



ICTサービスの利用環境を巡る 諸問題について(案)

～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～

令和7年6月6日
総合通信基盤局

今後の検討スケジュール

1

	ICTサービスの利用環境の整備に関する研究会 (親会)	不適正利用対策に関するワーキンググループ
1月	<u>1月22日</u> ➤ ICTサービスの不適正利用への対処等について - 論点提示	当面の活動
2月~5月	 通信ログ保存の在り方の検討については、専門的に議論し、親会へ報告 - 3月26日、27日 - 4月11日、14日、18日	<u>4月21日(済)</u> ➤ (1) 携帯電話本人確認のルール (事業者ヒアリング 有) <u>5月9日(済)</u> ➤ (2) 闇バイト、特殊詐欺等対策 (事業者ヒアリング 有) <u>5月16日(済)</u> ➤ 携帯電話本人確認のルール (事業者ヒアリング 有)
6月	 <u>6月下旬</u> ➤ WG中間整理案 ➤ 通信ログ保存の在り方	<u>6月6日</u> ➤ 論点整理
7月~	<u>7月3日</u> ➤ とりまとめ	

課題1

● 特殊詐欺、闇バイト等対策(固定・携帯電話対策)

- ・国際電話番号からの特殊詐欺が増加しているところ、固定電話向けの電話について、以下の観点等を含め、どのような対策が取りうるのか。また、携帯電話の迷惑電話被害防止に向けて、どのような対策が取りうるのか。
 - ①国際電話不取扱センターの体制強化、キャパシティ向上、運用改善等
 - ②新規・切替等の顧客に対する利用休止申請に係る周知対応
 - ③国際電話を使用しない顧客に対する効果的な措置

課題2

● 特殊詐欺、闇バイト等対策(SMS・メール対策)

- ・昨年末より、一部キャリアの回線で、ユーザー宛てに闇バイトを募集するSMSが届いていたが、現在は闇バイト募集に係るSMSの申告件数は、減少。
- ・このほか、携帯電話利用者における詐欺被害の増加があるところ、迷惑SMS、迷惑メール等に伴う被害防止に向けて、どのような対策が取りうるのか。



事業者は国際電話不取扱センターの早期の積滞解消を目指し、6月に開設する総務省の迷惑電話相談窓口とも官民連携を行ってはどうか。また、事業者は、5/9に発表いただいた各種詐欺対策の推進・周知を進めながら、一層の対策の低廉化を含めた効果的な取組を実施していくこととしてはどうか。

課題3

● 既存番号へのスプーフィング(なりすまし)

- ・携帯・固定電話のディスプレイの表示を警察署の番号にするなど、電話番号を偽装するケースが報告されている。



通信事業者と連携して効果的な対策を検討し、できるところから実施中。国民に対して電話番号を偽装する手口に関しての更なる注意喚起を推進してはどうか。また、電話番号を偽装する手口について、引き続き検討を行ってはどうか。

課題4

● 海外電話番号による詐欺電話

- ・海外電話番号が、簡単にアプリで取得可能なところ、使い捨て可能な番号として、詐欺のツールとして使われうる状況。



国民に対して国際電話発の詐欺電話に関する注意喚起を推進してはどうか。また、引き続き実態把握を行ってはどうか。

1 SIMの不正転売

- ・SIMの不正転売が増加し、詐欺への転用等の可能性が指摘されている中、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。

2 法人の代理権(在籍確認)

- ・法人の担当者が契約を行う場合における在籍確認の手法について、法令上の規定がなく、事業者によって異なる取扱いとなっている中、利用者視点に立ってどのような方策が考えられるか。

3 他社の本人確認結果への依拠

- ・携帯電話の契約時における他社の本人確認結果への依拠について、これまでの議論を踏まえ、利便性と不正対策のバランスの観点から、どのように考えるべきか。

4 追加回線

- ・2回線目以降の回線契約時の本人確認について、法令上の要件が1回線目とは異なっている中、昨今の犯罪手口の巧妙化、高度化に対し、どのような効果的な対策が考えられるか。

5 上限契約台数

- ・上限契約台数について、本人確認が適切になされない場合に、大量不正契約に繋がる可能性があるが、利用者のニーズと不正対策のバランスの観点から、どのように考えるべきか。

6 データSIM

- ・データSIMの本人確認について、法令上の要件が音声SIMと異なっている中、昨今の犯罪手口の巧妙化、高度化に対し、どのような効果的な対策が考えられるか。

1 SIMの不正転売の事例について

考え方(案)

⇒ 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うる対策として、不正転売の違法性について政府及び事業者が利用者に対してわかりやすい周知啓発を一層強化していくことに加え、事業者による与信強化や定期的な本人確認なども考えられるのではないかな。

2 法人の代理権(在籍確認)

考え方(案)

⇒ 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最低限必要な書類(電子的なものも含む)の提出を求めるなど、所要の規定見直し求められるのではないかな。【省令事項:携帯電話不正利用防止法施行規則第4条】

3 他社の本人確認結果への依拠

考え方(案)

⇒ 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他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最新の本人特定事項となっていることや、依拠元の当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、改めて本WGにおいて検討を深めてはどうか。

5/16発表の概要

- 【犯罪実態】 大手モバイルキャリアを舞台としたSIMの不正発行事案の捜査で立件したeSIM約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の手続きを一部省略してSIMが不正発行されたものであったことが判明。(警察庁)
- 【利用者利便】 デバイスの追加において本人確認が必要となるため、利用者にとっては利便性が低下する可能性があるが、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いることから、確認方法によっては、そこまで利便性が低下しないとも考えられる。(NTTドコモ)
- 【犯罪悪用可能性】 ワンナンバーサービスについては、同一の電話番号で動作するので、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する。(NTTドコモ)

構成員からのご意見

- ID・パスワードのみの確認では不安なので、本人認証がデジタル庁ガイドラインの少なくともレベル2に当たるような本人確認を実施してほしい。同じ番号でデバイス追加の場合は、犯罪悪用可能性が低そうなことから、レベル1でも良いと思うが、悪用事案が出れば、今後再検討が必要。(沢田構成員)
- 1回線目とは別機会の契約であり、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。AppleWatchなどのデバイス追加の際に有意な悪用リスクがないという評価ができるかが問われている。(中原構成員)
- キャリアが発行しているIDとパスワードが一つの軸になると思われるところ、JPKIを活用するなど本人確認とリンクさせたID・パスワードの管理をガイドライン等で業界横断的にルール化していくことも考えられるのではないかと。(辻構成員)

考え方(案)

- 簡易な本人確認手法には一定の利便性が認められる一方、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、本人認証性を向上させるべく、デジタル庁の本人確認の手法に関するガイドラインも参考に、厳格化に向けた規定の見直しが必要ではないか。その際、犯罪実態を踏まえ、すべての回線契約(音声SIM、音声SIM付AppleWatch)に等しくルールを適用するかどうかについても検討すべきではないか。【省令事項：携帯電話不正利用防止法施行規則第3条第3・4項、同規則第19条第5項等】

5/16発表の概要

- 【犯罪実態】 大手モバイルキャリアを舞台としたSIMの不正発行事案の捜査では、被疑者は、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が判明。(警察庁)
- 【利用者利便】 おひとりで6回線以上契約される方は、一事業者でも数万規模あり、市場全体での一定のボリュームはあると考えられる。家族での多回線契約のニーズとして、金銭管理がしやすい、ポイントが貯めやすい、管理のしやすさといった理由が考えられるのではないかと。(楽天モバイル)

構成員からのご意見

- 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、上限契約台数の考え方が不要となるのではないかと。(辻構成員)
- 多数台契約をすること自体に怪しさはないか、また、それが現実化して不正利用されれば、被害規模が大きくなるのではないかという点について、複数台契約のニーズは様々に想定され、定型的な悪用リスクを想定できない。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べきではないかと。(中原構成員)
- 複数回線で問題になるケースというのは、無断で譲渡するとか名義貸しだと理解した上で、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、使用用途を聞くことも考えられる。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することもありうる。こうした方法がとれるのであれば、法律ではなくて自主規制でも良いのではないかと。(沢田構成員)

考え方(案)

- ⇒ 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もあるものの、不自然に多数の契約が行われるケースもありうる。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を踏まえ、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と。
- ⇒ その上で、今後、少なくとも業界ルールの適用状況について検証を行い、更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べきではないかと。

5/16発表の概要

- 【犯罪実態(SMSあり)】 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、把握できたもので、SIM種別の特定に至ったものは244件。そのうちの185件はSMS機能つきデータ通信SIMであり、残りの59件は音声SIMという結果であった。(SMS機能がついていないデータ通信SIMについては対象外。)(警察庁)
- 【犯罪実態(SMSあり/本人確認の実施)】 把握した185件のSMS機能つきデータ通信SIMについて、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はなかった。残りの約41%に当たる75件は、事業者による自主的な本人確認がなされていたが、外国の身分証明書が使用されるなど、事業者としても本人確認が困難なものであり、本人確認が実質的に機能していないものが多数あった。(警察庁)
- 【犯罪実態(SMSなし)】 SMSなしのデータSIMに関しては、事例はあるが、現時点での定量的な犯罪実態を具体的に示すことは難しい状況。(警察庁)

構成員・発表者からのご意見

【総論】

- データSIMについては、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はないか。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、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べきかどうか。これ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であれば除外してもよいと思う。(中原構成員)
- SaaSや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ことから、本人確認の導入が議論されていると考えられるところ、SIMの通話機能・SMS機能の有無によって、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と考えられる。(仲上構成員)
- MVNOについては、MNOと違ってデータSIMの本人確認をやっていない事業者も一定数いるので、義務化となった場合、一定の準備期間が必要であり、開発コスト等もかかる。(U-NEXT)

【対象SIM】

- 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合意の方向だと考えるが、それを前提として、例外のところを精緻に議論する段階に入っているかと思う。リスクが低いと考えられる理由と、どういうものが例外とすべきかというのの精緻な議論が必要なのではないか。(沢田構成員)
- SMS無しのSIMについて、どの程度の悪用実態が現時点であるのかも併せて考えて、どのくらい厳格化していく必要があるのか考えていく必要がある。ネット経由で訪日前に購入されるというケースも多いと思われるところ、義務化は相当大がかりな変更が必要になるので、慎重な検討が必要。(鎮目構成員)
- SMS無しのデータSIMについては、インターネット上で様々なサービスが利用できるが、Wifiや海外から持ち込まれたSIMへのローミングについても同じことが言えるのではないかと。トラストアンカーについての役割を考えた際に、仮にデータ通信についても本人確認をすると、利便性の多大なる低下も予想される中、犯罪を抑制する効果を期待しているのか、捜査の精度を高めていく効果を期待しているのか疑問。(仲上構成員)

【利用用途(IoT)】

- サービスの形態、運用により既に一定の対策は講じられており、IoT機器向けデータSIM(SMSなし)に関する本人確認は不要と考える。(U-NEXT)

【利用用途(訪日外国人向けプリペイド)】

- SMS機能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。(山根構成員) → **警察庁から説明**
- 警察庁の4/22発表の事例②の架空の契約者情報で契約したSMS機能がないデータ通信SIMを使用していた事件では、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。(沢田構成員) → **警察庁から説明**
- 自販機での販売は、厳格化した場合は事業継続が難しい事業者もいるとのことだが、日本人でも簡単に買うことができ、抜け穴にもなり得るのではないか。(鎮目構成員)
- プリペイドSIMを除外するべきかについては、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るが、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。訪日外国人に対しても原則どおりの厳格な本人確認を要求することは、訪日外国人にデータ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については、筋論としては本人確認自体は必要であり、検討すべきはその方法の緩和である。貸与時の本人確認の規律を参考にするという案も含めて、引き続き検討が必要ではないか。(中原構成員)
- 訪日外国人向けのプリペイドSIMの内、特にSMSなしについては、問題となっているSMSを使った詐欺や、電話番号の転売などのリスクの少ない商品であり、利用期間を限定しており、本人確認不要と考える。義務化された場合、事業継続自体が非常に困難になる。(U-NEXT)

【本人確認の実効性】

- 例えば、ホテル宿泊の際に必ずパスポートの提示を求めている。パスポートが偽造かどうかにかかわらず、記録自体を残すことは、偽造パスポートの出所の調査にも繋がるなど、捜査に資するのではないか。(星構成員) → **警察庁から説明**
- パスポートによる本人確認については、判断するのが店舗スタッフであることやから、実効性の確保が難しいのではないか。(U-NEXT)

考え方(案)

- ⇒ 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、一部の事業者ですでに自主的に行われている本人確認の取組を確実に行う観点から、義務化について検討すべきではないか。【法律事項:携帯電話不正利用防止法】
- ⇒ ただし、義務化を検討するにあたっては、貸与時の本人確認の規律も参考に、対象SIMや利用用途(訪日外国人やIoT機器)等に関して、利便性と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。