副　本

平成１４年(ワ) 第１６３０６号　住民基本台帳ネットワーク差止等請求事件

原　　告　　齋藤貴男

被　　告　　国　ほか３名

準 備 書 面 (7)

平成１６年４月２０日

東京地方裁判所民事第２５部甲２Ａ係　御中

被告国，同東京都及び同中野区指定代理人

武　笠　圭　志

池　原　桃　子

板　山　　久

飯　田　幸　司

被告国指定代理人

高　原　　剛

宇　野　雅　憲

上仮屋　　尚

百　武　和　宏

伊　藤　哲　也

松　谷　　朗

海　老　敬　子

被告東京都指定代理人

中　村　次　良

和久井　孝太郎 (代)
鈴木　清 (代)
小林　禮齊 (代)
武利　幸 (代)

被告中野区指定代理人

原田　憲治 (代)
齊藤　俊朗 (代)
白土　純 (代)
中谷　博 (代)

被告国，同東京都及び同中野区は，本準備書面において，原告の平成１６年１月１６日付け「準備書面（原告第７回）」（以下「原告準備書面(7)」という。），同日付け「準備書面（原告第８回）」（以下「原告準備書面(8)」という。）に対し，必要と認める範囲で反論する。

なお，略語等は，本準備書面で新たに用いるもののほかは，従前の例による。

第１　住基ネットのセキュリティについて

１　はじめに

(1) 原告は，住基ネットが運用されることにより，国民の個人情報は，漏洩，目的外利用・悪用，改ざんなどの具体的かつ現実的危険に直面させられている，住基ネットではセキュリティ対策が十分に講じられているとは言い得ない旨主張する（原告準備書面(2)１１ページ以下）。

しかしながら，被告らの平成１６年１月２７日付け準備書面(5)２４ページ以下で詳述したとおり，住基ネットは，制度面，技術面及び運用面における様々な措置を適切に講ずることにより，セキュリティの確保が図られているのであって，原告の主張は全く根拠がない。

(2) これに対し，原告は，原告準備書面(7)において，長野県が平成１５年９月２２日から同年１０月１日及び同年１１月２５日から同月２８日にかけて行ったとされる「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。）の結果により，①長野県の特定の市町村のＣＳサーバが乗っ取られて踏み台となり，住基ネット網を介して，被告中野区のＣＳサーバや被告財団法人のサーバ内にある原告の本人確認情報が漏洩する危険や住民票の広域交付の方法により原告の住民票上の情報が漏洩する危険があり，②全国の市町村にあるいずれかのＣＳが乗っ取られて，①と同様に，原告の本人確認情報や住民票上の情報が漏洩する危険があり，さらに③被告中野区のＣＳに直接不正侵入されることによって，原告の本人確認情報が閲覧，改

ざん等される危険や，被告中野区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があるなどとして，「住基ネットの安全性が極めて脆弱なものであって，原告の本人確認情報などのプライバシーが危機に瀕していることが明らかになった」（同準備書面２ページ）と主張する。

原告がかかる主張の主な根拠としているのは，長野県が平成１５年１２月１６日に速報として発表した「市町村ネットワークの安全性調査について（速報）」（甲第１２号証の１。以下「長野県調査速報」という。）及び同日の長野県知事田中康夫氏，長野県侵入実験を行った長野県本人確認情報保護審議会委員吉田柳太郎氏らの記者会見（甲第１２号証の２。以下「知事会見」という。）である。

なお，上記吉田柳太郎氏は，知事会見において，「来週中には，最終報告をお出し」する旨（知事会見２４ページ）述べ，同年１２月１６日から約１週間後に，長野県侵入実験の最終報告を公表すると明言していたが，実際には，実験から３か月も経過した平成１６年２月２９日になって，ようやく「住基ネットに係る市町村ネットワークの脆弱性調査最終結果について」（以下「長野県最終報告」という。丙第１７号証）が発表され，インターネットの長野県ホームページでも公表された。

(3) しかし，以下に詳述するように，長野県調査速報の公表及び知事会見は，全般的に，安全性が確認できた事実は正面から取り上げず，他方で，庁内ＬＡＮの脆弱性を住基ネットの安全性の問題であるかのようにすり替え，さらには，実験で確認していない事実を，さも侵入実験によって確認されたかのように述べるなど，住基ネットに関して公正な評価をしたものとは到底言えず，いたずらに国民の不安を煽るものと言わざるを得ない。むしろ，この長野県調査速報及び長野県最終報告によれば，長野県侵入実験により住基ネット本体（別添資料「長野県侵入実験結果」の指定情報処理機関が監視するフ

ァイアウォールから左側をいう。なお，同ファイアウォールについては，被告ら準備書面(5)３３ページ参照。）への侵入はできなかったこと及び被告財団法人において管理する本人確認情報への影響が全くなかったことが明らかとなり，長野県侵入実験によって，住基ネットの安全性がより明確になったと言うべきである。

(4) 原告の前記(2)の主張は，公正とは言い難い長野県による侵入実験の結果の公表（長野県調査速報及び知事会見）に基づく主張であり，まず，この点において失当である上，さらに，長野県の侵入実験が失敗に終わった箇所にまで，さもその実験が成功したかのように事実を歪曲して主張している点においても，失当である。

(5) そこで，以下，まず，長野県が公表している情報（長野県調査速報，知事会見及び長野県最終報告）から，長野県が侵入実験を行った経緯及び目的を述べた上で（後記２），その侵入実験の内容及び結果並びにその評価を述べ（後記３），さらに，侵入実験後に発表された長野県調査速報が，実験の客観的な内容や客観的な評価から乖離した信用性がないものであることを指摘する（後記４）。しかる後，原告が長野県「侵入実験の結果判明した事実」として指摘する事項についても検討を加え（後記５），長野県侵入実験の結果から，原告のプライバシーの侵害の具体的危険性があることが判明したとの原告の主張に反論する（後記６）。

なお，住基ネットの安全性とは別個の問題であるが，長野県最終報告で触れられている庁内ＬＡＮのセキュリティレベルの維持・向上についても，国として施策を積極的に引き続き講じていくこととしていることについて述べることとする（後記７）。

２　長野県侵入実験の経緯及び目的

(1) 長野県調査速報によると，長野県侵入実験は，平成１５年９月２２日から同年１０月１日（以下「第１次実験」という。）及び同年１１月２５日から

同月２８日（以下「第２実験」という。）にかけて行われたとされ，長野県側が公表した情報によると，かかる実験が行われた経緯は，以下のとおりである。

(2) 長野県は，「住民基本台帳法に基づく本人確認情報の保護に関する条例」を制定し（施行日平成１４年８月５日），同条例４条に基づき，法３０条の９第１項の規定に基づく本人確認情報の保護に関する審議会として，「長野県本人確認情報保護審議会」（以下「長野県審議会」という。）を設置した。

長野県審議会は，平成１５年５月２８日，「長野県本人確認情報保護審議会第１次報告」を発表したが（甲第３号証の１），その報告書の中で，住基ネットのセキュリティに関し，「審議会は市町村の調査を続け，さらに驚くべき事実に直面した。県下の２７の自治体でなんと，住基ネットとインターネットが物理的に接続されているのだ。この事態は真に重大であり，長野県下の自治体に内外からインターネット経由でアクセスが殺到し，情報が流出する恐れがある。そのような事になると，長野県民と県下の自治体のみならず，日本全国の自治体と国民全員が被るであろう被害は測りようがない。」（該当個所・甲第３号証の１・４ページ）と指摘し，住基ネットが物理的に庁内ＬＡＮと接続され，当該庁内ＬＡＮがインターネットと接続している団体（自治体）が存在していることを問題視した。

(3) 長野県は，かかる指摘に基づき，同年８月１５日に，「長野県の住基ネットに関する今後の方針」（丙第２２号証）を公式に発表した。

その中で，長野県側は，「住基ネットのセキュリティ対策」と称して，次のような方針を明らかにした。

「１　インターネット接続団体における侵入実験

数市町村を選定し，実際に侵入が可能かどうかを検証するための実験を行う。

２　インターネットに接続している２２自治体への対応

実験後，早急に分離の対策を実行するよう，また，分離が完了するまでは，住基ネットへの接続を，「媒体交換方式」とするよう求める。

3　県外のインターネット接続団体からの侵入の危険への対応

各都道府県へ，早急に分離がなされるよう依頼する。

4　このような無責任なシステムが構築された大きな理由は，住民自治を無視した国中心のシステム設計にある。このため，ＬＡＳＤＥＣ（引用者注：被告財団法人）に委任している事務を再検証し，市町村の意見を聞きながら，県の対応を検討する。」

(4) そして，長野県は，この「長野県の住基ネットに関する今後の方針」に基づき，長野県侵入実験を行ったとするが（長野県調査速報本文１ページ），長野県調査速報によると，その「調査の趣旨」として，「市町村ネットワークのさらなる安全性の確保のため，市町村の庁内ネットワークを通じた住基ネットシステムの不正アクセス及び住基ネットシステムからの情報漏洩の可能性の有無について確認するため」としている（甲第１２号証の１，１ページ）。

(5) このように，長野県は，一貫して，住基ネットが物理的に庁内ＬＡＮと接続され，当該庁内ＬＡＮがインターネットと接続している自治体が存在していることが危険であると主張していたものであり，長野県が行った実験は，インターネットから庁内ＬＡＮに侵入し，さらに住基ネットシステムに侵入することが可能であるかどうかを明らかにすることが真の目的であって，このような侵入形態に対するセキュリティが問題とされていたことが明らかである。

3　長野県侵入実験の内容及びその結果と評価

(1) 長野県侵入実験の内容及びその結果

長野県が平成１５年１２月１６日にした長野県調査速報は，簡単な速報であり，長野県侵入実験の具体的な手法や結果の詳細は全く明らかにされなか

った。

前記のように，長野県調査速報の発表と同時に行われた知事会見において，吉田柳太郎長野県審議会委員は，１週間内に最終報告を出すつもりであると明言していた（知事会見２４ページ）が，実験から３か月も経過した平成１６年２月２９日になって，ようやく長野県最終報告が出された。

しかし，この長野県最終報告によっても実験の具体的手法や結果の詳細が明らかにされているとは到底言い難いが，長野県調査速報，知事会見及び長野県最終報告を総合すると，長野県侵入実験の内容及びその結果は，おおむね以下のものであったと考えられる。

ア　第１次実験は，長野県阿智村，下諏訪町及び波田町において，実施された（長野県調査速報１ページ，長野県最終報告７ページ）。

(ｱ) 波田町の実験では，都内からインターネット経由で，インターネットと庁内ＬＡＮとの間のファイアウォールを突破して庁内ＬＡＮへの侵入を試みた（長野県最終報告８ページ，別添資料「長野県侵入実験結果」に①と記入）。

しかし，ファイアウォールを突破できず，庁内ＬＡＮへの侵入は失敗した（長野県調査速報８ページ（伊藤穣一氏の知事田中康夫氏への報告中，「インターネットからの侵入テストは成功しませんでした。」と記載。），同速報９ページ１３行目，知事会見４ページの最終行から５ページ１行目，長野県最終報告３－３（１０ページ））。

(ｲ) 阿智村及び下諏訪町の実験では，このファイアウォールを物理的に回避して，庁舎内に入り，攻撃端末を町村の庁内ＬＡＮにつなぎ，市町村設置ファイアウォール（被告ら準備書面(5)３４ページ参照）を突破して，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監視ファイアウォールにより通信制御されたＣＳ（被告ら準備書面(5)８ページ）が設置されるエリアをいう。以下同じ。）への侵入を試みた（長野

県最終報告２－１－１－１，２－１－２－１（７ページ），別添資料「長野県侵入実験結果」に②と記入）。

その結果について，長野県調査速報４ページでは，「通常の仕組発見」と意味不明の記述するだけで，いずれの報告にも成功の記載がなく，これも失敗したものと推察される。

(ｳ) また，阿智村及び下諏訪町では，第１次実験において，インターネットと庁内ＬＡＮとの間のファイアウォールを物理的に回避して，庁舎内に入り，市町村の庁内ＬＡＮにつないだ攻撃端末から，庁内ＬＡＮ上にある既存住基システムの機器の脆弱性を検査し，これを攻撃する実験を行った（長野県最終報告２－１－１－１，２－１－１－２，２－１－２－１，２－１－２－２（７ページ），別添資料「長野県侵入実験結果」に③と記入）。

その結果，既存住基システムの管理者権限を取得した（知事会見５ページ２５ないし３５行目，長野県最終報告３－１－２（９ページ））。

イ　第２次実験は，阿智村のみで実施された（長野県調査速報１ページ，長野県最終報告２－１－１－１（７ページ））。

この実験においては，前記「長野県の住基ネットに関する今後の方針」１で意図していたファイアウォール（①インターネットと庁内ＬＡＮとの間のファイアウォール，②市町村設置ファイアウォール及び③指定情報処理機関監視ファイアウォール）を突破することを目的とする侵入実験から機器自体を直接攻撃する実験だけに切り替えた。

すなわち，阿智村において，阿智村の許可を得て，重要機能室に立ち入り（同室は，厳重に入退室管理されており，容易にその中に立ち入ることはできない。），かつ，ラックの鍵を開け（厳重に施錠管理されており，容易に開錠することができない。），市町村設置ファイアウォールを物理的に回避して，攻撃端末をハブ（ＬＡＮケーブルの集線装置）につないだ

（長野県最終報告２－１－３－１（８ページ），別添資料「長野県侵入実験結果」に④と記入）。

その結果，ＣＳ及びＣＳ端末のＯＳの管理者権限を取得した（長野県調査速報６ページ，長野県最終報告３－２－２，３－２－３（１０ページ））。

なお，ＣＳ端末のＯＳの管理者権限の奪取の方法について，長野県調査速報では，セキュリティホールを攻撃したバッファー・オーバーフロー（bufferoverflow）によるものとしていたにもかかわらず（長野県調査速報１５ページ），長野県最終報告では，「管理者権限を奪取したＣＳで得られたデータを利用すること」によるもの（長野県最終報告３－２－３（１０ページ））と変更している。長野県最終報告では，かかる重要な事項について発表を変更した理由について，何ら説明されていない。

(2) 長野県侵入実験に対する評価

以上の長野県侵入実験の結果は，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セグメントへの侵入にことごとく失敗したものであり，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されたものであって，わずかに，一部の市町村において，庁舎内に人間が文字どおり物理的かつ違法に侵入した上，攻撃端末が接続された場合などに，市町村の庁内ＬＡＮ上にある当該市町村の住民の個人情報という限定された情報について漏洩，改ざん等の可能性があることが示されたにすぎない。

かかる評価をより具体的に述べれば，以下のとおりである。

ア　インターネット経由での庁内ＬＡＮへの侵入に失敗したこと及びいずれのファイアウォールも突破できていないこと

長野県侵入実験においては，長野県が当初意図していたインターネット経由での侵入は失敗し，①インターネットと庁内ＬＡＮとの間のファイアウォール，②市町村設置ファイアウォール及び③指定情報処理機関監視フ

ァイアウォールの合計３つのファイアウォールは，そのいずれも突破できていない。

住基ネットは，ファイアウォールの多重防御などにより高いセキュリティを確保しているが，この実験結果からは，むしろ住基ネットの安全性が明確となった。

イ　市町村設置ファイアウォールの攻略及び当該ファイアウォール越しのＣＳの攻略に成功していないこと

長野県侵入実験では，市町村設置ファイアウォールを通過する方法を発見したとしている（長野県調査速報６ページ，）。

しかし，長野県調査速報はもちろん，知事会見においても，その詳細は何ら明らかにされていない。佐藤千明委員は，知事会見において，「市町村調達ファイアウォールに関しては，仕掛けは分かりました。」（知事会見（甲第１２号証の２）２３ページ９行目）と述べているが，その詳細は明らかにされていない。

しかも，長野県最終報告では，この記載自体がなくなっている。

仮に，「通過する方法の発見」が，「通過を許可しているポートの判明」を意味するとすれば，通過を許可しているポートが分かったからといって，直ちに，ファイアウォールの攻略やファイアウォール越しにＣＳに対する攻撃を行うことはできないのであるから，それ自体は何の意味もない（そもそも，ファイアウォールの通信ルールは，攻撃端末をつなげばポートスキャン等により容易に知ることができるものである。）。

実際，長野県侵入実験では，ファイアウォールの攻略及びファイアウォール越しのＣＳの攻略に成功していない。

なお，市町村設置ファイアウォールが被告財団法人の指示に即した設定がされている限りＣＳを攻略できないことは，品川区において実施したペネトレーションテストにおいても実証済みである（丙第１４号証）。

ウ　庁内ＬＡＮについても危険性が明らかにされたものではないこと

(ｱ)　知事会見では，下諏訪町において無線ＬＡＮを利用して侵入実験を行い，庁内ＬＡＮに侵入できることがわかったとしている（知事会見１３ページの８ないし１３行目）。

しかし，その実態は，無線ＬＡＮ環境をわざわざ構築した上で，正常な接続をしてみたにすぎず，何かしらの脆弱性を攻撃して不正な侵入（接続）を成功させたものではない。

したがって，この実験は，何ら無線ＬＡＮの危険性を実証するものでなく，また，このことにより，市町村の庁内ＬＡＮの具体的危険性が示されたわけではない。まして，かかる接続がされたことにより，住基ネットの具体的危険性が明らかにされたものでないことはもちろんである。

(ｲ)　また，知事会見では，出先機関につないだ攻撃端末からダイアルアップ・アカウント経由でＩＳＤＮを通じて市町村の庁内ＬＡＮに接続することができたとされている（知事会見５ページの末行ないし６ページ，８ページの１ないし８行目）。

しかし，この接続方法も，出先機関の庁舎内に物理的に入り込んだ上で，出先機関のＩＳＤＮ回線を接続したものにすぎず，庁舎外の端末から，セキュリティ対策の不備を突いて，ダイヤルアップ接続により庁内ＬＡＮに不正に侵入したものではない。

したがって，このことにより，何ら庁内ＬＡＮの具体的危険性が示されたものではない。まして，かかる接続がされたことにより，住基ネットの具体的危険性が明らかになったわけではないことはもちろんである。

エ　ＣＳ及びＣＳ端末のＯＳの管理者権限の取得が何ら住基ネットの具体的危険性を示すものではないこと

(ｱ)　長野県侵入実験は，ファイアウォールで防御された区画内に直接攻撃端末をつなぐという物理的な侵入を伴う方法で実験を実施し，その結

果，ＣＳ，ＣＳ端末のＯＳの管理者権限を奪取したとしている。そして，知事会見では，ＣＳのハブの空き口に攻撃端末をつないで侵入実験を行ったところ，ＣＳについては，約１時間ないし１時間半で完全に管理者権限を奪取することに成功し，ＣＳ端末も同様に管理者権限を奪取し，ＩＤパスワードがなくても，自由に操作できる状態になったとしている（知事会見６ページ１６行目ないし２３行目）。

(ｲ) しかし，そもそも，長野県が，第２次実験により，ＣＳやＣＳ端末のＯＳの管理者権限を取得したと主張する方法は，重要機能室に立ち入り，かつ，ラックの鍵を開け，市町村設置ファイアウォールを物理的に回避して，攻撃端末をハブにつないだという，通常想定し難い極めて特異な条件の下で，ＣＳやＣＳ端末のＯＳの管理者権限を取得したと主張するものである。

すなわち，ＣＳは，市町村設置ファイアウォールで防御された上，重要機能室の中の施錠されているラックの中に置かれており，権限のない者が容易に近づけないように市町村で厳重に管理されているのであって，これらの点は，チェックリストにより全市町村でその実施を確認している（被告ら準備書面(5)４０ページ）のであって，長野県侵入実験で行われたように，重要機能室に入り，攻撃端末をファイアウォールで防御された区画内に直接つなぐこと自体がそもそもできないようになっているのである。

長野県侵入実験におけるＣＳのＯＳの権限奪取は，重要機能室に入り込み，施錠されたラックを解錠するという物理的侵入等を果たしたことを前提として初めて成功したものであって，市町村における庁舎の保安対策が極めて不十分であり，かつ，庁舎に侵入するという違法行為を前提とするものであり，住基ネット本体のセキュリティの不備を示すものではない。

ＣＳ及びＣＳ端末とも，適切にセキュリティホール対策が講じられており（被告ら準備書面(5)３２ページ），特に，ＣＳ端末については，品川区において被告財団法人が実施したペネトレーションテストにおいて侵入できなかったように（被告ら準備書面(5)４２ページ），迅速に動作検証を行い速やかにパッチの適用を行っている。長野県最終報告でも，「ＣＳ端末が使用しているＯＳには既知の脆弱性は存在していなかった」（長野県最終結果３－２－３（１０ページ））とされているのである。

(ｳ) 以上の点をおくとしても，仮に，ＣＳ，ＣＳ端末のＯＳの管理者権限を奪取したとしても，被告財団法人が管理する本人確認情報には全く問題がない。

すなわち，たとえＣＳ及びＣＳ端末のＯＳの管理者権限が取得されたとしても，住基ネットに関する業務を行うための住基ネットアプリケーションは，操作者識別カードによる認証を経ないと一切の操作を行えないように設定されている等，各種のセキュリティ対策が講じられている。

したがって，ＣＳ及びＣＳ端末のＯＳの管理者権限を取得したからといって，住基ネットアプリケーションを起動させることすらできないわけであるから，当該市町村以外の住民の本人確認情報を閲覧（盗取）することはおよそ不可能である。すなわち，ＣＳ及びＣＳ端末のＯＳの管理者権限を取得したことは，住基ネットの危険性を何ら示すものではない。

実際，長野県侵入実験では，当該市町村以外の住民の本人確認情報を閲覧（盗取）することに成功していないものである。

(ｴ) なお，最終報告では，ＣＳで得られたデータを利用してＣＳ端末のＯＳの管理者権限を取得したとしている（長野県最終報告３－２－３（１０ページ））が，ＣＳは，ＣＳ端末よりも強固なセキュリティが採られ

ており，長野県侵入実験のようにＣＳのハブの空き口に攻撃端末をつなぐなどという極めて特異なケースは，ほとんど想定できず，ＣＳのＯＳの管理者権限を取得した上で，ＣＳで得られたデータを利用してＣＳ端末のＯＳの管理者権限を取得するというのは，本末転倒である。

(オ)　第１次実験では，庁内ＬＡＮや既存住基システムに脆弱性があったとし（長野県最終結果３－１－１，３－１－２（９ページ）），知事会見でも，既存住基サーバ及び庁内ウェブサーバとつながる庁内クライアント端末と同じ場所に攻撃端末を接続して脆弱性について調査したところ，約１時間で既存住基サーバ及び庁内ウェブサーバの管理者権限を略奪したとしている（知事会見５ページの２５ないし３５行目）。

しかし，これらのサーバは，税，国民健康保険等これまで各市区町村において独自に電算化を行ってきたシステムのうちの一つであり，平成１１年法律第１３３号による住民基本台帳法の改正前から導入されていたものであって，同改正によって新たに導入された住基ネット本体とは，区別されるべきであり，住基ネット本体のセキュリティの問題とは直接関係はない。

オ　結論

長野県侵入実験の結果を公正に評価すれば，住基ネットは，市町村設置ファイアウォール及び指定情報処理機関監視ファイアウォール等により厳重に防御されているのであって，長野県侵入実験ではこれらのファイアウォールを突破できていないのであるから，住基ネット本体の安全性が明確となったというべきである。

しかも，長野県侵入実験は，インターネット経由でインターネットと庁内ＬＡＮとの間のファイアウォール越しにこれらのサーバを攻略することができなかったため，ファイアウォールを回避して物理的侵入を伴う方法で行われたものであり，通常想定し難い極めて特異な条件の下で，ＣＳや

ＣＳ端末のＯＳの管理者権限を取得したものであって，侵入実験の名に値しないというべきものである。

そして，長野県侵入実験の結果から明らかとなった前記の諸点については，専門家と地方公共団体の代表で構成される住民基本台帳ネットワークシステム調査委員会（被告ら準備書面(5)２８ページ参照。以下「住基ネット調査委員会」という。）が，平成１５年１２月２６日に発表した「長野県が実施した「市町村ネットワークの安全性調査」を受けての対応」においても，明らかにされているところである（丙第２１号証）。

4　長野県侵入実験，長野県調査速報及び知事会見の問題点等

(1) 長野県侵入実験，長野県調査速報及び知事会見の問題性について

ア　長野県侵入実験は，指定情報処理機関に何の連絡もなく行われたもので方法において相当とは言い難いこと

長野侵入実験は，住基ネット本体を監視ないし管理する指定情報処理機関に何の連絡もないまま実施されたものであり，その方法において相当とは言い難い。

被告国（総務省）は，長野県の実験（阿智村における第２次実験）について地元紙が第一報を報じた平成１５年１２月６日に，「住基ネットの運用状況について」と題するコメント（丙第１８号証）を発表し，その中で，指定情報処理機関が，阿智村における指定情報処理機関管理，監視に係る住基ネットの機器について，不審な通信や接続異常等を検知したため，阿智村に報告を求めたところ，その回答で初めて長野県が侵入実験を行ったという事実が判明したこと，長野県にその侵入実験の詳細を明らかにするように求めたが，いずれ公表すると述べるにとどまったことなどの事実関係を明らかにした上で，「侵入実験を行う場合には，管理責任者の事前の了解を得ることは当然のことであり，地方公共団体の共同のネットワークである住基ネットの本体において，他の地方公共団体及び運用管理を行っ

ている指定情報処理機関に事前の了解なく実験を行うことは，誠に遺憾であるというほかない。」「総務省としては，・・・長野県に対し，侵入実験の内容と手段について，指定情報処理機関，住基ネット推進協議会（全国の都道府県で構成）及び総務省に，早急に説明を行うよう，求めることとする。」とした。

しかし，長野県調査速報が公表された後も，いまだに長野県から何らの回答を得ておらず，実験の手順自体相当とは言い難い。

イ　長野県調査速報は，情報セキュリティ監査報告書としての要件を著しく欠いていること

長野県調査速報は，それが速報であるという性格を考慮したとしても，なお，実験環境，実験手順，事前入手情報等の実験の前提条件についての記述が全くないことに加え，情報セキュリティ監査報告書として必要な条件を著しく欠いている。

前記のとおり，被告国（総務省）及び同財団法人は，その管理領域における機器の異常が検知された直後から，長野県に対し，その実験内容についての報告を求め，その後も文書を含め，再三にわたり報告を求めているが（総務省自治行政局市町村課の平成１５年１２月６日付け「住基ネットの運用状況について」・丙第１８号証），長野県調査速報が公表された後も，いまだに長野県から何らの回答を得ていない。

そのため，いまだ情報セキュリティ監査報告書の要件ともいうべき実験環境，実験手順，事前入手情報等の実験の前提条件が明らかにされておらず，被告国及び同財団法人は，長野県調査速報に存する多くの疑問点について，十分な検証ができない状況にある。

ウ　長野県調査速報及び知事会見はその内容において公正とは言い難い

長野県調査速報及び知事会見は，実験結果として，以下に指摘するように，住基ネット本体の本人確認情報に対する危険性が全くないことが明ら

かになったことについて触れておらず，かえって，庁内ＬＡＮの問題を住基ネットのセキュリティの脆弱性の問題であるかのようにすり替えて公表するなど，公正な内容とは言い難い。

(ｱ) いずれのファイアウォールも侵入できなかった事実に触れていないこと

住基ネットは，ファイアウォールの多重防御などにより，高いセキュリティを確保している。長野県侵入実験では，①インターネットと庁内ＬＡＮとの間のファイアウォール，②市町村設置ファイアウォール及び③指定情報処理機関監視ファイアウォールの合計３つのファイアウォールは，そのいずれもが突破されていないのに，長野県調査速報は，その事実に全く触れていない。

(ｲ) インターネット経由で侵入できなかったことについての総括をしていないこと

長野県侵入実験では，インターネット経由でファイアウォールを攻略して侵入しようとしたが，結局，成功しなかったにもかかわらず，長野県調査速報では，その点について正当な評価をしていない。すなわち，長野県が当初意図した侵入実験が失敗し，安全性が確認できた事実を明確に述べていない。

(ｳ) 庁内ＬＡＮの問題をあたかも住基ネット自体の問題であるかのように取り上げていること

前記のように，長野県侵入実験は，長野県下の個々の市町村の庁内ＬＡＮの脆弱性を指摘しているにすぎず，実験の結果，住基ネット本体の本人確認情報に対する危険性は全く確認されておらず，むしろその安全性が確認されているのである。

しかし，長野県調査速報は，その全体にわたって，庁内ＬＡＮの個々の脆弱性をあたかも住基ネット本体の安全性の問題であるかのように事

実を歪曲して取り上げている。

例えば，長野県調査速報は，「何が起こりえるのか？」との大きな見出しの下に，「選挙人名簿に登載されていないことにして，選挙をできなくさせる。」，「国民年金データを改ざんして転居させ，転居した場所でより多い額の年金をもらう。」，「介護保険や児童手当の受給データを改ざんして，本来の受給者をもらえなくさせる。」，「税金の滞納データを消去し，そのデータを持たせて，勝手に転出させる。」としているが（長野県調査速報８ページ），これらの指摘事項は，住基ネット本体のセキュリティと全く関係がない上，最終報告では，理由は不明であるが，これらの記述は全くされていない。

したがって，このような公表態度は，国民の不安をいたずらに煽るものと言わざるを得ず，誠に遺憾である。

(2) 長野県調査速報等による社会的影響について

ア　長野県侵入実験の結果及びその評価について前述したように，住基ネット本体のセキュリティには何ら問題がないにもかかわらず，長野県調査速報等において，住基ネットのセキュリティに危険性があるかのような公表がされたことにより，社会的にも重大な悪影響があった。

例えば，長野県市長会及び町村会は，平成１６年１月７日の長野県経営戦略局長への要望書の中で，「最近の県政運営を見ておりますと，県民に身近な行政を担う市町村の意見が十分に反映されず，市町村との共通認識が欠けたまま事業が先行されたり，或いは，先送りされようとしていることは，今後の市町村行政を推進するうえで大変心配であり心を痛めています。特に，住基ネットの実験結果は不透明な中で実施され，一部の自治体のみの事例を大きく取り上げられておりますが，このことは，慎重に事業を進めております市町村との信頼関係を損ない，地域住民の不安を引き起こすものと苦慮いたしております。」「また，発表された内容は主に市町

村庁内ネットワークの脆弱性を指摘したものであり，いたずらに市町村に不安や戸惑いを与え，説明責任の観点からも県への不信を拡大した。」（丙第２４号証）としている。

イ　国（総務省）は，知事会見により長野県調査速報の発表がされた平成１５年１２月１６日に，「長野県の侵入実験に対する総務省コメント」（丙第１９号証）と題するコメントを発表し，その中で，「長野県の実験は，その手法に違法性のおそれがあることに加え，庁内ＬＡＮの小さな脆弱性を住基ネット本体の安全性の問題であるかのようにねじ曲げことさら誇大に取り上げた結果を公表しており，誠に遺憾である」とのコメントを発表するとともに，全地方公共団体に通知し，さらに総務省のホームページにおいても，総務省コメントを公表した。

また，国（総務省）は，長野県最終報告が公表された平成１６年２月２９日に，長野県最終報告に対して，コメント（丙第２０号証）を発表し，その中で，長野県侵入実験によって，住基ネット本体の安全性が確認されたことを指摘した上で，「今回の報告は，昨年１２月１６日の中間報告及びその発表時における記者会見での長野県知事や長野県本人確認情報保護審議会委員の発言内容とは，示された事実及びその説明において多くの点で異なっている。特に，中間報告及びその発表時における記者会見で示された住基ネット本体の危険性に関する内容が最終報告では何故かほとんど言及されていない。市町村庁内ＬＡＮの脆弱性を住基ネット本体の安全性の問題であるかのように取り上げ，ことさらに危険性を強調し，国民及び他の地方公共団体に対して誤解を与えてきた，これまでの長野県の姿勢が一層明白になったものであり，誠に遺憾と言わざるを得ない。」と指摘した。

ウ　この長野県調査速報及び知事会見の問題点については，平成１５年１２月２６日，住基ネット調査委員会により発表された「長野県が実施した

「市町村ネットワークの安全性調査」を受けての対応」（丙第２１号証）においても，長野県侵入実験について，「実際に住基ネット本体へは侵入されておらず，また，指定情報処理機関の本人確認情報は全く問題ない状況であるにもかかわらず，庁内ＬＡＮの脆弱性を住基ネット本体の安全性の問題であるかのように取り上げるなど，事実と異なる情報が喧伝されている。」と指摘されているところである。

エ　また，実験が実施された下諏訪町の町長は，平成１６年２月２日の会見において，「町が通常使用していない無線ＬＡＮを使うなど，職員が不正行為をするか，外部から何者かが庁舎内に侵入しない限り，考えられない状況を想定した実験だった」と指摘しつつ，その実験の結果につき，「住基ネット本体の（侵入される）危険性はなかったといっていい」（平成１６年３月３日付け信濃毎日新聞３ページ・丙第２３号証）と明言している。

5　原告が長野県「侵入実験の結果判明した事実」として指摘する事項について

(1)　「侵入実験の結果判明した事実」と称して原告が指摘する事項の要旨

ア　以上述べたように，長野県侵入実験の手法及びその公表の在り方には様々な問題があるが，原告は，原告準備書面(7)において，かかる問題を含む長野県侵入実験の結果につき，長野県が行った「侵入実験の結果判明した事実」と称して，要旨以下の事項を主張する。

①　庁内ＬＡＮへの侵入口が多数存在し，侵入が容易であった（第２の１（５，６ページ））。

②　既存住基サーバ，庁内ウェブサーバの権限奪取に成功した（第２の２（６，７ページ））。

③　ＣＳ端末及びＣＳサーバの権限奪取に成功した（第２の３（７，８ページ））。

④　市町村設置ファイアウォールを通過する仕組み及び方法を発見し，さらに，インターネット側のファイアウォールは通過することができた

（第２の４（８，９ページ））。

⑤　被告財団法人の住基ネット監視が不十分であることが判明した（第２の５（９ページ））。

⑥　さらに，伊藤穣一氏の第三者評価からも，住基ネットの安全性に問題があることは明らかである（第３（９ページ））。

イ　しかし，原告らの主張のうち①ないし④の各事項については，長野県知事速報及び知事会見と同様に，住基ネット本体のセキュリティに関して何ら問題のない事実を，長野県侵入実験の結果，さも何か問題がある事実が判明したかのように主張するものか，あるいは庁内ＬＡＮの脆弱性を住基ネットの安全性の問題にすり替えて主張するものであって，失当である。

また，⑤の事項については，全く事実誤認に基づくものであって，失当であり，⑥の事実についても，伊藤氏の評価の限界を無視した主張であって失当である。

しかも，いずれの点についても，住基ネットの安全性の観点から，意味のない主張である。

以下，原告の主張に即して，詳述する。

(2) ①庁内ＬＡＮへの侵入口が多数存在し，侵入が容易であるとする点について

ア　原告の主張の要旨

原告は，長野県侵入実験の結果，庁内ＬＡＮが組まれている庁舎に隣接する建物内に庁内ＬＡＮの接続口が存在し，ここに攻撃端末を接続するだけで，庁内ＬＡＮに侵入できること，無線ＬＡＮを利用した侵入が可能であること，庁内ＬＡＮのダイヤルアップ接続が可能であったこと，その他住基ネットへの接続口（侵入口）が多数存在することが明らかになったと主張する（原告準備書面(7)第２の１（５，６ページ））。

イ　被告らの反論

(ｱ) しかし，前記のとおり，長野県侵入実験は，ファイアウォールを物理的に回避して，庁内に入り，攻撃端末を町村の庁内ＬＡＮにつないだり，あるいは厳重に入退室が管理され，容易にその室内に立ち入ることができない重要機能室に立ち入った挙げ句，厳重に管理されているラックの鍵を開け，市町村設置ファイアウォールを物理的に回避して，攻撃端末をハブにつなぐという通常は想定し難く極めて特異な条件の下で実験しているものである。

また，無線ＬＡＮを利用した侵入についても，無線ＬＡＮ環境をわざわざ構築し，また，ダイヤルアップ接続も出先機関のＩＳＤＮ回線に接続し，いずれも通常の正常な接続を行っているだけのことであり，このことにより，市町村の庁内ＬＡＮに関する脆弱性や対策の不備を明らかにしたものではないし，ましてや，住基ネット本体のセキュリティの不備を示すものでもない。

原告は，かかる当然の事実を，さも長野県侵入実験によって，初めて判明したかのように誇張して述べているにすぎず，当然のことながら，長野県最終報告では，このような点を問題とする記述はない。

(ｲ) 被告ら準備書面(5)（２４ページ以下）で述べたとおり，住基ネットは，庁内ＬＡＮ経由の脅威に対する対策や，住基ネット本体における対策が適切に施されており，特に市町村設置ファイアウォール，指定情報処理機関監視ファイアウォール等により厳重に防御されているのであって，長野県侵入実験では，これらのファイアウォールはいずれも突破されていないのであるから，住基ネット本体の安全性に影響を及ぼすものではない。

また，市町村の庁内ＬＡＮは，各市町村において管理するものであるが，住基ネットと物理的に接続する庁内ＬＡＮについては，セキュリティ基準に基づき，当該市町村において適切な対策が講じられており，被

告国（総務省）及び被告財団法人においても，チェックリストを活用する等によりその対策の徹底を図っている（被告ら準備書面(5)４０ページ）。

(ｳ) なお，原告は，ＣＳ端末の背面にネットワークケーブルがむき出しにして配置してあったり，操作者識別カード読取装置のＵＳＢの接続線がむき出しになっているところが多数存在するから，住基ネットに直接侵入することも物理的に難しくない状態にあったことが判明したとする（原告準備書面(7)６ページ）。

しかし，かかる事実は，長野県調査速報では全く触れられていない。

原告の主張は，おそらく知事会見における吉田柳太郎委員の発言をその根拠としているものと思われるが（知事会見１２ページ），同委員は，長野県侵入実験の結果として，かかる事実を確認したなどとは述べていない。わずか３町村において実施されたにすぎない長野県侵入実験によって，ネットワークケーブルや操作者識別カード読取装置のＵＳＢの接続線がむき出しになっているところが「多数存在する」という事実が確認されたというのは，誇張以外の何ものでもない。当然のことながら，長野県最終報告では，この点に関する記述がない。

そもそも，ＣＳ端末は，権限のない者が容易にアクセスできない場所に設置するなどの物理的セキュリティ対策がセキュリティ基準で義務付けられ，チェックリストで徹底を図っている。さらに，ＣＳ端末の背後のネットワークケーブルに持ち込んだ攻撃端末をつないだとしても，操作者識別カードによる認証やファイアウォールなどの多重防御が施されていることから，住基ネット本体への侵入を行うことができるわけではないのである。

結局のところ，原告は，長野県侵入実験によって確認された事実でないものをあたかも同実験によって確認された事実であるかのように偽り，

あるいは誇張して主張するものであり，かかる主張は，不当である。

(3) ②既存住基サーバ，庁内ウェブサーバの管理者権限を奪取したとする点について

ア　原告の主張

原告は，長野県が，既存住基サーバ及び庁内ウェブサーバとつながる庁内クライアント端末と同じ場所に攻撃端末を接続して，侵入実験を行ったところ，約１時間で既存住基サーバ及び庁内ウェブサーバの管理者権限の奪取に成功したとし，これにより，既存住基サーバ内の個人情報を書き換えたり，削除したりすれば，ＣＳサーバに不正アクセスしなくても，ＣＳサーバ内の本人確認情報を改ざん，削除等することが可能であると主張する（原告準備書面(7)第２の２（６，７ページ））。

イ　被告らの反論

(ｱ) しかし，前記のように，長野県が行った既存住基システムに対する侵入実験は，インターネット経由では既存住基システムの侵入に成功できず，ファイアウォールで防御された区画内に直接攻撃端末をつなぐという方法で行われたものである。

その上，前述のとおり，既存住基システムのサーバは，住基ネット本体とは市区町村の管理する指定情報処理機関の提示に沿って設定されたファイアウォールと指定情報処理機関の監視するファイアウォールにより隔てられており，これらファイアウォールを攻略しない限り，住基ネット本体とは関係を持たない。

既存住基システムにおける本人確認情報の改ざん等の防止は，飽くまで当該システムを管理する市町村において対処すべき問題であり，既存の住基システムにおいて改ざん等がされた本人確認情報が住基ネットのＣＳに送信されたとしても，それは，何ら住基ネットシステムの危険性を示すものではない。

(イ) その点をおくとしても，そもそも，既存住基システムは，通常，データベースに保存されている個人情報を書き換えただけで，自動的に書き換えられた情報がＣＳに対して送出されるような仕組みで構成されていない。すなわち，更新等の情報は，既存住基システムからＣＳに別途，送信する必要があり，自動的に改ざん情報が更新されるわけではない。さらに，ＣＳは，既存住基システムからの要求データの内容をチェックしているため，既存住基システムから不正な要求があると，処理ができないような仕組みとなっている。このようにＣＳに改ざんされた情報が反映される可能性は極めて低いものである（丙第２０号証２ページ）。

したがって，かかる原告の主張も失当というほかない。

(4) ③ＣＳ及びＣＳ端末の管理者権限を奪取したとする点について

ア　原告の主張

原告は，住基ネットのＣＳのハブの空き口に攻撃端末をつないで侵入実験を行ったところ，ＣＳについては，約１時間ないし１時間半でバッファーオーバーフローを起こさせて完全に管理者権限を奪取することに成功し，ＣＳ端末も同様に管理者権限を奪取し，操作者識別カード及びパスワードがなくても，自由に操作できる状態になったと主張する（原告準備書面(7)第２の３（７，８ページ））。

イ　被告らの反論

しかし，前記のとおり，長野県侵入実験におけるＣＳ及びＣＳ端末のＯＳの管理者権限の取得は，通常の状態で成功したものではなく，ファイアウォール等による多重防御を回避し，重要機能室に入り込み，施錠されたラックを解錠して物理的侵入等を果たすという，通常は想定し難い極めて特異な条件の下で初めて成功したものであっる。ＣＳ及びＣＳ端末とも，十分なセキュリティホール対策が講じられており，このような通常ではあり得ない物理的侵入を伴わない限り，これらの管理者権限を取得すること

は極めて困難である。なお，長野県最終報告３－２－３（１０ページ）によれば，ＣＳ端末のＯＳにはそもそも脆弱性は存在していなかったとされている。

また，仮に，ＣＳ及びＣＳ端末のＯＳの管理者権限を取得したとしても，直ちに住基ネットアプリケーションを起動できるわけではない。当然のことながら，長野県調査速報も知事会見も，操作者識別カード及びパスワードがなくとも，住基ネットを自由に操作できた，すなわち，ＯＳのみならず，操作者識別カード認証を突破し，住基ネットアプリケーションの管理者権限まで奪取したなどとは述べていない。この点は，最終報告でも同様である。

したがって，仮に，長野県侵入実験の結果，ＣＳ及びＣＳ端末のＯＳの管理者権限を奪取したとしても，それは，何ら住基ネット本体における本人確認情報の漏洩等の具体的危険性を示すものではない。

(5) ④ファイアウォールが通過できたなどとする点について

ア　原告の主張

原告は，長野県侵入実験によって，(a)市町村設置ファイアウォールを通過する仕組み及び方法を発見し，さらに(b)インターネット側からの侵入実験を行ったところ，インターネット側のファイアウォールを通過できたと主張する（原告準備書面(7)第２の４（８，９ページ））。

イ　被告らの反論

(ｱ) しかし，(a)の点については，前記３(2)イでも論じたとおり，何ら問題とはいえないものである。

また，原告は，「実際に流れるデータをキャッチすることができれば，そのデータに成りすますことは可能であり，そのようにデータを流し込めば，ここの脆弱性を突いて，管理者権限を略奪できる」（原告準備書面(7)８ページ）とも主張するが，一般的に，ファイアウォールにおいて

許可されたポートに対応する脆弱性が，コンピューターにおいて存在しなければ，当該コンピューターに対してファイアウォール越しに攻撃することはできないものであり，ＣＳにはファイアウォールにおいて許可されたポートに対応する脆弱性は存在しないため，攻撃はできない。このことは，総務省の行った品川区におけるペネトレーションテストによっても明らかにされたところであり，原告の主張は失当である。

結局，長野県侵入実験では，ファイアウォールの攻略に成功していないのであるから，以上の指摘も何ら住基ネットの具体的危険性を示すものではない。

(ｲ) 次に，(b)の点については，原告らは，「実際は，インターネット側のＦＷを通過できており」と述べて，あたかも，ファイアウォールの設定上通過を許可されている通信がファイアウォールを通過したこと自体が問題であるかのように主張する。しかし，ファイアウォールは，いわば物理的な壁ではなく，通信制御を行う機器であり，許可する通信と，拒否する通信とを制御するものであり，通信を全く許可しないというものではない。通過を許可した通信をファイアウォールが遮断せず，通過させることは当然であって，ファイアウォールの設定上通過を許可されている通信がファイアウォールを通過したことをもって，ファイアウォールが無効となる，いわゆるファイアウォールが攻略されたという意味で「通過」したものでないことは明らかである。

更に付言するならば，このファイアウォールは，各市町村が庁内ＬＡＮとインターネットとの間に設置しているものであって，その管理は当該市町村においてされるものであり，住基ネット本体のセキュリティとは，直接関連しないものである。

(6) ⑤被告財団法人の住基ネット監視が不十分であるとする点について

ア　原告の主張

原告は，長野県侵入実験においてＣＳの管理者権限を奪取しているにもかかわらず，指定情報処理機関監視ファイアウォールのＣＳ側の線を外すまで，被告財団法人から何らの連絡もなかったとし，被告財団法人による住基ネットの監視は，指定情報処理機関監視ファイアウォールの市町村側においては不正侵入を検知できないなどと主張する（原告準備書面(7)第２の５（９ページ））。

イ　被告らの反論

(ｱ) しかし，被告財団法人は，指定情報処理機関監視ファイアウォールまでの住基ネット本体について２４時間監視を行っており（被告財団法人は，ＣＳについて稼働状況のみを監視している。），ＣＳについては，各市町村において厳重な管理がされている（被告ら準備書面(5)２６，３３ページ）。この点については，住基ネットの設計段階において，被告財団法人から地方公共団体に通知されており，また，被告国（総務省）及び被告財団法人の各種説明資料等でも公表されている周知の事実である。

この点，長野県調査速報では，平成１５年８月５日に行われた公開討論会における総務省担当者の発言として，被告財団法人がＣＳを２４時間監視している旨述べたかのような記載がある（長野県調査速報本文５ページ）が，上記公開討論会の討論内容（テープ起こし）を見れば明らかなように，総務省井上源三市町村課長は，被告財団法人による監視は住基ネット本体についてのみであり，市町村におけるＣＳ等については行われていないと明確に述べている（丙第２５号証）。

市町村におけるＣＳは，市町村が責任を持って管理する分野であって，その部分について，被告財団法人がＣＳを２４時間監視していないことをもって住基ネットの監視が不十分であるとする原告の主張は，およそ失当である。

そして，「住基ネット県調達ＦＷのＣＳサーバ側の線をはずした。すると，これを外した途端に，ＬＡＳＤＥＣの方から，何かありましたかという確認が来た。」との原告の主張こそ，被告財団法人が適切に監視を行っていることを明快に示すものといえる。

ちなみに，長野県最終報告では，「全国の都道府県からの委託を受けてＬＡＳＤＥＣが管理している部分」が「ＣＳの都道府県ネットワーク方向にあるファイアウォールから上流部分」であると記述されており（長野県最終報告６ページ），長野県調査速報における指摘が誤っていたことを実質的に認めている。

また，原告は，「いかなる監視を行っているかを調査する目的で，同月２８日に住基ネット県調達ＦＷのＣＳサーバ側の線をはずした。」と主張しているが，そもそも長野県においてかかる目的意識を持って線を外したかは極めて疑わしい。なぜなら，実際に外されたのは，ＣＳサーバ側の線ではなく，住基ネット本体における回線であり，長野県は，かかる基本的事実すら誤認しているからである。

(ｲ) なお，指定情報処理機関監視ファイアウォールは，県調達ではなく，外された回線を含め，指定情報処理機関が調達，管理しているものである。長野県は，何ら権限がないのに，無断で回線を外し，その結果として，被告財団法人の阿智村における常時監視が一時中断させられた。しかも，長野県は，被告財団法人からの問い合わせに何ら回答しないことから，同被告において，本人確認情報に異常がないことの確認，阿智村におけるネットワーク機器の確認といった作業を強いられた。このように，長野県が被告財団法人に無断で住基ネット本体の回線を外したことは，同被告の監視業務に無用の負担を与えたものであって，大いに問題である。

(7) ⑥伊藤穣一氏による第三者評価について

ア　原告の主張

原告は，長野県侵入実験の結果が，「総務省の住民基本台帳システムネットワーク調査委員会委員でもある伊藤穣一氏が行った第三者評価において，これらの実験結果について何ら異議は述べられず「平均的コンピュータ・ネットワークエンジニアなら誰でも侵入することが可能で，住基ネット情報を含む様々な個人情報を盗んだり損害を与えることができるでしょう」「私は，市民と彼らの情報を守るべき担当者が，際立って危険な状態にさらされていると考えます。」という評価が下した。」（原告準備書面(7)第３（９ページ））と主張して，伊藤氏の評価においても，住基ネットのセキュリティにつき危険性があるかのような主張をする。

イ　被告らの反論

しかし，そもそも監査の信頼性とは，その実施主体及び報告書自体により判断されるべきものであるところ，長野県の実験は，監査法人がその責任において実施したものでもなく，その報告書は，監査報告書としての要件を著しく欠いているものであり，第三者がコメントを寄せたとしても，監査の信頼性が担保されるものでは到底言えない。

この点をおくとしても，伊藤穣一氏のコメントは，「調査は，地方公共団体オフィスの中のコンピュータに限定されていたため，総務省が管理する住基ネットは直接アタックされませんでした。」（長野県調査速報本文９ページ）などとしていることから明らかなように，主に庁内ＬＡＮについて述べているものであって，住基ネットの安全性について述べたものではない。

したがって，原告の主張は失当である。

(8) 小括

以上述べたように，原告の長野県侵入実験の結果に対する事実認識及び評価は誤っている。

かかる誤った事実認識及び評価に基づいて，住基ネットの安全性を論ずることは全くの無意味であるが，原告は，原告準備書面(7)９ないし１４ページにおいて，「第４　侵入実験結果から判明した原告のプライバシー侵害の具体的危険性」を主張するので，以下，原告の主張に即して，検討を加えることとする。

6　侵入実験結果から原告のプライバシー侵害の具体的危険性が判明したとの原告の主張について

(1) 原告の主張について

原告は，長野県侵入実験の結果により，原告の個人情報（プライバシー）は極めて重大な具体的危険に瀕しているとして，要旨，以下の事項を挙げる。

① 長野県内の市町村のＣＳサーバの管理者権限を奪取することによって，それを踏み台にして，住基ネット網を経由して，被告地方自治情報センターのセンターサーバや被告中野区内のＣＳサーバの中にある原告の本人確認情報を閲覧等することが容易となることが明らかとなった（原告準備書面(7)９ないし１３ページ）。

② 被告中野区のＣＳサーバも長野県侵入実験を行った町村のＣＳサーバと同様の危険にさらされているから，被告中野区のＣＳサーバ内の本人確認情報を閲覧，改ざん等する具体的危険性があることが明らかとなった（同準備書面１３，１４ページ）。

③ 被告中野区の既存住基サーバ内の原告の本人確認情報等の閲覧，改ざん等の具体的危険性があることが明らかとなった（同準備書面１４ページ）。

しかし，いずれの主張も根拠のない失当な主張である。

(2) 被告らの反論

ア　原告主張①について

(ｱ) まず，原告の住基ネットに具体的危険性ある旨の主張の前提には，誰でも，長野県内の市町村のＣＳサーバの管理権限を奪取することできる

ことを前提とする。

a　原告は，かかる主張の根拠として，知事会見で，信越放送の高島哲也がした「桜井委員が・・・例えば長野県から侵入できて，ほかの自治体に他の県も含めてすべて侵入できるという可能性があるという風に言っていた点があると思いますが，今回の実験ではそれがどうであったか」（知事会見１６ページ），「阿智村なり下諏訪から入ってですね。例えば他の町にも同じようにそこに拠点にして入るということは今回の実験では可能だったのか否か」（知事会見１７ページ）との質問に対し，長野県審議会委員吉田柳太郎氏が，「答えは可能だということになります。」（同ページ）などと答えている点を引用する（原告準備書面(7)１０ページ）。

b　しかし，前記のように，長野県侵入実験は，市町村設置ファイアウォールを回避して，重要機能室に物理的に侵入し，施錠を開けるなど通常の対策を幾重にも外して，ＣＳに直接攻撃端末をつなぎ，初めてそのＯＳの管理者権限を取得したとしているものである。かかる取得方法自体が，およそ想定し難い極めて特異な方法である。かかる特異な方法でＣＳのＯＳの管理者権限が取得されたからといって，このような特異な条件がない場合に，ＣＳの管理者権限の取得が容易に行われることを示すものではないことは明らかである。しかも，長野県侵入実験の結果は，特定の限られた条件下における庁内ＬＡＮ，既存住基システムへの侵入の可能性が指摘されたにすぎない。

しかも，前述のとおり，ＣＳ及びＣＳ端末のＯＳの管理者権限を取得したからといって，住基ネットに関する業務を行うための住基ネットアプリケーションは，操作者識別カードによる認証を経ないと一切の操作を行えないように設定されている等，各種のセキュリティ対策が講じられている。したがって，ＣＳ，ＣＳ端末のＯＳの管理者権限

を取得したからといって，住基ネットアプリケーションを起動させることすらできないわけであるから，当該市町村以外の住民の本人確認情報を閲覧（盗取）することはおよそ不可能であって，ＣＳ，ＣＳ端末のＯＳの管理者権限を取得したことは，住基ネットの危険性を何ら示すものではない。実際，長野県侵入実験では，当該市町村以外の住民の本人確認情報を閲覧（盗取）することに成功していないのである。

c　吉田柳太郎氏は，前記答弁の箇所で，他の市町村のＣＳへの侵入が可能であるとする理由として，検索条件の入手ができれば，検索は可能である旨述べているが（知事会見１７ページ），検索条件以前の問題として，操作者識別カードによる認証を経なければ住基ネットアプリケーションを起動させることすらできない。同委員の上記回答は，何ら具体的な根拠を伴ったものではなく，何らの説得性もない。

d　また，長野県侵入実験では，住基ネット本体に対する実験は何ら行われていない。それゆえ，被告財団法人のサーバはもちろん，他の市町村のＣＳにも全く侵入できていない。

以上からすると，長野県侵入実験の結果，ＣＳないしＣＳ端末の管理者権限が第三者に容易に取得される危険があることが明らかになったとは到底言えないのであり，第三者が被告財団法人のサーバや他の市町村のＣＳに不正に侵入して，原告の本人確認情報を閲覧等することが容易に可能であるなどと言えないことは明らかである。なお，長野県最終報告においても，住基ネット本体の本人確認情報に関し，閲覧や検索ができる旨の記述はないのである。

しかも，庁内ＬＡＮ，既存住基システムへの侵入の可能性が指摘されたからといって，市町村ファイアウォール，重要機能室，施錠等により厳重に守られたＣＳの管理者権限が容易に取得されることになるわけではない。さらに，前述のとおり，ＣＳ及びＣＳ端末のＯＳの管

理者権限を取得したからといって，住基ネットに関する業務を行うための住基ネットアプリケーションは，操作者識別カードによる認証を経ないと一切の操作を行えないように設定されている等，各種のセキュリティ対策が講じられている。したがって，ＣＳ，ＣＳ端末のＯＳの管理者権限を取得したからといって，住基ネットアプリケーションを起動させることすらできないわけであるから，当該市町村以外の住民の本人確認情報を閲覧（盗取）することはおよそ不可能であって，ＣＳ，ＣＳ端末のＯＳの管理者権限を取得したことは，住基ネットの危険性を何ら示すものではない。実際，長野県侵入実験では，当該市町村以外の住民の本人確認情報を閲覧（盗取）することに成功していないのである。

ｅ　なお，原告は，ソーシャルエンジニアリングの手法による侵入が注目されており，これに注意すべきであるなどと主張する（原告準備書面(7)１０ページ）。しかし，ソーシャルエンジニアリングの手法による侵入に注意すべきことは，一般にあらゆるシステムにおいて必要なことであり，そのこと自体が，住基ネットの具体的危険性を示すものではない。

(ｲ) 次に，原告は，インターネット経由の侵入が可能であり，また住基ネット市町村調達ファイアウォールは不正侵入を防止できないと主張する（原告準備書面(7)１１，１２ページ）。

しかし，前記のように，長野県侵入実験の結果，いずれのファイアウォールも突破できなかったことが明らかとなっている。すなわち，長野県は，当初意図したインターネット経由での侵入に失敗し（波田町を対象とする第１次実験結果），また，町村の庁内ＬＡＮに攻撃端末をつなぎ，市町村設置ファイアウォールを突破して，ＣＳセグメントへの侵入を試みたが，これも失敗している（阿智村及び下諏訪町を対象とする第

１次実験結果）。長野県調査速報では，市町村設置ファイアウォールの通過の仕組みを発見したとしているが，その具体的な内容は全く明らかにされていないし，長野県最終報告では，その点について一切の記述がない。また，前記のように，ファイアウォールを通過する方法が分かったからといって，ファイアウォールの攻略やファイアウォール越しにＣＳに対する攻撃を行うことはできないのである。

したがって，原告のこの主張も失当である。

なお，原告は，長野県侵入実験において，インターネット側のファイアウォールは通過できており，その先のウェブサーバに必要なパッチが当たっていたため，その管理者権限が奪取できなかったにすぎず，かかる適切な安全管理がなされていない自治体があれば，ウェブサーバの管理者権限は奪取されることになり，その場合，庁内のＣＳサーバを含む他のサーバに対する攻撃の踏み台とされ，ＣＳサーバの管理者権限が奪取される結果となる旨主張する（原告準備書面(7)１１ページ）。

しかし，原告らの主張，すなわち，適切にパッチが当たっていなければ，当該脆弱性が攻撃され得ること，及びあるサーバの管理者権限を奪取すると他のサーバに対する攻撃の踏み台となり得るという事実は，一般的にそうした可能性があるということを指摘しているにすぎないものである。しかし，今回の長野県侵入実験では，ウェブサーバに必要なパッチが当たっていたため，管理者権限を奪取できなかったのである。

なお，ファイアウォールの通過自体に何らの問題が存するものではなく，これをもって侵入と評価し得ないことは，前記５(5)イ(ｲ)で述べたとおりである。

(ｳ) さらに，原告は，長野県侵入実験の結果，ＣＳサーバ及びＣＳ端末の管理者権限が「バッファーオーバーフロー」によって容易に奪取されることが判明したと主張する（原告準備書面(7)１２ページ）。

しかしながら，これまで述べてきたように，ＣＳ及びＣＳ端末とも，適切にセキュリティホール対策が講じられており，長野県侵入実験では，通常は想定し難い極めて特異な条件の下で，初めて管理者権限を奪取し得たものであり，原告らの主張は失当である。加えて，特に，ＣＳ端末については，長野県調査速報では，バッファーオーバーフローにより管理者権限を奪取したとされていたものが（長野県調査速報１５ページなど），長野県最終報告では，完全に記述が逆転し，「ＣＳ端末が使用しているＯＳには既知の脆弱性は存在していなかった」とすると共に，管理者権限の取得の方法は，ＣＳで得られたデータを利用してＣＳ端末のＯＳの管理者権限を取得したものとしている。しかしながら，ＣＳは，ＣＳ端末よりも強固なセキュリティ対策が講じられているのであって，その方法が容易であるとは到底言えない。

(ｴ) また，原告は，ＯＳ（基本ソフト）として使用されているウインドウズ２０００において，セキュリティホールが頻繁に発見されていることを指摘し，そのセキュリティホールの穴埋めをするパッチが当てられるまでのタイムラグを突いて不正侵入がされる危険がある旨主張する（原告準備書面(7)１２ページ）。

しかし，かかる原告の主張は，世界で最もシェアを有するＯＳであるウインドウズを採用しているシステムがすべて不正侵入の具体的危険性があると主張するに等しく，到底，住基ネットの具体的危険性の根拠となるものではない。

(ｵ) さらに，原告は，ＣＳを利用することにより，住民票の広域交付を要求することもできるなどとも主張する（原告準備書面(7)１３ページ）。

しかし，ＣＳに搭載されている住基ネットアプリケーションは，操作者識別カードによる認証がなければ操作することができないし，そもそも住基ネットアプリケーションには住民票の広域交付を要求する機能は

ない。長野県最終報告にも，原告の主張するような記述は一切ない。

(ｶ) 以上に述べたように，原告は，るる述べるが，いずれも根拠のない主張であって，失当である。

イ　原告主張②について

(ｱ) 原告は，阿智村等の市町村設置ファイアウォール，ＣＳ，ＣＳ端末の脆弱性は，被告中野区についても同様に認められるから，被告中野区のＣＳについても不正侵入の危険性があり，特に被告中野区のＣＳが直接攻撃にさらされた場合には，原告の本人確認情報が閲覧，改ざん，消去等が可能であり，その侵害程度は重大であると主張する。

(ｲ) しかし，既に何度も指摘しているように，長野県侵入実験は，市町村設置ファイアウォールを物理的に回避して，ファイアウォールで防御された区画に直接攻撃端末をつなぎ，通常の対策を幾重にも外して初めてＣＳ及びＣＳ端末のＯＳの管理者権限を取得したにすぎず，指定情報処理機関監視ファイアウォールを突破して，被告財団法人のＣＳや他の市町村のＣＳに侵入することには失敗しているのである。

長野県侵入実験から言えることは，せいぜい，被告中野区のＣＳセグメントについても，そのセキュリティレベルを阿智村と同じように下げて直接攻撃端末をつなげば，被告中野区のＣＳ，ＣＳ端末のＯＳの管理者権限が取得される可能性があるというものにすぎないところ，被告中野区のＣＳ，ＣＳ端末に直接攻撃端末をつなぐこと自体，重要管理室やラックが厳重に管理されている中で，容易に行うことができないのであって，およそ非現実的な想定というほかない。

したがって，この点の原告の主張も失当というほかない。

ウ　原告主張③について

(ｱ) 原告は，被告中野区の既存住基サーバ内の本人確認情報等について閲覧，改ざん等の危険があるとも主張する（原告準備書面(7)１４ページ）。

(イ) しかし，かかる原告の主張は，住基ネット導入前から存在している既存住基システムのセキュリティの脆弱性について述べるものであって，何ら住基ネットの脆弱性について触れるものではない。

既存住基システムは，住基ネットの構築以前から各市区町村において管理されてきたものであり，住基ネットの危険性とはおよそ関係がないのである。原告が主張するような危険は，既存住基システムのセキュリティを確保することにより防止すべき筋合いのものであって，これを住基ネットの危険性であるかのようにいうことは，論理のすり替えである。

しかも，被告中野区においては，既存住基システムについて，アクセス権限やパスワードの管理なども適切な対策を行うことで，セキュリティの確保がされており，原告は，被告中野区の管理する既存住基システムについての具体的危険性については何ら明らかにしていない。

原告の主張がおよそ成り立たないことは明らかである。

7　市町村の庁内ＬＡＮのセキュリティレベルの維持・向上について

(1) 既に述べてきたとおり，既存住基システム等の庁内ＬＡＮと住基ネット本体は別個であり，ファイアウォールによって区画されているから，既存住基システムないし庁内ＬＡＮに不正にアクセスされたからといって，それが住基ネットの安全性を脅かすものではない。

しかし，市町村の庁内ＬＡＮに不正な侵入がされると，各自治体における行政事務の円滑な遂行に支障を来たし，また，既存住基システムの個人情報が改ざんされるなどすると，極めて可能性は低いとしても，それが住基ネットにも反映されるなど好ましくない結果を生ずるおそれがあるから，既存住基システムを含む庁内ＬＡＮのセキュリティ強化を継続的に図ることは，国家の施策として重要である。

そこで，被告国（総務省）は，住基ネット調査委員会の提言（丙第２１号証）やペネトレーションテストを実施した監査法人の助言（丙第１４号証）

等を踏まえ，安全性のある電子自治体を構築する観点から，以下に述べるように，全国の市町村の庁内ＬＡＮのセキュリティレベルの維持・向上を図るための取組を積極的に行っていくこととしている。

(2) まず，被告国は，各市町村に対し，セキュリティ対策の強化について財政的支援及び技術的支援を引き続き実施することとしている。

さらに，被告国は，これまでの指導・助言に加え，既存住基システムの管理者権限取得の要因になり得る，推測容易なパスワードの不正取得，セキュリティパッチの適用時間差によるセキュリティホールの悪用等の脅威により適切に対応するため，庁内ＬＡＮの委託事業者（ベンダー）に対して，各市町村において独自に電算化を行ってきた庁内ＬＡＮについても，セキュリティパッチを適用する，強固なパスワードを設定する，ソフトウェアにおけるセキュリティ強化措置を実施するなどのセキュリティ対策の徹底を求めることとしている。

また，平成１６年中に「地方公共団体における情報セキュリティ監査の在り方に関する調査研究会報告書」に基づき，セルフチェックリストを市町村に配布し，庁内ＬＡＮについてもチェックリストにより対策の徹底を図ることとしている。

さらに，ＣＳ，ＣＳ端末等の庁内ＬＡＮにおける住基ネット関係機器のサーバレベルのセキュリティ強化を図る。すなわち，ＣＳのセキュリティパッチの適用については，十分なシステムの動作検証を行い，より早期にセキュリティパッチを適用するとともに，類推困難なパスワードの設定等についても，市町村に対し引き続き適切な技術的な支援を行う予定である。

8　小　括

以上述べたように，長野県侵入実験の結果によって，住基ネットの安全性が立証された。

本来，セキュリティの向上に活用されるべきである脆弱性診断をシステムの

否定に利用しようとした長野県調査速報は，脆弱性診断の基本的目的から外れるものであって，極めて遺憾と言わざるを得ない。

この点は，政府のＩＴ戦略本部においても，問題視された。すなわち，平成１５年１２月１８日，長野県侵入実験について議論がされたが，その中で，村井純委員（慶應義塾大学環境情報学部教授）は，「長野県の住基ネットの議論であるが，あれもネットワークの安全性を上げていくというプラスの方向に色々な話が出ていかなければならない。脆弱性のチェックというのは，私は訓練としてはとても大事だと思う。しかし，訓練というのは安全性を向上させるためにあるわけで，その議論と，システムとして幾つかのところに不具合があるということから，別の議論とすり替えられているというのは，多分これはいろいろな意味で不幸な例ではないかと思う。」（ＩＴ戦略本部（第２２回）での発言，丙第２６号証５ページ）と述べている。また，茂木敏充情報通信技術（ＩＴ）担当大臣も，「住基ネットの御議論があったが，意見集約すると，今回の長野県の対応はあたかも住基ネットに欠陥があるかのような誤解を与え，これによって電子政府・電子自治体に対する，国民の不安感をいたずらにあおる恐れがあるというのが１点だったと思う。」と述べている（丙第２６号証１１ページ）。

被告ら準備書面(5)で詳述したように，住基ネットは，電子政府・電子自治体の実現のために不可欠な基盤をなすものである。住基ネットが支えるインターネット申請を実現する公的個人認証サービスも，平成１６年１月２９日からスタートしている。住基ネットは，その役割をますます発揮し，住民サービスが向上し，行政効率がより高まることは明らかである。

長野県侵入実験により，住基ネットの本人確認情報が漏出，改ざん等される具体的危険があることは明らかにされず，かえって，住基ネットの安全性が確認された。そして，住基ネットの稼働により原告の本人確認情報が漏出，改ざん等される具体的危険があるという原告の主張が何ら合理的な根拠を持ち得な

いことも明らかになった。

「新しい技術が社会のなかに入り込もうとするとき，人々は大きな不安を抱き，怖れ，拒否反応を示す。これはどこの地域，どの時代にも現れる現象である。産業革命時においては，自動機械によって職を奪われるという危機感を抱いた労働者が機械を破壊するという行動を起こした。」（榎並利博・「住基ネットで何が変わるのか」（ぎょうせい）２ページ）と言われるが，そのような轍を踏んではならない。

第２　「所要の措置」について

１　原告の主張の要旨

この点に関する原告の主張の要旨は，以下のとおりである。

すなわち，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」と規定しているが，政府が「所要の措置」（改正法附則１条２項）を講ずる義務は，改正法施行に当たっての不可欠の前提とされていた。したがって，被告国は「個人情報保護に関する法整備」，「住民基本台帳法におけるさらなる個人情報保護措置を講ずるため所要の法改正」を行うまでは，住基ネットの稼働をしてはならない義務を負っていた。ところが，政府は，かかる措置を講じないまま，改正法を施行し，原告のプライバシー権が侵害の危険にさらされているから，原告の個人情報に関して住基ネットの運用を差し止める必要があり，また，被告国には，損害賠償義務がある（原告準備書面(8)４ページ）。

しかし，以下詳述するように，原告の主張は失当である。

２　被告国の反論

(1) 住民基本台帳法の一部を改正する法律（平成１１年法律第１３３号。以下「改正法」という。）は，同法附則１条１項において，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定めており，

政府は，公布の日から３年を超えない日に改正法を施行することが法律上義務付けられていた。このため，政府は，平成１３年１２月２８日政令第４３０号をもって，平成１４年８月５日を改正法の施行日と定め，改正法を施行したのであって，違法な点は全くない。

(2) しかも，政府は，以下のとおり，「所要の措置」を講じている。

ア　改正法附則１条２項の規定は，平成１１年の改正法案の国会審議の過程において，住基ネットについては，同法によって，十分な個人情報保護措置が講じられているものの，なおプライバシー保護に対する漠然とした不安，懸念が残っていることを踏まえ，議員修正により規定されたものである。

また，その国会審議において，小渕恵三内閣総理大臣から「住民基本台帳ネットワークシステムの実施に当たり，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を速やかに整えることが前提であると認識」との答弁がされた。この答弁は，行政府の長として，個人情報保護の必要性についての認識を示したものである。

そこで，政府は，これらを踏まえ，平成１３年３月２７日に「個人情報の保護に関する法律案」（以下「個人情報保護法案」という。）を第１５１回国会に提出した。

イ　そもそも，政府は，立法機関でなく，自ら法律を制定することはできない。したがって，改正法附則１条２項にいう「所要の措置」が法律案の検討，作成，国会への提出を意味することは明らかであって，政府としては，平成１３年３月に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」を講じたことになる。

ウ　なお，上記法案が提出された後，平成１４年１２月６日に，「与党三党修正要綱」（与党三党としては，政府原案に対する修正方針を取りまとめ，政府に提示し，法案の次期通常国会への再提出を求めることを内容とす

る。）が公表され，同月１３日に個人情報保護法案は，審議未了により廃案（第１５５回国会）となった。その後，政府は，上記与党三党修正要綱に基づき，平成１５年３月７日に，個人情報保護関係５法案（①個人情報の保護に関する法律案，②行政機関の保有する個人情報の保護に関する法律案，③独立行政法人の保有する個人情報の保護に関する法律案，④情報公開・個人情報保護審査会設置法案，⑤行政機関の保有する個人情報保護法等の施行に伴う関係法律の整備等に関する法律案）を提出し，これらは，国会で可決成立し，同年５月３０日に公布された。

(3) 原告は，「所要の措置」を講ずる義務の内容として，「行政機関の保有する電子計算機処理にかかる個人情報の保護に関する法律」の改正を指すものであって，主に民間を規制する個人情報保護法は直接には関係がないと主張する（原告ら準備書面(8)７ページ）。そして，自己情報コントロール権としてのプライバシーの権利が憲法上保障されていることを前提に，「所要の措置」を講ずる義務の具体的な内容として，①本来の業務処理に必要な範囲を超えた名寄せの制限，②複数の行政機関相互におけるデータマッチングの制限，③第三者機関による電子政府の監督及び監視，④罰則による担保であると主張する（原告ら準備書面(8)１５ページ以下）。

しかしながら，「所要の措置」とは，民間部門における個人情報保護に関する制度についての措置を指すものである。

すなわち，改正法成立当時，公的部門における個人情報保護制度としては「行政機関の保有する電子計算機処理にかかる個人情報の保護に関する法律」が存在する一方，民間部門における個人情報保護制度は存在しなかった。このような状況を受けて，政府は，住民基本台帳ネットワークのシステムの実施に当たり，「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を速やかに整えること」としたものである（原告準備書面(8)５ページにおいて引用されている小渕首相答弁及び野田国務大臣答弁）。

実際，民間部門の個人情報保護制度を定めた「個人情報の保護に関する法律案」は，第１５１回国会において，平成１３年３月２７日に提出され，同法案１１条１項において，「政府は，国の行政機関について，その保有する個人情報の性質，当該個人情報を保有する目的等を勘案し，その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。」と定められた。この規定を受けて，公的部門の個人情報保護制度について定めた「行政機関の保有する個人情報の保護に関する法律」（以下「行政機関個人情報保護法」という。）等の４法案が第１５４回国会において，平成１４年３月１５日に提出されている。

「所要の措置」が「行政機関の保有する電子計算機処理にかかる個人情報の保護に関する法律」の改正であるとする原告の主張も，独自の見解であり，およそ失当というべきである。したがって，かかる誤った前提に立って，その具体的内容を論ずることも無意味というほかない。

なお，原告が主張する自己情報コントロール権が憲法１３条の権利として認められないことは，被告ら準備書面(3)（第３の３）において述べたとおりである。

(4) また，原告は，「住基ネットが稼働した２００２年８月から，個人情報関連法が可決成立した２００３年５月までは，必要とされた法律が制定ないし改正されていなかったのであるから，住基ネット稼働の形式的な前提すら欠いて運用されていたものである」として，個人情報関連法がいまだ成立していない段階における住基ネットの稼働は違法であると主張し，①総務省が個人情報保護法案を国会に提出したことをもって「所要の措置」を講じたとしているのは詭弁であり，政府の態度は無責任である，②地方自治体が個人情報保護法の未制定・未改正の段階で住基ネットに参加することこそ，違法と評価されるべきであり，地方自治体が住基ネットに参加しないことは，当然の義務であり，当然の行為であると主張する（原告準備書面(8)２０ないし２

２ページ）。

しかしながら，前記(1)で述べたとおり，改正法は，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こととされており，個人情報保護法案が成立すると否とにかかわらず，３年以内の定められた日に施行することが法律上義務付けられていた。そして，政府は，改正法の施行期日を定める政令を制定し，平成１４年８月５日を改正法の施行日と定めた。

したがって，住基ネットを平成１４年８月５日から稼働したことは適法であり，これを違法と評価する余地などない。

また，政府は立法機関でなく，「所要の措置」が法律案の検討，作成，国会への提出を意味するものであることは，前記のとおりである。

なお，住基ネットは，改正法に基づき運用されているものであり，各地方公共団体は，改正法を執行する義務がある。幾つかの地方公共団体が住基ネットに参加しないことは，改正法によらない違法な運用をしているものであり，到底容認することができない。

(5) 原告は，新たに成立した行政機関個人情報保護法は，住民基本台帳法附則にいう「所要の措置」と呼ぶのにふさわしい内容を充分に備えておらず，現在でも，「所要の措置」は講じられていないと主張する（原告準備書面(8)２２ないし２９ページ）。

しかし，「所要の措置」が行政機関個人情報保護法を成立させることでないことは，前記の述べたとおりである。したがって，行政機関個人情報保護法の内容は，何ら改正住基法の施行に影響を及ぼすものではない。

既に述べているように，改正法の施行は適法にされており，「所要の措置」も適法に講じられている。

かかる原告の主張も，独自の見解に基づくものであり，到底採用し得ない。

(6) 以上述べたように，原告の主張は失当である。

第３　最高裁平成１５年９月判決と被告らの主張との整合性について

１　最高裁平成１５年９月判決は，学生の学籍番号，氏名，住所及び電話番号並びに当該学生が講演会の参加申込者であるといった個人情報について，プライバシーに係る情報として，不法行為規範において法的保護の対象となると判示したものである。

２　ところで，被告らは，被告ら準備書面(3)において，憲法１３条によりプライバシー権が保障されているとは言い難いと主張した（被告ら準備書面(3)５ないし９ページ）。

３　そこで，かかる被告らの主張と最高裁平成１５年９月判決との関係が一応問題となるが，前記のとおり，最高裁平成１５年９月判決は，学籍番号，氏名，住所及び電話番号等の個人情報がプライバシーに係る情報として不法行為規範において法的保護の対象となると判示したものであるところ，個人のプライバシーに係る利益が不法行為法の領域において保護される法的利益となり得ることは，上記最高裁判決以前においても既に認められていたところである（最高裁平成６年２月８日第三小法廷判決・民集４８巻２号１４９ページ，最高裁平成７年９月５日第三小法廷判決・裁判集民事１７６号５６３ページ）。最高裁平成１５年９月判決は，かかる前提に立った上で，学籍番号，氏名，住所及び電話番号等の個人情報を自己が欲しない他者にみだりに開示されない利益を不法行為の保護法益として認めたものである。

４　しかし，最高裁平成１５年９月判決は，飽くまでも個人のプライバシーに係る情報が不法行為の被侵害利益として法的保護に値するものであるかどうかについて判断を示したものであって，プライバシーが憲法１３条により保障された権利であるかどうかについて判断を示したものではない。被告ら準備書面(3)において主張したように，プライバシーの概念は多義的であり，その内容は流動的であって，最高裁は，これを一義的な内容をもった権利として認めること

になお慎重である。したがって，最高裁の一連の判例からは，個人のプライバシーに係る利益が憲法１３条に規定された幸福追求権によって基礎付けられる法的保護に値する人格的利益であり，憲法１３条により尊重されるべきものであることが導かれるとしても，プライバシーが一つの明確な内容をもった権利として憲法上保障されていることが判例上確立しているわけではないというべきである。

この点に関し，杉原則彦「時の判例」ジュリスト１２５８号１６７ページも，本判決について「本件の事案は，本来一定範囲の他者には当然開示すべき単純な個人情報や特に秘匿されるべきものとはいえない情報の開示が問題となった点に，事案の特徴がある。しかし，このような情報であっても，自己が欲しない他者にはこれを開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきものである。本判決は，このような観点から，本件個人情報はプライバシーに係る情報として法的保護の対象になると認めたものである。その上で，本判決は，大学が開示についてあらかじめ学生の承諾を求めることが困難であった特別の事情はうかがわれないという事実関係の下では，本件個人情報を無断で開示した行為は，Ｘらが任意に提供したプライバシーに係る情報の管理にについて合理的な期待を裏切るものであり，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との判断を示した。」としており，およそ自己情報コントロール権が憲法上保障され，これを侵害したなどとするものではない。

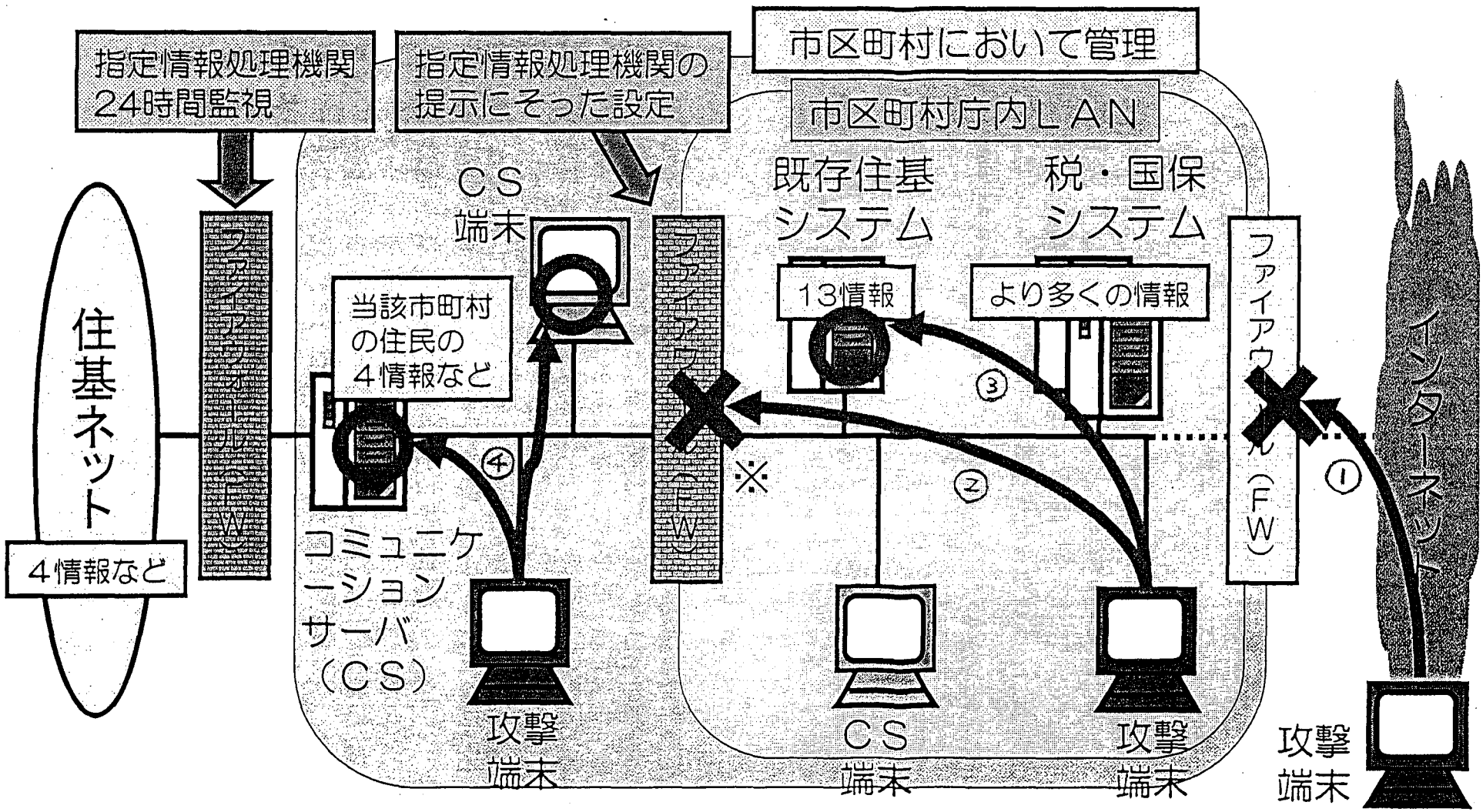
また，情報コントロール権説に立つ内野教授も，最高裁平成１５年９月判決は，学籍番号，氏名，住所及び電話番号について，プライバシーに係る情報として，不法行為規範において法的保護の対象になると判示しているにすぎないのであって，これらが憲法１３条によりプライバシー権として保障されていることを判示しているわけではないと評価している（内野正幸「時の判例　講演会参加者名簿とプライバシー ── 早大江沢民講演会名簿提出事件」法学教室２

００４年２月号－№２８１，１４７ページ参照）。

長野県侵入実験結果

○ 管理者権限取得（ただし、住基ネットの操作は一切できず）

× 侵入できず



※ 長野県では、通過の仕組みを発見したとしているが、実際の侵入はなされていない。