特集　共通番号制度に関する最近の動向

海外における国民番号の活用事例とその課題

特定非営利活動法人 東アジア国際ビジネス支援センター 事務局長
リサーチネットワーク株式会社 代表取締役
安達　和夫

現在、社会保障改革検討本部を中心に、全国民に番号を付番し納税や年金情報などを一元管理する「共通番号制度」の導入が検討されており、2015年1月に税務分野の一部で運用を開始する方針が固められた。当面の対象は社会保障分野と税分野に限っているが、今後国民の理解を前提に利用範囲を民間へと拡大する方針であることから、実質的に共通番号制度は「国民番号制度」と捉えることができる。

国民番号制度を既に導入している国は、IT先進国を中心に数多く存在している。本稿では、そうした海外諸国における国民番号の活用実態とその課題について考察を行いたい。

1 国民番号制度の意味

国民番号制度は、個人に特定の番号を付与し、その番号を用いて本人を識別するための制度であるが、その意味するところは極めて深く重要である。

これまで、紙に書かれた文書が、情報を記録・蓄積し交換する唯一の手段であった時代が長く続き、本人を確実に確認する方法は基本的に対面によるものであった。そのため、結婚、出産、転居、死亡等、人生の大きなイベントが発生するたびに役所に出向いて届出を行い、その結果は紙の台帳に記載され保存される。また、台帳に記載された事項の証明が必要な際は、役所の窓口で紙の証明書の交付を受ける必要があった。

同時に、台帳に記載する事項は本人の申し立てを前提とした「申請主義」の考え方も長く踏襲されてきた。行政への申請は国民の義務であり、申請を忘れた際の不利益は本人の責任であるという自己責任の考え方である。

こうした行政の考え方は、わが国の行政では今日でも踏襲されているが、デジタルネットワークの発展の結果、当然のように次のような要求が提起される。

- ●役所に出向くのではなく、ネットワークを介して手続きが行えないか
- ●証明書類を電子的に交換することができないか
- ●複数の申請を束ねて一本化できないか
- ●必要な申請等を行政から通知するようなプッシュ型行政サービスができないか

こうしたデジタルネットワークを活用した行政サービスは、IT先進国ではすでに一般的に活用されており、国民向けサービスの向上や効率化等の面で多くの成果が報告されている。すなわち、「紙中心の文化」から「デジタルネットワーク前提の文化」への大きな変貌であり、そのベースには本人を確実に識別、確認できる国民番号制度がある。

紙と申請主義と対面確認を前提としたわが国の行政システムは、IT先進国に比べ少なくとも20年以上は遅れていると言っても過言ではない。

2 デジタルネットワーク時代の行政サービス

以下、海外でのデジタルネットワークを活用した行政サービスの事例を、いくつか紹介する。

(1) 韓国の行政情報共同利用制度

韓国では、市民に対する証明書や通知書類の交付と諸手続きでの添付を削減することを目的に、行政機関が管理する情報のネットワークを介した共同利用施策を2003年から推進している。行政、公共、金融分野へ申請を行う際に必要な証明書類の添付を廃止し、証明書で確認すべき情報を申請受付け機関が行政情報共同利用センターを介して情報保有機関に照会する制度である。この制度では、韓国の国民番号制度である住民登録番号によって個人を確実に識別・確認できることが重要な要件となっている。

こうした施策を実行した結果、4,600種類の添付書類を削減し、年間2億9千万件の文書発行が削減された。これをコスト換算すると、官民合計で1兆7,743億ウォンのコスト削減に結びついたと言われている。

このような制度では個人情報保護が大きな問題となるが、韓国の行政情報共同利用の基盤となるシステムでは「公共機関の個人情報保護法」にもとづいたプライバシー・ポリシーを反映したアクセス管理機能によって個人情報を保護している。さらに、情報保有機関から提供された情報の用途は照会、突合、閲覧等に限定され、提供を受けた機関での蓄積や保存は禁止されており、目的外利用を制限している。

また、証明書の発行が必要な場合についても、KIOSK端末や在宅でのオンライン発行サービスが定着しており、行政窓口に出向く機会は大幅に減り、行政機関自体の業務効率化に大きく貢献している。

(2) 記入済み税務申告制度

韓国や北欧諸国などで採用されている制度で、納税義務者の給与収入や利子、不動産の売却益、有価証券の取引利益、1年間にかかった医療費等の申告に必要な情報を予め税務署が収集し、記入済みの税務申告書類を作成して納税義務者に送付する。納税義務者はそれを確認、同意することで申告手続きが完了する。もちろん、必要がある場合は修正申告を行うこともできる。従来大きな負担となっていた税務申告が大幅に簡素化され、納税義務者、税務当局双方にとっての大きな効率化につながっている。

こうした仕組みは、雇用主、銀行、信用供与会社、不動産、保険会社等の関係する機関が、税務署に対しネットワークを介して個人の税務申告に係る情報を国民番号によって確実に個人を識別できる形で伝達することで成り立っており、この仕組みを採用している国では、法律で電子的な情報提供が義務付けられている。

このことは、国民番号が行政分野だけでなく、民間分野でも広範囲に利用されることが重要であることを示している。

(3) My-Pageサービス

デンマークを始めとする欧州主要国ならびに韓国、マレーシアなどで行われているプッシュ型行政サービスに、My-Pageサービスがある（国によって多少名称が異なる）。

インターネット上の政府サイトに個人のページが設けられ、本人とその家族に関して行政が保有している情報を閲覧することができる。過去に申請・届出した内容や、申請を要する事項の案内、受給権利のある交付金や助成金等の案内などが、国民番号によってパーソナライズされた情報として表示され、必要に応じてそのサイトを通じて申請を行うことができる。

わが国では、厚生年金保険での3号被保険者切り替え漏れが問題になっているが、これは申請主義に起因する代表的な事例であり、My-Pageのような行政からのプッシュ型サービスによってこうした齟齬も解消できる。

さて、これらの行政サービスは、本人を確実に識別し、番号に紐付けられた情報を確実に活用することで成り立っている。すなわち、全ての国民を対象とした国民番号制度を導入することで成立したサービスである。言い換えれば、国民番号制度は、デジタルネットワーク社会を実現する上で重要な基盤としての位置づけを持っている。

同時に、国民番号制度は、本人を識別し番号に紐付けられた情報を相互に交換するための基盤であることから、その運用にあたっては各国とも細心の注意を払っている。

国民番号を運用する上で考慮すべき点は、大きく次の脅威に対する万全な考慮である。

●番号の盗用や番号詐称の脅威
●恣意的な名寄せの脅威
●個人情報の侵害の脅威

以下、それぞれの脅威に対して各国が行った対応について述べたい。

3 番号の盗用や番号詐称の脅威に対する対応

過去、アメリカの社会保障番号や韓国の住民登録番号が盗まれ、他人名義の番号を不正に使用した事件が大きな社会問題になった。

アメリカでは、社会保障番号はかなり広範囲に利用されており、銀行口座の開設やクレジットカード申込などの民間での利用も頻繁に行われている。社会保障番号は、confidentialな情報として位置づけられており、個人情報保護の対象にもなっている。しかしながら、番号を本人確認のために記載する場面が多いため、情報漏えいの機会も増大することになる。そのため、運転免許証や年金通知等の書類上から、社会保障番号をマスクする等の措置が取られ、不正使用が発覚した際には番号の変更申請も認められたが、完全に払しょくされたとはいえない状況である。

一方の韓国でも、住民登録番号が公的機関以外でも、例えばネットオークションなど様々な分野で本人確認手段として使われており、サイトへのハッキングや管理情報の流出などで住民登録番号が漏えいし、銀行口座開設、オンライン融資、携帯電話の取得、製品やチケットの購入等での不正使用が発覚している。韓国では、住民登録番号漏えい対策として、ネットワーク上で通用する新たなコードとしてi-PINを制度化し、行政安全部ならびに5つの民間認証局で発行されている。また、不正利用防止のため、i-PINの使用状況を本人へメールで通知するサービスや、番号の変更や複数番号を所持することを認めるなどの対応を取った。しかしながら、i-PIN取得にコストがかかることもあり、取得状況は国内18サイトの平均認証率で7.3%（2008年時点）に留まっている。一日の平均利用者数が5万名以上のポータルサイト、アクセス数1万名以上のサイトなど対象に、i-PINの導入を義務化するなどの措置を講じてはいるが、課題は依然残されている。

さて、両国で生じたこうした問題で共通しているのは、番号それ自体を本人確認の手段として使用した点である。番号は個人を一意に識別するための機能を持つが、番号を知っているから本人であるという理屈は果たして成り立つのであろうか？ さらに、個人を識別するための番号を、本人確認の手段として書面やサイト上に記載することは適正な運用と言えるのだろうか？

欧州の多くの国で採用されているID管理モデルを見る限り、答えは否である。オーストリアでは、

ネットワークで使用する個人番号は、出生時に付与される国民登録番号（ZMR）にもとづいてデータ保護委員会が付与するSourcePINと呼ばれるコードを使用している。SourcePINは発給時にIdentity Linkという本人確認の認証が行われ、証明書としての効力をもつ。**（図1参照）**

また、ベルギーやエストニアなどでも、e-カードもしくはeIDカードといった媒体に保管された電子証明書によって本人であることを確認する方法を採っている。これらの国では、国民番号自体は決してconfidentialな情報ではなく、氏名と同様の公知の情報と位置づけられており、ネットワーク上では個人番号とその電子証明書によって個人の識別と本人の確認ができる。

このように、国民番号を個人の確認手段として位置づけるのではなく、番号を認証する手段（クレデンシャル）によって個人を確認する仕組みの導入は必須であると考える。

わが国では、個人の識別と確認（認証）が同一もしくは混同して議論されることが多いが、国民番号の機能要件として両者を区別した議論が必要であると感じている。**（図2参照）**

4 恣意的な名寄せの脅威に対する対応

国民番号によって紐付けられた情報が、本人の意図に反した連携もしくは不正な活用を回避するためには、情報ならびに情報の連携を適正に管理するための基盤の構築が不可欠である。こうした基盤を「情報連携基盤」と呼んでいる。

情報連携基盤には、以下のような機能が求められる。

－アクセス権限の評価・確認
－セキュリティポリシーに基づくアクセスコントロール
－アクセス状況のモニタリング、ロギング機能
－全体環境の集中監視機能
－ヘルプデスク

情報連携基盤は、公的情報を連携させることで付加価値の高いサービスを実現している多くの国で構築されているが、ここではベルギーのモデル

図1　オーストリアのID管理モデル

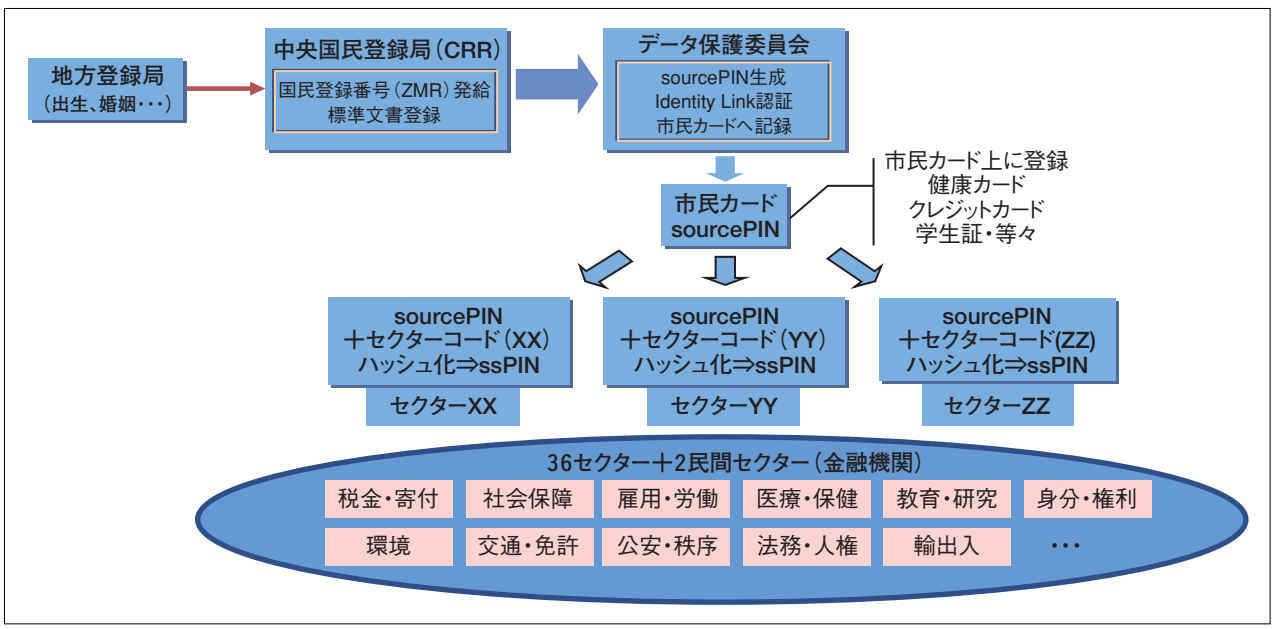
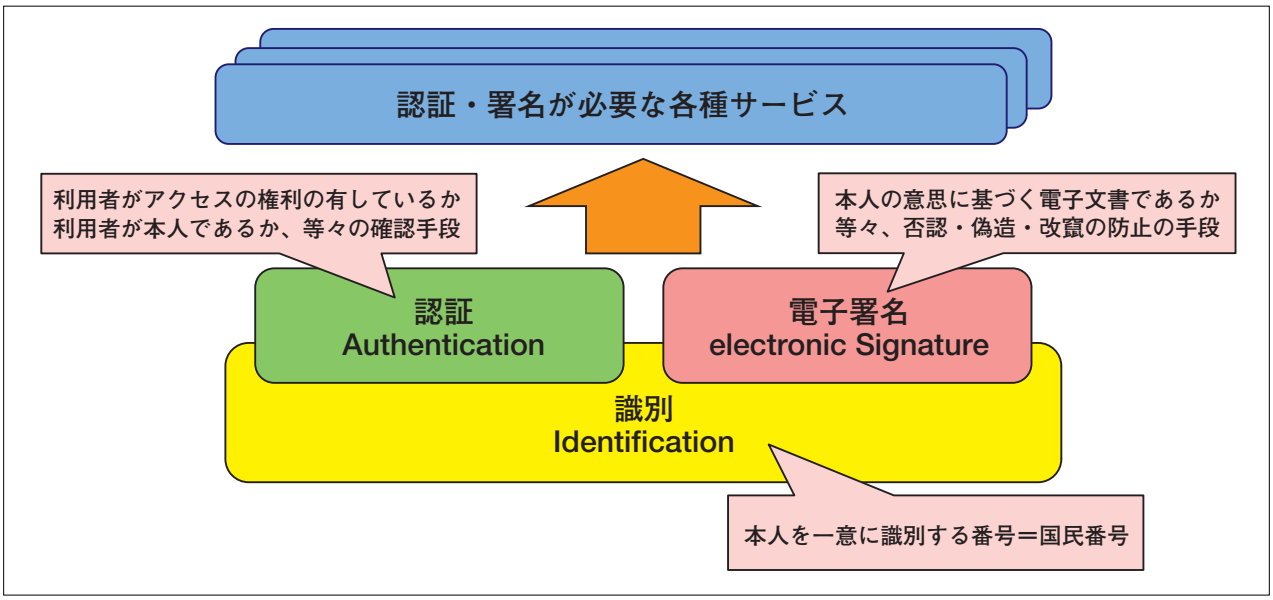


図2　識別・認証・署名の位置づけ



を例にその機能について解説する。

ベルギーでは「Crossroade Bank for Social Security（CBSS)」と呼ばれる社会保障分野の情報連携基盤が構築されており、官民合わせて約3,000機関の共通プラットフォームとして活用されている。CBSSを介して情報が連携されたことで、次のような効果が報告されている。

●諸手続に必要な証明書等の約210種類の添付書類を廃止
●手続の統合により約50の申請書類を廃止、約30種類の申請書類を簡略化
●同一イベントで関連する手続のワンストップ化
●雇用者の社内人事、経理システムとのシームレスな連携
●受給資格が確認できるクライアントに対する補助金等を申請なしに自動給付

ベルギーでは、議会が指名したプライバシー保護委員会によって「アクセス制御ポリシー」が制定され、そのポリシーは国民に公開される。CBSSは、こうして制定されたアクセス制御ポリシーのもとで、適正な運用が保証される仕組みになっている。

アクセス制御ポリシーは、CBSS上のアプリケーション登録簿、利用可能データ登録簿、アクセス認可登録簿に登録され、全てのトランザクションはCBSSのアクセス制御機能により登録されたポリシーと照合され、データ・アクセスの妥当性が評価される仕組みになっている。その結果、アクセスが妥当と判断されたトランザクションについてのみ、必要なデータを管理しているアプリケーションへデータを要求し、交換されることになる。

また、全てのデータ・アクセスはログ情報として記録され、本人は自分に係る情報のアクセス記録を閲覧することで、適正な連携が行われたことを確認するとともに、万一身に覚えのない情報が交換された場合は、プライバシー保護委員会に照会することができる。

さらに、これらのアクセス記録は分析・評価され、今後のポリシー改正にも反映されている。**（図3参照）**

ベルギーの情報連携基盤が、情報の適正な交換に寄与しているポイントは、以下のように整理することができる。

●議会の指名による第三者機関であるプライバ

シー保護委員会の存在

- ●アクセス制御ポリシーの国民への公開
- ●全てのアクセスを記録し必要に応じて当事者へ開示
- ●アクセス実態の分析・評価とポリシーへの反映

恣意的な名寄せに対する不安は、国民の関知できない場面で情報が連携され、その結果国民に不利益を与えることを防止する仕組みを確立することで、その多くは防止できる。そのためには、明確なアクセス制御ポリシーを確立し、それを国民の監視のもとで適正に運用することが極めて重要である。

5 個人情報の侵害の脅威に対する対応

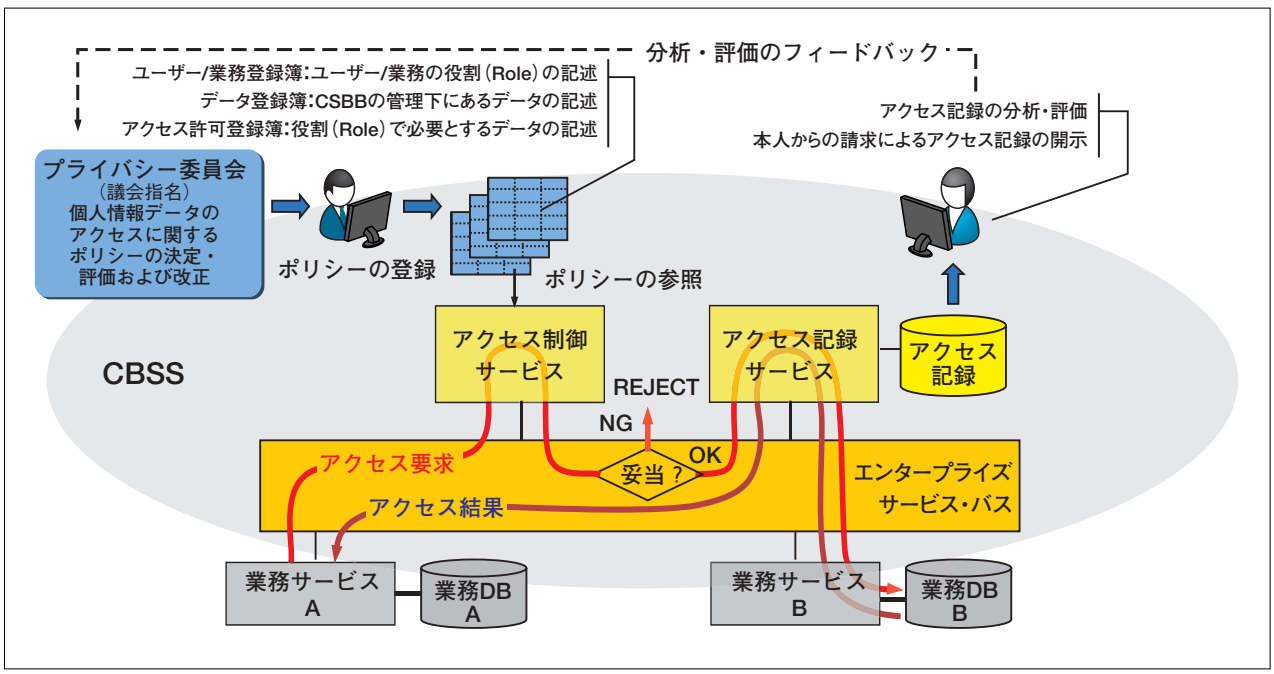
欧州では、EUデータ保護指令（EU Data Protection Directive）に基づき、すでに1970年台には、データ保護機関（Data Protection Authority = DPA）の設置を含めた、個人情報保護法制定に向けた立法措置が取られた。

EUデータ保護指令では、DPAを中心とする監督機関に以下のような強い権限を与えている。

- ✓監督遂行上必要なデータにアクセスする権限
- ✓監督遂行上必要なすべての情報を収集する権限
- ✓個人情報を取扱うすべての業務をチェックし是正指導等を行う権限
- ✓データのブロックや消去または破壊を命じる権限
- ✓データの取扱いの中断もしくは禁止を命じる権限
- ✓管理者に対し警告または懲戒を命じる権限
- ✓議会等への問題点の照会を行う権限
- ✓違反事案に対する法的手続きを開始する権限
- ✓違反を司法機関に通知する権限

－等々

図3　ベルギーの情報連携基盤



欧州の多くの国では、こうした強い権限を持つ監督機関が、行政とは独立した第三者機関として設立されており、前述のベルギーのプライバシー保護委員会も同様の機関である。

筆者は、3年前にデンマークのデータ保護機関（The Danish Data Protection Agency）を訪問したが、ここでもEUデータ保護指令に基づき、健康管理面の法律、金融管理面の法律、ならびに法務省令の運用細則等で規定された個人情報保護が適正に適応されているかなどをチェックする機関として機能していた。

また、国民からの苦情を取り上げる仕事や、法律に対するガイドラインの作成も行っており、国際会議や専門化レベルの作業を通じて関係各国との連携などにも参加している。

デンマークのDPAでは、訪問当時35名が常勤職員として勤務しており、その職員は法律の専門家と技術面の専門家で構成されている。

DPAのもとで重要な案件を審議するための委員会が設けられ、議長は最高裁判事が勤めている。委員は6名で、法務省から任命される。この委員会で重要案件を審議する際には、DPAが調査レポートを提出し、それを議論のベースにする。審議結果によっては、裁判所に提訴することもあり得る。

また、新しい法律が提案されると、DPAには議会提案前に送付され、DPAが事前に判断し意見書を提出する。同様に、民間や公的企業のデータプロセスに関する情報もWebを通じて送られてくる。それらが個人情報保護法に抵触しているか否かのチェックを行い、その結果に基づいて許認可を行う権限をDPAは持っている。

一方、国民からの苦情は、PC、電話、書面等を通じて随時受け付け、個々のケースについて法律上で不正行為が行われていないかをチェックする。これらの審査結果はWeb上で公開している。公開することで苦情の数は年々減少する傾向にあり、最近では故意によるケースでも年間10～20件程度に抑えられているという。

また、デンマークでは市民オンブズマン制度も活用されており、国民が自分の個人情報が破られたと判断した場合、オンブズマンに訴えるケースも多い。オンブズマンも、苦情処理についてはDPAと同じ機能があり、同じ案件をDPAとオンブズマンが併行してアプローチするケースもあるようだ。

個人情報の侵害の脅威は、あらゆる場面で想定される。そのため、事前の防御策に加えて、侵害が発生した際の対処手段が重要である。国民のプライバシー意識が高いデンマークであっても、一旦官庁に登録された個人情報が必要に応じて省庁間を横断することを拒否することはできない。むしろ、個人の情報がデータベースに蓄積され、必要な書類が省庁間で交換されることを多くの国民は期待している。こうした意識の背景には、国民の政府に対する信頼度の高さがあると推察するが、DPAの存在は、そうした信頼感の醸成にも大きく寄与していると考えられる。

6 まとめ

国民番号制度はデジタルネットワーク社会の基盤であり、便利で効率的な社会を形成する上ではなくてはならない制度である。デジタルネットワークを基盤とした社会制度面では先進諸外国から20年以上も遅れているともいわれるわが国とすれば、国民番号の導入とその活用は喫緊の課題である。

同時に、国民番号は社会全般に大きな影響を与えるものであり、導入にあたっては法制度や運用体制等で十全の対策が求められる。

安心・安全を担保し得る制度設計と、その運用ビジョンを形成する上で、海外の取組み事例には今後も多くの学ぶべき点があると感じている。