

住基ネットと一切関わらない公的個人認証サービスの提案

■ 公的個人認証サービスがはじまる

2003 年中にサービス開始と言われていたインターネット上の印鑑登録制度である「電子署名に係る地方公共団体の認証業務に関する法律（公的個人認証法）」に基づく公的個人認証サービスがいよいよ来年（2004 年）1 月にスタートするようです。

総務省サイト内にある「住民基本台帳ネットワークシステム」のページの「電子政府・電子自治体における住基ネットの役割」（http://www.soumu.go.jp/c-gyousei/daityo/juki_yakuwari.html）には、「申請・届出をインターネットで行うためには・・・確かな本人確認ができるセキュリティ確保の手段（電子署名と言います）が必要」であり、そのために「全国どこに住んでいる人に対しても安い費用で提供する制度として、公的個人認証サービスを創設」と書かれています。また、その後、次の記述があります。

住民基本台帳ネットワークシステムから公的個人認証サービスに対して、異動等失効情報（公的個人認証サービスを受けている住民が住所や氏名が変わったり、死亡の事実が生じた情報）を提供することにより、正確な本人確認を実現することが可能となります。

果たしてこれはどういう意味なのでしょう。本稿では、公的個人認証サービスが住民基本台帳ネットワーク（住基ネット）とどう関係するのか、住基ネットを使う必然性はあるのか、住基ネットと一切関わらない個人認証サービスはできないのかについて考えてみたいと思います。

■ 電子証明書と失効リスト

住民が行政機関への電子申請を行う際には、申請書にそれが正しく本人からのものであることを示すために電子署名とその電子署名が正しく本人のものであることを示す電子証明書を添付しなければなりません。

電子証明書の発行業務は既に民間企業（日本認証サービスなど）が行っていますが、今後、自治体にも電子証明書の発行をさせようというのが公的個人認証サービスです。

公的個人認証サービスによる電子証明書を必要とする住民は、まず市町村の窓口で「電子証明書発行申請書」を提出します。市町村は申請者が本人であることを運転免許証などで確認した上で都道府県に通知します。都道府県は通知に基づき電子証明書を発行し、市町村は、これを住民基本台帳カードなどの IC カードに格納し交付します。

住民が行政機関への電子申請を行う際には、パソコンにこの IC カードを挿入することによって、申請書に電子証明書を添付することが可能となります。

電子証明書は、氏名、生年月日、性別、住所の変更があった場合や住民票が削除された場合（死亡等）には効力を失います（公的個人認証法第 15 条）から、電子申請書を受けた行政機関は添付された電子証明書が有効なものであるかどうか電子証明書の発行元である都道府県に確認する必要があります。

行政機関からのこうした問い合わせに答えるため、都道府県はあらかじめ失効リストを作成しておき、これを提供することになっています。

電子署名に係る地方公共団体の認証業務に関する法律

（異動等失効情報の記録）

第 12 条 都道府県知事は、利用者について、住民基本台帳法第 30 条の 8 第 3 項に規定する通知があったときは、直ちに、当該通知に係る利用者に発行した電子証明書の発行の番号、当該通知があった旨及びこれらの事項をこの条の規定により記録する年月日（以下「異動等失効情報」という。）を、総務省令で定めるところにより、電磁的記録媒体に記録し、これを当該記録をした日から政令で定める期間保存しなければならない。

(電子証明書の失効)

第 15 条 電子証明書は、次の各号のいずれかに該当するときは、その効力を失う。

- 一 都道府県知事が第 11 条の規定により失効申請等情報を記録したとき。
- 二 都道府県知事が第 12 条の規定により異動等失効情報を記録したとき。
- 三 都道府県知事が第 13 条の規定により記録誤り等に係る情報を記録したとき。
- 四 都道府県知事が前条の規定により発行者署名符号の漏えい等に係る情報を記録したとき。
- 五 電子証明書の有効期間が満了したとき。

住民基本台帳法

(都道府県における本人確認情報等の利用)

第 30 条の 8

3 都道府県知事は、第 30 条の 5 第 1 項の規定により第 7 条第 1 号から第 3 号まで及び第 7 号に掲げる事項(同号に掲げる事項については、住所とする。)の全部又は一部について住民票の記載の修正(総務省令で定める軽微な修正を除く。)があつた旨の通知又は住民票が消除された旨の通知があつたときは、これらの通知があつた旨の情報を、電子署名に係る地方公共団体の認証業務に関する法律第 12 条に規定する事務に利用することができる。

では、都道府県はどのようにして失効リストを作るのでしょうか。実はそれを考える前に一つ知っておくべきことがあります。

都道府県の公的個人認証サービスにおける主な業務は、電子証明書の発行とその記録、失効リストの作成・保存・提供などですが、これらの業務を総務大臣の指定する「指定認証機関」に委託することができるのです(公的個人認証法第 34 条)。そして、この「指定認証機関」には総務省からの正式な発表はまだありませんが、同省の外郭団体である「財団法人 自治体衛星通信機構」が指定されるようです(注 1)。

電子署名に係る地方公共団体の認証業務に関する法律
(指定認証機関の指定等)

第 34 条 都道府県知事は、総務大臣の指定する者(以下「指

定認証機関」という。)に、次に掲げる認証業務の実施に関する事務(以下「認証事務」という。)を行わせることができる。

- 一 第 3 条第 5 項の規定による電子証明書の発行の申請書の内容及び利用者署名検証符号に係る通知の受理に係る電子計算機処理等並びに同条第 6 項の規定による電子証明書の発行に係る電子計算機処理等及び同項の規定による通知に係る電子計算機処理等
- 二 第 8 条の規定による発行記録の記録に係る電子計算機処理等及び発行記録の保存
- 三 第 9 条第 2 項において準用する第 3 条第 5 項の規定による電子証明書の失効の申請書の内容に係る通知の受理に係る電子計算機処理等及び第 9 条第 3 項の規定により送信される電子証明書の失効を求める旨の申請の受理に係る電子計算機処理等
- 四 第 10 条第 2 項において準用する第 3 条第 5 項の規定による利用者署名符号の漏えい等の届出書の内容に係る通知の受理に係る電子計算機処理等
- 五 第 11 条から第 14 条までの規定による失効情報の記録に係る電子計算機処理等及び失効情報の保存
- 六 第 15 条第 2 項の規定による通知及び同条第 3 項の規定による公表
- 七 第 16 条の規定による失効情報ファイルの作成及び保存
- 八 第 18 条第 1 項の規定による保存期間に係る失効情報の提供に係る電子計算機処理等及び同条第 2 項の規定による保存期間に係る失効情報ファイルの提供に係る電子計算機処理等
- 九 第 18 条第 3 項の規定による保存期間に係る失効情報及び保存期間に係る失効情報ファイルの提供の停止に係る電子計算機処理等
- 十 第 18 条第 4 項の規定による報告書の作成及び公表

(注 1) 財団法人自治体衛星通信機構は、同法人 Web サイト(<http://lascom.or.jp/www/outline/outline03.html>)によれば「全国の地方公共団体及び防災関係機関等において通信衛星を共同利用するための設備を設置し、運用することによって、防災情報及び行政情報の伝送を行うネットワークの整備促進を図る」ことを目的として、1990 年 2 月に設立されたそうです。

■ 電子証明書発行時の情報の流れ

以上を踏まえた上で、失効リストがどのようにして作成されるのか知っていただくのにたいへんわかりやすい図(図1)があります。この図は、長野県本人確認情報保護審議会第10回会合(<http://www.pref.nagano.jp/soumu/sichoson/jyukisys/singikai/dai10.htm>)で配付された情報政策課名の資料3「公的個人認証サービスの概要」の中に収められた参考2「電子証明書発行情報・異動等情報の流れ」です。図には細かい説明が書かれていませんので多少間違いがあるかも知れませんが、当通信の筆者である黒田の推定も含めて解説を試みてみます。

まず、上半分は電子証明書発行時の情報の流れです。市町村は申請者からの求めに応じ、窓口におかれた公的個人認証専用受付窓口端末を使って、都道府県から業務を委託された「指定認証機関」に電子証明書の発行を求めます。その際に電子署名に使う公開鍵とともに申請者の基本4情報(氏名、生年月日、性別、住所)を総合行政ネットワ

ーク(LGWAN)を使って送付する必要があります。基本4情報は住基ネットのCS端末からフロッピーディスクを使って公的個人認証専用受付窓口端末にコピーします。

「指定認証機関」は、送られてきた基本4情報をもとに電子証明書を発行するとともに、基本4情報と電子証明書のシリアル番号を「基本4情報とシリアル番号対応データベース」に記録します。と同時に、住基ネットの「指定情報処理機関」(財団法人 地方自治情報センター)に電子証明書発行者の基本4情報を送付します。

電子証明書発行者の基本4情報の送付を受けた「指定情報処理機関」は証明書発行データベースにこれらを記録します。

以上が電子証明書発行時の情報の流れです。次に下半分の異動等情報の通知時における情報の流れを見てみます。

■ 異動等情報の通知時の情報の流れ

市町村は電子証明書の発行を受けたものだけでなく全ての住民について、住民基本台帳法の規定に基づき、本人

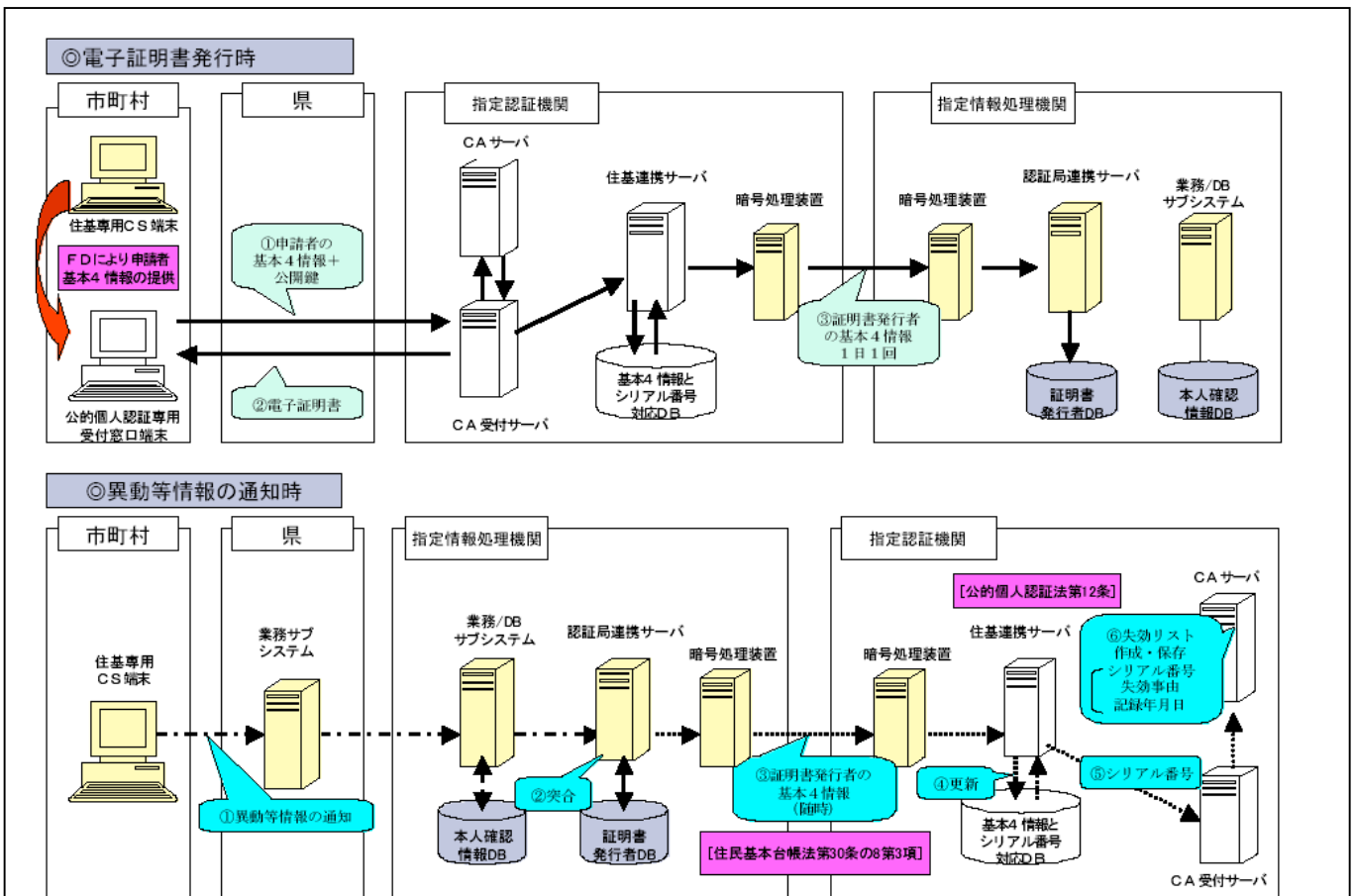


図1 電子証明書発行情報・異動等情報の流れ

長野県本人確認情報保護審議会第10回会合配付資料3「公的個人認証サービスの概要」より

確認情報（氏名、生年月日、性別、住所、住民票コードと、これらの変更情報）の異動があった場合、住基ネットを使ってこれを異動等情報として都道府県経由で住基ネットの「指定情報処理機関」に通知します。

「指定情報処理機関」は送られてきた異動等情報をもとに本人確認情報データベースを更新するとともに、送られてきた異動情報が電子証明書の発行を受けた者に関わる情報でないかどうか、証明書発行データベースで調べます。証明書発行データベースに記録されている基本4情報と、送られてきた異動情報に含まれる異動前の氏名、生年月日、性別、住所とが一致する者はないか突合させて調べるのです。もし、一致する者があれば、その者の基本4情報を電子証明書の発行を受けた者に関わる異動情報として公的個人認証の「指定認証機関」に送付します。

送付を受けた「指定認証機関」は、異動によってこの者の電子証明書は失効したとして、「基本4情報とシリアル番号対応データベース」の情報を更新するとともに、この者の電子証明書に関わるシリアル番号、失効事由、記録年月日を失効リストに付け足します。

読者のみなさんもこれで公的個人認証サービスが失効情報を得るために住基ネットと関係していることがわかりになったと思います。

■ 異動等情報の入手先は「指定情報処理機関」しかないのか

では、公的個人認証の「指定認証機関」が「異動等失効情報（公的個人認証サービスを受けている住民が住所や氏名が変わったり、死亡の事実が生じた情報）」を手に入れる先は、住基ネットの「指定情報処理機関」しかないのでしょうか。筆者はそうではないと考えます。

そもそも住基ネットの「指定情報処理機関」は、住民の「住所や氏名が変わったり、死亡」した異動情報は市町村から得ています。ならば、公的個人認証の「指定認証機関」は「指定情報処理機関」を経由せずに直接市町村から異動情報を得ても、正確な本人確認を実現する上で何らの問題もないはずです。いや、むしろ直接得るようにした方が、「指定認証機関」は「指定情報処理機関」経由よりも異動の事実を早く知りうるができるでしょうから証明書の有効性を確認する点では優れているでしょう。また、経由しないことによって公的個人認証のシステムをよりシ

ンプルにする、すなわち今後の運用も含めてより安く実現することが可能ではないでしょうか。

■ 住基ネットと一切関わらない公的個人認証システムの提案

そこで、筆者は公的個人認証の「指定認証機関」が「指定情報処理機関」を経由せずに直接市町村から「異動等失効情報」を得るシステムを先に見た「電子証明書発行情報・異動等情報の流れ」を元に考えてみました（図2）。

まず、電子証明書発行時の情報の流れについてです。市町村は「指定認証機関」に申請者の基本4情報（氏名、生年月日、性別、住所）を公的個人認証専用受付窓口端末を使って「指定認証機関」に送付しなければなりません、これらの情報は住基ネットのCS端末だけでなく、当然、住基ネット以前から市町村にあった住民基本台帳処理システム（既存住基システム）にも記録されています。したがって、基本4情報は住基ネットのCS端末ではなく既存住基システムから得ることにします。

「指定認証機関」は、送られてきた基本4情報をもとに電子証明書を発行するとともに、基本4情報と電子証明書のシリアル番号を「基本4情報とシリアル番号対応データベース」に記録します。このシステムでは電子証明書の発行に住基ネットは一切関係しませんから、「指定認証機関」は、住基ネットの「指定情報処理機関」にはいかなる情報も送付しません。

次に異動等情報の通知時における情報の流れです。住民の基本4情報に変更があった場合や住民票が削除された場合（死亡等）は、市町村は電子証明書交付した住民に関するものについてのみ、これを異動情報として公的個人認証の「指定認証機関」に直接送付します。

送付を受けた「指定認証機関」は、異動によってこの者の電子証明書は失効したとして、「基本4情報とシリアル番号対応データベース」の情報を更新するとともに、この者の電子証明書に関わるシリアル番号、失効事由、記録年月日を失効リストに付け足します。失効リストの作成にも住基ネットは一切関係しません。

筆者が提案する住基ネットと一切関わらない公的個人認証システムは以上ですが、実はこのシステムを実現する上で大事な点が一つあります。現在準備が進められている公的個人認証のシステムでは市町村には電子証明書の交

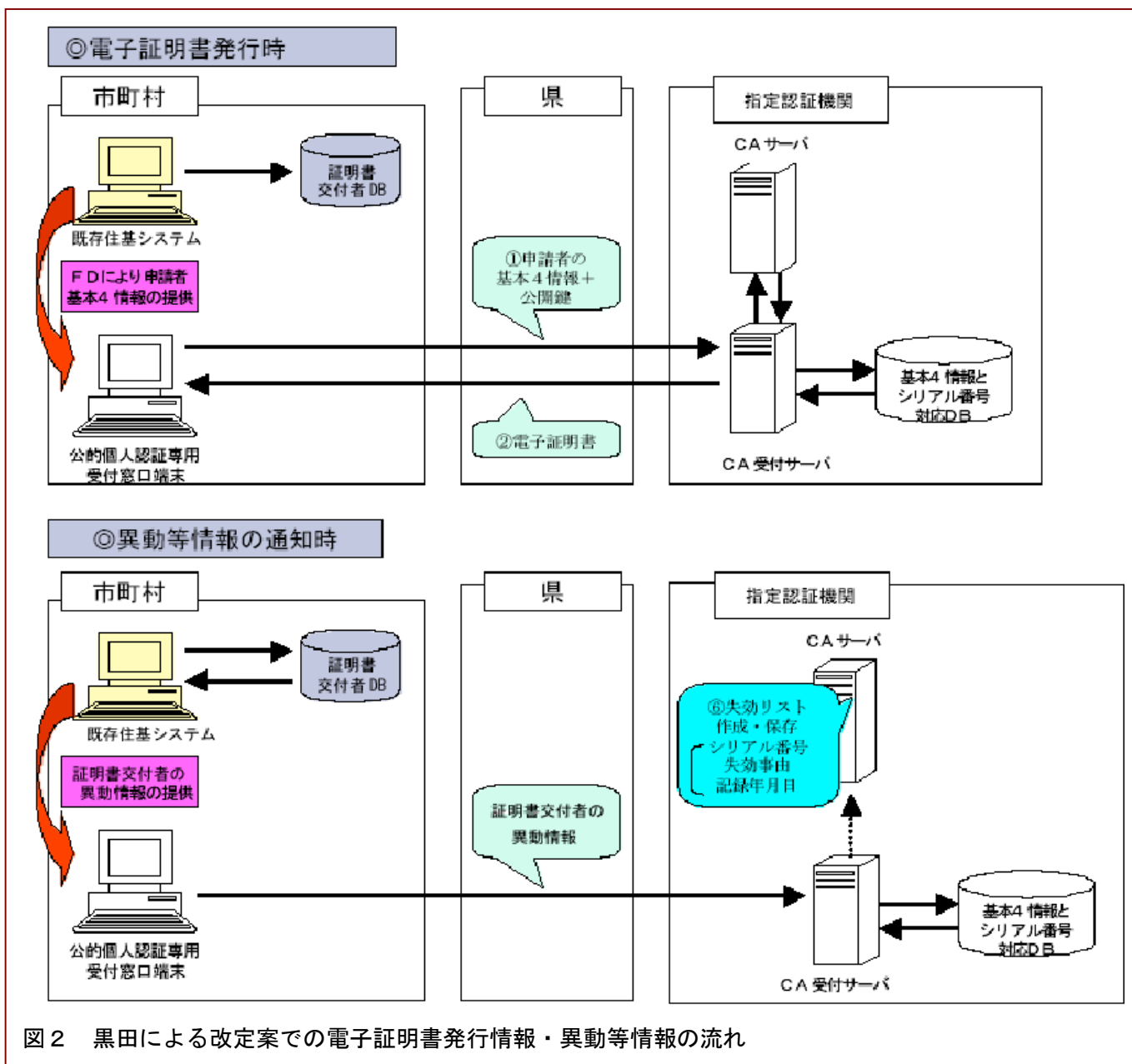


図2 黒田による改定案での電子証明書発行情報・異動等情報の流れ

付記録は残りません。そのため住民から転居の届けや死亡の届けがあっても、市町村はその者が電子証明書の交付を受けた者かどうか見分けがつかず。そのためこれらの情報を異動等失効情報として公的個人認証の「指定認証機関」に送付して良いのかどうか判断できません。

そこで、あらたに市町村に電子証明書の交付記録を残すようにする必要があります。もちろんその分、コストが上がることになると思いますが、これは受け入れられるべきでしょう。なぜなら、市町村は電子証明書の交付を自らの業務として行っているながら誰に交付したか知ることができないという現在のシステムの方にこそ、筆者は問題があると考えているからです。

以上のようにすれば、住基ネットと関わることもなく、

もっと言うなら、住基ネットがなくても公的個人認証サービスを実現することは可能になるでしょう。住基ネットが必要な理由として政府は、電子政府・電子自治体を実現するための公的認証サービスに不可欠だからだとしています。しかし、決してそうではないことが以上の考察からわかると思います。

■ 公的個人認証サービスは再考すべき

さらに、この住基ネットと一切関わらない公的個人認証サービスには大きな利点があります。それは住民登録ではなく外国人登録を市町村に行っている住民も公的個人認証サービスによる電子証明書の交付を受けられるようになる点です。外国人登録者の場合は、既存住基システムか

らではなく市町村の外国人登録の処理システムから基本4情報（氏名、生年月日、性別、住所）を得て「指定認証機関」に送付するようにします。また、異動のあった場合も住民登録者の場合と同様に、電子証明書の交付記録をもとに電子証明書の発行を受けた住民に関わるものについてのみ「指定認証機関」に送付すれば良いのです。これで、公的個人認証サービスにおける国籍の有無による差別的取り扱いの問題は解決します（注2）。

（注2） 法務省入国管理局「平成14年末現在における外国人登録者統計について（概要）」（<http://www.moj.go.jp/PRESS/030530-1/030530-1.html>）によれば、2002年末現在における外国人登録者数は1,851,758人（総人口の1.45%）であり、特に東京都では人口の2.74%が外国人登録者です。現在の公的個人認証サービスは、こうした多数の人たちをはじめから排除したものとなっています。外国人登録者でも政府や自治体に申請や申告を当然するのですから、これはあまりにも理不尽な取り扱いです。

筆者は『研究所通信』No.2にて公的個人認証サービスの必要性について疑問を呈しましたが、本稿では、百歩譲ってそれが電子政府・電子自治体を実現するためにはどうしても必要だとしても、住基ネットを使う必然性はなく、むしろ使わない方が優れたものになることを明らかにできたのではないかと考えます。

1999年当時、住基ネットの根拠である住民基本台帳法の改正案が国会で議論された際には、公的個人認証サービスとの関係については全く議論されませんでした。公的個人認証サービスに住基ネットワークを使おうという話が公の場に出てきたのは、改正案が可決された後の1999年12月に発足した「地方公共団体における個人認証基盤検討委員会」（委員長 大山永昭東京工業大学教授）がまとめた2

000年3月の報告書「地方公共団体における個人認証基盤の在り方について」（<http://www.soumu.go.jp/kokusai/pdf/ninsyou.pdf>）が最初ようです。法律をまず通し、後から使い方を思案するのも、一旦作ってしまったからには兎に角使わないと考えるのもおかしな話です。

政府は、公的個人認証サービスが日本のIT立国にとって必要不可欠と考えるなら、また広く国民（在日外国人も含めて）に使われるようにしたいと考えるなら、そして危険性が様々に指摘され国民の評価が最悪の住基ネットと心中する気がないなら、この際、住基ネットと一切関わらないシステムとして構築をやり直すべきではないでしょうか。同時に、住基ネットが必要だとする理由の一つが根拠のないものであることも以上のように明らかなのですから、住基ネットそのものについても再考すべきではないでしょうか。

※ 本稿は、議論をわかりやすくするために、都道府県が公的個人認証サービスに関わる業務を「指定認証機関」に委託することを前提として進めています。しかし、委託せずに都道府県が独自にこれらの業務を行うことは法的にはもちろん可能です。個人認証に関わる個人情報を「指定認証機関」に一元的に集約することで政府による国民監視が強まる問題や、一元的に集約することによって生じるセキュリティ上の問題についても当然議論されるべきだと考えます。

また、市町村と「指定認証機関」との公的個人認証に関わる情報のやり取りに、住基ネットよりもセキュリティが甘いと考えられる総合行政ネットワーク（LGWAN）が使われることについても問題があると考えます。こうした問題については、あらためて議論をしたいと思っています。

自治体情報政策研究所 JJ-SOUKO.com

URL : <http://www.JJ-SOUKO.com/>

E-mail : kuroda@JJ-SOUKO.com