

情報連携基盤の構築に当たっての論点整理

平成 23 年 6 月 7 日

情報連携基盤技術ワーキング・グループ事務局

はじめに

情報連携基盤技術WGでは、これまで住民基本台帳ネットワークシステムの最高裁合憲判決の趣旨を十分に踏まえた個人情報を取り扱うシステムとすることを前提に検討してきたところであるが、情報連携を行うための仕組みとその仕組みを実現させるための方法等に関して、性能、コスト、拡張性等の様々な観点から検討・整理する。

1 本資料の位置づけ

番号制度に係る電子計算処理組織による情報の連携を実現させるために必要なもののうち、以下の項目について、事務局から検討のたたき台を示したものである。

- (1) 個人に対する付番
- (2) 情報連携基盤
- (3) ICカード

なお、マイ・ポータルにおける認証方法、情報保有機関における「番号」との初期突合と4情報の最新化等についても今後検討が必要である。

2 個人に対する付番（「番号」と符号との関係、桁数）

(1) 「番号」の付番

社会保障・税に関わる番号制度においては、新たに国民一人ひとりに付番される唯一無二の「民－民－官」で利用可能な見える番号である「番号」を付番することとしている（社会保障・税番号要綱）。

個人に付番する「番号」については、住基ネット等、既存のインフラをできる限り生かした効率的なシステムを構築した上で、国民に対して悉皆的に付番されている既存の番号である住民票コードと一対一で対応する新たな番号とすることとされている（社会保障・税番号要綱）。

(2) 情報連携で活用する符号の生成

社会保障・税に関わる番号制度における情報連携では、「個人情報を一元的に管理することができる機関又は主体が存在しないこと」を実現するた

めの1つの方策として、「番号」を情報連携の手段として直接用いず、当該個人を特定するための情報連携基盤及び情報保有機関等でのみで用いる符号を用いることとしている（社会保障・税番号要綱）。

符号とは、情報連携において個人を特定するため、情報連携に係る電子情報処理組織内において用いる識別子である。

この符号が備えるべき要件としては、次の二点が考えられる。

一点目としては、異なる分野間で、個人情報の不正なマッチングを不可能とするため、それらの分野で別々の符号を用いる必要がある。

二点目としては、各情報保有機関の内部の利用番号が情報連携基盤に集まるような形にすることは個人情報の一元管理につながるため、利用番号のいわゆる仮名として符号を用いる必要がある。

さらに、情報連携基盤において、各情報保有機関が用いる別々の符号を個々の対象者と紐付け、対象者を一意に特定するための符号が必要であると考えられる。

符号は、情報連携に関する処理を行う情報連携基盤及び情報保有機関等のシステムの内部で処理されるものであることから、符号は人が認識することが困難な程度の桁の長さであったとしても、システム上の処理等には大きな差は生じないと思われる。

そこで、符号の桁数について相当程度の長さを持たせることで、将来の情報連携の拡張に向けて、多くの符号を生成する余地を持たせることができる（注）。

（注）「番号」については、人が「番号」として認識することができる程度の桁の長さであることが要求されるとともに、一旦、「番号」を交付した後は、その後に「番号」の桁数の変更を行うことは、運用上、非常に困難であると考えられるため、「番号」の桁数は固定となると考える。

（3）情報連携で活用する符号の生成方法

情報連携で活用する符号の生成方法としては、次の2つの方策が考えられる。

イ 案1 可逆暗号方式により生成する方法

可逆暗号方式とは、番号連携の都度、対象となる番号及び符号を暗号化するものであり、暗号鍵により、必要が生じた都度変換生成するため、変換後の値を紐付けて管理する必要が無く、変換前後の値に遡ることができる方法である。

第2案のコード変換テーブル方式の場合と比較した場合、変換前後の

値を紐付けて管理することが不要であり、変換処理が終了次第、保持する必要の無い情報を消去する運用が可能であるため、情報漏洩時の影響範囲は局所的なものにとどまる。

実現性については、第2案のコード変換テーブル方式で必要となるデータベースへのアクセス時間が生じない分、高速な処理を実現できる可能性も考えられる。ただし、案1の方式と同様の仕組みを採用したシステムは前例がない。

稼働の安定性については、案2のコード変換テーブル方式と比べ、必要が生じた都度符号を変換生成することによる障害発生の契機が高くなるという指摘がある一方で、案2においてもテーブルを暗号化して管理する必要があることから、稼働の安定性においては大きな相違点はないという意見もある。

また、暗号危殆化への対応に伴い発生する、符号の入れ替えに要するコストが問題点として考えられる。

現在の暗号技術は、電子計算機を用いても解読までに莫大な時間と費用を要することを前提に安全性を保障しており、今後の技術の進歩等を考慮すると、暗号危殆化への対応は長期的には必然なものと考えられる。

暗号危殆化への対応としては、危殆化を懸念される暗号鍵の改良あるいは交換を実施することが考えられるが、これにより、可逆暗号生成される符号は別の値が生成され、それまでの値を用いることはできないことから、符号を用いる全ての情報保有機関において、符号の更新作業が必要となる。

ロ 案2 コード変換テーブル方式により生成する方法

コード変換テーブル方式とは、乱数を用いて論理的に遡れない形でコードを変換し、変換前後のテーブルを保持する方法である。

乱数計算は一般的な演算技術を活用することで実施可能であることに加え、変換前後のコードをテーブルで管理して変換する方式は、既に一般的となっている技術により構築することが可能である。

案1の可逆暗号方式では暗号変換後の値を紐付けて管理する必要が無いことに対し、変換前後のコードを紐付けし、コード変換テーブルとしての完全性を維持管理する必要がある。また、コード変換テーブルの情報が漏洩した場合は、全ての番号及び符号を別の値に変更する必要があるなど、案1の可逆暗号方式よりも影響が広範囲に及ぶ。

一方、案1の可逆暗号方式と比べ、暗号危殆化への対応に伴う符号の更新作業が原則生じないものと想定される。

なお、「当該符号を「番号」から推測できないような措置を講じる」とされているところであり、符号については、番号連携の方法により符号の種類及びその生成方法が異なることとなると思われるが、「番号」から符号を、あるいは符号から「番号」を推測することができない仕組みが求められる。

以上を前提として、符号の生成方法については、次の2つの方法が考えられる。

案1 住民票コードを変換して生成する方法

「番号」と符号の間において、直接的な関係性を有しないものとする 것을考慮し、「番号」とは別の生成手順で、住民票コードを変換して符号を生成する方法である。

案2 「番号」を変換して生成する方法

符号が「番号」の代わりに情報連携で用いるものであることを考慮し、「番号」を変換して符号を生成する方法である。「番号」から直接符号を生成することで、「番号」と符号との間に関係性が存在することになるが、「番号」を乱数により変換して符号を生成する場合には、一方からもう一方を推測することは困難となると思われる（「番号」の付番方法（住民票コードから「番号」を付番する方法）と同じ。）。一方、乱数で生成するとはいえ、住民票コードから生成する場合と比べ、リンクコードから「番号」が見破られるリスクが高まるのではないかといった懸念がある。

(4) 「番号」の桁数

個人の「番号」の桁数については、「番号」が個人に通知され、又は「番号」が記載されたICカードが交付され、その「番号」が窓口等で人に確認されるものであることが想定されることから、人が「番号」として把握することができる程度の長さの桁数とすることが適当であると考ええる。

また、個人の「番号」は、住民票コードを乱数により変換することで生成することを想定していることから、個人の「番号」の桁数は、住民票コードの桁数（11桁）を勘案したものとなることが考えられる。

さらに、個人の「番号」と法人の「法人番号」について、番号制度の運用上の効率性等を考慮し、両者の桁数を統一するかどうか、また、個人と法人において、重複を認めるかどうかについて、以下のとおり検討する必要がある。

	桁数の統一	重複の可否
案1	する	可
案2	する	不可
案3	しない	不可

「番号」と「法人番号」の桁数を統一する場合、それぞれの桁数に関する要件を満たしたものとする必要がある。

法人の「法人番号」については、「商業・法人登記の申請に係る会社法人等番号を活用した番号」とすることから（社会保障・税に関わる番号制度についての基本方針）、「法人番号」の桁数は、会社法人等番号の桁数（12桁）を勘案したものとなることが想定される。

そのため、個人の「番号」と法人の「法人番号」について桁数を統一する場合には、両方の番号の桁数は会社法人等番号や住民票コードの桁数を勘案したものとなることが考えられる。

「番号」と「法人番号」との間で重複を認める場合、同じ数字の組み合わせで特定される社会保障・税に関わる番号制度の主体が複数存在する可能性があることになり、「番号」が国民一人ひとりに付番される唯一無二の番号であるとする性質上、適当でないのではないかと考える。この考え方もある。

これに対し、「番号」と「法人番号」との間で重複を認めない場合、「番号」のある桁を「個人と法人を分類するための桁」とする等の方法により、個人と法人で番号として使用する数字の組み合わせが異なるように「番号」の桁数及び各桁の性質を設計した上で、付番機関のシステム開発を行う必要がある。

一方、「番号」と「法人番号」の桁数を統一しない場合、桁数に関する両者の要件を満たす必要はないが、個人及び法人の両方の番号に係る情報を保有する各情報保有機関においては、個人と法人で異なる桁数の番号が窓口等で提供され、事務処理を行うことになることから、これを前提としたシステム設計を行う必要がある。

以上の点を踏まえて、「番号」の桁数を決定していく必要があると考える。

3 情報連携基盤

(1) 番号連携

社会保障・税に関わる番号制度における機関間の情報連携に当たっては、情報連携基盤及び情報保有機関において情報連携を行う情報の対象者に係る識別子を用いることを想定している。

識別子として何を用いて、どのように機関間の情報連携を行うかについては、次の5つの案が考えられる。

案1 「番号」を用いた情報連携

案2 情報連携のためのシステム内部の符号（2種類）を可逆暗号方式で生成し、そのうちの1種類の符号（リンクコード）を情報保有機関が保有する情報連携

案3 情報連携のためのシステム内部の符号（2種類）をコード変換テーブル方式で生成し、そのうちの1種類の符号（リンクコード）を情報保有機関が保有する情報連携

案4 情報連携のためのシステム内部の符号（2種類）をコード変換テーブル方式で生成し、情報保有機関が保有する情報と「番号」との紐付けがされるか否かに応じて、2種類の符号のうちの1つを情報保有機関が保有する情報連携

案5 情報連携のためのシステム内部の符号（1種類）を生成し、当該符号（リンクコード）を情報保有機関が保有する情報連携

イ 案1「番号」を用いた情報連携

(1) 概要

情報連携基盤を通じた機関間の情報連携において、国民に交付される「番号」をそのまま使用することとし、情報連携基盤と情報保有機関との間での「番号」に係る情報（属性情報）をやりとりする際に、これを用いるものである。

(2) 他の案との比較

案1については、情報連携基盤を通じた情報保有機関間の連携において、「番号」を変換した符号を生成し、情報連携に用いる必要がないことから、情報連携基盤における符号の変換処理を要しない点で、他の案よりも情報連携基盤におけるシステム処理上の負荷は低く、システムの安定性は高いと考える。

しかし、「番号」をキーとした機関横断的な情報連携が行われることで、国が「個人情報を一元的に管理することができる主体」となり得る可能性についての懸念が示されることへの配慮を求められることが考えられる。

加えて、情報保有機関間において、「番号」と「番号」に紐付けられた属性情報を用いて、不正なマッチングが可能となる危険性がある。

そのため、流失した「番号」を変更し、情報保有機関が保持してい

る「番号」をすべて置き換える必要が生じ、他の案と比較してプライバシー影響度は非常に大きい。

また、「番号」で情報連携を行う場合には、情報保有機関は保有する個人の情報と「番号」との紐付けを行っていることが必須となるため、「番号」との紐付けを行っていない機関とは、番号制度に係る情報連携を行うことができないこととなる。

さらに、案１においては、社会保障・税の番号制度において、将来的に実現することが求められる「民間の機関等との情報連携」の場面においても、「番号」をそのまま活用した連携を行うことになるが、民間の事業者が情報連携時に使用するネットワークは、国・地方公共団体が利用するネットワークとはセキュリティ対策が異なる場合があることが想定されるところ、民間の事業者が使用するネットワークにどこまでのセキュリティの保持を求めることができるのか等の課題があると考えられる。

以上の点から、他の案と比較して、案１は拡張性が劣るとと思われる。

なお、番号制度要綱においては、「番号」は「個人情報保護の観点から、これを直接、個人を特定する共通の識別子として用いてはならないこと」とし、「番号」を用いない情報連携を行うこととしているところである。

ロ 案２ 情報連携のためのシステム内部の符号（２種類）を可逆暗号方式により生成し、そのうちの１種類の符号（リンクコード）を情報保有機関が保有する情報連携

（イ）概要

情報連携基盤を通じた機関間の情報連携において、「番号」をそのまま用いるのではなく、「住民票コード」を変換して符号を生成し、システム内部でこの符号により対象となる個人を特定し、情報連携を行うものである。

符号については、「住民票コード」を可逆暗号方式により変換してＩＤコードを生成し、更に、ＩＤコードを可逆暗号方式により変換してリンクコードを生成する（２種類の符号の生成）。

ＩＤコードは、情報連携基盤において、情報連携を行う情報の対象者を一意に特定するための情報として活用するものである。

情報連携の際、情報連携基盤においては、情報保有機関ごとに提供されるリンクコードを変換する必要があるため、これらを束ねる識別子として、情報連携基盤でＩＤコードを保持し、ＩＤコードからリンクコードへの変換を行う。

一方、情報保有機関には、機関ごとに異なるリンクコードを提供し、リンクコードと情報保有機関が保持する属性情報に紐付けることとする。

情報連携において、機関毎に異なるリンクコードにより情報連携を行うこととすることで情報保有機関間において、情報連携基盤が関与しない不当な情報連携が行われることを技術的に回避するものである。

(ロ) 他の案との比較

案2の方法では、万が一、情報保有機関AのリンクコードAとリンクコードAに紐付けられている属性情報が漏洩した場合、他の情報保有機関とはリンクコードが異なっていることから、他の情報保有機関が保有する個人情報との不正なマッチングはできないため、情報保有機関AのリンクコードAのみを変更することで対処可能であることから、他の案よりもプライバシー影響度は低いと思われる。

また、案2の情報保有機関に異なるリンクコードを提供する情報連携は、「番号」を利用しない機関に係る情報連携についても対応できるものであり、段階的に増加することが想定されるユースケースへの対応や将来的な情報連携を行う分野の拡大の可能性等を考慮すると、拡張性の点で案1よりも優れていると考えられる（案3から案5まで同様）。

一方、案2は、すべての情報連携において、情報連携基盤で可逆暗号方式による符号変換処理（情報保有機関Aが保持するリンクコードAからIDコードへの変換、IDコードから情報保有機関Bが保持するリンクコードBへの変換）が必要となるため、情報連携基盤での変換処理に係るシステム負荷が生じることになる。この点については、大量のデータベースの検索を行う必要のあるコード変換テーブル方式を採用する案3と比べ、どの程度のシステム運用面での負荷が生じ、どの程度、コストパフォーマンスに差が出るのか、今後、比較検討する必要がある。

また、情報連携基盤にコード変換機能が必要となるが、当該方式と同様の仕組みを採用したシステムは前例がないため、当該機能を調達し実装する段階においては、案1よりも調達の透明性・公平性の確保に留意する必要がある（案3から案5までと同様）。

- ハ 案3 情報連携のためのシステム内部の符号（2種類）をコード変換テーブル方式により生成し、そのうちの1種類の符号（リンクコード）を情報保有機関が保有する情報連携

(イ) 概要

情報連携基盤を通じた機関間の情報連携において、「番号」をそのまま用いるのではなく、「住民票コード」を変換して符号を生成し、システム内部でこの符号により対象となる個人を特定し、情報連携を行う点は案2と同様であるが、符号（IDコード、リンクコード）の生成を可逆暗号方式ではなくコード変換テーブル方式により行う点が案2と異なる。

IDコードは、情報連携基盤において、情報保有機関ごとに異なるリンクコードを生成し提供する際に活用する。リンクコード生成後は、コード変換テーブルにこれを格納し、情報連携の際には、このコード変換テーブルにより、リンクコードから別のリンクコードへの変換を行う。

(ロ) 他の案との比較

案3は、万が一、情報保有機関Aのリンクコードとリンクコードに紐付けられている属性情報が漏洩した場合、案2と同様に、他の情報保有機関とはリンクコードが異なっていることから、他の情報保有機関が保有する個人情報との不正なマッチングはできないため、情報保有機関AのリンクコードAのみを変更することで対処可能であることから、他の案よりもプライバシー影響度は低いと思われる。

また、案3の情報保有機関に異なるリンクコードを提供する情報連携は、「番号」を利用しない機関に係る情報連携についても対応できるものであり、段階的に増加することが想定されるユースケースへの対応や将来的な情報連携を行う分野の拡大の可能性等を考慮すると、拡張性の点で案1よりも優れていると考えられる（案2、案4及び案5まで同様）。

一方、案3は、すべての情報連携において、情報連携基盤でコード変換テーブル方式による符号変換処理（情報保有機関Aが保持するリンクコードAから情報保有機関Bが保持するリンクコードBへの変換）が必要となるが、情報連携基盤での変換処理に係るシステム負荷は、案2と比べ、どの程度のシステム運用面での負荷が生じ、どの程度、コストパフォーマンスに差が出るのか、今後比較検討する必要がある。

また、情報連携基盤におけるコード変換機能が必要となり、当該機能を調達し実装する段階においては、案1よりも調達の透明性・公平性の確保に留意する必要がある（案2、案4及び案5と同様）。

二 案4 情報連携のためのシステム内部の符号（2種類）をコード変換

テーブル方式により生成し、情報保有機関が保有する情報と「番号」との紐付けがされるか否かに応じて、２種類の符号のうちの１つを情報保有機関が保有する情報連携

(イ) 概要

「番号」と保有する情報の紐付けを行っている機関間又は特定の分野内での情報連携については、住民票コードから生成されるＩＤコードを用いて情報連携を行い、それ以外の機関間の情報連携については、ＩＤコードから生成される機関ごとに異なるリンクコードを提供した上で情報連携を行うものである。

情報連携基盤を通じた機関間の情報連携において、「番号」をそのまま用いるのではなく、「住民票コード」を変換してＩＤコードを生成し、さらに、ＩＤコードを変換してリンクコードを生成することについては、案２及び案３と同じである。

一方、「番号」との紐付けが行われている情報保有機関間や一定の分野内における情報連携については、共通の符号（ＩＤコード）を用いて情報連携を行い、それ以外の機関間における情報連携は、機関毎に生成・提供されるリンクコードを用いて情報連携を行うとする点が案２及び案３との違いである。

(ロ) 他の案との比較

案４の場合、一部の情報連携については、ＩＤコードを用いて情報連携が行われるため、情報連携基盤でリンクコードＡからＩＤコード、ＩＤコードからリンクコードＢへの変換をせずに情報連携が行われることから、変換処理に係る情報連携基盤のシステムの負荷は、すべての情報連携においてコード変換処理を行う案２よりも低くなることが見込まれる。

また、案４は、「番号」を利用しない機関に係る情報連携についても対応できるものであり、段階的に増加することが想定されるユースケースへの対応や将来的な情報連携を行う分野の拡大の可能性等を考慮すると、拡張性の点で案１よりも優れていると考えられる（案２、案３及び案５と同様）。

一方、ＩＤコードを保持する情報保有機関間において個人情報の不正なマッチングを防ぐことができなくなる点において、案４のように共通のＩＤコードによる情報連携はプライバシー保護の観点から問題がある。加えて、万が一、ＩＤコードによる情報連携を行う情報保有機関のＩＤコードとＩＤコードに紐付けられた属性情報が漏洩した場合、同じＩＤコードにより情報連携を行う複数の情報保有機関が保有

する個人情報とのデータマッチングが可能となる危険性があり、該当する複数の情報保有機関においては、IDコードの入れ替えが必要となるため、案2及び案3よりもプライバシー影響度は大きいと思われる（リンクコード漏洩時の影響は、案2と同等である。）。

また、情報連携基盤におけるコード変換機能が必要となり、当該機能を調達し実装する段階においては、案1よりも調達の透明性・公平性の確保に留意する必要がある（案2、案3及び案5と同様）。

ホ 案5 情報連携のためのシステム内部の符号（1種類）を生成し、当該符号（リンクコード）を情報保有機関が保有する情報連携

(イ) 概要

機関間の情報連携は、機関毎に異なるリンクコードを使用して情報連携を行うが、「番号」と保有する情報の紐付けを行っている機関間又は特定の分野内での情報連携については、共通のリンクコードを用いて情報連携を行うものである。

情報連携基盤を通じた機関間の情報連携において、「番号」をそのまま用いるのではなく、符号を生成し、この符号をシステム内部で使用するについては、案2から案4までと同じであるが、住民票コードから生成された「番号」を更に変換してリンクコードを生成する点や、IDコードは生成せず、リンクコードで情報連携を行う点で案2から案4までとは異なる。

具体的には、リンクコード付番機関において「番号」から機関毎のリンクコードを生成し、情報連携基盤に生成したリンクコードに関する情報を提供する。情報連携基盤は、各機関のリンクコードをコード変換テーブルで管理し、情報保有機関AのリンクコードAから情報保有機関BのリンクコードBへの変換を行う。

なお、「番号」を乱数により変換して生成した符号（リンクコード）を用いて情報連携を行うことと「番号」そのものを用いて情報連携を行うことの差異については、整理が必要であると考える。

(ロ) 他の案との比較

案5の場合、一部の情報連携については、共通のリンクコードを用いて情報連携が行われるため、情報連携基盤でリンクコードAからIDコード、IDコードからリンクコードBへの変換をせずに情報連携が行われることから、変換処理に係る情報連携基盤のシステムの負荷は、すべての情報連携においてコード変換処理を行う案2よりも低くなることが見込まれる。

また、案5は、「番号」を利用しない機関に係る情報連携についても対応できるものであり、段階的に増加することが想定されるユースケースへの対応や将来的な情報連携を行う分野の拡大の可能性等を考慮すると、拡張性の点で案1よりも優れていると考えられる（案2、案3及び案4と同様）。

一方、案5では、リンクコードは情報保有機関ごとに提供することを原則とするが、「番号」との紐付けが行われる情報保有機関間の情報連携や複数の情報保有機関で共通のリンクコードを用いることが当該機関間の情報連携に伴う情報保有機関の業務の効率性等の面で適当であると認められる場合には、複数の機関に同一のリンクコードを提供して情報連携を行うこととするものである。

共通のリンクコードを保持する情報保有機関間において個人情報の不正なマッチングを防ぐことができなくなる点において、案5のように共通のリンクコードによる情報連携は、プライバシー保護の観点から問題がある。加えて、この場合、限られた情報保有機関でのみリンクコードを共用することになるが、万が一、共通のリンクコードによる情報連携を行う情報保有機関のリンクコードとリンクコードに紐付けられた属性情報が漏洩した場合、共通のリンクコードにより情報連携を行う複数の情報保有機関が保有する個人情報とのデータマッチングが可能となる危険性があることから、該当する複数の情報保有機関において、リンクコードの入れ替えが必要となるため、案2及び案3よりもプライバシー影響度は大きいと思われる。

また、情報連携基盤におけるコード変換機能が必要となり、当該機能を調達し実装する段階においては、案1よりも調達の透明性・公平性の確保に留意する必要がある（案2、案3及び案4と同様）。

(2) 情報連携

照会元情報保有機関及び照会先情報保有機関間の個人情報等のデータの送受信方式については、情報連携基盤を介して送受信を行う方式と、各情報保有機関同士で直接送受信する方式が考えられる。

イ 案1 情報連携基盤を介して送受信を行う方式（ゲートウェイ方式）

情報連携基盤にデータ送受信機能を実装し、情報連携に係る全てのデータ送受信を情報連携基盤を経由して行う方式である。

この方式は案2に比し、情報保有機関側のデータ送受信機能の負担が軽く、比較的容易に構築することができる一方、情報連携基盤が障害等で機能不全に陥った際は情報連携基盤に接続される全ての情報連携に影

響を及ぼすことになる。

また、情報連携に係るデータの送受信が情報連携基盤に集中することから、送受信を制御するサーバにボトルネックが発生し、情報連携が円滑に行われない可能性が懸念されるほか、これを解消するためには高性能なサーバが必要となることから、案２に比し情報連携基盤の構築費用は高額となる。

ただし、情報連携に係る証跡が情報連携基盤に集約される点で案２に比し可監査性において優れる。

その他、情報連携基盤のデータ送受信機能は、これに接続される全ての情報保有機関のシステム運用時間及び稼働状況に応じた送受信制御を行う必要があることから、案２に比し、情報連携基盤の構築費用が高額になるほか、情報連携基盤の運用が複雑になるなどの問題点がある。

なお、この方式では、情報連携に係る個人情報が一時的に情報連携基盤に留まるため、個人情報が集約しうるとの指摘がある。

ロ 案２ 情報保有機関間で直接送受信を行う方式（アクセストークン方式）

情報連携に係るデータ送受信を情報連携基盤を介することなく、情報保有機関間で直接行う方式である。

この方式は案１に比し、情報保有機関側にのみデータ送受信機能を実装するため、各情報保有機関がネットワーク上の連携先に関する宛先情報及びシステム稼働状況等を把握する必要があるため、案１に比し、情報保有機関側のデータ送受信機能の構築費が高額になるほか、運用が複雑になるなどの問題がある。

ただし、データの送受信が分散されることから情報連携基盤の負荷が小さく、機器等も最小構成で良いため、案１に比し情報連携基盤の構築費用は安価となるが、一方で情報連携に係る行政機関の監視が不十分との指摘がある。

また、情報連携基盤が障害等で機能不全に陥った際もデータ送受信機能は情報保有機関側にあることから、臨時的・限定的な代替措置が容易である。

なお、案１の方式と案２の方式の複合型も考えられる。

４ ＩＣカードの発行主体・方法、交付主体・方法、義務化

I. 社会保障・税番号要綱における記述

VIII ICカード

1 概要

自己の「番号」に係る個人情報についてのアクセス記録の確認等を行うことができるマイ・ポータルにログインするため、また、法令に基づき「番号」を取り扱い得る事業者等が本人確認をした上で「番号」を確認できるようにするため、「番号」、「氏名」、「住所」、「生年月日」及び「性別」が記載され、また、公的個人認証サービスが搭載された番号制度に対応するＩＣカードを交付できるようにする。

ＩＣカードは、住民基本台帳カードのこれまでの国及び地方公共団体における普及の拡大の取組の経過等を踏まえて、可能な限り、現行の住民基本台帳カード、住基ネットや公的個人認証サービス等を活用しつつ、住民基本台帳カードが有する機能等に加え、次のとおり改良するものとする。

なお、住民基本台帳カードの交付同様、ＩＣカード交付時に厳格な本人確認を行い、不正取得等がないよう適切な措置を講じることとする。

- (1) マイ・ポータルにログインするために、現在は署名サービスのみに限られている公的個人認証サービスに認証用途を付加する。
- (2) 電子証明書の有効期間を現行の３年から５年に延長し、公的個人認証の利便性を高める。
- (3) 民間事業者の窓口等で電子的に本人確認を行うため署名検証者を民間事業者に拡大する。
- (4) 「番号」の告知の際、「番号」の真正性を担保するため、ＩＣカードの券面に「番号」を記載する。

2 交付等

自己に関するアクセス記録を確認する権利を個人に対して保障する観点から、交付の対象者、交付時期、交付方法、費用負担等について、引き続き検討する。

Ⅱ．論点項目

1 ICカードに記載・記録する情報の範囲

- (1) ICカードへの記載・記録が必須と考えられる情報項目

①券面記載事項

番号、氏名、住所、生年月日、性別

②ICチップ記録事項

「番号」、公的個人認証サービス（署名用、認証用）の秘密鍵・電子証明書

(2) IC カードへの記載・記録について検討が必要と考えられる項目

①券面記載事項

顔写真 等

②IC チップ記録事項

住基ネット関連機能、条例対応機能、健康保険証機能 等

(注) 上記については、社会保障サブワーキンググループにおける検討結果も踏まえて対応する必要がある。

(3) IC カードへの記載・記録についての考え方

事項が少ないほど発行・再発行が容易であるが、カードの利用にあたって常にオンラインでの確認が必要となる。

事項が多いほどカード1枚で多くの分野を、オンラインを使わず現場での確認により利用可能であるが、発行・再発行に手間と時間がかかる。

2 IC カードに関係する各種イベントへの対応

(1) IC カードに関係する物理的イベントへの対応

イ 初回交付

(イ) 発行者、交付者

(ロ) 交付方法（義務化の有無、交付期間等）

(ハ) 券面記載事項

(ニ) 半導体集積回路記録事項

ロ 更新・再交付

(イ) 有効期間

(ロ) 手続方法

ハ 紛失・破損

(イ) 手続方法

(ロ) 臨時的代替措置

ニ 失効

(イ) 手続方法

(ロ) 技術的対応方法

ホ 返納

(イ) 手続方法

へ 廃棄

(イ) 手続方法

(2) IC カードに記載・記録する情報の変更に係るイベントへの対応

イ 券面記載事項変更

(イ) 氏名変更

(ロ) 住所変更

(ハ) 番号変更

(ニ) 性別変更

ロ IC チップ記録事項変更

(イ) 公的個人認証サービス

(ロ) 健康保険証機能等

(ハ) 条例対応機能

(ニ) 住基ネット関連機能