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被告地自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にタ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（端末機に自動的にＩＰアドレスを割り当てるサーバ）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，公開サーバの管理者権限を奪取することはできなかった。

(カ) 品川区におけるペネトレーションテスト（乙１２）

被告地自センターは，平成１５年１０月１０日及び翌１１日，品川区の協力を得て，住基ネットの機器に対するペネトレーションテスト（ネットワークへの侵入実験）を実施した（実際のテストは，クロウ社（Crow Chizek and Company LLC）が実施）。総務省は，同テストの結果について，次のとおりであるとの発表をした。

a 住基ネットーＣＳ間のＦＷ（指定情報処理機関監視ＦＷ）について，ＣＳセグメントから３時間のテストを実施したが攻略できず，脆弱性も見いだせなかった

b ＣＳー庁内ＬＡＮ間のＦＷ（市町村設置ＦＷ）について，庁内ＬＡＮセグメントから６時間のテストを実施したが攻略できず，脆弱性も見いだせなかった

c　庁内ＬＡＮ上のＣＳ端末に対し庁内ＬＡＮセグメントから６時間のテストを実施したが，ＣＳ端末の権限奪取できず，弱点も見出せなかった

イ　前記前提事実及び上記認定事実によれば，次のようにいうことができる。

(ｱ)　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についてみるに，前記のとおり，電気通信にはＶＰＮによる専用回線が使用され，ＣＳと既存庁内ＬＡＮとの間，ＣＳと専用回線との間，都道府県サーバと既存庁内ＬＡＮとの間，全国サーバと専用回線との間，全国サーバと国の機関等のサーバとの間にはそれぞれＦＷが設置され，さらに，ネットワーク上にはＩＤＳが設置されるなどのセキュリティ対策が講じられており，これらのセキュリティが破られる抽象的な危険性が無いとはいえないが，具体的な危険性が存在するとまでいうことはできない。

この点，原告らは，長野県侵入実験において，住基ネットのセキュリティ上の不備が具体的に明らかになった旨主張するが，上記(7)ア(ｵ)記載の事実によれば，長野県侵入実験の結果は，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者権限を奪取することはできなかった，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端末の管理者権限奪取はできなかった，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し，またＣＳ端末の管理者権限を奪取できたが，住基アプリを任意に操作できるかについては実験を行わなかったというものであって，同実験においては，様々な制約があったとはいえ，設置されているＦＷ越しの攻撃は全て失敗しており（①，②），また，管理者権限を奪取し得たのは，庁舎内ないし隣接建物において物理的に

端末に接続して実験した場合（②，③）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ができるかは実証されていないし，その場合でも，住基アプリを任意に操作できるかについても実証されていない（②，③）から，結局，長野県侵入実験においては，住基ネット内における本人確認情報その他の情報の漏洩，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できない。

なお，品川区において実施された上記ペネトレーションテストについては，同テストの内容の詳細が不明であり，評価を行うことはできない。

(イ) 住基ネットのソフトウェアその他運用面についてみるに，前記のとおり，種々の制度ないし運用基準が定められており，一定の個人情報保護措置が講じられていると評価することができる。

しかしながら，定められた個人情報保護措置が全国３０００の市町村で確実に実施されるか疑問であり，次々と発表されるＯＳのセキュリティーホールに対するパッチを速やかに当てることができるかすら疑問である。また，いわゆるソーシャルエンジニアリングに対する対策が行われていることについては何ら証拠がない。これらは，住基ネットに特有の問題ではなく，すべてのネットワークに共通の問題であるが，住基ネットの扱うデータの量が膨大であり，漏洩したり，改ざんされればその結果は深刻であるだけに，これらの点についても万全の対策をとるべきものである。

(ウ) 以上を総合すると，上記(イ)に示したように疑問はあるものの，本訴において，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，同情報が漏洩する具体的危険性があることが立証されたとまでいうのは困難である。

(8) 通知，保存，提供の態様が個人の人格的自律を脅かす危険の有無，程度

ア　前提事実で記載したように，住基ネットは，市町村長が本人確認情報を都道府県知事に通知し，都道府県知事が，国の機関や法人，他の都道府県や市町村の執行機関等に対して本人確認情報を提供するものであるが，都道府県知事は，これらの提供事務等を，総務大臣が指定した指定情報処理機関である被告地自センターに委任している（法文上は，「都道府県知事は，指定情報処理機関に本人確認情報処理事務を行わせることができる」と規定されているが，現実には，すべての都道府県知事が被告地自センターに上記事務を行わせている。）。

これによって，すべての住民の本人確認情報は，被告地自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，都道府県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，同年１２月６日に成立した行政手続きオンライン化３法によって，２６４事務に拡大された。提供を受ける事務は，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。提供される本人確認情報には，住民票コードが含まれている。すなわち，被告地自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る。しかし，それだけに止まらず，これによって，行政機関が持っている膨大な個人情報がデータマッチングされ，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される危険性が飛躍的に高まったというべきである。

なお，行政機関では，従前から住民に対して，年金番号，運転免許証番号，健康保険証番号等，様々な番号を付番してきた。しかし，これらの限定された範囲内で使用される番号と異なり，住民票コードは，あらゆる行政事務に利用されうるものであるから，従前の番号とは質的に異なるとい

わなければならない。

また，住民は，住民票コードの記載の変更を請求できる（第２の２の(3)のイ）が，変更してみても，本人確認情報に変更情報が含まれるから，住民票コードのマスターキーの役割に影響を与えない。

イ　なるほど，住基法では，本人確認情報の受領者には，当該本人確認情報の提供を求めることができる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旨が定められている（第２の２の(6)のイの(イ)，法３０条の３４）。しかし，これがデータマッチングや名寄せを禁ずるものであるか否かは文言上判然としない上，仮にそうだとしても，その違反行為に対する罰則は定められていないし，第三者機関の監視のシステムもないから，その実効性は疑わしい。また，行政機関における個人情報の取扱については，「行政機関の保有する個人情報の保護に関する法律」が平成１７年４月１日から施行されているが，これによれば，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（同法３条２項）が，その利用目的と相当の関連性を有すると合理的に認められる範囲内では利用目的を変更することができる（同法３条３項）し，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）が，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情報を内部で利用する場合であって，当該保有個人情報を利用するについて相当の理由があるとき，あるいは，他の行政機関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には，当該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場合を除き，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，又は提供することが許容

されている（同法８条２項２号，３号）から，同法も，上記のデータマッチングや名寄せを防止できるとする根拠にはなり得ない。

ウ　また，住民が住基ネットの便益を享受するために必要な住基カードは，ＩＣカードで，大容量のデータ蓄積機能があり，氏名，住所，生年月日，性別，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，更に，市町村長その他の市町村の執行機関は，条例によって，住基カードを様々な目的に使用できる。市町村が提供するサービスとしては，①証明書自動交付機を利用して，住民票の写し，印鑑登録証明書その他の証明書の交付を受けるサービス，②申請書を自動的に作成するサービス，③検診，健康診断又は健康相談の申込，結果の照会等を行うサービス，④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を医療機関等に提供するサービス，⑤災害時等において，避難者情報の登録，避難場所の検索等を行うサービス，⑥公共施設の空き照会，予約等を行うサービス，⑦図書館の利用，図書の貸出等を行うサービス，⑧健康保険，老人保健等の資格確認を行うサービス，⑨介護保険の資格確認等を行うサービス，⑩高齢者等の緊急通報を行うサービス，⑪病院の診察券等として利用するサービス，⑫商店街での利用に応じ，ポイント情報を保存し，これを活用するサービス，⑬公共交通機関の利用に係るサービス，⑭地域通過，電子福祉チケット等に係るサービス，⑮公共料金等の決済に係るサービス等が考えられている（弁論の全趣旨）。

しかし，住民が住基カードを使って各種サービスを受ければ，その記録が行政機関のコンピュータに残るのであって，これに住民票コードが付されている以上，これも名寄せされる危険がある。なお，上記のとおり，住基カード技術的基準では，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から，上記危険を否定することはできない。

エ　行政機関は，住民個々人について膨大な情報を持っているところ，これらは，住民個々人が，行政機関に届出，申請等をするに当たって，自ら開示した情報である。住民個々人は，その手続に必要な限度で使用されるとの認識のもとにこれらの情報を開示したのである。ところが，これらの情報に住民票コードが付され，データマッチングがなされ，住民票コードをマスターキーとして名寄せがなされると，住民個々人の多面的な情報が瞬時に集められ，比喩的に言えば，住民個々人が行政機関の前で丸裸にされるが如き状態になる。これを国民総背番号制と呼ぶかどうかはともかくとして，そのような事態が生ずれば，あるいは，生じなくとも，住民においてそのような事態が生ずる具体的危険があると認識すれば，住民１人１人に萎縮効果が働き，個人の人格的自律が脅かされる結果となることは容易に推測できる。そして，原告らが上記事態が生ずると具体的危険があると認識していることについては相当の根拠があるというべきである。

(9)　(6)ないし(8)の検討の結果によれば，本人確認情報の一部は秘匿を必要とする程度が相当高いし，住基ネットのセキュリティは，不正アクセスや情報漏洩の具体的危険があるとまではいえないものの，抽象的な危険は否定できないものであるし，住基ネットの運用によって個人の人格的自律を脅かす具体的な危険があるから，住基ネットの運用によるプライバシーの権利の侵害は，相当に深刻であるというべきである。そこで，これらの事情を踏まえ，住基ネットのシステムを運用することがいかなる場合に許されるかを検討するに，住民が，プライバシーの権利を明示又は黙示に放棄した場合はこれが許されることが明らかであるが，プライバシーの権利を放棄していない住民との関係では，住基ネットの運用によって達成しようとしている行政目的が正当であること，住基ネットを運用することについて，住民のプライバシーの権利

を犠牲にしてもなお達成すべき高度の必要性があることを必要とするというべきである。そして，原告らは，住基ネットからの離脱を求めていてプライバシーの権利を放棄していないことが明らかであるから，以下，(10)において，住基ネットの目的の正当性について，(11)において，住基ネットの必要性について検討することとする。

(10) 住基ネットの目的の正当性について

ア 被告らが主張する住基ネットの目的は，次の(ア)ないし(エ)のとおりであるので，それぞれについて検討する。

(ア) 被告地自センターから行政機関に対して本人確認情報が提供されることによる住民負担の軽減と行政事務の効率化

本人確認情報の提供を受ける行政事務は，すでに２６４事務に及んでいる。これによって，住民側は，申請，届出，住民票の写しの添付等の負担が解消され，行政側としても，事務効率の向上や事務の正確性の向上が実現していることは容易に推測できる。もっとも，住民一人一人の立場から見た場合，これらの負担解消の程度がささやかであることは否定できない。

(イ) 住民基本台帳事務の簡素化，広域化による住民負担の軽減と行政事務の効率化

住民票の写しの広域交付及び転出・転入手続の簡素化が既に実現している（第２の２の(5)）。しかし，住民一人一人の立場から見た場合，住所地市町村以外の市町村で住民票の交付を受けることができるというメリットを享受する機会がどの程度あるか疑問である。また，転入届出の際に転出証明書の添付を要しないとしても，付記転出届をすることが必要であること（住基法２４条の２第１項），従前から転出届の郵送送付，転出証明書の郵送交付を利用して転出市町村に出頭しない方法があったこと，住民が転居する場合には，国民健康保険，介護保険等の様々な手

続のために転出地の市町村役場に出向く必要がある場合が多いこと等に鑑みると，そのメリットはさしたるものではない。

(ウ) 電子政府，電子自治体の基盤（行政手続のインターネット申請の実現）

a 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，同平成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