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）－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－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