

とする住基台帳事務の効率化が阻害されることとなる。さらに、選択方式は、非通知申出者の把握に多大なコストがかかり、住基ネットの目的を阻害する。

- c. 行政事務の効率化が達成されれば、税金の負担、福利施設の充実等といった住民の利益にも還元されるのであるから、住民の便益と行政事務の効率化とを単純に区別することは相当ではなく、両者は一体のものとして総合的に検討されるべきである。そして、住基ネットは、我が国の国家戦略である電子政府構想を推進するための基盤として極めて重要な機能を担うものであり、また、旅券発行、年金受給者に対する現況確認等様々な行政事務の基盤として機能し、今後拡充されることも見込まれるのであるから、仮に一部の住民について本人確認情報が提供されない事態を容認するとすれば、このような事務の実施に著しい悪影響を及ぼして、行政の効率化に支障を来すのみならず、行政の公平性の観点からみても問題がある。

以上のとおり、住基ネットの運用により原告らのプライバシー権が侵害されているとはいえないうえ、住基ネットには、正当かつ必要な目的があるから、原告らの差止請求を認めることはできない。

(2) 争点(2) (氏名権侵害に基づく差止請求の当否) について

ア 原告らの主張

氏名権は、人格権の一内容として憲法13条によって保障されている。国民全員に、重複しない識別番号として11桁の数字からなる住民票コードを付し、この識別番号をもとに個人情報処理し、国民を、氏名ではなく、住民票コードによって特定することは、「氏名」を、住民票コードで分類される個人情報の中の一つにおとしめるものである。

このように、住基ネットの運用において、原告らを、氏名ではなく、番号で取り扱うことは、原告らの明示の意思に反してその氏名権を侵害する

ものである。そして、住基ネットによる原告らの氏名権侵害の程度は深刻であり、その精神的苦痛は著しいから、住基ネットの運用は差し止められるべきである。

イ 被告らの主張

原告らが主張する氏名権は、実体法上及び判例上の根拠を有するものではないから、憲法13条により保障される権利であると解する余地はない。

また、住民票コードは、4情報を電子計算機及び電気通信回線を用いて効率的に送信するために、技術的な観点から設けられた符号にすぎず、そもそも個人の人格的価値とは無関係であるから、住民票に住民票コードが記載されることによって、氏名権が侵害されるなどと解する余地はない。

(3) 争点(3)（「行政によって包括的に管理されない自由」の侵害に基づく差止請求の当否）について

ア 原告らの主張

「行政によって包括的に管理されない自由」とは、行政機関によって個別に保有されている個人情報、他の行政機関と交換して結合し、いつでも利用できる状態に置かれることを拒絶する自由をいい、個人の人格的生存に不可欠な利益として、憲法13条によって保障されている。

住基ネットにより、共通番号である住民票コードを付し、本人確認情報を流通させることは、原告らの個人情報の名寄せを可能にし、情報の集約化を進めるものであり、原告らの「行政によって包括的に管理されない自由」を侵害していることは明らかである。しかも、行政機関は、個別に保有する個人情報を、他の行政機関と交換結合し、いつでも利用できる状態にしているのであるから、その侵害の程度は深刻である。したがって、「行政によって包括的に管理されない自由」の侵害に基づき、住基ネットの運用は差し止められるべきである。

イ 被告らの主張

原告らが主張する「行政によって包括的に管理されない自由」とは、実体法上及び判例上の根拠を有するものではないから、憲法13条により保障される権利であると解する余地はない。

前記(2)イのとおり、住民票コードは、4情報を電子計算機及び電気通信回線を用いて効率的に送信するために、技術的な観点から設けられた符号にすぎず、そもそも個人の人格的価値とは無関係であるから、住民票に住民票コードが記載されることによって、「行政によって包括的に管理されない自由」が侵害されるなどと解する余地はない。また、住基ネットの運用により、住民票コードをいわばマスターキーのように使用し、本来の目的以外の目的のために行政機関が保有している個人情報名寄せされる具体的危険などおよそ想定できないのであるから、原告らが、行政によって包括的に管理されるなどという事態が生じるものでないことも明らかである。

(4) 争点(4) (損害賠償責任の成否について)

ア 原告らの主張

(ア) 被告国について

被告国(内閣並びに内閣総理大臣及び総務大臣)は、憲法11条、13条、99条を遵守し、国民の人権を保障する義務を負うところ、憲法に違反する法律については、改廃をしたり、施行を延期するなどの相当の手段を講ずることにより、国民の権利が侵害されるのを防止する義務を負っている。しかし、内閣は、改正法が憲法に違反しているにもかかわらず、①前記のとおり、改正法附則1条2項所定の所要の措置を講ずることなく、また、施行日までに講ずることが出来る見込みがないのに、平成13年12月28日、改正法を平成14年8月5日から施行する政令を定め、②施行日までに、改正法の施行・運用の開始を停止する等の措置を講じず、③改正法を施行し、④改正法施行後、改正法を廃止又は

運用の停止等の相当の方策を講じなかった。

また、内閣総理大臣及び総務大臣は、憲法に違反する改正法の施行運用を積極的に推進し、その結果、原告らの自己情報コントロール権、氏名権及び「行政によって包括的に管理されない自由」を侵害し、今後も侵害する危険にさらしているものである。したがって、被告国は、原告らに対し、国賠法上の損害賠償責任を負う。

(イ) 被告県らについて

被告県ら及び本件知事らは、憲法 11 条、13 条、99 条により憲法を遵守し、都県民の人権を保障する義務を負っており、また、住基法においては、住基ネットから離脱する権限(ネットワークの接続を断つ権限)をも含む「当該本人確認情報の適切な管理のために必要な措置」を講ずる権限を付与されていたにもかかわらず、これらの義務を怠り、①本件市区町長らに対し、住民票コードを指定して通知し、②本人確認情報を磁気ディスクに記録して保存し、③国の機関等に対し、本人確認情報を提供し、④被告センターに対し、住民票コードの指定及び通知並びに国の機関等への本人確認情報の提供等の本人確認情報処理事務を委任し、⑤被告センターに対し、本人確認情報を通知する等の事務を実施し、その結果、原告らの自己情報コントロール権、氏名権及び「行政から包括的に管理されない自由」を侵害し、今後も侵害する危険にさらしているものである。よって、被告県らも、原告らに対し、国賠法上の損害賠償責任を負う。

(ウ) 被告センターについて

被告センターは、指定情報処理機関として、被告県らからの委任を受け、原告らの本人確認情報について事務処理を行い、これにより、原告らの自己情報コントロール権及び氏名権を侵害したから、原告らに対し、不法行為責任(民法 709 条)を負う。

(エ) 損害

a 原告らは、被告国の違法行為により、自己情報コントロール権等を侵害され、多大な精神的苦痛を被っている。この精神的苦痛を慰謝するには、少なくとも原告ら一人当たり別紙請求目録の「慰謝料額」欄記載の金員の支払が相当である。また、弁護士費用のうち原告らの慰謝料額の1割に相当する額は、前記違法行為と相当因果関係のある原告らの損害である。

b 原告らは、被告県ら及び被告センターの違法行為により、自己情報コントロール権等を侵害され、多大な精神的苦痛を被っている。この精神的苦痛を慰謝するには、少なくとも原告ら一人当たり別紙請求目録の「慰謝料額」欄記載の金員の支払が相当である。また、弁護士費用のうち原告らの慰謝料額の1割に相当する額は、前記違法行為と相当因果関係のある原告らの損害である。

イ 被告らの主張

(ア) 被告国について

国賠法1条1項にいう違法とは、公務員が個別の国民に対して負う職務上の法的義務に違背することを指し（最高裁判所昭和60年11月21日第一小法廷判決・民集39巻7号1512頁参照）、公務員の行為は、当該公務員が職務上通常尽くすべき注意義務を尽くさず、漫然と当該行為をしたと認め得るような事情がある場合に限り、同項にいう違法があったとの評価を受けるものというべきである（最高裁判所平成5年3月11日第一小法廷判決・民集47巻4号2863頁参照）。

内閣は、専ら法律を誠実に執行すべき責務を負うものであり（憲法73条1号）、法律の規定に従って適切に事務を行っている限り、職務上通常尽くすべき注意義務を尽くしたことになるのであり、住基ネットの運用について国賠法1条1項にいう違法があったとの評価を受ける余地

はない。

また、原告らが主張する内閣の行為①及び③は、所要の措置が適切に講じられていないことなどを前提とするものであるところ、改正法は適法に施行されており、所要の措置も適法に講じられているから、何ら違法ではない。同様に、内閣の行為②及び④は、改正法が違憲であることを前提とするものであるところ、自己情報コントロール権が憲法上の権利として保障されたものでないことは前記のとおりであるし、仮に、そのような権利があるとしても、改正法の憲法適合性については緩やかな審査基準に服するものであって、その基準に照らせば、改正法の運用も含めて、到底違憲といえるものではない。

したがって、プライバシー権等の侵害の有無を論じるまでもなく、原告らが主張する行為については、国賠法1条1項の違法がないことが明らかである。

(イ) 被告県らについて

前記(ア)のとおり、公務員の行為は、当該公務員が職務上通常尽くすべき注意義務を尽くさず、漫然と当該行為をしたと認め得るような事情がある場合に限り、国賠法1条1項にいう違法があったとの評価を受けるものというべきところ、自治体において行政の執行に当たる首長は、法律の規定に従って適切に事務を行っている限り、職務上通常尽くすべき注意義務を尽くしたことになり、住基ネットの運用について、国賠法1条1項にいう違法があったとの評価を受ける余地はない。

原告らが主張する本件知事らの行為①ないし⑤は、いずれも法の明文の規定に従って適切に行われたことが明らかであるから、本件知事らは、住基法の規定に従って適切に事務を行うことによって、職務上通常尽くすべき注意義務を尽くしたものであって、国賠法1条1項にいう違法があったとの評価を受けることなどあり得ない。

したがって、プライバシー権等の侵害の有無を論じるまでもなく、原告らが主張する行為については、国賠法1条1項の違法がないことが明らかである。

(ウ) 被告センターについて

被告センターは、住基法に従って、所定の事務を行っているにすぎず、住基ネットの運用について何ら違法とされる行為を行ってはいない。

(エ) 損害について

原告ら主張の損害の発生を争う。

第3 争点に対する判断

1 争点(1) (プライバシー権侵害に基づく差止請求の当否) について

(1) プライバシー権の内容について

ア 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。そして、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、個人の私生活における平穩が害され、個人の人格的自律が脅かされることとなるのであるから、このような他人に知られたくないと感じる個人の私生活上の情報（プライバシー）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といふべきである。

イ 個人の情報にも様々なものが存在するところ、氏名、出生の年月日、男女の別及び住所（4情報）、住民票コード及び変更情報という本人確認情報は、個人の識別情報ないし客観的外形的事項としての性格も強く、純粋な私生活上の情報とはいいい難い側面もあり、また、秘匿の必要性も、必ずしも常に高度であるとまではいうことができない。しかしながら、近時、コンピュータを利用した情報管理技術の進展に伴い、行政機関や民間企業において、大量の個人情報収集、蓄積されるに至っており、実際にも、

個人情報の漏洩や目的外利用の問題が発生していることが認められる（甲共45, 81の1・2, 82, 121, 165）。このような状況において、国民の間にも、情報を保有し、管理する機関について、収集、蓄積された個人情報が漏洩することや、目的外のことに使用されること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。そして、このことは、本人確認情報のような単純な個人情報であっても同様であり、その漏洩、売買等により、本人が開示を許容していない者にまで情報が提供され、その情報を取得した者から何らかの働きかけを受けることによって、私生活の平穩が害されるのではないかと心理的負担や不安が増大する傾向にある。このような社会状況においては、情報提供の相手方、利用方法等に関する本人の合理的な期待が保護されるべきであり、前記アのプライバシーに係る利益にも、個人情報を本人の合理的な期待に反して開示提供されない利益が含まれると解すべきである。

ウ そして、前記のような私生活の平穩及び個人の人格的自律を維持するというプライバシー保護の趣旨に照らせば、本人確認情報、すなわち、氏名、出生の年月日、男女の別及び住所（4情報）、住民票コード及び変更情報についても、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になれば、個人が不安を感じ、その私生活の平穩及び人格的自律が害される可能性があるから、本人確認情報が、予定された者や利用範囲以外には通知提供されることはないという限度において、個人の期待は保護されるべきものである。

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利益は、法的な保護に値するものというべきである（最高裁判所平成15年9月12日第二小法廷判決・民集57巻8号973頁参照）。原告らの主張する自己情報コントロール権も、基本

的には、同様の趣旨をいうものと理解され、その限度において理由があるというべきである。

なお、被告らは、本人確認情報のうち4情報は、住基法が改正される前から閲覧することが可能であったから、プライバシーに含まれるものではないと主張する。しかしながら、従前閲覧が可能な情報であったとしても、秘匿の必要性の程度が低いことを示す事情として論ずるのであればともかく、そのことをもって直ちにプライバシー保護の対象からはずれるということとはできないから、被告らのこの点の主張は採用できない。

ところで、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利益が法的な保護に値するものであるとしても、国家権力の行使に対して無制限に保護されるものではなく、公共の福祉のために必要がある場合には相当の制限を受けることは憲法13条自体においても定められているところであるから、以下、住基ネットによるプライバシー侵害あるいはその危険性の有無について検討した上で、上記利益の制限が認められた場合であっても、さらに、公共の福祉による制限として許容され得るものか否かにつき、原告らが請求する差止めの必要性に係る判断の中で総合的に検討することとする。

(2)ア 住基ネットによるプライバシー権の侵害の有無について

原告らは、従来、市町村だけが保有していた情報が、住基ネットにより、一体としてネットワーク上で共有されるようになったため、どのように流通、蓄積、利用されているかが認識できず、深刻な不安を抱くようになり、また、住基ネットは、国民一人一人に重複しない番号を付したうえで、全国の地方公共団体、国の機関及び被告センターを接続しているネットワーク上で、個人情報と共有するものであり、これによって、行政機関等は、自ら保有している個人情報と、本人確認情報及びその他の機関が保有している情報とを名寄せすることが可能となったのであるから、このような事

態は、原告らの人格的自律を甚だしく脅かしており、原告らのプライバシー権はすでに侵害されていると主張する（前記第2の4(1)ア(イ)a）。

確かに、後述のとおり、改正前の住基法においては、居住する市町村だけに保有管理されていた本人確認情報が、住基ネットでは、都道府県知事に通知されて保有されることとなり、また、国の法人等、他の市町村の執行機関などにも通知提供され、都道府県知事によって利用されるようになったのであり、4情報を保有し、管理する主体が、住基法の改正前に比して、拡大し、増加したことは事実である。

そして、このような状況の下で、本人確認情報が通知提供される相手方を逐一把握認識することができない以上、住基ネットの運用により原告らが不安を感じているとすることについては理解できないわけではない。しかしながら、住基法が改正される前も、国又は地方公共団体の職員が、その職名、職務上の請求である旨及びその者の住所氏名を明らかにすれば、市町村長から、住民票写しの交付を受けることは可能であったのであり（改正前住基法12条1項、2項、住民基本台帳の閲覧及び住民票の写し等の交付に関する省令3条2号）、原告らの4情報は、住基法の改正前から、行政目的に使用される場合には、国や他の自治体に対して開示されていたものというべきである。住基ネットの運用開始後は、国、自治体のコンピュータがネットワーク化されたことによって、本人確認情報の通知提供が、技術的に容易になって、その機会も格段に増加したというべきであるが、他の自治体、国に対する4情報の開示そのものは、住基法改正前から行われていたものであるから、住基ネットの運用開始によって、本人確認情報の開示対象又は利用範囲に質的な変化があったとはいうことができない。

原告らの主張する不安ないし心理的負担も、住基ネットの運用により、原告らの本人確認情報が、予定された開示対象及び利用範囲を逸脱して現

真に開示されたことが認められない以上、それは抽象的な不安ないし心理的負担にとどまるのであり、何らかの権利ないし利益を具体的に侵害したとまではいうことができない。

また、原告らが主張する名寄せの可能性についても、住基ネットによって、名寄せが行われることが技術的に可能となった以上、原告らが、それに対して不安感を抱くことも理解できないわけではない。しかしながら、単に不安感を抱いているというだけで、直ちにプライバシーを侵害したことになると考えるのが相当でないことは前示のとおりであり、予定された範囲を逸脱して個人情報を利用された場合に初めて、プライバシー侵害の問題が生じるというべきである。そして、住基ネットにおいては、証拠によっても、未だ名寄せが行われたとは認めることができないのであるから、現にプライバシーが侵害されたとまではいうことができない。

したがって、住基ネットの運用は、原告らのプライバシーに関する利益を現に侵害するものではないと判断するのが相当である。

イ 住基ネットによるプライバシー権の侵害の危険性について

原告らは、外部の者や運用関係者が住基ネットから原告らの本人確認情報を漏洩する可能性や名寄せが行われる可能性があり、原告らのプライバシー権が侵害される危険が生じていると主張する。

(ア) 外部からの侵入及び運用関係者による漏洩の危険

後記(3)ウイ)において詳述するとおり、証拠(乙共13, 41)によれば、インターネットに接続したコンピュータと住基ネットとが、庁内LANで接続されている自治体が依然として存在する実情を考えると、外部の者が、何らかの手法で、庁内LANに侵入し、さらに、住基ネットにも侵入することは、技術的には可能であるというべきである。

また、本人確認情報の提供に当たっては、本人確認情報を格納した磁気ディスクを送付する方法も採られており(住基法施行令30条の7な

いし10各第2号)、運用関係者が、本人確認情報を入手、漏洩することも、技術的には可能であるというべきである。

(イ) 名寄せの危険

前記のとおり、住基ネットでは、自治体、被告センター及び国の機関等のコンピュータがネットワーク化されており、このネットワークを通じて情報が通知提供される以上、個人情報の管理主体が、住基法改正前に比べて格段に増加し、また、個人情報のデータベース化も技術的に容易になったのであるから、行政機関が、本人確認情報及びその他の個人情報をも名寄せすることが、技術的に可能となり、また、容易になったというべきである。

ウ 以上によれば、住基ネットの運用により、原告らのプライバシーに関する情報が原告らの認識なくして提供利用され、また、外部者及び運用関係者による本人確認情報の漏洩等の可能性が存在する以上、住基ネットの運用による、原告らのプライバシー侵害の危険性は完全には否定しきれないというべきである。

(3) 差止めの必要性(許容性)について

(2)において判示したとおり、住基ネットの運用による、原告らのプライバシー侵害の危険性は完全には否定しきれないとしても、プライバシーに関する利益も、無制限に法的な保護を受けるものではなく、公共の福祉のために必要がある場合には相当な範囲内で制限を受けるものであることは、前述したところである。そして、住基ネットの運用が、原告らのプライバシーを侵害する危険性を有していたとしても、公共の福祉に基づく制限として許容されるか否かは、住基ネットの制度目的の合理性及び制度の必要性と、住基ネットの運用による原告らのプライバシー侵害の危険性の内容及び程度を検討して総合的に判断するのが相当である。

ア 住基ネットの目的の合理性

(ア) 住民負担の軽減と行政事務の効率化及び正確性の向上、市町村のネットワーク化による住民基本台帳事務の簡素化及び広域化、経費の削減

前記第2の2(3)アのとおり、住基法は、住基台帳の制度について、市町村における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、住民に関する記録を正確かつ統一的に行うものであり、これにより、住民の利便を増進し、国及び地方公共団体の行政の合理化に資することを目的とするものと定めている。また、証拠(乙共89)によれば、第145回衆議院本会議においても、当時の小淵恵三内閣総理大臣は、改正法について、住民の利便を増進し、国及び地方公共団体の行政の合理化に資することを目的とするとの趣旨の答弁をしたことが認められる。以上の住基法の目的及び改正の経緯に照らすと、住基ネットの目的は、第一次的には、住民の利便の増進ないし国及び地方公共団体の行政の合理化にあるというべきであり、これらの目的が、それ自体合理性を有するものであることは明らかである。

そして、前記第2の2(3)キによれば、住基ネットにより、住基カードの保持者については、転出転入時の転出証明書の添付が不要となり、また、住民票写しを、居住市町村以外の市町村から取得することが可能となり、住民の利便及び窓口事務の短縮が図られること、行政機関等への申請や届出の際に義務づけられていた住民票写しの提出が不要となり、また、年金受給者及び恩給受給者の書類の提出が不要となり、住民の利便、窓口事務の短縮化及び行政事務の正確性の向上が図られることが認められ、これらもまた住基ネットの具体的な目的としてその合理性を裏付けるものといえる。

なお、原告らは、利便の享受よりもプライバシーの保護を優先させることを求め、自ら住基ネットによる利便を享受しないとしているのであるから、住基ネットにおける、住民の利便が増進するという目的は、原

告らに対する関係では、合理性がないと主張する。しかし、住基ネットが目的とする住民の利便とは、原告らがそれぞれ享受し得る個々の利便をいうのではなく、行政の合理化と表裏一体となった住民が全体として享受する利便をいうと解するのが相当であるから、原告らの利便享受の意思の有無によって、前記の判断が左右されるものではないというべきである。そうすると、住基ネットの運用によって、行政の合理化と表裏一体のものとしての住民全体の利便を図ることが目的としての合理性を有する以上、目的の合理性に欠けるところはないことになる。

(イ) 電子政府構想の実現、行政手続のオンライン化

前記第2の2(7)のとおり、IT戦略本部が発表した平成13年1月22日付けの「e-Japan戦略」によれば、電子政府構想は、行政内部や行政と、国民、事業者との間で書類を通して、または対面で行われている業務をオンライン化し、情報ネットワークを通じて、省庁横断的に、また、国及び地方公共団体を一体として情報を瞬時に共有・活用する新たな行政を実現するものとされている。そして、その実現に当たっては、行政の既存業務をそのままオンライン化するのではなく、IT化に向けた中長期にわたる計画的投資を行うとともに、業務改革、省庁横断的な類似業務・事業の整理及び制度・法令の見直し等を実施し、行政の簡素化・効率化、国民・事業者の負担の軽減を実現することが必要となり、またこの実現により、国民が、自宅や職場からインターネットを経由し、全ての行政手続の受付が24時間可能となって、国民生活がより快適で便利なものとなり、産業活動が活性化するとされている。このように、行政手続をオンラインで申請できるようにすることが電子政府構想の前提となっているところ、前記第2の2(3)オ(イ)のとおり、行政手続オンライン化関係3法の成立により、住民が行政機関に対する申請及び届出をインターネットで行うことが可能となり、インターネットでの

行政手続においては、住民票写しの提出を省略したり、公的個人認証サービスによって本人確認を行うなど、住基ネットの活用場面が想定されるところである。

以上のとおり、行政手続のオンライン化、電子政府構想（行政手続のオンライン化と電子政府構想の実現を一括して、以下「電子政府構想の実現」という。）を実現するためには、住基ネットが、その基盤の一つとなることが予定されていること、情報通信技術の発展に伴い、国内外でコンピュータネットワークが構築、活用されていること、また、前記第2の2(7)のとおり、「高度情報通信ネットワーク社会形成基本法」、
「e-Japan戦略」、
「e-Japan戦略Ⅱ」等において、日本の重要な国家戦略としてIT国家の実現が掲げられていることに照らせば、これらは、住基ネットの目的として合理性を有するといふべきである。

なお、原告らは、改正法に関する閣議決定が平成10年3月10日であることから、平成12年に提唱された電子政府構想が、住基ネットの目的となることはないと主張する。確かに、電子政府構想が具体的に立案されたのは、前記第2の2(7)のとおり、平成12年以降のことである。しかし、差止請求の判断は、口頭弁論終結時までの事情を基礎とすべきであり、その前提となるプライバシーの制限の許否についても、住基法改正当時の事情に限られず、口頭弁論終結時までに存在した事情を考慮して、目的の合理性の有無を検討するのが相当である。また、もともと、電子政府構想は、高度情報通信ネットワーク社会に対応するために考案されたものと考えられるところ、証拠（乙共42、43）によれば、高度情報通信ネットワーク社会に対応するための動きは、平成8年3月の住基ネットの研究会においても見られるところである。したがって、電子政府構想の基礎となるべき基本的考え方自体は、改正法成立時にも既

に存在していたと認められる以上、電子政府構想としての提唱が改正法成立の後であったとしても、この構想が住基ネットの目的として合理性を有するという前記判断を左右するものではないというべきである。

(ウ) 住基カードによる利益

前記第2の2(3)ク、(8)オによれば、住基カードは、公的個人認証法による個人認証制度において、電子証明書及び秘密鍵の格納媒体として利用されることが予定され、市町村が条例で定めることにより、多目的カードとして利用することができる。また、転出・転入の手続の特例では、住基カードの交付を受けている者等が、「付記転出届」をした場合には、転出証明書の添付を要しないこととされるのであり、転出入手続特例の基盤にもなるものである。このように、住基カードは、住民の利便の増進ないし行政の合理化につながるものであり、住基ネット導入の目的の合理性を支える重要な要素となり得るものと認められる。

以上のとおりであるから、住民の利便の増進ないし行政の合理化を図るという住基ネットの目的は合理的なものというべきであり、この点は、住基ネットによる利便の増進を望まないとする原告らとの間でも何ら差異を生じない。

イ 住基ネットの必要性

(ア) 住民の利便の増進ないし行政の合理化

前記第2の2(8)アのとおり、被告国の平成10年試算によると、行政側には約240億円の、住民側には約270億円の費用削減効果がそれぞれあったものとされているが、この試算は、住基ネットの運用前の推定に基づくものにすぎない。また、前記第2の2(8)エ(ウ)のとおり、住基カードの全国における発行枚数は、平成17年3月末現在、累計54万枚であり、特に、東京都では、平成15年8月25日から平成16年3月末までの住基カードの申請件数は、約4万枚であって、申請率は対人

口比で1パーセントに満たなかったし、横浜市における住基カードの申請件数も、約1万5000枚であったから、平成10年試算の前提となっているカードの所持率(1/2)等の数値がそのまま妥当しないことは明らかである。このような事情に照らせば、上記の平成10年試算の結果を直ちに採用することは相当でないというべきである。また、総務省の平成14年概要(第2の2(8)イ参照)によると、平成11年度から平成15年度までに、住基ネットの導入費用として約390億円、経常費用として毎年約190億円を要したとされているが、これらの具体的な根拠も明らかではない。したがって、住基ネットの導入による具体的な経費削減効果については、必ずしも明らかとはいえないところである。

しかしながら、前記第2の2(8)エのとおり、住民票写しの省略件数(年間約300万件)、年金受給者及び恩給受給者の書類省略件数(年間合計500万件)、住民票写しの広域交付、転出入手続の簡素化の利用状況からすると、これらの制度は、現時点においても住民によって一定程度利用されているものと認めることができるのであり、また、制度の定着に伴い、今後、これらの利用は拡大していくものと推認し得るものでもある。そうすると、住基ネットの導入により、住民側及び行政側それぞれに、一定の負担ないし事務の削減効果があったもの、あるいは今後相当程度の削減効果が生じ得るものと推認することができるというべきである。

また、住基法改正前には、自治体や国の機関等に対して住民票写しが交付されていたところ、住基ネットにより、本人確認情報の磁気ディスクによる一括提供やオンラインでの即時提供が可能になった(第2の2(3)オ、(6)イ)。さらに、行政手続において住民票写しの提出が省略され、転出転入時の転出証明書発行の事務が削減された(第2の2(8)エ)。

このように、住基ネットにより、一定程度行政事務が簡素化されたと

いうべきであり、これに伴って、行政事務の正確性も向上したと判断するのが相当である。

以上のとおり、住基ネットにより、住民の利便の増進ないし行政の合理化として一定の事務の削減効果等が認められるというべきである。

(イ) 電子政府構想の実現

電子政府構想においては、行政機関への申請及び届出がインターネットで行われるようになるところ、そのためには、個人認証制度の確立が不可欠の前提となる。前記第2の2(8)オのとおり、個人認証制度の一種である公的個人認証サービスでは、電子証明書の発行を受けた者に関して、住民票の記載の修正等があった場合は、失効リスト作成のために住基ネットによって本人確認情報が通知され、また、住基カードを、電子証明書及び秘密鍵の格納に利用することも可能となるから、住基ネットは、公的個人認証サービスの基盤となっているというべきである。

また、前記のとおり、電子政府構想は、行政内部や行政と、国民、事業者との間で書類又は対面により行われてきた業務を、オンライン化した情報ネットワークを通じて、省庁横断的、国及び地方一体的に情報を瞬時に共有・活用する新たな行政の実現を目指すものであり、これらの実現に当たっては、行政の既存業務をそのままオンライン化するのではなく、行政の簡素化・効率化、国民・事業者の負担の軽減を実現することとされているのであるから、前記のように住民の利便の増進ないし行政の合理化に資する住基ネットは、共通基盤の構築という役割を果たすことにもなるというべきである。

したがって、住基ネットは、電子政府構想の実現の基盤の一部となるものであり、そのための一定の役割を果たしているというべきである。

以上からすると、住基ネットは、住民の利便の増進ないし行政の合理化について、一定の負担削減効果ないし事務削減効果を達成することに

寄与しており、また、電子政府構想の実現のために一定の役割を果たしているものというべきである。したがって、前記アの目的を達成するための手段としての住基ネットの必要性はこれを肯定することができ、この点は、こうした利便の増進を望まない原告らとの間でも何ら差異は生じない。

ウ 侵害の危険性の内容及び程度

(ア) 住基ネットによる利用提供の態様等

住民票は、居住する市町村の長によって編成されるものである（住基法6条1項）ところ、本人確認情報のうち4情報は、住基法が改正されるまでは、原則として、居住する市町村だけが、住民票の記載事項として保有管理するものであった。ところが、改正後の住基法に基づき、住基ネットが運用を開始したことに伴い、前記第2の2(3)オのとおり、市町村、都道府県、被告センターに、それぞれCS、都道府県サーバ、全国サーバが設置接続され、市町村長が、住民票の記載、削除をしたり、4情報及び住民票コードの記載を修正した場合、都道府県知事に対して、本人確認情報を通知し、都道府県知事も、通知された情報を一定期間保存するようになった。また、市町村長は、条例の定めに従って、他の市町村長その他の執行機関、国の行政機関から事務処理に関し求めがあった場合は、本人確認情報を提供し、都道府県知事も、国の機関等、区域内の市町村の執行機関、他の都道府県の執行機関から事務処理に関し求めがあった場合は、保存する本人確認情報を提供するようになった。さらに、都道府県知事は、事務を遂行する場合、保存する本人確認情報を利用することも可能となった。このように、住基ネットにより、4情報を保有し、管理する主体が、住基法の改正前に比して、拡大し、増加したことは前示のとおりである。

しかしながら、原告らの4情報は、個人の識別情報としての性質も有

するものであり、住基法の改正前から、行政目的に使用される場合には、国や他の自治体に対して開示されていたものであるから、住基ネットの運用開始により本人確認情報の通知提供が、技術的に容易になって、その機会も格段に増加したとしても、それによって、本人確認情報の開示対象又は利用範囲に質的な変化があったということができないことは、前記1(2)アにおいて判示したとおりである。

そうすると、原告らの4情報については、予定された開示対象及び利用範囲を逸脱して開示されないという期待を保護する法的利益は認められるとしても、完全に秘匿される必要性が高いものであるとまでいうことはできない。また、住民票コードも、氏名等に代わり用いられるというものでもなく、私生活上重要なものということとはできず（後記2参照）、その他の情報についても、必ずしも私生活上重要で、完全に秘匿される必要性が高いものであるとまではいえない。

このような事情も考慮すると、住基ネットの運用による原告らの本人確認情報の利用提供の態様は、原告らの期待に反する不相当なものであるということとはできない。

(イ) 外部者及び運用関係者による漏洩の危険性

前記(1)イのとおり、情報管理技術の進展及び個人情報の大量収集・蓄積という社会状況に照らすと、個人情報外部に漏洩すれば、インターネット等を通じ、短時間で、不特定多数の者の間で広範に流通し、その拡散状況を把握することも困難となる可能性が存在する。そして、それらの情報が嫌がらせや犯罪等に使用される危険性も否定できない以上、一旦個人情報外部に漏洩すれば、個人の私生活上の平穏及び人格的自律が害され、その回復も容易でないことが予想される。したがって、外部から住基ネットに侵入することによって、原告らの本人確認情報が現に漏洩することになれば、原告らのプライバシーが侵害されるものとい

うべきである。もつとも、前述のとおり、住基ネットによって通知提供される情報は、4情報、住民票コード及び変更情報（本人確認情報）に限られるところ、これらの情報は、個人の識別情報ないし客観的外形的事項としての性質も有するものであり、本人の私生活やその内心等を直接に表すものではない点において、個人の思想に関する事実や、私生活上の事実とは異なるというべきである。その意味において、本人確認情報と、個人の思想や私生活上の事実等との間で、秘匿の必要性に差が生じることは否定できないところであり、本人確認情報の秘匿の必要性が高いものであるとまではいい難いことも前記(ア)において判示したとおりである。

他方、前記第2の2(3)ア、(6)アのとおり、住基ネットは、市町村、都道府県及び被告センターに設置された各サーバ、国の機関等のコンピュータを専用回線で接続するものである。そして、セキュリティ基準では、住基ネットに関する建物及び重要機能室への侵入防止策を講じること、電気通信回線からのデータの盗取を防止するため、CS、都道府県サーバ、指定情報処理機関サーバ、国の機関のコンピュータは専用回線によって接続されていること、不正アクセス行為から住基ネットを保護するため、CS、都道府県サーバ及び指定情報処理機関サーバ間等、必要な部分には、指定情報処理機関FWを設置し、通信制御を行うこと、通信に際しては相互認証をして、交換するデータの暗号化を実施すること、端末機の取扱いは、管理を行う責任者の指示又は承認を受けた者だけがを行い、操作者が正当な権限を有していることを識別カード及びパスワードによって確認すること、住基ネットの開発、変更、運用、保守等について委託を行う場合には、委託先事業者等の社会的信用と能力を確認し、セキュリティ基準と同様の対策を実施させ、適切な監督を行うこと、住基ネットと既存住基システムとを接続する場合は、既存住基システムに

において、体制の整備、専用回線の使用、住基ネットとの間のFWの設置、電気通信回線等の不共有等、厳重な通信制御の実施等の措置を講ずることが定められている（前記第2の2(6)ア(イ)ないし(エ)参照）。そして、これに基づき、ネットワークには専用回線が使用され、情報も全て暗号化され、既存住基システムとCSとの間、都道府県サーバと既存の庁内LANとの間には、それぞれFWが、CSと都道府県サーバとの間、都道府県サーバと全国サーバとの間、全国サーバと国の機関等との間には、いずれも指定情報処理機関FWが設置され、被告センターが不正通信を24時間監視することとされている（前記第2の2(3)ア参照）。また、「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存住基システムに関する調査票による点検状況」（前記第2の2(6)ウ参照）によれば、市町村のセキュリティ対策に関する自己点検を実施し、一定程度の対策が採られていることも認められる。

以上を総合すると、住基ネットには、外部者の侵入による本人確認情報の漏洩を防止するための、合理的なセキュリティ対策が講じられているというべきである。

原告らは、長野県侵入実験によって、住基ネットのセキュリティの不備が明らかになったと主張する。しかし、前記第2の2(6)エのとおり、長野県侵入実験では、庁舎内あるいは隣接した施設内の端末にコンピュータを接続したうえでの庁内LANへの侵入、公開サーバ及びCSサーバの管理者権限の奪取には成功しているものの、インターネット回線を通じた状態でのFW越しの庁内LANへの侵入及び管理者権限の奪取には失敗し、また、CSと庁内LAN間のFW突破にも失敗している。すなわち、長野県侵入実験において管理者権限を奪取し得たのは、重要機能室に入室して、また、庁舎又は隣接した施設において物理的に端末に接続し、FWの制約を回避した状態という極めて限定された条件のもと

で実施された場合にとどまるのであり、これらの条件が存在していなかった場合にまで、住基ネットへの侵入が可能であることが判明したと認めることはできないというべきである。したがって、長野県侵入実験の結果から、住基ネットのセキュリティに不備があるとは判断することができない。同様に、前記第2の2(6)オの品川区ペネトレーションテストの結果によっても、住基ネットのセキュリティに不備があるとは認められない。

また、運用関係者による漏洩の危険についても、前記第2の2(5)ウのとおり、住基法では、被告センターの職員、被告センターから委託を受けた者、自治体の職員等は、本人確認情報処理事務等に関して知り得た秘密を漏らしてはならないこととされており、これに違反した者は、2年以下の懲役又は100万円以下の罰金が科せられることが定められている。このように、住基ネットの運用関係者には秘密保持義務が課されており、これに反した場合、他の公務員に守秘義務違反があったときよりも重い刑事罰が定められている。さらに、前記第2の2(6)ア(ア)のとおり、セキュリティ基準では、自治体に関して、監査の体制を確立し、住基ネットの企画、開発及び運用の各段階におけるセキュリティ対策の評価を行うこと、住基ネットの運用に必要な職員を配置し、職員に対して、住基ネットの操作及びセキュリティ対策についての教育及び研修を実施するための体制を確立することとされ、証拠（乙共13、41）によれば、市町村では、セキュリティ規定や手引書を作成したり、住基ネットの教育及び研修計画を策定し、セキュリティに関する教育及び研修を行っているところが多いことが認められる。

住基カードも、前記第2の2(3)ク(イ)のとおり、住基カード基準によって、外部から内部情報を読み取られることがないような措置を講じること、住基カードに記録された情報を保護するために、アクセス権限の制

御を行うこと、情報の読み取り又は解析を防止する仕組みを保持すること、基本利用領域、公的個人認証サービス利用領域とそれぞれの条例利用領域は住基カードの内部で独立し、相互に他の領域に記録された情報を読み取ることができない仕組みを保持すること、市町村長その他の市町村の執行機関、都道府県知事その他の都道府県の執行機関又は国の機関等は、法定の事務処理のため必要がある場合を除き、基本利用領域の利用を禁止することとされている。

以上のとおり、運用関係者による漏洩の危険に対しても、これを防止するための様々な措置が講じられているというべきである。

次に、原告らは、斜里町事故、帯広市事故及び瑤町事故から、住基ネットの本人確認情報漏洩の危険性が明らかになったと主張する。

しかしながら、前記第2の2(6)カのとおり、斜里町事故は、職員の自宅の使用パソコンから、Winnnyを通じて、情報がネットワークに流出したというものであり、住基ネットそのもののセキュリティに問題が存在した事実は認められないし、斜里町では、インターネットと接続する情報系LANと、既存住基システム、CSは、接続されていないのであるから、住基ネットが外部から侵入される危険性は存在しない。また、流出した情報には、被告センターから各市町村の担当課長宛に出された通知（平成16年通知）及びパスワードが記載された斜里町作成マニュアル（平成15年マニュアル）が含まれていたところ、平成16年通知は、同年当時のOS上の脆弱性に関する公開情報とその対応策を通知したものであり、既に対応策は完了していたものであるから、現在の住基ネットのセキュリティに影響を及ぼすものではない。平成15年マニュアルについても、同年当時使用されていたパスワードが記載されていたが、現在は当該パスワードは使用されていないし、前記第2の2(6)ア(ウ)のとおり、住基ネットを作動するためには、パスワードを入力するだけ

ではなく、識別カードを所持している必要があり、パスワードのみでは、住基ネットアプリケーションを起動することもできない。したがって、流出した情報は、いずれも住基ネットのセキュリティに影響を及ぼすものではないというべきである。

そして、総務省は、平成18年3月29日付け「住民基本台帳ネットワークシステムのセキュリティ対策について（通知）」と題する文書により、各都道府県担当部長宛てに、住基ネットのセキュリティに関する文書の管理並びにパスワード及び操作者識別カード等の管理について市区町村の関係職員に周知徹底するよう通知しているのであるから、斜里町事故を受けた対策も講じられているものというべきである。したがって、斜里町事故によって、上記の住基ネットのセキュリティに関する判断が左右されるものではない。

また、帯広市事故は、前記第2の2(6)キのとおり、同市の嘱託職員が、本来の職務外で既存住基システムの業務端末を操作し、画面上で閲覧したものであるところ、住基ネットのCSが操作された事実はなく、住基ネットのセキュリティに問題があったものではない。埴町事故は、同クのとおり、同町が、住民票コードの記載された名簿を行政区長会合で配布したというものであるところ、当該名簿は、全て回収されており、住基ネットのセキュリティには直接関係しない。このほか、運用関係者には、秘密保持義務が課され、それが刑罰によって担保されていることは前記のとおりである。

以上のとおりであるから、斜里町事故、帯広市事故及び埴町事故は、いずれも、住基ネットからの情報漏洩の危険に関する判断を左右するものではない。

(ウ) 名寄せの危険

住基法においては、住民票コードによって個人情報を検索、集積する

ことは予定されていないのであるから、名寄せが行われれば、個人情報
が予定された利用範囲を逸脱して開示利用されることになり、当該対象
者のプライバシーに係る利益を侵害することになるというべきである。
そして、住基ネットでは、自治体、被告センター及び国の機関等のコン
ピュータがネットワーク化されており、このネットワークを通じて情報
が通知提供される以上、個人情報の管理主体が、住基法改正前に比べて
格段に増加し、また、個人情報のデータベース化も技術的に容易になっ
たのであるから、行政機関が、本人確認情報及びその他の個人情報を名
寄せすることが、技術的に可能となり、また、容易になったというべき
である。

しかしながら、前記第2の2(2)エ、(3)オ及び(5)のとおり、住基法では、
本人確認情報の利用事務及び通知提供先を法律で制限しており、行政個
人情報保護法でも、行政機関は、特定された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こと、行政機関の長は、法令に
基づく場合を除き、原則として、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ことが定められている。そ
して、行政機関の職員等については、正当な理由がないのに、個人の秘
密に属する事項が記録された個人情報ファイルを提供したときは、2年
以下の懲役又は100万円以下の罰金を科すものとされている。もっと
も、目的外利用の禁止規定には、例外規定も存在しているが、同規定で
は、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が付されている。また、
前記第2の2(6)イのとおり、即時提供方式による本人確認情報の検索の
場合には検索条件が限定され、住基カードについても、前記のとおり、
住基カード基準によって、基本利用領域、公的個人認証サービス利用領
域とそれぞれの条例利用領域が住基カードの内部で独立し、相互に他の

領域に記録された情報を読み取ることができない仕組みを保持することとされている。このように、目的外利用の禁止、これを担保する刑事罰、住民票コードによる本人確認情報検索の制限など、名寄せに対する措置が講じられている。

これらの点を総合すると、名寄せの危険についても、実効性のある防止措置が講じられていると評価することができるというべきである。

なお、原告らは、目的外利用の禁止措置について、提供先や利用事務が、法律の改正によっていくらかでも拡大し得るため、実効性がないと主張している。しかし、法改正により、本人確認情報の提供先、利用事務が変更される場合、国民の代表機関である国会において、討議がされ、議決されることが前提となるのであり、提供先等が無制限に拡大することが予定されるものではないというべきである。したがって、法律の改正による提供先及び利用目的の変更が許容されていることが、目的外利用の禁止の実効性を妨げるということとはできない。

(エ) その他の危険

原告らは、住民票コードが民間企業によって利用される危険性があり、これによるプライバシー侵害の危険性があると主張する。

しかしながら、前記第2の2(5)キのとおり、自治体の機関、被告センター又は国の機関等以外の者が、住民票コードを告知するよう要求することは禁止されており、業務に関して告知を要求し、また、データベース化した場合、都道府県知事の中止勧告及び命令にも従わなければ刑事罰が科されるなどの措置が講じられているのであり、実効性のある防止措置が講じられているというべきである。

エ(ア) 前記イ及びウで認定判断した事情を総合すると、住基ネットは、住民の利便の増進ないし行政の合理化、電子政府構想の実現という制度目的を有しており、これらは、原告らとの間においても合理性を有するもの

であるし、この目的を達成するための住基ネットの必要性も肯定することができるというべきである。そして、住基ネットによる本人確認情報の通知利用の態様は不相当なものであるということとはできず、情報漏洩や名寄せの危険性についても、前記のような防止措置が採られており、その侵害の危険性の内容及び程度は一般的に許容される限度を超えない範囲のものというべきである。以上のような、住基ネットの制度目的、制度の必要性、プライバシー侵害が行われた場合の侵害の程度、プライバシー侵害の危険の防止措置を合わせ考慮すれば、住基法自体が憲法に違反するものと認めることはできないし、住基法に基づく住基ネットの運用によるプライバシー侵害の危険性は、公共の福祉によって許容される範囲のものと判断するのが相当である。

なお、情報技術社会の発展過程においては、何らかのリスクが発生すること自体はやむを得ないものというべきところ、そのリスクを踏まえたうえで、健全な発展を実現していくためには、リスクを最小限に押さえるための合理的な措置を講じることが極めて重要である。そして、前記認定判断のとおり、住基ネットの運用に際しては、外部からの侵入や運用関係者による情報漏洩の危険、名寄せの危険等といったプライバシー侵害の危険性が皆無とまではいうことができない以上、今後も、厳重な漏洩等防止措置を講ずることが期待されるところである。

(イ) 原告らは、住基ネットの運用そのものの差止めを求めているのではなく、原告らの本人確認情報の提供の差止め及び記録からの削除だけを求めており、原告らの本人確認情報の提供等が差し止められたとしても、住基ネットの運用には何ら支障は生じないのであるから、差止請求が認容されるべきであると主張する。

しかしながら、前記ア(ア)のとおり、原告らの本人確認情報の提供等を差止めた場合、住基ネットによる行政事務と従来事務の併存を認める

ことになり、その分、職員を配置する必要が生じるなど、新たな負担が生じることになるのであるから、住基ネットの運用に支障が生じるというべきであり、結局、全体として、住基ネットの目的である住民の利便の増進及び行政の合理化という目的が達成されないことにつながることになるというべきである。したがって、原告らだけの分に限ってみても、住基ネットの運用を差止めることは相当でない。

(ウ) また、原告らは、所要の措置を講じることなく住基ネットを運用していることが、原告らのプライバシーを侵害し、あるいは、侵害の危険性を高めており、このような場合は直ちに差止請求が認められるべきであると主張する。前記のとおり、差止請求の許否の判断においては、口頭弁論終結時まで生じた事由を考慮することが許されるのであるから、所要の措置の有無を判断するに当たっても、改正法施行前の事由のみならず、口頭弁論終結時までの事由を考慮して判断すべきである。そして、証拠（乙共96ないし98）によれば、改正法成立の際、求められていた所要の措置とは、政府に対し、プライバシー保護の観点から、民間部門をも含めた個人情報保護に関する法整備を推進する義務を課したものであり、具体的には、①民間部門をも対象とした個人情報保護に関する法整備を含めたシステムを速やかに整えること、②①のシステムの整備状況を踏まえ、住基法における更なる個人情報保護措置を講ずるため、所要の法改正等を図ること、③地方公共団体が適切に住基ネットを運用できるよう、自治省として個人情報保護に係る指導を十分に行うことが想定されていたものと認められ、さらに、証拠（乙共1、13、41）によれば、政府が、平成13年3月27日、個人情報保護法案を国会に提出し、平成15年5月30日、個人情報保護法が成立したこと、平成14年6月10日付け及び平成15年5月27日付けでセキュリティ基準が制定されていること、平成15年及び平成16年、市町村を対象に、

セキュリティに関する調査が行われ、平成15年8月8日付け及び平成16年12月1日付けの「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存住基システムに関する調査票による点検状況」が公表されていること、平成17年4月1日に行政個人情報保護法が施行されたことからすると、所要の措置も講じられたというべきである。

したがって、所要の措置を講じることなく住基ネットを運用しているとの原告らの主張は採用することができない。

- (エ) 以上によれば、住基ネット運用による原告らのプライバシー侵害の危険性は、公共の福祉による制限として許容されるというべきであるから、プライバシー権に基づく本件差止請求は理由がない。

2 争点(2) (氏名権侵害に基づく差止請求の当否) について

原告らは、氏名は、社会的にみれば、個人を他人から識別して特定する機能を有するものであるが、その個人からみれば、個人として尊重される基礎であり、その個人の人格の象徴であって、人格権の一内容(氏名権)を構成するものというべきである旨主張する。

しかしながら、仮に原告らが主張する氏名権が人格権の一内容を構成するものであるとしても、住民票コードは、住基ネットにおける個人情報の整理及び保管の便宜のために付された番号であるところ、住基ネットのように多人数の個人情報を管理する場合、氏名だけでは個人の特定が不十分であることから、技術的な観点から採用されている方法にすぎず、また、住民票コードは、氏名を含む本人確認情報と一体として利用が予定されているものであるうえ、住民票コードを付されたからといって、行政機関等が原告らに対する呼称として、氏名を使用しなくなるというものでもないことは明らかというべきである。

したがって、原告らに対して住民票コードの番号を付して、住基ネットを運用することが、原告らを氏名ではなく番号で取り扱うことになるとの原告らの主張を採用することはできず、原告らに住民票コードの番号を付すことが原告

ら主張の氏名権の侵害に当たると認めることもできない。

3 争点(3) (「行政によって包括的に管理されない自由」の侵害に基づく差止請求の当否) について

原告らは、住基ネットが、原告らの「行政によって包括的に管理されない自由」を侵害していると主張する。原告らが主張する「行政によって包括的に管理されない自由」が、人格権の一つとして法的保護の対象となるものであるか否かは必ずしも明確ではないが、仮に、法的保護の対象となるとしても、住基ネットの目的が、住民の利便の増進ないし行政の合理化、電子政府構想の実現にあり、これらが合理性を有すること、また、その目的達成のために、住基ネットを運用する必要性が存在することは、前記1(3)で検討したとおりである。原告らは、住基ネットにより原告らの個人情報の名寄せが可能になり、情報の集約化が進むことになるので、「行政によって包括的に管理されない自由」が侵害されることになる旨主張するが、住基ネットは、個人情報の包括的な管理を目的とするものではなく、また、そのような包括的な管理を行う一元的な行政主体も存在せず、原告らが危惧するように、本人確認情報をもとに、原告らの個人情報名寄せされ行政主体により包括的に管理される危険性があるとまではいうことができない。したがって、いずれにしても、住基ネットによる原告らの本人確認情報の利用は、原告らが主張する「行政によって包括的に管理されない自由」の侵害に当たるものと認めることもできない。

4 争点(4) (損害賠償請求責任の成否) について

(1) 被告国の責任

ア 原告らは、内閣が、改正法が憲法に違反しているにもかかわらず、①所要の措置を講ずることなく、改正法を施行する政令を定めたこと、②施行日までに、改正法の施行・運用の開始を停止する等の措置を講じなかったこと、③改正法を施行したこと、④内閣総理大臣及び総務大臣が、施行後、住基法を廃止もしくは運用を停止する等の相当の方策を講ずることなく、

住基法の施行運用を積極的に推進したことにより、原告らの自己情報コントロール権、氏名権及び「行政によって包括的に管理されない自由」（一括して、以下「プライバシー権等」という。）が侵害され、今後も侵害の危険にさらされているから、被告国は国賠法1条1項の損害賠償責任を負う旨主張する。

ところで、国賠法1条1項は、国又は公共団体の公権力の行使に当たる公務員が個別の国民に対して負担する職務上の法的義務に違背して当該国民に損害を与えたときに、国又は公共団体が、賠償する責任を負うことを規定するものである。そして、内閣の立法に関する行為が、国賠法1条1項所定の違法なものとされるのは、内閣の立法過程における関与が、国民に対する職務上の義務に違背したものであることを要件とすると解するのが相当である。そして、国会を、唯一の立法機関としている憲法41条の趣旨に鑑みれば、法律案に関する立法行為について、第一次的に責任を負うのは国会であるから、内閣の立法過程における関与については、原則として、政治的責任を負うにとどまり、個別の国民の権利に対応した関係での法的義務を負うものではないというべきである。

しかも、本件においては、既に前記1ないし3において認定判断したとおり、住基ネットの制度目的の合理性、制度の必要性及びプライバシー権等の侵害の危険性の内容ないし程度を総合勘案すれば、住基法及びこれに基づく住基ネットの運用には違憲、違法が認められないというべきである。

したがって、その余の点について判断するまでもなく、この点に関する原告らの主張は理由がない。

(2) 被告県らの責任

原告らは、被告県ら及び本件知事らが、①本件市区町長らに対し住民票コードを指定して通知し、②本人確認情報を磁気ディスクに記録して保存し、③国の機関等へ情報を提供し、④被告センターに対し、住民票コードの指定

及び通知、並びに国の機関等への本人確認情報の提供等の本人確認情報処理事務を委任し、⑤被告センターへ本人確認情報を通知する等の事務を実施し、その結果、原告らのプライバシー権等を侵害しているから、被告県らは国賠法1条1項の損害賠償責任を負う旨主張する。

前記第2の2(3)のとおり、上記①ないし⑤は、いずれも、都道府県知事が行うものであるから、原告らが主張する被告県らの行為は、本件知事らの行為を指すものと解される。しかしながら、前記(1)のとおり、住基法及びそれに基づく住基ネットの運用に違憲、違法が認められない以上、本件知事らの①ないし⑤の各行為は、いずれも法に基づくものであり、本件知事らの職務上の法的義務に違背していたということとはできない。

したがって、その余の点について判断するまでもなく、原告らの主張は理由がない。

(3) 被告センターの責任

被告センターは、住基法に基づいて、総務大臣から指定情報処理機関としての指定を受け、各都県知事から委託された事務等を行ったものである。そして、前記(1)のとおり、住基法及びこれに基づく住基ネットの運用に違憲、違法は認められないから、被告センターの行為も原告らのプライバシー権等を侵害するものということとはできない。

したがって、被告センターが、不法行為責任を負う余地もない。

5 結論

以上によれば、原告らの第1事件ないし第10事件の各請求はいずれも理由がないから、これらをすべて棄却することとする。

よって、主文のとおり、判決する。

裁判長裁判官 菅 野 雅 之

裁判官 杉 山 順 一

裁判官 岡 本 典 子

番号	氏名	金額	慰謝料額	訴状送達の日 の翌日 (被告県ら)	訴状送達の日 の翌日 (被告センター)	訴状送達の日 の翌日 (被告国)
40	■■■■■	11万円	10万円	平成15年5月17日	平成15年5月17日	平成15年5月17日
41	■■■■■	11万円	10万円	平成15年5月17日	平成15年5月17日	平成15年5月17日
42	■■■■■	11万円	10万円	平成15年5月17日	平成15年5月17日	平成15年5月17日
43	■■■■■	11万円	10万円	平成15年5月17日	平成15年5月17日	平成15年5月17日
44	■■■■■	11万円	10万円	平成15年5月17日	平成15年5月17日	平成15年5月17日
45	■■■■■	11万円	10万円	平成15年5月17日	平成15年5月17日	平成15年5月17日
46	■■■■■	11万円	10万円	平成15年8月29日	平成15年8月29日	平成15年8月29日
47	■■■■■	11万円	10万円	平成15年8月29日	平成15年8月29日	平成15年8月29日
48	■■■■■	11万円	10万円	平成15年8月29日	平成15年8月29日	平成15年8月29日
49	■■■■■	11万円	10万円	(被告となっていない)	平成15年8月29日	平成15年8月29日
50	■■■■■	11万円	10万円	平成15年8月29日	平成15年8月29日	平成15年8月29日

用語一覧表

番号	用語	意味
1	既存住基システム	各市町村に設置され、居住する住民の住民票を記録、管理するサーバ。
2	コミュニケーションサーバ (CS)	各市町村に設置され、既存住基サーバから連携された各市町村の住民の本人確認情報を記録、管理するサーバ。
3	都道府県サーバ	各都道府県に設置され、管下の全市町村のCSから送信された本人確認情報を記録、管理するサーバ。
4	全国サーバ	指定情報処理機関に設置され、全都道府県の都道府県サーバから送信された本人確認情報を記録、管理するサーバ。
5	コールセンター	市町村及び都道府県からの住基ネットの障害連絡や問い合わせを一元的に受け付け対応する機関。
6	専用回線	接続先が固定されており、所定の伝送速度が保証されている回線。
7	ファイアウォール (FW)	組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム。 機能的には、組織内外からの通信要求をすべて捕捉し、定められたルールに従って通過させたり禁止したりすることによって、必要なサービスだけをユーザーに提供しつつ、セキュリティを確保する。
8	住基ネットアプリケーション	CS、都道府県サーバ、全国サーバで稼働する住基ネットの業務を行うためのアプリケーションソフト。市町村ごとに独自に導入されている既存住基システムのアプリケーションと異なり、指定情報処理機関において全国統一の仕様で開発し、配付している。 【アプリケーションソフト】 文書の作成、数値計算等、ある特定の目的のために設計されたソフトウェア。「応用ソフト」とも呼ばれ、どのソフトウェアにも共通する基本的な機能をまとめたOS(基本ソフト)に、ユーザが必要とするものを組み込んで利用する。
9	アクセス	1) ネットワーク越しに他のコンピュータと接続すること。ネットワークケーブルなどで物理的に接続するという意味ではなく、一定の手続(プロトコル)を使用して、コンピュータ間でデータの転送ができる状態にすることをいう。 2) ハードディスク等の記憶装置に対してデータの書き込みや読み出しを行なうこと。

番号	用語	意味
10	重要機能室	電子計算機室(電子計算機及び電子通信関係装置を設置する室)、磁気ディスク等保管室、受電設備、定電圧・定周波電源装置等の設備を設置する室。
11	相互認証	接続する相手が正しいかどうかの確認を相互に行うこと。認証し合う双方が互いに、共通の秘密鍵を知っていることを確認することで、相手を認証する等の方法がある。
12	管理者権限	管理者権限とは、マシンの全機能を利用／管理することができる管理者用アカウントとその権限をいう。Windows 2000/XPではAdministrator権限、UNIXではroot権限を指す。
13	CS端末	CSが提供する機能(広域交付等)やデータ(本人確認情報等)を利用する端末。

番号	用語	意味
14	公開サーバ	誰でも接続することが可能な、インターネット一般に公開したサーバをいう。メールサーバ、WWWサーバやFTPサーバ等を指す。
15	HUB	機器をLANに接続するために使われる集線装置。各機器に接続されたケーブルはいったんHUBに接続され、HUBを介して相互に通信する。
16	LAN	Local Area Networkの略。「構内通信網」のこと。 より対線(ついせん)や同軸ケーブル、光ファイバーなどを使って、同じ建物の中にあるコンピュータやプリンタなどを接続し、データをやり取りするネットワーク。〔「より対線(ついせん)」「ツイストペアケーブル Twisted Pair Cable)とは、導線を2本ずつ対にしてより合わせたケーブルのこと。10BASE-Tや100BASE-TXのようなLANケーブル、USBケーブル、一部のモジュラーケーブルなどがツイストペアケーブルとなっている。より対線は、導線をより合わせていない並行型のもの比べると、外部からのノイズの影響を受けにくい構造になっており、安価で取り扱いが容易なことから広く普及している。〕
17	ポート	インターネット上の通信において、複数の相手と同時に接続を行なうためにIPアドレスの下に設けられたサブ(補助)アドレス。TCP/IP(インターネットで標準的に使われる通信プロトコル)で通信を行うコンピュータはネットワーク内での住所にあたるIPアドレスを持っているが、複数のコンピュータと同時に通信するために、補助アドレスとして複数のポートを持っている。ポートの指定には0から65535までの数字が使われるため、「ポート番号」とも呼ばれる。

番号	用語	意味
18	ダイヤルアップ接続	電話回線やISDN回線などの公衆回線を通じてインターネットや社内LANに接続すること。
19	セグメント	ブリッジ、ルータあるいはスイッチ(いずれもネットワーク上を流れるデータを中継する機器。)によって境界付けられたネットワークのセクション。LANの構成単位になる。 【CSセグメント】 市町村設置FWと指定情報処理機関監視FWの間に位置し、CSが設置されるセグメント。
20	パッチ	一旦完成したプログラムの一部を修正すること。また、修正を行なうために変更点(差分情報)のみを抜き出して列挙したファイル。「パッチファイル」、「差分ファイル」などとも呼ばれる。パッチを使って修正することを「パッチを当てる」と言う。
21	無線LAN	有線ケーブルを使わず、電波や光等による無線通信でデータの送受信をするLANのこと。

番号	用語	意味
22	DMZ	<p>DeMilitarized Zoneの略。</p> <p>インターネットに接続されたネットワークにおいて、FWIによって外部ネットワーク(インターネット)からも内部ネットワーク(組織内のネットワーク)からも隔離された区域のこと。外部に公開するサーバをここに置いておけば、FWIによって外部からの不正なアクセスを排除でき、また万が一公開サーバが乗っ取られた場合でも、内部ネットワークにまで被害が及ぶことはない。</p>
23	バッファオーバーフロー	<p>様々なアプリケーションソフトに共通する代表的なセキュリティホールの一つ。</p> <p>プログラムが確保したメモリサイズ(記憶容量のサイズ)を超えて文字列が入力された場合に、領域(バッファ)があふれて直後にある他の目的で確保された領域の一部または全部が上書き(データとしては意図しない内容に破壊)され、プログラムが意図しない動作をすることを指す。</p> <p>通常、想定外のサイズのデータに対しては、事前にチェックしてエラー処理を行うのが一般的だが、バッファオーバーフローのことを考慮していないプログラムでは、渡されたデータをそのまま全てバッファに書き込もうとして、オーバーフローを引き起こすことになる。</p>
24	セキュリティホール	<p>ソフトウェアの設計ミスやプログラムのバグ等によって生じた、システムのセキュリティ上の弱点を指す。セキュリティホールを放置しておくと、悪意のあるユーザに不正にコンピュータを操作されてしまう可能性がある。攻撃を受けると、外部のユーザが本来実行できない操作が可能になるため、情報の改ざんや漏洩等が行われてしまう可能性がある。</p>
25	リスクアセスメント	<p>資産に対する脅威と脆弱性を特定し、発生頻度などのデータに基づいてどれだけの影響があるかを評価すること。</p>
26	セキュリティポリシー	<p>ネットワークの開発・運用面等において守るべき基準を定めた規定。</p>

番号	用語	意味
27	公開鍵暗号方式	<p>対になる2つの鍵を使ってデータの暗号化・復号化を行なう暗号方式。非対称暗号とも呼ばれる。片方は他人に広く公開するため公開鍵と呼ばれ、もう片方は本人だけが分かるように厳重に管理されるため秘密鍵と呼ばれる。秘密鍵で暗号化されたデータは対応する公開鍵でしか復号できず、公開鍵で暗号化されたデータは対応する秘密鍵でしか復号できない。暗号化と復号化を同じ鍵で行なう秘密鍵暗号方式に比べ、鍵を安全な経路で輸送する必要がないため、鍵の管理が楽で安全性が高い。</p>
28	通信プロトコル	<p>ネットワークを介してコンピュータ同士が通信を行なう上で、相互に決められた約束事の集合。</p>
29	コンピュータウイルス	<p>第三者のプログラムやデータに対して意図的に何らかの被害を及ぼすように作られたプログラムの一種。このようなプログラムはコンピュータ上での存在方法や侵入方法によって、ウイルス、ワーム、トロイの木馬等に分類される。</p>
30	OS	<p>Operating System(オペレーティングシステム)の略。 キーボード入力や画面出力といった入出力機能やディスクやメモリの管理など、多くのアプリケーションソフトにより共通して利用される基本的な機能を提供し、コンピュータシステム全体を管理するソフトウェア。</p>
31	ログ	<p>コンピュータの利用状況やデータ通信の記録を取る。また、その記録。操作やデータの送受信が行われた日時と、行われた操作の内容や送受信されたデータの中身などが記録される。 【アクセスログ】 住基ネットにおいては、住基ネットアプリケーションの操作によるログを「アクセスログ」と定義している。</p>