主　　文

１　原告らの請求をいずれも棄却する。

２　訴訟費用は原告らの負担とする。

事実及び理由

第１　請求

１　被告国は原告らに対し，各１１万円及びこれに対する甲事件原告らにつき平成１５年４月１８日から，乙事件原告らにつき同年７月１５日から，丙事件原告らにつき同年１１月１５日から，丁事件原告らにつき平成１６年４月２４日から，戊事件原告らにつき平成１７年１月５日からそれぞれ支払済みまで年５分の割合による金員を支払え。

２　被告大阪府は甲事件原告１ないし３３，乙事件原告１ないし３９，丙事件原告２ないし２２，丁事件原告２ないし１６，戊事件原告１ないし８の原告らについて，被告京都府は甲事件原告３４，３５，乙事件原告４０，丙事件原告１，２３ないし２７，丁事件原告１，１７，戊事件原告１１の原告らについて，被告奈良県は甲事件原告３６，３７，乙事件原告５０ないし５２の原告らについて，被告兵庫県は甲事件原告３８，３９，乙事件原告４１ないし４９，丙事件原告２８，２９，丁事件原告１８ないし２０，戊事件原告９，１０の原告らについて，被告滋賀県は甲事件原告４４，丙事件原告３０の原告らについて，被告三重県は丁事件原告２１の原告について，

(1)　住民基本台帳法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，原告らに関する各本人確認情報（原告らの氏名，住所，生年月日，性別の４情報及び住民票コード並びにこれらの変更情報をいう。以下同じ。）を提供してはならない。

(2)　被告財団法人地方自治情報センター（以下「被告財団法人」という。）に対し，原告らに関する住民基本台帳法３０条の１０第１項記載の各本人確認情報処理事務を委任してはならない。

(3)　同被告に対し，原告らに関する各本人確認情報を通知してはならない。

(4)　原告らに関する各本人確認情報を，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。

３　被告財団法人は，

(1)　被告大阪府，同京都府，同奈良県，同兵庫県，同三重県，同滋賀県から受任した原告らに関する住民基本台帳法３０条の１０第１項記載の各本人確認情報処理事務を行ってはならない。

(2)　原告らに関する各本人確認情報を，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。

４(1)　被告大阪府及び被告財団法人は，連帯して，甲事件原告１ないし３３，乙事件原告１ないし３９，丙事件原告２ないし２２，丁事件原告２ないし１６，戊事件原告１ないし８の原告らに対し，各１１万円及びこれに対する被告大阪府は甲事件原告１ないし３３の原告らにつき平成１５年４月１７日から，乙事件原告１ないし３９の原告らにつき同年７月１５日から，

丙事件原告２ないし２２の原告らにつき同年１１月１４日から，丁事件原告２ないし１６の原告らにつき平成１６年４月２３日から，戊事件原告１ないし８の原告らにつき平成１７年１月５日から，被告財団法人は甲事件原告１ないし３３の原告らにつき平成１５年４月１８日から，乙事件原告１ないし３９の原告らにつき同年７月１５日から，丙事件原告２ないし２２の原告らにつき同年１１月１５日から，丁事件原告２ないし１６の原告らにつき平成１６年４月２４日から，戊事件原告１ないし８の原告らにつき平成１７年１月５日からそれぞれ支払済みまで年５分の割合による金員を支払え。

(2)　被告京都府及び被告財団法人は，連帯して，甲事件原告３４，３５，乙事件原告４０，丙事件原告１，２３ないし２７，丁事件原告１，１７，戊事件原告１１の原告らに対し，各１１万円及びこれに対する被告京都府は甲事件原告３４，３５の原告らにつき平成１５年４月１８日から，乙事件原告４０につき同年７月１５日，丙事件原告１，２３ないし２７の原告らにつき同年１１月１４日から，丁事件原告１，１７の原告らにつき平成１６年４月２３日から，戊事件原告１１の原告につき平成１７年１月５日から，被告財団法人は甲事件原告３４，３５の原告らにつき平成１５年４月１８日から，乙事件原告４０の原告につき同年７月１５日から，丙事件原告１，２３ないし２７の原告らにつき同年１１月１５日から，丁事件原告１，１７の原告らにつき平成１６年４月２４日から，戊事件原告１１の原告につき平成１７年１月５日からそれぞれ支払済みまで年５分の割合による金員を支払え。

(3)　被告奈良県及び被告財団法人は，連帯して，甲事件原告３６，３７，乙事件原告５０ないし５２の原告らに対し，各１１万円及びこれに対する被告奈良県は甲事件原告３６，３７の原告らにつき平成１５年４月１７日から，乙事件原告５０ないし５２の原告らにつき同年７月１５日から，被告財団法人は甲事件原告３６，３７の原告らにつき平成１５年４月１８日から，乙事件原告５０ないし５２の原告らにつき同年７月１５日からそれぞれ支払済みまで年５分の割合による金員を支払え。

(4)　被告兵庫県及び被告財団法人は，連帯して，甲事件原告３８，３９，乙事件原告４１ないし４９，丙事件原告２８，２９，丁事件原告１８ないし２０，戊事件原告９，１０の原告らに対し，各１１万円及びこれに対する被告兵庫県は甲事件原告３８，３９の原告らにつき平成１５年４月１７日から，乙事件原告４１ないし４９の原告らにつき同年７月１５日から，丙事件原告２８，２９の原告らにつき同年１１月１４日から，丁事件原告１８ないし２０の原告らにつき平成１６年４月２３日から，戊事件原告９，１０の原告らにつき平成１７年１月５日から，被告財団法人は甲事件原告３８，３９の原告らにつき平成１５年４月１８日から，乙事件原告４１ないし４９の原告らにつき同年７月１５日から，丙事件原告２８，２９の原告らにつき同年１１月１５日から，丁事件原告１８ないし２０の原告らにつき平成１６年４月２４日から，戊事件原告９，１０の原告らにつき平成１７年１月５日からそれぞれ支払済みまで年５分の割合による金員を支払え。

(5)　被告滋賀県及び被告財団法人は，連帯して，甲事件原告４４，丙事件原告３０の原告らに対し，各１１万円及びこれに対する被告滋賀県は甲事件原告４４の原告につき平成１５年４月１７日から，丙事件原告３０の原告につき同年１１月１４日から，被告財団法人は甲事件原告４４の原告につき平成１５年４月１８日から，丙事件原告３０の原告につき同年１１月１５

日からそれぞれ支払済みまで年５分の割合による金員を支払え。
(6)　被告三重県及び被告財団法人は，連帯して，丁事件原告２１の原告に対し，１１万円及びこれに対する平成１６年４月２４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
１　本件は，原告らが，住民基本台帳法の一部を改正する法律（平成１１年法律第１３３号。以下「改正法」という。）の制定又はその施行が憲法１３条で保障されている人格権及び自己情報コントロール権を侵害し違法であるとして，被告国に対し国家賠償を，原告らが居住する各被告府県に対し国の機関又は法人に対する本人確認情報の提供の差止め，被告財団法人に対する本人確認情報処理事務の委任及び本人確認情報の通知の差止め，原告らの本人確認情報の抹消並びに国家賠償を，被告財団法人に対し本人確認情報処理事務の差止め，原告らの本人確認情報の抹消及び不法行為に基づく損害賠償を求めている事案である。なお，国家賠償請求その他の損害賠償請求については，各訴状送達の日の翌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も求めている。
２　前提事実（当事者間に争いがない。）
(1)　当事者
ア　原告らはそれぞれ，各事件原告目録記載の各市町に居住している者である。
イ　被告財団法人は，旧自治大臣（現総務大臣）により改正法上の指定情報処理機関として指定され，都道府県知事の委任により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。）に係る事務を行う機関である。
(2)　住民基本台帳法の改正
住民基本台帳法（以下「法」という。）は，平成１１年８月１８日，改正法の公布により，以下のとおり改正された。なお，改正法は，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ていたところ（改正法附則１条１項本文），住民基本台帳法の一部を改正する法律の施行期日を定める政令（平成１３年政令第４３０号。以下「本件政令」という。）により，平成１４年８月５日から施行された。
ア　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のできる住民票コード（法７条１３号）を指定し，市町村長に通知する（法３０条の７第１項）。市町村長は，新たに住民基本台帳に記録されるべき者につき，その者が住民基本台帳に記録されたことがない者であるときは，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（法３０条の２第２項前段）。都道府県知事は，上記住民票コードの指定及びその通知を指定情報処理機関に行わせることができる（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，保存する（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（法３０条の５）。
ウ　都道府県知事は，法の定める場合に，法所定の国の機関・法人等へ本人確認情報を提供する（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（法３０条の１０第１項）。

オ　委任都道府県知事は，指定情報処理機関に本人確認情報を通知する（法３０条の１１第１項）。
カ　本人確認情報等の通知及び提供は，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（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ものとする（改正法附則１条２項）。
(3)　住基ネットの稼働
ア　原告らの居住する市町村の長は，法に基づいて原告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，被告府県知事から委任を受けた被告財団法人は，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，原告らに関する個人情報が記録された既存のサーバを住基ネット専用のコミュニケーションサーバ（以下「ＣＳ」という。）に接続し，ＣＳを被告府県のサーバにつながる電気通信回線に接続した。こうして，市町村長は被告府県知事に，被告府県知事は被告財団法人に本人確認情報を通知している。被告財団法人は，法の定める場合に，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　被告府県は，自己のサーバをＣＳにつながる電気通信回線に接続し，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，被告府県知事が事務を委任した被告財団法人に対して，本人確認情報を通知した。こうして，被告財団法人は，法の定める場合に，法所定の国の機関・法人等に対し，本人確認情報を提供している。
ウ　被告財団法人は，都道府県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，その情報を磁気デイスクに記録し保存する（法３０条の１１第１項，３項）とともに，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　市町村長は，平成１４年８月５日以降，原告らに対し，住民票コードを通知した。市町村及び被告らの住基ネットは同年７月２２日から仮運用され，同年８月５日から本運用された。
３　争点及び当事者の主張
(1)　国家賠償請求その他の損害賠償請求について
ア　国会議員の立法行為の違法性等について
(ア)　総論
（原告らの主張）
改正法は，後述するとおり，憲法上の重大かつ基本的な人権である人格権及び自己情報コントロール権を侵害し，その侵害の程度も著しく大きく，救済の必要性が高いから，国会議員が改正法を立法した行為は国家賠償法（以下「国賠法」という。）上の違法に該当する。また，改正法が違憲であることについて，国会議員に故意又は重大な過失があり，改正法によって，原告らに損害が生じていることは明白である。

仮に，改正法が違憲であるとはいえない場合でも，改正法附則１条２項は，改正法の施行に当たり「所要の措置」を執ることにより，人権侵害を未然に防止するという条件が付されている。したがって，所要の措置として必要な立法を講じない国会の立法不作為は違法であり，そのことにつき，国会議員に故意又は過失があった。

（被告らの主張）

国会議員の立法行為が国賠法上違法とされるためには，立法の内容が憲法の一義的な文言に違反しているにもかかわらず国会があえて当該立法を行うというがごとき，容易に想定し難いような例外的な場合であることが必要である（最高裁判所昭和６０年１１月２１日第一小法廷判決・民集３９巻７号１５１２号）。原告らは上記例外的場合を基礎付ける事実を何ら主張していないから，主張自体失当である。改正法は違憲でなく，まして憲法の一義的な文言に違反しているものとはいえないから，国会議員の立法行為に違法はない。また，改正法附則１条２項は，政府に対して，個人情報の保護に係る所要の措置を講じることを求めているものであって，国会議員に対して個人情報保護法を立法すべき義務を課したものではないから，国会議員の行為に違法はない。

（イ）　住民票コードの付番による人格権侵害

（原告らの主張）

憲法１３条は，個人の人格的生存に不可欠の利益を人格権として保障しているが，公権力から一方的に全人格的な管理の客体に置かれないという自由権も同条により保障されている。住民票コードは，国民全員に対して重複しないように付された個人識別番号であり，多数の行政機関がそれぞれ保有している個人情報を統合し，個人情報を検索するために不可欠なものである。このように，それぞれの行政機関が個人情報を蓄積，管理し，自由自在に利用するための住民票コードを付す行為は，国民が公権力から一方的に管理の客体に置かれないという人格権を侵害するものであり，憲法１３条に違反する。

（被告らの主張）

原告らが主張する「国民が公権力から一方的に全人格的な管理の客体に置かれないという自由権」の意味するところは不明確であり，これが憲法上保障されるとの主張は争う。

仮に上記の権利が憲法上保障されるとしても，住民票コードは，住基ネットを構築するに当たり，行政において確実な本人確認をし，迅速かつ効率的な検索を実現するために住民票に記載することとされたものであり，原告らが主張するような行政機関が個人情報を一元的に管理するために記載したものではない。また，複数の行政分野で収集した個人情報を蓄積，結合，検索するためのパスワードとして住民票コードを利用することは，法が定める目的外利用の禁止，告知要求制限等（３０条の３４，３０条の４２，３０条の４３）に違反することになるため，そのような目的のために住民票コードを住民票に記載しているわけではない。したがって，住民票コードを住民票に記載する行為は人格権を侵害するものではない。

（ウ）　自己情報コントロール権の侵害

（原告らの主張）

憲法１３条は，他人に知られたくない自己情報の収集・取得，保有・利用，開示・提供をコントロールでき，誤った情報を保有されている場合や違法に収集・使用されている場合には，自

己の情報を訂正・抹消できる権利（以下「自己情報コントロール権」という。）を保障している。
従来は，法所定の個人情報を市町村だけが保有し，住民の居住関係の公証等を目的に使用していた。しかし，住基ネットの設立により，本人確認情報が全国の市町村，都道府県，指定情報処理機関を結ぶコンピュータネットワーク上に流通することとなった。しかも，この本人確認情報は，個人の同意を得ることなく，他の市町村，都道府県及び国の機関・法人等に提供され，その事務処理等に使用されることになった。その結果，本人確認情報だけでなく，行政機関等の当該事務に関連する個人情報が，すべて住民票コードを付して管理され，蓄積されることとなり，住民票コードによって検索すれば，それらの行政事務に関連するすべての個人情報が容易に結合されることになる。このような状況は原告らの自己情報コントロール権を侵害する。
（被告らの主張）
プライバシーは，法的保護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憲法上の権利とまではいえない。また，プライバシーの内容は，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であり，自己情報をコントロールする権利は含まれない。
仮に，自己情報コントロール権が憲法上保障されているとしても，法は，個人情報保護に関する国際的基準ともいうべき，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。）を踏まえ，以下のような厳重な保護措置を講じており，住基ネットが直ちに自己情報コントロール権を侵害するものではない。
法は，①　本人確認情報の提供先を公共部門に限定し（法３０条の６ないし３０条の８，別表），民間の者が他人に住民票コードを告知するよう求めることを禁止している（法３０条の４３，４４条）。②　指定情報処理機関や都道府県の保有情報を本人確認情報に限定し（法３０条の１１第１項），③　行政機関に情報を提供する場合でも，提供先機関と利用事務が法律で具体的に列挙されたものでなければ提供できない（法別表）。④　情報提供先の行政機関に安全確保措置義務を課したり（法３０条の３３），法律で定められた利用事務以外の目的による利用を禁止し（法３０条の３４），提供先の関係職員に罰則付きの守秘義務を課している（法３０条の３５，４２条）。⑤　市町村長，都道府県知事，指定情報処理機関等関係機関に対し，情報漏えい防止のために，安全確保措置義務を課し（法３０条の２９，３０条の３３，３６条の２），総務大臣は，電気通信回線を通じた送信または磁気ディスクの送付並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（以下「セキュリティ基準」という。乙５の１から５の５まで）を定め，情報処理機関の職員を含め，関係職員に重い罰則付きの守秘義務を課している（法３０条の１７，３０条の３１，４２条）。⑥　市町村では，ネットワーク接続用のＣＳを導入して，住民基本台帳システムのホストコンピュータに直接つながらないようにしている。⑦　住民からの苦情の適切な処理に努め（法３０条の４１，３６条の３），自己の情報の開示請求・訂正等の申出の手続を設けている（法３０条の３７，３０条の４０）。⑧　市町村，指定情報処理機関及び都道府県は，記録の最新性及び正確性の確保に努

めている（法３０条の５第１項，３０条の１１第８項，３０条の７）。
（エ） 権利侵害の違法性（住基ネットを支える立法事実等）
（原告らの主張）
住基ネットは，全国民に付番する制度であるから，希望者だけではなく，全国民に対して付番しなければ達成できない立法目的がなければならないことは当然であるが，そのような必要性は全く認められない。被告らは，住基ネットによる本人確認情報等の通知及び提供を希望しない住民について，住基ネットを用いた本人確認情報等の通知及び提供を行わないこととした場合（以下「選択制」という。），経費がかかると主張するが，経費節減は人権を制約してよい根拠となり得ない。また，選択制の導入によっても住基ネット利用者の利便性や行政の効率化が阻害されることはない。
さらに，住基ネットには，以下のとおり，やむにやまれぬ必要性はないから，住基ネットは憲法１３条に反し，違法である。
ａ 行政手続の際の住民票の写しの提出を省略・電子化すること
行政手続の際は，住民票の写しだけでなく，手続の申請書等各書類を提出することが必要であるから，住民票の写しの提出だけを省略又は電子化しても，住民の負担はほとんど減らない。
ｂ 年金受給の際の現況届等の省略・電子化
高齢者の年金受給に関する負担を軽減するためには，年金受給者のうち希望者だけを対象にした制度を作れば十分であり，年金の受給は，すでに番号で整理する制度になっているため，新たに住民票コードを付する必要もない。また，年金，恩給等の受給者が概ね高齢者であることを考えると，コンピュータ操作を伴う住基ネットの利用は，従前の手続より高齢者の負担を増大する危険性が大きい。
ｃ 住民票の写しの広域交付
住民が住民票の広域交付を必要とすることはそれほど多くない。また，交付を受けることができる住民票の写しには戸籍の表示などが省略されるので，さらに用途が限定される。
ｄ 転出・転入手続の簡素化
手続の簡素化のためには，住民基本台帳カード（以下「住基カード」という。）の交付を受けていることが前提であるが，住基カードの申請と交付を受けるために通常２回，市町村の窓口に足を運ぶ必要がある。また，転出地で交付を受けていた住基カードは転出時に返却しなければならない。さらに，手続を簡素化するには付記転出届を提出しなければならないが，そのためには市町村の窓口に赴いて届出書の用紙を入手しなければならない。しかも，住民が転居する際に転出地の市町村の窓口で行うのは住民票の異動の手続だけではなく，国民健康保険，国民年金，福祉医療受給，児童手当，介護保険，水道等の手続を行うことが必要であり，転出・転入手続のみを簡素化しても意味がない。さらに，住基ネットの導入以前から転出証明書を郵送する扱いは有効なものとして行われており，転出地の市町村の窓口に足を運ばなくとも転出の手続をすることは可能であった。よって，この手続によるメリットは考えにくい。
ｅ 住基カードの活用
被告らは，住基カードは，① 身分証明書としての活用，② 本人確認のための利用，③ オンライン申請に必要な公的個人認証サービスで使用する送信文書を暗号化する秘密鍵や，都道

府県知事が本人であることを証明する電子証明の保存用カードとしての利用，④　ＩＣの空きメモリを利用して市町村の独自利用に有用であると主張するが，③は改正当時，念頭に置かれていなかった。また，身分証明書（①）や本人確認のための資料（②）が住基カードである必要はない。さらに，全国的には市町村の独自利用がほとんど進んでおらず（④），住基カードの発行枚数は，極めて少ないのが現状である。したがって，住基カードが住民の利便性を増進するものではないことは明らかである。

ｆ　電子政府・電子自治体の構築

立法事実は，法律の制定の際に存在していなければならない。しかし，住基ネットが電子政府・電子自治体を構築する上で不可欠であることは改正法成立時には全く想定されていなかった。また，電子政府・電子自治体を構築することと住基ネットとは本来無関係である。日本よりはるかに電子社会化が進んでいる米国や北欧諸国でも住基ネットは採用されていない。日本では，政府が住基ネットを基礎とした公的個人認証制度を採用し，同制度を電子政府・電子自治体の基盤として位置付けるから住基ネットとの関連性が生じているにすぎない。

（被告らの主張）

仮に，住基ネットが原告らの権利を制約するものであり，かつ，その制約に対する違憲審査基準として原告らの主張する「やむにやまれぬ基準」に依拠すると仮定したとしても，住基ネットは我が国の国家戦略である電子政府・電子自治体の実現のために不可欠な基盤をなすものとしてやむにやまれぬ必要性があるから，違法とはいえない。

ａ　行政手続における住民票の写しの提出及び住民票の写しの交付

住民基本台帳は，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重要なものである。しかし，住民基本台帳は，各市町村ごとに設けられているから，他の市町村，都道府県及び国の機関等は，当該市町村の住民に関する氏名，住所等の情報を必要とする場合には，住民に住民票の写しの提出を求めていた。住基ネットの設立により，現在，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事務は２６４事務であり，それぞれの事務について住民の負担が解消され，行政側としても，事務の効率性や正確性の向上を実現している。

ｂ　年金受給者の現況届の提出の省略

年金受給者は，毎年，現況届又は身上報告書を提出しなければならなかったが，住基ネットにより，加給年金対象者等を除き，上記書面の提出が不要となった。年金支給機関も，年金受給者への現況届用紙等の送付やその受付処理に係る事務を削減できる上，年金支給の都度（毎年４ないし６回）確認できることから過誤払を防止できるようになった。

ｃ　恩給受給者の受給手続の簡素化

恩給受給者は，毎年，市町村長の証明印を受けて受給権調査申立書を提出する必要があったが，住基ネットにより上記書面の提出が不要となった（乙４）。その結果，恩給受給者が受給権調査に伴う負担を免れ，また，市町村は当該事務を削減でき，受給権の確認を恩給支給の都度（年４回）できるようになったことから過誤払を防止できるようになった。

ｄ　電子政府・電子自治体の構築

我が国は，平成１２年に「５年以内に世界最先端のＩＴ国家となる」という目標を掲げ，これ

を実現するために，「電子政府・電子自治体」の構築を最重要課題の１つとした。「電子政府・電子自治体」の核心は，自宅や職場から原則２４時間，パソコンとインターネットを通じて行政サービスを受けることができることにある。平成１４年１２月６日には，行政手続オンライン化関係３法（①　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，②　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の施行に伴う関係法律の整備等に関する法律，③　電子署名に係る地方公共団体の認証業務に関する法律）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行われた。これによって，婚姻届・離婚届（年間約１００万件），パスポートの交付申請（年間約５００万件），戸籍謄抄本の交付請求（年間約３５００万件），所得税の確定申告（年間約７００万件），国民年金・厚生年金の裁定請求（年間約８０万件）等がインターネットでできるようになると同時に，申請・届出に際して住民票の写しの提出も不要になる。これらの基盤となるのが，公的個人認証サービスであり，住基ネットは，そのサービスにとって不可欠の役割を果たすものである。

ｅ　住民票の写しの広域交付

住民票の写しの交付は，膨大な枚数（平成１４年度においては年間約８５００万枚）に上っている。従来，住民票の写しの交付は，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みでしか受けることができなかったが，住基ネットにより，住民はどの市町村でも住民票の写しの交付を受けることができるようになった。

ｆ　転出・転入手続の簡素化

住民の転出・転入は，多大な件数（平成１４年度においては約４５０万件）に上っているが，住民の転出・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しなければならなかった（法２２条２項，住民基本台帳法施行令（以下「施行令」という。）２３条）。しかし，住基カードの交付を受けている者が，施行令に定める一定の事項が記載された付記転出届を郵送等により提出した場合には，当該付記転出届をした日の後にその者が最初に行う転入届であって，その者の住基カードを添えて行われるものについては，転出証明書の添付を要しないこととされた（法２４条の２第１項）。

ｇ　住基カードの有用性

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となるものであり，①　カードに格納された住民票コードにより本人確認を迅速かつ確実に行うことができること，②　市町村が条例で定めるところにより，多目的カードとして活用できるなど，電子政府・電子自治体において，キーデバイスとしての役割を果たすものである。さらに，③　写真付きのものは公的な身分証明書としても活用できる。

（オ）　地方自治の侵害

（原告らの主張）

市町村の各自治体は，住民の個人情報を管理してきた主体であり，地域住民の個人情報が違法に使用されないよう住民の自己情報コントロール権を保護すべき義務を負っている。住基ネットにより，住民の個人情報が市町村外に流出する場合，住民はもとより，その権利を保護すべき市町村自体も，その情報が，いつ，いかなる機関から，何の目的で使用されたのか，という

使用履歴を情報処理機関に対して開示請求できてしかるべきである。しかし，このような開示請求権は保障されていない。したがって，住基ネットの稼働は，地方自治の本旨にもとり，憲法９２条，９４条等に違反するものである。
（被告らの主張）
住基ネットは，法に基づき運用されているものであり，地方自治を侵害するものではない。なお，市町村長は，都道府県知事・指定情報処理機関を経由して国の機関等に対して，報告要求等を行うことができる。
イ　内閣による改正法施行等の違法性等
（原告らの主張）
（ア）　内閣，内閣総理大臣及び各主務大臣は憲法１１条，１３条，９９条に基づき，法が違憲であることが明白な場合は，当該法の執行により違憲状態が惹起されることを回避する義務を負う。
内閣，内閣総理大臣及び総務大臣は，法が違憲であることが明白であるのに，平成１３年１２月２８日，改正法を平成１４年８月５日から施行する本件政令を定めたものであって，その行為は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行われたものとして違法であり，そのことについて内閣，内閣総理大臣及び総務大臣には故意又は重大な過失があった。
（イ）　内閣，内閣総理大臣及び総務大臣は，改正法施行日である平成１４年８月５日までに，改正法附則に定める万全の「所要の措置」を講じる義務があったにもかかわらず，これを行わなかった。また，改正法附則１条２項は，政府に対し，３年以内に「個人情報保護に関する法整備を含めたシステムを速やかに整え」た上で，これを施行することを義務付けている。したがって，政府としては３年以内に「個人情報保護に関する法整備を含めたシステムを速やかに整えること」ができないと判明した段階で，施行の延期を含めた改正法案を提出する義務があった。よって，平成１４年８月５日に漫然と住基ネットを稼働したのは，改正法附則１条２項に反して明らかに違法である。
なお，行政機関の保有する個人情報の保護に関する法律（以下「行政個人情報保護法」という。）は，①　本来の業務処理に必要な範囲を超えた名寄せの制限が規定されていない，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が規定されていない，③　行政機関による個人情報の利用状況等を監視する第三者機関を置いていない，④　利用目的の変更を広範に認め（同法３条３項），また目的外利用も緩やかに認めている（同法８条）という問題点がある。したがって，政府はいまだに「所要の措置」を講じているとはいえず，改正法附則１条２項に違反した違法状態は継続しているというべきである。
内閣，内閣総理大臣及び総務大臣は，改正法附則に違反して事務を処理してはならない旨の職務上の法的義務に違背して，本件政令を制定し，本件政令どおりの施行を各府県に指導，強要したものであり，この行為は違法であり，内閣，内閣総理大臣及び総務大臣に故意又は過失がある。
（ウ）　内閣，内閣総理大臣及び総務大臣は，住基ネットのセキュリティが極めて脆弱であり，個人情報の漏えい（外部接続による危険，システムの施設・管理の外注委託による危険，内部からの漏えいの危険）や目的外利用の危険性が極めて高い実情にあることを知りながら，漫然

と平成１４年８月５日に住基ネットを稼働したのは，原告らのプライバシー権を侵害するものであって違法である。

ａ　住基ネットは，全国の市町村の個人情報を共有するシステムであり，システムの規模が壮大であり，外部を含めてネットワークで結ばれるものであるから，どこか１か所でもセキュリティが不十分なところがあればシステムへの不正侵入や情報漏えいが生ずる危険性が高い。

ｂ　都道府県又は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とはいえ，市町村のＣＳには本人確認情報以外の住民基本台帳データも蓄積され，住基ネットを通じて流通することになる。

ｃ　長野県の個人情報保護審査会が行った住基ネットの侵入実験でも，市町村のＣＳが乗っ取られて踏み台となり，住基ネット網を介して，各市町村のＣＳや指定情報処理機関のサーバ内の本人確認情報が閲覧され，漏えいしたり，改ざんされたりする危険があることが実証された。各種サーバの乗っ取り自体は，平均的なコンピューター・ネットワークエンジニアであれば可能であり，侵入実験でも既存住基システムのサーバやＣＳの管理権限奪取には１時間から１時間半で成功しているほか，出先機関の端末からダイアルアップ接続を通じて庁内ＬＡＮに進入することも３０分程度で可能であった。

ｄ　市町村によるチェックリスト方式の点検は自己点検にすぎず，都道府県等による指導・助言も，市町村の自己申告に基づいて行うにすぎない。点検項目も恣意的に設定されている。また，この点検により，住基ネット稼働後約１０か月が経過した段階で，３２１５ある市町村のうち１割の市町村で，基本的なセキュリティ対策が不十分であることが明らかになった。また，外部監査法人による市町村のシステム運営監査については，監査が行われた市町村が１０８団体のみであり，その監査の方法や結果も明らかでない。さらに，指定情報処理機関による各市町村のＣＳに対する監視も不十分である。

ｅ　コンピューターウイルス，セキュリティホール対策も十分ではない。

ｆ　セキュリティ基準及び「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（以下「チェックリスト」という。）」を遵守していなければ，本人確認情報の漏えい，改ざんの具体的危険があることは当然であるが，以下のとおり，多くの市町村では遵守できていないのが実情である。

例えば，吹田市では，平成１６年１２月以前に重要機能室への入退室管理簿が作成されていなかったこと，住基ネットの構築・保守等の委託業務について吹田市の書面による承諾を得ずに，系列会社に再委託をしていたことが判明した。

柏原市では，重要機能室の入退室管理簿の記載が正確でなく，入退室管理が杜撰であったり，ＯＳに対するログオン失敗履歴，アプリケーションの操作履歴及びファイアウォール（以下「ＦＷ」という。）のアクセスログについての確認が不十分であったり，セキュリティ責任者のコンピューターの知識経験が乏しいなどの問題がある。

木津町では，委託業務に関する契約書に再委託を制限する規定がなく，木津町による再委託の事前承認がなかったり，住基ネットの担当職員が不要なアクセスか否かを確認できるほどの技術的知識を有しておらず，ＦＷの具体的な設定内容の確認も業者任せになっていた。

加茂町では，担当職員がセキュリティ設定について委託業者に丸投げして，何も監督していな

かったり，アクセスログの確認を十分していないという問題がある。
八尾市では，重要機能室への入退室管理簿の記載が出勤簿のような記載になっており，入退室管理が不十分であること，住基ネットのオペレーションシステムに対するログオン失敗履歴記録などの確認を行った記録がなく，アクセス権限や操作権限の管理がされていないこと，住基ネット機器の保守業務について八尾市による事前の承認を得ずに再委託が行われていたこと，住基ネットと情報系の庁内ＬＡＮが物理的につながっていること，ＣＳ端末が既存住基端末と共用端末であることなど，セキュリティが脆弱である。
被告兵庫県では，操作者識別カードを複数の職員が使い回していたこと，業務端末が設置されていない出先機関の担当者が，業務端末のある出先機関の担当者に対し，本人確認情報の検索等を依頼し，その検索結果をファックスで送信していたことが判明した。
（被告らの主張）
内閣による改正法施行等の行為について，国賠法上の違法が認められるためには，憲法の一義的文言に違反する法をあえて施行したなど，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ことが必要であるところ，内閣等にこのような義務違反はない。
平成１１年の改正法案の国会審議において，小渕総理大臣から，住基ネットの実施に当たり，民間部門をも対象とした個人情報保護に関する法整備を含めたシステムを速やかに整えることが前提であるとの答弁がされた。そこで，政府は，平成１３年３月２７日に，個人情報の保護に関する法律案を第１５１回国会に提出した。そもそも，政府は，立法機関でないから，「所要の措置」とは，法律案の検討，作成，国会への提出を意味するものであって，政府としては上記法律案を国会に提出したことにより，「所要の措置」を講じたことになる。また，改正法自体は，附則１条１項により，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こととされており，上記法律案の成否にかかわらず，定められた日に施行することが義務付けられていた。したがって，上記法律案の提出により，所要の措置を講じたことになり，その法案が改正法施行までに成立しなかったとしても，政府に何ら違法はない。
（なお，上記法律案が提出された後，平成１４年１２月６日に，「与党三党修正要綱」が公表され，同月１３日に「個人情報の保護に関する法律案」は，審議未了により廃案（第１５５回国会）となった。その後，政府は，上記与党三党修正要綱に基づき，平成１５年３月７日に，個人情報保護関係５法案（①　個人情報の保護に関する法律案，②　行政個人情報保護法案，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案，④　情報公開・個人情報保護審査会設置法案，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案）を提出した。これらは，国会で可決成立し，同年５月３０日に公布された。）
また，住基ネットには，後記(2)イ（被告らの主張）(イ)のとおり，セキュリティ対策が講じられているのであり，プライバシーが侵害される具体的危険はない。
ウ　被告府県の知事の改正法施行等の違法性等
（原告らの主張）
(ア)　被告府県の知事は，①　市町村の長に対し住民票コードを指定し，通知すること（法３０条の７第１項），②　本人確認情報を磁気ディスクに記録し，保存すること（法３０条の５第１項，３項，３０条の１１第３項），③　国の機関，他の都道府県の執行機関，法人等へ情

報を提供すること（法３０条の７第３項，５項），④　被告財団法人に対し，住民票コードの指定及び通知，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（法３０条の１１第１項），⑤　被告財団法人へ本人確認情報を通知すること(同項)を行い，これらの行為は，被告府県の知事が職務を行うにつきした行為である。
被告府県の知事は，改正法が違憲であることが明白であるにもかかわらず，上記の各行為を行い，住基ネットの施行及び運用を開始したのであって，職務上の法的義務に違反したものであり，そのことについて故意又は重過失があったといえる。
(イ)　被告府県の知事は，万全の所要の措置が講じられていないにもかかわらず，漫然と上記のような施行業務を行い，各知事が有する住基ネット接続を断つ権限を行使していない。このことは，職務上の法的義務違背に該当する。
(ウ)　被告府県の知事は，住基ネットのセキュリティが極めて脆弱であり，個人情報の漏えい（外部接続による危険，システムの施設・管理の外注委託による危険，内部からの漏えいの危険）や目的外利用の危険性が極めて高い実情にあることを知りながら，漫然と住基ネットの施行業務を行い，各知事が有する住基ネット接続を断つ権限を行使しておらず，これは原告らのプライバシー権を侵害するものであって違法である。
プライバシー権侵害の具体的内容は，上記イ（原告らの主張）(ウ)記載のとおりである。
（被告らの主張）
被告府県の各知事の行為につき国賠法上の違法性が認められるためには，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ことが必要である。
改正法が違憲でないこと，改正法の施行が違憲・違法でないことは既述のとおりであり，被告府県の知事の各行為に上記のような違法はない。また，被告府県の各知事は，改正法を施行すべき義務を負うのであって，住基ネット接続を断つ権限を行使すべき義務を負わない。
また，住基ネットには，後記(2)イ（被告らの主張）(イ)のとおり，セキュリティ対策が講じられているのであり，プライバシーが侵害される具体的危険はない。
エ　被告財団法人による運用業務の違法性
（原告らの主張）
(ア)　被告財団法人は，改正法が違憲であるにもかかわらず，被告府県の各知事から提供された本人確認情報を保有し，同情報を行政機関等に提供するなど住基ネットの運用業務を行っている。
(イ)　被告財団法人は，住基ネットのセキュリティが極めて脆弱であり，個人情報の漏えい（外部接続による危険，システムの施設・管理の外注委託による危険，内部からの漏えいの危険）や目的外利用の危険性が極めて高い実情にあることを知りながら，漫然と住基ネットの運用業務を行っていることは，原告らのプライバシー権を侵害するものであって違法である。
プライバシー権侵害の具体的内容は，上記イ（原告らの主張）(ウ)記載のとおりである。
（被告財団法人の主張）
住民基本台帳のうち，住所，氏名，生年月日及び性別に係る部分の写しは，従前から何人も閲覧できる上，原告らの主張する自己情報コントロール権の侵害の危険性も抽象的なものにすぎないから，原告らの自己情報コントロール権を侵害することはない。

オ　原告らの権利侵害及び損害
（原告らの主張）
(ア)　国会議員は，人格権及び自己情報コントロール権を侵害する法改正を行い，内閣，内閣総理大臣及び総務大臣は，国民のプライバシー権の保護のための「所要の措置」を講じないまま，平成１４年８月５日から住基ネットの運用を強行した。原告らの本人確認情報は，既に国の２６４事務で使用されており，この範囲は今後も拡大されるおそれがあり，最終的には民間による利用も行われるおそれがある。本人確認情報の範囲も，無制限に拡大されるおそれがある。本人確認情報は，非常にセキュリティの弱い住基ネット上で流通しているのであり，住基ネット上の本人確認情報は，外部からの侵入や漏えいあるいは目的外利用や不正使用の危険性にさらされている。原告らのこの精神的苦痛を慰謝するには，被告国に対し，原告１人当たり１０万円の慰謝料の支払を負担させるのが相当である。
(イ)　被告府県の各知事は，違憲の改正法に基づいて，原告らの本人確認情報を被告財団法人に提供した。そして，被告財団法人は，これらの本人確認情報を保有し，行政機関等に提供している。これにより，原告らは，現に人格権，自己情報コントロール権を侵害されているほか，今後も，原告らの本人確認情報が外部からの侵入や漏えいあるいは不正使用の危険にさらされる。原告らの精神的苦痛を慰謝するには，被告府県及び被告財団法人に対し，原告１人当たり１０万円の連帯支払を負担させるのが相当である。
(ウ)　原告らは，それぞれ，本件各訴訟を原告らの訴訟代理人らに委任し弁護士費用を支払う旨約した。そこで，被告らには，原告らの支払う弁護士費用相当損害金として，原告らの損害請求額の１割を負担させるべきである。
（被告らの主張）
否認する。原告らの主張するように，住民票コードを住民票に記載したり，法定の事務について本人確認情報を行政機関等に提供したりするだけで，原告らの権利が現実に侵害されたといえないから，損害も発生していない。
(2)　差止請求及び抹消請求（以下「差止請求等」という。）について
ア　差止め及び抹消（以下「差止め等」という。）の可否
（原告らの主張）
憲法１３条は，国民が公権力から一方的に管理の客体に置かれないという人格権を保障している。また，同条は，自己情報コントロール権を保障している。住基ネットの稼働により，人格権又は自己情報コントロール権が侵害される危険性がある場合には，住基ネット事務の差止めや本人確認情報の抹消を求めることができる。
（被告らの主張）
前述したとおり，原告らが主張する「国民が公権力から一方的に全人格的な管理の客体に置かれないという人格権」は憲法上保障されていない。プライバシーは，法的保護に値する人格的利益であるが，その概念自体不明確であり，差止めが認められるほどに排他性を有する絶対権又は支配権とはいえない。また，プライバシーの内容は，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であり，自己情報コントロール権は含まれない。

イ　権利侵害の危険性
（原告らの主張）
原告らは，一方的に住民票コードを付されることにより，公権力の管理の客体とされないという人格権を侵害されている。
また，被告らによる住基ネットの構築・運用は，個人情報の漏えい（外部接続による危険，システムの施設・管理の外注委託による危険，内部からの漏えいの危険）や目的外利用の危険性が極めて高い。具体的危険の内容は，上記(1)イ（原告らの主張）(ウ)記載のとおりである。
（被告らの主張）
(ア)　人格権侵害について
前記(1)ア(イ)（被告らの主張）記載のとおり，住民票コードを住民票に記載することが原告らの人格権を侵害することにはならない。
(イ)　セキュリティ対策
住基ネットには，以下のとおりのセキュリティ対策が講じられているのであり，プライバシー権が侵害される具体的危険はない。
ａ　制度面からの対策
①　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おり（法３０条の５第１項），②　本人確認情報の提供を受ける行政機関の範囲や利用目的を限定し（法３０条の６，３０条の７第３項ないし第６項，３０条の８，別表），本人確認情報の提供を受ける者に対し，目的外の利用又は提供を禁止し（法３０条の３４），都道府県知事及び指定情報処理機関に対し，法律の規定によらない本人確認情報の利用及び提供を禁止している（法３０条の３０）。③　市町村はＣＳの管理責任を負い，都道府県は都道府県サーバ（都道府県の住民の本人確認情報を保存）と都道府県ネットワークの管理責任を負い，指定情報処理機関は全国サーバ（全住民の本人確認情報を保存）と全国ネットワークの管理責任を負う。④　住民票コードの利用を厳しく制限し，⑤　都道府県，市町村及び指定情報処理機関は緊急時対応計画を定め，本人確認情報の漏えい等の危険が具体的に発生した場合には，相互に連絡調整を行い，被害拡大を防止するための措置等を講ずることとされている。
ｂ　外部からの侵入防止対策（物理的なセキュリティ対策）
セキュリティ基準において，建物等への侵入の防止，重要機能室の配置及び構造，入退室管理，磁気ディスク，構成機器及び関連設備，データ・プログラム・ドキュメント等の管理等，外部からの侵入に対する物理的なセキュリティ対策を関係機関に義務付けている。特に，市町村においてチェックリストに基づく自己点検，これに基づく都道府県，指定情報処理機関及び総務省による指導，助言を実施している。
なお，セキュリティ基準及びチェックリストは，これを遵守しなければ，本人確認情報の漏えい，改ざん等の具体的危険が生じないという基準を設定したものではなく，更に高いレベルの安全性を実現することを目的としているため，仮にセキュリティ基準の一部が達成されていなくても，またチェックリストで最高点に満たない項目があったとしても，直ちに，本人確認情報の漏えい，改ざんの具体的危険があるとはいえない。
ｃ　外部からの侵入防止対策（電気通信回線経由による侵入に対する対策）

以下のような対策を実施している。①　専用回線と専用交換装置を採用し，閉鎖的ネットワークを実現している。②　サーバ間で相互認証・暗号通信を実施している。③　住基ネットの通信プロトコルには，インターネットで用いられる汎用的なプロトコルを使用せず，独自プロトコルによる通信を行っている。④　指定情報処理機関において，コンピュータウイルス，セキュリティホールの発生情報を入手し，ウイルス対策ソフトの新パターンファイルの配布や対応方法の通知を全団体に対して行っている。⑤　指定情報処理機関監視ＦＷ等により不正な通信の遮断と監視を行っている。⑥　システム全体で統一ソフトウェアを導入することにより，住基ネット全体で均質かつ高度なセキュリティ確保を実現している。

ｄ　内部の不正防止対策

①　住基ネット事務の関係者に対する重い刑罰や監督の実施，②　本人確認情報の照会条件の限定，③　住基ネットの操作者識別カード認証によるアクセス制御，④　アクセスログの定期的解析と調査，⑤　住民に対する本人確認情報提供状況の開示，⑥　一定時間に一定数以上の住民票の写しの広域交付を停止すること，⑦　担当職員に対する教育・研修の実施等の対策を採っている。

ｅ　外部監査等によるセキュリティの確保

①　チェックリストを活用した市町村のセキュリティ対策の徹底，外部監査法人による市町村のシステム運営監査，②　模擬攻撃によるセキュリティの確認・強化を行っている。

ｆ　住基カードのセキュリティ対策

①　住基カードは，住民の申請により交付する（法３０条の４４第３項）。②　市町村の独自サービスの範囲は，市町村が条例で定める目的に限定され（法３０条の４４第８項），どの市町村の独自サービスを受けるかは住民が選択できる。③　住基カードの半導体集積回路上に割り当てられた領域には，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以外の個人情報を記録しない（カード内に，様々な個人情報が蓄積されることはない。）こととされている。④　基本利用アプリケーションの利用領域を利用することのできる機関及び目的は制限されており，それ以外の利用は禁止されている。⑤　住基カードの券面記載は４情報のみであり，希望する場合には，氏名のみにすることができる（住民基本台帳法施行規則（以下「施行規則」という。）３８条)。⑥　ＩＣカードを用いて，暗証番号の設定，不正利用防止情報の設定等を行うなど技術面のセキュリティ対策を実施している。⑦　発行前の住基カードの適正管理，適切な交付，発行委託の制限，発行した住基カードの適正管理等を行っている。

ｇ　長野県が行った住基ネットの侵入実験について

上記侵入実験は，市町村設置ＦＷを回避して，重要機能室に物理的に侵入し，施錠を開けるなど通常の対策を幾重にも外して，ＣＳに直接攻撃端末をつなぎ，初めてそのＯＳの管理者権限を取得したとしているものであって，このようなおよそ想定し難い極めて特異な方法でＣＳのＯＳの管理者権限が取得されたからといって，ＣＳの管理者権限の取得が容易に行われるということはできない。さらに，住基ネットアプリケーションは各種のセキュリティ対策が講じられており，ＣＳ，ＣＳ端末のＯＳの管理者権限を取得したとしても，住基ネットアプリケーションを起動させることすらできないから，ＣＳ，ＣＳ端末のＯＳの管理者権限を取得したこと

は，住基ネットの危険性を何ら示すものではない。
出先機関の端末からダイヤルアップ接続を通じて庁内ＬＡＮに侵入することができたとの点も，出先機関の庁舎内に物理的に入り込んだ上で，出先機関のＩＳＤＮ回線を接続したものにすぎず，庁舎外の端末から，セキュリティ対策の不備を突いて，ダイヤルアップ接続により庁内ＬＡＮに不正に侵入したものではないから，何ら庁内ＬＡＮの具体的危険性が示されたものではなく，まして，住基ネットの具体的危険性が明らかになったわけではない。
以上のとおり，上記侵入実験の結果は，住基ネットの危険性を何ら実証するものではなく，かえって，同実験の結果によって，住基ネットの安全性が確認された。
ウ　差止め等の必要性
（原告らの主張）
原告らは，住基ネットの稼働により，人格権を侵害され，強い精神的苦痛を被っている。また，原告らの自己情報コントロール権は現に侵害されており，これまでも内部者の情報漏えい行為や住基ネットの運用に関する事故が頻発しているのであり，常に外部からの侵入や情報の漏えい，不正使用の具体的かつ切迫した危険にさらされている。また，原告らは，原告らの本人確認情報の抹消及び提供の差止めを求めるものであるが，原告らの人格権及び自己情報コントロール権を侵害してまで，国民全員を住基ネットに参加させる必要性は認められない。
（被告らの主張）
前記イ（被告らの主張）で述べたとおり，住基ネットの稼働により，人格権や自己情報コントロール権が侵害される具体的危険はない。むしろ，住基ネットの目的には合理性が認められる。また，希望者だけを住基ネットに参加させる選択制を採用した場合，経費の節減効果が著しく減殺される上，行政事務の効率化・利便性の実現が困難になる。よって，住基ネット事務を差し止めたり，本人確認情報を抹消したりする必要性はない。
第３　当裁判所の判断
１　証拠（甲３６の１４，乙４から６まで，１５，１６，２４から２６まで，４３から４７まで（書証番号は枝番を含む。以下同じ。），証人Ａ（以下「Ａ」という。），証人Ｂ（以下「Ｂ」という。），証人Ｃ（以下「Ｃ」という。），証人Ｄ（以下「Ｄ」という。），証人Ｅ（以下「Ｅ」という。））及び弁論の全趣旨によれば，以下の事実が認められる。
(1)　住基ネットが目的とする行政事務の効率化と住民の利便性
住基ネットは，次のような行政事務の効率化と住民の利便性の向上を目指す制度である（乙４，６）。
ア　行政手続における住民票の写しの提出の省略
住基ネットにより，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２６４事務（パスポートの交付申請，建設業の技術検定の受検申請等）について，住民票の写しの提出が不要となる。
イ　年金受給者の現況届の提出の省略
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，不要となる。
ウ　恩給受給者の受給手続の簡素化

恩給受給者は，毎年，市町村長の証明印を受けて受給権調査申立書を提出する必要があったが，住基ネットにより，上記書面の提出が不要となる。

エ　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することができる（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事項を送信通知し，住民票の写しを作成し，交付する（同条２項から５項まで）。

オ　転出・転入手続の簡素化

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（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が，住基カードの交付を受けている者が，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，当該付記転出届をした日の後にその者が最初に行う転入届であって，その者の住基カードを添えて行われるものについては，転出証明書の添付を要しない（法２４条の２第１項）。

カ　公的個人認証サービス

住基ネットから情報提供を行うことにより，公的個人認証サービス（インターネットで行政手続を行う場合，第三者による情報の改ざんを防止し，通信相手の確認を行うサービスを提供する制度）が実施可能となる。公的個人認証サービスの活用により，行政手続（戸籍謄抄本交付請求，住民票の写しの交付請求，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）をインターネットで行うことができるようになる。

キ　住基カードの活用

住基カードの交付を受けると，住基ネット端末において，住基カードに記録された住民票コードにより本人確認が可能になり，住民票の広域交付や転出・転入手続の簡素化に活用できたり，公的個人認証サービスの秘密鍵，電子証明書等の保存用カードとして機能したり，各市町村の独自サービスに利用したり，公的な身分証明書としても利用できる。

(2)　各市町村等における電子計算機の接続状況等について

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録媒体（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，その間には不正な進入を防ぐＦＷが設置されている。

各市町村には，ＣＳが設置され，既存住基システムからＣＳに，記録媒体を介し，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，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が設置される。

都道府県のサーバとＣＳは専用回線で接続され，ＣＳから都道府県のサーバに，都道府県のサ

ーバから被告財団法人のサーバに，本人確認情報が送信され，保存される。ＣＳと都道府県のサーバ，都道府県サーバと被告財団法人のサーバ，被告財団法人のサーバと国の機関のサーバの間には，それぞれ指定情報処理機関が監視するＦＷが設置されている（乙４，６，１５）。

(3)　住基ネットのセキュリティ対策について

ア　保有情報の制限

法は，都道府県，指定情報処理機関が保有する情報を本人確認情報に限定している（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

法は，本人確認情報の提供を受ける行政機関の範囲や利用目的を限定している（法３０条の６，３０条の７第３項から第６項まで，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を禁止し（法３０条の３４。なお，同規定は行政個人情報保護法８条２項に優先して適用される（同条３項）。），都道府県知事及び指定情報処理機関に対し，法律の規定によらない本人確認情報の利用及び提供を禁止している（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，法律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以外に，住民票コードの告知を求めることはできないとされている（法３０条の４２）。

市町村長等以外の者は，自己と同一の世帯に属する者以外の者に対し，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，同データベースに記録されている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としている（法３０条の４３第１項から３項まで）。

ウ　秘密保持義務

法は，住基ネット事務に従事する者（指定情報処理機関の役員・職員，市町村又は都道府県の職員で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，市町村長又は都道府県知事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及び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従事する職員並びにこれらの職にあった者等）に対し，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保持すべき義務を課している（法３０条の１７第１項，２項，３０条の３１，３０条の３５，３５条）。そして，これらの秘密保持義務に違反した場合には，懲役刑又は罰金刑を科すこととしている（４２条，４５条）。

エ　安全確保義務

法は，住民票記載事項の全部又は一部の修正を行った場合に，市町村長から本人確認情報の通知を受けた都道府県知事，指定情報処理機関及びこれらの者から委託を受けた者，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，都道府県知事その他の都道府県の執行機関及び国の機関の長等に対し，本人確認情報の漏えい，滅失及び毀損の防止その他の本人確認情報の適正な管理のために必要な措置を講ずるよう定めている（法３０条の２９，３０条の３３）。

総務省は，セキュリティ基準において，①　重要機能室の入退室管理（重要機能室の所在を明らかにしないこと，電子計算機及び磁気ディスク等を専用の部屋に設置すること，鍵又は入退

室管理カード等により入退室者が正当な権限を有しているか確認することなど），②　住基ネットのアクセス権限や操作権限を限定し，操作者識別カード及びパスワードにより権限のない者が操作していないか，権限のある者でもその利用の正当性をチェックすること，③　ＣＳと既存住基システムを接続する場合には，その間にＦＷを設置し，当該ＦＷのアクセスログを保存し，チェックすること，④　住基ネットの開発，変更，運用，保守等の委託を行う場合は，委託先事業者等の社会的信用と能力を確認すること，委託先事業者等に対し適切な監督を行うこと，再委託の制限と再委託時の事前申請及び承認を行うこと，などを義務付けている。

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，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する。主務大臣は都道府県知事又は市町村長に対し，都道府県知事は市町村長に対し，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（法３１条１項，２項）。また，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，必要な措置を講ずべきことを指示することができる（法３０条の２２）。

市町村では，チェックリストに基づく自己点検を行っているが，これに基づいて，国又は都道府県等が指導，助言を行っている。

カ　報告及び立入検査

総務大臣及び委任都道府県知事は，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，同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，指定情報処理機関の事務所に立ち入り，同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（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

本人確認情報の保護に関する事項を調査審議し，これらの事項に関し建議したり，必要と認める意見を述べることができる本人確認情報の保護に関する審議会を都道府県に，本人確認情報保護委員会を指定情報処理機関に設置している（法３０条の９，３０条の１５）。

ク　自己の本人確認情報の開示等

法は，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の本人確認情報について，開示，訂正等を請求できるとしている（法３０条の３７，３０条の４０）。

ケ　外部からの不正侵入，情報の漏えいの防止（乙４から６まで）

住基ネットにおいて，①　専用回線と専用交換装置を採用し，閉鎖的なネットワークを構築している，②　ネットワーク上の通信データを暗号化している，③　通信時に公開鍵暗号方式により通信相手への接続を相互に認証している，④　通信は独自の住基ネットアプリケーションにより行っており，インターネットで用いられる汎用的なプロトコルを使用していない，⑤　ウイルスチェックプログラムを常時起動させている，⑥　指定情報処理機関が監視するＦＷをＣＳのネットワーク方向，都道府県サーバ及び被告財団法人のサーバの全方向に設置している，⑦　電磁波漏えいを防止する機器を採用している，⑧　ネットワーク内に侵入検出装置

（ＩＳＤ）を設置しているなどの対策を講じている。
コ　住基カードのセキュリティ対策（乙６）
①　住基カードは，住民の申請により交付する（法３０条の４４第３項），②　市町村長その他の市町村の執行機関は，条例に規定する目的のために住基カードを利用する（法３０条の４４第８項），③　住基カードの利用時にはシステム間の相互認証を行う，④　住基カードの利用時にパスワード照合を行い，規定回数以上の照合失敗により，カードを自動的にロック状態にする，⑤　偽造等が容易にできないように耐タンパー装置を利用したカードを交付している，⑥　住基カードの半導体集積回路上に割り当てられた領域には，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以外の個人情報を記録しない，⑦　住基カードの券面記載は４情報のみであり，希望する場合には，氏名のみにすることができる（施行規則３８条)などの対策を講じている。
２(1)　国家賠償請求その他の損害賠償請求について
ア　国会議員の立法行為の違法性等について
(ア)　国会議員の立法行為が国賠法上違法とされるのは，立法の内容が，国民に憲法上保障されている権利を侵害するものであることが明白な場合など，憲法の一義的な文言に違反しているにもかかわらず国会があえて当該立法を行うような例外的な場合をいうと解される（最高裁判所昭和６０年１１月２１日第一小法廷判決・民集３９巻７号１５１２頁，最高裁判所平成１７年９月１４日大法廷判決・裁判所時報１３９６号１頁）。
(イ)　原告らは，住民票コードを付す行為が，国民が公権力から一方的に管理の客体に置かれないという人格権を侵害するものであり，憲法１３条に反すると主張する。
原告らが主張する上記権利は，その内容が不明確なこともあり，直ちに法的保護に値する利益であるとはいえないが，憲法１３条が個人の尊重と生命・身体・幸福追求の権利の尊重を定め，同法１９条以下において思想良心の自由等を保障している趣旨に照らせば，個人がその人格の生存や発展を阻害されるような態様で公権力の管理下に置かれない利益は，その権利の名称はともかくとして，人格的生存に不可欠な利益として法的に保護されるべきである。
しかし，改正法において住民票コードを指定し，住民票への記載を規定したことが，直ちに個人の人格の生存や発展を阻害するものであるとはいえない。原告らは，住民票コードを付す行為は，行政機関等が保有する個人情報を統合して，蓄積，管理，利用することになると主張するが，前提事実及び前記１(3)イの認定事実のとおり，市町村長及び都道府県知事が提供する情報は本人確認情報に限定されており，法別表の事務を行うため本人確認情報を受領した者は，当該事務処理の遂行に必要な範囲で，受領した本人確認情報を利用し，又は提供することとされ（法３０条の３４），本人確認情報の目的外利用が禁止されていることからすれば，住民票コードは，効率的かつ正確に本人確認をするための役割を果たすものにとどまり，それを超えて本人確認情報以外の個人情報を結合し，一元的に管理することは予定されていないというべきである。そして，上記目的外利用の禁止に違反した公務員は，懲戒処分の対象になる（国家公務員法８２条，地方公務員法２９条）ほか，守秘義務違反の罪（国家公務員法１０９条１２号，１００条１項，地方公務員法６０条２号，３４条１項）に問われることを考えれば，改正法立法時において，法３０条の３４に違反した運用がされる具体的危険があったとは

いえず，これがあることを前提とする原告らの上記主張は理由がない。
また，原告らは，改正法附則１条２項を根拠に，国会議員には人権侵害を未然に防止する所要の措置を執るための立法不作為があったと主張する。しかし，同条項は，第２の２(2)キのとおり，国会議員ではなく，政府に対して，個人情報の保護に万全を期するための所要の措置を講ずることを求めたものであるから，原告らの上記主張は失当である。
(ウ)　原告らは，改正法は自己情報コントロール権を侵害するものであり，憲法１３条に反すると主張する。

プライバシー権は，個人の私生活上の自由を保護するものであり，人格権の一種として，憲法１３条によって保障されている。そして，個人に関する情報が行政機関や民間企業において収集，管理，利用され，また，インターネットを通じて情報が瞬時に流通する現代の情報化社会において，個人の私生活上の自由や人格的自律を保障するためには，個人に関する情報について，行政機関等から不当に収集されたり，利用されたり，他に提供されたりしないように保護することにとどまらず，行政機関等が不当に個人情報を保有，利用しているような場合には，その情報が他の行政機関等へ提供されることを差し止めたり，その情報の抹消を求めたりする権利も保障される必要がある。もっとも，プライバシー権が，人格権の一種として憲法１３条の個人の尊重の理念に基礎を置くものである以上，保護の対象として中心となるのは，人格の生存や発展に不可欠な情報であり，それに直接かかわらない，外的事項に関する個人情報については，行政機関等が正当な目的で，正当な方法により収集，利用，他へ提供しても，プライバシー権の侵害とはならないと解される。自己情報コントロール権は，このような内容の権利として，憲法上保障されているというべきである（以下，原告らの主張する権利内容と区別する意味で，この権利を「自己情報管理権」という。）。

本件で問題となっている本人確認情報は，いずれも思想，信条などの人格の生存や発展に不可欠な情報ではなく，外的事項に関する個人情報であるから，行政機関による収集，利用，他への提供が，正当な目的に基づいて，正当な方法によってされる場合には，自己情報管理権の侵害とはならない。

そして，前記のとおり，国会議員の立法行為が国賠法上違法となるのは，立法の内容が憲法の一義的文言に違反するような場合であるところ，前記１で認定した住基ネットの目的及びセキュリティに関する改正法の各規定に照らし，改正法が原告らの自己情報管理権を侵害することが明白といえないことは明らかであるから，国賠法上の違法はない。
(エ)　地方自治の侵害
原告らは，改正法が，住基ネットにより住民の個人情報が市町村外に流出する場合に，住所地市町村において，同情報がいつ，いかなる機関により，いかなる目的で使用されたのかを把握する手段を保障していないことは，地方自治の本旨に反するものであり，同法は違憲であると主張する。しかし，法の規定によれば，①　市町村長は，他の市町村長等から条例に定める事務について求めがあったときに，条例で定めるところにより，本人確認情報を提供すること（法３０条の６），②　都道府県知事等が本人確認情報を提供する場合は，一定の事務処理に関し，住民の居住関係の確認のため求めがあったときなど限定的なものであること（法３０条の７第３項から６項まで，３０条の８第２項），③　本人確認情報の受領者は，法に定められ

た事務処理の遂行に必要な範囲で同情報を利用し，提供すること（法３０条の３４）が定められており，これらの規定は，担当者に対する懲戒処分や刑罰規定により，その実効性が担保されている。このように，本人確認情報が，それを提供した住所地市町村が予期しない形で，利用されることは想定されていない以上，住所地市町村の意思決定は尊重されているというべきであるから，改正法が，住基ネットにより本人確認情報が住所地市町村外に提供されることを定めたことは，同市町村の地方自治の本旨に反するものではなく，ましてや改正法を立法した行為が，前記国賠法上の違法の要件を満たさないことは明らかである。

イ　内閣による改正法施行等の違法性等

（ア）　原告らは，内閣，内閣総理大臣及び総務大臣は，法が違憲であることが明白であるのに，改正法を施行する政令を定めたことは，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行われたものであり，違法であると主張する。

しかし，前記前提事実及び前記１で認定した住基ネットの目的，改正法が規定する住基ネットのセキュリティ対策及び前記アの認定事実に照らせば，改正法施行令が定められた時点で，同法が明白に違憲であったとはいえないから，これを前提とする原告らの上記主張は理由がない。

（イ）　原告らは，内閣，内閣総理大臣及び総務大臣は，改正法施行日である平成１４年８月５日までに，改正法附則に定める万全の「所要の措置」を講じる義務があったにもかかわらず，これを行わなかったことは違法であると主張する。

しかし，改正法附則１条２項は，改正法の施行に当たって，速やかに，個人情報の保護のために所要の措置を講ずるものとされており，法の施行までに所要の措置を講じることを義務付けている規定と解することはできないから，内閣等に同義務があることを前提とする原告らの上記主張は理由がない。

ウ　被告府県の知事の改正法施行業務等の違法性等

原告らは，被告府県の知事は，改正法が違憲であることが明白であること，万全の所要の措置が講じられていないこと，住基ネットのセキュリティが極めて脆弱であり，個人情報の漏えいや目的外利用の危険性が極めて高いことを知りながら，漫然と住基ネットの施行業務を行い，住基ネットの接続を断つ権限を行使しなかったことは違法であると主張する。

しかし，前記前提事実及び前記１で認定した住基ネットの目的，改正法が規定する住基ネットのセキュリティ対策及び前記アの認定事実に照らせば，改正法が違憲であることが明白であるとも，住基ネットのセキュリティ対策が，制度として本人確認情報の漏えいの危険が極めて高く，本人確認情報の目的外利用の危険も極めて高いものであるとも認めることはできず，また，後記(2)イ(ウ)で述べるとおり，実際の運用上も本人確認情報の漏えい等の危険性が極めて高い実情にあるとも認められないから，これらが存在することを前提とする原告らの上記主張は理由がない。

エ　被告財団法人による改正法施行等の違法性

原告らは，被告財団法人が，住基ネットが原告らのプライバシー権を侵害するなど違憲なものであるにもかかわらず，その運用業務を行っていることは違法であると主張する。

しかし，改正法が，その規定のみならず，実際の運用状況に照らしても，原告らのプライバシ

一権を侵害する具体的危険性のあるものといえないことは，後記(2)イ(ウ)で述べるとおりであり，被告財団法人が住基ネットの運用業務行為を違法と評価することはできない。
オ　結論
上記のとおり，被告らの行為を国賠法上の違法又は不法行為における違法と評価することはできないから，原告らの国賠請求又は不法行為に基づく損害賠償は認められない。
(2)　差止請求等について
ア　公権力の管理の客体に置かれない権利に基づく差止請求等
前述したとおり，個人が，その人格の生存や発展を阻害されるような態様で公権力の管理に置かれない利益は，その権利の名称はともかく，法的に保護されるべきものである。
しかし，住民票コードを指定し，住民票にそれを記載する旨を規定したことが，このような利益を直ちに侵害するとはいえないこと，住民票コードを付す行為が，改正法立法時において，行政機関等の保有する情報の統合につながる具体的危険がなかったことは，前記(1)ア(イ)で述べたとおりであり，この状況は，現時点でも変わっていない（改正法施行後に制定された行政個人情報保護法８条２項は，一定の要件の下，個人情報の目的外利用を認めているが，同条３項の規定により，法３０条の３４が優先的に適用されると解される。）。
なお，将来における法令の改正によって，住所地市町村から提供された本人確認情報の利用範囲が広がる可能性は否定できないが，法改正が確実であるというような特別な事情がない限り，現行の法令を前提として上記危険性の有無を判断すべきであり，本件で，特別な事情があったとはいえない。
以上によれば，原告らの上記請求は理由がない。
イ　自己情報コントロール権に基づく差止請求等
(ア)　差止請求等の可否
前述したとおり，本人確認情報は，いずれも個人の外的事項に関する個人情報であるから，行政機関が正当な目的により，正当な方法に基づいて収集，利用，他への提供をする限り，原告らの自己情報管理権を侵害するものとはいえない。
そこで，以下，住基ネットの必要性（目的の正当性）の有無及び住基ネット稼働による本人確認情報の漏えいの具体的危険性（方法の正当性）の有無を検討した上で，住基ネットの稼働が，原告らに重大な損害をもたらす差し迫った具体的危険があり，その損害を避けるために住基ネット事務の差止めや本人確認情報の抹消をする必要があるか否かを検討する。
なお，住基ネットの稼働が，現時点において行政機関等の保有する情報の統合につながる具体的危険を有するものでないことは，上記アで述べたとおりである。
(イ)　住基ネットの必要性
ａ　住基ネットの目的の合理性
前記１(1)で述べたとおり，住基ネットには，①　行政手続の際に住民票の写しの提出を省略すること，②　年金受給者が現況届等を提出することを省略すること，③　恩給受給者が受給権調査申立書を提出することを省略すること，④　住民票の写しの広域交付，⑤　転出・転入手続の簡素化，⑥　住基カードの活用，⑦　公的個人認証サービスの提供による行政事務のオンライン化などの目的がある。これらの目的は，行政事務の効率化や適正化を図り，ひいては

行政サービスの向上を実現して住民の利便性を高めること，行政事務のオンライン化による行政サービスの広域化を図り，電子政府・電子自治体の実現に資することを目指すものとして，その合理性が認められる。

ｂ　住基ネットの必要性

上記目的①については，本人確認情報の提供及び利用が可能な２６４の事務について，住民が住民票の写しを提出する負担を免れるとともに，行政機関はオンラインで本人確認情報の提供を受けることにより，住民票の交付や受付事務を省略できる上，正確な本人確認情報を把握できる利点がある。②③についても，年金又は恩給の受給者が届出書等を提出する負担を解消するとともに，行政側も届出書等の受付事務等を省略できるほか，支給の都度，本人確認情報を確認できるため，過誤払いの防止につながるという利点がある。④の住民票の広域交付や⑤の転出・転入手続の簡素化についても，住民の利便に資する。もっとも，現時点では，これらの利用は少ない（甲３８の３の２９，３８の５，Ｂ２４頁以下，Ｃ２，２６頁，Ｄ２２頁）。⑥の住基カードは，公的個人認証サービスの秘密鍵や電子証明書等の保存用カードとして活用できるなど，電子政府，電子自治体の実現にとり重要な役割を果たす（乙４）。もっとも，同カードの発行枚数は，平成１６年３月末日時点で５４万枚にとどまるなど普及の程度は低い（甲３９の５，４３，Ｄ２１頁，Ｃ２４頁）。⑦の公的個人認証サービスは，インターネットで行政事務を行うときに，本人確認システムとしての役割を果たすものであり，行政事務のオンライン化，広域化を実現することになる。

このように，現時点における住基ネットの活用は，かなり低調ではあるものの，住基ネットの利用により行政事務における住民の負担が少なくとも一定程度軽減されるとともに，行政事務の効率化・適正化が図られること，さらには，将来における電子政府，電子自治体の実現に資することなどを考えれば，住基ネットの必要性は肯定できる。

なお，住基ネットの必要性は，上記のとおり，電子政府，電子自治体など将来に向けた発展的なものも含むことから，現時点における便益と経費を単純に比較して費用対効果の観点からその必要性を判断するのは，相当でない。

ｃ　全国民を住基ネットに参加させる必要性

原告らは，住基ネットに全国民を参加させる必要性がないと主張するので検討する。

住基ネットの導入により，行政機関等に対する各種手続において，従来必要であった住民票の写しの提出が不要となったにもかかわらず，選択制を採用するとすれば，住基ネットにより本人確認をする者と住民票の写しにより本人確認をする者とが併存することになり，行政事務の効率化を損なうことになる。

また，住基ネットの導入により，加給年金対象者等を除く年金受給者等について，現況届等の提出を省略し，年金支給の都度受給権の確認をすることが可能になったにもかかわらず，選択制を採用すれば，住基ネットにより受給権確認をする者と従来の現況届により受給権確認をする者とが併存することになり，年金支給事務の一括処理が困難となり，行政事務の効率化を損なうことになる。

さらに，住基ネットの導入により，住民の転出・転入手続において，転出地及び転入地の市町村間の通信が，郵送による通知から電気通信回線を用いた通知に変わり（Ｂ１頁），行政事務

の効率化が図れたにもかかわらず，選択制を採用すれば，このような事務の削減効果を損なうおそれがある。
したがって，住基ネットが目指す目的のうち，行政事務の効率化を図るという観点からは，住基ネットを通じて，全国民の本人確認情報を利用できることが必要であり，選択制ではなく，全国民を住基ネットに参加させる必要性があるというべきである。もっとも，この必要性は，あくまで上記観点からのものであるから，仮に住基ネットによって，国民の本人確認情報が漏えいするなどの具体的危険がある場合には，選択制を前提として住基ネットの必要性を判断すべきことになる。
（ウ） 権利侵害及び損害発生の具体的危険性
ａ 住基ネットの制度上・技術上のセキュリティ対策
住基ネットにより，住所地市町村の他に都道府県知事や指定情報処理機関等が本人確認情報を保有することになり，法律に規定に基づいて他の都道府県や市町村，国の機関等に対し，本人確認情報が提供されることになる。
しかし，都道府県知事や指定情報処理機関が保有し，提供する情報は本人確認情報に限定されており，前記１(3)のとおり，住基ネットには，本人確認情報の適正な利用を確保し，漏えいなどを防止するため，制度的，技術的なセキュリティ対策が講じられている。
ｂ 長野県が行った住基ネット侵入実験について
長野県が実施した侵入実験では，重要機能室に物理的に侵入し，ＣＳサーバが入っているラックの施錠を開けて，ＣＳサーバに直接攻撃端末をつなぎ，ＯＳの管理者権限を取得したこと，ＣＳから得られたＩＤとパスワードでＣＳ端末のＯＳの管理者権限を取得することに成功したが，これらは重要機能室の入退室管理，ラックの施錠，操作者識別カード及びパスワード管理等，住基ネット自体に備わっているセキュリティ対策を外した上での実験結果であることが認められる。また，インターネットからＦＷ越しに庁内ＬＡＮへ侵入したり，庁内ＬＡＮから市町村設置ＦＷ越しにＣＳに侵入することを試みた実験は失敗しており，その他住基ネット本体へ直接侵入したり，ＣＳ端末の住基ネットアプリケーションを操作したりすることが可能であることは実証されていない（以上について，乙２４から２６まで）。
ｃ 住基ネットの実際の運用状況等
（ａ） 吹田市等後記各市町村のセキュリティ対策
上記各市町村は，それぞれ住基ネット管理運用要領や緊急時対応計画書を定め，これらに基づいて住基ネットのセキュリティ対策を行っている。住基ネット事務を担当する職員は，被告財団法人や各自治体が開催するセキュリティ対策に関する研修に参加している。
ＣＳは，重要機能室内にある施錠されたラックの中に設置している。ＣＳは，操作者識別カードとパスワードにより，権限のある者でなければ操作できないように管理されている。ＣＳ端末も，操作者識別カードとパスワードにより，権限のある者でなければ操作できないように管理されている。
住基ネットを構成する機器については，被告財団法人又は被告府県等の指示に従って，セキュリティ設定を行っている。また，機器の故障等の不測の事態に備えて，ＣＳのシステム情報やデータのバックアップを定期的に行ったり，夜間・休日を含めて緊急時の連絡体制を確保して

いる。
住基ネットの保守等は，業務委託を行い，委託業者に秘密保持義務を課し，委託作業の際は，委託業者の作業員の身分確認を行い，担当職員が立ち会っている（以上について，甲３６の１４，乙４３から４７まで，Ａ，Ｂ，Ｃ，Ｄ，Ｅ，弁論の全趣旨）。
（ｂ） 吹田市の状況
原告らは，吹田市において，平成１６年１２月以前に，重要機能室への入退室管理簿が作成されておらず，セキュリティに大きな問題があると主張する。そして，同時期まで入退室管理簿が作成されなかったことは事実である（Ａ１０頁）。しかし，平成１７年１月以降は，委託業者又は再委託業者の重要機能室への入退室は記録され，現在は入退室管理をカードで行っており（甲３６の１６，Ａ９頁以下），上記問題は解消されている。
また，原告らは，吹田市は，住基ネットの構築・保守等の業務を委託している会社との間で，委託業務の再委託の禁止し，再委託をする場合には事前に吹田市の書面による承諾を得ることが必要とされていたにもかかわらず，受託会社が平成１５年度に，吹田市の書面による承諾を得ずに，系列会社に委託業務の再委託を行っており，マスコミからの投稿で初めてこれに気づいたことは，セキュリティに関するチェック体制に問題があることを示すものであると主張する。そして，上記時期に無断再委託が行われていたことは事実である（甲３６の５，３６の６）。しかし，平成１６年度以降は，吹田市が業務の再委託を書面で承認しており（甲３６の４），現時点では，無断再委託という問題はない。また，上記(ａ)の事実に照らせば，マスコミの報道によりこの問題が発覚したことから，同市のセキュリティのチェック体制に，本人確認情報の漏えい等の具体的危険に結びつくまでの問題があるとは認められない。
（ｃ） 柏原市の状況
原告らは，柏原市における重要機能室への入退室管理簿の記載は正確でなく，入退室管理が杜撰であると主張する。確かに，入退室管理簿の記載を見ると，入退室の都度，入退室管理簿に記載するのではなく，最初に入室した時刻と最後に退室した時刻のみが記載されており，また，入室の際の入退室管理簿に氏名を記載しなかった業者がいたこともうかがわれる（甲３８の３の３３から３８の３の３５まで，Ｂ１９頁）。同市における入退室管理が十分であったとは言い難い。しかし，上記(ａ)の事実，特に，業者が重要機能室に立ち入るときは職員が立ち会っており（Ｂ８頁），住基ネットは入退室管理簿以外にもＣＳやＣＳ端末のアクセスをＩＤやパスワードによって管理していること（乙４４）などからすると，入退室管理に上記のような不十分な点があることから，直ちに本人確認情報の漏えい，改ざん等の具体的危険があるはいえない。
また，原告らは，アクセスログの確認記録がないことから，ログの確認が不十分であると主張するが，ＣＳ端末はＩＤとパスワードにより権限のある者でなければ操作できないよう管理されており，アクセスログも保存されていること（乙４４）からすれば，本人確認情報の漏えい等の具体的危険があるとはいえない。
原告らは，セキュリティ責任者であるＢがコンピューターの知識経験に乏しく，柏原市のセキュリティに対する認識が低レベルであると主張するが，同人は，企画情報政策室と連携，協働することにより，自己の経験不足を補いながら，セキュリティ責任者，アクセス管理責任者と

しての仕事をしており（Ｂ３０頁），必ずしも柏原市のセキュリティに対する認識のレベルの低さを示すものとはいえない。

（ｄ） 木津町の状況

原告らは，木津町が締結した住基ネットの構築・保守等の業務委託に関する契約書には，再委託を制限する規定がなく，木津町による再委託の事前承認がなかったと主張する。そして，平成１６年度以前に，上記契約者に再委託を制限する規定がなかったことは事実である（甲４０の８の１の２）。しかし，木津町は，平成１７年度以降，再委託契約を制限する条項を契約書に設け，再委託の際に委託業者が再委託の承認申請をし，木津町長が承認する体制をとっており（乙５６の１から５６の３まで，Ｃ１２頁），上記問題は解消されている。

また，原告らは，Ｃ自身がアクセスログを確認して，不要なアクセスか否かの区別ができる技術的知識を有しておらず，ＦＷの設定の具体的内容についての確認も業者任せになっており，セキュリティに大きな問題があると主張する。しかし，同人自身が詳しいコンピューターネットワークセキュリティの知識を有していないとしても，同人は，アクセスログを委託業者又は再委託業者とともに確認し，また，ＦＷの設定の内容の確認を業者を通じてしているのであり（Ｃ２０，２１頁），上記(ａ)の事実を併せて考えれば，このような形でのセキュリティの確認方法が，直ちに情報漏えいの具体的危険をもたらすものとはいえない。

（ｅ） 加茂町の状況

原告らは，加茂町の住基ネット担当職員であるＤが委託業者のセキュリティ設定について委託業者に丸投げし，何も監督をしていないと主張する。確かに，同人はコンピューター関連技術についての専門的教育を受けておらず，コンピューターについての知識は限定的である。しかし，同人は委託業者の作業に立ち会い，作業報告書によって作業内容の報告を受け，作業内容に不明な点があれば，それを口頭で確認するという方法で，業者に対する監督を行っており（甲３９の４，Ｄ８，２８頁），これに上記(ａ)の事実を併せて考えれば，加茂町において，本人確認情報の漏えい等の具体的危険があるとはいえない。

また，原告らは，加茂町がアクセスログの確認を十分していないと主張する。しかし，加茂町では，最近になってからではあるが，ＯＳに対するログオン失敗履歴やアプリケーションの操作履歴を記録化し，ログオンの失敗履歴については毎日，アプリケーションの操作履歴については定期的に確認しており（Ｄ２３頁），上記問題点は解消されている。

（ｆ） 八尾市の状況

原告らは，重要機能室への入退室管理簿の記載が出勤簿のような記載であり，入退室管理が不十分であると主張する。しかし，上記入退室管理簿は，重要機能室ではなく，情報政策課フロアへの入退室管理簿であり，重要機能室の入退室はカードによって管理されている（Ｅ１９，２６頁）から，入退室管理が適切にされていないとはいえない。

原告らは，住基ネットのオペレーションシステムに対するログオン失敗履歴記録などについての確認作業を行った記録が存在しないことから，アクセス権限や操作権限の管理がされたとはいい難いと主張する。しかし，上記確認作業を行った記録が存在しないこと（甲３７の１８の４）から，担当職員がこれらの作業を行っていないとまで認定することはできない。

原告らは，住基ネット機器の保守業務について八尾市による事前承認を得ずに再委託が行われ

ていたと主張する。確かに，平成１６年度以前には，そのような実態があったが，平成１６年４月１日以降は，八尾市の事前承認を得て再委託を行っており（甲３７の８から３７の１０まで），上記問題点は解消されている。
原告らは，八尾市において，住基ネットと情報系の庁内ＬＡＮとが物理的に回線がつながっていることが，危険なネットワーク接続であると主張する。しかし，同市において，住基ネットは，基幹系のＬＡＮに接続し，インターネットとは接続していない（乙４７，Ｅ１４頁）以上，危険なネットワーク接続であるとはいえない。
原告らは，八尾市のＣＳ端末が既存住基端末と共用端末であることから，セキュリティが脆弱であると主張する。しかし，端末を共用していても，既存住基端末とＣＳ端末は操作者権限やパスワードが別々に設定されており（Ｅ１５頁），共用端末であるからといってセキュリティが脆弱であるとはいえない。
これらの検討結果に上記(ａ)の事実を併せて考えれば，八尾市においても，本人確認情報が漏えいする具体的危険があるとはいえない。
（ｇ） 兵庫県の状況
原告らは，被告兵庫県において，操作者識別カードを複数の職員が使い回していることの危険性を主張する。しかし，兵庫県においてもＣＳの操作権者を限定し，アクセス管理者を置いていたこと（乙４９），兵庫県本人確認情報保護審議会も現行の「操作者用ＩＣカード＋パスワード」方式による操作者の確認は総合的に安全なシステムであると評価していること（甲４４の３）などに照らせば，操作者一人ひとり専用のカードを作成していないことが直ちにセキュリティ上の具体的危険をもたらすものとはいえない。また，原告らは，被告兵庫県において，業務端末が設置されていない出先機関の担当者が，業務端末のある出先機関の担当者に対し，本人確認情報の検索等を依頼し，その検索結果をファックスで送信していたと主張するが，これを認めるに足りる証拠はなく，また，仮にこのような事実があったとしても，住基ネット自体の危険性を示すものとはいえない。
（ｈ） その他
原告らは，上記自治体以外の自治体においても，セキュリティ基準を遵守していないと主張する。そして，証人尋問を実施した上記自治体の実情に照らせば，上記自治体以外の各自治体の住基ネット運用においても，セキュリティ基準のうち忠実に遵守されていない事項があることは推認できる。しかし，前述した住基ネットの制度上・技術上のセキュリティ対策や上記各自治体の運用状況等を考慮すれば，その他の市町村においても，直ちに本人確認情報の漏えい，改ざん等の具体的危険があると認めることはできない。
ｄ　小括
以上のとおり，住基ネットの制度上・技術上のセキュリティ対策，長野県侵入実験の結果及び各市町の運用状況を考慮しても，住基ネットの稼働により本人確認情報が漏えいし，原告らに重大な損害をもたらす差し迫った具体的危険があると認めることはできない。
(エ) 結論
以上のとおり，住基ネットには，行政事務を効率化し，行政サービスの利便性を高めるという観点からの必要性が認められる上に，行政機関による情報の統合や本人確認情報の漏えい，改

ざんなどの具体的危険は認められない。したがって，住基ネットの稼働は，原告らの自己情報管理権を侵害するものとはいえず，同人らが求める本人確認情報の提供等の差止め又は本人確認情報の抹消請求は認められない。

３　以上のとおり，原告らの請求はいずれも理由がないから棄却することとし，主文のとおり判決する。

大阪地方裁判所第７民事部

裁判長裁判官　　廣　谷　章　雄

裁判官　　山　田　　明

裁判官　　芥　川　朋　子