平成１４年（ワ）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　　東京都中野区ほか３名

準　備　書　面　（原告第１４回）

２００４年6月１１日

東京地方裁判所　民事第２５部甲２Ａ係　御中

原告訴訟代理人
弁護士　山　　本　　博
同　　相　　磯　　ま　つ　江
同　　佐　　藤　　典　　子
同　　武　　田　　博　　孝
同　　寺　　崎　　昭　　義
同　　長　　島　　亘
同　　永　　見　　寿　　実
同　　西　　澤　　圭　　助
同　　林　　千　　春
同　　町　　田　　正　　男
同　　水　　永　　誠　　二
同　　矢　　澤　　昇　　治
同　　渡　　辺　　千　　古
ほか１３２名

はじめに

原告は、２００４年１月１６日付準備書面（７）において、「長野県侵入実験」によって、住基ネットシステムには、システム上に看過できないいくつかの脆弱性があり、この脆弱性を攻撃することにより権限のない者が住基ネットシステムに侵入することが可能であり、原告の個人情報が侵害される現実的な危険にさらされていることが明らかになったと主張した。

これに対し被告らは、平成１６年４月２０日付準備書面（７）において、実験の手法について論難するとともに、長野県の実験は、「侵入」に失敗したと決めつけて、「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…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。」（2～3頁）などと主張する。

しかしながら被告らの主張は、客観的で科学的な裏づけをもたない極めて独善的なものであり、失当というほかない。

以下、被告らの主張の根幹部分に焦点をしぼり、反論を加えるものとする。

第１　被告らの主張の概要

１　被告らは、おおよそ以下の諸点をあげ、長野県「侵入実験」の手法や結果等に対して、種々批判・論難する。

Ａ　庁内ＬＡＮ（既存住基サーバ等）の脆弱性に関して

①　インターネット経由での庁内ＬＡＮへの侵入に失敗している。

（インターネットと庁内ＬＡＮ間のＦＷは突破されなかった）

② 無線ＬＡＮは、実験のために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（10 頁）。

③ ダイアルアップアカウント経由で庁内ＬＡＮに侵入というが、「出先機関の庁舎内に物理的に入り込んだ上で」接続したにすぎず、「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」（10 頁）。

④ 庁内ＬＡＮや既存住基サーバなどの脆弱性は、「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」（13 頁）。

Ｂ 市町村管理の住基ネット本体部分（市町村設置のＦＷ、ＣＳ、ＣＳ端末）の脆弱性に関して

① 市町村設置のＦＷ（庁内ＬＡＮとＣＳサーバ間）の攻略、及び、当該ＦＷ越しのＣＳの攻略に失敗している。

② 長野県が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ＦＷ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」である。「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」から、「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」（11 頁）。

③ 長野県の実験は、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が、ＣＳは、ＣＳ端末よりも強固なセキュリテ

ィがとられているのであって、このような手法は「本末転倒」である。

④　仮に、ＣＳやＣＳ端末のＯＳの管理者権限を奪取されたとしても、「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」おり、「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」であり、何ら住基ネットの危険性を示すものではない（12 頁）。

Ｃ　被告センター管理の住基ネット本体部分（被告センター監視のＦＷ、都道府県サーバ、センターサーバ、他の市町村のＣＳサーバ）の脆弱性について

被告センター監視のＦＷは突破されておらず（8～９頁）、その先の各サーバの本人確認情報の閲覧（盗取）にも成功していない(32 頁）。

２　以上の被告らの主張を整理するならば、被告らの「長野県侵入実験」に対する主張の要点は次のようにまとめられる。

①　ＣＳおよびＣＳ端末の管理者権限の奪取は、通常想定し難い極めて特異な条件下において行われたものであって、方法において相当ではない（たとえばＰ８、Ｐ１０、Ｐ１１、Ｐ１３、Ｐ１４、Ｐ１９、Ｐ２１、Ｐ２４、Ｐ２８等）

②　たとえＣＳ端末のＯＳの管理者権限を取得できても、アプリケーションを起動させることはできない（Ｐ１２、Ｐ２２、Ｐ２５）

③　庁内ＬＡＮに接続した手法は、セキュリティ対策の不備を突いた攻撃ではなく、庁内ＬＡＮへの侵入の危険性が実証されたわけではない（Ｐ８、Ｐ１０、Ｐ２１）。

④　いずれのＦＷも突破できていない（Ｐ８、Ｐ９、Ｐ１６、Ｐ２１、Ｐ２５、

Ｐ２６）

⑤　既存住基システムは、住基ネット本体から区別されるべきであり、既存住基の脆弱性は住基ネット本体のセキュリティとは直接関係がない（Ｐ１３、Ｐ１６、Ｐ２３）

第２　被告ら主張の失当性

上述した被告らの主張は、実験によって実証された数々の脆弱性そのものにはふれずに、実験の手法や手続を問題視することで長野県実験の価値を否定しようと意図するものと言わざるを得ない。もとより重要なことは、実験によってどのような脆弱性が実証されたのかという点である。この意味で被告ら主張は、ネットワークセキュリティの常識を無視した誤った事実認識と、そのリスク評価を行っているものであって、全く失当である。

以下、上述の各主張に対応して詳論する。

１　実験は、通常想定し難い極めて特異な条件下において行われたものであって、方法において相当ではないという被告らの反論について

(1) 被告らは、長野県が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ＦＷ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」で行ったものあり、「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」から、「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」と主張する。

ア　しかしながら、まず第１に、「攻撃端末を…直接つなぐこと自体ができな

いようになっている」という主張は誤っている。すなわち、ＣＳとＣＳ端末は同じＣＳセグメント（市町村設置ＦＷのＣＳ側の区画）にあり、ＣＳは「重要機能室」内のラックに収納されているものの、ＣＳ端末は住民サービスの窓口に設置してあり、同端末は何らの遮蔽もされていない。そして、このＣＳとＣＳ端末はケーブル（それ自体は何ら防護されていない）でつながれている。

よって、わざわざ「重要機能室」に立ち入らなくても、ＣＳからＣＳ端末につながっているケーブル（もしくはそれにつながるハブ）に攻撃端末をつなぐことによって、ＣＳやＣＳ端末に対して、「ラックの鍵を開け」た場合と同様の攻撃環境が手に入るのである。

また、ＣＳからＣＳ端末まで伸びているケーブル自体をタッピング（タコ足配線的に物理的な細工を施すこと・３分程度で工作できる）することによっても、同様の攻撃環境が手に入るものである。

以上述べたように、重要機能室に入らなくても、容易にＦＷで防御された区画内に攻撃端末を「直接つなぐこと」はできるのであり、被告ら主張のように、そのような攻撃が「通常想定し難い極めて特異な条件の下」で行われたなどとは全くいえない。被告らの主張は、このようなネットワークセキュリティの初歩的な「常識」をも無視したものといわざるを得ない。

イ　そもそも、実験箇所における「重要機能室」の物理的セキュリティ自体がさほど高くなかったばかりか、全国的にみれば、鍵のかかった重要機能室を備えていなかったり、ＣＳを収納している部屋等への出入りの監視や記録すら満足に行っていない自治体すら相当数存する（丙１３・「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

査票による点検結果集計表」）。この点からいうならば、ＣＳ近くのハブにつなぐということ自体も容易であると言わなければならない。

ウ　さらに、総務省がペネトレーションテストを実施したとされる品川区などでは、ＣＳ端末が市町村設置ＦＷよりも庁内ＬＡＮ側に接続されているが、この場合は、攻撃端末を庁内ＬＡＮに接続しさえすればＣＳ端末に対する攻撃が可能になるものである（この場合、ＣＳ端末は市町村設置ＦＷによる防護も受けていないことになる）。（甲２３の１・１１頁参照）

エ　被告国は、全国自治体が現に設置している住基ネットシステムの現状を、十分承知しているはずである。そのような現状を把握し、かつ、ネットワークセキュリティの「初歩的知識」さえ有していたならば、「極めて特異な」「想定しがたい条件」などという「反論」が出てこようはずがないものである。

(2) 被告らは、長野県の実験は、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が、ＣＳは、ＣＳ端末よりも強固なセキュリティがとられているのであって、このような手法は「本末転倒」であるとも主張する。

ア　しかし、被告らの主張は、ＣＳが、規格どおりの「重要機能室」に収納されている場合に、物理的な侵入に対しては、「ＣＳ端末よりも強固なセキュリティ」を有していることを述べているに過ぎない。

　先述のＣＳとＣＳ端末とをつなぐケーブルに攻撃端末が接続された場合など、ネットワークからの攻撃、という観点からすると、ＣＳ端末もＣＳもその脆弱性の高さに変わりがない。

イ　しかも、セキュリティパッチの適用という面から言えば、ＣＳは、ＣＳ端

末よりも適用される時期が遅いのであるから、この点では、ＣＳの方がＣＳ端末よりも脆弱であるといえる。

２００４年２月２９日開催の長野県審議会議事録（甲２４の１）14 頁・中澤委員の発言によれば、ウィンドウズ２０００のセキュリティパッチ（MS03-026）は、２００３年７月１７日にマイクロソフト社が情報開示を行ったものの、ＣＳ端末へのセキュリティ修正プログラムの適用指示は９月３日と、１ヶ月半も後であった。

（なお、２００３年８月１９日付毎日新聞夕刊において、「ブラスターウイルスの感染が拡大していたなかでも、ウイルス対策ソフトの最新情報が更新されないまま１０日近くも住基ネットの運用が続けられている」、また、「７月１７日にマイクロソフト社が公表したＯＳのセキュリティパッチについて、地方自治情報センターが１ヶ月以上たった１９日現在でも修正ソフトが住基ネットで正常に動くかどうかを検証中」と報道されている。）

よって、ＣＳ端末のセキュリティパッチの適用も、極めて遅いと言わざるを得ない。セキュリティパッチ適用の遅れは、直ちにバッファ・オーバーフロー攻撃の成功という結果をもたらす危険性を有するものである（この場合の危険性は、１００パーセント確実に管理者権限の奪取可能というものである）。

(3)　なお、長野県の実験において、重要機能室に立ち入って調査を行ったのは、調査を行う適当な場所が確保できなかったからに過ぎないものである（この点は、既に２００３年１２月２４日の長野県審議会で説明済みである。甲２３の１・１６～１７頁）。

被告らは、このような事情を無視して、「極めて特異な条件」とか「想定

しがたい条件」などと８回も繰り返し、あたかも実験が不正に行なわれたかのような印象を与えることによって、ＣＳやＣＳ端末のＯＳの管理者権限を奪取できたという重大な危険性を隠蔽しようとするものである。

２　ＣＳやＣＳ端末のＯＳの管理者権限を取得できても、アプリケーションを起動させることはできないという被告らの主張について

被告らは、ＣＳやＣＳ端末のＯＳの管理者権限を奪取されても、「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」であり、何ら住基ネットの危険性を示すものではないと主張する。

しかしながら、管理者権限を略奪したＣＳ端末を、攻撃端末から遠隔で監視・コントロール（マウス、キーボード、画面）することが可能であることは、長野県「侵入実験」により実証されている。よって、攻撃端末から遠隔で監視しているＣＳ端末に対して、正規の操作者が操作者カードで認証を得た後に、当該ＣＳ端末を遠隔操作すれば、正規のユーザーと全く同等な操作が可能となり、センターサーバにアクセスして本人確認情報を閲覧したり、他の市町村に対して住民票の写しの広域交付を要求したりすることができることになる。

ＯＳの管理者権限の奪取は、コンピュータの根源的な支配権の略奪なのであり、被告ら主張のように軽視することは明白な誤りである。この危険を予防するためには、やはり３０００を超える全自治体が、一斉に、かつ迅速確実に、パッチ適用を行いつづけなければならないのである。

３　セキュリティ対策の不備を突いて庁内ＬＡＮへの侵入ができていないという被告らの主張について

被告らは、実験では、庁内ＬＡＮへの侵入に失敗したという。しかしこれまた

事実に反した見解であるといわざるを得ない。

(1) 無線ＬＡＮについて

被告らは、実験では、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、脆弱性を攻撃して接続を成功させたものではないと主張する（Ｐ１０・ウ）

しかし、長野県の実験において、無線ＬＡＮを構築した目的は、実験作業場所が確保できなかったことによる。したがって、実験においては、無線ＬＡＮの脆弱性を突いた侵入を試みたものではないが、そもそも無線ＬＡＮを使用している地方自治体や官公庁は相当数存すること、及び、無線ＬＡＮのセキュリティを高度に保つことは困難であることは、よく知られた事実である。無線ＬＡＮにおけるセキュリティ対策といわれている、ＭＡＣアドレスによる制限＝登録した子機からしかアクセスできないようにする、ＷＥＰ＝暗号化等は、技術的にはいずれも破ることが可能となっている。

よって、本実験によって無線ＬＡＮを利用した侵入の危険性は、何ら否定されない。

（なお、近年、官公庁の無線ＬＡＮが無防備であることがマスコミ等で報道されるなどしており、その危険性を認識した総務省自身が、無線ＬＡＮのセキュリティ対策については、注意を喚起しているところである）。

(2) ダイアルアップアカウント経由での庁内ＬＡＮへの侵入について

被告らは、本実験は、庁舎外の端末から、セキュリティ対策の不備を突いて、ダイアルアップにより不正侵入したものではなく、住基ネットの具体的危険性が明らかになったものではないと主張する（Ｐ１０・ウ(ｲ)）。しかし以下のとおり、被告らの主張は前提の認識自体を誤っているものである。

ア　出先機関（支所、出張所、公民館など）は、夜間･休日に無人になることから、不正侵入するなどして、同所の端末を不正操作したり、不正な工作をするなどして、庁内ＬＡＮに不正侵入することは容易である。

イ　また、相当数の自治体において、保守業者に、遠隔地からリモートによるコンピュータのメンテナンスを許している（丙１３・４５－６項）が、この場合、ダイヤルアップ接続が用いられている。

このように庁内ＬＡＮに外部からのダイヤルアップ接続を使用している場合には、電話番号、ＲＡＳ（リモートアクセスサーバ）ＩＤ、パスワードが分かれば、全世界のどこからでも公衆回線（ＩＳＤＮなど）を経由して庁内ＬＡＮへの侵入が可能となる危険性が高い。

かつ、一旦、ダイヤルアップ接続を許したならば、攻撃端末は、FW の内側の庁内ＬＡＮに接続されている端末と全く同様の環境となるのであって、既存住基サーバ等に対して、直接的攻撃が可能となる危険性を有する。

(3) インターネット経由での庁内ＬＡＮへの侵入に失敗したとの被告らの主張について

ア　実験を行った波田町において、侵入が成功しなかった理由は、実験当時における同町の住基ネットの運用管理の担当者が、セキュリティに関して相当程度の理解を有しており、かつ、迅速適切にセキュリティパッチ当てなどのセキュリティ対策を行っていたことによる。

被告らの主張するように、「ＦＷを突破できなかった」＝インターネット側ＦＷによって攻撃がブロックされたのではない。

イ　しかも、同町において、インターネット経由で庁内ＬＡＮへの侵入ができなかったという「事実」は、波田町という特定の自治体における、実験の時

点（それ以前でも、それ以後でもない）における、かつ限られた実験時間内での「安全性」が確認されたことしか意味しない。

全国３０００以上の市町村においては、このような能力を有する担当者を確保しているとはおよそ考えられないから、他の市町村における「安全性」は全く確かめられていないといいうるものである（実際ＨＰの改ざん等は頻発している）。また、波田町などにおいても、担当者は、２～３年ごとの人事異動により交代するから、このような能力を有する担当者を常に確保し続けるのは極めて困難である。

ウ　また、特にインターネットに接続している以上、自治体としては、今後も永久に、新たなセキュリティパッチが公表されるたびに、迅速確実にパッチを当てる体制をとり続けなければならないという負担を負うことになる。全国の市町村でこのような迅速かつ的確なパッチを当てる能力や経済力を有する自治体は極めて少ないことは明白である。したがって、本実験の結果、波田町と同程度のセキュリティ技術レベルを有していない圧倒的多数の自治体にとっては、庁内ＬＡＮがインターネットと接続されていることは重大な脆弱性であることが明らかとなったというべきである（なお、ⅰ）セキュリティパッチを適用しないと安全性が保てない仕組みとなっていること自体が間違いである。パッチ適用をしなくても、ある程度のセキュリティが保たれる仕組み、例えばパケットフィルタリング、不必要なサービスの停止といった基本的な事項が全く実施されていないことは極めて問題である。さらに、ⅱ）公表されていない脆弱性に対する攻撃に全く対処できない。セキュリティホールはパッチ発表の相当以前に発見されるものであるから、パッチが発表された直後にパッチ当てを行ったからといって、その安全性が“保証”

されるという関係にあるものではない・eEye 社がマイクロソフト社に報告しているが、公表されていない脆弱性については、例えば http:www.eeye.com/html/research/upcoming/index.html などを参照）。

エ　以上の点に加えて、庁内ＬＡＮに不正接続する方法は、インターネット経由だけではなく、他にも多数存在する。

被告らが反論において触れることを避けている、隣接庁舎に庁内ＬＡＮにそのままつながる接続口が存した事実などは、けっして看過し得ない重大な脅威である。

(4)　以上のとおり、セキュリティ対策の不備を突いた庁内ＬＡＮへの侵入は失敗し、この点での安全性が証明されたという被告らの主張が誤りであることは明らかである。

４　いずれのＦＷも突破できていないという被告らの主張について

被告らは、①インターネットと庁内ＬＡＮ間のＦＷ、②市町村設置のＦＷ、③指定情報処理機関監視のＦＷのいずれのＦＷも突破できていないと主張する。これまた事実認識を誤った見解である。

(1) そもそも、前述のとおり、インターネットと庁内ＬＡＮ間はＦＷで防御されたわけではない。

(2)ア　市町村設置のＦＷ（庁内ＬＡＮとＣＳサーバ間）の攻略、及び、当該ＦＷ越しのＣＳの攻略に失敗しているとの被告ら主張について

長野県「侵入実験」においては、限られた時間と環境、さらに不正アクセス禁止法の制約の中で、実際にＦＷ越しのＣＳ攻略実験は行っていないが、バッファオーバーフローを起こさせる攻撃が可能であると判断できる脆弱性が発見されている。よって、ＦＷで防御できているとは言えない。

吉田柳太郎氏は、以下のように述べている。

「ＣＳと既存住基サーバがどのような関数を持って通信しているかということがはっきりと分かっています。この関数は非常に脆弱性の高い関数で、ネットワークの設計者であれば、通常は用いないような関数を多用しているということが分かっておりますので、この関数が持つ脆弱性をつけば、ほぼ間違いなくバッファーオーバーフローを起こすだろうということを想定できております。よって、これは時間さえあれば、必ずこの脆弱性によって起こるバッファーオーバーフローが発生する危険性が極めて高い。よって、それを行ってさえいれば、ファイアウォールを通過してＣＳの管理者権限を奪取するということは可能になっただろうというふうに考えております」（甲２４の１・2004 年 2 月 29 日の長野県本人確認情報保護審議会速記録 12 頁）

イ　そして、前述した、ＣＳ端末に接続されているケーブルに対しタッピングをしたり、ＣＳ端末の側にあるハブに攻撃端末を接続したりすれば、そもそも「ＦＷを突破」する必要がないものである。

(3) 被告らは、被告センター監視のＦＷは突破されておらず、その先の被告センター管理の住基ネット本体部分（都道府県サーバ、センターサーバ、他の市町村のＣＳサーバ）の本人確認情報の閲覧（盗取）にも成功していないと主張する。

しかし、長野県は、不正アクセス禁止法に抵触するため、この範囲について、実験を行っていないのである。実験を行っていないにもかかわらず、「安全性が証明された」と言い得ないことは当然である。

むしろ、後述のように、今回の実験によって判明した事実を綜合すれば、セ

ンターサーバや他の市町村のＣＳサーバへのアクセスも可能と考えられるものである。

(4)　その他にも、①ＦＷの設定ミスを突いたＦＷ越しの攻撃や、②ＦＷ自体の脆弱性を突いてＦＷ自体の乗っ取りをした上で、その先の既存住基サーバやＣＳ、ＣＳ端末の攻撃等は可能である（ＦＷ自体の脆弱性も、次々と発見されているところである）。

５　既存住基システムは、住基ネット本体から区別されるべきであり、既存住基に脆弱性があったとしても住基ネット本体のセキュリティとは直接関係がないとの被告らの主張について

被告らは、庁内ＬＡＮや既存住基サーバなどの脆弱性は、「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」と主張する。

(1)　しかし、既存住基サーバとＣＳとは、住基データ（本人確認情報の異動、住民票の写しの広域交付、他の市町村への異動の場合など）のやりとりをしているのであって、「住基ネット本体」内で保存（流通）する住民の個人情報は、既存住基システムのセキュリティが守られて初めて、その安全性が確保されるものである。よって、「関係がない」などとは到底言えない。

(2)　しかも、既存住基サーバとＣＳとは、相互にやりとりをしているのであるから、前述した既存住基サーバとＣＳ間の通信を行なっているアプリケーションに脆弱性のある関数が使われていることから、既存住基サーバの管理者権限を奪取した上で、例えばＣＳに対する「受動的攻撃」を仕掛けるなどして、ＦＷ越しにＣＳの管理者権限を奪取することが現実的に可能である。

「受動的攻撃」とは、ＦＷなどで区画された攻撃対象に外部から到達する

ことが困難な時に、攻撃対象が、例えば不正なプログラムを仕込んだＨＰ等にアクセスしてくるという行動を引き金として、ＨＰにアクセスしただけでウイルスに感染させるというような攻撃である。ＣＳと既存住基サーバの場合、攻撃対象であるＣＳが、攻撃主体となる既存住基サーバにデータの送信を要求することを引き金として、既存住基サーバからＣＳに対して「受動的攻撃」を仕かけることが可能と考えられる。

したがって、既存住基サーバの脆弱性は、ＣＳ権限奪取などに直結するものと言わざるを得ない。被告ら主張の、既存住基システムは、住基ネット本体とは無関係などというのは、全く成り立たないものである。

６　その他の点について

１　被告らは、

①「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」（33 頁）、

②「適切にパッチがあたっていなければ、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うるという事実は、一般的にそうした可能性があるということ指摘しているにすぎないものである」（34 頁）、

③（ウィンドウズ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、という原告の主張に対して）「原告の主張は、世界で最もシェアを有するＯＳであるウィンドウズを採用しているシステムが全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」（35 頁）などと主張する。

２　しかし、これらはコンピューターネットワークのセキュリティに関する「常識」を無視した恐るべき見解であるといわなければならない。

セキュリティを考えるにあたっては、

①システムにおける脆弱なポイントを洗い出し、

②そのポイントに対してどのような攻撃が想定できるか、

③その場合、どのような被害が想定できるか、を検討し、

④その損害を評価して、費用対効果の観点から、その対策を考えるものである。

被告らは、上述のように、長野県の「侵入実験」は、「通常想定し難い極めて特異な条件の下」であり、「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」から、「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」と評価し、また、上記１の①から③のように、これらは「具体的危険性」ではないと評価している。

つまり、これらの危険性は具体的なリスク（危険性）として評価していないということである。

しかし、既に述べたように、これらの問題は、決してそのように無視できるリスクなどではない。

例えば、そもそも、内部事務関与者であれば、上述の攻撃は容易に行えるものである。たとえば、ラックを開けなくても、ＣＳやＣＳ端末に対する攻撃は容易に可能である。国の主張は、「情報漏洩の７割が内部関与者によるものである」と言われ、現に内部関与者による情報漏えいが頻発している事実を全く無視するものである。

また、部外者であろうと、上述のように庁舎外からでも容易に庁内ＬＡＮやＣＳなどにアクセスできる方法は多数存する。さらに、ソーシャルエンジニアリングの

手法を用いた攻撃例も、多数発生しており（甲１５・『欺術』に詳しく出ている事例を参照されたい）、この危険性に対する対策（セキュリティポリシーの制定と徹底した教育･訓練など）が自治体現場で行われていない具体的危険性を無視するものである。（平成１６年５月２０日の総務省発表資料によれば、同年４月１日現在においても、全国の３１２３市町村の内、「情報セキュリティポリシー」を制定しているところは７４．４％しか存しない。このポリシーが現場で実効的に運用されている可能性は更に低いと言わざるを得ないのは明白である。なお、個人情報保護条例ですら、８２％しか制定されていない。）

さらに、上述したセキュリティホールを突いたバッファ・オーバーフロー攻撃や「受動的攻撃」などは、いまや極めて一般的な攻撃方法となっている。よって、これを無視して安全であるとは到底言えないものである。全国３０００あまりの全自治体は、システムが稼働している限り、未来永劫にわたって、一斉に、かつ、迅速確実にパッチを適用し続けなければならない。もしも一つの自治体でも手当てが遅れるならば、住基ネット全体のセキュリティ強度は一挙に低下せざるを得ない。そのような負担を、資金も能力も乏しい市町村に強いているのが、全国ネットワークである住基ネットシステムである。このように、全国の自治体をその能力にふまえずに、一律にネットワーク化したことによって不可避に生ずるこの克服が困難な脆弱性が、長野県実験によって明らかにされたのである。

少なくとも、被告らにおいて、一般的に上述のような可能性があるという危険性を認識しているというのであれば、その危険性に対する対策が設計され、実施に移されていなければならないものである。被告らの主張は、これらの対策が設計も、実施もされていないことを自白するものであるといわなければならない。

以上述べたように、被告らの主張は全く失当である。

長野県「侵入実験」の結果からは、住基ネットシステムには重大な脆弱性が存し、権限のないものがシステムに侵入し、原告の個人情報を侵害する現実的危険性も明らかとなったと言わざるを得ないものである。

以上