

不適正利用対策に関するワーキンググループ（第13回）

令和8年7月9日

【園部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。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13回会合を開催いたします。

このたび、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電気通信事業部利用環境課課長補佐の園部でございます。

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

本日の資料は、議事次第と資料13－1から13－4までを用意しております。

注意事項は以上でございます。

また、本日は、鎮目構成員及び仲上構成員が御欠席となっております。

これ以降の議事進行は大谷主査にお願いしたいと存じます。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。

本ワーキンググループは昨年11月まで、不適正利用対策をめぐる環境変化を踏まえた新たな対策といたしまして、いくつかの議論を進めてまいりました。そこで、ひとまず議論の一区切りを迎えましたので、その後、総務省におきまして、このワーキンググループの議論を踏まえたルール化の検討を行っていただいたものと承知しております。

今回ルール化の検討結果も踏まえまして、ワーキンググループを再開させていただくことになりました。そこでワーキンググループの再開に当たりまして、利用環境課長の大内様から御挨拶をいただきたいと思います。どうぞよろしくお願いいたします。

【大内利用環境課長】 ありがとうございます。平素より情報通信行政に御理解、御支援いただきまして、感謝申し上げます。総務省利用環境課長の大内でございます。

本ワーキンググループの御議論を受けまして、通信サービスを悪用した特殊詐欺などの新たな不適正利用に対応するため、政府において本特別国会に携帯電話不正利用防止法の改正案を提出し、5月に可決成立をいたしました。まさに時宜を得た御提案をいただいたおかげであり、総務省を代表いたしまして、御礼申し上げたいと思います。

改正法の施行は公布後1年以内とされておりまして、利用者への周知であるとか、事業

者の方々の対応など、やらなければならないことは多くあるところでございます。本日は改正法の省令委任事項の明確化を中心に、施行に向けた御審議をいただく予定でございます。我々としても非常に気が引き締まる思いでございますが、引き続き、この規制、新たなルールの実効性と事業者の利便性のバランスをしっかりと図ってまいりたいと考えているところでございます。本日はどうぞよろしくお願い申し上げます。

【大谷主査】        ありがとうございます。

それでは、早速議事に入りたいと存じます。本日は、携帯電話不正利用防止法の改正に基づく制度整備の方向性につきまして、事務局から御説明をいただいた後に、警察庁様から、データ通信専用SIMの不正利用の実態につきまして御説明をお願いしております。その後に質疑応答を行いたいと思います。

そして、制度整備の方向性につきまして、一般社団法人電気通信事業者協会様、そして一般社団法人テレコムサービス協会様、この2つの事業者団体からヒアリングを行わせていただきまして、その後の意見交換に進みたいと存じます。

それでは、まず事務局からの御説明をお願いいたします。

【園部利用環境課課長補佐】        大谷先生、ありがとうございます。それでは、携帯電話不正利用防止法の改正に基づく制度整備の方向性について事務局から御説明をいたします。

1 ページ目でございます。まず、これまでの検討経緯でございます。本ワーキンググループにおける御議論の経緯を振り返りますと、特殊詐欺等における通信サービスの不正利用がさらに多様化・巧妙化した等の環境変化を踏まえ、昨年4月以降、携帯電話の本人確認のルール及び闇バイト、特殊詐欺対策等について検討を深めてまいりました。同年9月には、親会において報告書を取りまとめて公表いたしました。その後も本ワーキンググループにおいてさらに議論を深めていただき、本年1月には、その結果を研究会に報告いただきました。

議論の中では、制度整備を含めた方向性といたしまして、主に①データSIMの本人確認、②上限契約台数及び③法人の代理権について整理いただいたと理解しており、総務省においては、これ以降、法改正も含めた制度整備について検討を進めたところでございます。

2 ページ目でございます。こちら振り返りでございますが、昨年9月の報告書の内容でございます。先ほど申し上げた点と重複する点は割愛いたしますが、携帯電話の本人確認のルールにつきまして、主に6つの論点を御議論いただきまして、うち2、5、6につきまして、後ほど述べます法改正によって措置をされているところでございます。

3 ページ目でございます。携帯電話不正利用防止法の改正についてでございます。以上のような御議論を踏まえまして、政府においては、携帯電話不正利用防止法の改正法案を取りまとめまして、本年3月に閣議決定し、国会に提出いたしました。国会での御審議をいただきまして、本年5月に成立、公布を見たところでございます。

改正の内容について御説明させていただきます。第1に、データSIMの本人確認に関する改正でございます。まず、まさに本ワーキンググループにおいて御議論いただいた内容でございますが、1として、近年の詐欺におきまして、携帯データ通信が不正に利用されていることを踏まえ、データ通信専用SIMを本人確認義務等の措置の対象といたしました。これに伴い、2として、短期滞在外国人がデータ通信専用SIMを利用している実態を踏まえ、パスポート等による本人確認に関する規定を整備いたしました。具体的には、レンタル携帯電話に関する規定を参考として、通常、氏名、生年月日、住居である自然人の本人特定事項につきまして、短期滞在外国人にあつては、住居に代わる本人特定事項を定めるものでございます。住居に代わる本人特定事項につきましては、国籍及び旅券等の番号とすることを想定しております。この点、次のページに参考資料がございますので、必要に応じて御覧いただければと思います。3として、こちらもデータ通信専用SIMへの措置の拡大に伴う改正でございますが、メッセージアプリ等における携帯データ通信の不正な利用におきまして、当該メッセージアプリ等の運営事業者から犯罪に利用されたアカウントに紐付く情報の提供を受けるため、契約者確認の求めに必要な範囲に限りまして、警察から関係する電気通信事業者に照会をし、報告を求めることができる規定を整備いたしました。具体的には、警察署長におきまして、メッセージアプリ等のアカウントにSMS認証により紐付けられた電話番号などをメッセージアプリの運営事業者に照会することを想定していると聞いております。この点も、次々ページに参考資料がございますので、必要に応じて御覧ください。

大きく分けて2つ目、第2に契約回線数に関する改正でございます。こちらも本ワーキンググループにて御議論いただいた内容でございますが、4として、個人による利用が通常想定されない回線数の多回線契約につきまして、携帯通信事業者が役務の提供を拒否できる場合に、特定の個人に提供する回線数の合計が一定数を超える場合を追加いたしました。また、この改正は自然人を対象としていることから、5として、法人契約を抜け道とした不正な多回線契約を防止するため、また、在籍確認に関する携帯通信事業者間の運用を統一し、利用者の利便性を確保するため、一定の方法で法人の契約担当者等の在籍確認

を行う義務を追加いたしました。なお、以上の改正に伴いまして、法律の題名についても、音声を削除する形で改めております。

以上が法改正の内容でございます。4ページ目及び5ページ目は、先ほど述べました点についての参考資料でございますので、割愛させていただきます。

6ページ目でございます。携帯電話不正利用防止法の改正を踏まえた制度整備の方向性についてでございます。これ以降、本日の御議論の論点案について御説明いたします。

改正法では、改正法に基づく具体的な制度の内容につきまして、総務省令に一部委任しております。そのため、施行に向けまして、総務省令の改正などの制度整備を進める必要がございます。そこで、総務省といたしましては、これまでの本ワーキンググループにおける議論などを踏まえつつ、この制度整備に向け、主要な論点について事業者団体の皆様からヒアリングを行うとともに、先生方から御意見を賜りたいと考えております。

主な論点は3つあるのではないかと考えてございます。第1に、どのようなデータ通信専用SIMを本人確認義務等の対象とするか。第2に、携帯通信役務等の提供を拒むことができる回線数につきましてどのように定めるか、第3に、法人の契約担当者等の権限・地位の確認の具体的な方法についてどのように定めるかというものでございます。

以上の3点について、検討のスケジュールでございます。まず、本日の会合において、本説明の後、事業者団体からのヒアリングを実施いただきたいと考えてございます。事業者団体としては、電気通信事業者協会より主にMNOの立場からの御意見を、テレコムサービス協会MVNO委員会より主にMVNOの立場からの御意見を、御説明いただきたいと考えてございます。続いて、7月下旬に、今回の御議論を踏まえた論点の整理をお願いしたいと考えてございます。取りまとまりましたら、研究会に御報告いただきたいと考えております。

7ページ目でございます。まず第1の論点、本人確認義務等の対象となる電気通信役務の範囲でございます。改めて改正法の内容について御説明いたします。現行法上、本人確認義務等の対象となっていなかったデータ通信専用SIMにつきまして、不正利用の実態を踏まえ、本人確認義務等の対象とするものでございます。この点、赤字部分でございますが、具体的な対象役務、すなわちSIMの種類につきましては、総務省令で定めることとされているものでございます。

よって、主な論点といたしましては、改正前の対象であった音声SIMに加えまして、どのようなデータ通信専用SIMを本人確認義務等の対象に乘せるかということでございます。まず、警察庁の調査では、本人確認なく不正利用されていたSIMの多くがSMS機能付きのも

のであったということを踏まえまして、SMS機能付きのデータ通信専用SIMを対象とすることにつきましてどのように考えるか。また、下段に報告書の抜粋をつけてございますが、具体的な対象役務については、利便性と実効性のバランスを確保しながら検討すべき論点ではないかと考えてございます。これらを勘案いたしまして、例えばIoT機器向けのSIMを対象外とすることが考えられるのではないかと承知してございますが、この場合、どのようなものを対象とするか。利用用途や機能制限の有無などの切り口が考えられると承知してございます。

なお、警察庁の調査につきまして、昨年第9回会合で警察庁から御発表いただきましたが、その後の状況も含め、後ほど警察庁より御説明をいただきたいと考えてございます。

8ページ目は、改正後の携帯電話不正利用防止法の条文を付けているものでございますが、割愛いたします。

続きまして、9ページ目でございます。第2の論点、役務提供拒否を可能とする回線数でございます。改正法の内容について説明させていただきます。現状、多回線契約につきましては、主要な携帯通信事業者において自主的な対策が講じられており、一定の成果を上げていると承知してございます。他方、これが不十分な携帯通信事業者を標的といたしました不正な転売などの事案が発生しているほか、事業者によって異なる運用が利用者にとって分かりにくい等の課題が指摘されていると承知してございます。これらを踏まえまして、改正法では携帯通信事業者が役務提供を拒否できる場合に、特定の個人に提供する回線数の合計が一定数を超える場合を追加することとしてございます。この点、赤字の部分でございますが、役務提供拒否を可能とする具体的な上限回線数につきまして、総務省令で定めることとしてございます。

よって、主な論点といたしましては、携帯通信役務等の提供を拒むことができる回線数、すなわち通信可能端末設備の数につきまして、どのように定めるかでございます。まず、主要な携帯通信事業者、具体的には電気通信事業者協会の所属事業者でございますが、自主的に設定されている「原則5回線」を踏まえまして、具体的にどの程度の上限数を設定するかでございます。この点、後段でございますが、SMS機能付きのデータ通信専用SIMについても、別途同数の上限を設定することとしてはどうかというところでございます。また、「ただし」としている点でございますが、次ページにおいて本ワーキンググループの報告を抜粋しておりますとおり、本規定については、利用目的等を踏まえた利便性への配慮も必要と承知してございます。この点、正当な利用用途が確認できる場合等、不正な利

用のおそれが低い場合を上限の例外とすることについて、どのように考えるかでございます。例えば、家族の利用者登録が行われている場合などについてどのように考えるか整理する必要があるのではないかと考えてございます。

10ページ目及び11ページ目につきましては、それぞれ報告書の抜粋及び改正後の条文でございますので、割愛いたします。

12ページ目でございます。最後に、第3の論点として、代表者等の権限・地位確認の方法でございます。改正法の内容について説明いたします。現状、法人契約や自然人の代理人による契約等につきまして、契約担当者等、すなわちこの法律におきましては代表者等と呼ばれているものでございますが、その権限・地位の確認は法律上義務付けられておらず、携帯通信事業者によっては十分な確認が行われておりません。この点、個人の多回線契約のルール整備に伴いまして、法人契約における不正な契約の増加が懸念されるほか、本ワーキンググループにおいても御指摘いただいておりますとおり、運用が携帯通信事業者によって異なることが利用者にとって分かりづらいといった側面もございます。こちらを踏まえまして、改正法では、一定の方法により、代表者等が契約者に代わって契約締結を行う権限・地位を有していることの確認を義務付けております。この点、赤字部分でございますが、具体的な権限・地位の確認方法につきましては、総務省令で定めることとしているものでございます。

よって、主な論点といたしましては、法人の契約担当者等の権限・地位確認の具体的な方法といたしまして、どのようなものを定めるかということでございます。まず、他の法令における規定や利用者の利便性、あるいは用いる書類の偽造可能性などを勘案する必要があると承知してございまして、これらを踏まえまして、資料に記載してございます5つの方法を認めることにつきまして、どのように考えるかというものでございます。重要なものをピックアップいたしますと、例えば③の委任状等の提示を受ける方法、④の電話をかける等の方法でございます。

13ページ目でございます。名刺や社員証の取扱いでございます。現状、携帯通信事業者の自主的な運用において、名刺や社員証が利用されている場合があると承知してございます。他方、これを制度化するに当たりましては、これらの書類の偽造が比較的容易なのではないか、また、その法人に所属していることは証明できても、契約締結の権限・地位そのものは証明できないのではないかとといったことを踏まえ、認めないこととしてはどうかという論点でございます。最後に、報告書の記載を抜粋しております。

14ページ目以降につきましては、参考資料でございますので、割愛いたします。

以上、事務局からの御説明でございます。どうぞよろしくお願いいたします。

【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、警察庁のサイバー警察局サイバー企画課の根本サイバー企画官様から御説明をいただきたいと思います。

【根本サイバー企画官】 警察庁サイバー企画課の根本でございます。どうぞよろしくお願いいたします。私から、データ通信専用SIMの不正利用実態について御説明をいたします。

昨年5月の第9回会合におきましては、データ通信専用SIMの不正利用実態について説明いたしましたが、このときには、SNS型投資・ロマンス詐欺に係る事件に使用したSMS機能付きのデータ通信専用SIMを対象としており、対象が限定的であったことから改めて調査を行っております。

今回皆様にお示ししております資料は、令和6年9月から令和7年5月までの9か月間において、各都道府県警察のサイバー犯罪対策部門及び刑事・組織犯罪対策部門が把握をしている、データ通信専用SIMが犯罪に利用されていたサイバー犯罪事件、特殊詐欺事件等について、事案概要やデータ通信専用SIMの種別、本人確認状況等の調査を行ったものであります。この調査は各事件捜査における事業者への照会結果に基づくもので、その回答内容から、SIM種別や本人確認の有無が判然としない場合や、照会先事業者と連絡がつかないものについては、いずれも不明としております。

それでは、資料の内容について御説明をいたします。

まず、資料の左側の円グラフでございますが、本調査により不正利用が確認をされたデータ通信専用SIMはトータルで708枚であり、そのうち、本人確認されていたものは30枚、30枚というのは、この円グラフでいう青の部分が相当いたします。割合では4.2%でございます。また、本人確認をしていなかったものが458枚、円グラフでいうとだいたい色の部分で、割合では64.7%でございます。また、本人確認の有無が不明だったものが220枚、31.1%ございました。

続いて、今回の708枚のデータSIMの種別の内訳について、「参考」のところに記載をいたしております。708枚のうち、SMS機能付きが458枚、割合でいいますと64.7%、また、SMS機能なしが87枚、割合でいうと12.3%、また、SMS機能不明が163枚、23.0%となっております。さらに、このSMS機能付きデータ通信専用SIM458枚の本人確認の有無の内訳に

については、本人確認ありが23枚、割合では5.0%、また、本人確認なしが379枚、割合では82.8%、また、本人確認の有無不明が56枚、割合では12.2%という結果となっております。一部の事業者におきましては、データ通信専用SIMについても、自主的な取組として、音声SIMと同等の方式で本人確認が行われていることは承知をしておりますが、今回の調査では、データ通信専用SIM全体でも6割以上、SMS機能付きのデータ通信専用SIMにあっては8割以上で本人確認がなされていないという状況でありました。このように、本人確認がなされないデータ通信専用SIMについては、犯行に利用するSNS等のアカウントの作成、不正送金やクレジットカード不正利用時の通信、犯行グループ内での連絡時の通信に不正利用されている実態が確認をされているところでございます。

簡単ではございますが、私からの説明は以上となります。ありがとうございます。

【大谷主査】 御説明ありがとうございました。

それでは、ここまでの事務局、そして警察庁からの御説明につきまして、御質問がありましたらお願いしたいと思います。制度整備に関する論点についての意見交換につきましては、事業者団体からのヒアリングを行った後に進めていきたいと思いますので、まず質疑応答の時間とさせていただきますと思います。いかがでしょうか。

まず私のほうから一言、警察庁の根本企画官様に教えていただきたいのですが、一部本人確認がされているものがあったわけですが、やはり本人確認がされていると足がつく、犯人にたどり着きやすくなると理解してもよろしいものなのでしょうか。

【根本サイバー企画官】 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。

警察では様々な情報を総合的に活用して捜査を進めております。そういった観点で、本人確認がされているものであれば、それだけ活用できる情報が増えますので、そういった意味で捜査に有利になると考えております。

以上でございます。

【大谷主査】 どうもありがとうございます。捜査上も有用な情報になり得るということでございますね。御質問はよろしいでしょうか。

ありがとうございます。山根構成員から、お願いいたします。

【山根構成員】 山根でございます。警察庁様に御質問でございまして、最後少し御説明いただいたんですけども、不正利用というときの使われ方についてなのですが、SNSのアカウントの認証に使われたり、犯行時の連絡に使われたりという状況の御説明があったかと思うんですが、SMS機能付きのものとSMS機能なしのものでの使われ方の違いがあれ



ば、これまでのワーキングの議論の中でも少し御説明の機会もあったかと思うのですが、改めて御説明いただきたいと思います。

【根本サイバー企画官】 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機能付きのデータ通信専用SIMとSMS機能なしのデータ通信専用SIMの悪用の実態でございますが、全体的に見ますと、SMS機能付きのデータ通信専用SIMについては、おっしゃるとおりSNSのアカウントの作成に悪用されている実態が目立っております。一方で、SMS機能なしのデータ通信専用SIMについては、こちら当然SMSを送受信できませんので、アカウントの作成の利用に使うことができず、先ほども申し上げましたとおり、犯行グループ内での連絡時の通信であるとか、そういった悪用が目立っているところでございます。

以上でございます。

【山根構成員】 ありがとうございます。どの機能を対象にするかという議論の中で、どれぐらいリスクがあるかは重要なポイントになるかと思ひまして、その検討に当たって、どのような不正利用の実態があるかについては1つ重要になってくるかと思ひましたので、念のため確認させていただいた次第です。

【大谷主査】 大変貴重な御質問いただきまして、ありがとうございました。ほかの構成員につきましてはいかがでしょうか。

そもそも本人確認の有無が不明なものが非常に多いことは、なかなか驚きではあったのですが、調べても分からなかった、問合せいただいても分からなかったということですね。

それでは、次に進ませていただきまして、意見交換の中で疑問点等が出てきましたら、それぞれの方に御回答いただくようにしたいと思います。

続けてまいりたいと思いますが、携帯電話不正利用防止法の改正に基づく制度整備の方向性につきまして、事業者団体様へのヒアリングを行いたいと思います。一般社団法人電気通信事業者協会、それから一般社団法人テレコムサービス協会からの御説明をお願いいたします。その後にとりまとめて質疑応答の時間を取りたいと存じます。

それでは、一般社団法人電気通信事業者協会の丸山様から御説明をお願いいたします。

【TCA（丸山）】 電気通信事業者協会の丸山と申します。よろしくお願いいたします。

では、携帯電話不正利用防止法改正への対応検討、制度整備の方向性につきまして、意見を御説明いたします。今回論点3点ございましたので、その3点それぞれにつきまして意見を申し上げます。

まず1点目がデータ通信専用SIMの本人確認義務の対象についてとなりますが、まず、

今回SMS機能付きデータ通信専用SIMを対象とする方向性については賛同いたします。なお、SMS機能なしデータ通信専用SIMにつきましては、現状モバイルWi-Fiルータ等の多様な用途で利用がされているところがございますので、お客様の利便性への影響等を考慮して、今回は対象外することに賛同いたします。

その上で、SMS機能付きデータ通信専用SIMの本人確認義務の対象の考え方ですが、不特定多数へのSMS送受信が技術的に制限されるデータ通信専用SIMについては、不正利用のおそれが低いと考えられることから、今回の本人確認義務の対象外とすることを要望いたします。例えば、IoT機器等の制御監視ですとか、あるいは子供・高齢者の方の安全管理による見守り等において使われているSMS機能付きデータ通信専用SIMについては、本人確認義務の対象外とすることを要望するものです。SMS送受信が技術的に制限されるという点につきまして、下の方に4点ほど例を挙げております。例えば、SMS送信先の電話番号数がそもそも制限される場合、閉域網を構築した上で通信利用されている場合、あるいはIoT機器や特定サーバ等の機器同士の通信利用がされている場合、あるいはSIMを差し替えた際にその通信利用を制限できる仕組みが入っている場合は、不特定多数へのSMS受信の技術的制限ができていない例となるのではないかと考えております。

続いて、2点目の携帯通信役務等の提供を拒むことができる回線数についてとなります。こちらは先ほど御紹介もありましたが、TCAの自主基準として現状個人契約における音声SIMの上限契約回線数を原則5台に制限する運用を行っております。こうしたTCAの自主基準も参考としていただきまして、個人契約において役務等の提供を拒むことができる回線数、いわゆる閾値については、音声SIM、それから今回法令対象となるSMS機能付きデータ通信専用SIM、それぞれ5回線ずつの形で設定するのが適当と考えております。

続きまして、法人の契約担当者等、いわゆる代表者等の権限・地位確認についてでございます。こちらにつきましては、先ほど御紹介いただきました権限・地位確認の具体的方法や名刺・社員証について取扱い不可とする方針については、当協会としても一定の合理性があると考えております。その上で、権限・地位の確認の点につきまして、例えば契約担当者が前回契約時と同一と確認された場合については、その権限・地位の確認を省略可とすることを要望いたします。下に簡単にイメージを記載しており、新規回線契約時と追加回線契約時がございますが、新規回線の契約時においては、法人の本人確認、契約担当者の本人確認を行い、その上で契約担当者の権限・地位確認を行うことになると思っております。ここで、先ほど御紹介のありました委任状や架電による確認が行われることにな

りますが、その後、その下段にあります追加回線の契約申込みがあった場合、当然ながら法人の本人確認と契約担当者の本人確認は行うこととなりますが、ここで契約担当者の本人確認を行った場合において、契約担当者が前回契約時と同一であることが確認できた場合は、権限・地位の確認を省略可としても良いのではないかと考えているところです。

なお、「※」のところで、契約担当者の本人確認についても触れておりますが、現状追加回線契約時の本人確認につきまして、法人の本人確認については本人確認記録との照合による確認が可能とされております。一方で契約担当者につきましては、そうした本人確認記録との照合による確認は現状認められておりませんので、再度書類での本人確認を行うこととなります。この点、契約担当者の本人確認において、回線契約の申込みの都度、書類等による本人確認が必要となる点につきましては、相手方の法人様と携帯電話事業者双方にとって負担となる点が現状も見られておりますので、触れております。

以上、当協会からの御説明になります。ありがとうございました。

【大谷主査】 丸山様、どうもありがとうございました。

それでは、続きまして、一般社団法人テレコムサービス協会の井原様から御説明をいただきます。

【テレコムサービス協会（井原）】 資料13-4について説明いたします。2ページ目から4ページ目までは当協会の概要でございますので、説明は割愛いたします。

5ページ目を御覧ください。本日の説明は、こちらの28社からの意見をまとめたものでございます。

6ページ目を御覧ください。まず、データSIMにおける本人確認義務の対象についてです。SMS機能のないデータSIMについて本人確認義務の対象とした場合、利用者の利便性への影響が非常に大きく、また、SMS機能のないデータSIMにはSIM特有の不正利用のおそれが少ないため、本人確認義務の対象としないことに賛同をいたします。ただし、SMS機能付きデータSIMの場合であっても、IoT機器向けなどの不正利用のおそれが想定しにくいと考えられるものについては対象外とすべきと考えますので、下表の「用途」、「機能」、「差し替え可否」の視点を踏まえて御検討いただきますようお願いをいたします。

7ページ目を御覧ください。役務提供拒否事由としての上限回線数についての意見でございます。まず音声SIMについて、不正利用抑止による役務提供拒否事由として、上限回線数原則5回線を基本とする考え方に違和感はありません。また、音声SIMとSMS機能付きデータSIMでは、利用用途や不正利用リスクが異なることから、音声SIMとSMS機能付き

データSIMのそれぞれに上限回線数を設定することについて賛同いたします。なお、家族利用等での多回線ニーズや、今後の技術進展によるIoTデバイス等への利用用途の拡大を踏まえると、それらを不当に制限しないことが重要ではないかと考えております。

8 ページ目を御覧ください。法人契約における契約担当者の権限・地位確認についてです。現段階では、お示しいただいている①から⑤までの方法を原則とすることで問題ないと考えております。一方、解釈の違いによって、事業者側の確認方法や確認結果が異なることを避ける必要があると考えます。実施に当たり、事業者に求められる具体的な運用方法や対応について明示いただきますようお願いをいたします。また、法人契約は個人契約に比べますと、同一顧客からの追加回線契約を承る機会が多いところ、既取引実績がある法人契約については不正利用のリスクが低いことから、利用者側の申込手続の負担軽減のために、追加回線契約時は代表者等の権限・地位確認を省略できるようにお願いいたします。なお、名刺や社員証等を確認する方法は、書面の偽造が比較的容易であると考えられますので、不正契約抑止の観点から認めないことに違和感はありません。

MVNO委員会からの説明は以上でございます。

【大谷主査】      ありがとうございました。

それでは、この事業者団体様からの御説明につきまして、御質問がありましたらお願いしたいと思います。いかがでしょうか。

それでは、星構成員、どうぞよろしくお願いいたします。

【星構成員】      東京都立大学、星と申します。ありがとうございます。

TCA様、それからテレコムサービス協会様からお話をいただきまして、状況について私なりに理解をさせていただいたところでございます。これは皆様方からいただいた御意見にどうこうということではなく、事実について確認をさせていただければと思います。本当に現状が分かっていないというだけのことなのですが、TCA様のほうから、既に自主規制という形である程度の本人確認のようなことをされているというお話を伺っているんですが、現状において、特に実務上のお困り事があるとか、あるいは利用者側からこういう不満が一定程度見られるとか、そういうことがあるのかなのか、あるのであればどういったようなものがあるのか教えていただければと思います。それが1点目でございます。

もう一つ、法人契約での法人の本人確認について、例えば回線の追加といった場合であれば、例えば支払い方法については、従前の支払い方法をそのまま使うという形なのか、契約の際の支払い・決済手段の確認はどのような形で行っているのかということを、差し

支えのない範囲で教えていただければと思います。

【大谷主査】 それでは、今いただいた御質問について、それぞれの団体から御回答をお願いしたいと思います。それでは、電気通信事業者協会様から順にお願いいたします。

【TCA（丸山）】 電気通信事業者協会の丸山です。御質問ありがとうございます。

1点目はデータ通信専用SIMに関する本人確認の状況とのことで、現状、我々では、データ通信専用SIMにつきましても音声SIMと同等の本人確認を行っております。こちらにつきましては、特にお客様から何か御指摘をいただくとの懸念はございませんし、事務処理の面でも音声SIMと同じ事務処理で本人確認を行うことで、特に何か課題があるようなこととはなく運用できていると思っております。

また、先ほど御説明しましたとおり、法人契約における本人確認につきましては、課題として捉えている点を説明させていただきましたが、契約担当者の本人確認を都度行うことにつきましては、携帯電話事業者内で指摘、意見のあるところではございました。

2点目の法人契約における支払い手段の確認につきましては、基本的にはその法人様から申し出ていただいて支払い方法が決まっていくものと思っておりますが、正直、両面あると思っております。前回と同じ支払い方法を使われるケースもあれば、今回の契約については別な支払い方法を選択されるケース、両方あり得ると思っております。

以上でございます。

【星構成員】 ありがとうございます。

【大谷主査】 同じ御質問について、テレコムサービス協会からもお願いします。

【テレコムサービス協会（井原）】 テレコムサービス協会の井原でございます。御質問いただいた法人契約の際の追加回線における支払い方法につきましては、MVNO各社によって対応が異なるかと思いますが、おおむね先ほどTCA様が御説明された内容と大きく変わりないと思っております。法人様におきましては様々な支払い方法があったり、回線ごとに方法を分けられたりする可能性も出てくるかと思しますので、法人様と相談をさせていただきながら、支払い方法を決定する形になっているかと思われます。

以上でございます。

【星構成員】 ありがとうございます。そういったようなプロセスを踏んだ上で、当然のことながら、支払いがしっかり確保できていなければ簡単に契約に応じられないという実情はあるという理解でよろしいわけですね。ありがとうございます。

【大谷主査】 御質問いただきまして、ありがとうございました。

それでは、ほかの方からはいかがでしょうか。私からも御質問させていただきたいのですが、両方の団体様に対してなのですが、先ほど警察庁から御説明いただいたSIMの本人確認の有無が不明のものが、かなり相当数、220枚あるとのことでしたが、本人確認の実施状況が後で確認されたときに分からないというのはどのようなケースが考えられるのか教えていただければと思います。TCA様から順番にお願いしてもよろしいでしょうか。

【TCA（丸山）】 電気通信事業者協会の丸山です。先生、ありがとうございます。

今、我々の取組としては、データ通信専用SIMの場合においても本人確認を音声と同等のレベルで行うことをルールとしておりますので、基本的には本人確認がされていないデータ通信専用SIMはないと考えております。警察の捜査の結果、本人確認がされていたかどうか不明のものにつきましては、我々の立場ではその理由がうまくイメージがつかないところなのが正直なところでございます。

以上です。

【大谷主査】 ありがとうございました。

続きまして、テレコムサービス協会の井原様、お願いいたします。

【テレコムサービス協会（井原）】 御質問ありがとうございます。

MVNOとしましても、現状、MVNO委員会の中では、2021年から、SMS機能付きのデータSIMについては音声SIMと同様の厳格な本人確認を実施するという事で申合せを行ってございまして、MVNO委員会に加盟している全ての事業者が参加しているわけではございませんが、おおむね本人確認を音声と同様に実施をさせていただいているところでございます。ただし、現状の携帯電話不正利用防止法上では、データSIMにおいては音声SIMと同様の本人確認は義務化されていないこともありまして、MVNOの中では当然本人確認を行っていない事業者も存在しているかと思っておりますので、その際、問合せをいただいた際に、本人確認が実施されていない状況は実際発生しているのではないかとと思われます。

以上でございます。

【大谷主査】 ありがとうございます。皆様の自主的な対応の外で本人確認ができない可能性がありますと、やはりアウトリーチ、制度上の対応がとても重要になると考えられるところです。

ほかに御質問がないようでしたら、意見交換に入らせていただければと思います。

それでは、事務局からいただいた資料の6ページ目に、今回、方向性を議論したい内容があります。特に順番は決めますので、それぞれ御意見をいただければと思います。

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】      いろいろ御説明ありがとうございました。

総論として、今までのワーキンググループでの議論の内容を適切に反映していただき感謝申し上げます。もちろん大きな方向性には異論がございません。関係事業者も基本的に賛同していただいているようで、良かったと思いました。

まず、(1) について意見を申し上げたいと思います。SMS機能付きのデータ通信専用SIMをまずは対象とすることはもう既定路線で、過剰規制にならないようにというのも全くそのとおりに思っております。ですので、今後はその中で何を対象外とするかが焦点となると理解していますが、同時に、なぜ対象外として良いかという検討が必要だと思います。先ほどいろいろお示しいただいた点もありますが、今回の見直しの目的は、不正利用の抑制と追跡可能性の確保ということかと思しますので、不正利用の可能性をゼロにすることは現実的ではないかもしれませんが、犯罪者にとって、不正を行うには費用対効果が悪いという状態になれば良いと思います。

今まで御提示いただいたもののほか、問題が無いのではないかとされるケースを紹介させていただきたいのが、フードデリバリー業界の例でございます。Uber Eats、出前館、menuといったサービスを思い浮かべていただければと思いますが、それぞれプラットフォームとして、自社のシステムを組み込んだ端末を飲食店にレンタルしている実態があります。カウンターに端末が並んでいる様子を御覧になったことがある方もあると思います。注文が入ると店側ですぐ分かる、注文番号が付与されて配達員と共有するといったことに使うため、その端末にはデータ専用SIMが組み込まれています。プラットフォームは電気通信役務を提供する者という位置付けになるかと思います。このデータ専用SIMにSMS機能がない場合は、今までの流れからも問題ないという扱いで良いと思いますが、SMS機能があったとしても、プラットフォーム側で一元的に端末を管理する機能を持っていて、それによって、技術的にSMSを送受信できない状態にすることができる、もしSIMの抜き取り等の異変があった場合には、すぐに検知・無効化することができて、もちろんログが残ることです。特殊詐欺に使うSIMが欲しい犯罪者にとってみると、そこを狙ったとしても、手間とリスクに比べて得るものがあまりないと言えるのではないかと思います。そういった点に着目して、省令で対象外とするカテゴリーは、例えば「IoT機器向け」というような形で列挙するよりも、原則は本人確認等の対象としつつ、こういう機能制限とか安全管理がされていれば免除するという構成とする、つまり機能要件を書き込んだ方が技術

中立的ですし、将来の環境変化に応じた見直しがしやすいのではないかと思います。その機能制限に関しては、先ほどTCAさんやテレコムサービス協会さんからも御紹介があったとおりかと思いますが、例えば通信機能が限定的であることとか、事業者による一元管理ができて、異常時の即時対応ができるといったことを書き込めれば良いのではないかと思います。たまたまフードデリバリーの例を挙げましたが、自動販売機、POS端末、車両管理など、色々なことに応用ができると思います。ただ、その機能要件を満たしているかを誰がどのように確認するかという課題は残り、その点は考えなくてはいけないかもしれないと思いました。

長くなりそうなので、取りあえずこの1点だけ申し上げます。ありがとうございます。

【大谷主査】      ありがとうございました。

続きまして、辻構成員から御意見を頂戴したいと思います。その後に沢田構成員におかれては、言い残したことがあると思いますので、もう一度御発言いただければと思います。

【辻構成員】      よろしくお願いいたします。

まずは論点1点目ですが、警察庁さんの御発表もありましたが、やはりSMSが使えるか使えないかはすごく大きなポイントになっているということはよく分かりました。それが不明だということは、私もすごく気になったのですが、それはともかく、やはりSMSが使えるものはしっかり規制対象にすべきではないかという点はそのとおりかと思います。

また、先ほど沢田さんもおっしゃっていたのですが、私はどちらかというデジタル側の人間なので、IoT向けの制限となると競争力が無くなることは、実際そうだと思っておりますので、IoT向けの利用を考慮することは重要だと思いますが、テレコムサービス協会さんの発表のような整理は、整理としてはいいと思いますが、曖昧というか、現実はどう判別されるのか見えないことが少し気になりました。もしかすると、そのサービスの種類の判断ができる仕組み等も含めて検討しないと、曖昧にならないかという点は少し気になります。この点に関しては、まずSMS機能付きはちゃんと管理する。「IoT」という言葉に関しても、定義・確認方法を少し整理した方が良いということが論点1点目です。

次に、回線数です。私は、このワーキンググループで以前より何度か発言させていただいていますが、この「原則5回線」について、前回か前々回の会議でも議論がありましたが、事業者さんによってはこの5回線という数字が、利用者のメリットを制限していることにもなっていると思えるのですが、とりあえず私は、5回線という数字の妥当性がよく分からないとよく思っていて、先ほどの事業者団体の御発表にもありましたけれども、



「5で良いのではないか」というように、従前の数字を引っ張るのは少しどうかと思うところであります。下段のように、正当な利用用途が確認できる場合、上限の例外を検討することは正しいかと思っていまして、基本的には回線を増やすときの確認をしっかりと行い、やはり、確認を行う上で必ずしも5回線である必要はないという考え方があってもいいのではないかと考えております。「5」として、5回線で済んでいる人と済まない人の大きな差ができてしまうのは良くないのではないかと考えております。

最後の点ですが、私は、名刺や社員証での確認は曖昧な確認だと思っていまして、より厳密な確認を行うことはよろしいと思います。論点として、①から⑤まで書かれておりますが、これを紙・対面で行うのか、電子的な方法で行うのかという点、電子的な方法の可能性に特に具体的に言及されていないことが少し気になりました。GビズIDというものがあって、GビズIDは法人だけなのですが、そういった仕組みの上でしっかり電子的に確認できる方法であれば取り入れていくということを、それこそこれまでのeKYCの議論と一緒にと思いますが、少し添えていただいた方が良いのではないかと考えました。

ということで、3点私からコメントさせていただきました。ありがとうございます。

【大谷主査】 貴重なコメントをありがとうございました。確かに最後の点、何か「紙っぽい」感じが伝わってきますが、もちろん電子的なものも排除されていないのだろうと想像しております。具体例として何か示せば、イメージに合った形になるのではないかと考えながらお聞きしました。

続きまして、中原構成員から、よろしくお願いいたします。

【中原構成員】 それぞれの論点についてであります。まず、(1)の本人確認義務等の対象となる電気通信役務の範囲につきましては、本日の警察庁のプレゼンテーションによりますと、本人確認のされていないSMS機能付きデータSIMの不正利用の実態が顕著に認められると思いますので、これを本人確認義務等の対象とすることは適切であると思います。その上で、用途・機能に即して具体的な対象を列挙していくのか、それとも全体に規制をかけた上で不正利用のおそれが小さいものを除外していくのか、規制の在り方として1つの問題であります。不正利用の実態が明確な中で規制漏れが生じることは望ましくないので、後者のように規制対象外のものを列挙する方式が望ましいと思います。私も沢田構成員、辻構成員の御意見を聞いて、用途だけではなく機能面に着目した規制も検討すべきではないかと考えました。

(2)の役務提供拒否を可能とする回線数につきましては、改正法によれば総務省令で

具体的な数を定めることとなっており、ここでも用途等に応じてその回線数を定めていくのか、それとも原則的な回線数を定めた上で例外を列挙するのかという問題があるかと思っています。現状の事業者の自主的な取組との連続性という観点からは後者が望ましく、「5」という数字の妥当性はなお検討の余地があるのかもしれませんが、原則的な回線数を定めた上で、正当な利用用途が確認できる場合等を例外として扱うのが穏当だろうと思います。ただ、この正当な利用用途というのは、(1)の不正利用のおそれが小さいものにも増して多様であるように思われますので、省令だけではなく、ガイドライン等で指標を示すことが特に求められると思います。

(3)の代表者等の権限・地位確認の方法につきましては、これまで法的な規制が無かった中で、望ましくない確認方法を排除しつつ、利用者及び事業者の負担を考慮した現実的・合理的な確認方法を一般的に定める、そういった課題なのだろうと思います。名刺・社員証を確認する方法は認めないことについては賛成でありますし、①から⑤までの方法は犯収法も参照したものと伺っていますが、犯収法という前例をさしあたり踏襲した一般的な枠組みを立て、今後の推移を見ていくことも合理的であると思います。本日の事業者団体ヒアリングで共通して御要望があった、追加回線契約時の確認の省略につきましては、論理的には追加回線契約までにその者が代理権を失うことはあり得ますが、しかし、レアケースであるように思います。もともと規制が無かったところに規制を設けるという今回の経緯からすると、こういった点については、さしあたり事業者の負担とならない仕組みとしておいて様子を見ていくということでもよいのではないかと思います。

以上です。

【大谷主査】 貴重な御意見ありがとうございました。特に指針、ガイドライン等で、きめ細かに補足していくことの重要性等を御指摘いただいて、なるほどと思った次第です。

続きまして、山根構成員からお願いいたします。

【山根構成員】 私といたしましても、全体的な方向感としては、基本的には違和感ないものでして、その上で、個別の論点についてコメントさせていただければと思います。

まず、1点目の本人確認義務等の対象となる電気通信役務の範囲につきましては、先ほどの警察庁様の御発表にもあったとおり、やはりSMS機能付きのデータSIMには不正利用の実態も広く認められているとのことで、ここを一般的には対象にしていく方向で違和感ないところです。SMS機能なしのものについても、一定の不正利用の実態があるところではあるかと思いますが、現状で把握できている範囲では、SMS機能付きの場合と比べると、

そこまで不正利用は広がっていないことと、定性的なリスクの面で見ても、やはりSMS機能付きのものであるとSNSのアカウントの作成に利用され、従前のワーキンググループの発表の中で金融サービスのアカウントの作成等にも利用されているとの話があったと記憶しており、やはりこういった、定性的な不正利用のリスクという面でも、SMS機能の有無で差分があるのではないかとと思います。こういった定性的なリスクの程度と、現状の不正利用の実態を踏まえて、SMS機能なしのものには、現状の段階としては本人確認義務の対象とはせずに、SMS機能付きのものを対象とする方向で良いのではないかと考えます。

また、SMS機能付きのものにつきましても、IoT機器向け等のSIMは対象外とするという点につきましては、やはりリスクの程度という点で見ると、一定の技術的な機能制限がかかっているものについては、定性的な不正利用のリスクは低いと言えるのではないかとと思いますので、そういったものについては例外的に対象から外していく形で良いのではないかと考えているところでございます。

続きまして、2点目の役務提供拒否を可能とする回線数のところでして、他の構成員からも御指摘があったとおり、5回線で良いのかという点は、現状5回線で実務上もあまり支障なく運用されているという話も従前あったかと記憶しておりますので、1つの目線になる数字かと思っております。なぜ5回線なのかという理由づけは、もう少し要素があったほうが良いのではないかとと思いますが、最後、ここはもう一定の基準を省令で定めることになっていますので、ある意味、最終的には決めの問題になってしまう気もしております。この5回線というところが、やはり目線になるのではないかと考えております。

また、役務提供拒否の規定につきましては、もともとの趣旨として事業者による自主的な取組を促進するというのがあったかと思っておりますので、制度をつくっていくこともさることながら、事業者の自主的な対応において、多数の回線契約についてきちんと必要性を確認していくこと、多数に上る場合には実際に役務提供を拒否する運用を確立していくこと、そういった取組をしていくことも重要になるのではないかと考えております。

最後、代表者等の権限・地位の確認の方法については、こちらは基本的に事務局にまともていただいたもので違和感ないところでして、名刺や社員証につきましては、やはり書いていただいたとおり、偽造の容易性等を踏まえて認めないということで良いかと思えますし、こちらの①から⑤までの確認方法も、先ほど中原構成員から御指摘もありましたとおり、犯収法の規定を参考にしたものと理解しており、確認方法として、犯収法に基づく実務の蓄積もあろうかと思っておりますので、それに倣ってこういった規定にする形で違和感な

いかと思っております。

【大谷主査】 山根構成員からもコメントをいただき、方向性について概ね賛同の御意見を頂戴いたしました。特に、これまでの事業者の自主的な御対応を尊重するという方向性についてコメントをいただけたと思います。

それでは、沢田構成員には、このタイミングで残りの御意見をいただきたいと思います。が、いかがでしょうか。

【沢田構成員】 先ほど申し上げなかった（２）（３）について意見を申し上げます。

（２）の回線数のところですが、私も皆様と同様に、業界の自主ルールを踏襲する形で、音声SIMとSMS機能付きデータ通信SIMと、それぞれ５回線で異論は無いです。それを超える分につきましては、もちろん必要があれば認めるべきだと思いますが、その点は、行政規制というよりは事業者さんが説明責任を果たせるかどうかのポイントと思っています。多回線契約を許容し、若しくは推奨した結果として、不正譲渡が起きて犯罪に使われてしまった場合に、事業者さんとしては、たとえ行政規制の違反が無かったとしても、道義的な責任を問われるのではないかと。レピュテーションリスクの問題にもなり得ると思います。その観点で、上限を超える申込みに対して、正当な用途と判断したことを後から説明するために何をどこまで確認するかというのは、各社の責任において対応を検討していただきたいです。総務省が「ああしろ、こうしろ」と言うのではなく、各社の判断と責任で、正当な理由があれば５回線を超えるものも認めていくというトーンがにじみ出ると良いということです。法令の中では難しいかもしれませんが、このように思いました。

（３）の代表者等の権限・地位確認ですが、これも名刺や社員証では駄目だという点は賛成いたします。駄目だと思います。その前のところで、そもそも論として整理しておきたいのは、契約担当者の権限等の確認が甘かったら何が起こるかということです。基本的には、利用料を回収できない等、困るのは契約した事業者さん御自身だと思うので、やはりこれも前の論点と同じで、事業者さんがどこまで確認すれば自らのリスクを回避できるかという観点で考えるべき話ではないかと。その点、追加回線の場合のリスクについては、必要な確認はもちろん行っているのですが、事業者さんは負えるのだと、先ほどのプレゼンテーションをお聞きして思いました。また、権限のない人が法人名義で契約して、利用料をその法人につけようとしたら、被害者は名義を使われた法人ということになると思いますが、これもこの規制の話とは別です。今回考えなくてはならないのは、法人名義で多数回線契約をして転売されることです。この場合、特殊詐欺に使われてしまったとき

の被害は一般市民に及ぶので、多少先回りの整理をして行政規制としておくことは望ましいのではないかと。

結論、反対でも何でもないので、少し回りくどい発言になりました。以上です。

【大谷主査】      ありがとうございます。各事業者の自主性について、かなりプレッシャーとなるような御意見をいただいたと思っております。利用者としては、事業者によってここが緩い、ここが強い等の差があまりない方が良い面もあると思っておりますが、そこも競っていただき、よりクリアな方法を事業者が考えるという御意見なのかと思って受け止めました。

星構成員からも御意見を頂戴したいと思います。

【星構成員】      ありがとうございます。主な論点の（１）、（２）、（３）について、僭越ながら私からも若干コメントさせていただければと思います。

まず、１点目のデータ通信専用SIMをどこまで対象とするかという点で、現時点でSMS機能が付いているか否かが１つの基準線として論じられているところ、現状において私自身もそこを１つの線にすることについては賛同すると申しますか、事業者様からお話がありました、自主規制という形で御対応はいただけているはずですが、なぜか本人確認のないSMS機能付きのデータSIMが出回ってしまっている現状もありますので、まずはここをしっかりと御対応いただくようお願いしたいと思います。先ほどリーチの御指摘もありましたが、まずはその観点からも、SMS機能付きであるかどうかで１つ線を引いて、SMS機能付きのものについてはしっかりと御対応いただける体制をつくっていただきたいと思います。

ただ、これも他の構成員からも御指摘がありましたように、SMS機能が無ければ不正利用の防止という観点から安心だと言い切れる現状があるのかということ、そうとも言い切れないと思いますので、今後の検討課題と申しますか、今回このような方向を示すことが、SMS機能なしについて今後はもう考えなくても良いということを意味するわけではないことは、確認をさせていただければと思います。

それから２点目の回線数の問題。これも数値基準の設定の仕方の難しさ、何でこうなのか、これも難しいことはあるかと思いますが、利用者の利便性、利用状況、事業者様の御対応の慣習という言い方が良いかどうかはともかく、今までの経緯、犯罪での不正利用の抑止とのバランスの中で出てきた数字だということが実際のところなのだろうと思います。これも実務上の実効性の観点も含めまして、まずは５回線を基準としながら、やはり５回線だと結構多めに回線契約して転売をしてしまうような現状が目立つことが、もしあ

るのであれば、今後見直しを否定するものではないと私自身は認識いたしております。

3点目の法人の契約担当の形については、駄目な方法も含めまして、現状の犯収法のレベル感にも合わせた方向性が1つの基準になるのだろうと思いますので、ここについては特には私のからはコメントございません。

ということで、概ね原案に私としても賛同させていただくものではございますが、最後に一言と申し上げたいのが、やはりSIMの不正利用が、「トクリュウ」等の緩いものも含めた組織犯罪といいますか、犯罪を組織的に回していく上での肝となるツールであることは間違いないので、今回このような規制を課すことにより、不正利用を試みている側が諦めることは考えられないということでございます。色々な制度的な、「抜け」という言い方が良いかはともかく、やはりこういったところをつけるのではないかという形で、新しい不正利用のやり方をどんどん考えていくことが想定されますので、状況の変化を踏まえて不断に、省令で対応できるのであればもちろん省令での見直しも随時行っていただければと思いますし、考えたくはないことですが、更なる法改正が必要だという状況が出てくるのであれば、そういったこともあり得るのだということも含めて、今後も検討させていただきたい観点、論点なのではないかと思っている次第でございます。

長くなりましたけれども、私からは以上でございます。

【大谷主査】 貴重なコメントをありがとうございました。本当に規制と犯罪のいたちごっこになっておりまして、ここの規制が有効になり、事業者の皆さんがそれに合わせて動き出したときには、もう何か新たな犯罪が起きることにならないように、絶えず見直しも必要だという御意見を頂戴しております。

ひととおり、欠席された構成員以外の御意見は頂戴いたしましたが、それぞれの御意見を踏まえて、さらにお話しいただきたいことがあるようでしたら、お願いいたします。

ここまで、各構成員からいただいた御意見を受けて、特に星先生から、1つ目の論点で、SMS機能なしのデータSIMについて御確認があったかと思いますが、何か補足説明等があるようでしたら、事務局の御発言をお願いしたいと思います。いかがでございましょうか。

【園部利用環境課課長補佐】 事務局でございます。

本日も様々な御意見いただきまして、ありがとうございました。基本的には、今回お伺いいたしました御意見、事業者の御要望等を踏まえまして、次回に向けて、論点整理の案の作成を進めさせていただきたいと考えております。

その上で、個別の論点についていただいたコメント等について若干触れますと、SMS機

能のないデータ通信専用SIMについて、現時点での状況については、警察庁から御発表いただいたとおりにかと思っております。不正利用が絶無ではないという状況と承知している一方で、これまでのワーキンググループにおいても御議論いただいたとおり、利便性とのバランスの確保も図っていくべきだとの観点の御指摘も頂戴したと思っております。こういった点を踏まえて方向性を整理させていただきたいと思っております。

また、今後の見直しの必要性を御指摘いただいたかと思っております。この点も、御指摘のとおり、犯罪の状況を踏まえて不断に対応していくべきとの観点を踏まえ、整理させていただきたいと考えているところでございます。

2点目の役務提供拒否を可能とする回線数については、「原則5回線」の根拠等について御指摘をいただいたところかと思っております。現時点の携帯通信事業者の御運用の根拠について、総務省で詳細に把握をしているものではございませんが、携帯電話の利用実態等を踏まえまして、平成20年頃に御設定されたものだと承知をしております。この点、携帯通信事業者においてさしあたり5回線という基準を置きつつ、個別の状況に応じてしっかり対処いただき、約15年間、大きな問題なく運用されてきたと承知をしております。この点、本ワーキンググループにおいてもTCAから御説明いただいたことも踏まえ、これをまず目安にすることが考えられるのではないかとという形で記載したものでございます。まさに今後の運用も重要になってくると思っており、さしあたりどのような形で基準を整理するかという点、今後どのように見直していくかという点の両面を検討することも考えられるのではないかと承知しております。

3点目の権限・地位の確認方法については、電子的な方法に関する御指摘、①から⑤までの書き方が紙ベースのように見えるのではないかと御指摘がございました。この点、いずれの方法につきましても、電子的な方法を排除しないことが分かるように整理することが考えられるのではないかと承知しております。GビズIDの活用については、機能の今後の拡充の方向について把握をしているものではございませんが、今後、民間にそういった機能が開放されたときに活用が可能となるような整理が考えられるのではないかと承知しております。

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。今の事務局の御説明など踏まえまして、さらに御意見などございますでしょうか。

大丈夫なようです。私としては、基本的に事務局でまとめていただく内容に沿って省

令の改正の準備を進め、1日も早く施行の準備が整い、事業者としても予測可能な状態で体制が整えられることを非常に期待しているところですが、パターンリズムに陥ってはいけないものの、きめ細やかな指針等も御用意いただく必要があると思いますので、できるだけ早く結論に至りたいと個人的に思っているところでございます。

それでは、本日の意見交換は以上とさせていただきたいと思います。

本日のヒアリングと意見交換の内容を踏まえまして、次の会合、これは7月下旬ということですが、制度整備に向けた論点整理に進んでまいりたいと思います。

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。

【園部利用環境課課長補佐】 次回会合の日程につきましては、別途事務局から皆様に御案内させていただきます。

以上でございます。

【大谷主査】 ありがとうございました。

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第13回会合を終了いたします。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。