資料７－４

不適正利用対策に関するワーキンググループ（第7回）
事業者ヒアリング　ご説明資料

KDDI株式会社

2025年4月21日

Tomorrow, Together
KDDI

本日のご説明事項

1. SIMの不正転売に対する取り組み事例
2. 法人の代理権（在籍確認）
3. 他社の本人確認結果への依拠について
4. 追加回線の本人確認
5. 上限契約台数
6. データSIMの本人確認

Ⅰ．SIMの不正転売に対する取り組み事例

新規契約時等に、お客さまに対して
周知啓発を継続して実施

店頭POP

au通信サービス ご利用にあたって

携帯電話不正利用防止法

- 携帯電話やSIMカード等を、携帯電話事業者に無断で譲渡してはいけません。携帯電話事業者の承諾を得ずに、業として、有償（転売）で譲渡すると、2年以下の懲役または300万円以下の罰金に処せられます。
- 携帯電話の契約時に氏名、住居および生年月日について虚偽の申告をしてはいけません。本人特定事項を隠蔽する目的で違反すると、50万円以下の罰金に処せられます。

２.法人の代理権（在籍確認）

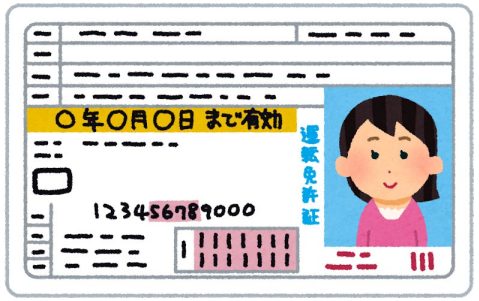
犯罪等の情勢を踏まえつつ、厳格な審査に加え、適切な追加的確認書類について引き続き検討

現行法令の定め

登記簿謄本
印鑑証明書
など

＋

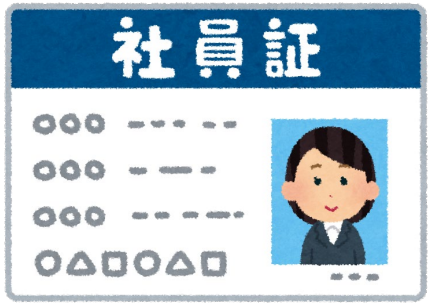
マイナンバーカード
運転免許証
など



＋

追加的確認書類

名刺
社員証



３.他社の本人確認結果への依拠

携帯電話の本人確認強化が行われる状況において他の事業者への依拠を認めることは適当ではない

非対面契約時の本人確認強化

１　非対面における券面を確認する方法の廃止

本人確認書類の写しを用いた本人確認では、偽変造の看破が困難なことに鑑み、本人確認書類の写しを用いた非対面における本人確認方法は廃止することが適当である。（第３条第１項第１号ハ、ヘ等）

対面契約時の本人確認強化

２　対面における電子的な確認方法の義務化

携帯電話の不正契約に使われた本人確認書類において、精巧に偽変造された本人確認書類が多く使われている実態に鑑み、対面（特定事項伝達型本人限定受取郵便を用いる場合を含む）での本人確認においては、ICチップを読み取る等デジタル技術を活用した方法により本人確認を実施することが適当である。（第３条第１項第１号イ、ト等）

不適正利用対策に関するワーキンググループ報告書(2024年11月29日)

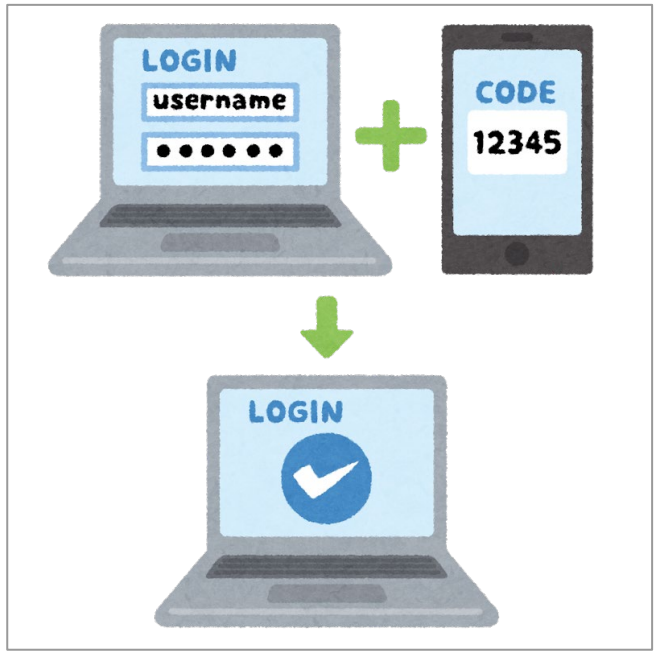
まずは、現状の方向性を踏まえて本人確認強化の取り組みを実施すべき

4.追加回線の本人確認

追加回線について、現行の簡易な方式は存置しつつ、ID/PWだけでない確認も実施する必要がある

＜確認方法の例＞

SMSによる二段階認証



当人認証保証レベル	レベルの定義
レベル１ （AAL1）	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、単要素若しくは複数要素を使うことにより、当人認証の信用度がある程度ある。
レベル２ （AAL2）	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、複数要素を使うことにより、当人認証の信用度が相当程度ある。
レベル３ （AAL3）	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、耐タンパ性を有するハードウェアを含む複数要素を使うことにより、当人認証の信用度が非常に高い。

出典）「デジタルアイデンティティガイドライン（SP800-63-3）」より作成

図 17　身元確認及び当人認証の保証レベル[36]

不適正利用対策に関するワーキンググループ報告書(2024年11月29日)

上記を参考とし、多要素認証等の適切な確認が求められる

５.上限契約台数

上限契約台数について、一定の制限は必要と考えるが
新たなサービス提供の妨げとならないよう、
犯罪等の情勢を踏まえ、例外措置等の検討が必要

＜サービスの例＞

みまもりGPS端末

IoT

通信先が限定されているサービス等は不正利用のリスクが
少ないと考えられ、例外措置とすべきではないか

6.データSIMの本人確認

データ通信利用が増えている情勢を踏まえ、その規制の在り方はニーズと犯罪事例、リスク対策のバランスで検討していくべき

＜サービスの例＞

訪日外国人向け

IoT

旅行や急なリモート会議

契約期間が一定期間に設定された訪日外国人向けサービスや、その通信先が限定的なサービス、機能がデータ通信に限定されSMSが使えないサービス等は、例外措置とすべきではないか

ご提示の論点について　1/6

		回答
1. SIMの不正転売の事例について	不正転売の事例において、アルバイトの応募者から契約時に「闇バイトではない」旨の虚偽申告や、契約後も不正契約であった旨の申告を行うことが期待されず、事業者として不正検知が困難である中、どのような有効な対策が考えられるか。	• 現在、店頭等でPOPや「au通信サービス ご利用にあたって」等を用いて注意喚起等実施しております
	応募者の中には、無断譲渡の違法性を認識せず、軽い気持ちで犯罪に手を染めてしまう者も想定されることから、犯罪を少しでも減らす観点から、違法性に対する理解を高めていく必要があるのではないか。	• お客さまの理解向上の取り組みを引き続き実施してまいります

ご提示の論点について　2/6

		回答
2.法人の代理権（在籍確認）	法人の担当者が来店して契約を行う場合、来店する担当者とその法人の代理権の有無（在籍確認）について、犯罪実態を踏まえつつ、分かりやすさや整合性の観点から、求められる要件を明確化すべきか。	• 犯罪等の実態を踏まえた対応は必要と考えます • 法人契約については、契約台数等も含め、厳格に審査を行っております • 必要な書類や在籍確認について、どのような対応がお客さまにとって負担が少なく、適切な対応となるか、引き続き検討してまいります
	在籍確認の在り方について何らか法令上の規定を設けるとした場合、どのような要件を定めるべきか。	
	仮に法令上の要件を定める場合、どのような確認書類を認めるべきか。	

ご提示の論点について　3/6

		回答
3. 他社の本人確認結果への依拠	他社への本人確認結果への依拠を実施する場合、他社の本人確認結果の保証レベルが高く、継続的に本人確認事項が更新された最新情報を照合することが必要となるが、これをどのように担保するべきか。	• 例えば、「不適正利用対策に関するワーキンググループ報告書」記載のように、マイナンバーカードの公的個人認証（JPKI）の利用が考えられます • 常に最新の情報を確認、保持するためには各事業者側のシステム対応等の課題があります
	他社への本人確認結果への依拠についてメリットや課題がある中、近時、ID/PASS等による本人確認が可能な契約形態を突いた不正契約が報告されていることも踏まえ、依拠を認める是非をどのように考えるか。	• 携帯電話の本人確認強化が行われる状況において、まずはその本人確認の強化について対応すべきであり、現時点で他の事業者への依拠を認めることは適当ではないと考えます • 本人確認強化の取り組みを進める中で、依拠についてどう考えるかを継続して検討すべきと考えます
	少なくとも携帯電話事業者への依拠については、保証レベルを上げる取組がまさに行われている段階にあることについて、どのように考えるか。	
	他方、金融機関の依拠については、金融機関からのニーズや運用の実現可能性を勘案して、議論を行っていく必要がある。	

ご提示の論点について　4/6

		回答
4.追加回線の本人確認	追加回線の本人確認については、省令上は簡易な方式が認められているが、そのような方式は利用者の利便性が高い一方、そこを狙った犯罪に悪用されている実態があることも踏まえ、規定の見直しを行うべきか。	• 犯罪等が発生している実態を踏まえ、規定の見直しを行うことは、1つの選択肢であると考えますが、多様なサービス展開に影響が出ないよう、そのサービスのニーズと犯罪のリスクや対策等を考慮し、例外規定を設ける必要があると考えます
	本人確認は、当該ユーザーの本人特定事項とその正確性を確認する「身元確認」と、ある行為の作業者が当人によってなされていることを確認する「当人認証」の二つの組み合わせによって成り立っているところ、ID/PASS等による本人確認の規定は、1回線目の身元確認に対して、当人認証を行っていることだと考えられるが、現行法令上のID/PASS等のみによる当人認証の認証レベルは、十分に高いと言えるのか。	• 事業者において、セキュリティ確保の取り組みが必要であり、ID/PASS等のみによる当人認証は十分ではないと考えます
	仮に規定の見直しを行う場合、音声SIMと音声SIM付AppleWatchなど様々なサービスがある中で、2回線目以降の回線契約に関する本人確認方式をどのような形で強化すべきか。なお、貸与（規則第19条第5項）においても同様に見直すべきか。	• 契約形態（例：音声SIM、データ専用SIM（SMS有／SMS無）、Apple Watch等）によって、それぞれのサービスを用いた犯罪のリスクは異なってくるため、多様なサービスを含めたルールは柔軟に決める必要があります • 事業者の適切な対応について、業界自主ルールという形で検討していくことも考えられます

ご提示の論点について　5/6

		回答
5. 上限契約台数	契約台数の上限については、音声SIMについて自主的な業界ルールが存在するが、何らかの制度的な担保を行うべきか。	• 契約形態（例：音声SIM、データ専用SIM（SMS有／SMS無）、Apple Watch等）によって、それぞれのサービスを用いた犯罪のリスクは異なってくるため、多様なサービスを含めたルールは柔軟に決める必要があります • 事業者の適切な対応について、業界自主ルールという形で検討していくことも考えられます
	音声SIMに限らず、データSIMやAppleWatchの契約台数の上限についても、何らかの明確化が必要か。	
	契約台数の上限については、回線数が多ければ多いほど、不正契約があった場合に、被害が広がることを踏まえると、上限の基準を何回線とするべきか。	

ご提示の論点について　6/6

		回答
6.データSIMの本人確認	データSIMについて、訪日外国人の本人確認などを簡易な方式で行うことにメリットがある一方、犯罪悪用の実態があることを踏まえ、本人確認義務の規定を設けるべきか。	• 契約形態（例：音声SIM、データ専用SIM（SMS有／SMS無）、Apple Watch等）によって、それぞれのサービスを用いた犯罪のリスクは異なってくるため、多様なサービスを含めたルールは柔軟に決める必要があります • 事業者の適切な対応について、業界自主ルールという形で検討していくことも考えられます
	仮にデータSIMについて本人確認を義務付ける場合、音声SIMとの違いとして、訪日外国人を含めて多様な形態での利用があることから、利用実態や実効性の観点を配慮した規定が必要なのではないか。例えば、訪日外国人の本人確認について、外国人に対する貸与の規定も参考になるのではないか（携帯電話不正利用防止法規則第19条第1項2号）。	
	また、データSIMには、IoT機器に利用されているものがある点について、どのように考えるか。	
	SMS付データSIMとSMS無データSIMのそれぞれの悪用の典型例はなにか。悪用実態の違いについて、どのように考えるか。	• SMSは日常のコミュニケーションの中で利用されており、その日常に溶け込ませる形で、スミッシング等、直接的な詐欺のツールに使われる可能性があります • 一方でデータ通信は、様々なコミュニケーションアプリが存在しており、そのうちの一部が犯罪に使われる可能性がありますが、データ通信契約そのものは直接的に犯罪に結びついているわけではないと考えます • よって、SMS有無により、その悪用実態は異なるものと考えます

＜参考＞
povo2.0データ専用（SMS無）
・訪日外国人向けは在留資格「短期滞在」の最長である90日間が利用期限
・また、契約時SMS認証を求めているので、SMS認証を受けた契約に対して本人追跡が可能

Tomorrow, Together

KDDI

「つなぐチカラ」を進化させ、
誰もが思いを実現できる社会をつくる。

KDDI VISION 2030