平成１８年１０月２６日判決言渡　同日原本領収　裁判所書記官　福嶋聡禮

平成１４年(ワ)第４１２９号　住民基本台帳ネットワーク差止等請求事件（甲事件）

平成１５年(ワ)第１１５８号　住民基本台帳ネットワーク差止等請求事件（乙事件）

口頭弁論終結日　平成１８年７月２０日

判　　決

当事者の表示　　別紙当事者目録記載のとおり

主　　文

1　原告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　被告県は，

(1)　住民基本台帳法（平成１８年法律第８３号による改正後の住民基本台帳法。以下「住基法」という。）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（以下「住基法上の国の機関等」という。）に対し，原告らの氏名，住所，生年月日，性別，住民票コード及びこれらの変更情報（以下「本人確認情報」という。）を提供してはならない。

(2)　被告センターに対し，原告らに関する住基法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)　被告センターに対し，原告らの本人確認情報を通知してはならない。

(4)　住民基本台帳ネットワーク（以下「住基ネット」という。）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。）から原告らの本人確認情報を削除せよ。

2　被告センターは，

(1)　被告県から受任した原告らに関する住基法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) 住基ネットの磁気ディスクから原告らの本人確認情報を削除せよ。

3 被告県及び被告センターは，原告らに対し，連帯して，各１１万円及びこれに対する甲事件原告らにつき平成１４年１１月１２日（甲事件訴状送達の日の翌日）から，乙事件原告らにつき平成１５年４月２５日（乙事件訴状送達の日の翌日）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１４年１１月１２日（甲事件訴状送達の日の翌日）から，乙事件原告らにつき平成１５年４月２５日（乙事件訴状送達の日の翌日）から各支払済みまで年５分の割合による金員を支払え。

第２ 事案の概要

本件は，神奈川県内に居住する原告らが，住基ネットの運用により原告らのプライバシー権等の人格権が侵害されているなどと主張して，被告県及び被告センターに対し，上記人格権に基づき，原告らに関する住基ネットの運用の差止め及び住基ネット上の磁気ディスクに保存された原告らの本人確認情報の削除を求める（以下，上記差止請求及び上記削除請求を併せて「本件差止請求等」という。）とともに，被告国及び被告県に対し，国家賠償法１条１項に基づき，被告センターに対し，不法行為に基づき，連帯して，損害賠償金各１１万円及びこれらに対する訴状送達の日の翌日から支払済みまで年５分の割合による遅延損害金の支払を求めた事案である。

1 前提事実（当事者間に争いがないか，又は後掲証拠により容易に認定できる事実。以下の証拠番号は注記しない限り，甲事件の番号による。）

(1) 当事者

ア 原告[redacted]は，神奈川県藤沢市に，原告[redacted]，原告[redacted]，原告[redacted]，原告[redacted]及び原告[redacted]は，横浜市に，原告[redacted]は，神奈川県鎌倉市に，原告[redacted]及び原告[redacted]は川崎市に，原告[redacted]は神奈川県平塚市にそれぞれ居住し，住民登録をしている者であ

る（甲１の②から⑥，乙事件甲１の①，③，④。以下，横浜市に居住する原告らを総称して「横浜市に居住する原告ら」という。）。

イ　被告センターは，昭和４５年５月１日に設立され，国と地方公共団体との間における情報処理システムの調整に関する調査，研究等の事業を行う財団法人である。被告センターは，住基法３０条の１０に基づき，総務大臣から指定情報処理機関として指定され，被告県知事から委任を受けて，住基法３０条の１０第１項記載の本人確認情報処理事務を行っている。

(2)　住基法

ア　住基法の目的

住基法は，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住民基本台帳の制度を定め，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して制定され（１条），昭和４２年１１月１０日から施行された法律である。

イ　住民基本台帳

市町村長は，住基法に基づき，個人を単位とする住民票を世帯ごとに編成して，住民基本台帳を作成することを義務付けられている（住基法６条１項）。

住民票には，①氏名，②生年月日，③性別，④世帯主についてはその旨，世帯主でない者については世帯主の氏名及び世帯主との続柄，⑤戸籍の表示，ただし，本籍のない者及び本籍の明らかでない者については，その旨，⑥住民となった年月日，⑦住所及び一の市町村の区域内において新たに住所を変更した者については，その住所を定めた年月日等について記載をする（住基法７条）。

(3) 住基ネットの概要

ア　住基ネットの導入

平成１１年，住民基本台帳法が一部改正され（平成１１年法律第１３３号。以下この改正を「平成１１年改正」といい，平成１１年改正により改正された住民基本台帳法を「平成１１年改正住基法」という。），住基ネットが導入された。

住基ネットは，市町村長，都道府県知事，指定情報処理機関等がそれぞれ設置した住基ネット専用の電子計算機（以下，市町村長が設置した電子計算機をコミュニケーションサーバ，略して「ＣＳ」，都道府県知事が設置した電子計算機を「都道府県サーバ」，指定情報処理機関が設置した電子計算機を「指定情報処理機関サーバ」という。）等から成る住民基本台帳ネットワークシステムを用いて，専用の電気通信回線を通じて，市町村長においては都道府県知事に本人確認情報を通知し，都道府県知事及び指定情報処理機関においては本人確認情報の記録，保存及び提供等を行うシステムである（乙１）。

イ　住民票コード

(ア) 住民票コードの内容

平成１１年改正により，住民票には，無作為に作成された１０けたの数字と１けたの検査数字の組み合わせから成る住民票コードを記載することとされた（住基法７条１３号，３０条の２，住民基本台帳法施行規則〔以下「施行規則」という。〕１条）。

(イ) 都道府県知事による指定

都道府県知事は，他の都道府県知事と協議し，住民票コードが重複しないよう調整を図り，当該都道府県の区域内の市町村ごとに，当該市町村長が住民票に記載することのできる住民票コードを指定し，当該市町村長に通知する（住基法３０条の７第１，２項）。

(ウ) 指定情報処理機関への委任

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，前記(イ)の事務を行わせることができる（住基法３０条の１０第１項１，２号）。

(エ) 市町村長による住民票コードの記載及び住民への通知

市町村長は，住民基本台帳に記録されたことがない者につき，新たに住民票に記載をする場合，都道府県知事から指定された住民票コードのうちいずれか一を選択してこれを住民票に記載し，速やかに，当該記載に係る者に対し，その旨及び当該住民票コードを書面により通知する（住基法３０条の２第２項，３項，平成１１年改正住基法附則３から５条）。

市町村長は，新たに住民票に住民票コードを記載する場合を除いて，住民票には直近に記載された住民票コードを記載する（住基法３０条の２第１項）。

(オ) 住民票コードの変更請求

住民基本台帳に記録されている者は，市町村長に対し，住民票コードの記載の変更を請求することができる（住基法３０条の３第１項）。

ウ 本人確認情報

(ア) 本人確認情報の内容

住基法上における本人確認情報とは，住民票に記載されている①氏名，②生年月日，③性別，④住所，⑤住民票コード，⑥政令で定める事項をいう（住基法３０条の５第１項，７条１号から３号，７号及び１３号。以下，①氏名，②生年月日，③性別，④住所を総称して「基本４情報」という。）。政令で定める事項としては，①住民票の記載を行った場合は，住民票の記載を行った旨並びに転入その他の総務省令で定める記載の事由及びその事由が生じた年月日，②住民票の削除を行った場合は，住民票の削除を行った旨並びに転出その他の総務省令で定める消除の事

由及びその事由が生じた年月日，③基本４情報の全部又は一部についての記載の修正を行った場合は，住民票の記載の修正を行った旨並びに転居その他の総務省令で定める記載の修正の事由及びその事由が生じた年月日，④住民票コードについて記載の修正を行った場合は，住民票の記載の修正を行った旨，総務省令で定める記載の修正の事由及びその事由が生じた年月日並びに当該住民票の記載の修正前に記載されていた住民票コードと規定されている（住民基本台帳法施行令〔以下「施行令」という。〕３０条の５。以下，これらを総称して「変更情報」という。）。

(イ) 本人確認情報の通知

a　市町村長から都道府県知事への通知

市町村長は，住民票の記載等を行った場合，本人確認情報を都道府県知事に通知する（住基法３０条の５第１項）。

b　都道府県知事から指定情報処理機関への通知

指定情報処理機関に本人確認情報に関する事務処理を委任した都道府県知事（以下「委任都道府県知事」という。）は，市町村長から通知を受けた本人確認情報を指定情報処理機関に通知する（住基法３０条の１１第１項）。

(ウ) 本人確認情報の保存

a　都道府県知事による保存

本人確認情報の通知を受けた都道府県知事は，当該本人確認情報を磁気ディスクに記録，保存し，情報の内容変更後も，原則として５年間は変更前の情報を保存する（住基法３０条の５第３項，施行令３０条の６第１号）。

b　指定情報処理機関による保存

委任都道府県知事から通知を受けた指定情報処理機関は，前記ａと同様に本人確認情報を記録及び保存する（住基法３０条の１１第３項，

施行令３０条の１１）。

(エ) 本人確認情報の提供

a　市町村長から他の市町村長等への提供

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（住基法３０条の６）。

b　都道府県知事から住基法上の国の機関等への提供

都道府県知事は，住基法上の国の機関等から，住基法別表第一下欄に掲げる事務処理に関し，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）。

c　都道府県知事から当該都道府県の区域内の市町村長等への提供

都道府県知事は，政令又は条例で定めるところにより，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から住基法又は条例で定められた事務処理等に関し求めがあったとき，当該市町村長等に対し，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）。

d　都道府県知事から他の都道府県知事等への提供

都道府県知事は，政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から住基法等の法令で定められた事務処理等に関し求めがあったとき，当該都道府県知事等に対し，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）。

e　都道府県知事から他の都道府県の区域内の市町村長等への提供

都道府県知事は，政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から住基法等の法令

で定められた事務処理等に関し求めがあったとき，当該市町村長等に対し，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）。

f　都道府県知事から指定情報処理機関への委任

都道府県知事は，指定情報処理機関に，前記ｂからｅまでの事務等を行わせることができる（住基法３０条の１０第１項３から６号）。

(オ)　本人確認情報の通知及び提供の方法

a　市町村長から都道府県知事への通知

市町村長は，ＣＳから電気通信回線を通じて，都道府県サーバに本人確認情報のデータを送信する方法で通知する（住基法３０条の５第２項）。

b　都道府県知事から他の都道府県知事への提供

都道府県知事は，都道府県サーバから電気通信回線を通じて，相手方の都道府県サーバにデータを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で提供する（住基法３０条の７第７項，施行令３０条の９）。

c　都道府県知事から住基法上の国の機関への提供

都道府県知事は，都道府県サーバから電気通信回線を通じて，住基法上の国の機関等の電子計算機（以下「国の機関等サーバ」という。）にデータを送信する方法又は磁気ディスクを送付する方法で提供する（施行令３０条の７）。

d　都道府県知事から当該都道府県の区域内の市町村長等への提供

都道府県知事は，都道府県サーバから電気通信回線を通じて，相手方のＣＳにデータを送信する方法又は磁気ディスクを送付する方法で提供する（施行令３０条の８）。

e　委任都道府県知事から指定情報処理機関への通知

委任都道府県知事は，都道府県サーバから電気通信回線を通じて，指定情報処理機関サーバにデータを送信する方法で通知する（住基法３０条の１１第２項）。

ｆ　指定情報処理機関から他の都道府県知事への提供

指定情報処理機関は，指定情報処理機関サーバから電気通信回線を通じて，相手方の都道府県サーバへデータを送信する方法で提供する（住基法３０条の１１第４項）。

(カ)　本人確認情報の利用

都道府県知事は，住基法で定められた事務並びに条例で定められた事務及び利用につき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（住基法３０条の８第１項）。

エ　住民基本台帳カード

(ア)　住民基本台帳カードの交付

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に対し，自己に係る住民基本台帳カード（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たカードをいう。以下これを「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）。

(イ)　住基カード所持者の届出の特例

住基カード所持者が，付記転出届をした場合においては，転入届を提出する際，転出証明書を添える必要がない（住基法２４条の２第１項，施行令２３条）。転入地の市町村長は，転入届を受けた旨を転出地の市町村長に通知し，通知を受けた転出地市町村長は，氏名，生年月日，性別，住所等を転入地市町村長に通知する（住基法２４条の２第３，４項，施行令２４条の４）。これらの通知は，転入地ＣＳ又は転出地ＣＳから

電機通信回線を通じて，相手方である転出地ＣＳ又は転入地ＣＳにデータを送信する方法で行う（住基法２４条の２第５項）。

オ　住民票の広域交付

住民基本台帳に記録されている者は，住基カード又は所定の書類を提示することにより，住所地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の交付を請求することができる（住基法１２条の２第１項）。

前記住民票の請求を受けた市町村長は，請求者の住所地の市町村長に対し，交付請求があった旨等を通知し，住所地の市町村長から住民票に記載すべき情報をＣＳを通じて受信し，住民票を作成して，請求者に交付する（住基法１２条の２第２から５項，施行令１５条の２）。

(4)　住基ネット関連の法律の施行及び住基ネットの稼働状況（乙２９）

平成１１年１０月１日，平成１１年改正住基法のうち，指定情報処理機関の指定，住民票コードの指定等に関する規定が施行された（平成１１年改正住基法附則１条１項２号，平成１１年９月政令３０２号）。

平成１４年８月５日，平成１１年改正住基法のうち，住民票コードの記載，本人確認情報の通知，提供等に関する規定が施行され（平成１１年改正住基法附則１条１項本文，平成１３年１２月政令４３０号），市町村長は，当該都道府県知事に対し，住民の本人確認情報の通知を開始した（以下，上記施行による住基ネットの稼働を「住基ネット第一次稼働」という。）。

平成１４年１２月１３日，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，電子署名に係る地方公共団体の認証業務に関する法律（以下，これら３法を総称して，「行政手続オンライン化３法」という。）が成立した。

平成１５年５月３０日，個人情報の保護に関する法律（以下「個人情報保

護法」という。〕，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。），独立行政法人等の保有する個人情報の保護に関する法律，情報公開・個人情報保護審査会設置法，行政機関の保有する個人情報保護法の施行に伴う関係法律の整備等に関する法律（以下，これら５法を総称して，「個人情報保護関連５法」という。）が成立した。

平成１５年８月２５日，平成１１年改正住基法のうち，住基カード等に関する規定が施行された（平成１１年改正住基法附則１条１項３号，平成１５年１月政令２０号。以下，上記施行による住基ネットの稼働を「住基ネット第二次稼働」という。）。

(5) 本人確認情報の提供が可能な事務

本人確認情報の提供が可能な事務は，当初，９３事務であったが，平成１７年４月１日現在，２７５事務に拡大されている。

(6) 横浜市の対応

ア 横浜市は，住基ネット第一次稼働前の準備段階において，被告県知事に本人確認情報を通知したが，住基ネット第一次稼働後はＣＳの接続を行わなかった（乙２）。横浜市では，横浜市民に対し，横浜市から被告県等への本人確認情報の通知を希望しないことを申し出る機会を与えたところ，約８４万人の市民が非通知の申出をした（甲４９。以下，非通知の申出をした者を「非通知希望者」という。）。横浜市は，非通知の申出をしなかった者（以下「通知希望者」という。）についても，住基ネットの運用を行っていなかったが，総務省との間で，平成１５年４月９日，順次，通知希望者の更新データ及び非通知希望者の更新されていない旨のデータを送信し，通知希望者については，住基ネットの運用を可能とする旨の合意をした（乙２）。

イ 横浜市に居住する原告らの本人確認情報の取扱い

横浜市に居住する原告らは，横浜市に対し，それぞれ「非通知の申出」

を行った。それを受け，横浜市は，住基ネット第一次稼働後，原告らの本人確認情報を通知していないが，準備段階において通知した情報は，被告県及び被告センターが消除せずに保存している。

2　主たる争点

(1)　差止請求等の可否

ア　プライバシー権としての自己情報をコントロールする権利（以下「自己情報コントロール権」という。なお，自己情報コントロール権の内容に関する当裁判所の見解は後記第４，１，(1)のとおりである。）に基づく差止請求等の可否

イ　氏名権に基づく差止請求等の可否

ウ　公権力による包括的管理からの自由権に基づく差止請求等の可否

(2)　損害賠償請求の可否

第３　主たる争点に対する当事者の主張

1　争点(1)ア（プライバシー権としての自己情報コントロール権に基づく差止請求の可否）について

【原告らの主張】

(1)　差止めの要件

当該行為等の差止めが許容されるためには，①差止めの根拠となり得る排他的権利があり，②その排他的権利が侵害される危険性があれば足りる。また，本件の請求が住基ネットからの個別の離脱請求であることからすれば，差止めを認めることにより生ずる支障の程度は低いといえるので，②の侵害の危険性が高度である必要はない。被告らは，①及び②の要件に加え，③その権利侵害の程度が重大であり，権利者が著しく回復困難な損害を被るおそれがあることが必要であると主張するが，自己情報コントロール権は憲法１３条により保障された重要な権利であり，公権力による侵害が問題となっていることからすれば，③の要件は不要である。

もっとも，自己情報コントロール権も無制限に保護されるわけではなく，公共の福祉のため必要がある場合には相当の制限を受ける余地がある。しかし，自己情報コントロール権の制限の許否については，自己情報コントロール権の重要性や，いったん侵害された場合には回復が不可能な権利であるという性格からすれば，安易な比較衡量ではなく，厳格な審査を行うべきである。具体的には，最高裁平成１４年(受)第１６５６号平成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年最判」という。）で示された基準のとおり，原則として，個人情報の取扱いには，個人の同意・承諾が必要であり，同意・承諾が存しない場合には，例外の要件（同意・承諾を得ることが不可能，困難であったという緊急性の要件の存否，「やむにやまれぬ利益」〔必要不可欠な利益〕の存否，その場合の手段の相当性，より制限的でない他に選び得る手段の存否）について厳格に判断すべきである。

(2) プライバシー権としての自己情報コントロール権に基づく本人確認情報の保護

ア　プライバシー権としての自己情報コントロール権の保障

プライバシー権は，私人間における不法行為上の概念として，私事の公開や私生活への侵入を拒絶する権利ととらえるだけでは不十分であり，全体主義の経験をその成立の歴史的背景とし，近代立憲主義そのものをその成立の根源的基礎とする極めて重要な公法上の権利として，憲法１３条によって保障されているというべきである。

とりわけ，今日のコンピュータ技術の進展に伴う高度に発達した情報化社会においては，自己に関する情報の他者への開示，利用及び提供の可否を自分で決める権利，すなわち自己情報をコントロールする権利を認める必要があり，プライバシーの権利には，この自己情報コントロール権が重要な一内容として含まれると解すべきである。自己情報コントロール権は，

具体的には，情報主体が，①自己に関する情報の収集・取得，②その保有・利用，③その開示・提供をコントロールする権利をいい，更に派生的には，④自己の情報の開示請求権，訂正請求権が含まれる。

イ　プライバシー権の保護の対象としての本人確認情報

(ア)　基本４情報について

基本４情報は，個人識別のため，最も基本的かつ不可欠な情報である。そして，基本４情報は，それ自体が重要な情報であるというだけでなく，付加して記録及び保存されている「個人情報」総体の索引・検索情報として意義を有するものである。

被告らは，住基法上，氏名，生年月日，性別，住所といった情報は従来から公開の対象とされてきたことから，基本４情報は秘匿性，要保護性が低いと主張するが，基本４情報は，住民票コード，変更履歴と一体となり，「個人情報」総体の索引・検索情報として意義を有するものであり，従前から住基法上，公開されてきた氏名，住所，生年月日及び性別とは性質が異なるものであるから，これを同一に論ずることは誤りであるし，現在，この住基法上の公開規定は見直しが進められているのであるから，被告らの主張は不合理である。

(イ)　住民票コードについて

住民票コードは，１１けたという長大なけた数を用いて国民一人一人に対して重複しないように付されている国民各個人の固有の番号であるとともに，各行政事務ごとの垣根を取り払って用いられる「共通番号」でもある。

そして，住民票コードが付されたデータベースが作成された場合，住民票コードは，特定の個人情報について，正確無比かつ簡便に検索や名寄せやデータマッチングを行うことのできる「マスターキー」となり得るものである。

したがって，住民票コードが，秘匿，保護する必要性が極めて高度な情報であることは疑いのないものである。

(ウ) 変更情報について

変更情報とは，異動事由（「転入」，「出生」，「職権記載等」，「転出」，「死亡」，「職権消除等」，「転居」，「職権修正等」，「住民票コードの記載の変更請求」，「住民票コードの職権記載等」のいずれかの記載がされる。），異動年月日及び異動前の本人確認情報をいう。住所に関わる変更は「転入」，「転出」，「転居」として扱われ，生年月日に関わる変更は「出生」等として扱われ，住民票コードの変更については，「住民票コードの記載の変更請求」等として扱われるから，氏名又は性別に関わる変更のみが「職権修正等」として扱われることになる。

したがって，「職権修正等」は，それが氏名又は性別に関わる変更などの身分上の重要な変動が生じたことを推知させることになる。

したがって，変更情報も秘匿性が高く，重要な情報であることは明らかである。

(エ) 情報の一体性

住基ネットにおいて，本人確認情報が基本的には一体となって流通し，ネットワーク上で共有されているということは，本人確認情報の要保護性の程度を判断する上で重要なことである。ひとかたまりとしての本人確認情報の方が，個々の情報が別々に存在する場合に比して，飛躍的に要保護性が高まることは明らかである。

(オ) 国民の懸念，拒絶感

実際に多くの国民が，自己の本人確認情報が住基ネット上を流通させられることについて，深刻な懸念を抱き，住基ネットの参加の意思を問われた場合には，住基ネットへの参加を拒絶している。例えば，住基ネ

ットへの参加について選択権を与えられた横浜市民は，人口総体のおよそ４分の１に当たる約８４万人が住基ネットへの参加を明示的，自発的に拒絶した。

(カ) 以上の各事実を踏まえ，住基ネット上で流通させられる本人確認情報は，プライバシー権の保護の対象となるというべきである。

(3) 自己情報コントロール権侵害及びそのおそれ

ア 住基ネット上に情報を流通させること自体による侵害

前述のとおり，住基ネット上を流通させられてい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ものである。

したがって，住基ネットにより，原告らの本人確認情報を，原告らの同意なく，むしろ明確な意思に反して，各居住自治体以外の機関に通知や提供をする形で流通させ，保存することは，それ自体により原告らが有している本人確認情報に対するコントロール権を現に侵害しているというべきである。

イ データマッチングによる自己情報コントロール権の侵害のおそれ

住基ネットの導入により，すべての国民に固有の１１けたの住民票コードを付したことから，住民票コードをマスターキーとして，集積した情報をデータマッチングすることが可能となった。被告らは，住基法上，データマッチングは禁止されているから，そのおそれはないと主張するが，住基ネット導入までの経緯等からすれば，住基ネットは，国民総背番号制を実現するための端緒というべきであるし，住基ネットのシステム上，データマッチングすることが可能である以上，そのおそれは高いというべきである。

ウ 情報漏えい及び目的外利用等による侵害のおそれ

(ア) 関係者による漏えい及び目的外利用等のおそれ

従前の住民基本台帳関連での個人情報の漏えい等の多くは，内部的要因

によるものである。これらは，いずれも，法規や契約等によって，保護措置が講じられ，守秘義務や罰則によって戒められていながらも，公務員を含めた従事者その他の者によって，漏えいや目的外利用がされてきたものである。

また，法による規制等は，法改正でいくらでも，制限等を解除することができる。現に，住基ネットに関してみても，住基ネットで利用できる国の機関等の事務の種類について，平成１１年の住基法改正時には９３事務であったものが，その後，平成１４年２月，平成１５年１２月，平成１６年１月，同年４月，同年１２月と度重なる法改正によって，現在では２７５事務に拡大されている。

したがって，法制度等の整備によって，漏えい・目的外利用の危険を避ける万全な措置を執ることはできないものである。

(イ) セキュリティの不備による漏えい・改ざん等の危険性

住基ネットの端末は，すべてネットワーク化されているため，そのうちどこか１か所にでも脆弱な点があればネットワーク全体が脆弱となるというシステム的，構造的な脆弱性を有している。しかるに，各自治体の住基ネットシステムの現場では，セキュリティ基準を守り，コンピュータネットワークの安全を確保するための体制と設備を整え，かつ日々更新していくだけの能力も，財政的な裏付けもないところが多数ある。以上のとおり，住基ネットは，構造的な脆弱性を有している。

例えば，平成１５年９月から１１月の間，長野県本人確認情報保護審議会の委員である吉田柳太郎らによる調査チームが，長野県内の３つの自治体（下伊那郡阿智村，諏訪郡下諏訪町，東筑摩郡波田町）のＣＳ等について安全性を確認するための実験調査（以下「長野県侵入実験」という。）を行った結果によれば，ＣＳ，ＣＳ端末のＯＳ（ＯＳとは，キーボード入力や画面出力といった入出力機能やディスクやメモリの管理

等，多くのアプリケーションソフトから共通して利用される基本的な機能を提供し，コンピュータシステム全体を管理するソフトウェアをいう。甲３５）の管理者権限（ネットワークを管理するシステム管理者の権限であり，管理者権限を有する者は，ウィンドウズＮＴ等のＯＳのすべての機能を使える。甲３５）を略奪することが容易であり，遠隔の攻撃端末からＣＳ，ＣＳ端末のＯＳを操作することが可能であり，庁内ＬＡＮ及び既存住基ネットのセキュリティが極めて不十分であるなどの脆弱性が認められた。

そうすると，住基ネットの管理者以外の者が，原告らの居住自治体以外の市町村にあるＣＳ端末の管理者権限を略奪し，同端末を攻撃端末から遠隔操作することにより，指定情報処理機関サーバ，被告県サーバ，原告ら各居住自治体のＣＳサーバに正規の操作者を装ってアクセスして，原告らの本人確認情報を不正に閲覧する危険性及び原告らの住民票の写しを取得する危険性があるといえる。さらに，住基ネットの管理者以外の者が，原告らの居住自治体の既存住基サーバに不正侵入し，住民票コードを含む原告らの個人情報を不正に閲覧する危険性及び既存サーバ内の原告らの個人情報を改ざんし，その情報を住基ネットシステム内に送り出すことにより，同システム内の原告らの本人確認情報を改ざんする危険性があるといえる。

(ウ) 情報流出の事例

北海道斜里郡斜里町の職員が，平成１６年１０月ころ，自宅に住基ネット関連の情報を含むデータをＣＤ－ＲＯＭに格納して持ち帰り，私用のパソコンに入れ，このパソコンを利用していたところ，コンピュータウィルスに感染したため，平成１８年ころになって，上記データファイルが外部に流出したことがあった。また，福島県東白川郡塙町において，平成１６年，会議の出席者に住民票コードが記載された名簿が配布され

たこともあった。さらに，北海道帯広市において，平成１５年から平成１７年の間，複数回にわたり，職員により，住基ネット関連のデータが不正に閲覧されたことが発覚した。

(4) 住基ネットの目的について

ア 経費及び行政事務の増大

被告らは，住基ネットの導入により経費削減及び行政事務の効率化が図られると主張するが，被告らの試算には根拠がなく，現実には，かえって地方公共団体に多大の経費及び行政事務の増大をもたらす可能性があり，極めて非効率的なものである。

イ 住民の便益

被告らは，住基ネットの導入により，住民票の広域交付，各種申請手続における住民票提出の省略，年金事務における現況届の提出の廃止，転出入手続の簡素化など，住民の便益が図られると主張する。

しかし，一般住民が住民票の交付を受ける機会はさほどないし，各自治体において，住基ネット導入前から，駅付近の出張所等での住民票の取寄せ，並びに，夜間及び休日等における住民票の交付等のサービスを行っており，莫大な費用を投下してまで住民票の広域交付制度を作る必要はない。また，現在国の機関等が住基ネットを利用することができるとされている２７５事務のうちには，申請書等の際の添付書類として，戸籍謄本・抄本，印鑑証明書等が必要とされる事務もあり，すべて住民票の写しのみで足りるということでもないから，被告らが主張するほどの利便性は存しないというべきである。さらに，年金事務における現況届の提出の廃止についても，対象となる住民の負担は，毎年１回郵送されてくるはがきに必要事項を記入して切手を貼って返送するというものでしかないから，住民がそのような負担を苦痛と感ずるという事実自体何ら根拠のない主張である。転出入手続の簡素化についても，従来から，転出届を郵送で提出し，転出証

明書を郵送で返送してもらうことが可能であったから，特に，住基ネットにより住民の負担が軽減するというわけでもない。しかも，実際の転居に際しては，住民票の異動の手続だけではなく，子どもの転入学手続，介護保険や国民健康保険の給付手続，年金や水道料の清算などのために役所の窓口に行く必要がある。

したがって，多くの住民にとっては，住基ネットの導入にプライバシー権を侵害してもやむを得ないようなメリットがあるわけではない。

ウ　住基カードの利用率

被告らは，住基カードの有用性を強調するが，住基カードの利用率は極めて低率である。このことは，国民にとって，住基カードの有用性が存しないことを示すものといえる。

エ　公的個人認証サービス

公的個人認証サービスの有用性は，住基ネットシステムの導入を内容とする平成１１年改正住基法が成立した後に問題にされてきたものであって，国会での論議も経ておらず，後から付け加えられた理由というほかない。

オ　電子政府・電子自治体の実現について

電子政府・電子自治体構想が浮上したのは，平成１１年改正住基法の成立以後のことであり，電子政府・電子自治体の実現が住基法改正の目的であり，立法事実であるということは，事実に反するものである。

(5)　本件差止請求の必要性・許容性

原告らが求めているのは，住基ネットの運用全体の差止めではなく，原告らのみの離脱であるから，本件差止請求を認めることによる支障は少ないはずである。

(6)　結論

以上，住基ネットには，原告らの自己情報コントロール権を現に侵害している，又は侵害するおそれがある以上，本件差止請求を認めるべきである。

【被告らの主張】

(1) プライバシー権としての自己情報コントロール権に基づく本人確認情報の要保護性

ア　プライバシー権としての自己情報コントロール権の保障

プライバシーの法的保護の内容は，みだりに私生活へ侵入されたり，他人に知られたくない私生活上の事実又は情報を公開されたりしない利益として把握されるべきであって，原告らが主張するような自己情報コントロール権は，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ものであるから，差止請求の根拠となる排他的権利とはいえない。

イ　プライバシー権の保護の対象としての本人確認情報

仮に，自己情報コントロール権を肯定する見解に立ったとしても，基本４情報は，個人を識別するための単純な情報にすぎないものであり，もともと住基法１２条に基づき，何人でも閲覧等を求めることができるものであるから秘匿性は低く，プライバシー権の保護の対象にはならない。また，住民票コード及び変更情報も，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，信条など個人の道徳的自律に関係するようなものでもないから，プライバシー権の保護の対象とはならない。

また，法は，住民票コードを名寄せのマスターキーにして，データマッチングすることを許容していないのであるから，原告らの主張のように，データマッチングのおそれがあることを前提にして，秘匿の必要性を判断すべきではない。

(2) 権利侵害及びそのおそれの不存在

ア　自己情報コントロール権の侵害の不存在

(ア) 住基法は，本人確認情報の行政目的の利用について，本人の承諾を必

要としていないことについて

仮に，本人確認情報が自己情報コントロール権による保護の対象となるとしても，住基法は，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を当然に予定している。

したがって，住民票記載情報を個人の承諾を得ることなく行政目的のため利用したからといって，これが自己情報コントロール権の侵害に当たると解する余地はない。

(イ) データマッチングによる侵害とそのおそれの不存在

a　住基法によるデータマッチングの禁止

住基法３０条の３４は，本人確認情報の受領者は，当該本人確認情報の提供を受けることが認められた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利用又は提供をしてはならない旨を明確に規定し，目的範囲内の利用等に当たらないデータマッチングを禁止している。

また，行政機関は，特定された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ないし（行政機関個人情報保護法３条２項），行政機関の長は，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のであるから（同法８条１項），行政機関は，これらの規定によっても，目的範囲内の利用等に当たらないデータマッチングを禁じられている。

b　違反行為に対する処罰規定の存在

目的範囲内の利用等に当たらないデータマッチングを行うことは，住基法３０条の３４所定の職務上の義務の違反に該当するため，懲戒処分の対象となる（国家公務員法８２条，地方公務員法２９条）。

また，行政機関の職員が，目的範囲内の利用等に当たらないデータ

マッチングや名寄せを行うために，本人確認情報に関する秘密が記載された文書，図画又は電磁的記録を収集した場合には，行政機関個人情報保護法５５条による処罰規定がある。

さらに，目的範囲内の利用等に当たらないデータマッチングや名寄せを行わせるために，指定情報処理機関の役員及び職員（住基法３０条の１７第３項），本人確認情報の提供を受けた国の機関等の職員が，その知り得た本人確認情報に関する秘密を他の国の機関等に漏らした場合には，公務員の守秘義務違反等に該当し，刑罰の対象となる（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条，５４条，住基法４２条）。

c　違反行為に対する第三者による監視機関の存在

住基法３０条の９第１項は，都道府県に，目的範囲内の利用等に当たらないデータマッチングや名寄せ等を監視する役割を担う第三者機関の設置を義務付けている。また，同法３０条の１５第１項は，指定情報処理機関にも，同様の役割を担う第三者機関を設置するよう義務付けている。

さらに，「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（総務省告示第３３４号。以下「セキュリティ基準」という。乙１，４１）により，都道府県知事は，本人確認情報の提供先である国の機関等における本人確認情報の管理状況について国の機関等に報告を求め，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前記のような報告等を要請することができるとされており，この点においても，住基法上の国の機関等が本人確認情報を不適切に扱うことを防止する制度的な担保ある。

d　データマッチングできない住基ネットの仕組み

指定情報処理機関は，住基法上の国の機関等に対し，本人確認情報を提供することが予定されているものの（同法３０条の１０），本人確認情報以外の個人情報を収集，管理する権限は付与されておらず，国の機関等もそのような情報を指定情報処理機関に対して提供する権限や義務は認められていない。したがって，指定情報処理機関において，国の機関等が保有する情報を結合することは不可能である。

また，住基ネットは，それぞれの機関がそれぞれ受領した本人確認情報を分散して管理することを制度として予定している上，実際上も，指定情報処理機関及び本人確認情報の提供を受けた住基法上の国の機関等は，それぞれ分散して情報を管理しているところ，これらの機関等が分散管理している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。

(ウ)　ＯＥＣＤ８原則に即した保護措置

住基法は，①個人データの収集制限の原則，②データ内容の原則（利用目的とデータ内容の適合性，正確性及び最新性），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責任の原則を定めたＯＥＣＤ８原則を踏まえ，(1)民間での利用禁止，(2)指定情報処理機関サーバや都道府県サーバでの保有情報の限定，(3)ネットワークの外部への情報提供の限定，(4)行政機関に対する保護措置義務，(5)情報漏えい防止，(6)市町村における住民基本台帳システムの保護，(7)制度運用に関する住民参加，(8)記録の最新性及び正確性の確保を講じている。

イ　自己情報コントロール権の権利侵害の危険性の不存在

(ア)　十分なセキュリティ対策

a　制度面からの対策

住基ネットに関しては，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こと，住基法上，本人確認情報の提供を受ける機関や目的が限定されていること，本人確認情報を取り扱う者の責任を明確化し，本人確認情報の保護のための第三者機関の設置が義務付けられていること，住民票コードの利用を制限していること，セキュリティ基準により，関係各機関における緊急時対応計画を策定するよう定められていることなど，制度面からセキュリティ対策が講じられている。

b　外部からの侵入防止策

物理的な侵入に対しては，セキュリティ基準により，建物等への侵入防止策が規定されている。

また，電気通信回線経由による侵入に対しては，住基ネットのための専用回線及び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ことから，正しい通信相手以外の者と接続することがなく，混線や漏えいが起こることやコンピュータウィルスに侵入されることもない。さらに，住基ネットでは，暗号技術評価委員会において安全性が確認された公開鍵方式により，相互認証，暗号通信を行っている。加えて，住基ネットでは，通信プロトコルの制限，徹底したコンピュータウィルス・セキュリティホール対策の実施を行い，不正な通信に対しては，ファイアウォールにより厳重な遮断，常時監視を行っている。

c　内部の不正防止策

住基法や関係法令により，内部の不正行為に対しては，重い刑罰が科せられ，指定情報処理機関に対する監督が行われる規定が設けられている。

また，本人確認情報の検索に際し，端末に所定の照会条件を入力し

ないと本人確認情報の提供を受けられないようにするなど，担当者が当該個人情報を容易に検索できないような措置が講じられているし，そもそもアクセス権限のない職員等が本人確認情報データベースへアクセスすることはできないようになっている。そして，指定情報処理機関は，定期的にアクセスログ（アクセス記録）を解析することとされ，不正アクセスに対する適切な措置を講ずることができる。

さらに，本人確認情報の提供状況について住民から開示請求があった場合，個人情報保護条例により，開示することとされている。

d　外部監査等によるセキュリティ確保

平成１５年，各市町村は，指定情報処理機関及び総務省の作成したチェックリストによりセキュリティ対策の点検を実施し，点検結果に基づく指導を受けた。同年１月から３月までの間に全国１０８の地方自治体において，さらに，平成１６年７月から１１月までの間に全国９９の地方自治体において，それぞれ外部監査法人によるシステム運営監査を実施し，その結果をセキュリティ強化に活用した。

e　住基カードのセキュリティ対策

住基カードの交付及び携帯は，希望者に限られ，地方自治体が独自に提供する住基カードを利用したサービスは条例により限定され，どのようなサービスを受けるかについても住民に選択権が与えられている。技術面でも，ＩＣカードを採用し，暗証番号の設定等により，不正利用を防止する対策が講じられている。

(イ)　長野県侵入実験による安全性の確認

長野県侵入実験について，原告らの主張は，公正とは言い難い調査速報及び知事会見に基づくものであり，むしろ，長野県調査速報及び長野県最終報告によれば，長野県侵入実験により，外部のインターネットから住基ネット本体への侵入ができなかったこと及び被告センターにおい

て管理する本人確認情報への影響が全くなかったことが明らかとなり，住基ネットの安全性がより明確になったというべきである。

(3) 住基ネット導入による住民の便益の増進，行政事務の効率化

ア 住基ネットの意義及び目的等

高度に情報化された現代社会において，全国的な広がりを持った住民の移動や交流という実態に合わせて，行政サービスを的確かつ効率的に提供していく必要があり，また，高齢者や被災者等の弱者に対する配慮に行き届いた社会を構築するためのセイフティネットも必要である。住民基本台帳の全国的な電算化が進んでいることから，これをネットワークで接続すれば，全国的な本人確認システムが安価に構築できるし，住民にとっては面倒な行政手続が簡略化され，行政職員の削減も可能となる。住基ネットは，このような発想から生まれたシステムであって，その目的は，行政サービスの向上と行政事務の効率化である。

イ 電子政府・電子自治体の実現のための住基ネットの必要性

平成１２年，政府はＩＴ戦略会議を設置し，ＩＴを国家戦略として推進することとした。そのような流れの中で，住基ネットは，電子政府・電子自治体の基盤となる不可欠なシステムであると位置付けられている。

ウ 住民の負担軽減と行政事務の効率化

各種の申請及び届出の際に，住民に義務付けられていた住民票の写し等の提出の負担が解消され，行政側も事務効率の向上や事務の正確性が実現した。

エ 行政手続のオンライン化のための公的個人認証サービス

平成１４年，電子政府・電子自治体の推進のため，行政手続オンライン化３法が成立し，行政手続について，オンラインによることも可能とするための法整備が行われた。

住基ネットは，公的認証サービス電子証明書を取得する際に実施される

本人確認や，同証明書発行後の異動等情報を反映するための具体的方法として利用されている。また，住基カードは，インターネット申請を行うためのＩＣカードとして利用されており，住基ネットは，公的個人認証サービスにとって不可欠の役割を果たすものである。

オ　市町村のネットワーク化による住民基本台帳事務の簡素化，広域化

住基ネットの導入により，住基カードの交付を受けている住民は，転入届の際に転出証明書の添付を要しないとされたことから，転出証明書の交付を受けるために，転出地の市町村役場等に赴く必要がなくなった。これにより，住民の負担が軽減するのはもちろん，市町村でも転出証明書の発行に伴う事務を削減でき，事務の効率化を図ることができる。

また，住基ネットの導入により，住民は，いずれの市町村から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（住民票の広域交付）。

カ　住基カードの有用性

住基カードは，住基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，市町村が条例で定めることにより，多目的カードとして活用できることから，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。また，住基カードは，公的な身分証明書としても活用できる。

キ　生じ得る便益の試算

被告国は，住基ネット構築に係る費用として，システム開発経費等の導入的な経費として約３９０億円，コンピュータ維持費等の年間経費として約１９０億円を見込み，毎年，行政側の経費削減として２４０億円，住民側の負担軽減として２７０億円の便益があると試算した。

また，住基ネットは，行政機関等における本人確認情報の共有機能，住民基本台帳事務における市町村間のネットワーク機能，住基カードというＩＣカードの基盤を提供する機能等を有するものであり，公的個人認証サ

ービスの不可欠の前提となるなど，その間接的な効果は極めて大きい。

(4) 差止めの必要性（許容性）

ア 必要性の考慮要素

差止請求の適否を判断する場合の違法性の判断においては，損害賠償請求の場合以上に，差止めの効果が公共的な利益に及ぼす影響を考慮しなければならない。

また，原告らは，差止請求の一態様として，原告らの本人確認情報の住基ネット磁気ディスクからの削除をも求めるが，このような削除請求は，通常の差止請求を認容しただけでは回避できない甚大な損害が生ずる具体的蓋然性が認められる場合など，ごく例外的な場合においてのみ許容されるものである。

イ 一部の住民の離脱による住基ネットの行政目的の阻害

住民の一部にでも不参加者がいると，住基法上の国の機関等をはじめとする本人確認情報の利用者において，従来のシステムや事務処理を存置しなければならず，経費削減効果や行政事務の効率化が著しく減殺されるばかりか，新たな事務処理やシステムの改修が必要となり，これらの経費は住基ネットの利用を希望する者を含めた全住民の負担となる。

(5) 結論

したがって，住基ネットの運用に伴う権利侵害は，全く存在しないか，極めて軽微なものであるのに対し，住基ネットの運用を差し止めることに伴う行政上の不都合は極めて重大であるから，差止めの必要性が存在しないことは明らかである。

2 争点(1)イ（氏名権に基づく差止請求等の可否）について

【原告らの主張】

(1) 氏名権の保障

人の存在のかけがえのなさ，代替不可能性を表すただ一つの手段が人の氏

名であるから，人の氏名は最大限尊重されなければならない。個人の尊重を謳った憲法１３条の趣意からすると，同条は，国民はその有する氏名を中核として個人が個人として尊重され，他と識別され，取り扱われることを内容とする権利，利益（氏名権）の保護を内包するものというべきである。判例においても，氏名は人格権の一内容であるとされている（最高裁昭和５８年(オ)第１３１１号昭和６３年２月１６日第三小法廷判決・民集４２巻２号２７頁参照。以下「昭和６３年最判」という。）。

(2) 氏名権の侵害

前記，第３，１【原告らの主張】，(2)，イ，(イ)及び同(3)，イで主張した住民票コードを付し，運用することの意味，氏名を尊重することの重要性，憲法１３条の趣意，昭和６３年最判の趣旨等からすると，住基ネットにより国民に住民票コードを付し，番号で国民を扱うことは，憲法１３条によって保障される人格権の一内容である氏名権を侵害するものであり，その侵害の程度は深刻である。

(3) 差止めの必要性・許容性

原告らは，番号を付されることにより氏名権を侵害され，著しい精神的苦痛を受けていることから，速やかにその回復が図られるべきである。

原告らの住民票コードの削除自体は容易に行えるものであるし，削除したとしてもそれにより生ずる支障は些少であるから，本件差止請求等は認められるべきである。

【被告らの主張】

(1) 原告らが主張する氏名権の内容

原告らが主張する氏名権は，法文上及び判例上の根拠が全く存在せず，これらを憲法１３条に基づく人格権の一内容として認める余地はない。

原告らは，昭和６３年最判を指摘するが，同判決は「氏名は，社会的にみれば，個人を他人から識別し特定する機能を有するものであるが，同時に，

その個人からみれば，人が個人として尊重される基礎であり，その個人の人格の象徴であって，人格権の一内容を構成すべきものというべきであるから，人は，他人からその氏名を正確に呼称されることについて，不法行為法上の保護を受け得る人格的な利益を有する」と判示したものにすぎず，「氏名で扱われる」ことを人格権の一内容として認めるものなどではない。

(2) 権利侵害の不存在

住民票コードは，基本４情報をサーバ及び電気通信回線を用いて効率的に送信させるために技術上新たに設けられた符合に過ぎず，そもそも個人の人格的価値とは無関係であるから，住民票コードが付されることによって氏名権が侵害されると解する余地はない。

3 争点(1)ウ（公権力による包括的管理からの自由権に基づく差止請求等の可否）について

【原告らの主張】

(1) 公権力による包括的管理からの自由権の保障

公権力によって包括的に管理されない自由とは，各行政機関において，それぞれ個別に保有する国民個人に関する情報を他の行政機関と交換する等して有機的に結合し，いつでも利用できる状態に置かれることを拒絶する自由をいい，個人の人格的生存に不可欠な利益として，憲法１３条の「生命，自由及び幸福追求権」によって保障され，裁判規範性を有する具体的な権利である。

(2) 公権力による包括的管理からの自由権の侵害

名寄せの検索キーとして使用され得るという住民票コードの持つ意味，住民票コードの利用の拡大，住基カードによる情報の集約化等からすると，住基ネットの運用が原告らの公権力による包括的管理からの自由権を侵害していることは明らかであり，その侵害の程度は深刻である。

(3) 差止めの必要性及び許容性

公権力による包括的管理からの自由は，人格権の中でも重要な位置を占める権利，自由であり，そこには他の各種基本権の侵害が伴っていることを併せ考えれば，公権力による侵害行為を直ちに排除する緊急の必要性があるし，原告らについてのみ住基ネットの運用を差し止めることにより生ずる支障は些少であるから，本件差止請求等は認められるべきである。

【被告らの主張】

(1) 原告らが主張する公権力による包括的管理からの自由権の内容

氏名権同様，原告らが主張する権利は，法文上及び判例上の根拠は全く存在せず，憲法１３条に基づく人格権の一内容として認める余地はない。

(2) 権利侵害の不存在

前記のとおり，住民票コードは人格的価値とは無関係であるし，住基ネットの運用により，目的範囲内の利用を超えてデータマッチングされ，住民票コードをマスターキーとして名寄せされる具体的危険性があるとはおよそ想定できないことから，公権力による包括的管理という事態が生じるものではないことは明らかである。

4 争点(2)（損害賠償請求の可否）について

【原告らの主張】

(1) 被告国の国家賠償責任について

被告国（内閣，内閣総理大臣及び総務大臣）は，憲法１１条，１３条，９９条等により，憲法を遵守し，国民の人権を保障する義務を負っており，違憲の法の改廃や延期など相当の手段を講ずることによって，国民の人権の侵害を防止する義務を負っているにもかかわらず，①平成１１年改正住基法附則１条２項に定める「個人情報の保護の万全を期するための所要の措置」を講じず，また施行日までに講ずることができる見込みがないのに，平成１３年１２月２８日，平成１１年改正住基法を平成１４年８月５日から施行する政令を定め，②同日までに，憲法に違反する平成１１年改正住基法の施行，

運用の開始を停止又は同法を廃止する相当の措置を講じず，③前記「所要の措置」も講じないまま施行させ，④住基ネットの運用開始後，廃止又は運用停止等の相当な措置を講じなかった。

その結果，原告らのプライバシー権等が現に侵害され，今後も侵害される危険に晒されているのであるから，被告国が，原告らに対し，国家賠償法１条１項の責任を負うことは明らかである。

(2) 被告県の国家賠償責任について

被告県は，憲法１１条，１３条，９９条等により，憲法を遵守し，県民の人権を保障する義務を負っており，住基法上，都道府県知事が住基ネットから離脱する権限（ネットワークを切断する権限）をも含む「当該本人確認情報の適切な管理のために必要な措置」を講ずる権限を付与され，法的義務を課されているにもかかわらず，①被告県内の市町村長に対し，住民票コードを指定，通知し，②本人確認情報を磁気ディスクに記録，保存し，③住基法上の国の機関に情報提供し，④被告センターに対し，住民票コードの指定及び通知並びに本人確認情報の提供等の本人確認情報の処理に関する事務を委任し，⑤被告センターへ本人確認情報を通知する等の事務を行った。

その結果，原告らのプライバシー権等が現に侵害され，今後も侵害される危険に晒されているのであるから，被告県が，原告らに対し，国家賠償法１条１項の責任を負うことは明らかである。

(3) 被告センターの不法行為責任について

被告センターは，指定情報処理機関として，被告県から委任を受け，原告らの本人確認情報の処理に関する事務を行っているから，これにより，プライバシー権等を侵害された原告らに対し，不法行為責任を負う。

(4) 損害額

原告らは，住基ネットの運用により，プライバシー権等を侵害され続け，甚大な精神的苦痛を被ったが，これを慰謝する金額として少なくとも原告ら

１人当たり１０万円が相当である。

したがって，原告らの損害額は，本件訴訟を弁護士に委任したことにより生じた損害請求額の１割に当たる弁護士報酬各１万円と併せ，各１１万円は下らないものである。

【被告らの主張】

(1) 被告国及び被告県の責任について

ア　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，国家賠償法１条１項にいう違法があったと評価されるものである（最高裁平成元年(オ)第９３０号平成５年３月１１日第一小法廷判決・民集４７巻４号２８６３頁等）。

法令の違憲審査権は，裁判所のみが有するものであり（憲法８１条），内閣は専ら法律を誠実に執行すべき責務を負うものであるから（憲法７３条），内閣がある法律を違憲であると自ら判断し，その執行を拒むことは許されず，このことは，地方公共団体において行政の執行に当たる首長についても同様というべきである。

したがって，内閣や地方公共団体の首長は，法律の規定に従って適切に事務を行っている限り，職務上通常尽くすべき注意義務を尽くさなかった違法があるとの評価を受けることはないというべきである。

イ　また，住基ネットの運用開始に当たり，内閣は個人情報保護関連５法を国会に提出し，平成１１年改正住基法附則の「所要の措置」を講じていること，前記のとおり，住基ネットの運用は違憲ではないことなどからすると，内閣，内閣総理大臣及び総務大臣の行為等について，国家賠償法１条１項が適用される余地はない。

そして，被告県の知事についても，住基法の規定に従い，適切に事務を行うことによって，職務上通常尽くすべき注意義務を尽くしているといえ

るから，国家賠償法１条１項にいう違法があったとの評価を受ける余地はない。

(2) 被告センターの責任について

被告センターは，住基法に基づき，総務大臣から指定を受けた指定情報処理機関として，被告県から委託された事務及び同法に定められた事務を同法の定めるところに従い行うものであり，その事務の遂行については何らの違法性もない。

したがって，被告センターは，原告らに対し，不法行為に基づく損害賠償責任を負うものではない。

第４ 争点に対する判断

１ 争点(1)ア（プライバシー権としての自己情報コントロール権に基づく差止請求の可否）について

(1) プライバシー権の保障

憲法１３条は，すべての国民が個人として尊重されることを保障しているが，個人として尊重されるためには，私生活上の自由を保障することが不可欠であるから，「私生活をみだりに干渉されない権利」としてのプライバシー権は，憲法１３条により保障されているというべきである。さらに，高度に情報化された現代社会においては，インターネット等を通じた個人情報の収集，利用，提供により個人の尊厳が脅かされるおそれがある。そうすると，個人の尊厳を保障するためには，プライバシー権を単に「私生活をみだりに干渉されない権利」と解するだけでは足りず，「みだりに自己の情報を収集，利用，提供されない権利」（自己情報コントロール権）をも含む権利であると解するのが相当であり，このような自己情報コントロール権は，憲法１３条により保障されているものというべきである。

(2) 自己情報コントロール権の保護の対象となる情報

住基ネットにおいて本人の同意なく提供される本人確認情報には，①氏名，

②生年月日，③性別，④住所，⑤住民票コード，⑥変更情報がある。

上記①から④の基本４情報は，個別にみれば，個人識別のための単純な情報であって，その限りでは秘匿すべき必要性の高い情報とまではいえない。しかし，基本４情報を一体としてみた場合には，個人識別という側面を超え，個人の私生活に密接に結びつく情報として，秘匿すべき必要性のある情報となり得るというべきである。例えば，ストーカー行為等を行う相手（ストーカー行為等の規制等に関する法律第２条２項参照）に対しては，基本４情報であっても，開示されたくないと考えることは自然なことであり，その期待は保護の対象となるというべきである。また，平成１５年５月３０日に施行された個人情報保護法は，氏名，生年月日を含む個人識別情報を保護の対象としていること（個人情報保護法２条１項），従来，原則として誰でも住民基本台帳の一部の写しを閲覧できるとしていた住基法は，平成１８年６月，一部改正され，閲覧することにできる場合を法律で定める一定の場合に限定し，不正の手段による閲覧，閲覧事項の目的外利用等の禁止に対する違反への制裁措置を強化したこと（平成１８年法律第７４号。１１条，１１条の２，４６条，４７条，４９条，５１条，５４条等。平成１８年９月政令２９７号により，平成１８年１１月１日より施行。）からも，基本４情報のような個人情報についても保護されるべき情報に当たるとの認識が広まっていることをみてとることができる。

また，住民票コードそれ自体は，１１けたの数字の羅列でしかないが，住民一人一人に付された重複することのない固有の番号であり，住基ネットにおいては，基本４情報と共に提供され，本人確認情報の提供を受けた機関等がこれを基に当該機関が有している情報と結合することを予定していることからすると，秘匿する必要性の高い情報というべきである。

さらに，変更情報についても，住基ネット上，変更内容それ自体が記録されるわけではないが，性別及び氏名に関する変動のみが「職権修正等」とし

て記録され（住基法７条１項１号，同項３号，施行令３０条の５第３号，施行規則１１条３項２号），これにより，性別の変更，結婚，離婚等の身分上の重要な変動があったことを容易にうかがわせることになるから，秘匿する必要性があるというべきである。

したがって，住基ネットにおける本人確認情報は，一体としてみた場合，自己情報コントロール権の保護の対象となるというべきであり，また，住民票コードはそれ自体，秘匿性の高い情報といえるから，これも自己情報コントロール権の保護の対象となるというべきであって，住民は，原則として，自己の同意なしにこれらの情報が収集，利用，提供されることを拒むことができるとするのが相当である。

(3) 自己情報コントロール権に基づく本件差止請求の可否

ア 「公共の福祉」による制約

前記のとおり，本人確認情報は，憲法１３条を淵源とする自己情報コントロール権によって保護されることからすると，市町村長が，他者に当該住民の本人確認情報を通知，提供するためには，当該住民の同意を得ることが必要とされることになる。

しかし，自己情報コントロール権も，絶対に制限を許さないという権利ではなく，公共の福祉による制約を受けるというべきである。

したがって，本件差止請求等が認められるか否かは，住基ネットにおいて，本人の同意なく本人確認情報を通知，提供することが，公共の福祉による制約として許されるか否かという観点から検討する必要がある。

そして，当該制約が許されるか否かは，住基ネットにおいて，本人確認情報を提供等する目的に必要性，合理性があるか否か，本人確認情報の提供等の手段方法が相当か否かという基準によって判断すべきであり，当該制約が許されることについてのその主張立証責任は，被告ら側にあるというべきである。

イ　目的の必要性，合理性

(ア) 前記前提事実，後掲の各証拠及び弁論の全趣旨によれば，以下の事実を認めることができる。

a　住基法の改正の経緯（乙４，５，４９から５５，８９から９５）

自治省は，同省行政局内に学識経験者等により構成された「住民記録システムのネットワークの構築等に関する研究会」を設置し，平成６年から平成７年にわたり，住民基本台帳事務のネットワーク化について調査，検討を重ねた。同研究会は，平成８年３月，一部の地方公共団体において市町村の単位を越えた住民サービスのネットワーク化の試みがあること等を踏まえ，地方分権化社会における相互連携の必要性，高齢化社会の本格化等も考慮し，住民サービスの向上，住民基本台帳事務の効率化・広域化を図るために，全国的なネットワークシステムを構築する必要があると報告した。同報告では，住民基本台帳のネットワーク化には，①住民基本台帳事務の効率化（年間約４６０万件に上る転入・転出事務，年間約８４００万件に上る住民票写し等の交付事務の効率化）及び広域化（広域的な住民票写しの交付の実現），②行政機関における本人確認への利用，③行政手続における住民票の写し等の添付の省略，④申請手続等の簡素化の手段等としての住基カードの活用等による住民の利便性の向上といったメリットがあるとしている（乙４９）。

その後，住基法改正試案の公表等を経て，平成１０年３月，「住基法一部改正案」が閣議決定され，国会への提出，審議等を経て，平成１１年改正住基法が成立し，同年８月１８日に公布された（乙５１）。

b　改正後の事情

住基法の改正後，政府は，国家戦略として，電子政府・電子自治体の実現を目指し，ペーパーレス，国等が提供する行政手続のオンライ

ン化，行政情報のインターネット公開等を具体的目標とし（乙７，７５から７７），行政手続のオンライン化の前提として，住基ネットによる本人確認制度を必要不可欠なものとして位置付けた（乙１２）。

c　行政事務の効率化及び住民の便益の向上（乙１０，２９）

住基ネットの導入により，住民登録をしている自治体以外の自治体や住基法上の国の機関等が，これまで自治体が個別に保有していた本人確認情報をデータとして容易に入手し，次のような行政手続等において利用できるようになったことにより，行政事務の効率化，住民の負担軽減，便益の向上が図られている。また，住基カードは，公的な身分証明書としても活用することができる。

(a)　継続的に行われる給付行政事務（恩給，年金等），資格付与に関する行政事務（建設業の許可等）に関する本人確認事務

住民は，年金受給のための現況届，各種申請の際の住民票の写しを提出する必要がなくなった。国の機関等は，本人確認事務等を効率的に行い，受給者や資格者等の現況変更，住所変更を確実かつ迅速に把握することができるようになった。

住基ネット第一次稼働後の１年間において，各種年金支給のための現況届等が省略された件数は約５００万件，パスポートの申請等の行政手続における住民票の写しが省略された件数は約３００万件あった（乙５７）。

(b)　全国の市町村における住民票の写しの交付事務（広域交付）

住民は，自己の居住しない地方自治体において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。

(c)　転入転出事務

住基カード所持者は，付記転出届をすれば，転出証明書の提出が不要となり，転出証明書の発行を受けるためだけに転出地の市町村

窓口に赴く必要はなくなった。転入地の市町村は，転出地の市町村から電子データで情報を受け取ることができるようになった。

(d) 申請・届出等手続に関する本人確認事務

行政手続のオンライン化を進めることにより，インターネットで各種の申請，届出等を行うことができるようになった。また，併せて，公的個人認証サービスを行うことで，インターネットによる手続における第三者による情報の改ざんや成りすましを防止することができる（乙５７から５９）。

(e) 条例で定める事務

条例の定めにより，各市町村独自の利用サービス（福祉サービス，公共施設の利用等）に住基カードを利用することができる（乙６１）。

(イ) 以上のとおり，住基ネットの導入は，行政事務の効率化，住民負担の軽減，便益向上を目的としたものであるから，平成１１年改正住基法の立法目的には合理性，必要性があると認めることができる。また，電子政府・電子自治体の実現が具体的に進められるようになったのは，住基法の改正後であるが，具体的には，ペーパーレス，行政手続のオンライン化，行政情報のインターネット公開等を目的とするものであり，民間におけるオンライン手続の普及等に照らすと，行政手続のオンライン化には，必要性，合理性が認められる。そして，行政手続のオンライン化を行うためには，住基ネットの運用が前提となるから，現段階において行われている電子政府・電子自治体の推進も，平成１１年改正住基法の目的の必要性，合理性を根拠付けるものということができる。

したがって，住基ネットにおいて，本人確認情報を提供等する目的には，必要性，合理性があると認めることができる。

ウ 手段としての相当性

(ア) 前記前提事実，後掲の各証拠及び弁論の全趣旨によれば，以下の事実を認めることができる。

a 通知・提供する情報の内容

前記前提事実（第２，１，(3)，ウ，(ア)）のとおり，住基ネットにおいて，通知，提供，利用される情報は，①氏名，②生年月日，③性別，④住所，⑤住民票コード，⑥変更情報に限定されている。その他の情報が付加されて，住基ネット上を流通することはない。

b 通知・提供の相手方

前記前提事実（第２，１，(3)，ウ，(イ)及び同(エ)）のとおり，本人確認情報を通知又は提供し得る相手方は，市町村長，都道府県知事，指定情報処理機関及び住基法上の国の機関等に限定されている。また，指定情報処理機関は，総務大臣から指定を受けた被告センターのみしか存在しない。

c 本人確認情報の提供・利用事務の限定

(a) 住基法上の国の機関等に対する提供

前記前提事実（第２，１，(3)，ウ，(エ)，ｂ）のとおり，国の機関等に情報提供する場合は，住基法で定められた事務処理に関し，住民の居住関係の確認のために求めがあったときに限られる。

(b) 都道府県知事に対する提供

他の都道府県知事に提供する場合も，前記前提事実（第２，１，(3)，ウ，(エ)，ｄ）のとおり，住基法等の法令で定められた事務処理のために求められたときに限られる。

(c) 市町村長に対する提供

他の市町村長に提供する場合も，前記前提事実（第２，１，(3)，ウ，(エ)，ａ，同ｃ及び同ｅ）のとおり，住基法等の法令で定められた事務処理，住民基本台帳に関する事務処理のために求められたと

きに限られる。

(d) 都道府県知事及び指定処理機関自身による利用等の制限

都道府県知事及び指定情報処理機関は，住基法で定められた場合を除き，市町村長から通知を受けた本人確認情報を利用又は提供してはならないとされている（住基法３０条の３０）。

(e) 受領者の利用及び提供の制限

本人確認情報の受領者は，法の定めにより本人確認情報の提供を求めることが許されている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，提供するものとし，当該事務処理以外の目的のために利用，提供してはならないとされている（住基法３０条の３４）。

d 住民票コードに関する制限

(a) 住民票コードの告知要求制限

市町村長，都道府県知事，指定情報処理機関及び住基法上の国の機関等は，法定された場合を除き，何人にも住民票コードの告知を求めてはならない（住基法３０条の４２）。

市町村長，都道府県知事，指定情報処理機関及び住基法上の国の機関等以外の者は，何人も，自己と同一の世帯に属する者以外の者に対し，住民票コードの告知を求めてはならない（住基法３０条の４３第１項）。

市町村長，都道府県知事，指定情報処理機関及び住基法上の国の機関等以外の者は，その者が業として行う行為に関し，売買契約等の相手方に対し，住民票コードの告知を求めてはならない（住基法３０条の４３第２項）。

(b) 住民票コードの利用制限

市町村長，都道府県知事，指定情報処理機関及び住基法上の国の

機関等以外の者は，業として，住民票コードを付記した情報をデータベース化してはならない（住基法３０条の４３第３項）。

(c) 都道府県知事による勧告，命令，罰則

前記(a)及び(b)による告知要求，住民票コードを付記した情報のデータベース化を行った場合において，都道府県知事は，当該行為をした者が更に反復してこれらの規定に違反する行為をするおそれがあると認めるときは，当該行為をした者に対し，当該行為の中止を勧告し，又は当該行為が中止されることを確保するために必要な措置を講ずべきことを勧告することができる（住基法３０条の４３第４項）。

都道府県知事は，前記勧告を受けた者がその勧告に従わないときは，都道府県の審議会の意見を聴いて，その者に対し，期限を定めて，当該勧告に従うよう命ずることができる（住基法３０条の４３第５項）。

上記命令に違反した者は，１年以下の懲役又は５０万円以下の罰金に処される（住基法４４条）。法人の代表者又は法人若しくは人の代理人，使用人その他の従事者が，その法人又は人の業務に関して，前記命令に違反したときは，その行為者を罰するほか，その法人又は人に対し，前記罰金刑を科する（住基法４８条）。

e 住基カードの交付対象者

住基カードは，申請した者に対してのみ交付されるものであり，すべての住民に交付されるものではない（住基法３０条の４４）。

f セキュリティ（乙１，１３，４６の①）

(a) 技術的基準

住基ネット上のデータの送信方法又は磁気ディスクへの記録及び保存等の技術的基準は，総務大臣が定めることとされ（施行規則２

条，６条，８条，１２条，１３条，１６条から２０条），平成１４年６月１０日，総務大臣は，総務省告示をもって，セキュリティ基準（乙１，４１）を定めた。セキュリティ基準は，平成１５年５月２７日（総務省告示第３９１号。以下「第３９１号セキュリティ基準」という。乙３の①），同年９月２９日（総務省告示第６０１号。以下「第６０１号セキュリティ基準」という。乙３の②）にそれぞれ一部改正された。また，平成１５年５月２７日，住民基本台帳カードに関する技術的基準（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。乙１６，４２）を定めた。

(b) 専用回線の使用（乙１，１３，４６の①，②）

セキュリティ基準３－3(1)を受け，住基ネットは，電気通信回線からのデータの盗取を防止するため，ＣＳ，都道府県サーバ及び指定情報処理機関サーバを結ぶ電気通信回線，国の機関等に本人確認情報を提供する場合の都道府県サーバ又は指定情報処理機関サーバと国の機関等サーバを結ぶ電気通信回線について，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）を使用している。

セキュリティ基準５により，既設ネットワークと住基ネットを接続する場合にも，専用回線の使用，ファイアウォールによる通信制御等を行うことが求められている。

(c) 通信相手の相互認証・暗号通信（乙１，１３）

セキュリティ基準４－３－(4)及び同(5)を受け，住基ネットの通信では，暗号技術評価委員会において安全性が確認されている公開鍵方式（対になる２つの鍵を使ってデータの暗号化・復号化を行う暗号方式。鍵の片方は他人に広く公開されるため公開鍵と呼ばれ，もう片方は本人だけが分かるように厳重に管理されるため秘密鍵と呼

ばれる。）を採用し，通信を行うごとに，意図した通信相手に接続されたことを相互に認証することとされている。公開鍵方式における秘密鍵は，指定情報処理機関で耐タンパー装置に封入設定後，当該耐タンパー装置ごと都道府県知事等に配送するため，第三者が内容を読み出したり，変更することはできない。

通信相手の相互認証の過程で，その都度耐タンパー装置内で，暗号技術評価委員会において暗号強度が認知されている暗号方式の一つにより，通信の都度共通番号鍵を設定し，これを更に公開鍵方式における公開鍵で暗号化した上で通信相手に輸送する暗号通信が採用されている。通信を行う２つのサーバは，その共通暗号鍵により暗号化してデータの送信を行い，通信が終われればその共通暗号鍵は廃棄される。

(d) 不正通信の遮断（乙１３）

住基ネットの通信プロトコル（プロトコルとは，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をいう。甲３５）は，ＴＣＰ／ＩＰ（Transmission Control Protocol ／ Internet Protocol インターネットやイントラネットで標準的に使用されるプロトコル。甲３５）を基盤としているが，独自のアプリケーションによる通信を行っており，ＳＭＴＰ（電子メールを送信するためのプロトコル。甲３５），ＨＴＴＰ（WWWデータ送信のためのプロトコル。甲３５）等，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。また，すべてのＣＳのネットワーク側，都道府県サーバのネットワーク側・端末機側，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のネットワーク側に指定情報処理機関が不正侵入を監視するファイアウォール（以下「指定情報処理機関監視ファイアウォール」とい

う。ファイアウォールとは，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，又はそのようなシステムが組み込まれたコンピュータをいう。甲３５）を設置し，インターネットで用いられるプロトコルの通過を遮断するシステムを採用し，２４時間監視している。

さらに，指定情報処理機関は，ネットワーク内に侵入検知装置（ＩＤＳ）を設置し，常時監視を行うほか，定期的にアクセスログの解析を行っている。

コンピュータウィルスに対しては，指定情報処理機関において，コンピュータウィルスの発生情報を常時入手し，定期的に（危険度の高いものは随時），パターンファイルをすべての関連機関に配布している。また，ＯＳのセキュリティホール発生情報を入手し，危険度が高いものは，システムの影響度を確認した上で，すべての関連機関にセキュリティホール情報及び対応方法を通知することとしている。

(e) 重要機能室への入退室管理

セキュリティ基準４－１では，重要機能室への入退室管理に関し，入室者を限定し，入退室管理カード等により権限者か否かを確認すること，鍵又は入退室管理カードの管理方法を定めること，搬出入物品の内容を確認すること等が求められている。

(f) 端末機操作の管理

セキュリティ基準４－４では，端末機（住基ネット上の通信を行う国の機関等の電子計算機の端末機も含む）の取扱いは，管理責任者からの指示又は承認を受けた者が行うこと，操作者がアクセス権限を有していることを確認すること，ファイル（磁気ディスクに記録されているデータ等）の利用を制限する方法を定めること，操作

履歴を記録すること等が求められている。

(g) 電子計算機の管理

セキュリティ基準４－５では，データの暗号化等を行うための秘密鍵を厳重に保護するための外部漏えい防止措置を講ずること，ＣＳ，都道府県サーバ及び指定情報処理機関サーバでは，住基ネットの管理及び運用に必要なソフトウェア以外のソフトウェアを作動させないこと等が求められている。

(h) 構成機器及び関連設備等の管理

セキュリティ基準４－７では，管理方法を明確化すること，指定情報処理機関において稼働状況を監視すること，コンピュータウィルス等の不正プログラムの混入防止のための監視，駆除措置を講じ，発見時の必要な措置を定めること等が求められている。

(i) 住基カードのセキュリティ

住基カードは，暗証番号の設定，中央演算処理装置付きの半導体集積回路（ＩＣ）を組み込んだカードである。住基カードは，条例の定めにより，住基法で認められたもの以外の情報を搭載することができる。住基カードは，住基法上の利用に供する基本利用領域と条例利用領域とに分けられ，それぞれ割り当てられた領域以外の領域に情報を記録したり，他の領域に記録された情報を読み取ることはできない仕組みとなっている。また，住基カードのセキュリティ対策として，暗証番号の設定，情報の読取り又は解析を防止する仕組みを保持することとされている（住基カードセキュリティ基準。乙１６）。

g セキュリティに関する点検，テスト

(a) 住基ネット運用状況の自己点検（乙１３）

平成１５年１月及び２月，すべての市町村は，住基ネット及びそ

れに接続する既存のネットワークに関し，「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」（乙１４）に基づく自己点検を実施した。重要機能室を設置できない場合，重要機器及び磁気ディスク等が盗まれたり，権限のない者により容易にアクセスされないように適切な管理を行うことなど重要と思われる７項目については，すべての市町村が満点を達成するように，都道府県，総務省及び指定情報処理機関による指導が行われた。

平成１６年にも，すべての市町村は，調査票に基づき，セキュリティ対策について自己点検を行った（乙４８）。

(b) 住基ネットに対するペネトレーションテスト（乙１５）

被告センターは，平成１５年１０月１０日から１２日，東京都品川区の協力を受け，監査会社による住基ネットの重要機器に対するペネトレーションテストを行った。その結果として，住基ネットとＣＳとの間のファイアウォール，ＣＳと庁内ＬＡＮとの間のファイアウォール，庁内ＬＡＮ上のＣＳ端末に対し，ファイアウォール等の攻略を試みたが成功せず，脆弱性も見出せなかったと発表した。ただし，監査会社は，住基ネットの範囲外ではあるが，庁内ＬＡＮに対してもチェックリストによる自己点検やセキュリティ監査と庁内ＬＡＮ上のデータ送信における高度なセキュリティレベルを維持するための方策を実施すべきであるとの助言を付加した。

(c) 長野県の侵入実験（甲１２の①，②，１３，２０の①，２６，２８の①から④，３１，３７，乙１８，２０から２３）

平成１５年９月から１１月までの間，長野県本人確認情報保護審議会の委員である吉田柳太郎らによる調査チームが，長野県内の３つの自治体（下伊那郡阿智村，諏訪郡下諏訪町，東筑摩郡波田町）

のＣＳ等について安全性を確認するための実験調査（長野県侵入実験）を行った（甲１２の①，②，２８の①，乙１８）。

[redacted]の第１次調査では，役場サーバ室内のＨＵＢ（ＨＵＢとは，スター型ＬＡＮで使われる集線装置をいう。甲３５），隣接する施設のＬＡＮポート，庁内ＬＡＮにダイヤルアップで接続されている出先機関のルータ（ルータとは，ＬＡＮとＬＡＮ，ＬＡＮとＷＡＮのようにネットワーク間を接続する機器をいう。甲３５）に調査用コンピュータを接続して調査した。[redacted]第２次調査では，ＣＳが格納されている役場サーバ室内のラックを開錠し，ＣＳセグメントにあるＨＵＢに調査用コンピュータを接続して調査した。[redacted]の調査では，調査用に構築した無線ＬＡＮを利用して，[redacted]役場に隣接する建物から調査用コンピュータを庁内ＬＡＮに接続して調査した。この[redacted]及び[redacted]の調査の結果，庁内ＬＡＮへの接続及びＣＳ（端末ではなくサーバ）の管理者権限を奪取することができた。[redacted]の調査では，遠隔地より，インターネットを経由した侵入実験を行ったが，適切なセキュリティパッチ（セキュリティパッチとは，ソフトウェアに保安上の弱点が発覚したときに配布される修正プログラムをいう。甲３５）が当てられていたため，ファイアウォール越しにサーバの管理者権限を奪取することはできなかった（甲１３，２８の①）。

平成１６年２月２９日，長野県侵入実験の最終結果として，「パスワード設定等の問題があり，庁舎の内外から既存住基サーバや庁内ＷＥＢサーバに管理者権限でログインできたほか，データベースへのアクセス制限にも問題があり，住民票コードなどの個人情報を含む重要なデータを閲覧できた」，「住基ネットＣＳを含むコンピュータネットワーク上のサーバのＯＳが既知の脆弱性を含んだまま

運用されており，一定の条件下においては，一般に入手可能なツールによる管理者権限の奪取も可能であった」，「既存住基サーバとＣＳとの間に置かれたファイアウォールについては，不要と思われるポート（ポートとは，インターネット上の通信において，複数の相手と同時に接続を行うためにＩＰアドレスの下に設けられたサブアドレスをいう。甲３５）が空いている例があったほか，ファイアウォールのＯＳのバージョンが古く，既知の脆弱性を利用した攻撃が行われる可能性が存在した」など，住基ネット上，いくつかの脆弱性が発見されたと報告された（甲１３，乙１８）。

これに対し，総務省は，長野侵入実験は，ファイアウォールで防御された区画内に攻撃端末をつなぐなどしていて調査手法に問題がある上，住基ネット関係のいずれのファイアウォールも突破することができず，住基ネット本体にインターネットから侵入することはできなかったというのであるから，住基ネット本体の本人確認情報に対する具体的危険性は確認されなかったとの見解を表明した（乙２０から２２）。

他方で，総務大臣の諮問機関として総務省に設置された住民基本台帳ネットワークシステム調査委員会において，総務省の事務局担当者からは庁内ＬＡＮには最新のセキュリティパッチが施されていない，適切なパスワード管理ができていないなどの問題等があり，各市町村のセキュリティ対策の向上を図る必要があるなどの説明があり（甲１４８），庁内ＬＡＮ，ＣＳ等に関するセキュリティ対策が提案された（乙２２）。

h　秘密保持義務

住基法上，市町村又は都道府県の職員等（住基法３０条の３１），指定情報処理機関の役職員等（住基法３０条の１７），本人確認情報

受領者の職員等（住基法３０条の１７）には，秘密保持義務が課せられている。

前記秘密保持義務に違反して秘密を漏らした者に対しては，２年以下の懲役又は１００万円以下の罰金に処する旨の刑罰規定がある（住基法４２条）。

i　提供情報の管理状況についての報告要請等

(a)　市町村長は，必要に応じ，都道府県知事を経由して，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，本人確認情報の適切な管理のための措置の実施について要請を行うこととされている（第６０１号セキュリティ基準６－8(1)エ）。

(b)　委任都道府県知事は，住民からの自己の本人確認情報の提供状況に関する情報開示請求に備え，指定情報処理機関に対し，国の機関等に対する提供状況について報告を求め，その情報を保存することとされている（第６０１号セキュリティ基準６－8(5)イ）。

j　本人確認情報の提供状況の公表

(a)　都道府県知事による提供状況の公表

都道府県知事は，毎年少なくとも一回，住基法上の国の機関等に対する本人確認情報の提供状況について，報告書を作成し，これを公表する（住基法３０条の７第８項）。

(b)　指定情報処理機関による提供状況の公表

指定情報処理機関は，上記(a)と同様，報告書を作成し，これを公表する（住基法３０条の１１第６項，乙２８，３２はその例。）。

(c)　利用状況の開示

住民は，当該都道府県の個人情報保護条例に基づき，自己の本人確認情報の提供状況について開示請求をすることができる（乙３の②，４７の①）。

k　本人確認情報の保護のための第三者機関

(a)　都道府県における審議会の設置

都道府県に置くこととされた審議会は，市町村長から都道府県知事へ通知される本人確認情報の保護に関し，調査審議し，都道府県知事に建議することができる（住基法３０条の９第１，２項）。

(b)　指定情報処理機関における本人確認情報保護委員会の設置

指定情報処理機関に置くこととされた本人確認情報保護委員会は，委任都道府県知事から通知される本人確認情報の保護に関し，調査審議し，指定情報処理機関の代表者に意見を述べることができる（住基法３０条の１５第１，２項）。

l　住基ネット関連の情報漏えい

北海道斜里郡斜里町の職員が住基ネット関連の情報を含むデータが格納されたＣＤ－ＲＯＭを自宅に持ち帰り，私用のパソコン内にそのデータを保存していたところ，平成１８年１月から３月ころまでの間，パソコンがコンピュータウィルスに感染し，住基ネットに関連するパスワード（ただし，流出時には既に使用されていなかったもの）を含む情報が流出した（甲１７４の②）。

また，北海道帯広市においては，平成１５年及び平成１７年，複数回にわたり，複数の職員が，職務外で既存の住基システム端末等により，住民の住所，氏名の情報（平成１５年は，住民基本台帳上の情報すべて）を閲覧していたことが発覚した（甲１７５の②）。

さらに，福島県東白川郡塙町では，平成１６年９月１３日，行政区長が出席した敬老会打合せ会議において，住民票コードを付した招待者名簿を配布した（甲１７６の②）。

m　横浜市の事例（甲４６，５４の①，乙２，証人花園）

横浜市長は，平成１４年７月１０日，平成１１年改正住基法附則１

条２項の「必要な措置」である個人情報保護に関する法整備が行われないまま，住基ネット運用が開始されることは問題であるとして，内閣総理大臣及び総務大臣に対し，「住民基本台帳ネットワークシステムの実施の延期を求める要望書」（甲５４の①）を提出した。

横浜市長は，平成１４年８月５日の住基ネット第一次稼働の前の準備行為として，被告県知事に同月２日時点の本人確認情報を通知したが（乙２），住基法３６条の２第１項の「本人確認情報の適切な管理のために必要な措置」として（花園証人１８頁），住基ネット第一次稼働後の本人確認情報の通知は行わなかった。

横浜市は，平成１４年９月２日から同年１０月１１日までの間，横浜市民に対し，横浜市から被告県等への本人確認情報の通知を希望しない旨の申出を行う機会を与えたところ，同日の時点で，住民基本台帳人口３４６万０７４２人（同月末の人口）のうち８３万９５３９人の市民が非通知の申出をした（甲４９）。新たに市民となった者も非通知の申出をすることができるが，平成１７年２月２８日の時点での非通知希望者数は，住民基本台帳人口３５１万６４８４人のうち８３万９７６０人であった（甲４６の②）。

横浜市は，平成１５年４月９日，総務省との間で，順次，通知希望者の更新データ及び非通知希望者の更新されていない旨のデータを送信し，通知希望者については，住基ネットの運用を可能とする旨の合意をし（乙２），同年６月９日から，通知希望者に関する住基ネットの利用が開始された（花園証人５頁）。

現在，横浜市では，通知希望者のみについて住基ネットの運用を行っているが，この方式で実施していることについて，横浜市内部の行政手続において，特に支障は生じていない（甲４６の②，花園証人１３頁）。

n　住基ネット運用に要する費用

総務省は，平成１４年１０月３１日，平成１１年度から平成１５年度までの住基ネット導入経費として合計約３９０億円，住基ネット稼働後の毎年の経費として合計約１９０億円を要すると発表した（被告国及び被告県準備書面(8)別紙１）。他方，毎年見込まれる利益としては，行政側が合計約２４０億円，住民側が合計約２７０億円であると試算した（同準備書面(8)別紙２）。

これに対し，長野県は，平成１６年２月，住基ネット運営の費用対効果について，行政側のメリットと住民側のメリットから経費を控除した額は，平成１５年度マイナス約５億４９８４万円，平成１６年度マイナス約２億７５８３万円であり，平成１９年度にプラスに転じるものの，導入経費を累積するとマイナスが続くと再試算した（甲２０の②）。ただし，この再試算においては，公的個人認証サービスの活用による住民サービスの向上，住基カードの多目的利用による住民サービスの向上等の効果については数値化されていない。

(イ)　上記(ア)の事実に基づき，住基ネットが手段の相当性を具備しているか否かについて判断する。

a　前記のとおり，住基ネットにおいては，①通知・提供される情報の内容，通知・提供される相手方，本人確認情報を利用できる事務等が限定されていること，②住基法で定められた者以外は，原則として，住民票コードの告知要求や利用を制限されていること，③本人確認情報以外の情報を登載することが可能な住基カードの交付は希望者のみに交付されるものであること，④通信につき，閉鎖された専用回線，相互認証，暗号通信，通信プロトコルの制限等を採用していること，⑤指定情報処理機関監視ファイアウォール等による２４時間監視が行われていること，⑥住基ネット関連機器に関する管理基準が設けられ

ていること ⑦住基ネット関連の事務に従事する職員等に対しては秘密保持義務が課せられ，処罰規定が設けられていること，⑧市町村長や委任都道府県知事は，提供した情報の管理状況について報告を要請することができること，⑨都道府県知事及び指定情報処理機関は提供状況を公表することとされ，住民は個人情報保護条例に基づき，自己の本人確認情報の提供状況について開示請求することができること，⑩都道府県及び指定情報処理機関において，本人確認情報の保護のための第三者機関を設置することとされていること，⑪セキュリティテストとして，すべての市町村は調査票に基づく自己点検を行い，その結果に基づき，指定情報処理機関及び総務省が，適宜指導等を行っていること，⑫被告センターが実施したペネトレーションテストでは，ファイアウォールの攻略を試みたが成功しなかったことが認められる。

他方，長野県侵入実験では，庁内ＬＡＮへの接続に成功したことが認められるが，ファイアーウォールを越えて，住基ネット独自のネットワークへの侵入に成功したものではないし，ＣＳの管理者権限の奪取は，調査用コンピュータを役場のサーバ室内のＨＵＢに直接接続するなど物理的な侵入を伴う態様で調査した結果であるから，現実には，ＣＳの管理者権限を奪取される危険性が高いとはいえず，長野侵入実験から直ちに住基ネットのセキュリティに問題があるとまではいえない。

また，北海道斜里郡斜里町等において，住基ネットに関連する情報や本人確認情報が流出したことが認められるが，これらは，いずれも，住基ネット上のセキュリティの不備を原因とするものではなく，職員らの認識不足等に基づくものであり，住基ネット固有の問題とは言い難い。

そうすると，住基ネットは，本人確認情報を保有し得る主体及び情

報の内容が前記イの目的を達成するために必要な範囲に限定され，情報漏えい防止に対しても，相応の措置が講じられているということができる。

また，高度情報化社会を前提として，地方分権化社会の促進，高齢化社会への対応等のため市町村単位を越えた情報のネットワーク化を図ることが必要的かつ合理的であり，そのためには，希望者だけを対象とするのではなく，すべての住民を対象とした住基ネットの構築が必要であるということができる。

したがって，住基ネットは，手段としての相当性を備えていると認めることができる。

b　なお，本人確認情報自体は保護する必要性のある情報であること，長野県侵入実験の結果から明らかとなったように，重要機能室内へ物理的な侵入があった場合には，パスワードの管理状況等により，管理権限を奪取される危険性のある自治体が存在していたこと，地方自治体の職員の認識不足等による住基ネット関連の情報流出がみられたこと，コンピュータ技術は日々進化していくものであること，住基ネットのセキュリティに対する不安の声があること（甲９等），横浜市民の約４分の１は非通知を希望していること（甲４６の②），東京都品川区のペネトレーションテストを行った監査会社及び住民基本台帳ネットワークシステム調査委員会が，庁内ＬＡＮのセキュリティ対策等を行うべきとの意見を出していること等からすると，住基ネットを運用していくためには，長野県侵入実験の結果等も真摯に受け止め，庁内ＬＡＮも含めて適切なセキュリティ対策の維持，向上に努めることが不可欠であることを付言する。

c　また，原告らは，住基ネットが経済的効率化をもたらしていないことを指摘するが，コストの問題は，政策の妥当性の問題である側面が

強いこと，住基ネットの運用実施後，数年でその適否を判断すべきではないこと，長野県が行った試算は，住基ネットの効果を網羅するものではなく，経済的効率化の面で住基ネットが無効であることを論証し得ているものではないこと，原告らの住基ネットの運用のみを差し止めることはかえってコストの増大をもたらすものであること等からすれば，住基ネットのコストの問題をもって，原告らの権利を制約することが不当であると結論付けることはできないというべきである。

(ウ) 名寄せ，データマッチングに関する原告らの主張について

原告らは，住基ネットの導入により，個人情報の名寄せ，データマッチングが現に行われ，又は行われるおそれがあり，これが原告らの自己情報コントロール権を侵害し，又は侵害するおそれがあると主張することから，この点についても付言する。

前記認定事実のとおり，住基ネットにおいて，すべての地方公共団体が有する住民の本人確認情報を住基ネットの通信回線を通じて集約し得る機関は，指定情報処理機関のみである。したがって，技術的には，指定情報処理機関が，住民票コードを利用し，名寄せ，データマッチングをし得るシステムとなっている。しかし，前記認定事実のとおり，指定情報処理機関は，住基法上の事務を処理する以外に本人確認情報を利用することを禁止され，本人確認情報を提供した相手方の国の機関等から情報の提供を受けることはできない。そうすると，住基ネットにおいては，住民票コードをマスターキーとして名寄せをしたり，本人確認情報をそれ以外の情報とデータマッチングして情報を集約し，これを一括管理したりする主体は現実にはないということができる。

また，住基ネットの運用により，国の機関等が住民票コードを含む本人確認情報を保有し得ることになったため，抽象的には，本人確認情報を保有する国の機関等に情報照会し，住民票コードをマスターキーとし

て，本人確認情報以外の情報を名寄せ，データマッチングすることができることは事実である。しかし，前記前提事実のとおり，住基法上，本人確認情報の受領者は，法定の事務処理以外の目的で，受領した本人確認情報を利用，提供することは禁止されているし，行政機関個人情報保護法上も，行政機関が個人情報を保有，提供又は利用することが許されるのは，法令で定められた場合に限定され，目的外の保有等が禁止され（行政機関個人情報保護法３条，８条１項），行政機関の職員等に対しても罰則を伴う守秘義務等が課せられている（行政機関個人情報保護法５３条から５５条）から，現時点の法制下において，住民票コードをマスターキーとして本人確認情報以外の情報が収集，結合される具体的危険性があるとは認め難い。

したがって，この点に関する原告らの主張は採用することができない。

なお，「住民記録システムのネットワークの構築等に関する研究会」が作成した報告書（乙４９）や，平成１７年６月２１日，税制調査会が発表した「論点整理」において，納税者番号制度の導入に当たり，住基ネットや住民票コードの利用を指摘している（甲１３７）。しかし，住民票コードを納税者番号として利用するためには，住基カードの利用及び住民票コードの民間利用が前提であるところ，現在，住基カードの交付は希望者のみに限られ，住民票コードの民間利用は禁止されていることから，現在の住基法の下で，住民票コードが納税者番号制度に利用されることによる名寄せのおそれがあると認めることはできない。なお，仮に，住民票コードを納税者番号として利用する場合には，住民票コードの民間利用を許すことになり，データマッチングされる情報量も格段に広がることが予想されることから，現在の住基法の下では，本人の同意なしに，納税者番号として住民票コードを利用，提供することは，許されないことが明らかである。

エ　自己情報コントロール権に基づく本件差止請求の可否についての結論

以上により，住基ネットの運用は，その目的に必要性，合理性が認められ，手段もその目的を達するのに相当なものといえることから，自己情報コントロール権に対する公共の福祉による制約として許容されるとするのが相当である。

したがって，自己情報コントロール権に基づく本件差止請求等についての原告らの主張は理由がない。

2　争点(1)イ（氏名権に基づく差止請求等の可否）について

原告らが主張するように，氏名を中核として，個人として尊重され，他と識別されて取り扱われることを内容とする権利，利益が人格権の一内容として憲法上保障されるとしても，住民票コードは，個人識別を容易にするために付されたものであって，原告らを番号のみで扱うものでも，原告らを氏名によって識別し，取り扱うことを妨げるものでもないから，住基ネットにより，原告らの主張する氏名権が侵害されているとはいえない。

したがって，氏名権に基づく本件差止請求等についての原告らの主張は理由がない。

3　争点(1)ウ（公権力による包括的管理からの自由権に基づく差止請求等の可否）について

原告らが主張するように，公権力によって包括的に管理されない自由が憲法上保障されるとしても，前記のとおり，住基法上，本人確認情報の提供を受けた機関等が有するその他の情報を収集，管理する主体はなく，それぞれの機関等が個別に有する情報について，住民票コード等をマスターキーとして名寄せすることは，禁止されているから，住基ネットの運用により，公権力による包括的管理からの自由権が侵害されているとはいえない。

したがって，公権力による包括的管理からの自由権に基づく本件差止請求等についての原告らの主張も理由がない。

4　争点(2)（損害賠償請求の可否）について

(1)　被告国の責任

前記のとおり，住基ネットの運用は，原告らの権利利益を違法に侵害するものではなく，また，個人情報保護関連５法が成立したのは平成１５年５月３０日であるが，平成１１年改正住基法附則１条２項の文理からすれば，「所要の措置」を講ずることは施行の条件とはされていないと解すべきであり，むしろ，同条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施行することが義務付けられていることから，被告国がこれに従い，政令により平成１４年８月５日に施行日を定め，平成１１年改正住基法を施行したことに，国家賠償法上の違法はないというべきである。

したがって，被告国に対する損害賠償請求についての原告らの主張は理由がない。

(2)　被告県及び被告センターの責任

前記のとおり，住基ネットの運用は，原告らの権利利益を違法に侵害するものではないから，住基法の規定に従い，被告県の知事及び同知事から委託を受けた被告センターが，住基ネット運用に係る事務を行ったことに，国家賠償法上又は不法行為上の違法はないというべきである。

したがって，被告県及び被告センターに対する損害賠償請求についての原告らの主張も理由がない。

第５　結論

以上の次第で，原告らの本件請求はいずれも理由がないから，これを棄却することとし，主文のとおり判決する。

横浜地方裁判所第４民事部

裁判長裁判官　　小　　林　　正

裁判官　　志　田　原　信　三

裁判官　　樋　口　真　貴　子