主文

１　原告らの請求をいずれも棄却する。

２　訴訟費用は原告らの負担とする。

事実及び理由

第１　原告らの請求

１　被告は，住民基本台帳法に基づく住民基本台帳カードの交付に関して，公金を支出し，契約を締結若しくは履行し，又は債務その他の義務を負担してはならない。

２　被告は，Ｐ１に対し，２０００万円を支払うよう請求せよ。

第２　事案の概要

本件は，名古屋市の住民である原告らが，住民基本台帳法（平成１１年法律第１３３号（以下「改正法」ともいう。）による改正後のもの。以下「住基法」というが，条文を引用する場合は，単に「法」と表示する。）に基づく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。）が憲法１３条等に違反するものであり，これを前提とする住民基本台帳カード（以下「住基カード」という。）の交付に関して公金を支出することや，その原因となるべき契約を締結する行為なども違法であると主張して，被告に対し，①地方自治法２４２条の２第１項１号に基づき，上記公金支出行為等の差止めと，②同項４号に基づき，支出が確定した公金２０００万円の損害賠償を市長の地位にあったＰ１（以下，個人としての同人を「Ｐ１市長」という。）に請求するように求めた住民訴訟である。

１　前提事実等（争いのない事実，各項末尾記載の証拠により容易に認定できる事実等）

(1)　当事者

ア　原告らは，いずれも名古屋市の住民である。

イ　被告は，名古屋市の長としてその事務を管理，執行する機関である。

ウ　返還請求の相手方とされたＰ１市長は，名古屋市の長として，住基カード等の調達契約を締結し，その代金支払債務を確定させた者である。

(2)　住基法の定める住基ネット等の概要

ア　住基ネット

住基ネットとは，法３０条の２以下に基づいて創設され，市町村長が本人確認情報（氏名，生年月日，性別，住所及び住民票コード並びにこれらの変更情報）を都道府県知事に通知し，法３０条の１０第３項所定の委任都道府県知事が本人確認情報を指定情報処理機関に通知し，並びに都道府県知事及び指定情報処理機関が本人確認情報の記録，保存及び提供を行うためのコンピュータネットワークシステムであって，各市町村に設置されたコミュニケーションサーバ（以下「ＣＳ」ともいう。），各都道府県に設置されたサーバ（以下「都道府県サーバ」という。），指定情報処理機関に設置されたサーバ（以下「全国サーバ」という。），端末機，電気通信関係装置（ファイアウォールを含む。），電気通信回線，プログラム等により構成されている（平成１５年総務省告示第６０１号による改正後の電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成１４年総務省告示第３３４号。以下「セキュリティ基準」という。）第１の１参照。乙２の１ないし３）。

なお，住基ネットのイメージ概略図は，別紙１及び別紙２のとおりである。

イ　住民票コード

住民票コードとは，１１けたの番号（無作為に作成された１０けたの数字と１けたの検査数字）であって，市町村長がそれぞれの市町村の住民の住民票に対して割り当てるものである（法７条１３号，３０条の２第１項，第２項，改正法附則３条，住基法施行規則（以下，条文を引用する場合は，単に「規則」と表示する。）１条）。

ウ　指定情報処理機関

都道府県知事は，総務大臣の指定する者（指定情報処理機関）に対して，本人確認情報処理事務を行わせることができるところ（法３０条の１０第１項），全国４７の都道府県知事すべてが総務大臣の指定した指定情報処理機関である財団法人地方自治情報センターに本人確認情報処理事務を行わせている。

エ　市町村長から都道府県知事への本人確認情報の通知

市町村長（なお，法３８条１項により，政令指定都市においては，政令で定めるところにより，区長が市長とみなされている。）は，住民票の記載，消除又は法７条１号から３号（氏名，生年月日，性別）まで，７号（住所）及び１３号（住民票コード）に掲げる事項の全部若しくは一部についての記載の修正を行った場合には，当該住民票の記載に係る本人確認情報を，市町村に設置されたＣＳから住基ネットを通じて都道府県サーバに送信することによって，都道府県知事に通知する。この通知を受けた都道府県知事は，本人確認情報を，政令で定める期間保存しなければならない（法３０条の５）。

オ　都道府県知事から指定情報処理機関への本人確認情報の通知

都道府県知事は，上記エにより市町村長から通知を受けた本人確認情報を，都道府県サーバから住基ネットを通じて全国サーバに送信することによって，指定情報処理機関に通知する。この通知を受けた指定情報処理機関は，本人確認情報を磁気ディスクに記録して，政令で定める期間保存しなければならない（法３０条の１１第１項ないし３項）。

カ　指定情報処理機関による本人確認情報等の提供

(ア)　指定情報処理機関は，住基法別表第１の上欄に掲げる国の機関又は法人（以下「国の機関等」という。）から同表の下欄に掲げる事務の処理に関し，住民の居住関係の確認のための求めがあったときに限り，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（法３０条の１０第１項３号，同条の７第３項）。

(イ)　指定情報処理機関は，①市町村の執行機関であって住基法別表第２の上欄に掲げるものから同表の下欄に掲げる事務の処理に関し求めがあったとき及び②市町村長から住民基本台帳に関する事務の処理に関し求めがあったときには，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ことができる（法３０条の１０第１項４号，同条の７第４項）。

(ウ)　指定情報処理機関は，①他の都道府県の執行機関であって同法別表３の上欄に掲げるものから同表の下欄に掲げる事務の処理に関し求めがあったとき及び②他の都道府県の都道府県知事から，当該都道府県の区域内の市町村の住民基本台帳に住民に関する正確な記録が行われるよう，市町村長に対する必要な協力の求めがあったときには，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（法３０条の１０第１項５号，同条の７第５項，第１０項）。

(エ)　指定情報処理機関は，①当該他の都道府県の都道府県知事を経て当該他の都道府県の区域内の市町村の執行機関であって同法別表第４の上欄に掲げるものから同表の下欄に掲げる事務の処理に関し求めがあったとき及び②当該他の都道府県の都道府県知事を経て当該他の都道府県の区域内の市町村長から住民基本台帳に関する事務の処理に関し求めがあったときには，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（法３０条の１０第１項６号，同条の７第６項）。

(オ)　指定情報処理機関は，国の行政機関がその所掌事務に必要があるとして，都道府県知事に対して，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たときには，同資料の提供をする（法３０条の１０第１項７号，３７条２項）。

キ　都道府県知事による本人確認情報等の提供

(ア)　都道府県知事は，①区域内の市町村の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときには，条例で定めるところにより，保存期間に係る本人確認情報を提供するほか，②区域内の市町村の執行機関であって法別表第２の上欄に掲げるものから同表の下欄に掲げる事務の処理に関し求めがあったとき及び③区域内の市町村の市町村長から住民基本台帳に関する事務の処理に関し求めがあったときには，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ことができる（法３０条の１０第３項，１項４号，同条の７第４項）。

(イ)　都道府県知事は，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，他の都道府県の執行機関に対し，保存期間に係る本人確認情報を提供する（法３０条の７第５項２号）。

(ウ)　都道府県知事は，当該他の都道府県の都道府県知事を経て当該他の都道府県の区域内の市町村の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときには，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（法３０条の７第６項２号）。
（エ） 都道府県知事は，国の行政機関がその所掌事務に必要があるとして，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たときには，同資料を提供する（法３０条の１０第３項，１項７号，３７条２項）。
ク 市町村長による本人確認情報の提供
市町村長は，他の市町村の市町村長その他の執行機関であって条例で定めるものから条例で定める事務の処理に関し求めがあったときは，条例で定めるところにより，本人確認情報を提供する（法３０条の６）。
ケ 住基カード
住基カードとは，住民票に記載された氏名及び住民票コードその他政令で定める事項が記録されたカードをいう（法３０条の４４第１項）。
住民基本台帳に登録されている者は，その者が記録されている住民基本台帳を備える市町村の市町村長に対して，所定の交付申請書を提出して，住基カードの交付を求めることができ，交付を求められた市町村長は，その者に対し，住基カードを交付しなければならない（法３０条の４４第２項，第３項）。
住基カードの交付を受けている者は，それを紛失したときは，直ちにその旨を市町村長に届け出なければならず，また，転出をする場合その他政令で定める場合には，当該住基カードを市町村長に返納しなければならない（法３０条の４４第５項，第６項）。
また，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（法３０条の４４第８項）。
コ 住民票の写しの広域交付
住民基本台帳に記録されている者は，その者が記録されている住民基本台帳を備える市町村の市町村長（以下「住所地市町村長」という。）に対し，自己又は自己と同一の世帯に属する者に係る住民票の写しの交付を請求することができる（法１２条１項）ほか，住所地市町村長以外の市町村長に対し，住基カード又は総務省令で定める書類（旅券又は運転免許証等）を提示して，住民基本台帳を備える市町村以外の市町村長に対し，住民票の写し（ただし戸籍の表示，選挙人名簿の登録，国民健康保険の被保険者の資格に関する事項，介護保険の被保険者の資格に関する事項，国民年金の被保険者の資格に関する事項，児童手当の受給資格に関する事項，米穀の配給に関する事項などの記載を省略したものに限る。）の交付（以下「広域交付」という
。）を請求することができる（法１２条の２第１項，規則５条２項）。
住民票の写しの広域交付の請求があった場合には，住基ネットを通じて，①請求を受けた市町村長（以下「交付地市町村長」という。）は，住所地市町村長に対し，政令で定める事項（住民票の写しの広域交付の請求があった旨，請求者の氏名及び住民票コード，請求者及び請求者と同一の世帯に属する者のうち住民票の写しに記載する者，世帯主及び世帯主との間柄並びに住民票コードの記載の請求の有無）を通知し，②住所地市町村長は，交付地市町村長に対し，政令で定める事項（氏名，生年月日，性別，住民となった年月日，住所及びその住所を定めた年月日。なお世帯主及び世帯主との間柄又は住民票コードの記載の希望があったときにはこれらの事項も含む。）を通知することとされている（法１２条の２第２項，第３項，第５項，住基法
施行令（以下，条文を引用する場合は，単に「令」と表示する。）１５条の２）。
サ 転入転出特例
転出をする者は，あらかじめ，その氏名，転出先及び転出の予定年月日を市町村長に届け出なければならず，転入の届出の際には，転出証明書の添付が必要である（法２４条，２２条２項，令２３条１項）が，住基カードの交付を受けている者が，付記転出届（転出届であって，当該届出に係る書面に法２４条の２第１項の手続による届出をする旨が付記されたものをいう。）をした場合には，最初の転入届については，転出証明書の添付が不要となる（法２４条の２第１項，令２４条の２。以下「転入転出特例」という。）。
転入転出特例による転入届があった場合には，住基ネットを通じて，①当該転入届を受けた市町村長（以下「転入地市町村長」という。）は，その旨を付記転出届を受けた市町村長（以下「転出地市町村長」という。）に対して通知し，②転出地市町村長は，転入地市町村長に対して，政令で定める事項（転出前の住所，転出先及び転出の予定年月日，国民健康保険の被保険者である者についてはそ

の旨及びその者が退職被保険者等である場合にはその旨，介護保険の被保険者である者についてはその旨，国民年金の被保険者である者については，国民年金の被保険者の種別並びに国民年金手帳の記号及び番号並びに児童手当の支給を受けている者についてはその旨）を通知する（法２４条の２第３項ないし５項，令２４条の４）。

シ　改正法の施行経緯の概略

（ア）　改正法附則１条２項（個人情報の保護に万全を期するため所要の措置を講ずること）は公布の日（平成１１年８月１８日）から施行された。

（イ）　改正法附則１条１項ただし書２号所定の指定情報処理機関の指定，本人確認情報の処理及び利用等の準備行為に関する規定等は，平成１１年政令第３０２号により，平成１１年１０月１日から施行された。

（ウ）　住民票コードの記載及び本人確認情報の保存・提供に関する規定等は，平成１３年政令第４３０号により，平成１４年８月５日から施行された（いわゆる住基ネットの第１次稼働）。

（エ）　改正法附則１条１項ただし書３号所定の転入転出特例，住民票の写しの広域交付及び住基カードの交付に関する規定等は，平成１５年政令第２０号により，平成１５年８月２５日から施行された（いわゆる住基ネットの第２次稼働）。

(3)　名古屋市における住基ネット構築の取組

ア　名古屋市における住基ネットへの接続状況等

名古屋市においては，平成２年に導入した既存住基システム（既存の住民基本台帳電算処理システムをいうが，名古屋市においては「住民基本台帳サブシステム」がこれに該当する。乙１２）や既存住基端末（既存の住基システムにおける端末機器をいう。）などをもって既存ネットワークが構成されていたところ，同ネットワークは，ファイアウォールを介して中間サーバと，中間サーバは，ファイアウォールを介して名古屋市のＣＳとそれぞれ接続され，さらに，名古屋市のＣＳは，ファイアウォール及び交換装置を介して他の県内市町村のＣＳ，愛知県サーバ，他の都道府県サーバ，他の都道府県内のＣＳ，全国サーバと接続されて住基ネットが構築された。なお，名古屋市の既存ネットワークは，ファイアウォールを介してインターネットに接続している。

上記接続状況のイメージ概略図は，別紙３記載のとおりである（乙４８）。

イ　住基カード原盤に関する公金支出等

（ア）　平成１５年度

名古屋市は，住基カード４万枚の交付を予定し，同市の平成１５年度一般会計補正予算に住基カードの原盤（以下「住基カード原盤」という。）の調達経費として４２００万円を計上した（乙２７の１・２）。

名古屋市市民経済局長は，助役以下代決規程（平成１２年名古屋市達第４０号）７条１項，別表第１財務関係５号に基づき，平成１５年５月２日，住基カード原盤２万枚の購入を決定した。

Ｐ１市長は，同年６月５日，住基カード原盤２万枚の納入について一般競争入札に付したところ，同年７月１６日の開札の結果，凸版印刷株式会社（以下「凸版印刷」という。）が落札した。そこで，Ｐ１市長は，同月２２日，名古屋市を代表して，凸版印刷との間で，住基カード原盤２万枚を９４５万円（消費税含む。）で購入する旨の契約を締結し，凸版印刷は，同年８月１５日までに住基カード原盤１万枚を，同年９月１２日までに，同１万枚をそれぞれ納入した（甲２，乙１，２８，４３）。

名古屋市市民経済局地域振興部区政課長Ｐ２は，平成１６年１月５日，上記購入代金９４５万円を支出するよう命令し，名古屋市収入役は，同月２２日，凸版印刷に対し上記購入代金を支払った（以下「本件公金支出」という。乙２８）。

（イ）　平成１６年度

名古屋市は，平成１６年度一般会計予算に住基カードの調達経費として６３０万円を計上した（乙２９）。

ウ　住基カード発行用端末機賃借に関する公金支出等

（ア）　平成１５年度

名古屋市は，平成１５年度一般会計予算に住基カード発行用端末機の

賃借料（リース料）として２８５１万６２８４円を計上した（乙３０）。
名古屋市は，平成１５年５月１日，住基カード発行用端末機器を月額１８万８３７０円で賃借する旨の賃貸借契約を締結し，同年８月１日，さらに住基カード発行用端末機器を月額２１５万５３９８円で賃借する旨の賃貸借契約を締結し，これら端末機械の引渡しを受けて，使用を開始した（乙３２の３，３５の３，弁論の全趣旨）。
名古屋市収入役は，市民経済局企画経理課長の支出命令に基づき，平成１５年６月３０日から平成１６年４月３０日までの間に，上記賃料（リース料）合計１９３１万５２５４円を支払った（乙３２ないし４２の各１ないし３，弁論の全趣旨）。
（イ） 平成１６年度
名古屋市は，平成１６年度一般会計予算に住基カード発行用端末機の賃借料（リース料）として２８１２万５２１６円を計上した（乙３１）。
(4) 監査請求
原告らを含む名古屋市の住民２４０人は，平成１５年７月１７日ないし同月２４日，名古屋市監査委員に対し，地方自治法２４２条１項に基づき，平成１５年度予算に計上された住基カードの作成経費４２００万円の支出の差止めのための措置，及び，仮に作成経費が支払われている場合には，その返還のための措置を，それぞれ講ずるように請求した（甲１）。
これに対し，名古屋市監査委員は，同年８月１４日付けで，上記住民らに対して，住基カードの作成経費の支出は，地方自治法２４２条１項所定の違法・不当な公金の支出には当たらず，措置する必要は認められない旨の監査結果を通知した（甲２）。
(5) 本訴提起
原告らは，平成１５年９月１０日，本訴を提起した。
２ 本件の争点
本件公金支出その他住基カードの交付に関する支出，契約の締結及び履行並びに債務負担行為（以下「本件公金支出等」という。）は，違法な公金支出に該当するか。具体的には以下の各点が争点となる。
(1) 住基ネット及び住基カードは，国民のプライバシー及び個人の尊厳を侵害する点で憲法１３条に違反するか。
(2) 法３６条の２及び改正法附則１条２項所定の措置を講ずることが，改正法の施行条件であるか。
(3) 住基ネット及び住基カードは，個人情報の漏えいの危険性がある点で，法３６条の２及び改正法附則１条２項に違反するか。
(4) 住基ネットはほとんど効用がないから，住基カードの発行に公金を支出することは，最少経費・最大効果を定めた地方自治法２条１４項及び地方財政法４条１項に違反するか。
３ 争点に対する当事者の主張
(1) 争点(1)（住基ネット及び住基カードは，国民のプライバシー及び個人の尊厳を侵害する点で憲法１３条に違反するか）について
（原告らの主張）
ア プライバシー権が憲法１３条によって保障されること
プライバシー権は，憲法１３条によって保障される憲法上の権利である。このことは，憲法学説上ほぼ異論がないほか，最高裁判所が，プライバシー権の用語を直接的に使用したことはないものの，しばしば憲法１３条に言及しつつ，プライバシーや私生活上の自由の法的保障を承認し，公法上及び私法上の保護を認める判断を下していることからも明らかである。
イ 住基ネットは国民の個人情報を一元的に管理する点で憲法１３条に違反すること
従来，行政の各分野において行政効率を高めるために，その目的ごとに別の番号（以下「限定番号」ともいう。）が付されていたが，これは個人のプライバシーと行政効率化の要請のバランスをとったものとして一定程度許容され，国民の理解が得られてきた。
しかし，国は，改正法に基づき，日本在住の国民全員に対して１１けたの数字から成る住民票コードを付した。この住民票コードは，すべての行政分野に利用できる番号（以下「共通番号」という。）であるという点で，運転免許証番号や年金番号等の限定番号とは質的に異なっており，国民総背番号制の基礎となるも

のである。国は，住基ネット稼働により，住民の氏名，性別，生年月日，住所，住民票コード及びそれらの変更履歴の６情報を，市区町村から都道府県のサーバ，指定情報処理機関を通じて取得することができるようになったが，氏名，生年月日よりも検索機能においてはるかに優れた住民票コードをマスターキーとして利用することにより，「名寄せ」（正確には「番号寄せ」）を行い，国民の個人情報を一元的に管理・支配するこ
とが可能となる。

現に，行政機関の保有する個人情報の保護に関する法律（平成１５年法律第５８号。以下「行政機関個人情報保護法」という。）８条２項は，法令の規定する事務の利用のために相当な理由があると行政機関が認めれば，その保有する情報の目的外使用や他の行政機関等への提供を許容している。

このような国家による個人情報の一元的管理によって，原告らのプライバシー及び個人の尊厳を侵害されることはいうまでもなく，これを可能とする住基ネット自体が，憲法１３条に違反するものである。

なお，住基ネットがプライバシーを保障した憲法１３条に違反することは，私立大学の学生の学籍番号，氏名，住所及び電話番号を記載した参加者名簿を大学が警察署に提供した事案において「プライバシーに係る情報として法的保護の対象となり，本人の同意を得ずに警察に提供した大学の行為はプライバシーを侵害するものとして不法行為を構成する」旨判断した最高裁判所平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁からも明らかである。

ウ　被告の主張に対する反論

（ア）　被告は，住民票コードは，住民票に対して付せられたものであって，国民に対して付せられたものではない旨主張する。しかし，住民票コードが国民一人一人に対し，個人を識別するために（あるいは本人確認のための道具として）付せられたことは多言を要しない。被告の主張は，本件裁判及び全国で係属中の住基ネット裁判が問題としている共通番号を国民全員に強制的に付することにより国民を管理する住基ネットの本質論を回避するためのものにほかならない。

（イ）　また，被告は，住基ネットは地方公共団体共同のシステムであって，国の下に全国民の個人情報を一元管理するものではない旨主張するが，地方公共団体共同のシステムという言葉は実態とかけ離れており，住民票コード付きの個人情報が指定情報処理機関を通じて国に流れる以上，国による一元管理，国民の管理・監視が可能となる。

エ　小括

住基カードは住基ネットを不可欠の前提とするものであるから，住基ネットが憲法１３条に違反する以上，市町村長が住基カードを発行することも憲法１３条に違反するのであって，本件公金支出等は，違法な公金の支出に当たる。

（被告の主張）

原告らの主張は争う。

原告らの主張する「名寄せできるようにすることにより，国民の個人情報を国家が一元的に管理」する状態が具体的にどのような状態を指すのかは不明であり，また，それがいかなる内容の法益をどのように侵害するのか具体的に主張されていないので，上記主張は，それ自体失当である。

住基ネットは，本人確認情報のみを管理する地方公共団体共同のシステムであって，国のもとに全国民の個人情報を一元管理するものではなく，国家による国民の強権的な管理・監視体制を築くものでもない。

また，住民票コードを住民票に付した理由は，住基ネットというコンピュータネットワークを構築するに当たり，行政において個人の確実な特定を可能とし，かつ迅速かつ効率的な検索を実現するために不可欠であるからである。すなわち，氏名・住所を用いてアクセスする方法には，①各市町村において使用漢字や表記などの記載方法が異なる可能性があること，②処理の際に大きな負荷がかかり，効率性が失われること，③氏名や住所が同一の場合があること，④氏名や住所は変更されることがあり，それに備えて過去の履歴をすべて保存するのは効率的でないことなどの問題がある。

そして，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することができ（法３０条の３），民間部門がこれを利用することは禁止されており（法３０条の４３，４４条），行政機関がこれを利用する場合も，目的外利用の禁止，告知要求制限等の規定によって利用が制限されている（法３０条の３４，同条の４２，同条の４３）から，国の機関等と他の国の機関等との間で住民票コー

ドを利用してデータマッチングすることは禁止されている。
したがって，仮に，プライバシー権が憲法１３条で保障された人権であるとしても，住基ネットが憲法１３条に違反する旨の原告らの主張は，理由がない。
(2) 争点(2)（法３６条の２及び改正法附則１条２項所定の措置を講ずることが，改正法の施行条件であるか）について
（原告らの主張）
ア 法３６条の２及び改正法附則１条２項所定の措置は法３０条の４４を含む改正法の施行条件であること
法３６条の２第１項は，「市町村長は，住民基本台帳……に関する事務の処理に当たっては，住民票……に記載されている事項の漏えい，滅失及びき損の防止その他の住民票……に記載されている事項の適切な管理のために必要な措置を講じなければならない。」と規定し，２項は，これを事務の委託を受けた者にも準用している。また，改正法附則１条は，１項本文において「この法律は，公布の日から起算して３年を超えない範囲内において政令で定める日から施行する。」とした上で，さらに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。」と規定している。これらは，国会審議において，国民総背番号制，プライバシーの侵害及びセキュリティ等の不安
が強く指摘され，その対応として特に定められた重要な規定である。このような立法経緯及び附則が附帯決議と異なり法律そのものであることにかんがみると，これらは法３０条の４４を含む住基ネット関係の改正法の施行条件と解すべきであって，これを充足していない限り，同規定は施行されてはならない。
イ 施行条件を充足していないこと
（ア） 被告は，行政機関個人情報保護法をもって所要の措置が講ぜられたと主張するが，住基ネット第１次稼働の段階では，同法が成立していないから，施行条件を充足していないことは明らかである。
（イ） また，平成１５年５月に同法が成立したものの，本件公金支出時点ではいまだ施行されていない（平成１７年４月１日施行）上，同法には，①利用目的の特定（３条１項），利用目的の変更（３条３項），目的外利用及び他機関への提供（８条２項）について行政機関が広い裁量を有していること，②人種，民族，思想，信条，宗教，犯罪歴及び社会的差別の対象となる社会的身分などのいわゆるセンシティブ情報の収集制限がないこと，③二つ以上の記録システムに含まれる複数の情報をコンピュータでデータマッチングすることを禁止する規定がないこと，④制度の運営を監督・監視する第三者機関の規定がないことなどの問題点があることから，同法はいわば「行政機関による個人情報利用促進法」であるとの批判を受けており，個人情報の
保護に万全を期すための措置が講ぜられているとはいえず，住基ネット関係の規定の施行条件はいまだに充足されていない。
ウ 小括
したがって，現時点においても法３０条の４４を含む住基ネット関係法規の施行条件は満たされておらず，本件公金支出等は，法３６条の２及び改正法附則１条２項に反して違法である。
（被告の主張）
原告らの主張は争う。
ア 法３６条の２及び改正法附則１条２項は，法３０条の４４を含む改正法の施行条件ではないこと
法３０条の４４を含む住基ネット関係法規が，法３６条の２及び改正法附則１条２項を施行条件とする旨の明文規定は一切存在しない。むしろ，改正法は，同法附則１条１項本文の規定により，公布の日から起算して３年を超えない範囲内において政令で定める日等から施行することとされており，法律上，個人情報保護法案が成立すると否とにかかわらず，法令で定められている日に施行することが義務付けられているから，個人情報保護法制が整備されることを施行条件としていないことは明白である。
イ 所要の措置が講じられたこと
なお，改正法附則１条２項は，国会審議の過程において，民間部門をも対象とした個人情報保護に関する法整備を含めたシステムの整備の必要性について幅広い議論がされ，住基ネットについては，改正法において十分な個人情報保護措置が講じられているものの，なお漠然とした不安，懸念が残っていることを踏ま

え，議員修正によって加えられたものであるところ，政府は立法機関でなく，自ら法律を制定することができないから，同項にいう「所要の措置」とは，政府において法律案を検討，作成し，国会へ提出することを意味するものと考えられ，政府としては行政機関個人情報保護法案を国会に提出したことにより所要の措置を講じたものと考えられる。

したがって，原告らのこの点に関する主張は失当である。

(3)　争点(3)（住基ネット及び住基カードは，個人情報の漏えいの危険性がある点で，法３６条の２及び改正法附則１条２項に違反するか）について

（原告らの主張）

法３６条の２は，地方公共団体の首長に対して個人情報の安全管理義務を課しており，改正法附則１条２項は，政府に対して個人情報の保護に万全を期するための所要の措置を講ずることを義務付けているところ，現状の住基ネット，名古屋市の住基ネット接続方法等，住基カードには情報漏えいを防止する対策が不十分である点があり，上記の要請が全うされていない。

このようなセキュリティに問題がある状況で，住基カードを発行することは法３６条の２及び改正法附則１条２項に反して違法であり，そのための公金支出等も違法である。

ア　運用関係者による情報漏えいを防止すべき措置について

(ア)　刑罰や監督による不正行為の抑止効果

a　刑罰

被告は，住基ネットの運用関係者に秘密保持義務を課し，違反した者には通常の公務員の守秘義務違反よりも重い刑罰を科していると主張する。

しかしながら，刑罰の加重によって不正行為を防止する効果を期待することはほとんどできない。なぜならば，第１に，最近の個人情報の流出事件の多くは過失によるものであるにもかかわらず，刑罰の対象となるものは故意犯に限定されており，第２に，故意犯に対する刑罰として２年以下の懲役，１００万円以下の罰金では抑止効果がないからである。

b　報告・立入検査等の監督

被告は，上記罰則のほかに，指定情報処理機関は，総務大臣，都道府県知事から報告・立入検査等の監督を受けることを挙げる。

しかしながら，住基ネットのコンピュータシステムそのものは極めて専門的であり，監督する側にその知識がなければ監督できないのが実情であり，総務大臣や都道府県知事による監督ではその効果は期待できない。

(イ)　アクセスログの定期的解析と調査

被告は，定期的にアクセスログの解析を行い，不正使用の兆候を検出したときは必要な対策等が実施されると主張する。

しかしながら，コンピュータ通信は，その性質上，即座に情報が流失するものであり，兆候を発見したときでは既に手遅れである。また高度の技術を持つハッカーの場合，アクセスログも残さないので，侵入されたことすら気づかないことがあるといわれている。

(ウ)　住民に対する本人確認情報提供状況の開示

被告は，準備が整った都道府県から順次，個人に対しても当該個人の本人確認情報提供状況の開示をすることにより，不正使用の端緒が判明するようにすると主張する。

確かに，この制度は，事後的な個人情報の不正使用に関する端緒となり得る。しかしながら，これとても既に流失した後の事後的なものであることに変わりはなく，流失の防止策としては不十分である。

(エ)　住民票の写しの広域交付における不正防止

被告は，一定時間に一定数以上の住民票の写しの広域交付要求があった場合は，これを停止する措置が講じられていると主張する。

しかしながら，紙媒体の住民票の写しを大量に不正請求することは考えにくく，それよりもデジタル情報の不正取得が懸念されるから，上記措置が働く場面はほとんどないであろう。

イ　セキュリティ対策について

(ア)　重要な情報の分散化への逆行

コンピュータの専門家によると，内部者の故意過失による流失，外部からの侵入を防止する手だてをいかに施したとしても，これらを防止することはできないとのことである。とするならば，重要な情報の流失による被害を最小限に食

い止めるには，近時の欧米等のＩＴの考え方に見られるように，情報を堅牢なシステムの中に集中させて防護するのではなく，最初から情報を集中化させず，分散化することが必要である。住基ネットは，このような傾向に逆行しており，古い考えに基づいている。

（イ） 保有情報の限定

被告は，保有情報が６情報に限定されているとして，センシティブな個人情報が住基ネット上で流れることはないと主張する。

しかし，住基ネット上に流れるのは，氏名，生年月日，性別及び住所の４情報だけでなく，住民票コードが含まれている上，現在ＤＶ（ドメスティック・バイオレンス），ストーカー，性同一性障害者などへの配慮から戸籍事務のオンライン化，戸籍事務取扱準則制定標準の改正の検討がなされているように，４情報だけだから大丈夫という軽率な考えは否定されている。

ましてや，転出転入手続の特例の場合は，６情報の外，さらに世帯主との続柄，戸籍の表示，転出前の住所，転出先及び転出の予定年月日並びに国民健康保険，介護保険，国民年金及び児童手当の支給に関する情報も一緒にネット上に流れるのであり，システム自体が危険な設計になっている。

（ウ） 本人確認情報の利用及び提供の制限

被告は，利用目的を法律で限定しており，法改正による以外に利用事務の追加はできないとする。

しかし当初９３事務だけであったのが，住基ネット第２次稼働前に２６４事務に拡大されており，また２６４事務だけでは到底住基ネットを稼働させた実益が発揮できず，今後も法律による追加がなし崩し的になされることが予想される。

（エ） 住民票コードの利用制限

被告は，住民票コードは住民の申請で変更できるほか，民間部門が住民票コードを利用することが禁止されていると主張する。

しかし，住民票コードを変更しても，変更履歴の情報が付くので追跡することができ，変更したことにはならない。また，民間部門が住民票コードの告知を要求することは禁止されているものの，任意に提供を受けることは禁止されていない。したがって，住民が民間部門との契約の必要から，「任意に提供する」ことを迫られることがあり得る。そのほか，民間部門が，住民票コードをデータベース化して他に提供することが予定されるものを構築することは禁止されているが，自社の使用する目的でデータベース化することは許されている。

なお，被告は，国の機関等と他の国の機関等との間で住民票コードを利用してデータマッチングすることは禁止されていると主張するが，その根拠は明らかではない。

ウ 外部の侵入防止対策について

被告は，住基ネットにおいては，外部の侵入防止対策として物理的なセキュリティ対策や，専用回線を使用し電気通信回線経由による侵入に対する対策等がとられているところ，東京都品川区の機器への模擬攻撃によっても侵入は成功せず，その安全性が確認されていると主張する。

しかしながら，平成１５年９月ないし１１月に長野県で行われた侵入実験（以下「長野県侵入実験」という。）の結果が示すように，セキュリティ対策が無力であることが実証されている。被告の主張するように，住基ネットの安全性が確認されているのであれば，国は，長野県が提唱している合同侵入実験を行うべきである。

また，専用回線を使用しているとの総務省の説明は虚偽であり，この点を指摘されるや，総務省は物理的専用回線ではないが「論理的に他回線と完全に隔離された専用回線である。」と言い換えている。

エ 住基カードのセキュリティ対策について

（ア） 非接触型カードの危険性

住基カードは非接触型カードであるから，保有者本人が知らないうちに情報を読み取られる，あるいは改ざんされるなどの危険性が存する。

（イ） 住基カードの独自利用サービスの記録情報の制限

被告は，住基カードの中に様々な個人情報が蓄積されることはないと主張する。そうであれば，多目的サービスの実行ができなくなり，矛盾している（例えば「事故，急病等で救急医療を受ける場合，あらかじめ登録した本人情報」はどこに登録されるのかが説明できない。）。

オ　名古屋市におけるセキュリティ対策について

住基ネットの第２次稼働で，氏名，生年月日，性別，住所のほかに，本籍，世帯主，続柄，介護保険などのセンシティブな情報が住基ネット上を流れることになるが，名古屋市は政令指定都市の中で唯一，住基ネットが庁内ＬＡＮを経由してインターネットと接続しており，セキュリティに重大な危険性がある。

（被告の主張）

原告らの主張は争う。

住基ネット及び住基カードのセキュリティが脆弱で個人情報漏えいの危険性があることは，原告らが主張立証責任を負っているところ，本件において，住基ネット及び住基カードのセキュリティが脆弱で個人情報漏えいの危険性があることが明らかになったとは到底いえない。

すなわち，住基ネット及び住基カードに高度かつ十分なセキュリティ対策が講じられていること，名古屋市においてもセキュリティ基準以上の十分なセキュリティ対策が講じられていることは，下記に詳論するとおりである。

ア　運用関係者による情報漏えいを防止すべき措置について

住基ネットにおいては，以下のとおり本人確認情報保護措置が講じられており，運用開始以来，不正行為等は生じていない。

（ア）　重い刑罰や監督による不正行為の防止

住基法や行政機関個人情報保護法は，住基ネットに係る事務の関係者や本人確認情報の提供を受ける行政機関の関係者に対し，知り得た本人確認情報に関する守秘義務を課し（法３０条の１７第１項，第２項，同条の３１第１項，第２項，同条の３５第１ないし第３項，行政機関個人情報保護法５３条ないし５５条），その違反には重い刑罰を科する旨を定める（法４２条は，国家公務員法や地方公務員法よりも重い２年以下の懲役又は１００万円以下の罰金を定めている。）ほか，指定情報処理機関に対する監督措置（総務大臣の権限について，法３０条の１６，同条の１８，同条の１９，同条の２２第１項，同条の２３第１項，同条の２５，委任都道府県知事の権限について同条の２２第２項，同条の２３第２項）を定め，情報漏えいや不正な目的
での提供等が生じないような措置が講じられている。

（イ）　照会条件の限定

本人確認情報の検索に際して，①即時提供の場合，「住民票コード」，「氏名及び住所」又は「氏名及び生年月日」を入力しないと本人確認情報の提供を受けられない仕組みとなっており，②一括提供の場合も，①と同様に，照会元から送られてきた「住民票コード」，「氏名及び住所」，「氏名及び生年月日」等のファイルに，都道府県サーバ又は指定情報処理機関サーバにおいて，本人確認情報を追記して照会元にファイルを返送するなどの措置が講じられている。

このように，担当者が当該個人情報を容易に検索できないような措置が講じられている。

（ウ）　操作者識別カード認証によるアクセス制御

本人確認情報は，ＣＳ，都道府県サーバ及び全国サーバ内に保存されており，端末機には存在しないところ，住基ネットにアクセス権限のない者がアクセスできないようにするため，端末機の住基ネットアプリケーションを起動し，本人確認情報データベースにアクセスするには，操作者識別カードと端末機との間で相互認証を要求しているから，アクセス権限のない職員や外部の者が本人確認情報データベースへアクセスすることはもちろん，住基ネットアプリケーションを起動することもできない。

その上，操作者識別カードの種別により，システム操作者が住基ネットの保有するデータ等へ接続できる範囲を限定している。

（エ）　アクセスログの定期的解析と調査

指定情報処理機関は，定期的に全国サーバのアクセスログの解析を行い，万一不正使用の兆候を検出した場合，緊急時対応計画等に基づき必要な連絡，対策等が実施される。また，市町村及び都道府県も，指定情報処理機関に対し，住民のアクセスログの解析要請を行うことができる。

（オ）　住民に対する本人確認情報提供状況の開示

都道府県サーバ及び全国サーバに，本人確認情報提供状況の開示用データ（提供先ないし検索元，提供年月日，利用目的等）を生成する機能を実装することにより，都道府県は，平成１５年１０月１日から，本人確認情報提供状況の開示用データの保存を開始し，同年１１月以降，順次，それぞれの個人情報保護条例

に基づく住民からの請求があった場合，その開示を行うこととした。
このように，当該個人に対しても，本人確認情報の提供状況を明らかにすることにより，不正使用の端緒が分かるようにしている。
（カ） 住民票の写しの広域交付における不正防止
交付地市町村の特定の操作者識別カードから一定時間に多量の住民票の写しの広域交付要求があった場合は，住所地市町村において，システム上，広域交付を停止する措置が講じられている。
（キ） 担当職員に対する教育・研修
国は，市町村の住基ネット担当者を対象としたセキュリティ研修会を，また，本人確認情報の提供を受ける国の機関等の担当職員向けの研修会を，それぞれ適宜に実施している。
イ セキュリティ対策が講じられていること
住基ネットについては，体系的な制度面，技術面及び運用面における様々な措置が講じられることにより，高いセキュリティが確実に確保されている。
（ア） 制度面からの対策
ａ 保有情報の限定
都道府県・指定情報処理機関が保有する情報は，法律上，前記４情報，住民票コード及びこれらの変更情報の本人確認情報に限定されている（法３０条の５第１項，令３０条の５，規則１１条）。
また，住民票の写しの広域交付，転入転出特例等の際には，市町村から市町村へ続柄等の情報も送信されるが（令１５条の２第２項及び２４条の４），これら情報送信は，すべて任意の二つのＣＳ間で直接行われるので，当該通信が都道府県サーバや全国サーバを通過したり，そこに保有されることはない。
ｂ 本人確認情報の利用及び提供の制限
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を法律で具体的に規定し，これを限定している（法３０条の６，同条の７第３項から第６項まで，同条の８及び別表）。なお，法３０条の６，同条の７第４項２号，第５項２号，第６項２号の場合は，具体的な利用事務等は条例において規定されるが，これは法律の委任に基づくものであり，法律と民主的意義において同等であることなどから，何ら問題はない。
また，国の機関等が提供を受ける場合は，法改正による以外に利用事務の追加はできない。
さらに，本人確認情報の提供を受ける者についても，目的外の利用又は提供が禁止され（法３０条の３４），都道府県知事及び指定情報処理機関も，法律の規定によらない本人確認情報の利用及び提供が禁止されている（法３０条の３０）。
ｃ 責任体制の確立
住基ネットの各機器に関する市町村，都道府県，指定情報処理機関の管理責任の範囲を明確化し，それぞれ責任を持ってセキュリティを確保しているほか，総務省，指定情報処理機関，都道府県及び市町村において，セキュリティに対する対策や監督措置等が講じられている（法３０条の９，同条の１１第７項，同条の１５，同条の１８，同条の２２，３１条）。
ｄ 住民票コードの利用の制限
諸外国では，特定の番号を複数の行政分野のみならず，民間においても広く活用している国があるが，我が国においては，住民票コードの民間利用の在り方等について検討した結果，以下のとおり，これを厳しく制限することとした。
（ａ） 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（法３０条の３）。
（ｂ） 民間部門の住民票コード利用を禁止している。特に，民間部門が契約締結時の住民票コード告知要求及び住民票コードの記録されたデータベースで他に提供されることが予定されているものの構築に対して，都道府県知事は中止勧告や中止命令を行うことができる。都道府県知事の中止命令に違反した者は，１年以下の懲役又は５０万円以下の罰金が科せられる（法３０条の４３及び４４条）。
（ｃ） 行政機関が住民票コードを利用する場合も，目的外利用の禁止，告知要求制限等の規定により利用が制限（法３０条の３４，同条の４２及び同条の４３）されており，国の機関等と他の国の機関等との間で住民票コードを利用

してデータマッチングすることは禁止されている。

ｅ　各関係機関における緊急時対応計画の策定

セキュリティ基準においては，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，削除及び改ざん等（以下「漏えい等」という。）の危険が具体的に発生した場合には，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。具体的な応急的な措置として，市町村長又は都道府県知事は，住基ネットとの切断等の措置を講ずることができ，不正アクセス等が発生した場合にも，それぞれの緊急時対応計画に基づき適切な対応がなされる。

（イ）　外部からの侵入防止対策その１（物理的なセキュリティ対策）

セキュリティ基準において，建物等への侵入の防止等，重要機能室の配置及び構造，入退室管理，磁気ディスク，構成機器及び関連設備等，データ・プログラム・ドキュメント等の管理等，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ネットワークにおける対策については，「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表（チェックリスト）」に基づく市町村の自己点検と，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・助言によって，対策の強化・徹底が図られている。

（ウ）　外部からの侵入防止対策その２（電気通信回線経由による侵入に対する対策）

①ＣＳ，都道府県サーバ及び全国サーバ間の通信は，すべて専用回線及び専用交換装置で構成されたネットワークを介して行い，また，全国サーバと国の機関等サーバとの間は，専用回線又は磁気媒体でデータ交換を行うことにより，論理的な閉鎖的ネットワークが実現されており，②暗号技術評価委員会において安全性が確認されている公開鍵方式により，サーバ間で相互認証を実施し，また，通信が終われば廃棄される共通暗号鍵を使用した暗号通信を実施し，③住基ネットの通信プロトコル（ネットワークを介してコンピュータ同士が通信を行う上での約束ごとの集合）は汎用的なプロトコルを使用せず，独自プロトコルを使用し，また，必要な箇所に指定情報処理機関監視ファイアウォールを設置して，インターネットで用いられるプロトコル
の通過を遮断し，④住基ネット全体で徹底したコンピュータウィルス・セキュリティホール対策を実施し，⑤指定情報処理機関監視ファイアウォールやＩＤＳ（侵入検知装置）を設置し，不正な通信の厳重な遮断と２４時間常時の監視を行い，⑥ソフトウェアの統一による住基ネット全体の高度なセキュリティ確保が実現されている。

（エ）　外部監査等によるセキュリティの確保

ａ　外部監査による市町村のセキュリティ確保

指定情報処理機関と総務省が作成したチェックリストに基づき，市町村は，平成１５年１月ないし２月，セキュリティ対策の自己点検を実施した。上記自己点検の結果を踏まえて，総務省は，平成１５年５月１３日，住基ネット担当課長会議を開催し，この点検結果を踏まえて，都道府県において，市町村に対し必要な技術的指導を行うことを要請した。

これを受けて，再度，市町村が自己点検を行ったところ，各都道府県，総務省及び指定情報処理機関における徹底した技術的助言，指導の実施，市町村の積極的な取組により，すべての市町村において，重要点検項目の７項目について満点を達成した。また，その他の項目についても，第２次稼働に向け，市町村のセキュリティ対策は大幅に向上した。

また，平成１５年１月から３月までの間，全国１０８団体の市町村において，外部監査法人によるシステム運営監査を実施し，その結果をセキュリティ強化に活用した。

ｂ　模擬攻撃によるセキュリティの確認・強化

平成１５年１０月１０日から１２日までの間にアメリカの監査法人クロウ社のセキュリティ部門により，ペネトレーションテスト（模擬攻撃）が実施された。その結果，住基ネットの主要な機器への侵入は成功せず，脆弱性も見いだせず，住基ネットの安全性が確認されている。

（オ）　住基カードのセキュリティ対策

住基カードについても様々な対策を講じることにより，セキュリティ

を確保している。

住基カードについて講じるべきセキュリティ対策等は，住基法及び住基法の規定に基づく「住民基本台帳カードに関する技術的基準」（平成１５年総務省告示第７０８号による改正後の平成１５年総務省告示第３９２号。以下「住基カードセキュリティ基準」という。）等により定められている。

ａ　住基カードのセキュリティ対策の基本的考え方

住基カードの交付は希望する住民に対してのみ行われ，携帯は義務付けられていない。

住基カード内の住基ネットで利用する領域から独立した空き領域を利用して，様々な住民サービスを提供することができるが，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され（法３０条の４４第８項），市町村が許可したサービス以外のサービスを提供できないシステムとなっている。また，どのような市町村独自サービスを受けるかについても，住民が選択できる。

また，住基カードの領域のうち市町村独自サービスに割り当てられた部分には，特に必要性がある場合を除き，利用者番号以外の個人情報を記録しないこととされており，カード内に，様々な個人情報が蓄積されることはない。さらに，住基ネットに係るアプリケーションのために割り当てられた領域は，市町村長その他の執行機関，都道府県知事その他の執行機関又は国の機関等に限り，かつ法に規定する事務又はその処理する事務であって，法の定めるところにより当該事務の処理に関し本人確認情報の提供を求めることができることとされているものの遂行のため必要がある場合のみ，活用することができる。すなわち，それ以外の場合に，住基カードに記録された住民票コードを利用することは一切禁止されている。

そのほか，住基カードの券面記載は，４情報のみに限定されており，さらに，希望する場合には，氏名のみのカードも選択できる（規則３８条）。

ｂ　技術面のセキュリティ対策

住基カードには，中央演算装置付きの半導体集積回路を組み込んだカード（以下「ＩＣカード」という。）を用いることとされ，これにより，①暗証番号の設定，②発行前の不正利用防止のための情報設定，③住基ネットと住基カードの相互認証，④アクセス権限の制御，⑤アプリケーションごとの独立性の確保，⑥外部から情報の読み取り又は解析ができない仕組みの確保（耐タンパー性），⑦券面の偽造等の防止，⑧国際標準化機構及び国際電気標準会議（以下「ＩＳＯ等」という。）の規格第１５４０８の認証及び同規格による評価を受けたカードを利用することなどの対策を講ずることが可能となり，高いセキュリティが確保されている。

ｃ　管理・運用面のセキュリティ対策

発行前の住基カードの適正管理，適切な交付，発行委託の制限，発行した住基カードの適正管理等を行っている。

（カ）　長野県侵入実験の結果について

原告らは，長野県侵入実験の結果が示すように，住基ネットのセキュリティ対策が無力であることが実証されていると主張する。

しかし，長野県侵入実験は極めて特異な条件の下で行われた上，同実験では，庁内外の端末からセキュリティ対策の不備を突いて庁内ＬＡＮへ不正に侵入できることは明らかになっておらず，また，ファイアウォールに対する攻略は成功していない。そのほか，既存住基サーバ内のデータが万一書き換えられたとしても，その情報は，自動的にＣＳに送信されるのではなく，別途送信する必要がある。

これらの事情に照らすと，①全国の市町村のいずれかのＣＳが乗っ取られて踏み台となり，住基ネット網を介して，他の市町村のＣＳや都道府県サーバ及び全国サーバ内にある本人確認情報が漏えいする危険，②全国の市町村にあるいずれかのＣＳに直接不正侵入されることによって，当該市町村の住民の本人確認情報が閲覧，改ざん等される危険，又は③全国の市町村にあるいずれかの既存住基サーバに不正侵入されて個人情報が書き換えられ，その情報が住基ネットを通じて送信される危険などは，長野県侵入実験によりその存在が判明したとはいえない。

したがって，長野県侵入実験により住基ネットのセキュリティ対策が無力であることが実証された旨の原告らの主張は，根拠を欠いた憶測にすぎず，かえって，外部のインターネットから庁内ＬＡＮへの侵入及び庁内ＬＡＮからＣＳセグメント（市町村設置ファイアウォールと指定情報処理機関ファイアウォールにより通信制御されたＣＳが設置されるエリア）への侵入にことごとく失敗したことか

ら，住基ネット本体の本人確認情報に対する危険性がないことが明らかになった。

ウ　名古屋市における独自のセキュリティ対策

名古屋市は，セキュリティ基準に基づく住基ネットのセキュリティ対策のほか，以下に述べるようなセキュリティ基準以上の名古屋市独自のセキュリティ対策を講じており，かつ，十分な個人情報の保護措置がとられているかについて，名古屋市個人情報保護審議会のチェックを受けている。

（ア）　制度面での対策

名古屋市は，住基ネットの運用に当たり，セキュリティを確保するための組織・体制について規定した「名古屋市住民基本台帳ネットワークシステムセキュリティ組織要綱」，住基ネットに係るアクセス管理，情報資産管理，本人確認情報管理，住基カード管理について規定した「名古屋市住民基本台帳ネットワークシステム管理要綱」及びサーバ等の障害により市民サービスが停止する場合や不正行為による脅威の可能性が高い場合等の緊急時の対応について規定した「名古屋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」をそれぞれ策定し，住基ネットのセキュリティの確保に努めている。

この「名古屋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」においては，住基ネットのセキュリティを侵犯する不正行為又は障害が発生し，それにより個人情報の保護が図れないと判断された場合には，名古屋市の判断で住基ネットとの切断を行うこととしている。

また，住基ネットの第２次稼働が平成１５年８月２５日に開始することや，名古屋市独自の事務においても個人情報の電子計算機処理が急速に進んでいる状況を踏まえ，個人情報の保護をより推進するため，同月２２日，名古屋市個人情報保護条例（平成８年名古屋市条例第２８号）の一部を改正し，職員や委託業務の従事者が個人情報を不正に取り扱った場合の罰則（１年以下の懲役又は５０万円以下の罰金）を設けるなど，職員による不正行為の防止を図っている。

（イ）　外部からの侵入防止対策

ａ　ＣＳに対する不正な通信の遮断及び監視

名古屋市では，住基ネット上の本人確認情報を既存住基システムで行われた異動処理に連携して即時に更新するため，住基ネットを既設ネットワークに接続しているが，既設ネットワークとＣＳとの間には市町村設置ファイアウォールを設け，既設ネットワーク側からの不正な通信を遮断する設定となっている。また，既設ネットワークと市町村設置ファイアウォールの間には，住基ネットに必要なデータのみを蓄積した中間サーバを設置するとともに，当該中間サーバと既設ネットワークの間にもファイアウォールを設置し，セキュリティ基準に定められた以上の措置を講じている。

なお，ファイアウォールについては，毎日定期的にログの内容を確認し，不正な通信が行われていないかを監視している。

ｂ　インターネットとの接続に係るセキュリティ対策

セキュリティ基準では，住基ネットと接続する既設ネットワークがインターネットに接続する場合については，「既設ネットワークの管理責任者は，既設ネットワークを外部ネットワークに接続するための手続，方法等を定め，接続及び運用に関する業務を総括的に管理すること」及び「既設ネットワークと外部のネットワークを接続する場合は，既設ネットワークと外部のネットワークとの間にファイアウォールを設置し，厳重な通信制御を行うこと」の二つの事項が規定されている。

このうち，前者については，「名古屋市行政情報ネットワーク運用管理要領」及び「名古屋市インターネット接続運用管理要領」を定め，総務局企画部情報化推進課長をネットワーク管理者として，行政情報ネットワークの運用管理を総括させている。また，後者については，行政情報ネットワークとインターネットとの間にファイアウォールを設置し，厳重な通信制御を行っている。

名古屋市は，さらに独自に上乗せした対策を行っている。まず第１は，ファイアウォールには，別途設置されているウィルスチェックサーバと連携して，ファイアウォールを通過する通信について，ゲートウエイ型のウィルスチェックを行わせており，発見したウィルスを駆除若しくはファイルごと削除を行っている。当然ながら，ウィルスのパターンファイルは，継続的に最新のものに更新させている。第２は，インターネットとの接続点周辺に，侵入検知装置を設置し，名古屋市行政情報ネットワーク（との接続点のファイアウォール）に入ろうと試みる通信を監視している。

（ウ） システム監査の実施

名古屋市では，専門的知識を有する監査法人に委託し，平成１５年２月，住基ネットのセキュリティ対策について独自にシステム監査を実施した。この監査では，住基ネットに係るセキュリティ管理体制等の整備状況及び技術面の妥当性について，関連資料の閲覧，ヒアリング，観察等の方法により検証が行われた結果，４２項目について改善の必要があるとの指摘を受けたため，速やかに所要の措置を講じた。さらに，同年５月に改めて改善の状況について監査法人による監査を行い，改善が進んでいることの確認を受けている。

また，名古屋市は，地方自治法２５２条の１９第１項に規定する指定都市であるため，区役所及び支所において本人確認情報を扱う事務を行う（法３８条）ことから，住基ネット第２次稼働後の平成１６年２月から３月にかけて，区役所及び支所２１か所において監査法人による監査を実施した。その結果，緊急かつ重大なセキュリティ上の問題はなく，よりセキュリティを高めるために検討の必要性があるとされた２３項目についても，速やかに所要の措置が講じられた。

（エ） 名古屋市情報あんしん条例の制定

名古屋市では，住基ネットの第２次稼働に際して，名古屋市個人情報保護条例を改正し，個人情報保護が適切に行われるよう取り組んできたが，平成１６年４月，名古屋市が保有する情報の保護及び管理に関して，基本的な仕組みを定めた名古屋市情報あんしん条例（平成１６年名古屋市条例第４１号）を施行した。これによれば，市長，行政委員会等の実施機関は，名古屋市の保有する情報システム及びネットワークに関して，人的，物理的及び技術的に情報保護対策を講ずることが義務付けられるほか，自己点検，システム監査を実施することが求められている。

エ 小括

以上のとおり，住基ネット及び住基カードについては，高度かつ十分なセキュリティ対策がとられており，個人情報の漏えいのおそれはない。したがって，住基カードの交付は，法３６条の２及び改正法附則１条２項に反するものではなく，そのための公金の支出が違法となることはないから，原告らの主張は根拠がない。

(4) 争点(4)（住基ネットはほとんど効用がないから，住基カードの発行に公金を支出することは，最少経費・最大効果を定めた地方自治法２条１４項及び地方財政法４条１項に違反するか）について

（原告らの主張）

地方自治法２条１４項は，最少経費・最大効果の公金支出を義務付けており，地方財政法４条１項も，目的達成のための必要最少限度の経費支出を義務付けているところ，これらの規定は，単なる訓示規定ではなく，地方自治体に対する法的義務を課したものである。そして，国が行うべき事業を自治事務の名の下に地方公共団体に責任と費用負担を押しつけることは，地方公共団体の自主性・自律性の尊重を定めた地方財政法２条２項や地方自治法１条の２第２項の精神に反するというべきである。

ア 住基ネット及び住基カードの効用は経費に見合わないものであること

住基ネットの立ち上げ費用は全国で８０４億９４００万円であり，今後その維持費用として毎年１９０億３６００万円を要するとされている。このような巨額の費用に比べ，住基ネット及び住基カードにはほとんど効用がない。このことは，住基カードの発行枚数が全国で３６万１４２０枚（人口比０．３パーセント。ただし，交付開始後１年経過時点），名古屋市で５３２９枚（同０．２パーセント。ただし，平成１６年８月末時点）にとどまっており，総務省が当面予想していた同３パーセントと比較して実に３３分の１でしかないことからも明らかである。このように，住基ネット及び住基カードは費用対効果の観点を全く欠くものである。

イ 住基ネット及び住基カードには効用が乏しいこと

（ア） 住民票の写しの広域交付について

被告は，交通・通信手段の発達により住民票写しの広域交付の要請が高まっているところ，住民票登録地以外の地域からでも住民票の写しの交付を受けられることが住基ネットのメリットであると主張する。

しかし，①そもそも，住民票の写しの広域交付を請求することは，一生の間にほとんどないこと，②住基カードを保有しなくても，運転免許証，パスポート，顔写真付きの住民カードなどにより本人確認を受ければ住民票の写しの広域

交付を受けられること，③現在でも，郵送によって（数日間の日数はかかるものの）同様の便益を受けることができることなどに照らすと，立ち上げ費用と維持費用を合わせて１０００億円近い経費のかかる住基ネットのメリットとしては薄弱である。

（イ） 転入転出特例について

被告は，住基カードを保有する者は転入転出特例を受けることができ，郵送によっては同様の効果が得られない旨主張する。

しかし，住基ネット及び住基カードがなくとも，今まで居住していた市町村に対し，「転出証明書郵送交付申請書」を郵送し，返信用封筒と切手を同封すれば，（数日間の日数はかかるものの）転出証明書の交付を受けることができ，それを転入市町村に提出すれば足りる。すなわち，１６０円の切手代を負担すれば，転入市町村に１回行くだけで済むことは住基カードを保有する場合と同じである。逆に，住基カードを利用する場合には，①まず住基カード交付申請と住基カードの受領をするために住民票登録地の市町村に出向く必要があり，②住基カードの交付を受けるため手数料（通常５００円）を負担し，③他の市町村への転居の際，転出市町村に付記転出届をし（郵送の場合には切手代８０円を負担する。），④転居者が転入市町村に転入届
を提出するという手続を要するから，住基カードを使用する場合の方が手間と費用とが余分にかかることになる（この点に対して被告は何ら反論しない。）。

しかも，住基カードは，発行する市町村から借りているにすぎないのであって，転居をする場合には，これを返還する必要があり（法３０条の４４第６項），手数料は無駄となってしまう。転入市町村で新たに住基カードの交付を受けようとすると，再度手数料が必要になる。

そして，実際の転居には，転出届及び転入届だけではなく，学校の転校届その他転出地でのいろいろな手続を要するのが通例であるから，住民票の移動の手続が簡易かどうかだけの議論は余り意味がない。

（ウ） 住民票の写し等の提出の不要化（住民の負担軽減・行政手続の簡略化）について

また，被告は，住民は住民票の写し，年金受給のための現況届，身上報告書等の提出の負担が解消されると主張する。しかし，住民票の写しの提出だけが省略されたところで，住民の負担はほとんど減らない（例えば，パスポートの申請手続では，他にも戸籍謄本や写真，ハガキ等の提出が必要である）。また，現況届は年金の受給者にとって問題となるにすぎないから，何故に生まれたばかりの赤ちゃんや年金の受給資格のない者を含めた全国民に対して住民票コードを付さなければならないのかが説明されていない。

（エ） 公的個人認証のサービスについて

被告は，利用者署名符号及びこれに対応する利用者署名検証符号を住基カードに記録することにより，公的個人認証サービスを受けることができるから，住基ネット及び住基カードは電子政府・電子自治体を実現するための基盤となると主張する。

確かに，電子政府等の実現のためには，インターネットを利用するときの本人確認（いわゆる「なりすまし」の排除）が必要である。

しかし，電子申請を希望する国民は全体の数パーセント程度にとどまる上，電子申請のために必要となる電子署名の認証は民間（例えば，日本認証サービス）によるものでも構わないとされている（ちなみに，外国人や法人は，公的個人認証を受ける余地はない。）から，住基カードが電子政府・電子自治体の実現のために必要であるとはいえない。

（オ） その他

そのほか，被告は，①市町村が条例で定める多目的利用に使うことができる，②本人確認が迅速にできる，③公的な身分証明書としても使うことができるなどと主張する。

しかしながら，①については，可能性を挙げているだけであって，現在，全国３２００余の市町村のうち室蘭市，水沢市，福光町，志雄町，福井市，掛川市，知多市，日南町，新見市，大牟田市，宮崎市の１１市町が条例を定めているにすぎない。また，名古屋市については，偽造，個人情報保護の観点から多目的利用をしていない。

そして，②については，その必要性はなく，③については，ＩＣを格納した高価な住基カードでなくとも，これまでの多くの市町村が発行する硬質紙な

いしプラスチック製の身分証明書で足りる。
ウ　電子政府の実現と住基ネットとの関係について
被告は，電子政府・電子自治体の実現のためには公的個人認証が必要であり，公的個人認証のためには住基ネットが必要であると主張する。
しかし，もともと電子政府・電子自治体の実現の構想と住基ネットが結びついていないことは，住基法改正法の成立時期が平成１１年であるにもかかわらず，被告が「住基ネットが平成１２年ころから電子政府・電子自治体の実現のための必要不可欠な制度として位置づけられた」と述べていることからも明らかであり，電子政府・電子自治体の実現の要請と住基ネットの必要性を強引に結びつける被告の主張は誤りである。
エ　小括
以上のとおり，住基ネット及び住基カードにはほとんど効用がなく，住基ネットの導入及び住基カードは費用対効果の観点を全く欠くものである。したがって，多額の予算をかけて住基カードを購入すること自体が最少経費・最大効果を定める地方自治法２条１４項及び地方財政法４条１項に違反するのであって，本件公金支出等は違法である。
（被告の主張）
原告らの主張は争う。
ア　地方自治法２条１４項，地方財政法４条１項の趣旨
地方公共団体は，その事務を処理するに当たり，住民の福祉を増進することが第一義的な目的であり，その実現に努めなければならないのはもとより，住民の責任とその負担によって地方自治が運営されるものである以上，常に効率的に処理されなければならず，最少の経費で最大の効果を挙げることが要請されている。地方自治法２条１４項は，かかる基本原則を規定し，地方財政法４条１項は，かかる基本原則を予算執行の立場から簡潔に表現したものである。
もっとも，地方自治法２条１４項は，「……ようにしなければならない」との文言からも明らかなように，純粋な訓示規定にとどまり，個々の支出行為を違法ならしめるものではないと考えられるから，違法事由としては地方財政法４条１項違反の有無を問題とすれば足りる。
イ　地方財政法４条１項違反の判断基準
ところで，予算の執行において，事務の目的を達成するために何をもって必要かつ最少の限度というべきかは，当該事務の目的，当該経費の額のみならず，予算執行時における経済状態，国民の消費及び生活の水準等の諸事情の下において，社会通念に従って決定されるべきものであるから，予算の執行権限を有する財務会計機関の社会的，政策的又は経済的見地からする裁量にゆだねられていると解すべきである。
したがって，当該具体的な支出の違法性の有無については，諸事情を上記各見地から総合的に判断し，当該公金支出が社会通念上著しく妥当性を欠き，裁量権の濫用に当たると認められる場合に限って違法となると解するのが相当である。
ウ　本件公金支出の適法性
以下の各点に照らせば，住基カードの発行に係る本件公金支出は，当該事務の円滑な遂行という目的達成のために必要不可欠な行為であって，そのための支出金額も妥当といえる金額であるから，Ｐ１市長の行為が上記の「社会通念上著しく妥当性を欠き，裁量権の濫用に当たる」と認められる余地は全くなく，住基カードの交付に係る支出が，地方財政法４条１項等に違反するものでないことは明白である。
（ア）　市町村長は，法３０条の４４第３項に基づき住基カードを発行する事務を行わなければならない。なお，住基ネット及び住基カードが，憲法１３条や法３６条の２及び改正法附則１条２項に抵触するものでないことは，既述のとおりである。
（イ）　被告は，当初，名古屋市の人口の約２パーセントに当たる４万枚の住基カードの調達を予定し，平成１５年度一般会計補正予算において，その購入経費として４２００万円（原盤１枚当たり１０５０円）を計上した。そして，Ｐ１市長は，平成１５年７月２２日，原盤カード２万枚を合計９４５万円で購入する契約を業者との間で締結し，平成１６年１月２２日，同金額を支出した。
また，住基カードの交付には，原盤カードに住民の氏名等を印刷するための住基カード発行機が必要となるところ，被告は，そのリース料として，平成

１５年度一般会計予算に約２８５１万６０００円を計上した。そして，Ｐ１市長は，平成１５年度において，住基カード発行機２３台のリース代金１９３１万５２５４円を支出した。

これらの金額は，業者数名による一般競争入札を行い，最低価格（住基カード原盤については１枚当たり４７２円５０銭）で申し込んだ業者との間で締結された契約に基づくものであって，公正な手続により確定したものである。

（ウ） また，被告は，平成１６年度一般会計予算において，１万枚の原盤カードの調達経費６３０万円及び住基カード発行機２３台のリース料約２８１２万５０００円を計上した。

予算の執行は，計上した予算の範囲内でしか支出できないところ，平成１６年度も原盤カードが前年度の１枚当たり４７２．５円で落札されるとは限らないから，６３０万円を予算に計上したものである。

エ 住基ネット及び住基カードの効用

住基ネット及び住基カードは，下記のとおり，行政サービスの向上及び行政事務の効率化に大きく寄与し，電子政府・電子自治体実現のために必要であるから，この点からも，住基カードの発行に関する支出は，「目的を達成するための必要且つ最少の限度」を超えるものでないことは明らかであり，本件公金支出が地方自治法２条１４項及び地方財政法４条１項に違反するとはいえない。

（ア） 住基ネットの導入の経緯及び目的

高度に情報化された現代社会において，既に民間部門では，コンピュータ・ネットワークシステムが構築，活用されており，顧客サービスの向上及び業務の効率化が積極的に進められてきている。このような中にあって，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必要性があり，また，高齢者や被災者等の弱者に対する配慮の行き届いた社会を構築するためのセーフティネットも必要である。

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，情報通信技術を的確に活用することが必要不可欠といえる。

ところで，住民基本台帳の全国的な電算化が進んでいたことから，これをネットワークで接続すれば，全国的な本人確認システムが安価に構築できるし，住民にとっては面倒な行政手続が簡略化され，行政職員の削減も可能となる。

まさに住基ネットは，このような発想から生まれたシステムであって，その目的は，行政サービスの向上と行政事務の効率化である。

（イ） 電子政府・電子自治体実現のための住基ネットの必要性

住基ネットは，平成１２年ころから，「電子政府・電子自治体」の実現のための必要不可欠な制度であるとの位置づけがされることとなった。すなわち，我が国は，電子政府戦略の点で諸外国よりも遅れていたため，ＩＴを基盤としたＢＰＲ（ビジネス・プロセス・リエンジニアリング）を実行しなければ諸外国との競争に負けるなどの強い危機感の下，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Ｐ３氏を議長とするＩＴ戦略会議が設置された。ＩＴ戦略本部とＩＴ戦略会議の合同会議は，同年１１月２７日，「５年以内に世界最先端のＩＴ国家となる」ことを目標とする「ＩＴ基本戦略」を立案し，これに対応して，国会も，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推進することを目的とする「
高度情報通信ネットワーク社会形成基本法（ＩＴ基本法）」を制定した。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，ＩＴ基本法３５条に基づいて策定された「ｅ－Ｊａｐａｎ重点計画」が発表された。その中で，平成１５年度を目標として，その前提条件となる社会環境を構築するために電子政府の実現を推進することとなった。すなわち，平成１５年度には，「原則として２４時間，自宅やオフィスからインターネットを利用して実質的にすべての行政情報の閲覧，申請・届出等の手続，手数料納付・政府調達手続が可能」となるような社会を目指すこととされ，その後，政府は，行うべき施策を定めた各種計画を次々と策定し，着実に実行してきた。

このような電子政府・電子自治体の基盤となる不可欠なシステムが，ネットワーク社会における本人確認手段としての住基ネットである。すなわち，住基ネットの導入によって，①広範な行政事務において，住民負担の軽減と行政事務の効率化及び正確性の向上を実現し（下記(ウ)ｃ），②行政手続のインターネット申請を実現し（下記(ウ)ｄ），さらに，③市町村のネットワーク化による住民基本

台帳事務の簡素化及び広域化を実現することができる（下記(ウ)ａ・ｂ）のであり，もって，我が国社会の発展に寄与するものである。

（ウ）　具体的効用

ａ　住民票の写しの広域交付

住基カードは，住民票の写しの広域交付を受ける場合の本人確認資料として利用でき（法１２条の２第１項），当該請求を受けた交付地市町村長は，住所地市町村長に対して，請求があった旨を通知し，住所地市町村長は，交付地市町村長に対して，必要事項を通知して，交付地市町村長が請求に係る住民票写しを作成，交付する（同条の２第２項ないし４項）。そして，上記各通知は，規則の定めるところにより，電気通信回線を通じて，電子計算機から相手方の電子計算機に送信する方法により行う（同条の２第５項）。

この点につき，原告らは，①運転免許証等を提示すれば住基カードを必要としないこと，②現在でも，郵送によって同様の便宜を受けることができること，③住民票登録地以外からの住民票の写しの申請が一生の間にほとんどないことなどを理由に，住基ネットのメリットはない旨主張する。

しかし，①の点については，運転免許証等を有しない者にとっては，住基カードは広域交付のために必須のものである。また，運転免許証等を有する者にとっても，住基カードによる広域交付も可能とする点で，利便性を高めるものである。②の点については，郵送による住民票の取得は可能であるが，住民票の広域交付に比較して日数を要する。③の点については，住民票の写しの交付は膨大な枚数に上っており，また，交通や通信手段のめざましい発達により，住民の生活圏や行動範囲は飛躍的に増大し，市町村や都道府県の圏域を越えた住民の交流や移動が一般化している中で，広域交付の要請は高まっていることを考慮すると，住民票登録地以外からの住民票の写しの交付のニーズは十分にあるというべきである。

ｂ　転入転出特例（住民の転入・転出事務の簡素化）

法２４条の２によれば，住基カードの交付を受けている者があらかじめ郵送等により付記転出届を行い，転出地市町村長が当該付記転出届に基づいて転出の処理を行い，その後，転入地市町村長において付記転入の処理を行うことにより，転出証明書情報が転入地市町村長に送信されることから，転入に際して転出証明書の添付が不要となり，他の市町村への転居の手続で窓口に行くのが転入時の１回だけとなる。

この点についても，原告らは，①郵送による転出届の提出及び転出証明書の取得によって，同様の便宜を得ることができること，②実際の転居では，転出届及び転入届だけではなく，学校の転校届その他転出地でのいろいろな手続が必要であり，住民票の移動の手続が簡易か否かどうかだけの議論は余り意味がない旨主張する。

しかしながら，これまでの郵送による転出届は，急に住所を移動することが決定し，旧住所地で届出を行う時間的余裕がない場合等にのみ認められる例外的なものであり，また，この方法では，転出証明書が本人あてに送付されるまでの間は転入手続を行うことができないし，返送料を負担しなければならないなど，住民にとって必ずしも簡便な手続であるとはいい難く，市町村にとっても，郵送による転出届を受けて転出証明書をその住民の住所地に郵送する手続があったことから，事務処理上の負担が大きく，不便な手続であったというほかない。次に，②の点については，学校の転校届のために市町村役場に赴くことを要するものではないし，その他の所要の手続についても住民が郵送により行うことができるから，原告らの主張は妥当ではない。

ｃ　住民票の写し等の提出の不要化（住民の負担軽減・行政手続の簡略化）

住民基本台帳は，市町村ごとに設けられているから，他の市町村，都道府県及び国の機関等は，従来より，当該市町村の住民に関する氏名，住所等の情報を必要とする場合には，住民に対して，事務ごとに住民票の写しの添付等の負担を課していた。そのため，平成１４年度において約８５００万枚という膨大な枚数の住民票写しが提出されていた。

そこで，住民の負担軽減，行政の効率化及び事務の正確性の向上を図るため，法３０条の６，同条の７，同条の８，同条の１０の各規定により，一定の場合に本人確認情報の提供ができることになった。すなわち，住民は，パスポート申請の際の住民票の写し，年金受給者の提出すべき現況届，身上報告書，恩給受

給者の提出する受給権調査申立書に必要な市町村長の証明印等の提出の負担が解消され，あるいは解消が予定され，行政側としても，事務効率の向上や，事務の正確性の向上が実現することになる。その他，国の機関等による本人確認情報の利用スケジュール及び利用法の概要は，別紙４のとおりである。

ｄ　公的個人認証サービスに住基ネットが寄与すること

さらに，電子署名に係る地方公共団体の認証業務に関する法律（平成１４年法律第１５３号）が施行されると，同法３条４項の規定により，電子証明書を住基カードに記録することができるようになり，これにより公的個人認証サービスを受けることができるようになる。

これは，行政手続のインターネット申請の基盤となるものであり，平成１４年１２月６日に成立した上記法律を含む行政手続オンライン化関係３法（他の２法は，「行政手続等における情報通信の技術の利用に関する法律」と「行政手続等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」である。）によって，国民と行政機関との間の申請・届出等の手続約２万１０００と行政機関相互の間の手続約３万１０００の合計５万２０００の手続がオンライン化されることとなった。

ｅ　その他

さらに，住基カードは，①市町村が条例で定めることにより，多目的カードとして活用でき，②カードに格納された住民票コードにより，本人確認がスピーディかつ確実に行うことができるなど，電子政府・電子自治体において，キーデバイスとしての役割を果たし，しかも，③公的な身分証明書としても活用できる。

第３　当裁判所の判断

１　主張・立証責任の所在について

本訴は，地方自治法２４２条の２第１項１号に基づく差止請求と同項４号に基づく損害賠償等請求（ただし，平成１４年法律第４号による改正後のもの）を内容としているところ，後者については，当該地方公共団体が，請求の相手方とされた者に対して，実体上の損害賠償請求権ないし不当利得返還請求権を有していることが前提となるから，その発生原因事実について，原告側が主張・立証責任を負うというべきである。また，前者についても，住民訴訟が，自己の有する権利・利益と関わりなく，住民たる資格において，地方公共団体の違法な財務会計行為を是正し，もってその財政運営の健全化を図る客観訴訟であることにかんがみると，差止めの対象たる行為が違法であることは，原告側において主張・立証すべきである。

２　争点(1)（住基ネット及び住基カードは，国民のプライバシー及び個人の尊厳を侵害する点で憲法１３条に違反するか）について

(1)　住基カードの発行に関する公金支出の違法性との関係

原告らは，住基ネットが共通番号である住民票コードを用いて国による全国民の個人情報の一元管理を可能とするものであるから憲法１３条に違反し，これを不可欠とする住基カードも同様である旨主張するところ，住基ネット及び住基カードのいずれもが改正法に基づいて創設されたものであるから，上記主張は，住民票コードを前提とする住基ネット本体に関する規定が憲法１３条に違反して無効であり，したがって，これと不可分一体の住基カードに関する規定も同様に無効であるというものと解される。

しかるところ，被告の主張によっても，住基カードは，単体でもある程度の有用性が存在するものの，その効用の大部分は，住基ネット本体と一体化されて使用されることによってもたらされるものであり，また，住基カード自体にも，住民票コード等が記録されることになっている（法３０条の４４）から，仮に住民票コードを用いることが違憲の原因となるのであれば，住基カードに関する規定が違憲として無効とされる余地はあると考えられる。

そこで，以下では，原告らの主張する憲法１３条違反の点について検討を加える。

(2)　プライバシーの権利について

プライバシーの権利をどのように理解するかについては，いろいろな考えがあるが，一般には，自己に関わる情報を開示する範囲を自ら決定することのできる権利と構成するのが相当である（原告らも，このような内容のものとして理解していることは，その主張に照らして明らかである。）。

プライバシーの権利をこのように把握するならば，憲法１９条，２１条１項，同条２項後段，３５条，３８条などは，その一側面あるいは行使の一場面を保

障するものと理解することができるが，さらにこれらの規定によって直接保護の対象とされない場合であっても，個人の尊厳を指導原理とする憲法１３条の幸福追求権に含まれ得るというべきである（被告も，プライバシーが憲法１３条で保障された権利であることを積極的に争っていない。）。

もっとも，このことは，自己に関する情報であれば，そのすべてが同人のコントロール下に置かれなければならないことを意味するものではなく，表現の自由を定めた憲法２１条１項や公務員の選定・罷免権を定めた１５条１項などの反射的効果として制約を受けることがあり得るし，また，一口に自己に関する情報といっても，思想・信条など個人の人格的自律に直接関わり，プライバシーのいわば中核に位置するような情報と，かかる人格的自律には直接には関わらない客観的・外形的事項に関する情報に大別されるところ，共同社会においては，他人と全く無関係に存在することは不可能であるから，後者については絶対的な保護の対象となるものではない。したがって，当該情報の内容・性質，当該情報の利用目的，当該情報の収集の態様などを
総合考慮して，その侵害の当否を決すべきであり，当該個人の明示的な同意を得ない場合や当該個人の意思に反する場合であっても，当該情報の保有・提供がプライバシーの権利の侵害とならないこともあり得るというほかない。

この点について，原告らは，大学が，講演会に参加を申し込んだ学生の学籍番号，氏名，住所及び電話番号の情報を本人の同意なく警察に提供した行為が不法行為を構成すると判断した最高裁判所平成１５年９月１２日第二小法廷判決を援用するが，同判決は，大学による情報提供行為が法令に基づくものでなく，当該情報を提供することへの承諾を求めることが困難であった特別な事情もうかがわれない事案に関するものであるから，上記判断と抵触するものでないことが明らかである。

(3)　本人確認情報等の管理とプライバシーの侵害について

以上を前提として，まず，住基ネットを通じた本人確認情報等の取得，管理，提供，利用を定める住基法の違憲性の有無について検討する。

ア　住民基本台帳の備付けと届出

住基法によれば，市町村長は，個人を単位とする住民票を世帯ごとに編成して，住民基本台帳を作成しなければならない（法６条１項）ところ，住民票には，①氏名，②出生の年月日，③性別，④世帯主ないし世帯主との続柄，⑤戸籍の表示，⑥住民となった年月日，⑦住所及び同一市町村内で住所を変更した場合はその住所を定めた年月日，⑧新たに市町村内で住所を定めた場合の届出年月日及び従前の住所，⑨選挙人名簿登載の事実，⑩国民健康保険の被保険者の資格に関する事項，⑪介護保険の被保険者の資格に関する事項，⑫国民年金の被保険者の資格に関する事項，⑬児童手当の受給資格に関する事項，⑭米穀の配給に関する事項，⑭住民票コード，⑮その他政令で定める事項が記載される（法７条）。

また，住民は，当該市町村に転入した場合には，①氏名，②住所，③転入の年月日，④従前の住所，⑤世帯主ないし世帯主との続柄，⑥転入前の住民票コード等を，同一市町村内で転居した場合には，上記①ないし⑤を，他の市町村に転出する場合には，①氏名，②転出先，③転出予定年月日を，それぞれ市町村長に届け出なければならず（法２２条ないし２４条），世帯又は世帯主に変更があった場合も同様に届け出なければならず（法２５条），また，国民健康保険の被保険者等である場合は，当該届出に付記するとされ（法２８条，同条の２，２９条，同条の２，３０条），この場合に，虚偽の内容を届け出た者（上記の付記を含む。）や正当な理由なく届出をしなかった者は，５万円以下の過料に処せられる（法５１条）。

このように，住基法は，住基ネットの創設以前から，住民に対して本人確認情報等の届出を強制し，市町村長がこれを基に住民票を編成して住民基本台帳を作成すべきことを定めている。

イ　本人確認情報の内容及び性質

ところで，住基ネットによって都道府県知事及び指定情報処理機関がそれぞれ取得し，国，行政機関，都道府県，市町村に提供する個人情報は，転入転出特例の場合を除き，①氏名，②生年月日，③性別，④住所に住民票コード（及びこれらの変更情報）を加えた本人確認情報に限られる（法３０条の５，同条の１１）ところ，これらの各情報は，個人の人格的自律に直接関わらない客観的・外形的事項に関するものにとどまり，思想・信条など個人の道徳的自律に関するものでないことは明らかであるから，秘匿の必要性が必ずしも高くないと考えられる。このこ

とは，立法論としての批判があることはともかくとして，不当な目的に基づくものでない限り，何人でも住民基本台帳を閲覧することができ，かつ，住民票の写しを取得できるとされている（法１１条１項，１２条２項）ことからも裏付けられる。

そうすると，住基ネットを通じて取得，保存，提供される本人確認情報については，必ずしも秘匿の必要が高度なものであるとはいえない。

ウ　本人確認情報の利用目的

住基法は，「……住民の居住関係の公証，選挙人名簿の登録その他の住民に関する事務の処理の基礎とするとともに住民の住所に関する届出等の簡素化を図り，あわせて住民に関する記録の適正な管理を図るため，住民に関する記録を正確かつ統一的に行う住民基本台帳の制度を定め，もつて住民の利便を増進するとともに，国及び地方公共団体の行政の合理化に資することを目的」とするものであり（法１条），このことは，住民票に記載される情報が，本人確認情報のほかは一定の行政事務に関する事項であることからも明らかである。

そして，住基ネットを通じて提供される本人確認情報は，法別表第１ないし第５所定の行政事務や条例で特に定めた事務等を処理するために用いられるとされており（法３０条の７，同条の８），それ以外の利用及び提供は禁止されている（法３０条の３０，同条の３４）から，その利用目的は正当なものというべきである。

エ　本人確認情報の取得の態様

前記のとおり，市町村長は，個人を単位とする住民票を世帯ごとに編成して住民基本台帳を作成しなければならないところ，その基礎となる情報は，基本的には住民の届出によって取得される。

もっとも，市町村長は，定期的あるいは必要があるときは，そこに記載された事項を調査するものとされており（法３４条），その結果，住民基本台帳等に脱漏，誤載があった場合には，届出義務者に対する届出の催告その他住民基本台帳の正確な記録を確保するための措置を講ずるとされている（法１４条１項）ところ，届出の催告以外の方法を取る場合でも，これに準ずる相当な手段によるべきことは当然というべきである。

そうすると，市町村長による本人確認情報の取得の態様は，社会通念に照らしても，是認できるものというべきである。

以上の検討によれば，本人確認情報は，絶対的な秘匿の対象となるものではなく，国や地方公共団体による利用目的も正当なものであって，その取得の態様も社会通念上相当であると認めることができるから，住基ネットを通じた本人確認情報の管理，利用自体がプライバシーの侵害として憲法１３条に違反するとはいえない（なお，転入転出特例の場合には，本人確認情報のほかに，転出前の住所，転出先及び転出の予定年月日，国民健康保険の被保険者である旨の情報等が，転出地市町村長から転入地市町村長に対して通知されるが，前記前提事実等(2)サ記載のとおり，これらの情報は，都道府県サーバ及び全国サーバを経由することなく論理的専用回線で構築された住基ネットによって直接通知されるのであり，また，これらの情報は，転入地市町村長が当該転入に係る住民票の作成に当たって必要な情報であることが明らかであるから，上記判断の妨げとなるものではない。）。

(4)　住民票コードによる一元的な情報管理の可能性について

ところで，原告らは，住基ネットは，個々の国民に対して住民票コードという共通番号を付し，これをマスターキーとして利用して「名寄せ」を行うことにより，国民の個人情報を一元的に管理，支配することを可能としており，憲法１３条に違反する旨主張する。

原告らのいう「一元的な情報管理」がどのような状態をいうのかは必ずしも明白ではないものの，その主張に照らせば，ある行政機関が特定の国民の個人情報を知りたいと考えたときに，コンピュータで住民票コードを入力して検索することにより，当該行政機関とネットワークで結ばれているあらゆる行政機関が保有する情報を直ちに入手することができる状態を指すと考えられる。

なるほど，かかる状態が実現したならば，行政機関は，その担当する事務内容とは無関係に国民の個人情報を入手，利用できることになり，特にその収集する情報が，政治的意見や宗教的信条等にわたるときは，国家の国民個人に対する強度の監視社会を成立せしめることになりかねず，そのような事態は，個人の自律と尊厳を基本原理とする憲法１３条に違反するとの疑いを否定することはできない。

しかしながら，前記のとおり，住基ネットの対象となる情報は原則として本人識別情報に限定され，かつこれを提供，利用できる事務は法定されて，それ以外の提供，利用が禁止されている（行政機関個人情報保護法８条２項は，この例外を認めるものではない。）上，国や地方公共団体の執行機関は，住基法の規定する事務の遂行のため必要がある場合を除いては，何人に対しても，住民票コードを告知することを求めてはならないとされていること（法３０条の４２）などに照らせば，住基法自体は，上記のような違憲の疑いのある事態を否定し，禁止していることが明らかであるから，技術的な見地からは，住基ネットが上記のような事態を可能ならしめる基盤としての意味を持ち得るとしても，そのような可能性が存在するだけでは，住基ネット
が憲法１３条に違反するとはいえず，したがって，住基カードについても同様というべきである。

(5) 小括

以上のとおり，住民票コードを前提とする住基ネット本体に関する規定や，これと不可分一体の住基カードに関する規定が憲法１３条に反する無効なものということはできず，原告らの前記主張は採用できない。

３ 争点(2)（法３６条の２及び改正法附則１条２項所定の措置を講ずることが，改正法の施行条件であるか）について

原告らは，法３６条の２及び改正法附則１条２項は法３０条の４４を含む改正法の施行条件であるところ，本件公金支出時はもちろん現在においても，これが満たされていない旨主張する。

しかしながら，法３６条の２第１項は，「市町村長は，住民基本台帳……に関する事務の処理に当たっては，住民票……に記載されている事項の漏えい，滅失及びき損の防止その他の住民票……に記載されている事項の適切な管理のために必要な措置を講じなければならない。」と規定している（同条２項は，これを事務の委託を受けた者に準用している。）ところ，その置かれた位置（住基ネットに関する第４章の２中ではなく，これに続く第５章雑則中に置かれている。）や，住基ネットの運用については，市町村長のみならず，総務大臣，指定情報処理機関及び都道府県知事らが関与するにもかかわらず，同項の主語が市町村長（２項は事務受託者）のみであることをも考慮すると，同項は，文言どおり，市町村長が，住民票記載事項の漏えい等を抑
止すべく適切な管理を行うべき義務を負うことを定めるものにすぎず，かかる義務を履行したことが，住基ネット及び住基カードの関係規定の施行条件になっていると解する余地はない。

また，改正法附則１条２項は，「この法律の施行に当たっては，政府は，個人情報の保護に万全を期するため，速やかに，所要の措置を講ずるものとする。」と規定しているところ，「この法律の施行に当たっては」とあって，施行条件であることをうかがわせる「この法律を施行するためには」との表現になっていないこと，条件であるならば，その内容が一義的に明確でなければならないにもかかわらず，「所要の措置」と抽象的な表現が採用されていること，さらに，１項本文において「この法律は，公布の日から起算して３年を超えない範囲内において政令で定める日から施行する。」と規定されており，２項の措置を講ずることが施行条件となっているのであれば，矛盾する内容となっていることなどに照らせば，同項は，政府に対して，各議院
における附帯決議よりも重い政治的責務を負わせる内容のものにすぎず，改正法の施行条件を定めたものと解する余地はないといわざるを得ない。

したがって，原告らの上記主張は採用できない。

４ 争点(3)（住基ネット及び住基カードには，個人情報の漏えいの危険性がある点で，法３６条の２及び改正法附則１条２項に違反するか）について

(1) 個人情報の漏えいの危険性と本件公金支出の違法性との関係について

原告らは，①住基ネット全般，②名古屋市の住基ネット接続方法等，③住基カードのいずれにおいても，情報漏えいを防止する対策が不十分であり，法３６条の２や改正法附則１条２項に違反していると主張する。

ところで，住民訴訟における違法性とは，当該財務会計行為自体が地方自治法その他の法令によって定められた具体的な財務会計法規上の義務に違反することをいう（最高裁判所平成４年１２月１５日第三小法廷判決・民集４６巻９号２７５３頁）ところ，法３６条の２及び改正法附則１条２項の趣旨は前記のとおりであり，これらが財務会計上の法規たる性質を有しないことは明らかであるから，仮に

名古屋市の設置した住基ネットが個人情報の漏えいの危険性を内包するとしても，それだけで名古屋市長による本件公金支出が直ちに違法となるとは考え難い。まして，公金支出が私法上有効に成立した債務を履行するために行われたときは，当該支出行為は違法とはいえないと解される（最高裁判所昭和６２年５月１９日第三小法廷判決・民集４１巻
４号６８７頁）ところ，原告らは，住基カード原盤購入契約や印字機械リース契約が違法・無効であることについて何ら主張するものでないから，この観点からも，本件支出行為が違法であるとの原告らの主張は，明確でないといわざるを得ない。
もっとも，名古屋市が発行する住基カードについては情報漏えい等の可能性が高く，およそ住基法が予定しているものとかけ離れた性能しか有しないことが明らかである場合には，これらの発行を目的とする契約締結行為等は，地方自治法２条１４項や地方財政法４条１項の趣旨を没却するものとして違法とされる余地があり，既に締結された原盤購入契約や印字機械リース契約についても，かかる事実を契約当事者らが認識していたなどの特段の事情が存する場合には，当該契約は無効とされる余地がないとはいえない。そして，住基カードと一体的に利用されることが予定されている住基ネット本体における情報漏えい等の可能性が高い場合にも，以上の理が基本的には妥当すると考えられるから，このような限定的な場合に限り，本件公金支出等が
違法となり得ると解するのが相当である。
なお，上記の情報漏えい等の可能性がどの程度存在するかについては，技術的要素を重視するか人的要素を重視するかによって異なり得るし，前者についても，技術開発の進展によってその水準が変化すると考えられるが，あくまでも本件公金支出等の違法性判断の考慮要素である以上，その時点における技術水準等を前提とし，社会通念に従って判断されるべきものと解される。
以下においては，このような観点から，住基カード及び住基ネット本体における個人情報漏えい等の可能性について検討する。
(2)　住基カード自体のセキュリティ対策について
ア　住基カードの技術的基準
規則４６条に基づき，住基カードのセキュリティについては，住基カードセキュリティ基準が定められているところ，具体的には下記のような対策が講じられることになっている（乙８，４７）。
(ア)　住基カード及び住基ネットアプリケーションの利用のためには，暗証番号が必要であるところ，暗証番号は住基カードに記録された上，その照合は，住基カード内部で行われ，暗証番号を住基カードの外部から読み取ることはできない（カードセキュリティ基準第２の２(1)）。
(イ)　発行前の住基カードに対し，不正使用を防止するための情報を設定する（住基カードセキュリティ基準第２の２(2)）。
(ウ)　交付後の住基カードと住基ネット相互間の認証を行うための情報を住基カードに設定し，同情報を住基カードの外部から読み取ることができないようにする（住基カードセキュリティ基準第２の２(3)）。
(エ)　住基カードに記録された情報を保護するために，アクセス権限の制御を行う（住基カードセキュリティ基準第２の２(4)）。
(オ)　住基カードの半導体集積回路に物理的又は電気的な攻撃を加えて，住基カードに記録された情報を取得しようとする行為に対し，情報の読み取り又は解析を防止する（住基カードセキュリティ基準第２の２(5)）。
(カ)　基本利用領域とそれぞれの条例利用領域は，住基カードの内部でそれぞれ独立し，割り当てられた領域以外には情報を記録し，又は記録された情報を読み取ることができないようにされる（住基カードセキュリティ基準第２の
２(6)）。
(キ)　住基カードの券面の偽造等を防止するための対策が講じられる（住基カードセキュリティ基準第２の２(7)）。
(ク)　上記(ア)ないし(キ)のセキュリティ対策を実施することを可能とするため，ＩＣカードが用いられる（住基カードセキュリティ基準第２の１）。また，その安全性を担保するため，住基カードは，ＩＳＯ等の規格第１５４０８の認証を受けたもの（これに加えて，当分の間は，同規格の評価を受けて合格した設計書に基づいて作成されたカードも許容される。）に限られる（住基カードセキュリティ基準第２の３）。
イ　要約

以上の(ア)ないし(ク)によれば，住基カードのセキュリティ対策が不十分であって，個人情報漏えい等の可能性が高いとは認められない。

ウ　原告らの主張の検討

この点について，原告らは，①住基カードは非接触型カードであり，保有者本人が知らないうちに情報の読み取り，改ざんなどの危険性がある，②住基カードに様々な個人情報が蓄積される可能性がある旨主張する。

しかしながら，①の点については，前記のとおり，住基カードについて情報の読み取り，改ざんの危険性の防止措置が講じられているところ，これらの防止措置が有効でないことをうかがわせる主張立証は存在しない。また，②の点については，確かに，条例利用領域内には，特に必要性が認められる場合には，利用者番号等以外の個人情報を記録することも認められている（住基カードセキュリティ基準第６の３(2)）。しかし，様々な個人情報が蓄積されたからといって，これらが漏えいする危険性が高いとはいえない上，そもそも，名古屋市は，セキュリティへの配慮の関係から条例による独自利用サービスを行っていないから，こと名古屋市が発行する住基カードに限っていえば，そのような危険性を認める余地はない。

よって，前記判断を覆すことはできない。

(3)　住基ネット本体についてのセキュリティ対策について

ア　運用関係者らによる情報漏えい等の防止措置

（ア）　担当職員に対する教育・研修

国は，平成１４年度以降毎年度，住基ネット関連のセキュリティ研修として，市町村の住基ネット担当者を対象に，個人情報保護意識の向上及び住基ネットの安全の確保等を目的としたセキュリティ研修会を実施し，今後も毎年実施する予定である。また，本人確認情報の提供を受ける国の機関等の担当職員向けの研修会を，提供開始時及び適宜，実施している（乙５，弁論の全趣旨）。

（イ）　住基法の定める刑罰や監督

ａ　住基法による守秘義務及び同法等による処罰

住基法は，住基ネットに係る事務に従事する市町村，都道府県，指定情報処理機関及び本人確認情報の提供を受けた国の機関等，地方公共団体の機関等の職員に対し，本人確認情報処理事務に関して知り得た本人確認情報に関する秘密又は本人確認情報の電子計算機処理等に関する秘密の保持義務を課し（法３０条の１７第１項，同条の３１第１項，同条の３５第１項及び第２項），これに違反した者に対しては，２年以下の懲役又は１００万円以下の罰金に処することとしている（法４２条）。

また，同法は，市町村，都道府県，指定情報処理機関及び本人確認情報の提供を受けた国の機関等，地方公共団体の機関等の委託事業者に対しても，同様に，その事務に関して知り得た本人確認情報に関する秘密又は本人確認情報の電子計算機処理等に関する秘密の保持義務を課し（法３０条の１７第２項，同条の３１第２項，同条の３５第３項），これに違反した者に対しても，２年以下の懲役又は１００万円以下の罰金を科すこととしている（法４２条）。

ｂ　指定情報処理機関に対する監督

指定情報処理機関は，役員の選任等の認可，解任命令（法３０条の１６），本人確認情報管理規程の認可（同条の１８），事業計画の認可等（同条の１９），監督命令（同条の２２第１項），報告及び立入検査（同条の２３第１項），指定の取消し（同条の２５）等を通じて総務大臣の監督に服するほか，都道府県知事による指示（同条の２２第２項），報告及び立入検査（同条の２３第２項）等の監督にも服することとされている。

（ウ）　操作者識別カードを使用した認証

本人確認情報は，ＣＳ，都道府県サーバ及び全国サーバ内に保存されており，端末機には存在しないから，市町村の職員が，転入届の処理等を始めとする住民基本台帳事務の処理に当たっては，端末機からＣＳにアクセスする必要がある。しかし，端末機からサーバにアクセスする際には，常に操作者識別カードと端末機との間で相互認証を行わないと住基ネットアプリケーションが起動しない設計となっている。すなわち，操作者識別カードを持たない職員等及び外部の者は，住基ネットアプリケーションを起動すらできないし，本人確認情報データベースにアクセスすることもできない。また，操作者識別カードの種別ごとに，住基ネットが保有するデータ等へ接続できる範囲が制限されている（セキュリティ基準第４の３(1)，第４の４(1)ないし(3)，同(5)。乙２の１，乙５）。

（エ） 照会条件の限定

本人確認情報の検索に際して，①即時提供（端末機から照会条件を入力し，都道府県サーバ又は全国サーバから即時に本人確認情報の提供を受ける方式をいう。）の場合，「住民票コードの全部」，「氏名及び住所」又は「氏名及び生年月日」のいずれかを端末機に入力しないと本人確認情報の提供を受けられない仕組みとなっている。また，「氏名及び住所」又は「氏名及び生年月日」を入力する場合には，前方一致検索が可能であるものの，そのためには，少なくとも「氏名の先頭一文字及び住所全部」，「氏名全部及び住所の都道府県・市町村名を除いた先頭一文字」，「氏名の先頭一文字及び生年月日全部」のいずれかの入力が必要であり，しかも，該当者が５０人を超えるときは本人確認情報の提供を受けられない設定となっている。

また，②一括提供（本人確認情報照会対象者の情報をファイル化して都道府県サーバ又は全国サーバに照会し，これらのサーバから照会結果ファイルを受け取る方式）の場合も，①と同様に，照会先から送られてきた「住民票コード」，「氏名及び住所」，「氏名及び生年月日」等のファイルに，都道府県サーバ又は全国サーバにおいて，本人確認情報を追記して照会元にファイルを返送するなどの措置が講じられている（乙５）。

（オ） 住民票の写しの広域交付における不正防止

住所地市町村において，交付地市町村の特定の操作者識別カードから一定時間当たり一定数以上の住民票の写しの広域交付要求があった場合は，システム上，住民票の写しの広域交付を停止する措置が講じられている（乙５）。

（カ） アクセスログの定期的解析と調査

指定情報処理機関は，運用管理規程に基づき，定期的に全国サーバのアクセスログの解析を行い，万一不正使用の兆候を検出した場合，緊急時対応計画等に基づき，必要な連絡，対策等を実施する。

都道府県は，同様に，運用管理規程に基づき，定期的に都道府県サーバのアクセスログの解析を行い，万一不正使用の兆候を検出した場合，緊急時対応計画等に基づき，必要な連絡，対策等を実施するほか，指定情報処理機関に対し，住民のアクセスログの解析を要請することができる。

また，市町村は，都道府県に対し，あるいは都道府県を経由して指定情報処理機関に対し，住民のアクセスログの解析を要請することができる（乙５）。

（キ） 住民に対する本人確認情報提供状況の開示

平成１５年１０月１日から，都道府県サーバ及び全国サーバにおいて，本人確認情報提供状況の開示用データ（提供先ないし検索元，提供年月日，利用目的等）を生成し，都道府県は，都道府県サーバの開示用データ及び指定情報処理機関から送信された全国サーバの開示用データを保存することとし，同年１１月以降，準備が整った都道府県から順次，それぞれの個人情報保護条例により住民から請求があった場合，その開示を行うこととした（セキュリティ基準第６の８(5)，乙２の３，乙５，弁論の全趣旨）。

（ク） 要約

上記(ア)ないし(キ)の各対策を総合すれば，担当職員に対する教育・研修により本人確認情報保護の意識の向上が図られているほか，刑罰規定の整備や監督措置，本人確認情報の照会に際する条件の限定，端末機のアクセス制御，多量の住民票の写しの広域交付の防止などの措置が講じられることにより，正規の権限を有しない者が住基ネットを通じて他人の情報に接し，これを利用することを抑止するとともに，アクセスログの定期的解析及び住民に対する本人確認情報提供状況の開示をすることを通じて，不正の兆候ないし不正行為の早期発見，調査及び再発防止を図っていると認められるから，社会通念上，運用関係者らによる情報漏えいの可能性が高いとはいえない。

（ケ） 原告らの主張の検討

この点について，原告らは，要旨，①運用関係者による情報漏えい行為に対する罰則は故意犯に限定されており，しかも法定刑が軽すぎる上，総務大臣及び都道府県知事による指定情報処理機関への監督は実効性がない，②全国サーバ及び都道府県サーバのアクセスログの解析により，不正使用の兆候が発見されたときにはもはや情報が流失しており手遅れである，③本人確認情報提供状況の開示では，流出の防止策としては不十分である，④一定数以上の住民票の写しの広域交付があった場合にこれを停止する措置が働く場面はほとんどないなどと主張する。

なるほど，どのような情報漏えい防止措置を講じようとも，技術水準が日進月歩の今日において，完璧な効果を期待することはできず，また，住基ネットを扱うのが人間である以上，そこに過誤等の入り込む余地が全くないとはいえないが，前記のとおり，情報漏えいの可能性の有無についての判断は，その時点における技術水準等を前提とし，社会通念に従って判断されるべきものであるところ，原告らの上記主張はいずれも例外的な事態を前提としたものであり，上記(ア)ないし(キ)の各措置が情報セキュリティの保全に寄与しているとの上記判断を覆すものとはいえない。

イ　制度面からの対策

(ア)　保有情報の限定等

都道府県及び指定情報処理機関が，それぞれ都道府県サーバ及び全国サーバにおいて保存して保有する情報は，住基法上，本人確認情報（氏名，住所，性別，生年月日，住民票コードとこれらの変更情報）に限定されている（法３０条の５第１項）。

なお，変更情報とは，異動事由（「転入」，「出生」，「職権記載等」，「転出」，「死亡」，「職権消除等」，「転居」，「職権修正等」，「住民票コードの記載の変更請求」，「住民票コードの職権記載等」のいずれか），異動年月日と異動前の本人確認情報であり（令３０条の５及び規則１１条），国外転出者等を除いて過去５年間分を保存し，保存期間経過後確実に消去することとしている（セキュリティ基準第６の７）。

また，住民票の写しの広域交付，転入転出手続の特例等の際には，市町村から市町村へ続柄等の情報も送信されるが（令１５条の２第２項及び２４条の４），市町村のＣＳからの情報は，すべて直通の回路を通じて送信されるので，当該情報が都道府県サーバや全国サーバを通過することも，そこに保有されることもない（セキュリティ基準第３の３(3)）。

(イ)　本人確認情報の利用及び提供の範囲

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法律で具体的に規定されている（法３０条の６，同条の７第３項ないし第６項，同条の８，別表第１から第５）。なお，市町村長ないし都道府県知事は，他の市町村の執行機関ないし他の都道府県の執行機関に対して，条例で定める事務の処理に関して本人確認情報を提供することができるが（法３０条の６，同条の７第４項２号，同条の７第５項２号，同条の７第６項２号），法律の規定により条例に委任されているのであって，なお法律に基づく場合と同視することができる。

(ウ)　住民票コードの利用の制限

市町村長等の行政執行機関や指定情報処理機関は，住基法の定める事務を遂行するために必要な場合を除き，住民票コードを告知することを求めてはならない（法３０条の４２）。

また，上記以外の者も，住民票コードの告知を求めてはならない（法３０条の４３第１項）上，契約の締結に際して住民票コードの告知を要求したり，住民票コードの記載されたデータベースで他に提供されることが予定されているものを構成したりしてはならない（法３０条の４３第２項，３項）。そして，都道府県知事は，これに違反する行為が行われた場合，中止を勧告することができ（法３０条の４３第４項），中止勧告に従わない者に対しては，都道府県の審議会の意見を聴いて中止命令を発することができる（法３０条の４３第５項）。そして，都道府県知事の中止命令に違反した者は，１年以下の懲役又は５０万円以下の罰金に処せられる（法４４条）。

なお，住民票コードは無作為の番号であり，住民の申請によりいつでも変更できる（法３０条の３）。

(エ)　管理責任の範囲の明確化

住基ネットの各機器に関する市町村，都道府県，国，指定情報処理機関の管理責任の範囲を明確化し，それぞれ責任を持ってセキュリティを確保することとされている。

ａ　総務省は，制度を所管し，指定情報処理機関に対して監督を行う立場から，指定情報処理機関への監督命令等（法３０条の２２），地方公共団体への指導，助言・勧告等（法３１条），本人確認情報処理規程の認可（法３０条の１８），セキュリティ基準の策定等の権限を有する。また，総務省には，①セキュリティ面での緊急対応のために，住民基本台帳ネットワークシステム緊急対策本部及び②住基ネットの運営等の在り方について幅広く調査審議を行い，総務大臣に意見

を述べるために，住民基本台帳ネットワークシステム調査委員会がそれぞれ設置されている。

ｂ　指定情報処理機関は，国の機関等に本人確認情報の提供を行う際には，あらかじめ国の機関等が行う個人情報保護措置等を定めた協定書を取り交わすこととされており，また，指定情報処理機関は，本人確認情報の保護を図るため必要がある場合には，国の機関等に対し，報告要求，情報提供停止等を行うことができる。なお，指定情報処理機関には本人確認情報保護委員会が設置されている（法３０条の１５）。

ｃ　都道府県は，当該住民の本人確認情報の保護を図るため必要がある場合には，指定情報処理機関に対し，あるいは，指定情報処理機関を経由して国の機関等に対し，報告要求等を行うことができる（法３０条の２３第２項）。また，都道府県には，本人確認情報保護審議会が設置されている（法３０条の９）。

ｄ　市町村は，都道府県・指定情報処理機関を経由して国の機関等に対し，報告要求等を行うことができる。

(オ)　要約

(ア)ないし(エ)の措置を総合すれば，本人確認情報や住民票コードを提供し，利用するに際しては，その目的が住基法によって厳しく限定され，また，住基ネットに関与する行政機関等の権限と責任が明確化されることにより，制度面から，情報漏えい等の不測の事態の発生を抑止する措置が講じられている上，万一，情報漏えいが起きた場合の被害が最小のものとなるような制度設計となっていると認められる。

(カ)　原告らの主張の検討

ａ　この点についても，原告らは，①重要な情報の流出による被害を最小限にするには情報を分散すべきである，②保有情報の限定等について，ⅰ住基ネット上を流れる情報には，住民票コードも含まれる，ⅱ氏名，住所，性別，生年月日の４情報だけでも大丈夫とはいえない，ⅲ転入転出特例の場合には，世帯主との間柄，戸籍の表示，国民健康保険に関する情報等も一緒に住基ネットを流通する，③法律改正によって本人確認情報の利用及び提供の範囲がなし崩し的に拡大される，④ⅰ民間企業が任意の提供を受けることを禁止していないため，事実上住民票コードの告知を要求される危険性がある，ⅱ民間部門が自ら使用する目的でデータベースを構築することは許されている，ⅲ国の機関等と他の国の機関等との間で住民票コードを利用しデータマッチングすることを禁止する根拠が明らかではない，ⅳ住民票コードを変更しても変更履歴が残るので変更前の情報を追跡することができるから，変更に意味はない旨を主張して，制度的側面からの対策も不十分であるなどと主張する。

ｂ　そこで検討するに，原告らの上記主張は，住基ネットにおける個人情報の漏えい等の可能性が高いことを指摘するものではなく，情報漏えい等があることを前提とした弊害や，事実上の危惧を指摘するものであって，つまるところ，住基法（及び同法施行令やセキュリティ基準）に対する制度的批判にすぎないというべきであるが，同法が憲法１３条に反する無効なものと解することができないのは既述のとおりである。

また，個別的に検討しても，①については，そもそも情報の分散化は，負担の軽減と行政上の効率化を目的とした住基ネットの存在理由と正面から抵触するといわざるを得ないこと，②については，本人確認情報等だからといって，住基ネットにおいてそのセキュリティが軽視されているものでないこと，③については，法律改正によって本人確認情報を利用等できる事務が増加する可能性を否定することはできないが，それが直ちに不当であるとか憲法１３条に違反するものであるとはいえないこと，④については，上記のとおり，住基法は，民間部門による住民票コードの告知要求やこれを記録したデータベースの構成を禁止しており，これが遵守されない事態が考えられるからといって，住基ネットが情報漏えい等の可能性の高いものであるとはいえないし，住民票コードを利用したデータマッチングを正面から禁止する規定は置かれていないとしても，争点(1)についての判断で述べたとおり，国の機関等は，提供を受けた本人確認情報を法別表第１掲記の事務の処理に限って用いることができ，他者にこれを提供，利用することはできないから，国の機関等と他の国の機関等との間で住民票コードを利用したデータマッチングを行うことは許されていないと考えられ，また，住民票コードの変更は，正規の権限を有しない情報取得者に対する関係では，有用性を否定できないことなどを考慮すると，住基ネットにお

いて情報漏えい等の不測の事態の発生を抑止するとともに，万が一の場合における被害を限定する制度的手当が講じられているとの前記判断を覆すものとはいえない。

ウ　外部からの侵入防止対策その１（物理的なセキュリティ対策）

セキュリティ基準においては，関係機関は，建物及び重要機能室への侵入の防止等（第３の１(1)），重要機能室の配置及び構造（第３の１(2)），重要機能室の入退室管理（第４の１），磁気ディスク，構成機器及び関連設備等並びにデータ，プログラム，ドキュメント等の管理（第４の６，第４の７及び第４の８）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義務付けられている（乙２の１ないし３）。

したがって，これらが遵守される限り，権限を有しない者が住基ネット関連の機器に物理的に接近することは困難であると認められる。

エ　外部からの侵入防止対策その２（電気通信回線経由による侵入に対する対策）

（ア）　論理的専用回線による通信

住基ネットにおいては，ＣＳ，都道府県サーバ及び全国サーバ間の通信は，すべて論理的な専用回線（物理的な専用回線ではないが，セキュリティ技術を利用することによって，あたかも専用回線であるかのように利用できる仮想的なネットワーク）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，また，全国サーバと国の機関等サーバとの間は，論理的な専用回線又は磁気媒体でデータ交換が行われる（セキュリティ基準第３の３。乙２の１，５，弁論の全趣旨）。

（イ）　相互認証

住基ネットにおいては，暗号技術評価委員会において安全性が確認されている公開鍵方式により，通信を行うごとに意図した通信相手に接続されたことを相互に認証する仕組みが採用されている（セキュリティ基準第４の３(4)）。この公開鍵方式における秘密鍵は，指定情報処理機関が耐タンパー装置に封入設定後，地方公共団体及び国の機関等に配送するため，第三者が内容を読み出したり，変更することはできない。

また，通信相手の相互認証の過程で，耐タンパー装置内で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，通信相手に送信するとされている（セキュリティ基準第４の３(5)）ところ，住基ネットにおけるデータ送受信は短時間であり，その都度共通暗号鍵が変わるため，盗聴による恒常的な暗号鍵の解読は極めて困難である。

（ウ）　通信プロトコルの制限

住基ネットの通信プロトコル（通信規約）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しておらず，独自の住基ネットアプリケーションによる独自プロトコルによる通信を行っている（乙５，弁論の全趣旨）。

また，すべてのＣＳの住基ネット側，すべての都道府県サーバの住基ネット側と端末機側（端末機側については，都道府県サーバと既存庁内ＬＡＮを接続しない団体を除く。），全国サーバの全方向及び国の機関等サーバ（全国サーバと接続しない国の機関等サーバを除く。）のネットワーク側に，それぞれ指定情報処理機関監視ファイアウォールを設置して，インターネットで用いられるプロトコルの通過を遮断している（セキュリティ基準第４の３(2)，乙２の１，５）。

（エ）　コンピュータウィルス・セキュリティホール対策

指定情報処理機関は，コンピュータウィルスの発生情報を常時入手し，定期的に（危険度が高いものについては随時），全地方公共団体の全サーバ，全端末に対して，パターンファイルを自動的に配付し更新している。

また，ＯＳ（ウィンドウズ，ＵＮＩＸ等）のセキュリティホール発生情報を入手し，危険度が高いものは，システムの影響度を確認した上で全団体にセキュリティホール情報及び対応方法を通知し，その他のものは，システムの動作確認後，サービスパックを適用するように通知している（乙５，弁論の全趣旨）。

（オ）　不正な通信の遮断と監視

ａ　指定情報処理機関監視ファイアウォール，ＩＤＳ（侵入検知装置）の設置による厳重な遮断と監視

指定情報処理機関監視ファイアウォールは，全国サーバと住基ネットの間，住基ネットとＣＳとの間に設置され，あらかじめ正常なものとして設定した通信以外の通信を遮断するほか，不正アクセスの兆候等を検出する。

また，指定情報処理機関は，ネットワーク内にＩＤＳを設置し，指定情報処理機関のネットワーク監視室からＣＳとの間に設置されたファイアウォールまでの範囲では常時，ＣＳについては１５分に１回の割合で機器が正常に作動しているか否かの監視（死活監視）を行っている。

そのほか，指定情報処理機関は，定期的なログの解析を行い，指定情報処理機関監視ファイアウォールを通過した不正アクセスを検出した場合は，緊急時対応計画等に基づき必要な連絡，対策等を実施する（セキュリティ基準第４の９(3)(4)，乙２の１，５）。

ｂ　各サーバの保護

全国サーバ，都道府県サーバ及びＣＳと住基ネットとの間並びに国の機関等サーバと全国サーバとの間には，いずれも双方向からの不正な通信を遮断するため，指定情報処理機関監視ファイアウォールが設置されている（なお，国の機関等の中には，回線を利用した通信の方法によらず，媒体交換の方法によるところもある。）。

また，端末機を設置するため都道府県サーバ，ＣＳ，国の機関等サーバと各既存庁内ＬＡＮを接続する場合，それぞれ都道府県，市町村，国の機関等が厳格に管理するファイアウォールないし指定情報処理機関監視ファイアウォールによって，端末機・既存住基システム側からの不正な通信を遮断し，既存庁内ＬＡＮがさらに外部ネットワークと接続する一部の都道府県ないし市町村は，さらに都道府県ないし市町村管理のファイアウォールを設置している（セキュリティ基準第４の９(3)(4)，第５の１(3)(6)イ，乙２の１，５，弁論の全趣旨）。

（カ）　ソフトウェアの統一

①相互認証，②暗号化，③コンピュータウィルス，セキュリティホール対策，④操作者識別カードと暗証番号による操作者確認，⑤本人確認情報データベースへの接続制限，⑥データ通信の履歴管理及び操作者の履歴管理などの対策を行うため，住基ネットのシステム全体で統一ソフトウェアが導入されている。

（キ）　内部点検や外部監査によるセキュリティの確保

ａ　チェックリスト方式による市町村の自己点検

指定情報処理機関と総務省は，市町村における住基ネットとそれに接続する既設ネットワークにおけるセキュリティ対策の徹底を図り，もって住基ネットのセキュリティ強化を図るため，協力してチェックリストを作成し，市町村に配布した。市町村は，平成１５年１月ないし２月，これに基づきセキュリティ対策の自己点検を実施した。

総務省は，平成１５年５月１３日，住基ネット担当課長会議を開催し，この点検結果を踏まえて，都道府県において，市町村に対して必要な技術的指導を行うことを要請した。

これを受けて，対策状況について自己点検結果を調査したところ，平成１５年８月８日の集計では，すべての市町村が，重要点検項目（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，盗難されたり，権限のない者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。②ＣＳ端末について，ウィ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。③ＣＳと既設ネットワークの間にファイアウォールを設置し，適切な運用管理を行う。④ＣＳと既設ネットワークの間のファイアウォールについて，適切な設定を行う。⑤住基ネットと接続する既設ネットワークがインターネットに接続する場合には，当
該既設ネットワークとインターネットとの間にファイアウォールを設置し，厳重な通信制御を行う。⑥メールサーバ及びWWW（ワールドワイドウェブ）サーバ等の公開サーバについて，ＤＭＺ（公開領域）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。）につき満点を達成した。また，その他の項目についても，市町村のセキュリティ対策は強化された（乙６）。

平成１６年６月ころにも，各市町村において，同様の方式による自己点検が行われ，平成１５年度の重要点検項目については，すべての市町村が満点を達成し，平成１６年度の重要点検項目（①ＣＳ，ＣＳ端末，市町村設置ファイアウォールのＯＳのパスワードが容易に推測されることのないような措置を講じる。②ＣＳ，ＣＳ端末，市町村設置ファイアウォールのＯＳについて，不正なアクセスを予防するため，同じユーザＩＤで複数回パスワードの入力を間違えた場合，ロックアウト（無効化）するように設定する。③ＣＳ端末の住基ネットアプリケーショ

ンを起動させるために必要となる操作者識別カードのパスワードが，容易に推測されることのないような措置を講じる。④電気通信関係装置（ルータ，ハブ，ファイアウォール）に対して権
限のある者以外による操作を防止するため，電気通信関係装置へログイン，操作するためのユーザＩＤ，パスワードを適切に管理する。）についても，ほぼすべての市町村が満点を達成した（乙５４）。

ｂ　外部監査法人による市町村のシステム運営監査

平成１５年１月から３月までの間，全国１０８団体の市町村において，外部監査法人によるシステム運営監査が実施された（弁論の全趣旨）。

ｃ　クロウ社による外部監査

指定情報処理機関は，平成１５年１０月１０日から１２日までの間に，東京都品川区の協力を得て，アメリカの監査法人（クロウ社）のセキュリティ部門による外部監査を実施した。

クロウ社は，指定情報処理機関に対し，住基ネットの主要な機器（住基ネットーＣＳ間のファイアウォール，ＣＳ－庁内ＬＡＮ間のファイアウォール，ＣＳ端末）に関するペネトレーションテスト（模擬攻撃）では，これらの機器への侵入は成功せず，脆弱性も見いだせなかったとの結果を報告するとともに，庁内ＬＡＮに対してもチェックリストによる自己点検やセキュリティ監査を行うべきであること，庁内ＬＡＮ上のデータ送信における高度なセキュリティレベルを維持するための方策を実施すべきであることを助言した（乙７）。

（ク）　要約

(ア)ないし(キ)によれば，住基ネットの内部から個人情報の漏えい等が生ずる可能性は極めて乏しいと認められる上，電気通信回線経由による外部からの侵入に対しても，論理的専用回線の採用等，相互認証・暗号通信，通信プロトコルの制限，コンピュータウィルス及びセキュリティホール対策，不正な通信の遮断と監視並びにソフトウェアの統一などのセキュリティ対策が施されていると認められる。

もっとも，例えば，ファイアウォール（一般には，外部からコンピュータネットワークへの侵入を防ぐために，不正なアクセスを検出・遮断するためのソフトウェアないしかかるソフトウェアを組み込んだハードウェアを指す。）にも，セキュリティホールが含まれていることがあり得るところ，攻撃者が，これを利用してその機能を無力化することが考えられるし，ファイアウォールが正常な通信と判断した通信の中には，コンピュータにとって有害なソフトウェアが含まれていることもあり得るので，個人情報の漏えい等が生ずる可能性は，皆無とまではいえないが，そうであるとしても，現在の技術水準でおよそ考えられる対策が講ぜられている以上，その可能性が高いといえないことが明らかである。

（ケ）　原告らの主張の検討

ａ　原告らは，長野県侵入実験の結果によれば，外部の侵入防止対策が無力であることが実証されていると主張するので，これについて検討するに，証拠（甲４２の１・２，５０，５８，６２，７０，７１，７４，７５，７７，乙５２）及び弁論の全趣旨によれば，以下の事実が認められる。

（ａ）　長野県侵入実験の方法

ｉ　長野県下伊那郡α

平成１５年９月２２日ないし２４日に行われたαの第１次調査では，村役場のサーバ室の庁内ＬＡＮのＨＵＢ，村役場に隣接する出先機関のＬＡＮポート，庁内ＬＡＮにダイヤルアップで接続されている出先機関のルータにそれぞれ調査用コンピュータを接続して，実験が行われた。

同年１１月２５日ないし同月２８日に行われたαの第２次調査では，村役場のサーバ室の庁内ＬＡＮのＨＵＢに調査用コンピュータを接続して，実験が行われたほか，村役場のサーバ室のラックを開錠し，ＣＳセグメントにあるＨＵＢに調査用コンピュータを接続して，実験が行われた。

ⅱ　長野県諏訪郡β

平成１５年９月２５日及び２６日に行われたβの調査では，調査用に構築した無線ＬＡＮを利用して，町役場に隣接する建物から調査用コンピュータを庁内ＬＡＮに接続して，実験が行われた。

ⅲ　長野県東筑摩郡γ

平成１５年９月２９日ないし同年１０月１日に行われたγの庁内ＬＡＮへの調査では，遠隔地からインターネットを経由した侵入実験が行われ

た。
ⅳ　なお，いずれの実験においても，当該町村の管理するＣＳから他のＣＳ，都道府県サーバ，全国サーバへの攻撃は，試みられなかった。
（ｂ）　長野県侵入実験の結果の概要
ⅰ　αの庁内ＬＡＮからの実験結果
αの庁内ＬＡＮに接続したコンピュータから，既存住基サーバで使用されているＯＳ（基本ソフト）の既知の脆弱性を利用して同サーバの管理者権限を奪取することができた。また，既存住基サーバの管理者権限のユーザ名及びパスワード設定に問題があったため，既存住基サーバにアクセスすることができたほか，データベースのユーザ名及びパスワード設定に問題があったため，データベースの内容を閲覧することが可能であった。
そのほか，ファイル共有の設定に問題があったため，個人情報を含む重要なデータファイルにアクセスすることが可能な状態であった。さらには，庁内ＷＥＢサーバが使用しているＯＳの既知の脆弱性を利用することによって，同サーバの管理者権限を奪取することもできた。
庁内ＬＡＮとＣＳとの間のファイアウォールには不要と思われるポートが開いていたものの，ファイアウォールの管理権限の奪取はできなかった。
ⅱ　αの出先機関からの実験結果
αの出先機関に設置されているダイヤルアップ・ルータから，庁内ＬＡＮに接続する際にパスワード等は必要でなかったほか，不正常な通信を制御するためのパケット・フィルタリングも行われていなかった。したがって，攻撃者は，αの村役場内のＬＡＮからの攻撃と同程度の攻撃を，αの出先機関から行うことが可能であった。
なお，一般住民が立入可能なところにも，同出先機関のＬＡＮ端末が存在した。
ⅲ　βの庁内ＬＡＮからの実験結果
βの庁内ＬＡＮに接続したコンピュータから，既存住基サーバで使用されているＯＳの既知の脆弱性を利用して同サーバの管理者権限を奪取することができた。
しかし，既存住基サーバと市町村設置ファイアウォールとの間の通信の解析を試みたが，十分に解析ができなかった。
ⅳ　γの庁内ＬＡＮへの侵入実験結果
インターネットに接続されたコンピュータから，γの庁内ＬＡＮとの間に設置された庁内ファイアウォール越しに庁内ＬＡＮに設置された公開サーバ群への攻撃を行ったが，既知の脆弱性がなかったために，同サーバの管理者権限を奪取することができなかった。
ⅴ　αの第２次実験結果
αの庁内ＬＡＮに接続したコンピュータから，市町村設置ファイアウォールの管理権限を奪取したり，市町村設置ファイアウォールを越えた攻撃によってＣＳの権限を奪取することはできなかった。しかし，同ファイアウォールの中には不要と思われるポートが開放されているものがあったほか，ファイアウォールのＯＳのバージョンが古く，サービス拒否攻撃に対する脆弱性が存在した。
ＣＳセグメントに接続したコンピュータから，ＣＳが使用しているＯＳの既知の脆弱性を利用してＣＳの管理者権限を奪取することができた。
ＣＳ端末には既知の脆弱性がなかったが，ＣＳの管理者権限を奪取後得られたデータを利用することによって，ＣＳ端末の管理者権限でログオンすることができた。
ｂ　上記実験結果等によれば，①公開サーバ群及びファイアウォールに対して適切な設定及び保守管理を行えば，インターネットを通じた既存住基システム及びＣＳ等への攻撃は極めて困難であること，②他方，庁内ＬＡＮにいったん接続することができれば，既存住基サーバ等が適切に管理されていない場合には，既存住基サーバの管理者権限が奪取され，同サーバに保存されている住民票記載事項に関するデータの削除，改ざん等を行うことが可能であり，削除ないし改ざんされたデータがＣＳを通じて，都道府県サーバ及び全国サーバに送信される危険性があること，③市役所や町村役場以外にも，庁内ＬＡＮへの接続が可能な場所が存在し，その中には一般住民が立ち入ることが比較的容易なものもあること，④既存住基システムないし庁内Ｌ

ＡＮからファイアウォール越しに攻撃してＣＳの管理者権限を奪取することができなかったこと，⑤ＣＳが適切に管理されていないと，ＣＳセグメントからＣＳの管理者権限を奪取することが可能であること，以上のとおり要約することができる。

このような状況を総合すると，庁内ＬＡＮ及び既存住基システムのセキュリティ対策が不十分であった場合には，これを介在させて住基ネットから個人情報を取得し，あるいはそのデータを改ざんすることが不可能とはいえないところ，長野県侵入実験の対象となった地方公共団体の中には，この点について危惧を抱かせる状態にあったものが存在したと認められる。

しかしながら，上記の問題点は，厳密には，住基ネットそのもののセキュリティに関するものではなく，庁内ＬＡＮ等のセキュリティに関するものにすぎないほか，適切な設定，保守管理が行われる限り，住基ネットに対する外部からの攻撃は極めて困難であると認められるから，住基ネット一般の情報漏えい等の可能性を示すものではないといわざるを得ない。したがって，住基ネットについては，現在の技術水準でおよそ考えられる対策が講じられているとの前記判断を覆すものとはいえない。

(4)　名古屋市における住基ネットのセキュリティ対策

ア　制度面における対策

名古屋市は，セキュリティ基準に基づいて，「名古屋市住民基本台帳ネットワークシステムセキュリティ組織要綱」，「名古屋市住民基本台帳ネットワークシステム管理要綱」及び「名古屋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」を策定している（乙１１ないし１３）。

この「名古屋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」では，住基ネットのセキュリティを侵犯する不正行為又は障害が発生し，それにより個人情報の保護が図れないと判断した場合には，名古屋市のセキュリティ会議が，システムの停止等についての決定を行うこととしている。

また，名古屋市は，平成１５年７月１７日，名古屋市個人情報保護条例の一部を改正して，職員又は委託業務の従事者が業務に関して知り得た個人情報を自己若しくは第三者の不当な利益を図る目的で提供し，又は盗用した場合には，１年以下の懲役又は５０万円以下の罰金に処する旨の罰則を設けた（同条例３２条。乙１４の１・２）。

イ　外部からの侵入防止対策

(ア)　ＣＳに対する不正な通信の遮断及び監視に関する措置

名古屋市は，セキュリティ基準第５の１(6)イに適合するように，既設ネットワークとＣＳとの間に市町村設置ファイアウォールを設置している。さらに名古屋市は，既設ネットワークと市町村設置ファイアウォールとの間に，住基ネットに必要なデータのみを蓄積した中間サーバを設置するとともに，当該中間サーバと既設ネットワークの間にもファイアウォールを設置している（乙４８，証人Ｐ２。なお，別紙３参照）。

(イ)　名古屋市の管理する住基ネットに関する外部監査の結果

監査法人トーマツは，平成１５年２月１０日から同年３月２７日までの間，名古屋市の依頼に基づき，名古屋市の管理する住基ネットに関する外部監査を行った。技術面の監査の対象は，地域振興部区政課の管理に係るＣＳ，中間サーバ，ＣＳの管理端末，中間サーバの管理端末，住基ネットと庁内ＬＡＮとのファイアウォールに関する管理端末，ＣＳ端末（区役所，支所及びサービスセンターに設置されているものを除く。）であった。これに基づき，監査法人トーマツは，同月３１日付け「名古屋市住民基本台帳ネットワークシステムに係るシステム監査報告書（最終版）」を提出して，委託先に対してセキュリティ状況の報告を求めていないこと，機器類の最新状況が台帳で把握されていないこと，ユーザＩＤの権限の明確化が不十分であること
，パスワードの有効期限の設定，最低けた数や複雑さの規定が不十分であることなど，４２項目の問題点を指摘した（乙１５）。

名古屋市は，上記問題点を検討して改善措置を講じた上，監査法人トーマツに対して，改善状況調査を依頼したところ，同監査法人は，同年５月２９日及び３０日に改善状況調査を実施し，これに基づいて，上記問題点のうち２１項目が「具体的対応作業が完了し，現在，運用中又は運用開始が可能な状況にあ」り，２０項目が「対応の方向性の検討が完了し，現在，具体的対応作業（略）を行っている状況にあ」り，１項目が「現在，対応の方向性を検討している状況にある」との報告を行った（乙１６）。

さらに，監査法人トーマツは，平成１６年２月２４日から同年３月３１日までの間，名古屋市の依頼に基づき，名古屋市の管理する住基ネットに関する外部監査を行った。技術面の監査の対象は，１６区役所及び５支所のＣＳ端末，住基カード発行端末であった。これに基づいて，監査法人トーマツは，同月３１日付けで「名古屋市平成１５年度住民基本台帳ネットワークシステムに係るシステム監査報告書」を提出して，市民課事務室の構造，操作者識別カードの貸与状況，住基カードの保管枚数の確認等２３項目についてセキュリティ上の検討すべき事項を指摘した（なお，セキュリティを維持向上するため，区役所独自にマニュアルを作るなど，セキュリティ確保のために評価されるべき事項も指摘されている。乙４９）。

（ウ） 既存ネットワークとインターネットとの接続に関する対策

ａ 運用管理要領等の制定

住基ネットと接続する既設ネットワークがインターネットに接続する場合には，セキュリティ基準第５の１(6)アにより，「既設ネットワークの管理責任者は，既設ネットワークを外部ネットワークに接続するための手続，方法等を定め，接続及び運用に関する業務を総括的に管理すること」が規定されているところ，「名古屋市行政情報ネットワーク運用管理要領」及び「名古屋市インターネット接続運用管理要領」を定め，総務局企画部情報化推進課長をネットワーク管理者として，行政情報ネットワーク（既設ネットワーク）の運用管理を総括させている（乙２の１，弁論の全趣旨）。

ｂ 名古屋市における独自対策

ウィルスチェックサーバと連携して，市町村設置ファイアウォールを通過する通信について，ゲートウエイ型のウィルスチェックを行わせており，発見したウィルスは駆除若しくはファイルごと削除を行っている。また，インターネットとの接続点付近に，侵入検知装置を設置し，既設ネットワーク及びその接続点とのファイアウォールに侵入しようとする通信を監視している（乙４８，証人Ｐ２）。

ｃ インターネットとの接続状況に関する外部監査の結果

名古屋市は，平成１５年８月１１日，庁内ＬＡＮと接続している公開サーバ，庁内ＬＡＮとインターネットとの接続点に設置されたルータ及びファイアウォールについて監査法人トーマツの外部監査を受けた。外部監査では，ポートスキャン，各種自動スキャンツール，各種脆弱性検出スクリプト及び担当者へのヒアリングが行われた（インターネットから庁内ＬＡＮへの侵入などの実験は行われなかった。）。その結果，ファイアウォールには特段の脆弱性は発見されなかったが，公開サーバに脆弱性があり，インターネットからの不正アクセスによって，サービス拒否状態にさせられたり，攻撃者から任意のコマンドを実行されたりする危険性が発見された。特に電子メールサーバには，使用されているプログラムにバッファオーバーフローの脆
弱性があるため，適切なバージョンにアップグレードすることが必要であると指摘された（甲２７）。

これを受けて，名古屋市は，同月２０日及び２１日に，電子メールサーバのプログラムをアップグレードした（乙２４，２５）。

ウ 要約

上記のとおり，名古屋市はセキュリティ基準にのっとった制度面及び技術面におけるセキュリティ対策を講じている上，これに独自のセキュリティ対策を上乗せしていること，その有効性につき，適宜に外部監査を受け，その結果に基づいた改善措置を講じていること，インターネットと既設ネットワークとが接続される点についても一応セキュリティが確保されていることなどにかんがみると，名古屋市における住基ネットの運用においては，住基法が予定している以上のセキュリティが確保されており，少なくとも住基ネットを通じた情報の漏えい等の可能性が高いとはいえない。

エ 原告らの主張の検討

この点について，原告らは，名古屋市は政令指定都市の中で唯一，住基ネットが庁内ＬＡＮを経由してインターネットと接続しており，セキュリティに重大な危険性があると主張するところ，証拠（甲２９，６７，６８，証人Ｐ２）及び弁論の全趣旨によれば，平成１５年８月１２日から同月２０日にかけて，名古屋市の庁内ＬＡＮに接続するパソコン２８台が，コンピュータウィルスＢｌａｓｔｅｒに感染したこと，感染の原因は，名古屋市の職員３人が，名古屋市行政情報ネット

ワーク運用管理要領の定める承認を得ず，無断でＰＨＳカードないし固定電話でインターネットと既存ネットワークとを接続したため，パソコン３台が感染し，その後，庁内ＬＡＮを通じて感染が拡大した（なお，同ウィルスの感染の際に，住基ネットと既設ネットワークとの切離しは行われなかった。）ものであること，以上の事実が認められる。

しかしながら，上記事故は，当該職員が定められた手順を逸脱したことによりもたらされたものであって，住基ネットそのものがセキュリティ上の問題点を内包しているとはいえないばかりか，前記のとおり，名古屋市は，インターネットと既設ネットワークとの接続点に侵入監視装置を設置していること，ＣＳと中間サーバの間，中間サーバと既設ネットワークとの間にそれぞれファイアウォールを設置していること，平成１５年８月１１日の監査法人トーマツによる監査結果を受けて，電子メールサーバの使用するプログラムの更新を行う（乙２５）などの対応を行っていること，さらに，上記の事故によってもウィルスは既設ネットワークから住基ネットに伝染することはなく，実害の発生はなかった上，名古屋市総務局情報化推進課は，直ちに各局区室に対し，無許可での接続禁止等の対応策を周知徹底するよう指示している事実が認められること（甲６７），これらを総合すれば，社会通念上，インターネットの接続点からの攻撃に対しても，現時点における技術水準に対応した保護措置が講じられていると認められ，少なくとも，インターネットの接続点からの攻撃により，住基ネットを通じた個人情報の漏えい等の可能性が高いとまではいえない。

(5)　小括

上記の検討結果によれば，名古屋市が発行を予定している住基カードや，その構築した住基ネット本体は，セキュリティ上の問題点があって，情報漏えい等の危険性が相当程度高く，およそ住基法が予定しているものとかけ離れた性能しか有しないとはいえない。したがって，住基カードの原盤購入契約や印字機械リース契約の締結行為等は，その余について判断するまでもなく，違法，無効なものとはいえないから，本件公金支出等が違法となることもないと判断するのが相当である。

５　争点(4)（住基ネットはほとんど効用がないから，住基カードの発行に公金を支出することは，最少経費・最大効果を定めた地方自治法２条１４項及び地方財政法４条１項に違反するか）について

改正法附則７条は，「市町村長，都道府県知事及び指定情報処理機関は，施行日前においても，新法第４章の２に規定する事務（住基ネットを利用した本人確認情報の処理及び利用等）の実施に必要な準備行為をすることができる。」と規定しているところ，法３０条の４４第１項，２項は，住民は市町村長に対して自己に係る住基カードの交付を求めることができ，交付申請があったときは市町村長は住基カードを交付しなければならない旨定めているから，市町村長が住基カードの発行等のためにその原盤カードを購入し，必要な機器のリースを受け，これに要する費用を支出するなどの行為を行うことは，住基法が当然に予定している（むしろ義務付けている）ところと解される。

したがって，本件において，Ｐ１市長が，予算に計上された金額の範囲内で，一般競争入札において最低価格を入札した業者との間で上記各契約を締結し，その給付を受けて代金を支出すること（乙１，２７の１・２，２８ないし３１，３２ないし４２の各１ないし３，４３）は，法律の施行に必要な財務会計行為として，適法というべきである。

この点について，原告らは，被告の主張する住基ネット及び住基カードの効用（住民票写しの広域交付や提出の不要化，転入転出特例，公的個人認証サービス等の行政サービスの向上と行政事務の効率化）はほとんどなく，したがって，本件公金支出は地方自治法２条１４項及び地方財政法４条１項に違反する旨主張する。

しかしながら，住基ネットの構築によってどの程度の行政サービスの向上と行政事務の効率化がもたらされるか，それが果たして投入される導入費用，維持費用と釣り合うものであるかなどの問題は，改正法の審議過程で論議されるべき問題であり，これが成立して施行される以上，法律で定められた事務を処理することを義務付けられた市町村長が判断すべき事項でないといわざるを得ない（被告の主張するように，地方自治法２条１４項が訓示規定にとどまるかどうかはさておき，同項及び地方財政法４条１項が，住基カードの市町村長の交付義務を定めた法３０条の４４の上位規範たる性質を有するものでないことは明らかである。）。

そうすると，単に住基ネット及び住基カードの効用が乏しいことを理由に，

本件公金支出が違法であるとの原告らの上記主張は，それ自体失当というべきであり，採用できない。

６　結論

よって，原告らの本訴請求は，その余について判断するまでもなく理由がないから，いずれも棄却することとし，訴訟費用の負担について行政事件訴訟法７条，民事訴訟法６１条，６５条１項を適用して，主文のとおり判決する。

名古屋地方裁判所民事第９部

裁判長裁判官　　加藤幸雄

裁判官　　舟橋恭子

裁判官　　尾河吉久