

平成18年12月11日判決言渡 同日原本領収 裁判所書記官

平成17年(ネ)第154号 住民基本台帳ネットワーク差止等請求控訴事件

(原審：金沢地方裁判所平成14年(ワ)第836号，平成15年(ワ)第114号)

口頭弁論終結の日 平成18年6月12日

判 決

当事者の表示 別紙当事者目録記載のとおり

主 文

- 1 原判決中，控訴人ら敗訴部分を取り消す。
- 2 被控訴人らの請求をいずれも棄却する。
- 3 訴訟費用は，第1，2審とも，被控訴人らの負担とする。

事実及び理由

第1 当事者の求めた裁判

1 控訴人ら

主文第1，2項と同旨

2 被控訴人ら

本件各控訴をいずれも棄却する。

第2 事案の概要

- 1 本件は，控訴人石川県内の市町村に住民登録をしている被控訴人らが，平成11年法律第133号による改正後の住民基本台帳法に基づく住民基本台帳ネットワークシステムの導入により，被控訴人らのプライバシー権（自己情報コントロール権），氏名権及び行政権力による包括的管理からの自由が侵害されたとして，上記各権利に基づき，(1)控訴人石川県に対し，①住民基本台帳法30条の7第3項の別表第一の上欄に掲げる国の機関及び法人に対する，被控訴人らに関する本人確認情報（被控訴人らの氏名，住所，生年月日，性別の4情報及び被控訴人らに付された住民票コード並びにこれらの変更情報）の提供禁止，②控訴人財団法人地方自治情報センターに対する，被控訴人らに関する

同法30条の10第1項記載の本人確認情報処理事務の委任禁止、③控訴人財団法人地方自治情報センターに対する、被控訴人らに関する上記本人確認情報の通知禁止、④その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。）からの被控訴人らに関する上記本人確認情報の削除を請求し、(2)控訴人財団法人地方自治情報センターに対し、⑤控訴人石川県から受任した被控訴人らに関する住民基本台帳法30条の10第1項記載の本人確認情報処理事務の禁止、⑥その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の被控訴人らに関する上記本人確認情報の削除を請求するとともに、(3)控訴人らに対し、⑦控訴人石川県に対しては国家賠償法1条1項に基づき、控訴人財団法人地方自治情報センターに対しては民法709条に基づき、それぞれ、慰謝料10万円及び弁護士費用1万円の合計11万円並びにこれに対する訴状送達日の翌日（被控訴人■■■■■及び被控訴人■■■■■につき平成15年4月1日、その余の被控訴人らにつき同年1月17日）から支払済みまで民法所定の年5分の割合による遅延損害金の連帯支払を求めた事案の控訴審である。

原審は、被控訴人らの上記①ないし⑥の各請求をいずれも認容し、上記⑦の請求を棄却したところ、控訴人らが本件控訴を提起した。したがって、上記⑦の請求は当審における審判の範囲外である。

なお、略語は、控訴人財団法人地方自治情報センターを「控訴人センター」とするほか、特に断らない限り、原判決に準ずるものとする。

2 前提事実

次の(1)のとおり補正するほかは、原判決の事実及び理由の第2、2に記載のとおりであるから、これを引用するが、次の(2)及び(3)において改正法の概要及び住基ネットの概要を要約摘示する。

(1) 原判決の補正

ア 原判決11頁17、18行目の「拡大された。」を「拡大され、現在（

当審の口頭弁論終結日)では275事務となっている。」と改める。

イ 原判決22頁13行目と同14行目との間に次のとおり加える。

「なお、横浜市は、平成18年5月10日、横浜市本人確認情報等保護審議会から、住基ネットの安全性が稼働当初と比較して格段に高まっており、現時点において問題はない旨の同年4月付け答申を受けて、横浜市の住民全員について住基ネットに参加することを表明した(乙59, 60)。」

(2) 改正法の概要

住民基本台帳法は、改正法(平成11年法律第133号)により次のとおり改正された。

ア 都道府県知事は、その区域内の市町村の市町村長ごとに、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(住基法7条13号)を指定し、これを当該市町村長に通知する(住基法30条の7第1項)。市町村長は、新たにその市町村の住民基本台帳に記録されるべき者につき住民票の記載をする場合において、その者がいずれの市町村においても住民基本台帳に記録されたことがない者であるときは、都道府県知事から指定された住民票コードのうちから選択するいずれかの1つの住民票コードを住民票に記載する(住基法30条の2第2項前段)。都道府県知事は、指定情報処理機関に上記住民票コードの指定及びその通知を行わせることができる(住基法30条の10第1項1号)。都道府県知事及び指定情報処理機関は、本人確認情報を磁気ディスクに記録し、これを所定の期間保存する(住基法30条の5第3項, 30条の11第3項)。

イ 市町村長は、都道府県知事に本人確認情報を通知する(住基法30条の5)。

ウ 都道府県知事は、住基法の定める場合に、住基法所定の国の機関・法人等へ本人確認情報を提供する(住基法30条の7)。

エ 都道府県知事は、指定情報処理機関に対し、国の機関・法人等への本人

確認情報の提供等の本人確認情報処理事務を委任することができる（住基法30条の10第1項）。

オ 委任都道府県知事は、本人確認情報を指定情報処理機関に通知する（住基法30条の11第1項）。

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

キ 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（改正法附則1条2項）。

(3) 住基ネットの概要

改正法は、平成13年政令第430号により平成14年8月5日から施行され、被控訴人らの各居住する、控訴人県内の各市町村においても、住基ネット（住民基本台帳ネットワークシステム）が導入された。その概要は次のとおりである。

ア 被控訴人らの居住する市町村の長は、住基法に基づき、被控訴人らの住民票を作成し、氏名、住所、生年月日、性別等の個人情報を電子計算機（以下「サーバ」という。）に記録し、管理している。改正法により、控訴人県の知事から委任を受けた控訴人センターは、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市町村長に通知し、市町村長は、指定された住民票コードのうちから選択するいずれか1つの住民票コードを住民票に記載した。市町村は、被控訴人らに関する個人情報が記録された既存のサーバを住基ネット専用のコミュニケーションサーバ（以下「CS」という。）に接続し、これを電気通信回線を通じて控訴人県のサーバに接続した。これにより、被控訴人らの居住する市町村の長は控訴人県の知事に、同知事は控訴人センターに、本人確認情報を通知している。控訴人センターは、住基法の定める場合に、住基法所定の国の機関・法人等に

対して本人確認情報を提供している。

イ 控訴人県は、自己のサーバを電気通信回線を通じてＣＳに接続し、通知された本人確認情報を自己のサーバの磁気ディスクに記録して保存するとともに、控訴人県の知事が事務を委任した控訴人センター（控訴人センターは、総務大臣から住基法３０条の１０第１項の「指定情報処理機関」の指定を受けている。）に対し、本人確認情報を通知した。これにより、控訴人センターは、住基法の定める場合に、住基法所定の国の機関・法人等に対し、本人確認情報を提供している。

ウ 控訴人センターは、控訴人県の知事から電気通信回線を通じて各市町村長から通知された本人確認情報の通知を受け、その情報を磁気ディスクに記録し、所定期間保存するとともに（住基法３０条の１１第１項、３項）、通知を受けた本人確認情報を国の機関又は法人等に提供する業務を行っている。

エ 被控訴人らの居住する各市町村長は、平成１４年８月５日以降、被控訴人らに対し、住民票コードを通知し、同日から住基ネットの本運用が開始された。

３ 当審における争点及びこれに関する当事者の主張

(1) プライバシー権（自己情報コントロール権）侵害の有無

次のとおり補正するほかは、原判決の事実及び理由の第３、３(1)に記載のとおりであるから、これを引用する。

(原判決の補正)

ア 原判決２９頁１９行目から３０頁３行目までを次のとおり改める。

「(ウ) 上記各情報のうち、氏名、住所、生年月日及び性別の４情報はそれ自体が重要な情報であるというだけではなく、その下に記録保存等された個人情報に分け入っていく上での索引・検索情報として機能するものであるから、要保護性が高い。変更情報も、身分上の重要な変動が生じた

ことを推知させるものとして要保護性が高い。そして、簡便かつ正確に個人情報を検索できるマスターキーとなり得る住民票コードが付されることにより、一体とされた個人情報が全国ネットワークである住基ネット上に流通させられることにより、被控訴人らのプライバシーが侵害され、又はその侵害の具体的危険にさらされることになる。」

イ 原判決 37 頁 8 行目と同 9 行目との間に次のとおり加える。

「そもそも被控訴人らは、住民票の写しの広域交付という利便性よりも、自らのプライバシーの権利の保持を望むのであるから、このような被控訴人らに対し、住民の利便性を根拠として住基ネット導入の必要性を基礎付けることはできない。」

ウ 原判決 37 頁 11 行目の「すぎない。」を「すぎず、その利用率も極めて低いから、住基カードが有用であるとはいえない。」と改める。

エ 原判決 37 頁 22 行目と同 23 行目との間に次のとおり加える。

「控訴人らは、被控訴人らが住基ネットに参加しないことによる支障につき、原審裁判所から再三にわたり求釈明を受けたにもかかわらず、必要がないものとして、何ら主張しない応訴態度に終始していたのであるから、そのような控訴人らが、当審になってこの点に関する主張をにわかに行うことは禁反言の法理に反する。仮にそうでないとしても、控訴人らの主張する、被控訴人らが住基ネットから離脱することによって生じる支障とは、極めて抽象的なものであるばかりか、いずれも住基ネットの運用を開始してしまったことを前提とするところ、被控訴人らが住基ネットの運用の中止を求めたにもかかわらず、これを強行したのであるから、自らの強行によって築いたシステム等に支障が生じることを根拠に住基ネットの正当性を基礎付けることはできず、また、住基ネット自体が許容されるか否かが問われているにもかかわらず、これを予め正しいものとして前提とする立論であるから、控訴人らの主張は失当であ

る。

(カ) 以上によれば、改正法中住基ネットに関する規定は、少なくとも住基ネットに不参加を表明し、あるいは住基ネットからの離脱を表明して、本人確認情報の提供に同意していない住民に適用し、これを運用する限り、憲法13条に違反して無効である。」

オ 原判決37頁24行目と同25行目との間に次のとおり加える。

「被控訴人ら主張の自己情報コントロール権なる権利は、実定法上の根拠がなく、また、実質的に考えても、その内容、範囲、法的性格に関して様々な見解があり、権利としての成熟性が認められないから、実体法上の権利とはいえない。また、住基法は、住基ネットの運用により、被控訴人らの権利が侵害されることのないよう十分な立法措置を行っており、行政機関とその構成員たる公務員も法令の遵守義務を負うのであるから、住基ネットの運用により被控訴人らの権利が侵害され、その侵害の程度が重大で、被控訴人らが回復困難な損害を被るおそれがあるとはいえないから、被控訴人らの差止等請求は棄却されるべきである。その具体的な主張は次のとおりである。」

カ 原判決40頁1行目の「プライバシー侵害の事実」を「プライバシーの侵害又はその具体的危険の不存在」と改める。

キ 原判決40頁6行目末尾に次のとおり加える。

「そもそも、被控訴人ら主張の本人確認情報のうち4情報（氏名、住所、生年月日及び性別）は、社会通念上、秘匿を要する程度が高いとはいえないし、住民票コード及び変更情報についても、前者は住民票に付された11桁の数字であり、後者も上記4情報が変更した旨の情報であって、およそ個人の人格的自律などにかかわらない客観的・外形的事項に関するものであって、思想、信条など個人の道徳的自律に係る人格権の内容を成すものではないから、これらの本人確認情報について被控訴人らのプライバ

シー権を侵害するものとはいえず、その具体的危険も存在しない。」

ク 原判決４０頁１３行目の「いえない。」を「いえず、その具体的危険も存在しない。」と改める。

ケ 原判決４３頁１５行目の「講じており」から同１７行目の「よって」までを「講じているから」と、同１８行目の「危険性」を「具体的危険性」と、それぞれ改める。

コ 原判決４７頁４行目から同１７行目までを次のとおり改める。

「(カ) 被控訴人らが住基ネットから離脱することによって生ずる支障

住基法は、住基ネットのシステム上ですべての本人確認情報がもれなく提供、利用されることを当然の内容として立法されており、住基ネットが、国の機関等、都道府県、市町村で本人確認情報を共有することにより、行政コストの削減等を図ることを一つの重要な行政目的としているのであって、一部でも不参加があると、本人確認情報の共有がなされなくなるから、国の機関等などにおいて、従来のシステムや事務処理を存置せざるをえないこととなり、法の予定する効果を達成することは不可能になる。また、住基ネットは、市町村間をネットワーク化し、住民基本台帳事務の広域化、効率化を図ることを一つの重要な行政目的としているところ、不参加者を認めることになれば、上記ネットワークが寸断され、他の市町村の効率化が阻害されていることは明らかである。このような事態は法のおよそ想定するところではなく、情報通信技術を利用して住民サービスの向上と行政事務の効率化を図ることを目的とした改正法の意義を没却し、住基ネットの存在そのものを否定することになる。

したがって、被控訴人らが住基ネットから離脱することにより重大な支障が生ずる。」

(2) 氏名権侵害の有無

(被控訴人らの主張)

ア 氏名は、人の同一性を示すものとして人格と密着するものであるから、氏名により呼称され、氏名によって扱われることは、氏名権として憲法13条により保障される。

イ 住基ネットは、個人の情報を住民票コードという番号をもとにして流通させ、個人の特定を氏名ではなく番号によって行うものであり、また、異なる行政分野にまたがり番号が共通化されることと相まって、行政担当者は個人の氏名よりも番号を重視することになり、個人の人格の同一性を表す中核となる氏名を住民票コードで分類される個人情報の一つにおとしめるものである。さらに、個人を番号によって扱うこと、特に全国民に住民票コードをその生涯にわたって付すことは、氏名を中核とする個人のアイデンティティ又はその感覚を害するものである。したがって、住基ネットは被控訴人らの氏名権を侵害する。

(控訴人らの主張)

争う。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、およそ被控訴人らの人格権も人格的利益も侵害したとはいえないから、被控訴人らの上記主張は失当である。

(3) 公権力による包括的管理からの自由侵害の有無

(被控訴人らの主張)

ア 国民個人は、他人によって自己の人格的自律に関わる個人情報を収集さ

れないこと、又はその他の個人情報から自己の人格的自律に関わる個人情報
を推知されないことを前提として、その理性又は感性等に主体的に従っ
て自己決定をなすことができ、自由に行動することができる。ところが、
公権力による包括的管理（各行政機関において、それぞれ個別に保有する
国民個人に関する情報を、他の行政機関と交換する等して有機的に結合し、
いつでも利用できる状態におくこと）は、このような個人の基本的な意思
決定や行動（特に公権力にとって不都合な思想、公権力に対する批判的行
動等）を著しく萎縮させることになるから、人格的自律の存在として自己
を主張し、そのような存在であり続ける上で必要不可欠な利益として、公
権力による包括的管理からの自由も、憲法13条により保障される。

イ 住基ネットにおける住民票コードは、全国民を確実に識別するために付
されたものであり、また、今後、住民票コードの利用が可能な事務が無限
定に拡大されていくことが予想され、個人の全生活分野において住民票コ
ードを基点として様々な個人情報が蓄積され、かかる個人情報を公権力が
事実上無制限な利用目的をもって一元的に管理することを可能とするもの
である。したがって、住基ネットは、被控訴人らの公権力による包括的な
管理からの自由を侵害する。

（控訴人らの主張）

争う。被控訴人らは、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にのみ利
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。

(4) 被控訴人らの請求に係る差止等の必要性、許容性の有無

(被控訴人らの主張)

住民個々人は、自己に関する個人情報の収集・取得、管理（保有）・利用、開示・提供のすべてにつき、情報主体としてコントロールする権利を有するのであるから、情報主体の同意も法令上の根拠もないまま、行政機関がこれを違法に占有している場合には、その原状回復を請求できるところ、被控訴人らの情報が住基ネットに提供される限り、被控訴人らの権利の侵害という違法状態が継続しているのであるから、被控訴人らは、この違法状態からの回復として差止等請求ができる。

(控訴人らの主張)

争う。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請求を認めることはできない。仮にそうでないとしても、差止請求が認められるためには、差止請求の根拠となる権利侵害の程度が重大であり、権利者が著しく回復困難な損害を被るおそれがあることが必要であるところ、住基ネットの導入により、被控訴人らの権利が侵害される具体的危険は存在しないから、被控訴人らが著しく回復困難な損害を被るおそれがあるとはいえず、被控訴人らの請求に係る差止等の必要性も

ない。

第3 当裁判所の判断

1 認定事実

前記前提事実並びに証拠（乙28，後記各証拠）及び弁論の全趣旨によれば，住基ネットに関して，次のとおり認められる。

(1) 住基ネットの目的等

住基ネットは，住民サービスの向上と行政事務の効率化を目的として設けられたシステムであり，大別して次の実現事項を予定している。

ア 市町村の区域を越えた住民基本台帳に関する事務の処理

(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，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住基法7条5号，9号から12号まで及び14号に掲げる事項の記載を省略したものの交付を請求できる（住基法12条の2第1項）。この請求を受けた市町村長は，住所地市町村長との間で，電気通信回線を通じて各使用に係る電子計算機に必要事項を送信通知し，住民票の写しを作成し，交付する（同条第2項ないし第5項）。このように，住基カードなどを窓口で提示することにより，全国どこの市町村でも，本人や世帯の住民票の写しの交付が受けられるようになる。

(イ) 転入・転出の特例処理

転入届をする者は，前住所地の市町村長が作成する転出の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），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が，住基カードの交付を受けている者が付記転出届をした場合には，最初の転入届については，転出証明書の添付を要しない（住基法

24条の2第1項)。つまり、住基カードの交付を受けている場合は、他の市町村に引っ越したときでも、付記転出届を転出地市町村に郵送すれば、転出地市町村の窓口に出向いて転出証明書を受け取る必要がなく、転出証明書に記載されている情報を電子情報として市町村間で送信するので、転入地市町村窓口で1回出向いて住基カードを添えて転入届を提出することで足りる。

イ 法律で定める行政機関（国、地方公共団体等）に対する本人確認情報の提供

住基ネットにおいて、法律で定める行政機関（国、地方公共団体等）に対して本人確認情報が提供されることにより、各種手続の簡素化が図られる。たとえば、①住基法別表に規定されている本人確認情報の提供及び利用が可能な多数の事務について、住民票の写しの提出が不要となり、②共済年金（地方公務員、国家公務員、私立学校教職員）、戦没者遺族等援護年金の受給者が、毎年提出していた現況届又は身上報告書の提出が、加給年金額対象者等を除き、不要となり、③毎年、市町村長の証明印を受けて受給権調査申立書を提出する必要があった恩給受給者は、同申立書の提出が不要となる。

ウ 住基カードの活用

- (ア) 住基カードの交付を受けると、上記アの住民票の写しの広域交付や転入・転出の特例処理が利用できる。
- (イ) 市町村が条例で定めるところにより、カードメモリの空き領域を活用して必要な情報を記録し、印鑑登録証明事務、福祉サービス、公共施設の利用予約等、多目的に独自の行政サービスを行うことができる。
- (ウ) 市町村等の窓口において、住基ネットを通じて、居住する市町村の住民であることを確認できる。
- (エ) 写真付きの住基カードは、市町村民証明書として活用することが可能

となる。

(㊦) 電子政府、電子自治体の基盤となること

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、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）。

- (カ) 今後も、公的個人認証サービスに活用したり（電子署名に係る地方公共団体の認証業務に関する法律参照）、申請・届出等手続のオンライン化に活用することが可能となる。

(2) 個人情報保護のための対策等

住基ネットは、住民の個人情報を取り扱うことから、個人情報の保護が重要な課題とされており、制度面、技術面及び運用面にわたり、次のような個人情報保護のための対策が講じられている。

ア 制度面

(ア) 保有情報の制限

都道府県、指定情報処理機関が保有する情報は本人確認情報に限定されている（住基法３０条の５第１項）。

(イ) 本人確認情報の利用及び提供の制限等

本人確認情報の提供を受ける行政機関の範囲や利用目的も限定されている（住基法３０条の６，３０条の７第３項ないし第６項，３０条の８，別表）。また、本人確認情報の提供を受ける者に対し、目的外の利用又は提供が禁止され（住基法３０条の３４。この規定は、行政機関の保有する個人情報の保護に関する法律８条３項により、同条２項に優先して適用されるものである。），都道府県知事及び指定情報処理機関に対し

ても、法律の規定によらない本人確認情報の利用及び提供が禁止されている（住基法３０条の３０）。さらに、市町村長その他の市町村の執行機関は、住基法に規定された事務等で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、遂行のため必要のある場合を除き、住民票コードの告知を求めることが禁止されている（住基法３０条の４２）。

市町村長等以外の者は、何人も、自己と同一の世帯に属する者以外の者に対し、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たり、その者が業として行う行為に関し、その者に対し売買、貸借、雇用その他の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たり、業として、住民票コードの記録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たりすることが、いずれも禁止されている（住基法３０条の４３第１項ないし３項）。

(ウ) 秘密保持義務

役職員等（住基法３０条の１７第１項第２項）、本人確認情報の電子計算機処理等に従事する市町村又は都道府県の職員等（住基法３０条の３１第１項第２項）、本人確認情報の電子計算機処理等に従事する受領者の職員等（３０条の３５第１項ないし第３項）、住民基本台帳に関する調査に関する事務に従事している者又は従事していた者（住基法３５条）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して知り得た秘密を漏らしてはならないこととされ、各秘密保持義務に違反して秘密を漏らした者に対しては、

懲役刑又は罰金刑を科すこととされている（住基法４２条、４５条）。

(エ) 安全確保義務

都道府県知事又は指定情報処理機関が、所定の本人確認情報の電子計算機処理等を行うに当たって、当該本人確認情報の漏えい、滅失及び毀損の防止その他の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じなければならないとされ（住基法３０条の２９）、その受領者等についても、同様に、受領した本人確認情報の漏えい、滅失及び毀損の防止その他の本人確認情報の適切な管理のために必要な措置を講じなければならないこととされている（住基法３０条の３３）。

(オ) 国又は都道府県の指導

国は都道府県及び市町村に対し、都道府県は市町村に対し、住基法の規定により都道府県又は市町村が処理する事務について、必要な指導を行うものとされ、また、主務大臣は都道府県知事又は市町村長に対し、同事務について必要があると認めるときは、報告を求め、又は助言若しくは勧告をすることができることとされている（住基法３１条１項２項）。さらに、総務大臣は、本人確認情報処理事務等の適正な実施を確保するため必要があると認めるときは、指定情報処理機関に対し、監督上必要な命令をすることができ、委任都道府県知事は、指定情報処理機関に対し、本人確認情報処理事務等の実施に関し監督上必要な命令をすることができ、委任都道府県知事も、指定情報処理機関に対し、本人確認情報処理事務の適正な実施のために必要な措置を講ずべきことを指示することができることとされている（住基法３０条の２２第１項第２項）。

(カ) 報告及び立入検査

総務大臣は、本人確認情報処理事務等の適正な実施を確保するため必要があると認めるときは、指定情報処理機関に対し、本人確認情報処理

事務等の実施の状況に関し必要な報告を求め、又はその職員に、指定情報処理機関の事務所に立ち入り、本人確認情報処理事務等の実施の状況若しくは帳簿、書類その他の物件を検査させることができ、委任都道府県知事も、指定情報処理機関に対し、本人確認情報処理事務の実施の状況に関し必要な報告を求め、又はその職員に、当該本人確認情報処理事務を取り扱う指定情報処理機関の事務所に立ち入り、当該本人確認情報処理事務の実施の状況若しくは帳簿、書類その他の物件を検査させることができることとされている（住基法３０条の２３第１項、２項）。

(キ) 第三者機関による本人確認情報の保護

都道府県に本人確認情報の保護に関する審議会を置き、同審議会は、住基法の規定によりその権限に属させられた事項を調査審議するほか、都道府県知事の諮問に応じ、当該都道府県における本人確認情報の保護に関する事項を調査審議し、及びこれらの事項に関して都道府県知事に建議することができる（住基法３０条の９）、また、指定情報処理機関には、本人確認情報保護委員会を置き、同委員会は、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、及び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ことができる（住基法３０条の１５）。

(ク) 自己の本人確認情報の開示等

何人も、都道府県知事又は指定情報処理機関に対し、磁気ディスクに記録されている自己に係る本人確認情報について、書面により、その開示を請求でき、都道府県知事又は指定情報処理機関は、開示請求があったときは、開示請求をした者に対し、書面により、当該開示請求に係る本人確認情報について開示しなければならない（住基法３０条の３７第１項第２項）、同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、その結果を当該申出をした者に対し、書面で通知することとされている（住基法３０条の４０）。

イ 技術面

(ア) ネットワークのセキュリティ対策

各市町村にはＣＳが設置され、ＣＳのネットワーク側には、指定情報処理機関が２４時間体制で監視を行うファイアウォール（以下「ＦＷ」という。）が設置され、ＣＳと既存住基システム（既存庁内ＬＡＮ）を回線により接続する場合には、ＣＳと既存住基システムの間に市町村設置のＦＷが設置される。ＣＳ、都道府県サーバ及び全国サーバを結ぶ電気通信回線は、専用回線が使用され、すべてのＣＳの全国及び都道府県ネットワーク側、すべての都道府県サーバの全国及び都道府県ネットワーク側並びに全国サーバの全方向に指定情報処理機関監視ＦＷも設置されている。このように、ネットワークの物理的・論理的隔離が行われているほか、通信の暗号化、電子記録媒体の暗号化、通信相手相互認証及びログ取得と監査によるネットワーク上の通信への不正対策や、ネットワーク機器での不正アクセス対策及び不審な通信パターンの監視によるネットワークへの不正アクセス・不正侵入対策がとられている。

(イ) システムのセキュリティ対策

端末の不正利用・不正操作防止として、操作者用ＩＣカード認証、ログイン認証が行われる。重要情報への不正アクセス防止として、アクセス制御、不審な業務パターンの常時監視、ログ取得と監査、電磁波漏えいの防止が行われている。その他、暗号鍵の不正対策やコンピュータウイルス対策も行われている。

(ウ) 住基カードのセキュリティ対策

住基カード交付時にはセキュアＩＣカード交付方式がとられ、未交付カードの盗難による不正利用対策として、輸送鍵の設定やパスワード設

定によるカード有効化の措置がとられている。また、カードのなりすまし対策として、相互認証機能、パスワード照合・カードロック機能、カードの一時停止措置がとられているほか、カードの偽造・改ざん対策として、耐タンパー機構や強制アクセス制御機能を持たせるように構成されている。

ウ 運用面

(ア) 本人確認情報管理規程

指定情報処理機関は、本人確認情報管理規程に基づき、入退室管理規則や本人確認情報取扱規則を定めることとされている。

(イ) セキュリティ対策に関する指針

各地方公共団体は、住基ネットの運営に係る責任体制、監査体制を確立し、セキュリティ組織規程、入退室管理規程及び委託管理規程等の規程を整備することとされている。

(ウ) 緊急時対応計画

指定情報処理機関及び各地方公共団体は、それぞれ緊急時対応計画を定めることとされている。

(エ) 教育・研修

地方公共団体においては、住基ネットの稼働前に、セキュリティ対策等についての教育・研修を行い、本人確認情報の提供を受ける行政機関においても、同様の教育・研修を行うこととされ、指定情報処理機関がこれに協力することとされている。

エ 上記アないしウを踏まえた住基ネットシステムのセキュリティ対策及びその検証結果は、次のとおりである。

(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するプロトコルの通過を遮断する措置がとられている。
 - d 控訴人センターは、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1

4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えい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つ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の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、本人確認情報の漏えい、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ている。

(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)。

(戊) 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。

(己) 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えいの可能性を確認し、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控訴人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）

控訴人センターは、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、クロウ社（Crow Chizek and Company LLC）が実施した。）。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－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、脆弱性も見出せなかった。
- b ＣＳ－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、脆弱性も見出せなかった。
- 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。

２ 争点(1)（プライバシー権の侵害の有無）について

- (1) 前記前提事実のとおり、住基ネットは改正法によって創設された制度であり、控訴人県の知事が、住基法所定の国の機関及び法人からの住基法所定の事務に関して求めがあったときにおいて、その区域内の市町村長から通知を受けた住民（被控訴人らが含まれる。）に係る本人確認情報を上記の国の機関等に対して住基ネットにより提供するのであるが、上記提供を含む住基法所定の本人確認情報事務処理を控訴人センターに委任しているため、上記の本人確認情報を控訴人センターに通知し、上記委任を受けた控訴人センターにおいて、これを住基ネットの磁気ディスクに住基法所定の期間保存し、控訴人県の知事に代わって、住基ネットを通じて、上記提供を含む本人確認情

報事務処理を行うこととなっている。上記のような控訴人らによる本人確認情報事務処理は、いずれも住基法という法律の規定に基づく措置であるところ、住基法には、上記提供を含む住基法所定の本人確認情報事務処理に関し、本人確認情報に係る住民の同意又は住基ネットへの参加表明をその要件とし、あるいは、住基ネットへの不参加又は離脱を表明している者についての除外を定める規定はないから、住基法は、控訴人県の知事に対し、本人確認情報に係る住民の同意又は住基ネットへの参加意思の有無を問うことなく、一律に、その区域内の市町村長から通知を受けた住民（被控訴人らが含まれる。）に係る本人確認情報に関して住基法所定の本人確認情報処理をすることを命じているものであること（このことは控訴人県の知事からその委任を受けた控訴人センターによる本人確認情報事務処理に関しても同様であること）は明らかであり、住基ネットに関係する住基法の諸条項の文言に照らしても疑いを入れない。そして、住基ネットにおいて控訴人らが保存し、国の機関等に提供する本人確認情報は、住民票コードとその変更情報を除き、改正法施行前から、市町村長が、住基法により備え付けるべき住民基本台帳の編成単位である住民の住民票の作成（その内容の変更を含む。）に関して、住基法に基づき、住民からの届出により、又は自ら収集して取得した情報であり、住民票コードとその変更情報は、改正法により市町村長が住基法所定の方法で住民に付することとなった住民票コードとそれに関する変更情報であるから、いずれも、市町村長が住民票の作成に関して住基法に基づき取得した情報である。

したがって、控訴人ら（控訴人県の知事又はその委任を受けた控訴人センター）が、控訴人県の区域内に居住する被控訴人らの本人確認情報に関して上記のような本人確認情報事務処理を行うことは、いずれも、住基法という法律の規定に基づくものであって、上記のような本人確認情報処理を定めた改正法が有効なものである限り、適法なものというべきものである。

(2) 被控訴人らは、控訴人らが、住基ネットからの離脱を表明するなどして本人確認情報が住基ネットを通じて国の機関等に提供されることに同意していない住民の本人確認情報を、住基ネットを通じて国の機関等に提供するために住基ネットの磁気ディスクに保存し、これを国の機関等に提供するものとしていることは、憲法13条が当該住民に保障しているプライバシー権（自己情報コントロール権）を侵害するから、住基法中の住基ネットに関する規定（以下「住基ネット規定」という。）は、少なくとも住基ネットからの離脱を表明するなどして本人確認情報が住基ネットを通じて国の機関等に提供されることに同意していない被控訴人らとの関係では違憲無効である旨主張するので、以下において、住基ネット規定が憲法13条に違反して無効なものであるか否か検討する。

ア 憲法13条は、「すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。」と規定し、すべての国民は、人格的存在（社会的関係性にある人間）であるがために個人として尊重されるべき存在であり、生命、自由及び幸福追求に対する権利（以下、一括して「幸福追求権」という。）を有することを確認し、その保障すべき旨を定めているところ（最高裁昭和44年12月24日大法廷判決・刑集23巻12号1625頁参照）、国民が個人として尊重されるためには個人の人格的自律を可能とする人格的生存に不可欠な利益を国家機関等の公権力の行使から保護する必要があることから、憲法13条は、その保護のために、国民に対し、幸福追求権として、包括的に個人の人格的自律を可能とする人格的生存に不可欠な利益を憲法上の権利として保障しているものと解されるのである。そして、個人の人格的自律ないし人格的生存は個人の私生活上の自由及び平穩が国家機関等の公権力の行使から保護されて初めて確保される関係にあるから、憲法は、その13条により、

幸福追求権の一内容をなす憲法上の権利として、個人の人格的自律ないし人格的生存の基盤をなす個人の私生活上の自由及び平穩を国家機関等の公権力の行使から包括的に保障するとともに、過去の侵害の事実等を踏まえて、上記の個人の私生活上の自由及び平穩の保護に関し、信教の自由に関する憲法20条、集会等の自由に関する憲法21条、居住等の自由に関する憲法22条、学問の自由に関する憲法23条、身体の自由に関する憲法33条及び34条、住居等の不可侵を定める憲法35条等による基本権を個別に列挙してその保障を明示しているものと解されるのである。

そして、国家機関等の公権力が、他者に知られたくない個人の私生活上の情報を密かに収集し、それをみだりに他者に開示したり、そのような情報に基づき、直接にあるいは間接に個人の私生活に対して干渉する事態が生ずることになれば、個人の私生活における平穩が侵害され、個人が自由に自らの生き方を決定するという人格的自律が脅かされることになるから、このような国家機関等の公権力による個人の私生活上の情報の収集、公開及び私生活に対する干渉からの自由は、憲法13条が保障している幸福追求権の一内容として、個人の私生活上の自由及び平穩に関する利益で、個人の人格的自律ないし人格的生存に必要不可欠な利益（上記個別規定で保障されている基本権と同等の憲法的価値を有する人格的利益）を内容とする人格権に基づくプライバシーに関する権利（以下「プライバシー権」という。）として、すべての国民に保障されているものというべきであり、国家機関等の公権力といえども、正当な理由がなく、社会生活上当然に受忍すべき限度を超えて、上記のような私生活上の平穩を害し、あるいは、その自由・自律に干渉するような態様において、個人の私生活上の情報を収集し、管理し、利用（他者への開示を含む。）することは、憲法13条が保障するプライバシー権を侵害するものとして許されない。

したがって、国民は、国家機関等の公権力が、正当な理由がなく、社会

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

イ　ところで、本人確認情報のうち、住民票コードとその変更情報を除いた氏名、住所、生年月日及び性別の4情報とこれらの変更情報は、その内容に照らして、それ自体では個人の人格、思想、信条、良心等の内心に関する情報とはいえないし、表現、集会等の私生活上の行動に関する情報ともいえないのであつて、個人の人格的自律ないし人格的生存の維持や発展に直接関わるような情報に当たるものではないのであり、また、住民票コー

ドは、特定の個人についての迅速な検索処理を可能とし、かつ、確実な本人確認を可能とする目的で、無作為に作成された10桁の数字及び1桁の検査数字からなる11桁の数字にすぎないから、住民票コードとその変更情報がそのものとして個人の人格的自律ないし人格的生存の維持や発展に関わるような情報に当たらないことは明らかである。したがって、本人確認情報そのものが、個人の人格的自律ないし人格的生存に必要不可欠な、個人の私生活上の自由及び平穩に関する利益（憲法の個別規定で保障されている基本権と同等の憲法的価値を有する人格的利益）として、憲法13条により保障されているものと解することには疑問がないわけではない。

しかし、本人確認情報のうち、住民票コードとその変更情報を除いた氏名、住所、生年月日及び性別の4情報とこれらの変更情報は、その一体的な取扱いにより、特定の個人を極めて容易に検索することができるため、国家機関等の公権力が、これらの情報を媒介にして、その情報に係る個人の私生活に関する情報を広範囲に収集し、そのことにより、その言動等を把握し、監視し、さらには、これに直接あるいは間接に干渉することが可能となることから、国民がそのことに対する危惧、不安を感じ、その言動（例えば、集会や市民運動への参加）を抑制するなどのおそれがないわけではなく、その意味で、これら情報は、その取扱い（収集、管理又は利用）次第では、個人の人格的自律ないし人格的生存に必要不可欠な利益としての個人の私生活上の自由又は平穩に影響を及ぼし、プライバシー権を侵害する危険があり、また、住民票コードは、特定の個人についての迅速な検索処理を可能とし、かつ、確実な本人確認を可能とする目的で住民に付されたものであるから、住民票コードとその変更情報は、その高度な個人識別性の故に、他の本人確認情報以上に、その取扱い次第では同様の危険があり、したがって、国家機関等の公権力が住基ネットにおいて本人確認情報を取り扱うことは、憲法13条が国民に対して保障している、個人の

格的自律ないし人格的生存に必要不可欠な利益としての私生活上の自由及び平穩と密接な関連をもつものということができる（指紋押なつに関する最高裁平成7年12月15日第三小法廷判決・刑集49巻10号842頁参照）。

そして、情報通信技術の飛躍的な発展に伴い、インターネット等を通じて情報が瞬時にかつ大量に流通する現代社会にあつては、国家機関等の公権力が、本人確認情報を使用して、コンピュータ上の国民の私生活上の自由及び平穩に関連する私的領域に関する情報を広く収集し、これを管理し、利用（他の公的な機関に対する提供を含む。）することが容易になったのであるが、国家機関等の公権力が上記のようにして個人の私的領域に関する情報を広く収集し、管理し、利用するような事態となった場合には、上記で指摘した観点から、その管理又は利用に関する法制度とこれに関連する同法制度の運用の実情のいかんによっては、憲法13条により保障されているプライバシーに関する権利を害し、あるいはこれを害する具体的なおそれがあることになるだけでなく、収集又は管理されている情報の規模、内容等のいかんによっては、収集又は管理していること自体が、憲法13条により保障されているプライバシー権を害し、あるいは、これを害する具体的なおそれがあるため、憲法13条に違反する状態にあるものと評価されるに至ることもあり得ないではない。

以上を要するに、本人確認情報は、憲法13条が、国民に対して保障するプライバシー権の中核をなすところの、個人の人格的自律ないし人格的生存に必要不可欠な、個人の私生活上の自由及び平穩に関する利益（憲法の個別規定で保障されている基本権と同等の憲法的価値を有する人格的利益）には直接に関わるものとはいえないが、その高度な個人識別性の故に、これに密接に関連する利益として、なお憲法13条が国民に保障するプライバシー権の内容となり、それによる保護の対象となるものと解するのが

相当である。

そして、住基ネット上の本人確認情報に関して上記のような違憲状態が生じた場合において、その原因が上記アの観点からの住基ネット規定によるものであるときには、同規定は憲法 13 条により無効となり、本人確認情報に係る住民は、人格権としてのプライバシー権に基づく妨害排除請求権又は妨害予防請求権によりその差止め等の救済（憲法 13 条が国民に対して保障している人格権としてのプライバシー権に基づき、公権力による個人情報の提供を禁止し、公権力が保有する個人情報の削除を求めること）を求めることができるものというべきである。被控訴人ら主張のプライバシー権（自己情報コントロール権）は、上記の趣旨と範囲において、これを肯定することができる。

なお、控訴人らは、被控訴人ら主張の自己情報コントロール権なる権利は、実定法上の根拠がなく、権利としての成熟性も認められないから、被控訴人ら主張の請求権はそもそも実定法上の権利としては認められない旨主張するが、上記説示のとおり、個人の私的領域に関する情報が公権力によって不当に収集、管理、利用され、それが憲法 13 条により保障されるべきプライバシー権を害し、又は、これを害する具体的なおそれがある一定の場合には、人格権としてのプライバシー権に基づきこれを差し止める権利があるのであり（その権利を自己情報コントロール権と称するか否かは別として）、これに反する控訴人らの上記主張は採用できない。

ウ しかしながら、本人確認情報は、そのものとして、個人の人格的自律ないし人格的生存に必要不可欠な、個人の私生活上の自由及び平穩に関する利益（憲法の個別規定で保障されている基本権と同等の憲法的価値を有する人格的利益）に直接に関わるものではないから、本人確認情報のプライバシーとしての要保護性について、憲法 13 条が、国家機関等の公権力との関係で、国民に対し、本人確認情報に係る住民の同意を得ることなくし

ては、国家機関等の公権力においてこれを収集し、管理し、利用することができないような強度なものとして保障しているものと解することはできないのであり、国家機関等の公権力において、その行政事務の処理の必要等の正当な理由がある限り、相当な方法で、これを収集し、管理し、利用することは、その本人確認情報に係る住民の同意がなくとも、憲法13条に違反するものではなく、これにより、当該本人確認情報に係る個人の私生活上の自由及び平穩が一定の範囲で制限されることがあったとしても、憲法13条にいう「公共の福祉」による制限として、許されるものというべきである。

なお、被控訴人らは、本人確認情報もセンシティブな情報であり、秘匿の要請が大である旨主張するが、本人確認情報は、上記のような内容のものであるから、そのような内容の本人確認情報が国家機関等の公権力によって収集され、単なる本人確認情報として管理され、住基法所定の事務に利用される限りにおいては、そのこと自体で、国民が危惧、不安を感じ、その言動を抑制するなどして行動を規制することはほとんど考え難いから、被控訴人らの主張中上記説示の趣旨に反する部分は、採用できない。

しかるところ、都道府県知事及びその委託を受けた控訴人センターが保存し、国の機関等に対して提供する本人確認情報は、住基法により市町村長が適法に取得した住民に関する情報であるところ、上記1で認定したとおり、住基ネットは、住民サービスの向上と行政事務の効率化を目的とするものであり、また、都道府県知事及びその委託を受けた控訴人センターによる本人確認情報の保存及び国の機関等に対する提供、国の機関等によるその利用は、いずれも住基法所定の事務の処理に関して必要なものである上、その利用は、上記事務に係る住民の居住関係の確認等の住基法所定の目的に限定され、住基法が定める以外の利用は許されないものとされているのであって、住民の本人確認情報がみだりに公開されたり、上記事務

の処理以外の用途で利用されるものではないのであるから、控訴人らが住基法に従って住基ネットにおいて本人確認情報を取り扱うことについては、正当な理由があり、その方法も相当であるので、上記保存及び提供が、そのことに関して住民の同意がなければ、住民の本人確認情報に関するプライバシー権を侵害するものとはいえない。したがって、住基ネット規定がその内容自体において憲法13条に違反するものということとはできない。

エ 被控訴人らは、住基ネットが、コンピュータネットワーク上で住民の個人情報を通達させるものであり、システムの性格上、いったん漏えいされれば、当該個人情報が大勢かつ網羅的に流出し、また、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、個人情報の大勢、包括的な入手・集積がなされる危険性があり、さらに、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旨主張し、具体的には、外部からのネットワーク侵入の危険性や、運用関係者等による漏えい等の危険性、法律の改変による利用範囲の拡大等の危険性があり、ハード面及びソフト面の両面にわたってセキュリティ対策の不備等もあることを指摘した上、長野県侵入実験においても、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あることが確認されたなどと主張するので、さらに検討する。

(7) 住基法は、本人確認情報を含む個人情報保護のための施策として、上記1(2)ア記載のとおり、本人確認情報を含む個人情報保護を目的とする多数の規定を置いているのであり、これによれば、都道府県知事及び指定情報処理機関が住基ネットに関して保有する情報は本人確認情報のみに制限され、都道府県知事及び指定情報処理機関が本人確認情報を利用し、提供できる場合及び提供の相手は住基法により限定され、その提供を受けた国の機関等（受領者）が受領した本人確認情報の利用及び提

供も住基法により制限されているのであり、また、指定情報処理機関の役職員、住基ネットにおいて本人確認情報事務処理に従事する都道府県及び受領者（国の機関等の職員等）に対して秘密保持義務を課し、その違反に対して刑事罰を科することとし、控訴人ら及び受領者に対して本人確認情報の漏えい等の防止のために必要な安全確保措置を講ずる義務を課しているほか、本人確認情報の適正処理のための指導監督あるいは検査等権限を国又は都道府県知事に対して付与し、都道府県知事及び指定情報処理機関には本人確認情報の保護に関する事項を調査審議するための第三者機関を設置するものとされている。

被控訴人らは、住基ネットについて、セキュリティに不備がある上、管理及び運用面にも不備があるため、本人確認情報の漏えい、流出の危険があると主張する。しかし、住基ネットのセキュリティのために、上記1(2)イ及びエ記載の種々の対策が講じられており、また、管理及び運用面でも、被控訴人らを含む住民の個人情報保護のために上記1(2)ウ及びエのとおり種々の措置が講じられているのであるから、住基ネットワーク及びシステムについて、そのセキュリティの不備や管理及び運用面での不備があるため、本人確認情報が漏えいし、流出する具体的な危険があるとは認められない。

したがって、住基法は、本人確認情報を含む個人情報保護に相応の配慮をし、その保護のための施策を講じているものといえることができる。

(イ) 被控訴人らは、住基ネットによるプライバシー侵害の危険性に関する立証責任につき、当事者間の公平の観点から、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とも主張するが、仮にそうであるとしても、既に認定説示したところによれば、被控訴人らが上記の事実上の推定についての一応の立証に成功したものとはいえない。

この点に関し、被控訴人らは、住基ネットのセキュリティ上の不備が

あることを裏付けるものとして、長野県侵入実験について言及するが、上記 1 (2) エ(オ)の事実及び証拠（乙 1 5 ないし 1 7, 乙 1 8 の 1, 乙 1 9, 2 2, 乙 3 1 の 1 及び 2, 乙 3 2 の 1 及び 2）によれば、住基ネットに対する外部からの侵入の可能性の有無等を検討するために実施された長野県侵入実験においては、外部インターネットから庁内 LAN への侵入はできていないばかりか、同インターネットと庁内 LAN との間の FW, 市町村設置の FW 及び指定情報処理機関監視の FW のいずれも突破できなかったことが認められ、個人情報の漏えい等の具体的危険性があるとはいえないから、上記の長野県侵入実験の結果によって、住基ネットが外部からの侵入等に対してシステムとして脆弱であることを認めるには十分でないし、他にこれを認めるに足りる証拠はない。

もっとも、北海道斜里町において、住基ネットに関する情報がファイル交換ソフト Winny を介してネット上に流出したことが認められるものの（甲共 1 8 1 ないし 1 8 3）、これは、同町職員の自宅にある私用パソコンがコンピュータウィルスに感染した結果発生したものであって、住基ネットを構成するコンピュータ等から当該情報が直接流出したのではなく、結果的にも流出した情報によりもたらされるおそれのあるシステムの脆弱性はパスワードの変更等により既に対応済みであることが認められる（乙 6 1, 6 5, 6 6）。また、帯広市において、同嘱託職員が当該施設に配置してある業務端末を用いて住民基本台帳の目的外閲覧を行ったことが認められるものの（甲共 1 8 4, 乙 6 7）、内部者による漏えいの抽象的な危険性は住基ネット以外の制度にもないわけではなく、これに対しては法令の規定や又は運用基準を遵守させることにより対応せざるを得ないものであって、住基ネット固有のシステムの脆弱性があることを基礎付けるものではないから、住基ネットが、その制度として、被控訴人ら主張のプライバシー権侵害の具体的な危険があ

る制度であるとはいえない。

(ウ) 被控訴人らは、住基ネットには本人確認情報を使用したデータマッチングの危険がある旨主張する。しかし、上記１で認定のとおり、住基法は、本人確認情報に関する利用又は提供の制限、本人確認情報の処理事務に従事する職員に対する刑事罰を伴う守秘義務等を規定することで、本人確認情報が住基法所定の事務処理又は目的以外での使用を制限しているのであるから（なお、行政機関の保有する個人情報の保護に関する法律は、行政機関による個人情報について、法令の定める所掌事務を遂行するために必要な場合に、できるかぎり特定された利用目的の達成に必要な範囲でのみ保有することを許すものとし（３条）、利用目的以外の利用又は提供も同法所定の場合に限定している（８条）のであり、行政機関の職員等による保有個人情報の不正な提供や不正な目的での個人情報の収集については刑事罰を科することとしている（５４条、５５条）。）、被控訴人ら主張の本人確認情報を使用したデータマッチングは、住基ネットに関係する都道府県知事、国の機関等あるいはその職員がこれら法律の定めを遵守する限りは実現しないのであり、これらの者がこれら法律の定めに違反することを当然の前提として、上記データマッチングの具体的な危険があるとするのは、当を得たものということとはできない。被控訴人ら指摘の上記事例（甲共１８１ないし１８４）も、住基ネットの管理の末端における、ごく例外的な事例に関するものであって、住基ネットについての制度的な欠陥を示すものとはいえず、上記判断を左右するものではない。

被控訴人らは、本人確認情報を使用したデータマッチングの危険に関連して、これを防止するための第三者監視機関の不存在を指摘して、行政機関による個人情報の目的外利用禁止の制度的担保の不備を主張する。しかし、住基法は、本人確認情報の適正な取扱い確保のため、都道

府県知事及び指定情報処理機関には本人確認情報の保護に関する事項を調査審議するための第三者機関（都道府県にあっては「本人確認情報の保護に関する審議会」、指定情報処理機関にあっては「本人確認情報保護委員会」）を設置するものとしているのであるから、これらが、その組織及び権限等において本人確認情報の適正な取扱い確保のための第三者監視機関として将来にわたっても十分なものか否かに関しては議論があり得るとしても、住基法が行政機関による個人情報の目的外利用禁止の制度的担保を設けていないということとはできない（乙４１）。

(エ) 被控訴人らは、住基ネットについてその導入の必要性がない旨主張するが、上記１で認定したとおり、住基ネットは、住民サービスの向上と行政事務の効率化を目的とするものであり、これにより住民票の写しの広域交付、転入・転出の特例処理、各種手続の簡素化等、住民の利便性の増進を図ることが可能となるのであって、住基ネット導入の必要性を否定することはできないというべきである。なお、被控訴人らは、住基ネット導入に伴う行政事務の効率化が導入に伴うコストに遠く及ばないとも主張するが、この点は、国又は地方公共団体における行政事務の処理に関する立法政策又は行政上の施策の当否の問題として、立法府又は行政府が広範な裁量権を有する事項であるから、被控訴人ら指摘のような事情があるとしても、そのことから直ちに住基ネットについてその導入の必要性がないと断定することはできないというべきである。したがって、被控訴人らの上記主張は採用できない。

また、被控訴人らは、住民の利便性よりも自らのプライバシーの権利の保持を望む被控訴人らに対し、住民の利便性を根拠として住基ネットを導入する必要性はないとも主張するが、住基法は、住基ネットのシステム上ですべての本人確認情報が網羅的に提供、利用されることを当然の前提としており、住民の一部でもこれに参加しないことを許容すれば、

住基ネットのシステムの本来予定する機能を果たし得ないばかりか、従来のシステムや事務処理を併存的に存置せざるを得ないことになるなど、被控訴人らが住基ネットから離脱することにより重大な支障が生ずるというべきであるから（甲共125，乙59によれば，非通知希望者につき神奈川県への本人確認情報を送信しないことを暫定的に許容した横浜市では，通知希望者及び非通知希望者の混在により，本来，書類の作成すら必要のない年金受給者の現況届を自ら作成の上，郵送，提出しなければならないなど，住基ネットの利便性を享受できない実際上の支障が生じていることが認められる。），被控訴人らの上記主張は採用できない。

なお，被控訴人らは，控訴人らが，従前の審理経過に反して，当審になってこの点に関する主張をにわかに行うことは禁反言の法理に反するし，仮にそうでないとしても，控訴人ら主張の，被控訴人らが住基ネットから離脱することによって生じる支障は極めて抽象的なものであり，また，被控訴人らが住基ネットの運用の中止を求めたにもかかわらず，これを強行することによって築いたシステムなどに支障が生じることを根拠に住基ネットの正当性を基礎付けることはできないとも主張するが，上記で説示したとおり，住民の一部が住基ネットに参加しないことにより支障が生ずることは法の予定するところに照らして明らかである上，控訴人らは，原審においても，その旨の主張をしていた（原判決47頁の「(カ)」欄の主張）から，この点に関する控訴人らの主張が禁反言の法理に反するとはいえず，また，上記支障は具体的かつ現実的なものであり，これを抽象的なものとは言い難いし，さらに，住基ネットの導入が被控訴人らのプライバシー等の権利利益を直ちに侵害するものではなく，被控訴人らの中止要請の有無によって，その必要性が否定されるものでもないから，被控訴人らの上記主張は採用できない。

オ 以上によれば、住基ネット規定が、その内容自体において憲法 13 条に違反するものということとはできないのみならず、住基ネットに使用されるシステムの安全に関する規定や住基ネットの管理運営に関してプライバシーを保護する規定を欠くなどのために、使用されているシステムについて安全上無視し得ない欠陥があつて、容易に外部からの侵入を許すものであったり、住基ネットの管理及び運営が著しく杜撰になされ、住基ネットの管理運営に従事する者が不正に本人確認情報にアクセスするなどして、本人確認情報が簡単に漏えいし、あるいは流出する具体的な危険があるという場合にも当たらないため、控訴人らが住基ネットにおいて本人確認情報を取り扱うことが憲法 13 条に違反するものということもできない。

なお、住基法は、平成 18 年法律第 74 号により、何人でも住民基本台帳の一部の写しの閲覧を請求できるという現行の閲覧制度（住基法 11 条 1 項）を変更し、閲覧することができる場合を法律で定める一定の場合に限定する旨改正されたものの（平成 18 年政令第 297 号により同年 11 月 1 日施行）、これは、現行の閲覧制度の下では、ダイレクトメールなどの営業活動のために住民基本台帳の一部の写しが大量に閲覧され広く利用されていること、制度を悪用したと考えられる事件が発生していること、不当な目的又はそのおそれがある場合等には閲覧請求を拒否できるとしても（住基法 11 条 3 項）、その審査基準が不明確なこともあつて市町村の審査は区々になっていること等の問題点を踏まえた改正であつて（乙 45, 46）、住基ネットにプライバシー権侵害等の具体的な危険性があることを前提とした改正であるとは解されないから、上記判断を左右するものではない。

(3) 被控訴人らのその余の主張について

ア 被控訴人らは、控訴人らが、被控訴人らの同意を得ることなく、住基ネットにより本人確認情報を当該市区町村から全国に流通させることによつ

て、被控訴人らが自己の情報をコントロールすることが不可能となっているから、そのことで直ちに被控訴人らの自己情報コントロール権としてのプライバシー権が侵害され、また、被控訴人らが有する自己情報の開示に関する権利も侵害される旨主張する。

しかし、被控訴人らは、住基法の定めるところに従い、自己の本人確認情報の開示、訂正等を請求することができるのであるから、控訴人らが、被控訴人らの同意を得ることなく、住基ネットにより本人確認情報を当該市区町村から全国に流通させることによって、自己の情報をコントロールすることがおよそ不可能となるものではないから、被控訴人らのプライバシー権や自己情報の開示権を侵害するものともいえない。

イ 被控訴人らは、本人確認情報以外の個人情報、すなわち、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、本人確認情報と同様に、住基ネットにより被控訴人らの自己情報コントロール権が侵害されているとも主張するが、既に認定説示したところに照らして採用できない。

ウ 被控訴人らは、改正法附則 1 条 2 項にいう「個人情報の保護に万全を期するために、速やかに、所要の措置」が講じられていない旨主張するが、既に認定説示したことに加え、平成 15 年 5 月には、上記の「所要の措置」の一環として、個人情報の保護に関する法律（平成 15 年法律第 57 号）、行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）、独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）等の法律が成立し、同年 5 月から平成 17 年 4 月にかけて施行されたことも考慮すると、上記の「所要の措置」が講じられていないということとはできない。

エ その他、被控訴人らは、住基ネット規定又は住基ネットの実際の運用が憲法 13 条の保障するプライバシー権を侵害し、又は、その危険がある違

憲違法なものである旨を種々主張するが、いずれも、既に認定説示したところに照らして、採用できない。

3 争点(2) (氏名権の侵害の有無) について

(1) 被控訴人らは、住基ネットが、個人の情報を住民票コードという番号をもとにして流通させ、個人の特定を氏名ではなく番号によって行うものであり、異なる行政分野にまたがり番号が共通化されることと相まって、行政担当者は個人の氏名よりも番号を重視することになり、個人の人格の同一性を表す中核となる氏名を住民票コードで分類される個人情報の一つにおとしめるものである、また、個人を番号によって扱うこと、特に住民票コードが全国民にその生涯にわたって番号を付すものであることは、氏名を中核とする個人のアイデンティティ又はその感覚を害するものであるから、住基ネットは被控訴人らの氏名権を侵害する旨主張する。

(2) 氏名は、社会的にみれば、個人を他人から識別し特定する機能を有するものであると同時に、その個人からみれば、人が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、人格権の一内容を構成するものというべきであるから、個人の尊厳を害するような態様で上記の人格的利益が侵害された場合には、これを氏名権と称するか否かは別として、憲法13条による保護を受け得るというべきである。

しかし、上記1及び2の認定説示に照らせば、住基ネットにおいて各個人の住民票に住民票コードを付すことは、住民サービスの向上と行政事務の効率化の目的に資するための手段にすぎず、住民票コードが無作為の番号で住民の申請により変更可能なものである点でも、行政機関が住民に対する呼称として氏名等に代替すべく住民票コードを用いるものではないから、これをもって行政担当者が個人の氏名より住民票コードという番号を重視することにはならず、個人の人格的利益を侵害するものとはいえないし、個人のアイデンティティを侵害するものとはいえない。仮に、被控訴人らが自らに住民

票コードが付されたことにより不快な感情を抱くところがあったとしても、顧客番号、登録番号等にみられるように、個人情報の簡便かつ正確な処理のために、個人の氏名や住所に加え、英数字等の組合せにより構成された番号を付すことは一般に広く行われており、社会通念上許容されるものというべきであるから、被控訴人らの感情いかんが上記判断を左右するものとはいえない。

(3) したがって、被控訴人らの上記主張は採用できない。

4 争点(3) (公権力による包括的管理からの自由の侵害の有無) について

(1) 被控訴人らは、住基ネットにおける住民票コードが、全国民を確実に識別するために付されたものであり、また、今後、住民票コードの利用が可能な事務が無限定に拡大されていくことが予想され、個人の全生活分野において住民票コードを基点として様々な個人情報が蓄積され、かかる個人情報を公権力が事実上無制限な利用目的をもって一元的に管理することを可能とするものであるから、住基ネットは、被控訴人らの公権力による包括的な管理からの自由を侵害する旨主張する。

(2) 被控訴人ら主張の公権力による包括的管理からの自由の具体的な権利内容は必ずしも明確ではないものの、憲法13条、19条及び21条等の趣旨に照らせば、個人の人格的自律を害するような態様で個人を公権力の包括的な管理下に置くことは許されないというべきであるから、そのような態様で上記人格的利益が侵害された場合には、これを公権力による包括的管理からの自由と称するか否かは別として、憲法13条等による保護を受け得るというべきである。

しかし、上記1及び2の認定説示に照らせば、住基ネットが行政機関において個人を包括的に管理することを目的とするものでないことはもとより、個人情報保護のための対策等に照らせば、公権力が住基ネット上の個人情報を事実上無制限な利用目的をもって一元的に管理したり、又はそのような具

体的危険性があるものとはいえない。

(3) したがって、被控訴人らの上記主張は採用できない。

5 結論

以上によれば、被控訴人らの請求は、争点(4)につき判断するまでもなく、いずれも理由がないから、これを棄却すべきである。なお、被控訴人らは、2006年11月21日付け口頭弁論再開申立書をもって、口頭弁論再開の申立てをするが、その内容を検討しても、口頭弁論再開の必要は認められないので、これをしない。

よって、これと異なる原判決中、控訴人ら敗訴部分を取り消し、被控訴人らの請求をいずれも棄却することとして、主文のとおり判決する。

名古屋高等裁判所金沢支部第1部

裁判長裁判官 長 門 栄 吉

裁判官 沖 中 康 人

裁判官 田 中 秀 幸