

個人番号制度の法的課題（中）

広 田 恭 子

はじめに

第一章 住基ネットと個人番号制度

1. 住基ネット導入までの経緯（1970年～1999年）
2. 住基ネットの概要
3. 個人番号制度導入までの経緯（2009年～2013年）
4. 個人番号制度の概要（以上、第71巻第3号）
5. 考察

第二章 住基ネット訴訟

1. 大阪地方裁判所平成16年2月27日判決
2. 大阪高等裁判所平成18年11月30日判決
3. 最高裁判所第一小法廷平成20年3月6日判決（以上、本号）
4. 考察

第三章 個人番号制度の法的課題

1. 住基ネット最高裁判決と個人番号制度の関係
2. 個人番号の保護の必要性
3. 情報の蓄積問題とその他の課題

おわりに

5. 考察

（1）個人番号の要件と必要性

①個人番号の要件

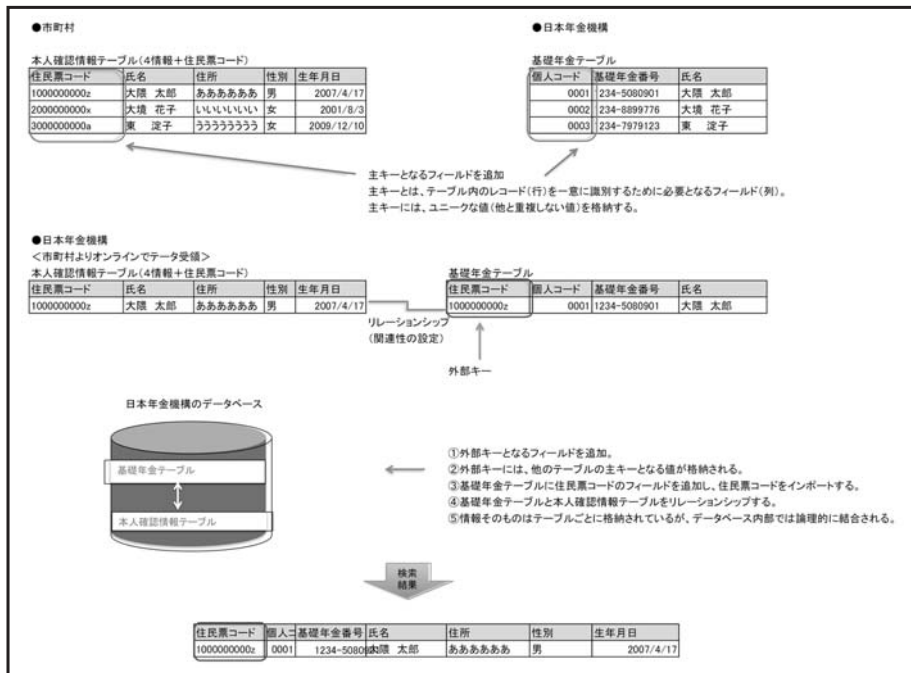
個人番号の生成要件は、番号法第8条第2項に定められている。第一に、他のいずれの個人番号とも異なること（同法第8条第2項第1号）、第二に、住民票コードを変換して得られるものであること（同第2号）、第三に、住民票コードを復元することのできる規則性を備えるものではないこと（同第3号）である。これらの要件を全て充足した番号が個人番号として割り当てられる。

②個人番号の必要性

住基ネットでは、住民票コードという番号を個人に付番し、システムを構築して、居住関係の公証の目的のために住民票コードを利用している。番号制度では、個人番号という番号を個人に付番し、システムを構築して、法定された利用範囲内で個人を特定する目的のために個人番号を利用している。この2つの制度は、住民票を有する個人を対象として

いることから、大量の個人データを扱う点で共通の基礎がある。また、システム化にあたり、個人に重複しない「番号」を付番し、利用している点で共通した考え方を採っている。

大量のデータの中から、特定の、あるいは一定の条件に合致するデータを迅速、かつ、正確に確定するために「番号」の付番は重要な意義を持っている。ここでは図2の例を使って、「番号」を付番する意義とその必要性をデータベース構築の観点から確認する。



【図2：主キー、テーブル、フィールドの説明】

大量のデータの中から、特定の、あるいは一定の条件に合致するデータを迅速、かつ、正確に確定するための有効な手段としては、一般的にデータベースの構築が考えられる。

電子計算機の操作を行う者は、特定の、あるいは一定のデータ呼び出すために、データベースに対して条件を入力する。データベースは、入力された条件に基づいて、データの検索、抽出、更新、削除等を排他的に処理する。そのためデータベースは、大量のデータの中から条件に合致するデータと他のデータとを識別しなければならない。また、データベースは、大量のデータが保存される性質ゆえに応答時間の遅延が発生する可能性がある。その場合、応答時間の遅延を回避するための何らかの「工夫」が必要となる。

そこで、テーブルの機能を活用する。具体的には、大量のデータを目的や種類ごとに区分けして保存することができる「テーブル」(テーブルは複数作成可能)を作成し、テーブルごとにデータを保存していく方法で応答時間の遅延を回避する工夫を行う。保存エリアの細分化である。図2の例では、本人確認情報テーブルと基礎年金テーブルが存在する。各々のテーブルには保存されたデータを一意に識別するためのフィールドを設け、「主キー」

を設定する。例えば、本人確認情報テーブルでは、重複しない「番号」である住民票コードを主キーとして設定することで本人確認情報を他者と識別することができる。

また、各テーブルの関連付けの設定が行われる場合がある（これを「リレーションシップ」あるいは「テーブルの関連付け」と呼ぶことがある）。図2の例では、本人確認情報テーブルと基礎年金テーブルの関連付けを行うため、外部キーとなるフィールドを追加し、基礎年金テーブルに他のテーブルの主キーとなる値として住民票コードのフィールドを追加、データをインポートする。そして、2つのテーブルの関連付けの設定を行う。

このように大量のデータを構築する場合、テーブル化を行うことで、検索等の時間の短縮化、データ管理の効率化を図ることが期待できるうえ、必要な場合には、テーブルを関連付けしてテーブル間の横断的な検索等を行うことが可能となる。

以上の確認から、次の点を強調しておきたい。大量のデータの中から特定の、あるいは一定のデータを迅速、かつ、正確に確定するためには、テーブル内のデータを一意に識別するために必要となる、他と重複しない「番号」である主キーが必要である。また、主キーは、テーブル間を関連付けるための外部キーにもなり得る。自動処理において、大量のデータを扱う場合、重複しない「番号」を付番する必要性はこの点にあるといえる。

番号制度において利用される個人番号は、前述した通り、唯一無二性、悉皆性を有する。加えて、原則として生涯普遍的「番号」である。このような特徴を持つ個人番号は、強力な識別性を持つ「番号」として、データベース構築の観点からも重要な意義を持っている。

（２）社会保障・税に関わる個人番号制度と国民 ID 制度の一体的な検討過程

現在の番号制度に至るまでの前史として検討されていたのは社会保障・税に関わる番号制度と国民 ID 制度であり、番号制度が導入される直接の契機は、IT 総合戦略本部において、電子行政の推進を国の重点施策に打ち出していたことによると考えられる。そこでは番号を活用した「国民 ID 制度」を整備することが明確に示されている³⁴⁾。前述した民主党政権を中心とした番号制度の検討は、2010年2月から5月にかけて内閣官房国家戦略室において開催された「社会保障・税に関わる番号制度に関する検討会」において、IT 戦略として検討されてきた国民 ID 制度を取り込む形で番号制度に繋がっていったと推察される³⁵⁾。

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ワーキンググループ（以下「ワーキンググループ」という）による検討会において、「情報連携基盤

34) 首相官邸 IT 総合戦略本部「新たな情報通信技術戦略（平成22年5月11日）」3頁には、「社会保障の安心を高め、税と一体的に運用すべく、電子行政の共通基盤として、官民サービスに汎用可能ないわゆる国民 ID 制度の整備を行うとともに、自己に関する情報の活用については、政府及び自治体において、本人が監視・コントロールできる制度及びシステムを整備する」との記述がされている（<http://www.kantei.go.jp/jp/singi/it2/100511honbun.pdf>）3頁。

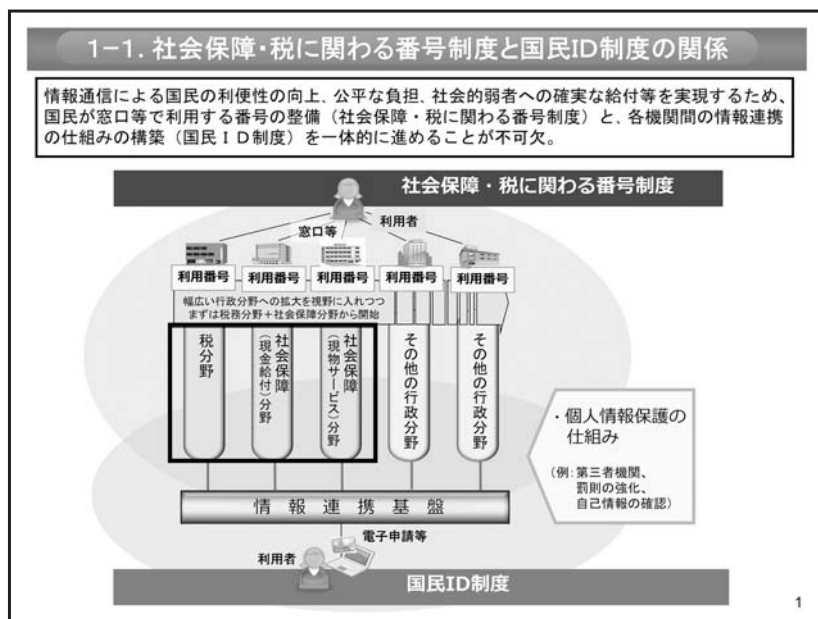
35) 近藤佳大「日本の番号制度（マイナンバー制度）の概要と国際比較—個人識別子と行政統制の視点から」情報管理56巻6号345頁参照（https://www.jstage.jst.go.jp/article/johokanri/56/6/56_344/_pdf/-char/ja）。

技術の骨格案（その1）」³⁶⁾（以下「骨格案」という）が作成され、個人に対する付番や番号連携及び情報連携に関する基本的な考え方が示された。2011年7月28日には「中間とりまとめ」³⁷⁾（以下「中間とりまとめ」という）が公表され、そこでは個人に対する付番や番号連携及び情報連携に関しての基本的考え方として、「住基ネット最高裁判決」³⁸⁾が合憲とした理由が列挙されており、番号制度の検討に際し、同判決を強く意識したことが窺える。

番号制度を理解するためには、まず番号がどのような視点で検討されてきたのかを確認することが重要であろう。又、個人番号の保護性を検討するに当たり有益でもあると考えられる。そこで以降では、「ワーキンググループ」の検討資料及び「骨格案」の中から情報連携に関わる番号の考え方が示されている点に絞って概観する。

①社会保障・税に関わる個人番号制度と国民ID制度の関係

図3では、社会保障・税に関わる番号制度と国民ID制度との関係について、国民が窓口等で利用する番号の整備と各行政機関の情報連携の仕組みの構築（国民ID制度）を一体的に進めることが不可欠であると記されている。



【図3：社会保障・税に関わる番号制度と国民ID制度の関係】³⁹⁾

36) 情報連携基盤技術ワーキング・グループ「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）1頁以下（<http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai2/siryou3.pdf>）。

37) 情報連携基盤技術ワーキング・グループ「中間とりまとめ」（平成23年7月28日）（<http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/cyukan/cyukan.pdf>）。

38) 前掲注13)。

本図を見ると、国民ID制度は、社会保障・税番号分野での利用（図3黒囲線）の他、その他の行政分野においても利用を可能とする汎用的な情報連携基盤として整備する計画が検討されていたことがわかる。

②国民IDコードに利用する番号の比較

「国民IDコード」⁴⁰⁾に利用する番号については、基礎年金番号、住民票コード、住民票コードに対応させた新しいコードが候補として検討されたものの、番号の一意性、悉皆性、不可視生の観点で優れていると考えられた住民票コードに対応させた新しいコードが選択された（図4黒囲線参照）。

3-4. 国民IDコードに利用する番号の比較例(第6回TF資料再掲)			
「社会保障・税に関わる番号制度に関する検討会 中間取りまとめ」において選択肢として示された3案を例として、国民IDコードに利用する番号について比較。			
	①基礎年金番号を利用	②住民票コードを利用	③住民票コードに対応させた新しいコードを利用
	分野A 分野B 分野C 利用番号1 利用番号2 利用番号3 ①基礎年金番号 ②住民票コード ③住民票コード	分野A 分野B 分野C 利用番号1 利用番号2 利用番号3 ①基礎年金番号 ②住民票コード ③住民票コード	分野A 分野B 分野C 利用番号1 利用番号2 利用番号3 ①基礎年金番号 ②住民票コード ③住民票コード
検討の観点	一意性 ※一人に一つのコードが付番されていること ①基礎年金番号 ②住民票コード ③住民票コード	一意性 ※一人に一つのコードが付番されていること ①基礎年金番号 ②住民票コード ③住民票コード	一意性 ※一人に一つのコードが付番されていること ①基礎年金番号 ②住民票コード ③住民票コード
一意性	・重複付番の可能性について指摘あり。	・一意性あり。	・一意性あり。
悉皆性	・年金未加入者に悉皆性がない。	・悉皆性あり。	・悉皆性あり。
不可視性	・目視可。(法律上一定の場合を除き第三者が告知を求めることは禁止) ※年金手帳、各種本人への通知等に記載	・容易に目視できない。(法律上第三者が告知を求めることは禁止)	・暗号化等により不可視のコードとすることが可能であり、個人情報保護・セキュリティ対策の観点で優位性
可変性	・生涯変更されない。	・本人の請求により変更可能。(年間70件程度の変更請求あり)	・新規付番のため可変・不変いずれも可能。
コスト	導入期 ・既存の付番の仕組みを利用するため、その分のコストを節約できる。	導入期 ・既存の付番の仕組みを利用するため、その分のコストを節約できる。	導入期 ・対象となる全ての者に対して付番・周知・配布するための作業と総額が必要。

【図4：国民IDコードに利用する番号の比較例】⁴¹⁾

その理由は、住民票コードは唯一無二性、悉皆性、最新の基本4情報と関連づけられる点で「番号」に好適であるものの、見える番号とするためには、住基ネット制度のシステム改修や法改正が大幅に見込まれること、万一、漏えい等で不正利用された場合、情報連携に対して国民の不安や懸念が生じる可能性があること、住民票コードを直接用いず住民票コードから変換される番号を用いることで、これらの問題点がクリアになることが主な

39) IT 総合戦略本部電子行政に関するタスクフォース「国民ID制度における国民IDコードの考え方（その2）」（平成22年12月27日）1頁をもとに黒囲線を追記した。（http://www.kantei.go.jp/jp/singi/it2/denshigyousei/dai8/siryou2_1.pdf）

40) 国民IDコードはその後、現行の番号制度の情報連携の図には登場してこない。しかし筆者は、国民ID制度の基本的構想は番号制度に継承されたのではないかと考えている。

41) IT 総合戦略本部・前掲注39) 10頁をもとに黒囲線を追記した。

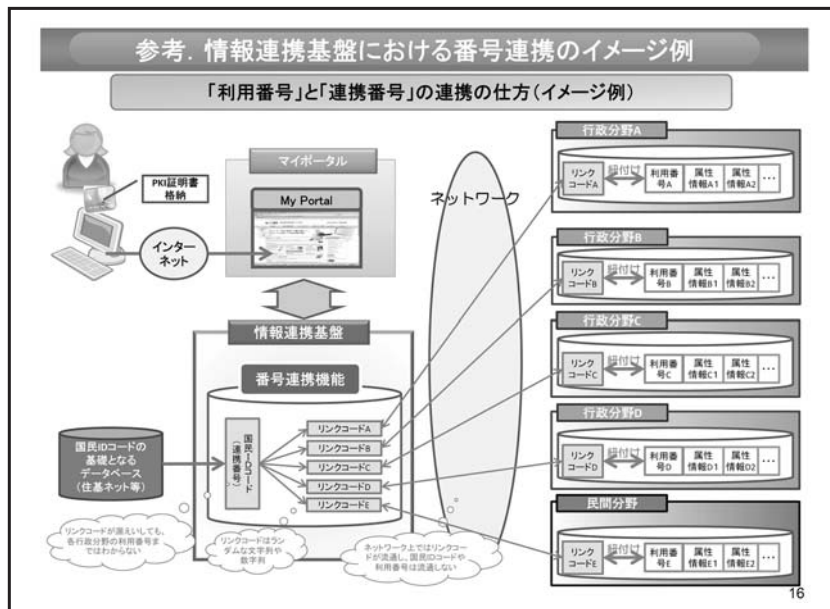
理由であったと推察される。

③情報連携基盤における番号連携（骨格案）

当初示されていた番号連携のイメージは、国民IDコードと行政分野ごとのリンクコードを対応させて情報連携を行うものあった（図5参照）。この方式がイメージされた背景は、情報連携に際し、3つの原則が掲げられたからである。すなわち、【1】「見える」「番号」を直接用いない情報連携、【2】「見えない」IDコードを用いる情報連携、【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とすることである。【1】の理由は、異なる情報保有機関等で情報連携を行うためには、該当する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」は民間で広く利用される「見える番号」であることから、IDコードとしてそのまま用いることは、個人情報保護の観点から適切ではないこと。【2】の理由は、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最小限とすることが必要であると考えられることから、住民票コードに対応した新しいコードとすべきであること。【3】の理由は、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機関にも波及する可能性があることが説明されている。

そこで「番号」を含む利用番号とIDコードとの間に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、情報保有機関ごとに異なるリンクコードを付与して、異なる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方針が挙げられている⁴²⁾。

42) 情報連携基盤技術ワーキング・グループ・前掲注36) 1～2頁参照。



【図5：情報連携基盤における番号連携のイメージ例】⁴³⁾

④番号、IDコード、リンクコードの生成方法

また、骨格案では、「住基ネット最高裁判決」⁴⁴⁾で指摘された個人情報の一元管理を避けるため、「番号」を含めた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方式にすべき方針が謳われていた⁴⁵⁾。この基本方針は番号制度に導入されている。番号法上、個人番号の生成については法定されている。まず、市町村長が地方公共団体情報システム（以下「機構」という）に対し、住民票コードを送信し個人番号の生成を求める（同法第8条第1項）。要求を受領した機構は、住民票コードから不可逆暗号化措置を講じて番号を生成する（同法第8条第2項第2号及び第3号）。

続いて、IDコードとリンクコードの生成に関する事項についても次のような記載がある。情報連携基盤のIDコードとリンクコードには、各行政分野に付与されるリンクコードと情報連携が行えるように双方向性を備える必要があり、リンクコードからIDコードに遡れること、またIDコードからリンクコードに遡れることができる必要がある。したがって、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式は可逆暗号方式とすべきことが明記されている⁴⁶⁾。

43) IT 総合戦略本部・前掲注39) 16頁。

44) 前掲注13)。

45) 情報連携基盤技術ワーキング・グループ・前掲注36) 2頁参照。

46) 情報連携基盤技術ワーキング・グループ・前掲注36) 2～3頁参照。

でいうところの「符号」の表現に変更されている点、情報連携基盤内で行われる ID コードとリンクコードの変換についての記述が「符号同士を紐付ける仕組み」との抽象的な表現に改められた点に相違がある。

現時点では番号制度における情報連携を説明した資料には ID コードの記載は無い。しかし、行政分野ごとに異なる符号同士を紐付けして情報連携を行うといっても、同一人であることを特定しなければ情報連携はできないのであるから、例えば符号 A と符号 B が同一人であることを確定させるためには、符号 A が符号 B であることを紐付ける符号変換テーブル方式（符号は乱数を用いて遡れない形で符号を変換し、変換前後のテーブルを保持する）か、符号から個人の ID コードに遡る ID コード方式のいずれかを採らなければ異なる符号同士を同一人と特定することは難しいのではないかと考えられる。

ここでいう ID コードが個人番号として説明される文献⁴⁹⁾も存在していることを鑑みれば、番号制度の立法過程においては、情報連携を行う際に個人を一意に特定するための ID コードに何を用いるのか、議論の変遷があったことが窺えるのだが、仮に ID コードが個人番号だとすれば、情報の一元管理を行わないとした「中間とりまとめ」の基本方針と矛盾することになる。したがって、ID コードに個人番号は用いないと解釈するほうが、「中間とりまとめ」の基本方針に適した理解であろう。

（３）「符号」の変遷

①国民 ID 制度から初期の社会保障・税番号制度における「符号」の意味

さて、情報連携を行う際に非常に重要となる「符号」の持つ意味について考察する。「符号」の持つ意味は、初期の番号制度と現在の番号制度に至るまでに変遷がある。そのことを確認するためにもまずは、国民 ID 制度から初期の社会保障・税番号制度における「符号」の意味について確認していくことにする。

符号は、「情報連携の符号（リンクコード）は住民票コードから生成される」⁵⁰⁾と説明されている。骨格案よれば、「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）とする」との考え方が示されており、番号制度の情報連携においては、住民票コードから可逆暗号で ID コードを生成し、さらに ID コードから可逆暗号で符号を生成するという形式が採られるのではないかと考えられる。

情報連携基盤内で符号同士を紐付ける仕組みがこのような方式が採られていると考える

49) 佐藤教授は情報連携を次のとおり、説明する。「たとえば符号 A で個人を特定している行政機関 X が、別の行政機関 Y において符号 B で特定される同一人の個人情報を入力したい場合、X は情報提供ネットワークシステムに対して符号 A を通知すれば、これがマイナンバーに変換され、さらに符号 B に変換されて Y に通知される。このようにして、Y から X に対して、情報提供ネットワークシステムを経由して、当該符号 B で特定される個人情報が提供されることになるのである」（佐藤信行「IC 技術と法システム-電子署名法とマイナンバー法案をめぐって-」法學新報120巻 1・2 号598頁）。

50) 宇賀・前掲注 9) 51頁。

根拠は次の理由からによる。

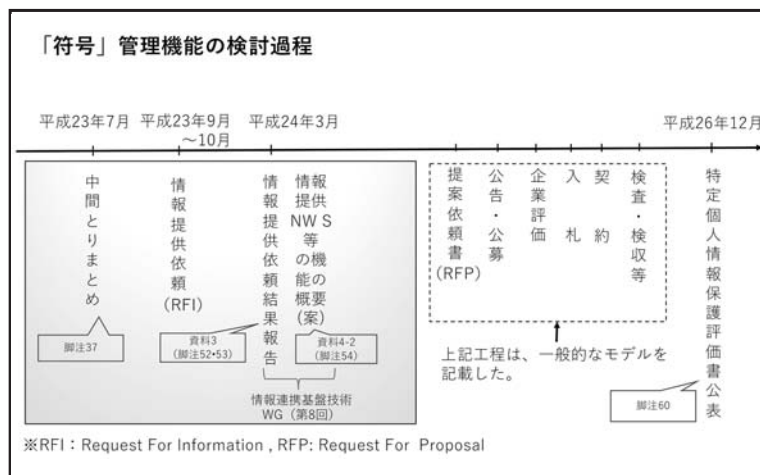
第一の理由は、内閣官房社会保障改革担当室参事官が情報連携基盤の仕組みについて問われ、それに応答しているのだが、それによれば、「情報提供を許可し符号同士を紐付ける仕組みが設けられており、情報連携がなされるその瞬間だけは、(中略)同一人であることが情報連携基盤において確認されることとなる」⁵¹⁾と説明されている。情報連携の際には、異なる符号同士を「同一人」であることの確認処理が行われることがこの説明から読み取れる点が挙げられる。

第二の理由は、第8回ワーキンググループの「RFI(情報提供依頼⁵²⁾)の結果について資料3」⁵³⁾において、2011年9月2日から同年10月28日まで情報提供依頼の実施を行なった結果が記載されている。当該資料3では、符号の生成・管理方式に関して、中間とりまとめで示した5案中、19事業者から情報提供があったこと等が報告されているのだが、同日に「情報提供ネットワークシステム等の機能の概要(案)資料4-2」⁵⁴⁾も配布されている。当該資料4-2には、符号管理機能について次の記述がある。符号管理機能1として、「情報提供等記録開示システム⁵⁵⁾及び情報提供者・情報照会者からの求めに対し、符号(IDコード、リンクコード)を生成する機能」、符号管理機能2として、「地方公共団体情報システム機構から受信した住民票コードをもとにIDコードを生成し、それをもとにリンクコードを生成する機能」が記述されている。当該資料4-2は、「要件定義書」⁵⁶⁾に類するものと思われ、この段階で符号に関する機能は、相当程度仕様が固まっていたのではないだろうか。そして、当該資料4-2には、各事業者からの情報提供を受けて検討した結果が反映されていると考えるのが自然であろう。以上の推察を前提として、符号管理機能の検討過程を整理すると概ね次のような流れになるであろう(図7参照)。

-
- 51) 阿部知明「情報提供ネットワークシステム、マイ・ポータルなど番号法関連のシステムについて」ジュリスト(有斐閣、2013年8月No.1457)50頁。
 - 52) 一般に「RFI」と呼ばれるものである。必要とする機能やその実現方法、費用等を含め、発注元がシステムを調達するにあたり、必要な情報の提供を各システムベンダーに依頼するために作成する。システムを調達するにあたり、必要に応じて、RFIを実施、各システムベンダーから情報提供を受ける。その結果を検討したうえで提案依頼書(RFP)の作成が行われる。
 - 53) 内閣官房情報連携基盤技術ワーキンググループ「RFI(情報提供依頼)の結果について資料3」(2012年3月23日)(<https://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai8/gijisidai.html>)。
 - 54) 内閣官房情報連携基盤技術ワーキンググループ「情報提供ネットワークシステム等の機能の概要(案)資料4-2」(2012年3月23日)(<https://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai8/gijisidai.html>)。
 - 55) マイナポータルと呼ばれる(番号法附則第6条第3項)。政府が運営するオンラインサービスのことである。個人情報関連で注目すべき機能としては、①自己情報表示[あなたの情報](行政機関などが持っている自分の特定個人情報が確認できる)、②情報提供等記録表示[やりとり履歴](情報提供ネットワークシステムを通じた住民の情報のやり取りの記録を確認できる)であろう。詳細は、「マイナポータルとは」を参照(<https://www.cao.go.jp/bangouseido/myna/index.html>)。
 - 56) 「要件定義書」とは、システム開発において、当該システムに必要とする機能と要件を定義したものをいう。開発工程において取り纏められる作業である。

当初、中間とりまとめで提案されていた5案を含む情報提供ネットワークに必要な機能等に関して、RFIを実施した。次に、その結果を踏まえて情報提供ネットワーク等の機能の概要（案）として、情報連携基盤技術WG（第8回）で資料4-2の提示を行った。当該資料4-2は、RFIの結果を踏まえた機能の概要書であり、一般的にシステム開発の要件を確定するために作成される要件定義書に類する資料であると考えられる。

これらの点から、符号管理機能について、この段階で大枠の仕様が固まっていたことが窺える。



【図7：符号管理機能の検討過程】

続いて、第三の理由は、番号法における第2条第8項（特定個人情報の定義）の逐条解説を見ると、「個人番号自体ではなくても、個人番号に代わって用いられる番号、記号その他の符号で個人番号を認識しうるものである場合、個人番号と同様に保護する必要がある。符号（リンクコード）や情報提供を許可し符号同士を紐付けるIDコードのみならず、脱法的に個人番号を変換したもので可逆的に個人番号を識別できるものを含む⁵⁷⁾と解説されていることが挙げられる。つまり、符号がリンクコードを指すこと、符号同士を紐付けるのはIDコードであることが示唆されている点が挙げられる。

以上の3つの理由から、当初の番号制度には、国民ID制度で検討されてきた番号に関する考え方が継承されていると考えるべきであろう。行政機関ごとに配布された異なる符号を、同一人の情報へと紐付けを行うのは符号である。符号は総称で表現されているものの、符号の持つ意味は、住民票コードからIDコードを生成し、IDコードから行政機関と情報連携するためのリンクコードを生成する仕組みが採用されていることがわかる。

57) 宇賀・前掲注9) 25頁。

②現行制度における「符号」の意味⁵⁸⁾

その後、2014年12月には、「特定個人情報保護評価」⁵⁹⁾が行われ、番号法 第28条第4項に基づき、「情報提供ネットワークシステムの運営に関する事務（全項目評価書）（以下「評価書」という）」⁶⁰⁾が公表された。評価書によれば、各種の符号が存在する。**【1】** 情報連携を行う場合に情報連携基盤内で個人を一意に特定するために使用される住民票コードから生成する「連携用符号」、**【2】** 情報保有機関と情報連携基盤間で個人を一意に特定するために使用し、連携用符号から生成した機関ごとに異なる符号「情報提供用個人識別符号」、**【3】** 情報連携における情報照会・提供に関わる記録を情報提供等記録ファイルに保存あるいは抽出する際、個人を一意に特定するために使用される「情報提供等記録用符号」⁶¹⁾がある。

符号の生成は次のように行われる。「情報照会者等から情報提供用個人識別符号生成の依頼を受ける。情報照会者等から住基ネットを介して、情報提供用個人識別符号生成の対象者の住民票コードを受領する。当該住民票コードをもとに、暗号演算により、対象者ごとに異なり、情報提供用個人識別符号等の生成の基となる全ての情報照会者等に共通の連携用符号を生成し、連携用符号発行管理ファイルに保存する。住民票コードは連携用符号生成後、直ちに削除する。次に、連携用符号に暗号演算による変換を行うことにより、情報照会者等ごとに異なる情報提供用個人識別符号を生成し、情報照会者等へ送信する。ただし、情報提供用個人識別符号は情報提供ネットワークシステムに保存しない。また、情報連携が行われる際にはその情報連携の記録を情報提供等記録ファイルに保存することとし、その際も個人を特定するために連携用符号に暗号演算による変換を行うことにより、情報提供等記録用符号を生成し、情報提供等記録ファイルに保存する」⁶²⁾。

住民票コードから連携用符号生成に関しては、住民票コードへの不可逆性をシステムで担保する設計であり、住民票コードから連携用符号の生成の際には不可逆暗号演算処理が行われる⁶³⁾。

以上をもとに、現行の番号制度における符号生成、情報連携イメージを図に表すと、図8のように表すことができる。

58) 執筆段階（2020年5月）の時点で確認できた資料をもとに記述している。

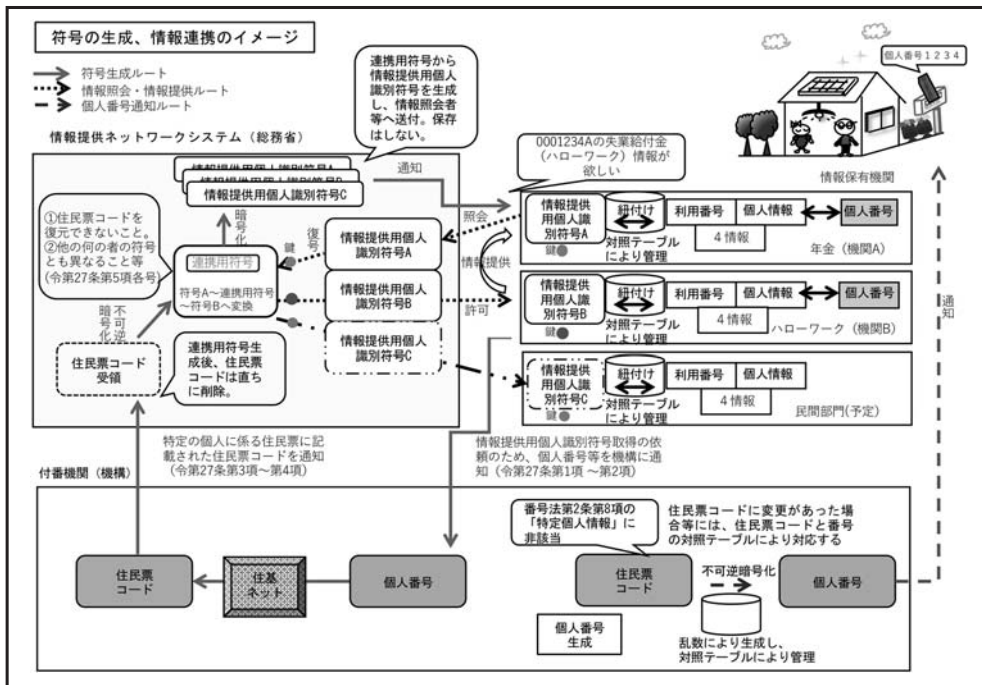
59) 特定個人情報の漏えいその他の事態の発生の危険性及び影響に関する評価をいう（番号法第27条第1項）。

60) 総務省「情報提供ネットワークシステムの運営に関する事務を対象とする特定個人情報保護評価書（別添1）」（https://www.soumu.go.jp/menu_news/s-news/01kanbo05_02000067.html）

61) 前掲注7)。

62) 総務省・前掲注60) 4頁参照。

63) 総務省・前掲注60) 14頁参照。



【図8：符号の生成、情報連携イメージ】

図8に基づき情報連携の流れを説明する⁶⁴⁾。情報照会機関である年金機関（機関番号はAと仮定）から、自己の保有する特定個人情報に係る個人番号1234に対し、総務大臣から情報提供用個人識別符号Aを取得し（番号法第21条の2第1項）、現在利用しているA機関における利用番号等と個人情報が紐付けられる。

情報提供機関であるハローワーク（機関番号Bと仮定）も、自己の保有する特定個人情報に係る個人番号1234に対し、総務大臣から情報提供用個人識別符号Aを取得し、現在利用しているB機関における利用番号等と個人情報が紐付けられる。以上を前提に、年金機構は照会したい特定個人情報名と情報提供用個人識別符号Aを情報提供ネットワークシステムに送信する（同法第19条第7号及び第8号、番号法施行令（以下「令」という）第20条）。受信した情報提供ネットワークシステムは、暗号化された情報提供用個人識別符号Aから連携用符号に復号し、個人を一意に特定する。そして、連携用符号から情報提供機関であるハローワークにおける情報提供用個人識別符号Bに変換する。次に、情報提供ネットワークシステムからハローワークに対し、照会したい特定個人情報名と情報提供用個人識別符号Bを送信する（同法第21条の2第2項、令第27条）。電文を受信したハローワークは、該当する特定個人情報を抽出し、年金機構へ送信する（同法第22条第1項、令第28条）。

64) 岡村久道『番号利用法-マイナンバー制度の実務』（商事法務、2015年）70～71頁を参考にした。

ここまで、国民 ID 制度から番号制度創立に至るまでの符号の変遷及び情報連携の仕組みについてみてきた。以上を整理すると大要次のことがいえるであろう。

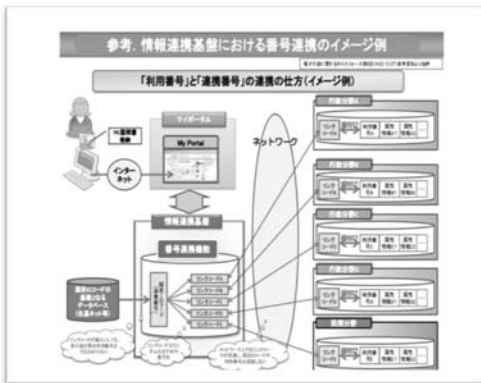
国民 ID 制度で示されていた情報連携の基本的考え方は【1】、番号制度の分科会「情報連携基盤技術 WG」においても検討され【2】、社会保障・税番号制度における情報連携の骨格を形成し【3】、現在の番号制度における情報連携の仕組みへと幾多の変遷を経て完成された【4】（図9：符号の変遷図参照）。

このような「符号」の変遷を考慮に入れば、番号制度において構築された情報連携の仕組みは、本制度で利用する機能を実現しただけでなく、国民 ID 制度の機能をも取り込んで構築されたのではないか、という一つの推測が成り立ち得る。すなわち、番号制度で構築された情報連携の仕組みは、社会保障、税、災害対策の3分野における利用の実現だけでなく、国民 ID 制度としての機能——その他の行政分野、その他の行政分野以外の分野における情報連携——が技術的には実現されていると考えるべきではないのか。

以上までの検討で次の点を指摘しておきたい。まず、これまで幾度も反対に合い、成立し得なかった国民総背番号制ないし国民 ID 制度を、番号制度として導入する際、社会保障、税、災害対策の3分野での限定した利用である旨を強調することで、税負担に関する公正・公平な社会の実現という目的に対する国民の一定の理解を得ながら、制度導入に対する従前の抵抗感の払拭に功を奏した。

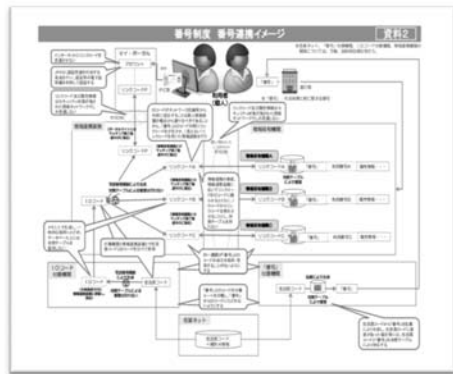
しかし、本制度の主眼は、番号法の基本理念に現れているように、個人番号や個人番号カードの利用を幅広い分野において活用することにある。今回、構築された情報連携の仕組みには、本制度が将来的に幅広い分野で利用することが可能となるための技術的基盤が既に構築されているとあって良いであろう。

【1】



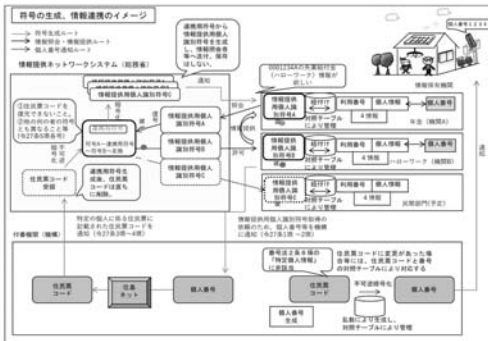
国民 ID 制度で検討されていた「情報連携基盤における番号連携のイメージ」

【2】



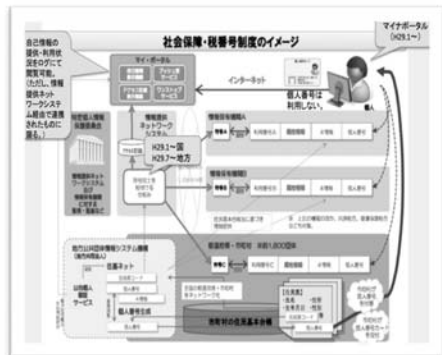
情報連携基盤技術 WG で示されていた「番号制度 番号連携イメージ」

【4】



国民 ID は連携用符号へ、リンクコードは情報提供用個人識別符号等に変化を遂げる。

【3】



「社会保障・税番号制度のイメージ」この段階で、ID コード、リンクコードの明記は「符号同士を紐づける仕組み」との抽象的表現にかわる。

【図 9：符号の変遷図】

二. 住基ネット訴訟

番号制度の導入にあたり、立法者が強く意識したと思われるのが、「住基ネット最高裁判決」⁶⁵⁾であろう。番号制度では、個人情報の情報連携基盤を構築するにあたり、「大綱」において、住基ネットに係る最高裁判決を十分に踏まえる必要があるとして、次の基本的な考え方が示されていた⁶⁶⁾。

第一に、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という事、第二に、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、第三に、個人情報の管理・利用等が法令等の根拠に基づき、正当な行政目的の範囲内で行われること、第四に、システム上、個人情報が容易に漏えいする具体的な危険がないこと、第五に、目的外利用又は秘密の漏えい等は、懲戒処分又は刑罰をもって禁止されていること、第六に、第三者機関等の設置により、個人情報の適切な取扱いを担保するための制度的措置を講じていることである。

そこで、これらの基本的考え方が示されるもとになった住基ネット訴訟を概観し、訴訟において何が問題となり、どういった判決が下されたのかを確認した後、若干の考察を行うことにしたい。

本章では、住基ネット訴訟のうち、大阪地方裁判所平成16年2月27日判決（以下「第一審判決」という）、大阪高等裁判所平成18年11月30日判決（以下「控訴審判決」という）、最高裁判所第一小法廷平成20年3月6日判決（以下「最高裁判決」という）を取り上げることにする。

1. 大阪地方裁判所平成16年2月27日判決⁶⁷⁾

(1) 事案の概要

①概要

2004年2月27日の第一審判決は、大阪府内の各市（豊中市、箕面市、吹田市、大阪市、守口市、泉佐野市、東大阪市、八尾市）に居住する住民ら（以下「原告ら」という）が、1999年8月に成立した住基法に基づく住基ネットによって、人格権、公権力から監視されない権利、自己情報コントロール権及び平穏な生活を営む権利が侵害され、精神的損害を被ったと主張し、原告が居住する被告各市（以下「被告ら」という）に対して、国家賠償法第1条に基づいて損害賠償請求を求めた事案である。

65) 前掲注13)。

66) 首相官邸「大綱」・前掲注17) 17頁参照。

67) 大阪地判平成16年2月27日民集62巻3号760頁。住基ネット関連の下級審裁判例を研究した文献として、岡村久道「住基ネット関連判例の研究（上）（下）」NBL814号12頁以下、同816号26頁以下、右崎正博「住基ネット関連判例の総合的研究」法律時報79巻12号80頁以下参照。

②原告らの主張

原告らの主張は、憲法第13条を根拠とする人格権の侵害とプライバシー権の侵害等であり、おおむね次の主張がなされた。

憲法第13条は個人の尊厳を保護しており、人格権を保護している。被告らが勝手に個人に番号をつけることは、人格権、幸福追求権を侵害する。また、憲法第13条が保障するプライバシー権の一態様として、公権力から監視されない権利を有するところ、住基ネットによる本人確認情報の送信は、個人の情報を1か所に集中させる。そのこと自体、公権力から監視されない権利を侵害する。さらに、将来の国民総背番号制に道を開くものであり、国民総背番号制は監視社会そのものであり、公権力から監視されない権利を侵害する。

憲法第13条の幸福追求権は、プライバシーの権利を自己に関する情報をコントロールする権利と定義づけたものであり、自己の情報の秘匿のみならず、その閲覧、訂正、削除を求める権利をも包摂する。個人の情報が個人の手から離れると、漏洩、目的外利用等の恐れが生じ、秘匿はもちろんのこと、訂正、削除が困難となり、自己情報コントロール権を侵害する。

他者から、自己の欲しない刺激によって心の静穏を乱されない利益を有するところ、住基ネットで国によって集中的に管理されることにより、不安感、危惧等を常に抱きながらの生活が余儀なくされる。これは、心の静穏を乱されることにほかならず、プライバシー権の一態様として平穏な生活を営む権利（平穏生活権）を侵害する。

（２）判旨（請求棄却）

第一審の争点となったのは、被告らが、住基法に基づき住民に対して住民票コードを付番し、住基ネットに接続したことにより、原告らの主張する人格権、公権力から監視されない権利、自己情報コントロール権、平穏生活権が侵害されたと認められるか否かであった。第一審は、主として次の理由を述べて、原告らの請求をいずれも退けた。

①住民票コードについて

住民票コードの評価について、第一審は、住民票コード自体は、無作為に作成された数字であり、個人情報が推知されるものではないことや、いつでも何度でも変更請求ができること、行政機関から住民に対する呼称に氏名等ではなく、住民票コードの数字が用いられるというものでないことを理由に原告らの主張する人格権の侵害、あるいは何らかの人格的利益の侵害を否定している。

②本人確認情報について

本人確認情報は、住民票の記載事項のうち、氏名、出生の年月日、男女の別、住所及び住民票コード並びにその変更に関する情報に限定されている（住基法第30条の5第1項⁶⁸⁾）。しかし、第一審は、「これら限定された個人情報であっても、みだりにこれを開示されたくないと思えることは自然なことであり、そのことへの期待は保護されるべき」と

の見解を示し、「本人確認情報は、原告らのプライバシーに係る情報として法的保護の対象になる」と述べている。

しかし一方で、「住民票の記載事項のうち、基本4情報については、請求事由を明らかにする等、不当な目的によることが明らかな場合でない限り、何人も閲覧し得る事項であり（住基法第11条）、また、これらの事項を記載した住民票の写しは、何人も交付を請求できる（住基法第12条）」ことから、本人確認情報の秘匿の必要性が必ずしも高いものということとはできない」とした。

そして、本人確認情報の内容・性質と、公益の必要性を照らし合わせて判断し、「原告らのプライバシーに係る法的利益が直ちに侵害されたと見ることはできない」と判断している。

③目的外使用について

目的外使用について、第一審は、「このような本人確認情報であっても、本人の確認という目的以外に利用される場合には、原告らのプライバシーに係る法的利益を侵害すること考えられる」と述べたのだが、しかし、原告らは、この点について請求をしている訳でもなかった。

また、目的外使用の事実についても、「原告らの本人確認情報が、目的外使用されたり、被告らの各市長が、他の目的外使用させた事実をうかがわせる証拠はない」と否定している。

④住基ネットの安全性について

住基ネットの安全性について、第一審は、「住基ネットの施行に伴い、本人確認情報保護のため、様々の措置が講じられており、住基ネットが、本人確認という目的以外に使用されたり、個人のプライバシーに係る法的利益に対する侵害を容易に引き起こすような危険なシステムであるとは認められない」として、原告らの住基ネットの危険性についての主張を退けた。

⑤本人確認情報の訂正等について

原告らは、住基ネットに接続されることにより、自己の本人確認情報がコントロールできなくなり、訂正、削除が困難になる旨を主張したが、第一審は、「住基法は、何人も、

68) 平成18年6月15日法律第74号による改正前の住基法第30条の5第1項。現行法では、氏名、出生年月日、男女の別、住所、個人番号及び住民票コード並びに住民票コードの記載に必要な事項として政令で定めるもの（住基法第30条の5）であり、個人番号が追加されている。

なお、住民基本台帳制度は、制定当初、居住関係を公証する公簿として、一般公開原則がとられていた。その後、1999年の本法改正により、閲覧の対象が基本4情報に限定された経緯がある。住民基本台帳の閲覧制度の変遷につき、宇賀克也『個人情報保護の理論と実務』（有斐閣、2009年）355～357頁参照。

…自己の本人確認情報について、その開示を請求することができ、都道府県知事又は指定情報処理期間は、上記請求に対し、本人確認情報につき開示しなければならない（住基法第30条の37）し、開示を受けた者が、本人確認情報につき、その内容の全部又は一部の訂正、追加、削除の申出があった時は、都道府県知事又は指定情報処理機関は、遅滞なく調査を行い、その結果を通知しなければならない（住基法第30条の40）と規定しており、住民からの本人確認情報の開示、訂正の申出を認めている」。

以上の理由から、大阪地裁は、原告らの請求にはいずれも理由がないとして、原告らの国家賠償請求を棄却した。

2. 大阪高等裁判所平成18年11月30日判決⁶⁹⁾

（1）事案の概要

①概要

2006年11月30日の控訴審判決は、控訴人らのうち、4名による住基ネットを使用した本人確認情報を大阪府知事に送付することの差止め等を求める訴えの追加的変更に関し、本件国家賠償請求と請求の基礎に同一性があり、これを認めるべきであると判断し、相手方の同意は要しないとして認容した⁷⁰⁾。

控訴人らは、住基ネットにより控訴人らのプライバシーの権利等の人格権を違法に侵害され、精神的損害を被ったと主張して、控訴人らが居住する被控訴人各市に対し、国家賠償法第1条に基づく損害賠償請求をし、かかる権利に基づく妨害排除請求（侵害状態の除去請求）として、住民基本台帳からの住民票コードの削除及び本人確認情報を大阪府知事に通知することの差止め（以下これらを合わせて「差止め」という）を請求した。

②控訴人らの主張

控訴人らからの主な主張は、第一審同様に行われたが、さらに、当審における追加的請求として、住基ネットからの離脱を請求した。控訴人らは、住基ネットに接続されることにより、自己に関するプライバシー情報が漏出し、これにより控訴人らのプライバシー権が侵害され、あるいはその侵害の具体的、かつ急迫の危険がある場合には、これを回避するために住基ネットからの離脱請求権が認められる旨を主張、権利侵害あるいはその危険を排除するため、住民票コードの削除及び本人確認情報を大阪府知事に通知することの差止めを求めた。

（2）判旨（一部認容、その余の追加請求棄却）

①プライバシーの権利

控訴審は、一般論として、プライバシーの権利について、「他人に自己の私的な事柄を

69) 大阪高判平成18年11月30日民集62巻3号777頁。

70) 宇賀克也「判例で学ぶ行政法 第21回住基ネット制度の合憲性(1)」自治実務セミナー52巻7号49頁参照。

みだりに第三者に公表されたりしない私生活上の自由としてのプライバシーの権利は、人の人格的自律ないし私生活上の平穩の維持に極めて重要なものというべき」とし、「人格権の一内容として憲法第13条により保障されると解するのが相当である」と判示した。その上で、「情報化社会が進展している今日においてはコンピュータによる膨大な量の情報の収集、保存、加工、伝達が可能となり…人は自己の個人情報が他者によってどのように収集、利用等されるかについて予見、認識することが極めて困難となっている」との見解を述べた。

控訴審は、第一審では言及しなかった「自己情報コントロール権」について、次のように説明し、自己情報コントロール権が憲法第13条によって保障されることを認めた。「自己のプライバシーに属する情報の取扱い方を自分自身で決定することが極めて重要」であり、「自己のプライバシーに属する情報の取扱いについて自己決定する利益（自己情報コントロール権）は、憲法上保障されているプライバシーの権利の重要な一内容となっているものと解するのが相当である」。

②本人確認情報のプライバシー性

控訴審は、本人確認情報のプライバシー性を一律に判断せずに、基本4情報と住民票コード及び変更情報について、プライバシー性を分けたうえで、それぞれの判断を行っている。

本人確認情報のうちの4情報については、「人が他者との関わりを持つ社会生活の基礎となる個人識別情報であって、個人の私的情報ではあるが、同時に公共領域に属する個人情報であるといえるものであり、もともと秘匿性の高いものとは言えない」と述べ、「住基ネット導入以前から何人も本人の同意なく閲覧でき（住基法第11条）、交付（住基法第12条）が請求できていた点も秘匿性が高くない」と判断した理由としている。

しかし、変更情報については、本人確認情報について変動が生じた場合に、「住民票の記載の修正を行った旨」の記載が行われ、婚姻、離婚等の具体的内容が記載されるわけではないが、「氏の変更は身分関係に変動があったことを推知させることになることから、秘匿の必要性も軽視できないといえる」と言及している。また、住民票コードに関しては、「それ自体は数字の羅列に過ぎない技術的な個人識別情報であるが、住民票コードが記載されたデータベースが作られた場合には、検索、名寄せのマスターキーとして利用できることから、その秘匿の必要性は高度であるといえる」として、第一審判決とは明らかに評価が異なっている。

さらに控訴審は、「一般的には、秘匿の必要性の高くない4情報や数字の羅列にすぎない住民票コードについても、その取扱い方によっては、情報主体たる個人の合理的期待に反してその私生活上の自由を脅かす危険を生ずることがある」として、「本人確認情報はいずれもプライバシーに係る情報として、法的保護の対象とな」として、「早稲田大学江沢講演会名簿提出事件（最判平成15年9月12日）」を引用し、自己情報コントロール権の対象となるというべきである」と評価した。

もっとも、控訴審は、プライバシーに係る情報の中でも、人格的自律に直接関わるよう

な秘匿の必要性の高い情報（固有情報）と、そこまでの秘匿の必要性のない情報（外延情報）が存在し、公権力との関係でみれば行政目的の実現のために必要な範囲で個人識別情報として収集、保有、利用等の必要性があることも認めている。

そこで、控訴審は、次の判断基準を明示した。**【1】**「本人確認情報の収集、保有、利用等については、それを行う正当な行政目的があり、それらが当該行政目的の実現のために必要であり」、かつ、**【2】**「その実現手段として合理的なものである場合には、本人確認情報の性質に基づく自己情報コントロール権の内在的制約により（あるいは、公共の福祉による制約により）、原則として自己情報コントロール権を侵害しないと解するのが相当」であるが、本人確認情報の漏えいや目的外利用等による、住民のプライバシーないし私生活上の平穏が侵害される具体的危険がある場合には、上記 **【2】** の実現手段として合理性がないものとして、自己情報コントロール権を侵害することになり、住基ネットによる当該本人確認情報の利用の差止めをすべき場合も生じるものと解される」というものである。

【1】 は、行政目的の正当性及び必要性について、**【2】** はその実現手段としての合理性の判断である。さらに合理性判断は、本人確認情報の漏えいの危険性の有無とデータマッチング等の危険性の有無とについて、それぞれ判断が行われている。

③行政目的の正当性及び必要性

控訴審は、「行政事務の効率化（経費削減）がどの程度実現できるかについては不透明なところがある」と述べながらも、行政目的の正当性及び必要性については、住基ネットの導入により、「住民サービスの向上及び行政事務の効率化に役立つところがあることも否定できない」として、行政目的の正当性及び必要性を是認している。

④本人確認情報の漏えいの危険性の有無（手段の合理性判断1）

本人確認情報の漏えいの危険性の判断について、控訴審は、住基ネットに関するシステムのセキュリティ面、人的側面について詳細な検討を行っている⁷¹⁾。セキュリティについては相当嚴重であること、人事管理等運用基準も定められ実施されていること等を評価し、「現時点において、住基ネットのセキュリティの不備で、本人確認情報に不当にアクセスされたりして、同情報が漏えいする具体的危険があるとまで認めることはできない」と評価した。

⑤データマッチング等の危険性の有無（手段の合理性判断2）

ところが、データマッチング等の危険性については、その危険性が相当あるものと認められると指摘している。行政機関個人情報保護法は、第3条第3項⁷²⁾において、保有個人

71) システムのセキュリティ面の検討としては、例えば、通信の認証、暗号化措置、不正通信の遮断及び監視措置住基ネットが管理される環境等、である。人的側面としては、適正な人事管理、アクセス権限の限定、担当職員の教育、研修等である。

72) 同法第3条は、個人情報の保有の制限に関する規定である。同条第3項は、「行政機関は、利用目

情報の利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲内の利用目的の変更を許容しているのだが、控訴審は、この利用目的の変更が「一種の目的外利用ということができる」と指摘した。

そして、「利用目的以外利用・提供が恒常的に行われる場合には、同法第3条第3項に基づく利用目的の変更該当し、臨時的に行われる場合は、同法第8条第2項⁷³⁾に基づく利用目的以外の目的・提供に該当するが、その変更された目的による利用や提供については、同法第8条第3項⁷⁴⁾のような規定は置かれていないから、住基法第30条の34⁷⁵⁾の違反にはならないことになる」との解釈を行った。そして、「行政機関の裁量によって行われるそのような目的変更による利用、提供について、適切な監視機関は置かれていない」ことを問題視した。

さらに、行政機関個人情報保護法第8条第2項第2号及び第3号は、行政機関が法令の定める事務等の遂行に必要な限度で、かつ、相当の理由のあるときは、利用目的以外の目的のために保有個人情報を利用し又は提供できる旨定めているが、「上記の『必要な限度』、『相当な理由』等の要件の有無は、行政機関が自ら判断するのであるから、実際には、実効性のある利用制限の歯止めになり得」ないと指摘して、結論として次のとおり判示した。

「以上の諸点を考慮すれば、住基ネット制度には個人情報保護対策の点で無視できない欠陥があるといわざるを得ず、行政機関において、住民個々人の個人情報が住民票コードを付されて集積され、それがデータマッチングや名寄せされ、住民個々人の多くのプライバシー情報が、本人の予期しない時に予期しない範囲で行政機関に保有され、利用される危険が相当あるものと認められる。そして、その危険を生じさせている原因は、主として住基ネット制度自体の欠陥にあるものといえることができ、…上記の危険は、抽象的な域を超えて具体的な域に達しているものと評価することができ」とし、「住基ネットは、その行政目的実現手段として合理性を有しないものといわざるを得ず、控訴人らの人格的自律を著しく脅かすものであり、住基ネットの行政目的の正当性やその必要性を考慮しても、控訴人らのプライバシー権（自己情報コントロール権）を著しく侵害する」ものであり、当該侵害行為は、憲法第13条に違反すると判示している。そして、差止請求のうち、住民票コードの削除についてはこれを認容し、大阪府知事に対する本人確認情報の通知の差止請求は棄却した。

的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない」と定める。

73) 同法第8条は、利用及び提供の制限に関する規定である。同条第2項は、「行政機関の長は、次の各号のいずれかに該当すると認めるときは、利用目的以外目的のために保有個人情報を利用し、又は提供することができる」と定める。

74) 同条第3項は、「前項の規定は、保有個人情報の利用又は提供を制限する他の法令の規定の適用を妨げるものではない」と定める。

75) 本条は改正されており、現行法第30条の29に該当する（受領者の本人確認情報等の利用及び提供の制限）。

3. 最高裁判所第一小法廷平成20年3月6日判決⁷⁶⁾

（1）事案の概要

控訴審判決に不服があるとして、吹田市と守口市が上告及び上告受理の申立てを行ったのが本事案である。

（2）判旨（破棄自判）

控訴審の判断に対して、最高裁は、次の理由からこれを是認することはできないと述べている。

①憲法第13条が保障する私生活上の自由

「憲法第13条は、国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定しているものであり、個人の私生活上の自由の一つとして、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ものと解される」とし、「京都府学連事件大法廷判決」⁷⁷⁾を引用して、住基ネットが被上告人らの上記の自由を侵害するか否かを検討している。

②本人確認情報の性質、秘匿性の程度について

住基ネットによって管理、利用等される本人確認情報の秘匿性について、最高裁は、「氏名、生年月日、性別及び住所から成る4情報に、住民票コード及び変更情報を加えたものにすぎない」との見解を示した。それに加えて、「このうち4情報は、人が社会生活を営む上で一定の範囲の他者には当然開示されることが予定されている個人識別情報である」であり、「変更情報も、転入、転出等の異動事由、異動年月日及び異動前の本人確認情報にとどまるもので、これらはいずれも、個人の内面に关わるような秘匿性の高い情報とはいえない」という。

また、これらの情報は、住基ネットが導入する以前から、住民票の記載事項として、住民基本台帳を保管する各市町村において管理、利用等されるとともに、法令に基づき必要に応じて他の行政機関等に提供され、その事務処理に利用されてきたものである」と説明している。

住民票コードについては、「住基ネットによる本人確認情報の管理、利用等を目的として、都道府県知事が無作為に指定した数列の中から市町村長が一つを選んで各人に割り当てたものであるから、上記目的に利用される限りにおいては、その秘匿性の程度は本人確認情報と異なるものではない」と述べて、本人確認情報の秘匿性について、いずれも秘匿性は高いものとはいえないと評価した。

76) 前掲注13)。

77) 最判昭和44年12月24日刑集23巻12号1625頁。

③システム技術又は法制度上の不備による具体的危険について

控訴審は、住基ネット制度自体に欠陥があり、データマッチングや名寄せの危険性が抽象的域を超え、具体的危険の域に達していると判断したが、最高裁は、この点について次の理由を挙げて、控訴審の判断を破棄した。その理由は、「(原審の適法に確定された)前記事実によれば、住基ネットによる本人確認情報の管理、利用等は、法令等の根拠に基づき、住民サービスの向上及び行政事務の効率化という正当な行政目的の範囲内で行われているものということができる。住基ネットのシステム上の欠陥等により外部から不当にアクセスされるなどして本人確認情報が容易に漏えいする具体的な危険はないこと、受領者による本人確認情報の目的外利用又は本人確認情報に関する秘密の漏えい等は、懲戒処分又は刑罰をもって禁止されていること、住基法は、都道府県に本人確認情報の保護に関する審議会を、指定情報処理機関に本人確認情報保護委員会を設置することとして、本人確認情報の適切な取扱いを担保するための制度的措置を講じていること」である。そして、「(上記諸点に照らせば)住基ネットにシステム技術又は法制度上の不備があり、そのために本人確認情報が法令等の根拠に基づかずには又は正当な行政目的の範囲を逸脱して第三者に開示又は公表される具体的な危険が生じているということもできない」。

④住基法第30条の34と行政機関個人情報保護法の法適用について

最高裁は、控訴審が判断した住基法第30条の34と行政機関個人情報保護法第3条第3項及び第8条第2項第2号及び第3号の法適用の解釈に誤りがあると述べている。曰く、「原審は、行政機関個人情報保護法によれば、行政機関の裁量により利用目的を変更して個人情報を保有することが許容されているし、行政機関は、法令に定める事務等の遂行に必要な限度で、かつ、相当の理由のあるときは、利用目的以外の目的のために保有個人情報を利用し又は提供することができるから、同法の規定に基づき利用目的以外の目的のために保有個人情報を利用し又は提供する場合には、本人確認情報の目的外利用を制限する住基法第30条の34に違反することにはならないので、同法による目的外利用の制限には実効性がないという原審の判断には法適用の解釈に誤りがある」として控訴審の判断を否定した。その理由は次のとおりである。「行政機関個人情報保護法は、行政機関における個人情報一般についてその取扱いに関する基本的事項を定めるものであるのに対し、住基法第30条の34等の本人確認情報の保護規定は、個人情報のうち住基ネットにより管理、利用等される本人確認情報につきその保護措置を講ずるために特に設けられた規定であるから、本人確認情報については、住基法の保護規定が行政機関個人情報保護法の規定に優先して適用されると解すべきであって、住基法による目的外利用の禁止規定に実効性がないとの原審の判断は、その前提を誤るものである」と判示した。その上で、データマッチング等による具体的危険の有無について、現行制度では次の事実が明らかであるから具体的危険が生じているということとはできない、としたのである。

すなわち、「データマッチングは、本人確認情報の目的外利用に当たり、それ自体が懲戒処分の対象となるほか、データマッチングを行う目的で個人の秘密に属する事項が記録

された文書等を収集する行為は刑罰の対象となり、さらに、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、現行法上、本人確認情報の提供が認められている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機関又は主体は存在しないこと」とし、具体的危険が生じないといえるに足る前提事実を確認している。

⑤結論

「行政機関が住基ネットにより住民である被上告人らの本人確認情報を管理、利用等する行為は、個人に関する情報をみだりに第三者に開示又は公表するということとはできず、当該個人がこれに同意していないとしても、憲法第13条により保障された上記の自由を侵害するものではないと解するのが相当である」。

なお、上記結論に続いて、最高裁は、次のようにも判示している。「また、以上に述べたことからすれば、住基ネットにより被上告人らの本人確認情報が管理、利用等されることによって、自己のプライバシーに関わる情報の取扱いについて自己決定する権利ないし利益が侵害されたとする被上告人らの主張にも理由がないものというべきである」。