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

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

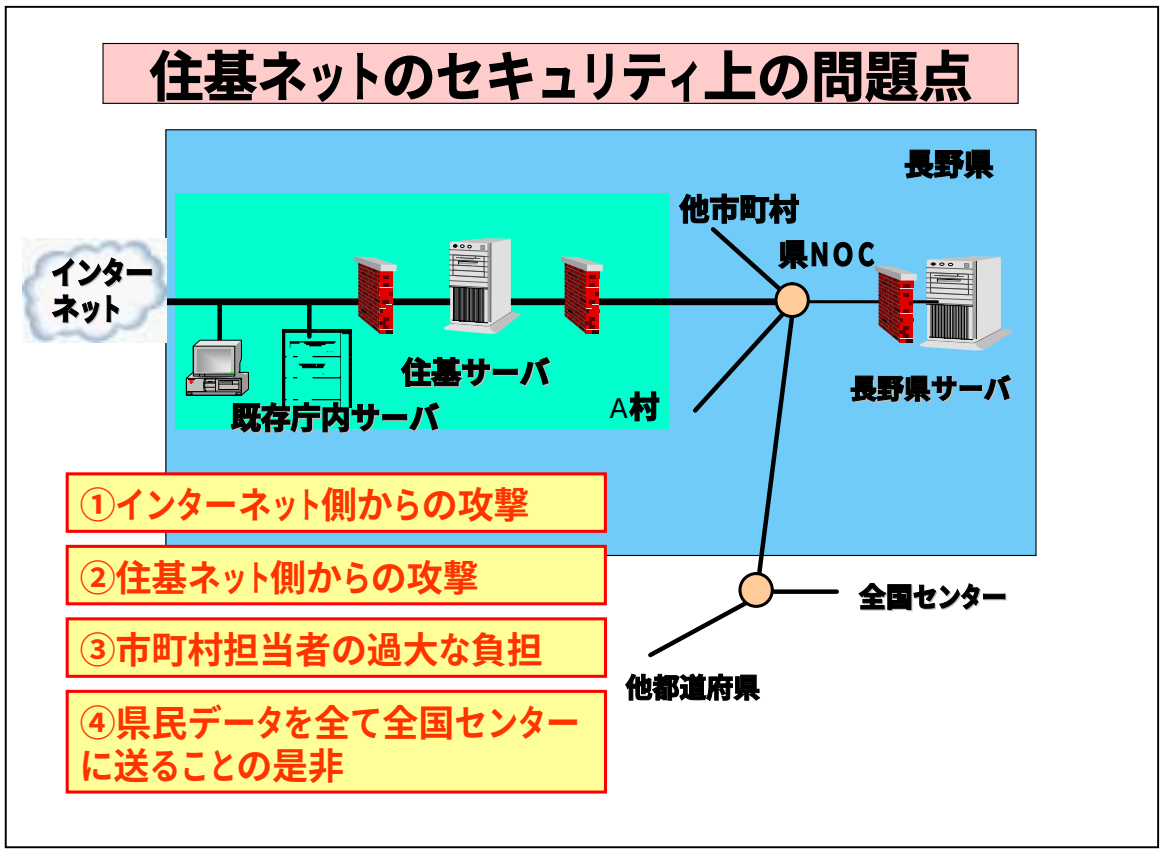
5月24日　電子自治体協議会セキュリティ対策ワーキンググループ会合（県庁：18団体参加）

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.

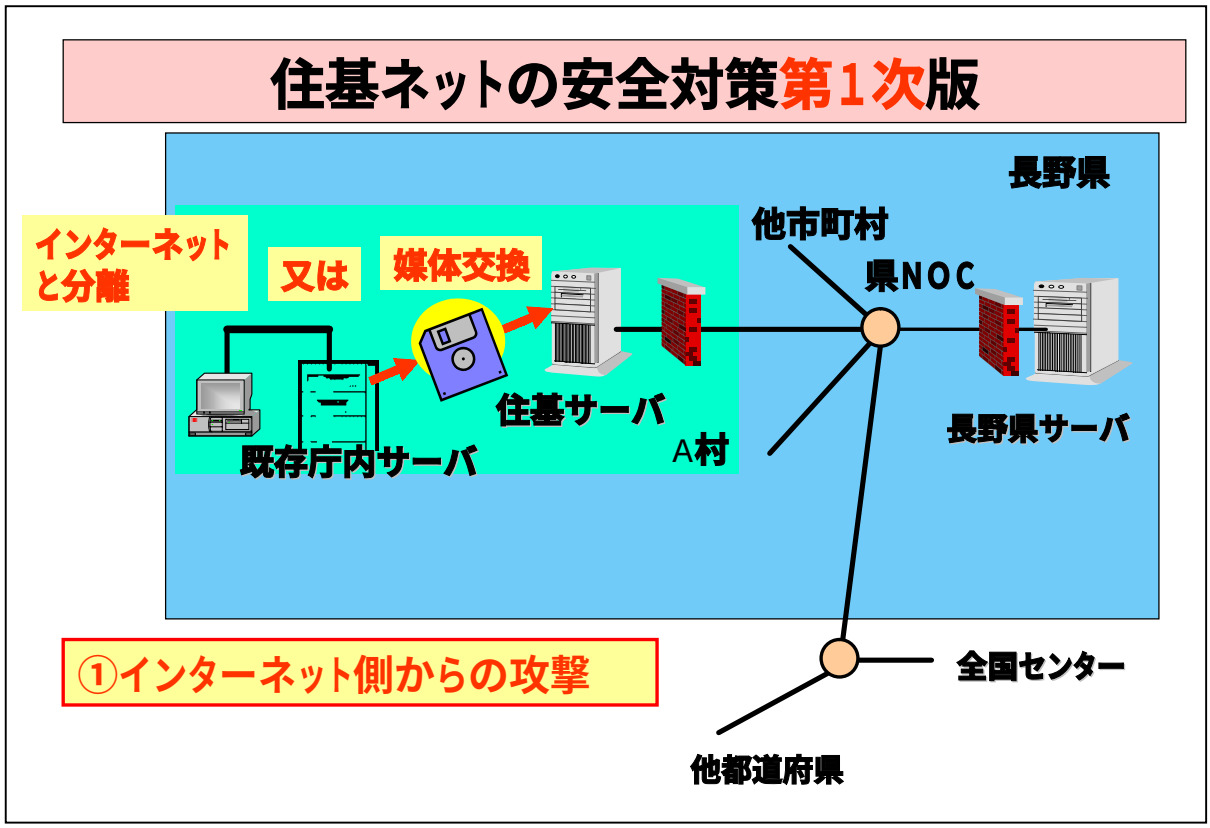
④地方自治情報センターにデータをすべて持っていくという体制が、本当に本人確認情報を守るという意味で正しい選択なのか.

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.

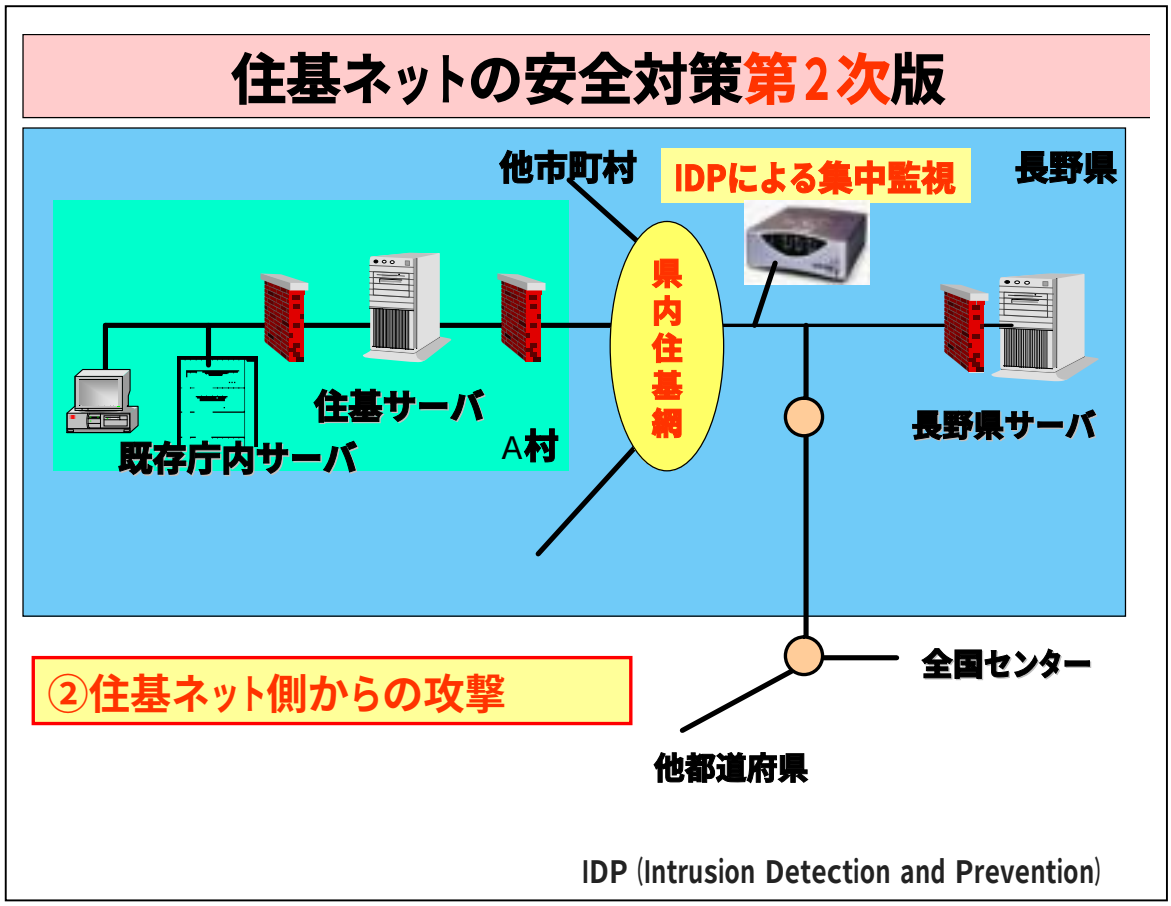
対策は，この4つの安全性の問題点を順次解決しようというものです．

(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）



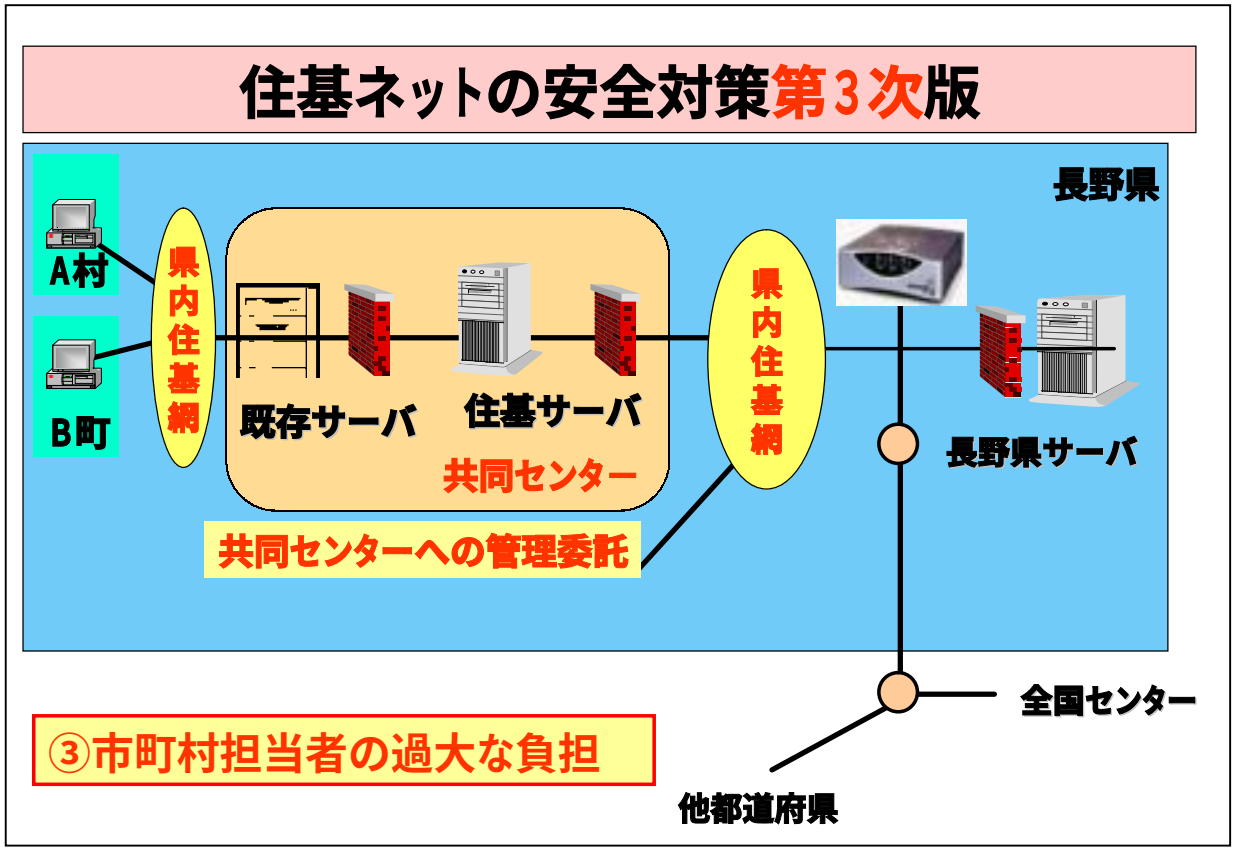
２００３年８月に全国でブラスタと呼ばれるウィルスが問題になったときに，長野市がこのことを懸念して用心のために一時的に住基ネットを切断しました．

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．

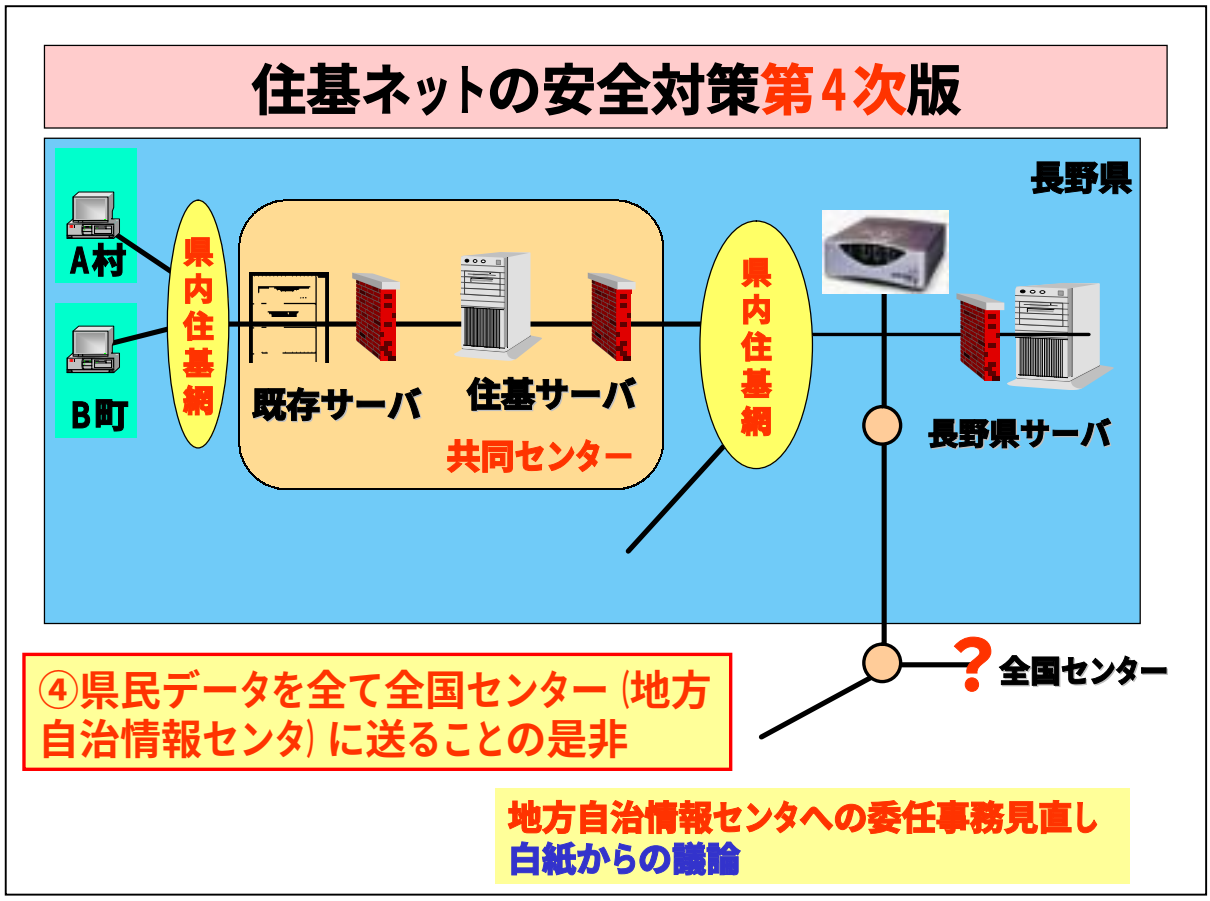
(3)各市町村の住基ネット担当者が過大な負担を負っている問題（安全策第3次版）



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.