資料６－２

# 不適正利用対策に関するWG
# 中間とりまとめ（案）

令和６年６月２０日

総 合 通 信 基 盤 局

# 不適正利用対策に関するワーキンググループについて



■ 令和６年２月から「不適正利用対策に関するワーキンググループ」を開催し、特殊詐欺やフィッシング詐欺等のICTサービスの不適正利用への対処に関し、最近の動向等を踏まえ、専門的な観点から集中的に検討を実施。

| 論　点 | |
|---|---|
| ①　特殊詐欺対策 | 1.　特殊詐欺被害が引き続き深刻な状況。**「足のつかない電話」の発生抑止のため、本人確認書類の偽変造への対応など、本人確認の実効性の向上※に関して取り組むべき事項はあるか。**<br>※非対面契約でのマイナンバーカードの公的個人認証の活用等<br>2.　特殊詐欺に悪用された電話番号の**利用停止スキーム**が効果をあげていることから、本スキームの**適用事業者の拡大**※に向けて取り組むべき事項はあるか。 ⇒電気通信番号制度に係る検討と合流<br>※業界団体に加盟していない事業者等 |
| ②　SMSによるフィッシング詐欺（スミッシング）対策 | 1.　SMSを利用したフィッシング詐欺（スミッシング）の被害が拡大する中、スミッシングメッセージの**発信元※への警告など、実効性ある対応策はあるか。**<br>※マルウェアに感染したスマートフォンの利用者など |

**構成員**

| | | |
|---|---|---|
| 座長 | 大谷　和子 | 株式会社日本総合研究所 執行役員 法務部長 |
| | 沢田　登志子 | 一般財団法人　ECネットワーク　理事 |
| | 鎮目　征樹 | 学習院大学　法学部教授 |
| | 辻　秀典 | デジタルアイデンティティ推進コンソーシアム(DIPC) 代表理事 |
| | 中原　太郎 | 東京大学大学院法学政治学研究科教授 |
| | 仲上　竜太 | 日本スマートフォンセキュリティ協会(JSSEC) 技術部会 部会長 |
| | 星　周一郎 | 東京都立大学 法学部 教授 |
| | 山根　祐輔 | 片岡総合法律事務所　弁護士 |

# 不適正利用対策に関するワーキンググループについて



## 開催状況

| | |
|---|---|
| 第１回（令和６年２月26日） | ○ICTサービスの不適正利用対策を巡る諸課題について<br>○SMSの不適正利用の実態について<br>・事業者ヒアリング：株式会社マクニカ、トビラシステムズ株式会社 |
| 第２回（令和６年３月14日） | ○SMS対策に関する関係者からのヒアリング<br>・事業者ヒアリング：NTTドコモ、KDDI、ソフトバンク<br>・オブザーバーからの報告：警察庁（サイバー警察局） |
| 第３回（令和６年４月15日） | ○SMS対策の方向性（案）について<br>○携帯電話不正利用防止法に基づく本人確認方法の見直し状況について<br>○本人確認に関する関係者ヒアリング<br>・オブザーバーからの報告：警察庁（刑事局）<br>・事業者ヒアリング：楽天モバイル |
| 第４回（令和６年５月15日） | ○本人確認に関する関係者ヒアリング<br>・有識者ヒアリング：デジタルアイデンティティ推進コンソーシアム<br>・事業者ヒアリング：イオンリテール、日本通信 |
| 第５回（令和６年６月６日） | ○携帯電話不正利用防止法に基づく本人確認方法の見直しに係る論点整理・意見交換 |
| 第６回（令和６年６月20日） | ○携帯電話不正利用防止法に基づく本人確認方法の見直しの方向性（案）について<br>○不適正利用対策に関するワーキンググループ中間とりまとめ（案）について |

# SMSの不適正利用対策

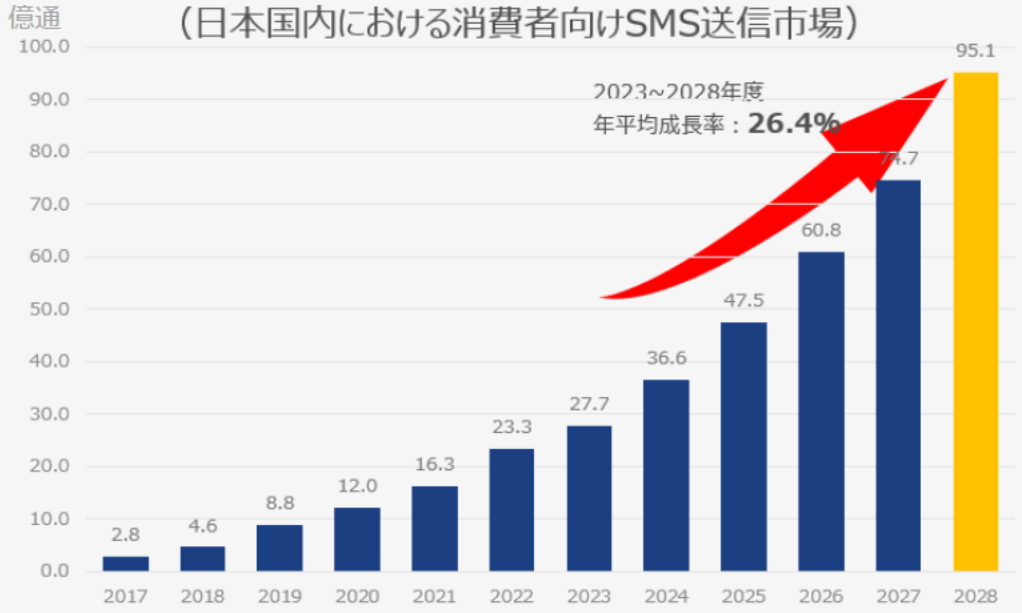
# SMSの不適正利用対策について（第１回WG資料抜粋）

一部誤植修正

## SMSの利活用状況

SMSは、①携帯端末から発信　②SMS配信事業者から発信　があり、特に後者、
企業が発信するSMS通数は年々増加しています。SMSの利点を活かし、様々な業界・用途で活用されています。

国内アグリゲーターとキャリア・アグリゲーターのSMS送信数
（日本国内における消費者向けSMS送信市場）




利用用途例

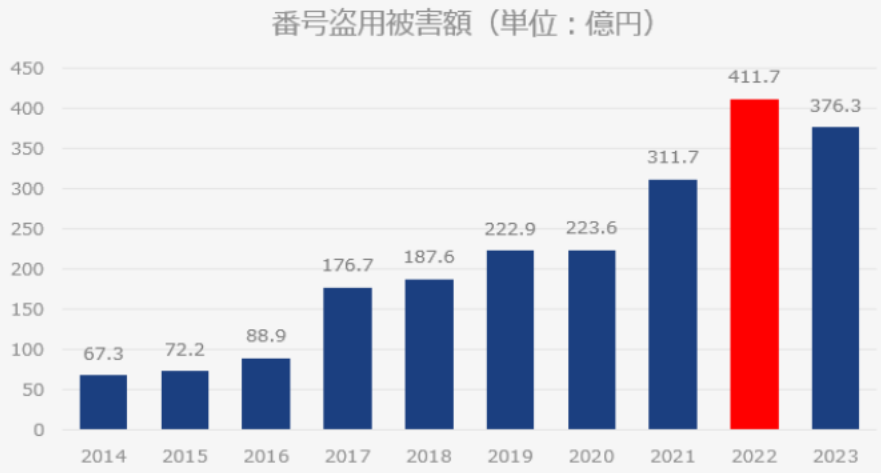

出典：ミックITリポート2024年1月号「2023年度に急ブレーキがかかるも2028年度まで成長期が続くA2P-SMS市場」より。
デロイト トーマツ ミック経済研究所株式会社

# SMSの不適正利用対策について（第１回WG資料抜粋）

## スミッシング詐欺の拡大状況

フィッシング詐欺が深刻な社内問題となる中で、SMSを悪用したスミッシングが注目を集めています。

＜クレジットカードの番号盗用被害額＞
スミッシングがトリガーとなって発生している可能性が考えられます。
2022年は411億円、2023年は376億円の被害が申告されています。




日本クレジット協会　「日本のクレジット統計」
P34 クレジットカード不正利用被害の発生状況　よりマクニカ作図

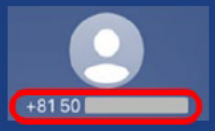
＜インターネットバンキングに関わる不正送金被害額＞
フィッシングによるものと思われる不正送金の被害額も
2023年には、80億円を超えています。

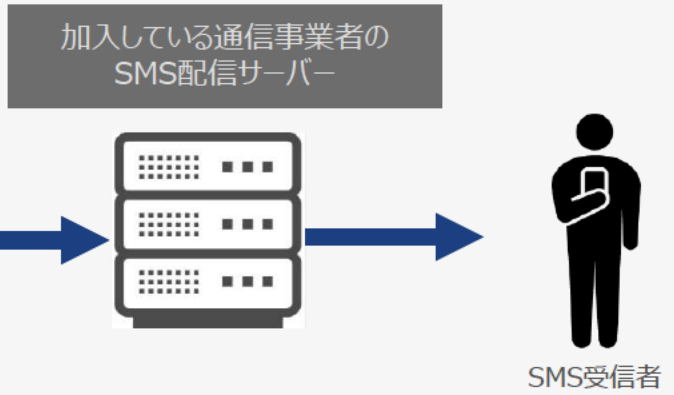

警察庁
フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について
（注意喚起）

一部誤植修正

# SMSの配信経路

配信経路は、①国内携帯電話端末、② 国内SMS配信事業者、③海外通信事業者　の3つのルートがあり、
利用者がSMSを受信する前には**必ず加入している通信事業者のSMS配信サーバーを経由**します。

| 配信経路 | 送信元番号の表示<br>  |
|---|---|
| ①国内携帯電話端末 | 携帯電話番号<br>(090~ 080~ 070~など) |
| ②国内SMS配信事業者 | 国内固定電話番号<br>キャリア共通番号<br>(03~ 0120~ 0005~など) |
| ③海外通信事業者 | 海外電話番号<br>アルファベット<br>ランダムな英数字など |



# SMSの不適正利用対策について（第１回WG資料抜粋）

一部誤植修正

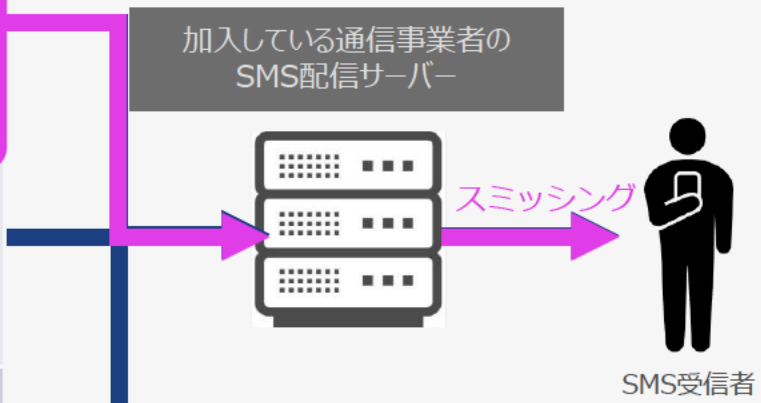
## スミッシングの発信源はマルウェア感染端末

一昔前は海外通信事業者からのスミッシング発信が多かったが、現在は、マルウェア感染した端末が主な発信源となっており、国内発信のスミッシング比率が高くなっています。

| スミッシングの分布比率※ | 配信経路 | 送信元番号の表示 |
|---|---|---|
| **99%** | ①国内携帯電話端末 | 携帯電話番号<br>(090~ 080~ 070~など) |
| | ②国内SMS配信事業者 | 国内固定電話番号<br>キャリア共通番号<br>(03~ 0120~ 0005~など) |
| 1% | ③海外通信事業者 | 海外電話番号<br>アルファベット<br>ランダムな英数字など |

感染端末は、一般の個人が所有し、いたるところで日常利用しているため、対策が非常に難しい

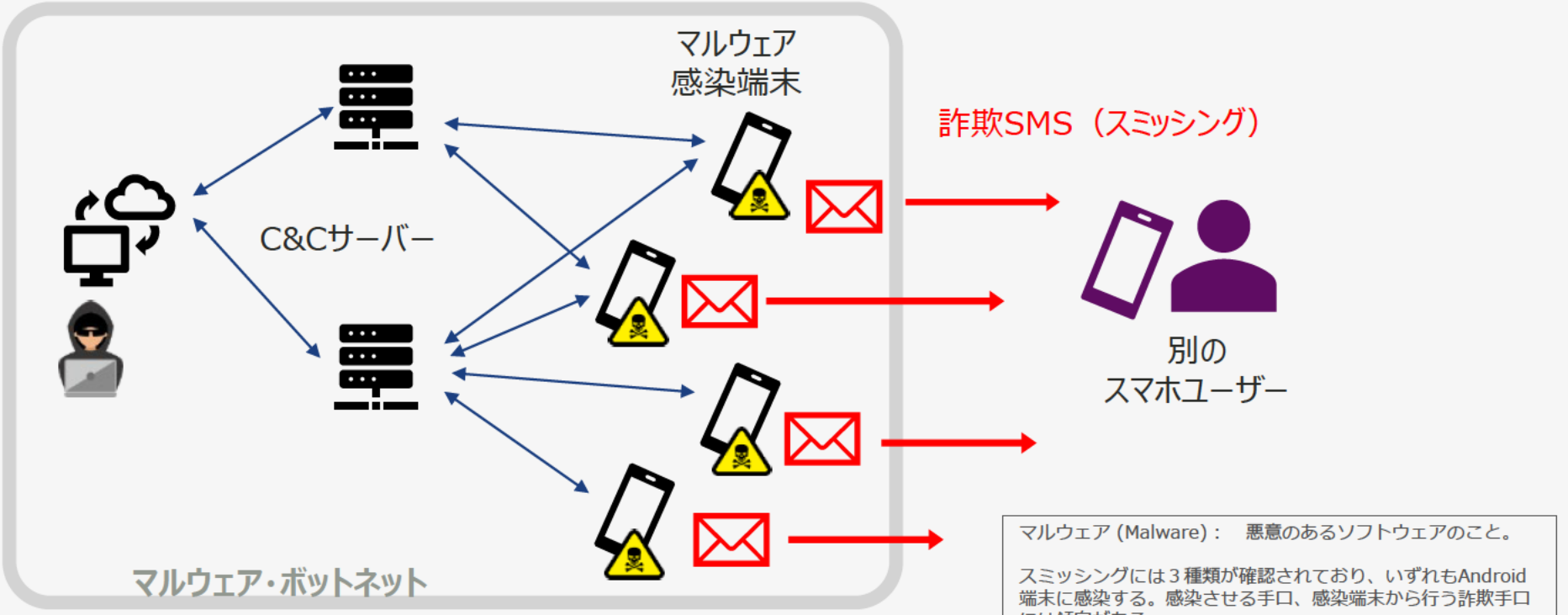
感染数の把握、端末の特定、無害化・・・などが急務である




※：NTTドコモ 三谷咲子様　2023/11/7 JPAAWG6登壇資料
携帯キャリアによるSMSフィッシング(スミッシング)対策の最新情報

# マルウェア感染端末のスミッシング配信のしくみ

スマートフォンが、意図しない不正アプリ導入によりマルウェア感染し（本人は無自覚）、攻撃の踏み台にされています。




マルウェア (Malware)：　悪意のあるソフトウェアのこと。

スミッシングには３種類が確認されており、いずれもAndroid端末に感染する。感染させる手口、感染端末から行う詐欺手口には傾向がある。

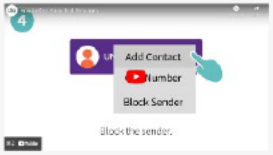
# 海外事例：スミッシング共通窓口による対策推進

通信事業者横断のスミッシング申告として、Spam Reporting Service (7726) が広く使われています。


## １．Spam Reporting Service とは

- 不正SMSを7726に転送すると、通信事業者を横断したSMSトラフィックを分析して、悪用を集約するサービス
- GSMAが2010年にパイロットサービスを開始、現在は個々の通信事業者が実施している
- 7726は、スマホのキーボードで SPAM にあたることから使われている

## ２．Spam Reporting Service のサービス提供例

| 国 | イギリス | アメリカ | ニュージーランド |
|---|---|---|---|
| 運用主体 | Ofcom（情報通信省） | CTIA（携帯電話事業者の業界団体） | DIA（内務省） |
| 概要 | • 利用者は、不正SMSを受信したら7726に転送する<br>• iPhone/Androidの両方から利用可能で、使い方のYouTubeチュートリアルを公開<br>  | • 利用者は、不正SMSを受信したら7726に転送する<br>• iPhone/Androidの両方から利用可能で、使い方のYouTubeチュートリアルを公開<br>  | • Email/SMSに共通の不正申告サイトを設置している<br>• 利用者は、不正SMSを受信したら7726に転送する<br>• iPhone/Androidの両方から利用可能<br>  |
| URL | https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams/7726-reporting-scam-texts-and-calls | https://www.ctia.org/consumer-resources/protecting-yourself-from-spam-text-messages | https://www.dia.govt.nz/Spam-Report-TXT-Spam |

# SMSの不適正利用対策について（第１回WG資料抜粋※一部追記）

一部誤植修正

## 国内事例：通信事業者による迷惑SMS対応

通信事業者３社は、ネットワーク側で不正SMSのブロックを実施しています。
サービス利用の選択はオプトアウト方式で、ユーザはブロックを選択しない場合は、設定をオフに変更可能です。

| | NTTドコモ | au | ソフトバンク |
|---|---|---|---|
| ネットワーク側の対応 | 危険SMS拒否<br>2022/03開始<br>https://www.docomo.ne.jp/info/spam_mail/sms/ | 迷惑SMSブロック<br>2023/02開始<br>https://www.au.com/mobile/service/sms/filter/ | 迷惑SMS対策機能<br>2022/06開始<br>https://www.softbank.jp/mobile/info/personal/news/service/20220602a/ |
| 端末側の対応 | あんしんセキュリティ<br>https://www.docomo.ne.jp/service/anshin_security/ | 迷惑メッセージ・電話ブロック<br>https://media2.kddi.com/meiwakublock/safecall/PC/PC.html | セキュリティOne<br>https://www.softbank.jp/mobile/service/security-one/ |

楽天モバイルはネットワーク側対応、端末側対応側共に未提供

本年７月より「迷惑SMS拒否設定」の提供開始予定（５月発表）

一部誤植修正

# 国内事例：通信事業者の新たな取り組み（RCS、共通番号）

通信事業者はメッセージサービスの高度化のために、電話番号でリッチコンテンツを利用できるRCS、契約する通信事業者に関わらず共通の送信元番号を利用できるキャリア共通番号を提供しています。

## RCSとは

RCS は、世界標準に基づき、SMSと同様に携帯電話番号で送ることができるメッセージサービス

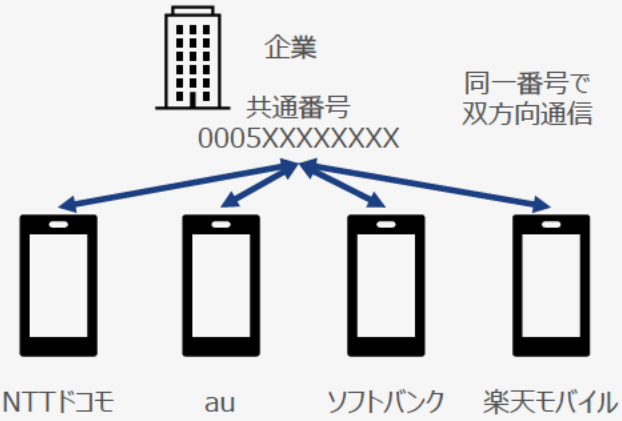
- 正式名称はRich Communication Service
- SMSより、多くの文字数を送付できる
- 公式マークを設定して、メッセージを発信できる
- テキスト以外に画像を送ったり、グループチャットが使える
- 日本では、NTTドコモ・au・ソフトバンクが＋メッセージ、楽天モバイルがRakuten Link の名称でサービスを提供している
- Appleは、RCS Universal Profile を2024年後半にサポートする予定を表明

| 通信事業者 | NTTドコモ | au | ソフトバンク | 楽天モバイル |
|---|---|---|---|---|
| サービス名称 | ＋メッセージ | | | Rakuten Link |

## キャリア共通番号（０００５）とは

通信事業者４社（NTTドコモ、au、ソフトバンク、楽天モバイル）が管理する「0005」から始まる8～10桁の番号

- ユーザが契約している通信事業者に関わらず、送信番号として同じ番号が表示される（通信事業者での審査がある）
- 企業が事前にWebサイトなどで共通番号を公表することで、公表済の番号として携帯4社すべてのお客さまへSMSを届けられる
- 企業は、SMS送信サービス事業者と契約をして番号が割り当てられる



参考

# SMS不適正利用対策事業者連絡会の立ち上げについて



| | |
|---|---|
| 目的 | SMS配信市場が著しく成長し、民間事業者だけでなく地方自治体等の公共機関においてもSMSを活用する機会が増えている一方で、SMSを悪用するフィッシング詐欺（スミッシング）の被害が増加していることを踏まえ、SMSに関わる主要事業者間で、定期的にSMSの不適正利用に係る情報を交換し、事業者間の自主的な対策を推進する。 |
| 活動内容 | ● SMSの不適正利用状況に関する**定期的な情報交換**<br>● SMSの不適正利用対策のための**事業者間の自主的な取組**の検討<br>● スミッシング詐欺対策に関する**利用者への周知広報**の検討 |
| 構成員 | ● 【携帯電話キャリア】 NTTドコモ、KDDI、ソフトバンク、楽天モバイル<br>● 【MVNO】テレコムサービス協会（MVNO委員会）<br>● 【SMS配信事業者】<br>NTTコムオンライン、メディア4u、アクリート、りーふねっと、AI CROSS<br>● 【セキュリティ関係】 マクニカ<br>● 【総務省】 利用環境課、番号企画室　（その他必要に応じて声かけ） |

# SMS対策に関する事業者の動き



- フィッシング対策協議会において、事業者間でスミッシング対策等の意見交換を行うワークショップを開催
- 「フィッシング対策ガイドライン」が更新され、2024年度版として公開（2024年６月４日）
- フィッシング被害抑制対策の22個の要件のうち、10個がSMSに関連し、事業者における対策への活用が期待される

| カテゴリ | # | 要件 | Email | SMS | Web |
|---|---|---|---|---|---|
| 利用者が正規メールとフィッシングメールを判別可能とする対策 | 要件1 | 利用者が確認できるように利用環境と分かりやすい説明に配慮した上で、どのように確認すればいいのかを分かりやすく端的に説明すること。 | ✓ | | |
| | 要件2 | 外部送信用メールサーバーを送信ドメイン認証に対応させること | ✓ | | |
| | 要件3 | 利用者へのメール送信では、制作・送信に関するガイドラインを策定し、これに則って行うこと | ✓ | ✓ | |
| | 要件4 | 利用者に送信するSMSには国内直接接続の配信、または、RCS準拠サービスを利用すること | | ✓ | |
| フィッシング被害を拡大させないための対策 | 要件5 | 利用者が安全にサービスを利用する環境を整えるように促すこと（※旧要件9） | ✓ | ✓ | ✓ |
| | 要件6 | 複数要素認証を要求すること | | | ✓ |
| | 要件7 | 資産の移動に限度額を設定し、変更・移動時は通知を行うこと | | | ✓ |
| | 要件8 | 利用者の通常とは異なるアクセスや登録情報の変更や登録情報の変更に対しては追加のセキュリティを要求すること | | | ✓ |
| | 要件9 | 重要情報の表示については制限を行う | | | ✓ |
| | 要件10 | 不正利用も含めたアクセス履歴の可視化 | | | ✓ |
| ドメイン名に関する配慮事項 | 要件11 | ドメイン名を自社のブランド戦略の一貫として考えること | | | ✓ |
| | 要件12 | 使用するドメイン名と用途の情報を利用者に周知すると | | | ✓ |
| | 要件13 | ドメイン名の登録、利用、廃止にあたっては、自社のブランドとして認識して管理すること | | | ✓ |
| フィッシングへの備えと発生時の対応 | 要件14 | フィッシング対応に必要な機能を備えた組織編制とすること | ✓ | ✓ | ✓ |
| | 要件15 | フィッシング被害に関する対応窓口を明記すること | ✓ | ✓ | ✓ |
| | 要件16 | フィッシングの手法および対策に関わる最新の情報を収集すること | ✓ | ✓ | ✓ |
| | 要件17 | フィッシングサイトへの対応体制の整備をしておくこと | ✓ | ✓ | ✓ |
| 利用者への啓発 | 要件18 | 利用者が実施すべきフィッシング対策啓発活動を行うこと | ✓ | ✓ | ✓ |
| | 要件19 | フィッシング発生時の利用者への連絡手段を整備しておくこと | ✓ | ✓ | ✓ |
| フィッシング被害の発生を迅速に検知するための対策 | 要件20 | Webサイトに対する不審なアクセスを監視すること | | | ✓ |
| | 要件21 | フィッシング検知に有効なサービスを活用すること | ✓ | ✓ | |
| | 要件22 | DMARCレポートやバウンスメールを監視すること | ✓ | | |

※マクニカHPコラム引用（https://www.macnica.co.jp/business/consulting/columns/145478/）

# SMSの不適正利用対策について構成員から頂戴したご意見



## マルウェア感染端末からのSMS発信対策

- マルウェア感染端末/回線の特定及び利用者への警告/注意喚起については、通信の秘密の取扱いに留意した上で、積極的に進めるべきである。（中原構成員ほか）
- 利用者への警告/注意喚起の方法については、実効性のある方法を検討し、その結果マルウェアの削除や対策アプリの導入などの行動変容が実現したかどうかについて、フォローアップすべき。（中原構成員、星構成員、鎮目構成員）
- スミッシングメッセージについて、円滑にユーザーからの申告を受け付けられるようにし、事業者横断で活用できるような環境を整備すべき。（沢田構成員、山根構成員）

## SMS配信者・受信者の不適正利用対策

- 正規のメッセージがきちんと正規のものであると見分けられるよう、SMS発信元の明確化・透明化に係る取組を進めるべき。（沢田構成員）
- 事業者間の連携に当たっては、SMSを利用する側の事業者とも連携してもらいたい。（沢田構成員）
- SMS認証代行が悪用されていることから、対策を進めるべき。（星構成員）
- 国外におけるSMS不適正利用対策の動向を確認し、参考として進めるべき。（仲上構成員）
- 事業者側で行われている各種対策について、まだ利用者の理解が高まっていないことから、周知啓発を行うべき。（大谷構成員ほか）

# SMSの不適正利用対策の方向性（案）



## ①マルウェア感染端末の特定・警告の推進

- 通信の秘密の取扱いに留意した上で、通信キャリアが提供するSMSフィルタリングにおいて得られたデータを分析し、マルウェア感染端末の特定・警告を行う取組を進めることにより、マルウェア感染端末の利用者の損害の拡大の防止に加え、利用者の行動変容を促し、スミッシングメッセージの拡散を抑制する。

## ②スミッシングメッセージの申告受付の推進

- スミッシングメッセージ等の迷惑SMSを受け取った利用者から、さらに円滑に申告を受け付けられるようにしていくとともに、申告データを事業者横断で活用できるようにする仕組みを構築することにより、迅速な迷惑SMS対策ができるようにする。

## ③SMS関連事業者による業界ルールの策定

- SMS不適正利用対策事業者連絡会の枠組を活用し、SMSを利用する側の事業者を含め、関連する業界団体と連携することにより、SMS発信元の明確化・透明化に係る取組や、SMS認証代行事業者等の悪質事業者への対策などを盛り込んだ業界ルールを策定し、正規のメッセージがしっかり正規のものとわかる形で配信されるよう、効果的な対策を実行する。

## ④迷惑SMS対策に係る周知啓発の推進

- スミッシングの攻撃手法は時々刻々と変化をしていることから、官民が連携し、最新の対策方法に関する情報発信を行うとともに、キャリア共通番号の仕組みの周知広報やRCSの活用推進など、SMSに関する利用者のリテラシー向上につとめ、自主的な防衛を推進する。

# 携帯電話不正利用防止法に基づく本人確認方法の見直し

# 「携帯電話不正利用防止法」の概要



## これまでの経緯

■ 平成17年4月、議員立法により「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」が成立。（平成17年法律第31号）

■「レンタル携帯電話事業者による本人確認の厳格化等」を内容とする改正法が平成20年6月成立。同年12月から施行。

## 携帯電話不正利用防止法の概要

**◇ 契約者の管理体制の整備の促進 及び 携帯音声通信サービスの不正利用の防止のため、以下を措置**

**1．契約締結時・譲渡時の本人確認義務等**

・ 携帯電話事業者及び代理店に対し、① 運転免許証等の公的証明書等による契約者の本人確認とともに、② 本人確認記録の作成・保存（契約中及び契約終了後３年間）を義務付け。

**2．警察署長からの契約者確認の求め**

・ 警察署長は、犯罪利用の疑いがあると認めたときは、携帯電話事業者に対し契約者確認を求めることが可能。また、本人確認に応じない場合には、携帯電話事業者は役務提供の拒否が可能。

**3．貸与業者の貸与時の本人確認義務等**

・ 相手方の氏名等を確認せずにレンタル営業を行うことを禁止。 ① 運転免許証等の公的証明書等による契約者の本人確認とともに、② 本人確認記録の作成・保存（契約中及び契約終了後３年間）を義務付け。

**4．携帯電話の無断譲渡・譲受けの禁止**

・ 携帯電話事業者の承諾を得ずに譲渡することを禁止。

**5．他人名義の携帯電話の譲渡・譲受けの禁止**

# 携帯電話の新規契約時本人確認の方法（概要）



## 自然人

- 第三者が入手できない本人確認書類の提示
  （マイナンバーカード、運転免許証・健康保険証・パスポート等）
- 第三者が入手できる本人確認書類の提示・送付（住民票の写し等）
  ＋ 本人確認書類に記載の住所に携帯電話等を書留郵便等により転送不要扱いで送付
  又は
  本人確認書類に記載の住所に事業者が赴いて携帯電話等を交付
- 本人確認書類の写しの送付
  ＋ 本人確認書類に記載の住所に携帯電話等を書留郵便等により転送不要扱いで送付
  又は
  本人確認書類に記載の住所に事業者が赴いて携帯電話等を交付
- ソフトウェアを通じて、本人の容貌の画像を送信
  ＋ 写真付き本人確認書類の画像（本人特定事項記載面や書類の厚み等の特徴等）を送信
  ＋ 写真付き本人確認書類に付属するICチップに記録された本人特定事項を送信
- 特定事項伝達型本人限定受取郵便等により携帯電話等を送付
- 電子署名及び電子証明書を付した本人特定事項の送信

※代理人による契約の場合は、代理人についても本人確認が必要

## 法人

- 本人確認書類（登記事項証明書等）の提示
  ＋ 契約担当者の本人確認
  ※自然人の場合と概ね同じ方法
- 本人確認書類又はその写しの送付
  ＋ 本人確認書類に記載の本店等に携帯電話等を書留郵便等により転送不要扱いで送付
  ＋ 契約担当者の本人確認
  ※自然人の場合と概ね同じ方法
- 電子署名及び電子証明書を付した本人特定事項の送信

※国等との契約の場合は、契約担当者を相手方とみなして本人確認を実施

## 本人確認終了

# 携帯電話不正利用防止法の本人確認に用いることができる公的書類



## 個人の場合

**①提示のみで足りる公的証明書**（契約者の氏名、住居及び生年月日の記載があるものに限る。）

A:運転免許証、運転経歴証明書
B:被保険者証（国民健康保険、健康保険、船員保険、介護保険）
C:医療受給者証、健康保険日雇特例被保険者手帳、国家公務員共済組合員証、地方公務員共済組合員証、私立学校教職員共済加入者証
D:マイナンバーカード、在留カード、特別永住証明書
E:児童扶養手当証書、母子健康手帳、身体障害者手帳、精神障害者保健福祉手帳、療育手帳、戦傷病者手帳
F:パスポート、乗員手帳（契約者の氏名及び生年月日の記載があるものに限る。）
G:そのほか官公庁から発行され、又は発給された書類その他これに類するもので、契約者の氏名、住居及び生年月日の記載があり、当該自然人の写真があるもので、一つだけ発行されているもの

**②提示に加え携帯電話やサンキューレター等の送付が必要な公的証明書**

A:官公庁から発行され、又は発給された書類その他これに類するもので、契約者の氏名、住居及び生年月日の記載があり、当該自然人の写真があるもので、複数発行されているもの
B:印鑑登録証明書、戸籍の附票の写し、住民票の写し、住民票の記載事項証明書（以上、契約者の氏名、住居及び生年月日の記載があるものに限る。）
C:そのほか官公庁から発行され、又は発給された書類その他これに類するもので、契約者の氏名、住居及び生年月日の記載があるもの

**③ソフトウェアを通じて送信できる証明書**

A:契約者本人の顔写真があり、本人特定事項が記録されたICチップが付属している公的証明書（マイナンバーカード、運転免許証等）

**④電子署名（電子署名法第2条第1項）及び電子証明書（電子署名法第4条第1号又は公的個人認証法第3条第1項）**

## 法人の場合

A:登記事項証明書（法人の名称及び本店又は主たる事務所の所在地の記載があるものに限る。）
B:そのほか官公庁から発行され、又は発給された書類その他これに類するもので、法人の名称及び本店又は主たる事務所の所在地の記載があるもの
C:電子署名及び電子証明書（商業登記規則第33条の８第２項に規定するもの）

# デジタル重点計画に基づく非対面の本人確認方法の見直しの方向性



## デジタル社会の実現に向けた重点計画（令和５年６月９日閣議決定）

犯罪による収益の移転防止に関する法律、**携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律（携帯電話不正利用防止法）**に基づく**非対面の本人確認手法**は、**マイナンバーカードの公的個人認証に原則として一本化**し、**運転免許証等を送信する方法**や、**顔写真のない本人確認書類等は廃止**する。対面でも公的個人認証による本人確認を進めるなどし、本人確認書類のコピーは取らないこととする。

## 重点計画を踏まえた見直しの方向性（案）

- 顧客等から顔写真のある本人確認書類を撮影した画像情報の送信を受ける本人確認方法については、精巧に偽変造された本人確認書類が悪用されている実態に鑑み、廃止する。

- 同様に、顧客等から本人確認書類の写しの送付を受ける本人確認方法についても、一般的に写しは偽変造が容易であり、その看破も困難であることから、廃止する。

- 顔写真のない本人確認書類を用いる非対面の本人確認方法については、原則廃止するが、偽造・改ざん対策が施された本人確認書類（住民票の写し等）の原本の送付を受ける本人確認方法については、引き続き、一定条件の下、本人確認に利用可能とする。

- 上記のほか、顔写真のない本人確認書類を用いる対面の本人確認方法についても、上記に準じて見直しを検討する。

# デジタル重点計画に基づく非対面の本人確認方法の見直し方針



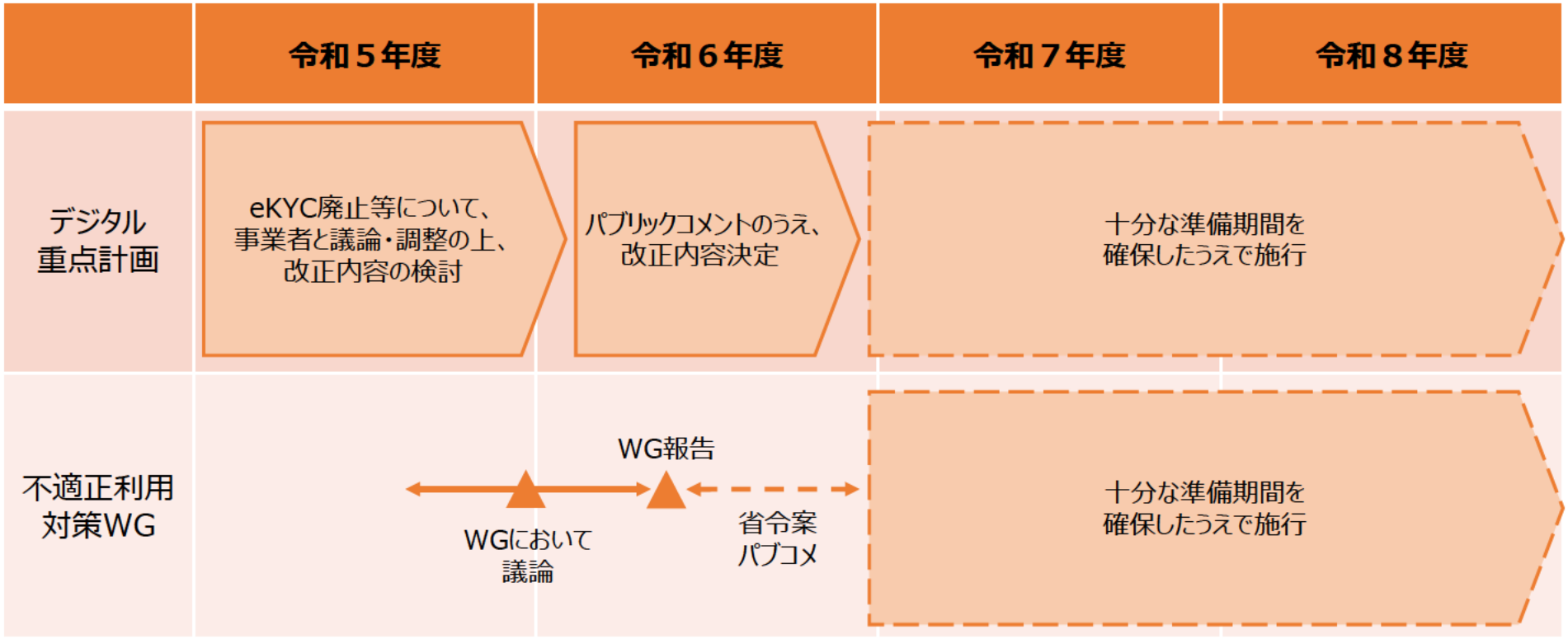
| 対面／非対面 | 規定※ | | 本人確認方法の内容 | 方針 |
|---|---|---|---|---|
| | 契約時・譲渡時 | 貸与時 | | |
| 対面 | イ・ロ | イ・ロ※ | 書類の提示等 | 注：今回のとりまとめで決定 |
| 非対面 | ハ | ハ | 書類の画像＋容貌 | **廃止** |
| | ニ | ニ | ＩＣチップ＋容貌 | 存置 |
| | ホ | ロ※ | 原本＋転送不要郵便等 | 存置 |
| | ヘ | ロ※ | 写し＋転送不要郵便等 | **廃止** |
| | ト | ホ | 特定事項伝達型本人限定郵便 | 存置 |
| | チ | ヘ | 電子署名に係る電子証明書 | 存置 |

※　携帯電話不正利用防止法施行規則の各対応条項を参照
契約時：第３条第１項第１号　　譲渡時：第11条第１項第１号　　貸与時：第19条第１項第１号

※　貸与時の規則第19条第１項第１号ロについては、
・顔写真のない本人確認書類の提示（対面）　・原本の送付（非対面）　・写しの送付（非対面）
の場合に、通常の契約時の転送不要郵便の送付だけでは足りず、
・支払い方法の確認＋転送不要郵便　・本人限定受取郵便
のどちらかを行う確認方法を指しているが、このうち写しの送付（非対面）については廃止する、と言う趣旨である。

# デジタル重点計画に基づく非対面の本人確認方法の見直しスケジュール





# 第３・４回WGにおいて構成員・発表者から頂戴したご意見



## 自然人の本人確認方法

- 本人確認書類の偽変造が大きな問題になっている現状を踏まえると、本人確認書類の券面の画像を確認する方法やその写しを確認する方法は廃止せざるを得ない。（鎮目構成員、山根構成員ほか）
- マイナンバーカードの公的個人認証に原則として一本化していくことについて同意。（鎮目構成員、沢田構成員、仲上構成員ほか）
- 対面の場合においても、ICチップを確認する方法や電子証明書を確認する方法など、デジタル技術を活用した確認方法の導入に向けて検討を進めるべき。（辻構成員、山根構成員、DIPC、イオンリテール、日本通信ほか）
- 利用者に対し、公的個人認証サービスなどのデジタル技術を活用した確認方法についてその意義や重要性をきちんと説明し、普及を進めるべき。（沢田構成員、辻構成員ほか）
- 公的個人認証などのデジタル技術を活用した確認方法の普及に当たっては、事業者に準備コストがかかることから、支援が必要ではないか。（沢田構成員、イオンリテールほか）
- 公的個人認証を利用する事業者・サービスが増えていけば、コストは低廉化していくのではないか。（DIPC）
- デジタル技術を活用する本人確認においては、犯罪への悪用率が下がることから、不適正利用対策にもつながるのではないか。（日本通信）

# 第３・４回WGにおいて構成員・発表者から頂戴したご意見



## 法人の本人確認方法

- 登記情報提供サービスの登記情報を用いた方法の導入について検討すべきではないか。（楽天モバイル、山根構成員）
- 法人の代表者等の本人確認において、電子証明書を活用する確認方法を導入すべきではないか。（日本通信）

## 他の事業者への依拠

- 犯収法で認められる金融機関への依拠の仕組みを導入してはどうか。（楽天モバイル）
- 他事業者への依拠の導入に当たっては、信頼性を確保するため、身元確認レベルを合わせるべきではないか。（大谷構成員、辻構成員、鎮目構成員ほか）
- 金融機関に依拠するとした場合、責任のあり方について留意すべき。（沢田構成員、山根構成員）
- 他事業者への依拠の仕組みを導入する際には、より確実な本人確認方法を用いて確認した実績に基づいて、依拠を行うべきではないか。（大谷構成員、辻構成員ほか）
- 公的個人認証で本人確認を実施済みの事業者に対して、適切な当人認証を行った上で依拠するのであれば、事業者・利用者にとって負担の少なく利便性の高い本人確認が実現できるのではないか。（DIPC）
- 携帯電話事業者間の依拠については、業界全体として、本人確認が適切な方法で行われることが前提となるため、それを踏まえて検討すべき。（星構成員、中原構成員ほか）
- 携帯電話不正利用防止法と犯罪収益移転防止法の確認方法の整合性をはかりながら検討すべき。（辻構成員ほか）

# 第３・４回WGにおいて構成員・発表者から頂戴したご意見



## その他の論点

- 携帯電話が社会のハブとなっており、携帯電話自体が運転免許証と同じような存在になってきていることから、信頼性を確保する必要がある。（星構成員）
- 本人確認書類の写しや画像データの保存については、プライバシーの観点に加えて、漏洩した場合に更に不適正利用されてしまうリスクという観点でも、将来的には検討が必要。（沢田構成員）
- 警察からの求めによる契約者確認の仕組み自体が十分に機能しているかは、常に検証していく必要があるのではないか。（中原構成員）
- 本人確認義務の対象範囲について、将来的には検討していくべき。（星構成員）
- eコマースやSNSのアカウント登録の際に行う本人確認についても、公的個人認証などのデジタル技術を活用する本人確認方法が低コストで使える形で普及するとよい。（沢田構成員）
- デジタル技術の活用が難しい高齢者等の利用者への対応や災害時（通信障害時）の対応として、別の方法を準備するのではなく、デジタル化した方法に対応できるよう、サポートが必要ではないか。（沢田構成員）

# 検討すべき論点（携帯法施行規則第１・３条関係）



## 用語（規則第１条）

- 電子署名、電子証明書の定義の在り方

## 自然人の本人確認方法（規則第３条第１項第１号）

【非対面】

- 写しの送付＋転送不要郵便方式の廃止（規則§3(1)①ヘ）
- eKYC厚み方式の廃止（規則§3(1)①ハ）
- 特定事項伝達型本人限定受取郵便（§3(1)①ト）における電子的な確認方法

【対面】

- 対面提示（規則§3(1)①イ）における電子的な確認方法の導入
  - ICチップを読み取る方法（真贋判定機、券面事項表示ソフトウェア等）
  - 電子証明書を確認する方法
  - スマートフォンに格納された本人確認情報（カード代替電磁的記録）を活用する方法

【非電子的方法】

- 対面における非電子的方法（代替手段）の在り方
- 原本送付＋転送不要郵便方式（規則§3(1)①ホ）の取扱い

# 検討すべき論点（携帯法施行規則第３・４条関係）



## 法人の本人確認方法（規則第３条第１項第２号）

- 登記情報提供サービスとの連携による確認方法の導入
  - （参考）犯罪収益移転防止法施行規則第６条第１項第３号ロ
    ロ　当該法人の代表者等から当該顧客等の名称及び本店又は主たる事務所の所在地の申告を受け、かつ、電気通信回線による登記情報の提供に関する法律（平成十一年法律第二百二十六号）第三条第二項に規定する指定法人から登記情報（同法第二条第一項に規定する登記情報をいう。以下同じ。）の送信を受ける方法（当該法人の代表者等（当該顧客等を代表する権限を有する役員として登記されていない法人の代表者等に限る。）と対面しないで当該申告を受けるときは、当該方法に加え、当該顧客等の本店等に宛てて、取引関係文書を書留郵便等により、転送不要郵便物等として送付する方法）
- その他電子的な確認方法の検討（例：gBizID等）

## その他の確認方法（規則第３条第２項～第５項）

- 既契約者と契約を締結する際の確認方法の在り方
  - 当人認証レベルの確保の在り方
  - 継続的顧客管理との連携（住所変更の確認記録への反映等）

## 代表者等の本人確認方法（規則第４条）

- 自然人の本人確認と同様の見直し
- 電子証明書を確認する方法の導入
- 既契約者（法人）と契約を締結する際の確認方法の在り方

# 検討すべき論点（本人確認済みであることの確認）



## 他の事業者への依拠の在り方

- 引き落とし先の銀行の本人確認への依拠
- 決済手段のクレジットカードの本人確認への依拠
- 他の携帯音声通信事業者の本人確認への依拠
- MNPの際の転出元の本人確認との連携
- 身元確認レベル／当人認証レベルの確保の在り方

## 公的個人認証等で確認済みであることの確認

- 公的個人認証で本人確認を実施済みの事業者（PF事業者・SP事業者）への依拠
- 当人認証レベルの確保の在り方

# 検討すべき論点（携帯法施行規則第５～２０条関係）



## 自然人の本人確認書類（規則第５条第１項第１号）

- ICチップの有無による本人確認書類の取扱い
- 写真のない本人確認書類の取扱い
- 原本送付方式に使用可能な本人確認書類の取扱い

## 本人確認記録（規則第８条）

- 継続的顧客管理との連携（住所変更の確認記録への反映等）

## 本人確認に用いた書類等の保存（規則第１０条）

- 電子的確認方法における保存の在り方

## 譲渡時本人確認の方法（規則第１１条）

- 役務提供契約締結時の確認方法と同様の見直し

## 契約者確認の方法（規則第１３・１４条）

- 電子的な確認方法の導入
- 遠隔地居住の際の確認方法の在り方

## 貸与時本人確認の方法（規則第１９・２０条）

- 役務提供契約締結時の確認方法と同様の見直し

# 第５回WGにおいて構成員から頂戴したご意見



## 対面における電子的な確認方法

- マイナンバーカードに係る機能のスマートフォンへの搭載の仕組み（カード代替電磁的記録）の活用を進めるべき（辻構成員、山根構成員ほか）
- 対面におけるICチップの読み取りによる確認方法の導入に当たっては、単にICチップを読み取ることを要件とするのではなく、セキュアなICチップに格納された本人特定事項を券面情報等と照合するなど、セキュリティの確保されたICチップの中の情報を確認する方法とすべき（辻構成員、山根構成員ほか）

## 非電子的な確認方法の在り方

- 何らかのやむを得ない理由により、ICチップ付き本人確認書類を所持できない場合など、代替手段として非電子的な確認方法を認めることは考えられる（鎮目構成員ほか）
- 非電子的な確認方法は、あくまで例外的な確認方法とし、やむを得ない場合に限り、補充的に理由できることとすべきではないか（鎮目構成員、星構成員、山根構成員、大谷構成員ほか）
- 非電子的な確認方法の検討に当たっては、電子的な確認方法と比較して悪用リスクが高くならないよう、検証を行う必要がある（中原構成員ほか）

## 他の事業者への依拠の在り方

- 他の事業者への依拠の検討に当たっては、当該事業者における身元確認レベルが一定以上（例えば、公的個人認証等で確認済み）であることを確認できた場合に限り依拠を行うこととすべき（辻構成員、大谷構成員、沢田構成員ほか）

# 携帯電話不正利用防止法の本人確認方法の見直しの方向性（案）



## ①自然人の本人確認方法

- 非対面における券面を確認する方法（写しの送付方式、eKYC厚み方式）の廃止
- 対面における電子的な確認方法（ICチップの読み取り等）の義務化（特定事項伝達型本人限定受取郵便を含む）
- カード代替電磁的記録（マイナンバーカードの機能のスマートフォンへの搭載）の活用による確認方法の導入
- 例外的な確認方法としての非電子的な確認方法の存置

## ②法人の本人確認方法

- 登記情報提供サービスとの連携による確認方法の導入
- 法人の契約担当者（代表者等）の本人確認における電子証明書の導入

## ③過去の確認結果への依拠

- 公的個人認証で本人確認を実施済みの事業者への依拠の導入
- 当人認証レベルの確保（多要素認証等）
- 継続的顧客管理による確認記録の更新（住所変更の確認記録への反映等）

## ④その他の見直し事項

- 譲渡時・貸与時本人確認における同様の見直し
- 電子的確認方法における確認記録への保存の在り方の見直し
- 警察からの求めに基づく契約者確認方法の見直し
- 犯罪収益移転防止法との整合性の確保

→ 十分な準備期間を確保した上で省令改正の施行時期を決定する。

# 本人確認方法の見直し以外の留意事項



## デジタルデバイド等への対応

- デジタル技術の活用が難しい高齢者等の利用者への対応や災害時（通信障害時）の対応として、別の方法を準備するのではなく、デジタル化した方法に対応できるよう、サポートが必要ではないか。

## 本人確認の意義に係る周知広報

- 携帯電話不正利用防止法の目的や、契約時の本人確認の意義・重要性について、利用者に対する説明を行うとともに、周知広報を進めるべき。

※参考　携帯電話不正利用防止法　目的規定

（目的）

第一条　この法律は、携帯音声通信事業者による携帯音声通信役務の提供を内容とする契約の締結時等における本人確認に関する措置、通話可能端末設備等の譲渡等に関する措置等を定めることにより、携帯音声通信事業者による契約者の管理体制の整備の促進及び携帯音声通信役務の不正な利用の防止を図ることを目的とする。