乙第37号証

平成１９年２月１６日判決言渡　同日原本領収　裁判所書記官

平成１４年(ワ)第２２４０号　住民基本台帳ネットワーク差止等請求事件

平成１５年(ワ)第７１５号　　住民基本台帳ネットワーク差止等請求事件

口頭弁論終結日　平成１８年９月２９日

判　　決

当　　事　　者　　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

1　被告埼玉県は，

(1)　住民基本台帳法３０条の７第３項の別表第一の上欄に掲げる国の機関及び法人に対し，原告らの本人確認情報（氏名，出生の年月日，男女の別，住所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。なお，上記氏名から住所までの４つの情報を併せて，以下「４情報」という。）を提供してはならない。

(2)　被告財団法人に対し，原告らに関する住民基本台帳法３０条の１０第１項記載の本人確認情報処理事務を委任してはならない。

(3)　被告財団法人に対し，原告らの本人確認情報を通知してはならない。

(4)　原告らの本人確認情報を，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。

2　被告財団法人は，

(1)　被告埼玉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項記載の本人確認情報処理事務を行ってはならない。

(2) 原告らの本人確認情報を，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。

3 被告埼玉県及び被告財団法人は，原告らそれぞれに対し，連帯して，１１万円及びこれに対する平成１４年(ワ)第２２４０号事件原告[redacted]については平成１４年１１月１９日から，その余の原告らについては平成１５年４月１２日から各支払済みまで年５分の割合による金員を支払え。

4 被告国は，原告らそれぞれに対し，１１万円及びこれに対する平成１４年(ワ)第２２４０号事件原告[redacted]については平成１４年１１月１９日から，その余の原告らについては平成１５年４月１２日から各支払済みまで年５分の割合による金員を支払え。

5 訴訟費用は被告らの負担とする。

6 第３，４項につき仮執行宣言

第２ 事案の概要

１ 事案の要旨

本件は，埼玉県内に居住する原告らが，住民基本台帳法（昭和４２年法律第８１号。以下「住基法」という。）の平成１１年の改正（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。））により導入された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。）の稼働，運用によって，原告らの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」が侵害され，仮に侵害されていないとしても，住基ネットの稼働，運用によって原告らの自己情報コントロール権が侵害される具体的危険が存在する旨主張して，これらの権利ないし自由に基づき，被告埼玉県及び被告財団法人に対し，原告らについて住基ネットを稼働，運用することの差止め及び原告らの本人確認情報（住基法３０条の５第１項）の住基ネットの磁気ディスクからの削除を求めるとともに，被告らに対し，国家賠償法（以下「国賠法」という。）１条１項又は民法７０９条に基

づき，これらの権利ないし自由が侵害されたことについて，慰謝料及び弁護士費用並びに各訴状送達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を求めた事案である。

２　争いのない事実

(1)　当事者

ア　原告らは，いずれも埼玉県内に居住し，住民登録をしている者である。

イ　被告財団法人は，国と地方公共団体の間における情報処理システムの調整に関する調査等を目的とする法人であり，平成１１年１１月１日，自治大臣（当時。現総務大臣）から，改正法による改正後の住基法３０条の１０第１項所定の「指定情報処理機関」（後記(2)エ）に指定された。

(2)　住基ネットの概要

ア　住民基本台帳制度

住民基本台帳制度は，特別区を含む市町村において，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，住民に関する記録を正確かつ統一的に行う制度である（住基法１条）。

イ　改正法による住基ネットの構築

(ア)　平成１１年８月１８日，改正法が公布され，住基ネットを構築することとされた。住基ネットは，市町村の区域を越えた住民基本台帳に関する事務の処理や，国の行政機関等に対する本人確認情報の提供を行うためのネットワークシステムである。

(イ)　本人確認情報とは，住民票の記載事項のうち，氏名，出生の年月日，男女の別，住所及び住民票コード並びにこれらの変更情報をいう（住基法３０条の５第１項）。変更情報とは，①住民票の記載，消除若しくは記載の修正を行った旨又は住民票コードについて記載の修正を行った旨，

②転入，転出，出生，死亡等住民基本台帳法施行規則（平成１１年自治省令第３５号。以下「住基法施行規則」という。）１１条に定める事由，③その事由が生じた年月日等をいう（住民基本台帳法施行令（昭和４２年政令第２９２号。以下「住基法施行令」という。）３０条の５）。

(ウ) 住民票コードとは，改正法により新たに住民票の記載事項とされた，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（住基法7条１３号），無作為に作成された１０桁の数字及び１桁の検査数字であり（住基法施行規則１条），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を指定し，これを当該市町村長に対し，通知する（住基法３０条の７第１項）。

市町村長は，改正法の施行日に，現に住民基本台帳に記録されている者の住民票に，都道府県知事から指定された住民票コードのうちからいずれか一つを選択して記載する（改正法附則３条）。

市町村長が住民票の記載をする場合，当該記載に係る者につき直近に住民票の記載をした市町村長が当該住民票に直近に記載した住民票コードを記載する（住基法３０条の２第１項）が，いずれの市町村においても住民基本台帳に記録されたことがない者については，市町村長が，新たにその市町村の住民基本台帳に記録して住民票の記載をする場合，都道府県知事から指定された住民票コードのうちからいずれか一つを選択し，これを住民票に記載する（住基法３０条の２第２項）。

(エ) 住基ネットの導入により，①各市町村に，既存住基サーバ（各市町村において住民の住民票を記録，管理するサーバ）とは別に，橋渡しをするためのコミュニケーションサーバ（以下「ＣＳ」という。）を設置し，②既存住基サーバからＣＳに本人確認情報を送信してＣＳにこれを保存し，③各市町村のＣＳを専用回線（接続先が固定されており，所定の伝送速度が保証されている回線）で結んでネットワーク化し，④各都道府

県に都道府県サーバ（各都道府県管下の全市町村のＣＳから送信された本人確認情報を記録，管理するサーバ）を，指定情報処理機関（後記エ）に指定情報処理機関サーバ（指定情報処理機関に設置され，全都道府県の都道府県サーバから送信された本人確認情報を記録，管理するサーバ）をそれぞれ設置し，その上で，後記ウのとおり，本人確認情報の通知，提供等を行うことになった。

ウ　本人確認情報の通知，保存，提供，利用

本人確認情報の通知，保存，提供，利用について，住基法及び住基法施行令に次の定めがある。なお，住基ネットを利用することが可能な事務は，平成１８年５月１５日の時点で，２９３種類である。

(ｱ)　市町村長は，住民票の記載，消除又は氏名，出生の年月日，男女の別，住所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，都道府県知事に対し，その使用する電子計算機（ＣＳ）から電気通信回線を通じて都道府県知事の使用する電子計算機（都道府県サーバ）に送信する方法により，当該住民票の記載に係る本人確認情報を通知する。都道府県知事は，市町村長から通知を受け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として５年間保存しなければならない（住基法３０条の５，住基法施行令３０条の６）。

(ｲ)　市町村長は，条例で定めるところにより，他の市町村の市町村長等から求めがあったときは，本人確認情報を提供する（住基法３０条の６）。

(ｳ)　都道府県知事は，住基法別表第一の上欄に掲げる国の機関又は法人（以下「国の機関等」という。）から同表の下欄に掲げる事務の処理に関し，住民の居住関係の確認のための求めがあったときに限り，保存期間に係る本人確認情報を提供する（住基法３０条の７第３項）。

(ｴ)　都道府県知事は，住基法施行令又は条例で定めるところにより，当該都道府県の区域の市町村の市町村長その他の執行機関に対し，保存期間

に係る本人確認情報を提供する（住基法３０条の７第４項）。

(オ) 都道府県知事は，住基法施行令又は条例で定めるところにより，他の都道府県の都道府県知事その他の執行機関に対し，保存期間に係る本人確認情報を提供する（住基法３０条の７第５項）。

(カ) 都道府県知事は，住基法施行令又は条例で定めるところにより，他の都道府県の区域内の市町村の市町村長その他の執行機関に対し，保存期間に係る本人確認情報を提供する（住基法３０条の７第６項）。

(キ) 上記(ウ)～(カ)の本人確認情報の提供は，電気通信回線を通じて送信する方法又は本人確認情報を記録した磁気ディスクを送付する方法により行う（住基法施行令３０条の７～１０）。

(ク) 都道府県知事は，所定の事務を遂行するとき，保存期間に係る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）。

(ケ) 都道府県知事は，条例で定めるところにより，都道府県知事以外の当該都道府県の執行機関に対し，保存期間に係る本人確認情報を提供する（住基法３０条の８第２項）。

(コ) 国の行政機関は，その所掌する事務について必要があるときは，都道府県知事に対し，保存期間に係る本人確認情報に関して資料の提供を求めることができる（住基法３７条２項）。

エ 指定情報処理機関

(ア) 都道府県知事は，総務大臣の指定する指定情報処理機関に対し，住基法３０の１０第１項所定の本人確認情報処理事務（上記イ(ウ)記載の住民票コードの指定，通知，ウ(ウ)～(カ)記載の本人確認情報の提供等）を行わせることができる。指定情報処理機関にその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（委任都道府県知事）は，原則として，本人確認情報処理事務を行わない（住基法３０条の１０第１項本文，同条３項）。

(イ) 委任都道府県知事は，その使用する電子計算機（都道府県サーバ）から電気通信回線を通じて指定情報処理機関の使用する電子計算機（指定情報処理機関サーバ）に送信する方法により，指定情報処理機関に対し，本人確認情報を通知する。指定情報処理機関は，委任都道府県知事から通知を受け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として５年間保存しなければならない（住基法３０条の１１，住基法施行令３０条の１１）。

オ　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，自己の住民基本台帳カード（その者の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。以下「住基カード」という。）の交付を求めることができる（住基法３０条の４４第１項）。市町村長その他の市町村の執行機関は，条例の定めるところにより，住基カードを条例の定める目的のために利用することができる（同条の４４第８項。以下，市町村が条例に基づいて提供する住基カードを利用した行政サービスを総称して，「市町村独自サービス」という。）。

(3) 改正法の施行と住基ネットの稼働

改正法のうち，指定情報処理機関の指定，住民票コードの指定等に係る規定は平成１１年１０月１日に，住民票コードの記載，電気通信回線を通じた本人確認情報の通知，提供等に係る規定は平成１４年８月５日に，住基カード等に係る規定は平成１５年８月２５日に，それぞれ施行され，住基ネットの仮運用が平成１４年７月２２日に，本運用が同年８月５日に，それぞれ開始された。

被告財団法人は，埼玉県知事から委任を受けて，住基法３０条の１０第１項所定の「本人確認情報処理事務」を行っている。原告らについても，住基

法に基づき，住民票コードの住民票への記載，本人確認情報の通知，保存等が行われている。

3　争点

(1)　差止請求について

ア　自己情報コントロール権の侵害を理由とする差止請求の可否（争点1）

イ　自己情報コントロール権侵害の具体的危険を理由とする差止請求の可否（争点2）

ウ　氏名権に基づく差止請求の可否（争点3）

エ　「公権力によって包括的に管理されない自由」に基づく差止請求の可否（争点4）

(2)　損害賠償請求について

ア　被告らの責任の有無（争点5）

イ　損害額（争点6）

4　争点に関する当事者の主張

(1)　争点1について

（原告らの主張）

ア　自己情報コントロール権の内容等

(ア)　プライバシー権は，全体主義の経験を歴史的背景として成立し，近代立憲主義そのものをその成立の根元的基礎とし，憲法13条により保障される具体的権利である。

そして，現代社会においては，情報処理技術の発展により，情報の収集，利用，加工，検索等を行うことが容易になり，とりわけ公権力が個人情報を本人の知らないうちに収集，管理等できるとすると，個人の意思決定や行動を萎縮させ，その人格的自律が脅かされるおそれがあることにかんがみれば，プライバシー権には，自己情報コントロール権（自己に関する情報をコントロールする権利）が含まれると解すべきである

（最高裁判所平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁（以下「平成１５年判決」という。）参照）。すなわち，個人は，憲法１３条に基づき，自己に関する個人情報の収集・取得，管理（保有）・利用，開示・提供のすべて（以下「収集等」という。）について，原則として自らの意思に基づいて決定することができるというべきであり，さらに，派生的には，自己に関する個人情報の開示・訂正請求権が認められるというべきである。

このようなプライバシー権の沿革，内容等に照らせば，自己情報コントロール権は，排他的権利であり，差止請求の根拠となるというべきである。

(イ) 住基ネットを通じて流通する本人確認情報は，いずれも自己情報コントロール権による保護の対象となる。

そして，４情報は個人識別のための基本的な情報であり，個人情報の検索に用いられる機能を有すること，住民票コードはその性質上個人情報の検索，名寄せ（行政機関が保有する個人情報を集積すること），データマッチング（複数の個人情報データをコンピュータを通じて比較，検索及び結合すること）を行う「マスターキー」となり得ること，変更情報は身上の変更を推知させるものであることからすれば，本人確認情報を構成する各情報は，そもそもその一つ一つが慎重な取扱いを要する情報であるというべきである。そして，住基ネットは，これらの各情報を一体のものとして，全国的なコンピュータネットワーク上を流通させるシステムであり，しかも，本人確認情報を取り扱うのが公権力（行政機関）であることに照らせば，本人確認情報を保護する必要性は高く，その収集等について個人が自ら決定する機会を与えられることの必要性や重要性もまた高いといえる。

イ　自己情報コントロール権の侵害

(ア) 住基ネットの稼働，運用により，原告らの本人確認情報は，原告らの同意なく（むしろその意思に反して），原告らが居住する市町村以外の行政機関等に通知，提供することができる状態に置かれることになったものであり，また，改正法の定める個人情報保護措置は，自己情報コントロール権の内容を表すところのＯＥＣＤ８原則に照らして不十分であるから，改正法を施行して住基ネットを稼働，運用したこと自体，直ちに原告らの自己情報コントロール権を侵害するものである。

(イ) そうでないとしても，住基ネットのように，公権力による個人情報の取扱いが問題となる場面においては，私人間における場合と異なり，自己情報コントロール権と他の人権（表現の自由等）との調整は不要であるから，公権力が本人の承諾なく個人情報の収集等を行うことは，原則として許されず，厳格な要件を満たす場合にのみ許容される。したがって，住基ネットによる本人確認情報の流通を承諾していない原告らとの関係で住基ネットを稼働，運用することが許容されるためには，①住基ネットの稼働，運用について原告らの自己情報コントロール権を犠牲にしてもなお達成すべき高度の必要性があり，かつ，②すべての国民について住基ネットを稼働，運用させなければ，施策として成り立たないこと，すなわち，原告らが住基ネットから離脱することにより重大な支障が生じることを要すると解すべきである。

しかるに，住基ネットの導入は費用対効果の観点からみればむしろ非効率的であり，また，住基ネット導入前の行政手続における住民の負担は軽微なものにすぎず，住基ネットによる便益を享受するか否かは各個人の選択にゆだねるべきであるといえ，さらに，住基ネットないし住基カードに関連する行政サービスの利用状況は低調であるから，原告らの自己情報コントロール権を犠牲にしてまで住基ネットを稼働，運用すべき高度の必要性は皆無である。被告らは，住基ネットは行政事務の効率

化や住民の便益に資するものであり，電子政府・電子自治体の実現に必要不可欠な基盤となると主張するが，被告らの主張は恣意的な数値に基づくものであるし，電子政府・電子自治体構想は，改正法の成立後に策定されたものであるから，住基ネットの目的とはいえない。

また，現在，住基ネットに参加していない自治体が存在するにもかかわらず，住基ネットの運用に特段の支障は生じていないことからすると，原告らが住基ネットから離脱しても重大な支障が生じることはないといえる。

したがって，原告らとの関係で住基ネットを稼働，運用し，住基ネットを通じて原告らの本人確認情報を通知，提供等することは，原告らの自己情報コントロール権を侵害し，違憲，違法である。

ウ　セキュリティ対策の不備による自己情報コントロール権侵害の危険

住基ネットにおいては，全国の市町村の既存住基サーバ，ＣＳ，都道府県サーバ，指定情報処理機関サーバがすべてネットワークで接続されているため，このうちの１か所にでもセキュリティ上の不備があれば，原告らのプライバシーに係る個人情報が漏えいの危険にさらされることになる。

長野県が実施した侵入実験の結果，住基ネットには，①ＣＳや，ＣＳ端末（ＣＳが提供する機能やデータを利用する端末）のＯＳ（コンピュータシステム全体を管理するソフトウェア）の管理者権限（マシンの全機能を利用，管理することができる管理者用アカウントとその権限）を略奪することが容易であり，しかもＣＳ端末の画面を遠隔の攻撃端末（不正侵入を図る者が使用するコンピュータ）から操作可能である，②庁内ＬＡＮ及び既存住基サーバのセキュリティが極めて不十分である，③ＣＳサーバと既存住基サーバの間でデータのやりとりをするのに使うアプリケーションに使用されている関数に重大な脆弱性が存在するというセキュリティ上の脆弱性があることが明らかになった。このような脆弱性を突いて不正な攻撃

がされ，ＣＳ，ＣＳ端末，既存住基サーバの管理者権限が略奪されれば，原告らの本人確認情報の閲覧・改ざんや住民票の写しの広域交付等を行うことが可能になるのであるから，原告らの自己情報コントロール権が侵害される具体的かつ現実的な危険があるといえる。

また，一定の目的のもとに集められた個人情報が，複数の機関相互で交換されたり，１か所で集中的に管理されたりすると，コンピュータやネットワークシステムの技術的な性質上，情報の流出・流用や目的外利用が発生することは経験的に知られているところであるし，また，住基ネットに関係した事務に従事する者による個人情報の漏えいや目的外利用の危険もある。そして，住基ネットに関連して，①北海道斜里郡斜里町における住基ネットに関する情報の流出，②北海道帯広市職員による業務外での住民票等交付業務端末の不正閲覧，③福島県東白川郡塙町における住民票コードが記載された名簿の配布等の看過できない事故が発生していることからすると，その危険は具体的かつ現実的なものとなっていることは明らかであるし，上記事故により流出した情報を利用して第三者が住基ネットに不正に侵入する危険性も飛躍的に高まったというべきである。

これに対し，被告らは，外部からの不正な侵入や関係者の不正利用を防止するために，各種の基準や規定を設けており，各自治体が自己点検を行うことによりこれらの規定等の遵守が担保されているから，住基ネットのセキュリティ対策は十分である旨主張する。しかしながら，上記のような住基ネットシステムの脆弱性に照らせば，被告らの主張する対策は不正侵入や不正利用を防止するためには不十分である。そして，原告らの居住地を含む多くの地方自治体においては，住基ネットの稼働，運用に当たり，①ＣＳやＣＳ端末に関し，ｉ設置場所や管理方法等に問題がある，ii パッチを当てる作業（一旦完成したプログラムの修正を行うためのファイル（パッチ）を使ってプログラムの不備を修正すること）が極めて遅い，iii

パスワードの管理が不十分である，②セキュリティポリシーの制定やリスクアセスメントを行っていない，③外部監査を受けていない等の問題点が発生しており，被告らの主張するセキュリティ対策でさえ実効的に運用されているとはいえないのが実情である。また，改正法施行前の住民基本台帳制度の下でも，守秘義務や罰則等の定めがありながら，行政機関関係者による個人情報の漏えいや目的外利用が行われてきたことに照らせば，改正法をはじめとする各種規定による規制は，プライバシー保護のための万全な措置といえないことは明らかである。

エ　データマッチングによる自己情報コントロール権侵害の可能性

住基ネットは，住民票コードを含む本人確認情報を流通させるシステムであるところ，住民票コードは国民一人一人に固有の番号であるから，これを利用して国民の個人情報について正確かつ完全にデータマッチングをすることが可能になった。

そして，近年，行政機関のコンピュータネットワークとして，各省庁のＬＡＮを相互に接続する霞が関ＷＡＮ，各省庁のＬＡＮと地方公共団体のＬＡＮを相互に接続する統合行政ネットワーク（ＬＧＷＡＮ）が整備され，かつ，霞が関ＷＡＮとＬＧＷＡＮとは相互に接続されていることからすれば，これらのネットワークと住基ネットとがあいまって，国民の個人情報についてデータマッチングをするシステムは既に整ったといえる。

さらに，①各省庁において，「一省庁一ネットワーク」の実現を目指し，従来のネットワークを再構築してすべての端末間で情報の共有を可能にし，運用管理を一元化する「最適化計画」が策定され，実現化されつつあること，②入国管理に関して，各航空会社の提供する顧客の電子データ情報を，警察庁，法務省及び財務省が保有するデータベースと照合できるようにする事前旅客情報システム（Advance Passenger Information System。以下「ＡＰＩＳ」という。）が導入されたこと，③外国人の入国及び在留に関

する情報を一元的に管理するシステムが計画され実行に移されつつあること，④政府の諸機関において，納税者番号制度や社会保障番号制度の導入と住民票コードの利用が検討されていること等に照らせば，国民の個人情報を検索，照合し，ひいては，住民票コードを利用した「国民総背番号制度」を導入してすべての個人情報を統合するシステムを構築することは，技術的に十分可能であるし，それが具体的な立法もないまま現実化する危険も高まっているといえる。

この点について，被告らは，住基法はデータマッチングを禁止しており，違反行為には罰則規定が存在すること，現在本人確認情報の提供が認められている事務について，国の機関等の有する情報を一元的に管理する主体もシステムも存在しないことを理由に，原告らの主張するような危険はないと主張する。しかしながら，住民票コードを用いてデータマッチングをすることを明確に禁止する規定は，住基法にも行政機関の保有する個人情報の保護に関する法律（以下「行政機関個人情報保護法」という。）にも存在しないし，上記のとおり，行政機関による個人情報のデータマッチングは，現実化されつつあるのであるから，個人情報を一元的に管理する主体もシステムも存在しないから危険はないなどといえる状況ではない。

オ　まとめ

以上のとおり，自己情報コントロール権は差止請求の根拠となる排他的な権利であるところ，住基ネットの稼働，運用により原告らの自己情報コントロール権は現に侵害されている。そして，住基ネットには原告らの自己情報コントロール権を犠牲にしてまでこれを導入し，稼働，運用すべき高度の必要性がなく，原告らが住基ネットから離脱することにより特段の支障が生じることはない。したがって，原告らの差止請求は認められるべきである。

（被告らの主張）

ア　自己情報コントロール権の内容等について

(ア)　プライバシーの法的保護の内容は，「みだりに私生活（私的生活領域）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り，自己情報コントロール権がプライバシー権の内容に含まれるとはいえない。原告らが引用する平成１５年判決は，個人のプライバシーに係る情報が不法行為法上の被侵害利益として法的保護に値するかどうかについて判断を示したものにすぎない。

仮に，自己情報コントロール権がプライバシーの一内容に含まれるものであるとしても，自己情報コントロール権は，実体法上の根拠がない上，その実質的な内容，範囲，法的性格についても様々な見解があり，権利としての成熟性が認められないから，名誉権と同様の排他性を有する人格権であるとはいえず，これに基づく差止請求は認められない。

(イ)　本人確認情報のうち，４情報は，個人を識別するための単純な情報であり，従前から住基法１１条，１２条に基づく閲覧等の請求が可能であったものであるし，住民票コードは１１桁の数字にすぎず，変更情報は身分関係の変動を端的に推知させる情報ではないことからすると，本人確認情報を構成する情報は，いずれもおよそ個人の人格的自律などにかかわらない客観的外形的事項に関するものにすぎず，思想，信条等個人の道徳的自律に関係したり，人格権の内容を構成するものでもない。

イ　プライバシー侵害の有無について

(ア)　住民票記載の情報のように社会生活の基礎となる個人情報は，いわば公共領域に属する個人情報であり，住基法は，少なくとも行政機関内部で使用される限り，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これを利用することを当然に予定しているものといえる。このことは，改正法施行の前後を通じて何ら変わりない。また，

ＯＥＣＤ８原則に照らして本人の同意が要件になるのは，本来の利用目的以外のために個人データの利用等を行おうとする場合であって，個人情報の収集目的の範囲内又は法律の規定による場合については，個別の住民の同意を得ることが求められているとはいえない。したがって，原告らの同意を得ずに住基ネットにおいて原告らの本人確認情報を利用することは，原告らの権利，利益を何ら侵害するものではない。

(イ) また，次に述べるとおり，改正法には正当な行政目的があり，住基ネットは，行政目的の実現のために必要であるといえる。

すなわち，住基ネットは，高度に情報化された現代社会における行政サービスの向上と行政事務の効率化を目的とし，その実現のために不可欠の全国的な本人確認システムとして，全国の市町村に設置された既存住基サーバを利用して構築されたものである。そして，その導入により，行政手続における住民票の写しの提出の省略，年金受給者の現況届の提出の省略，恩給受給者の受給手続の簡素化，住民票の写しの広域交付及び転出・転入手続の簡素化等が実現し，住民の負担も軽減した。そのほか，住基ネットは，公的個人認証サービスを利用する際に必要な電子証明書を取得する際の本人確認や同証明書発行後に異動等の事由が生じた場合にそれを反映するための手段として利用されており，現在，公的個人認証サービスやこれを利用した行政手続のオンライン化に不可欠の役割を果たすものとして，我が国の国家戦略である電子政府・電子自治体の基盤をなしている。

このほか，住基カードは，公的個人認証サービスを利用する際に電子証明書及び秘密鍵の格納媒体となる等，各種行政サービスを受ける際に利用されるだけでなく，公的な身分証明書の機能も果たす上，条例の定めにより市町村独自サービスを受けるための多目的カードとして活用できるという有用性がある。

加えて，改正法制定当時の試算によれば，住基ネット導入時の経費として約３９０億円，維持管理のための年間経費として約１９０億円が必要となるのに対し，毎年，行政側の経費節減として約２４０億円，住民側の負担軽減として約２７０億円の便益があると見込まれている。

(ウ) このように住基ネットには正当な行政目的及び必要性があるから，原告らの同意なく本人確認情報を利用しても，違法となるものではない。なお，住民の一部が住基ネットから離脱することを認めれば，本人確認情報を利用する行政機関等において，従前の事務処理体制やシステム等を存置し，本人確認情報の提供又は利用の都度，住基ネットの利用を希望する者か否かを確認することが必要となり，行政事務を効率化してコストを削減するという住基ネット本来の目的の達成を著しく阻害する結果となる。したがって，住民の一部が住基ネットから離脱することを認めることはできない。

ウ セキュリティ対策の不備によるプライバシー侵害の危険性について

(ア) 住基ネットについては，次のとおりセキュリティ対策がされている。

a セキュリティ確保のための定め

住基法上，本人確認情報を保護するため，ＯＥＣＤ８原則を踏まえて，①本人確認情報の提供先を公共部門に限定し（住基法３０条の６～８，別表），民間での利用を禁止し（住基法３０条の４３，４４条），②指定情報処理機関サーバや都道府県サーバにおける保有情報を本人確認情報に限定し（住基法３０条の５第１項），③本人確認情報を利用できる場合を限定し（住基法３０条の６，３０条の７第３項～第６項，３０条の８，別表），④住民票コードについては特に利用を制限し（住基法３０条の４２，３０条の４３），⑤情報提供を受けた者について，法律で規定された利用事務以外の目的での本人確認情報の利用を禁止し（住基法３０条の３４），⑥本人確認情報を取り扱

う機関に本人確認情報等の安全確保措置義務を課し（住基法３０条の２９，３０条の３３，３６条の２），⑦関係職員に罰則付きの守秘義務を課し（住基法３０条の１７，３０条の３１，３０条の３５，４２条），⑧制度運用に関する住民参加等の制度を定め（住基法３０条の３７，３０条の４０，３０条の４１，３６条の３），⑨記録の最新性及び正確性を確保する（住基法３０条の５第１項，３０条の１１第１項）等の様々な定めが置かれている。

また，「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年総務省告示第３３４号。以下「セキュリティ基準」という。）においても，個人情報保護のための具体的なセキュリティ対策が定められている。

b　外部からの不正な侵入の防止対策

第三者の物理的な侵入を防止するため，セキュリティ基準は，建物への侵入の防止，重要機能室の配置及び構造，入退室管理，磁気ディスクや関連設備等の管理等につき定めている。

電気通信回線を経由した侵入防止対策としては，①ＣＳ，都道府県サーバ及び指定情報処理機関サーバ間の通信はすべて専用回線及び専用交換装置で構成された閉鎖的ネットワークを介して行い，②サーバ間では，解読が困難なようにデータを暗号化して相互認証・暗号通信を実施し，③通信プロトコル（ネットワークを介してコンピュータ同士が通信を行う上で，相互に決められた約束事の集合）については，住基ネットに固有のアプリケーションによる独自のものを使用し，④コンピュータウイルスやセキュリティホール対策を実施し，⑤すべてのＣＳ及び都道府県サーバの各ネットワーク側並びに指定情報処理機関サーバの全方向に指定情報処理機関が管理するファイアウォール

（組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム。以下「ＦＷ」という。）を設置し，かつ，ネットワーク内に侵入検知装置を設置し，不正通信の監視と遮断を行い，⑥ＣＳと既存住基サーバ又は庁内ＬＡＮを接続する場合や，庁内ＬＡＮと外部ネットワークとを接続する場合は，市町村が管理するＦＷを設置して不正な通信を遮断する等の措置を講じている。

なお，被告財団法人は，平成１５年１０月，東京都品川区を対象として，アメリカの監査法人によるＦＷとＣＳ端末の模擬攻撃（ペネトレーションテスト）を行ったが，これらの機器への侵入は成功せず，セキュリティ上の脆弱性も見出されなかった。

c　内部の不正防止対策

情報の漏えいや不正な目的での提供等を防止するため，住基法上，本人確認情報を取り扱う行政機関の職員や委託事業者に対する秘密保持義務（住基法３０条の１７，３０条の３１，３０条の３５）及び罰則（通常の公務員の守秘義務違反よりも重い。）が定められている（住基法４２条）ほか，行政機関個人情報保護法５３条～５５条にも同趣旨の定めがある。指定情報処理機関に対しても，これを適切に監督するための様々な手段（住基法３０条の１６，３０条の１８，３０条の２２，３０条の２３等）が講じられている。

また，①本人確認情報検索の照会条件の限定，②ＣＳ端末からサーバにアクセスする際の操作者識別カードの利用，③アクセスログの解析，④住民の請求による本人確認情報の提供状況の開示，⑤住民票の写しの広域交付に係る不正を防止するためのシステムの採用，⑥担当職員に対する教育・研修等を通じて，権限のない職員や第三者がみだりにサーバにアクセスして個人情報を検索することを防止するとともに，万一不正があった場合にはその端緒を発見して対処できるような

措置がとられている。

d　住基カードのセキュリティ対策

住基カードについても，「住民基本台帳カードに関する技術的基準」（平成１５年総務省告示第３９２号。以下「住基カードセキュリティ基準」という。）が定められ，ＩＣカードの採用，暗証番号の設定，耐タンパー性（非正規な手段による機密データの読取りを防ぐ能力）の確保等の技術面及び管理・運用面の双方について，十分なセキュリティ対策が講じられている。

e　自己点検の実施

市町村が，平成１５年及び同１６年に，チェックリストを用いて，所定のセキュリティ対策の実施につき自己点検を行った結果，すべての市町村において，重要点検項目につき３点満点を達成し，セキュリティ対策が徹底していることが明らかになった。

(イ) 以上によれば，住基ネットについては，制度上もシステム上も十分なセキュリティ対策が講じられており，住基ネットによるプライバシー権侵害の危険性はないといえる。

(ウ) 原告らは，長野県において行われた侵入実験により住基ネットのセキュリティ上の脆弱性が明らかになった旨主張するが，上記実験においては，インターネットから庁内ＬＡＮへ侵入する実験及び庁内ＬＡＮからＦＷ越しにＣＳセグメントへ侵入する実験は，ことごとく失敗に終わったものであり，バッファオーバーフロー攻撃によるＣＳ端末の管理者権限の取得も実現していない。上記実験の結果，一部の市町村において，庁舎内に物理的かつ違法に侵入した上で，攻撃端末が接続されたという極めて特異な条件の下で，当該市町村の庁内ＬＡＮ上にある当該市町村の住民の個人情報について漏えい等の可能性があることが示されたが，その可能性が現実化することは想定し難い。したがって，長野県侵入実

験の結果により住基ネットのセキュリティの脆弱性が裏付けられるものではない。

エ　データマッチングによるプライバシー侵害の可能性について

(ア)　住基法及び行政機関個人情報保護法等の関係法令は，法令の許容する目的範囲内の利用等に当たらないデータマッチング（複数の個人情報ファイルに含まれる電子データを比較，検索及び結合すること）を絶対的に禁止する（住基法３０条の３４，行政機関個人情報保護法３条２項，８条１項，３項）とともに，公務員がこれに反してデータマッチングを行ったり，本人確認情報に関する秘密を他の行政機関に漏らしたりした場合の懲戒処分（国家公務員法８２条，地方公務員法２９条）や，罰則（住基法４２条，国家公務員法１０９条１２号，１００条１項，２項，地方公務員法６０条２号，３４条１項，２項，行政機関個人情報保護法５３～５５条）を定めている。しかも，平成１８年５月１５日現在，本人確認情報の提供が認められている事務は２９３事務あるが，住基ネットの制度上，それぞれの機関が受領した本人確認情報は分散して管理されることが予定されており，指定情報処理機関及び本人確認情報の提供を受けた国の機関等が管理している個人情報を統一的に収集し得る主体もシステムも存在しない。

また，都道府県には本人確認情報の保護に関する審議会を，指定情報処理機関には本人確認情報保護委員会を，それぞれ置かなければならない旨の定めがある（住基法３０条の９，３０条の１５）ほか，都道府県知事は，セキュリティ基準に基づき，本人確認情報の提供先である国の機関等に対して，本人確認情報の管理状況について報告を求め，適切に管理するよう要請することができ，市町村長も，都道府県知事を経由して報告を求めることができることとされており，本人確認情報の取扱いについては第三者機関や他の行政機関が監視の役割を担っている。

さらに，市町村が市町村独自サービスを提供する場合には，住基カードに格納された住民票コードにアクセスできない構造となっており，住基カードを使用することによって住民票コードを利用したデータマッチングが行われる危険性もない。

(イ) このように，関係法令の定め並びに住基ネット及び住基カードの仕組みに照らせば，原告らが懸念するようなデータマッチングが行われる具体的危険は全くないといえる。

(ウ) 原告らは，近年，各省庁における「最適化計画」の推進，霞が関ＷＡＮやＬＧＷＡＮの整備，ＡＰＩＳの導入，外国人のデータを一元管理するシステムの構築，納税者番号や社会保障番号の検討等が行われていることから，公権力が国民の情報を一元管理する体制が整いつつある旨主張するが，これらはいずれも住基ネットとは関係のない制度であり，その制度目的を超えて，いついかなる形で国民の情報の一元化につながるのか全く明らかになっていない。結局，現行制度の下でデータマッチングが行われる具体的危険があるとする原告らの主張は認められない。

オ まとめ

以上によれば，原告ら主張のプライバシー侵害を理由とする差止請求が認められる余地はない。

(2) 争点２について

（原告らの主張）

仮に，住基ネットの稼働，運用によって，原告らの自己情報コントロール権が侵害されたといえないとしても，住基ネットにはセキュリティ上の不備があり，また，その運用により，原告らの個人情報が漏えいする具体的危険があるから，予防的差止請求が認められるべきである。なお，住基ネットによる自己情報コントロール権侵害の危険性については，原告において一応の主張，立証（潜在的な危険の主張，立証）をしたときは，被告国において相

当の根拠を示して危険性のないことを具体的に主張，立証すべきであるところ，被告国はこれを行わないから，住基ネットによる自己情報コントロール権侵害の危険の存在が事実上推認される（最高裁判所平成４年１０月２９日第一小法廷判決・民集４６巻７号１１７４頁参照）。

（被告らの主張）

原告らの主張するような具体的危険は存在しない。したがって，仮に自己情報コントロール権に基づく予防的差止請求が認められるとしても，本件においてこのような差止請求を認める余地はない。

(3) 争点３について

（原告らの主張）

氏名で呼称され，氏名により他と識別され，取り扱われること（氏名権）は，人格権の一内容として，憲法１３条により保障される国民の権利である（最高裁判所昭和６３年２月１６日第三小法廷判決・民集４２巻２号２７頁参照）。住基ネットの導入に伴い，国民全員に対し，住民票コードが一方的に付され，個人情報は住民票コードのもとに処理されることになった。原告らに住民票コードを付すことは，原告らを氏名ではなく住民票コード（番号）で特定し，取り扱うことにほかならず，住基ネットの稼働，運用により原告らの氏名権は侵害されている。

（被告らの主張）

原告らが主張する，「氏名で扱われる」ことを内容とする「氏名権」を認める法文・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。住民票コードは，４情報を電子計算機及び電子通信回線を用いて効率的に送信させるために技術上設けられ，新たに住民票の記載事項とされた符号にすぎず，個人の人格的価値とは無関係である。したがって，原告らの住民票に住民票コードを記載して住基ネットを稼働，運用することにより，原告らの人格権が侵害されるものではない。

(4) 争点４について

（原告らの主張）

「公権力によって包括的に管理されない自由」とは，各行政機関が個別に保有する個人情報を結合していつでも利用できる状態に置かれることを拒絶する自由をいい，憲法１３条により保障されると解すべきである。そして，住基ネットの導入により，各行政機関が住民票コードを利用して個人情報の検索，照合等を行い，一元的に管理することが可能かつ容易になったこと，住基ネットの利用が可能な事務の範囲は拡大し続けていることからすると，住民票コードは，国家による国民の包括的な管理を実現する手段であるというほかなく，住基ネットの稼働，運用により，原告らの「公権力によって包括的に管理されない自由」が侵害されることは明らかである。

（被告らの主張）

原告らが主張する「公権力によって包括的に管理されない自由」を認める法文・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ことはできないし，行政機関が住民票コードを利用してその保有する個人情報につきデータマッチングをする具体的危険があるとはいえない。よって，住基ネットの稼働，運用により原告らの「公権力によって包括的に管理されない自由」が侵害されると解する余地はない。

(5) 争点５について

（原告らの主張）

被告国は，憲法１１条，１３条，９９条により，憲法を遵守し，国民の人権を保障する義務を負い，憲法に反する法律については，改廃や施行の延期等の手段を講じて国民の権利侵害を防止する義務を負う。ところが，内閣は上記義務を怠り，①改正法附則１条２項所定の「個人情報の保護に万全を期するための所要の措置」（以下「「所要の措置」という。）を講じず，また施行日までに講じることができる見込みがないのに，平成１３年１２月２８

日，改正法を平成１４年８月５日から施行する政令を定め，②施行日までに改正法の廃止等の措置を講じず，③改正法を施行し，また，内閣総理大臣及び総務大臣は，改正法の廃止又は住基ネットの運用停止等の方策を講じず，むしろその運用を積極的に推進した。

被告埼玉県及び埼玉県知事は，憲法１１条，１３条，９９条により，憲法を遵守し，県民の人権を保障する義務を負い，住基法上，「本人確認情報の適切な管理のために必要な措置」を講じる義務を負うにもかかわらず，これを怠り，①市町村の長に対し住民票コードを指定して通知し，②本人確認情報を磁気ディスクに記録して保存し，③国の機関等に対し本人確認情報を提供し，④被告財団法人に対し本人確認情報処理事務を委任し，⑤被告財団法人に対し本人確認情報を通知する等の行政事務を実施した。

被告財団法人は，指定情報処理機関として，被告埼玉県からの委任を受けて原告らの本人確認情報処理事務を行っている。

原告らは，被告らの上記行為により，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」を違法に侵害された。

（被告らの主張）

改正法は原告らの権利を何ら侵害するものではなく，違憲であるとはいえないから，改正法が違憲であることを前提とする原告らの主張は認められない。

国賠法１条１項の違法とは，公務員が個別の国民に対して負う職務上の法的義務に違背することをいい（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），また，公務員の行為は，当該公務員が職務上通常尽くすべき注意義務を尽くさず漫然と当該行為をしたと認め得るような事情がある場合に限り，同項にいう違法があったとの評価を受けるものというべきである（最高裁判所平成５年３月１１日第一小法廷判決・民集４７巻４号２８６３頁等）。そして，法令の違憲審査権は裁判所のみが有

するものである（憲法８１条）から，内閣及び地方公共団体の首長は，法律に従って適切に事務を行っている限り，国賠法１条１項にいう違法の評価を受けることはないというべきである。政府は，平成１３年３月に「個人情報の保護に関する法律案」を国会に提出して「所要の措置」を講じ，適法に改正法を施行しており，被告埼玉県の知事は，住基法に基づいて所定の事務を適法に行ったのであるから，被告国及び被告埼玉県の上記行為が国賠法１条１項にいう違法の評価を受けることはない。

被告財団法人は，住基法に基づいて総務大臣から指定情報処理機関としての指定を受け，埼玉県知事から委託されて住基法所定の事務を行うものであり，その事務の遂行についても何ら違法とはいえない。

(6) 争点６について

（原告らの主張）

原告らは，住基ネットが稼働した平成１４年８月５日以降，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」を侵害され続け，多大な精神的苦痛を被っている。原告らの精神的苦痛を慰謝するためには，原告らのそれぞれに対し，少なくとも，被告国において１０万円を，被告埼玉県及び被告財団法人において連帯して１０万円を，それぞれ負担させるのが相当である。

また，本件訴訟の弁護士費用のうち，少なくとも上記各請求額の１割に相当する額は，被告らの行為と相当因果関係のある損害であるから，原告らのそれぞれに対し，被告国において１万円を，被告埼玉県及び被告財団法人において連帯して１万円を，それぞれ負担させるのが相当である。

（被告らの主張）

原告らの主張は争う。

第３ 当裁判所の判断

１ 争点１（自己情報コントロール権の侵害を理由とする差止め）について

(1) 本人確認情報と法的保護

ア 前記第２の２(2)のとおり，住基ネットは，本人確認情報を一体のものとして全国的なコンピュータネットワーク上に流通させるシステムであり，これを稼働，運用させることにより，本人確認情報は，全国的なコンピュータネットワークの流通に置かれ，これを本人の居住する市町村以外の行政機関等が利用することが可能となる。そして，この本人確認情報の住民票コードを用いることにより，理論上，名寄せやデータマッチング（複数の個人情報ファイルに含まれる電子データを比較，検索及び結合すること）を行うことが可能となる。原告らは，上記のような住基ネットの稼働，運用によって，原告らの本人確認情報は，原告らの同意なく，原告らが居住する市町村以外の行政機関等に通知，提供することができる状態に置かれ，これにより，原告らの自己情報コントロール権は侵害されたとして，その妨害排除請求権に基づき，被告らに対し，住基ネット稼働，運用の差止めを求めているものである。そして，原告らは，この自己情報コントロール権について，憲法１３条によって認められるプライバシー権をより積極的なものとして発展させた権利であり，自己に関する個人情報の収集等について，自らの意思に基づいて決定することができる権利であると主張するものである。

イ なるほど，高度情報化社会の発展により，個人情報が私的にも公的にも利用される頻度が拡大している今日，個人情報保護の見地から，プライバシー権を発展させた形での自己情報コントロール権なるものを認める必要性が高くなっていることは当裁判所も否定するものではない。しかし，原告らのいう自己情報コントロール権なるものは，未だこれが認められる範囲，権利の内容等について不確定な要素が多く，これを直ちに憲法１３条に基づく権利として認めることは困難である。したがって，自己情報コントロール権の侵害を理由に，住基ネットの運用の差止めを求める原告らの

請求は理由がない。

もっとも，他人に知られたくないと感じる個人の私生活上の情報（プライバシーに係る情報）がみだりに開示されてはならないという人格的利益は，実定法上の明文の根拠がないとしても，法的保護に値し，これをみだりに開示することは，個人の人格的利益を違法に侵害したものとして，損害賠償の対象となり，しかも，その侵害が重大であり，それにより回復困難な損害が生じると認められるときは，侵害の差止めも認められるというべきである。

しかし，そもそもこのようなプライバシーに係る情報には様々なものがあり，当該情報の内容，侵害の態様等によって，保護の必要性も異なるものといえるから，どのような範囲の情報について，どのような行為がされたならば個人の人格的利益が侵害されたとみるかについては，個別に，情報の内容，侵害の態様，損害の性質等をみて判断すべきである。

ウ　そこで，これを本件で問題とされている本人確認情報についてみるに，本人確認情報は，個人の氏名，出生の年月日，男女の別，住所の４情報と，住民票コード及びこれらの変更情報であって，特にこれが一体のものとして第三者に開示されるときは，個人が特定され，その結果，個人の私生活上の平穏が害されるおそれが生ずるものであるから，上記のプライバシーに係る情報に当たり，法的保護に値するものというべきである。もっとも，本人確認情報それ自体は，個人の私生活や人格，思想，信条，良心等個人の内心に直接かかわる情報ではなく，秘匿されるべき必要性が必ずしも高いものではない。このことは，本人確認情報のうち４情報が，個人が社会生活を行う上での基本的な情報として，改正法施行前から住民に届出義務があるものとされ（住基法３条３項），住民基本台帳に記載されて原則として何人も閲覧可能な状態に置かれていたこと（住基法１１条。なお，「住民基本台帳法の一部を改正する法律」（平成１８年６月１５日法律第

７４号。同年１１月１日施行）１１条は，上記の閲覧制度を廃止したが，国又は地方公共団体の機関が，法令で定める事務の遂行のために閲覧する場合は，請求事由等を明らかにした上で，４情報の閲覧を請求できると定めている。）からも窺い知ることができる。また，４情報について，住基法１条が，「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や住民に関する記録の適正な管理を図り，もって住民の利便を増進するとともに，行政の合理化に資することを目的とする。」と定め，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，本人の同意なくこれを使用することが予定されていることも，このことを裏付けるものといえる。さらに，住民票コードは，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に無作為に作成された数字であり（住基法施行規則１条），それ自体から個人情報が推知されるものではないし，変更の請求も可能である（住基法３０条の３）。変更情報は，これらが変更した旨の客観的事実を表すものである（住基法施行令３０条の５）。

エ　このような本人確認情報の性質に照らすと，本人確認情報は，これを開示することが絶対に許されない性質の情報であると解することはできず，一定の制約の下にこれを利用し，開示することも許されるというべきである。そして，本人確認情報が，種々の行政事務を効率的に進めるための必要不可欠なものであり，しかもそれにより多大な社会的利益がもたらされるものであることに照らすと，たとえ行政機関が，これを本人の同意なくして他の行政機関等に開示したとしても，それが行政目的実現のため正当な目的に出たもので開示の必要性があり，しかも開示の手段として合理性があるときは，違法なプライバシー侵害には当たらないというべきである。

そこで，以下，住基ネットの稼働，運用が，正当な目的に出たものでそ

の必要性があるものか，そしてそれが行政目的達成の手段として合理性があるものであるかどうかについて，検討する。

(2) 住基ネットの目的と必要性

ア 前記第２の２の事実，証拠（当該認定箇所の末尾に掲記）及び弁論の全趣旨によれば，次の各事実が認められる。

(ア) 改正法の目的

住基法の改正が検討されていた平成８年ころ，コンピュータ技術の発展に伴い高度に情報化された社会状況を踏まえて，行政機関においても，民間部門と同様に情報通信技術を活用し，全国的な住民の移動や交流の実態に合わせて的確かつ効率的に行政サービスを提供すべく，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とされていた。改正法は，平成１１年，こうした状況を踏まえて，既に全国的に電算化が進んでいた住民基本台帳をネットワークで接続して全国的な本人確認システムを構築し，行政サービスの向上及び行政事務の効率化を図ることを目的として制定された。住基ネットは，このようにして構築された本人確認システムである。（乙３，乙４４）

(イ) 住基ネットの導入による行政事務の効率化

住基ネットの導入により，①パスポートの交付申請等，行政機関等への申請や届出を行う際，住民票の写しの提出が不要となり，②各種年金の受給に係る現況届や，恩給の受給に係る市町村長の証明印を受けた受給権調査申立書の提出が不要となり，かつ，支給の都度，本人確認ができるようになり，③住基カードの交付を受けている者は，住所地の市町村長以外の市町村長に対し，住民票の写しの交付を請求できるようになった（住基法１２条の２）。また，転入・転出の際に付記転出届を行った場合は，転入届の際，転出証明書を添付することが不要となる（住基法２４条の２）等，一定の行政事務の効率化が実現した。（乙９）

(ウ) 電子政府・電子自治体の実現及び公的個人認証サービスの創設

平成１２年７月に政府が設置したＩＴ戦略本部は，平成１３年１月，「我が国が５年以内に世界最先端のＩＴ国家となることを目指す」ことを内容とする「e-Japan戦略」を発表して電子政府の実現を重点政策分野の一つとし，これに基づく「e-Japan重点計画２００２」においても，電子政府・電子自治体の構築を最重要課題の一つとした。そして，平成１４年１２月６日，いわゆる行政手続オンライン化関係３法（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及びその施行に伴う関係法律の整備等に関する法律並びに電子署名に係る地方公共団体の認証業務に関する法律）が成立し，地方公共団体が電子署名の認証業務（電子証明書の発行）を行う公的個人認証サービス制度が創設され（その提供が開始されたのは平成１６年１月２９日である。），インターネットと電子署名を利用して行政機関への申請・届出等の手続を行うことが可能となった。住基ネットは，公的個人認証サービスにおいて電子証明書取得時の本人確認や，電子証明書の失効に係る情報の提供等のために用いられており（住基法３０条の８第３項，第４項，３０条の１１第９項），住基カードは，電子証明書及び秘密鍵を記録する媒体として用いられている（電子署名に係る地方公共団体の認証業務に関する法律３条４項，７項）。こうして，住基ネットは，行政手続のオンライン化及び電子政府・電子自治体の実現に不可欠の基盤であると位置付けられている。（甲１９４，乙５～１１，乙５１～５４，乙７６～７８）

イ 以上の事実によれば，住基ネットは，行政サービスの向上及び行政事務の効率化を図り，住民の便益を向上させるために構築されたものであり，電子政府実現の一翼をも担うものであって，その目的は正当ということができ，しかも，そのような行政目的実現のため，必要なシステムであるということができる。

ウ　原告らの主張に対する判断

(ア) 原告らは，住基ネットは費用対効果の面からみればむしろ非効率的であるし，その利用状況は低調であるから必要性がない，電子政府・電子自治体の実現は改正法の立法目的とはいえないなどと主張するので，この点について検討するに，証拠（当該認定箇所の末尾に掲記）及び弁論の全趣旨によれば，次の各事実が認められる。

a　平成１６年３月３１日現在の東京都の人口は１２０７万３７８５人であったのに対し，平成１５年８月２５日から平成１６年３月３１日までの間の東京都における住基カードの申請件数は約４万０７００件，住民票の広域交付件数（他区市町村住民への交付及び自住民の利用の合計）は約１万６０００件，付記転出届の件数は１０４件，最初の転入届の件数は１０３件であった。（甲２８，甲２９）

b　原告らが居住する埼玉県内の５市町において，平成１５年度から平成１７年度（平成１７年１２月まで）において発行された住基カードの枚数は，合計約１万枚であった。（甲１７６～甲１８０，調査嘱託の結果）

c　財務省が実施した平成１８年度予算執行調査において，インターネットを利用したパスポートの申請手続について，利用が低調であることや１件当たりの経費が高額過ぎることを理由に，これを見直すべきであると結論付けられた。利用率が低調な理由の一つとして住基カードの取得者数が未だに僅少であることが挙げられた。（甲２１２の１～４）

d　長野県本人確認情報保護審議会が，平成１８年３月，県内の８３市町村を対象に住基ネットに関するアンケートを実施したところ，過半数の自治体が住基ネットは費用対効果という観点からバランスを欠いているとの回答をした。（甲２０９）

(イ) これらの事情に照らせば，確かに住基ネットや住基カードの利用状況は，未だに低調であり，また，住基ネットを導入する費用に見合った効果が認められるかどうかについても不透明なところがあるといえる。しかしながら，住基ネットの規模やこれを利用した事務の内容に照らせば，住基ネットの利用状況や費用対効果については，全国的かつ長期的な観点から評価する必要があるといえるし，個別の事務ごとに運用方針を見直すことも可能であるといえる。そうすると，上記の各事情の存在は，住基ネット全体について，その目的の正当性及び必要性を否定するものではないというべきである。また，電子政府・電子自治体構想が改正法の直接の目的であったとはいえないとしても，行政サービスの向上及び行政事務の効率化という住基ネットの目的の正当性は左右されないし，差止請求の当否を判断する上で考慮すべき要素としての住基ネットの必要性については，口頭弁論終結時までの事情を考慮すべきであるところ，電子政府・電子自治体構想は，住基ネットの必要性を基礎付ける事情であると評価できる。したがって，原告らの上記主張は採用できない。

(3) 住基ネットの合理性

ア 住基ネットのセキュリティ対策について

(ア) 証拠（当該認定箇所の末尾に掲記）及び弁論の全趣旨によれば，住基ネットのセキュリティ対策等に関し，以下の事実が認められる。

a 住基法上のセキュリティ対策

住基法は，住基ネットのセキュリティ対策について，次の定めを置いている。

(a) 住基法上，都道府県及び指定情報処理機関が保有する情報は，本人確認情報に限定されている（住基法３０条の５第１項，３０条の１１第１項）。

(b) 本人確認情報の提供を受ける行政機関の範囲及び利用目的は，住

基法又は条例で規定され，限定されており（住基法３０条の6，３０条の７第３項～第６項，法３０条の８，別表），本人確認情報の提供を受けた受領者は，本人確認情報を目的外で利用又は提供してはならない（住基法３０条の３４）。また，都道府県知事及び指定情報処理機関は，法律の規定によらない本人確認情報の利用及び提供をしてはならない（住基法３０条の３０）。さらに，本人確認情報のうち，特に住民票コードについては，行政機関がみだりに住民票コードの告知を求めること及び住基法で定められた行政機関以外の者が住民票コードの告知を求めることは，いずれも禁止されている（住基法３０条の４２，３０条の４３第１項）。そのほか，市町村長等以外の者が，業として行う行為に関して契約の相手方に住民票コードの告知を求めることや，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も禁止されており（住基法３０条の４３第２項，第３項），都道府県知事は，これに違反する行為をした者に対し，中止の勧告及び命令をすることができ（住基法３０条の４３第４項，第５項），命令に違反した者には罰則が科される（住基法４４条，４８条）。

(c) 本人確認情報を取り扱う都道府県知事，指定情報処理機関，本人確認情報の提供を受けた受領者及びこれらから委託を受けた者並びに市町村長は，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（住基法３０条の２９，３０条の３３，３６条の２）。

(d) 住基ネットに係る事務に従事する者ないし関与した者に対しては，その事務に関して知り得た本人確認情報に関する秘密又は本人確認情報の電子計算機処理等に関する秘密を保持すべき義務が課され（住基法３０条の１７，３０条の３１，３０条の３５），これらに

違反した場合，罰則が科される（住基法４２条）。

(e) 都道府県に本人確認情報保護に関する審議会が，指定情報処理機関に本人確認情報保護委員会が，それぞれ設置されている（住基法３０条の９，３０条の１５）。指定情報処理機関の本人確認情報処理事務等の適正な実施を確保するため，総務大臣及び委任都道府県知事は，必要があると認めるときは，指定情報処理機関に対し，監督命令等を行い，報告を求め，立入検査を行うことができる（住基法３０条の２２，３０条の２３）。

(f) 住民は，自己の本人確認情報の開示及び訂正を請求することができる（住基法３０条の３７，３０条の４０）。また，市町村，都道府県知事及び指定情報処理機関は，本人確認情報処理事務等の実施に関して，住民の苦情の適切かつ迅速な処理に努めなければならない（住基法３０条の４１，３６条の３）。

b システム上のセキュリティ対策

住基ネットのセキュリティ確保のため，次のとおり，セキュリティ基準に様々な定めがあるほか，システム上も安全性確保のための対策が講じられている。（乙１，乙２の１及び２，乙１２，乙２８，乙３１）

(a) 外部からの物理的な侵入を防止するため，関係機関に対し，建物等への侵入の防止等，重要機能室（電子計算機室，磁気ディスク等保管室，受電設備，定電圧・定周波電源装置等の設備を設置する室等）の配置及び構造，入退室の管理，磁気ディスク，構成機器及び関連設備等，データ・プログラム・ドキュメント等の管理等に関して，セキュリティ基準所定の対策を講じることが義務付けられている。（セキュリティ基準第３－１，第４－１，第４－６～８）

(b) ＣＳ，都道府県サーバ及び指定情報処理機関サーバ間の通信は，

すべて専用回線及び専用交換装置で構成されたネットワークを介して行い，また，指定情報処理機関サーバと国の機関等のサーバとの間は，専用回線又は磁気媒体でデータ交換を行うものとされている。（セキュリティ基準第３－３，乙１２，乙４１の１及び２）

(c) 住基ネットによるデータ通信については，通信の都度，共通暗号鍵を設定し，さらに公開鍵方式による暗号化を行い，意図した通信相手に接続されたことの相互認証を行う仕組みが採用されている。（セキュリティ基準第４－３(4)，(5)，乙１２）

(d) すべてのＣＳのネットワーク側，すべての都道府県サーバのネットワーク側と端末機側（都道府県サーバと既存庁内ＬＡＮを接続しない団体を除く。），指定情報処理機関サーバの全方向及び国の機関等サーバ（指定情報処理機関サーバと接続しない国の機関等サーバを除く）のネットワーク側に，指定情報処理機関監視ＦＷを設置し，不正な通信を遮断するものとされている。また，市町村，都道府県及び国の機関等において，既存庁内ＬＡＮとサーバ（ＣＳ，都道府県サーバ，国の機関等サーバ）を接続する場合や，既存庁内ＬＡＮを外部ネットワークと接続する場合は，それぞれＦＷを設置し，外部からの不正な通信を遮断するものとされている。（セキュリティ基準第４－３(2)，第５－１(3)，(6)，乙１２）

(e) 住基ネットの通信プロトコルは，独自の住基ネットアプリケーションによる独自プロトコルであり，ＳＭＴＰ等の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。（乙１２）

(f) 端末機からサーバにアクセスする際には，常に操作者識別カード（操作者用ＩＣカード）と端末機との間で相互認証を行ってから住基ネットアプリケーションが起動する設計とされている上，操作者識別カードの種別によりデータ等へ接続できる範囲を限定している。

（セキュリティ基準第４－４，乙１２）

(g) 本人確認情報の検索における照会条件の限定により，無制限に本人確認情報を検索することを防止する措置がとられている。（セキュリティ基準第４－４(7)，乙１２）

(h) 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は，システム上，これを停止する措置が講じられている。（乙１２）

(i) 指定情報処理機関は，定期的にアクセスログを解析し，不正使用の兆候を検出した場合は，緊急時対応計画等に基づき，必要な連絡，対策等を実施するものとされている。（乙１２）

c 住基カードのセキュリティ対策

住基カードはＩＣカードであり，住基カードセキュリティ基準において，暗証番号の設定，住基ネットと住基カードの相互認証，アクセス権限の制御，アプリケーションごとの独立性の確保，耐タンパー性の確保等のセキュリティ対策がとられている。（乙１５，乙２８，乙３２）

d 地方公共団体におけるテスト結果等

(a) 被告財団法人は，平成１５年１０月１０日から１２日までの間，東京都品川区を対象として，住基ネットの主要な機器（ＣＳのネットワーク側のＦＷ，ＣＳと庁内ＬＡＮの間のＦＷ及び庁内ＬＡＮ上のＣＳ端末）に対する模擬攻撃を実施した。その結果，いずれの機器についてもシステム上の脆弱性は発見されなかった。（乙１４）

(b) 平成１５年及び平成１６年に，各市町村が，「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」を使ってセキュリティ対策の実施について自己点検を行った結果，一定程度の対策が講じられていることが確認された。ま

た，総務省及び指定情報処理機関は，これに基づき技術的助言，指導を行っている。（乙１３，乙４３）

(イ) 以上の事実によれば，住基ネットについては，本人確認情報の漏えい，改ざんを防止するために，制度上及びシステム上，相応の措置が講じられているというべきである。

(ウ) 原告らの主張に対する判断

原告らは，長野県の行った侵入実験の結果や自治体職員の不祥事の発生を挙げて，住基ネットのセキュリティ対策は不十分であり，原告らの個人情報が漏えい，改ざんされる具体的危険がある旨主張するので，この点について検討する。

ａ　長野県侵入実験について

証拠（甲１６の１及び2，甲１７，甲２３の１，甲２４の１，甲３０，甲３１，甲３２の１～４，甲３３の１～５，甲３４～甲４１，甲１５４，乙１７～２４，乙２９の１～８，乙５８，乙５９，乙６０の１及び２，乙６１の１及び２，乙６２，乙６３）及び弁論の全趣旨によれば，長野県は，インターネット側から市町村の庁内ネットワークを経由した住基ネットへの不正アクセス及び住基ネットからの本人確認情報漏えいの可能性を確認し，必要な対策を講じるための資料を得ることを目的として，県内の３町村を対象に，次のとおり調査を行ったことが認められる。

(a) 平成１５年９月２２日から同月２４日までの間，下伊那郡阿智村において，同村役場サーバ室内，隣接施設及び出先機関から庁内ＬＡＮに攻撃端末を接続し，既存住基サーバやＣＳの管理者権限を取得することを試みた結果，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，庁内ＬＡＮとＣＳとの間に設定されたＦＷに脆弱性は発見されず，ＣＳの管理者権限を取得することはできなかった。

(b) 平成１５年９月２５日及び同月２６日，諏訪郡下諏訪町において，調査用に構築した無線ＬＡＮを利用して，町役場に隣接する建物から庁内ＬＡＮに攻撃端末を接続し，既存住基サーバやＣＳの管理者権限を取得することを試みた結果，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，庁内ＬＡＮとＣＳとの間に設定されているＦＷに脆弱性は発見されず，ＣＳの管理者権限を取得することはできなかった。

(c) 平成１５年９月２９日から同年１０月１日までの間，東筑摩郡波田町を対象として，東京都内からインターネット経由で，ＦＷ及びＤＭＺ（インターネットに接続されたネットワークにおいて，ＦＷによってインターネットからも内部ネットワークからも隔離された区域）内に置かれた公開サーバ（誰でも接続することが可能な，インターネット一般に公開したサーバ）の情報を収集し，得られた情報をもとに公開サーバの権限取得を試みたが，実現することはできず，ＦＷを突破して庁内ＬＡＮに侵入することもできなかった。

(d) 平成１５年１１月２５日から同月２８日までの間，下伊那郡阿智村において，サーバ室内のラックを開錠の上，ＣＳセグメント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を試みた結果，ＣＳの管理者権限を取得することができ，これにより得られたユーザー情報（ＩＤとパスワード）を用いて，ＣＳ端末の管理者権限を取得することができた。

上記の実験結果は，何者かが住基ネットに不正に侵入する可能性が皆無とはいえないことを示すものであり，原告らに，住基ネットを通じて原告らの本人確認情報が漏えい，改ざんされるおそれがあるとの不安を抱かせるものであることは否定できない。しかしながら，上記実験によっても，①インターネット経由でＦＷ越しに公開サーバや庁

内ＬＡＮへ侵入すること，②庁内ＬＡＮからＦＷ越しにＣＳの管理者権限を取得すること，③ＣＳの管理者権限の取得を経ずにＣＳ端末の管理者権限を取得することにはいずれも成功していない。また，既存住基サーバやＣＳの管理者権限を取得できたのは，庁内ＬＡＮやＣＳセグメントに直接攻撃端末を接続した場合に限られ，しかも，これらの管理者権限を取得した後，実際に住基ネットアプリケーションを不正に操作するためには，正規の操作者が操作者識別カード及びパスワードにより住基ネットアプリケーションを起動させ，かつ不正操作を看過する等の条件が重なることを要するから，住基システムを不正に攻撃して原告らの本人確認情報を改ざん等することは通常困難である。そして，阿智村及び下諏訪町においては，既存住基サーバとＣＳは同期（複数のコンピュータ等の間で，保持している情報の内容を同一にすることを「同期を取る」という。）を取っていない（乙６０の２，乙６１の２）から，仮に，同町村の既存住基サーバ内の情報が改ざんされたとしても，それが直ちにＣＳに保存されている本人確認情報に反映されるものでもない。したがって，長野県侵入実験によって，原告らの本人確認情報が，漏えい，改ざんされる具体的危険があることが裏付けられたとはいえない。

b　住基ネット等に関する情報の取扱いをめぐる不祥事の発生について

証拠（当該認定箇所の末尾に掲記）及び弁論の全趣旨によれば，次の事実が認められる。

(a)　平成１８年３月，北海道斜里郡斜里町職員の自宅の私物パソコンがウイルスに感染し，パソコン内に保存されていた，住基ネットに関連する情報を含む業務資料が，ファイル交換ソフトWinnyのネットワーク上に流出したことが明らかになった。（甲１８１，甲１８２，甲１８８，甲１８９の１～４，乙１１２の１及び２，乙１１

3）

(b) 平成１５年８月２１日から平成１６年１月１３日までの間，北海道帯広市職員が，既存住基サーバと連携して宛名情報を提供するシステムにより表示された宛名情報（住所，氏名）を職務外で閲覧した。また，平成１７年6月１８日から同年１０月１２日までの間には，同市嘱託職員が，既存住基システムの端末を操作して，職務外で住民基本台帳を閲覧した。（甲１８３，甲１８８，甲１９０の１及び２，乙１１４）

(c) 平成１６年９月１３日，福島県東白川郡塙町で開催された会合において，住民票コードが記載された名簿が配布され，出席者の指摘を受けて，その場ですべて回収された。（甲８９，甲１８８，甲１９１の１及び２）

これらの事実から，原告らが，個人情報を扱う自治体の職員の情報管理に対する姿勢を問題視することも首肯できなくはない。しかしながら，上記(a)は，住基ネットではなく職員の私物パソコンから情報が流出したものであり，流出した住基ネット関連の情報の内容も，既に対応済みのセキュリティホール対策に関する通知及び現在使用されていないパスワードであったこと（乙１１２の１及び2，乙１１３），上記(b)は，住基ネットを操作して行われたものではないこと，上記(c)で配布された名簿はその場ですべて回収されたことからすると，これらの事情は，住基ネット自体のセキュリティに直接かかわるものであるとはいえない。

c　地方公共団体における住基ネットの運用の実態について

さらに，原告らは，地方自治体における住基ネットの管理，運用状況について，サーバの管理，端末の設置状況，操作者識別カード及びパスワードの管理等が適切でない旨指摘し，ＣＳ及びＣＳ端末へのパ

ッチ当ての遅れがみられることを問題視する。そして，証拠（甲１７６～甲１８０，調査嘱託の結果）及び弁論の全趣旨によれば，原告らの居住する市町についてみても，同一のパッチについて作業した時期が一律ではないこと，埼玉県狭山市においては，住基ネットの導入以来一度もパスワードの変更を行っていないことが認められ，各自治体におけるセキュリティ対策は，必ずしも完璧とはいえないことが窺われる。

しかしながら，上記(ｳ)ａの長野県侵入実験の結果に照らせば，住基システムを不正に攻撃して原告らの本人確認情報を改ざん等することは通常困難であること，住基ネットには専用回線が使用されており，直接インターネットと接続していないため，セキュリティパッチ当てについて通常のインターネット環境と同視することはできない（甲１００）ことからすると，上記の事情から直ちに住基ネット全体の安全性が左右されるものではないというべきである。

(ｴ) 以上のとおり，原告らの主張を検討しても，住基ネットのセキュリティに不備があるとまでは認められず，住基ネットを通じて原告らの本人確認情報が漏えい，改ざんされる具体的危険があるものとはいえない。

イ　住基ネットとデータマッチングについて

(ｱ) 前記のとおり，住民票コードそれ自体は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に無作為に作成された数字であり，それ自体から個人情報を推知されるものではない。しかしながら，住基ネットの稼働，運用により，すべての住民の本人確認情報がネットワーク上で一元的に保存，利用される環境が整ったのであり，住民票コードを「マスターキー」のように使用することにより，個々の行政機関が収集，保有している多数の個人情報について，無制限にデータマッチング（複数の個人情報ファイルに含まれる電子データを比較，検索及び結合

すること）を行う基盤が構築されたとみることもできる。そして，このようなデータマッチングにより，個人の健康状態等のいわゆるセンシティブ情報をも系統的，包括的に管理することが現実化すれば，本人確認情報というそれ自体は秘匿されるべき必要性が必ずしも高くない情報の管理を越えて，個人の人格的自律の基本にかかわる諸情報を行政機関が一元的に把握することが可能となり，個人の私生活に対する重大な脅威となりかねない。乙５１及び弁論の全趣旨によれば，住基カードを利用した市町村独自サービスとして，救急医療を受ける場合の本人情報の提供や診察券としての利用等が想定されており，技術的にもこのようなセンシティブ情報を含めた情報を包括的に管理することは不可能ではないと認められる。原告らも，このような事態が現実化することを危惧し，本件差止請求に及んだものと解される。

しかしながら，前記(2)アで認定したとおり，住基ネットの稼働，運用には，個人に関する多数の情報を整理して行政の一層の効率化を図るという効用があり，今後も，電子政府・電子自治体の基盤として住基ネットを有効に活用することが期待されている。しかも，弁論の全趣旨によれば，①改正法施行前も，行政機関は，行政事務の遂行に当たり，４情報を利用して本人確認（電子データを用いることはなかったにせよ，一種のデータマッチングということができる。）を行っていたこと，②住基ネットを利用して上記のような行政の効率化や電子政府・電子自治体の構築を実現するためには，行政機関が行政事務の遂行に必要な範囲内でデータマッチングを行うことは不可避であること，③データマッチングという概念自体多義的なものである上，行政機関の業務内容やその保有する個人情報にも様々なものがあり，データマッチングを行うことの功罪を一律に評価することは困難であることが認められる。そうすると，住民票コードを利用したデータマッチングを行うことが技術的に可能と

なったということ自体から，住基ネットに本質的欠陥があるとまではいうことはできず，住民票コードを利用して個人の人格的自律に著しい脅威となるようなデータマッチングが現実的に行われる体制となっているかどうかをさらに検討して，その是非を検討すべきである。

(イ) 前記第２の２の事実，証拠（当該認定箇所の末尾に掲記）及び弁論の全趣旨によれば，次の事実が認められる。

ａ 住基法上，本人確認情報の受領者は，住基法の定めにより本人確認情報の提供を求めることが認められた当該事務の遂行に必要な範囲内で，受領した本人確認情報を利用し，又は提供するものとし，当該事務の処理以外の目的のために受領した本人確認情報の全部又は一部を利用し，又は提供してはならない旨の定めがある（住基法３０条の３４）。

ｂ 行政機関個人情報保護法上，行政機関は利用目的の達成に必要な範囲を超えて個人情報を保有してはならず（同法３条２項），行政機関の長は，法令に基づく場合を除き，利用目的以外の目的のために保有個人情報を自ら利用し，又は提供してはならない（同法８条１項）旨の定めがある。そして，同法８条２項は，一定の要件を満たす場合に個人情報の目的外利用を許容するが，同条３項は，「前項の規定は，保有個人情報の利用又は提供を制限する他の法令の規定の適用を妨げるものではない。」旨定めており，上記ａの住基法３０条の３４は，「他の法令」に当たると解されるから，結局，行政機関個人情報保護法８条２項に優先して住基法３０条の３４が適用されることになる。

ｃ 行政機関の職員が上記ａ，ｂに違反して利用目的外で本人確認情報を利用してデータマッチングを行ったり，データマッチングや名寄せのために本人確認情報に関する秘密が記載された文書等を収集したり，本人確認情報に関する秘密を他の行政機関に漏らしたりした場合，懲

戒処分（国家公務員法８２条，地方公務員法２９条）や，罰則（住基法４２条，国家公務員法１０９条１２号，１００条１項，２項，地方公務員法６０条２号，３４条１項，２項，行政機関個人情報保護法５３～５５条）の適用があり得る。

d　都道府県には本人確認情報の保護に関する審議会を，指定情報処理機関には本人確認情報保護委員会を，それぞれ置かなければならない旨の定めがある（住基法３０条の９，３０条の１５）。

e　都道府県知事は（委任都道府県知事は指定情報処理機関を経由して），本人確認情報の提供先である国の機関等に対し，本人確認情報の管理状況について報告を求め，適切に管理するよう要請することができ，市町村長も，都道府県知事（指定情報処理機関が本人確認情報の提供を行った場合は，都道府県知事及び指定情報処理機関）を経由して報告を求めることができるとされている。（セキュリティ基準第６－8(1)，乙４２の２）

f　本人確認情報の提供が認められている事務は，平成１８年５月１５日現在で２９３事務あるが，現在，住民票コードを利用して各行政機関が保有する情報を統一的に収集し，管理するためのシステムは存在しない。（弁論の全趣旨）

g　住基カードは，その構造上，住基ネットサービスを利用するためのアプリケーションと市町村独自サービスを利用するためのアプリケーションとを独立して搭載し，利用する仕組みとなっているため，市町村がその独自サービスを提供する際は，住基ネットサービス利用エリアに格納された住民票コードにアクセスすることができない。したがって，市町村独自サービスの利用のために住基カードを利用することが住民票コードを利用したデータマッチングに直結するものではない。（乙２８，乙３２，乙５１）

h　都道府県知事は，国の機関等に対し本人確認情報の提供を行った場合又は本人確認情報を利用した場合は，個人ごとの本人確認情報の提供又は利用の状況に係る情報を保存しなければならず，委任都道府県知事は，指定情報処理機関に対し，本人確認情報の提供の状況について報告を求め，その情報を保存しなければならない。住民は，都道府県の個人情報保護条例に基づき，上記の情報の開示請求をすることができる。（セキュリティ基準第６－８(5)，甲２０，乙４２の１）

このような関係法令の定め並びに住基ネット及び住基カードの仕組みに照らせば，住基法の予定する目的の範囲内の利用に当たらない態様でデータマッチングが行われる具体的危険があるとまでは認められない。

(ウ)　原告らの主張に対する判断

a　原告らは，住民票コードを利用してデータマッチングをすることを明確に禁止する規定は存在しない旨論難する。しかしながら，上記(ア)で述べたとおり，行政機関は，その事務の遂行に当たり，改正法施行前から，市町村から提供を受けた４情報と自己の保有する個人情報を比較，照合して本人確認を行っていたところ，そのような意味でのデータマッチングを行う必要性は住基ネットの導入後も変わりはないのであるし，住基ネットの目的である行政の効率化を実現するためには，既存システムの統廃合や新たな行政サービスの創設をも伴うことが予想されるから，利用目的を問わず，あらゆる態様のデータマッチングを一律に禁止することは実体に則しない。

また，上記(イ)のとおり，住基法所定の利用目的以外でのデータマッチングが禁止されていることは，住基法３０条の３４の文言上明らかであり，その違反に対する罰則の定めも設けられているから，一定の抑止効果もあると認められる。また，本人確認情報の利用等の状況については，都道府県に置かれた本人確認情報保護審議会，指定情報処

理機関に置かれた本人確認情報保護委員会，都道府県知事，市町村長という複数の異なる機関が監視する体制がとられており，住民本人も自己の本人確認情報の利用又は提供について情報開示請求ができるのであるから，住基法所定の目的を超えてみだりに本人確認情報が流通することについても一定の防止策がとられているということができる。さらに，本人確認情報を利用できる事務は，法律又は条例の制定や改正を経て定められるものであるから，行政機関が恣意的かつ無制限にこれを拡大することは不可能である上，指定情報処理機関や国の機関等が国民の個人情報を一元的に管理することも予定されていない。

したがって，上記(イ)の諸規定は，利用目的外のデータマッチングを防止するための合理的な措置であると評価することができるから，原告らの主張は採用することができない。

b　また，原告らは，住民票コードを利用して国民の個人情報を一元的に管理するシステムは既に構築されつつある旨主張するので，この点について検討するに，証拠（当該認定箇所の末尾に掲記）及び弁論の全趣旨によれば，次の事実が認められる。

(a)　行政部門におけるＩＴ化推進の一環として，各府省等の間における情報の流通，共有等を図るため，各府省等のＬＡＮを相互に接続する政府内専用ネットワーク「霞が関ＷＡＮ」が，各地方公共団体の庁内ＬＡＮを相互に接続し，情報の共有等を図ることを目的とする行政専用のネットワーク「ＬＧＷＡＮ」が，それぞれ整備され，霞が関ＷＡＮとＬＧＷＡＮは，各府省等と地方公共団体との間における情報の伝達及び共有を円滑に行うため，相互に接続されている。（甲１９９，甲２１１の２）

(b)　政府は，平成１５年から，「電子政府構築計画」に基づき，業務・システムの「最適化計画」を策定し，ＩＴを活用した包括的な改

革を行っている。（甲１９６の２）

(c) 警察庁，法務省及び財務省は，平成１７年１月４日，入国管理局による上陸審査，税関による検査及び警察による国際組織犯罪やテロ等の取締りの効率化等を図るため，共同で，航空会社が搭乗手続時に取得した旅客等に関する情報（電子データ）の提供を受け，警察庁，法務省及び財務省の各省庁が保有するデータベースと自動的に照合するＡＰＩＳを導入した。（甲２０４）

(d) 平成１８年３月３１日付けで法務省情報化統括責任者が決定した「出入国管理業務の業務・システム最適化計画」において，「現在複数のシステムで分散管理されている外国人の入国・在留に関するデータを統合，また，関係行政機関などから提供される諸データを一元的に管理」する「インテリジェンスシステム」を導入する旨の記載があるが，政府は，その詳細やＡＰＩＳとの関係については，今後検討するとしている。（甲２０２の１，甲２１１の２）

(e) 昨今，政府の機関において，納税者番号制度や社会保障番号制度の導入が議論されている。（甲１３０，甲２０５）

原告らは，以上の事実を前提として，行政機関が無制限にデータマッチングを行う事態は現実の危険として今まさに進行しており，データマッチングの運用を厳格にチェックする第三者機関が必要である旨主張し，証人[redacted]は，陳述書（甲１８７）及び当裁判所において，これに沿う供述をする。しかしながら，上記の事情のうち，(b)及び(c)については，いずれも住基ネットとの関係が不明であり，(d)及び(e)は検討中の段階であって具体的内容が明らかではないから，現時点で，直ちに，住民票コードを用いて利用目的外のデータマッチングが行われる可能性があるものと評価することはできない。また，住基ネットについては，情報の保護の観点から，専用回線を使用することとされて

おり，霞が関WAN，LGWANを利用することは検討されていない（甲２１１の２）。証人[redacted]も，同証人のいうデータマッチングをどの行政機関がどのような方法で行いつつあるのかについて，必ずしも明確に述べているものではなく，同証人の供述を総合しても，個人の私生活に重大な脅威をもたらすようなデータマッチングの体制が整備されつつあるという現実の可能性を認定することはできない。

c　以上を要するに，住基ネットをデータマッチングの基盤として利用することは可能であるとしても，現時点において，特定の行政機関が国民の多数の個人情報を一元的に管理するために住民票コードを利用する現実的可能性があるとはいえないから，住民票コードを利用して，個人の私生活に著しい脅威となるようなデータマッチングを行う体制が現に構築されているものではないというべきである。

したがって，原告らの主張はいずれも採用することができない。

(ｴ) なお，以上認定した住基ネットの仕組み及び弁論の全趣旨によれば，住民の一部にでも住基ネットを利用しない者があれば，住基ネットによる事務処理体制と既存のそれを併存させた上で，個々の事務について，その対象となる住民が住基ネットを利用する者であるか否かの確認を経る作業が必要となることが認められる。その場合は，住基ネットの目的である住民基本台帳を統一のネットワークで接続することによって得られる行政事務の効率化を大きく損なうことになることが容易に推認できるから，上記の目的を達成するためには，原則としてすべての住民について住基ネットが運用されることを要するというべきである。

(4) 住基ネットの違法性について（まとめ）

以上(2)，(3)において検討したところによれば，住基ネットには正当な目的及び必要性があり，行政目的達成のための手段としても合理性があるといえるから，被告らが住基ネットを稼働，運用したことが，原告らのプライバシ

ーを違法に侵害したことには当たらないというべきである。したがって，上記侵害を理由とする原告らの差止請求は理由がない。

2　争点２（自己情報コントロール権侵害の具体的危険を理由とする差止め）について

原告らは，住基ネットにおいて，セキュリティ対策の不備により外部の第三者に本人確認情報が漏えい等する危険を重視し，セキュリティ上の危険性を理由とする差止請求が認められるべきであると主張する。これは，原告らの本人確認情報に係る人格的利益の侵害が現に存在しないとしても，その危険性があるとして，予防的な差止請求を認めるべきであるとするものである。

なるほど，このような予防的差止請求も一定の場合には認められる余地があるといえるが，前記１(1)のような本人確認情報の性質や前記１(2)認定の住基ネットの必要性等に照らすと，このような差止請求が認められるためには，少なくとも，①原告らの本人確認情報に係る人格的利益が侵害される具体的な危険の存在すること，及び②差止めが認められなければ原告らが回復困難な損害を被るおそれがあることを要するものと解すべきである。そして，この①，②の要件は，予防的差止請求の請求原因であるから，これを基礎付ける事実については原告らにおいてこれを主張立証する責任があるというべきである。

そこで，これを本件についてみると，前記１(3)で検討したとおり，本件全証拠によっても，住基ネットの稼働，運用により，原告らの本人確認情報が第三者に漏えい等する具体的危険性までは認めることができない。したがって，その余の点について判断するまでもなく，上記予防的差止請求もまた，理由がない。

3　争点３（氏名権に基づく差止め）について

原告らは，憲法１３条により，氏名で呼称され，氏名により他と識別され，取り扱われることを内容とする「氏名権」が保障されているところ，原告らは，住基ネットの導入により，住民票コードで取り扱われるようになり，氏名権を

侵害された旨主張する。

しかしながら，原告らが主張するような憲法１３条に基づく人格権の一内容としての「氏名権」はこれを認めることはできない。もっとも，氏名は，その個人の人格の象徴であり，人格権の一内容を構成するものというべきであるから，氏名を正確に呼称される利益は，法的保護に値する人格的利益であるということができ，これを違法に侵害されたときは，その侵害の態様，違法性の程度等によっては侵害行為の差止めを求めることができる場合もあり得ると解すべきである（最高裁判所昭和６３年２月１６日第三小法廷判決・民集４２巻２号２７頁，最高裁判所平成１８年１月２０日第二小法廷判決・裁判所時報１４０４号１１頁参照）。

そこで，この観点から本件について検討するに，弁論の全趣旨によれば，住民票コードは，電子通信回線を用いて４情報を効率的に送信するために無作為に作成された符号であり，一度住民票に記載された住民票コードは，本人の請求により変更することができること（住基法３０条の３）が認められるから，住民票コードは，行政事務の遂行上，氏名に代わる機能を果たすものではないということができる。したがって，住基ネットの稼働，運用に当たり，住民票コードのような符号を用いることによって，個人の人格の象徴である当該個人の氏名の重要性が損なわれるものではない。そうすると，原告らの住民票に住民票コードが記載されたことによって，原告らの氏名を正確に呼称される利益が違法に侵害されたと認めることもできないし，それに基づく差止めも認めることができない。

したがって，原告ら主張の「氏名権」に基づく差止請求も理由がない。

４　争点４（「公権力によって包括的に管理されない自由」に基づく差止め）について

原告らは，憲法１３条により，「公権力によって包括的に管理されない自由」が保障されているところ，原告らに住民票コードを付した上で原告らの本

人確認情報を流通させることは，国家による国民の包括的な管理につながるものであるから，上記の自由の侵害に当たる旨主張する。

しかしながら，原告らの主張する上記の自由が，法的に保護される利益であるかどうかはともかくとして，前記認定判断のとおり，住基ネットは，行政機関が国民を包括的に管理することを目的とするものではなく，住民票コードを利用した包括的なデータマッチングが行われる具体的な危険性があるとまではいえないから，原告らの住民票に住民票コードを記載して住基ネットを稼働，運用することによって，原告らが主張する上記の自由が侵害されたものとはいえないし，その危険があるとも認められない。

したがって，原告ら主張の「公権力によって包括的に管理されない自由」に基づく差止請求も理由がない。

5　争点5（損害賠償請求）について

原告らは，内閣が「所要の措置」を講じることなく改正法を施行した行為や，被告らが，改正法所定の事務を行った行為は，国賠法上あるいは不法行為法上違法である旨主張する。

しかしながら，前示のとおり，改正法の制定・施行や住基ネットの稼働，運用により，原告らの権利ないし利益が違法に侵害されたとは認められず，改正法が違憲であるとは認められない。したがって，被告らが改正法所定の事務を実施して住基ネットを稼働し，運用する行為は，いずれも適法なものであって，国賠法上あるいは不法行為法上の違法な行為に当たるとすることはできない。

なお，改正法附則1条1項及び同条第2項の定めによれば，政府は，「所要の措置」を講じたか否かにかかわらず，改正法公布の日から3年以内に改正法を施行することが義務付けられていたと解されるところ，政府は，改正法附則1条1項に従って政令で改正法の施行日を定め，改正法を施行したものであり，この点についても国賠法上の違法な行為であるとはいえない。

以上によれば，原告らの被告らに対する損害賠償請求は，その余について判断

するまでもなく理由がない。

6　結論

よって，原告らの本訴請求は理由がないからこれをいずれも棄却することとし，訴訟費用の負担につき民訴法６１条，６５条１項本文を適用して，主文のとおり判決する。

さいたま地方裁判所第６民事部

裁判長裁判官　近　藤　壽　邦

裁判官　太　田　晃　詳

裁判官　板　橋　愛　子