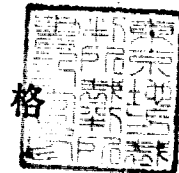


これは正本である。

平成18年4月7日

東京地方裁判所民事第25部

裁判所書記官 岡崎



平成18年4月7日判決言渡 同日原本領収 裁判所書記官岡崎格

平成14年(ワ)第16306号住民基本台帳ネットワーク差止等請求事件

口頭弁論終結の日 平成18年2月7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 原告の請求をいずれも棄却する。
- 2 訴訟費用は、原告の負担とする。

事 実 及 び 理 由

第1 請求

1 被告中野区は、

- (1) 被告東京都に対し、原告の氏名、住所、生年月日、性別、住民票コード及びこれらの変更情報（以下「本人確認情報」という。）を通知してはならない。
- (2) 住民基本台帳から原告の住民票コードを削除せよ。

2 被告東京都は、

- (1) 住民基本台帳法別表第1の上欄に掲げる国の機関及び法人に対し、原告の本人確認情報を提供してはならない。
- (2) 被告センターに対し、原告に関する住民基本台帳法30条の10第1項所定の本人確認情報処理事務を委任してはならない。
- (3) 被告センターに対し、原告の本人確認情報を通知してはならない。
- (4) 原告の本人確認情報を、保存する住民基本台帳ネットワークシステムの磁気ディスク（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。

3 被告センターは、

- (1) 被告東京都から受任した原告に関する住民基本台帳法30条の10第1項

所定の本人確認情報処理事務を行ってはならない。

(2) 原告の本人確認情報を、保存する住民基本台帳ネットワークシステムの磁気ディスクから削除せよ。

4 被告国は、原告に対し、55万円及びこれに対する平成14年9月20日から支払済みまで年5分の割合による金員を支払え。

5 被告東京都及び被告センターは、原告に対し、連帯して55万円及びこれに対する平成14年9月20日から支払済みまで年5分の割合による金員を支払え。

第2 事案の概要

本件は、被告中野区に住民登録をしている原告が、住民基本台帳法（以下「住基法」という。）の平成11年改正により導入された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。）が、憲法13条により保障されている原告のプライバシー権（自己情報コントロール権）、氏名権及び公権力によって包括的に管理されない自由権を侵害するものであるなどと主張し、これらの権利に基づき、被告中野区、被告東京都及び被告センターに対し、原告の本人確認情報を住基ネットから削除することなどを求めるとともに、被告国、被告東京都及び被告センターに対し、国家賠償法又は不法行為による損害賠償請求権に基づき、慰謝料等及びこれに対する訴状送達の日（平成14年9月20日）から支払済みまで民法所定の遅延損害金の支払を求める事件である。

第3 前提となる事実（証拠等により認定した事実は証拠等を掲記する。）

1 当事者（甲1，175，弁論の全趣旨）

(1) 原告は、被告中野区に住民登録をしている者である。

(2) 被告センターは、昭和45年5月、地方公共団体におけるコンピュータの利用を促進するため、設立された法人である。

被告センターは、平成11年11月1日、自治大臣（当時。現総務大臣）

によって、都道府県知事の委任により住基法30条の10第1項所定の住基ネットに係る事務（以下「本人確認情報処理事務」という。）を行う指定情報処理機関に指定された。

被告センターは、現在、東京都知事を含む全国47都道府県知事の委任を受け、本人確認情報処理事務を行っている。

2 住民基本台帳（住基法1条，3条3項，6条1項，7条）

住民基本台帳は、住基法に基づき、市町村（特別区を含む。以下同じ。）の長が作成し、住民票によって編成される公簿であり、住民に関する記録を正確かつ統一的行うことによって、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処理の基礎となるものである。住民票には、住民の氏名，生年月日，性別，世帯主，戸籍，住民となった年月日，住所，選挙人名簿への登録に関する事実，国民健康保険，介護保険，国民年金の被保険者の資格に関する事項及び児童手当の支給を受けている者の受給資格に関する事項などが記載される。住民は、常に、住民としての地位の変更に關する届出を正確に行うように努めなければならない，虚偽の届出その他住民基本台帳の正確性を阻害するような行為をしてはならない責務がある。

3 住基法の平成11年改正

住基法は、平成11年法律第133号により改正され、これにより住基ネットが導入された（以下、平成11年法律第133号を「改正法」という。）。

住基ネットは、行政機関が、行政事務を処理するに当たり、市町村の区域を越えて、氏名，生年月日，性別及び住所等の情報（本人確認情報）を利用することができるようにするために構築されたものである。

具体的には、各市町村長，各都道府県知事及び指定情報処理機関において電子計算機を設置し、これらを専用の電気通信回線で結んでネットワーク化し、市町村長が都道府県知事に、都道府県知事が指定情報処理機関に対し、本人確認情報を上記ネットワークを通じて通知し、各市町村長，各都道府県知事及び

指定情報処理機関が本人確認情報を保有し、①各市町村長は、他の市町村長に対し、条例で定めるところにより本人確認情報を提供し（住基法30条の6）、②各都道府県知事及び指定情報処理機関は、市町村長、他の都道府県知事並びに国の機関及び法人（以下「国の機関等」という。）に対し、住基法で定めるところにより本人確認情報を提供し（住基法30条の7、30条の10）、③各都道府県知事は、住基法で定めるところにより本人確認情報を自ら利用する（住基法30条の8）というものである。

4 住基ネットの概要

(1) ネットワークの構築

市町村長は、既に設置されている住民基本台帳を管理する電子計算機（以下「既存住基サーバ」という。）とは別に、本人確認情報を管理しネットワークに接続するための電子計算機（コミュニケーションサーバ。以下「CS」という。）を設置する。また、都道府県知事及び指定情報処理機関は、本人確認情報を管理するための電子計算機をそれぞれ設置する（以下、それぞれ「都道府県サーバ」、「指定情報処理機関サーバ」という。）。

そして、市町村長、都道府県知事及び指定情報処理機関は、CS、都道府県サーバ及び指定情報処理機関サーバを専用の電気通信回線で結び、ネットワークを構築する。

(2) 住民票コード

ア 住民票コードの内容

改正法は、氏名、生年月日、性別及び住所等の情報をネットワークにおいて効率的に送信するため、住民票の記載事項として、新たに住民票コードを設けた（住基法7条13号）。住民票コードは、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成る（住民基本台帳法施行規則〔以下「施行規則」という。〕1条）。

イ 住民票コードの指定

都道府県知事は、その区域内の市町村長が住民票に記載することができる住民票コードを指定し、市町村長に対して通知する（住基法３０条の７第１項）。

都道府県知事は、市町村長に対して住民票コードの指定を行う際、あらかじめ他の都道府県知事と協議して、住民票コードが重複しないように調整をする（住基法３０条の７第２項）。

ウ 住民票コードの記載及び住民に対する通知

(ア) 市町村長は、前記のとおり都道府県知事から指定された住民票コードからいずれか１つを選択し、重複しないように住民票に住民票コードを記載する（改正法附則３条，４条）。

(イ) 市町村長は、住民票に住民票コードを記載したときは、速やかに、その者に対し、書面により住民票コードを通知する（改正法附則５条）。

(ウ) 市町村長は、新たに住民票に住民票コードを記載する場合を除いて、住民票の記載をする場合には、その者につき、直近に記載された住民票コードを記載する（住基法３０条の２第１項）。

(エ) 以上により、各住民の住民票に全国的に重複しない住民票コードが記載される。

エ 住民票コードの変更請求

住民基本台帳に記録されている者は、市町村長に対し、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）。

(3) 本人確認情報

住基ネットにおいて利用又は提供（以下「利用提供」という。）される本人確認情報とは、住民票の記載事項のうち、①氏名、②出生の年月日、③男女の別、④住所等、⑤住民票コード及び⑥住民票の記載、消除及び修正を行った場合につき、その原因となるべき事由及びその事由が生じた年月日等である（住基法３０条の５第１項，住民基本台帳法施行令３０条の５，施行規

則 11 条。以下、①ないし④を併せて「基本 4 情報」という。))。

(4) 本人確認情報の管理、通知

ア 市町村長による管理

市町村長は、既存住基サーバと CS とを電気通信回線で接続し、既存住基サーバから CS に対して本人確認情報を送り、CS で本人確認情報を管理する（弁論の全趣旨）。

イ 都道府県知事に対する通知

市町村長は、住民票の記載等を行った場合、都道府県知事に対し、本人確認情報を通知することとされ（住基法 30 条の 5 第 1 項）、上記通知は、CS から都道府県サーバに対し、電気通信回線を通じて行われる（住基法 30 条の 5 第 2 項）。

ウ 指定情報処理機関に対する通知

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を行わせることができる（住基法 30 条の 10 第 1 項）。

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は、指定情報処理機関に対し、市町村長から通知された本人確認情報を通知することとされ（住基法 30 条の 11 第 1 項）、上記通知は、都道府県サーバから指定情報処理機関サーバに対し、電気通信回線を通じて行われる（住基法 30 条の 11 第 2 項）。

(5) 本人確認情報の提供

ア 市町村長による提供

市町村長は、他の市町村の長その他の執行機関であって条例で定める者に対し、条例で定める事務の処理に関し、本人確認情報を提供する（住基法 30 条の 6）。

イ 都道府県知事による提供

(ア) 都道府県知事は、住基法別表第 1 の上欄に掲げる国の機関等に対し、

同表の下欄に掲げる事務の処理に関し、本人確認情報を提供する（住基法 30 条の 7 第 3 項）。

(イ) 都道府県知事は、当該都道府県の区域内の市町村長に対し、住基法 30 条の 7 第 4 項各号のいずれかに該当する場合、本人確認情報を提供する（住基法 30 条の 7 第 4 項）。

(ウ) 都道府県知事は、他の都道府県知事に対し、住基法 30 条の 7 第 5 項各号のいずれかに該当する場合、本人確認情報を提供する（住基法 30 条の 7 第 5 項）。

(エ) 都道府県知事は、他の都道府県の区域内の市町村長に対し、住基法 30 条の 7 第 6 項各号のいずれかに該当する場合、本人確認情報を提供する（住基法 30 条の 7 第 6 項）。

(オ) 都道府県知事は、住基法 30 条の 8 第 1 項各号のいずれかに該当する場合、自ら本人確認情報を利用することができる（住基法 30 条の 8 第 1 項）。

ウ 指定情報処理機関による本人確認情報処理事務の処理

都道府県知事から本人確認情報処理事務の委任を受けた指定情報処理機関は、本人確認情報処理事務を行う（住基法 30 条の 10 第 1 項）。

エ 平成 17 年 4 月 1 日現在、本人確認情報の提供が認められている事務は、275 事務である（弁論の全趣旨）。

(6) 住民基本台帳カード

住民は、希望により、住民基本台帳カード（住民票に記載された氏名及び住民票コードその他政令で定める事項が記録されたカードのこと。以下「住基カード」という。）の交付を受けることができ、住基カードの交付を受けた住民は、転入転出の特例の適用などを受けることができる（住基法 24 条の 2、30 条の 44）。

(7) 改正法の施行

改正法のうち、指定情報処理機関の指定及び住民票コードの指定など制度準備に必要な規定は、平成11年10月1日に施行された（改正法附則1条1項2号，平成11年政令第302号）。

また、改正法のうち、住民票コードの記載，本人確認情報の通知，提供など，制度の基本的部分に係る規定は，平成14年8月5日に施行された（改正法附則1条1項本文，平成13年政令第430号。以下，この施行を「第1次稼働」という。）。

さらに，改正法のうち，住民票の写しの広域交付，転出転入の特例及び住基カードなどに係る規定は，平成15年8月25日に施行された（改正法附則1条1項3号，平成15年政令第20号）。

5 被告中野区の住基ネットに対する対応（弁論の全趣旨）

- (1) 中野区長は，住基ネットの第1次稼働日である平成14年8月5日，東京都知事に対し，住基法30条の5第1項所定の本人確認情報の通知を行った。
- (2) しかし，中野区長は，平成14年9月11日，被告中野区のCSと被告東京都の都道府県サーバとの間の電気通信回線の接続を切断し，以降，東京都知事に対する住基法30条の5第1項所定の本人確認情報の通知を中止した。

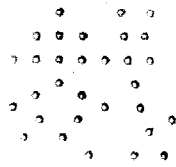
もともと，中野区長は，東京都知事に対する本人確認情報の通知を中止しながら，住基法30条の2所定の住民票コードの記載に関する事務は継続して実施した。

- (3) その後，中野区長は，平成15年8月13日，被告中野区のCSと被告東京都の都道府県サーバとの間を電気通信回線で再接続した。

中野区長は，上記再接続の際，東京都知事に対し，被告中野区が接続を切断していた期間において修正のあった本人確認情報を通知した。

第4 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）に基づく差止請求（「第1 請求」の1ないし3の請求を指す。以下同じ。）の可否



【原告の主張】

(1) プライバシー権（自己情報コントロール権）の保障と本人確認情報

ア プライバシー権（自己情報コントロール権）の保障

(ア) プライバシー権は、人格権の一内容として憲法13条によって保障される憲法上の権利である。

プライバシー権は、かつては、1人で放っておいてもらう権利として把握されていた。しかし、現代国家における積極国家化、行政国家化現象及びコンピュータによる情報処理技術の進展は、国家が、従来からは知られていない方法で個人の行動を監視し、個人を全面的に管理する危険性を増大させた。このような状況下では、国家が、関心を持つ情報については容易に収集、管理等をすることができるという心理的な圧迫を加えることで、個人の意思決定や行動に対して容易に影響を及ぼすことができるのであり、このような事態は、個人の尊厳の原理から導かれる個人の自己決定に対する重大な阻害要因となる。そこで、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せしめることが強く意識されるに至ったのであり、現代社会においては、プライバシー権としての自己情報コントロール権は、憲法によって保障された基本的人権であるというべきである。

ここでいう自己情報コントロール権とは、自己の情報を、同意なく、①収集・取得、②保有・利用、③開示・提供されず、これらを自分で決定することができる権利であり、派生的には④自己の情報の開示・訂正を請求することができる権利である。

(イ) また、原告は、被告中野区に住民登録しているところ、中野区個人情報の保護に関する条例（以下「中野区条例」という。）は、原則として、保有している個人情報をその収集目的の範囲を超えて外部提供すること及び個人情報を処理するために被告中野区の電子計算組織と被告中野区

以外の電子計算組織とを通信回線その他の方法により結合することを禁じている（中野区条例18条1項，21条1項）。

したがって，中野区条例は，憲法上保障された自己情報コントロール権を具体化しているといえることができる。

イ 本人確認情報

ある個人情報の要保護性は，いかなる当事者間において，当該個人情報がどのような状態に置かれ，どのように扱われているか，などの個別的事情によって全く異なるものであり，情報の内容から一義的に決まるものではない。また，前記のとおり，自己情報コントロール権の保障の問題は，公権力による干渉を排除して個人の自己決定権に基づき自律的に形成される領域を保護する必要性が増大してきたことに端を発しており，個人識別情報についても要保護性を否定すべきではない。これらからすれば，個人情報のすべてが自己情報コントロール権による保護の対象となるというべきである。

したがって，本人確認情報は，自己情報コントロール権による保護の対象となる。

(2) 自己情報コントロール権の侵害

ア 住基ネットは，自己情報コントロール権による保護の対象となる原告の本人確認情報を，原告の同意なく，むしろ明確な意思に反して，被告中野区以外の行政機関に対して通知，提供する形で流通させ，保有するものであるから，原告の自己情報コントロール権を侵害するものである。

イ この点，憲法13条によって保障された自己情報コントロール権は，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といえることができる。

もともと，このような制限が許されるか否かの判断に当たっては，公権力による個人情報の取扱いが問題となる場面では，情報主体の意思決定が

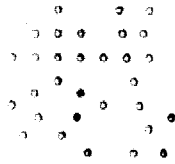
最大限に尊重されなければならない、また、前記のとおり、個人の尊厳を左右するような個人情報に関する公権力の諸活動を憲法上の規律に服させることが意識されるように至った経緯にかんがみれば、厳格な審査基準が適用されるべきである。

ウ そして、以下のとおり、住基ネットの必要性、重要性の有無を検討しても、原告が自己情報コントロール権の制限を受忍しなければならない事情はないというべきである。

(ア) 住基ネットは、これによって行政経費の節減をもたらすものではなく、かえってその維持管理費など地方公共団体に多大の経費の増大をもたらす可能性があるものである。

(イ) 住基ネットは、住民票の写しの広域交付等の利便性をもたらすとしても、これに応じて個人のプライバシーが犠牲にされるものであるから、原告のように住基ネットによる利便性よりも自らのプライバシーの保持を望む国民との間では、住基ネットが国民の利益に資するということとはできない。また、一般の国民が住民票の写しの交付を受ける機会はほとんどなく、行政機関に対する申請がすべて住民票の写しのみで足りるというわけではないなど、住基ネットによる利便性の向上は極めて限定されたものといわざるを得ない。さらに、住基カードは、その利用率が極めて低率であることから明らかなように、その有用性はないということができる。

(ウ) 電子政府・電子自治体構想、公的個人認証サービスにおける電子証明書の失効に係る事務への住基ネットの利用は、その構想等が浮上したのが改正法成立後のことであり、電子政府・電子自治体の実現が改正法の目的であり、立法事実であるというのは事実と反するというほかない。また、公的個人認証サービスは、そもそもこのようなサービスが国民から必要とされているとは考えられないものである。



エ 以上によれば、住基ネットには、原告の自己情報コントロール権を犠牲にしてまでなお達成すべき高度の必要性は存在せず、原告に対して改正法を適用することは憲法13条に違反するものである。

(3) 差止請求の可否

ア このように住基ネットは、原告の自己情報コントロール権を侵害するものであるが、自己情報コントロール権が憲法上の権利として保障される以上、原告がその侵害の排除（差止め）を求めることができることは当然とすべきである。

イ また、住基ネットは、以下のとおり、原告の個人情報の漏えい、改ざんなどの具体的危険性があるというべきであるから、差止請求が認められるべきことは一層明らかである。

(ア) 住基ネットの危険性

a セキュリティ対策の不備による危険性

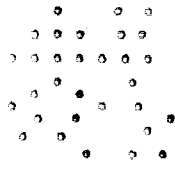
住基ネットは、そのセキュリティ対策の不備により、以下のとおり、原告の個人情報の漏えい、改ざんなどの危険性を生じさせている。

(a) 市町村、都道府県、指定情報処理機関及び本人確認情報の提供先となる国の機関等に設置された電子計算機から原告の本人確認情報が不正に閲覧される危険性がある。

(b) 既存住基サーバの原告の個人情報が不正に閲覧される危険性や既存住基サーバの原告の個人情報が改ざんされて住基ネットに流通される危険性がある。

(c) 市町村のCS端末（端末とは、電子計算機を操作するための電子計算機のことであり、CS端末とは、CSを操作するための端末のことである。）から原告の住民票の写しに係る情報を不正に取得される危険性がある。

(d) 住基カードを、原告に成りすまされて不正取得されたり、偽造さ



れたりする危険性がある。

- (e) その他、本人確認情報の提供先となる国の機関等において、原告の本人確認情報を元にして作成される各種データベースを不正に閲覧される危険性やバックアップデータを盗難等される危険性がある。

b 名寄せ、データマッチングの危険性

住基ネットは、すべての国民に対して重複しない番号として住民票コードを付すものであり、完全な個人識別を可能にするものである。そして、個人情報を保有する行政機関のコンピュータが現にネットワークで結ばれていることにかんがみれば、完全な個人識別を可能にする住民票コードの下、個人情報のデータマッチングがされ、住民票コードをマスターキーとして名寄せがされる危険性があるというべきである。これは、国民の個人情報を一元的に管理し、その一挙手一投足まで見張る国民総背番号制の現実的端緒となるものである。

c コンピュータネットワークシステム特性による危険性

住基ネットは、コンピュータネットワークシステムである。コンピュータネットワークシステムにおいては、ネットワークの1か所でも脆弱性があると、ネットワーク全体が脆弱性を有することになる。また、コンピュータ技術が日進月歩であるため、不正侵入等に対する対策情報を日常的に的確に収集し、設備や体制を更新していくことが必要である。

したがって、住基ネットは、その構造からして危険性が高いものといわざるを得ない。

(イ) 長野県侵入実験の評価

上記のような危険性は、長野県本人確認情報保護審議会委員である吉田柳太郎（以下「吉田」という。）が、平成15年9月ないし10月、長野県内の市町村において行った住基ネットの脆弱性調査（以下「長野

県侵入実験」という。)によって、現に明らかにされた。

a すなわち長野県侵入実験によれば、住基ネットに対し、以下のような不正攻撃ができることが判明した。

(a) CSが設置されている区画に攻撃端末を接続する方法により、CSやCS端末の管理者権限を略奪することができる。

(b) 既存住基サーバにつながる庁内LAN（庁舎の構内通信網のこと。）に攻撃端末を接続する方法により、既存住基サーバの管理者権限を略奪した上で、庁内LANとCSとの間にあるファイアウォール（ネットワークにおいて不正な通信を制御する電子計算機のこと。）を突破してCSの管理者権限を略奪し、CS端末の管理者権限を略奪することができる。

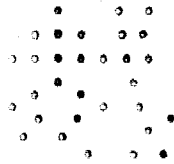
(c) 既存住基サーバの個人情報を改ざんなどし、その情報をCSに送信する方法により、CSの本人確認情報を改ざんなどすることができる。

b したがって、原告の個人情報には、以下のような危険性が生じている。

(a) 被告中野区以外の市町村にあるCS端末の管理者権限が略奪され、CS端末が攻撃端末から遠隔操作されることにより、CS、都道府県サーバ及び指定情報処理機関サーバの原告の本人確認情報が不正に閲覧されるほか、住民票の写しの広域交付がされる危険性がある。

(b) 被告中野区の既存住基サーバが不正侵入されることにより、既存住基サーバの住民票コード付きの原告の個人情報が不正に閲覧されるほか、既存住基サーバの原告の個人情報が改ざんなどされ、その情報がCSに送信されることにより、CSの原告の本人確認情報が改ざんなどされる危険性がある。

(ウ) 原告のみの離脱であること



原告は、住基ネットから原告のみの離脱を求めているから、差止請求によって生じる住基ネットへの支障の程度は低いといえることができる。

したがって、差止請求のための危険性といっても、住基ネット全体の運用を差し止めるために必要な危険性とははるかに低い危険性で足りるというべきである。

- (4) 以上によれば、原告は、自己情報コントロール権に基づき、差止請求をすることができるというべきである。

【被告らの主張】

- (1) プライバシー権（自己情報コントロール権）と本人確認情報

ア プライバシー権（自己情報コントロール権）

(ア) 自己情報コントロール権は、その内容、範囲及び法的性格に関し、様々な見解があり、その概念は不明確であり、権利として成熟性が認められないから、実体法上の権利とは認められず、憲法13条によって保障されるものではない。

また、自己情報コントロール権を肯定する見解には、自己に関するすべての情報がその権利の対象になるとすると広範にすぎる一方、保障の程度に差を付けようとしてもその区別は必ずしも明確ではないこと、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のは、憲法13条の文言解釈を逸脱するのではないかとの疑問があることなど、少なからず問題がある。

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、原告が主張するように、自己の情報を、同意なく、①収集・取得、②保有・利用、③開示・提供されず、これらを自分で決定することができることを内容とする権利とは認められない。

(イ) 中野区条例は、自己情報コントロール権を具体化するものではない。

また、中野区条例は、個人情報の外部提供の禁止及び電子計算組織の結合の禁止につき、法令の定めがある場合を除外しているところ（中野区条例18条1項1号、21条1項1号）、住基法は上記法令に該当するから、被告中野区が住基ネットに接続したことや東京都知事に対して本人確認情報を通知したことは、何ら中野区条例に反するものではない。

イ 本人確認情報

本人確認情報は、個人を識別するための単純な情報であり、およそ個人の人格的自律にかかわらない客観的、外形的事項に関するものであるから、プライバシーに係る情報としての法的保護の対象にならないことは明らかである。

(2) 自己情報コントロール権が侵害されていないことなど

ア 仮に、本人確認情報が自己情報コントロール権による法的保護の対象になるとしても、住民票記載に係る情報は、もともと住民に届出義務があり、かつ、人間の社会生活の基礎となる情報であるから、いわば公共領域に属する情報である。行政機関は、行政目的で行政機関内部で使用する限り、このような情報を個人の承諾なく使用することができるというべきである。

住基ネットは、本人確認情報を行政目的で行政機関内部で使用するものであるから、原告の自己情報コントロール権を侵害しないことは明らかである。

イ 住基ネットは、行政サービスの向上と行政事務の効率化を目的とする重要なシステムである。

すなわち、高度に情報化された現代社会において、民間部門では、コンピュータネットワークシステムが構築、活用されており、顧客サービスの向上や業務の効率化が積極的に進められてきている。このような中であって、行政も、全国的な広がりを持った住民の移動や交流という実態に合わ

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る。そのためには、市町村や都道府県の区域を越えた本人確認システムが必要不可欠であり、行政部門において、民間部門と同様に、情報通信技術を的確に活用することが必要不可欠であるといえる。そして、住民基本台帳の全国的な電算化が進んでいることから、これをネットワークで接続すれば、全国的な本人確認システムを安価に構築することができるし、住民にとっては面倒な行政手続が簡略化され、行政職員の削減も可能となる。

住基ネットは、このような発想から生まれたシステムであって、その目的は、行政サービスの向上と行政事務の効率化である。そして、住基ネットの導入により、住民は申請、届出及び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。

原告の主張は、以上のような住基ネットの必要性、重要性を正しく理解しないもので、失当である。

(3) 差止請求の可否

ア 差止請求は、その根拠となる権利に排他性があることが必要である。しかし、自己情報コントロール権は、前記のとおり、その概念は不明確であり、憲法13条によって保障されるものではなく、ましてや排他性を有する権利とはいえない。また、仮に、自己情報コントロール権がプライバシー権の一内容に含まれるとしても、プライバシー権の概念自体がいまだ不明確であり、統一的な理解が得られていないものであるから、そもそもプライバシー権を名誉権と同様の排他性を有する権利であるととらえることはできない。

したがって、自己情報コントロール権に基づく差止請求は認められないというべきである。

イ また、住基ネットには、以下のとおり、原告の個人情報の漏えい、改ざ

んななどの具体的危険性は存在しないから、差止請求が認められないのは、一層明らかである。

(ア) セキュリティ対策が取られていること

a 制度面からの対策

(a) 本人確認情報の利用提供の限定

本人確認情報の提供を受ける行政機関及び事務の範囲は、住基法及び条例で具体的に規定されるなど、本人確認情報の利用提供は、限定されている。

(b) 住民票コードの利用の制限

民間部門は、住民票コードを利用することを禁止されており、行政部門が住民票コードを利用する場合も、目的外利用の禁止及び告知要求制限等の制限がされている。

(c) 緊急時対応計画の策定

市町村長、都道府県知事及び指定情報処理機関は、緊急時対応計画を策定することされ、本人確認情報の漏えい、改ざんなどの具体的危険性が発生した場合、電気通信回線の切断を含む措置等を講じることができる。

b 外部からの侵入防止対策（物理的なセキュリティ対策）

住基ネットを運営する関係機関は、重要機能室の配置及び構造並びに入退室管理等、外部からの侵入に対する物理的なセキュリティ対策をすることとされている。

c 外部からの侵入防止対策（電気通信回線経路による侵入に対する対策）

(a) 専用回線及び専用交換装置の採用

住基ネットを構成する電子計算機間の通信は、すべて専用回線及び専用交換装置（以下「専用回線等」という。）で構成されたネッ

ネットワークを介して行われ、また、指定情報処理機関サーバと国の機関等の電子計算機との間は、専用回線等又は磁気媒体でデータ交換を行うなど、閉鎖的ネットワークが実現されている。

(b) 相互認証及び暗号通信の実施

住基ネットを構成する電子計算機間では、相互認証（接続する相手が正しいか否かの確認を相互に行うこと。）を行い、暗号通信を実施している。

(c) ファイアウォールの設置

住基ネットには、指定情報処理機関が監視するファイアウォールなどが設置され、住基ネットを構成する電子計算機は、不正な通信から防御されている。

d 内部の不正防止対策

(a) 重い刑罰や監督による不正行為の防止

住基法や関係法令は、住基ネット担当職員に対し、重い刑罰による秘密保持に関する義務を課している。

(b) 本人確認情報の照会条件の限定

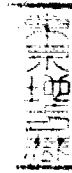
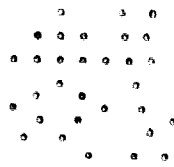
住基ネット担当職員が、本人確認情報を検索する際、照会条件が限定されており、多くの本人確認情報の提供を受けないようにされている。

(c) 操作者識別カードによる接続の制御

住基ネットを構成する電子計算機に端末から接続するためには、操作者識別カードと端末との間の相互認証が必要であり、権限のない職員は住基ネットに接続することができない。

(d) 住民票の写しの広域交付における不正防止

住所地市町村において、交付地市町村の特定の操作者識別カードから一定時間に一定数以上の住民票の写しの広域交付要求があった



場合、システム上、住民票の写しの広域交付を停止する措置が講じられる。

e 住基カードのセキュリティ対策

住基カードは、希望者のみに対し、交付される。また、住基カードは、技術的なセキュリティ対策として、これにＩＣカードを用いることとし、暗証番号の設定、外部から情報の読み取り又は解析ができない仕組みを取るなどして安全性を確保している。

(イ) 長野県侵入実験の評価

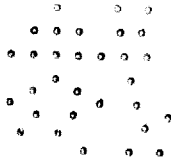
長野県侵入実験は、インターネットから庁内ＬＡＮへの侵入及び庁内ＬＡＮからＣＳが設置されている区画への侵入にことごとく失敗したものである。長野県侵入実験により、本人確認情報に対する危険性がないことが明らかにされた。わずかに、一部の市町村において、庁舎内に人間が文字どおり物理的かつ違法に侵入した上、攻撃端末が接続された場合などに、市町村の庁内ＬＡＮにある当該市町村の住民の個人情報という限定された情報について、漏えい、改ざんなどの可能性があることが示されたにすぎない。

(ウ) 名寄せ、データマッチングの危険性がないこと

住基法や関係法令は、住基法が認める以外の本人確認情報の利用提供を禁止するとともに、これに違反した場合には懲戒処分や罰則を課し、合などに、市町村の庁内ＬＡＮ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、漏えい、改ざんなどの可能性があることが本人確認情報のみを保有するという住基ネットの仕組みから、名寄せ、データマッチングの危険性はないというべきである。

(エ) 原告のみの離脱の影響は大きいこと

原告のみが住基ネットから離脱することを認めると、原告のみのために既存住基システムを存置しなければならないなど、住基ネットの目的



である行政事務の効率化を害することが明らかである。

- (4) 以上によれば、自己情報コントロール権は、差止請求を認めることができるような排他性を有する実体法上の権利ではない上、住基ネットは、原告の個人情報の漏えい、改ざんなどの具体的危険性を有するものではないから、差止請求が認められないことは明らかである。

2 氏名権に基づく差止請求の可否

【原告の主張】

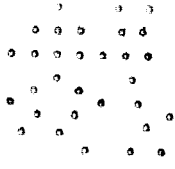
- (1) 憲法13条は、国民はその有する氏名を中核として、他と識別され、取り扱われることを内容とする権利利益（以下、この権利利益を「氏名権」という。）を保障している。
- (2) 住基ネットは、すべての国民に対し、重複しない識別番号として11けたの数字から成る住民票コードを付すものである。住基ネットは、個人の特定を氏名によってではなく、住民票コードで行うものであり、住基ネットにおいて、氏名は、住民票コードで分類される個人情報の中の1つにおとしめられることになる。

住基ネットにより国民に対して住民票コードを付すことは、単に氏名の不正確な呼称という問題にとどまらず、そもそも人を氏名で扱わず、番号で扱うものである上、原告の明示の意思に反するものであるから、原告の氏名権の侵害の程度は深刻である。

- (3) このように氏名権の侵害が深刻である以上、原告の住民票コードの削除を含む差止請求により、速やかにその回復が図られるべきである。

【被告らの主張】

- (1) 原告が主張する氏名権を認める法文や判例上の根拠は全く存在せず、これを憲法13条に基づく人格権の一内容として認める余地はない。
- (2) 住民票コードは、基本4情報を電子計算機及び電気通信回線を用いて効率的に送信するために、技術上新たに設けられた符号にすぎず、そもそも個人



の人格的価値とは無関係である。

(3) したがって、氏名権に基づく差止請求が認められないことは明らかである。

3 公権力によって包括的に管理されない自由権に基づく差止請求の可否

【原告の主張】

- (1) 憲法 13 条は、各行政機関において、それぞれ個別に保有する個人情報、他の行政機関と交換するなどして有機的に結合し、いつでも利用することができる状態に置かれることを拒絶する権利（以下、この権利を「公権力によって包括的に管理されない自由権」という。）を保障している。
- (2) 国民に付された住民票コードは、名寄せの検索キーとして使われることが前提となっている。住基ネットが稼働されることにより、各行政機関において、それぞれが個別に保有する個人情報を他の行政機関と交換するなどして有機的に結合し、いつでも利用することができる状態になっており、公権力による個人情報の一元的管理を可能にする状態が生じているから、原告の公権力によって包括的に管理されない自由権の侵害の程度は深刻である。
- (3) このように公権力によって包括的に管理されない自由権の侵害が深刻である以上、侵害行為である公権力の行為を直ちに排除する緊急の必要があり、差止請求が認められなければならない。

【被告らの主張】

- (1) 原告が主張する公権力によって包括的に管理されない自由権を認める法文や判例上の根拠は全く存在せず、これを憲法 13 条に基づく人格権の一内容として認める余地はない。
- (2) 住民票コードは、技術上の符号にすぎず、個人の人格的価値と無関係であるし、住基ネットの運用により、国民が行政によって包括的に管理されるなどという事態が生じるものではないことは明らかである。
- (3) したがって、公権力によって包括的に管理されない自由権に基づく差止請求が認められないことは明らかである。

4 プライバシー権等の侵害などによる損害賠償請求の可否

【原告の主張】

(1) 被告国の責任

ア 内閣総理大臣及び総務大臣並びに内閣（以下「内閣総理大臣ら」という。）は、憲法11条、13条及び99条により、憲法を遵守し、国民の人権を保護する義務を負っているところ、改正法は、国民のプライバシー権等を侵害するものであるから、内閣総理大臣らは、改正法を廃止し、又はその施行を延期する義務があったというべきである。

また、改正法附則1条2項によれば、内閣総理大臣らは、改正法の施行に当たっては、速やかに、個人情報の保護に万全を期すための所要の措置（以下「所要の措置」という。）を講じる義務があったというべきである。ここに所要の措置とは、具体的には、行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律の個人情報保護制度の不備を改め、同法を行政機関の行為を厳格に規制する制度に改正することを含めて、個人情報保護法制を整備することである。この所要の措置は、住基ネットの運用に関し、憲法によって保障された人権である国民のプライバシー権等を保護するための必要不可欠な措置といえることができる。

ウ しかしながら、内閣総理大臣らは、所要の措置を講じないまま、平成14年8月5日に改正法を施行した（第1次稼働）。

なお、上記施行後に成立した個人情報保護関連5法（①個人情報の保護に関する法律、②行政機関の保有する個人情報の保護に関する法律、③独立行政法人の保有する個人情報の保護に関する法律、④情報公開・個人情報保護審査会設置法、⑤行政機関の保有する個人情報保護法等の施行に伴う関係法律の整備等に関する法律）は、住基ネットの運用に関し、プライバシー権等の保護に対する万全の措置とは到底いい難いものである。

エ 内閣総理大臣らが、上記のとおり、改正法を施行したことにより、原告



は、プライバシー権等を侵害され、精神的苦痛を被った。これを慰謝するのに相当な慰謝料額は、50万円を下らない。また、原告は、本件訴訟を原告訴訟代理人らに委任しており、上記慰謝料額の1割に相当する5万円の弁護士費用は、相当因果関係のある損害である。

オ したがって、原告は、被告国に対し、国家賠償法1条1項による損害賠償請求権に基づき、損害金55万円及びこれに対する訴状送達の日翌日である平成14年9月20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支払を求める。

(2) 被告東京都及び被告センターの責任

ア 東京都知事は、憲法11条、13条及び99条により、憲法を遵守し、都民の人権を保護する義務を負っているところ、改正法は、都民のプライバシー権等を侵害するものであるから、東京都知事は、住基ネットから離脱するなど本人確認情報の適切な管理のために必要な措置を講じる義務があったというべきである。

イ しかしながら、東京都知事は、住基ネットから離脱するなど本人確認情報の適切な管理のために必要な措置を講じずに、被告センターに対して原告の本人確認情報を通知するなど、住基法所定の行政事務を実施した。また、被告センターは、改正法が原告のプライバシー権等を侵害するものであるにもかかわらず、住基法上の指定情報処理機関として、東京都知事から委任を受け、原告の本人確認情報処理事務を実施した。

ウ この結果、原告は、プライバシー権等を侵害され、前記と同様に慰謝料50万円及び弁護士費用5万円の損害を被った。

エ したがって、原告は、被告東京都及び被告センターに対し、国家賠償法1条1項及び不法行為による損害賠償請求権に基づき、連帯して損害金55万円及びこれに対する訴状送達の日翌日である平成14年9月20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支払を求め

る。

【被告らの主張】

(1) 被告国の責任

改正法は、憲法に違反するものではないから、内閣総理大臣らにおいて、改正法を施行したことが違法となる余地はない。

また、所要の措置とは、改正法成立当時の状況から判断して、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、内閣が立法機関ではないことからして、法律案の検討、作成及び国会への提出を意味するものである。そして、内閣は、平成13年3月、国会に対し、個人情報の保護に関する法律案を提出しているから、所要の措置が講じられたことは明らかである。

(2) 被告東京都及び被告センターの責任

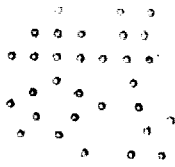
改正法は、憲法に違反するものではないから、東京都知事が住基法所定の行政事務を実施したこと及び被告センターが東京都知事から委任を受け、原告の本人確認情報処理事務を実施したことが違法となる余地はない。

第5 争点に対する判断

1 プライバシー権（自己情報コントロール権）に基づく差止請求について

(1) プライバシー権について

ア 憲法13条は、個人の尊厳の原理を踏まえ、個人の幸福追求の権利の尊重等を規定している。そして、個人が個人として尊重されるためには、個人の私的な生活領域の尊重が必要不可欠である。したがって、憲法13条は、個人の私的な生活領域が干渉されない利益としてのプライバシー権を保障しているというべきである。さらに、コンピュータの普及等に伴う情報化社会の進展によって、国家権力や企業による広範な分野に及ぶ個人情報の収集、保有、利用及び伝播等が可能となり、個人情報の濫用のおそれが増大した現代社会の状況にかんがみれば、プライバシー権は、その内容



を「1人にしておいてもらう権利」としてとらえるだけでは足りず、個人に関する情報が利用提供されることにつき、当該個人の意思が尊重され、個人の同意なく、みだりにこれを利用提供されない権利利益としてとらえることが相当であり、憲法13条は、このような権利利益をも保障していると解される。

これを国家権力との関係でいうならば、憲法13条は、個人の私生活上の自由の1つとして、個人の同意なく、みだりに個人情報を利用提供されない自由を保障しているというべきであり、国家機関が正当な理由もなく、個人の同意なく、みだりに個人情報を利用提供することは、同条に反して許されないというべきである。

イ 住基ネットにおいて利用提供がされる本人確認情報は、氏名、生年月日、性別、住所及び住民票コード等から構成されるものであり、個人情報といえることができるから、上記自由における保護の対象になる。

ウ しかしながら、上記自由も、国家権力の行使に対して無制限に保護されるものではなく、公共の福祉のため必要がある場合には相当の制限を受けることは、憲法13条に定められているところである。

そして、上記自由の制限が公共の福祉による制限として許容されるか否かは、住基ネットにおける個人情報の利用提供の目的に必要性、合理性があるか否か、住基ネットにおける個人情報の利用提供の態様が一般的に許容される限度を超えない相当なものであるか否かという基準によって判断すべきである。

エ そこで、以下、①住基ネットにおいて利用提供される個人情報である本人確認情報の利用提供の目的の必要性、合理性、②本人確認情報の利用提供の態様の相当性をそれぞれ検討する。なお、本人確認情報の利用提供の態様の相当性については、本人確認情報の利用提供の態様そのものと利用提供によって生じる本人確認情報の漏えい、改ざんなどの危険性の程度と

に分けて検討する。

(2) 住基ネットにおける本人確認情報の利用提供の目的の必要性、合理性

ア 証拠（丙 3 ないし 11, 42 ないし 54, 88 ないし 107）及び弁論の全趣旨によれば、以下の事実が認められる。

(ア) 住基法の目的

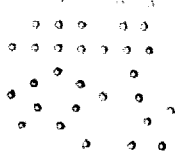
住基法は、住民の住所の変更等に伴う各種届出を一本化し、また、住民に関する記録を正確かつ統一的に行うため、住民基本台帳の制度を定めるものであり、住民の利便性の増進並びに国及び地方公共団体の行政事務の効率化に寄与するという目的を有するものである（住基法 1 条）。

(イ) 改正法の目的

住基法には上記の目的があったところ、住基ネットの導入を定めた改正法は、社会の高度情報化、住民の移動や交流の広域化及び住民基本台帳の電算化の全国的な進展などの状況を踏まえ、各市町村に備え付けられていた住民基本台帳をコンピュータネットワークで結び、従前は市町村長のみが保有していた住民の基本 4 情報に住民票コードを付した上で本人確認情報として他の市町村長、都道府県知事及び国の機関等に対して提供することなどにより、多くの行政手続において住民票の写しなどの提出を不要とするとともに、住民票の写しの広域交付を行い、転入転出手続を簡素化し、もって、行政事務の効率化、住民負担の軽減や住民の便益の向上を図ることを目的として成立したものである。

また、政府は、改正法成立後、住基ネットを電子政府・電子自治体の実現のための本人確認手段として必要不可欠な制度として位置付けるようになった。

さらに、行政手続のオンライン化に当たっては、本人確認のための公的個人認証サービスにおいて電子証明書を利用することが必要になるところ、政府は、改正法成立後、住所の異動等に伴う電子証明書の失効に



係る事務を効率的かつ正確に行うための制度として、住基ネットを利用するようになった。

(ウ) 行政事務の効率化、住民負担の軽減

住民基本台帳は、住基ネットの導入前、各市町村ごとに備え付けられていた。そのため、行政機関は、その事務を行うために住民に関する基本4情報を必要とする場合、各事務ごとに、住民に対し、住民票の写しなどの添付等を求めている。しかし、住基ネットが導入され、例えば、以下のとおり、多くの行政手続で住民票の写しなどの添付等が必要でなくなった。

- a 住民は、パスポートの交付申請などの際に必要とされていた住民票の写しの提出が不要になり、住民票の写しの交付請求に伴う窓口への出頭、手数料の支払などの負担を免れた。他方、市町村は、住民票の写しの交付に伴う事務を削減することができた。

結果として、年間約300万枚の住民票の写しの提出が不要になっている。

- b 年金受給者は、毎年提出することが必要とされていた現況届又は身上報告書の提出が不要になり（ただし、加給年金対象者等を除く。）、現況届等の提出に伴う書面への記入、年金支給機関への郵送などの負担を免れた。他方、年金支給機関は、年金受給者の現況届等の提出に伴う事務を削減することができたほか、年金支給の都度、受給権を確認することができ、過誤払を削減することができた。

結果として、年間約500万枚の現況届等の提出が不要になっている。

- c 恩給受給者は、毎年市町村長の証明印を受けて提出することが必要とされていた受給権調査申立書の提出が不要になり、受給権調査に伴う負担を免れた。他方、市町村は、受給権調査申立書の提出に伴う事

務を削減することができたほか、恩給支給の都度、受給権を確認することができ、過誤払を削減することができた。

結果として、年間約140万枚の受給権調査申立書の提出が不要になっている。

(エ) 住民の便益の向上

住基ネットの導入により、①住民が、全国の市町村において、住基カード等の提示により、本人や同一世帯の住民票の写しの交付を受けることが可能になり（住基法12条の2）、②住基カードの交付を受けている住民は、転入転出する場合、転出地市町村長に対して付記転出届を提出すれば、転入地市町村役場に1回出向くだけで、転入転出手続をすることが可能になった（住基法24条の2）。

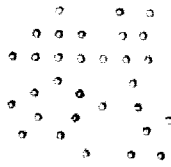
イ 以上のとおり、住基ネットは、行政事務の効率化、住民負担の軽減を図るとともに、住民の便益を向上させることを目的とするものであり、その目的には必要性、合理性を認めることができる。

なお、電子政府・電子自治体の実現、公的個人認証サービスにおける電子証明書の失効に係る事務への住基ネットの利用は、時期的にみて、それ自体が直接的に改正法の目的であるということとはできない。しかしながら、電子政府・電子自治体の実現及び電子証明書の失効に係る事務への住基ネットの利用は、社会の高度情報化等に伴い、住民の利便の増進並びに国及び地方公共団体の行政事務の効率化を図るという改正法の目的を発展させたものといえることができ、これらは、改正法の目的の必要性、合理性を支えるものというべきである。

(3) 住基ネットにおける本人確認情報の利用提供の態様の相当性

ア 本人確認情報の利用提供の態様

(ア) 住基ネットは、前記のとおり、従前は市町村ごとに保有されていた基本4情報を、住民票コードを付した上で本人確認情報として、個々の住



民の同意の有無にかかわらず、コンピュータネットワークを通じて、市町村の区域を越えて、他の市町村長、都道府県知事及び国の機関等に対し、提供するものである。

- (イ) しかしながら、住基ネットにおいて利用提供される本人確認情報のうち、基本4情報は、人が社会生活を営む上で、一定範囲の他者に対し、必然的に開示され、利用されている情報であり、個人の思想、信条等に関する情報と比べると、平均的な一般人がその開示に苦痛を感じる程度は相対的には低いものである。

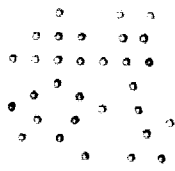
また、基本4情報は、改正法施行前から住民基本台帳の記載事項とされ、住民はこれらの情報について市町村長に対して届出義務があり、届出を受けた市町村長はその情報を住民基本台帳に記載して保有していたものである。そして、行政機関が行政事務を処理するに当たって必要がある場合など正当な理由があるときは、社会通念上、これを使用することが容認されている情報である。

さらに、住民票コードは、基本4情報の利用提供に当たって、技術上これを効率的に送信するための便宜的数字であり、それ自体に格別の意味がある数字ではない。

したがって、このような情報が結合された本人確認情報は、個人の人格的自律に直接かかわるものとまではいえないし、社会通念上、個人の思想、信条等に関する情報と比べて、秘匿の必要性が必ずしも高いということはできないものである。

- (ウ) そして、住基法は、住基ネットにおいて本人確認情報の提供を受ける行政機関及び事務を制限しており（住基法30条の6、30条の7第3項ないし第6項、30条の8）、住基法又は条例に定めがない行政機関及び事務に本人確認情報を利用提供することはできない。

また、住民票コードの利用についても、次のとおりの制限がある。



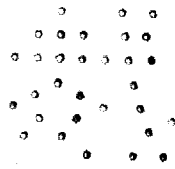
a 民間部門は、契約に際して住民票コードの告知を求めたり、住民票コードが記録され、他に提供されることが予定されたデータベースを作成したりしてはならないとされている（住基法30条の43第3項）。都道府県知事は、これらに違反する行為をした者に対し、中止勧告及び中止命令等を行うことができ（住基法30条の43第4項、第5項）、この中止命令に違反した者は、1年以下の懲役又は50万円以下の罰金に処せられるとされている（住基法44条）。

b 市町村長等は、住基法で認められる場合を除き、何人に対しても、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）。

(エ) 以上によれば、本人確認情報は、その秘匿の必要性が必ずしも高くない上、住基ネットにおける本人確認情報の利用提供は、住基法又は条例で定められた行政機関及び事務に限定されていること、住民票コードについては、住基法又は条例で定められた行政機関及び事務以外の方法で利用することを特に禁止していることが認められ、住基ネットにおける本人確認情報の利用提供の態様は、限定されたものであるといえることができる。

(オ) 加えて、本人確認情報の利用提供は本人の同意の有無にかかわらず一律に行われるが、証拠（甲84、丙31）及び弁論の全趣旨によれば、原告のみの住基ネットからの離脱を認めると、住基ネット導入前の既存の制度を存置せざるを得なくなることが認められ、このような事態は、国及び地方公共団体の行政事務の効率化という住基ネットの目的に反し、混乱を招くことが明らかであり、同意の有無にかかわらず一律に本人確認情報を利用提供することは必要かつやむを得ない方法であるといえるべきである。

イ 住基ネットにおける本人確認情報の漏えい、改ざんなどの危険性の程度



後掲証拠及び弁論の全趣旨によれば、住基ネットにおける本人確認情報の利用提供によって生じる本人確認情報の漏えい、改ざんなどの危険性の程度に関し、以下のとおり認められる。

なお、プライバシー権等に基づき、住基ネットの差止めを求めたり、国家賠償法又は不法行為による損害賠償請求権に基づき、慰謝料等の支払を求めたりするに当たって、これらの請求権を基礎付けるものとして主張される本人確認情報の漏えい、改ざんなどの危険性の主張立証責任は、これらの請求権の存在を主張する原告が負担するものと解される。

(ア) セキュリティ対策

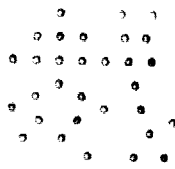
住基法には、住基ネットのセキュリティ対策に係る事項が定められている。また、総務大臣は、総務省告示をもって、住基ネットのセキュリティ対策として、「電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準」（以下「セキュリティ基準」という。）を定めるとともに、住基カードのセキュリティ対策として、「住民基本台帳カードに関する技術的基準」（以下「住基カードセキュリティ基準」という。）を定めている。

これらの住基ネットのセキュリティ対策をまとめると、以下のとおりである（丙12）。

a 物理的なセキュリティ対策

(a) 重要機能室の管理等

CS、都道府県サーバ及び指定情報処理機関サーバといった住基ネットを構成する電子計算機を設置する部屋を重要機能室とし、壁、窓及びドア等が容易に破壊されないような措置を講じるとともに、侵入を検知するための措置を講じることとされている（セキュリティ基準第3-1-(1)）。



また、重要機能室は、原則として他の部屋と区別した専用の部屋とし、仮に専用の部屋を確保することができない場合は、電子計算機を厳重に固定する措置を取ることとされている（セキュリティ基準第3-1-(2)）。

さらに、所定の者が、所定の場所において、重要機能室の出入口のかぎを管理するほか、入退室管理カードの管理方法を定めるとされ、重要機能室の入退室管理を適切に行うこととされている（セキュリティ基準第4-1）。

(b) 専用回線等の使用

住基ネットを構成する電子計算機間の通信は、専用回線等を使用することとされ、閉鎖的ネットワークが実現されている（セキュリティ基準第3-3-(1)）（丙39の1, 2）。

b 技術的なセキュリティ対策

(a) 通信の相互認証・暗号化

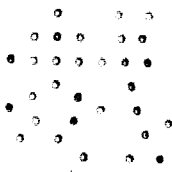
住基ネットを構成する電子計算機間の通信は、通信相手の相互認証及び交換するデータの暗号化を行うこととされている（セキュリティ基準第4-3-(4), (5)）。

(b) ファイアウォールの設置

市町村、都道府県及び指定情報処理機関には、以下のとおり、ファイアウォールが設置され、不正な通信を制御している（セキュリティ基準第4-3-(2), 第5-1-(3), (6)）（丙29の1, 2）。

① 市町村

庁内LANとCSとの間には、指定情報処理機関の提示にそった設定のファイアウォールが設置される。CSが都道府県サーバ等と接続される側には、指定情報処理機関が監視するファイアウォールが設置される。



また、庁内LANをインターネットと接続するときは、その間にファイアウォールが設置される。

② 都道府県

都道府県サーバが他の都道府県サーバ等と接続される側には、指定情報処理機関が監視するファイアウォールが設置される。

また、庁内LANに都道府県サーバの端末を設置する場合、庁内LANと都道府県サーバとの間に指定情報処理機関が監視するファイアウォールが設置される。

③ 指定情報処理機関

指定情報処理機関サーバが指定情報処理機関以外の機関の電子計算機と接続される側には、指定情報処理機関が監視するファイアウォールが設置される。

(c) 指定情報処理機関による通信の監視

指定情報処理機関は、上記のとおり設置された指定情報処理機関が監視するファイアウォールなどにより、不正な通信について監視を行っている（セキュリティ基準第4-9-(3)）（丙60, 61）。

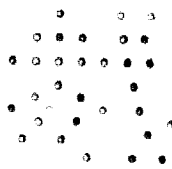
c 人的なセキュリティ対策

(a) 操作者識別カード等によるアクセス制御

住基ネットの業務を行うためのソフトウェアを起動するためには、操作者識別カード及び暗証番号が必要である（セキュリティ基準第4-4-(2)ないし(4)）。

(b) 本人確認情報の提供方法の限定等

住基ネット担当職員が、本人確認情報の提供を受ける際、提供される本人確認情報の数を限定するなど、一度に多くの本人確認情報の提供がされないように提供方法が限定されている（セキュリティ基準第4-4-(7)）。



また、住民票の写しの広域交付では、住所地市町村において、交付地市町村の特定の操作者識別カードから一定時間に一定数以上の交付要求があった場合、住民票の写しの広域交付が停止される。

(c) 刑罰等による不正行為の防止

住基ネット担当職員が、本人確認情報を住基法所定の範囲外で利用提供したときは、職務上の義務違反として、懲戒処分の対象となる（国家公務員法 82 条 1 項 2 号，地方公務員法 29 条 1 項 2 号）。

さらに、住基法は、住基ネット担当職員及び行政機関又は指定情報処理機関から本人確認情報の電子計算機処理等の委託を受けた者に対し、本人確認情報処理事務等に関して知り得た本人確認情報に関する秘密及び本人確認情報の電子計算機処理等に関する秘密の保持義務を課し、上記義務に違反して秘密を漏らした者を、2 年以下の懲役又は 100 万円以下の罰金に処するものとしている（住基法 30 条の 17，30 条の 31，30 条の 35，42 条）。

また、行政機関以外の者に対しても、不正アクセス行為の禁止等に関する法律が、刑罰をもって、不正アクセス行為を禁止し、不正行為を防止している。

d 住基カードのセキュリティ対策

(a) 交付は希望者のみであること

住基カードは、これを申請した住民に対してのみ交付される（住基法 30 条の 44 第 1 項ないし第 3 項）。

(b) 利用領域の制限

民間部門は、住基カード内の住基ネットで利用する領域を利用してはならず、行政部門は、住基法で認められる場合を除き、上記領域を利用してはならないとされている（住基カードセキュリティ基準第 4-1）。



(c) 技術的セキュリティ対策

住基カードは、中央演算処理装置付きの半導体集積回路を組み込んだカードを用いることとされ（住基カードセキュリティ基準第2-1）、半導体集積回路に物理的又は電氣的な攻撃を加えて、住基カードに記録された情報を取得することが困難な仕組みを保持することとされている（住基カードセキュリティ基準第2-2-(5)）。

e 住民票コードの変更

住民は、市町村長に対し、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）。

f 小括

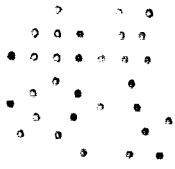
住基ネットにおいては、上記のセキュリティ対策がとられているところ、これらの対策は、本人確認情報の漏えい、改ざんなどを防止するための相応の措置と評価することができる。

もとより、これらのセキュリティ対策がとられていても、なお住基ネットの担当者が、自己の担当した事務に関する本人確認情報を漏えいすることなどの可能性は絶無ではない。しかし、このような行為は刑罰等をもって禁止されているのであるから、あえて違法な犯罪行為等を想定し、そのことを前提として、制度の危険性を判断することは相当ではない。また、前記アの(イ)記載のとおり、住基ネットで利用提供される本人確認情報の秘匿の必要性が必ずしも高度ではないことを考慮すると、その漏えい、改ざんについて前記の程度の若干の可能性が否定できないとしても、制度全体では相応の安全性を有していると評価してよいというべきである。

(イ) 名寄せ、データマッチングの可能性

a 住基ネットの仕組み

前記前提となる事実のとおり、本人確認情報の提供が認められてい



る事務は、平成17年4月1日現在、275事務であるところ、弁論の全趣旨によれば、これらの事務に関して行政機関が保有する個人情報を一元的に管理する主体は存在しないことが認められる（指定情報処理機関には、市町村等の行政機関からその保有する本人確認情報以外の住民に関する情報を収集、保有する権限はなく、市町村等の行政機関が、そのような情報を指定情報処理機関に対して提供することはない。）。

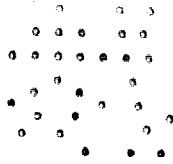
また、住基法の規定により本人確認情報の提供を受けた者（市町村長、都道府県知事及び国の機関等。以下「受領者」という。）は、住基法所定の範囲内に限り、本人確認情報を利用提供することとされている（住基法30条の34）。したがって、受領者は、住基法所定の範囲内に限り、本人確認情報とその保有する個人情報とを、比較、検索及び結合することができるものであり、その範囲外においては、比較、検索及び結合することはできない。

b 小括

以上によれば、住基ネットが利用される事務に関して行政機関が保有する個人情報を一元的に管理する主体は存在せず、かつ、特定の行政機関が自己の有する個人情報と他の行政機関が有する個人情報とを比較、検索及び結合することは認められていないのであるから、現行法制の住基ネットにおいて、原告の個人情報について名寄せ、データマッチングの危険性があるとはいえない（原告の主張は、将来の法改正等による名寄せ、データマッチングの抽象的危険性を主張するものであって、現行法制の住基ネットの危険性を基礎付けるものとはいえない。）。

(ウ) 長野県侵入実験について

証拠（甲32の1ないし4、甲41、証人吉田のほか、個別に掲記す



る。)及び弁論の全趣旨によれば、以下の事実が認められる。

- a 長野県知事は、平成15年9月22日付け文書及び同年11月21日付け文書をもって、長野県本人確認情報保護審議会委員である吉田に対し、住基ネットに係る市町村ネットワークの脆弱性調査を依頼し、吉田は、上記各文書に基づき、長野県阿智村、下諏訪町及び波田町において、調査を実施した（長野県侵入実験）（甲33の2ないし5）。なお、阿智村における調査は、2度にわたり実施された。

b 長野県侵入実験の内容及び結果

(a) 阿智村（第1次）

阿智村（第1次）の調査は、平成15年9月22日から同月24日までの間、出先機関であるコミュニケーションセンターの会議室の接続口等から庁内LANに攻撃端末を接続し、既存住基サーバの管理者権限を取得することや庁内LANとCSとの間に設定されているファイアウォールを突破してCSの管理者権限を取得することが試みられた。

この結果、既存住基サーバの管理者権限を取得することができたが、上記ファイアウォールを突破してCSの管理者権限を取得することはできなかった。

(b) 下諏訪町

下諏訪町の調査は、平成15年9月25日及び26日、調査のための無線LAN環境を構築した上で、役場に隣接する建物から庁内LANに攻撃端末を接続し、既存住基サーバの管理者権限を取得することや庁内LANとCSとの間に設定されているファイアウォールを突破してCSの管理者権限を取得することが試みられた。

この結果、既存住基サーバの管理者権限を取得することができたが、上記ファイアウォールを突破してCSの管理者権限を取得する

ことはできなかった。

(c) 波田町

波田町の調査は、平成15年9月29日から同年10月1日までの間、東京都内からインターネットを経由して、インターネットと庁内LANとの間に設置されたファイアウォールを突破してインターネットから庁内LANへ侵入することが試みられた。

この結果、上記ファイアウォールを突破してインターネットから庁内LANへ侵入することはできなかった。

(d) 阿智村（第2次）

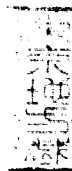
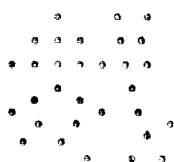
阿智村（第2次）の調査は、平成15年11月24日から同月28日までの間、CSが設置されている区画（両端をファイアウォールで防御された区画。以下「CSセグメント」という。）等に直接攻撃端末を接続し、CS及びCS端末の管理者権限を取得することが試みられた。なお、CSセグメントへの攻撃端末の接続は、職員の協力を得て、通常は施錠されている重要機能室に開錠して入り、通常は施錠されているラックのかぎを開けて接続された。

その結果、CSの管理者権限を取得することができ、CSの管理者権限を取得することで得られたID及びパスワードを用いて、CS端末の管理者権限を取得することができた。もっとも、CS端末の管理者権限をCSの管理者権限の取得を経ないで直接取得することはできなかった。

c 長野県侵入実験の評価

(a) 長野県侵入実験においては、まず、インターネットから庁内LAN経由でCSに侵入する方法は、CSの管理者権限を取得することができずに失敗している。

次に、庁内LANに攻撃端末を直接接続してCSに侵入する方法



についても、CSの管理者権限を取得することができずに失敗している。

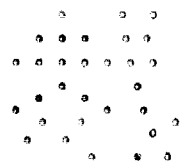
他方、CSセグメントに攻撃端末を直接接続する方法では、CSの管理者権限の取得に成功している。しかしながら、これは、職員の協力を得て、通常は施錠されている重要機能室に開錠して入り、通常は施錠されているラックのかぎを開けて攻撃端末を接続したのであり、通常想定することができない非現実的な状況下でされたものである。

したがって、長野県侵入実験の結果からは、CSの管理者権限を取得することが一般的に可能であることが明らかになったということとはできず、CSの管理者権限を取得することで、本人確認情報を漏えい、改ざんなどさせる具体的危険性があるということとはできない。

- (b) また、庁内LANに攻撃端末を直接接続する方法では、既存住基サーバの管理者権限の取得に成功している。しかしながら、庁内LANに攻撃端末を直接接続することは、職員等がいることなどから、一般的に容易であるとはいえない上、証拠（丙58の1、2、丙59の1、2）及び弁論の全趣旨によれば、既存住基サーバとCSとは同期を取っていないと認められる（これに反する証人吉田の証言は信用することができない。）から、既存住基サーバの情報の改ざんが直ちにCSに保管されている本人確認情報に反映されるとはいえない。

したがって、長野県侵入実験の結果からは、既存住基サーバの管理者権限の取得をもって、本人確認情報の漏えい、改ざんなどの具体的危険性があるということとはできない。

d 小括



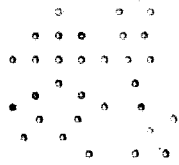
長野県侵入実験を踏まえて、住基ネットにおける本人確認情報の利用提供によって生じる本人確認情報の漏えい、改ざんなどの危険性を検討しても、具体的危険性があると認めることはできない。

(エ) 以上によれば、①住基ネットにおいては、専用回線等による閉鎖的ネットワークシステムを採用し、主要機器間にはファイアウォールを設置していること、通信は相互認証を行い暗号化して行っていること、端末を操作するには操作者識別カードが必要であることなどの各種セキュリティ対策が定められているほか、本人確認情報に関する秘密の漏えいや不正アクセス行為に対する罰則が定められていることなどにより、本人確認情報の漏えい、改ざんなどを防止するための相応の措置がとられていること、②名寄せ、データマッチングの危険性があるとはいえないこと、③現に長野県侵入実験の結果によっても、本人確認情報の漏えい、改ざんなどの具体的危険性があるとは認められないことから、住基ネットにおいて本人確認情報の漏えい、改ざんなどの具体的危険性があるとはまではいえない。

ウ 以上のとおり、本人確認情報はその秘匿の必要性が必ずしも高くない上、住基ネットにおける本人確認情報の利用提供の態様は限定されたものであるということができ、住基ネットにおいて本人確認情報の漏えい、改ざんなどの具体的危険性があるとはまではいえないことからすれば、住基ネットにおける本人確認情報の利用提供の態様は、一般的に許容される限度を超えない相当なものであるということが出来る。

(4) プライバシー権（自己情報コントロール権）に基づく差止請求の可否についての結論

上記(2)及び(3)の検討によれば、住基ネットにおける本人確認情報の利用提供は、その目的の必要性、合理性を認めることができ、かつ、その態様においても、一般的に許容される限度を超えない相当なものであるということが



できるから、住基ネットによる本人確認情報の利用提供は、公共の福祉による相当な制限であり、原告のプライバシー権（自己情報コントロール権）を侵害するものではないというべきである。

したがって、原告のプライバシー権（自己情報コントロール権）に基づく差止請求に理由はない。

2 氏名権に基づく差止請求について

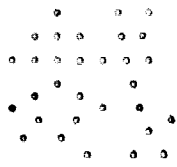
原告は、憲法13条により、国民がその有する氏名を中核として、他と識別され、取り扱われることを内容とする権利利益（氏名権）が保障されており、住基ネットは、国民に住民票コードを付し、番号で国民を扱うことになるから、氏名権を侵害するものであると主張する。

しかしながら、仮に、原告が主張する氏名権が人格権の一内容を構成するものだとしても、住民票コードは、基本4情報を利用提供するに当たって、技術上これを効率的に送信するために住民票の記載事項とされた便宜的数字にすぎず、個人の人格的価値との関係で個人を番号で扱っているということとはできないこと、社会生活においても、個人情報をも的確かつ効率的に整理、管理するため、便宜上数字や記号を組み合わせることは一般に行われており、これが容認されているということができることにかんがみれば、住基ネットにおいて住民票に住民票コードを使用していることが、原告が主張する氏名権を侵害するものということとはできない。

したがって、原告の氏名権に基づく差止請求に理由はない。

3 公権力によって包括的に管理されない自由権に基づく差止請求について

原告は、憲法13条により、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などして有機的に結合し、いつでも利用することができる状態に置かれることを拒絶する自由（公権力によって包括的に管理されない自由権）が保障されているところ、住基ネットは、国民に住民票コードを付しており、これを名寄せの検索キーとして使用するこ



とにより、国家による国民の包括的な管理を可能とするものであるから、公権力によって包括的に管理されない自由権を侵害すると主張する。

しかしながら、仮に、原告が主張する公権力によって包括的に管理されない自由権が憲法上保障される権利利益だとしても、住基ネットは、行政機関が個人情報を含括的に管理することを目的とするものではなく、前記1(3)イ(イ)記載のとおり、住基ネットが利用される事務に関して行政機関が保有する個人情報を一元的に管理する主体は存在せず、かつ、行政機関が自己の有する個人情報と他の行政機関が有する個人情報とを比較、検索及び結合することは認められておらず、現行法制の住基ネットにおいて、原告の個人情報が名寄せ、データマッチングにより包括的に管理される危険性があるとはいえないから、住基ネットが原告が主張する公権力によって包括的に管理されない自由権を侵害するものということとはできない。

したがって、原告の公権力によって包括的に管理されない自由権に基づく差止請求に理由はない。

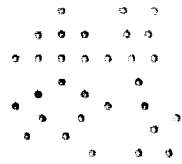
4 損害賠償請求について

(1) 被告国の責任について

ア 原告は、内閣総理大臣らが、改正法を廃止し、又はその施行を延期しないばかりか、所要の措置を講じないまま、平成14年8月5日に改正法を施行したことが違法であると主張する。

イ しかしながら、前記認定説示から明らかなように、そもそも改正法は、原告の権利利益を違法に侵害するものではないから、内閣総理大臣らが所要の措置を講じたか否かにかかわらず、改正法を施行したことが原告との関係において違法となることはないというべきである。

また、所要の措置について、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。」と定めているところ、同条項は、所要



の措置につき、「施行に当たっては」、「速やかに」、「講ずるものとする」と規定しており、その規定振りからして、所要の措置を講じることを改正法の施行要件として定めたものとみることは困難である。したがって、改正法を施行したことが改正法附則に違反するものであるともいえない。

ウ したがって、原告の被告国に対する国家賠償法に基づく損害賠償請求は理由がない。

(2) 被告東京都及び被告センターの責任について

前記認定説示から明らかなように、そもそも改正法は、原告の権利利益を違法に侵害するものではないから、東京都知事が、被告センターに対して本人確認情報を通知するなど、住基法所定の行政事務を実施したこと及び被告センターが東京都知事の委任を受けて原告の本人確認情報処理事務を実施したことが違法となることはないというべきである。

したがって、原告の被告東京都及び被告センターに対する損害賠償請求は理由がない。

第6 結論

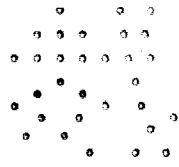
以上によれば、原告の本件請求はいずれも理由がないから、これを棄却することとし、主文のとおり判決する。

東京地方裁判所民事第25部

裁判長裁判官 瀧 澤 泉

裁判官 佐 久 間 健 吉

裁判官吉澤邦和は、転官につき署名押印することができない。



裁判長裁判官

瀧

澤

泉