平成１８年１２月１１日判決言渡　同日原本領収　裁判所書記官

平成１７年(ネ)第１５４号　住民基本台帳ネットワーク差止等請求控訴事件

（原審：金沢地方裁判所平成１４年(ワ)第８３６号，平成１５年(ワ)第１１４号）

口頭弁論終結の日　平成１８年６月１２日

判　　決

当事者の表示　　別紙当事者目録記載のとおり

主　　文

1　原判決中，控訴人ら敗訴部分を取り消す。

2　被控訴人らの請求をいずれも棄却する。

3　訴訟費用は，第１，２審とも，被控訴人らの負担とする。

事実及び理由

第１　当事者の求めた裁判

1　控訴人ら

主文第１，２項と同旨

2　被控訴人ら

本件各控訴をいずれも棄却する。

第２　事案の概要

1　本件は，控訴人石川県内の市町村に住民登録をしている被控訴人らが，平成１１年法律第１３３号による改正後の住民基本台帳法に基づく住民基本台帳ネットワークシステムの導入により，被控訴人らのプライバシー権（自己情報コントロール権），氏名権及び行政権力による包括的管理からの自由が侵害されたとして，上記各権利に基づき，(1)控訴人石川県に対し，①住民基本台帳法３０条の７第３項の別表第一の上欄に掲げる国の機関及び法人に対する，被控訴人らに関する本人確認情報（被控訴人らの氏名，住所，生年月日，性別の４情報及び被控訴人らに付された住民票コード並びにこれらの変更情報）の提供禁止，②控訴人財団法人地方自治情報センターに対する，被控訴人らに関する

同法３０条の１０第１項記載の本人確認情報処理事務の委任禁止，③控訴人財団法人地方自治情報センターに対する，被控訴人らに関する上記本人確認情報の通知禁止，④その保存する住民基本台帳ネットワークの磁気ディスク（これに準ずる方法により一定の事項を確実に記録しておくことができるものを含む。以下同じ。）からの被控訴人らに関する上記本人確認情報の削除を請求し，(2)控訴人財団法人地方自治情報センターに対し，⑤控訴人石川県から受任した被控訴人らに関する住民基本台帳法３０条の１０第１項記載の本人確認情報処理事務の禁止，⑥その保存する住民基本台帳ネットワークの磁気ディスクからの被控訴人らに関する上記本人確認情報の削除を請求するとともに，(3)控訴人らに対し，⑦控訴人石川県に対しては国家賠償法１条１項に基づき，控訴人財団法人地方自治情報センターに対しては民法７０９条に基づき，それぞれ，慰謝料１０万円及び弁護士費用１万円の合計１１万円並びにこれに対する訴状送達日の翌日（被控訴人[redacted]及び被控訴人[redacted]につき平成１５年４月１日，その余の被控訴人らにつき同年１月１７日）から支払済みまで民法所定の年５分の割合による遅延損害金の連帯支払を求めた事案の控訴審である。

原審は，被控訴人らの上記①ないし⑥の各請求をいずれも認容し，上記⑦の請求を棄却したところ，控訴人らが本件控訴を提起した。したがって，上記⑦の請求は当審における審判の範囲外である。

なお，略語は，控訴人財団法人地方自治情報センターを「控訴人センター」とするほか，特に断らない限り，原判決に準ずるものとする。

２　前提事実

次の(1)のとおり補正するほかは，原判決の事実及び理由の第２，２に記載のとおりであるから，これを引用するが，次の(2)及び(3)において改正法の概要及び住基ネットの概要を要約摘示する。

(1) 原判決の補正

ア　原判決１１頁１７，１８行目の「拡大された。」を「拡大され，現在（

当審の口頭弁論終結日）では２７５事務となっている。」と改める。

イ　原判決２２頁１３行目と同１４行目との間に次のとおり加える。

「　なお，横浜市は，平成１８年５月１０日，横浜市本人確認情報等保護審議会から，住基ネットの安全性が稼働当初と比較して格段に高まっており，現時点において問題はない旨の同年４月付け答申を受けて，横浜市の住民全員について住基ネットに参加することを表明した（乙５９，６０）。」

(2) 改正法の概要

住民基本台帳法は，改正法（平成１１年法律第１３３号）により次のとおり改正された。

ア　都道府県知事は，その区域内の市町村の市町村長ごとに，当該市町村長が住民票に記載することのできる住民票コード（住基法７条１３号）を指定し，これを当該市町村長に通知する（住基法３０条の７第１項）。市町村長は，新たにその市町村の住民基本台帳に記録されるべき者につき住民票の記載をする場合において，その者がいずれの市町村においても住民基本台帳に記録されたことがない者であるときは，都道府県知事から指定された住民票コードのうちから選択するいずれかの１つの住民票コードを住民票に記載する（住基法３０条の２第２項前段）。都道府県知事は，指定情報処理機関に上記住民票コードの指定及びその通知を行わせることができる（住基法３０条の１０第１項１号）。都道府県知事及び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，これを所定の期間保存する（住基法３０条の５第３項，３０条の１１第３項）。

イ　市町村長は，都道府県知事に本人確認情報を通知する（住基法３０条の５）。

ウ　都道府県知事は，住基法の定める場合に，住基法所定の国の機関・法人等へ本人確認情報を提供する（住基法３０条の７）。

エ　都道府県知事は，指定情報処理機関に対し，国の機関・法人等への本人

確認情報の提供等の本人確認情報処理事務を委任することができる（住基法３０条の１０第１項)。

オ　委任都道府県知事は，本人確認情報を指定情報処理機関に通知する（住基法３０条の１１第１項)。

カ　本人確認情報の通知及び提供は，原則として相互の電子計算機間を電気通信回線を通じて送信することにより行う（住基法３０条の５第２項，３０条の７第７項，３０条の１１第４項等)。

キ　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（改正法附則１条２項)。

(3) 住基ネットの概要

改正法は，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，被控訴人らの各居住する，控訴人県内の各市町村においても，住基ネット（住民基本台帳ネットワークシステム）が導入された。その概要は次のとおりである。

ア　被控訴人らの居住する市町村の長は，住基法に基づき，被控訴人らの住民票を作成し，氏名，住所，生年月日，性別等の個人情報を電子計算機（以下「サーバ」という。）に記録し，管理している。改正法により，控訴人県の知事から委任を受けた控訴人センターは，市町村長が住民票に記載することのできる住民票コードを指定して市町村長に通知し，市町村長は，指定された住民票コードのうちから選択するいずれか１つの住民票コードを住民票に記載した。市町村は，被控訴人らに関する個人情報が記録された既存のサーバを住基ネット専用のコミュニケーションサーバ（以下「ＣＳ」という。）に接続し，これを電気通信回線を通じて控訴人県のサーバに接続した。これにより，被控訴人らの居住する市町村の長は控訴人県の知事に，同知事は控訴人センターに，本人確認情報を通知している。控訴人センターは，住基法の定める場合に，住基法所定の国の機関・法人等に

対して本人確認情報を提供している。

イ　控訴人県は，自己のサーバを電気通信回線を通じてＣＳに接続し，通知された本人確認情報を自己のサーバの磁気ディスクに記録して保存するとともに，控訴人県の知事が事務を委任した控訴人センター（控訴人センターは，総務大臣から住基法３０条の１０第１項の「指定情報処理機関」の指定を受けている。）に対し，本人確認情報を通知した。これにより，控訴人センターは，住基法の定める場合に，住基法所定の国の機関・法人等に対し，本人確認情報を提供している。

ウ　控訴人センターは，控訴人県の知事から電気通信回線を通じて各市町村長から通知された本人確認情報の通知を受け，その情報を磁気ディスクに記録し，所定期間保存するとともに（住基法３０条の１１第１項，３項），通知を受けた本人確認情報を国の機関又は法人等に提供する業務を行っている。

エ　被控訴人らの居住する各市町村長は，平成１４年８月５日以降，被控訴人らに対し，住民票コードを通知し，同日から住基ネットの本運用が開始された。

3　当審における争点及びこれに関する当事者の主張

(1) プライバシー権（自己情報コントロール権）侵害の有無

次のとおり補正するほかは，原判決の事実及び理由の第３，３(1)に記載のとおりであるから，これを引用する。

（原判決の補正）

ア　原判決２９頁１９行目から３０頁３行目までを次のとおり改める。

「(ｳ)　上記各情報のうち，氏名，住所，生年月日及び性別の４情報はそれ自体が重要な情報であるというだけではなく，その下に記録保存等された個人情報に分け入っていく上での索引・検索情報として機能するものであるから，要保護性が高い。変更情報も，身分上の重要な変動が生じた

ことを推知させるものとして要保護性が高い。そして，簡便かつ正確に個人情報を検索できるマスターキーとなり得る住民票コードが付されることにより，一体とされた個人情報が全国ネットワークである住基ネット上に流通させられることにより，被控訴人らのプライバシーが侵害され，又はその侵害の具体的危険にさらされることになる。」

イ　原判決３７頁８行目と同９行目との間に次のとおり加える。

「　そもそも被控訴人らは，住民票の写しの広域交付という利便性よりも，自らのプライバシーの権利の保持を望むのであるから，このような被控訴人らに対し，住民の利便性を根拠として住基ネット導入の必要性を基礎付けることはできない。」

ウ　原判決３７頁１１行目の「すぎない。」を「すぎず，その利用率も極めて低いから，住基カードが有用であるとはいえない。」と改める。

エ　原判決３７頁２２行目と同２３行目との間に次のとおり加える。

「　控訴人らは，被控訴人らが住基ネットに参加しないことによる支障につき，原審裁判所から再三にわたり求釈明を受けたにもかかわらず，必要がないものとして，何ら主張しない応訴態度に終始していたのであるから，そのような控訴人らが，当審になってこの点に関する主張をにわかに行うことは禁反言の法理に反する。仮にそうでないとしても，控訴人らの主張する，被控訴人らが住基ネットから離脱することによって生じる支障とは，極めて抽象的なものであるばかりか，いずれも住基ネットの運用を開始してしまったことを前提とするところ，被控訴人らが住基ネットの運用の中止を求めたにもかかわらず，これを強行したのであるから，自らの強行によって築いたシステム等に支障が生じることを根拠に住基ネットの正当性を基礎付けることはできず，また，住基ネット自体が許容されるか否かが問われているにもかかわらず，これを予め正しいものとして前提とする立論であるから，控訴人らの主張は失当であ

る。

(カ) 以上によれば，改正法中住基ネットに関する規定は，少なくとも住基ネットに不参加を表明し，あるいは住基ネットからの離脱を表明して，本人確認情報の提供に同意していない住民に適用し，これを運用する限り，憲法１３条に違反して無効である。」

オ　原判決３７頁２４行目と同２５行目との間に次のとおり加える。

「　被控訴人ら主張の自己情報コントロール権なる権利は，実定法上の根拠がなく，また，実質的に考えても，その内容，範囲，法的性格に関して様々な見解があり，権利としての成熟性が認められないから，実体法上の権利とはいえない。また，住基法は，住基ネットの運用により，被控訴人らの権利が侵害されることのないよう十分な立法措置を行っており，行政機関とその構成員たる公務員も法令の遵守義務を負うのであるから，住基ネットの運用により被控訴人らの権利が侵害され，その侵害の程度が重大で，被控訴人らが回復困難な損害を被るおそれがあるとはいえないから，被控訴人らの差止等請求は棄却されるべきである。その具体的な主張は次のとおりである。」

カ　原判決４０頁１行目の「プライバシー侵害の事実」を「プライバシーの侵害又はその具体的危険の不存在」と改める。

キ　原判決４０頁６行目末尾に次のとおり加える。

「そもそも，被控訴人ら主張の本人確認情報のうち４情報（氏名，住所，生年月日及び性別）は，社会通念上，秘匿を要する程度が高いとはいえないし，住民票コード及び変更情報についても，前者は住民票に付された１１桁の数字であり，後者も上記４情報が変更した旨の情報であって，およそ個人の人格的自律などにかかわらない客観的・外形的事項に関するものであって，思想，信条など個人の道徳的自律に関係する人格権の内容を成すものではないから，これらの本人確認情報について被控訴人らのプライバ

シー権を侵害するものとはいえず，その具体的危険も存在しない。」

ク　原判決４０頁１３行目の「いえない。」を「いえず，その具体的危険も存在しない。」と改める。

ケ　原判決４３頁１５行目の「講じており」から同１７行目の「よって」までを「講じているから」と，同１８行目の「危険性」を「具体的危険性」と，それぞれ改める。

コ　原判決４７頁４行目から同１７行目までを次のとおり改める。

「(カ)　被控訴人らが住基ネットから離脱することによって生ずる支障

住基法は，住基ネットのシステム上ですべての本人確認情報がもれなく提供，利用されることを当然の内容として立法されており，住基ネットが，国の機関等，都道府県，市町村で本人確認情報を共有することにより，行政コストの削減等を図ることを一つの重要な行政目的としているのであって，一部でも不参加があると，本人確認情報の共有がなされなくなるから，国の機関等などにおいて，従来のシステムや事務処理を存置せざるをえないこととなり，法の予定する効果を達成することは不可能になる。また，住基ネットは，市町村間をネットワーク化し，住民基本台帳事務の広域化，効率化を図ることを一つの重要な行政目的としているところ，不参加者を認めることになれば，上記ネットワークが寸断され，他の市町村の効率化が阻害されていることは明らかである。このような事態は法のおよそ想定するところではなく，情報通信技術を利用して住民サービスの向上と行政事務の効率化を図ることを目的とした改正法の意義を没却し，住基ネットの存在そのものを否定することになる。

したがって，被控訴人らが住基ネットから離脱することにより重大な支障が生ずる。」

(2)　氏名権侵害の有無

（被控訴人らの主張）

ア　氏名は，人の同一性を示すものとして人格と密着するものであるから，氏名により呼称され，氏名によって扱われることは，氏名権として憲法１３条により保障される。

イ　住基ネットは，個人の情報を住民票コードという番号をもとにして流通させ，個人の特定を氏名ではなく番号によって行うものであり，また，異なる行政分野にまたがり番号が共通化されることと相まって，行政担当者は個人の氏名よりも番号を重視することになり，個人の人格の同一性を表す中核となる氏名を住民票コードで分類される個人情報の一つにおとしめるものである。さらに，個人を番号によって扱うこと，特に全国民に住民票コードをその生涯にわたって付すことは，氏名を中核とする個人のアイデンティティ又はその感覚を害するものである。したがって，住基ネットは被控訴人らの氏名権を侵害する。

（控訴人らの主張）

争う。確かに，氏名については，不法行為法上の保護を受けうる人格的利益を有するものである。しかし，住民票コードは，特定の住民の本人確認を確実かつ効率的に行うために使用される１１桁の番号であって，住基ネットを稼働させる上で必要不可欠な情報（記号）であり，住民基本台帳に記載された４情報を電子計算機及び電気通信回線を用いて効率的に送信させるために，技術上新たに設けられた符号にすぎず，個人の人格的価値とは無関係である。よって，本件住民票コードの記載により，およそ被控訴人らの人格権も人格的利益も侵害したとはいえないから，被控訴人らの上記主張は失当である。

(3) 公権力による包括的管理からの自由侵害の有無

（被控訴人らの主張）

ア　国民個人は，他人によって自己の人格的自律に関わる個人情報を収集さ

れないこと，又はその他の個人情報から自己の人格的自律に関わる個人情報を推知されないことを前提として，その理性又は感性等に主体的に従って自己決定をなすことができ，自由に行動することができる。ところが，公権力による包括的管理（各行政機関において，それぞれ個別に保有する国民個人に関する情報を，他の行政機関と交換する等して有機的に結合し，いつでも利用できる状態におくこと）は，このような個人の基本的な意思決定や行動（特に公権力にとって不都合な思想，公権力に対する批判的行動等）を著しく萎縮させることになるから，人格的自律の存在として自己を主張し，そのような存在であり続ける上で必要不可欠な利益として，公権力による包括的管理からの自由も，憲法１３条により保障される。

イ　住基ネットにおける住民票コードは，全国民を確実に識別するために付されたものであり，また，今後，住民票コードの利用が可能な事務が無限定に拡大されていくことが予想され，個人の全生活分野において住民票コードを基点として様々な個人情報が蓄積され，かかる個人情報を公権力が事実上無制限な利用目的をもって一元的に管理することを可能とするものである。したがって，住基ネットは，被控訴人らの公権力による包括的な管理からの自由を侵害する。

（控訴人らの主張）

争う。被控訴人らは，住民票コードが総背番号制としての役割を果たす旨主張するが，行政機関が住民票コードを利用する場合には目的外利用の禁止，告知要求制限等の規定により利用が制限されており（法３０条の３４，３０条の４２及び３０条の４３），さらに，居住関係の確認を行うためにのみ利用されるものであり（法３０条の７第３項），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をすることは禁止されているのであり，共通番号としては機能しないものである。

なお，住民票コードを付さないと，①氏名や住所の記載が住民基本台帳上

の記載と異なる場合にアクセスできない，②処理の際にサーバに大きな負荷がかかる，③氏名及び住所が同一の場合には同一人物か否かが確認できない，④行政機関が保有する情報が最新のものでない場合に，これに基づいてアクセスするためには，住基ネット内に本人確認情報の過去の履歴を保存しておく必要があり，効率的でない等の不都合があり，住民票コードは住基ネットに不可欠である。

(4) 被控訴人らの請求に係る差止等の必要性，許容性の有無

（被控訴人らの主張）

住民個々人は，自己に関する個人情報の収集・取得，管理（保有）・利用，開示・提供のすべてにつき，情報主体としてコントロールする権利を有するのであるから，情報主体の同意も法令上の根拠もないまま，行政機関がこれを違法に占有している場合には，その原状回復を請求できるところ，被控訴人らの情報が住基ネットに提供される限り，被控訴人らの権利の侵害という違法状態が継続しているのであるから，被控訴人らは，この違法状態からの回復として差止等請求ができる。

（控訴人らの主張）

争う。プライバシーについては，上述のとおり，その概念自体が不明確であり，統一的理解を得られていないことから，現段階においては，名誉権と異なり，プライバシーを保護する利益を排他性を有する絶対権ないし支配権としての人格権であるとして差止めが容認される状況にはなく，プライバシーの侵害のみを理由として差止請求を認めることはできない。仮にそうでないとしても，差止請求が認められるためには，差止請求の根拠となる権利侵害の程度が重大であり，権利者が著しく回復困難な損害を被るおそれがあることが必要であるところ，住基ネットの導入により，被控訴人らの権利が侵害される具体的危険は存在しないから，被控訴人らが著しく回復困難な損害を被るおそれがあるとはいえず，被控訴人らの請求に係る差止等の必要性も

ない。

第３　当裁判所の判断

１　認定事実

前記前提事実並びに証拠（乙２８，後記各証拠）及び弁論の全趣旨によれば，住基ネットに関して，次のとおり認められる。

(1) 住基ネットの目的等

住基ネットは，住民サービスの向上と行政事務の効率化を目的として設けられたシステムであり，大別して次の実現事項を予定している。

ア　市町村の区域を越えた住民基本台帳に関する事務の処理

(ア) 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。）以外の市町村長に対し，自己又は自己と同一の世帯に属する者に係る住民票の写しで住基法７条５号，９号から１２号まで及び１４号に掲げる事項の記載を省略したものの交付を請求できる（住基法１２条の２第１項）。この請求を受けた市町村長は，住所地市町村長との間で，電気通信回線を通じて各使用に係る電子計算機に必要事項を送信通知し，住民票の写しを作成し，交付する（同条第２項ないし第５項）。このように，住基カードなどを窓口で提示することにより，全国どこの市町村でも，本人や世帯の住民票の写しの交付が受けられるようになる。

(イ) 転入・転出の特例処理

転入届をする者は，前住所地の市町村長が作成する転出の証明書を添付することが必要であり（住基法２２条２項，施行令２３条），住民は，転出証明書の交付を受けるため，転出地の市役所・町村役場に出向く必要があるが，住基カードの交付を受けている者が付記転出届をした場合には，最初の転入届については，転出証明書の添付を要しない（住基法

２４条の２第１項)。つまり，住基カードの交付を受けている場合は，他の市町村に引っ越したときでも，付記転出届を転出地市町村に郵送すれば,転出地市町村の窓口に出向いて転出証明書を受け取る必要がなく，転出証明書に記載されている情報を電子情報として市町村間で送信するので，転入地市町村窓口に１回出向いて住基カードを添えて転入届を提出することで足りる。

イ　法律で定める行政機関（国，地方公共団体等）に対する本人確認情報の提供

住基ネットにおいて，法律で定める行政機関（国，地方公共団体等）に対して本人確認情報が提供されることにより，各種手続の簡素化が図られる。たとえば，①住基法別表に規定されている本人確認情報の提供及び利用が可能な多数の事務について，住民票の写しの提出が不要となり，②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の受給者が，毎年提出していた現況届又は身上報告書の提出が，加給年金額対象者等を除き，不要となり，③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恩給受給者は，同申立書の提出が不要となる。

ウ　住基カードの活用

(ア)　住基カードの交付を受けると，上記アの住民票の写しの広域交付や転入・転出の特例処理が利用できる。

(イ)　市町村が条例で定めるところにより，カードメモリの空き領域を活用して必要な情報を記録し，印鑑登録証明事務，福祉サービス，公共施設の利用予約等，多目的に独自の行政サービスを行うことができる。

(ウ)　市町村等の窓口において，住基ネットを通じて，居住する市町村の住民であることを確認できる。

(エ)　写真付きの住基カードは，市町村民証明書として活用することが可能

となる。

(オ) 電子政府，電子自治体の基盤となること

我が国においては，平成９年に内閣により打ち出された「ミレニアム・プロジェクト」により電子政府の基盤構築がなされることとなり，平成１２年７月には，いわゆるＩＴ革命の恩恵をすべての国民が享受でき，国際的にも競争力を持つ「ＩＴ立国」の形成を目指すため，政府全体での総合的な施策を推進するＩＴ戦略本部が内閣に設置され，同年８月には，自治省における「ＩＴ革命に対応した地方公共団体における情報化推進本部」から，各地方公共団体において高度な情報通信技術の便益を最大限活用し，情報化施策を推進するに当たり留意すべき事項について報告がなされ，これらを受け，平成１３年１月６日からは，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して「高度情報通信ネットワーク社会形成基本法」（平成１２年法律第１４４号）が施行された。同法は，高度情報通信ネットワーク社会を形成するために，国には，高度情報通信ネットワーク社会の形成についての基本理念にのっとり，高度情報通信ネットワーク社会の形成に関する施策を策定し，実施する責務を，地方公共団体には，基本理念にのっとり，高度情報通信ネットワーク社会の形成に関し，国との適切な役割分担を踏まえて，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，実施する責務を課した。

ＩＴ戦略本部は，平成１３年３月に発表した「ｅ－Ｊａｐａｎ重点計画」において，「我が国が５年以内に世界最先端のＩＴ国家となる」ことを目標に掲げ，同年６月に「ｅ－Ｊａｐａｎ２００２プログラム」，同年１１月に「ｅ－Ｊａｐａｎ重点計画，ｅ－Ｊａｐａｎ２００２プログラムの加速・前倒し」，平成１４年６月に「ｅ－Ｊａｐａｎ重点計画－２００２」を発表し，平成１５年８月８日には「ｅ－Ｊａｐａｎ重点

計画－２００３」を発表するなど，政府の行うべき施策を定めた各種計画を策定し，政府においてその実施がなされている。

上記「ｅ－Ｊａｐａｎ重点計画－２００３」においては，行政サービスとして，行政に関する手続につき，３６５日２４時間ノンストップで，関連手続の申請・届出等の案内情報の入手から実際の手続までをインターネットにより一元的に行うことのできる総合的なワンストップサービスの仕組みを平成１７年度末までに整備することを目標として掲げている（乙５，６，弁論の全趣旨）。

(カ) 今後も，公的個人認証サービスに活用したり（電子署名に係る地方公共団体の認証業務に関する法律参照），申請・届出等手続のオンライン化に活用することが可能となる。

(2) 個人情報保護のための対策等

住基ネットは，住民の個人情報を取り扱うことから，個人情報の保護が重要な課題とされており，制度面，技術面及び運用面にわたり，次のような個人情報保護のための対策が講じられている。

ア 制度面

(ア) 保有情報の制限

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

(イ) 本人確認情報の利用及び提供の制限等

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も限定されている（住基法３０条の６，３０条の７第３項ないし第６項，３０条の８，別表）。また，本人確認情報の提供を受ける者に対し，目的外の利用又は提供が禁止され（住基法３０条の３４。この規定は，行政機関の保有する個人情報の保護に関する法律８条３項により，同条２項に優先して適用されるものである。），都道府県知事及び指定情報処理機関に対し

ても，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（住基法３０条の３０）。さらに，市町村長その他の市町村の執行機関は，住基法に規定された事務等で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，遂行のため必要のある場合を除き，住民票コードの告知を求めることが禁止されている（住基法３０条の４２）。

市町村長等以外の者は，何人も，自己と同一の世帯に属する者以外の者に対し，当該第三者又は当該第三者以外の者に係る住民票に記載された住民票コードを告知することを求めたり，その者が業として行う行為に関し，その者に対し売買，貸借，雇用その他の契約の申込みをしようとする第三者若しくは申込みをする第三者又はその者と契約の締結をした第三者に対し，当該第三者又は当該第三者以外の者に係る住民票に記載された住民票コードを告知することを求めたり，業として，住民票コードの記録されたデータベースであって，当該住民票コードの記録されたデータベースに記録された情報が他に提供されることが予定されているものを構成したりすることが，いずれも禁止されている（住基法３０条の４３第１項ないし３項）。

(ウ) 秘密保持義務

役職員等（住基法３０条の１７第１項第２項），本人確認情報の電子計算機処理等に従事する市町村又は都道府県の職員等（住基法３０条の３１第１項第２項），本人確認情報の電子計算機処理等に従事する受領者の職員等（３０条の３５第１項ないし第３項），住民基本台帳に関する調査に関する事務に従事している者又は従事していた者（住基法３５条）は，その事務に関して知り得た本人確認情報に関する秘密又は本人確認情報の電子計算機処理等に関して知り得た秘密を漏らしてはならないこととされ，各秘密保持義務に違反して秘密を漏らした者に対しては，

懲役刑又は罰金刑を科すこととされている（住基法４２条，４５条）。

(エ) 安全確保義務

都道府県知事又は指定情報処理機関が，所定の本人確認情報の電子計算機処理等を行うに当たって，当該本人確認情報の漏えい，滅失及び毀損の防止その他の当該本人確認情報の適切な管理のために必要な措置を講じなければならないとされ（住基法３０条の２９），その受領者等についても，同様に，受領した本人確認情報の漏えい，滅失及び毀損の防止その他の本人確認情報の適切な管理のために必要な措置を講じなければならないこととされている（住基法３０条の３３）。

(オ) 国又は都道府県の指導

国は都道府県及び市町村に対し，都道府県は市町村に対し，住基法の規定により都道府県又は市町村が処理する事務について，必要な指導を行うものとされ，また，主務大臣は都道府県知事又は市町村長に対し，同事務について必要があると認めるときは，報告を求め，又は助言若しくは勧告をすることができることとされている（住基法３１条１項２項）。さらに，総務大臣は，本人確認情報処理事務等の適正な実施を確保するため必要があると認めるときは，指定情報処理機関に対し，監督上必要な命令をすることができ，委任都道府県知事は，指定情報処理機関に対し，本人確認情報処理事務等の実施に関し監督上必要な命令をすることができ，委任都道府県知事も，指定情報処理機関に対し，本人確認情報処理事務の適正な実施のために必要な措置を講ずべきことを指示することができることとされている（住基法３０条の２２第１項第２項）。

(カ) 報告及び立入検査

総務大臣は，本人確認情報処理事務等の適正な実施を確保するため必要があると認めるときは，指定情報処理機関に対し，本人確認情報処理

事務等の実施の状況に関し必要な報告を求め，又はその職員に，指定情報処理機関の事務所に立ち入り，本人確認情報処理事務等の実施の状況若しくは帳簿，書類その他の物件を検査させることができ，委任都道府県知事も，指定情報処理機関に対し，本人確認情報処理事務の実施の状況に関し必要な報告を求め，又はその職員に，当該本人確認情報処理事務を取り扱う指定情報処理機関の事務所に立ち入り，当該本人確認情報処理事務の実施の状況若しくは帳簿，書類その他の物件を検査させることができることとされている（住基法３０条の２３第１項，２項)。

(キ) 第三者機関による本人確認情報の保護

都道府県に本人確認情報の保護に関する審議会を置き，同審議会は，住基法の規定によりその権限に属させられた事項を調査審議するほか，都道府県知事の諮問に応じ，当該都道府県におけ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都道府県知事に建議することができ（住基法３０条の９)，また，指定情報処理機関には，本人確認情報保護委員会を置き，同委員会は，指定情報処理機関の代表者の諮問に応じ，本人確認情報の保護に関する事項を調査審議し，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（住基法３０条の１５)。

(ク) 自己の本人確認情報の開示等

何人も，都道府県知事又は指定情報処理機関に対し，磁気ディスクに記録されている自己に係る本人確認情報について，書面により，その開示を請求でき，都道府県知事又は指定情報処理機関は，開示請求があったときは，開示請求をした者に対し，書面により，当該開示請求に係る本人確認情報について開示しなければならず（住基法３０条の３７第１項第２項)，同開示を受けた者から，書面により，開示に係る本人確認情報についてその内容の全部又は一部の訂正，追加又は削除の申出があ

ったときは，遅滞なく調査を行い，その結果を当該申出をした者に対し，書面で通知することとされている（住基法３０条の４０）。

イ　技術面

(ア)　ネットワークのセキュリティ対策

各市町村にはＣＳが設置され，ＣＳのネットワーク側には，指定情報処理機関が２４時間体制で監視を行うファイアウォール（以下「ＦＷ」という。）が設置され，ＣＳと既存住基システム（既存庁内ＬＡＮ）を回線により接続する場合には，ＣＳと既存住基システムの間に市町村設置のＦＷが設置される。ＣＳ，都道府県サーバ及び全国サーバを結ぶ電気通信回線は，専用回線が使用され，すべてのＣＳの全国及び都道府県ネットワーク側，すべての都道府県サーバの全国及び都道府県ネットワーク側並びに全国サーバの全方向に指定情報処理機関監視ＦＷも設置されている。このように，ネットワークの物理的・論理的隔離が行われているほか，通信の暗号化，電子記録媒体の暗号化，通信相手相互認証及びログ取得と監査によるネットワーク上の通信への不正対策や，ネットワーク機器での不正アクセス対策及び不審な通信パターンの監視によるネットワークへの不正アクセス・不正侵入対策がとられている。

(イ)　システムのセキュリティ対策

端末の不正利用・不正操作防止として，操作者用ＩＣカード認証，ログイン認証が行われる。重要情報への不正アクセス防止として，アクセス制御，不審な業務パターンの常時監視，ログ取得と監査，電磁波漏えいの防止が行われている。その他，暗号鍵の不正対策やコンピュータウィルス対策も行われている。

(ウ)　住基カードのセキュリティ対策

住基カード交付時にはセキュアＩＣカード交付方式がとられ，未交付カードの盗難による不正利用対策として，輸送鍵の設定やパスワード設

定によるカード有効化の措置がとられている。また，カードのなりすまし対策として，相互認証機能，パスワード照合・カードロック機能，カードの一時停止措置がとられているほか，カードの偽造・改ざん対策として，耐タンパー機構や強制アクセス制御機能を持たせるように構成されている。

ウ　運用面

(ア)　本人確認情報管理規程

指定情報処理機関は，本人確認情報管理規程に基づき，入退室管理規則や本人確認情報取扱規則を定めることとされている。

(イ)　セキュリティ対策に関する指針

各地方公共団体は，住基ネットの運営に係る責任体制，監査体制を確立し，セキュリティ組織規程，入退室管理規程及び委託管理規程等の規程を整備することとされている。

(ウ)　緊急時対応計画

指定情報処理機関及び各地方公共団体は，それぞれ緊急時対応計画を定めることとされている。

(エ)　教育・研修

地方公共団体においては，住基ネットの稼働前に，セキュリティ対策等についての教育・研修を行い，本人確認情報の提供を受ける行政機関においても，同様の教育・研修を行うこととされ，指定情報処理機関がこれに協力することとされている。

エ　上記アないしウを踏まえた住基ネットシステムのセキュリティ対策及びその検証結果は，次のとおりである。

(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（乙１０，１１）

a　ＣＳ，都道府県サーバ，全国サーバ間の通信は，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，また，全国サー

バと国の機関等のサーバ間では，専用回線ないし記憶媒体のやりとりによる情報交換が行われる。

上記専用回線は，ＶＰＮ（バーチャル・プライベート・ネットワーク）によるもので，物理的に独立した回線ではなく，他の通信と共用の通信回線において，暗号により他の通信と独立した回線を形成するものである。

b　住基ネットにおける情報通信に際しては，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る通信相手の認証を行っている。

c　住基ネットにおいては，住基アプリケーションによる独自の通信プロトコル（データ通信におけるデータ受送信のための手順や規則のこと）による通信を行っており，インターネットで用いられている汎用のプロトコルを使用していない。そして，指定情報処理機関監視ＦＷにおいてインターネットで使用さ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　控訴人センターは，指定情報処理機関監視ＦＷについて，ネットワーク側への不正通信，ネットワーク側からの不正通信の有無につき２４時間の監視体制をとり，また，ネットワーク内にＩＤＳ（侵入検知装置）を設置して常時監視を行っている。

e　ＣＳ端末において住基ネットアプリケーション（以下「住基アプリ」という。）を立ち上げるためには，ＣＳ端末のＯＳの権限のほかに，住基アプリの専用カードと暗証番号が必要とされている。

(イ)　総務省告示による住基ネットのセキュリティ基準について（乙１の１ないし３）

総務省は，施行規則２条，６条，７条，１０条ないし１４条及び１８条ないし２０条までの規定に基づき，セキュリティ基準を定めて平成１

４年８月５日から適用し，その後，同基準を総務省告示第３９１号及び同６０１号で改正し，同６０１号は平成１５年１０月１日から適用された（以下，同６０１号による改正後の上記基準を「現行セキュリティ基準」という。）。

現行セキュリティ基準により，住基ネットにおいては，秘密保護措置として，上記記載のほか，都道府県，市町村及び指定情報処理機関において次のような措置が講じられている。

a　体制，規程等の整備

都道府県知事，市町村長及び指定情報処理機関に対し，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の設置，異常の早期発見，連絡のための体制整備，住基ネットの企画，開発，運用に関する規程及び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の整備，住基ネット運用のための職員配置及び適切な人事管理，同職員に対する教育・研修計画の策定・実施，住基ネットのセキュリティ対策の評価及び改善努力をそれぞれ義務づけ，また，緊急時の体制として，住基ネットが構成機器やソフトウェアの障害により作動停止した際や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の策定，そのための連携及び研修の実施を義務づけている。

b　重要機能室について

電子計算機室や磁気ディスク保管室は専用の部屋を確保し，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で施錠保管することとしたほか，電子計算機室や磁気ディスク保管室等の重要機能室について，侵入防止のための各種措置をとることとされている。

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の限定及び管理，鍵または入退室管理カードの管理，重要機能室への搬入物品の確認や，事務室における職員不在時の施錠等の措置が義務づけられている。

(b) ソフトウェア開発等の管理

住基ネットシステムの開発，変更時におけるセキュリティ確保，不正行為の防止等が義務づけられている。

(c) 住基ネットシステムの管理

住基ネットを運用する職員には必要なアクセス権限を付与し，電気通信関係装置の管理につき不当な運用防止のため厳重な確認を行い，管理者権限がない者の操作を防止する措置を講じ，ネットワーク経由の模擬攻撃を適宜実施してその結果に基づき必要な措置を講じ，また，セキュリティ対策に関する情報の収集，分析を実施して必要な措置を講じることとされている。

(d) 端末機，電子計算機の管理

端末機の取り扱いは，管理責任者の指示ないし承認を受けた者のみが行うこととし，アクセス権限を有していることの操作者識別カード及び暗証番号による確認，操作者確認カード及び暗証番号の適切な管理，電子ファイルの利用制限，操作履歴の記録保存，本人確認情報照会の条件設定，複数回の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こととされ，また，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ェア以外のソフトウェアを作動させないこととされている。

(e) 磁気ディスクの保管

磁気ディスクについては保管庫等を設置して保管し，磁気ディスク盗難防止のため，持ち出し及び返却の措置，磁気ディスクによる

本人確認情報の送付の際の保管状況の確認等の措置を講じることとされている。

(f) 構成機器及び関連設備の管理

構成機器及び関連設備についても，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じることとされている。

(g) データ等の管理

データやプログラム，ドキュメントの管理についても，使用，複写，消去，廃棄等における適切な管理体制，データの入出力時の適切な管理等が要求されている。

(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の整備，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こととされている。

(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，業者に委託する際には，委託先事業者の社会的信用と能力を確認し，セキュリティ対策実施や不正行為防止のための監督を行い，再委託の制限，分担範囲の明確化等の措置を講じることとされている。

d 既設ネットワークとの接続

住基ネットと既設のネットワークを接続する場合には，既設ネットワークについてもセキュリティ対策を行い，接続状況について相互に連絡調整を行うこととされている。

e 住基ネットの運用

(a) 市町村においてＣＳに記録された本人確認情報について，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

後に確実に消去することとされ，また，都道府県サーバ及び全国サーバにおける本人確認情報についても，施行令３０条の６又は３０条の１１規定の期間経過後に確実に消去することとされている。

(b) また，国の機関等に本人確認情報を提供する際には，都道府県知事に，国の機関等と，本人確認情報の漏えい，滅失，毀損の防止その他適切な管理のための措置について協議することとされ，本人確認情報の提供を受ける国の機関等についても，本人確認情報の適切な管理のための措置を講じることとされている。

(c) 必要に応じて，都道府県知事（この項において，指定情報処理機関に対し委任した都道府県知事を含む。）は国の機関等及び当該都道府県の執行機関に対し，都道府県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都道府県知事，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説明を求め，その実施の要請を行うこととされている。

(d) 自己に係る本人確認情報の提供又は利用の状況に関する情報の開示請求に適切に対応するため，都道府県知事は，本人確認情報を提供した際及び自己が利用した際には，その状況に係る情報を必要な期間保存することとされる（指定情報処理機関に対し事務委任をした都道府県知事は，指定情報処理機関に上記状況の報告を求めた上で，同様の措置をとることとされる。）。上記期間経過後は同情報を確実に消去することとされている。

(ウ) 各市町村のセキュリティ対策に対する自己点検

各市町村は，「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票」に基づき，住基ネットにおけ

るセキュリティ確保について，各項目ごとに３点満点とする数十項目の自己点検を実施した。その結果は，平成１５年５月１２日時点で計３２０７団体の平均点が２．４８点，同年８月２５日時点で同じく２．８３点，平成１６年１１月２４日時点で計２９５９団体の平均点が２．８８点であった（乙１１，３３）。

(エ) 住基カードに関する情報について（乙１３）

総務省は，平成１５年５月２７日，施行規則４６条の規定に基づき，住基カード技術的基準を定め，同基準は平成１５年８月２５日から適用された。同基準によれば，住基カードの運用に際し，次のとおり，住基カードに関する情報が通知ないし提供されることとなっている。

a　市町村長は都道府県知事に対し，委任都道府県知事は指定情報処理機関に対し，市町村長，都道府県知事又は指定情報処理機関は，国の機関等に対し，それぞれ，住基ネットを通じ，当該住民の住基カードの運用状況が運用中，一時停止又は廃止の状況にあることを通知する。

b　住基カードの発行を受けている住民の住民基本台帳がある市町村以外の市町村が本人確認情報の提供を受ける際には，都道府県知事又は指定情報処理機関は，住基カードの有無について通知する。

(オ) 長野県侵入実験について（乙１９，甲共３２の１ないし４，甲共３３の１ないし４，甲共３９，４１）

a　長野県は，平成１４年１２月に発足した長野県本人確認情報保護審議会が，平成１５年５月に県に提出した「長野県本人確認情報保護審議会第１次報告」を受け，住基ネットにおいて，インターネット側から市町村の庁内ネットワークを経由した住基ネットシステムへの不正アクセス及び住基ネットシステムからの本人確認情報漏えいの可能性を確認し，有効な対策を講ずるための資料を得ることを目的として「住基ネットに係る市町村ネットワークの脆弱性調査」を実施すること

とし，平成１５年９月２２日から同年１０月１日まで第一次調査を，同年１１月２５日から同月２８日まで第二次調査を実施した（以下，第一次，第二次調査をあわせて「長野県侵入実験」という。）。

長野県侵入実験及びその調査結果の概要は次のとおりである。

b　調査方法

(a)　市町村の庁内ＬＡＮから住基ネットへの侵入（内部からの侵入）とインターネットから庁内ＬＡＮへの侵入（外部からの侵入）の２種類の調査を行った。

(b)　内部からの侵入調査

庁内ＬＡＮに調査用コンピュータを接続して庁内ＬＡＮ及び庁内ＬＡＮ上に存在する各種サーバについての情報を収集し，その情報をもとにサーバの管理者権限奪取を試みた。管理者権限を奪取した既存住基サーバから既存住基サーバ・ＣＳ間の市町村設置ＦＷについての情報を収集するとともに，既存住基サーバに偽装した調査用コンピュータによりＣＳとの通信を試みた。また，ＣＳセグメントに接続した調査用コンピュータにより，ＣＳ及びＣＳ端末についての情報を収集し，既知の脆弱性を利用してＣＳ及びＣＳ端末の管理者権限奪取を試みた。

(c)　外部からの侵入調査

遠隔地からインターネットを経由してＦＷ及びＤＭＺ（非武装セグメント，ＦＷを経由した場所に置かれているＬＡＮセグメント）に置かれた公開サーバについての情報を収集し，得られた情報をもとに公開サーバへの侵入を試みた。

(d)　留意事項

調査対象自治体において実際に稼働しているコンピュータ・システムに関して実施した。また，不正アクセス行為の禁止等に関する

法律への配慮から，全国の都道府県の委託を受けて控訴人センターが管理している部分，すなわちＣＳの都道府県ネットワーク方向にある指定情報処理機関監視ＦＷから上流部分については調査対象とはしなかった。

c　下伊那郡阿智村における第一次調査（平成１５年９月２２日から同月２４日）

事前に既存住基サーバ及び庁内ＷＥＢサーバのＩＰアドレス（コンピュータ識別のため割り当てられた番号）について情報を得た上，役場サーバ内のＨＵＢ，隣接する施設の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調査した。結果は次のとおりであった。

(a)　庁内ＬＡＮのネットワークに調査用コンピュータで接続することができた。

(b)　その後，既存住基サーバ及び庁内ＷＥＢサーバの管理者権限を奪取することができた。

(c)　庁内ＬＡＮとＣＳの間にある市町村設置ＦＷを通過可能な通信によってはＣＳの管理者権限を奪取することはできなかった。なお，ＣＳの管理者ポートが庁内ＬＡＮ側に向け開放されていたが，同ポートを利用して市町村設置ＦＷの権限奪取ないし無効化が可能かどうか確認しなかった。

d　同第二次調査（平成１５年１１月２５日から同月２８日）

ＣＳが格納されている役場サーバ室内のラックを開錠し，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調査した。結果は次のとおりであった。

(a)　ＣＳの管理者権限を奪取することができた。また，ＣＳに保存されている住基ネットのデータベースにアクセスし，当該市町村の住

民の住基ネットデータを閲覧することができた。

(b) ＣＳ端末には適切なパッチが当てられていてその管理者権限を奪取することはできなかった。管理者権限を奪取したＣＳのＩＤとパスワードを使用したところ，ＣＳ端末の管理者権限を奪取することができたが，住基アプリを改めて起動することができるかどうか，住基アプリが正規に起動している状況でＣＳ端末の操作を遠隔で行い住基アプリを操作できるかどうかについてはいずれも確認しなかった。

e 諏訪郡下諏訪町における調査

平成１５年９月２５日及び２６日に調査が実施された。事前に既存住基サーバのＩＰアドレスについて情報を得た上，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に接続して調査した。結果は次のとおりであった。

(a) 庁内ＬＡＮのネットワークに調査用コンピュータで接続することができた。

(b) その後，既存住基サーバ及び庁内ＷＥＢサーバの管理者権限を奪取することができた。

(c) 庁内ＬＡＮとＣＳの間にある市町村設置ＦＷに脆弱性は認められず，また，ＣＳの管理者権限を奪取することはできなかった。

f 東筑摩郡波田町における調査

平成１５年９月２９日から同年１０月１日まで調査が実施された。事前に対象ネットワークのＩＰアドレスについて情報を入手した上，遠隔地（東京）からインターネット経由で接続して調査した結果，インターネットとＤＭＺ間のＦＷと兼用になっているＤＮＳサーバ（ホスト名とＩＰアドレスの対応情報を保有するサーバ）に脆弱性はなく，上記ＦＷを通過することのできる通信によっては，公開サーバの管理