平成１９年２月１日判決言渡　同日原本交付　裁判所書記官

平成１７年(ネ)第６３１号　住民基本台帳ネットワーク差止等請求控訴事件（原審・名古屋地方裁判所平成１５年(ワ)第４９１号［甲事件］，平成１６年(ワ)第１５９３号［乙事件］）

口頭弁論終結日　平成１８年１０月１１日

判　　決

当事者の表示　　別紙当事者目録記載のとおり

主　　文

本件控訴をいずれも棄却する。

控訴費用は控訴人らの負担とする。

事実及び理由

第１　控訴の趣旨

１　原判決を取り消す。

２　被控訴人愛知県は，

(1)　住民基本台帳法３０条の７第３項の別表第１の上欄に記載する国の機関及び法人に対し，控訴人らに関する本人確認情報（控訴人らの氏名，住所，生年月日，性別の４情報及び控訴人らに付された住民票コード並びにこれらの変更情報）を提供してはならない。

(2)　被控訴人財団法人地方自治情報センターに対し，控訴人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)　被控訴人財団法人地方自治情報センターに対し，控訴人らに関する本人確認情報（控訴人らの氏名，住所，生年月日，性別の４情報及び控訴人らに付された住民票コード並びにこれらの変更情報）を通知してはならない。

(4)　控訴人らに関する本人確認情報（控訴人らの氏名，住所，生年月日，性別の４情報及び控訴人らに付された住民票コード並びにこれらの変更情報）を，

保存する住民基本台帳ネットワークの磁気ディスク（これに準ずる方法により一定の事項を確実に記録しておくことができるものを含む。以下同じ。）から削除せよ。

3　被控訴人財団法人地方自治情報センターは，

(1)　被控訴人愛知県から受任した控訴人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)　控訴人らに関する本人確認情報（控訴人らの氏名，住所，生年月日，性別の４情報及び控訴人らに付された住民票コード並びにこれらの変更情報）を，保存する住民基本台帳ネットワークの磁気ディスクから削除せよ。

4　被控訴人愛知県は，控訴人らに対し，各１１万円及びこれに対する控訴人（１審甲事件原告）らについては平成１５年２月２０日から，控訴人（１審乙事件原告）らについては同年５月２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　被控訴人国は，控訴人らに対し，各１１万円及びこれに対する控訴人（１審甲事件原告）らについては平成１５年２月２１日から，控訴人（１審乙事件原告）らについては同年５月７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。

6　訴訟費用は１，２審とも被控訴人らの負担とする。

7　仮執行宣言

第２　事案の概要

1　本件は，平成１１年法律第１３３号による改正後の住民基本台帳法に基づき設置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。）は，控訴人らの人格権，プライバシー権，公権力による包括的管理からの自由を侵害し，あるいは侵害する危険性を有するものであるとして，愛知県住民である控訴人らが，①被控訴人愛知県及び被控訴人財団法人地方自治情報センター（以下「被控訴人センター」という。）に対して，控訴人らの本人確認情報に関す

る住基ネットの運用の差止めを求めるとともに，②被控訴人国及び被控訴人愛知県に対し，国家賠償法（以下「国賠法」という。）１条に基づき，損害賠償（訴状送達の日の翌日から支払済みまで民法所定年５分の割合による遅延損害金を含む。）を求めたところ，原審が控訴人らの請求を全部棄却したため，これに不服である控訴人らが控訴した事案である。

2　前提となる事実（末尾に証拠等を掲記したものを除き，当事者間に争いがない。）

(1)　当事者

ア　控訴人らは，それぞれ肩書住所地に居住し，住民登録をしている者である（甲２ないし４，甲２２の１ないし９）。

イ　被控訴人センターは，地方公共団体における電子計算組織による情報処理を推進し，地方行政の近代化に寄与することを目的として昭和４５年５月１日に設立された財団法人である。

(2)　住民基本台帳法

ア　住民基本台帳法は，市町村（特別区を含む。以下同じ。）において，住民の居住関係の公証，選挙人名簿の登録その他の住民に関する事務の処理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（以下「住基台帳」という。）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する法律である（同法１条）。

イ　住民基本台帳法は，平成１１年８月１８日，同年法律第１３３号の住民基本台帳法の一部を改正する法律（以下「改正法」といい，同法による改正後の住民基本台帳法を「住基法」という。また，改正前の住民基本台帳法を「旧住基法」という。）により改正され，住基法のうち，指定情報処理機関の指定（住基法３０条の１０第１項），住民票コードの指定（住基

法３０条の７第１，２項）等に係る規定は，同年１０月１日に，住民票コードの記載（住基法３０条の２），電気通信回線を通じた本人確認情報の通知（住基法３０条の５），本人確認情報の提供（住基法３０条の６）に係る規定は，平成１４年８月５日に，住民票写しの広域交付（住基法１２条の２），転出転入特例（住基法２４条の２），住民基本台帳カード（住基法３０条の４４。以下「住基カード」という。）等に係る規定は，平成１５年８月２５日にそれぞれ施行された（改正法附則１条１項，平成１１年政令第３０２号，平成１３年政令第４３０号，平成１５年政令第２０号）。

(3) 住基ネットの概要

ア 住基ネット

住基ネットは，地方公共団体の共同システムとして，住基台帳のネットワーク化を図り，それまでは各市町村内で利用されてきた住基台帳の情報を共有することにより，全国的に特定の個人情報の確認ができる仕組みを構築し，市町村の区域を越えて住基台帳に関する事務処理を行うものである。

イ 本人確認情報

住民票の記載事項のうち，氏名，出生の年月日，男女の別及び住所（以下，これらの情報を単に「４情報」ということがある。），住民票コード並びに住民票の記載等に関する事項で政令で定めるものを「本人確認情報」という（住基法３０条の５第１項，７条１ないし３号，７号，１３号）。政令は，住民票の記載等に関する事項として，①住民票の記載又は消除を行った旨並びにその事由及びその事由の生じた年月日，②４情報の記載の修正を行った旨並びにその事由及びその事由の生じた年月日，③住民票コードの記載の修正を行った旨，その事由及びその事由の生じた年月日並びに修正前住民票コードを定めている（住基法施行令３０条の５）。具体的

には，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），異動年月日，異動前の本人確認情報がこれに当たる（以下，これらを「変更情報」という。）。

ウ　住民票コード

(ア)　住民票コードは，無作為に作成された１０桁の数字と１桁の検査数字（住民票コードを電子計算機に入力するときの誤りを検出することを目的として，総務大臣が定める算式により算出される数字）からなるものであり，全国を通じて重複しないように指定されている（住基法施行規則１条）。

(イ)　都道府県知事は，総務省令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（なお，住基法３８条１項により，政令指定都市においては，政令で定めるところにより，区を市と，区の区域を市の区域と，区長を市長とみなすこととされている。）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，これを当該市町村長に通知する（住基法３０条の７第１項）。

上記の指定及び通知について，都道府県知事は，総務大臣の指定する者（以下「指定情報処理機関」という。）に行わせることができる（住基法３０条の１０第１項柱書，１号）。総務大臣は，被控訴人センターを指定情報処理機関に指定した。

(ウ)　市町村長は，平成１１年法律第１３３号の施行日に，現に住基台帳に記録されている者に係る住民票に，他の住民の住民票に記載する住民票コードと異なる住民票コードを選択して記載するものとされ（住基法附則３条），住民票コードを記載したときは，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しなければならない（住基法附則５条）。

(エ) 市町村長は，住民票の記載をする場合には，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ものとする（住基法３０条の２第１項）。

また，市町村長は，新たにその市町村の住基台帳に記録されるべき者につき住民票の記載をする場合において，その者がいずれの市町村においても住基台帳に記録されたことがない者であるときは，その者に係る住民票に，他の住民の住民票に記載する住民票コードと重複しない住民票コードを記載するものとし（住基法３０条の２第２項），住民票コードを記載したときは，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しなければならない（住基法３０条の２第３項）。

(オ) 住基台帳に記録されている者は，住基台帳を備える市町村の市町村長に対し，住民票に記載されてい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第１項）。

エ　住基ネットの構成

市町村には，既存の住基台帳電算処理システム（以下「既存住基システム」という。）のほか，既存住基システムと住基ネットとを接続するコミュニケーションサーバ（以下「ＣＳ」という。）が設置され，本人確認情報が既存住基システムからＣＳに伝達されて保存されている。都道府県には，都道府県サーバが，また，指定情報処理機関には，全国サーバ及びコールセンターが設置され，全国サーバ，都道府県サーバ及びＣＳは，いずれも専用交換装置を介して専用回線で接続しており，全国サーバは，国の機関等のサーバとも専用回線で接続している。既存住基システムとＣＳとの間，都道府県サーバと既存の庁内ＬＡＮとの間には，それぞれファイアウォール（以下「ＦＷ」という。）が設置され，ＣＳと都道府県サーバとの間，都道府県サーバと全国サーバとの間，全国サーバと国の機関との間

には，いずれも指定情報処理機関が監視するＦＷ（以下「指定情報処理機関ＦＷ」という。）が設置されている。指定情報処理機関は，構成機器の稼働状況を監視し，指定情報処理機関ＦＷを２４時間監視している。

オ　本人確認情報の保存・送信

市町村長は，住民票の記載，消除又は４情報及び住民票コードの全部若しくは一部について記載の修正を行った場合には，当該住民票の記載に係る本人確認情報を，都道府県知事に通知する（住基法３０条の５第１項)。都道府県知事は，指定情報処理機関に国の機関・法人等への本人確認情報の提供等の本人確認情報処理事務を行わせることができ（住基法３０条の１０第１項)，この場合，当該都道府県知事は，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)。

都道府県知事及び指定情報処理機関は,総務省令で定めるところにより，本人確認情報を磁気ディスクに記録し，これを当該通知の日から政令で定める期間（原則は５年間）保存しなければならない（住基法３０条の５第３項，３０条の１１第３項，住基法施行令３０条の６)。

カ　本人確認情報の提供及び利用

(ｱ)　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には，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)。

a　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，政令で定めるところにより，保存期間に係る本人確認情報（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であって同条３項の規定による保存期間が経過していないものをいう。）を提供する（住基法３０条の７第３項)。

b　都道府県知事は，当該都道府県の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又は当該都道府県の区域内の市町村の市町村長から住基台帳に関する事務の処理に関し求めがあったときには政令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執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときには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)。

c　都道府県知事は，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又は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政令で定めるところにより，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に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)。

d　都道府県知事は，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住基法別表第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又は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基台帳に関する事務の処理に関し求めがあったときには政令で定めるところにより，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には

条例で定めるところにより，当該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）。

e　都道府県知事は，住基法別表第５に掲げる事務を遂行するとき，条例で定める事務を遂行するとき，本人確認情報の利用につき当該本人確認情報に係る本人が同意した事務を遂行するとき又は統計資料の作成を行うときには，保存期間に係る本人確認情報を利用できる（住基法３０条の８第１項）。

f　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）。

g　都道府県知事は，住基法３０条の７第１項の規定による住民票コードの指定及びその通知，同条２項の規定による協議及び調整，同条３項の規定による本人確認情報の別表第１の上欄に掲げる国の機関及び法人への提供，同条４項の規定による本人確認情報の別表第２の上欄に掲げる区域内の市町村の執行機関及び同項第３号に規定する当該都道府県の区域内の市町村の市町村長への提供，同条５項の規定による本人確認情報の別表第３の上欄に掲げる他の都道府県の執行機関及び同項３号に規定する他の都道府県の都道府県知事への提供，同条６項の規定による本人確認情報の別表第４の上欄に掲げる他の都道府県の区域内の市町村の執行機関及び同項３号に規定する他の都道府県の区域内の市町村長への提供並びに住基法３７条２項の規定による本人確認情報に関する資料の国の行政機関への提供につき，指定情報処理機関に行わせることができる（住基法３０条の１０第１項。以下，委任を行った都道府県知事を「委任都道府県知事」という。）。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３項)。

(イ) 本人確認情報等の通知及び提供は，総務省令の定めるところにより，原則として相互の電子計算機間を電気通信回線を通じて送信することにより行う（住基法３０条の５第２項，３０条の７第７項，３０条の１１第２，４項)。

(ウ) 平成１４年１２月，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，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）が成立し，このうち，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により，住基法別表第１ないし第５が改正され，住基ネットを利用することが可能な事務は，従来の９３事務に１７１事務が追加されて２６４事務となり，さらに，信託業法附則５８条（平成１６年法律第１５４号）等により２７５事務となった（平成１７年４月１日現在)。

キ 住基カード

住基台帳に記録されている者は，その者が記録されている住基台帳を備える市町村の市町村長に対し，自己の住基カード（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）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，住基カードを，条例の定めるところにより，条例に規定する目的のために利用することができる（住基法３０条の４４第８項)。

ク 住基ネットの運用開始

(ア) 控訴人らの居住する各市町村（以下「各自治体」という。）は，住基

法に基づき，各自治体がそれぞれ有し，データベース化している住民票情報を入力し，控訴人らに関する個人情報が記録された既存の電子計算機を，総務省が全国市町村に統一仕様で配布した住基ネットシステム専用のＣＳに接続し，これを電気通信回線を通じて被控訴人愛知県が使用している電子計算機に接続した。.

各自治体と各被控訴人間の住基ネットワークシステムは，準備が完了し，平成１４年７月２２日から仮運用がされ，同年８月５日から本運用が開始された。

(イ) 愛知県知事の委任を受けた被控訴人センターは，同県下の市町村に対して１１桁の数字からなる住民票コードを指定し，各自治体は，それぞれ，住民票コードを各控訴人の住民票に記載し，平成１４年８月５日以降，控訴人らに対し，郵便等で，住民票コードを通知した。

(ウ) 以上の住基ネットの構築の結果，各自治体，被控訴人愛知県，被控訴人センターは，控訴人らの本人確認情報を被控訴人らが運用するコンピュータネットワーク上において保有することとなり，他の都道府県，その区域内にある市町村，国の一定の機関・法人などは，控訴人らの同意なく，本人確認情報の提供を受けることができることとなった。

3　争点

(1) プライバシー権侵害に基づく差止請求の可否

(2) 人格権侵害に基づく差止請求の可否

(3) 公権力から包括的に管理されない自由の侵害に基づく差止請求の可否

(4) 損害賠償請求の可否

4　争点に関する当事者の主張

(1) 争点(1)（プライバシー権侵害に基づく差止請求の可否）について

（控訴人らの主張）

ア　プライバシー権について

(ア) プライバシー権は，憲法１３条によって保障された基本的人権である。そして，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，私生活の平穏や個人の人格的自律を守るためには，プライバシー権を，「みだりに収集，開示されないという限度での法的利益」と捉えるだけでは十分でなく，自己に関する情報の他者への開示の可否及び利用，提供の可否を自分で決める権利，すなわち自己情報コントロール権を重要な一内容として含むものと解すべきである。この自己情報コントロール権は，自己の情報について，①収集・取得，②保有・利用，③開示・提供を自分でコントロールする権利と，派生的には，④自己の情報の開示請求権・訂正請求権を含むものである。

(イ) 住基ネット上を流通する本人確認情報のうちの４情報は，個人に関する最も基本的な情報であり，国民のプライバシー意識の高まった現在，秘匿性は著しく高まっているものである。また，住民票コードは，その番号のみをもってすれば簡便かつ正確に本人確認を行いうる機能・性質を有し，この住民票コードが記録されたデータベースが作成された場合には，特定個人の個人情報について，正確無比かつ簡便に検索や「名寄せ」（各行政機関や自治体が保有する特定個人に関する情報を集積すること。）を行うことを可能とするものであるから，これを秘匿し，保護する必要性の極めて高い情報である。更に，変更情報は，婚姻，離婚，養子縁組，離縁，氏名の変更，戸籍訂正等の身分上の重要な変動があったことを推知させるものであるから，プライバシーの核心に触れる内容を持つ重要な情報である。そして，これらの本人確認情報は，住基ネット上を一体となって流通させられ，ネットワーク上で共有されていることから，その要保護性は極めて高いというべきであり，自己情報コントロール権による保護の対象となるものと解すべきである。

イ　住基ネットによりプライバシー権が侵害されていること

住基ネット上を流通している本人確認情報は，控訴人らが自己の居住する地方自治体が利用するものとして当該自治体に提供したものである。ところが，住基ネットの運用によって，控訴人らの承諾のないままこれらの個人情報が流通させられており，控訴人らは，これらの情報の提供先や提供先においていかに利用されているかを知ることはできないのである。

したがって，住基ネットにより控訴人らの本人確認情報を自己の居住する市町村以外の機関に通知や提供をする形で流通させることは，それ自体により，控訴人らが有している本人確認情報に対する自己情報コントロール権を侵害していると解すべきである。

ウ　住基ネットによりプライバシー権の侵害の危険性があること

(ア)　不正閲覧・漏えい等の危険性

a　住基ネットによって，全国の都道府県，市町村及び被控訴人センターのコンピュータが接続されたことにより，ハッカー等がシステムに侵入し，控訴人らの個人情報を不正閲覧，取得及び改ざんする危険性や，住基ネット運用従事者等による情報漏えいや目的外利用等の現実的危険が生じている。

b　長野県は，住基ネットの安全性に関して，平成１５年９月２２日から同年１０月１日まで，下伊那郡阿智村（以下「阿智村」という。），諏訪郡下諏訪町（以下「下諏訪町」という。），東筑摩郡波田町（以下「波田町」という。）を対象に第１次調査を行い，同年１１月２５日から同月２８日まで，阿智村を対象に第２次調査を行った（以下，これらの調査を一括して，以下「長野県侵入実験」という。）。その結果，①ＣＳ端末のＯＳの管理者権限の略奪の危険性が存すること，②既存住基台帳データに対する不正アクセスの危険性が存すること，③既存住基台帳データベースの不正書き換えにより，住基ネット上の本人確認情報の改ざんの危険性が存すること，④本人確認情報提供先

における不正閲覧・漏えい等の危険性が存することが明らかとなった。

c　しかも，個人情報の漏えいについては，現実にも以下のような事故が発生している。

(a)　北海道斜里町事故

平成１８年３月，北海道斜里町（以下「斜里町」という。）職員が自宅の個人用パソコンに斜里町の保有する業務資料データを保存し，その後ファイル交換ソフト「Winny」をインストールしたところ，暴露ウイルスに感染し，上記データが「Winny」のネットワーク上に流出した（以下「斜里町事故」という。）。

(b)　北海道帯広市事故

平成１５年８月２１日から平成１６年１月１３日までの間に，一般事務を担当する北海道帯広市（以下「帯広市」という。）職員が，「宛名管理システム」によって表示された宛名情報を閲覧した。また，平成１７年６月１８日から同年１０月１２日までの間に，帯広市嘱託職員が，住基台帳の情報が入った既存住基システムの端末を，業務以外目的で閲覧していた（以下，これらを「帯広市事故」という。）。

(c)　福島県塙町事故

平成１６年９月１３日，福島県塙町（以下「塙町」という。）が，住民票コードが記載された名簿を行政区長の会合で配布した（以下「塙町事故」という。）。

d　住基ネットシステムの現場における安全管理を任されている全国の自治体においては，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存在している。自治体によっては，住基ネ

ットとインターネットが物理的に接続されていたり，重要機能室が設置されていなかったり，重要機能室への入退室が何ら管理されていなかったり，インターネットに接続している庁内ＬＡＮにＣＳ端末を設置しているなどの問題をかかえており，また，自治体のＣＳ及びＣＳ端末のセキュリティパッチ当ては極めて遅く，ウィルス対策及びセキュリティホール対策も不十分な状況にある。そもそも，いまだに，安全対策の第一歩である「プライバシーポリシー」すら制定せず，「個人情報保護条例」も制定していない自治体すら存するのである。それにもかかわらず，住基ネットの端末は全てネットワーク化されているため，そのうちどこか１か所が脆弱で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・構造的な脆弱性が存している。

(イ) データマッチングの危険性

住民票コードの下に，国の機関等の各データベースの個人情報が統一的に作られた場合，この番号をマスターキーとして，データマッチングすることは極めて容易かつ確実となる。すなわち，住民票コードを用いることにより，国の機関等の各事務ごとに個別的に作成され保有されているデータベースから，その者固有の番号で各個人の個人情報を名寄せして，データマッチングできることになるため，氏名，生年月日等で名寄せをしてデータマッチングするよりも，その作業は極めて容易となり，かつ確実となるのである。

さらに注意しなければならないことは，現在，国家機関のデータベースやネットワークの「最適化計画」が急ピッチで進められていることである。これは，これまで省庁ごとに（省庁内でも事務ごとに）互換性のないデータベースやネットワークが作られていたもの（いわゆるレガシーシステム）を，オープンシステム化して，霞が関ＷＡＮやＬＧＷＡＮを使って，省庁を越えて共通利用が可能なようにデータベースを共通化

し，ネットワークも共通化しようという計画である。この「最適化計画」は，国家プロジェクトとして強力に推進されており，既に各省庁の計画はできあがり，この２，３年程度の間にシステムが構築されようとしている。これが完成すれば，これまで，省庁ごとに互換性がないシステムであったことが障害となってデータマッチングの危険性から事実上守られていた国民の個人情報は，コンピュータネットワークを用いて，システム的にも極めて容易にマッチングを行い得る状態に置かれるのである。まさに，この意味において，住基ネットシステムの構築，運用は，「国民総背番号制度」への第一歩を踏み出したものであり，国民が，行政によって管理・監視される社会を招来する危険性の高いものであるといわなければならない。

(ウ) 保護措置の不十分性

a ＯＥＣＤ（経済協力開発機構）理事会は，１９８０年に，「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」を採択し，その中で個人情報の保護に関する原則（ＯＥＣＤ８原則）を定めている。この原則は，以後個人情報の保護に関し，国際的な基準とされてきたものであり，保護されるべきプライバシーの内容を，情報主体が自己の個人情報をコントロールする権利（自己情報コントロール権），自分の情報について自分で決定する権利（自己情報決定権）であることを前提とするものであるとされている。しかし，ＯＥＣＤ８原則が定められた１９８０年以後，データベースのさらなる巨大化やコンピュータネットワークを用いた情報管理技術の発展は著しく，このような社会状況の中においては，データマッチングの危険性の増大など，個人情報の保護は，ＯＥＣＤ８原則ではもはや十分ではないと指摘されているところである。ところが，住基ネットは，現在ではやや時代遅れともいい得るＯＥＣＤ８原則をも満たし

ていないものであり，住基ネットにおいては，個人情報の保護のための十全な措置は講じられていないといわざるを得ない。

b　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，あるいは１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７割ないし９割は，内部の者の関与によるものであるといわれており，庁舎内に存したパソコンの盗難例も数多く報道されている。従前の住基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り，いずれも，規定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なされてきたものである。また，民間利用の禁止等についても，本人や家族が住民票コードを告知することを許容しており，同禁止を担保する制度もないことから，いくらでも抜け道が存在するものであり，現に，住基ネットの運用開始早々，銀行などの金融機関において，利用者に住民票コードの告知を求めるという違法行為が大々的に行われているのである。

したがって，住基法上の禁止規定や制限条項，さらには公務員に対する守秘義務，罰則が設けられているというだけでは，目的外利用や情報の漏えい等の防止の担保とは決してならないものである。

なお，改正法は，附則１条２項によって，「個人情報保護の万全を期するための所要の措置」を講じることを義務付けており，この所要の措置を講じることによって，国民のプライバシーの権利の侵害を防止するものとしている。しかし，改正法が施行された際にはこの措置は何ら講じられていなかったし，その後成立した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。）及び行政機関の保有する個人情報の保護に関する法律（以下「行政個人情報保護法」という。）は，住基ネットの運用に関し，プライバシーの保護について万全の措置であるとは到底いい得ないものである。

(エ) まとめ

以上のとおり，住基ネットは，控訴人らのプライバシー権を侵害する現実の危険性を有するものであり，その運用は，控訴人らが有している本人確認情報に対する自己情報コントロール権を侵害するものというべきである。

エ　住基ネットの差止めの可否

(ア) 差止めの要件

自己情報コントロール権は，憲法によって保障された権利であるから，それが侵害された場合は，他の人格権侵害の場合と同様に，自己情報コントロール権に基づく侵害の差止請求が認められるべきである。

もとより，控訴人ら個々人の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」のために必要がある場合には一定の制限を受けることは否定できない。しかし，公権力による個人情報の取扱いが問題となる場面は，私人間における表現の自由・知る権利との相互調整等が必要とされるような場面ではなく，公権力の活動が事務処理の効率化等といった利益のために，憲法の保障する基本的人権としてのプライバシーの権利を侵害する場面であるから，一個人の憲法上の人権の保障が十全になされることこそが求められるのであって，あくまでも，情報主体のコントロール（意思決定）権が最大限に保障されるべきであり，公権力の側に圧倒的な比重をおく衡量が行われる危険性のある手法はとられるべきではなく，厳格な審査基準に基づく審査がなされなければならないというべきである。そして，本件のように，公権力によ

る個人情報の取扱いについて，国民本人の同意・承諾が存しない場合，あるいは，その意思に反することが明らかな場合には，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有無，やむにやまれぬ利益の存否，その場合の手段の相当性について厳格な判断がなされなければならない。

(イ) 差止めの必要性

a 既に述べたとおり，住基ネットの運用によって控訴人らの自己情報コントロール権が侵害されている上，将来にわたって，控訴人らの本人確認情報が拡散され，データマッチングの危険にさらされるなど，さらに深刻な被害を受ける具体的，現実的な危険が存する。したがって，住基ネットの運用による控訴人らのプライバシー権の侵害の程度は深刻である。

b 被控訴人らは，住基ネットが行政事務の効率化に資するとしているが，被控訴人らがその根拠としている試算は，そもそも前提とする数値自体虚偽のものであるか，少なくとも恣意的なものであり，検討の資料とはなり得ないものである。住基ネットの安全性を維持するためには，毎年，バージョンアップしたコンピュータ及びソフトウェアの導入，メインテナンス及び職員の研修等に膨大な費用を要するものであって，住基ネットは極めて非効率なものであり，むしろ経費の増大をもたらすものである。また，被控訴人らは，住基ネットによって，行政機関への申請等の際，住民票写しの提出が省略されることによって，市町村の住民票交付事務に伴う経費を削減できるとしているが，住基ネット導入後今日まで，市町村の窓口において，住民票の写しの交付の省略をする業務の利用の程度は極めて少ないものである上，住民票写しの提出省略は住民票交付に伴う手数料収入の減少をもたらすものである。

被控訴人らは，電子政府及び電子自治体（以下，併せて「電子政府等」ということがある。）の実現が，当面するわが国の国家戦略であり，この国家戦略である電子政府等の実現にとって必要不可欠の基盤となるシステムが住基ネットであると主張しているが，そもそも，「電子政府・電子自治体構想のもとになるＩＴ革命あるいはＩＴ戦略」が問題になったのは平成１２年以降であり，これに対して，改正法の閣議決定は平成１０年３月１０日であり，その国会成立は，平成１１年８月１２日である。このように，電子政府等の構想が浮上したのは，改正法の成立以後のことであり，電子政府等の実現が住基法改正の目的であるというのは事実に反するものである。

また，被控訴人らは，電子政府等を実現するためには，行政手続のオンライン化が前提であり，これらの基盤となるのが公的個人認証サービスであり，住基ネットはその不可欠の役割を果たすとも主張しているが，上記のとおり，電子政府等の構想が浮上したのは，改正法の成立以後のことである上，このような「公的個人認証サービス」の実現ということが，すべての国民をその意思に反して住基ネットに参加させる理由となるものではない。

c　仮に，住基ネットが住民の便益に資するものであったとしても，そのことは全員の参加を強制する理由とはなり得ないものである。

控訴人らは，住基ネットの運用そのものの差止めを求めているのではなく，控訴人らが住基ネットから離脱することを求めているにすぎない。そして，控訴人らが住基ネットから離脱をしても，当該市町村や他の自治体，あるいは，国の機関等の行政事務に住基ネット全体の運用が成り立たないような重大な支障を生じさせるものではない。現に，福島県矢祭町，東京都国立市，同杉並区は，自治体として住基ネットに接続しておらず，また，横浜市は，住基ネットの参加に同意し

た住民の情報だけを通知する選択制を採用しているが，これらによっても住基ネットの運用に不都合が生じたということはない。

d　以上のとおり，住基ネットは控訴人らのプライバシー権を深刻に侵害しており，これに対して，住基ネットには，控訴人らのプライバシー権を犠牲にしてもなお達成すべき高度の必要性は存在しておらず，また，控訴人らが住基ネットに参加しなくとも，重大な支障が生じることはないのであるから，控訴人らの差止請求は認容されるべきである。

（被控訴人らの主張）

ア　プライバシー権について

(ア)　プライバシー権は，その概念が不明確であり，それ自体は一つの統一的な憲法上の権利とは認められないので，プライバシー権が憲法１３条によって保障される憲法上の権利であることを前提とする控訴人らの主張は失当である。

また，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，控訴人らが主張するような，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。

(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，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，ましてや思想，信条など個人の道徳的自律に関係したり，人格権の内容を成すものでもないから，当該情報についての秘匿の必要性の程度はさほど高くないというべきである。また，住民票コードも，住民票につけられた１１桁の番号であって，住基ネット上で個人を識別するための単純な情報であり，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，まして，思想，信条など個人の道徳的自律に関係したり，人格権の内容を成すものではないから，住民票コードの秘匿の必要性はさほど高くないというべきである。更に，変更情報についても，住基ネットにおいて，婚姻や，離婚，養子縁組や離縁などの経歴が，変更情報として保有されている事実はないし，また，住基ネットに保有される変更情報は身分関係の変動を推知させる情報ではないから，これを秘匿する必要性が高いということはできない。

なお，関係法令は，住基法３０条の３４を超えるデータマッチングを禁止しており，控訴人らの主張が，これを超える形でのデータマッチングの危険性を前提として，住民票コードの秘匿の必要性が高いとするものならば，同主張は失当である。

イ　住基ネットによるプライバシー権の侵害について

控訴人らは，控訴人らの承諾のないまま本人確認情報を住基ネットで流通させること自体が，控訴人らの自己情報コントロール権を侵害すると主張する。しかし，旧住基法も，行政の合理化のため，都道府県や国の機関が，個々の住民の同意を得ずに住民票上の情報を利用することを認めていたのであるから，これらの情報は，公共領域に属する個人情報として，行政の合理化の目的で，行政機関内部で使用される限り，本人の同意なしに利用することができるというべきである。また，行政機関が事務を遂行する際には，住基ネットの導入前から市町村から住民票写しの交付を受けるなどしていたのであるから，住基ネットの導入によってはじめて控訴人らの個人情報が広範囲で流通することになったということもできない。

したがって，仮に，憲法１３条によって自己情報コントロール権が保障されているとの見解に立ったとしても，住基ネットがプライバシー権を侵害するものでないことは明らかである。

ウ　住基ネットによるプライバシー権の侵害の危険性について

(ア)　不正閲覧・漏えい等の危険性について

a　住基ネットにおいては，保有情報は本人確認情報に限定され，その利用方法及び提供先も法律により限定されている。また，市町村はＣＳの管理責任を負い，都道府県は都道府県サーバと都道府県ネットワークの管理責任を負い，指定情報処理機関は全国サーバと全国ネットワークの管理責任を負うなど，関係機関の責任が明確化されているほか，第三者機関による本人確認情報の保護も図られている。更に，外部からの侵入防止対策としても，建物等への侵入の防止，重要機能室の配置及び構造，入退室管理等の物理的なセキュリティ対策が関係機関に義務付けられているほか，専用回線と専用交換装置を採用し閉鎖的ネットワークを実現し，サーバ間で相互認証・暗号通信を実施し，通信プロトコルを制限し，住基ネット全体で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を実施し，不正な通信の遮断と監視を行い，システム全体で統一のソフトウェアを導入することにより高度なセキュリティを確保するなど，電気通信回線経由による侵入に対する対策も講じられている。これらの対策を含め，住基ネットには十分なセキュリティ対策が講じられており，控訴人らが主張するような不正閲覧・漏えい等の現実的な危険性があるということはできない。

b　控訴人らが長野県侵入実験の結果から明らかとなったとする住基ネットの具体的現実的危険性は，いずれも何ら実証されておらず，むしろ実験結果からはそれらが存在しないことが明白となっている。また，斜里町事故等も，控訴人らの主張を何ら根拠付けるものではなく，むしろ，斜里町事故等によって，現実に住基ネット自体から個人情報が流出したものではなく，いずれも住基ネットのセキュリティ上は問題がないこと，更に，各市町は，住基ネットのセキュリティの確保に適

切に努めていることなどの事実がより明らかになったというべきである。

c　仮に，ある特定の市町村におけるセキュリティ対策に不十分な点があるとしても，直ちに他の市町村の住民の本人確認情報のセキュリティに具体的危険が生じるものではない。すなわち，市町村のＣＳは，当該市町村の住民の本人確認情報を保持するのみであり，他の市町村の住民の本人確認情報を保有していない。そもそも，他の市町村の住民の本人確認情報は，他の市町村のＣＳ，都道府県サーバ及び全国サーバに保有されているものであり，これらの情報を閲覧，改ざんするためには，他の市町村，都道府県及び指定情報処理機関が管理するＦＷを突破して，地方公共団体の共同のネットワークである住基ネット本体に侵入する必要があるが，極めて困難である。したがって，住基ネットに控訴人らの主張するようなシステム的・構造的な脆弱性があるということはできない。

(イ)　データマッチングの危険性について

本人確認情報が提供される事務は平成１７年４月１日現在２７５事務あるが，これらの国の機関等の保有する情報を一元的に管理する主体は存在しない。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おり，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国の機関等は，それぞれ分散して情報を管理しており，これらの機関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。

住民票コードを用いたデータマッチングや名寄せについては，それが住基法に規定された事務の目的を超えて行われる場合には，それ自体が本人確認情報の目的外利用に該当し，住基法３０条の３４によって絶対的に禁止されている。また，これに違反する行為については，懲戒処分，

罰則，第三者機関による監視といった制度的な担保も規定されている。

(ウ) 保護措置について

住基ネットでは，個人情報保護に関する国際的基準ともいうべきＯＥＣＤ８原則を踏まえた厳重な保護措置が講じられている。

また，住基法は，目的外利用や情報の漏えい，民間部門の利用を禁止し，違反には罰則を設けているのであって，これらの面における保護措置が不十分であるということはできない。

なお，政府は，改正法附則１条２項に定める所要の措置として，平成１３年３月２７日，「個人情報の保護に関する法律案」を第１５１回国会に提出した。政府は，自ら法律を制定することはできないのであるから，法律案の検討，作成及び国会への提出によって上記所要の措置を講じたことになる。

エ 住基ネットの差止めの可否について

仮に，本人確認情報がプライバシーとして保護の対象になるとしても，住基ネットの導入により，住民負担の軽減と行政事務の効率化及び正確性の向上，行政手続のオンライン化，住基台帳に係る市町村の窓口業務の簡素化等，住民の利便性の増進を図ることが可能となる上，住基ネットは，電子政府等の基盤となる不可欠な本人確認システムであることから，住基ネットには正当かつ必要な目的があり，控訴人らの差止請求は認められない。

(2) 争点(2)（人格権侵害に基づく差止請求の可否）について

（控訴人らの主張）

憲法１３条は，国民が，その有する氏名を中核として，個人として尊重され，他と識別されて取り扱われる権利・利益をも保障するものである。ところが，住基ネットは，行政が，国民に対し，出生から死亡に至る生涯にわたって，一方的に番号（住民票コード）を付し，これを本人の意向を無視して

行政の便宜のために利用しようとするものであって，国民を番号で扱うことにほかならず，国民の人格権を侵害するものであり，憲法１３条に違反するものである。住基ネットによる控訴人らの人格権侵害の程度は深刻であり，控訴人らの精神的苦痛は著しいから，住基ネットの運用は差し止められるべきである。

（被控訴人らの主張）

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する１１桁の番号であって，住基台帳に記載された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なので，その記載によって控訴人らの人格権や人格的利益が侵害される余地はない。

(3) 争点(3)（公権力から包括的に管理されない自由の侵害に基づく差止請求の可否）について

（控訴人らの主張）

憲法１３条は，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（公権力から包括的に管理されない自由）を国民に保障している。ところが，住基ネットは，住民票コードをすべての国民個人に重複することなく付番することを前提としており，このような住民票コードは，さまざまな行政機関が個別に蓄積・保有していた個人情報を結合させる基点となるものであり，公権力による国民個人の情報の一元的管理を可能とするものであるから，控訴人らの公権力による包括的管理からの自由を侵害するものである。住基ネットによる控訴人らの公権力から包括的に管理されない自由の程度は深刻であり，控訴人らの精神的苦痛は著しいから，住基ネットの運用は差し止められるべきである。

（被控訴人らの主張）

控訴人らの主張する「公権力による包括的管理からの自由」は，そもそもその具体的内容が不明確であり，権利としての成熟性を備えていないから，憲法によって保障された権利とはいえない。しかも，住基ネットの運用によって，控訴人らの主張するように，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という状態が生じるものでもないから，控訴人らの主張は前提を欠いており失当である。

(4) 争点(4)（損害賠償請求の可否）について

（控訴人らの主張）

ア 被控訴人国は，プライバシー及び人格権を侵害する法改正を行い，改正法の施行の延期を内容とする議員立法である凍結法案を審議することなく無視し，その施行を延期しないばかりか，国民のプライバシー権の保護のための所要の措置が講じられていないのに政令を制定し，平成１４年８月５日から住基ネットの運用を強行している。この結果控訴人らは，前述のとおりプライバシー権及び人格権を侵害され，さらに今後控訴人らの個人情報が外部からの侵入や漏えいあるいは目的外利用や不正使用の危険性にさらされ精神的に不安な状態におかれることとなった。被控訴人国は，控訴人らのこれらの精神的損害を賠償する責任を負う。

控訴人らの上記精神的損害に対する慰謝料としては，各自１０万円が相当であり，弁護士費用としては，その１割に相当する各１万円が相当である。

イ 控訴人らは，被控訴人愛知県及び被控訴人センターが各自治体の有する本人確認情報をネットワーク化することにより，そのプライバシーの権利若しくは利益を侵害された。控訴人らは，今後，更に控訴人らの個人情報や住民票コードが外部からの侵入や漏えいあるいは不正使用の危険性にさらされることによって常に精神的に不安な状態におかれることとなる。被

控訴人愛知県は，控訴人らのこれらの精神的損害を賠償する責任を負う。

控訴人らの上記精神的損害に対する慰謝料としては，各自１０万円が相当であり，弁護士費用としては，その１割に相当する各１万円が相当である。

（被控訴人らの主張）

国賠法上の違法性が認められるためには，被控訴人国及び被控訴人愛知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したことが必要である。そして，内閣，総理大臣，愛知県知事の行為について違法性が認められるためには，各人が，職務上通常尽くすべき注意義務を尽くすことなく漫然と当該行為をしたことが必要である。しかし，本件においてこれらの法的義務違反の行為がないことは明らかであり，被控訴人国及び被控訴人愛知県が控訴人らに対して損害賠償責任を負うことはない。

第３　当裁判所の判断

１　争点(1)（プライバシー権侵害に基づく差止請求の可否）について

(1)　プライバシー権について

憲法１３条は，すべての国民を個人として尊重し，個人が幸福を追求することを憲法上の権利として定めているところ，他人に知られたくない個人の私生活上の情報がみだりに開示されれば，個人の私的な生活領域における平穏が害され，個人の人格的自律が脅かされることとなるから，このような個人の私生活上の情報，すなわちプライバシーに係る情報を開示されないという期待は，憲法１３条によって保障される人格権の一内容として，法的保護を受けることができる利益に当たるものと解される。したがって，控訴人らが主張するような自己情報をコントロールする権利がプライバシー権として認められるか否かは別としても，国家機関が，正当な理由もないのに，個人の同意を得ず，みだりに個人の私生活上の情報を収集，開示することは，同条に反して許されないというべきである。

ところで，住基ネットにおいて利用提供される本人確認情報のうちの４情報は，個人の識別情報ないし客観的・外形的な事項としての性格が強いものであり，社会生活上一定の範囲では必然的に開示され，利用されている情報であるから，個人の思想，信条等に関する情報と比較すると，平均的な一般人がその開示に苦痛を感じる程度は相対的には低いものと考えられる。また，住民票コードは，住基ネットにおいて，個人を識別するために技術的に用いられる１１桁の便宜的な数字であって，それ自体は個人の人格的自律に直接かかわるものではないし，変更情報も，「前提となる事実」の(3)イに記載したとおり，転入，転出，出生，死亡の他は，「職権記載等」，「職権修正等」であり，これらの職権記載の原因となる婚姻や離婚，養子縁組や離縁などの身分上の変動事由は記載されないから，他人に知られたくない個人情報が開示されるとはいえないし，「職権記載等」，「職権修正等」の記載と従前の本人確認情報との対比により身分上の変動事由が推測可能であるとしても，これらの情報が純粋に私生活上の情報とは言い難い面もあり，結局，これらの情報はいずれも秘匿する必要性が高いということはできないものである。

しかし，コンピュータを利用した個人情報の大量収集・蓄積という社会状況のもとで，収集，蓄積された個人情報の漏えいや目的外使用に対する不安を抱く者が少なからず存することは否定できないところであり，上記のように必ずしも秘匿する必要性が高いとはいえない情報であっても，その開示が予定されていない者に対して，あるいは予定されていない利用目的のために，本人の同意なくしてみだりに情報が開示されることとなれば，本人が不安を感じ，その私生活の平穏及び人格的自律が害される可能性があることは否定できない。したがって，本人確認情報が，予定された開示対象及び利用範囲を逸脱してみだりに開示されないという限度では個人の期待は法的保護に値するものというべきである。

(2) プライバシー権の侵害の有無について

控訴人らは，住基ネットにより控訴人らの本人確認情報を自己の居住する市町村以外の機関に通知や提供をする形で流通させることは，それ自体により，控訴人らが有している本人確認情報に対する自己情報コントロール権を侵害していると主張する。

確かに，旧住基法においては，居住する市町村だけに保有管理されていた４情報が，住基法では，都道府県知事に通知されて保有されることとなり，また，国の機関及び法人等（以下「国の機関等」という。），他の市町村の執行機関などにも通知提供され，都道府県知事によって利用されるようになったのであるから，住基ネットの導入により，４情報を保有，管理する主体が旧住基法当時よりも拡大されたことは明らかである。

しかし，４情報は，旧住基法においても住基台帳の記載事項とされ，住民にはこれらの情報について市町村長に対する届出義務があり，届出を受けた市町村長はその情報を住基台帳に記載して保有し，国又は地方公共団体の職員が，その職名，職務上の請求である旨及びその者の住所氏名を明らかにすれば，市町村長から，住民票写しの交付を受けることが可能とされていた（旧住基法１２条１項，２項，住基台帳の閲覧及び住民票の写し等の交付に関する省令３条２号）のであるから，４情報については，行政目的に使用される場合には，旧住基法当時から，国や他の自治体に対して開示されていたものというべきであり，住基ネットの運用開始により４情報の通知提供が容易になり，その機会が増加したとしても，それによって，４情報の開示対象又は利用範囲に質的な変化があったということまではできない。

また，前記認定のとおり，住民票コードは，個人を識別するために技術的に用いられる１１桁の便宜的な数字であって，それ自体は個人の人格的自律に直接かかわるものではなく，変更情報も含め，これらの情報はいずれも秘匿する必要性が高いということはできないものであるから，４情報，住民票コード及び変更情報が本人確認情報として一体となって住基ネットにより通

知提供されているとしても，それが本来の目的に従って行われている限り，そのこと自体によって控訴人らのプライバシーに関する利益が侵害されているとみることはできないといわざるを得ない。そして，弁論の全趣旨によれば，住基ネットの運用開始後現在に至るまで，住基ネット自体からの情報の漏えい事故は発生していないことが認められるから，結局，現時点において，住基ネットの運用自体によって控訴人らのプライバシー権が侵害されているとは認められないというべきである。

したがって，控訴人らの上記主張は採用できない。

(3) プライバシー権の侵害の可能性の有無について

ア 不正閲覧・漏えい等の危険性について

(ア) 住基法は，本人確認情報の保護に関して，次のとおり規定している。

a 監督命令等

総務大臣は，制度を所管する立場あるいは指定情報処理機関に対して監督を行う立場から，指定情報処理機関への監督命令等（住基法３０条の２２第１項），地方公共団体への指導，助言・勧告等（住基法３１条），指定情報処理機関の定める本人確認情報管理規程の認可（住基法３０条の１８），電気通信回線を通じた送信の方法に関する技術的基準の策定等（住基法施行規則２条１項等）の権限を有している。また，委任都道府県知事は，指定情報処理機関に対する指示をする権限を有しており（住基法３０条の２２第２項），指定情報処理機関は，委任都道府県知事に対する技術的助言等を行うものとされている（住基法３０条の１１第７項）。

委任都道府県知事は，その行わせることとした本人確認情報処理事務の適正な実施を確保するため必要があると認めるときは，指定情報処理機関に対し，当該本人確認情報処理事務の実施の状況に関し必要な報告を求め，又はその職員に，当該本人確認情報処理事務の実施の

状況若しくは帳簿，書類その他の物件を検査させることができる（住基法３０条の２３第２項）。

都道府県に，本人確認情報の保護に関する審議会（以下「都道府県の審議会」という。）を置く。都道府県の審議会は，住基法の規定により，その権限に属させられた事項を調査審議するほか，都道府県知事の諮問に応じ，本人確認情報の保護に関する事項を調査審議し，これらの事項に関して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，第２項）。

b　本人確認情報の安全確保

都道府県知事又は指定情報処理機関が住基法３０条の５第１項又は３０条の１１第１項による通知に係る本人確認情報の電子計算機処理等を行う場合，都道府県知事又は指定情報処理機関から本人確認情報の電子計算機処理等の委託を受けた者が受託した業務を行う場合には，本人確認情報の漏えい，滅失及びき損の防止その他の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）。

本人確認情報の提供を受けた市町村長その他の市町村の執行機関若しくは都道府県知事その他の都道府県の執行機関又は住基法別表第１の上欄に掲げる国の機関等（以下「受領者」という。）が本人確認情報の電子計算機処理等を行う場合，受領者から本人確認情報の電子計算機処理等の委託を受けた者が受託した業務を行う場合にも，前記のような措置を講じなければならない（住基法３０条の３３）。

市町村長及び市町村長から委託を受けた者は，住基台帳又は戸籍の附票に関する事務の処理に当たっては，住民票又は戸籍の附票に記載されている事項の漏えい，滅失及びき損の防止その他の住民票又は戸籍の附票に記載されている事項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３６条の２）。

c　利用又は提供の制限

都道府県知事は，住基法が定める一定の場合（前記第２の２(3)カ(ア)）を除き，本人確認情報を利用又は提供してはならない（住基法３０条の３０第１項）。また，指定情報処理機関は，委任都道府県知事の事務を行う場合を除き，本人確認情報を利用又は提供してはならない（住基法３０条の３０第２項）。

受領者は，住基法に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ものの事務の遂行に必要な範囲内で，本人確認情報を利用又は提供するものとし，それ以外の目的のために受領した本人確認情報を利用又は提供してはならない（住基法３０条の３４）。

d　秘密保持義務等

住基ネットに係る事務に従事する市町村，都道府県及び指定情報処理機関並びに本人確認情報の提供を受けた市町村，都道府県及び国の機関等の役員，職員又はこれらの職にあった者に対し，本人確認情報処理事務等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の保持義務を課し（住基法３０条の１７第１項，３０条の３１第１項，３０条の３５第１，２項），これに違反した者は，２年以下の懲役又は１００万円以下の罰金に処することとしている（住基法４２条）。

また，市町村，都道府県及び指定情報処理機関並びに本人確認情報の提供を受けた市町村，都道府県及び国の機関等から本人確認情報の電子計算機処理等（電子計算機処理又はせん孔業務その他の情報の入力のための準備作業若しくは磁気ディスクの保管をいう。）の委託を受けた者，その役員若しくは職員又はこれらの職にあった者に対して

も，本人確認情報処理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の保持義務を課し（住基法３０条の１７第２項，３０条の３１第２項，３０条の３５第３項），これに違反した者は，２年以下の懲役又は１００万円以下の罰金に処する（住基法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）。

受領した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）。

e　住民票コードに関する制限

市町村長その他の市町村の執行機関は，住基法規定の場合を除き，何人に対しても，当該市町村の住民以外の者の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第１項）。都道府県知事その他の都道府県の執行機関，指定情報処理機関及び住基法別表第１の上欄に掲げる国の機関等は，住基法規定の場合を除き，何人に対しても，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第２ないし第４項）。

市町村長その他の市町村の執行機関，都道府県知事その他の都道府県の執行機関，指定情報処理機関又は住基法別表第１の上欄に掲げる国の機関等（以下「市町村長等」という。）以外の者は，何人も，自己と同一世帯に属する者以外の第三者に対し，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）。

市町村長等以外の者は，その者が業として行う行為に関し，その者に対し売買，賃借，雇用その他の契約の申込みをしようとする第三者若しくは申込みをする第三者又はその者と契約の締結をした第三者に対し，当該第三者又は当該第三者以外の者に係る住民票に記載された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）。また，市町村長等以外の者は，何人も業として，住民票コードの記録されたデータベースであって，当該住民票コードの記録されたデータベースに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してはならない（住基法３０条の４３第３項）。都道府県知事は，これらに違反する行為が行われた場合において，当該行為をした者が更に反復してこれらに違反する行為をするおそれがあると認めるときは，その者に対し，当該行為の中止等を勧告し，その勧告に従わない場合は，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，当該勧告に従うべきことを命ずることができ（住基法３０条の４３第４，５項），当該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する（住基法４４条）。

(イ) 証拠（乙Ａ１の１ないし３，乙Ａ１０ないし１３，乙Ａ２２の１，２，乙Ａ２３，乙Ａ２５の１，２，乙Ａ２６の１ないし３，乙Ａ２８，２９，乙Ａ３４の１，２，乙Ａ３５の１，２，乙Ａ３６，乙Ａ３７の１，２，乙Ａ３８，乙Ａ３９の１，２，乙Ａ５０の１，２）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 総務省は，住基ネットのセキュリティについて，「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，平成１５年総務省告示第３９１号，同第６０１号。以下

「セキュリティ基準」という。）によって，次のような定めを設けている。

(a) 体制，規程等の整備

住基ネットのセキュリティを確保するため，責任体制，連絡体制を明確にし，通常時及び非常時の責任体制を確立する。都道府県知事，市町村長及び指定情報処理機関は，住基ネットのセキュリティ対策に関し，連絡調整を行う場を設け，住基ネットの運用上，異常な状態を早期に発見し，相互に連絡することができるよう体制の整備を図る。住基ネットの企画，開発及び運用に関する規程，住基ネット設計書，操作手順書，緊急時における作業手順書等を整備する。住基ネットの運用に必要な職員を配置し，職員に対して，住基ネットの操作及びセキュリティ対策についての教育及び研修を実施するための体制を確立する。監査の体制を確立し，住基ネットの企画，開発及び運用の各段階におけるセキュリティ対策の評価を行う。

(b) 住基ネットの環境及び設備

住基ネットに関する建物及び重要機能室への侵入防止策を講ずる。重要機能室の所在を明らかにしないようにし，その配置及び構造については，セキュリティ対策が行えるよう配慮する。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は，専用回線を使用する。また，国の機関等に本人確認情報を提供するために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の使用する電子計算機を結ぶ電気通信回線は，専用回線を使用する。

(c) 住基ネットの管理

重要機能室への入室者を限定する。重要機能室に入退室する者に鍵を貸与する際に，その者が入室する権限を有することを確認する

こと等により，重要機能室への入退室の管理を適切に行う。住基ネットを運用する職員に対して，電子計算機，端末機，電気通信関係装置，電気通信回線，ファイル等に関し，必要なアクセス権限を付与する。電気通信回線に接続する電子計算機における不正な行為や，電予計算機への不正アクセス行為から住基ネットを保護するため，ＣＳ，都道府県サーバ及び指定情報処理機関サーバ間等，必要な部分に指定情報処理機関ＦＷを設置し，通信制御を行う。エラー，不正行為により電気通信関係装置の不当な運用が行われないようにするため，電気通信関係装置の管理に際しては厳重な確認を行い，通信に際しては相互認証をする。ＣＳ，都道府県サーバ又は指定情報処理機関サーバ間の通信については，相互の認証を行い，交換するデータの暗号化を実施する。都道府県サーバ又は指定情報処理機関サーバから国の機関等に本人確認情報を提供するためのデータ交換についても，相互の認証を行い，データの暗号化を実施する。端末機は，管理を行う責任者の指示又は承認を受けた者が取り扱い，操作者が正当な権限を有していることを識別カード及びパスワードによって確認する。住基ネットの開発，変更，運用，保守等について委託を行う場合には，委託先事業者等の社会的信用と能力を確認し，本基準と同様のセキュリティ対策を実施させ，適切な監督を行う。

(d) 既存住基システムとの接続

住基ネットと既存住基システムとを接続する場合は，既存住基システムにおいて，体制の整備，専用回線の使用，住基ネットとの間のＦＷの設置，住基ネットと電気通信回線等の不共有を，既存住基システムと外部のネットワークとを接続する場合は，ＦＷ設置による厳重な通信制御の実施等の措置を講ずる。

(e) 適切な管理のための措置の実施要請

市町村長，都道府県知事，指定情報処理機関は，必要に応じ，情報の提供先に対して，提供を行った本人確認情報の適切な管理のための措置の実施状況について報告を求め，当該本人確認情報の適切な管理のための措置の実施の要請を行うことができる。

(f) 本人確認情報の提供又は利用の状況に係る情報の保存

都道府県知事は，住民からの本人確認情報に関する情報開示請求に適切に対応するため，国の機関等に対する情報の提供又は利用の状況に係る情報（アクセスログ）を必要な期間保存する。保存した情報は，保存を行う必要がある期間経過後遅滞なく，確実に消去する。

b また，総務省は，住基カードのセキュリティ対策について，「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。）によって，次のような定めを設けている。

(a) 住基カードには，後記のセキュリティ対策を実施することが可能な中央演算処理装置付きの半導体集積回路を組み込んだカードを用いること。

(b) 暗証番号を設定して初めて，住基カード又は住基ネットに係るアプリケーションを利用可能な状態となること。暗証番号は，住基カードに設定し，外部から読み取ることができないようにすること。暗証番号の照合は，住基カードの内部で行うこと。暗証番号の照合ができない場合が続いたときは，暗証番号の照合ができず，当該暗証番号の照合を必要とする処理が実施できない状態となること。

(c) 発行前の住基カードに対し，不正使用を防止するための情報を設定すること。

(d) 交付後の住基カードと住基ネット相互間の認証を行うための情報

を住基カードに設定し，住基カードの外部から内部に記録された情報を読み取ることができないようにすること。

(e) 住基カードに記録された情報を保護するために，アクセス権限（住基カードに記録された各情報ごとに，認証，暗証番号照合等が正しく行われた場合に限り情報へのアクセスを可能とするようにあらかじめ設定した権限）の制御を行うこと。

(f) 半導体集積回路に物理的又は電気的な攻撃を加えて，住基カードに記録された情報を取得しようとする行為に対し，情報の読み取り又は解析を防止する仕組みを保持すること。

(g) 基本利用領域（住基ネットに係るアプリケーションのために住基カードの半導体集積回路上に割り当てられた領域）とそれぞれの条例利用領域（条例利用アプリケーションのために住基カードの半導体集積回路上に割り当てられた領域）は，住基カードの内部で独立し，それぞれのアプリケーションのために割り当てられた領域以外の領域に情報を記録し，又は他の領域に記録された情報を読み取ることができない仕組みを保持すること。

なお，条例利用領域が設けられたのは，住基カードの多目的利用のために，住基カードの空き領域を住基ネットとは別個独立のものとして活用できるというものにすぎず，同領域の活用それ自体は住基ネットのシステムそのものには含まれない。そして，同領域には，特に必要性が認められる場合を除き，条例利用アプリケーションに係るシステムへアクセスするための利用者番号など以外の個人情報を記録しないこととされており，住基カードに直接住民個人の情報が蓄積されることはなく，上記利用者番号等に住民票コードを用いることも禁止されているから，住基カードの多目的利用が進んでも，個人情報やプライバシーの保護に対しては，十分な措置が講じられており，住基カー

ドがデータマッチングに利用されることもない。

c　住基ネットは，上記住基法の諸規定，セキュリティ基準，住基カードセキュリティ基準に沿って構築されているが，セキュリティ対策として講じられている具体的な措置には次のようなものがある。

(a)　外部からの侵入防止対策（電気通信回線経由による侵入に対する対策）

①　ＣＳ，都道府県サーバ及び全国サーバ間の通信は，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，全国サーバと国の機関等サーバとの間は，専用回線又は磁気媒体でデータ交換を行っている。また，住基ネットの全国ネットワーク等で採用しているIP－VPNは，デジタル専用回線，多重化装置等及び住基ネット専用の交換装置により構成され，各拠点と交換装置は常に固定的に接続され，論理的に他回線と完全に隔離された専用回線となっている。

②　暗号技術評価委員会（CRYPTREC）において安全性が確認されている公開鍵方式により，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仕組みを採っている。この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を地方公共団体及び国の機関等に配送するため，第三者（地方公共団体及び国の機関等を含む。）が内容を読み出したり，変更することはできない。また，通信相手の相互認証の過程では，その都度耐タンパー装置内で，CRYPTREC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，通信の都度共通暗号鍵を設定し，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。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，通信が終わればその共通暗号鍵は廃棄される。

③　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によって通信を行っており，SMTP（電子メール転送プロトコル），HTTP（WWWデータ転送プロトコル），ＦＴＰ（ファイル転送プロトコル），Telnet（仮想端末プロトコル）等のインターネットで用いられる汎用的なプロトコルは使用していない。また，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（端末機側については，都道府県サーバと既存庁内ＬＡＮを接続しない団体を除く。），全国サーバの全方向及び国の機関等サーバ（全国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ＦＷ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過を遮断している。

④　指定情報処理機関において，コンピュータウイルスの発生情報を常時入手し定期的に（危険度が高いものについては随時），パターンファイルを全団体に配布している。住基ネットでは，全地方公共団体の全サーバ，全端末について，全国センターから自動的に配布され更新されるシステムを有しており，対策の徹底を実現している。また，ＯＳ（Windows，UNIX等）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全団体にセキュリティホール情報及び対応方法を通知している。

⑤　指定情報処理機関ＦＷはラックに厳重に格納・施錠されており，指定情報処理機関のネットワーク監視室から運用管理規程に基づき，ネットワーク側への不正な通信がないか，あるいは，ネットワーク側からの不正な通信がないかにつき，２４時間常時監

視を行っている。万一不正アクセスの前兆を検出した場合は，緊急時対応計画等に基づき必要な連絡，対策（関係サーバの一時切り離し等を含む）等が実施される。また，ネットワーク内にＩＤＳ（侵入検知装置）を設置し，運用管理規程に基づき，指定情報処理機関のネットワーク監視室から常時監視を行うほか，定期的にログの解析を行っている。万一指定情報処理機関ＦＷを通過した不正アクセスを検出した場合は，緊急時対応計画等に基づき必要な連絡，対策等が実施される。

指定情報処理機関ＦＷは，全国サーバ，都道府県サーバ，ＣＳ，国の機関等サーバに対する全方向からの不正な通信を遮断し，これらを保護している。

⑥　システム全体で統一ソフトウェアを導入することにより，全体で，相互認証，暗号化，コンピュータウイルス，セキュリティホール対策，操作者識別カードと暗証番号による操作者確認，本人確認情報データベースへの接続制限，データ通信の履歴管理及び操作者の履歴管理などの対策を採用している。

(b)　内部の不正利用防止対策

①　本人確認情報の検索に際して，即時提供（端末機から照会条件を入力し，都道府県サーバ又は指定情報処理機関サーバから即時に本人確認情報の提供を受ける方式）の場合，「住民票コード」，「氏名＋住所」又は「氏名＋生年月日」を端末機に入力しないと本人確認情報の提供を受けられない仕組みとなっている。また，「氏名＋住所」又は「氏名＋生年月日」を入力する場合は，前方一致検索が可能であるが，該当者が５０人を超えるときは本人確認情報の提供が受けられない。なお，前方一致検索は，少なくとも「氏名の先頭１文字＋住所全部」，「氏名全部＋住所の都道府

県・市町村名を除いた先頭１文字」，「氏名の先頭１文字＋生年月日全部」の入力が必要である。

一括提供（本人確認情報照会対象者の情報をファイル化して都道府県サーバ又は指定情報処理機関サーバに照会し，これらのサーバから照会結果ファイルを受け取る方式）の場合も，上記の場合と同様，照会元から送られてきた「住民票コード」，「氏名＋住所」，「氏名＋生年月日」等のファイルに，都道府県サーバ又は指定情報処理機関サーバにおいて，本入確認情報を追記して照会元にファイルを返送するなどの措置が講じられている。

② 本人確認情報は，ＣＳ，都道府県サーバ及び指定情報処理機関サーバ内に保存されており，端末機には存在しない。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と端末機との間で相互認証を行って初めて住基ネットアプリケーションが起動する設計とされており，アクセス権限のない職員等及び外部から本人確認情報データベースへアクセスすることはもちろん，住基ネットアプリケーションを起動することもできない。その上，操作者識別カードの種別により，システム操作者ごとに住基ネットが保有するデータ等へ接続できる範囲を限定している。

③ 指定情報処理機関は，運用管理規程に基づき，定期的に指定情報処理機関サーバのアクセスログの解析を行い，万一不正使用の兆候を検出した場合，緊急時対応計画等に基づき必要な連絡，対策等を実施することとされている。また，市町村は，都道府県に対し，あるいは，都道府県を経由して指定情報処理機関に対し，住民のアクセスログの解析要請を行うことができ，都道府県は，指定情報処理機関に対し，住民のアクセスログの解析要請を行うことができることとされている。

④　住所地市町村において，交付地市町村の特定の操作者識別カード（操作者用ＩＣ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，住民票の写しの広域交付を停止する措置が講じられている。

⑤　住基ネット関連のセキュリティ研修として，４７都道府県において，市町村の住基ネット担当者を対象に，個人情報保護意識の向上，住基ネットの安全性の確保等を目的としたセキュリティ研修会が実施されている。その他，総務省も地方公共団体職員向けのセキュリティ研修の実施に力を入れている。

(c)　外部監査等によるセキュリティの確保

①　指定情報処理機関と総務省は，市町村における住基ネットとそれに接続する既設ネットワークにおけるセキュリティ対策の徹底を図り，もって住基ネットのセキュリティ強化を図るため，協力してチェックリストを作成し，市町村に配布した。市町村は，平成１５年１，２月，これに基づきセキュリティ対策の自己点検を実施し，その調査結果は，同年５月１２日に住基ネット調査委員会に報告された。総務省は，平成１５年５月１３日，住基ネット担当課長会議を開催し，この点検結果を踏まえて，都道府県において，市町村に対して必要な技術的指導を行うこと（政令指定都市にあっては，必要な対策を講じること）を要請した。その結果，対策状況について自己点検結果を調査したところ，各都道府県，総務省及び指定情報処理機関における徹底した技術的助言，指導の実施，市町村の積極的な取組により，すべての市町村において，重要点検項目の７項目について３点満点を達成した。また，その他の項目についても，第二次稼働に向け，市町村のセキュリティ対策は大幅に向上した。市町村は，引き続き，自主的にセキュリ

ティの強化を，各都道府県及び指定情報処理機関は，技術的助言及び指導に務め，セキュリティの維持向上を図っている。

② 平成１５年１月から３月までの間，全国１０８団体の市町村において，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。

d 長野県は，住基ネットの安全性に関して，阿智村，下諏訪町，波田町を対象に，内部からの侵入（庁内ＬＡＮから住基ネットへの侵入を試みるもの）と外部からの侵入（インターネットから庁内ＬＡＮへの侵入を試みるもの）の２種類の安全性調査（長野県侵入実験）を行った。

内部からの侵入調査では，庁内ＬＡＮに調査用コンピュータを接続して，庁内ＬＡＮ及び庁内ＬＡＮ上に存在する各種サーバについての情報を収集し，その情報をもとにサーバの管理者権限の奪取を試みた。また，管理者権限を奪取した既存住基システムから，ＣＳとの間のＦＷに関する情報を収集し，既存住基システムに偽装した調査用コンピュータにより，ＣＳとの通信を試みた。さらに，ＣＳに接続した調査用コンピュータにより，ＣＳ及びＣＳ端末についての情報を収集し，既知の脆弱性を利用して，ＣＳ及びＣＳ端末の管理者権限の奪取を試みた。外部からの侵入調査では，遠隔地からインターネットを経由して，ＦＷ及び公開サーバについての情報を収集し，得られた情報をもとに公開サーバへの侵入を試みた。これらの調査では，指定情報処理機関ＦＷを突破して，ＣＳに直接侵入することは試みられていない。

(a) 阿智村での調査

平成１５年９月２２日から同月２４日までの間，出先機関であるコミュニケーションセンターの会議室の接続口等から庁内ＬＡＮに攻撃端末を接続し，既存住基サーバの管理者権限を取得することや

庁内ＬＡＮとＣＳとの間に設定されているＦＷを突破してＣＳの管理者権限を取得することが試みられた。この結果，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，ＦＷを突破してＣＳの管理者権限を取得することはできなかった（第１次調査）。

次に，同年１１月２５日から同月２８日までの間，ＣＳセグメント（ＣＳが設置されている区画で，両端をＦＷで防御されている。）等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が試みられた。ＣＳセグメントへの攻撃端末の接続は，職員の協力を得て，通常は施錠されている重要機能室に開錠して入り，通常は施錠されているラックの鍵を開けて接続された。その結果，ＣＳの管理者権限を取得することができ，ＣＳの管理者権限を取得することで得られたＩＤ及び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が，ＣＳ端末の管理者権限をＣＳの管理者権限の取得を経ないで直接取得することはできなかった（第２次調査）。

(b)　下諏訪町での調査

平成１５年９月２５日及び２６日，調査のための無線ＬＡＮ環境を構築した上，町役場に隣接する建物から庁内ＬＡＮに攻撃端末を接続し，既存住基サーバの管理者権限を取得することや庁内ＬＡＮとＣＳとの間に設定されているＦＷを突破してＣＳの管理者権限を取得することが試みられた。この結果，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，ＦＷを突破してＣＳの管理者権限を取得することはできなかった。

(c)　波田町での調査

平成１５年９月２９日から同年１０月１日までの間，東京都内からインターネットを経由して，インターネットと庁内ＬＡＮとの間

に設置されたＦＷを突破してインターネットから庁内ＬＡＮへ侵入することが試みられた。この結果，ＦＷを突破してインターネットから庁内ＬＡＮへ侵入することはできなかった。

e　被控訴人センターは，平成１５年１０月１０日ないし１２日，東京都品川区の協力を得て，ペネトレーションテスト（侵入テスト）を行った。その結果，①住基ネットとＣＳ間，②ＣＳと庁内ＬＡＮ間の指定情報処理機関ＦＷに侵入を試みたが，成功せず，脆弱性も見出せなかった。また，③庁内ＬＡＮ上のＣＳ端末の管理者権限の奪取を試みたが，成功せず，不正侵入を許すような弱点も見出すことができなかった。

テストを実施した米国クロウ社の助言としては，庁内ＬＡＮについても，チェックリストによる自己点検及びセキュリティ監査を行い，また，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ことであった。

f　住基ネットに関連して，次のとおりの事故が発生している。

(a)　斜里町事故

平成１８年３月，斜里町職員が自宅の個人用パソコンに斜里町の保有する業務資料データを保存し，その後ファイル交換ソフト「Winny」をインストールしたところ，暴露ウイルスに感染し，上記データが「Winny」のネットワーク上に流出した。

流出情報には，被控訴人センターが，平成１６年に各市町村に送付した「セキュリティーホールの対策について」と題する通知，斜里町で平成１５年に使用されていたＣＳのパスワードが記載された，斜里町作成の業務操作マニュアルが含まれていた。上記通知は，平成１６年当時のＯＳ上の脆弱性に関する公開情報とその対応策を通知したものであり，既に対策は完了していた。斜里町では，既存

住基システム及び住基ネットは，インターネットに接続する情報系ＯＳとは切断されており，インターネットとは接続されていなかった。

斜里町では，平成１８年３月１６日，全職員に対し，個人情報や業務資料等が記載されている媒体の外部持ち出しの禁止，私物パソコンを含め，「Winny」をはじめとするファイル交換ソフトの使用の禁止について指示を出した。

(b) 帯広市事故

平成１５年８月２１日から平成１６年１月１３日までの間に，一般事務を担当する帯広市職員が，「宛名管理システム」によって表示された宛名情報を閲覧した。また，平成１７年６月１８日から同年１０月１２日までの間に，帯広市嘱託職員が，住基台帳の情報が入った既存住基システムの端末を，業務以外目的で閲覧していた。

帯広市は，同職員らに対し，厳重注意処分をした。

(c) 塙町事故

平成１６年９月１３日，塙町が，住民票コードが記載された名簿を行政区長の会合で配布し，指摘を受けてその場で全て回収した。

(ウ) 以上によれば，住基ネットにおいては，住基法によって本人確認情報の保護のための禁止規定やこれに違反した場合の罰則が設けられているほか，住基ネットや住基カードについてセキュリティ対策が講じられており，これらによって，運用関係者による漏えいの危険や外部の第三者の侵入による本人確認情報の漏えいや改ざんを防止するための合理的な措置が講じられているものと認めるのが相当である。

この点，長野県侵入実験においては，一定の条件のもとで，庁内ＬＡＮへの侵入，公開サーバ及び既存住基サーバの管理者権限の奪取には成功しているものの，インターネット回線を通じた状態でＦＷを突破して

庁内ＬＡＮへ侵入することや管理者権限の奪取には失敗し，また，ＣＳと庁内ＬＡＮ間のＦＷ突破にも失敗しており，結局，長野県侵入実験においてＣＳ及びＣＳ端末の管理者権限を奪取し得たのは，重要機能室に入室して，物理的に攻撃端末を接続し，ＦＷの制約を回避した状態という通常は想定することができない極めて例外的な条件のもとで実施された場合にとどまるものである。したがって，長野県侵入実験の結果からは，住基ネットの危険性が明らかになったということはできず，むしろ，ＦＷが期待された機能を発揮しており，通常の状態における住基ネットの安全性が確認されたものというべきである。同様に，品川区ペネトレーションテストの結果によっても，住基ネットのセキュリティに不備があるとは認められない。

また，斜里町事故等についてみても，斜里町事故は，職員の個人用パソコンから情報が流出したものである上，流出した情報も既に使用されていないパスワード等であって，今後の住基ネットのセキュリティに影響を及ぼすものであるとは認められないし，帯広市事故も，住基ネットのＣＳが操作されたというようなものではないから，これらの事故は住基ネットのセキュリティに問題があったことを示すものではなく，塙町事故は，住基ネットのセキュリティには直接関係のない事故であったと認められる。したがって，これらの事故が発生したことによって，住基ネットのセキュリティに不備があるとは認められない。

イ　データマッチングの危険性について

控訴人らは，住民票コードを用いることにより，国の機関等の各事務ごとに個別的に作成され保有されているデータベースから，その者固有の番号で各個人の個人情報を名寄せして，データマッチングできることになるため，住基ネットは個人情報のデータマッチングを極めて容易とするものであり，国民が行政によって管理・監視される社会を招来する危険性の高

いものであると主張するところ，本人確認情報の提供を受けられる事務を遂行する国の機関等は，当該事務を遂行のために必要な場合には，住民票コードの告知を求めることができ（住基法３０条の４２），住基ネットにより本人確認情報として住民票コードの提供を受けることができるから，上記事務に関して，住民票コードを要素とするデータベースを作成し，保有しているものと認められる。そして，住民票コードは，住民固有の番号で重複しないため，住民票コードによる検索が，氏名や生年月日，住所による場合に比べて正確であることは明らかである。また，住民票コードの一義性から，住民票コードはデータマッチングのキーとして容易に使用できるものである。

ところで，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日現在，２７５事務であるが，弁論の全趣旨によれば，これらの事務に関して行政機関が保有する個人情報を一元的に管理する主体は存在しないことが認められる。また，国の機関等に本人確認情報を提供する指定情報処理機関が保有している個人情報は，保存期間内の本人確認情報に限られ，指定情報処理機関が住民に関するデータベースを作成，保有することはないし，国の機関からデータベースの提供を受けることもないから，指定情報処理機関が，控訴人らの指摘するようなデータマッチングをする可能性はない。そして，住基法の規定による本人確認情報の受領者は，住基法により，当該事務の処理に関して提供を受けるものとされた事務の遂行に必要な範囲内に限り本人確認情報を利用するものとし，当該事務処理以外の目的のために本人確認情報の全部または一部を利用してはならないとされており（住基法３０条の３４），受領者は，住基法所定の範囲内に限り，本人確認情報とその保有する個人情報とを，比較，検索，結合することができるものであり，当該事務に属さない事務のために他の事務に関するデータベースと結合することは禁止されている。更に，国の機関等が，

他の国の機関等が保有する住民票データを含むデータベースの提供を受けることは，住基法３０条の４２により禁止されているから，他の国の機関等が保有するデータベースと結合を行うことはできないものというべきである。そのほか，都道府県知事や指定情報処理機関は，国の機関等に対する本人確認情報の提供の状況について，毎年少なくとも１回，報告書を作成して，公表することとされており（住基法３０条の７第８項，３０条の１１第６項），都道府県知事は，国の機関等に対して，提供した情報の適切な管理のための措置の実施状況につき報告を求め，適切な措置の実施を要請を行うものとされ，住民からの情報開示請求に対応するために，本人確認情報の提供と利用の情報を保存するものとされていて（セキュリティ基準第６の８），不正な利用に対する監視措置が講じられている。

また，行政個人情報保護法が，住基ネットにも適用（住基法が特別法であり，優先して適用される。）されるところ，同法においても，個人情報を保有するに当たっては，行政機関は，法令に定める事務を遂行するため必要な場合に限り，かつ，その利用の目的をできる限り特定しなければならないこと，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こと（行政個人情報保護法３条），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こと（同法８条）が定められており，これらの規定に抵触する個人情報の保有，利用又は提供が行われていると思料するときは，何人も行政機関の長に対して，個人情報の利用の停止，消去又は提供の停止を求めることができ（同法３６条ないし４１条），同請求に対する決定に関し，情報公開・個人情報保護審査会への諮問を含む不服申立手続が設けられている（同法４２条）。

住基ネットにおいて上記のとおりのセキュリティ対策が講じられていることに加え，行政個人情報保護法において国の機関等が保有する個人情報の利用制限が定められ，違法な利用等について是正を求める制度が設けら

れていることからすれば，現在，国の機関等において，控訴人らの個人情報が名寄せ，データマッチングの危険にさらされているということはできない。

控訴人らの主張は，将来における名寄せ，データマッチングの抽象的な危険性を指摘するものであって，現時点での住基ネットに具体的な危険性があることを主張するものとは認められない上，住基ネットにおける本人確認情報の提供先，利用目的の変更等は法律の改正によるべきものであって，国民の意思を離れて無制限に拡大する性質のものではないから，将来法律の改正によって提供先及び利用目的の変更があり得るからといって，住基ネットが名寄せ，データマッチングの可能性をもち，プライバシー保護の見地から危険な制度であるということはできない。

ウ　保護措置について

(ア)　控訴人らは，住基ネットは，現在ではやや時代遅れともいい得るＯＥＣＤ８原則をも満たしていないものであり，住基ネットにおいては，個人情報の保護のための十全な措置は講じられていないといわざるを得ないと主張する。

この点，弁論の全趣旨によれば，ＯＥＣＤ８原則は，昭和５５年９月２３日，ＯＥＣＤにおいて採択された「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」で定められたプライバシー保護のための原則であり，①収集制限の原則（個人データの収集には，制限を設けるべきであり，いかなる個人データも，適法かつ公正な手段によって，かつ適当な場合には，データ主体に知らせ又は同意を得た上で，収集されるべきである。），②データ内容の原則（個人データは，その利用目的に沿ったものであるべきであり，かつ利用目的に必要な範囲内で正確，完全であり，最新に保たれなければならない。），③目的明確化の原則（個人データの収集目的は，収集時より遅

くない時点において明確化されなければならず，その後のデータの利用は，当該収集目的の達成又は当該収集目的に矛盾しないで，かつ，目的の変更ごとに明確化された他の目的の達成に限定されるべきである。)，④利用制限の原則（個人データは，明確化された目的以外の目的のために開示，利用その他の使用に供されるべきではないが，(a)データ主体の同意がある場合，又は(b)法律の規定による場合は，この限りではない。)，⑤安全保護の原則（データは，その紛失若しくは不当なアクセス・破壊・使用・修正・開示の危険に対し，合理的な安全保障措置により保護されなければならない。)，⑥公開の原則（個人データに係る開発，運用及び政策については，一般的な公開の政策が取られなければならない。個人データの存在，性質及びその主要な利用目的とともに，データ管理者の識別，通常の住所をはっきりさせるための手段が容易に利用できなければならない。)，⑦個人参加の原則（個人は，(a)データ管理者が自己に関するデータを有しているか否かについて，データ管理者又はその他の者から確認を得る権利がある，(b)自己に関するデータを合理的期間内に，もし必要ならば過度にならない費用で，合理的な方法で，かつ，自己に分かりやすい形で自己に知らしめることができる権利がある，(c)上記２つの要求が拒否された場合には，その理由が与えられること及びそのような拒否に対して異議を申し立てることができる権利がある，(d)自己に関するデータに対し異議を申し立て，その異議が認められた場合には，そのデータを消去，修正，完全化，補正させることができる権利を有する。)，⑧責任の原則（データ管理者は，上記諸原則を実施するための措置に従う責任を有する。)，からなるものであることが認められる。

これを住基ネットについてみるに，住基法は，民間部門での利用の禁止（住基法３０条の６ないし３０条の８，３０条の４３第１ないし５項，

４４条，別表），都道府県及び指定情報処理機関での保有情報の限定（住基法３０条の５第１項），外部への情報提供の限定（住基法別表），行政機関の保護措置義務（住基法３０条の３３，３０条の３４，３０条の３５，４２条），情報漏えいの防止（住基法３０条の１７，３０条の２９，３０条の３１，３０条の３３，３６条の２，４２条），市町村におけるシステムの保護（住基法３６条の２），制度運用に関する住民参加（住基法３０条の３７，３０条の４０，３０条の４１，３６条の３），記録の最新性及び正確の確保（住基法３０条の５第１項，３０条の７，３０条の１１）等を定めているほか，住基ネットが前記認定のとおりのセキュリティ対策を講じていることからすれば，住基ネットは，少なくともＯＥＣＤ８原則には沿った内容となっているものと認められる。

(イ) 控訴人らは，住基ネットにおいては，内部者による情報漏えいを防ぐことはできず，プライバシーの保護は不十分であると主張する。

しかし，前記認定のとおり，住基ネットには合理的なセキュリティ対策が講じられている上，住基法は関係者には守秘義務を課し，違反行為に対しては通常の公務員の秘密保持義務違反の場合（国家公務員法１０９条１２号，１００条１，２項）よりも重い刑罰を科し（住基法３０条の３５，４２条），更に，行政個人情報保護法は，個人情報の保有を制限し（３条１，２項），利用及び提供を制限している（８条１項，２項２号，３号）ほか，関係者に対する罰則を設けている（５３ないし５７条）のであって，これらによって，内部者による情報漏えいの防止が図られているものということができる。確かに，将来にわたり内部者による個人情報の漏えいが絶無であると断定する根拠はないといわざるを得ないが，内部者による情報漏えいは，個人情報を扱う機関や団体においては常に起こりうる問題であり，個人の情報を収集，管理している者が，悪意をもってまたは興味本位で，職務上知り得た個人の情報をインター

ネット上を流通させるようなことは観念できないではないのであるから，このような非違行為は，コンピュータ社会の有する一般的な危険の範疇に属するものというべきであり，住基ネット固有の危険であるとはいえない。もとより，内部者による個人情報の流出はできる限りの措置を講じて防止すべきであることは当然であるが，そのことからコンピュータシステムに依存する住基ネットの運営自体を否定すべきことにはならないというべきである。

(ウ) 控訴人らは，住民票コードが民間利用される危険についても指摘するが，前記認定のとおり，住基法は，住民票コードの民間利用について禁止及び違反した場合の罰則を定めており，実効性のある防止措置が講じられているというべきである。

なお，証拠（乙Ａ２１の１，２）及び弁論の全趣旨によれば，全国銀行協会が調査したところ，住基法施行後に，住民票コード通知書を本人確認書類として受理した事例が７９行，２３６件あったが，いずれも銀行側から提示を求めたのではなく，顧客自らが提示したものであり，しかし，その後，全国銀行協会からの指示により，各行において住民票コードの本人確認記録書からの削除，住民票コード通知書のコピーの破棄を行い，金融庁から全国銀行協会に対して，住民票コードの利用制限の遵守について周知徹底を図ったことが認められる。このことからいえば，住基法施行後民間においてその趣旨を十分理解しない行為があったことは窺われるものの，その後是正措置も執られたものと認められ，現時点においても同様の事態が発生する具体的な危険があるとは認められない。

(エ) 控訴人らは，改正法施行の際には附則１条２項の定める所要の措置は何ら講じられていなかったし，その後成立した個人情報保護法及び行政個人情報保護法は，住基ネットの運用に関し，プライバシーの保護につ

いて万全の措置であるとは到底いい得ないものであると主張する。

しかし，改正法附則１条２項は，「この法律の施行に当たっては，政府は，個人情報の保護に万全を期するため，速やかに，所要の措置を講ずるものとする。」と定めているところ，同条項は，所要の措置につき，「施行に当たっては」，「速やかに」，「講ずるものとする」と規定しており，その文言に照らし，所要の措置を講じることが改正法の施行要件として定められたものとみることはできない。そのうえ，前記認定のとおり，住基法自体が国民のプライバシーの保護を十分配慮した内容となっている上，その後，個人情報保護法及び行政個人情報保護法が成立したこと，また，セキュリティ基準及び住基カードセキュリティ基準が制定され，プライバシー保護のための技術的措置が講じられていることからすれば，改正法附則１条２項の定める所要の措置が何ら講じられていないということはできないし，その内容がプライバシーの保護に関して万全の措置ではないということもできないというべきである。

(4) 住基ネットの差止めの可否について

ア 住基ネットの導入により改められた住基台帳事務には次のようなものがある。

(ア) 住民票写しの広域交付

住基台帳に記録されている者は，住基カード又は運転免許証等を提示して，その者が記録されている住基台帳を備える市町村の市町村長（以下「住所地市町村長」という。）以外の市町村長に対し，自己又は自己と同一の世帯に属する者に係る住民票写しで，住基法１２条の２第１項所定の事項を省略したものの交付を請求することができる（住基法１２条の２第１項，住基法施行規則５条２項）。この請求を受けた市町村長（以下「交付地市町村長」という。）は，電気通信回線を通じて住所地市町村長に通知し，住所地市町村長は，①氏名，②出生の年月日，③男

女の別，④世帯主・続柄（選択），⑤住民となった年月日，⑥住所，⑦住所を定めた旨の届出の年月日及び従前の住所，⑧住民票コード（選択）を交付地市町村長に電気通信回線を通じて通知して，この通知を受けた交付地市町村長が住民票写しを作成して，交付する（住基法１２条の２第２項ないし４項）。

(イ) 転出・転入手続の特例

転出・転入の手続には，転入届の際に転出地での住民票の情報を記載した転出証明書を添付しなければならない（住基法２２条２項，住基法施行令２３条）。しかし，住基カードの交付を受けている者が，住基法施行令に定める一定の事項が記載された「付記転出届」をした場合には，当該届出をした日以後最初に行う転入届であって，住基カードを添えて行われるものについては，転出証明書の添付を要しない（住基法２４条の２第１項）。

イ 住基ネットによる本人確認情報の提供を受けることにより，各種申請手続等における住民票の写しの提出が不要になったり，文書の提出が不要になるなどの住民の利便性の向上と行政の効率化が図られている。

また，住基カードにより，行政手続のオンライン申請など，オンライン利用行為に有用な公的個人認証サービスを行うことや，条例利用アプリケーションの活用が可能となっている。

すなわち，証拠（甲１９６，２０１，乙Ａ２ないし９，４２，４３，４５）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。

(ア) 平成６年１２月２５日付けの閣議決定「行政情報化推進基本計画」によれば，政府機関内における情報の円滑な流通，情報共有等を図るため，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として霞が関ＷＡＮを整備することとされ，平成９年１月からその運用が開始された。

平成８年３月に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発表した「『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』報告書」によれば，ネットワークシステムを構築することは，住基台帳事務の効率化・広域化や，その他住民の利便性の向上等に大きく資するものとされた。

平成１２年８月２８日付けの「ＩＴ革命に対応した地方公共団体における情報化施策等の推進に関する指針」では，国の電子政府構築に対応して，地方公共団体についても，各地方公共団体を相互接続し，霞が関ＷＡＮとも接続する総合ネットワークの整備を促進するとともに，住民の利便の観点から，行政手続のオンライン化を進めるべきであるとされた。また，改正法の趣旨を踏まえて地方公共団体がＩＴ革命に対応し，情報化政策を総合的に推進していくための新たな指針として，地方公共団体には，住基ネットの整備促進に向けた対応を行う必要があるとされた。

(イ) ＩＴ戦略本部は，平成１３年１月２２日，「ｅ－Ｊａｐａｎ戦略」を発表し，５年以内に世界最先端のＩＴ国家となることを目的として掲げた。そして，その前提条件となる社会環境を構築するためには，電子政府の実現が推進されるべきものとされ，これにより，平成１５年度には，原則として２４時間，自宅やオフィスからインターネットを利用して実質的にすべての行政情報の閲覧，申請・届出等の手続，手数料納付・政府調達手続が可能となるような社会を目指すものとされた。

その後，ＩＴ戦略本部は，平成１３年３月２９日に「ｅ－Ｊａｐａｎ重点計画」，同年６月２６日に「ｅ－Ｊａｐａｎ２００２プログラム」，同年１１月７日に「ｅ－Ｊａｐａｎ２００２プログラムの加速・前倒し」，平成１４年６月１８日に「ｅ－Ｊａｐａｎ重点計画－２００２」をそれぞれ策定し，平成１５年７月２日には，ＩＴ基盤整備は達成され

たものとし，「ｅ－Ｊａｐａｎ戦略Ⅱ」を発表し，同年８月８日に「ｅ－Ｊａｐａｎ重点計画－２００３」を発表し，電子政府の構想を具体化させていった。

(ウ) 住基ネットの運用開始により，現在では，パスポートの交付申請などの際に必要とされていた住民票の写しの提出が不要となり，年金受給者（加給年金対象者等を除く。）が毎年提出することが必要とされていた現況届又は身上報告書の提出が不要となり，恩給受給者が毎年市町村長の証明印を受けて提出することが必要とされていた受給権調査申立書の提出が不要となるなど，住民の利便性及び行政の効率化が図られている。

ウ 以上によれば，住基ネットは，行政事務の効率化，住民負担の軽減及び利便の向上を図るものであると認められる上，電子政府等の実現のために一定の役割を果たしているものと認められ，これらによれば，住基ネットの必要性及び合理性が肯定できるものというべきである。

なお，控訴人らは，「電子政府・電子自治体構想のもとになるＩＴ革命あるいはＩＴ戦略」が問題になったのは平成１２年以降であり，これに対して，改正法の閣議決定は平成１０年３月１０日であり，その国会成立は，平成１１年８月１２日であるから，電子政府等の構想が浮上したのは，改正法の成立以後のことであり，電子政府等の実現が住基法改正の目的であるというのは事実に反するものであると主張する。しかし，上記認定のとおり，政府機関内における情報の円滑な流通，情報共有等を図るためのネットワーク化という構想は早くからあった上，証拠（乙Ａ２，３）によれば，住基法は，検討時点から，高度情報化社会に対応していくことを目的としていたものであることが認められるから，住基ネットを使用して高度情報通信ネットワーク社会に対応するという動きは当初からあったものといえ，住基ネットは電子政府等の構想に合致するものであるということができるから，電子政府等の構想が具体化したのが平成１２年以降であるか

らといって，住基ネットの有用性を否定する根拠とはならないというべきである。

そして，前記のとおり，本人確認情報が，予定された開示対象及び利用範囲を逸脱してみだりに開示されないという限度では個人の期待は法的保護に値するものというべきであるが，住基ネットには上記のような必要性，合理性がある上，プライバシー保護のための合理的な措置が採られていること，一方で，本人確認情報は必ずしも秘匿する必要が高い情報であるとはいえないことを考慮すると，住基ネットの運用によって控訴人らのプライバシー権が侵害される可能性及び程度は低いということができ，住基ネットの運用によって控訴人らが精神的苦痛を受けたとしても，受忍限度を超えるものであるとは認め難い。

エ　控訴人らは，住基ネットの運用そのものの差止めを求めているのではなく，控訴人らが住基ネットから離脱することを求めているにすぎず，控訴人らが住基ネットから離脱をしても，当該市町村や他の自治体，あるいは，国の機関等の行政事務に住基ネット全体の運用が成り立たないような重大な支障を生じさせるものではないと主張する。

しかし，仮に控訴人らの本人確認情報の提供等を差し止めた場合，住基ネットによる事務と従来の方式による事務とを併存させざるを得ないこととなり，そのための職員を配置する必要が生じて，新たな負担を余儀なくされることが予想されるし，本人確認情報の提供・利用が行われる都度，住民票コードの記載や本人確認情報の通知提供を希望しない住民であるかどうかを確認せざるを得ないことになり，事務が繁雑となることは避けられない。しかも，控訴人らの本人確認情報の提供等を差し止めた場合，市町村間のネットワークが寸断され，控訴人らの居住地以外の自治体においても，住基ネットによらない従来の方式による事務を併存させざるを得なくなるから，住基法の目的とする住基台帳事務の効率化が阻害されること

は明らかである。

したがって，控訴人らの上記主張は採用できない。

(5) 以上によれば，控訴人らのプライバシー権侵害に基づく差止請求はいずれも理由がない。

2 争点(2)（人格権侵害に基づく差止請求の可否）について

控訴人らは，住基ネットは，行政が，国民に対し，一方的に番号（住民票コード）を付し，これを本人の意向を無視して行政の便宜のために利用しようとするものであって，国民を番号で扱うことにほかならず，国民の人格権を侵害するものであると主張する。

しかし，住民票コードは，多人数の個人情報を管理するための技術的な観点から便宜上付された番号であるにすぎず，行政機関が住民に対する呼称として氏名等に代わって使用するという性質のものではない。今日においては，膨大な情報を管理する便宜上，情報整理のための番号等を用いて個人ごとの情報を管理することは，日常生活のさまざまな場面において通常に行われていることであり，住民票コードの割当て，あるいはその使用により，控訴人らの人格権あるいは何らかの人格的利益が侵害されたものとは認められない。

したがって，控訴人らの人格権侵害に基づく差止請求はいずれも理由がない。

3 争点(3)（公権力から包括的に管理されない自由の侵害に基づく差止請求の可否）について

控訴人らは，憲法１３条は，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（公権力から包括的に管理されない自由）を国民に保障しているところ，住基ネットは，住民票コードをさまざまな行政機関が個別に蓄積・保有していた個人情報を結合させる基点として，公権力による国民個人の情報の一元的管理を可能とするものであるから，控訴人らの公権力による包括的管理からの自由を侵害するものであると主

張する。

しかし，控訴人らの主張する「公権力による包括的管理からの自由」は，そもそもその具体的内容が不明確であり，憲法によって保障された権利であるとは認め難い。しかも，仮に，控訴人らの主張するような「行政によって包括的に管理されない自由」が法的保護に値するとしても，前記認定のとおり，住基ネットによって，控訴人らの個人情報が名寄せ，データマッチングにより包括的に管理される危険性があるとは認められないから，いずれにしても，住基ネットが，控訴人らが主張する「行政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とは認められない。

したがって，控訴人らの公権力から包括的に管理されない自由の侵害に基づく差止請求はいずれも理由がない。

4　争点(4)（損害賠償請求の可否）について

控訴人らは，被控訴人国については，プライバシー及び人格権を侵害する法改正を行い，その施行を延期しないばかりか，所要の措置を講じないまま，平成１４年８月５日から住基ネットの運用を強行したことから，また，被控訴人愛知県については，各自治体の有する本人確認情報をネットワーク化したことから，控訴人らに精神的損害を与えたため，国賠法１条により控訴人らに対する損害賠償責任を負うと主張する。

しかし，既に認定したとおり，住基ネットに控訴人らの主張するような危険性が認められないことや，住基ネットに必要性・有用性が認められることからすれば，住基ネットの運用が控訴人らの受忍限度を超えてそのプライバシーないし人格権を侵害しているものとは認められない。

したがって，控訴人らの損害賠償請求はいずれも理由がない。

5　結語

以上の次第で，控訴人らの請求はいずれも理由がないから棄却を免れず，これと同旨の原判決は正当である。

よって，本件各控訴はいずれも理由がないから棄却することとし，主文のとおり判決する。

名古屋高等裁判所民事第４部

裁判長裁判官　　野　田　武　明

裁判官　　戸　田　彰　子

裁判官　　濱　口　浩