平成１８年３月２０日判決言渡

平成１４年（ワ）第２４２７号　住民基本台帳ネットワーク差止等請求事件

判　　決

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　被告千葉県（以下「被告県」という。）は，

（１）　住民基本台帳法（昭和４２年法律第８１号，以下「住基法」という。）３０条の７第３項の別表第一の上覧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（以下「被告情報センター」という。）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）　被告情報センターに対し，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。

２　被告情報センターは，

（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）　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。

３　被告県及び被告情報センターは，原告らに対し，連帯して，各金１１万円及びこれらに対する平成１４年１１月２１日から支払済みまで年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，各金１１万円及びこれらに対する平成１４年１１月２１日から支払済みまで年５分の割合による金員を支払え。

第２　事案の概要

本件は，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）により導入された住民基本台帳ネットワーク（以下「住基ネット」という。）が，原告らの人格権，プライバシー権等を侵害しているないしは侵害する危険がある等と主張して，千葉県民である原告らが，①被告県に対し，原告らに関する本人確認情報の提供・通知及び被告情報センターへの本人確認情報処理事務の委任の差止め，並びに原告らに関する本人確認情報の磁気ディスクからの削除，②被告情報センターに対し，原告らに関する本人確認情報処理事務の差止め及び原告らに関する本人確認情報の磁気ディスクからの削除，③被告らに対し，国家賠償法１条１項又は不法行為に基づき，損害賠償金の支払をそれぞれ求めた事案である。

１　前提となる事実

（１）　当事者

ア　原告らは，いずれも千葉県内の肩書地に住民登録をしている者である。

イ　被告情報センターは，地方公共団体におけるコンピュータの利用を促進するために昭和４５年５月に設立された法人である。

（２）　住基ネットシステムの概要

ア　住民基本台帳

住民基本台帳とは，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ための公簿である（住基法１条）。

イ　住基法改正

住基法は，平成１１年８月１８日，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）により改正され，住基ネットが導入された（以下，平成１１年法律第１３３号による改正後の住基法を「改正住基法」ということがある。）。

ウ　本人確認情報

（ア）　本人確認情報とは，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変更情報をいう（住基法７条，３０条の５第１項，住民基本台帳法施行令（以下「施行令」という。）３０条の５）。

（イ）　変更情報とは，①住民票の記載，消除及び記載の修正を行った旨，②政令及び総務省令で定める事項，具体的には転入，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（住民票コードの記載の修正を行った場合には，修正前に記載されていた住民票コード）及び住民票コードの職権記載等の１０事項，③その事由が生じた年月日をいう（住民基本台帳法施行規則（以下「施行規則」という。）１１条）。

（ウ）　住民票コードとは，無作為に作成された１０けたの数字及び１けたの検査数字を組み合わせた番号であり，全国を通じて重複しないこととされている住民票の記載事項である（住基法３０条の２，３０条の７第２項，７条１３号，施行規則１条）。住民基本台帳に記載されている者は，理由の如何を問わず，その者に係る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）。

エ　本人確認情報の提供及び利用

（ア）　市町村長から都道府県知事への通知及び保存

市町村長は，都道府県知事に対し，住民票の記載，消除又は氏名，生年月日，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，当該住民票の記載に係る本人確認情報を通知する（住基法３０条の５第１項）。

都道府県知事は，市町村長から通知された本人確認情報を，当該通知を受けた日から原則として５年間保存しなければならない（住基法３０条の５第３項，施行令３０条の６）。

（イ）　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に対し，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）。

（ウ）　都道府県知事から国の機関等への提供

都道府県知事は，住基法別表第１の上欄に掲げる国の機関又は法人（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）。

また，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）　都道府県知事から市町村長等への提供

都道府県知事は，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（以下「区域内の市町村の執行機関」という。）に対し，①区域内の市町村の執行機関であって住基法別表第２の上欄に掲げるものから同表の下欄に掲げる事務の処理に関し求めがあったとき，②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，③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には，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）。

都道府県知事は，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（以下「他の都道府県の区域内の市町村の執行機関」という。）に対し，①当該他の都道府県の都道府県知事を経て当該他の都道府県の区域内の市町村の執行機関であって別表第４の上欄に掲げるものから同表の下欄に掲げ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他の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，③当該他の都道府県の都道府県知事を経て当該他の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には，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）。

（オ）　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，他の都道府県の都道府県知事その他の執行機関（以下「他の都道府県の執行機関」という。）に対し，①他の都道府県の執行機関であって，住基法別表第３の上欄に掲げるものから同表の下欄に掲げ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，③他の都道府県の都道府県知事から住基法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には，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）　都道府県内部における利用

都道府県知事は，①住基法別表第５に掲げる事務を遂行するとき，②条例で定める事務を遂行するとき，③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，④統計資料の作成をするときには，保存期間に係る本人確認情報を利用することができる（住基法３０条の８第１項）。

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（住基法３０条の８第２項）。

（キ）　以上の本人確認情報の通知等は，電子計算機から電気通信回線を通じて受領者の使用する電子計算機へ送信する方法，本人確認情報を記録した磁気ディスクを送付するなどの方法によって行う（住基法３０条の５第２項，３０条の７第７項，施行令３０条の７ないし１０）。

住基ネットの利用が可能な事務は，平成１７年４月１日時点で，２７５事務である。

オ　指定情報処理機関

指定情報処理機関とは，都道府県知事の委任により，住基法３０条の７第１項ないし第６項，３７条２項に規定されている本人確認情報処理事務等を行う機関である（住基法３０条の１０）。

被告情報センターは，総務大臣から指定情報処理機関の指定を受けており，千葉県知事から上記の委任を受けている。指定情報処理機関に事務を委任した都道府県知事は，住基法３０条の７第１項ないし第３項，第５項及び第６項の事務を行わない（住基法３０条の１０第３項）。

カ　住民基本台帳カード

住民基本台帳カード（以下「住基カード」という。）とは，自己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い，住民基本台帳事務に利用される他，市町村長その他の市町村の執行機関は，住基カードを市町村の条例の定める目的のために

利用することができる。住基カードは，住民基本台帳に記録されている者の交付申請があった場合に交付される（住基法３０条の４４）。

キ　住基ネットの稼働

改正住基法は，附則１条１項柱書において，公布の日から起算して３年を超えない範囲内において政令で定める日から施行することとされ，平成１３年１２月政令４３０号により，平成１４年８月５日から施行された。

改正住基法の附則１条２項は，同法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旨規定している。

２　争点

本件における争点は，住基ネットによる①プライバシー権の侵害ないしその危険性の有無，②氏名権侵害の有無，③公権力によって包括的に管理されない自由の侵害ないしその危険性の有無，④住基ネットの運用が国家賠償法上の違法性を有するか否か，⑤損害額の５点である。

３　争点に関する当事者の主張

（１）　争点１（プライバシー権の侵害ないしその危険性の有無）について

（原告らの主張）

ア　住基ネットによるプライバシー権の侵害について

（ア）ａ　プライバシー権は，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権利であり，憲法１３条で保護される憲法上の権利である。

ｂ　プライバシー権の内容は，公的機関が自己に関する情報を本人の知らない間に収集・管理等できるとすれば，自己決定に対する重大な阻害要因となり得ること，現代社会においてはコンピュータが普及し，情報化が高度に進展していることなどからすれば，自己情報コントロール権としてとらえるべきである。

ここにいう自己情報とは，個人情報のすべてを指すと解すべきであり，住基ネットで流通させられる４情報（氏名，住所，生年月日及び性別）も，プライバシーに係る情報として，憲法１３条により保護されるべきである。すなわち，基本的な本人識別情報であっても，他のデータと結合されることによってセンシティヴなデータに変化するなど，すべての情報に一定の潜在的なセンシティヴ性が認められる上，公権力との関係においては，私人間の場合に比して自己情報のコントロールが十全に図られるべきであるから，情報の要保護性を個別具体的な問題状況を総合的に考慮した上で慎重に検討すべきである。そして，個人情報保護の重要性について国民の関心ないし法的意識が急速に高まりつつあること，住民票コードは個人情報検索のマスターキーとなり得ること，住基ネットが全国的なコンピュータ・ネットワークであることなどに照らせば，住基ネットにおける本人確認情報の要保護性は高いというべきである。このことは，最高裁平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁からも明らかである。

そして，コントロールとは，個人の情報の収集・取得，保有・管理，利用・提供（以下「収集等」ということがある。）のすべての段階において，原則として，これらの行為が当該個人の意思に反して行われてはならないことを指すと解すべきである。また，派生的には自己情報の開示請求権及び訂正請求権が認められなければならない。

c　被告らは，自己情報コントロール権が憲法１３条によって保障された人権ではないなどと主張するが，学説や判例を恣意的に引用するものにすぎない。かかる主張は，プライバシーの権利ないし自己情報コントロール権に対する理解のない行政機関が上記権利の重大な侵害又はその危険性がある住基ネットを運用していることを示すものであり，原告らの権利侵害の深刻さを示すものである。

（イ）　上記のプライバシー権の内容からすれば，個人情報を，本人の同意を得ないで第三者に提供する行為は原則として違法であり，具体的な被害の有無にかかわらず，同意のない提供それ自体がプライバシーを侵害する違憲・違法な行為というべきである。

しかるに，住基ネットは，すべての国民に一方的に１１けたの住民票コードを付し，そのコードとともに，本人確認情報が本人のあずかり知らないままに住基ネットシステムを流通し，利用されるものであり，被告情報センターから国へ提供され，利用される事務は平成１７年４月１日時点で２７５にまで及ぶのである。さらに，原告らは，住基ネットによって，本人確認情報が，いかなる機関・法人のいかなる事務に対して提供されたかを知るすべがない。

よって，かかる改正住基法は憲法１３条に違反するものであり，それ自体自己情報コントロール権を侵害する違憲・違法なものである。

（ウ）ａ　仮にそうでないとしても，プライバシー権が重要な権利であること，公権力との関係では表現の自由等の相互調整も不要であること，本人確認情報は，より多くの個人情報を検索可能にする機能を有していることから，その要保護性は高度であること，個人情報保護に関する国民意識ないし社会通念が変化していることなどからすれば，公権力を行使し，本人の意思に反してプライバシー情報を収集等をするためには，合理的な正当な目的の下に，国民全体の利益を達成するためやむにやまれぬ手段であり，必要不可欠な限度という要件を満たさなければならないと解すべきである。

さらに，プライバシー情報の収集等を国民一律に適用するものである場合には，国民が一律に適用を受けなければ施策として成り立たない場合に限り許されるというべきである。

しかるに，原告らが住基ネットの適用を受けないことによって達せ

られない行政目的もなければ，住基ネットの運用に支障を来すなどの不都合もなく，住基ネットには必要性も重要性もないのであるから，住基ネットをこれに反対する国民に適用することは，プライバシーの侵害として許されないというべきである。

b　これに対し，住基ネットの必要性に関し，被告らは，住基ネットシステムが公的個人認証サービスに必要不可欠であり，電子政府・電子自治体実現の基礎となること，また，行政サービス向上に資するものであり，さらには行政側にコストの削減がなされるとともに住民側にとっても負担が軽減するなどと主張する。

しかし，公的個人認証サービスに不可欠との点は，改正住基法の成立後に問題とされたにすぎない上，仮にこれを作る必要があるとしても，それを必要とする者が個人の判断で個人情報を登録すれば足りることであり，住基ネットを整備する必要など全くない。また，電子政府実現との点も，電子政府構想が問題になったのは平成１２年ころであり，改正住基法が成立した後のことであるから，そもそも住基ネットシステムは，電子政府・電子自治体の実現を目的としたシステムではない。行政サービス向上の点も，単に住民票の写しの広域交付が可能となり，一定の場合に，転出届出の際に住基カードを提示すれば転出証明書の添付が省略されるなどというものにすぎない上，それを必要とする者が個人の判断で個人情報を登録すれば足りることであり，原告のプライバシー権侵害を正当化し得るものではない。さらに，コスト削減の点についても，その試算の内容は，実態と想定数値の間に甚だしい乖離があるなど極めてずさんであり，到底裏付ける資料たり得ない。そもそも，コスト削減を図れなくなるとの点は，住基ネットの運用を開始してしまったことが前提となっており，既成事実を作り上げて支障があると主張するものであって不当である。また，原告ら

が住基ネットに参加しないことによって生ずる支障の程度が低いことは，住基ネットに参加していない自治体が存することによって，住基ネットの運用に不都合が生じていることが窺えないことからも明らかである。

したがって，被告らの主張は，住基ネットの必要性を基礎づけるものとはいえず，すべて失当である。

イ　住基ネットによるプライバシー権侵害の危険性について

（ア）　情報漏えいの危険について

a　長野県において行われた侵入実験によれば，住基ネットによって，原告らの個人情報が不正に閲覧されるなどの具体的現実的危険性が存することは明らかである。すなわち，①既存住基サーバが接続された庁内ＬＡＮのセキュリティは脆弱であることから，当該庁内ＬＡＮに侵入した上，既存住基サーバの管理者権限を奪取するなどして，サーバ内に存する住民票コードが付された住民基本台帳上の全データを不正に閲覧ないし改ざんする危険性がある，②全国ネットワーク化された約３０００の市区町村のうち，１か所においてセキュリティが脆弱な市区町村が存在して，コミュニケーションサーバ（市町村長が本人確認情報の通知等に使用するコンピュータ，以下「ＣＳ」という。）セグメントに接続した攻撃端末からの攻撃によるＣＳ端末の管理者権限が略奪されたならば，このＣＳ端末を遠隔操作して正規の操作者になりすまして，原告らの本人確認情報を不正に閲覧等する危険性がある，③たとえＣＳセグメントに攻撃端末を接続できなくても，１か所の市区町村において，既存住基サーバの管理者権限を奪取できれば，ＦＷ越しにＣＳサーバの管理者権限を奪取し，さらにＣＳ端末の管理者権限を奪取することによって，同様に原告らの本人確認情報を不正に閲覧等する危険性がある。さらには，④住基カードを本人に成りす

まされて不正取得される危険性，⑤本人確認情報提供先において作成されている各種データベースを不正閲覧される危険性等がある。

被告らは，安全確保措置を講じていると主張するが，全国の自治体においては，住基ネットのＣＳサーバを重要機能室に保管していなかったり，サーバや端末用のＩＤ番号やパスワードの設定や管理・保管がずさんであったり，セキュリティ対策上根本的重要性を有するセキュリティホールのパッチ当て作業が極めて不十分なところが多数存在し，総務省告示に記載されたセキュリティ基準すら満たされている状況にはほど遠い。これらセキュリティ対策が脆弱な市町村の住基ネットに不正侵入がされることにより，原告らの個人情報が漏えい等する現実的具体的危険性が存することは明らかである。

b　次に，住基ネット関係の事務に従事する者の権限濫用による漏えいが考えられる。

すなわち，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，一か所に集中管理されると，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，情報の流出や流用，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。情報漏えいの多くは内部的要因によるものであり，守秘義務や罰則等の規制があっても，現実には数え切れないほどの行政機関関係者による目的外利用や漏えいが発生しており，これらの規制のみで目的外利用や漏えいを防止できないことは明らかである。

したがって，法による規制では何らの歯止めにはならず，権限濫用のおそれは高いというべきである。

（イ）　データマッチングの危険について

コンピュータによる情報処理技術の発展により公権力による個人の全面的管理の危険性が増大している状況下では，従来からは知られていな

い方法で個人の行動を監視する可能性が増大し，当局が関心を持つことで個人の意思決定に対して多大な萎縮的効果をもたらすものである。そして，個人情報の収集等の形態が，紙に書かれた情報であるか，コンピュータ化されたデジタル化された情報であるか，コンピュータ・ネットワーク化されたものであるかにより，その危険性・重大性，国民に与える萎縮的効果，個人の全面的管理の危険性の程度には雲泥の差があるものである。

これに対し，被告らは，住基ネットはそれぞれの国の機関等が保有する情報を分散管理することを予定しており，データマッチングを禁止したり罰則規定が存在することなどから，データマッチングの具体的危険性はないと主張する。

しかし，法の規定は何ら目的外利用の歯止めにはならない。また，すべての国民に重複しない番号である住民票コードを付したことにより，データベース間での個々人の同一性の判断を阻害する要因がなくなったこと，省庁間は霞ヶ関ＷＡＮによって相互にネットワーク化されていること，住基ネットの推進者は国民総背番号制の実現を目的として住基ネットを整備してきたものであることなどからすれば，国の機関等によってデータマッチングがなされる具体的，現実的な危険があり，少なくともそのような危険があると考えることには合理的根拠があるというべきである。

（ウ）　プライバシー権侵害の現実的危険性の主張・立証責任について

プライバシー権侵害の現実的危険性については，住基ネットのセキュリティ対策に関する資料はすべて被告らが所持している上，具体的資料を明らかにしないことなどからすれば，最高裁平成４年１０月２９日第一小法廷判決と同様に，原告らがその危険性について一応の主張・立証をなしたときは，被告らにおいて，その危険性がないことを具体的に主

張・立証すべきであり，これを行わない場合には，住基ネットはプライバシー権侵害の危険があるものと事実上推認すべきである。

ウ　差止めの可否について

（ア）　プライバシーは，その性質上，いったん漏えい等によって侵害されれば，取り返しがつかないものである。また，住基ネットの運用はコンピュータの運用に伴って行われるものであることから，原告らのプライバシー権侵害行為は瞬時に行われるとともに，原告ら本人には察知できずかつ直ちには判明しない。このように，住基ネットの運用によって侵害される原告らの権利は重大であり，かつ，侵害の発生前に食い止める必要がある。

（イ）　これに対し，原告らに関する情報提供等の差止めによって，住基ネットの運用に何らの支障も生じず，被告らに生じる被害・不都合は皆無といってよい。被告らは，住基ネットの重要性・必要性について主張するが，これには何らの根拠もないことは明らかである。

被告らは，プライバシーの権利は差止請求の根拠となるような排他的権利として認められていないなどと主張するが，被告ら独自の見解にすぎず，判例・学説がプライバシー権に基づく差止請求を認めていることは明らかである。

（ウ）　また，被告らは，差止請求が認容されるためには，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などと主張するが，公権力による個人情報の取扱いに際しては表現の自由等との調整が必要となるものではない上，原告らの請求も住基ネット全体の運用差止めを求めているものではなく，個別の離脱請求にとどまることなどから，そのような要件は不要であると解すべきである。しかも，住基ネットの運用による権利侵害の危険性は，既に述べたところからすれば，原告らの差止請求が認められる程度に高度か

つ具体的というべきである。

（エ）　したがって，原告らの本件差止請求は認められるべきである。

（被告らの主張）

ア　住基ネットによるプライバシー権の侵害について

（ア）ａ　原告らの主張する自己情報コントロール権は，実体法上の根拠がない上，その実質的なコントロールの内容，自己情報の範囲，権利の具体性等の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。

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って，プライバシーに属する情報をコントロールすることを内容とする権利とは認められない。

ｂ　住基ネット上で送受信される情報のうち，氏名・住所・生年月日及び性別の４情報は，個人を識別するための単純な情報にすぎず，住基法の規定に基づき閲覧等を求めることができるものである。また，住民票コード及び変更情報も，個人の人格的自律にかかわらない外形的・客観的事項に関するものにすぎず，思想信条などの道徳的自律に関係するものではない。原告らが指摘する平成１５年最高裁判決は，当該学生らが講演会の参加申込者であるという公開することが当然視できない情報も合わせた全体の情報について，法的保護の対象となることを認めたものであり，参加者の個人情報の開示についてあらかじめ承諾を求めることは容易であったにもかかわらず，同意を得ることなく個人情報を開示したことが違法とされたという特殊な事案に関するものであるから，その射程は限定的にとらえるべきである。

また，変更情報についても，身分関係の変動等を端的に推知させる

情報ではなく，住民票コードについても，名寄せのマスターキーとすることは法が禁じており，データマッチングに利用されることを前提に秘匿の必要性を判断すべきではないから，秘匿の必要性の程度が相当高いなどということはいえない。

（イ）ａ　そもそも住基法は，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。すなわち，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るから，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，これらの情報を個人の承諾を要することなく利用できるとの法制度が採られているのであり，この点は住基法の改正前と改正後とで変わりはない。

ｂ　したがって，本人の同意を得ることなく本人確認情報を利用することは，何らプライバシー権を侵害するものではない。

なお，プライバシー権の内容につき，自己情報コントロール権説に立つ論者も，住基ネットの運用が直ちにプライバシー権を侵害するものではないとの見解を表明している。

（ウ）ａ　住基ネットは，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になることから，導入されたシステムであって，行政サービスの向上と行政事務の効率化である。そして，住基ネットは，平成１２年ころから，電子政府，電子自治体の実現のために必要不可欠な制度であるとの位置づけがなされるに至ったものである。また，住基ネットの導入によって，各事務ごとの住民票の写しの添付の省略が可能となったり，行政事務の正確性・効率の向上が実現しているほか，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。

住基カードも，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，条例により多目的カードとして活用できること，公的な身分証明書として活用できることなどの有用性がある。

被告国は，改正住基法制定当時，住基ネットの構築に必要な経費として約３９０億円，年間経費として約１９０億円を見込み，数値化可能な便益については，行政側の経費削減として約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んでおり，多大な便益があると試算された。また，電子政府・電子自治体の推進においても不可欠な存在であるなど，その間接的効果も極めて大きい。

b　住基ネットは，行政コストの削減を図ることを一つの重要な行政目的としているのであって，住民の一部にでも不参加があると，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するとともに，本人確認情報の提供・利用の都度，いわゆる非通知希望者であるかどうかを確認せざるを得ないこととなるが，このような事態は住基法のおよそ想定するところではなく，住基法が予定する効果の達成は困難となり，住基ネットの存在そのものを否定することにほかならない。

c　以上によれば，上記の住基法の行政目的が正当なものであることは明らかであり，一部の住民の離脱を認めることは，このような総体としての住基ネットの行政目的を著しく阻害するものであり，すべての国民の本人確認情報を住基ネットにおいて利用することには十分な合理性があるというべきである。

イ　住基ネットによるプライバシー権侵害の危険性について

（ア）　情報漏えいの危険について

a　総務省は，セキュリティ基準を定め，本人確認情報等の安全確保のための具体的基準を定めた。例えば，外部からの侵入防止のため，専用回線の利用，通信データの暗号化，通信相手となるサーバとの相互認証，他のネットワークと接続する場合にはファイアウォールを設置することなどを義務づけているほか，操作者識別カードやパスワードによる本人確認を行い，操作履歴を保存するなど不正利用を防止するための措置を講じている。

住基ネットのセキュリティに関しては，都道府県及び指定情報処理機関の保有する情報は本人確認情報のみに限定しているほか，本人確認情報の利用を法律又は条例に規定された場合に限定していること，住民票コードの利用を制限していること，緊急時対応計画の策定など，制度面から対策を講じている。

外部からの侵入防止対策としては，重要機能室の配置及び構造，入退室管理，データ・プログラム・ドキュメントの管理等に関する対策などを行っている。また，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閉鎖的ネットワークを介して行っていること，サーバ間で相互認証，暗号通信を実施していること，通信プロトコルは独自プロトコルであること，指定情報処理機関監視ファイアウォールを設置してインターネットで用いられるプロトコルの通信を遮断するなどの措置を講じている。また，コンピュータウイルス，セキュリティホール対策を実施しているほか，指定情報処理機関監視ファイアウォール，侵入検知装置による不正通信の監視と遮断を実施している。

b　内部の不正防止対策としては，刑罰（住基法４２条，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。）５３条ないし５５条）や指定情報処理機関に対する監

督（住基法３０条の１６，１８，２２，２３等）等の措置を講じている。また，本人確認情報の検索に際し，即時提供方式の場合，検索の方法を限定することにより，容易に個人情報を検索できないような措置が講じられている。さらに，操作者識別カードを用いることにより，権限のない職員がアクセスできないような措置を講じているほか，関係職員には，通常よりも重い罰則付きの守秘義務を負わせている。また，アクセスログの解析により，不正アクセスが行われた場合にはこれを発見することができる。

さらに，住民の請求があった場合に，本人確認情報の提供状況を開示することが可能となり，当該個人にも不正使用の端緒がわかるようにしている。また，市町村に対する外部監査法人による監査，チェックリストを使用したセキュリティ対策，模擬攻撃（ペネトレーションテスト）によるセキュリティの確認・強化を実施している。

長野県侵入実験については，平成１５年１２月１６日に発表された調査速報，Ａ氏の記者会見がされたが，住基ネットに関して公正な評価をしたものとは到底いえず，侵入実験結果の最終報告によれば，外部のインターネットからの侵入及び庁内ＬＡＮからＣＳセグメントへの侵入にことごとく失敗したものであり，住基ネット本体の本人確認情報に対する危険性がないことが明らかとなったものであって，一部の市町村において，庁舎内に侵入した上で攻撃端末が接続された場合等に，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にすぎない。

（イ）　データマッチングについて

a　住基法では，別表の事務の範囲内で本人確認情報と他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（以下「目的範囲内の利用」という。）は許されている。これに対し，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本人確認情報を利用してはならない（住基法３０条の３４）とされており，目的範囲内の利用に当たらないデータマッチングは全面的に禁じられている。そして，これに違反して目的範囲内の利用に当たらないデータマッチングを行うことは，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）だけでなく，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条ないし５５条，住基法４２条）。

都道府県には本人確認情報の保護に関する審議会が置かれ，指定情報処理機関にも本人確認情報保護委員会を置かなければならないこととされており，これらが第三者機関として違反行為に対する監視の役割を担っている（住基法３０条の９，１５）。また，総務省が定めたセキュリティ基準に基づき，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る。

b　本人確認情報の提供が認められている事務は，平成１７年４月１日の時点で２７５あるが，指定情報処理機関は，本人確認情報以外の住民に関する情報を収集する権限はなく，また，２７５の事務に関する情報を一元的に管理する主体は存在せず，個人情報が統一的に結合されることはない。

そうすると，住民個々人の多面的な情報が瞬時に集められるためには，個人情報を扱う公務員が，法令上の根拠もないのに他の国の機関等に情報提供し，これを統一的に管理した上，住基法３０条の３４に反してデータマッチングを行うか，不正アクセス防止法に違反して多数の国の機関から個人情報を盗取し，これを統一的に集約管理するこ

とが必要であり，かつこれを可能にするシステムを構築する必要があるが，このような事態は想定し得ない。

ｃ　住基カードは，住基ネットエリアと独自利用エリアに分かれており，住基ネットエリアに格納されている住民票コードにアクセスするには相互認証を経る必要があるが，独自利用エリアを利用する機関には認証権限がないから，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名寄せが行われる危険性はない。

また，住基カードの交付・携帯は希望者のみであるほか，独自利用サービスについても住民が選択でき，カード内には特に必要性がある場合を除き，システムにアクセスするための利用者番号以外の個人情報を記録しないこととされていることから，カード内に様々な個人情報が蓄積されることはない。

さらに，住基カードは，ＩＣカードの採用，暗証番号の設定，耐タンパー性の確保等の技術的なセキュリティ対策を講じている。

ｄ　以上のとおり，法の許容しないデータマッチングが行われる具体的危険は皆無である。

（ウ）　原告らは，原告らにおいてプライバシー権侵害の危険性について一応の主張・立証をなしたときは，被告らにおいて，相当の根拠を示して危険性のないことを主張・立証すべき旨主張するが，原告らの引用する最高裁平成４年１０月２９日第一小法廷判決は，本件とは訴訟類型を異にする事案に関するものである上，本件では，上記最高裁判決とは異なり，証拠の偏在も認められず，原子力関係訴訟とは被侵害利益の内容や侵害態様等を全く異にすることから，これらの裁判例と同様に考えることはできない。

なお，国家賠償請求に関しては，原告らの法的利益が現に侵害されていることが請求原因事実となるものであるから，プライバシー侵害の危

険性について立証責任の所在を論じる意味はない。

ウ　差止めの可否について

（ア）　仮に，自己情報コントロール権がプライバシーの権利の一内容に含まれるものであるとしても，プライバシーの権利は差止請求の根拠となるような排他的権利として認められない。

（イ）　そもそもプライバシーの権利が未だ憲法上の権利として判例上確立されているわけではなく，仮に権利性を認めたとしても，名誉権と同様の排他性を有する人格権ととらえ，差止請求を認容することはできない。

（２）　争点２（氏名権侵害の有無）について

（原告らの主張）

ア　氏名で呼称され，氏名で扱われることは，個人の尊厳を保障した憲法１３条で保障される国民の権利であり，人格権に内包される憲法上の権利と解すべきである。

イ　住基ネットは，原告らに住民票コードを付し，他から識別するために一律に番号を振っているが，これによって，１１けたの番号で区別される情報の一つのエリアに氏名欄があるにすぎないという事態が生じ，原告らを氏名ではなく，番号で取り扱うこととなってしまう。

ウ　したがって，住基ネットは，氏名権を侵害しているというべきである。

（被告らの主張）

ア　そもそも，原告らが主張する「氏名権」なるものを認める法文・判例上の根拠は全く存在せず，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。

イ　住民票コードは，特定の住民の本人確認を確実かつ効率的に行うために使用される１１けたの番号であり，氏名，住所，生年月日及び男女の別の４情報を電子計算機及び電気通信回線を用いて効率的に送信させるために

技術上新たに設けられた符号にすぎず，個人の人格的価値とは無関係である。また，住民票コードは，住民票の記載事項であって，人に対して番号を付しているものではない。

ウ　したがって，住民票コードの記載により，原告らの人格権も人格的利益も侵害したとはいえない。

（３）　争点３（公権力によって包括的に管理されない自由の侵害ないしその危険性の有無）について

（原告らの主張）

ア　公権力によって包括的に管理されない自由，すなわち，各行政機関において，それぞれが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おくことを拒絶する自由は，思想良心の自由，表現の自由といった個別的な人権保障の前提となるものであり，何ら他人の基本権を侵害するおそれがないことなどから，人格的自律の存在として自己を主張し，そのような存在であり続ける上で必要不可欠な利益であり，人格権に内包される権利として，憲法１３条の幸福追求権によって保障されているものと解すべきである。

イ　住基ネットは，国民全員の本人確認情報を，サーバに結合して一元化するものであり，すべての国民に重複しない１１けたの住民票コードが付されており，この住民票コードにより，各行政機関が個別に保有していた情報について，検索・照合等を行うことが容易となる。さらに，住基ネットの利用が可能な事務が今後無限定に拡大されていくことが容易に予想され，民間生活を含めた全生活分野において住民票コードが浸透していけば，本人確認情報と各行政機関が個別に保有していた情報とが有機的に結びつくことによって，行政機関は，個人情報を一元的に管理することが可能となるが，これは当該個人そのものを監視下・支配下におくことに他ならない。

ウ　よって，住基ネットは，国民に住民票コードという番号を付し，この番

号の下に個人の情報を一元的に集約・管理することに他ならず，公権力によって包括的に管理されない自由を侵害するものである。

（被告らの主張）

ア　そもそも，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。

イ　なお，原告らは，行政機関又はその構成員たる公務員が法令遵守義務を負うにもかかわらず，これを遵守しないことを前提に，大規模なデータマッチングや名寄せの危険を主張するものにすぎず，むしろ，これらの法令に基づく義務等に照らせば，原告らの人格権が侵害される具体的な危険は存在しない。

（４）　争点４（国家賠償法上の違法性の有無）について

（原告らの主張）

ア　被告らは，住基ネットの運用によって，上記のとおり憲法上の人権を侵害する違憲行為を行っており，その結果，原告らに精神的苦痛を与えているから，住基ネットの運用は，国家賠償法上違法との評価を受けるというべきである。

イ　また，政府は，改正住基法の施行にあたって，個人情報の保護に万全を期するための所要の措置を講じることが義務づけられた（改正住基法附則１条２項）。しかるに，政府は，所要の措置を講じることなく，改正住基法を施行させており，改正住基法の施行及び住基ネットの運用は違法である。その後個人情報保護法が成立したが，その内容からして何ら所要の措置を講じたとはいえないから，その違法性に変わりはない。

ウ　したがって，内閣等が，①所要の措置を講じないか又は講じることのできる見込みのないまま施行日を平成１４年８月５日とする政令を定めたこと，②所要の措置を講じないまま改正住基法を施行させたこと，③違憲の

改正住基法を廃止せず，又は運用を停止する相当の方策を講じていないことは，それぞれ国家賠償法上，違法な行為というべきである。

また，千葉県知事が，①市町村長に対して住民票コードを通知したこと，②本人確認情報を磁気ディスク等に保存したこと，③国の機関等に情報を提供したこと，④被告情報センターに対して本人確認情報処理事務を委任したこと，⑤被告情報センターへ本人確認情報を通知したことは，それぞれ国家賠償法上，違法な行為というべきである。

同様の理由により，被告情報センターが，①被告県から本人確認情報処理事務を受任したこと，②本人確認情報を磁気ディスク等に保存したこと，③国の機関等に情報を提供したことは，いずれも不法行為に当たるというべきである。

（被告らの主張）

ア　国家賠償法上の違法性が認められるためには，被告国及び県の公務員が個別の国民に対する職務上の法的義務に違反することが必要であると解すべきである。

原告らは，内閣による政令制定行為や千葉県知事による改正住基法の実施等を違法行為と主張するようであるが，これらの行為について違法性が認められるには，当該公務員が職務上通常尽くすべき注意を尽くすことなく漫然と当該行為をしたことが必要であるところ，行政機関には法令の違憲審査権はなく，法律を誠実に執行する義務を負うのであるから，法律の規定に従って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しているというべきである。

イ　また，所要の措置を講じていないとの点についても，改正住基法は，附則１条１項柱書において，公布の日から起算して３年を超えない範囲内において政令で定める日から施行すると定めており，政府は，公布の日から３年を超えない範囲で改正住基法を施行することが義務づけられていたも

のであるから，平成１４年８月５日に施行したことに何ら違法な点はない。しかも，政府がなすべき個人情報の保護に万全を期するための所要の措置とは，政府が立法機関ではないことから，個人情報の保護に関する法律案を提出する行為を指すところ，政府が所要の措置を講じたことは明らかである。

ウ　したがって，人格権及びプライバシー権の侵害の有無を論じるまでもなく，原告らが主張する行為については，国家賠償法上の違法性がないことは明らかである。また，同様の理由により，被告情報センターの行為が不法行為とならないことは明らかである。

・　争点５（損害額）について

（原告らの主張）

ア　住基ネットの運用により，原告らが被った精神的苦痛を慰謝するには，原告らそれぞれにつき，被告国については金１０万円を，被告県及び被告情報センターについては連帯して金１０万円をそれぞれ負担させるのが相当である。

イ　弁護士費用相当損害金として，原告らそれぞれにつき，被告国については金１万円を，被告県及び被告情報センターについては連帯して金１万円をそれぞれ負担させるべきである。

（被告らの主張）

争う。

第３　争点に対する判断

１　争点１（プライバシー権の侵害ないしその危険性の有無）について

（１）　認定事実

後掲各証拠及び弁論の全趣旨によれば，以下の各事実が認められる。

ア　住基ネットによる行政サービス等について

（ア）　広域交付・転出入手続の簡素化について

ａ　住基ネットの導入によって，住基カードの交付を受けている者は，転出の際に付記転出届を行った上，転入の際に住基カードを添えて転入届を出した場合には，転出証明書が不要となった（住基法２４条の２）。

ｂ　住基ネットを利用することにより，住所地の市町村長以外の市町村長に対しても，自己の属す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）。

（イ）　公的個人認証サービス

公的個人認証サービスとは，地方公共団体が，電子署名（デジタル文書において，作成者の特定や文書が改変されていないことを確認するために文書に行われる措置をいう。）が当該本人のものであることを地方公共団体が保証するサービスである。（電子署名に係る地方公共団体の認証業務に関する法律）

住基ネットは，公的個人認証サービスにおいて，電子署名の利用者の氏名・住所・性別・生年月日の変更又は死亡の事実が生じた場合に，その旨の情報を，失効情報として提供することに利用されている。（住基法３０条の８第３項）

（ウ）　行政機関内での本人確認等手続の省略

住基ネットが導入される以前は，国の機関等が，各種行政事務を行うために，年金の受給権者に対して現況届の提出を求めたり，届出人に住民票の写しの提出を求めたり，各市町村から住民票の提出を求めるなどして，現況の確認や本人確認等を行っていたが，住基法改正後は，本人確認情報の提供を受けることによってこれを行うことが可能となった。

イ　住基ネットにおけるセキュリティについて

（ア）　法令の規定等

都道府県知事及び指定情報処理機関は，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されている（住基法３０条の２９）。

本人確認情報の受領者も，受領した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（住基法３０条の３３第１項）。

ａ　目的外利用の禁止

都道府県知事は，住基法３０条の７第３項から６項まで，３０条の８第１項若しくは第２項又は３７条２項の規定により保存期間に係る本人確認情報を利用し，又は提供する場合を除き，通知に係る本人確認情報を利用し，又は提供してはならない（住基法３０条の３０第１項）。

指定情報処理機関は，住基法３０条の１０第１項の規定により委任都道府県知事の事務を行う場合を除き，通知に係る本人確認情報を利用し，又は提供してはならない（住基法３０条の３０第２項）。

本人確認情報の受領者は，その者が住基法の定めるところにより本人確認情報の提供を求めることができることとされている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，又は提供することができ，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（住基法３０条３４）。

ｂ　審議会

都道府県には本人確認情報保護審議会が，指定情報処理機関には本人確認情報保護委員会が設置されており，それぞれ本人確認情報の保護に関する事項を調査審議することができる（住基法３０条の９，１５）。

ｃ　守秘義務

指定情報処理機関の役員若しくは職員又はこれらの職にあった者は，本人確認情報処理事務に関して知り得た秘密を漏らしてはならず，違反行為には２年以下の懲役又は１００万円以下の罰金に処する旨の罰則が規定されている（住基法３０条の１７第１項，４２条）。

指定情報処理機関から住基法３０条の１１第１項の規定による通知に係る本人確認情報の電子計算機処理等の委託を受けた者若しくはその役員若しくは職員又はこれらの者であった者は，その委託された業務に関して知り得た本人確認情報の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漏らしてはならず，違反行為には同様の罰則が規定されている（住基法３０条の１７第２項，４２条）。

本人確認情報の電子計算機処理等に関する事務に従事する市町村の職員若しくは職員であった者又は住基法３０条の５第１項の規定による通知に係る本人確認情報の電子計算機処理等に関する事務に従事する都道府県の職員若しくは職員であった者は，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漏らしてはならず，違反行為には同様の罰則が規定されている（住基法３０条の３１第１項，４２条）。

市町村長又は都道府県知事から本人確認情報又は住基法３０条の５第１項の規定による通知に係る本人確認情報の電子計算機処理等の委託を受けた者若しくはその役員若しくは職員又はこれらの者であった者は，その委託された業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漏らしてはならず，違反行為には同様の罰則が規定されている（住基法３０条の３１第２項，４２条）。

本人確認情報の受領者は，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漏

らしてはならず，違反行為には同様の罰則が規定されている（住基法３０条の３５，４２条）。

都道府県知事又は指定情報処理機関の委託を受けて行う住基法３０条の５第１項又は３０条の１１第１項の規定による通知に係る本人確認情報の電子計算機処理等に関する事務に従事している者又は従事していた者は，その事務に関して知り得た事項をみだりに他人に知らせ，又は不当な目的に使用してはならない（住基法３０条の３２）。

本人確認情報の受領者の委託を受けて行う本人確認情報の電子計算機処理等に関する事務に従事している者又は従事していた者は，その事務に関して知り得た事項をみだりに他人に知らせ，又は不当な目的に使用してはならない（住基法３０条の３６）。行政機関個人情報保護法は，国の機関等の担当職員が正当な理由なく個人情報を提供した場合や不正な利益を図る目的で個人情報の提供又は盗用を行ったり，職務の用以外の用に供する目的で職権を濫用して個人の秘密を収集した場合に罰則を定めている（行政機関個人情報保護法５３条ないし５５条）。

d　住民票コードの利用制限

市町村長その他の市町村の執行機関は，法の定めるところにより本人確認情報の提供を求めることができることとされている事務の遂行のため必要がある場合を除き，何人に対しても，当該市町村の住民以外の者に係る住民票に記載された住民票コードを告知することを求めてはならない（住基法３０条の４２第１項）。

都道府県知事その他の都道府県の執行機関は，法の定めるところにより本人確認情報の提供を求めることができることとされている事務の遂行のため必要がある場合を除き，何人に対しても，住民票コードを告知することを求めてはならない（住基法３０条の４２第２項）。

指定情報処理機関は，住基法に規定す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，住民票コードを告知することを求めてはならない（住基法３０条の４２第３項）。

住基法別表第１の上欄に掲げる国の機関又は法人は，法の定めるところにより本人確認情報の提供を求めることができることとされている事務の遂行のため必要がある場合を除き，何人に対しても，住民票コードを告知することを求めてはならない（住基法３０条の４２第４項）。

民間部門においては，①第三者に対し，住民票コードの告知を求めること，②業として住民票コードが記載されたデータベースであって，記録された情報が他に提供されることが予定されているものを構成することが禁止されている。そして，①のうち業として行う行為に関し，その者に契約の申込をしようとする第三者若しくは申込をする第三者又は契約締結した第三者に対して住民票コードの告知を求めた場合及び②に違反した場合において，当該行為をした者が更に反復して違反行為をするおそれがあると認められるときは，当該行為をした者に対し，違反行為の中止等を勧告し，中止勧告に従わないときは都道府県の審議会の意見を聞いて，期限を定めて勧告に従うべきことを命ずることができ，この命令違反は刑罰の対象となる。また，上記勧告又は命令の措置に関し必要があると認めるときは，その者に対し，必要な事項に関し報告を求め，又は立ち入り検査をすることができ，その違反は刑罰の対象となる（住基法３０条の４３，３４条の２，４４条，４７条）。

ｅ　セキュリティ基準

施行規則の規定に基づき，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，以下「セキュリティ基準」という。）が定められている。

ｆ　チェックリストによる監査

市区町村は，平成１５年１月及び２月，総務省の要請に基づき「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。）」に基づいてセキュリティ対策の自己点検を実施し，総務省，各都道府県，被告情報センターは，その結果を踏まえて，技術的改善を指導した。

総務省は，平成１５年８月２５日の二次稼働に際して，１０８の市町村を選定し，システム運営監査を行い，チェックリストの記載内容の検証を実施した。

（イ）　技術的な防止策

ａ　住基ネットは，通信回線にＩＰ－ＶＰＮ（論理的に他の回線と隔離された専用回線）を採用するとともに，通信内容を暗号化した上，通信を行うごとに，意図した相手に接続されたことを相互に認証している。また，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通信を行っており，ＳＭＴＰ，ＨＴＴＰ，ＦＴＰ，Ｔｅｌｎｅｔ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。

ｂ　指定情報処理機関は，ＯＳのセキュリティホール及びコンピュータウイルスの発生情報を常時入手し，システムの影響度を確認した上で全団体にパターンファイル，セキュリティホール情報及び対応方法を通知している。また，指定情報処理機関は，ネットワーク内にファイアウォール，侵入検知装置を設置し，不正な通信の監視を行うほか，定期的にログの解析を行っている。

ｃ　住基ネットを利用するための端末機から，本人確認情報の即時提供

を受けようとする場合，住民票コードを入力するか，氏名及び住所を入力するか，又は氏名及び生年月日を端末機に入力しなければ，本人確認情報の提供を受けることができない。また，前方一致検索も可能であるが，その場合には氏名の先頭一文字及び住所全部，氏名全部及び住所の都道府県・市町村名を除いた先頭一文字，氏名の先頭一文字及び生年月日全部のいずれかを入力する必要があり，これらを入力しても，該当者が５０人を超えるときは本人確認情報の提供を受けられない。

d　住基ネットにおいて，端末機から本人確認情報データベースへアクセスするためには，住基ネットアプリケーションを起動する必要があるが，ＩＤカードと端末機の間で相互認証を行わなければ，住基ネットアプリケーションを起動することができない。また，ＩＤカードの種別により，システムの操作者ごとに，データ等へ接続できる範囲を限定している。

e　被告情報センターは，平成１５年１０月１０日から１２日の間に，品川区において，住基ネットとＣＳとの間に設置したファイアウォール，ＣＳと庁内ＬＡＮとの間に設置したファイアウォール及び庁内ＬＡＮ上のＣＳ端末に対し，ペネトレーションテスト（模擬攻撃）を実施したところ，いずれの機器についても不正侵入は成功せず，これを許すような脆弱性も発見されなかった。

（ウ）　住基カードについて

a　住基カードに記録された情報を読みとるためには，住基カードと住基ネット相互間の認証を行う必要がある。また，基本利用領域，公的個人認証サービス利用領域及び条例利用領域は，住基カード内部でそれぞれ独立しており，それぞれのシステムに割り当てられた領域以外の領域へ情報を記録すること，及び他の領域から情報を読みとること

はできない。

b　住基カードには，住基カード内の半導体集積回路から記録された情報を読みとろうとする行為に対し，これらを防止する仕組み（耐タンパー性）が採用されている。

c　住基カードは，市町村長が住民申請により交付するものであり，携帯が義務づけられることはない（住基法３０条の４４第３項）。

ウ　本人への情報開示等

住民は，都道府県知事又は指定情報処理機関に対し，磁気ディスクに保存されている自己に係る本人確認情報について，書面により，その開示を請求することができ，請求を受けた都道府県知事又は指定情報処理機関は，これを開示しなければならず，開示を受けた者から，書面により，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があったときは，遅滞なく調査を行い，その結果を通知しなければならない（住基法３０条の３７，４０）。

住民は，各都道府県の準備が整い次第，それぞれの個人情報保護条例によって，自己に係る本人確認情報の提供又は利用の状況に関する情報（本人確認情報提供状況）について開示を受けることができる。

エ　長野県侵入実験

（ア）　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システムへの不正アクセス及び住基ネットシステムからの本人確認情報漏えいの可能性を確認し，有効な対策を講ずるための資料を得ることを目的として侵入実験を行った。第１次調査は平成１５年９月２２日から１０月１日まで，阿智村，下諏訪町，波田町を対象として行われ，第２次調査は同年１１月２５日から同月２８日まで，阿智村を対象として行われた。

（イ）　実験の結果，既存住基サーバの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ため，庁内ＬＡＮに接続した調査用コンピュータから管理者権限で既存住基サーバにログインできた。また，既存住基サーバで使用されているＯＳ（オペレーティングシステム）の脆弱性を利用して，既存住基サーバの管理者権限を奪取した。

ＣＳセグメントに接続した調査用コンピュータから，ＣＳが使用しているＯＳの脆弱性を利用して，ＣＳの管理者権限を奪取した。そして，ＣＳで得られた情報を利用してＣＳ端末の管理者権限を奪取した。

（ウ）　他方，庁内ＬＡＮに接続した調査用コンピュータから，市町村が設置したファイアウォール越しに，ＣＳの管理者権限を奪取することはできなかった。また，インターネットからの攻撃に関しては，脆弱性は発見されなかった。

（２）　プライバシー権侵害の有無について

ア　原告らは，本人の同意なしに本人確認情報を住基ネットに流通させることそれ自体がプライバシー権を侵害すると主張し，仮にそうでないとしても，公権力を行使し，本人の意思に反してプライバシー情報を収集等をするためには，同意を得ることが困難であるという緊急性の要件，目的の正当性の要件，手段の必要不可欠性という要件を満たさなければならないところ，住基ネットはこれらの要件を満たしていないなどと主張する。

イ　そこで検討するに，情報処理技術の発展に伴い，多くの分野において大量の個人情報が収集等されている状況下においては，個人情報が不当な目的のために収集されたり，想定された本来の目的以外に使用されるなどすると，著しく私生活の平穏を害するなど不都合な結果を招くおそれがあるのであって，かかる不都合を防止するためには，みだりに個人情報を収集・管理・利用されない利益を法的にも保護に値する個人の利益として認めるのが相当である。そこで，自己に関する一定の情報について，みだりに収集等されない権利は，人格権の一内容として憲法１３条により保護され

る権利と解するのが相当である。

そして，本人確認情報は，それ自体は個人を識別するための比較的単純な情報であるということがいえるものの，みだりに開示等されることにより当該個人に不利益や不都合な結果が生じる場合があり得ることは否定し難いから，一律に保護を否定することは相当ではない。もっとも，本人確認情報は，個人を識別するためなどに利用する必要性が高く，一定範囲の他者には当然開示すべき情報であるといえることなどからすれば，その秘匿の必要性の程度は，一般的には必ずしも高くないといわざるを得ない。

そうすると，正当な目的のために必要かつ合理的な範囲で，公権力が本人確認情報の収集等を行うことは，公共の福祉による制約又は上記権利に内在する合理的な制約として許容されると解するのが相当である。

ウ　これを本件についてみるに，住基ネットでは，平成１７年４月１日時点において２７５の事務について本人確認情報の提供が行われているところ，これらの事務を行う際に本人確認情報を収集等する目的は，主として，正確な情報に基づき本人確認等をすることにより，これらの事務を誤りなく，かつ効率的に遂行することにあると解されるところ，その目的は正当であると認められる。

そして，本人確認情報を提供する際に本人の同意を要すると解した場合，本人に本人確認情報を提供しない自由を認めることとなるが，それでは行政事務の正確性及び効率性等を確保することは到底困難となってしまうのであって，住基法で定められた目的のため，国の機関等が，本人の同意を得ることなく本人確認情報の提供を受けることは，上記の目的達成のために必要かつ合理的であると認められる。

したがって，住基ネットの利用が可能な２７５の事務について，国の機関等に対して本人確認情報の提供がなされること自体は，原告らの本人確認情報をみだりに収集等されない権利を侵害するものとはいえない。

エ　この点に関し，原告らは，プライバシー情報の収集等に際しては，プライバシーに対してより制限的にならない態様でしか許されないなどと主張し，ネットワーク化され，デジタル情報の形でなされるという本人確認情報の提供方法について，特に問題である旨主張しているものと解される。

しかし，情報提供が書面の形でなされるのか，磁気媒体等を用いるのか，あるいは電気通信回線（ネットワーク）を利用するのかなど，提供方法の違いは，本人確認情報の漏えいや不当なデータマッチングなどの行為が行われる可能性の程度に差異が生じ得ることが考えられるものの，情報が提供されること自体は何ら異ならないから，直ちに上記に認めた自己の情報についてみだりに収集等されない権利の侵害の問題を生ずるものではないというべきである。

もちろん，いかなる方法で情報提供を行うかについての選択権が本人に認められるか否かは別途問題となり得るが，これが法的保護に値する利益か否かについては，情報提供の方法いかんによって，情報の漏えいや不当なデータマッチングなどがなされる危険性にどの程度の差違があるかを検討する必要があるから，その危険性の程度に関する判断と合わせて検討するのが相当である。

（３）　プライバシー権侵害の危険性の有無ないしその程度について

ア（ア）　原告らは，住基ネットには，本人確認情報の外部への漏えいや，不当なデータマッチング等により，原告らのプライバシー権を侵害する具体的危険性があるので，住基ネットからの離脱請求が認められるべきであるなどと主張する。

（イ）　そこで検討するに，個人情報の目的外利用や漏えいは，当該個人の私生活上の平穏を害する場合があり得るなど，個人情報保護の観点から望ましくない行為であるから，個人情報を取り扱う者としては，できるだけ目的外利用や漏えいの危険性が低い方法で慎重に取り扱うべきで

あることは疑いの余地がない。これに反して目的外利用や漏えい等の危険性が高い方法で個人情報を取り扱っている場合，自己に関する情報の保護について不安を感じる者があることも無理からぬことであるから，その危険性の程度によっては，自己に関する情報の収集等を事前に差し止め得るものと解すべきである。

もっとも，このような危険性については，抽象的なものから，具体的根拠に基づく差し迫ったものまでその程度は様々であり，これらのすべての場合を法的に保護し，これを差止めの根拠となる権利として認めるのは，権利の明確性及び権利保護の適格性の観点から相当ではなく，その危険性が具体的・合理的な根拠を有するものである場合に限り，法的保護に値するものとして，人格権に基づきこれを差し止めることができるものというべきである。

（ウ）　そこで，本人確認情報の提供方法が，その外部への漏えいや不当なデータマッチング等がなされる相当の具体的な蓋然性が認められるものである場合には，当該情報提供方法による本人確認情報の提供を差し止めることができるものと解するのが相当である。

イ　情報漏えいの危険性について

（ア）　まず，外部からの不正アクセスの危険性について検討する。

上記に認定した長野県における侵入実験等によれば，市町村によっては，当該市町村の庁内ＬＡＮに不正侵入される危険性があり，当該市町村内の個人情報が改ざん等される危険性があることを否定することはできない。もっとも，ある市町村のネットワークから都道府県のネットワークや他の市町村等のネットワークへさらに侵入するためには，被告情報センター設置のファイアウォール越しに侵入を試みる必要があるところ，このような方法で他の市町村の管理するサーバーの管理者権限を奪取することは，他の市町村のＣＳに不正にアクセスする方法としては考

え難い方法であることなどからすれば，ある市町村の庁内ＬＡＮ内に不正侵入されたとしても，他の市町村等のネットワーク内にまで直ちに不正侵入し得るとは認められない。

また，ＣＳ端末の管理者権限を取得しても，住基ネットアプリケーションを起動するためには，少なくともＩＤカードが挿入されている必要があることから，ある市町村のネットワーク内に不正侵入した者が，他の市町村に居住する住民の本人確認情報を検索ないし閲覧するためには，ＩＤカードが挿入されている間に，侵入者が住基ネットアプリケーションを操作し，かつ，原告らの氏名及び住所（ないしその一部）又は住民票コードを入力する必要があり，これらの条件を満たして初めて被告情報センターの管理する全国サーバ内に保存されている原告らの本人確認情報を閲覧し得るというのにとどまる。しかも，即時提供方式によるデータの検索については，上記に認定したとおり，照会条件の限定がされていることからすれば，模索的に本人確認情報を収集することはほとんど不可能であるなど，意図した個人の本人確認情報を入手することは相当困難であるといえる。

（イ）　次に，関係者による権限濫用の危険性について検討する。

上記認定事実によれば，住基ネットにおいては，本人確認情報の照会条件が限定されており，不正取得の方法が限られていること，住基ネット上の本人確認情報に関する秘密の漏えいについて，罰則付きの禁止規定が定められていること，アクセスログを保存・解析することにより不正行為発覚の可能性を高めていることなど，権限濫用に対しては，一定の抑止策が採られているということができる。

（ウ）　そうすると，関係者が，住基法等の禁止規定に違反して権限を濫用し，原告らの本人確認情報を漏えいする可能性は必ずしも高いとはいえない。

ウ　データマッチングの危険性について

（ア）　住基法３０条の３４の規定により，本人確認情報の受領者が，これを法で定められた目的外に利用することは禁止されている。そして，行政機関の職員がこれに反して，専らその職務の用以外の用に供する目的で個人の秘密に属する事項が記録された文書，図画又は電磁的記録を収集した場合には刑罰の対象となる（行政機関個人情報保護法５５条）。本人確認情報の提供を受けた関係職員が，知り得た本人確認情報に関する秘密を漏らした場合にも，刑罰の対象となる（住基法４２条）。

（イ）　また，都道府県には本人確認情報保護審議会が，指定情報処理機関には本人確認情報保護委員会が設置されており，これらを活用することによって，本人確認情報の目的外利用を監視し得る（住基法３０条の９，１５）。さらに，住民は，自己の本人確認情報の提供状況について開示を受けることができるが，これにより不正利用の有無について，調査の端緒とすることができる。

（ウ）　以上によれば，個人に関する情報を全面的にデータマッチングすることは法で禁止されており，これを担保するための措置も一応講じられていると認められるから，これらの法に違反して不当なデータマッチングが行われる可能性は高いとはいえないというべきである。

エ　したがって，住基ネットにおいて，原告らの個人情報が漏えいしたり，住民票コードをマスターキーとした不当なデータマッチングが行われる可能性は高いとはいえず，これらが行われる相当の具体的蓋然性があると認めることはできないのであって，これらのおそれがあることを理由とする原告らの差止請求も認められないことになる。また，以上に述べたところからすれば，本人確認情報の提供方法に関する選択権についても，法的保護に値するとまではいえず，これについて原告らの同意を得ていないことが違法であるともいえない。

（４）　したがって，住基ネットに関する法の諸規定及び住基ネットを運用することがプライバシー権を侵害し，違憲・違法であるとはいえず，争点１に関する原告らの主張は，いずれも採用できない。

２　争点２（氏名権侵害の有無）について

（１）　原告らは，住民票コードを原告らに付することにより，原告らを番号で扱うことは，氏名で呼称され，氏名で扱われるべき個人の権利を侵害するものである旨主張する。

（２）　しかし，住民票コードは，前記前提となる事実のとおり，住民基本台帳に記載された個人情報を効率的に送信等するため無作為に作成された技術上の数値であり，本人の請求によっていつでも変更できるものであって，氏名に代わる呼称として扱われるものではないから，住民票コードが住民票の記載事項とされたことは，原告らの氏名権ないし人格的権利を何ら侵害するものではないというべきである。なお，住民票コードは，住基ネットにおいて，本人確認情報を正確に処理するために使用されるものであり，事務処理上の必要性があるものと認められる。

（３）　したがって，争点２に関する原告らの主張は，採用できない。

３　争点３（公権力によって包括的に管理されない自由の侵害ないしその危険性の有無）について

（１）　原告らは，住民票コードを利用して原告らに関する個人情報を一元的に管理することが，公権力によって包括的に管理されない自由を侵害するものであるなどと主張する。

（２）　しかしながら，そもそも，住基法には原告らの個人情報を一元的に管理する旨の規定は存しない。また，原告らのいう公権力による包括的な管理とは，主として原告らに関する個人情報の全面的なデータマッチングが行われること，ないしはこれが行われる危険性のある状況をいうものと解されるところ，争点１に対する判断において述べたとおり，原告らの個人情報に関

し，包括的なデータマッチングが現になされているとは認められず，これが行われる相当の具体的蓋然性があるとも認められない。

よって，原告らの主張はその前提を欠くというべきである。

（３）　したがって，争点３に関する原告らの主張は，採用できない。

４　争点４（国家賠償法上の違法性の有無）について

（１）　原告らは，住基ネットの運用が違憲であること，政府が所要の措置を講じていないことなどから，被告らの行為が違法であるなどと主張する。

（２）ア　しかし，上記に述べたところからすれば，住基法の諸規定が憲法に違反するとはいえず，住基法に基づく被告らの行為が違法であるということはできない。

イ　また，所要の措置を講じていないとの点についても，改正住基法の附則１条１項及び同条２項の文理等を検討すれば，所要の措置を講じたか否かに関係なく，公布の日から３年以内に改正住基法を施行することが政府に義務づけられていたと解すべきである。

そうすると，所要の措置を講じないまま改正住基法を施行したとしても，これを違法と解する余地はないから，所要の措置の内容について検討するまでもなく，原告らの主張は失当である。

（３）　したがって，争点４に関する原告らの主張は，採用できない。

第４　結論

よって，原告らの本訴請求は，その余の争点について判断するまでもなく，いずれも理由がないからこれを棄却することとし，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。

千葉地方裁判所民事第２部

裁判長裁判官　　小　　磯　　武　　男

裁判官　　田　　原　　美　奈　子

裁判官　　吉　野　内　　謙　　志