副本

平成１４年(ワ)第８３６号　住民基本台帳ネットワーク差止等請求事件
平成１５年(ワ)第１１４号　住民基本台帳ネットワーク差止等請求事件
原　　告　　成房恵夫　ほか２７名
被　　告　　国　ほか２名

第１０準備書面

平成１７年３月２日

金沢地方裁判所民事部合議特乙係　　御中

被告国及び同石川県指定代理人

合　百　枝　信　肇　美　和　蔵　一　茂
大　村　光　博　紀　正　雅
藤　田　増　佐　岩　中　所　馬
田　木　佐　農　田　場
々

被告国指定代理人

山　口　英　樹
宇　野　雅　憲
上　屋　武　尚
百　藤　和　宏
伊　谷　哲　也
松　老　敬　朗
海　　　　子

被告石川県指定代理人

藤　原　知　朗
柏　野　健　治
広　川　達　也
村　角　美　登

目　次

略語等は，略語一覧によるほかは従前の例による。

（略語一覧）

用　語　……略　語

「長野県侵入実験」に関する聴き取り報告書(甲共第１３号証)　……聴取報告書１

「長野県侵入実験」に関する聴き取り報告書２(甲共第３１号証)……聴取報告書２

第１１回長野県本人確認情報保護審議会議事録（甲共第２３号証の１）

……第１１回審議会議事録

第１２回長野県本人確認情報保護審議会議事録（甲共第２３号証の２）

……第１２回審議会議事録

ネットワーク・セキュリティ調査報告書（甲共第３２号証の１）……第１次報告書

ネットワーク・セキュリティ調査報告書第２次報告書（甲共第３２号証の２）

……第２次報告書

ＣＳサーバ上のアプリケーションに存在するbuffer over flowに関する補足説明

（甲共第３２号証の３）……報告書補足説明

ネットワーク・セキュリティ調査報告書別紙（甲共第３２号証の４）

……報告書別紙

東京地方裁判所において平成１６年１０月１５日に実施された吉田柳太郎証人の証人尋問　……証人尋問

東京地方裁判所において平成１６年１０月１５日に実施された吉田柳太郎証人の尋問調書（甲第３９号証）　……尋問調書

吉田柳太郎証人の平成１６年１１月２６日付け上申書（甲共第４１号証）

……吉田証人上申書

長野県調査速報（乙第１８号証の１，甲共第１２号証の１），知事会見（乙第１８号証の２，甲共第１２号証の２），長野県最終報告（乙第１９号証），第１１回審議会議事録（甲共第２３号証の１），第１２回審議会議事録（甲共第２３号証の２），第１次報告書（甲共第３２号証の１），第２次報告書（甲共第３２号証の２），報告書補足説明（甲共第３２号証の３）及び報告書別紙（甲共第３２号証の４）を合わせて　……長野県各種報告書等

第１　はじめに

原告らは，原告ら準備書面５において，長野県の「侵入実験の結果，住基ネットの安全性が極めて脆弱なものであって，原告ら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（１ページ下から１行目）」と主張し，被告らは，これに対し，被告ら第７準備書面において詳細に反論を加え，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ことを主張した。

被告らは，本準備書面の第２において，被告ら第７準備書面における主張を補充するとともに，本準備書面の第３において，原告ら準備書面１４における長野県侵入実験に関する主張に対し，反論する。

第２　長野県侵入実験により，住基ネットの安全性が明確にされたこと

１　はじめに

(1)　長野県侵入実験の内容及びその結果については，被告ら第７準備書面５ないし８ページにまとめているが，その概要は，別紙「長野県侵入実験の概要」のとおりである。関係各証拠，特に証人尋問の結果によれば，この実験棟により以下の９つの事実が明らかになった。以下の９つの項目のうち，具体的な実験と関係している事柄を整理すると，別紙「実験結果一覧」のようになる。

ａ　実験市町村以外の住民の個人情報に不正にアクセスされる具体的危険性が実証されず，むしろ安全性が確認されたこと

ｂ　インターネットから庁内ＬＡＮへ侵入される具体的危険性は実証されておらず，むしろ安全性が確認されたこと

ｃ　庁内ＬＡＮから市町村設置ファイアウォール越しにＣＳへ侵入される具

体的危険性は実証されておらず，むしろ安全性が確認されたこと

d　ＣＳのＯＳの管理者権限の取得は特殊な実験環境においてされたものであり，通常の状態ではむしろ安全であることが確認されたこと

e　ＣＳ端末のＯＳの管理者権限の取得は，特殊な実験環境下において得られたものであり，通常の状態ではむしろ安全であることが確認されたこと

f　甲共第４０号証の方法により，庁内ＬＡＮから市町村設置ファイアウォール越しにＣＳのＯＳの管理者権限が取得される具体的危険性は実証されておらず，一般論として，そもそも不可能であること

g　住基ネット本体に対する監視が適正に実施されていること

h　既存住基システムの改ざんが直ちにＣＳに反映されるものではないこと及び既存住基システムは住基ネットと峻別してとらえるべきこと

i　庁舎外から庁内ＬＡＮへ侵入される具体的危険性は実験で実証されておらず，むしろ安全性が確認されたこと，及び実験市町村における庁内ＬＡＮの脆弱性は限定的であり、一般論としても、市町村における対策が徹底されていること

(2)　被告らは，以下において，ａからｉまでの各事実に係る証拠を検討した上，住基ネットの安全性に対する原告らの主張が失当であることを明らかにする。

2　実験市町村以外の住民の個人情報に不正にアクセスされる具体的危険性が実証されず，むしろ安全性が確認されたこと（上記ａ）について

(1)　証人尋問等により明らかとなった事実

ア

実験市町村からそれ以外の市町村の住民の個人情報にアクセスするためには，①住基ネット本体に直接侵入する（別紙図面１「①直接侵入する方法」）か，②ＣＳ端末の住基ネットアプリケーションを操作する（別紙図面２「②住基アプリを操作する方法」）かのいずれかが必須と

なること

証人尋問において，吉田証人は，実験市町村の側から実験市町村以外の市町村（証言においては「中野区」を指す。）のＣＳの個人情報に不正アクセスしようとした場合，その方法としては，①指定情報処理機関監視ファイアウォール（別紙図面１（尋問調書中の「丙第２９号証の１」と同じもの）におけるエ）を越えてサーバ（別紙図面１におけるア，イ又はウ）に直接侵入するという方法（尋問調書３８ページ１１行目，別紙図面１におけるＡ，Ｂ又はＣの実線に該当），②実験市町村に置いてあるＣＳ端末（別紙図面１におけるオ又はカ）にある住基ネットアプリケーションを操作して本人確認情報に不正アクセスするという方法が考えられる旨証言している（尋問調書３８ページ２０行目）。

なお，吉田証人は，それ以外に，実験市町村の側から実験市町村以外の市町村のＣＳ（別紙図面１におけるウ）の本人確認情報に不正アクセスする可能性がある旨述べ（尋問調書３８ページ１８，２４行目），その方法について，「既存住基システムの脆弱性をついて，まず管理者権限を奪取します。その状態で，転入転出の作業を行う形にします。で，例えば中野区の住民の方の情報を改ざんして転出しますね。で，実験市町村に対して改ざんした情報を転入という形で持ち込めば，中野区で改ざんされた情報を，実験市町村では改ざんされたまま既存住基システムに埋め込んでしまうということになろうかと思います。」と証言している（尋問調書３９ページ４行目）。

しかし，吉田証人が具体的に述べた転入転出の作業を，実験市町村から行うことは不可能である。なぜなら，中野区の住民の情報は，実験市町村の既存住基サーバにはなく，中野区の既存住基サーバに保存されているから，その改ざんのためには，中野区の既存住基サーバへの侵入が必要とな

るからである。すなわち，吉田証人の述べた方法は，実験市町村の側から実験市町村以外の市町村のＣＳの個人情報に不正アクセスする方法ではないのである。

吉田証人は，実験市町村からそれ以外の市町村の住民の個人情報にアクセスする方法として，他の方法につき言及しておらず，結局①住基ネット本体に直接侵入するか，②ＣＳ端末の住基ネットアプリケーションを操作するかのいずれかの方法が必須となることが改めて確認された。

イ

実験市町村からそれ以外の市町村の住民の個人情報にアクセスするために必須となる①住基ネット本体への侵入，②ＣＳ端末の住基ネットアプリケーションの操作が，実験で行われていないこと

吉田証人は，長野県侵入実験において，指定情報処理機関監視ファイアウォールを越えていずれかのサーバに直接侵入する方法の可否を実験していない旨証言している（尋問調書３９ページ１０ないし１９行目）。なお，このことは，長野県最終報告（６ページ２行目）のほか，長野県調査速報（４ページ），聴取報告書１（１２ページ３行目）にも記載されている。

また，吉田証人は，長野県侵入実験において，実際に住基アプリの操作者権限を取得して，住基アプリを起動する実験はしていない旨証言している（尋問調書４０ページ１４行目，同７９ページ３ないし６行目）。

(2)　小括

ア　上記したところによれば，実験市町村からそれ以外の市町村の住民の個人情報にアクセスするためには，①住基ネット本体に直接侵入するか，②ＣＳ端末の住基ネットアプリケーションを操作するかのいずれかが必須となるところ，長野県侵入実験では，実験の行われたいずれの町村においても，①及び②とも行われていないのであって，実験市町村以外の市町村の

住民の個人情報にアクセスできなかったことが明らかとなった。

イ　なお，聴取報告書２の１３ページ下から２行目には，「少なくとも，正規の操作者が操作者識別カードをカードリーダに挿入した後」，「攻撃端末からＣＳ端末を操作して，その操作者用カードの持ち主である正規の操作者に成りすまし，盗み取ったパスワードを打ち込んで，不正アクセスすることが可能になる」との記載があり，吉田証人もこれに沿う証言をする（尋問調書４３ページ１１行目ないし４４ページ１行目）。しかし，当該方法は，長野県侵入実験では，いずれの町村でも行われていない（尋問調書４４ページ７，８行目）。

一般論としても，当該方法は，ＣＳ端末のＯＳの権限の取得が前提条件となるところ（尋問調書４４ページ１０ないし１２行目），ＣＳ端末のＯＳの権限を取得するだけでも，到底容易とはいえない（ＣＳ端末のＯＳの権限の取得の危険性が確認されなかったことについて，下記６で後述する。）。さらに，当該方法は，正規の職員が操作者識別カードを差し込みパスワードを入力している間にのみ行えるものであり（尋問調書４４ページ１５ないし１９行目），かつ，当該方法により不正操作を行う間，正規の職員の操作画面が不正操作したとおりに動くことから（尋問調書４４ページ下から７ないし４行目），当該方法による不正操作は正規の職員の離席を確認しつつ行う必要があるなど，およそ，現実的な方法とはいえないものである。

このように，長野県侵入実験では，いずれの町村においても，実験市町村以外の市町村の住民の個人情報にアクセスしておらず，また，一般論として指摘する方法も，到底容易とはいえない非現実的なものでしかない。

ウ　よって，同実験において，実験市町村以外の住民の個人情報に不正にアクセスされる具体的危険性が実証されなかったことは明らかである。

3　インターネットから庁内ＬＡＮへ侵入される具体的危険性は実証されておらず，むしろ安全性が確認されたこと（上記ｂ）について

(1)　証人尋問等により明らかとなった事実

ア

波田町のファイアウォールに脆弱性は存在せず，ファイアウォールの権限を取得できる状態になく，安全性が確認されたこと

吉田証人は，波田町の実験では，インターネット経由で市町村が管理するファイアウォール（別紙図面２（尋問調書中の「丙第２９号証の２」と同じもの）におけるア）を越えて公開サーバ（別紙図面２におけるウ）を攻撃する方法（別紙図面２における①）が行われたことを肯定した（尋問調書４６ページ１５ないし１９行目）上で，波田町の実験では，インターネットと庁内ＬＡＮの間のファイアウォール（別紙図面２におけるア）の脆弱性が発見されたか否かにつき，確認していない旨証言している（尋問調書４７ページ６行目）。

しかしながら，吉田証人の上記証言は，長野県各種資料とそごしている。

すなわち，波田町のファイアウォールは，ＤＮＳサーバと兼用になっているところ（報告書別紙４枚目上段の図），当該ＤＮＳサーバについては脆弱性がなかったとされている（第１次報告書２０ページ６行目，２１ページ７行目）。また，そもそも，長野県侵入実験の主な目的は，インターネット経由の侵入の可否を調査することにあった（被告ら第７準備書面５ページ１２行目）のであるから，主目的であったはずの当該ファイアウォールの脆弱性を調査していないとは，到底考えられない。実際にも，阿智村及び下諏訪町においては，市町村設置ファイアウォール（別紙図面２におけるイ）の脆弱性を調査している（第１次報告書１５，１９ページ，第２次報告書１２ページ）。

結局，吉田証人が波田町のインターネットと庁内ＬＡＮの間のファイアウォールの脆弱性が指摘できなかったということは，権限を取得できる状況になく，安全性が確認されたということを意味する。

イ

波田町のファイアウォールが通信を制御し不正アクセスを防御していたこと

(ｱ) 当該ファイアウォールは，インターネットから公開サーバセグメントへの通信を制御し，不正アクセスを防御していたこと

吉田証人は，ファイアウォールがその役割を果たしていたかについては，「ファイアウォールは・・・意図していない通信は防ぐようになっています。波田町もこれになっていました。ただし，偽装された通信を判定できる機能をファイアウォールは持っていません。そういうことだと思います。」と証言し（尋問調書４７ページ７ないし１９行目），波田町のファイアウォールがインターネットから公開サーバへの通信を制御し，不正アクセスを防御していたこと（別紙図面３（尋問調書中の「丙第２９号証の３」と同じもの）における図Ａの状態）を認めている。

なお，ファイアウォールのアクセスルール上，許可された通信が存在し，当該通信がファイアウォールを通過することは当然であり，このことは被告ら第７準備書面（２５ページ１３行目）で既に述べているとおりである。

(ｲ) 当該ファイアウォールは，公開サーバセグメントから庁内ＬＡＮセグメントへの通信を制御し，不正アクセスを防御していたこと

吉田証人は，波田町の実験において，ＤＭＺと庁内ＬＡＮの間の通信（別紙図面４（尋問調書中の「丙第２９号証の４」と同じもの）における(2)）がどのように制御されているかについて確認したと述べた上で

（尋問調書４７ページ下から６行目以下），「ＤＭＺ上からは庁内ＬＡＮのネットワークに通信できないように設定されていました。」と証言し（尋問調書４８ページ１１行目），波田町のファイアウォールが公開サーバセグメントから庁内ＬＡＮへの通信も制御し，不正アクセスを防御していたことを認めている。

なお，吉田証人は，ＤＭＺ上にあるサーバと庁内ＬＡＮ側の通信がどのようなルールで細かく設定されているかによっては，ＤＭＺを踏み台にして庁内ネットワークに侵入するという手だてがあると指摘するが（尋問調書４７ページ最終行ないし４８ページ５行目），設定が不適切であれば，攻撃の余地が広がり，権限取得の可能性が広がるのは当然であり，吉田証人のこの指摘は，一般論としての可能性の指摘にすぎない。吉田証人は，前記のとおり，波田町のファイアウォールについては，「ＤＭＺ上からは庁内ＬＡＮのネットワークに通信できないように設定されていました。」として，それが適切に設定されていたことを暗に認めている。

なお，波田町の実験において侵入が成功しなかった理由について，原告らの提出証拠には，「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ものです（国側が主張するように，「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ありません）。」（聴取報告書２の１０ページ下から４行目，同趣旨として，聴取報告書１の１１ページ１０行目，第１１回審議会議事録１２ページ下から５行目）との記載がある。

被告国が，その準備書面やコメントなどにおいて，「ファイアウォールを突破できなかった」と表現するところの内容は，ファイアウォール

が通信を制御し保護されたネットワークを構築するものであるところ，保護されたネットワークに存在するサーバの権限を，ファイアウォール越しに取得するに至らなかったという意味であり，これは社会通念上，妥当な用い方であるから，上記記載内容は誤っている。

ファイアウォールの許可する通信に対応する脆弱性に対しては，パッチ当てが大切であることは当然であるが，波田町のファイアウォールがインターネットから公開サーバセグメントへの通信（別紙図面４における(1)を制御し，攻撃の可能性を大きく減殺していたことも事実である。さらに，庁内ＬＡＮへの通信（別紙図面４における(2)）も制御していたものであって，ファイアウォールを通過できたとする原告らの主張（原告ら準備書面５の７ページ）は明らかに失当である。

(2)　小括

ア　上記のとおり，実験では，波田町においてインターネットから庁内ＬＡＮへの侵入（別紙図面２における①）が試みられたが，これに失敗している。具体的には，ファイアウォール（別紙図面２におけるア）に脆弱性は存在せず，その権限を取得できる状況になかったため，許可された通信（別紙図面４における(1)①）のみにより，公開サーバ（別紙図面２におけるウ）の権限取得を試みたが成功しなかった。すなわち，庁内ＬＡＮのサーバには攻撃をかける段階にすら至らなかったのであり，完全な失敗と評価できるものであった。

この事実関係は，長野県各種報告書等にも記載されており，また，原告らも，原告ら準備書面等で一貫して認めている。

イ　上記の結果によれば，実験において，インターネットから庁内ＬＡＮへ侵入される具体的危険性（別紙図面２における①）は実証されておらず，むしろ安全性が確認されたことは明らかである。

そして，住基ネットと接続している市町村の庁内ＬＡＮがインターネットと物理的に接続していても，ファイアウォールの適切な設定等の対策を講じることにより，セキュリティを確保できることもまた明らかである。

4　庁内ＬＡＮから市町村設置ファイアウォール越しにＣＳへ侵入される具体的危険性は実証されておらず，むしろ安全性が確認されたこと（上記ｃ）について

(1)　証人尋問等により明らかとなった事実

ア

下諏訪町及び阿智村の市町村設置ファイアウォールに脆弱性は存在せず，その権限を取得できる状態になく，安全性が確認されたこと

吉田証人は，下諏訪町の実験においては，市町村設置ファイアウォール（別紙図面２におけるイ）に脆弱性は発見されず，その権限を取得することはできなかったことを認めている（尋問調書４８ページ下から４行目ないし６行目）。このことは，第１次報告書（１９ページ下から２行目）の記述とも一致している。

なお，吉田証人は，十分な時間などがあれば，色々な可能性が十分発見できた旨証言しているが（尋問調書４９ページ１ないし６行目），具体的なことは何も指摘していない。

また，吉田証人は，阿智村の実験では，市町村設置ファイアウォール（別紙図面２におけるイ）自体の脆弱性は発見されなかったが，管理用ポートが庁内ＬＡＮ側に向けて開いていることが分かった旨述べているものの，実際にこの管理用ポートを用いてファイアウォールの管理者権限を取得したり，これを無効化したりすることはできていない旨証言している（尋問調書４８ページ下から３行，４９ページ７ないし１１行目）。

なお，吉田証人は，ファイアウォールの管理者権限を取得したり，これ

を無効化したりする「可能性があると示しました。」と証言しているが（尋問調書４９ページ１１行目），長野県各種報告書等とそごがある。すなわち，「現時点ではこのポートで提供されているサービスに関しての脆弱性は公開されていませんが，これらに今後脆弱性が発見される可能性は十二分に存在します。」（第２次報告書１２ページ１０行目，同旨として７ページ９行目），「ファイアウォールのバージョンがある一定以下のものであれば」（第１次報告書７ページ１４行目）とされており，管理用ポートが開いていた点は，改善すべき点ではあっても，実験当時，セキュリティ上の脅威となり得る脆弱性ではなかったことは明らかである。

イ

下諏訪町において市町村設置ファイアウォール越しにＣＳのＯＳの権限を取得することに失敗し，安全性が確認されたこと

また，吉田証人は，第１次報告書１７ページ下から７行目以下の記載（下諏訪町の実験においては，既存住基サーバが市町村設置ファイアウォールとの間で授受しているパケットを受信し，解析を試みたが，受信内容を理解することが困難であったため，受信したパケットをそのまま市町村設置ＦＷに送ることを試み，その結果，既存住基サーバと市町村設置ファイアウォールとのやり取りと全く同等の動作をしたが，その意味を確定できなかった旨の記載。注：報告書別紙５枚目，下から１３行目にも記載がある。）について，市町村設置ファイアウォールを越えてＣＳの管理者権限を取得すること（別紙図面２における②）は，実際にはできなかったという意味であることを認めた上で，「時間切れでできなかったというのが事実です。」と証言している（尋問調書４９ページ１２行目ないし５０ページ３行目）。

このように，吉田証人は，市町村設置ファイアウォールを越えてＣＳの

ＯＳの管理者権限を取得することに失敗したことを端的に認めている。なお，吉田証人は，ここでも時間切れでできなかった旨証言するが，どうして時間切れとなったかについては何も説明しないし、時間があったらできたとする具体的根拠は何ら存しない。

ウ

ＣＳの住基アプリに関し，バッファオーバーフローを起こす危険な関数に係る重大な脆弱性を突く実験を行ったものではなく，市町村設置ファイアウォール越しにＣＳの権限を取得し得ることを実験で実証していないこと

吉田証人は，報告書補足説明２段落目及び３段落目の市町村調達ファイアウォールの設定とある部分以降の記載（聴取報告書１の１０ページ１３行目にも同様の記述あり。）の意味について，具体的には，ＣＳの住基アプリにおいて，文字列を扱う際にバッファの境界チェックをしないため，バッファオーバーフローを起こす危険性のある関数を使用しているという，そういう脆弱性があって，これを突いた攻撃を行うことが可能であることを提示したものである旨証言している（尋問調書５０ページ４ないし１４行目）。

しかし，吉田証人は，実際に長野県侵入実験の中で（いずれの町村においても），危険な関数の存在を突いた攻撃を行っていない旨証言している（尋問調書５０ページ１５ないし１７行目）。なお，この証言は，長野県最終報告（１０ページ１９行目）とも符合する。

エ

ＣＳの住基アプリにバッファオーバーフローを起こす危険な関数に係る重大な脆弱性がそもそも存在しないこと

(ア) 住基アプリを直接確認せず，既存住基サーバのアプリを確認し，類推していること（実験が不当なものであることを含む。）

吉田証人は，阿智村の２次実験に関し，住基アプリにおいて，危険な関数が使用されているということを実際に確認した旨証言しているが（尋問調書５０ページ１８ないし２０行目），長野県各種報告書等（報告書補足説明，第２次報告書８ページ，１５ページ）では，一貫して，「ＣＳの住基アプリと通信を行っている既存住基における独自アプリをリアセンブルしたところ，危険な関数の存在が類推された。よって，ＣＳの住基アプリにも同様の危険な関数が存在する可能性が極めて高い。」とされ，ＣＳの住基アプリを直接確認したとはされていないのであって，これとそごを来している。

そのため，この点について，吉田証人は証人尋問において，国ら指定代理人から様々な角度から問いただされたが，結局吉田証人は明確な証言をすることはできず（尋問調書５０ページ２１行目ないし５６ページ１１行目，６１ページないし６２ページ１９行目），最終的には，証人尋問終了後に，原告らから吉田証人上申書が提出された。同上申書で，吉田証人は，「私の記憶は，実験の補助者が行ったディスアセンブルした結果の画面を見せてもらい，それがＣＳサーバのものであったという記憶でした。しかし，「補助者」の一人に確かめたところ，彼は，自分が行ったのは既存住基サーバ側のディスアセンブルであったと述べています。したがって，私の「ＣＳサーバのものであった」という記憶は勘違いであった可能性が高くなります。」と述べており（２ページ，３），住基アプリを直接確認せず，阿智村の２次実験で既存住基サーバのアプリを確認して類推していることをおおむね認めたのである。

(イ) ＣＳの住基アプリに危険な関数に係る重大な脆弱性が存在するとする具体的根拠が存在しないこと

吉田証人は，証人尋問において，長野県各種報告書等に記載された根拠（既存住基の独自アプリからの類推）以外に，ＣＳの住基アプリに危険な関数に係る重大な脆弱性が存在するとの具体的根拠について，何ら示すことができなかった（尋問調書５５ページ１６行目ないし５６ページ１１行目参照）。

(ｳ) 危険な関数については，バッファオーバーフロー対策が可能であり，その場合には脆弱性は存在しないこと

吉田証人は，仮に危険な関数を使用していた場合であっても，バッファへのデータの書き込みをする際に，そのサイズを超える書き込みでないことを確認するような仕組みがとられていればバッファオーバーフローは起きない旨証言している（尋問調書６２ページ４ないし９行目）。

(2) 小括

ア 上記のとおり，実験では，下諏訪町及び阿智村の市町村設置ファイアウォール（別紙図面２におけるイ）に脆弱性は存在せず，その権限を取得できる状態になく，安全性が確認されている。また，下諏訪町において市町村設置ファイアウォール越しにＣＳの権限の取得が実験で試みられた（別紙図面２における②）が，失敗している。

イ 原告らは，ＣＳの住基アプリにバッファオーバーフローを起こす危険な関数に係る重大な脆弱性が存在するため，市町村設置ファイアウォール越しにＣＳの権限を取得することが可能であると強調しているが（原告ら準備書面１２の８，９ページ），実験では全く実証されていない。

ウ そもそも，ＣＳの住基アプリには，バッファオーバーフローを起こす危険な関数に係る脆弱性は存在しない。このことは，国において確認し，公表している（乙第１７号証）。そして，現在では，このことは，長野県自身が，「事後の確認によりその点への措置ができていたことがわかっている。」としており（乙第２９号証の【実験内容について】の項目４．９），

この長野県の見解は吉田証人も確認しているものである（乙第２９号証の【実験内容について】の項目４．９は，脚注において，「＊吉田柳太郎氏に回答を求めている部分」とされているように，総務省が７月２７日付けで長野県に文書で報告を求めた（乙第３０号証）のに対して，長野県が吉田証人に照会，確認しつつ，作成したものである。）。

このように，客観的な事実として，脆弱性が存在しないことは，明らかである。

そもそも，阿智村の２次実験では，危険な関数の存在につき，住基アプリを直接確認せず，既存住基サーバのアプリを確認し，類推するという方法によったものであるが，その方法は，そもそも推論として破綻している。すなわち，既存住基の独自アプリは，各ベンダが開発するものであり，それに対しては通信制御部分のみの仕様が示されているものであるところ，それはインターフェース仕様のみであり，関数はもちろん，既存住基側の処理方法，開発言語などについても指定されていない（甲第３９号証中の丙第２９号証の５）。よって，仮に既存住基のアプリにおいて危険な関数が実際に使われていたとしても，同じ関数をＣＳの住基アプリで使用している可能性は高くも低くもない。

さらに加えていえば，吉田証人も認めているとおり，これらの関数は，存在すると不可避的に危険であるというものではなく，対策を講じることにより脆弱ではなくなる。よって，危険な関数の存在が類推されただけで，「バッファ・オーバーフローを起こす重大な脆弱性」（聴取報告書２の７ページ）の存在が類推されたということにはならない。

エ　上記アないしウの結果によれば，長野県侵入実験の行われたいずれの町村においても，庁内ＬＡＮから市町村設置ファイアウォール越しにＣＳへ侵入される具体的危険性（別紙図面２における②）は実証されておらず，むしろ安全性が確認されたというべきである。

5　ＣＳのＯＳの管理者権限の取得は特殊な実験環境においてされたものであり，通常の状態ではむしろ安全であることが確認されたこと（上記ｄ）について

(1)　証人尋問等により明らかとなった事実

ア

ＣＳのＯＳの管理者権限の取得は，特殊な実験環境の下で行われたものであること

吉田証人は，阿智村の２次実験においてＣＳを攻撃してＯＳの権限を取得する実験（別紙図面２における④）が試みられたこと，同実験は重要機能室内に入って実施したこと，重要機能室は通常は施錠して管理がされていること，同実験の際には通常は施錠されているラックの鍵を開けて，その中のハブに調査用のパソコンを接続したこと，このような方法は，市町村設置ファイアウォール（別紙図面２におけるイ）は物理的に回避されていて，ＣＳセグメントに直接調査用ハブのパソコンが接続された状況と同じであることを明確に証言している（尋問調書５６ページ１３行目ないし５７ページ１４行目）。

なお，阿智村の２次実験における実験環境については，長野県最終報告（７ページ１７行目），聴取報告書１（９ページ２行目），第１２回審議会議事録（１２ページ１６行目）にも同旨の記述がある。

イ

市町村設置ファイアウォール越しに，ＣＳのＯＳの管理者権限の取得に成功しておらず，むしろ失敗していること

吉田証人は，かかる特殊な実験環境（阿智村の２次実験）以外においては，実際に市町村設置ファイアウォールを通過して，ＣＳのＯＳの管理者権限を取得することはできなかったことを認めている（尋問調書５７ペー

ジ２２ないし２５行目）。

なお，吉田証人は，隣接施設から実験を行った可能性を指摘しているが（尋問調書５７ページ１５ないし２１行目），当該場所から実験は行われていない（長野県最終報告７ページ下から９行目）。なお，そもそも当該場所からは既存住基サーバにすらアクセスできない構成となっていたものであり，攻撃はし得なかったものである（乙第３１号証の２，別添資料の質問調査項目４－４）。

(2)　小括

ア　以上述べたところによれば，阿智村の２次実験においてはＣＳのＯＳの管理者権限の取得に成功しているものの，同実験は，物理的に庁舎内に立ち入り，通常は施錠されている重要機能室に立ち入り，さらに通常は施錠されているラックを開けた実験環境において得られたものにすぎないのである。

イ　そして，同実験では，市町村設置ファイアウォール越しに，ＣＳのＯＳの管理者権限の取得（別紙図面２における②）に成功しておらず，むしろ，試みはしたが失敗しているものである。

ウ　原告らは，特殊な実験環境がなくとも，ＣＳセグメントのハブやＣＳ端末自体に攻撃端末をつなぎ込んで行うという方法もある旨主張する（原告ら準備書面１２の４ページ）。しかし，当該方法は，実験で行っておらず，かつ，一般論としても，当該ハブやＣＳ端末は執務室内に存在するものであり，これを探すこと，不法侵入を行うこと，攻撃端末を差し込んで攻撃を行う間，職員の目を欺くことなどが必要となるものであって，到底容易とはいえない。

エ　上記の事実によれば，ＣＳのＯＳの管理者権限の取得は，特殊な実験環境下においてなされたものであり，通常の状態ではむしろ安全であることが確認されたというべきである。

6　ＣＳ端末のＯＳの管理者権限の取得は，特殊な実験環境下において得られたものであり，通常の状態ではむしろ安全であることが確認されたこと（上記ｅ）について

(1)　証人尋問等により明らかとなった事実

ア

ＣＳ端末において，セキュリティホール対策が適切になされていたこと

吉田証人は，阿智村の２次実験の際に，ＣＳの端末を攻撃してＯＳの権限を取得するために攻撃が試みられた（別紙図面２における⑤）が，ＣＳ端末にはパッチが適切に適用されていたことを認めている（尋問調書５８ページ３ないし８行目）。

このことは，長野県最終報告（１０ページ１２行目）の記述とも合致する。

イ

長野県調査速報において，ＣＳ端末の脆弱性の有無，権限取得の方法という重要な事実につき誤って記載していたこと

吉田証人は，長野県調査速報の添付図４ページについて，ＣＳクライアントについて，リモートからのバッファオーバフローによる管理者権限の取得に成功した旨の記載であり，実際の実験（阿智村の２次実験）の経過には合致しないことを認めた上，そのような記載がされた理由について，「最終報告書ではＩＤとパスワードだったというふうに報告しました。よって，この中間報告では不正確な情報という形で報告を出しました。最終的に気が付くには時間がかかりました。」と証言している（尋問調書５８ページ９ないし１９行目）。

このように，長野県調査速報において，ＣＳ端末の脆弱性の有無，権限取得の方法という極めて重要な事実につき誤って記載していた事実は，長野県侵入実験が，信用できないものであることを端的に示すものである。

この点について，吉田証人は，上記のとおり，長野県調査速報（中間報告の意。）は不正確な情報という形で報告を出したと説明するが，関係各資料にはこれに沿う記載はない。しかも，長野県最終報告などで明確な訂正も行われていない。

なお，実験の指揮監督者である吉田証人自身，長野県調査報告の際の知事会見において，「エクスプロイトによって略奪したＣＳクライアント」（知事会見６ページ下から１０行目）と説明していることから，資料の一部の記載が単に誤記されていたものではなく，完全に同証人の認識に誤りがあったことは明らかである。

ウ

ＣＳ端末のＯＳの管理者権限の取得は，特殊な実験環境下で得られたものであること

吉田証人は，阿智村の２次実験におけるＣＳ端末のＯＳの管理者権限については，ＣＳから得られたＩＤとパスワードを入れる方法によったものであることは認めている（尋問調書５８ページ最終行ないし５９ページ７行目）。

なお，第１２回審議会議事録１０ページ下から１行目，第２次報告書１４ページ下から６行目にもこれに関係する記述がある。

いずれにしても，ＣＳ端末のＯＳの管理者権限の取得は，特殊な実験環境下，すなわち，庁舎内に立ち入り，施錠されている重要機能室に立ち入り，ラックの鍵を開けてＣＳのＯＳの管理者権限を取得して，そこから得られたＩＤとパスワードを活用して同じ環境下でこれを打ち込むという条

件の下で得られたものである。

エ

ＣＳ端末のＯＳの管理者権限の取得は，仮に強固なＩＤ，パスワードが設定されていれば，特殊な実験環境下であっても得られなかったものであること

吉田証人は，強固なＩＤ，パスワードが設定されているとすれば，十分なパッチが当たっていれば，ある一定レベルのセキュリティは確保できていたと証言している（尋問調書５９ページ８ないし１３行目）。

そうすると，実験（阿智村の２次実験）当時は，十分なパッチが当たっていたのであるから（上記ア），吉田証人は，仮に強固なＩＤ，パスワードが設定されていれば，特殊な実験環境下であっても，権限の取得に至らなかったことを認めたものといえる。

(2)　小括

ア　上記のとおり，阿智村の２次実験では，ＣＳ端末において，セキュリティホール対策が適切にされていたことが確認されたものであって，実験で得られたＣＳ端末のＯＳの管理者権限の取得は，特殊な実験環境下，すなわち，庁舎内に立ち入り，施錠されている重要機能室に立ち入り，ラックの鍵を開けてＣＳのＯＳの管理者権限を取得して，そこから得られたＩＤとパスワードを活用して同じ環境下でこれを打ち込むといった環境下で得られたものにすぎない。

このような結果によれば，ＣＳ端末のＯＳの管理者権限の取得は，特殊な実験環境下において得られたものであり，具体的危険性があったことを示すものではないことは明らかである。

イ　また，仮に強固なＩＤ，パスワードが設定されていれば，特殊な実験環境下であっても，なお，ＣＳ端末のＯＳの権限取得という結果は得られな

かったことも確認されている。

現在，実験市町村において，パスワードは類推困難なものにするなど改善されている（乙第３１号証の２及び第３２号証の２，別添資料の質問・調査項目８－１）。

また，全国の市町村においても，今年度も，チェックリストを活用して市町村におけるセキュリティ対策の徹底を図ったところ，強固なＩＤ，パスワードの設定について，この中で重要点検項目に位置づけて特に徹底し，全団体において３点満点を達成しているものである（乙第３３号証）。

7　甲共第４０号証の方法により，庁内ＬＡＮから市町村設置ファイアウォール越しにＣＳのＯＳの管理者権限が取得される具体的危険性は実証されておらず，一般論として，そもそも不可能であること（上記ｆ）について

(1)　証人尋問等により明らかとなった事実

ア

当該方法を，実験で行っていないこと

吉田証人は，実際に当該方法を長野県侵入実験において実施したことはなく，単に可能性を提示したにすぎない旨証言している（尋問調書５９ページ１４ないし１８行目）。

イ

当該方法は，生年月日を確認するプログラムの部分に特定の危険な関数が使用されていることが条件であるが，これは存在しないこと

吉田証人は，当該方法が成功する条件について，第１に，生年月日を確認するようなプログラムの部分に，特定の危険な関数が使用されているという脆弱性が存在する必要がある旨証言している（尋問調書５９ページ１９ないし２３行目）。

ところで，ＣＳの住基アプリにおいて，そのような脆弱性は存在しない。すなわち，ＣＳの住基アプリでは，既存住基から送信されたデータ（生年月日のみならずすべてのデータ）について，その長さをチェックし，適切な長さのデータ長のみ，次の処理に渡す（異常な長さのデータ長である場合にはエラーとして破棄し，その旨，既存住基側に通知する）ようにプログラムされている。

よって，「生年月日の日付に１０００桁のような大きな情報を入れると異常な行動を起こす可能性があるＣＳ側のプログラム関数」（甲共第４０号証本文１ないし２行目）という条件は成立し得ない。

ウ

当該方法は，ＣＳからの通信が発生することが条件であり，発覚しやすい方法であること

吉田証人は，当該方法が成功する条件として，第２に，ＣＳの側から既存の住基サーバに向けて何らかの通信がされている必要がある旨証言している（尋問調書５９ページ下から３行目）。

ところで，「受動的攻撃」という言葉からも明らかであるが，当該方法は，ＣＳの側から既存住基サーバに通信がされるタイミングでしか攻撃を行うことができない。そして，通常の記載，修正においては，ＣＳは通信の起点とならず，ＣＳから既存住基サーバへ通信を行う場合は，ＣＳが，①広域交付の請求を他市町村から受信した場合，②転入転出特例に係る転出証明書情報を他市町村から受信した場合，③転入通知情報を転入地から受信した場合に限られている。当該方法は，これらの通信が発生するまで，既存住基サーバに不正侵入の証拠となる不正プログラムを埋め込んだままにしておく必要があるから，発覚しやすい方法であるといえる。

エ

当該方法は，既存住基サーバのＯＳの権限の取得が条件であり，これは到底容易とはいえないこと

吉田証人は，当該方法を成功させる条件として，第３に，既存住基の側のＯＳの権限を取得している必要がある旨証言している（尋問調書６０ページ１ないし３行目）。

しかし，下諏訪町及び阿智村の１次実験では，既存住基サーバのＯＳの権限の取得に成功しているが（別紙「長野県侵入実験の概要」），役場の許可を得て庁舎内に立ち入り得た結果であって（別紙図面２における③），通常の状態で成功したものではない。

一般論としても，不法侵入，不正アクセス等禁止法違反を伴い，サーバを特定すること，重要機能室などの物理的セキュリティ対策を回避すること，職員の目を欺くことなどが必要であるから，到底容易であるとはいえない。

オ

当該方法は，遠隔操作のため，ファイアウォールの権限の取得等が条件であり，これは到底容易とはいえないこと

吉田証人は，当該方法を成功させる条件として，仮にＶＮＣをインストールして遠隔操作を実施しようとした場合には，受動的攻撃を行うだけではなくて，ファイアウォールの権限を取得してアクセスルールを変更するなどの作業を行う必要はない旨証言している（尋問調書６０ページ４ないし１７行目）。

しかし，吉田証人の証言に，具体的根拠はない。ＶＮＣについては，ファイアウォールのアクセスルールにおいて特殊なポートを通信可能に設定する必要があるから，当該方法の条件として，市町村設置ファイアウォー

ル及びインターネットと庁内ＬＡＮの間のファイアウォールの権限を取得し，その設定を変更する必要がある。

なお，ＶＮＣにおいてポート番号を変更することも考えられるが，そもそも市町村設置ファイアウォール及びインターネットと庁内ＬＡＮの間のファイアウォールのアクセスルールを知らなければ，これを行うこともできない。

(2)　小括

上記のとおり，当該方法は，何ら実証されたものではなく，一般論としても，当該方法は，生年月日を確認するプログラムの部分に特定の危険な関数が使用されていることが条件となるところ，これは存在しないから，そもそも不可能である。

また，当該方法を実施するためには，既存住基サーバのＯＳの権限の取得や，遠隔操作のためファイアウォールの権限の取得等が必要となるが，これらは到底容易とはいえない。さらに，当該方法は，ＣＳからの通信が発生することが条件であり発覚しやすい方法でもある。

以上より，甲共第４０号証の方法により，庁内ＬＡＮから市町村設置ファイアウォール越しにＣＳのＯＳの権限が取得される具体的危険性は実証されておらず，一般論として，そもそも不可能であることは明らかである。

8　住基ネット本体に対する監視が適正に実施されていること（上記ｇ）について

(1)　証人尋問等により明らかとなった事実

ア

指定情報処理機関監視ファイアウォールが２４時間の即時監視を行っていること及び証人がこれを誤って認識していたこと

吉田証人は，県調達ファイアウォール（吉田証人は，このように表現し

たが，正確には，県が設置するものではなく指定情報処理機関が設置するものである。以下，「指定情報処理機関監視ファイアウォール」という。）は，２４時間で生き死にのみの監視を行っていると認識している旨証言している（尋問調書６２ページ下から５行目ないし６３ページ最終行まで）。

しかしながら，客観的な事実として，指定情報処理機関監視ファイアウォールは，２４時間の即時監視を行っている（乙第３４号証，尋問調書中の「丙第２９号証の６」）のであって，吉田証人は，明らかに誤解している。

イ

実験において指定情報処理機関監視領域のケーブルが外されたこと及び被告財団法人が適切な監視をしていること

吉田証人は，阿智村の２次調査の際に，指定情報処理機関監視ファイアウォールとＣＳとの間にあるハブのＣＳ側のケーブルを外したこと，その場所が，甲第３９号証中の丙第２９号証の８中の①番である旨証言している（尋問調書６４ページ１ない８行目。なお，聴取報告書１の１０ページ下から５行目にも同様の記載がある。）。

しかし，被告ら第７準備書面（２７ページ１５行目）で述べたとおり，これは客観的事実に反するものであり，外したケーブルは甲第３９号証中の丙第２９号証の８中の②番である。

仮にこれが①番であるとすれば，①番を外したことにより，①番より住基ネット本体側にある指定情報処理機関監視ファイウォールの監視の状況が判明することは論理的にあり得ないのである。仮に①番の箇所が外されたのであれば，１５分おきの定期監視の記録しか採取できず，甲第３９号証中の丙第２９号証の７のような秒単位の即時監視の記録を採取すること

はできない（甲第３９号証中の丙第２９号証の６）。したがって，外されたケーブルが２４時間即時監視の領域である②番であることは明らかである（乙第３５号証）。

吉田証人はこうした誤った事実認識を，実験の結果判明したこととして発表している（知事会見７ページ下から８行目）にすぎないのである。

なお，吉田証人は，外したとたんにＬＡＳＤＥＣの方から第一報が来ましたと発言しているが（知事会見７ページ下から１２行目），このことからも抜いた箇所が即時監視箇所であることに疑いの余地はない。

(2)　小括

上記のとおり指定情報処理機関監視ファイアウォールを含め住基ネット本体側は，被告財団法人が２４時間の即時監視を行っている。

これを事実を把握することなく，誤解を基に監視がずさんであるとする批判は明らかに不当である。

そして，阿智村の２次実験において指定情報処理機関監視領域のケーブルが外されたことは，大いに不当な事実であるが，かかる行為により，被告財団法人の２４時間即時監視が適切に行われている（通報アラーム及びログの記録）ことが明らかになったといえる。

以上のとおり，長野県各種報告書等においてなされている住基ネットの監視に関する批判は不当であり，実験において，むしろ適正な監視が実施されていることが確認されたことは明らかである。

9　既存住基システムの改ざんが直ちにＣＳに反映されるものでないこと及び既存住基システムは住基ネットと峻別してとらえるべきこと（上記ｈ）について

(1)　証人尋問等で明らかとなった事実

ア

実験市町村の既存住基システムとＣＳが同期を取っていないこと

吉田証人は，既存住基も住基ネットに含まれるという考えを示し，その理由として，既存住基とＣＳが同期を取っていて，既存住基中のデータの変更や削除などがそのままＣＳに反映するという関係にあるからである旨証言し，既存住基とＣＳが同期を取っていることを，阿智村の実験において確認した旨証言している（尋問調書６６ページ１ないし１１行目）。

さらに，吉田証人は，長野の審議会の中でその旨の発言をした記憶がある旨証言し，次いで，確認の方法につき，「審議会の議事録に残ってると思うんですが，データベースのレコードレイアウトですね，どういった情報をそのデータの中に格納するようになっているかというのを確認して，１４項目１４情報が移動するようになっている，つまり４情報と言われているようなログ情報だけではないということを確認したという話をした記憶があります。」と証言している（尋問調書６６ページ１２ないし２６行目）。

このように，吉田証人は繰り返し長野県侵入実験において確認したと述べているが，そのような記述は，議事録を含む長野県各種報告書等に一切ない。

そして，実験市町村における既存住基とＣＳは同期を取っていないことは客観的な事実である（乙第３１号証の２及び第３２号証の２，別添資料中，質問・調査項目５－１）。

なお，長野県は，乙第２９号証（【実験内容について】の項目４．６）において，実験を行ったいずれの町村においても，既存住基の改ざんがＣＳに反映される可能性があるかを「確認はしていない。」と回答している。また，長野県は，どのような場合に既存住基の改ざんがＣＳに反映され得るかについて，「住民票の広域交付，転入転出の際にＣＳに反映されると考える。」とも回答しているが，広域交付の場合は，一切，ＣＳ，都道府県サーバ，全国サーバの４情報等が反映されるものではないし，転入転出

特例についても，虚偽の転出届が加えてなされ，かつ窓口職員がこれを見逃した場合に限られる。

また，既存住基が改ざんされた場合，当該改ざんされた情報が，住民票の広域交付や，転入転出特例により，請求されることは論理的にあり得るが，このことは，通常の住民票の写し等の請求や，通常の転出届による転出証明書の取得においても同様であるから，住基ネットの問題ではない。むしろ，広域交付及び転入転出特例ともに，住民基本台帳カードなどによる厳格な本人確認が義務付けられているから，通常の請求や届出に比べ，改ざんされた情報を請求し，引き出すことは，はるかに困難である。

イ

既存住基が住基ネットの範囲に含まれるとする主張は，総務省がかつてしたものでもないこと

吉田証人は，総務省は当初は既存住基も住基ネットの一部に含まれるという見解を取っていたが，実験後にその主張を変更して，責任の限定を図っている旨証言している（尋問調書６７ページ１行目ないし４行目）。そして，そのような認識を抱いている理由は，吉田証人も委員として出席していた長野県公開討論会でのやりとりであると証言している（尋問調書６７ページ５ないし２０行目）。

しかし，吉田証人が指摘する長野県公開討論会のやりとりでは，総務省の井上課長の発言を踏まえて，長野県本人確認情報保護審議会の佐藤委員は，「今はっきりしたのは，国が言っている住基ネットという範囲は，国と県を結ぶネットワークだけではなくて，そこにつながっている市町村のＣＳ，並びにそこにアクセスできるＣＳ端末までを含めて住基ネットと言うと，こういう定義でございます。そうしますと，安全だとおっしゃるということは，ＣＳ並びにＣＳ端末まで含めて全体が安全だとおっしゃって

いることになります。」と述べ，既存住基システムは住基ネットには含まれない旨明確にしている（乙第３６号証，１６ページ下から９行目）。

このように，総務省は実験前から一貫して，既存住基は住基ネットとは別であると説明しているのであって，吉田証人が指摘するように，公開討論会でこれと違う見解を示したとか，実験前に違う説明をしていた事実はない。

(2)　小括

ア　通常，既存住基システムは，データベースを書き換えただけで，自動的にＣＳに送出されるような仕組みで構成されていない（被告ら第７準備書面２３ページ６行目）。上記のとおり，実験市町村でも，既存住基システムとＣＳは同期を取っていないことが確認されている。

イ　既存住基は，住基ネット導入と関係なく従来から存在するものであり，かつ，個別の市町村において設置され管理されるものであるから，住基ネットの範囲に包摂されるものではない。

また，住基ネットセキュリティ基準（乙第１号証，第１号証の２及び３）において，「住民基本台帳ネットワークシステム」が定義されているが，既存住基は含まれていない（第１，１）。既存住基のセキュリティの確保については，別途，「住民票に係る磁気ディスクへの記録，その利用並びに磁気ディスク及びこれに関連する施設又は設備の管理の方法に関する技術的基準（昭和６１年自治省告示第１５号，乙第３７号証）が定められ，「住民記録システム」（第１，一）として，技術的基準が定められているものである。

そして，既存住基とＣＳが同期を取っているという指摘が誤りであることは上記のとおりであって，既存住基システムは住基ネットと峻別してとらえるべきことは明らかである。

また，既存住基が住基ネットの範囲に含まれるとする主張は，総務省

がかつて主張したものでもない。原告らの主張は失当である。

ウ　以上より，原告らの「既存住基サーバ内の個人情報（本人確認６情報）を書き換えたり，削除したりすれば，そのデータがそのままＣＳサーバ内の本人確認情報に反映し，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」との主張（原告ら準備書面５の５ページ）や，既存住基システムを住基ネットの一部としてとらえなければならないという吉田証人の見解（聴取報告書１の３ページ，尋問調書６６ページ１ないし６行目）が，失当であることは明らかである。

10　庁舎外から庁内ＬＡＮへ侵入される具体的危険性は実験で実証されておらず，むしろ安全性が確認されたこと，及び実験市町村における庁内ＬＡＮの脆弱性は限定的であり，一般論としても，市町村における対策が徹底されていること（上記ｉ）について

(1)　証人尋問等により明らかとなった事実

ア

庁舎外から庁内ＬＡＮへ侵入できていないこと

吉田証人は，長野県侵入実験の評価として，庁舎外から庁内ＬＡＮに侵入される危険性が実証されたか否かについて，脆弱性を突くという形には至らなかった旨証言し（尋問調書６７ページ２１行目ないし６８ページ７行目），実験を行っていずれの町村においても，庁舎外から庁内ＬＡＮに侵入できていないことを端的に認めている。

なお，吉田証人は，実験にもっと長い時間があり，もっと多くの自治体で行ったならば，危険性が実証できるところがあった旨証言するが（尋問調書６８ページ８ないし１０行目），一般論としても，何らの根拠も存しない。

イ

ダイヤルアップ接続に係る脆弱性をついて，庁舎外から庁内ＬＡＮに侵入できていないこと

吉田証人は，ダイヤルアップ接続を用いた侵入について，阿智村（１次実験）において，出先機関のダイヤルアップ・ルータに調査用のパソコンを接続して庁内ＬＡＮに接続して実験した旨証言するが（なお，聴取報告書１の７ページ１０行目以下に同旨の記載がある。），かかる実験は，役場の許可を得て，職員の案内によりその場所に立ち入って接続を行ったものであることは吉田証人自身も認めており（尋問調書６８ページ１１ないし２３行目），阿智村において，ダイヤルアップ接続に関する脆弱性が存在し，これをついて庁舎外から庁内ＬＡＮに侵入したものではないことが確認された。

このように，実験において，ダイヤルアップ接続に係る脆弱性をついて，庁舎外から庁内ＬＡＮに侵入できていないことが明らかである。

ウ

ダイヤルアップアカウントが知られただけで危険であるとはいえないこと

吉田証人は，何者かにこのダイヤルアップ・アカウントが知られた場合は，世界中のどこからでもこの庁内ＬＡＮに接続することが可能である旨証言している（尋問調書６８ページ下から３行目ないし６９ページ下から９行目。なお，聴取報告書１の７ページ１０行目，聴取報告書２の１０ページ下から８行目においても，同様の記載がある。）。

しかし，一般論として，発信者番号の偽装は困難である。このため，発信者番号認証などが有効なセキュリティ対策として認識されている。証人

の見解は，具体的な根拠に欠け，失当であることは明らかである。

よって，原告らの「このことは，何者かにこのダイヤルアップアカウント（電話番号等）が知られた場合は，世界中のどこからでも，この庁内ＬＡＮに接続（侵入）することができるということを意味する」という主張は明らかに失当である。

エ

阿智村では，ダイヤルアップ接続に係る脆弱性は存在せず，むしろ安全性が確認されたこと

吉田証人は，阿智村では，発信者番号の認証が必要とされているかどうか確認していない旨述べているが（尋問調書６９ページ１６ないし１８行目），阿智村では，実験当時も現在も，発信者番号認証が対策として設けられ，特定の番号，すなわち，出先機関のダイヤルアップ・ルータからでなければ庁内ＬＡＮのリモートアクセスサーバに接続できない構成となっている（乙第３１号証の２，別添資料中の質問・調査項目４－４）。さらに，物理的に侵入され直接ダイヤルアップ・ルータに繋ぎ込まれる脅威に対しても，当該ダイヤルアップ・ルータは執務室の奥，一般の目が届かない箇所に配置されるなどの対策が講じられている（乙第３１号証の２，別添資料中の質問・調査項目４－３）。なお，実験では，職員が当該場所まで案内したものである。

これらによれば，阿智村においては，ダイヤルアップ接続に係る脆弱性は存在していなかったことは明らかである。

オ

無線ＬＡＮに係る脆弱性をついて，庁舎外から庁内ＬＡＮに侵入できていないこと（実験の不当性が明らかになったことを含む）

吉田証人は，実験を行ったいずれの町村でも，無線ＬＡＮを経由して庁内ＬＡＮに侵入できることが確認できた事実はない旨証言し，実際の実験においては，下諏訪町で無線ＬＡＮ環境を構築して，その無線ＬＡＮ環境から接続を試みた旨証言している（尋問調書６９ページ１９行目ないし７０ページ４行目）。

このことは，長野県最終報告（７ページ下から３行目，「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。」），聴取報告書１（７ページ下から６行目）の記述とも合致する。

このように，下諏訪町において，無線ＬＡＮに係る脆弱性が存在し，これをついて庁内ＬＡＮに侵入したものではなく，実験において，無線ＬＡＮに係る脆弱性をついて，庁舎外から庁内ＬＡＮに侵入できていないことが明らかとなった。

なお，吉田証人は，無線ＬＡＮというものを正しく設定しなければ非常に危険であるという話をした記憶があると述べる（尋問調書６９ページ下から２行目）。これは，知事会見を指していると思われるが，無線ＬＡＮを調査環境として構築したことを明確にせず，逆に，「無線ＬＡＮを通じて庁内のネットワークに入ることが分かったということになります。」（知事会見１３ページ１２行目）と説明したため，下諏訪町において無線ＬＡＮが通常，基幹系業務で使われており，これに脆弱性があり，侵入ができたとの誤解を生み，下諏訪町の信用失墜と，住民の無用の不安を醸成した（乙第３２号証の２，別添資料中の分類１１）。

カ

阿智村において，隣接施設から侵入される脆弱性は存在せず，むしろ安全性が確認されたこと

吉田証人は，阿智村の１次実験において，隣接する施設（コミュニケーションセンターのこと）の会議室から侵入を試みたことを明らかにした上（尋問調書７０ページ５ないし１１行目。なお，聴取報告書１の６ページ下から３行目，第１次報告書７ページ下から９行目に，これに係る記載がある。），当該施設は夜１０時までだれでも立ち入れる部屋で，使用されていない時は施錠はされていない部屋である旨証言している（尋問調書７０ページ１５ないし２５行目，７３ページ１９行目ないし７４ページ１１行目）。

しかし，結局のところ，吉田証人は，実験以外のときに施錠がされているかどうかは確認していない旨証言しているし（同７４ページ１２，１３行目），客観的な事実としても，実験当時も現在も，当該コミュニケーションセンター自体は午後１０時まで立ち入れるが，その中の会議室は，通常は施錠管理され，立ち入ることはできず，また，当該会議室は主に公用で使用するものであり，例外的に使用を許可する場合でも，予約制で利用者，目的，使用時間を管理しているのである（乙第３１号証の２，別添資料中の質問・調査項目４－２）。すなわち，第１次報告書７ページ下から９行目における「不特定多数の人間が出入りしさらに不特定多数の人間が自由に使用することの可能な会議室」という記述は，事実に反する。

実際に，阿智村の１次実験では，会議室の鍵を職員が解錠しており（乙第３１号証の２，別添資料中の質問・調査項目４－２），職員に案内されて立ち入ったことは，吉田証人も認めている（尋問調書７３ページ下から３行目）。

なお，聴取報告書１（７ページ３行目）において，「このネットワークにおいては，接続されたコンピュータに対し，ＩＰアドレスをＤＨＣＰで自動的に割り当てるようになっていたため，物理的にケーブルを繋ぎさえすれば，ネットワーク技術に関する知識がない者でも庁内ＬＡＮに接続可

能となった。」と，あたかも阿智村あるいは下諏訪町のセキュリティに問題があるかのような指摘があるが，一般的に会議室であれば，ＤＨＣＰで接続するようになっていることは普通のことであり，何ら脆弱性を示すことにはならない。なお，阿智村及び下諏訪町のＣＳセグメントについては，ＤＨＣＰで自動接続となるものではない（乙第３１号証の２及び第３２号証の２，別添資料中の質問・調査項目２－７）。さらに，阿智村では，実験後，当該会議室のハブから伸びている回線を，通常時はサーバから外し，必要な場合に殊更，繋ぎ込むという運用面での対策を講じることとし，さらに安全性を向上させている（乙第３１号証の２，別添資料中の質問・調査項目１０－２）。

キ

実験市町村においてＣＳ端末の配置が適切であったこと及び一般的に当該対策が徹底されていること

吉田証人は，阿智村，下諏訪町において，ＣＳ端末の背面にケーブルがむき出しにしてあったり，操作者識別カード読み取り装置のＵＳＢの接続線がむき出しにしてあるところが多数あった旨証言し，そのことを実際に長野県侵入実験の際や長野県の審議委員として自治体を回ったときにも確認した旨証言している（尋問調書７０ページ最終行ないし７１ページ７行目。なお，聴取報告書１の７ページ下から３行目にも同趣旨の記載がある。）。

そして，吉田証人は，その旨の記載は長野県の審議会の議事録の中に記録が残っている旨証言している（尋問調書７１ページ８ないし１１行目）。

しかしながら，長野県各種報告書等においては，実験市町村のＣＳ端末の配置状況について脆弱性があったとの指摘は一切なく，吉田証人の証言は誤りである。

客観的な事実としても，実験当時から現在まで，阿智村及び下諏訪町とも，ＣＳ端末は来庁者が容易に触れることはできない位置に配置されており，安全性が確保されていたものである（乙第３１号証の２及び第３２号証の２，別添資料中の質問・調査項目３－２）。

なお，吉田証人は，一般論として，同様の状態を他の市町村でも目で見たとしているが（尋問調書３３ページ），客観的な根拠は何もない。また，全国の市町村において，チェックリスト（ＣＳ端末については，管理目標9）により，対策が徹底されていることは，既に被告ら第５準備書面（３９ページ１５行目）で主張したとおりである。

ク

実験市町村において操作者識別カードの管理が適切であったこと及び一般的に当該対策が徹底されていること

吉田証人は，阿智村，下諏訪町の実験の際に確認できたこととして，操作者識別カードの管理も特に厳しくなかった，担当の職員から口頭で確認できた旨証言している（尋問調書７１ページ１２ないし２３行目。なお，聴取報告書１の８ページ２行目にも同様の記載がある。）。

しかし，この点についても，客観的な事実として，実験当時も現在も，阿智村及び下諏訪町とも，そのような事実はなく，操作者識別カードは，担当者が専用でそれぞれ１枚を使用し，使用しない場合には施錠して保管しており，カード管理簿により適切に管理されている（乙第３１号証の２及び第３２号証の２，別添資料中の質問・調査項目７－１）。そもそも，阿智村及び下諏訪町とも，吉田証人に口頭で確認を受けた記憶はないとしている（乙第３１号証の２及び第３２号証の２，別添資料中の質問・調査項目７－２）。

吉田証人の証言は誤りというべきである。

なお，全国の市町村において，チェックリスト（操作者識別カードについては，管理目標１６）により，対策が徹底されていることは，既に被告ら第５準備書面（３９ページ１５行目）で主張したとおりである。

(2)　小括

ア　上記の結果によれば，庁舎外から庁内ＬＡＮへ侵入できる具体的危険性は実験で何ら実証されておらず，むしろ安全性が確認されたといえ，原告らの庁内ＬＡＮへいろいろな方法により不正侵入し得るとする主張が失当であることは，明らかである。

イ　また，実験市町村において，ＣＳ端末の配置や操作者識別カードの管理は適切になされていたものである。原告らのこれらについて脆弱性が存在するとの主張が失当であることは明らかである。また，これらの対策は，一般論としても全国の市町村において徹底されている。

第３　原告ら準備書面１４における長野県侵入実験に関する主張に対する反論

原告らは，原告ら準備書面１４の４ページ(イ)において，長野県侵入実験の結果，住基ネットの脆弱性が立証され，これらの脆弱性を突いて原告らの個人情報が不正に閲覧されるなどの具体的現実的危険性が存することが明らかになったとし，具体的に以下の点を指摘する。

しかし，原告らの指摘する点は実験において実証されておらず，むしろ安全性が確認されたものであるから，原告らの主張は全く失当である。

１(1)　原告らの主張

原告らは，

ａ　既存住基サーバが接続された庁内ＬＡＮの脆弱性を突いて，当該庁内ＬＡＮに侵入した上で，

ｂ　既存住基サーバの管理者権限を奪取するなどして，同サーバ内に存する住民票コードを付された住民基本台帳上の全データを不正に閲覧，改ざん

できる

などと主張する。

(2)　被告らの反論

そもそも，ここに述べる原告らの主張は，何ら「住基ネットの脆弱性」と関係ないものである。すなわち，既存住基システムは，住基ネットの導入以前から存するものであり，また，住基ネットと直接の関係を持たないから，住基ネットとは峻別してとらえるべきものである（本準備書面第２の９）。

その点をおくとしても，ａについては，長野県進入実験では，インターネットから庁内ＬＡＮへ侵入される具体的危険性は実証されておらず，むしろ安全性が確認されたというべきであることは，本準備書面第２の３で述べたとおりであるし，庁舎外から庁内ＬＡＮへ侵入される具体的危険性は実験で実証されておらず，むしろ安全性が確認されたこと，及び，実験市町村における庁内ＬＡＮの脆弱性は限定的であり，一般論として，市町村における対策が徹底されていることは，第２の１０で述べたとおりである。よって，ｂについて論ずるまでもなく，実験において上記の具体的現実的危険性は実証されず，むしろ安全性が確認されたことは明らかである。

なお，念のため付言すると，ｂについては，第２の７(1)エで述べたとおり，下諏訪町及び阿智村の１次実験では，既存住基サーバのＯＳの権限の取得に成功はしているが，これは役場の許可を得て庁舎内に立ち入り得た結果であり，通常の状態で成功したものではない。

一般論としても，不正侵入，不正アクセス防止法違反を伴い，サーバの特定，重要機能室などの物理的セキュリティ対策の回避，職員の目を欺くことなどが必要であるから，到底容易とはいえないものである。

２(1)　原告らの主張

原告らは，

ａ　どこか一箇所の市区町村のＣＳセグメントに攻撃端末を接続し，

b　攻撃端末からの攻撃によりＣＳ端末の管理者権限を奪取した上で，

c　管理者権限を奪取したＣＳ端末を遠隔操作して，正規の操作者になりすまし，他の市区町村に存する原告らの本人確認情報を不正に閲覧したり，原告らの住民票の写しの広域交付を行ったりできる

などと主張する。

(2)　被告らの反論

まず，ａについては，第２の５(2)で述べたとおり，阿智村の２次実験は，通常は施錠されている重要機能室に立ち入り，さらに通常は施錠されているラックを開けて，その中のハブに調査用のパソコンを接続するという特殊な環境で行われたものにすぎず，上記ａの方法が現実に行われる危険性を示したとは到底いえない。そして，一般論としても，ＣＳセグメントのハブやＣＳ端末は執務室内に存在するものであり，これを探すこと，不正侵入を行うこと，攻撃端末を差し込んで攻撃を行う間，職員の目を欺くことなどが必要となるものであり，到底容易とはいえない。よって，ｂ及びｃについて論ずるまでもなく，実験において上記の具体的現実的危険性は実証されず，むしろ安全性が確認されたことは明らかである。

念のため付言すると，ｂについては，第２の６(2)で述べたとおり，阿智村の２次実験におけるＣＳ端末のＯＳの管理者権限の取得は，特殊な実験環境下で得られたものであり，具体的危険性があったものではなく，通常の状態ではむしろ安全であることが確認された。現在，強固なＩＤ，パスワードの設定が更に徹底されてもいる。

また，ｃについては，第２の２(2)イで述べたとおり，正規の操作者が操作者用カードをカードリーダに挿入した後，攻撃端末からＣＳ端末を操作して，その操作者カードの持ち主である正規の操作者になりすまし，盗み取ったパスワードを打ち込んで，不正アクセスする方法（他の市区町村の住民の本人確認情報を不正閲覧したり，広域交付を行ったりすること）は，実験で

は行っておらず，かつ，一般論としても，到底容易とはいえない。

3 (1)　原告らの主張

原告らは，

a　既存住基サーバの管理者権限を奪取し，

b　同サーバを踏み台としてＦＷ越しにＣＳの管理者権限を奪取した上で，

c　さらにＣＳ端末の管理者権限を略奪することによって，②と同様の操作ができる

などと主張する。

(2)　被告らの反論

まず，aについては，上記１(2)で述べたとおりである。よって，b及びcについて論ずるまでもなく，実験において上記の具体的現実的危険性は実証されず，むしろ安全性が確認されたことは明らかである。

念のため付言すると，bについては，第２の４(1)エ及び７(3)で述べたとおり，庁内ＬＡＮから市町村設置ＦＷ越しにＣＳのＯＳの権限が取得される具体的危険性は実験で実証されておらず，むしろ安全性が確認されたものである。

また，cについては，上記２(2)でb及びcについてで述べたことがそのまま該当することになり，これも具体的危険性はない。

4　以上述べたとおり，原告らの指摘する具体的現実的危険性など存在しない。長野県侵入実験では，それらの存在は実証されず，むしろ安全性が確認されたものである。原告らの主張は全く失当であるというほかない。

第４　結語

以上のとおり，原告らが長野県侵入実験の結果等から明らかとなったとする住基ネットの具体的現実的危険性は，いずれも何ら実証されておらず，むしろ実験結果からは，それらが存在しないことが明白となった。

原告らの請求は，いずれも速やかに棄却されるべきである。

以　上

別紙

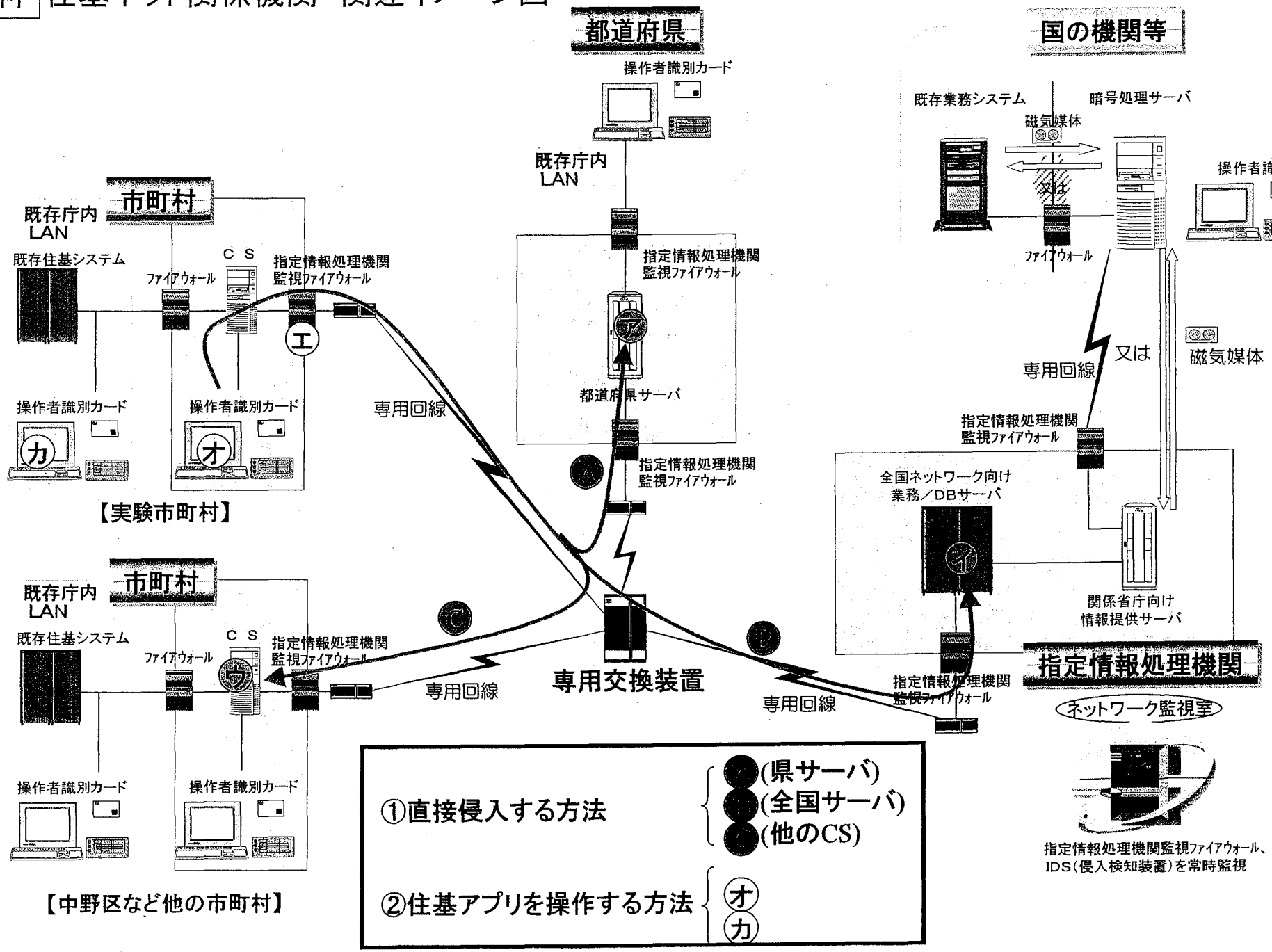
長野県侵入実験の概要

実験の場所	日時	実験内容	実験結果	本準備書面の第2における項目
波田町（東京都千代田区）	平成15年9月22日から24日	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（別紙図面2における①）。	失敗	b
下諏訪町	平成15年9月25日から26日	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，攻撃端末を村の庁内LANにつなぎ，市町村設置ファイアウォールを突破して，CSセグメント（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が設置されるエリア）への侵入を試みた（別紙図面2における②）。	失敗	c
		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（別紙図面2における③）。 ※　既存住基システムは、住基ネットに含まれない。	成功	f,h
阿智村	（第1次） 平成15年9月29日から10月1日	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，攻撃端末を村の庁内LANにつなぎ，市町村設置ファイアウォールを突破して，CSセグメント（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が設置されるエリア）への侵入を試みた（別紙図面2における②）。	失敗	c
		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（別紙図面2における③）。 ※　既存住基システムは、住基ネットに含まれない。	成功	f,h
	（第2次） 平成15年11月25日から28日	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）につなぎ，CSのOSの権限取得を試みた（別紙図面2における④）	成功	d
		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）につなぎ，CSのOSの権限取得を試みた（別紙図面2における⑤）	失敗	e
		OSの権限を取得したCSから得られたID・パスワードでCS端末のOSの権限を取得	成功	e

実験結果一覧

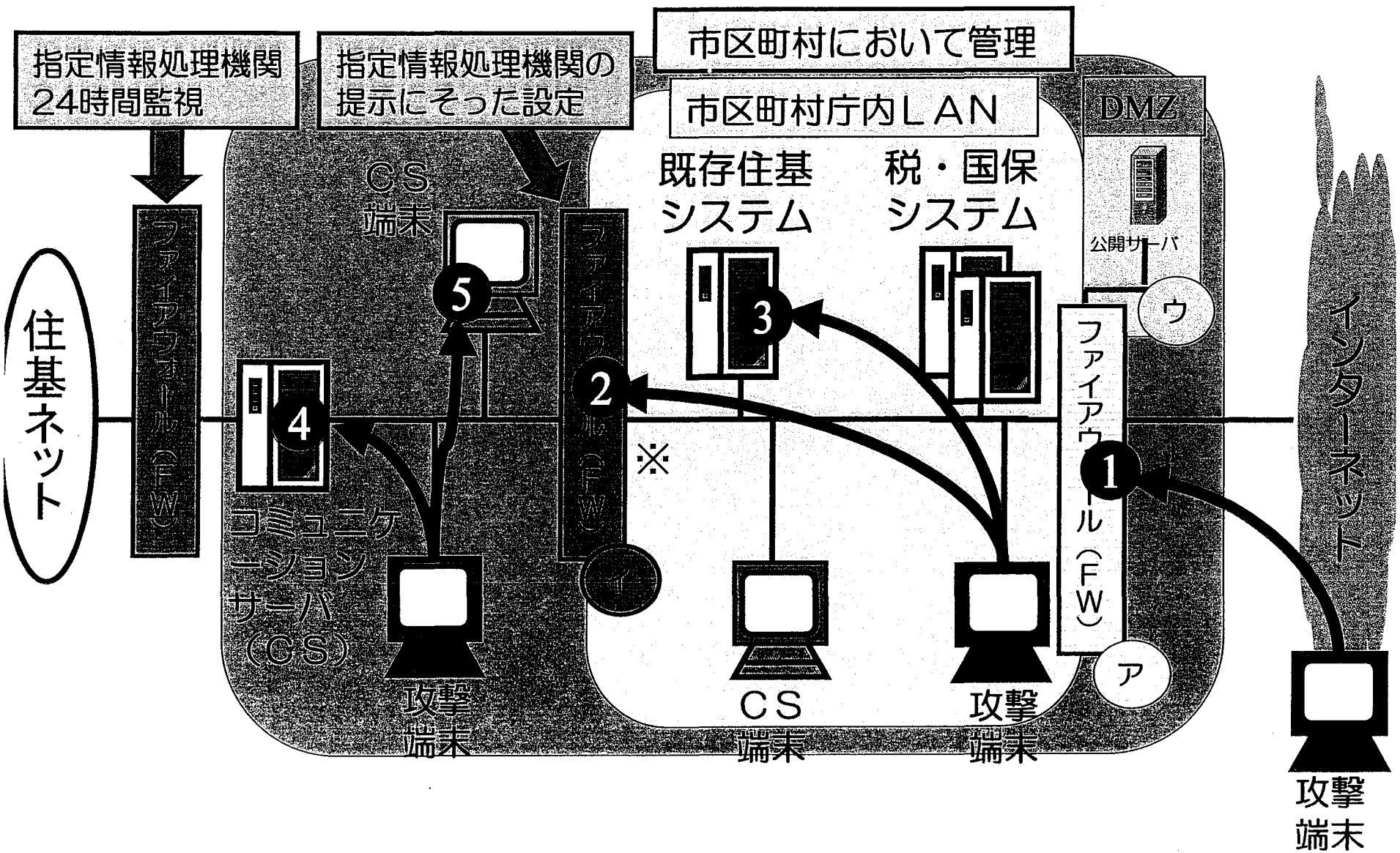
項目	事実	イメージ図	実験結果
a	①住基ネット本体への直接侵入 ②CS端末の住基ネットアプリケーションの操作	別紙図面1における①②	未実施
b	インターネットからファイアウォール越しに庁内LANへ侵入	別紙図面2における①	・波田町で実験 →失敗
c	庁内LANから市町村設置ファイアウォール越しにCSへ侵入	別紙図面2における②	・下諏訪町で実験 →失敗 〔・阿智村(1次) →FWに脆弱性無し〕
d	直接CSセグメントに攻撃端末をつなぎ込み、CSのOSの権限を取得	別紙図面2における④	・阿智村(2次)で実験 →成功
e	直接CSセグメントに攻撃端末をつなぎ込み、CS端末のOSの権限を取得	別紙図面2における⑤	・阿智村(2次)で実験 →失敗
	CSから得られたID・パスワードでCS端末のOSの権限を取得	—	・阿智村(2次)で実験 →成功
f	甲共第40号証の実験	別紙図面2における②	未実施
h	既存住基システムを改ざんしCSへ反映させる	—	未実施
i	庁舎外から庁内LANへの侵入(b以外)	—	未実施

資料 住基ネット関係機関　関連イメージ図



別紙　図面1

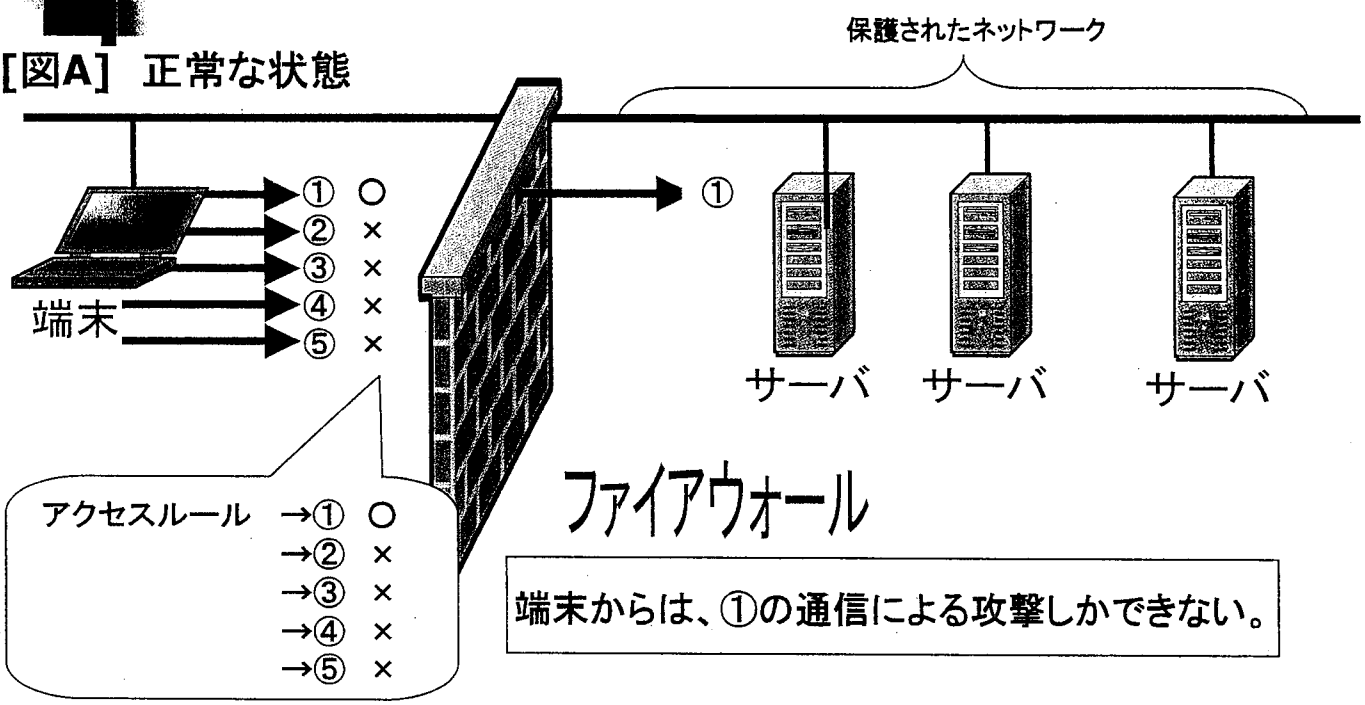
実験市町村イメージ図



別紙　図面２

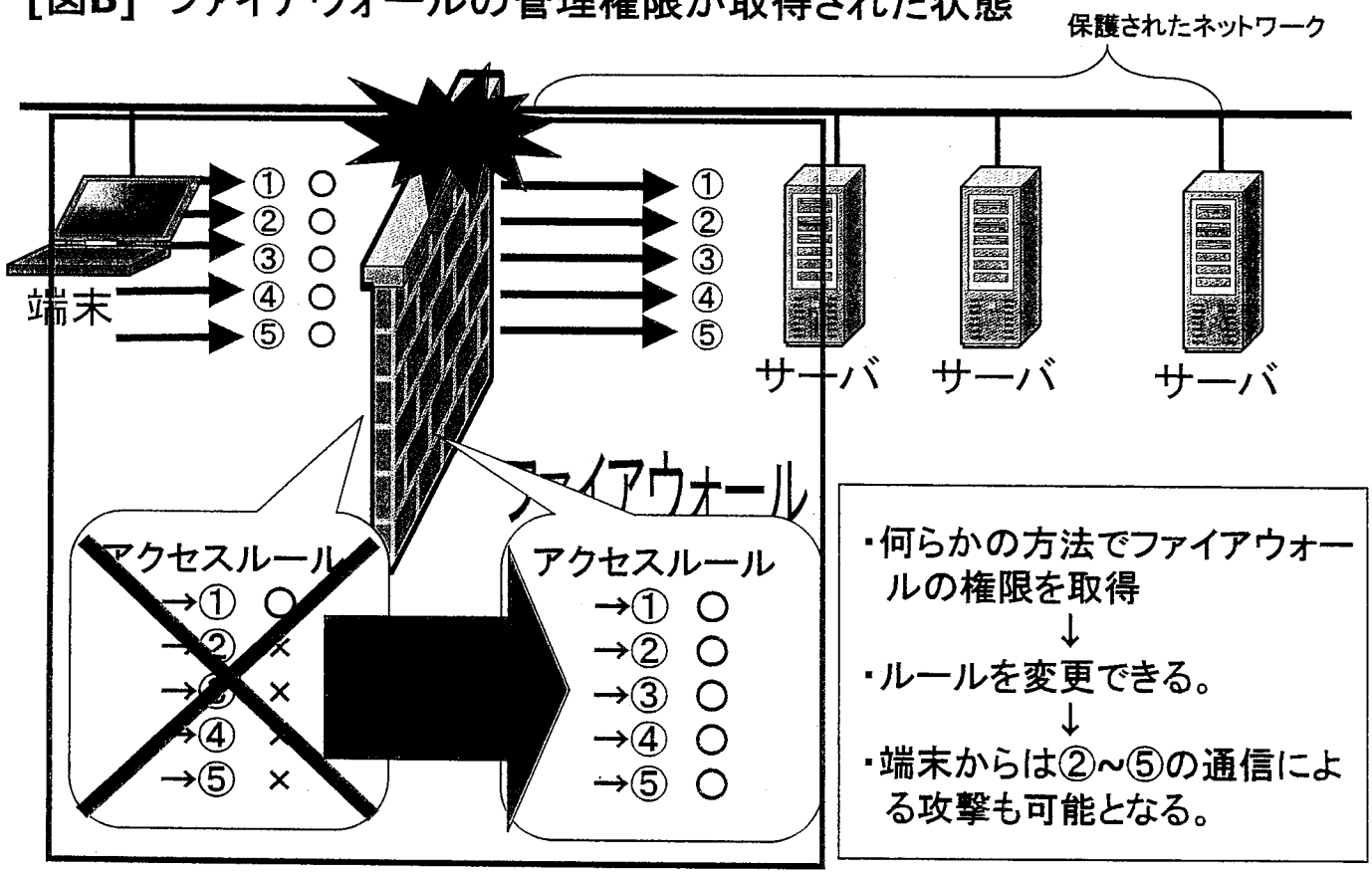
ファイアウォールの通信制御について(イメージ図)

[図A] 正常な状態



端末からは、①の通信による攻撃しかできない。

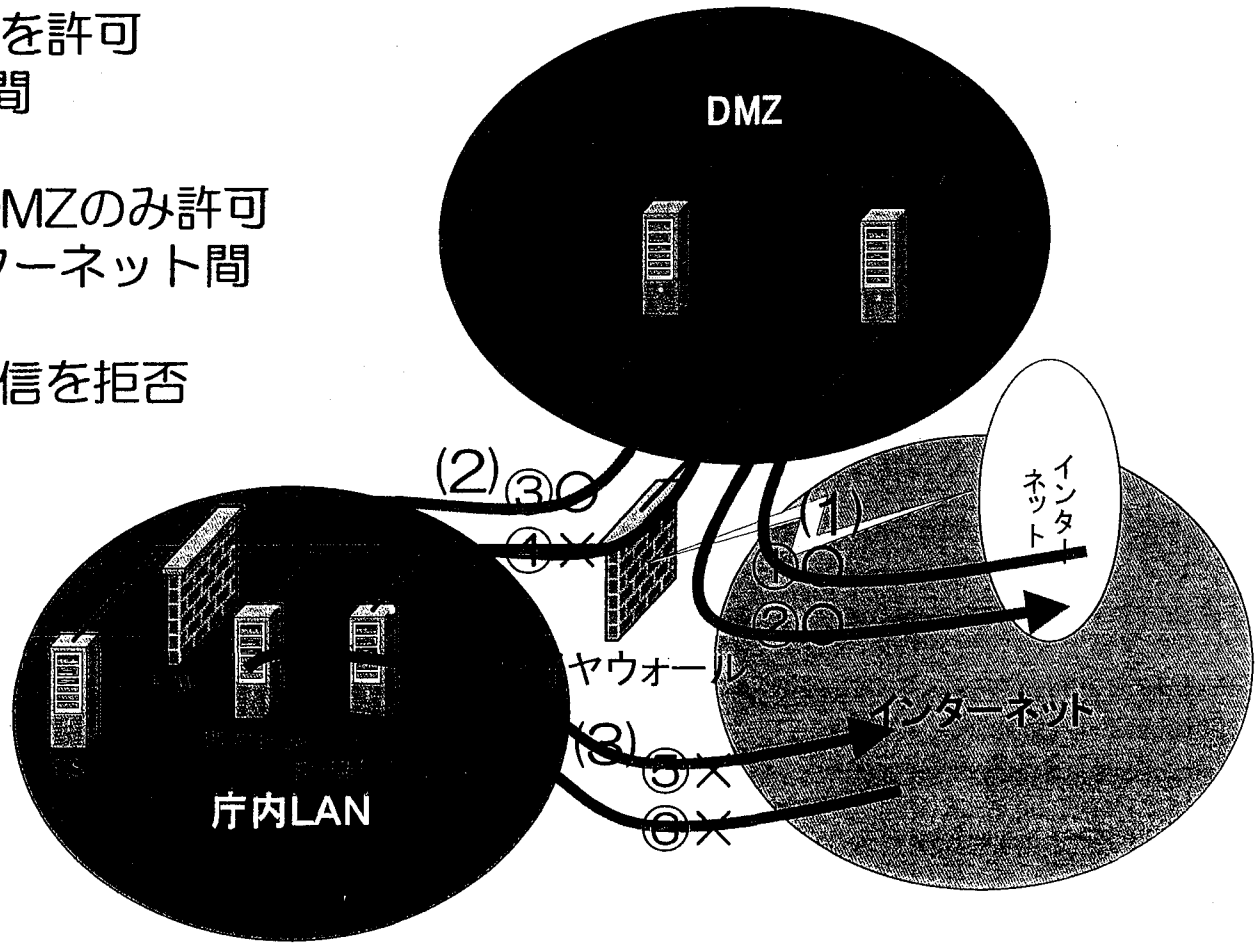
[図B] ファイアウォールの管理権限が取得された状態



・何らかの方法でファイアウォールの権限を取得
↓
・ルールを変更できる。
↓
・端末からは②~⑤の通信による攻撃も可能となる。

DMZを設定した場合の一般的な通信制限例

（1）インターネット～DMZ間
　　①　○　②　○
　　⇒双方向の通信を許可
（2）DMZ～庁内LAN間
　　③　○　④　×
　　⇒庁内LAN→DMZのみ許可
（3）庁内LAN－インターネット間
　　⑤　×　⑥　×
　　⇒双方向とも通信を拒否



別紙　図面4