

平成18年6月9日判決言渡
 平成18年6月9日原本交付
 裁判所書記官

平成15年(ワ)第1984号, 第2594号, 平成16年(ワ)第1175号各住民
 基本台帳ネットワーク差止等請求事件 (口頭弁論終結日: 平成18年3月17日)

判 決

原告ら及び原告ら訴訟代理人(弁護士)の表示は別表1のとおりであり, 被告ら
 及び被告ら訴訟代理人の表示は別表2のとおりである。

主 文

- 1 原告らの請求をいずれも棄却する。
- 2 訴訟費用は原告らの負担とする。

略 語 の 説 明

本判決においては, 次の左欄の略語は, その右欄を指す。

A原告ら	別表1 A欄記載の原告ら (他の原告らも同様にいう。)
被告財団	被告財団法人地方自治情報センター
被告市町	被告財団及び被告兵庫県を除く被告ら14市町
神戸市長ら	被告市町の首長ら
法	住民基本台帳法
知事	都道府県知事
市町村(長)	特別区(長)を含む市町村(長)
本人確認情報	氏名・出生の年月日・男女の別・住所・住民票コード及びこ れらの変更情報
住基ネット	法30条の2以下が定める, 電気通信回線を通じて本人確認 情報を通信する住民基本台帳ネットワークシステム
住基ネット事務	法30条の10第1項記載の本人確認情報処理事務
磁気ディスク	磁気ディスク又はこれに準ずる方法により一定の事項を确实

	に記録しておくことができるもの
ファイアウォール	電気通信回線経由の不正侵入を防止するコンピュータ
指定機関	法30条の10第1項所定の指定情報処理機関
CS	既存の住民基本台帳システムと住基ネットを接続するため各市町村に設置されたコミュニケーションサーバ
委任知事	指定期間に住基ネット事務を委任した都道府県知事
住基カード	法30条の44所定の住民基本台帳カード(その者に係る住民票に記載された氏名及び住民票コードその他政令で定める事項が記録されたカード)
個人情報保護法	行政機関の保有する個人情報の保護に関する法律

事 実 及 び 理 由

第1 請求の趣旨

1 被告市町に対する請求

(1) 情報提供の差止請求

被告神戸市はA原告らの、被告川西市はB原告らの、被告宝塚市はC原告らの、被告伊丹市はD原告らの、被告西宮市はE原告らの、被告尼崎市はF原告らの、被告猪名川町はG原告らの、被告芦屋市はH原告らの、被告小野市は原告[]の、被告姫路市はJ原告らの、被告加古川市はK原告らの、被告高砂市はL原告らの、被告明石市は原告[]の、被告篠山市は原告[]の各本人確認情報を、被告兵庫県に通知してはならない。

(2) 住民票コード削除請求

被告神戸市はA原告らの、被告川西市はB原告らの、被告宝塚市はC原告らの、被告伊丹市はD原告らの、被告西宮市はE原告らの、被告尼崎市はF原告らの、被告猪名川町はG原告らの、被告芦屋市はH原告らの、被告小野市は原告[]の、被告姫路市はJ原告らの、被告加古川市はK原告らの、被告高砂市はL原告らの、被告明石市は原告[]の、被告篠山市

は原告 [REDACTED] の各住民票コードを、住民基本台帳から削除せよ。

2 被告兵庫県に対する請求

(1) 情報提供の差止請求

被告兵庫県は、法第30条の7第3項の別表第一の上欄に記載する国の機関及び法人に対し、原告らの本人確認情報を提供してはならず、かつ、被告兵庫県は、被告財団に対し、原告らに関する住基ネット事務を委任してはならない。

(2) 記録削除請求

被告兵庫県は、その保存する住基ネット磁気ディスクから原告らの本人確認情報を削除せよ。

3 被告財団に対する請求

(1) 事務の差止請求

被告財団は、被告兵庫県から受任した原告らに関する住基ネット事務を行ってはならない。

(2) 記録削除請求

被告財団は、その保存する住基ネットの磁気ディスクから原告らの本人確認情報を削除せよ。

第2 事案の要旨

原告らは、法30条の2に基づき自己の住民票に住民票コードが記載されることによって、あるいは、住基ネットが稼働することによって、現に、人格権（自己情報コントロール権又は公権力から監視されない権利）が侵害されていると主張し、人格権に基づく妨害排除請求（侵害状態の除去請求）として、居住地の被告市町に対し住民票コードを削除すること、被告兵庫県及び被告財団に対し住基ネットの磁気ディスクから自己の本人確認情報を削除することを求めるとともに、人格権に基づく妨害予防請求（侵害をしてはならない不作為義務の履行請求）として、被告らに対し、住基ネットを使用しての本人確認情報

の送受信の差止めを求めるものである。

第3 争いのない前提事実

平成11年8月18日に公布された平成11年法律第133号によって法が改正され、次のとおり、住基ネットに関する規定が置かれ、住基ネットが稼働し始めた。

- 1 知事は、当該都道府県内の市町村長が住民票に記載することのできる住民票コード（法7条13号）を指定し、市町村長に通知する（法30条の7第1項）。

市町村長は、新たにその市町村の住民基本台帳に記録されるべき者につき、その者が住民基本台帳に記録されたことがない者であるときは、その者に係る住民票に知事から指定された住民票コードのうちから選択するいずれか1つの住民票コードを記載するものとする（法30条の2第2項前段）。

知事は、住民票コードの指定及びその通知を指定機関に行わせることができる（法30条の10第1項1号）。

知事及び指定機関は、本人確認情報を磁気ディスクに記録し、一定期間保存しなければならない（法30条の5第3項、30条の11第3項）。

- 2 市町村長は、知事に本人確認情報を通知するものとする（法30条の5）。
- 3 知事は、法の定める場合に、法所定の国の機関、法人、当該都道府県内の市町村長その他の執行機関、他の都道府県内の知事、市町村長その他の執行機関に対し、保存中の（「保存期間が経過していない」の意味である。以下も同じ。）本人確認情報を提供する（法30条の7第2ないし6項）。
- 4 知事は、法の定める場合に、保存中の本人確認情報を利用することができ、また、条例で定めることにより、他の都道府県の知事その他の執行機関から求めがあったときに、保存中の本人確認情報を提供するものとする（法30条の8）

5 知事は、指定機関に対し、法の定める国の機関・法人への本人確認情報の提供等の本人確認情報処理事務を行わせることができ（法30条の10第1項）、委任知事は、本人確認情報を指定機関に通知する（法30条の11第1項）。

被告財団は、地方公共団体におけるコンピュータの利用促進のため昭和45年5月に設立された財団法人で、平成11年11月1日、当時の自治大臣から、指定機関に指定され、知事の委任を受けて住基ネット事務を行っている。

6 本人確認情報の通知及び提供は、原則として相互の電子計算機の間を電気通信回線を通じて送信することにより行う（法30条の5第2項、30条の7第7項、30条の11第4項等）。

7 住民基本台帳に記録されている者は、その者が記録されている住民基本台帳を備える市町村の市町村長に対し、自己の住基カードの交付を求めることができる（法第30条の44第1項）。

8 被告市町は、従前から法7条に規定する事項を記載した住民票を編成し、住民基本台帳を作成していたが、平成11年法律第133号による法の改正後、被告財団から指定され通知された住民票コードを住民票に記載し、原告らに関する個人情報が記録された既存のサーバを住基ネット専用のCSに接続し、CSを都道府県のサーバにつながる電気通信回線に接続した。こうして、被告市町は、兵庫県知事に原告らの本人確認情報を通知している。

9 被告兵庫県は、自己のサーバをCSにつながる電気通信回線に接続し、被告市町から通知された原告らの本人確認情報を自己のサーバの磁気ディスクに記録して保存するとともに、被告財団に対し、本人確認情報を通知した。

被告財団は、被告兵庫県経由で電気通信回線を通じて被告市町から本人確認情報の通知を受け、その情報を磁気ディスクに記録し保存している（法30条の11第1項、3項）。そして、被告財団は、法の定める場合に、法所

定の国の機関、法人等に対し、本人確認情報を提供している。

- 10 住基ネットは、平成14年8月5日から稼働し（第1次稼働）、神戸市長らは、同日以降、原告らに対し、その住民票に記載された住民票コードを通知した。また、平成15年8月25日以降、住基カードの交付が開始された（第2次稼働）。

第4 争点の摘示

- 1 本件請求は、現に、人格権である自己情報コントロール権又は公権力から監視されない権利が侵害されていることを原因とするものである。

したがって、まず、原告らが主張するように、本人確認情報の自己情報コントロール権が、具体的な権利義務発生の根拠となり得るのか、すなわち実体法上の権利として成り立つのかどうか、本件の第1の争点となる。

本人確認情報の自己情報コントロール権が実体法上の権利として成立していると判断された場合、その権利は、生命・身体に関する権利やプライバシーに関する権利などとともに人格権を構成することになるから、物権と同様、何人に対してもこれを主張することができ、何人も、原告らのそれら権利を侵害してはならない不作為義務を負う。

そして、原告らの同意を得ることなく、原告らの住民票に住民票コードを付した上で原告らの本人確認情報を住基ネットで管理し送受信することは、本人確認情報の自己情報コントロール権の侵害となることが明らかであるから、裁判所は、被告らに対し、不作為義務の履行、つまり、侵害状態の除去と将来の侵害行為の禁止を命ずることになる。

- 2 次に、自己情報コントロール権とは別に、公権力から監視されない権利が実体法上の権利として成り立つのかどうか、同意なしに住民票コードを付したり本人確認情報を住基ネットで送受信することがこの権利の侵害となるのかどうか、本件の第2の争点となる。

これらが肯定されれば、裁判所は、やはり、被告らに不作為義務の履行を命

ずることになるのであって、この権利に基づく請求の当否も、情報漏えいの危険の有無・程度と直接に関係しない。

3 以上のとおり、自己情報コントロール権や公権力から監視されない権利に基づく請求は、情報漏えいの危険の有無・程度と直接に関係しないのであるが、住基ネットにおける情報漏えい防止策が不十分で、情報漏えいの危険がある場合、その危険の程度によっては、原告らは、みだりに自己の個人情報に他人に知られない権利、すなわち、(通常の)プライバシーに関する権利を含む人格権の侵害を予防するため、住基ネットによる本人確認情報の管理及び送受信の禁止を求めることができるかと解される。そのような人格権的請求権の成否が、本件の第3の争点となる。

そのような人格権的請求権の成否の判断においては、公共の福祉の観点から人格権の外延がどのように画されるのかを検討する必要がある。したがって、争点3において、具体的に検討すべきは、情報漏えいの危険の有無・程度と住基ネットの必要性・有用性の2点である。

第5 争点1 (自己情報コントロール権) に関する当事者の主張

【原告らの主張】

1 憲法13条は、自分に関する個人情報をいつ、どのように、どの程度まで、他人に開示するのかわからないのかを自ら決定する権利を保障しており、国民は、自己に関する個人情報の収集、管理、利用、開示のすべてをコントロールする権利を有する。

したがって、行政機関による個人情報の取扱いが問題となる場面においては、情報主体である個々の国民の「コントロール」(同意・意思決定)が最大限に保障されなければならない。行政機関が同意なく国民のプライバシー情報を収集・取得し、保有・利用し、開示・提供することは、原則として違法である。例外として許容される場合があるとしても、それは、本人の同意を不要とする程のやむにやまれない利益を達成する必要がある場合でなければならない。

いし、あるいは厳格な合理性を有する正当な目的により行われなければならない。しかも、プライバシーに対し、より制限的でない態様でしか許されない。それゆえ行政機関が、国民のプライバシー情報をこのような要件を満たすことなく収集・取得し、保有・利用し、開示・提供すれば、国民のプライバシーの権利を侵害することになる。

ところで、今日のコンピュータによる情報処理技術の進展という状況下では、人格権の自由な発達は、自己の個人的情報の無制限な調査、蓄積、使用及び提供から各人を保護することが前提となり、個人情報に関する公権力の諸活動を憲法上の規律に服しめることが不可欠となっている。

このようにプライバシー権（自己情報コントロール権）は、現代社会における極めて重要な人権というべきであり、憲法13条によって新しい人権として保障されている。

- 2 本人確認情報は、対外的に周知されることが予定されていないものであり、いずれも個人の私生活上の事実に関する情報である（私事性）。また、本人確認情報は、社会の一般の人々にまだ知られていない情報であるということができる（非公知性）。そして、本人確認情報は、今日、個人情報売買の対象とされ、情報の開示を許容していない者にまで提供され、これらの者からの電話、郵便などにより、私生活の平穩が害される危険性が增大しているから、社会通念上、自己が欲しない他者には開示されたくないと考えるものに当たる。したがって、本人確認情報は、社会一般の人の感受性を基準として、当該個人の立場に立った場合、みだりに開示されることを欲しないであろう情報であると言える（非公開性）。また、各情報を検索できる住民票コードについては、当該私人の立場に立った場合、みだりに公開を欲しないのは明らかであり、本人確認情報について、みだりに他者に開示されない利益は、プライバシーの権利として保護されるものである。これは、最高裁第二小法廷平成15年9月12日判決が、「学籍番号、氏名、住所及び電話番号」について、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した判断がそのまま当てはまる。

- 3 また、氏名の変更履歴（ここでは、氏名がAからBに変わったという結果だけの情報を指すものとする）は、それだけでもその本人に婚姻や離婚、養子縁組や離縁等の可能性あるいは他の何らかの理由による改姓改名の可能性があったことを意味することになるから、その秘匿性は極めて高く、まさに個人の人格的自律に直接関わるプライバシーの中核に位置する「固有情報」にほかならないし、住所の変更履歴についても、それが記録され追跡可能にすることは、憲法22条が保障する居住・移転の自由に照らしても疑義のあるところである。

そして、男女の別の変更履歴についても、それが性同一性障害を理由とする男女の別の変更を意味する可能性があることを考慮すると、まさに「プライバシー固有情報」にほかならない。さらに、生年月日の変更履歴についても、何らかの理由による変更という事情を推測させるものであり、まさしく「固有情報」というほかない。

以上要するに、上記の各情報の変更履歴というものは、それがあるということとそれ自体で、その個人に何らかの私的な出来事（事情）が発生したことを意味するのであり、それはまさしく他者には秘匿しておきたい情報というべきであり、典型的な「プライバシー固有情報」に該当するのである。

- 4 住基ネットは、すべての国民に一方向的に11桁の住民票コードを付し、そのコードとともに氏名、生年月日、男女の別、住所及びそれらの情報の変更履歴が、本人の与り知らないままに、市区町村と都道府県・地方自治情報センターの間で専用回線をもって構築された住基ネットを流通し、本人確認情報として提供され、利用されるものである。そして、被告財団から国へ提供され、国が利用する事務は、275事務に及ぶ。この間、本人の同意を得られることはなく、本人に選択の余地は全く与えられていない。

住基ネット上の本人確認情報は、住民票コードという「共通番号」の付され

たデジタル化された情報であり、その伝播力は、紙に書かれた情報に関する上記最高裁判決の事案の比ではなく、住基ネットによるプライバシーの侵害の危険性は計り知れないものがある。まさに、住基ネットは、今日のコンピュータ社会・管理社会における新たな形態によるプライバシー権の侵害の危険性を有する。この点からも、当該個人の同意を得ない個人情報の提供・利用はより厳しく制限されるべきである。

したがって、原告らの同意も関与もなしにその個人情報を住基ネットにより管理し送受信することにした法の規定は、憲法13条に違反するものであり、住基ネットの構築及び稼働は、自己情報コントロール権を侵害する違憲・違法なものというべきである。

【被告らの主張】

- 1 原告らは、憲法13条によりプライバシー権が保障されており、その一態様として、自己情報コントロール権が保障されていると主張する。

しかし、プライバシーは、法的に保護に値する人格的利益であるものの、多義的で、外延が極めて不明確なものであるから、それ自体を一個の統一的な憲法上の権利とまでいうことはできない。

それに、プライバシーの法的保護の内容は、みだりに私生活へ侵入されたり、他人に知られたくない事実又は情報を公開されたりしない利益として把握されるべきであり、原告らが主張するように、プライバシーに属する情報をコントロールすることを内容とするものとは認められない。

- 2 また、プライバシーについては、その権利の性質上、その概念自体が不明確で、いまだ統一的な理解が得られていないことからすれば、仮に、プライバシーに権利性を認めたとしても、これを排他性を有する人格権であるにとらえ、差止請求を認めることはできない。

第6 争点2（公権力から監視されない権利）に関する当事者の主張

【原告らの主張】

- 1 憲法は、国民主権・平和主義・基本的人権の尊重を保障し、福祉国家を目指しており、国家が国民を監視する警察国家は許されない。そして憲法13条は、各個人が有する「尊厳ある地位」に最大価値を認めているから、各個人がその人格の発展を目的として行う諸活動は、公権力の監視・干渉から自由でなければならず、公権力が意に反して個人の諸活動に関する情報を収集することは原則的に禁止されるべきである。
- 2 住基ネットに流れる情報は、将来的には、病院の診療や図書館の利用等にまで利用される予定であり、そうなる個人についての莫大な情報が住基ネット上を流れ、行政機関に集積・保有されることになる。かかる状況下では、個人は、公権力に自己の個人情報に掌握されていることになり、自己の思想的傾向、行動傾向等が公権力に掌握されることになり、このことはとりもなおさず、各個人が公権力から監視されることを意味する。
- 3 ~~したがって、住基ネットを通じて個人情報~~が行政機関に保有・蓄積されない利益は、公権力から監視されない権利（憲法第13条）として保護されるものである。
- 4 さらに、国民には「公権力から包括的に管理されない権利」があると考えられる。これは、憲法13条の幸福追求権に基づくものである。公権力からの管理があるところに、個人的人格的自立や幸福追求はありえないからである。

また、今日、憲法が想定している福祉国家は、専ら国民・市民のための福祉に資する国家・公権力の存在であり、国民・市民を管理の対象としていないことは言うまでもない。憲法の想定する福祉国家観からしても、いわば当然に認められるものである。

- 5 改正法の住民票コードによる付番は、公権力から管理されない自由を侵害する。

住民票コードは、当初から様々な行政分野に共通に使用される共通番号として構想されており、本質的に個人情報の多目的利用が予定されている制度であ

るし、ある特定の個人(国民)に対して官庁・公権力が必要に応じてあらゆる分野の個人情報を番号によって名寄せすることができることになる。すなわち、ある特定の個人(国民)がどのような状態下にあるかを様々な行政分野が把握している情報を通じてすべて知ることができるのである。そのため、国・公権力は、いつでも個人の全体像を形成し、特定の個人を全体的に評価することができる。ここで重要なのは、現実には、国・公権力がそのようなことをしているかどうかではない。国・公権力がしようと思えば、いつでもそういうことはできるということが問題なのである。

このように国民の個人情報を一元的に管理することができ、また、利用することができるということは、取りも直さず、公権力から包括的に管理されない自由を侵害することになる。つまり、いわゆる国民総背番号制(国民全(すべて)てに使用目的を限定せずに個人コードを付けること)に通じる途が開かれたということが、上記自由を侵害するものとして辞さないのである。

【被告らの主張】

- 1 公権力から監視されない権利、あるいは公権力から包括的に管理されない権利は、プライバシー権が憲法13条により統一的な憲法上の権利として保障されているとはいえない上、その権利の内容、根拠、外延などいずれをとっても不明確であり、これが憲法上保障されるとはいえない。
- 2 仮に、上記権利が憲法上保障されるとしても、住民票コードは、住基ネットを構築するに当たり、行政において確実な本人確認をし、迅速かつ効率的な検索を実現するために住民票に記載することとされたものであり、原告らが主張するような行政機関が個人情報を一元的に管理するために記載したものであるのではない。

また、住基ネットで保有される情報は、本人確認情報のみであり、いろいろな広範な情報を集中して管理するものではない。

それに、個人情報を一元的に収集、管理することは、法律上認められてい

ない（法30条の34，30条の42，30条の43）。

したがって，原告らの主張は失当である。

第7 争点3に関する当事者の主張

【原告らの主張】

1 住基ネットにおける情報漏えいの危険

(1) コンピュータ通信網全体の安全性（以下，本判決において，通信網やCSの安全性という場合の「安全性」とは，情報取得権限のない者が磁気ディスクに記録された情報を取得することができないようにされていることを意味する。）は，通信網につながるすべてのコンピュータの安全性が技術面においても運用面においても確保されていなければ，結局，十分に確保されているとは言えず，全国約3000の各市町村に置かれているすべてのCSを含めて十分なセキュリティが確保されなければならない。CSの安全性が不十分な市町村が一つでもあれば，当該市町村の住民の個人情報のみならず，すべての国民の個人情報が流出することになるのであるから，住基ネット稼働下では個人情報流出の危険は飛躍的に高まった。

(2) 長野県本人確認情報保護審議会の調査結果をみても，担当職員がCSの安全性の不十分さを感じていることが明らかになっている。また，長野県が行った住基ネットの侵入実験の結果，通信網に幾つかの脆弱性が発見され，住基ネットの安全性の程度は平均以下で，平均的なコンピュータエンジニアなら誰でも侵入し，情報を盗んだり損害を与えることができることが実証された。すなわち，CSセグメントへ直接接続したり，市町村の既存の住民基本台帳システムを踏み台にすることなど様々な方法により，CSの管理者権限を取得することが具体的に可能な状況にある。そして，管理者権限を奪取すると，遠く離れたところでも自由に操作できることになるから，本人確認の不正閲覧や他の市町村の住民票の写しの広域交付が不正に行われる危険性があり得，直ちに，原告らを含んだ全国民のプライバシー権が侵害されるので

ある。

(3) また、通信網やCSの安全性にとって最も脅威なのは人間そのものである。すなわち、「人間の心のすき間、弱い部分を利用して情報を奪取する」という方法での住基ネットへの侵入行為も、セキュリティに対する大きな脅威であり、末端の職員まで統一した考え方で十分な教育を受けていなければ、情報が持ち出されてしまう可能性がある。そして、全国の多数の自治体において、セキュリティが職員の信頼関係のみに支えられており、各職員の信頼関係が悪用され情報が持ち出される危険性は高く、また、それを防ぎうる十分な体制は全く整っていない。

(4) 大阪地裁において平成17年6月16日に行われた自治体職員の証人尋問の結果をみても、各自治体が、総務省が指導する技術水準を満たしておらず、住基ネットの管理の不十分さが明らかになった。

例えば、八尾市、吹田市及び柏原市では、CSが設置されている重要機能室への入退室の管理がずさんであり、八尾市、木津町及び加茂町では、端末機の操作者が正当なアクセス権限を有していることを確認するために必要なアクセスログのチェックが適切に行われていないことが判明した。また、吹田市は、CSの整備、保守及び点検を委託した業者が無断で再委託していたし、加茂町では、委託した業者に作業を任せ、その内容について詳細な確認をしていないことが判明した。

(5) 被告市町の状況

被告兵庫県は、区域内の市町村におけるCSの管理体制、安全性を点検するため、「本人確認情報提供に当たってのセキュリティ体制チェックリスト」（システム管理主管課用と税務課・用地課用とがある。以下、システム管理主管課用のものを「兵庫県チェックリスト」という。）を各市町村に配布し、その回答を得たが、その回答をみると、被告市町の管理体制には重大な欠陥があることが明らかになった。

すなわち、被告は、総務省が行った「住民基本台帳ネットワークシステム及びそれに接続している既設通信網に関する調査票」（以下「総務省チェックリスト」という。）を活用して各市町村における管理体制の徹底を図っており、特に重要な重点7項目については、すべての市町村において3点満点を達成したから、管理体制は万全であると主張するが、兵庫県チェックリストには、重点7項目と重複する項目があり、その項目につき、被告姫路市、同加古川市、同猪名川町、同芦屋市、同伊丹市及び同宝塚市がクリアしていないとの回答をしている。したがって、被告市町は、国が定めた「電気通信回線を通じた送信又は磁気ディスクの送付並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準」（以下「安全基準」という。）を満たしておらず、重点7項目すらクリアしていない市町が多くあるという深刻な事態が明らかとなった。

被告伊丹市についてみると、①重要機能室の鍵又は入退室のカードの管理責任者を定めていない、②CSが存在するLANの通信網機器の物理的配線状況を管理していない、③通信網機器の保守内容及び点検項目を明確にしていない、④重要機器に対する保守を行う場合に職員が立ち会っていない、⑤データのバックアップの実施記録簿を保管していない、⑥自己チェックリストによる点検を定期的に行っていない、⑦委託業者の管理も極めて不十分であり、庁内LANの管理が極めてずさんである、等の多数の問題があり、信じがたい管理状況にある。このように、被告市町の管理体制が不十分なことは明らかで、住基ネットの安全性が危機的な状況にある。

2 住基ネットの必要性について

(1) 総務省は、これまで、住基ネットは「国家による国民の管理」という趣旨のものではない、ということを強調するために、住基ネットの存在意義についての次の点を指摘してきた。

① 国の行政機関等に何らかの申請・届出(例えば資格取得手続や許認可手続

等)をするときに住民票の写しの添付が不要であること。

② 住基カードを持っている人は、全国どこの市町村からでも自分の住民票の写しの交付が受けられること。

③ 住基カードを持っている人については、市町村を越えた転居の際に、転出市町村役場に行く必要がなく、転入市町村役場に1回行けばすむこと。

(2) しかしながら、これらが市民にとってのメリットなどとは到底いえない。

まず、上記①については、そもそも一般市民が国の行政機関等へ申請・届出をする場面はほとんどない。一般市民が住民票を必要とするパスポートの取得や運転免許証の取得の際、通常は同時に戸籍謄抄本も必要とされるから、いずれにしても市民は市町村役場に行かなくてはならない。

次に、上記②については、そもそも一般市民にとって住民票を必要とする場合自体ほとんどないのに、居住する市町村以外のところで交付を受けることができる、ということを利用と受け止められることなどほとんど考えられない。住居地以外の市町村で住民票の交付が受けられるにしても、少なくとも市町村役場には出向かなければならない。上記②の言い分もほとんど現実的ではない。

上記③についても、一般市民が市町村を越えて転居することは、一生で数回あるかないか、という程度であって、その際に転出元・転入先の各市町村役場に出向くことを不便と感じている市民はほとんどいない。それに、現在でも転出届は郵送で可能で転出元の市町村役場に出向く必要はないし、転出証明書が必要な場合も郵送によることが可能である。

(3) 以上のとおり、住基ネットは、総務省がいうような、国民にとっての必要性や有用性が認められるものではない。

【被告らの主張】

1 住基ネットにおける情報漏えいの危険

(1) 住基ネットは、以下のとおり、様々な措置を適切に講ずることによっ

て、安全性が確保されており、本人確認情報の漏えいの危険性はない。したがって、仮に、住基ネットに原告らのプライバシー侵害の危険性があるとしても、それは極めて抽象的なおそれにとどまる。

(2) 制度面からの対策

- ① 法30条の5第1項は、都道府県、指定機関が保有する情報は、法律上、本人確認情報に限定している。
- ② 法30条の6、30条の7第3項ないし第6項、30条の8は、本人確認情報の提供を受ける行政機関の範囲や利用目的を限定しているし、法30条の34は、本人確認情報の提供を受ける者に対し、目的外の利用又は提供を禁止しており、法30条の30は、知事及び指定機関に対し、法律の規定によらない本人確認情報の利用及び提供を禁止している。
- ③ 市町村はCSの管理責任を負い、都道府県は都道府県サーバ（都道府県の住民の本人確認情報を保存）と都道府県通信網の管理責任を負い、指定機関は全国サーバ（全住民の本人確認情報を保存）と全国通信網の管理責任を負い、それぞれ安全性を確保する責任を負っている。また、総務省は、指定機関への監督命令等（法30条の22第1項）、地方公共団体への指導、助言、勧告等（法31条）、本人確認情報処理規程の認可（法30条の18）、安全基準の策定等の権限を有し、委任知事は、指定機関に対する指示（法30条の22第2項）、指定機関は、委任知事に対する技術的助言等（法30条の11第7項）の権限を有し、これらの権限により、安全性の確保を担保している。

そして、指定機関が、国の機関等に本人確認情報の提供を行う際には、協定書を取り交わすこととして国の機関等の責任を明確にし、委任知事は、指定機関に対し、報告要求等を行うことができ、都道府県及び指定機関には、本人確認情報保護のための諮問機関が設置されるなど、

個人情報の保護を図る制度が確保されている（法30条の23第2項、30条の9及び30条の15）。

- ④ 住民票コードは、無作為の番号で、住民の申請によりいつでも変更できるとし（法30条の3）、さらに、民間部門が住民票コードを利用することを禁止し、行政機関が利用する場合も目的外利用を禁止するなどし、住民票コードの利用を厳しく制限する措置を講じている（法30条の34、42ないし44）。そして、⑤ 都道府県、市町村及び指定機関は緊急時対応計画を定め、本人確認情報の漏えい等の危険が具体的に発生した場合には、相互に連絡調整を行い、被害拡大を防止するための措置等を講ずることとされている（安全基準第2-5）。

(3) 物理的な侵入防止対策

安全基準においては、建物等への侵入の防止、重要機能室の配置及び構造、入退室管理、磁気ディスク、構成機器及び関連設備、データ・プログラム・ドキュメント等の管理等、外部からの侵入に対する物理的なセキュリティ対策を関係機関に義務付けている。

特に、市町村における住基ネット及びこれに接続している既設通信網における対策については、総務省チェックリストに基づく自己点検と、これに基づく都道府県、指定機関及び総務省による指導、助言を実施し、対策の強化、徹底を図っている。

なお、安全基準及び総務省チェックリストは、高いレベルの安全性を実現することを目的としており、これを遵守しなければ、本人確認情報の漏えい、改ざん等の具体的危険が生じないという基準を設定したものではない。仮に安全基準の一部が達成されていなくても、また総務省チェックリストで最高点に満たない項目があったとしても、そのことが直ちに、本人確認情報の漏えい、改ざんの具体的危険が存在するといえるものではない。

(4) 電気通信回線上の侵入防止対策

- ① CS、都道府県サーバ及び全国サーバの間の通信網は、すべて専用回線及び専用交換装置で構成された閉鎖的な通信網である。
- ② サーバ間で相互認証・暗号通信を実施しており、仮に、他のコンピュータを住基ネットに接続できたとしても、通信を行うことはできないし、盗聴による恒常的な暗号鍵の解読が極めて困難となる対策がとられている。
- ③ 住基ネットの通信プロトコル（コンピュータ限定の型式）には、インターネットで用いられる汎用的なプロトコルを使用せず、住基ネットに独自のものが用いられており、すべてのCSの通信網側、すべての都道府県サーバの通信網側と端末機側、全国サーバの全方向及び国の機関等サーバの通信網側にファイアウォールを設置して、インターネットで用いられるプロトコルの通過を遮断しており、CS、都道府県サーバ、全国サーバ及び国の機関等サーバに対し、住基ネットのアプリケーション以外の通信を使用してアクセスすることはできないようにされている。
- ④ 指定機関において、コンピュータウイルス、セキュリティホールが発生情報を入手し、ウイルス対策ソフトの新パターンファイルの配布や対応方法の通知を全団体に対して行い、徹底したコンピュータウイルス・セキュリティホール対策が実施されている。
- ⑤ 指定機関は、監視ファイアウォール等により、不正な通信がないか、24時間常時監視を行っている。
- ⑥ システム全体で統一ソフトウェアを導入することにより、住基ネット全体で均質かつ高度な安全性の確保が実現されている。

(5) 内部的な不正防止対策

- ① 法は、住基ネットに係る事務に従事する市町村、都道府県、指定機関及び本人確認情報の提供を受けた国の機関、地方公共団体の機関等の職

員や、本人確認情報の提供を受けた委託事業者に対し、秘密の保持義務やこれに違反した者に対する刑罰を科すなど（法30条の17第1項及び第2項、30条の31第1項及び第2項、30条の35第1ないし第3項、42条）、刑罰をもって不正を防止する対策を講じているほか、指定機関を適切な監督下に置いており（法30条の15、16、18、19、22、23、25）、担当者が個人情報を容易に検索できないよう、本人確認情報の照会条件を限定している。

- ② 住基ネットにアクセス権限のない職員がアクセスできないよう、操作者識別カード認証による制御を行うことになっている。
- ③ アクセスログを定期的にチェックし、不正アクセス等を発見して適切な措置を講ずることになっている。
- ④ 住民から請求があった場合、本人確認情報提供状況を開示することとなっており、住民が本人確認情報の提供状況を把握することが可能となっている。
- ⑤ 一定時間に一定数以上の住民票の写しの広域交付を停止する措置を講じるほか、担当職員に対し、住基ネットの安全性の確保等を目的とした教育・研修が実施されている。

(6) 外部監査等によるセキュリティの確保

指定機関と総務省は、市町村に対し、総務省チェックリストを活用して、指導、助言するなどしてセキュリティ対策の維持、向上を図り、外部監査法人による市町村のシステム運営監査を実施して管理体制の強化に活用した。また、住基ネットの主要な機器に対する模擬攻撃を実施して安全性の確認を行った。

(7) 住基カードの安全性の確保

住基カードについても、住民の申請により交付する（法30条の44第3項）、市町村の独自サービスの範囲は、市町村が条例で定める目的に限

定する（法30条の4第8項）など、様々な対策を講じることにより、安全性を確保している。

(8) 長野県が行った住基ネットの侵入実験

上記侵入実験は、①市町村設置ファイアウォールを回避して、重要機能室に物理的に侵入し、施錠を開けるなど通常の対策を幾重にも外した上、直接CSに攻撃端末をつなぎ、CSのOSの管理者権限を取得し、そのCSから得られたID、パスワードでCS端末の管理者権限を取得したことや、②庁舎内に入り、市町村の庁内LANにつないだ攻撃端末から、庁内LAN上にある既存住基システムの機器の脆弱性を検査し、これを攻撃することに成功したというものにすぎない。外部のインターネットから庁内LANへ侵入することや、庁内LANからCSセグメントへ侵入することにはことごとく失敗したのである。

実験結果から明らかになったのは、特殊な環境の下でCSのOSの管理者権限が取得できるということや、住基ネットに含まれない既存住基システムに対する攻撃がされたことに留まるのであって、住基ネットの危険性を示すものではない。また、住基ネットアプリケーションを起動させるには、操作者が識別カードをカードリーダーに挿入することなどが必要となるから、CS、CS端末のOSの管理者権限を取得したとしても、住基アプリケーションを起動させることすらできないのである。

上記侵入実験の結果は、住基ネットの危険性を実証するものではなく、かえって、その安全性が確認された。すなわち、①実験市町村以外の住民の個人情報に不正にアクセスされたり、インターネットから庁内LANへ侵入されることや、庁内LANからファイアウォール越しにCSへ侵入される具体的危険性が実証されず、むしろ安全性が確認され、②CSのOS管理者権限やCS端末のOS管理者権限の取得は、通常の状態ではむしろ安全であることが確認され、③庁内LANからファイアウォール越しにC

SのOS管理者権限を取得することが不可能であること、④住基ネット本体に対する監視が適正に実施されていること、⑤既存の住民基本台帳システムの改ざんが直ちにCSに反映されるものではないこと及び既存の住民基本台帳システムは住基ネットと峻別してとらえるべきこと、⑥庁舎外から庁内LANへ侵入される具体的危険性は実験で実証されておらず、むしろ安全性が確認され、実験市町村における庁内LANの脆弱性は限定的であり、一般論としても市町村における対策が徹底されていること、が明らかになったのである。

2 住基ネットの必要性・有用性について

(1) 住基ネットは、以下のとおり、複数の多角的な行政目的を有しており、我が国の国家戦略である電子政府・電子自治体の実現のために不可欠な基盤をなすものとして是非とも必要なものである。

(2) 行政機関への申請や届出の際に住民票の写しの提出が不要となること

住基ネットの稼働により、行政機関への各種申請の際、年間2500万件以上の住民票の写しの提出が不要になることが見込まれている（平成16年度の省略枚数は年間300万件以上であった。）。このことは、住民票の写しの交付手数料（200から300円）の負担や市町村窓口まで行く手間が省けるという「住民の便益」に資するだけでなく、住民票の写しの交付を行うために配置している市町村の多数の職員を、福祉等他の行政分野に配置することが可能になり、「行政事務の効率化」にも資する。

(3) 年金の大半の現況届が不要となること

住基ネットの稼働により、平成15年度には、共済年金（地方公務員、国家公務員、私立学校教職員）や戦没者遺族等援護年金等を対象とし、今後は、国民年金、厚生年金をも対象として、年金受給者の現況届を不要とする取扱いが予定されている（平成16年度の省略枚数は約500万件であった。）。

このことは、年金受給者が、現況届を年金支給機関へ郵送する手間や切手代の負担が不要になるという「住民の便益」に資するだけでなく、年金支給機関が現況届を年金受給者に郵送するための経費が不要になるほか、年金の過誤払を防止することが可能になり、「行政事務の効率化」にも資するものである。

(4) 市町村間での転入通知等のオンライン化が可能となること

住基ネットの稼働により、住民票の写しが住所地以外で取得できるほか、従来郵送により行われていた転入地市町村から転出地市町村への通知（年間約440万件）について、オンラインにより行うことが可能となっている。

(5) 住基カードの利用による利便性が向上すること

住基カードについては、必ずしも全国的に普及が進んでいるとはいえないが、住基ネットと住基カードの利用により、住民サービスの向上と確実・簡便な本人確認が可能となる。

(6) 公的個人認証サービスが実施可能になること

住基ネットから情報提供を行うことにより、公的個人認証サービスが可能になり、行政手続をインターネットで行うことが可能になる。そうすると、住民は行政機関の窓口まで出かけていなくても、自宅でいつでも申請や届出ができることになるから、「住民の便益」に資することになるだけでなく、行政機関にとっても、申請や届出の処理を平均して行うことや業務システムとの連携を図ることにより、職員の配置をより適正に行うことが可能になり、「行政事務の効率化」にも資することになる。

第8 争点1、2に関する当裁判所の判断

1 自己情報コントロール権に基づく請求（争点1）について

(1) 原告らは、憲法13条が、プライバシー権としての自己情報コントロール権を保障していることを前提として、住基ネットにおける本人確認情報の管理及び送受信は、原告ら各人の自己情報コントロール権を侵害するものであ

り、許されないと主張する。

- (2) プライバシーに関する権利（プライバシー権）が人格的利益の一種として不法行為における保護法益となることは、今日では広く承認されており、他人の私生活に関する情報をみだりに暴くことは不法行為を構成する。

プライバシー権は、生命・身体に関する権利、名誉に関する権利などと同様に、いわゆる人格権の一種であると解されるから、その侵害に対する救済は、事後の損害賠償だけに限られると解すべきではなく、例えば、私生活に関する情報をみだりに開示するというプライバシーの侵害行為に対しては、その情報の性質、これを公表することの正当性、これが公表されることによって当該他人に生じるであろう不利益の重大性等を総合考慮し、人格権的請求権の行使により、その侵害行為の禁止（不作為義務の履行）を求める差止請求も許されると解される。

- (3) 個人が、プライバシー権の一内容として、他人（特に行政機関）が有する自己の個人情報コントロールする権利を有するのかという点については、もともとプライバシー権が実体法の根拠がなく、その外延が極めて不明確であることから、解釈によって確定することが極めて困難であるが、個人情報の訂正請求権を含む意味での自己情報コントロール権を一般的に否定することはできないように思われる（例えば、東京高等裁判所昭和63年3月24日判例時報1268号15頁参照）。法も、本人確認情報の過誤の訂正請求権を規定することにより、限られた範囲ではあるが、住基ネットにおける自己情報の訂正請求権を規定している（法30条の37、30条の40）。

しかしながら、住基ネットにおける本人確認情報の管理や送受信それ自体を制御するための自己情報コントロール権までを肯定する、つまり、当該個人の個別的な同意なしに、住基ネットでの本人確認情報の管理及び送受信が禁止されるとまで解するだけの根拠は乏しいというべきである。その理由は、次のとおりである。

(4) 本人確認情報は、氏名、生年月日、男女の別、住所、住民票コード及びそれらの変更情報である。もちろん、それらは、みだりに公表されてもかまわない私生活に関する情報ではないが、それ自体では、当該個人の思想信条あるいは社会生活の状況を推知させるような情報ではなく、個人を特定したりその同一性を識別するための情報であるから、本質的に、他人に知られることが嫌忌される情報ではないのである（なお、本人確認情報のうち変更情報とは「転入」「出生」「職権記載等」「転出」「死亡」「職権削除等」「転居」「職権修正等」「住民票コード記載の変更請求」という異動事由と異動年月日であり、離婚・離縁等の身分変動を示す情報を含まない。）。

なぜなら、氏名はもちろん、住所、生年月日、性別といった情報は、行政機関に何かを申請するといった場面のほか、社会生活上、様々な場面で、人物を特定しその同一性を識別するための情報として、かなり頻繁に他人に開示する必要があり、秘匿が常態となる情報とはいえない。

実際のところ、わが国においては、本人確認情報のうち氏名、生年月日、男女の別、住所については、長年にわたり、住民基本台帳に記載され、何人でもこれを閲覧することができるものとされ（法11条）、実際にも、行政上必要な調査活動、報道機関や学術機関が行う各種調査の際には、住民基本台帳に記載された個人の同一性確認情報が開示され、これが利用されていたが、このことが憲法や法律に違反する事態であると受け止められてはいなかったのである（現在では、住民基本台帳の記載を商業的に利用することさえも禁止していないことが問題として取り上げられてはいるが。）。

要するに、本人確認情報は、これまでは、その管理や開示に当たって当該個人の意思を反映させ、一定限度で個別的なコントロールを認めなければ、憲法13条に違反することになるような情報とは解されていなかったのである。

したがって、本人確認情報について、一般的・抽象的に自己情報コントロ

ール権が認められるとすることはできない。

- (5) もっとも、住基ネットは、電気通信回線を利用した通信網を使用して、電磁情報となった本人確認情報を全国的に送受信しようとする仕組みであるから、ここでの本人確認情報の送受信は、もしも情報漏えいに対する相応の防止策を講じるのでなければ、極めて簡単かつ短時間で本人確認情報を外部に漏えいさせる危険を伴う仕組みであるといえることができる。したがって、そのような危険がかなり大きいという場合には、住民基本台帳という紙に書いた個人情報の取扱いとは異なり、住基ネットにおける本人確認情報の管理及び送受信を行うについては当該個人の同意を必要と解する（その限度で個人情報の自己情報コントロール権を認める。）余地がないわけではない。

しかしながら、後記第9に認定説示のとおり、住基ネットにおける本人確認情報の管理及び送受信には、情報漏えいを防止するため、かなりの制度上の措置と技術的な対策がとられていると認められるから、住基ネットの稼働によって、それ以前の状況（住民基本台帳という紙に書かれた個人の同一性確認情報が一般に開示されていた状況）と比較して、みだりに本人確認情報が外部に流出する危険が顕在化しており、これに対する個人の自己情報コントロール権を認めなければならない事態が出現したとはいえない。

- (6) 以上のとおりであって、自己情報コントロール権に基づく原告らの請求は、その前提となる具体的な権利が認められないから理由がない。

2 公権力から監視されない権利に基づく請求（争点2）について

- (1) 原告らは、住基ネットが稼働し、住民票コードが国民一人一人に付されることにより、国民総背番号制となり、ある特定の個人につき、官庁・公権力が、もしそうしようと思えば、必要に応じてあらゆる分野の当該個人の情報を番号によって名寄せすることができる状態となったと主張し、このことによって、人格権の一内容である上記権利が侵害されていると主張する。

(2) 公権力がみだりに個人の私生活を監視することは、プライバシー権を侵害する違法な行為であり、その意味では国民は、公権力からみだりに監視されない人格的利益を有するが、そうだとしても、公権力の具体的な不作為義務発生の根拠として、国民一人一人に「公権力から監視されない権利」というものがあると解するための実体法上の根拠は乏しいし、憲法13条から直ちに、そのような私法上の具体的な権利が国民一人一人に認められると解することも困難である。

したがって、「公権力から監視されない権利」に基づく請求は、その前提となる具体的な権利が認められないから理由がない。

(3) また、住基ネットの利用制限、住基ネット事務に従事する公務員に対する懲戒処分、あるいは刑罰により、住基ネットにおける情報の不正使用・不正流出は抑制されているから、住民票コードの付番と住基ネットの稼働により、公権力が「必要に応じてあらゆる分野の当該個人の情報を番号によって名寄せすることができる状態となった。」という原告らの主張も誤りではないかと思われる。

すなわち、法は、後記第9の1にみるように、本人確認情報の利用を制限しているし、個人情報保護法により、行政機関は、特定の利用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され（同法3条2項）、行政機関の長は、利用目的以外の目的のために保有する個人情報を自ら利用し、又は提供してはならないとされ（同法8条1項）、行政機関が利用目的を超えて、本人確認情報を集約したり利用することは、法律上禁じられている。また、行政機関や指定機関の職員が法や個人情報保護法に違反する行為を敢行すれば、法、国家公務員法又は地方公務員法により、懲戒処分又は刑事罰が加えられる。それら刑事罰の内容は、決して軽微なものではない。

例えば、法30条の35第2項に規定する電子計算機処理等に関する事

務に従事する者が、その知り得た本人確認情報を漏えいした場合には、法42条により、2年以下の懲役又は100万円以下の罰金に処せられるのである。

また、住基ネットを使用して本人確認情報が提供される行政事務は275あるが（平成17年4月1日時点における集計である。）、それら住基ネット事務を処理する過程で取得した本人確認情報を一元的に管理する国家行政機関は存在しないのである。

(4) 原告らの主張は、結局のところ、懲戒処分や刑罰には何ら抑制力を期待することができず、法令によってどのような規制をしても、住基ネットを利用した違法な情報の集約や集約した情報の濫用的な利用を食い止めることはできないという認識に基づくものと考えられるのであるが、わが国の公権力は、終戦後長らく、法律による行政の原理の遵守を標榜し、（その不遵守が問題になる面が全くなかったと言い切れないものの）この原理に乗っ取った実務を積み重ねてきた実績があるというべきであり、現時点で、裁判所が、住基ネットの利用規制、守秘義務や刑罰による実効性がおよそ期待できないと断定することは相当ではない。

(5) 以上のとおりであって、「公権力から監視されない権利」に基づく請求は、原告ら主張の前提事実が認められないという意味でも理由がない。

第9 争点3に関する当裁判所の判断

1 住基ネットの個人情報保護のための規制について

法は、国民の個人情報がみだりに送受信されないよう、次のとおり、住基ネットにおける情報の管理及び送受信を規制している。

(1) 都道府県、指定機関が保有する情報は、本人確認情報に限定し（法30条の5第1項）、本人確認情報の提供を受ける行政機関の範囲や利用目的を法律で限定列挙している（法30条の6、30条の7第3ないし6項、30条の8、別表）。

- (2) 本人確認情報を保存する知事及び指定機関に対し、法律の規定によらない本人確認情報の利用及び提供を禁止し（法30条の30）、本人確認情報の提供を受ける受領者に対し、目的外の利用又は提供を禁止している（法30条の34）。
- (3) 住民票コードが行政事務以外の商業事務等に利用するのを防ぐため、住民の申請によりいつでも変更できるとし（法30条の3）、住民票コードの利用主体を、市町村長、知事、国の機関等に限定している（法30条の43）。そして、行政機関は、法令所定の事務の遂行のため必要のある場合以外に住民票コードの告知を求めることはできないとされている（法30条の42）。
- (4) 住基ネットを使用しての本人確認情報の管理及び送受信に従事する国、地方公共団体、指定機関の職員に対し、事務処理によって知り得た本人確認情報に関する秘密又は本人確認情報の電子計算機処理等に関する秘密の保持義務を課している（法30条の17第1項、30条の31第1項、30条の35第1項及び第2項）。また、市町村等の委託事業者についても、同様に、その事務に関して知り得た本人確認情報に関する秘密又は本人確認情報の電子計算機処理等に関する秘密の義務を課している（法30条の17第2項、30条の31第2項、30条の35第3項）そして、これらに違反した者に対し、刑罰を科している（法42条）。
- (5) 住民票記載事項の全部又は一部の修正を行った場合に、市町村長から本人確認情報の通知を受けた知事、指定機関、執行機関等に対し、本人確認情報の漏えい、滅失及び毀損の防止その他適正な管理のために必要な措置を講ずることとしている（法30条の29、30条の33）。
- (6) 総務大臣は、住基ネット事務の適正な実施を確保するため必要があると認めるときは、指定機関に対し、必要な命令をすることができ、委任知事は、指定機関に対し、必要な措置を講ずべきことを指示することができる

としている（法30条の22）。また、総務大臣は、指定機関が定める本人確認情報管理規程の認可権限を有する（法30条の22）。そして、国は、都道府県及び市町村に対し、都道府県は市町村に対し、必要な指導を行うものとし、主務大臣は知事又は市町村長に対し、知事は市町村長に対し、必要があると認めるときは、報告を求め、又は助言若しくは勧告をすることができるとしている（法31条1項、2項）。

また、総務大臣及び委任知事は、住基ネット事務の適正な実施を確保するため必要があると認めるときは、指定機関に対し、必要な報告を求め、事務所に立ち入り、帳簿、書類その他の物件を検査することができる（法30条の23第1項、2項）。

(7) 都道府県には、本人確認情報の保護に関する審議会を置くものとされ、この審議会は、本人確認情報の保護に関し知事に建議することができることとされ、指定機関には、本人確認情報保護委員会を置くものとされ、この委員会は、本人確認情報の保護に関し必要と認める意見を指定機関の代表者に述べることができるとされている（法30条の9、30条の15）。

(8) 何人も、知事又は指定機関に対し、磁気ディスクに記録されている自己の本人確認情報について、開示、訂正等を請求できるとしている（法30条の37、30条の40）。

2 住基ネットの電子計算機の接続状況と安全対策について

前記前提事実、乙第3号証の1ないし6、第13号証、第14号証、第16号証、第32号証、第35号証、第36号証及び弁論の全趣旨によれば、次の事実が認められる。

(1) 市町村は、既存の住民基本台帳システムと住基ネットを橋渡しをするため新たにCSを設置し、本人確認情報を電気通信回線による送信又は磁気ディスクによって、既存住基システムからCSに伝達し、CS内に本人確認情報を保存した。そして、CSから都道府県のサーバに、都道府県のサ

サーバから被告財団のサーバに、本人確認情報が送信され保存された。

(2) 総務省は、安全基準を作成し、関係機関に対し、以下のような安全性確保のための対策を義務づけている。

- ① CS、都道府県サーバ及び全国サーバ間の通信は、すべて専用回線及び専用交換装置で構成された通信網を介して行い、全国サーバと国の機関等サーバの間は、専用回線又は磁気媒体でデータ交換を行い、閉鎖的な通信網を構築する。
- ② 既存の住民基本台帳システムを含む市町村の役場内通信網（庁内LAN）がインターネットと接続されている場合、その間にファイアウォールを設置する。また、庁内LANとCSが接続されている場合には、その間にファイアウォールを設置し、CSと都道府県のサーバ、都道府県サーバと被告財団法人のサーバ、被告財団法人のサーバと国の機関のサーバの間には、それぞれ指定機関が監視するファイアウォールを設置する。
- ③ 通信時に公開鍵暗号方式により通信相手への接続を相互に認証する仕組みをとり、通信は独自の住基アプリケーションにより行い、インターネットで用いられる汎用的なプロトコルを使用しないこととする。
- ④ 指定機関において、コンピュータウイルスの発生情報を常時入手し定期的にウイルス対策ソフトの最新パターンファイルを全団体に配布し、OSのセキュリティホール発生情報を入手し、危険度が高いものは、システムの影響度を確認した上でセキュリティホール情報及び対応方法を通知する。また、通信網内に侵入検出装置（ISD）を設置し、運用管理規程に基づき、指定機関の通信網監視室から常時監視を行うほか、定期的にログの解析を行う。
- ⑤ CSが設置されている重要機能室の入退室の管理は厳重にする（重要機能室の所在を明らかにしないこと、電子計算機及び磁気ディスク等を

専用の部屋に設置すること、鍵又は入退室管理カード等により入退室者が正当な権限を有しているか確認することなど）。住基ネットの開発、変更、運用、保守等の委託を行う場合は、委託先事業者等の社会的信用と能力を確認すること、委託先事業者等に対し適切な監督を行い、再委託を制限し、再委託時には事前申請及び承認を行うものとする。

⑥ 本人確認情報は、CS、都道府県サーバ及び全国サーバ内に保存されており、端末機には存在しないが、端末機からサーバにアクセスする際には、常に操作者識別カードと端末機との間で相互認証を行って初めて住基アプリケーションが起動する設計とされ、操作者識別カードの種別により、システム操作者ごとに住基ネットが保有するデータ等へ接続できる範囲を限定し、操作者識別カードが挿入され住基アプリケーションが起動していない限り、端末機からサーバにアクセスすることはできない設計とする。

(3) 指定機関と総務省は、平成15年1月と2月、市町村におけるセキュリティ対策の徹底を図るため、協力してチェックリストを作成し、これを市町村に配布して安全性の状況を調査した。そして、総務省は、同年5月13日、都道府県において、市区町村に対して必要な技術的指導を行うことを要請し、特に重要なものとして下記の7項目（以下「重要7項目」といい、個々の項目を「重要項目①」などという。）を挙げ、そのすべてで3点満点を達成することを目標として、各都道府県、総務省及び指定機関において、技術的助言、指導を実施した。

そして、総務省は、平成15年8月8日付けで、被告市町を含むすべての市町村において、重要7項目について3点満点を達成したとの調査報告をまとめた（乙第14号証）。

記

① 重要機能室を設置できない場合、重要機器並びに磁気ディスク及びド

キュメントについて、盗難にあつたり、権限のないものが容易にアクセスすることができないように、適切な管理を行う。

- ② C.S 端末について、ウイルスの侵入の脅威を最小限にとどめるとともに、外部への情報発信ができないようにするため、インターネットに接続できないよう制限を行う。
- ③ C.S と既設通信網の間のファイアウォールを設置し、適切な運用管理を行う。
- ④ C.S と既設通信網の間のファイアウォールについて、適切な設定を行う。
- ⑤ 住基ネットと接続する既設通信網がインターネットに接続する場合には、当該通信網とインターネットとの間にファイアウォールを設置し、厳重な通信制御を行う。
- ⑥ メールサーバ及びWWWサーバ等の公開サーバについて、DMZ上の設置など適切な対策を講じる。
- ⑦ 公開サーバ等について、最新のパッチを当てる。

(4) 長野県の侵入実験について

甲第4号証の1ないし8、第5号証、第16号証、第19号証、第20号証、第21号証の1ないし4、第22号証の1ないし5、乙第27号証、第28号証、第29号証の1、2、第30号証の1、2及び弁論の全趣旨によれば、長野県が実施した住基ネットへの侵入実験について、次の事実が認められる。

- ① 平成15年9月22日から同年10月1日まで、波田町、阿智村、下諏訪町で第1次の実験が行われた。波田町では、都内からインターネット経由でインターネットと庁内LANとの間のファイアウォールを突破して庁内LANへの侵入を試みたが、成功しなかった。
- ② 阿智村及び下諏訪町における第1次実験では、インターネットと庁内

LANの間のファイアウォールを突破することを避け、庁舎内に入り、庁内LANにつないだ攻撃端末から庁内LAN上にある既存の住民基本台帳システムの機器の脆弱性を検査し、攻撃する実験を行った結果、既存の住民基本台帳システムの管理者権限を取得した。もっとも、庁内LANから市町村設置のファイアウォールを突破してCSに侵入しようと試みたが成功しなかった。

なお、仮に、既存の住民基本台帳システムに侵入して個人情報を書き換えたとしても、書き換えられたデータが直ちにCS内や都道府県サーバ、全国サーバに保存された本人確認情報に反映されることはない（乙第29号証の2、第30号証の2）。

- ③ 平成15年11月25日から同月28日まで、阿智村において第2次実験が行われた。そこでは、インターネットと庁内LANとの間のファイアウォール及び庁内LANとCSとの間のファイアウォールの突破を避け、CSが置かれている重要機能室に入室し、CSが入っているラックを解錠し、CSに直接攻撃端末をつなぎ、攻撃する実験を行い、CSサーバのOS管理者権限を取得することと、CSから得られたIDとパスワードでCS端末のOS管理者権限を取得することに成功した（甲第4号証の2、第5号証）。

しかし、重要機能室に入室せずにCSサーバのOSの管理者権限を奪取することは行われていない。

- ④ 住基ネット本体へ直接侵入したり、CS端末の住基アプリケーションを操作したりすること、当該市町村以外の本人確認情報を閲覧することには成功しなかった。

3. 被告兵庫県及び被告市町における住基ネットの運用状況について

甲第29号証、第30号証、第38号証（枝番含む。）、乙第54号証及び弁論の全趣旨によれば、次の事実が認められる。

(1) 被告兵庫県は、本人確認情報の提供、利用及び保護に関する条例を制定し、平成16年7月1日の施行に先立ち、同年4月、区域内の各市町村の住基ネット管理体制を確認するため、兵庫県チェックリストを交付し、回答を求めたところ、被告市町において、総務省がまとめた重要7項目に関する報告と矛盾する回答結果が得られた。

(2) すなわち、前記のとおり総務省は、重要7項目については、全国すべての市町村において、3点満点を達成したと発表していたが、兵庫県チェックリストのうち、重点7項目と内容が重複するとみられる項目の一部について、被告姫路市、同加古川市、同猪名川町、同芦屋市、同伊丹市及び同宝塚市が安全基準をみたしていないと回答した。

具体的には、重要項目③と重複する「CSと庁内LANの間にファイアウォールを設置している－兵庫県チェックリスト114」につき、被告伊丹市が「いいえ」と回答し、重要項目④と重複する「CSと庁内LANの通信をファイアウォールの設定において住基ネットに必要な通信のみに制限している－同115」につき、被告伊丹市が「いいえ」と回答し、重要項目⑤と重複する「庁内LAN上の端末機からインターネットに接続できないよう制限している－同124」について、被告姫路市、同加古川市、同猪名川町、同芦屋市、同伊丹市、同宝塚市が「いいえ」と回答し、重要項目⑥と重複する「庁内LANにインターネットからアクセス可能な公開サーバを設置していない（DMZ構成としている）－同126」については、被告芦屋市、同伊丹市が「いいえ」と回答し、重要項目⑦と重複する「公開サーバに最新のパッチを当てている－同130」について、被告芦屋市が「いいえ」と回答している。

(3) また、上記回答結果によると、被告尼崎市において、OSに関し、ログオン失敗履歴を記録していない、被告明石市において、庁内LANとインターネット間のファイアウォールのアクセスログを保存していない、被告

伊丹市において、CS及び通信網機器を設置する重要機能室の部屋の鍵又は入退室カードの管理責任者を定めていない、CSが存在するLANの通信網機器の物理的配線状況を管理していない、委託業者の管理が不十分であるなど、セキュリティが不十分であることを示す回答がみられる。

(4) 被告伊丹市は、平成18年3月時点では、庁内LANのうち、外部のインターネット通信網と接続した情報系LANは、住民基本台帳システムと接続しておらず、住民基本台帳システムを含む基幹系LANとCSとは接続しているが、その間にファイアウォールが設置され、重要項目③（兵庫県チェックリスト114）を充足しない状態はなくなっている。

4 住基ネットの存在意義について

住基ネットは、行政事務の効率化・合理化を図るとともに、行政手続における住民の負担軽減、住民サービスの高度化等により利便性を図ることを目的としており（乙第4ないし第9号証）、その運用により、以下のとおり、事務の省略化が図られるなどの有用性が認められる。

(1) 各種申請手続の簡素化

各種の行政的申請手続の際、市町村、都道府県及び国の機関等が、他の市町村に居住する申請者（又は関係者）の同一性を識別する必要がある場合、以前は、当該申請者（又は関係者）の住民票の写しの提出が求められていた。

しかし、住基ネットが稼働したことにより、市町村、都道府県、国の機関の相互間で、電気通信回線により本人確認情報の送受信がされることになったため、本人確認情報の提供及び利用が可能な275の行政事務について、国民は住民票の写しの有償取得の負担を、市町村はその写しの交付事務を、行政機関はその写しの受付事務を省略することができることになった。

(2) 年金・恩給支給事務の合理化

年金受給者は、以前は、毎年、現況届又は身上報告書を年金支給機関に提出しなければならなかったが、住基ネットにより、加給年金対象者を除いて上記書面の提出が不要となった。そして、年金支給機関も現況届等の送付及び受付事務を削減することができるようになった。

また、年金支給機関は、支給の都度、住基ネットによって簡易迅速に本人確認情報を確認することができるようになったため、以前は極めて頻繁に発生した年金の過誤払（死亡を看過して年金を支給すること）を防止することができ、そのため、過誤払金の回収事務の負担を大幅に軽減できることになった。

さらに、恩給受給者についても、以前は、毎年、市町村長の証明印を受けて受給権調査申立書を提出する必要があったが、住基ネットの利用により証明印の提出が不要となり（乙第10号証）、受給者及び市町村の負担が削減できるとともに、過誤払金の削減、回収事務の負担が軽減できることになった。

(3) 住民基本台帳事務の簡素化

住民の転入届の際に転出元の市町村作成の転出証明書を添付しなければならず（法22条2項、施行令23条）、住民は、他の市町村に転居しようとするれば、転出する市町村の役場に出頭して転出証明書の交付を受ける必要があるが、住基カードの交付を受けている者は、「付記転出届」を郵送等により行うなどの手続を行えば、転出証明書の添付を要しないこととされ、転出する市町村の役場に出頭する必要がなくなった（法24条の2第1項）。

(4) 住民票の写しの広域化

住民は、住基カード又は総務省令で定める書類を提示して、当該住民の住民票（住民基本台帳）を備える市町村以外の市町村の首長に対し住民票の写し（法7条5号、9号ないし12号及び14号に掲げる事項を省略し

たもの)の交付を請求することができることになった(法12条の2第1ないし第4項)。

(5) 将来的な電子政府への備え

国は、将来的に電子政府、電子自治体を実現するとし、その核心として、自宅や職場からパソコンとインターネットを通じて行政サービスを受けることができるよう取り組んでいる。この基盤となるのが、公的個人認証サービスであり、住基ネット及び住基カードは、そのための不可欠な役割を果たすことが期待されている(乙第6号証、第10ないし第12号証)。

5 人格権的妨害予防請求権の成否について

(1) 以上に説示のとおりであって、住基ネット上で知事や指定機関が保有する情報は、個人を特定しその同一性を識別するための本人確認情報だけであり、これを利用する機関や目的も限定されている。

また、住基ネットからの情報漏えいは、単に刑罰をもって抑止されているだけではなく、全国一律の安全基準が定められ、これに沿った取扱いを実施するための種々の指導監督の措置を講じることによっても防止されることになっている。

さらに、住基ネットは、通常のインターネット通信網との接点が全く存在しない完全な閉鎖型通信網ではないと考えられるが、閉鎖的な専用通信網によって、独自の暗号通信を用いて稼働しており、CSその他のサーバへの不正侵入を防止するため、ファイアウォールの設置を含む様々な措置が義務付けられており、長野県の侵入実験の結果に照らしても、通常のインターネット通信網からの侵入によって本人確認情報が不正取得される危険はかなり少ないといえることができる。

(2) 確かに、兵庫県チェックリストの回答結果をみると、総務省が定めた安全基準がすべて守られている状況になく、平成16年4月時点における被

告伊丹市の管理体制に問題があったことは否定できない。

被告らは、CSや重要機能室の管理体制を明らかにすることに終始消極的であり、平成16年4月以降、被告市町のCSや重要機能室の管理体制が改善されたかも具体的に明らかにほしないが、少なくとも、伊丹市のCSの管理体制の重大な欠陥とみられる重要項目③（兵庫県チェックリスト114）を充足しない状態はなくなっている。

そして、住基ネットにおいては、端末機からCSにアクセスする際、常に操作者識別カードと端末機との間で相互認証を行って初めて住基アプリケーションが起動する設計がされていること、また、住基アプリケーションを起動させるためには、操作者識別カードを挿入する必要があることからすれば、兵庫県チェックリストに対する回答においてみられた前記認定の管理体制の不備は、直ちに、本人確認情報の漏えいにつながるものということはできない。

(3) また、仮に、全国の市町村のいずれかにおいてCS及び重要機能室の管理体制に不備な点があるとしても、このことによって、直ちに被告市町の住民の本人確認情報の漏えいの危険が生じるということとはできない。すなわち、市町村のCSは、当該市町村の住民の本人確認情報を保持するのみで、他の市町村の住民の本人確認情報は、他の市町村のCS、都道府県サーバ、全国サーバに保有されているから、他の市町村の通信網から、被告市町のCSに不正侵入するためには、他の市町村、都道府県、指定機関が管理するファイアウォールを突破する必要があるが、これは極めて困難であるし、市町村設置のCSやその端末機に不正侵入したとしても、識別カードを挿入することなしに住基アプリケーションを起動させることができないから、本人確認情報を閲覧し取得することは困難なのである。

(4) 以上にみたとおり、住基ネットは、本人確認情報の漏えいを防止するための制度上の仕組みや技術上の対策がとられており、現時点で、本人確認

情報の漏えいの具体的な危険があるとまでは認められない。すなわち、みだりに自己の個人情報を他人に知られない原告らの権利（プライバシーに関する権利を含む人格権）が侵害される具体的な危険があるとまではいえない。したがって、その危険をあらかじめ防止するため、原告らの本人確認情報を住基ネットで管理・送受信することを禁ずる人格的請求権が発生しているとは認められない。

- (5) もっとも、住基ネットは人間が稼働させているものである以上、そこには、常に、情報漏えいの抽象的な危険があることは否定できない。しかしながら、住基ネットの有用性に鑑みれば、そのような抽象的な危険があるというだけでは、住基ネットによる本人確認情報の管理及び送受信の禁止を求めることはできないと解される。

住基ネットの稼働により、個々の国民が具体的な便益を享受するという場面は少なく、したがって、個々の国民がその利便性を実感するということも少ないであろうが、上記3にみたとおり、住基ネットは、国や地方公共団体の行政事務の合理化のために有用な仕組みである。殊に、毎年かなり頻繁に発生していた年金の過誤払を防止するという観点からみれば、住基ネットは極めて簡便かつ効果的にこれを防止する仕組みであり、この観点からは住基ネットに代わる簡便かつ効果的な代替措置は想定し難いのであって、住基ネットは公共の利益に資することが明らかである。

そうすると、情報漏えいの抽象的な危険があるというだけで、原告らの本人確認情報を住基ネットで管理・送受信することを禁ずる人格的請求権が発生すると解することは、明らかに行き過ぎである。

- 6 以上のとおりであって、プライバシーに関する権利を含む人格権に基づく原告らの請求は理由がない。

第10 結論

以上の次第で、原告らの請求はいずれも理由がないから棄却し、訴訟費用の

負担につき民事訴訟法61条を適用して、主文のとおり判決する。

神戸地方裁判所第6民事部

裁判長裁判官 橋 詰 均

裁判官 官 端 謙 一

裁判官大藪和男は転勤のため、署名押印することができない。

裁判長裁判官 橋 詰 均

(別表1)

原告らの表示	
A	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
B	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]

E	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
F	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]

	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
G	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
H	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
I	[Redacted]	[Redacted]	
J	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
K	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
L	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
	[Redacted]	[Redacted]	
M	[Redacted]	[Redacted]	
N	[Redacted]	[Redacted]	
原告ら訴訟代理人（弁護士）の表示			
在 間 秀 和	上 原 康 夫	島 村 美 樹	大 川 一 夫
井 上 二 郎	桜 井 健 雄	平 栗 勲	

(別表 2)

被告ら及び被告ら訴訟代理人の表示	
神戸市中央区加納町6丁目5番1号	
被 告	神 戸 市
同代表者市長	矢 田 立 郎
同指定代理人	古田 隆・坂本健三・田嶋 徹・久保阿左子
兵庫県川西市中央町12番1号	
被 告	川 西 市
同代表者市長	柴 生 進
同指定代理人	高塚昌樹・堀 哲雄・芝 良一
兵庫県宝塚市東洋町1番1号	
被 告	宝 塚 市
同代表者市長	阪 上 善 秀
同指定代理人	坂田 響・立花 誠・樋之内登志・中出勝也
兵庫県伊丹市千僧1丁目1番地	
被 告	伊 丹 市
同代表者市長	藤 原 保 幸
同指定代理人	小宮正照・村上 正・松本好彦
兵庫県西宮市六湛寺町10番3号	
被 告	西 宮 市
同代表者市長	山 田 知
同指定代理人	西原直志・大濱 弘・宮島茂敏
同	小林 誠・荒川 卓
兵庫県尼崎市東七松町1丁目23番1号	
被 告	尼 崎 市
同代表者市長	白 井 文
同指定代理人	丹羽益蔵・高寺秀典

兵庫県川辺郡猪名川町上野字北畑11番地の1	
被 告	猪 名 川 町
同代表者町長	真 田 保 男
同指定代理人	水越久子・小東治夫・村本尋之
兵庫県芦屋市精道町7番6号	
被 告	芦 屋 市
同代表者市長	山 中 健
同指定代理人	北口泰弘・山名雅昭・和泉みどり
兵庫県小野市王子町806番地の1	
被 告	小 野 市
同代表者市長	蓮 葉 務
同指定代理人	岸本浩幸・藤木一人・松井 孝
兵庫県姫路市安田4丁目1番地	
被 告	姫 路 市
同代表者市長	石 見 利 勝
同指定代理人	坂田基秀・森下裕子・笹井 誠
同	島尾善之・山本泰廣
兵庫県加古川市加古川町北在家2000	
被 告	加 古 川 市
同代表者市長	樽 本 庄 一
同指定代理人	荻内和彦・加古善彦・森山知子
兵庫県高砂市荒井町千鳥1丁目1番1号	
被 告	高 砂 市
同代表者市長	田 村 広 一
同指定代理人	天野住子・原 廣幸

兵庫県明石市中崎1丁目5-1

被 告

明 石 市

同代表者市長

北 口 寛 人

同指定代理人

小林正文・古河 環・杉浦隆志

兵庫県篠山市北新町4-1

被 告

篠 山 市

同代表者市長

瀬 戸 亀 男

同指定代理人

横山美佐子・山本一也・吉田鉄夫

同

田中義明・畑 一成

神戸市中央区下山手通5丁目10番1号

被 告

兵 庫 県

同代表者知事

井 戸 敏 三

同指定代理人

田代浩之・山田真太郎・勝本 勲・名倉嗣朗

同

綾木隆弘・小倉豊道・小林宏識

被告兵庫県，同神戸市，同姫路市，同尼崎市，同西宮市，同芦屋市，同伊丹市，同加古川市，同宝塚市，同高砂市，同川西市，同小野市，同猪名川町，同明石市及び同篠山市指定代理人

酒 井 一 成 奥 畑 薫 石 井 義 規

堀 江 明 子 山 本 小 夜 子 橋 本 一 郎

北 村 修 田 中 芳 弘

東京都千代田区一番町25番地

被 告

財団法人地方自治情報センター

同代表者理事

芳 山 達 郎

同訴訟代理人弁護士

橋本 勇・小倉秀夫・大下 信

これは正本である。

平成18年6月9日

神戸地方裁判所第6民事部

裁判所書記官 前 中 一 正