２００４年１２月２日

長野県本人確認情報保護審議会最終報告

長野県本人確認情報保護審議会

1. はじめに

長野県本人確認情報保護審議会は，長野県民の本人確認情報の保護を目的として，法律に基づき２００２年１２月に設置されました．審議会委員の任期は2年で，２００４年１２月の審議会でその任期が終了します．その間，審議会を１５回，審議会委員による市町村調査が６日間，説明会を９回，公的個人認証についての調査と安全策検討会議を４回開きましたので，審議会委員が集まった回数は 34 回になります．

これまでの審議会が歩んできた2年間を総括する目的で本報告書を作成することにしました．当初は審議会が行ってきた事柄を若干の解説を加えながら時系列に列挙する形で報告書を作成する予定でしたが，できあがった報告書は，審議会が２００３年に示した安全策の説明と各委員個人毎の総括文章のほうが多くなるという体裁となりました．

審議会が行ったことは，県のＨＰにある審議会のページに全ての議事録と資料を示していますので，こちらを見て頂くほうが正確に全てが明らかとなります．それよりも，今我々が訴えたいことの記載が優先されました．

その一つが安全策です．

審議会が 2003 年の5月に提出した中間報告書では，それまでに行った市町村調査の結果明らかとなったインターネットからの侵入の危険性に対処するため緊急の対策を求め，その対策が完了するまでの間は緊急避難的に住基ネットから離脱することを提言しました．その後，その対策が次々と進められたこととあわせて，２００３年8月にインターネットからの侵入対策を含む住基ネット全体の問題点を4つに整理し，それぞれに対する安全策を提言しました．今審議会がもっとも訴えたいことはこの安全策の速やかな実施です．

さらに個人毎の総括です．

審議会委員は，様々な分野の人間があつまりました．各自が住基ネットについて持っている思いや立場はそれぞれ異なります．しかし，審議会ではその立場の違いを越えて，本人確認情報の保護の一点で協力しあい，精力的に調査を行い，様々な安全策や改善策の提言をしてきました．その間，各委員はそれぞれがいろいろな思いを込めて活動してきました．委員の

4 各委員の所感

4－1.　不破泰会長

(1) 審議会の役割

本人確認情報保護審議会は，住民基本台帳法で設置することが定められている審議会で，全国全ての都道府県でそれぞれ設置されています．

その役割についても法律と条例で定められていて，長野県民の本人確認情報（氏名，性別，生年月日，住所の4情報に住基ネット実施にともない付加された11桁の住民票コードとこれらの変更情報を加えた6情報）を保護することが目的です．

具体的には，この本人確認情報を利用したサービスを行う等の場合に，そのことで本人確認情報が漏洩する等の事態が発生しないかを検討し，危ないときには危ないと言うのが役割です．

2003 年の5月の審議会で県に提出した中間報告書では，インターネットから侵入の危険性があるため緊急の対策を求め，その対策が完了するまでの間は緊急避難的に住基ネットから離脱することを提言しました．

この住基ネットからの一時的離脱は，本人確認情報に漏洩の危険が差し迫った場合は，県や市町村は必要な措置をとることが義務づけられており（住民基本台帳法第 30 条の 29，第 36 条の 2），また県知事や市町村長が住基ネットの本人確認情報に対する危険性が現実化したときに一時的に接続を切ることはあり得ると総務省も述べておられます（平成 15 年6月に発表した「長野県本人確認情報穂審議会第 1 次報告についての考え方」）．

その当時の状況が本当に危険が差し迫った状況であったのかどうかについては，審議会としては，当時インターネットとの接続がある市町村の中に，大変危険な接続形態となっている市町村が複数あると認識し，危険があると判断しましたが，当時の県の方々や総務省の方々から多くの疑問が出されました．疑問を述べられた県の方に「ではどういった状況になれば危険が差し迫った状況と言えるのでしょうか」とお尋ねしたところ，「実際に数人の本人確認情報漏洩が発生した場合等です」と答えが返ってきました．でも，それでは実際に漏洩された方々は救われません．当時，関東地方でストーカー行為で身の危険を感じておられた女性が警察にいくらそのことを訴えても行動してもらえず，その女性が駅前で殺されてから警察が捜査に乗り出した事態と同じだと感じました．それと同じことをしてはいけない．危険性があると考えたら迷わずその対処をしようと考えていました．

また，審議会では5月に危ないと提言したあと，その危ない状況を解決するための安全策を作り上げ，8月に提言しました．そして，その実行を県に迫っています．

審議会は，相手が国であろうと県であろうと，危ないことは危ない，そしてその改善策があればそのことを申し上げるということに徹してきました．

審議会が設置されたときに，審議会メンバーを見て，この審議会が住基ネットのそもそも論を論じるところだと思われた方が大勢おられました．しかし，それは本来の審議会の役割ではありません．審議会ではこのことについては慎重にそして厳密に区別して対処してきたつもりです．個々の委員は，個人としていろいろな考えを持ち，また他の場所では様々な発言をしておられますが，審議会では役割にそって対応して頂いています．

審議会の役割について繰り返しますが，この審議会は本人確認情報を利用したサービス等を行うに際して，情報漏洩等の危険性があるかどうかを調べ，危ないならばそのことを申し上げるところです．危険性というのはなにも技術的なことだけにとどまりません．技術的に完璧であったとしても操作する人が不慣れであったり仕事に無理があったりするのではなにもなりません．また，その技術を維持するための経費が膨大であったのでは，技術の維持そのものに無理が生じます．様々な点について危険性を調べ，問題があれば指摘することが役割です．調べていく過程でより安全な方法等がわかればそのことを提言もします．実際にそのサービスを実施するか否かを審議するのがこの審議会の役割ではありません．サービスを実施するかどうかを決めるのは行政です．

県はよく次のような説明を発表されていました．「実施については本人確認情報保護審議会で審議中で，その結果から判断します」 審議会が判断するのではありません．判断するのは県自身です．審議会は県が判断されたことについて安全面から検証をしますし（住基ネット自体はそのケースでした），判断前に諮問をうけてその検証を行うこともありました（公的個人認証サービス，パスポート発行サービスはこのケースでした）．

(2) 本人確認情報の価値論について

審議会が本人確認情報保護の不完全性について指摘したときに，様々な方から本人確認情報はたかが6情報にすぎず，そのうちの4情報は閲覧情報であることもあって，それほど厳密に守るものではないのではないかというご意見が出されました．

まず，閲覧情報であるということと公開情報ということとは違うことを認識しなければなりません．閲覧は閲覧者が閲覧しようとする特定の個人の住民票情報を管理している市町村役場まで出向き、担当職員の面前でその身分を明らかにして閲覧条件（住民基本台帳法 11 条2項3項参照）を充たしていることを確認され許可を得て，限定された範囲で見ることが許されます．DVの関係等で閲覧が許可されない場合もあります．役所に行くと公開情報として壁に4情報が張り出されているわけではありません．

2004 年に長野県南部でお一人暮らしのご老人が連続して殺されました．その町の有線放送電話の電話帳には電話を引いておられるそれぞれの家庭の家族全員の名前が記載されていて，犯人はお一人暮らしの家を電話帳で調べたといいます．おそらく，電話帳を作られた方は親切心で全員の名前を記載されたのだと思います．そして，たかが名前ぐらいは記載しても大丈夫だと判断されたと思います．おそらく大多数の人はこの「たかが」という判断の通り，記載されても大丈夫です．しかし，現実に「たかが」ですまない方がおられた，そして亡くなられてしまったという

ことです．氏名と住所だけの名簿でさえ、このような事件に利用されることがあるのです．

まして，本人確認情報はこの4情報に加えて住民票コードと変更情報（住民票コードは自由にこれを変更することができますが、変更履歴として過去の住民票コードも記録され続けます．）が付加されています．住民票コードは行政機関が個人データをコンピュータ処理するうえで極めて重要な個人識別番号で、行政機関にとっては極めて便利なものになる可能性を持っていますが、そうであるだけに住民票コードが第三者に知られると、逆に特定の人の住民票コードさえ分れば、特定の人の住所を追跡したり、個人データを不正取得したりすることが極めて容易になります．だからこそ、住民基本台帳法は住民票コードの告知要求制限に関する規定（30条の42参照）をわざわざ設けているのです．

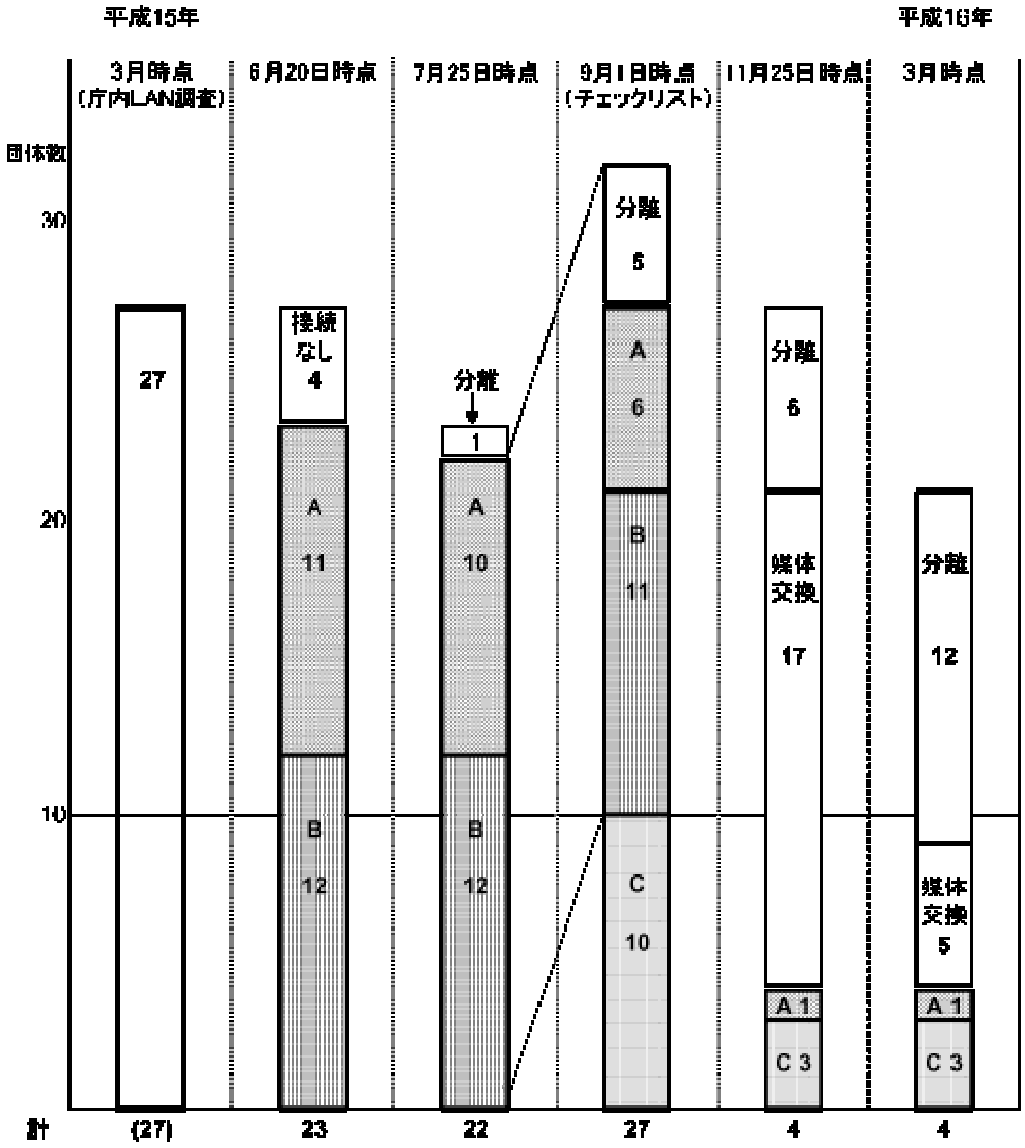
6情報が「たかが6情報」なのかどうか，それは個人お一人お一人によって違います．おそらく私も含めて大多数の方にとっては「たかが」だと思います．しかし，ご主人の家庭内暴力から逃れるために子供を連れて身を隠しておられる奥さん（子供の就学のために住民票はその町で登録していて，ご主人にはＤＶ法や住基法令により閲覧不可にしている）にとって，新しい住所は「たかが」ではすみません．同じような事情をもたれた方は少なくないと思います．

本人確認情報保持し管理しているものは，まちがっても「たかが」という言葉を使ってはいけないのだと思います．必要なのは，「たかが」ではなく人の痛みを配慮できる大いなる「想像力」だと思います．

もう一つ大切な問題として，ここで扱っている本人確認情報はディジタルデータであるということです．本人確認情報が盗まれたと言う事態を，家宝の花瓶が盗まれたということと同じに扱う事は出来ません．花瓶が盗まれたら取り返せば解決します．しかし，ディジタルデータが盗まれたら次々とコピーされてあらゆるところに配布され，二度と取り返すことはできません．

(3) 市町村におけるネットワークの問題（インターネットからの侵入の危険性について）

インターネットとの物理的接続状況の推移



A: 基幹系・情報系2系統のLANが、FW等を介して接続され、情報系がインターネットに接続されている団体

B: 基幹系・情報系が同一のLAN上に構築され、インターネットに接続されている団体

C: 平成15年3月時点の調査には全団体が回答していないことから、同年8月にチェックリストによる調査結果に基づき確認した結果、住基ネットが庁内LANを介してインターネットと物理的に接続していることが新たに判明した団体

※ なお、残り4団体のうち、1団体は平成16年12月末に分離予定。他の3団体については、脆弱性調査の結果を見て判断するとしていたが、現在まで分離していない。

審議会が設置されて最初に行ったことは，市町村の実態調査でした．調査の結果最初に懸念された情報漏洩の危険性のひとつが，市町村のネットワークの管理問題でした．

庁内には大きくわけて3種類のネットワークがあります．1つ目は住基ネットワークのデータが格納されている住基サーバが接続されている住基ネットワークです．2つ目は市町村が元々有している住基データよりもっと多くの個人情報が格納されているサーバが接続されている基幹系ネットワークです．3つ目は市町村が住民に情報提供するためのホームページを運営したり，庁内の職員がインターネットを利用したりするための情報系ネットワークです．

本来，住基ネットを安全に運用するためには，少なくとも住基ネットワークは隠蔽して勝手にこのネットワークにパソコンなどを接続できないようにすることが大前提です．接続したパソコンからの侵入や，そのパソコンがウィルスに感染していた場合に住基サーバがウィルスに感染する恐れがあるからです．しかし，実際には住基ネットワークの HUB ポートが外に置いてあり，パソコンの接続が可能になっているケースをはじめ，いろいろな問題があることが判りました．

また，住基ネットワークと基幹系ネットワークは通常はファイアウォールと呼ぶ装置を介して接続されています．これは，基幹系ネットワークにある住民情報を定期的に住基サーバに反映させる必要があるからです．ファイアウォールがあるから基幹系ネットワークから住基ネットワークへの侵入を 100%防げるという保証がない以上，住基ネットワークと接続されているこの基幹系ネットワークは少なくともインターネットと接続されている情報系ネットワークとは完全に分離すべきです．

しかしながら，20以上の市町村で基幹系ネットワークと情報系ネットワークの分離がなされていませんでした．基幹系ネットワークと情報系ネットワークとの間にファイアウォールがある場合はまだよいのですが，基幹系ネットワークと情報系ネットワークがまったく同一のネットワークとなっている，危険が懸念される市町村が10以上ありました．

市町村のご協力を得て県が市町村の庁内ネットワークを図面で調べ，平成15年3月の時点で27の市町村において何らかの形でインターネット－情報系ネットワーク－基幹系ネットワーク－住基ネットワークが接続されていて，インターネットから基幹系ネットワークの情報や住基ネットワークの情報が漏洩する恐れがあるという結果が出ました（接続状況推移図を参照）．

審議会ではこの結果を重視し，平成15年5月に緊急の中間報告を作成してこの問題の危険性を訴え，対処が完了しない間は緊急避難的に住基ネットからの離脱も訴えました．

その後，4つの市町村では図面とは異なり実際にはこのような危険な接続は無いことが判りましたが，残りの23市町村では平成15年6月の時点でインターネットとの接続問題がありました．このうち，基幹系，情報系ネットはファイアウォールで一応分離されていてファイアウォールの運営をきちんとやることで安全が確保できるところが11（推移図の A），基幹系，情報系ネットが同一で危険が懸念されるところが12（推移図のB）でした．

このなかで，特に危険なのはBでした．4月から県の情報政策課が市町村を回って分離の説明

を行い，5月の審議会の中間報告を経て6月に県内各地で行われた説明会等で市町村の担当職員の方々にお話しをしてきたこと等を経て，大部分の市町村で8月までにインターネットとの分離を決定し，予算措置をして業者との契約手続き等を経て11月下旬の時点では，A は残り1に，Bはゼロになりました.

このように，インターネットとの接続の問題は，多くの市町村のご協力を得て，長野県では殆ど問題が無くなったと言っても良いと思います．しかし，全国にはまだ長野県の市町村のような対応をとっていない市町村が多く残っています.

なお，図面等の提出を最初に頂いていなかったところであらたに10市町村でのインターネットとの接続問題が9月に明らかになりましたが，これも11月には3に減っています.

(4) 市町村が決めたことなのか

住基ネットを開始するにあたり，総務省は「このネットは市町村が求めたから総務省で作ったものであって，総務省が求めたものではない」と説明されていました．審議会では長野県下120市町村（当時．今は市町村合併で市町村数は少し減っています）にアンケート調査を行い，またいくつかの市町村には委員が訪れてご意見を伺っています．そして，「住基ネットは私たちが求めていたものです」ということを言われたところは1つもありませんでした.

(5) 市町村の混迷

どの市町村も，住基ネットは国の法律（改正住民基本台帳法）で定められているから接続していなければならないのだという認識でした．しかし、住基ネットの実施主体になることと常に接続していなければならないこととは全く別のことです。実施主体であっても、個々の自治体の事情で接続できないことはあり得ます。市町村長、都道府県知事は住基ネットの管理運用に関して「適切な管理のために必要な措置」を講じる義務を負っている（住民基本台帳法 30 条の 29 第1項、36 条の2）ので、その具体的な内容のひとつとして、住基ネットの管理運用について費用面や職員の管理能力面などに自信がなく、住民や他の自治体に対して責任ある管理運用ができない場合に、これらの問題を解決できるまで住基ネットとの接続を中止することが、現実的な対処法として考えられます。できないことは「できない」とはっきり言って接続しない方が、迷惑や被害を防止する上で実際的です。

また，住基ネットでは県も大切な役割を果たしています．総務省からのネット管理等に関する様々な指示は，県を通じて伝えられます．ですから，この指示を受けた市町村は指示は総務省と県が合同で出したものだと受け取ります．国がその実施を決め，国と県が具体的に実施作業や管理作業を指示してきて，市町村はその指示に忠実に従ったのであって，決して市町村が実施を求めたものではない．市町村から見ると，指示をしているという点においては，県は国と同レベルになっていました.

その県が，住基ネットについて疑問を突然言い出したことで，多くの市町村は大変困惑された，また憤りも感じられたという実態がありました.

(6) 安全策について

2003年5月に中間報告をしてから3ヶ月，中間報告で明らかとなったネットの問題点を解決する安全策について考え続けていました．そして，8月の審議会で1次から4次までの安全策を提案し，審議委員の了解を得て県に提出しました．この段階で，住基ネットの安全性に関する議論は第3フェーズに入ったと思っています（第1フェーズ：調査，第2フェーズ：危険性の指摘，第3フェーズ：安全性確保のための行動）．

安全策については何度も繰り返し発言していますが，1次（インターネットからの分離）はほぼ完了しています．残りの2，3，4次の安全策については，たまたまこのような順番で番号を振ってありますが（番号はこの順番で説明すると理解して頂けやすいと思った順で付けました），それぞれの策は基本的には独立していて，出来るところからどんどん実施していけばよいものです．決してこの順番で実施する必要があったり，かならず全てを実施しなければ意味が無くなってしまうというものではありません．

(7) 侵入実験について

侵入実験について，私は次の趣旨の発言を6月にしました．「インターネットとの接続を切ることに疑問を持たれるのであれば，実際にそれぞれの市町村で接続したままでどのような危険性があるのかを実験して試した方が良いです．ただし，その実験はその目的を明らかにして公開の場で行い，だれもが参考にできるようにすることと市町村を混乱させることがないように配慮しなければなりません．そして，その結果危ないことが判った市町村は切って頂き たいし，危なくないことが判った市町村は今すぐ切る必要はないがこれからも監視を続けた方がよいです．」

その後，インターネットとの接続問題は，上述のように7月末の時点ではほぼ解消されていました．そして，接続が残った市町村はネットワーク構成図面上危険性が高くないところでした．その結果，私が申し上げた意味での侵入実験はその必要が無くなりました．

県は侵入実験を2003年9月から11月にかけて行いました．実験には県からの求めに応じて審議委員の一人が協力しています．当事者を除き，実験の時期や場所，実験の方法等は審議会には知らされることは有りませんでした．もちろん県民に知らされることもありませんでした．

侵入実験の結果は12月に速報が公表され，最終報告書は 2 月に公表されました．その結果から審議会は多くのことを学び，その具体的な安全策を得ることが出来ましたし，市町村が中心となって構成して県も参加している電子自治体協議会がもうけたセキュリティ対策WGにおいても，侵入実験から明らかとなった庁内ネットワークの問題点を元に安全策を決定するなど，意味のある実験となりました．

しかしながら，県の公表の仕方等，審議会として多くの疑念を感じる実験でもありました．実験に協力された審議委員の方も，県の対応によって大変な思いをされました．

実験の有意性とは別の問題として県のこの対応は批判されても仕方がないと思います．そのことについて，私は2003年12月の審議会で次のように発言しています．

「(侵入実験に関する)県の対応に問題があったのではないかと思っております．それから、これは私自身自問している問題なんですけれども、セキュリティの問題があるから一切公表しないと．何もかも公表しないというのは問題があったのではないかと思っております．セキュリティ上問題がないこともたくさんあったと思います．それについては適宜、その都度公表すべきであったし、少なくとも実験を始める前にこの実験は何のためにやるのかということをしっかり公表してから実験をすべきであったのではないかというふうに、私自身、県に強く、今後こういうことがないように申し入れたいと思いますし、私自身も審議会の中でそういうことをもっと問いただすべきだったのではないかと考えております．」

(8) 公的個人認証サービスについて

2003 年 11 月の審議会で，知事より 2003 年度に県が実施を計画している公的個人認証サービスについて，安全性の検証をするように依頼がありました．このことにもとづき，このサービスの安全性検証を始めました．

始めてから判ったことは，このサービスは 2003 年 11 月の時点ではまだ岐阜県でシステム構築中で，どのようにして情報が伝わり，どのようにして安全性が確保されるのかといったことが都道府県に明らかにされていないということでした．実際には LASCOM ((財)自治体衛星通信機構)という組織に業務を県は委任するように国から指示が出ていたのですが，LASCOM に委任するには，本当に委任をして安全かといったことについてきちんと調べなければなりません．しかし，その時点では LASCOM が県から委任された場合に，県から送られた県民の個人情報をどのように扱うかについて，まだ不確定な部分もあることから教えてもらえませんでした．つまり，安全性の検証が出来ない状況で，それでも委任を迫られていました．

審議会では，11月から審議会を3回，検討会を4回開催して公的個人認証システムの仕組みを調べ，その結果から全部で 108 項目に上るチェック項目についてそれぞれの安全性の検証作業を行いました．明らかではない点や疑問点は次々と LASCOM，総務省等に問い合わせを行い，一つ一つ疑問点を解消しながら，検証に努めました．また，どうしても LASCOM や総務省等からセキュリティ上問題があるため回答出来ないと言われた点について，総務省に出かけて問い合わせを行う等の作業を行いました．

その結果，108項目のうち99項目については安全が確認され， 運用状況により確認が必要なものが4項目，長野県独自の対策・支援により安全が保たれる項目が5項目(そのそれぞれについて，審議会としての安全性確保の方法を提示)という結果になり，そのことを2月の審議会で県に報告しました．

公的個人認証サービスは，審議会にその安全性検証が付託された初めての県が行う住基ネットを利用したサービスでした．そして，審議会は決してサービス反対のための論を張ったりするのではなく，危ないことは危ないと国にも県にも申し上げ，また危ない点について可能であれば改善策を提示するという対応に終始し，厳密に審議会としての職務をこなしてきたと思っています．また，長野県は審議会と共にその調査をきちんと行ってきました．

この過程で残念であったことは，総務省とLASCOM等が審議会や長野県に対して不信感を述べられ，その結果いくつかの点について安全性を高めるための具体的な技術について回答を拒否されたことです．審議会は，審議の過程で明らかとなった事項について，安全面で問題があるため機密厳守を求められた場合は，これまでも厳密にそのことを遵守してきています．まして，この回答を拒否された箇所は，安全性確保のための技術名が例え公開されても，そのことをもって安全性が脅かされるという部分ではありませんでした，むしろその技術名が明らかとなることでだれもがその安全性を確認できると審議会として判断している部分ですので残念でした．

もう一つ残念であったことは，長野県は上記のような過程で検証を続けていたために，実際にはLASCOMへの委任は他の都道府県より5ヶ月遅れました．他の都道府県は11月から12月の間に委任をすませていました．そして，遅れたことで長野県だけがサービス開始時の作業について国の財政措置が無く、県独自に作業経費を支払う結果となりました．私はこの審議･検証作業はどうしても必要な作業であり，仕様が決まっていく過程でそれに併せて検証できるものから検証を続けていったことで生まれた遅れであることから，仕方のないことだと考えましたが，多くの方々より長野県だけが経費を負担したことで批判をいただきました．

(9) 他の都道府県の審議会

法律で設置が決められている本人確認情報保護審議会は，日本中全ての都道府県に設置されています．審議会をやっていていつも感じていたのは，他の都道府県の審議会ではどのような判断をされているのかということでした．　公的個人認証サービスを開始するにあたってのLASCOM との委任も，このサービスで県民の情報がどのように扱われ処理されるかをいろいろLASCOM や総務省等に問い合わせをしても，いくつかの点について LASCOM や総務省自体が仕様が決まらず返答出来ない状況の時点で長野県以外の都道府県では委任が行われました．どのようにこのサービスで安全性が確保されると確認されたのか，大変不思議に思いました．

住基ネットワークを運営しているのは，市町村です．その市町村でどのような運営をしているのか，市町村の実態調査は情報保護を議論する上で必ず必要な作業です．それを他の都道府県で実施されたということを聞いたことがありませんでした．実質的に審議会が一度も開かれていない都道府県もあるそうです．

(10) 県の対応について

県の対応について，私にはいろいろな側面を感じて来ました．

現場で共に活動してきた方々は大変多くの時間と労力と工夫を凝らして精力的に活動して頂きました．審議会がそれなりに活動できたのもこういった方々のおかげです．

その一方で，その対応に疑問を持ったことも幾度もありました．このことについては，2004 年 8 月の審議会で知事に申し上げた下記の言葉が全てです．

「今、知事も冒頭におっしゃられたとおり、長野県の住基ネットというのは、危ない部分を自ら検証して、その部分については独自の安全策を策定して実施する段階になっています．それから、

住基ネットを利用するシステムである公的個人認証もパスポートの発行についても、その安全性を自分で検証して独自の安全策を練っていくという、他の都道府県で見られない独自の安全なネットワークを作るフェーズが今始まっていると思っております．このことに関しては、私どもの審議会も関与をさせていただいてはいますけれども、ここで是非県にお願いをしたいのは、その安全策実施の主体はあくまでも県であることです．県が自ら責任を持って安全策を実施しているんだということを是非ご確認いただければと思っております．審議会は、国や県が行うことに対してチェックをして、問題があればそのことを指摘もし、また安全策があればそのことを提案させていただきますけれども、それを実施するのは県です．しかしながら、時々、県の対応に県が主体であることを自覚しておられるのか疑問に感じる場合もございまして、例えば、安全策の実施についても、それから侵入実験に対する対応であったり、県議会での答弁などで、あたかも審議会にみんな丸投げしているかのようなご発言をされる場合もありまして、大変困惑をしています．困惑は私ども審議会委員だけではなくて、市町村もその点では困惑をしていまして、住基ネットを実際に運用している市町村が困惑しているというのは、住基ネットの安全策を実施する上でも大きな影響があります．市町村の困惑を解消して、安全策への理解を得ていくために、安全策実施に県が主体的に取り組んでいるという姿勢を県の皆様が是非示していただきたい．知事をはじめとして県の皆様も、私ども審議会委員も、県民の情報保護という大変重い使命を担って、それぞれの立場で活動をしておりますので、是非、この点をよろしくお願いをしたいです．」

(11) 2年間を振り返って

審議会委員の任期は2年間です．この2年間で審議会は最後の12月の審議会を含めて15回開催しました．また，審議委員による市町村調査が6日間，説明会を9回，公的個人認証についての調査と安全策検討会議を4回開きましたので，審議委員が集まった回数は34回になります．このうち，東京で集まったのは5回で，全体のほぼ9割になる 30 回は長野県で開催しました．各委員は東京や伊那から毎回集まって頂き，ご審議頂きましたことを本当に深く感謝してこの2年間を締めくくりたいと思います．本当にありがとうございました．

中にはその思いをある程度は世間に表現出来てきた方もいますが，大多数の委員はそのような表現の場は与えられずにいました．審議会委員を終えるにあたって，各委員が改めてその思いを報告書の形で表現したいと思います．

これから情報処理技術と情報ネットワーク技術の進歩を上手に取り入れて，効率的で利便性の高い電子社会の到来を全委員が望んでいます．しかし，そのなかで個人の情報をきちんと保護して，不幸な目にあう人，苦しい思いをする人がないようにしなければならないことは言うまでもありません．我々委員の2年間はその安全な電子社会を作るための2年間でした．任期はこれで終了しますが，これに続く審議会がさらにこの意志を引き継いでいただき，よりすばらしい電子社会が到来することを，切に望んでいます．

2. 審議会活動経過

2. 1　平成 14 年 12 月－平成 15 年 5 月

審議会が発足した一昨年12月から昨年5月までのフェーズで, このフェーズでは住基ネット運営の現場を見, 現状の住基ネットそのものを調べるというフェーズ. そして, 最初事務局が審議会に提出した書類上の住基ネットと, 現実に様々な市町村のネットとの間には大きな違いがあること, 現場での担当者は本当に大変な思いをされて必死で運用をされていること, そしてインターネットと庁内ネットワークが不用意に接続されているケースがあること等がわかった. その後, インターネットと庁内ネットワークの接続を切ることがなかなか進まない事態となる.

(1) アンケートの実施

県下120の自治体における住基ネットの実態把握のために、審議会独自のアンケート調査を実施し、112の自治体から回答をいただいた.

(2) ヒアリングの実施

アンケートの調査結果から、更に自治体の聞き取り調査が必要と判断し、市3ヵ所、町4ヵ所、村4ヵ所の計11ヵ所を選定し、6名の委員が2名ないし3名に分かれて、各自治体に足を運び、担当職員及び担当課長を含めて面談、同時にネットワーク機器やＬＡＮ環境の現場も調査した。ここで、インターネットと庁内基幹系 LAN が何らかの形で接続されている問題が見つかった.

(3) 県による市町村のネットワーク構成調査

県は全市町村に対するネットワーク構成調査を実施し、平成15年3月時点で27市町村がインターネットとの接続問題を有していることが判った（その後の調査で23と判明）。審議会ではインターネットとの接続を分離指導するよう県に提言した.

2. 2　平成 15 年 5 月－平成 15 年 8 月

平成 15 年5月から8月までの期間、第一フェーズで明らかとなったインターネットとの接続問題を緊急のセキュリティ問題としてこれを解消するまでの一時的な住基ネットからの離脱を第 1 次報告として提出し、そのあと各地で説明会を開いた. 中間報告は大変大きな流れをつくり、説明会でも様々なご意見があった. また、このフェーズでは多くの市町村のご協力のもと、インターネットと庁内基幹系ネットワークとの分離が進んだ. 8 月 5 日には住基ネットに関して、国と長野県による公開討論会を開催し、安全性について議論を交わした.

(1)　第 1 次報告書の提出

インターネットと庁内基幹系ネットワークの接続を切ることがなかなか進まない事態解消のために、平成 15 年 5 月 28 日に第 1 フェーズ活動をまとめた報告書を県に提出した. この報告

書では市町村アンケートや市町村への聞き取り調査をもとに、現場担当者がどれだけ悩んでいるか、インターネットとの安易な接続の危険性、情報セキュリティ確保方法、住基ネットの法的問題などを論じ、結論として、「インターネットから侵入の危険性があるため緊急の対策を求め，その対策が完了するまでの間は緊急避難的に住基ネットから離脱すること」を提言した.

それに対して総務省からは、「県が離脱することは明確に違法であり，認められない」との見解が出された.

しかし、6月5日付けの総務省通達文書には、「住民基本台帳法上，本人確認情報に対する危険が現実化したとき，市町村長や都道府県知事が一時的に接続しないことはあり得るが，この規定を独自に解釈し，参加しないことはできない.」とあり、審議会では，インターネットとの接続問題は，まさにこの「危険が現実化」している状況であると認識し、一時的な非接続を提言したものである.

それに対して総務省は、「インターネットと接続していてもファイアウォールがあるため問題ない」との認識であったが、総務省の住民基本台帳ネットワークシステム調査委員会委員からさえも、「ファイアウォールがあるから安全だなんて大臣が言ってもらっては日本のレベルの低さがわかるから困る」との発言が以前からなされていた.

(2) インターネットと庁内基幹系 LAN、住基 CS サーバとの分離指導

平成15年3月時点の調査回答で27の市町村において何らかの形でインターネットと庁内基幹系 LAN が接続されていたため、県を通して分離指導を開始し、直ぐにインターネットと分離できない市町村に対しては、基幹系ネットと住基ネットを分離し、異動データを媒体交換する運用に変更するよう指導した. その結果、平成 16 年 11 月時点では4団体を残してインターネットと住基ネットが完全分離された.

5月28日に緊急避難的な非接続提言をした原因となっていたインターネットから庁内基幹系 LAN 経由でのＣＳサーバ侵入に関しては、ネットワーク分離や媒体交換などの対策により少なくとも長野県内自治体での「危険の現実化」は実質的に解消され、インターネットからの侵入実験による「危険の検証」は緊急課題ではなくなった. しかしながら、全国的には依然としてインターネットと庁内 LAN が接続されているケースがあり、総務省もその分離を指導している.

(3) 第 1 次報告書の県民説明会

6月11日の夜、阿智村公民館主催の緊急学習会に委員5名が出席し、住基ネットの仕組み、庁内 LAN の危険性、セキュリティ対策コストと情報漏洩によるリスク、法的課題、などを踏まえて現状の危険性を訴え、「当面の離脱」を提言した理由を説明した. 第 1 次報告後県民に直接説明する初めての機会ということもあり、村長や県会議員をはじめ近隣市町村の住民や職員など 250 名が参加、予定時間を大幅に超えて 22 時過ぎまで熱心に意見交換した.

6 月 15 日には県が主催する初の説明会を下諏訪町にて開催. 委員 6 人全員と、知事や町長も含めて、350 名が参加した. 以後、添付資料「第 1 次報告に関する住民説明会開催経過」にあるとおり、全県で同様な説明会を 7 月 10 日までに計 10 回開催し、延べ 1235 名が参

加、委員は 1 回の説明会に平均 3.8 人が出席した.

全ての会場で県民からの質問を受け付け、その場で回答した他、それらをとりまとめて、添付資料「第 1 次報告書に関する住民説明会での質問と回答」を県のホームページにて公開し、広く県民の皆さんと住基ネット問題を共有した.

(4) 国との公開討論会で、住基ネットの安全性を論議

平成 15 年 8 月 5 日東京麹町会館で、国の住民基本台帳ネットワークシステム調査委員会委員と県の審議会委員による公開討論会を開催した. 双方から 4 名ずつメンバーを出し、前半はお互いのプレゼンテーションで国側は住基ネットの安全性と IT 化推進の必要性を訴え、県側は櫻井委員が現場の調査結果をもとにした市町村の現状とインターネット接続の危険性を訴えた. 後半では、住基ネットの範囲の定義や安全性、侵入試験の是非について討論した.

http://www.pref.nagano.jp/soumu/shichoson/jyukisys/toron-1.pdf (長野県作成)

http://www.pref.nagano.jp/soumu/shichoson/jyukisys/toron-2.pdf (長野県作成)

http://www.soumu.go.jp/c-gyousei/daityo/pdf/koukai_gijiroku.pdf (総務省作成)

この討論会を通して、以下が明らかになった.

住基ネットの範囲は、国が管理･監視できているＣＳより内側のファイアウォール、県内ネット、全国ネット部分だけでなく、市町村管理のＣＳ、ＣＳ端末まで含まれること、

市町村の庁内ＬＡＮの安全性確保は市町村の責任であり、住基ネットの安全性はその責任の上に成り立つことになること、

住基ネットは、住民票広域交付などの利便性のためというよりも、インターネットで各種申請や取引を行う際の個人認証基盤として必要であると国が考えていること、

庁内 LAN の監査やインターネットからの侵入試験は、公開方法は別にして、実施する必要があることを国側委員も認めたこと.

2. 3 平成 15 年 8 月―平成 16 年 12 月

昨年8月以降住基ネットに関する長野県独自の安全策を提言し, その実施を県に促していったフェーズである. はじめの半年はなかなか安全策が実施されず, 審議会で何度も県の態度を批判した. 現在では県が実施した侵入実験の結果もふまえて安全策はより具体的になり, 長野県電子自治体協議会が策定した市町村の安全策にもつながっている. また, 県の県域ネットワーク構想にもこの安全策は取り入れられ, 着実に実施されようとしている.

具体的に県と市町村は平成 16 年 3 月より安全対策として次のような取り組みを行っている.

3月3日　県が市町村に対して安全策について説明会を開催（長野市会場：30団体参加，塩尻市会場：49団体参加）

3月25日　電子自治体協議会セキュリティ対策ワーキンググループ会合（松本市会場：26団体参加）

5月21日　市町村セキュリティ研修会（塩尻市会場：90団体参加）を電子自治体協議会及び県が開催

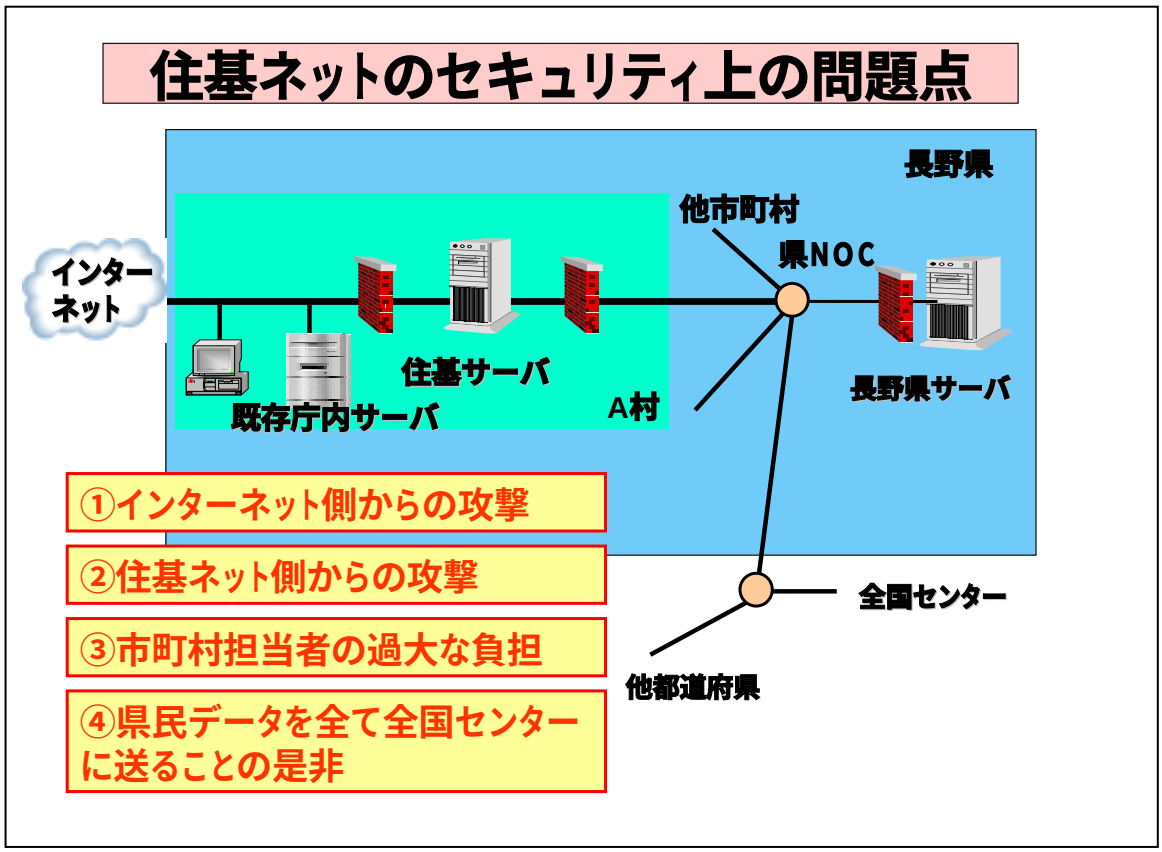
5月24日　電子自治体協議会セキュリティ対策ワーキンググループ会合（県庁：18団体参加）

6月17日　住基ネット担当者研修会（松本合同庁舎：110団体参加）において，住基ネット運用とセキュリティについて，地方自治情報センター，総務省及び県が説明

3. 本人確認情報保護のための課題と提言

3-1. より安全な住基ネット運用への４方策

審議会が２００３年８月の審議会で提出した住基ネットの安全策を説明します.



これが現在の住基ネットの構成です. 緑色の部分がそれぞれの市町村で, この緑色が１２０(当時) あります. そして, それらが図でピンク色の○で示した一点 (県 NOC (POI) と呼ばれるところ) に接続されています. 県のサーバも同じように県 NOC に接続されています. そして, 本人確認情報が県のサーバに集められます. 県はこの集められた本人確認情報の運用を地方自治情報センター (全国センター) に委任していて, この委任に基づいて全県民のデータが全国センターのサーバに送られます.

審議会では, 本人確認情報保護についての次の４つの問題を指摘しました.

①各市町村のインターネット側から市町村の中にある住基サーバが攻撃をされて、そこにある本人確認情報が漏えいしてしまうのではないか.

②市町村にとっては上位の住基ネット側から何らかの不正なアクセスがあって、その市町村のCSなり市町村の既存の住基のデータを盗まれるのではないか.

③各市町村担当者に過大な負担をおわせているのではないか.

審議会は各市町村を個々に回らせていただいて、現場の声をたくさん聞きました. これはアンケートのかたちでも聞いてきましたし、現実にその現場に伺って、話を伺ったりもしました. そういう中で、特に小さな町村においては、現場で住基ネットの管理が大変な重荷になっている, 困っておられる現場が現実にたくさんある、そういう現場をたくさん見ました. この状況では、故意ではない人為的なミスで個人の情報が漏えいする危険も考えなければなりません. 現場の担当者の負担をともかく減らさなければいけないと思いました.

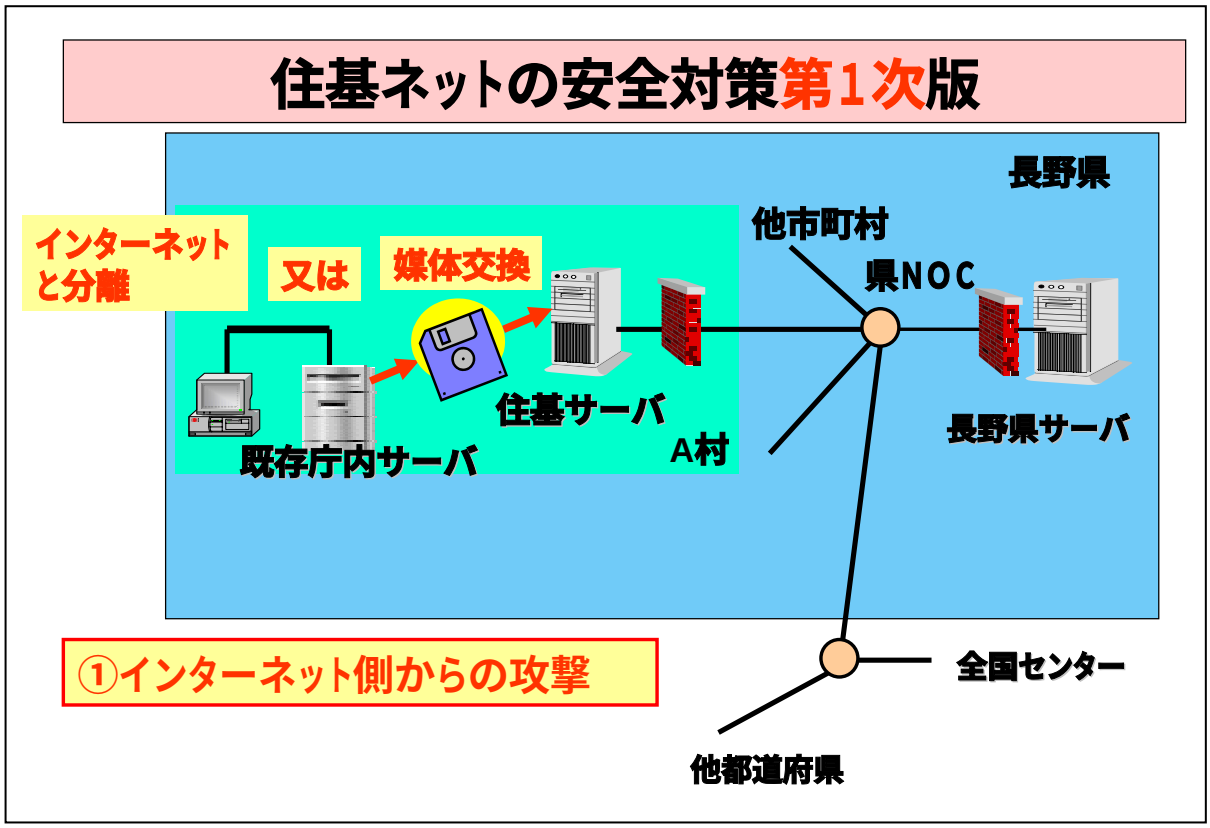
④地方自治情報センターにデータをすべて持っていくという体制が、本当に本人確認情報を守るという意味で正しい選択なのか.

現在分散のデータベース処理が可能な技術があり、長野県のデータは長野県でしっかり管理をして、他都道府県からこの人は本人ですかという問い合わせに対して長野県がイエスかノーかを答える体制を作っても, 住基ネットは成り立ちます. 県民のデータをそっくりそのまま全国サーバに上げる必要があるのかということを考える必要があります. もちろんそこには費用対効果という話も出てくるでしょうし、どういう形が最もセキュリティ上安全でコストもリーズナブルなものになるのかということをしっかりと検討をしていくという必要もあろうかと思います.

審議会では, その後県内10カ所で説明会を開催し, 1200人以上の人にご参加頂きました. そして, 300を超える多くの質問や感想を頂きました. そのなかに, 危険性はよくわかったが, 具体的にその解決方法についての案を提言してほしいという意見が多くありましたし, 私たちも解決方法を検討してきました. それを, 8月の審議会で正式に県に提出しました.

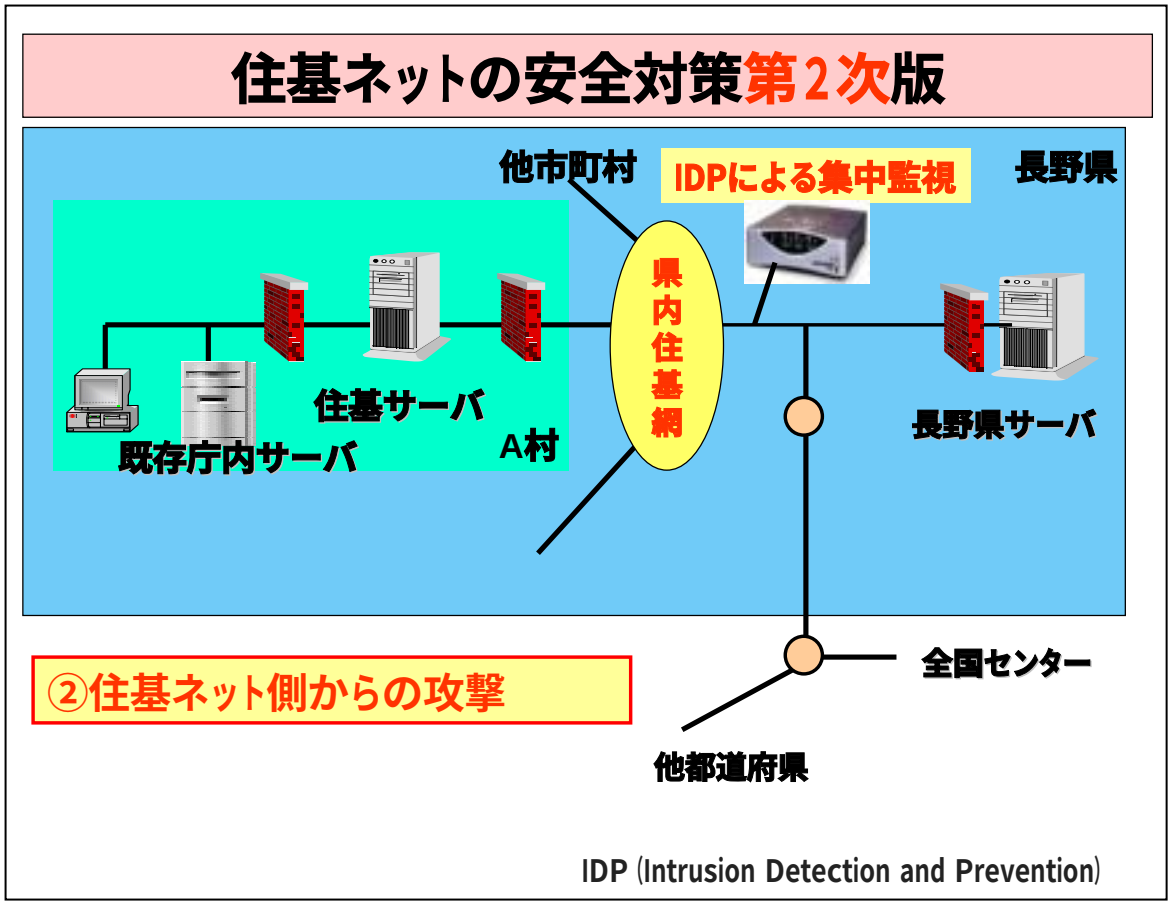
対策は，この4つの安全性の問題点を順次解決しようというものです．

(1)インターネット側から個人情報が攻撃される問題について（安全策第1次版）



抜本的には市町村のネットワークの構成を変えてインターネットと庁内のサーバとを分離する必要があります．又は，それが出来るまでの間は，庁内サーバと住基サーバとの接続をやめて，フロッピーディスクなどの媒体を使ってデータ交換を行おうというものです．

(2)他の市町村から住基ネットを通って市町村の個人情報が攻撃される危険について（安全策第2次版）



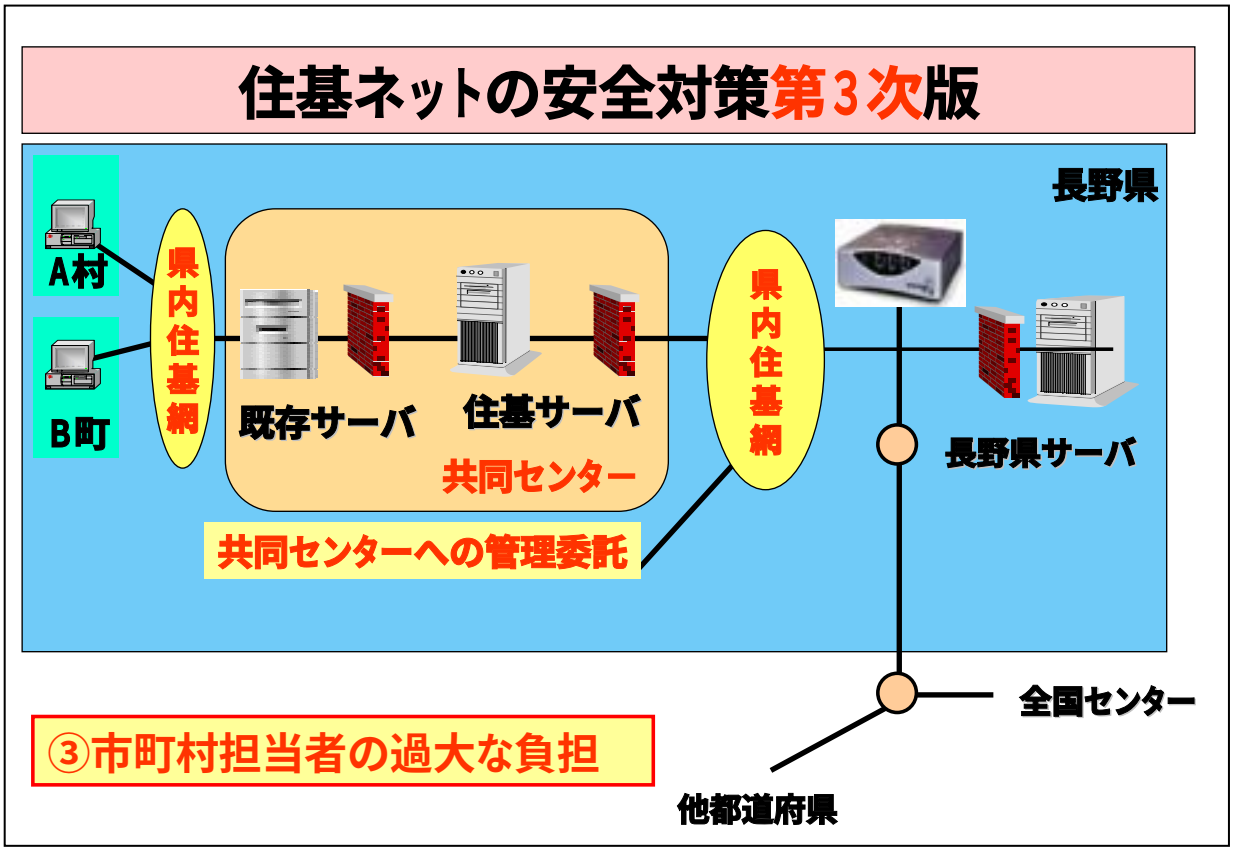
2003年8月に全国でブラスタと呼ばれるウィルスが問題になったときに，長野市がこのことを懸念して用心のために一時的に住基ネットを切断しました．

各市町村が安心出来るように，県は県 NOC から各市町村に繋がる経路上にIDP，IDSと呼ばれるネットワーク監視装置を設置して監視すべきです．審議会ではこのIDP、もしくはIDSの必要性について、既に5月の報告書の中で、これを各市町村に置くことを提案しています．IDSを置いて、それを相関分析ができる人間も配置して24時間監視します．

現在のネットワーク構成では，県 NOC から各市町村まで線が1本ずつ出ています．このため，各市町村までの間の1本1本についてこのIDP，IDSを置いて、全ての線を監視しなければいけません．そうすると、装置は120台必要となり，試算すると5年間で80億という経費もかかることを5月の報告書で述べています．

県のネットワーク構成を変えてより効率的に監視がきるようにすることが第2次版です．県内の地域ネットワーク網をセキュリティに十分配慮して構築し，その大元のところにIDPを1台置きます．

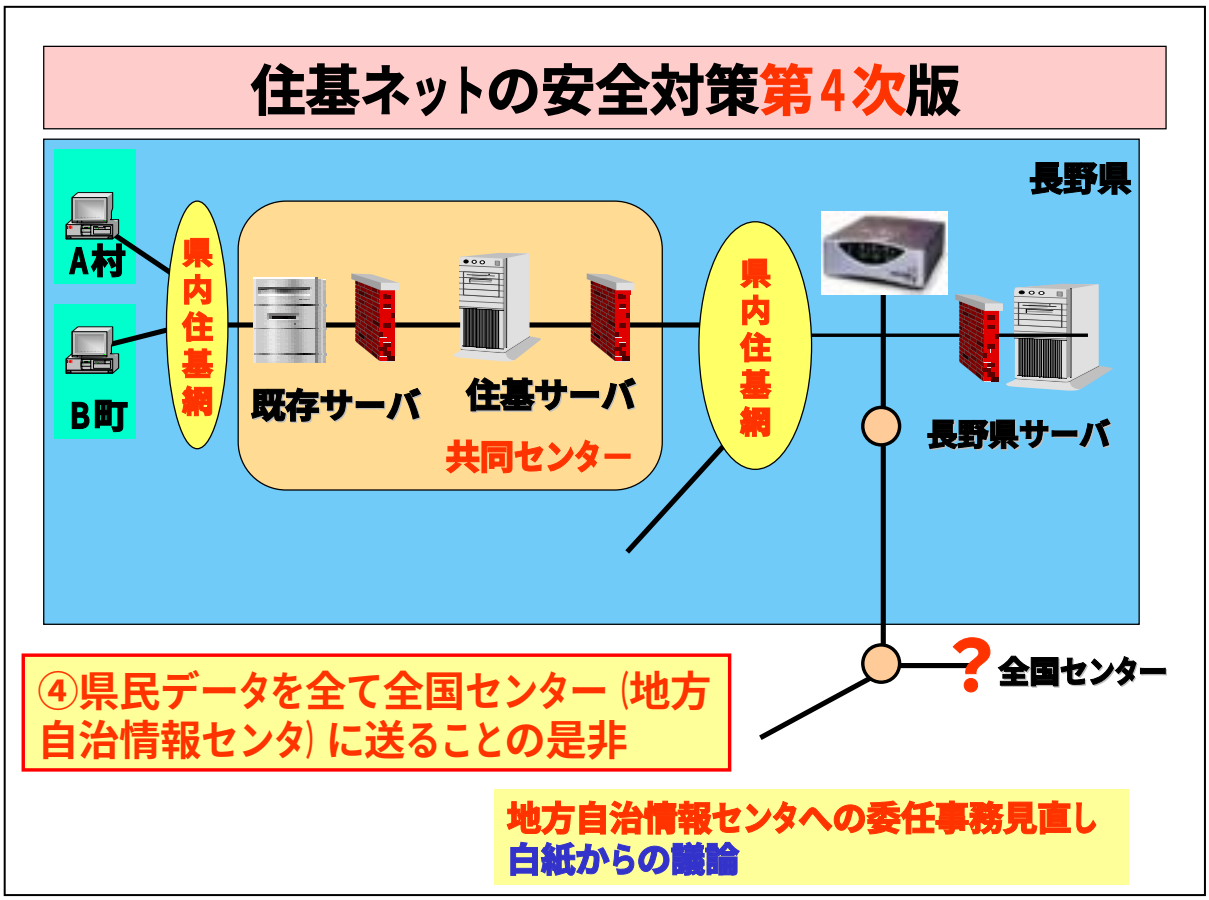
(3)各市町村の住基ネット担当者が過大な負担を負っている問題（安全策第3次版）



市町村の方々は，大変忙しい仕事のなかで何とか住基ネットを安全に運用しようと，必死に分厚いマニュアルと格闘しておられます．しかし，過大な負担の中での無理な運用が続き，操作ミスによる個人情報漏洩の危険があります．心配で夜も寝られないという担当者もおられます．

このことを解決するために，セキュリティの専門家を備えた共同センターをつくって，そこに住基ネットの機器を預け，その管理を委託するという方法が安全策3次版です．市町村には住基の端末だけが設置されます．

(4)国（地方自治情報センター）に全ての情報を上げる方式が良いのかどうかという問題（安全策第4次版）



県に集まった県民情報を用い，国や他の都道府県からの本人確認の問い合わせに答えられるように県が運営することを法律で定めています．その時に，県が独自に運営出来ない場合は，国が指定した地方自治情報センターにその運営を委任することができることになっていて，長野県をはじめとする都道府県は全て地方自治情報センターに委任しています．でも，これはかならず委任しなければならないということではありません．　県が独自に運営してもよいのです．そこで，本当に委任した方がよいのか県が運営したほうがよいのか，情報の安全性やコストといったいろいろな観点からきちんと白紙からの議論を市町村とともにしましょうというのが，審議会の考えです．

安全策の進め方

安全策については審議会でも何度も繰り返し発言していますが，1次（インターネットからの分離）はほぼ完了しています．残りの2，3，4次の安全策については，たまたまこのような順番で番号を振ってありますが（番号はこの順番で説明すると理解して頂けやすいと思った順で付けました），それぞれの策は基本的には独立していて，出来るところから順次，そして可能であれば並行して実施していただきたいと考えます．また，全ての実施がたとえ出来なくても，他の実施出来

た部分で確実に住基ネットの安全性は向上します.

3-2.　県事務への住基ネット活用に当たっての安全性確保

県が県の事務サービス提供のために、住基ネットを活用して、住民サービスの向上と事務の合理化をすすめるにあたっては　最大限の安全対策を講じる必要がある.

審議会では、市町村が住基ネットをより安全に運用するためには国の提示した142項目のセキュリティチェックリストの遵守だけでなく、セキュリティ監査や侵入テストによる安全性確保の必要性があると示してきたが、県事務での活用においてもそのことは当然であると同時に、それらに付け加えて、県固有の環境に合わせたセキュリティ対策が別途必要である、として以下の対策を提言してきた.

運用開始に当たっては、これらが１００％対応できるシステム環境の構築と、該当する職員への十二分なセキュリティ教育と運用指導の徹底をはかり万全の体制で臨むとともに、定期的な内部監査、外部監査により安全な運用管理に努めているかを常時チェックしていく必要がある.

(1) 技術面での対策

1)　県住基サーバと県現地機関に設置される住基ネット業務端末間を接続する通信網の安全対策をはかる.

インターネットからの独立は当然として、住基ネット以外の他の県事務ネットワークとも論理的に完全に独立した回線とし、送受信データは暗号化する. なお、役所本庁にて CS サーバと CS 端末を同一 LAN 上で接続している自治体では問題ないが、支所に CS 端末を設置する大規模自治体では CS サーバと CS 端末間通信に同様の対策を施すことで、より安全性が増す.

2)　住基ネット業務端末のネットワーク的な安全対策をはかる.

現地機関の庁内LAN上に業務端末を設置する場合は、その庁内LAN上の他の端末から業務端末への一切のアクセスを不可能にするために業務端末に特殊な機構を装備する. これにより、万が一庁内 LAN 上にウィルスやワームが侵入しても業務端末には届かなくなる.

3)　住基ネット業務端末の操作者限定を強化する安全対策をはかる.

操作者個人専用のICカードとパスワード運用を徹底するとともに、本人以外の操作防止策をより強化するために、操作者の生体認証システムを導入する.

4)　住基ネット業務端末からの情報漏洩を防止する安全対策をはかる.

住基ネットプログラム以外を動作不能にするとともに、外部補助記憶装置の無効化、画面コピー機能の無効化を OS レベルで設定する.

5) 住基ネット業務端末のソフトウェア資源一元管理で安全対策をはかる.

ＯＳのセキュリティパッチやウィルス対策ソフトの最新パターンファイル等を迅速かつ確実に適用、反映させるため、リモート操作が可能な業務端末運用支援ソフトを導入し、ソフトウェア資源の一元管理を図る.

6) 各機器のログ解析による不正アクセスの検出で安全対策をはかる.

ＯＳに対するログオン失敗履歴、ファイアウォールログ、業務端末の操作履歴を記録し、解析に利用する.

(2)運用面での対策

1) 住基ネット利用に関する業務別の要領を新たに定め、本人確認情報の適切かつ確実な保護を図る.

2) 操作用ICカードは業務開始の都度事務利用責任者が利用者へ貸与し、業務終了時に返却する. 事務利用責任者はICカード使用簿で、貸与と返却を管理する.

3) 端末操作者は操作の都度、端末使用管理簿に利用日時、利用者、本人確認情報検索件数等を記録する. 事務利用責任者は、住民からの申請書と使用管理簿を突合して業務外検索の有無を確認し、システムログの本人確認情報提供件数と使用管理簿を突合して業務外検索の有無を確認する.

どんなに優れたシステムをつくったとしても、それを運用する人次第で情報漏洩してしまう危険性があるならば、その人の面に注目して可能な限りの対策を講ずるべきであり、県下市町村が管理主体である住民の個人データを利用させてもらう県であるから、その安全性確保には慎重すぎるほどの準備をするべきである.

今後県の事務サービスの電子化が順次検討される場面も出てくるであろうが、電子化にあたっては、費用対効果や住民のニーズを十分に勘案するとともに、そのことにより個人情報の漏洩が発生しないよう、慎重なシステム設計をしていくべきである.

4－2.　櫻井よしこ委員

長野県の本人確認情報保護審議会の委員となって二年がすぎた。今回の審議会が最終回となり、 一連の調査と議論はひとつの区切りを迎える。振り返ってみればこの国の個人情報の扱い方、使い方、護り方についてさまざまな面で大変貴重な勉強をさせて貰ったと思う。全国の四七都道府県のなかで、長野県ほど住基ネットの抱える問題について詳細な調査を実施し、県下の市町村の担当職員の意識を問い、現実の事務処理のなかの問題点を洗い出し、コストを計算し、導入のメリットとデメリットを明らかにした県はないだろう。

日本全国の自治体を結ぶコンピュータネットワークのなかに国民全員の個人情報を入れていくということの恐ろしさとは対照的に、調査を始めてみて実感した、そのような仕組みを実際に作り上げていく地方自治体側の無意識と無防備には驚かざるを得なかった。

たとえば、県下の一二〇の自治体のうち二七の自治体の住基ネットがインターネットにつながっていた。 審議会はただちに長野県に対して対策を取るよう要請、県は回線の切り離しなどについて業者に見積もりを出させた。にもかかわらず、その状態は尚、長く改善されなかった。理由は切りはなしコストが高額で、各自治体の財政事情から、コスト負担は無理と判断され、結果として回線はずっとつながっていたのだ。

巧まずして、インターネットと住基ネットがつながっていることへの危機感の欠如と、たとえ、危機感を抱いても経済上の理由で対処出来ないという自治体側の財政事情が浮き彫りにされた。県下の市町村の実態は日本全国の市町村の実態でもあり、問題の根深さが明らかになった。

長野県下の市町村は県の指導によってやがて殆んどがインターネット回線と住基ネット回線を切りはなした。一連の長野県での動きは総務省及び地方自治情報センターに対しても教訓を与え、全国の自治体の住基ネット体制の改善につながったと思う。

それにしても、住基ネットに登録される私たちの個人情報がどれほど危うい仕組みのなかに入れられていることか。この点については審議会で多くの時間を費し議論した。最終的には住基ネットへの侵入実験も行った。技術面の説明は吉田柳太郎委員の説明を読んでほしいが、結果は、ファイアウォールは通過されてしまい、ファイアウォールによって情報は守られているとの総務省の主張が誤りだったことが明らかになった。

だが、総務省側は、住基ネットの脆弱性を決して認めようとはしない。
総務省は住基ネットに関しては、当初より、その仕組みは地方自治体の側からの要請で構築したものだなどとの事実に反した主張を展開してきた。ファイアウォールについても、彼らは破られたなどとは決して認めようとはしない。それでも、事実はひとつしかない。総務省が大丈夫だと言ったファイアウォールは、確かに破られ通過されたのだ。

審議会にとって予期せぬことだったのはこの侵入実験の結果をメディアがどう報じるかだった。メディア、特に地元のメディアはこのことを正しく報じなかった。というより、住基ネットの中のファイアウォールの構造上の問題についてそもそも報じなかった。その

うえで、批判のための批判と言われても弁明出来ないような報道を展開した。典型は『信濃毎日』である。同紙は「県の実験　説明不足」「市町村の県不信拡大」「田中県政に改善迫る」などの見出しを掲げて、侵入実験の詳細よりも田中知事への批判を軸に報じ、ファイアウォールが通過されたという最も重要な事実を無視したのだ。

これらの記事は信じ難くも目に余るものだった。このような報道が先行するのでは、県民に住基ネットの真の問題点が伝わることもないだろうと思わざるを得なかった。

住基ネットの脆弱性と共に、経済的な不合理性も審議会の調査で明らかになった。住基ネットの運営には、県全体で毎年五億円を超える経費がかかる。それだけの費用をかけて住民が得る利便性は、住民票を住居地域以外の自治体で取得出来るなど、およそ評価し難い事柄である。住基ネットは利便性とコストを計算すれば、経済的に見合わないということだ。

こうしてみれば、住基ネットは問題の塊りだとさえいえる。まず、情報を守ることに技術面の大きな不安が存在する。常にセキュリティレベルを上げ続けなければならず、膨大なコストがかかる。住基ネットの利便性は引越の際の住民票提出やパスポート申請時の住民票添付の省略程度にとどまる。こうした状況だからこそ、現場を知る職員であればある程、住基ネットの導入に反対していた。

もうひとつ指摘しなければならないのは、住基ネットが炙り出す総務省と自治体の関係だ。地方分権や地方の自立が必要だと言われながら、住基ネットは従来からの中央政府と地方自治体間の哀しくも隷属的な関係を象徴しているのではないか。

この仕組みは周知のように総務省の押しつけによって導入された。地方自治体にコストと人手と苦労を押しつけるにすぎないものだが、結局、殆どの自治体が唯々諾々と受け入れた。中央政府への精神的従属現象が全国でおきるなかで、長野県が当初、そのような押しつけも制度も拒否したいと考えたとしても無理からぬことだったと思う。むしろ、私は国の指示に無条件に従うより、疑問をもって立ち止まろうとした長野県の在り方は健全だと考えた。

長野県のジレンマは、しかし、県が住基ネットを離脱すれば、県下の市町村が取り残されてしまうという実態である。

そのこと故に長野県は現実的な打開策として、いま、住基ネットのセキュリティの向上に力を注ぎ、遂にはパスポート発給での利用を考慮中だ。いずれも弥縫策にすぎず、本質的な打開策とは程遠い。弥縫策が近い将来、綻びをみせることは十分に考えられる。にもかかわらず、住基ネットを現実的に受け入れていかざるを得ない県の現状は、二年間の審議会を振りかえれば意外というしかないというのが、私自身の感じ方である。

住基ネットは住基カードの普及と共に、広く国民に活用されると説明されてきた。しかしその普及率は県下では〇・二三%にとどまっている。九九・七七%の住民が住基ネットにソッポを向いているのだ。圧倒的多数の住民が住基ネットは不必要と考えている証拠であろう。同制度が活用され、定着することもおそらくないだろう。となれば、この仕組み

に税金を投入して維持していくことの是非を、根本から考えなおさなければならないと、私は強く思う。

安全性、利便性、有用性と共に、このシステムの非経済性、危険性、非合理性をも考慮し賢い決断を導き出すことだ。県全体の議論をもう一歩も二歩も突っ込んで行い、住基ネットにとどまることの是非を真正面から論ずることが重要だと強調して、私の感想としたい。

4－3. 佐藤千明委員

(1) 公開討論会により明らかになった、住基ネットの安全性と市町村の責任

2.2 (4)にあるとおり、国との公開討論会が開催されたが、この討論会のやり取りを通して、IT化への大きな流れの中で、そのネットワーク社会を構築するためには、ベースとなる個人情報を管理する現場の市町村が管理責任を果たせるかどうかが鍵を握っていることが明らかになった. 国が安全性を国なりの監査で確保できたという範囲は中核部分でしかなく、そこに繋がる 3000 以上の市町村ネットの安全性は各市町村の費用と責任で確保することが要求されているのである. 以下、当日の討論内容を整理してみる.

「住基ネットの範囲は」に対して、「全体として、CS、ＣＳ端末を含めて住基ネットの範囲である」との回答.

「ＣＳ, CS端末まで含む住基ネットが安全であるというのであれば、ＣＳ, CS端末の安全性をどうやって確認しているのか」に対しては、「LASDECではCS、CS端末の管理、監視は行っておらず、そこは市町村の管理責任である」、「市町村がチェックリストで全てをチェックしている」との回答.

これにより、国が住基ネットは安全だという根拠は、市町村による管理、市町村によるチェックに依存していることが明らかになった.

そこで、「市町村現場を見て全く問題がないところばかりだったのか」に対しては、「問題のない団体は少なくない」、「チェックリストで様々な団体において不十分なところについてはチェックをしていただいています」との回答.

問題のある団体が存在することとなり、国の言う安全だとの根拠は崩れてしまった. 国の言う安全はＣＳより内側のネットワークに限定され、国の定義する住基ネットを安全にしていくためには、全市町村がＣＳやＣＳ端末を自らの費用と責任において維持･管理していく必要があることを意味している.

そこで、次に、市町村が管理する CS、CS 端末を含む庁内 LAN の安全性、インターネットから CS への侵入の危険性、ＣＳ内データ保護に関して討論.

「インターネットからの侵入でファイアウォールを越えて庁内 LAN や CS までアクセスされる危険性があるはず」に対しては、「アクセスはできるがちゃんと設定されているのでそれ以上動かない」との回答.

ならば、その設定は LASDEC の責任で実施したのでしょうか、各市町村任せであり、設定内容も確認していない国がなぜその設定が正しいと保証できるのでしょうか. それこそ仮定の話です. そして、後の県による試験により、庁内 LAN とＣＳ間のファイアウォールに不要と思われるポートが開放されていたり OS が古いままでシステム的な脆弱性が存在することが判明し、「それ以上動かない」との断定は極めて怪しくなった.

「ソーシャルエンジニアリングにより情報を積み上げて僅かな侵入経路を作り出せるが、このレベルの問題は地方自治体運用では考慮されていないのではないか」に対しては、「技術的な問題を内部犯行にすり替えましたね、セキュリティをやるからにはきちんとしましょう」と、県が出した市町村アンケート結果の回答数の細かな記入ミスを指摘しただけで、ソーシャルエンジニアリングの危険性には一切の回答なし. 総務省のホームページ資料でも全てが100%になるわけではなく、些細なことで肝心な議論のすり替えをして来られたのには参った. そこでまたファイアウォールの安全性議論に戻す.

「ファイアウォールがあっても内部のパソコンやサーバにセキュリティホールがあればインターネットからの侵入ができてしまいますね」に対しては、「ファイアウォールがきちんと設定されていれば守れるはず」との驚くべき回答. セキュリティの専門家が口にする言葉ではないことを百も承知で押し切ろうとする. 国の委員である小川さんにこの発言を聞いていただきたいものである.

「設定が 100%正しいかどうか、セキュリティ監査をしたことがあるなら監査結果を公表してほしい」と迫ると、「監査の結果、ここにセキュリティホールがあると公表すると皆さんそこからハッキングするので公表できない」との回答. ということは、仮になかったのなら結果を公表しても被害は出ないはずで隠す必要はありませんから、セキュリティホールがあったということになります.

また、インターネットとの間のファイアウォールを議論しているのになぜか「LASDEC が監視しているファイアウォールと全国サーバについてのネットワーク分析ツールを用いての監査は実施済で、脆弱性は発見されておりません」と、国の監視対象範囲の安全性を自賛するだけ. 「市町村に管理責任のある庁内 LAN 部分は業者丸投げでその仕事内容のチェック機能がない実態なのに、そこに足を運ぶことなく現場を知らずしてネットワークを語ることは無責任」であると指摘.

「国がシステム監査で安全性を確認できた部分以外の市町村管理部分の運用管理がきちんとされていると判断されますか」に対しては、「住基ネットにいかなる具体的な危険性があるか指摘してほしい」との回答で、議論がかみ合わない. 「アンケートによればセキュリティ確保のための 8 項目をちゃんと実施しているし、市町村のネットワーク管理者はそんなに馬鹿ではありません. また担当者のレベルも上がってきており、セキュリティ意識も高くなってきている」とのご認識. 国と県には、現場の実態に関する認識に乖離があり、実態を知る県としては、「いくらセキュリティ意識が高くなったとしても現実にインターネットと接続している市町村が全国で 813 にも上っている現実がある限り市町村のセキュリティは担保されない」と主張する.

「総務省は市町村が望んだものだというが具体的な市町村名を挙げてほしい」との質問には、「地方公共団体六団体から要請があった」との回答のみで、最後まで具体名を挙げられなかった.

安全性云々について抽象的な議論が続いたので、「インターネット側と内部側とソーシャル

エンジニアリング側の 3 方向から、国と県が一緒に、公開で侵入テストを行う」、「国が安全だと監査できていない部分、即ち、セキュリティチェックリストでまだ対応できていない項目が沢山残る市町村 LAN 部分の脆弱性検査を一緒にどうか」と提案するも、「業者が実施したファイアウォール設定が国の指示どおりになっているかを内部監査するのが先、職員のレベルが低くて監査できないならセキュリティ教育から始めなさい、侵入テストはその次です」とテスト提案に応じない回答. そこで、「2,3 年ごとに人事異動があり、業者任せにせざるを得ない地方自治体の実態を知らない机上の空論であり、そのような脆弱な市町村環境をベースとした住基ネットの仕組みはボロボロである」と指摘する.

「住基ネットの安全性を確保するには、それぞれのシステムから吐き出されるログ情報を 24 時間フルタイムで相関分析すべきであるが、現実にはコストがかかってできていない」との指摘に対して、「費用対効果を勘案すれば、本当に守らなければならない個人情報は何でどこにあるかを議論すべき」との回答. CS サーバ内にある 6 情報よりも庁内 LAN のパソコンやサーバ内にあるセンシティブな個人情報保護を優先すべきとのご意見であるが、だからといって 6 情報を軽んじていいはずはないのである.

国側から、「住基ネットの危険性が現実化しているとの指摘であるが、具体的に示してほしい」との質問があり、「監視していない部分で何も問題がないとどうして言えるのか、宇治市のケースもローソンのケースも、問題が発覚したのは 1 年くらい後である. ディジタルデータはコピーされても気づかないことがあり得る」と回答するも、国側は「両ケースとも内部犯行、人間の問題であり、住基ネットのネットワークそのものの問題とは関係ない. 住基ネットでは内部犯行への手当てをしている. 更に、全国センターではＩＤＳ等により不審なアクセスはログでわかる. 一朝一夕で全ての情報が取られるわけではない」と、国が監視している部分の安全性を強調するが、現時点で県はその部分の安全性を確認する情報を持ち合わせていないし、国も監査結果を公表していない.

「世界に向けてモノを発信しにくい現在、日本は知恵を売らなければならないが、そのためには、ネットワークを整備しその上にコンテンツを載せていく必要があり、その環境整備のための先行投資である」と、ネットワーク整備の意義を説明されたが、その方向性認識に差異はない. しかし、住基ネットの安全性議論を一般論としての IT 化賛成論にすり替えてしまっている.

国は、「インターネットと庁内 LAN、基幹系 LAN は、例えば民間企業であれば銀行でも全部繋がっています. 繋がっているから直ちに危険ということではなく、いかなるセキュリティ対策を講じていくかが重要. 住基ネットでは市町村の住基ネットを通って他の市町村へ侵入することはできない. また庁内 LAN の安全性議論は住基ネット以前からあり、様々な情報を守ることは大事である」と主張. 一見同意できる内容もあるが、銀行オンラインのサーバがインターネットと「直接」つながるはずはなく、ネットワーク担当者はインターネットと接続している LAN セグメントのセキュリティ確保にどれほど留意して努めているか、インターネットとの接続に関する危険性認識が甘い. また庁内 LAN まで含めて住基ネットという共通認識に立っているのであるから、庁内 LAN のセキュリティ確保を市町村任せにしてはいけない.

国:「具体的に住基ネットの危険性を指摘してほしい」

県:「800 を越える自治体でインターネットと庁内 LAN が繋がっている事実です．それが安全だというのであれば一緒に侵入試験をやって確認したい」

国:「第三者の監査法人によって安全性は確認済みである」

県:「ならば、その監査結果を公表してほしい」

国:「ファイアウォールの監査をしている．セキュリティ監査で今まで公開している例はありますか」．

監査対象がどこのファイアウォールか不明であり、更には、脆弱性はファイアウォールの設定だけでなくそれを越えた相手側ＬＡＮセグメント内のパソコンやサーバのセキュリティレベルにもある．監査概要すら公開されないのでは、安全であるとの発表は信用できない．長野県ではこの後独自に市町村の協力を得て1自治体でインターネットからの侵入試験を実施したが、ファイアウォールが侵入を防いだのではなく、内部のサーバのセキュリティホールが当時としては完全に塞がれていたことによりなんとか庁内 LAN を守れたという事実であり、どこかのファイアウォールの監査で全国の住基ネットの安全性を担保できるものではない．

県:「試験について、公開ということについて形にはこだわらない」

国:「あくまでも第三者的にきちっとしたところで、要はどういうふうに監査をするか、そこの基本的な部分が必要であると、そういうふうな対応は取らせていただいております．」

県:「はい、そうです．じゃあ、それをやってくださることが決まりました．」一歩前進した．

国:「住基ネットの議論と庁内 LAN の議論を分けていただきたい．住基ネットのセキュリティは極めて高めているので、もしそれが危ないとするなら、住基ネットよりも前に市町村の庁内 LAN が危ないことになり、そうならば、住基ネットを止めろという議論の前に先ずこの市町村のシステムを全て止めなければいけない．」、「霞ヶ関の部分にも個人情報はあるが、市町村システムのレベルが上がっていくのかどうかがより重要である．」

庁内 LAN の安全性確保が焦点であることまでの認識では一致した．が、住基ネットにより庁内 LAN が全国的な繋がりを持ったことにより、そのひとつの庁内 LAN の脆弱性が持つ危険性がどれほど増すか、ネットワーク化に対する危機意識に大きな乖離がある．それは、国が監視対象とする住基ネット中核部分の安全性に対する認識の差から来ているが、県としてはそこの安全性確認試験はまだできていない．何の情報もなく、安全だから信用しろ、には従えない．

国:「これからはモノではなくて、コンテンツが重要となる．長野県には軽井沢もアルプスもあるので、もっともっと情報発信して引きつけたらどうでしょう．住基ネットの一番の問題は、要するに認証をすること．認証をしないとインターネットのサービスは受けられない．それでもやめますか」

最後になって、個人認証基盤として住基ネットが必要である、との発言が出た．非常に重要な内容だが、残念ながら今回の討論会ではこの意義について十分議論する時間がなかった．インターネットサービスの内容を国民はどこまで期待しているのか、個人認証システムに住基ネットは必須であるのかどうか、そこをしっかり吟味する必要がある．

県側からまとめとして、「CS から上位の脆弱性には言及していない．CS サーバとそこにつながる庁内ＬＡＮの脆弱性を問題視している．特にインターネットと接続されているケースは試験が必要である．住基サーバやＣＳ端末と CS 間にはファイアウォールがありきちんと設定されているとの説明であるが、仮にＣＳが乗っ取られると正々堂々と全国の住基ネットの中に行けてしまう．従って、市町村ＬＡＮの侵入試験をやって市町村 LAN も安全であるということを確認した上で、住基ネット全体の安全性を評価していきたい．是非とも一緒に試験をやらせていただきたい．」と再度要請．

それに対して国側から、「公開の場でみんなの前で試験することはできないが、監査はどんどんやっていけばいい．ただし、ネットワークを止めるということではなく、セキュリティレベルを上げながらネットワークをどんどん大きくして発信を続けようということである．」「ネットワーク化によってひとつの市町村の影響が他の市町村に及ぼすという議論だが、CS のセキュリティ確保には取り組んでいきたい．ただ、やはり庁内 LAN をいかに守るかは第一義的に市町村にきちっと責任を持ってもらい、国はこれに対して全面的にバックアップしてゆく．」

国は、庁内 LAN の安全性確保は市町村の責任であると明言した．市町村の責任は重大である．そこまで言うのであれば、規模の大小を問わずに、全市町村が責任をもって庁内 LAN の安全性を確保できるよう国には支援する義務と責任がある．できないことをやらせてはいけない．できていない実態があるならば、それを認めて、国の責任で改善策を提示していく必要がある．

県側からの「公開方法はともかくとして、やはりペネトレーションテストはやったほうがいい」との再度の提案に対して、国側委員から「問題があるという状況ではないが監査は必要だ．ペネトレーションテストも必要だ．それは正しい．ですから全ての市町村についてどう監査をしていくかについて議論したい．なお、いまだにインターネットに繋がっている市町村があることについては憂慮しており、随分責めました．その結果年内には全てが3の対策済レベルになることだけは確保してあります．」との回答．

ペネトレーションテストの必要性も、インターネットと接続している危険性も国側委員のお一人は認めたのである．これは非常に大きな成果であった．なお、平成 15 年末時点で全てが3になったとの報告はまだ受けていない．

(2) 国も、地方自治体も情報セキュリティ意識と個人情報保護意識を身体に覚え込ませよ

住民の個人データを預かる各自治体は、中途半端なセキュリティ対策のまま住基ネットを運用することは個人情報保護やプライバシー保護の観点から許されない状況にあることを再認識して運用に当たっていただきたい．その結果として、責任ある安全対策を講じることができない状況

になった場合には、システムのあり方を根本から見直すくらいの勇気と決意をもって、住民の個人情報保護に努めていただきたい.

システム的技術的対策を施して庁内 LAN の安全性確保に努めることは当然であるが、加えて、運用面での対策として職員の情報セキュリティに関する研修や徹底が必須であり、戸籍・住民係だけでなく、自治体職員全員が住民データ保護の重要性を再認識する必要がある. 個人情報保護は国民的課題であり、それを破る最大のセキュリティホールが人なのである.

なお、このように全国の地方自治体の情報セキュリティ対策の上に成り立っている住基ネットであるからして、情報セキュリティの重要性を最も認識していなければならないのは、いうまでもなく主管である総務省である. 現場の実態を自らの目で調査し、どこまでのセキュリティ対策ならば現場が受け入れ可能かを把握した上で、住基ネット運用の安全対策指導をすべきであり、存在する脆弱性を隠すことにより安全性を確保しようとする姿勢は「臭いものにふたをする」発想でしかない. 脆弱性があることを認識し、その解消にどの程度の費用と時間と人員が必要となるかを分析し、できない対策は強要せずに、脆弱性があることを前提とした新たな運用案を提示すべきである.

情報漏洩は 100%阻止すべきであり、住基ネットは、「多少漏れてもいいから走りながら考えよう」、という性格のシステムではない. これだけインターネットやパソコンソフトウエアの脆弱性が叫ばれ、ソーシャルエンジニアリングという人間の心理の弱点を突いたアタックも大きな問題となってきたネットワーク社会では、従来型の性善説に立脚した対策では生ぬるく、管理責任を果たすためには性悪説に沿った対策を講じていく必要があり、総務省はそのために全面的な支援をすべきである. 市町村の庁内 LAN の安全性検査は国の予算で早急に完全実施すべきである. これだけ続発する Windows のセキュリティホール対策としては、全国の何千という職員による手作業によるパッチ適用に依らずとも OS を自動更新できる仕掛けをマイクロソフトの責任で構築、導入させるべきである.

更には、安全性確認が済むまでは新たなシステム運用を開始すべきではない. 長野県を除く他の全ての県では、公的個人認証システム導入にあたって、委託先である LASCOM の運用実態や運用基準を十分精査することなく総務省の指導により「めくら判」を押してしまった. そしてその LASCOM に納入されたシステムに致命的ともいえる不具合が内在していたにもかかわらず、仕様確認段階でも、納入検査段階でも、運用に入ってからでも、誰一人としてその不具合を検出できず、平成 16 年 5 月末から 2 ヶ月間、電子証明書の発行情報が LASDEC の住基全国センターに通知されない状況が続いてしまった. そして、その障害経過公表要求に対しても当初は、「セキュリティ上」という極めて都合のいい言い訳によりこれを拒絶し、またしても「臭いものにふたをする」スタンスをとった. 大切な国民のデータを 1 箇所に集めて管理するシステムを運営することの重要性をどこまで認識していたのか、地方自治体に一方的なセキュリティ対策を強要する前に、蛇足ながらも、自らの足元を固めることをお勧めしたい.

ファイアウォールがあるから大丈夫とか、国が設計したシステムだから大丈夫という神話は見

事に崩れてしまった．従って、各自治体は、日々、最新のパッチ充てを完全実施してセキュリティホールの縮小に努め、個人情報を漏洩させない組織的取り組みを継続していかねばならない．それが個人情報を扱う組織の責務であると考える．波田町でのインターネットからの侵入実験の教訓は、ファイアウォールが侵入を防止したのではなく、職員が必至になって内部のサーバのセキュリティホール解消に努めてサーバを守ったという事実であり、その絶え間ない改善作業の重要性を物語っているのである．

情報セキュリティポリシーは策定しただけでは不十分であり、全職員にそのポリシーに準拠した行動基準を遵守することを義務付け、定期的な監査も必要である．頭でなく身体に染み込ませなければならない．

- サーバの管理者 ID やパスワードの変更を定期的に実施していますか、まだ業者任せですか．容易に推測できる文字列は使っていないでしょうか．
- 個人のパソコンのログイン ID やパスワードの変更はどうでしょうか．
- USB カードメモリー等でパソコン内のデータを外部に持ち出すことができないシステム的な防御策を講じていますか．電子メールに添付して外部に放り出すことも可能ですが、その対策を始めましたか．嫌なことですが、電子メール検閲も視野に入れざるを得ない時代です．
- Windows の最新パッチを当ててないパソコン動作には、何日の猶予を与えているでしょうか．
- 毎日大量に飛び込んで来るウイルスメールの検出と削除の仕掛けを導入していますか．個人任せにした結果、うっかりミスでウイルスメールが庁内に蔓延する危険性が増します．
- パソコンにワームやウィルス対策ソフトは装備されていますか、その定義ファイルの更新を義務付けていますか．できれば更新状況管理システムを導入すべきです．
- ＣＳ端末のアクセス制御は住基ネット操作者カードとそのパスワードでしか守られていませんが、操作者カードの管理を個人ごとに徹底しましたか、今でも、机の引き出しや共通ロッカーに無造作に置かれていませんか．
- ＣＳ端末の操作ログをどのようにチェックしていますか．
- ＣＳ端末が庁内 LAN から不正アクセスされてないことをどうやって確認していますか．また、国は認めていますが、CS 端末機は基幹系 LAN 上でなく、CS サーバの LAN 上に置くべきです．
- 役場の現地機関にあるパソコン端末から庁内 LAN へのアクセス制御、管理は大丈夫ですか．ダイアルアップ接続に関しては運用時間外のモデム電源オフやコールバック方式や発信者番号チェックなどである程度は不正アクセスを防止したわけですが、今や常時

接続の時代です．LAN 接続可能なコネクタが剥き出しになっていたり、DHCP 運用で IP アドレスを知らなくとも接続できる仕掛けになっていたり、職員離籍時に第三者が不正操作できてしまう危険性はどこまで排除できていますか．

- LGWAN ネットの LAN セグメントと庁内の基幹系 LAN セグメント間の接続はどうなっていますか．今後電子自治体システムが発展し、インターネットからの電子申請や各種問い合わせなどがシステム化されてくると、LGWAN 側から庁内 LAN 上にあるサーバへのアクセス問題が顕在化してきます．情報を守りながら公開していく仕掛けは慎重に設計していく必要があります．住民サービス向上、電子自治体化推進、IT社会という言葉に流されることなく、確実な安全対策を施しながら電子化を検討することです．

これらは庁内LANの運用上の問題であり、総務省が定義する狭義の住基ネットの範疇には入りません．しかし、これらの庁内 LAN の安全性が担保されて初めて、住基ネットの安全性を語れるのです．仮に総務省が言うように CS サーバから上位の県、国側の住基ネット部分がある程度安全であったとしても、肝心の住民データは庁内 LAN 内にあるのですから、その住民データを守る責任は各自治体にあり、総務省はその部分には一切の責任をとってくれないことを念頭に、自らの責任で自治事務を進めていかねばなりません．

(3) 個人認証を必要とする電子行政サービスの開発･運用が鍵

平成 16 年 9 月時点で長野県が取りまとめた住基ネット状況では、住基カード発行枚数が 6,972 件で人口比僅か 0.32%、住民票の写しの広域交付発行枚数が交付地分で 1,186 件、住所地分で 1,213 件、転入転出手続きの特例としての付記転入届けが 18 件、付記転出届けが 11 件である．

また、平成 29 年までの住基ネットの費用対効果試算では、旅券事務を含まない場合には費用累計 97.9 億円に対して効果累計 82.4 億円で、差し引き 15.5 億円の赤字、含む場合でも費用累計 98.7 億円に対して効果累計 84.9 億円で、差し引き 13.8 億円の赤字、となっている．

これらの数字からは、広域交付や転入転出時の手続き簡素化という利用目的だけでは住基ネットを運営維持する価値がない、ということは明白である．一元管理という異次元の成果は見込まれるが、それはあくまでも国側からみた一効能であり、費用対効果を国民に説明できる数字には使えない．

そこで、総務省は途中から住基ネットの存在意義を住民票広域交付から公的個人認証システム基盤に切り替えてきた．電子政府･電子自治体システムを構築し、ネットワークを介して住民が様々な行政サービスを受けられるための電子申請制度の確立であり、そのためには、申請者が本人であることを証明する電子証明書発行が必須となる．既に民間事業者による電子証明書発行サービスは国内においても複数開始されているが、これを使わずに、県知事が公的に証明するサービスとして、各県ごとに公的個人認証局を構築することとしたわけである．そして、その県公的個人認証システムには住基ネットが不可欠であるという論理展開である．住基ネットの利用方法をあとから付け加えてきた．

ネットワーク社会においての電子証明書の必要性は認めるし、その基盤のうえでの電子政府化、電子自治体化という大きな流れにも賛成ではあるが、だからといって、今のすすめ方、手順まで黙認するわけにはいかない.

- なぜ、既存民間認証サービスを利用せずに個人認証局を公的に構築する必要性があったのか.
- なぜ、各県ごとの公的個人認証局運営を全国一律で LASCOM に全面委任しなければならなくなったのか.
- なぜ、LASCOM への委託の可否を判断するための十分な検討時間や情報提供がなされなかったのか.
- なぜ、県公的個人認証システムを単独で運用せず、敢えて住基ネットと連動する必然性があったのか. 後で述べるとおり、必然性の根拠が弱い.
- なぜ、電子証明書格納媒体として、専用の SMART カードでなく、住基カードを活用したのか.
- いつまでにどの行政サービスを電子化するか、その詳細スケジュールは提示されているのか. その計画どおりに進行しているのか.
- 行政サービスを電子化した結果として、どの程度の公務員合理化を見込んでいるのか.
- 受託機関である LASCOM の運用体制をシステム監査する権限が県に与えられているのか.

こういう基本的事項に関して総務省は十分な情報開示をしてきたと言えるのでしょうか. まさか、それは各県の協議会として、県自らが決めた自治事務だとおっしゃるのでしょうか. 他県では LASCOM への委託にあたって、どこまでの安全性審議をしたのでしょうか.

2005 年度末に電子政府･電子自治体が構築されれば、国の事務の 98%で約 1 万手続き、自治体事務の 95%で約 5 千手続きがインターネットで電子申請や文書送付できるようになるとの情報もあるが、その結果どれだけの公務員合理化ができるのか、数値目標を示し、国自らが実行しなければ国民は納得しないし、そもそも肝心の電子申請制度そのものが普及する兆しが見えない限り、「だから住基ネットは必要なのです」という論理は説得力に欠ける. いきなり公務員合理化とまではいかなくても、ネットワークを駆使して縦割り行政を根本から改革できるほどの効果がなければ国民は納得しない.

国税申告を電子化することに敢えて反対はしないが、申告に必要な各種証明書が各機関から電子署名付きで発行されない限り各種証明書を別途郵送する必要が生じてしまう段階では、電子申請が住民にとってどれだけの利便性があるのか判断しかねる.

- 保険会社による保険料支払い証明書の電子発行はどこまで対応できているのか.

- 源泉徴収票の電子発行はどこまで対応できているのか.
- 医療費控除のための電子署名付き医療費支払い証明書はどこまで対応できているのか.
- そもそも税理士などと相談しながら申告額を計算していく過程は電子化によってどうなるのか.
- 一般経費となる物品購入の領収書は SCAN して画像化すれば受け付けてくれるのか.

住民票の写しの交付申請をネットでできるという利用方法があるそうだが、そもそも紙の住民票添付をなくす方向での住基ネット活用であり、電子申請制度導入ではなかったのか. 電子申請が紙の住民票の写しの交付申請程度にしか利用価値がないとしたら、システム化の価値は半減してしまう. それでは折角の投資が無駄になってしまう. 仮に、いつまでも有効活用の見通しがつかない状況が続くようなことになれば、これ以上無駄な投資は継続しない、という判断をせざるを得なくなる可能性が出てくる.

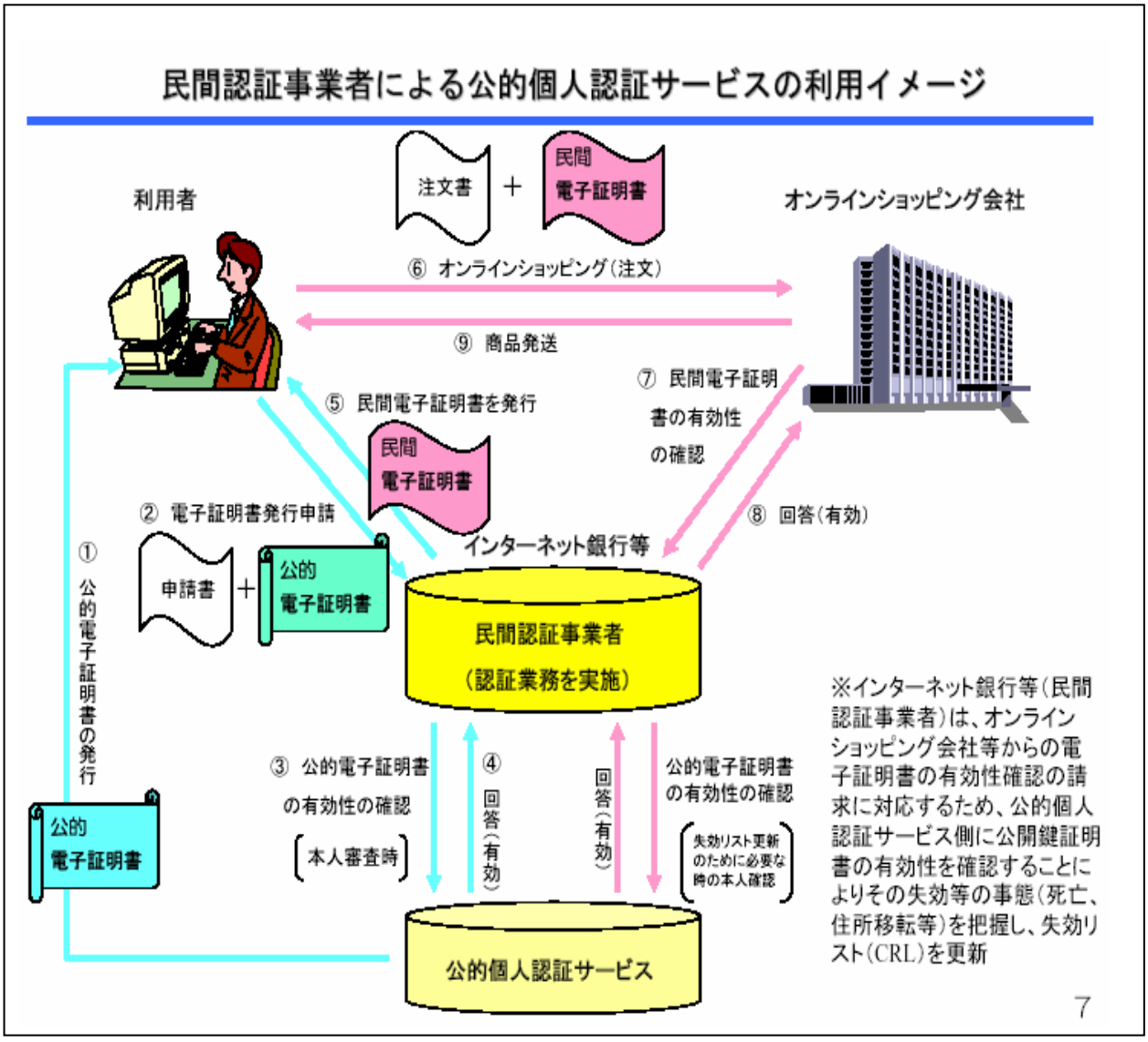
長野県では、パスポート発給申請時の住民票添付をなくして住基ネットで住所確認するシステムを県下各地方事務所に展開するにあたり、その安全性を慎重に検討している段階であるが、公的個人認証システムを利用して自宅からのパスポート発給申請サービスを開始した県もある. ただし、戸籍謄抄本は別途郵送、写真が本人かどうかを確認するためにも受領には本人が役所に出かける必要があり、県民にとってどれほどの住民サービス向上となるか疑問である. その結論は近いうちに利用者数実績が示してくれるはずである.

ちなみに電子証明書発行件数は、平成 16 年 10 月 27 日時点で、全国で 51,979 枚、県内で 357 枚であった. 自治体職員以外の住民への発行枚数がどの程度なのか興味があるが、それ以上に、発行された電子証明書をどんなサービスに利用しているのかが重要である. 紙の住民票写しの電子申請に利用するという笑い話に近い利用はさておき、パソコンに専用の IC カードリーダを装備し、それなりのソフトウェアを組み込んで、一体どんな申請に利用しているのであろうか. 主な利用事例としては、現時点では、所得税確定申告、住民票の写しの交付申請、戸籍謄抄本の交付申請、結婚届･離婚届、市町村県民税所得証明書の発行申請、納税証明書の発行申請、パスポート交付申請、恩給関連申請、社会保険関係手続き、無線従事者免許関連申請、などが挙げられているが、どれも個人にとっては年に数回しか活用の場がなさそうである. このままでは総務省が世界に誇れる高信頼なシステムだとしても、利用されないという意味では世界に笑われるシステムになってしまう可能性もある.

個人がネットワークを介して取引や申請する相手は、役所だけでなく民間会社も想定される. 既に銀行取引、株取引、オークション、通信販売、チケット予約、施設予約、有料映画配信など多くの民間サービスがネット取引可能な時代であり、その取引回数は役所への申請よりも明らかに多そうである.

そのような民間取引においては、申請を受け付ける側の民間会社自体はすでに民間認証局

を利用しているため、申請する側の個人の認証をどの方法で行うかが今後の検討課題であり、下記の図のとおり、公的個人認証システムがそれらの民間認証局での個人認証に利用される可能性が出てきている．下記の②の民間電子証明書発行申請時に公的電子証明書の拡張領域に格納されている氏名、生年月日、性別、住所が公開鍵とともに民間認証事業者に渡るが、万が一、⑤で発行する民間電子証明書にそれらの情報が書き込まれた場合には、⑥にてその電子証明書付きの取引を受け付ける民間企業にも伝わる．（公的個人認証法第 19 条第 2 項において、署名検証以外の利用を禁止していることから発行する民間電子証明書への転記等の行為は法律上禁止されているが、②の申請時に利用者が入力したものを民間電子証明書にて管理することまでは禁止されていない．）



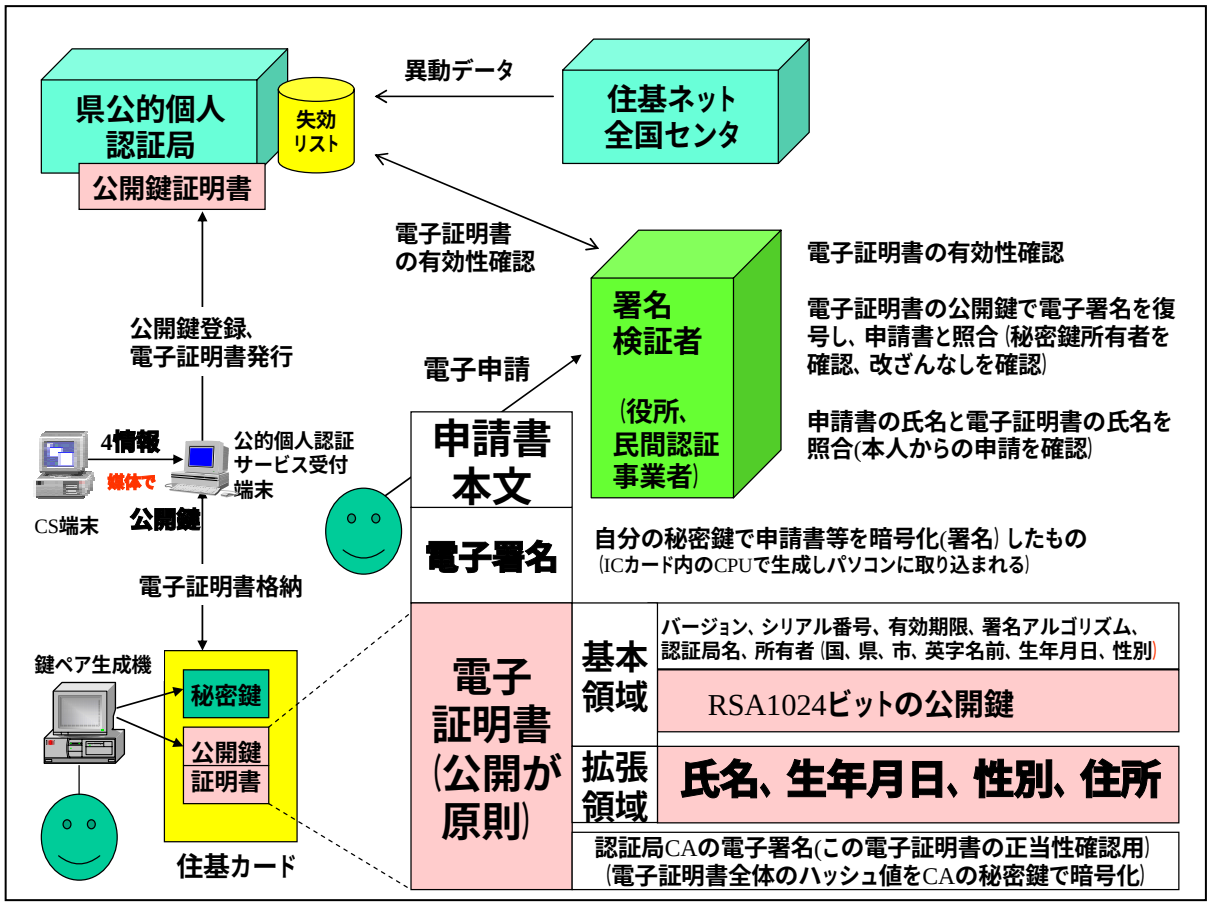
(総務省が公開している公的個人認証サービスの概要 PDF より)

電子証明書であるから公開鍵と最低限の所有者情報は公開、流通するとしても、役所への申請時に必要となる住所、性別、生年月日が、民間認証局発行の電子証明書の拡張領域内で民間の取引においても常に付いて回る可能性があることをどれだけの人が認識しているのであろう

か．役所が役所での活用のために設計した公的電子証明書であるが、民間がそれに準じた運用をすることの是非については、利便性対プライバシー保護という観点から慎重な検討をしていく必要がある．今後民間の電子証明書を活用する人は、その電子証明書内に格納されている情報は秘匿できないものとの認識で臨む必要があり、認証事業者はそのことを十分説明する責任がある．

同時に、住基ネットを前提とした公的個人認証システムの維持管理費に見合うだけの住民サービス向上が可能なのかどうか、さらには、それらのサービス提供にあたって本人確認情報保護が十分に担保されていくのか、今後の展開を注意深く見守っていく必要がある．

(4) 住基ネットは公的個人認証システムにとってどこまで必要不可欠なのか



電子証明書発行者に住所変更、氏名変更、死亡などの異動が生じた場合、公的個人認証システムの認証局 LASCOM では発行済みの電子証明書を失効させる必要がある．その異動情報を市町村にある公的個人認証システム端末から入力する方法と、住基ネットを経由して指定情報処理機関である LASDEC のサーバから入手する方法の 2 通りが考えられ、総務省（形式的には県協議会か）は後者を選択した．

認証局の LASCOM 側から予め電子証明書発行者の基本 4 情報を LASDEC に送付し、LASDEC 内で証明書発行データベースとして管理し、異動等情報が市町村端末から住基ネット

を使って都道府県経由で LASDEC に通知された際に証明書発行データベースに登録済みの基本 4 情報と突合し、一致すれば LASDEC から LASCOM に異動データが通知される仕掛けである.

この基幹となる連携システムは 2 ヶ月間も不具合が継続するという信じがたいミスを犯したが、運用体制も含めて全てが改善され正常に機能すると仮定すれば、市町村担当者の失効登録などの事務処理が少しは軽減され、また、異動情報が速やかに機械的に LASCOM に連動するため、それなりの合理性はある. しかし、あれば便利程度で、公的個人認証システムには住基ネットが必要不可欠である、との論理展開には無理があることも事実である. LASCOM での失効管理のために LASDEC から異動情報を通知することが本質であるので、別の方法で LASCOM の失効管理が実現できてしまうならば住基ネットとの連携は必須でなくなってしまうからである.

そもそも住基ネットに異動データを入力するのは市町村の住民係であり、異動情報を持っているので住民台帳システムでの異動処理と同時に電子証明書発行者の失効登録を公的個人認証システムサービス受付端末から入力するシステムを構築できるはずである. ただ、異動処理をする住民係にはその住民に電子証明書が発行されているかどうか見分ける情報が必要となるので、電子証明書を発行した記録を市町村に残すよう現在の公的個人認証システムを変更する必要がある. また、電子証明書を格納する IC カードとして現在は住基カードのみが利用されているが、住基カードと同等のハードウエア仕様の IC カードを新たに電子証明書格納専用カードとすることに技術的問題はないはずである.

このような議論が不十分なまま、電子政府、電子自治体、電子申請、個人認証サービス実現のために住基ネット、住基カードが必須であるかのような説明がなされてきたことが残念である.

(5) 究極的にはネットワークを活用した分散管理システムを

住民データの国への集中は一部の機関にとっては効率的であるかもしれないが、漏洩時の影響、障害時の影響、目的外利用への危険性の増加という負の要因を含んでいることも事実である. そこで、各基礎自治体が自分の住民データを自分たちの手の届く範囲で管理しつつ、その住民情報を必要に応じてネットワークを介して個別に他組織からも照会可能とする「Pear To Pear 型」のシステム形態への切り替えを提案したい.

これは、自治体本庁で管理する住民データに支所端末からもアクセスできることと原理は同じである. 支所端末が県端末あるいは国機関の端末となっても、住民データは自治体本庁にだけ存在し、それぞれの自治体が責任を持って自分たちの住民データの管理を徹底することにより、その自治体が知らない所、目の行き届かない所で、大量の情報漏洩や目的外利用されてしまう危険性を少なくすることができる.

なお、蛇足ながら付け加えるならば、住民票の異動や広域交付では市町村同士が直接情報交換をしており、本質的には国の指定情報処理機関で情報交換していないことなら、システム的には Pear To Pear 型という発想は決して受け入れない形態ではないのです.

いきなり全ての基礎自治体同士が「Pear To Pear 型」接続するネットワークシステムは構築が大変だというのであれば、複数の基礎自治体がある程度まとまって共同 ASP 的にサーバ運用する方式もよし、あるいは、県レベルでのデータ一元管理からでも構わない．これは即ち、審議会が平成 13 年 8 月に提案した安全策のうちの第 3 次案の共同データセンター構想と、第 4 次案の県レベルでのデータ一元管理案である．

(6) 自ら制御でき、責任を持てるシステム運用を

IT 化、電子化、ネットワーク化には反対していない．電子化することによって得られる利便性とその裏に潜む、費用、危険性をバランスしながら電子社会、ネットワーク社会を築いて行く必要があり、自らコントロールできない IT 化には賛成できないのである．

新しいシステムを考案して普及させる過程ではどうしても新たな問題が出現する．その問題を克服して初めて新しいシステムを全面展開できる環境になる．問題を放置したり先送りしたまま新システム展開を急ぐと、取り返しのつかない状況になったり、甚大な害を被ることになりかねない．その問題をどこまで予見できるか、認識度の違いにより意見が分かれてくる．楽観的、悲観的判断での違いであれば愛嬌であるが、予見能力の違いから来るとすると笑い事では済まさせなくなる．

車社会になって便利になったが、多くの対策を講じて今日に至っている．左右運行、信号機設置、運転免許制度、自動車保険、自動車専用道路、シートベルト、車検制度、携帯電話禁止、など実に多くの知恵がある．パソコンもインターネットも便利なツールであるが、ウィルス、ワーム、情報漏えい、機器故障による情報喪失、情報氾濫、迷惑メール大量発生など多くの問題も出現している．これらへの対応は必須であり、放置はできない．利便性と危険性は裏腹であり、それをわきまえて活用すべきである．怖がる必要はないが、冷静沈着な対処は必要である．

では、住基ネットはどうであろうか．IT 化、ネットワーク社会、電子政府、電子自治体、電子申請と浮かれてばかりはいられない．いかなる漏洩、プライバシー侵害、改ざん、不正利用もさせまいとする、シビアな運用に耐えられるだけの準備と自信を持つまでは安易な運用拡大は避けるべきである．身の丈にあったシステム運用でいいではないか．

究極的には、自らコントロールできる範囲内でのデータ活用を担保できるシステムを目指すべきである．それが、大切な住民データを預かる組織の責務であると考える．

(7) 2 年間を総括して

審議会では一貫して県民や市町村のために活動してきたつもりだが、「本人確認情報保護には市町村の庁内 LAN のセキュリティ確保が何よりも大切」と提言した辺りから、一部の市町村の皆さんとの意識に齟齬が生じ、真意を正しく伝えられなかったことが残念であった．

誰に何をサービスするための住基ネットなのかを原点に戻って再確認し、その目標達成に向かって採用する手法、システムが技術的にも財政的にもセキュリティ的にも正しいのかどうかを常に検証し、住民が納得しながら、住民に役立つネットワークにしていくべきある．

安全性に 100%はあり得ず、いつまで経っても盾と矛の繰り返しであり、「100%でなければ導入すべきでない」との極論までは主張して来なかった.「一定レベルの安全性が確保され大局的にみて住民のサービスレベルを向上させるなら技術を導入する決断が必要だ」との政府関係者の意見も拝聴に値する. しかし、今の住基ネットにはそのサービスレベルが向上する気配すら感じられないのである.国家公務員の身分証明書を住基カードにしなければ住基カードが普及しないほどに、国民からそっぽを向かれている現実をしっかり認識しなければならない.

IT やネットワークをやっていて電子化社会を否定するのか、と短絡的なご批判もいただいたが、その分野を多少なりともかじった職人であれば、がむしゃらに突き進むことの危険性を認識しないはずはなく、危険性を推察できるがゆえに、時としてそれを是正し、適切な手段で、適切な速度で、適切な方向に軌道修正していく提言をする役目であったと認識しております.

IT 化、ネットワーク化は住民にとって必要欠くべからざる技術ですが、同時に生きている人間を管理する側面があることを十二分に認識し、真に住民が幸せになるネットワーク社会構築に向けて精進していくつもりです.

４－４．清水勉委員

はじめに

今回、長野県本人確認情報保護審議会に参加し、一委員として県知事・県職員・県議会議員、市町村長・市町村職員・市町村議員、総務省市町村課、財団法人地方自治情報センター（LASDEC)、報道関係者など様々な立場の人々と住基ネットに関して意見交換をし、あるいは意見を聞く機会を持てたことは、たいへん勉強になりました。

その中で特に気がついたことは、①市町村という行政組織が外から見るほど一枚岩ではなく、個々の問題について立場によって問題意識に大きな隔たりがある組織であること、②現場の担当職員の多くは住基ネットの問題点についてよく考えているのに比べて、決裁権のある上司になればなるほど住基ネットの問題点についての認識が低いこと、③現場の職員と首長との間で意思疎通が欠けていること、でした。

住基ネットの第一次稼動が始まる 2002 年（平成 14 年）８月前後、片山虎之助総務大臣は、臆面もなく、「住基ネットは全国の自治体が望んでつくったものだ」と言い、昨年８月５日の総務省側との公開討論会でも、井上源三市町村課長は同じことを言いました。しかし、日弁連が３回にわたって実施した全国市町村アンケートの結果にも、全国の自治体が望んでできたネットワークだという様子は全く現れて来ませんでしたし、長野県内の市町村の聞き取り調査でも市町村の側から住基ネットの法制化を望んでいたところは見出せませんでした。それどころか、住基ネットの仕組みさえ知らない自治体がたくさんありました。

住基ネットに関して市町村が本当に求めていることは何なのか。そのために審議会や県は何をすればよいのか。それが審議会の課題だと考えるようになりました。ただ、これには更に大きな前提問題がありました。それは、そもそも市町村は自治事務である住基ネットについて独自に考えているのかという、「地方自治の本旨」（憲法 92 条）に関わる問題です。これこそが最大の難問でした。

「法による行政」

恣意的な行政、すなわち「人による行政」は、人を見て態度を変えることを許容する仕組みですから、その社会に住む人々はいつ何が原因で自分が不利益を受けるか予測がつきません。そうなると、人々は安心して暮らすことができません。これに対して、「法による行政」は人の恣意的な判断を排除して合理的な法によって行政を行なおうとするものですから、合理性・効率性・公平性を実現するものとして、人々は安心して暮らすことができるというわけです。もちろん、時代や社会情勢の推移によって法律が時代に合わなくなることはあります。そのときは時代や社会情勢に合った法律改正をすればよいし、改正までの間は合理的な法解釈によって“繋げば”よいのです。

日本国憲法によれば、日本は民主主義国家です（前文、１条)。民主主義社会における行

政は人の恣意を排除する「法による行政」でなければなりません。憲法もこの考え方を採用しています（41 条)。地方自治体の場合は「条例による行政」ということになります（94 条)。

しかし、「法による行政」は、「「法による行政」が行なわれている」と誰かが言えば、そのとおりになっているというものではありません。それは、「日本は民主主義社会だ」とだれかが言ったら途端にそうなるわけではなく、民主主義社会になる努力が日々その担い手となる人々によって行なわれなければ実現しないのと同じように、「法による行政」を現実化する仕組みをつくり、それを日々実行して行くことが必要です。それがあって初めて「「法による行政」が行なわれている」と言えるのです。

「法による行政」になっていない日本の自治体の現場

例えば、ドイツでは自治体職員になる者に対して、２年、３年という時間をかけて自治体職員になるための研修を行い、職員になった途端、一定範囲の権限を与えられ、決裁権者として住民の前に現れます。訴訟になれば、その職員が法廷に行って、自分がした処分の正当性を説明します。まさに自治体が「法による行政」を実行しているという感じがします。

しかし、残念ながら、日本の自治体の行政実務は「法による行政」になっていません。

日本にはドイツのような新人・職員研修制度がありません。自治体によっては数日ないし数週間程度の研修をしているかもしれませんが、そのようなもので法律の素人だった人たちが「法による行政」を身につけるはずがありません。教えている人たちが「法による行政」を十分に実践している人たちかどうかも疑問です。訴訟になれば、弁護士に代理人を依頼するのが日本ではほとんど常識になっています。「法律問題は弁護士に」というわけです。日常業務は先輩職員や同僚の見よう見まねで覚えて行くというのが、日本の市町村行政の実態です（国や県も本質的には同じようなものです。情報公開法・条例の解釈運用のように、市町村が最も適切に行なっていて、県はそこそこ、国の機関が最もひどいということもあります。)。これは「法による行政」ではありません。

法律や条例を日々、自分で解釈していない職員は、新たな問題に直面したとき、自分で解釈して合理的な解決法を見つけ出すことができません。どこかおかしいと思っても、法律や条例の条文に照らして何がどのように問題なのかを整理することができません。そのため自分で考えることをしないで、ただ大勢に従っているのが無難だということになるのです。

しかし、「みんながやっているから正しい」という理屈は、法の世界では通用しません。みんながやっていることであっても間違っていることは間違っている。みんながやっていることであっても違う選択肢を選んでもよい。そのことを指摘し、是正させて行くことが法律を解釈運用する者の責任であり、それが法の世界というものです。

市町村においては、一番問題をよくわかっている現場の職員の問題意識こそが尊重され

るべきです。そして、そこで指摘される問題が法律や条例に照らすとどのような問題になるのか、どのように解決されるべきなのか、どの規定をどのように解釈すればそれが実現できるかなどを各市町村で考えるべきです。

国と県と市町村の法律関係

そんなことが市町村にできるのか。この場合、現実にいまそういう能力があるかという問題と、法律的にそのようなことが許されるかという問題とがあります。ここでは後者について説明します。

よく、国と県と市町村の関係を言うときに「上」「下」という言い方をすることがあります。現に、市町村は国と県が何を言うかを気にし、県は国が何を言うかを気にし、「下」は「上」の言うことの法的根拠や当否を吟味することなく、ひたすら従うものとされてきました。

長野県庁でも総務省から出向してきていた市町村課長が、「法律の有権解釈は国にある」と公開討論の場で発言したことがありました。国から出向してきている人がこんな基本的な法律知識もないのかと驚きましたが、いかにも国からの出向者らしい意見だとも思いました。

このような考え方が正しいとすれば、国の法解釈の誤りを県は批判もできなければ訴訟も出来ないということになります。地方自治法では「地方公共団体に関する法令の規定は、地方自治の本旨に基づいて、かつ、国と地方公共団体との適切な役割分担を踏まえて、これを解釈し、及び運用するようにしなければならない。」（２条 12 項前段）と規定しています。法律の解釈権限は、国にも県にも市町村にも対等にあるだけでなく、自治体に関する法令に関しては、「地方自治の本旨」（憲法 92 条）に基づいて国と自治体の「適切な役割分担」を踏まえて解釈運用すべきだと規定しているのです。

国と自治体が上下関係ではなく役割分担であることは、地方自治法で明記しています（１条の２第２項）から、自治体の役割分担である事務に関する法令の解釈運用では、自治体の解釈が尊重されるべきだということになります。

住基ネットは自治事務

地方自治体が行なう事務には自治事務と法定受託事務とがあります。地方自治法は、国が本来やるべき仕事を県や市町村がやる場合を第１号法定受託事務、県が本来やるべき仕事を市町村がやる場合を第２号法定受託事務と規定しています（２条９項）。どのような事務が第１号・第２号法定受託事務に当たるかは、地方自治法別表に明記されており、各法律にも明記されています。法定受託事務に当たらないものが自治事務です（２条８項）。

住基ネットは住民基本台帳を根拠法とする制度です。第１号法定受託事務でも第２号法定受託事務でもありませんから、自治事務だということになります。住民基本台帳法は住民基本台帳の管理責任を市町村長としています（３条１項）。住基ネットの管理責任も市町

村の権限領域内については市町村長にあることになります。

住基ネットは市町村にとって自分の仕事であり、国の仕事でも県の仕事でもありません。市町村が自分で管理し、その管理運用費用を自分で負担し、問題が起こったら自分で責任を負うことになります。市町村の立場から国や県に財政援助を求めることは、法律的には筋違いです。

「住基ネットは国に押し付けられたものだ」と言ってみたところで、それは実態がそうだというだけのことであって、自治事務という法的性格が変わるわけではありません。事実は事実、法律は法律というわけです。

自治事務と国との関係

住基ネットが自治事務だということは、市町村が国（法律）から「これはあなたの仕事です。あなたが責任を持ってやってください」と言われているということですから、市町村は住基ネットの担い手として責任を負わなければなりませんが、その代わり、どのように責任を負うかを決めるのは市町村自身です。市町村の自治事務の運用については、県も国も市町村の判断を尊重しなければならないということです。

地方自治法は 245 条以下で、自治体の行政実務への国と県と市町村の関わり方を規定しています。ここをしっかり規定しておかないと、「下は上に従え」という旧来型の中央集権的手法の行政が罷り通ってしまうおそれがあるからです。地方自治法は、地方自治ないし地方分権の実現に関して国と自治体との関係を性善説で見ていないということです。

まず、市町村の事務処理に関して国や県が関与するには法令の根拠が必要です（245 条の２）。国だから、県だからということだけで、好き勝手に関与することは違法だというわけです。

次に、関与に関する法令の根拠がある場合であっても、その関与は、「目的を達成するために必要最小限のもの」でなければならず、市町村の「自主性及び自立性に配慮しなければならない」（245 条の３第１項）とされています。法的な根拠があっても関与の仕方程度は必要最小限にしなければならないと釘を刺しています。

そして地方自治法は、市町村の自治事務に関して国が直接是正要求をすることを原則的には認めていません。「法令の規定に違反していると認めるとき、又は著しく適正を欠き、かつ、明らかに公益を害していると認めるとき」は、都道府県知事に対して、当該事務の処理について違反の是正又は改善のため必要な措置を講ずべきことを当該町村に求めるよう指示をすることができる」とされています（245 条の５第２項１号）。自治事務の運用が法令の規定に違反しているか否かについては市町村の解釈運用が尊重されるべきことが前提となっていますから、国としてもそう簡単に「法令の規定に違反している」と決め付けることはできません。「著しく適正を欠き」という条件にしても同様です。しかも、「かつ」「明らかに公益を害していると認めるとき」という条件がついています。「公益」とは何か。「明らかに害している」と言えるか。これらもそう簡単に決め付けることはできません。

このように条件をつけていることは市町村の自己決定を尊重するものとして合理的です。

しかし、この規定に基づいて知事から市町村に対して指示をすると、市町村は「当該事務の処理について違反の是正又は改善のための必要な措置を講じなければならない。」（245条の５第５項）という法的義務を負うことになっています。この点は国会において国と自治体の業務の役割分担（１条の２第２項）や自治体の法解釈権限の尊重（２条 12 項）に反するという指摘がなされ議論になりました。そして衆参両議院で以下のような付帯決議がなされました。

〔衆議院付帯決議〕「自治事務に対する是正の要求の発動に当たっては、地方公共団体の自主性及び自立性に極力配慮すること」

〔参議院付帯決議〕「自治事務に対する是正要求については、地方公共団体の自主性及び自立性に極力配慮し、当該事務の処理が明らかに公益を侵害しており、かつ、地方公共団体が自らこれを是正せず、その結果、当該地方公共団体の運営が混乱・停滞し、著しい支障が生じている場合など、限定的・抑制的にこれを発動すること。なお、是正改善のための具体的な措置の内容は地方公共団体の裁量に委ねられているものであり、国はこの地方公共団体の判断を尊重すること」

参議院付帯決議についてみると、是正命令が発動されるべき場合は、「当該事務の処理が明らかに公益を侵害しており、かつ、地方公共団体が自らこれを是正せず、その結果、当該地方公共団体の運営が混乱・停滞し、著しい支障が生じている場合など」に限定し、しかも、是正改善のための具体的な措置の内容は自治体の裁量に委ねられているとしています。

この規定に関連して住基ネットの接続を止めるということを考えた場合、そうすることが当該市町村の業務の「運営が混乱・停滞し、著しい支障が生じ」ないのであれば、是正命令が発動されるべき場合には当たらないということになります。仮に是正命令が出たとしても、「違反の是正又は改善のための必要な措置」の具体的内容については市町村の裁量に委ねられることになります。

立法事実

「住基ネットは国に押し付けられたものだ」ということをよく聞きます。それが事実だとすれば、そして実際に市町村の実情を知れば知るほど、市町村が住基ネットの法制化を求めた事実は見出しがたいのですが、住基ネットの法制化という立法の正当化を基礎付ける立法事実に重大な嘘があるということになります。

嘘を基礎とする法律は、民主主義社会の法律としては出来が悪いと言わざるを得ません。そのような法律は国民に支持されないだけでなく、実は実施機関にさせられている市町村にも支持されません。

市町村が望んだということは市町村や住民にメリットが大きいことが原因になっているはずですが、市町村は住基ネットにほとんどメリットを感じていません。むしろ重荷と感

じている市町村がほとんどです。住基ネットに接続していない自治体が３（福島県矢祭町、東京都杉並区、東京都国立市）で、段階的参加自治体が１（横浜市）しかないにもかかわらず、住基カードの普及状況をみると、実情はほとんどの市町村、ほとんどの国民が住基ネットを必要としていないことが歴然としています。

立法事実に重大な嘘がある法律を市町村や国民に守ることを要求することは、守るに値しないことを無理やり守らせようとすることですから、却って、市町村の法令遵守義務と国民の遵法精神を損なうことになります。そのような法律の存在を放置することは、民主主義社会を荒廃させます。嘘をなくすために速やかに法律を廃止するか、重大な改正（市町村選択制、個人選択制など）をするべきです。それが民主主義社会として当然、とるべき対応です。

費用対効果

市町村の仕事は住基ネットの管理運用だけではありません。住民の生活の全分野に及ぶ業務を広く担っています。その運用のために多額の費用を必要とします。しかし、いくら住民のためであっても、各市町村には予算の限界というものがあります。したがって、費用対効果のバランスが必要不可欠です。

地方自治法は「地方公共団体は、その事務を処理するに当たっては、住民の福祉の増進に努めるとともに、最小の経費で最大の効果を挙げるようにしなければならない。」（２条 14 項）と規定し、地方財政法は「地方公共団体の経費は、その目的を達成するための必要且つ最小の限度をこえて、これを支出してはならない。」（４条１項）と規定している。費用対効果は地方自治体の経営の大原則です。

監査委員の職務権限に関して、地方自治法があえて２条 14 項を明記して、「特に、意を用いなければならない。」（199 条３項）としているのも、費用対効果を重視しているからです。

ましてや現在は国も自治体も財政難の時代です。財政的に潤っている市町村はごく一部にはあるかもしれませんが、多くの市町村は膨大な財政赤字に喘いでいます。そのような時代に各市町村の財政状況を無視して、全国すべての市町村が同時期に、管理運営費を自己負担しなければならない住基ネットに参加させるというのは、財政的に見ても無謀な計画です。ここで住民のメリットを数値化して、これがプラスで市町村のマイナスを上回れば、全体としてプラスになるという考え方もあるようですが、住民のプラスは経済的利益として自治体財政に戻ってくるものではありません。両者を相殺勘定することはできません。両者を相殺してよい場合があるとすれば、住民のメリットが極めて大きくかつ明確で、住民が他のサービスを犠牲にしてもよいと評価してくれるような場合に限られるでしょう。住民の多くが果たして住民票の広域交付や 10 年に１度の旅券発行手続における住民票添付の省略などにどれほどのメリットを実感し、このメリットのために他の行政サービスが削られ犠牲になることを了解しているでしょうか。大いに疑問です。また、住基ネットによ

り職員の人員削減や職務時間の短縮がどれほど進んだでしょうか。これも疑問です。こうしてみると、現在、住基ネットによって自治体の赤字財政を減少させている市町村は存在しないのではないでしょうか。

繰り返しますが、各市町村がやるべき仕事は住基ネットだけではありません。他にいくらでも仕事はあります。それらにかける出費を削ることまでして住基ネットを維持管理する価値がどれほどあるのでしょうか。住基ネットそのものの費用対効果と、他の行政サービスを後退させることを含めての全体の費用対効果を、各市町村はしっかり見極めるべきです。「よそが住基ネットに接続しているから自分の自治体も接続する」「よそが止めないから自分の自治体も止めない」という考え方では、責任ある対応はできません。

住基ネットに参加しないことができるか

このように、住基ネットを長期的に適切に管理運用できるものでなければ参加する資格がないものだとすると、個人選択制の採否以前の問題として市町村選択制が採用されるべきです。

しかし、住民基本台帳法は、都道府県が住基ネットの運用に関して指定情報処理機関に業務の一部を委任することを認める規定（30 条の 10）を設け、都道府県が委託するか否かを選ぶことができるようになっていますが、市町村が住基ネットに参加するか否かを選ぶことができるような規定はありません。

したがって、これらの規定を見る限りでは、市町村が独自の判断で住基ネットに参加しないことは、現在の住民基本台帳法では認めていないと言わざるを得ません。

住基ネットに接続しないことができるか

住基ネットに参加していることを前提に住基ネットに接続しないことはできます。

都道府県知事と市町村長には「適切な管理のために必要な措置を講じなければならない」義務（30 条の 29、36 条の２）義務があります。

しかし、実際には住基ネットを適切に管理運用する財政的余裕も人材もないということであれば、そのような自治体にとっては、住民と他の自治体に迷惑をかけないようにするために、財政的及び人的に責任を持って管理運用できるようになるまで、住基ネットに接続しないことが最善の対応策ということが言えるのであって、接続しないことこそが採るべき「必要な措置」だということが言えます。

市町村にとっての「必要な措置」の内容をどのように解釈するかは、第一次的に各市町村が自らの責任において決めることであって、国や県の解釈が優越するわけではありません。

住基ネットに接続していない自治体の首長はそれぞれ考えをもっていると思いますが、住民基本台帳法の解釈として説明すれば、このようになります。

参加しないことと接続しないことの差

理論的な違いありますが、実際の差はそれぞれの市町村の考え方によって違ってきます。

昨年夏、ブラスター問題が発生したときに住基ネットの接続を止めた自治体がありました。これはブラスター問題が解決するまでという条件で接続を止めたものですから、この問題が解決すれば再び接続することになります。したがって、首長が住民に住民票コードをつけ住民票に記録し、本人に通知するなど、接続しない間でも住基ネットに関する他の業務は通常通り行なうことになります。

これとは対極的に、接続しない理由が、当該自治体の財政難や住基ネットを適切に管理するだけの専門能力のある職員がいないことだったりすると、これらはすぐに解決する問題ではないので、当面、首長が住民に住民票コードをつける必要もないということで、このような作業もしないということがあり得るでしょう。

長野県と市町村

これまでの説明で理解していただけたと思いますが、県と市町村は法律上、命令する側とされる側という関係にはありません。対等です。ましてや住基ネットは市町村の自治事務ですから、市町村が住基ネットにどう関わるかを決めるのは各市町村です。県庁は各市町村の独自の考えを尊重し、必要に応じて応援すべき立場です。

県内各地の市町村を回っていたときや説明会をしていたときに、「県はどうするつもりなのか」「知事は何を考えているのか」という質問が自治体関係者やマスコミ記者などからよく出ていました。まるで、県（知事）が市町村の住基ネットへの関わり方を決める立場にあるかのように。

しかし、そうではないのです。各市町村がどうしたいのか、そのためにはどうしたらよいのか、ということをしっかり考え、はっきりさせることが先決なのです。このことを県も市町村も県民もしっかりと認識すべきです。

この点をはっきり認識するならば、各市町村がそれぞれの方針をしっかり立てることこそが最優先課題とされるべきです。マスコミも各市町村がどのような状況にありどのように考えているかということを詳しく取材して報道すべきです。そうすれば、県民は自分の住んでいる自治体がどのような状況になっているかを知ることができ、自分の住んでいる自治体が住基ネットとどう関わるべきかを考え、自治体に自分の考えを伝えることができます。そうなって行けば、市町村は独自の方針を立てることもできるようになって行くでしょう。

主役は市町村です。県はサポート役です。そのことをはっきり認識した協力関係が重要です。そのことを前提に市町村から県や審議会に協力が求められるなら、県も審議会も大いに協力すべきです。

住基ネット問題で問われているのは市町村の自治力です。

4－5.　中澤清明委員

1. はじめに

住基ネット運営の一端を担う市町村から選ばれた委員としてとまどい、困惑し続けた 2 年間でありました。

特に「住基ネット離脱勧告をした中間報告」は市町村に大きな混乱をもたらしました。市町村は既に改正住基法に基づき住基ネット関連機材やシステム整備を終え、平成 14 年 8 月からの一次稼働を順調にこなし、15 年 8 月からの二次稼働に向けて住民への広報･住基カード関係予算措置などを行い、まさに運用開始を待つだけの時点でした。不安に駆られた住民や議会への説明に追われる一方で、県が離脱すれば「住基法で定められた市町村長の責務が果たせない･住民サービスが提供できない」などの事態が想定される中、住基ネット本体の運営主体として適正な管理運営に努力すべき県の対応が見えず、市町村も大変困惑いたしました。

本審議会は県からの諮問事項もないまま審議会主導でテーマや審議内容などはその都度次回の内容を決めるという形で動き始めました。住基法解釈や審議会の役割･権限など、住基ネットの事業主体者或いは本審議会設置者としての判断が求められる局面でも県側の見解が示されることは殆どなく、審議会に丸投げしその解釈に基づいて進められたため、私としてはわかりにくいものでありました。

2. 住民基本台帳ネットワークにおける県･市町村の役割

住基ネットでは県と市町村の役割･責務は概ね以下のように定められています。

市 町 村	都 道 府 県
[役割] ・ 既存住基システムと連携した住基ネットワークシステムの構築と運営 [業務･運用面] ・ 住民基本台帳の管理 ・ 市町村ＣＳ内の本人確認情報の管理 ・ 住民票写しの広域交付、住基カードの交付、転入転出特例処理 ・ 都道府県知事への本人確認情報の通知 ・ ＣＳの運用管理 など	[役割] ･市町村及び指定情報処理機関と連携した住基ネットワークシステムの構築と運営 [業務･運用面] ・ 都道府県内住民の本人確認情報の記録保存 ・ 指定情報処理機関への本人確認情報の通知 ・ 都道府県サーバの運用管理 ・ 都道府県執行機関への本人確認情報の通知 など

市町村長には住基法第三十条の五第１項で本人確認情報の都道府県知事への通知が義務づけられ、第３項で都道府県知事はこの通知された本人確認情報を県サーバに記録保存しなければならないとされています。

セキュリティ責任範囲については都道府県協議会で作成した基本設計書でも明示されており、市町村のセキュリティ責任範囲はＣＳをはじめとする市町村側に設置する機器類と庁内既設ネットワークなどとされていました。

3. 審議会の位置付け･審議事項など

本審議会は住基法第三十条の九に基づく必置の審議会であり、住基法第三十条の五第一項の規定による通知に係る本人確認情報の保護に関する調査審議を主たる任務としています。住基法第三十条の五第一項の規定による通知に係る本人確認情報とは市町村長が住基ネットを通じて県知事に通知した情報で県知事が県サーバに記録した情報のことであります。本審議会の審議対象は住基ネットによって初めて県が保持するようになった県民の本人確認情報や住基ネットにおいて県知事の事務とされた部分（前掲の表において都道府県の役割とされている部分）と考えます。

本審議会は住基ネットの運用を前提として設置されています。本人確認情報の保護に関して調査審議し、適正な管理運用のために問題点指摘や改善を求めることなどが任務であり、運用停止を意味する離脱まで勧告出来るのかは疑問に思っています。

また、費用対効果や利用価値、必要性の有無などから住基ネット制度自体に議論が及ぶこともありましたが、住基ネットの運用を前提とした本審議会の審議事項ではないのでないでしょうか。国民の間に住基ネットに関して多様な意見があるのは事実でしょうし、あって当然のことと思いますが、住基ネットは国会で定められた法に基づいて運用されているものですから、住基ネットの改廃など制度自体に関する議論は本審議会でなく、国会に求めるべきではないでしょうか。

4. 中間報告について

私は住基ネットから離脱を勧告した中間報告に同意いたしませんでした。

○ インターネットとの物理的接続は住基ネット以前から

問題とされたインターネットに接続した庁内ＬＡＮ上に既存住基が配置されていたのは住基ネットによってもたらされたものではありませんでした。

住基ネットが来る以前から市町村で住基事務を始めとする一連のコンピュータ処理事務に使われていたものです。

○ 既存住基のある庁内ＬＡＮ上の方が個人情報満載

この庁内ＬＡＮ上には住基台帳、選挙人名簿、国保被保険者台帳、住民税課税台帳・・・・・を始めとする市町村事務の根幹台帳が存在し、これらは住民にとっては非常にセンシティブな個人情報であり、市町村にとっては行政事務に欠くことの出来ない大切な情報であります。

○　住基ネットから離脱しても個人情報は守れない

インターネットと庁内ＬＡＮの物理的接続を問題とした場合、住基ネットから離脱し住基ネットとの接続を絶っても、インターネットとの接続を絶たない限り、既存住基を始めとするよりセンシティブな個人情報が、インターネットに晒されていることには変わりなく、より重要な個人情報は守れません。

住基ネット離脱でなく、インターネットと庁内ＬＡＮの物理的接続の解消をまず求めるべきということではないでしょうか。

○　住基ネット接続を停止しなければならない差し迫った危険状態であったか

知事、市町村長は差し迫った危険状態にあるときには住基ネット接続を一時的に停止させる措置ができるとされていますが、この状態について平成14年総務省告示第334号においては「都道府県、市町村及び指定情報処理機関は緊急時対応計画を定め、ファイアウォールで不正アクセスの兆候を発見したときなど本人確認情報に脅威を及ぼすおそれの高い事象が確認され、本人確認情報の漏洩等の危険が具体的に発生した場合は、相互に連絡調整を行い、被害拡大を防止するための措置等を講ずること」とされております。

インターネットとの物理的接続は具体的危険性が現実化した状態と言えたでしょうか。少なくもそれまでこの状態で続けられた８ヶ月の住基ネット運用や長年にわたる庁内ＬＡＮ上の既存基幹業務運用では情報漏洩や不正アクセスなど具体的な現実化した危険は聞いていませんでした。理論的には起こりうる危険性を指摘し、早期の対策を促すことで良かったのではないでしょうか。

自然災害に例えるなら火山や断層があるからと言うだけで避難勧告をするようなことはしないでしょう。火山性微動や地殻の歪みの拡大など火山活動や地震につながる事象が観測されて避難勧告や命令がなされます。

5. 審議会への県の姿勢について

○　県には法解釈など住基ネット事業主体者として、審議会設置者としての見解が求められる局面では明確な見解を示して頂きたいと考えています。審議会運営にあたってはこのことがたいへん大切と考えます。

○　審議会に付すべき事項を精査して頂きたいと思います。特に技術的検証を求めることなどは、それなりの能力･責任体制を備えたシステム監査法人などに委託すべきだと考えます。審議会で責任の持てる事柄ではないのではないでしょうか。

6. おわりに

今回のセキュリティ論議は住基ネット本体よりも、市町村長の責任範囲である市町村庁内ＬＡＮやＣＳ、既存住基の方に集中していました。このことによって市町村においてはネットワークセキュリティに関する関心も高まり、既存住基や庁内ＬＡＮのセキュリティ対策が向上したことは本審議会活動の大きな成果であったと思っております。

4－6.　吉田柳太郎委員

［IT 社会の「ﾒﾘｯﾄと闇」］

コンピュータネットワークは現代の怪獣、モンスターです。それは、社会に非常に大きな影響を及ぼす存在になっています。有名芸能人が自分のホームページで、状況によってはプロダクション事務所を離れると宣言すれば、社長が辞任し三〇代の役員が社長に就任することになったりします。ホームページの意見が、企業の株価を急落させる要因となる時代なのです。

そういう時代のなかで、国は万全の体制と対策で IT を国家戦略として推進するとしてきました。たとえば、二〇〇一年一月 IT 戦略本部が策定した「e-Japan 戦略」では、「我が国が五年以内に世界最先端の IT 国家となる」ことが目標とされています。その構想には、IT の推進によって新規雇用が生み出され、高度情報社会によってすべての国民が一律に大きなメリットを享受できる……といったバラ色の表現ばかりが並んでいました。

しかし IT には本質的に、深くて目には見えない深海のような闇が広がっているのです。

各省庁のホームページの改ざんや海外からの攻撃、電子個人情報の漏洩、誹謗中傷掲示板の存在、対策を誤れば人事や株価にまで影響を及ぼすネットワーク社会……。長野県「安全確認」実験の結果をふまえて発言してきたことや、個人情報保護の観点で指摘した内容はコンピュータネットワーク社会が生みだしてきた、この深い闇の部分を指摘することだったつもりです。しかし、長野県本人確認情報保護審議会や長野県安全確認実験の経験をふまえて発言してきた論点に対する、マスコミを中心とした各界の反応は穏やかなものではありません。

・具体的な危険が起こっていないのに安全性を問題視することが問題だ。

・具体的な危険性を示せないなら黙っていろ。

・IT 推進にブレーキをかける行為である。

・国家プロジェクトに君ごときが意見をする立場にない。

・米国の著名な団体の意見なら聞く耳はあるが、長野県の田舎審議会の委員から意見をされる覚えはない。

繰り返しますが、IT 社会はバラ色だけではありません。もちろんメリットはたくさんある。本当の意味で社会に IT が活用されることを切望しています。だからこそ、それを実現するためには「IT の闇」にしっかり目を向けて行くべきなのです。分かりにくいからとか、国が安全と言っているからということで問題すら認識しない状態では、ほんとうの意味でのＩＴの活用はできるはずがありません。

たとえば、IT 社会は新たな差別を生むものです。

あらゆる情報を入手することの手間は格段に減りました。現在は、検索エンジンを使うことができれば、ほぼ入手できない情報はないとも言われる状況にあります。そのため、IT を活用して情報を得る人と、IT を活用しない人あるいはできない人との間での、情報の乖離は急速に広がり埋まらなくなっているのです。そこにさまざまな新しい差別が生まれ、拡大していく素地が存在しています。

ネットワーク上で情報を共有し活用する「IT 社会」と、人間と人間が直接触れ合うことで情報の占有的利用が行われてきた従来型の社会とでは、他の社会（コミュニティ）との接点で公開される情報の量と質が、格段に異なっています。そして、国や自治体のそれぞれの行政執行組織は、明らかに「人間と人間が直接触れ合う」型の社会です。

それでも、IT 化推進で先行した国はまだましだといえます。成功しているとは思えないまでも、国はそれなりに「IT を活用して情報を得る」ことで「ネットワーク社会における勝ち組」になろうとしています。ところがここで「IT 社会の深い闇」に落ち込んでいるのは、多くの自治体なのです。

それらの自治体には、「検索エンジンを使えば入手できる」レベルの「情報セキュリティ」や「個人情報保護」のための対策についてすら、情報を入手したり活用したりすることができていません。国と自治体の間には、「IT 社会の深い闇」から生み出される新たな差別がすでにできあがってしまっているのです。

……これが、長野県での本人確認情報保護審議会における自治体の実地調査や安全確認実験を通じて見聞してきた、多くの自治体の現実でした。

本当の意味で社会に IT が活用されるためには、IT 社会の浸透によって新たに生まれる「闇」に対して、適切で強力な対策が必要です。そうすることではじめて、多くの国民ができるだけ安全に日々をすごせるような IT 社会を作り上げていくことができます。

リスクを承知で危険なスポーツを楽しむ方々に危険だからやめろ！などという話をしているのではありません。リスクを正しく認識することを棚上げにして法律を作り、実行すべき時期が来たからと言って、準備ができていないにも関わらず「安全」だということにしてスタートすることは、ＩＴ社会では通用しません。ＩＴ社会に一度解き放たれた情報は二度と回収できないからです。

言ってしまえば「住基ネット」は、財政能力もある、技術能力もある、責任能力もある自治体が先行して導入すればよいシステムです。その導入、運用ノウハウを後に続く自治体に提供できれば、広がりもでてくるはずです。ところが現実は、そうではありません。安全対策を十分に行えない自治体が問題を抱える存在であることは、今や総務省も認めています。それは地方交付税支出の事務連絡を出している点からも明らかです。

だから住基ネットの議論は、「安全／危険」の話ではありません。ネットワーク社会の「メリットと闇」をどう読み取るかがポイントとなる議論なのです。多くの情報セキュリ

ティ技術者・研究者からは、現在の住基ネットをめぐる国（総務省市町村課）の議論は、技術以前の「超低レベル」のものに見えています。つまりここで必要とされているのは、議論の質的転換なのです。

ネットワーク社会の「メリットと闇」を直視した、広範な社会的議論が、的確なポイントを押さえるものとして深化されて行くなら、住基ネットは現在のものとは本質的に異なるシステムになっていくでしょう。

情報セキュリティの問題を考えることは、実は「IT 社会の闇」に対する適切で強力な対策を考えることそのものなのです。

先般、静岡県のある役所でパソコン十台と現金七〇万円の盗難が発覚しました。社会教育課、国民年金課、総務課などのノートパソコンだそうです。市役所の夜間警備は守衛二人で行っていて、防犯装置などは設置されていないとのことです。

これでも個人情報の漏洩はありえないと言えるのでしょうか。この事件では、そもそも個人情報保護論議以前の問題が露呈しています。安心とはそもそも何なのでしょうか。

国民の、地域住民のキビ情報が入っているコンピュータを運用、管理しているのに警備保障会社にも入っていないことがまかり通っていたことが明るみになっています。

この文章をまとめている読売新聞の朝刊一面にも、社会保険庁がＩＴゼネコンと呼ばれる企業に１０６億円もの契約外の支払いをしていたことが指摘されました。内容がわからないので誰も確認をしないでいわれるがままに支払いを続けてきたことも露呈しました。

マスコミは、長野県本人確認情報保護審議会と総務省の平行線の議論と書き続けました。徹底的な間違いは、住基ネットの範囲を定義している長野県本人確認情報保護審議会と数年前から話をするたびに範囲が狭くなる総務省側の認識の違いを指摘すべきだと考えています。

個人情報保護の観点からの議論をしているのであって、論理的に別でも物理的につながっている「庁内にある既存住基サーバは住基ネットではない」と主張すること自体に総務省側の無理があることを指摘しなければなりません。

［あたまの転換］

情報漏洩が発覚しても毅然とした態度でいいわけができなければなりません。

■なんでもかんでも怖いと言っているつもりはありません

　何でもかんでも怖いと言っているつもりはいっさいありません。住基ネットがなくなればいいという話をしてきたつもりもありません。それなのにいろいろなところで、

「住基や背番号に反対しているやつの話なんか聞く耳はない！」

などと言われたりします。先般も長野県内で、市町村のみなさんを対象とした説明会をしましたが、田中知事とは異なるお考えを持つ自治体の課長さんなどから

「住基ネット自体の侵入が心配だったんだ。でも実験では侵入に失敗しているじゃないか。世間を混乱させたのはおまえなんだから謝罪しろ」

というおしかりをいただきました。私の話が、おっしゃるように理解されてしまっているのであれば、そうした混乱――誤解をさせている責任の一端は私にもあるのだということで、反省をし、おわびをしたいということで謝罪しました。それで、私が頭を下げた写真を使って、

「彼はまちがってたんだ」

という報道がされるわけです。マスコミの報道というものも、もうちょっと何とかならんのかと思うのですが、なかなか正確に報道していただけません。

　私が言っていることはどういうことかと言いますと、

国が安全だと言っているから、コンピュータシステムは万全で安心できるから、

どんどん使いましょうというわけにはいかない。

　ということです。なぜかというと、コンピュータのネットワークっていろんなところに問題があるからなのです。

■「自治体が守り通す、賠償を含めて責任を負う」と言えますか

　自治体のみなさんへの説明会などで、こんなご意見をよくいただきます。

「とどのつまりは何だ？　結論聞かせてくれ。長野の話はもういいんだ！」

　結論は何かと言うと、住民のみなさんの個人情報を預かっている自治体さんそれぞれが、「私のところは絶対に完璧に守り通す、何か問題があっても賠償責任も含めて全部負う、その所存で運用しているのだから、何があっても心配ない、大丈夫なんだ」と言い切れるかどうか、ということだと思います。

「言い切れるから心配してもらわなくてもかまわないんだ」と言われるところは、どんどん推進されるのがいいと思います。ただし、住民の方が窓口に来て、

「僕の個人情報が漏れた。あなたは担当責任者としてこの問題にどういうふうに責任とってくれるんだ？

首長はどのような形で謝罪をし、責任をとるのか？

お金がありませんとか、伝票がなくなりましたとか、書類を紛失したという話じゃない。僕の個人情報がどんどん漏洩していったんだ。僕のプライバシーに対してあなたの自治体ではどういうふうに責任をとってくれるのか？」

と言われたときに、賠償訴訟というものが起きます。日本弁護士連合会の先生方もいろいろなケースを考えられておられるのですが、どうも頭を下げるだけではすまない。

「そんな問題は、世間一般的には起こっていないのだから、そんなこと起こるはずがないんだ」というようなお話もありますが、来年の４月には個人情報保護法が施行されます。今後は自治体も例外なくコンプライアンス（規定やルール）が問われることになります。さらに、アカウンタビリティ（説明責任）やトレーサビリティ（情報追跡）といった、フォレンジック（法的根拠になる証拠）が問われることになります。米国ではＳＯＸ法（コンプライアンスに関する責任者の個人責任追及法）も始まりました。日本も近々同じことが求められるようになり日本の法も経済産業省が音頭をとり整備が始まっています。

来年の４月からは個人情報保護法も施行されます。自治体も例外ではありません。

危険性がゼロでない限り「あり得ない脅威論」なのだと放置することはもはや不可能です。

■住民から賠償請求がされたとき窓口で毅然とした対処ができますか

情報が漏洩してしまう危険性をゼロにすることは、技術的にも論理的にもできません。

窓口に「俺の個人情報漏洩の賠償を支払え」という人が何万人と来ても、毅然とした態度で対処ができるようにしておく必要がある、ということです。

その毅然とした態度で対応ができるようにするということはどういうことかと言うと、きちんと窓口で「いいわけ」ができるかどうかです。

たとえば、こんなふうにいいわけができるでしょうか

「僕のところはここまでやりました。その証拠がここに記録されています。正直言うと僕にもよくわかっていません。でも、わからないなりに一生懸命やってたんです。職員は勉強会も行った。わかんないなりに試験も受けて、やっぱり落ちて、それでもうまくいかないなりに一生懸命やった記録がこれなんです。

だから、あなたが問題があったと言ってる〇月〇日の記録もここにあります。これを見てください。

何が書いてあるか、僕には分かりません。でも、機密保持の誓約にあなたが今サインしてくれるんだったら、ご覧になっていただいてけっこうです。それで、問題がどういうことだったかを追求してください。

僕の責任がゼロだとは言いません。幾分の責任はあると思います。でも、僕が一〇〇%悪いという話になりますか？　僕は一生懸命やりましたけど、あなたに、僕が一〇〇%悪いと言われる覚えはありません。その比率がどこかということは法廷でどうぞ」

こういう話を窓口ですれば､相手は｢おまえは一〇〇%全部悪い｣と言えないわけです。これが結論です。

ところが今、実際の市町村の状況はどうなっているでしょうか　多くの自治体では

「国がだいじょうぶだと言ってます｡僕に言われてもわかんないので上長に聞いてください」

という話になります｡そこで､責任のある上長に僕が｢あなたは対策をどうしてましたか？これ、ルールどうなってましたか？」と聞くと、

「そんなの俺に聞くな。問題があったらボチボチ直せばいいんだ。

はじめから否定するようなやつの話なんて問題外だ。議論になるか。出てけ！」

こうおっしゃる方が少なからずおられます｡対策の記録も､セキュリティ管理のルール(運用細則など）も、たぶんどこかにそれなりのものがあるのでしょう。だけど責任ある上長が把握していないし、理解もしてない｡だから記録もルールも窓口の苦情に対して有効に使えません。コンプライアンス的に問題なのです。

そういう状況です。

■毅然とした態度で「いいわけ」をするためにとにかく「パッチ」をあてましょう！

「あたまの転換」をしてください。

より安全で安心できる状態に持っていく一〇〇%はそもそもないのですから､できるだけお金をかけずにいろんなことをやる、ということです。

具体的には、まず、とにかくパッチをあてることです。「パッチ」というのは、プログラムの「つぎあて」です。プログラムの穴（セキュリティホール）をふさぐ小さなプログラムですね。

マイクロソフト社からセキュリティ対策のパッチが出たら、その日の内にあてるのがベストです。そうしておいたら、誰にもなんにもつっこまれる筋合いのない話です。マイクロソフト社が対策をたてていない未知のアタックを受けたら、それはもうしょうがないです。だけど、マイクロソフトが公表した既知のアタックだけは、せめてその日に対策しておかなければいけないと考えています。

問題発生時に、かならず「いいわけ」の材料のひとつになるからです。これをきちっとやっておけば、みなさんのネットワークはかなりよくなります

そこから次にどうしていくかを考えながら、最終的には、

たくさんのお金をかけてシステムやネットワークを維持運営し続けていかなければなりません。

［セキュリティ対策の限界］

セキュリティレベルを 100%にできないのはなぜか

■小学校六年生程度の日本語を読む力があれば、他人のコンピュータを乗っ取ることができてしまいます

「IT のセキュリティ対策にはまったくお金をかけませんでした」となると、セキュリティレベルはどうでしょうか

書店で簡単に入手できる「ハッカーになろう！」とかいうタイトルの本が一〇〇〇円かそこらで売っています。そういう本を読んでいくと、

小学校六年生くらいから中学レベルの日本語を読む力があれば、

絶対に他人のコンピュータが乗っ取れるくらいの知識が、「おまけの CD-ROM」で付いてきます。

これはほんとの話です。

まったくお金をかけなかったら、セキュリティレベルはゼロ。

だからセキュリティ対策はしないといけません。でも、三〇万円お金をかければ、セキュリティレベルはがーんと上がるんです。もうちょっと行こうかということで「六〇万円かけましょう」となると、セキュリティレベルは ガガ〜ン と上がります。

だけど、「一億円かけました、一〇〇兆円かけました」……セキュリティレベルは絶対に一〇〇%になりません。

なりようがない。「セキュリティレベルの限界」があるためです。

■ソーシャルエンジニアリングこれをやられると、盗れない情報なんてありません

「ソーシャルエンジニアリング」とは、ケビン・ミトニックという男をご存知でしょうか

彼は「ハッカー」です。「世界でみんなが知ってたハッカー」でした。で、彼はある日考えます。

「どこにだってどんどん入れる。俺は天才だ。だからどんな情報でもお金にできるし、知的好奇心を満足させることができる。」

そこで彼は、こともあろうにアメリカの FBI 犯罪者リストというデータベースに侵入します。犯罪者の顔が正面とか横から写されていて、住所とか年齢とか全部はいっている、そんなデータベースのデータをボーンと抜いてきて、インターネット上のホームページで誰でも閲覧できる場所に置いたのです。

それでアメリカ政府はアタマにきて、彼を追いかけまわすことになります。

彼は逮捕されて牢屋に入ります。そこで五年間生活して、二〇〇三年の一月にやっと出てきました。彼がその時何を考えたか、「このまま同じことを繰り返しても、きっと捕まる。そうだ、俺はこのノウハウを売ろう」ということになりまして、彼のノウハウを本にします。それが『欺術』(岩谷弘訳・ソフトバンクパブリッシング刊、二〇〇三年。原題 "The Art of Deception" ）という本です。この本にはいろいろなことが書いてありますが、その中心は「ソーシャルエンジニアリング」です。

みなさんの経験の中にも、相手から「こいつは口がうまいな」とか「こいつは信用できねえな」とか思われてしまったことがあると思います。相手は心をガチャンと閉ざします。閉ざしてしまったら、「こいつには絶対に俺のことは教えない」となります。そうなるとどんな話をしても、よっぽどでない限り、個人の情報は教えていただけることがありません。それはあり得ない。敵とみなしたやつには何もあげないし何も教えない、何も話してやらない――こうなります。みなさん共通の、人間の心のシステムがそうできている。

だけれども、同僚が困ってる、仲間が困ってる、きのうお世話になったなになにさんが困ってらっしゃる――そうなると人間はどうするかというと、みんな幼いときから教育を受けていますので、「困ってる人を助けなさい」と教わってきています。僕も、小さな頃おばあちゃんにもよく言われました。「知らない人にはついて行くな。でも、困っている人は助けなさい」、こうなるのですね。

どういうことが起きるかといいますと、たとえば日弁連に電話をかけます。本当の目的は「大江先生の携帯番号が知りたい」ということなのですが、

「清水先生いらっしゃいますか？」

という話から始めます。

「清水先生は今日はちょっといらっしゃいません」

「そうですか。じつは清水先生に書類を送りたいのがあって、ファックスの番号教えていただけないでしょうか」

「そうですか。私ではちょっとそんなことお教えできるか判断できる上司がいませんので、お答えしかねます」

こうなるわけですね。だけれども、

「そうですか。じゃあ大江先生にいつもお世話になっているんですが…」

「あ。大江先生にはいつもお世話になってるんですよぉ…」

「じゃあ、大江先生の携帯番号は…えっと〇九〇の六四……ああ、ちょっと今忘れた。大江先生の番号、今わかります？　だったらそこから清水先生のファックスの番号教えてもらうんで……」

ここまでくれば、

「えぇと、六四七のぉ……」

と始まってしまうわけです。

全く関係ない話を振っておいて、後から言った話がほんとうの目的です。なんか言ってるうちに「この人知ってる人で、そういえば聞いたことある声だなぁ」なんて気分になると、教えちゃうものなのですね、人間って。「吉田さんてそういえばいつも日弁連でしゃべってるし、清水さんも大江さんも知ってらっしゃるって言うし、困ってるんだからいいか」と、こうなるわけです。

人間って不思議なもので、「言っちゃいけないよ」と言われたことを言ってしまうと、心の中にずっと引っかかっています。「ああ、言っちゃったなぁ。なんていいわけしようか」……長い間忘れません。でも、人を助けたこと、困っている人によいことをしたときはすぐ忘れるようにできています、心の仕組みがそうなっている。

ケビン・ミトニックの『欺術』には、そういう、人間の心の隙間をいかに突けば人間はしゃべってくれるか、どんな情報でも手に入れられるかということが、ことこまかに、ぜーんぶ書いあります。すごい本です。読んでびっくりしました。ここまで言っちゃうの？……これをやられると、盗れない情報なんてありません。もう絶対、犯罪ですね。

というわけで、『欺術』にはソーシャルエンジニアリングということが、細かく、わかりやすく、日本語で解いてあります。お時間があればぜひご一読ください。

■人間の心から情報が漏れていくことを一〇〇%止めることはできません

　このソーシャルエンジニアリングに対するセキュリティ対策に限界がある

ためだ、という話になります。人の心には鍵はかけられません。よかれと思ってやった行為まで、「おまえはまちがっている」と責めることはできない。そのひとを責めるのであれば、何を言ってはいけないのか、何が危険なのかということをあらかじめことこまかにみなさんに通知して、問題の起こりうる危険性のある事項をみなさんが正しく理解しているという状態でなければならないはずです。

　でも、そうしたことを国はおざなりにして、

「自治体のみなさんで考えるべきことだから自治事務なんです。国はそれに口を出しません。自治体の箸の上げ下げまで国が意見を言うはずがありません」

みたいなことをまことしやかに言います。もちろん、やれと言ってるのは国です。なのに「口を出しません」と言う。何をしゃべっちゃいけないか、どういうことをしゃべったら問題になるか、情報漏洩につながる行為とはこういうことだ、ということを国は具体的に示していないのです。

　人間の心から、口から情報が漏れていくことを一〇〇%止めることはできません。アメリカの国防総省だってできませんね。できるはずがありません。それができる生き物って、この地球にはいなのです。

できないようになっている。

これがソーシャルエンジニアリングです。

　よって、セキュリティレベルには限界があるのですね。心の隙間にあるセキュリティホールは埋めることができません。

■人的ミスによるセキュリティホールと未知のセキュリティホール

　人間の心から、口から情報が漏れていくのは、「人的ミスによるセキュリティホール」の一種とも考えられますが、それ以外にも「人的ミス」はたくさん起きています。「人的ミス」を完全に防止することは、やっぱり人にはできないようになっているのです。

［セキュリティの限界］

「未知のセキュリティホール」が存在します。

　セキュリティ対策は、やみくもにやっているわけではなくて、すでにわかっている「既

知のセキュリティホール」を埋めるために実施しているのです。でも、世の中には「未知」の穴もたくさんあります。単純に、知られていないから「脅威ではない」と言うわけにはいきません。少なくとも、新たなセキュリティホールが発見されてから、実際の対策が実施されるまでの間はまったく無防備です。

この問題はとくに、自治体のパソコンやサーバに使われている Windows などの基本ソフト（OS）のセキュリティホールが、毎月のように新たに発見されていることと深く関係してきます。

いずれにしても、どれだけお金をかけても「実現できるセキュリティレベルには限界がある」ということになっています。

「未知のセキュリティホール」を使って不正侵入はできる

「マイクロソフト社がパッチを公表する前の『未知のセキュリティホール』を突いてサーバを乗っ取ることなんかできないのに、それをやったと吉田は言っている――あいつはウソツキだ」という話が、一部の人たちの間で言われているそうです。でも、マイクロソフト社がパッチを公開しているもの以外を「未知のセキュリティホール」だと言うのであれば、「未知のセキュリティホール」を突いてサーバを乗っ取ることは、実は誰にでも可能です。

現実のマイクロソフト社が自分たちでパッチ対策を実施するプロセスはどうなっているかというと、「社内で自ら脆弱性（セキュリティホール）を認知して改善対策としてパッチを公表する」というパターンと、ぜんぜん違う他人（利用者など）から「指摘を受けて確認したらセキュリティホールがあったので対策プログラムを作って公開する」というパターンの、二つがあります。ところがマイクロソフト社は今や巨大企業になって、世界中にそのマジョリティを広げてしまっています。そのため、従来なら利用者がセキュリティホールを発見した場合、マイクロソフト社に知らせて改善を求める人がほとんどでしたが、巨大化して動きが鈍くなっているので、

「マイクロソフトがまたやってるよぉ。こないだも注意したのに対策できてないじゃないか。もう報告なんてしないで、こういう問題があるって公表してしまうぞ！」

というホームページが、実は世界中に山ほどできています。そういうサイトはいっぱいあり、著名なサイトがいくつか決まってきています。たとえば、eEye 社（http://www.eeye.com/html/）などが一番有名です。

そこを見たら、今マイクロソフトが対策パッチを作れていない脆弱性にはどんなものがあるか、一覧できます。そういう環境がすでにインターネット上の公開された場所にできている。ここには、

「マイクロソフト社が､対策パッチを公表できていないセキュリティホールはこれだけあります。こうすればこの脆弱性を突くことができます」

という情報が、ずらっと並んでいる。だから､「マイクロソフト社がパッチを公表する前におまえが知ってること自体、おかしいんだ。情報入手先を明らかにしろ！」とか言われても､「あなた、eEye 社のホームページ、知らないの？」という話になる。セキュリティ関係者なら eEye 社のことを知っていてあたりまえなのです。

ネットワーク上にはそういう情報があるわけで､私が特殊な技能を持っているわけでも何でもない。ちょっと英語が分かるとか自動翻訳ソフトを使ってやれば、どんな人でも分かるような情報として「未知のセキュリティホール」の情報はパブリックな場所、インターネット上で公開されているのです。

だから､マイクロソフト社が公表していないセキュリティホールは､知ることができます。その脆弱を突いて、管理者権限を乗っ取る方法まですぐに分かります。技術に精通していればよりリアルに具体的に分かります。

したがって､マイクロソフト社がパッチを公開したら即座にあてるというのは「最低限の防御」でしかないですね。マイクロソフト社が「緊急です、パッチをあててください」と言っているにもかかわらず対応していないということでは、いいわけもできません。損害賠償の全責任を負わなければいけない、ということですね。「だって、メーカーが公表していないものすら､インターネット上で公表されているんだから！」という理屈です。

［セキュリティ対策の基本］

やっておかなければならないことはなにか

■事前の対策＋有事の対策これが理想的なセキュリティ対策の考え方です

最も重要なことは「危機管理」の観点で対策に取り組むことです。セキュリティ事故を一〇〇%防止することはできないから､「危機をできるだけ回避する対策」と、実際の「危機に対処する対策」で、二段階の危機管理をするという考え方です。

（1）事前の対策：「有事の可能性をできるだけ低くする」

まず「事前の対策」として、

論理的にあらゆる「有事の可能性」を洗い出し、ひとつひとつに対する対策を考えて実施することが必要です。これはやはり、ベンダー（納入業者）さんの技術の方、みなさんの

お仲間のコンピュータに明るい方……いろんな方の複数の知恵を出しあって、取り組んでください。ベンダーさんまかせでは、やっぱりうまくいきません。

できるだけ問題が小さくなるように机上で問題をつぶしていくということ――有事の可能性をできるだけ低くするために何をすればよいかをまず考えて、その結果にもとづいた強固なシステムを作り、継続してそれを維持してください。

（2）有事の対策：「有事の被害をできるだけ小さくする」

それでもなにか起こります。さきほどのソーシャルエンジニアリングもそうですが、どういうところに問題があるか勉強し続けないといけません。でも情報を漏らすことはかならずあります。だからリカバリーオペレーション――問題があったときに、被害をできるだけ小さくするためにどうリカバリーするかということが非常に重要な問題になってきます。

■「その場でネットワークケーブルを抜ける」ルールを作ってください

「事前の対策」が十分でないまま、現に全国の自治体でシステムは動いています。

で、「有事」が発生したとします。

「問題が起こってる？　誰かがこのコンピュータに侵入しているみたい」

……「みたい」じゃなくて、きっと入っているのですね。

「情報をとってるみたい……もしかしたらデータベースの情報、抜かれてる、かも……」

さあどうしよう？――となると、上長に報告しなければなりません。でも上長は席を外している。誰かに聞いても「止めていい」って言ってくれそうな人はどこを見てもいません。どうしよう……と思っている間に情報は、ずーと、ずーと、抜かれている。

ではどうしたらいいか

問題があると気づいた時点で、コンピュータに勝つ絶対の方法がひとつだけあります。

「ネットワークケーブルを抜く」

ことです。

コンピュータは疲れません。だから人間よりも早く、いろいろな計算をして結果を出してくれる。だけどコンピュータは万全ではないし、完全でもないし、神様でもありません。ただの計算機、電卓のばけものです。こういうやつらに人間が絶対に勝つ唯一の方法が「コンセントを抜く」ことなのです。電気を与えなければ、コンピュータはただの箱、鉄のか

たまりだけれども、「リカバリーオペレーション」として「コンセントを抜く（電源を切る）」ということを決めて（定義して）おかないと、後から問題になります。

「おまえ、誰の責任で抜いたんだ！　誰が OK って言ったんだ！」

と叫ぶ人が絶対います。

「コンピュータもわかってないで勝手なことしやがって、どうしてくれるんだ。

窓口業務止まったじゃないか」

　そんなこと言われるんですが、情報が出てしまって四〇億円払わされるんじゃ遅いのですね。コンセント抜いた方がよっぽど安くつきます。二〇〜三〇万円払えば、ベンダーさんが、がたがたガタガタ言いながら収まるようになっています。どっちが差し引き得ですかを判断しなくてはいけないのです。その場で判断することは難しいならルールで決めておけばよいということなのです。

　確かに多くの方にめいわくをかける。窓口の業務も止まるでしょう。でもそこでは、毅然とした態度で

「情報漏洩の可能性がありました。今コンセントを抜いてその危険性をくい止める努力をしています。まことにもうしわけありませんが、みなさんにはお時間をいただきたい」

こう言うしかないわけです。

　多くのみなさんの個人情報を守ることの方が大切なはずです。目の前のお客さんがどなりちらすからといって、それに従っていたら、残りの何十万人のみなさんの情報が出ていってしまう。最終的に差し引きしたらどちらが安いか判断できるようにしないといけない。だからこそ、リカバリーオペレーションとして、気づいた人がその場で対処するルールを作っておかないといけないのです。

■住民のみなさんの情報を守るために線を抜いたのに誰かにぶーぶー言われる筋合いはありません

　今、僕は極論を言ってます。要はコンピュータを孤立させることですから。

「その場で線を抜く」ルールをはっきりと決めておかないと、勝手に抜いたとか、誰の判断で抜いたんだとか、誰が抜けと言ったのかとかいう話になる。でも「誰が抜けと言ったのか」という話ではありません。何が起こっているかの方がだいじなのです。そういうことをあらかじめルール（規定）にしておかないと、後で問題になります。

　だからここできちっと、「それでも何か起こるから」とう有事の対策を考えておかなければならないということですね。要は、

誰の責任もないようにしておかないといけない

のです。住民のみなさんの情報を守るために線を抜いたのに、誰かに苦言を言われる筋合いはない、ということです。誰も悪者にならないように、ルール化しておく。それをぜひとも大きな声で言って実施してください。

　たとえば税の「消し込み」のような業務はすごくセンシティブですね。税金払うと自分のところに「消し込み」がされます。それがたとえば三〇〇〇人分、まだデータベースに書き込まれる前に「飛んじゃった」となると、お金のことですから大変です。それをきちんとなおそうと思ったら、一行ずつ目で確認するほかありません。そうしますと、一日一万人くらい窓口に来られる自治体の場合、こういう手間のかかる確認の作業が一日六人の自治体と比べて圧倒的に多くなる。

　むろん、その後本当にそれがきちんと戻ったか、途中で消えているものがないか、という確認があります。それはやっぱり、職員のみなさんにやってもらわないといけないわけです。おそらく業者も手伝ってやるということになりますが、それをやっても何億円にはなりません――でも、このくらいのコストはかかる。だけど「ネットワークケーブル」を抜かないで全部情報漏洩してしまったら何億円になる――ということです。

■「運用・管理状況に対するコンサルティング」はベンダーさんが仕様書まで書いている自治体では必須です

　オーディットをやることで器械やネットワークがどうなっているかはわかった。では運用だとかルールはどうなっているのか？

器械はルールにマッチした動きをしているのだろうか？

器械はちゃんと動いているけどわれわれの運用がちゃんとできていないのではないか？

ということで現状を評価しようというのが、「運用・管理状況の評価」です。でも、自分たちのやっていることを自分たちで評価するのは難しい。中規模以下の自治体では、ネットワークのデザインは仕様書までベンダーさんに書いてもらっているところがほとんどという実情だと思います。何の器械を買ってどういうネットワーク構成にするかということ自体を、ベンダーさんに全部書いてもらっているわけですから、そもそも自治体自身に現在動いているネットワークが分かるわけないのです。その上担当はぐるぐる替わっている。「前任者がやりました、そんなもの俺に分かるわけねえ」ということになります。そこで、

第三者に客観的に「運用・管理」について評価してもらいましょう。

同時にアドバイスもいただきましょう。

ということが大切になってきます。

「あなたの既存のネットワークのセキュリティレベルを評価しました。器械は五段階評価の４ですが、運用がぜんぜんでたらめなので、総合レベルでは２しかあげられません。落第点ですね」

「では、どこを直したらいいの？」

という相談ができる相手を見つけないといけません。これが、

「運用・管理状況に対するコンサルティング」

です。で、コンサルタントとディスカッションすることによって、セキュリティのレベルを上げていくことができるようになってくると、実は必然的に、現在のネットワークのデザインに「セキュリティ上のボトルネック」が見つかってきます。そのため「ネットワークのこの部分は意味がないですね。この部分はこういう構成にした方がいいですね」という話が出てくるのですが、そこから始まるのが、

「既存ネットワークデザインの改善」の相談ということになります。

　オーディットのようなある程度おまかせ可能なサービスとは違って、運用・管理のコンサルティングは、ツーウェイの「相談」です。担当者とコンサルタントが相談して、納得したら担当者が実行する――そういうものがコンサルティングです。

■「相関分析」の重要性をぜひ理解してください

　運用・管理状況の評価をする上で、ネットワークがどのように運用されているかを調べるだけではなくて、「あなたのネットワークが日々どのようなセキュリティ上の脅威にさらされているか」も調べる必要があります。それを明らかにするのが「相関分析」です。

　これはけっこうめんどうな作業なのですが、「相関分析の実施」ということを、ぜひみなさんの認識として持っていていただきたいと思っております。何の話かというと、

ネットワークは「一個の器械」のように思いますが、実はたくさんの器械で構成されているわけです。たとえば「ルータ」という器械があります。ネットワークの出入り口です。電話線を使って LAN の間を接続するときの出入り口には「ダイヤルアップルータ」が使われます。

　それから「ハブ」とか「スイッチ」と呼ばれる器械があります。ネットワークケーブルを分岐・合流させる装置です。

「サーバ」があります。ＷＥＢサーバやメールサーバ、データベースのサーバなどいっぱいある。

「ファイアウォール」もあります。自治体によっては「不正侵入検知システム」があるかもしれません。

ほかにもいろいろな器械が使われています。たくさんの器械でネットワークは構成されているわけですね。こういう器械は一個ずつが「ログ」というそれぞれの器械の動作の記録をはき出しています。それから、システムの運用上の記録があります。たとえば「サーバルーム（重要機器室）の入退室記録」のような記録が作られているはずです。

何か問題が発生したとき、たとえば不正侵入を受けたときには、そういう、記録を全部集めてきて、時系列に並べて相互につじつまが合っているかじっくり時間をかけて分析していきます。分析は専門技術者が行います。これが「相関分析」です。これをやれば、実際に何が行われたかが分かってきます。「やられた」というサーバのログだけを見ても分かりません――プロ中のプロが分析しても「たぶんこうだろうなぁ」ということぐらいしか分からないので、本当にすべてを知ろうとしたら、今言いましたルータやスイッチやサーバなどの全部の記録を集めてきて、「相関分析」をします。

「管理・運用の評価」の中で行う相関分析の実施は、たぶん不正行為が行われていない時のログを集めて行う分析ですが、それでもいろいろなことが分かります。

たとえば、相関分析の結果、「入退室記録もないのに、祝日の深夜にデータベース更新がかけられていた」ことが分かるかもしれません。よく調べてみると、この入退室記録は実は別の部屋のもので、サーバルームの入退室記録は完備されていなかった、ということが分かるかもしれません。逆に、今まで気づかなかったデータベースの不正な書き換えが発見されるかもしれません。不正侵入には至らなかったけれど、サーバが乗っ取られそうになっていたことが分かって改善点が指摘される場合もあるでしょう。ネットワークに対する日常的な脅威の現実が明らかにできるわけです。

もう一つ重要なことは、

相関分析に必要とされている記録（ログ）が、意図した手段によってきちんとそろえられるかどうかを確認することです。これがうまくできないということは、ネットワークのどこかに問題があるか、あるいは管理や運営のどこかに問題があることを意味しています。そのために、「何か起きた」とき相関分析によってネットワークの何を改善すればよいかを明らかにすることができない――ということがないように、きちんと確認しておいてください。「ログ」そのものも法廷で記録として通用するような正確で改ざんされていないことを担保することも必要になります。デジタルフォレンジックが問われるでしょう。

実は、この「相関分析」をリアルタイムで行うことは「究極のセキュリティ監視」だと言われていて、つい最近になって製品も発売され、自治体のみなさんも注目しています。

■何か困ったときに相談できる人を作っておいてください

　セキュリティ対策のサービスメニューとして、「緊急レスポンス」も広く活用されています。

　何か困ったときに相談できる人、技術的に明るい人、具体的に親身になってくれる人――それをキチンと作っておくということです。ベンダーさんの方かもしれませんし、緊急レスポンスを外部の技術者にアウトソースする場合もあるでしょう。自治体職員の中で特にシステムやネットワークに詳しい人、職場の上司かもしれません。そういう人を作っておく、ということが非常にだいじだということです。

「なんかおかしいんだけど、どうすればいいの？」

ということを、その場ですぐに相談できる。最初に、どんなアクションを起こせばいいのか――ファーストエイドと呼ばれている一番最初の手当てを相談できる相手を作るということです。で、相談する相手を作るということは、

「すぐに相談する」というルールを作る

　ということです。とにかく、今何かおかしい――という時に一番最初の手当てを施すのが緊急レスポンスですが、「する」というルールを持っていなければ、「おかしいなぁって思って見てたんですが、やっぱりなんかおかしくなってたんですか」で終わってしまいます。

　重要なのは「ネットワークケーブルを抜いてください！」と言ってもらえる相手を作っておく、そう言ってもらえるルールを作っておく、ということですね。そうしておけば、被害を小さくすることができる、たくさんの住民のみなさんが被害を受けなくてすむ。担当者も悪者にならないですむ。

　そういうサービスを利用できるようにしておけば、メニュー化されているし、契約書なり規則なりがあってルール化されているわけですから、安心してアクションが起こせます。

　住基ネットとそれに物理的に接続された自治体のネットワークのセキュリティを考えた場合、二十四時間三六五日の「セキュリティ監視」は必要です。そんなにお金のかかることをと言われる方も多いのではないかと思いますが、理由は簡単です。

　九時―五時の勤務時間には誰かがシステムを見ている可能性が高いので、「何かが起」きても気づくかもしれません。でも、たいていのサーバは二十四時間運転されています。誰もいない深夜に「何かが起」っても誰も気づきません。翌朝になっても誰も気づかないかもしれません。だから二十四時間のセキュリティ監視は必要なのです。「うちのサーバ

は、時間がくるとタイマーで電源を切るから大丈夫だ」という自治体さんがあるかもしれません。でも、確実にタイマーで電源が切られていることが保障されているでしょうか？

これが、二十四時間のセキュリティ監視が必要になる理由です。ネットワークを運用するには、お金がかかります。

ここで少し、「リアルタイム相関分析」について考えてみたいと思います。

リアルタイムで実施することは、人間わざではできません。分析する情報の項目が、ルータ、ファイアウォール、不正侵入検知システム、各種サーバなどのログや警報などすごい数になっています。それらを並列で見比べて、つじつまが合っているかどうかを人間の目で瞬時に判断することはとうていできません。器械にやらせるしかない作業です。

そんなリアルタイム相関分析によるセキュリティ監視が、つい最近になって数社から提供され始め、注目されています。リアルタイム相関分析が、必要とされる情報のすべてにわたって実施できたら、確かに究極のセキュリティ監視と言えるでしょう。きちんと動作すれば、本当のプロ中のプロでなければ侵入に成功しなくなります。

しかし「リアルタイム相関分析」は、現在ようやくサービスとして出始めたところです。まだまだ、コスト、クオリティ、チューンアップの手間など、課題はたくさんあります。

■それでも実害は発生するのだとしたら、「最終的なリスクヘッジは保険しかない」

さて、お金もかけ勉強もして、必要なセキュリティ対策をかなりのレベルで実施しました。でも、セキュリティは一〇〇%ではないので残余リスクが残っています。

……とういことで、「保険」はその残余リスクをヘッジする究極の対応策です。

最近日本の保険会社が、自治体を含めて上場会社にだけ、個人情報の漏洩に対する保険を作りましょうということを言っています。二月半ばの日本経済新聞だったと思います。ところがその二日後に、「四五〇万人の個人情報漏洩」と報道されて、保険会社は大変な状況ですね。「やるといったけどやばいぞ……」。

「保険」というものは究極の考え方です。アメリカの CIA や FBI の IT セキュリティのコンサルタントをしているカウンター・ペインという会社があります。ここの技術責任者をしている取締役に、ブルース・シュナイアーという暗号の世界では「神様」と呼ばれている男がいるのですが、彼が言っています―― IT セキュリティの究極は保険だ。人に依存しても無理、器械に依存しても無理。最終的なリスクヘッジは保険しかない ――彼の『暗号の秘密とウソ』（翔泳社刊、二〇〇一年）という本の中に書かれていることです。

■「パッチがあてられない」というのはウソです

　先日、ある講演会で出た質問に、

「パッチあてろと言うけど、『パッチあてたら動かなくなっても知りませんよ』と業者に言われました。だからパッチなんてあたらないと言われたけど、なんで？」

というものがありました。

これ、ウソです。

　パッチはあたるんです。で、プログラムが動かなくなったら、それは業者の責任です――それはもう、まちがいありません。はっきりしています。

　でも、業者はそう言う。なぜかというと、技術者は後ろ向きの仕事はしたくありません、作って納めたら終わりなんです。でも、パッチをあてるたびに、納めたプログラムの全部の機能をひとつひとつ動かして、「収税消し込み動作 OK、……」ってやらないといけない。機能のありとあらゆる組み合わせの作業項目表を作って、ここはまる、これはいけた、これもいけた――という形でチェックしないと、「プログラムが動かなくなる」ことを予測できないのですね。こういうチェック作業は何も新しいものを生みません。後ろ向きの仕事です。だから技術者はやりたくない。

　営業課長さんあたりがお客さんのところで「パッチあてて」と言われて「はい、見積ってみます」と答える。ところが帰ってきて技術担当に相談するとこう言われます。

「えー、そんなのやるのぉ？　やるんだったら、僕、会社辞めるもんね」

　そんなわけで

「わかったわかった。何とか断ってくるからよぉ、どう言えば断れるんだ？」

「そんなのやったら、業務のプログラム、動かなくなっても保障できないって言ったらいいんじゃないですかぁ」

「じゃあそう言うよ」

　というわけで営業課長さんはお客さんにそう言う。

「何とかお客さんは納得してたからさ、お客さんとの話はずっとそれで通せよ！」

「わかったぁ」

――という話に業界ではなっているのですね。これが真実です。でも、パッチがあたらないようなプログラムを納めた業者が悪いんです。ここだけは覚えておいてください。

　これは当然、住基ネットの業務用プログラムの問題だけではありません。既存住基やそのほかの事務処理で使っているプログラムでも同じです。そこまで含めて「全国いっせい

に、パッチをあてる方法」を考えておく必要があったのです。

　簡単ではありません。でもやっぱりパッチは、きちんとあててください。

緊急対策

委託業者とのサービスレベル・アグリーメント：ＳＬＡを確認してください

　これは何かと言うと、自治体のみなさんをいかに守れるか、という問題です。損害賠償が求められたとき、「ここまでやってたんですけどダメでした」と言って責任を分ける切り札がこれです。

　業者の方にアウトソースしたときの、サービス上の契約書に、

どこまでが役所の仕事で、どこまでが業者さんの仕事です ――という、

「責任分界点」がはっきりと書かれているかどうか

という問題です。

　現実の市町村の契約には、「サービスレベル・アグリーメント」はほとんど書かれていません。自治体のなかで今までＳＬＡを明記してきたところというのは、たいへん少ないのです。人口が三〇〇万人以上いるような自治体なら、業者さんの方から喜んで作ってくるのですが、そうでなければ SLA は書かれていないでしょう。

　これがないと役所のみなさんは守れません。窓口で被害を受けた住民のみなさんから、

「やっぱりお前たち、何も考えてなかったんだろう！　だからこんな問題が発生したんだ」

　こう一方的に言われるに決まってます。いいわけできません。だからみなさん、現在この責任分界点がどうなっているかをぜひ確かめてください。

　日本の行政機関や自治体は、「性善説」で永年にわたって業者との関係を構築してきています。だから「SLA なんて今さら作れない。コミュニケーションコストだって無視できないし」という声も強い。でも、これって、ただのナニワブシです。

■ネットワーク管理者と協力関係を作り上げるために

　さて、セキュリティ対策をうまく実施していくために、「ネット管理者」の立場についてもご理解をいただきたいと願っています。「ネット管理者」はつらいです、本当につらいです。

よく言われます。

「情報化の利便性とセキュリティのバランスをちゃんと取ってね！」

――そんなのネット管理者に分かりません。システムを運用する人が「何をどれだけ守りたい」のか、「利便性をどれだけ犠牲にしてもセキュリティを優先するのか」を決めてください。それはネット管理者が勝手に決めることじゃありません。

「ウチのセキュリティはだいじょうぶかね？」

――そんなことネット管理者に聞かれてもこまります。私がどんなに一生懸命働いたって、セキュリティは一〇〇％にならないのですから、情報漏洩はいつだって起きる可能性があるのですね。

人手と予算は？

――コスト削減をまっさきに求められるのがネット管理者です。

年中多忙なのに、でも評価は？

――事故は起きなくて当然、なんかあれば「お前のせいだ」となる。セキュリティはそもそも利益を生まないのですね。だから個人情報の保護と運用の板挟みにあいます。

そして情報収集に終わりはありません。ハッカーさんとのイタチごっこ、新しい技術がつぎつぎと出てくる。

お前技術担当だろう！

――知っていて当然のように扱われます。迷惑千万です。

だから問題発生でスキルが疑われることになる……

「お前、本当はたいしたことないんじゃないか？」

ネット管理者なんてそんなものなのですね。押しつけられてもこまります。だからみんなで考えないといけない問題なのです――セキュリティはネット管理者だけに押しつけるような問題じゃない、ということですね。

パッチは、無料でできる有効なセキュリティ対策です

パッチって何？どうやってパッチをあてるの？

マイクロソフト社は「パッチ」について、ホームページで次のように説明しています。

インターネットにはウイルスや、ハッカーなどからの不正アクセスといったさまざまな危険性があります。コンピュータのセキュリティ対策を行わないとこれらの問題により、

ウイルスに感染したり、ハッカーなどの不正なユーザーから個人情報が盗まれるといった被害を受ける可能性があります。これらの被害を受けないようにするためにもセキュリティ対策が大切です。セキュリティ対策を行うためには次に紹介する対策を行うことをお勧めします。Windows Update は、コンピュータの状態を診断して、Windows を常に最新の環境に整えるオンラインサポート機能です。こまめに行うことで、ウィルスが悪用するセキュリティホールを修正し、悪質な攻撃に負けない頑丈な環境を構築します。これがパッチ対策です。

（http://www.microsoft.com/japan/security/security_bulletins/より）

これを読むと、「不正アクセスを受ける危険性」はインターネット上に一般的に存在しているかのような印象を受けるかもしれませんが、少なくともここで公開されているパッチが修正しようとしている「セキュリティホール」は、マイクロソフト社のプログラム開発に問題があって発生したものです。マイクロソフト社はこのミスに責任を取るため、対策用の「パッチ」を作って公開しています。

これは自動車の「リコール」とよく似た考え方だと言ってさしつかえないと思うのですね。自分で作ったものに自分で問題を発見しました、だからこうしてください――ということです。自動車だったら「部品を交換させていただきますので、お近くのサービス店においでください」ですが、Windows の場合は「自分で対策をしてください」という話になっているのです。

「パッチ」は、プログラム（ここでは Windows やそれに付属しているインターネットエクスプローラーなど）のミスが原因となって攻撃を受ける可能性がある時、そのプログラムを書き換えて攻撃を受けないように修正する小さなプログラムです。自宅のパソコンなどでは、Windows Update の機能などを使って自分で適用する（パッチをあてる）ことができます。でも、企業や自治体の中で使っているパソコンやサーバの場合は、自分で勝手にパッチをあてることはできないようになっているのではないかと思います。その場合はネットワーク管理者がパッチをあてるか、「こういう手順でパッチをあててください」という指示をみなさんに出している「はず」です。

Windows のパッチってどのくらいあるのか

では、このような脆弱性の問題――修正プログラム（パッチ）は、何個あるのかというと……パソコンをお持ちの方は、ホームページブラウザ（インターネットエクスプローラーなど）で次のＵＲＬにアクセスして、ゾッとしてください。めっちゃくちゃあるんです。だから大変だということなんですが。

http://www.microsoft.com/japan/technet/security/current.asp?sel_id=Windows+2000&

info=ALL&optTop=all

（このＵＲＬは将来無効になるかもしれません。その場合は、マイクロソフト社のトップページから「セキュリティ」および「その他のセキュリティ情報」などをキーワードにして探してください）

このページには、住基ネットの CS サーバや CS 端末で一般的に使われている Windows に関連するセキュリティ対応「パッチ」だけで、

二〇〇四年八月四日現在　一一五件

が公開されています。このページ全部の「パッチ」の総数は

三〇八件

でした。

皆さんがいま使っておられるサーバやパソコンなどの基本ソフト（OS）と呼ばれている一番重要なプログラムには、いくつか種類があるります。マイクロソフト社の基本ソフトは Windows と呼ばれていますが、それにも WindowsNT 4.0、Windows2000、WindowsMe、WindowsXP だとか、Windows2000 Server、Windows2000 Server Advanced などいっぱいあります。パソコンやサーバー用の基本ソフトを発売しているのはマイクロソフト社以外にも数社あって、MacOS とか Linux といったそれぞれ独自の種類の基本ソフトを提供しています。

皆さんがお使いの基本ソフト（OS）がその内のどれかを調べて、Windows の場合はここにある該当するパッチが、いまどこまであたっているかを調べてみてください。すでに使っている方がほとんどだと思いますが、Windows Update という機能を使うと、自動的にこれを調べてくれます。

Word や Excel などにもパッチがあります。あててください

それから、このページで公開されているいろいろなセキュリティ情報（パッチ）には、「Microsoft Word」とか「Microsoft Excel」などと書かれているものも含まれています。何かというと、CS 端末もそうですが、パソコンが Windows2000 などを使っていて Windows のパッチはあててあるから安心だと思っていると、Microsoft Word などマイクロソフト社のワープロや表計算用などのプログラムが使われていて、いやらしいことにこれにもパッチがあるのですね。それがあたっていないと、まあ中級以上のコンピュータ乗っ取りが大好きなお兄さんたちが「Word の脆弱性がある！」と言って管理者権限を奪取する、ということが起こります。

非常にやっかいです。Windows（基本ソフト：OS）のパッチをあてているだけではダ

メで、ほかにアプリケーション（プログラム）が動いていると、そのアプリケーション自体の脆弱性を突いて管理者権限がとれることがあるのですね。

これはマイクロソフト社のプログラムに限りません。たとえば常識的に考えれば、住基ネットの CS サーバや CS 端末で動いている住基ネットの業務用プログラムにだって、セキュリティ対策の「パッチ」はあるはずです。おそらく「バージョンアップ」とか「機能追加」という形で、地方自治情報センターから配布された「追加プログラム」に含まれていると考えていいでしょう。

［情報セキュリティ 10 原則］

■できないことはしない、しなければ問題は発生しない

最後に、みなさんといっしょに考えてきた情報セキュリティについて、「１０原則」という形でまとめてみました。

この「原則」は僕の発明ではありません。

RSA 暗号システムというものの開発者アディ・シャミア博士というセキュリティの専門家がいます。①〜⑨の「原則」は、彼が講演の中でしばしば言っていたことばを、そのままままとめたものです。僕が付け加えたことは、これの⑩番だけ。あとは全部シャミア博士が言っていたことです。

原則①　パーフェクトなセキュリティを求めるな

一〇〇%は求められないよ！――ということです。何かが必ず起こると考えて、「有事の対策」を立ててください。

原則②　まちがった解を解くな

問題はシステムやネットワークの上で起きるとは限りません。銀行の小切手詐欺の内、ネット犯罪被害は一〇%です。むしろ問題の九〇%は、ネットワーク以外の場所で発生していたりするのです。

だから、僕が怖いと言ってるのは、ネットワークの何もかもが怖いと言っているわけではないのです。そこを勘違いされないようにお願いいたします。

原則③　全体でセキュリティの問題を考えろ

ここ一カ所だけ安全だったらいいという話じゃないのですね。ほかにつながっていると

ころもぜーんぶ見ないと、何にもならないですよ、という話です。それと、ネットワーク管理者や業者まかせにしてもいけないのです。

原則④　暗号のかけ過ぎは正しくない

　何でもかんでも「良く」しちゃうと、やりすぎになります。やりすぎでもうかるのはベンダーさんだけです。

原則⑤　高価にするな（何かを買えばすむ話ではない）

　やっぱりやりすぎはダメ、ということですね。業者さんがこんなふうに勧めるかもしれません。

「不正侵入検知システムがあったらいいって言ってますからね。長野はうるさいんですよ。長野に文句言われないようにしましょう。どうぞこの器械買ってください。三〇〇万円です！」

　そんなものすぐ買う必要はないのです。

　まずパッチをあてればいいのです。パッチは「無料でできるセキュリティ対策」ですね。これを忘れていくらお金をかけたって、初心者さんにやられます。パッチから始めてください。ものを買うのはその検討後にしましょう。

原則⑥　防御ラインは一つだけでは意味がない

　ファイアウォールがあるから安全だ――そんな話はウソです。いろんなところから、統合的に、多角的にものごとを考えてみましょう。

原則⑦　アタックがあることを忘れるな

　プロ中のプロ以外は、いきなり本丸にはたどり着けません。チョロチョロと兆候があるのですね。それをみのがしていたらダメです。そこで防ぐのが皆さんの仕事になるのだと思います。でも、今の自治体にそんなことができるのか、というところが問題なのですが……。

原則⑧　システムを信じるな

国が安全だと言ってることを鵜呑みにしてると大変なことになります。

原則⑨　人を安易に信じるな

これは「ソーシャルエンジニアリング」のことですね。何を言ってもいいか、何を言ってはいけないか――これをはっきり「ルール（規定）」にしておいてください。

原則⑩　できないことは、するな！

「できないことはしない」

これが一番正しいことなのかもしれません。僕はそう思って生きております。だからできないことは「すいません、できません」と言います。

「でも、お前できるみたいに言っただろう！」

「僕じゃなかったら、できる人はいると思います」

そういう話なんですね。僕にはそんな能力はないです。頭もそんなに賢くないと思います。でも、こういうことはやっとかなきゃいけないんだろうな、ということはわかります。だからできないことはしない。しなければ問題は発生しない――僕はそう思っています。

最後に

マスコミなどからはさんざんに書かれるという経験をしてき吉田ですが、捨てる神あれば拾う神ありで、少数ながら吉田の活動に「がんばれ」と激励をくださった自治体の担当職員の皆さんに感謝したいと思います。数行の激励メールに励まされたことが、吉田のダイナモを回してきました。

現場を担当する自治体職員や民間のネットワーク管理者のみなさん、そして住基ネットの問題の解決に強い関心を寄せている地域住民と自治体議会議員のみなさんの努力に少しでも役立つことを切に望みます。

下記書籍の本文から内容を抜粋しています。

地域住民と自治体のための住基ネット・セキュリティ入門

吉田柳太郎・西邑亨著／七つ森書館刊

長野県本人確認情報保護審議会　委員名簿

氏　　名	職　　業　　等
櫻井（さくらい）　よしこ	ジャーナリスト
佐藤（さとう）　千明（ちあき）	㈱長野県協同電算ネットワーク部長
清水（しみず）　勉（つとむ）	弁護士
中澤（なかざわ）　清明（きよあき）	上伊那情報センター所長
不破（ふわ）　泰（やすし）	信州大学大学院工学系研究科教授
吉田（よしだ）　柳太郎（りゅうたろう）	ネットワークセキュリティコンサルタント

（注）50 音順