(イ) 被告県から通知を受けた原告らの本人確認情報を磁気ディスクに記録し，保存している。

（弁論の全趣旨）

第３　争点及びそれに対する当事者の主張

１　当事者の主張の骨子

(1) 原告らの主張の骨子

ア　原告らの住基ネットからの離脱（被告県及び被告地自センターに対する差止め請求）について

(ア) 憲法は，憲法が保障する人格権が侵害される危険性がある場合には，侵害をもたらす者に対する差止め請求権を認めている。

(イ) 被侵害権利

a　住基ネットの運用により，原告らのプライバシーの権利としての自己情報コントロール権が現に侵害されており，更に新たな侵害の危険性が存在する。

b　住基ネットは，原告らの氏名権を侵害している。

c　住基ネットは，原告らの「公権力による包括的管理からの自由」を侵害している。

(ウ) 上記各権利は，憲法１３条によって保障されている。原告らは，上記各権利に基づき，原告らの住基ネットからの離脱，すなわち請求の趣旨記載の差止めを求める。

イ　損害賠償請求について

(ア) 被告県の谷本知事は，住基ネットを運用することにより，原告らのプライバシーの権利，氏名権ないし「公権力による包括的管理からの自由」を侵害したもので，国家賠償法上違法である。

(イ) 被告地自センターは，住基ネットを運用することにより，原告らの上記各権利を侵害したもので，民法上の不法行為に該当する。

(ウ) 被告国の小泉内閣総理大臣は，「所要の措置」を講じるまでは改正法の施行を開始しない法的義務があったのに，これに違反し，「所要の措置」を講じないまま改正法を施行し，原告らの上記各権利を侵害したもので，国家賠償法上違法である。

(2) 被告らの主張の骨子

ア 差止め請求について（被告県，被告地自センター）

(ア) 差止め請求が認められるには，差止めができる排他的権利があること，権利侵害の危険性があること，差止めの必要性があることが必要である。

(イ) 自己情報コントロール権は憲法１３条で保障される権利とはいえないし，プライバシーの侵害のみを理由として差止め請求権は認められない。住基ネットのセキュリティ対策は十分なものであり，住基ネットによりプライバシー権の侵害の危険性があるとはいえない。

(ウ) 氏名権，「公権力による包括的管理からの自由」についての主張は争う。

イ 損害賠償請求について

(ア) 被告県

谷本知事の行為に何ら違法はない。

(イ) 被告地自センター

被告地自センターの行為に何らの違法はない。

(ウ) 被告国

小泉内閣総理大臣の行為に何ら違法はない。

2 主要な争点

(1) プライバシーの権利は憲法１３条によって保障されているか。住基ネットの運用が開始されたことにより，原告らのプライバシーの権利が侵害されたか。あるいはその危険性があるか。

(2) 氏名権及び「公権力による包括的管理からの自由」が憲法１３条によって

保障されているか。住基ネットの運用が開始されたことにより，原告らの氏名権及び「公権力による包括的な管理からの自由権」が侵害されたか。

(3) 被告県及び同地自センターが住基ネットを運用したことが違法か。

(4) 被告国が改正法を施行したことが違法か。

(5) 損害

3 主要な争点についての当事者の主張

(1) プライバシーの権利は憲法１３条によって保障されているか。住基ネットの運用が開始されたことにより，憲法１３条によって保障されている原告らのプライバシー権が侵害されたか。あるいはその危険性があるか。（争点(1)）

（原告らの主張）

ア プライバシー権は憲法上の権利であること

(ア) 社会の変革にともない，「個人の人格的生存に不可欠な権利自由」として保護するに値すると考えられるようになった権利，いわゆる「新しい人権」は，憲法１３条の「幸福追求権」として，憲法上保護される人権の一つと解されてきた。この幸福追求権によって基礎づけられる権利は，裁判上の救済を受けることができる具体的権利であると解すべきである。

プライバシーの権利は，このようにして認められた新しい人権の典型例とされており，判例，学説上も憲法１３条の保障する人格権の一つであることは異論がない。そして，プライバシーの権利については，個人的・消極的権利としての性格の強い「ひとりで放っておいてもらう権利」という概念から，より積極的な「自己に関する情報をコントロールする権利」という概念をも認める方向に理解されてきており，少なくとも広義のプライバシーの権利に，その重要な柱の一つとして，自己に関する情報をコントロールする権利が含まれることは明らかである。

すなわち，もともと個人の尊厳の原理から要求されるのは，個人の自律的な社会関係の形成を尊重することであり，公権力からこのような個人の自律領域が保護されなければ，個人の決定や行動に萎縮的効果が生じ，自己決定が阻害されることになる。そして，現代国家における積極国家・行政国家現象の進展に加え，情報化社会の進展，さらにはコンピュータによる情報処理技術の進展は，国家による個人の全面的管理という危険性を増大させるものであり，このような状況下において，立憲主義原理の維持・展開をはかることの重要性を認識し，個人の尊厳を左右するような個人情報に関する公権力の諸活動を憲法上の規律に服させることが意識されるようになったのであって，プライバシーの権利としての自己情報コントロール権は，新しい人権として，憲法１３条により保障された人権であるといえる。

(イ) 自己情報コントロール権の内容としては，他人に知られたくないと思う正当性のある自己の情報について，①収集・取得，②保有・利用，③開示・提供を自分でコントロールする権利が認められるべきであり，派生的には，④自己の情報の開示請求権・訂正請求権が認められなければならない。

そして，ここにいう「自己情報」とは，センシティヴ性の高低によって個人情報を二分し，センシティヴ性の高い情報のみが保護の対象となると考えるべきではなく，個人情報全てが保護の対象となると解すべきである。なぜなら，個人情報を二分し保護の度合いに強弱を付けることは，区別の基準及びその判断が容易でないし，前述のとおり，自己情報コントロール権が公権力から個人の自律領域を保護しようとするものであり，積極・行政国家化，情報社会化により公権力による個人の全面的管理の危険性が増大していることに鑑みれば，センシティヴ性の低さを理由として保護の対象から外すことは妥当でないからである。最高裁判

所の判例も，同様の判断を示している（最高裁判所平成１５年９月１２日判決・判タ１１３４号９８頁，以下「早稲田事件最高裁判決」という。）。

また，「公権力」による個人情報の取り扱いが問題となる場面は，私人間における表現の自由・知る権利との相互調整（「思想の自由市場機能」）等が必要とされるような場面ではなく，公権力の活動が事務処理の効率化等といった口実の下に，憲法の保障する基本的人権としてのプライバシーの権利を侵害する場面であるから，一個人の憲法上の人権の保障が十全になされることこそが求められるのであって，かかる公権力による個人情報の取り扱いが問題となる場面においては，あくまでも，情報主体のコントロール（意思決定）権が最大限に保障されなければならないというべきである（早稲田事件最高裁判決参照）。

(ウ) 審査基準について

公権力による個人情報の取り扱いが問題となる場面においては，個人の同意・承諾の有無が基本とされるべきであって，このような同意・承諾が存在しない場合には，その例外の要件（同意・承諾を得ることが不可能・困難であったという緊急性の要件，その場合の手段の相当性）について厳格な判断が求められるというべきである。そして，これら以外の，「個人情報の秘匿性の程度」，「具体的な不利益の不存在」，「公権力による収集等取り扱いの目的の正当性と必要性」といった要素についてはあくまでも付随的要素として位置づけられるべきである（早稲田事件最高裁判決参照）。

イ 住基ネットにより侵害されあるいは侵害される危険性のある原告らのプライバシーに関わる情報について

(ア) 住基ネットにおいては，次に述べる情報が取り扱われている。

a 市町村長から都道府県知事に，都道府県知事から被告地自センター

に通知され，それらのサーバ（以下，ＣＳ，都道府県サーバ及び全国サーバを合わせて「住基ネットサーバ」ともいう。）に記録・保存される本人確認情報（住基法３０条の５，７条）。

b　住基ネットサーバには，ａのほか，氏名のふりがなが記載され，また，平成１５年８月以降，住基カードに関する情報が記録・保存されている。

c　以上のほか，平成１５年８月以降，住基ネットの電気通信回線上を流れる情報は次のとおりである。

(a)　住民票の広域交付の際に必要な住民票記載事項情報として，本人確認情報のほか，世帯主，続柄，従前の住所及び届出年月日

(b)　他の市区町村へ転出する際の転出証明書情報として，本人確認情報のほか，世帯主であるかどうか，世帯主の氏名及び世帯主との続柄，戸籍の表示，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，国民年金の種別，国民年金手帳の記号及び番号，児童手当の受給の有無

d　以上に加え，現在１１省庁２６４事務に本人確認情報が利用されるため，これらの事務に使用されるサーバには，住民票コードと共にこれらの事務に関する個人情報が記録・保存される。

e　さらに，住基ネットシステムにおいては，従前市区町村が住民基本台帳を管理していたサーバと住基ネットサーバを接続し，他の市区町村のＣＳや既存住基台帳サーバ，都道府県のサーバ，被告地自センターのサーバとネットワークシステムを構築しているところ，上記既存住基台帳サーバには，住民基本台帳の全個人情報が記載されている（住基法７条）。

(イ)　上記の内容の情報は，原告らのプライバシーであって，これらのプライバシーが，後述のとおり，住基ネットの運用によって侵害され，ある

いは侵害の危険にさらされている。

ウ　プライバシー侵害の事実について

(ア)　本人確認情報については，住基ネット運用前は当該本人が所属する市区町村だけが保有しており，そのこと自体は地方自治の理念にもかなうものであったが，住基ネット運用により，本人確認情報が本人の同意を得ずして当該市区町村から全国に流通させられることにより，原告らは，自己の情報をコントロールすることが不可能となるのであって，住基ネットの運用は，直ちに原告らの自己情報コントロール権を侵害するものである。

さらに，原告らは，住基ネットにより，被告県及び同地自センターに保存された本人確認情報について，日本全国のいかなる機関・法人の，どの事務にどのような情報が提供されたかを知るすべがなく，これは，自己情報コントロール権のうち，自己情報の開示権を侵害するものである。

(イ)　氏名のふりがな，住基カードに関する情報及び本人確認情報の提供を受ける事務に関する個人情報についても，上記本人確認情報と同様，住基ネットの運用により原告らの自己情報コントロール権が現に侵害されている。

(ウ)　被告らは，本人確認情報は「プライバシー外延情報」であり，原則としてプライバシー保護の対象にならない旨主張する。

しかし，住基法の国会審議の際には，政府委員も，本人確認情報のうち４情報も，住民票コードと一体化した場合には全体として秘密事項，すなわちプライバシー事項となると答弁していること，早稲田事件最高裁判決においても同旨の判断がなされていることに加え，４情報とそれらの変更履歴とは不可分一体の形で本人確認情報の内容をなしていると解されるところ，変更履歴は，当該個人の私的な事情ないし出来事の存

在を推認させるものであり，まさに他人には秘匿しておきたい情報であって，典型的な「プライバシー固有情報」といえ，強く保護される必要がある。

エ　プライバシー侵害の危険性について

(ア)　立証責任について

本件のような国等の行政の施策による国民の権利侵害事案における主張立証責任については，民法の一般不法行為や差止め請求における主張立証責任とは別個に考えるべきである。

行政庁の裁量処分の取消訴訟等における行政庁の処分の違法性に関する主張立証責任については，主張立証責任の転換を認めた判決が複数存在するところ（最高裁判所平成４年１０月２９日判決・判時１４４１号３７頁［伊方原発事件］，名古屋高裁金沢支部平成１５年１月２７日判決・判時１８１８号３頁［もんじゅ事件］，金沢地裁平成６年８月２５日判決・判時１５１５号３頁［志賀原発差止め訴訟］），これらの裁判例をふまえ，主張立証責任については，被侵害利益の重大性，侵害行為の主体及び態様，証拠への距離等を総合考慮して，当事者間の公平の観点から，場合によって事実上の推定による主張立証責任の転換を図るべきである。

本件においては，被侵害利益はプライバシー権ないし人格権であり現代社会において重要な権利利益であること，侵害行為の主体は公権力であり，思想の自由市場の問題等を考慮する必要がなく権利侵害の有無につき厳格に審査されることが求められる場面であること，侵害の態様は，後述のとおりであって，住基ネットにおいてひとたびプライバシーが侵害された場合に回復不能な被害が生じること，住基ネットのセキュリティ対策についての資料は被告国らにおいて所持していること等を総合考慮すれば，本件における住基ネットによるプライバシー侵害の危険性に

ついての主張立証責任に関しては，原告らにおいてその危険性について一応の主張立証（潜在的な危険の主張立証）をなしたときは，被告らにおいて，これに対して相当の根拠を示して危険性のないことを具体的に主張立証すべきであり，これを被告らが行わない場合には，本件住基ネットはプライバシー侵害の危険があるものと事実上推認されるべきものとするのが妥当である。

(イ) 住基ネットにおける具体的なプライバシー侵害の危険性について

a 住基ネットにおける情報の流通と漏洩の危険について

住基ネットは，従来各市区町村内で収集取得され完結的に管理されてきた住民の個人情報が，コンピュータネットワーク上を流通するようにしたものであるところ，コンピュータネットワークにおいて流通する情報は，情報の大量蓄積・即時伝達を機能とするコンピュータを使用するシステムの性格上，いったん漏洩すれば，その情報が大量かつ網羅的に流出し，甚大な被害が発生するものであり，また，プライバシーはその性格上，いったん侵害されたらその回復は不可能である。そして，住基ネットにおいては，住民票コードによる名寄せが可能であることから，個人の情報の大量，包括的な入手集積がなされる危険性が飛躍的に高まっている。

b 想定される危険

(a) 外部からのネットワーク侵入の危険性

住基ネットは，ハッカー等によって，セキュリティの最も弱い部分から侵入され，原告らの個人情報が流出・漏洩し，悪用・改ざんされるなどプライバシー権を侵害される危険がある。

(b) 運用関係者等による漏洩等の危険

住基ネットの運用に関わる職員の不正行為，警察官らによる職権濫用による個人情報の収集のための住基ネットの利用，個人情報提

供先である国の機関・法人における個人情報の目的外利用，自治体が住基ネットシステムの開発・管理を委託した民間委託業者の不正行為，バックアップ用磁気テープその他のバックアップデータの盗難等，個人情報が漏洩する危険性が存在している。

c　セキュリティ対策の不備

以上のとおり，住基ネットの運用により原告らのプライバシーが侵害される危険が常に存在するところ，このような危険を防止するためのセキュリティが，ハード面，ソフト面の両方において，到底十分に講じられているということはできない。

(a)　ハード面のセキュリティ対策の不整備

本件住基ネットの安全対策としては，①専用回線，②ＦＷ，③ＩＤＳ（侵入検知装置）が挙げられているが，それらの実効性は疑わしい。

(b)　ソフト面のセキュリティ対策の不整備

運用関係者等による漏洩等の危険防止につき，「セキュリティポリシー」の設定，関係者への教育，関与者権限の明確化，使用記録保存，システムの第三者機関による事後監視等が必要であるが，住基ネットにおいてはこれらの制度が整備されていない。また，住基ネットシステムの保守管理等を委託された民間業者等を監視監査する人員・組織・方法も不備であり，この点についての総務省の指示通達は，予算措置や専門家の養成配備が伴っておらず，実効性がない。

(c)　市区町村には，システムの安全性やセキュリティに問題が生じた場合の調査・監査権限が与えられておらず，都道府県においては委任の範囲で一定の権限が認められているが実効性がない。

そして，被告地自センターは情報公開の対象とされていない団体

であり，同被告あるいはその職員が不正に個人情報を漏洩する等しても，原告ら国民が事後的に監視することは不可能である。

また，情報漏洩等があった場合に，都道府県及び市区町村が住基ネットの接続を切断することに関する規定が住基法上明定されていない。

(d) 住基法においては，国民の個人情報の保護の万全を期するため必要な「所要の措置」を講じることが義務づけられているが，後述のとおり，被告国は未だ何らの措置を講じていない。

(ウ) 長野県侵入実験

長野県は，平成１５年９月１日から同年１１月２８日までの間，長野県内において，「市町村ネットワークの安全性」に関する調査（以下「長野県侵入実験」という。）を行い，その結果，次のような事実が明らかになった。

a 既存住基システムやその他の個人情報を保存するコンピュータで構築される庁内ＬＡＮを外部からの侵入から守るインターネット側ＦＷを突破して庁内ＬＡＮに侵入することが可能であること，さらに，市町村設置ＦＷを突破してＣＳ端末やＣＳに到達することが可能であること

b 「操作者識別カード」や「パスワード」がなくともＣＳ端末やＣＳの管理者権限（アクセス権限）を奪取することが可能であること

c ＣＳの管理者権限が剥奪されても，被告地自センターは全く検知することができなかったこと

以上によれば，石川県以外の市町村のＣＳが乗っ取られて，住基ネットを介し原告らの本人確認情報や住民票上の情報が漏洩する危険，さらに，石川県内の市町村のＣＳあるいは既存住基サーバに不正侵入されることにより，原告らの本人確認情報の閲覧や改ざん，それらの情報の不