甲第４１号証

上　申　書

２００４年１１月２６日

吉田裕太郎㊞

私の証人尋問調書について、以下の通り補足、訂正致します。

１　調書ｐ．２０

「品川区などのように、ＣＳ端末が庁内ＬＡＮに接続されているときに、ＣＳ端末は庁内ＬＡＮに接続された攻撃端末から直接攻撃できることになるのか」という趣旨の質問に対して、私は、そのような直接攻撃が可能であることを前提にして、そのような直接攻撃によりＣＳ端末の管理者権限を奪取した後の話をしました。すなわち、ＣＳ端末は、ＦＷの向こう側にあるＣＳと通信することを許されているので、「庁内ネットワーク（上の権限を奪取されたＣＳ端末）からＣＳに対する攻撃の可能性がある、たやすくなる、要は、ハードルが少なく攻撃できる可能性が極めて高いといわざるを得ないと認識しています」とお答えしました。

ですから、「直接攻撃できるということになるのか」という質問に対する直接の答えは、「イエス」ということになります。

２　調書ｐ．４８

私は、波田町において、「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」と答えましたが、これについては、少し舌足らずなので、補足します。

（日本ネットワークセキュリティ協会　http://www.jnsa.org/nsf2002/pdf/B81.pdf
の図を末尾に添付しましたので、参照してください）

一般に、ＤＭＺ上にある公開のウェブサーバやメールサーバと庁内ＬＡＮ上の端末とは、ＦＷで隔てられていますが、このＦＷは庁内ＬＡＮ側からＤＭＺ上にあるサーバに通信を許可することによってウェブサーバやメールサーバのサービスを受けることができます。つまり、インターネットから直接庁内ＬＡＮに入ってくる通信は許可していませんがＤＭＺ上にあるサーバがインターネットから来る通信を受け取り、サーバ自身のサービスの内容を庁内ＬＡＮ側の端末から要求の都度バケツリレー的にサービスを提供するために通信を行っているのです。（そうしなければ、たとえば、庁内ＬＡＮ上の端末でメールの受信、発信ができなくなってしまいます）。そこで、私たち実験チームでは、波田町のＤＭＺ上のウェブサーバ、メールサーバの脆弱点をついてこれらのサーバの管理者権限を略奪し、そこを踏み台として、ＤＭＺと庁内ＬＡＮ間のＦＷ越しに、庁内ＬＡＮに侵入しようと試みたのです。

ところが、（証言の中でもご説明したように）インターネット側のＦＷを超えてウェブサーバやメールサーバの脆弱点を探して攻撃を仕掛けてみたのですが、その当時、その時間内で私たちが用いることのできた脆弱点に対するパッチが当たっていたために、これらのサーバの管理者権限の奪取に至らなかったのです。

このような対策はＦＷの構造を正しく理解し自治体によってネットワーク構成や構造が固体差があるなかで担当者が極めて優秀であったといわなければなりません。このような担当者が日々のメンテナンスを行っているネットワークでは仮にＤＭＺ上のサーバの管理者権限を奪取できたとしても、庁内ＬＡＮに侵入することは困難といえるでしょう。

この波田町についてインターネットからの攻撃を成功させるためには、２週間から１ヶ月程度の期間をとって、その間に発見された脆弱点を突くなどの攻撃によってＤＭＺ上のウェブサーバやメールサーバのＯＳの管理者権限を略奪し、その上で、ＤＭＺと庁内ＬＡＮ間のＦＷの設定ミスやＦＷ自体の脆弱点を発見して、そこを攻撃してその管理者権限を略奪するなどのことを行わない限り、庁内ＬＡＮへの侵入はできないことになります。

但し、繰り返しますが、波田町のような厳格な設定・管理と運営を行える自治体は、全国でも稀だということはいえると思います。

（なお、このあたりは、全て「町内ＬＡＮ」となっていますので、「庁内ＬＡＮ」に訂正してください。）

3　調書ｐ．５０、およびｐ．６１以下で、ディスアセンブルしたのは、ＣＳ側か、既存住基側かについて

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１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。

（なお、ｐ．５０以下は、「リアセンブル」となっていますが、これは「ディスアセンブル」（disassemble）に訂正してください。）

4　調書ｐ．６２以下

被告側は、私たちが実験中に、指定情報処理機関監視ＦＷの内側（センターサーバ側）のケーブルを抜いたのだと主張してますが、私たちが抜いたのは、このＦＷよりＣＳ側です。この点は、「補助者」の人にも再度確認しましたが、間違いありません。

もし、被告側が、指定情報処理機関監視ＦＷの内側だとあくまでも主張されるならば、丙２９の６～８について、その内容が正しく、改ざんされていないことなどを証明して頂きたいと思います。特に、「丙２９の８」の図の②部分を抜くと、「丙２９の７」のようなメッセージがでることを証明して頂きたいと思います。

5　調書ｐ．７８

ここで私は、「中野区のＣＳの管理者権限（の略奪）を実験市町村（のＣＳ端末）からできるという認識はありません」と答えています。

私が、現時点において、実験の結果、可能性があると答えられるのは、中野区のＣＳの管理者権限の略奪に関しては、①中野区のＣＳセグメントに攻撃端末を接続して攻撃

した場合、および、②インターネットやダイヤルアップ接続などによって、中野区の庁内ＬＡＮに侵入して、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、中野区が設置したＣＳをＦＷ越しに（受動的）攻撃をした場合、③仮に、中野区が品川区などのように庁内ＬＡＮにＣＳ端末を接続している場合は、②と同様の方法によって中野区の庁内ＬＡＮに侵入して、庁内ＬＡＮ上にあるＣＳ端末を攻撃して管理者権限を略奪し、このＣＳを踏み台にしてＣＳを攻撃した場合だと考えています。

物理的に庁内に侵入しなければ情報は盗み出せないと定義付ける声がありますがそれは素人の安全と思いたい願望に過ぎません。地方の多くの庁舎はいまだに木造で内部に侵入しても警備会社とも契約もなく、庁舎内の端末が盗み出されている事件が後を立たないことかからも明白です。つまり、無線や特殊な回線と接続できる端末を庁舎内に忍ばせておいて情報を盗み出すことができる庁舎はたくさんあることでしょう。対策が不十分な自治体から他の自治体の情報を直接攻撃が可能かどうかの問題ではなく、検索できる仕組みである事実によって、特定の人を意図して狙った情報が弱い自治体から漏洩しその情報を元に予期せぬ危険性を発生させる可能性を否定できないことが問題だと考えています。

6　調書ｐ．８３など

私は、証言を通じて、「可能性がゼロではない」などという表現を何度も使っています（たとえばｐ．１８など）。しかし、そこで言いたかったのは、「可能性がゼロではない」ということは「危険性がある」ことを意味するということです。コンピュータネットワークセキュリティの世界では、「可能性がある」ということは、それに対する対処が必要ということであり、必要な対処を行わないことは、すなわち危険であるということです。責任ある立場の方が、「危険性がある」ことがわかっていながら、即座に必要な対策を講じないなどということは、許されません。

私が見たり、実験したりしたのは、全国に３０００以上ある自治体のうち、長野県のごく一部の自治体にすぎません。しかし、その中でさえも、セキュリティ的な対処ができていないため、初心者でも、侵入し、サーバの管理者権限を略奪し、データの書き換え等が容易にできる自治体を発見しました。

また、私たち実験チームは、時間的制約、場所的制約、インターネットが使えないなどの制約など、数多くの制約の中でも、報告書にあげたような数多くの脆弱性を発見しました。したがって、もっと多くの時間と、人的リソースがあれば、更に多くの、そして更に重大な危険性を指摘できた可能性は大です。実験の「補助者」として参加してくれた技術者は、「破壊者」のレベルにある、有数の技術能力を持った技術者であり、かれらの技術力によって、これだけの悪条件の中でも、これだけの「脆弱性」を発見できたわけですが、これら発見された「脆弱性」そのものは、いわば「初心者」でも容易に管理者権限を略奪できるレベルのものがほとんどです。

以上に補足してきたように、重大な脆弱性のある自治体が現にあることを知りながら放置すること、漫然と全国ネットワークに接続し続けさせることは、全国の自治体における「危険性」を放置するということであって、許されることではないと思います。

以上

e-GovSecProj/JCA-NET

吉田証人「上申書」添付資料について

本資料に添付された「図」(p.1 「2 調書 p. 48」参照)については、当該箇所に吉田証人が記載している URL に、当該「図」が公開されているため、この「上申書」からは削除しています。ご了承ください。

当該「図」(「インターネット・サイトの脆弱性 ファイアウォールの効用と限界 DNS の正しい理解」日本ヒューレット・パッカード株式会社)は、以下の URL にアクセスしてご確認ください。

http://www.jnsa.org/nsf2002/pdf/B81.pdf

e-GovSecProj/JCA-NET プロジェクト事務局