

不適正利用対策に関するワーキンググループ（第9回）

令和7年5月16日

【田中利用環境課課長補佐】 お時間となりましたので、不適正利用対策に関するワーキンググループ、第9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、田中でございます。よろしくお願いいたします。

事務局からのウェブ会議による開催上の注意点については、先ほど投映していた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9－1から9－4を用意してございます。

また、本日は仲上構成員、星構成員が遅参の予定で、中原構成員が遅参で、もしかしたら欠席と伺っております。

注意事項は以上となります。

では、早速ですけれども、議事に入りたいと思います。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。大谷先生、お願いします。

【大谷主査】 大谷でございます。それでは、早速議事に入りたいと思います。

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、その後に警察庁、それからNTT様、楽天モバイル様から、第7回、前々回を踏まえた補足説明をいただきます。その後、U-NEXT様から御発表いただきまして、その後にまとめて質疑応答を実施した後で意見交換を進めさせていただきたいと思います。

それでは、事務局からの御説明、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、不適正利用対策をめぐる環境変化の課題の一つである携帯電話本人確認のルールについて、引き続き御議論いただきます。資料を投影しながら御説明させていただきます。

こちらは今後の検討スケジュールです。当面の活動として、前々回、4月21日に、携帯電話の本人確認のルールについて、MNOの4社の方とMVNO委員会の事業者ヒアリングを踏まえて御議論いただきました。本日はそちらで御議論いただいた中から、構成員や事業者の指摘やコメントについて御紹介した後で、幾つかの点について補足を行ってまいります。

また、事業者ヒアリングとして、前回はMNO4社とMVNO委員会に御説明いただいたとこ

ろですけれども、本日は訪日外国人ですとかIoT向けのサービスを提供していらっしゃるU-NEXTさんからお話をいただく予定です。6月6日の論点整理に向けて整理した後に親会へ報告する予定でございます。

2ページ目は、これまでの議論の課題としていた論点の6つについて資料を再掲してございます。

3ページ目ですけれども、それぞれの論点についての御意見を御紹介させていただくとともに、現時点の考え方についてお示しさせていただいております。

SIMの不正転売ですけれども、こちらは前回の御議論で、周知を改めて徹底することが必要といった御意見ですとか、周知する際に分かりやすさとして関与した本人も不利益を被る可能性があるなどのストーリーですとか、関与した本人が捜査対象になる可能性があるということをストレートに伝えていくほうがいいのではないかとといった御意見をいただきました。

また、利用者の本人確認を事業者の取組として定期的に行い、転売を防ぐような仕組みも必要ではないかといった御意見もございました。また、与信時の審査強化などの仕組みも考え得るというような御意見もございました。

こういった御意見を踏まえまして、下に記載がございます考え方でございます。事業者による不正検知が困難である中、犯罪抑止の観点から当面取り得る対策として、不正転売の違法性について政府及び事業者において、利用者に対して分かりやすい周知啓発を一層強化していくことが必要ではないか。それに加え、事業者による定期的な本人確認の仕組みの導入も有効だと考えられるのではないかとことを示させていただいております。こちらが1点目です。

2点目、法人の代理権ないし在籍確認の部分です。こちらは委任状というよりも、来店者が当該法人に在籍している事実を示す書類であるかが重要であるというところですか、とはいいつつも、中小企業や零細企業は現実的な在籍確認が難しいので、電子的な手法などの導入も考えられないかといった御意見がございました。

こちらについて考え方としまして、法人契約については、現行の事業者の取組も踏まえつつ、利用者目線に立って予見可能性を高める観点から、来店する担当者と法人の関係性を明らかにするために必要な書類の提出を求めるなど、所要の規定見直しが求められるのではないかとございます。

次、3点目でございます。こちらは他社の本人確認結果への依拠です。こちらは慎重な

検討が必要という御意見が多くございました。不正の対応について十分に議論した上で、余裕がある限りに検討するという事としてはどうかという御意見ですとか、そもそもJP KIをベースに本人確認を行っている事業者に限定するのが検討の前提になると考えるといった御意見もございました。

考え方のところでは、他社の本人確認結果への依拠については、一部事業者からのニーズが認められるものの、昨今の犯罪手口の巧妙化、高度化も踏まえると、ID/PASSの不正入手への対策や、ほかの見直し事項の議論の進展を見極めた上で、依拠先の本人確認の保証レベルが高く、かつ最新のものであることや、依拠元の本人確認が適切に行われることなど、依拠が適切にできる要件を整理した上でルール整備を行うことも視野に、改めてワーキンググループにおいて検討を深めてはどうかとしてございます。

次、4点目です。追加回線の本人確認です。こちらは、御意見の前提となる部分の検討が必要ではないかといった御指摘がございました。1点目のところで、2回線目以降の簡易な契約というのがどれだけ犯罪に寄与しているのか、検証が必要ではないかといった御意見ですとか、2点目の部分で、この簡易な本人確認手法を残すことが利用者の利便性の確保としてどれだけ切実な問題なのかについて検討が必要といった意見をいただきました。こちらについては、警察庁から補足発表と事業者から補足発表をそれぞれいただく予定です。また、ユーザーとしては、なりすまし防止のために本人確認を厳密にしてもらったほうが安心感があるのではないかといたした御指摘もいただきました。

考え方については、上述の補足を今日発表いただく予定ですので、そちらを踏まえた上で考え方を整理していくこととしてはどうかと考えております。

5点目です。こちらは上限契約台数でございます。こちらについても、前提となる情報をしっかり整理するべきという御指摘がございました。過少規制も過剰規制もよくないので、基礎的な現状認識をしっかりとさせる必要があるという御指摘や、それに関連して、ニーズや利用実態を確認する必要があるといった御指摘をいただきました。こちらについても本日事業者から補足で発表いただく予定です。

また、契約時の本人確認の強化や定期的な本人確認を行うことができれば、回線数の制限は不要ではないかといった御意見や、そういった契約が慎重にされれば問題ないと思う一方で、本当にその本人認証の強化によって十分な効果が生じるのか、丁寧な検証が必要といった御意見もございました。

考え方としては、本日いただく補足も踏まえて、考え方を整理していくこととして

はどうかしております。

最後の論点である6点目です。データSIMの本人確認です。こちらは総論、対象SIM、利用用途と分けて記載しております。

総論については、犯罪の観点から特定できる仕組みを残すべきではないかという御意見をいただいております。対象SIMについては、SMSあり・なしデータSIMについて定量的な犯罪実態の確認が必要ではないかといった御意見をいただきました。こちらについても、本日、警察庁さんから補足の発表をいただく予定です。

また、利用用途については、IoT用のSIMについて、ほかの用途に利用できないかを確認する必要があるといった御意見ですとか、自動販売機のデータSIMの販売への影響を確認する必要があるといった御意見、また、訪日外国人については、法令ではなくガイドライン等で短期間の利用にとどめるなどのルールを設けて、事業者間でレベル感を合わせていくといった取組が必要ではないかといった御意見がございました。

考え方としては、上述の補足も踏まえて考え方を整理していくこととしてはどうかしております。

最終ページです。補足事項を一覧して再掲しております。論点4について、警察庁と事業者、NTTドコモから御発表いただく予定です。論点5については、楽天モバイルから補足発表をいただく予定でして、論点6の警察庁からの補足発表については、後ほど警察庁から御発表いただく予定です。

事務局からは以上となります。

【大谷主査】 御説明ありがとうございました。

不正利用の実態面について、より事実関係をつぶさに確認したいという前回御意見をいただいておりますので、今回また警察庁の方から御説明いただくこととなっております。

今日は御準備いただきましてありがとうございます。警察庁様、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。本日もよろしくお願いいたします。

まず、論点4、追加回線の本人確認として、2回線目以降の契約が簡易なことがどれだけ犯罪に寄与しているのか検証が必要であるとの御指摘をいただいております。この点につきまして、口頭で補足説明をさせていただきます。

前回の悪用事例に関する発表でも触れさせていただいておりますが、大手モバイルキャリアを舞台としたSIMの不正発行事案におきまして、少年被疑者のパソコンからは約2,700

件のeSIMが発行できるQRコードが見つかっております。少年らは、契約の上限数が多く本人確認が甘い事業者を狙ったとの供述も行っております。この捜査では、この約2,700件のeSIMのうち、約100件について立件をしております。この立件した100件のうちの17件は音声SIMであり、2回線目以降で本人確認がなされずに不正発行されたものであったことが判明しております。

また、少年らは生成AIを使って自動的にSIMの発行申請を行うツールも作成していましたが、当該事業者のモバイル通信契約者であれば、契約上限の10回線まで不正契約を行っていたとの供述を行っており、契約上限数までeSIMを不正発行していた実態も明らかとなっております。

続きまして、論点の6、データSIMの本人確認について、SMSあり・SMSなしデータSIMについて、定量的な犯罪実態の確認が必要であるとの御指摘をいただいております。まず、SMS付きのデータSIMに関して御説明いたします。こちらについては、資料に沿って御説明いたします。

資料で示しておりますSNS型投資・ロマンス詐欺に係る被疑事件に使用されたSMS付きデータSIMについて御説明いたします。この資料では、SNS型投資・ロマンス詐欺に係る被疑事件で使用されたSIMについて、令和6年4月から9月までの間に都道府県警察から警察庁に報告され、把握できたものを記載しております。

なお、SNS型投資・ロマンス詐欺においては、当初の接触ツールや被害時の連絡ツールとしてSNSが使用される場合が多いことが明らかとなっております。今回、警察庁で把握したSIMについては、アカウントを取得する際に電話番号によるSMS認証が必要となるSNSを対象として都道府県警察から報告されたものであり、SMS機能がついていないデータSIMについては本資料の対象外となります。

それでは、この資料の内容について説明いたします。SIM種別の特定に至ったものは244件あり、そのうちの185件はSMS付きデータSIMであり、残りの59件は音声SIMという結果でありました。つまり、把握できたSIMのうち、約76%は契約時の本人確認が義務づけられていないSMS付きデータSIMでありました。

次に、把握した185件のSMS付きデータSIMについて、契約時に事業者による自主的な本人確認がなされていたかどうかについて確認しております。この185件のうち、約59%に当たる110件については、事業者による自主的な本人確認がなされておりました。残りの約41%に当たる75件については、事業者による自主的な本人確認がなされておりました。

したが、この点についても補足しておきたい事項がございます。

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を行っていることは承知しておりますが、今回把握しておりますこの75件については、そのほとんどが訪日外国人向けのプリペイド型SIMでありました。本人確認書類としては、我が国では在留カードやパスポートの利用が一般的ではありますが、今回把握したものについては外国の身分証明書が使用されており、真正なものかどうか不明であるなど、事業者としても本人確認を行うことが困難なものであり、本人確認が実質的には機能していないものが多数となっております。

以上をまとめますと、今回把握できたSIMのうち、約76%は契約時の本人確認が義務づけられていないSMSつきデータSIMであり、さらにそのうちの約59%は事業者による本人確認がなされていなかったということであります。また、先ほども補足させていただいたとおり、事業者による自主的な本人確認がなされていた約41%についても、一般的に本人確認で求められる在留カードやパスポートといったものはほとんど使用されておりませんでした。

今回把握しておりますSIMについては、冒頭でも申し上げましたとおり、アカウントを取得する際に電話番号によるSMS認証が必要となるSNSを対象として都道府県警察から報告されたものであり、SMS機能がついていないデータSIMについては本資料の対象外となりますが、契約時の本人確認が義務づけられていないSMSつきデータSIMの悪用実態が認められていることから、データSIMの契約時に厳格な本人確認を義務づけることが、SNS型投資・ロマンス詐欺における悪用を防止する対策の一つとなり得るのではないかと考えております。また、実際の犯罪の捜査においても、本人確認の義務づけが被疑者の事後追跡可能性の確保につながるのではないかと考えております。

続きまして、SMSなしデータSIMについても補足説明させていただきます。携帯電話が悪用された様々な事件の捜査において、どの通信がデータSIMによるものなのか。また、使われたデータSIMにSMS機能があるかどうかといった照会までは、必ずしも行われているわけではありません。そのため、SMSなしのデータSIMに関しては、現時点での定量的な犯罪実態を具体的にお示しすることは難しい状況でございます。

ただ一方で、前回の悪用事例に関する発表でも触れさせていただいたとおり、SMSなしのデータSIMについても、クレジットカードの不正利用や不正アクセス、匿名性の高いSNSを用いた首魁との連絡に悪用されていた事例が認められることから、SMSなしのデータSIM

についても同様に厳格な本人確認を求めていると考えているところでございます。

警察庁からの補足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、続きましてNTTドコモ様からの補足説明をお願いしたいと思います。よろしくをお願いします。

【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9-3に基づきまして補足説明いたします。当社からは、追加回線の本人確認を厳格化した場合に、どのような利用者において利便性の低下が考えられるかという点でございます。

当社においては、今回例示させていただくのは、スマートフォン契約のオプションサービスとして提供しているウェアラブルデバイスサービスになります。こちらはスマートフォンとペアリングして使うものでありまして、このデバイス自体も単体では動作しますが、電話番号はスマートフォンと同一のものを使用して送受信するものでございます。基本的にこちらについては、法令遵守の観点では追加回線のルールを用いた本人確認を実施しております。それ以外にも副回線サービスという、同一のスマートフォンの中にサブでもう一つ回線を申し込むことができるサービスがあります。こちらの2つが追加回線ルールを用いております。

ワンナンバーサービスにおきましては、この図の左の真ん中になりますが、サービスを契約する際とデバイスを追加する際に、それぞれ本人確認を実施する必要がございます。プランとしては、1台だけ利用するプランとそれを追加して利用するプランの2種類があるということでございます。本来これはスマートフォンのオプションサービスでありますので、簡便な方法で本人確認できることが望ましいと考えております。また、同一の電話番号で動作しますので、これが犯罪に使われる可能性というのは非常に低い性質のものと考えております。

これが本人確認ルール見直しとなった場合には、デバイスの追加において本人確認が必要となりますので、利用者にとっては煩瑣となりまして、利便性が低下する可能性があるというものでございます。

他方で、このサービスを始めたのはもう五、六年以上前になりますが、今となりましてはJPKIなど、オンラインにおいて確実に簡便な本人確認の方法も出てきておりますので、現状を鑑みるとそこまで利便性が低下しないとも考えられるかなと思っております。

我が社の説明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。

それでは続きまして、楽天モバイル様から御説明をお願いいたします。

【楽天モバイル（小田）】 楽天モバイルでございます。多数の回線を契約することについてのニーズですとか利用実態について、楽天モバイルでコメントさせていただきます。

まずニーズの観点では、回線数シェアが約4%である当社におきまして、お一人で6回線以上の契約をお持ちの方の回線が数万規模でございます。よって、市場全体での一定のボリュームはあるものと考えてございます。

次に利用実態といたしまして、前々回、辻先生からも御発言がありましたように、御家族分をお一人に集約されるというケースが多くを占めると当社では考えてございます。また、背景としましては、大きく3つの理由があろうかと考えております。

1つ目は金銭管理の観点でして、毎月の支払い口座あるいはクレジットカードを御家庭内で集約することで金銭管理をしやすく、また、一覧性を高めたいと。そんな考え方があると考えてございます。

2つ目としましてはポイントプログラムの観点でして、ポイントをためるですとかお使いになるといった両方の観点で、1か所にまとめることで、分散するよりも集中することで経済的メリット、利用機会を高めていきたいという考え方が2つ目でございます。

3つ目としましては、こういったスマートデバイスの集中管理の考え方です。そもそも携帯電話の契約というのは、法律ですとかITに関するリテラシーを一定要しまして、苦手な方にとっては難しいこともさることながら、心理的に非常に負担が大きいという捉え方をされる方が一定数いらっしゃるなど我々も肌感覚として持っております。近しい身内の中でも最も得意な方にできるだけ任せたいという考え方なのではないかと考えてございます。

特にスマートフォンにつきましては、購入後においてもアプリケーションですとかソフトウェアの更新が継続的に必要でして、また、トラブル対応に際して原因を切り分けたり、あるいはショップで相談するに際しても、知識やスキルが一定ないとというところで尻込みされてしまう方もいらっしゃるのかなというところがございます。特に高齢の方ですとか機械が苦手という方は、身内で得意な方に任せたいという心理が働くのかなと感じ取っております。

そういった観点でいきますと、2世代で親子のみですと5回線以内に多く収まることも現代では多いのかなと思いますけれども、3世代となりますと、それを超えてくるケース

も多かろうということを想定してございます。

こういった利用実態の観点から、当社といたしましては、契約台数を制限するよりも多要素認証と本人認証をしっかり強化することで不正契約そのものを防ぐといった取組が重要だと考えている次第でございます。

楽天モバイル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。

それでは、続きまして、事業者様からの御説明をお願いしたいと思っております。U-NEXT様には御準備いただきまして、ありがとうございます。今回は、訪日外国人へサービスを提供しているということでお引き受けいただきました。質疑応答も含めまして、御説明を伺ってからにしたいと思っております。それでは、よろしくお願いいたします。

【U-NEXT（野田）】 よろしくお願ひいたします。御紹介いただきましたU-NEXTと、グループ企業でありますY.U-mobileを担当しております野田と申します。ここまで、すみません、ワーキンググループに初めての参加となりますので、ちょっと御説明等拙いところがあれば大変申し訳ございませんが、よろしくお願いいたします。

それでは、資料に沿って御説明させていただきます。まず、U-NEXTなんですけれども、いわゆる映像サービスのイメージが強いかなとは思いますので、U-NEXTのやっているモバイル事業とは何ぞやというところを簡単に前段で御説明させていただいた後に、本日の議題について御説明させていただければと思っております。

大きく2つの領域に分けております。左側が、いわゆるBtoC、コンシューマー向けのサービス、右側がBtoBのサービスとなっております。

一般ユーザー向け、コンシューマー向けのものに関しましては、U-NEXTとして、MVNOサービス、U-mobileというものを展開しておりましたけれども、左上になります。こちらに関しましては既に新規申込みは終了しております、現在、下にありますY.U-mobile社で、y.u mobileというサービスに集約しているという形になっております。一般ユーザー向けには、もう一点右上になりますプリペイドSIM。こちらはU-mobileのサービスの中の一つになるんですけれども、彩という名称でサービス展開させていただいております。

右側、BtoBの領域に関しましては、主にグループ企業、弊社はU-NEXTグループが約30弱ございまして、その多くがBtoB向けのサービスを展開しておりますので、特にUSEN社を中心に、店舗向けIoTサービスのところでSIMを活用しているという形になっております。

続きまして、モバイルサービスと一括りに御説明させていただいたんですけれども、サ

ービスの展開にも少し差がありますので、そこも事前に御説明させていただきます。いわゆるMVNOサービス、格安SIMとして展開させていただいているものに関しましては、回線はドコモ様の回線をお借りして展開させていただいております。上流にMVNEがございまして、U-NEXTでピーゲートウェイを用意しておりますので、そういった接続方法で一般ユーザーに向けて回線提供をしているという形になっております。

一方プリペイドSIMなんですが、こちらは上流のフルMVNOより御提供いただくような形になっておりますので、OEM提供を受けてサービス展開をしているという形になっておりますので、弊社側で何かネットワーク側でコントロールするとか、仕組みを用意しているとかということではありませんので、この辺り、ちょっと事前の情報として記載しております。

続きまして、従前ここでもう御議論されていることかと思いますが、弊社のMVNOサービスにおける本人確認といったところも少しだけお伝えしておこうと思ひまして、追加しております。

まず、本人確認のところなんですけれども、データSIM。これは、SMSあり・なしいずれも音声通話SIMと同等の方式で本人確認というものを実施してございます。先ほど少しお話しにありました本人確認の書類といったところも、外国人の方に関しましても、在留カード、永住証明書、外国人登録証明書、この辺りに絞って展開しているという形になっております。

続きまして、SIMの契約台数は、記載のとおり音声、データともに最大4回線という形で、比較的數字としては少ないほうの上限になっているのかなと思っております。

その他の対策としましては、やはり昨今SMSをたくさん使うというところが數字としては明らかに異常なものもあつたりしますので、こういったものは独自の基準値を設けまして、明らかにおかしいものに関しましては、利用規約に沿ってこちらから利用停止の処理を行うといったところの自主的な取組というものも行っております。

ここまで前段の御説明となっております、ここからが本日の本題となっております、本人確認義務化における影響というところでございます。

まず、BtoCの領域です。MVNOサービスで展開しているところの影響に関しましては、先ほど御説明させていただいたとおり、音声同様の本人確認を実施しておりますので、弊社としましては大きな影響はないのかなというふうには考えております。ただ、MVNOサービス各社様におかれましては、まだデータSIMの本人確認をやっていないというところもご

ございますので、そういったところに関しましては、義務化となりましたら一定の期間といったものは必要になるのかなとは思っております。

一応、下に要望として記載させていただいたんですが、御承知のとおり、来年の4月にはJPKIの一本化というところもございますので、弊社も準備等を含めて既に取組を開始しておりますが、我々のような規模の事業者になりますと、一概に一本化といいましてもいろいろなところに影響がございまして、当然開発コスト等もかかってきますので、本人確認義務化における中で、何かこれまでにないような取組が追加されるとかということがあれば、当然事前の準備にも影響してきますので、この辺りは早めのタイミングで事業者にも共有いただけると非常にありがたいなと考えております。

続きまして、プリペイドSIMのところになります。こちらは先ほどの御説明の補足も含めたスライドになっておりますので、上段は見ていただければと思いますが、コロナ禍以前は、各国際空港様であるとかメトロ様といったところで、非常に多く自動販売機も置かせていただいて展開していたんですけれども、コロナ禍に入りましてかなり規模を縮小しております。現状でいいますと、ヤマダ電機様、一部70店舗ほどで扱っていただいているのと、ミニストップ様、これはもう成田空港様のみ1店舗のみ扱っていただいております。空港に関しましては佐賀空港のみの1店舗になっておりまして、一部、金沢の観光協会様で扱っていただいているという形になっております。

展開しているSIMカードにつきましては、物理SIMのみです。eSIMは対応しておりません。データSIMのSMSなしのタイプのものを展開させていただいております。提供プランも利用期間を定めておりまして、短いもので7日間から長いものでも30日間という形で展開しております。それぞれに通信容量が3.5ギガから100ギガまでという形で制限を設けている形になっております。備考のところにも書かせていただきましたが、現状、プリペイドSIMに関しましては、本人確認というものは実施しておりませんという形になっております。

プリペイドSIMに関しまして、本人確認義務化における影響というところでまとめさせていただいております。下段にいろいろ書かせてはいただいているんですが、結論、弊社としましては、訪日外国人向けのプリペイドSIMに関しまして、特にSMSなしに関しましては、本人確認は不要なのではないかなと考えております。

まず、影響に関しましては、現在の仕組みですね。これはサービスを展開するに当たる仕組みにおいて、同様のサービスが義務化となると難しいのかなと考えておりますので、義務化となった場合は、弊社では事業継続自体が非常に困難かなと考えております。

また、見解のところにも少し書かせていただいておりますが、SMSなしのものになりますので、必ずしも全てにおいて影響はないということではないんですけれども、SMSを使った、先ほどの御説明があったロマンス詐欺であるとか電話を使ったもの、もしくは電話番号を転売するといったところはリスクの少ない商品かなと考えております。また、先ほどのとおり利用期間というものも定めておりますので、そういった意味では義務化することによる効果というものは、かなり限定的なものになるのかなと考えております。

また、ユーザーの利便性としまして、本人確認を実施するとなりますと、当然本人確認に必要なデータをアップロードしていくとかいう形で通信が必要になりますし、それを実施するための時間というのも一定時間必要になってくるのかなと思います。また、先ほどもありましたとおり、本人確認書類は、じゃ、何を使うのか、何をもって正しいとするのかと、リスクが少ないのかというところも非常に難しい課題があるのかなと思っております。それらを鑑みた全く新しいサービス設計というものが必要になってきますので、この辺りちょっと難しいのかなと思っております。

最後に、BtoB領域、グループで展開しているものになります。右に少し図も入れているんですけれども、特に分かりやすいUSENで表示させていただいております。USENは、一昔前は電柱から電線を引かせていただいて、そこから配信するというような形を取らせていただいていたんですけれども、現状で言いますと、右側にあるとおりタブレット型の配信となっております。こういった機器にSIMを直接入れて通信させるという形で音楽配信であったり、監視カメラであったり、デジタルサイネージであったり、一部IPフォンであったり、決済の機能であったりと、様々な端末にSIMで通信させているという形になっております。

簡単ではございますが、SIMの不正転売、この辺りも専用の端末を使って我々のほうでキッティングした上で納品をしているといったところと、機器にもシールを貼り付けることによって、SIMを出そうとして抜くとシールが剥がれてしまうというような工夫もしてございます。また、契約も、店舗向けサービスであるという特性上、必ずオーナー様との契約を結んでいる。もしくは、チェーン店様であれば包括の契約を結んでいるという形態を取らせてもらっておりますので、代理の方が契約をして、SIMのみを抜き取って不正に使っていくというのは非常に考えにくい事業モデルになっているのかなと思っております。また、一部、先ほどIP電話等のサービスも行っておりまして、こちらに関しましては本人確認も独自にやっているという形になってございます。

いわゆるBtoB領域のところの義務化における影響をまとめさせていただいておりますが、先ほどありましたとおり、弊社においてではございますが、IoT機器向け、特にデータSIM、SMSなしのものに関しましては、こちらも本人確認は不要なのかなと考えてございます。当社で取っているサービスの形態、運用といったものによっては不要とは考えますが、一部SIM単体を納品するようなものがある場合に関しましては、当然検討は必要かなというふうには思いますが、弊社のような形態といったところに準じて規制等は検討していく必要があるのかなと考えてございます。

弊社から御説明は以上となります。長くなりまして申し訳ございません。

【大谷主査】 丁寧な御説明をありがとうございました。

それでは、警察庁様、それから事業者様からのただいまの御説明につきまして御質問を受け付けたいと思います。

それでは、沢田構成員、よろしくお願いいたします。

【沢田構成員】 皆様、御説明ありがとうございました。大変よく分かりました。いろいろ勉強になりました。

U-NEXT様の御説明の中で、訪日観光客の方向けのプリペイドのSIMに関しては、實際上本人確認は難しいというお話がありました。先ほど警察庁からの補足の御説明の中で、プリペイドのSIMが犯罪に使われたケースがあるとおっしゃっていたように思います。その点をもう一度確認させていただきたいのですが、それは、短期間の観光客の方がプリペイドのSIMを入手することによって犯罪に加担していたケースと思ってよろしいのでしょうか。警察庁さんへの質問です。

【警察庁（根本）】 警察庁の根本でございます。御質問ありがとうございます。

SMSなしのデータSIMの悪用について、前々回の発表時、契約時の本人確認がなされなかった事例の2番目において御説明させていただいております。この事例では、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なしデータSIMを使用していた事件でございます。なお、この事例において、観光客向けのいわゆるプリペイドのSIMを悪用していたかどうかというのは、今すぐには確認はできませんが、事例としては、そういったSMSなしのデータSIMの悪用というのは幾つか確認はされているところでございます。

【沢田構成員】 観光客向けに、何か別に考えなければいけないことがあるのかどうかという視点でお聞きした次第です。

【警察庁（根本）】 前々回、御報告をしたものについて、これは観光客向けのものだったかどうかというのは、確認ができましたら、また共有させていただければと考えております。

【沢田構成員】 ありがとうございます。日本にずっといらっしゃる方であれば、在留カードとかいろいろなものを確認できると思うのですが、短期間に来られる方でそれは無理だなと思ったものですから。すみません。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。

それでは、警察庁様のほうで、前々回に他人名義のクレジットカードを利用して架空の契約者情報で契約した件、これが訪日外国人向けのプリペイドSIMであったかどうか御確認いただいて、事務局を通じて御連絡いただければと思います。

山根構成員、よろしくお願いいたします。

【山根構成員】 御説明ありがとうございます。

すみません。沢田構成員からの御質問と同じポイントにはなってくるかなとは思うんですけども、警察庁さんのほうで本日御説明いただいた資料で、先ほどはSMS機能なしのプリペイドSIMのお話だったかなと思うんですけども、本日御用意いただいた資料のいろいろ件数が書かれているものについては、SMS機能付きのもので詐欺事件に使用されたデータSIMの件数を書かれているかなと思っております。

この中で本人確認ありとなっているところの御説明として、ここも訪日外国人向けのプリペイドSIMのものだったというような補足説明があったかなというふうに記憶しているんですけども、SMS機能付きのもので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、そういう実態はあるということになるんでしょうか。警察庁様向けの質問になります。

【警察庁（根本）】 御質問ありがとうございます。

SMSつきデータSIMについて、本人確認がなされ、これは資料に掲載しておりますとおり、75件確認されております。この詳細を申し上げますと、70件以上は訪日外国人向けのプリペイド型SIMであります。その他については、詳細は不明となっております。

【山根構成員】 ありがとうございます。SMS機能なしのもので訪日外国人向けのプリペイドSIMについて、先ほど本人確認を実施するのが難しいんじゃないかというようなお話もU-NEXTさんからありましたけれども、SMS機能付きのものについては、事業者の自主的な取組として本人確認を実施しているものもあるということなんですかね。

【大谷主査】 本人確認はされていらっしゃるんですが、あるけれども、何か本人確認資料が在留カードとかパスポートを使ったものではなく、海外での身分証明書などを使っているの、厳密な意味での本人確認と少し違っているというような御説明を先ほどいただいていたと思いますが。

【警察庁（根本）】 ありがとうございます。そのとおりでございます。今回把握したものについては、外国の身分証明書が使用されており、真正なものかどうか不明であるなど、事業者としても本人確認を行うことが困難なものであり、本人確認が実質的には機能していないものが多数となっております。

【山根構成員】 素朴な疑問として、その本人確認できるかどうかというところで、販売実態の違いがある、販売の仕方の違いがあるというところかなとは思ったところなんです。ありがとうございます。

【大谷主査】 ありがとうございます。

今の点ですけれども、なかなかSMS機能がないものについての定量的な犯罪実態の把握が警察庁でもなされていないということで、実態の確認が難しいんですけれども、SMS機能があるものについては、一定の本人確認がなされているものについても犯罪実態があるということで御説明いただいたものと理解しております。

仲上構成員、よろしくお願いいたします。

【仲上構成員】 本日、御説明いただいて非常に理解が深まったところでございますが、SaaSですとか金融サービスの利用において、携帯電話番号が本人確認をするためのトラストアンカーになっているというところからこういった議論が入ってきていると思いますし、そこにSIMの通話機能あり、それからSMS機能のあり・なしといったところが、大きくSIMごとの、SIMが果たすトラストアンカーとしての役割というのが変わってくるかと思います。

他方、警察庁様からの御発表ですね。SMSなしのSIMにおいても、当然データ通信のみでできる機能ではあっても、インターネット上で様々なサービスが利用できれば、それは詐欺等に使われるというのは、それはもうWi-FiであってもSIMであっても同じことかと思えます。あと、ちょっとすみません、いろいろばらばらとしてしまいますが、同じく、海外から持ち込まれたSIMに対してのローミングについても同じようなことが言えるのかなと思った次第です。

警察庁様へのちょっと質問にはなるんですけれども、SMSありの本人確認というのは、

冒頭申し上げたトラストアンカーについて考えると妥当性が非常に高いと思いますし、ぜひやるべきだと思うんですけど、データ通信しかできないSIMに対しての本人確認が、当然本人に対する真正性が高まることは予想されますが、非常に利便性は下がってしまうというふうな効果もあると思います、ここについて期待される効果としては、犯罪を抑制する効果を期待されてのことなのか、もしくは捜査を効率的に、もしくは捜査の精度を高めていくための方法論として期待されているのかというところをお聞きできればと思いました。

【警察庁（根本）】 警察庁の根本でございます。御質問ありがとうございます。

効果として期待されることについて、当然各種のサイバー犯罪の未然防止という観点に加え、事後追跡可能性の確保という観点も挙げられます。そういった両面の観点があるのかと考えております。

【仲上構成員】 ありがとうございます。そういったところも加味して、検討を引き続き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】 貴重な論点の質問をありがとうございました。

それでは、星構成員、お願いいたします。

【星構成員】 ありがとうございます。

私から、U-NEXT様の8ページにございました訪日外国人向けのプリペイドSIM、SMSなしについて、本人確認を義務化した場合、現在の仕組みでは同様のサービスが提供できませんといったところをちょっと聞き漏らしてしまったので、既に御説明していただいたということであれば大変申し訳ないんですけども、1点確認させていただければと思います。

この場合の本人確認の内容といいますかレベルというのはかなり高いものになるというのは、現在の仕組みではという理解になるのでしょうか。といいますか、特にインバウンドの場合であれば、当然パスポートは基本的には携帯して持ち歩いているというところになるかと思うので、オンラインでの販売というのがどれだけあるのかというところがあるかと思うんですけども、例えばパスポートの提示を求めるということだけであれば、それほど大きなコスト負担にはならないのかなと素人考えでは思ってしまったんですけども、そういう理解ではちょっと違っているということであれば、ぜひ御説明といいますか御教示をいただければということで質問させていただきました。

【U-NEXT（野田）】 ありがとうございます。

まさにおっしゃっていただいたとおり、本人確認をどのレベルでやるかというところにはなるかと思う。弊社で行っております、MVNO、格安SIMと同じような、いわゆるJPK

Iに近いような本人確認となりますと、これはもう仕組み上も難しいなと思っております。

一方、おっしゃっていただいたような、パスポートを提示いただくというところに関しては、まさに運用のみのところにはなりますので、実施の可能、不可能で言いますと可能かなというふうには思っている一方、やはりパスポートの御提示を受けて、判断するのが店舗のスタッフであると。人の目でございますので、それが確実に行われたかどうか、そのパスポートが本当に真偽が確認できるのかみたいところで言いますと、かなり信憑性としては薄いものになるのかなというところと、当然スタッフ側のオペレーションみたいなことも発生しますので、我々で言いますとヤマダ電機さんの全社員にどこまで周知できるのかとか、ミニストップさんのコンビニで非常に列が並んでいるようなところ、どこまで実施できるかといったところは非常に難しい点もあるのかなと。あと1点、自動販売機が1台だけございますので、この辺りは当然難しいかなと思っております。

以上でございます。

【星構成員】 自販機は、要するにお金なりクレジットカードを入れたりすれば、もう特に何もなくぽんと出てきちゃうという感じなんですかね。

【U-NEXT（野田）】 ジュースとかと同じで。決済はクレジットカードのみになります。

【星構成員】 クレジットカードの番号自体は控えることはできるということなんです。

【U-NEXT（野田）】 もちろんカード情報非保持がございしますので、弊社側では当然保持はできませんが、いわゆるクレカベンダーには当然購入履歴としては残っております。

【星構成員】 という形なんですね。分かりました。ありがとうございました。

ですから、ホテル宿泊の際に必ずパスポートの提示というのは多分やっていると思うので、それが偽造のものかどうかはともかく、何が使われたのかということの確認自体はひもづける、記録自体は残せるという可能性。そういったレベルでの本人確認かどうかということも含めて、何をもって本人確認とするのか。あるいは、先ほどのやり取りでもございましたけれども、ひもづけできる場合に、偽造されたパスポートとひもづくのであれば、じゃ、その偽造パスポートはどこから出てきたんだという形でさらにひもづけていけるとかね。そういったようなところの可能性というのはあると、捜査する側としてはそれだけでもかなり違うのかなと素人考えでは思った次第です。

【U-NEXT（野田）】 ありがとうございます。

【大谷主査】 ありがとうございます。御質問を引き続き受け付けますけれども、幾つか事実確認もできたところですので、ヒアリングを踏まえた全体討議、コメントなども頂戴したいと思います。コメントも含めて、構成員の皆様、いかがでしょうか。

それでは、辻構成員、よろしくお願いいたします。

【辻構成員】 私は質問というよりコメントになるのかなと思うんですけれども、総務省さんが整理いただいた資料につきまして、基本的な考え方の案というところを書いてくださっているんですけれども、これまでのクイックに皆さんでディスカッションした内容がうまくまとめられているのかなと思うんですが、この1から6を読む中で1つポイントとなるのが、やっぱりキャリアさんが発行されているIDとパスワードというところが一つの軸になるのではないかなと思って。全部そこにする必要はないと思うんですが、1つは、やっぱり既にキャリアさんがID・パスワードというか、ちょっとすみません、キャリアさんごとのものを知らなくて、私はドコモを使っていることが多いので、ドコモで言うとDアカウントのようなものがあって、Dアカウントのようなものが、ドコモさんに関しては認証レベルのように設定されているんです。ちゃんと安全である。つまり、例えば2段階認証なら2段階認証なるものを加えているかでしたっけね。あと、本人確認です。免許証とかマイナンバーカードによる本人確認が済みであるかということによって、認証レベルをたしか幾つか設定されていたかと思うんです。そういったものを多分ほかのキャリアさんもやられていると思うんですけれども、キャリアさんごとの独自の仕組みではなくて、そういったものをルール化して、本人確認とリンクできるようなガイドラインであったり基準というのを設けていくのがいいんじゃないかな。

考え方の中でGPKIを活用するとか、ID/PASSをどうするであるとか、厳格化するというようなところは書かれているんですけれども、具体的にどうするかの一案として、キャリアさんのID自体を軸にそれを整備していくと、例えば3番なんかに関しても、ID・パスワードの不正入手云々というところに関しても、ID・パスワードをどう管理していくか。あと4番、5番なんかもそうですね。今あるID・パスワードを軸に増やしていくとかすれば、5番なんかも考え方がそもそも要らなくなるんじゃないかとか。そういったところを検討されてもいいんじゃないか。

前回もお話ししましたように、各個の会社で対策されていることをうまく整理して、共通の仕組みとしていくということを検討されてもいいんじゃないかなと思いました。

【大谷主査】 貴重なコメントをありがとうございます。

それでは、鎮目構成員、お願いいたします。

【鎮目構成員】 本日は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。

SMSがないデータのみのSIMについては、事務局の案では、上記補足も踏まえて考え方を整理ということで、割とニュートラルなまとめ方をしていただいておりますが、先ほど訪日外国人向けSIMについて、U-NEXT様から、現在の本人確認の状況を踏まえると、厳格化した場合は事業継続が難しいという御説明があったと思います。もっとも、SIMが自販機でも販売しているというような話もありましたので、日本人でも訪日外国人向けSIMを簡単に買うことが当然できるということになるのだとすると、それが規制の抜け穴にもなり得るところはやはりあるのかなとも思います。

そうすると、データのみSIMについて、どの程度の悪用の実態が現時点であるのかを踏まえ、どのくらい厳格化を今後していく必要があるのかを考えていく必要があるのかと思います。ただ、データのみSIMについては定量的なデータがないということで、それは非常に難しく、どうすべきかについて、私は確固たる意見を示すことはできないのですが、そういった観点から考えていく必要があるのかなと思います。

なお、データのみSIMに関しては、アメリカのアマゾンとかでも普通に販売されており、訪日前に購入されるという方もかなり多いようですので、これを変えていくということになると、相当大がかりなことが必要になる。それはU-NEXT様の御指摘のとおりかと思っています。慎重な検討が必要になるかなと思います。

感想めいたコメントになりますが、以上でございます。

【大谷主査】 貴重なコメントをいただいたと思っております。

ほかの構成員の皆様もいかがでしょうか。

それでは、沢田構成員、お願いいたします。

【沢田構成員】 ありがとうございます。

総務省におまとめいただいた1から6までの課題それぞれにつきまして、1から3までは、考え方の案に全く異論はないです。

4番目の追加回線の件で、何をどこまで確認するかですが、利用者としては、ID・パスワードだけというのはやっぱり不安ですし、パスワードにうんざりしているところもあるので、別の方法がいいと思っていました。

デジタル庁の本人確認ガイドライン、今まだ改定案の段階なのか、セットされたのか分かっていないのですが、その当人認証のレベル整理にしたがって申し上げれば、保証レベ

ル3がもちろんありがたいですが、せめて2にしてほしいと思いました。ID・パスワードプラス何かで認証してもレベル1と評価されるケースもあるようなので、2を最低ラインとしていただきたいと思います。

ただ、ドコモ様からApple Watchの御紹介があり、それだけあっても犯罪できそうな気はしないので、同じ番号でデバイスを追加するだけといったパターンは例外的にレベル1でもいいのかもしれません。ただ、悪用事案がもしも今後出てきたときには再検討ということかと思いました。

5番目の上限契約台数の件ですが、複数回線で問題になるのは、無断で譲渡するとか名義貸しとかと理解しました。余った回線を犯罪者に使わせることで小遣い稼ぎをするみたいなケース、これを防止することが目的なのかなと。

かつて詐欺的なECサイトで、振込先に使われている銀行口座が、留学生が日本でつくった日本の銀行の口座を母国に帰るときに売って行ったものというケースが随分あったようで、同じようなことがあったらまずいと思います。が、契約の段階では正規の契約、本人が契約していると思うので、契約時の本人確認の強化ではこれは防げないと思いました。

なので、4回線でも5回線でもそれ以上でも、上限というよりは目安を決めて、それを超える台数を契約したい人に、何に使うのかを聞くのはどうかと。先ほど楽天モバイル様から、御家族がたくさんいらっしゃるので集約すると御説明いただき、よく分かりました。そういう場合には、家族に使わせるという選択肢にチェックを入れればよいと思います。それ以外にどんな選択肢を設ければいいか、実ニーズがそれ以外にあるのかいまだに分からないので提案しようがないのですが、少なくとも利用目的が不明とか予備とかは駄目としておく、というようなことを考えてはどうかと。

いずれにしても申告ベースの話なので、犯罪防止の実効性という意味では、その申告内容が正しいかどうかというのを確認する必要があると思いますが、プライバシーの領域でもあり、あまり踏み込むのもどうかと思います。確認することの費用対効果も気になる場所なので、次善の策として、もしも申告内容と異なる利用が発覚した場合には、規約違反として既存の通信契約を全部解除しますみたいなことを1行入れて、そこに同意チェックを入れてもらうとかで少しは抑止効果があるのではないのでしょうか。課題1のところにも通じる話だと思います。皆様の御意見も伺えればと思いますが、えもし事業者の皆さんが合意できるのであれば、法律ではなく自主規制でも良いと思います。

課題6は結構難しいと思いながら伺っていましたが、少なくともSMS付きのデータSIM

については厳格な本人確認が必要ということで、皆さんもう合意されているので、そこは前提として、例外のところを精緻に議論する段階に入っていると思いました。それにはU-NEXT様の御発表でいただいたように、リスクが低いと考えられる理由と、どういうものを例外とすべきかをセットにした精緻な議論、専門家でない私は具体的なことは申し上げられないのですが、精緻な議論が必要と思いました。

顕在化した犯罪については警察庁様からの情報提供を待つとして、先ほど鎮目先生もおっしゃっていたかと思いますが、今後の悪用リスクとしてどんなことが考えられるか、抜け穴にならないよう犯罪者の気持ちになって、本人確認の必要性が低いものをリストアップして、その理由とともに抜いていく作業が要するという感想を持ちました。

【大谷主査】 ありがとうございます。

それでは、一通りメンバーの方からは質問や御意見を頂戴していたと思いますが、遅れて参加される御予定でいらした中原構成員はまだおいでになっていないのでしょうか。たしか事務局でお預かりいただいていたコメントがあると承っておりますので、差し支えなければ代読をお願いできないでしょうか。

【田中利用環境課課長補佐】 事務局でございます。中原構成員から事前にコメントをお預かりいたしましたので、読み上げさせていただきます。

論点4から6についてコメントいたします。前々回のヒアリングやほかの構成員の御意見を伺って、また、今回のヒアリングの資料を拝見して、個人的には問題の所在や方向性がある程度明確になったように思います。

追加回線は、1回線目とは別機会の契約であるという点に悪用されるリスクが定型的に見いだされるため、本来、本人確認をしっかりする必要があって、基本的には現状許容されている簡便な確認方法では足りない状況が生じてきているということなのかと思います。

音声SIM付きAppleWatch、デバイス追加にすぎない場合など、簡便な確認方法を残すべきケースがないか。今回全体を通じて、それらにも有意な悪用リスクがあるという指摘はなかったように思いますが、そう評価してよいかとさらに問われるという問題構造なのだと理解しています。それに対し、上限契約台数の問題は、複数の回線を持つことになるにせよ、同一の機械の契約でなされる限りは、そこでの本人確認をしっかりやればよいということになります。

問題は、多数台契約をすること、それ自体に怪しさはないか。また、それが現実化して不正に利用されれば、被害規模が大きくなるのではないかとこのところではありますが、複

数台契約のニーズは様々に想定されるのであって、現状こうしたあり得る負の側面を一律に語ることはできない。要するに、定型的な悪用リスクを想定できないということなのではないかと思います。常識的な範囲内での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事業者に継続してもらいながら、状況を注視していくことになるのかと思います。

こうした観点から考えた場合、データSIMについては、今回警察庁の資料によれば、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、筋論としては、本人確認の義務づけの対象となるのが原則であるということになるものと思います。

問題は、一定の観点から例外を設けるべきではないかということであり、1つはSMS機能がついていないものを除外するべきかどうか。あるいは、IoT機器等に利用されるものを除外するべきかどうか。これは悪用リスクの評価の問題なのではないかと思います。仮にそれが低い、あるいは今回のU-NEXTのヒアリング資料にあるように、技術的にコントロール可能であるというのであれば除外してもよいということになるかと思います。

もう一つは、プリペイドSIMを除外するべきか。これについても利用可能期間の限定などによる、悪用リスクの評価・コントロールの問題がありますが、より大きいのは、想定される利用者との関係での本人確認の現実的困難性の問題であると思います。訪日外国人のような人に対しても原則どおりの厳格な本人確認を要求するというのは、そのような人たちはデータSIMを使うなど言うに近くなる、サービス自体が立ち行かなくなるという問題ですが、筋論としてはこれについても本人確認それ自体は必要であって、検討すべきはその方法の緩和であるということかと思います。

前々回の事務局資料では、貸与時の本人確認の規律を参考にするという案が示されていましたが、どういうものがあり得るかについて、引き続き検討が必要ではないかと思いました。

以上でございます。

【大谷主査】 代読いただきまして、ありがとうございました。かなり論点に沿った形でコメントを頂戴したと思っております。

それでは、これまでいろいろ議論してまいりまして、6つの論点のうち、1番から3番までのところについては、おおむねその方向感が出てきていると考えておりますけれども、論点の4ですね。追加回線、それから5番目の上限契約台数、そして6番目のデータSIMのところにつきましては議論が尽きないところでございまして、引き続きたくさんの御意見をいただきましたので、本日寄せていただいた御意見を踏まえて、論点整理をさらに進

めていく必要があるかと思っております。

本日の御議論を踏まえて、次回のワーキンググループでまず事務局に取りまとめ案を御用意いただきまして、それをベースに議論を進めていきたいと思いますが、いかがでしょうか。

大丈夫ではないかと思しますので、特に異議はないようですので、そのように進めさせていただきたいと思います。

事務局から御連絡をお願いしたいと思います。

【田中利用環境課課長補佐】 次回会合は6月6日を予定しておりますけれども、詳細については別途事務局から御案内いたします。

【大谷主査】 ありがとうございました。

今日は、多岐にわたる論点につきまして、活発な御議論、そして貴重な御意見をいただきまして、誠にありがとうございました。

本日は、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9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誠にありがとうございました。閉会とさせていただきます。