（第２回情報連携基盤技術ＷＧ（３／４）提出資料）

参考資料２

社会保障・税に関わる番号制度及び国民ＩＤ制度における情報連携基盤技術の骨格案（その１）

平成２３年３月４日
情報連携基盤技術ワーキング・グループ

第１　個人に対する付番、番号連携及び情報連携

１．基本的な考え方

（１）「番号制度構築に当たっては、各機関間の情報連携は情報連携基盤を通じて行わせることにより、情報連携基盤がデータのやり取りの承認やアクセス記録の保持を行い、国民が自己情報へのアクセス記録を確認できるようにするなど、個人情報保護に十分配慮した仕組みとする」（基本方針Ｐ．６）必要がある。

（２）情報連携基盤の構築に当たっては、住民基本台帳ネットワークシステム（以下「住基ネット」という。）に係る最高裁合憲判決（最判平成２０年３月６日）で示された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、何人も個人に関する情報をみだりに第三者に開示又は公表されない自由を有することなどの判断枠組みに適合した形で個人情報を取り扱うシステムとすることが必要である。さらに、社会保障・税に関わる番号制度及び国民ＩＤ制度においては、取り扱う個人情報が、住基ネットの本人確認情報よりも格段に秘匿性の高い社会保障・税に係る情報を中心としており、かつ、住基ネットが行わないこととしているデータマッチングを行うこととするものであることから、より一層高度の安全性を確保することが求められるのではないか。

２．情報連携の原則

（１）「見える」「番号」を直接用いない情報連携

情報連携基盤において、異なる情報保有機関等が有する同一人の情報を連携するためには、当該個人を特定する共通の識別子（以下「ＩＤコード」という。）を用いることとなるが、「番号」は「民－民－官」で広く利用される「見える番号」であることから、これをそのままＩＤコードとして用いることは、個人情報保護の観点から適切でないのではないか。

（２）「見えない」ＩＤコードを用いる情報連携

したがって、ＩＤコードは、これを認知できる者を極力最小限とする「見

えない番号」とすべきではないか。その際、従来の電子行政タスクフォースにおける国民ＩＤ制度の検討においては、①「住民票コード」又は②「住民票コードに対応した新しいコード」の２案が選択肢として示されていたが、個人情報保護の観点をより重視し、ＩＤコードを認知できる者を極力最小限とすることが必要であるということを前提とすれば、住民票に記載されている住民票コードではなく、②「住民票コードに対応した新しいコード」とすべきではないか。

（３）情報保有機関ごとに付与されるリンクコードを用いる情報連携

ＩＤコードは情報連携基盤において管理されることとなるが、仮にこれを情報保有機関も共有し、それで情報連携基盤にアクセスさせることとすると、万一漏洩した際にはその影響が他の情報保有機関にも波及する可能性がある。そこで、「番号」を含む利用番号とＩＤコードの間にＩＤコードと対応関係のある別の「見えない」コード（以下「リンクコード」という。）を介在させ、原則として情報保有機関ごとに異なるリンクコードを付与し、情報保有機関はそれぞれのリンクコードを用いて情報連携基盤にアクセスすることとすべきではないか。

３．付番と番号管理について

（１）「番号」とＩＤコード・リンクコードの付番のあり方

前述の最高裁判決で指摘された個人情報の一元管理を避け、「番号」を含めた「見える」利用番号から情報連携に用いるＩＤコードに直接アクセスできないようにするという観点から、住民票コードから「番号」を生成する方式と、住民票コードからＩＤコード、さらにリンクコードを生成する方式は別の方式とし、「番号」から論理的にＩＤコードに遡れないようなものとすべきではないか。

（２）ＩＤコード及びリンクコードの生成方法

異なる情報保有機関同士の情報連携を図るためには、それぞれの情報保有機関ごとに付与されたリンクコードからＩＤコードに遡ることができ、また、ＩＤコードからリンクコードに遡ることができることとする必要がある。このためには、住民票コードからＩＤコード、さらに、ＩＤコードからリンクコードを生成する方法は、可逆暗号方式（その都度可逆暗号によってリンクコードからＩＤコード、又はＩＤコードからリンクコードを生成する）又はコード変換テーブル方式（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）が考えられる。コード変換テーブル方

式は、同一の機関において住民票コードとＩＤコードのリストの一元管理を行う必要があり、その場合、万一漏洩した際の影響範囲が広くなる可能性があることから、可逆暗号方式を採用すべきではないか。

（３）「番号」の生成方法

３．（１）で述べた観点から、住民票コードから見える「番号」を生成させる方法は３．（２）とは異なる方法とすべきであり、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「コード変換テーブル方式」を採用することが適切ではないか。その際、変換前後のテーブルは、「番号」の付番機関のみにおいて保持し、二重付番の回避、住民票コードの変更時への対応等に活用してはどうか。

（４）「番号」とＩＤコード・リンクコードの管理のあり方

情報の分散管理により、漏洩時の波及リスクを最小化する観点から、「番号」とＩＤコードは、できる限り分離して管理することが望ましいのではないか。また、情報連携基盤においては、ＩＤコードのみを保有することとし、リンクコードは情報連携ごとに可逆暗号で生成して、連携終了後直ちに消去することとすべきではないか。

（５）「番号」とＩＤコード・リンクコードの個人への通知の必要性

「番号」については、個人が行政機関等の窓口や申告書への記入等の方法により使用されるものであるため、「番号」が付番される各個人に対して安全な方法で通知されることが必要である。

一方、ＩＤコードについては、情報連携基盤においてのみ保有することとし、リンクコードについては情報保有機関においてのみ保有することとするが、セキュリティを確保するため、各個人に対しても通知されないこととすべきではないか。

（６）「番号」とＩＤコード・リンクコードの変更可能性

住民票コードについて個人による変更請求が認められており、かつ、「番号」については個人にも通知され、見える番号として様々な手続に用いられるものであることから、その安全性を確保する観点から、「番号」については個人からの変更請求を認めることを検討すべきではないか。

一方、ＩＤコード・リンクコードについては、個人に通知されるものではないため、変更請求は想定されない。しかしながら、万一の場合を想定し、システム上・運用上の負荷を勘案した上で、セキュリティの観点からの変更

可能性について検討すべきではないか。

（７）分野別に考慮すべき事項とリンクコードの付与単位について

リンクコードについては、通常は、各地方公共団体を含め、情報保有機関ごとに付与されるものと考えるべきではないか。

ただし、制度上情報の共有が想定されており、現に書面又は電子的手法を通じて情報共有がなされている場合（例：地方税法第４５条の３では、前年分の所得税について所得税法上の確定申告書を提出した場合には、原則として地方税法上の申告書が提出されたものとみなす仕組みを採用）には、情報連携基盤を通じた情報連携とは異なる取扱いを行うことも検討すべきではないか。

また、年金、医療、福祉、介護、労働保険の各社会保障分野については、基本方針において、本ワーキング・グループ及び個人情報ワーキング・グループによる検討経過を踏まえ、社会保障分野における具体的な措置について検討するサブ・ワーキング・グループにおいて検討が進められることとされている。

その際には、特に各社会保障分野においては、よりセンシティブな個人情報が含まれていることや医療機関や薬局等情報保有機関が極めて多数に上る分野が存在すること等に鑑み、分野内の情報のやりとりについては、例えばサブシステムを設けて分担させ、当該分野を超えて情報連携を行う場合には当該サブシステムを経由して情報連携基盤に照会を行う仕組みにするなど、その特性に応じた仕組みを検討することが考えられるのではないか。

したがって、各社会保障分野におけるリンクコードの付与に当たっては、個別の情報保有機関ごとに付与すること以外の選択肢についても検討を行うことが考えられるのではないか。

４．番号連携について

（１）番号連携の前提としての紐付けの必要性

リンクコードと「番号」及びその他の利用番号（以下「「番号」等」という。）は、セキュリティの観点から論理的関連性を持たないものとなる。これを前提として、２．及び３．で述べたＩＤコード・リンクコードによる情報連携を可能とするためには、情報連携基盤により各情報保有機関に対して割り振られたリンクコードが、当該情報保有機関の持つ個人情報データベース（対象者についての「番号」等と属性情報等から構成されたデータベース）に紐付けられることが必要となる。

これによって、各情報保有機関の持つ属性情報が、リンクコード・ＩＤコ

ードを通じて他の情報保有機関の持つ属性情報と連携されることとなる。

（２）４情報の突合の必要性

リンクコードが情報保有機関の個人情報データベースに紐付けられるためには、情報保有機関が保有する利用番号の属性情報として管理される４情報と、リンクコード・ＩＤコードの基礎となっている住民票コードに係る住基ネットの保有する最新の４情報とを突合することが必要である。

そのためには、情報保有機関の責任で、情報保有機関の保有する４情報を最新のものとすることが不可欠であり、このために、住基ネットを活用できるようにすることが求められるのではないか。

（３）リンクコードと「番号」等との対照テーブル

紐付けをした後のリンクコードと「番号」等は、４．（２）により４情報の突合をすることにより、各情報保有機関においてその対照テーブルを保持すべきではないか。

（４）番号連携の流れ

３．（２）によりＩＤコード・リンクコード間が可逆的に変換可能となり、かつ、４．（１）～（３）によって、各情報保有機関においてリンクコードと「番号」等とが紐付けられることにより、「(照会元情報保有機関の)「番号」等－（照会元情報保有機関の）リンクコード－ＩＤコード－（照会先情報保有機関の）リンクコード－（照会先情報保有機関の)「番号」等」の順序で全ての「番号」等が紐付けられ、「番号」等間の連携が可能となる。

５．情報連携について

（１）法令に基づく情報連携を行う情報保有機関と情報連携対象個人情報の特定

基本方針においては、「当面の情報連携の範囲は、年金、医療、福祉、介護、労働保険の各社会保障分野と国税・地方税の各税務分野とする」とされているが、１．（２）に述べた観点から、予め法律又はこれに基づく政令によって、情報連携を行う目的、情報連携を行う情報保有機関及び情報連携の対象となる個人情報の種類及び情報連携のパターンについて、明確に定めておくべきではないか。

（２）情報連携基盤における情報連携の承認

５．（１）により定められた情報保有機関及び情報連携対象個人情報のリス

トの中に、照会元情報保有機関による情報連携の照会が含まれることが情報連携の条件となるが、その条件が満たされているかどうかについては、情報連携基盤が、照会に対してその都度承認を行うこととし、その上で「(照会元情報保有機関の）リンクコードーＩＤコードー（照会先情報保有機関の）リンクコード」という情報連携基盤内の手順を進めることとすべきではないか。

（３）情報連携の際の適切なアクセス制御

照会元情報保有機関、照会先情報保有機関においては、各機関におけるシステム改修の負担等も考慮しつつ、情報連携に関連する業務に携わることができる職員を予め限定し、関係する端末やデータベースへのアクセスを適切な方法により制御することにより、不正アクセスや情報漏洩を防止するとともに、事後的な当該機関内又は第三者機関等による監査の対象とすることを検討すべきではないか。

（４）情報連携の手順

① まず、照会元の情報保有機関において、４.（３）の対照テーブルを活用し、情報連携を行う対象者についてのリンクコードを用いて、入手しようとしている情報連携対象個人情報及び照会先の情報保有機関を原則として指定して、情報連携基盤に問い合わせることによって、手続が開始することとすべきではないか。

このため、照会元情報保有機関においては、情報連携を行う際に、対象者に係る４情報を、予め住基ネットの持つ最新の４情報に更新する等の方法により、可能な限り照会先情報保有機関（例えば現住所がある地方公共団体）を予め知っておくこととすべきではないか。その手法としては、４.（２）の方法に準じて、住基ネットと各情報保有機関との間で行うこととすべきではないか。

なお、将来的に、日本年金機構や全国健康保険協会等住基ネットから４情報を直接提供することが可能とされているような団体以外の民間の情報保有機関が情報連携を行うことになった場合には、民間の機関の側で情報連携について本人の同意を得て本人から入手した４情報を用いて、情報連携基盤を通じて照会し、住基ネット側の４情報と合致した場合のみにリンクコードを付番するといった仕組みを検討すべきではないか。

② 続いて、情報連携基盤においては、５.（２）に述べたように、当該照会に係る情報連携の内容が、予め法令によって特定されたリストに含まれていることを確認し、確認できた場合には、これを承認の上、「(照会元情報保有機関の）リンクコードーＩＤコードー（照会先情報保有機関の）リン

クコード」という手順を経て、照会先情報保有機関に対してそのリンクコードとともに情報連携対象個人情報の種類を伝達することとすべきではないか。

③　その後、情報連携基盤より伝達を受けた照会先情報保有機関においては、当該リンクコードに係る個人の情報連携対象個人情報を付して、情報連携基盤を通じて照会元情報保有機関に対して、回答すべきではないか。

その際、６．で述べるように、いつ、誰が、どの情報に関して、何の目的のために情報連携を行ったかといった事項に関する履歴（以下「アクセスログ」という。）を保存し、対象者である個人及び第三者機関等が事後的に閲覧できるようにすべきである。

しかしながら、情報の集中管理とならないようにするため、情報連携対象個人情報そのものについては、情報連携基盤を通じて回答がされることにとどめ、情報連携基盤においては保存されないようにすべきではないか。

６．アクセスログの保存及び提供

（１）アクセスログの種類と使用目的に応じた検討のあり方

想定されるアクセスログの種類としては、例えば、①管理用のシリアル番号、②情報連携の照会等のアクセスを行った日時、③情報連携の根拠（法令等で予め定められた情報連携のパターン）、④照会元情報保有機関の名称、⑤照会先情報保有機関の名称、⑥情報連携対象個人情報の種類、⑦照会元情報保有機関で端末を操作した担当職員名（又は担当部署や職員名に代わる属性情報）、⑧照会先情報保有機関で端末を操作した担当職員名（又は担当部署や職員名に代わる属性情報）、⑨照会元情報保有機関において使用された端末、⑩照会先情報保有機関において使用された端末、⑪提供された情報連携対象個人情報の内容、⑫情報連携対象個人情報の用途などが考えられるが、情報の分散管理及び費用対効果の観点を踏まえつつ、アクセスログの使用目的に応じて、その保管及び提供のあり方を検討すべきではないか。

その際、大きく分けて、個人がマイポータル等を通じて事後的に閲覧するアクセスログの範囲と第三者機関が不正アクセス・情報漏洩等を検知するために閲覧・分析を行うアクセスログの範囲とでは、後者の方がより詳細かつ広範囲なものとして設定すべきではないか。

（２）アクセスログの保存に係る役割分担

アクセスログもその多くが個人情報であり分散管理すべきものであることから、全てを情報連携基盤で保存するのではなく、できる限り情報保有機関側で保存すべきものは保存するように工夫すべきではないか。

そこで、例えば、６．（１）に示したリストの中では、５．（４）③の考え方も踏まえ、①～⑥までは情報連携基盤で、⑦・⑨・⑪・⑫については照会元情報保有機関で、⑧・⑩・⑪については照会先情報保有機関で保存をすることが考えられるのではないか。

（３）アクセスログの保存期間

アクセスログの保存期間の検討に当たっては、その使用目的との関連で、必要最小限とし、かつ費用面で過度な負担を生じることがないよう配慮すべきではないか。

その際、不正アクセスや情報漏洩によって犯罪を構成する可能性に鑑み、刑法第２４６条の２（電子計算機使用詐欺）等の公訴時効が刑事訴訟法第２５０条により７年と規定されていることとの関係を検討すべきではないか。

（４）個人によるマイポータル等を通じたアクセスログの閲覧

情報連携の対象者である個人によるアクセスログの閲覧の仕組みの検討に当たっては、マイポータルはインターネットから接続されるものであることに鑑み、閲覧を求める個人からの申請があった場合にのみ、その申請内容に応じて、アクセスログを保存する機関から提供されることとすべきではないか。

その際、マイポータルにおいて直接閲覧できるアクセスログは、原則として情報連携基盤が保存するものに限ることとし、情報保有機関において保存すべきアクセスログのうち、例えば６．（１）の⑪・⑫については、別途各情報保有機関に対して申請する手続を設け、当該手続を経た後にマイポータルにおいて閲覧するといった方策を検討すべきではないか。

同時に、パソコンや行政キオスク端末等を使用することが困難な個人に対してもアクセスログの閲覧を可能にするため、例外的措置として、行政機関の窓口による対応等も可能とすることを検討すべきではないか。

（５）第三者機関によるアクセスログの閲覧・分析

第三者機関の役割は、個人情報保護ワーキング・グループにおいて検討されているところであるが、情報連携に関しては、アクセスログの閲覧・分析等により、情報連携基盤及び情報保有機関の情報連携に係る個人情報の取扱いを監視・調査する権限等を有することが想定される。

したがって、６．（１）の考え方を踏まえ、第三者機関は、情報連携基盤において保存するアクセスログのみならず、情報保有機関において保存するアクセスログについても、原則として全て閲覧・分析ができるように検討すべ

きではないか。

７．情報保有機関の機能と既存システム・情報連携基盤間のインターフェイス

（１）情報保有機関において備えるべき機能

情報保有機関においては、照会元情報保有機関及び照会先情報保有機関としての機能、例えば、情報連携に必要なアクセス制御、アクセスログのうち情報保有機関において保存すべき情報の保存、照会を受けた際に情報連携対象個人情報を特定して一定期間内に回答する機能等を持つことが考えられる。

（２）既存システムと情報連携基盤をつなぐインターフェイスの確保

情報連携に関わる業務分野について、各情報保有機関が持つ既存システムには様々な種類があり、これらを直接７．（１）に例示したような機能を持つように改修することは、費用を可能な限り抑制する観点から必ずしも適切ではないのではないか。

そこで、住基ネットにおいて用いられているコミュニケーション・サーバー方式などを参考に、既存システムの差異を吸収するインターフェイスの確保方法について、個別の既存システムの状況を踏まえた検討が必要ではないか。

８．情報連携基盤・情報保有機関間等の回線

情報連携の仕組みの構築に当たっては、情報連携基盤と各情報保有機関間等を結ぶ回線についても検討が必要である。

その際には、できる限り既存のシステムを有効利用するという観点から、情報連携基盤と各情報保有機関を結ぶ回線については、原則として国の各行政機関間において用いられている霞ヶ関ＷＡＮ並びに各地方公共団体間及び各地方公共団体と国の行政機関との間で用いられている総合行政ネットワーク（ＬＧＷＡＮ）を改良することにより対応することを検討すべきではないか。

第２　個人認証とマイポータル・ＩＣカード等の活用

第３　法人に対する付番

第４　その他