平成１８年４月１１日判決言渡　同日原本領収　裁判所書記官

平成１５年（ワ）第４３１号　住民基本台帳ネットワークシステム差し止め等請求事件

口頭弁論終結日　平成１８年１月３１日

判　　決

（当事者及び訴訟代理人等は別紙当事者目録記載のとおり）

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　請求の趣旨

１　被告国，被告和歌山県，被告財団法人地方自治情報センターは，各原告に対し，連帯して金２２万円及びこれに対する訴状送達の日の翌日から支払済みまで年５分の割合による金員を支払え。

２　被告和歌山県は，

(1)　住民基本台帳法第３０条の７第３項の別表第一の上欄に記載する国の機関及び法人に対し，原告らに関する本人確認情報（原告らの氏名，住所，生年月日，性別の４情報及び原告らに付された住民票コード並びにこれらの変更情報・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に対し，原告らに関する住民基本台帳法第３０条の１０第１項記載の本人確認情報処理事務を委任してはならない。

(3)　同被告に対し，原告らに関する本人確認情報を通知してはならない。

(4)　原告らに関する本人確認情報を，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　被告財団法人地方自治情報センターは，

(1)　被告和歌山県から受任した原告らに関する住民基本台帳法第３０条の１０第１項記載の本人確認情報処理事務を行ってはならない。

(2)　原告らに関する本人確認情報を，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)　被告和歌山市は，原告[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]，同[redacted]に関する本人確認情報を被告和歌山県に通知してはならない。

(2)　被告海南市は，原告[redacted]，同[redacted]，同[redacted]，同[redacted]に関する本人確認情報を被告和歌山県に通知してはならない。

(3)　被告田辺市は，原告[redacted]，同[redacted]，同[redacted]に関する本人確認情報を被告和歌山県に通知してはならない。

(4)　被告橋本市は，原告[redacted]，同[redacted]，同[redacted]に関する本人確認情報を被告和歌山県に通知してはならない。

(5)　被告岩出町は，原告[redacted]，同[redacted]に関する本人確認情報を被告和歌山県に通知してはならない。

5　訴訟費用は被告らの負担とする。

6　第１項について仮執行宣言

第２　事案の概要

本件は，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。）につき，原告らが，同法は，被告国が全国民に強制的に付した住民票コードを利用して個人情報を管理する「国民総背番号制度」を導入するものであって，憲法が保障する国民の人格権，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あって違憲であり，また，同法が施行されて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

稼働を開始したことにより，住民票コードを利用して個人の情報が包括的に集約，管理されることにより「国家による包括的な管理を受けない自由」，プライバシー権，自己情報コントロール権が現に侵害され，あるいは侵害の危機にさらされ，また，原告らが住民票コードを付されて番号で扱われることにより，氏名権等が侵害されていると主張して，① 国会議員，内閣等が改正法を制定し，施行したことにつき被告国を，改正法施行を受けて住基ネットに接続したことにつき被告和歌山県を，改正法による指定情報処理機関であり，和歌山県知事から本人確認情報処理事務を委託されてこれを行ったことにつき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。）をそれぞれ相手方として，国家賠償法及び不法行為に基づく慰謝料等の支払を求めるとともに，② 被告和歌山県，各居住市町（被告和歌山市，被告田辺市，被告海南市，被告橋本市，被告岩出町〈以下「被告市町」という。〉），被告財団法人に対して，原告らに関する本人確認情報の磁気ディスク等からの削除や，改正法における住基ネットに関する処理等の差止めを求めている事案である。

I 前提事実（末尾に証拠の記載のない事実については当事者間に争いがない。）

1 当事者

原告らは，それぞれ肩書地記載の各市町（被告市町）に居住し，住民登録をしている者である（ただし，原告[redacted]は，和歌山県[redacted]に居住する。甲１の１ないし３０，４６，４８ないし５１，弁論の全趣旨）。

被告財団法人は，自治大臣（当時。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基ネットに係る事務を行う機関である。

2 住民基本台帳法の改正

(1) 住民基本台帳法（昭和４２年法律第８１号，以下「法」ともいう。）は，

平成１１年８月１８日公布された改正法により，以下のとおり改正された。

ア　住民票コードの指定及び記載

住民票コードは，全国を通じて重複しない番号，記号その他の符号であって，無作為に作成された１０桁の数字及び１桁の検査数字からなり（住民基本台帳法施行規則〈以下「施行規則」という。〉１条），改正法により住民票の記載事項とされた番号である（法７条１３号）。

都道府県知事は，互いに重複しないよう協議，調整した上で，その区域内の市町村長（特別区の区長を含む。以下同じ。）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（法３０条の７第１項），市町村長は，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）。なお，現実には，上記住民票コードの指定及びその通知は，指定情報処理機関に指定された被告財団法人が行っている。

なお，住民票コードは，一般人の住民基本台帳の一部の写しの閲覧の際には閲覧の対象から除外されており（法１１条１項），また，自己又は自己と同一の世帯に属する者以外の者に係る住民票の写し等の交付の際には，住民票コードは住民票の写し等の記載から省略される（法１２条２項）など，他人に知られないような法的措置が講じられており，さらに，民間の利用について制限規定が設けられている（法３０条の４３第１項ないし第３項）。

イ　本人確認情報

本人確認情報とは，住民票に記載されている事項のうち，氏名，生年月日，性別，住所（以下「基本４情報」という。）に，住民票コード，住民

票の記載等に関する事項で政令で定めるものをいう（法３０条の５第１項）。政令で定める事項としては，①　住民票の記載又は消除を行った場合は，その記載又は消除を行った旨及び記載又は消除の事由，その事由が発生した年月日，②　氏名，生年月日，性別，住所の全部又は一部について記載の修正を行った場合には，記載の修正を行った旨，記載の修正の事由及びその事由が生じた年月日，③　住民票コードについて記載の修正を行った場合には，記載の修正を行った旨，記載の修正の事由及びその事由が生じた年月日並びに修正前の住民票コードが定められている（住民基本台帳法施行令（以下「施行令」という。）３０条の５。以下「変更情報」という。）。

ウ　本人確認情報の保存及び通知

市町村（特別区を含む。以下同じ。）は，電子計算機を設置し，これに，市町村の既存の住民基本台帳システムと連携した各住民の本人確認情報を保存する。

市町村長は，住民票の記載，消除又は基本４情報及び住民票コードの全部若しくは一部について記載の修正を行った場合には，当該住民票の記載にかかる本人確認情報を，施行規則で定めるところにより，市町村長の使用にかかる電子計算機から，電気通信回線を通じて，都道府県知事の使用にかかる電子計算機に送信して通知する（法３０条の５第１項，２項）。

都道府県知事は，電子計算機を設置して，施行規則で定めるところにより，市町村長から通知された本人確認情報を磁気ディスクに記録し，これを通知の日から原則５年間（施行令３０条の６）保存しなければならない（法３０条の５第３項）。

都道府県知事は，指定情報処理機関に本人確認情報処理事務を行わせることができる（法３０条の１０第１項本文）。その場合，指定情報処理機関に本人確認情報処理事務を行わせることとした都道府県知事は，住民の

本人確認情報を電気通信回線を通じて指定情報処理機関に設置された電子計算機に送信して通知する。指定情報処理機関は，施行規則で定めるところにより，都道府県知事から送信された本人確認情報を磁気ディスクに記録し，これを原則５年間（施行令３０条の１１）保存しなければならない（法３０条の１１第１項ないし３項）。

エ　本人確認情報の利用及び提供

(ｱ)　市町村相互の提供

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

(ｲ)　都道府県知事から国の機関等への提供

都道府県知事は，法所定の国の機関又は法人（以下「国の機関等」という。）から法所定の事務の処理に関し，住民の居住関係の確認のための求めがあったときに限り，政令で定めるところにより，保存期間に係る本人確認情報を提供する（法３０条の７第３項）。

(ｳ)　都道府県知事から市町村長等への提供

都道府県知事は，①　当該都道府県の区域内の市町村の執行機関であって法所定の者から法所定の事務の処理に関し求めがあったとき，又は当該都道府県の区域内の市町村の市町村長から住民基本台帳に関する事務の処理に関し求めがあったとき，②　当該都道府県の区域内の市町村の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときには，当該都道府県の区域内の市町村の市町村長その他の執行機関に対し，保存期間に係る本人確認情報を提供する（法３０条の７第４項）。

(ｴ)　都道府県相互の提供

都道府県知事は，①　他の都道府県の執行機関であって法所定のもの

から法所定の事務の処理に関し求めがあったとき，又は他の都道府県の都道府県知事から法３０条の７第１０項に規定する事務の処理に関し求めがあったとき，②　他の都道府県の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときは，他の都道府県の都道府県知事その他の執行機関に対し，保存期間に係る本人確認情報を提供する（法３０条の７第５項）。

(オ)　他都道府県の市町村への提供

都道府県知事は，①　他の都道府県の都道府県知事を経て当該都道府県の区域内の市町村の執行機関であって法所定のものから法所定の事務に関し求めがあったとき，又は他の都道府県の都道府県知事を経て当該都道府県の区域内の市町村の市町村長から住民基本台帳に関する事務の処理に関し求めがあったとき，②　当該他の都道府県の都道府県知事を経て当該都道府県の区域内の市町村の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときは，他の都道府県の区域内の市町村の市町村長その他の執行機関に対し，保存期間に係る本人確認情報を提供する（法３０条の７第６項）。

(カ)　都道府県知事による利用

都道府県知事は，法所定の事務を遂行するとき，条例で定める事務を遂行するとき，本人確認情報の利用につき当該本人確認情報に係る本人が同意した事務を遂行するとき，又は統計資料の作成を行うときには，保存期間に係る本人確認情報を利用することができる（法３０条の８第１項）。

(キ)　都道府県内での提供

都道府県知事は，都道府県知事以外の当該都道府県の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときは，条例で定めるところにより，保存期間に係る本人確認情報を提供

する（法３０条の８第２項）。

(ク) 本人確認情報提供の方法

なお，上記(イ)ないし(カ)について，本人確認情報の提供の方法としては，① 都道府県知事の使用にかかる電子計算機から，電気通信回線を通じて国の機関等の使用にかかる電子計算機に送信する方法，② 都道府県知事から本人確認情報を記録した磁気ディスクを送付する方法が定められている（施行令３０条の７ないし３０条の９）。

(ケ) 法所定の事務

本人確認情報の提供が行われる法所定事務は，平成１４年８月５日時点では９３事務であったが，同年１２月６日に成立した「行政手続等における情報通信の技術の利用に関する法律」，「行政手続等における情報通信の利用に関する法律の施行に伴う関連法律の整備等に関する法律」，「電子署名に係る地方公共団体の認証業務に係る法律」等によって，現在では２７５事務に拡大されている。

オ 指定情報処理機関

都道府県知事は，総務大臣の指定する者，すなわち指定情報処理機関に，法が定める本人確認情報処理事務を行わせることができる（法３０条の１０第１項）ところ，平成１１年１１月１日，当時の自治大臣は，上記の指定情報処理機関として被告財団法人を指定した。

カ 住民基本台帳カード

住民基本台帳に記録されている者は，その者が記録されている住民基本台帳を備える市町村の市町村長に対し，自己に係る住民基本台帳カード（以下「住基カード」という。）の交付を求めることができる（法３０条の４４第１項）。

住基カードには，その者に係る住民票に記載された氏名及び住民票コードその他政令で定める事項が記録されている（同上）。住基カードは，住

民基本台帳事務に利用される（法１２条の２，２４条の２）ほか，市町村長その他の市町村の執行機関は，住基カードを，条例の定めるところにより，条例に規定する目的のために利用することができる（法３０条の４４第８項）。

住基カードは，半導体集積回路（ＩＣ）が組み込まれたいわゆるＩＣカードである。住基カード内部のＩＣには，住基ネットに係るアプリケーションのために割り当てられた領域（基本領域）と，法３０条の４４第８項による条例に規定する目的を達成するためのアプリケーションのために割り当てられた領域（条例利用領域）とが設けられている。両領域はそれぞれ独立し，各システムがそれぞれ割り当てられた領域以外の領域の情報を読み書きできない仕組みが採られている。

また，条例利用領域には，特に必要性が認められる場合を除き，条例利用アプリケーションに係るシステムへアクセスするための利用者番号等以外の個人情報を記録しないことや，利用者番号として住民票コードを使用しないことなどが定められている（弁論の全趣旨）。

(2) 住基ネットの構成（乙２の１・２，１１，１２，弁論の全趣旨）

ア　各市町村には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。）が設置され，全国の各都道府県にも専用のサーバ（以下「都道府県サーバ」という）が設置されているほか，全国レベルで１つのサーバ（以下「全国サーバ」という。）が設置されており，相互に専用回線で接続されている。そして，各ＣＳと上記回線との間，都道府県サーバと上記回線の間，全国サーバと上記回線の間には，指定情報処理機関が監視するファイアウォール（以下「指定情報処理機関監視ＦＷ」という。また，ファイアウォールのことを以下では「ＦＷ」という。）が設置されている。

イ　各地方自治体が住民基本台帳事務を処理するために設置していた既存の

コンピュータ及び記憶媒体（以下「既存住基システム」という。）は，その他の事務処理に使用するコンピュータなどを含めて構成されているＬＡＮに接続され，ネットワークを形成している（以下「庁内ＬＡＮ」という。）。また，都道府県サーバと都道府県の庁内ＬＡＮとの間，全国サーバと国の機関のサーバとの間にも，指定情報処理機関監視ＦＷが設置されている。

ウ　市町村においては，庁内ＬＡＮとＣＳとが接続されている場合，市町村が両者の間にＦＷを設置している（以下「市町村設置ＦＷ」という。）。また，庁内ＬＡＮがインターネットに接続されている場合もあるが，この場合には，庁内ＬＡＮとインターネットとの間にはＦＷが設置される。

エ　被告財団法人（同法人内に設置された住民基本台帳ネットワーク全国センター）は，指定情報処理機関として，指定情報処理機関監視ＦＷについて２４時間の監視を行い，ＣＳに対しては１５分ごとに死活状態の監視を行っている（乙３８，３９，弁論の全趣旨）。

(3)　施行期日

改正法は，公布の日から起算して３年を超えない範囲で政令で定める日から施行されることとされていた（改正法附則１条１項）ところ，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，改正法が公布された平成１１年８月１８日から３年以内の平成１４年８月５日から施行されることとなった。

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

3　住基ネットの稼働

(1)　各市町の既存のサーバと住基ネットとの接続

原告らの居住する被告市町の長は，法に基づいて，原告らの住民票を作成

し，法７条各号に規定されている氏名，住所，生年月日及び性別等の個人識別情報を，電子計算機に記録し管理している。改正法により，被告市町は，原告らに関する上記各事項が記録された既存のサーバを，ＦＷを経由させて住基ネット専用のＣＳに接続し，電気通信回線を介してＣＳを被告和歌山県のサーバに接続した。被告市町の長は，このＣＳを通じて和歌山県知事に本人確認情報を通知している。

(2) 被告和歌山県のサーバと住基ネットとの接続

被告和歌山県は，ＦＷを経由させて自己のサーバをＣＳにつながる電気通信回線に接続した。

和歌山県知事は，和歌山県内の各市町村長から通知を受け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し，和歌山県知事が事務を委託した被告財団法人に対して本人確認情報を通知している。

(3) 被告財団法人の事務

被告財団法人は，和歌山県知事から，和歌山県知事が電気通信回線を通じて県内の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て保存するとともに，通知を受けた本人確認情報を法別表に規定する国の機関又は法人等に，法別表に規定する事務に利用する限りにおいて提供する業務を行っている。

(4) 住民票コードの指定

被告財団法人は，被告和歌山県ほか各都道府県の知事から事務の委任を受け，各市町村長に対し，当該市町村長が住民票に記載することのできる住民票コードの指定及び通知をした。

被告市町の長は，被告財団法人から指定された住民票コードのうちから１個を選択して，各住民の住民票に記載し，平成１４年８月５日以降，原告らを含む各住民に対して住民票コードを通知した。

(5) 住基ネットの稼働状況

住基ネットは，平成１４年７月２２日から仮運用され，同年８月５日から本運用されている。

自治体の中には，個人情報保護や情報漏洩等への対策が不十分であるなどとして，本運用の開始に際して住基ネットへの不参加を表明して住基ネットへの接続を行なわず（東京都杉並区，東京都国分寺市，福島県矢祭町），あるいは本運用開始から数日遅れて接続を開始した自治体（三重県小俣町，同県二見町），住基ネットへの不参加を申し出た住民については住基ネットでの本人確認情報の通知を行わないこととした自治体（横浜市）のほか，本運用開始後に住基ネットから離脱した自治体（東京都中野区，東京都国立市）もある。

このうち，平成１５年５月２３日に個人情報保護法が成立したことを契機に，住基ネットへの接続を開始した自治体（東京都国分寺市，東京都中野区）もあるが，現在もなお住基ネットへの接続を行わず（東京都杉並区，福島県矢祭町，東京都国立市），あるいは不参加の申し出をしなかった住民についてのみ本人確認情報の通知を行っている自治体（横浜市）もある（甲２５）。

(6) 住基カードの普及率

総務省は初年度分として約３００万枚の住基カードの発行を見込んでいたが，平成１６年３月までの住基カード発行枚数は約２５万枚（普及率０．４３パーセント）にとどまっている（甲４４）。

Ⅱ 争点及び当事者の主張

１ 差止請求の可否について

(1) 「公権力による包括的管理からの自由」に基づく差止めの可否

（原告らの主張）

ア 「公権力による包括的管理からの自由」

(ア) 権利の内容，性質及び憲法上の根拠

公権力による包括的管理とは，各行政機関においてそれぞれ個別に保有してい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，いつでも利用できる状態に置くことをいう。このような支配を拒絶する自由が「公権力による包括的管理からの自由」であり，これは，憲法１３条後段の幸福追求権によって基礎づけられる具体的権利である人格権の１つである。

(イ) 差止めの根拠となること

行政機関が，全ての国民に重複することのない住民票コードを付し，国民個人に関する情報を有機的に結合し，いつでも利用できる状態の下では，国民個人の生の生活実態があらわにされ，世界観など人格的自律にかかわる個人情報も容易に推知されることになるため，国民個人が主体的に良心を働かせ自己決定をすることができなくなり，また，思想信条の自由や表現の自由など憲法上重要な価値を担う自由権も萎縮することになる。

したがって，「公権力による包括的管理からの自由」が侵害されているような状態は到底許されるものではないから，その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る。

(ウ) 差止めの要件

「公権力による包括的管理からの自由」が侵害されている場合には，国民は各種の自由権を全く享受できない状況に陥るのであり，民主主義，自由主義は崩壊し，憲法秩序は全く維持できないことになる。このような事態は到底許されるものではなく，その侵害行為についてはすぐに差し止めるべき緊急の必要がある。一方，このような深刻な権利侵害に優越する行政上の利益など存在しない。

したがって，公権力主体の行為により「公権力による包括的管理からの自由」が侵害されている場合には，直ちに侵害行為の差止めが認めら

れなければならない。

イ　権利侵害事実

住基ネットは，特定の行政事務に限定されない共通番号として，すべての国民に重複することのない住民票コードを付して管理するものであって，専ら，行政において，国民のありとあらゆる情報を一元的，効率的に管理するための名寄せのキーとして利用することを目的としている。

住基ネットの稼働により，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等して有機的に結合し，いつでも利用できる状態となっている。つまり，公権力による国民個人の情報の一元的管理を可能にする状態が生じている。

そして，原告らは，国民総背番号制の下，強制的に住民票コードを付され，上記状態を拒絶することはできないのであるから，人格権の中でも重要な位置を占める，原告らの「公権力による包括的管理からの自由」は明らかに侵害されている。

ウ　小括

このように，原告らの「公権力による包括的管理からの自由」は，住基ネットが稼働し，原告ら個人に関する情報の一元的管理が可能な状態に置かれることによって侵害されているのであるから，原告らは，その侵害行為の差止めとして，請求の趣旨第２ないし４項の差止めを求めることができる。

（被告らの主張）

ア　「公権力による包括的管理からの自由」

(ア)　権利の内容，性質及び憲法上の根拠

「公権力による包括的管理からの自由」の意味するところは明らかでなく，これが憲法上保障されるとの主張は争う。

(イ)　差止めの根拠とならないこと

「公権力による包括的管理からの自由」が憲法上保障されるとしても，差止めの根拠となるものではない。

イ　権利侵害がないこと

原告らが主張するような，複数の行政分野で収集した個人情報を蓄積，結合，検索するための鍵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（法３０条の３４，３０条の４２及び３０条の４３）に違反する行為であるから，現行法上，住民票コードによって情報の一元化を行うことは不可能である。

住民票コードは，住基ネットというコンピューターネットワークを構築するに当たり，行政において，確実な本人確認を可能にし，迅速かつ効率的な検索を実現する上で不可欠であるために設けられたものにすぎず，国民の個人情報を一元的に管理することを目的としたものではない。

住民票コードは，原告ら主張に係る「国民の包括的な管理」を実現することを目的とするものではなく，また，そのような管理をすることは法律上不可能でもある。

(2)　プライバシー権・自己情報コントロール権に基づく差止めの可否

ア　権利の内容，性質及び憲法上の位置付け

（原告らの主張）

(ア)　プライバシー権

個人の尊厳の原理に基づく幸福追求権は，憲法１３条により保障されており，憲法上に列挙されていない新しい人権の根拠となる一般的かつ包括的な権利であって，この幸福追求権によって基礎づけられる個々の権利は，裁判上の救済を受けることができる具体的権利である。

そして，プライバシーの権利は，上記のような新しい人権の典型例とされているところであり，判例上も，「私生活をみだりに公開されない法的保障ないし権利」として私法上の権利として承認され，さらには憲

法に基礎づけられた権利として承認されるに至っている。

(イ) 自己情報コントロール権

今日ではさらに，プライバシー権は，コンピュータ技術の発達に伴う高度に進展した情報化社会において，行政機関による個人情報の一極集中，管理に対抗して，プライバシー権に「自己情報をコントロールする権利」がその重要な一内容として含まれると解されるに至っている。

このように憲法１３条によって保障される自己情報をコントロールする権利は，個人の自己情報の開示の可否や開示相手，開示方法等について個人が自ら決定でき，公権力がその個人の意思決定に反して介入することを禁止することができるという内容を含むものであって，このことは判例上も認められている。

(被告らの主張)

(ア) プライバシーについて

プライバシーは，名誉権などとともに，個人の人格的権利ないし人格的利益の総称としての人格権の一つであるとされている。

しかし，プライバシーは，名誉とは異なり，成文法に直接規定されていない概念であり，その定義も，学説上も判例上も未確定，不明確である。最高裁判所も，プライバシー権が憲法１３条によって保障されている旨明言することを避けているが，これは，憲法上の権利として承認できるほどに権利内容が具体的に明らかになっていないからである。

プライバシーは憲法上の権利ではなく，法的保護を受け得る利益として把握するべきである。

(イ) 情報コントロール権について

一般に，情報コントロール権は，保護対象となる情報の範囲が不明確であり，「コントロール」の意味も包括的すぎてあいまいである。また，情報コントロール権の内容として，国家に対する情報の開示請求権や訂

正請求権などの請求権的内容を導き出す解釈は憲法１３条の文言解釈を逸脱するものである。原告らの主張する自己情報コントロール権は，憲法により保障される権利ではない。

イ　プライバシー権及び情報コントロール権が差止めの根拠になるか

（原告らの主張）

プライバシー権及び自己情報コントロール権が差止請求の根拠となる排他性を有することは明らかである。

そして，プライバシー権及び自己情報コントロール権が排他性を有し，絶対的かつ支配的な権利である人格権に含まれることからすれば，これらの権利のみに基づく差止めも認められる場合があるというべきである。

（被告らの主張）

プライバシーも自己情報コントロール権も，排他性を有する絶対権ないし支配権としての人格権に属するものととらえることはできず，これらを根拠に差止めが容認される状況にはない。

ウ　差止めの要件

（原告らの主張）

(ｱ)　差止めが認められるための要件

プライバシー権・自己情報コントロール権に対して，現実に侵害が発生し，又は侵害が発生する蓋然性がある場合には，プライバシー権・自己情報コントロール権に基づく差止めを求めることができると解すべきである。

(ｲ)　損失の重大性・回復困難性が要件とならないこと

一般に，プライバシー権に基づく差止めの要件として，①　侵害行為が明らかに予想され，②　その侵害行為によって，被害者が重大な損失を受けるおそれがあり，かつ，その回復を事後に図ることが不可能又は著しく困難となると認められることが必要と考えられている。

しかし，②の要件は，プライバシー権と等価値的な権利である，相手方の表現の自由の保護の要請との均衡を図るものである。本件のように，国及び地方公共団体を通じた行政の効率化・合理化を図るという国家の便宜と対置される場合には，原則としてプライバシー権が優先するから，②の要件は不要であり，①の要件のみで差止めが認められる。

（被告らの主張）

争う。

エ　自己情報コントロール権の侵害について

（原告らの主張）

(ア)　承諾の必要性

本人確認情報は氏名，性別，年齢，住所の基本４情報が，住民票コード・変更履歴と一体となって住基ネット上で流通するものであり，それ自体が重要な情報であるだけでなく，各行政機関において大量の個人情報が収集・蓄積されている現状では，個人情報総体の索引や検索を可能とする情報としての意味も持つ。

このように，住基ネットにおける本人確認情報は，氏名，性別，年齢，住所の基本４要素に住民票コードを組み合わせ，高度の検索性を与えたものであるから，住民票コードが名寄せのための鍵（キー）として用いられると，住民個人の多面的な情報が瞬時に統合されることとなり，住民個人が行政機関の前で丸裸にされるがごとき状態になる。したがって，この本人確認情報は，極めて秘匿性の高い慎重な取扱いを要する重要な情報である。

(イ)　承諾を得ない流通が正当化されないこと

a　判断基準の厳格性

本人確認情報は，住民票コードと一体となって，個人情報総体の索引や検索を可能とする情報としての意味を持つ，極めて秘匿性の高い

プライバシーである。したがって，情報主体である個別の住民の同意がある場合はともかく，情報主体の同意を得ない流通や利用は認められない。

本人の同意がない場合や，本人の意思に反することが明らかな場合には，例外的に流通や利用が許容されるべき要件（緊急性，やむにやまれぬ利益，より制限的でない他の選びうる手段の存否）について，厳格な判断が求められるべきである。

b　制約の正当化根拠の有無

(a)　改正法成立時に念頭に置かれていた利用目的について

改正法成立の当時考慮されていたその利用目的は，①　行政手続の際の住民票の写しの提出の省略，②　高齢者が年金を受給するため毎年提出を義務付けられている現況届等の省略，③　住民票の写しの広域交付，④　転出・転入手続の簡素化，⑤　住民基本台帳カードの活用にとどまる。

これらによって住民が現実に得られる利益は実態として微々たるものであるか，国民全員を対象とした住基ネットを導入しなくとも十分実現できるものであり，住基ネットの導入を正当化するにはほど遠いものである。

(b)　電子政府・電子自治体の基礎とするとの目的について

i　立法事実を論ずる際においては，当該立法がなされていた時点で，立法事実が存在しなければならないところ，電子政府・電子自治体の基礎となるという利用目的については，立法当時，制度の目的とされていたものではなく，かかる制度を要求する立法事実も存在しなかった。

ii　仮に電子政府・電子自治体の実現及びその場合の本人確認の必要性を前提としても，公的個人認証制度に必要不可欠の制度では

なく，また，公的個人認証法にとっても，そもそも住基ネットは必要がない。

(c) 小括

このとおり，全国民に付した住民票コードと一体となり，個人情報の名寄せを行うための鍵として使われる本人確認情報を，住基ネットを通して，各居住市町村の範囲を越えて国家機関に提供することについて，情報コントロール権の制約を正当化するに足りる根拠となる「やむにやまれぬ必要性」も，手段の最小限度性及び政府目的との密接な関連性も，全く認められない。

したがって，住基ネットにより各居住市町村の範囲を越えて第三者に本人確認情報を提供することは，住民の情報コントロール権を侵害するものである。

(被告らの主張)

仮に，プライバシー権又は情報コントロール権が憲法により保障されているとしても，住基ネットはこれらの権利を侵害するものではない。

(ア) 承諾が不要であること

a 本人確認情報の位置付け

本人確認情報はプライバシー周辺情報にほかならない。

b 本人確認情報が公開を予定された情報であること

住基ネットの基本４情報は，住民の居住関係の公証，選挙人名簿の登録，その他の住民に関する事務の処理の基礎とするために住民基本台帳に記載されているものであって，改正法制定前から公開情報とされていた。

c 法が予定していた本人確認情報の利用範囲

そもそも，法の目的は，「市町村（特別区を含む。以下同じ。）において，住民の居住関係の公証，選挙人名簿の登録その他の住民に関

する事務の処理を基礎とするとともに住民の住所に関する届出等の簡素化を図り，あわせて住民に関する記録の適正な管理を図るため，住民に関する記録を正確かつ統一的に行う住民基本台帳の制度を定め，もつて住民の利便を増進するとともに，国及び地方公共団体の行政の合理化に資すること」（法１条）というものであり，その立法目的において，行政の合理化のため，都道府県や国の機関が個々の住民の承諾を得ずに住民票記載情報を利用することが予定されている。

d　住基ネット導入後の本人確認情報の利用範囲

改正法においては，関係者に守秘義務を課し，目的外利用を規制し，オンラインでの個人情報保護に関する国際的基準ともいうべきＯＥＣＤ８原則（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，①　収集制限の原則，②　データ内容の原則，③　目的明確化の原則，④　利用制限の原則，⑤　安全保護の原則，⑥　公開の原則，⑦　個人参加の原則　⑧　責任の原則という８つの原則）をふまえて，十分な秘密保護の措置をとっている。

このような措置の下で，住民基本台帳に係る窓口事務の簡素化，住民の利便増進を図るため，住基ネットにより，住民基本台帳のネットワーク化を図り，全国規模で本人確認情報の確認を可能としたことは，住民基本台帳法の目的にかなうものである。

e　小括

したがって，住基ネットの稼働について個々の住民の承諾がないことは，何ら問題とならない。

(イ)　憲法上許される制約であること

原告らの主張する情報コントロール権説を前提にしたとしても，住基ネットの稼働により，住民の情報コントロール権が憲法に反して侵害さ

れることにはならない。

a　目的の正当性

住基ネットは，高度に情報化された現代社会において，①　電子政府・電子自治体の実現，②　住民負担の軽減と行政事務の効率化，正確性の向上，③　行政手続のオンライン化，④　公的個人認証サービス，⑤　住民基本台帳事務の簡素化・広域化等という目的を実現するために必要な情報システムである。

b　手段の正当性

国民の本人確認のシステムを整備し，住所を把握するという目的は，重要な政府目的と考えられ，そのために住民の住所や移動に関する個人情報を統一的包括的に収集・取得し，管理・利用することは必要最小限度の手段といってよい。

住基ネットの稼働以前にも，行政機関は，住民に住民票写しを提出させること，行政機関自らが住民票写しを取得すること等の方法により，必要な情報を取得していたのであり，住基ネットは，これをネットワークを用いて提供を受けるようにしたにすぎないから，プライバシー権，情報コントロール権に対する新たな制約は何ら生じていない。

そして，希望者のみを対象とするいわゆる住民選択制を採用すると，住基ネットのメリットを著しく阻害し，住民票コードの記載並びに住基ネットを用いた本人確認情報の通知及び提供を希望しない住民のみならず，これらを希望する住民及び行政機関の利益をも害し，電子政府・電子自治体の実現の妨げとなることから，全住民の住民票に住民票コードを記載する必要がある。

また，改正法においては，関係者に守秘義務を課し，目的外利用を規制し，オンラインでの個人情報保護に関する国際的基準ともいうべきＯＥＣＤ８原則をふまえて，十分な秘密保護の措置をとっている。

c　小括

このように，十分な秘密保護の措置の下において，正当な目的に基づいて，正当な手段で提供するのであれば，本人確認情報を他の行政機関に提供しても，情報コントロール権の不当な侵害には当たらず，憲法に反しない。

オ　プライバシー権の侵害について

（原告らの主張）

(ア)　セキュリティ対策が不完全であることによるプライバシー侵害

住基ネットのセキュリティ対策は極めて不完全であるため，個人情報保護施策の不十分さとあいまって，被告らが保有している原告らの個人情報は既に不特定第三者に漏洩しているも同然の危機に瀕している。

原告らの個人情報がかような状況に置かれていることで，プライバシー権が現に侵害されており，今後も侵害行為が継続するものと考えられる。

(イ)　住基ネットが充分なセキュリティを有していないこと

a　本件で問題とされるべきセキュリティの範囲

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，外部を含めてネットワークで結ばれるものであるから，住基コードの漏洩等を防止するためには，全市町村のＣＳすべては当然のこと，庁内ＬＡＮ上の既存の住基サーバなど，住基コードが蓄積されるあらゆるデータベースのセキュリティが確保されなければならない。また，住基コードは住基ネットの導入に伴って付番されたものであるから，住基コードが漏洩するという事態は，漏洩箇所にかかわらず，住基ネットのセキュリティの問題にほかならない。

b　市町村レベルのセキュリティの不備

(a)　住基ネットの対象として含まれる市町村レベルでは，大規模な住

基ネットに無数に存在する不正侵入の糸口に対応できるだけの能力はない。

(b) 長野県の侵入実験（長野県が平成１５年９月１日から同年１１月２８日までの間，長野県内において行った「市町村ネットワークの安全性」に関する調査。以下「長野実験」という。）では，市町村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たり，漏洩したり，改ざんされる危険性があることが実証された。

(c) 被告らの主張するチェックリスト方式による点検は，市町村の自己点検結果を自主申告させたものであって，外部監査と評価できるものではない上，要求水準を恣意的に引き下げたものである。

また，市町村に対する外部監査法人による監査も十分に実施されていない。

(d) 被告らは，被告財団法人により各市町村のＣＳの監視が行われているというが，これはＣＳが稼働しているか否かを監視するものにとどまり，ＣＳの管理者権限の奪取については検知できていない。

(e) 被告財団法人ウイルス対策ソフトの最新のパターンファイルの配付や，自動更新によるセキュリティホール対策を実施しているというが，市町村における実際の対策実施は迅速に行われていない。

(f) これまでにも，三重県四日市市や横浜市西区，京都府宇治市で，自治体職員が，自治体で管理している他人の個人情報を不正に入手したり，システム開発などの委託先の民間業者から，住民の個人情報が大量に流出する事件が起こっている。住基ネットにおいても，多くの自治体は民間業者にシステムの開発，設置，運用等をゆだねているのであって，同様の事件が起こる危険がある。

（被告らの主張）

(ア) 住基ネットの運用稼働により違憲・違法なプライバシー権侵害やそのおそれが生じていないこと

住基ネットにおいては，以下に述べるように，充分なセキュリティ対策が講じられており，住基ネットの導入によって原告らの個人確認情報が流出する危険性が高まったわけではない。

プライバシーの利益を憲法上の権利として位置付ける論者でさえ，プライバシー権の侵害の具体的おそれがある場合と，抽象的なおそれにとどまる場合とを区別し，後者の場合には違憲や違法の問題が生じないものと考えている。プライバシー情報について悪用を防ぐための法的及び機械工学技術的な対策がかなりの程度まで備わっており，違法かつ困難な作業を通してでなければ情報を引き出せない場合には，プライバシー権侵害の抽象的なおそれがあるにとどまる。

住基ネットの導入によって原告らのプライバシー権への侵害の具体的なおそれは生じていない。

(イ) 住基ネットにおいて十分なセキュリティ対策が採られていること

a 本件で問題とされるべきセキュリティの範囲

市町村や国の機関等は，そもそも住基ネットとは別に個人情報を保有しており，これらの個人情報については，それぞれの保有者がそのセキュリティを確保すべきものである。

このように，市町村等が保有する情報の管理の問題と，住基ネットのセキュリティの問題とは，明確に区別されるべきである。

b 住基ネットの安全性

(a) 一般に，セキュリティは，制度面，技術面及び運用面にわたり，あらゆる見地から多重的に対策が講じられるものであり，仮にその一部が十分でなかったとしても，直ちに本人確認情報等の漏洩の具体的な危険性が存在することを意味しない。

(b) 住基ネットは，制度面，技術面及び運用面における様々な措置を適切に講ずることにより，セキュリティの確保が図られている。仮にいずれかの市町村において問題が生じたとしても，他の市町村にその影響が波及しないよう対策が講じられているから，ある市町村のＣＳに事故が発生したとしても，そのことから直ちにプライバシー権が侵害される具体的危険性があるということにはならない。

i 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を本人確認情報に限定し，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法律で具体的に規定し，本人確認情報の目的外使用や法律によらない本人確認情報の提供を禁止し，③ 関係機関の責任を明確化し，④ 住民票コードの利用について，民間部門による利用を禁止し，国の機関等相互のデータマッチングを禁止し，⑤ 各関係機関において緊急時対応計画を策定し，不正アクセスの徴候が発見された場合に備えている。

ii 外部からの物理的侵入防止対策

セキュリティ基準において，関係各機関に対して，外部からの侵入に対する物理的なセキュリティ対策を義務づけ，特に，市町村における住基ネット及びこれに接続している既設ネットワークについては，「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」（以下「チェックリスト」という。）に基づく市町村による自己点検と，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，助言による対策の強化徹底を図っている。

iii 電気通信回線経由による侵入に対する対策

住基ネットでは，専用回線の使用により閉鎖的ネットワークを

実現した上，サーバ間の相互認証，通信の暗号化などで通信の安全を図るとともに，ＦＷを設置して汎用プロトコルの通過を遮断している。このＦＷは，指定情報処理機関が常時監視し，不正アクセスの前兆が検出された場合には，関係サーバの一時切り離しを含む対策がとられることとなっている。

また，住基ネット全体で，コンピュータウイルスやセキュリティホールに対する対策を実施している。

さらに，住基ネット全体で統一ソフトウェアを導入することで，全体で上記の対策を徹底し，均質かつ高度なセキュリティ確保を実現している。

iv　内部の不正防止対策

改正法及び関連法令により，住基ネットの内部関係者や外注委託先に対して秘密保持義務を課し，これに対する違反には重い刑罰を科したり，指定情報処理機関による監督を通じて，情報の漏洩や不正な目的での提供を防止している。

(c)　長野実験は，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等において，市町村の庁内ＬＡＮ上にある当該市町村の住民の個人情報という限定された情報について漏洩，改ざん等の可能性があることを示したにすぎず，これによって本人確認情報が漏洩及び改ざんの危機にさらされているとは到底言えない。

平成１５年１０月１０日から同月１２日までの間，被告財団法人において，東京都品川区の協力を得て，アメリカの監査法人（クロウ社）のセキュリティ部門により，住基ネットの主要な機器（住基ネットーＣＳ間のＦＷ，ＣＳ－庁内ＬＡＮ間のＦＷ，ＣＳ端末）に対するペネトレーションテスト（模擬攻撃）を実施した。その結果，

これらの機器への侵入は成功せず，脆弱性も見出せず，住基ネットの安全性が確認されている。

(d) 被告国は，住基ネットの安全性とは無関係ではあるものの，市町村の庁内ＬＡＮへの不正な侵入や既存住基システムの個人情報の改ざんがあれば，各自治体における行政事務の円滑な遂行に支障を来すことにかんがみ，安全性のある電子自治体を構築する観点から，外部監査（外部監査法人による監査，チェックリストに基づく自己点検），ウイルス対策ソフトのパターンファイルの配布及び自動適用，ＯＳのセキュリティホール発生情報及び対応方法の通知など，全国の市町村の庁内ＬＡＮのセキュリティレベルの維持向上を図るための取組みを積極的に行うこととしている。

総務省，各都道府県，指定情報処理機関による徹底した技術的助言，指導を実施した結果，既に，すべての市町村において，チェックリストによる自己点検項目中の重要点検項目の７項目について３点満点が達成され，その他の項目についても，市町村のセキュリティ対策は大幅に向上している。

c 小括

このように，住基ネットはセキュリティが法的・技術的に確保されており，住基ネットによる本人確認情報の流出の具体的なおそれはないから，プライバシーを憲法上の権利とする立場に立つとしても，違憲・違法の問題を生じさせるものではない。

カ 小括

（原告らの主張）

住基ネットを用いて，原告ら住民の承諾なく，各居住市町の範囲を越えて，本人確認情報を第三者に対して提供することは，不当にプライバシー情報を流通させるものであって，情報コントロール権を侵害するものであ

るところ，改正法が施行されて住基ネットが稼働している現状においては，これらの情報コントロール権の侵害に当たる本人確認情報の提供が行われており，住基ネットの稼働が続く限り，本人確認情報の提供が継続して行われる蓋然性が高い。

また，住基ネットのセキュリティは極めて不完全であって，被告らが住基ネットの磁気ディスクに保有している原告らの個人情報は既に不特定第三者に漏洩しているも同然であって，このことによるプライバシー権の侵害は現に生じているが，今後も住基ネットが稼働する限り継続して生じることになる。

よって，住基ネット自体が違憲であるから，本来はその全体が差し止められるべきものであるが，少なくとも，原告らが被告らの主張する住基ネットのメリットを放棄することは許されるべきである。原告らは，被告らに対し，情報コントロール権を侵害する行為である改正法による本人確認情報の提供と，その前提となる本人確認情報の通知，情報処理の委任の差止めとを求めるとともに，プライバシー権の侵害又はその具体的なおそれが生じている状態を除去するための措置として，既に住基ネットの磁気ディスクに記録されている本人確認情報の削除を求めるものである。

（被告らの主張）

原告らの主張するプライバシー権及び自己情報コントロール権は，差止請求の根拠となる権利とはいえず，また住基ネットの導入によってこれらの権利が不当に侵害されたり，不当に侵害されるおそれが生じるものでもないから，原告らの差止等の請求が認められる余地はない。

2　損害賠償請求の可否について

(1)　国会議員の立法行為の違法性の有無

（原告らの主張）

ア　改正法の制定

改正法は，それ自体，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著しく大きく侵害するものであるから，国会議員が改正法を制定した立法行為は，国家賠償法１条１項にいう違法な行為にあたるというべきである。

改正法が違憲であることについて，国会議員には故意又は重大な過失があった。

イ　所要の措置に必要な立法義務違反

改正法附則１条２項には，人権侵害を未然に防止するため，「所要の措置」を講じることが条件とされており，国会には所要の措置に必要な立法を行う義務がある。

所要の措置に必要な立法を行わない国会の立法不作為は，国家賠償法１条１項にいう違法な行為に当たる。

この立法不作為について，国会議員には故意又は重大な過失があった。

（被告らの主張）

ア　立法行為の国家賠償法上の違法性

国会議員の立法行為が，国家賠償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敢えて当該立法を行うがごとき，容易に想定しがたいような例外的場合に限られる。

原告らは，この例外的場合に当たることを基礎づける事実を何ら主張していないから，この点に関する主張自体が失当である。

イ　改正法の制定

改正法は，違憲ではなく，まして憲法の一義的な文言に違反しているものではないから，国会議員が改正法を立法したことに国家賠償法上の違法はない。

ウ　所要の措置に必要な立法の義務

改正法附則１条２項は，「政府」に対して，個人情報保護に係る所要の

措置を講ずることを求めているのであって，国会議員らに対して，個人情報保護法を可決成立させるなどの法的義務を課したものではない。

(2) 内閣による改正法施行等の違法性の有無

ア 法律の施行

（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条により，法が違憲であることが明白な場合には，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。

(イ) 内閣，内閣総理大臣及び総務大臣は，改正法が違憲であることが明白であるにもかかわらず，職務上通常尽くすべき注意義務を怠り漫然と，平成１３年１２月２８日，改正法を平成１４年８月５日から施行する政令を定めたものであって，その行為は違法であり，かつ，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存する。

（被告らの主張）

内閣は，憲法７３条６号に基づき，国会で成立した法律である改正法を施行すべく政令を制定したものであるから，その法律の内容いかんにかかわらず，上記の職務上の義務違反はない。なお，改正法は，憲法に反することが明白なものではない。

イ 附則に反する改正法施行

（原告らの主張）

(ア) 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職務上の義務がある。

(イ) 附則は，内閣，内閣総理大臣及び総務大臣に，改正法の施行日である平成１４年８月５日までに万全の「所要の措置」を講じることを求めていたのに，実際には「所要の措置」は講じられていない。

平成１５年５月２３日，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）が成立したが，これらは，思想，信条，病歴，犯罪歴などのセンシティブ情報の収集制限を規定しておらず，目的外利用や他の行政機関への情報提供ができ，行政機関による個人情報の使い回しを認めるなど，個人情報保護の観点からは極めて不十分なものとなっており，「所要の措置」の実質を有するものとはいえない。

(ウ) 附則１条は，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。政府としては３年以内にそれが実現できないことが判明した段階で，施行の延期を含めた改正法案を提出する義務があった。

(エ) それにもかかわらず，内閣，内閣総理大臣及び総務大臣は，平成１３年１２月２８日，改正法を平成１４年８月５日から施行する政令を定め，この政令どおりの施行を各都道府県に指導強要したものであって，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は故意又は過失がある。

（被告らの主張）

(ア) 附則１条２項は，個人情報保護の法整備を待って改正法を施行することを義務付けたものではない。

附則１条１項の規定により，個人情報保護法案が成立すると否とにかかわらず，定められた日に施行することが義務付けられていたため，内閣は，平成１４年８月５日を改正法の施行日と定めたものである。

(イ) 附則の「所要の措置」とは，民間部門における個人情報保護に関する制度に係る措置をいう。政府としては，民間部門の個人情報保護制度を

定めた「個人情報の保護に関する法律案」を，平成１３年３月２７日に国会に提出したことにより，「所要の措置」を講じた。

また，政府は，平成１４年３月１５日には，同法案の規定を受けて，国の公的部門の個人情報保護制度について定めた「行政機関の保有する個人情報の保護に関する法律」等の４法案を国会に提出している。平成１５年３月７日には，政府は，個人情報保護関連５法案を国会に提出し，これらは，同年５月３０日に公布された。

政府は，立法機関でなく，自ら法律を制定することはできないものであるため，「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り，その法案が改正法施行時までに可決成立しなかったとしても，政府に何ら違法はない。

ウ　セキュリティが脆弱なままの運用継続

（原告らの主張）

内閣，内閣総理大臣及び総務大臣は，住基ネットが極めてセキュリティの脆弱なものであり，個人情報の漏洩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させた。このことは，原告らのプライバシー権を侵害する違法な行為であり，かつ，そのことについて故意又は重過失がある。

（被告らの主張）

内閣，内閣総理大臣及び総務大臣の行為について国家賠償法上の違法性が認められるのは，内閣，内閣総理大臣及び総務大臣が職務上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場合に限られる。

住基ネットにはセキュリティ対策が講じられていて，プライバシーが侵害される具体的危険性もないのであるから，内閣，内閣総理大臣及び総務大臣が住基ネットを稼働させたことが，職務上尽くすべき注意義務を尽くすことなく漫然と職務を行ったものとは認められない。なお，自己情報コ

ントロール権は，実体法上保障された権利ではない。

(3) 和歌山県知事の不法行為の有無

（原告らの主張）

ア　法律の実施

和歌山県知事は，違憲な改正法を施行しない職務上の義務を負うところ，改正法が違憲であることが明白であるにもかかわらず，総務省からの指示のままに改正法を施行し，以下の行為を行い，住基ネットの運用を開始した。

a　県内の市町村の長に対し住民票コードを指定し，通知すること（法第３０条の７第１項）。

b　本人確認情報を磁気ディスクに記録し，保存すること（法第３０条の５第１項，第３項，第３０条の１１第３項）。

c　国の機関，他の都道府県，法人等へ情報を提供すること（法第３０条の７第３項ないし第６項）。

d　被告財団法人に対し，住民票コードの指定及び通知，国の機関及び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（法第３０条の１０第１項）。

e　被告財団法人へ本人確認情報を通知すること（法第３０条の１１第１項）。

これらは，和歌山県知事がその職務を行うについてした行為にして職務上の義務に反する違法な行為であり，かつ，和歌山県知事は，そのことについて故意又は重過失があった。

イ　所要の措置が講じられないままの運用継続

和歌山県知事は，前述(2)イ（原告らの主張）のとおり，万全の所要の措置が講じられないままの改正法の施行は違法であるにもかかわらず，漫然と上記アのように改正法上の事務を継続し，その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，職務上の法的義務に違背するものであり，かつ，そのことについて故意又は重過失がある。

ウ　セキュリティが脆弱なままの運用継続

和歌山県知事は，住基ネットが極めてセキュリティの脆弱なものであり，個人情報の漏洩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，漫然と上記アのように改正法上の事務を継続し，その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，原告らのプライバシー権を侵害する違法な行為であり，かつ，そのことについて故意又は重過失がある。

（被告らの主張）

県知事の行為について国家賠償法上の違法性が認められるのは，県知事が職務上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場合に限られる。

被告和歌山県の知事は，改正法の内容いかんにかかわらず，これに基づいた行為を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ことは明らかである。

なお，改正法が違憲であることが明白などということはない。

(4)　被告財団法人の不法行為の有無

（原告らの主張）

ア　法律に基づく業務

被告財団法人は，改正法が違憲であるにもかかわらず，和歌山県知事から提供された本人確認情報を保有し，これ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。このような，違憲な法律に基づく行為は違法である。

被告財団法人には，これらの行為について，故意又は過失が認められる。

イ　セキュリティが脆弱なままの運用

被告財団法人は，住基ネットが極めてセキュリティの脆弱なものであり，個人情報の漏洩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。このことは，原告らのプライバシー権を侵害する違法な行為であり，かつ，そのことについて故意又は過失がある。

（被告財団法人の主張）

改正法は違憲ではなく，住基ネットにはセキュリティ対策が講じられていてプライバシーが侵害される具体的危険性もないのであるから，被告財団法人が住基ネットの運用を行っていることに違法性は認められない。

(5) 損害の有無及び額

（原告らの主張）

ア 慰謝料

原告らは，上記の違法行為を経て，被告らが共同して運用している住基ネットにより，前述のとおり，住民票コードを鍵として個人情報が一元管理されて人格権を侵害され，本人確認情報が漏洩や改ざん，目的外利用等の具体的危機にさらされてプライバシー権を侵害され，個人の承諾がないまま市町村の範囲を越えて本人確認情報を流通させられて自己情報コントロール権を侵害され，精神的苦痛を被っている。

原告らのこの精神的苦痛を慰謝するには，被告国，被告和歌山県，被告財団法人らは，連帯して，各原告に対し，それぞれ２０万円ずつの慰謝料を支払うのが相当である。

イ 弁護士費用

原告らは，本件訴訟の提起及び遂行を原告ら訴訟代理人弁護士に委任した。上記不法行為との因果関係がある弁護士費用相当損害金として，各請求額の１割に当たる各２万円が賠償されるべきである。

（被告らの主張）

争う。

被告らの行為には，原告らの主張するような違法はなく，原告らの権利ないし利益の侵害も生じていない。

第３　当裁判所の判断

【差止請求の可否について】

１　「公権力による包括的管理からの自由」に基づく差止めの可否について

原告ら主張の「公権力による包括的管理からの自由」の内容，外延は，必ずしも明確とは言い難いが，憲法１３条，１９条等の趣旨に照らせば，個人の人格的な生存や発展，道徳的自律が阻害されるような態様で公権力による管理下に置かれない利益は，普遍的に保護されるべきである。

しかしながら，後記２(2)カ，(4)アないしウ，【損害賠償請求の可否について】１ア(イ)のとおり，行政機関が住民票コードを指定し，各個人の住民票にそれを記載することが上記の利益を侵害するとまではいえないし，また，現時点において，原告ら主張のように，各行政機関が保有する個人情報が有機的に結合されるという具体的危険も存しないうえ，今後，そのような事態が発生することが窺われるような具体的事実も認められないことから，原告らの上記請求は理由がない。

２　プライバシー権及び自己情報コントロール権に基づく差止めの可否について

(1)　原告らは，憲法１３条は，プライバシー権を保障しており，その中には自己情報をコントロールする権利が含まれている旨主張し，自己に関する情報の収集・取得，その保有・利用，その開示・提供の各レベルで，情報主体によるコントロールの権利が保障されている住基ネットの稼働によりかかる権利が侵害されている旨主張する。

プライバシーの権利は，私生活上の領域にみだりに侵入されない権利ないしは他人に知られたくない自己に関する情報を公開されない権利として，憲法１３条によって保障されているものと解される。

また，近年，巨大データバンクやコンピュータなどの情報処理技術の発達に伴い，行政機関のみならず民間企業や民間団体においても多量の個人情報が収集，蓄積，管理，利用，提供され，また，このようなデジタルデータは，半永久的に劣化しないで保存することができ，かつ，簡単に原本と同様に複製が可能であり，さらに，インターネット等を通じて，情報が瞬時かつ大量に流通，伝達することが可能になっている。かかる状況下の現代社会においては，個人の私生活上の平穏，人格的自律を保障するためには，プライバシーの権利の一態様として，個人に関する情報につき，単に，行政機関等から不当に収集，利用されたり，そのような情報が他に提供されたりしないように保護される必要があるにとどまらず，他の行政機関等に提供されることを差し止めたり，不当に蓄積，保存されている個人情報の抹消を求める権利も保障される必要があるというべきである。

もっとも，個人情報といっても多様であり，その保護の必要性も一律ではないことから，思想，信条，宗教等個人の自己同一性や人格の生存にかかわる事柄を推知させるような，いわば道徳的自律の存在にかかわる個人情報については最大限尊重されるべきであるが，個人の道徳的自律の存在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により，正当な方法によって収集，利用，提供しても；上記の権利の侵害とはならないものと解するのが相当である。

(2) 本人確認情報の要保護性について

ア 氏名について

氏名は，個人の固有の名称であって，過去及び現在の当該個人のプライバシーに関する情報を当該個人と連結する手がかりとして利用されたり，当該個人の行動や言辞の履歴などプライバシーに関する情報を収集，集積する手がかりとして利用され得るほか，氏名の変更などによって身分関係の変動が推知される場合もある。

しかしながら，反面で，氏名は，人が他者と何らかの関わりが生じる場面において，その行動主体としての自身を特定するために最も基本的な情報として相手方に開示されるのが通常であって，たしかに，他の情報との連結や，プライバシーに関する情報の集積・収集・推知といった文脈において氏名情報を公開することはプライバシーの侵害に当たる場合があることはいうまでもないが，このような文脈を離れて氏名情報それ自体に秘匿性が認められるものとはいえない。

イ　住所について

住所は，当該個人の生活の本拠であって，一般に当該個人のプライバシーに関わる私的活動が多く行われる場所であるとともに，休息の場として平穏が要求される場所でもあるところ，住所情報が，他のプライバシー情報の収集に利用され，あるいは当該個人の私生活の平穏の侵害に利用されることがあり得るほか，他者の住所情報と照らし合わせて同居・別居の別を知ることによって，家族関係を推知させる情報となり得ることもある。

もっとも，住所は，私的な交遊関係だけでなく，社会的関係に伴う往来や連絡通知の宛先としても利用される情報であって，社会的関係の中で一定範囲で開示されることが前提とされている場面もあり，他の情報（特に氏名）との連結や情報の集積・収集・推知という文脈を離れては秘匿性が求められるものではない。

ウ　生年月日について

生年月日は，変更が不可能な情報であるため，同姓同名の者を識別したり，氏名及び住所の変更があった場合の前後同一性を判断するための手がかりともなり得る。また，性別と並んで，当該個人の年齢といった基本的属性を示すものともなる。

そして，これらの情報は当該個人の社会的活動の範囲を大きく離れて伝播することは少ないため，全く見ず知らずの者に知られた場合には，当該

個人が，これらの情報をてことして更にプライバシー情報を収集されたり，私生活の平穏を害されることを恐れたり，他のプライバシー情報も把握されているのではないかという不安を感じることは少なくない。

しかしながら，生年月日は，氏名及び住所に比較すれば，開示が求められる範囲は限られるものの，個人的な親密さを前提としない業者と一般顧客という程度の社会的関係においても，氏名及び住所に付随して同姓同名の者を識別するための情報として利用されたり，当該個人を名乗る者が真実当該個人であるか否かを確認するための質問事項として利用されることも少なくないことや，生年月日それ自体が個人の思想信条や内面の精神活動，純粋な私的活動の内容を推知させるものではないことに照らせば，秘匿性が要求される程度はさほど高くはないものといえる。

エ　性別について

性別は，直接に接触を有する関係であれば明らかに知り得ることが普通であり，日常生活において特に秘匿されることのない情報である。性同一性障害など，社会生活上の性別と医学上，住民登録上の性別との間に差異が存する場合には，その情報の取り扱いには十分な配慮が必要となるが，そのような例外的な場合を除けば，それ自体については秘匿性が要求される程度は低いものといわざるを得ない。

オ　基本４情報の統合

氏名，住所，生年月日，性別の基本４情報が統合されて存在する場合には，それぞれの情報が単独で存在する場合に比較して，当該個人の特定の精度が格段に高くなり，当該個人に関するその他の情報を集積するための鍵として利用されたり，当該個人をねらい打ちにして私生活の平穏が害されるような事態に至る可能性は高まるものといえる。

以上によれば，基本４情報は，それぞれそれ自体がプライバシー情報として強く保護されるものではなく，①　当該個人の社会的活動，私的活動

に関わる情報や，通常人であれば他人に知られたくないような犯罪歴，病歴，収入，趣味嗜好，性癖といった社会的あるいは人格的な評価に関する情報や，当該個人の思想信条，世界観，価値観等を推知させるような個人の活動，言動などに関する情報と結びつけられる場合，あるいは，② 当該個人のプライバシーを暴いたり，ストーカー行為等私生活の平穏を害したりする意図を有している者にとって容易に利用できる状態に置かれている場合など，プライバシー情報としての意味づけを伴って初めて，その意味づけの程度に応じて法的保護に値するプライバシー権の対象となるものというべきである。

カ　住民票コードについて

(ア)　住民票コードの特性

住民票コードは，重複のない１１桁のコードであって，全ての国民の住民票に対して個別に割り当てられて記載されている結果，当該住民票の対象とされている住民個人の氏名，住所，生年月日，性別を住基ネットのシステムを利用して取得するための鍵となるだけでなく，当該住民個人を一意的に識別することが可能なコード番号として機能し得ることにもなる。

また，住民票コードには表記のぶれや重複がない上，氏名，住所等の変更があっても住民票コードはそれに伴って変更されることがないため，その前後の同一性を確認することが可能であって，単なる個人識別情報を組み合わせたものと比較すれば，氏名や住所の表記のぶれに左右されず，また，同姓同名・同一生年月日・同性の者についても同一性を識別することが可能であるという点で，高い精度で個人のプライバシー情報の集積や統合，分析が可能となるという特徴を有する。

(イ)　プライバシーとの関係

しかしながら，住民票コードそれ自体は無作為に割り当てられた数字

の組み合わせに過ぎないため，住民票コードそのものから，当該個人の氏名，住所，生年月日，性別を推知することができるものではない。

住民票コードは，住基ネットそのものを利用し，または別途入手した情報を用いて，特定の住民票コードに結びつけられている当該個人の氏名や住所等，個人を識別することが可能な情報を得られることを前提として，かかる情報を取得するための手段として利用される場合や，住民票コードを主キーとして当該個人の内心を推知させる事実，プライバシー関連情報を取得，集積し，統合，分析するために利用される場合に初めて，当該個人のプライバシーを害し得る情報となるものであって，その限度でプライバシーに関する情報としての性質を有するに過ぎない。

(ウ) 小括

以上によれば，住民票コードは，他の個人識別情報に比較して，個人を高い精度で特定することが可能であって，プライバシー関連の情報の統合の精度を高めるものであり，その点ではプライバシーの侵害に利用される危険性は高いものとはいえるが，それ自体は特定の意味合いを持たない抽象的な情報に過ぎない。住民票コードは，当該個人に関するその他の情報を集積するための鍵として利用される場合や，これを用いて，氏名や住所といった個人識別情報を取得して当該個人を社会的に識別し，これを踏み台にしてプライバシーが侵害されるような場合にはじめて，その程度に応じて，プライバシー権ないし法的保護に値するプライバシーの利益の侵害となりうるものというべきである。

キ 小括

以上の結果，本人確認情報は，それ自体は個人の道徳的自律の存在に直接かかわらない外的事項に関する個人情報であるというべきであって，行政機関等が正当な目的により，正当な方法によって収集，利用，提供しても，権利侵害とはならないものというべきであるが，本人確認情報がプラ

イバシーを暴いたり私生活の平穏を害する意図などの害意を有する者が容易に利用できる状態に置かれていたり，また，当該個人の他のプライバシーに関する情報と結び付けられた状態で第三者が容易に入手できる状態に置かれている場合や，個別に集積されたプライバシーに関する情報を他者が集積した情報と結合するために利用され，あるいはそのような利用が容易な状態に置かれている場合には，当該個人のプライバシーを害するものというべきである。

そこで，以下において，まず，住基ネットのセキュリティ（本人確認情報の漏洩の危険性），次に，行政機関等によるプライバシー情報統合の現実的可能性，最後に，行政機関等による本人確認情報の収集・取得等が正当な目的により，正当な方法によるものか否かについて順次検討する。

(3) 住基ネットのセキュリティについて

ア プライバシー侵害との関係

上記(2)で検討したところによれば，住基ネットが，何者かが住基ネット上の本人確認情報にアクセスしたり，住基ネットからデータを持ち出して公開する具体的な危険性を残す程度のセキュリティしか備えていないような場合には，当該個人のプライバシーの利益に対する現実の危機が存するものと評価できるということとなる。

イ 住基ネットの技術的セキュリティ

(ア) 長野実験

証拠（甲９，１０，１８，２１，２２，２６，２７，乙３１）及び弁論の全趣旨によれば，長野県の依頼による同県内の阿智村，下諏訪町，波田町での実験（平成１５年９月２２日から同年１０月１日まで及び同年１１月２５日から同月２８日まで）によって発見されたセキュリティ上の脆弱性は，概ね以下のとおりであったことが認められる。

a 庁内ＬＡＮの脆弱性

庁内ＬＡＮに接続された住民基本台帳事務を処理するための既存のサーバ（以下「既存住基サーバ」という。）には，管理者権限のユーザ名及びパスワード設定に問題があったことや，ＯＳ（オペレーティングシステム）の既知の脆弱性を解消するためのパッチが適用されていなかったことにより，管理者権限を奪取することが可能な状況のままであったというような問題点があった。

b　ＣＳセグメント上のサーバ・端末の脆弱性

阿智村では，ＣＳのＯＳにも既知の脆弱性を解消するためのパッチが適用されていなかったため，ＣＳセグメントに接続した調査用コンピュータから管理者権限を奪取することができ，また，ＣＳに既存住基サーバのデータベースのユーザ名及びパスワードがバッチファイルの中に暗号化されずに記述されていたため，これを見ることにより，データベースにアクセスすることが可能であり，かつ，このデータベースのデータも暗号化されていなかったため，住基ネット情報の閲覧が可能であった。

c　ＣＳアプリケーションの脆弱性

阿智村では，既存住基システム上の既存住基サーバとＣＳ端末・ＣＳサーバとの間の通信に使われるＣＳアプリケーションには，プログラム中にバッファオーバーフローの脆弱性がある関数が使われていた。

d　市町村管理ＦＷの設定

阿智村では，庁内ＬＡＮとＣＳセグメントとの間で通信制御を行うＦＷは，管理用のポートが開かれていた。また，特定のポートで双方向の通信を許可する設定がされており，このポートを介して庁内ＬＡＮ側からＣＳセグメント側に行われるデータの送受信は遮断されない状態にあった。

e　外部からの侵入経路

阿智村では，ダイヤルアップ接続で庁内ＬＡＮに接続されている出先機関に設置されているダイヤルアップルータに攻撃用端末を接続することにより，庁内ＬＡＮへの接続が可能であった。

また，ＣＳサーバをはじめとするＣＳセグメントに含まれる機器の大部分は施錠されたラック内に格納されていたが，ＣＳ端末は村役場の窓口に設置されていたため，ここがＣＳセグメントの進入路となる可能性があった。

(イ) 市町村において取られている対策

証拠（乙１３，１４，３７，被告和歌山県，被告市町に対する調査嘱託の結果）及び弁論の全趣旨によれば，以下の事実が認められる。

a　品川区での実験

平成１５年１０月に品川区で実施されたペネトレーションテスト（模擬攻撃）の結果，同区の住基ネットーＣＳ間のＦＷ，ＣＳー庁内ＬＡＮ間のＦＷともに脆弱性が発見されなかったこと，前者は被告財団法人が管理し，常時監視を行っているもので，全国共通の機種が採用されていること，後者は市区町村で管理されているＦＷであるが，多くの市区町村で同一機種が採用されており，被告財団法人の定めるルールどおりに設定されているものであったことが認められる（乙１４）。

b　チェックリストによる自己点検

公開サーバ等について最新のパッチを当てること，及びインターネットに接続する場合にはＦＷを設置して厳重な通信制御を行うことは，平成１５年５月に，セキュリティ確保のために特に重要な項目として示された７項目のうちの一つとされ，いずれも平成１５年８月（乙１３）及び平成１６年１２月（乙３７）の時点では，全市町村で，定められた手続が関係する職員に周知され，適切に運用されているとの自

己点検結果が得られており，相応のセキュリティ対策が全市町村で共通して取られていることが認められる。

また，平成１６年１２月時点では，ＣＳサーバ及びクライアントについては，パスワードの管理の適正化（有効期限の設定，最低桁数の設定，パスワードを利用者に設定させ，マニュアルなどに記載させない，ログイン失敗時にロックアウト）などの対応はほとんど全ての市区町村で取られていることが認められる（乙３７）。

c　被告和歌山県，被告市町における管理の実情

証拠（被告和歌山県及び被告市町に対する調査嘱託の結果）及び弁論の全趣旨によれば，被告和歌山県及び被告市町は，少なくとも，住基ネットの管理のために最低２名の管理者を任命していること，ハードウェアの保守管理については外部業者に委託しており，運用管理については一部外部業者に委託している自治体もあるが，委託業者との間では，委託契約において，業務上知り得た情報について委託契約終了後にも秘密を守る義務を課し，事前に書面による許諾がない限り委託業務の再委託を許さないこととしていること，委託業者又は再委託業者が作業を行う際には，管理者が必ず立ち会うこととしていることが認められる。

(ウ)　情報漏洩の危険性の程度について

a　セキュリティの評価について

一般に，セキュリティ対策に論理的に絶対と言える完璧なものは存在しないが，各段階で考えられる危険性に対する対応を幾重にも重ねることにより，全体としてのセキュリティを十分高度なものにすることが可能であり，仮にその一部にセキュリティが不十分な点があったとしても，全体として確保されているセキュリティの程度が十分なものと評価することができれば足りるものというべきである。

b　複数の市町村にまたがって情報が漏洩する可能性

(a)　想定される攻撃

i　庁内ＬＡＮへの接続

上記(ア)で認定した事実を前提とすれば，①　出先機関からダイヤルアップ接続により，あるいは直接に庁内ＬＡＮに端末を接続して，②　庁内ＬＡＮ上の既存住基サーバの管理者権限を奪取するとともに，③　庁内ＬＡＮとＣＳセグメントとを仕切るＦＷを無効化した上で，④　ＣＳ側から既存住基サーバへ情報を取得しに行くときに，ＣＳ側のアプリケーションのバッファを溢れる長さのデータを返すことにより，バッファオーバーフローの意図どおりの異常を生じさせ，⑤　この異常発生とタイミングを合わせて，予め管理者権限を奪取しておいた既存住基サーバなどから攻撃を仕掛けてＣＳサーバの管理者権限を奪取して，⑥　このＣＳサーバ上のデータを入手してＣＳクライアントの権限を奪取して遠隔操作可能な状態に置き，⑦　ＣＳクライアントの操作者が操作者カードを挿入してログインしている状態において，その操作画面を閲覧したり，操作者がログインしたまま離席したような時点を狙って操作者に気付かれないよう遠隔操作でＣＳクライアントを操作して，正規のユーザがＣＳクライアントにおいて実行できるデータの検索などの操作が可能となるという事態を想定することは可能である。

なお，（上記①の代わるものとして，）①’ＤＭＺ（ＦＷの内側にあって，外部〈インターネット〉とも内部のＬＡＮとも切り離された区域）に公開サーバが設置されている場合，その原理上，ｉ）インターネットとＤＭＺとの間では，ＷＷＷや電子メールの送受信などに用いられるポートは開放されているため，これらの

ポートを用いた攻撃は防ぐことができないから，これらのポートを利用して公開サーバを攻撃することが可能であり，ii）公開サーバを自己の管理下に置くことができれば，ＤＭＺから庁内ＬＡＮへの通信が許可されていたり，庁内ＬＡＮ側に受動的攻撃が可能となるような脆弱性がある場合には，これを利用してインターネットから庁内ＬＡＮへ侵入される事態を想定することは可能である。

ii　ＣＳセグメントへの直接接続

また，長野実験当時の阿智村では，重要機能室外にあるＣＳクライアントなどを利用して物理的にＣＳセグメントに接続可能であるならば，容易にＣＳセグメントに攻撃用端末を接続して，ＣＳの管理者権限を奪取することが可能であったことが認められる。

この場合には，直接にＣＳクライアントの脆弱性を攻撃することによってＣＳクライアントを遠隔操作可能な状態に置くことができれば，上記⑦の行為の前提条件が整うこととなる。

(b)　侵入の具体的可能性

i　上記(a)の態様による侵入を成功させるためには，上記(a) i ①または①’ないし⑦の条件が整うか，物理的にＣＳセグメントに攻撃用端末を接続でき，これを用いてＣＳクライアントを遠隔操作可能な状態に置けることが必要となる。

ii　しかしながら，ＣＳアプリケーションに現実にバッファオーバーフローを生じさせるためには，バッファオーバーフローの危険性のある関数へ引き渡されるパラメータの範囲がプログラムコード上チェックされていないことが前提となるところ，ＣＳアプリケーションのプログラムコードにおいてこのようなチェックが行われていないことを示す的確な証拠はない。

また，上記(イ)ａに認定したところによれば，庁内ＬＡＮとＣＳセグメントとを仕切るＦＷについて，機器や設定に未知の脆弱性が存することを論理的に否定することはできないが，一応適切な設定が行われ，安全性が検証されているということができ，これを無効化することが具体的に可能であることを示す的確な証拠は存しない。

iii　また，ＣＳセグメントへの直接接続の可能性についても，ＣＳセグメントを構成する部分の大半は施錠された重要機能室内に存していて，部外者が物理的に接続することは極めて困難であるし，ＣＳクライアントも一般には庁舎内に設置されており，職員や来庁者の目の届く場所にあるものと考えられるのであって，論理的にはケーブルのつなぎ換えなどの可能性は存するものの，これらの作業を密かに行うことには一定の困難さが伴うものと考えられる（乙２の１，１３，２７，弁論の全趣旨）。

iv　そして，上記(ア)のとおり，長野実験の際には，庁内ＬＡＮ上の既存住基サーバやＣＳサーバには，セキュリティパッチが適用されていなかったために既存の脆弱性を利用した攻撃が容易であったり，ユーザ名及びパスワードの管理が極めて不十分であったために，これらのサーバの管理者権限が奪取される具体的な危険性がある状態であったことは認められるものの，上記(イ)ｂの事実によれば，このような具体的危険性を生む前提条件について相当の改善が行われていることが認められる。

この点について，原告らは，被告市町に対する調査嘱託の回答によれば，委託業者の作業回数が少ないことなどを根拠に，被告市町においてセキュリティパッチが適切に適用されている保証はない旨主張する。

しかしながら，セキュリティパッチを適用する作業は，委託業者によらなければならないほど専門的，技術的知識を要するものではなく，当該自治体の担当者が自ら作業を行うことが容易であると考えられるのであって，セキュリティパッチが被告財団法人から各市町村に随時配付されていることをも併せて考慮すれば（乙３７，弁論の全趣旨），委託業者による作業の頻度が低いことをもって，チェックリストによる自己点検結果の報告が実態に反するものであって現実にセキュリティパッチの適用が適切に行われていないとまで認めることはできない。

v　原告らは，委託業者が点検作業に際して不正を働いた際に，被告市町においてその不正を見抜くことができるとは考えられない旨主張する。

たしかに委託業者の不正に対しては十分な警戒を怠らないことは重要であるが，上記(イ)ｃのとおり，被告市町においては委託業者の点検作業の際には必ず担当職員が立ち会っている上，委託業者との契約において守秘義務を課したり，住民基本台帳法において情報の漏洩に対して刑罰を科すこととするなどの対策を重畳的に取っていることが認められ，これらの対策にもかかわらず担当者が委託業者が不正な作業を行おうとしていることに気付かないうちに委託業者の不正が行われる具体的な危険があることを示す的確な証拠は存しない。

vi　なお，上記(イ)ａで認定した事実に加えて，指定情報処理機関監視ＦＷについては，被告財団法人によって２４時間監視が行われ，ケーブルの抜き差しなども検知できる状態に置かれているのであって（乙３８，３９，弁論の全趣旨），これらの事実によれば，指定情報処理機関監視ＦＷを攻撃して無効化し，他の市町村のＣ

Ｓサーバや庁内ＬＡＮなどへ侵入することは，現実的にはほとんど考えられない。

(c) 小括

以上のように，住基ネットを利用した不正な情報取得のためには，何段階もの関門を全て一時に越える必要があるところ，上記(ア)によれば，長野実験の時点では，物理的接続経路の管理の甘さや，サーバのパッチの適用の遅れなどのために，比較的容易に既存住基サーバの管理者権限が奪取できる状態にあるなど，危険性の高い部分が存在したものの，乗り越えるべき関門が他にも複数存在していたことや，その後セキュリティ対策が強化され，特に管理者権限の奪取などに直結する部分については対策の徹底が図られているのであって，これらの事実を総合すれば，第三者によって住基ネット上の本人確認情報にアクセスしたり，住基ネットからデータが漏洩するような具体的な危険性を残す程度のセキュリティしか備えていないという状態にはなく，その結果，住基ネットには，当該個人のプライバシーの侵害に対する現実の危機が存しないものというべきである。

ウ 法的保護措置

法は，以下のとおり，個人情報保護に関する国際的基準ともいうべき，いわゆるＯＥＣＤ８原則を踏まえたと思われる多角的な保護措置を講じている。

(ア) 保有情報の限定

法は，都道府県及び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，３０条の１０第１項）。

(イ) 本人確認情報の利用及び提供先の制限等

法は，本人確認情報の提供を受ける行政機関等の範囲や利用目的を具体的に規定し，これを限定している（したがって，民間部門には情報提

供されることはない。法３０条の６，３０条の７第３項ないし第６項，３０条の８及び別表）。さらに，本人確認情報の提供を受けた受領者に対し，法律で規定された利用事務以外の目的のために本人確認情報を利用したり提供することを禁止するとともに（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や提供を禁止している（法３０条の３０）。

また，行政庁の執行機関等及び指定情報処理機関は，法律により本人確認情報の提供を求めることが許容されている事務の遂行のために必要がある場合を除き，何人に対しても，住民票コードの告知を求めることが禁じられており（法３０条の４２），それ以外の者は，何人も，第三者に対し，住民票コードの告知を求めたり，業として行う行為に関し，契約の相手方に住民票コードを告知するよう求めることを禁止するとともに，業として住民票コードの記録されたデータベースを構成することを禁止しており，都道府県知事は，これらの規定に違反する行為者に対して中止の勧告や命令をすることができ，この命令に違反した者には罰金刑を科することとしている（法３０条の４２，４３，４４条）。

(ウ) 役職員等に対する秘密保持義務等

法は，職務上，本人確認情報に接する機会のあった指定情報処理機関の役職員や市町村，都道府県又は国の職員及びそれらの者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等に対し，当該事務に関して知り得た本人確認情報に関する秘密等を保持すべき義務を課しており（法３０条の１７，３１，３５），これに違反した場合には，通常の公務員の守秘義務違反よりも重い懲役刑又は罰金刑を科することとしている（法４２条）。

(エ) 安全確保義務

法は，都道府県知事，市町村長その他の行政機関等又は指定情報処理

機関が本人確認情報の電子計算機処理等を行うに当たっては，当該本人確認情報の漏えい，滅失及びき損の防止その他の当該本人確認情報の適切な管理のために必要な措置を講じなければならないと定めている（法３０条の２９，３３）。

これを踏まえて，総務省は，「電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準」（平成１４年総務省告示３３４号，平成１５年総務省告示３９１号，平成１５年総務省告示６０１号）によって具体的な基準を定めている（乙２の１ないし３）。

(オ) 監督命令等並びに報告及び立入検査

法は，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，① 総務大臣においては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，② 委任都道府県知事においては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旨規定するとともに（法３０条の２２），③ 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，書類等を検査することができる旨定めている（法３０条の２３）。

(カ) 自己の本人確認情報の開示，訂正等

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に係る本人確認情報について，開示を請求することができるとともに，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，追加又は削除の申し出をすることができる旨定めている（法３０条の３７，４０）。

エ　小括

以上の結果，無権限の第三者によって住基ネット上の本人確認情報にアクセスしたり，行政機関等の担当役職員等が住基ネットからデータを持ち出して公開するような具体的危険性は認められず，したがって，住基ネットの運用によって，当該個人のプライバシーの利益に対する現実の危機が存するものと認めることはできない。

(4)　行政機関等によるプライバシー情報統合の現実的可能性について

ア　プライバシー情報の統合への住民票コードの利用

住民票コードが種々の行政目的に利用されるに際しては，当該行政目的に関して，当該個人が行政機関に申告した情報や，当該個人と行政機関との相互関係に関する履歴，行政機関が独自に収集した情報などが結び付けて保存されることが考えられる。このようにして収集集積された当該個人に関する情報が，住民票コードを主キーとして連結されれば，当該個人の社会生活全般にわたる情報となり，思想や良心などの内心を推知することが可能となる事態にも至りかねず，公権力主体による国民の管理統制につながる危険性を有するものであることは否定できない。

行政機関等によりそのような事態が発生する具体的危険が存する場合，さらに，住民票コードが，当該個人の他のプライバシーに関する情報と結び付けられた状態で第三者が容易に入手できる状態に置かれている場合や，個別に集積されたプライバシーに関する情報を他者が集積した情報と結合するために利用され，あるいはそのような利用が容易な状態に置かれている場合には，当該個人のプライバシーを害するものということができる。

イ　住民票コードの利用制限

しかしながら，前提事実２ア及び上記(3)ウ記載のとおり，改正法においては，民間部門が住民票コードを利用することを禁止しており，住民票コードが記録されたデータベースを作成したり，契約締結に際して住民票コ

ードの開示を求めることは刑罰をもって禁じられていう

また，民間部門において，仮に住民票コードを入手したとし
ネットに接続することはできず，住民票コードを利用して正規の方法で個人確認情報を得ることはできないのであるから，何らの利益も存しないのが通常であって，民間部門が住民票コードを取得することにより何らかの利益を得られる場面は，何らかの経路で住民票コードが含むデータが漏洩して公開されていたり，複数の機関や個人が相互にこれらの情報を交換しているなどという，住基ネットによらずに住民票コードに結び付けられている個人識別情報やプライバシー情報等の情報を入手することができる状況に置かれているなどの前提条件が整っている場合など，極めて限定された場面に限られると考えられるが，かかる前提条件が現在整っている状況ではないし，将来的にそのような前提条件が整う可能性を認めるに足りる証拠も存しない。

さらに，行政機関等についても，個人情報保護法の適用対象とはされていないものの，改正法上，地方公共団体，指定情報処理機関，本人確認情報の受領者のシステム操作者，委託業者には守秘義務が課せられ，刑罰をもって情報の漏示を禁じられている上，本人確認情報の提供を受けた行政機関等がその情報を目的外に利用することも禁じられていることは上記(3)ウのとおりであり，現実にプライバシー情報が集約されていることをうかがわせるような証拠は全く存しない。

ウ　小括

以上によれば，少なくとも現在においては，民間部門はもとより，行政機関等においても，住民票コードを利用して国民のプライバシー情報を集約することが予定されているものとはいえず，現にプライバシー情報の集約が行われているとも認められないのであって，現時点において，住基ネットの導入によって，プライバシーの利益ないしプライバシー権が現実に

侵害され，あるいは侵害が生じる危険が現実化しているものとはいえない。

(5) 行政機関等による本人確認情報の収集・取得等が正当な目的により，正当な方法によるものか

原告らは，本人確認情報が原告らの意思に基づかずに，行政機関等の間で遣り取りされることが自己の個人情報のコントロール権を侵害する旨主張する。

しかしながら，本人確認情報それ自体は個人の道徳的自律の存在に直接かかわらない外的事項に関する個人情報であるというべきであるから，行政機関等が正当な目的により，正当な方法によって収集，利用，提供しても，何らの権利侵害とはならないものと解すべきことは前記(2)のとおりである。そこで，以下において，住基ネットの目的，方法の正当性の有無について検討する。

ア 証拠（乙３ないし１９，証人黒田充）及び弁論の全趣旨によれば，次の事実が認められる。

(ア) 住民基本台帳は，昭和４２年に制定された住民基本台帳法に基づき，市町村において，住民の居住関係の公証，選挙人名簿の登録その他の住民に関する事務の処理の基礎とするとともに住民の住所に関する届出等の簡素化を図り，あわせて住民に関する記録の適正な管理を図るために制定された制度で，住民に関する記録を正確かつ統一的に行い，もって，住民の利便を増進するとともに，国及び地方公共団体の行政の合理化に資することを目的とする（法１条）ものであり，公的部門において，最も正確で，すべての住民の基礎的な情報を保有し，住民の居住関係等を正確に把握できる唯一の制度である。

しかしながら，住民基本台帳は，各市町村ごとに設けられているため，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，従前から，住民に対して，各

事務ごとに申請，届出，住民票の写しの添付等の負担を課していた。

(イ) その後，各市町村において，電子計算機を利用した事務処理の効率化が図られ，平成７年４月１日時点において，全市町村の９１．１パーセント，人口割合で９８．７パーセントもの住民基本台帳が電算システムにより稼働していたところ，民間部門においては，コンピュータ・ネットワークシステムが構築され，顧客サービスや業務の効率化が急速度で進展していく中，行政部門においても，住民サービスの向上や行政事務の効率化のために，情報通信技術を有効に活用する必要性に迫られていた。

(ウ) そのため，改正法は，住基ネットを創設し，各市町村，各都道府県，指定情報処理機関に電子計算機を設置し，市町村長が都道府県知事に，委任都道府県知事が指定情報処理機関に本人確認情報をネットワークシステムを利用して通知し，それぞれ各市町村，各都道府県，委任都道府県の住民に係る本人確認情報を保存することとし，その上で，本人確認情報について，① 各市町村は，他の市町村に対し，条例で定めるところにより提供し（法３０条の６），② 各都道府県は，法律で規定する事務を遂行する場合に利用し（法３０条の８），③ 各都道府県及び指定情報処理機関は，法律の定めるところにより，市町村，他の都道府県，国の機関等に提供できる（法３０条の７，１０）こととした。

(エ) その結果，住基ネットを利用することにより，これまではそれぞれの事務ごとに住民に義務付けられていた，申請，届出，住民票の写しの添付等の住民側の負担が解消される一方，行政側においても，事務の効率や事務処理の正確性が向上しており，今後も，以下のような事務につき，上記のような住基ネットの効用の拡大が期待されている。

a 行政手続における住民票の写しの提出の省略

b 年金受給者の現況届の提出の省略

c　恩給受給者の受給手続の簡素化

d　住民票の写しの広域交付

e　転出・転入手続の簡素化

f　公的個人認証サービスの実現

g　住基カードの活用

イ　以上のように，住基ネットは，高度に情報化された現代社会において，社会からの要請に基づき，住民の負担軽減（行政サービスの向上），行政事務の効率化及び事務の正確性の向上を図るために導入されたものであり，その目的は正当なものと評価できる。

また，前記前提事実２ウ，エ及び上記(3)ウのとおり，行政機関等の間において収集，提供，利用される情報は，本人確認情報のみに限定され，本人確認情報の提供先や利用目的は法により限定されており，提供された本人確認情報を目的外に利用することは禁じられているうえ，漏洩の危険性に対しては様々な法的保護措置も講じられていることから，その手段においても正当なものと評価することができる。

なお，原告らは，住基ネットに参加を希望する者のみ利用すればよいのであって，希望しない者については参加させる必要はない旨主張するが，いわゆる選択制を採用した場合，非希望者について，従来の手続のための事務処理体制やシステムを残置せざるを得ず，経費の削減効果が著しく減殺されるばかりか，本人確認情報の提供または利用の都度，希望者であるか否かの確認作業が必要となり，事務効率が低下することは明らかであって，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重要な行政目的の一つとする住基ネットの目的を阻害されることは明らかであるから，原告らの上記主張は採用できない。

3　まとめ

以上の結果，住基ネットの稼働により原告らの権利が侵害されているとは認

められないことから，これを前提とする原告らの差止請求は理由がないものといわざるを得ない。

【損害賠償請求の可否について】

1　被告国に対する損害賠償請求について

ア　国会議員の立法行為の違法性

(ア)　国会議員の立法行為が国家賠償法の適用上違法と評価されるのは，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場合に限られると解すべきである（最高裁判所昭和６０年１１月２１日第１小法廷判決・民集３９巻７号１５１２頁）。

改正法は，上記【差止請求の可否について】において検討したとおり，違憲ではないし，まして憲法の一義的な文言に違反しているものとも認められないから，国会議員が改正法を立法したことにつき何ら違法性は存しない。

(イ)　なお，原告らは，国民一人一人に住民票コードという番号を付すること自体が人格権の侵害である旨主張するので，この点について付言する。

氏名は，個人固有の名称であって，個人を特定する機能を有するものであるが，それと同時に個人のアイデンティティ（自己同一性）の拠り所ともなり得るものであって，ゆえなく個人から氏名が奪われるなどする場合には，人格権あるいは人格的利益の侵害に当たると解する余地はある。

しかしながら，従来から，民間部門・公的部門を問わず，個人に対して，当該個人の氏名と並び，あるいは氏名に代えて，当該個人を特定できる一意的なコード番号（会員番号，顧客コード等）を付し，内部的な事務処理にコード番号を利用し，さらには事務手続等に際して当該コード番号の申告を求めることによって，事務処理の機械化・効率化を図ることは，当然許容されることとして広く行われており，このことによって，民間部門・

公的部門と相手方個人との関係において，相手方個人の氏名が無視されたり，氏名を持ち個性を有する存在であることが否定されているものではないことはいうまでもないことである。

住民票コードは，全地方公共団体の住民の住民票に対して全国一律に割り振られ，複数の行政目的のために共通に利用されるという特性を有するものではあるが，一定の限られた行政目的にためにのみ使用されるに過ぎず，個人の精神活動や日常生活に何らの影響も及ぼさないものであり，また，市町村長に対する変更請求によりいつでも何度でも変更できるものであって，一旦割り当てられると，一生，これを固定的に使用し続けなければならないものでもない。さらに，本件全証拠によっても，公権力主体が個々の国民・住民の呼称として住民票コードを用いることが予定されていたり，個々の国民が社会生活を営む上で住民票コードが呼称として利用されてゆくような事態が生じることをうかがわせる具体的な事情は全く認められない。

したがって，この点に関する原告らの主張も採用できない。

(ウ) 原告らは，改正法附則１条２項により「所要の措置」を講ずることが義務付けられているにもかかわらず，国会が何らの必要な立法措置を講じなかったことが違法である旨主張するが，同条項は，「政府」に対して「所要の措置」を講ずることを求めているのであって，国会に対し法的義務を課したものでないことは文言上明らかである。

イ　内閣の改正法施行等の違法性

(ア) 原告らは，改正法が違憲であることが明白であるにもかかわらず，これを施行する政令を定めた内閣，内閣総理大臣及び総務大臣の行為は違法である旨主張するが，改正法が憲法に明白に反するものでないことはすでに検討したとおりである。

(イ) また，原告らは，内閣，内閣総理大臣及び総務大臣は，改正法附則１条

２項に定める「所要の措置」を講ずる義務があったにもかかわらず，これを講じないまま，漫然と改正法を施行した点に違法がある旨主張する。

しかしながら，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。」と定めているものの，これをもって，改正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とまでは認められず，他方，改正法附則１条１項により，改正法は公布の日から起算して３年を超えない範囲内で施行することが義務付けられていたのであるから，内閣が，改正法の施行日を平成１４年８月５日と定める政令を制定し，改正法を施行したことが違法性を有するとは到底認められない。

(ウ) さらに，原告らは，内閣がセキュリティが脆弱なまま住基ネットの運用を開始し継続していることが違法である旨主張するが，住基ネットのセキュリティが脆弱でないことは，前記【差し止め請求の可否について】２，(3)において，すでに検討したとおりである。

ウ　小括

以上のとおりであるから，原告らの被告国に対する損害賠償請求は，その余の点について検討するまでもなく理由がない。

2　被告和歌山県及び被告財団法人に対する賠償請求

原告らは，被告和歌山県及び被告財団法人が，違憲である改正法に基づき，所要の措置が講じられないままで，セキュリティが脆弱なままの住基ネットの運用を継続したことが違法である旨主張するのであるが，いずれもその前提を欠くことがすでに検討したところから明らかであるから，被告和歌山県及び被告財団法人の行為に違法性は認められない。

したがって，原告らの被告和歌山県及び被告財団法人に対する損害賠償についても理由がないものと言わざるを得ない。

【結論】

以上の次第で，原告らの被告らに対する各請求はいずれも理由がないからこれらを棄却することとし，主文のとおり判決する。

和歌山地方裁判所民事部

裁判長裁判官　　村　岡　　寛

裁判官秋本昌彦及び裁判官寺元義人は，転勤のため，署名押印することができない。

裁判長裁判官　　村　岡　　寛