、そういうデータSIMの悪用について抜け穴というのが出てきているので、今後もそういうものが爆発的に増えていく可

能性があるという、予防的な意味での対応の要請なのか、それとも、MVNO委員会様などの御指摘とは異なって、かなりそういう悪用の実態が既に一般化しているという、何かエビデンスがあるのかどうか。

私は、既に悪用がかなり一般化していない限り規制すべきではないという趣旨ではなくて、もちろん、そういうのが出て、手口があるのであれば塞いでいくという、先手を打っていくということも必要なのではないかなと考えておりますが、その辺りの事実の認識について御説明いただけると大変ありがたく存じますというのが、質問というか意見でございます。

【大谷主査】　ありがとうございます。やはり犯罪の手口の実情を踏まえて検討したいということで、何人かから御意見をいただいていると思うのですが、この場で御回答いただける内容など、警察庁様にございますでしょうか。

【警察庁（根本)】　御質問ありがとうございます。

簡単に申し上げますと、本日の御説明した事例の中でも、SMSなしのSIMが悪用された事例についても紹介をしております。

そういった点では、悪用の実態はあるものと認識をしておりますし、また加えまして、おっしゃられるように予防的な観点からも、こういった対応をしていくことが必要であろうとも考えております。

【鎮目構成員】　ありがとうございます。もし、今後この点を検討していく上で、数字的なものを出すのは難しいのかもしれませんけれど、かなり悪用の実態として、このデータ専用SIMの通信が実行犯と首魁との間の連絡手段として使われているケースが多いという、把握されているそういう建設的な意味でのデータをお示しいただけると、強い対応を取る意味で、より説得的になるのかなと思いました。

もしそういうものをお出しいただくことが可能なのであれば、今後お願いできるといいかなというのが、感触でございます。

【大谷主査】　ありがとうございます。やはり規律強化が必要だということであれば、説得力を持たせるためにも、何らかの統計であるとか量的なものがいただけるとありがたいと思っておりますので、可能な範囲で警察庁様にも御検討いただければと思います。貴重な御提案をありがとうございました。

議論は尽きないところではありますが、この辺りで本日の討議を終了させていただきたいと思います。

今日は６点にわたっての議論でしたけれども、活発な御議論、それから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。

それから、事業者の方からも、実際の本人確認の方法であるとか実務の状況について、丁寧な御説明をいただきましてありがとうございました。

本人確認の在り方などについては、本人確認という一言で言い表せないところもあって、当人認証であるとか、あるいはフェデレーションといったようなところも含めて、どのようにするのが、犯罪を防止するために実効性があって、ミニマムな規律なのかといったところについては、まだまだ御議論が必要な点ではないかなと思っております。

また、利便性であるとかニーズといったことについても、ある程度事業者の方から御意見いただきましたけれども、それと規律強化とのバランス、また改めて検討の機会を持っていく必要があるのではないかと思っております。

ちょうどデータSIMについて、特に警察庁様からも情報の提供をいただきましたが、IoTであるとか、訪日外国人向けのサービスなどの利用者への影響ですとか、それから犯罪の実態、事実関係といった観点の検討も必要になってくるかと思います。

先ほどもお願いしましたが、警察庁様にはできる限り、今回、事例を中心に御説明いただきましたけれども、統計的な情報であるとか、検挙されたケースに加え、検挙に至らなかった内容も含めて、さらなる情報提供の御協力をいただければと思います。

それぞれの論点について、何となく方向性は見えつつありますけれども、次々回以降のワーキンググループで取り上げまして、引き続き議論を進めさせていただきたいと思いますが、いかがでしょうか。

特に御異議もないようですので、引き続きこのテーマについて検討させていただきたいと思います。

それでは最後に、次回の会合につきまして、事務局からお願いいたします。

【田中利用環境課課長補佐】　事務局でございます。次回会合は５月９日を予定しておりますけれども、詳細については別途御案内いたします。

事務局からは以上です。

【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７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、御出席いただきましてありがとうございました。