２００３年5月２８日

長野県本人確認情報保護審議会第１次報告

長野県本人確認情報保護審議会

１．はじめに　（担当：櫻井委員）

長野県本人確認情報保護審議会は２００２年１２月に発足した．これまでに約６ヵ月にわたり，住民基本台帳ネットワークの中で，県民の個人情報を守りながら如何により効率的に地方自治を推進出来るのかについて，議論を重ねてきた．

県民の個人情報保護に適切な対策を立てるには，まず県下１２０の自治体における住基ネットの実態を知る必要があった．そこで審議会は，審議会独自のアンケート調査を行った．県の担当課に調査を委ねることも出来たが，国が進めている政策に対して，市町村の立場から県に率直な意見は言いにくいという関係があることを承知していたので，市町村の率直な意見を引き出すために，審議会が自ら調査することにした．同調査には，県はアンケート用紙の郵送にのみ関与し，個々の自治体の回答は，直接委員長にＦＡＸ又は郵送してもらった．内容は６名の審議会委員のみが閲覧出来ることとし，県には統計処理された結果だけを報告した．こうして各自治体の匿名性を守ることで，忌憚のない意見を引き出すことが出来た．

アンケートには１２０市町村中１１２の自治体が回答し，住基ネットに関する関心の高さが示された．

調査結果は，実に衝撃的だった．住基ネットの仕組みや管理運営について最も詳しいのは，担当職員（９６％）であるが，担当職員の９１％が住基ネットは「自治体の負担が大きい割にメリットが少ない」と答えたのだ．さらに５６％が「住民のメリットが少ない」又は「本人確認情報の漏洩などプライバシーが心配」とも答えた．

住基ネット周辺機器の仕様書の内容のかなりの部分は地方自治情報センターが指定しているとは言うものの，９９％の自治体が独力で仕様書を作成することが出来ず，全て，或いは殆ど全てを，業者などに頼っていたことも明らかになった．

外部依存度の高さ，及び住基ネットは使う税金の割に何のメリットもないという意見の強さは，審議会委員らの予想を遙かに越えるものだった．

住基ネットの導入に際して，片山虎之助総務大臣は，この仕組みが地方自治業務の合理化につながり，国民にとっては全国どこでも住民票が取得出来るなど大層便利になるとして，そのメリットを強調した．だが，アンケートの回答からは，片山大臣の国民へ

の説明とは正反対の実情が浮かんできた.

アンケート調査でさらに目を開かせられたのは，自由記載の欄に綴られた訴えである．そこには自治体職員の本音が，住基ネットの矛盾や問題点を指摘する形で噴き出していた．不満の一つは，住基ネットは自治体が責任を負うべき“ 自治事務 ”とされた点だ．法律上は自治事務と位置づけられながら，実際は国及び国の意向を受けた地方自治情報センターの指示どおりにやることを強く期待されていることに，多くの自治体は反発していたのだ．自由記載欄には次のような記述が並んだ.

・自治事務でありながら，その意識の決定権が市町村にない.

・システムハードを取ってみても，法により市町村に整備を求め，その管理は市町村の責任において行えというように捉えられ，地方分権どころか目的のために手段を選ばずの感がある.

・国の一方的な押しつけと言わざるを得ない

・実態は自治事務というより受託事務に近い性格でありながら自治事務とされた．導入にあたっても自治体の負担が大きい.

・自治事務でありながら，国から押しつけ或いは責任転嫁されている.

・事務処理などの効率化が図られるわけでもなく，負担はより増大するばかりである.

また，財政面からの住基ネットへの批判も多数あった．情報が漏洩するなどの場合の予想外の出費も含めての質問には，「財政難で本当に大変です．（住民票サービスによる）収入は減るし，交付税も減っている」など，悲鳴に近い声が多く，次のような訴えもあった.

・住基ネットの運用そのものが予想外の出費である.

・交付税措置が取られているとはいえ，今後新たなシステムなどの導入を求められる場合は不安.

・対策はない．財政難のため心配している.

これらのコメントから，「住基ネットは全国津々浦々の自治体から，こんなものを作ってほしいという要望があったから，総務省が作った」と述べた片山大臣の言葉と現実の間には大きなギャップがあることが見てとれる.

いわば偽りの言葉から生まれた住基ネットは，その一点において民主主義の根本的価値観を侵害するものである.

アンケートだけでもこれほど強い反対の意見や訴えが出てきたことに審議会は注目し，さらに自治体の聴き取り調査に乗り出した．対象となった自治体は，自治体人口の差や北部・中部・南部の地域差を考慮して，市３カ所，町４カ所，村４カ所の計１１カ所を選んだ．この選定作業においても，県関係者は関与しておらず，委員のみで選んだ．選んだ市町村名は県に知らせていない．訪問先への交通は公用車を使用しているが，運転者は住基ネットに関連しない業務の職員を充て，聴き取りに県関係者は立ち合っていない．６名の委員が２名乃至３名に分かれて，自治体に足を運び，担当職員及び担当課長を含めて面談，住基ネット機器の設置されている現場も調査した．

この調査内容についても委員は各自治体の聴き取り内容を知ることが出来るが，県に対する報告では，各問題の答えにスクランブルをかけ，回答内容から特定自治体が分からないよう配慮した．こうして得た現地調査結果は，俄には信じ難い内容だった．

まず，住基ネット関連機器が置かれている環境である．ある自治体では，庁内の同一セグメントにイントラネットと従来の住基システムなどの業務系ネットが同居しており，加えて，インターネットと住基オンラインが同一ネット上に置かれていた．インターネット経由で全ての情報が取られかねない事態である．

住基ネット端末機が収容されているＨＵＢポートが，無雑作に机の下に剥き出しになっており，その空き部分にパソコンを接続することが出来るようになっていた自治体もあった．パソコンを繋げば，住基ネット情報はいとも容易く取られ兼ねない．

業者が住基オンラインのバッチ処理とシステムの遠隔監視，保守を担当している自治体もあった．つまり，業者は外部からリモートで住基ネットに接続して操作することが可能なわけだ．

仕様書は全て外部業者に委託し，セキュリティの確保も外部業者に頼りきりの自治体は，情報漏洩をチェックすることは不可能で，業者を信ずるしかないと述べた．担当職員は，ファイアウォールがあるから安心だと信じているとも語った．但し，これらの職員はファイアウォールの仕組みを知らなかった．

担当職員でセキュリティについて安心していると答えたところは，審議会の聴き取り調査ではゼロであった．反対にセキュリティに関する不安の声は，極めて強かった．

担当責任者なのに「コンピュータ操作もよく分からず，とにかく不安」と述べた職員は，問題が発生したときの対応が全く分からず，ウイルスなどの侵入は誰がチェックしてくれるのかと問うてきた．

国の指示に従っているが，国がセキュリティについて何を保証してくれるのかが不明であり，不安であると述べた職員は，重い責任に夜もなかなか眠れないと訴えた．

春の人事異動が早く来てほしいという声，これほど人事が待ち遠しかったことは今迄なかったと語った職員もいて，担当職員らの話は実に悲惨だった．

各自治体で約２時間づつかけて語り合ううちに，本音の話が相次いだ．担当職員も課長も，住基ネットについては，利便性も必要性も疑問だと述べ始めたのだ．彼らは事務効率化と費用の両方でデメリットしか発生しないと断言，「市町村のシステムだと国は言うが，実は国のためのシステムである」，「住基ネットのメリットは市町村にも住民にもなく，国による個人情報活用にある」と喝破したのだ．

「住民へのメリットはない」「市町村へのメリットもない」との訴えは，少数の自治体の声ではなく，行く先々で繰り返し強調されたものだ．「国の押しつけ」であり，本音は住基ネットを止めたいのだとの訴えも少なくなかった．

小さな自治体にとって住基ネットからの離脱を望んでも，国に楯を突くことになるので怖くて言い出せない．だからこそ，県が県下の自治体全てを纏めて住基ネットから離脱してほしいと要望した自治体もあった．国の方針に背く大胆な要望にもみえるが，財政的負担の重さ，情報漏洩のリスクの高さ，その場合の自治体の法的責任の重さを考えれば，当然の要望でもある．

その後も審議会は市町村の調査を続け，さらに驚くべき事実に直面した．県下の２７の自治体でなんと，住基ネットとインターネットが物理的に接続されているのだ．この事態は真に重大であり，長野県下の自治体に内外からインターネット経由でアクセスが殺到し，情報が流出する恐れがある．そのような事になると，長野県民と県下の自治体のみならず，日本全国の自治体と国民全員が被るであろう被害は測りようがない．

そこで審議会は，県に対して直ちに２７自治体に適切な処理をするようお願いした．これを受けて県は，抜本的な解決策として，インターネットを利用する系統と，住基ネットを利用するネットワークを切り離すために，自治体のネットワークを実質的に保守管理している業者に対して，実態の確認とネットワークの構成について要件整理，具体的構成案の提示を依頼した．その結果，役場内のネットワークだけでなく支所，支庁舎との接続の関係で，思った以上の改造，コストが必要になることが判明したため，現在取りうる対応策の検討を進めているところである．

以上の説明及び添付資料から，長野県内の市町村の実情が如何に深刻な問題を抱えているかが明らかになった．

ここで注意していただきたいのは，長野県の実情は，決して長野県に特異なものではなく，全国の多くの市町村に共通しているであろうという点だ．そのため，長野県外にも，住基ネットとインターネットが繋がっている自治体は必ずある，しかも，かなりの数，あると見るべきだろう．したがって長野県が対策を立てても，コンピュータネット

ワークで繋がっている他県の何千という自治体も同じように，対策を講じなければ，県民の個人情報はいとも容易く流出する．

住基ネットがインターネットに接続されていたことは，一言で言えばセキュリティ以前の問題であるが，そのことに対処したとしても，長野県下の自治体で住基ネットの情報が守られるかと言えば，その保証もない．詳しくは３章の記述に見られるように，ある程度信頼出来るところまでセキュリティを高めるには，最終的には数十億円のコストが必要だ．長野県にも県下の自治体にも到底背負いきれない額である．しかもこの高額のコスト負担は一度切りのものではなく，未来永劫続く性質のものだ．当然のことだが，住基ネットは自治事務であるため，コストは地方自治体の負担である．そこまでの財政負担を覚悟して続ける価値が，住基ネットにあるのか．住民への責任として地方自治体はこの点をよく考えなければならない．

昨年８月の導入以来，この間の政府の動きには，納得出来ないことが多々ある．住基ネットによる本人確認情報は当初９３の行政事務に限って使われると説明された．それが今は，２６４事務に広がっている．中央政府の行政事務に加えて，地方自治体の行政事務にも住基ネットの使用を拡大すべく，働きかけが行われてきた．

１月２４日の衆議院予算委員会で，警察情報の処理に関して片山大臣は「実際の運用に当たっては各都道府県議会で慎重なご検討，ご審議を要する」と条件をつけながらも，警察行政に住基ネット番号を使うことは「法律上は可能」と述べた．

各県が条例を作れば，住基ネットは個々人の警察情報をも取り込めることになる．犯罪歴，交通事故などの情報も番号一つで見ることが出来る状況になることを示唆している．

住基ネットの使用範囲拡大についての総務省の働きかけとして，１月２１日の自治行政局市町村課長の事務連絡がある．

各都道府県下の市区町村の住基ネット担当課長，財政担当課長，情報政策担当課長に宛てた「事務連絡」は丁重な表現ながら，地方自治体にもっと積極的に住基ネットを使用せよとハッパをかける内容だ．

具体的には８月２５日に発行予定の電子カードについて，経費を計上し，手数料条例を制定し，カードの「有効利用の検討」を「積極的に行う」よう指示し，カードの利用は「公共的団体に限定されません」との表現で，民間にも広く利用させよとするものだ．

例として１５項目が並んでいるが，当初から強調されていた住民票交付を遙かに越えて，図書館，健康保険，介護保険，病院，商店街，交通機関，公共料金などにも使用を広げよという．

長野県下の自治体からは，審議会の現地調査に対して「際限ない使用拡大が不安である」との，複数の強い懸念が表明された．住民からも自治体に対して，住基ネットの利用範囲が拡大されることへの懸念が寄せられている．

住基カードの発行について県下の自治体は「独自利用計画はない」「活用アイデアなし」「現時点では有効性に疑問」「ご老人がカードを持つことは危ない」「広報に説明するとき，何のメリットがあると言って良いのか分からない」「カードを使って役所に寄らずに転出した場合，水道料，保険の手続きを考えると，町の対応の手間はかえって増えるかもしれない」など，消極的である．

住基カードの発行費用は１枚あたり１５００円から２０００円と見込んでいる自治体が多いが，総務省はこれを一律５００円にするよう求めており，差額は特別交付税で埋めるとも言われている．

だが，メリットのないカードを何故発行するのか，差額を特別交付税で賄うことは正しい税金の使い方なのか．住民の税金をこんなことに使って良いのか．他に予算措置が必要な事案はないのか．

住基ネットは自治事務であるからこそ，自治体自身がこうした点について考えなければならない．そして考えた場合の答えはあまりにも明らかである．

住基ネットの問題点は，住基ネットを管理する現場に近づけば近づくほどよく見えてくる．小さな自治体では対処出来ない財政負担，法的責任の重さであるからこそ，県が責任をもって束ねて対応してほしいというのが本音である．審議会はこうした一連の自治体の要望を重視する．

県下の１２０自治体中，２７自治体がインターネットに接続していたというセキュリティの粗雑さと，コストをかけてもかけても万全の対策にはなりにくいという事情もまた，審議会は重く見る．住基ネットは財政的に地方自治体の重荷になり，個人情報の漏洩の危険を永遠に突きつけ続けるものである．

加えて，民主主義の根幹である説明責任を政府が果たしてこなかったことも，審議会は重視する．地方自治体の住基ネットに対する疑問や戸惑いを無視して傍若無人にその使用範囲を広げようとする総務省の姿勢には，強く異を唱えるものだ．

民主主義，個人情報の保護，個人の自立，地方分権と地方の自立．２１世紀の日本に最も必要なこれらの価値観に悉く背く住基ネットに留まることは，責任ある首長にとっては如何なる合理的かつ正当な理由もない．

従って審議会は，県下の自治体及び県民の個人情報を守り，民主主義を守り，自治体の財政負担を減じるためにも，長野県知事が県下の市町村とともに離脱の決断を下すの

が，最も理にかなった方策であると結論づけるものである．

２．住基ネットの現状と市町村 LAN 環境について　（担当：佐藤委員）

２．１　住基ネットに関する市町村アンケート調査（添付資料１）

第 1 次稼動した住基ネットに関して各市町村担当者や首長がどう感じているかについて，平成 14 年 12 月 25 日から平成 15 年 1 月 23 日にかけて，県下 120 市町村を対象に書面でのアンケート調査を実施し，112 市町村から回答を得た．主な集計結果は以下の通りである．

- 住民にとって有意義であると想定される活用，市町村事務において有意義であると想定される活用ともに，「国等の行政機関に対する本人確認情報の提供」が最も多く，「住民票の広域交付」や「住基カード活用」は期待されていない．
- 本人確認情報の安全性を脅かす要因は，国等の行政機関に対する本人確認情報の提供」と「住基カード活用」．
- 住基ネットの仕組みに関して首長はほとんど理解しておらず，担当職員任せになっており，職員は，「自治体の負担が大きい割に自治体や住民のメリットが少なく，情報漏洩やセキュリティ面での不安」を感じている．
- 住基ネットシステム構築は仕様書作成から構築まで「委託業者」の全面的な支援に頼っている．
- 自治事務とはいえ国からの押し付けの感が強く，自治体に裁量の余地が少なく，実質的には法定受託事務に近い．しかしコストは自治体負担である．
- 住基カード発行計画は半数が未定であり，計画ありと回答した市町村でも，60%が人口比 2%以下，80%が 6%以下と極めて少ない．
- 住基担当者は十分なコンピュータ知識のないまま他業務との兼務の中で，膨大なマニュアルを理解することもできず，非常に不安である．

２．２　住基ネットに関する市町村調査（添付資料 2）

上記市町村アンケートで各市町村担当者の意見を書面で収集できたが，文書には表現しきれない生の声の収集と，実際の稼動実態把握，ネットワーク環境把握のために，審議会員委員が平成 15 年 2 月 14 日から 3 月 19 日にかけて，県下 11 市町村の現地調査を実施し，環境面，不安と感じている項目，住基ネットに関する意見，住基カードへの対応方針，県･審議会・LASDEC への要望等を聴き取り調査した．主な意見は以下のとおり．

①機器環境

- 庁内同一セグメント上にイントラネットと既存住基システムなどの基幹業務系ネットが同居している.
- インターネット環境と既存住基システムのオンライン環境が同居している.
- 操作者カードの保管方法に問題があり，担当者以外の方もカードを取り出せる.

② 不安と感じている項目

- マニュアルを全部理解できないほど複雑な事務処理になっている.
- 複数業務掛け持ちのところに更に住基ネットという大変重い責任が重なり，不安で夜も寝られない.

③ 住基ネットに関する意見

- 住民や市町村にとってのメリットが少なく，コストや事務処理増加のデメリットしかない．小さな村では財政的に苦しい.
- 本音を言えば止めたいが国や県に逆らうのは得策でなく，市町村単独での離脱は困難である.
- ネットワークの安全対策を施してから運用開始すべきであり，自治事務であるならば各市町村で責任を持てる体制整備をしてから全国ネットに参加すべし.
- 将来の電子政府・電子自治体の必要性，IT 化方針は理解できるが，その実現のためには，市町村の責任による市町村メリットを強調するのでなく，国の責任の下にどんな電子化が実現できるのかの説明を求む.

④ 住基カードへの対応方針

- 当面独自サービスの予定はない.
- 標準タイプⅡカードへ既存の地域 IC カード機能を取り込めるか, その開発費負担も心配.
- カード発行手数料への地方交付税補填がいつまで継続するか疑問.

⑤ 県･審議会・LASDEC への要望

- 戸籍事務協議会は戸籍事務に関する話題が多いので，県の担当者も出席した住基ネット，コンピュータ，ネットワーク，セキュリティに関する意見交換会や学習会を別途希望.

- 市町村別に離脱すると風当たりが強くて耐えられないので，県の段階でまとめて対応してもらいたい.

２．３　住基ネットに関する市町村 LAN 調査（添付資料３）

聴き取り調査の結果, インターネットに繋がっている庁内イントラネットと住民票オンライン等の業務系ネットが同居している事例が見つかり, 重大な問題だということから，2 月 28 日から 3 月 12 日にかけて急遽情報政策課主体で全市町村の LAN 環境を調査した．住基ネットや庁内 LAN の概要図提出を求め，120 市町村中 114 市町村から回答があった．それによると,

① 住基ネットが業務系庁内 LAN，事務系庁内 LAN，イントラネット系庁内 LAN 等の他ネットワークと接続しているのが 80 団体，接続していないのが 31 団体で，7 割が他ネットワークと接続している．

② 住基ネットがインターネット利用のある庁内 LAN と接続しているのが 27 団体, 接続していないのが 84 団体で，24%がインターネットと接続している．

そこで, 更にインターネットに接続している 27 団体に関して現地調査が必要との判断から，情報政策課と情報技術試験場にて逐次現地調査を実施しており，4 月 22 日までに８団体の調査を終えた.

その 8 団体の調査資料ならびにこれまでの 11 市町村への現地聴き取り調査結果から次節にて市町村ネットワークの接続形態とその危険性を考察する.

２．４　市町村ネットワークの接続形態とその危険性

市町村庁舎内ネットワークは，大きく以下の４つの LAN セグメントに分類できる.（資料４参照）

①住民票を管理する住民台帳システムや，戸籍管理システム，税務システム，財務システムなど, 行政事務そのものをオンライン処理するための**基幹系ネットワーク（既存住基システム）**

②行政事務を効率的に遂行するために庁内で発生するさまざまな情報を管理, 交換したり, 電子メールや庁内掲示板等のグループウエアを稼動する**情報系ネットワーク（庁内イントラネット）**

③行政情報を住民に知らせる公開サーバが稼動する, インターネットから直接的にアクセス可能な**公開系ネットワーク**

④全国の住基ネットに接続するための住基 CS サーバを収容する**住基ネットワーク**

各セグメントは概念的には独立しているが，データ共有・データ連携を図る必要があるため，現実的には各セグメント間を物理的に接続せざるを得ず，そのために間にファイアーウォール（F/W）やルータなどを介して一定のセキュリティを確保している．その接続形態は，これまでのネットワーク構築経過，コスト，運用方法の違いから県内各市町村ごとに異なり，容易な接続性と高い危険性を持つ形態から，運用性やコストを犠牲にして高い安全性を確保する形態まで，まちまちである．

少なくとも，県内市町村を調査した限りにおいては，「住基ネットワークはインターネットとは独立した閉じたネットワークであるから安全である」ということは断定できず，何らかの装置を介して住基ネットワークがインターネットに繋がっている事例が複数存在している．

市町村職員が住民基本台帳法や各自治体の個人情報保護条例を犯してまで不正アクセスする危険性も皆無とは言えないが，それ以上に，意識しない間に外部からの不正アクセスや自己増殖型不正アクセスプログラム（ワーム）により住基 CS サーバや住基ネットが不正侵入され，個人データ漏洩となる危険性の方が大きい．毎週のようにパソコンやサーバソフトの安全面での不具合であるセキュリティホールが報告され，全世界のパソコンやサーバがインターネットを介して接続していることを鑑みるに，個人情報を管理する既存住基サーバや住基 CS サーバをいかにしてインターネットの脅威から守るかが最重要課題である．

これまでも基幹系ネット，情報系ネット，公開系ネットが存在し，インターネット側からこれらのネットワークへ不正アクセスの危険性はあったが，仮に攻撃されたとしても自市町村内のサーバだけであり，被害が他の市町村まで及ぶことはなかった．が，基幹系ネットが全国に繋がる住基ネットに繋がったことにより，自らが被害者だけでは済まなくなり，住基ネットを通して外部に被害をもたらす加害者となってしまうことが，従来とは比べ物にならない高いセキュリティ対策を市町村ネットに要求しているのである．

２．４．１．　安全性の高いネットワーク接続形態

上記４セグメント間のデータ連携度と安全性を勘案すると，以下の接続形態が要求される．

① 既存住基サーバのある基幹系ネットワークは F/W を介して住基ネットワークと接続する．その F/W では既存住基サーバと住基 CS サーバ間のみの通路を確保する．

② 住基ネットワーク内には住基 CS サーバや IC カード発行端末, CS 端末を配置する.

③ CS 端末は住基ネットワーク内に配置するのがベストであるが, 庁内 LAN 配線上の都合により既存住基システムと同一の基幹系ネットワーク内に配置する場合には，両ネット間をつなぐ F/W に CS 端末用の通路を追加で開ける.

④ 庁内イントラネットと公開系ネットワークをインターネットに接続するには, インターネットとの境界に F/W を設置する.

⑤ 公開系サーバは非武装セグメント DMZ 内に配置し，インターネットからのアクセス先は DMZ 上の公開サーバだけに限定する.

⑥情報系や電子メール，グループウエアとして使う庁内イントラネットは，基幹系ネットとは物理的に分離する.

基幹系ネット上の既存住基端末，財務端末，業務端末あるいは住基 CS 端末がワーム等で不正アクセスされた場合には，F/W を介して住基ネットワークに侵入する危険性があるが，その危険性に関しては接続事例４，５，６で言及することとし，ここでは, 少なくともインターネットからのアクセスが基幹系ネットに及ばない接続形態を安全性の高いネットワーク接続形態とする.

２．４．２ 危険性のあるネットワーク接続事例その１

基幹系ネットと情報系の庁内イントラネット間が，F/W やルータ，VLAN 機能付スイッチなどで接続されているケース

情報系ネットと基幹系ネットは物理的に分離して, お互いの情報のやり取りやアクセスを禁止することが安全性面から言うとベストであるが, 基幹系ネット上のパソコンからインターネットや庁内イントラネットサーバ, 電子メールサーバにアクセスすることを許している.

両ネットワーク間のアクセス制御として F/W やルータ，VLAN 機能付スイッチが用いられているが，それらの設定が甘かったり，あるいは完全と思われても，所詮通信可能な通路があるので, インターネット側から庁内イントラネットに侵入したワームがそれらの通路を通って基幹系ネットのサーバに侵入できない保証はない.

なお，VLAN 機能付きのスイッチで両ネットワークを分離運用しているケースがあるが, 仮にそのスイッチが遠隔からの不正アクセスにより管理者権限が乗っ取られた場合には，そのスイッチは単なる中継装置になってしまい，以降，基幹系へのアクセスが容易になってしまう危険性がある.

２．４．３．　危険性のあるネットワーク接続事例その２

庁内 LAN に基幹系，情報系の区別がなく，どのパソコンからでも，ネットワーク的にみて, インターネットへのアクセスも住基サーバへのアクセスも出来てしまうケース

各サーバはスイッチング HUB にて接続されているが, 基幹業務系サーバと庁内イントラネットサーバが同じネットワークアドレスを有していることから, このスイッチング HUB では VLAN 機能を用いてない可能性があり，同じセグメントと同義であり，事例その１よりも危険な形態である.

インターネットとの間には VPN ルータと F/W が入っているが, このセグメント上のパソコンからインターネットにアクセスできるということは, 何らかの通路が開いていることになり, その通路を通してインターネット側からワームなどが侵入してくる危険性がある.

２．４．４．　危険性のあるネットワーク接続事例その３

基幹系ネットと情報系の庁内イントラネット間がレイヤ３スイッチで接続され, なおかつインターネットから F/W を介してそのスイッチに接続されているケース

インターネット側から F/W を経由してレイヤ３スイッチに到達し，そのスイッチで基幹系サーバにアクセスできてしまう.

F/W があるから安心というわけではないので，このケースではレイヤ３スイッチがどこまで強固な設定となっているかにかかってくる.

事例その１と同様, 仮にそのスイッチが遠隔からの不正アクセスにより管理者権限が乗っ取られた場合には，そのスイッチは単なる中継装置になってしまい，以降，基幹系へのアクセスが容易になってしまう危険性がある.

２．４．５．　危険性のあるネットワーク接続事例その４

公衆電話網で出先機関から基幹系ネットにダイアルアップしてくる場合で, 発信元を電話番号でチェックしないケース

全市町村のダイアルアップ環境を調査中であり, その結果を待たないと安全とは宣言できない.

ISDN 接続であれば発信者番号チェック機能を必須とし, 登録された電話番号からしか着信しないようにするとともに, 万が一アナログモデムによる接続があるとすれば早急に ISDN に変更する必要がある.

なお，出先機関は一般的に本庁に比べて人数的にも少数で，また事務所の管理やパソコンの管理も本庁と同程度になっていない可能性があり，仮に発信者番号チェックが正しく機能していたとしても，権限外や外部の操作者によるダイアルアップという危険性もある．通常，ダイアルアップルータはデータが流れて相手に伝送する必要が生じた時に自動的にダイアルアップするので，接続に当たり特別なパスワードは不要であるので，これらの接続ログを常に確認する運用が求められる．

２．４．６．　危険性のあるネットワーク接続事例その５

委託業者側からダイアルアップないしは専用線接続にて庁内 LAN に常時接続可能となるケース

障害発生時の迅速な対応，サーバ類の遠隔保守管理による経費節減などの理由から，委託事業者から基幹系ネットへの遠隔アクセスが可能となっている．ダイアルアップであれば発信者番号チェックをかけるか，コールバック方式により，相手を委託業者に限定する必要がある．更には，常時ダイアルアップ可能とはせずに，市町村が許可した場合のみ接続可能とする運用に改め，万が一ではあるが，委託業者からの不正アクセスを極力防止すべきである．

２．４．７．　危険性のあるネットワーク接続事例その６

住基ネットに繋がる基幹系ＨＵＢに空きポートがあり，持ち込んだノートパソコンをそこに接続可能なケース

最近は市町村でも一人 1 台のパソコン運用になり，個人のパソコンを職場に持ち込むケースは少なくなったようであるが，現地調査したある村では，個人のパソコンを自宅と職場で使っているケースがあった．自宅でインターネット接続した際に気づかないままウイルス感染したパソコンを職場の LAN に接続すると，ウイルスやワームを基幹系ネットのパソコンやサーバに感染させてしまう危険性がある．

基幹系ネットをインターネットとは完全に分離しておいたとしても，このように個人のパソコンを基幹系ネットに接続できてしまえば，タイミングによっては住基ネットサーバにワームが侵入する危険性があるのである．

２．４．８．　考察

ネットワークの安全性確保には 100%ということは有り得ない．どんなに F/W やルータでアクセス権限を制御してみても，その装置を通して許可したいサービスポートは開いているのである．そのポートを正々堂々と通過して内部の LAN に侵入できるので，問題は内部のパソコンやサーバのセキュリティレベルとなってくる．

そして，サーバやパソコンのソフトウエアが完全だとは誰も断言できない．マイクロソフト社のセキュリティパッチが完璧になくならない限り，その OS には未知のセキュリティホールが存在する可能性がある．もうこれ以上不具合はないですねと念を押しても無駄である．

さらには，システムや装置が完璧だとしてもそれを運用する人間に不注意や不正があれば不正アクセスを断ち切ることができない．住民基本台帳法や個人情報保護条例などの規定があっても，法律や条例は一定の行為を一般的に禁止するだけで，実際にだれもが従うかどうかはわからない．どこからでも不正侵入が可能で，しかも発覚しにくいとなれば，不正は起こりやすい．法律や条例の存在は不正アクセスを物理的に不可能にするわけではない．

上記の危険性のあるネットワーク接続事例は杞憂に終わるケースもあるが，可能性としては存在している．その危険性を承知した上で，リスク対リターンの判断をしなければならない．

コンピュータやネットワークといった IT 技術は確かに便利であり，それをうまく活用することにより我々の生活レベルや業務効率が向上することは確かである．ウイルスやワームの危険性を覚悟の上で我々はインターネットを使い込んできたわけである．リスク以上のリターンが得られているから利用しているわけである．

では，住基ネットはどうであろうか．これだけのコストと個人情報漏洩というリスクを冒してまで導入するからには，単に自分の住民票が全国で発行できる程度のリターンでは割に合わない．もっと有効な活用方法がないのであろうか．その活用方法に対する国民的なコンセンサスを得るまでは全国の全ての市町村で一斉に休止すればいい．

ネットワークの安全性を高めるために膨大な運用監視システム費用を追加投入するのがいいのか，このまま安易な手抜き運用を続けるのがいいのか，あるいは無駄なシステム運用を止めるのがいのか．判断材料は出揃ったのではないか．

３．住基ネットのセキュリティ確保について　－コストと効果－（担当：吉田委員）

県下の自治体を調査し知りえた事実に基づき, 住基ネットのセキュリティ確保について論じる.

３．１　脅威のヘッジとコストについて

ＩＴセキュリティを考えるに際しては, ネットワークに関わる人間を含めた全体的なリスク管理を考えることが重要になる．しかしながら長野県内の市町村を調査の結果, 多くの自治体担当者は, 自らの責任において管理しなければならない自治事務という認識がなく, 国からやれといわれたのでやっていると，ＩＴセキュリティを考えることにすら到達できていない状況である.

あらためて基本的な防御装置について定義を統一する.

Firewall

いわゆる関所．ビルに例えると警備員のいる**入退室警備**.

VPN

暗号のトンネルをネットワーク上に張ることでベストエフォートのネット上に自社の専用線を敷設したような利用方法を提供する技術.

IDS　（Intrusion Detection System:不正侵入検知システム）

NIDS（ネットワーク型 IDS）

サポートするＯＳを**限定しない**性質

ネットワークを流れるデータを全部見て，異常と認識できるものがあった時お知らせするシステム．廊下にある**監視カメラ**.

HIDS（ホスト型 IDS）

サポートするＯＳを**限定する**性質

最後の砦と呼ばれるホストへの侵入を検知するシステム．侵入されると困ってしまうホストに直接インストールし，異常な方法でのアクセスがあった場合にお知らせするシステム．**大量の金塊の周りを囲む赤外線**のようなもの.

上記のように定義した上で対策とコストを考えることにする.

論理的に 100%のセキュリティを施すには無限のコストが必要になる．クラッカーは強固なセキュリティシステムに侵入することに動機付けされる．ある程度のコストをかけるとセキュリティレベルは急激に向上するが，ある点からはあまり上がらなくなる．＜資料５のＰ４参照＞

システムに起因する脅威はある程度のコストでその可能性を低くすることができる．しかしソーシャルエンジニアリング，未知のセキュリティホール，人的ミス等々に起因する不正侵入の危険性を，かけるコストだけで回避することは不可能である．これが**どのようなセキュリティ装置を設置しても解決しないセキュリティレベルの限界**である．

この脅威のリスクヘッジを考えるとセキュリティ対策と責任の関係を明らかにしていく必要がある．

言葉の定義は様々であるが，ここでは以下のように定義する．この二つの考え方を統合してセキュリティ対策に盛り込んでいく必要がある．

■論理的な対策

強固なセキュリティ対策を「事前の策」と定義する．専門技術者によるファイアウォールや IDS（不正侵入検知システム）の導入，24 時間監視等に該当する．

この観点が必要不可欠であることは明らかである．しかしセキュリティに 100%というものは存在しない．この観点のセキュリティ対策は有事の可能性を低くすることのみに留まる．

■有事の対策

いくら強固なセキュリティシステムを構築していたとしても，それでも何かが起こることがある．「事前の策」以外にもう一つ大事な観点がある．それが「有事対策」である．「有事対策」とは有事の際の対応を予め考えておくことである．不正侵入があったときの対応フローを予め設定し，対応マニュアルによるオペレーションや高度な技術スタッフによる対応等が不可欠である．これにより被害の拡大を最小限に抑えることができる．

悲しいことにサイバーテロは永遠になくならない．残念ながら現状では，この危機管理の部分がたいへん曖昧になっている．

３．２　どのようにセキュリティ対策を考えれば良いのか

ＩＴセキュリティ対策の具体策では**事前の策**と**有事対策**の観点から自分自身で行うにはあまりにもハードルの高いセキュリティサービスを知り，どのようなものがありど

れを導入すれば良いのかを検討する必要がある.

これらを検討することによって有事の責任リスクを小さくすることが出来る.

例えば, 運送業社が運送業務中のドライバーにより事故を起こしたとき免許の有効期限を確認していなかったため無免許運転中の事故と確定した場合, 事業者責任から逃れることは出来ない. これと同じように, ネットワークを使って利便性を追求した分のリスクヘッジを世間に理解の得られる範囲で事前に対策を講じておくことが大変重要になる. これだけしていた, けれど事故が発生した. 保険で処理したい. これが常識である. 後から保険に入ることは出来ない.

自治体は民間企業以上の情報セキュリティレベルが必要なことはいうまでもない.

３．３　不正アクセスがもたらす損失を換算する.

ある 2 つの会社がインターネットからアタックを受け, それぞれ 10 万人の顧客リストを盗まれその 1 万人が団体訴訟を起こしたとする.

企業が 1 人に支払う損害賠償額は 1 万円から 10 万円と言われており, 全体で 1 億から 10 億の損失になる. そして, **その金額はどのようなセキュリティ対策をおこなっていたのかに依って決まる.** インターネットに繋がれた環境の中で, 情報資産の残余リスクを如何に減らしていたかが重要なポイントになる.

このケースでは 90 億円の効果をもたらすのがセキュリティ対策である. 対策への投資で直接のリターンはないが, 損失を防ぐ投資と利益を生む投資は同じものであるという認識を持つことが大切である. ＜資料５　Ｐ７参照＞

しかしＩＴセキュリティ対策を単純な費用対効果では語れない. といいながら, 対策を施した場合のリスクヘッジ効果は驚くべき効果がある.

３．４　実際の具体的な進入について

１）　対象ネットワークに対する情報収集（whois , nslookup , search engine 等）

２）　ネットワークに対するポートスキャン

３）　ファイヤウォールの検出

３）　ファイヤウォールのルールの推測

４）　DMZ 内のサーバに対する攻撃

buffer overflow , formatstrings attack 等による

５） DMZ 内のサーバに侵入，裏口の設置

６） web サーバ経由で，データベースに対して SQL インジェクション攻撃の実行による，不正な情報の搾取，書き換え

７） 侵入したサーバ経由で社内 LAN に対して情報収集，攻撃，侵入

８） 社内 LAN 経由で，企業間接続している他社ネットワークに対する情報収集攻撃，侵入，裏口の設置

攻撃手法の実際のパターンはこれ以上である．これらはすべて無償のプログラムで実行可能であり，有名なサーチエンジンですべて入手できる．

＜資料５　Ｐ９参照＞

３．５　とりあえず安全な環境を構築するための最低限の具体的費用

１）セキュリティ監査（オーディット）

標準オーディット実施

簡易オーディット実施

２）運用，管理コンサルティング

既存ネットワークに対するセキュリティレベルを含むコンサルティング

新規ネットワークデザインの相談

その他

３）緊急レスポンス

攻撃を受けた際にスポットで緊急の相談

第一報を受信後，電話にてファーストエイドの相談

アウトソースを行うことも価値は有る．しかし，安心度合いが高いものは金額も高くなるのは必然である．ちなみに，ＬＡＣ社のシニアアナライザーは１人月３５０万円となっている．

＜資料５　Ｐ１４参照＞

なかでも不正侵入検知ＩＤＳは優れた装置であるが，十分な設定・調整を行って初めて，有用となる．さらに既存のファイアーウォールとの相関分析を行わうことがより重

要である．その相関分析についてのコスト面を考えてみる．

False Positive

IDS は攻撃の可能性があると判断したとき, たとえ本当に攻撃があった場合ではなくてもアラートを発する. この様に実際には攻撃ではない行為を過剰に検出することを false positive という．⇒**切り分けが必要**

NIDS が発する警告のうち，本当に問題なことがらは約５%以下と言われている．このため，先ほどの相関分析が大変重要となる．

＜資料５　Ｐ１６参照＞

ＬＡＳＤＥＣは定期診断を行いＩＤＳも設置しているので安全であるといっているが定期診断の内容を公表していない. これでは客観的な第三者による監査が行えない状態で安全とはいえない. さらにどの程度の相関分析がなされているのかさえ定かではない．どの程度の設定・調整が施されているのかも重要である．

＜資料５　Ｐ１７以降参照＞

３．６　結　論

１．いかなる手法を用いても**万全な状態を確保することは不可能**である．

２. 安全性を高めるためにはリスクとする目的単位に**リスクをコンポーネット化**する．

３．コンポーネント化したリスクに**対するセキュリティポリシー**を作成する．

４．セキュリティポリシーに**マッチした運用**をおこなう．

５．運用の状況を管理する**管理監視体制を整備**する．

６．管理監視体制は**客観的な第３者**とし, 県は審議会等によりその第３者を監査できる．

７．問題発生時に最大限の**運用維持とリスクの最小化**を行うべく

対応フォーメーションをポリシーとは別に**アクションルールを確立**する．

８．上記項目を**永遠に維持**する．

上記セキュリティ対処にかかる経費を業界標準価格を元に算出すると**初年度で必要な投資は最低２２億円に上る．**ここにはコンサルティングや相談費用はなく HIDS と

CS サーバーの OS 入れ替え検討費用は含まれていない. **総額コスト（24 時間 365 日監視付）５年間の累計はおよそ８０億円強と計算できる.**

＜資料５　Ｐ２５以降参照＞

　このように費用対効果という観点では語れない費用を予算化さえできない自治体はどのように対処すればよいのか自ずと見えてきている. 国の対応はあまりにも杜撰と言わざるを得ない.

４．住基ネットの法的問題について　（担当：清水委員）

４．１　住民基本台帳ネットワークシステムの仕組み

昨年８月５日に第一次稼動を開始した住民基本台帳ネットワークシステム（以下「住基ネット」という.）の運用に関する法的根拠は住民基本台帳法にある．言い方を換えれば，住基ネットは住民基本台帳管理業務の一部分という，法律上の位置づけになる.

住民基本台帳管理業務の主体は市町村であり（１条，３条，５条)，そのため市町村長は個人を単位とする住民票を世帯ごとに編成して, 住民基本台帳を作成しなければならない（６条１項)．住民票に記載すべき事項は７条に法定されており，住基ネットによる管理利用の対象となる「本人確認情報」（氏名，生年月日，性別，住所，住民票コード，変更履歴）（３０条の５第１項）は，住民票情報の一部（７条１号，２号，３号，７号，１３号，１４号）である．これまでの住民基本台帳法に規定がなく，住基ネットとの関連で新たに設けられることになったのが住民票コード（１１桁の番号)である（７条１３号).

住民票コードは，本人の意思とは無関係に，市町村長がひとりひとりの住民（日本国籍を有する者）に一方的に附番して, 本人に通知することになっている（３０条の２)．住基法が住民票コードの告知要求制限規定（３０条の４２）を設けていることなどからすると，住民票コードは秘密扱いのようであるが，全国の市町村では各家庭の事情を問わずに世帯単位で１枚の通知書で住民票コードを知らせており, そのことを総務省が何ら問題にしていないことからすると，かなりいい加減な秘密性である.

市町村長から都道府県知事に住民票コードを含む「本人確認情報」が通知される（３０条の５第１項)．そして都道府県から国の行政機関等へ「本人確認情報」を提供する（３０条の７第３項)．但し，都道府県から国の行政機関等へ提供事務は「指定情報処理機関」に委任することができ（３０条の１０第１項３号)，長野県を含むすべての都道府県が「指定情報処理機関」である財団法人地方自治情報センター（以下「地方自治情報センター」という。）に上記事務等を委任している.

昨年８月５日に始まった第一次稼動では，市町村で集めた「本人確認情報」は，独自のコンピュータネットワーク（住基ネット）によって都道府県に送られ，そこからさらに地方自治情報センターに送られ, 国の行政機関等は地方自治情報センターのコンピュータにアクセスすることによって特定の個人の「本人確認情報」を確認することができる.

今年８月２５日に始まる第二次稼動では, 全国どこの市町村からでも地方自治情報センターにアクセスして全国どこに住んでいる人の「本人確認情報」でも確認することが

できるようになる（３０条の１０第１項４号・５号・６号).

４．２　立法事実

一定の新たな法制度を設けようとするとき，それを必要とする社会的背景事情（立法事実）が必ず存在する．法律はその法律の実施主体となる者が守らなければならないと同時に，規制対象になった者が守らなければならないルールである．民主主義社会において国が「この法律はだれもが守るべきだ」と言えるためには，一定の新たな法制度を必要とする社会的背景事情が存在し，かつそのことをその法律の影響を受けることになる人々だれもが理解できるということでなければならない．そうであって初めてだれもが法律を守ることの意味を理解し，納得して法律を守るのである．

これに対して，一定の新たな法制度を必要とする社会的背景事情が存在しないのに，「ある」と強弁して強引に法律を作ってしまうと，その法律を執行する行政機関内部においても市民社会においても様々な歪みを生じることになる．

住基ネットの立法事実について見ると，片山虎之助総務大臣の説明によれば，住基ネットは，全国の地方自治体の希望でつくった全国の地方自治体が管理する仕組みであって，国が支配するというようなものではない．ここで重要なのは，住基ネットが全国の地方自治体の希望で作られたという事実である．この事実があるのであれば，全国の市町村がすべての管理責任と費用を負担する住基ネットという仕組みを作ることは立法事実としては特に問題はなく，住基ネットを作ることを前提とした問題点が検討されるべきことになる．

しかし，立法事実に関する片山総務大臣の説明が真実でないなら，立法事実が存在しないのであるから住基ネットの法制化そのものが間違いであったという大問題になる．この点に関して，片山総務大臣は，いつどこの市町村が住基ネットの制度化を望んだのか一切明らかにしない．

日本弁護士連合会が行った３回にわたる全国市町村アンケート調査（2001 年 11 月，2002 年 6 月，同年 9 月）でも，当審議会の長野県内の市町村アンケート調査（2003 年 1 月）でも，圧倒的多数の市町村が住基ネットに懐疑的ないし否定的な評価をしている．一部には積極的な回答をしている地方自治体もあるが，それでもせいぜい総務省や地方自治情報センターの意向に沿うよう努力しているという内容のものであり，住基ネットが法制化される以前に住基ネットを明確にイメージして，総務省に積極的に提案していたというものではない．全国の地方自治体が国に対して住基ネットの法制化を求めた形跡はない．国民に至っては，昨年８月５日の第一次稼動の直前になるまで住基ネットのことを知らなかったという人が大半である．住基ネットの法制化に向けての立法事実はない．このことはもはや紛れもない事実である．

国主導により法制化された住基ネットを，全国市町村の希望により法制化されたものだと，立法事実をねじ曲げて法律の条文を構成することは，制度の運用全体に深刻な歪みを生じることになる．

４．３　法的責任

（１）　市町村の責任

住民基本台帳事務は「自治事務」（地方自治法２条８項）である．住基ネット事務は住民基本台帳管理事務の一内容として規定されているものであるから，市町村の自治事務である．

従って，住基ネットの関連法令の解釈運用，住基ネットの管理運用は市町村の責任において行うべきことになるとともに，管理運用費用も市町村の負担となる．国や都道府県の仕事を肩代わりするわけではないから，国や都道府県から補助金が出ることはない．総務省では，市町村の経費は地方交付税で賄うという説明をしているが，地方交付税は同法１条の規定（「地方自治の本旨の実現に資するとともに，地方公共団体の独立性を強化することを目的とする．」）から明らかなように，本来，地方自治体が自らの判断において使途を自由に決めることができるものであり，国が特定の使途を指定することは法の趣旨に反する．

市町村は，住基ネットの管理運用上のミスによりだれか（当該市町村内の住民に限らない）に損害を与えた場合には，国家賠償法に基づく責任を負わなければならない．意図的な不正操作の場合だけでなく，自らの管理運用ミスによって広範な被害を生じた場合にも，全責任を負わなければならない可能性を覚悟する必要がある．

（２）　国の立場

国の行政機関等は，「本人確認情報」の提供を受ける立場であり，住基ネットの管理責任の主体ではない．取得後の管理利用については責任があるが，市町村の住基ネットの管理については責任を負わない．

自治事務に関して国が市町村に対してできることは，地方自治法によれば，是正の要求（２４５条の５）だけであり，是正の指示（２４５条の７）や代執行等（２４５条の８）はできない．そして，国は市町村が是正要求に従わなかったことを理由に不利益な取扱いをしてはいけないことになっている（同法２４７条３項）．

国の指示には法的拘束力がなく，地方自治体の自主的な判断が尊重されることになるが，それは地方自治体の責任が重いということを意味する．例えば，ある対策を取らなかったことで住民に被害を与えた場合に，「国から住基ネットの管理運用に関する具体的な指示等がなかったから対策を取らなかった」という弁解をしたとしても，自治事務

である住基ネットにおいては絶対的な免責理由になるわけではなく，市町村が責任を問われる場面は出てくる．各市町村は自分の判断で必要な対応をしなければならない．

（３）　都道府県の立場

市町村との関係では，都道府県も国と同様の立場にある．都道府県は市町村に対して是正の勧告（同法２４５条の６）ができるが，是正の指示や代執行等はできないし，勧告に従わなかったことを理由に不利益な取扱いをすることはできない．その反面，問題が発生した場合には，（２）と同じく，「都道府県から住基ネットの管理運用に関する具体的な指示等がなかったから対策を取らなかった」と弁解しても通用しない．

国と都道府県の関係は，国・都道府県と市町村の関係と同様である．

しかし，都道府県は住基ネットの管理主体でもあるから，市町村の責任とは別に，都道府県独自の管理責任がある．地方自治情報センターに対する監督命令権限（３０条の２２）や，同センターへの報告要求・立入り検査権限（３０条の２３），本人確認情報の安全確保義務（３０条の２９）などのほか，当該都道府県内の市町村相互間の連絡調整や必要な協力もすべきものとされている（３０条の７第９項・１０項）．市町村に対する法的な命令権限はないが，都道府県が市町村のために働くべきことが制度上予定されている．

（４）地方自治情報センターの立場

地方自治情報センターは，都道府県の住基ネット事務の一部（３０条の１０）の処理を肩代わりできる機関として国から指定され（３０条の１２），都道府県との委任契約に基づいて住基ネット事務の一部の処理を行うものである．市町村とは直接の法律関係はない．

地方自治情報センターから都道府県を経由して市町村に送られる住基ネット管理のマニュアルは，地方自治情報センターの都道府県知事に対する「必要な協力」（３０条の１１第８項）の一内容であって，市町村と地方自治情報センターとの直接の法律関係ないし契約関係に基づくものではない．

上記マニュアルは市町村において守るべき基準とされているが，文字通りマニュアルであって法律ではないから，市町村に対する法的拘束力はない．マニュアルに従わなくても直ちに違法ということにはならないが，逆にマニュアルに従ってさえいれば問題が起こっても免責されるという関係にもならない．

また，地方自治情報センターに問い合わせて得た回答どおりに実行したとしても必ず免責されるわけではない．例えば，住基ネットを管理する独立の部屋を用意できない地方自治体では，衝立を立てるのでもよいという回答がなされているが，この回答どおり

に対応したために問題が起こった場合，当該自治体は免責されない可能性が大きい．

（５）　小括

前段の立法事実の不存在と併せてみるならば，市町村は自ら制度化を望んでいない住基ネットの管理運用について最も重い責任を負わされるという歪みを生じている．

４．４　法律とその限界

立法事実がない上に多くの問題をかかえている住基ネットに多くの市町村が不満を抱くのは当然である．にもかかわらず，ほとんどの市町村が住基ネットから離脱していない．その理由は，「法律があるから」「総務省から離脱してはいけないと言われているので」などである．後者は，「上司に言われたから」という程度のもので，自ら法的な検討をしている者の態度ではない．前者は，法律の存在を理由に挙げており，検討する必要がある．

（１）　「法律は守らなければならない」

一般論として，「法律は守らなければならない」ということが言われる．一般的に法律を守っても守らなくても構わないものだとしてしまうと，社会秩序を維持できなくなるから，「法律を守れ」という考え方は妥当である．

しかし，すべての法律が厳格に守らなければならないものとして法的に位置づけられているわけではなく，個人と個人の間の契約などでは法律の規定よりも当事者の合意（特約）が優先することが珍しくない．主に行政機関の仕事の範囲や内容を定める行政法規の場合は，行政機関に恣意的な運用をさせないために一律の運用を義務づけるというのが原則である．住民基本台帳法は行政法規の一種である．行政法規一般の考え方からすれば，全国の市町村は住基ネットに参加し接続しなければならない．

（２）　行政法規は厳格に守られているか

しかし，行政法規の実情を見ると，行政法規は行政機関において必ずしも守られていない．「守らなければならない」ということと，「守られている」ということとは違うのである．行政法規であっても，意識的に守られていないこともあれば，意識されずに守られていないこともある．

例えば，最近国会で取り上げられた，自衛官募集に関する住民情報の提供は住基法，自衛隊法・同施行令の解釈としては無理があり，違法である．住基法は，氏名・生年月日・性別・住所の４情報の「写し」の「閲覧」（１１条１項）と，住民票情報の一部の事項の「写し」の「交付」（１２条２項ないし４項）を規定しているだけであり，自衛隊法施行令１２０条は「内閣総理大臣」の「資料の提出」権限を規定しているものの，

条文の規定の仕方からして，個人情報収集の根拠規定にはなり得ない．このような解釈は常識的な法解釈能力がある者であれば，だれもがすることであって，政府は国会答弁で「適法である」と強弁し続けたことは異常としか言いようがない．ここでは法は守らなければならないものではなく，自らの行為を正当化するための“口実”になりさえすればよいものになってしまっている．

地方自治法違反は全国の地方自治体で恒常的に行われている．例えば，地方議会の議長の任期は４年と法定されている（１０３条２項）が，これを守っている議会はほとんどない．１年交替にしている議会が多い．議員の監査委員としての任期も４年（１９７条）だが，守っている地方自治体はほとんどない．

また，首長・議長などの交際費や，食糧費，出張旅費，海外視察などに関する違法支出は全国的に行われてきたし，現在でも一掃されたわけではない．２００１年４月から地方自治法上の根拠を持つようになった政務調査費（１００条１３項）も「政務調査」の名にはほど遠い飲食などに費消されているものが少なくない．

このように，国においても地方自治体においても法律は必ずしも厳格に守られているわけではない．

（３）　「法律は不可能を要求しない」

正されるべき違法は正されなければならないが，そもそも守ることを期待することが難しい法律はなるべく作らないことである．そのようにしないと，法律を執行する現場において多大なコストや労力を要する反面，執行される側からすると法律を守らされることが心理的な負担ないし苦痛になり，「法律は守るべきもの」という忠誠心が法律を執行する側からも執行される側からも失われる．表面的には法律は守られているように見えて，実はだれも守らないという二重構造が生まれるおそれがある．

行政法規の執行にもこのことは当てはまる．

当該行政事務を実際に行う現場担当者にできないことを無理矢理やらせようとすると，担当者は，できるようになるために相当ないし高度の努力を強いられ（続け）る．それでも能力的に「できない」ということはあり得る．「できない」ことはサボらざるを得ない．しかし，そのような状態はもちろん「違法」である．「違法」だと指摘されることを恐れて，「やっているふり」でごまかすことになる．

難しいことを要求すればするほど，要求する対象者の範囲を広げれば広げるほど，法律は守られなくなる．法律が守られるためには，法律を守ることを要求する対象者に「できない」ことを要求しないことである．法律は不可能を要求してはいけないのである．

４．５　住基法と住基ネット

旧来の住民基本台帳の管理は全国の市町村が責任を負える内容だった．したがって，特に制度的欠陥とも言うべき重大な問題が生じることはなく，運用されてきた．

しかし，住基ネットは，全国の市町村の意向をほとんど無視する形で進められてきた．その上，コンピュータの専門知識と管理能力と財政負担能力が必要不可欠であるにもかかわらず，多くの市町村においてこの点の手当が極めて不十分である．住基ネットの管理運用は，コンピュータを専門職としていない現在の自治体職員には能力的に無理がある．また，多くの地方自治体では，その組織内で最も住基ネットに詳しい者が住基ネットの管理運用に関して決定権限を持つ仕組みになっておらず，従来のピラミッド型人事の中に組み込まれたままになっている．補助金制度が廃止の方向に進む中，膨大な赤字をかかえた市町村が確実に高額化する住基ネットの管理費用を支払い続けることなどできない．莫大な損害賠償請求に応じなければならない場合どうするかなどの財政面の問題についてもほとんど検討されていない．

住基ネットの実情は，法律が市町村に不可能を要求していると言わざるを得ない．

４．６　法律が不可能を要求している場合の対応

そのような法律は守らくてよい，というのもひとつの考え方ではある．しかし，「法律は守らなければならない」という考え方に沿って合理的な解釈が導けるのであれば，極力，合理的な解釈の方向性を検討すべきである．

住基ネットはコンピュータネットワークという“生き物”である．この“生き物”を絶対確実に管理することはだれにもできない．ましてや，管理能力に著しい高低差のある 3,200 余の市町村が全体として高度の管理状態を維持することは不可能である．

市町村長と都道府県知事には，そのような実情にある住基ネットの「適切な管理」のために「必要な措置」を講じる法的義務がある（住基法３６条の２第１項，３０条の２９第１項）．「適切な管理」は住基ネット特有の要請である以前からの住基法の要請であり，住基法の根幹である（１条参照）．適切な管理のために最もよい方法として市町村長，都道府県知事が考えた合理的な対応が「必要な措置」である．

問題が解決するまで一時的に住基ネットから離脱するという対応は，自分の自治体の住民の情報を外部から守るために有効であるだけでなく，自分の自治体の管理が原因となって他の自治体ないし住民に被害を与えないためにも有効である．昨年８月５日，全国で２００以上の自治体が総務省ないし地方自治情報センターの指示で住基ネットとの接続を停止したことがあるが，これも一種の一時的な離脱であって，法律的には，住基法３６条の２に基づいて市町村長の判断として行われたものである．

住基ネットから離脱する場合，どれくらいの期間が「必要な措置」と言えるかが問題になるが，それは離脱を実行した市町村長が住基ネットの何を問題視したかによる．自分の自治体の住基ネットが庁内ＬＡＮと接続していたことを問題視するのであれば，庁内ＬＡＮとの接続を止めた時点で住基ネットに再接続することになる．個人情報保護法案が成立していないことのみを問題視していたのであれば，同法案の成立によって接続することになる．住基ネット全体の危険性を問題視しているのであれば，その危険がすべて除去されるまで接続しないということになる．

このようなことを法解釈論として認めるとなると，各自治体の問題意識によって対応がバラバラになってしまうが，これは住基ネットを市町村の自治事務として法的に位置づけ，全国の市町村を住基ネットの管理責任者としたことによるであって，やむを得ないことである．全国で最も危機意識の低い首長の判断に全国の市町村長の判断を揃えなければならないとすることの方が遙かに非現実的であるし，実際にそのような基準で運用されるなら，全国各地でトラブルが発生し，多くの市町村で訴訟が発生することになるであろう．

したがって，市町村長，都道府県知事の「適切な管理」のための「必要な措置」の内容は，それぞれの判断に委ねるほかない．

４．７　「必要な措置」の内容

「必要な措置」の内容については法律的に特に限定があるわけではない．文字通り，住基ネットの実際の運用において必要な措置であり，各市町村長，各都道府県知事の住基ネットの問題点の理解内容に対応する．本審議会は，以下の内容が現時点における県が取るべき「必要な措置」だと考える．

住基ネットは立法事実を欠いおり，市町村が過重な責任を負わされる仕組みになっており，いつ重大なトラブルが起こってもおかしくない．このことをよく理解している市町村の住基ネット担当者は少なくない．しかるに，長野県内の市町村アンケート調査によれば，住基ネットの担当者の問題意識が首長に共有されていない市町村がかなりの数を占めている．聴き取り調査によれば，「実は共有されていない」と説明した自治体もある．これは一つの自治体組織内においてさえ住基ネットの問題が理解されていないということである．県は，県内市町村の首長及び住基ネット担当者と住基ネットの実情について十分な情報提供と意見交換を行い，市町村が自らにとって最善の対策が取れるよう協力すべきである．

また，市町村が最善の対策を取れるようにするためには，住民が住基ネットの問題を理解することが必要不可欠であるので，県として県民に対して十分な情報を提供し，県民の意見を聞くための場を設けるべきである．

しかし, 市町村との意見交換や県民との対話の場を設けるだけでは問題は解決しない. 県は, 市町村が独自の判断として住基ネットから離脱しようとするときには, これに全面的に協力すべきである. 従来, 県は国と市町村の間にあって, 国の指示を市町村に「下ろす」仕事をしてきた面が強く, そのために市町村は県に対して本音を語らないという関係ができあがってしまったが, 地方分権の時代のいま, 県は国のため以上に, 市町村と県民のために仕事をすべきである. 市町村が切実に住基ネットからの離脱を望んでいるのであれば, 県は全面的にこれを支援すべきである.

県内の市町村の住基ネットの管理状況にかなり深刻な問題があり, かつそのことを指摘しても対処できない状態が続いているという現実を踏まえるならば, 県は, 県内市町村の独自の判断とは別に, 県内市町村と県民のために住基ネットからの離脱すべきである. 県内市町村の問題の深刻な状況を知りながら, 各市町村のみに判断を委ねるのは, 県としての責任放棄である.

本審議会では独自の県内市町村調査を行うことによって, 県内市町村の住基ネットの管理の深刻な実情を知ったが, 他の都道府県では同様の調査は行われていない. 本審議会では, 他の都道府県でも同様な, 場合によってはより深刻な事態が発生しているに違いないと推測している. 住基ネット問題がひとつの県だけで解決できるものでないことからすれば, 県は, 他の都道府県に長野県内の住基ネットの運用の実情を説明して, 長野県と同種の手法により各都道府県内の市町村における住基ネットの運用の実態を調査するよう勧め, 住基ネットの問題点について共通認識を持つようにすべきである. その上で, 他の都道府県とともに国に対して, 住民基本台帳法の改正による住基ネットの廃止を含めて, 今後の住基ネットの運用について根本的な見直しをするよう働きかけるべきである.

４．８　個人情報保護法案の成立との関係

個人情報保護法案の成立と住基ネットの接続との関係について若干説明しておく.

去る５月２３日, 個人情報保護関連５法案が成立した. この点をとらえて,「個人情報保護法案が成立した以上, 住基ネットからの離脱は違法だ」という指摘があり得ないではないので, 念のため一言, 説明しておく.

個人情報保護法制の充実は, ２０年以上も前から指摘されて来たことであり, 全国の多くの自治体が個人情報保護条例を制定して来ていることだけを見ても明らかなように, 住基ネットとは直接なんらの関係もない. 住基ネット法案を作成した立場からでさえ, 個人情報保護は住基ネット法案（住基法の一部）で十分だという説明がなされているほどである.

これに対して, 住基ネットから離脱している, あるいは個人選択制を採用している地

方自治体が指摘しているのは, 個人情報保護法制さえできていないのに住基ネットを稼動させるのは問題だということであり,「個人情報保護」という名称のついた法律が成立しさえすれば接続するという形式論を言っているのではない. 住基ネットがかかえている問題は, 別の項でも説明しているように,「個人情報保護」という名称のついた法律が成立するか否かなどではない.

住基ネットへの接続ないし全面的な接続は, 各市町村長, 各都道府県知事が危険だと考える問題が解決されているか否かにかかっているのである.

５．結論　－市町村への提言と県の役割－　（担当：不破委員）

本審議会は，長野県（以下「県」という.）における本人確認情報の保護について審議を行うものである．住民基本台帳ネットワークシステムの構造上，県のサーバーは県庁建物内及び県出張所等建物内だけで独立完結しておらず，県内すべての市町村に接続している．そのような関係から，県として県民の本人確認情報の保護を実効的に行うには，県の住基ネット管理の実情調査を行うだけでは不十分であり，県のサーバーと接続している県内の全市町村における住基ネット管理の実情を調査する必要があった．これまで行ってきた県内市町村アンケート調査や市町村現地調査などの結果については，本報告書ですでに述べた通りである．

上記調査の結果，現段階における長野県内の市町村の住基ネット管理の実情は，個人情報保護が十分になされる体制になっておらず，かつ，これを直ちに解決することが極めて困難であることが明らかとなった．

本審議会では今後も，更に詳細な調査を行う予定であるが，現段階における長野県内の市町村の住基ネット管理の実情の深刻さと緊急性に鑑みたとき，現時点で報告できる事項について報告することが本審議会の責務であるということを確認し，県が速やかに行うべき「必要な措置」として下記の結論を報告することにした．

(1)県は，県民の個人情報保護の観点から，当面，住基ネットから離脱すべきである．

(2)県は，市町村が独自の判断で緊急の「必要な措置」として住基ネットから離脱しようとする場合には，これに協力すべきである．

(3)県は，(1)の実行に先立って，県内市町村長及び各市町村の住基ネット担当職員と，本審議会で調査した県内の住基ネットの実情について意見交換の機会を設け，実情に関する理解を共通にする努力をすべきである．

(4)県は，(1)の実行に先立って，県民に対して本審議会で調査した県内の住基ネットの実情を知らせる機会を設け，県内の住基ネットの実情に関する理解を共通にするよう努力すべきである．

(5)県は，上記(1)乃至(4)と並行して，他の都道府県に対して，長野県内の住基ネットの運用の実情を説明して，住基ネットの問題点について共通理解を広め，他の都道府県とともに国に対して，住民基本台帳法の改正を含めて，今後の住基ネットの運用について根本的な見直しをするよう働きかけるべきである．