２００４（平成１６）年7月２５日

東京地方裁判所　御中

原告訴訟代理人

弁護士　渡　辺　千　古

同　　水　永　誠　二

同　　長　島　　亘

「長野侵入実験」に関する聴き取り報告書　２

はじめに

以下、２００４（平成１６）年3月３０日付「『長野県侵入実験』に関する聴き取り報告書」を前提として、第１において、長野県「侵入実験」の結果、及びコンピュータネットワーク技術における一般的知見を総合することにより考えられる住基ネットシステムへの侵入の方法と原告の個人情報の危険性について報告すると共に、第２において、住基ネットの安全性（危険性）を考えるにあたっては、個人情報管理システムの安全性に関する「考え方」を前提としなければならないことから、吉田柳太郎氏、及びその他の専門家の方から聴き取った「考え方」について報告します。

第１　長野県「侵入実験」の結果等から考えられる具体的侵入方法などについて

１　はじめに

（１）長野県の「侵入実験」は、法的には「不正アクセス禁止法」に抵触しないように実験の範囲を限定せざるを得ませんでした。その上、時間的な制約及び実験場所の制約など、さまざまな制約があった中で行われたため、いわゆる「侵入実験」としてなすべきことを十分行えたわけではありません。

しかし、その限られた実験の中でも、

①ａ　ＣＳサーバ、ＣＳ端末のＯＳの管理者権限を、バッファ・オーバーフロー攻撃（※前回の報告書を参照）や管理が不十分なＩＤやパスワードを入

手することなどにより略奪できること、及び、

ｂ　管理者権限を略奪したＣＳ端末の画面を、攻撃端末（※）の画面からそのまま監視することができ、かつ攻撃端末からＣＳ端末のマウスやキーボードを遠隔で操作することができること、

※不正侵入をはかる者が使用するコンピュータのこと

②　ＣＳサーバとＦＷを介して接続され、ＣＳサーバとの間で住民基本台帳上のデータのやりとりを行っている既存住基サーバについてもＯＳの管理者権限を略奪したり、既存住基サーバ内の個人情報の改ざん等が可能であること、

③　ＣＳサーバと既存住基サーバとの間でデータをやりとりするのに使うアプリケーションに使用されている関数に、バッファ・オーバーフローを起こす重大な欠陥が存すること、

などの重大な脆弱性に関する事実を発見しました。

（２）これにより、

①　ＣＳセグメントに攻撃端末を接続する方法により、ＣＳサーバやＣＳ端末の管理者権限を略奪する攻撃が可能であること、

②　仮に、ＣＳセグメントに直接攻撃端末を接続することができなくても、既存住基につながる庁内ＬＡＮに攻撃端末を接続する方法により（もしくは、攻撃端末を、無線ＬＡＮ、ダイヤルアップ接続、インターネットからの接続により庁内ＬＡＮに接続する方法により）、既存住基サーバを攻撃して、同サーバの管理者権限を略奪し、

その上で、その既存住基サーバを踏み台にして、ＦＷ越しにＣＳサーバを攻撃して、ＣＳサーバの管理者権限を略奪し、

更に、そのＣＳサーバを踏み台にして、ＣＳ端末の管理者権限を略奪する攻撃が可能であること、

が明らかとなりました。また、

③　②と同様の手口で既存住基サーバを攻撃して、同サーバ内の住民基本台帳情報を改ざんし、その情報をＣＳサーバ（更に都道府県サーバや地方自治情報センターのセンターサーバ）に送信するという手法により、それら

のサーバに保存されている本人確認情報を改ざんするという攻撃が可能であること、も明らかとなったのです。

（3）以上の明らかとなった事実からすれば、中野区に住民票をおく原告の個人情報（プライバシー）には、以下のような具体的危険性が発生していることも明らかとなったというべきです。

①a　中野区以外の市町村にあるＣＳ端末の管理者権限を略奪し、同端末を攻撃端末から遠隔操作することにより、センターサーバ、東京都のサーバ、中野区のＣＳサーバに「正規の操作者」を装ってアクセスして、原告の本人確認情報を不正に閲覧する危険性。

b　同じく、中野区以外の市町村にあるＣＳ端末の管理者権限を略奪し、同端末を攻撃端末から遠隔操作して、中野区のＣＳサーバに「正規の操作者」を装ってアクセスし、原告の住民票の写しの広域交付を受ける危険性。

②　原告が住民票をおく中野区の既存住基サーバに不正侵入し、

a　住民票コード付の原告の個人情報を不正に閲覧したりする危険性。及び、

b　既存住基サーバ内の原告の個人情報を改ざんし、その情報を住基ネットシステム内に送り出すことによって、同システム内の原告の本人確認情報の改ざんを行う危険性。

２　不正侵入の手法について

以下、長野県「侵入実験」の結果を基礎として、これにコンピュータネットワーク技術の一般論を含めた一般的知見から合理的に推測できることを加味して、住基ネットへの不正侵入が可能であることを説明します。

（1）ＣＳセグメントに攻撃端末を接続する方法により、ＣＳサーバやＣＳ端末の管理者権限を略奪する攻撃について

ア　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－ネットワークの接続上の「区画」のことであり、物理的に一定の部屋などを指すものではありません）にあります。ごく簡単に言うと、庁内ＬＡＮ－市町村設置ＦＷ－ＣＳ－情報センター監視ＦＷ－都道府県サーバ・センターサーバという接続となっていて、このＣＳに、ＣＳ端末やＣＳ端末用プリンターなどが接続されています。この、市町村設置ＦＷと情報センター監視ＦＷの間がＣＳセグメ

ントということです。

ＣＳは「重要機能室」内のラックに収納されていることが多いものの、ＣＳ端末は住民サービスの窓口に設置してあって、住民の請求に応じて、本人確認情報を検索したり、住民票の写しの広域交付請求を行ったりしています。ＣＳ端末は何らの遮蔽もされていません。このＣＳとＣＳ端末はケーブルでつながれています（ケーブル自体も、何ら防護されていません）。

また、ＣＳ端末の背面のネットワークケーブルの差し込み口や、ＣＳ端末用の操作者認証カード読み取り装置のＵＳＢ（接続ケーブル）の差し込み口等が、一般住民からすぐ手の届くところにあるところが多数あります（甲１２の２・12 頁など）。

a　よって、ＣＳからＣＳ端末につながっているケーブル（やＵＳＢの差し込み口、もしくは、ＣＳ端末近くにあるハブ（※））に攻撃端末をつなぐことによって、ＣＳやＣＳ端末に対して、直接攻撃をかけることができます。

※ハブ＝ケーブルの分岐・中継機器

b　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、同様にＣＳやＣＳ端末に対して、直接攻撃をかけることができます。

イ（ア）以上述べたように、ＣＳサーバが保管されている「重要機能室」にわざわざ立ち入らなくても、容易にＦＷで防御されたセグメント内に攻撃端末を「直接つなぐこと」はできます。国側は、このような攻撃が、「通常想定し難い極めて特異な条件の下」であると主張していますが、このような主張がおよそ成り立たないものであり、ネットワークセキュリティの初歩的な「常識」をも無視したものであることは明らかです。

（イ）そもそも、「重要機能室」に鍵がかかるといっても、その鍵や出入り口自体がピッキングや物理的な破壊攻撃に対して強いものであるところが、どの位存するかは大いに疑問です。

また、長野県内の市町村では、「スチールラック剥き出しのところにＣＳサーバも既存住基サーバも置いてあって住民サービス側に剥き出しに置いてあるところもある」というような箇所もありました（甲１２の

２・12 頁等）。

更に、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します（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」６項～９項等）。

以上の点からいうならば、ＣＳ近くのハブに攻撃端末をつなぐということすら容易であると言わなければなりません。

（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言われている品川区などでは、ＣＳ端末が市町村設置ＦＷよりも庁内ＬＡＮ側に接続されています。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ります。この場合は、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のです（甲２３の１・11 頁参照）。

ウ　以上のように、攻撃端末をＣＳセグメントに接続できたならば、ＣＳやＣＳ端末を直接攻撃して、そのＯＳの管理者権限（※）を略奪することは容易であるといわなければなりません。

なぜなら、ＣＳやＣＳ端末には、セキュリティパッチ当て（プログラムの欠陥に対する修正プログラムのインストール）が遅いという弱点があるため、バッファ・オーバーフロー攻撃に弱いという欠点があるからです。

たとえば、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いましたが、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ヶ月半も後でした（甲２４の１・14 頁参照）。これは、セキュリティパッチ当てをすると、それまで「順調に」動作していたプログラムソフトが、うまく動作しなくなることがあるため、その動作を検証・確認する作業を地方自治情報センターで行い、その確認後に、センターから各自治体にパッチ当ての指示がでることから、必然的に遅くならざるを得ないのです。

また、その動作確認は、ＣＳ端末よりもＣＳの方が時間がかかることか

ら、ＣＳはＣＳ端末よりも更にパッチ当てが遅くならざるを得ません。

（２００３年８月１９日付毎日新聞夕刊においても、「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」、「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」などと報道されています。（甲９の２・№50 の記事））

このように、ＣＳやＣＳ端末のセキュリティパッチの適用は、遅いと言わざるを得ませんし、このパッチ当ての遅れは、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します。そして、バッファ・オーバーフロー攻撃が成功すれば、１００パーセント確実に管理者権限が奪取されるということになるのです。

※「管理者権限」とは、コンピュータのシステムの保守管理をする権限のこと。

「管理者」は、①基本ソフト（ＯＳ）の変更・更新操作や、②新たなプログラムのインストールや削除、③そのコンピュータに記録されている全ての情報を閲覧、書き換え、削除をすることができるほか、④そのコンピュータの利用者（のＩＤ、パスワード）の登録・削除、⑤その利用者の「利用者権限」の設定・変更など、強大な権限を有しています。

この管理者権限を略奪する方法としては、ａ：「管理者」のＩＤ、パスワードそのものを入手する方法や、ｂ：プログラムやＯＳのセキュリティホールをついて、バッファ・オーバーフローを起こさせることによって行う方法などがあります。

（２）庁内ＬＡＮ上の既存住基サーバの管理者権限を略奪し、そのサーバを踏み台にして市町村設置ＦＷ越しにＣＳ・ＣＳ端末の管理者権限を略奪する攻撃について

次に、ＣＳセグメントに直接攻撃端末を接続できなくても、ＣＳやＣＳ端末の管理者権限を略奪できることについて説明します。

ア　市町村設置ＦＷ越しの攻撃が可能なことについて

（ア）ＣＳの管理者権限の略奪

既存住基サーバの管理者権限を略奪し、ここを拠点（踏み台）として、

市町村設置ＦW越しにＣＳを攻撃し、ＣＳの管理者権限を略奪することが可能です。

長野県「侵入実験」においては、限られた時間と環境等の制約の中での実験であったため、実際にＦW越しのＣＳ攻略実験は行ってはいません。しかし、実験の中で、ＣＳと既存住基サーバ間でデータのやりとりをするアプリケーションに使われている関数に、バッファ・オーバーフローを起こす重大な脆弱性があることが発見されています。

したがって、後述の「イ」で述べるいずれかの方法で庁内ＬＡＮに侵入し、庁内ＬＡＮ上に存する既存住基サーバの管理者権限を略奪できれば、この既存住基サーバを拠点（踏み台）にして、市町村設置ＦW越しにＣＳサーバを攻撃（受動的攻撃の手法（※）を含みます）して、ＣＳサーバの管理者権限を略奪することが可能であると合理的に推測できるのです。

吉田柳太郎氏は、長野県本人確認情報保護審議会で、以下のように述べています。

「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議事録 12 頁）。

※「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手法です。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ます。

※※　バッファ・オーバーフローを起こす脆弱性のある「関数」について

例えば、Microsoft.com Japan の「コンパイラセキュリティの徹底調査」というページ（日本語版最終更新日２００２年９月２６日）には、以下のような記述があります。

「はじめに

ソフトウェアセキュリティはハイテク業界にとって大きな関心事ですが、中でも最も恐ろしく、誤解されているソフトウェアの脆弱性が、バッファオーバーラン（注：バッファ・オーバーフローと同じ意味）です。近頃では、バッファオーバーランの話をすれば、人々が足を止めて耳を傾けるほどです。……

バッファオーバーランとは？

バッファとは、通常配列の形式をとるメモリブロックのことです。配列のサイズを確認しないと、確保したバッファの外部に書き込む可能性があります。書き込みがバッファよりも上位のメモリアドレスに行われる場合、これをバッファオーバーランと呼びます。……実行中のプロセスにコードを書き込むバッファオーバーランは、悪用されかねないバッファオーバーラン（exploitable buffer overrun）と呼ばれています。

ｓｔｒｃｐｙ，ｇｅｔｓ，ｓｃａｎｆ，ｓｐｒｉｎｔｆ，ｓｔｒｃａｔなど特定のクラスの関数は、バッファオーバーランに対して本質的に脆弱であり、なるべく使用しないようにマニュアルに明記されています。」

以上のように、脆弱性のある関数は、コンピュータ技術者の間では、重大なセキュリティ対策上の問題として認識されているものです。

以上のように、既存住基サーバの脆弱性を踏み台として、ＣＳサーバの管理者権限を略奪することに結びつけられるのですから、「既存住基や庁内ＬＡＮの脆弱性は、住基ネット本体の安全性とは無関係である」旨の国側の主張が誤りであることは明らかであるといわなければなりません。

（イ）ＣＳ端末の管理者権限の略奪

ＦＷ越しにＣＳサーバの管理者権限を略奪した後に、このサーバを拠点として、それとつながるＣＳ端末にバッファ・オーバーフロー攻撃をかけたり、ＩＤとパスワードを把握して管理者権限でアクセスしたりすることによって、ＣＳ端末の管理者権限を略奪することは可能となります。

（なお、ＩＤとパスワードは、設定や管理がずさんなところが多いことが指摘されています。本実験においても、その設定・管理がずさんであることが明らかとなっています。また、パスワードに関しては、「辞書攻撃」（コンピュータが辞書に載っている単語を、極めて短時間の内に、総当たりに試してパスワードを破るという攻撃手法）などが一般化していますから、この設定・管理を高度に保つことは極めて困難になっているといわなければなりません。）

イ　既存住基サーバの管理者権限を略奪する方法について

以上述べたように、既存住基サーバの管理者権限を略奪できれば、それを踏み台として市町村設置ＦＷ越しにＣＳの管理者権限を略奪する攻撃が可能となります。

そこで、次に、その前提となる既存住基サーバの管理者権限の略奪の方法について説明します。

既存住基サーバは、以下のような経路と手法を用いて庁内ＬＡＮに侵入できれば、容易に攻撃が可能となり、かつ、その管理者権限を奪うことも容易です。

（ア）庁内ＬＡＮへの不正侵入の方法

まず、市町村の庁舎の外から、庁内ＬＡＮに不正侵入するには、いろいろな方法があります。

すなわち、①庁内ＬＡＮが隣接庁舎の会議室などに直接つながっている場合は、その会議室内のＬＡＮポートに攻撃端末を接続することによって、庁内ＬＡＮに侵入することができます。長野県の実験箇所では、隣接するコミュニケーションセンター（夜１０時まで誰でも利用できる）にも、庁内ＬＡＮケーブルがつながっており、その会議室内にあるＬＡＮポート（接続口）に攻撃端末をＬＡＮケーブルで接続したところ、それだ

けで、庁内ＬＡＮに接続することができました。

また、②無線ＬＡＮを使用している庁舎においては、無線ＬＡＮ経由で庁内ＬＡＮへの侵入が可能です。長野県の実験箇所においては、無線ＬＡＮを使用していませんでしたが、全国的に見れば相当数の自治体等で無線ＬＡＮを使っていること、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す（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ます）。したがって、無線ＬＡＮ機能を持つ攻撃端末から庁内ＬＡＮへ不正侵入することは可能です。

さらに、③ダイヤルアップ接続を利用した侵入方法も可能です。

すなわち、出先機関（支所、出張所、公民館など）が庁内ＬＡＮにダイヤルアップ接続している場合、それらの箇所は、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す。

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ます（これは、丙１３・45-6 項からも見て取れます）が、この場合、ダイヤルアップ接続となります。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、パスワードが分かり、callerＩＤを偽装することができれば、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ります。④インターネット経由で庁内ＬＡＮへ侵入することも可能です。

確かに、長野県波田町における実験において、インターネットからの侵入は成功しませんでした。しかし、その理由は、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）。

全国のインターネット接続を行っている市町村において、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ませんから、他の市町村においては侵入できるところは必ずあるはずです（実際ＨＰの改ざん等は頻発しています）。

また、波田町においても、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ません。そして波田町においても、担当者は、２～３年ごとの人事異動により交代しますし、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す。

インターネットに接続している自治体は、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、全世界のどこからでもインターネット経由で不正侵入をされてしまうという危険を負担することになるのです（後述の、第２でも説明します）。そして、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す。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と体制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は明らかなのです（甲１２の２・17 頁等参照）。

なお、ｉ）そもそも、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り、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といっていいほど実施されていないことは極めて問題です。

※　ルーターやＦＷにそなえられている、不審なパケット（データ）を遮断する機能。ネットワークから送られてくるパケットのヘッダ情報からＩＰアドレスやポート番号を参照し、設定された条件に合致するものを遮断する。

また、ⅱ）公表されたセキュリティパッチを迅速に当てるだけでは、公表されていない脆弱性に対する攻撃に全く対処できません。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すから、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ありません。たとえば、eEye 社がマイクロソフト社に報告しているものの、公表されていない脆弱性については、

http:www.eeye.com/html/research/upcoming/index.html に出ています。

（イ）ソーシャルエンジニアリングの手法について

ところで、このような攻撃において、「ソーシャルエンジリアリング」という手法が頻繁に活用されることに着目する必要があります。例えば、県庁の役人や保守管理業者を詐称して、地方自治体職員に電話をして情報を手に入れるというような手法です（甲１２の２・24～25 頁参照）。詳しい事例は、甲１５・『欺術』（ケビン・ミトニック著）に紹介してありますが、その「序文」は、以下のように結んでいます。

「セキュリティを単に技術（テクノロジ）の問題として捉えると、そこに大きな落とし穴が待ち構えている。ケビンのような人物は、その落とし穴を封じる手助けをしてくれる。本書を読めば、セキュリティの人間的側面に関する、かけがえのないガイド役として、ミトニックの存在価値を誰もが認めるだろう。」

この手法を用いるならば、部外者であっても、庁内ＬＡＮに接続するＩＤやパスワードなどを入手したり、身分を詐称して庁内に入り込んで、庁内ＬＡＮに攻撃端末を接続することも、困難でないことが明らかとなります。

（ウ）バッファ・オーバーフロー攻撃

以上のような手法により庁内ＬＡＮに侵入した上で、庁内ＬＡＮ上にある既存住基サーバにバッファ・オーバーフロー攻撃をかければ、同サーバの管理者権限を略奪することは容易です（長野県の実験においても容易でした）。これは、既存住基サーバの、セキュリティパッチ当てが非常に杜撰であることが多いことによるものです。

管理者権限を略奪すれば、同サーバに、他のサーバのセキュリティホ

ールを攻撃（受動的攻撃を含む）するための悪意のプログラムをインストールすることなどが可能となりますから、ＦＷ越しにＣＳサーバを攻撃する前提が作られるわけです。

（３）管理者権限を略奪したＣＳ端末を、攻撃端末から遠隔操作して不正アクセスを行う方法について

ア　以上に述べた（１）、（２）のいずれかの方法によって、ＣＳ端末の管理者権限を略奪できれば、そのＣＳ端末を攻撃端末から遠隔操作して、

①　センターサーバ、都道府県サーバ、他の市町村のＣＳサーバに「正規の操作者」を装ってアクセスして、誰かの本人確認情報を不正に閲覧したり、

②　同じく、他の市町村のＣＳサーバに「正規の操作者」を装ってアクセスして、誰かの住民票の写しの広域交付を受けることが可能となります。

イ　この点、国側は、「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」と主張していますが、これは誤りです。

長野県「侵入実験」において、管理者権限を略奪したＣＳ端末について、その画面を攻撃端末からそのまま監視することができましたし、ＣＳ端末のマウスを攻撃端末から動かすこともできました（甲１２の２・6頁参照）。

管理者権限を略奪していますから、攻撃端末からＣＳ端末にキーボード操作を全て監視・記録するソフト（キーロガー）をインストールすることも可能です。これにより正規の操作者がキーボードで打ち込むパスワード等を盗み取ることも可能です。

したがって、仮に、「操作者用カードがＣＳ端末に付けられたカードリーダーに差し込まれていないと住基ネットアプリケーションを操作できない」という国側の主張を前提としても、少なくとも、正規の操作者が操作者用カードをカードリーダーに挿入した後（これ自体は、日常的に起こる事象です）であれば、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わけです。

（４）小括

以上より、

α）直接、ＣＳセグメントに攻撃端末を接続する手法を用いて、ＣＳ端末を直接攻撃してその管理者権限を略奪することにより、また、

β）既存住基サーバの管理者権限を略奪し、同サーバを踏み台として、市町村設置ＦＷ越しにＣＳサーバの管理者権限を略奪し、更にＣＳサーバを踏み台としてＣＳ端末の管理者権限を略奪することにより（もしくは、ＩＤ、パスワード等を取得することにより、ＣＳ端末に管理者権限でアクセスすることにより）、

このＣＳ端末を攻撃端末から遠隔操作することが可能となりますから、遠隔操作によって、センターサーバや都道府県サーバ、他の市町村のＣＳサーバに対し、「正規の操作者」を装って、不正アクセスができることは明らかです。

３　原告が住民票をおく中野区の既存住基サーバに侵入することにより、

ａ　住民票コード付の原告の個人情報を不正に閲覧、入手等する危険性、及び、

ｂ　既存住基サーバ内の原告の個人情報を改ざんし、その情報を住基ネットシステム内に送り出すことによって、同システム内の原告の情報の改ざんを行う危険性について

（１）２で指摘したように、既存住基サーバは脆弱性が高いところが多いものであって、その管理者権限の略奪が容易であることは明らかです。

したがって、中野区の既存住基サーバ内の住民基本台帳上の「本人確認情報」データが閲覧・改ざん・削除等される危険性も高いといわなければなりません。

そして、既存住基サーバ内の原告の「本人確認情報」が書き換えられた場合は、そのデータがＣＳや都のサーバ、センターサーバに送られるのですから、住基ネットにおける原告の「本人確認情報」も改ざん等がなされる結果

とならざるを得ません。

（２）これに対して、国の側は、住基ネットシステムの範囲について、ＣＳのセンターのＦＷ（地方自治情報センター監視ＦＷ）からセンター側を「住基ネット本体」と呼んで、この部分は高度に安全性が保たれている旨、そして、既存住基サーバ部分は、住基法の改正以前から存する部分であって、この部分の安全性は、住基法の改正で新たに付け加えられた「住基ネット本体」部分の安全性とは関係ない旨の反論を行っています。

（３）しかし、これは住基ネットにおけるデータの安全性という面から見るならば、全くの誤りです。

なぜなら、上述したように、国の言う「住基ネット本体」に保存されている本人確認情報は、各自治体において、既存住基サーバ内に保管されている住民基本台帳情報の一部であり、かつ、その既存住基サーバと「住基ネット本体」はネットワーク化されている、ということを無視しているからです。

ア　すなわち、改正住基法によって、

① 各自治体において、住民基本台帳上の住民データに、新たに「住民票コード」が付加されました（既存住基サーバに記録される情報が、１４情報となりました）。

② そして、既存住基サーバ内の住民基本台帳上の情報の内、住民票コード、氏名、住所、生年月日、性別、そしてこれらの異動情報の６情報が、ネットワーク化された各市町村に設置され、管理されているＣＳサーバに送られ、保存されるようになりました。

③ このＣＳサーバ内の６情報が、「住基ネット本体」である都道府県サーバや地方自治情報センターのサーバに送られ、保存される事になったのです。

このことから明らかなように、既存住基サーバ内のデータが「住基ネット本体」内のデータの元なのです。

イ　したがって、仮に「住基ネット本体」のセキュリティを既存住基システムよりも高度に保つことができたとしても、既存住基システムにセキュリティ上の脆弱性があれば、「住基ネット本体」内で保存・流通する「本人

確認情報」の安全性（特に、改ざん等に対する安全性）は全く保たれないことになります。

つまり、既存住基サーバに不正侵入を受けて、既存住基サーバ内の個人情報が書き換えられた場合は、その書き換えられた情報がＣＳサーバやセンターサーバに送られるのですから、「住基ネット本体」に侵入しなくても個人情報の改ざんは可能となるのです（しかも、書き換え前のデータも、書き換え後のデータも、デジタル化されたデータですから、紙媒体である帳簿の場合と違って書き換えの痕跡が残らず、書き換え後のデータが「真実のデータ」として扱われる危険性が高くなります。）。

（４）また、既存住基サーバ内に存する原告の個人情報を閲覧すれば、改正住基法で付加された住民票コードを知ることができます。一旦住民票コードを知ることができれば、その後、原告が全国どこへ住民票を移転させようとも、住民票コードを検索キーとしてセンターサーバで検索できます。そうすれば、今、原告が、どこでどのような本人確認情報を有しているかを閲覧でき、更に、住民票をおいている市区町村に対して住民票の写しの広域交付を求めれれば、その者の家族関係を含めて、その個人情報を知ることができるのです。

（５）以上述べたように、住基ネットシステムは、「住基ネット本体」の中だけでデータを作成・保管・移動させるシステムではなく、全国の市区町村から、住民基本台帳上の個人情報の一部（本人確認６情報）を強制的に国（地方自治情報センター）側に吸い上げるシステムとなっているため、「住基ネット本体」の中だけを高度に防衛しようとしても、「本人確認情報」の安全性を守ることができないシステムになっているといわざるを得ないのです。

第２　住基ネットの「安全性」に関する考え方について

はじめに

国は、「長野県の実験では、ＦＷを突破できなかった」とか、「住基ネットシステムは、ファイアウォール（ＦＷ）や侵入検知装置（ＩＤＳ）などを備えており、（技術的に）十分な安全対策をとっている」旨繰り返し述べています。

しかし、「高価なＦＷやＩＤＳなどのＩＴ機器を導入したから安全」、つまり、技術で安全を守ることができるという考え方は、以下に説明するように全く誤っています。

この点を中心に、「住基ネット」という、コンピューターネットワークにおいて処理されている個人情報の安全性の問題点について、以下、若干の説明を加えます。

１　「住基ネットの安全性問題」を考える際に、「私は、コンピュータの専門家でないから、分からない問題」と頭から考えてしまう人がいますが、その様に考えると、問題が見えなくなります。「『ＩＴ』や『コンピュータ』は難しい」と考えるから、分からなくなるのです。次のように順を追って考えれば、全く専門知識がない人でも、「住基ネット」というコンピュータネットワークの安全性に関する考え方は理解できるはずです。

２　人は、誰でも紙に書いた個人情報（例えば住所録）を保有しており、それの安全な利用法、管理法ならイメージすることができます。コンピュータ（ネットワーク）を利用した個人情報の安全な利用や管理ということも、考え方としてはこれと全く同じです。

つまり、個人情報管理の手段が、

α）従来、管理者が、個人情報の管理手段として、紙媒体の帳簿を使っていた、

というものであったのが、

β）現在、管理者が、個人情報の管理手段として、コンピュータ（ネットワーク）を使うようになった、と変わっただけと考えればいいのです。

「手段」が新しくなったことによって、紙媒体の時代と異なる新たなリス

クが発生していますが、このリスクを理解して、それに見合った対策をとりうる能力と財力があるならば、新しい「手段」を利用して、個人情報を管理するという考え方もありえます。裏を返せば、このリスクの理解力と対策能力がない場合は、安全性の確保ができず、「危険」ということになるのです。

なお、便利さ（効率）と危険性とは相反する関係になります。つまり、情報の管理者が個人情報の処理に便利さを求めて、そのための「手段」を導入した場合、それを盗み出して悪用する者にとっても便利に使えるという危険性が高くなるという関係になるのです。

3　例えば、A町を例にとって考えてみます。

A町の町長は、A町の住民の個人情報を管理します。

（1）紙媒体の帳簿で管理していた時代

ア　A町では、コンピュータが導入される以前は、紙媒体に個人情報を書き込み、それを帳簿にして管理していました。

イ　その安全性、セキュリティを守るためには、どうしていたかというと、帳簿に対する攻撃を想定して、それに対する防衛対策をとっていたはずです。

帳簿に対して、想定できる攻撃は、（部内者、部外者による）帳簿の盗み出しが主です。そして、それに対する対策は、管理者が、帳簿をしっかり見張る（勤務時間中に使用する場合は、執務室から持ち出させない、コピーさせない。勤務時間以外は、金庫に入れておく、など）ということです。

ウ　このような帳簿による個人情報管理の時代であれば、管理者である町長は、そのような攻撃方法や、それに対する防御方法も理解可能であり、かつ、そのような対処能力も十分ありました。

（2）コンピュータ化（電算化）時代

ア　その後、個人情報をコンピュータで管理する時代になりました。

イ　そのセキュリティはどのように守るかというと、やはり同じように、コンピュータ（やフロッピーディスクなどの記録媒体）に対して、どのような攻撃が想定できるかを検討して、その対策をとるということにな

ります（いわゆる「システムにおけるリスクの洗い出し」）。

この場合、コンピュータを「手段」として利用することに伴って、新たに発生する攻撃手法を想定しなければなりません。コンピュータの特性を理解できないと、新たなリスクが想定できなくなるのです。

たとえば、①紙媒体の時代であれば、帳簿を盗み出せば、帳簿自体がなくなるわけですから、盗み出しの事実は一見して明らかになりました。しかし、コンピュータにおいては、記録媒体に情報をコピーして盗み出すわけですから、元のコンピュータ内の情報には何ら変化はありません。管理者が、勤務時間終了時や勤務時間開始に、コンピュータ内の情報に異常がないことを確認しただけでは、「盗みだし」の事実は発見できなくなったのです。

② また、紙媒体の時代には、帳簿をコピーして持ち出そうとするにしても、帳簿自体をコピー機のところにもっていって、長い時間かけて一枚一枚コピーする必要がありました。ところが、コンピュータにおいては、コンピュータのボタンを一つ押せば、大量の個人情報が記録媒体に一瞬にしてコピーされてしまいます。管理者が、コンピュータの操作者を監視していたとしても、一瞬にして行われるこのような「盗みだし」を見破り、防止することは困難となりました。

③ 以上のような新たな攻撃に対処するためには、このようなコンピュータの特性に応じた新たな「盗みだし」の形態を想定して、例えば、コンピュータに記録媒体装置をつけないし、つけられないようにして、情報のコピーや持ち出し自体を不可能にするとか、操作者に個別のＩＤ番号を与えた上で、アクセスログ（コンピュータへの接続記録）をとって、事後的に、誰が、いつ、どのような情報にアクセスしたかを把握できるようにして、事後的に不正アクセスが発覚したら、その者を摘発して処罰できるシステムを実装する（＝組み込む）などといった対策をとらなければならなくなるわけです（但し、ＩＤ番号を与えても、その管理が杜撰であれば、事後的な不正アクセス者の把握は困難となるので、この厳格な運用が必要です－四日市市の住民情報の覗き見事件を参照・

甲９の２・№30）。

（３）コンピュータネットワーク時代

ア　さらに、現在では、このコンピュータがネットワーク化される時代になっています。

イ　この時代のセキュリティは、ネットワーク化により発生した新たな攻撃方法（リスク）が想定できなければならないということになります。

①　たとえば、ネットワーク化されていない単体のコンピュータで、個人情報を管理していた時は、そのコンピュータを物理的に守ることで、相当程度のセキュリティは守られていました。つまり、そのコンピュータの中の個人情報は、そのコンピュータからしか取り出せないのですから、「盗みだし」を行うものは、直接、物理的に当該コンピュータに触れなければならなかったのです。

したがって、その防衛手段としては、管理者が、勤務時間中は当該コンピュータを見張り、夜間は厳重に鍵のかかる部屋に設置しておくことなどが考えられます。これによって、少なくとも、部外者に対しては、かなりの程度のセキュリティは守られていたと言えました。

②　ところが、ネットワーク化されたことにより、たとえ、直接そのコンピュータに触れなくても、ネットワークにつながっている全てのコンピュータから（例えば、全国３０００以上の市町村のコンピュータがネットワーク化されているとすれば、全国津々浦々のコンピュータから）、当該コンピュータにネットワークを通じてアクセスすることが可能となりました。ネットワークのラインがつながっている限り、当該コンピュータを鍵のかかる部屋に入れておいても、不正アクセスを防止するという観点からは意味がなくなってしまったのです。Ａ町のコンピュータに対する不正アクセスを防ぐためには、ネットワーク化されている全てのコンピュータを鍵のかかる部屋に入れておかなければならないことになります。

つまり、全国市町村のコンピュータがネットワーク化された場合、全国の全てのコンピュータのセキュリティが、例えば「鍵のかかる部屋に

入れてある」という状態に保たれていなければ、A町のコンピュータ内の個人情報の安全性は保たれないということになったのです。

これが、「セキュリティもプライバシーもシステムの最も弱い部分が全体のレベルになる」といわれているものの１つの例です。

ウ　ところで、全国的にネットワーク化されることに伴って、発生する困難な問題が幾つかあります。

その１つが、A町の町長の管理権限は、A町にしか及ばないということです。他のＢ町やC町の町長がいい加減で、「鍵のかかる部屋」でネットワークコンピュータを管理していないような場合でも、A町の町長は、彼らに対して、「鍵のかかる部屋で管理しろ」と命令するわけにはいきません。

この場合に、A町として、Ｂ町のコンピュータからの不正アクセス攻撃を想定し、それによる情報漏洩を防止するためには、A町のコンピュータのネットワーク接続を切断するのがもっとも簡便かつ確実です。（各自治体の個人情報保護条例が、「外部ネットワークとの接続禁止」条項を入れていたのは、このような危険性を考慮したからでもあります）

「Ｂ町からのアクセスだけを遮断する」ということも考えられますが、実際的ではありません。

なぜなら、①A町においては、Ｂ町など他の町の実情を把握することは困難であるからです。仮に、Ｂ町からのアクセスを遮断したとしても、その他のC町やD町のセキュリティが守られているかも分からないからです。これが、一元管理されていないネットワークのセキュリティ上の問題です。

②　また、個別に、しっかりと管理していると認められるC町やD町にだけＩＤ番号とパスワードで認証した上、A町のコンピュータにアクセスすることを許可するという方法も考えられます。しかし、例えば、他の町のコンピュータからでも、C町のＩＤ番号とパスワードを利用されて、C町のコンピュータに成りすまされてアクセスされたら、A町のコンピュータとしてはそれを「成りすまし」の不正アクセスであると見破ることはできません。

A町の町長としては、他の町には権限を及ぼすことができないため、「他の町ではセキュリティは守られていない」という前提の下で、ネットワークに接続するしかないのです。（もちろん、A町自体のセキュリティ水準を高めなければ、反対に、他の自治体に対して不正アクセスの被害を発生させることにもなります）

A町の町長が、A町の住民の個人情報を守るためには、このような危険性を想定できる能力と、危険に対応する力（技術力、及び、それを保有する要員や教育訓練の費用、対応するための機器の導入・維持管理の費用負担に耐えうる財政力）が必要となるわけです。

エ　更に、住基ネットの場合、第２の問題として、A町の住民のデータが、A町のコンピュータ（サーバ）だけでなく、県や地方自治情報センターのサーバ、さらには、そこから提供された先のサーバに保存されているという問題があります。

県のサーバは各県の管理責任ですし、地方自治情報センターのサーバは同センターの、提供先のサーバは提供先の機関の管理責任ですから、A町の町長は、これらに対しても権限を及ぼすことができません。A町の町長は、それらの安全性について責任を持つことができないという問題が発生します。

国の側は、「住基ネット本体は、地方自治情報センターが一元的かつ高度に安全性を管理しているから大丈夫である」旨主張していますが、その範囲は、センターサーバと各県のサーバ手前のＦＷまで、センターサーバと各市町村のＣＳサーバ手前のＦＷまででしかありません。その上、管理が杜撰な市町村などの端末から、「正規」の操作者を装って（すなわち、正規の操作者カードとパスワードを用いて）アクセスされれば、個人情報の漏洩は防ぎようがありません。

４　以上述べたことからすれば、A町の住民の個人情報をあずかり、その安全性を確保する義務を負うA町（町長）としては、安全性が担保されていないＢ町やＣ町から不正アクセスがあってもA町住民の個人情報の安全性は確保できる、と自信をもってからネットワークに接続すべきことになります。また、県や地

方自治情報センターのサーバの安全性（さらには、その提供先のサーバの安全性）が確保されている、そして、今後も確保され続ける体制にある、ことを確認した上で、A町の住民の個人情報を送信（情報管理等の委託）するべきということになります。

また、自らの個人情報の主体である各住民とすれば、それらの安全を確認できない限り、自らの個人情報の提供や送信を拒めることにならなければ、自らの情報を守ることができないということになります。

このように、ネットワーク化されたコンピュータで個人情報を扱う場合は、ネットワークにつながる全国の全てのコンピュータ（サーバ）の安全性が、技術面においても、運用面においても、確保されてから接続するというのが筋道となるのです。

決して、「法律ができて、実行すべき時期が来たから、実は万全の準備ができていないにもかかわらず、安全だということにして、スタートする」などということは、町の住民の個人情報の安全管理の責任者である町長としては、責任の放棄であるといわなければなりません。

5　以上の基本的な考え方の上に立って、長野県「侵入実験」結果を見てみます。すると、単に「技術的に安全だった」とか「危険だった」という話しではなく、既存の住基システムを含めて、そこにおいて扱われている個人情報（プライバシー情報）が安全なシステムの中で管理されているかどうかが問題であるということが分かると思います。

ですから、長野県「侵入実験」の結果も、単に「技術」の面から数々の脆弱性が実証されたか否か、ということだけではなく、そこで指摘されている諸々の「事実」を「どう読み取るか」がポイントとなるはずです。

つまり、長野県の実験において、町や村においては、既存住基システムですら十分に管理できていない状況が明らかにされました（類似の指摘は、東京都国立市の検証結果でもされています）。このような「リスク管理能力」しかない全国の自治体が、一斉に、全国ネットでつながれてしまった、という事態をどのように評価するかが問題とされるべきなのです。

このような状態であるにもかかわらず、「ＦＷが突破されなかったから安全

だ」などと、「技術」によって安全が守られているかのように主張すること自体が、正に安全性を無視した、「危険」な考え方に基づいて住基ネットシステムが構築されていることを如実に示していると言わなければなりません。

6　「技術」だけで「安全性」に関して解決がつくことは決してありません。

そうであれば、世界でも屈指の「技術者」であるブルース・シュナイアーが、その著書である『暗号の秘密と嘘』の「序文」において、以下のような執筆動機（自らの失敗の反省）を明らかにするはずがありません。

彼は、次のように述べています。

「この本を書いたのは、一部は自分のまちがいを正すためだ。

七年前、わたしは別の本を書いた。『Applied　Cryptography』という本だ。その本でわたしは数学的ユートピアを描いた。深い深い秘密でさえも、幾千年にわたり安全にしておけるアルゴリズム。規制なしのギャンブル、探知不可能な認証、匿名電子マネーなど、想像を絶するような電子的なやりとりを可能にするプロトコル。それも安全で高セキュリティに。わたしのビジョンでは、暗号こそは人々を平等にする偉大なテクノロジーだった。

安い（そして毎年もっと安くなる）コンピュータさえ持てば、だれでも巨大政府と同じ水準のセキュリティが持てる。二年後に書いた同書の第二版では、わたしはこんなことさえ書いたほどだ：「法律で自衛するだけでは不十分だ。いまや、数学で自衛しなければならない」

別に暗号が一九九四年以来弱くなったというわけじゃないし、あの本でわたしが書いたことが事実でなくなったというわけでもない。ただ問題は、世の中は暗号だけでできてるわけじゃない、ということなのだ。

暗号は数学の一分野だ。そしてすべての数学と同じく、数字や等式や論理がかかわってくる。ところがセキュリティ、それもわたしやあなたが生活の上で使えるような、現実のセキュリティは人間が絡んでくる。その人の知識、他の人との関係、人と機械とのつきあいかたも絡んでくる。デジタルセキュリティには、コンピュータも絡んでくる。しかもそれが、複雑で不安定でバグだらけのコンピュータだ。

数学は完全だ。現実は主観的だ。数学は定義されている。コンピュータは強情で言うことをきかない。数学は論理的だ。人はいい加減で、気まぐれで、ほとんどわけがわからない。

『Applied　Cryptography』のまちがいは、わたしが暗号を取り巻く環境のことにまるで触れなかったことだ。暗号について、これぞ究極の答え、とでもいわんばかりに語った。

わたしもずいぶんナイーブだったわけだな。

その結果は、あまりうれしくないものだった。読者たちは、暗号というのが何か魔法の砂で、それをソフトウェアにふりかけるとセキュリティが高まる、と信じるようになった。一二八ビット鍵とか、公開鍵インフラストラクチャとかいった呪文を唱えればいいんだと思うようになった。同業者があるときこう話してくれた：世の中、『Applied Cryptography』を読んだ人たちの設計したひどいセキュリティシステムだらけだぜ、と。

あの本を書いて以来、わたしは暗号コンサルタントとして生計を立ててきた。セキュリティシステムの設計と分析をしてきたわけだ。そして最初のうちびっくりしたのが、システムの弱点は数学とはぜんぜん関係ないところにある、ということだった。弱点はハードウェアだったり、ソフトウェアだったり、ネットワークだったり、人だったり。見事な数学の成果が、ひどいプログラミングやできの悪いオペレーティングシステム、またはだれかの安易きわまるパスワードのおかげで、ぜんぜん役に立たなくなっていた。わたしも暗号の先を見ることを覚えた。システム全体を見て、その弱点を探さなきゃいけない。やがてわたしは、この本のいたるところでお目にかかる意見を繰り返すようになってきた。「セキュリティは鎖のようなもの。全体の強さは、いちばん弱いリンクの強さで決まってくる」「セキュリティはプロセスであって、製品じゃない」

実世界のシステムはすべて、複雑につながりあっている。セキュリティはシステム全体に浸透しなきゃいけない。そのコンポーネントにも接続部分にも。そして本書でわたしは、現代のシステムはあまりにコンポーネントや接続が多すぎるーーその一部は、システムの設計者や実装者やユーザさえ知らないものーーために、セキュリティの低い部分は絶対に残ると論じている。完全なシステムはありえない。どんなテクノロジーも、究極の答え」なんかではありえない。

これは、実世界のセキュリティにかかわっている人ならだれでもわかりきったことだ。実世界では、セキュリティはプロセスにかかわってくる。防止技術だけでなく、検出と対応のプロセス、さらには悪者を追いつめて処罰する、法医学的な一大システム。セキュリティは製品じゃない。それ自体がプロセスなのだ。だから、デジタルシステムのセキュリティを高めたいんなら、プロセス構築をはじめるしかない。

数年前、わたしは誰かの引用を耳にした。ここではそれを修正して披露する：セキュリティ問題を技術で解決できると思っている人は、問題も分かっていないし、技術もわかっていない。

本書はそういうセキュリティ問題と技術の限界、そしてその解決法についての本だ。」

以上の序文からも、「技術」とそれを使う人のトータルなシステムないしプロセスとしてセキュリティを考えなければならないということは明らかと

言わなければなりません。

7　以上を前提に住基ネットシステムの安全性について考えます。

１から６で述べたように、住基ネットシステムには、ネットワーク化された全国の市町村の全ての箇所において、均質に高度のセキュリティが確保されていないというシステム上の構造的な「欠陥」が存するといえます（点検基準が甘い「自己点検」の結果においてすら、全１３９項目中、重点７項目しか「３点満点」をとっていません）。

このことから、同システム内に保管されている個人情報には、以下のような危険性が発生しているといえます。

（１）内部者によるＣＳ端末の不正操作

「情報漏洩は、その７割（一説には９割）が内部者によるものである」と言われています（甲９の１・新聞記事資料集・№.７の記事等参照）。したがって、内部者による不正対策がなされているかが、第１に問題となります。

ア　市町村のＣＳ端末を操作する職員、保守管理をする業者等に対する管理が十分でない場合、これらの者が、不正にＣＳ端末を操作して、センターサーバ、都道府県サーバ、他の市町村のＣＳサーバ内の本人確認情報を閲覧したり、他の市町村から住民票の写しの広域交付を行う危険性があります。

ＣＳ端末の技術的な安全対策としては、ＣＳ端末を起動するときのパスワード、住基ネットシステムのアプリケーションを使用する場合の「操作者用カード」とパスワードによる権限確認があります。

しかし、そもそもＣＳ端末を操作する職員や保守管理をする業者は、操作用のパスワードや操作者用カードを持っています。よって、これらの者が権限を濫用して不正利用を行う場合、これを防止することは技術的には極めて困難です。運用面で防止をはかるしかありませんが、これも実際上、困難です。しかも、アクセスログはセンターサーバへのアクセス分しか記録されていないと考えられますし、このアクセスログを調べても、正規の操作者がアクセスしているのですから、その「不正」を見破るのは困難であるといわなければなりません。

ところで、最近、大阪府堺市において、保守管理業者（富士通）との間で、孫請け禁止を求める堺市に対して業者がこれを受け入れずに、保守管理に関する契約が結ばれないまま、堺市が保守管理要員に保守管理業務を行わせていた事実が明らかとなりました。このように、地方自治体が、厳格に機密保持等に関する契約を結ぶなどして監督権限を及ぼすことなく住基ネットシステムの保守管理を行わせたり、元請け業者とは契約を結んでも、その下請けや孫請け業者の社員が事実上住基ネットシステムの保守管理等を行っているなどの事例は、全国では相当数あると考えられます。

イ　操作者用カード及びパスワードの管理がずさんな場合、例えば、操作者用カードをカードリーダーに挿しっぱなしにしておく、パスワードがメモして貼り付けてあるなどという運用がなされている場合、ＣＳ端末の操作者でなくても、“自由に”ＣＳ端末を使用することができることになります（甲３の４・長野県における市町村のネットワークに関する現地調査結果、甲５・「ｅ－ｇｏｖフォーカス」で紹介されたセキュリティ監査実例等を参照）。

ウ　A町の町長は、A町の職員に対して、以上のような不正操作をさせないように、セキュリティポリシー（組織内のセキュリティに関する基本的な方針や行動指針）を整備し、操作者用カードやパスワードの管理等を厳格に運用するような体制をとる必要があります。

しかし、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、わずか７４．４％しか存在しません。しかも、このポリシーが現場で実効的に運用されるためには、現場での日常的な訓練が必要となりますが（甲１５・『欺術』で書かれている事例を参照してください）、日常業務に追われている現場の職員にそのような日常的な訓練を課すことは事実上不可能です（甲３の長野県の現地調査結果を参照）。したがって、このポリシーが現場で実現されている可能性は、発表されている数字よりもずっと低いと言わざるを得ません（なお、個人情報保護条例ですら、８２％しか制定されていない状況にあります。）。

しかも、Ｂ町やＣ町の職員や保守業者などが、このような不正操作を行ってＡ町のＣＳ内の本人確認情報を閲覧した場合（もしくは、県サーバやセンターサーバ内のＡ町住民の本人確認情報を閲覧した場合）は、それを防ぐ方法はありません。

（２）技術的な侵入・攻撃について

ア（１）は、ＣＳ端末を職員や関係者が直接操作して、情報を漏洩したり、改ざんしたりするという問題でしたが、ＣＳ端末を直接操作しなくても、攻撃端末からの遠隔操作で同様のことが可能となることが、長野県の「侵入実験」の結果、明らかとなりました。その点については、既に第１で詳しく述べたとおりです。

イ　しかも、住基ネットが全国的にほぼ共通のシステムであることから、一カ所でそのような不正侵入が可能となれば、全国３０００以上の市区町村の（しかも最もセキュリティの弱いところで）、同様の手口による不正侵入が可能となります。

ウ　更に恐ろしいことは、一旦その不正侵入の手法が（インターネット等で）明らかにされれば、専門的技術を持たない「素人」でも不正侵入が可能となるという危険性が高いということです。

エ　ネットワーク化されたコンピュータシステムには、このような危険性が内在されているのです。

（３）まとめ

以上述べてきたように、住基ネットシステムには、具体的に見ても、不正侵入が可能となる脆弱性が幾つも存します。

ア　特に、地方自治体の各現場におけるセキュリティに関する体制や教育訓練は、未だ全く不十分といわなければなりません。人的な側面の安全対策が、極めて不十分であることが、住基ネットシステムの現実的な危険性を示しているのです。

イ　また、技術的な面から見ても、例えばＣＳやＣＳ端末、そして、既存住基のサーバなどのセキュリティパッチ当ては全く不十分であり、その点を突かれて不正侵入される危険性が高いといわざるを得ません。

既に説明したように、ＣＳやＣＳ端末に対するパッチ当てを、マイクロソフト社などが発表した後、直ちに行わなければ、そのパッチに対するバッファ・オーバーフロー攻撃が行われた場合、確実に、それらの管理者権限が略奪されます。ところが、このパッチ当てには、発表後数週間が必要とされているのです。これは、「構造的な欠陥」ともいえるものであり、これでは、このような攻撃による侵入が起こることは“必然”といわなければなりません。

また、既存住基サーバのパッチ当てについても同様です。このパッチ当ても迅速に行わなければ、既存住基サーバの管理者権限が略奪されてしまい、さらに、既存住基サーバが踏み台となって、ＣＳサーバなどの管理者権限が略奪されてしまう結果となるのです。

ウ　反対に、不正侵入をはかる側は、以上に指摘した脆弱点のどこを突いてもいいわけです。また、ソーシャルエンジニアリングの手法にせよ、技術的な侵入手法にせよ、それらの手法は、今日では、出版物やインターネットで今や容易に入手できます（長野県の「侵入実験」において、庁内ＬＡＮへの侵入は、雑誌の付録のＣＤロムに入っている程度のソフトで可能なものでした）。

なお、一旦不正侵入が成功した場合、バックドア（ハッカーなどに侵入や攻撃を受けたサーバに仕掛けられた裏の侵入経路）を作っておく可能性が高いといわれています。バックドアは、２回目以降の侵入をより容易にするもので、パスワードの不正使用などログイン操作をすることなく侵入できる方法が仕掛けられていることが多いものです。このような状態では、ログも消去されていると考えた方がよく、侵入の痕跡も残りません。したがって、侵入や攻撃を受けたサーバは、バックドアが仕掛けられている可能性が高いため、全てのパスワードを変更するなどの善後策だけではなく、ＯＳやアプリケーションの再インストールなどが必要であるとされています。

エ　以上のように、攻撃側の裾野は広がり、その技術水準は上がってきているのですから、セキュリティを維持する側も、それに見合ったレベルアップを常に行ってゆく体制を作っていなければ（いわゆるＰＤＣＡサイクル

の確立）、進歩の激しいＩＴセキュリティにおいては、直ちに危険な状態に陥ってしまうのです。

オ　以上のような総合的な安全対策が、全国全ての市区町村、都道府県、本人確認情報の提供を受ける機関でなされていることが、住基ネット稼働の安全性の面からの前提であるといわなければならないのです。

ところが、実際には、最低限の安全対策であるセキュリティパッチあてすら満足に行なうことのできない（それを実行しうるだけの体制と、それを支える財政力のない）全国３０００以上の自治体を、一斉に・強制的にコンピュータネットワークでつないでしまいました。これにより、そこで扱われている原告をはじめとした住民の個人情報は極めて危険な状態におかれているのです。

このように、現状の住基ネットには、克服困難な、構造的な脆弱性が存することを、長野県「侵入実験」は実証したと言えるのです。

以上