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 に全面委託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.

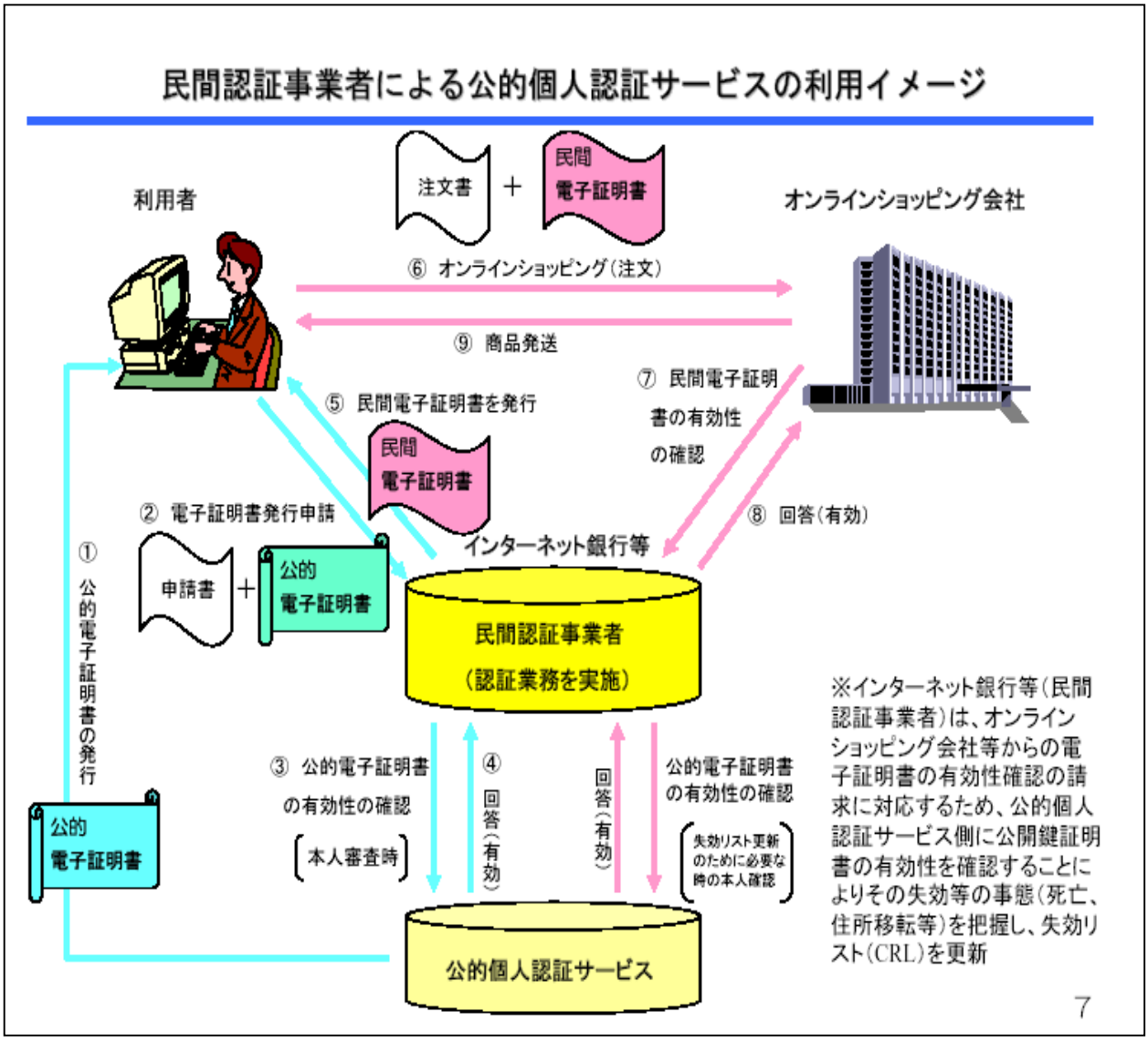
長野県では、パスポート発給申請時の住民票添付をなくして住基ネットで住所確認するシステムを県下各地方事務所に展開するにあたり、その安全性を慎重に検討している段階であるが、公的個人認証システムを利用して自宅からのパスポート発給申請サービスを開始した県もある. ただし、戸籍謄抄本は別途郵送、写真が本人かどうかを確認するためにも受領には本人が役所に出かける必要があり、県民にとってどれほどの住民サービス向上となるか疑問である. その結論は近いうちに利用者数実績が示してくれるはずである.

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．）



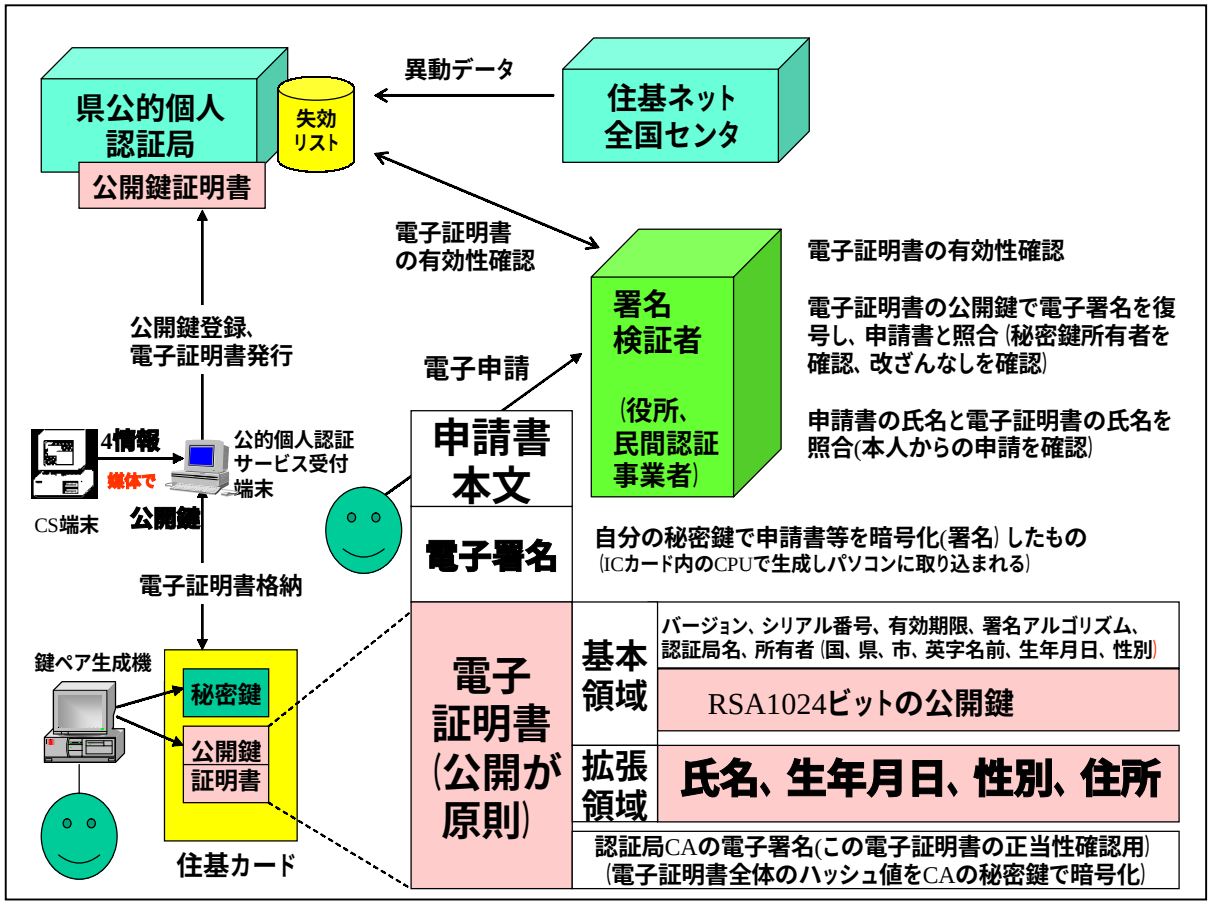
(総務省が公開している公的個人認証サービスの概要 PDF より)

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.