

個人番号制度の法的課題（下）

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、第71巻第4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（以上、本号）

4. 考察

住基ネット関連訴訟は全国各地で多数提起され、社会的にも関心の高い事件であったことは周知のとおりである。結果的には、2008年3月6日最高裁第一小法廷合憲判決により、住基ネット関連訴訟に終止符が打たれることになる。

ここでは、住基ネットの合憲性について、対照的な判断をした控訴審判決と最高裁判決とを比較し、それぞれの判断理由を確認しながら検討する。

（1）憲法上保障される権利

控訴審は、現代の情報化社会においては、自己の情報をコントロールする権利（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正面から肯定したのに対して、最高裁は、自己情報コントロール権について憲法上保障されるか否かについての言及をしていない⁷⁸⁾。最高裁は、先例として「京都府学連事件大法廷判決」⁷⁹⁾を引用し、「憲法第13

78) 最高裁が、本判決で自己情報コントロール権に言及しなかったのは、当該権利が憲法上保障され得

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ひとつとして、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」と述べるにとどまっている。

プライバシーの権利については、佐藤幸治教授が提唱した自己情報コントロール権または情報プライバシー権（以下「自己情報コントロール権」という）が通説的見解である。佐藤教授は、プライバシーの権利を、「個人が道徳的自律の存在として、自ら善であると判断する目的を追求して、他者とコミュニケーションし、自己の存在にかかわる情報を開示する範囲を選択できる権利」と述べている。そして、「このような理解からは、プライバシーの権利として法的保護の対象とされるべき『情報』は個人の心身の基本に関する情報（いわゆるセンシティブ情報）、すなわち、思想、信条、精神、身体に関する基本情報、重大な社会的差別の原因となる情報」であり、「これを『プライバシー固有情報』と呼び、公権力がかかる情報を収集し、あるいは利用ないし対外的に開示することが原則として禁止されると解する」という。また、「これ以外の情報、すなわち道徳的自律性に直接かわらない外的事項に関する個別的情報（筆者はこれを『プライバシー外延情報』と呼ぶ）を、公権力が正当な政府目的のために、正当な方法を通じて収集・保有・利用しても、直ちにはプライバシーの権利の侵害とはならない。しかし、このような外延情報も悪用されまたは集積利用されるとき、個人の道徳的自律の存在に影響を及ぼすものとして、プライバシーの権利侵害の問題が生ずる。“データ・バンク社会”の問題は、まさにこれである」と指摘している⁸⁰⁾。

佐藤説の立場を採れば、住基ネットにおける本人確認情報は、プライバシー外延情報に該当するであろう。また、原告らが第一審で主張していた「公権力から監視されない権利」の問題は、外延情報が悪用され又は集積利用されることを想定とした「データ・バンク社

る権利ではないことを明示的に否定せず、黙示的に否定した趣旨であったと解することもできるとする見解もある。「もっとも、本判決があえて原判決と異なる判断枠組みを採用していること、『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』については明示的に憲法上の人権として認める判断をしていることとの対比からすれば、少なくとも、原判決が肯定したところの、行政機関による個人識別情報の管理、利用等に同意するか否かを自ら決定する権利という内容の『自己情報コントロール権』については、憲法上の人権とは認められないとの判断を前提にしたものとも解される」（増森珠美「最高裁判所判例解説（平成20年3、7月分、平成21年1、2、10月分）」曹時62巻11号170頁。

79) 前掲注77)。

80) 佐藤幸治『現代国家と人権』（有斐閣、2008年）489～490頁）。また、佐藤教授は、「学説やアメリカの判例の中には、個人的事柄を自ら決定することができるという『自己決定のプライバシー権』と称すべきものや、『ひとりで居させてもらいたいという権利』に最も近い『静穏のプライバシー権』と称すべきものをも、プライバシーの権利に含めて観念するものがある。が、権利はその内実が明確で同質的であることを本来の性質とするものと解され、また、後2者の多くは次に述べる人格的自律権（自己決定権）の問題として捉えることができるから、プライバシーの権利は『情報プライバシー権』の意味に限定するのが妥当と解される」との見解を述べている（佐藤幸治『日本国憲法論』（成文堂、2011年）182頁）。

会」に関わる問題として捉えることができる。

佐藤説は、プライバシーの権利を自己情報コントロール権として提唱し、法的保護の対象となる情報を固有情報と外延情報とに分け、保護の程度を区別した点で重要な意義を持つ学説であり、今日の通説的地位を占めるが、しかし、プライバシーの権利についての学説の統一的な見解は未だ見られない⁸¹⁾。

最高裁は、本判決においても、憲法第13条が「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」を有するとは認めているものの、自己情報コントロール権について言及しておらず、判断を避けたとの批判もあり得る。しかし、被上告人らの請求内容は、自己の住民票コードの削除が認められるかどうかという点が争点のひとつとなっている。つまり、被上告人らは、自らの本人確認情報に関して同意を得ずに住基ネットで利用されることがプライバシーの侵害に当たるとする主張に基づいて住民票コードの削除を請求していたのだが、その実質的な要求内容は、住基ネットに接続されないとする防御権としての請求であったように思われる。そのため最高裁は、本件審査の判断過程において、自己情報コントロール権に言及する必要性がなかったのではないかと考えられる⁸²⁾。そうだとすると、最高裁は、自己情報コントロール権を全面的に否定する趣旨ではなく、本判決に関する限り、被上告人らが自己情報コントロール権を主張するに足る実質的な「理由がない」と述べたに過ぎないと考えることも可能であろう⁸³⁾。それだけに、

- 81) プライバシーの権利を巡る代表的な見解として、「他者による評価の対象となることのない生活状況または人間関係が確保されている状態」がプライバシーそのものであるとし、プライバシー権をこうした状態に対する「正当な要求または主張」であると理解する学説として、阪本昌成『プライバシー権論』（日本評論社、1986年）4頁以下。その他にプライバシーを「『人間が多様な社会関係に依拠して、多様な自己イメージを使い分ける自由をプライバシーと呼ぶ』（自己イメージのコントロール権）」と構成する学説として、棟居快行『人権論の新構成』（信山社、1992年）190頁。プライバシーの程度を区別し、それに依じた違憲審査の基準となるべきことを説示する学説として、「個人情報」は、①だれが考えてもプライバシーであると思われるもの、②一般的にプライバシーと考えられるもの、③プライバシーに該当するかどうか判然としないもの、に大別できるとし、「①は人の人格的生存の根源にかかわるので、最も厳格な審査基準（目的は必要不可欠な『やむにやまれぬ利益』で、手段はその目的を達するための必要最小限度のものに限定される旨を要求する基準）によって、②等の情報については、原則として『厳格な合理性』の基準（立法目的が重要なものであり、規制手段が目的と実質的な関連性を有することを要求する基準）を用いるのが妥当ではないか、と解される」芦部信喜著・高橋和之補訂『憲法〔第6版〕』（岩波書店、2017年）125頁。
- 82) 本件審査を解説するものとして、「自己情報コントロール権という理論構成を必ずしも必要な」く、「原審判決と最高裁判決の結論の差異は、自己情報コントロール権説の採否の有無によるものではないと考えられる」（宇賀克也「判例で学ぶ行政法～住基ネット制度の合憲性(2)」自治実務セミナー52巻8号44頁）。その他に「自己情報コントロール権説を採用することが結論に及ぼす影響は、必ずしも大きいとはいえない」（岡村久道「住基ネット関連判例の研究（下）」NBL 816号33頁）や、「判例の趨勢は、憲法13条によって保障されるプライバシーの権利に「自己情報コントロール権」が含まれると考える方向にある。したがって、判決の結論の分岐は、自己情報コントロール権を認めるかどうかによるものではないといえる」（右崎正博「住基ネット関連判例の総合的研究」法時79巻12号89頁）等がある。

再び自己情報コントロール権が争点となる訴訟が提起された場合にまで本判決の射程が及ぶと考えるのは、些か早計ではないだろうか。

（２）本人確認情報の秘匿性判断の構造

両判決とも、本人確認情報がみだりに第三者に開示又は公表されてプライバシーを侵害するかどうかについて具体的な検討を行っており、憲法第13条の保護の対象となると考えて良いだろう。

控訴審は、本人確認情報のうち氏名等の基本4情報は、個人の私的情報であるが、同時に公共領域に属する個人情報であると述べている。個人の私的情報であっても公共的に用いられるものは、もともと秘匿性の程度は高いものとはいえないとの前置きをした上で、しかし他方で、例えば、ストーカー被害に遭っている人からすれば基本4情報は秘匿の必要性が高いとも述べており、秘匿の必要性を一律に評価するのではなく、個別の事情によっても異なることを示唆している。さらに、本人確認情報のうち変更情報については、身分関係の変動を推知させる可能性があり、秘匿の必要性を軽視できないとしている。

本人確認情報のうち最も評価が分かれたのは、住民票コードである。控訴審は、住民票コードについて、それ自体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、データベースの検索や個人に関する情報を名寄せするためのマスターキーとして利用できるものであるから、その秘匿の必要性は高度であると評価した。控訴審は、個人に関する情報であっても情報の性質やその機能に着目して、一律に秘匿の必要性を判断すべきではないことを明らかにした。これに対して、最高裁は、本人確認情報を秘匿性の高い情報とはいえないと結論づけている。

番号制度においては、個人番号と紐付けされた符号を用いて情報連携が行われるが、番号法で扱われる個人情報には、例えば、戸籍関係や預貯金口座の個人情報等、本人確認情報以上に他人に知られたくないと通常感じる情報も扱われる。したがって、最高裁が示した住民票コードに関する情報の秘匿性判断の基準がそのまま番号制度においても妥当するとは考え難い⁸⁴⁾。

しかしながら、最高裁が示した情報の秘匿性判断の「構造」は、番号制度において一定の影響が及ぶのではないかと考えられる。例えば、個人に関する情報について、個別の事情（例えば、ストーカーやDV被害に合っている等の個人の事情）を主張、立証していない場合には、次のような判断が採られるのではないだろうか。

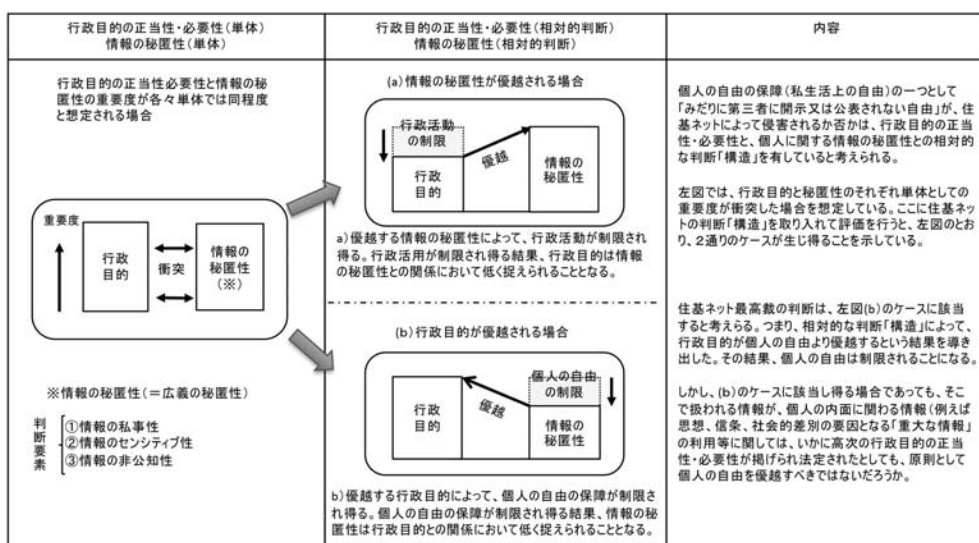
83) 調査官解説によると、自己情報コントロール権を主張する被上告人らに対し、理由がないと判示して、これを排斥したことの意味は、「コントロールする権利等を肯定する余地を完全に否定したものではないが、少なくとも、個人識別情報等の個人情報一般について、その管理、利用等に同意するか否かを自ら決定する権利（同意権）を広く肯定する見解は採用しなかったものと解される」（増森・前掲注78）170頁）。

84) 宇賀・前掲注82) 47頁には、「社会保障、税、災害対策の分野で個人番号と紐付けされた符号を用いてデータマッチングが行われるから、漏えいした場合の危険は、住民票コードよりもはるかに大きいといえ、その意味で秘匿性の程度は、住民票コードを上回るといえる」との記述がある。

第一に、最高裁は、本人確認情報の管理、利用等について「(…) 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」と述べている。この点、最高裁は、行政目的の正当性・必要性の判断に関して、根拠規定の存在、すなわち「法令等」で利用範囲が定められていること（正当性）、及び「住民サービスの向上及び行政事務の効率化」が認められること（必要性）、これらの観点から本人確認情報の管理、利用等について正当な行政目的の範囲内で行われていると述べており、個人に関する情報の管理、利用を評価するにあたり、「法令等」の根拠、及び目的の必要性が考慮要素となり、判断が行われ得る⁸⁵⁾。

第二に、管理、利用等される情報の秘匿性の判断は、行政目的の正当性・必要性和関連性があり、その関連性は図10のように想定され得る。

そこで、最高裁による本人確認情報の判断過程を情報の秘匿性（＝広義の秘匿性）の判断要素との対比で確認する（図10参照）。



【図10：行政目的の正当性・必要性和情報の秘匿性の関係】⁸⁶⁾

85) 本判決を、「住基ネットによる本人確認情報のやり取りが、『〔①〕 法令等の根拠に基づき、〔②〕 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』点を指摘し、それが『わけもなく』、『むやみに』なされるものでないこと、すなわち、(少なくとも建前上は)『みだりに……開示又は公表されない自由』を侵害するものではないことを論証している」と評価する見解がある（山本龍彦「番号制度の憲法問題——住基ネット判決から考える」法教397号51頁）。

86) 「重大な情報」(図10)とは、自己情報コントロール権説でいうところの「プライバシー固有情報」を、あるいは、「だれが考えてもプライバシーであると思われるもの」に相当する情報のことを意味している（芦部・前掲注81) 125頁）。自己情報コントロール権説では、公権力が、「プライバシー固有情報」を収集、利用等を行うことは、原則として禁止される。また、芦部説では、「だれ

本人確認情報のうち、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り（図10情報の秘匿性（①，②評価）（以下「図10情報の秘匿性」を省略する））、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（①，②評価）、これらはいずれも、個人の内面に関わるような秘匿性の高い情報ではないこと（①，②評価）、これらの情報は、住基ネットが導入される以前から、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、その事務に利用されてきたものであること（③評価）、そして、住民票コードは、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を選んで各人に割り当てたものであること（①評価）とし、「上記目的に利用される限りにおいては」との留保を付けながらも、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（②評価）と判断した。このような最高裁の判断は、基本4情報及び変更情報と住民票コードの秘匿性を一律に評価したようにみえる。

けれども、最高裁が、「上記目的に利用される限りにおいては」との留保を付けている点に着目すれば、最高裁は、住民票コードの評価について、行政目的の正当性・必要性との相対的な判断を行ったと考えられる。そして、住基ネットの場合、個人に関する情報の秘匿の必要性よりも行政目的が優越される場合として（図10）、本人確認情報の秘匿性が判断されたのではないだろうか。

以上のとおり、最高裁判決における本人確認情報の秘匿性判断の「構造」を考察してきた。翻って最高裁が示した個人に関する情報の秘匿性の判断の「構造」とは、どのようなものだったのだろうか。ここで今一度、本人確認情報の秘匿性の程度に関する最高裁判決を参照しつつ整理しておきたい。

まず、最高裁は、本人確認情報を①「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」と述べている。これは、扱われる個人に関する情報それ自体の秘匿性を評価している。続いて、②「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」と評価している。この評価は、当該4情報が社会通念上一定の範囲の他者に

が考えてもプライバシーであると思われるもの」については、「人の人格的生存の根源にかかわるので、最も厳格な審査基準によって、合憲性を判断しなければならない」と説く（芦部・前掲注81）125頁）。芦部は、厳格審査基準の事例として、前科照会事件最高裁判決（最判昭和56年4月14日民集35巻3号620頁）における伊藤正己裁判官補足意見を紹介する。伊藤正己裁判官曰く、「前科等は、個人のプライバシーのうちでも最も他人に知られたくないものの一つであり、……公開が許されるためには、裁判のために公開される場合であつても、その公開が公正な裁判の実現のために必須のものであり、他に代わるべき立証手段がないときなどのように、プライバシーに優越する利益が存在するのでなければならず、その場合でも必要最小限の範囲に限って公開しうるととどまるのである」と述べている。

当然開示が予定されているものであるという認識に基づいている。この最高裁の認識からは、個人に関する情報であっても絶体的な保護が得られるのではなく、社会通念上、一定の範囲の他者に開示が予定される情報があり得るという認識が窺える。さらに最高裁は、4情報に変更情報を加えたこれらの情報について、③「住基ネットが導入する以前から、(…)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」とし、当該本人確認情報が従前から扱われてきた既存の情報であると評価した（情報の既知性ないし公知性）。そして、住民票コードの秘匿性については、④「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、(…)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」と述べている。ここで最高裁が、「上記目的に利用される限りにおいては」と注意深く目的による限定を加えていることから、行政目的の正当性・必要性和情報の秘匿性は相対的に判断され得ることが示唆されている。

このように捉えると、住基ネット訴訟において最高裁が示した判断には、対象となる情報それ自体の性質のみから秘匿性の判断を行うのではなく、行政目的の正当性・必要性和情報の秘匿性を相対的に判断するという「構造」を見出すことができる。

番号制度においては、本人確認情報よりセンシティブ性の高い情報が扱われる。それゆえに行政目的の正当性や必要性は、住基ネット以上の具体的、かつ、高次の目的が求められるべきである。けれども、扱われる情報が、たとえセンシティブ性の高い情報であったとしても、そのことから直ちに違法性、違憲性の評価を受けることにはならないであろう。なぜなら、情報の秘匿性の程度は、行政目的の正当性・必要性和との相対的な判断「構造」において、当該情報の秘匿性が評価され得るからである⁸⁷⁾。したがって、個人に関する情

87) 最高裁が判示した本人確認情報の要保護性の判断に批判的見解がある。例えば、「本人確認情報のなかで特に変更情報や住民コードを他の四情報と特段区別しないで、その役割や機能、その結果としてのプライバシー保護の程度を丁寧に吟味することをしておらず、またこれらの情報を個別に切り離し、住民票コードも含め本人確認情報が全体として住基ネットのシステムの中でどう利用され、扱われるのかの観点も欠落している」とし、「ここで肝要なのは、本人確認情報の内容面の要保護性そのものというより、住基ネットによりこうした個人情報にコンピュータネットワークで繋がれ、管理、運用され、住民票コードを媒介に行政機関が他のデータベースに集積された個人情報と簡単にデータマッチングされる条件と前提が技術的に構築されているというその役割や機能である」（田島泰彦「最高裁住基ネット合憲判批判」法時80巻6号3頁以下）。

確かにこの点に関しては、控訴審判決は詳細に検討が行われていた。しかし、最高裁も無条件に認めているとは思えない。なぜなら、最高裁は、住民票コードの秘匿性について、本人確認情報と異なることの理由について、「住民票コードは、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、(…)上記目的に利用される限りにおいては、その秘匿性は本人確認情報と異なるものではない」（傍点筆者）と述べているので、法令の定める範囲内で管理、利用等がなされることを前提の下に秘匿性の評価をしており、法令違反を承知で目的外利用が行われる場合の住民票コードの利用の危険性を考慮する必要性が現時点では無いと判断しただけではないかと思われる。また、「住基ネットによって本人確認情報が『みだりに第三者に開示又は公表』されることはないとしても、意図せざる情報漏洩と不正利用のリスクはゼロにはならない。(…)最高裁もこれらのリスクを否定していない。ただ、現時点ではそれを『具体的危険』と見なすことはできないと判断

報の管理、利用等に関し、その根拠を法令等で定め、形式的な高次の行政目的を規定した場合、扱われる情報が、たとえセンシティブ性の高い情報であってもその秘匿性の程度は、高次の行政目的との関係において相対的に変化し得るのであり、その意味では、行政目的の正当性・必要性の評価が非常に重要ということになる。

前述したとおり、番号法は、立法者自身による利用範囲の拡大に関する縛りが必ずしも固くない法制度である。それだけに今後、番号制度で扱われることになる情報の秘匿性が前記のような判断の「構造」で審査されるとすれば、例えば、個人の内面に關わるような「重大な情報」⁸⁸⁾の場合には、行政事務の効率化や国民の利便性の向上といった概括的な目的だけではなく、より具体的な高次の行政目的、それを支える立法事実の存在、目的を達成するための必要性や手段の相当性については厳しく問われなければならないであろう⁸⁹⁾。

(3) 具体的危険の判断

控訴審と最高裁判所の結論が大きく分かれたのは、具体的危険の判断であろう。控訴審は抽象的危険性の域を超えて具体的危険が生じていると判断した。その大きな理由は、行政機関個人情報保護法と住基法の適用関係に関する解釈の点にある。控訴審は、住基ネットによって、取り扱われる本人確認情報も個人情報に該当し、行政機関個人情報保護法と住基法の双方の適用があるとの解釈を行った。控訴審の解釈では、行政機関個人情報保護法は、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こと、行政機関は、法令に定める事務の遂行に必要な限度、かつ、相当の理由があるときは、利用目的以外の目的のために個人情報を利用、提供することが認められていること、そして、同法の定めに即して行われる本人確認情報の目的外利用については、住基法第30条の34が定める目的外利用の禁止規定に違反することにはならないことから、住基法第30

しただけである」と指摘する見解がある（松本和彦「住基ネットと憲法13条」法学教室編集室編『判例セレクト2001～2008』（有斐閣，2010年）89頁）。

88) 前掲注86) 参照。

89) この点につき、「プライバシーが侵害されたか否かは、問題の情報が個人の私的な情報か否かと同時に、問題となった具体的状況で、本人がどの範囲での流通（あるいは非流通）を合理的に想定すべきかにも依存する。個人の私的情報の保護が個人の自律のために不可欠であることを考慮すると、信条、社会的身分、病歴、犯罪歴等、特に取扱いに配慮を要するセンシティブな情報を、政府が本人の同意なく収集・利用・伝達する措置は、厳格な違憲審査に服することになり、措置が正当化されるのは、それが必要不可欠な利益を達成するための必要最小限の手段であることを政府が立証した場合に限定されるべきである」長谷部恭男『憲法〔第7版〕』（新世社，2018年）154頁が参考になる。この観点から言うと、例えば、高次の行政目的を実現するために個人の病歴や遺伝情報等を医療機関に提供する場合に、個人番号と情報連携する必然性が問われることになると思われる。政府は、明らかに関連性の少ない分野でありながらすべての個人情報を個人番号と紐付けを行って管理する必然性はどこにあるのかを説明しなければならないであろう。なぜ分野別の番号では目的が実現できないのかという問いにも答える必要がある。そこでは、共通番号である個人番号と紐付けなければならない必要不可欠な理由とは何か。目的を実現するために他の手段は存在しないのかについても説明しなければならないと思われる。

条の34の目的外利用の禁止には実効性が無いと判示し、住基ネットにより、住民票コードが付され、データマッチングされ、本人の予期しない利用等が生じうる可能性に言及し、具体的危険が有ると認めた。

これに対して、最高裁は、控訴審の法解釈には誤りがあると述べ、これを否定した。本人確認情報は、住基ネットにより管理、利用等されるための保護措置を講ずるために特に設けられた規定である点を強調し、本人確認情報については、明文の規定が無くとも、住基法中の規定が行政機関個人情報保護法の規定より優先適用されると解すべきであると反論した。さらに、最高裁は、データマッチングは、本人確認情報の目的外利用に該当し、それ自体懲戒処分の対象となること、秘密に属する個人情報を保有する職員が正当な理由無く、他の行政機関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（住基法の別表で定められている事務）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（以下「一元的管理機関という」）⁹⁰⁾は存在しないことなどを理由に控訴審が指摘した具体的危険の存在を否定している。

控訴審と最高裁では行政機関個人情報保護法と住基法の適用関係の解釈で大きく異なる結果となった。住基法は、本人確認情報の管理、利用等を法令で定める範囲に限定することで、一定の範囲内での利用にとどめ、闇雲な情報の拡散防止を図り、情報の取得後においても目的の範囲内での利用を担保するために同法第30条の34による目的外利用の禁止規定が設けられた趣旨であることからすれば、最高裁の解釈のほうが立法者の意思に即しているであろう。本人確認情報のうち基本4情報は、個人にとって私事性を有する情報であるものの、行政機関等との関係においては、行政と個人を接合するための一定の範囲で開示が必要となる公共性の高い情報であるともいえる。したがって、基本4情報は、行政目的の必要性との相対的判断から情報の秘匿性の評価は低減される。また、公知性に関して、一般的には行政機関等において従前から管理されている情報と考えられるため、その点で公知性を有するといえる。

以上のとおり、具体的危険の判断の場面では、主として行政機関個人情報保護法と住基法の適用関係が問題となったが、この点については最高裁の判断が妥当である。

ただし、問題がなかったというわけではない。最高裁は、データマッチングの危険性を否定する理由として次のようにも述べていた。「データマッチングは、本人確認情報の目的外利用にあたり、それ自体が懲戒処分の対象となること、（…）現行法上、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」である。この問題点について詳しくは第3章において言及するが、当該一元的管理機関の不存在要件が、データマッチングの危険性を否定する理由のひとつになっていることは間違いない。

けれども、この最高裁が述べた一元的管理機関の概念が不確定であり、いくつかの解釈

90) 本稿では、最高裁が述べた「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」と述べられている部分については、「一元的管理機関」と統一し、政府等が説明する「一元管理」の表現とは区別して表記する。

が考えられる。例えば、個人情報を一元的に管理する機関が存在していたとしよう。一見すると、合憲の要件に抵触するかのように見えるのだが、そう簡単には判断できない。その理由は、番号法が規定する特定個人情報ファイルの該当性判断に関する個人情報保護委員会の見解にある。

特定個人情報ファイルとは、個人番号をその内容に含む個人情報と定義される（番号法第2条第9項）。番号法上、特定個人情報ファイルの保有に関しては、指針が定められている（同法第27条）。個人番号関係事務の取扱者は、特定個人情報ファイルに該当するかどうかの判断を行い、該当する場合には指針に基づく適切な管理が求められるため、特定個人情報の該当性判断は正確に行わなければならない。

そのため、個人情報保護委員会の公式サイトには、個人番号関係事務の取扱者から、特定個人情報ファイルの該当性判断に関する質問が寄せられ、それに対する回答が公表されている。質問の内容は、「個人番号をその内容に含むデータベースを複数の事務で用いている場合、個人番号関係事務以外の事務で個人番号にアクセスできないよう適切にアクセス制御を行えば、その個人番号関係事務以外の事務においては、当該データベースが特定個人情報ファイルに該当しないと考えて良いか」⁹¹⁾ というものである。それに対する回答は、「個人番号関係事務以外の事務において、個人番号にアクセスできないよう適切にアクセス制御を行えば、特定個人情報ファイルに該当しない」⁹²⁾ という見解が示されている。

つまり、個人番号と紐付けられている個人情報ファイルに関して、個人番号関係事務に係る者には、当該ファイルへのアクセス権を設定してアクセスできるようにし、当該事務に係らない者には、当該ファイルへのアクセス権の付与を行わない。このようにファイルにアクセスできる者とできない者を権限付与によって適正にアクセス制御していれば、複数の事務で扱うデータベースの中に特定個人情報ファイルが管理されていたとしても、個人番号関係事務以外の事務においては、当該データベースは特定個人情報ファイルに該当しないというのが個人情報保護委員会の見解である。

もし、特定の行政機関が、新たにデータベースを構築し、現在分散管理している個人情報を当該データベースに集約して、管理、利用等を行うとしたなら、最高裁は当該行政機関の存在をどのように判断するだろうか。個人情報を一元的に管理する機関が存在すると判断するであろうか。前述した個人情報保護委員会の見解をそのまま採用した場合、行政目的に必要な個人情報を許された者だけが管理、利用等が行えるように適切にアクセス権を設定し、アクセス制御を行っていれば、たとえ、個人情報が物理的にはひとつのデータベースに集約されたとしても、論理的には分散的に管理している状態と等しい状態であるといえるのではないか。すなわち、物理的には一箇所に集約して一元的に管理されている状態となるものの、論理的には分散的管理であると評価することもできるのではないか。

91) 個人情報保護委員会公式サイト「特定個人情報の適正な取扱いに関するガイドライン（事業者編）及び金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関する Q2-3 参照 (<https://www.ppc.go.jp/legal/policy/faq/#seigen>)。

92) 前掲注91) A2-3 参照。

行政機関等がこのような主張をすることは十分に予想できる。

そもそも一元的管理機関という概念は、一義的に定義することは難しい概念である。例えば、データベースが物理的に各遠隔地にあって、それ自体は分散的に管理されていても、ネットワーク化され、かつ、それぞれのデータベースにアクセス可能な状態であれば、どこからでもアクセスできる点で、それは一種の一元的に配備されたデータベースともいえるし、逆に、物理的には同一のハードウェア内に集約化されたデータベースに情報が格納されていたとしても、アクセス制御が適切に講じられていれば、それは一種の分散的に管理されている状態である、とも捉えることができる。

したがって、一元的管理機関概念をどのように解釈するのか、どのように定義するのかによって、最高裁が示した一元的管理機関の不存在要件の適合性は変わり得るのである。

三．個人番号制度の法的課題

前章まで住基ネット及び番号制度の概要と住基ネット訴訟に関連する事項をみてきた。番号制度の創設に当たっては、国民ID制度の基本構想を取り込みながら、社会保障、税、災害対策分野の利用だけでなく、幅広い分野での利用を視野に入れた制度設計が進められたことを確認した。

本章では、番号制度の法的課題を考察するにあたり、住基ネット最高裁判決を参照軸として対比しながら、同制度の法的課題を以下の3つの視点から整理を行う。

第一に、番号制度と住基ネット最高裁判決の関係につき、住基ネット最高裁判決の指摘事項、番号制度の大綱に記載された同制度の要件、当該要件に対する制度上の保護措置の対応関係を説明する。

第二に、控訴審が住基ネット違憲判決で指摘した具体的危険を最高裁が否定するための要件として述べた、個人情報の一元的管理機関の不存在要件について、当該要件の不確定概念から起因する問題点を指摘する。

第三に、個人番号は、個人情報を名寄せ、収集するための検索キーになり、個人情報に関するプライバシー侵害のおそれを脅かすような存在であるのか、情報連携局面と行政内部の局面に分けて検討する。

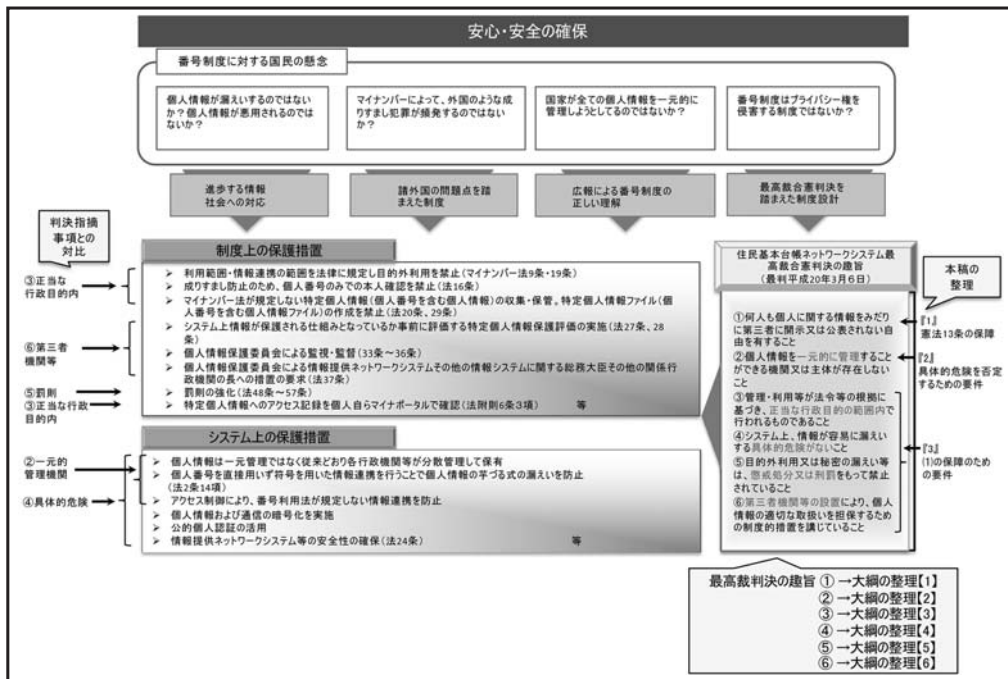
最後に、情報の受領者による情報の蓄積の問題が考えられるので、若干ではあるが今後の課題として示しておくことにする。

1．住基ネット最高裁判決と個人番号制度の関係

（1）住基ネット最高裁判決と個人番号制度の関係

前章で確認したとおり、番号制度の構築に当たっては、住基ネット最高裁判決の趣旨を十分踏まえる必要があるとし、同判決を「個人情報扱うシステムが合憲なシステムでありうるための最低限の条件」⁹³⁾と捉えて制度設計が行われている。

そこで、最高裁判決の趣旨（①～⑥）、番号制度の大綱に記載された要件（【1】～【6】）、



【図11：住基ネット最高裁判決とそれに対する保護措置】⁹⁴⁾

本稿における整理（『1』～『3』）、判決の指摘事項に対する制度上、システム上の保護措置の関係を図11に示す。本図は番号制度設計に際して、内閣官房社会保障担当室によって作成された資料をもとに番号法改正に伴い条文を改定し、筆者が加筆を加えたものである。

住基ネット最高裁判決では、①「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」と述べている（大綱の整理【1】）。その上で、上記①が保障されるためには、②「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」（大綱の整理【2】）、③「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ものであること」（大綱の整理【3】）、④「システム上、情報が容易に漏えいする具体的危険がないこと」（大綱の整理【4】）、⑤「目的外利用又は秘密の漏えい

93) 第1回個人情報保護ワーキンググループ会合では、社会保障・税に関する番号制度及び国民ID制度の導入における個人情報の保護に関する基本論点の整理を行う上で、基本的視点として、次のような発言がなされている。「最高裁の判決で、この種の個人情報を扱うシステムが合憲なシステムでありうるための条件が示されておりますので、その物差しというのは最低限押さえておかないと、後で制度として憲法違反だといわれますと、作り直さなくてはいけなくて大変無駄になりますし、ひいては住基ネットまで一体不可分で憲法違反だということになりかねません。」「第1回個人情報保護ワーキンググループ会合議事録（2011年2月7日）」19頁〔長谷部恭男座長代理発言〕（<http://www.cas.go.jp/jp/seisaku/jouhouwg/dail/gijiroku.pdf>）。

94) 内閣官房社会保障改革担当室『マイナンバー 社会保障・税番号制度』（2014年2月）14頁をもとに作成・追記した。（https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/number/dail/sankou.pdf）。

等は、懲戒処分又は刑罰をもって禁止されていること」（大綱の整理【5】）、⑥「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」（大綱の整理【6】）とする要件を掲げた。

本稿においては、住基ネット最高裁判決の分析に基づき、次のとおり整理し直した（本稿の整理）。

まず、①を保障するために（本稿の整理『1』）、④ないし⑥の要件が掲げられている（本稿の整理『3』）。次に、②の要件については、控訴審の指摘したデータマッチングの具体的危険を否定するための要件として最高裁が述べた要件であると考えられる（本稿の整理『2』）。『1』の自由が保障されるか侵害されるかの判断の過程においては、情報の秘匿性評価のみならず、行政目的の正当性・必要性の評価、及び制度の安全性評価との相対的な判断がされ得る。

したがって、『1』の自由が保障されるか、侵害されるかの判断は、情報の秘匿性評価に加え、『3』の要件が充足されるか否かが分水嶺になると考えて良いだろう。

（２）住基ネット最高裁判決と個人番号制度上の保護措置

住基ネット最高裁判決の指摘事項に対して、番号制度上の保護措置はどのように講じられているのか。大別すると制度上の保護措置とシステム上の保護措置に分類されて対策が講じられている。そこで、制度上の保護措置及びシステム上の保護措置と住基ネット最高裁判決の指摘事項を対比させた（判決指摘事項との対比）。

まず、正当な行政目的の範囲内に留められていること（③要件）については、法律によって手当てを行っている。具体的には、番号法第9条（利用範囲）及び同法第19条（特定個人情報の提供の制限）で法定した範囲内での利用及び提供に限定し、それ以外の利用及び提供を禁止している。

また、同法第20条及び同法第29条で法の規定しない特定個人情報の収集・保管及び特定個人情報ファイルの作成を禁止。特定個人情報へのアクセス記録をマイナポータルで個人が確認できる措置を講じている（附則第6条第3項）。

続いて、具体的危険がないこと（④要件）については、主に技術的措置で手当てを行っている。例えば、アクセス制御により、法が予定しない情報連携を防止し、符号を用いた情報連携を行うことにより、個人情報が漏えいしても個人情報が芋づる式に漏えいすることを防止する仕組みを採用している。その他データの暗号化や通信の暗号化を実施する等の安全保護措置を講じている。

次に、目的外利用又は秘密の漏えい等を行った者に対する罰則（⑤要件）については、番号法において懲戒処分や刑罰をもって禁止され、行政機関個人情報保護法より一段重い処分が定められている（例として、個人番号利用事務等に従事する者が、正当な理由なく特定個人情報ファイルを提供した場合、行個法では、2年以下の懲役又は100万円以下の罰金であるが（行個法第53条）、番号法は、4年以下の懲役若しくは200万円以下の罰金又は併科（番号法第48条）となっている）。

最後に、第三者機関等の設置要件（⑥要件）については、個人情報保護委員会（いわゆる3条委員会）⁹⁵⁾を設置し、監視、監督にあたらせている（同法第29条の3『委員会による検査等』、同法第29条の4『特定個人情報の漏えい等に関する報告義務』、及び同法第33条～第36条『指導及び助等』）。

番号法では、特定個人情報ファイルを保有、変更する場合に、特定個人情報保護評価の実施（同法第27条『指針』、第28条『特定個人情報保護評価⁹⁶⁾』）を義務付けている。番号制度において採用された。

このように番号制度は、法制度上もシステム上も住基ネットに比べて個人情報に関する保護措置が強化されている。これらの保護措置をみれば問題がないように思える。しかし、次の点は改めて指摘しておきたい。

第一に、正当な行政目的の範囲内であること（③要件）については、取り扱う個人に関する情報の秘匿性との相対的評価によって、求められる正当な行政目的、必要性の程度も異なってくる点である。現行法のように、「行政の効率化」や「国民の利便性の向上」という概括的な目的だけではなく、扱われる情報の性質や秘匿性の程度、利用分野の拡大によって行政機関等が保有することとなる個人情報の蓄積量に見合うだけの、具体的な高次の行政目的の正当性・必要性が求められるべきである。番号制度は、国民の社会生活に大きな影響を与える制度である。とりわけ、行政機関等が現在保有しない新たな個人情報との連携に関しては、慎重な検討が必要であろう。番号法に規定されれば、国民の自由な意思に基づく、個人情報の開示、非開示の選択の機会とは与えられず、法律によって一律に情報の開示（情報連携）が求められることになる⁹⁷⁾。それだけに、国民の側も開示の対象となる情報の性質や秘匿性等とそれに見合うだけの立法目的の正当性や必要性について、より詳細な説明を政府に求めている必要があると思われる。

第二に、住基ネット最高裁判決が述べた一元的管理機関の不存在要件（②要件）であるが、前述したように、一元的管理機関がどのような機関を意味するのかについては一義的に確定しない。この点については項を改めて述べる。

第三に、具体的危険のないこと（④要件）である。情報連携には個人番号を用いず、新たに「符号」を考案し、それを用いて情報連携を行う仕組みは、確かに個人情報保護に対して、配慮された安全性の高いシステムであると評価することができる。しかし、個人番号は行政機関等が保有する個人情報と紐付いて管理、利用等が行われる。そのため、その局面での問題点はないだろうか。この点については次節で検討する。

第四に、第三者機関等の設置（⑥要件）についてである。これについては、個人情報保護法に基づいて、個人情報保護委員会が2016年に設置された。前身は、特定個人情報保護委員会である。法改正⁹⁸⁾により、個人情報保護委員会に改組され、引き続き任務に当たっ

95) 国家行政組織法3条に基づく委員会を指す。

96) 日本版プライバシー影響評価（Privacy Impact Assessment＝PIA）とも呼ばれる。

97) 行政機関等が現在保有しない新規性のある個人情報の例としては、預貯金口座情報がある（現状は新規口座開設時の義務付け）。

ている。しかし、法制度上、問題ではないかと思われる点がある。番号法は、第19条第1号から第16号に該当する場合を除き、特定個人情報を提供できる範囲を限定している。同条第16号は、「その他これらに準ずるものとして個人情報保護委員会規則で定める」場合として、提供制限の例外を定める。そのため、個人情報保護委員会には、監視・監督のみならず、特定個人情報を提供する範囲を自ら決定する権限が与えられている。問題は、当該委任の規定が白紙委任にあたらないのかという点である。本来、法律の改正手続きを経るのが正当な手続である。個人情報保護委員会の判断で提供を認める必要性はどこにあったのか。

この点、「法律で明確に規定することが望ましいが、すべての場合を予想して網羅的に規定することは困難であることから、臨機応変に対応するために、個人情報保護委員会の判断で例外を認めることとしている」との説明がなされている⁹⁹⁾。

確かに網羅的に規定することは困難であろう。しかし、同法第19条は、同条に定める以外の提供の制限を設ける規定である。特定個人情報に関しては、扱われる個人情報が秘匿性の高い情報も扱われるのであり、本来国会の議決によって改正手続きを経ることが望ましい。臨機応変に対応するために個人情報保護委員会に制定権を認めるという説明は、十分に説得的ではないだろう。

それに加えて、個人情報保護委員会への委任立法の権限の付与について、同条第16号からは委任の趣旨や範囲を読み取ることが困難である。そもそも、同法第19条によって提供先を限定する趣旨は、「特定個人情報の提供は、提供先において個人番号と個人情報を紐付けて管理することを可能にする」が、「個人番号は、悉皆性、唯一無二性、視認性を有し、『民—民—官』で流通するものであるため、より厳格に第三者提供を制限しなければ、不正なデータマッチングが行われる蓋然性が高い」¹⁰⁰⁾ ことにある。その意味で、特定個人情報の提供先は、法律で限定しておく必要があったからであり、それを臨機応変に対応できるからという理由で個人情報保護委員会に制定権を与えることの趣旨が、この説明では明確ではないのではないか。もともと個人情報保護委員会は、個人情報（特定個人情報を含む）の適正な取扱いを担保するために設置されている。

したがって、活動の透明性を確保するためには、その権限については、原則として監督等のみを行使できる機関に限定されていることが望ましいであろう。それにも関わらず制定権をも委任するのであれば、それ相応の理由が必要となろう。それが現時点では明確でなく、同法第19条第16号の規定には問題がある¹⁰¹⁾ というべきであろう¹⁰²⁾。

98) 2015年（平成27年）法律第65号による改正。

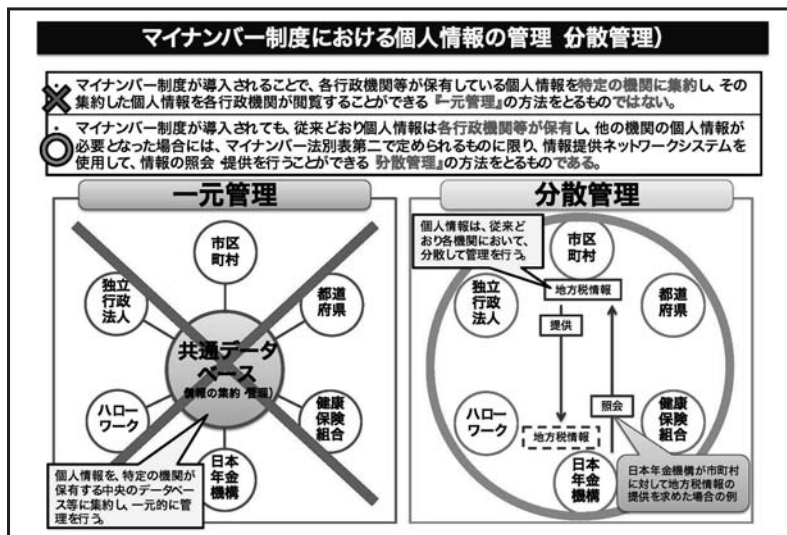
99) 宇賀・前掲注9) 127頁。

100) 宇賀・前掲注9) 107頁。

101) 山本・前掲注85) 57頁は、個人情報保護委員会の権限について、「委員会は、あくまでも法律で定められた範囲どおり番号制度が運用されていることを担保する監視機関であって、その範囲を決定する機関ではない」。また、「同機関は、立法『指針等の策定』を行う正当性を与えるものであっても、情報経路を決定・拡張する『立法』を行う正当性を与えるものではない。したがって、委員会規則のみに基づいてなされる特定個人情報の提供は、形式的根拠を欠くものとして違憲と解すべ

(3) 一元的管理機関の不存在要件

番号法上、個人情報の一元的管理を禁止する規定が設けられているわけではない。図12の説明によれば、一元管理とは「番号制度が導入されることで、各行政機関等が保有している個人情報を特定の機関に集約し、その集約した個人情報を各行政機関等が閲覧することができる」方式だという。また、分散管理とは「番号制度が導入されても、従来どおり個人情報は各行政機関等が保有し、他の機関の個人情報が必要となった場合には、番号法別表第二で定められるものにより、(…)情報の照会・提供を行うことができる」方式だという。



【図12：番号制度の個人情報の管理（分散管理）】¹⁰³⁾

ところが、図12の説明とは対照的に各自治体が保有する特定個人情報については、一見すると中央データベースのような「自治体中間サーバ・プラットフォーム」を整備して各センターに集約する構成を採り（図13参照）、各都道府県・市町村が保有する特定個人情報は、各団体内で保存され、かつ、自治体中間サーバを共同化・集約化した全国2拠点（東日

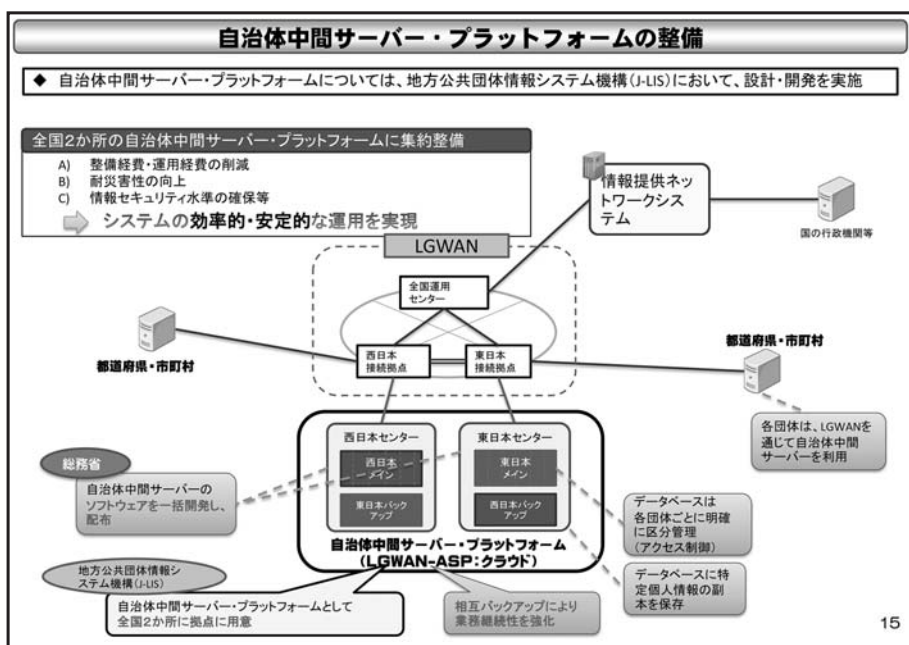
きであろう」と述べている。

102) マイナンバー訴訟が各地（九州、大阪、名古屋、横浜、東京、金沢、新潟、仙台）で係争中である。昨年、横浜地裁が原告の訴えを棄却したが（横浜地判令和元年9月26日判例集未搭載（裁判所ウェブサイト））、争点の一つとして、同法第19条第14号（政令への委任）、第16号（規則への委任）の規定が白紙委任ではないかについて判断している。結論として、委任の趣旨に反する政令や規則が制定されれば、そのことを理由に当該政令や規則は無効となるものと解されるが、同法第19条各号はいずれも政令等に白紙委任するものではないとしている。しかし同判決は、肝心の委任の趣旨について明らかにしておらず、理由として不十分であろう。

103) 内閣官房番号制度推進室・内閣府大臣官房番号制度担当室・「マイナンバー社会保障・税番号制度概要資料」（令和2年5月）20頁（<https://www.cao.go.jp/bangouseido/pdf/seidogaiyou.pdf>）。

本、西日本センター）に置かれる自治体中間サーバ・プラットフォーム（LGWAN-A SP：クラウド）のデータベースに副本として保存される。

本図で特筆すべき点は、「データベースは、各団体ごとに明確に区分管理（アクセス制御）」と明記されている点である。この説明は、住基ネット最高裁判決のいう一元的管理機関の不存在要件を意識して記述されているのではないと思われる。おそらくこの記述で説明したいことは、各センターで集約管理されていても明確に区分管理（アクセス制御）を設定することで正統なアクセスとそうでないアクセスを制御することにより、特定個人情報の一元管理には該当しない、という点を強調したかったのではないだろうか。



【図13：自治体中間サーバ・プラットフォームの整備】¹⁰⁴⁾

特定の機関に個人情報のデータベースを構築し、そこに特定個人情報を集約したとしても、アクセス権の設定により、閲覧できる機関を分散管理的に制御することは可能である。例えば、ハローワークや日本年金機構が保有する特定個人情報を、内閣府にデータベースを構築し集約したと仮定する。ハローワークの職員には、当該機関で保有していた特定個人情報へのアクセス権を付与するが、日本年金機構が保有していた特定個人情報にはアクセス権を付与しないことで、分散管理に似た管理状況を作り出すことは可能であろう。

それとは反対に、個人情報のデータベースが各機関において物理的に分散管理されてい

104) 総務省個人番号企画室「マイナンバー制度における情報連携について」(平成28年5月)15頁
(https://www.soumu.go.jp/main_content/000429540.pdf)。

たとしても、各機関のデータベースがネットワークで繋がれ、それぞれの機関から他の機関のデータベースにアクセスが可能であるとしたら、それは一種の一元的に管理されている状態といえるのではないだろうか。問題は、最高裁が述べた一元的管理機関の概念が定義の曖昧さゆえに個人情報の管理がどのような方法で管理されていると該当し、あるいは該当しないのかについて、解釈によって見解が分かれてしまう点である。

この点につき筆者なりに推察すると、最高裁は、具体的危険の存在の判断において、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、懲戒処分や刑罰をもって禁止されていることに加え、「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」を理由のひとつにしていた。したがってこの文脈からは、個人情報を何処で管理するのか（特定の行政機関に集約して管理するのか、行政機関ごとに個人情報を管理するのか）という問題は、さほど重要ではなく、目的外にアクセスできるような法制度ないしシステムであるのか、そうでないのかという点が具体的危険の存在を判断するうえで重要な観点であったと考えられる。

このように考えると、特定個人情報の管理が、図12の定義のような一元管理であるとか分散管理であるとかというよりも、むしろ、行政機関等が、他の行政機関等に保存されている特定個人情報を目的外に利用することができるような状況こそが問題とされるべき点ではないかと思われる。

換言すると、最高裁のいう一元的管理機関とは、「個人情報が一元的に管理されたデータベースに目的外に利用できる状態（したがって、この理解を前提にすれば、必ずしも特定の機関に集約されたデータベースが存在する必要はない）が現実存在すること」を意味していたのではないかと思われる。

この想定に基づくなら、一元的管理機関の非該当要件として考えられるのは、個人情報が集中して管理・蓄積されていない場合（以下「非該当要件①」という）、あるいは個人情報が集中して管理・蓄積されている場合であってもアクセス権の設定等によって、個人情報の不正な目的外利用が禁止されている場合（以下「非該当要件②」という）が考えられる。また、一元的管理機関の該当要件として考えられるのは、個人情報が集中して管理・蓄積されている場合（以下「該当要件①」という）、あるいは個人情報が分散して管理・蓄積されている場合であってもアクセス権の設定等がない、または対策が不十分である場合（以下「該当要件②」という）が考えられる。

そうであれば、たとえひとつのデータベースに個人情報を集約して管理・蓄積する方式が採られたとしても、そのことから直ちに一元的管理機関の不存在要件に抵触すると考えることは難しいのではないだろうか。適切なアクセス権の設定等、十分な保護措置を講じていれば、なお合憲と判断される余地は依然として残るように思える。

2. 個人番号の保護の必要性

（1）個人番号の保護の必要性

ここでは、個人番号をなぜ法的に保護する必要があるのか、という個人番号の保護の必要性について確認する。情報連携を行う場合、個人番号を連携するためのキーとして用いず、行政機関ごとに割り当てられた符号を用いて情報連携が行われる。情報連携を行う際は情報連携基盤において異なる符号同士を変換する処理が行われる。この仕組みを採用することにより、仮にある行政機関で情報漏えいが発見されたとしても、他の行政機関とは符号が異なっていることから、漏えいした情報から他の行政機関が保有する個人情報を探る式に漏えいされる危険性を回避している。同時に、符号による情報連携を行うことで、特定個人情報が情報連携基盤内に蓄積される状態を回避することができる。それにも拘らず、番号法上、個人番号の利用範囲の限定列挙、特定個人情報の提供の制限等、個人番号の扱いについて厳格に定めているのは、どのような理由によるものであろうか。

それは、個人番号が「悉皆性」及び「唯一無二性」の性質を有し、特定の個人を識別するための高い識別性を備えるという特徴を持つことと関係しているだろう。すなわち、個人番号は住民票を有する全ての個人に対して番号が振られ、原則として死後も含め生涯不変である。生誕から生涯を終えるまでをひとつの変わらない番号を用いて行政機関等を跨ぎ、分野横断的に個人を一意に特定することができるのが個人番号の特徴である。

住基ネットは、住民票コードという重複しない番号を住民登録のある全ての住民に対して番号を付番し、居住関係を公証する住民基本台帳をネットワーク化し、全国共通の本人確認ができるシステムとして構築された。個人情報保護に配慮し、住民からの申請に基づき住民票コードはいつでも変更可能とされている（住基法第30条の4）。住基法では、利用範囲を限定列挙し、目的外利用は禁止されている（同法第30条の29）。また、民間部門の利用も禁止されている。番号法も利用範囲を限定列挙し、それ以外の利用を禁止する点では住基法と同様である。

しかしながら、番号法第3条では、個人番号の利用に関する施策の推進を図ることを基本理念として掲げられていることから、今後も利用範囲の拡大が検討されていくことになろう。住基ネットは、居住関係を公証するための本人確認に利用するという目的のみに利用されていたのに対して、番号制度は、個人番号を様々な行政手続に利用する目的を有している。その意味では、制度創立当初から両制度はその目的が本質的に異なっている。

立法者は、番号制度の制度設計の過程で、符号による情報連携を考案し、自動処理による情報連携を行う方式を採用した。それによって、人的な要因による不正な情報連携の回避を実現している。他方で立法者は、個人番号を様々な行政手続に利用する番号として制度設計を行っており、行政機関等においては、従前の保有個人情報と個人番号を紐付けして管理することになる。その結果、行政機関等において、個人番号を不正に利用した情報連携や漏えいの危険性は高くなる。その危険性を低減するために、個人番号の取扱いについて、法律で厳格に保護をする必要がある。

番号法が、個人番号の取扱いについて、住基法より厳格に保護規定を設けた背景は、換

言すると、番号制度においては、個人情報の情報連携を行うことが重要な目的であるためである。そして、個人番号が情報連携のための検索キーとして強力な識別機能を有し、利用範囲の拡大に伴う不正な情報連携によって、個人のプライバシーを侵害するおそれが高まることを、他ならぬ立法者自身が強く認識していたからであろう。

（２）具体的危険の検討（情報連携の局面）

情報連携は番号法第19条第7号及び第8号に規定された事務において行われる。個人番号を用いずに符号において行われる情報連携の局面において、情報漏えいや不正な情報連携に対しては高い安全性を有すると考えられる。しかし本当に問題点はないだろうか。

住基ネット控訴審判決で認容された具体的危険の存在とは、不正なデータマッチングや名寄せの危険性が具体的に生じているというものであった。後に最高裁で否定されることになったが、その理由のひとつが一元的管機関の不存在という要件であった。

最高裁が言及した一元的管理機関の不存在要件については、情報連携の局面と行政内部の局面の2つの局面が考えられる。まずは、番号制度の情報連携の局面において、当該要件が充たされているかを確認する。一元的管理機関の候補としては、付番機関と情報提供ネットワークシステムが想定され得るので、以下では、それぞれに分けて確認する（図8参照）。

まずは付番機関の一元的管理機関の危険性について確認する。住民票コードは、番号法上、特定個人情報には非該当であるが（同法第2条第8項）、住基法上の規制を受ける。付番機関において、個人番号は住民票コードから不可逆暗号で生成が行われる。そのため、個人番号から住民票コードに遡ることはできない。付番機関は、住民票コード及び個人番号の双方を扱うことになるが、双方の番号を復元した形で保有することにはなっていない。したがって、少なくとも非該当要件①は充たされており、一元的管理機関の不存在要件に適合しているであろう。

続いて、情報提供ネットワークシステムの一元的管理の危険性について確認する。最初に情報連携の場面から確認する。情報提供ネットワークシステムは、情報保有機関Aから情報提供用個人識別符号を受信後、連携用符号に復号し、該当する個人を一意に特定する。そして、情報提供機関における情報提供用個人識別符号Bへ変換し、情報提供機関Bへ送信する。送信後、情報提供用個人識別符号の保存は行われない。

次に、情報照会者等からの符号生成の依頼が来た場面を確認する。情報照会者等は、個人番号から住基ネットを介して、照会者の住民票コードを情報提供ネットワークシステムに送信する。情報提供ネットワークシステムは、住民票コードを受信後、符号生成依頼に基づいて、住民票コードを不可逆暗号で連携用符号を生成する。生成後、住民票コードは直ちに削除される。連携用符号から、機関ごとに異なり、情報提供ネットワークシステムと情報保有機関で個人を一意に特定するための情報提供用個人識別符号を生成し、各機関に送信する。送信後、情報提供用個人識別符号の保存は行われない。以上が情報連携の場面及び情報提供用個人識別符号の生成場面である。これら2つの場面においても情報提供ネットワークシステムに残るのは、連携用符号のみであり、情報提供ネットワークシ

テムは特定個人情報そのものを保有する仕組みにはなっていない。この点で少なくとも非該当要件①は充たされており、一元的管理機関の不存在要件に適合しているであろう。

さらに、情報保有機関を検討する。情報連携を行う場合、情報保有機関は、個人番号を用いず、特定個人情報の提供を管理するために個人番号に代わって用いられる特定の個人を識別する符号である情報提供用個人識別符号を用いる。当該符号は、他の情報保有機関のいずれとも異なることから、当該符号を保有するのは、情報保有機関のみということになる。したがって、情報連携のために情報保有機関が当該符号を保有することについては、少なくとも非該当要件①は充たされており、一元的管理機関の不存在要件に適合しているであろう。

以上のとおり、住基ネット最高裁判決が述べた一元的管理機関の不存在要件について、番号制度における付番機関及び情報提供ネットワークシステムともに当該要件は充たされている。

（３）具体的危険の検討（行政内部の局面）

①提供・収集・保管の制限

次に、情報連携後の行政機関内部における特定個人情報の提供・収集・保管の局面を検討する。番号法は、特定個人情報の収集等の制限を定めている。同法第20条は、「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（他人の個人番号を含むものに限る）¹⁰⁵⁾を収集し、又は保管してはならない」と規定し、同法第19条に規定される場合を除き、特定個人情報の収集、保管を禁止し、みだりに特定個人情報が拡散することを阻止し、特定個人情報の保護を図っている（表1参照）。

同法第20条が規定する「収集」の意味は、「『収集』とは、集める意思をもって自己が所持する状態に移すこと」である。ただし、「単に閲覧をして特定個人情報の内容を知ったとしても特定個人情報を所持したとはいえず、収集には当たらない」¹⁰⁶⁾。例えば、電子計算機の画面上に個人番号のみを表示させただけの行為は収集には当たらないが、その表示画面を印刷する行為は、収集に該当する¹⁰⁷⁾。

また、「保管」の意味は、「『保管』とは、自己の支配下に保持すること」¹⁰⁸⁾である。例えば、電子計算機の画面上に個人番号を表示させ、その画面を印刷し保持する行為は、収集に該当するだけでなく保管にも該当することになる¹⁰⁹⁾。

もっとも、同法第19条によって提供を受けた特定個人情報であっても、無制限に保管できるわけではない。特定個人情報も個人情報の一種であると考えられることから、個人情報の利用に関する制限規定が適用される。その結果、特定された利用目的の達成に必要な

105) 「他人」とは、自己と同一の世帯に属する者以外の者をいう（同法第15条）。

106) 宇賀・前掲注9) 129頁。

107) 岡村・前掲注64) 250頁参照。

108) 宇賀・前掲注9) 129頁。

109) 岡村・前掲注64) 250頁参照。

範囲においてのみ保管が許されることとなる（行政機関個人情報保護法第3条第2項、個人情報保護法第16条、独立行政法人等個人情報保護法第3条第2項）。

番号法ではこのように、特定個人情報の収集、保管については、同法第19条のいずれかに該当する場合を除き、原則として禁止し（同法第20条）、本条違反には罰則が設けられている（同法第52条）¹¹⁰⁾。

【表1：特定個人情報の提供・収集等の制限】

番号法	原則	例外
第19条 (特定個人情報の提供の制限)	第19条各号に該当しない場合の特定個人情報の提供を禁止。	第19条各号に該当する場合には提供ができる。 (ただし、本条第7号に該当する場合は提供は義務『第22条』)。
第20条 (特定個人情報の収集等の制限)	第19条各号に該当しない場合の特定個人情報の収集、保管を禁止。	第19条各号に該当する場合には収集、保管ができる。

②不正な情報連携と一元的管理機関の不存在要件の適合性

ここでの確認事項は、行政内部における不正な情報連携がどのように防止されているのかという点と、情報連携後の行政内部が一元的管理機関の不存在要件に適合しているかという点について確認する。

この点について日本弁護士連合会は、「『社会保障・税番号大綱』に関する意見書」¹¹¹⁾で、「大綱は、『共通番号』を用いない情報連携の仕組みを構築することで、国家管理や情報漏洩の懸念に対応できるシステム上の安全措置が図られていると主張する。しかし、情報連携基盤技術WGで議論されているモデルでは、各情報保有機関が『共通番号』と結ぶ形で個人情報を保有することになっている。よって、情報保有機関同士が（情報連携を通さずに）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」¹¹²⁾と指摘している。

情報提供ネットワークシステムを介した情報連携の局面では、行政機関ごとに異なる符号を用いて情報連携を行うことにより、個人が特定されにくい仕組みを採っていた。

一方で行政内部では、個人番号利用事務等を処理するために必要な範囲で特定個人情報を「特定個人情報ファイル」¹¹³⁾として保管することができる（番号法第29条）。そこで、

110) 「国の機関、地方公共団体の機関若しくは機構の職員または独立行政法人等の職員がその職権を濫用して、専らその職務の用以外の用に供する目的で個人の秘密に属する特定個人情報が記録された文書、図画または電磁的記録を収集したときは、2年以下の懲役または100万円以下の罰金に処する」。

111) 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）
(<https://www.nichibenren.or.jp/var/rev0/0001/3712/110729.pdf>)。

112) 日本弁護士連合会・前掲注111) 8頁。

113) 番号法上、「特定個人情報ファイル」とは、個人番号をその内容に含む個人情報ファイルと定義さ

情報提供ネットワークシステムを介さずに行政機関同士が、潜脱的に特定個人情報の授受を行うことを回避するための防止策が手当てされているのかという点が問題となるが、この点については、現在まで検討資料等の存在を確認することができず判然としていない。この違法な行為をより厳格に防止しようとするなら、「各情報保有機関が個人番号を保有しないようにするか、情報機関ごとに別の個人番号を用意するしかない」¹¹⁴⁾と思われるのだが、現状では、先に見たように特定個人情報の収集等を制限（同法第20条）し、罰則（同法第52条）による対策が図られていると考えられる。

だが、せっかく符号を用いた情報連携を行うことで特定個人情報の目的外利用を技術的に排除しているにもかかわらず、情報提供ネットワークシステムを介さない行政機関同士の情報の授受を防止する技術的な対策が採られていないとすれば、同法19条第7号及び第8号に該当しない場合の行政内部における不正な目的外利用や提供に関して、保護措置としてこれで十分であるのかという疑問が生じ得る。この点については、同法第19条の提供の制限の例外が今後も維持されるか否かにも依存するため、本条の改正には慎重な検討が必要であるというべきであろう。

以上のとおり、行政内部における不正な情報連携の防止については、罰則をもって禁止し、対策が図られている。また、一元的管理機関の不存在要件の適合性については、現行法上では、少なくとも非該当要件①に該当していると思われ、一元的管理機関の不存在要件に適合しているであろう。

3. 情報の蓄積問題とその他の課題

行政機関同士の不正な特定個人情報の授受以外に問題となり得るのは、情報の蓄積問題であろう。特定個人情報の利用範囲の拡大や提供制限の例外を拡大すれば、新たに特定個人情報を保有することになる機関の増加の可能性、あるいは既存の保有機関においても情報の蓄積量が増加することが予想される。

特定個人情報を保有する機関が増加することは、個人の側から見れば自己の特定個人情報が様々な機関に分散して保有されることでもあり、機関が分散されているだけに外部からの不正な攻撃等による情報漏えいの対象となる危険性が高まるだけでなく、内部からの情報漏洩の危険性も高まるという点が問題点として考えられる。

その他に、番号法第19条第14号が問題となり得ると考えられる。同条第14号に該当する場合には、特定個人情報の提供の制限のみならず、特定個人情報ファイルの作成の制限（同法第29条）、個人情報保護委員会の指導及び助言（同法第33条）、勧告及び命令（同法第34条）、報告及び立入検査（同法第35条）のいずれも適用が除外されている（同法第36条）¹¹⁵⁾。特に問題と思われるのは、同条第14号に該当するものとして、刑事事件の捜査、

れる（番号法第2条第9項）。

114) 高木浩光ほか「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～」3頁参照（<https://staff.aist.go.jp/takagi.hiromitsu/paper/ipsj-csec61-29-takagi-dist.pdf>）。

115) 宇賀・前掲注9) 124～125頁及び163頁では、提供の制限を適用除外する理由について、「特定個人

租税に関する法律の規定に基づく反則事件の調査が含まれている点である。同法は、原則として利用や提供に関する限定列举方式を採用しながらも、同条第14号に定める行政機関に関しては、無制約に利用や提供を許しており、その意味では必ずしも行政の自己拘束は硬くはない。

情報は、蓄積されることにより、付加価値が高まるという性質を持つ。とりわけ、対象者の情報が揃うほど分析の正確性も高まる。したがって、これらの行政機関が、個人番号を基にして特定個人情報を収集し、蓄積した個人情報を類型化し、分析することによって一定の個人像を作出し、社会的評価を下す危険性が全くないと断言することはできない。

この点、行政機関個人情報保護法においても番号法においても、プロファイリングに関する法的な規制が整備されていない現状において、今後センシティブな個人情報が収集、管理されるとすれば、個人にとってプライバシーの脅威となりかねないであろう。

それゆえ立法者は、番号制度の個人情報の管理方式が分散管理に該当し、住基ネット最高裁判決が掲げた一元的管理機関の不存在要件に適合的な制度であることを強調するのであれば、そのことを担保するためにも、同法第9条の特定個人情報の利用範囲及び同法第19条の特定個人情報の提供の制限の例外を安易に拡大せずに十分に限定的な運用とすべきであろう。また、特定個人情報を保有する機関の増加や保有する特定個人情報の蓄積量の増加に伴って、一元的管理機関の該当要件①、あるいは該当要件②の危険性についても相対的に高まり得る。したがって、特定個人情報の利用範囲や特定個人情報の提供制限の例外の拡大を検討するにあたっては、一元的管理機関の該当要件①、あるいは該当要件②に該当しないかを常に検証し、その権限の行使は、絶えず抑制的、かつ、慎重に行われることが求められるであろう。そうでなければ、最高裁判決が指摘する一元的管理機関の不存在要件の適合性に疑義を生じさせかねないとも考えられよう。

最後に、マイナポータルについて言及しておきたい。マイナポータルは、インターネット回線を通じて提供されるサービスであることから、情報漏えい等を完全に排除することは難しい点である。加えてマイナポータルの場合、利用者側のセキュリティ対策も課題となろう。使用環境に脆弱性があるとIDやパスワードを窃取されるなどの危険性は高くなる。現状においては、マイナポータルの利用は利用者の選択に基づくものであり、義務化されているわけではない。マイナポータルを利用する際は、個人の側もインターネットを利用する際のリスクが内在することに対する理解と、利用環境に十分に意を払う必要がある。

また、マイナポータルには、情報提供ネットワークシステムを経由した自己の個人情報のやり取りの記録を確認できる機能（やりとり履歴）があるが、これは、情報提供ネットワークシステム経由で情報連携が行われて提供された情報（番号法第19条第7号及び第8

情報の提供の必要性が大きい一方、不正な情報提供は想定し難いという理由で」、また、特定個人情報ファイルの作成の制限が適用除外される理由について、「特定個人情報ファイル作成の必要性が認められ、かつ、特定個人情報ファイル作成による個人の権利利益侵害のおそれが認められないからである」との説明がなされている。

号）が対象であり、それ以外（同法第19条第1号から第6号及び第9号から第16号）に該当する提供や、情報提供ネットワークシステムを使用しない同一内組織の情報連携に関しては、やり取りの記録の対象外である点に留意が必要である。

これまで番号制度について、住基ネットをひとつの参照軸に、制度の構想段階から情報連携の仕組み、そして情報の管理、利用等の局面の問題へと考察を進めてきた。これまでの考察では、現行制度においては、必ずしも個人のプライバシーを侵害するおそれの高い制度ではないと評価することができる。

しかし、それはあくまで番号法第9条が規定する特定個人情報の利用範囲及び第19条が規定する特定個人情報の提供の制限の例外が十分に限定的であることが前提である。

番号法は、限られた分野で利用することとして、利用の範囲を法定しているものの、基本理念では、利用拡大の施策の推進が謳われている。一見矛盾するような立法政策が行われているように思えるが、そうではない。番号制度の構想段階から個人番号の利用範囲の拡大を視野に入れた制度設計が行われたことは、国民ID制度との一体的な検討過程で明らかであった。また、居住関係を公証するための限定的な制度設計が行われていた住基ネットと、広く個人番号の利用の推進を目的とする番号制度では、その目的に本質的な相違があることも明らかである。

また番号法は、住基法では認められていなかった本人確認情報の目的外利用に当たるデータマッチングに関して、情報連携という言葉を用いて、行政機関等が同法の定めにより本人の同意を得ずとも個人情報の名寄せを行えるように法定した点に最大の特徴がある。そのため情報連携は、同制度の目的には欠かせない手段として位置付けられている。この点こそが、両制度の本質的で決定的な相違であるといえるであろう。

その意味では、住基ネット最高裁判決が否定した目的外利用の具体的危険性に関して、番号法においては、はじめから目的外利用の危険性を孕んだ制度である、ともいえるかもしれない。それだけに、番号制度は、住基ネット以上の高い公共性のある行政目的を実現するための必要最小限の利用の範囲内に留めるべきであろう¹¹⁶⁾。

立法者が、番号制度を構想するうえで、同制度の合憲性を担保するために住基ネット最高裁判決を踏まえた制度設計を行ったことは確認した。しかしながら、両制度には、本質的な違いがある。それだけに、本制度の合憲性の淵源を住基ネット最高裁判決に求めるのであれば、特定個人情報の利用範囲及び特定個人情報の提供の制限の例外の拡大は、慎重に検討しなければならない、というのが本稿筆者のひとまずの結論である。

116) 同趣旨として、「住基ネットに比べますとセンシティブティーは高い情報を扱うことになりますし、データマッチングを行う範囲が広がるということですから、やはり高い公共性のある行政目的に限定をして考えていくべきですし、高い公共性にかなう行政目的を実現するための必要最小限の範囲内での利用ということで議論を出発させていくべきではないかと考えております」個人情報保護ワーキンググループ会合議事録・前掲注93) 19頁〔長谷部恭男座長代理発言〕。

お わ り に

本稿では、わが国の番号制度の法的課題について考察を行った。筆者の中で印象的であったのは、住基ネット控訴審判決である。誌面の関係で、原文全てを記載できなかったが、同判決は、法制度のみならず、住基ネットのシステムに関する安全性の有無等について、実に詳細に検討が行われている。

また、控訴審は、自己情報コントロール権に言及し、住民票コードの秘匿性についても、それ自体数字の羅列に過ぎない個人識別情報であるが、データベースが作られた場合には、検索、名寄せキーとして利用できるものであることを指摘し、秘匿性を高いと判断している。

それに対して最高裁は、現に一元的に管理された機関または主体が存在しないことを前提として、その秘匿性は高くないと判断している。結果的に控訴審判決は、最高裁判決で破棄されることとなるが、合憲か違憲かの分水嶺は、住基法上の適用解釈に関する判断の違いであった。これについては、最高裁の判断が妥当であろう。

しかしながら、情報の秘匿性についての最高裁の判断は、本件訴訟においては妥当性があると思われるものの、番号制度のような将来的に個人情報が行政機関に蓄積され得る場合にまで、この判断の基準が妥当し続けるのかについては疑問に思われる。情報の付加価値をそれ単体で評価することが、果たして、いつまで通用するのであろうか。蓄積される情報の性質や量によって利用価値は格段に高まるのであり、今日ビッグデータ時代を生きる私達にとって、懸念を抱かざるを得ない。

最後に、現在各地でマイナンバー訴訟に係争されているが、本稿との関係で、横浜地裁判決¹¹⁷⁾が述べた、個人番号及び特定個人情報の法的性質の部分について、引用する。

曰く、「番号制度において利用等の対象とされている個人番号自体は、住民票コードを変換して得られる番号であり、それ自体に何らかの個人のプライバシーに属する情報を含むものではないと認められる。同様に利用等の対象とされている特定個人情報は、個人番号及びこれと結び付けられた個人情報によって構成されている（同法2条8項）ところ、個人番号自体、個人のプライバシーに属する情報を含むものではないことは上記のとおりであり、個人番号と結びつけられる個人情報も、番号制度の導入前から行政機関等で収集、保有、管理、利用等をされていた情報であって、番号制度の導入により新たに行政機関等が収集、保有、管理、利用等を行うことができるようになったものではない」。

いうまでもなく、当該判決における個人番号等の秘匿性の判断は、住基ネット最高裁判決と同じ立場を採る説明である。住基ネットは、当該システムの利用の目的や範囲が明確である。

それに対して、番号制度は、個人情報の利用拡大の施策を推進している制度であり、両

117) 前掲注・102)

者の目的は明らかに異なる。

今後、番号制度の利用範囲の拡大に伴い、行政機関等にとって新たな情報の収集等が行われることが十分予想されるだけに、当該判決の理由は説得力に欠けているであろう。

加えて、個人番号等の法的性質の判断にも疑問がある。番号法は住基法とは異なり、個人番号がそれ自体単なる番号であっても、個人番号と紐付けられる情報が、秘匿性の高い情報をも扱うことを予定し、だからこそ利用範囲を法定し（同法第9条）、個人番号を利用するための保護措置を定めているのであり（同法第12条）、個人番号等の保護の必要性の程度が、住民票コードと同程度と判断する当該裁判所の解釈には疑問が残るのである¹¹⁸⁾。

118) 本判決の評釈において同趣旨の見解がある。毛利透「個人番号（マイナンバー）制度の合憲性」法教472号133頁参照。