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保護審議会第 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．

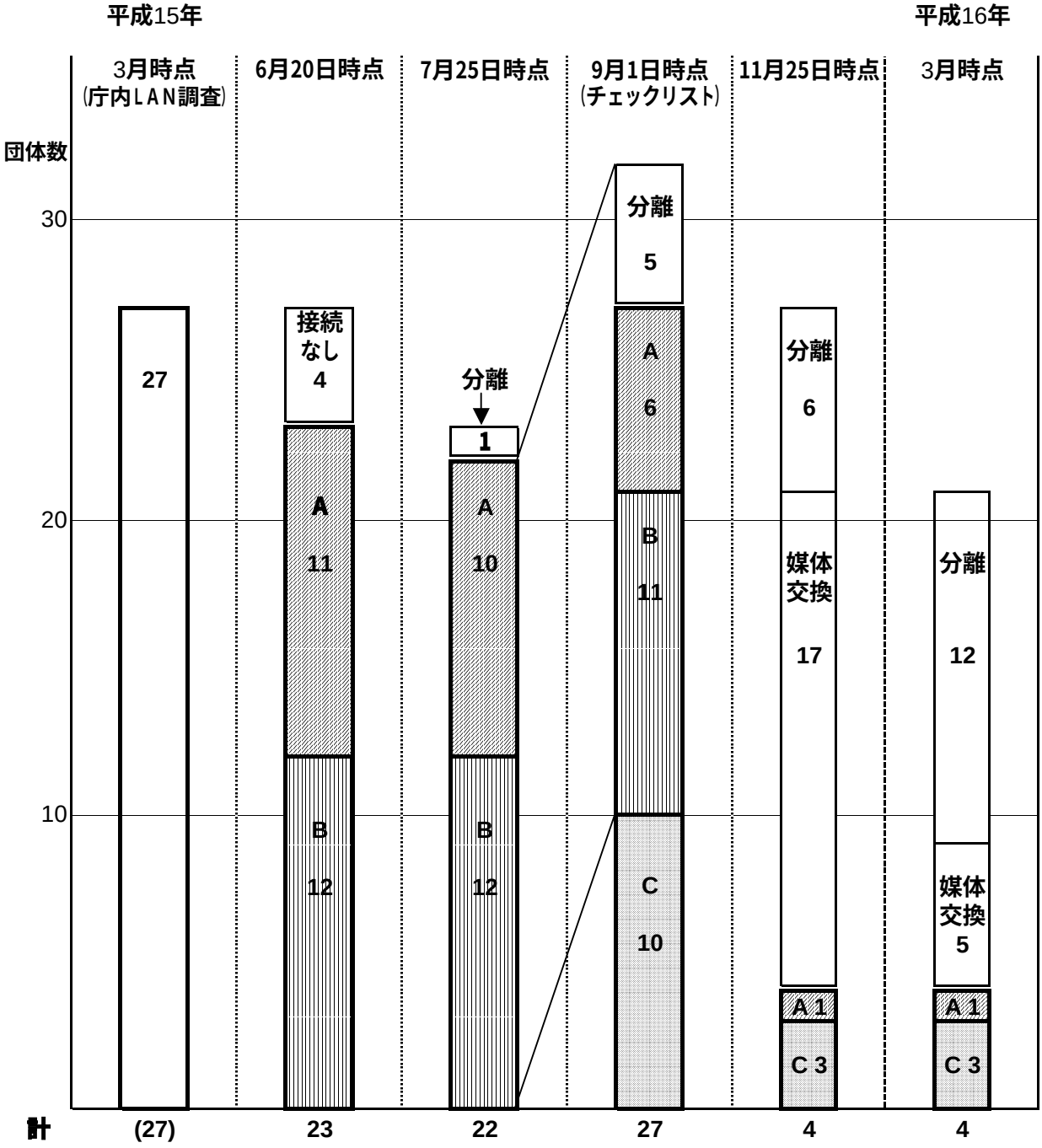
6情報が「たかが6情報」なのかどうか，それは個人お一人お一人によって違います．おそらく私も含めて大多数の方にとっては「たかが」だと思います．しかし，ご主人の家庭内暴力から逃れるために子供を連れて身を隠しておられる奥さん（子供の就学のために住民票はその町で登録していて，ご主人にはＤＶ法や住基法令により閲覧不可にしている）にとって，新しい住所は「たかが」ではすみません．同じような事情をもたれた方は少なくないと思います．

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．