甲第72号証

平成１８年１１月３０日判決言渡　同日原本領収　裁判所書記官

平成１６年（ネ）第１０８９号損害賠償請求控訴事件（原審・大阪地方裁判所平成１４年（ワ）第１１４００号）

口頭弁論終結日　平成１８年４月２５日

判　　決

控訴人	別紙控訴人目録ＡないしＥ記載のとおり
控訴人ら訴訟代理人弁護士	桜井健雄
同	上原康夫
同	大川一夫
同	井上二郎
同	平栗勲
被控訴人	別紙被控訴人目録記載のとおり
被控訴人ら指定代理人	石井義規
同	奥畑薫
同	堀江明子
同	橋本一郎
被控訴人豊中市指定代理人	小野勝康
同	山崎光昭
被控訴人箕面市指定代理人	高橋正信
同	西尾仁志
被控訴人吹田市指定代理人	船津克己
同	前村誠一
被控訴人守口市指定代理人	小林憲和
被控訴人八尾市指定代理人	山野公嗣
同	奥田紀明

主　　文

1　被控訴人箕面市は，住民基本台帳から控訴人[redacted]の住民票コードを削除せよ。

2　被控訴人吹田市は，住民基本台帳から控訴人[redacted]の住民票コードを削除せよ。

3　被控訴人守口市は，住民基本台帳から控訴人[redacted]及び同[redacted]の各住民票コードを削除せよ。

4　控訴人[redacted]，同[redacted]　同[redacted]及び同[redacted]のその余の当審追加請求を棄却する。

5　控訴人らの控訴を棄却する。

6　控訴費用は，控訴人[redacted]と被控訴人箕面市との間においては，これを２分し，それぞれを各自の負担とし，控訴人[redacted]と被控訴人吹田市との間においては，これを２分し，それぞれを各自の負担とし，控訴人[redacted]と被控訴人守口市との間においては，これを２分し，それぞれを各自の負担とし，控訴人[redacted]と被控訴人守口市との間においては，これを２分し，それぞれを各自の負担とし，その余の控訴人らの控訴費用は，同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　被控訴人豊中市は，別紙控訴人目録Ａ記載の各控訴人らに対し，それぞれ５万円及びこれに対する平成１４年８月５日から支払済みまで年５分の割合による金員を支払え。

3　被控訴人箕面市は，別紙控訴人目録Ｂ記載の控訴人に対し，５万円及びこれに対する平成１４年８月５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　被控訴人吹田市は，別紙控訴人目録Ｃ記載の控訴人に対し，５万円及びこれに対する平成１４年８月５日から支払済みまで年５分の割合による金員を支払え。

5　被控訴人守口市は，別紙控訴人目録Ｄ記載の各控訴人らに対し，それぞれ５万円及びこれに対する平成１４年８月５日から支払済みまで年５分の割合による金員を支払え。

6　被控訴人八尾市は，別紙控訴人目録Ｅ記載の控訴人に対し，５万円及びこれに対する平成１４年８月５日から支払済みまで年５分の割合による金員を支払え。

7　（控訴人[redacted]の当審追加請求）

(1)　被控訴人箕面市は，控訴人[redacted]の本人確認情報を大阪府知事に通知してはならない。

(2)　主文第１項と同旨

8　（控訴人[redacted]の当審追加請求）

(1)　被控訴人吹田市は，控訴人[redacted]の本人確認情報を大阪府知事に通知してはならない。

(2)　主文第２項と同旨

9　（控訴人[redacted]及び同[redacted]の当審追加請求）

(1)　被控訴人守口市は，控訴人[redacted]及び同[redacted]の各本人確認情報を大阪府知事に通知してはならない。

(2)　主文第３項と同旨

第２　事案の概要

本件は，控訴人らが，住民基本台帳ネットワークシステム（以下「住基ネット」という。）により，プライバシーの権利等の人格権を違法に侵害され，精神的損害を被ったと主張して，控訴人らが居住する被控訴人各市に対し，国家賠償法１条に基づく損害賠償（慰謝料）の請求（附帯請求は遅延損害金請求）

をし，また，当審において，控訴人[redacted]，同[redacted]，同[redacted]及び同[redacted]（以下，この４名を「控訴人[redacted]ら４名」といい，差止め請求関係では単に「控訴人ら」ということもある。）が，各居住地の被控訴人市に対し，上記権利に基づく妨害排除請求（侵害状態の除去請求）として住民基本台帳からの住民票コードの削除及び上記権利に基づく妨害予防請求として住基ネットを使用して本人確認情報を大阪府知事に通知することの差止め（これらを合わせて，以下「差止め」という。）を追加請求した事案である。

原審裁判所は，控訴人らの原審請求を棄却した。控訴人らは，これを不服として控訴し，控訴人[redacted]ら４名は，上記のとおり当審において差止め請求を追加した。

1　前提となる事実（証拠を掲記しない事実は，当事者間に争いがない。）

(1)　当事者

ア　控訴人らは，それぞれ肩書き住所地に居住し，住民登録をしている者である。

イ　被控訴人らは，いずれも普通地方公共団体である。

(2)　住民基本台帳制度

住民基本台帳制度は，住民基本台帳法（昭和４２年法律第８１号）に基づき，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制度として創設され，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ものである（同法１条）。

住民基本台帳は，同法７条に規定する事項を記載（磁気ディスクをもって調製する場合は記録）する住民票を編成して作成される（同法６条）。

(3)　住民基本台帳法の改正（住民基本台帳ネットワークシステムの導入）

ア　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」という。）により改正され（以下同法による改正後の住民基本台帳法を「住基法」という。），同法のうち，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（同法３０条の７第１項，第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（同法３０条の２），都道府県知事（以下「知事」という。）への電気通信回線を通じた本人確認情報の通知（同３０条の５），本人確認情報の提供（同法３０条の６）に係る規定は，平成１４年８月５日に，住民票の写しの広域交付（同法１２条の２），転出転入特例（同法２４条の２），住民基本台帳カード（同法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）。

イ　改正法は，附則１条２項において，「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。」と定めた。

(4)　住基ネットの概要

ア　住基ネットの仕組み

住民基本台帳の情報は，住民基本台帳を保有する各市町村内で利用されてきたが，住基ネットは，地方公共団体の共同のシステムとして，住民基本台帳のネットワーク化を図り，特定の情報の共有により，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民基本台帳に関する事務処理を行うものである。

すなわち，市町村には，既存の住民基本台帳電算処理システム（居住する住民の住民票を記録，管理するサーバ。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を接続し，その市町村の住

民の本人確認情報を記録，管理するシステムであるコミュニケーションサーバ（以下「ＣＳ」という。）が設置され，本人確認情報は，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，管下の全市町村のＣＳから送信された本人確認情報を記録，管理するシステムである都道府県サーバが設置されている。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。）に本人確認情報処理事務を行わせることができる（住基法３０条の１０第１項本文）。指定情報処理機関に本人確認情報処理事務を行わせることとした知事から送信された住民の本人確認情報が，指定情報処理機関に設置されたサーバに保存される（同法３０条の１１）。指定情報処理機関には，全国サーバ（全都道府県の都道府県サーバから送信された本人確認情報を記録，管理するサーバ）及びコールセンター（市町村及び都道府県からの住基ネットの障害連絡や問い合わせを一元的に受け付け対応する機関）が設置されている。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いる。また，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（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であり，機能的には，組織内外からの通信要求をすべて捕捉し，定められたルールに従って通過させたり禁止したりすることによって，必要なサービスだけをユーザーに提供しつつ，セキュリティを確保するシステム。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。

イ　本人確認情報

本人確認情報とは，住民票の記載事項のうち，氏名，出生の年月日，男女の別及び住所（以下「４情報」という。），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（変更情報）をいう（住基法３０条の５第１項，７条１号ないし３号，７号及び１３号）。

上記の変更情報は，政令により，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が生じた年月日，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が生じた年月日，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が生じた年月日並びに修正前住民票コードが定められている（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。

ウ　住民票コード

(ｱ)　住民票コードの意義

住民票コードは，全国を通じて重複しない，無作為に作成された１０桁の数字及び１桁の検査数字をその順序により組み合わせた数列であり，住民票に記載される（住基法７条１３号，同法施行規則１条）。

(ｲ)　住民票コードに係る措置等

a　住民票コードの指定

知事は，区域内の市町村の市町村長ごとに，住民票に記載することのできる住民票コードを無作為に指定し，市町村長に通知する（住基法３０条の７第１項，同法施行規則１４条１項）。

知事は，住民票コードの指定を行う場合には，あらかじめ他の知事と協議し，市町村長に対して指定する住民票コードがそれまでに指定された住民票コード又は他の知事が指定しようとする住民票コードと

重複しないよう調整を図る（住基法３０条の７第２項）。

b　住民票コードの住民票への記載と通知

市町村長は，新たにその市町村の住民基本台帳に記録されるべき者について住民票の記載をする場合，その者がいずれの市町村においても住民基本台帳に記録されたことがない者であるときは，上記知事から指定された住民票コードのうちから選択するいずれか一の住民票コードを記載する（同法３０条の２第２項）。この場合，市町村長は，速やかに，住民に対し，その旨及び住民票コードを書面によって通知する（同条の２第３項）。

c　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，住民基本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自己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（同法３０条の３第１項）。

d　住民基本台帳の一部の写しの閲覧等の際の住民票コードの除外

住民票コードは，一般人の住民基本台帳の写しの一部の閲覧の際には閲覧対象から除外されており（同法１１条１項），また，自己又は自己と同一世帯に属する者以外の者に係る住民票の写し等の交付の際には，住民票コードは住民票の写し等の記載から省略される（同法１２条２項）。

エ　本人確認情報の通知・保存

(ｱ)　通知

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記載の修正を行った場合には，本人確認情報を知事に通知する（住基法３０条の５第１項）。この通知は，市町村長の使用に係る電子計算機から電気通信回線を通じて知事の使用に係る電子計算機に送信することによって行う（同条の５第２項）。

(イ) 保存

市町村長から通知を受けた知事は，通知された本人確認情報を磁気ディスクに記録し，これを通知の日から政令で定める期間（原則５年間）保存しなければならない（同条の５第３項，同法施行令３０条の６）。

オ　本人確認情報の提供及び利用

(ア) 市町村長による提供

市町村長は，条例で定めるところにより，他の市町村の市町村長その他の執行機関から事務処理に関し求めがあったときは，本人確認情報を提供する（住基法３０条の６）。

(イ) 知事による提供

a　国の機関又は法人に対する提供

知事は，住基法別表第１の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を提供する（住基法３０条の７第３項）。

b　当該都道府県の区域内の市町村の市町村長等に対する提供

知事は，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区域内の市町村の市町村長から求めがあったときは，いずれも政令で定めるところにより，③区域内の市町村の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときは，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（同法３０条の７第４項）。

c　他の都道府県の知事等に対する提供

知事は，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は，いずれも政令で定めるところにより，③他の都道府県の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときは，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７第５項）。

知事は，①他の知事を経て他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他の知事を経て他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は，いずれも政令で定めるところにより，③他の知事を経て他の区域内の市町村の執行機関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７第６項）。

知事は，当該都道府県の条例で定める執行機関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）。

(ウ) 都道府県における本人確認情報の利用

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統計資料の作成を行うとき，のいずれかに該当する場合には，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）。

(エ) 国の行政機関による資料提供要請

国の行政機関は，その所掌事務について必要があるときは，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）。

カ　住基ネット利用可能事務の範囲

住基ネットの利用による本人確認情報の提供，利用が可能な事務は，住基法別表第１ないし第５の改正等により，現在（平成１７年４月１日現在）２７５事務となっている。

キ　都道府県審議会

都道府県に，本人確認情報の保護に関する審議会を置き，住基法によりその権限に属させられた事項を調査審議させるとともに，知事の諮問に応じ，本人確認情報の保護に関する事項の調査審議及び知事への建議をさせることができる（住基法３０条の９）。

ク　指定情報処理機関

(ア) 知事は，指定情報処理機関に，住基法３０条の１０第１項所定の本人確認情報処理事務を行わせることができる（同条項）。

その本人確認情報処理事務は，住民票コードの指定及びその通知（同法３０条の７第１項），協議及び調整（同条第２項），国の機関又は法人，区域内外の市町村長又は市町村の執行機関に対する本人確認情報の提供（同条第３項ないし第６項），国の行政機関に対する本人確認情報に関する資料の提供（同法３７条２項）と定められている。

委任知事は，原則として本人確認情報処理事務を行わない（同法３０条の１０第３項）。

委任知事は，電子計算機から電気通信回線を通じて指定情報処理機関の電子計算機に送信することによって，本人確認情報を指定情報処理機関に通知する（同法３０条の１１第１，第２項）。委任知事から通知を受けた指定情報処理機関は，当該通知に係る本人確認情報を磁気ディスクに記録し，これを通知の日から政令で定める期間（原則５年間）保存する（同条第３項）。

旧自治大臣は，平成１１年１１月１日，指定情報処理機関として財団

法人地方自治情報センター（以下「情報センター」という。）を指定した。

(イ) 指定情報処理機関は，毎年，国の機関等への本人確認情報の提供状況を公表する（住基法３０条の１１第６項)。また，委任知事に対し，本人確認情報の電子計算機処理に関し必要な技術的な助言及び情報の提供を行う（同条第７項)。

(ウ) 指定情報処理機関には，本人確認情報保護委員会を置き，指定情報処理機関の代表者の諮問に応じ，本人確認情報の保護に関する事項を調査審議し，これに関し必要と認める意見を指定情報処理機関の代表者に述べることができる（住基法３０条の１５第１，第２項)。

(エ) 総務大臣は，本人確認情報処理事務等の適正な実施を確保するため必要があると認めるときは，指定情報処理機関に対し，上記各事務の実施に関し監督上必要な命令をすることができる。委任知事も，指定情報処理機関に対し，上記各事務の適正な実施のために必要な措置を講ずべきことを指示することができる。（同法３０条の２２）

総務大臣及び委任知事は，本人確認情報処理事務等の適正な実施を確保するため必要があると認めるときは，指定情報処理機関に対し，本人確認情報処理事務等の実施状況に関して必要な報告を求め，また，職員に，指定情報処理機関の事務所に立ち入って本人確認情報処理事務等の実施の状況，帳簿，書類その他の物件を検査させることができる（同法３０条の２３第１，第２項)。

ケ　住民基本台帳事務

(ア) 住民票写しの広域交付（交付の特例）

住民基本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民基本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（同法１２条の２第１項，同法施行規則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（同法１２条の２第２項ないし第４項)。

(イ) 転出・転入手続の特例

転出・転入手続には，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することが必要とされ（住基法２２条２項，同法施行令２３条)，住民は，通常，転出証明書の交付を受けるため，転出地の市役所等に出向く必要がある。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，当該転出届をした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（同法２４条の２第１項)。

コ 住基カード

住民基本台帳に記録されている者は，住民基本台帳を備える市町村の市町村長に対し，自己の住基カード（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)。

(5) 本人確認情報の開示

何人も，知事又は指定情報処理機関に対し，自己に係る本人確認情報について，書面により開示請求ができ，知事又は情報処理機関は，その請求があったときは，開示請求者に対し，これを開示しなければならない（住基法３０条の３７）。

(6) 住基ネットの稼働（甲１０，弁論の全趣旨）

平成１４年８月５日，住基ネットの本運用（第１次稼働）が開始された。

しかし，東京都杉並区，東京都国分寺市，福島県矢祭町は，個人情報保護のための法制度が未だ十分整備されていないなどとして，住基ネットへの不参加を表明し，住基ネットへの接続を行わなかった。第１次稼働開始後，三重県二見町及び小俣町は，同月９日から参加したが，東京都中野区は同年９月１１日，東京都国立市は同年１２月２６日，住基ネットから離脱した。また，神奈川県横浜市は，住基ネットに参加することを前提にしつつ，安全性が確認できるまでの間，非通知の申出をした住民の住民票コードは通知しないこととする選択方式（横浜方式）を採用し，本人確認情報について神奈川県へ非通知とすることの申出を受け付けたところ，約８４万人（全人口の約２４％）から非通知の申出があった。総務省は，当初，選択制は住基法３０条の５に反し違法であるとの見解を表明し，神奈川県も，参加者のみの一部データは受入できないとしていたが，平成１５年４月９日，横浜市，神奈川県，総務省，情報センターとの間で，段階的受入の合意がされた。

平成１５年５月２３日に個人情報保護法が成立した後，東京都国分寺市（同月２８日）及び東京都中野区（同年８月１３日）が，住基ネットへの接続を表明した。

２ 争点

(1) 住基ネットによる控訴人らの権利の侵害の有無（被控訴人らが，住民票コードを控訴人ら住民に割り振り，住民票コードを住民票に記載し，平成１４

年８月５日，住基ネットに接続したことにより，控訴人らの主張する権利が侵害されたと認められるか。）

(2) 控訴人らの慰謝料請求権の有無

(3) 控訴人[redacted]ら４名の差止め請求権の有無と差止め請求の可否

3 争点についての当事者の主張

(1) 住基ネットによる控訴人らの権利の侵害の有無

【控訴人らの主張】

ア 控訴人らの権利

(ア) プライバシーの権利

a 憲法１３条は，国民のプライバシーの権利として自己情報コントロール権（自己情報決定権）を保障している。自己情報コントロール権とは，自己に関する情報を，いつ，どのように，どの程度まで，開示するのかしないのか，及び，利用ないし提供の可否を自ら決定する権利である。国民は，自己に関する個人情報の収集・取得，管理（保有）・利用，開示・提供につき，情報主体によるコントロール権を有する。

したがって，行政機関による個人情報の取扱いが問題となる場面においては，情報主体の「コントロール」（同意・意思決定）が最大限保障されなければならず，行政機関が本人の同意なく国民のプライバシー情報を収集・取得し，保有・利用し，開示・提供することは，原則として違法である。それが例外として許容される場合があるとしても，それは，本人の同意を不要とする程のやむにやまれない利益を達成する必要がある場合でなければならず，あるいは，厳格な合理性を有する正当な目的により行わなければならない。しかも，プライバシーに対しより制限的でない態様でしか許されない。それゆえ，行政機関が，国民のプライバシー情報をこのような要件を満たすことなく収集・取得し，保有・利用し，開示・提供すれば，それは国民のプライ

バシー権の侵害として憲法違反となる。

b　また，国民は，プライバシー権の一環として，公権力から監視され，包括的に管理されない自由権（公権力から一方的に全人格的な管理の客体に置かれないという自由権）を有している。また，プライバシー権は，それが個人の尊厳に由来するものであることから，多様な権利概念を含むものとして認識されるようになった。その中には，平穏生活権も含まれる。平穏生活権は，法的保護に値する人格的利益として観念される。すなわち，人は，他者から，自己の欲しない刺激によって心の静穏を乱されない権利，利益を有する。これらの権利は，プライバシー権が認められるのと同様に，憲法１３条の幸福追求権に基づくものであり，同条により保障されているものである。

(イ)　人格権

憲法１３条は個人の尊厳を保護し，人格権を保護している。人は個人としての尊厳を有し，その人格は最大限尊重されるべきことは論をまたない。人はそれぞれに姓名を持ち，人格を持っているのであって，番号ではない。人を番号で呼び合うようなことは，個人の尊厳を侵害するものである。

イ　住基ネットによる控訴人らの権利の侵害

(ア)　プライバシー権の侵害

住基ネットは，すべての国民に一方的に１１桁の住民票コードを付し，そのコードとともに氏名，生年月日，性別，住所及びそれらの情報の変更履歴が，本人の与り知らないままに，市町村と都道府県・情報センターの間で専用回線をもって構築された住基ネットを流通し，本人確認情報として提供され，利用される。情報センターから国へ提供され，国が利用する事務は，２６４に及ぶ。この間，本人の同意を得られることはまったくなく，本人に選択の余地はまったく与えられない。とりわけ，

住基ネットは，住民票コードという「共通番号」の付されたデジタル化された情報であり，その伝播力は大きく，その提供，利用による被害の危険性は，計り知れないものである。そして，住基ネットは，必要性，有用性のないものであり，個人情報漏えいの危険性のあるものである。

このような住基ネットにより，控訴人らの同意なく控訴人らの個人情報を流通・提供・利用することは，憲法１３条により保障されている控訴人らのプライバシー権としての自己情報コントロール権を侵害するものである。

(イ) 公権力から監視，包括的に管理されない自由権，平穏生活権の侵害

住民票コードは，国民全員に対して重複しないように付された個人識別番号であり，多数の行政機関がそれぞれ保有している個人情報を統合し，個人情報を検索するために不可欠のものである。住基ネットによる個人情報は，現状では一応限定されているが，住基法は，政省令に多くを委任しており，将来，住基ネットによる個人情報の拡大を防ぐ保証はない。また，情報が限定されているとしても，そもそも個人の情報を一か所に集中させること自体，その個人の公権力から監視されない権利を侵害するものである。さらに，本人確認情報の送信は，将来のいわゆる国民総背番号制に道を開くものであり，国民総背番号制となれば，まさに監視社会そのものであり，公権力から監視されない権利を侵害するものである。現在の住基ネットでは，公権力から監視されず，包括的に管理されない自由権が侵害される具体的危険性がある。

また，住基ネットにより，住民は，自己の個人情報が，住基ネットで国によって集中的に管理されることにより，それが漏えいされるのではないか，他人に知られたくない自己の情報が不当に利用されるのではないか，ときには公開されるのではないか，との不安感，危惧，危機感を常に抱きながらの生活を余儀なくされる。これは，まさに，他者から自

己の欲しない刺激によって心の静穏を乱されることにほかならず，これは，生活における精神的平穏の侵害であって，プライバシーの権利の一態様である平穏生活権を侵害するものである。

(ウ) 人格権の侵害

人はそれぞれに姓名を持ち，人格を持っているのであって，番号ではない。人を番号で呼び合うようなことは個人の尊厳を侵害するものである。被控訴人らが，勝手に，１１桁の番号を控訴人らにつけることは，そのこと自体，憲法１３条で保護されている控訴人らの人格権を侵害している。

各行政機関が，その各行政機関ごとに国民の情報を保有することはその限りでやむを得ないものであるが，住民票コードは，そのような限定番号ではなく，１１桁の番号によって，個人の情報が一か所に集められることが可能な共通番号であり，個人情報の蓄積，結合，検索のマスターキーとして使用して，個人情報のデータファイルを作成し，個人のあらゆる行政情報を１箇所にまとめることを可能にするものである。このような住民票コードによって，個人の情報が一か所に集められるのは，行政目的をはるかに超え，その個人を全人格的に管理するものであって，その個人の人格権を侵害するものである。

ウ 住基ネットによる個人情報漏えいの危険性

(ア) 住基ネットによる控訴人らの個人情報の流出の危険性が，次のとおり考えられる。

a ハッカー等による外部からのネットワークへの侵入の危険性

b 運用関係者などによる漏えい等の危険

(a) 住基ネットの運用従事者による情報漏えい等の危険

(b) 公務員等の職権濫用等による情報利用の危険

(c) 民間委託者の不正行為による情報漏えいの危険

(d) バックアップデータの紛失，窃取による情報漏えいの危険

c セキュリティ対策の不整備

(a) ハード面でのセキュリティ対策の不整備

(b) ソフト面でのセキュリティ対策の不整備

(イ) 住基ネットの安全性は，コンピュータ通信網全体が外部や内部からの情報取得権限のない者が磁気ディスクに記録された情報を取得することができないようになっているかどうかにかかっている。通信網につながるすべてのコンピュータの安全性が技術面においても運用面においても確保されていなければ，結局，住基ネットの安全性は十分に確保されているとはいえず，全国の各市町村に置かれているすべてのＣＳを含めて十分なセキュリティが確保されなければならない。ＣＳの安全性が不十分な市町村が一つでもあれば，当該市町村の住民の個人情報のみならず，すべての国民の個人情報が流出することになる。住基ネットの各市町村のセキュリティ体制には重大な欠陥があり，本人確認情報に不当にアクセスされたり，同情報が漏えいしたりする具体的危険性があるというべきである。住基ネット稼働下では，個人情報流出の危険は飛躍的に高まった。

(ウ) 長野県本人確認情報保護審議会の調査結果をみても，担当職員がＣＳの安全性の不十分さを感じている。また，長野県が行った住基ネットの侵入実験の結果，通信網に幾つかの脆弱性が発見され，住基ネットの安全性の程度は平均以下で，平均的なコンピュータエンジニアなら誰でも侵入し，情報を盗んだり損害を与えることができることが実証された。すなわち，パスワードの設定に問題があったほか，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，一定の条件の下においては，一般に入手可能なツールによるＣＳの管理者権限を取得することが具体的に可能な状況にあった。そして，管理者権限を奪取すると，住基ネッ

ト網を介して各市町村ＣＳや指定情報処理機関のサーバ内の本人確認情報が閲覧され，漏えいしたり，改ざんされたりする危険があることが実証された。

また，通信網やＣＳの安全性にとって最も脅威なのは，人間そのものである。末端の職員まで統一した考え方で十分な教育を受けていなければ，情報が持ち出されてしまう可能性がある。そして，全国の多数の自治体において，セキュリティが職員の信頼関係のみに支えられており，各職員の信頼関係が悪用され情報が持ち出される危険性は高く，また，それを防ぎ得る十分な体制は全く整っていない。

(エ) 総務省告示による「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及び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年同第３９１号，同第６０１号。以下「セキュリティ基準」という。）により，各自治体における住基ネットの運用及びセキュリティ（正確性，機密性及び継続性の維持）について一定の技術水準を求めている。しかしながら，以下のとおり，各自治体の運用状況は，セキュリティ基準からほど遠いものであり，セキュリティの上で欠陥がある。

a　重要機能室（電子計算機室，磁気ディスク等保管室，受電設備等の設備を設置する室，空気調和機及びその付属設備を設置する室）の配置及び構造として，電子計算機室及び磁気ディスク等保管室は他の部屋と区別して専用の部屋とすること（セキュリティ基準第３－１－(2)エ），重要機能室への入室者を限定し入退室管理カードによって重要機能室に入退室する者が入室する権限を有すること等により，入退室の管理を適切に行うこと（同第４－(1)）とされている。このため各自治体は住基ネットのＣＳの管理運用のため庁内に重要機能室を設置しているが，その運用は杜撰であり，セキュリティ基準を満たしていな

い。例えば，被控訴人八尾市では，重要機能室への入退室の管理簿もなく，重要機能室への入退室を記録する管理簿に記入するなどすることなく入退室しているなど，重要機能室への入退室の厳正なチェックが行われていない。被控訴人吹田市においては，平成１７年１月まで入退室管理簿は作成されず，その作成後それに実際に記録されているかどうかは，確認されていないし，ＣＳを設置した重要機能室の入退室の管理も十分でないなかで，その運用上の問題が指摘されている。柏原市においては，重要機能室の入退室管理簿は企画情報政策室が管理しているが，企画情報政策室の職員の名前がタイプ印刷され，一日のうち何度か出入りしても，一度しか記入する余地はなく，職員の入退室はあたかも出勤簿のような体裁となっており，業者が入室する場合も本人に記入させるだけで偽名で入室されれば誰が入退室したか分からない状況である。

b　アクセスログ（履歴）の確認については，セキュリティ基準によれば，端末機の操作者について正当なアクセス権限を有していることを操作者識別カード及びパスワードにより確認する（同第４－４－(2)）とともに，住基ネットを操作した履歴を磁気ディスクに記録し，法令を遵守していることを監視する等，その利用の正当性について確認すること（同第４－４－(6)）とされており，このためにはアクセスログの確認が必要であるが，木津町では，技術上の問題もあり，業者任せにして，アクセスログをほとんどチェックしていないし，柏原市においては，ログオン失敗歴も定期的にチェックしているとされるが，本来管理責任者である住民課長が自らしているのではなく，住民課の誰かがしているというにすぎない状態であり，被控訴人八尾市においても，責任者たる市民課長は自らアクセスログをチェックできず，操作主任に一任している。このように，各自治体におけるアクセスログの

確認は，セキュリティ基準を満たしているとはいえないものである。

c　ＣＳの保守・点検は，一般に地方自治体の職員はコンピュータ技術について専門的な知識を有せず，せいぜい運用上の知識やセキュリティに関する研修を受けている程度であるため，民間の業者に委託するほかはないところ，セキュリティ基準によれば，住基ネットの開発，変更，運用，保守等について，委託を行う場合は，委託先事業者等の社会的信用と能力を確認し（同第４－１０－(1)），委託事業の一部を第三者に委託する場合は，その制限，事前承認及び承認に関する事項を委託先事業者と取り交わすこととされ（同第４－１０－(3)），複数の委託業者が関わる場合は，分担して行う範囲及び責任の範囲を明確にするとともに，作業上必要な情報交換を行えるような措置を講ずることとされている（同第４－１０－(4)）。多くの地方自治体では，民間委託業者は住基ネットの運用，保守等について，第三者の事業者に再委託しているが，被控訴人吹田市においては，事前の再委託承認を得ることなく自治体が知らない間に再委託がなされており，このため受託業者は謝罪文を作成しているし，加茂町においては，実情は，業者に任せた上，作業報告書に基づいて報告を受けている程度であり，作業報告書に書かれている以上の詳細な確認はなされておらず，木津町においては，再委託のセキュリティの状況についても，業者が作成する作業報告書の内容以上のことは確認されていない。

(オ)　兵庫県内の市町におけるＣＳの管理体制，安全性を点検するため，「本人確認情報提供に当たってのセキュリティ体制チェックリスト」（以下「兵庫県チェックリスト」という。）を各市町に配布し，その回答を得たが，その回答をみると，市町の管理体制には重大な欠陥があることが明らかになった。

すなわち，被控訴人らは，総務省が行った「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通信網に関する調査票」（以下「総務省チェックリスト」という。）を活用して各市町村における管理体制の徹底を図っており，特に重要な重点７項目については，すべての市町村において３点満点を達成したから，管理体制は万全であると主張するが，兵庫県チェックリストには，重点７項目と重複する項目があり，その項目につき，姫路市，加古川市，猪名川町，芦屋市，伊丹市及び宝塚市がクリアしていないとの回答をしている。したがって，市町には，セキュリティ基準を満たしていないところがあり，伊丹市についてみると，①重要機能室の鍵又は入退室のカードの管理責任者を定めていない，②ＣＳが存在するＬＡＮの通信網機器の物理的配線状況を管理していない，③通信網機器の保守内容及び点検項目を明確にしていない，④重要機器に対する保守を行う場合に職員が立ち会っていない，⑤データのバックアップの実施記録簿を保管していない，⑥自己チェックリストによる点検を定期的に行っていない，⑦委託業者の管理も極めて不十分であり，庁内ＬＡＮの管理が極めて杜撰である，等の多数の問題があり，信じ難い管理状況にある。このように，市町の管理体制が不十分なことは明らかで，住基ネットの安全性が危機的な状況にある。

(カ)　国立市の住基ネット切断

国立市は，平成１４年１２月２６日に，住基ネットを切断している。国立市は住基ネットで流通する住民の情報の管理に責任を持てないことをその理由として挙げている。そして，国立市長は，その問題点として，住民から届けられた個人情報の管理者として，住基ネットで拡散する個人情報が，どこでどのように取得，管理，消去されるのかを，具体的に把握できず，かつ，その安全性を確認できない，住基ネットに参加するということは，情報漏えいの危険性が付きまとうが，その危険性を上回るようなメリットがあるのだろうか等と指摘し，住基ネットの切断によ

って，住民に対するサービスの面でも，国立市の住民関係の行政事務の面でも，国の機関や他の自治体との関係，それらの機関の事務の面においても，いずれも特段の支障は生じないとしている。

(ｷ) 以上のところからすれば，住基ネットは本人確認情報の漏えいや不正利用される具体的な危険がある。

エ　住基ネットの必要性・有用性の不存在

住基ネットを推進してきた総務省は，住基ネットの存在意義として，①国の行政機関等に何らかの申請，届出をするときに住民票の写しの添付が不要となること，②住基カードを所持する者は，全国どこの市町村からでも住民票の写しの交付を受けられること，③住基カードを持っている人については，市町村を越えた転居の際に，転出市町村役場へ行く必要がなく，転入市町村役場へ１回行けばすむことを指摘し，宣伝してきた。

しかしながら，①については，一般市民が国の行政機関等へ申請，届出をする場合はほとんどない。一般市民が住民票の写しを必要とする場合は，パスポートの取得や運転免許証の取得の場面である。しかしこれらの場合，通常は同時に戸籍謄抄本も必要とされ，いずれにしても一般市民は市町村役場へ行かなければならない。②については，一般市民にとって，住民票の写しを必要とする場合自体ほとんどない。また，住基カードを所持する場合でも，住民票の写しの交付を受けるためには，どこかの市町村役場へは行かなければならない。さらに，昨今では，ほとんどの自治体で，夜間サービスや，土曜日，日曜日の行政サービスを実施している。③については，一般市民が市町村を越えて転居することが頻繁にあるとは通常考えられない。また，一生で数回あるかないかの転居の際，転出先，転入先の各市町村役場に出向くことを不便と感じている住民は少ない。さらに，現在でも転出届は，郵送で可能であり，転出元の市町村役場に出向く必要はない。転出地での住民票の情報を記載した転出証明書が必要な場合も，郵送

によって取得することが可能である。したがって，総務省の強調する，住民にとっての利益はほとんどない。

さらに，総務省の作成した住基ネットに関する条例規定例によれば，各市町村において，各個人の健康診断結果，血液型，公共施設予約サービス等に利用することが想定されている。そうなると，氏名，住所，生年月日，性別そして住民票カードという情報だけが住基ネットを流れるのではなく，各個人が知らない間に，それぞれの個人の様々な情報が，市町村から都道府県，そして情報センター，国へと住基ネット上を流されることになる。しかも，住基ネットは，そうした情報が流されることをその当該個人が確認することができないシステムである。

以上のとおり，住基ネットには，国民にとって必要性や有用性が認められない。

オ　以上のところからすれば，住基ネットは，控訴人らの権利を違法に侵害しているというべきである。

【被控訴人らの主張】

ア　控訴人ら主張の権利と住基ネットの非侵害性について

(ア) プライバシー権について

a　プライバシーは，憲法１３条に規定された幸福追求権によって基礎づけられる法的保護に値する人格的利益である。しかし，プライバシーの概念は多義的であるとともに，プライバシーは，一般人を基準として通常他人に知られたくないか否かによって保護範囲が左右されるものであるから，同じ情報であっても，利用される場面あるいは公表される相手方によってその侵害となるか否かが左右される外延の極めて不明確なものであり，権利としての明確性がない。プライバシーの権利は，その概念の不明確さゆえに，それ自体は一個の統一的な憲法上の権利とまでは認められないというべきである。

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に，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を含むものとは認められない。また，公権力から監視されない権利を含むものでもない。控訴人らが主張する自己情報コントロール権は，実定法上の根拠があるとはいえない。行政機関の保有する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。）１２条，２７条，３６条において，保有個人情報につき，本人からの開示請求権，訂正請求権及び利用停止請求権が明文で認められたが，これらの規定は自己情報コントロール権を認めたものではない。

また，プライバシー権が，自己情報コントロール権であり，公権力から包括的に管理されない権利であるとしても，その権利の内容や権利の外延については不明確であって，実定法上の権利としての適格性や成熟性を欠いており，到底憲法上の権利と認めることはできない。したがって，プライバシーについては，人格権としての名誉権等とは異なり，権利性を認めることはできず，排他性を有する人格権であるととらえて名誉権等と同一の差止め請求ができる権利であるとは認められない。

b　仮に控訴人らが主張するようなプライバシーの権利が認められるとしても，住基ネットはそれを侵害するものではない。

住基法においては，その目的（同法１条）にも示されているとおり，社会生活の基礎となる個人情報（同法７条各号記載の情報）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，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，この点は平成１１年

の住民基本台帳法の改正前と後で何ら変わりないのである。

そして，住民票コードは，住基ネットを構築するに当たり，行政において確実な本人確認をし，迅速かつ効率的な検索を実現するために住民票に記載することとされたものであり，控訴人らが主張するような行政機関が個人情報を一元的に管理するために記載したものではなく，目的以外の使用を禁止され，住民票コードを利用して個人情報を名寄せすることは認められていないのである。

したがって，住基ネットは，控訴人ら主張のプライバシー権（自己情報コントロール権等）を侵害するものではない。

(イ) 公権力から監視，包括的に管理されない自由権，平穏生活権について

憲法１３条により「プライバシー権」が一個の統一的な憲法上の権利として保障されているとはいい難い上，控訴人らが主張する「公権力から監視されない権利」も，その権利の内容，根拠，外延などのいずれをとっても明確ではなく，およそ憲法１３条により保障されているとはいい難い。また，住基ネットがいわゆる国民の総背番号制としてイメージされているものを企図した制度ではない。控訴人らの主張は理由がない。

(ウ) 人格権について

住民票コードは，住基ネットにおいて本人確認を確実かつ効率的に行うために使用される１０桁の数字及び１桁の検査数字にすぎず，住民基本台帳に記録されている者は，理由のいかんを問わず，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）のであるから，住民票コードは，個人の人格的価値とは無関係である。住民票コードの記載により，控訴人らの人格権及び何らかの人格的利益が侵害されるとはいえない。また，住民票コードを用いてデータの名寄せをすることは禁じられており，この場合には懲戒処分を受けたり，刑事罰を科せられることになるのであって，これらの違法行為がなされることを

前提として，その具体的危険性があるとすることはできない。

イ　住基ネットの安全性（セキュリティ対策の構築）

住基ネットにおいては，情報漏えいを防止するための各種の措置がとられ，セキュリティ対策が具体的に講じられている。

(ア)　制度面からの対策

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

b　本人確認情報の提供を受ける行政機関の範囲や利用目的は限定されているし（同法３０条の６，３０条の７第３項ないし第６項，３０条の８），本人確認情報の提供を受ける者に対し，目的外の利用又は提供は禁止されており（同法３０条の３４），知事及び指定情報処理機関は，法律の規定によらない本人確認情報の利用及び提供を禁止されている（同法３０条の３０）。

c　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（都道府県の住民の本人確認情報の保存）と都道府県通信網の管理責任を負い，指定情報処理機関は全国サーバ（全住民の本人確認情報の保存）と全国通信網の管理責任を負い，それぞれ安全性を確保する責任を負っている。また，総務省は，指定情報処理機関への監督命令等（同法３０条の２２第１項），地方公共団体への指導，助言，勧告等（同法３１条），本人確認情報管理規程の認可（同法３０条の１８），セキュリティ基準の策定等の権限を有し，委任知事は，指定情報処理機関に対する指示（同法３０条の２２第２項），指定情報処理機関は，委任知事に対する技術的助言等（同法３０条の１１第７項）の権限を有し，これらの権限により，安全性の確保を担保している。

そして，指定情報処理機関が，国の機関等に本人確認情報の提供

を行う際には，協定書を取り交わすこととして国の機関等の責任を明確にし，委任知事は，指定情報処理機関に対し，報告要求等を行うことができ，都道府県及び指定情報処理機関には，本人確認情報保護のための諮問機関が設置されるなど，個人情報の保護を図る制度が確保されている（同法３０条の２３第２項，３０条の９及び３０条の１５）。

d　住民票コードは，無作為の番号で，住民の申請によりいつでも変更できるとし（同法３０条の３），さらに，民間部門が住民票コードを利用することを禁止し，行政機関が利用する場合も目的外利用を禁止するなどし，住民票コードの利用を厳しく制限する措置を講じている（同法３０条の３４，４２ないし４４）。

e　都道府県，市町村及び指定情報処理機関は緊急時対応計画を定め，本人確認情報の漏えい等の危険が具体的に発生した場合には，相互に連絡調整を行い，被害拡大を防止するための措置等を講ずることとされている（セキュリティ基準第２－５）。

(イ)　内部的な具体的不正防止対策

a　担当者が多数の個人情報を容易に検索できないよう，本人確認情報の照会条件を限定している。

b　住基ネットにアクセス権限のない職員がアクセスできないよう，操作者識別カード認証による制御を行うことになっている。

c　アクセスログを定期的にチェックし，不正アクセス等を発見したときは，適切な措置を講ずることになっている。

d　住民から請求があった場合，本人確認情報提供状況を開示することとなっており，住民が本人確認情報の提供状況を把握することが可能となっている。

e　一定時間に一定数以上の住民票の写しの広域交付を停止する措置

を講じるほか，担当職員に対し，住基ネットの安全性の確保等を目的とした教育・研修が実施されている。

(ウ) 物理的な侵入防止対策

セキュリティ基準においては，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，磁気ディスクの管理，構成機器及び関連設備の管理，データ・プログラム・ドキュメントの管理等，外部からの侵入に対する物理的なセキュリティ対策を関係機関に義務付けている。

特に，市町村における住基ネット及びこれに接続している既設通信網における対策については，総務省チェックリストに基づく自己点検と，これに基づく都道府県，指定情報処理機関及び総務省による指導，助言を実施し，対策の強化，徹底を図っている。

なお，セキュリティ基準及び総務省チェックリストは，高いレベルの安全性を実現することを目的としており，これを遵守しなければ，本人確認情報の漏えい，改ざん等の具体的危険が生じないという基準を設定したものではない。仮にセキュリティ基準の一部が達成されていなくても，また総務省チェックリストで最高点に満たない項目があったとしても，そのことから直ちに，本人確認情報の漏えい，改ざんの具体的危険があるとはいえない。

(エ) 電気通信回線上の侵入防止対策

a ＣＳ，都道府県サーバ及び全国サーバの間の通信網は，すべて専用回線及び専用交換装置で構成された閉鎖的な通信網である。

b サーバ間で相互認証・暗号通信を実施しており，仮に，他のコンピュータを住基ネットに接続できたとしても，通信を行うことはできないし，盗聴による恒常的な暗号鍵の解読が極めて困難となる対策がとられている。

c　住基ネットの通信プロトコルには，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せず，住基ネットに独自のものが用いられており，すべてのＣＳの通信網側，すべての都道府県サーバの通信網側と端末機側，全国サーバの全方向及び国の機関等サーバの通信網側に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おり，ＣＳ，都道府県サーバ，全国サーバ及び国の機関等サーバに対し，住基ネットのアプリケーション以外の通信を使用してアクセスすることはできないようにされている。

d　指定情報処理機関において，コンピュータウイルス，セキュリティホールの発生情報を入手し，ウイルス対策ソフトの新パターンファイルの配布や対応方法の通知を全団体に対して行い，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が実施されている。

e　指定情報処理機関は，監視ＦＷ等により，不正な通信がないか，２４時間常時監視を行っている。

f　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，住基ネット全体で均質かつ高度な安全性の確保が実現されている。

g　被控訴人ら以外の，ある特定の市町村におけるセキュリティ対策につき仮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わけではない。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，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，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，これは

極めて困難な対策がとられていることは上記のとおりである。

(オ) 外部監査等によるセキュリティの確保

指定情報処理機関と総務省は，市町村に対し，総務省チェックリストを活用して，指導，助言するなどしてセキュリティ対策の維持，向上を図り，外部監査法人による市町村のシステム運営監査を実施して管理体制の強化に活用した。また，住基ネットの主要な機器に対する模擬攻撃を実施して安全性の確認を行った。

(カ) 住基カードの安全性の確保

住基カードについても，住民の申請により交付する（住基法３０条の４４第３項），市町村の独自サービスの範囲は，市町村が条例で定める目的に限定する（同法３０条の４４第８項）など，様々な対策を講じることにより，安全性を確保している。

(キ) 長野県が行った住基ネットの侵入実験について

上記侵入実験は，①市町村設置ＦＷを回避して，重要機能室に物理的に侵入し，施錠を開けるなど通常の対策を幾重にも外した上，直接ＣＳに攻撃端末をつなぎ，ＣＳのＯＳの管理者権限を取得し，そのＣＳから得られたＩＤ，パスワードでＣＳ端末の管理者権限を取得したことや，②庁舎内に入り，市町村の庁内ＬＡＮにつないだ攻撃端末から，庁内ＬＡＮ上にある既存住基システムの機器の脆弱性を検査し，これを攻撃することに成功したというものにすぎない。外部のインターネットから庁内ＬＡＮへ侵入することや，庁内ＬＡＮからＣＳセグメントへ侵入することにはことごとく失敗したのである。

実験結果から明らかになったのは，特殊な環境の下でＣＳのＯＳの管理者権限が取得できるということや，住基ネットに含まれない既存住基システムに対する攻撃がされたことに止まるのであって，住基ネットの危険性を示すものではない。

そして，住基ネットアプリケーションを起動させるには，操作者が識別カードをカードリーダに挿入することなどが必要となるから，ＣＳ，ＣＳ端末のＯＳの管理者権限を取得したとしても，住基ネットアプリケーションを起動させることもできないし，住基ネットにおいては，サーバ間で相互認証するシステムを採っており，他のコンピュータをネットワークに接続できたとしても，通信を行うこともできない。

上記侵入実験の結果は，住基ネットの危険性を実証するものではなく，かえって，その安全性が確認された。すなわち，①実験市町村以外の住民の個人情報に不正にアクセスされたり，インターネットから庁内ＬＡＮへ侵入されることや，庁内ＬＡＮからＦＷ越しにＣＳへ侵入される具体的危険性が実証されず，むしろ安全性が確認され，②ＣＳのＯＳ管理者権限やＣＳ端末のＯＳ管理者権限の取得は，通常の状態ではむしろ安全であることが確認され，③庁内ＬＡＮからＦＷ越しにＣＳのＯＳ管理者権限を取得することが不可能であること，④住基ネット本体に対する監視が適正に実施されていること，⑤既存の住民基本台帳システムの改ざんが直ちにＣＳに反映されるものではないこと及び既存の住民基本台帳システムは住基ネットと峻別してとらえるべきこと，⑥庁舎外から庁内ＬＡＮへ侵入される具体的危険性は実験で実証されておらず，むしろ安全性が確認され，実験市町村における庁内ＬＡＮの脆弱性は限定的であり，一般論としても市町村における対策が徹底されていること，が明らかになったのである。

ウ　住基ネットの目的の合理性・必要性

(ア)　住基ネットは，行政サービスの向上と行政事務の効率化を目的とするシステムである。住基ネットにより，パスポート申請の際の住民票の写しの提出の省略をはじめ，行政機関等への申請，届出の際に，住民票の写しの提出が不要になった事務が多数あり，将来的には，より多数の事

務で，住民票の写しの提出を不要とする計画である。これにより，住民は，住民票の写しの交付に伴う負担を免れ，市町村は，交付事務に伴う人件費などの行政経費を削減できることとなった。また，年金受給者は，毎年現況届又は身上報告書を提出しなければならなかったが，住基ネットにより，上記書面の提出が不要となった。このように，住基ネットにより，住民の申請，届出，住民票の写しの添付等の負担が解消され，行政側としても，事務効率の向上や，事務の正確性が向上している。さらに，住基ネットにより，行政機関への申請，住民の転入，転出事務の簡素化，住民票の写しの交付の広域化も実現されている。このように行政事務の効率化が達成されることにより，税金負担の軽減，福祉施設の充実等といった「住民の利益」にも還元されるものである。行政事務の効率化と住民の利益の便益とは，それぞれ全く別の行政目的ではなく，総合的に評価されるべきものである。

(イ) 住基ネットは，高度に情報化された現代社会において，すでに民間ではコンピュータ・ネットワークシステムが構築されて，顧客サービスの向上や業務の効率化が積極的に進められてきている中にあって，行政も，全国的な広がりをも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等の必要性があり，そのためには，市町村や都道府県の区域を越えた本人確認情報システムが不可欠であり，行政部門においても，民間部門と同様に，情報処理技術を的確に活用することが不可欠であるとの認識から，行政サービスの向上と行政事務の効率化を目的とするものとして，構想され，導入されたものである。

(ウ) そして，住基ネットは，我が国が実現を目指す電子政府・電子自治体の基盤となる最も重要なシステムである。

すなわち，我が国政府は，情報通信技術（ＩＴ）の活用により世界的

規模で急激に生じている社会経済構造の変化に的確に対応することの緊急性にかんがみ，高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に実施する必要があるとの認識の下に，平成１２年７月７日，内閣総理大臣を本部長とするＩＴ戦略本部とＩＴ戦略会議を設置した。ここでは，ＩＴを国家戦略として推進することが検討され，平成１２年１１月２７日，ＩＴ戦略本部とＩＴ戦略会議合同会議は，「ＩＴ基本戦略」の内容を明らかにして，「５年以内に世界最先端のＩＴ国家となる」との目標を掲げた。

国会は，これに対応するものとして，平成１２年１１月，「高度情報通信ネットワーク社会形成基本法」（同年法律第１４４号，以下「ＩＴ基本法」という。）を制定した（平成１３年１月６日施行）。このＩＴ基本法は，基本理念として，①すべての国民が情報通信技術の恵沢を享受できる社会の実現（同法３条），②経済構造改革の推進及び産業国際競争力の強化（同法４条），③ゆとりと豊かさを実感できる国民生活の実現（同法５条），④活力のある地域社会の実現及び住民福祉の向上（同法６条），⑤国及び地方公共団体と民間との役割分担（同法７条），⑥利用の機会等の格差の是正（同法８条），⑦社会経済構造の変化に伴う新たな課題への対応（同法９条）を定めた。

そして，国及び地方公共団体は，このような基本理念にのっとり，①高度情報通信ネットワーク社会の形成に関し，相互の適切な役割分担を踏まえ，その地方公共団体の区域の特性を生かした自主的な施策を策定し，及び実施する責務を有するとされ（同法１０条，１１条），②高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては，国民の利便性の向上を図るとともに，行政運営の簡素化，効率化及び透明性の向上に資するため，国及び地方公共団体の事務におけるインターネットその他の高度情報通信ネットワークの利用の拡大等行政の情報化を

積極的に推進するために必要な措置が講じられなければならないとされた（同法２０条）。

さらに，平成１３年１月２２日，「ＩＴ基本戦略」を衣替えした「ｅ－Ｊａｐａｎ戦略」が決定発表され，その後の同年３月２９日，ＩＴ基本法３５条に基づいて策定された「ｅ－Ｊａｐａｎ重点計画」が発表され，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」となる社会の実現が目標とされた。そして，平成１５年７月２日，第２期の国家戦略として，「ｅ－Ｊａｐａｎ戦略Ⅱ」が決定され，これを受けて，同年８月８日，「ｅ－Ｊａｐａｎ重点計画－２００３」が策定された。

そして，住基ネットは，ネットワーク社会における本人確認手段として，上記のような電子政府・電子自治体の基盤となる最も重要なシステムとして位置づけられているのである。

エ　住民票コードと住民のプライバシー等について

(ｱ) 住民票コードは，住基ネットを構築するに当たり，行政において確実な本人確認をし，迅速かつ効率的な検索を実現するために住民票に記載することとされたものであり，控訴人らが主張するような行政機関が個人情報を一元的に管理するために記載したものではない。

そして，前記のとおり，住基ネットにおいては，住民票コードについての目的以外の使用を禁止しており（住基法３０条の３４，同条の４２，同条の４３，個人情報保護法８条３項），住民票コードを利用して，個人情報を名寄せすることは認められておらず，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す行為は，公務員の守秘義務違反となり，その職権を濫用して，専らその職務の用以外の用に供する目的で行ったものとして，個人情報保護法５５条の規定に該当し，刑事罰

により処罰されることになる。民間においても，住民票コードの告知を要求することは禁じられており，業としてデータベースを作ることも禁じられている。知事は中止の勧告及び命令をすることができ（住基法３０条の４３第３項），命令に違反した者には懲役刑又は罰金刑が科せられるのである（同法４４条）。

(イ) 住民票コードは，個人の人格的価値とは無関係であり，住民票コードの記載により，控訴人らの人格権及び何らかの人格的利益が侵害されるものでないことは，前記被控訴人らの主張のとおりである。

(ウ) 住民票コードは，住民基本台帳に記録された本人確認情報を市町村の区域を越えて確実かつ効率的に利用するために必要不可欠なものである。すなわち，住基ネットは，住民基本台帳に記録された市町村の区域を越えて全国共通に効率よく利用できるようにするための情報システムとして構築されたものであるところ，このシステムを構築するためには，電気通信回線に接続された電子計算機を利用して，市町村の区域を越えた住民基本台帳に関する事務の処理，国の機関等への本人確認情報の提供等を行うための体制を整備する必要がある。かかる観点からすると，市町村の区域を越えた住民基本台帳に関する事務の処理を行うためには，市町村長が保有する住民基本台帳に記載された個人に係る情報にアクセスすることが可能であることが必要であり，電子計算機の処理によるアクセスの確実な方法として住民票コードが最適なのである。

オ 以上のとおり，控訴人らにその主張のような権利が憲法上保障されているとはいえないし，仮に控訴人ら主張の権利が認められたとしても，住基ネットは，セキュリティその他の組織的な個人情報保護制度からいっても，本人確認情報の漏えいや不正利用の具体的危険性はなく，他方で合理的な行政目的を達成するために必要性のあるものであるから，控訴人らの権利を侵害するものではない。

(2) 控訴人らの被控訴人らに対する慰謝料請求権の有無

【控訴人らの主張】

ア 被控訴人らは，住基法に基づき，各被控訴人の電子計算機と電気通信回線を接続し，控訴人らの本人確認情報を大阪府に提供している。これは，被控訴人らの各市長が，公権力の行使として，職務を行うにつきなした行為である。被控訴人らの各市長は，住基ネットに接続すれば，控訴人らの本人確認情報が，住民登録をした地方自治体から外部に漏出し，これにより控訴人らの上記の権利が侵害されることは容易に認識予見できたものであるから，被控訴人らの各市長には，故意又は過失がある。

イ 控訴人らは，被控訴人らの地方公共団体に住む一般市民である。控訴人らは，前記控訴人ら主張のとおり権利を侵害され，各５万円を下らない精神的損害を受けた。

ウ よって，控訴人らは，それぞれ住所を有する自治体の被控訴人らに対し，国家賠償法１条に基づき慰謝料各５万円及びこれに対する違法行為（住基法施行）の日である平成１４年８月５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の支払を求める。

【被控訴人らの主張】

ア 住民票コードを住民票に記載したり，本人確認情報を住基ネット上に保有したり，法定事務について本人確認情報を行政機関等に提供したりするだけで控訴人らの権利を侵害するものといえないことは，前記被控訴人らの主張のとおりである。

イ 国家賠償法上の違法性が認められるためには，被控訴人ら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（最高裁判所昭和６０年１１月２１日第一小法廷判決・民集３９巻７号１５１２頁）。そして，被控訴人らの各市長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（最高裁判所平成５年３月１１日第一小法廷判決・民集４７巻４号２８６３頁）。

被控訴人らの各市長が住基法に基づいて実施することは，その職務上の法的義務に違反するものではなく，被控訴人ら各市長に上記の注意義務違反行為がないことは明らかであり，その行為は，国家賠償法１条１項の違法性を有するものではない。したがって，控訴人らの慰謝料請求は理由がない。

(3) 控訴人[redacted]ら４名の差止め請求権の有無と差止め請求の可否

【控訴人らの主張（当審追加）】

ア　住民の住基ネット離脱請求権

(ア) 住基ネットにより，住民のプライバシー情報が漏出し，これにより控訴人らのプライバシーの権利が侵害され，あるいはその侵害の具体的かつ急迫の危険がある場合には，これを回避するため，差止め請求権の一内容として住基ネット離脱請求権（妨害排除としての住民票コードの削除，妨害予防としての住基ネット使用による本人確認情報の大阪府知事への通知の差止め）が認められる。

(イ) 上記住基ネット離脱請求権は，次のところからも実定法上の根拠を有するものである。

個人情報保護法３６条は，「何人も，自己を本人とする保有個人情報が次の各号のいずれかに該当すると思料するときは，この法律の定めるところにより，当該保有個人情報を保有する行政機関の長に対し，当該各号に定める措置を請求することができる。」として，当該保有個人情報の利用の停止，消去，又は提供の停止が請求できることを規定している。これは，行政機関が保有する個人情報の処理について，情報主体たる個人情報の自己の削除を求める権利及び自己情報の利用提供を拒否する権利を認めるものであり，一定の条件下における本人の個人識別情報

の差止め請求の一態様として，利用の停止，消去又は提供の停止請求権を認めようとするものである。これを住基ネットに即していえば，行政機関が保有する個人識別情報である４情報について，これを住基ネットで運用されることによる第三者への個人識別情報の流出・漏えいを防止し，もって人格権としてのプライバシー権を保護することが必要である。このためには，住基ネットからの離脱を認めるほかはない。このための具体的な離脱の方法は住民票コードの削除を求めることであり，このことが同法の規定する利用の停止請求権を構成する。したがって，住基ネットからの離脱請求権は実定法上の根拠を有するものといってよい。

(ウ) ＯＥＣＤ８原則自己情報コントロール権

ＯＥＣＤ８原則とは，１９８０年９月３０日ＯＥＣＤ（経済協力開発機構）理事会勧告により定められたものであり，日本もその加盟国となっているものであり，①収集制限の原則，②データ内容の原則，③目的明確化の原則，④利用制限の原則，⑤安全保護の原則，⑥公開の原則，⑦個人参加の原則，⑧責任の原則と呼ばれるものである。このうち個人参加の原則は，個人の権利として，㋐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求める権利，㋑自己に関するデータを合理的な期間内に，もし必要なら過度にならない費用による合理的な方法で自己にわかりやすい形で自己に知らしめることを求める権利，㋒上記請求が拒否された場合にはそのような拒否に対して異議を申し立てる権利，㋓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内容とするものである。このような個人参加の原則は，ＯＥＣＤ勧告においては，データ保護の核心部分として理解されており，個人の自己情報コントロール権を裏付けるものである。そのための法的整備こそがプライバシー保護法となるものであり，ＯＥＣＤ加盟国たる我が国に課

せられた義務といってよい。ところが，住民基本台帳法はこの点において極めて不十分である。このためＯＥＣＤ８原則の趣旨に照らせば，現行法上，保護が不十分な自己情報コントロール権について，これを補完するものとして住基ネットからの離脱請求権が認められるべきである。

(エ) 人格権に基づく差止め請求権に関する判例

最高裁判所昭和６１年６月１１日大法廷判決（民集４０巻４号８７２頁）は，名誉を違法に侵害された者は，損害賠償又は名誉回復のための処分を求めることができるほか，人格権としての名誉権に基づき，加害者に対し，現に行われている侵害行為を排除し，又は将来生ずべき侵害を予防するため，侵害行為の差止めを求めることができると判示している。本件において控訴人らが主張するプライバシー権は，まさに同判決のいう人格権としての名誉権と同質性を有する重大な保護法益である。同最高裁判決の趣旨からすれば，プライバシー権も排他性を有する人格的権利であり，権利侵害行為に対して妨害排除請求権の行使として侵害行為の差止め請求が認められるべきは当然である。

(オ) 離脱請求権行使の合理性

a　離脱請求権は，住基ネットの運用自体の差止めを求めるものではなく，それを請求する特定の個人についてのみ住民票コード番号を削除することにより，容易に住基ネットからの離脱を可能とするものである。このため離脱請求を認容することによる住基ネット制度全体への影響も少なく，プライバシーの侵害行為に対し，侵害を回避するための最小限度の措置により救済が可能となる。したがって，具体的な権利救済方法としても合理的かつ妥当なものである。

b　住民票コード番号を付することにより控訴人らのプライバシー情報を住基ネット上におくことは，第三者からのアクセスを容易にし，プライバシー情報に対する侵害の危険性は，個別の登録住所地において，

住民票の不正交付により受ける個々の権利の侵害とは比較にならないほど甚大である。

c　仮に住基ネットからの離脱を認めても，住基ネットそのものの運用を困難にするものではなく，当該個人情報自体は登録住所地の市町村に登録されたままであるから，住民基本台帳制度の趣旨を没却することもなく，公共性を阻害することはない。また，控訴人らのような特定個人の住民票コード番号を削除しても何ら制度の障害とはならず，被控訴人らが被る損害はまったくないといってよい。これに対し，離脱が認められないことによる控訴人らのプライバシー権の侵害による不利益の重大性及び危険性は計り知れないものである。受忍限度論によってこのような重大な人格権侵害が許容されるべきでないことは明らかである。

d　離脱を実行するための手続費用

控訴人らが住基ネットから離脱するに必要な措置は，単に住民票コード番号を削除するだけであるから，被控訴人らとしても極めて容易になし得ることである。このため，被控訴人らにおいて格別の費用等損害が新たに発生することもない。しかも，実際に住基ネットから離脱した国立市，矢祭町，杉並区，横浜市等の自治体においても，何ら行政上の不都合や障害は発生していない。

(カ)　以上のとおりであり，控訴人らの同意もないまま，一方的に控訴人らについて住民票コード番号が付されて住基ネット上に控訴人らの個人情報が流出されており，第三者に漏出される危険性は極めて高いものである。したがって，このような危険を回避するため，速やかに控訴人らの住民票コード番号の削除請求及び控訴人らの本人確認情報の大阪府知事への通知に対する差止め請求が認められるべきである。

(キ)　訴えの追加的変更について

a　控訴人[redacted]ら４名は，原審において，同控訴人らがそれぞれ住所を有する被控訴人らに対して，住基ネットを使用しての本人確認情報の大阪府送受信の差止等を求める追加的訴えの変更を申立てたが，原審裁判所は，従前の控訴人らの慰謝料請求と請求の基礎に同一性がないとして訴えの変更を認めなかった。しかし，控訴人らが，慰謝料の支払を求めたのは，控訴人らのプライバシー等の権利を侵害したことによる精神的損害の賠償を求めたものであり，これにプライバシー等の人格権に基づく妨害排除・予防として本人確認情報の差止め請求を追加したに過ぎないものであるから，被侵害利益も同じであり，訴訟資料，証拠資料を審理において共通に利用でき，かつ，両請求の主張が社会生活上同一事象，同一紛争，同一権利侵害を基礎としているのものであり，請求の基礎に同一性がある。原審裁判所が，控訴人[redacted]ら４名の訴え変更の申立てを却下したのは失当である。

b　被控訴人らは，差止め請求は民事訴訟の形式を取りながら実質的には公権力の行使，不行使に関する訴訟であるとして，両請求の内容が大きく異なり，当審において追加的請求を審理するに当たっては，被控訴人らの同意を必要とすべきであると主張する。しかし，控訴人[redacted]ら４名が求める差止め請求は，行政事件としての処分の取り消しを求めているのではなく，プライバシー等の人格権に基づく妨害排除請求権に基づく差止めを民事訴訟手続によって求めているのであり，被控訴人らの審級の利益を害するものではない。

c　仮に，当審において控訴人[redacted]ら４名の差止め請求について審理することが実質的に被控訴人らの審級の利益を害するものであるならば，上記差止め請求については，原審に差戻されるべきである。

【被控訴人らの主張】

ア　訴えの追加的変更について

(ア) 控訴人[redacted]ら４名は住基法により大阪府知事に対して本人確認情報の送信を公法上義務付けられている各市長に対して，控訴人らの一部に係る本人確認情報を送信しないように義務付けるものであるから実質的には公権力の行使，不行使に関する訴訟ともいうべきである。そうすると，従前の控訴人らの慰謝料請求と追加的請求の被侵害利益は共通であるとしても，その実質的な内容は異なるものといわざるを得ず，請求の基礎の同一性を欠くというべきである。

(イ) 仮に，請求の基礎の同一性を欠くものでないとしても，実質的には義務付け訴訟であり，無名抗告訴訟ともいうべきであるから，当審において追加的変更を認めて審理するに当たっては，被控訴人箕面市，同吹田市及び同守口市の審級の利益を害さないように，同意が必要であると解すべきである。そして，上記被控訴人らは，上記同意を予定していないから，訴えの変更は許されないというべきである。

イ 差止め請求について

(ア) 差止め請求が認められるためには，①差止めができる排他的権利があること，②違法な権利侵害の危険性があること及び③差止めの必要性があることが必要である。

(イ) 差止めができる排他的権利の不存在

a 控訴人[redacted]ら４名は，差止め請求の根拠として，憲法１３条で保障されたプライバシーの権利（自己情報コントロール権）を主張しているが，その自己情報コントロール権は憲法１３条で保障された権利といえないことは，被控訴人ら主張のとおりである。

b また，控訴人[redacted]ら４名は，プライバシーの権利を人格権として基礎づけ，プライバシーの権利の一態様である公権力から監視されない権利や自己情報コントロール権を根拠に差止めを求めているとみる余地もあるが，プライバシーについては，その概念自体が不明確であり，

統一的な理解を得られないことから，現段階ではプライバシーを保護する利益を排他性を有する絶対権ないし支配権としての人格権に属するものととらえ，これを根拠に差止めが認容される状況にない（名誉権が，歴史が古く，内容も一義的であって，権利としての成熟性が高いことから，人格権として排他性を認めることに異論がないのと異なる。）。プライバシーの侵害のみを理由として，差止め請求を認めることはできないというべきである。

(ウ) プライバシーの権利等の侵害やその危険性の不存在

住基ネットのセキュリティは十分なものであり，住基ネットに人格権を侵害する危険性がないことは，前記被控訴人らの主張のとおりである。

(エ) 住民の一部の差止めを許容することの不合理性

住基ネットは，本人確認情報を，国の機関等，都道府県，市町村で共有することにより，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する全国民，全員参加の制度である。そして，一部でも不参加があると，本人確認情報の共有がなされなくなるから，国の機関等などにおいて，従来のシステムや事務処理を存置せざるを得ないこととなり，住基法の予定する効果を達成することは不可能になる。

また，住基ネットは，市町村間をネットワーク化し，住民基本台帳事務の広域化，効率化を図ることを一つの重要な行政目的としているところ，不参加を認めることにより，ネットワークが寸断され，他の市町村の効率化が阻害されることは明らかである。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，情報通信技術を利用して，住民サービスの向上と行政事務の効率化を図ることを目的とした住基法の意義を没却し，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。

(オ) したがって，住民の一部の者の住基ネットの使用を差止めることは，住基法は予定しておらず，許されないことというべきであるから，控訴

人らの差止め請求は理由がない。

第３　争点に対する判断

１　争点(1)（住基ネットによる控訴人らの権利の侵害の有無）について

(1)　プライバシーの権利について

ア　個人の人格の尊厳は近代民主主義思想の根底をなすものであり，憲法１３条は，そのような個人の尊重，その生命・自由及び幸福追求という個人の人格的生存に不可欠の権利を宣明し，公共の福祉の実現を任務とする国家も，これらの権利に最大の尊重を払うべきことを要求している。他人からみだりに自己の私的な事柄についての情報を取得されたり，他人に自己の私的な事柄をみだりに第三者に公表されたり利用されたりしない私生活上の自由としてのプライバシーの権利は，人の人格的自律ないし私生活上の平穏の維持に極めて重要なものというべきであるから，いわゆる人格権の一内容として，憲法１３条によって保障されているものと解するのが相当である。

イ　自己の私的事柄に関する情報（個人情報）が，自己の知らないうちに，他者によって勝手に収集，利用されるということが行われれば，民主主義社会における自己責任による行動の自由（人格的自律）や私生活上の平穏が脅かされることになる。他方，社会の変化に伴い個人情報の取り扱われ方は変化していく。とりわけ，情報通信技術が急速に進歩し，情報化社会が進展している今日においては，コンピュータによる膨大な量の情報の収集，保存，加工，伝達が可能となり，また，インターネット等によって多数のコンピュータのネットワーク化が可能となり，人は自己の個人情報が他者によってどのように収集，利用等されるかについて予見，認識することが極めて困難となっている。このような社会においては，プライバシーの権利の保障，それによる人格的自律と私生活上の平穏の確保を実効的なものにするためには，自己のプライバシーに属する情報の取扱い方を自分

自身で決定するということが極めて重要になってきており，その必要性は社会において広く認識されてきているといえる。今日の社会にあって，自己のプライバシー情報の取扱いについて自己決定する利益（自己情報コントロール権）は，憲法上保障されているプライバシーの権利の重要な一内容となっているものと解するのが相当である。

もっとも，プライバシーに属する情報といっても，その中には，思想，信条，宗教などといった，人の人格的自律ないし評価に直接関わり，一般に秘匿の要請が高度な情報（固有情報）もあれば，そうでないもの（外延情報）もあり，特に後者に属する情報の内容や秘匿性の程度については明らでないところがあるが，それは今後の具体的な事例の積み重ねによって自ずと明らかになっていくものであり，現在それが明確になっていないからといって，自己情報コントロール権自体を認めるべきではないとは解されない。

(2) 本人確認情報のプライバシー権性（自己情報コントロール権の対象性）

ア 住基ネットの対象となる本人確認情報は，「氏名」「生年月日」「男女の別」及び「住所」の４情報に，「住民票コード」及び「変更情報」を加えた６情報である。そして，上記変更情報は，政令により，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が定められており（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。

ところで，本人確認情報のうち４情報は，人が他者との関わりを持つ社

会生活の基礎となる個人識別情報であって，個人の私的情報ではあるが，同時に公共領域に属する個人情報であるといえるものであり，もともと秘匿性の高いものとはいえない。そして，４情報については，住基ネットシステムの導入前から，不正な目的によるものでないことが明らかであるとして市町村長から拒まれない限り，何人も，本人の同意なく，住民基本台帳の一部の写しを閲覧し（住基法１１条），住民票の写し等の交付を請求する（同法１２条）ことができた。また，住民基本台帳制度は，国及び地方公共団体の行政の合理化に資することをも目的としており（同法１条），住民登録事項が国及び地方公共団体の行政に利用されることが予定されているといえる。

しかし，そうだからといって，直ちに本人確認情報が法的に保護されるべき人格的利益に当たらないと結論できるわけではない。人は素性を知らない他人に対して然るべき理由もないのに自己の氏名や住所を明かすことはないといえるし，今日の社会においては，一般的に秘匿性の低い個人情報であっても，人によってはある私的生活場面では秘密にしておきたいと思う（秘匿性の高い）事柄があり，そのような個人情報の取扱い方についての本人の自己決定を承認する社会的意識が形成されていると認めて差し支えないと思われる。例えば，ストーカー被害に遭っている人にとっては氏名，年齢，住所等について，性同一性障害の人にとっては性別について，それぞれ秘匿の必要性は高いといえる。また，変更情報は，本人確認情報について変動が生じた場合に，「住民票の記載の修正を行った旨」の記載に加え，「職権修正等」，「事由が生じた年月日」のみが記載され，これが「変更履歴」となり，婚姻，離婚等の具体的事由が記載されるわけではない（同法３０条の５第１項，同施行令３０条の５，同施行規則１１条）けれども，氏の変更は身分関係（婚姻，離婚，養子縁組，離縁等）に変動があったことを推知させることにもなるから，秘匿の必要性も軽視できない

といえる。住民票コードは，それ自体数字の羅列にすぎない技術的な個人識別情報であるが，住民票コードが記載されたデータベースが作られた場合には，検索，名寄せのマスターキーとして利用できるものであるから，その秘匿の必要性は高度であるといえる。さらに，４情報について何人も本人の同意なく住民基本台帳の一部の写しの閲覧や住民票の写し等の交付を請求することができたことについては，市町村長において閲覧を拒絶できる場合があったから，それが無制限に許されたわけではないし，そもそもその取扱いについてはプライバシー保護の観点から疑問が提起されていたものである（なお，上記住基法１１条の取扱いは，住民基本台帳法の一部を改正する法律〈平成１８年法律第７４号〉が制定され〈平成１８年６月１５日公布，同年政令第２９７号により同年１１月１日施行〉，住民基本台帳の一部の写しの閲覧につき，閲覧することができる場合を法律で定める一定の場合に限定し，閲覧の申出の際に明らかにすべき事項を法律上明示すること〈改正後１１条１項ないし３項〉，個人又は法人に係る申出者等による閲覧事項の目的外利用を禁止することなど閲覧の手続を整備する〈同法１１条の２〉とともに，偽りその他不正手段による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〈同法４６条，４７条，５１条〉する等の改正が行われた。）。また，住民基本台帳制度は，国及び地方公共団体の行政の合理化に資することも目的としているが，そうだからといって，本人確認情報を自由に収集，利用することが許されるものではなく，利用の目的と手続について法の規制に従わなければならないものである。

上記のところからすれば，一般的には秘匿の必要性の高くない４情報や数字の羅列にすぎない住民票コードについても，その取扱い方によっては，情報主体たる個人の合理的期待に反してその私生活上の自由を脅かす危険を生ずることがあるから，本人確認情報は，いずれもプライバシーに係る

情報として，法的保護の対象となり（最高裁判所平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁参照），自己情報コントロール権の対象となるというべきである。

イ　もっとも，プライバシーに係る情報の中にも，思想，信条等の人格的自律に直接関わるような秘匿の必要性の高い情報（固有情報）もあれば，そこまでの秘匿の必要はない情報（外延情報）もあることは上述のとおりであり，それらの保護の必要性が一様のものであるとは考え難い。特に，本人確認情報は，公権力との関係でみれば，他の地方公共団体や行政機関において行政目的実現のために必要な範囲で個人識別情報として収集，保有，利用等する必要のある場合があることはいうまでもないことである（住基法１条もそれを予定している。）。このような個人識別情報としての本人確認情報の性質を考慮すれば，その収集，保有，利用等については，①それを行う正当な行政目的があり，それらが当該行政目的実現のために必要であり，かつ，②その実現手段として合理的なものである場合には，本人確認情報の性質に基づく自己情報コントロール権の内在的制約により（もしくは，公共の福祉による制約により），原則として自己情報コントロール権を侵害するものではないと解するのが相当である。しかし，本人確認情報の漏えいや目的外利用などによる，住民のプライバシーないし私生活上の平穏が侵害される具体的危険がある場合には，上記②の実現手段として合理性がないものとして，自己情報コントロール権を侵害することになり，住基ネットによる当該本人確認情報の利用の差止めをすべき場合も生じるものと解される。

そこで，上記の点につき，以下検討する。

2　住基ネットの行政目的の正当性及び必要性について

(1)　前記前提となる事実，証拠（乙６ないし９）及び弁論の全趣旨によれば，次の事実が認められる。

住基ネットは，本人確認情報を，市町村，都道府県及び国の機関等で共有することにより，住民基本台帳事務の広域化による住民サービスの向上と行政事務の効率化を図ることを重要な行政目的とするものである。そして，例えば，次のような行政効果が期待され，実施に移されてきている。

ア　住民サービスの向上，行政事務の効率化について

(ア) 住民は，転入・転出に伴う負担（転出地の市町村への出頭等の負担）を免れ，また，転出地及び転入地の市町村においては，転出証明書の発行に伴う事務を軽減でき，市町村間の通信を従来の郵送に代えて電気通信回線を通じて行うことになり，事務の効率化が図れる。

住民の転出・転入は，多大な件数（平成１４年度においては約４５０万件）に上っているが，住基カードの交付を受けている者についての転入届出が，従来必要であった転出証明書の添付を要せずに行えるようになり，また，住民は，どの市町村でも住民票の写しを入手できるようになった。

(イ) 国の試算によれば，国の機関等への申請や届出の際に従来必要であった住民票の写しを提出することが不要となる件数は２５００万件以上であると見込まれ（平成１６年度の省略件数は年間３００万件以上であった。），住民は，住民票の写しの交付に伴う負担（手数料負担や交付を受けるための郵送や出頭の負担）を免れ，また，市町村は，交付事務に伴う行政経費を削減できる。

(ウ) 加給年金対象者等を除く年金受給者は，毎年行っていた現況届又は身上報告書の提出に伴う負担（記入や年金支給機関への郵送の負担）を免れ，また，年金支給機関も，年金受給者への現況届用紙等の送付やその受付処理に係る事務を削減でき，さらに，現況届の確認が毎年１回であったのに対し，住基ネットを利用すれば年金支給の都度（毎年４回ないし６回）受給権を確認できることになるから過誤払を防止でき，過誤払

金の削減，回収事務の負担軽減につながることとなった。平成１４，１５年度は共済年金（地方公務員，国家公務員，私立学校教職員），戦没者遺族等援護年金において年間約２００万件が実施された。

(エ) 恩給受給者は，これまでは毎年市町村長の証明印を受けて受給権調査申立書を提出する必要があった（平成１４年度は年間約１４０万件）が，その負担を免れ，また，市町村は，当該事務を削減でき，さらに，従前は受給権の確認が年１回であったのに対し，住基ネットを利用すれば恩給支給の都度（年４回）確認できることから過誤払を防止でき，過誤払金の削減，回収事務の負担軽減につながることとなった。

(オ) 平成１４年１２月６日には，行政手続オンライン化３法が成立し（同月１３日公布），これによって，婚姻届・離婚届（年間約１００万件），パスポートの交付申請（年間約５００万件），戸籍抄本の交付請求（年間約３５００万件），所得税の確定申告（年間約７００万件），国民年金・厚生年金の裁定請求（年間約８０万件）等がインターネットでできるようになると同時に，行政機関が住基ネットを利用して確認するため申請・届出に際して住民票の写しの提出も不要になることになったが，住基ネットはその基礎となるものである。

イ　電子政府・電子自治体について

平成１２年７月７日，内閣総理大臣を本部長とするＩＴ戦略本部とＩＴ戦略会議が設置された。ここでは，情報通信技術（ＩＴ）の活用により世界的規模で急激に生じている社会経済構造の変化に的確に対応することの緊急性にかんがみ，高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に実施する必要があるとの認識の下に，ＩＴを国家戦略として推進することが検討された。同年１１月２７日，ＩＴ戦略本部とＩＴ戦略会議合同会議は，「ＩＴ基本戦略」の内容を明らかにして，「５年以内に世界最先端のＩＴ国家となる」との目標を掲げた。

国会は，これに対応するものとして，平成１２年１１月，ＩＴ基本法を制定した（平成１３年１月６日施行）。このＩＴ基本法は，基本理念として，①すべての国民が情報通信技術の恩沢を享受できる社会の実現（同法３条），②経済構造改革の推進及び産業国際競争力の強化（同法４条），③ゆとりと豊かさを実感できる国民生活の実現（同法５条），④活力のある地域社会の実現及び住民福祉の向上（同法６条），⑤国及び地方公共団体と民間との役割分担（同法７条），⑥利用の機会等の格差の是正（同法８条），⑦社会経済構造の変化に伴う新たな課題への対応（同法９条）を定めた。

そして，国及び地方公共団体は，このような基本理念にのっとり，①高度情報通信ネットワーク社会形成に関し，相互の適切な役割分担を踏まえ，その地方公共団体の区域の特性を生かした自主的な施策を策定し，及び実施する責務を有するとされ（同法１０条，１１条），②高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては，国民の利便性の向上を図るとともに，行政運営の簡素化，効率化及び透明性の向上に資するため，国及び地方公共団体の事務におけるインターネットその他の高度情報通信ネットワークの利用の拡大等行政の情報化を積極的に推進するために必要な措置が講じられなければならないとされた（同法２０条）。

さらに，平成１３年１月２２日，「ＩＴ基本戦略」を衣替えした「ｅ－Ｊａｐａｎ戦略」が決定発表され，その後の同年３月２９日，ＩＴ基本法３５条に基づいて策定された「ｅ－Ｊａｐａｎ重点計画」が発表され，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」となる社会の実現が目標とされた。そして，平成１５年７月２日，第２期の国家戦略として，「ｅ－Ｊａｐａｎ戦略Ⅱ」が決定され，これを受けて，同年８月８日，「ｅ－Ｊａｐａｎ重点

計画－２００３」が策定された。

そして，住基ネットは，ネットワーク社会における本人確認手段として，上記のような電子政府・電子自治体の基盤となる最も重要なシステムとして位置づけられている。

ウ　公的個人認証サービスについて

平成１４年，「電子署名に係る地方公共団体の認証業務に関する法律」（同年法律第１５３号，以下「公的個人認証法」という。）が成立した。同法は，電子署名に係る地方公共団体の認証業務に関する制度その他必要な事項を定めることにより，電磁的方式による申請，届出その他の手続における電子署名の円滑な利用の促進を図り，もって住民の利便性の向上並びに国及び地方公共団体の行政運営の簡素化及び効率化に資することを目的とするものであり（同法１条），住民基本台帳に記録されている者は，その市町村長を経由して当該市町村を包括する都道府県の知事に対し，自己に係る電子証明書の発行を申請することができるが（同法３条），知事（知事から委託を受けている都道府県センター〈財団法人自治衛生通信機構〉）は，住基ネットから，住基法７条１号から３号及び７号の事項について住民票の記載の修正又は消除の通知を市町村から受け，これを電磁的記録媒体に記録し，失効リストを作成するが（公的個人認証法１２条），行政機関は，オンラインでの申請，届出等を受け取る際に，上記失効リストに照会することによって失効していないことの確認をすることができる（同法１８条１項）。また，公的個人認証サービスの電子署名に用いる秘密鍵等の格納媒体として，住基カードが利用されることとされている。

(2) 他方，証拠（甲３７，３８）及び弁論の全趣旨によれば，次の事実も認められる。

ア　住民サービスの向上，行政事務の効率化について

(ア) 転入，転出届の特例による届出（転入届及び付記転出届）の利用状況

についてみると，東京都全体においては，このサービスが開始された平成１５年８月２５日から平成１６年１月３１日までの約５か月間で１２２件であり（東京都における年間移動者数（市区町村の境界を越えて住所を移動した者の数）は毎年およそ１２０万人である。），大阪府においては，平成１６年３月３１日までで８０件，京都府においては，同日までで１４件，愛知県では同年５月２８日までで６３件，長野県においては，同年６月３０日までで２４件であった。全国集計は明らかにされていないが，上記都道府県の利用状況と大差ないであろうとした上で，上記特例手続を利用して転出地の市町村役場へ手続のために出向くことを省略するには，あらかじめ転出市町村へ付記転出届を郵送等で届け出る必要がある上，転出地の市町村からあらかじめ交付を受けた住基カードを転入地の市町村役場て提出しなければならないことから，当該住民に手続の負担軽減感がそれほどないこと，転出の際には，国民健康保険や介護保険に関わる手続や子どもの転校手続など，住民登録の異動に伴う様々な手続が付随するのが一般的であるし，法律上の手続が要求されていない場合でも，実際には転入先での各種の手続等について相談する目的で転出地の市町村役場へ出向くことが多いことなどがあり，それらの事情が上記特例の利用状況の低調さに大きく影響していると見られるとの指摘もされている。

(イ) 住民票の写しの広域交付の利用状況についてみると，京都府においては，このサービスが開始された平成１５年８月２５日から平成１６年３月３１日までの約７か月間の広域交付は１１４１件（ちなみに，国の資料によれば，全国で年間約８５００万件であり，これを人口比で京都府に当てはめると約１７０万件〈１か月平均の７か月分は約９９万件となる。〉である。），東京都においては，平成１６年１月３１日までに約１万１６００件，大阪府においては，同年３月３１日までに８８３４件，

愛知県においては，同年５月２８日までに２８２１件，長野県においては，同年６月３０日までに１８４９件であり，交付請求総件数の１％にも満たない状態であった。

(ウ) 行政手続等への住民票の写しの添付省略等についてみると，上記認定のとおり，国の試算によれば，住基ネットによって住民票の写しの提出が不要になる行政手続は年間約２５００万件と見込まれているが，平成１６年度の省略枚数は年間３００万件程度であるし，年間２５００万件の見込み数を前提としても，国民１人当たりで見ると１年当たり０．２件（５年に１回手続をする程度）にすぎないとの指摘もある。

(エ) 住基カードの交付数については，国は具体的な枚数を明らかにしていない。総務省は，平成１５年８月の制度スタート当初，初年度３００万枚と見込んでいたが，毎日新聞が平成１６年７月に行った独自調査によれば，初年度の交付枚数はわずか２５万枚であり，総務省の見込み数の１０％にも満たなかった。また，福岡県においては，平成１５年８月２５日から平成１６年３月３１日までの住基カードの発行は，県内全市町村計で７３３９枚であり，同年３月末の住民基本台帳人口で割った普及率は０．１５％にすぎなかった。

また，住基カードの多目的利用（市町村条例に基づく独自サービス）について，東海大学政治経済学部の小林隆講師が行った人口１０万人以上の２４８自治体を対象としたアンケート調査（調査期間平成１６年５月２２日から同年６月１２日，有効回答率４８．４％）によると，独自サービスを現に搭載している自治体は２６自治体（２１．７％）であり，今後５年以内に独自サービスを搭載する予定も１８自治体にすぎず，６３％以上の自治体では独自サービスを搭載する予定がないと回答している。

(オ) 住基ネットによる行政経費削減効果について，国は，平成１０年３月

付けの「住民基本台帳ネットワークシステムのベネフィット（試算）」において，転入・転出手続の簡素化によって住民は２７４．２時間（時給換算で３２．１億円に相当）を，行政側は５１．７万時間（同じく１８．７億円）を節約できるとした。この計算では，４７０万件と見積もった転入届のうち半分（２３５万件）がこの制度を利用するものとされている。しかし，東京都（我が国の全人口の約１０％が居住）の平成１６年１月末までの約５か月間の転入届のうち，上記住基ネットによるサービスを利用したのはわずか６４件（年間推定１５４件）であった。また，国の上記試算では，住民票の写しの広域交付件数が交付件数全体の約１２％を占めるとして，住民は７５８．０万時間（時給換算で９８．５億円に相当）を節約できると計算されているが，およそ交付件数１７０万件と推定される京都府では，平成１６年３月末までの約７か月間で１１４１件（年間推計約２０００件）で，全体の０．１２％にすぎない。

(カ) 公的個人認証サービスにおける住基ネットの役割については，都道府県センターは，電子証明書の交付を受けた住民の死亡等の異動情報を情報センターからネットワークを介して得るシステムとなっており，これによれば住基ネットは重要な役割を担っているが，上記異動情報は，もともと市町村において住民からの届出によって作成されるのであるから，あえて住基ネットの全国センターである情報センターを介さなくても，市町村から公的個人認証サービスの都道府県センターに電子証明書の被交付者に関する異動情報のみ直送すれば足り，その方が，簡素に，より低コストでシステムを実現でき，住基ネットは公的個人認証サービスに不可欠のものとはいえないとの意見もある。

イ　市町村の負担について

(ア) 住基ネット構築等の経費について，総務省（自治行政局市町村課）の平成１４年１０月３１日付けの資料によれば，平成１１年から同１５年

度の住基ネット導入経費は，関連経費も含めて，情報センター，都道府県，市町村合わせて約３９１億円であるが，このうち８０％に近い３０７億円が市町村の負担となっており，住民基本台帳に基づく全人口から１人あたりの負担額を求めると約２４０円となる。各市町村ごとの導入経費は明らかでないが，例えば神奈川県横須賀市（人口約４３万人）では，平成１３年度から同１５年度の３か年に約１億６３００万円の予算を住基ネットに支出しており，これを住民１人あたりに換算すると約３８０円となり，上記総務省の資料による推計額と約１４０円の差が生じる。この差は，横須賀市の経費には総務省の資料には計上されていない人件費（約５８００万円）が含まれていることから生じたものである。したがって，全国の市町村が住基ネット導入のために支出した金額は，人件費も含めれば，さらに１．５倍程度に膨らむ可能性がある。

他方，住基ネット稼働後の経費について，総務省の上記資料によれば，毎年要する経常経費として全体で約３９１億円が必要であり，そのうち約８８億円を市町村が負担することが見込まれている（いずれも人件費は含まれていない。）。

(イ) また，全国の市町村は，財政規模の大小を問わずすべて，住基ネットの構築と維持に関する費用の負担と，住基ネットの運用について万全のセキュリティ対策（人員配置や監視態勢）を実現しなければならない責任を負っているが，財政事情の厳しい中でそれらを果たしていくことが相当大きな負担となってきており，これが住基カードの普及率の低調さの原因となっているとの指摘もある。

(3) 上記(2)の事実を考慮すれば，住基ネットの導入による住民サービスの向上や行政事務の効率化（経費削減）がどの程度実現できるかについては不透明なところがあり，特に市町村に求められる効率化以上の負担を課すというところもなきにしもあらずという実態が窺えるが，上記(1)認定の事実を併せて

考えれば，住民サービスの向上及び行政事務の効率化に役立つところがあることも否定できないところであり，住基ネットの行政目的の正当性及び必要性は，これを肯認することができるというべきである。

3　住基ネットによる本人確認情報漏えいの危険性の有無（住基ネットの実現手段としての合理性－その１）

(1)　システムのセキュリティについて

ア　証拠（後掲）及び弁論の全趣旨によれば，次の事実が認められる。

(ア)　住基ネットのハード面におけるセキュリティについては，以下のような措置がとれている（乙１２）。

a　住基ネットの閉域性

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，全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われる。また，指定情報処理機関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が行われる。したがって，これらのサーバ以外との通信を行うことはできない措置がとられている。

b　通信相手の相互認証・暗号通信

(a)　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を行う。また，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ず，したがって，仮に他のサーバをネットワーク接続できたとしても，通信を行うことはできない措置がとられている。

(b)　通信相手の相互認証の過程で，その都度耐タンパー装置で，ＣＲ

ＹＰＴＲＥＣ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，これをさら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。通信を行う二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。

c　通信プロトコルの制限

住基ネットの通信プロトコルはＴＣＰ／ＩＰを基盤としているが，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（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を使用していない。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，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監視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する措置がとられている。

d　不正な通信の遮断と監視

(a)　指定情報処理機関監視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，２４時間常時監視を行っている。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。

(b)　指定情報処理機関監視ＦＷによって，全方向からの不正な通信を遮断する措置がとられている。

(c) 指定情報処理機関監視ＦＷによって，ネットワーク側からの不正な通信を遮断している。端末機を設置するため都道府県サーバと既存庁内ＬＡＮを接続する場合，都道府県側が厳格に管理するＦＷと指定情報処理機関監視ＦＷによって，端末機側からの不正な通信を遮断する措置がとられている。既存庁内ＬＡＮがさらに外部ネットワークと接続する一部団体は，さらに都道府県管理のＦＷを設置し外部からの不正な通信を遮断する措置がとられている。

(d) 指定情報処理機関監視ＦＷによって，ネットワーク側からの不正な通信を遮断する措置がとられている。既存住基システムと接続し，端末機を設置するためＣＳと既存庁内ＬＡＮを接続する場合，市町村が厳格に管理するＦＷによって，既存住基システム・端末機側からの不正な通信を遮断する措置がとられている。既存庁内ＬＡＮがさらに外部ネットワークと接続する一部団体は，さらに市町村管理のＦＷを設置し外部からの不正な通信を遮断する措置がとられている。

(e) 国の機関等サーバ

指定情報処理機関監視ＦＷによって，ネットワーク側からの不正な通信を遮断している（ネットワーク接続を行わず媒体交換を行うところもある。）。端末機を設置するため，国の機関等サーバと既存庁内ＬＡＮを接続する場合，国の機関等が厳格に管理するＦＷによって，端末機側からの不正な通信を遮断している。既存庁内ＬＡＮがさらに外部ネットワークと接続する場合は，さらに国の機関等管理のＦＷを設置し外部からの不正な通信を遮断する措置がとられている。

(イ) セキュリティ基準について（乙２の１ないし３）

総務省は，セキュリティ基準により，関係機関に対して，以下のような安全性確保のための対策を義務づけている。

a　体制，規程等の整備

知事，市町村長及び指定情報処理機関は，住基ネットにおけるセキュリティ対策のための連絡調整の場を設置し，異常の早期発見・相互連絡のための体制の整備を図る。住基ネットの企画，開発，運用に関する規程，住基ネットシステム設計書，操作手順書，緊急時の作業手順書等を整備する。住基ネット運用に必要な職員配置及び適切な人事管理を行い，同職員に対する教育・研修計画を策定し，その実施体制を確立する。住基ネットのセキュリティ対策の評価を行い，その改善に努める。緊急時の体制として，住基ネットが構成機器やソフトウエアの障害等により作動停止した際のデータ漏えいのおそれがある場合の行動計画，住民への周知方法及び相互の連絡方法を策定し，そのための連携及び研修を行う。

b　住基ネットの環境及び整備

住基ネットシステムに係る建物及び重要機能室への侵入防止のための措置を講ずる。重要機能室は，専用の部屋を確保し，所在は明らかにしないようにする。専用の部屋を確保できない場合は，電子計算機及び電気通信関係装置を厳重に固定し，磁気ディスク等を専用保管庫により施錠保管する。

c　住基ネットシステムの管理

(a)　入退室管理

重要機能室への入室者を限定，入退室者の入室権限の確認，鍵又は入退室管理カードの管理，搬出入物品の確認，事務室における職員不在時の施錠等の必要な措置を講ずる。

(b)　ソフトウエア開発等の管理

セキュリティを高める設計の実施，住基ネットシステムの試験の実施，住基ネットシステムの開発等に際してのエラー及び不正行為の防止の措置を講ずる。

(c) 住基ネットシステムの管理

住基ネットシステムの運用をする職員に対して，必要なアクセス権限を付与する。電信関係装置の管理について，不当な運用防止のための厳重な確認を行い，管理者権限のない者の操作防止，その他の措置を講ずる。

(d) 端末機，電子計算機の管理

端末機の取扱いは，管理責任者の指示又は承認を受けた者が行い，操作者識別カード及びパスワードにより，操作者のアクセス権限を確認する。操作履歴を磁気ディスクに保存する。本人確認情報の提供を求める際の照会条件を限定する。複数回アクセス失敗による端末機の強制終了等の措置を講じる。各サーバについて住基ネットシステムの管理及び運用に必要なソフトウエア以外のソフトウエアを作動させない。

(e) 磁気ディスクの保管

磁気ディスクは，保管庫等を設けて保管する。盗難防止等のため，持ち出し及び返却の措置を講じ，磁気ディスクによりデータを送付する場合は，データの送付を実施するごとに，保管状況を確認する。

(f) 構成機器及び関連設備の管理

構成機器，関連設備につき，管理方法の明確化，保守の実施，稼働状況の監視，不正プログラムの混入防止等の措置を講ずる。

(g) データ等の管理

データ，プログラム，ドキュメントの管理について，使用，複

写，消去，廃棄等における適切な管理，データを処理する者の牽制体制等必要な措置を講ずる。

(h) 障害時の対応

住基ネットシステムの障害及び不正アクセスの早期発見機能を整備し，不正アクセス判明時の相互の連絡調整及び被害拡大防止のための必要な措置を講じる。

(i) 委託を行う場合の措置

住基ネットシステムの開発，変更，運用，保守等について，業者に委託する場合は，委託先業者の社会的信用と能力を確認し，セキュリティ対策の実施，エラー・不正行為の防止等のための必要な措置を講じ，再委託の制限・分担範囲の明確化等の措置を講ずる。

d 住基ネットの運用

(a) 本人確認情報の消去

市町村においてＣＳに記録された本人確認情報について，その者の新たな本人確認情報が記録された場合，従前の本人確認情報は，５年経過後遅滞なく確実に消去する。都道府県サーバ及び指定情報処理機関サーバにおける本人確認情報についても，住基法施行令３０条の６又は３０条の１１に規定する期間経過後遅滞なく確実に消去する。

(b) 国の機関等に本人確認情報を提供する際には，知事は，国の機関等と，あらかじめ，本人確認情報の漏えい，滅失，毀損の防止その他本人確認情報の適切な管理のための措置等について協議して定め，本人確認情報の提供を受ける国の機関等も，本人確認情報の適切な管理のための措置を講ずる。

(c) 必要に応じ，知事（この項において，指定情報処理機関に委任

した知事を含む。）は国の機関等及び当該都道府県の執行機関に対し，知事及び指定情報処理機関は区域内の市町村，他の都道府県及びその区域内の市町村の執行機関に対し，市町村長は，他の市町村の執行機関及び知事，都道府県の執行機関に対し，提供が行われ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，その実施について要請を行う。

(d) 知事は，自己に係る本人確認情報の提供の状況に関する情報の開示請求に適切に対応するため，本人確認情報を提供した場合及び自己が利用した場合は，その状況に係る情報を必要な期間保存する（指定情報処理機関に事務委任した知事は，指定情報処理機関に上記状況の報告を求めた上で，同様の措置をとる。）。上記情報については，上記期間経過後遅滞なく，確実に消去する。

(ウ) 各市町村長のセキュリティ対策に対する点検

指定情報処理機関と総務省は，市町村長と協力して，平成１５年，市町村におけるセキュリティ対策の徹底を図るため，「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」に基づき，各項目ごとに３点満点とする数十項目の点検調査を実施した。その結果は，平成１５年５月１２日時点で，３２０７団体の総平均点が２．４８であった。総務省は，同年５月１３日，都道府県において，市区町村に対して必要な技術的指導を行うことを要請し，特に重要な点検項目として下記の７項目（以下「重要７項目」という。）を挙げ，そのすべてで３点満点を達成することを目標として，各都道府県，総務省及び指定情報処理機関において，技術的助言，指導を実施した。そして，総務省は，平成１５年８月８日付けで，３２０７団体の総平均点は２．８２点であるが，重要７項目については，すべての市町村において３点満点を達成したとの調査報告をまとめた

（乙１３）。

記

① 重要機能室を設置できない場合，重要機器並びに磁気ディスク及びドキュメントについて，盗難にあったり，権限のないものが容易にアクセスすることができないように，適切な管理を行う。

② ＣＳ端末について，ウイルスの侵入の脅威を最小限にとどめるとともに，外部への情報発信ができないようにするため，インターネットに接続できないよう制限を行う。

③ ＣＳと既設通信網の間のＦＷを設置し，適切な運用管理を行う。

④ ＣＳと既設通信網の間のＦＷについて，適切な設定を行う。

⑤ 住基ネットと接続する既設通信網がインターネットに接続する場合には，当該通信網とインターネットとの間にＦＷを設置し，厳重な通信制御を行う。

⑥ メールサーバ及びＷＷＷサーバ等の公開サーバについて，ＤＭＺ上の設置など適切な対策を講じる。

⑦ 公開サーバ等について，最新のパッチを当てる。

(エ) 長野県調査について

証拠（甲１８，２０の１・２，２１，２２，２３の１ないし４，２４の１ないし５，３１，乙１７ないし２４〈２２，２３について枝番を省略する。〉）及び弁論の全趣旨によれば，次の事実が認められる。

a 長野県は，市町村の庁内ネットワークを通じ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情報漏えいの可能性の有無について確認するための実験調査を，第１次調査として，平成１５年９月２２日から同年１０月１日まで，阿智村，下諏訪町，波田町を対象に，第２次調査として，同年１１月２５日から同月２８日まで，阿智村を対象に行った。

b　第１次調査

(a)　波田町では，都内からインターネット経由でインターネットと庁内ＬＡＮとの間のＦＷを突破して庁内ＬＡＮへの侵入を試みたが，成功しなかった。

(b)　阿智村及び下諏訪町では，インターネットと庁内ＬＡＮの間のＦＷを突破することを避け，庁舎内に入り，庁内ＬＡＮにつないだ攻撃端末から庁内ＬＡＮ上にある既存の住民基本台帳システムの機器の脆弱性を検査し，攻撃する実験を行った結果，既存の住民基本台帳システムの管理者権限を取得した。もっとも，庁内ＬＡＮから市町村設置のＦＷを突破してＣＳに侵入しようと試みたが成功しなかった。

なお，仮に，既存の住民基本台帳システムに侵入して個人情報を書き換えたとしても，書き換えられたデータが直ちにＣＳ内や都道府県サーバ，全国サーバに保存された本人確認情報に反映されることはない。

c　第２次調査

阿智村において，インターネットと庁内ＬＡＮとの間のＦＷ及び庁内ＬＡＮとＣＳとの間のＦＷの突破を避け，ＣＳが置かれている重要機能室に入室し，ＣＳが入っているラックを解錠し，ＣＳに直接攻撃端末をつなぎ，攻撃する実験を行い，ＣＳサーバのＯＳ管理者権限を取得することと，ＣＳから得られたＩＤとパスワードでＣＳ端末のＯＳ管理者権限を取得することに成功した。

しかし，重要機能室に入室せずにＣＳサーバのＯＳの管理者権限を奪取することは行われていない。

d　上記の調査では，住基ネット本体へ直接侵入したり，ＣＳ端末の住基アプリケーションを操作したりすること，当該市町村以外の本

人確認情報を閲覧することには成功しなかった。

e　住基アプリケーションの操作のためには操作者識別カードの挿入と，同カードと端末機の間で必要とされる相互認証を行って初めて住基アプリケーションが起動できた。

(オ)　兵庫県調査

証拠（甲６３ないし７７）及び弁論の全趣旨によれば，次の事実が認められる。

a　兵庫県は，本人確認情報の提供，利用及び保護に関する条例を制定し，平成１６年７月１日の施行に先立ち，同年４月，区域内の各市町村の住基ネット管理体制を確認するため，兵庫県チェックリストを交付して回答を求める調査を行った。

b　その結果によると，兵庫県チェックリストのうち，前記の総務省がまとめた重要７項目と内容が重複するとみられる項目とみられる一部について，次のとおりセキュリティ基準を満たしていないとする回答があった。これは，総務省の，重要７項目については全国すべての市町村において３点満点を達成したとの報告と矛盾するものである。

(a)　重要項目③と重複する「ＣＳと庁内ＬＡＮの間にＦＷを設置している－兵庫県チェックリスト１１４」につき，伊丹市が「いいえ」と回答した。

(b)　重要項目④と重複する「ＣＳと庁内ＬＡＮの通信をＦＷの設定において住基ネットに必要な通信のみに制限している－同１１５」につき，伊丹市が「いいえ」と回答した。

(c)　重要項目⑤と重複する「庁内ＬＡＮ上の端末機からインターネットに接続できないよう制限している－同１２４」について，姫路市，加古川市，猪名川町，芦屋市，伊丹市，宝塚市が「いいえ」

と回答した。

(d) 重要項目⑥と重複する「庁内ＬＡＮにインターネットからアクセス可能な公開サーバを設置していない（ＤＭＺ構成としている）ー同１２６」については，芦屋市，伊丹市が「いいえ」と回答した。

(e) 重要項目⑦と重複する「公開サーバに最新のパッチを当てているー同１３０」について，芦屋市が「いいえ」と回答した。

(カ) 大阪府下等の市町の管理状況

a 被控訴人吹田市

証拠（甲５３）及び弁論の全趣旨によれば，被控訴人吹田市においては，「吹田市住民基本台帳ネットワークシステム管理運用要領」及び「吹田市住民基本台帳ネットワークシステム緊急時対応計画書」が策定され，研修の実施，適切な委託契約の締結，重要機能室の設置・管理，ＣＳ及びＣＳ端末の適切な管理運用が行われており，ＣＳないしＣＳ端末の操作者識別カードについても，権限ごとに管理し，パスワードの設定も権限の設定を受けた操作者が規則に従って行っていること，平成１５年度において，事前の再委託承認を得ることなく再委託契約が締結されていたが，これは平成１６年度以降改められたこと，また，重要機能室への入退室については，情報政策課が担当しているところ，平成１７年１月まで入退室管理簿は作成されていなかったが，現在はそれも改善されたことが認められる。

b 被控訴人八尾市

証拠（甲５７，乙３３）及び弁論の全趣旨によれば，被控訴人八尾市においては，「八尾市住民基本台帳ネットワークシステム運営管理要綱」及び「八尾市住民基本台帳ネットワークシステム緊急時対応計画書」が策定され，研修の実施，適切な委託契約の締結，重要機能室

の設置・管理，ＣＳ及びＣＳ端末の管理・運用が行われていること，重要機能室の整備管理は企画財政部情報政策課が担当し，住基ネットの運用（住民基本台帳事務）は市民課が担当し，市民課長が重要機能室に設置されているＣＳ収納専用ラックの鍵の管理，ＣＳ運用の操作者識別カード及びパスワードの管理権限を有していること，そのため，操作者識別カードを使用するには，職員が操作者カード管理簿に日付，作業時間，返却予定時間等を記入して借り出すが，重要機能室への入退室管理簿はなく，重要機能室への入退室を記録する管理簿に記入することなく同室への入退室をしていたが，重要機能室への入退室は，入退室管理カード（八尾市住民基本台帳ネットワークシステム運営管理要綱１７条３項）によって管理されており，これまで問題は生じていないことが認められる。

c　柏原市

証拠（甲５４，乙３０）及び弁論の全趣旨によれば，柏原市においては，住基ネットの管理は市民課が所管しているが，そのほかの住民記録システム（その一部がいわゆる既存システムである。），国民健康保険等のシステムを含む基幹系（業務係）の庁内ＬＡＮや，メール等に用いる情報系の庁内ＬＡＮの管理は，総務部企画情報政策室の所管であること，住基ネットの運営に関しては，「柏原市住民基本台帳ネットワークシステム管理運営に関する要綱（施行平成１５年８月２５日）」，「柏原市住民基本台帳ネットワークシステム運用要領」，「柏原市住民基本台帳ネットワーク緊急時対応計画書」が定められており，これらに基づいて住基ネットのセキュリティ対策が講じられていること，市民課では，情報センターや大阪府等の開催する研修に参加し，そこで得られたセキュリティに関する知識を課内で共有するようにしていること，業者が電算室又はサーバ室に立ち入って作業を行う際に

は，企画情報政策室の職員が立ち会い，住基ネットのＣＳの作業を行う場合についても，企画情報政策室の職員が立ち会うこと，しかし，重要機能室の入退室管理簿は企画情報政策室が管理しているが，企画情報政策室の職員の名前がタイプ印刷され，一日のうち何度か出入りしても，一度しか記入する余地はなく，入退室の状況を正確に把握し管理するものとなっていないこと，職員の入退室はあたかも出勤簿のような体裁となっていたが，現在は，企画情報政策室の職員も入退室の都度入退室管理簿に記載するようにしていることが認められる。

d　木津町

証拠（甲５５，乙３１，３５の１ないし３）及び弁論の全趣旨によれば，木津町においては，アクセスログの確認を専門業者に委託しているが，担当の住民課長が必要に応じて業者から報告，説明を受けることができることが認められる。

イ　住基法は，本人確認情報の安全確保の措置として，知事，指定情報処理機関及びそれら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ずる義務があり（３０条の２９第１項，第２項），市町村長とその受託者は，本人確認情報に限らず，住民票記載事項すべてにつき上記と同様の義務がある（３６条の２）ことを定める。これは，個人情報を安全に管理するための技術や組織の確立というセキュリティ面での原則を定めたものであり，それについては，「技術的側面」と「人的側面」とからの安全管理の対策が要求されているものと解される。そして，「技術的側面」については，アクセスログの保存や開示，情報の暗号化，内部の者が権限なしに情報にアクセスできないように使用アプリケーションやシステムのセキュリティを高めることなどが問題となり，「人的側面」につ

いては，個人情報管理責任者の選任，当該情報へのアクセス権限の限定や関係者に対する管理体制の確立などが問題となる。そこで，前記前提事実及び上記認定事実に基づき，それらの点について検討する。

(ア) 技術的側面について

住基ネットは，システムの構成機器その他いわゆるハードウェアの面については，電気通信にはＶＰＮによる専用回線が使用され，各サーバ間にはそれぞれＦＷが設置され，ネットワーク上にはＩＤＳが設置されるなど，技術面では全般にわたって相当厳重なセキュリティ対策が講じられており，その内容から見れば，抽象的にはそのセキュリティが破られる可能性が全くないとまではいえないとしても，少なくともその具体的危険性が存在するとまで認めることはできない。

長野県侵入実験の結果については，①インターネット回線を通じてインターネット側ＦＷ越しにＤＭＺに設置された公開サーバの管理権限を奪取できなかった，②庁舎内あるいは隣接した施設にある端末から庁内ＬＡＮに接続した攻撃用コンピュータにより既存住基システムのサーバの管理者権限の奪取には成功したが，庁内ＬＡＮを通じ市町村設置ＦＷ越しにＣＳないしＣＳ端末の管理者権限は奪取できなかった，③ＣＳセグメント内の端末に接続した攻撃用コンピュータによりＣＳの管理者権限を奪取すること及びＣＳ端末の管理者権限を奪取することはできたが，住基アプリケーションを任意に操作できるかについては実験は行われていないのであり，同実験においては，設置されているＦＷ越しの攻撃に全て失敗していること，管理者権限を奪取できたのは，庁内ないし隣接建物において物理的に端末に接続した場合であって，当該市町村の職員が許諾しない状態で物理的な庁舎の警備等を回避して端末に接続して攻撃を加

えることの現実的可能性や，その場合の住基アプリケーションの任意操作の可能性については実証されていない。

これらの点を考慮すれば，同実験には様々な制約があったことが窺われるけれども，長野県侵入実験の結果によって，住基ネット内における本人確認情報その他の情報の漏えい，改ざん等の具体的な危険性の存在が証明されたとまでいうことは難しい。

(イ) 人的側面について

セキュリティ基準や条例によって，住基ネットの運用や住基ネットシステムの管理について，個人情報管理責任者の選任等の適正な人事管理，当該情報へのアクセス権限の限定や関係者に対する管理体制の確立，担当職員に対する教育・研修等が策定，実施されてきている。

確かに，兵庫県調査の結果によれば，総務省の重要７項目の一部を満たしていない市町があり，また，大阪府下の市町の中にも，重要機能室への入退室の管理等に不十分なところや，アクセスログの確認を委託業者に委ねているところがあるなど，自治体の中にはセキュリティシステムの重要性についての認識が十分でないところがあったといわざるを得ない。

しかし，兵庫県調査の対象市町に見られた問題点は，セキュリティの極めて基本的な事柄についてのものであることから，その後の兵庫県の指導等により改善措置が講じられたであろうと推認して差し支えないものと思われるし，上記大阪府下の市町に見られた問題点も，管理運営に関する要綱等に基づいて改善，管理強化の対策が講じられてきている。

(ウ) 以上のところからすれば，技術的側面では，住基ネットシステムの構成機器その他いわゆるハードウェアの面について相当厳重なセ

キュリティ対策が講じられるなどし，また，人的側面でも，人事管理，研修・教育等種々の制度や運用基準が定められて実施されてきており，一定の個人情報保護措置が講じられているものと評価することができ，現時点において，住基ネットのセキュリティが不備で，本人確認情報に不当にアクセスされたりして，同情報が漏えいする具体的危険があるとまで認めることはできない。

4　住基ネットによるデータマッチング等の危険性の有無（住基ネットの実現手段としての合理性－その２）

(1)　住基ネットは，市町村長が本人確認情報を知事に通知し，知事が，国の機関や法人，他の都道府県や市町村の執行機関に対して本人確認情報を提供するものであるが，知事は，これらの提供事務を，総務大臣が指定した指定情報処理機関である情報センターに委任している。そして，全都道府県知事が，情報センターに上記事務を委任している。

これによって，すべての住民の本人確認情報は，情報センターのコンピュータで一元的に保存されるとともに，国の機関や法人，知事や市町村長に対して提供される。提供される事務は，住基ネットの一次稼働が始まった平成１４年８月５日時点では９３事務であったが，現在（平成１７年４月１日）までに２７５事務に拡大されており，法律及び条例の制定，改正によって，今後も更に拡大されることが予想される。そして，提供される本人確認情報には，住民票コードが含まれており，したがって，情報センターから本人確認情報の提供を受ける行政事務に関するデータベースには，個人の情報に住民票コードが付されることになるから，これによって，そのデータベース内における検索が極めて容易になり，また，行政機関が収集・保存している膨大な個人情報をデータマッチングし，住民票コードをいわばマスターキーのように使って名寄せすることにより，個人情報を共同利用することを可能とするインフラが，住基ネットにより整備されたということができる。

(2) ところで，住基ネットによる本人確認情報の利用，提供等については，次のような法規制がされている。

ア　本人確認情報の利用，提供

(ア) 住基法では，住基法別表の事務を行うため本人確認情報を受領した者（「受領者」）は，当該事務処理の遂行に必要な範囲内で，受領した本人確認情報を利用し，又は提供するものとされている（同法３０条の３４）。

(イ) (ア)の範囲を超える「目的外の使用」の禁止

a　住基法３０条の３４（同法３０条の４２，３０条の４３も同じ）

同規定によれば，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とされている。

b　個人情報保護法

同法によれば，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（同法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（同法８条１項）としている。

個人情報保護法８条２項２，３号は，一定の要件のもと，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，又は提供することを許容する規定であるが，同条３項は，「前項の規定は，保有個人情報の利用又は提供を制限する他の法令の規定の適用を妨げるものではない」と規定する。そして，住基法３０条の３４は，個人情報保護法８条３項に定める「他の法令の規定」に該当すると解されるから，同条２項に優先して住基法３０条の３４が適用されることとなり，本人確認情報についての目的外利用は禁止されているものと解される。

c　違反行為に対する罰則等

(a)　上記(ア)（住基法３０条の３４）で許される範囲を超えたデータマッチングは，同規定の職務上の義務に違反した場合に該当するため，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）。

(b)　行政機関の職員が，上記(ア)の範囲を超える利用のために，本人確認情報に関する秘密が記録された文書，図画又は電磁的記録を収集した場合には，「その職権を濫用して，専らその職務の用以外の用に供する目的で」行ったもの（個人情報保護法５５条）に当たり，刑罰（１年以下の懲役又は５０万円以下の罰金）の対象となると考えられる。

(c)　上記(ア)の範囲を超える利用のために，指定情報処理機関の役員及び職員や（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す行為は，公務員の守秘義務違反（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）として刑罰の対象となる。

また，秘密の提供方法が，電算処理ファイル（個人情報保護法２条４項１号）によってなされた場合には，同法５３条に該当することとなり，刑罰（２年以下の懲役又は１００万円以下の罰金）の対象となり，自己若しくは第三者の不正な利益を図る目的で秘密を提供した場合には，提供された秘密が電算処理ファイルではなくとも，刑罰（１年以下の懲役又は５０万円以下の罰金）に処せられる（同法５４条）。

さらに，秘密を漏らした者が住基法３０条の３５第２項に規定する電子計算機処理等に関する事務に従事する者であれば，同項

の秘密保持義務にも違反することとなり，住基法４２条の刑罰（２年以下の懲役又は１００万円以下の罰金）の対象となる。

イ　違反行為に対する監視機関

(ア)　住基法は，都道府県に同法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保護に関する審議会（以下「都道府県審議会」という。）を置くことを定め（同法３０条の９第１項），当該審議会は，「この法律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，知事の諮問に応じ，当該都道府県における同法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保護に関する事項を調査審議し，及びこれらの事項に関して知事に建議することができる」（同法３０条の９第２項）ものとされている。

(イ)　住基法は，「指定情報処理機関には，本人確認情報保護委員会を置かなければならない」（同法３０条の１５第１項）とし，当該委員会は，「指定情報処理機関の代表者の諮問に応じ，第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保護に関する事項を調査審議し，及びこれに関し必要と認める意見を指定情報処理機関の代表者に述べることができる」（同法３０条の１５第２項）ものとされている。

(ウ)　セキュリティ基準は，「都道府県知事（委任知事にあっては，指定情報処理機関）は，必要に応じ，国の機関等に対し，提供を行った本人確認情報の適正な管理のための措置の実施について要請を行うこと。また，委任知事は，必要に応じ，指定情報処理機関を経由して，国の機関等に対し，指定情報処理機関が提供を行った当該都道府県の住民に係る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について要請を行うこと。」（第６－８－(1)－ウ）と規定し，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

ついて報告を求め，適切に管理するよう要請することができるものとされている。

(3) 上記(2)の法規制からすれば，データマッチングや名寄せは目的外利用に当たるものとして禁止され，その違反に対して罰則も用意されている。そして，本人確認情報を記録，保有する指定情報処理機関は，住基法別表で定める国の機関等に対し，その求めに応じて本人確認情報を提供することは予定されているが，指定情報処理機関が国の機関等から，その保有する本人確認情報以外の住民に関する情報を収集し，これを管理することができ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提供する義務はないから，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り，国の機関等が保有する個人情報を統一的に収集し得る主体もシステムも制度化されていない。これらの点を考慮すれば，住基ネットの運用によって控訴人らが主張するようなデータマッチングや名寄せが行われることは考え難いといえなくもない。

(4) しかしながら，次の点を指摘することができる。

ア 本人確認情報保護の法制について

(ア) 個人情報保護法は，個人情報の保有につき，法令の定める所掌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（同法３条１項），その特定された利用目的の達成に必要な範囲を超えて，保有してはならないこと（同条２項）を定めるが，その利用目的を変更する場合には，変更前の利用目的と相当の関連を有すると合理的に認められる範囲を超えて行ってはならない（同条３項）と定め，保有個人情報を保有を開始した利用目的を変更して保有することができることを許容している。この利用目的の変更は一種の目的外利用ということができる（総務省行政局監修

の「行政機関等個人情報保護法の解説」（２６・２７頁）も，利用目的以外の利用・提供が恒常的に行われる場合は，同法３条３項に基づく利用目的の変更に該当し，臨時的に行われる場合は，同法８条２項に基づく利用目的以外の利用・提供に該当するとしている。）が，その変更された目的による利用や提供については，同法８条３項のような規定は置かれていないから，住基法３０条の３４の違反にはならないことになる。そして，行政機関の裁量によって行われるそのような目的変更による利用，提供について，適切な監視機関は置かれていない。住基法３０条の９第１項は，都道府県に都道府県審議会を設置し，同審議会は本人確認情報の保護に関する事項の調査審議及びこれらの事項に関する知事への建議をすることができると定めているが，同審議会は部内機関であって第三者機関ではないし，個人情報保護法では，その存在さえ知らされない個人情報ファイルが多数予定されている（同法１０条２項，１１条１項）ことを考えると，都道府県審議会に対して上記利用目的変更についての適切な監視機能を期待することは困難であろうと思われる。のみならず，都道府県審議会は，国の行政機関等の本人確認情報の利用については調査権限はない。これらのことからすると，上記利用目的変更の適切な運用が厳格になされる制度的な担保は存在しないといわざるを得ず，住基法の利用目的明示の原則（同法４条）が形骸化する危険性は高いというべきである。

(イ) 個人情報については，情報取扱者の使用目的や使用の実態を知ることができるように，利用目的を明確にし，本人がそれを知ることができるようにし，本人において個人情報保護の救済手段がとれるようにすべきことが要請されていると解されるが（個人情報保護法４条，３０条の３７，３６条ないし４１条参照），行政機関が保有する本人確認情報を利用できる国の事務は，当初は９３事務であったものが現在で

は２７５事務にまで拡大され，それは今後さらに拡大することが予想される。加えて，条例で定めれば，自治体が独自に他の機関に本人確認情報を提供することも可能である。もちろん住民は，法令上の拡大を知ろうと思えば知ることはできるであろうが，上記のように拡大してくれば，実際上利用対象事務を把握することは困難であり，本人の同意や利用をめぐる異議申立ての機会は保障されないに等しいといえる。また，本人確認情報についての開示請求権（住基法３０条３７第１項）は，自己に関してどのような情報が収集管理されているかを確認し，必要に応じて訂正請求を行うために極めて重要な意味を有するが，開示対象は本人確認情報の記録された磁気ディスクに限定されており，本人確認情報がいかなる機関に提供されたか，それ以外の情報を都道府県や国，指定情報処理機関が保有していないかどうかといった重要な点について，本人において確認することが事実上不可能な状態にあるといえる。

(ウ) 住基法上，第三者は他人の住民票コードのついた住民票の写しの交付を求めることはできず（同法１２条２項），何人も業として住民票コードの告知を求めることが禁止されている（同法３０条の４３第２項）が，本人や家族が，住民票の写しを請求して第三者に交付したり，住民票コードを告げたりすれば，第三者は人の住民票コードを知ることができる。また，住民票コードの民間における利用は禁止されているが（同法３０条の４３第３項），法の規制にかかわらず，個人情報そのものが商品価値を持ち，大量の個人情報の収集や流出が少なからず行われている社会の現状を考えると，違法な利用がたまたま発覚することを期待する以外に，実際に上記の禁止を担保する制度は存在しないといわざるを得ず，その意味では，民間利用禁止の実効性は，現実には非常に疑わしい。

また，住基法３０条の４２第１項から第４項は，住民票コードの不必要な収集禁止を定めるが，ここでいう「不必要な」場合とは，住基法上の事務ないし同法に基づき本人確認情報の提供を求めることができる事務の遂行に必要な場合以外のことを指しているから，法律や条例によって，利用できる事務の範囲を将来的に無制限に拡大できる以上，これもまた，実質を伴わないに禁止に堕する危険も小さくない。

(エ) 個人情報保護法は，利用・提供の制限を定めるが，①行政機関が法令の定める所掌事務の「遂行に必要な限度で」保有個人情報を内部で利用する場合であって，当該個人情報を利用することについて「相当な理由のあるとき」（同法８条２項２号），②他の行政機関，地方公共団体等に保有個人情報を提供する場合において，保有個人情報の提供を受ける者が，法令の定める事務又は業務の遂行に「必要な限度で」提供に係る個人情報を利用し，かつ，当該個人情報を利用することについて「相当な理由のあるとき」（同３号）は，本人の同意がなくとも，利用目的以外の目的のために保有個人情報を利用し又は提供することができる（ただし，それが本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは，その限りでない。）と定める。上記の「必要な限度」，「相当な理由」等の要件の有無は，行政機関が自ら判断するのであるから，実際には，実効性のある利用制限の歯止めになり得ず，行政機関が住基ネット上における本人確認情報の利用を事実上自由に行いうることになってしまう危険性が高い。個人情報の取得について，本人に対しあらかじめ「利用目的を明示」することを要求し（同法４条），目的外の利用，提供の禁止の例外として「本人の同意」（同法８条２項１号）を定めている同法の制度趣旨にかんがみ，目的外利用禁止の例外については，「本人同意」とみなすことができるような相応の制度的担保が必要であると解されるが，目的外利用の禁止違反に対する前記の罰則

等の規制を考慮しても，上記の目的外利用禁止のための制度的担保は十分とはいい難い。

(オ) 行政機関においては目的外利用が可能な場合もあるが，それらの外延が明らかであるとはいえず，その外延目的情報については複数の行政機関の間で関連性が競合することがあることも十分予想され，そうなれば各行政機関の間でデータマッチングが進められ，現在の住基ネットのシステムの上では一元化の主体機関は存在しないことから，個人情報の完全な一元化までの具体的危険があるとはいえないにしても，行政機関が個別に保有する個人情報の範囲が拡大して，少数の行政機関によって，行政機関全体が保有する多くの部分の重要な個人情報が結合・集積され，利用されていく可能性は決して小さくないといえる。

(カ) 公権力を行使する行政機関による個人情報の取扱いに対する監視機関は，行政から独立した第三者機関（外部機関）であって実効性のある監視機能が果たせるといえるが，住基ネットの運用について，データマッチングや名寄せを含む目的外利用を中立的立場から監視する第三者機関は置かれていない。

イ 個人情報の集積・結合，利用について

(ア) 証拠（甲１１）及び弁論の全趣旨によれば，平成１５年４月２３日，防衛庁長官が防衛庁の適齢者情報収集問題についての内部調査の結果を衆議院個人情報保護特別委員会において公表したことが新聞で報道されたが，これによると，自衛官募集に関する適齢者情報を提供していた市町村が７９４あり，このうち住民基本台帳法で閲覧が認められている４情報以外も提供した市町村が３３２市町村であったことが明らかにされたこと，また，防衛庁により，自衛官募集に関する手引を作成した地方公共団体が，２４都道府県，１２８市町村あり，このうち３県，２７市町村が，上記手引の中に４情報以外である「健康状態」

「技能免許」「職業」「世帯主の氏名と本人の続柄」「電話番号」等を提供するよう取り決めていたこと，そして，実際には上記手引を作成していない自治体からも適齢者情報の提供があったこと，また，自衛官の募集などを担当する全国５０の地方連絡部のうち１７地方連絡部では，こうした情報がコンピュータなどで電算処理され，うち７地方連絡部では，４情報以外の世帯主や学校名，筆頭者，保護者名なども入力されていたことが明らかになったとされていることが認められる。

上記のような個人情報の収集や取扱いが行われていたことは，住基ネットの本人確認情報を利用して当該本人に対する個人情報が際限なく集積・結合されて，それが利用されていく危険性が具体的に存在することを窺わせるものといえる。

(イ) 住基カードは，ＩＣカードで，大容量のデータ蓄積機能があり，４情報及び住民票コードが記録されている（住基法３０条の４４第１項，同法施行令３０条の１２）ほか，公的個人認証アプリケーションがプレインストールされている。そして，市町村長その他の執行機関は，条例によって，住基カードを様々な目的に使用することができ，市町村が提供するサービスとして，検診，健康診断等の申込み，結果の照会等を行うサービス，公共施設の空き照会，予約等を行うサービス，介護保険の資格確認を行うサービス，病院の診察券として利用するサービス，公共料金等の決済に係るサービス，その他多くのことが考えられている（弁論の全趣旨）。そして，住民が住基カードを使ってそれらのサービスを受けた場合には，その記録が行政機関のコンピュータに残り，それらの記録を住民票コードで名寄せすることも可能である。住基カードに関する技術的基準（総務省告示第３９２号第５，３(2)）では，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に住民票コードを使用しないことが定められているが，総務省は，告示の改正によ

っていつでもこれを改めることができる。

(5) 上記(4)の諸点を考慮すれば，住基ネット制度には個人情報保護対策の点で無視できない欠陥があるといわざるを得ず，行政機関において，住民個々人の個人情報が住民票コードを付されて集積され，それがデータマッチングや名寄せされ，住民個々人の多くのプライバシー情報が，本人の予期しない時に予期しない範囲で行政機関に保有され，利用される危険が相当あるものと認められる。そして，その危険を生じさせている原因は，主として住基ネット制度自体の欠陥にあるものということができ，そうである以上，上記の危険は，抽象的な域を超えて具体的な域に達しているものと評価することができ，住民がそのような事態が生ずる具体的な危険があるとの懸念を抱くことも無理もない状況が生じているというべきである。したがって，住基ネットは，その行政目的実現手段として合理性を有しないものといわざるを得ず，その運用に同意しない控訴人らに対して住基ネットの運用をすることは，その控訴人らの人格的自律を著しく脅かすものであり，住基ネットの行政目的の正当性やその必要性が認められることを考慮しても，控訴人らのプライバシー権（自己情報コントロール権）を著しく侵害するものというべきである。

控訴人らは，住基ネット全体の運用の停止を求めているのではなく，住基ネットからの離脱を求めているにすぎないところ，住基ネットは全住民を対象として構想，構築されていることから，一部の者の離脱を認める場合には，住基ネットの目的の完全な達成が阻害されることになり，また，離脱者の把握のためのコストが必要となることになるということはいえるが（もっとも，それらがどの程度のものであるかは明らかでない。）住基ネットの運用により，住民票コードをもって行政機関に保有されている多くの個人情報がデータマッチングや名寄せされて利用される具体的危険がある（民間においてもそのような事態が生じる危険がある。）状態は，住基ネ

ットを利用する住民の人格的自律を著しく脅かす危険をもたらしているものといえるのであり，個人の人格的自律の尊重の要請は，個人にとってだけでなく，社会全体にとっても重要なものであることも合わせ考慮すれば，控訴人らが住基ネットから離脱することにより生ずる上記障害等を回避する利益が，控訴人らの自己情報コントロール権により保護される人格的利益に優先するものとは考え難い。

そうであれば，明示的に住基ネットの運用を拒否している控訴人らについて住基ネットを運用すること（改正法を適用すること）は，控訴人らに保障されているプライバシー権（自己情報コントロール権）を侵害するものであり，憲法１３条に違反するものといわざるを得ない。

5　争点(2)（控訴人らの慰謝料請求権の有無）について

国家賠償法１条１項は，国又は地方公共団体の公権力の行使に当たる公務員が，個別の国民に対して負担する職務上の法的義務に違反して当該国民に損害を加えたときに，国又は公共団体がこれを賠償する責に任ずることを規定したものである。

ところで，普通地方公共団体の長は，当該団体を統轄し，これを代表する立場において，当該団体の事務を管理及び執行する権限を有し（地方自治法１４７条，１４８条），それら執行行為等は法律，政令，条例等に基づいて行うべき義務を負っているものであることを考慮すると，普通地方公共団体の長が法令に基づいて行った執行行為は，原則として職務上の法的義務に違反しないものと解するのが相当である。もっとも，その法令が憲法に違反する無効のものであり，当該地方公共団体の長がそのことを認識し得た場合には，その執行行為は違法性を具備するものと解するべきである。

これを本件についてみると，被控訴人らの各市長は，地方自治体の執行機関として，住基法に従って住基ネットを運用したものであり，改正法の住基ネットについては国民各層に様々な意見があったこと（周知の事実である。）を考

慮すれば，被控訴人らの各市長において，改正法の控訴人らに対する適用が憲法に違反する無効のものであることを認識し得たとは認められないから，被控訴人らの各市長の行為が国家賠償法上違法であるとは認められない。

6　争点(3)（控訴人[redacted]ら４名の差止め請求権の有無と差止め請求の可否）について

(1)　自己に関する住基ネットの運用の差止めを求める控訴人[redacted]ら４名に対する住基ネットの運用は，上記のとおり同控訴人らの権利を違法に侵害するものであり，その権利侵害の状態は，主として住基ネット制度自体の欠陥に原因するものと認められるものである上，同控訴人らの人格的自律を脅かす程度も相当大きいと評価できるものであることを考慮すれば，それが続く場合には同控訴人らに回復し難い損害をもたらす危険があるというべきである。

このような場合には，権利を侵害されている者はその侵害行為の差止めを請求することができると解するのが相当であり，控訴人[redacted]ら４名は，各自に対する住基ネットの運用の差止めを求めることができるというべきである。

(2)　控訴人[redacted]ら４名が各住民登録地の被控訴人市に対して求めている行為は，同控訴人らの本人確認情報の大阪府知事に対する通知及び同控訴人らに係る住民基本台帳上の住民票コードの削除である。

上記の大阪府知事に対する通知の差止めは，行政機関の行為で，法律に基づく行為であるが，国民に対して権利を設定し，義務を課し，その他具体的な法律上の効果を発生させる行為（処分）ではなく，事実行為であり，行政事件訴訟の差止めの訴えによって救済を求めることができないものと解されるから，民事訴訟において差止めを求めることができると解される。

また，住民基本台帳上の住民票コードの削除は，作為を求めるものであるが，実質は差止め（権利侵害状態の停止）を実効あるものとするための原状回復行為であるから，差止め請求と同様に求めることができるものと解され

る。

(3) ところで，控訴人[redacted]ら４名の本人確認情報については，住基法３０条の５に基づき既に大阪府知事に対して通知されているものと認められるから，今後大阪府知事に対して同控訴人らの本人確認情報について通知することが住基法上義務づけられているのは，本人確認情報について変更を生じた場合（変更情報）に限られることになる（住基法３０条の５第１項)。そして，住基ネットは，本人確認情報を住民票コードによって管理，利用されているものであるから，住民票コードを除く本人確認情報が大阪府に保有されているだけの状態の下では，本人確認情報の目的外利用等による権利侵害の危険性は小さいと考えられ，控訴人[redacted]ら４名についての個人情報のデータマッチングや名寄せの危険による権利侵害状態の排除は，住民票コードの削除によって最も実効性があるといえる（住民基本台帳上の住民票コードのみの削除は住基法の予定していないことと解されるが，それが行われた場合には，市町村においては，住基法８条により住民票上の住民票コードの記載を削除し，市町村長から知事に対し，変更情報のうちの「住民票コードの記載の変更請求」に準じて，住基法３０条の５第１項により通知され，知事において保有する当該本人についての住民票コードを削除すべきものと解される。)。

したがって，控訴人[redacted]ら４名の差止め請求のうち，同控訴人ら各自の住民票コードの削除の請求を認容し，大阪府知事に対する本人確認情報の通知差止め請求を棄却すべきである。

(4) 控訴人[redacted]ら４名は，原審第５回口頭弁論期日前の平成１５年１１月２１日，提訴した被控訴人らに対する国家賠償法１条１項に基づく損害賠償（慰謝料）請求に加えて，それぞれの住民登録地の各被控訴人市に対して上記当審における追加請求と同一の請求を追加する訴えの変更の申し立てをしたが，原審裁判所は，両請求は請求の基礎が同一でないとして，訴えの変更を許さなかった。控訴人[redacted]ら４名は，当審において，上記原審において訴え

の変更を申立てた請求と同一の請求である前記当審追加請求をしたものであるところ，同控訴人らが上記各請求において主張する被侵害権利ないし利益及びその原因行為である被控訴人らの行為の内容は，両請求とも同一のものであり，その同控訴人ら主張の権利ないし利益の侵害が認められるか否かが両請求共通の中心争点となるものである。そして，控訴人[redacted]ら４名の当審追加請求が民事訴訟事項であることは上記のとおりである。これらの点からすれば，上記両請求は，社会生活上同一の紛争に関するものであり，訴訟資料及び証拠資料も共通のものということができるから，請求の基礎に同一性があるものと認められるし，控訴人[redacted]ら４名申立ての訴えの変更を認めても，審理を著しく遅滞させることになるとは認められない。

以上のところからすれば，控訴人[redacted]ら４名の当審における追加的訴えの変更（当審追加請求）は，これを認めるべきである。

上記被控訴人らは，上記訴えの変更申立ては，同被控訴人らの審級の利益を害するものであるから，同被控訴人らの同意を要すると主張する。

しかし，控訴審における訴えの変更は，追加的訴えの変更を含め，相手方の同意は要しないと解される（民訴法１４３条の制約を受けるだけである（２９７条））。最高裁判所平成５年７月２０日第三小法廷判決（民集４７巻７号４６２７頁）は，国家賠償法１条１項に基づく損害賠償請求に憲法２９条３項に基づく損失補償請求を控訴審において予備的・追加的に併合申立てした事案において，両請求は請求の基礎を同一にするものとして旧民訴法２３２条の規定による訴えの追加的変更に準じて損害賠償請求に損失補償請求を追加することができるとした上で，その場合には，損失補償請求が公法上の請求として行政訴訟手続によって審理されるべきものであることなどを考慮すれば，相手方の審級の利益に配慮する必要があるから，控訴審における上記訴えの変更には相手方の同意を要すると判示しているが，同判決が通常の民事訴訟における訴えの変更と異なる解釈を示したのは，新たに追加される

損失補償請求についての訴訟が，行政事件訴訟法の規定上，実質的当事者訴訟とされ，行政庁が訴訟に参加することができること（行政事件訴訟法４１条１項，２３条）を考慮し，第１審における行政庁の参加の機会を一方的に奪うことは適当でないことなどを考慮したものと理解されるものであり，上記最高裁判所の判決の事案は，本件と事案を異にするものである。上記被控訴人らの主張は採用できない。

7　結論

以上によれば，控訴人[redacted]ら４名の当審追加請求は，住民基本台帳から同控訴人らの住民票コードの削除を求める限度で理由があるが，その余は理由がなく，控訴人らの控訴は理由がないというべきである。

よって，主文のとおり判決する。

大阪高等裁判所第７民事部

裁判長裁判官　竹　中　省　吾

裁判官　竹　中　邦　夫

裁判官　矢　田　廣　高