Vol.2013-CSEC-61 No.29
Vol.2013-IOT-21 No.29
2013/5/10

国家による個人識別番号とその利用システムのあり方 ～ プライバシーの観点から ～

高木 浩光[1,a)]　山口 利恵[1,b)]　渡辺 創[1,c)]

概要：日本政府は、「社会保障と税の番号制度」[1] の創設を進めており、法整備に続いて、番号連携機能を備えた「情報連携基盤」の構築を計画している。本稿執筆時点で「情報連携基盤」の技術設計は案が公表されているものの未決定の段階であり、設計案に対しては「符号の存在意義が不明確」といった指摘もある。本稿では、「情報連携基盤」の番号連携機能の技術方式について再検討し、従来方式より合理的な設計の別案を提案し、プライバシー保護と情報セキュリティ技術の観点から従来方式と比較検討する。

キーワード：個人識別番号, 社会保障と税の番号制度, プライバシー, 電子政府

Toward the better design of a national identification number and its utilization system — from the viewpoint of privacy —

Abstract: Japanese government is developing "Identification Number System for Social Security and Taxation"[2] now. Following its ongoing legislation, building an information linkage system, which can correlate this number with other national identification numbers, is planned. The design of the system has not been fixed yet at this moment, but its draft is in public. It is pointed out that the significance of the code named "link code" in the draft is unclear. In this paper, we revisit the design of information linkage system, particularly how to link one number with another number, and propose a alternative solution. Finally we compare our solution with that in the draft from the viewpoint of security and privacy, and show that the proposed one is more reasonable than that in the draft.

Keywords: National identification number, Identification Number System for Social Security and Taxation, Privacy, e-Government

1. はじめに

日本政府は、社会保障と税の番号制度（以下、番号制度という。）の創設を進めており、平成 25 年 3 月、「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案」[3]（以下、法案という。）を国会に提出し、本稿執筆時点では、衆議院内閣委員会が法案について審議を進めている段階にある。

法案は、「個人番号」、「特定個人情報の保護」、「特定個人情報保護委員会」等について規定するが、平成 23 年 6 月の「社会保障・税番号大綱」[4]（以下、大綱という。）で記述されていた「情報連携基盤」[*1]については、特定個人情報の提供と、提供があった場合の記録、 秘密の管理について規定しているものの、大綱で記述されていた「符号」（以下、リンクコード[*2]という。）及びリンクコードを用いた情報連携の仕組みについては何ら規定していない。

情報連携基盤のリンクコード周辺の技術設計は、本稿執筆時点では、 平成 23 年 7 月の情報連携基盤技術ワーキン

[1] 産業技術総合研究所
AIST, 1-1-1 Umezono, Tsukuba, Ibaraki, 305-8568 Japan
[a)] takagi.hiromitsu@aist.go.jp
[b)] rie-shigetomi@aist.go.jp
[c)] h-watanabe@aist.go.jp

[*1] 法案では「情報提供ネットワークシステム」の語で規定されているが、本稿では、大綱の「情報連携基盤」の語を用いる。

[*2] 大綱では単に「符号」と表記されているが、ここでは、一般語としての符号との混同を避けるため、平成 23 年 3 月の情報連携基盤技術ワーキング・グループ資料「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）」[5] において同じものを指す語として用いられていた「リンクコード」の語を用いる。

グ・グループ（以下、WG という。）「中間とりまとめ」（以下、中間とりまとめという。）で示された「番号連携方式検討表」[6] に掲載の案 1 から案 5 が最新の検討案であり、平成 23 年 11 月の「社会保障・税番号大綱に対する取りまとめ」[7] において「システム設計及び費用精査の必要性」があるとされたまま、未決定の状況にある。情報連携基盤の技術設計については、平成 24 年 3 月に経済同友会が「次世代へ誇れる番号制度システムの実現を」と題した提言 [8] で「情報連携基盤や符号の存在理由が不明確」と指摘している。

本稿は、このような状況に鑑み、プライバシー保護と情報セキュリティ技術の観点から、リンクコードの意義について再検討し、法案の趣旨に照らして、従来方式より合理的な情報連携基盤の技術設計を提案するものである。

以下、番号制度におけるプライバシー保護の解決手段について考え方を整理した後、情報連携基盤における連携方式の別案を示し、プライバシー保護と情報セキュリティ技術の観点から従来方式と比較検討する。

2. 番号制度におけるプライバシー保護の解決手段

大綱は、「安心できる番号制度の構築」のため、個人番号の保護の必要性、特定個人情報の保護の必要性、住民基本台帳ネットワークシステム最高裁判決との関係を踏まえることの必要性を示し、「番号制度に対し国民の間に生じるのではないかと考え得る懸念」として、(1) 国家管理への懸念、(2) 個人情報の追跡・突合に対する懸念、(3) 財産その他の被害への懸念の 3 点を挙げ、それぞれに対する制度上の保護措置とシステム上の安全措置を講ずるとしている。これらはいずれも、国民のプライバシーを保護するためにも必要な措置といえる。本稿では、これら 3 点の懸念に対して番号制度がどのように問題解決を図っているかについて、以下のように整理する。

2.1 「国家管理への懸念」への対応

2.1.1 一元管理主体不存在要件と法令による保護

大綱は、「最高裁判決との関係」として、「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」（以下、一元管理主体不存在という。）を要件として挙げている。これは、最高裁判決が、「住基ネットの運用によって原審がいうような具体的な危険が生じているということはできない」と判断する理由として、「秘密に属する個人情報を保有する行政機関の職員等が、正当な理由なくこれを他の行政機関等に提供してデータマッチングを可能にするような行為も刑罰をもって禁止されていること」を挙げつつ、続けて、「（中略）行政事務において取り扱われる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は存在しないことなどにも照らせば」との理由も挙げたことによるものと考えられる。

一元管理主体不存在の要件を満たすため、大綱は、まず、「情報連携の対象となる個人情報につき情報保有機関のデータベースによる分散管理」とするとして、個人情報を保管する主体は基本的には従来通りとした上で、情報保有機関の間で情報の連携を行うことについては、「情報連携基盤を用いることができる事務の種類、提供される個人情報の種類及び提供元・提供先等を逐一法律又は法律の授権に基づく政省令に明示することで番号制度の利用範囲・目的を特定する」とし、かつ、「行政機関の職員等による不正利用、不正収集等を処罰する罰則を設ける」としている。これらにより、法令違反がない前提の下では、一元管理主体不存在の要件は満たされることになる。

2.1.2 情報連携基盤を利用した不正行為の防止

次に、法令違反が生じ得ることを前提として、情報連携基盤が提供する機能によって一元管理が可能な機関又は主体が生じないことが求められる。この点について、中間とりまとめは、「情報連携を実現するに当たり、情報連携基盤では、認められた手続きのみが情報連携基盤にアクセスすることを可能にする」として、情報保有機関での法令違反行為による不正な情報連携は、情報連携基盤のアクセス認可制御の機能によって防止するとしている。

続いて、情報連携基盤内部での法令違反行為が問題となり得る。この点については、大綱にも中間とりまとめにも明確な記載はないが、中間とりまとめの「データ送信方式検討表」[9] に、「案 1（ゲートウェイ方式）」の「プライバシー影響度」の検討として、「情報連携に係る個人情報が一時的に情報連携基盤に溜まるため、個人情報が集約しうるとの指摘がある」との記載があるように、情報連携に際して受け渡しされる個人情報が情報連携基盤で取得可能な設計とするのは、一元管理主体不存在の要件を満たさないのではないかと懸念されている。

これについて、「データ送信方式検討表」は、「案 2（アクセストークン方式）」を検討しており、この案では、情報連携基盤は、情報連携に際して、情報保有機関へのアクセスの許可を与えるだけで、個人情報自体（個人情報の属性情報）は取り扱わない構成となっている。この案が採用されて、情報連携基盤からの不正なアクセス要求に情報保有機関が情報提供をしてしまうことがない技術設計がなされれば、情報連携基盤で法令違反行為があることを前提としても、情報連携基盤が一元管理主体となることはないといえる。

2.1.3 データマッチングの想定と防止手段

しかし、これらだけでは一元管理主体不存在の要件が満たされないとする指摘がある。日本弁護士連合会は、平成 23 年 7 月に公表した「「社会保障・税番号大綱」に関する意見書」[10] で、「情報保有機関同士が、（情報連携基盤を通さずに）直接に「共通番号」を用いて情報のやりとりを行

うことが極めて容易であり、まったく「システム上の安全措置」たり得ていない」と指摘する。情報連携基盤を通さずに直接にデータマッチングする行為（以下、データマッチングという。）は、法案により刑罰をもって禁止されるが、法令違反を前提にそれが可能である限り、一元管理主体不存在の要件を満たさないとの指摘である。

データマッチングが容易となるのは、情報保有機関が個人情報を保有するに際して、他の情報保有機関と共通で用いることのできる個人番号に紐付けて個人情報を保有することによるものである。番号制度の導入によるデータマッチングリスクの増大を回避するには、情報保有機関ごとに異なる番号を用いることとし、情報保有機関の間で共通に用いることのできる番号を利用しないこととする方策が考えられる。大綱においても「諸外国の制度」として、「国家による一元管理を回避するため情報技術を駆使したセクトラルモデルを採用するオーストリア」との記述があるように、オーストリアの分野別符号を用いる方式がそれに該当するとされている。

この点について、中間とりまとめでの情報連携基盤の設計案では、「番号連携方式検討表」[6] の案 2 及び案 3 で、情報保有機関ごとに独立のリンクコードを付与し、これを用いて情報連携を行うとしており、同表の「セキュリティ・プライバシー影響度」には、「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。」との記述がある。同一人に対応するリンクコードは情報保有機関ごとに異なる値であることから、リンクコードがデータマッチングを容易にすることはないというわけである。

しかし、実際には、この案 2 及び案 3 において、各情報保有機関は、個人番号を共通の番号として個人情報に紐付けて保有する[*3]のであるから、そのような情報保有機関の間に関しては、データマッチングのリスクは番号制度の導入によって増大することになる。

このリスクの増分をゼロとするには、各情報保有機関が個人番号を保有しないようにするか、情報保有機関ごとに別の個人番号を用意するしかない。しかし、法案が規定する個人番号は、税務当局に提出する申告書や法定調書に記載して用いることになっているように、大綱がいうところの「「民―民―官」で広く利用される「見える番号」」であることから、各情報保有機関が個人番号を保有しないこととするのは非現実的であるし、そのような用途の個人番号は情報保有機関の間で共通に利用する番号とせざるを得ない。

2.1.4 個人番号の利用範囲の制限

このように、中間とりまとめで示されたリンクコードを用いた情報連携基盤（案 2 又は案 3）をもってしても、データマッチングのリスクの増分はゼロにはできていない。ただし、データマッチングのリスクがいくらか増大したとしても、そのことが直ちに一元管理主体不存在の要件を満たさなくなるわけではないと考えられる。法案では、個人番号を利用する行政事務を法案別表第 1 に示された範囲に限定しており、十分に狭い範囲の行政事務にしか共通の個人番号を用いないようにしていれば、データマッチングのリスクは限定的であって一元管理主体不存在の要件を阻害しないという考え方も可能であろう。

法案が規定する個人番号の利用範囲が、一元管理主体不存在の要件にとって、十分に限定的であるといえるかについては、本稿の検討範囲を超えるため示す立場にないが、少なくとも、大綱では、社会保障と税の幅広い分野で用いるものとされ、例えば「診療情報等の二次利用を行えば、医療統計データの効率的な収集が可能となり、医学の向上にも資することとなる。」といった記述があったのに比べれば、法案では、個人番号の利用範囲を金銭情報に限定しており、身体情報（大綱で書かれていた診療内容の情報がこれに当たる）を含めていない[*4]という点では、利用範囲はある程度狭く規定されたといえる。

2.1.5 小括

以上をまとめると、番号制度は、国家管理への懸念への対応として一元管理主体不存在の要件を掲げ、これを満たすために、(1) 個人情報を情報保有機関のデータベースによる分散管理とすること、(2) 番号制度の利用範囲・目的を法律又は政省令に明示すること、(3) 不正利用、不正収集等を処罰する罰則を設けること、(4) 政省令に基づかない情報連携は情報連携基盤を通じてではできないようにすること、(5) 情報連携基盤は個人情報自体（個人情報の属性情報）を扱わないようにすること、(6) 個人番号の利用範囲を狭く限定することの、6 つの点によって解決しようとしているといえる。

2.2 「個人情報の追跡・突合に対する懸念」への対応

2.2.1 民間事業者等による追跡・突合の可能性

大綱は、番号制度の創設に伴って生じ得る「国民のプライバシーの侵害」の例として、「様々な個人情報が、本人の意思による取捨選択と無関係に名寄せされ、結合される」可能性を挙げ、「個人情報の追跡・突合に対する懸念」として、「集積・集約された個人情報が外部に漏えいするのではないかといった懸念」と、「集積・集約された個人

[*3] 中間とりまとめの「番号連携方式検討表」は、案 2 及び案 3 の「連携概要」の図において、情報保有機関が持つデータとして「リンクコード」と「属性情報」の記載はあるものの、個人番号が保有されていることについてなぜか書かれていない。中間とりまとめの「番号制度における符号連携のイメージ」[11] の図ではそこに「「番号」」と記載されているように、実際にはそれらの情報保有機関は個人番号を保有する。

[*4] 平成 25 年 4 月 3 日の衆議院内閣委員会で、政府参考人は、「今回の番号法案では、医療の身体情報につきましては対象の範囲となっておりませんが、医療の身体情報などについて、仮に似たような番号制度を作るとすれば、別の番号を使うことも考えられます。」と述べている。

情報によって、本人が意図しない形の個人像が構築されたり、特定の個人が選別されて差別的に取り扱われたりするのではないかといった懸念」を示している。この懸念のうち、国家によりなされ得るものについては、前節「国家管理の懸念への対応」で示した解決が図られているが、それ以外の主体によるもの、すなわち、地方公共団体や民間事業者、さらには個人によってなされ得るものに対応する必要がある。

集積・集約の懸念の対象となる個人情報は、番号制度で実現する行政事務に用いる個人情報に限られない。例えば、民間事業者が、顧客の購買履歴を個人番号に紐付けて集積・集約するといった場合もこの懸念に含まれる[*5]。

民間事業者が購買履歴を集積・集約することは、番号制度のない現在でも既に何らかの方法で可能であるが、番号制度の創設によって、精度の高い集約が可能になると考えられる。これは、番号制度で附番される個人番号が「唯一無二性」（一人に二つ以上の番号が附番されることがない性質）を有していることによるものである。例えば、もし仮に、民間事業者が消費者との取引において個人番号の提供を求めることが許され、そのような取引形態が常態化した場合を想定すると、従来であれば、複数のクレジットカードや、複数の住所表記、電話番号等を使い分ける方法によって、購買履歴が集約される可能性を回避できたのに対し、番号制度の個人番号が利用されるとなれば、一つの個人番号で集約されることから逃れられなくなってしまう。

また、購買履歴などの属性情報を含まずとも、個人番号単体の利用であっても、集積・集約の懸念の対象となる。例えば、民間事業者が、サービスを提供するに際して、都合の悪い客を恣意的に閉め出す目的で、個人番号の提示を求めてブラックリストを作成するといった場合がこの懸念に含まれる[*6]。

ブラックリストの実現は、番号制度のない現在では、運転免許証番号を用いるなどの方法が考えられるところ、すべての人が運転免許証を所持しているとは限らないことから、所持しない人へもサービスを提供する場合には実現できない。しかし、番号制度の個人番号を利用できるとなると、個人番号の「悉皆性」（国民などすべての人に個人番号が附番されるという性質）から、そのようなブラックリスト運用が現実に可能となってしまう。

これらの懸念に対応するため、法案は、以下に示すように、特定個人情報の目的外利用を禁止するとともに、個人番号単体であっても特定個人情報として扱うよう規定している。

2.2.2 特定個人情報の目的外利用の禁止

法案は、「特定個人情報」、「特定個人情報ファイル」、「個人番号利用事務」を定義した上で、「個人番号利用事務等を処理するために必要な範囲を超えて特定個人情報ファイルを作成してはならない」（第 28 条）、「何人も、次の各号のいずれかに該当する場合を除き、特定個人情報の提供をしてはならない」（第 19 条）、「何人も、前条各号のいずれかに該当する場合を除き、特定個人情報（中略）を収集し、又は保管してはならない」（第 20 条）と規定して、 個人番号利用事務以外の目的で（法案に規定された例外を除き）特定個人情報を利用すること等を禁止している。

これらには罰則も規定されている。特定個人情報の提供には直罰規定があり、「個人番号利用事務等又は（中略）に従事する者又は従事していた者が、正当な理由がないのに、その業務に関して取り扱った個人の秘密に属する事項が記載された特定個人情報ファイル（中略）を提供したときは、四年以下の懲役若しくは二百万円以下の罰金に処し、又はこれを併科する。」（第 67 条）としている。これに該当しない場合でも、第 19 条（特定個人情報の提供の制限）、第 20 条（収集等の制限）、第 28 条（特定個人情報ファイルの作成の制限）の規定に違反する行為があった場合は、特定個人情報保護委員会が、違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告、命令できる（第 51 条）としており、その命令に違反した者は「二年以下の懲役又は五十万円以下の罰金に処する。」（第 73 条）として、間接罰の構成になっている。

ここで禁止の対象となる「特定個人情報」や「特定個人情報ファイル」は、いずれも「個人番号をその内容に含むものをいう」として規定されている（第 2 条第 8 項及び第 9 項）ので、禁止の対象となるのは、個人番号利用事務に用いる個人情報に限られず、民間事業者における購買履歴など、個人に関する情報を個人番号に紐付けた情報のすべてがこれに該当する。

したがって、個人番号利用事務に用いるもの以外のあらゆる個人に関する情報は、個人番号と紐付けて個人情報ファイル（個人情報データベース）を作成したり、個人番号と紐付けて提供したり、個人番号と紐付けて収集、保管することが禁止される。

2.2.3 個人番号の目的外利用の禁止

個人情報の保護に関する法律においては、番号や符号が単体で個人情報に該当するかは、「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるもの」（同法第 2 条第 1 項）に当たることが要件とされ、番号や符号の置かれた状況によって該当性は変わるものであったが、法案では、法律名が「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」であることから明らかなように、番号自体が特定の個人を識別するものであることから、個人番号単体であっても特定個人情報に該当する[*7]。

[*5] 大綱のいう「本人が意図しない形の個人像が構築されたり」に該当するであろう。
[*6] 大綱のいう「特定の個人が選別されて差別的に取り扱われたり」に該当するであろう。
[*7] 法案は、特定個人情報を「個人番号（中略）をその内容に含む個人情報」と定義している。

したがって、前記のブラックリストへの利用は、特定個人情報ファイルを作成することに他ならず、法案によって禁止される行為となる。また、仮にブラックリストが作成されたとしても、それを提供したり、収集、保管する行為も禁止される。

加えて、法案は、「何人も、（中略）場合を除き、他人（中略）に対し、個人番号の提供を求めてはならない。」（第 15 条）との規定も置いており、特定個人情報ファイルが作成される前の段階でそれを防止している。

2.3 「財産その他の被害への懸念」への対応

2.3.1 個人番号を用いた成りすましの危険性

大綱は、「財産その他の被害への懸念」として「『番号』や個人情報の不正使用又は改ざん等により財産その他の被害を負うのではないかといった懸念」を示し、具体的に、「本人の申告による『番号』のみで本人確認が行われていたアメリカや韓国等でも成りすまし等の不正な利用が社会問題化している。」との例を挙げて、「このような諸外国の状況を踏まえると、『番号』を取り扱う機関において、本人であることの証明手段がないまま、『番号』のみで本人確認が行われれば、成りすましの温床となり、制度そのものの根幹を揺るがしかねない」と記している。

番号制度の個人番号に限らず、一般に、何らかの番号が本人確認手段になると誤解する例は、まだ番号制度のない日本でも既に散見される。近年、公共交通機関の IC カードや、コンビニエンスストア等のポイントカードが広く普及し、インターネットを介したサービス提供が一般的となったことで、カードに記載の番号を Web サイトに入力させることをもって本人確認とする（生年月日や電話番号の入力が併用される場合もある）サービスが現れるようになった。それらの番号を秘密に保つようにしなければ他人に当該サービスを利用されかねないという状況が見られる。こうしたサービスがさらに広がり、他人になりすます者の利益が増大すれば、他人の番号を収集、提供する行為が横行するようになりかねない。

番号制度の導入は、国民等のすべての人に個人番号を附番するものであるから、個人番号で本人確認ができるとの誤解はさらに広がることが懸念される。個人番号の目的外利用が法案によって禁止されることから、個人番号利用事務以外の場面でそうした不適切な本人確認が行われるようになる事態は防止されるが、個人番号利用事務において個人番号が本人確認に用いられてしまう懸念が残る。

そのような個人番号の使われ方が広まれば、成りすましの温床となって、個人番号の不正な取得や流通が横行するようになり、社会不安を招くことになる。番号制度の創設が社会不安をもたらすという事態を回避するためには、これを防止する必要がある。

2.3.2 法案による成りすましの防止

法案は、第 16 条で、「個人番号利用事務等実施者は、第十四条第一項の規定により本人から個人番号の提供を受けるときは、当該提供をする者から個人番号カード若しくは通知カード及び当該通知カードに記載された事項がその者に係るものであることを証するものとして主務省令で定める書類の提示を受けること又はこれらに代わるべきその者が本人であることを確認するための措置として政令で定める措置をとらなければならない。」と規定して、この懸念に対応している。

「主務省令で定める書類」及び「政令で定める措置」の内容は本稿執筆時点では明らかでないが、例えば、既存の事務のすべてにおいて従来通りの本人確認手段を用いることを政令で規定した場合、少なくとも、それらについて本人確認の確かさが従来より弱くなることにはならない。番号制度で新たに生じることとなる個人番号利用事務について、各事務の性質に照らして相応しい本人確認措置が規定されれば、番号制度の創設が成りすましの温床をもたらすという事態は回避されることになる。

3. 情報連携基盤における連携方式の別案

第 2 節で整理したように、番号制度は、「国家管理への懸念」と「個人情報の追跡・突合に対する懸念」を払拭するために、情報連携を情報連携基盤を通じて行うこととし、法案に禁止・罰則規定を設けることでそれを達成しようとしている。情報連携基盤の技術方式は、これらに対応できる設計としなければならないが、一方で、必要のない仕組みは可能な限り省いて合理的な設計とするべきでもある。これまでの検討案では、情報連携基盤のリンクコードを用いた方式に対して「存在理由が不明確」とする指摘もあり、再検討が必要であると考える。

3.1 これまでの検討案

中間とりまとめは、情報連携基盤の設計案として、「番号連携方式検討表」[6] の案 2 及び案 3（骨格案）で、情報保有機関ごとに独立のリンクコードを付与し、これを用いて情報連携を行うとしている。しかし、この設計案に対し、経済同友会の提言 [8] は、「国家による一元管理を回避するために（中略）「セクトラルモデル+情報連携基盤」の採用を予定している。一方で（中略）6 分野全てにおいて行政手続識別番号を利用するかは判然としないものの、仮に利用するのであれば、情報連携基盤や符号の存在理由が不明確となる。」と指摘している。

この指摘は、第 2.1.3 節で示したものと同じ指摘であり、リンクコードが、国家による一元管理を回避するためにセクトラルモデルを採用するもの（データマッチングを防止するもの）であるにしては、情報連携に参加する各情報保有機関が同一の個人番号を共通の番号として保有するので

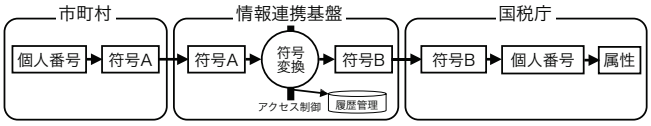

図 1 リンクコードを用いる情報連携基盤での情報連携の例

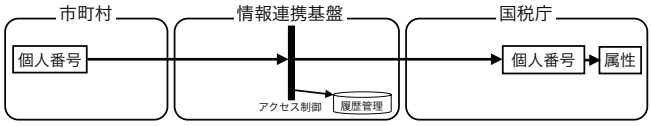

図 2 リンクコードを用いない情報連携基盤での情報連携の例

あるから、データマッチングを防止する機能を果たしておらず、このようなリンクコードには存在意義がないとする指摘であろう。

図 1 は、市町村と国税庁が情報連携をする場合を例に、リンクコード（図中では「符号」）がどのように用いられるかの具体例を示したものである。市町村は、ある個人に係る個人情報を国税庁に提供する際、当該個人の個人番号を「符号 A」に変換して情報連携基盤に送信し、情報連携基盤は当該市町村の「符号 A」を国税庁向けの「符号 B」に変換して国税庁に送信し、国税庁は受け取った「符号 B」を個人番号に変換して使用することになる。

このような、始点と終点が同じ個人番号であるにも関わらず中間で何度も符号変換を行う方式には、何の意義があるのか。この疑問は、平成 23 年 4 月の WG 第 4 回で、山口英委員が提出した質問書 [12] でも問われている。

WG で当初示された骨格案 [5] では、リンクコードを用いた符号変換方式の意義は、情報漏洩対策として想定された記述になっていた。質問書は、この点について、「政府基本方針は、情報連携基盤について（中略）個人情報保護に十分配慮した仕組みとするとしているが、その実現に際して、ID コードとリンクコードを用いた方式を採用する狙いは、はたして情報漏洩対策なのか。そうではないのではないか。」と指摘している。

この指摘に対応し、中間とりまとめには、リンクコードの意義について、「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。」との記述（データマッチングの防止）が盛り込まれたものの、先に述べたように、同じ個人番号を持つ情報保有機関同士の連携においては、そのような役割を果たしていない。

したがって、同じ個人番号を持つ情報保有機関においてはリンクコードは不要であると言うべきである。情報連携基盤からリンクコードを排除した場合、先の図 1 の例の市町村と国税庁の間の情報連携は、図 2 のようになる。市町村から個人番号が直接、情報連携基盤に送信され、それが直接、国税庁に送信される。このとき、情報連携基盤の担う役割は、情報連携の要求が法に定められた利用目的に合致するかのアクセス認可制御と、連携の履歴を記録し管理することにある。

なお、リンクコードを用いた方式が情報漏洩対策として意義を成すかについては、第 4 節で検討する。

3.2 提案する別案

以上の検討を踏まえ、情報連携基盤の連携方式の別案として、リンクコードを排除した合理的な方式を提案する。

まず、リンクコード用いた連携方式がデータマッチングの防止に効果がないのだとしても、リンクコードを排除して、すべての情報保有機関が同じ個人番号を用いて情報連携する方式とした場合には、第 2.1.3 節で検討したデータマッチングの懸念が解決されないことになり、一元管理主体不存在の要件を満たさず、「国家管理への懸念」が払拭されないことになりかねない。

この点については、第 2.1.4 節で述べたように、法案は、個人番号を利用する行政事務を法案別表第 1 に示された範囲に限定しており、これが十分に狭い範囲であると評価されるならば、一元管理主体不存在の要件は満たされ得る。これはリンクコードを排除した場合においてもである。

問題となるのは、法案は附則第 6 条で、「政府は、この法律の施行後三年を目途として、（中略）個人番号の利用及び情報提供ネットワークシステムを使用した特定個人情報の提供の範囲を拡大すること（中略）について検討を加え、（中略）所要の措置を講ずるものとする。」としており、法案別表第 1 に示された範囲以外にも利用が拡大される可能性がある点である。

そのような利用の拡大に際しては、法案の個人番号とは別の同種の番号を用いることが考えられる。具体的には、既に医療の分野について「医療等 ID」（医療番号）の創設が厚生労働省において検討されており [13]、これが個人番号と同種の性質を持つ番号となることが想定されるところ、法案の個人番号とは別の番号として附番する（脚註*4 参照）ことにより、一元管理主体不存在の要件を満たしたままの拡張が可能となる。

このような別の番号が附番される将来の拡張を想定して、情報連携基盤を今の段階から設計しておくことが重要と考えられる。そのような設計の案として、リンクコードを用いない方式を図 3 に示す。

図 3 の青の逆 L 字型の領域は、法案が規定する個人番号の利用範囲（法案別表第 1）[*8]を表している。社会保障の 5 分野と税の領域のうち「金銭情報」に当たる領域において法案の個人番号は利用される。社会保障の 5 分野には残された領域「身体情報」（図中赤の領域）があるが、これについて、個人番号とは別に附番された医療番号（厚生労働省報告書 [13] の「医療等 ID」）を用いることが考えられる。

これら個人番号と医療番号は必要に応じて情報連携する

[*8] 防災分野については記載していない。

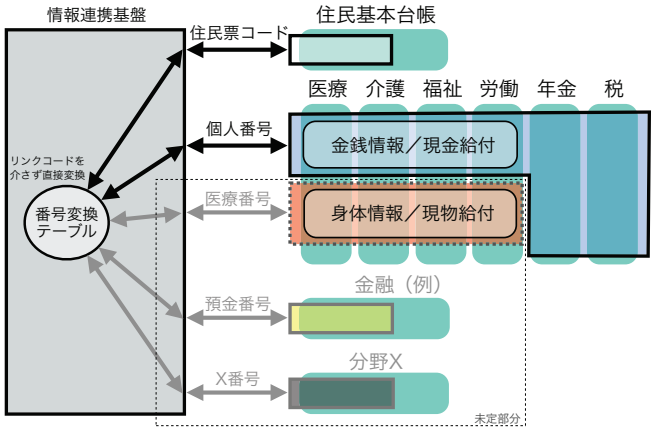

図 3 情報連携基盤における連携方式の別案

場面が想定されるところ、その際の両番号に対する同一個人の同定は、情報連携基盤内に設けられた「番号変換テーブル」によって可能である。

この番号変換テーブルは、個人番号を附番する際に住民票コードに対応付けて生成するために必要となる対照テーブル[*9]の機能を兼ねることができる。また、中間とりまとめでの情報連携基盤の設計案「番号連携方式検討表」[6] の案 2 及び案 3 で必要とされていた「ID コード」も不要となり、合理的である。

また、このように設計しておくことにより、将来、さらに別の分野向けの番号が必要になった場合にも、図 3 中の「預金番号」[*10]、「X 番号」のように、次々に加えて拡張することができる。法改正によって個人番号の利用範囲（法案別表第 1）を広げるのではなく、このように別番号を附番して情報連携基盤を通じて拡張する方法を採用することで、「国家管理への懸念」を払拭したままの拡張が可能となる。

4. リンクコード方式のセキュリティ上の意義

第 3 節では情報連携基盤からリンクコードを排除する設計案を示したが、WG で当初示された骨格案 [5] では、リンクコードの意義は情報漏洩対策として想定されたものと思われる記述になっていた。したがって、リンクコードを排除することが、情報漏洩対策の上で不適切なものとならないかを検討する必要がある。しかしながら、WG の資料には、リンクコードがどのような意味において情報漏洩対策となり得るのか明確には書かれていないため、反証することが難しい。そこで以下では、リンクコードの情報漏洩対策上の意義として考えられ得る想定を列挙して、それぞれについて反証を試みる。

[*9] WG 第 2 回配布資料 2「番号制度 番号連携イメージ」の図中右下の「対照テーブル」を指す。

[*10] 金融分野では、犯罪による収益の移転防止に関する法律への対応と、預金保険法及び農水産業協同組合貯金保険法で破綻時の名寄せのために、個人番号と同種の性質を持つ番号への需要があるが、別の番号を附番して用いることも考えられる。

4.1 個人番号から芋づる式に漏洩するか

政府の説明において、リンクコードを用いない方法、すなわち、図 2 のように個人番号を直接指定して情報連携を行う方法について、「個人番号が漏れると芋づる式に情報を取得できてしまう」とし、それを理由に「個人番号を情報連携に直接用いない」として説明される様子[*11]が散見される。

確かに、個人番号は、税務当局に提出する法定調書等に記載して多くの人々の目に触れることのある、いわゆる「見える番号」であるから、個人番号は秘密情報とは言えず、個人番号だけで情報連携基盤を通じて他の情報保有機関から個人情報を取得できてしまうのは大いに危険である。しかし、それを解決するためとして「見えない番号」である「リンクコード」を用いるというのには疑問がある。

そもそも、たとえリンクコードを用いるにしても、リンクコードを送信するだけでどこからでも個人情報を引き出せてしまうような設計は、情報セキュリティ技術の観点から言って、通信システムのプロトコルとしてあり得ないものである。当然、情報連携基盤及び各情報保有機関は、権限のある接続元からの接続しか受付けず、かつ、一定の接続時の認証処理を経て、その接続セッションが有効な期間中にのみ、情報連携のリクエストを受け付けるように設計するのが当然であろう。

システムがそのようなごく普通の設計になっていれば、情報連携のリクエストに、個人番号を用いて指定するのも、リンクコードを用いて指定するのも、セキュリティ上の強度は同じであるのだから、このような理由は意義を成さない。

4.2 情報保有機関に不正侵入された場合への対策か

通信システムのプロトコルが前記のようにごく普通の設計になっていて、システムの外部から不正に情報を引き出すことができないようになっているとしても、情報連携基盤への接続元となる情報保有機関の端末等が侵入された場合に、芋づる式に情報が引き出されてしまうことが考えられる。すなわち、端末等への侵入者が、情報連携基盤への接続のセッションを乗っ取って、データ上は正規のものと区別のつかないリクエストを送信することにより、任意の個人番号の個人情報を情報連携基盤経由で引き出すという犯行が考えられる。

確かに、このような事態が起きないように防止する必要

[*11] 例えば、平成 25 年 4 月 3 日の衆議院内閣委員会では、委員の「なぜこんな仕組みになっているのですか」との質問に対して政府参考人が、「情報提供ネットワークシステムにおいては個人番号を使わずに、それぞれの機関が別の符号を（中略）使って情報連携をしようとしております。その最大の理由は、（中略）番号で情報連携をいたしますと、番号が漏れた際に、かつハッキングされた場合に、芋づる式に情報が漏れる危険がございます。したがいまして、個人番号から推測できないように加工された符号を連携に用いることによりまして、個人情報が芋づる式に漏洩することがないような仕組みとしております。」と述べている。

があるが、情報連携基盤へのリクエストに個人番号を用いずにリンクコードを用いたとしても、これは防止できるものではない。なぜなら、情報保有機関の端末は、正規の利用時において、個人番号を指定して情報連携のリクエストを出すようになっているのであり、端末に侵入した者は、個人番号を指定して端末からリクエストを送信することができる。すると、その先のシステムが、当該個人番号に対応するリンクコードに自動的に変換して、それを情報連携基盤にリクエストとして送信することになるのであるから、侵入者はいずれにせよ個人番号から個人情報を引き出せてしまう。

なお、このような攻撃が可能となるのは、個人番号とリンクコード間の符号変換を行うシステムより端末側に位置する部分に侵入した場合であり、符号変換を行うシステムより情報連携基盤側の部分に侵入した場合にはこの攻撃は成立せず、その場合は、リンクコードが流出しない限り不正なリクエストを情報連携基盤に送信できないことになる。しかし、だからといってリンクコードを用いる方式が正しい設計だと言うべきではない。ごく限定的なケースに対してのみ有効な対策に惑わされることなく、全体に対して、そもそも侵入が起きないように対策するべきであるし、侵入が起きた場合への対策も合わせて講じるべきである。

4.3 情報連携基盤の内部での不正行為への対策か

次に、情報連携基盤に侵入された場合や、情報連携基盤内での内部犯行のケースを想定してみる。

これまでの検討案 [6] では、情報連携基盤内の符号変換は、参照テーブルによる方法と暗号関数による方法が検討されているが、どちらの方法を使うにせよ、変換用に必要となる「ID コード」を内部に持つ。情報連携基盤内の不正者は、ID コードを指定して任意の個人に関するリクエストを送信できてしまうから、リンクコードを用いることが対策になるわけではない。

また、そもそも、第 2.1.2 節で述べたように、情報連携基盤は、個人情報を直接扱わないアクセストークン方式を採用するべきであるから、情報連携基盤内の不正者が、情報保有機関から個人情報を引き出すことは直ちにはないのであり、やはり、リンクコード方式が何らかの対策になるわけではない。

5. まとめ

以上の通り、日本政府が創設を進めている「社会保障と税の番号制度」について、どのような手段でプライバシー保護の問題が解決されているのか整理した上で、近々構築が計画されている「情報連携基盤」（情報提供ネットワークシステム）の技術設計について再検討したところ、これまでの検討で案とされてきた「リンクコード」（符号）を用いた連携方式は、プライバシー保護の観点からも、情報セキュリティ技術の観点からも、無用なものであることが示された。

そこで、国会に提出されている「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案」の趣旨に照らして、より合理的な情報連携基盤の設計案（図 3）を提案した。この方式は、将来予定されている番号制度の利用範囲の拡大に際しても、「国家管理への懸念」を惹起することなく、柔軟に拡張できるものである。

参考文献

[1] 内閣官房, ”社会保障・税番号制度”, 入手先 ⟨http://www.cas.go.jp/jp/seisaku/bangoseido/⟩（2013 年 4 月 8 日閲覧）
[2] Masato Hirose, ”Towards Introducing an Identification Number System for Social Security and Taxation”, NRI Papers, No.161, March 1, 2011, 入手先 ⟨http://www.nri.co.jp/english/opinion/papers/2011/pdf/np2011161.pdf⟩（2013 年 4 月 8 日閲覧）
[3] ”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案”, 第 183 回国会閣法第 3 号, 2013 年 3 月 1 日
[4] 政府・与党社会保障改革検討本部, ”社会保障・税番号大綱 ―主権者たる国民の視点に立った番号制度の構築―”, 2011 年 6 月 30 日
[5] 内閣官房, ”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）”, 社会保障・税に関わる番号制度に関する実務検討会及び IT 戦略本部企画委員会 情報連携基盤技術ワーキング・グループ, 2011 年 3 月 4 日
[6] 内閣官房, ”番号連携方式検討表 ― 情報連携基盤技術ワーキンググループ中間とりまとめ（資料 1-2）”, 社会保障・税に関わる番号制度に関する実務検討会及び IT 戦略本部企画委員会 情報連携基盤技術ワーキング・グループ, 2011 年 7 月 28 日
[7] 民主党社会保障と税の一体改革調査会, ”社会保障・税番号大綱に対する取りまとめ”, 2011 年 11 月 22 日
[8] 経済同友会国家情報基盤改革委員会, ”次世代へ誇れる番号制度システムの実現を ～ 国益 ＞ 国民益 ＞ 政治家益・省益・企業益～ ”, 2012 年 3 月 21 日, 入手先 ⟨http://www.doyukai.or.jp/policyproposals/articles/2011/120321a.html⟩（2013 年 4 月 8 日閲覧）
[9] 内閣官房, ”データ送信方式検討表 ― 情報連携基盤技術ワーキンググループ中間とりまとめ（資料 1-3）”, 社会保障・税に関わる番号制度に関する実務検討会及び IT 戦略本部企画委員会 情報連携基盤技術ワーキング・グループ, 2011 年 7 月 28 日
[10] 日本弁護士連合会, ”「社会保障・税番号大綱」に関する意見書”, 2011 年 7 月 29 日, 入手先 ⟨http://www.nichibenren.or.jp/activity/document/opinion/year/2011/110729_5.html⟩（2013 年 4 月 8 日閲覧）
[11] 内閣官房, ”番号制度における符号連携のイメージ ― 情報連携基盤技術ワーキンググループ中間とりまとめ（資料 1-1）”, 社会保障・税に関わる番号制度に関する実務検討会及び IT 戦略本部企画委員会 情報連携基盤技術ワーキング・グループ, 2011 年 7 月 28 日
[12] 山口英, 情報連携基盤技術に関する私的勉強会, ”情報連携基盤技術に関する質問／情報連携基盤に関する個人情報保護に関する質問”, 情報連携基盤技術ワーキング・グループ 第 4 回 資料 7, 2011 年 4 月 12 日
[13] 厚生労働省, ”医療等分野における情報の利活用と保護のための環境整備のあり方に関する報告書”, 社会保障分野サブワーキンググループ及び医療機関等における個人情報保護のあり方に関する検討会, 2012 年 9 月 18 日