資料４－３

不適正利用対策に関する
ワーキンググループ報告書（案）

令和６年〇月〇日

不適正利用対策に関するワーキンググループ

はじめに. 2
第１部　SMS の不適正利用対策 3
第１章　現状と課題. 3
１　SMS 及びその送信経路 3
２　SMS の犯罪利用 5
３　通信事業者等の対策の状況. 7
４　諸外国の取り組み. 10
第２章　対策の方向性. 11
１　SMS フィルタリングサービスを活用したマルウェア感染端末の特定・注意喚起の推進. 11
２　スミッシングメッセージの申告受付の推進. 13
３　SMS 関連事業者による業界ルールの策定 14
４　迷惑 SMS 対策に係る周知啓発の推進. 14
第２部　携帯電話不正利用防止法に基づく本人確認方法等の見直し. 15
第１章　　現状と課題 15
１　電話を巡る特殊詐欺の状況及び現在の対策. 15
２　デジタル重点計画に基づく非対面における本人確認方法の見直し. 17
３．新たな本人確認方法等の検討. 18
(1)　自然人の本人確認方法. 19
(2)　法人の本人確認方法. 20
(3)　過去の確認結果への依拠. 21
(4)　その他の事項. 24
第２章　携帯電話不正利用防止法に基づく本人確認方法等の見直しの方向性. 25
１　非対面における券面を確認する方法の廃止. 25
２　対面における電子的な確認方法の義務化. 25
３　例外的な確認方法としての非電子的な確認方法の存置. 25
４　登記情報提供サービスとの連携による確認方法の導入. 25
５　法人の契約担当者の本人確認における電子証明書の導入. 25
６　過去の本人確認結果への依拠. 26
７　継続的顧客管理による確認記録の更新. 27
８　その他見直し事項. 27
おわりに. 28

はじめに

総務省では、「オレオレ詐欺等対策プラン」（令和元年６月 25 日犯罪対策閣僚会議決定）や「ＳＮＳで実行犯を募集する手口による強盗や特殊詐欺事案に関する緊急対策プラン」(令和５年３月17日犯罪対策閣僚会議決定)も踏まえながら、携帯電話不正利用防止法、犯罪収益移転防止法及び電気通信事業者による特殊詐欺に利用された固定電話番号等の利用停止等スキーム等により、特殊詐欺への対策を実施してきたところである。

しかし、令和５年における特殊詐欺の被害額は約 452.6 億円と前年から約 80 億円も増加しており、また、キャッシュレス決済の普及等が進む中で、実在する企業等を装い、ID・パスワード等を詐取して不正送金等を行うフィッシングについても、インターネットバンキングに係る不正送金被害が令和５年に約 87 億円となり過去最多となった。

このように犯罪の手口が急激に巧妙化、多様化することにより引き起こされる詐欺等の被害が加速度的に拡大している状況に対処すべく、特殊詐欺、ＳＮＳ型投資・ロマンス詐欺及びフィッシングを対象にした「国民を詐欺から守るための総合対策」（令和６年６月 18 日犯罪対策閣僚会議決定)が策定されたところである。

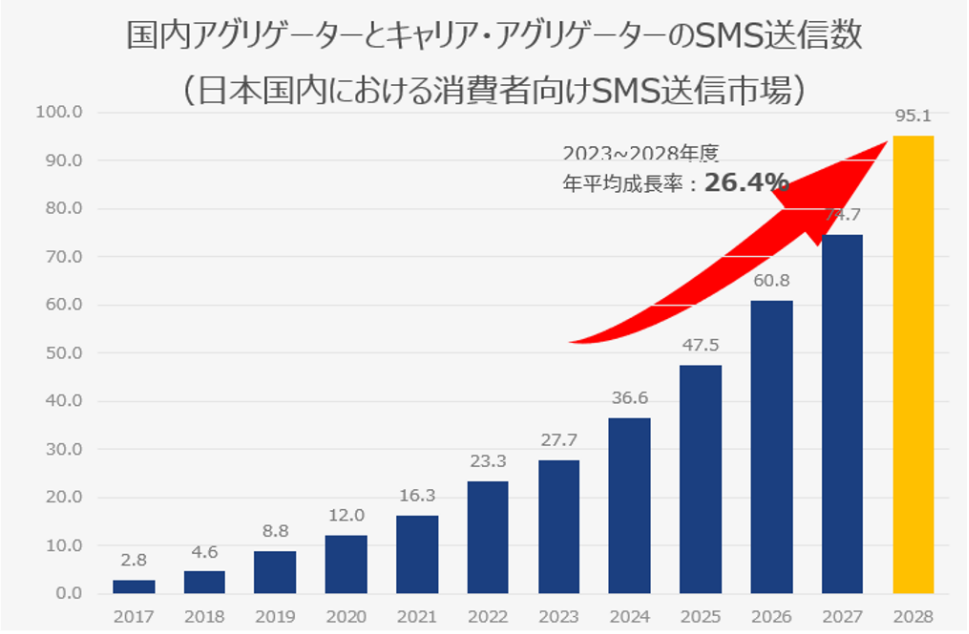
上記の状況も踏まえながら、ICT サービスを悪用した特殊詐欺及びフィッシングをより効果的に防止するため、更なる対策を講じる必要がある。

第１部　SMS の不適正利用対策

第１章　現状と課題

１　SMS 及びその送信経路

SMS（ショートメッセージサービス）とは、電話番号を宛先にし、携帯電話事業者のネットワークを介して、短いテキストをやりとりするメッセージングサービス。[1]現在では、基本機能として携帯電話・スマートフォンに基本的に標準搭載されている。相手方の電話番号がわかれば、簡単にメッセージを送れることから、簡易な連絡手段として、利用者間で利用される。また、受信者側のアクションを促しやすいことから、その利便性を活かし、事業者が利用者に宛てて、本人確認時のワンタイムパスワードの送信やアンケート、督促等を送信する際に用いるなど、幅広い用途にも用いられており、ビジネス利用も増加している。SMS を一斉送信するサービスを提供する SMS 配信事業者から送信される SMS の通数は年々増加しており、2023 年度には、27.7 億通だったものが、2028 年度には 95.1 億通になるとの予測もある。[2]



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

図１　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[3]

---

[1] 迷惑メール対策推進協議会「迷惑メール白書　2022-24 年度版」２ページ　引用
[2] ミック IT リポート 2024 年１月号、デロイトトーマツミック経済研究所株式会社
[3] 第１回資料 1-3「SMS・スミッシングについて（株式会社マクニカ）」４ページ　抜粋。なお、「アグリゲーター」は SMS 配信事業者を指す。

SMS の送信経路は主に３つに分けることができる。一つ目は、国内携帯電話端末から配信される方法であり、この場合、受信者側には、相手方の送信した携帯電話番号が表示される。二つ目は、国内の SMS 配信事業者から送信される方法であり、受信者側には、03 や 0120 から始まる国内の固定電話番号等や 0005 から始まるキャリア共通番号などの番号が表示される。三つ目は、海外通信事業者から送信される方法であり、受信者側には、海外電話番号のほか、外国語やランダムな英数字が表示されることがある。なお、いずれの送信経路の場合も、受信者が加入している国内キャリア[4]の SMS 配信サーバーを経由して送信される。

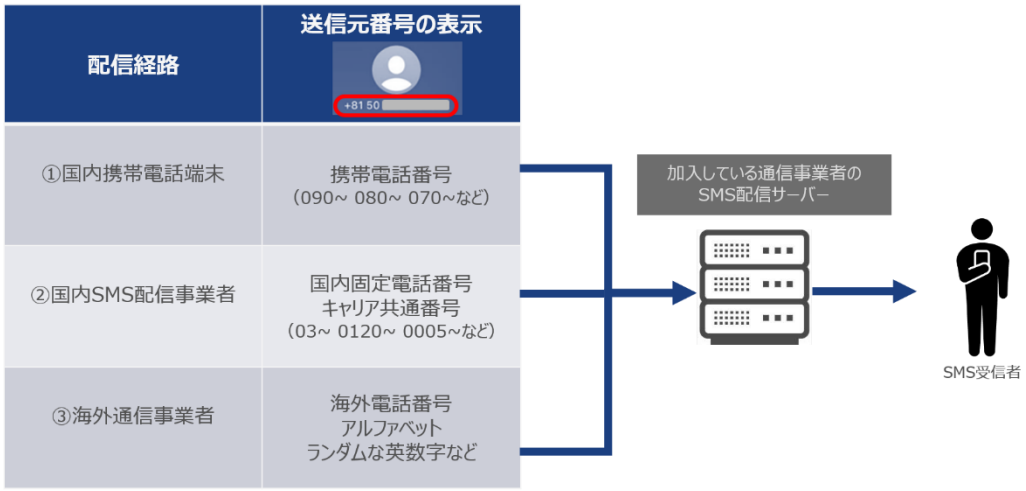


図２　SMS の配信経路[5]

[4] (株)NTT ドコモ、KDDI(株)、ソフトバンク(株)、楽天モバイル(株)を指す。
[5] 第１回資料 1-3「SMS・スミッシングについて（株式会社マクニカ)」５ページ　抜粋

２　SMS の犯罪利用

近年、実在する企業・金融機関等を装って、電子メールや SMS を送信するなどしてリンクから偽サイトに誘導し、ID・パスワード等を入力させ、個人情報を詐取するフィッシングによる詐欺の被害が拡大している。(一社) 日本クレジット協会の調査では、令和５年のクレジット番号盗用被害額は約 504.7 億円に、また、警察庁の調査では、令和５年のインターネットバンキングに係る不正送金被害額は約 87 億円に及んでおり、被害は深刻なものとなっている。

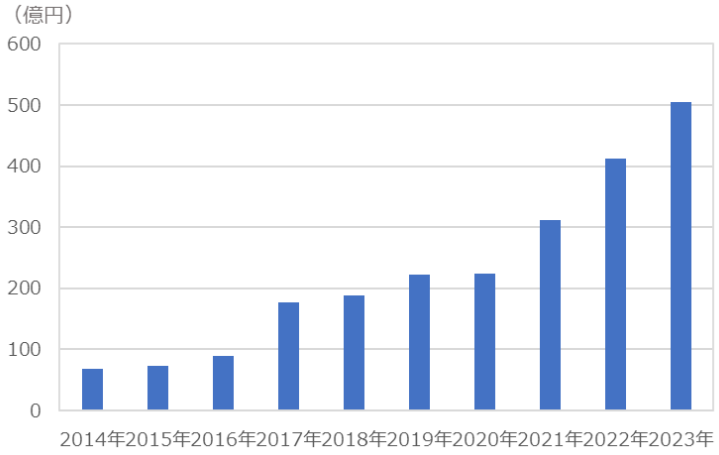


図３　クレジット番号盗用被害額の推移[6]

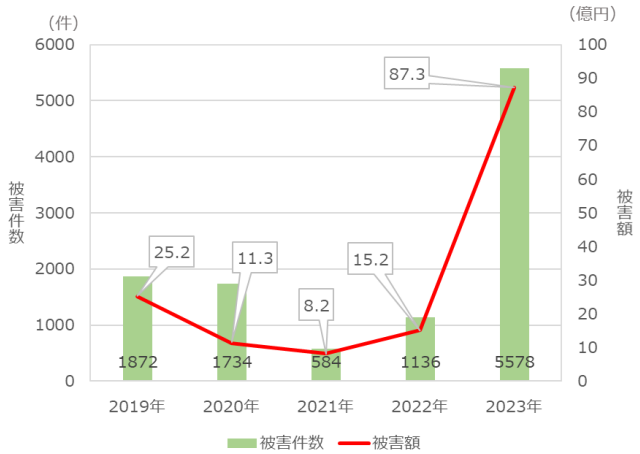


図４　インターネットバンキングに係る不正送金被害額の推移[7]

---

[6] （一社）日本クレジット協会調査（https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf?a8=Vhfv-h6e1m0TdmZdQG0HmKZUHmoWuezvlG0TEHZaelCe1mfZIm7mPm0kIYcipi7u3lRdA2fz3hfvss00000020151001?a8）から作成

[7] 国民を詐欺から守るための総合対策（概要）（犯罪対策閣僚会議（令和６年６月 18 日決定）から作成

上述のとおり、SMS は、ビジネスにおいても簡易な連絡手段として活用されているが、電話番号さえわかればメッセージを送信できることが悪用され、フィッシングメッセージの送信[8]にも多く利用されている。なお、SMS を悪用するフィッシングは、スミッシングと呼ばれている。かつては海外通信事業者を経由したスミッシングメッセージが多いとされていたが、現在、(株)マクニカの発表によれば、不正 SMS メッセージのうち約 99%が、マルウェアに感染した国内の個人の端末から送信されていることが判明している。そうした端末は、一般個人が所有しており、端末利用者本人も気づいていないまま勝手に SMS を送信されていることが多いと考えられるため、マルウェア感染を防ぐための対策が急務となっている。

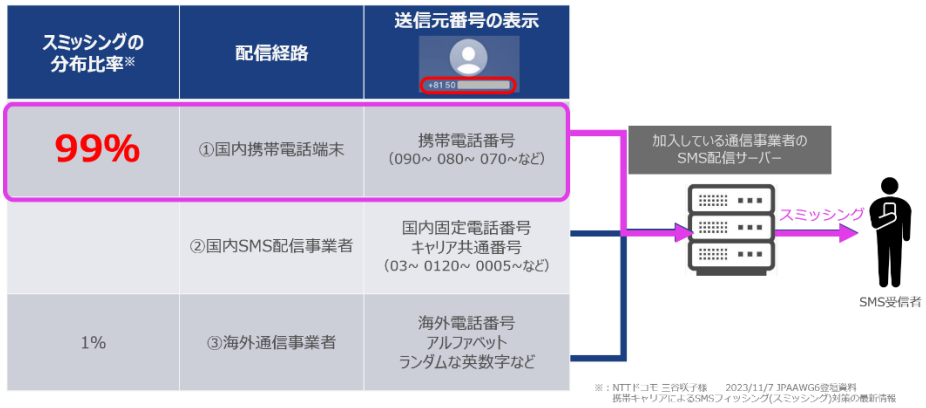


図５　スミッシングの送信経路ごとの発生分布[9]

また、スミッシングの他にも、ポイントの不正取得やフリーマーケットサイトにおける不正出品等に利用するサービスアカウントの不正取得をするために、本人の代わりに SMS 認証のやり取りを行い、認証コード等を転送することで SMS 認証を代行する、「SMS 認証代行」と呼ばれる手口が発生しており、同様に対策が必要となっている。

[8] メッセージ中の URL をクリックさせ、フィッシングサイトに誘導し、個人情報を抜き取ったり、マルウェアを感染させたりする手口などがある。
[9] 第１回資料 1-3「SMS・スミッシングについて（株式会社マクニカ）」10 ページ　抜粋

３　通信事業者等の対策の状況

スミッシングの対策に当たっては、SMS を送信するネットワーク側における対策と SMS を受け取る端末側における対策が考えられるが、国内キャリアでは、ネットワーク側における対策として、SMS フィルタリングサービスをデフォルトオン[10]で導入しており、SMS メッセージ内の URL や電話番号、発信者などの情報を総合的に分析した上で危険だと判断されるものをネットワーク側でブロックしている。

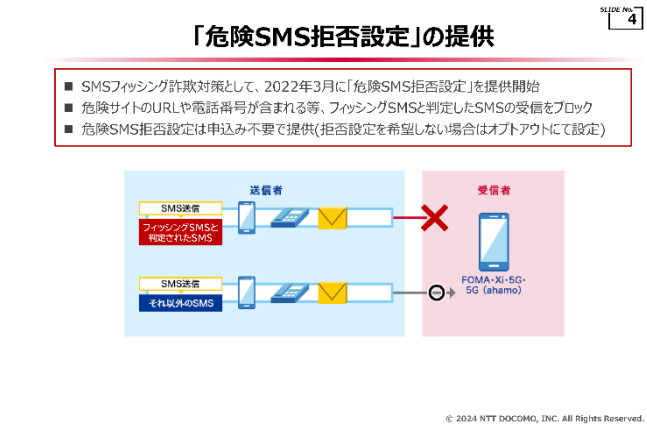


図６　(株)NTT ドコモが提供する危険 SMS 拒否設定[11]

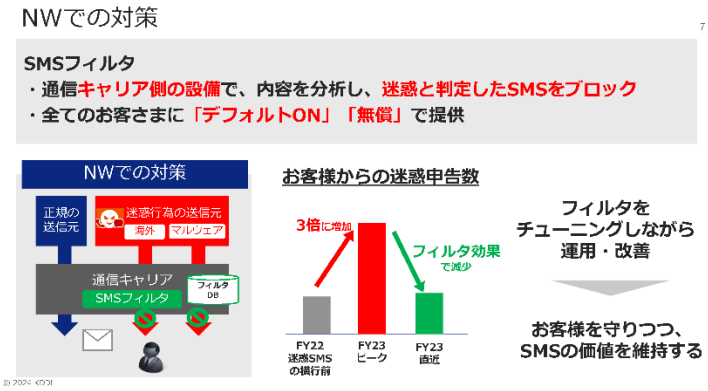


図７　(株)KDDI が提供する迷惑 SMS ブロック[12]

---

[10] SMS フィルタリングサービスの適用については、メールのフィルタリングサービスと同様に、オプトアウト付きの包括同意に基づいてサービス提供が行われている。
[11] 第２回資料 2-1「フィッシング SMS 対策の現状取組みについて（株式会社 NTT ドコモ)」４ページ　抜粋
[12] 第２回資料 2-2「携帯電話キャリアによる迷惑 SMS 対策の取組状況（KDDI 株式会社)」７ページ　抜粋

図８　ソフトバンク(株)が提供する迷惑 SMS 対策機能[13]

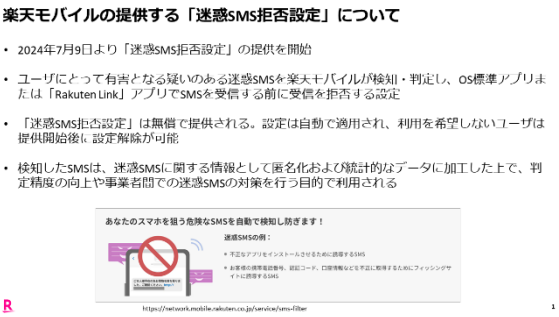


図９　楽天モバイル(株)が提供する迷惑 SMS 拒否設定

端末側における対策としては、キャリア等が提供しているアプリケーションをインストールすること等により、迷惑 SMS を自動で専用フォルダに振り分けたり、受信時に警告を表示するサービスが提供されている。

また、RCS[14]の規格を利用した、NTT ドコモ(株)、KDDI(株)、ソフトバンク(株)が提供する「＋メッセージ」のサービスでは、送信元の電話番号によりフォルダを分けて表示する、３社の審査を通過したアカウントに対して認証済みマークを付与する等、正規のメッセージか否かを判断するための取組が行われている[15]。

---

[13] 第２回資料 2-3「迷惑 SMS 動向（ソフトバンク株式会社)」２ページ　抜粋
[14] 正式名称は「Rich Communication Service」といい、SMS と同様に電話番号を用いて送信することができるサービスであり、SMS より多くの文字数を送信したり、画像を送信することができる。
[15] 同様に RCS の規格を利用した、楽天モバイルが提供する「Rakuten Link」についても、公式アカウントへの認証済みマークの付与等、正規のメッセージか否かを判断するための取組が行われている。

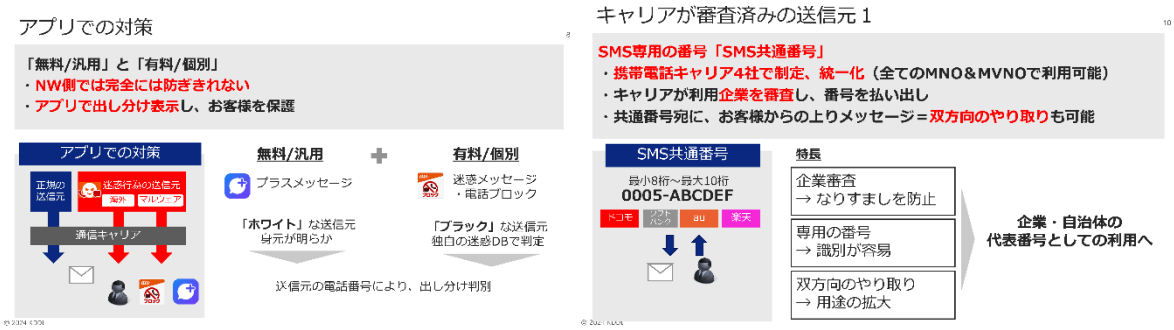


図 10　＋メッセージにおけるスミッシング対策[16]

事業者等において様々な対策がとられている中ではあるが、受信者は、正規の SMS を見抜くことが難しいことから、企業が送信する SMS について、受信者が契約する国内キャリアに関わらず、0005 から始まる共通の送信元番号を表示できる「キャリア共通番号」を提供するサービスが 2021 年６月から開始されている。キャリア共通番号を用いてメッセージの送信を行う場合、SMS 配信事業者は、キャリア共通番号の利用を希望する者を事前に確認している。また、送信者は、この共通番号を自社の Web サイト等に公表することにより、受信者は、安心してメッセージを受信することが可能となる。

さらに、（一社）フィッシング対策協議会において、事業者間でフィッシング対策について意見交換を行うワークショップが開催されており、フィッシング対策ガイドラインが更新されている。同ガイドラインにおいて示された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 に関連するものであり、事業者における対策への活用や事業者間で連携した対策の実施が期待される。

[16] 第２回資料 2-2「携帯電話キャリアによる迷惑 SMS 対策の取組状況（KDDI 株式会社）」９，11 ページ　抜粋

４　諸外国の取り組み

諸外国では、通信事業者横断のスミッシング申告窓口として、Spam Reporting Service（7726）が用いられている例がある。不審な SMS メッセージを受信した利用者から、当該メッセージの転送を受け、その情報を集約するサービスであり、これにより、スミッシングの傾向やパターンを、通信事業者を横断した SMS トラフィックを用いて分析することが可能となる。

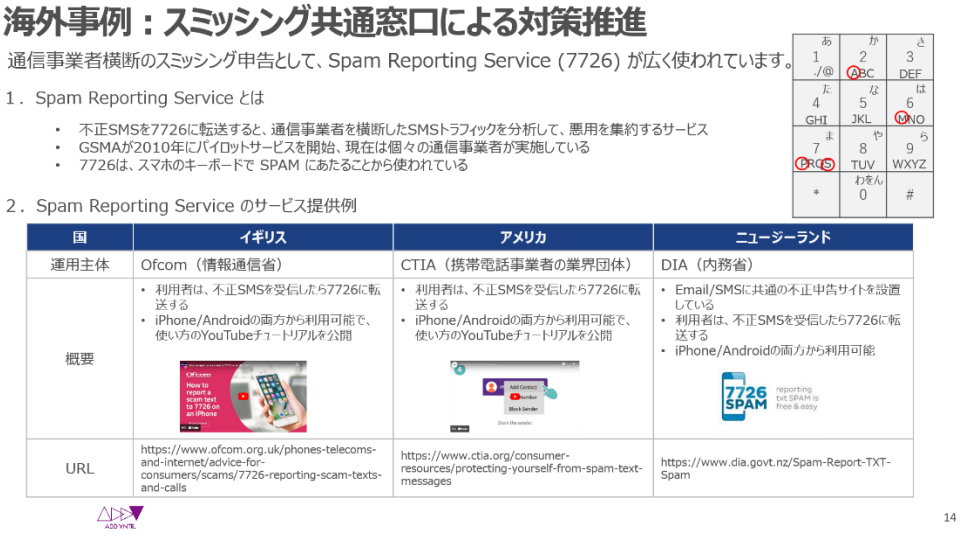


図 11　諸外国におけるスミッシング申告の受付状況[17]

[17] 第１回資料 1-3「SMS・スミッシングについて（株式会社マクニカ）」10 ページ　抜粋

第２章　対策の方向性

１　SMS フィルタリングサービスを活用したマルウェア感染端末の特定・注意喚起の推進

不正 SMS メッセージのうち約 99%が、マルウェアに感染した個人端末から送信されている現状を踏まえると、マルウェア感染した端末及び回線を特定の上、同端末及び回線利用者への注意喚起を行うことが必要である。

これまで通信キャリアでは、迷惑 SMS 対策として、各社ごとにフィルタリング機能を提供していたところであるが、スミッシング被害がますます深刻化している状況を踏まえ、通信キャリアが、事業者自身の SMS フィルタリングサービスでブロックした SMS メッセージの通信内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報に基づきマルウェア感染端末の利用者を特定した上で、特定した利用者に対して電子メールの送付等の方法により注意喚起を行うことが考えられる。

この取組を実施するに当たっては、SMS フィルタリングサービスでブロックした SMS メッセージの通信内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報等と、通信キャリアが保有している契約者情報、通信履歴等を照合し、当該端末に係る通信回線の契約者及び連絡先を特定する行為は通信の秘密の窃用等に該当することから、これをどのように整理するかが論点となる。通信当事者の有効な同意がある場合には、通信当事者の意思に反しない利用であるから、通信の秘密の侵害には該当しないとされている。この点に関して、有効な同意があるとは、原則として、通信の秘密を取り扱うことに対する認識、認容がある場合をいい[18]、通常は、契約約款等に基づいた事前の包括同意のみの場合を含まない。ただし、次の場合には、例外的に、契約約款等による事前の包括同意であっても、有効な同意といい得る場合があるとされている[19]。

① 利用者が、事業者において通信の秘密を取り扱うことについて通常承諾すると想定し得るため、契約約款等による同意になじまないとはいえない場合であって、

② 利用者に将来不測の不利益が生じるおそれがない場合

---

[18] 同意の有効性に疑義を招かないためには、外形的にみても明確な同意を得ることが要求されることから、「個別具体的かつ明確な同意」が必要とされている。

[19] 「電気通信事業におけるサイバー攻撃の適正な対処の在り方に関する研究会　第三次取りまとめ」（平成 30 年９月 26 日公表）p.10

本件のケースについては、個別具体的な同意よりも事前の包括同意の方が、効果的であると考えられ、以下、マルウェアに感染している可能性が高い端末の利用者の特定及び注意喚起について、契約約款等に基づく包括的な同意を取得することで足りると解する余地があるか検討する。

① 契約約款等による同意になじむか

マルウェアに感染している端末については、知らぬ間に大量の SMS メッセージが送信されて高額の携帯電話料金が生じていること、場合によっては送信者が「詐欺師扱い」されるなど風評被害も生じ得ること等からすれば、マルウェアに感染している端末の利用者に対する注意喚起を通信キャリアが行うことは、一般的、類型的に見て、利用者における安心・安全な通信環境の確保に向けられた行為といえる。また、このような注意喚起を行うために、通信の秘密に当たる情報のうち、SMS フィルタリングサービスでブロックした SMS メッセージの通信内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報（例えば、通信日時）[20]を元に、利用者の具体的な氏名及び連絡先を確認し、当該端末の利用者を特定する行為についても、一般的、類型的にみて、利用者における安心・安全な通信環境の確保に向けられた行為といえる。したがって、通常の利用者であれば、自らが利用している端末についてマルウェアに感染している可能性が高い場合には、注意喚起に必要最小限の範囲において通信キャリアが通信の秘密を利用することを承諾することが想定し得ることから、①の要件を満たすと解される[21]。

② 利用者において将来生じる不測の不利益を回避し得るか

注意喚起に関して利用される通信の秘密の対象、範囲は上記で述べたとおり明確であり、利用者に不測の不利益が生じる可能性は高くない。このような状況下で、以下のような条件を満たす場合には利用者が不測の不利益を被る危険を回避できると考えられる旨整理されていることを参考に、次の条件を満たす場合は、②の要件も満たすと解される[22]。

- a 注意喚起を希望しない者（オプトアウトした者）の利益が侵害されないような態勢を整える

---

[20] 本整理に基づいて、マルウェア感染端末の特定・注意喚起を実施する場合には、通信の秘密の問題を含むため、同意取得方法につき総務省に相談の上実施することが望ましい。

[21] 一例として、通信事業者のスミッシング対策検討におけるサンプル調査において、調査対象の８割以上の者の利用意向を確認した事例がある。

[22] 「電気通信事業におけるサイバー攻撃の適正な対処の在り方に関する研究会　第三次取りまとめ」（平成 30 年９月 26 日公表）p.13

- b 利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更できる（設定変更できる）ようにする
- c 同意内容の変更の有無にかかわらず、その他の提供条件が同一である契約内容とする
- d 本件対策の内容とともに、注意喚起を望まない利用者は随時同意内容を変更できる（設定変更できる）こと及びその方法につき利用者に相応の周知を図る[23]

以上から、通信キャリアが提供する SMS フィルタリングサービスでブロックした SMS の通信通内容等を用いて注意喚起すべきマルウェア感染端末を検知し、通信に係るログ情報を利用し、マルウェア感染端末を使用している利用者を特定の上、個別に注意喚起を行う取組については、上述の条件を満たす場合には、契約約款等による包括同意であっても本件対策を行うための通信の秘密に属する事項の利用等について有効な同意であるということができ、有効な同意に基づいて実施するのであれば、通信の秘密の侵害に当たらないと整理することができる。

通信キャリアにおいては、本整理を参考にすることで、利用者の有効な同意を得た上でマルウェア感染端末を特定し、個別に注意喚起を行うことなど、利用者の損害の拡大防止を図り、スミッシングメッセージの拡散の抑制の取組が包括的に推進されることを期待する。[24]

２　スミッシングメッセージの申告受付の推進

ニュージーランドでは、政府においてスミッシングメッセージの申告を受け付け、その情報を元に対策を講じている。我が国においては、現在、国内キャリアや事業者団体を中心に、スミッシングメッセージの申告を受け付けているが、申告情報の横連携も限られているといった意見があった。これらを踏まえ、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が、国内キャリア等へさらに円滑に申告をできるようにしていくとともに、国内キャリア等が保持する迷惑 SMS に係る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、迅速で実効的な迷惑 SMS 対策を講じることが必要である。

---

[23] 利用者に対し、契約締結時に書面等を用いて明確に説明することが考えられる。また、既に契約している者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によってマルウェアに感染している可能性が高い端末の利用者に対して注意喚起をすることを周知するとともに随時同意内容を変更できる（設定変更できる）こと及びその方法を説明すること等が考えられる。

[24] 令和６年７月から(株)NTT ドコモにおいて、「意図せぬ迷惑メッセージ送信に関するお知らせ」の提供が開始された。

３　SMS 関連事業者による業界ルールの策定

従前より迷惑メールやフィッシングへの対策を協議する場は存在しているが、令和６年３月に、総務省として、国内キャリア、SMS 配信事業者、セキュリティ事業者等が参加する SMS 不適正利用対策事業者連絡会を立ち上げ、SMS に特化して情報交換を行っている。本連絡会の枠組みを活用し、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必要がある。

４　迷惑 SMS 対策に係る周知啓発の推進

時々刻々と変化するスミッシングの攻撃手法に合わせ、通信事業者において様々な対策がとられているが、利用者の認知度は低くとどまっているといった意見があった。これに関し、官民が連携し、最新のスミッシング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認証アカウント等の機能を持った 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ことが必要である。

第２部　携帯電話不正利用防止法に基づく本人確認方法等の見直し

第１章　現状と課題

１　電話を巡る特殊詐欺の状況及び現在の対策

特殊詐欺とは、被害者に電話をかけるなどして対面することなく相手を信頼させ、現金等をだまし取る犯罪を言い、オレオレ詐欺や預貯金詐欺、キャッシュカード詐欺等の手口が存在する。令和５年の特殊詐欺の被害額は 452.6 億円（前年比 22.0%増）[25]に及んでいる。

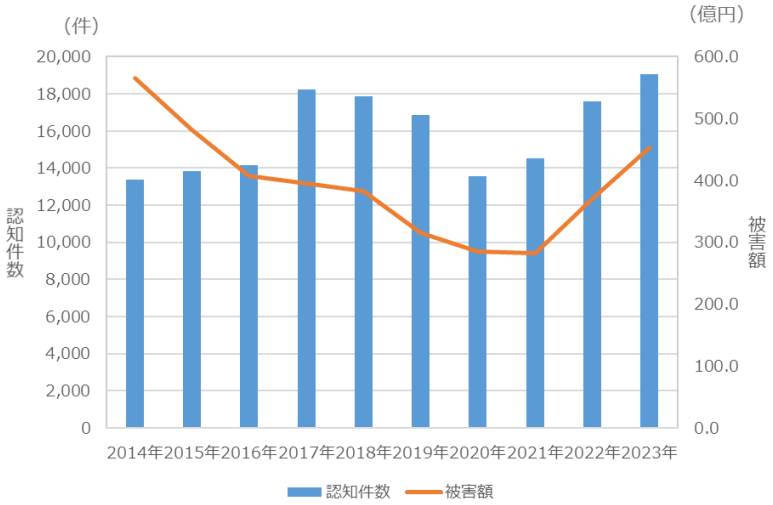


図 12　特殊詐欺の被害額の推移[26]

これに対し、総務省は、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（平成十七年法律第三十一号。以下「携帯電話不正利用防止法」という。）や犯罪による収益の移転防止に関する法律（平成十九年法律第二十二号。以下「犯罪収益移転防止法」という。）を通じて、電話の悪用への対策を実施している。

携帯電話不正利用防止法は、携帯電話を用いた特殊詐欺の発生を防ぐため、携帯電話の契約時、譲渡時及び貸与時における本人確認等を義務付けており、総務大臣は、本人確認義務を履行していない携帯電話事業者等に対して是正命令を行うことが可能となっている。また、警察署長は、携帯電話事業者から提供された携帯電話について犯罪利用の疑いがあると認めたとき、携帯電話事業者に対し契約者確認を求めることができ、その確認に利用者が応じない場合、携帯電話事業者は役務提供を拒否することができることとされている。

---

[25] 警察庁「令和５年における特殊詐欺の認知・検挙状況等について（確定値版）」から引用
[26] 警察庁「令和５年における特殊詐欺の認知・検挙状況等について（確定値版）」から作成

犯罪収益移転防止法は、金融機関をはじめとした特定事業者を規制する法律であり、この特定事業者の中に、電話受付代行事業者及び電話転送サービス事業者が含まれる。本法律では、マネーロンダリング対策として、携帯電話不正利用防止法と同様に取引時の本人確認等を義務付けているほか、疑わしい取引の届出義務等が定められている。

いずれの法律においても、主務省令（施行規則）において、具体的な本人確認方法等が定められており、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施行規則（平成十七年総務省令第百六十七号。以下「携帯電話不正利用防止法施行規則」という。）に定める本人確認方法の見直し・検討に当たっては、これまでも犯罪による収益の移転防止に関する法律施行規則（平成二十年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令第一号。以下「犯罪収益移転防止法施行規則」という。）に定める本人確認方法を参考にしながら、検討が行われてきた。

携帯電話不正利用防止法施行規則に定められた本人確認方法及び使用可能な本人確認書類の概要は図 13 のとおりであり、本人確認に当たっては、対面における契約に際し、本人確認書類の提示を受ける方法のほか、非対面における契約に際し、本人確認書類の写しの送付を受け、その本人確認書類に記載された住所に転送不要郵便物を送付する方法等、様々な本人確認方法が定められている。

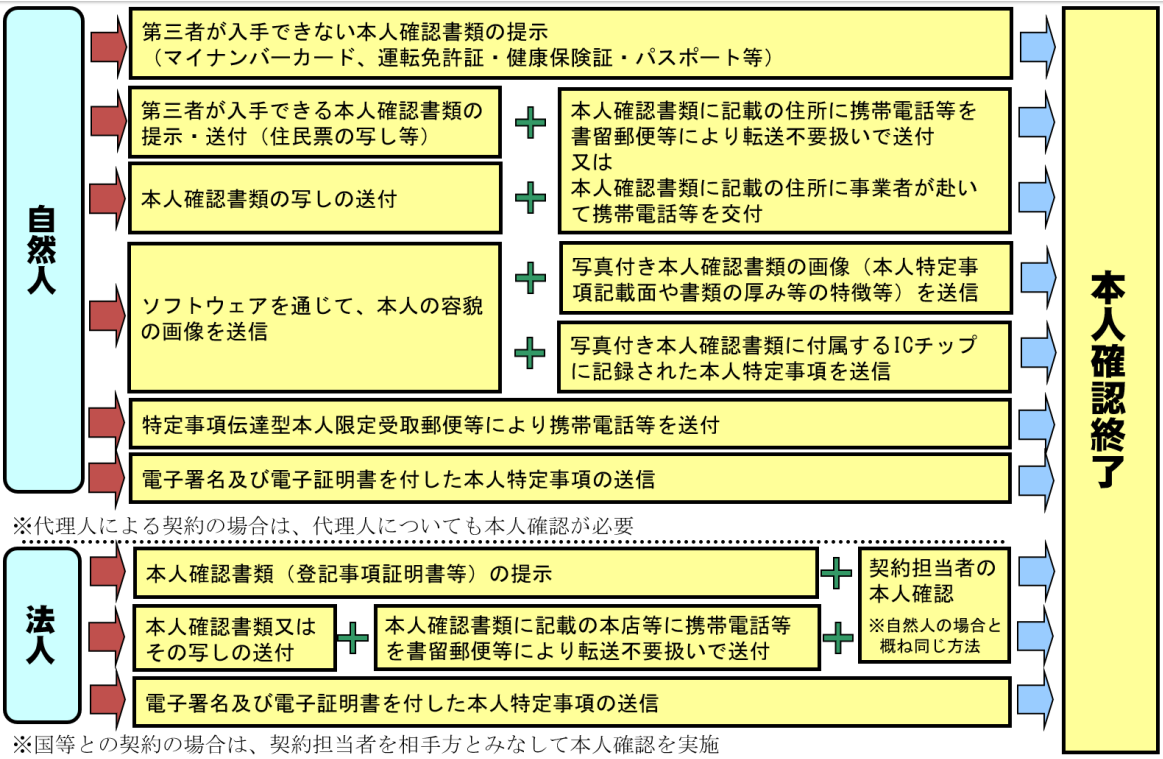


図 13　携帯電話新規契約時における本人確認方法の概要[27]

２　デジタル重点計画に基づく非対面における本人確認方法の見直し

近年、目視による真贋判定が困難なほど、券面が精巧に偽変造された本人確認書類を用いた携帯電話の不正契約が発生している。また、実在する人物になりすまして、携帯電話や SIM カードの紛失・故障等の理由を装い、携帯電話事業者等の店舗にて、本人確認書類として偽造した運転免許証やマイナンバーカード等を使い、SIM カードの再発行を受けることにより、実在する人物の携帯電話番号を詐取し、インターネットバンキング等の SMS 認証を回避し、不正送金等を行うという、「SIM スワップ」と呼ばれる手口も発生している。

このような状況を踏まえ、令和５年６月に閣議決定された「デジタル社会の実現に向けた重点計画」において[28]、「犯罪による収益の移転防止に関する法律、携

[27] 第３回資料 3-2「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について（事務局）」４ページ　抜粋

[28] 「デジタル社会の実現に向けた重点計画」（令和６年６月閣議決定）においても、「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

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。」と定められたところであり、本ワーキンググループにおいて、事務局から、犯罪収益移転防止法における検討状況や事業者への意見聴取結果を踏まえ、図 14 のとおり、携帯電話不正利用防止法施行規則の見直しの方向性（案）を示したところである。

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	検討中
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。

図 14　携帯電話不正利用防止法施行規則の見直しの方向性（案）[29]

３．新たな本人確認方法等の検討

前述の課題を踏まえ、本ワーキンググループの中で 11 つの本人確認方法等の提案があった。

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。対面でもマイナンバーカード等の IC チップ情報の読み取りを犯収法及び携帯電話不正利用防止法の本人確認において義務付ける。また、そのために必要な IC チップ読み取りアプリ等の開発を検討する。加えて、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。」と示されている。

[29] 第３回資料 3-2「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について（事務局）」７ページ　抜粋

(1)　自然人の本人確認方法

①非対面契約時における本人確認書類の券面を確認する方法の廃止

前述のとおり、本人確認書類の券面の精巧な偽変造が可能となっており、特に非対面契約における本人確認に当たっては、画像情報に頼った本人確認方法から、公的個人認証や本人確認書類に搭載された IC チップを読み取るなど、デジタル技術を活用した本人確認方法に移行することが必要であるとの意見があった。具体的には、「デジタル社会の実現に向けた重点計画」にも示されているとおり、本人確認書類の写しを送付する方法や、容貌及び写真付き本人確認書類の画像情報を送信する方法[30]を廃止することが望ましいとの意見があった。

②対面契約時におけるデジタル技術を活用した本人確認方法の導入

対面契約における本人確認に当たっては、基本的に目視により真贋判定が行われているが、前述のとおり、近年、精度の高い偽造身分証を用いた不正契約や SIM スワップ等の事案が発生している。対面契約の場合でも目視による真贋判定だけに頼るのではリスクが高くなっているのではないかと指摘されている状況を踏まえ、マイナンバーカードに搭載されている IC チップを活用した公的個人認証による確認方法や、運転免許証等の本人確認書類に搭載された IC チップの情報を読み取る方法など、デジタル技術を活用した本人確認方法を導入すべきではないかとの意見があった。

③例外的な確認方法としての非電子的な確認方法の存置

上記の見直しに伴い、デジタル技術を活用した本人確認方法が中心となることにより、利用者の利便性の低下を懸念する意見があった。これについて構成員からは、何らか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、デジタル技術の活用が難しい場合には、例外的な措置として非電子的な確認方法を存置することも考えられるのではないかという意見があった。

---

[30]当該写真付き本人確認書類に記載されている氏名、住居及び生年月日、当該写真付き本人確認書類に貼り付けられた写真並びに当該写真付き本人確認書類の厚みその他の特徴を確認することができるもの

④カード代替電磁的記録の活用

令和６年５月に行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）が改正され[31]、スマートフォンにマイナンバーカードの機能を搭載することが可能となった。これにより、物理的なマイナンバーカードを持ち運ぶことなく、スマートフォンに搭載された情報（カード代替電磁的記録）の活用によって本人確認を行うことが可能となるため、携帯電話契約時の本人確認にも適用されるよう、携帯電話不正利用防止法施行規則を整備するべきではないかと提案があった。

(2) 法人の本人確認方法

⑤登記情報提供サービスとの連携による本人確認方法の導入

犯罪収益移転防止法施行規則第６条第１項第３号ロにおいて、法人の代表者等から法人の名称及び本店または主たる事務所の所在地の申告を受けるとともに、（一社）民事法務協会が提供している登記情報提供サービスにより、登記情報の送信をうける方法[32]による本人確認が認められている。一方、携帯電話不正利用防止法施行規則においては、登記情報提供サービスとの連携による本人確認方法を規定していないことから、登記事項証明書の提示等が必要となってしまっているため、利用者の利便性の観点から、携帯電話不正利用防止法施行規則においても、登記情報提供サービスと連携した本人確認を可能とするべきではないかと提案があった。

⑥法人の契約担当者（代表者等）の本人確認方法

携帯電話不正利用防止法第３条第２項において、役務提供契約の相手方と役務提供契約の締結の任に当たっている自然人が異なるとき、その契約締結の任に当たっている自然人（代表者等）についても本人確認を行うことが義務づけられており、その方法が携帯電話不正利用防止法施行規則第４条等に定められている。代表者等の本人確認方法は、概ね自然人の本人確認方法と同様の規定となっているが、電子証明書を用いた方法が規定されていない。一方、犯罪収益移転防止法施行規則において定められている代表者等の本人確認方法については、犯罪収益移転防止法施行規則第 12 条により

[31] 情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るためのデジタル社会形成基本法等の一部を改正する法律（令和６年法律第 46 号）による改正

[32] 法人の代表者等（法人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）と対面しないで申告を受ける場合は、この方法に加え、法人の本店等に宛てて、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必要がある。

読み替えて適用する同規則第６条第１項第１号ヲ～カにおいて、電子証明書を用いた本人確認方法が認められている。これに関し、オンラインによる法人契約の推進等、利用者の利便性の向上にもつながることから、携帯電話不正利用防止法施行規則においても、電子証明書を用いた代表者等の本人確認を可能とするべきではないかと提案があった。

(3)　過去の確認結果への依拠

⑦金融機関等が過去に実施した本人確認結果への依拠

犯罪収益移転防止法施行規則第 13 条第１項において、犯罪収益移転防止法の適用を受ける一部の収納機関における金融取引について、当該金融取引に係る決済を銀行やクレジットカード会社が行う場合、当該銀行や当該クレジットカード会社が過去に実施した取引時確認に係る確認記録を保存していることを確認する方法（この方法を用いる収納機関と当該銀行や当該クレジットカード会社が、あらかじめ、この方法を用いることについて合意をしている場合に限る。）という、他事業者の本人確認結果に依拠する本人確認方法が認められている。一方、携帯電話不正利用防止法施行規則における本人確認方法には、他事業者の本人確認結果に依拠する本人確認方法が定められていない。他事業者の本人確認結果に依拠する方法が認められた場合、新たな契約を締結する際、同様の本人確認を再度実施する必要がなくなり、契約時における利用者の利便性が高まるため、携帯電話不正利用防止法施行規則についても犯罪収益移転防止法施行規則と同様に、銀行やクレジットカード会社、さらには、他の携帯電話事業者や他の金融機関における本人確認結果に依拠することを可能としてはどうかと提案があった。

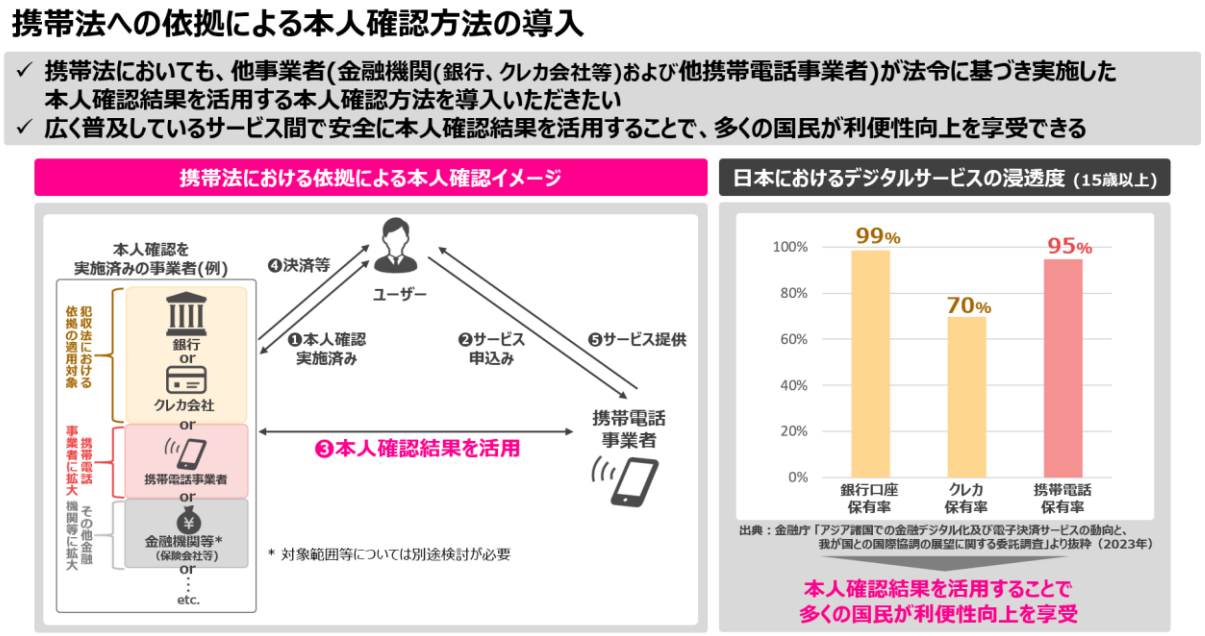


図 15　他事業者の本人確認結果を活用した本人確認方法[33]

⑧公的個人認証を用いて本人確認を実施した事業者への依拠

公的個人認証とは、マイナンバーカード等に搭載された IC チップ内の電子証明書を活用し、インターネット上で本人確認を行うものであり、申請等の際、第三者によるなりすましやデータの改ざんを防ぐことが可能となる。携帯電話不正利用防止法施行規則における公的個人認証を用いた本人確認に当たっては、マイナンバーカードの署名用電子証明書のほか、スマートフォンに搭載された署名用電子証明書[34]を用いることができる。

なお、民間事業者が、公的個人認証を利用する（マイナンバーカードの電子署名を検証（認証）する）ためには、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成十四年法律第百五十三号）第 17 条第 1 項に基づき、内閣総理大臣及び総務大臣の認定を受けるとともに届出を行うプラットフォーム事業者（以下「PF 事業者」という。）、もしくは、電子証明書の保管を含めた署名検証業務の全てを PF 事業者へ委託することで、みなし認定取得したサービスプロバイダー事業者（以下「SP 事業者」という。）になる必要があり、また、認証の流れは図 16 のとおりである。

[33] 第３回資料 3-4「「デジタル認証を活用した本人確認方法の普及等」に関するご提案（楽天モバイル(株)）」 6 ページ　抜粋

[34] 一定の基準を満たしたチップを搭載したスマートフォンに限定される。

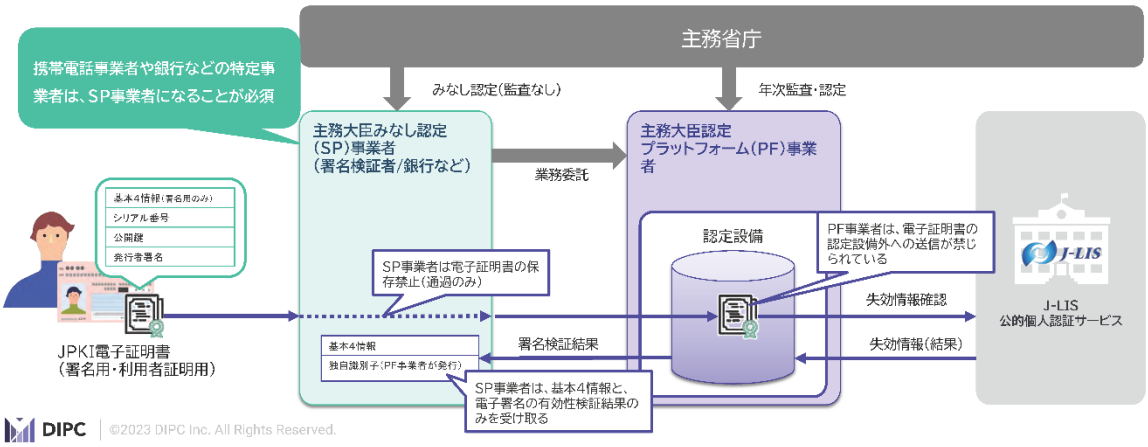


図 16　公的個人認証の流れ[35]

例えば、携帯電話事業者が SP 事業者となり公的個人認証を行う場合、契約者から携帯電話事業者を介し PF 事業者に署名用電子証明書を送付し、その電子証明書について、地方公共団体情報システム機構（J-LIS）に失効情報を確認し、その署名検証結果を PF 事業者から携帯電話事業者に回答することとなる。

現在、犯罪収益移転防止法施行規則では、一部の取引について、特定事業者から他の特定事業者への依拠による本人確認を認めている一方、携帯電話不正利用施行規則では依拠による本人確認は認められていない。今後、本人確認方法が原則公的個人認証に一本化されることを考えると、公的個人認証を用いて本人確認を行った事業者に依拠することにより、本人確認の厳格さを担保しつつ、事業者及びユーザーにとって利便性の高い本人確認が実現できないかと提案があった。

⑨継続的顧客管理の導入

犯罪収益移転防止法施行規則第 20 条第３項において、本人特定事項等に変更等があることを知った場合は、当該変更等に係る内容を確認記録に付記することが求められている。一方、携帯電話不正利用防止法施行規則においては、当該変更等に係る内容に係る確認記録における取扱いに関して規定していない。このため、特に契約途中で住所が変更となった場合に、２回線目の契約を行おうとした際に、携帯電話不正利用防止法施行規則第３条第３項及び第４項に定める方法が利用できないなどの事象が発生していることから、携帯電話不正利用防止法施行規則においても、本人特定事項の変

[35] 第４回資料 4-1「本人確認手法の JPKI 一本化を前提とした、不正対策と利便性の高い本人確認の実現（(一社）デジタルアイデンティティ推進コンソーシアム)」９ページ　抜粋

更等について確認記録に付記することを可能とするべきではないかと提案があった。

(4) その他の事項

⑩その他の見直し事項

携帯電話不正利用防止法においては、役務提供契約締結時のみならず、通話可能端末設備等の譲渡時や貸与時においても本人確認が義務付けられていることから、上記の議論を踏まえ、譲渡時や貸与時の確認方法についても、役務提供契約時と同様の見直しを図るべきとの意見があった。

また、プライバシーの保護や新たな不正利用のリスクへの対策という観点から、本人確認書類の写しや券面の画像情報なども確認記録に保存しないようにするといった、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を行うべきではないかといった意見があった。

また、警察署長は、犯罪利用の疑いがあると認めたとき、携帯電話事業者に対して契約者確認を求めることが可能であるが、上記の議論を踏まえ、契約者確認時の確認方法についても、役務提供契約時における本人確認方法と同様の見直しを図るべきとの意見があった。

さらに、前述のとおり、携帯電話不正利用防止法施行規則と犯罪収益移転防止法施行規則では、本人確認方法やそれに対する使用可能な書類等に差異があることから、事業者の利便性の確保等の観点から、それらの整合性の確保を進めるべきではないかといった意見があった。

⑪本人確認方法の見直し以外の事項

本人確認方法の見直しに伴い、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）の対応への考慮が必要である。もっとも、単に非電子的な本人確認方法を準備するだけではなく、デジタルディバイドへの対応としては、高齢者等がデジタル化した方法に対応できるよう、サポートを充実させることが必要ではないかとの意見や、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との意見があった。

第２章　携帯電話不正利用防止法に基づく本人確認方法等の見直しの方向性

第１章のとおり、ワーキンググループにおいて、犯罪収益移転防止法における検討状況の確認や事業者への意見聴取を実施し、こうした結果を踏まえて、携帯電話不正利用防止法施行規則に定める本人確認方法の見直しの方向性を検討したところ、以下の方向性が適当と考えられる。

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）

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）

３　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に記載のとおり、対面における本人確認についてもデジタル技術を活用する方法に移行することが必要だが、何らかのやむを得ない理由により IC チップ付本人確認書類を所持できない場合等においては、例外的に、代替手段として、非電子的な確認方法を認めることも考えられる。（第３条第１項第１号ロ等）

４　登記情報提供サービスとの連携による確認方法の導入

登記情報提供サービスとの連携による法人の本人確認について、犯罪収益移転防止法施行規則においても、法人の本人確認方法の一つとして認められていることに鑑み、携帯電話不正利用防止法施行規則においても法人の本人確認方法の一つとして認めることが適当である。（第３条第１項第２号）

５　法人の契約担当者の本人確認における電子証明書の導入

電子証明書を用いた、法人の契約担当者の本人確認について、犯罪収益移転防止法施行規則においても、代表者等の本人確認方法の一つとして認められていることに鑑み、携帯電話不正利用防止法施行規則においても代表者等の本人確認方

法の一つとして認めることが適当である。（第４条第１項）

６　過去の本人確認結果への依拠

本人確認のプロセスは、通常、身元確認と当人認証の２つのプロセスに分けられる。身元確認とは、手続の利用者の氏名等を確認するプロセスのことであり、当人認証は、ある行為の「実行主体」と、当該主体が主張する「身元識別情報」との同一性を検証することによって、「実行主体」が身元識別情報にあらかじめ関連付けられた人物（あるいは装置）であることの信用を確立するプロセスのことである。身元確認と当人認証の保証レベルは、下図のとおり分類がなされている。

身元確認保証レベル	レベルの定義
レベル１ （IAL1）	身元識別情報が確認される必要がなく、身元確認の信用度がほとんどない。身元識別情報は、自己表明若しくは自己表明相当である。
レベル２ （IAL2）	身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある。
レベル３ （IAL3）	身元識別情報が特定された担当者の対面で確認され、身元確認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

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]

[36] 「行政手続におけるオンラインによる本人確認手法に関するガイドライン」（平成 31 年２月 25 日各府省情報化統括責任者（CIO）連絡会議決定）９ページ及び 10 ページから引用

過去の本人確認結果に依拠するに当たっては、依拠先の本人確認結果に依存することとなるため、保証レベルの低い本人確認結果に依拠することは、現行の法令に則った本人確認と同等の手続きがとられたとは必ずしもみなせないものと考えられる。従って、本人確認における保証レベルが高く、一定の手続きのもと継続的に最新の本人特定事項を取得可能な本人確認を実施することが望ましい。こうした本人確認方法は、例えば、公的個人認証による方法が考えられ、過去の本人確認結果の依拠方法としては、公的個人認証を用いて本人確認を行った結果に依拠するとともに、依拠先において多要素認証等の当人認証を実施する方法が考えられる。なお、過去の本人確認結果に依拠する方法については、事業者のニーズや本人確認の保証レベルとのバランス等を鑑みつつ、今後、総合的に検討することが適当である。

７　継続的顧客管理による確認記録の更新

犯罪収益移転防止法施行規則の規定を鑑み、携帯電話不正利用防止法施行規則においても、本人特定事項の変更等について確認記録に付記することを可能とすることが適当である。

８　その他見直し事項

携帯音声通信役務の提供に係る契約締結時の本人確認方法の見直しについては上記のとおりだが、通話可能端末設備等の譲渡時や貸与時における本人確認の方法や契約者確認の方法についても、契約時の本人確認方法と同様の見直しを行うことが必要である。また、電子的な確認方法における確認記録への保存の在り方について、プライバシーの保護や新たな不正利用のリスク対策という観点から、券面の画像情報なども確認記録に保存しないようにするといった見直しを実施する必要がある。さらに、携帯電話不正利用防止法施行規則における本人確認と犯罪収益移転防止法施行規則における取引時確認は、その方法や使用可能な書類に差異があることから､事業分野における状況や各法令で求める法益を鑑みながら、検討を進めていくべきである。

なお、見直しに当たっては、デジタルディバイド等への対応や利用者への本人確認の目的やその重要性の説明等にも配慮する必要がある。

おわりに

本ワーキンググループでは、「国民を詐欺から守るための総合対策」（令和６年６月 18 日犯罪対策閣僚会議決定）等も踏まえながら、特殊詐欺及びフィッシングへの更なる対策として、SMS の不適正利用対策及び携帯電話不正利用防止法に基づく本人確認方法等の見直しについて議論してきた。

引き続き、特殊詐欺やフィッシング等の ICT サービスの不適正利用へ対処すべく、対応の方向性として前述した事項について、速やかに検討を行うことが適当である。

参考資料

「不適正利用対策に関するワーキンググループ」開催要綱

1　目的

本ワーキンググループ（以下「WG」という。）は、「ICT サービスの利用環境の整備に関する研究会」の下に開催される WG として、特殊詐欺等の 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することを目的とする。

2　名称

本 WG は、「不適正利用対策に関するワーキンググループ」と称する。

3　検討事項

（1）携帯電話や電話転送サービスの契約の本人確認のあり方
（2）SMS を利用したフィッシング詐欺への対応のあり方
（3）その他

4　構成及び運営

（1）本 WG の主査は、ICT サービスの利用環境の整備に関する研究会の座長が指名する。
（2）本 WG の構成員は、別紙のとおりとする。
（3）本 WG の構成員は、中立の立場をもって、専門的知見に基づき議論を行う。
（4）主査は本 WG を招集し、主宰する。
（5）主査は、必要があると認めるときは、主査代理を指名することができる。
（6）主査代理は、主査を補佐し、主査不在のときは主査に代わって本 WG を招集し、主宰する。
（7）本 WG の構成員は、やむを得ない事情により出席できない場合において、代理の者を指名し、出席させることができる。
（8）主査は、必要に応じ、オブザーバーを招聘することができる。
（9）主査は、必要に応じ、構成員以外の関係者の出席を求め、意見を聴くことができる。
(10) その他、本 WG の運営に必要な事項は、主査が定める。

5　議事・資料等の扱い

（1）本 WG は、原則として公開とする。ただし、主査が必要と認める場合については、非公開とする。
（2）本 WG で使用した資料は、原則として、総務省のウェブサイトに掲載し、公開する。ただし、公開することにより、当事者若しくは第三者の利益を害するおそれがある場合又は主査が必要と認める場合については、非公開とする。
（3）本 WG の議事概要は、原則として公開する。ただし、主査が必要と認める場合については、非公開とする。

6　その他

本 WG の事務局は、総務省総合通信基盤局電気通信事業部利用環境課が行う。

（別　紙）

「不適正利用対策に関するワーキンググループ」構成員

（敬称略・五十音順）

【構成員】

（主査）	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　代表理事
	仲上　竜太	日本スマートフォンセキュリティ協会　技術部会　部会長
	中原　太郎	東京大学大学院　法学政治学研究科　教授
	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

【オブザーバー】

警察庁　刑事局　捜査支援分析管理官

警察庁　サイバー警察局　サイバー企画課

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。** ※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 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 ※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。** ※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 ○SMSの不適正利用の実態について ・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 ・事業者ヒアリング：NTTドコモ、KDDI、ソフトバンク ・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 ○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 ○本人確認に関する関係者ヒアリング ・オブザーバーからの報告：警察庁（刑事局） ・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 ・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 ・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 ○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

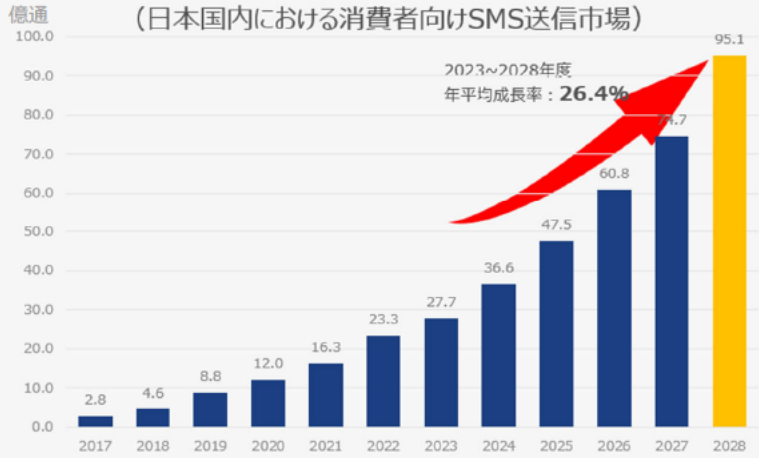
SMSの不適正利用対策について（第１回WG資料抜粋）

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

ADD VNTR

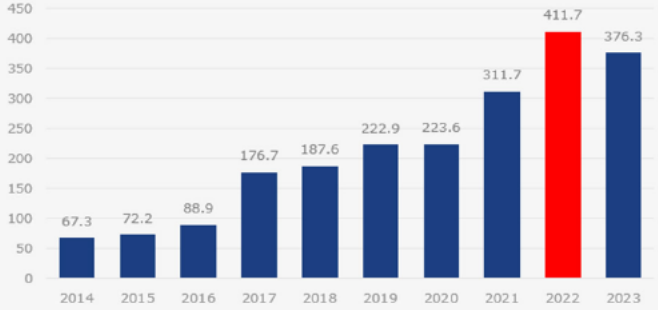
SMSの不適正利用対策について（第１回WG資料抜粋）

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。

番号盗用被害額（単位：億円）



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。

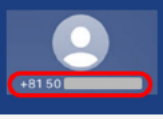
警察庁
フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について
（注意喚起）

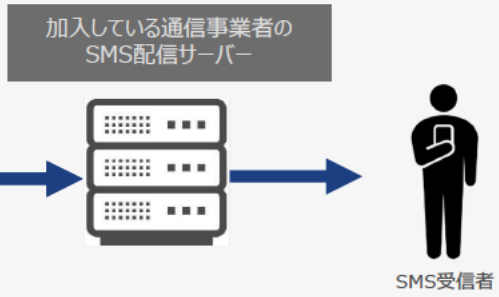
ADD VNTR

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。

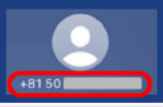
配信経路	送信元番号の表示 
①国内携帯電話端末	携帯電話番号 (090~ 080~ 070~など)
②国内SMS配信事業者	国内固定電話番号 キャリア共通番号 (03~ 0120~ 0005~など)
③海外通信事業者	海外電話番号 アルファベット ランダムな英数字など



一部誤植修正

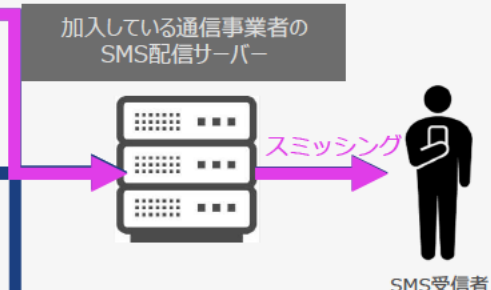
スミッシングの発信源はマルウェア感染端末

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 (090~ 080~ 070~など)
	②国内SMS配信事業者	国内固定電話番号 キャリア共通番号 (03~ 0120~ 0005~など)
1%	③海外通信事業者	海外電話番号 アルファベット 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

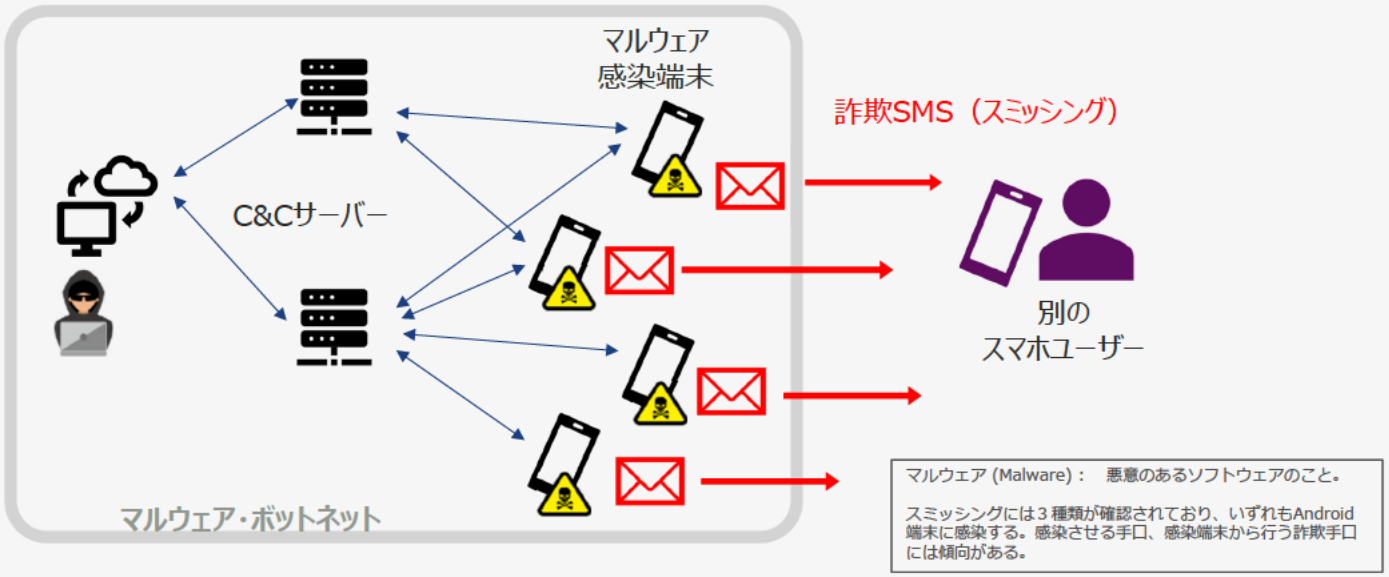
感染数の把握、端末の特定、無害化･･･などが急務である



※：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。

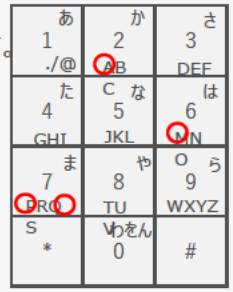


マルウェア (Malware)：　悪意のあるソフトウェアのこと。

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

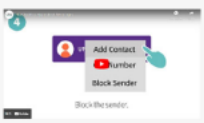
通信事業者横断のスミッシング申告として、Spam Reporting Service (7726) が広く使われています。



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 • 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 	• 利用者は、不正SMSを受信したら7726に転送する • 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 	• Email/SMSに共通の不正申告サイトを設置している • 利用者は、不正SMSを受信したら7726に転送する • iPhone/Androidの両方から利用可能 
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 2022/03開始 https://www.docomo.ne.jp/info/spam_mail/sms/	迷惑SMSブロック 2023/02開始 https://www.au.com/mobile/service/sms/filter/	迷惑SMS対策機能 2022/06開始 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 https://www.docomo.ne.jp/service/anshin_security/	迷惑メッセージ・電話ブロック https://media2.kddi.com/meiwakublock/safecall/PC/PC.html	セキュリティOne 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）

ADD VNTR

MACNICA

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

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

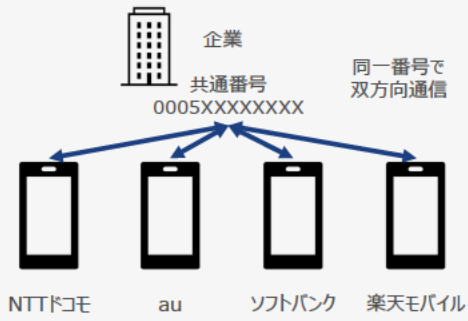
- 正式名称はRich Communication Service
- SMSより、多くの文字数を送付できる
- 公式マークを設定して、メッセージを発信できる
- テキスト以外に画像を送ったり、グループチャットが使える
- 日本では、NTTドコモ・au・ソフトバンクが＋メッセージ、楽天モバイルがRakuten Link の名称でサービスを提供している
- Appleは、RCS Universal Profile を2024年後半にサポートする予定を表明

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



ADD VNTR

MACNICA

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** ● 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 ● 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 ● 【MVNO】テレコムサービス協会（MVNO委員会） ● 【SMS配信事業者】 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 ● 【セキュリティ関係】 マクニカ ● 【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）

参考

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
- 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）

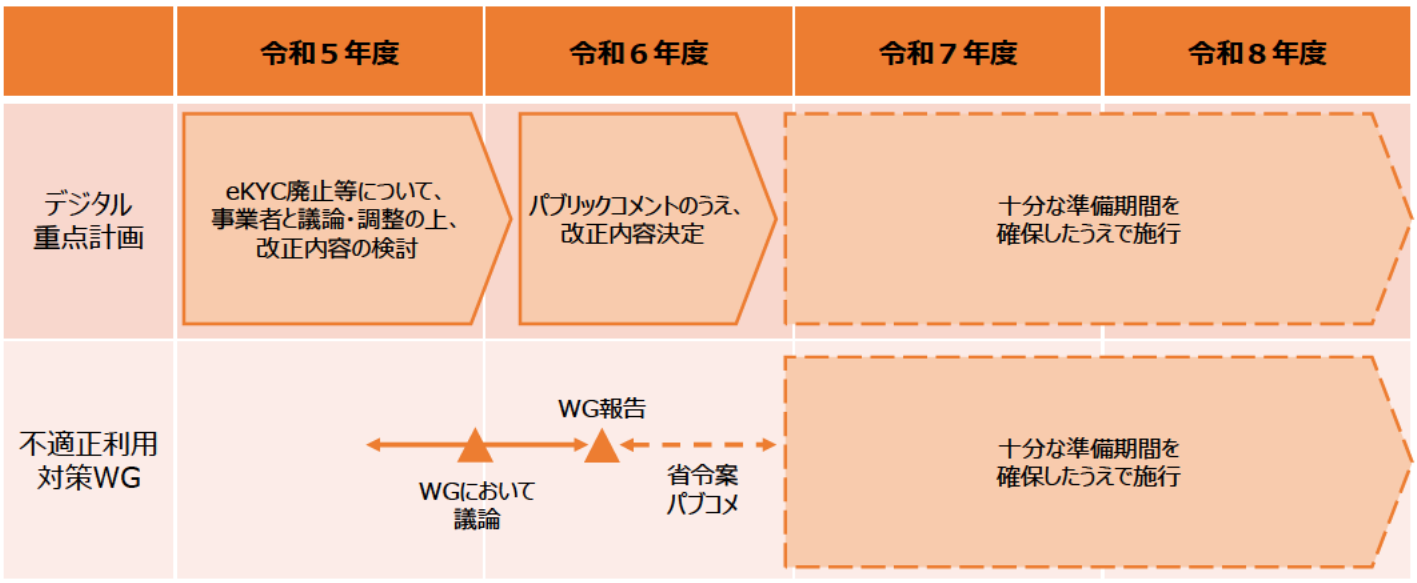
- 顧客等から顔写真のある本人確認書類を撮影した画像情報の送信を受ける本人確認方法については、精巧に偽変造された本人確認書類が悪用されている実態に鑑み、廃止する。
- 同様に、顧客等から本人確認書類の写しの送付を受ける本人確認方法についても、一般的に写しは偽変造が容易であり、その看破も困難であることから、廃止する。
- 顔写真のない本人確認書類を用いる非対面の本人確認方法については、原則廃止するが、偽造・改ざん対策が施された本人確認書類（住民票の写し等）の原本の送付を受ける本人確認方法については、引き続き、一定条件の下、本人確認に利用可能とする。
- 上記のほか、顔写真のない本人確認書類を用い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**。