２００４（平成１６）年3月３０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

当職らが、吉田柳太郎氏（以下、「吉田氏」という）の会見、講演、及び面談（平成１６年1月２２日、２月２６日、３月６日及び3月１７日）を通じて、同氏が２００３（平成１５）年に長野県の依頼で行った「住基ネットに係る市町村ネットワークの脆弱性調査」（以下、「侵入実験」という）に関して聞き取った結果は以下のとおりである。

第１　吉田氏の経歴について

吉田氏は、約７年前に、商社系のセキュリティ事業部を立ち上げる際の責任者として関与した。その後、一部上場企業や関東圏の県のセキュリティ監査などを多数実施した経験を有する。

なお、セキュリティ監査にもレベルがあり、２０～３０万円程度の費用で、各種ツールを使用して一通りの検査を行うというレベルのものも存するが、これでは十分ではなく、吉田氏は、そのような検査で７０点（いわゆる合格点）をつけられた企業の再監査を行なうことにより、重大なセキュリティ上の欠陥を発見したことも存する。

現在は、ネットワークセキュリティ会社コンサルタントとして活動中で、長野県の本人確認情報保護審議会の委員（情報通信技術の利用に関し識見を有する委員）を務め、長野県侵入実験はその責任者として実施にあたっている。

第２　「セキュリティ」に関する考え方について

１　コンピューターネットワークのセキュリティとは何か。

ファイアウォール（FW）や不正侵入検知システム（IDS）、暗号技術などを絶対化してはならない。住基ネットの構造は脆弱である。これは、われわれの世代

の技術者はみんなが言っていることである。しかし、それを公言すると会社でポストがなくなるから公然とは言えない状況にあるだけである。

2　そもそも、コンピュータ（ネットワーク）セキュリティに関して、技術的に「万全の体制」を作ることは不可能である。

確かに、セキュリティ対策にお金をかけると、かなりの程度セキュリティレベルが高度になってはゆく。しかし、永久に１００％にはならない。セキュリティレベルには限界が存する。

それは何故か。作っているのが人間、運用しているのが人間だからである。人間に対する脆弱点を突けば、絶対に情報を持ち出すことは可能であり、過去において「万全」であった例などない。

「ソーシャルエンジニアリング」という技法がある。攻撃者がもっともらしい嘘を言うなどして、情報へのアクセスが許されている善意の人たちから情報を直接引き出す技法である。

ケビン・ミトニックというアメリカ人が、『欺術（ぎじゅつ）－史上最強のハッカーが明かす禁断の技法』という本を出版しており（ソフトバンクパブリッシング、２００３年）、その中でソーシャルエンジリアリングの技法を具体的に紹介している。この本は必読である。

この人物は、ＦＢＩやＣＩＡの犯罪者リストというデータベースに侵入して、犯罪者の情報を抜き取って他人に売却したり、ＡＴ＆Ｔ（日本のＮＴＴに相当）のネットワークに侵入したり、シスコシステムズというルータのシェア世界一の会社のコンピューターネットワークの中心部に侵入したり、サンマイクロシステムズ（ＵＮＩＸと呼ばれるコンピュータ、ネットワーク、サーバ等を販売している会社）の人事データベースに侵入して、誰がどのような給料をもらっているか、家族構成はどうなっているかなどのデータを全部引き出した者であり、結局逮捕されて、５年の禁固刑を科せられ、２００１年に出獄し２００３年に保護観察期間が終了した。そこで出版したのが『欺術』である。

ここでは、どのようにして人の心理に入り込めば情報が手に入るかが、きわめて具体的に述べられている。

上述の最先端のＩＴ企業の情報データベースに侵入できるのであれば、住基ネットに入り込めないはずがない。

この本にもあるように、セキュリティのウィーケストリンク（最も弱い部分）はハードウェアやソフトウェアではなくて、「人間」である。人間を含めたシステムとして、安全性を考えなければならない。

現在３２００あまりの地方自治体の担当職員は、ソーシャルエンジニアリングに対するトレーニングを受けていないし、予定もないのはおかしい。

３　デジタルの世界では、改ざんされた個人情報が真正な情報になってしまう。これがウソであることを証明することはきわめて困難である。

住基ネット上の個人情報が改ざんされたら、それが改ざんされた情報であるということを証明することは不可能に近いことを考えなければならない。

４　さらに、個人に共通番号を付ければ、永久にその個人の情報を追及できることになる。共通番号をトリガーにして追っかけられるようにしておけば、コンピュータは疲れないから、追いかけ続けられる。そのような危険性を認識する必要がある。技術者は、みなこのような認識で共通している。

第３　「住基ネット」とはどの範囲か。

吉田氏は、「住基ネットシステム」とは、どの範囲を指すのかをはっきりさせることが必要であると強調する。

長野県の審議会においては、改正住基法によって新たに構成された住基ネットシステム部分（＝狭義の住基ネット部分）と、従来から存する既存住基システム部分の全部を含んで住基ネットシステムとしてとらえなければならないと考えている。何故なら、狭義の住基ネット部分は、既存の住基システムとネットワーク化され、①既存住基システム中のデータと狭義の住基ネット部分の「本人確認情報」は同期をとって、既存住基中のデータの変更・削除等がそのまま狭義の住基ネット中のデータに反映する関係にあること、及び、②住民票の広域交付や他市町村への異動の際には、既存住基中の「続柄」や「本籍」などのデータがそのまま狭義の住基ネットを流通させられる関係にあるからである。

総務省の側も、当初はこれに近い見解を示していたが、長野県の調査等によってその安全性に疑問が出てくるや、新たに付け加えた部分だけを「住基ネット」であると主張するようになり、しかも、国の責任範囲はその中でもさらに CS サーバのネットワーク側にある県が設置した FW からであるなどとして、その責任の限定を図っている。

第４　本件長野「侵入実験」について

吉田氏は、本侵入実験に関して、そのログとともに、長野県に対して詳細な報告書を提出している。長野県が発表した平成１６年２月２９日付「最終報告書」は、吉田氏作成の報告書を基にして、長野県の職員が作成したものであるという。

しかし、吉田氏が長野県に提出した報告書の内容は、そのまま発表するならば、不正侵入を助長することになるため、現段階で全ての事実を明らかすることは出来ないという。

吉田氏は、「長野県に提出した報告書は、長野県知事に開示するよう要請したらいかがか。是非、報告書の本文を見て欲しい。」と述べていた。

以上の前提の下で、以下、侵入実験の経過と結果について聴取した事実等を報告する。

１　目的等

(1) 目的

本侵入実験は、市町村ネットワークの更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への不正アクセス、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に実施された。

(2) 実施主体

長野県が、阿智村、下諏訪町、波田町の協力を得て実施した。

実際の実験は、同県本人確認情報保護審議会委員でもある吉田氏の指揮監督の下に、高度な専門知識・技術を持つ補助者を付けて行った。

(3) 日時、場所

第１次　２００３（平成１５）年９月２２日～１０月１日まで。

阿智村、下諏訪町、波田町

第２次　同年１１月２５日から２８日まで。

阿智村

(4) 調査方法

内部からの侵入（庁内 LAN から住基ネットへの侵入）と外部からの侵入（インターネットから庁内 LAN への侵入）との２種類の調査を行い、これらの結果を組み合わせることにより住基ネットシステムにおける脆弱性を明らかにしようとした。

ア　内部からの侵入調査

庁内 LAN に調査用コンピュータを接続して庁内 LAN 及び庁内 LAN 上に存在する各種サーバについての情報を収集し、その情報をもとにサーバの管理者権限（注１）奪取を試みた。

管理者権限を奪取した既存住基サーバから既存住基サーバ／（コミュニケ

ーションサーバ（CS サーバ）間の市町村設置ファイアウォールについての情報を収集するとともに、既存住基サーバに偽装した調査用コンピュータにより CS サーバとの通信を試みた。

また、CS セグメント（注２）に接続した調査用コンピュータにより、CS サーバ及び CS 端末についての情報を収集し，既知の脆弱性を利用して CS 及び CS 端末の管理者権限奪取を試みた。

イ　外部からの侵入調査

遠隔地からインターネットを経由してファイアウォール及び DMZ（注３）に置かれた公開サーバについての情報を収集し、得られた情報をもとに公開サーバへの侵入を試みた。

（注１）管理者権限＝全ての機能を使えるユーザー権限のこと。

管理者権限の一般的奪取方法

（「バッファ・オーバーフロー攻撃」（バッファ・オーバーランも同じ）

＝「バッファ・オーバーフロー攻撃」とは、バッファ（メモリ領域＝限度がある）の許容量を超えてデータを送りつけ、意図的にバッファ・オーバーフロー（データがあふれてプログラムが暴走すること）をおこし、あふれ出たデータを実行させてしまう攻撃。正常なプログラムの動作ではオーバーフローしないように制御されるが、セキュリティホールがあり、これに対する exploit を用いれば攻撃できる。

Exploit（エクスプロイト）＝元々はセキリュティホール（セキュリティ上の欠陥＝プログラムの不具合）を検証するために、セキュリティホールを発見した者が、インターネット上で公開する小さなプログラムのこと。この exploit を広く配布し、セキュリティ診断ツールとして活用するのが目的。この exploit を用いることで、自分のパソコン（のＯＳやアプリケーション）にセキュリティホールがあるか、修正プログラムを適用したあとであればセキュリティホールは修復されたか、ということがわかる。

ところが、exploit を少し改変するだけでワームや攻撃ツール（ハッキング・プログラム）に作りかえられてしまう。典型例としては、０３年７月１７日にマイクロソフトがセキュリティホールの発覚を公表し修正プログラムの提供を開始、７月２６日には exploit が公開されると、８月４日にはこの exploit を悪用したトロイの木馬型ウイルスが、８月１１日にはブラスターワームが検出された。Exploit が公開されると数日で攻撃プログラムがつくられるので、マイクロソフトがセキュリティホールを公表したら、ただちに修正プログラム（パッチ）を適用することが必要である。

（注２）「セグメント」（segment）＝分割されたものの一部分という意味。

この場合は、市町村設置 FW で仕切られた CS サーバ側の区画にある HUB ポートに調査用コンピュータを接続したことを指す。

ハブ（HUB）とは、LAN ケーブルの集線装置。ネットワークの中継点の役割を果たす。

（注３）「DMZ」（DeMilitarized Zone）

＝非武装地帯のこと。ネットワーク用語で、外部からの接続要求があるｗｗｗサーバや電子メールサーバなどを設置するためにイントラネットとは別に構築される公開用ネットワークのことをさす。公開用ネットワークをイントラネットから分離することにより、イントラネット側により強固なセキュリティを設定できるという利点がある。なお、実際には Proxy サーバによって保護されている。

「イントラネット」とは、インターネットで利用される技術やサービスを転用して構築した企業内の LAN やＷＡＮのこと。

２　阿智村及び下諏訪町における調査結果

（１）実験態様

ア　阿智村

第一次調査では、役場サーバ室内の HUB、隣接する施設の LAN ポート、庁内 LAN にダイヤルアップで接続されている出先機関のルータ（注４）に調査用コンピュータを接続して調査した。

（注４）※「ルータ」（router）＝LAN と LAN、LAN と WAN を接続するネットワーク機器。

第二次調査では、CS が格納されている役場サーバ室内のラックを開錠し、CS セグメントにある HUB に調査用コンピュータを接続して調査した。

イ　下諏訪町

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。

（２）判明した脆弱性

ア　庁内 LAN の脆弱性

（ア）既存住基サーバなどが接続されている庁内 LAN が組まれた本庁舎に隣接する施設（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いた。そして、その施設内の会議室

内にあるLANポート（接続口）に調査用コンピュータをLANケーブルで接続したところ、それだけで、庁内LANに接続することが出来た。

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（注５）をＤＨＣＰが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。

（注５）TCP/IPプロトコルを利用したネットワーク上の個別コンピュータの識別番号。[192.168.10.1　255.255.255.0]のような０から２５５までの数字を４個並べて表される。

（イ）村役場の出先機関においてある端末は、ISDN回線（電話等に利用されているデジタルネットワーク回線）を通じて庁内LANと接続できるような仕組みになっており、この出先機関の端末のところに調査用コンピュータを接続して、庁内LANに接続（侵入）することができ、既存住基のサーバ内の情報に自由にアクセスすることができた。

この侵入のために必要な技術レベルは、コンピュータ専門雑誌にＣＤ－ＲＯＭでついてくる無償ツールを使うだけで簡単にできるといったものであり、侵入に要した時間は、約３０分であった。

このことは、何者かにこのダイアルアップアカウント（電話番号等）（注６）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。

（注６）※公衆回線とモデムを使うなどして離れた場所にあるコンピュータにログインしたり、その資源を使用したりする権限。リモートアクセス権限。

（ウ）このネットワーク系列は、インターネットとつないでいない閉じたネットワークであるという「前提」があるため、この既存住基サーバのファイル共有サーバには ID とパスワードというような設定が全くなされていない状況にあり、誰でもこのネットワークに接続さえできれば、既存住基サーバの情報を、閲覧、書き換え、追加等が可能という状態であった。

（エ）下諏訪町において、市販されている業務用無線LANを利用して無線LANシステムを構築し、隣接する建物から調査用コンピュータを使って侵入実験を行ったところ、庁内のネットワークに接続（侵入）ができた。

（オ）CS端末は住民サービス窓口にあるが、その端末の背面にネットワークケーブルが剥き出しにして配置してあったり、操作者識別カード読み取り装置のＵＳＢの接続線が同様に剥き出しにしてあったりするところが多数

存在し、住基ネットのネットワークに直接接続することも、物理的に難しくない状態にあった。また、監理も、特に厳しくもなかった。

イ　既存住基サーバ及び庁内ウェブサーバの脆弱性について

（ア）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（住民課の窓口等で使われている端末コンピュータ）と同じ場所に、調査用コンピュータを接続して、侵入実験（脆弱性の確認）を行ったところ、朝９時半から１０時ぐらいから実験を開始して、約１時間で、この既存住基サーバと庁内ウェブサーバの管理者権限の奪取に成功した。

これはバッファ・オーバーフロー攻撃による管理者権限の奪取である。

この「略奪」のレベルは、これらのサーバの画面を調査用コンピュータの画面に映し出して、そのサーバ自体を自由に操作でき、調査用コンピュータからサーバのデータの消去・改ざんが可能というものであった。

また、既存住基サーバ中には、リレーショナルデータベースが入っていたが、それを管理している ID とパスワードに関しても、管理者権限（いわゆるルート権限）を略奪し、このデータの中身を自由に改ざんができる状態になった。

（イ）既存住基と CS サーバとはデータの同期をとっており、既存住基でデータの入力・削除・変更が行われれば、即時に CS サーバのデータに同様の変更が自動的に反映される関係にある。

（ウ）以上のことから、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ことになる。

ウ CS 端末及び CS サーバの脆弱性

（ア）下諏訪町、阿智村ともに、住基ネットの CS 端末は、住基ネット市町村調達 FW の CS サーバ側に配置してあったが、このハブの空き口に、調査用コンピュータをつないで、侵入実験を行った。

（なお、一部の自治体では、CS 端末を市町村設置 FW の外側＝庁内 LAN 側に設置してあるため、侵入はさらに容易となる。）

（イ）CS サーバ

実験の結果、CS サーバについて、約１時間～１時間半で、バッファ・オ

ーバーフロー攻撃により、完全に管理者権限を略奪した。

なお、「役場サーバ室内のラックを開錠」して実験しているが、ハブ自体は鍵がかかっていないところに設置されているものであり、また、CS端末自体は住民サービスカウンター側に設置されているものである。よって、総務省の、「物理的な侵入を伴う実験としての的確性を完全に欠いた方法で行われている」との批判は当たらない。

（ウ）CS 端末

CS 端末には、当時の最新のセキュリティパッチがあたっていた。そのため、バッファ・オーバーフロー攻撃によっては管理者権限を奪取できなかった。

しかし、CS サーバで得られたデータを利用することにより、管理者権限でログオンできた（この詳細については、長野県への報告書には記載してあるが、その詳細は未だ公表されていないため、述べることが出来ない。）

この攻撃によって管理者権限を略奪した CS 端末については、操作者識別カードおよびパスワードがなくても、自由に操作（CS 端末の画面を調査用コンピュータの画面でそのまま監視することができ、CS 端末のマウスも動かすことができるなど）ができる状態となった（管理者権限を奪取できたことを示す画面を写して、長野県への報告書に添付している）。

このことは、CS 端末で操作している ID やパスワードや操作方法全てが、そのまま調査用コンピュータ画面で見ることが出来るということである。調査用コンピュータで、その操作方法をそのまま真似て検索や住民票の広域交付等をすれば、真正な操作者が操作しているのと同じことになるから、検索や住民票の広域交付等が出来ることになると考えられる（但し、これは不正アクセス禁止法に抵触するため、実際に実施してはいない）。

エ　市町村設置ファイアウォール（FW）の脆弱性

（ア）FW は、いわゆる「関所」であり、ビルにたとえると警備員のいる入退室管理になる。ここの警備員に対し、「Ａという人は通すように」という指示を出すと、警備員は「Ａ」以外の人の通過を阻止することになる、という仕組みである。

ところが、FW は機械であるから、「Ａという人はこのような条件に合致する人」という情報を与え、この条件に合致するか否かで機械的に判断させることになる。よって、この「条件」に合致さえすれば、「Ａ」にな

りすました「Ｂ」は、この「関所」を通過できることになる（２５番とか、８０番のポートが開いている、という状態）。

その他にも、この「関所」自体を乗っ取って、それまで定められていた条件をなくすことによって、FW を通過するという方法も存する。FW もコンピュータであるから、この管理者権限を乗っ取ってしまえば、このような方法も可能である。

（イ）本侵入実験においては、第２の方法である、この FW の管理者権限を略奪することは行わなかった。

しかし、調査の結果、FW に不要なポートが空いていることが判明した。このポートは、遠隔メンテナンス用と考えられるものであり、このポートを利用すれば、FW 自体を攻撃することは可能である。

（ウ）この FW を通過する仕組み、方法は発見できた。

「仕組み・方法を発見した」とは、今回の実験は、庁内の業務に影響が出ないようにするために深夜の時間帯に行ったため、実際に FW を流れるデータを捕まえることができなかったが、この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（全く同じデータを作って流し込む）ことは可能であり、そのようなデータを流し込めば、ここで使用されているアプリケーションの脆弱性を突いて、FW 越しに CS サーバの管理者権限を略奪できるということである。

このアプリケーションの脆弱性は、アプリケーションが全国共通仕様であるため、具体的に述べるならば全国 3200 市区町村においてハッキングを助長する結果となってしまう重大な脆弱点である。そのため、長野県への報告書には詳細に報告してあるがここで具体的に述べることは出来ない。

３　地方自治情報センター（LASDEC）の住基ネット監視の不十分性

（１）本調査において、平成１５年１１月２５日午前中に CS サーバの管理者権限を略奪していたにもかかわらず、LASDEC から何の連絡もなかった。

そのため、LASDEC が、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 と CS サーバの間にある HUB 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。

（２）この調査により、LASDEC の住基ネット監視は、少なくとも、県設置 FW の市

町村側においては、不正侵入は検知できず、サーバやファイアウォールに電源が入っているか、配線が切断されていないかなどの「生き死に」の判断が付く程度の監視しか行っていないことが明らかとなった。

4　波田町におけるインターネット側 FW の通過

（1）波田町において、遠隔地より、インターネットを経由した侵入実験を行った。インターネット側 FW 越しに DMZ にあるウェブサーバを攻撃したが、当時知りうる限りのセキュリティパッチが適切にあたっていたために、バッファ・オーバーフローを起こさせることができず、同サーバの管理者権限が略奪できなかった。

（2）この調査は、FW 越しにウェブサーバに対して攻撃を行ったのであり、総務省のように、「実験では FW を突破できなかった」というとらえ方は間違いであり、FW というものが分かっていない発言である。

（3）波田町においては、実験の時点では適切なパッチ当てを怠らずに行っているために、脆弱性はなかったが、このような努力を怠れば、サーバの管理者権限を奪われる危険性が存することは間違いがない。

したがって、住基ネットとインターネットが物理的に接続していることが危険であることには変わりがない。

第3　まとめ

1　吉田氏は、今回の調査で明らかになった最も重要な点を次のように指摘した。

セキュリティホールおよびその対策のためのパッチが、マイクロソフト社などから発表されるたびに、直ちに（その日の夜の内に）、当該のウェブサーバや端末のコンピュータ、FW、ルータに至る全ての機器にパッチを当て続ける努力を怠らないようにしなければ、そのネットワークシステム内に存するデータを守ることは出来ない。これを怠るならば、バッファ・オーバーフロー攻撃などによって管理者権限を略奪される危険性が極めて高いことが、今回の侵入実験で実証された（特に、未だにインターネットと接続をしている市町村においては、その危険性が高い）。しかも、全国 3200 ある自治体の全てが、もれなく、直ちに、パッチをあて続けなければ、そのネットワークの脆弱性は修復されたことにはならないのである。

しかし、こうした対策を、全自治体が、一斉に実行し続けることは不可能である。こうした、根本的にして、克服しがたい脆弱性を、常に内包せざるを得ない

ネットワークシステムが現在の住基ネットシステムである。このようなネットワークシステムの中を、センシティブな個人情報が流通させられているのである。

2　吉田氏の行った実験は、不正アクセス禁止法に抵触しないことを大前提として行われたため、承諾を得られた地方自治体の管理するネットワークに限定されたものでしかなかった。しかし、その範囲においても、以上のような重大な脆弱性を発見できた。

以上の脆弱性は、①住基ネットシステムが全国共通仕様であることから、長野県内の市町村だけの脆弱性ではなく、他の全ての市区町村でも同様の脆弱性が存するということであり、同様の不正侵入の危険性が存するということである。

さらに、②一旦、何者かによって脆弱性が見いだされ、その手法が明らかにされたならば、その後は専門家ではない「初心者」によっても真似され、侵入される結果をもたらすものである（平成１５年１１月、京大知的財産企画室研究員が不正アクセスの方法を公開したことによって、その後、その不正アクセス手法が真似された例などに端的である）。

なお、今回の実験において、管理者権限奪取のために使用したセキュリティホールは、既にマイクロソフト社が公表済みのものであった。その意味で、今回の攻撃は、「ネットワーク技術の初心者」のレベルでも可能なものであったと言いうる。

3　吉田氏は、この侵入実験に関して、長野県に対して調査結果をありのままに報告している。

しかるに、記者会見等の場においては、その脆弱性を具体的に指摘するならば、高度のハッキング技術を有しない初心者に対してまでも不正侵入の方法を教えてしまうことになることから、具体的に指摘できていない。この点をとらえて、総務省などがいわれなき非難を行っているが、反論を控えている面が存する。

4　吉田氏は、法廷などで、長野県で行った侵入実験を基に、①仮想的に構築した住基ネット環境を操作し、住基ネット環境に侵入し、②FW 越しに、管理者権限を略奪し、③住基ネット環境内の情報を閲覧、改ざん、削除等を行う仮想侵入実験を行うことが出来るとのことである。

5　さらに、吉田氏は、「是非、総務省（LASDEC）や中野区などの被告自治体の同意を得て、実際の住基ネットシステムにおいて、調査実験を行いたい。そうすれば、どちらが正しいことをいっているかはっきりする。」と繰り返し述べていたことを最後に付け加える。

【補足】

吉田氏は、弁護団に対して、住基ネットシステムの安全性等について考えるにあたって参考となる、以下の３冊を紹介して下さった。

① 前述の『欺術－史上最強のハッカーが明かす禁断の技法』（ケビン・ミトニック著、ソフトバンクパブリッシング、２００３年）

② 『ＣＯＤＥ－インターネットの合法・違法・プライバシー』（ローレンス・レッシグ著、株式会社翔泳社、２００１年）・・・サイバー空間の特質とそこにおけるプライバシーの問題を考える際の参考。

③ 『暗号の秘密とウソーネットワーク社会のデジタルセキュリティ』（ブルース・シュナイアー著、株式会社翔泳社、２００１年）・・・コンピューターネットワークの技術とセキュリティに関する基礎的理解を持つための参考。

２ 吉田氏はまた、「映画はフィクションだから」と言わずに、いろいろな映画も見て欲しいと述べた。

例えば、「ＴＨＥ　ＮＥＴ」（邦題「ザ　インターネット」）。冒頭シーンで下院議員が自殺する。ゲイであることを隠していた下院議員が、個人情報をＨＩＶ陽性に改ざんされることにより、ついに発病したかと誤信して自殺するところから始まる映画である。

実際に、オーストラリアの軍隊で、血液型を改ざんされて、違う血液を輸血されて死亡するという事件が発生しているという。

３ 吉田氏は、その他にも、アメリカなどでは、個人情報の改ざんについて、訴訟になっている事例が多数存することを紹介して下さっている。

以上