

平成17年5月30日判決言渡

平成14年(ワ)第836号 住民基本台帳ネットワーク差止等請求事件(以下「甲事件」という。)

平成15年(ワ)第114号 住民基本台帳ネットワーク差止等請求事件(以下「乙事件」という。)

判決

(以下、甲事件原告ら及び乙事件原告らを「原告ら」、甲事件及び乙事件被告石川県を「被告県」、甲事件及び乙事件被告地方自治情報処理センターを「被告地自センター」、甲事件及び乙事件被告国を「被告国」という。)

主文

- 1 被告県は、
 - (1) 住民基本台帳法第30条の7第3項の別表第一の上欄に掲げる国の機関および法人に対し、原告らに関する本人確認情報(原告らの氏名、住所、生年月日、性別の4情報および原告らに付された住民票コード並びにこれらの変更情報)を提供してはならない。
 - (2) 被告地自センターに対し、原告らに関する住民基本台帳法第30条の10第1項記載の本人確認情報処理事務を委任してはならない。
 - (3) 被告地自センターに対し、原告らに関する上記本人確認情報を通知してはならない。
 - (4) 原告らに関する上記本人確認情報を、保存する住民基本台帳ネットワークの磁気ディスク(これに準ずる方法により一定の事項を確実に記録しておくことができるものを含む。以下同じ)から削除せよ。
- 2 被告地自センターは、
 - (1) 被告県から受任した原告らに関する住民基本台帳法第30条の10第1項記載の本人確認情報処理事務を行ってはならない。
 - (2) 原告らに関する上記本人確認情報を、保存する住民基本台帳ネットワークの磁気ディスクから削除せよ。
- 3 原告らの被告国に対する各請求並びに被告県及び被告地自センターに対するその余の各請求をいずれも棄却する。
- 4 訴訟費用は、甲事件、乙事件を通じ、原告らに生じた費用は、これを2分し、その1を被告県及び同地自センターの負担とし、その余を原告らの負担とし、被告県に生じた費用は、これを3分し、その2を被告県の負担とし、その余を原告らの負担とし、被告地自センターに生じた費用は、これを3分し、その2を被告地自センターの負担とし、その余を原告らの負担とし、被告国に生じた費用は、原告らの負担とする。

事実及び理由

第1 原告らの請求

1(甲事件)

- (1) 主文1項(1)ないし(4)、2項(1)、(2)同旨(ただし、「原告ら」とあるのを「甲事件原告ら」と読み替える。)
- (2) 被告県、被告地自センターは、連帯して各甲事件原告らに対し、各金11万円及びこれらに対する平成15年1月17日から支払い済みまで年5分の割合による金員を支払え。
- (3) 被告国は、各甲事件原告らに対し、各金11万円及びこれらに対する平成15年1月17日から支払い済みまで年5分の割合による金員を支払え。

2(乙事件)

- (1) 主文1項(1)ないし(4)、2項(1)、(2)同旨(ただし、「原告ら」とあるのを「乙事件原告ら」と読み替える。)
- (2) 被告県、被告地自センターは、連帯して各乙事件原告らに対し、各金11万円及びこれらに対する平成15年4月1日から支払い済みまで年5分の割合による金員を支払え。
- (3) 被告国は、各乙事件原告らに対し、各金11万円及びこれらに対する平成15年4月1日から支払い済みまで年5分の割合による金員を支払え。

第2 事案の概要

- 1 本件は、石川県内に在住する原告らが、いわゆる住民基本台帳ネットワークシステム(以下「住基ネット」という。)を導入した平成11年の住民基本台帳法の改正法は憲法に違反しており、これによって、原告らのプライバシーが現に侵害され、あるいは侵害される危険に晒されており、また、原告ら一人一人が住民票コードを付さ

れ、番号で扱われることによって原告らの氏名権が侵害され、かつ、住民票コードのもとに個人の情報が包括的に集約、管理されることによって、原告らの「行政権力によって包括的に管理されない自由」が侵害されているとして、住基ネットを運用している被告県及び同地自センターに対し、原告らの個人情報について住基ネットの運用の差止め及び上記権利侵害によって被った精神的損害の賠償を求めるとともに、被告国に対し、内閣総理大臣小泉純一郎は、国民のプライバシー権保護のための所要の措置が講じられるまで住基ネットの稼働を開始しない法的義務があったのに、これに違反して住基ネットの稼働を強行し、原告らに精神的苦痛を与えたとして、その賠償を求めた事案である。

2 前提事実(争いがないか、証拠[各項末尾記載]及び弁論の全趣旨により明らかに認められる)

(1) 当事者等

ア 原告らは、石川県内に居住し、石川県内の金沢市ほかの市町村に住民登録をしている住民である。(甲1ないし28)

イ 被告地自センターは、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、住民基本台帳法30条の10第1項の「指定情報処理機関」に指定され、都道府県知事の委任を受けて、同項記載の「本人確認情報処理事務」を行っている。

(2) 住民基本台帳法の改正

ア 平成11年8月18日、平成11年法律第133号住民基本台帳法の一部を改正する法律(以下「改正法」といい、同法による改正後の住民基本台帳法を「住基法」という。)が公布された。改正法は、附則1条柱書により、公布の日から起算して1年を超えない範囲内において政令で定める日から施行されるものと定められた同条2号に掲げられた各規定(概ね住基ネットの稼働とは直接の関係のない規定である)、公布の日から起算して5年を超えない範囲内において政令で定める日から施行されるものと定められた同条3号に掲げられた規定(後述の、住民票の写しの広域交付(住基法12条の2)、転出転入特例(住基法24条の2)、住民基本台帳カード(住基法30条の44)等に関する規定)を除いて、公布の日から起算して3年を超えない範囲内において政令で定める日から施行するとされた。そして、平成13年12月政令430号により、附則1条柱書の施行日が平成14年8月5日と、平成11年9月政令302号により附則1条2号の施行日が平成11年10月1日と、平成15年1月政令20号により附則1条3号の施行日が平成15年8月25日とそれぞれ定められ、いずれも各施行日から施行された(以下、平成14年8月5日の施行を住基ネットの「第一次稼働」と、平成15年8月25日の施行を住基ネットの「第二次稼働」という。)

イ 改正法附則1条2項には、「この法律の施行に当たっては、政府は、個人情報の保護に万全を期するため、速やかに、所要の措置を講ずるものとする。」との規定がもうけられた。

(3) 住基ネットの仕組みについて

ア 概要

住民基本台帳は、市町村の住民に関する記録を正確かつ統一的行うことにより、市町村における住民の居住関係の公証、選挙人名簿の登録その他住民に関する種々の事務の基礎となる公簿である(住基法1条)。住基ネットは、地方公共団体の共同のシステムとして、住民基本台帳のネットワーク化を図り、後記の本人確認情報を各地方公共団体が共有することにより、全国的に特定の個人情報の確認ができる仕組みを構築し、市町村の区域を越えて住民基本台帳に関する事務処理を行おうとするものである。

イ 住民票コードについて

住民票コードとは、全国を通じて重複しない番号、記号その他の符号であって、無作為に作成された10けたの数字及び1けたの検査数字からなり(住民基本台帳法施行規則[平成11年自治省令第35号。以下「施行規則」という。]第1条)、改正法によって住民票の記載事項とされたものである(住基法7条13号)。

都道府県知事は、他の都道府県知事と協議し、重複しないように調整した上、区域内の市町村長に対し、当該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を指定して通知し(住基法30条の7第1項、2項)、市町村長が都

道府県知事から指定された住民票コードのうちからいずれかの住民票コードを記載し、これを当該住民に対し書面により通知する(住基法30条の2第2項、3項)。なお、都道府県知事が行う上記協議、調整、指定及び通知は、指定情報処理機関に行わせることができるものとされ(住基法30条の10第1項1号、2号)、現実には、指定情報処理機関に指定された被告地自センターが行っている。

住民基本台帳に記載されている者は、理由の如何を問わず、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、その者に係る住民票に記載されている住民票コードの記載の変更を請求することができる(住基法30条の3第1項)。

住民票コードは、一般人の住民基本台帳の一部の写しの閲覧の対象から除外されており(住基法11条1項)、また一般人が住民票の写しの交付を請求した際には、自己又は自己と同一の世帯に属する者に係る場合のほかは、交付される住民票の写しの記載事項から省略されている(住基法12条2項)。

ウ 本人確認情報

本人確認情報とは、住民票に記載されている事項のうち、氏名、出生の年月日、男女の別、住所(以下、これらを「4情報」という。)及び住民票コード並びに住民票の記載等に関する事項で政令で定めるものをいう(住基法30条の5第1項)。上記の政令で定める事項として、現在、①住民票の記載、削除を行った場合は記載、削除を行った旨並びに記載、削除の事由、その事由が生じた年月日、②氏名、出生の年月日、男女の別、住所の全部又は一部について記載の修正を行った場合は、記載の修正を行った旨並びに記載の修正の事由及びその事由が生じた年月日、③住民票コードについて記載の修正を行った場合は、記載の修正を行った旨、記載の修正を行った事由及びその事由が生じた年月日並びに修正前の住民票コードが定められている(住民基本台帳法施行令[昭和42年政令第292号。以下「施行令」という。]30条の5)(以下、上記の政令で定められた事項を「変更情報」という。)

エ 本人確認情報の通知及び保存等

(ア) 市町村は、電子計算機を設置して、これに、市町村の既存の住民基本台帳システムと連携した各住民の本人確認情報を保存し、市町村長は、住民票の記載、削除又は4情報及び住民票コードの全部若しくは一部について記載の修正を行った場合には、当該住民票の記載に係る本人確認情報を、市町村長の使用に係る電子計算機から電気通信回線を通じて都道府県知事の使用に係る電子計算機に送信して通知する(住基法30条の5第1項、第2項)。

(イ) 都道府県知事は電子計算機を設置して、市町村長から通知された本人確認情報を磁気ディスクに記録し、これを通知の日から政令で定める期間(施行令30条の6により原則5年間)保存しなければならない(住基法30条の5第3項)。

(ウ) 都道府県知事は、指定情報処理機関に本人確認情報処理事務(イ記載の指定、通知、協議及び調整事務並びにオの(イ)のaないしd及び(ウ)記載の各提供事務)を行わせることができ(住基法30条の10第1項本文)、その場合、指定情報処理機関に本人確認情報処理事務を行わせることとした都道府県知事(以下「委任都道府県知事」という。)は、住民の本人確認情報を電気通信回線を通じ指定情報処理機関に設置された電子計算機に送信し、指定情報機関は、委任都道府県知事から送信された本人確認情報を磁気ディスクに記録し、政令で定める期間(施行令30条の11により原則5年間)保存する(住基法30条の11第1項ないし3項)。

指定情報処理機関は、毎年少なくとも1回、法30条の10第1項に基づき当該指定情報処理機関が行う法30条の7第3項の規定による国の機関等に対する本人確認情報の提供の状況について、施行規則の定めるところにより、報告書を作成し、これを公表しなければならない(法30条の11第6項、施行規則21条)。

オ 本人確認情報の利用及び提供

(ア) 市町村長は、他の市町村の市町村長その他の執行機関であって条例で定めるものから、条例で定める事務の処理に関し求めがあったときには、条例で定めるところにより、本人確認情報を提供する(住基法30条の6)。

(イ)a 都道府県知事は、住基法別表第一の上欄に掲げる国の機関又は法人か

ら同表の下欄に掲げる事務の処理に関し、住民の居住関係の確認のための求めがあったときに限り、政令で定めるところにより、保存期間に係る本人確認情報を提供する(住基法30条の7第3項)。この場合の提供方法は、施行規則に定めるところにより、都道府県知事の使用に係る電子計算機から、電気通信回線を通じて国の機関等の使用に係る電子計算機に送信する方法か、②施行規則で定めるところにより、都道府県知事から本人確認情報を記録した磁気ディスクを国の機関等に送付する方法によって行う(施行令30条の7)。

- b 都道府県知事は、①当該都道府県の区域内の市町村の執行機関であって住基法別表第二の上欄に掲げるものから同表の下欄に掲げる事務の処理に関し求めがあったとき又は当該都道府県の区域内の市町村の市町村長から住民基本台帳に関する事務の処理に関し求めがあったときには政令で定めるところにより、②当該都道府県の区域内の市町村の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときには条例で定めるところにより、当該都道府県の区域内の市町村の市町村長その他の執行機関に対し、保存期間に係る本人確認情報を提供する(住基法30条の7第4項)。上記①の場合の提供方法は、aの場合と同様、電気通信回線を通じあるいは磁気ディスクを送付する方法によって行う(施行令30条の8)。
 - c 都道府県知事は、①他の都道府県の執行機関であって住基法別表第三の上欄に掲げるものから同表の下欄に掲げる事務の処理に関し求めがあったとき又は他の都道府県の都道府県知事から住基法30条の7第10項に規定する事務の処理に関し求めがあったときには政令で定めるところにより、②他の都道府県の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときには条例で定めるところにより、他の都道府県の都道府県知事その他の執行機関に対し、保存期間に係る本人確認情報を提供する(住基法30条の7第5項)。上記①の場合の提供方法は、aの場合と同様、電気通信回線を通じあるいは磁気ディスクを送付する方法によって行う(施行令30条の9)。
 - d 都道府県知事は、①当該他の都道府県の都道府県知事を経て当該他の都道府県の区域内の市町村の執行機関であって住基法別表第四の上欄に掲げるものから同表の下欄に掲げる事務の処理に関し求めがあったとき又は当該他の都道府県の都道府県知事を経て当該他の都道府県の区域内の市町村の市町村長から住民基本台帳に関する事務の処理に関し求めがあったときには政令で定めるところにより、②当該他の都道府県の都道府県知事を経て当該他の都道府県の区域内の市町村の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときには条例で定めるところにより、他の都道府県の区域内の市町村の市町村長その他の執行機関に対し、保存期間に係る本人確認情報を提供する(住基法30条の7第6項)。上記①の場合の提供方法は、aの場合と同様、電気通信回線を通じあるいは磁気ディスクを送付する方法によって行う(施行令30条の10)。
 - e 都道府県知事は、住基法別表第五に掲げる事務を遂行するとき、条例で定める事務を遂行するとき、本人確認情報の利用につき当該本人確認情報に係る本人が同意した事務を遂行するとき又は統計資料の作成を行うときには、保存期間に係る本人確認情報を利用できる(住基法30条の8第1項)。
 - f 都道府県知事は、都道府県知事以外の当該都道府県の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときは、条例で定めるところにより、保存期間に係る本人確認情報を提供する(住基法30条の8第2項)。
- (ウ) 国の行政機関は、その所掌する事務について必要があるときは、都道府県知事に対し、保存期間に係る本人確認情報に関して資料の提供を求めることができる(法37条2項)。
- (エ) 住基法別表一ないし五に記載されている、本人確認情報の提供がなされる事務は、住基ネットの一次稼働が始まった平成14年8月5日時点では93事務であったが、同年12月6日に成立した「行政手続等における情報通信の技術の利用に関する法律」「行政手続等における情報通信の利用

に関する法律の施行に伴う関係法律の整備等に関する法律」「電子署名に係る地方公共団体の認証業務に関する法律」(以下「行政手続きオンライン化3法」という。)によって、264事務に拡大された。

カ 住民基本台帳カードについて

(ア) 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、自己に係る住民基本台帳カード(以下「住基カード」という。)の交付を求めることができる。住基カードには、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ている(住基法30条の44第1項)。住基カードは住民基本台帳事務に利用される(住基法12条の2、24条の2)ほか、市町村長その他の市町村の執行機関は、住基カードを市町村の条例の定める目的のために利用することができる(法30条の44第8項)。

(イ) 「住民基本台帳カードに関する技術的基準」(平成15年総務省告示第392号、以下「住基カード技術的基準」という。)によると、住基カードは、中央演算処理装置付の半導体集積回路を組み込んだいわゆるICカードであり、暗証番号を設定すること、住民基本台帳ネットワークシステムに係るアプリケーションのためにカードの半導体集積回路上に割り当てられた領域(基本利用領域)と住基法30条の44第8項の条例に規定する目的を実現するためのアプリケーションのためにカードの半導体集積回路上に割り当てられた領域(条例利用領域)がカードの内部でそれぞれ独立し、各システムがそれぞれのアプリケーションのために半導体集積回路上に割り当てられた領域以外の領域に情報を記録し、又は当該領域に記録された情報を読みとることができない仕組みを保持すること等の様々なセキュリティ対策がとられるとともに、条例利用領域には、特に必要性が認められる場合を除いて条例利用アプリケーションに係るシステムへアクセスするための利用者番号等以外の個人情報記録せず、利用者番号には住民票コードを使用しないこと等が定められている。(乙13)

(4) 各市町村等における電子計算機の接続状況等について(甲39、乙1、1の2、3、乙34)

ア 既存の住民基本台帳事務を処理するコンピュータ及び記憶媒体(以下「既存住基システム」という。)は、その他地方公共団体の行う事務処理に使用するコンピュータとLANによりネットワークを形成している(以下「庁内LAN」という。)。庁内LANはインターネットと接続されていることがあるが、その間には不正な侵入を防ぐファイアウォール(以下「FW」という。)が設置されている(以下「インターネット側FW」という。))。

イ 各市町村には、コミュニケーションサーバ(CS)と呼ばれるコンピュータが設置され、既存住基システムからCSに、記憶媒体を介し、あるいは、庁内LANとCSを接続して電気通信による送信によって、本人確認情報が伝達されてCS内に本人確認情報が保存される。庁内LANとCSが接続されている場合には、その間にFW(以下「市町村設置FW」という。)が設置される。

ウ 全国の各都道府県にコンピュータ(以下「都道府県サーバ」という。)及び全国レベルで1つのコンピュータ(以下「全国サーバ」という。)がそれぞれ設置され、各都道府県サーバ、全国サーバ及び各CSとは専用回線で接続され、各市町村のCSから都道府県サーバに、都道府県サーバから全国サーバに、それぞれ本人確認情報が送信され、保存される。各CSと上記回線の間、都道府県サーバと上記回線の間、都道府県サーバと都道府県の庁内LAN、全国サーバと上記回線の間、全国サーバと国の機関のサーバとの間には、それぞれ指定情報処理機関が監視するFW(以下「指定情報処理機関監視FW」という。)が設置されている。

指定情報処理機関である被告地自センターは、指定情報処理機関監視FWについて24時間の監視を行い、また、各CSについて15分毎に死活状況のみの監視を行っている。

(5) 住民基本台帳事務の拡充

ア 住民票の写しの広域交付

住民基本台帳に記録されている者は、住基カード又は運転免許証等総務省令で定める書類を提示して、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(以下「住所地市町村長」という。)以外の市町村長に対し、自己又は自己と同一の世帯に属する者に係る住民票の写しで、法7条5号、

9号から12号まで及び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(住基法12条の2第1項)。

この請求を受けた市町村長(以下「交付地市町村長」という。)は、住所地市町村長との間で、電気通信回線を通じてそれぞれの設置する電子計算機に必要な事項を送信通知し、住民票の写しの作成、交付を行う(住基法12条の2第2項ないし第5項)。

この場合には、本人確認情報ないし住民票情報は市町村間で送受信され、都道府県サーバを経由しない。(乙28)

イ 転出・転入手続の簡素化について

転出・転入の手続には、転入届の際に転出地での住民票の情報を記載した転出証明書を添付することが必要であり(住基法22条2項、施行令23条)、通常、住民は、転出証明書の交付を受けるため、転出地の市役所・町村役場に出向く必要があるところ、住基カードの交付を受けている者等が、施行令に定める一定の事項が記載された「付記転出届」をした場合には、その者の住基カードを添えて行われる転入手続については、転出証明書の添付を要しない(住基法24条の2第1項)。

この場合においても、本人確認情報ないし転出証明書記載事項は市町村間で送受信され、都道府県サーバを経由しない。(乙28)

(6) 住基ネットにおける本人確認情報に関する保護措置について

ア システム構築主体に係る本人確認情報の保護措置

(ア) 安全確保措置義務

都道府県知事、指定情報処理機関は、通知に係る本人確認情報の電子計算機処理等を行うに当たり、当該本人確認情報の漏えい、滅失及びき損の防止その他の当該本人確認情報の適切な管理の為に必要な措置を講ずる義務があり(住基法30条の29第1項)、また、都道府県知事又は指定情報処理機関から同処理等の委託を受けた者が受託した業務を行う場合、これらの者も同様の措置を講ずる義務がある(同条2項)。

市町村長は、住民基本台帳又は戸籍の附票に関する事務の処理に当たり、住民票又は戸籍の附票に記載されている事項の漏えい、滅失又はき損の防止その他の住民票又は戸籍の附票に記載されている事項の適切な管理のために必要な措置を講じる義務があり(住基法36条の2第1項)、市町村長から同事務の処理の委託を受けた者も同様の義務がある(同条2項)。

(イ) 本人確認情報の利用及び提供に関する義務

都道府県知事は、上記(3)オ(イ)及び(ウ)記載の場合のほか、本人確認情報を利用し、又は提供してはならない義務があり(住基法30条の30第1項)、指定情報処理機関も住基法30条の10第1項の規定により上記(3)オ(イ)及び(ウ)記載の委任都道府県知事の事務を行う場合を除き、本人確認情報を利用し、又は提供してはならない義務がある(住基法30条の30第2項)。

上記義務違反に対する罰則は定められていない。

(ウ) 秘密保持義務

a 指定情報処理機関の役員、職員あるいはこれらの職にあった者及び指定情報処理機関から本人確認情報の電子計算機処理事務等の委託を受けた者若しくはその役員又はこれらの職にあった者には、本人確認情報処理あるいは委託された業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を漏らしてはならないという守秘義務が課せられている(住基法30条の17第1項、第2項)。

b 本人確認情報の電子計算機処理等の事務に従事する市町村の職員又は職員であった者、住基法30条の5第1項の規定による通知に係る本人確認情報の電子計算機処理等の事務に従事する都道府県の職員又は職員であった者及び市町村長又は都道府県知事から住基法30条の5第1項の規定による通知に係る本人確認情報の電子計算機処理等の事務の委託を受けた者若しくはその職員又はこれらの者であった者には、本人確認情報処理あるいは委託された業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を漏らしてはならないという守秘義務が課せられている(住基法30条の

31第1項, 第2項)。

- c 上記義務違反に対しては罰則が定められている(住基法42条)。
- (エ) 本人確認情報に係る住民に関する記録の保護義務
都道府県知事又は指定情報処理機関の委託により住基法30条の5第1項又は住基法30条の11第1項の規定による通知に係る本人確認情報の電子計算機処理等に関する事務に従事する者あるいは従事していた者は、その事務に関して知り得た事項をみだりに他人に知らせ、あるいは不当な目的に使用してはならない義務がある(住基法30条の32)。
上記義務違反に対する罰則は定められていない。
- (オ) 都道府県審議会について
都道府県には、本人確認情報の保護に関する審議会を置き、住基法によりその権限に属させられた事項を調査審議させるとともに、都道府県知事の諮問に応じ、本人確認情報の保護に関する事項の調査審議及び都道府県知事への建議をさせることができる(住基法30条の9)。
- (カ) 指定情報処理機関について
 - a 指定情報処理機関は、住基ネットの適正な運営管理を行うため、委任都道府県知事に対し、本人確認情報の電子計算機処理に関し必要な技術的な助言及び情報の提供を行い(住基法30条の11第7項)、委任都道府県知事の統括する都道府県の区域内の市町村の住民基本台帳に住民に関する正確な記録が行われるよう、委任都道府県知事に対し必要な協力をしなければならない(同条8項)。
 - b 指定情報処理機関には、指定情報処理機関の代表者の諮問に応じ、本人確認情報の保護に関する事項を調査審議し、これに関し必要と認める意見を指定情報処理機関の代表者に述べる事ができる「本人確認情報保護委員会」を置かなければならない(住基法30条の15)。
 - c 指定情報処理機関は、名称又は主たる事務所の所在地を変更しようとするときは総務大臣及び委任都道府県知事にその旨を届け出る(住基法30条の13第2項)とともに、本人確認情報処理事務等の実施に関する事項について本人確認情報管理規程を定め、総務大臣の認可を受ける(住基法30条の18)ほか、事業計画の作成などについて委任都道府県知事の意見を聴き及び総務大臣の認可を受け、事業報告書等を総務大臣及び委任都道府県知事に提出する(住基法30条の19)。また、総務大臣は、指定情報処理機関の役員を選任及び解任の認可をする(住基法30条の16)ほか、総務大臣及び委任都道府県知事は、指定情報処理機関に係る交付金、監督命令、報告及び立入検査、指定の取消しなどの監督権を有する(住基法30条の22ないし25)。
- イ 本人確認情報の受領者に係る本人確認情報の保護措置
 - (ア) 安全確保措置義務
住基法30条の6、30条の7第3項から第6項まで又は30条の8第2項の規定により本人確認情報の提供を受けた市町村長その他の市町村の執行機関若しくは都道府県知事その他の都道府県の執行機関又は住基法別表第一の上欄に掲げる国の機関若しくは法人(以下「受領者」という。)に対して、上記アのシステム構築主体と同様、安全確保措置義務が課せられている(住基法30条の33第1項)。
 - (イ) 本人確認情報の利用に関する義務
本人確認情報の受領者には、当該本人確認情報の提供を求めることができる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利用又は提供をしてはならない義務が定められている(住基法30条の34)。
上記義務違反に対する罰則は定められていない。
 - (ウ) 秘密保持義務
住基法30条の6、30条の7第4項から第6項まで又は30条の8第2項の規定により市町村長その他の市町村の執行機関又は都道府県知事その他の都道府県の執行機関が提供を受けた本人確認情報の電子計算機処理等に関する事務に従事する市町村又は都道府県の職員又は職員であった者、住基法30条の7第3項の規定により住基法別表第一の上欄に掲げる国の機関又は法人が提供を受けた本人確認情報の電子計算機処理等に関する事務に従事する同欄に掲げる国の機関の職員若しくは職員であった者又は同欄に掲げる法人の役員若しくは職員若しくはこれらの職にあつ

た者及び本人確認情報の電子計算機処理等の委託を受けた者若しくはその役員若しくは職員又はこれらの者であった者には、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を漏らしてはならないという守秘義務が課せられている(住基法30条の35)。

上記義務違反に対しては罰則が定められている(住基法42条)。

(エ) 受領した本人確認情報に係る住民に関する記録の保護義務

本人確認情報の受領者の委託を受けて本人確認情報の電子計算機処理等に関する事務に従事している者又は従事していた者は、その事務に関して知り得た事項をみだりに他人に知らせ、又は不当な目的に使用してはならない義務が課せられている(住基法30条の36)。

上記義務違反に対する罰則は定められていない。

ウ 自己の本人確認情報の開示

何人も、都道府県知事又は指定情報処理機関に対し、自己に係る本人確認情報について、書面により開示請求ができ、都道府県知事又は指定情報処理機関は、その請求があったときは、開示請求者に対し、これを開示しなければならない(住基法30条の37)。

都道府県知事又は指定情報処理機関は、上記により開示を受けた者から、書面により、開示に係る本人確認情報についてその内容の全部又は一部の訂正、追加又は削除の申出があったときは、遅滞なく調査を行い、その結果を通知しなければならない(住基法30条の40)。

エ 苦情処理

都道府県知事、指定情報処理機関及び市町村は、住基法が定める事務の実施に関する苦情の適切かつ迅速な処理に努めなければならないとされている(住基法30条の41、36条の3)。

オ 住民票コードの告知要求制限

(ア) 市町村長その他の市町村の執行機関は、住基法に規定する事務又はその処理する事務であって住基法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のため必要がある場合を除き、何人に対しても、当該市町村の住民以外の者に係る住民票に記載された住民票コードを告知することを求めてはならない(住基法30条の42第1項)。

(イ) 都道府県知事その他の都道府県の執行機関は、住基法に規定する事務又はその処理する事務であって住基法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のため必要がある場合を除き、何人に対しても、その者又はその者以外の者に係る住民票に記載された住民票コードを告知することを求めてはならない(住基法30条の42第2項)。

指定情報処理機関及び住基法別表第一の上覧に掲げる国の機関等についても同様の義務が課せられている(住基法30条の42第3項、第4項)。

カ 住民票コードの利用制限

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、指定情報処理機関又は住基法別表第一の上欄に掲げる国の機関若しくは法人以外の者について、住民票コードの利用等に関して次のような規制がなされている。

(ア) 自己と同一の世帯に属する者以外の者(以下「第三者」という。)に対し、当該第三者又は当該第三者以外の者に係る住民票コードを告知することを求めてはならない(住基法30条の43第1項)。

上記義務違反に対する罰則は定められていない。

(イ) その者が業として行う行為に関し、その者に契約の申込みをしようとする第三者若しくは申込みをする第三者又はその者と契約の締結をした第三者に対し、当該第三者又は当該第三者以外の者に係る住民票に記載された住民票コードを告知することを求めてはならない(住基法30条の43第2項)。

(ウ) 業として、住民票コードに記載されたデータベースであって、当該住民票コードの記録されたデータベースに記録された情報が他に提供されることが予定されているものを構成してはならない(住基法30条の43第3項)。

(エ) 都道府県知事は、上記(イ)又は(ウ)に違反する行為が行われた場合において、当該行為をした者が更に反復してこれらに違反する行為をするおそれ

があると認められるときは、当該行為をした者に対し、違反行為の中止等を勧告し、当該中止の勧告に従わないときには、都道府県の審議会の意見を聴いて、その者に対し、期限を定めて、当該勧告に従うべきことを命ずることができる(住基法30条の43第4項、第5項)。

(オ) 都道府県知事は、上記(エ)の措置に関し必要があると認めるときは、その必要と認められる範囲内において、上記(イ)又は(ウ)に違反していると認めらるるに足りる相当の理由がある者に対して、必要な事項に関し報告を求め、又は、立入検査をすることができる(住基法34条の2)。

(カ) 上記(エ)の命令違反及び(オ)の報告懈怠・立入検査拒否に対しては、罰則が定められている(住基法44条、47条)。

(7) 住基ネットの稼働状況

平成14年8月5日、前記のとおり、住基ネットの第一次稼働が始まった。同年7月中には、すべての市区町村から都道府県に本人確認情報の通知がなされていたものの、同年8月5日、個人情報保護や情報漏洩等への対策が不十分であることなどを理由として、東京都杉並区、東京都国分寺市、福島県矢祭町の3自治体が住基ネットへの不参加を表明して住基ネットへの接続を行わず、三重県小俣町及び三重県二見町は同日の施行から数日遅れて接続を開始した。また、神奈川県横浜市は、第一次稼働当初から、住基ネットへの参加を希望しない住民の本人確認情報を通知しないとする選択方式(横浜方式)を採用することとし、市民から「非通知」の申出を受け付けたところ、申し出た市民は約84万人に上った。平成15年4月9日、横浜市、神奈川県及び被告地自センターは、全員参加に至るまでの段階的な対応として、同年6月9日を目処として参加希望者のみの本人確認情報の利用提供が可能になることを目指す旨の合意をした。その後、東京都中野区は同年9月11日に、東京都国立市は同年12月26日に住基ネットから離脱した。

当初、住基ネットへの接続を行わなかった東京都杉並区は、平成15年6月4日、横浜方式を採用することを表明したが、総務省及び東京都は杉並区の方針を認めなかった。平成16年8月24日、杉並区は東京都及び国を相手取り、東京都に、杉並区が送信する住基ネットへの参加を希望する住民の本人確認情報を受領する義務があることの確認を求めるとともに、東京都が受信義務を履行しないこと及び国が東京都に対して受信するよう指導する義務を怠ったことがいずれも違法であるとして、東京都及び国に対し、国家賠償を請求する旨の訴訟を提起した。

平成15年5月23日に個人情報保護法が成立したことを契機に、東京都国分寺市は同月28日、東京都中野区は同年8月13日、それぞれ住基ネットへの接続を表明した。

第二次稼働時点においては、東京都国立市および福島県矢祭市が住基ネットへの接続を行っておらず、東京都杉並区は上記の経緯から不参加の状態となっており、神奈川県横浜市は一部住民の本人確認情報のみが神奈川県に通知されている状況となっている。

また、平成16年7月4日付の毎日新聞には、平成15年8月の二次稼働開始から平成16年3月までの住基カード発行枚数は約25万枚、普及率は0.2パーセントで、総務省が初年度分として見込んだ約300万枚の1割にも達しなかったことが掲載された。

(甲38の1, 2, 甲42, 甲共9の3, 4, 甲共20)

(8) 住基ネットの一次稼働に伴い、

ア 被告県は、

(ア) 原告ら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から原告らの本人確認情報の通知を受けてこれを磁気ディスクに記録し、保存している。

(イ) 被告地自センターに対して、本人確認情報処理事務を委任した。

(ウ) 被告地自センターに対して、原告らの本人確認情報を通知した。

(エ) 住基法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、受任者である被告地自センターをして原告らに関する本人確認情報を提供させたか、求めがあれば提供させる態勢にある。

イ 被告地自センターは、

(ア) 被告県から、本人確認情報処理事務を受任した。

(イ) 被告県から通知を受けた原告らの本人確認情報を磁気ディスクに記録

し、保存している。

(弁論の全趣旨)

第3 争点及びそれに対する当事者の主張

1 当事者の主張の骨子

(1) 原告らの主張の骨子

ア 原告らの住基ネットからの離脱(被告県及び被告地自センターに対する差止め請求)について

(ア) 憲法は、憲法が保障する人格権が侵害される危険性がある場合には、侵害をもたらす者に対する差止め請求権を認めている。

(イ) 被侵害権利

a 住基ネットの運用により、原告らのプライバシーの権利としての自己情報コントロール権が現に侵害されており、更に新たな侵害の危険性が存在する。

b 住基ネットは、原告らの氏名権を侵害している。

c 住基ネットは、原告らの「公権力による包括的管理からの自由」を侵害している。

(ウ) 上記各権利は、憲法13条によって保障されている。原告らは、上記各権利に基づき、原告らの住基ネットからの離脱、すなわち請求の趣旨記載の差止めを求める。

イ 損害賠償請求について

(ア) 被告県の谷本知事は、住基ネットを運用することにより、原告らのプライバシーの権利、氏名権ないし「公権力による包括的管理からの自由」を侵害したもので、国家賠償法上違法である。

(イ) 被告地自センターは、住基ネットを運用することにより、原告らの上記各権利を侵害したもので、民法上の不法行為に該当する。

(ウ) 被告国の小泉内閣総理大臣は、「所要の措置」を講じるまでは改正法の施行を開始しない法的義務があったのに、これに違反し、「所要の措置」を講じないまま改正法を施行し、原告らの上記各権利を侵害したもので、国家賠償法上違法である。

(2) 被告らの主張の骨子

ア 差止め請求について(被告県、被告地自センター)

(ア) 差止め請求が認められるには、差止めができる排他的権利があること、権利侵害の危険性があること、差止めの必要性があることが必要である。

(イ) 自己情報コントロール権は憲法13条で保障される権利とはいえないし、プライバシーの侵害のみを理由として差止め請求権は認められない。住基ネットのセキュリティ対策は十分なものであり、住基ネットによりプライバシー権の侵害の危険性があるとはいえない。

(ウ) 氏名権、「公権力による包括的管理からの自由」についての主張は争う。

イ 損害賠償請求について

(ア) 被告県

谷本知事の行為に何ら違法はない。

(イ) 被告地自センター

被告地自センターの行為に何らの違法はない。

(ウ) 被告国

小泉内閣総理大臣の行為に何ら違法はない。

2 主要な争点

(1) プライバシーの権利は憲法13条によって保障されているか。住基ネットの運用が開始されたことにより、原告らのプライバシーの権利が侵害されたか。あるいはその危険性があるか。

(2) 氏名権及び「公権力による包括的管理からの自由」が憲法13条によって保障されているか。住基ネットの運用が開始されたことにより、原告らの氏名権及び「公権力による包括的な管理からの自由権」が侵害されたか。

(3) 被告県及び同地自センターが住基ネットを運用したことが違法か。

(4) 被告国が改正法を施行したことが違法か。

(5) 損害

3 主要な争点についての当事者の主張

(1) プライバシーの権利は憲法13条によって保障されているか。住基ネットの運用が開始されたことにより、憲法13条によって保障されている原告らのプライバシ

一権が侵害されたか。あるいはその危険性があるか。(争点(1))
(原告らの主張)

ア プライバシー権は憲法上の権利であること

(ア) 社会の変革にとまない、「個人の人格的生存に不可欠な権利自由」として保護するに値すると考えられるようになった権利、いわゆる「新しい人権」は、憲法13条の「幸福追求権」として、憲法上保護される人権の一つと解されてきた。この幸福追求権によって基礎づけられる権利は、裁判上の救済を受けることができる具体的権利であると解すべきである。

プライバシーの権利は、このようにして認められた新しい人権の典型例とされており、判例、学説上も憲法13条の保障する人格権の一つであることは異論がない。そして、プライバシーの権利については、個人的・消極的権利としての性格の強い「ひとりで放っておいてもらう権利」という概念から、より積極的な「自己に関する情報をコントロールする権利」という概念をも認める方向に理解されてきており、少なくとも広義のプライバシーの権利に、その重要な柱の一つとして、自己に関する情報をコントロールする権利が含まれることは明らかである。

すなわち、もともと個人の尊厳の原理から要求されるのは、個人の自律的な社会関係の形成を尊重することであり、公権力からこのような個人の自律領域が保護されなければ、個人の決定や行動に萎縮的効果が生じ、自己決定が阻害されることになる。そして、現代国家における積極国家・行政国家現象の進展に加え、情報化社会の進展、さらにはコンピュータによる情報処理技術の進展は、国家による個人の全面的管理という危険性を増大させるものであり、このような状況下において、立憲主義原理の維持・展開をはかることの重要性を認識し、個人の尊厳を左右するような個人情報に関する公権力の諸活動を憲法上の規律に服させることが意識されるようになったのであって、プライバシーの権利としての自己情報コントロール権は、新しい人権として、憲法13条により保障された人権であるといえる。

(イ) 自己情報コントロール権の内容としては、他人に知られたくないと思う正当性のある自己の情報について、①収集・取得、②保有・利用、③開示・提供を自分でコントロールする権利が認められるべきであり、派生的には、④自己の情報の開示請求権・訂正請求権が認められなければならない。

そして、ここにいう「自己情報」とは、センシティブ性の高低によって個人情報二分し、センシティブ性の高い情報のみが保護の対象となると考えるべきではなく、個人情報全てが保護の対象となると解すべきである。なぜなら、個人情報二分し保護の度合いに強弱を付けることは、区別の基準及びその判断が容易でないし、前述のとおり、自己情報コントロール権が公権力から個人の自律領域を保護しようとするものであり、積極・行政国家化、情報社会化により公権力による個人の全面的管理の危険性が増大していることに鑑みれば、センシティブ性の低さを理由として保護の対象から外すことは妥当でないからである。最高裁判所の判例も、同様の判断を示している(最高裁判所平成15年9月12日判決・判タ1134号98頁、以下「早稲田事件最高裁判決」という。)

また、「公権力」による個人情報の取り扱いが問題となる場面は、私人間における表現の自由・知る権利との相互調整(「思想の自由市場機能」)等が必要とされるような場面ではなく、公権力の活動が事務処理の効率化等といった口実の下に、憲法の保障する基本的人権としてのプライバシーの権利を侵害する場面であるから、一個人の憲法上の人権の保障が十全になされることこそが求められるのであって、かかる公権力による個人情報の取り扱いが問題となる場面においては、あくまでも、情報主体のコントロール(意思決定)権が最大限に保障されなければならないというべきである(早稲田事件最高裁判決参照)。

(ウ) 審査基準について

公権力による個人情報の取り扱いが問題となる場面においては、個人の同意・承諾の有無が基本とされるべきであって、このような同意・承諾が存在しない場合には、その例外の要件(同意・承諾を得ることが不可能・困難であったという緊急性の要件、その場合の手段の相当性)について厳格な判断が求められるというべきである。そして、これら以外の、「個人情報の秘匿性の程度」、「具体的な不利益の不存在」、「公権力による収集等取り

扱いの目的の正当性と必要性」といった要素についてはあくまでも付随的要素として位置づけられるべきである(早稲田事件最高裁判決参照)。

イ 住基ネットにより侵害されあるいは侵害される危険性のある原告らのプライバシーに関わる情報について

- (ア) 住基ネットにおいては、次に述べる情報が取り扱われている。
- a 市町村長から都道府県知事に、都道府県知事から被告地自センターに通知され、それらのサーバ(以下、CS、都道府県サーバ及び全国サーバを合わせて「住基ネットサーバ」ともいう。)に記録・保存される本人確認情報(住基法30条の5、7条)。
 - b 住基ネットサーバには、aのほか、氏名のふりがなが記載され、また、平成15年8月以降、住基カードに関する情報が記録・保存されている。
 - c 以上のほか、平成15年8月以降、住基ネットの電気通信回線上を流れる情報は次のとおりである。
 - (a) 住民票の広域交付の際に必要な住民票記載事項情報として、本人確認情報のほか、世帯主、続柄、従前の住所及び届出年月日
 - (b) 他の市区町村へ転出する際の転出証明書情報として、本人確認情報のほか、世帯主であるかどうか、世帯主の氏名及び世帯主との続柄、戸籍の表示、転出先及び転出の予定年月日、国民健康保険の被保険者である旨、国民年金の種別、国民年金手帳の記号及び番号、児童手当の受給の有無
 - d 以上に加え、現在11省庁264事務に本人確認情報が利用されるため、これらの事務に使用されるサーバには、住民票コードと共にこれらの事務に関する個人情報が記録・保存される。
 - e さらに、住基ネットシステムにおいては、従前市区町村が住民基本台帳を管理していたサーバと住基ネットサーバを接続し、他の市区町村のCSや既存住基台帳サーバ、都道府県のサーバ、被告地自センターのサーバとネットワークシステムを構築しているところ、上記既存住基台帳サーバには、住民基本台帳の全個人情報に記載されている(住基法7条)。

(イ) 上記の内容の情報は、原告らのプライバシーであって、これらのプライバシーが、後述のとおり、住基ネットの運用によって侵害され、あるいは侵害の危険にさらされている。

ウ プライバシー侵害の事実について

(ア) 本人確認情報については、住基ネット運用前は当該本人が所属する市区町村だけが保有しており、そのこと自体は地方自治の理念にもかかなうものであったが、住基ネット運用により、本人確認情報が本人の同意を得ずして当該市区町村から全国に流通させられることにより、原告らは、自己の情報をコントロールすることが不可能となるのであって、住基ネットの運用は、直ちに原告らの自己情報コントロール権を侵害するものである。

さらに、原告らは、住基ネットにより、被告県及び同地自センターに保存された本人確認情報について、日本全国のいかなる機関・法人の、どの事務にどのような情報が提供されたかを知るすべがなく、これは、自己情報コントロール権のうち、自己情報の開示権を侵害するものである。

(イ) 氏名のふりがな、住基カードに関する情報及び本人確認情報の提供を受ける事務に関する個人情報についても、上記本人確認情報と同様、住基ネットの運用により原告らの自己情報コントロール権が現に侵害されている。

(ウ) 被告らは、本人確認情報は「プライバシー外延情報」であり、原則としてプライバシー保護の対象にならない旨主張する。

しかし、住基法の国会審議の際には、政府委員も、本人確認情報のうち4情報も、住民票コードと一体化した場合には全体として秘密事項、すなわちプライバシー事項となると答弁していること、早稲田事件最高裁判決においても同旨の判断がなされていることに加え、4情報とそれらの変更履歴とは不可分一体の形で本人確認情報の内容をなしていると解されるところ、変更履歴は、当該個人の私的な事情ないし出来事の内容を推認させるものであり、まさに他人には秘匿しておきたい情報であって、典型的な「プライバシー固有情報」といえ、強く保護される必要がある。

エ プライバシー侵害の危険性について

(ア) 立証責任について

本件のような国等の行政の施策による国民の権利侵害事案における主

主張立証責任については、民法の一般不法行為や差止め請求における主張立証責任とは別個に考えるべきである。

行政庁の裁量処分取消訴訟等における行政庁の処分の違法性に関する主張立証責任については、主張立証責任の転換を認めた判決が複数存在するところ(最高裁判所平成4年10月29日判決・判時1441号37頁[伊方原発事件]、名古屋高裁金沢支部平成15年1月27日判決・判時1818号3頁[もんじゅ事件]、金沢地裁平成6年8月25日判決・判時1515号3頁[志賀原発差止め訴訟])、これらの裁判例をふまえ、主張立証責任については、被侵害利益の重大性、侵害行為の主体及び態様、証拠への距離等を総合考慮して、当事者間の公平の観点から、場合によって事実上の推定による主張立証責任の転換を図るべきである。

本件においては、被侵害利益はプライバシー権ないし人格権であり現代社会において重要な権利利益であること、侵害行為の主体は公権力であり、思想の自由市場の問題等を考慮する必要がなく権利侵害の有無につき厳格に審査されることが求められる場面であること、侵害の態様は、後述のとおりであって、住基ネットにおいてひとたびプライバシーが侵害された場合に回復不能な被害が生じること、住基ネットのセキュリティ対策についての資料は被告国らにおいて所持していること等を総合考慮すれば、本件における住基ネットによるプライバシー侵害の危険性についての主張立証責任に関しては、原告らにおいてその危険性について一応の主張立証(潜在的な危険の主張立証)をなしたときは、被告らにおいて、これに対して相当の根拠を示して危険性のないことを具体的に主張立証すべきであり、これを被告らが行わない場合には、本件住基ネットはプライバシー侵害の危険があるものと事実上推認されるべきものとするのが妥当である。

(イ) 住基ネットにおける具体的なプライバシー侵害の危険性について

a 住基ネットにおける情報の流通と漏洩の危険について

住基ネットは、従来各市区町村内で収集取得され完結的に管理されてきた住民の個人情報、コンピュータネットワーク上を流通するようになったものであるところ、コンピュータネットワークにおいて流通する情報は、情報の大量蓄積・即時伝達を機能とするコンピュータを使用するシステムの性格上、いったん漏洩すれば、その情報が大量かつ網羅的に流出し、甚大な被害が発生するものであり、また、プライバシーはその性格上、いったん侵害されたらその回復は不可能である。そして、住基ネットにおいては、住民票コードによる名寄せが可能であることから、個人情報の大量、包括的な入手集積がなされる危険性が飛躍的に高まっている。

b 想定される危険

(a) 外部からのネットワーク侵入の危険性

住基ネットは、ハッカー等によって、セキュリティの最も弱い部分から侵入され、原告らの個人情報が流出・漏洩し、悪用・改ざんされるなどプライバシー権を侵害される危険がある。

(b) 運用関係者等による漏洩等の危険

住基ネットの運用に関わる職員の不正行為、警察官らによる職権濫用による個人情報の収集のための住基ネットの利用、個人情報提供先である国の機関・法人における個人情報の目的外利用、自治体が住基ネットシステムの開発・管理を委託した民間委託業者の不正行為、バックアップ用磁気テープその他のバックアップデータの盗難等、個人情報が漏洩する危険性が存在している。

c セキュリティ対策の不備

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が侵害される危険が常に存在するところ、このような危険を防止するためのセキュリティが、ハード面、ソフト面の両方において、到底十分に講じられているということはできない。

(a) ハード面のセキュリティ対策の不整備

本件住基ネットの安全対策としては、①専用回線、②FW、③IDS(侵入検知装置)が挙げられているが、それらの実効性は疑わしい。

(b) ソフト面のセキュリティ対策の不整備

運用関係者等による漏洩等の危険防止につき、「セキュリティポリシー」の

設定、関係者への教育、関与者権限の明確化、使用記録保存、システムの第三者機関による事後監視等が必要であるが、住基ネットにおいてはこれらの制度が整備されていない。また、住基ネットシステムの保守管理等を委託された民間業者等を監視監査する人員・組織・方法も不備であり、この点についての総務省の指示通達は、予算措置や専門家の養成配備が伴っておらず、実効性がない。

- (c) 市区町村には、システムの安全性やセキュリティに問題が生じた場合の調査・監査権限が与えられておらず、都道府県においては委任の範囲で一定の権限が認められているが実効性がない。

そして、被告地自センターは情報公開の対象とされていない団体であり、同被告あるいはその職員が不正に個人情報等を漏洩する等しても、原告ら国民が事後的に監視することは不可能である。

また、情報漏洩等があった場合に、都道府県及び市区町村が住基ネットの接続を切断することに関する規定が住基法上明定されていない。

- (d) 住基法においては、国民の個人情報の保護の万全を期するため必要な「所要の措置」を講じることが義務づけられているが、後述のとおり、被告国は未だ何らの措置を講じていない。

(ウ) 長野県侵入実験

長野県は、平成15年9月1日から同年11月28日までの間、長野県内において、「市町村ネットワークの安全性」に関する調査(以下「長野県侵入実験」という。)を行い、その結果、次のような事実が明らかになった。

- a 既存住基システムやその他の個人情報を保存するコンピュータで構築される庁内LANを外部からの侵入から守るインターネット側FWを突破して庁内LANに侵入することが可能であること、さらに、市町村設置FWを突破してCS端末やCSに到達することが可能であること
- b 「操作者識別カード」や「パスワード」がなくともCS端末やCSの管理者権限(アクセス権限)を奪取することが可能であること
- c CSの管理者権限が剥奪されても、被告地自センターは全く検知することができなかったこと

以上によれば、石川県以外の市町村のCSが乗っ取られて、住基ネットを介し原告らの本人確認情報や住民票上の情報が漏洩する危険、さらに、石川県内の市町村のCSあるいは既存住基サーバに不正侵入されることにより、原告らの本人確認情報の閲覧や改ざん、それらの情報の不正送信等がなされる危険が具体的に存在することが明らかとなった。

被告らは、上記侵入実験の結果について、むしろ住基ネットの安全性が実証された旨主張するが、その主張は、ネットワークセキュリティの常識を無視した誤った事実認識とリスク評価を行っているものである。

(エ) 被告らの主張に対する反論

被告らは、住基ネットのセキュリティ対策について、OECDにおいて1980年に採択された「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」中で定められた8原則(以下「OECD8原則」という。)をふまえた厳重な秘密保護措置が講じられていることや総務省告示334号により情報漏洩防止措置が執られている旨主張する。

しかし、そもそも、現代の情報化社会においては、OECD8原則では既に十分ではないと指摘されている上、被告がOECD8原則に沿った秘密保護措置と主張するものは、実際にはOECD8原則を満たしていないのであって、個人情報保護のための十全な措置が採られているということとはできない。

また、被告らは、住基法30条の29、30条の33、36条の2で規定される本人確認情報等の安全保護措置義務を受けて、総務省告示334号により基準を設けている旨主張するが、自治体の現場においては上記基準すら満たしていない状況にあり、また、上記基準は、セキュリティ対策の大前提である個別現場に見合った情報資産の洗い出し、リスクの洗い出しとリスク評価を行わずに対策面の基準を定めるものであって、セキュリティ対策としては不十分である。

オ 住基ネットに必要性がないこと

(ア) 住基ネットの導入とその目的について

被告らは、住基ネットの導入の目的として、行政サービスの向上と行政事務の効率化を挙げ、また、我が国が実現を目指す電子政府・電子自治体の基

盤となる公的個人認証サービスのために住基ネットが不可欠である旨主張するが、次に述べるとおり、このような被告らの主張は失当である。

(イ) 住民負担の軽減と行政事務の効率化、正確性向上について

被告らは、住民負担の軽減の例として、住民票の写し交付の省略化、年金受給者の現況届の省略等を挙げる。しかし、個々の住民において、住民票の写しの交付を受ける必要が生じるのは、現実の住民票交付申請の実績を元に被告の行った試算をもとにしても年間1回に満たない上、現実に行われている住民票交付申請の大半は本人以外の申請によるものであるから、一般住民が住民票の交付申請をする機会は更に少ない。また、年金受給者の現況届についても、年1回の葉書送付程度の負担である上、対象者は限定されているから、これらを、プライバシー権を侵害してでも軽減を図らねばならない負担などということとはできない。また、行政事務の効率化とは、結局のところ経費削減を目的とするものであるが、市町村によっては、住民票の写し交付の手数料収入が減少し、かえって住基ネットの維持費による経費がかかっているのであって、これらは結局住民の負担となるのであるから、行政事務の効率化の面ではマイナスともなりうるものである。

(ウ) 行政手続のインターネット申請の実現について

- a 住基ネットは、国が電子政府・電子自治体構想を打ち出す前に導入が決まったものであって、電子政府・電子自治体実現のために住基ネットが導入されたものではない。
- b また、公的個人認証サービスについては、このような行政サービスを受受したいと思う者のみが住基ネットに自己情報を提供、保存すればよいのであって、全国民を住基ネットに参加させる理由とはならない。
- c インターネット申請のサービスを受けられる者は、住基カードを所持し、パソコンを所有しかつインターネットを利用する者に限られるのであって、少なくとも、住基カードの交付を受けている者は、平成16年3月末時点において約25万人で、全人口の0.2%に満たず、公的個人認証サービスも、これらに該当しない者にとっては何の必要性もない。また、インターネット申請を行う場合には、民間事業者が発行する電子証明書も使用できるのであって、公的個人認証サービスがインターネット申請に必要不可欠との主張は事実と反している。そして、国民が日常生活において行政機関に何らかの申請を行うことはほとんどなく、逆に、その需要があると考えられる企業については、住基ネットを利用した公的個人認証サービスを利用できないのであり、外国人についても同様であって、住基ネットを利用した公的個人認証サービスは意味のある認証制度ということとはできない。

(エ) 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、広域化について

- a 転出・転入事務の簡素化について、このような行政サービスを受受したい者が住基ネットに参加すればよいのであって、全国民を住基ネットに参加させる根拠とはならない。現に、このサービスを利用できるのは住基カードの交付を受けた者だけである。また、上記サービスによっても、省略できるのは転入届への転出証明書の添付のみであるから、現行の、転出届の郵送送付・転出証明書の郵送交付を利用すれば、転出市町村に出頭しなくて良い点は同じであり、また、実際の転居の際には、その他の種々の手続のため役所に出頭する必要があるのであって、上記メリットの存在自体が疑問である。経費節約についての被告らの試算は、例えば、住基カード所持者が転入届提出者のうち50%を占めることを前提としているが、その前提は上記の現実とあまりに乖離しており、その他の想定する数字にも根拠がなく、恣意的なものである。
- b 住民票の写しの広域交付も、住民にとって必要性が乏しい。また、経費節約についての被告らの試算は、全国で人口比約11.8%の利用を前提としているが、2次稼働後の1年間で、広域交付利用率実績が長野県や東京都においてせいぜい人口比0.1%であったことからすると、上記試算は恣意的なものとして評価せざるを得ない。
- c 住基カードの有用性についても、上記のとおり、平成16年3月末時点での発行枚数は、国が想定した300万枚の8%強である約25万枚にすぎない。

(オ) 原告らが住基ネットに参加しないことによる不都合性について

本件訴訟は、住基ネットの運用それ自体の差止めを求めているのではなく、原告ら個人の本人確認情報の流通等の差止めや記録からの削除を求めているに過ぎない。そして、住基ネットにおいて、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おいて何ら支障はない。現に、福島県矢祭町、東京都国立市、同杉並区は自治体として住基ネットに参加せずあるいは接続を切断し、横浜市は住基ネットの参加に同意した住民の情報のみを通知する選択方式を採用しており、それでも住基ネットの運用に殊更な支障を生じていないことを考えると、住民の本人同意・選択方式を採用するのに実際上の不都合があるとは考えられない。

(被告らの主張)

ア プライバシー権の憲法上の権利性について

(ア) 憲法13条の規定する幸福追求権は、個人の人格的生存に不可欠な利益を内容とする権利の総体とされ、新しい人権の憲法上の根拠となり得、また裁判規範性を有するものであるが、幸福追求権という概念が包括的で外延も明確でないだけに、その具体的権利性をもしルーズに考えると、人権のインフレ化を招いたり、それがなくても、裁判官の主観的な価値判断によって権利が創設されるおそれがあることから、幸福追求権の内容として認められるために必要な要件を厳格にしぼることが要求されている。

(イ) プライバシー権は、20世紀に入ってから「ひとりで放っておいてもらう権利」として主張され始めたものであるが、プライバシーの概念は多義的であり、また、プライバシーは、一般人を基準として「通常他人に知られたくない」か否かによって保護範囲が左右されるものであるから、同じ情報であっても、利用される場面あるいは公表される相手方によってその侵害となるか否かが左右される外延の極めて不明確なものであり、未だ権利としての明確性がない。したがって、プライバシーは、憲法13条に規定された幸福追求権によって基礎づけられる法的に保護するに値する人格的利益であるが、その概念の不明確さゆえにそれ自体は一個の統一的な憲法上の権利とまでは認められないというべきである。

(ウ) 原告らは、自己情報コントロール権もプライバシー権に内包された憲法上の権利である旨主張する。しかし、そのような見解(以下「情報コントロール権説」という。)と従来のプライバシー概念による見解とでは、第1に、一般人の感受性を基準として通常他人に知られたくない情報であるという限定を付するか(情報の限定の問題)、第2に、自由権的側面について、私生活へ侵入(それによる個人情報の収集・取得)されないという利益及びみだりに個人の情報を開示されないという利益に止まるのか、それともそれらに限らず、収集・取得をされない利益、保有・利用されない利益を認めるか(権利の内容)、第3に、個人情報の開示請求権・訂正請求権といった請求権的内容を認めるか(請求権的性格の有無)という点において異なっている。

そして、まず、保護対象となる情報の範囲について、自己に関する情報すべてが対象となると解することは広範にすぎることが明らかであるところ、情報の内容により保護の対象とそれ以外を区別することはその基準が不明確であって、結局保護対象となる情報の範囲が不明確である。次に、権利内容については、包括的すぎる権利内容のため、知られたくない利益のみならず、正当に評価してもらう利益も保護することとなり、名誉とプライバシーの双方を包括して保護の対象とすることになり、その区別が曖昧になり、真実性の抗弁の妥当範囲等についての的確な説明が困難となる。さらに、個人情報の開示請求権・訂正請求権といった請求権的内容を認める点については、そもそも、憲法13条の解釈としてこれが可能か問題があるし、仮に憲法上保障される権利・自由として認められたとしても、当然に国家に対する直接請求権という請求権的内容が認められるわけではない。そして、開示請求権・訂正請求権をプライバシー権に含める見解においても、開示請求権・訂正請求権については、原則として、法令の裏付けがあってはじめて具体的権利となると解されている。したがって、プライバシー権の内容として、個人情報の開示請求権・訂正請求権といった請求権的内容を認めるべきではない。

よって、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私生活上の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って、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権利とは認められない。

- (エ) 原告らの引用する早稲田事件最高裁判決は、あくまで個人のプライバシーに係る情報が不法行為の被侵害利益として法的保護に値するものであるかにつき判断を示したものであって、プライバシーが憲法13条により保障されるかどうかについて判断を示したものではない。

イ 本人確認情報についてのプライバシー侵害の事実について

- (ア) 原告らは、原告らの同意なく本人確認情報を金沢市ほかの行政機関等に常時情報が提供できる状態におくことは、原告らの自己情報コントロール権を侵害し、憲法13条に反する旨主張するが、原告らとその主張の前提とする「自己情報コントロール権」は憲法13条により保障された権利とは認められない。

- (イ) 情報コントロール権説をとる学者の見解によっても、住基ネットが直ちにプライバシーを侵害するものとしてはとらえられておらず、十分な秘密保護の措置等がとられているか否かを問題としているところ、住基ネットにおいては、後述のとおり、十分な秘密保護措置がとられているから、仮に原告らの主張するように、情報コントロール権説を前提とするとしても、住基ネットが原告らのプライバシー権を侵害するものとはいえない。

ウ 住基ネットの秘密保護の措置について

- (ア) OECD8原則をふまえた保護措置

住基法は、住基ネットにおける本人確認情報の保護・適正な利用を図るため、市町村長、都道府県知事、指定情報処理機関及び本人確認情報の受領機関に対する安全確保措置義務(住基法30条の29、30条の33、36条の2)を初めとする、OECD8原則をふまえた厳重な保護措置を講じており、さらに、総務省は、住基法の規定をふまえて、「電気通信回線を通じた送信又は磁気ディスクの送付の方法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」(平成14年総務省告示334号、以下「セキュリティ基準」という。)によって、セキュリティ対策についての基準を定めている。その結果、住基ネットにおいては、次のような安全保護措置がとられている。

まず、制度面からのセキュリティ対策としては、保有情報の制限並びに本人確認情報の利用及び提供の制限、各地方公共団体、指定情報処理機関の責任体制の確立及び第三者機関による監督、住民票コードの利用制限、緊急時における対応計画の策定等の措置がとられている。外部からの侵入防止策としては、建造物への侵入防止その他の物理的なセキュリティ対策が義務づけられ、電気通信回線経由による侵入に対する対策としては、専用回線の使用、公開鍵方式によるサーバ間の相互認証システム、通信プロトコルの制限、セキュリティホール対策、IDS(侵入検知装置)による監視とFWIによる不正な通信の遮断と監視、ソフトウェア統一による住基ネット全体の高度なセキュリティ確保等の措置がとられている。内部の不正利用防止対策としては、関係者に対する秘密保持義務及びその罰則による担保、指定情報処理機関に対する総務大臣による監督、照会条件の限定、操作者識別カード認証によるアクセス制御、アクセスログの定期的解析と調査、住民票の写しの広域交付における不正防止、担当職員に対する教育・研修等の措置がとられているほか、住民に対する本人確認情報提供状況の開示等として、石川県においては、平成15年11月20日から、石川県個人情報保護条例に基づく本人確認情報提供状況の開示がなされている。外部監査等によるセキュリティ確保としては、指定情報処理機関と総務省の協力による各市町村におけるセキュリティ対策の自己点検の実施及び指導、外部監査法人によるシステム運用監査の実施、平成15年10月の東京都品川区におけるペネトレーションテスト(模擬攻撃)の実施による安全性の確認等の措置を講じている。また、住基カードについても、希望者のみへの交付、記録される情報及び券面記載事項の限定、ICカードの採用による暗証番号の設定やアクセス権限の制御、カード内の記憶領域のアプリケーション毎の独立性、偽造防止策等、種々のセキュリティ対策を講じている(住基カード技術的基準)。その他、住基ネットにおける記録の最新性及び正確性の確保や庁内LANのセキュリティレベルの強化・維持等も図られている。

(イ) 長野県侵入実験について

原告らは、長野県が実施した侵入実験により、住基ネットの安全性が極めて脆弱であり、原告らのプライバシーが危機に瀕していることが明らかになった等と主張する。

しかし、公正に評価すれば、長野県侵入実験においては、インターネット経由での庁内LANへの侵入はいずれも失敗し、インターネット側FW、市町村設置FW及び指定情報処理機関監視FWのいずれも突破できておらず、各種FWにより保護されている住基ネットの安全性が明確になったというべきである。しかも、長野県侵入実験は、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FW越しにこれらのサーバを攻略することができなかったため、FWを回避して重要機密室等への物理的侵入を伴う方法で行われたものであり、通常想定しがたい極めて特異な条件の下で、CSやCS端末のOSの管理者権限を取得したものであって、むしろ通常の状態における安全性が確認されたというべきである。また、CSやCS端末のOSの管理者権限を取得しただけでは、住基ネットアプリケーションを立ち上げることはできない。更に、指定情報処理機関が監視しているのは、指定情報処理機関FWまでの住基ネット本体であって、CSは市町村が責任をもって管理すべき分野であるから、CSの監視を指定情報処理機関が行っていないことは住基ネットの監視が不十分であることを示すものではない。

長野県侵入実験の結果は、住基ネット本体の本人確認情報に対する危険性がないことを明らかにしており、わずかに、庁舎内に物理的かつ違法に侵入する方法によった場合に、市町村の庁内LAN上にある当該市町村の住民の個人情報という限定された情報について漏洩、改ざん等の可能性があることが示されたに過ぎない。

(ウ) 立証責任について

なお、原告らは、プライバシー権侵害の危険性についての事実上の立証責任が転換されるべきである旨主張している。

まず、被告らに対する国家賠償請求ないし損害賠償請求が認められるためには、原告らの法的利益が現実侵害されていることを要し、プライバシー侵害の危険それ自体は賠償を要する法的利益になり得ないから、これについて、立証責任を論ずる必要はない。

また、差止め請求については、原告らの引用する裁判例は、原子力発電所関係訴訟であって、本件訴訟とは被侵害利益、侵害態様等においても事情を全く異にしており、これらの判決例の判断を類推する基礎がない。本件においては、証拠の偏在も認められず、立証責任を事実上転換させる理由がない。

(エ) 以上のように、住基法は、本人確認情報を保護するために嚴重なる保護措置等を講じており、プライバシー侵害のおそれがあるとしても、それは抽象的なおそれにとどまるというべきである。

よって、原告らのプライバシー権が現実侵害されているとの原告らの主張は失当であり、また、プライバシー侵害の危険性があるとの主張も失当である。

エ 住基ネットの必要性

(ア) 住基ネットの導入とその目的

高度に情報化された現代社会においては、行政も、全国的な広がりを持った住民の移動や交流といった実態に合わせて行政サービスを的確かつ効率的に提供していく必要があり、そのために市町村や都道府県の区域を超えた本人確認システムが必要不可欠であるし、そのために、行政部門においても情報通信技術を的確に利用することが求められている。住基ネットは、すでに全国的な電算化の進んでいる住民基本台帳をネットワークで接続することで、本人確認システムを構築し、行政サービスの向上と行政事務の効率化を図るという発想に基づくものである。さらに、国は、情報通信技術(IT)の活用により世界的規模で生じている急激な社会経済構造の変化に的確に対応することが緊急に求められているとの認識から、「電子政府・電子自治体」の実現を目指しているが、このような電子政府・電子自治体の基盤となる不可欠なシステムが、ネットワーク社会における本人確認手段としての住基ネットである。

このような住基ネットの導入により、次に述べるようなメリットがある。

(イ) 住民負担の軽減と行政事務の効率化, 正確性向上

住基ネットによって他の市町村, 都道府県, 国の機関等において本人確認情報を利用できることにより, それぞれの事務毎に住民に義務づけられていた, 申請, 届出の際の住民票の写しの添付等の負担が解消され, 行政側としても, 事務効率の向上や事務の正確性の向上が実現している。

- a 従前, パスポート交付申請を初めとする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の写しの提出が不要となることで, 住民は住民票の写しの交付に伴う負担(手数料負担や交付を受けるための郵送や出頭の負担)を免れ, また, 市町村は, 交付事務に伴う負担を削減できることとなった。
- b 従前, 年金受給者に毎年義務づけられていた現況届又は身上報告書の提出が不要となり, また, 恩給受給者に毎年義務づけられていた受給権調査申立書の提出が不要となることで, 年金受給者及び恩給受給者は上記提出に伴う負担を免れ, 年金あるいは恩給支給機関も上記書面受付事務が削減されたことに加え, 毎年4ないし6回の各支給毎に本人確認が可能となることにより過誤払いを防止することができることになった。
- c その他, 国の機関等における種々の事務において, 本人確認情報の利用により住民票の写し提出等が不要となり, 住民の負担の軽減及び行政の効率化, 正確化が図られることになる。
- d これらの住民票の写し添付省略により, 試算では, 一年間で, 行政側で約90億円の, 住民側で約136.7億円の経費節約ができる。

(ウ) 行政手続のインターネット申請の実現

- a 平成14年12月に, 行政手続きオンライン化3法が成立し, 行政手続について, 書面によることに加えオンラインでも可能とするための法整備がなされた。これにより, 婚姻届・離婚届, パスポートの交付申請, 国民年金・厚生年金の裁定請求等がインターネットで可能となると同時に, 住基ネット利用により住民票の写し提出が不要となった。これらの基盤となるのが公的個人認証サービスと住基ネットである。
- b 行政手続のオンライン化においては, 各種申請の際に電子署名が必要となる。電子署名は, 文書を各個人が有する「秘密鍵」により暗号化したものであり, オンライン申請の際には, 電子署名と, 「秘密鍵」とペアになる「公開鍵」の電子証明書を共にインターネットで送信することになるところ, 当該電子証明書が当該個人のものであることを保証する公的個人認証サービスが必要となり, この公的個人認証サービスの提供を行うのは各地方公共団体であり, 電子証明書の発行は都道府県が, 電子署名発行申請受付, 「秘密鍵」と電子証明書のICカードへの書込み等発行事務は市町村が行い, この電子証明書の発行申請手続受理の際の当該市町村における本人確認の手段として住基ネットが利用される。また, 電子証明書の発行後の住民の住所氏名等の変更, 死亡による電子証明書の失効の際の異動情報の確認において住基ネットが利用される。このように, 公的個人認証サービスにおいて住基ネットは不可欠のものである。

なお, 上記電子証明書の格納媒体として, 住基カードが活用でき, そのため, 別個に公的個人認証サービスのためのICカードシステムの開発維持に関する費用約120億円が節約できる。

(エ) 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, 広域化による住民負担の軽減と行政事務の効率化

各市町村の住基台帳をネットワーク化することで, 住基台帳事務の簡素化・広域化を実現し, 住民負担の軽減と行政経費の節減を図ることができる。

- a 住民の転出・転入の際には, 住民は転入先で転出証明書を提出する必要があり, 転出証明書交付を受けるため, 転出地の市町村に出頭する必要があるところ, 住基カードの交付を受けている場合には, 一定の要件のもと, 転出証明書の提出が不要となり, 住民は転出・転入に伴う負担を軽減され, 市町村においては転出証明書に係る事務, 転入通知に関する事務を軽減できる。これにより, 試算では, 一年間で, 行政側で約50億円, 住民側で約32.1億円の経費が節約できる。
- b 住基ネットにより, 住民は, 当該市町村以外の市町村においても住民票の写しの交付を受けることができる。これにより, 試算では, 一年間で, 住民

側で約98.5億円の経費節約ができる。

- 希望者に交付される住基カードについては、①市町村が条例で定めることで多目的カードとして使用できる、②カードに格納された住民票コードにより本人確認が迅速かつ確実に行える、③公的な身分証明書として活用できる等のメリットがある。
 - (オ) 住基ネット導入により、導入経費として390億円、年間経費として約190億円が見込まれるが、他方、これに対する便益として、単純に試算しただけで、一年間で、行政側で上記合計約240億円の、住民側で合計約270億円の各経費節約が見込まれている。
 - (カ) 原告らは、原告ら個人が住基ネットワークに参加しないこととしても何らの不都合が生じない旨主張する。しかし、福島県矢祭町や東京都国立市、横浜市のような不参加等団体が存在することにより、同市町村住民の本人確認情報の共有がなされず、国の機関等においては従来のシステムや事務処理を存置せざるを得ず、行政コスト削減の効果が大きいに減殺され、また、不参加団体の存在により、ネットワークが寸断され、他の市町村の効率化も阻害されている。また、不参加等団体において住基ネット参加を希望する者が住基ネットによる負担軽減等を受けられないことは同住民にとって不利益であるし、不参加等団体自体が住基ネットによるコスト削減を享受できないことは当該不参加等団体にとっての不利益である。横浜市の行っている選択方式(横浜方式)は、非通知申出者の把握に多大なコストがかかり、上記の住基ネットの目的を阻害することは明らかである。したがって、不参加等団体の存在によって、住基ネットのメリットが大きいに減殺されていることは明白である。
- オ プライバシー侵害を理由とする差止めの可否について
原告らは、プライバシー権の侵害ないし侵害の危険性を理由として差止めを求めているが、プライバシーについては、上述のとおり、その概念自体が不明確であり、統一的理解を得られていないことから、現段階においては、名誉権と異なり、プライバシーを保護する利益を排他性を有する絶対権ないし支配権としての人格権であるとして差止めが容認される状況にはなく、プライバシーの侵害のみを理由として差止め請求を認めることはできないというべきである(最高裁判所平成14年9月24日第三小法廷判決・判時1802号60頁参照)。
- (2) 氏名権及び「公権力による包括的管理からの自由」が憲法13条によって保障されているか。住基ネットの運用が開始されたことにより、「氏名権」及び「公権力による包括的な管理からの自由権」が侵害されたか。(争点(2))
- (原告らの主張)
- ア 人格権とは、個人的人格的属性を対象とし、その自由な発展のために第三者の侵害に対し保護すべき諸利益の総体をいう。
憲法13条は、個人を尊重し、生命・自由・幸福追求の権利を尊重すべきとするものであるが、これは個人的人格的な生存・発展にとって不可欠と思われる権利・自由の保護の必要性を包括的に述べたもので、一方で憲法各条において個別に規定されている権利自由を包含する性質を有し、他方で人権のカタログにないものであっても個人の生存・人格的な発展にとって不可欠な利益(無名人権)は、法的に最大限に保障する趣旨の規定である。憲法13条が人格権を保障した規定であると解されることは、今日では判例・通説である。そして、人格権が、裁判規範性を有していることもまた判例・通説であり(北方ジャーナル事件・最高裁判所昭和61年6月11日大法廷判決・民集40巻4号872頁参照)、行政の管理が、国民各個々人の自由な発展の阻害をもたらすに至る場合には、国民は人格権に基づきその侵害を排除する権利を有するというべきである。
 - イ 各国民は、「行政の全人格的な管理の客体におかれぬ」権利・自由もしくは「公権力による包括的管理を拒否する」権利・自由(以下「公権力による包括的な管理からの自由」という。)を有しており、これは人格権に内包されるものとして憲法上の保護を受ける。なぜなら、公権力による包括的管理により、公権力に不都合な思想を有し、あるいは行動を行う者に対し事実上の不利益を課し、あるいはその恐れを国民が認識することで、国民個人の一人の人間としての基本的な意思決定や行動の自由を著しく萎縮させることになるからである。

住基法に基づいて付された住民票コードは、すべての国民に、重複しないように付された11桁の番号であり、1億2000万人を超える国民を確実に識別するために付されたものであるから、正に共通番号に他ならず、これまで行政機関が保有してきた個人情報を、全国一元的に管理するものである。そして、住民票コードの利用事務は、平成14年12月にそれまでの10省庁93事務から11省庁264事務に拡大されたが、今後も拡大されることが予想され、事実上利用事務に制限はなく、また平成15年8月に導入された住基カードは、今後様々な情報を搭載していくことが前提とされており、これらによって、住基カードが電子身分証明書化され、実質的な携帯義務化が進むこととなり、個人の生活が全面的に住民票コードの下に記録され、蓄積されていくことは必至である。住民票コードが、国民総背番号制としての役割を果たし、この番号をもとに、個人のあらゆる情報が行政によって把握され、管理される事態となるのであって、住基ネットの稼働が「公権力による包括的な管理からの自由」を侵害するものであることは明らかである。

ウ さらに、住民票コードによる付番は人格権に内包される氏名権を侵害するものである。

すなわち、氏名は、人の同一性を示すものとして人格と密着しており、他人による冒用等によって侵害されるときは、一般的人格権侵害の一種として法律上の保護が与えられる(最高裁判所昭和63年2月16日判決・判例タイムズ662号75頁参照)。住基ネットにおいては、住民票コードにより個人の情報が管理され、流通することになり、個人の人格の同一性を表す中核となる氏名は、住民票コードで分類される個人情報の一つにおとしまられることになる。しかも、住民票コードは全国的に生涯にわたって番号を付するものであり、人格権を侵害するものである。

エ そして、上記人格権侵害は現になされているものであり、また侵害の主体が公権力である以上、対立する他の人権との調整を考慮する必要もないから、原告らの上記人格権侵害を排除するために、原告らについて住基ネットの運用を差し止める必要がある。

(被告らの主張)

ア 住民票コードは、住民票に付するのであって、個々の住民に付するものではない。

イ 確かに、氏名については、不法行為法上の保護を受けうる人格的利益を有するものである。しかし、住民票コードは、特定の住民の本人確認を確実にかつ効率的に行うために使用される11桁の番号であって、住基ネットを稼働させる上で必要不可欠な情報(記号)であり、住民基本台帳に記載された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させるために、技術上新たに設けられた符号にすぎず、個人の人格的価値とは無関係である。よって、本件住民票コードの記載により、およそ原告ら的人格権も人格的利益も侵害したとはいえず、原告らの主張は失当である。

ウ また、原告らは、住民票コードが総背番号制としての役割を果たす旨主張するが、行政機関が住民票コードを利用する場合には目的外利用の禁止、告知要求制限等の規定により利用が制限されており(法30条の34、30条の42及び30条の43)、さらに、居住関係の確認を行うためののみ利用されるものであり(法30条の7第3項)、国の機関等と他の国の機関等との間で住民票コードを利用してデータマッチングをすることは禁止されているのであり、共通番号としては機能しないものである。

なお、住民票コードを付さないと、①氏名や住所の記載が住民基本台帳上の記載と異なる場合にアクセスできない、②処理の際にサーバに大きな負荷がかかる、③氏名及び住所が同一の場合には同一人物か否かが確認できない、④行政機関が保有する情報が最新のものでない場合に、これに基づいてアクセスするためには、住基ネット内に本人確認情報の過去の履歴を保存しておく必要があり、効率的でない等の不都合があり、住民票コードは住基ネットに不可欠である。

(3) 被告県及び同地自センターが住基ネットを運用したことが違法か(争点(3))

(原告らの主張)

ア 被告県の谷本正憲知事は、憲法11条、同13条、同17条、同99条等の規定から、石川県の機関及びそれを担う公務員として憲法を遵守する義務があるところ、これに違反して、上記のとおり、①当該市区町村の長に対し住民票コ

ードを指定し通知し、②本人確認情報を磁気ディスク等に記録して保存し、③国の機関等へ本人確認情報を提供し、④被告地自センターに対し、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被告地自センターへ本人確認情報を通知し、これらの違法行為により原告らの人格権ないしプライバシー権を侵害したものであり、これらの行為は国家賠償法上、違法である。

イ 被告地自センターは、金沢市他の市町村が有する本人確認情報をネットワーク化することにより、原告らの人格権ないしプライバシー権を侵害したものであり、これらの行為は不法行為(民法709条)に該当する。

(被告県の主張)

国賠法上の違法性が認められるには、被告県の公務員が個別の国民に対する職務上の法的義務に違反したことが必要である(最高裁判所昭和60年11月21日判決・民集39巻7号1512頁)。この場合、住基法の内容が憲法に違反するかは直接の争点とならず、住基法の施行に当たった公務員について、「職務上通常尽くすべき注意義務を尽くすことなく漫然と」当該行為をした事実があるか争点となるところ、本件において、谷本知事に、これらの法的義務違反の行為がないことは明らかである。

(被告地自センターの主張)

被告地自センターは、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、各都道府県知事から委託された事務及び同法に定められた事務を同法の定めるところにより行ったものであり、その事務の遂行につき何ら違法はない。

(4) 被告国が改正法を施行したことが違法か(争点(4))

(原告らの主張)

ア 「所要の措置」について

(ア) 「所要の措置」をとるべき義務

改正法附則1条2項は、「この法律の施行に当たっては、政府は、個人情報の保護に万全を期するため、速やかに、所要の措置を講ずるものとする」と規定しているところ、同附則制定の経緯からも、同附則の文言からも、改正法施行の前提として、政府は「所要の措置」をとらなければならない義務を負っていたことは明白である。被告国は、少なくとも「所要の措置」をとるまでは、住基ネットの稼働をしてはならないことは知悉していた。

(イ) 「所要の措置」の内容

「所要の措置」として要請される個人情報保護制度は、住基ネットの運用が開始されるに際して、憲法13条で保護された国民のプライバシー権を真に保障するために、行政機関によりプライバシーの権利が侵害されないような保護措置、すなわち、行政機関による個人のプライバシー権の侵害を防ぐために、行政機関の行為を厳格に規制する保護制度である。そして、住基ネットの稼働により、住民票コードが濫用され、多目的利用される危険性が存在するという観点からすれば、①本来に業務処理に必要な範囲を超えた名寄せの制限、②複数の行政機関相互におけるデータマッチングの制限、③第三者機関による電子政府の監督及び監視、④罰則による担保の4条件(以下「4条件」という。)が、国民が自己の個人情報を行政機関に委ねることができる最低限の条件として、「所要の措置」を講じる義務の不可欠の内容をなすものというべきである。具体的には、住基法制定当時存在した、公的部門における個人情報保護制度としての「行政機関の保有する電子計算機処理にかかる個人情報の保護に関する法律」(1988年制定、以下「1988年法」という。)について、その内容の不備を、4条件を最低限満たす内容に改正し、個人情報保護に関する法整備をすることが求められていたというべきである。

(ウ) しかし、政府は、1988年法が未改正であるにもかかわらず、政令で住基法の改正法の施行日を決め、平成14年8月5日から同法を施行した。

総務省は、平成13年3月に「個人情報保護法案」を提出したことで「所要の措置」を講じたと主張しているが、上記のとおり、住基法の改正法施行の前提として、1988年法の改正を含め個人情報保護法制を整備する法的義務があったのであるから、政府は、個人情報保護法制を整備できないのであれば、住基法の改正法施行を見送るべき法的義務があったというべきである。

(エ) ところで、平成15年5月に、行政機関個人情報保護法を初めとする個人情報関連5法が成立したが、うち行政機関個人情報保護法は、4条件のうち、①名寄せの制限、②データマッチングの制限、③第三者機関による監視の条項を全く欠き、④罰則も最小限のものに止まっているばかりか、個人情報の目的外利用を広く認める内容となっているのであって、同法は、「所要の措置」というべき内容を欠いているというべきであり、上記附則の形式的要件を満たしているとしても、実質的要件は未だ満たされていないというべきである。

イ 以上のとおりであるから、小泉内閣総理大臣には、改正法で政府に義務づけられている所要の措置を講じないまま住基法の改正法を施行し、住基ネットの運用を開始した違法があり、これらの行為により原告らの人格権ないしプライバシー権を侵害したものである。

(被告国の主張)

ア 所要の措置について

(ア) 改正法は、附則1条1項により、公布の日から3年を超えない範囲内で政令の定める日から施行する旨定めており、政府は公布日から3年以内に住基法を施行することが法律上義務づけられていたものであって、政令で平成14年8月5日を施行日と定め、同日施行したことに何ら違法はない。

(イ) 政府は立法機関ではないから、住基法の改正法附則にいう「所要の措置」が法律案の検討、作成、国会への提出を意味することは明らかであり、政府は、平成13年3月に「個人情報の保護に関する法律案」(以下「個人情報保護法案」という。)を提出したことで、「所要の措置」を講じたものである。

(ウ) そもそも、「所要の措置」とは、民間部門における個人情報保護に関する制度についての措置を指すものであり、「所要の措置」が1988年法の改正であるとの原告らの主張は独自の見解というべきであって、かかる誤った前提に立って、4条件といった「所要の措置」の具体的内容を論ずることは無意味である。

また、原告らは、行政機関個人情報保護法が「所要の措置」というべき内容を欠いていると主張するが、上記のとおり、「所要の措置」が行政機関個人情報保護法を成立させることではないから、その内容は何ら住基法の改正法施行に影響を及ぼすものではない。

イ 原告らは、小泉総理大臣が「所要の措置」を講じないまま住基法の改正法を施行し運用を開始したことが違法である旨主張する。しかし、上記(3)(被告国の主張)欄の主張と同様、小泉総理大臣に「職務上通常尽くすべき注意義務を尽くすことなく漫然と」当該行為をした事実がないことは明らかであり、また上記アのとおり、「所要の措置」は既にとられている。

(5) 争点(5)について(損害)

(原告らの主張)

ア 上記のとおり、原告らは、被告県及び同地自センターが運用する住基ネットによりプライバシーの権利ないし利益を侵害され、今後原告らのプライバシーの漏洩ないし不正使用の危険にさらされることにより常時精神的に不安な状態におかれることになった。その精神的苦痛を慰謝するのに各原告につき金10万円が相当である。

また、本件訴訟の弁護士費用としては各原告につき金1万円が相当である。

イ 上記のとおり、原告らは、被告国の行為により、プライバシー及び人格権を侵害され、今後原告らのプライバシーの漏洩ないし不正使用の危険にさらされることにより常時精神的に不安な状態におかれることになった。その精神的苦痛を慰謝するのに各原告につき金10万円が相当である。

また、本件訴訟の弁護士費用としては各原告につき金1万円が相当である。

(被告らの主張)

否認ないし争う。

第4 争点に対する当裁判所の判断

1 プライバシーの権利は憲法13条によって保障されているか。住基ネットの運用が開始されたことにより、原告らのプライバシーの権利が侵害されたか。あるいはその危険性があるか。(争点(1))

(1) 他者に知られたくない個々人の私生活上の情報がみだりに他者に開示されたり、他者が私事に属する領域に侵入してくる場合には、個人の私生活における

平穩が侵害されるのみならず、自らの生き方を自らが決定するという人格的自律を脅かされることとなるから、このような、私事の公開・私生活への侵入からの自由としてのプライバシーの権利は、憲法の基本原理の一つである「個人の尊重」を実現する上での要となる権利の一つであって、単に、不法行為法上の被侵害利益であるに止まらず、いわゆる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と解すべきである。

ところで、近年、IT(情報技術)の急速な発達により、コンピュータによる膨大な量の情報の収集、蓄積、編集、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った。公権力や一般企業においては、これらを利用して広範な分野にわたる個人情報収集、蓄積、利用、伝達されているところ、このようなデジタル情報は、半永久的に劣化しないで保存できること、瞬時に複製、伝達できて、短時間に爆発的に増殖させることができること、複製されても、そのことが容易には判らず、伝達先を把握することはほとんど不可能であること、書き換えも容易であり、書き換えられていることが外観上は判らないこと等の特性があり、一般の住民の間には、自己の個人情報が自己の知らぬ間に収集、利用されることについては、これが漏洩等によって拡散し、悪用され、自己の私生活の平穩が侵害されることへの不安が高まっており、実際に、個人情報の大量漏洩や個人データの不正な売買といった事案が相次いで社会問題化しており、住民の間に強い不安をもたらしている。このような社会状況に鑑みれば、私生活の平穩や個人の人格的自律を守るためには、もはや、プライバシーの権利を、私事の公開や私生活への侵入を拒絶する権利と捉えるだけでは充分でなく、自己に関する情報の他者への開示の可否及び利用、提供の可否を自分で決める権利、すなわち自己情報をコントロールする権利を認める必要があり、プライバシーの権利には、この自己情報コントロール権が重要な一内容として含まれると解すべきである。

ところで、コントロール権が認められる情報としては、思想、信条、宗教、健康等にかかわるいわゆるセンシティブな情報を挙げることができるが、その外延は明らかでない。しかし、それは、今後の具体的な事例の積み重ねの中で自ずと明らかになっていくもので、外延が明らかでないからといって、自己情報コントロール権自体を認めるべきではないとは解せられない。また、自己情報コントロール権から派生すると解されている開示請求権、訂正請求権がいかなる場合にいかなる要件で認められるかは困難な問題であるが、これも具体的な事例の中で検討されるべき問題であって、これが明確でないからといって、自己情報コントロール権自体を認めるべきではないとは解せられない。

- (2) 住基ネットは、住民が、転入、転居等の事由が生じたために市町村長に届け出た情報のうち、氏名、住所、生年月日、性別の4情報と、市町村長が記載した住民票コード及びこれらの変更情報、以上の6情報(本人確認情報)を、市町村長が都道府県知事に通知し、更に都道府県知事がこれらを被告地自センターに通知し、同地自センターがこれを国の機関又は法人、当該都道府県の区域内の市町村の執行機関、他の都道府県の執行機関、他の都道府県の区域内の市町村の執行機関等に提供するシステムであって、住民は、市町村長に対して上記届出をしたときに、市町村長や都道府県知事によって上記の通知がなされることや被告地自センターによって上記提供がなされることを承諾していたものではないし、上記の通知や提供がなされる際に個別に同意を求められるものでもないから、上記システムは、本人確認情報が自己情報コントロール権の対象となるのであれば、住民が有している本人確認情報に対するコントロール権を侵害するものであるということが出来る。
- (3) そこで、本人確認情報が自己情報コントロール権の対象となるか否かを検討するに、個人情報といっても、上記のセンシティブな情報から単なる個人識別に使われる情報まで様々なものがあり、その秘匿を要する有無、程度も様々であって、すべての個人情報がプライバシーにかかる情報として法的保護の対象となるとは解せられない。そして、上記4情報は、一般的には個人識別情報であって、その秘匿の必要性が高いものではないということはある。しかし、このような個人識別情報であっても、これを他者にみだりに開示されないことへの期待は保護されるべきものである上、秘匿の必要性は、個々人によって様々である。すなわち、ストーカー被害に遭っている人にとっては住所について秘匿されるべき必要性は高いし、性同一性障害によって生物学的な性と異なる性で社会生活を送っている人にとっては性別について秘匿されるべき必要性は高いといわなけ

ればならない。通名で社会生活を送っている人のうちには、それが戸籍上の氏名でないことを知られたくない人がいるであろうし、生年月日をむやみに人に知られたくないと思う人は少なくあるまい。また、住民票コードは、それ自体は数字の羅列に過ぎないが、住民票コードが記録されたデータベースが作られた場合には、検索、名寄せのマスターキーになるものであるから、これを秘匿する必要性は高度である(住基法30条の43によって、民間において、住民票コードの告知を求めることや、他に提供されることが予定されているデータベースを構成することが禁止されているが、本人が自主的に住民票コードを開示し、これをもとに特定の企業内部で利用するためにデータベースを構成することは禁止されていないから、民間においても、住民票コードの利用が広まっていく蓋然性は高い)。更に、上記変更情報は、婚姻、離婚、養子縁組、離縁、氏名の変更、戸籍訂正等の身分上の重要な変動があったことを推知させるものであるから、これらを秘匿する必要性も軽視できない。そうすると、本人確認情報は、いずれもプライバシーにかかる情報として、法的保護の対象となるというべきであり(早稲田大学事件最高裁判決参照)、自己情報コントロール権の対象となるというべきである。

(4) なお、本人確認情報のうち4情報については、住基ネットシステムの導入前から、何人も、不当な目的によることが明らかである等として市町村長から拒まれない限り、住民基本台帳の一部の写しの閲覧(住基法11条)、住民票の写し等の交付(同12条)の手続によって入手することができ、本人にはこれをコントロールするすべがなかったから、もともと4情報については、その情報の本人には、これをコントロールできる可能性がなかったということではある。しかし、だからといって、上記4情報が法的保護の対象にならないということではできない。なぜなら、住基ネットシステムにおける市町村長、都道府県知事及び被告地自センターによる本人確認情報の通知、保存、提供は、本人確認情報の新たな、しかも甚だしい拡散であるし、そもそも現代社会に於けるプライバシーの権利の重要性に鑑みると、住基法による上記閲覧及び写し等の交付を定めた規定自体の相当性を再検討すべきものと考えられるからである。

(5) そうすると、住基ネットは、住民らの本人確認情報に対する自己情報コントロール権を侵害しているというべきところ、自己情報コントロール権も無制限に保護されるわけではなく、公共の福祉のため必要がある場合には相当の制限を受けることはやむを得ない。

そこで、行政上の目的を実現するために、立法によって、自己情報コントロール権の対象となる本人確認情報を本人の承諾なく通知、保存、提供するシステムを運用することがいかなる場合に許されるかを検討する必要があるが、そのためには、①本人確認情報の秘匿を要する程度(社会通念上、誰もが、自ら開示する以外には強く秘匿を望む情報か、できれば秘匿したいという程度の情報か)、②システムのセキュリティ(通知、保存、提供することによって第三者が本人確認情報に不正にアクセスしたり、情報が漏洩する危険がどの程度あるか)、③通知、保存、提供の態様が個人の人格的自律を脅かす危険の有無、程度を検討する必要がある。そこで、以下、(6)ないし(8)において、上記①ないし③について検討する。

(6) 本人確認情報の秘匿を要する程度について

前記のとおり、本人確認情報のうち、4情報は、個人によって異なるものの、社会通念上、一般的には秘匿を要する程度が高いということではできない。しかし、住民票コード及び変更情報は、その程度は相当高いというべきである。

(7) システムのセキュリティについて

ア 証拠(各項記載)によれば、次の事実が認められる。

(ア) 住基ネットのハード面におけるセキュリティについて(乙10, 11)

a CS, 都道府県サーバ、全国サーバ間の通信は、専用回線及び専用交換装置で構成されたネットワークを介して行われ、また、全国サーバと国の機関等のサーバ間では、専用回線ないし記憶媒体のやりとりによる情報交換が行われる。

上記専用回線は、VPN(バーチャル・プライベート・ネットワーク)によるもので、物理的に独立した回線ではなく、他の通信と共用の通信回線において、暗号により他の通信と独立した回線を形成するものである。

b 住基ネットにおける情報通信に際しては、暗号技術評価委員会において安全性が確認されている公開鍵方式による通信相手の認証を行っている。

- c 住基ネットにおいては、住基アプリケーションによる独自の通信プロトコル(データ通信におけるデータ受送信のための手順や規則のこと)による通信を行っており、インターネットで用いられている汎用のプロトコルを使用していない。そして、指定情報処理機関監視FWにおいてインターネットで使用されるプロトコルの通過を遮断する措置がとられている。
 - d 被告地自センターは、指定情報処理機関監視FWについて、ネットワーク側への不正通信、ネットワーク側からの不正通信の有無につき24時間の監視体制をとり、また、ネットワーク内にIDS(侵入検知装置)を設置して常時監視を行っている。
 - e CS端末において住基ネットアプリケーション(以下「住基アプリ」という。)を立ち上げるためには、CS端末のOSの権限のほかに、住基アプリの専用カードと暗証番号が必要とされている。
- (イ) 総務省告示による住基ネットのセキュリティ基準について(乙1の1ないし3)
総務省は、施行規則2条、6条、7条、10条ないし14条及び18条ないし20条までの規定に基づき、セキュリティ基準を定めて平成14年8月5日から適用し、その後、同基準を総務省告示第391号及び同601号で改正し、同601号は平成15年10月1日から適用された(以下、同601号による改正後の上記基準を「現行セキュリティ基準」という。)
現行セキュリティ基準により、住基ネットにおいては、秘密保護措置として、上記第2の2(6)記載のほか、都道府県、市町村及び指定情報処理機関において次のような措置が講じられている。
- a 体制、規程等の整備
都道府県知事、市町村長及び指定情報処理機関に対し、住基ネットにおけるセキュリティ対策のための連絡調整の場の設置、異常の早期発見、連絡のための体制整備、住基ネットの企画、開発、運用に関する規程及び住基ネットシステム設計書、操作手順書、緊急時の作業手順書の整備、住基ネット運用のための職員配置及び適切な人事管理、同職員に対する教育・研修計画の策定・実施、住基ネットのセキュリティ対策の評価及び改善努力をそれぞれ義務づけ、また、緊急時の体制として、住基ネットが構成機器やソフトウェアの障害により作動停止した際やデータ漏洩のおそれがある場合の行動計画、住民への周知方法及び相互の連絡方法の策定、そのための連携及び研修の実施を義務づけている。
 - b 重要機能室について
電子計算機室や磁気ディスク保管室は専用の部屋を確保し、確保できない場合は電子計算機及び電気通信関係装置を厳重に固定し、磁気ディスク等を専用保管庫で施錠保管することとしたほか、電子計算機室や磁気ディスク保管室等の重要機能室について、侵入防止のための各種措置をとることとされている。
 - c 住基ネットシステムの管理
 - (a) 入退室管理
重要機能室への入室者の限定及び管理、鍵または入退室管理カードの管理、重要機能室への搬入物品の確認や、事務室における職員不在時の施錠等の措置が義務づけられている。
 - (b) ソフトウェア開発等の管理
住基ネットシステムの開発、変更時におけるセキュリティ確保、不正行為の防止等が義務づけられている。
 - (c) 住基ネットシステムの管理
住基ネットを運用する職員には必要なアクセス権限を付与し、電気通信関係装置の管理に付き不当な運用防止のため厳重な確認を行い、管理者権限がない者の操作を防止する措置を講じ、ネットワーク経由の模擬攻撃を適宜実施してその結果に基づき必要な措置を講じ、また、セキュリティ対策に関する情報の収集、分析を実施して必要な措置を講じることとされている。
 - (d) 端末機、電子計算機の管理
端末機の取り扱いは、管理責任者の指示ないし承認を受けた者のみが行うこととし、アクセス権限を有していることを操作者識別カード及び暗証番号による確認、操作者確認カード及び暗証番号の適切な管理、電子ファイルの利用制限、操作履歴の記録保存、本人確認情報照会の

条件設定、複数回のアクセス失敗による端末機の強制終了等の措置を講じることとされ、また、各サーバについて住基ネットシステムの管理及び運用に必要なソフトウェア以外のソフトウェアを作動させないこととされている。

- (e) 磁気ディスクの保管
磁気ディスクについては保管庫等を設置して保管し、磁気ディスク盗難防止のため、持ち出し及び返却の措置、磁気ディスクによる本人確認情報の送付の際の保管状況の確認等の措置を講じることとされている。
 - (f) 構成機器及び関連設備の管理
構成機器及び関連設備についても、管理方法の明確化、保守の実施、稼働状況の監視、不正プログラムの混入防止等の措置を講じることとされている。
 - (g) データ等の管理
データやプログラム、ドキュメントの管理についても、使用、複写、消去、廃棄等における適切な管理体制、データの入出力時の適切な管理等が要求されている。
 - (h) 障害時の対応
住基ネットシステムの障害及び不正アクセスの早期発見機能の整備、不正アクセス判明時の相互の連絡調整及び被害拡大防止のための必要な措置を講じることとされている。
 - (i) 委託を行う場合の措置
住基ネットシステムの開発、変更、運用、保守等について、業者に委託する際には、委託先事業者の社会的信用と能力を確認し、セキュリティ対策実施や不正行為防止のための監督を行い、再委託の制限、分担範囲の明確化等の措置を講じることとされている。
- d 既設ネットワークとの接続
住基ネットと既設のネットワークを接続する場合には、既設ネットワークについてもセキュリティ対策を行い、接続状況について相互に連絡調整を行うこととされている。
- e 住基ネットの運用
- (a) 市町村においてCSに記録された本人確認情報について、新たな本人確認情報が記録された場合、従前の本人確認情報は、5年経過後に確実に消去することとされ、また、都道府県サーバ及び全国サーバにおける本人確認情報についても、施行令30条の6又は30条の11規定の期間経過後に確実に消去することとされている。
 - (b) また、国の機関等に本人確認情報を提供する際には、都道府県知事に、国の機関等と、本人確認情報の漏洩、滅失、毀損の防止その他適切な管理のための措置について協議することとされ、本人確認情報の提供を受ける国の機関等についても、本人確認情報の適切な管理のための措置を講じることとされる。
 - (c) 必要に応じて、都道府県知事(この項において、指定情報処理機関に対し委任した都道府県知事を含む)は国の機関等及び当該都道府県の執行機関に対し、都道府県知事及び指定情報処理機関は区域内の市町村、他の都道府県その区域内の市町村の執行機関に対し、市町村長は、他の市町村の執行機関及び都道府県知事、都道府県の執行機関に対し、提供が行われた本人確認情報の適切な管理のための措置の実施状況について説明を求め、その実施の要請を行うこととされている。
 - (d) 自己に係る本人確認情報の提供又は利用の状況に関する情報の開示請求に適切に対応するため、都道府県知事は、本人確認情報を提供した際及び自己が利用した際には、その状況に係る情報を必要な期間保存することとされる(指定情報処理機関に対し事務委任をした都道府県知事は、指定情報処理機関に上記状況の報告を求めた上で、同様の措置をとることとされる)。上記期間経過後は同情報を確実に消去することとされている。
- (ウ) 各市町村のセキュリティ対策に対する自己点検
各市町村は、「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ネットワークに関する調査票」に基づき、住基ネットにおけるセキュリティ

確保について、各項目ごとに3点満点とする数十項目の自己点検を実施した。その結果は、平成15年5月12日時点で計3207団体の平均点が2.48点、同年8月25日時点で同じく2.83点、平成16年11月24日時点で計2959団体の平均点が2.88点であった。(乙11, 33)

(エ) 住基カードに関する情報について(乙13)

総務省は、平成15年5月27日、施行規則46条の規定に基づき、住基カード技術的基準を定め、同基準は平成15年8月25日から適用された。同基準によれば、住基カードの運用に際し、次のとおり、住基カードに関する情報が通知ないし提供されることとなっている。

- a 市町村長は都道府県知事に対し、委任都道府県知事は指定情報処理機関に対し、市町村長、都道府県知事又は指定情報処理機関は、国の機関等に対し、それぞれ、住基ネットを通じ、当該住民の住基カードの運用状況が運用中、一時停止又は廃止の状況にあることを通知する。
- b 住基カードの発行を受けている住民の住民基本台帳がある市町村以外の市町村が本人確認情報の提供を受ける際には、都道府県知事又は指定情報処理機関は、住基カードの有無について通知する。

(オ) 長野県侵入実験について(乙19, 甲共32の1ないし4, 甲共33の1ないし4, 甲共39, 41)

- a 長野県は、平成14年12月に発足した長野県本人確認情報保護審議会が、平成15年5月に県に提出した「長野県本人確認情報保護審議会第1次報告」を受け、住基ネットにおいて、インターネット側から市町村の庁内ネットワークを経由した住基ネットシステムへの不正アクセス及び住基ネットシステムからの本人確認情報漏洩の可能性を確認し、有効な対策を講ずるための資料を得ることを目的として「住基ネットに係る市町村ネットワークの脆弱性調査」を実施することとし、平成15年9月22日から同年10月1日まで第一次調査を、同年11月25日から同月28日まで第二次調査を実施した(以下、第一次、第二次調査をあわせて「長野県侵入実験」という。)

長野県侵入実験及びその調査結果の概要は次のとおりである。

b 調査方法

- (a) 市町村の庁内LANから住基ネットへの侵入(内部からの侵入)とインターネットから庁内LANへの侵入(外部からの侵入)の2種類の調査を行った。

(b) 内部からの侵入調査

庁内LANに調査用コンピュータを接続して庁内LAN及び庁内LAN上に存在する各種サーバについての情報を収集し、その情報をもとにサーバの管理者権限奪取を試みた。管理者権限を奪取した既存住基サーバから既存住基サーバ・CS間の市町村設置FWについての情報を収集するとともに、既存住基サーバに偽装した調査用コンピュータによりCSとの通信を試みた。また、CSセグメントに接続した調査用コンピュータにより、CS及びCS端末についての情報を収集し、既知の脆弱性を利用してCS及びCS端末の管理者権限奪取を試みた。

(c) 外部からの侵入調査

遠隔地からインターネットを経由してFW及びDMZ(非武装セグメント、FWを経由した場所に置かれているLANセグメント)に置かれた公開サーバについての情報を収集し、得られた情報をもとに公開サーバへの侵入を試みた。

(d) 留意事項

調査対象自治体において実際に稼働しているコンピュータ・システムに関して実施した。また、不正アクセス行為の禁止等に関する法律への配慮から、全国の都道府県の委託を受けて被告地自センターが管理している部分、すなわちCSの都道府県ネットワーク方向にある指定情報処理機関監視FWから上流部分については調査対象とはしなかった。

- c 下伊那郡阿智村における第一次調査(平成15年9月22日から同月24日)
事前に既存住基サーバ及び庁内WEBサーバのIPアドレス(コンピュータ識別のため割り当てられた番号)について情報を得た上、役場サーバ内のHUB、隣接する施設のLANポート、庁内LANにダイヤルアップで接続されている出先機関のルータにそれぞれ調査用コンピュータを接続して調

- 査した。結果は次のとおりであった。
- (a) 庁内LANのネットワークに調査用コンピュータで接続することができた。
 - (b) その後、既存住基サーバ及び庁内WEBサーバの管理者権限を奪取することができた。
 - (c) 庁内LANとCSの間にある市町村設置FWを通過可能な通信によってはCSの管理者権限を奪取することはできなかった。なお、CSの管理者ポートが庁内LAN側に向け開放されていたが、同ポートを利用して市町村設置FWの権限奪取ないし無効化が可能かどうか確認しなかった。
- d 同第二次調査(平成15年11月25日から同月28日)
- CSが格納されている役場サーバ室内のラックを開錠し、CSセグメントにあるHUBに調査用コンピュータを接続して調査した。結果は次のとおりであった。
- (a) CSの管理者権限を奪取することができた。また、CSに保存されている住基ネットのデータベースにアクセスし、当該市町村の住民の住基ネットデータを閲覧することができた。
 - (b) CS端末には適切なパッチが当てられていてその管理者権限を奪取することはできなかった。管理者権限を奪取したCSのIDとパスワードを使用したところ、CS端末の管理者権限を奪取することができたが、住基アプリを改めて起動することができるかどうか、住基アプリが正規に起動している状況でCS端末の操作を遠隔で行い住基アプリを操作できるかどうかについてはいずれも確認しなかった。
- e 諏訪郡下諏訪町における調査
- 平成15年9月25日及び26日に調査が実施された。事前に既存住基サーバのIPアドレスについて情報を得た上、調査用に構築した無線LANを利用して、町役場に隣接する建物から調査用コンピュータを庁内LANに接続して調査した。結果は次のとおりであった。
- (a) 庁内LANのネットワークに調査用コンピュータで接続することができた。
 - (b) その後、既存住基サーバ及び庁内WEBサーバの管理者権限を奪取することができた。
 - (c) 庁内LANとCSの間にある市町村設置FWに脆弱性は認められず、また、CSの管理者権限を奪取することはできなかった。
- f 東筑摩郡波田町における調査
- 平成15年9月29日から同年10月1日まで調査が実施された。事前に対象ネットワークのIPアドレスについて情報を入手した上、遠隔地(東京)からインターネット経由で接続して調査した結果、インターネットとDMZ間のFWと兼用になっているDNSサーバ(ホスト名とIPアドレスの対応情報を保有するサーバ)に脆弱性はなく、上記FWを通過することのできる通信によっては、公開サーバの管理者権限を奪取することはできなかった。
- (カ) 品川区におけるペネトレーションテスト(乙12)
- 被告地自センターは、平成15年10月10日及び翌11日、品川区の協力を得て、住基ネットの機器に対するペネトレーションテスト(ネットワークへの侵入実験)を実施した(実際のテストは、A社が実施)。総務省は、同テストの結果について、次のとおりであるとの発表をした。
- a 住基ネットーCS間のFW(指定情報処理機関監視FW)について、CSセグメントから3時間のテストを実施したが攻略できず、脆弱性も見いだせなかった
 - b CSー庁内LAN間のFW(市町村設置FW)について、庁内LANセグメントから6時間のテストを実施したが攻略できず、脆弱性も見いだせなかった
 - c 庁内LAN上のCS端末に対し庁内LANセグメントから6時間のテストを実施したが、CS端末の権限奪取できず、弱点も見出せなかった
- イ 前記前提事実及び上記認定事実によれば、次のようにいうことができる。
- (ア) 住基ネットシステムの構成機器その他いわゆるハードウェアについてみるに、前記のとおり、電気通信にはVPNによる専用回線が使用され、CSと既存庁内LANとの間、CSと専用回線との間、都道府県サーバと既存庁内LANとの間、全国サーバと専用回線との間、全国サーバと国の機関等のサーバとの間にはそれぞれFWが設置され、さらに、ネットワーク上にはIDSが設置されるなどのセキュリティ対策が講じられており、これらのセキュリティ

ィが破られる抽象的な危険性が無いとはいえないが、具体的な危険性が存在するとまでいうことはできない。

この点、原告らは、長野県侵入実験において、住基ネットのセキュリティ上の不備が具体的に明らかになった旨主張するが、上記(7)ア(オ)記載の事実によれば、長野県侵入実験の結果は、①インターネット回線を通じてインターネット側FW越しにDMZに設置された公開サーバの管理者権限を奪取することはできなかった、②庁舎内あるいは隣接した施設にある端末から庁内LANに接続した攻撃用コンピュータにより既存住基システムのサーバの管理者権限の奪取に成功したが、庁内LANを通じ市町村設置FW越しにCSないしCS端末の管理者権限奪取はできなかった、③CSセグメント内の端末に接続した攻撃用コンピュータによりCSの管理者権限を奪取し、またCS端末の管理者権限を奪取できたが、住基アプリを任意に操作できるかについては実験を行わなかったというものであって、同実験においては、様々な制約があったとはいえ、設置されているFW越しの攻撃は全て失敗しており(①、②)、また、管理者権限を奪取し得たのは、庁舎内ないし隣接建物において物理的に端末に接続して実験した場合(②、③)であって、当該市町村の職員が許諾しない状態で物理的な庁舎の警備等を回避して端末に接続して攻撃を加えることができるかは実証されていないし、その場合でも、住基アプリを任意に操作できるかについても実証されていない(②、③)から、結局、長野県侵入実験においては、住基ネット内における本人確認情報その他の情報の漏洩、改ざん等の具体的な危険性の存在が証明されたとまでいうことはできない。

なお、品川区において実施された上記ペネトレーションテストについては、同テストの内容の詳細が不明であり、評価を行うことはできない。

(イ) 住基ネットのソフトウェアその他運用面についてみるに、前記のとおり、種々の制度ないし運用基準が定められており、一定の個人情報保護措置が講じられていると評価することができる。

しかしながら、定められた個人情報保護措置が全国3000の市町村で確実に実施されるか疑問であり、次々と発表されるOSのセキュリティーホールに対するパッチを速やかに当てることができるかすら疑問である。また、いわゆるソーシャルエンジニアリングに対する対策が行われていることについては何ら証拠がない。これらは、住基ネットに特有の問題ではなく、すべてのネットワークに共通の問題であるが、住基ネットの扱うデータの量が膨大であり、漏洩したり、改ざんされればその結果は深刻であるだけに、これらの点についても万全の対策をとるべきものである。

(ウ) 以上を総合すると、上記(イ)に示したように疑問はあるものの、本訴において、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、同情報が漏洩する具体的な危険性があることが立証されたとまでいうのは困難である。

(8) 通知、保存、提供の態様が個人の人格的自律を脅かす危険の有無、程度
ア 前提事実で記載したように、住基ネットは、市町村長が本人確認情報を都道府県知事に通知し、都道府県知事が、国の機関や法人、他の都道府県や市町村の執行機関等に対して本人確認情報を提供するものであるが、都道府県知事は、これらの提供事務等を、総務大臣が指定した指定情報処理機関である被告地自センターに委任している(法文上は、「都道府県知事は、指定情報処理機関に本人確認情報処理事務を行わせることができる」と規定されているが、現実には、すべての都道府県知事が被告地自センターに上記事務を行わせている。)

これによって、すべての住民の本人確認情報は、被告地自センターのコンピュータで一元的に保存されるとともに、国の機関や法人、都道府県知事や市町村長に対して提供される。提供される事務は、住基ネットの一次稼働が始まった平成14年8月5日時点では93事務であったが、同年12月6日に成立した行政手続きオンライン化3法によって、264事務に拡大された。提供を受ける事務は、法律及び条例の制定、改正によって、今後も更に拡大されることが予想される。提供される本人確認情報には、住民票コードが含まれている。すなわち、被告地自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る。し

かし、それだけに止まらず、これによって、行政機関が持っている膨大な個人情報データがデータマッチングされ、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される危険性が飛躍的に高まったというべきである。

なお、行政機関では、従前から住民に対して、年金番号、運転免許証番号、健康保険証番号等、様々な番号を付番してきた。しかし、これらの限定された範囲内で使用される番号と異なり、住民票コードは、あらゆる行政事務に利用されるものであるから、従前の番号とは質的に異なるといわなければならない。

また、住民は、住民票コードの記載の変更を請求できる(第2の2の(3)のイ)が、変更してみても、本人確認情報に変更情報が含まれるから、住民票コードのマスターキーの役割に影響を与えない。

イ なるほど、住基法では、本人確認情報の受領者には、当該本人確認情報の提供を求めることができる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利用又は提供をしてはならない旨が定められている(第2の2の(6)のイの(イ)、法30条の34)。しかし、これがデータマッチングや名寄せを禁ずるものであるか否かは文言上判然としない上、仮にそうだとすると、その違反行為に対する罰則は定められていないし、第三者機関の監視のシステムもないから、その実効性は疑わしい。また、行政機関における個人情報の取扱いについては、「行政機関の保有する個人情報の保護に関する法律」が平成17年4月1日から施行されているが、これによれば、行政機関は、特定された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(同法3条2項)が、その利用目的と相当の関連性を有すると合理的に認められる範囲内では利用目的を変更することができる(同法3条3項)し、行政機関の長は、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(同法8条1項)が、行政機関が法令の定める所掌事務の遂行に必要な限度で保有情報を内部で利用する場合であって、当該保有個人情報を利用するについて相当の理由があるとき、あるいは、他の行政機関等に保有個人情報を提供する場合において、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係る個人情報を利用し、かつ、当該個人情報を利用することについて相当な理由のあるときには、当該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る場合を除き、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、又は提供することが許容されている(同法8条2項2号、3号)から、同法も、上記の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。

ウ また、住民が住基ネットの便益を享受するために必要な住基カードは、ICカードで、大容量のデータ蓄積機能があり、氏名、住所、生年月日、性別、住民票コードが記録されている(住基法30条の44第1項、同法施行令30条の12)ほか、公的個人認証アプリケーションがプレインストールされ、更に、市町村長その他の市町村の執行機関は、条例によって、住基カードを様々な目的に使用できる。市町村が提供するサービスとしては、①証明書自動交付機を利用して、住民票の写し、印鑑登録証明書その他の証明書の交付を受けるサービス、②申請書を自動的に作成するサービス、③検診、健康診断又は健康相談の申込、結果の照会等を行うサービス、④事故、急病等で救急医療を受ける場合、あらかじめ登録した本人情報を医療機関等に提供するサービス、⑤災害時等において、避難者情報の登録、避難場所の検索等を行うサービス、⑥公共施設の空き照会、予約等を行うサービス、⑦図書館の利用、図書書の貸出等を行うサービス、⑧健康保険、老人保健等の資格確認を行うサービス、⑨介護保険の資格確認等を行うサービス、⑩高齢者等の緊急通報を行うサービス、⑪病院の診察券等として利用するサービス、⑫商店街での利用に応じ、ポイント情報を保存し、これを活用するサービス、⑬公共交通機関の利用に係るサービス、⑭地域通過、電子福祉チケット等に係るサービス、⑮公共料金等の決済に係るサービス等が考えられている(弁論の全趣旨)。

しかし、住民が住基カードを使って各種サービスを受ければ、その記録が行政機関のコンピュータに残るのであって、これに住民票コードが付されている以上、これも名寄せされる危険がある。なお、上記のとおり、住基カード技術的基準では、条例利用アプリケーションに係るシステムへアクセスするための利用者番号に住民票コードを使用しないことが定められているが、総務省は、

告示の改正によっていつでもこれを改めることができるから、上記危険を否定することはできない。

- エ 行政機関は、住民個々人について膨大な情報を持っているところ、これらは、住民個々人が、行政機関に届出、申請等をするに当たって、自ら開示した情報である。住民個々人は、その手続に必要な限度で使用されるとの認識のもとにこれらの情報を開示したのである。ところが、これらの情報に住民票コードが付され、データマッチングがなされ、住民票コードをマスターキーとして名寄せがなされると、住民個々人の多面的な情報が瞬時に集められ、比喩的に言えば、住民個々人が行政機関の前で丸裸にされるが如き状態になる。これを国民総背番号制と呼ぶかどうかはともかくとして、そのような事態が生ずれば、あるいは、生じなくとも、住民においてそのような事態が生ずる具体的危険があると認識すれば、住民1人1人に萎縮効果が働き、個人の人格的自律が脅かされる結果となることは容易に推測できる。そして、原告らが上記事態が生ずると具体的危険があると認識していることについては相当の根拠があるというべきである。
- (9) (6)ないし(8)の検討の結果によれば、本人確認情報の一部は秘匿を必要とする程度が相当高いし、住基ネットのセキュリティは、不正アクセスや情報漏洩の具体的危険があるとまではいえないものの、抽象的な危険は否定できないものであるし、住基ネットの運用によって個人の人格的自律を脅かす具体的危険があるから、住基ネットの運用によるプライバシーの権利の侵害は、相当に深刻であるというべきである。そこで、これらの事情を踏まえ、住基ネットのシステムを運用することがいかなる場合に許されるかを検討するに、住民が、プライバシーの権利を明示又は黙示に放棄した場合はこれが許されることが明らかであるが、プライバシーの権利を放棄していない住民との関係では、住基ネットの運用によって達成しようとしている行政目的が正当であること、住基ネットを運用することについて、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があることを必要とするというべきである。そして、原告らは、住基ネットからの離脱を求めているプライバシーの権利を放棄していないことが明らかであるから、以下、(10)において、住基ネットの目的の正当性について、(11)において、住基ネットの必要性について検討することとする。
- (10) 住基ネットの目的の正当性について
- ア 被告らが主張する住基ネットの目的は、次の(ア)ないし(エ)のとおりであるので、それぞれについて検討する。
- (ア) 被告地自センターから行政機関に対して本人確認情報が提供されることによる住民負担の軽減と行政事務の効率化
本人確認情報の提供を受ける行政事務は、すでに264事務に及んでいる。これによって、住民側は、申請、届出、住民票の写しの添付等の負担が解消され、行政側としても、事務効率の向上や事務の正確性の向上が実現していることは容易に推測できる。もっとも、住民一人一人の立場から見た場合、これらの負担解消の程度がささやかであることは否定できない。
- (イ) 住民基本台帳事務の簡素化、広域化による住民負担の軽減と行政事務の効率化
住民票の写しの広域交付及び転出・転入手続の簡素化が既に実現している(第2の2の(5))。しかし、住民一人一人の立場から見た場合、住所地市町村以外の市町村で住民票の交付を受けることができるというメリットを享受する機会がどの程度あるか疑問である。また、転入届出の際に転出証明書の添付を要しないとしても、付記転出届をすることが必要であること(住基法24条の2第1項)、従前から転出届の郵送送付、転出証明書の郵送交付を利用して転出市町村に出頭しない方法があったこと、住民が転居する場合には、国民健康保険、介護保険等の様々な手続のために転出地の市町村役場に出向く必要がある場合が多いこと等に鑑みると、そのメリットはさしたるものではない。
- (ウ) 電子政府、電子自治体の基盤(行政手続のインターネット申請の実現)
a 我が国においては、平成9年に内閣により打ち出された「ミレニアム・プロジェクト」により電子政府の基盤構築がなされることとなり、平成12年7月には、いわゆるIT革命の恩恵をすべての国民が享受でき、国際的にも競争力を持つ「IT立国」の形成を目指すため、政府全体での総合的な施策を推進するIT戦略本部が内閣に設置され、同年8月には、自治省に

おける「IT革命に対応した地方公共団体における情報化推進本部」から、各地方公共団体において高度な情報通信技術の便益を最大限活用し、情報化施策を推進するに当たり留意すべき事項について報告がなされ、これらを受け、同平成13年1月6日からは、高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進することを目的として「高度情報通信ネットワーク社会形成基本法」(平成12年法律第144号)が施行された。同法は、高度情報通信ネットワーク社会を形成するために、国には、高度情報通信ネットワーク社会の形成についての基本理念にのっとり、高度情報通信ネットワーク社会の形成に関する施策を策定し、実施する責務を、地方公共団体には、基本理念にのっとり、高度情報通信ネットワーク社会の形成に関し、国との適切な役割分担を踏まえて、その地方公共団体の区域の特性を生かした自主的な施策を策定し、実施する責務を課した。

IT戦略本部は、平成13年3月に発表した「e-Japan重点計画」において、「我が国が5年以内に世界最先端のIT国家となる」ことを目標に掲げ、同年6月に「e-Japan2002プログラム」、同年11月に「e-Japan重点計画、e-Japan2002プログラムの加速・前倒し」、平成14年6月に「e-Japan重点計画-2002」を発表し、平成15年8月8日には「e-Japan重点計画-2003」を発表するなど、政府の行うべき施策を定めた各種計画を策定し、政府においてその実施がなされている。

上記「e-Japan重点計画-2003」においては、行政サービスとして、行政に関する手続につき、365日24時間ノンストップで、関連手続の申請・届出等の案内情報の入手から実際の手続までをインターネットにより一元的に行うことのできる総合的なワンストップサービスの仕組みを平成17年度末までに整備することを目標として掲げている。(乙5, 6, 弁論の全趣旨)

- b 公的個人認証サービスについては、既に「電子署名に係る地方公共団体の認証業務に関する法律(平成14年度法律第153号、以下「公的個人認証法」という。)が施行されている。これによると、公的個人認証サービスの都道府県センターでは、住基ネットから異動等失効情報の提供を受け(同法12条)、これによって失効リストを作ることができ、行政機関は、オンラインでの申請、届出等を受け取った際に、失効リストに照会することによって失効していないことの確認をすることができる(同法18条1項)。また、公的個人認証サービスの電子署名に用いる秘密鍵等の格納媒体として住基カードが利用されることとされている。
- c IT立国は、我が国の国家戦略であり、インターネットの急速な普及という社会情勢の中で、行政手続における申請、届出のオンライン化の推進は大きな政策課題であるということができるところ、その基盤の一つとしての公的個人認証サービスにおいて住基ネットが重要な役割を果たしているということが出来る。しかしながら、都道府県センターが失効情報を把握するためには、住基ネットを介さなくとも、市町村から直接提供を受ければ足りるし、電子署名の格納媒体は住基カードである必要はないから、公的個人認証サービスに住基ネットが不可欠であるとは言い難い。しかも、外国人や、オンライン申請、届出の必要性が高いと思われる企業には住基ネットシステムは使えないから、これらについては別なシステムを使う必要があること、既に「電子署名及び人証業務に関する法律」も制定されていて、オンライン申請、届出に民間事業者が発行する電子証明書を使うことが可能であること等を併せ考えると、オンライン申請、届出のために、公的個人認証サービスが必要不可欠であるとも言い難い。もっとも、公的個人認証法17条1項で、民間の認定認証事業者が行う特定認証業務に係る本人確認に公的個人認証サービスが活用できるとされたから、公的個人認証サービスが民間認証事業のインフラとしての役割を果たすこととなったということとはできる。

(エ) 住基カードによる住民の便益

被告は、住基カードには様々なメリットがあると主張する。すなわち、住基カードは、公的個人認証アプリケーションがプレインストールされ、電子証明書及び秘密鍵の格納媒体になるが、更に、市町村が条例で定めることにより前記のように多目的カードとして利用でき、また、上記4情報、住民票コ

ードによって本人確認がスピーディかつ確実に行うことができるというのである。

なるほど、利用の方法によっては様々な用途に使い、住民にとっても便利であるが、必要があれば、各自治体でカードを作ればよいのであって、全国共通規格のICカードでなければならない理由は判然としない。

イ 以上を総合すると、住基ネットの目的については、様々な疑問もないではないが、一応の理由はあり、正当なものと評価できないではない。

しかしながら、その目的は、詰まるところ「住民の便益」(アの(ア)ないし(エ))と「行政事務の効率化」(アの(ア)ないし(ウ))であるところ、「住民の便益」とプライバシーの権利は、いずれも個人的利益であり、そのどちらの利益を優先させて選択するかは、各個人が自らの意思で決定すべきものであり、行政において、プライバシーの権利よりも便益の方が価値が高いとして、これを住民に押しつけることはできないというべきである。すなわち、便益は、これを享受することを拒否し、これよりもプライバシーの権利を優先させ、住基ネットからの離脱を求めている原告らとの関係では、正当な行政目的たり得ないといわざるを得ない。

次に、「行政事務の効率化」についていえば、これは、行政にとって重要な政策課題であって、昨今の国及び地方自治体の厳しい財政事情やIT技術の急速な発展に伴って世界的規模で生じている社会経済構造の変化に適確に対応する必要があること等に照らせば、正当な行政目的であることは肯認できる。

(11) 住基ネットの必要性について

ア そこで、正当な行政目的であると認められる「行政事務の効率化」に関し、その必要性について検討するに、行政事務の効率化とは、突き詰めれば経費削減であるということが出来るが、証拠及び弁論の全趣旨(各項末尾に記載)によれば、住基ネットの運用についての経費削減効果に関して、次の事実が認められる。

(ア) 総務省自治行政局市町村課は、平成14年10月31日付で、住基ネットシステムの構築に要する経費概要を試算したが、これによれば、住基ネットの導入にあたり、平成11年度から平成15年度に必要とされる経費の累計額は、総額390億9300万円、うち都道府県負担分が28億5100万円、市町村負担分が306億6600万円であり、その後の住基ネットの運用経費は、年間総額が190億3600万円、うち都道府県負担分が68億6800万円、市町村負担分が87億8100万円とされている。(弁論の全趣旨)

(イ) 被告国は、平成10年3月時点において、住基ネット導入により、1年間に住民が受ける利益、同じく行政側が受ける利益について、次のような試算をした。(弁論の全趣旨)

a 行政側

住民の転入手続きについて、転入者の半数が住基カードの所持者として特例による転入手続きをなすとして、その簡素化によって人件費が約18.7億円、ネットワークによる市町村間の連絡等による省力化により人件費等の経費が約31億円それぞれ節約できる。

住民票の写しの交付の省略等による窓口業務の簡素化として、1000万件が省略できるとして、人件費が約60億円節約でき、これに伴い、国の事務においても、人件費が約30億円節約できる。

公的個人認証サービスのための新たなカードシステム開発を行わずにすむことにより、カードシステムのリース料として約25.1億円、開発費及び更新費用として約67.9億円が節約できる。

b 住民側

転入手続きの簡素化により、住民が節約できる時間を1時間あたり1000円で計算し、更に節約できる交通費と加算すると、約32.1億円の節約になる。

住民票写しの広域交付により、その利用者数を、域外通勤通学者3070万人の半分として、節約できる時間を同様に金銭評価し、これと交通費を合算すると、約98.5億円になる。

住民票の交付の省略等により節約できる時間を同様に金銭評価し、これと交通費を合算すると、約136.7億円になる。

(ウ) 長野県は、平成16年2月、同時点における住基ネットの運用状況をふ

まえ、平成15年から同29年までの間における住基ネットの導入により行政側及び住民側が受ける費用対効果を、県内の自治体を人口規模別に4つに区分し、今後の本人確認情報の利用事務の拡大に伴う住民票の写しの省略数等の増加を予想して試算した。これによると、行政側は、業務簡素化による時間の節約よりも、住民票の写しの省略による手数料の減額の方が大きく、恒常的に損失が予想され、他方、住民側は、住民票の写しの交付を受ける時間の節約等による利益が大きいと、これらに住基ネットの維持、機器の更新のための経費を加えると、その累計は、平成18年度までは損失であり、平成19年度から利益に転ずる、しかし、平成11年度から要した初期投資を加えると、平成29年度末においても、なお累計はマイナスであるとの結果となった。(甲共24の2)

イ アの(イ)に記載した被告国の試算は、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、住基カードの現実の普及率(第2の2の(7))に鑑みると、参考に値しない。アの(ウ)に記載した長野県の上記試算によれば、行政側及び住民側を総合した費用対効果は、長期的に見れば利益を生ずる可能性があるが、行政側だけでみると、恒常的に損失が予想されており、経費削減には役立たないという結果になっている。もっとも、これも住民票の写しの省略数等は予想値を使っており、その信頼性は定かではない。

ウ 以上を総合すると、住基ネットは、長期的に見て、住基カードが幅広く普及し、提供事務が大幅に拡大すれば経費削減効果が期待できないとまではいえないが、その効果の程度は未知数といわざるを得ない。経費削減のためには、適切な人員配置、必要性の乏しい公共事業の縮小、その他行政全般にわたって様々な改革の努力が必要であり、住基ネットにその効果があるとしても、それはその一翼を担うものにすぎないし、住基ネットがなければ達成できないものとも考えがたい。また、電子政府、電子自治体の実現は、短期的な経費削減効果の有無を超えた価値を持つというべきであるが、そのために住基ネットが必要不可欠とまで言えないことは前記のとおりである。

そうすると、「行政事務の効率化」自体は正当な行政目的であるが、住基ネットが住民のプライバシーの権利を犠牲にしてまで達成すべき高度の必要性があることについては、ただちにはこれを肯認できない。

ところで、原告らは、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。原告らが住基ネットから離脱しても、住基ネットの運用は続くのであって、これによって住基ネットの目的の完全な達成が阻害されるとはいえ、その目的の相当程度は達成できるのである。したがって、原告らのプライバシーの権利と比較衡量するのは、住基ネットの運用の必要性ではなく、希望者の離脱を認める住基ネットでは足りず、住民基本台帳に記録されている者全員を強制的に参加させる住基ネットでなければならぬ必要性であると捉えるべきである。そして、そう捉えた場合、その必要性は、行政コスト削減の所期の目的を全うすること、離脱者の把握のために要するコストを回避すること等に限定されると考えられるが、これらが、原告らのプライバシーの権利を犠牲にしてもなお達成すべきものとは到底評価することができない。

(12) 以上の検討の結果によれば、住基ネットは住民に相当深刻なプライバシーの権利の侵害をもたらすものであり、他方、住民基本台帳に記録されている者全員を強制的に参加させる住基ネットを運用することについて原告ら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あると認めることはできないから、自己のプライバシーの権利を放棄せず、住基ネットからの離脱を求めている原告らに対して適用する限りにおいて、改正法の住基ネットに関する各条文は憲法13条に違反すると結論づけるのが相当である。

(13) 差止め請求の許容性について

ア 明示的に住基ネットからの離脱を求めている原告らに対して改正法の住基ネットに関する各条文を適用することは憲法に違反する。すなわち、原告らとの関係では、改正法の上記各条文は無効であるから、被告県及び被告地自センターは、法令上の根拠なく、原告らの本人確認情報を通知、保存、提供していることとなる。

イ ところで、住基ネットからの離脱を求める原告らが、被告県及び同地自センターに対して具体的に求めているのは、次の行為である。

(ア) 被告県に対し

- a 国の機関及び法人に対して原告らの本人確認情報を提供する行為の差止め
- b 被告地自センターに対して原告らに関する本人確認情報処理事務を委任する行為の差止め
- c 被告地自センターに対して原告らの本人確認情報を通知する行為の差止め
- d 原告らの本人確認情報を磁気ディスクから削除すること

(イ) 被告地自センターに対し

- a 原告らに関する本人確認情報処理事務の差止め
- b 原告らの本人確認情報を磁気ディスクから削除すること

ウ 原告らが差止めを求めている行為(イの(ア)のaないしc, (イ)のa)は、行政機関ないし行政機関から行政権限を付与された私人の行為であり、法律に基づく行為であるが、国民の権利義務を形成し、またはその範囲を具体的に確定する行政行為ではなく、事実行為であり、行政事件訴訟の差止めの訴えによっては救済できないものであると解せられるから、民事訴訟において差止めを求めることができると解せられる。また、イの(ア)のd, (イ)のbは作為を求めるものであるが、実質は差止めを実効あるものにするための原状回復行為であるから、差止め請求と同様に求めることができるものと解せられる。

エ 被告県及び同地自センターは、法令上の根拠なく、原告らの個人識別情報を通知、保存、提供しているのであるから、原告らの権利を保護するために必要があり、これを差し止めることによって被告らの行政事務の遂行上特段の不都合が生じない限り、人格権の一つであるプライバシーの権利に基づき差止めを求める原告らの請求を認容すべきである。そして、原告らのプライバシーの権利は、原告らの本人確認情報が住基ネットに通知、保存され、住基ネットから提供され、あるいは提供されようとしていることによって侵害されているのであるから、これを保護するために原告らが請求している差止めを認める必要があるというべきである。他方、被告らの行政事務の遂行上の特段の不都合があることについては、被告らは、非通知申出者の把握に多大なコストがかかり、上記の住基ネットの目的を阻害すると主張するが、これが特段の不都合とまでは認められず、他に、不都合がある事実を認めるに足る証拠はない。

オ 以上の次第で、争点(2)について検討するまでもなく、原告らの被告県及び被告地自センターに対する各差止め請求を認容するべきである。

2 被告県及び同地自センターが住基ネットを運用したことが違法か(争点(3))

(1) 国家賠償法1条1項は、国又は地方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反して当該国民に損害を加えたときに、国又は公共団体がこれを賠償する責に任ずることを規定するものである。

ところで、被告県の谷本知事は、地方自治体の執行機関として、住基法に従って住基ネットを運用したものである。公務員が法律にしたがって職務行為に及んだ場合に、その行為が国家賠償法上違法と評価されるのは、その法律が憲法に違反して無効であることが誰の目にも明らかであるという特段の事情がある場合に限られるというべきである。改正法については、国民各層に、憲法違反であるとの意見から積極的に推進すべきであるとの意見まで、様々な意見があり、当裁判所は、離脱を表明する者の本人確認情報を通知、保存、提供する限度で憲法に違反すると考えるものであるが、これが憲法違反であることが誰の目にも明らかであるとは到底認めることができない。

よって、住基ネットを運用した谷本知事の行為が国家賠償法上違法であるということはできない。

(2) 被告地自センターは、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、各都道府県知事から委託された事務及び同法に定められた事務を同法の定めるところにより行ったものである。当裁判所は、被告地自センターが住基法30条の10に基づいて原告らの本人確認情報を国の機関の法人等へ提供したのであれば、その行為を違法と判断するものであるが、被告地自センターとしては、上記提供をしたとしても、そのことを認識できなかったものと考えられる。そうすると、被告地自センターに故意過失を認めることができず、被告地自センターが原告らの本人確認情報を国の機関等へ提供した行為が原告らに対する不法行為になると認めることはできない。

3 被告国が改正法を施行したことが違法か(争点(4))

改正法附則1条2項には、「この法律の施行に当たっては、政府は、個人情報の保護に万全を期するため、速やかに、所要の措置を講ずるものとする。」との規定がもうけられが、他方、附則1条柱書には、一部の規定を除いて、公布の日から日から起算して3年を超えない範囲内において政令で定める日から施行することが定められた。すなわち、これらはいずれも立法府の意思だったのであり、3年が近づいても「所要の措置」が講じられていない場合、どちらを優先するかは、立法府が定めるべきことである。そして、第154回国会で「住民基本台帳法の一部を改正する法律の一部を改正する法律案(第154回国会衆法37)」が提出され、これが廃案になった(弁論の全趣旨)から、立法府は、「所要の措置」を講ずることよりも、公布の日から起算して3年以内に施行することを優先したと考えざるを得ない。

そうすると、立法府は、附則1条柱書の施行日を平成14年8月5日と定めた平成13年12月政令430号を認めたというべきであるから、その施行に関与した小泉内閣総理大臣の行為が国家賠償法上違法と評価されるいわれはない。

4 結論

以上によれば、原告らの被告県に対する、住基法第30条の7第3項別表第一の上欄に記載する国の機関等に対する原告らの本人確認情報提供の差止めの請求、被告地自センターに対する原告らの本人確認情報処理事務の委任の差止めの請求、被告地自センターに対する原告らの本人確認情報の通知の差止めの請求及び原告らの本人確認情報について住基ネットの磁気ディスクからの削除の請求、並びに原告らの被告地自センターに対する、原告らの本人確認情報処理事務の差止めの請求及び原告らの本人確認情報について住基ネットの磁気ディスクからの削除の請求は、いずれも理由があるから認容し、原告らが被告県及び同国に対して求めた国家賠償請求及び被告地自センターに対して求めた不法行為に基づく損害賠償請求は、いずれも理由がないから棄却し、訴訟費用について民訴法61条、64条、65条1項を適用して主文のとおり判決する。

金沢地方裁判所第二部

裁判長裁判官 井 戸 謙 一

裁判官 村 山 智 英

裁判官野村賢は転補のため署名押印することができない。

裁判長裁判官 井 戸 謙 一