速　記　録（平成１６年１０月１５日　第１２回口頭弁論）

事件番号　平成１４年（ワ）第１６３０６号

証人氏名　吉　田　　柳太郎

原告代理人（水永）

甲第１３号証，甲第３１号証を示す

聴き取り報告書２通ですが，これらについてはお読みいただけましたでしょうか。

はい。

内容については間違いがございませんでしょうか。

はい。

吉田さんの経歴などについておうかがいしますが，甲第１３号証の「第１」の部分を見ますと，吉田さんは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そうですが，例えば，どういう業種のどういうシステムの監査を行った経験があるのか，簡単に御紹介ください。

過去の経験から申しますと，東証一部上場の製造業，それから金融機関，いわゆる銀行系さんの会社，これも大手の２行をさせていただきました。それから，東京近郊の自治体，都道府県単位の自治体ですね，こちらも過去，かかわらせていただいた経験がございます。

コンピュータネットワークのセキュリティ監査と言いますと，かなり守備範囲が広いと思うんですが，今回問題となっているコンピュータネットワークに対する不正侵入とか，コンピュータネットワーク上の情報の不正閲覧とか漏洩，こういうものとの関係では，どういう仕事をするということになるんでしょうか。

コンピュータネットワークが当初設計された段階で，意図した形で，意図したとおり動作しているのかどうか，あるいは動作するようにで

きているのかどうかというのを，初期段階，設計して実際に具体化したときに，意図した形で動作しているのかをチェックするという仕事，それから，実際に稼働した後に，当初の意図した状態から，意図しないことが起こっていないかどうか，こういったことを確認する仕事，こういったものが脆弱性の診断をするというテストになります。

よく擬似侵入テストとか，侵入実験ということも言われますけれども，こういうのとの関係では，どういうことになるんでしょうか。

例えば，個人情報を集めているような，ウェブサーバと呼ばれているような，個人の情報を集めるような仕組みを持つプログラムが，外からは誰もその固まった個人情報を取り出せない，抜き出せない。あるいは内部であったとしても，特定のコンピュータからではないと，その情報は抜き出しができないようにしているという設計がなされていても，プログラム自身が持っている脆弱性，あるいはオペレーティングシステムが持っている脆弱性，あるいはそのネットワークの間に存在する機器の脆弱性によって，情報が意図しない形で持ち出してしまえることがあるかもしれない，それを確認するのが擬似侵入テストという形になります。

今回の長野県の報告書を見ますと，安全性調査という表現がされているんですが，この長野県の安全性調査も，いわゆる擬似侵入テスト，これをやったというふうにお聞きしてよろしいんですか。

結構です。

吉田さんは平成１４年１２月から，長野県の本人確認情報保護審議会に，情報通信技術の利用に関し識見を有する委員として参加されていますね。

はい。

そして，吉田さんはその審議会の委員として，平成１５年の２月から３月にかけて，長野県下の市町村の住基ネットの現場も検分されていますね。

はい。

甲第３号証の３を示す

これは２００３年５月８日付けの「長野県本人確認情報保護審議会第１次報告」添付の資料の２，「住基ネットに関する市町村調査」ですが，住基ネットの現場を検分された結果は，ここに報告されているとお聞きしていいわけですか。

結構です。

その現場の検分をした上で，更に平成１５年の９月から１０月にかけて，長野県の安全性調査実験，以下単に実験とも言いますけれども，これを行っているわけですね。

はい。

甲第３２号証の１ないし４を示す

「ネットワーク・セキュリティ調査報告書」関係ですね，その結果がここにある報告書として長野県のほうに報告されているわけですか。

はい。

この報告書には，ほかにどのようなものが付けられて提出されているんでしょうか。

アクセスログという，機械が吐き出した，どのような操作をしたかという記録ですね，そのログというものをあわせて提出してあります。

そうすると，そのアクセスログと照らし合わせてみれば，今から証言していただく内容が，実験の結果得られたものであることが，そのアクセス記録からも裏付けられるということになるんでしょうか。

そのように考えております。

次に，長野県の調査，実験の目的とか手順などについてお聞きします。

甲第３３号証の２，甲第３３号証の４を示す

「住民基本台帳ネットワークシステムに係る市町村ネットワークの脆弱性調

査の実施について（依頼）」等ですが，平成１５年９月と１０月に行った長野県の第１次調査と第２次調査の目的とか対象の町村などは，ここに書かれたとおりですね。

はい。

そうすると，調査内容はここに書いてあるように，「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調査する。」ということになるわけですか。

はい。

これを見ますと，実験期間が２日間であるとか３日間であるとか５日間というふうになっていますけれども，こういう実験について，こういう期間というのは普通なんでしょうか。

極めて異例な短い時間だと認識しています。大体２週間から１か月かけるところが通常だと思っています。

だけど，この短い期間内で一応これだけのことは調べられたということになるわけですね。

はい。長野県からの御依頼の日程の中で，依頼された内容に従って，できる範囲のことをやったというふうに認識しております。

甲第３３号証の３，甲第３３号証の５を示す

ここに補助者として「[redacted]」という人が挙がっていますが，この人はどういう方なんですか。

彼も東証一部上場の企業，それから製造業，金融証券会社，あるいは大手商社系ですね，そういったところの脆弱性検査の技能を有する，非常に優秀なエンジニアだと私は認識しております。

いわゆる侵入実験とかセキュリティのチェック，これに関しては，高い能力を持っているというふうに聞いていいわけですか。

極めて高い能力を有するものと認識しております。

外国でもかなり有名な方というふうに聞いているんですが。

そうですね。米国の技能を持つエンジニアのグループの中では，彼の名前というのは周知されているというふうに認識しております。

次に，手順などについてお聞きします。

甲第３２号証の４を示す

５枚目ですが，これが上から順に，第１次調査の阿智村，下諏訪町，波田町の調査手順の概略ということですね。

はい。

６枚目ですが，これが第２次調査の阿智村の手順の概略を示したものということですね。

はい。

では，阿智村の手順などについてお聞きしますが，甲第３２号証の４の３枚目の上の図を見てください。これが第１次調査時の阿智村のネットワークと，どこに調査用のコンピュータを接続したかに関する概略の図ですね。

はい。

甲第３５号証を示す

甲第３２号証の４の５枚目にある阿智村の手順について，甲第３５号証も用いながら，その概略を示してください。

まず庁内ネットワークに対するノード確認スキャンというのを行います。調査用の端末を接続して，ＬＡＮ内におけるコンピュータがどのように返事をするのか，返事をするのはどれかというのを確認します。またＩＰアドレスが使用されているか否か。庁内ネットワークに対するポートスキャンというのを次に行います。どのようなサービスが動いているのかというのを確認します。その次に，住基サーバ，庁内ウェブサーバ，各種情報の取得ですね，オペレーティングシステムとい

うのが何に使っているのか，共有はされているのか，どこが共用利用になっているのか，というような情報の確認をします。次に，ウェブサーバの管理者権限の取得，これを試みます。あらかじめ読んで得られた情報を基に，管理者権限を取得，よく知られた脆弱性から始めます。その次のページで，既存住基サーバの管理者権限を取得します。ウェブサーバの情報，それからほかのサーバの情報，こういったものを取得した後に，住基サーバの管理者権限の取得ということを行います。それから，既存住基サーバの管理者に成り済まして，いわゆるバックドアというのを設置します。それから，バックドアを設置した後は，バックドアに今度はログインをします。バックドアを使って住基システムのサーバに侵入をします。その次に，既存住基サーバの設定を基に，市町村調達のファイアウォールというのがどこにあるかというのを調べます。最後に，ファイアウォールの脆弱性を調べます。こういった手順であります。

こういった手順は割とオーソドックスな手順というふうにお聞きしてよろしいんですか。

はい，結構です。

甲第３２号証の１を示す

１１枚目から１６枚目を見てください。調査結果詳細とありますが，今，述べていただいた調査の結果分かったことが，この報告書の当該部分に記載してあるというふうにお聞きしてよろしいわけですか。

結構です。

ここに墨塗りで隠してある部分も含めて，庁内ウェブサーバであるとか，既存住基サーバのＩＰアドレス以外は，調査の結果分かったこととお聞きしてよろしいわけですか。

はい。

ちなみに，この報告書，第１次報告書と第２次報告書の両方ですけれども，これを見ますと，各所に墨塗りしてある部分がありますね。

はい。

これらにはどういう類のことが書いてあるんでしょうか。

パッチと呼ばれるものがあります。用語集で見ていただければと思うんですが，そのパッチの種類，ＩＰアドレス，サービスの種類，ＩＤ，パスワード，アプリケーションの名前，サーバの固有名，こういったものが書いてございます。

関数なんかも書いてあるわけですか，具体名は。

書いてあります。

これらの墨塗り部分に書いてあることが明らかになってしまうと，セキュリティ上はどういう支障が発生するんでしょうか。

これを提出されたのは長野県さんでいらっしゃいますが，ある一定のスキルを持つ者が，今，この墨塗りをされたもの自身を読めば，もう十分侵入のマニュアルになるんだろうというレベルのものだと考えております。よって，この墨塗りの部分がもしすべて書いてあれば，もっと技能のレベルの小さな方であっても，十分興味本位的にネットワークの侵入を許してしまう可能性が極めて高くなると，認識しています。

次に，下諏訪町についてお聞きします。

甲第３２号証の４を示す

３枚目の下の図を見てください。これが下諏訪町のネットワークの概略図ということでよろしいわけですか。

はい。

甲第３２号証の１を示す

１７枚目ないし１９枚目を見てください。先ほど示していただいた手順で行

った調査の結果分かったことが，ここに記載してあるというわけですか。

はい。

次に，波田町についてお聞きします。

甲第３２号証の４を示す

４枚目の上の図を見てください。これが波田町の公開部分のネットワークの概略図ということですか。

はい。

甲第３２号証の１を示す

２０枚目と２１枚目を見てください。先ほど示した手順で行った調査の結果分かったことが，ここに記載してあるというふうにお聞きしてよろしいわけですか。

はい。

それでは，阿智村の第２次調査についてお聞きします。

甲第３２号証の４を示す

４枚目の下の図を見てください。これが第２次調査時の阿智村のネットワーク，及び，どこに調査用のコンピュータを接続したかについての概略図ですね。

はい。

そうすると，第２次調査のときはＣＳセグメント，すなわちファイアウォールよりＣＳサーバとかＣＳ端末の側の区画ですが，ここの部分のハブに調査用のコンピュータを接続しての調査も行ったというわけですね。

はい。

甲第３２号証の２を示す

第２次調査の報告書ですが，この７枚目以下に，第２次調査の結果分かったことが記載してあるというふうにお聞きしていいわけですか。

はい。

次に，長野県の調査とか実験で判明した，脆弱性に関する事実についておうかがいします。

甲第３２号証の１を示す

第１次調査の報告書ですが，これの７枚目を見てください。阿智村，下諏訪町，波田町の第１次調査の結果，どのような脆弱性が発見されたかのポイントについては，この概評部分に記載してありますね。

はい。

以下，順にお聞きしていきます。まず阿智村と下諏訪町に関しては，第１に，庁内ＬＡＮに接続されたサーバ類は，即侵入可能な脆弱性を有していたことが判明したわけですか。

はい，そうです。

この脆弱性の内容について補足的にお聞きしたいんですが，１２枚目の「既存住基サーバに関して」とあるページの３行目，「Servicepack,Hotfix」墨塗りとなっている部分，及びその下の「保有する脆弱性等の状況に関して」の部分を見てください。これが後で説明していただく，パッチ当てがどこの時点のものまで適用されていたかについて書いてあるところとお聞きしていいわけですか。

はい。

要するに，古いパッチしか当たっていなかったということですね。

最新ではなかったということであります。

そうすると，最新のほんの前までは付いているということになるんですか。

かなり古いという認識を記憶しております。

この古いパッチしか当たっていないと，例えば，雑誌の付録のＣＤ－ＲＯＭに付いているようなソフトを使うだけで，簡単にそのサーバの管理者権限を奪取できるという結果をもたらすものなんでしょうか。

間違いないと認識しております。

再度，７枚目の第１段落を見てください。阿智村，下諏訪町では，第２に，使用しているデータベースのユーザー名，パスワードが，簡単に分かったということですね。

はい。

ユーザー名とパスワードが分かるとどういうことができるのか，どういう被害が考えられるのかということについて，説明してください。

できないことはないです。情報を新たに作る，改ざんをする，消去する，付け加える，自由にできます。

要するに，何でもできる状況になってしまうということですか。

はい。

で，実験のときにそういうのが分かった結果，リモートのコンピュータから，容易にデータベースの閲覧とか改ざん可能な状態になったということですか。

はい。

ちなみにこれは住民基本台帳のデータベースも同様ということなんでしょうか。

はい。

ということは，リモートにある攻撃用のコンピュータから，既存住基台帳のデータベースの書換えなんかも可能になってしまうということですか。

はい。

あと阿智村についてお聞きしますが，３つ目として，阿智村においては，ファイアウォールの設定が庁内ＬＡＮから管理用ポートが確認可能な状況であって，ファイアウォールの無効化の危険があったということですか。

はい。

ファイアウォールが無効化されると，どういう被害というか危険性が考えられるんでしょうか。

ファイアウォールというのは，意図した通信のみを通すために設置さ

れている機器，機械であります。しかし，無効化すれば，意図しない通信であっても，自由に通信をさせることができます。もっと言いますと，自分だけが通信できるようにしてしまうということも可能になります。

そうすると，その自分にとってはファイアウォールはないに等しいから，どういう攻撃もできるしということになるわけですか。

攻撃もできるしという話になると，ちょっと長くなってしまうんですけれども，ほぼ同義でとらえていただいて間違いないと思います。

それでは，４番目として，小中学校や図書館といった出先機関から何の制限もなく庁内ＬＡＮに接続が可能であったとか，５番目として，村役場の隣接建物では不特定多数の者が自由に使用可能な会議室に接続口があり，それが庁内ＬＡＮに直結していたということがあったわけですか。

はい。

要するに，これは既存住基サーバが置いてある村役場の本庁舎に侵入しなくても，出先機関とか隣接建物からでも簡単に庁内ＬＡＮに侵入ができるということになるわけですか。

はい。

ちょっと離れて，ちなみにお聞きしたいんですが，本庁舎に侵入しなくても庁内ＬＡＮに侵入する方法としては，例えば，インターネット経由の侵入であるとか，無線ＬＡＮを使っているところでは無線ＬＡＮ経由の侵入，こういうものは想定はできるわけですね。

１００パーセント否定することは不可能だと思います。

それから，６番目ですが，ファイル，ディレクトリの共有が無制限だったということが分かったわけですか。

はい。

この共有ということになると，どういう被害を受けるということになるわけ

ですか。

長野県には提出済みではありますが，中に，ファイル共有エリアにあった表形式のデータ，それからワードプロセッサーで書かれたデータ，これが自由に閲覧，改ざん，消去，新規追加できる状態であり，その証拠を長野県さんには提出済みであります。

そうすると，以上述べていただいたような現状であれば，村役場の本庁舎以外のところから簡単に庁内ＬＡＮに侵入でき，かつ既存住基サーバの管理者権限を乗っ取ったり，その中のデータの改ざんを行ったりすることは，容易にできるということになってしまうんでしょうか。

はい。出先機関から本庁舎のデータ共有フォルダの中にあるデータを引き出し，その証拠の表形式のデータを長野県さんに証拠として提出をいたしました。

それでは第２次調査についてお聞きします。

甲第３２号証の２を示す

７枚目の概評部分を見てください。この阿智村の第２次調査で発見された脆弱性のポイントに関しては，ここに記載してあるわけですね。

はい。

以下，順にお聞きしますが，まず第１に，ＣＳ及びＣＳ端末は即侵入可能な脆弱性を複数保有していたことが分かったということですか。

はい。

この１３枚目と１４枚目を見てください。具体的には，ＣＳに関しては１３枚目，ＣＳ端末に関しては１４枚目に，その内容の記載があるということでよろしいわけですか。

はい。

そうすると，少なくともＣＳサーバに関してはパッチ当ての後れ，ＣＳ端末に関してはパスワードに関する脆弱性があったということになるわけですか

ね。

はい。

その結果，実際にＣＳやＣＳ端末の管理者権限が奪取できたということになるわけですか。

はい。

７枚目に戻りますが，２つ目として，ＣＳデータベースの閲覧が可能であったということですか。

はい。

３つ目としては，庁内ＬＡＮ側からファイアウォール越しにＣＳやＣＳ端末攻撃の可能性があったということですか。

はい。

４つ目として，ＣＳやＣＳ端末にセキュリティ上，問題のある動向を監視する装置が欠けていたことが分かったということですか。

はい。

それでは，今，３つ目に挙げていただいた点について詳しくお聞きします。

甲第３２号証の３示す

「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」ですが，この補足説明というのが調査報告書のどの部分の補足説明になっているかということについて，まずお聞きします。

甲第３２号証の２を示す

１２枚目の中段の「また，port[redacted]に於いて双方向の通信が可能な状態となっております。」の段ですが，この補足説明は当該部分の補足説明になっているということでよろしいんでしょうか。

はい。

同じく１５枚目の中段に「脆弱性に関して」で始まる段落，及び「対策」と題した段落がありますね。

はい。

先ほどの補足説明というのは，この部分の補足説明にもなっているんでしょうか。

はい。

３つ目ですが，同じく１６枚目を見てください。これの中段の「４）ＣＳ，既存住基サーバで通信をするアプリケーションに存在する脆弱性」の段落ですが，先ほどの補足説明はこの部分の補足説明にもなっているんでしょうか。

はい。

甲第３２号証の３を示す

ここはなかなか難しいんで若干誘導的に最初聞きますが，この補足説明において，第１に問題としているのは，ＣＳと既存住基サーバ間で通信するアプリケーションに，バッファ・オーバーフローを起こす非常に危険な関数が使用されている，ということなんでしょうか。

はい。

結論的でいいですが，バッファ・オーバーフローを起こすとどういう事態を招いてしまうということなんでしょうか。

意図しない計算結果が正しいとコンピュータが判断してしまうことになります。

その結果，どういう事態をもたらすということになるんでしょうか。

その状態に，かつ，意図しないプログラムを実行させることができてしまう。で，それは正しい行いではないのか，正しくないのか，計算機であるコンピュータが判断できないという状態を作ります。

そういうプログラムを実行されてしまうことによって，攻撃をする側からすると，どういうことができるようになるということなんですか。

端的に言うと，管理者権限を遠隔から奪取することが可能になります。

バッファ・オーバーフローを起こして管理者権限を奪取することができると

いう結果をもたらすことになるわけですね。

間違いないです。

それでは２つ目ですが，補足説明の第３段落目，ここで問題にしているのは，市町村調達ファイアウォールの設定が，何番かのポートで双方向通信を許可しているということになるわけですか。

はい。

この市町村調達ファイアウォールというのは，既存住基サーバとＣＳサーバの間にあるファイアウォールのことですね。

はい。

今挙げたこの２つの条件が揃えば，庁内ＬＡＮ側から自由にＣＳサーバを操作することが可能となる可能性があったということですか。

極めて高い可能性があったと認識しております。

ちなみに，ここの表現の仕方について念のためにお聞きしたいんですが，この段落の３行目に「受動的攻撃を実施すると共にバックドアを設置することが可能でした。」とありますね。

はい。

これは実際にそのような実験を行ったという趣旨なんでしょうか。

いえ，これは可能性がありますということでございます。

甲第４０号証を示す

「受動態攻撃の可能性について」ということで，説明の図がかいてあるんですが，ここに言う受動態攻撃というのは，受動的攻撃と同じ意味ですね。

はい。

では，受動的攻撃について，我々が分かるようなレベルで説明してください。

極めて複雑な話になろうかと思います。できるだけ端的にお話したいと思います。図で示してあるように，ＣＳ側から既存住基サーバへは，何がしかのきっかけによって，情報を取得しに行くようになっている

ようです。で，その取得しに行ったときに，例えば，生年月日は２桁です，２桁以上の人はいません。ということは，プログラムは２桁入っていると認識しています。そこに，例えば，１０００桁の文字列のようなものを入れてしまえば，コンピュータは異常を起こします。それはＣＳ側が異常を起こすんですね。で，異常が起こるときに，同時に，あらかじめこの前提は，既存住基サーバの管理者権限を奪取してあって，既存住基サーバが自由に管理者権限を操作できる状態にあるという前提で，ＣＳ側がバッファ・オーバーフローを起こしたときに，既存住基側で同時に管理者権限を奪取できるプログラムを走らせて，それをＣＳにつかませるんですね。こうやれば，ＣＳは管理者権限が奪取できる状態になる可能性が極めて高いと判断しました。３番目に書いてあるのは，更にファイアウォールが双方向の通信を許可していたために，既存住基サーバ側のネットワークエリアからＣＳを自由に遠隔操作可能になる可能性が極めて高かった。つまり，既存住基サーバに脆弱性があれば，ＣＳの管理者権限がファイアウォール越しに奪取できる可能性を示したものであります。

今，説明していただいた，この受動的攻撃の手法によって，庁内ＬＡＮ側よりファイアウォール越しにＣＳサーバの管理者権限を奪取することができるということになるわけですね。

極めて可能性が高いというふうに認識しております。

甲第３２号証の３の４段落目に「ＣＳサーバの権限を庁内ＬＡＮより取得可能であれば，同時に（ＣＳサーバから攻撃することで）ＣＳクライアントの権限も取得が可能です。」と書いてありますが，こういう可能性もかなり高いということなんですか。

極めて高くなると認識しています。

このＣＳクライアントというのは，いわゆるＣＳ端末のことですよね。

はい。

つまり，センターサーバにある全国民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ったりするのに使うコンピュータ端末のことですね。

はい。

このＣＳクライアントを庁内ＬＡＮに接続した攻撃端末であるコンピュータから遠隔操作することも可能になるということなんですか。

可能性があると思います。

この遠隔操作するというと，実際問題としては，例えば，画面がどうなるとか，マウス操作がどうなるということで言うと，どうなるんでしょうか。

最大限自由に管理者権限が奪取できる状態であると仮定すれば，画面もマウスも全く同じものを，遠く離れたところで，全く同じように操作できます。

そうすると，ＣＳクライアントに触らなくても，遠くにある攻撃用のコンピュータを操作すれば，そのＣＳクライアントを直接操作したのと同じ結果をもたらすということになるわけですか。

実際には，ＣＳ端末と呼ばれるものには，操作者カードというものを入れないと動作しないということの前提になっておりますが，そのカードを使ってログインした状態の間に，例えば，ログインしたままカードを差し込んだまま誰かが離席していたとします。で，その間には，遠隔で操作すれば，ＣＳ端末は閲覧操作可能になる可能性が極めて高いというふうに認識しております。

要するに，操作者カードのＩＣカードが入っている状態であれば，遠隔で自由に操作できるというふうにお聞きしていいわけですか。

きっとできるんだろうというふうに認識しております。

以上の前提で想定される危険性について，お聞きします。

甲第３１号証を示す

３枚目の「（３）」の「①」部分ですが，このＣＳ端末の管理者権限の奪取が行われた場合，この「ａ」に書いてあるように，地方自治情報センターのサーバや県のサーバ，他の市町村のＣＳサーバにある本人確認情報の不正閲覧や，「ｂ」に書いてあるように，他の市町村住民の住民票の写しの広域交付が不正に行われる危険性があるということになるわけでしょうか。

これについては，１００パーセント絶対行えないと断言することは，不可能だと思います。

専門家ですから，なかなか微妙な言い方ですけれども，反対に言えば，可能性はそれなりにあるということになるわけですね。

ゼロではないと思います。

理論的にはどういう言葉で言うと，要するに，正規のＣＳ端末を攻撃用の端末から遠隔操作することになるわけですよね。

はい。

ですから，この相手方としては，正規のＣＳ端末からのアクセスであるというのと区別がつかなくなるということになるわけでしょうか。

はい。一定の条件が整えば，可能になると思います。付記転入だとか付記転出，転入転出，いろんな条件によって，この不正なアクセスを正規のアクセスとして偽装し，それが全部うまくいけば，確実に行えると思います。

ＣＳ端末の管理者権限奪取のその他の方法についてお聞きしたいんですが，要するに，ＣＳ端末の管理者権限の奪取ということが，大きな問題になるわけですね。

はい。

このＣＳ端末の管理者権限の奪取の方法というのは，先ほど説明していただいた，ＣＳ既存住基サーバ間で通信するアプリケーションにバッファ・オー

バーフローを起こすといった場合しか，想定できないものなんでしょうか。

ほかにもいろんな可能性はあると思います。

以下ちょっとお聞きしたいんですが，吉田さんが長野県下の自治体の現場を見られた経験に踏まえて，ＣＳセグメントに直接攻撃用コンピュータを接続して，そこから攻撃をかけて，ＣＳサーバやＣＳ端末の管理者権限を乗っ取る，そういう可能性はあり得るとお考えでしょうか。

間違いないと思います。

だから，実際にそのＣＳセグメントに接続できるかどうか，この辺りの可能性については，現場の実態から見て，どうでしょうかね。

私が長野県の自治体さんに足を運んで，この目で見た事実をお話すれば，施錠されているところにＣＳは置いてあるということに，ルールとしてはなっていますが，現実には，むき出しのスチールラックの上にポンと置かれていました。で，これがＣＳですということで見せていただいたのは，その庁内役場の同じフロアで，どなたでも入っていけるところに，壁の隅のスチールラックの中に置いてありました。これが私の見た事実です。

そういうところに置いてあれば，誰でも物理的に制止されなければ，アクセスはできるということですね。

残念なことですが，町役場の方自身にお尋ねをしても，どちらがＣＳでどちらが既存住基か，あっ，これ古いから，こっちが既存住基だよねというようなレベルで，完全な認識，あっ，これシール張っていた，まずいよね，張ってあるからこっちだろう，というような会話をした記憶がございます。

こういうふうに，ＣＳセグメントに直接攻撃端末を接続できるというような場合であれば，先ほどおっしゃった，ファイアウォール越しの攻撃というのは不要になるわけですよね。

意味はないと思います。

直接攻撃しちゃえばいいということになるわけですね。

はい。

その関連でちょっとお聞きしたいんですが，品川区などの場合，ＣＳ端末がファイアウォールの庁内ＬＡＮ側に接続してあると言われていますね。

はい。

この場合は，庁内ＬＡＮに攻撃端末を接続さえできれば，直接ＣＳ端末を攻撃できるということになるんですか。

市町村調達と呼ばれているファイアウォールは，庁内ネットワークにあるＣＳ端末がＣＳに通信することを許しているはずですから，その通信のサービス，ポート番号というのは開いているはずです。つまり，庁内ネットワークから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言わざるを得ないと認識しています。

更に次の可能性の問題ですが，先ほど阿智村でファイアウォールの無効化の危険性というのを指摘されましたね。

はい。

それで，ファイアウォールの無効化ができれば，庁内ＬＡＮ側からＣＳセグメントにあるＣＳ端末の管理者権限を乗っ取るということも容易になるわけですか。

無効化すれば，そうです。

更に次の可能性としては，ＣＳ端末の管理者用のＩＤとパスワードを取得できた場合にも，管理者になり済ますことによって，その管理者権限を乗っ取ることができるということになるわけですね。

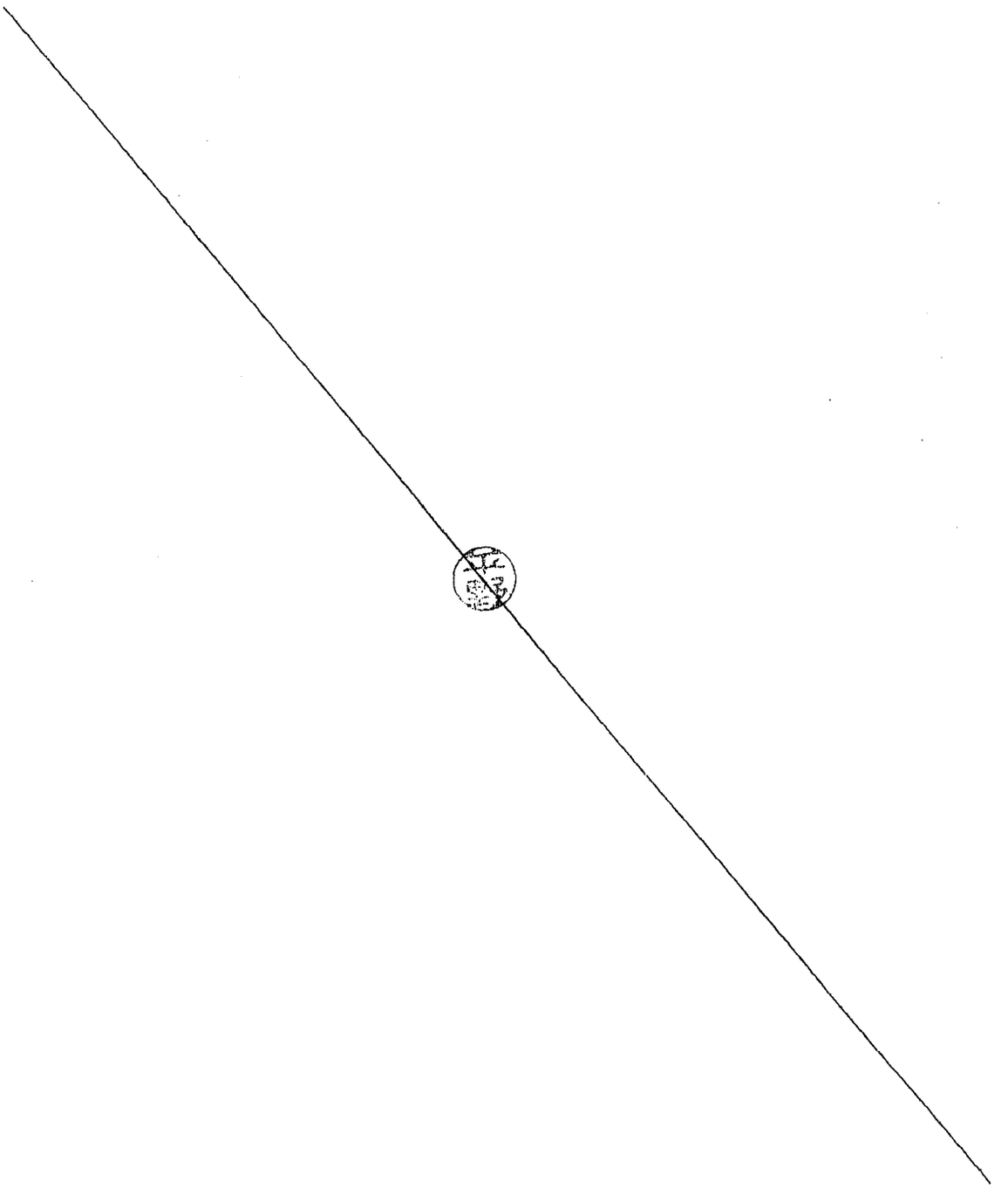
条件が整えば可能です。

今，幾つかの攻撃手法というのを挙げましたけれども，こういういろいろな

手法によって，ＣＳ端末の管理者権限を乗っ取る危険性は存するということになるわけですか。

はい。

（以　上　　平　野　道　子）



甲第３６号証を示す

吉田さんは，以上述べていただいた長野県の実験の経験などを基礎として，ここに記載された問題点などを指摘されたというふうにお聞きしていいわけですか。

結構です。

まず，ファイアウォールについてお聞きいたしますが，国の側では，長野県の実験ではインターネット側のファイアウォールを突破できなかった。だから，実験は失敗だったんだという主張をされていますね。

はい。

この点について，７－１からの図などを利用されて，反論も含めて御説明いただきたいんですが。

７－１から始まるファイアウォールは突破されていないというお話でございますが，現実にどのような作業が行われていたのかというのを説明したいと思います。まず，７－５が正常なインターネット側からのファイアウォールへのアクセスです。引き続き７－６を見ていただきますと，ＷＥＢサーバの情報が閲覧できるように，正常なアクセスは，ファイアウォールを越えてＷＥＢサーバの中にある磁気ディスクの情報を正常なアクセスの端末側に返すという作業を行っています。例えば，グループウェアやデータベースが存在していれば，あらかじめファイアウォールに意図した扉を通ってサーバにアクセスをするという状態です。で，今回のアクセスというのは，７－９から説明してある下の赤い「今回のアクセス」と書いたもので，ファイアウォール越しに設置されたサーバ群の管理者権限の奪取を行うものであります。７－１０から順を追ってめくっていただいて，７－１３を見ていただければと思いますが，正常なアクセスと同じように，今回は不正なアクセスが行えるかどうかの確認をファイアウォールの内側にあるサー

バ群に対して行いました。で，その通信の中に悪意のあるプログラムを仕込んで，管理者権限が奪取できるかどうかの確認をしました。それは，７－１５以降になります。最終的に７－１８のところまでアクセスを行った結果，ファイアウォールの内側にあるＷＥＢサーバの脆弱性，それから内側にあるサーバ群の脆弱性というものが管理者権限を奪取するに至らなかったものであります。管理者権限を奪取できなかったが故に，７－１９ページ以降ですが，ファイアウォールの内側にあるＷＥＢサーバ等のサーバ群を踏み台にして，更に内側の庁内ネットワークに侵入するということができなかったというのがインターネットからのファイアウォール越しのサーバの実験を行ったプロセスになります。で，これを見ていただければお分かりのように，一番最後のページになろうかと思いますが，７－２７で示していますように，ファイアウォールの内側にあるサーバ群の脆弱性の確認をレポートとして出しております。オペレーティングシステムの番号，動いていたアプリケーションのプログラムのバージョン番号といったものまで記録として長野県には説明をいたしました。提出もしております。よって，ファイアウォールを突破されていないということになるのであれば，ファイアウォールの内側にあるＯＳやプログラムのバージョン番号を報告できないはずであります。これは，インターネット越しに東京から長野県の波田町のインターネット側からのアクセスを行ったものであり，物理的に遠く離れた場所のサーバのファイアウォールの内側にある情報を確認し，その脆弱点をその時点で発見することができなかったために管理者権限の奪取ができなかったという結果になっています。御質問の答えになるのは，ファイアウォールが突破されていないという話にこれが結び付くのであれば，ファイアウォールの内側にある情報取得自体ができなかったということになるんではないかと

思います。つまり，ファイアウォールは突破されないとか突破されるといったものではない，そういう仕様のものではないということが明らかだろうと思っております。

念のため確認的にお聞きしたいんですが，ファイアウォールは危険な通信をシャットアウトしてくれるとか取り除いてくれるという俗説がありますよね。だから，ファイアウォールがあるから大丈夫なんだというような意見を持つ人もいるんですけれども，今の御説明との関係では，その辺のことはどうなんでしょうか。

ファイアウォールが，危険だろう，疑わしいだろう通信をシャットダウンしてくれるというのは幻想です。ファイアウォールはあらかじめ決められた通信を通過させるもので，それが偽りのものなのか正しいものなのかという判定はファイアウォール自身ではできません。通してしまったものは，中に何を持ってこようが，違う人が返送していようが，それを確認する手だてを持っていません。それがファイアウォールになると認識しております。

そうすると，許可された通信というのに成り済ましをされたら，それを見破ることはできないということになるわけですか。

はい。厳格に記録を取って，厳格に分析をしても，それを発見するのは極めて困難であることは間違いないと思います。

今回の波田町のいわゆる侵入実験は，最終的には管理者権限を奪取できるところまでは行かなかったということなんですが，このことは，すなわち波田町の公開部分のサーバの安全性が確認されたというふうに言えるんでしょうか。

波田町のサーバ群は，私が実験をさせていただいた時点において，既知の脆弱性，それからゼロアタックと呼ばれるような未知の脆弱性で，今，特定の人だけが知り得る脆弱性について，我々が知る範囲で確認

をしましたところ，脆弱性を発見できなかった。よって，管理者権限の奪取ができなかったというふうに認識しております。

今回は，例えば何日間の間で，更に短い時間しかできなかったわけですよね。

はい。

これを，例えば１か月ぐらいの間，継続的にアタックをかけるというふうなことをやれば，可能性としてはどうですか。

通常このような脆弱性検査というのは，ありとあらゆる脆弱点の可能性について徹底的に調査するという目的で我々は依頼者に雇われて仕事をしております。複数の高い技能を持った技術者を使ってあらゆる脆弱点を見付けて，そこを徹底的に掘り下げる。これには非常に長い時間を要します。冒頭でもお話ししたように，今般は非常に短い，異例の中で，しかも３日間だとか２日間ということになっておりますが，フルタイムではできませんでした。夜間だけとか特定の時間だけとかという限定された中でやった実験においては，結果として十分な脆弱点を発見するに至りませんでした。知り得る限りでやった中では，管理者権限の奪取に至らなかったということになります。

次に，いわゆるパッチとかパッチ当ての問題についてお聞きしたいというふうに思いますが，これは，セキュリティの限界という点も絡めてお伺いしたいんですけれども，甲第３６号証においても，サーバとか端末はパッチ当てが最新でないこととか，パッチは全国３２００の市町村全部で一斉に当たっていないと意味がないというようなことを主張されていますね。

はい。

これは４ページ目ですが，まず，パッチ当てというのはどういうもので，パッチが当たっていないとどういうことになるのかというのを簡単に御説明いただけますか。

パッチは，５ページで説明していますが，継ぎはぎととらえていただ

いて構わないと思っています。プログラムの脆弱性を，脆弱性のない形に変更するものですね。全体をすっきり入れ替えるんではなくて，継ぎはぎ的にけがをしたところを直す，そういったプログラムがパッチと呼ばれています。これは，利用されているオペレーティングシステムが，このケースの場合はマイクロソフトですけれども，マイクロソフトのホームページに行けば，今すぐ対策してくださいという形で緊急というところにチェックが入っているような脆弱点を告知したパッチが存在しています。これを対策として当てないと，このような形で攻撃を受ける可能性がありますということに対する攻撃を防ぐことができないということになっております。これは，どなたでも見られるインターネット上のサイトにマイクロソフト自身が攻撃の可能性を絵で示しています。

それで，パッチ当てをしないと，結論的にはどうなるんでしょうか。

管理者権限の奪取が可能になります。

管理者権限が奪取されて，例えばバックドアが作れるという場合がありますよね。そういう場合にその後パッチ当てをすると，そのバックドアというのは埋められてしまうものなんでしょうか。

パッチの中に，特定のオペレーティングシステムにファイアウォール機能を持つものが最近出てまいりました。それ以外は，幾らパッチを当てても，既にバックドアを仕込まれていれば，それ自身を発見できないかぎりは管理者権限をのっとる通信は遠隔で可能であります。

そうすると，ずっと遠隔で操作できるという状態が続けられるということですね。

気付かれない限りは可能です。

それで，パッチを最新のものにしておかないといけないということについてなんですが，このパッチというのは，例えばマイクロソフト社を例に挙げる

とどれくらいの頻度で発表されているということなんでしょうか。ばらつきはあると思いますが。

それは６ページなんですが，マイクロソフト社自身が自分の脆弱点を認知して，そのパッチを対策してインターネット上に公開するケースというのは１か月に３回も４回もあるときもあります。多いときには６回あったりもします。そういうふうになっているので，頻度というのは分からないですね。多いときもあれば短いときもある。ですけれども，容量で言うと，何十メガバイト，あるいは多ければ１００メガバイト近い情報をパッチとしてインターネットからダウンロードしない限り，マイクロソフトが既知の脆弱性として認知しているものを防ぐことはできないというのは明らかな事実です。しかしながら，残念なことに，マイクロソフトというのは自分たちが認識して対策を施したものしか公表できません。先ほど少し触れましたが，ゼロアタックとかゼロデイアタックと呼ばれているものが世の中にはあります。脆弱性を発見してもマイクロソフトに報告しないで，こうやればこの脆弱性をつくことができるよということを自分たちのホームページで事細かに解説しているホームページが世の中にはたくさんあります。英語のホームページになっていますけれども，無料で翻訳するサイトがたくさんあります。そこの翻訳機にかければ，コンピュータの若干の知識と，それからどこの書店でも売っているようなコンピュータ関係の雑誌を手に入れさえすれば，マイクロソフトが脆弱性対策のパッチを作っていない間の空白の期間分のアタックについて脆弱性をつくという作業が可能になってしまいます。これは，つまりマイクロソフト自身が持っている脆弱点ということになろうかと思いますが，このようなサイトが世の中にはたくさんあり，かつ，ホームページでやっているところは正当化されているほうですね。で，我々が報告してから，

何月何日にマイクロソフトに通告しました。すると，マイクロソフトは何月何日にこの脆弱性パッチを出しましたという記録までホームページにはのっています。こういった情報は，メッセンジャーだとかコミュニティだとかチャットと呼ばれている世界で，こういう技能を持った人たちの中で常に情報としてやり取りされているものであります。

そうすると，そういうパッチといいますか，継ぎ当てのプログラムが発表されていないうちに攻撃されたら全くお手上げということになってしまうわけですね。

はい。残念なことに，このオペレーティングシステムは世界中で大変な数が使われておりますので，いろいろなところでこの脆弱点を発見し，メーカーに報告しないで自分自身のホームページで発表されているところは山ほどあります。

いわゆるゼロデイアタックというのはさておいて，マイクロソフト社から公表されたパッチについては，公表後どれくらい速やかに当てないといけないものなんでしょうか。

最低限その日の夜に当てるのがよいのではないかというふうに考えています。

吉田さんの経験からして，まあ出る度に当てないといけないわけですが，地方自治体でその日の夜のうちにすべてのサーバ群にパッチを当てるということは可能だというふうにお考えになりましたか。

極めて難しい，不可能に近いことだろうというふうに認識しています。

その理由を簡単に挙げていただけますか。

業者の方を呼んでじゃないと作業できないというふうに現場担当者の方が考えられています。要は，壊してしまったら大変だという思いから，業者の方に作業を委託するという状態になっています。業者の方に来ていただきますと，お金が掛かります。で，この作業が，先ほど

言いましたように１か月に何回もあったり，頻度が多かったり少なかったりします。業者の方と契約するときにも，回数で契約するか，包括的な形で契約を結ばざるを得ません。それを行ってもらうには，スケジュール化も必要です。しかし，今日出て明日やってほしいとか，今日出て今日やってほしいという話になると，業者の方も人材やリソースが限られていますから，すぐ対応できるかどうかは非常に微妙です。それから，ある日突然全然知らない方を呼んできて契約をしてすぐにやるということも難しいだろうと思います。よって，これを即座に全国一斉に行うというのは不可能に近い作業だろうというふうに認識しています。

それで，更にＣＳサーバとかＣＳクライアントに関するパッチに関しては，既存住基のパッチとはまた違う問題もあるみたいですね。

はい。これは大変なことを知ってしまいましたけれども，そのオーナーがだれなのかというのは現場の自治体さんも認識がありません。これは県のものですかね。そう言えば契約書はどうなっていましたっけね。市町村が，僕たちがお金を払っているから，これは僕たちのものでいいんですよね。でも，これ中身を触ったこともないですし，そもそも知らないんですよというようなことを言われていました。そんな認識の中で，市町村さんが能動的にそのパッチを当てるといっても，そういえばＬＡＳＤＥＣから何か来ていたけどな。あれ，どこやったっけ。ほっぽらかしたままだな，みたいな話になっています。これが現実でした。なので，指示があっても，パッチを当てるということに対する準備，コストとか，自治体さん単位で対策をし終わるまでは行動が起こせていないという現実が分かりました。

ＣＳサーバとかＣＳクライアントに対するパッチというのは，別にＬＡＳＤＥＣが当てに来てくれるとか，そういうわけではないわけですね。

の，ようです。

そうすると，地方自治体でその手当ができる能力がないといけないということですか。

現場でできるようになっていないと，だれかに委託をしても，時間とコストが掛かるだけだと思います。

それで，１０ページなんですけれども，吉田さんは，現状では初心者レベルのアタックで十分侵入を許してしまう状況にあるんだということをおっしゃっていますね。

はい。

この点を簡単に説明していただけますか。

これは，すごく抽象的なイメージではありますが，初心者と呼ばれている方が世の中にはたくさんいらっしゃいます。雑誌を見て，コンピュータのハッキングってどんなのかなと興味のある人間がたくさんいます。先ごろ警察庁の発表でも，不正アクセス防止法で検挙した割合は未成年者が半分以上であったというような新聞報道を記憶しております。つまり，雑誌や専門書に付いているような説明を見て，興味本位でネットワークに侵入してみようという試みをする人，これを初心者と位置付けています。私が確認をした現状のチェックのレベルでは，この初心者の方々に十分に管理者権限を奪取されてしまう可能性を持っているんだということを認識として持つ必要があるんだろうということであります。

それに関連してお伺いしたいんですが，初心者レベルではちょっと太刀打ちできないようなセキュリティの欠陥であるというような場合でも，例えばプロに近い人とかが攻撃のプログラムを開発しましたと。それがインターネットに流れましたというような場合だって考えられるわけですか。

考えられると思いますが，プロ中のプロが作業をすると，足跡を消し

ます。自分が何を取ったかというのは，新聞に出るようなまねはしません。よって，何が起こったのか，何を取られたのか，その記録を出したところで，その記録が改ざんされていないことを担保する形で記録を取らない限りは全く価値がないと思います。

例えば，この前京都大学の研究員の人ですかね，ある手法を学会か何かで公表しちゃいましたよね。そういうような例が，本件のような住基ネットの場合でも考えられるかということなんですが。

あると思います。

そうすると，例えばこういう手法でやれば入れるよというようなのがインターネットに流されるというような場合だと，それをまねすれば初心者クラスでも侵入ができるということになるんでしょうか。

できると思います。

今，技術的な面についてお聞きしたんですが，あと，おれおれ詐欺じゃないですけれども，ソーシャルエンジニアリングというようなだましのテクニックによる不正侵入とか不正アクセスというのも問題になっているようですね。

はい。

ほんのちょっとでいいんですが，説明していただけますか。

私が行った自治体さんでは，担当主任さんは女性の方でした。それから，担当係長さんの方は男性の方でしたが，２人は小学生のときから顔見知りといいますか，同じ村で仲良しです。お互いランドセルを背負っているときから一緒でよく知っているんだわというお話がありました。何もかも信頼関係と性善説の中で運用が行われています。その中に疑いはありません。逆に言うと，よそ者が来ればすぐ分かるような小さな村でした。そこには１つの安全性が保たれているということが言えるかもしれません。しかし，人を疑う前提が入っていません。プログラムの中では，だれかが性悪説に立って物事をとらえない限り，

何かあったときにトレースする，トレーサビリティという言葉がございます。徹底的に追いかけて，これが私の情報でした，これは私の情報ではありませんと，追究して正しいことか間違っていることかを判別することが必要であろうと思っています。しかし，そのような仕組みがありません。よって，何が行われたのか，どうなったのか，最終的に，これは本当に記録から間違いないと担保できるのか，そういったところまでの扱いができないシステムが，非常に小さな信頼関係の高いところでも，そうでないところでも，同じ物差しで導入され，運用されているという事実が分かったと思っています。

そういう信用とか信頼なんかを悪用されてしまうということも考えられるということになるわけですか。

つまり，ソーシャルエンジニアリングというのは，人間の心のすき間，弱い部分を利用して情報を奪取するということです。人の心にはかぎは絶対に掛けられません。もしそういうことをするのであれば，この情報の取扱いについて，どのようなルールが必要で，どうしなければならないかという教育が徹底されていなければなりません。幾らマニュアルを送りつけて読んでおけと言っても，人間は読めません。やはりだれかに指導してもらい，教育をしてもらわないといけません。十分な教育がなければ，自治体は補うことができません。なぜなら，人がいないんです。ですから，何年か単位でどんどん業務を替わっていかないといけないということであれば，なおさら首長以下，末端の職員まで統一した考え方で十分な教育を受けていなければ，性善説に立って情報を持ち出してしまう可能性というのは否定できないと思います。

パッチ当てについて，最新のパッチを当てないといけないということと，そのほかに全国一斉にパッチを当てないといけないんだということをおっしゃ

っていますが，この全国一斉にという意味を簡単に説明していただけますか。

お金のある自治体さんは即座に対応できるところもあるでしょう。しかし，スケジューリングが合わない，人がいない，今日は早く帰りたい，いろいろな理由でその作業自体が延びてしまうことがあろうかと思います。先ほど提示したように，ＣＳというのが既存住基のセグメントからファイアウォール越しに管理者権限を奪取できる可能性がある以上，どこかで問題が発生した場合には，それは住基ネット全体のセキュリティレベルを低下する事態になりかねない可能性は依然残り続けるというふうに認識します。よって，同時一斉にきれいに最新のパッチ対策が行えないというのであれば，ネットワーク全体のセキュリティレベルが担保されないと，そのように認識しております。

今の御証言ともちょっと絡むと思うんですが，被告のほうでは，たとえ各自治体の既存住基に脆弱性があっても，既存住基システムは住基ネットシステム本体とは関係がないから，住基ネットシステムの安全性については問題がないんだという主張をされているんですが，この点についてはいかがでしょうか。

私の業界の中では，そういったことというのはほぼ通用しないと思っております。つまり，論理的に幾ら切れていても，物理的にはつながっています。何か一つ，ありの一穴でも問題があれば，そこから問題が拡大する危険性を含んでいます。よって，その全体のネットワークのセキュリティレベルを脅かしかねない事態になると認識しています。

２ページの下のほうの三つで，自治体にはネットワークに詳しい担当職員がいないとか，自治体は現状のネットワークを正確に管理，把握できていないとか，国の想定どおりの理解と対策は行えていないということを挙げていらっしゃいますが，国のほうは，例えば丙第１２号証などで，重要機能室を設置するとか，重要機能室を設置できないときは，重要機器並びに磁気ディス

クなどについて，盗難されたり権限のない者が容易にアクセスすることができないように適切な管理を行うことをセキュリティ基準としていまして，その点は，平成１５年１月，２月に行ったセキュリティ対策の自己点検結果で全国すべての市町村で３点満点だったという主張をされていますよね。吉田さんが見聞した自治体の現場の状況にかんがみて，こういうアンケート結果とか被告の主張についてはどういう御判断をされていますでしょうか。

できているところは確かにあるでしょう。否定はしません。ただ，できていないところがあります。これは現実です。この目で見てきました。アンケートにはそう書かざるを得なかったと，担当者はそう言いました。一番最初，私は担当職員として鉛筆で書きましたと。最終はボールペンで提出になっています。私は最終形を知りませんとはっきり聞きました。今でも鮮明に覚えております。アンケートの結果をうのみにして，こうなっているから大丈夫なんだというのでは，現場に一緒に行っていただければはっきりすると思います。むき出しのスチールラックのところにＣＳサーバは今だにあるでしょうし，かつ，国の想定どおりの設定や動作の理解がそのまま行われていると思うのは大きなおごりだと思います。現場はそんなに理解はできていません。かつ，自治体の現状のネットワーク自体でさえ正確に把握できている人はまれです。こんな絵があるんだけどな。こうなっているのかね。よく分からないなと，そう言われていました。今どうなっているかも知らない人が，国の想定どおりのネットワーク構成を運用まで理解して実施できている可能性はどこにあるのか，現場を見た限りでは極めて少ないと思いました。

以上，幾つか自治体現場の現状についても御証言いただいたんですが，このシステムは全国３２００の市町村を一斉にコンピュータネットワーク化しているわけですよね。そこで，住民の個人情報を流通させはじめたというこの

住基ネットシステムの安全性の評価について，吉田さんが，ネットワークセキュリティの専門家として最後に述べたいことがあったらおっしゃっていただきたいんですけれども。

途方もなくお金を掛けなければ，一定の安全性を確保することはできないんだということを現場を見て思いました。それから，国が意図して作った思いや動作というものに届かない。人がいないですとか，コストが掛かってそっちにお金が回せないとか，そもそもコンピュータのことがよく分からないとかという担当者の方をきれいに救えるような環境になかったというふうに思います。これは，できるところはやれるし，できないところはできなかったんだというふうに認識していて，大変な差別を生むような道具を押し付けられた形になっているんだなというふうに個人的な感想として持ちました。このような現状では，できる人しかやれない，できない人はできないんだという状態のまま，すべてが安全という物差しで運営し続けられていくことの危惧を強く感じ，残念に思います。

そうすると，こういう住基ネットの現場に踏まえれば，そこで扱われて流通させられている個人情報の安全性についてはどういうふうに判断されますか。

先ほども言いましたように，自分の情報はどこまでいっても自分の情報だと私は思っています。その情報がどのように扱われ，どのような利用形態を経て何に使われたのか，ずっと追いかけることができるようなものでないといけないと思っています。今はそのような状態になっていないと思っていますし，サーバごと盗み出す人は余りいないかもしれません。しかし，データをバックアップして小さなポケットに入る記録媒体に移してそれを持ち出してしまう可能性もあります。現実にそういった形で情報漏えいというのは起きておりますけれども，そういったバックアップのメディアでさえ全部バーコードで管理して，

今どこにあるのかまで追いかけるようなシステムというようなものに作り替えなければ，とても怖くて今のネットワークシステムに私の情報を預けるのは非常に危険だなと思っております。

被告国，東京都，東京都中野区代理人（榮）

甲第３２号証の１ないし４を示す

これらの報告書は，証人が今回の実験の指揮監督者として，[redacted]氏ほか１名を補助者として作成したものと理解してよいですね。

はい。

甲第１２号証の１，丙第１７号証を示す

これらの報告書はいずれも長野県のもので，便宜上甲第１２号証の１を中間報告，丙第１７号証を最終報告と呼びますが，これらの報告の内容は，証人が作成した調査報告書に基づいて長野県の職員が作成したものですね。

はい。

証人は，今回の実験の指揮監督者としてこれらの報告の内容を確認されていると理解してよいですか。

読みました。

発表前に確認されているということですね。

発表前に確認できたものもありますが，発表後に確認したものもあります。

具体的に，事前に確認しなかった部分というのを指摘することはできますか。

記憶があいまいですので分かりません。

甲第３５号証，甲第３６号証，甲第４０号証を示す

これらの文書の中には[redacted]氏の名前で作成されているものもあるんですが，やはりその内容は証人自身の認識や意見に合致しているということですね。

はい。

今までお示ししたすべての文書が，証人自身の認識，意見に合致していると

理解してよいでしょうか。

はい。

丙第２９号証の１を示す

阿智村など，侵入実験を実施した実験市町村以外の市町村，例えば中野区という前提で聞いていきますが，中野区民の個人情報は，都道府県サーバ，この図では㋐と記載された部分，それから，全国サーバ，この図では㋑と記載された部分，それから，中野区のＣＳ，この図では㋒と記載された部分，この三つの場所に保管されているということですね。

保管されているという定義は何でしょうか。

サーバの中にデータとして記録されているという意味です。

どの条件で，どの順番で，どう記録されているということでしょうか。

一般的な聞き方としてこういう聞き方をすることが許されると理解しているのですが，端的にサーバに情報が保管されているかどうかは答えられないということですか。

都道府県サーバの中に情報が入っていないこともあると認識しております。

では，証人自身の理解としてお尋ねしますが，証人は個人情報はどこに保管されているというふうに理解しているのですか。

個人情報の定義を教えてください。

中野区民の住民にかかる住民の情報ということです。

既存住基ネット内のシステムの中に個人情報が入っていると思っています。

そうすると，住基ネットの中にはどこにも保管されていない可能性があるというふうに考えていらっしゃるんですか。

住基ネットの範囲の定義を教えてください。

それでは，この図で言う都道府県サーバ，㋐と書いた部分，全国サーバ，㋑

と書いた部分，中野区のＣＳ，㋒と書いた部分，これ以外の部分に中野区民の個人情報が保管されている可能性はあるというふうにお考えですか。

前提を先に定義していただけないでしょうか。

本人確認情報という意味なのですが，それでは特定できますか。

いわゆる１４情報のことですかね。

そのことです。これからその意味で聞いていきますので，その前提でお答えください。そういった意味の本人確認情報というのが今指摘した部分に保管されているかどうかということについてはどうお考えですか。

基本的には，これで言う㋒の中ですね。中野区の情報は中野区のＣＳの中にあるというふうに認識しています。

今，中野区のＣＳとおっしゃいましたのでそれを例に聞いていきますが，実験市町村の側から中野区の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，まず第一に指定情報処理機関監視ファイアウォール，この図で㋓と記載された部分ですが，ここを越えてサーバに直接侵入するという方法が考えられますね。

考えにくいと思います。

理論的にあり得ないということですか。

いえ，あり得ないとは言いませんが，可能性はあると思いますが，そういう侵入はプロセスとしてほぼやらないと思います。

それから，もうひとつ考えられる方法として，実験市町村に置いてあるＣＳ端末，この図では㋑，㋐と記載された部分にあるものですが，この端末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ますか。

可能性はあると思います。

今説明した以外に，実験市町村の側から中野区のＣＳの本人確認情報に不正アクセスする方法というのは考えられるでしょうか。

直接的には難しいと思いますが，特定の条件を前提として持てば可能性はあると思います。

具体的にどのような方法が考えられるかを簡単に説明してください。

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。

丙第１７号証を示す

この最終報告の６ページの上から３行目部分を見ると，ＣＳの都道府県ネットワーク方向にあるファイアウォール，すなわち指定情報処理機関監視ファイアウォールから上流部分は実験対象とはしなかったということですか。

不正アクセス防止法に抵触する可能性があるので，そもそもドアのノックもしておりません。

そうすると，同じ意味になるのかもしれませんが，今回の実験においては，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というのは実験していないということになるのですね。

はい。

次に，ＣＳ端末の住基アプリを不正操作する方法についてお尋ねしますが，まず，今回の実験では，阿智村における２次調査の際に庁内ＬＡＮに攻撃端末を接続して，ＣＳ端末のＯＳの権限を取得したということですね。

はい。

ところで，住基アプリを起動するためには，ＣＳ端末のＯＳの権限に加えて，専用のカードと暗証番号が必要になるということですか。

まあそのように説明を受けています。

甲第２４号証の１を示す

これは，証人も出席されていた長野県の本人確認情報保護審議会の議事録ですが，１５ページの上から２０行目以下の阿部情報政策課長の発言部分で，証人に対して「アプリケーションを起動していないけれども，サンプルが見えたということで」と発言して，それに対して証人が「そのとおりです。」とお答えになっていますが，今回の実験では，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ことはなかったということでしょうか。

ここに書いてあるとおりですね。

この場でも確認したいのですが，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ことはなかったのですか。

操作者カードというものの扱いは行っておりません。

住基アプリを起動したかどうかということには端的には答えにくいということなんでしょうか。

住基アプリを起動したという記憶はありませんが，ＣＳ端末の管理者権限を奪取したと記憶しております。

甲第１２号証の２を示す

２５ページの下から１行目以下，信濃毎日新聞の小市記者と証人の応答の部分と，６ページの下から１３行目以下，証人の発言中の「先ほど，知事の方から」以下の部分を併せて見てください。これは，今回の実験の中間報告の際の知事会見の議事録なのですが，その中で証人は，住基アプリについて閲覧と検索はできるとか，カードと暗証番号が一致しなければ動作しないとなっているが，実際にはエクスプロイトで略奪したＣＳクライアントは自由に操作できるというふうに発言されていますね。

「検索と閲覧はできる？」ということに対して，「おっしゃるとおりです。検索と閲覧はできる。」と。「で，改変したものを外へ吐き出すことはできる。できるということはわかったということですね。」

・・・よく分からないんですが，できる可能性は確かに示しました。

そういう記憶があるということですね。

ええ，できる可能性はあるという記憶があります。

甲第３１号証の聴き取り報告書の２の３ページ以下の部分では，中野区以外の市町村にあるＣＳ端末の管理者権限を取得して遠隔操作することにより，中野区の住民のセンターサーバ，県のサーバなどにアクセスしたり，住民票の写しの広域交付を受ける危険性があるということが書いてあると思うのですが，そういう認識はあるでしょうか。

可能性は否定できないと思っています。

これは，住基アプリを起動してそのような操作を行うことができるという意味でしょうか。

住基アプリが起動する，しないという話ではないと思います。既に起動されていた状態のものを操作してそのような可能性があるということを示しています。

要するに，証人がここで存在する可能性があると述べている危険性というのは，中野区以外の市町村にあるＣＳ端末の管理者権限を取得して遠隔操作して，その遠隔操作の内容としては，住基アプリを操作して中野区の住民のセンターサーバなどにアクセスすることが可能になるというふうに考えているのではないですか。

そうではありません。そのように話を持っていきたい人が書いた文章だと思います。

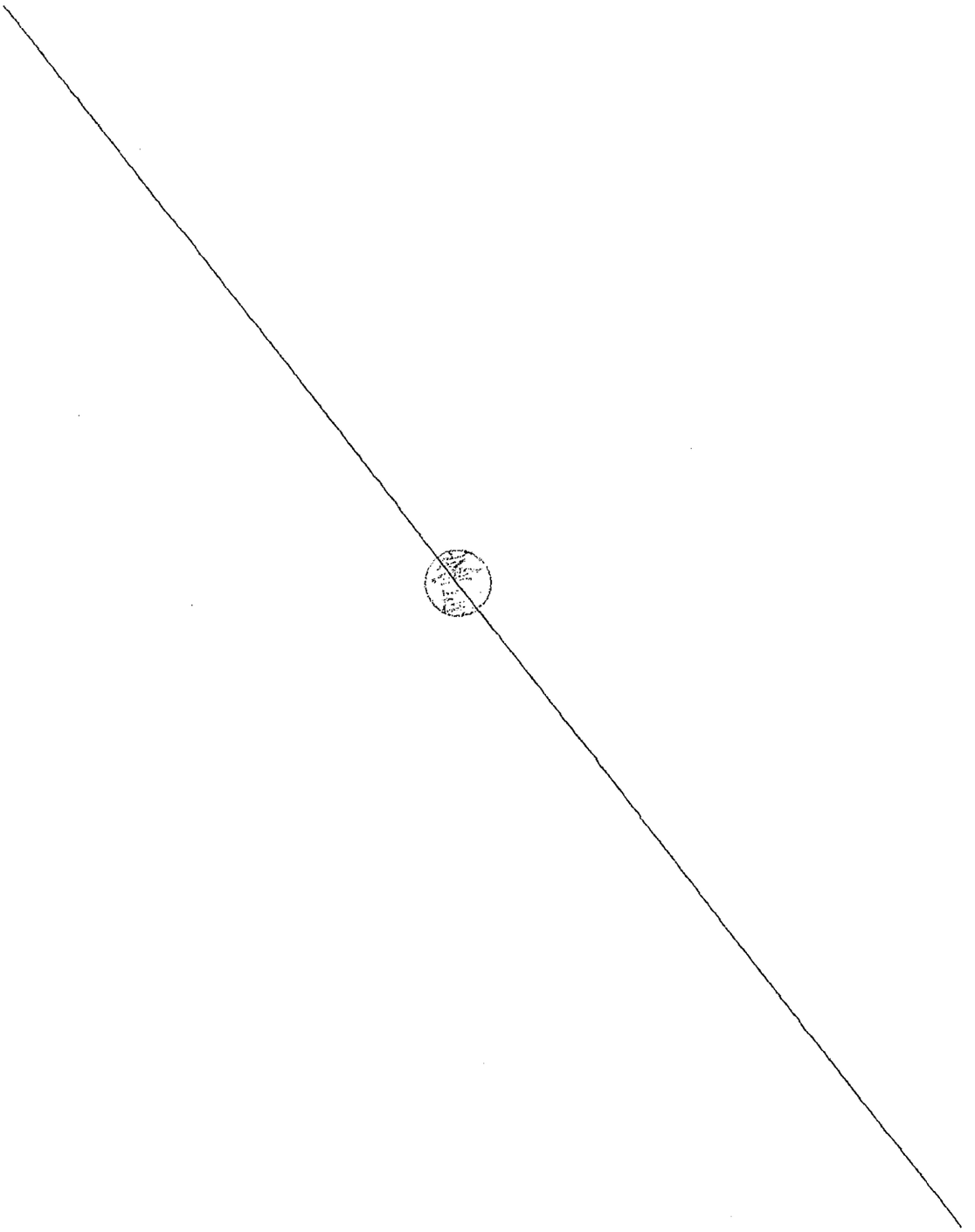
そうすると，具体的には，証人としてはどのような方法で実験した市町村から中野区のＣＳなどに侵入することが可能になるというふうに考えているんですか。

中野区のデータに直接侵入できるという発言をした記憶はありません。今おっしゃっているのは，住基アプリが起動していない状態で中野区などの

サーバに侵入することは難しいという意味になるんでしょうか。

そういった難しいとか難しくないという話をした覚えもありません。

（以上　峯 岸 佐 希 子）



それではもう一度確認させていただきたいんですけれども，証人のお考えでは，中野区以外の市町村にあるＣＳ端末の管理者の権限を取得して遠隔操作をすれば，まず，中野区の住民のセンターサーバなどにアクセスすることが可能だというふうにお考えなんですね。

実験市町村から中野区へのアクセスができるということを言っているんですかという質問ですか。

はい，そういう趣旨です。

そういったことは一切言っていません。

できるともできないとも言っていないということですか。

できる可能性があると言っています。

できる可能性があるとする根拠についてなんですが，具体的には実験市町村にあるＣＳ端末の住基アプリを操作して，そのようなアクセスが可能になるという意味なのでしょうか。

はい。住基アプリが起動したかどうかを争点にしたいように思いますので，細かい揚げ足取りの議論をするために来ているのではありませんので，はっきりお話ししたいと思いますが，操作者カードを使ってＣＳ端末を起動させている状態になっている，つまり前方一致だとか何だとかいう検索ができる前提が操作できる環境にある状態になっているＣＳ端末の管理者権限が，既に奪取されている場合は，遠隔よりＣＳの操作自体が百パーセントのぞき見できるようになると認識しています。画面がそのまま百パーセントのぞき見できる。のぞき見されていることを，操作している本人は全く気付かないということが可能だと思っています。その前提の中で，何がしかの状態により，操作者カードを付けたまま担当作業員が離席をしている間，この空白の間に，こちらから意図した操作を遠隔に行うことをすれば，自分のＣＳサーバの中にある情報以外の市町村の住民の情報を検索し，閲覧すること

は不可能ではないと思っております。

今述べられたような可能性の有無について，実験でどのようなことが分かったのかということを確認していきたいのですが，まず，実験の中で実際に今述べたような操作を行うことができるかどうかは確認されたのでしょうか。

できるはずだと認識しています。

裁　判　長

実験では，実際にそういうことが確認されたわけではないということですね。

ないです。

被告国，東京都，東京都中野区代理人（榮）

それから，先ほど述べたような方法で住基アプリを操作するためには，まずＣＳ端末のＯＳの権限を取得しなければならないんですか。

ほかにもやり方はあろうかと思いますけれども，まだそこまで追及はできていません。よって，ＣＳ端末の管理者権限奪取が今回の実験結果では前提となると認識しています。

それから，先ほど述べられたことの確認になるのだとは思いますが，今述べたような操作を行う前提としては，正規の操作者権限を有する職員が，カードを差し込んでパスワードを入力しているということが前提になるということですね。

今般の実験ではそのように認識しています。

それから次に，今述べられたような方法で不正に操作をしている間には，正規の職員が操作しているＣＳ端末の画面上のポインターなどは，不正操作者が攻撃端末から不正に操作したとおりに動くのでしょうか。

動くと認識しています。

このような不自然な動きをすれば，住基アプリを操作中の職員が容易に気付くのではないかと思うのですが，この点についてはどのようにお考えですか。

気付く可能性が何パーセントあるかというのを数値で出す方法があると

思います。

証人としては，先ほどの証言では，職員が席を離れた際などに侵入が考えられるということを述べられたのではないですか。

可能性の一つを上げました。

それから，職員が席から離れている間に侵入が可能だという御証言でしたけれども，職員が席から離れているかどうかということは，具体的にはどのような方法で確認するというふうにお考えですか。

離れているかどうかを判断するのではなくて，既に侵入している前提の後で，操作している間をのぞき見するという話をしています。よって前提が違います。かつ，離れているかどうかという判断はタイミングの問題です。操作しているから分かるかどうかというのは，やってみなければ分からないと思います。

それでは次に，インターネット経由で町内ＬＡＮのサーバの権限を取得することを試みたという部分についてお尋ねします。

丙第２９号証の３を示す

これは被告側で用意したファイアウォールの機能のイメージ図で，上段にある図Ａが正常な状態を，下段にある図Ｂが管理権限が取得された状態を表しています。図のＡに記載してあるように，ファイアウォールというものは一定のアクセスルールに従って通信を限定することによって，図のＡで言えば，①から⑤の通信のうち，②から⑤を制限することによって保護されたネットワークを構築する，そういうものと理解してよいでしょうか。

違うと思います。

それでは証人のお考えを説明してください。

意図したものだけを通過させるものであって，それ以外，開いていれば行けない，つまり全部ふさがっている中から必要なものだけを開けるものであって，幾つかあるというものをふさぐというものではない

と思います。

それでは次の質問に移るわけですが，その際，ファイアウォールが設置されている際，外部の端末からは，この図で言えば図のＡに言う①の通信による攻撃しかできないというふうに理解しているんですが，このような理解についてはどうでしょうか。

Ａの図に関しては①だけだと思います。

それでは次に図のＢのように，ファイアウォールの権限が不正に取得されて，アクセスルールが変更されてしまうと，禁止されていた通信，図で言えば②から⑤の通信も可能になって，ネットワークが想定外の通信による攻撃にさらされることになるというふうに理解しているのですが，この点についてはどうでしょうか。

ファイアウォールの管理者権限が取得された状態になれば，②番から⑤番が許されるのではなくて，自由に何番でも作れると，何番でも自由に通信させることができると認識しております。

丙第２９号証の２を示す

これを見ると，波田町の実験では図の①と書いてあるように，インターネット経由でファイアウォールを越えて公開サーバ，図面でいう㋒の部分を攻撃するという方法が実験されたということですか。

はい。

丙第１７号証を示す

１０ページの下から４行目ですが，これは最終報告の一部分なのですが，これを見ると，波田町の実験ではインターネットと町内ＬＡＮの間のファイアウォールに脆弱性は発見されなかったということですね。

ファイアウォールの脆弱性を発見されていないという話をしているのではありません。

それでは，何について脆弱性が発見されなかったということが述べられてい

るんでしょうか。

ＤＭＺ上にある公開サーバの管理者権限が奪取できませんでしたと言っています。

ファイアウォールのほうに脆弱性があるかどうかということは確認されたのでしょうか。

確認していません。

そうすると，先ほど確認したような意味において説明するとすれば，波田町の実験のほうでは，ファイアウォールが本来許可している通信によってのみ公開サーバを攻撃することが可能であったということになるのではないですか。

そのとおりです。

先ほど確認した通信の制御という意味においては，ファイアウォールはその役割を果たしていたということになるのではないかと思うのですが，この点についてはどうお考えでしょうか。

ファイアウォールは午前中からも述べているとおり，意図した通信だけを許可するものでありますから，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。

丙第２９号証の４を示す

これは被告側で用意したＤＭＺの機能のイメージ図ですが，波田町の公開サーバはＤＭＺに置かれているということですので，仮に公開サーバの権限を取得したとしても町内ＬＡＮのサーバの権限を取得するためには，それを踏み台にして，更にもう一段ファイアウォールを通過する必要があるのではないですか。

この絵はそのように理解したいがための絵に過ぎません。つまり，Ｄ

ＭＺ上にあるサーバと町内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を踏み台にして町内ネットワークに侵入するという手だて，これはごくごくベーシックなやりかたで，インターネットを少し検索すれば，たくさんやり方の手法が載っております。

今回の実験の内容ということで確認させていただきたいのですが，今回の実験において，ＤＭＺと町内ＬＡＮの間の通信がどのように制御されているかということは確認されたのですか。

確認しました。

それはどのようになっていましたか。

ＤＭＺ上からは町内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。

次の質問に移ります。町内ＬＡＮに接続した攻撃端末から市町村設置ファイアウォール越しにＣＳの権限を取得する方法について確認します。

丙第２９号証の２を示す

この図の②と書いてある部分に記載してあるとおり，町内ＬＡＮに接続した攻撃端末からＣＳの権限を取得しようとした場合には，市町村設置ファイアウォール，図で言う㋑の部分を突破しなければいけないのですね。

突破というか，既に許されている通信のコード番号を使って内側に攻撃を試みます。

今回の実験の中で，下諏訪町の調査においては，市町村設置ファイアウォールに脆弱性は発見されず，ＣＳの権限を取得することはできませんでしたね。

はい。

阿智村の調査においてはファイアウォール自体の脆弱性は発見されなかったのだけれども，管理用ポートが町内ＬＡＮ側に向けて開いていることが分かったということですか。

はい。一つ追加したいんですけれども，下諏訪町の実験においては，下諏訪町のサーバの管理を委託されている業者が，遠隔で監視，管理をされておられました。よって，その業務に影響を与えない範囲という限定で作業を行いましたので，十分な時間がなく，作業を限定せざるを得なかったと認識しております。よって，時間が十分にあれば，いろいろな可能性は十分発見できたのではないかと思っております。

次に阿智村の調査について聞いていきますが，管理用ポートが開いていたということについてなんですが，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たのですか。

できていません。可能性があると示しました。

甲第３２号証の１を示す

１７ページの下から７行目以下を示しますが，この報告書の記載を見ると，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ファイアウォールに送ることを試みた，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が，全く同じ動作をしたが，その意味を確定できなかったというふうに記載されていますが，これは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できるということが確認できなかったということになるのですか。

すみません，もう一度お願いします。

ここに書いている内容は読まれましたか。

はい。

ここに書いている内容の意味を確認したいのですが，ここに書いてある内容を前提にすると，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

取得することは，実際にはできなかったという意味になるのかと思ったのですが，この点についてはどうなのでしょうか。

はい。時間切れでできなかったというのが事実です。

甲第３２号証の３を示す

２段落目，Ｃ言語においてという以下の部分と，３段落目の上から２行目，しかし，市町村調達ファイアウォールの設定と書いてある部分から下を示しますが，この部分では，しかし町村調達ファイアウォールの設定などにより，受動的攻撃を実施するとともに，バックドアを設置することが可能でしたというふうに書かれているのですが，これは具体的には，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，これを突いた攻撃が可能であるということを述べたものですか。

可能性があるということを提示しました。

ただ，今回，実際に実験の中で行った内容としては，危険な関数の存在を突いた攻撃を実際にするということはなかったのですね。

実際にはしていません。

それから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のでしょうか。

はい。

それはどのような方法で確認したのですか。

リアセンブルですね。

内容をもう少し確認させていただきますが，何についてリアセンブルを実施したのですか。

プログラムの中に入っている情報ですね。いわゆるもっと具体的に言うと，ドットＤＬＬと呼ばれているものの幾つかをサンプル取得して，

その中を逆解析した形で，中にどのような関数が使われているかという事実を究明するという作業を実施者が行いました。

プログラムをリアセンブルしたと言いますが，そのプログラムはどのコンピュータに入っている，どのプログラムということになるのですか。

ＣＳ側に入っているプログラムであります。

それは報告書のどこかに記載がありますか。

いいえ，口頭で説明してあります。

実験の核心にかかわる極めて重要な部分ではないかと思いますが，なぜそのことを記載されなかったのでしょうか。

可能性を説明したに過ぎません。

リアセンブルは実際に実施したことではないのですか。

アセンブルしなければ可能性を提示できません。

実際にＣＳ内のプログラムについて，リアセンブルを実施したということを報告書に記載されましたか。

していません。

それは実際にやったことなので，可能性ではありませんから，記載するのが普通ではないかと思うんですが，なぜ記載されなかったのですか。

リアセンブルということをどこかに書いてないですかね・・・。甲第３２号証の３の１段落目の下から２行目，アセンブラーを使用し，アプリケーションがどのような構造になっているかの調査を実施しましたと書いてあります。

ここでそのことを記載したと，そういう御証言ですね。

はい。

既存住基のサーバ側にあるプログラムについては，リアセンブルは実施されたのですか。

していません。

甲第３２号証の３を示す

２段落目の３行目以下を示しますが，ここに記載してある内容を読むと，既存の住基アプリの中にあるプログラムについて，リアセンブルを実施して，その結果からＣＳ内にある住基アプリに危険な関数が使用されていることを推測したというような内容になっていると思うんですが，今述べたような理解で記載されたものと理解してよいでしょうか。

先ほど，４０号証の１枚ものを配布させていただきましたけれども，それの絵のとおりであります。

甲第４０号証を示す

これを見ながらその内容を説明してください。

１から３に書いてあるとおりですね。ＣＳ側からあるトリガーで既存住基サーバに情報を取りに来る，取りに来たときに既存住基サーバ側は既に管理者権限を奪取している前提になっていて，そこでＣＳがアクションを起こして既存住基側に情報を取りに来たときに，管理者権限を奪取するためのプログラムをつかませれば，ＣＳ側がバッファオーバーフローを起こす可能性があるということを提示しました。

甲第３２号証の２を示す

８ページの上から５行目，「但し」から後の部分を見ると，既存住基サーバにて稼働しているポートを使用するアプリケーションでは，数多くの関数が使用されていることが今回の調査にて分かりましたということですが，これは既存住基サーバ内にあるプログラムについて，リアセンブルを実施して，関数の使用されていることを確認したという趣旨ではないのですか。

いいえ，違います。既存住基サーバの話はしていません。

ちょっと消してある部分もあって文脈が読み取りにくいんですが，ここに書いてある意味を説明してください。

既存住基サーバ側にもＣＳサーバ側にも脆弱性があるであろうプログ

ラムが動いていると。その中で，ＣＳ側からのアクションによって既存住基サーバ側に問題のあるプログラムをつかませれば，ＣＳ側がバッファオーバーフローを起こすという可能性を示しています。

今確認したい内容は，ＣＳあるいは既存住基サーバの中にあるプログラムに危険な関数というものが使用されているかどうかということを，実際にどのような手順で確認したかということなのですが，具体的な方法としては，プログラムをリアセンブルして，その内容を解析したということなのですね。

それで正しいと思います。

どのプログラムについてリアセンブルをしたかということなんですが，ＣＳ内にある住基アプリの内容をリアセンブルしたということですか。

すみません，正確に記憶ありません。

複数のプログラムについてリアセンブルしたという記憶はあるんですか。

すみません，記録からしか記憶がたどれません。実施したのが私ではないので覚えていません。

実際に実施したのは笠原氏ですか。

かつ，もう１名の作業者であります。

証人自身はその場に立ち会わなかったんですか。

立ち会っておりますが，どれかまで今すぐ思い出せません。

実際にリアセンブルをした者から報告とか説明を受けてないんですか。

受けました。

その内容は今覚えてないということなんですか。

詳細な正確な記憶がありません。

そうすると，証人自身では，どちらのプログラムについてリアセンしたかは，今分からないということですか。

それは先ほど述べたようにＣＳ側のお話です。

結論としては分かってるということなんですか。

そうです。

もう一度説明してもらいたいんですが，実際にどういう作業をしたのかは，はっきり説明できないということなんですね。

詳細な記憶が今ないからできません。資料が手元にあればお話しできると思います。

結論として，ＣＳの住基アプリの中で危険な関数を使っていることが確認できたというのであれば，必ずＣＳ内の住基アプリについて，リアセンブルを実施してるということにはならないんですか。

なるという根拠はどういったものでしょうか。

直接，関数を使用されているということを確認されたという御証言でしたから，直接，確認した方法としては，リアセンブルをしたということ以外には考えられないと思いますので，そのＣＳ内の住基アプリについて，実際にリアセンブルを実施されたのではないですかというふうに確認してるのです。

先ほど申しましたＤＬＬをアセンブルしたというお話をしたとおりだと思っています。

そのＤＬＬというファイルですか，プログラムがＣＳ側に作成されているものをリアセンブルしたのか，既存住基サーバ側にあるものをリアセンブルしたのか，それがどちらであるかは分からないのですか。

いえ，何度も言ってるように，ＣＳ側です。

裁　判　長

そうすると，既存住基サーバ側にはやってないということでよろしいわけですね。

既存住基側のリアセンブルしたという記憶はありません。証拠があれば記録から詳細なお話をすることができると思います。

ＣＳ側についてはそれが記憶があると。

記憶があります。明確に覚えています。

被告国，東京都，東京都中野区代理人（榮）

それでは次の質問に移ります。これは被告側でこのたび確認したところによると，そもそもＣＳの住基アプリにおいては，既存住基から与えられたデータを扱う際に，そうした関数を使用している事実はないということなのですが，証人はこの点。

原告代理人（渡辺）

異議があります。調べたというのは何か証拠出てるんですか。

裁　判　長

出てないとそれが前提になって誤導になってはいけないと思うので。

被告国，東京都，東京都中野区代理人（榮）

それでは質問の仕方を変えさせていただきます。再確認になるのかもしれないのですが，ＣＳの住基アプリにおいて，そうした危険な関数を使っているというのは，現に自分の目で確認されたのですね。

結果を報告受けました。レポートをもらいました。それで認識しています。

丙第２０号証を示す

３ページの上から４行目以下を示しますが，これは最終報告に対する総務省のコメントですが，ここに記載してあるように，総務省の側では関数のチェックを実施し，脆弱性が存在しないことを確認したと公表しているのですが，先ほどの証人の御証言からすると，このコメントは事実ではないというふうにお考えということでしょうか。

実験した時点において可能性を提示したものでありますから，総務省が言っているから安全だということなのであれば，その根拠を提示する必要があろうかと思います。

もう一度質問しなおしますが，今確認したいのは，危険な関数を実際に使用しているかどうかということについて，どういう認識をされているかという

ことなのですが，総務省の側ではそういった関数のチェックを実施し，脆弱性が存在しないことを確認したと述べているのですが，こういう事実認識は誤りであるというふうにお考えですか。

誤りであると１回も言った覚えはありません。私がチェックした内容で，危険な可能性がある関数が使われていましたねと報告したまでにすぎません。

今回の実験の結果から使用が推測されるということを，今まで述べていたにすぎないという，そういう説明になるんでしょうか。

危険な脆弱点の可能性を依頼者に提示をする，それを依頼者が読み取って対策を御検討される，その材料を提供したのが私が仕事としてさせていただいた脆弱性の検査レポートであります。

次にＣＳのＯＳの管理者権限が奪取される具体的危険性について質問します。

丙第２９号証の２を示す

ＣＳを攻撃してＯＳの権限を取得するということは，この図では④と書いてある部分を攻撃することになるのではないかと思うんですが，このような攻撃は阿智村の２次実験において試みられたということですね。

はい。

この実験は重要機能室の中に入って実施したのですね。

はい。

阿智村の重要機能室は通常は施錠して管理がされているのではないですか。

質問の意図が，多分，重要機能室には通常鍵がかかっているので，施錠された中に入って作業を行うことは通常起こり得ないことなので，無効なんだということを主張されたいんだと思いますが，私がやった作業というのは，この阿智村や長野県の３市町村に限らず，いろんなところでやらしていただきましたが，依頼主さんがここでやってくださいと言われればそこでやります，ここでやってくださいと。

裁　判　長

分かりました。今のこちらの質問の意図はともかくとして，通常は施錠されている場所でしたかという部分についてはお答えはどうでしょうか。

はい，施錠されてある場所でした。

被告国，東京都，東京都中野区代理人（榮）

同様の質問ですが，この実験の際には，通常は施錠されているラックのかぎを開けて，その中のハブに調査用のパソコンを接続したということですね。

はい。

このような方法でやった実験の意味について確認したいのですが，内容としては，市町村設置ファイアウォール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というふうに理解していいでしょうか。

そうですね。ハブの中に接続をさせていただいた，そういうふうに記憶しております。

今回の実験では，今言った阿智村の２次実験のことですが，この実験の際にはＣＳセグメントに直接攻撃端末を接続する以外の方法では，ＣＳの権限を奪取するということは試みられていないということになるのでしょうか。

ちょっとログを見ないとはっきり思い出せないのですが，コミュニケーションセンターという隣の部屋と言いますか，ちょっと離れた部屋からは接続できる状態で，そこからＣＳに向いてのアタックをやったかどうか，ちょっと記憶があいまいですが。

結果のほうを確認したいのですが，実際に市町村設置ファイアウォールを通過して，ＣＳの管理者権限を取得することはできなかったということでしょうか。

はい，していません。

次に，ＣＳ端末のＯＳの管理者権限が奪取される具体的危険性の有無につい

てお尋ねします。

丙第２９号証の２を示す

ＣＳ端末を攻撃してＯＳの権限を取得するということは，この図で言えば⑤と書いてある部分を攻撃することになるのではないかと思うんですが，今回の実験においては阿智村の２次実験の際に，このような攻撃が試みられたが，結論としてはＣＳ端末にはパッチが適切に適用されていたということになるのでしょうか。

はい，そうですね。

甲第１２号証の１の添付図４ページを示す

これは中間報告の添付図ですが，これを見ると，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ーフローによる管理者権限の取得に成功したというふうに記載してありますね。

はい，そうですね，これは。

これはＣＳ端末について，バッファオーバーフローによる管理者権限取得に成功したという内容なのですが，実際の実験の経過には合わないのではないですか。

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。

この図表自体は証人が作成されたものでしょうか。

いえ，これは長野県さんのほうで作られた絵であります。

この図表を証人が発表前にチェックしたという記憶はありますか。

前夜に見た記憶があります。

ただ，誤りを見付けることができなかったということなんですね。

そうです。

それから，ＣＳ端末のＯＳの管理者権限については，実際にはＣＳから得た

情報を利用した，すなわちＣＳのＩＤとパスワードを入れてみたところ，ＣＳ端末のものが同じだったので管理者権限を取得することができたということなんでしょうか。

もうちょっと正確に記憶しているのは，ＣＳの中にあるユーザー情報の中に，幾つかのＩＤとパスワードが書かれていて，それを順番にＩＤとパスワードを入れていけば，ＣＳの管理者権限が取得できたということを記憶しております。

そうすると，仮に，このような設定ではなくて，強固なＩＤ，パスワードが設定されているとすれば，ＣＳ端末のＯＳの権限を取得することにも困難があったということにはならないんですか。

まあ，その時点のパッチ対策がどこまでできていたかということになろうかと思いますが，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んだろうと思います。

甲第４０号証を示す

甲４０号証では受動態攻撃，受動的攻撃とも言うようですが，その可能性について説明されているようですが，今回の実験において，実際に受動的攻撃というものが実施されたということはないのですね。

ないです。可能性を提示したということです。

それでは，その可能性，実際にそのような攻撃が成功する条件について確認させていただきます。まず，第一の条件として，ＣＳの，この例では生年月日の問題ですから，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，脆弱性がある必要がありますね。

はい。

それから，２番目の条件として，ＣＳの側から既存の住基サーバに向けて何らかの通信がなされている，そういう必要性がありますね。

はい。

それから３番目の条件として，既存住基の側のＯＳの権限を取得している必要がありますね。

はい。

次に，これらの条件を満たして受動的攻撃がなされた後のことを聞きたいのですが，遠隔操作が可能になるということを書かれているのですが，具体的にはＶＮＣをインストールして，それによって遠隔操作が可能になるという意味でしょうか。

ＶＮＣだけではないと思います。

典型例の一つとしてＶＮＣのインストールということはお考えになっているのでしょうか。

そうですね。分かりやすいというふうに思っております。

仮にＶＣＮ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があるのではないですか。

ファイアウォールの設定変更や無効化は必要ありません。

特に技術的な支障はないというふうにお考えということですか。

恐らくできるんだろうと思っております。

（　以上　　稲　村　嘉　子　）

先ほど出た危険な関数の話，もう若干確認させていただきたいんですが，証人の御理解では，ＣＳ内の住基アプリについてディスアセンブリをして，で，危険な関数が使用されていることを確認したんだと，こういう御理解なんですか。

はい。そのように理解しております。

甲第３２号証の２を示す

１５ページを示します。この真ん中の「脆弱性に関して」という部分を見ていただきたいのですが，これ，既存住基サーバについて実験の結果を説明した部分だと思うのですが，「port■番を使用しているアプリケーションをＩＤＡproというdisassemblerを用いることでdisassembleを実施致しました。」というふうに書いてあるんですが，これは既存住基サーバのほうのプログラムについてディスアセンブリを実施したという意味ではないんですか。

すみません，記憶にありませんが。関数として，既存住基のサーバとＣＳが同じ関数を使って通信しているんだろうというふうに記憶しております。

確認した内容は，どのパソコンのどのプログラムにどのような作業を行ったのかということなのですが。ここに書いてある内容を見ると，既存住基サーバの中にあるプログラムについて，ディスアセンブリを実施したように読めるんですが，そうではないのですか。

すみません，そこの記憶については，記録を正確に読み直してお答えしたいと思います。

で，下の段落を見ますと，末尾３行目ですが，「同じようなfunctionがＣＳから既存住基サーバに接続しにくるクライアントにも実装されていれば，受動的攻撃を既存住基サーバ経由で実行出来る可能性が非常に高いといえる。」と書いてあって，この記載を見ると，ＣＳ内の住基アプリについては，ディスアセンブリを実施していないようにも読めるのですが，この点につい

てはどうなのでしょうか。

すみません，ちょっと記憶が定かでないので正確にお答えできません。

申し訳ないです。

それから，仮に危険な関数を使用していた場合の対策について確認したいのですが，こういった関数を使用している場合であっても，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のではないかと思うのですが，この点についてはどうでしょうか。

そのときは起きないと思います。

裁　判　長

今の関数の部分ですけれど，どの部分についてディスアセンブラをかけたかというのを，記憶を喚起して明らかにしておいていただいたほうがよいのでしたら次回までにそれをお願いするようにしたいと思いますが。

被告国，東京都，東京都中野区代理人（榮）

そのようにお願いいたします。

裁　判　長

じゃあ，その部分は記憶をもし喚起できるようであれば明らかにしていただくと。客観的なことだと思いますので，よろしくお願いします。

はい。

被告国，東京都，東京都中野区代理人（榮）

それでは，次の質問に移ります。

甲第１３号証を示す

１０ページ，１１ページを示します。大体この部分においては，県設置ファイアウォールから市町村側ではＬＡＳＤＥＣは不正侵入を検知できず，サーバやファイアウォールについて生き死に程度の監視しか行っていないということが書いてあるんですが，証人の認識もこれと同じですか。

はい。

で，ここで言っているファイアウォールというのがどこのファイアウォールのことなのかということなのですが，市町村設置ファイアウォールのことを指していらっしゃるんでしょうか。

・・・・。

質問の仕方がわかりにくかったかもしれないので，もう一度質問しますが，証人が生き死に程度の監視しかしていないというサーバやファイアウォールのファイアウォールというのは，市町村設置ファイアウォールのことを指しているのでしょうか。

県調達側のファイアウォールですね。

で，具体的に県調達ファイアウォール，指定情報処理機関監視ファイアウォールと言いますが，それを含めた県サーバの側において，ＬＡＳＤＥＣがどのような監視を行っているかということは御存じですか。

詳細な情報は知りません。

丙第２９号証の６を示す

これはＬＡＳＤＥＣの監視範囲についての被告側の主張をまとめたものなのですが，ここに書いてあるように，ＬＡＳＤＥＣはＣＳの監視はしているのですが市町村設置ファイアウォールについては監視をしていないと。また，指定情報処理機関監視ファイアウォールからネットワーク側については２４時間の即時監視を行っていると，こういう認識なのですが，証人の理解はこれとは異なるものでしょうか。

いいえ。境界を含めて，こういう形だろうと認識しています。

その図を見ると，県調達ファイアウォールと言われる部分は２４時間の監視を行っている領域に入っているのですが，２４時間で生き死にのみの監視を行っているという理解なのですか。

そう思っています。

それから，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側の線を外したところ，ＬＡＳＤＥＣから確認があったということを述べていらっしゃいましたね。

はい。

丙第２９号証の８を示す

外した箇所は，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側の線ということで間違いないですか。

①番ですね。

丙第２９号証の７を示す

これは指定情報処理機関の監視室で検出したアラームのログなのですが，このうち①の黄色の部分がケーブルが抜かれたことを，赤の部分がケーブルが差し込まれたことを示していて，合計５回検知をしているということになるのですが，これを見ると実際に線が外されたのは指定情報処理機関ファイアウォールとルータの間の線，丙第２９号証の８の図面で言うと②の線を外しているのではないかと思うのですが，この点についてはどうですか。

はい。国はやっぱりこの程度のレベルでしか監視ができないんだというように思います。いまだにこのレベルでしかわかってないんだと。これは①番に相違ありません。で，このログがそうであるという根拠を出してください。この②番ということであれば，私がＬＡＳＤＥＣ側を切ったということになるので，前提項として不正アクセス防止法に抵触するということを言われたいんでしょうか。

裁　判　長

決して，吉田さんがなさったことについて攻撃しようとか何とかという意図は全くありませんので。客観的な事実をただ伺いたいだけですので，そのへんは安心してお答えいただいたらどうでしょう。

であれば，絵で示す①番が抜いたところであります。で，それを記録

としてこの②番なんだという根拠があるんであれば，このログ以外にですね，改ざんされていないという記録を提示していただく必要があると思います。

被告国，東京都，東京都中野区代理人（榮）

丙第２９号証の６を示す

これは被告側の認識を図で示したものではあるんですが，この図によりますと，指定情報処理機関監視ファイアウォールから内側については２４時間の監視を行っていて，ＣＳについては１５分に１回程度の定期監視というのを行っているという，こういう説明なのですが，こういった説明内容自体について何か意見はお持ちですか。

いいえ，ありません。

で，先ほど見ていただいた丙第２９号証の７のログを見ると秒単位で検出がされているので，２４時間監視を行っている部分の線を外したということになるのではないかと思うんですが，こういった見解についてはどういうお考えをお持ちでしょうか。

ここまでしか記録が取れていないんだと思います。

で，１５分置きの定期監視をしてる部分の線を外したときにこのようなログが取れるかどうかということについては，どうでしょうか。

いえ，このログがうそだという話ではなくて，②番ではなく①番でしたよということを言っています。

裁　判　長

今聞かれているのは，①番だとすると１５分置きにしか検知しないはずなので，こういう秒単位のログが出てこないと思うんだがどうだろうかという質問を受けているんですが。

それは私はわかりません。

被告国，東京都，東京都中野区代理人（榮）

次の質問に移ります。証人は，既存住基も住基ネットに含まれるという考え方を述べていらっしゃいますが，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って，既存住基の情報を書き換えればＣＳも書き換わるのだと，そういうことを述べていらっしゃいますね。

はい。

今回の実験において，既存住基とＣＳが同期を取っているということを確認されたのでしょうか。

はい。

どの市町村に対する実験で確認されましたか。

阿智村と記憶しています。

で，最終報告あるいは調査報告書などに，そういった成果があったということは記載されていますか。

ちょっと見ないとわかりませんけれども，長野の審議会の中でそういった発言をした記憶があります。

具体的に，どのような作業をして同期を取ったということを確認されたという御記憶ですか。

同期を取ったというか，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。

で，そういった作業をされたということは報告書の中には記載されてないのですか。

全部見ないとわかりませんけれども，書いてないやも知れません。

それから，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ましたが，実験後にその主張を変更して，責任の限定を図っているという，そういう趣旨のことを述べられていますね。

はい。

当初の見解が変更されたというのは，いつ，どこでというふうに認識されていますか。

古い記憶になりますけれども，どこかに記録が残っていると思います。一番最初はいつでしたですかね。総務省の若松副大臣室に櫻井よしこさんと一緒にお邪魔したときに，どこまでなんですかというお話を聞いて，非常に玉虫色の話があったと記憶してます。で，その後，昨年ですか，総務省さんと公開討論会ということを行って，住基ネットというものはどこまでの範囲なんですかということを公開討論会で議論した記憶があります。で，そのときには非常にあいまいな話であってですね，市町村のネットワークは住基ネットではないやに取れる話があったように記憶してますけれども，それもはっきりした境界線を提示するという結論に至っていなかったと記憶しています。

丙第２５号証を示す

１６ページを示します。証人が今指摘されたやり取りというのは，このやり取りのことを指しているのでしょうか。

はい，そうですね。

次に，実験で発見されたとされている庁内ＬＡＮの脆弱性について確認します。まず，庁舎外から庁内ＬＡＮに侵入される危険性があったのかという点についてなのですが，波田町の実験以外の実験については，役場の許可を得て，役場の庁舎内に立ち入った上で実験が行われたということですね。

はい。

で，波田町の実験では庁舎に立ち入らずに実験がなされたということなので

すが，その結果としては，外部に公開されているサーバ群に脆弱性は発見されなかったということなのでしょうか。

はい。

今回の実験の評価として，そうすると，庁舎外から庁内ＬＡＮに侵入される危険性が実証されたかどうかという点については，どうお考えなのでしょうか。

今回の実験の中では，脆弱性を突くという形には至りませんでした。もっと長い時間ともっとたくさんの自治体を選ばせていただける形で準備が整ってあれば，奪取できるところがあったんだろうというふうに思っています。

で，結果について説明されている中で，ダイヤルアップを用いた侵入の可能性について言及されている部分があるので，その点について確認しますが，ダイヤルアップを用いた実験というのは，今回の実験では実施されたのでしょうか。

はい。

どの実験で実施されたという記憶ですか。

阿智村において特定の出先機関に足を運びました。そちらからです。

甲第１３号証を示す

７ページ，１０行目以下を示します。この部分で，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に接続をしたと記載されているのだと思うのですが，まず，これは役場の許可を得て，職員の案内によってその場所に立ち入って接続を行ったということですね。

はい。

こういった方法による接続について，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に接続することができるということもおっしゃってるようなんですが，こういった

ことは可能であるとお考えですか。

可能であると思います。

例えば発信者番号の認証が必要とされている場合には，そのような特定の番号からでなければ接続できないのではないですか。

発信者番号を偽装するプログラムはインターネット上に無償で転がっております。

で，これは非常に容易なことであるというふうにお考えなのですか。

はい。

甲第１２号証の２を示す

８ページの５行目以下を示します。中間報告のこの部分では，極論ですけれども，ダイヤルアップでＩＳＤＮの番号を偽装することができればということを述べられていて，難しいことを証人自身が前提とされているようにも読めるのですが，その点についてはどうでしょうか。

難しいからできないということではなくて，極めて高い可能性でできるものである，そう思っています。

で，今回，実際に実験を行った阿智村では，発信者番号の認証が必要とされているかどうかということは確認されましたか。

確認しておりません。

次に無線ＬＡＮを経由した侵入について確認させていただきます。実験においては，無線ＬＡＮを経由して侵入ができることが確認できたということですか。

そのような話は，した記憶がありません。

無線ＬＡＮを経由して侵入できるかどうかについて説明していないということですか。

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ります。

で，実際の実験において，無線ＬＡＮ環境を構築して，その無線ＬＡＮ環境から接続を試みるということはしたのでしょうか。

下諏訪町において，そのような環境を構築していただいて，行いました。

それから，隣接施設から侵入するということについて確認しますが，これは阿智村の１次実験においてそのようなことが試みられたということですね。

隣接する場所ですね。はい。

一応の確認なのですが，隣接施設も庁舎の一部を利用したということですね。

建物は違う，隣の建物でした。

隣の建物だということですか。

庁舎と違う，隣の建物でした。

コミュニケーションセンターという場所であったのではないかと思うんですが。

はい。

どういう管理がされている場所かということは確認されましたか。

はい。村民の皆さんが，いつでも夜１０時までは自由に出入りしていいという場所にありました。

出入りできる場所というのは，具体的には会議室ですか。

会議室のようなフロアスペースになっていました。

その会議室のような部屋にも，夜１０時までだれでも立ち入れるということは確認していますか。

はい。

で，使用されていないときに施錠されているかどうかということは確認されましたか。

施錠はされていませんでした。

それから，阿智村，下諏訪町の実験で判明した脆弱性として，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ようなところが多数あったというようなことを述べていらっしゃるようなんですが，そのような事実は，実際に実験の際に確認されたのですか。

はい。実験の２箇所で目の当たりにしたというのもございますが，長野県の審議委員として自治体さんを回らしていただいたときに目で見たというのもございます。

証人が長野県に提出した調査報告書には特にそういった記載は見当たらないのですが，これはあえて記載されなかったということなのですか。

はい。長野県の審議会の議事録の中に記録が残っていると記憶しております。

それから，阿智村，下諏訪町の実験の際に確認できたこととして，カードの管理も特に厳しくなかったというようなことが聴き取り書には書いてあるんですが，証人もそのような認識でしょうか。

はい。

で，これは実際に実験の際に何らかの方法で確認をしたということですか。

何らかの方法というよりは，こんにちはと入っていって，カードというのはどこにあるんですか，'ああここだね，という形でコミュニケーションを取ってお話をして，このようになってます，ここにあります，というようなやり取りをした記憶がございます。

担当の職員の方から口頭で確認したというふうに理解してよいのでしょうか。

一緒に庁舎内を歩かせていただいてお話をした，そう記憶しております。

それから，最終報告の中では今回の調査についてはシステムに支障が生じないよう留意しつつ行われたというふうに記載されているのですが，実験中あるいはその直後にシステムに支障が生じるということはありませんでしたか。

一部，ございました。

下諏訪町の実験でのことということでしょうか。

はい。

その障害が発生した理由として，構成的に通常（常識として）冗長化されていることを前提に実施したためにそういった障害が生じてしまったというふうに書いてあるんですが，これは間違いないでしょうか。

結果はそうですが，非常に短い時間の中で何とかファイアウォールを越えたという事実をつかみたいという依頼者の強い依頼により，実施者が結論を急いだという形が事実だと記憶しています。

実験を実施する前に，システム確認をするようなことはなかったのですか。

はい。ざっくりと説明をいただきました。しかしながら，すべてのネットワーク構成図を御提供いただくには至りませんでした。

そういった一定の内容のネットワーク図をいただいた上で実験を実施した，ということではあるのですね。

はい。

それから，聴き取り書の中には，住基ネット上の個人情報が改ざんされたら，それを証明することは不可能に近いというようなことが書いてあるのですが，これは証人自身のご意見なのでしょうか。

そう思っております。

具体的にどのような点で証明が困難になるというふうにお考えなのか，説明できますでしょうか。

データそのもののハッシュ値で，ＭＤ５のような厳格にこのデータは改ざんされていないということを担保できるようなデータのトレーサビリティーというものができない状態の住基ネットワークシステムは，その改ざんが正であるか偽であるのかを判定できないようなものであるというふうに認識しております。

今おっしゃってるのは，パソコンのネットワーク上で確認することが困難になるということをおっしゃっているのでしょうか。

現実に新聞報道でもありましたけれども，鹿児島でしたですか，生きていらっしゃる方が死亡したことになっていたというのがございました。住基ネットワークでは，間違ってやってしまったことをそのまま正しいというふうに履行してデータが格納されてしまうという事実が新聞報道で明らかになっているんだと記憶しております。

甲第１２号証の２を示す

１６ページを示します。これは中間報告の知事会見の際の記録なのですが，その中で証人は，税金の滞納状況等が，その住民が転出すると住基ネットを流れるという趣旨のことを述べられているように見えるのですが，これはそういう趣旨で発言をされたのでしょうか。

わかりやすく説明をしたつもりでありますが。このような情報がＣＳの中にあるというふうには認識していません。

そういった情報がＣＳの中にあるかどうか，で，住基ネットの中を流れているかどうかは実際には確認されていないということですね。

はい。

被告国，東京都，東京都中野区代理人（池原）

先ほど阿智村の隣接施設からの実験についてお話しいただきましたけれども，その点について若干確認させていただきたいと思います。これは，阿智村の役場の隣の建物の中にある会議室らしき部屋，そこに調査用のパソコンを置いて実験をされたというふうに伺ってよろしいですか。

はい。

その部屋には，阿智村の職員の案内で立ち入られたわけですか。

はい。

その際には，その部屋には，当然，施錠はされていませんよね。

はい。

それ以外のときに，この会議室に施錠がされているかということは確認されましたか。

確認はしていませんでしたが，私たちが実験している途中で村民の方がお越しになられて，ソフトボールだったか野球の表彰とかをしたいからちょっとこの部屋を貸して，ということでわあって入ってこられましたので，隣の小さな部屋に移った記憶がございます。つまり，村民の方であれば，あらかじめ使うよということで自由に使えるんだなというふうに認識を持ちました。

実験中は施錠せずに実験をされてたわけですね。

そうです。

それ以外のときに施錠がされているかどうかは確認されていないわけですね。

していません。

被告財団法人地方自治情報センター代理人（小倉）

証人は，今回の実験をするにあたって，今何をするのかと，で，その結果がどうなったのかということを写真又はビデオ等で記録を取るようなことはしていましたか。

一部，長野県さんのほうで記録を取られていたと記憶しています。

一部というのは，どの実験のときですか。

１次実験のときに，下諏訪町と阿智村，それから波田町の実験をやった東京のときも，担当者の方が来られてビデオを回されていた記憶があります。

あと，アクセスログの関係ですが，証人が保有されていたアクセスログというのは，攻撃用端末として利用したコンピュータに記録されているアクセスログだけでしょうか，それとも，それ以外のコンピュータに記録されているアクセスログも保管されていたのでしょうか。

すみません，普通のノートパソコンをつないだかどうかということでしょうか。

使ったコンピュータがどういうものかということと，それについてアクセスログを保管しているのかということですね。

はい。保管しておりました。で，保管しておりましたものは長野県さんにすべて御提出をさせていただきました。

そのアクセスログを見ることができたのは，だれとだれだかということはわかりますか。

実施者，それから私，それから長野県の情報政策課の方々ですね。だと記憶しております。

今回の実験の結果については，第三者評価というものがあるわけですが，それを行った伊藤穣一さんは，そのアクセスログを見てるのでしょうか。

見てると記憶しております。

被告財団法人地方自治情報センター代理人（橋本）

丙第２９号証の１を示す

先ほどの証言でわかりにくかったことを確認するんですが，まずこの書証の左側に「市町村」が２つあって，上の欄が実験市町村で，下の欄がそれ以外の市町村というようになっていますが，今回の長野県の実験において，外部から侵入して操作できたものというのは，実験市町村の㋑と書いてある端末を操作することができたというふうに理解していいですか。

はい。

で，この端末を操作することによって，実験市町村以外の市町村の住民の本人確認情報を検索し，又は閲覧することができたということでいいんですか。

できたという話は１度もしていません。

いいかどうか答えてくれればいいです。

していません。

要するに，しなかったということですか。

していません。

それは，じゃあ，できるというふうに考えたということですか。

先ほど来のお話を聞いていただければわかると思います。

裁　判　長

もう一度お答えになってください。

可能性を示しました。

被告財団法人地方自治情報センター代理人（橋本）

検索と閲覧とおっしゃったんですよね，可能性の範囲は。

先ほどの議事録を読んでいただければ。もう一度同じ話はできません。

裁　判　長

可能性として，検索と閲覧ということでよろしいですかというふうに聞かれていると思って，もう一度お答えいただいたらどうでしょう。

可能性があると思います。

で，可能性があると思われるのは，検索と閲覧ということでよろしいですか。

同じ意味です。

被告財団法人地方自治情報センター代理人（橋本）

そのときに検索又は閲覧できる情報が保存されているサーバというのは，どこにあるサーバなんでしょうか。丙第２９号証の１の中にあればそれで教えてください。なければないということで結構です。

どこにあろうと，端末が引っ掛けてきて画面に映し出せばそれでいいことでありますから，どこにあろうと関係ないと思います。

どこにあろうとではなくて，ここにある・・・。

それは私は認識していません。

認識していないわけですね。

はい。

いや，それをわかってるかどうか聞きたかったわけです。

わかっているかという話ではないと思います。

それから，今，検索と閲覧ということでお聞きしたんですが，他の市町村の住民の本人確認情報を改ざんするというのはできるんでしょうか。

先ほど来お話ししたんですけれども，可能性はゼロにはならないというお話を何度もしてきたと思います。

可能性を議論するときには，どのサーバにある情報を改ざんするのかを想定しなければ可能性の議論もできないと思うのですが，その点はいかがでしょうか。

クライアント／サーバのようなものではないので。これはネットワークを利用したコンピュータの情報の取得という形になりますので，クライアント／サーバのようなお話の中でお答えを出すというのは無理だと思います。

相手方市町村のＣＳサーバにあるものであろうが情報管理機関のサーバにあるものであろうが国の全国ネットワーク向けのサーバにあるものであろうが，そういう区別は一切考えなくてよろしいということでいいんでしょうか。

区別が直接問題ではなくて，ＣＳ端末を操作することによって検索結果が出てきてしまえば，その管理者権限を奪取した画面上に意図した情報が出てきてしまうという可能性を示しています。

私が聞いてるのは，検索，閲覧できるかということではなくて，今証人がおっしゃったのは，管理者権限を奪取したというのは，実験市町村におけるものであると私は理解していますが，その他の，中野区などの他の市町村の・・・。

すみません，コミュニケーションが取れないので，質問の意図を教えてください。要は，よそのものはできなくなっているんだからできないんだ，ということでしょうか。

いや，私はわからないから聞いてるんですよ。

わからない方がどうやって質問するんでしょうか。

裁　判　長

今わからないと言っている意味は別にそういう意味ではないので。お聞きになりたいのは，実験市町村の端末で他のどこかのサーバに入っている情報を閲覧したと。それで，それについて改ざんできるかという可能性はゼロではないというふうにおっしゃったものだから，改ざんされる情報というのは，他の市町村のサーバ，若しくは情報センターのサーバ，国のサーバ，そのいずれのサーバに入っている情報でもその可能性はあるというふうに考えておるのかという質問だということでよろしいですね。

被告財団法人地方自治情報センター代理人（橋本）

はい，そうです。

わかりました。転出，転入するというような，要はＣＳの中にある情報を書き換える条件というのがあろうかと思います。その条件を満たす場所であれば，その変更された情報が流れていってしまう可能性というのはある，そう思っています。

つまり，ＣＳに入っている情報を書き換える権限ということなんですが，それは実験市町村の端末を操作することによって，それ以外の，ありていに言えば他の市町村ということですが，要するに他のサーバでもいいんですが，そちらのほうの管理者権限というのは奪取できるんでしょうか。

中野区のＣＳの管理者権限を実験市町村からできるという認識はありません。

原告代理人（水永）

先ほど来，可能性を提示した，それから実験自体は行っていないというようなことをおっしゃってるんで，その点について何点か確認したいんですが。まず，ＣＳ端末の住基アプリケーションを起動させてみたかというような質

間がございましたね。

はい。

これは，実際には起動はさせてないと。

はい。

実験自体としてはしてないと。

はい。

で，そういうことができるかどうかという実験をできなかったという理由とか何か，条件というのはあるんですか。

はい。物理的な時間，それから操作してよいと首長さんから言っていただいた時間の中では，それを十分に行うことはできませんでした。

特に，業務時間帯の業務に影響を与えてはいけないというのが絶対的な条件だったわけですね。

はい。段階もございました。ここまでだったら業務時間中でも問題ないんだろうということであればよい，ここまでをやるんだったら業務時間中には勘弁してくれ，というような段階で行ったものであります。

そういう時間とかが無制限であれば，もうちょっと実験で可能性を詰められたということになるんですか。

はい。２週間以上ですね，いわゆる１箇月ぐらいの時間，それから実施するエンジニアの数，これをもっといただければ，もっといろんなことがはっきりしたと思います。

それに付随して一点なんですが，先ほど国側の代理人から，遠隔からＣＳ端末を操作すれば，そのＣＳ端末に映るマウス・ポインタなんかの動きで，遠隔で操作されていることが気がつかれちゃうじゃないかというような質問がありましたよね。

はい。

それを気がつかれないようにするというような手法というのは，理論的には

考えられるんですか。

論理的に言って可能だと思います。

それをやればマウス・ポインタが不審な動きをしないとか，そういうこともあり得るわけですね。

はい。画面を複数持たせるプログラムというのがございます。それを使えば可能になると思っております。

それから，阿智村のファイアウォールについてですが，これは管理用のポートがあいていたからファイアウォールの無効化の可能性があるところまでしか提示できなかったんだというような趣旨の証言をなさいましたね。

はい。

これは，なぜそこまでしか調べられなかったんでしょうか。その条件なり何かはあったんでしょうか。

はい。十分な時間とネットワーク，いわゆるインターネットから情報を検索して，それを基にいろいろなアタックを行おうというふうに考えておりましたが，残念ながら阿智村というところは，いわゆるデータ通信のＰＨＳというようなものがあるんですが，それの電波さえなかなか届かない所で，インターネットを検索することも自由にできませんでした。よって，インターネットの情報をすぐさま見ながら通常はやらせていただくものもできなかった。よって，ファイアウォールのオペレーティング・システムのバージョンの番号や，今どのようなアプリケーションのバージョンで動いているか，というところまでの確認はできました。で，そのＯＳ自身も大変古いものでしたので，パッチ対策が，当てていなければファイアウォール自体を無効化して管理者権限を奪取できる可能性もあることを報告した記憶がございます。

そうすると，今の御証言は，インターネットでの検索，まあ調べる環境があって，もうちょっと時間とかがあればファイアウォールの無効化というよう

なところまで調べられた可能性は十分あったというようにお聞きしていいんですか。

間違いないと認識してます。

それから，実際に管理者権限を奪取したＣＳ端末を利用して，例えば阿智村なら阿智村以外のところへ検索とかそういうことを実際にはやってないじゃないかということですよね。

はい。

これは，どういう理由からやらなかったということですか。

先ほど来お話ししているように，作業は限定された中で行われました。つまり，大前提は不正アクセス防止法に抵触しない形の範囲，かつオーナーがはっきりしている首長さんの権限の及ぶ範囲，その中で実験をやりなさいということでした。あいまいな部分も多々あったかとは思いますが，その範囲の中でやる。それが極めて限定された時間と場所，内容という形での作業であったと。ゆえにだと認識しております。

実際に村外まで通信を及ぼしていたら，刑事的にも問題になるということはあったわけですね。

その可能性は事前に指摘を受けていました。

それで，例えばＬＡＳＤＥＣとかそういうところの同意とかがあれば，実際にそういう実験もやりたかったわけですよね。

はい。公開討論会の中でも何度もお話をしております。今でもそう思っておりますが，私が見てきた現場に一緒に行っていただいて，現実を確認していただいて実験をさせていただければ，もっといろんなことがはっきりすると思います。

あと，受動的攻撃，これも実際には行ってないということですね。

はい。

これも，時間と人的資源とかそういうのを使ってやればですね，実際にはで

きたというふうにお考えでしょうか。

はい。可能性を示したことになりますけれども。対策を打ってあるから大丈夫なんだよということでありますので，それも一緒に国側さんと実験をさせていただければ，まあ国側さんというかＬＡＳＤＥＣさんと実験することになるんだろうと思いますが，そういうことをさせていただければより明確になるんだろうというふうに思っております。

それから，先ほど，阿智村で施錠した所で実験したじゃないかということをおっしゃってましたよね。

（うなずく）

それについて，先ほど一応説明はされてたんですが，もうちょっとリアルな理由と，それが意味がないということについて御説明いただけますか。

はい。当初ですね，私はずっと公開で実験をさせていただきたいというように申し出をしておりました。でありますけれども，田中知事のほうからは，この範囲の中でやってくださいというふうに限定されて作業を行いました。それはいろんな理由があったんだろうと思います，私はその詳細までは理解しておりませんが。マスコミさん等がですね，どこかでやってるというような情報を聞きつけて，あちこち私も追いかけられました。そういった形からですね，できるだけ発見されないように配慮をしてもらいたいと。これはやはり正確な情報を取得したいという御依頼主の御意向に従ってですね，御指示どおりの場所で作業をやったというふうに記憶しております。ただし，通常はどこであっても同じ作業が結果として行えます。なぜなら，そのラックや施錠されている所からケーブルが庁内に延びております。そのケーブルを利用して，空いているハブと呼ばれている口に管理調査用の端末を設置すれば，あるいはそのケーブルを延ばして応接室のようなところにさえ持ち込めば，全く結果として同じことができたと，それは間違い

ありません。

要するに，重要機能室に入るかどうかというのは，まあネットワークの何ですか，どこのセグメントでつながるかという意味では全く意味がないということでいいんでしょうか。

間違いないと思います。

それで，先ほど来，被告のほうからは結構技術的な質問をされて，こうこうすれば大丈夫じゃないかとか，こういう危険はないんじゃないかという趣旨のような反対尋問が結構ありましたよね。吉田さんとしては，そういうテクノロジーの最先端の問題はあるのかもしれないですけれども，自治体の現場を見てきた，そういう問題意識からしてですね，攻撃の具体的な危険性というと，実際にはどの辺に一番ウエイトがあるというふうに考えられますか。

ウエイトというと結構難しいんですけれども，今日，私がお話しさせていただいてる中で可能性という言葉をたくさん使いました。その可能性は，可能性というのは極めて小さいものだから大丈夫だというふうに取るか，可能性があるから危険だというふうに取るのかというのが論点だろうと思いますけれども。私の業界の中で，私が出したレポート，これが多分今日，オフィシャルになるんだろうと思います。どなたの目にも触れるような状態になるんだろうと思いますが，それが見れる状態になれば，吉田というのは，この期間の中でこういうレポートを出したんだということは，多くの方がある一定の評価をいただけるんだろうというふうに固く信じています。つまり，非常に限定された中でもこれだけの問題があったということはですね，たくさんの時間と人的リソース，コストをかけてやれば，もっと危険な問題が必ず見つかるはずだということを提示したんだろうと思います。その意味では，単に今般やったような閉じ込められた世界の中で限定された実験ではなくて，開かれた形でオープンな形で，もっとお金をかけて

人的リソースをかけてやらせていただければ，ＬＡＳＤＥＣさんや園さんと一緒にやらせていただければ，もっといろんな脆弱点を明らかにし，その対策を考えることができるんだろうというふうに認識しております。

裁　判　官（吉澤）

まずファイアウォールについてお聞きします。ファイアウォールは許可された通信を通すと，そういうシステムだということでしたよね。

はい。

それで，不正に入ろうとする場合は，許可された通信に成り済まして入ることが考えられるともおっしゃいましたよね。

はい。

どのようにして許可された通信に成り済ますのでしょうか。

具体的には，非常に難しいんですが，やっぱり手順というのがございます。まずファイアウォール自体にどのような，いわゆる穴ですね，何を許しているのかというチェックをするツールがあります。これもインターネット上で無償に配布されているものがございます。で，それを利用して，そのファイアウォールに，いわゆるポート・スキャンという名前のものをやらせていただければ，どこにどのようなサービスがあるかというのがわかります。更に今度は，そのポート番号を限定し，理解した上で，どのようなプログラムが動作しているのかというのを調べます。それが，例えばメール配信のプログラムであったり，ホームページを閲覧するために動作しているプログラムであったり，メールを受信するために動作しているプログラムであったり，そのようなものが古いバージョンで既に広く知られている脆弱性があるかどうかを確認します。で，それがあるようであれば，その脆弱性を突いて管理者権限を奪取するにはこうしたらいいですよというプログラム

がインターネット上に幾つかございます。それは，初めから実行形式のものになっているものもあれば，ソース・コードのままで配布されているものもあります。で，それらを自分たちの手で作って，その脆弱性を突くという形を行います。それをやるにはですね，実際にはそのポート番号にアタックするためのプログラムを起動し，例えばエスケープキーを二，三回，ぽんぽんと押してあげると相手側の奪取したコンピュータの端末ログイン画面，いわゆるコンソール画面と呼ばれているものがあります。例えば，ウィンドウズですとＣプロンプトと呼ばれている，ＤＯＳプロンプトと呼ばれているＤＯＳ画面のようなものですね。ユニックスで言うとログイン画面，一番最初にログインというのが出てくる画面があります。そういったものが自分の攻撃側の端末の中に現れるんですね。それが現れると，相手側のプログラムにログインできる環境というのがいったん現れます。そのときに，今度はＩＤだとかパスワードを入れてみて，例えば，私であれば「ヨシダ」というＩＤでパスワードが「ヨシダ」になっているんであれば，「ヨシダ」，「ヨシダ」で入れてしまうという形で，その侵入の可能性を洗い出しながらチェックしていくという手順になります。

次に無線ＬＡＮについてお聞きします。下諏訪町では無線ＬＡＮ環境を構築して実験を行ったということですね。

はい。

証人が知っていらっしゃる範囲でよろしいのですが，市町村の庁内ＬＡＮとして無線ＬＡＮで構築してるというようなものというのはあるのでしょうか。

はい。私が住む市町村には無線ＬＡＮのベースステーションという機械が，皆から見えるところの柱の上に堂々と置いてあります。

無線ＬＡＮに入る場合には，外から何かしらの方法で入ると思うんですが，それは，無線ＬＡＮ環境が構築されている場所からの距離とかによって，そ

の入りやすさとかは変わってくるんですか。

はい，おっしゃるとおりです。しかしながら残念なことにですね，アマチュア無線，いわゆるハムと呼ばれている周波数帯に，無線ＬＡＮとほぼ共通の周波数帯域を持つものがあります。そのハムには，２０デシベルとか２５デシベルというような非常に高いゲンイを持っているような単一指向性のアンテナが販売されています。どなたでも買えます。それを基に向きを限定すれば，ものすごく遠い距離，例えば１００メートルぐらい離れていても，その通信を意図した形で行うことが物理的に可能になるものであります。

甲第３６号証を示す

最後に，証人のほうで「アジェンダ～長野の実験で何がわかったのか～」という書面を作られていますが，ちょっと変な質問かもしれませんが，１０ページ，ここに「初心者」とか「学生」とかというふうに分類されているんですが，証人としてはどのような技術力を持っていらっしゃるのかということなんですが。

目一杯背伸びをして「観光客」だと思います。例えば私が依頼をして手伝っていただいた補助者という技術者は，この「破壊者」だとかいうレベルだと思っています。で，彼らが３日でできることをもし私にやれと言われれば，２週間までにはできるかなというぐらいの差があるというふうに御理解いただいて構わないと思います。

（以上　堀　込　康　子）

東京地方裁判所民事第２５部

裁判所速記官　　平　野　道　子

裁判所速記官　　峯　岸　佐　希

裁判所速記官　　稲　村　嘉　子

裁判所速記官　　堀　込　康　子