資料7－3

携帯電話本人確認のルールについて

2025年4月21日

株式会社NTTドコモ

基本的な考え

- 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携帯電話不正利用防止法等の規律を遵守するとともに、**迷惑SMS・メール対策や携帯電話の本人確認の厳格な運用を通じ、特殊詐欺の防止・不正利用の対策に取り組んでおります**

- 昨今の特殊詐欺の発生状況等から、**不正利用対策に有効な規律の見直しは実施すべき**と考えますが、事業者の自主的取組みで対応可能な対策、利用者の利便性を損なう恐れのある対策については、**関係者の意見を十分に踏まえた検討をお願いいたします**

- 当社では、法令の規律に加え、業界団体（TCA）の自主基準を踏まえ自主的なルールを定めて運用しており、**規律の見直しを行った場合も大きな影響は想定しておりません**

- なお、規律の見直しにあたり、システム開発等、対応時間を要する対策は、**十分な移行期間の確保をお願いいたします**

1．SIMの不正転売

- 当社は現状、闇バイトでの携帯電話契約について、**店頭ツール掲示による注意喚起及び契約時の重要事項説明による確認**を実施
- 闇バイト目的の場合、申込者に契約意思があり本人確認も適正に行われることから、SIM不正転売の抑止が困難なケースが多い
- SIM不正転売の抑止には、**周知啓発の強化及び不正転売を難しくするしくみの導入、双方の対策検討が必要**
- 周知啓発の強化は、業界団体（TCA・テレサ協等）・事業者が連携した継続的な取組みが必要と考えるが、警察庁・総務省においても連携協力が必要と考える
- 不正転売を難しくするしくみは、**携帯電話契約・端末割賦契約の与信審査強化**が考え得る

構成員限り

- 与信審査については、不払者等情報の事業者間情報交換を現在実施している他、総務省「競争ルールの検証に関する報告書2024」を踏まえ、割賦代金未払い端末に関するIMEI情報の情報交換を実施予定

（参考）SIMの不正転売に関する注意喚起

【店頭ツール掲示】

docomo

＼ そのスマホ、あなたが使いますか？ ／

携帯電話契約を促す『闇バイト』は犯罪です

～ひとりで悩まず警察へ相談を～

NO

・Are you the one who will be using this smartphone? Shady part-time jobs that pressure you to make a contract with a mobile carrier are illegal!
・那部手机，是你自己用吗？ 让你签订手机合同的“黑兼职”是犯罪行为!
・Chính bạn sẽ sử dụng điện thoại thông minh đó chứ? Nghe lời xúi giục làm "công việc bán thời gian mờ ám" ký hợp đồng điện thoại di động là tội phạm!

支払い義務は契約者にあります

・The contract holder will be obliged to pay for the phone and other charges related to the contract.
・支付费用是合同签约人（契约者）的义务
・Chủ thuê bao có nghĩa vụ phải thanh toán.

契約は取り消せません

・There will be no annulation of the contract.
・合同不能取消
・Hợp đồng không thể bị hủy bỏ.

ドコモでは各種お手続き時の本人確認を強化しています

・DOCOMO is strengthening the identity verification during various procedures.
・DOCOMO 正在加强各种手续中的身份验证程序
・DOCOMO đang đẩy mạnh việc xác minh danh tính khách hàng khi thực hiện các loại thủ tục.

下記の方法で本人確認書類のチェックを実施する場合があります

“専用の機器”や“専門センター”でのチェック

・Identification documents are checked by special equipment or at contract review centers.
・使用“专业设备”在“契约审查中心”检查身份证件
・Kiểm tra giấy tờ xác minh danh tính bằng “thiết bị chuyên dụng” tại “Trung tâm xét duyệt hợp đồng”

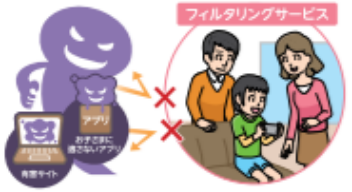
株式会社NTTドコモ
S24001CB

【重要事項説明】

本ページについてはスタッフからご説明させていただきます。

1 ご利用者さまの年齢確認
（18歳未満の場合、フィルタリングサービス加入のご確認）

インターネットのご利用により違法・有害情報に触れたり、犯罪に巻き込まれる可能性があるため、「青少年インターネット環境整備法」を踏まえ、ご利用者さまの年齢を確認させていただいております。



ご契約者さま、もしくはご利用者さまが18歳未満のお客さまへ

法令等により、原則フィルタリングサービスへご加入いただき、携帯電話販売時には設定を行うことが義務付けられております。
なお、フィルタリングサービスに加入されない場合、「フィルタリングサービス不要申出書」を保護者さまからご提出していただきます。

犯罪やトラブルに巻き込まれないよう、以下をご確認ください

●携帯電話を契約して第三者へ渡すことで報酬がもらえるなどと騙って契約をさせたり、名義貸しを求める事例が発生しています。
□名義貸しや第三者からの依頼に基づく、いわゆる闇バイト等による特殊詐欺などの犯罪に関する契約ではありません。
●携帯電話を狙った架空請求詐欺や個人情報を不正に収集するアプリケーションによるさまざまな被害が発生しているため、セキュリティ対策を行うことが重要です。
（あんしんセキュリティをご利用いただく場合は、初期設定が必要となります。）
□携帯電話の利用には、セキュリティ対策が重要であることを理解しました。
□あんしんセキュリティを利用する場合は、初期設定が必要であることを理解しました。

2．法人の代理権（在籍確認）

- 当社は現状、**委任状により来店者が法人代理権を有することの確認、又は名刺若しくは社員証により来店者の在籍確認**を実施
- **営業担当者（アカウントマネージャー）が対応する法人契約の場合**、原則として法人の事業所を訪問して手続きを行うため、不正契約の可能性は低く、また**来店者に求められる書類が分かりづらいとの問題は基本的に発生しない**と考える
- 一方、店頭窓口で手続きを行う法人契約の場合、分かりやすさ向上の観点から、**来店者に求められる書類の要件を事業者間で統一することは考え得る**

3．他社の本人確認結果への依拠

- 当社は現状、**他社の本人確認結果への依拠による本人確認は実施していない**
- 当社では、アメリカ国立標準技術研究所（NIST）ガイドライン等を参考に、身元確認・当人認証に関する**独自ガイドラインを策定しており、その後もフィッシング被害発生等の状況に応じて各サイトにおける身元確認/当人認証の対応レベルを常に見直している**

  【当社における取組み事例】
  - 身元確認：JPKIの導入、対面受付時におけるお客様容貌確認　等
  - 当人認証：回線認証の適切な利用、パスキー認証の必須化　等
  - フェデレーション：dアカウント連携を行うパートナー向けガイドラインの説明　等

- 他社の本人確認結果への依拠については、依拠先の本人確認（身元確認の保証レベル）、契約者の同一性確認（当人認証の保証レベル）が適切に行われない場合、**なりすまし等不正申込の発生がリスクとして想定**されるため、**慎重な検討が必要**
- そのため、①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、②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な検討が必要**

  【検討を要するポイント例】

  ① 依拠先の身元確認の保証レベルの確認と依拠可能な期間
  （金融サービスでは、都度の本人確認が求められている）

  ② 非対面での依拠先の契約者と依拠元との契約者の同一性の確認手段
  （SMS認証はフィッシング詐欺で突破されている事例が広く知られている）

４．追加回線の本人確認

- 当社は現状、2回線目以降の契約について、基本的には音声・データ通信契約に関わらず、**1回線目と同様に本人確認書類の提示による本人確認を実施**
- 例外として、Webサイトにおけるワンナンバーサービス・副回線サービスの申込みにおいて、ID/PASS等による本人確認を実施
- ID/PASS等による本人確認はなりすましの可能性があるリスクを認識しているが、音声SIMとのペアリングを前提とするウェアラブルデバイスの利用についてお客様利便性が下がる懸念があり、**例外規定の整理を検討することも一考**
- その場合、例外規定においては、当面ID/PASS等による本人確認を認めたうえで、**不正契約の発生のモニタリングを前提とすることを要件とすること等が考え得る**

5．上限契約台数

- 当社は現状、**TCA自主基準に則り個人名義における音声SIMの上限契約台数を5台としている**
- TCA自主基準を準用し、データSIM及びウェアラブルデバイスについてもそれぞれ上限契約台数を設定
- 上限契約台数のルール化を行う場合、**TCA自主基準を踏まえたルール化が考え得る**
- TCA自主基準の拡充対応（データSIMの上限契約台数設定、音声SIM上限契約台数の変更）も考え得るが、あくまで**TCA自主基準であり制度的担保とはならない可能性がある**
- 上限契約台数のルール化を行う場合、例えば世帯主が契約者となり家族全員分を契約することが不可となるケースが発生し得るため、**十分な周知期間を設けたうえでの対応等をお願いしたい**

6．データSIMの本人確認

- 当社は現状、**TCA自主基準に則り音声契約と同一方法での本人確認を実施**
- データSIMは現状携帯電話不正利用防止法に基づく本人確認義務の対象外だが、固定IP電話の転送役務を用いた詐欺電話や、メール・SMS送信等によるフィッシング詐欺への悪用は考え得るところであり、**規律の強化は一定の効果が見込まれると考える**
- 仮にデータSIMを本人確認義務対象とする場合、MVNO等の**関係事業者意見も踏まえたルール化の検討及びシステム対応等の十分な移行期間の設定が必要**
- またデータSIMは、IoT機器利用や訪日外国人利用等、利用用途が多岐に渡るため、**SIM利用の利便性と犯罪等の悪用可能性とのバランスを考慮した検討が必要**
- SMS付・SMS無データSIM双方とも犯罪等の悪用可能性があることは変わらないため、**SMS機能有無に応じて本人確認方法の整理を分けることは不要と考える**

（参考）本人確認の基本的要素

身元確認
（Identity Proofing）

申請者を一意に識別するとともに、その実在性を確認すること。

具体的には、申請者の属性情報を収集することで、申請者を一意に識別するとともに、収集した属性情報が真正かつ申請者自身のものであることを本人確認書類により検証することで、申請者が実在かつ生存する人物であることを確認する。

当人認証
（Authentication）

申請者の当人性を確認すること。

具体的には、対象手続を利用しようとする者が、身元確認時に登録された者と同一の人物であることを、申請者と紐づけて登録した認証器を用いて確認する。

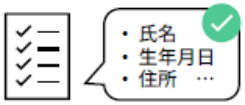
フェデレーション
（Federation）

身元確認や当人認証を、他者に依拠して実現すること。

具体的には、信頼できるIDプロバイダと連携し、IDプロバイダによって行われた身元確認や当人認証の結果に関する情報を入手することで、対象手続における本人確認を実現する。

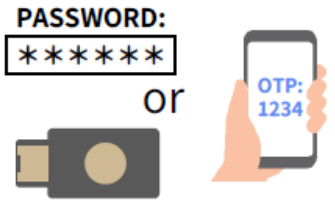
（出典）デジタル庁　本人確認ガイドライン改定方針　令和6年度とりまとめ（案）（デジタル庁、2025年3月）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/058ea13e-58e4-4e77-b18f-24833a65c7b1/c543b091/20250304_meeting_identification-guideline-revision_outline_01.pdf

（参考）身元確認の保証レベル

プロセス	対策基準（青字：上位レベルとの相違点）		
	身元確認保証レベル1	身元確認保証レベル2	身元確認保証レベル3
属性情報の収集 	（収集手法は任意とする）	（収集手法は任意とする）	本人確認書類の電子的な読取り
本人確認書類の検証 	以下のいずれか • デジタル署名の検証 • 信頼できる情報源への照会 • 券面の物理的検査（対面） • **券面の物理的検査（非対面）**	以下のいずれか • デジタル署名の検証 • **信頼できる情報源への照会** • **券面の物理的検査（対面）**	デジタル署名の検証
申請者の検証 	以下のいずれか • 対面での容貌確認 • 非対面での容貌確認 • 暗証番号等による検証 • **確認コードの送付による検証**	レベル3と同じ	以下のいずれか • 容貌の確認（対面） • 容貌の確認（非対面） • 暗証番号等による検証

（出典）デジタル庁　本人確認ガイドライン改定方針　令和6年度とりまとめ（案）（デジタル庁、2025年3月）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/058ea13e-58e4-4e77-b18f-24833a65c7b1/c543b091/20250304_meeting_identification-guideline-revision_outline_01.pdf

（参考）当人認証の保証レベル

保証レベル	対策基準	
	認証要素	脅威への耐性要件
当人認証 保証レベル3	**「公開鍵暗号に基づく認証器」を含む多要素認証** 例） ・ 暗証番号付きのICカード ・ パスキー 	・ **フィッシング耐性（必須）** 「必須」：全ての利用者に対してフィッシング耐性をもつ認証方式を適用する ＋ ・ 保証レベル2の耐性
当人認証 保証レベル2	**多要素認証** 例） ・ 暗証番号付きのICカード ・ パスキー ・ パスワード ＋ワンタイムパスワード 	・ **フィッシング耐性（推奨）** 「推奨」：フィッシング耐性をもつ認証方式を利用者に対して提供し、その利用を推奨するが、他の認証方式についても選択可能とする ・ **認証器等の盗用に対する耐性** ※ICカードやパスワード等の認証要素のうち一つが盗用された場合の耐性 ＋ ・ 保証レベル1の耐性
当人認証 保証レベル1	**単要素認証**（又は多要素認証） 例） ・ パスワード ・ ワンタイムパスワード ・ USB接続型セキュリティキー ・ 又は保証レベル2以上の手法 	・ 盗聴 ・ リプレイ攻撃 ・ オンライン上での認証情報の推測

（出典）デジタル庁　本人確認ガイドライン改定方針　令和6年度とりまとめ（案）（デジタル庁、2025年3月）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/058ea13e-58e4-4e77-b18f-24833a65c7b1/c543b091/20250304_meeting_identification-guideline-revision_outline_01.pdf

（参考）フェデレーションの対策基準

No.	項目	対策基準の定義方針	NIST SP 800-63-4 2pdの FAL要件との対応
1	信頼関係の確立	• フェデレーションによる連携にあたる信頼関係の確立は事前に行うこと。	“Trust Agreement Establishment”のFAL2に相当
2	設定・登録及び鍵管理	• 識別子や暗号鍵の設定・登録・鍵管理は、静的な方法を基本とするが、動的な方法についても採用可とする。	“Identifier and Key Establishment”のFAL2に相当
3	アサーションに関する対策	• フェデレーショントランザクションは原則として依拠当事者側から開始されること。 • IDプロバイダから連携されたアサーションに対して以下の検証を行うことで、インジェクション攻撃等への耐性を備えること。 ① 想定するIDプロバイダから発行されたものであること ② 第三者により偽造・改ざんされたものでないこと ③ 自身が要求したリクエストに対して発行されたものであること ④ 自身に向けて発行されたものであること ⑤ 再利用されたものでないこと ⑥ 有効期限内であること	“Injection Protection”のFAL2に相当 （NISTよりも要件を具体化して定義）

（出典）デジタル庁　本人確認ガイドライン改定方針　令和6年度とりまとめ（案）（デジタル庁、2025年3月）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/058ea13e-58e4-4e77-b18f-24833a65c7b1/c543b091/20250304_meeting_identification-guideline-revision_outline_01.pdf