●資料提供サイト管理者による注

本答弁書のサイト収録にあたって、代理人弁護士一覧を省略しました。
このため、1ページの下部が空白となり、2～8ページが欠番となっています。

平成１９年（オ）第４０３号

平成１９年（受）第４５４号

上 告 人　守口市ほか１名

被上告人　[redacted]ほか１名

答　　弁　　書

２００８年１月２４日

最高裁判所　第一小法廷　御中

被上告人[redacted]、同[redacted]両名訴訟代理人

目　　次

第１　はじめに

１　上告人らは、①自己情報コントロール権は差止請求の根拠たり得る実体法上の権利とは認められないこと、②プライバシーは、それのみで差止請求の根拠となるような排他的権利として確立されていないこと、③本人確認情報は自己情報コントロール権の保護の対象とはならないこと、という理由をあげて、「原判決には、憲法の解釈に誤りがある」と主張する。

しかし、上告人らの主張は、「本人確認情報」がデータマッチングに果たす機能（すなわち、本人確認情報が付される個人情報データベースの索引（インデックス）情報となる機能）を軽視し、データベースの情報内容と切り離して、「本人確認情報」の情報内容だけの要保護性を（しかも、その６情報をバラバラにした上で）論ずることに端的なように、コンピュータ・ネットワーク時代におけるプライバシー侵害に対する決定的な理解不足が存するものであり、失当である。

２　住基法の改正により創設された住基ネットシステムは、以下のような特質を有するものである。

①　全国民に漏れなく重複しない１１桁の個人識別番号（住民票コード）を付した上、

②　全国の市区町村、都道府県、地方自治情報センター及び国の機関等を結ぶ全国的コンピュータ・ネットワークシステムを構築して※、

③　この住基ネット（コンピュータ・ネットワーク）を通じて、住民票コードをインデックスとした「本人確認情報」（住民票コード、氏名、住所、生年月日、性別、それらの変更情報の６情報）が、常時、市区町村から都道府県を介して地方自治情報センターに集約され、一元管理されることになった。

④　そして、地方自治情報センターから、国の機関等に本人確認情報が提供され、国の機関等が保有するデータベースの情報と結合させられ、それらのデータベースの本人識別情報（索引情報）部分が、住基ネットの「本人確認情報」

※住基ネット創設以前は、住民基本台帳の情報は、各自治体の保有する個別のコンピュータ内で処理されていただけで、外部とのオンライン結合は条例で禁止されていた。住基ネットにより、全国津々浦々までコンピュータ・ネットワークにより、結合され、情報の、大量かつ即時の伝達・処理が可能ならしめられた。

に統一されるようになった。

⑤　住基法の別表上、本人確認情報を提供できる事務は、住基ネット稼働開始時（平成１４年８月）には９３事務であったが、平成１８年５月段階で２９３事務にまで増大している。

⑥　本人確認情報の住基ネットを通じての提供について、住民本人の個別同意は要件とされず、また、不参加ないし離脱を表明している者について、除外(離脱)を明文で認める規定はなく、一律に、全員の参加が強制されている。

3　このようなコンピュータ・ネットワーク社会において、上記の特質を有する住基ネットシステムを構築することが、プライバシーにいかなる深刻な影響を与えるのかの点について、今、その問題点を真剣かつ理性的に考察しておくことが、憲法の番人・国家理性の府である最高裁判所の責務であるといわなければならない。さもなければ、近い将来、必ずや「あのとき、なぜもっと真剣に検討しなかったのか」という後悔の時を迎えることは必然である。

そこで、上告人主張の上告理由の当否を検討するに当たっても、現代高度情報化社会、すなわちコンピュータ・ネットワークが高度に発達した社会におけるプライバシー侵害の特質について理解することが必要であるので、以下、まず、第２において、現代プライバシー権侵害の特質及び検討すべき点を総論的に述べた上で、第３以下で、上告人らの主張に対し更に具体的に反論する。

第２　現代プライバシー権侵害の特質

１　憲法上の権利としてのプライバシーの権利（プライバシー権）

上告人らは、「自己情報コントロール権は差止請求の根拠たり得る実体法上の権利とは認められない」と主張する。

そもそも、平成１１年制定の「守口市個人情報保護条例」を持ち、「実施機関は、自己の情報をコントロールする権利を市民に保障しているので、市民が自己情報の記録の削除を請求できるようにし、個人情報の取扱いの制限について、実効性のあるものにする」（「守口市個人情報保護制度　手引書」守口市

作成）という趣旨の下に「削除」請求権や、「利用の中止」請求権等を保障している上告人守口市自身が、上告理由でこのように「実体法上の権利とは認められない」と主張すること自体が、自己矛盾であり、許されないものであることが指摘されなければならない。

その上で以下、まず、本件で問題となるプライバシー権の保障と、それを通じた私生活の平穏と人格的自律の確保の必要性・重要性について述べる。

(1) プライバシー保障の必要性

個人は、自己に関するプライバシー情報を、国家や他人から、みだりに収集されたり、利用されたり、第三者に提供されたりすることから保護されなければならない。

何故なら、このようなことが無制限に許されるならば、あたかも個人は国家や他人から監視された状態に置かれるようなことになり、個人の私生活の平穏が害され、自己のことについて自己決定してゆく自由が侵害されるからである。そして、このような状況下では、自由で自律的な人格形成も困難となるからである。

さらに、国家との関係において、民主政治は、国家（政府）に従属しない、自律できる国民（主権者）の存在が前提である。国家が国民に関するプライバシー情報を、みだりに収集・保管等したならば、国民の人格的自律の形成・維持も困難となる（後述の「萎縮的効果」に端的である）。したがって、民主主義の前提を守るという観点からも、プライバシーは守られなければならない。（なお、同様のことは、行政権に対する司法権（裁判官、裁判所職員）の独立、自律の維持という観点からも、重要である。）

以上のように、プライバシーの保障は、「個人の尊厳」を守るために（そして民主主義社会を守る上で）、もっとも根源的で核心的な人権の１つであり、国政の上で最大限の尊重を要する人権であるといわなければならない。

(2) コンピュータ・ネットワーク時代におけるプライバシー保障の質的転換

ア　現代のプライバシー権－自己情報コントロール権

高度に情報化された現代のプライバシー情報は、その多くがコンピュータによりデジタル情報として管理され、それらのコンピュータはネットワーク化されている。これにより、かつてのように、紙媒体により「私生活が暴かれる」といった時代のプライバシー権の保障とは、全く質的に異なる時代に入っている。

本件では、この点の理解なしには問題の本質に迫ることができないものであるので、ここで、その特質の要点を再度まとめるならば、以下のとおりである。

①「高度情報化社会」においては、個々人の様々な個人情報が、大量に収集・保存されており、それらの個人情報が、コンピュータによって、デジタル情報として処理されている。

② デジタル化された情報は、瞬時かつ容易に複製を作成でき、しかも複製による情報の劣化は生じない。

③ デジタル化された情報は、ネットワークにより、瞬時・大量・広範囲に伝達・伝播することが可能であり、いったん伝播された情報を回収することは、事実上不可能である。そして、さらに、

④ ネットワーク上にある無限大ともいえる膨大な情報の中から、コンピュータによって、ある個人の、一定条件の情報を、検索・名寄せして、データマッチングすることが可能となっている。

以上のように、紙媒体時代とは、情報の収集、保管・管理、利用、開示・提供のすべての場面で、量的にも、質的にも大きく変わったと言わなければならない。

したがって、これに応じて、「プライバシー権」も、単に「一人で放っておいてもらう権利」という消極的なものから、情報の収集、保管・管理、利用、開示・提供のすべての場面において、自己に関する情報をコントロールできる積極的な権利へと発展させなければ、個人の尊厳と自律は保ち得なくなっているのである（注1、注2）。

注１：なお、「一人で放っておいてもらう権利」は１９２８年 Olmstead v. United States. 277 U.S. 438 事件のブランダイス裁判官の反対意見の中で定義されたものである。同裁判官は、たとえ屋外にある電話線に盗聴器を設置しても、実質的に「私的領域」を侵犯する以上、プライバシー侵害になると論じた。これは、「家を個人の聖域と観念し、その中で行われる生活、例えば、誰と生活を共にし、子供を作るかどうかといった個人生活の形成からそれに関わる情報に至るまで、政府による干渉を禁じるという考え方である。このような意味で、ブランダイス裁判官の『一人で放っておいてもらう権利』という定義には、情報の秘匿と自己決定という二つの側面がもともと内在していた。これがのちに、私生活上の秘密を暴露されないといった面に重点を置くいわゆる『情報プライバシー権』と、自分の人生を自分で決める『自己決定権』、そしてその二つの面を併せ持った『情報の自己決定』という意味での『自己情報コントロール権』という観念を生み出すもととなったのである」とも説明される・中島徹・早稲田大学法務研究科教授の「意見書」（平成１９年７月１１日付）参照）。）

注２：本件で問題となる「コントロール権」は、情報の収集や利用の仕方に関する自由権的側面に関するものである※。よって、その権利内容や外延は明確である。）

この点、原判決は、「とりわけ，情報通信技術が急速に進歩し，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，また，インターネット等によって多数のコンピュータのネットワーク化が可能となり，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。このような社会においては，プライバシーの権利の保障，それによる人格的自律と私生活上の平穏の確保を実効的なものにするためには，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ということが極めて重要になってきており，その必要

※ 『法律時報』79巻11号(2007年10月号)70頁「＜対談＞改めて憲法一三条裁判を考える－住基ネット訴訟に関連して」　樋口陽一・中島徹対談参照

性は社会において広く認識されてきているといえる。」（46～47頁）と的確に判示しているものである。

なお、学説においても、プライバシー権が自己情報コントロール権として認められるべきことは、今や通説というべきである（兼子仁・東京都立大名誉教授ほかによる「住基ネット憲法訴訟における憲法問題に関する研究座談会(要録)」(2007年6月23日)＝以下、単に『要録』という＝3～8頁参照）。

したがって、以下詳述するように、個人情報の収集や利用に対する「本人の同意」は、プライバシー権（自己情報コントロール権）を保障する上で、本質的な要素といわなければならない。

イ　データマッチング

④で指摘したように、紙媒体情報の時代では、それらの情報すべてを検索し、名寄せした上で、突き合わせてマッチングすることなどは、人間の肉体的能力の限界から到底不可能であったものが、コンピュータによる情報処理技術の飛躍的進展によって可能となっている。

したがって、この情報処理技術の質的転換に応じて、データマッチングに対しても、その情報主体によるコントロールを及ぼさなければ、国民はすべての情報をマッチングされて「丸裸」にされてしまう（もしくは、その一部の情報のみをマッチングされたりして、偏った「人物像」を勝手に構成されてしまう）危険性が発生している。そして、この危険性は、特に膨大な個人情報を既に収集保有しており、更に今後も種々の分野で収集権限を有する国（行政機関）との関係において顕著であるといわなければならない。

この危険性は、たとえば、インターネット検索により、全世界のホームページなどの中から、特定の人に関する様々な情報を名前などを「キーワード」として検索し、名寄せして、マッチングすることによって、その人の「人物像」を作り上げること（プロファイリング）ができるようになっていることを考えれば、容易に理解できるであろう。既に、行政機関はインターネット

上に存在する情報よりもセンシティブなものを含めて膨大な個人情報を保有しているのである。

したがって、このようなコンピュータ・ネットワーク上の情報を収集されること自体について、原則として本人の「同意」にかからしめること、そして、「同意」を得て収集した個人情報についても、その収集目的以外のために「データマッチング」されないようなシステム（更には、間違って保存されている情報について、訂正したり、削除したりする請求権を認めるシステム）を作っておかなければならないのである。

このようなシステムが作られていなければ、個人に関する情報は徹底的に収集された上で、たとえば、マーケッティング目的のために「データマッチング」されたり、行政機関が収集し、保有する膨大な個人情報が、収集目的以外の目的で「データマッチング」されて、「監視」の道具として利用されたりしてしまうことになることは必然である。何故なら、「データマッチング」は、それくらい情報の保有者にとって「便利」であるからであり、また、莫大な経済的価値を生むからである。

ウ　萎縮的効果（チリング・イフェクト）

ところでさらに、そのような「データマッチング」が“行われるかもしれない”という危惧感を抱かせるような状況が作られたならば、どのような状況がもたらされるか。たとえば、“マイノリティ”グループに関係すること、「反政府」的傾向を有する特定の集会に参加することや、意見を表明することなどについて、情報が収集され、自己に関する「評価像」が作られてしまうのではないか、だから、「参加しないでおこう」、「意見を表明しないでおこう」という「萎縮的効果」が発生することは必然である（1983 年 12 月 15 日ドイツ連邦憲法裁判所の国勢調査判決参照）。

ドイツ連邦憲法裁判所判決は以下のように指摘している。

「基本法秩序の中心は、自由社会の構成員として自由な自己決定を行う個人の価値と尊厳にあるといえるが、その保護に役立つのが、基本法一条一項と相俟って同法二条

一項において保障されている一般的人格権（Allgemeines Persönlichkeitsrecht）である。そして、人格権は、自己決定権の思想により、個人の生活状況が、いつ、いかなる範囲で開示されるかを、原則として自らが決定するという権能を含むものである。かかる権能は、今日及び将来の自動化されたデータ処理の状況下では、特別に保護を必要とする。とりわけこの権能は、今日では以下のような理由で危機にさらされている。すなわち、自動化されたデータ処理によって、特定の又は特定しうる個人の人的状況及び物的状況に関する事項（以下、個人に関連するデータという）を、技術上無制限に蓄積することができ、且いつでも距離に関係なく瞬時に引き出しうるということによってである。のみならず、自動化されたデータ処理は、複合的な情報システムが出来上がった場合には特に、他のデータ集積と結びつくことにより、一方的に市民の個人像を作り上げることを可能としてしまう。そしてその場合、当事者はこの個人像の正確性やその利用について十分なコントロールを行うことができないのである。それゆえ、従来からは知られていない方法で個人の行動を監視し、これに影響を与える可能性が増大しているといえる。それは、当局が関心を持つという心理的な圧迫を加えることで、各人の行動に影響を及ぼすことができるものなのである。したがって、人格権の自由な発達は、現代のデータ処理の諸状況の下では、自己の個人的データの無制限な調査、蓄積、使用、提供から各人を保護することを前提とする。それゆえ、この保護は、基本法一条一項と相俟った同法二条一項の基本権に含まれるものである。その限りで、この基本権は、各人に自己の個人的データの開示、使用について原則として自ら決定する権能を保障するものといえる。」（鈴木康夫・藤原静雄「西ドイツ連邦憲法裁判所の国勢調査判決［上］」『ジュリスト』８１７号・１９８４年７月１日付・６４頁）

このような「萎縮的効果」が発生するような状況下では、自由な人格の発展や「人格的自律」の維持形成などは到底おぼつかない。そして、そのような萎縮した個人の存在を前提としては、健全な民主主義社会など形成できないのである。

エ　単純情報

このような「データマッチング」の対象となる個人情報は、上述の「政治

的傾向」のように、内容的に誰の目にも「プライバシー」と評価される情報（センシティブ情報）に限らない。すなわち、たとえば、「Aという個人が、ある時点で、特定の場所を通過した」という情報は、それ自体を単独で取り上げれば「プライバシー」と評価できないような個人情報であることが多いであろう（しかも、個々の「通過情報」は公衆の目に触れている）。しかし、このような情報でも、一定数集積しマッチングすれば、「Aという特定人の行動および行動パターン、立ち寄り先」という、意味のある情報となるのであり、国家機関が勝手に収集してはいけない情報となることは明らかである（このことは、たとえば、警察官が、被疑者でもない人物を、追尾して、その行動を監視することの違法性を考えれば明らかである）。

そして、更にこのような「行動情報」と「Aに関するその他の公開情報」などを「データマッチング」すれば、Aの思想・信条や消費傾向などを推知できる情報までもが明らかとなる（＝プロファイリングできる）可能性は高いのである。また、現代のコンピュータ・ネットワーク技術を駆使すれば、そのような膨大な“単純情報”のマッチングは技術的には可能となっているのである。

（なお、本件で問題となる「本人確認情報」の内容自体の重要性・要保護性については、後述ク）

オ　「共通番号」（住民票コード）と「限定番号」

そのような「データマッチング」の強力な武器が「共通番号」である。

上述の「A」に対し特定の「共通番号」（たとえば「12345678901」）を割り振っておけば、Aに関する情報は、いろいろなデータベースや情報の集積の中から、当該番号を「マスターキー」として、漏れなく、かつ、他者のデータと間違うことなく、正確無比に名寄せすることが可能となるのである。

人格的自律を守るために、データマッチングや共通番号を付すことが許されない、という趣旨は、以上の点から明らかである。

なお、①本件で問題としている住民票コードが変更可能であることは何ら

影響を及ぼさない。何故なら、住基ネットシステムにおいては、変更前の住民票コードも保存されている（提供先事務の各データベースの中でも保存されている）からである。したがって、この「変更」は、コンピュータを利用した名寄せ・データマッチングにおいては、何ら障害とならないものである。

さらに、②本件と同種訴訟の下級審判決の中には、「これまでもコンピュータ処理には整理番号を使っていたのであるから、住民票コードを割り振っても問題はない」旨の判断を行っているものも見受けられる。しかし、これは、例えば「運転免許事務」という特定の事務におけるコンピュータ処理のための番号（限定番号）と、事務の種類を問わずに汎用に用いるために特定個人に共通に付けられた番号（共通番号）の区別が全くついていないことを露わにしているものである。

「限定番号」においては、他の事務においては別の番号が付されている。そして、それぞれの番号の下に付されている「氏名」や「住所」などは、統一されていない。したがって、当該事務と他の事務のデータをデータマッチングしようとしても、たとえば、甲という事務の「１２３４番の斉藤貴男」は、乙という事務の「５６７８番の齋藤貴男」と同一人であるかどうかが正確に判断できないから、正確なデータマッチングができないのである※※。

ところが、住基ネットにより、住民票コードという各事務共通の「共通番号」が付されたことにより、この「共通番号」さえ一致していれば同一人物であると、容易かつ正確に識別できるようになった。すなわち、「同一性」確認が正確無比にできるようになったため、正確無比なデータマッチングが可能となったのである。

※※ これまでの「同一性」確認は、氏名、住所、生年月日、性別の４情報とその変更履歴を管理している市区町村に問い合わせを行い、その人物の「４情報」の同一性から確認するしかなかった。すなわち、“２人”の「斉藤貴男」と「齋藤貴男」という人物の同一性を確認するためには、“２人”の住民票所在地であるＡ市に照会を行い、「斉藤貴男」が、Ａ市Ｂ町1-1-1に居住する昭和30年１月１日生まれの男性であることと、「齋藤貴男」がＡ市Ｂ町1-1-1に居住する昭和30年１月１日生まれの男性であることを比較対照して、住所、生年月日、性別が同一で、氏名も「斉藤」と「齋藤」であるから「同一人物である」と判断していたのである。また、２人の住所等が異なっているような場合には、住所の変更履歴をたどって、同一人物であるかどうかを判断していたのである。

その意味で、「住民票コード」の付された氏名、住所等の４情報は、正に「本人確認情報」（＝本人識別情報）として、完成した機能を有するに至ったのであり、さらに、この「本人確認情報」が地方自治情報センターにおいて一元管理されることにより、市町村がバラバラに有していた“同一性確認機能”はセンターに集中させられ、瞬時に、そして継続的に、その同一性確認ができるようになったのである。これにより、常に各データベースはデータマッチングを行いうる状態に置かれることになったのである。

（なお、さらに、各市町村からセンターに対して、常に最新の４情報等が提供されるから、センターにおいて保有する「本人確認情報」は、単に個人を「識別」できるだけではなく、「どこに住所を有する」「何歳の」「男（女）」であることが把握できる情報となっている。）

以上述べたように、住基ネットシステムの構築により、市町村が国の機関等に対して行う「住民票情報」の提供は、それ以前の、個別照会に応じて提供していたものとは全く質の異なる「情報提供」となっているのである。

この点を押さえなければ、本件の問題性と深刻性はとらえられない。

カ　「本人確認情報」における氏名、住所等を利用したデータマッチング

なお、更に指摘するならば、本人確認情報の統一により、「氏名」や「住所」も、住民票記載のものに統一された（たとえば、上述の「斉藤」と「齋藤」も、住民票記載の「齋藤」に統一されるなど）。この統一により、仮に、住民票コードを用いなくても、「氏名」「生年月日」「住所」等を「検索キー」として用いれば、――コンピュータ処理上の負荷はかかるものの――やはり正確な「データマッチング」は可能となっているものである。

キ　住基ネットシステムによるデータマッチングのインフラ整備

以上指摘したように、現代のコンピュータ・ネットワーク社会においては、「単純情報」に分類される個人情報も含めて保障して、コントロールの対象としなければ、プライバシーや人格の自律は保ち得ない状況に至っていることは明らかである。

そして、本件で問題となる住民票コードや、氏名、住所、生年月日、性別、変更履歴の「本人確認情報」は、その内容自体のプライバシー該当性もさることながら、むしろ、その機能（使われ方）が、データマッチングのための「マスターキー」（検索・名寄せのキー）となりうるものであることがポイントとなることも明らかである。本件原判決はその点を的確に捉えているのに対して、上告人らは、単純にその情報内容の重要性だけに着目して、“社会生活上、氏名、住所等は明らかにしているものである”という観点からだけ、その要保護性を主張している。上告人らのように捉えて、住基ネットの“負の側面”を軽視することは、本件の場合、問題の本質を見失っていると言わざるを得ない※。

原判決など、既にいくつかの下級審判決が明言しているように、まさに、本住基ネットシステムの構築と運用によって、データマッチングのインフラは基本的に整備されたと評価せざるを得ない。上述のドイツ憲法裁判所判決で問題とされたように、この危険性の評価、および、その危険性防止策の実効性（十分性）が、憲法１３条の解釈として問われているのである※※。

ク　本人確認情報の内容自体の重要性・要保護性

なお、念のため補足するならば、データマッチングの観点を別として、「本人確認情報」は、情報内容に関しても、いまやその要保護性自体が高いことは前提である。

(ｱ)　まず、平成１５年９月１２日最高裁判決（早稲田大学江沢民主席講演

※ 指紋押捺に関する平成７年１２月１５日最高裁判決も、「指紋は、指先の紋様であり、それ自体では個人の私生活や人格、思想、信条、良心等個人の内心に関する情報となるものではないが、性質上万人不同性、終生不変性をもつので、採取された指紋の利用方法次第では個人の私生活あるいはプライバシーが侵害される危険性がある」と判示している。

※※ なお、安全保障の観点から見て、非常時を想定するならば、このような「共通番号」の下に、国民の個人情報がデータマッチングしうる状態で保存されていることの危険性も指摘することができる（『ＩＢＭとホロコースト　ナチスと手を結んだ大企業』エドウィン・ブラック著（柏書房）では、ナチスドイツがユダヤ人等を選別して、輸送・管理していたが、その作業を効率的に行い得たのは、ＩＢＭの創始者が開発した国勢調査の集計機械として普及させていたパンチカードシステムであったことが指摘されている。その他、『半島を出よ』村上龍著（幻冬舎）参照。）

会参加者名簿提供事件判決）は、（a）「学籍番号、氏名、住所及び電話番号は、大学が個人識別等を行うための単純な情報であって、その限りにおいては、秘匿されるべき必要性が必ずしも高いものではない。また、本件講演会に参加を申し込んだ学生であることも同断である」としながらも、（b）「このような個人情報についても、本人が、自己が欲しない他者にみだりにこれを開示されたくないと考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ものであるから、本件個人情報は、プライバシーに係る情報として法的保護の対象となるというべきである。」としている。そして、更に、（c）「このようなプライバシーに係る情報は、取扱い方によっては、個人の人格的な権利利益を損なうおそれのあるものであるから、慎重に取り扱われる必要がある」とも指摘して、（d）「大学は、上告人らの意思に基づかずにみだりにこれを他者に開示することは許されない」と明確に判示しているところである。

上告人らは、同判決につき、「平成１５年最高裁判決は、講演会の参加申込者であるという、公開することが当然視できない情報が、氏名等のこれらの『単純な情報』と結びつくことによって、誰が講演会に参加したかが明らかになることから、この情報全体について、プライバシーに係る情報としての法的保護の対象となることを認めたものである」とし、「したがって、平成１５年最高裁判決の判示するところによっても本人確認情報自体を独立にプライバシーに係る情報としての法的保護の対象となると解することはできないというべきである」（上告理由書15頁）とするが、二重の意味で失当である。

第１に、最高裁判決の(a)、(b)の判示部分をみるならば、同事件で問題となった「学籍番号」「住所」「氏名」などの「その限りにおいては、秘匿されるべき必要性が必ずしも高いものではない」情報であっても、「本人が、自己が欲しない他者にみだりにこれを開示されたくないと考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もの」として、

「プライバシーに係る情報として法的保護の対象となる」と明確に認めているのである。その上で、「上告人らの意思に基づかずにみだりにこれを他者に開示することは許されない」、すなわち、本人の同意による“コントロール権”の対象となることを認めているのである。

（上告人らが引用する杉原解説においても、「プライバシーの権利とは、『私的領域への介入を拒絶し、自己に関する情報を自ら管理する権利』ということになる。高度情報化社会では、様々な方法へのアクセスが容易になったことによって、一度漏えいした私的情報は直ちに私生活の平穏を具体的に害するものでないとしても、情報の漏えいは意に反する他者への公開の危険（私生活の平穏を侵害する抽象的危険）を包含することになる。自己に関する情報を管理する権利は、必ずしも内容の明確な権利とは言い難いが、このような社会的背景を前提に理解されるべきものであろう。本判決が情報の開示について本人の『同意』を重要な要件としているのも、このような自己に関する情報を管理する権利の考え方と親和的なものと見ることができよう。」としており、最高裁調査官においても、同判決は自己情報コントロール権の考え方と親和的なものと解説されているのである。）

第２に、上告人らは、最高裁が、(c)部分において、「このようなプライバシーに係る情報は、取扱い方によっては、個人の人格的な権利利益を損なうおそれのあるものである」と判示している部分を無視して、「本人確認情報自体を独立にプライバシーに係る情報としての法的保護の対象となると解することはできない」と結論づけている。前述（オ、カ）したように、本人確認情報（特に住民票コード）は、それ自体を独立に評価するならば索引（インデックス）情報であり、要保護性が高いとはいえない。しかし、他のデータベースの様々な個人情報と結合されることによって、センシティブ情報への“入り口”となる情報であるから、本人確認情報の内容自体だけを、独立に評価することは適切ではないのである。現代の高度情報化社会においては、“どこの誰の”情報であるか、ということを識別すること、及び、その特定人の情報をいかに正確かつ大量に集め得るか（また逆に、一定の条件に合致する人物群を抽出し、それらが“どこの誰であるか”を正確に

特定すること）が、死活的重要性を有しているのであって、この索引情報たる「本人確認情報」の重要性は、それだけを切り離して、独立に評価できるものではないのである。

最高裁判決が、「取扱い方によっては、個人の人格的な権利利益を損なうおそれのあるものである」と判示しているのは、その意味で全く正鵠を得ているのである。

(イ) そして、原判決や、本件と類似訴訟である平成１７年５月３０日金沢地方裁判所判決においては、ストーカー被害者における「氏名」「住所」や性同一性障害者における「性別」などの例も挙げて、詳細にその重要性について判示している。

(ウ) さらに、平成１９年２月１日名古屋高裁判決（平成１７年（ネ）第６３１号・以下「名古屋高裁判決」という）では以下のように判示されている。

「 これらの（本人確認）情報はいずれも秘匿する必要性が高いということはできないものである。

しかし，コンピュータを利用した個人情報の大量収集・蓄積という社会状況のもとで，収集，蓄積された個人情報の漏えいや目的外使用に対する不安を抱く者が少なからず存することは否定できないところであり，上記のように必ずしも秘匿する必要性が高いとはいえない情報であっても，その開示が予定されていない者に対して，あるいは予定されていない利用目的のために，本人の同意なくしてみだりに情報が開示されることとなれば，本人が不安を感じ，その私生活の平穏及び人格的自律が害される可能性があることは否定できない。したがって，本人確認情報が，予定された開示対象及び利用範囲を逸脱してみだりに開示されないという限度では個人の期待は法的保護に値するものというべきである。」（29頁）

(エ) その他、上記平成１５年９月１２日最高裁判決の原審である平成１４年１月１６日東京高等裁判所判決などでも、現実に、企業の顧客名簿などの個人情報が大量に流出したり、個人情報が売買の対象とされるような事態も生じていることや、ストーカー行為の多発により、個人情報の開示を警

戒する気持ちが国民一般に強くなっている状況から、個人に関する情報の保護を図ることの重要性についての国民の関心ないしは法的意識が急速に高まりつつある、としている。

以上より、本件「本人確認情報」の内容の要保護性自体が高いことは大前提とされなければならない。

(3) 小括

以上述べたように、現代のコンピュータ・ネットワーク社会におけるプライバシー権は、自己情報コントロール権として保障されなければならず、データマッチングのプライバシーに与える深刻な危険性に鑑みるならば、そのインフラたる「住民票コード」とそれを利用するシステムの創設、利用に対しては極めて慎重な姿勢が必要となるものである。

2 「e－Japan」計画や「最適化計画」によるデータマッチング・システムの完成・高度化

(1) e－Japan計画による電子政府・電子自治体構想と最適化計画

上述のように、住基ネットシステムの構築により、データマッチング・システムはすでに基本的に完成したと言いうる。

しかし、これまでは、行政機関が保有する膨大なデータは、省庁毎の縦割り組織と、それぞれが独自仕様のデータベース、コンピュータシステム（旧式のいわゆる「レガシーシステム」）を使用していたことにより、分断されており、データマッチングを事実上阻止していた。

ところが、現在、政府が強力に推し進めている電子政府構想（や電子自治体構想）は、「行政情報の電子的提供、申請・届出等手続の電子化、文書の電子化、ペーパーレス化及び情報ネットワークを通じた情報共有・活用に向けた業務改革を重点的に推進する」ことを目指しており、その一環として政府省庁の情報システムも「最適化」されようとしている（甲17・黒田論文参照）。この「最適化計画」により、「効率化」の名の下に、今まで存したこれらの“事実上の分断障壁”は完全に取り払われようとしている。すなわち、

政府省庁のコンピュータシステムを、事務毎に独立した、旧式の「レガシーシステム」から共通のソフト・データが使える「オープンシステム」に置き換え、そして、そこで使用されるデータの仕様の統一化を図ることによって、情報システムは統一化されようとしているのである。

これが完成した暁には、コンピュータ・ネットワークを通じて、どこの省庁の端末からでも、どこの省庁の保有するデータにでもアクセスして、情報を収集することが可能となる。したがって、これまで事実上データマッチングを阻止してきた「縦割り組織」と「レガシーシステム」の障壁はなくなるのであり、データマッチングの危険性は飛躍的に高度になると言わなければならない。

まさに、「行政の前で丸裸」にされる危険性が高くなってきているのであり、また、後述のように、その明確かつ実効的な防止策がとられていない現状では、すでに、データマッチングの危険性による「萎縮的効果」は極めて現実的なものとなっているといわざるを得ないのである。

(2) データマッチングの主体

このようなシステムに更新された場合、「データマッチングの主体」も変化する。すなわち、かつての「レガシーシステム」においては、ピラミッド型に構成されたコンピュータ・ネットワークの頂点に位置する中央の大型コンピュータに全ての情報を集中させて「一元管理」する形での「データマッチングの危険性」であり、データマッチングの主体は、その中央コンピュータの管理主体に限られていた。

しかし、「最適化」された「オープンシステム」型のコンピュータ・ネットワークシステムにおいては、ネットワーク上の各コンピュータにデータが「分散」していても、それらが「共通番号」をマスターキーとして名寄せできるのであるから、形式面において「一元管理」されていなくても、データマッチングの危険性はより高くなっているといいうる。つまり、ネットワーク上のどの端末からでも、どのデータベースにでもアクセスできるのであるから、誰もが

「データマッチングの主体」となりうるように変わるのである（例えば、特定の人物のプロファイリングを行いたい官庁や、特定の属性を有する人物群をあぶり出したい官庁などにとって、極めて“魅力的な”システムが出現することになるーアメリカでは、例えば「テロ対策」推進などの名の下に、このような「プロファイリング・ビジネス」が巨大化していることが知られている※。）。（また、更に言うならば、どこからでもアクセスできるということから、不正閲覧等の危険性もより一層高まっているのである。）

3 個人情報の収集、管理、利用等をする場合の「本人同意の原則」

(1) 以上のような危険性を防止するためには、国家機関等の公権力は、個人情報をみだりに収集・取得、保管・管理、利用、開示・提供することは許されず、個人情報を収集・取得、保管・管理、利用、開示・提供する際には、本人の同意を得ることを原則としなければならない※※。何故なら、利用する機関、利用目的、利用態様が本人（情報主体）において「同意」を通じて明らかにならなければ、そのプライバシーに対する影響を予測することができず、私生活の平穏や人格的自律を保つことが出来なくなるからである（上述のドイツ憲法裁判所判決参照）。

上記平成１５年９月１２日最高裁判決は、「プライバシーに係る情報は、取扱い方によっては、個人の人格的な権利利益を損なうおそれのあるものであるから、慎重に取り扱われる必要があ」り、「大学は、上告人らの意思に基づかずにみだりにこれを他者に開示することは許されない」と明確に判示しているところである。

また、上記名古屋高裁判決も、以下のように判示している。

※ 『プロファイリング・ビジネスー米国「諜報産業」の最強戦略』（ロバート・オハロー著、日経BP社）

※※個人情報保護に関する古典的基準ともいうべき１９８０年のＯＥＣＤガイドラインが、①収集制限の原則（個人データの収集には、制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである。）、②目的明確化の原則（個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないで、かつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである、などの原則を定めているのは、正にこのためであるといわなければならない。

「　憲法１３条は，すべての国民を個人として尊重し，個人が幸福を追求することを憲法上の権利として定めているところ，他人に知られたくない個人の私生活上の情報がみだりに開示されれば，個人の私的な生活領域における平穏が害され，個人の人格的自律が脅かされることとなるから，このような個人の私生活上の情報，すなわちプライバシーに係る情報を開示されないという期待は，憲法１３条によって保障される人格権の一内容として，法的保護を受けることができる利益に当たるものと解される。したがって，控訴人らが主張するような自己情報をコントロールする権利がプライバシー権として認められるか否かは別としても，国家機関が，正当な理由もないのに，個人の同意を得ず，みだりに個人の私生活上の情報を収集，開示することは，同条に反して許されないというべきである。」（28～29 頁）

(2)　そして、上述した理由から、この「本人の同意」は、すでに行政機関が（本人の同意を得て、一定の行政目的のために）収集、管理、利用している情報であったとしても、①その情報の利用目的を変更する場合、および、②その情報を保管・管理、利用、開示・提供の方法あるいは形態を変更する場合にも、改めて同意を必要とするべきである。

同意のない、利用目的の変更や保管・管理、利用、開示・提供の方法あるいは形態の変更はプライバシーの権利を侵害するものとして、原則として許されないと言わなければならない。

(3)　なお、住基法の改正という国会の承認を得たから、「本人の同意」に代えることができる（本人の同意が擬制できる）とすることもできない。

何故なら、①そもそも、国家との関係において、多数決（に基づく法律）によっても奪われない権利を保障するためにこそ、憲法の人権規定が存するからである。法律により全て「本人の同意」が擬制されるならば、プライバシー権は保障されていないに等しい。また、②住基ネットの導入を採用した住基法の改正は、参議院において委員会の「中間報告」――委員会審議の打ち切り――本会議の採決という手法が強行されて採決されたものであるが、

「中間報告」等は、国会法５６条の３の要件が存しなかったことが明らかであるにもかかわらず、強行されたものであり、その手続きには重大な瑕疵があったものであり（国会議事録）、③住基法の改正をめぐる審議においては、政府委員や大臣らによって、住基ネットの内容に関して重要な点で、虚偽の説明がなされ、議会では、虚偽の事実を基に住基ネットの導入を採用したものであり(同)、④さらに、行政が自己の保存するデータとマッチングすることが法律的に容認される事務(住基法３０条の１０に定める別表所定の事務)が国会での審議がほとんどなされないまま追加されているというのが現実である（同）から、到底、本人の同意に代わりうる国会の審議・承認がなされたとも認められないからである（『要録』14頁以下）。

4 「公共の福祉」による制限の限界について

(1) 憲法１３条は、「すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、その他の国政の上で、最大の尊重を必要とする。」と規定しており、幸福追求の権利も、「公共の福祉に反しない限り」保障されるとされている。この規定から、プライバシー権も公共の福祉による制限を受けるかどうか、そして、受けるとした場合の基準等が問題になる。

(2) この点、原判決は、「その収集，保有，利用等については，①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（もしくは，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するものではないと解するのが相当である。しかし，本人確認情報の漏えいや目的外利用などによる，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。」(50 頁)との判断基準を示

した上で、実現手段の合理性が存しないと結論づけた。

(3)　この点を検討するに、先に述べた現代高度情報化社会におけるプライバシー保障の重要性、および、そのためには、国家機関等が国民の個人情報を収集、管理、利用等する場合には、本人（情報主体）の同意を得ることを原則とするべきである。そして、同意のない収集、管理、利用等がいかなる場合に許されるべきか、と問題が立てられるべきである。

この観点から見て、原判決の基準は、更に以下のように具体化すべきである。

すなわち、①本人の同意なく全国民に対してインデックス情報たる「共通番号」(住民票コード)を付した上で、②各行政分野で収集保管している個人情報にこの「共通番号」を付け、③もって、“データマッチングのインフラ”たるコンピュータ・ネットワークシステムを作り出すことは、原則として許されない。そして、仮に例外的に許されるとしても、それにより実現しようとする行政目的に高度の正当性、必要性が必要であり、かつ、その目的実現のために侵害されるプライバシーの権利の内容および程度と、「対立法益」である行政事務の正当性・必要性、および、「より制限的でない他のとりうる手段の有無」（「共通番号」ではなく、事務毎の「限定番号」を用いることなども含む）を含む「相当な方法」であるか否かを含めて、慎重に利益衡量をする必要が存するといわなければならない。

より具体的にいうならば、

①　住基ネット制度の目的や内容自体が、プライバシーの権利・利益を著しく侵害するものである場合は、プライバシーの権利保障の重要性に鑑み、そもそもそのような収集、利用等を「公共の福祉」（行政の効率化など）の名の下に行うことは許されず、

②　侵害がその程度まで至らない場合は、被侵害権利・利益たるプライバシー（や人格的自律）の権利・利益の程度を、セキュリティの不備に基づく侵害の危険性も含めて検討し、「対立法益」である行政等の利益との利益

衡量を慎重に行うことになる。

そして、利益衡量を行う場合、

ⅰ）その行政目的の正当性や必要性がそもそも低い場合や、当該行政目的達成のために他のとりうる手段が存する場合などには、被侵害権利利益の程度がさほど高度でなくとも、そのような収集、利用等は許されず、

ⅱ）その行政目的の正当性や必要性が相当高度に存した場合でも、当該行政事務処理において、個人のプライバシー（や人格的自律）の保障に関して、制度的な欠陥がないかどうかなどを検討し、α）それらの権利・利益の侵害の危険性が相当程度認められる、もしくは、β）そのような懸念を抱くことに無理がないため「萎縮的効果」が認められるような場合には、このような個人のプライバシー（や人格的自律）の保障を犠牲にしてもなお達成すべき「高度の」必要性・合理性が存するか否かを基準として厳格に利益衡量すべきである。

ⅲ）そしてさらに、本件では、住基ネット制度全体の「差し止め」を求めているわけではなく、被上告人らの住民票コードの削除という「個別離脱」を求めているだけであるから、当該個人の本人確認情報を住基ネットを通じて収集、利用等することを明示的に拒否をする住民を含めて、全員を、強制的に住基ネットに参加させなくても重大な支障が存しないかどうかも、利益衡量の要素として考慮されなければならない。そして、重大な支障が存しない場合には、当該住民を強制的に参加させることが、憲法１３条に照らして許されないとすべきである。

（なお、類似訴訟である平成１８年１２月１１日名古屋高等裁判所金沢支部判決（以下、「高裁金沢支部判決」という）が、以下のとおり判示していることも参考となる(32～34頁)――①、②の段落分けは代理人が行ったものである。

「　したがって、国民は、国家機関等の公権力が、正当な理由がなく、社会生活上当然に受忍すべき限度を超えて、上記のような私生活上の自由及び平穏を違法に侵害する行為に及んだときには、憲法１３条に違反するものとして、

その差止め等の救済を求めることができるところ、

① 住基ネット規定が、国家機関等の公権力が、正当な理由がなく、社会生活上当然に受忍すべき限度を超えて、上記のような国民の私生活上の自由及び平穏を違法に侵害を許す内容のものである場合には、そのうち同侵害を許す部分については、憲法１３条に違反して無効となるというべきである。

② また、住基ネット規定そのものは当然に憲法１３条が保障するプライバシー権の侵害を許す内容のものではないが、住基ネットに使用されるシステムの安全に関する規定や住基ネットの管理運営に関してプライバシーの保護を担保する規定を欠くなどのために、使用されているシステムについて安全上無視し得ない欠陥があって、容易に外部からの侵入を許すものであったり住基ネットの管理及び運営が著しく杜撰になされ、住基ネットの管理運営に従事する者が不正に本人確認情報にアクセスするなどして、本人確認情報が簡単に漏えいし、あるいは流出する具体的な危険があるという場合にも、控訴人らがそのような住基ネットにおいて本人確認情報を取り扱うことは、国家機関等の公権力が、正当な理由がなく、社会生活上当然に受忍すべき限度を超えて、上記のような国民の私生活上の自由及び平穏を違法に侵害する場合として、住基ネット規定は憲法１３条に違反し無効となることがあるというべきである」

５ プライバシー権の侵害に対しては差し止め等の救済を求めることができることについて

(1) 国家機関等の公権力が、行政事務の処理に際し、(5)ウ で述べた①②の要件を欠き、個人のプライバシーの権利を侵害し、もしくは、侵害する危険が存在する場合には、その行政事務は、少なくとも、その行政事務の適用を肯定しない者との関係では憲法１３条に違反し無効である。したがって、当該個人は、公権力の行為の差し止め等の救済を求めることができるというべきである（『要録』16頁以下）。

(2) この点、平成１４年９月２４日最高裁判決(「石に泳ぐ魚」判決)は、以下の

ように判断している。

「人格的価値を侵害された者は、人格権に基づき、加害者に対し、現に行われている侵害行為を排除し、又は将来生ずべき侵害を予防するため、侵害行為の差止めを求めることができるものと解するのが相当である。どのような場合に侵害行為の差止めを求められるかは、侵害行為の対象となった人物の社会的地位や侵害行為の性質に留意しつつ、予想される侵害行為によって受ける被害者側の不利益と侵害行為を差し止めることによって受ける侵害者側の不利益とを比較衡量して決すべきである。そして、侵害行為が明らかに予想され、その侵害行為によって被害者が重大な損失を受けるおそれがあり、かつ、その回復を事後に図るのが不可能ないし著しく困難になると認められるときは侵害行為の差止めを肯認すべきである」

(3) この事案は、表現・出版の自由という、これまた憲法上厚く保護されるべき権利との利益衡量の場合であったが、それでも差止が認められている。

この事例と比較しても、本件の場合は、対立法益が「行政の効率化」などの政策的利益でしかないこと、及び、プライバシー権は一旦侵害されてしまえば事後の回復は事実上不可能という性質のものであること、制度は一旦作られてしまえばそれを元に戻すことは著しく困難であることなどの諸事情を勘案すれば、差し止めが認められるのは当然といわなければならない。そして、プライバシー侵害の場合、人格的自律を脅かす具体的な危険があると認識する相当な根拠がある場合には、(予防的) 差止め等の救済の対象となることもまた、明らかであるといわなければならない (なお、原判決はもちろん、上記東京高裁判決や高裁金沢支部判決もそのことを認めている)。

(4) なお、上告人らは、①プライバシーの権利は、それ自体では差止請求権の根拠となるような排他性を有する人格権として確立されておらず、また、②上記「石に泳ぐ魚判決」は、「名誉権及びプライバシー等が侵害されたときには、名誉権及びプライバシーの利益等を併せて出版の差止めが認められる場合があることを明らかにしたものにすぎず、プライバシーの権利のみを根拠とする

差止請求が可能である旨を判示したものではない」と主張する（上告理由書13頁）。

しかし、まず、①上述したように、プライバシー権も憲法１３条で保障される権利・利益である。また、②同事件は「出版の差止」という極めて高度に保障される権利の差止を認めた事案に関するものであるから、本件とは比較衡量する対立利益が全く異なる（低い）上に、同最高裁判決は、「人格的価値」を侵害された者の差止請求に関する基準を摘示しているものである。「プライバシー」が人格的価値に係る権利・利益であることは明白であるから、プライバシー侵害に基づく差止請求が認められるのは当然といわなければならない。

６　まとめ

(1)　以上、総論的に述べたように、冒頭に述べた上告人らの上告理由はいずれも失当である。そして、憲法１３条によって保護されるべき権利であるプライバシー権に関する諸問題について考察するならば、本件については、以下に指摘する利益衡量の要素が認められるというべきである。すなわち、

①　住基ネットは、「共通番号」たる住民票コードを国の機関等の個人情報データベースに付番するシステムである点で、そもそも名寄せ、データマッチングによるプライバシー（私生活の平穏や人格的自律）を侵害する危険性が高いものである。その上、全国すべての市町村や諸機関をコンピュータ・ネットワーク化するものであることから、セキュリティ面でも漏洩、改ざん等の危険性が高い。

よって、その権利侵害の程度は高く、原則として、このようなシステムは構築が許されないといわなければならない。そして、仮に構築が許されるとしても、前述のように厳しい要件を満たさなければならないと言わなければならない。

②　現行住基法や行政機関個人情報保護法などには、住民のプライバシーの保護に関して、制度的な欠陥があり、プライバシーの侵害の危険性が相当程度認められる、もしくは、そのように感じさせることがもっともであり、

③　かつ、全国自治体のセキュリティの実態は、これまたプライバシー侵害の危険性が相当程度認められる、もしくは、そのように感じさせることがもっともと認められる状態にある。

④　以上の危険性は、前述のように、コンピュータ・ネットワークという情報処理技術の特質上、従前の紙媒体の時代とは全く質的に異なる（大量性、高速性など）ものであるから、一瞬にして大量の無断情報取得、漏えいや改ざんにつながるものであって、「抽象的危険性」は一瞬にして「具体的危険性」から大量かつ回復不可能な実被害の発生へとつながる。すなわち、「抽象的危険性」と「具体的危険性」は紙一重であり、連続しているといえる。

かつ、情報を預けた（預けることを法的に強制させられた）住民の側からするならば、その住基ネットシステムの安全性は“ブラックボックス”と化しているから、その安全性(危険性)情報は、行政の側のみが保有している。

⑤　反面、住基ネットによって実現しようとする行政目的（住民の利便性や行政の効率化）は、ｉ）憲法上、絶対的な価値ではなく、ii）住民の利便性はほとんど認められない上に、行政の効率化については「費用対効果」の面から「壮大なムダ」を生み出している。さらに、iii）当該行政目的実現のためには他のとりうる手段が存するし、iv）当該行政目的は、住基ネット稼働後４年以上経過した現在においても、（住基カードの普及率に端的なように）全くといって良いほど実現しておらず、また、今後も実現する現実的根拠のある見込みは存しない（少なくも立証されていない）。

⑥　住基ネットに参加を拒否する国民全員を、強制的に参加させなくても、重大な支障は存しない。

⑦　以上のように、制度的に見て危険性の高いシステムを、しかも本人の同意なく、強制的に作るのであるから、その行政目的の正当性・必要性や、プライバシーの安全性に関する立証責任は、それを推進する行政の側にあるといわなければならないが、後述するように、その具体的な立証は全くと言っていいほどなされていない。

このような諸事情を踏まえるならば、住基ネットへの参加強制（住民票コード付番の強制や各データベースへの付番など）は、住民（被上告人）らの私生活の平穏と人格的自律を著しく脅かすものであり、住基ネットを運用することに、住民のプライバシー権の侵害を犠牲にしてもなお達成すべき「高度の」必要性・合理性は存しないといわざるを得ない。

そもそも「効率化」は人権保障と背反する性質を有するものである点につき、念のため付言する。

『憲法Ⅰ』（有斐閣・法律学全集３）において、清宮四郎教授が、権力分立について、以下のように指摘されている点は、権力者による情報の集中に対する関係でも（特に本人の同意による個別の抑制も、独立の第三者機関によるチェックによる抑制も存しない現行システムにおいては）そのまま妥当するといわなければならない。

「権力分立論は、もともと積極的に能率を増進せしめるための原理ではなくて、消極的に権力の乱用または権力の恣意的な行使を防止するための原理である。そのねらいは、アメリカのブランダイス(Brandeis)判事のいうように、摩擦を避けることではなくて、政府の権力を三つの部門に配分することにともなう、不可避的な摩擦によって、国民を専主政から救うことにあった。」（64頁）

「権力分立の第三の特性は、その、国家の権力及びそれを行使する人間に対する懐疑的又は悲観的な態度にある。すなわち、権力分立論は、国家の権力、従って、権力を行使する人間に対する不信任(non-confidence, Misstrauen, méfiance)から出発している。神ならばいざ知らず、人間はすべて、国家の権力というような強大なものを手にすると、それに酔わされてしまって,権力を乱用するようになるという、いわば宿命的な、弱点をもつとみなすのである。モンテスキューも、「全て権力を持つものはそれを乱用しがちである。…それは不断の経験の示すところだ」といっている。そうして、権力の乱用が行われては,何よりも大事な国民の自由が侵されてしまうから、まえもってこれを警戒し,権力の乱用が行われないようにするに越したことはないとし、そのためには,国家権力の内部組織について、立法、司法及び行政という三つの権力の種別に応じて、それぞれ構成を異にする機関を分離して独立に設け、それらが互いに抑制し合い、均衡を保つように仕組む必要があるというのである」（同）

原判決は、これらの点を正しく指摘し、その適用を拒否している被上告人らに住基ネットへの参加を強制することが、憲法１３条に違反すると認定したものであって、憲法１３条の解釈適用として正当である。反対に、上告人らの主張はまったく失当である。

(2)　なお、以上に述べたことより、情報主体の同意を得ずに、住民票コードを索引情報として本人確認情報を通知・提供し、行政の保有する情報とマッチングして利用する住基ネットシステムは、制度的に違憲、少なくともこれを拒否する者に強制的に適用する場合には違憲とすべきである。

さらに、本人確認情報が、プライバシーとして憲法上の保護を受けるべきものである以上、それを扱う住基法の各規定は、憲法に適合するように解釈・適用されなければならない。すなわち、住基法は、憲法１３条および守口市個人情報保護条例の各規定と体系的・合目的的に解釈されなければならない（憲法適合解釈、合憲的限定解釈）のである。そうすると、住基ネット規定の適用を拒否し、住民票コードの削除を求める被上告人らについて住民票コードの削除を認めることが、住基法及び守口市個人情報保護条例の正当な解釈であるともいえるものである。したがって、この見地から見ても、住民票コードの削除を命じた原判決の結論は、やはり正当であるといわなければならない（『要録』17頁以下）。

以下、上告人らの上告理由および原判決に即して更に詳述する。

第３　住基ネットの強制適用が憲法１３条に違反することについて
――その１　いわゆる名寄せ、データマッチングの危険について

１　上告理由の要旨

上告人らは、原判決が、「各行政機関の間でデータマッチングが進められ、行政機関が個別に保有する個人情報の範囲が拡大して、少数の行政機関によって、行政機関全体が保有する多くの部分の重要な個人情報が結合・集積され、

利用されていく可能性は決して小さくないといえると判示する」として、これについて、「原判決のいうような……事態が生じるのは、個々の国の機関等が住基法別表の事務処理を行うために管理している個人情報について、これらを扱う公務員が、法令上の根拠もないのにあえてこれを他の国の機関等に提供し、当該機関等がこれを集約管理した上で、（住基法）３０条の３４等に違反して本人確認情報を利用して名寄せやデータマッチングを行うような場合に限られるのである。しかし、本人確認情報の提供を認められている事務２９３（平成１８年５月１５日現在）における保有情報を一元的に管理する国の機関や主体は、存在しない。」「指定情報処理機関において、国の機関等が保有する情報を結合することは不可能である。」「本人確認情報の提供について、その対象となる事務が法改正により追加されるとしても、法定された事務を遂行する範囲を超えた利用を禁止する諸規定が改正されたわけではないから、対象事務の拡大によって、データマッチングの具体的危険が認められることにはならないとういうべきである。」などと述べ、原判決は誤りであると主張する（１９頁～）。

しかし、上告人らは、そもそも、原判決の趣旨を正確に理解していないものであって、まずこの点で主張自体失当であり、さらに、住基ネット制度を具体的に検討するならば、原判決が名寄せやデータマッチングについて認定したことはまさに正当であって、上告人らの主張は誤りである。

以下この点について述べる。

２　上告理由の誤り

(1) 原判決の判示に対する理解の誤り

上告人らは、上述のとおり、「原判決のいうような……事態が生じるのは、個々の国の機関等が住基法別表の事務処理を行うために管理している個人情報について、これらを扱う公務員が、法令上の根拠もないのにあえてこれを他の国の機関等に提供し、当該機関等がこれを集約管理した上で、（住基法）

３０条の３４等に違反して本人確認情報を利用して名寄せやデータマッチングを行うような場合に限られるのである。」ということを前提に論じている。

しかし、原判決は、まず、「提供される本人確認情報には、住民票コードが含まれており、したがって、情報センターから本人確認情報の提供を受ける行政事務に関するデータベースには、個人の情報に住民票コードが付されることになるから、これによって、そのデータベース内における検索が極めて容易になり、また、行政機関が収集・保存している膨大な個人情報をデータマッチングし、住民票コードをいわばマスターキーのように使って名寄せすることにより、個人情報を共同利用することを可能とするインフラが、住基ネットにより整備されたということができる。」と判示し（７４頁・傍点は代理人）、さらに、行政による個人情報の収集や取扱の実例を挙げ、「住基ネットの本人確認情報を利用して当該本人に対する個人情報が際限なく集積・結合されて、それが利用されていく危険性が具体的に存在することを窺わせる。」とし（８２頁以下）、「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うことができ（る）」と結論しているのである。

このように、原判決は、住民票コードを付した、コンピュータ・ネットワークという住基ネット制度の特質から、住基ネットには、名寄せやデータマッチングの危険が構造的に内包されていること、それにもかかわらずプライバシーを保護するための十全の措置が講じられていないことを導き出しているのである。しかるに上告人らはこれを、公務員が他の国の機関に情報を提供する問題としているものであって、問題の焦点をそらすものである。

(2) データマッチング等の現実的具体的危険について

ア　データマッチングとはどういうことか

まず、本件において、被上告人らのいうデータマッチングとは、行政機関が、国および地方公共団体が有する膨大な個人情報のデータベースに蓄積されている国民の個人情報を、住民票コード（もしくは、本人確認情報によって「統一」された氏名、住所等）をキーとして、名寄せしたり、突合したり、あるいは、個々のデータベースを統合（結合）して新たなデータベースを構築したりすることなどを指す。

その結果、従前、個別に管理・利用されていたデータベースの利用範囲が飛躍的に拡大し、行政機関によって、国民個々人が、全体として把握されることになる。

このような、自分のさまざまな個人情報が、自分の知らないところで、自分の同意なく、行政によって、収集、蓄積・保有、管理、利用などされるならば、「１人１人の行動というのがすべて把握されることになりますから、人々はプライバシーを失い、更には人間の自由であるとか尊厳であるとか、民主主義社会においては最も重視、尊重されなければならないものが、根こそぎ奪われることになる」（甲５９・斎藤貴男証言・３頁）、「一人一人の人間がそれぞれ生きていく人生というものが、すべて政府の手のひらの上のものにしかすぎなくなるということ。したがって、自由だとか尊厳だとか、人間が持っていなければいけないものが失われてしまう」「（その情報を掌握できるものに一人一人が）従属し支配されるしかない。そして、それが長い間そのような状態が続いていきますと反発することもできなくなる。つまり、それが当たり前になってしまって。ですから、人間存在そのものが今までと全く違うものになってしまうんではないかというふうに思います。そして、常に権力の目を意識しながら行動するようになっていくでしょう。そしてまた実際に力を持っている人が一人一人の人間をどのように動かすことも思いのまま、このような時代が来てしまいかねないというふうに考えています。」（同３５～３６頁）というよ

うになってしまうのである。

まさに国民は、行政によって管理されている（行政の前で丸裸にされている）という意識に陥らざるを得ない。公権力において、このようなことが自由に行われれば、個人の人格的生存に著しい萎縮的効果が生ずることはいうまでもないことである。

したがって、住基ネットの利用によって、そのようなデータマッチングがなされる、もしくはなされうる危険があるとするならば、住基ネットシステムの創設と運用そのものが、「公共の福祉」によって許容されるプライバシーの権利の制限をはるかに逸脱するものとして、違憲・違法といわねばならない。

イ　データマッチングの現実性

(ｱ) 住民票コードによる正確な「データマッチング」

a　住基ネットシステムの創設以前においても、国民個々人の個人情報はデータベース化されていたが、そのデータは、保有する行政諸機関によってバラバラに収集・保存されていた。したがって、正確な検索・名寄せはできなかったし、ましてやデータマッチングは困難であった。

たとえば、行政機関においては、いかなるデータベースにおいても、その「検索キー」（インデックス）たる、“本人を確認する情報”（＝氏名を中心に、住所、生年月日、性別など）が付されるが、これまでは、ある機関は、氏名について、略字（たとえば「斉藤」）で登録しているが、他の機関は、正字（「齋藤」）で登録をしていたり、住所についても、ある機関は、アパート名まで記載しているのに、他の機関はアパート名を省略して記載している等々、統一性がなかった。このように、データベースの「検索キー」である人物の特定に関する登録内容がバラバラでは、いくらコンピュータを駆使しても、コンピュータ上は別人物と認識してしまっていたのである。

逆に、赤の他人であっても、同姓同名（ましてや同一生年月日）の

データであれば、同一人物と認識して、検索・名寄せされていた（たとえば、「山本博」という人物は、裁判官でも、弁護士でも、アーチェリー選手でも存在するが、これが別人であることは、データベース上の「氏名」だけからでは判明しない）。

このように、住基ネットシステムが創設される以前は、正確な検索や名寄せを行うことはできなかったし、ましてやデータマッチングを行うことは著しく困難であった。

b　ところが住基ネットの導入によって事態は一変した。

住基ネットは、すべての国民に、決して重複することのない、その者固有の万人不同の１１ケタの番号（住民票コード）を付し、この番号のもとに、国民個々人の情報を管理するシステムだからである。この“万人不同”の番号がデータベースの「検索キー」として付加されたことにより、住基ネット導入以前は著しく困難であった、確実な検索・名寄せやデータマッチングが容易に可能となったのである。

c　さらに言うならば、住基ネットによって、住民票コード以外の、「氏名」「生年月日」「性別」「住所」を「検索キー」とした検索・名寄せおよびデータマッチングも可能となっている。なぜなら、これら「４情報」は、万人不同の住民票コードによって、住民基本台帳記載のものに、いったん“統一”されたために、氏名の「正字」、「略字」などの不統一はなくなった。したがって、以後は、住民票コードを利用しなくても、４情報による、正確な検索・名寄せ等が可能になったのである。

(イ) 同一省庁内の複数データベースの「本人確認情報」の統一化

a　また、現在住基ネットを利用することができる事務は２９３に増えているが、この２９３事務を扱う諸官庁は、当然にも２９３あるわけではない。現在住基ネットを利用することのできる２９３の事務は、１１の省庁が管轄しているのであり、ひとつの省庁が、いくつもの事

務を分掌しているのである。

b　しかも、この各省庁内のコンピュータは、庁内ＬＡＮで結ばれている。したがって、少なくとも、一つの庁内で事務ごとに“分散管理”されていた国民一人一人に関する事務のデータは、上述したように、今や、個々人の同一性の判断を阻害する要因がなくなったのであるから、同一庁内では、国民一人一人の固有の情報として容易にマッチングすることができることになったのである。

c　そのことは、当該省庁内につくられた２９３事務以外の個々人のデータファイルの情報とマッチングしうる可能性が十分あることを意味する。政府行政機関の保有する個人情報ファイルは、平成１８年３月３１日現在で８万６２４件にのぼる。しかも、その存在が公表されていないファイル（行政機関個人情報保護法１０条２項、１１条２項、３項）も多数存在している。

これらの情報が、マッチングされない保障はどこにもない（非公表のファイルに関しては、目的内利用かどうかのチェックすらしようがない。）。

d　以上のような状況をふまえるならば、現実的に、住基法所定の事務を媒介にして、その事務と関連するあらゆる行政事務に、住基ネットの本人確認情報が利用されているとみるべきである。「住基法所定の事務以外に使わない」との建前をいくら述べてみたところで、それをチェックするシステムが十全に講じられていない以上無意味というほかない。

それればかりではなく、次に述べる一省庁一システムのもとでは、住基ネットの本人確認情報が、他のあらゆる事務にも使われるとみなされるべきである。

(ｳ)　「最適化計画」

さらに、前述したように、政府省庁の情報システムは、統一的なコン

ピュータ・ネットワークとされ、そこで利用されるデータベースの仕様なども共通化されている。

a　すなわち、政府は、「一府省一ネットワーク」を中心とする情報システムの「最適化計画」を進めている（各府省情報化統括責任者連絡会議決定など）。この「最適化計画」は、

①　省内でのネットワークの一元化、

②　省内での端末の共有化による情報共有手段の確保、

③　運用管理業務の一元化、

を図るもので、省内のあらゆる機関を、ネットワーク化し、情報の共有化を図るとともに、その管理運用の一元化を図るものである。

このような、データの共有、マッチングを可能にするシステムの構築が、現に計画され、実現化されつつあるのである。これによれば、行政機関のどこででも、省内において“分散管理”されている国民個々人の情報を検索し、収集・結合して、保存し、管理、利用するということが可能になるものであるし、国民個々人のあらゆる情報を特定の機関に集中させることも可能となるのである。

b　そのうえ、霞ヶ関ＷＡＮによる省庁間のネットワーク化の推進も図られている。これにより、省庁間も霞ヶ関ＷＡＮによって相互にネットワーク化されるのであり、これを利用して同一省庁間のみならず、他の省庁に保有する国民個々人の個人情報もまた容易にマッチングすることが可能になっているのである。このようなシステムの下では、ある行政機関（たとえば警察庁）が、各省庁が保有している特定の個人のデータを収集することもいとも簡単にできることになる。

c　たとえば、現にすでに、２００５年（平成１７年）１月から、航空会社が提供する乗客等の電子データ情報を、警察庁、法務省、財務省が、それぞれ保有するデータベースと自動的に照合し、上陸審査、税関による検査、国際組織犯罪やテロ等に対する警察等の取り締まりに

利用する「事前旅客情報システム（ＡＰＩＳ）」が導入され、旅客の個人情報の省庁をまたがる集約、管理、利用がなされている。

このシステムは、警察庁、法務省及び財務省の３省庁により共同で運用されているが、航空会社は、旅客・乗員情報を、国際航空情報通信機構が整備した回線を経由して、警察庁、法務省及び財務省が、共同で運用する「ＡＰＩセンター」にネットワークを介して送信し、さらに同センターから３省庁にそれぞれに転送されて、３省庁が保有する、上陸拒否事由に該当する者及び指名手配されている被疑者等の氏名等を電子的に記録したデータベースと自動的に照合するものである。こうして、「我が国にとって好ましくない者」を特定し、入国管理局による上陸審査、税関による検査及び警察による取締りを的確かつ確実に実施することを可能とするというものである。

まさに、省庁を超えて保有されている特定の人物の個人情報を、複数の省庁が共同で利用する体制が整っていること、すなわち、個人情報のデータマッチングがなされていることを意味するものにほかならない。

なお、同制度による航空会社の情報提供は、２００６年５月、入管法の改正により、義務付けられた。

(エ) 地方自治体における住民票コードの利用には制限がない

全国の市区町村は、条例の根拠がなくとも、それぞれの事務処理に住民票コードを利用することが可能である。都道府県も、条例に定めさえすれば、利用が可能である（住基法３０条の８第１項２号）。こうして２９３事務以外にも、多くの事務で、既に住民票コードが本人確認に利用され、それらすべてのデータベースに住民票コードが記録されているのである。

ところで、地方自治体では、住基ネット稼働以前から、それぞれの自治体ごとに、いわゆる「既存住基システム」を運用し、そのデータベー

スには、自治体の行政事務に関連する様々な個人情報に関するデータベースが接続されていたものである。

例えば、市町村は、住民税の課税事務や所得証明書の発行事務を所掌しているから、納税や所得に関する情報を把握しているし、他にも、児童扶養手当、障害年金、上下水道料金、生活保護受給、固定資産税、給食費など、日常生活に密着した情報のデータベースがあり、それらは、既存住基システムと接続している。

既存住基システムには、住民票コードが記録されている以上、必然的に、自治体の行政事務において使われる個人情報と住民票コードは１対１で対応しているのである。

(オ) 情報管理システムの核としての住基ネット

加えて、住基ネットは、とりわけ住民票コードを活用することによって、すべての行政分野における情報管理システムのインフラとして活用・利用し得るものであり、そのようなものとして構築されたといい得るものである。

このことは以下の事情からして明らかである。

① 住民票コードは、その機能として、単に個人を識別できるというだけでなく、“どこの誰であるか”を正確に識別できる“マスターキー”である。すなわち、住民基本台帳という全国民の“現住所”とともに記録された台帳を基礎として、正確無比かつ容易に個人を特定、検索しうる「鍵コード」である（したがって、省庁をまたぐ複数のデータベースにおける個人情報を、正確に突合・データマッチングさせるために最適な機能を有すること、いいかえるならば、そのためにこそ「共通番号」たる住民票コードは存在する）。

② 国が、住基ネットは、電子政府・電子自治体の実現にとって必要不可欠の基盤となるシステムである旨位置づけている。

③ 実際に莫大な経費を費やして構築され、運用・維持管理されてお

り、現在の利用形態（住民票の広域交付など）だけでは、まったく費用対効果が成立しないこと（パスポートの電子申請による発行費用が、1通当たり1600万円という天文学的な馬鹿げた結果を生じさせ、膨大なムダを指摘され、廃止に追い込まれた事態に象徴されている）。

④ 言い換えれば、さらに利用方法を拡大しなければ“無用の長物”であり続けること（例えば鳥取県知事の「壮大なムダの仕掛け」という批判）。

⑤ 住基ネットは国民の個人情報を扱うコンピュータシステムとしては、唯一全国的利用が可能な巨大ネットワークシステムである。

⑥ 現に「ＩＴ戦略会議・ＩＴ合同会議」などの政府諮問機関、あるいは税制調査会などにおいて住民票コードの「納税者番号」や「社会保障番号」としての活用等が公然と議論されている。

これらのさまざまな事実とその進展を、総合的に、通常の判断能力をもって判断すれば、既述の情報管理システムが住基ネットと無縁に構築されるなどということは考えられない。

それらの情報管理システムにおいて、集約された情報が「誰の」情報であるかをもっとも確実に示すもの、つまり、データベースにインデックスとして付くものは、住民票を基礎とした「本人確認情報」（特に住民票コード）であると考えるのがもっとも合理的かつ「効率的」である（税制調査会の納税者番号に住民票コードを利用するという提言理由を参照されたい）。

このように、住基ネットは、すべての行政分野における情報管理システムのインフラとして構築されたといい得るものである。このことは、斎藤貴男氏が住基ネットに関して取材をした結果を述べた証言など（甲５９）からも明らかである。

「直接、住基ネットが利用されているものではない」などとして、「最

適化計画」を住基ネットとは無縁のもの、まさに、情報システムの「最適化」に、住基ネットが組み込まれていくことを見ることができないものは、ことの本質を見抜く洞察力を欠くものの謂いというほかない。

(カ) まとめ――データマッチングのシステムも主体も存在する

a　以上見てきたことから明らかなとおり、①住民票コードは、すべての国民に万人不同の共通番号として付すものであり、国民個々人を正確無比に同定することができるものである。②このため、個人情報データベースに付された住民票コードは、個人情報の名寄せや、統合の「マスターキー」であり、このマスターキーで開錠できる個人情報は、国・自治体を含めたあらゆる行政事務に及んでいるといえる。原判決や金沢地裁判決が、住民票コードを「マスターキー」と呼ぶのは、このような意味において、まさに正鵠を得た指摘なのである。③したがって、住民票コードもしくはこれによって同定された本人確認情報によって、これが付された国民個々人の情報データベースは、行政機関によって、容易に検索し、データマッチングすることが可能なものである。④そして、この住民票コードは、すでに、法律や条令に定められた「利用事務」だけでも膨大な数の個人情報に「インデックス情報」として付されている。⑤他方、各府省では、情報システムの「最適化計画」によって、省内でのネットワーク化や情報の共有化、さらに省庁間のネットワーク化を進められており、この結果、行政機関が保有する国民個々人の情報がマッチングし得ることができる体制が構築されている、といいうるものである。⑥そして、そのインデックスとして住民票コードを利用することが検討されており、これが違憲である旨認定されなければいつ実行されてもおかしくない状況に立ち至っているといえるものである。

b　このように、行政により、行政が集積している（従来は事務ごとにばらばらに集積されていた）国民の情報を検索し、名寄せして、結合

等することが技術的には可能になったのである。したがって、行政によって、特定の人物について、いつでも、必要な情報を集め、結合し、プロファイリングなどに利用できるシステムが完成しているといえるものであり、このことこそが、本件において問題にされるべきことである。

c　以上のように、住基ネットシステムを構築することによって、現段階においてすでに、行政機関によって住民の個人情報をデータマッチングすることが技術的に可能になったシステムが構築されたというべきである。「住基ネットの下では、住民票コードが付された本人確認情報を鍵（キー）として利用すれば、さまざまな箇所に保有されている個人情報を名寄せして結合して保管するということも技術的には容易になった」(平成１９年１０月１７日東京高裁判決・67頁)のである。

数年後の情報システム「最適化」の暁には、どの省庁からでも各データベースの個人情報の名寄せ、結合が可能となるのであるから、住基ネットを基礎としたデータマッチングに関して、そのシステムも主体もないという主張が誤りであることは明らかである。

ウ　法による抑止を過大評価する誤り

上告人らは、名寄せ、データマッチング（そして、漏洩など）は、住基法などの法律によって禁止等されており、さらに審議会・委員会などの監視・監督機関が存在するとして、その危険はない旨主張し、本件と同種事件の下級審裁判所のいくつかもこのように認定する。

しかし、上告人（及び上記の裁判所等）は、実質的に、条文を羅列するのみで、その条文の持つ意味や、それによって採用されている措置について具体的に検討しているわけではなく、以下において指摘するとおり、この点に関する上告人らの主張および上記裁判所の判断も明らかに誤りである。

(ｱ) 住基法３０条の３４の規定について

a　まず、同条は、「受領者は、その者が処理する事務であってこの法律の定めるところにより当該事務の処理に関し本人確認情報の提供を求めることができることとされているものの遂行に必要な範囲内で、受領した本人確認情報を利用し、又は提供するものとし、当該事務の処理以外の目的のために受領した本人確認情報の全部又は一部を利用し、又は提供してはならない。」と規定するだけである。すなわち、同条は「利用、提供における目的外利用の禁止」を定めてはいるものの、「データマッチングの禁止」を規定した条項ではない（上告人らや国なども、「法の許容しないデータマッチングは禁止されている」と、将来のデータマッチングの余地を大幅に残した主張しか行っていない点に注意しなければならない）。

したがって、法律の規定上は、法律に定めさえすれば、際限なく「データマッチング」は可能ということにならざるを得ない曖昧さを有している。

前述したように、住基ネットを利用する立場（情報処理をする国や行政の立場）から見れば、利用できる事務が多くなればなるほど、このようなシステムは非常に利便性が高いものとなり得るのであるから、プライバシー保護のためには明確な歯止めをかけておかなければ、取り返しの付かない事態を招来する危険性が極めて高いといわなければならない。

b　第２に、実際に、住基ネット稼働時に９３であった利用事務は、平成１８年５月段階で２９３と、３倍以上に拡大しているのである。

c　第３に、住基法別表の定める目的の範囲内かどうかの規定も、極めて広範である。例えば、「年金である給付の支給に関する事務であって総務省令で定めるもの」（別表第一の一六～二〇など）の「年金である給付の支給に関する事務」は、省令で相当広範な範囲の事務を、法で定めた「目的事務の範囲内」とすることができるのであり、濫用の

危険性が高いものである。

d　第４に、目的の範囲内かどうかの判断は、行政の長の判断に委ねられており、実際に法や省令で定めた事務の範囲内だけで利用されているかは、全く第三者によってチェックされていないのである。

プライバシーが保障されているというためには、少なくとも、ＥＵ諸国やカナダなどで採用されている「データ保護監察官」や「データ検査院」、「プライバシーコミッショナー」など「行政から独立した第三者機関」のチェックは必要であり、これすら存しない現状では、「データマッチングが行われていない」「行われる危険性も存しない」という保証など存しないと言わざるを得ない。

なお、国民個々人がチェックすることなど、事実上不可能である。何故なら、住基法の別表は、三省堂の「模範六法」ですら掲載されていない。ましてや、別表記載の「省令」に至っては有斐閣の「六法全書」ですら掲載されていないのである。かつ、仮にインターネット等で「省令」まで調べようとしたならば、２９３事務に関する省令を一つ一つ調べなければならないものであって、到底個人の能力の及ぶところではないのである（そもそも、どう数えたら、別表記載の事務数が２９３となるのか、全く不明である）。

e　そもそも、住民基本台帳制度は、「住民の居住関係の公証、選挙人名簿の登録その他の住民に関する事務の処理の基礎とするとともに住民の住所に関する届出等の簡素化を図り、あわせて住民に関する記録の適正な管理を図るため」に設けられた制度である（住基法１条）。

住民はこの目的のもとに、自己の情報を自治体に提供するものである。ところが、改正住基法による住基ネットは、上記「居住関係の公証等」の目的で提供された住民の情報を、「本人確認情報」として、利用するのである。住基ネットはそもそもその出発において、「目的外利用」がなされているといわざるを得ない（『要録』11頁）。

f　結局のところ、このような一般的な本人確認システムが作られ、行政の利便性が際限なく許容されるような制度の下では、住基法３０条の３４のような規定をもっては、「目的外利用」やデータマッチングによるプライバシー侵害に対する実効的な防止策とはならないというべきであり、少なくとも、ＥＵ並の「独立の第三者機関」による実効的なチェック(歯止め)がなければならないと解するべきである。

なお、同規定には罰則規定がなく、この点でも、目的外利用の歯止めとはならないといわなければならない。

(イ) 行政機関個人情報保護法の問題点について

また、行政機関個人情報保護法が、データマッチングを実効的に防止しうる法律でないことも明らかである。

a　個人情報の利用目的の変更（＝恒常的な目的外利用）の許容（第３条）

i　この点について、行政機関個人情報保護法は、個人情報の保有について、「法令の定める所掌事務を遂行するため必要な場合に限り、かつ、その利用の目的をできる限り特定しなければならない」とし（第１項）、「前項の規定により特定された利用の目的の達成に必要な範囲を超えて個人情報を保有してはならない」とも定めている（第２項）。しかし同法は、第３項において「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」であれば、保有する個人情報の保有を開始した利用目的を変更できるとされている。

そして、「相当の関連性を有すると合理的に認められる範囲」についての判断は行政機関自身の裁量によるのであるから、いとも簡単に、しかも外延が不明確な範囲で、個人情報の“利用目的の変更”が許容されることになる。

さらに、この“利用目的の変更”は、総務省自身、「利用目的以外の利用・提供が恒常的に行われる場合」をいうとしており（総務

省行政局監修「行政機関等個人情報保護法の解説」２６・２７頁。なお臨時的に利用目的以外の利用提供が行われる場合は８条２項の場合に該当するとされる）、これはまさしく「目的外利用」の一種にほかならない（原判決７８頁。）。

要するに、行政機関個人情報保護法は、恒常的に利用目的以外の利用・提供（＝目的外利用）を行う場合の可否の判断を行政機関の著しく広範な裁量に委ねているのである。

ii　上告人らは、同法は、住基法との関係では一般法であり、本人確認情報には、住基法の本人確認情報の保護規定が当然に優先して適用されるべきである旨主張する（１９頁）。

しかし、この３条３項に基づく“恒常的な目的外利用”に関しては“臨時的な目的外利用”の場合（８条２項）と異なり、改正住基法の優先適用を定める８条３項のような規定が存在しない。したがって、この点からも、３条３項に基づく“恒常的な目的外利用”については、改正住基法３０条の３４の違反は問題とならないというべきである。この点に関する原判決の判断は正当である。

b　個人情報の利用・提供の制限について（第８条）

①　行政機関個人情報保護法８条１項は、「行政機関の長は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない」と規定する。上告人らは、この「法令に基づく場合を除き」という規定により、住基法３０条の３４の「目的外利用、提供の制限」は解除されると主張する。そして、これにより、例えば、刑事訴訟法１９７条２項の「捜査照会」に対して、国の機関等は、受領した本人確認情報を含むデータを提供することが許されるとする。

しかし、行政機関個人情報保護法上、この「法令に基づく場合」というのは、かなり広範な例外として認められているため、仮にこのよ

うな解釈が許されるならば、一方で、行政機関個人情報保護法８条３項により、住基法３０条の３４の「目的外利用・提供の禁止」を特別法とした意味が失われてしまうことになる。

たとえば、警察が、「捜査照会」を用いて、対象者の資産・金融情報から健康情報まで、あらゆる情報を収集して分析していることは、各種の刑事事件や国家賠償事件等で裁判所に顕著な事実であって、これでは全面的な名寄せ・データマッチングを認めたに等しいものである。

② さらに、同条１項には、８条２項という例外規定も存在する。

すなわち、「……所掌事務の遂行に必要な限度で……利用する場合であって、……利用することについて相当な理由のあるとき」（同項２号）や、「……保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供にかかる個人情報を利用し、かつ、……利用することについて相当な理由のある場合」（３号）等には、“臨時の目的外利用”が許容されるのである。

この「相当な理由の存在」「必要な限度」「本人又は第三者の権利利益を不当に侵害するおそれがあると認められない」等の“制限”の要件自体非常に抽象的かつ曖昧である上、その存否の判断を当の行政機関が自ら行うのであるから、原判決が説くように、「実際には実効性のある利用制限の歯止めになり得ず、行政機関が住基ネット上における本人確認情報の利用を事実上自由に行いうることになってしまう」ことは明らかであり（８１頁）、これらがデータマッチングや名寄せを防止できるとする根拠にはなり得ないのである。

上告人らは、行政機関個人情報保護法８条３項が「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」と規定し、住基法３０条の３４が「他の法令」に当たるから、「法の許容しない目的外利用は禁止されている」と主張するが、実際の利

用においてこれが厳格に守られる保証は全くない。かつ、上記aに記載したように、行政機関個人情報保護法3条には、そもそもこのような8条3項のような規定すら存しないのである。

(ウ) 法などによる規制ということについて

以上のとおり、上告人らが主張する「住基法によるデータマッチングの禁止」という主張が根拠を欠くものであるが、さらに、上告人らの主張は、法を万能化する条文操作主義とでも言うべきものであり、以下に述べる事情等からするならば、データマッチングの危険を否定する根拠となりうるものではない。

a　法などによる禁止などが、違法行為の防止について万全な有効性を持つものではないことについては、いまさら多くを論じるまでもないことである。

公務員が守秘義務や遵守義務に違反した例は巷にあふれている。

住基ネットに関しても、北海道斜里町や、愛媛県愛南町などで、情報が流出した例が多く報道されている。それらはすべて、住基ネットの運営や保守に従事するものが、禁止規定を破って発生したものである。

b　先に詳しく論じたとおり、住基ネットによって、何よりも、国民の情報のデータマッチングが現実的、技術的、物理的に可能になったのである。このことを厳然たる事実として措定して、その危険性の現実的有無について検討が加えられなければならない。

さらにいうならば、住基ネットが既存のコンピュータ・ネットワークとは質的に異なるシステムであることをふまえ、そこにおけるプライバシーの保護について、単に法制度が整えられているかどうかを形式面で判断するのではなく、予想される運用も視野に入れ、制度や技術の一体性を念頭において具体的に検討する実質的思考こそが要請されるものである。

そもそも、住基法３０条の３４で、「目的外利用」の禁止規定が設けられているのはなぜなのか。それは、その背後に、住基ネットにおいては、もともと提供された本人確認情報が、「目的外利用」をなされる危険性が存在するという認識が背後にあるためと推察しうる。そうである以上、このような事態を防止するためには、単に「禁止」を命じるだけではなく、防止のために実効性のある措置を具体的に講じる必要があるというべきである。

しかしながら、住基ネットにおいては、以下に述べるとおり、データマッチングを防止するための実効的な十全な措置が講じられていないというべきである。

(ｳ) 独立した第三者監視機関の不存在

データマッチングを防止するための具体的な措置として上告人らは、監視機関の存在を主張する。

a しかしながら、まず、上告人らは、条文を羅列するだけで、そこで採用されている措置が具体的にいかに実効性があるかというように検討されているわけではまったくない。

b そして、実際、住基ネットにおいて、データマッチング等の目的外利用等を監視する行政から独立し、調査権限や是正権限等を有する第三者機関が存在しないことは、原判決が説くとおりである。

すなわち、行政機関に与えられた広範な裁量に基づく利用目的の変更の当否について、適切な第三者機関による監視の体制は整えられていない。

たとえば、上告人らが挙げる、改正住基法３０条の９第１項に定められる「都道府県の審議会」や同法３０条の１５第１項に定められる指定情報処理機関の「本人確認情報保護委員会」が、独立した第三者機関性の面、あるいは行政機関個人情報保護法ではその存在さえ知らされない個人情報ファイルが多数予定されていること（１０条２項、１１条２項、

３項）、国の行政機関等の本人確認情報の利用については調査権限がないことなどからすれば、適切な監視機関たりえないことは明らかである（原判決７９頁参照）。

（ＥＵ指令２８条における「完全に独立した」監視機関は、［A］処理対象のデータにアクセスする権限や、[B]監視を遂行するために必要なあらゆる情報を収集する権限、具体的には、ａ：データ対象者の権利や自由に危険を及ぼす可能性のあるデータ処理作業について、作業が実施される前に勧告を行う権限や、そうした勧告が適切に公開されることを確保する権限、ｂ：データのブロック化や消去ないし破壊を命じる権限、ｃ：データの処理を一時的ないし確定的に禁止する権限、ｄ：データ管理者に対する警告や懲戒権限、ｅ：データ処理において問題となる点を議会等に照会する権限をはじめとする実効的な介入権限、さらには、[c]個人情報保護法制に違反する措置に対して訴訟を提起し、あるいは違反を司法当局に通知する権限などを有する機関で、個人データの処理に対する個人の権利及び自由に関して、個人又は個人を代表する機関からの請求を受理するものとされている――中島徹・早稲田大学法務研究科教授の「意見書」(平成19年7月11日)23～24頁参照）

要するに、住基法上規定する「監視機関」は、制度の運営主体ないしそれに関連する機関が、自らを、あるいは相互をチェックしているに過ぎないものであり、これをもって安全性が確保できるなどといい得ないことは明らかである。

データマッチング等を防止するためには、ＥＵ等には存在する、それを独立に調査・是正する権限を有する「独立の第三者機関」、すなわち、住基法上の業務とまったく無関係な公平、独立たる第三者機関の設置が何よりも必要であるが、住基法ではこれら第三者機関の設置がまったく想定されていない。

これでは、「法律で制限されている」といっても、何ら実効性は存在しないと言わざるを得ない。

(エ) 利用事務の拡大について

なお、提供先や利用事務が法律の改正等によっていくらでも拡大しう

る点について、国会において討議され、議決されることをもって、目的外利用の禁止の実効性を妨げるものではないなどとする見解が存する。

しかし、当初９３事務に過ぎなかった利用事務が、現在では２９３事務にまで拡大され、さらに拡大されようとしている。すでに、利用対象事務を把握することは一般国民にとって、著しい困難を伴うものとなっている（しかもそのほとんどは、国会による審議が行われることなく、拡大されている。）。

そのうえ、上述したように、条例によっても自治体が独自に他の機関に本人確認情報を提供することも可能であり、利用事務はさらに際限なく拡大していくものである（現に、膨大な補助金を使って、拡大されつつある）。

そうした場合に、何が目的内で何が目的外であるのかを判断し、目的外の利用について禁止してゆくことは、実際には著しく困難である。

しかも、改正住基法や行政機関個人情報保護法は、行政機関自身の判断による「関連性を有する」「相当な場合」の目的外利用を認めているのであるから、利用事務が拡大することで、これらと「関連性を有する」「相当な場合」も広範囲に拡大し、住基法の規定が実質を伴わない禁止にますます堕することになるのは必然である。

また、法などによる規制が住基ネットの運用関係者などによって破られており、歯止めにはなりえないことは、愛媛県愛南町における流出事件をはじめ数多くの実例が示すところである。

(オ) 小括――実効性ある防止措置は講じられていない

以上のとおり、原判決において指摘されているとおり、改正住基法や行政機関個人情報保護法を子細に検討すれば、これらにより、目的外利用が実効性を持って禁止されているとは到底いえないし、ましてや、これを担保する刑事罰や住民票コードによる本人確認情報検索の制限等によって名寄せを禁ずる「実効性ある防止措置が講じられてい

る」などと評価できないことも明らかである。それらの不正使用を監視する独立の機関も存しない。

よって、この点における上告人らの主張の誤りも明白である。

エ　まとめ

(ア) 以上見てきたように、改正住基法により住基ネットシステムが創設されたことによって、国民個々人の情報をデータマッチングするシステムは基本的に完成したといえるものである。そして、実際にもデータマッチングすることは十分可能であり、その現実性が高度に存するものである。

にもかかわらず、改正住基法その他の法令等によって、このようなデータマッチングを防止する実効的な対策は何ら講じられていない。

それだけではなく、行政による国民個々人の情報をマッチングするシステムや体制がますます構築されようとしており、住基ネット――とりわけ、住民票コードとネットワークシステムは、その中心軸となるものというほかないのである。

このように、現状においても、国民個々人は、「行政機関の前で丸裸にされるがごとき状態」におかれているし、少なくとも、被上告人らがそのような事態が生ずる具体的危険があると認識することには相当の根拠があるというべきであり、住基ネットの稼働は、国民個々人を萎縮させ、人格的自律を著しく脅かしているというべきである。

(イ) 以上のとおり、上告人らの主張は、国民のもっとも根源的な人権であり、民主主義の基本ともなる国民の「プライバシー」や「自律権」を保障するという観点から見て、憲法１３条の趣意を見失った誤りの主張というほかない。この点からして本件上告は棄却されるべきである。

第４　住基ネットの強制適用が憲法１３条に違反することについて
――その２「漏えい・改ざん等の危険」を併せ考えるべきこと

1　セキュリティ上の「危険性」の位置づけについて

(1) 住基ネットシステムの創設と運用によって、被上告人らのプライバシー情報が、漏えい・改ざん等の相当な具体性ある危険にさらされるようになっている。

原判決は、「現時点において、住基ネットのセキュリティが不備で、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」（74頁）と認定しているが、原判決の認定した諸事実を前提とし、その他発生している自治体からの情報漏洩等の公知の事実を加味するならば、「データマッチング」の危険性と併せて、住基ネットの危険性は裏付けられているといわなければならない。

(2) 第２、１、(2)で述べたとおり、現代のプライバシー情報の多くは、コンピュータによりデジタル情報として管理され、それらのコンピュータはネットワーク化されている。これにより、紙媒体時代の情報処理やセキュリティ（安全管理）技術とは、全く質的に異なる時代に入っている。

したがって、この質的転換に応じて、その「セキュリティ（安全管理）」対策も質的転換を遂げ、飛躍的に向上させなければ「安全」は保てなくなっている（甲22・長野侵入実験に関する聴取報告書２など）。

(3) 本件では、住民票コードを「マスターキー」とした名寄せ・データマッチングの危険性により、プライバシー権（私生活の平穏や人格的自律）などが侵害されていることを第１に問題としているが、この危険性は、「仮にセキュリティ(安全管理）が『万全』である」としても問題となるものである。そして、逆に、「仮にデータマッチングの危険性がない」としても、セキュリティ面の問題からプライバシー権等が侵害されることもあるから、「セキュリティ」に重大な問題があれば、その点からだけでも差止が可能となるものである（上述の高裁金沢支部判決は、そのことを示していると解される）。

本件においては、データマッチングの危険性が存する上に、セキュリティ(安全管理)上の危険性も高度である――住基ネット稼働開始時において、そのセキュリティが杜撰であったし、現在においてもなお、全国的コンピ

ュータ・ネットワークを安全に稼働させる水準には足りない安全性しか備えていない――から、憲法１３条に基づき、差止（被上告人らの住民票コード削除による個別離脱）が認められるべきであることを主張するものであるから、上告人らの上告理由の当否を判断するに当たっては、この点も加味すべきである。

２　セキュリティに関する安全基準と立証責任について

(1)　プライバシーという最も根源的でかつ傷つきやすい（上述したように、いったん漏えい・流出したならば、回復不可能である）人権に関して、原判決で認定されたような自治体現場における杜撰ともいえる管理運営の実態が認められながら、形式的な法規制のみで「安全性が確保されている」と判断することは誤りである。しかも、上告人らや大阪府、国などは、被上告人ら住民から、その大切なプライバシー情報を預かっている（ある面では、法的強制力を持って提出させている）のである。したがって、そのセキュリティを維持する義務（安全管理義務）は、一般私人間の契約に基づく安全管理義務よりも高度でなければならないとすらいえる。

(2)　以上述べたことから、安全性の有無については、少なくとも、被上告人らの指摘する安全管理上の問題点について、全国の現場等においてその安全管理が一定水準であることが立証されない限り、その安全性は確保されていないと推定されるべきである――平成１８年３月に発覚した北海道斜里町における漏洩事件、そして平成１９年５月に発覚した愛媛県愛南町ほかにおける住民票コードを含む住民情報大量漏洩事件など、相次いで自治体における情報漏洩事件が発覚しているのは公知の事実であるが、これらの事件に鑑みるならば、むしろ安全性は確保されていない――特に、保守や運営に従事する内部関係者による流出・漏洩等の危険に対する安全性は確保されていない――という推定が強く働くと言わざるを得ない。

以下、その要点のみを指摘する。

ア　「新たな危険性」の発生

まず、住基ネットシステムの構築によって、以下の危険性が新たに発生している。

① 今まで閲覧等することが不可能であった、他の自治体住民の本人確認情報の閲覧が可能となったこと。

② データの保存箇所が、住所地自治体だけでなく、都道府県、地方自治情報センターも含めて３倍になったことに伴って、(特に内部関係者による)不正閲覧・盗難、もしくは近時頻発している過失による漏えい等の危険が増大したこと。

③ 全国的ネットワーク網の構築により、ネットワーク経由の侵入の危険性も増大したこと。

④ 不正閲覧の誘惑が増大していること（とりわけ、金融業者などにおいては、住民基本台帳の閲覧等が厳格に制限されるように法改正（平成１８年６月。同年１１月１日施行）、条例の改正等がなされた後では、債務者の本人確認情報（特に現住民票所在地）を探知することに対して、高い需要が存する）。

⑤ 住基カードの不正取得などにより、身分証明を偽装される危険性が発生していること、等々。

イ 現場の実態は、現代のコンピュータ・ネットワーク時代の安全水準を備えていない

原審で取り調べられ、そして、一部原判決が認定しているように、現場のセキュリティの実態は、現代において求められている水準に達していない自治体が数多く存する。例えば、以下の点に端的である。

(ｱ)(a) 本件原原審とは別の大阪地裁における同種訴訟において、自治体の住基ネット担当者に対する証人尋問（甲 53～57）で明らかとなった、「セキュリティ基準」違反の杜撰な安全管理状況(入退室管理等)。

(b) 兵庫県下の自治体における「セキュリティ体制のチェックリスト」（甲 63～77）で判明した、①ＣＳ端末を庁内ＬＡＮ上に設置し

ている（姫路市、猪名川町、明石市、宝塚市－しかも、明石市は既存住基端末とＣＳ端末の共用端末となっている）、②庁内ＬＡＮ上の端末からインターネット接続が可能（姫路市、加古川市、猪名川町、芦屋市、伊丹市－なお、芦屋市、伊丹市はＤＭＺ構成にもしていない）などの問題（なお、これらの問題点のうち、「共用端末」などの点は、原判決が述べるように、「セキュリティの極めて基本的な事柄についてのものであることから、その後の兵庫県の指導等により改善措置が講じられたであろうと推認して差し支えないと思われる」（73 頁）というようなものではなく、未だに問題点を抱えたままであろうと推認されるものである）。

(ｲ)　地方自治体の現場においては、「セキュリティ対策上のイロハのイ」とされているＣＳサーバや既存住基サーバなどへの「セキュリティパッチ当て」（ソフトの欠陥を修正するプログラムをインストールすること）すら行われていないところが多数存すること。このことにより、ごく初歩的な攻撃をかけさえすれば、当該サーバや端末の管理者権限＝当該コンピュータに関するオールマイティともいえる権限＝を奪取することが可能となる、極めて危険なセキュリティ上の脆弱性がある(ちなみに、長野侵入実験が明らかにした脆弱性の第１は、まず大前提として行われなければいけないセキュリティパッチ当てすら、「内部関係者しか扱わないことになっているから安全である」ことを理由として、全く行われていない現場が多数存することを明らかにしたことである）。

(ｳ)　長野侵入実験などにおいて、パスワードの管理が非常に杜撰であることが明らかになっている、などである。

(ｴ)　これらに加えて、最近においても、内部関係者による不正閲覧や情報持ち出し、その過失による漏えい・流出事件が頻発していること（最近のものだけでも、自衛隊、警察(愛媛県警など)、国税局などからのＷｉｎｎｙを介した流出事件が相次ぎ、また、戸籍情報の漏洩や社会保険庁

職員による年金加入情報の不正閲覧事件などが頻発していること）は公知の事実である。また、１９９８年の、宇治市において発生した、システム開発会社の下請け関係者が、２２万件もの住民基本台帳情報を不正に持ち出し、売却したという事件（発覚は、翌９９年）は、裁判にもなった、忘れてはならない事件である。

ウ　これらの諸事実が認められるならば、そして、個人情報の流出事件が相次いでいるということに鑑みるならば、安全管理体制に問題があることは優に推認できるものである（「ハインリッヒの法則」[1]※参照）。

(3)　コンピュータ・ネットワークが発達した現代社会においては、このようないわば「抽象的危険性」は、一瞬にして「具体的危険性」に転化し、かつほぼ即時に被害として現実化して、重大かつ回復不可能な損害を発生させる。その意味において、「抽象的危険性」と「具体的危険性」は紙一重である。それがコンピュータ・ネットワークにおける情報漏洩等の危険性の特質である。これらの諸点について、全国すべての現場において、安全対策が整えられているという立証はなされていないのであるから、その「具体的危険性」は優に認められるべきものである。

３　「住基ネットそのもののセキュリティに問題には繋がらない」とはいえない

ところで、上述の流出事件などに対して、「住基ネットそのもののセキュリティに問題が存在したことには繋がらない」と考えるむきも存するので、その誤りについて付言する。

「セキュリティ」を評価する上において、「住基ネットそのもの」と　「それ以外」とを截然と区別することはできない。何故なら、第１に、住基ネットのセキュリティにおいて、「守るべきは、住基ネットそのものではなくて、住基ネットの中で利用される情報である」からである（中の情報を守るためのひ

1

※重大な災害１件が発生する背景には、軽度の災害が 29 件、そして災害にまでは至らなかった事故が 300 件存在する。すなわち１：２９：３００という比率を、ハインリッヒの法則という。このうち、組織の上層部にまで報告されるのは３３０件のうち多くて３０件、内部の意思疎通に問題を抱える企業の場合は、最悪の事態の１件だけで、あとは“隠される”。（現代用語の基礎知識 2006）

とつの防御策として、住基ネット本体への侵入がなされないようにする、という関係になるのであって、どこから漏れたかは問題ではない。住基ネット本体への侵入防止が完璧であったからといって、住基ネット（で利用される情報）の安全性が完璧であるとは全くいえない。特に、愛媛県愛南町における情報流出などは、住基ネットの中でも利用されている「本人確認情報」（６情報）が、住民票コードも含めてほぼ全町民分流出してしまったという事態なのである。そして、第２に、第１で指摘した点とも関係するが、物理的に、住基ネットシステムと既存住基システムとは、ネットワークで接続され、緊密に連携をとっているからである（既存住基サーバのデータがＣＳを通じて住基ネット上に送信されるのであるし、逆に、転入などにおいては、住基ネットからＣＳを通じて既存住基サーバにデータが送り込まれるのである。さらに、上述したように、一部の自治体では、１台の端末を既存住基端末とＣＳ端末の共用端末として使用したり、ＣＳ端末を既存住基系列の庁内ＬＡＮ上に置いたりしてもいる。）。

のみならず、第３に、人的にも、住基ネットも既存住基も、同一人物（職員や保守管理を担当する会社関係者）が、同一職場で取り扱うものであるからである。主体である「人」を捨象して「セキュリティ(技術）」を語ることはできないものである（このことは、甲22「聴き取り報告書２」24～25頁で紹介されているように、いくら解読困難な「暗号」を用いていても、それを用いる「人」が、安易な「暗号用パスワード」を用いたり、「暗号用パスワード」の管理を怠ったりすれば、その強固な「暗号」も、セキュリティ上何の意味もなくなる、という例を考えれば、よく理解できるものである）。

４　小括

以上述べてきたように、原判決の「セキュリティ」（安全管理）に対する判断は、憲法１３条の保障するプライバシー権に対する侵害性を判断するものとしては、甘いと言わなければならない。上述の「セキュリティ」上の危険性も併せ考えるならば、住基ネットの危険性は原判決の認定以上に高度であるといわなければならない。

第５　住基ネットには、住民のプライバシーの権利を犠牲にしてもなお達成すべき高度の必要性はないこと

１　住基ネットの強制的適用が許されるのはいかなる場合か

(1) 原審で詳しく論じたとおり、そして前述の第２の４（『公共の福祉』による制限の限界について）でも再説したように、コンピュータおよびインターネットを中心に高度に情報化社会として発展した現代社会においては、個人のプライバシーの保護は、極めて重要な問題である。

(2)ア　そもそもプライバシー権（自己情報コントロール権）は、憲法１３条に根拠を持つ権利であるのだから、憲法１３条の個人を個人として尊重する権利として、すなわち、人格的自律を保障する権利としてとらえられなければならないことはいうまでもない。そして、人格的自律ということは、他からの制御から脱して、自己の立てた規範に従って行動し、身を律するということであるのだから、それが権利として認められるということは、他者から自己の存立を容喙されないというものというべきである。

したがって、第三者が他者の存立に容喙しようとする場合には、当該本人の同意を要するということが、この権利の根幹となるものというべきである（同意原則）。

イ　このことは、たとえば、憲法１３条の権利とされている「肖像権」について考えてみれば明らかである。すなわち、人は、自分の顔ぼう等を外部にさらしている。したがって、他者は、人の顔ぼう等を容易に見、記録することができる。しかし、肖像権は、この自ら外部にさらしている顔ぼう等についても、これを撮影したり記録することについて、同意を原則として、一定の厳格な要件が存する場合にはじめて、同意のない撮影や記録が許容されるとされているのである。

ウ　したがって、とりわけ国家権力が、国民の個人情報を利用したり、他へ提

供をしたりする場合は、当該個人の同意を得ることを原則とするべきである。

例外的な当該個人の同意をえない個人情報の利用提供等は、①同意を得ることができない特別の事情がある場合、ないしは②同意を必要としないほどの必要性・有用性・合理性、言い換えれば、同意を得なくても実現しなければならないほどの「高度」の必要性・有用性、合理性がある場合に限って許容されるというべきである。

これをさらに他の側面からいうならば、その目的を達成するために失われる国民の権利利益との対比の上で、そのような国民の権利利益を犠牲にしてもなお達成すべき高度の必要性・有用性が存することが許容の要件とされるべきである。

(3) しかもコンピュータ・ネットワーク社会においては、紙媒体社会に比し、個人情報は無限に集積されうるし、その利用価値は著しく大きい。そして個人情報の侵害は容易であるし、プライバシーは、その性格からして侵害されたら取り返しが付かないものである。つまり、プライバシーが一旦侵害された場合、その被害は無限に拡がり、甚大となる。

また、その被害を、当事者において直ちに認識することも困難であり、たとえ認識できたとしても、その後に被害を回復することは絶望的である。

したがって、現代社会においては、個人の情報の扱いについては、慎重の上にも慎重であらねばならない。

(4) とりわけ、行政機関は、国民の個人情報を、権力をもって扱うものである。したがって、行政機関が、その公権力を行使し、権力をもって強制的に本人の意思に反して、国民のプライバシー情報を収集・取得し、管理・保有・利用し、開示・提供することが許容されるためには、その収集等の目的――特に、特定行政事務内における「限定番号」を用いた事務の効率化などではなく、本件住基ネットシステムのような「共通番号」を用いた汎用の本人確認システムを構築するという、危険性の高いシステムを作る目的――及びその目的達成のために用いる手段について、厳格な合理性が必要である。

すなわち、前述（第２の４の「『公共の福祉』による制限の限界について」）したとおり、個人情報を収集・利用等する目的が合理的かつ正当であることはもちろん、その目的を達成する手段・方法としても、より制限的でない他のとりうる手段は存在しないといえる程度の厳格な合理性が必要である、というべきである。

(5) それだけでなく、本件住基ネットのように、行政機関が進める施策が国民に対して一律かつ強制的に適用されるものである場合には、そのように全ての国民が一律かつ強制的な適用を受けなければ有効適切な施策として成り立たず、重大な支障が生じるような場合でなければ、自己の意思に反した個人情報の利用等について、自らのプライバシーが侵害されるとして、これを明示的に拒否する国民に対して強制的に適用することは許されないというべきである。

言い換えれば、その適用を明示的に拒否する国民をも一律にこの施策の適用対象としなければ、正当な行政目的の達成に重大な支障が生じると言いうるほどの高度の必要性、重要性が認められる場合でない限り、明示的に拒否をする者を強制的に参加させることは、この拒否をする者との関係ではプライバシー侵害として許されない、というべきである。

(6) 以上のように考えるならば、住基ネットによって、自己の情報が流通させられることをプライバシーの侵害であるとしてこれへの参加を明示的に拒否する者、すなわちプライバシーの権利を放棄していない者に対しても、その意に反して住基ネットへ強制的に参加させることが同意原則の例外として許容されるためには、少なくとも、

① 住基ネットを運用することによって、当該国民のプライバシーの権利を犠牲にしてもなお達成すべき高度の必要性が存し（目的達成手段としての高度の必要性）、

② さらに、すべての国民が住基ネットの適用を受けなければ、施策として成り立たないような重大な支障が存する場合

という２つの要件を具備する必要があるというべきである。

そして、以下述べるとおり、住基ネットには、①国民のプライバシーの権利を犠牲にしてもなお達成すべき高度の必要性は存せず、また、②被上告人らがこれに参加しなくても、行政目的の達成に重大な支障が生じないことも明らかである。

つまり、住基ネットを、参加を拒絶する住民に対しても強制的適用することは、プライバシーの侵害として憲法上許されないのである。

2　高度の必要性の不存在

この点に関し、原審等において上告人らが主張してきたのは、住基ネットが、①行政事務の効率化に資すること、②「電子政府・電子自治体」の基盤となるシステムであること、③住民の利便性の向上及び負担の軽減に貢献すること等である。

しかし、これらの主張は、いずれも誤りである。

(1)　「住基ネットは行政事務の効率化に資する」という主張の誤り

まず住基ネットは、「行政事務の効率化に資する」とされている点について検討する。

一般に「事務の効率化」は、まず何よりもその経費の削減を目的とするものである。しかしながら、住基ネットは、経費の節減をもたらすものではなく、逆に、地方公共団体に多大の経費の増大をもたらすものであって、極めて非効率的なものである。

ア　「効率化試算」のデタラメさ

「効率化」の点に関して、国は、まず、住基ネットの構築にかかる費用について、システム開発経費等の導入的な経費として約３９０億円、コンピュータ維持費等の年間経費として約１９０億円を見込み（甲３８の添付資料１０参照）、これに対する便益については、行政側のコスト削減として年間約２４０億円の便益がある（甲３８の添付資料１１等）と見込んだ試算を行った。

これに対し、被上告人らは、黒田充氏の、客観的なデータや資料に基づく意見書（甲３８）等によりながら、上述の国の「試算」は、そもそも前提とする数値自体虚偽のものであるか、少なくとも、恣意的なものというほかなく「行政事務の効率化」を裏付ける資料足り得ないものであることを指摘した。

例えば、国の試算は、住民の半数が住基カードを所持することを前提としたものであるが、住基カードの現実の普及率は、平成１７年３月末現在で、交付枚数５４万枚、住基人口の０．４３％にすぎないのであった（甲４０のうちの毎日新聞社説等参照。その後も現在に至るまで、住基カードの普及が全く進んでいないことは公知の事実である。）。

金沢地裁判決（甲３９）においても、このような国の「試算」は「参考に値しない」と厳しく排除されているところである（８２頁）。

イ　ランニングコスト・更新費用などの負担の無視

また、国は、前述の試算において、住基ネットシステムの維持管理等に要する経費（保守管理・プログラムの更新など）についてまったく埒外においている。

そもそも住基ネット導入により、毎年のランニングコストとして人的面でも、設備面でも、膨大な経費がかかる（甲３８の１０頁参照）。

例えば、常識的に考えれば当然のことであるが、住基ネットのような巨大なコンピュータ・ネットワークの安全性を維持するためには、セキュリティ対策（たとえばセキュリティホールにたいするパッチ当てなど）を含めて、高度の専門知識と操作能力を必要とする。

しかし、いうまでもなく、地方自治体においては、特定の職員が生涯一貫して同一業務に従事するわけではなく、人事の交代が避けられない。その人事の交代に当たって、その都度、住基ネットの従事者にたいする高度の専門教育・研修が特別に必要になる。

また、コンピュータのハード、ソフトも年とともにバージョンアップし、

その都度、特別の導入費がかかる。メンテナンスに要する費用も莫大なものである。特に機器の更新の際に要する費用は莫大なものとなる。

この点は、原審判決においても、「市町村に求められる効率化以上の負担を課すところもなきにしもあらず」と認定されている（５８頁）ところであり、金沢地裁判決（甲３９）においても、長野県の試算として、平成２９年に至ってもなお、累計的にはマイナス（住基ネットの導入・維持管理による損失が利益を上回る）であることが明らかにされているところであって、いずれにせよ、住基ネットは、市町村にとって、明らかに負担増大をもたらすもの以外の何ものでもない。

この点に関して、上告人らは、具体的な反論を行っていない。

ウ　自治体現場の声

以上のことは、全国各地で提訴された本件と同種の訴訟の審理において、自治体現場からの声としても明らかにされてきている。

例えば、平成１７年７月６日に東京地裁民事第５０部において実施された上原公子国立市長（当時）の尋問調書（甲５８）などによれば、住基ネットは、市町村の各自治体の業務の効率化に資するところがほとんどないことが窺え、これに要する莫大な経費が、財政難にあえぐ各地方自治体にとって、非常に重荷となっていることが窺える。とりわけ、小規模自治体において事態は深刻である。

なお全国各地で提訴された本件と同種の訴訟において、各地の自治体に対する調査嘱託が実施されているが、その結果からも、費用削減効果はなく、費用負担だけが重くのしかかってきている現実が判明している。

実際、被上告人らが居住する守口市においては、住基ネット運用のために、導入準備の平成１３年度から平成１８年度末までで、新たに４８１２万３５０２円の財政負担が発生しているが、その一方で住基事務に係る職員数の削減は見られない。

エ　小括

このように、本件住基ネットは、「行政事務の効率化」をもたらすものではない。逆に、地方公共団体に多大の経費の増大をもたらすものであり、極めて非効率的なものである。現に甲４０の毎日新聞社説では「行政の不効率化でしかない」と断じられているところである。

したがって、少なくとも国民のプライバシーの権利を侵害してもなお余りあるような効率化の利益が存しないことは明らかである。

(2) 「電子政府・電子自治体の基盤となる」という主張の誤り

そもそも、住基ネット導入の法的根拠である改正住基法の審議の際には、「電子政府・電子自治体」の基盤などという議論はなされておらず、このような後付の理由は立法事実足り得ないというべきである。

また、上告人らの主張は、公的個人認証サービスへの利用の点を除いては、非常に抽象的なものである。

しかも、公的個人認証サービスに関しても、そのために住基ネットが不可欠なシステムであることは何ら具体的に論じられていない。実は、公的個人認証サービスの提供は、住基ネット以外の方法でいくらでも可能なのである（甲 38・7 頁）。

このように、この点に関する上告人らの主張は、非常に漠としたものであり、被上告人らのプライバシーを制約する根拠足り得ないものであることは明らかである。

(3) 「住民の利便性の向上及び負担の軽減に貢献する」という主張の誤り

ア　上告人らは、住民の多数にとって住基ネットは便利であるとし、これをもって、被上告人らのプライバシーの権利を犠牲にしてまで住基ネットを甘受しなければならないことの根拠としている。

そして、住民の利便性が向上したという具体例としては「住民票の広域交付」が可能となったことなどを挙げている。

また、国も、この点について、莫大な「経済的利益」が存するかのような「試算」を行っている（甲３８の添付資料１０）。

しかしこの「試算」も現実とはまったくかけ離れたものである。

そして、この点についても、被上告人らは、原審等において、その誤りについて具体的に主張・立証を行った（甲３８ほか）。

すなわち今日まで、「広域交付」の利用率は、通勤･通学の範囲が広大な東京都などの大都会においてすら極めて低率なのであり(甲３９の２頁等)、これは原審判決においても認められている。守口市でも、平成１５年度から１８年度までの４年間の累計でわずか２５３枚しか利用されていないのである（先述のとおり、平成１３年度からの６年間で５０００万円近くの経費を要しているにもかかわらずである。）。

このように、莫大な費用を投下してまで住民票の「広域交付」制度など作る必要はないことは明らかである。まして、国民のプライバシーの権利に対する優越を認めるほどのメリットは全く存在しない。

イ　また、その他、転入・転出手続きの簡素化など、上告人らが住民の利便性として挙げるものは、被上告人らのプライバシーの権利を犠牲にしてまで実現しなければならないようなものでは全くないことが明らかである。

実際、被上告人らが居住する守口市においても、住基カードを利用した特例付記転出届の利用実績は、平成１５年～１８年度で０件、同じく転入届の方は９件のみである。これを利用率に換算すればそれぞれ０％、０．０４％になる。およそ住民の利便性の向上や負担の軽減に貢献した形跡は無きに等しいことが明らかである。

ウ　マスコミにおいても、「住基カードの交付枚数が…住民の利便の小ささを物語る。要するに住基カードなど持っていなくても何の支障もないのだ」（甲４０の毎日新聞）、「利点の乏しさもあるが、官側の発想だけで突き進んだ結果、国民にそっぽを向かれている状態である」（甲４０の北海道新聞）等々と指摘されているところである。

エ　以上から明らかなとおり、そもそも住基ネットにより住民の利便性が増進されるということ自体、過大に主張されてきているのである。

オ　なお、仮に住基ネットには一定の「利便性」であるとか「効率性」は認められるとしても、それが何ものにも優越するものでは決してない。

特に本件のようにプライバシー権という重要な権利・利益が犠牲とされるような場合には、住民一人一人において、「プライバシー」とこれを犠牲にして得られる「利便性」とのどちらを選ぶか、自らにおいての決定が許されるべきだからである。

そうすると、被上告人らは、「住民票の広域交付」等という「利便性」よりも、自らのプライバシーの権利の保持を望むのであるから、このような被上告人らに対しても、住基ネットにより「住民の利便性」が認められるから住基ネットの導入は必要であると短絡することは誤りである。

このような比較考量が問題になる場合には、得られる利益とそれによって失われるものがどんなものであるかということを真剣に検討することをしないで、ただ、「便利」とか「効率的」ということのみを追求し、そこに優越性を付与するなどという安易な姿勢は、必ずや人間社会を破壊に導いていくだろう。

「電子政府・電子自治体」構想、然りである。

さらに根本的には、安易に多数者の利益のためには少数者の正当な権利に基づく異議が制約されて良いとするのであれば、それは法治国家の否定にほかならないというべきである。

3　一部の住民の離脱による重大な支障は生じないこと

上告人らは、被上告人らが住基ネットから離脱することを求めていることに対して、仮に被上告人らの本人確認情報の提供等を差し止めた場合，住基ネットによる事務と従来の方式による事務とを併存させざるを得ないことになり、そのための負担を余儀なくされ、あるいは各団体間で“義務の衝突”が起きるなどとして、住基ネットを導入した所期の目的が達成できない、趣旨が没却される結果になるなどとする（上告理由書の３３頁等）。

しかしながら、このような主張もまた、以下において指摘するとおり、明ら

かに誤りである。

(1) そもそも事務の併存は不可避であり、予定されていたこと

上告人らは、あたかも住基ネット構築後は、従来方式による事務がすべてなくなり、住基ネットによる処理に一本化される形で効率化が進む予定であったかのように主張している。

しかしまずは、これ自体が全くのごまかしである。

すなわち、例えば住基ネットを利用した年金の「現況届」の廃止についても、常識的に考えれば当然であるが、全受給者が住基ネットにより処理されるものではない。受給者のうち、「外国籍(外国人登録)者」「外国に居住している者」はもちろんのこと、「加給年金額等が加算されている者」「障害の程度を確認する必要がある者」などの生死以外の事項についても確認する事項が存する者に対しては、今後も現況届を提出する必要があるとされているのである。

そもそも住基ネットに一本化して「効率化」することは、当初から予定されていなかったのである。

したがって、一部の住民が住基ネットに参加しないことにより、事務が併存したからといって、著しく効率化が阻害されるなどというのは不当に過度な主張である。

(2) 重大な支障の不存在

またいずれにしても、上告人らが主張する事務の併存等は、重大な支障と認められないことは明らかである。

すなわち被上告人らが、住基ネットから離脱をしても、当該市町村や他自治体、あるいは、国の機関等の行政事務に重大な支障――住基ネット全体の運用が成り立たないような重大な支障は存しないことは、現に原審までに明らかとなった以下の事実から明白だからである。

ア　まず、このことは、住基ネットに接続していない福島県矢祭町、東京都国立市、同杉並区等における実態をみてみるならば明らかである。

すなわちこれらの自治体は、住基ネットに接続をしていない。その結果、これらの住民の本人確認情報は、当該の都県や地方自治情報センターに通知、提供、保存等されていないし（ただし、仮運用の期間等一定の時期のものは通知等されている）、他市町村や国の機関・法人に住基ネットを通じて提供等されていない。しかるにこれらによって、全国ネットたる住基ネットの運用に不都合が生じていることは窺えない。

イ　また、前述の上原国立市長の証言（甲５８）などによれば、同市は、現に住基ネットを切断しているが、国立市内部においても、また他の市町村との関係などにおいて、支障が生じていることは窺えない。

ウ　さらに横浜市は、いわゆる「市民選択制」を採用し、住基ネットへの参加を拒否する者の本人確認情報等の提供を行っていなかったが（その数は８０万名を超える）、その当時、これによって住基ネットの運用に支障が生じていた事実は存しない。

実際、神奈川県の住民が、自分に対する住基ネットの運用の差止を求めた訴訟において、平成１７年１０月２７日、同市の担当職員であった花園勝氏の証人尋問が実施されたが、同氏は、横浜市内部、あるいは他の自治体との関係で支障が生じていない旨の証言を行い（甲６０）、横浜地裁判決も、「市民選択制」によって、横浜市の行政事務上、支障が生じたことはない旨判示している。

エ　なお、重大な支障ー被上告人らが住基ネットから離脱することにより、被上告人らのプライバシーの権利を犠牲にしてまで、なお必要とする制度としての住基ネットの運用に与える重大な支障ーについての検討は、未だになされていないものである（立証責任が、制度の必要性を主張する上告人らにあるということについては、前述のとおりである）。

(3) 単なる「効率化の阻害」はプライバシー権の制約根拠たり得ない

上告人らの主張は、前述のとおり、被上告人らの本人確認情報の提供等の差止めを認めると、新たな負担が生じることになり、効率化が阻害されると

いうものである。

しかし、そもそもにおいて、このような上告人らの主張は、「いったん制度を作ってしまったら、それに従え」というに等しく、その論理自体において著しく失当である。

すなわち、「行政事務の正確性及び効率性等を確保」することの必要性が、「本人確認情報を提供しない自由を認める」必要性に優越するものであるか否かを議論しているときに、アプリオリに、「行政事務の正確性及び効率性等を確保」の必要のためには、「本人確認情報を提供しない自由を認める」ことができない、と答えているものであって、問いでもって答えを出しているに等しく、非論理的な論法であるといわざるを得ない。

中島徹早稲田大学法務研究科教授が、平成１７年１１月２０日、横浜地裁における証人尋問で説いたように、「その制度に対して、合理的な疑いがある、あるいは疑問が差し挟まれた場合には、政府はそれを改善するということを当然の義務として負っているはず」である（甲３３、甲６１の26頁）。

また再三、再四述べてきたとおり、また前述の中島教授の口を借りるならば、「行政の効率というのは、個人の生活、日常生活の根幹にかかわるような事柄に関して、当然に優先するということはできない」のであり、「もし、行政効率だけでもってすべてを図るということになってしまいますと、人権保障というのは文字通り、危機に瀕するわけでして、むしろ、その人権保障にはある程度のコストが付随するのはやむをえない…もし、行政の効率化、経費の節約という観点から、人権保障をないがしろにすることができるというのであれば、何のための政府かということになるはず」である（甲６１の26頁）。

この点は、人権保障の府であり、その最後の砦でもある最高裁判所においてこそ、とくに留意されるべきである。

(4) 原判決の判示

なお、この点に関して、原判決は、次のように判示している。

控訴人らは、住基ネット全体の運用の停止を求めているのではなく、住基ネットからの離脱を求めているにすぎないところ、住基ネットは全住民を対象として構想、構築されていることから、一部の者の離脱を認める場合には、住基ネットの目的の完全な達成が阻害されることになり、また、離脱者の把握のためのコストが必要となることになるということはいえるが（もっとも、それらがどの程度のものであるかは明らかでない。）住基ネットの運用により、住民票コードをもって行政機関に保有されている多くの個人情報がデータマッチングや名寄せされて利用される具体的危険がある（民間においてもそのような事態が生じる危険がある。）状態は、住基ネットを利用する住民の人格的自律を著しく脅かす危険をもたらしているものといえるのであり、個人の人格的自律の尊重の要請は、個人にとってだけでなく、社会全体にとっても重要なものであることも合わせ考慮すれば、控訴人らが住基ネットから離脱することにより生ずる上記障害等を回避する利益が、控訴人らの自己情報コントロール権により保護される人格的利益に優先するものとは考え難い。そうであれば、明示的に住基ネットの運用を拒否している控訴人らについて住基ネットを運用すること（改正法を適用すること）は、控訴人らに保障されているプライバシー権（自己情報コントロール権）を侵害するものであり、憲法１３条に違反するものといわざるを得ない。

まさしく正論であり、最高裁においても維持されるべき判断である。

４　まとめ

以上検討してきたとおり、上告人らが主張する、住基ネットの必要性、重要性の主張は、虚偽の事実を前提とするものであったり、あるいは、恣意的な数値を基にするものであるなど、到底、その必要性や重要性について納得させ得るものではない。少なくとも、住基ネットに接続させられることを拒否する国民に対しても一律にこれを適用しなければならない高度の必要性や重要性は全く窺えない。

すなわち、上告人らの住基ネットの必要性や重要性に関する主張を検討しても、住基ネットの運用によって、被上告人らのプライバシーの権利ないし利益

の侵害や、住民票コードという番号を付され、番号によって、その個人情報を名寄せされて、一元的に管理されうる状態におかれることによる自由権の侵害を受忍しなければならない事情は毫も窺えないものである。

また、住基ネットへの接続を拒否している被上告人らが住基ネットから離脱をしても、これによって住基ネット全体の運用に重大な支障が生じる事実も存在しない。

したがって、比較衡量上、被上告人らのプライバシーを犠牲にしてまで認めるべき（少なくとも、被上告人らの離脱を拒否してまで認めるべき）ほどの住基ネットの利益は存在しないことは明らかである。

なお、これは国民あるいは世論の多数意見である。

すなわち、平成１７年５月３０日の金沢地裁判決（甲３９）、翌３１日の名古屋地裁判決をめぐる新聞各紙の論説を改めて検討すれば明らかなとおり、ここに挙げた２４社のうち、２０社が金沢地裁判決に賛意を表した（甲４０）。

そして、その理由として「事務能率向上、住民の便益向上など政府が主張するメリットは抽象的で、現実にある不安を上回るほど具体的な公益性があるとは思えない」（東京新聞）、「住基ネットが行政事務の効率化を優先させるあまり、住民のプライバシーを軽視する結果になってよいわけはない」（佐賀新聞）等が挙げられているのである。

まさにその通りであり、とりわけ憲法をはじめとする法の理念に忠実である限り、抽象的かつ曖昧な住基ネットの利便性・効率化が、被上告人らの基本的人権たるプライバシー権・自己情報コントロール権に優越させられるべき理由は何ら存しないのである。

原判決の判断はこの点でも正当であり、上告審においても維持されるべきである。

以上より、本件上告は、すみやかに棄却されるべきである。

以上