2025 年 5 月 23 日

「マイナンバー制度の問題点と解決策」に関する提言(総集編)

【2025 年 5 月総集編】

一般社団法人　情報システム学会　マイナンバー制度研究会

【目次】

1．はじめに

情報システム学会では、今までに『マイナンバー制度の問題点と解決策』に関する提言を、５回に亘って以下のように行ってきた。

① 「『マイナンバー制度の問題点と解決策』に関する提言（初版）」
2023年10月公表

② 「『マイナンバー制度の問題点と解決策』に関する提言の補足1（身元証明（身元確認）制度編）』」
2024年7月公表

③ 「『マイナンバー制度の問題点と解決策』に関する提言の補足2(システム移行編)」
2024年11月公表

④ 「『マイナンバー制度の問題点と解決策』に関する提言の補足2(システム移行編)」付録1【本人確認定義の見直し案】
2025年1月公表

⑤ 「『マイナンバー制度の問題点と解決策』に関する提言の補足2(システム移行編)」付録2【データソース・システム連携方式の整理・整備の提案】
2025年3月公表

2015年10月から開始されたマイナンバー制度は今年で10年目を迎えるが、過去の提言書で指摘したように設計に根本的な問題があり、そのため多くの問題が発生している。一言でいうと、マイナンバー制度の全体設計が不十分であるために、問題発覚の度にシステム修正や問題対策を実施しても、対策が局所的になってしまったり、その問題対策が別の新たな問題を引き起こしてしまったりすることを繰り返してしまっている。この問題を解決するためには、局所的・場当たり的な問題対策ではなく、今のマイナンバー制度を一度リセットする、つまり根本的な全体設計から見直して軌道修正することが必要である。マイナンバー制度は、今後の日本社会のデジタル化のデータ基盤となる制度であるため、非常に重要なシステムである。この基盤となるシステムの信頼性（データの「正確性」と「最新性」）が低く、国民の制度に対する理解が難しく使い辛い状態では、永遠に日本社会の真のデジタル化を実現することは不可能である。

そこで本稿では、過去の５つの提言内容の「総集編」という位置づけで、マイナンバー制度の全体設計を見直す際に、特に重要となる以下の４つのポイントについて整理を行った。

1） 国民の「理解度」向上のために必要なポイント：1枚のカードを多機能にし過ぎたため、国民がカードの使用方法を理解できない。加えて、多機能にし過ぎたことが原因となりカード運用上の問題やセキュリティ上の問題が生じている。これらの問題に対応するためには、カードに関する設計の根本的な見直しが必要である。

2） 本人確認の「厳密度」向上のために必要なポイント：本人確認の用語の定義が曖昧であることに伴い本人確認の保証レベルの「厳密度」も曖昧になっている。そのため、曖昧な本人確認が実施され銀行口座開設や携帯電話契約のなりすましができてしまうなど様々なセキュリティ上の問題が生じている。これらの問題に対応するためには、本人確認の用語の

定義と保証レベルの「厳密度」の定義の見直しが必要である。加えて、これらに関連する法令についても見直す必要がある。

３）　データの「正確性」確保のために必要なポイント：データの「名寄せ」作業が「名寄せ」方法が曖昧なまま実施されているため、システム間で紐付けられ、情報提供ネットワークで連携されたデータの「正確性」が確保できていない。これらの問題に対応するためには、「名寄せ」方法を見直し、「名寄せ」作業をやり直す必要がある。

４）　データの「正確性」、「最新性」確保のために必要なポイント：「データの紐付け」と「データの連携」のためのベースとなる番号として３つの番号（マイナンバー、符号、シリアル番号）を使用し、複雑なシステム設計をしていることによって、データの「正確性」と「最新性」の確保ができていない。加えて、データソースの内容に対する適切な見直しができていないため、データの「最新性」も確保できていない。マイナンバー制度のシステムは、将来の日本社会のデジタル化や医療ＤＸ、行政ＤＸを推進するためのデータ基盤となるシステムである。そのシステムのデータの「正確性」、「最新性」が確保されていないことは、将来のデジタル化推進の足かせとなってしまう。これらの問題に対応するためには、ベースとなる番号を１つに決定し、シンプルでセキュアなデータソース・システム連携方式を再構築することが必要である。

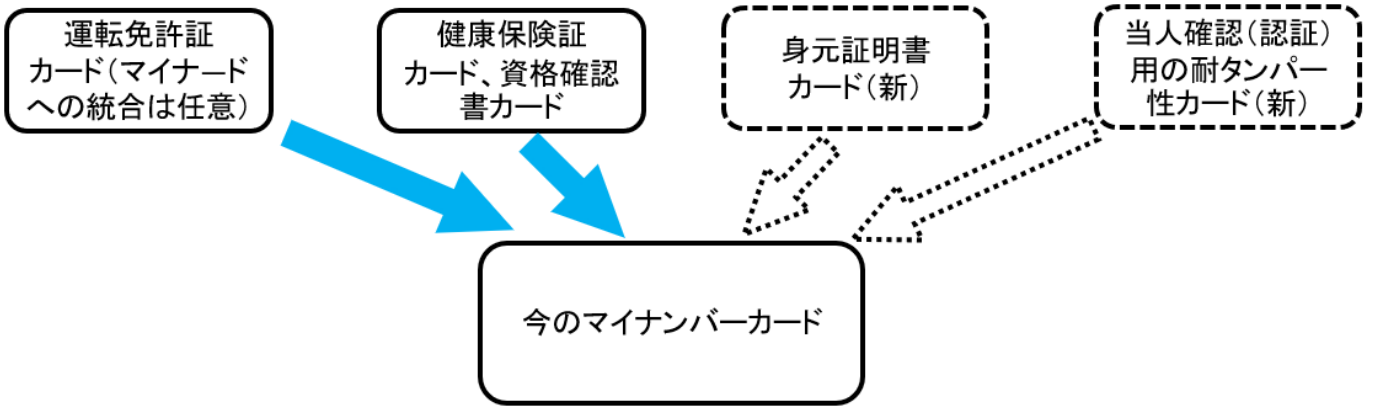
なお、本稿はあくまでも過去の提言書をまとめたものである。４つのポイントの概要について、あらためて次章以降に記述したが、より詳細な内容や４つのポイント以外の問題点と解決策については過去の５つの提言書を参照していただきたい。

2. カードに関する設計の見直し：国民の「理解度」向上のための提言

2.1. 1枚のカードに機能を搭載し過ぎた現在のマイナンバーカード（「初版」、「補足1」）

「初版」、「補足1」で述べたように、1枚のカード（マイナンバーカード）に3つの「本人確認機能」と「保険証機能」、「運転免許証機能」を搭載することにより、カードの運用設計が混乱し様々な問題を発生させている。加えて、国民がカードの使用方法を正しく理解できないことにもつながっている。実際に、2024年12月2日に「紙の保険証は本人確認ができずなりすまし使用などのセキュリティ上の問題があるため、廃止する」ことになったが、マイナンバーカードと保険証の統合には別の問題が発生することが明白になり、保険証から名前を変えただけの紙の資格確認書（実質的には紙の保険証と同じ物）を限定的ではあるが残すことになり、マイナ保険証と紙の資格確認書を並行運用する状態になっている。さらに、2025年4月3日の厚生労働省の審議会では、既にマイナ保険証を取得している人を含めた75歳以上の全員に紙の資格確認書を再配布することが決定された。マイナンバーカードと保険証の統合の目的は、本人確認の厳密化でありそのための紙の保険証の廃止であったはずだ。この迷走ぶりは目に余る。そして、2025年3月24日からマイナンバーカードに「運転免許証機能」を搭載することが可能になったが、カードの再発行や更新の運用方法に不安を感じた過半数の国民は、運転免許証を返納することなく従来の運転免許証とマイナ免許証の2枚を持つ状態となっている。過去の提言書で指摘したように、マイナンバー制度のカード設計に問題があるため、1枚のマイナンバーカードに「保険証機能」、「運転免許証機能」を搭載することは技術的には可能になったものの、従来のカードを無くすことはできず、中途半端なカード統合がされている状態である。今の制度設計のままでは、現在の運転免許証と資格確認書は永久に廃止することはできず、中途半端なカード統合状態は未来永劫継続することになるであろう。中途半端なカードの統合は、国民のカードの取り扱い方法を複雑にするだけでなく、カードに関する事務処理負担を増やしてしまうことにつながる。さらに、新旧のカードを運用するため、システムは両方を維持管理する必要が生じ、行政コストは増大することになる。旧カードを残す必要がある中途半端なカード統合の制度設計は百害あって一利なしである。

さらに、マイナンバーカードを常時携行する運用は、セキュリティ上の問題が発生するだけでなく、そのカードは犯罪者の一番のターゲットにもなる。「卵を一つの籠に盛るな」の諺通り、セキュリティ確保のためには目的別にカードを分けてリスク分散することが肝要である。住基ネットの最高裁判決に沿ってデータを分散管理したにもかかわらず、一人の個人情報へのアクセスやサービス利用が「1枚のカード＋暗証番号」のみに集約されてしまうことは、カードが1枚であるという一見の便利さと引き換えに多くのセキュリティ上の問題を引き起こしてしまうことにつながるからである。図1に現在のマイナンバーカードに搭載されている機能の概要を示す。



- 身元証明書として使用できる
- 当人確認（認証）用の所有物認証カードとして使用できる（電子行政などへのアクセス手段）
  （例）マイナポータルへのアクセス、住民票のコンビニ発行、健康保険のオンライン資格確認、等々で使用
- 健康保険証として使用できる（健康保険証は2024年12月に廃止し、資格確認書に名前を変更して存続）
- 運転免許証として使用できる（マイナンバーカードの併用も可能）
- 記載されているマイナンバーと基本4情報を使用して、マイナンバーの真正性確認として使用できる

図１　今のマイナンバー制度は、１枚のマイナンバーカードに多様な機能を搭載し過ぎた状態

2.2. 目的別に異なるカードやスマートフォンを使用することを提案（「初版」「補足１」「補足２」「付録１」）

国民に交付するカードは、そのカード導入の目的とカードの持つ役割を国民に対してしっかり説明し、理解してもらう必要がある。多機能過ぎるカードを国民に半ば強引に押し付けるのは、国民の反発を招くだけでなく、セキュリティ上の問題を誘発することにもつながるため、「補足１」ではカードは目的別に分割して交付することを提案している。そのために、現在の健康保険証（2024年12月2日から「資格確認書」に名前を変更）をICカード化し、既存の運転免許証（現在でもICカード化されている）を若干の変更を加えて活用し、加えて新たに「新身元証明書カード（図２参照）」を導入し15歳以上の国民全員に交付することを提案している（表１参照）。

＜身元証明書カード（３種類）の提案＞

- **「新身元証明書カード」：メインの身元証明書として、１５歳以上の全国民に交付する。**
- **「顔写真付き新保険証」：保険証として使用する、サブの身元証明書としても使用する。**
- **「新運転免許証」：運転免許証として使用する、サブの身元証明書としても使用する。**

- 「身元証明書カード」の券面管理番号
- 名寄せ用番号（特定個人情報ではなくしたマイナンバー）
- 基礎年金番号
- 氏名（フリガナ有り）
- 住所
- 生年月日
- 性別（※身元証明書から削除することは検討に値する）
- 顔写真
- カードの有効期限
- その他（臓器提供意思表示など、今後の検討項目）

図２　新身元証明書カードの券面記載内容（提案）

表１　新たな身元証明書の種類と特徴（提案）

項目	身元証明書		
	メイン	サブ	
券面名称	新身元証明書	新運転免許証	顔写真付き新保険証
券面の記載内容	券面管理番号、名寄せ用番号（特定個人情報でなくしたマイナンバー）、基礎年金番号、氏名（フリガナ有り）、住所、生年月日、顔社員、カード有効期限、その他	現在の運転免許証の記載内容に以下の項目を追加 ・名寄せ用番号（特定個人情報でなくしたマイナンバー） ※運転免許証番号が券面管理番号を兼ねる	現在の保険証の記載内容に以下の項目を追加 ・券面管理番号 ・顔写真 ・名寄せ用番号（特定個人情報でなくしたマイナンバー）
券面の所持方法	自宅で大切に保管して、必要な際に取り出して使用	常時携行	常時携行
使用できる 身元確認業務	・要求保証レベルの高い業務は、官民を問わず全て対象とする。 ・サブの身元証明書再発行業務を含めて、対象とする全ての身元確認業務について、法制度で身元確認方法を定め、定めた業務以外での使用は禁止とする。 （例）携帯電話契約業務、金融機関口座開設業務、本人限定郵便引渡し業務、確定申告業務など	【専用機器で偽造されていないことと券面管理番号を確認】 ・運転免許資格確認 ・職務質問 ・メイン、サブの身元証明書の再発行 【専用機器で偽造されていないことと券面管理番号の確認はなし】 ・要求保証レベルの低い業務 （例）図書館貸出カード発行、スポーツ施設会員証発行、ポイントカード発行など	【専用機器で偽造されていないことと券面管理番号を確認】 ・健康保険資格確認 ・職務質問 ・メイン、サブの身元証明書の再発行 【専用機器で偽造されていないことと券面管理番号の確認はなし】 ・要求保証レベルの低い業務 （例）図書館貸出カード発行、スポーツ施設会員証発行、ポイントカード発行など
券面のICカード化	カード偽造防止と券面管理番号格納目的でICチップを使用する。 ICチップ内に身元情報は格納は必要最小限にする。暗証番号は6桁数字とする。	カード偽造防止と券面管理番号格納目的でICチップを使用する。 ICチップ内に身元情報は格納は必要最小限にする。暗証番号は4桁数字とする。	同左
ICチップを使用した偽造と券面管理番号チェック専用機器利用	全業務で必須	要求保証レベルの低い業務を除いて、必須	同左
券面の偽造防止対策	最大限の対策を行う	同左	同左

さらに、「補足２」では公務員等に対して国民の個人情報へのアクセス管理をするために、担当者全員（医療機関窓口事務員、医師、役所職員など）に対して、公的個人認証用のカードとして TAAL3 保証レベルの「利用者証明用 IC カード」を交付して使用を義務づけることを提案している。つまり、国民が政府を監視する仕組み作りの提案である。そして、国民に対しては、国民自身が自分の個人情報にアクセスするための TAAL2 保証レベルの公的個人認証機能を、任意選択でスマートフォンに実装可能とすることを提案している（図３参照）。将来的には、「利用者証明用 IC カード（公的個人認証用のカード）」を任意選択で国民が取得する仕組み

の構築も検討に値する。

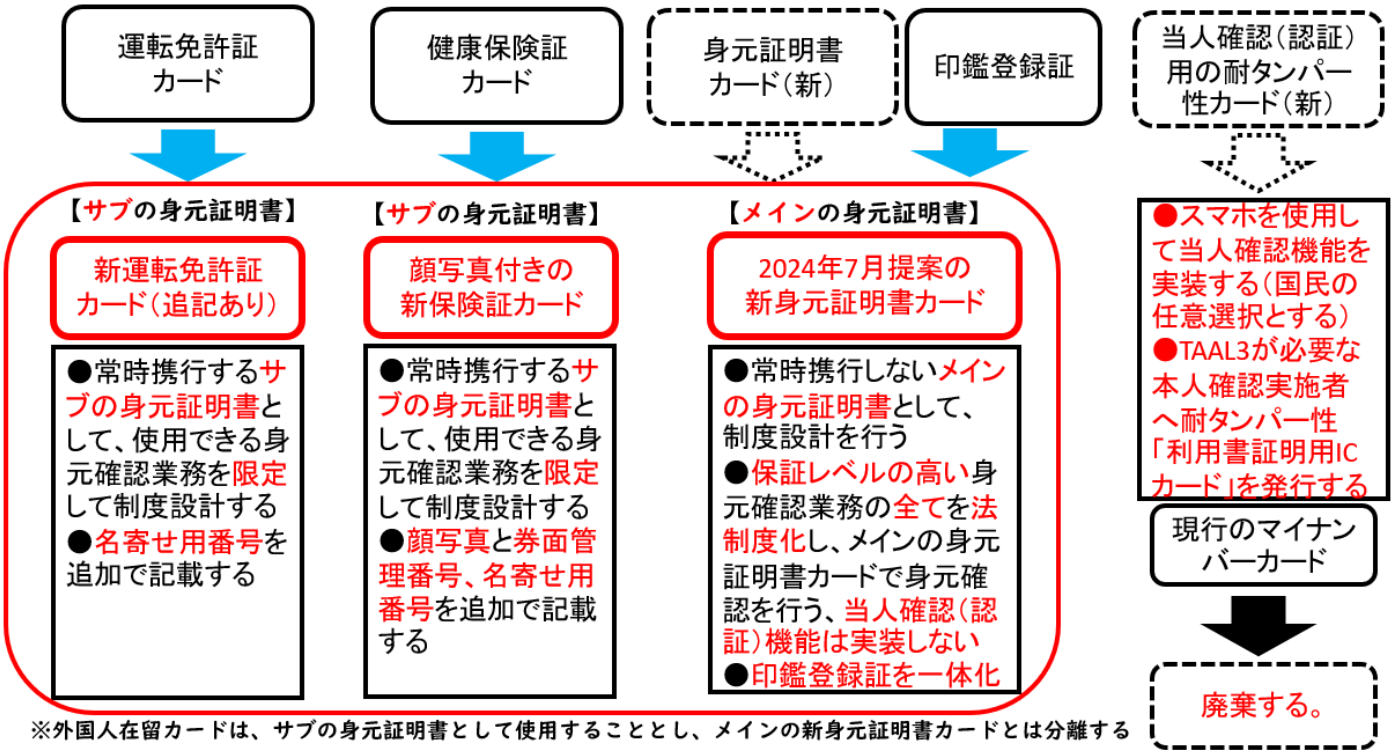


図３　使用目的ごとに国民が理解できるようにカードの運用設計を行ったうえで、３種類の「身元証明書カード（メイン、サブ）」と「利用者証明用 IC カード」を交付（提案）

なお、提言書で提案してきたカード機能と、今のマイナンバーカード機能の比較を表２にまとめたので参照していただきたい。１枚のカードに多くの機能を搭載し過ぎたことから発生している問題点と解決策については過去の提言書を参照していただきたいが、今のマイナンバーカードに対していかに多くの機能が搭載されているかが理解できる。加えて、カードを統合することによる問題点が数多く発覚したため、保険証の名前を変えた紙の資格確認書は残ることになり、運転免許証の保有に関しても多くの国民は２枚持ちをしており、マイナンバーカードへの統合は中途半端な状態になっているのが今の制度設計である。前述したように、今の制度設計を根本から見直さない限り、カード統合は未来永劫に中途半端な状態が継続することになるであろう。

表２　提言のカード機能と、今のマイナンバーカード機能の比較

機能＼カード種類	身元証明書カード			当人確認（認証）用カード		マイナンバーカード（運転免許証、資格確認書、スマホと併用）
	メイン	サブ		利用者証明用ICカード（TAAL3）	利用者証明用電子証明書格納スマホ（TAAL2）	
	新身元証明書	新運転免許証	顔写真付き新保険証			
電子証明書	署名用電子証明書（メイン用）	署名用電子証明書（新運転免許証用）	署名用電子証明書（新保険証用）	利用者証明用電子証明書	同左	・署名用電子証明書（運転免許証用は別） ・利用者証明用電子証明書
交付対象	全員（15歳以上）	希望者	希望者	・希望者 ・国民の個人情報にアクセスする公務員、医師等は全員	希望者	希望者
カード有無	ICカード	ICカード	ICカード	ICカード	（カード無し）スマートフォン	・ICカード ・スマートフォン
常時携行	×	○	○	×	○	○
本人を特定する番号	名寄せ用番号	同左	同左	同左	同左	・マイナンバー ・シリアル番号 ・符号
暗証番号	６桁数字	４桁数字	同左	４桁数字	同左	・６桁英数字 ・４桁数字
身元証明書	○	△（使用業務は再発行等に極めて限定）	同左	×	×	○
身元証明書カードの偽造チェック機器の導入	○	○	○	×	×	×
健康保険証	×	×	○	×	×	○（資格確認書と併用）
運転免許証	×	○	×	×	×	○（運転免許証と併用）
当人確認（認証） ・マイナポータルアクセス、保険資格確認等	×	×	×	○	○	○
印鑑登録証	○	×	×	×	×	○
高齢者施設での健康保険証	×	×	○	×	×	資格確認書（マイナンバーカードと併用）
カードの保有イメージ	新身元証明書ICカード	新運転免許証ICカード	顔写真付新保険証ICカード	利用者証明用ICカード		マイナンバーカードICカード  資格確認書（紙） 運転免許証ICカード

3．本人確認に関する設計の見直し：本人確認の「厳密度」向上のための提言

3.1.「本人確認」の用語の定義の見直しの提案（「初版」「補足２」「付録１」）

現在のマイナンバー制度では「本人確認」の用語が図４に示すように曖昧に、多様な意味で使用されている。そのことによって多くの問題が発生している、具体的な問題点については「付録１」を参照していただきたい。

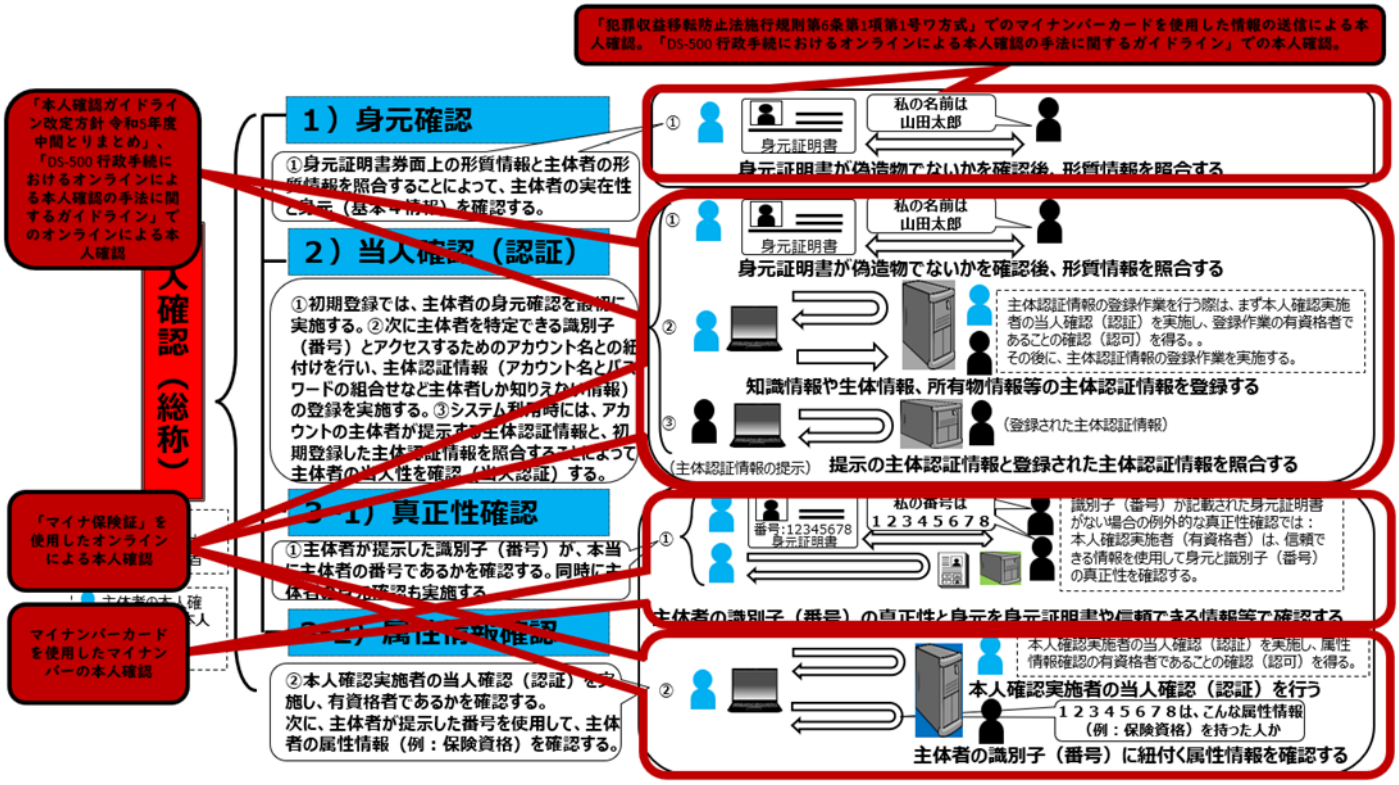


図４　今のマイナンバー制度における「本人確認」用語の曖昧な使用状態

この問題の解決策として、まず「本人確認ガイドライン改定方針 令和５年度中間とりまとめ」と「DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン」を改定し、さらに「番号法」、「犯罪収益移転防止法施行規則第６条第１項第１号」、「携帯電話不正利用防止法」、「公的個人認証法」などの法令を改定し、関連する eKYC などの設計を見直すことを提案している。具体的な「本人確認」の用語の定義の見直し案は、「付録２」を参照していただきたい。「本人確認」の用語の定義の見直し案の概要を以下に記す（図５参照）。

＜「本人確認」の用語の定義の見直し案の概要＞

・＜本人確認＞：本人確認とは、なんらかの手続きを行いたい主体者の本人性を確認するプロセスの総称であり、『身元確認』『当人確認（認証）』『真正性確認と属性情報確認』の３つの確認プロセスから構成される。

・＜身元確認＞：身元証明書券面上の形質情報と主体者の形質情報を照合することによって、主体者の実在性と身元（基本４情報）を確認する。

・＜当人確認（認証）＞：まず、本人確認実施者が、オンラインサイトを利用したい主体者の身元確認を行う。次に、主体認証情報の登録資格を有する本人確認実施者が、主体認証情報の

登録を行う。そして、主体者がオンラインサイトを実際に利用する際には、主体者が提示する主体認証情報と事前に登録された主体認証情報を照合することによって、本人確認実施者が主体者の当人性を確認（当人認証）することである。

・＜真正性確認と属性情報確認＞：まず、本人確認実施者は、なんらかの手続きを行いたい主体者が提示する身元証明書券面（この提示により、主体者の身元確認も同時に実施する）に記載された識別子（番号）が主体者に対して付番された正しい番号であることを確認（真正性確認）する。

そして、本人確認実施者が、真正性確認された識別子（番号）を検索キーとして、情報システムを使用して主体者の属性情報（保険資格、住所、氏名、性別、生年月日など）の確認をすることである。

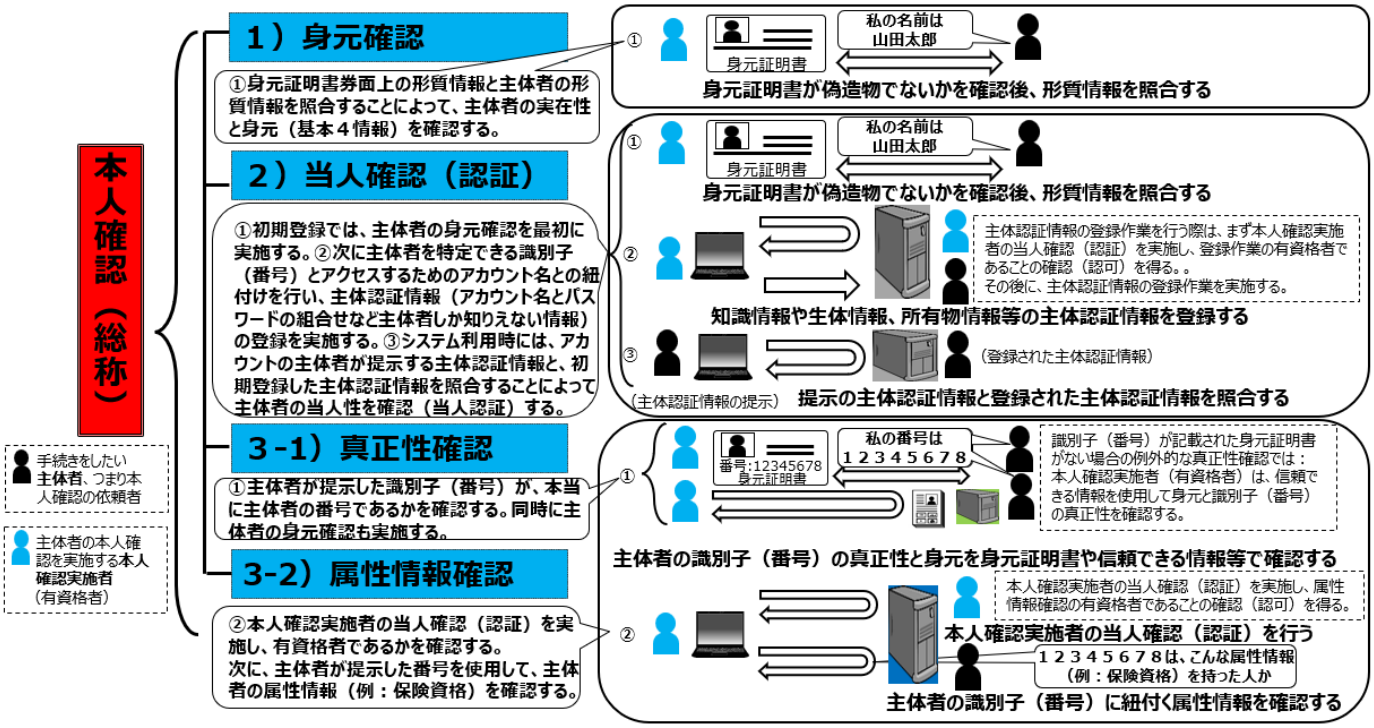


図５　「本人確認」用語の定義の見直し案（提案）

3.2.「本人確認」の保証レベルの厳密度の設計見直しの提案（「初版」「補足１」「補足２」「付録１」）

今のマイナンバー制度に関連する本人確認業務や法令では、前節に示したように「本人確認」の用語を曖昧に多様な意味で定義し使用している。しかし、「本人確認」の保証レベルの厳密度は、「DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン」において、表３に示すように「身元確認」と「当人認証」の掛け合わせのみで定義している。つまり、「本人確認」の用語は曖昧に拡大解釈して幅広く定義し使用しているにもかかわらず、「本人確認」の保証レベルの厳密度は「身元確認」x「当人認証」のみで大丈夫と定義している。言い換えると、保証レベルの高い厳密な本人確認業務は、「マイナンバーカードさえ使用していれば、何となく全て大丈夫である」、という曖昧で粗い設計になってしまっている。そのため、「付録１」6.2.事例検証で指摘したように、今の曖昧で粗い制度設計を実際の本人確認業

務に当てはめて検証してみると、多くの問題点と矛盾点が発生していることが分かる。

そこで、「付録Ⅰ」では、「米国立標準技術研究所（NIST）の Digital Identity Guidelines 第３版（NIST SP 800-63-3)」を曖昧に「本人確認」と解釈するのではなく、実際の本人確認業務に即した用語の定義と保証レベルの厳密度を再定義し、関連する法令も見直すことを提言している。まとめると、今のマイナンバー制度では、関連する様々な法令や実際の本人確認業務において「本人確認」の用語を多様な意味で使用しているにもかかわらず、「DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン」での本人確認の用語の定義は曖昧であり、一方で保証レベルの厳密度は「身元確認」x「当人認証」に依存するという矛盾した設計になってしまっている状態にあるということだ。参考に、今のマイナンバー制度の「本人確認」用語の定義と保証レベルの厳密度が定義されいる「DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン」における『別紙２ オンラインにおける本人確認の手法例の対応表（個人に係る行政手続)』を表３に転載しておく。

表３ 『DS-500 の別紙２ オンラインにおける本人確認の手法例の対応表（個人に係る行政手続)』を転載

①必要な保証レベル		②オンラインによる手法例		③実現できること・特徴
身元確認保証レベル	当人認証保証レベル			
レベル３ 対面での身元確認	レベル３ 耐タンパ性が確保されたハードウェアトークン	レベル A	・マイナンバーカード（公的個人認証：署名用電子証明書）による身元確認でアカウントを作成し、アカウント作成後はマイナンバーカード（公的個人認証：利用者証明用電子証明書）の耐タンパ性ハードウェアトークンによる当人認証を実施。 ・申請データに対するマイナンバーカード(公的個人認証：署名用電子証明書)による電子署名を付与。 ※耐タンパ性ハードウェアトークンの例： －PIN+IC カード（マイナンバーカード）	・行政手続の対象者や行政手続を実施している者について、個人の基本４情報を毎回確認している。 ・マイナンバーカード(公的個人認証：署名用電子証明書)の機能により付与された電子署名を検証することにより、非常に高い信用度で「身元確認」を行っている。また、耐タンパ性を有したハードウェアトークンにより非常に高い信用度で「当人認証」を行っている。
レベル２ 遠隔又は対面での身元確認	レベル２ 複数の認証要素	レベル B	・マイナンバーカード（公的個人認証：署名用電子証明書）等による身元確認でアカウントを作成し、アカウント作成後はマイナンバーカード（公的個人認証：利用者証明用電子証明書）若しくはこれによることができない場合、その他の多要素認証による当人認証を実施。 ・マイナンバーカードによるオンラインでの身元確認が行えない場合、対面での身分証明書等の確認や郵送した申込書（捺印付）、印鑑証明書、公的証明書（住民票等）等の確認によりアカウントを作成。 ・法人共通認証基盤における多要素認証の機能を利用する場合等、事業を行う個人についての押印及び印鑑証明書等の郵送による身元確認で、アカウントを作成し、アカウント作成後は多要素認証による当人認証の実施。 ※多要素認証の例： －ID・パスワード＋二経路認証アプリ －ID・パスワード＋ワンタイムパスワード生成アプリ －ID・パスワード＋生体認証	・行政手続の対象者や行政手続を実施している者について、登録時に個人の基本４情報を確認し、認証プロセス時には、同一の個人であることを確認している。 ・登録時に相当程度の信用度のある「身元確認」を行い、マイナンバーカード(公的個人認証：利用者証明用証明書）等の多要素認証の機能を用いることで、相当程度の信用度で「当人認証」を行っている。 ・特に法人共通認証基盤においては、登録時に事業を行う個人を相当程度の信用度で「身元確認」を行い、多要素認証の機能を用いることで相当程度の信用度で「当人認証」を行っている。
レベル１ 身元確認のない自己表明	レベル１ 単一又は複数の認証要素	レベル C	・身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単要素認証で当人認証を実施。 ・法人共通認証基盤における単要素認証の機能を利用する場合等、身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単要素認証で当人認証を実施。 ※単要素認証の例： －ID・パスワードのみ －認証デバイスのみ －生体認証のみ	・行政手続の対象者や行政手続を実施している者について、個人を正確に確認する必要がない場合で、単に毎回のアクセスが、同一の者により行われていることを確認しており、「当人認証」における信用度はある程度ある。
該当しない	該当しない	レベル D	・身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後もアカウントを入力するだけ（当人認証を行わない。)。	本人に関する情報は不要

「付録Ⅰ」で指摘した「本人確認」に関わる問題点を解決するために、前節で述べた「本人確認」用語の定義の見直しに加えて、その定義ごとに本人確認の保証レベルの厳密度を明確に定義することを提案している（表４参照)。表３と表４を比較しながら、「付録Ⅰ」を読んでいただければ、現在のマイナンバー制度の問題点が明確になるので参考にしていただきたい。

表４　３つの本人確認プロセスの厳密度（保証レベル）の定義（提案）

略称	正式名	内容
IAL	Identity Assurance Level	「身元確認」の保証レベル （注）「NIST SP 800-63-3」で使用されている「Identity Proofing（身元確認）」の内容とほぼ同義
EAL	Enrollment Assurance Level	「当人確認（認証）」の中での主体認証情報の「登録」の保証レベル （注）「付録Ｉ」独自の提案
AAL	Authentication Assurance Level	「当人確認（認証）」の中での「当人性の確認」の保証レベル （注）「NIST SP 800-63-3」で使用されている「Authentication（当人認証）」の内容とほぼ同義
TAAL	Total Authentication Assurance Level	「当人確認（認証）」全体の保証レベル。IAL、EAL、AAL の掛け合わせで保証レベルが決まる。 （注）「付録Ｉ」独自の提案
IAAL	Identifier Authenticity Assurance Level	「真正性確認」の保証レベル。 （注）「付録Ｉ」独自の提案
AIAL	Attribute Information Assurance Level	「属性情報確認」の保証レベル。 （注）「付録Ｉ」独自の提案
IAAAL	Identifier Authenticity Attribute Assurance Level	「真正性確認と属性情報確認」全体の保証レベル。IAAL と AIAL の掛け合わせで保証レベルが決まる。 （注）「付録Ｉ」独自の提案

4.「名寄せ」による「データの紐付け」に関する見直し：データの「正確性」向上のための提言

4.1.「名寄せ用番号」の明確化とデータソースの整備の提案（「初版」「補足２」「付録２」）

現在のマイナンバー制度の「名寄せ」作業は、各データソースの保有する基本４情報の漢字文字コードと漢字文字フォントを使用して行っている（図６参照）。そのため、「初版」、「付録２」で述べたように、マイナンバーと被保険者番号（記号-保険者番号）の紐付けの一部は、現在でも間違った状態のままであり、このままでは永遠に紐付けミスが残り続け、データの「正確性」が確保できないことになる。

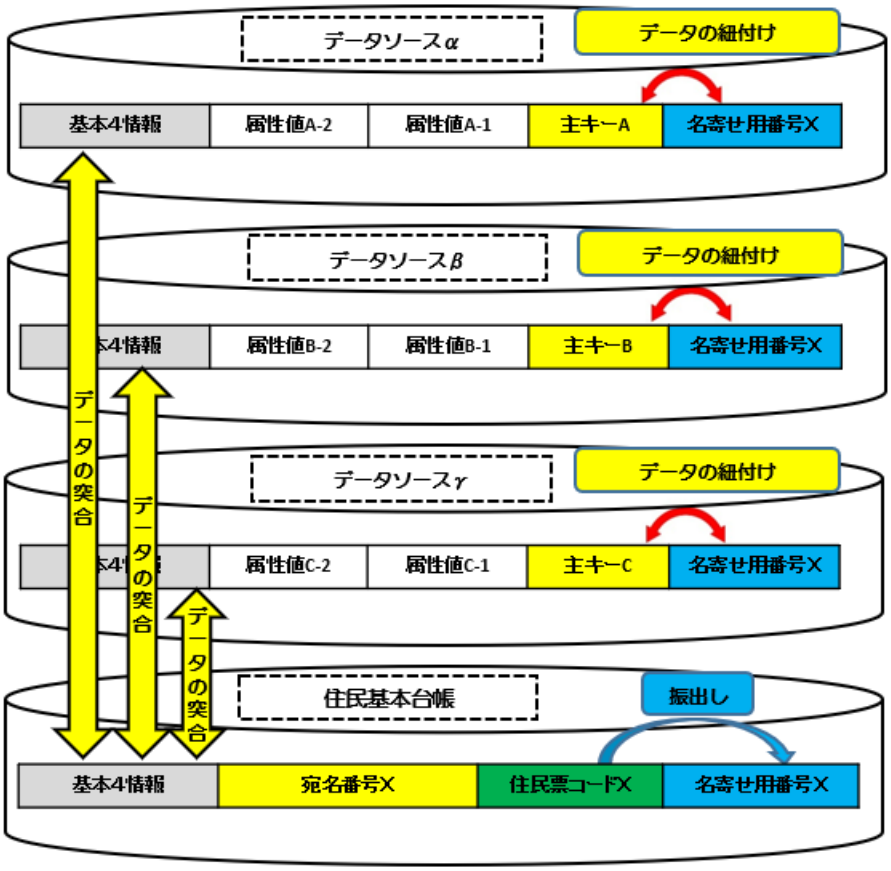


図６　現在の「名寄せ」作業による「データの紐付け」状態

正確性の高い「名寄せ」作業を実施して、可能な限り正確な「データの紐付け」を実現するためには、まず、国民を一意に識別できて、「名寄せ」作業の際にも目視確認できる番号を「名寄せ用番号」として明確化する必要がある。過去の提言書では、「特定個人情報の対象外としたマイナンバー」を「名寄せ用番号」として提案している。加えて、「付録２」では「特定個人情報の対象外としたマイナンバー＋生年月日」を「データの紐付け」作業の際の「名寄せ用番号」相当として使用する提案をしている。そして、各データソースの保有する基本４情報全てに全角カタカナでフリガナを振り、フリガナのデータをコンピュータで突合し、目視チェックと併せて「名寄せ」作業をやり直す必要がある。具体的な手順は、次節に示す。

4.2.信頼性の高い「名寄せ」作業の提案（「初版」「付録２」）

「名寄せ用番号」を明確化した後、以下の手順に従って「名寄せ」作業をやり直して、可能な限り正確な「データの紐付け」状態を各データソースに対して確立する必要がある。

① 「名寄せ」作業開始前に、詳細な「名寄せ」基準を明確にする。まずは、全ての「名寄せ」対象のデータソースの氏名と住所にフリガナを全角カタカナで振ることから始める。「名寄せ」基準は、全自治体、全組織で共通の判断基準（住所表記の「ゆらぎ」への対応など）を作成する。各データソースの氏名に対してフリガナを振る作業は、データの信頼性に直結する作業であるため、フリガナを振る手順と国民自身が確認する手順を明確にした上で慎重に実施しなければならない。マイナンバーと被保険者番号の紐付け作業時のような、拙速で曖昧な作業を行ってはいけない。住所に対するフリガナは、各自治体や関連組織で表記の「ゆらぎ」を全て洗いだし、各自治体や関連組織で慎重にフリガナを振る作業を行う。

② 「データの突合」には、コンピュータ（全角カタカナのフリガナを使用して突合）と人間の目視チェック（漢字とフリガナの両方を使用して突合）を併用する。

③ 人間の複眼チェックと十分な作業期間を確保する。

④ 「名寄せ用番号」はオープンな番号を使用する（つまり、「特定個人情報の対象外としたマイナンバー」を使用する）。

⑤ 「名寄せ用番号」として現在の「マイナンバー」を継続使用する場合、自治体や健康保険の保険者等は永久に修正作業を継続する体制を確保する。

※「付録２」では、上記の「名寄せ」作業のやり直しに加えて、「データの紐付け」の「正確性」向上のために以下の追加提案をしている。（詳細は「付録２」参照）

上記の「名寄せ」作業を実施する際の「名寄せ用番号」として「特定個人情報の対象外としたマイナンバー」に加えて「住民基本台帳に登録されている生年月日」を組み合わせて、「名寄せ」作業を実施するという提案である。具体的には、まず『「特定個人情報の対象外としたマイナンバー」＋「住民基本台帳に登録されている生年月日」』を「名寄せ用番号」相当として使用して上記の名寄せ作業を実施し、各データソースの「主キー」と「名寄せ用番号」相当の紐付けを行う。そして、紐付け完了後の最終確認ステップとして、各データソースの保有する「主キー」に対応する基本４情報中の「生年月日」と、「名寄せ用番号」相当の中の「住民基本台帳に登録されている生年月日」を比較チェックすることによって、「データの紐付け」ミスがあるか否かの確認をする仕組みの構築である。この比較チェックをコンピュータで行うことを加えれば、比較した「生年月日」が異なっていれば「データの紐付け」ミスが存在することに気が付くことができるため、「データの紐付け」の正確性が向上するからである。所詮は人間の目視チェックによるヒューマンエラーは残るというご指摘もあろうが、大切なのは、ヒューマンエラーを最小限にするためのコンピュータの活用とその仕組み作りである。（図７参照）

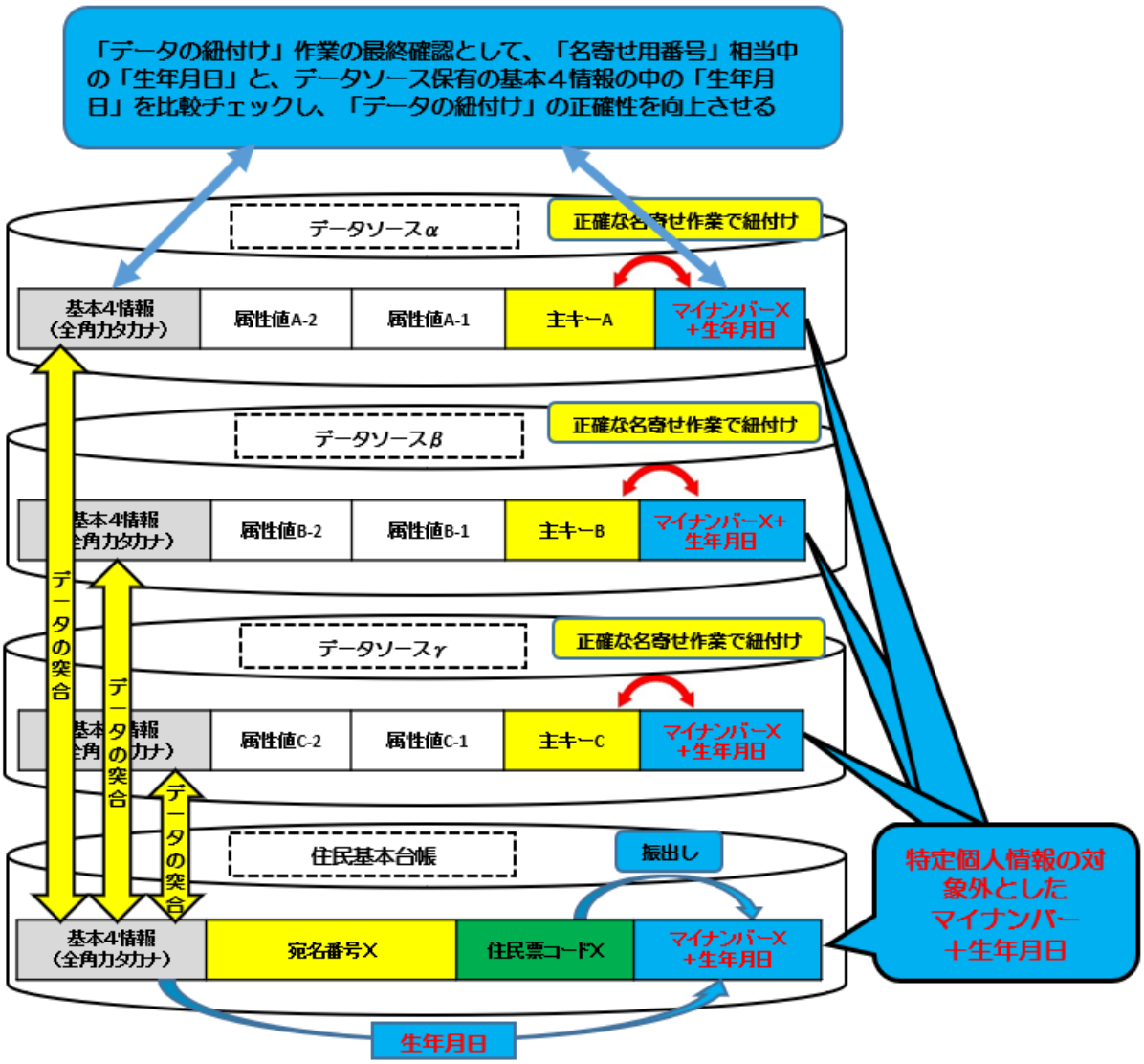


図７　正確性の高い「名寄せ」作業による「データの紐付け」状態（提案）

5.「データの連携」の共通システムに関する見直し：データの「正確性」、「最新性」向上のための提言

5.1.データの「正確性」、「最新性」を確保するためのデータソースの整備の提案（「補足２」「付録２」）

マイナンバー制度の目的を実現するためには、多様なデータソースの「データの紐付け」と「データの連携」を行うシステム開発が必要となる。その際の最重要テーマは、「システムの開発費用削減と開発期間短縮を実現する」ことと、「データの紐付けミスとデータの連携ミスを可能な限り最小化する（データの「正確性」の確保）」ことである。その実現のためには、データ中心アプローチの考え方を用いることによってデータソースの整備を行い「システム設計をシンプル化する」ことと、「データの連携」のシステムは１つの「名寄せ用番号」を用いた「共通のデータ連携システム」として開発し、データやシステムを「個別のアプリケーション」間で共有し使用することが肝要となる。

さらに、マイナンバー制度のシステムは日本社会のデジタル化推進のデータ基盤であり、データの「最新性」を確保することが肝要である。データの「最新性」確保のためには、「データの連携」の方式は「リアルタイム方式」を基本とする。加えて、データソースの整備の段階においてデータソースのデータの作成・更新方法の「リアルタイム方式」化のためのシステム改修や、データソース管理主体者やデータ構造の見直しを含めて整備する必要がある。

しかし、今のマイナンバー制度は図８に示すように、「データの紐付け」と「データの連携」のためのベースになる番号が複数（マイナンバー、符号、シリアル番号）に亘り、非常に複雑なシステム設計になってしまっており、データの「正確性」に不安がある状態である。加えて、今のマイナンバー制度では「付録２」で指摘したように一部のデータソースのデータの「最新性」も確保されておらず、取り扱うデータの「正確性」と「最新性」の両方が確保できていない状態である。

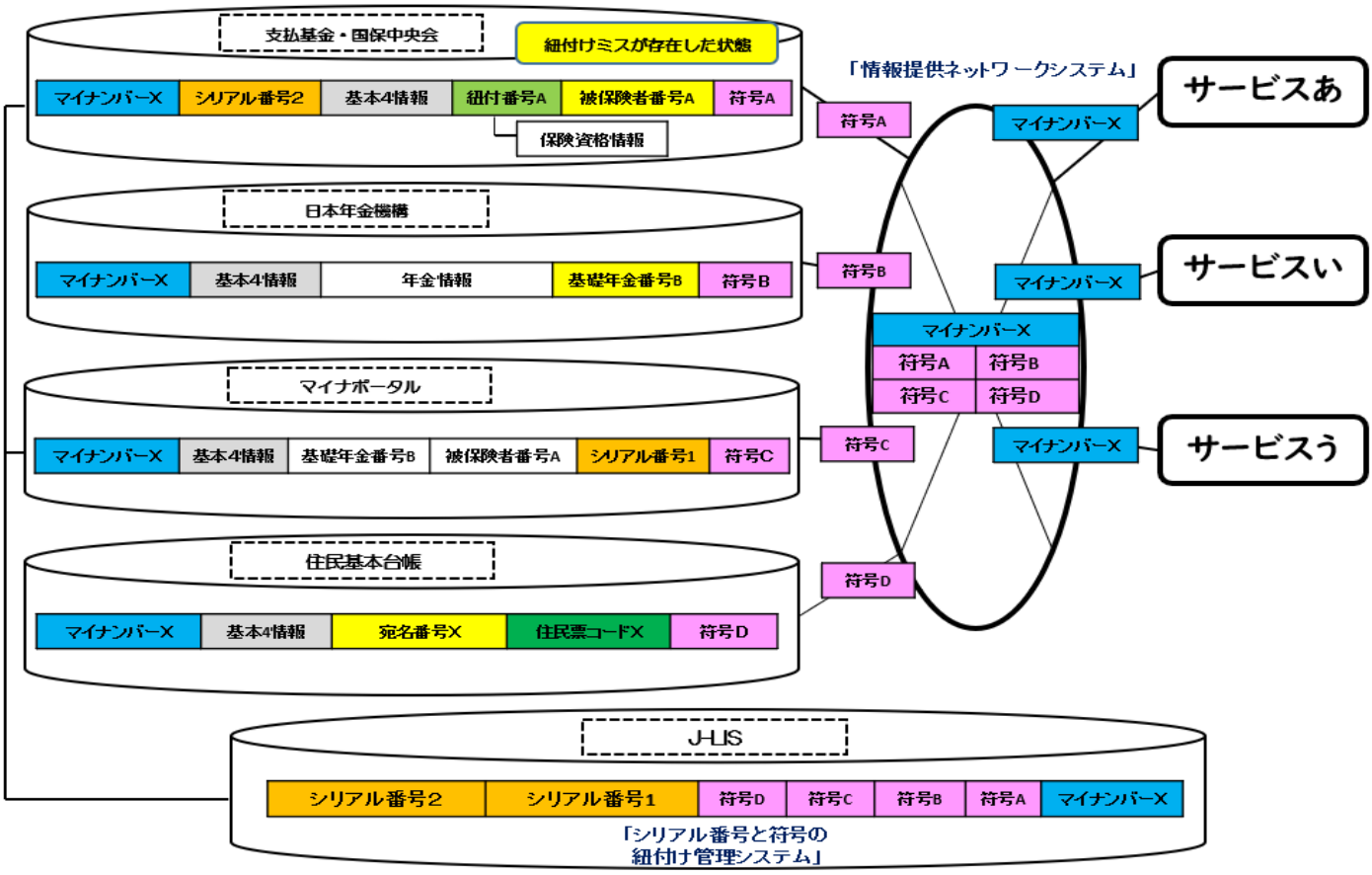


図８　「マイナンバー」、「シリアル番号」、「符号」を使用した現在のマイナンバー制度の複雑な「データの紐付け」と「データの連携」システムのイメージ

マイナンバー制度は日本社会のデジタル化のデータ基盤であり、取り扱うデータの「正確性」と「最新性」を確保することは必須のテーマである。今のままのマイナンバー制度では、せっかく作成したデジタル田園都市国家構想も絵に描いた餅となってしまう。杜撰な基礎工事の上に、巨大なタワーマンションを構築しているようなものである。杜撰な基盤のままでは、いくら表面上のひび割れ対策を施してもひび割れは発生し続けるし、いつか人命にかかわる大きな問題を引き起こしてしまうことに繋がりかねない状態にあると言える。そんなマンションには居住できないし、そんなシステムは怖くて使用できない、と考えるのが普通である。図８のような「名寄せ用番号」として複数の番号を使用することは止めて、図９に示すような１つの「名寄せ用番号」、つまり「特定個人情報の対象外としたマイナンバー」のみを使用し、シンプルな設計で「共通のデータ連携システム」を再構築することを提案している。

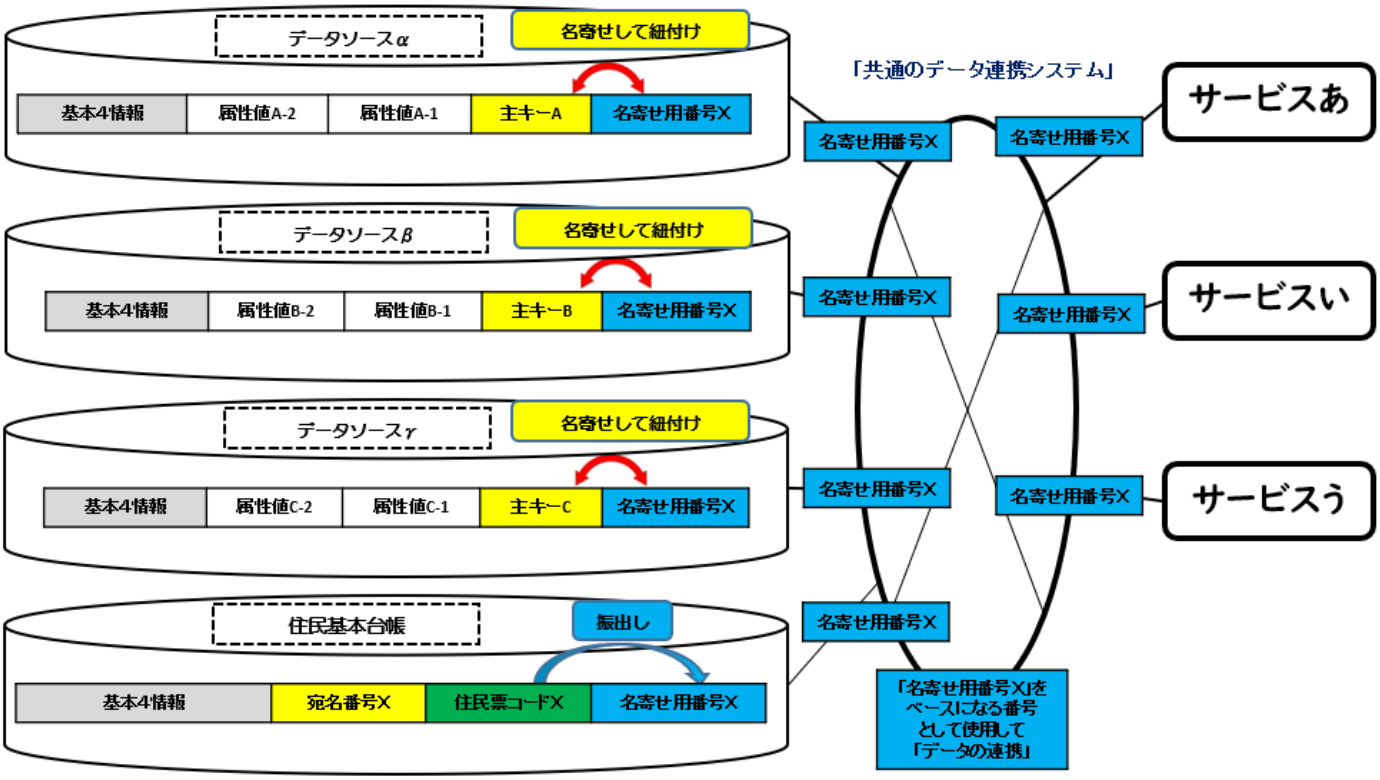


図９　シンプルな「データの紐付け」と「データの連携」システムの構築（提案）

5.2.シンプルでセキュアなデータソース・システム連携方式の提案（「付録２」）

「データの連携」を行う「共通のデータ連携システム」の構築には、具体的には大きく以下の３つの機能が要求される。

① 分散された多様なデータソースに対して、１つのベースになる番号を使用してシームレスにアクセスできること。

② サービスサイトとデータソース間の大容量のデータ交換が、「リアルタイム方式」と「バッチ方式」の両方で可能であること。基本は、「リアルタイム方式」で大容量のデータ交換が可能であることである。

③ サービスサイトとデータソース間の相互の信頼関係の確保と、データ交換のセキュリティが確保されていること。

提言書では、上記の機能要求を満たした「リアルタイム方式」の「共通のデータ連携システム」と、前述した「正確性」と「最新性」が確保されたデータソースと、提言「付録１」で提案した「当人確認（認証）」の仕組みとを組み合わせることによって、シンプルでセキュアなデータソース・システム連携方式のシステムを再構築することを提案している。そのイメージを図１０に示す。なお、「付録２」では、上記の機能要求を満たす「共通のデータ連携システム」方式として、「X-Road」技術（エストニアの電子政府のデータ基盤に採用されている「分散されたデータベースをセキュアに連携させる技術」）の適用を検討することを提案している。

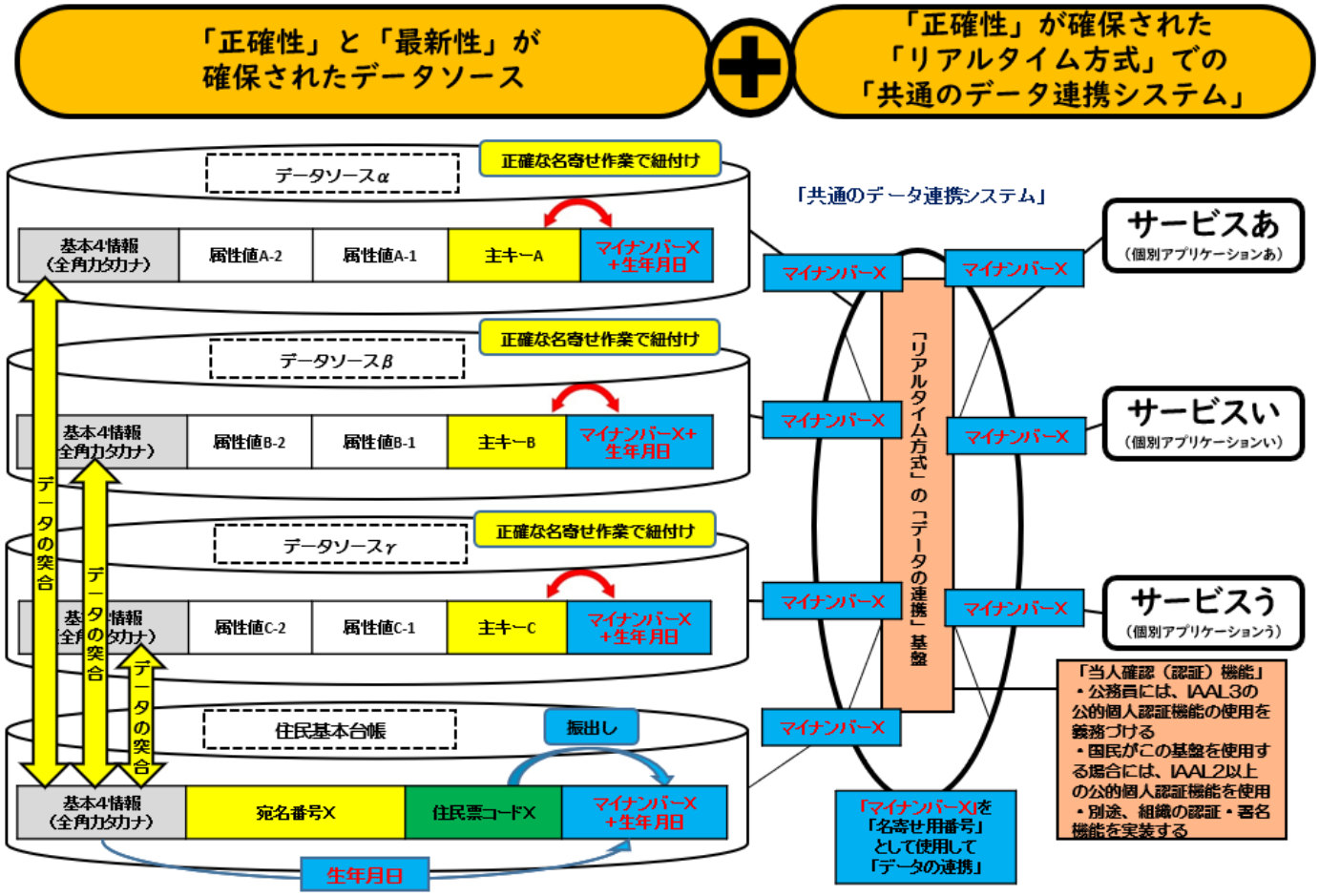


図 10　シンプルでセキュアなデータソース・システム連携方式（提案）

6．おわりに

マイナンバー制度に必要とされるシステムは、「本人確認」、「データの紐付け」と「データの連携」を行うシステムであり、今後の日本社会のデジタル化推進のデータ基盤となるシステムである。このシステムが信頼できる（本人確認の「厳密度」が確保されている、データの「正確性」と「最新性」が確保されている、セキュリティが確保されている）ことと、その結果としてシームレスでスムーズなデータ利活用ができることは、デジタル化推進を安全かつ効率的に行えることに直結する。加えて、最終的にシステムやカードを使用するのは国民であり、そのためには国民が理解できる仕組みであることが大前提である。繰り返し利便性を訴える広報活動をするだけでは不十分であり、システムやカードの使用方法と使用することのリスクについて、国民の「理解度」が上がるような仕組み作りを行う必要がある。

そのためには、システムの全体設計が重要となるが、過去の提言書で指摘したように現在のマイナンバー制度の全体設計は不十分であり、根本的な制度設計に問題を抱えてしまっている。そのため、現在の制度にいくら表面上の微修正を繰り返しても、国民が信頼できて、かつ使用方法を理解できるマイナンバー制度の構築は難しく、本質的な問題解決にはつながらないであろう。

今一度、現在のマイナンバー制度の推進を立ち止まり、全体設計からやり直すことを提案したい。「急がば回れ」である。表面上の微修正や問題対策を繰り返すのではなく、本当に日本社会のデジタル化に必要なマイナンバー制度の姿はどうあるべきかを考え直して、軌道修正を行っていただきたい。軌道修正のポイントは沢山あるが、最も重要な４つのポイントを以下にまとめる。

① カードに関する設計の見直し（身元証明（身元確認）制度構築を含む）：国民の「理解度」の向上のための提言

機能を搭載し過ぎた今のマイナンバーカードは国民の理解を得られない。利用目的が異なるカードごとに適切な運用設計を行い、国民にとって理解を得やすいカードとその仕組みを導入する（表２参照）。あわせて、「補足１」で提案した身元証明（身元確認）制度の構築を行う。カードを使用するのは国民であることを忘れてはいけない。国民目線での見直しが必要である。なお、マイナ免許証と免許証の２枚持ちや、マイナ保険証と資格確認書の共存のような中途半端なカードの統合は、利用者や事務担当者の混乱を招くだけでなく、事務処理コストやシステム運用コストの増大に繋がるためやってはならない。

② 本人確認に関する設計の見直し：本人確認の「厳密度」向上のための提言

今の曖昧な本人確認の用語の定義と保証レベルの厳密度の定義を再考し、「付録１」に示したように本人確認に関する設計を見直す。見直しを行った後に、関連する法令やガイドラインの改定を行い、システム開発を行う。本人確認の厳密化のために導入したはずのマイナンバーカード自体が、逆にマネーロンダリング発生原因となり得るような今の本人確認に関連する制度設計は見直すことが必須である。

③ 「名寄せ」による「データの紐付け」に関する見直し：データの「正確性」向上のための提

言

今の曖昧な「名寄せ」作業のやり方を見直し、「正確性」の高い「名寄せ」作業をやり直し、信頼できる「データの紐付け」状態のデータソースを整備する必要がある。そのためには、氏名と住所に対して、全角カタカナでフリガナを振り、住所表記のゆらぎにも対応した上で、適切な「名寄せ」作業をやり直す。データの「正確性」が確保されていない状態では、医療関係の業務では一歩間違えると生命の危険へと繋がる可能性があるため、適切な方法での「名寄せ」作業のやり直しは必須である。

④ 「データの連携」の共通システムに関する見直し：データの「正確性」、「最新性」向上のための提言

「データの紐付け」と「データの連携」のベースになる番号として、「マイナンバー」、「シリアル番号」、「符号」の３つの番号を使用した複雑なシステムを見直し、番号は１つの「名寄せ用番号」、つまり「個人特定情報の対象外としたマイナンバー」とする。「データの紐付け」と「データの連携」されたデータの「正確性」の確保のためである。その上で、データソースのデータの作成・更新方法の「リアルタイム方式」化やデータ管理主体者、データ構造の見直しを行うことによってデータソースの「最新性」を確保し、「リアルタイム方式」の「共通のデータ連携システム」と組み合わせてシステム開発を行う。そのことによって、シンプルで信頼性が高く（データの「正確性」と「最新性」が確保されている）、データを利活用しやすいデータ基盤として「データの連携」の「共通のデータ連携システム」を再構築する。

マイナンバー制度のシステムは、将来の日本社会のデジタル化（例えば、医療ＤＸや行政ＤＸ）推進のデータ基盤である。データの「正確性」と「最新性」が確保できていない今のシステムはデジタル化推進の足かせとなってしまうため、設計を根本から見直し再構築することが必要である。

最後に、今までの提言書の作成にあたり、「日本・エストニア EU デジタルソサエティ推進協議会」や「情報システム学会」のメンバーの方、その他にも多くの方々にご指導・ご意見をいただきました。ありがとうございました。

過去の提言書も含めて、当研究会の『マイナンバー制度の問題点と解決策』に関する提言が、日本のマイナンバー制度の最適化に向けた軌道修正とデジタル化推進のお役に立てることを願って一旦筆を置きたい。

情報システム学会　マイナンバー制度研究会一同