「国民ID制度」および「社会保障・税の番号制度」に向けたVRICSによる自治体情報基盤の構築における一考察 : 「国民ID制度」および「社会保障・税の番号制度」の政府取り組み状況

中井, 俊文
九州大学システムLSI研究センター : 特任准教授

https://doi.org/10.15017/25641

出版情報：SLRC Discussion Paper Series. 8 (1), pp.0-79, 2012-12. 九州大学システムLSI研究センター (SLRC)
バージョン：
権利関係：

「国民 ID 制度」および「社会保障・税の番号制度」に向けた VRICS による自治体情報基盤の構築における一考察

～「国民 ID 制度」および「社会保障・税の番号制度」の政府取り組み状況～

平成 24 年 12 月

九州大学　システム LSI 研究センター
中井　俊文

まえがき

現在、政府では行政システムの革新を目指し、「社会保障・税の番号制度」を進めるべく、国会にマイナンバー法案を提出し、審議がなされようとしている。ここでは、「社会保障・税の番号制度」とその考え方の基本となっている「国民 ID 制度」について、現在までの政府での検討内容を整理し、将来のこの両番号制度に対応を求められる自治体情報基盤について、九州大学が開発した社会情報基盤 VRICS（Value and Right Circulation control System）による自治体情報基盤の構築方法の検討を行った。

まず、政府が検討を進めている「国民 ID 制度」と「社会保障・税の番号制度」について説明する。「国民 ID 制度」と「社会保障・税の番号制度」に関し、政府・与党社会保障改革検討本部で決定した「社会保障・税に関わる番号制度についての基本方針」[1]を踏まえ、社会保障・税に関わる番号制度に関する実務検討会が作成した「社会保障・税番号要綱」[2]と「社会保障・税番号大綱」[3]の内容を咀嚼し、要件を整理した。

次に、自治体に求められる情報基盤について説明し、自治体の情報基盤として、九州大学が開発した社会情報基盤 VRICS（Value and Right Circulation control System）を用いる場合について、実際に自治体の情報基盤として設計するための検討要素について説明する。

これらの検討においては、「社会保障・税に関わる番号制度についての基本方針」[1]、「社会保障・税番号要綱」[2]、および「社会保障・税番号大綱」[3]と要綱と大綱の策定の技術的検討である「社会保障・税に関わる番号制度及び国民 ID 制度における情報連携基盤技術の骨格案」[4][5]と政府関連文書を参考とした。

また、本制度の基礎研究事業として、2009 年度、2010 年度の 2 ヶ年に渡り九州大学で行った厚生労働省からの受託事業「社会保障カード（仮称）の制度設計に向けた実証事業」の成果と経験より、自治体の情報基盤の在り方を考察している。

本考察は、自治体向け情報基盤を VRICS により実現する目的としたが、政府の「国民 ID 制度」と「社会保障・税の番号制度」の考え方の理解や将来自治体が構築すべき社会情報基盤の検討にも有用となるであろう。

目次

第１章　「国民 ID 制度」と「社会保障・税の番号制度」の考え方

1.1　背景と課題

政府の「社会保障・税に関わる番号制度についての基本方針」[1]では、“国民がこれまで行政に対して抱いてきた不満は、国民一人ひとりが公平・公正に扱われているだろうか、自分の納めた税金や保険料にふさわしい社会保障がきめ細やかに、また的確に行われているだろうか、自分の権利がしっかりと守られ、そのことを自分の目で確認することができるだろうか”、といった点としている。これに対して政府は、必ずしも十分な制度が構築されていない[1]と反省している。

また、行政手続においても、手続の重複、煩雑、不便、コストがかかることを指摘している。さらに、行政サービスがプル型であり、「知っているものだけが得をする」という仕組みであり、制度上利用できるサービスであってもそれを知らないため、みすみす受給の機会を逃してしまうような不公平が生じていることを指摘している。

一方、行政にとっては、個々のサービスを必要とする本人の特定ができなかったため、真に手を差し伸べるべき人に対してセーフティネットの提供ができなかったり、不正行為の防止が十分果たせなかったりした状態にあるとしている。このため、行政では多大なコストと時間と労力をかけて数多くの書類を審査し、結果、人的なミスを誘発しやすい作業を毎年繰り返しており、本来国民へのサービスに振り向けられるべき財源や人的資源が重複する作業等に費消されていると、基本方針では課題を挙げている。これは、国―地方の間、国の各府省間、地方公共団体間や各主体内の業務間の情報の連携が不足しているためだと分析している。[1]

さらに、基本方針では、国民が不満・負担等を感じる状況は、民間サービスにおいても生じており、この原因は、複数の機関に存在し、かつそれぞれに蓄積される個人の情報が同一人の情報であるということの確認を行うための基盤が存在しないことに起因するとしている。また、このことから、国民一人ひとりの情報が分野を超えて「ヨコ」につながる必要性が、この基盤なしには充足しがたいと結論付けている。[1]

この番号制度は、このような基盤を提供することにより、国民が公平・公正さを実感し、国民の負担が軽減され、国民の利便性が向上し、国民の権利がより確実に守られるような社会を実現することを目的としている。[1]

「国民 ID 制度」はかねてより政府の高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）にて検討が進められてきた。しかし、2007 年 5 月に発覚した年金記録問題に端を発し、社会保障制度の見直しの必要が論じられ、社会保障カード（仮称）の検討が開始された。2010 年 5 月には、高度情報通信ネットワーク社会推進戦略本部にて 2013 年までに「国民 ID 制度」の導入を予定した「新たな情報通信技術戦略」が発表された一方、2009 年、2010 年には、厚生労働省が九州大学を含む全国 7 か所で社会保障カード（仮称）の実証実験を行った。

2010 年、民主党に政権が交代し、政府は政策の目玉として「社会保障と税の一体改革」を掲げ、「社会保障・税の番号制度」を推進することとなった。この「社会保障・税の番号制度」はかねてより検討が進められてきた「国民 ID 制度」を基礎として、社会保障と税の分野に具体化されたものとなっている。「社会保障・税番号大綱」においては、2014 年 6 月、個人に「番号」、法人等に「法人番号」を交付し、2015 年 1 月以降、「番号」を利用する分野のうち、社会保障分野、税務分野のうち可能な範囲で「番号」の利用を開始するとしている。さらに、2018 年を目途に利用範囲の拡大を含めた番号法の見直しを引き続き検討するとしている。

しかし、2012 年度の通常国会に提出された「マイナンバー法案」は未審議となり、秋の臨時国会以降の成立の予定である。現状、2015 年 1 月からの「番号」の利用はそのままの日程となっているが、システム（情報提供ネットワークシステム（旧称：情報連携基盤、以下情報提供ネットワークシステムと言う。））としては 2016 年 1 月からの稼働となっており、自治体とのシステム連結は 2016 年 7 月以降の日程にシフトしている。

この政府が構築しようとしている「国民 ID 制度」と「社会保障・税の番号制度」が有効的に機能するためには、住民サービスの窓口となっている自治体における住民サービスと連動しなければならない。しかし、自治体における住民サービスは全国画一の法の定めるところの行政サービスのみに留まらず、地域による条例で定めた行政サービスや公共施設の利用などの住民サービスまでも広範囲に広がっている。住民は、金融や物品の購入、情報入手など様々な形で、自治体が提供する以外のサービスも利用し、あるところでは自治体が提供するサービスと関係することになる。現在自治体が抱える、住民サービスの充実、地域格差、防災・減災対策、業務の効率化などや、社会が抱える高齢化、生活の多様化、環境問題などのため、更に多様な安心・安全で便利なサービスを必要としている。

九州大学では、現在使用されているシステムは必ずしも最適な社会システムの設計とはなっていないと考える。従来の「既存の社会システムの部分的な電子化」というアプローチから「情報技術の利用を前提とした新しい社会システムの構築とそのための技術開発」［6］として VRICS（Value and Right Circulation control System）を開発し、自治体の社会情報基盤として利用することを提言している。そこで、「国民 ID 制度」と「社会保障・税の番号制度」を効果的に利用するために、VRICS を用いた地方自治体の社会情報基盤との連携方法について具体的な方法を考察するに至った。

1.2　現在の社会保障の問題点

社会保障とは、1950 年の社会保障制度審議会勧告によれば、「社会保障制度とは，疾病，負傷，分娩，廃疾，死亡，老齢，失業，多子その他困窮の原因に対し，保険的方法又は直接公の

負担において経済保障の途を講じ，生活困窮に陥ったものに対しては，国家扶助によって最低限度の生活を保障するとともに，公衆衛生及び社会福祉の向上を図り，もってすべての国民が文化的成員たるに値する生活を営むことができるようにすることをいうのである。」［7］と定義されている。

Wikipedia を引けば、“個人的リスクである、病気・けが・出産・障害・出産・障害・死亡・加齢・失業などの生活上の問題について貧困を予防し、貧困者を救い、生活を安定させるために国家または社会が所得移転によって所得を保障し、医療や介護などの社会サービスを給付すること”と、やや簡単に説明されている。非常に乱暴な説明を加えれば、“年金、医療保険などに代表される、行政サービス”と言える。

現在国民が受けられる社会保障の種類には、医療保険、年金、雇用保険、高額医療控除など様々あり、就職、結婚、出産、離婚、引っ越し、起業、退職、診療、介護、死亡などのライフイベントで様々な手続きが必要となっている。

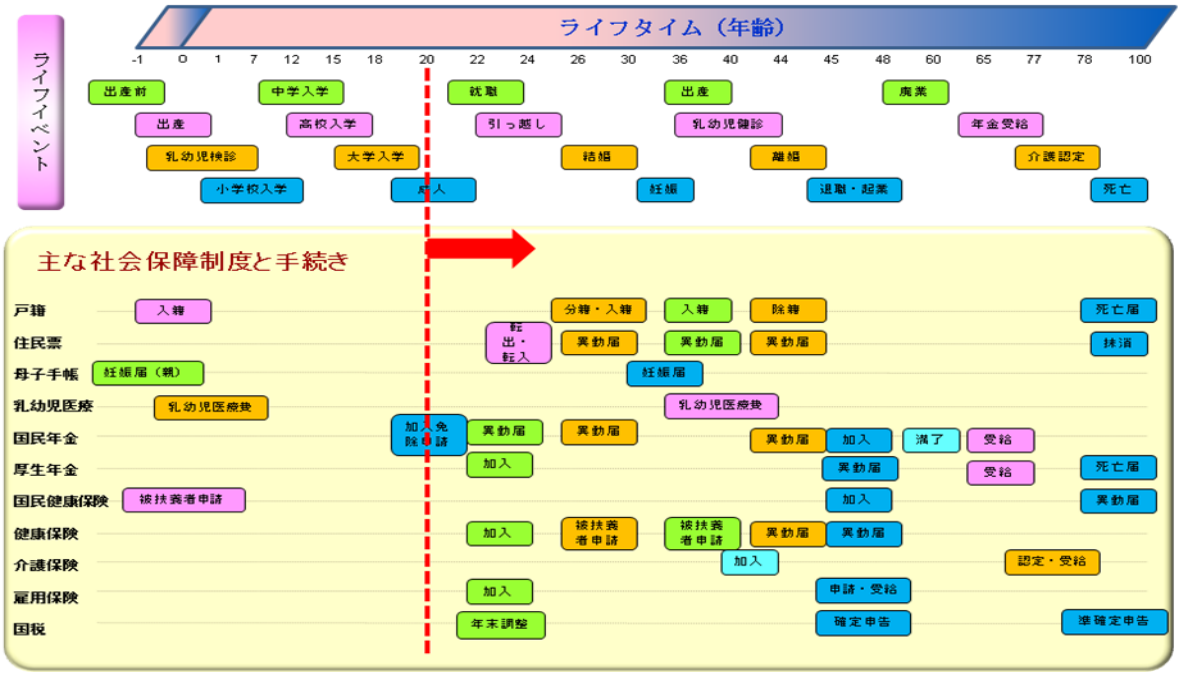


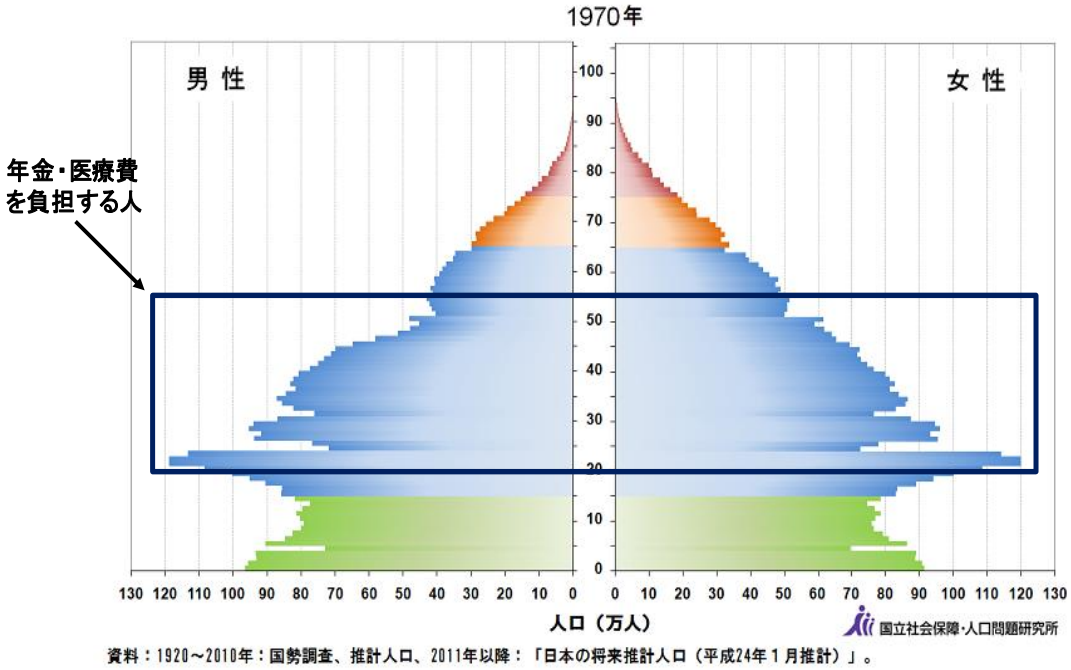
図１－１　ライフイベントと社会保障制度の手続き

例えば、図１－１に示すように、母親の妊娠から本人の死亡までを極めて荒く仮のライフイベントを横軸に並べ、代表する社会保障制度を縦軸に示した。多くの手続きは 20 歳を過ぎて行われるが、1 つのイベントに対し、複数の社会保障制度の手続きが必要になっていることが判る。

現在、社会保障制度が抱えている課題は以下のようである。

（1）人口構成

図１－２に現在の社会保障制度が考えられた頃の人口構成を示す。



（出典：国立社会保障・人口問題研究所、人口ピラミッドデータ）

図１－２　現在の社会保障制度の考えられた頃（1970 年）の人口構成

被用者保険や被用者年金に加入していない自営業者や農業従事者等に加入を義務づける新しい国民健康保険法が 1958 年に、国民年金法が 1969 年に制定された。その後、1961 年 4 月に全面施行され、国民皆保険・皆年金が確立された。 1973 年、田中内閣はこの年を「福祉元年」と位置づけ、社会保障の大幅な制度拡充（老人医療費無料制度の創設（70 歳以上の高齢者の自己負担無料化）、健康保険の被扶養者の給付率の引き上げ、高額療養費制度の導入、年金の給付水準の大幅な引き上げ、物価スライド・賃金スライドの導入など）を実施した。

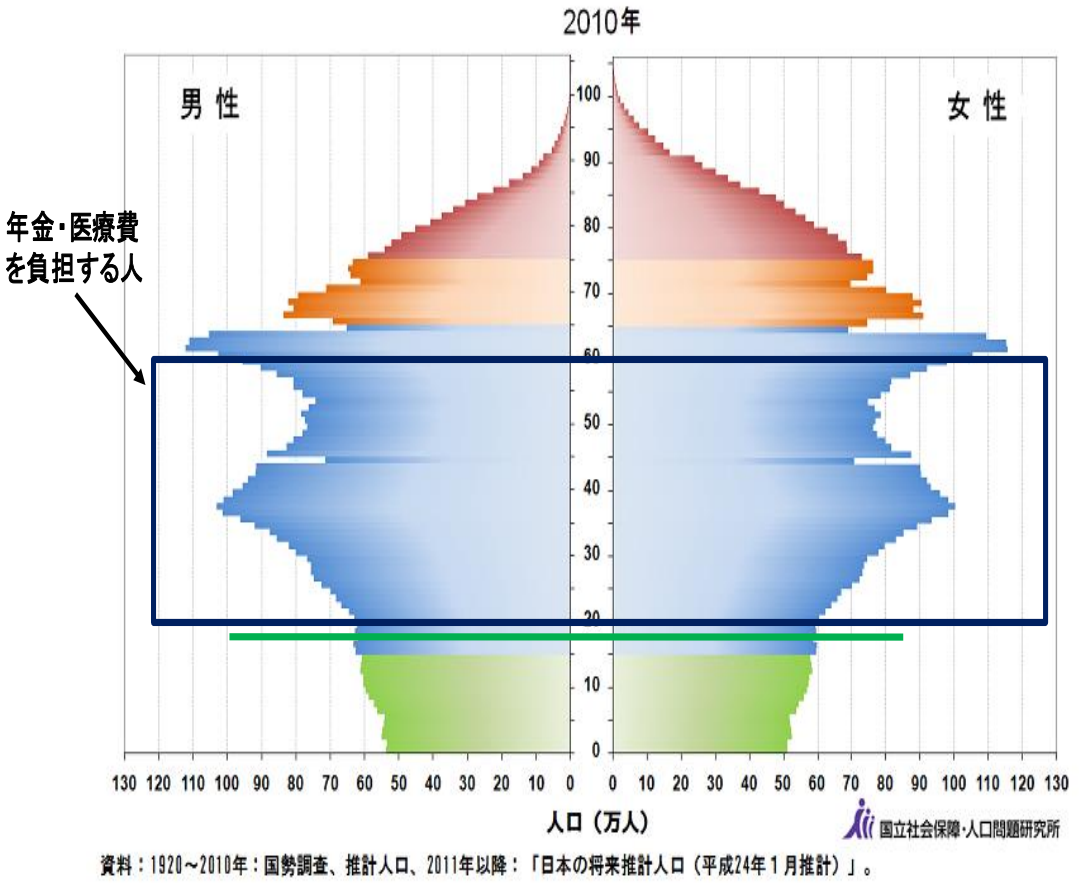
図 1-2 はこの当時の人口構成であり、青線で囲まれた年齢層が年金を納める層であり、また税金を納める主体となる層である。65 歳以上は年金の受給者であり、また医療にかかる機会が多く、一人当たりの医療費は高くなっている層である。青線で囲まれた社会保障の財源となる層とそれ以外の層を比較すれば、圧倒的に財源となる層が大きく、国民一人当たりの社会保障負担は小さなものと言える。

その後、1973 年秋にはオイルショックが勃発し、高度経済成長時代は終わった。これにより、低成長化による税収減と同時に、インフレに合わせ給付水準も上昇、社会保障関係費

が急増したため、社会保障制度を見直す必要性が出てきた。政府は、国の財政再建への対応や将来の超高齢化へ適合するよう、社会保障制度を見直していった。

図１－３は 2010 年の人口構成である。図１－２に示した 1970 年の人口構成と大きくことなり、完全にピラミッド形状は崩れ、釣鐘型になっている。高齢化社会の定義である高齢化率 7%からその倍の 14%になるまでわずか 24 年（1970 年～1994 年）と言う早さで高齢化が進んだ結果である。

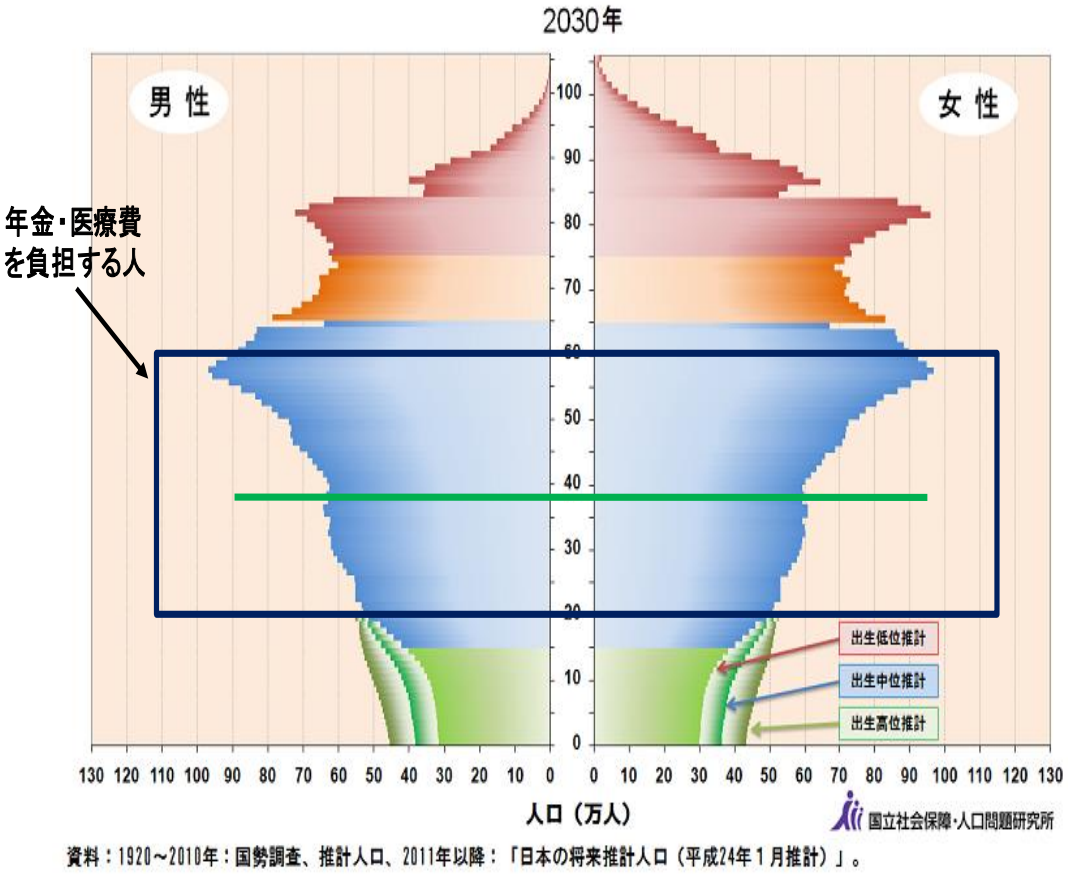
このため、青線で囲まれた社会保障の財源となる層とそれ以外の層の比率が変わり、青線で囲まれた層の負担が増していることが判る。これは国民１人当たりの社会保障負担が増加していることとも言える。また、将来の高齢者の介護問題が老後最大の不安要因となってくることが容易に想像できる。また、緑線で示した年齢は 2012 年で 20 歳の若者であり、これから社会保障制度に深く関っていくことになる人々である。



（出典：国立社会保障・人口問題研究所、人口ピラミッドデータ）

図１－３　2010 年（現在）の人口構成

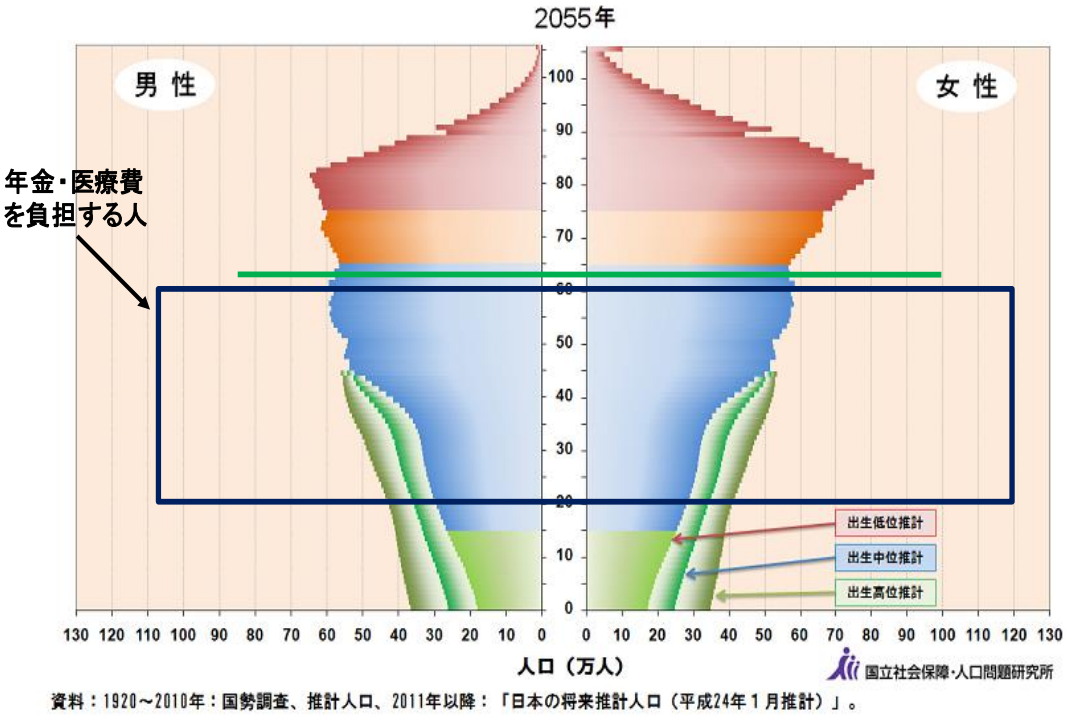
図１－４は 18 年後（2030 年）の人口構成である。図１－３で 18 歳だった若者は 38 歳となり、社会保障制度を財政時に支える層となっている。人口構成は更に根元が締まった形と変化し、60 歳以上の人口が青い線で囲まれた人口を超えることになってしまっている。つまり、青線で囲まれた社会保障の財源である層の負担が増していることが判る。また、高齢化により医療費も増えることが予想されるため、図で示された人口比率以上に負担が増えているとも考えられる。



（出典：国立社会保障・人口問題研究所、人口ピラミッドデータ）

図１－４　18 年後（2030 年）の人口構成

43 年後（2055 年）の人口構成を図１－５に示す。図１－３で 18 歳だった若者は 63 歳となり、仕事もリタイヤし、もうすぐ年金受給者になろうとしている。人口構成は完全に逆三角形に近づき、60 歳以上の人口が全人口の半数になろうとしている。青線で囲まれた社会保障の財源である層の負担がさらに増すことは疑う余地もない。さらに、高齢化により増加する医療費も国民一人当たりの社会保障負担を増やす要因となってくる。



（出典：国立社会保障・人口問題研究所、人口ピラミッドデータ）

図１－５　43 年後（2055 年）の人口構成

このように、近い将来若者が多くの老人を支える状況が訪れることを考えておく必要がある。一方、行政の立場から考えれば、限られた職員が増加する対象者の社会保障の手続きをサポートする必要がある。社会保障は今後さらに充実することとなるであろうことから、行政サービスを提供する自治体にとっては、より一層の効率化が求められるようになるであろう。

（2）縦割り行政

次に大きな問題となっているのは行政の縦割り構造である。前節でも説明したように社会保障制度を受けるためには、ライフイベントの度に様々な手続きが必要となる。これらの手続きは市役所、警察署、税務署や各中央行政の地区の出先機関などとばらばらであり、自治体の中でも行政サービスの担当する課によって窓口が異なっていることがある。さらに相互の情報の共有化がなされていないため、住民は類似の申請を異なる役所に提出することになっている。

例えば引っ越しをする場合、今住んでいる自治体に「転出届」を、これから住む自治体に「転入届」を提出するだけでなく、今受けている社会保障で住所が記載されているものについては全て住所変更の手続きが各々別々に行わなければならない。この手続きを行わないと

「住所不定」となり、行政サービスを受けることが出来なくなる。また、公共料金や免許証、車庫証明など変更手続きも不可欠である。児童を持っている家庭では、転入先の自治体の学校の手配なども含まれることになる。さらに、これらの手続きのために、住所が変更したと言う証明書や旧住所で受けていた社会保障制度の証明となる証明書などを要求されることがあり、これら証明書の取得手続きも必要となってしまっている。

社会保障制度や行政サービスは時代と共に充実してきたものであり、その都度新たにサービスが加わり、対象となった住民に対して用途別に管理されている。各省庁も様々な行政サービスを検討し、充実させてきた。このため、各々の社会保障や行政サービスは独自の仕組みとなり、情報の連携が出来ない構造となってしまった。各々の行政サービスを提供する機関は、行政サービスを円滑に実施するため、その制度の中で利用できる「利用番号」を対象となる住民に付番して管理してきた。その結果、住民は制度が異なる毎に異なる「利用番号」を持つこととなった。このため、住民にとって、ライフイベントの度に、類似の手続きのために何度も役所を訪れる事態が発生することとなる。一方、行政サービスを提供する機関側では、複数の機関にまたがる情報が本人のものであるかを特定できない、または特定するため多大な時間と労力が必要となってしまっていて、住民に類似の手続きをお願いしたり、必要以上の手間をかけたりすることとなっている。

（3）判りにくい制度

社会保障制度が判りにくいことも１つの課題である。住民の多くはどのような社会保障制度が用意されており、どのような人がそのサービスを受けられるのかと言う情報を持っていない。社会保障制度が多くあり、また複雑で判りにくいことが原因である。また、受けられる制度が判ったとしても、その審査基準が判らなかったり、審査過程や審査結果の理由などが不透明であったりすることもある。

現在の社会保障制度は「申請主義」であり、本人が申請することでサービスが受けられる制度となっている。本人が自分の受けられる社会保障制度を知らなければ、申請すら出来ないため、このことは「知っている者が得をする」仕組みとなっていると言わざるを得ない。つまり、社会保障制度が公平に作用されていないことを示している。全ての住民が今、自分が受けられる社会保障制度が一目で判り、容易に申請出来る仕組みが望まれている。

（4）制度の悪用

現在の課題の１つに社会保障制度を悪用した犯罪もある。例えば、医療保険制度（被保険者の医療費の７割を保険者が負担）を利用し、保険資格が無い者が他人の保険証で受診するケースや、複数の医療機関から保険制度を利用し薬剤を入手し他人に販売するなどのケースもある。これらは医療保険制度を悪用したものであり、被保険者が納めている保険料の基金を不法に使っている犯罪である。

また、1人の患者が自分の気に入る診断が下されるまで、様々な医療機関を渡り歩き、その都度、医療保険にて診察を受け続けると言った、犯罪とは言わずとも制度を使った保険料の無駄遣いとも言えるケースも少なからず見受けられる。社会保障費が増大していく中で、このような犯罪や、無駄遣いを無くすような安全な仕組みが必要である。

（5）住民の無関心

社会保障制度を受ける住民にも課題はある。日ごろから受けていたり、将来受ける可能性があったりする社会保障制度についてあまり関心を持っていないことである。医療機関にかかった際に医療費の7割が保険者から支払われており、自己負担が3割に留まっていることすら知らない人もいる。本人が年間幾らぐらいの医療費を使っており、医療保険から幾ら支出されているかを把握しておくことが大切である。また、国民年金は20歳になれば加入しなければならない。これは国民年金法にて、“日本国内に住所のある20歳以上60歳未満のすべての人が強制加入する”となっており、国民の義務である。これにもかかわらず、国民年金に加入しない若者が増えて来ていることも事実である。さらに、自分の年金に関して自分で管理することは必要である。社会保障制度が充実し、自分の受けられる社会保障制度について疎くなってきていることも事実である。2007年5月に発覚した年金記録問題は政府だけの問題とも言えない。それまで年金の記録管理を社会保険庁に任せきりにしておいた我々にも責任がある。社会保険庁のずさんな管理や記録が明らかとなり、5,000万件の「宙に浮いた年金記録」となった。自分の納付や社会保障の内容など、個人が責任を持って管理すると言う意識が必要である。このためにも、全国民が国の持っている自分の情報を簡単に入手し、間違いがあれば直ぐに訂正できるような仕組みが必要となる。また、社会保障制度に関心を持たすためにも今個人が受けている社会保障制度を見えるようにすることが大切である。

ここで挙げた課題点は解決されなければならない。社会保障サービス等の行政サービスのコストの低減、サービスの効率化、および国民への安心安全便利なサービスの実現である。具体的には、以下のような仕組が必要とされる。

① 業務の効率化とコスト削減

より多くのより充実した社会保障制度や行政サービスを提供する機関が少ない労力でコストを掛けずに提供できるような仕組み

② 1つの窓口で、全ての申請がワンストップで可能

複数の機関に存在する個人の情報が同一人の情報であると特定でき、情報連携出来ることで、住民の手間を省くことが出来る仕組み

③ 行政サービスの透明化

自分が受けられる社会保障制度が一目で判り、容易に申請出来、その処理過程や審査

内容がみえる仕組み

④ 安全性と信頼性の向上

社会保障制度の不正な使用が防止でき、個人情報が漏えいされず、個人の権利が守られる仕組み

⑤ 簡単に自分の情報を入手できる

政府や役所が保有している自分の情報が入手でき、その情報がどのように使われているかを監視できる仕組み

⑥ 身近な仕組み（24 時間いつでも、何処からでも、好きな端末で、アクセス可能 ）

「どのような住民(IT 弱者やハンディキャップ)でも」、「いつでも」、「どこからでも」自由に行政サービスを利用でききる仕組み

これは、住民の視線に立ってみれば、「便利・簡単になった」、「行政サービスが見える（良く判る）ようになった」、「行政サービスが身近になった」、「安全性が増した」と言える仕組みが必要である。

第２章　「国民 ID 制度」の考え方

本章においては国の「国民 ID 制度」の基本的な考え方について説明する。

2.1　言葉の定義

国の「国民 ID 制度」を理解するためには、そこで用いられている用語を正しく理解する必要がある。ここでは「国民 ID 制度」に登場する用語について説明する。

（利用番号）

行政またはサービス分野ではサービスを効率よく供給・管理するために、異なる個人番号を用いており、この番号を利用番号と呼ぶ。利用番号は１つの行政またはサービス毎に独立した番号を個人に与えている。この結果、個人は複数の異なった利用番号を持つことになる。

（共通番号）

複数の異なる行政分野またはサービス分野で共通して用いる個人番号を共通番号と呼んでいる。この共通番号を使用している行政分野またはサービス分野においては、個人ひとりに対し、１つの番号（共通番号）が与えられる。 複数の異なる行政分野またはサービス分野で１つの番号にて個人が特定されるため、共通番号を使用している機関では、情報の連携が可能となり、手続きの簡素化や連携した機関の複合した行政サービスを受けられることが可能となる。一方、簡単に情報の連携が可能となるため、一旦共通番号が漏えいすれば、共通番号を用いた名寄せや、それで得た個人情報の目的外使用などの危険性も高くなる。

（連携番号）

異なる行政分野またはサービス分野にまたがり、情報連携を可能とする番号を連携番号と呼んでいる。 政府の「社会保障・税に関わる番号制度及び国民 ID 制度における情報連携基盤技術の骨格案」では連携番号を用いることで、今まで分離・独立していた複数の異なる行政分野またはサービス分野のヨコの繋がりを実現させている。

（「見える番号」）

政府の「社会保障・税に関わる番号制度及び国民 ID 制度における情報連携基盤技術の骨格案」には、「見える番号」という表現が出てくる。これは、個人情報の利用が、民－民－官に渡るものを「見える番号」と呼んでいる。即ち、制度上「個人」と「官」の間だけではなく、その間に「民」が関与し、その「番号」を持って個人を識別し、行政サービスが供給される番号を言う。「民」が番号を識別する必要があるため、番号が見える必要がある。例えば、健康保険番号のように、個人が医療機関に番号を提示し、医療行為を受け、その保険

医療費を官が補助する。この一連の医療機関と官の事務処理は健康保険番号にて個人が特定されるため、「見える番号」でなくてはならない。納税番号も、個人－雇用者－税務署、が番号を認識する必要があるため、「見える番号」でなくてはならない。

(「見えない番号」)

政府から発行されている公式資料には「見えない番号」と言う記述はないが、「国民 ID 制度」を検討する上で、検討会などで論議された。これは、「見える番号」に対しての名称であり、個人情報の利用が民－官の利用に限定されるものを見えない番号と呼ぶことにしている。他人に知らせる必要のない番号であり、「見せない」番号と言った意味もある。この番号には、個人情報と密接に紐付いている場合があり、番号自体にも機密性が必要となるケースもある。住民基本台帳番号などもこの番号と言える。

(社会保障と税の共通番号)

今回の１つのメインテーマである「社会保障と税の共通番号」は、利用シーンから、民－民－官であるから、見える番号となるべきである。現在政府で討議されている番号で、共通番号はこの「社会保障と税の共通番号」だけであり、「国民 ID 制度」や「社会保障・税の番号制度」においても共通番号とされているのは「社会保障と税の共通番号」だけであるため、現時点で「共通番号」と言えば「社会保障と税の共通番号」を示すこととなる。しかし、「社会保障と税の共通番号」は見える番号であるため、民はこの共通番号を使ったデータベースを作成できることとなる。個人保護法の観点から利用範囲が制限される必要があり、監視が必要であることから、「社会保障・税番号大綱」や「社会保障・税番号要綱」には法律的に規制と監視することが盛り込まれている。

(国民 ID コード)

「国民 ID コード」とは、「国民 ID 制度」を技術的に検討している「政府・与党社会保障改革検討本部」の傘下の「情報連携基盤技術ワーキンググループ」において、分散された行政分野に存在する個人情報の連携を行うため、個人を特定するために用いる共通の識別子である。このため、行政分野にまたがる情報連携を可能とする、「連携番号」である。今回の政府の「国民 ID 制度」や「社会保障・税の番号制度」検討において、ID コードと言われるものは、この「国民 ID コード」以外にないことから、現時点で「ID コード」は、「国民 ID コード」を示すとして良い。また、この「ID コード」は秘匿される番号であり、個人にも知らせない番号を想定しているため、官－民で用いられる「見えない番号」でではなく、秘匿された連携番号という言い方になる。

(情報提供ネットワークシステム)

国民 ID 制度のシステムは、情報提供ネットワークシステム、マイ・ポータル、および IC カードの 3 つの要素から構成されている。情報提供ネットワークシステムはその中心となる機能であり、行政の効率化と異なる分野の連携した行政サービスを実現するために、またがった行政分野の情報を連携させるための基盤である。連携番号（国民 ID コード）を使って個人の特定と情報の連携を行う。

(マイ・ポータル)

国民 ID 制度のシステムの 1 つの構成要素であり、国民一人ひとりに設けられる「閲覧」、「申請」、「通知」の機能を実現した行政と個人を結ぶ窓口としての役割を持つ。

(IC カード)

国民 ID 制度のシステムの 1 つの構成要素であり、国民一人ひとりに配布され、本人確認（個人認証）のために用いる。 マイ・ポータルにはこの IC カードでのログインとなる。「社会保障・税の番号制度」においては、健康保険証、年金手帳に代わるものとしての利用が考えられており、住民基本台帳カード（住基カード）との統合が検討された。

2.2 社会的制約

政府で「国民 ID 制度」と「社会保障・税の番号制度」を検討する場合に直面した問題は、国民の懸念への対応である。番号制度の実施に伴い、国民の間には、以下のような懸念がありこれを払拭する必要があった。

① 国家管理への懸念

国家により個人の様々な個人情報が「番号」をキーに名寄せ・突合されて一元管理されるのではないかといった懸念[3]

② 個人情報の追跡・突合に対する懸念

「番号」を用いた個人情報の追跡・名寄せ・突合が行われ、

○ 集積・集約された個人情報が外部に漏えいするのではないかといった懸念

○ 集積・集約された個人情報によって、本人が意図しない形の個人像が構築されたり、特定の個人が選別されて差別的に取り扱われたりするのではないかといった懸念[3]

③ 財産的被害への懸念

番号制度の当面の利用範囲が社会保障及び税分野とされていることから、「番号」や個人情報の不正利用等により財産的被害を負うのではないかといった懸念が生じるのではないかと指摘されている。[3]

この問題を解決する手掛かりとなるのは、住民基本台帳ネットワークシステム最高裁判決の事例である。すなわち、番号制度の構築に当たっては、この住民基本台帳ネットワークシステム（「住基ネット」）に係る最高裁合憲判決（最判平成 20 年 3 月 6 日）[8]を十分踏まえる必要がある。[3]

この判決を踏まえれば、番号制度は、以下の 6 項目を満たす必要がある。

① 何人も個人に関する情報をみだりに第三者に開示又は公表されない自由を有すること
② 個人情報を一元的に管理することができる機関又は主体が存在しないこと
③ 管理・利用等が法令等の根拠に基づき、正当な行政目的の範囲内で行われるものであること
④ システム上、情報が容易に漏えいする具体的な危険がないこと
⑤ 目的外利用又は秘密の漏えい等は、懲戒処分又は刑罰をもって禁止されていること
⑥ 第三者機関等の設置により、個人情報の適切な取扱いを担保するための制度的措置を講じていること等の要件を備える必要がある。

政府では、法律・組織・運営の面から「個人情報保護ワーキンググループ」が、システムなどの技術面から「情報連携基盤技術ワーキンググループ」が検討した。

2.3 セクトラルモデルの採用

前節で説明した社会的制約を受けて、「情報連携基盤技術ワーキンググループ」が情報提供ネットワークシステムの技術検討を行った。検討の中心は、前節の①～④であり、①「何人も個人に関する情報をみだりに第三者に開示又は公表されない自由を有すること」と③「管理・利用等が法令等の根拠に基づき、正当な行政目的の範囲内で行われるものであること」については、アクセス者の認証、アクセス権限の設定、およびアクセスログを残すことで解決されている。また、④の「システム上、情報が容易に漏えいする具体的な危険がないこと」については、通信において「番号」を用いず、暗号化された「符号」を用いることや、本人認証などの一般的な通信技術のセキュリティ手法を用いることとしている。

情報提供ネットワークシステムを検討する上で一番の障害となった項目は②の「個人情報を一元的に管理することができる機関又は主体が存在しないこと」である。これは、1 つの情報保有機関が他の情報保有機関と連携するため、他の情報保有機関の情報だけでなく、それを特定するための「番号」を保有できないことになる。この「番号」自体は他の目的で使用される情報であり、個人情報に他ならないためである。つまり、情報連携させるために必要となる連携先の利用者番号と連携元の利用者番号の対照テーブルを情報保有機関は持てないことを意味している。

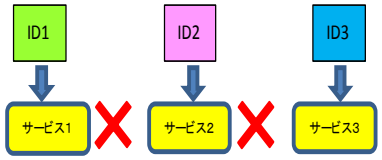
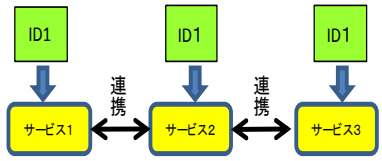
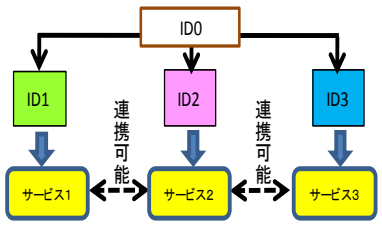
検討の参考にされたのが、諸外国での国民 ID 制度である。ID 管理の方式には、①フラットモデル、②セパレートモデル、③セクトラルモデルの 3 つの方式があり、それぞれフラットモデルはイタリア、米国、韓国で、セパレートモデルは英国、ドイツ、フランスで、セクトラルモデルはオーストリアで採用されている。

フラットモデルは国民が 1 つの ID により複数のサービスを受ける方式であり、国民 1 人に 1 つの ID が与えられることになる。1 つの ID で個人が特定できるため、情報の連携は可能であるが、ID が漏えいすれば全てのサービスに影響を与えることや、簡単に名寄せが出来るため、セキュリティに弱点がある。ここで言う、セキュリティ（情報セキュリティ）とは、「正当な権利を持つ個人や組織が、情報や情報システムを意図通りに制御できること」である。情報セキュリティマネージメントシステムの国際標準 ISO/IEC17799（2007 年に ISO/IEC 27002:2005 と改称)には、「情報の機密性、完全性および可用性を維持すること」と定義されている[9]。また、通信経路においては、送信者から送信相手までの通信経路において安全性を担保し、データの盗聴や改ざん、ネットワークへの侵入や妨害から守ることを意味するものである[10]。

セパレートモデルは国民がサービス毎に別々の ID を使用するものであり、各々のサービスが独立したものとなっている。このため、サービス毎のセキュリティは保たれており、ID の漏えいについても対象となるサービスだけの被害となる。しかし、サービスが独立しているため、情報連携が出来なく、サービスの統合も出来ないためサービスを提供する側の業務が重複する場合が多い。国民にとっても複数の ID の管理が必要であり、煩雑となってしまう。現在の日本の ID 管理は複数の ID（複数の利用者番号）を使ったこの方式である。

セクトラルモデルはオーストリアで採用されている ID 管理方式であり、1 つの ID からサービス毎の ID を生成し、サービスを提供する方式である。各々のサービスは独立しているため、セパレートモデルの様にセキュリティに優れている。また、1 つの ID からサービス毎の ID を生成しているため、フラットモデルほど単純ではないが、サービス毎の連携も可能となっている。各々の ID 管理方式については第 5 章に詳細に説明する。

表２－１　ID の管理方式の比較

方式	特徴	モデル	特長と課題	使用国
セパレートモデル	・サービス毎に異なるID ・各サービスが独立		（長所） ・サービス毎のセキュリティが独立している （課題） ・ID間に関連性がないので連携が取れない。 ・利用者のID管理が煩雑	日本 ドイツ
フラットモデル	・1人に対して1つのID ・サービス全て共通のID		（長所） ・利用者のID管理が容易 （課題） ・IDが流出すると全ての情報が流出する。 ・IDの流出で全てのシステムがダウンする危険性	シンガポール 韓国 エストニア アメリカ
セクトラルモデル	・サービス毎に異なるID ・サービス間の連携が可能		（長所） ・直接紐づけが出来ないためIDの流出した場合もそのIDのサービスの問題に留まる ・サービスの連携も可能 （課題） ・システムが複雑	オーストリア

政府の情報提供ネットワークシステムの技術検討では、日本のようなセパレートモデルの行政サービスを、どのようにすれば相互に連携させることが出来るかが検討された。この様なセパレートモデルを連携させるための手法は「シングルサインオン（SSO）」と呼ばれており、様々な方法が報告されている。

しかし、一般的に使用されている手法ではシステムのいずれかの部分に ID の連携を行うため、対応する ID 同士を紐づけるための照合テーブルを用意する必要がある。これは、②の「個人情報を一元的に管理することができる機関又は主体が存在しないこと」に反することになる。このように、連携先（サービス）の利用者番号（ID）と連携元（サービス）の利用者番号（ID）の対照テーブルを情報保有機関（連携先や連携元）は持てないため、これに抵触しない方式としてセクトラルモデルの採用が決定された。つまり、1 つの連携させるための連携 ID を用意し、その連携 ID から連携先の利用番号（ID）を発生させる方法とした。ただ、連携先の利用番号（ID）は既に存在することから、連携 ID から発生したコードと連携先の利用番号（ID）を紐づける仕組みは別に必要となる。この方式によれば、発生したコードは保存しないため、②の「個人情報を一元的に管理することができる機関又は主体が存在しないこと」を実現できることになる。

2.4　国民 ID 制度

国民 ID 制度とは、国民に ID を付番することで、国民平等に充実した社会保障などの行政サービスを実現し、手続きを簡略化するための仕組みである。政府では、行政機関における情報共有の推進と、国民が自己の情報を確認できる仕組みの整備を目的とした“電子行政の共通基盤”として位置付けられており、以下の 3 つの目的を掲げている。

①各種行政手続きのオンライン化/ワンストップ化

第一の目的は、「各省庁間・地方自治体間のデータ連携を可能とする」ことである。国民 ID によって、行政手続きの申請者がどこの誰かを確認できれば、行政機関同士で情報を共有し、類似の書類の提出を何度も求める必要がなくなることである。

国民（利用者）としては、重複した手続きが無くなり、申請のための時間や手間が省け、手続きにかかる負担が少なくなることになる。

例えば、引っ越しでは、現状の転出地の自治体と転入地の自治体や役所を訪問して住所変更のため、類似の書類や証明書を取得し、届出を行うようなことが、パソコン上からワンストップで手続きが行えるようになる。［12］

②行政機関が管理している自己情報の確認

第二の目的は、「行政が保有する自己に関する情報について、国民が内容を確認できる仕組みを整備する」ことである。

国民 ID により、行政機関の保有している自分の情報を閲覧できることになり、自分の情報を確認し、間違いがあれば修正を求めることが出来るようになる。また、誰がいつ自分の情報にアクセスしたかを監視することも出来、正当な目的で自分の情報が使用されていることを知ることが出来る。これにより、行政の透明化を行うばかりか、国民の行政サービスに対する関心を高める効果にもなる。[12]

③民間利用などへの拡大

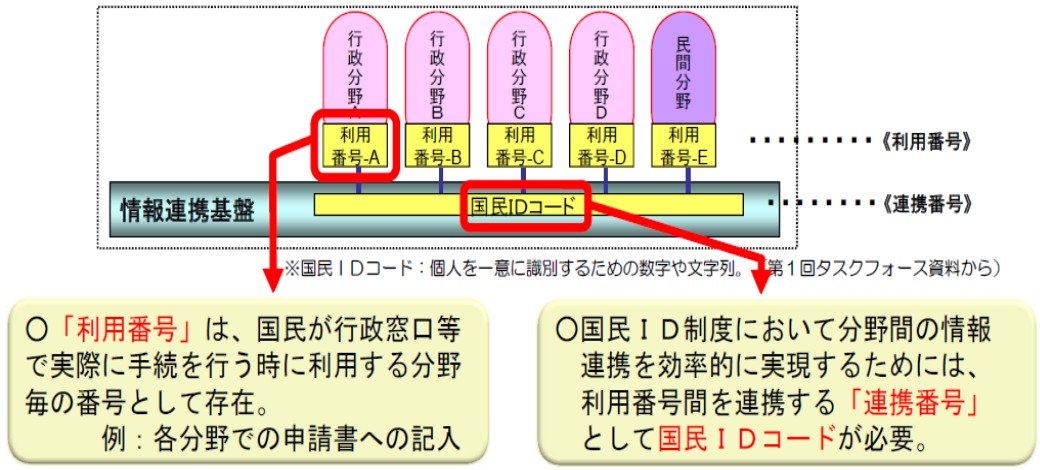
第三の目的は民間利用への拡大である。将来、国民 ID を公共事業者や一般企業と連携することにより、国民の生活をより安全で便利なものになる。

例えば、国民 ID と公共機関で使用している個人の ID とを連携させることで、引っ越し時のガスや電気の変更手続きが自治体への転出届（転入届）にて可能となり、引っ越したその日に、引っ越し先で直ぐにガスや電気が使用できることになる。また、国民 ID 制度では、法人にも「企業コード」を付番することとなっており、雇用の手続きなどのワンストップサービスにも繋がる。[12]

このような目的の国民 ID 制度のシステムには、大きく 2 つの機能、つまり行政機関（将来は公共機関や一般企業）が個別に使用している個人を識別する ID を連携させることと、国民がそれら機関の保有している個人情報を閲覧し、情報に誤りがある場合、この情報の修正が可能とさせることを実現する技術的な仕組みと法律上の仕組みが要求されることとなる。また、個人情報を扱うため、その情報の取り扱いにはセキュリティポリシーが不可欠であり、監視機能や法による罰則を設ける必要がある。

本考察では、技術的仕組みについてのみ説明することになる。法律上の仕組みについては、参照文献にある「社会保障・税番号要綱」[2]や「社会保障・税番号大綱」[3]を参照してもらいたい。

2 つの機能のうち、ID を連携させる機能については、情報提供ネットワークシステムが行い、個人情報を閲覧する機能については、マイ・ポータルが行うことになる。また、国民がマイ・ポータルにログインするためには、アクセスした人が本当に当人であるかを認証するために、IC カードを使った個人認証を利用することにしている。2.3 節で説明したように、政府では、社会的制約から ID を連携させるためにセクトラルモデルの採用を決定した。その連携のために情報提供ネットワークシステムの中で用いられる連携 ID がすなわち、国民 ID との位置付けに当たり、「国民 ID コード」と呼ばれている。図２－１に国民 ID コードのイメージを示す。



（出典：内閣官房・情報連携基盤技術 WG（第１回）議事録、資料 7「国民 ID 制度に関するこれまでの検討経緯」）

（情報連携基盤：情報提供ネットワークシステムに改称）

図２－１　国民 ID コードのイメージ

「国民 ID コード」は誕生と同時に、国民一人ひとりユニークな番号が付番されるが、諸外国で利用されている国民 ID 番号のように、行政サービスなどの申請時に国民が自分の番号を認識し記入して国民の個人識別に利用されるものではなく、あくまで、情報連携だけのために

個人を認識するための番号として利用されるものとなっている。このため、国民は自分の付番された「国民 ID コード」を知ることが出来なくなっている。これは、九州大学で開発した社会情報基盤 VRICS と同じセクトラルモデルの採用により実現しており、セキュリティの面からも評価できる。このように、今回発表された「国民 ID 制度」は、行政サービスの基本的な構造を示したものであり、全ての行政サービスはこの国民 ID 制度のシステム上もしくは、連携するものとなる。また、将来目指しているところは、民間企業とのサービス連携であることから、この「国民 ID 制度」の仕組みは今後の企業の情報基盤の構築にも影響を与えることとなる。

第３章　「国民 ID 制度」と「社会保障・税の番号制度」との関係

本章では、政府で検討されている 2 つの番号制度である「国民 ID 制度」と「社会保障・税の番号制度」の関係について説明する。

3.1　「社会保障・税の番号制度」

前章において「国民 ID 制度」について説明した。本節では「社会保障・税の番号制度」について説明する。

第１章で説明したように、現在の社会保障制度は様々な問題点を抱えている。中でも緊迫した課題は人口問題である。直面している高齢化社会においては、社会保障費の増大は避けられない事実であり、その一方その費用を支える人口は減少し、現状での税収入では支えきれないことは明白である。このためには、社会保障の質をそのままにし、それにかかる経費を抑えるような効率化が不可欠であることは言うまでもなく、税収入の増額を検討する必要があった。現在の社会保障制度では、年金、健康保険、雇用保険、介護保険など様々な個別の番号（ID）を使用しており、税分野では納税を管理する番号を用いられている。

社会保障と税は表裏の関係であり、公平な社会保障を実現し、その財源を公平な税とすることが求められる。政府・与党社会保障改革検討本部においては、社会保障と税をまとめて考える必要があり、「社会保障と税の一体改革」が打ち出された。

現在の社会保障はその受給者の所得と密接に関係している。日本国憲法で「第 25 条　すべて国民は、健康で文化的な最低限度の生活を営む権利を有する。国は、すべての生活部面について、社会福祉、社会保障、及び公衆衛生の向上及び増進に努めなければならない。」とされており、社会保障の基本を示したもので、国民の生存権を保障するものである。このように国民の所得に関わらず、最低の生活を保障するものであり、現在の社会保障制度では、多くの保護が必要な低所得者に対しては高所得者より保護を厚くする必要がある。

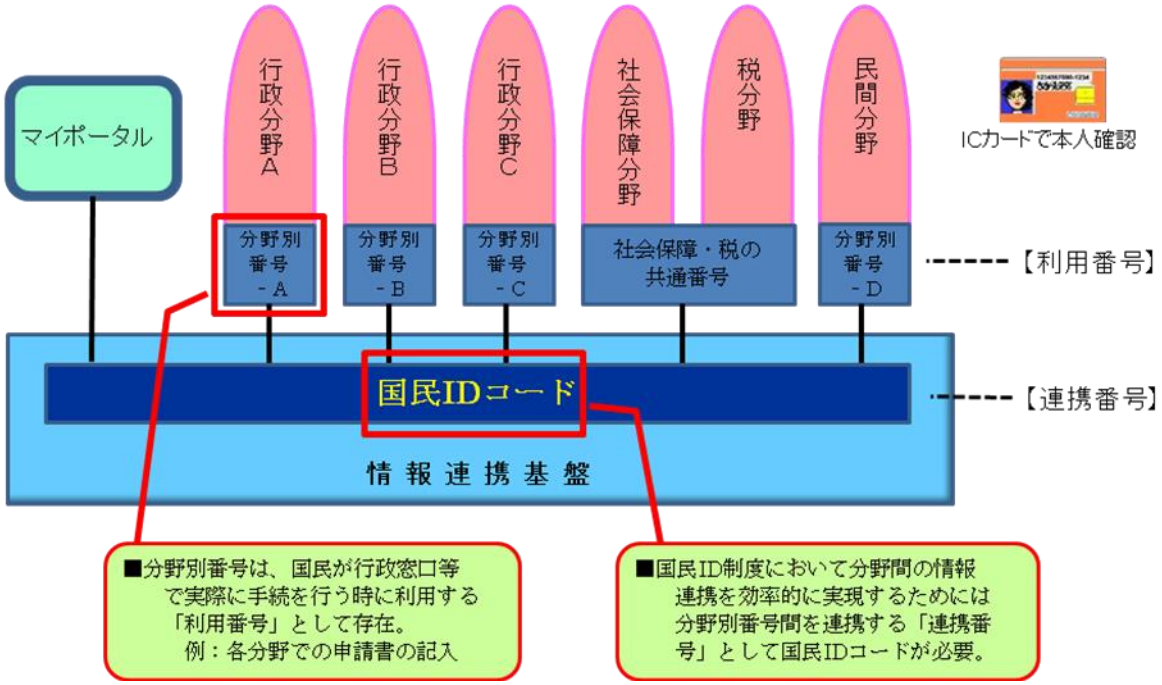
この個人の所得を知るためには、個人の納税を把握することで可能となる。また、保護すべき低所得者には減税などの対策を施すためにも、保護の対象となる人を特定する必要もある。このため、政府は社会保障と税を 1 つの制度と考え、1 つの統一した共通番号で個人を特定することで公平な社会保障と税の制度の実現を目指している。この共通番号は、例えば、税の分野で所得税を考えた場合、個人－企業－税務署、と民－民－官、に渡る番号であり、「見える番号」である必要がある。

社会保障の分野では、医療保険を考えてみれば、個人－医療機関－支払機関：保険者（国または保険組合）、となり民－民－官となる。「見える番号」は番号を知らす（見せる）ことにおいて、そのサービスが施されることとなる。しかし、「見える番号」については、一般的に人目に曝されるわけであるから、そのセキュリティは低くなり、法や罰則でのセキュリティ

確保が必要となる一方、社会保障で用いられる医療に関する情報などでは、機微情報が多く含まれることになる。この機微情報へのアクセスに「見える番号」を用いることはセキュリティ上好ましくない。このため、厚生労働省は「社会保障・税の共通番号」とは別に、医療の機微情報のみを扱う「保健医療番号」の新設を行った。この「保健医療番号」は「見えない番号」という位置付けになる。このように、社会保障分野と税の分野で「社会保障・税の共通番号」を共通の番号として使用することで、情報に連携や効率を上げようとする制度が、「社会保障・税の番号制度」と言われるものである。

3.2　「国民 ID 制度」における「社会保障・税の番号制度」

2.4 節で「国民 ID 制度」について、3.1 節で「社会保障・税の番号制度」についてそれぞれ説明した。2.4 節では、「国民 ID 制度」は、“電子行政の共通基盤”として位置付けられており、分野別の行政サービスで使用されている利用番号を連携させるために使用する連携基盤と説明した。これをイメージ図で表すと図３－１となる。



（出典：内閣官房・情報連携基盤技術 WG（第１回）議事録、資料７「国民 ID 制度に関するこれまでの検討経緯」より抜粋編集）

図３－１「国民 ID 制度」と「社会保障・税の共通番号」

情報提供ネットワークシステムは連携番号である「国民 ID コード」を用い、各行政分野で利用されている「利用番号」が同一人物のものであることを結びつけることで、各行政分野間の個人情報の連携を行う仕組みであり、行政システムの基盤である。この全体の仕組みを「国

民 ID 制度」としている。また、マイ・ポータルは情報提供ネットワークシステムから見れば、１つのアプリケーションであり、各々の行政サービスと同等の位置付けとなっている。ここで、「社会保障・税の共通番号」は、社会保障分野と税分野に共通に使われる番号であり、この部分を取り出して、「社会保障・税の番号制度」と言われる。全体の仕組みが「国民 ID 制度」であり、その一部が「社会保障・税の番号制度」と言える。

第４章　「国民 ID 制度」と「社会保障・税の番号制度」システム

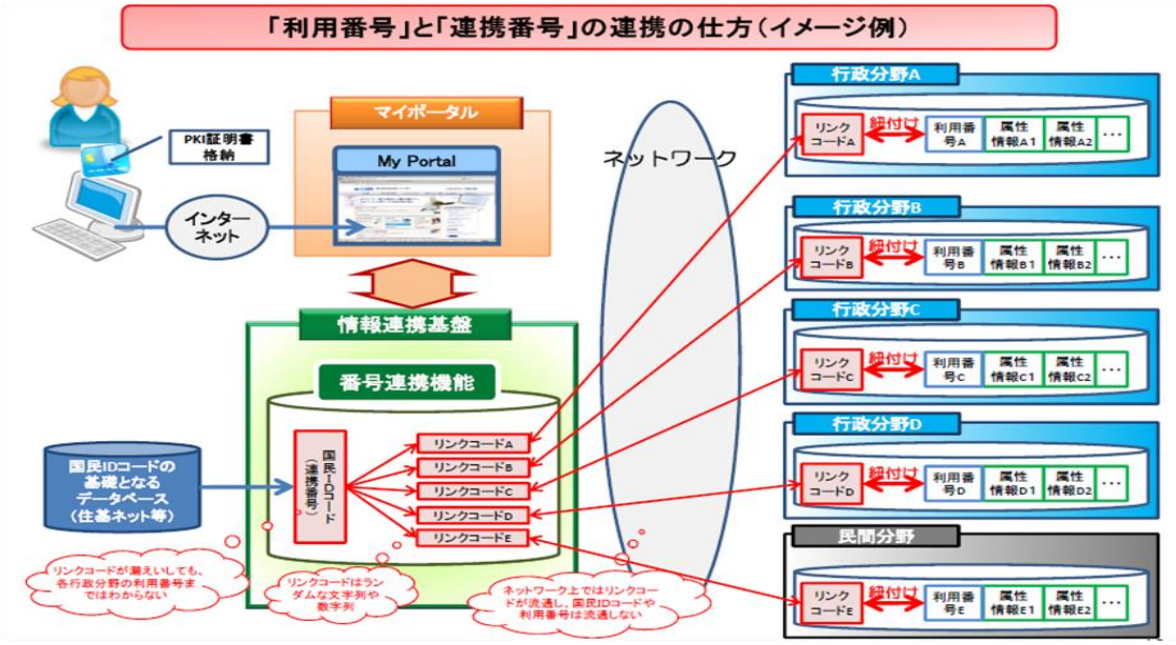
本章においては、「国民 ID 制度」を構成している「情報提供ネットワークシステム」、「マイ・ポータル」、および「IC カード」の技術的な仕組みについて説明する。

4.1　情報提供ネットワークシステム（旧称：情報連携基盤）

4.1.1　情報提供ネットワークシステムの構造

「国民 ID 制度」で中心的な役割を演じるのが「情報提供ネットワークシステム」である。

2.2 節、2.3 節で説明した様に、社会的制約により、情報提供ネットワークシステムはセクトラルモデルの考え方で設計される。基本的なイメージを図４－１に示す。



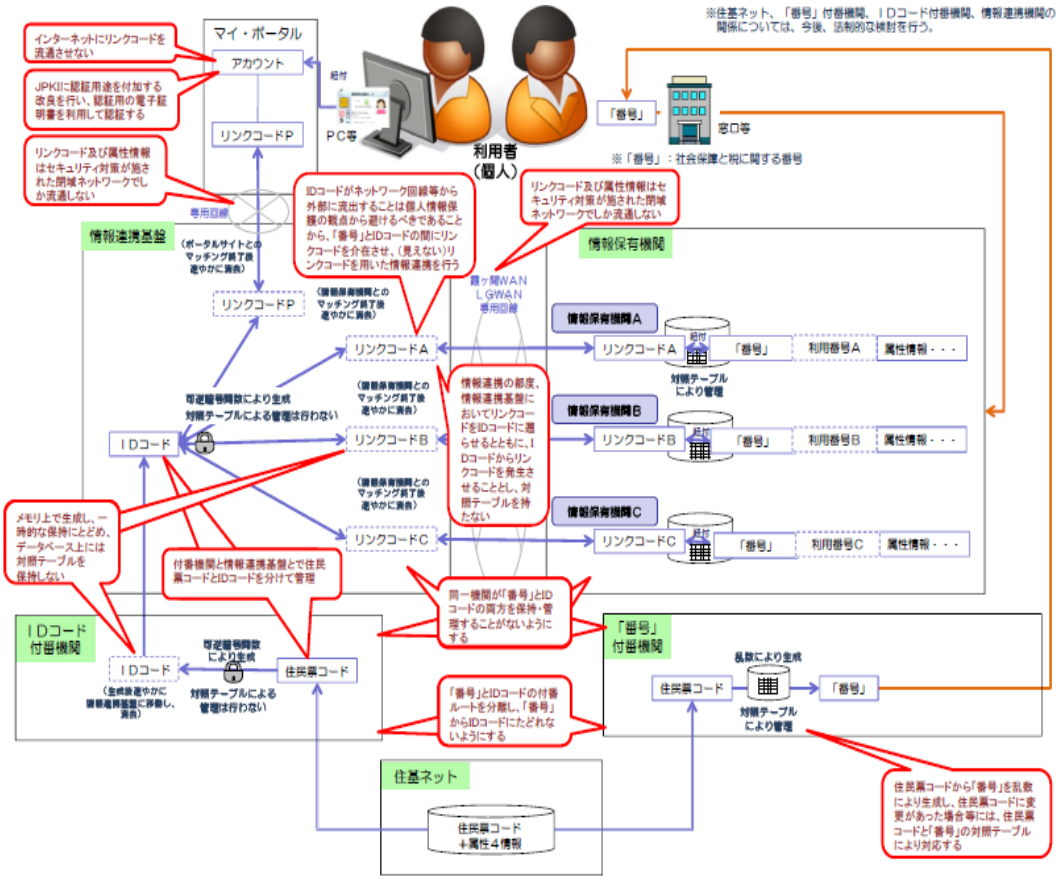
（出典：内閣官房・高度情報通信ネットワーク社会推進戦略本部・電子行政に関する TF 第８回参考資料）

図４－１　情報提供ネットワークシステムにおける番号連携のイメージ

図４－１で示した番号連携のイメージ図において、情報提供ネットワークシステムの動作を説明する。構成としては、主に情報提供ネットワークシステム、マイ・ポータル、および情報保有機関である各行政分野から成る。情報提供ネットワークシステムが情報の連携行うための中心的な役割を果たす。マイ・ポータルは情報提供ネットワークシステムに繋がっており、インターネットで住民のパソコンからの情報入出力の窓口となる。情報保有機関は、それぞれ行政分野ごとに独立しており、ネットワークで情報提供ネットワークシステムに繋がる。情報保有機関には将来の展開を考え、民間分野も含まれている。情報提供ネットワークシステムでは

連携番号として国民全員に付番した国民 ID コードから、情報保有機関ごとに異なるリンクコードを発生させる。各情報機関に対応したリンクコードは事前に情報保有機関に連絡されており、各々の情報保有機関では、情報保有機関で個々に使用しているいる利用番号とリンクコードの対照表を作成し、個人が紐付けされることとなる。情報提供ネットワークシステムで使用される国民 ID コードは、国民を一意に指定できる番号より生成されることとしている。

図４－１の情報提供ネットワークシステムにおける番号連携のイメージをさらに具体的に示せば、図４－２となる。



（出典：内閣官房・情報連携基盤技術 WG（第２回）議事録、資料２「番号制度　番号連携イメージ」）

図４－２　情報提供ネットワークシステムにおける番号連携の具体例

システムの全体の構成は、以下のようになっている。

① ID コード付番機関で、住民票コードより可逆暗号関数により、「ID コード」を生成する。

② この生成した「ID コード」は付番機関には残さず、情報提供ネットワークシステムに登録される。

③ 情報基盤では、登録された「ID コード」から、可逆暗号関数により「リンクコード」を生成

し、各情報保有機関に配布する。また、「リンクコード」は生成された後、一時的な保持に留められ、情報提供ネットワークシステムには残さない。

④ これらのいずれの番号の発生においても可逆暗号化で行われているが、情報保有機関から「ID コード」、さらに住民票コードに遡ることは不可能としている。

⑤ ここで「ID コード」と「リンクコード」は人が知りえない状態で、社会情報基盤と霞ヶ関 WAN・LGWAN・専用回線に限定されたネットワーク上を流通するものとなる。

⑥ 一方、「社会保障・税の共通番号」は、番号付番機関で住民票コードから、乱数により生成され、対照テーブルにより番号付番機関で管理されることになる。また、この対照テーブルは番号付番機関のみで利用され、外に出ていくことはない。

⑦ 番号付番機関で生成された「番号（社会保障・税の共通番号を含む）」は、政府窓口を通し、個人に伝えられるとともに、その「番号」を利用する情報保有機関に登録される。

⑧ 「番号」は可視化され、民間の事業者、個人、行政などで利用者を識別する符号として用いられる。また、「番号」は情報保有機関の情報システム内やその他ネットワーク上で流通するものとなる。

⑨ 以上の様な「住民票コード」、「ID コード」、「リンクコード」、および「番号」が各機関にて管理され構造を持つため、国民を一意に識別できる情報基盤を形成しながら、個人情報を一元的に管理することができる機関又は主体が存在しない仕組みを実現している。

図４－３に、この情報提供ネットワークシステムを使った場合の連携方法を図示する。

連携方法は、「住民票コード」から生成された「見える番号」である「番号」は窓口を通して、国民に配布され、これに関係する情報保有機関に連絡される。国民やサービスを提供する団体、また情報機関の住民窓口では、この「番号」を基に事務処理がなされることになる。例えば、情報保有機関 A が情報保有機関 B の保有している個人情報を入手し、情報連携する場合は以下のような手順となる。

① 情報保有機関 A において、連携させたい個人の「番号 A」から、その個人に対応する「リンクコード A」を対照テーブルから抽出。

② 情報保有機関 A は、対象としている個人の「リンクコード A」と情報の提供要求相手である情報保有機関 B を指定し、情報提供ネットワークシステムに送る。

③ 情報提供ネットワークシステムでは、情報保有機関 A から送られてきた「リンクコード A」を「国民 ID コード」に逆変換し、情報提供要求相手である情報保有機関 B に対応した個人の「リンクコード B」を発生させる。

④ 情報提供ネットワークシステムでは、情報保有機関 B に対し、「リンクコード B」と情報請求元の情報保有機関 A からの請求であることを投げる。

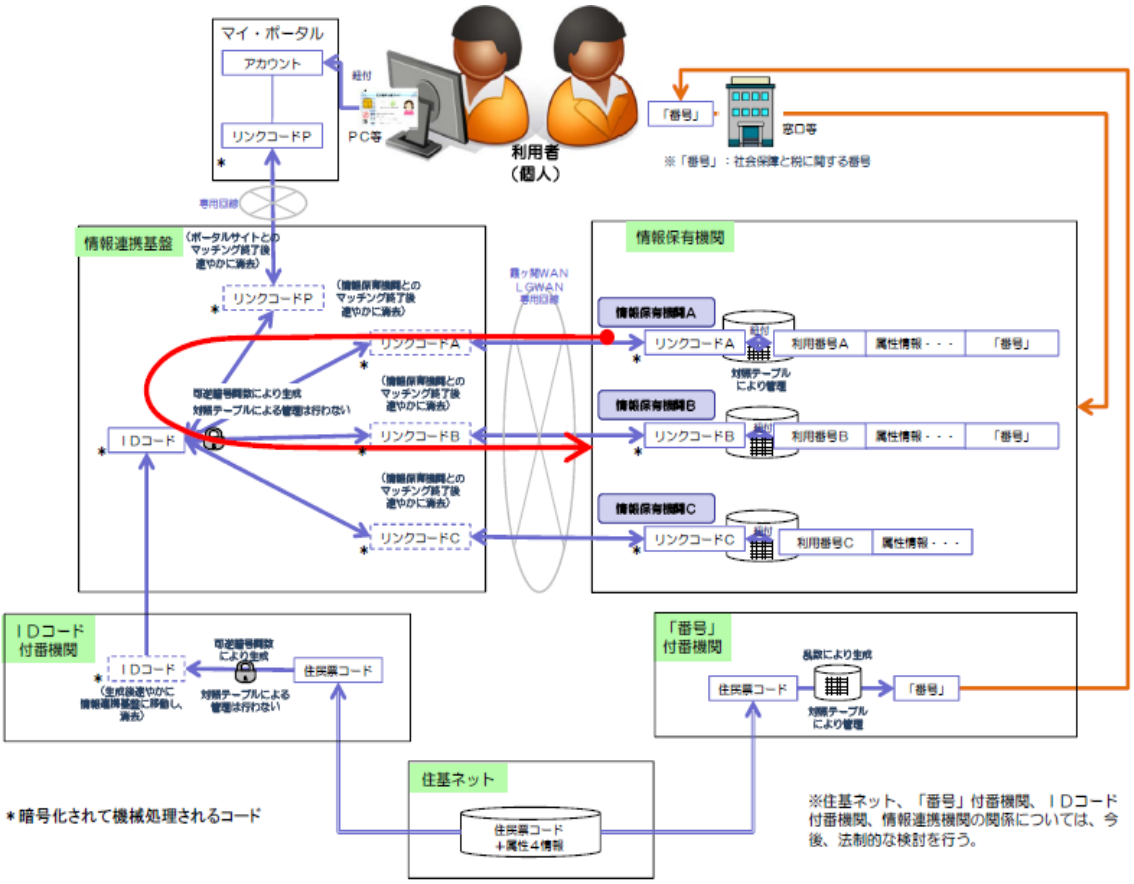
⑤ 情報保有機関 B では、情報提供ネットワークシステムから来た「リンクコード B」を、対

照テーブルを用いて、情報保有機関Ｂで個人特定のため使用している「番号Ｂ」を抽出。

⑥　情報保有機関Ｂにおいて、「番号Ｂ」で指定された個人データを情報保有機関Ａに送る。

⑦　情報提供ネットワークシステムでは、情報保有機関Ａから得た「リンクコードＡ」や、発生した「リンクコードＢ」は消去され、一連のデータ連携のログだけを残すこととする。

⑧　以上のような手続きにより、情報保有機関Ａの個人と情報保有機関Ｂの個人が同一の人物であると特定される仕組みである。



（出典：内閣官房、社会保障・税に関わる番号制度に関する実務検討会（第８回）　議事次第、資料 2-2「番号制度　番号連携イメージ」）

図４－３　連携方法のイメージ

情報提供ネットワークシステムの機能としては「情報連携」と「情報収集」の２つが示されている。

情報連携とは、個人の属性情報を含むデータベースを有する情報保有機関が、他の情報保有機関が有するデータベースのうち個人の特定情報を必要とする際に、本人を特定して新たに情報を取得することと定義している。

情報連携の例としては、住民が転入した際、転入した自治体が介護保険料等を算出する目的

で前住所地での個人の所得情報を取得することなどが挙げられる。

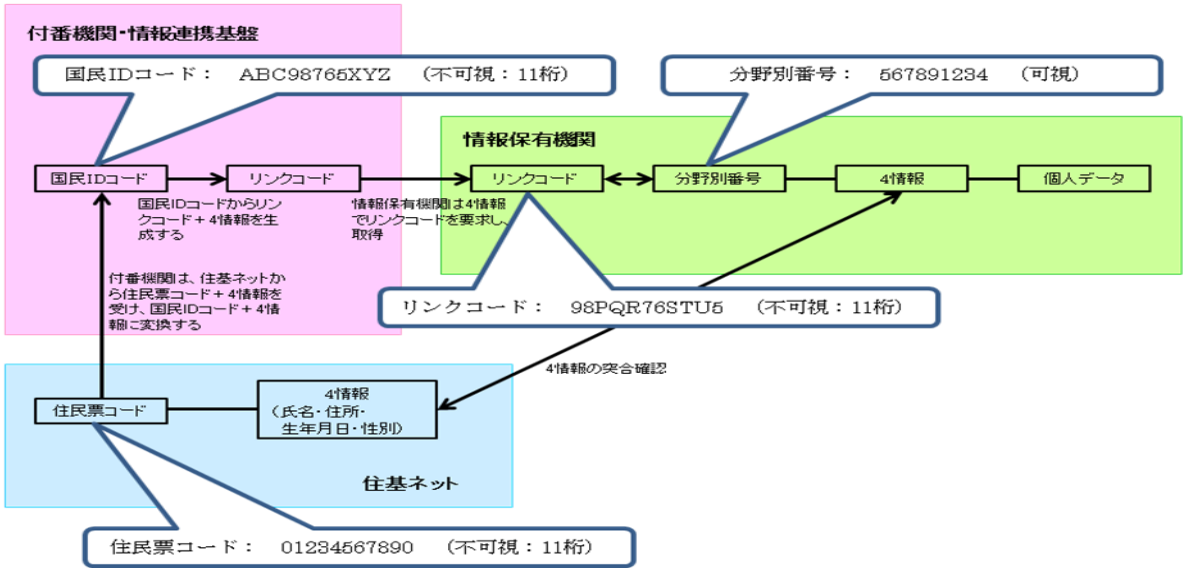
一方、情報収集とは、情報保有機関が、自らのデータベースを構築するため、情報保有機関固有の権限を行使し、個人または法人から新たに情報を取得することと定義している。

この情報収集の例としては、税務当局等への法令等に基づき、民間事業者や給与支払者としての情報保有機関（行政機関、日本年金機構等）が、源泉徴収票など給与支払情報を提出することが挙げられる。また、他の情報収集の例として、税務当局等へ所得税の確定申告書や住民税の申告書など所得情報等を申告することがあげられる。所得税と住民税においては、所得税の確定申告書の提出が住民税の申告書の提出とみなされ、市町村による所得税に関する情報の閲覧が法定されているためである。さらに、法令等に基づき、介護保険料等の年金からの特別徴収のために行われる年金保険者から市町村への情報提供（通知）も、情報収集にあたる。

4.1.2　コード生成と取得

さらに、各々のコード生成方法と情報保有機関でのリンクコードの取得方法について詳しく述べる。

図４－４に各々のコードの生成方法と取得方法を示す。



（出典：内閣官房・個人情報保護・情報連携基盤技術WG合同座長・座長代理会合議事次第、資料３「概念図」）

図４－４　コードの生成方法と取得方法

「住民票コード」は住基ネットの中で管理されており、11 桁の数字で表されている。付番機関では、住基ネットから「住民票コード」と住民基本台帳の４情報（氏名・住所・生年月日・性別：以下４情報と言う）を受け、可逆暗号にて 11 桁の「国民 ID コード」を生成し、 ４情報と共に情報提供ネットワークシステムに送り、情報提供ネットワークシステムで保管する。

情報保有機関は、情報提供ネットワークシステムに対し、4 情報にて分野別番号に対応する

個人のリンクコードを要求する。

情報提供ネットワークシステムでは、4 情報から「国民 ID コード」を割り出し、可逆暗号にて、11 桁の「リンクコード」を生成する。生成された「リンクコード」は情報保有機関に送られる。情報保有機関では、取得したリンクコードと分野別番号を紐づけ、以後の情報連携を行う際に必要な対照テーブルを作成する。

4.1.3　データ連携方法

情報提供ネットワークシステムでのデータの連携方法について説明する。

情報提供ネットワークシステムにおいて実際のデータを扱うには、ゲートウェイ方式とアクセストークン方式の 2 通りの方法が考えられる。ゲートウェイ方式は、情報提供ネットワークシステムにデータ送受信機能を実装し、情報連携に係る全てのデータ送受信を、情報提供ネットワークシステムを経由して行う方式情報である。

一方、アクセストークン方式は、情報連携に係るデータ送受信を、情報提供ネットワークシステムを介することなく、情報保有機関間で直接行う方式である。

この 2 つの方式を比べると、ゲートウェイ方式では、情報連携に係るデータの送受信が情報提供ネットワークシステムに集中することから、送受信を制御するサーバにボトルネックが発生し、情報連携が円滑に行われない可能性が懸念されるため、これを解消するためには高性能なサーバが必要となることから、アクセストークン方式に比し情報提供ネットワークシステムの構築費用は高額となる。一方、アクセストークン方式では、情報提供ネットワークシステムの負荷が小さく、最小限の機器構成で良いが、情報保有機関側のデータ送受信機能の構築費はゲートウェイ方式に比し高額になる。

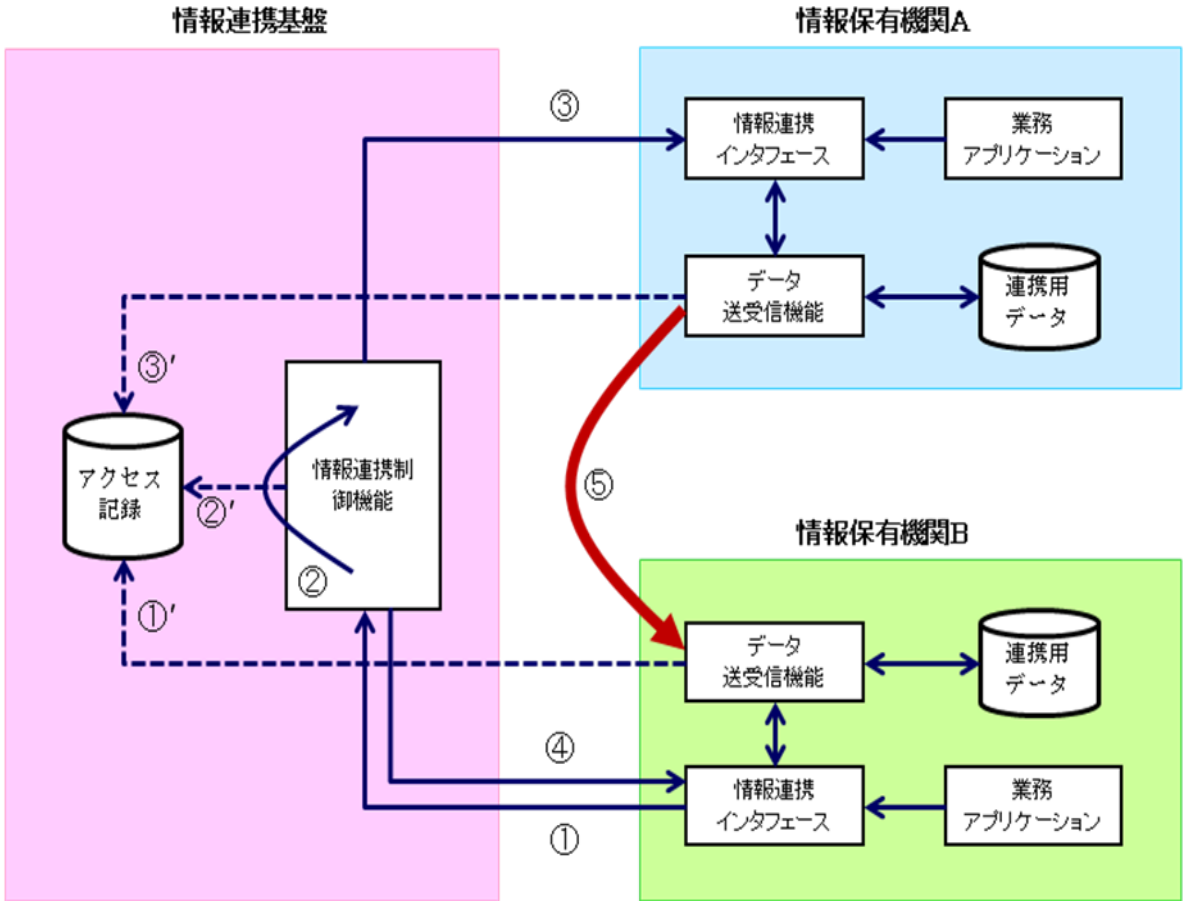
また、稼働の安定性・運用性から考えれば、ゲートウェイ方式では、情報連携に係るデータの送受信が情報提供ネットワークシステムに集中することから、送受信を制御するサーバにボトルネックが発生し、情報連携が円滑に行われない可能性が懸念される。情報提供ネットワークシステムに接続される全ての情報保有機関のシステム運用時間及び稼働状況に応じた送受信制御を行う必要がある。一方、アクセストークン方式では、情報提供ネットワークシステムの負荷が小さく、最小限の機器構成で良いため、障害等の発生契機もゲートウェイ方式に比し少ない。情報保有機関側にのみデータ送受信機能を実装するため、各情報保有機関がネットワーク上の連携先に関する宛先情報及びシステム稼働状況等を把握する必要があるため、運用が複雑になる可能性がある。

さらに、障害発生時の影響を比較すれば、ゲートウェイ方式では、情報提供ネットワークシステムが障害等で機能不全に陥った際は情報提供ネットワークシステムに接続される全ての情報保有機関に影響を及ぼすことになる。一方、アクセストークン方式では、情報提供ネットワークシステムが障害等で機能不全に陥った際もデータ送受信機能は情報保有機関側にあることから、臨時的・限定的な代替措置が容易である。

最後に、個人情報保護の観点からは、ゲートウェイ方式では、情報連携に係る証跡が集約するため可監査性に優れる。しかし、情報連携に係る個人情報が一時的に情報提供ネットワークシステムに留まるため、個人情報が集約しうるとの指摘もある。アクセストークン方式では、情報連携に係る証跡が情報提供ネットワークシステムと情報保有機関に分散するため可監査性に解決すべき問題があるだけでなく、情報連携に係る行政機関の監視が不十分との指摘がある。

現状結果は出ていないが、ゲートウェイ方式とアクセストークン方式の比較から、コストパフォーマンスに優れ、稼働の安定性に優れ、障害発生時の影響が少ないアクセストークン方式の採用が有力と言える。

図４－５にアクセストークン方式の動作を図示する。



（出典：内閣官房・情報連携基盤技術 WG（第５回）議事録、資料 3-3「データ送受信方式検討表」より抜粋編集）

図４－５　アクセストークン方式

アクセストークン方式では、情報提供ネットワークシステムで認証の連携を行い情報連携の制御は行うものの、情報連携に係るデータ送受信を、情報提供ネットワークシステムを介することなく、情報保有機関間で直接行うこととなる。

各々の情報保有機関は、連携用データ、業務アプリケーション、情報連携インタフェース、およびデータ送受信機能から構成される。また、情報提供ネットワークシステムは大きく分け、情報連携を行う情報連携制御機能と情報連携のアクセスログを蓄積するアクセス記録の 2 つから構成される。情報保有機関 B が情報保有機関 A のデータを取得するデータ連携の流れは以下のようになる。

① 情報保有機関 B において、業務アプリケーションが情報保有機関 A の個人データが必要と判断。業務アプリケーションは情報連携インタフェースに対し、リンクコード B を用いて、情報保有機関 A の個人情報を要求。

② 情報提供ネットワークシステムの連携制御機能では、情報保有機関 B から来たリンクコード B を情報保有機関 A に対応したリンクコード A に変換する。さらにこのリクエストに応じたトークンを作成する。

③ 連携制御機能は、リンクコード A とアクセストークンを情報保有機関 A に通知する。情報保有機関 A ではリンクコード A に対応する個人データを用意する。

④ 情報提供ネットワークシステムの連携制御機能は、情報保有機関 A へのリンクコード A とアクセストークンの通知と同時に、情報保有機関 B にアクセストークンと連携開始許可を通知する。

⑤ 情報保有機関 B では、情報保有機関 A に対しアクセストークンにて情報を要求し、情報保有機関 A は準備した個人データを情報保有機関 B に送る。

各々のデータアクセスの記録①′、②′、および③′はログとして情報提供ネットワークシステムのアクセス記録に蓄積される。

4.1.4 情報提供ネットワークシステムの制限と手続き

以下のような考えから情報提供ネットワークシステムで扱うべき情報と手続きを制限している。

① 情報連携を実施する際には、本人を特定する何らかの番号を介在して新たに情報を取得することになる。

② このような情報連携は、法定手続きであり、本人からの申請・申告等の何らかのイベント発生に基づく情報連携業務である。

③ 例えば転居の場合、運転免許証やパスポート、さらには所有している自動車等の登録等、何処までの手続きをバックオフィス連携で行うかは、本人の意向確認が必要と考えられる。

④ イベント発生に基づく一連の手続き BPF（Business Process Flow）は、情報提供ネットワークシステムの番号連携機能を用いることになるため、その流れと根拠を明確にするため、イベント発生事象の特定、手続きの種別およびそのシーケンス、手続きの流れ

と連携される情報の種別（情報実体を含まない）、進行状況等をコーディングし、認められた手続きのみが連携基盤にアクセスすることを可能とする。

このため、情報提供ネットワークシステムが扱う情報は、法定業務と言う制限になる。自治体が独自で行う住民サービスは法定業務には含まれないものも多くあり、また社会保障で取り扱われる医療情報の連携なども法定業務ではないことにより、情報提供ネットワークシステムにて情報連携できないこととなる。また反面、情報提供ネットワークシステムが扱う情報が法定業務とすることで、セキュリティの面からも監視が容易となり、業務手続き BPF（Business Process Flow）を情報提供ネットワークシステムに登録し実装することで、業務手順の標準化が可能となる。

また、「番号」を用いる情報収集等については、透明性を確保するためにログを残すことを原則としている。このことは、情報保有機関からはイベントを指定すれば、情報提供ネットワークシステムに書かれた BPF に従い、情報アクセスが行われることを意味する。すなわち、情報保有機関が情報提供ネットワークシステムに知らせるべき情報は、リンクコード、相手先の情報保有機関、およびイベントの種別となる。

4.2　マイ・ポータル

マイ・ポータルは国民 ID 制度の 1 つの重要な構成要素であると共に、1 つの情報保有機関との位置付けにある。マイ・ポータルは国民全員に用意されており、記録されたログの閲覧・確認、情報保有機関からの本人への問い合わせ、情報保有機関からのお知らせや通知等の受け取り、本人からの申請申告等を可能としている。ここで、マイ・ポータルからの閲覧・確認・申請の要求は法定手続きとしての位置付けにあるとされている。このため、マイ・ポータルは情報提供ネットワークシステムを利用し情報を取得できることとなる。同様の観点から、マイ・ポータルの個人フォルダーには、電子メールのアドレスを付けないものとしている。

また、利便性を確保するため、インターネットからのアクセスを可能としている。さらに、本人確認を確実に行うため、JPKI（公的個人認証サービス：2004 年 1 月 29 日より開始された個人向けの本人認証のための電子証明書の発行サービスであり、政府機関や各地方公共団体への各種届出・申請などに利用)による認証機能の利用を基本としているが、利便性の更なる向上を図るため、マイ・ポータルが取り扱う個人情報の性質に応じて、アクセス手段の多様化を検討するとしている［13］。付加的なアクセス手段については、そのセキュリティレベルとアクセスする個人情報の機微性を勘案した適切なアクセスコントロールを行うこととしており、柔軟的なアクセスを目指している。

マイ・ポータルの機能を実現するための要素としては、以下の 2 つが挙げられている。

① 情報保有機関が本人に対しマイ・ポータルを通じて通知文等を送信する際、官職証明等のため電子署名を付した場合には、本人が通知文に付された電子署名の署名検証をすること

は困難である。そのため、マイ・ポータルが本人に代わって署名検証を行い、その結果を本人に通知する機能をマイ・ポータルに付加する。［13］

② 情報提供ネットワークシステムに残されるアクセスログは、コーディングされているため、その内容を本人が理解できるように、自然言語に変換する。［13］

マイ・ポータルの機能は、「閲覧」、「申請」、「通知」の 3 つの機能に、アクセスログを確認する機能を加えた 4 つの機能である。

図４－６にそれぞれの機能を図示する。

① 自己情報へのアクセスログを確認

情報提供ネットワークシステムを通じ、自己のどのようなデータがどのような法定業務の下にどの情報保有機関がアクセスしたかを、情報保有基盤が蓄積しているログを閲覧・確認する機能である。

・利用者は、マイ・ポータルからアクセスログの確認を要求。
・マイ・ポータルから、情報提供ネットワークシステムにアクセスログの確認を問い合わせる。
・情報提供ネットワークシステムは該当のアクセスログの情報をマイ・ポータルに送付。
・マイ・ポータルで情報提供ネットワークシステムから送られてきた情報を一時的に保管。
・利用者はマイ・ポータルにログイン。
・マイ・ポータルは情報を表示。
・ログアウトと同時に、利用者フォルダーに一時的に保管していた情報を削除。

② 各情報保有機関が保有する自己情報を確認 「閲覧」

情報提供ネットワークシステムを通じ、各情報保有機関が保有する自己情報を確認し、誤りがあればその情報保有機関に対し、修正を求める。

・利用者は、マイ・ポータルから自己情報の閲覧を要求。
・マイ・ポータルから、情報提供ネットワークシステムに自己情報の確認を問い合わせる。
・情報提供ネットワークシステムは該当の情報保有機関に対し情報提供ネットワークシステムに自己情報の確認の問い合わせを伝達。
・情報保有機関は必要な情報を切り出し、マイ・ポータルに送付。
・マイ・ポータルで情報保有機関から送られてきた情報を一時的に保管。
・利用者はマイ・ポータルにログイン。
・マイ・ポータルは情報を表示。
・ログアウト後に、利用者フォルダーに一時的に保管していた情報を削除。

③ 電子申請を経由する機能（ワンストップサービス） 「申請」

利用者はマイ・ポータルから一度の申請を行うことで、情報提供ネットワークシステムを通じ、関連する情報保有機関全てがワンストップで処理を行う。

・利用者は、マイ・ポータルから電子申請を行う。

・情報提供ネットワークシステムは関連する情報保有機関全てに対し、申請を伝達する。

・情報提供ネットワークシステムから連絡を受けた情報保有機関は申請を受け付け、処理する。

④ 行政機関等からのお知らせを表示（プッシュ型サービス） 「通知」

例えば、年金定期便と言ったような行政機関から個人宛のお知らせを送付する機能。情報提供ネットワークシステムを通すため、法定業務に限定される。

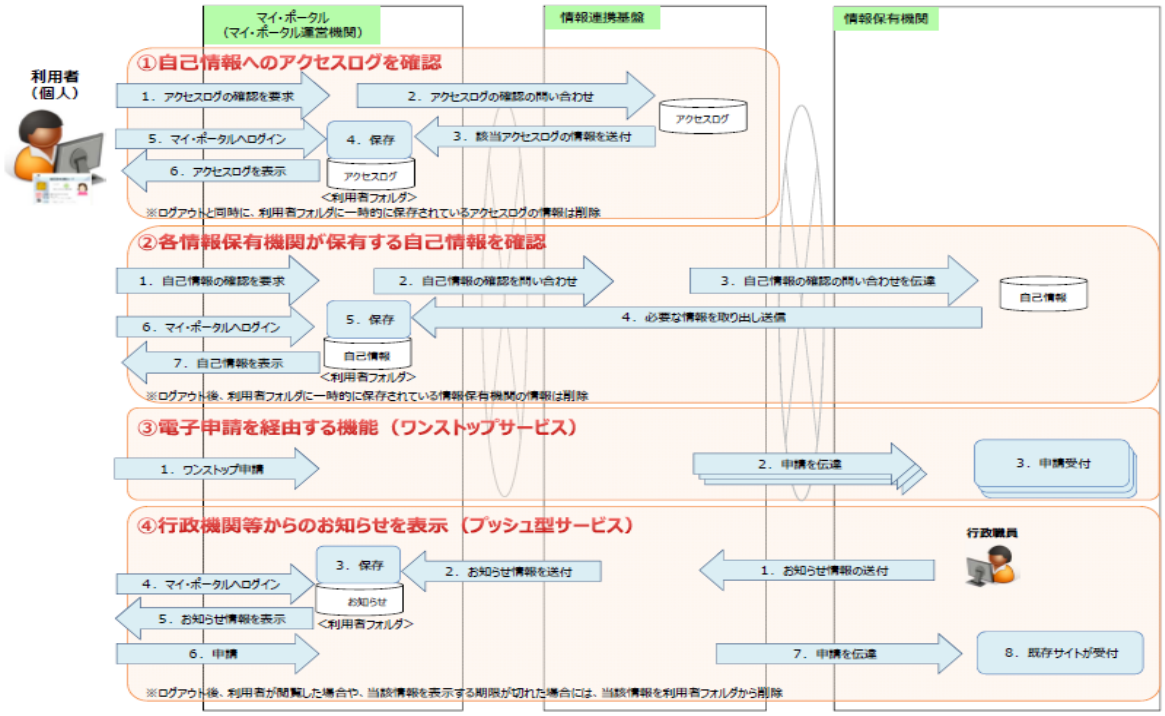
・情報保有機関は情報提供ネットワークシステムに個人宛のお知らせ情報を送付。

・情報提供ネットワークシステムは該当する個人のマイ・ポータルにお知らせ情報を送付。

・利用者はマイ・ポータルにログイン。

・マイ・ポータルは情報を表示。

・ログアウト後に利用者が閲覧した場合や、もしくは当該情報を表示する期限が切れた場合、利用者フォルダーに一時的に保管していた情報を削除。



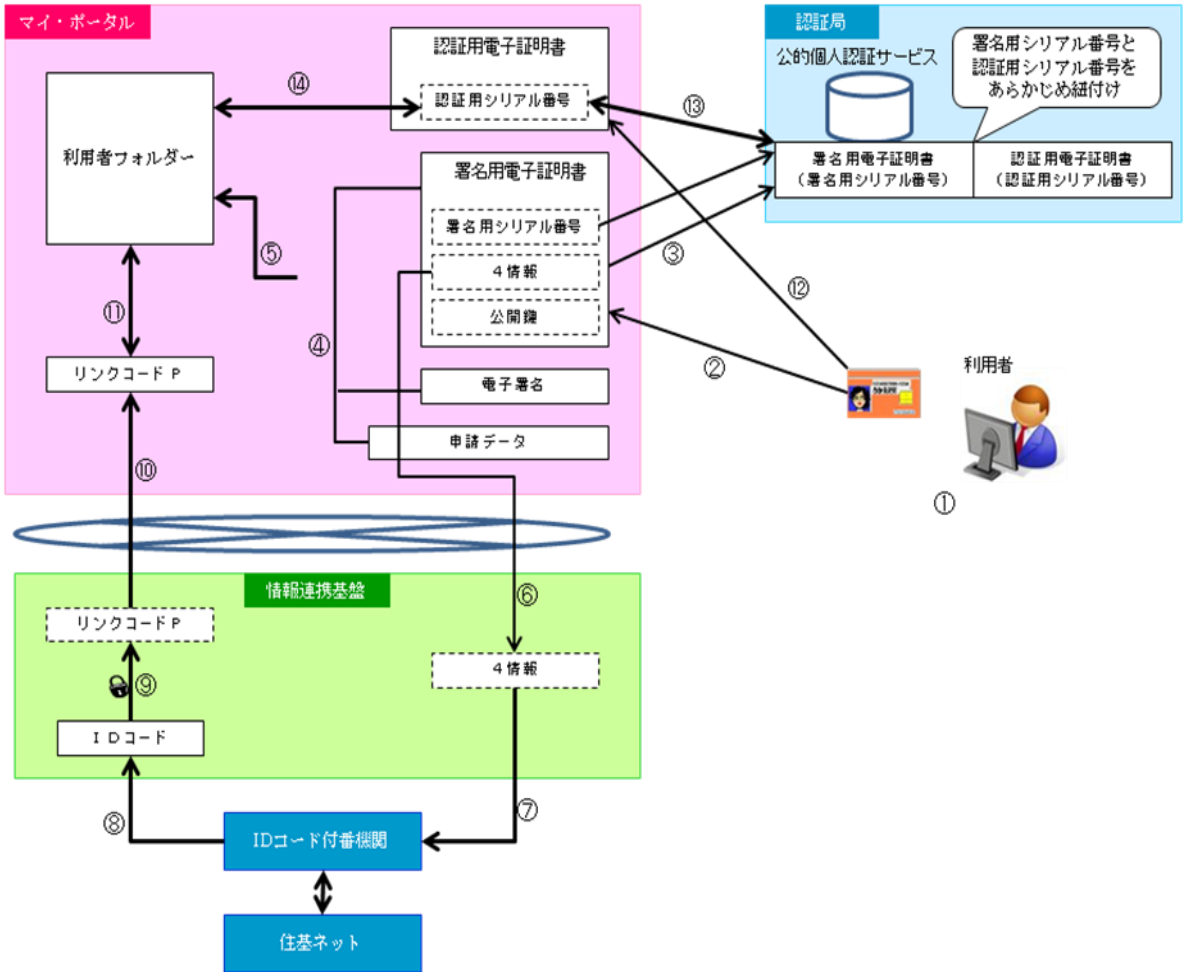
（出典：内閣官房・情報連携基盤技術 WG（第３回）議事録、資料 3-1「第２2.(1) マイ・ポータルの機能」）

図４－６　マイ・ポータルの機能

前述で、マイ・ポータルはインターネットからのアクセスを可能としおり、ログインにおいてはJPKI による認証、すなわち公的個人認証を基本としていると述べた。利用者がどのように利用者フォルダーを取得し、どのようにログインするかについて次に説明する。

ここでは、公的個人認証に現行の署名用鍵ペアとは別に、新たに認証用の鍵ペアを設けることにしている。このため、IC カードには署名用とは別に、認証用の秘密鍵、認証用の暗証番号、および認証用の電子証明書が格納される。

図４－７にマイ・ポータルの利用者フォルダーの取得方法について図示する。公的個人認証サービスではあらかじめ署名用シリアル番号と承認用シリアル番号は紐づけられているとする。



（出典：内閣官房・情報連携基盤技術 WG（第４回）議事録、資料 2-3「（修正案）第２２,(3)③ マイ・ポータルへのログインの手順（**a**）利用者フォルダ取得のフロー」より抜粋編集）

図４－７　利用者フォルダーの取得方法

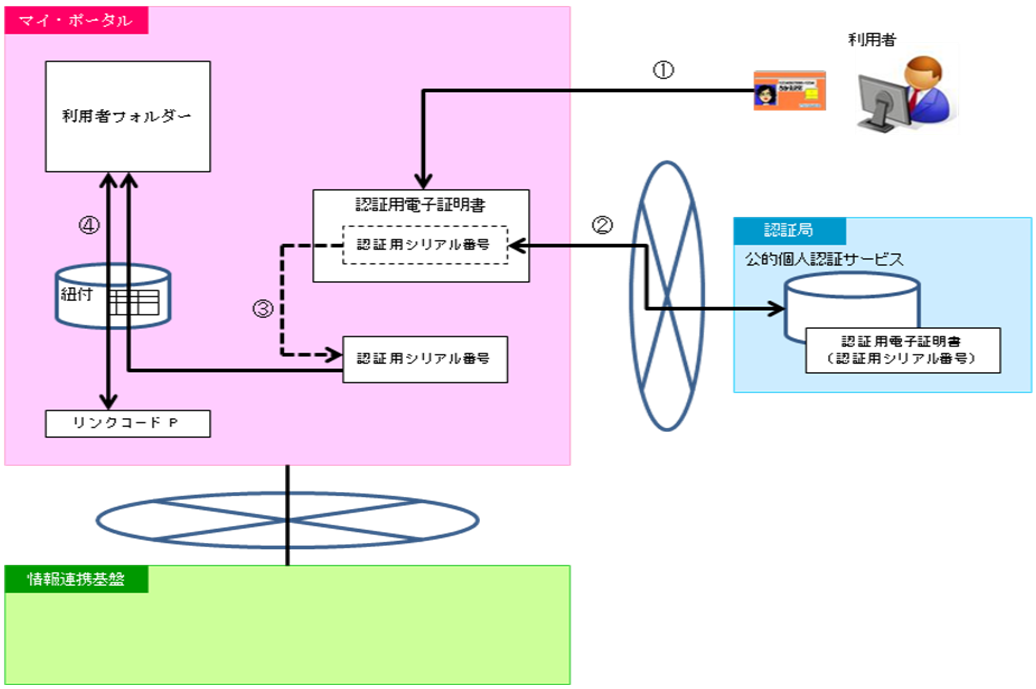
利用者フォルダーは認証用シリアル番号を ID とし、認証用電子証明書でログイン出来るように、署名用電子証明書で申請し、認証用シリアル番号と利用者フォルダーを紐づける必要が

ある。取得方法は以下のようになる。

① 利用者はパソコン等にICカードをセットし、署名用の暗証番号を入力する。
② 署名用の電子証明書を付けて、利用者フォルダーの取得申請を行う。
③ 利用者フォルダーの取得申請を受けたマイ・ポータルは、認証局に対し、署名用証明書の有効性を確認。
④ マイ・ポータルが電子署名を検証。
⑤ 利用者フォルダーを生成。
⑥ マイ・ポータルは情報提供ネットワークシステムに対して、署名用電子証明書の4情報を提示し、リンクコードPを要求。
⑦ 情報提供ネットワークシステムはIDコード付番機関に対して、マイ・ポータルから受け取った4情報を提示し、IDコードを要求。
⑧ IDコード付番機関は、情報提供ネットワークシステムに4情報に対応したIDコードを提供。
⑨ 情報提供ネットワークシステムはIDコード付番機関から提供されたIDコードを可逆暗号関数により、リンクコードPを生成。
⑩ 情報提供ネットワークシステムは、マイ・ポータルに対しリンクコードPを提供。
⑪ マイ・ポータルは生成した利用者フォルダーとリンクコードPを紐付け。
⑫ マイ・ポータルは利用者のICカードより認証用の電子証明書を取得。
⑬ マイ・ポータルは取得した認証用電子証明書から、認証用シリアル番号を抽出し、署名用シリアル番号と共に認証局に送付し、利用者であることを確認。
⑭ マイ・ポータルは認証用シリアル番号と利用者フォルダーを紐づける。

以上のような手続きにより、利用者フォルダーは認証用シリアル番号と紐づけられ、以後、利用者は認証用電子証明書にてマイ・ポータルにログインすることとなる。

次に、図５－８にマイ・ポータルへのログイン手順を図示する。



（出典：内閣官房・情報連携基盤技術 WG（第 4 回）議事録、資料 2-4「（修正案）第 2 2,(3)⑤マイ・ポータルへのログインの手順（b）ログインフローマイ・ポータルへのログインの手順（**a**）利用者フォルダ取得のフロー」より抜粋編集）

図４－８　ログイン手順

① 利用者はパソコン等に IC カードをセットし、認証用の暗証番号を入力する。
② マイ・ポータルは認証局に対して、認証用の電子証明書の有効性を確認。
③ マイ・ポータルは利用者の IC カードから取得した認証用電子証明書から、認証用シリアル番号を抽出。
④ マイ・ポータルは、認証用シリアル番号から利用者フォルダーを呼び出す。

以上のような手順にて、利用者はマイ・ポータルにログインすることになる。また、ここで、以前に説明した様にマイ・ポータルも 1 つの情報保有機関との位置付けにあることから、リンクコード P と認証用シリアル番号との対照テーブルを持ち、情報提供ネットワークシステムとの情報連携はリンクコード P において行われることとなる。

ただし、4. 4. 1 節で説明した様に、情報提供ネットワークシステムでは法定業務のみを取り扱うことより、このマイ・ポータルの「閲覧」・「申請」・「通知」の機能についても法定業務に限定された利用となっている。

4. 3　IC カード

IC カードも国民 ID 制度のシステムの重要な構成要素の 1 つである。国民一人ひとりに配布

され、本人確認（個人認証）やマイ・ポータルのログインに利用することとなる。また、「社会保障・税の番号制度」においては、健康保険証、年金手帳に代わるものとしての利用が考えられている。このために、新たに IC カードを配布するには、現在施行中の住民基本台帳カード（住基カード）と重複することになり、多くの機能で住基カードを包含することとなるため、住基カードを改良し利用することとしている。

つまり、自己の「番号」に係る個人情報についてのアクセス記録の確認等を行うことができるマイ・ポータルにログインするため、また、法令に基づき「番号」を取り扱い得る事業者等が本人確認をした上で「番号」を確認できるようにするため、IC カードには、以下のような要件が必要となる。

① その者に係る住民票に記載された氏名、住所、生年月日、性別及び「番号」その他政令で定める事項が記載されていること。

② 現行の住民基本台帳カードに記録されている事項に加え、「番号」及び公的個人認証サービスの電子証明書その他政令で定める事項が記録された半導体集積回路が組み込まれ、現行の住民基本台帳カードの機能を有すること。

また、可能な限り、現行の住民基本台帳カード、住基ネットや公的個人認証サービス等を活用しつつ、住民基本台帳カードが有する機能等に加え、以下の改良をするものとしている。

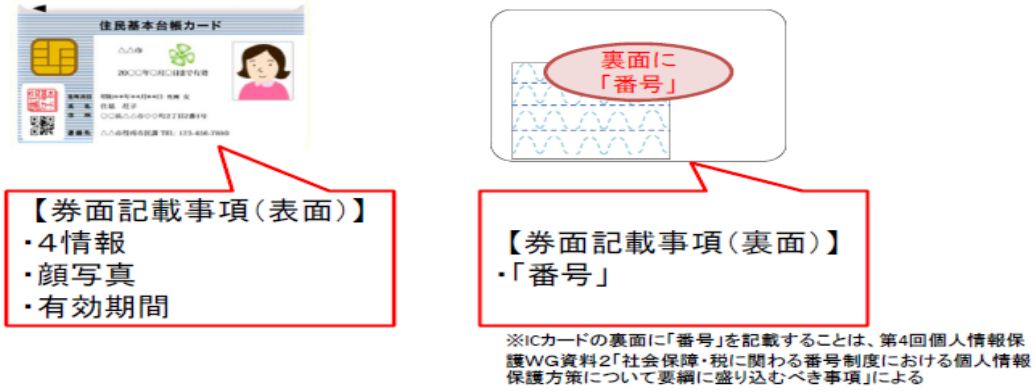
（1） マイ･ポータルにログインするために、現在は署名サービスのみに限られている公的個人認証サービスに認証用途を付加する。

（2） 電子証明書の有効期間を現行の３年から５年に延長､公的個人認証の利便性を高める。

（3） 民間事業者の窓口等で電子的に本人確認を行うため署名検証者を民間事業者に拡大する。

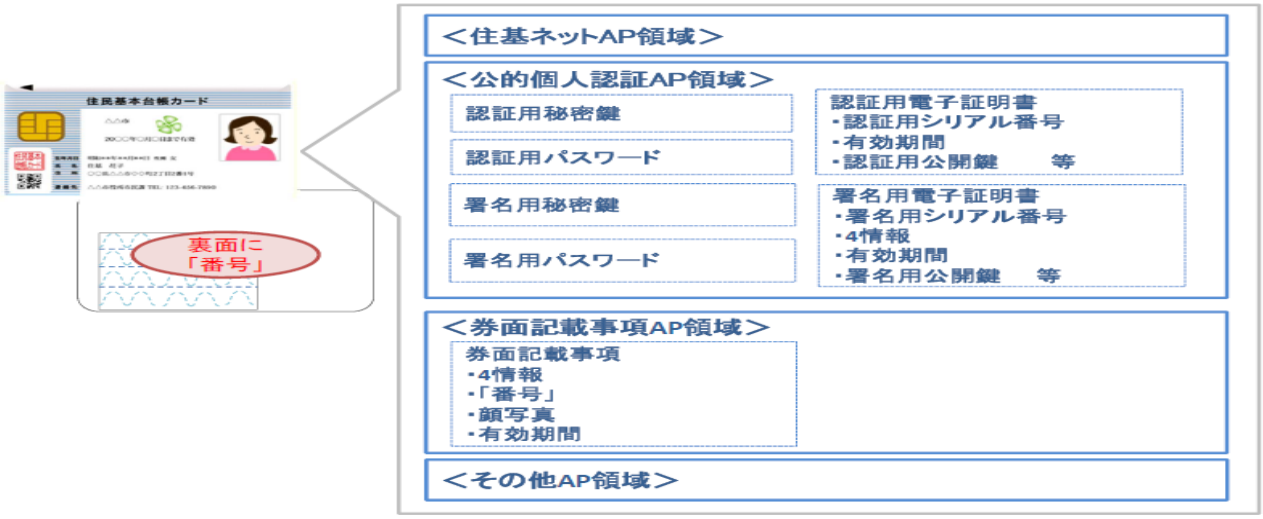
（4） 「番号」の告知の際、「番号」の真正性を担保するため、IC カードの券面に「番号」を記載し、IC チップに「番号」を記録する。

図４－９に IC カードの券面の概要をまとめる。また、図４－１０に IC カードに搭載するデータを示す。



（出典：個人情報保護・情報連携基盤合同WG議事次第、資料６「IC カードに関する検討事項」）

図４－９　IC カードの券面



（出典：個人情報保護・情報連携基盤合同WG議事次第、資料６「IC カードに関する検討事項」）

図４－１０　IC カードの搭載データ

今回、ここで注目すべきことは、

① 公的個人認証に認証用機能が加わったこと。

② 公的個人認証の署名検証者を民間事業者に拡大すること

③ 公的個人認証の有効期間が３年から５年に延びたこと。

④ 顔写真が必須となったこと。

⑤ IC カードの中にも顔写真データを搭載すること。

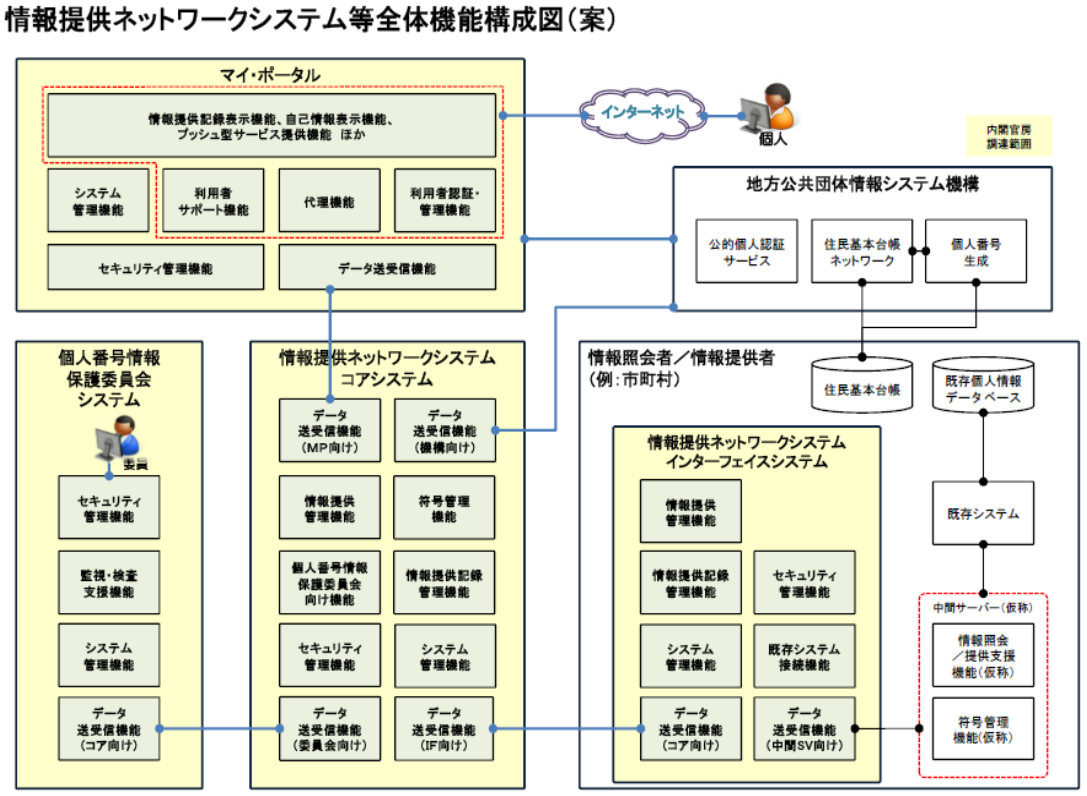
⑥ 券面に「共通番号」を記入すること。

が挙げられる。

4.4　自治体への接続

政府においても地方自治体に対し電子化の推進を援助している。今回の「国民 ID 制度」と「社会保障・税の番号制度」の制度の施行に向けて、「情報保護評価ガイドライン」を策定し、個人情報保護とプライバシー保護の観点から、システムや運用を評価、承認していくこととしている。一方、地方自治体とのインタフェースの検討も行われているが、まだ情報提供ネットワークシステムの仕様確定とはならないため十分な検討がされていない。

現在示されている、地方自治体との接続に関わる機能構成の案を図４－１１に示す。



（出典：内閣官房、情報連携基盤技術WG議事次第、資料 4-1「情報提供ネットワークシステム等全体機能構成図（案）」）

図４－１１　地方自治体との接続に関わる機能構成の案

また、現在政府の検討会で決定している内容としては以下の通りである。

地方公共団体のシステムについては現在検討中であり、「特定個人情報保護評価指針」の中に記される「評価書（システム設計のレポート：自己評価）」の提出と地方公共団体での独自の承認に留められ、政府の承認や「特定個人情報保護評価指針」通りの運用はしない方向となっている。

システムの開発については、各省や自治体とのインタフェースは政府から提供される予定であり、自治体では、情報提供用の中間サーバを用意する必要がある。

第５章　VRICS

本章では九州大学が開発した社会情報基盤 VRICS（Value and Right Circulation control System）についてその概要を説明する。

5.1　ID 管理

ID（Identification）とは、個人を識別するための番号である。情報システムでは誰でもが利用できるとは限らない。利用できる者と利用できない者とを区別し、利用できる範囲も制限することがある。情報システムでは ID を利用して、利用している者を認識し、利用制限を与えることになる。社会情報基盤においては、基盤上で複数システムが稼働し、それぞれのサービスが行われる。それぞれのサービスにおいて、個人を認識するために ID が用いられる。これら複数のシステムが 1 つの基盤上で連携し、サービスを提供するためには ID の管理が重要であり、その管理方法にてリスクヘッジも可能となる。

複数のシステムを扱う ID 管理モデルには、セパレートモデル、フラットモデル、セクトラルモデルの 3 種類がある。まず、その 3 種類の ID 管理について説明する。

5.1.1　セパレートモデル

図５－１にセパレートモデルのイメージ図を表わす。

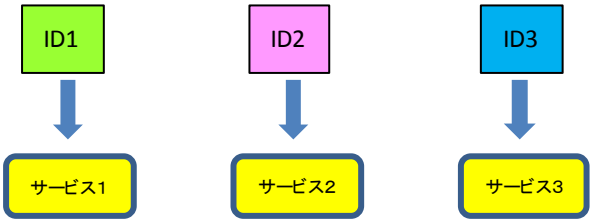


図５－１　セパレートモデル

セパレートモデルとは、システム毎に異なる ID にてサービスを提供する仕組みである。例えば、図５－１の様にサービスが 3 種類ある場合、サービス 1 に対して ID_1 を、サービス 2 に対して ID_2 を、サービス 3 に対して ID_3 を用いることになる。1 人の利用者が 3 つ全てのサービスを利用するためには、3 つの異なる ID を持つ必要がある。異なった会社のクレジットカードや銀行カードを想像すると良い。

このセパレートモデルでは、お互いのサービスが独立しており、相互に影響を与えることは無い。セキュリティ面から言えば、独立したセキュリティを保ち、万一 1 つの ID が盗まれたりセキュリティが破られたりしても、他のシステムに影響を与えず、利用者は他のサービスを

利用し続けることが出来る。

しかし、システム同士が独立しているため、情報の連携はなく、使用者は 3 つの ID を管理し、用途に応じて使い分けなければならない。また、個人情報の変更などがあれば、各々のシステムに別々に 3 回同じ登録変更の手続きが必要となる。さらに、システム間の連携が無いが故、1 人の利用者に対し、2 つ 3 つのシステムが連携してシームレスなサービスを行うことは不可能である。

各国政府の行政サービスを見た場合、日本やドイツはこのセパレートモデルとなっている。例えば、健康保険証の番号、運転免許証の番号、パスポートの番号、住民票コード、など住民 1 人ずつに対して様々な番号（ID）が与えられ、その番号でサービスが行われている。各々のシステムが独立しているため、セキュリティは守られているが、例えば住所変更をする場合には、全て 1 つずつ別々に手続きが必要となって、利用者の手間がかかるだけでなく、サービスを提供する側の業務も重複して行われることになる。

5.1.2　フラットモデル

フラットモデルは、全てのシステムが、1 つの ID で個人を識別し、サービスを提供するものである。図５－２にフラットモデルのイメージ図を示す。

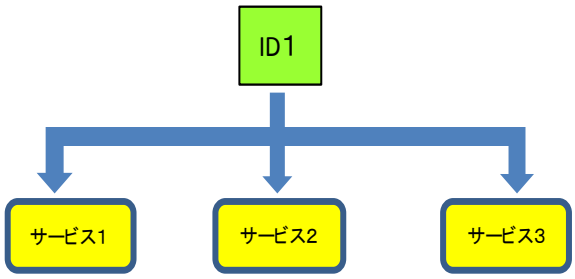


図５－２　フラットモデル

例えば、図５－２のように、サービス 1、サービス 2、およびサービス 3 は同じ ID_1 を用いてサービスを提供することになる。ホテルに宿泊した場合を想像してほしい。ホテルのルームナンバー一つで、ラウンジ、プール、売店、レストラン、車の手配、など全てのサービスが利用できる。

フラットモデルでは、利用者は 1 つの ID で認識されるため、多くのサービスがあったとしても、1 つの ID を管理すれば良いことになる。ホテルの例では、ルームナンバーを忘れなければ全てのサービスが受けられることとなる。また、例えば部屋の変更があったとしても、フロントに連絡するだけで、全てのサービスが新しい部屋のルームナンバーに継続されることに

なる。さらに、プールサイドでレストランから食事を取ったり、レストランの予約時間に合わせて車を用意したりするなど、連携したサービスが可能となる。

しかし、ルームナンバーを他人に悪用されれば、全てのサービスが勝手に使われ高額の請求を受けることになる。フラットモデルでは、ID を取られてしまうと全てのサービスに影響を与えることになる。セキュリティの考えでは、このように ID が盗まれたり、漏れたりする可能性は、利用者がサービスを使用する際に多く存在しており、1 つのサービスから ID が盗まれる可能性が高いと考える。

NPO 法人である日本ネットワークセキュリティ協会での 2009 年の情報漏洩に関する調査結果[14]をみると、情報漏洩の原因としては誤操作、管理ミス、紛失・置忘れ、盗難、不正な情報持ち出しと言った端末操作・管理やメディア管理に関わる情報漏洩が 9 割近く圧倒的に多く、不正アクセスは 1%以下との報告[14]がある。情報漏洩の媒体に関しては、紙媒体、USB 等可搬記録媒体、E-mail、PC 本体で 8 割以上の情報漏洩が起きており、情報漏洩のほとんどが端末および端末周辺で起きているものと考えられる。

フラットモデルでは、1 つのサービスが他のサービスに影響を与え、一番セキュリティの脆弱なシステムのセキュリティレベルに引きずられることとなる。リスクヘッジの面からもフラットモデルは問題を持っていると言わざるを得ない。

各国政府の行政サービスを見た場合、シンガポール、米国、エストニア、韓国などはこのフラットモデルとなっている。例えば、シンガポールでは、出生時に NRIC（National Registration Identification Card）番号が割り当てられ、全ての住民サービスはこの NRIC 番号で行われている。また、外国人居住者には FIN 番号（Foreign Identification Number）が付与される。NRIC 番号や FIN 番号は、パスポートの番号や運転免許証の番号にもそのまま使用され、行政手続、銀行口座の開設・不動産の売買といった個人の経済取引、契約など、公私様々な ID として個人の認証に使用されている。ID が 1 つであるため、住民にとっては行政手続きにおいて重複した申請がほとんど不要となっており、便利なものとなっている。

しかし、韓国の例に見るように個人情報流出などのセキュリティ問題が常に残る。韓国では 2008 年に 1800 万人の個人情報が流出し、ID を再付与する問題が起きた。さらに、2011 年に、3500 万人の ID と名前、住民番号、暗証番号、電話番号、メールアドレスなどの個人情報が流出し、住民登録制度の根幹が崩壊するかという危機に見舞われた。

5.1.3　セクトラルモデル

セパレートモデルの利点とフラットモデルの利点を合わせ持たせ、各々の欠点を補うように考えられた方式が、セクトラルモデルである。図５－３にセクトラルモデルのイメージ図を示す。

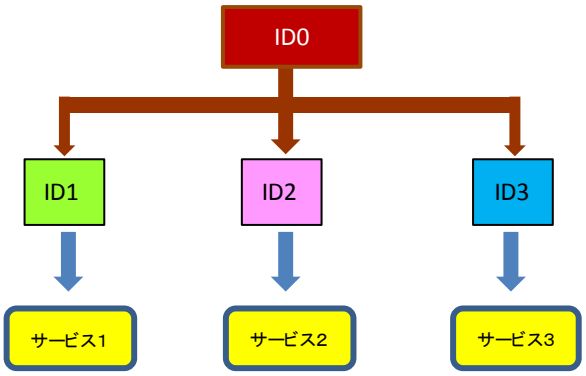


図５－３　セクトラルモデル

セクトラルモデルでは、基本となる ID からシステム毎に異なった別の ID を発生させて、その発生させた ID でサービスを提供すると言うものである。具体的には、図５－３の様に、基本となる ID_0 から、ある手法（不可逆暗号関数）を用いて、ID_1、ID_2、ID_3 を発生させる。サービス１ではこの発生させた ID_1 を、サービス２では ID_2 を、サービス３では ID_3 を各々利用してサービスを提供する。

サービスは各々異なる ID である ID_1、ID_2、ID_3 により提供されるため、各々が独立したシステムとなっているが、ID_0 にまで戻れば、各々のサービスは連携出来る。セキュリティの面から見れば、各々のサービスが独立しているため、ID_1、ID_2、ID_3 のいずれか１つの ID が盗まれようと、他の ID を使用しているサービスに影響を与えることは無い。利用者は、IC カードなどの認証デバイスを利用すれば、ID_1、ID_2、ID_3 の意識なく、３つのサービスを利用することになる。5.1.2 節のフラットモデルの説明でも触れたように、ID が盗まれたり、漏れたりする可能性は、利用者がサービスを使用する際に多く存在しており、１つのサービスから ID が盗まれる可能性が高くなる。

良く判るように、図５－４と図５－５にフラットモデルとセクトラルモデルの場合を比較してみる。

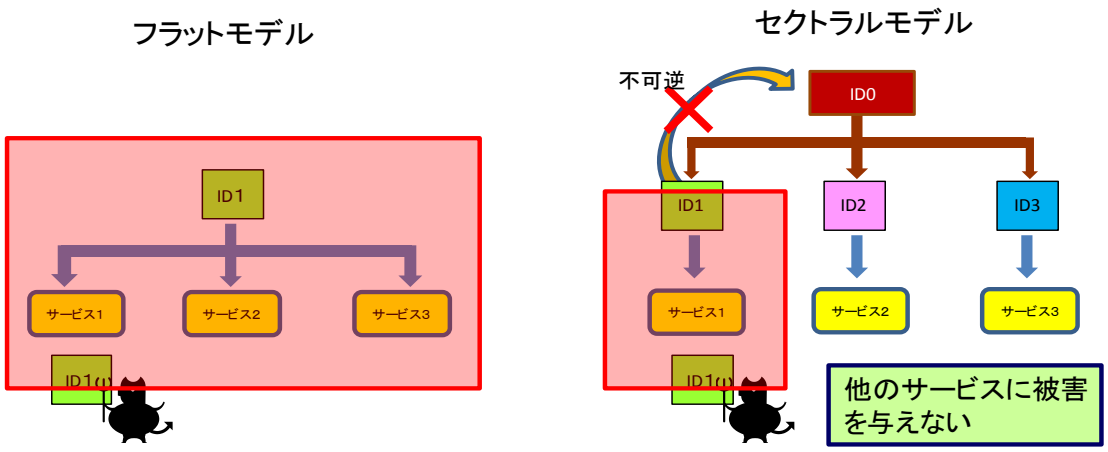


図５－４　フラットモデルとセクトラルモデルのセキュリティ比較１

図５－４では、何者かがサービス１から ID_1 を盗み出したとする。フラットモデルでは、サービス２もサービス３もサービス１と同じ ID_1 を使用しているため全部のシステムに被害が及んでいる。しかし、セクトラルモデルの場合、ID_0 から ID_1 は不可逆暗号関数で生成されているため、ID_1 から ID_0 には戻れない。このため、ID_1 を使用しているサービス１だけの被害に留まることになる。

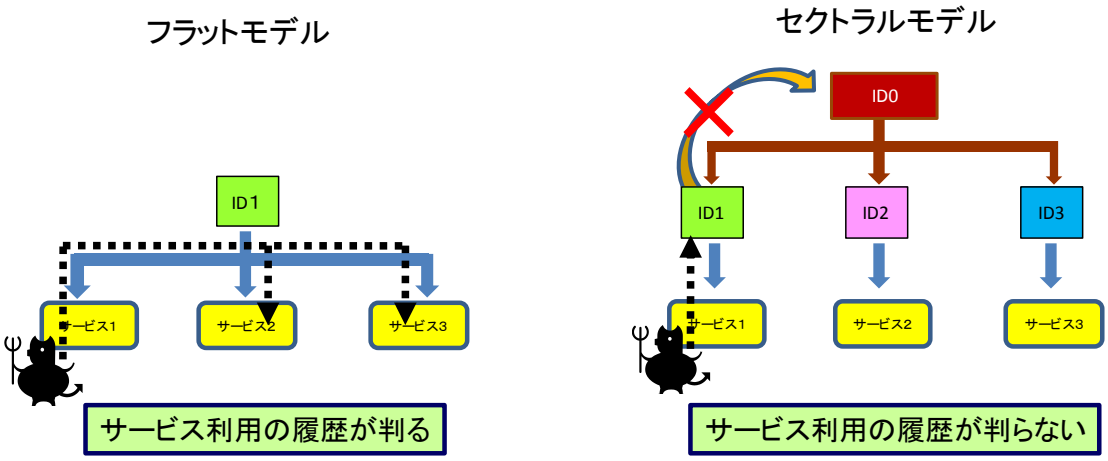


図５－５　フラットモデルとセクトラルモデルのセキュリティ比較２

同様に、図５－５において何者かが利用者のサービスの履歴調べようとしてサービス１に入り込んだとする。フラットモデルの場合、同じ ID で制御されているため、侵入者が利用者の履歴を調べることが可能となる。しかし、セクトラルモデルの場合、図５－４と同じ理由で ID_1 から ID_0 を追うことが出来ないため、侵入者は ID_2 や ID_3 で利用した履歴を知ることは出来ない。

このようにセクトラルモデルでは、ID がシステムごとに独立しているため、セキュリティが高く、リスクヘッジを考慮されたシステムと言える。当然、ID_0 や、ID_0 から ID_1、ID_2、ID_3 を発生させる部分は秘匿であるという前提である。これは、公開鍵暗号基盤（PKI）における認証局（CA）や鍵生成と同じように、システム運営者以外に流出しないよう、厳格に守られて運用されなければならない。

しかし、ID_0 からの ID_1、ID_2、ID_3 の発生や、サービス間の連携のためには一旦 ID_0 へ戻りお互いの ID を秘匿しながら連携を取らなければならないなどシステムが複雑となり、処理に時間がかかることが欠点であり、使用者が多くなればなるほどそれ以上にシステムが複雑となり、大規模な人数には不向きとされてきた。

今日、IT 技術の発達によりその課題も大きく改善されてきている。例えば、IC カードの発達により、IC カードに ID_1、ID_2、ID_3 を入れる必要はなく、秘匿に IC を入れた ID_0 から複雑な関数により、ID_1、ID_2、ID_3 を発生させることも、いとも簡単に瞬時にできるようになった。

既に別々に存在するシステムのサービス連携を行うために、シングルサインオン（SSO：Single Sign-On）と言う技術を用いて、セパレートモデルの情報連携を実現させることが出来る。

シングルサインオン（SSO）とは、個人の持つ ID が増加すれば、個人の ID やパスワードの管理の手間が多くなるため、この管理を無くそうとしたのが目的である。複数の異なるシステムがあり、個人の ID やパスワードが異なる場合、その中の 1 つの ID にて他のシステムにもアクセス出来るように ID を連携させてものである。１回のアクセスについてその都度連携を確認しながらアクセスを可能とした仕組みであり、複数のサービスを連携させる場合に、利用者は何度も ID やパスワードを入力する必要が無いので便利なシステムとなっている。しかし、1 つの ID 情報で複数のサービスにアクセスするシングルサインオン（SSO）は、確かに利便性は高いものの、フラットモデルの場合度同様に、ID とパスワードなどの本人確認情報を不正に入手した者が、その人間の全ての情報を盗みとることが容易となる。さらに ID 情報が漏洩した場合、シングルサインオン（SSO）で連携して提供するサービスの全てに被害を及ぼす可能性が高い。

同じように、1 枚の IC カードを用い、複数のサービスのパスワードの管理の手間を無くそうとした方法にマルチ ID アクセス方式がある。

マルチ ID アクセス方式とは、IC カードの中に独立したサービスの複数の ID を格納し、サービス毎に ID を使い分ける方式である。この方式は基本的にセパレートモデルと同じであり、不正な名寄せによる情報詐取は、全ての ID とそれに対応した本人確認情報を入手しなければならないため、1 つの ID の漏えいはそれに対応した 1 つのサービスに留まり、リスクヘッジが出来ていると考えられる。しかし、この方法は基本的にセパレートモデルと同じであり、

単に、まったく別の管理構造をもった複数の ID を入れているだけで、必要なデータの重複入力が必要になったり、個人のサービス履歴を確認するのに複数の異なる DB を参照が必要となったりするなど、サービス間の情報連携は全くない。つまりは、利用者の ID 管理の便利さだけであって、実際のサービスの利便性の悪さは残されたままとなっている。

ID の管理だけでなく、サービス間の情報連携も可能とするためには、システムの複雑さを引き換えに、セクトラルモデルを採用しなければならないのではないか。また、情報社会において日々膨大な量の情報が作られていると言う“ビッグデータ”の管理にはこのセクトラルモデルの ID 管理の手法が有用と考える。特に医療情報などは個人情報として機微な情報であり、日々膨大な量の情報が生まれ、1 つのサーバにおいては管理できない量であり、クラウド技術が有用となるが、これらすべての情報が同じ ID にてアクセスされる事は、安易に個人情報の紐付けが可能となり、セキュリティの面やプライバシー保護の面から非常に危険なものとなるであろう。セクトラルモデルの考え方が役に立つのではないであろうか。

各国政府の行政サービスを見た場合、オーストリアではセクトラルモデルが使用されており、将来の社会情報基盤を検討する中で注目を浴びている。図５－６にオーストリアのセクトラルモデルを図示する。

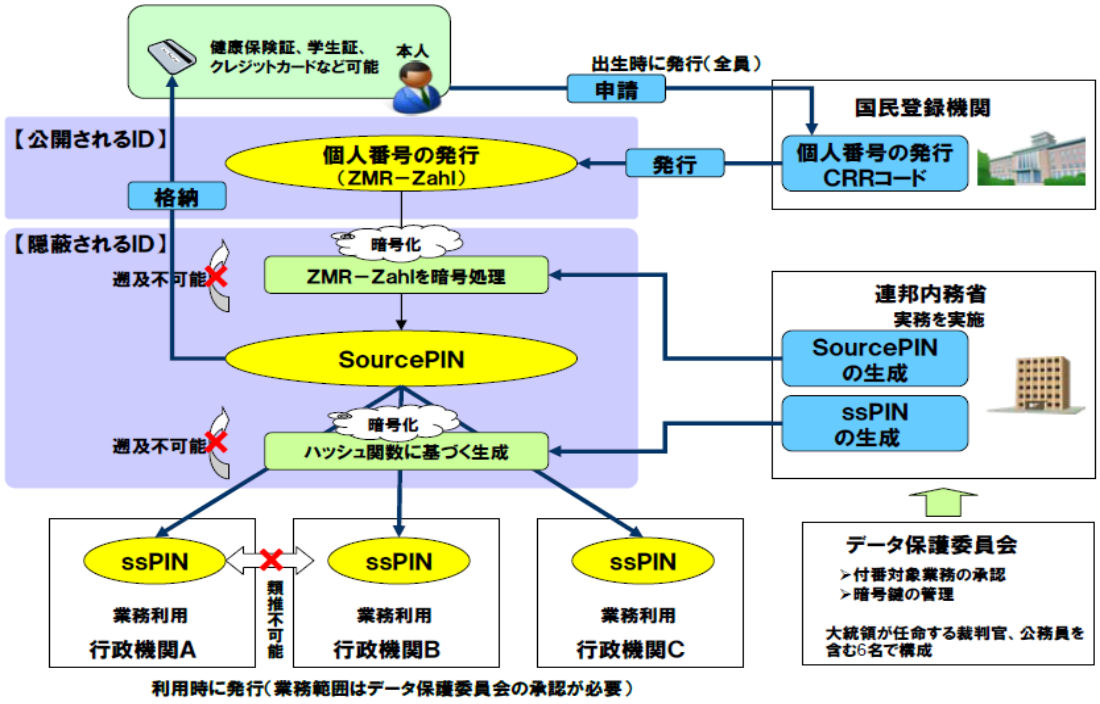


図５－６　オーストリアのセクトラルモデル

（内閣官房「社会保障・税に関わる番号制度に関する検討会」（第４回）資料 2、平成 22 年４月７日、国際公共政策研究センター田中直毅氏の資料より抜粋）

オーストリアでは、出生後すぐに国民登録機関（CRR：Central Register of Residents）に登録され、番号（ZMR-Zah）が与えられる。この ZMR をデータ保護委員会で、TDES により暗号化し、新たな ID（SourcePIN：sPIN）を作成する。作成された SourcePIN は、本人に渡される eID カードのみに格納され、データ保護委員会にもデータを残さない。データ保護委員会は大統領が任命する裁判官、公務員を含む 6 名からなり、TDES の暗号鍵を管理する。このため、SourcePIN から ZMR を推定することはできない。

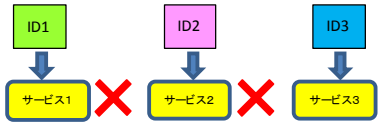
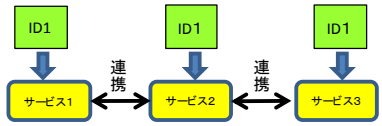
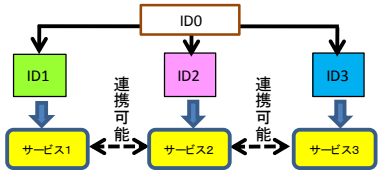
また、各サービスを提供する機関（セクターと呼ばれる）にはあらかじめ SectorID が振られる。SourcePIN とこの SectorID をつなぎ合わせた値に対して、Sha-1 のハッシュ関数により実際に個々のサービスで使われる ID 番号である ssPIN を作成している。このため、ssPIN から SourcePIN を知ることは出来ない。

もし、政府が個人の情報を収集する場合や各セクターにおいて情報連携を行いたい場合は、データ保護委員会の許可を得て、個人の ZMR から SourcePIN を発生させ、次に必要なサービス機関の複数の ssPIN を発生させ、必要な個人情報を収集することになる。

ただし、システムが複雑になることや、情報連携の度にデータ保護委員会への手続きや、データ保護員会での処理に時間がかかることが課題になると考える。

ID 管理のまとめとして、表５－１にセパレートモデル、フラットモデル、およびセクトラルモデル（表２－１再掲載）の比較をまとめる。

表５－１　ID の管理方式の比較（表２－１再掲載）

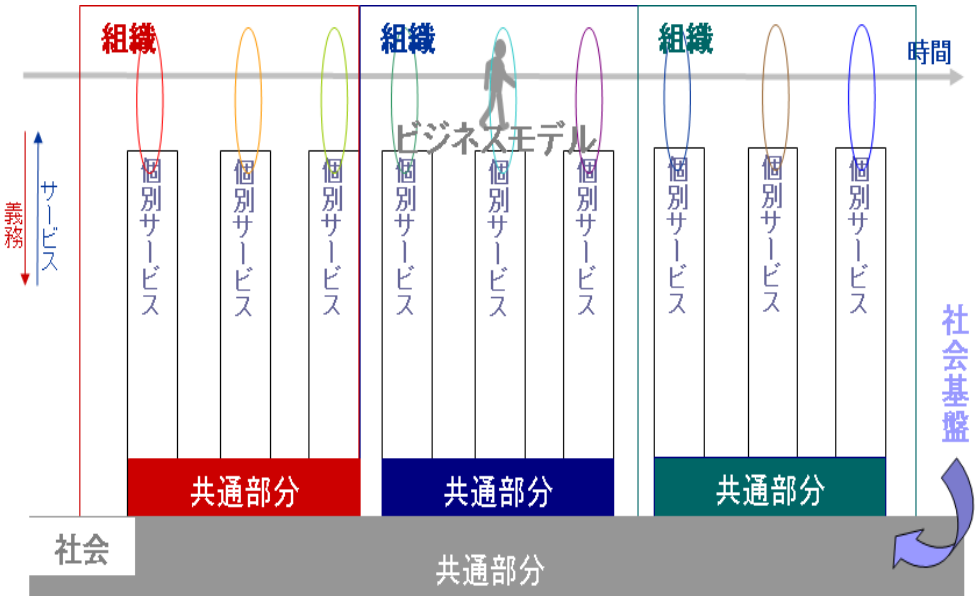
方式	特徴	モデル	特長と課題	使用国
セパレートモデル	・サービス毎に異なるID ・各サービスが独立		（長所） ・サービス毎のセキュリティが独立している （課題） ・ID間に関連性がないので連携が取れない。 ・利用者のID管理が煩雑	日本 ドイツ
フラットモデル	・1人に対して1つのID ・サービス全て共通のID		（長所） ・利用者のID管理が容易 （課題） ・IDが流出すると全ての情報が流出する。 ・IDの流出で全てのシステムがダウンする危険性	シンガポール 韓国 エストニア アメリカ
セクトラルモデル	・サービス毎に異なるID ・サービス間の連携が可能		（長所） ・直接紐づけが出来ないためIDの流出した場合もそのIDのサービスの問題に留まる ・サービスの連携も可能 （課題） ・システムが複雑	オーストリア

5. 2　VRICS[15]

VRICS（Value and Right Circulation control System）とは、九州大学において開発した PID を用いた社会情報基盤であり、電子化された価値と権利権限の流通を管理する仕組みである。

5. 2. 1　VRICS のコンセプト[15]

図５－７に示すように、人間の一日の生活の大部分はその人に選択された様々なサービスアプリケーションが提供するサービスから構成されている。社会情報基盤となるべきものは個別アプリケーションが持つべき共通の機能とアプリケーションの動作環境である。



一般的に、サービスを受けるためには、サービスを受ける権利を行使するための義務も発生する。義務を果たすことそのもの、もしくは義務を果たした証と交換にサービスが提供される。義務は労働であり、労働の対価であるお金（価値）の支払であり、義務を果たした証が権利証である。

様々なサービスを情報化した場合には、このサービスを受けるための権利と義務の関係を情報システム上で管理する仕組みが必要である。この仕組みは言い換えると情報システムにおいてサービスの供給を管理する仕組みであり、電子化された価値と権利権限の流通を管理することにほかならない。

5.2.2　基本構成[15]

VRICS は、システムと運用で価値と権利権限の流通を管理する仕組みである。

図５－８に VRICS の権利権限の考え方のイメージを示す。システムでは、権利権限の確認（Certification）をして、必要であれば権利の正当な行使者であるかを識別（Identification）し、行使を申し出ている人が本当に本人であるかを確認（Authentication）し、その権利権限が行使可能な状況にあるかを確認（Authorization）して問題がなければサービスを提供する。

しかしサービスの提供においてはシステムで対応しきれない外的な脅威やサービス運用のミスに起因するリスクもある。これを VRICS では抑止（精神的、物理的）、防御、担保、転嫁といった運用策で解消することを目指している。

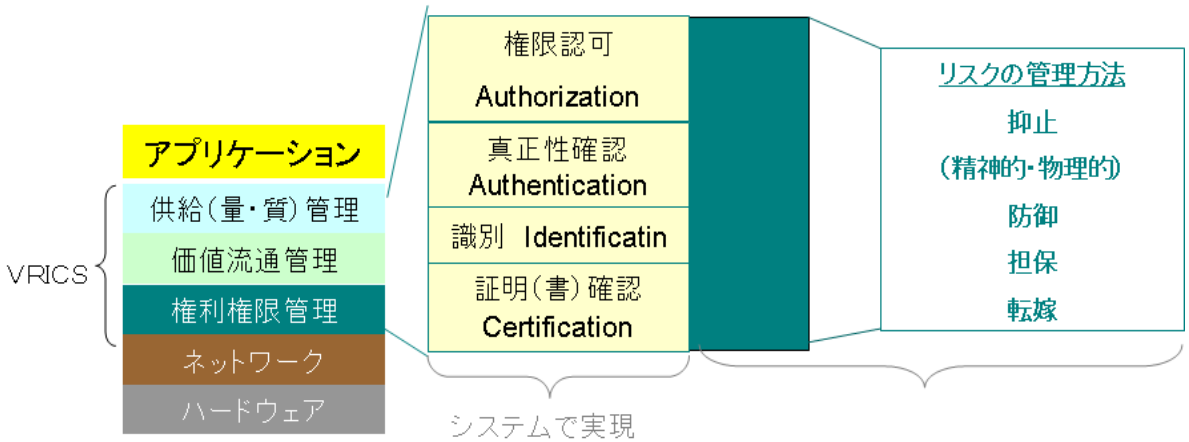


図５－８　VRICS の権利権限管理の考え方

5.2.3　PID を用いた社会情報基盤の構想[6][16]

九州大学では、従来の「既存の社会システムの部分的な電子化」というアプローチから「情報技術の利用を前提とした新しい社会システムの構築とそのための技術開発」という立場への転換[6]を行うべく、社会システムが将来の電子的な世界において弊害となるであろう問題点を探り出し、電子・情報技術の存在を前提とした社会システムの構築を検討した。

その結果、社会基盤の条件として、個人と社会の双方を守るためのしくみであること（個人の権利と社会の秩序）、しくみは単純で理解しやすいものであること（弱者にも不利にならないしかけ）、長期的に安定して運用が可能であること（柔軟性と拡張可能性）、攻撃や災害に対して強くかつ復旧が簡単に行えること（危機対応能力）、経済的に成り立たつこと（経済性）を満たすこととし、利用者（ユーザ）にとってわかりやすい仕組み、サービス提供者からの一方的な認証ではなく利用者もサービス提供者を認証できる双方向認証のシステム、個人情報の流出を防ぐプライバシーの保護、単一方式による複数のサービスの提供と個々のサービスの独立性の確保を実現する社会情報基盤の開発を行った。

基本的なモデルは、利用者、発行者、サービス提供者からなる１つの主体と、PID（Personal

IDentify）という一種の個人 ID からなる。ここで、利用者はサービス提供者と取引を行う主体であり、発行者に属し、PID を発行される。 発行者とは、一般社会において社会的に認知された集団（社会的集団）を代表するものである。利用者はこの集団の一員であり、発行者は利用者を保証する義務を負う。また、 サービス提供者は、利用者にサービスを提供する主体と定義[6]した。この３者モデルを図５－９に示す。

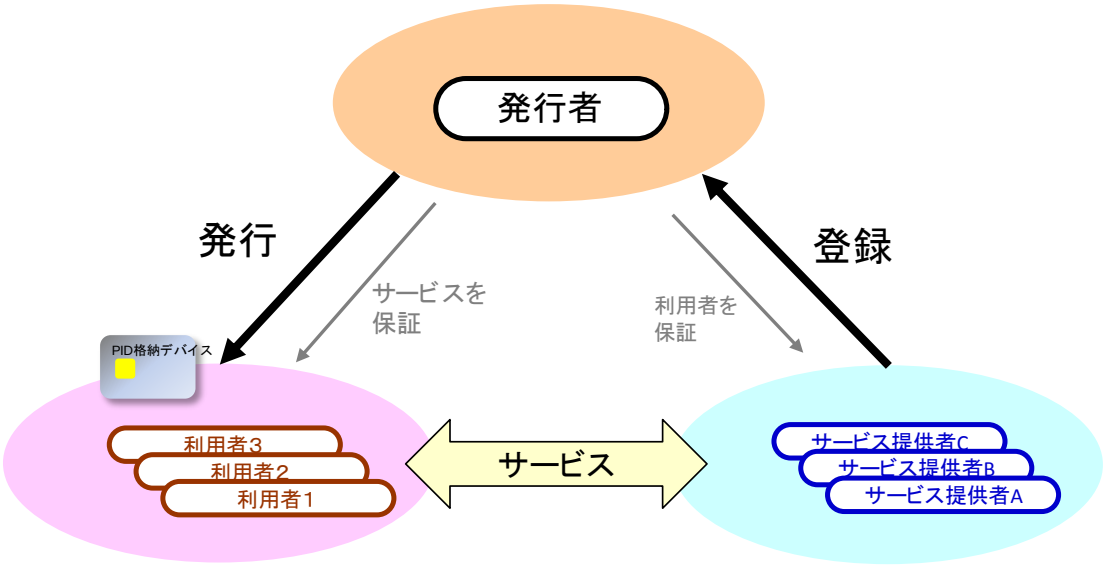


図５－９　３者モデル

３者モデルでは、利用者は発行者より本人性を認証する個人情報を提供し IC カードなどの安全なハードウェアに格納した PID の発行を受けることとなる。一方、サービス提供者は、サービスの信頼性、安全性などを調査した後、発行者に登録される。ここで、PID は発行者がユーザに対して発行する長いビット列である。これは各ユーザに対して固有のものである。発行者はデータベースに、利用者は IC カードなどの安全なハードウェアに保管しておく。また PID の一部もしくは PID から生成されるビット列のことを SubID(PID Subsecquence)と呼び[6]、サービスによって異なる。各々のサービスにおける個人認識 ID の役割を担う。PID の一部である SubID を利用者とサービス提供者が互いに共有し、SubID を用いて互いに相手が正当な者であるかを確認し合ったり、暗号通信などを行なったりすることで安全な電子サービスを実現できる。また、本方式である PID を用いた認証プロトコルは、認証プロトコルの安全性評価の方法について、攻撃への耐性の観点、攻撃の抑止、被害の最小化といった観点から検討し、PKI を用いた SSL/TLS 認証プロトコルに比べてなりすましの脅威に対して安全性を高くすることが可能であると分かった。[17]

5. 2. 4　システムの基本構造と機能[6]

VRICS の基本となる構造は、PID を用いた社会情報基盤の構想に基づいて開発された。VRICS の管理システムの基本構成は前節図５－９で示した３者モデルであり、その ID 管理は前節で説明した PID を用いた社会情報基盤の構想におけるセクトラルモデルとなっている。

VRICS は、管理情報発行者（以下「VRICS 情報発行者」という）と IC カード等の管理情報収納媒体発行者（以下「VRICS デバイス発行者」という）、本人確認情報照会機関（以下「本人確認認証局」という）、サービス提供者、サービス利用者の存在を前提としている。VRICS 情報発行者は IC カード等の VRICS デバイス発行者、本人確認認証局を兼ねることも可能となっており、この場合、PID を用いた社会情報基盤の構想における３者モデルとなる。

VRICS ではオフラインでのサービス提供に対応し、より柔軟な権利権限管理ができるように、参加証（以下「Trade Title」という）、電子的権利証（以下「Service Title」という）、サービス毎の ID（以下「SubID」という）、および本人確認証（以下「Certification Title」という）を用いてサービスの提供管理を行う。ここで、SubID はサービス毎に異なる ID であり、他の同様の ID との間に隠された関係性を有する Hidden relationship ID Access を実現している。これにより VRICS ではセキュリティを保ち、各々のサービスを連携させることを可能としている。PID を用いた社会情報基盤の構想においては、SubID は PID の一部分のビット列であったが、VRICS では PID より生成されるビット列としている。

Trade Title はフィッシング等を防止することを目的として、VRICS デバイスとリーダ間での相互認証をするためにやり取りする情報であり、VRICS デバイス発行時に VRICS 情報発行者によって当該デバイスに埋め込まれる。

Service Title はサービスが追加される度に、SubID 生成のための可変の種とともに、VRICS 情報発行者より VRICS デバイスに送り込まれる情報であり、提供されるサービスと、利用する ID や本人確認方法等の提供条件、Service Title そのものの価値（質と量）が記載されている。提供条件を満足することを前提として、これと交換にサービスが提供されることとなる。

SubID は、VRICS デバイス発行時に VRICS 情報発行者によりデバイスに組み込まれるサービス利用者 1 人に 1 つのユニーク情報である PID と、サービスが追加される度に Service Title とともに、VRICS 情報発行者より VRICS デバイスに送り込まれる ID 生成のための可変の種により、自動生成され利用者識別に利用する。

Certification Title は本人確認情報もしくは本人確認情報収納場所が記載されており、サービスが追加される度に Service Title とともに、VRICS 情報発行者より VRICS デバイスに送り込まれる。

図５－１０に VRICS の認証イメージと図５－１１に認証のフローを示す。

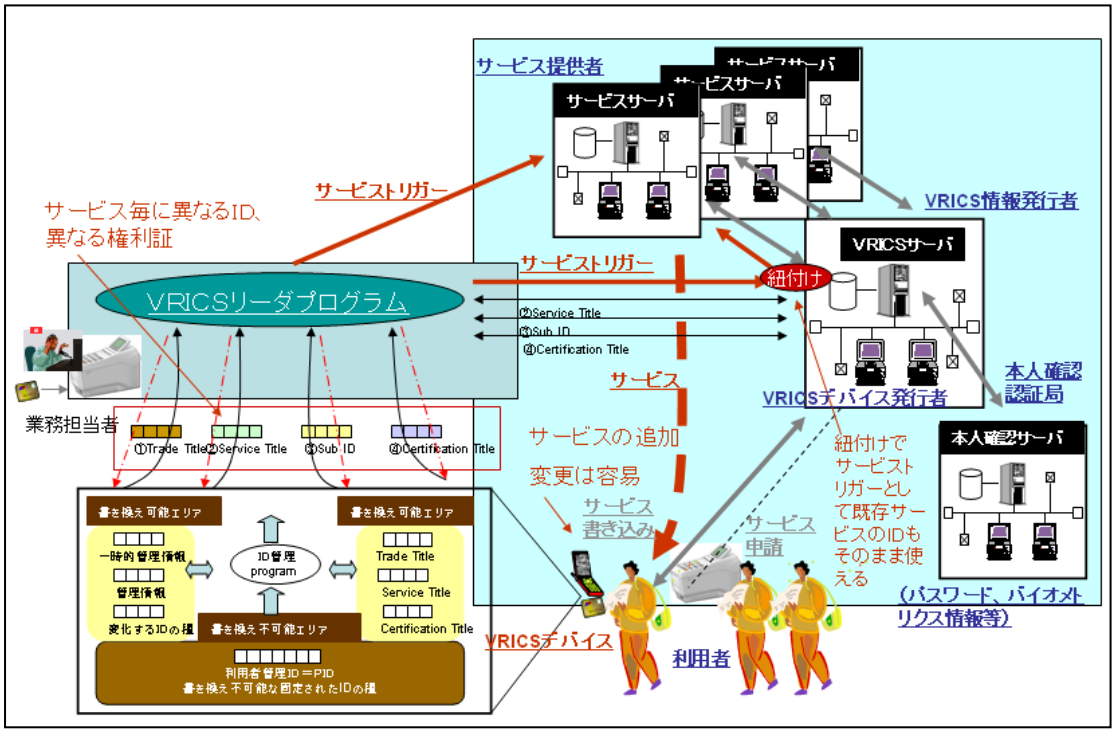


図５－１０　VRICS 認証フロー

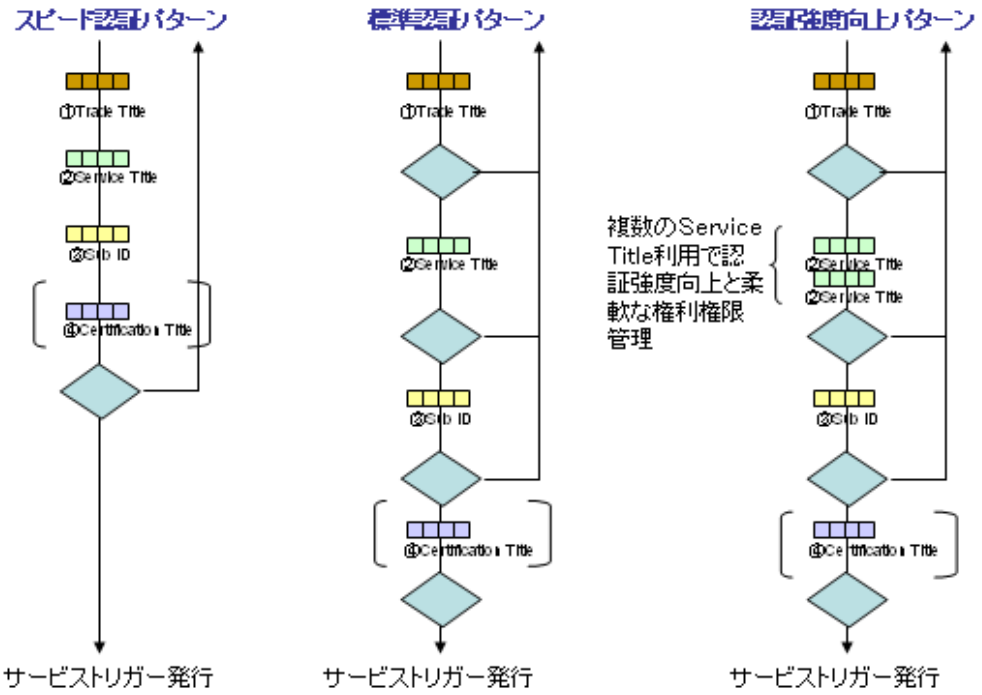


図５－１１　VRICS の認証パターン

VRICS での基本的なサービス提供は、図５－１１の標準認証パターンに示すように、まずVRICSデバイスを専用リーダにかざすとTrade Titleによる相互認証が行われ、次にリーダからの要求に対してService Titleの提供が行われる。ここで、Service Titleの利用条件に利用者識別が含まれていれば、リーダは要求を出しVRICSデバイスはSub IDを返す。さらに、利用条件に本人確認が記載されていれば、リーダは要求を出しVRICSデバイスはCertification Titleを返すか、または本人確認機能要求を出し、リーダで本人確認情報入手を指示して本人確認情報取得後情報を認証局もしくはカード内に送り、本人確認判定を行う。本人確認判定が終わり、リーダがOK信号を受け取ると、リーダはサービスサーバもしくはVRICSサーバにサービス開始トリガを送る。これによりサービスが開始されることとなる。

VRICSでは、既存サービスシステムの取り込みを可能としている。その方法としては２つ手段があり、１つの方法はVRICSのシステム内部に紐付けシステムを持っており、これを利用したService TitleもしくはService Title＋Sub IDの既存サービスIDへの紐付けである。既存のサービスIDでサービスを提供するサービスシステムを取り込む場合、紐付けシステムでService TitleもしくはService Title＋Sub IDを既存サービスのサービスIDに変更して既存システムに返すことにより、既存システムの大掛かりな変更をせずVRICSを用いた情報基盤に取り込むことが可能となる。

もう１つの方法はService Titleによるロケーション指定を用いた既存IDの直接利用である。この方法は、カード内の指定された場所にあらかじめ既存サービスのサービスIDを入れておくことで、Service Titleはサービスに利用する本人識別子として、VRICSで生成されるSubIDを指定せず、既存サービスのサービスIDが収納されているロケーションを指定することができる。これにより既存サービスのサービスIDを直接本人識別子として利用できることになる。

またVRICSでは複数のService Titleと複数のSubIDで一つのサービスの提供をすることも可能である。この特長を利用することで、権利権限管理におけるルート制御や権利のグルーピング管理、図５－１１の認証強度向上パターンのようにカードアクセスにおけるセキュリティ強度の向上も可能としている。

現在の一般的なICカード認証は、カード内にアプリケーションの利用IDが保管されており、そのIDで認証を行うが、VRICSでは、利用者にも知らされないカード内に秘匿されたPIDを種にして、サービス用の鍵と補正値を指定の関数で処理し、利用サービス用のSubIDを生成し認証を行うことになる。１つのIDが例え漏洩しても、関数の制御により、セキュリティの回復が可能となっている。また、VRICSでは、カード内に個人の権利・権限情報を保管し、オフラインで様々なサービスの利用を可能としている。通常、酒類購入（お金・年齢証明）、免税店（お金・パスポート）などでは、個人に固定されたIDだけでは社会の多様な要求にこたえられない場合もあるが、VRICSの認証では、SubIDと権利証を組み合わせた認証を基本とするため、オフラインでも多彩な認証を行うことが可能となっている。

VRICSの特長としては、サービス毎に異なるSubIDを利用し、異なるService Titleにより

多目的サービスに対応している。また、サービスの要求レベルに応じたセキュリティレベルの設定がサービス毎に可能であるうえに、バックエンドサーバ間でのデータ連携・サービス連携が可能となっている。フィッシング詐欺を防ぐ Trade Title の仕組みを持つだけでなく、攻撃や災害に対して強くかつ復旧が簡単に行える構造を持っている。加えて、災害などの有事に備え、最低限のサービスを保証するための オフライン処理に対応していることも大きな特徴である。紐付けによるサービストリガーとして既存サービスの ID もそのまま利用できることで、スムーズな既存システムからの移行も可能となっている。さらに、社会システムでは欠かせない本人の持つ権限の一部を委譲することなどを実現できる仕組みを備える。

VRICS は個々のサービス間の連携を保ちながら、サービスごとに独立したセキュリティを実現した社会情報基盤であり、サービスの OS とした位置づけにある。

第６章　検討（VRICS を用いた自治体向け社会情報基盤）

第１章～第 4 章において政府が検討している「国民 ID 制度」及び「社会保障・税の番号制度」について具体的に説明した。本章では、これら政府の施策を受け、自治体でどのような対応を行っていくべきか、VRICS を用いた自治体向けシステムに求められる機能について説明する。

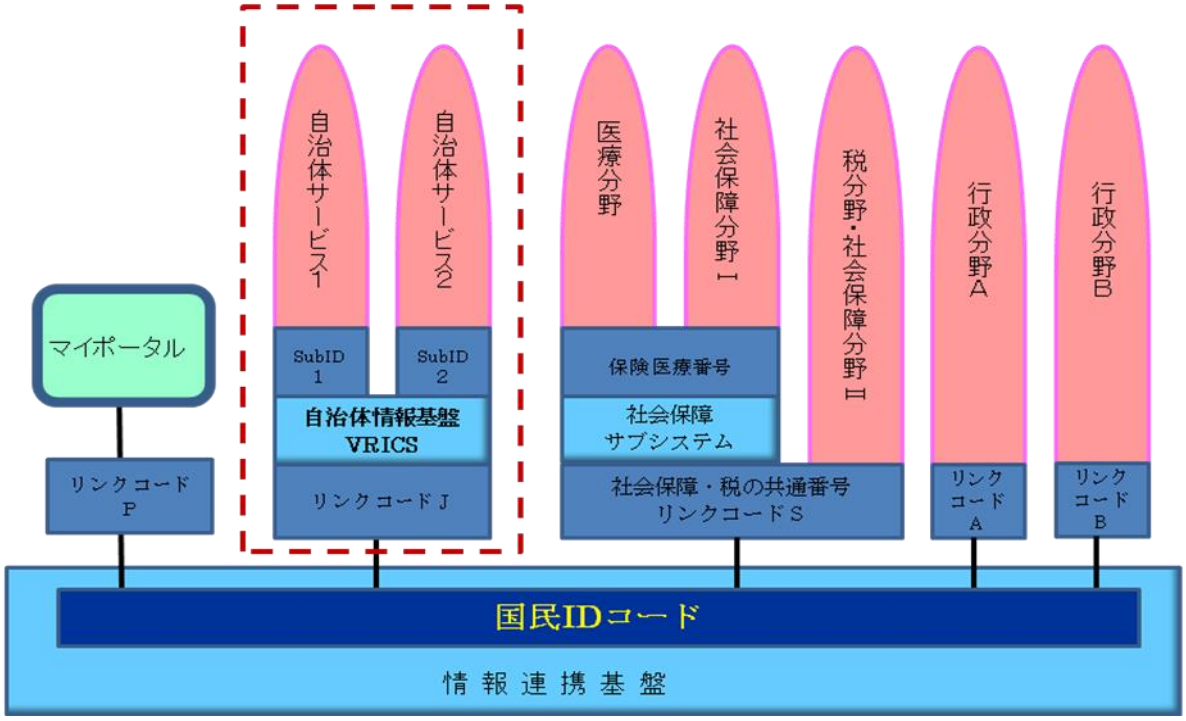
6.1　「国民 ID 制度」への対応

3.2 節で、「国民 ID 制度」の構造について説明した。しかし、4.4.1 節で説明した様に情報提供ネットワークシステムで取り扱う情報は、法定業務と限定している。このため、自治体が独自で行う住民サービスは法定業務には含まれないものも多くあり、また社会保障で取り扱われる医療情報の連携なども法定業務ではないことにより、情報提供ネットワークシステムにて情報連携できないこととなる。加えて、社会保障で取り扱われる医療情報には個人の生命・身体・健康等に関わる情報をはじめ、特に機微性の高い情報が含まれていることから、現行の個人情報保護法成立の際、特に個人情報の漏洩が深刻なプライバシー侵害につながる危険性があるとして医療分野等の個別法を検討することが衆参両院で付帯決議されている。これらのことより、各分野においても個別の情報基盤が必要と考えられる。社会保障分野では医療関係者で閉鎖している医療情報を扱う HPKI 文書の先頭（Healthcare Public Key Infrastructure：保健医療福祉分野公開鍵基盤）と言われる情報基盤が存在する。これと同様に、法定業務以外の情報を取り扱う情報基盤（社会保障サブシステム）を設けることとしている。また、自治体においても同様の問題があり、独自の情報基盤を設ける必要がある。

図６－１に、この考えに合わせ図３－１の構造をより詳しくした構造図を示す。

4.1 節で説明した様に、行政分野 A および行政分野 B は情報提供ネットワークシステムと、それぞれリンクコード A およびリンクコード B で連携している。また、4.2 節で説明した様に、マイ・ポータルはリンクコード P で情報提供ネットワークシステムと連携する。社会保障・税の分野は共通番号が用いられ、リンクコード S で情報提供ネットワークシステムと連携するが、医療分野と一部の社会保障分野は社会保障サブシステム上に構築されることになる。厚生労働省では、この社会保障サブシステムでは保険医療番号（仮称）を新しく付番する方向で検討されている。また、この社会保障サブシステムでは、同じ行政分野であり、目的外の番号を利用することはないため、個人情報の分散管理をする必要が無いため、厚生労働省では、情報連携の標準方式の 1 つである SAML と ID-WSF を使用する方針である。SAML と ID-WSF は情報関連技術の標準化団体である OASIS（Organization for the Advancement of Structured Information Standards）が提唱している情報連携の方式である。4.1.3 節で説明した様に、情報提供ネットワークシステムではデータの連携は、アクセストークン方式を用いるため、実際の情報は情報提供ネットワークシステム上を通ることはない。しかし、この社会保障サブシステムでは実際のデータもこのサブシステムを通過することとなる。

自治体にも複数のサービスがあり、自治体の情報基盤上にこれらの自治体サービスが構築されている。この自治体の情報基盤と情報提供ネットワークシステムとはリンクコードJにて連携されている。この自治体の情報基盤をVRICSで実現するとすれば、各々の自治体サービスはSubIDでサービスされることとなる。この図では示していないが、他の自治体も同様に情報提供ネットワークシステムとリンクコードにて連携される。このため、自治体間の情報連携もこの情報提供ネットワークシステムを通じて行われることとなる。



（図３－１をもとに作成）

図６－１　サブ連携システムを含めた「国民ID制度」の構造

このような「国民ID制度」において、自治体ではどのような事が出来、どのような事を行う必要があるのか、について説明する。

「番号制度」において自治体業務において改善できる点について以下のようなことが考えられる。

・情報入手手続きの簡素化
（例えば、引っ越しに係る自治体間での所得情報連携、依頼書など書類の省略）
・確認作業に係る業務の簡素化
（例えば、審査事務の効率化、課税資料の名寄せや突合作業の効率化）
・窓口業務の改善
（マイ・ポータルを使用した申請による窓口業務の軽減）

・住民への広報・通知などの周知の方法

（マイ・ポータルを用いた個人宛の通知・連絡による経費削減や周知の徹底）

・給付の適正化

（例えば、重複支給の解消、不正な生活保護受給の防止）

・法人番号導入による効果

（例えば、法人情報の登録作業の軽減、社名・所在地の変更手続きの遅れなどによる不一致の減少、法人情報の迅速な把握）

自治体は、この「国民 ID 制度」や「社会保障・税の番号制度」に対応した情報基盤を用意し、情報提供ネットワークシステムとのインタフェースを備える必要がある。

一方、現在自治体が直面している問題は、2009 年度、2010 年度の 2 ヶ年に渡り行った厚生労働省からの受託事業「社会保障カード（仮称）の制度設計に向けた実証事業」の中で、自治体への聞き取りアンケートから以下のような結果を得ている。

① 業務処理が煩雑、時間がかかる

制度が改定される度に、複雑となり、また必要となる証憑も増え、業務処理も複雑化して、時間を要す。

② 制度の理解に時間がかかる

制度が頻繁に変わり、制度が複雑になるため理解に時間がかかる。

③ 住民へ説明が不可欠

制度を住民に説明し、理解を得る必要がある。このため、職員は制度を詳しく知るだけでなく、住民の疑問にも答えなければならない。

④ 制度やパラメータの変更の対応が大変

制度が改定される度に、システムのパラメータの変更必要となり、変更の手間や費用がかかる。

⑤ なりすましの排除

不正を防止するためには、なりすましの排除が不可欠。

これらの問題点を解決するためには、自治体の情報基盤に、前述の「国民 ID 制度」や「社会保障・税の番号制度」への対応に加え、以下のような要求を加える必要がある。

・課を超えた情報連携した業務（重複業務の削除）

・制度を判り易く表示する手段

・住民に制度を周知させる手段の導入

・柔軟なシステムによる容易なパラメータ変更

・なりすましを防ぐ仕組み（認証技術）が必要

ここに上げた要求は自治体の中での情報連携を行い、自治体独自のマイ・ポータルのような機能を備え、セキュリティを持った柔軟なシステムが要求されていることを示している。つまり、「国民 ID 制度」で実現する情報提供ネットワークシステムやマイ・ポータルに似たシステムが必要である。つまり、自治体の情報基盤では、政府の情報提供ネットワークシステムへの接続、自治体のマイ・ポータル、および IC カードの検討が重要となる。同時に自治体の情報基盤においても、「国民 ID 制度」と同様に付番についても検討しなければならない。さらに、自治体では多くの法定業務以外の住民サービスもあり、「国民 ID 制度」で検討された IC カードやマイ・ポータルがそのまま使用できるものではない。

6.2　政府情報提供ネットワークシステムへの接続

自治体の情報基盤を「国民 ID 制度」の上で稼働させるためには、情報提供ネットワークシステムとのインタフェースを取る必要がある。

図６－２に自治体のシステムを含めた場合の「国民 ID 制度」の仕組みを図示する。

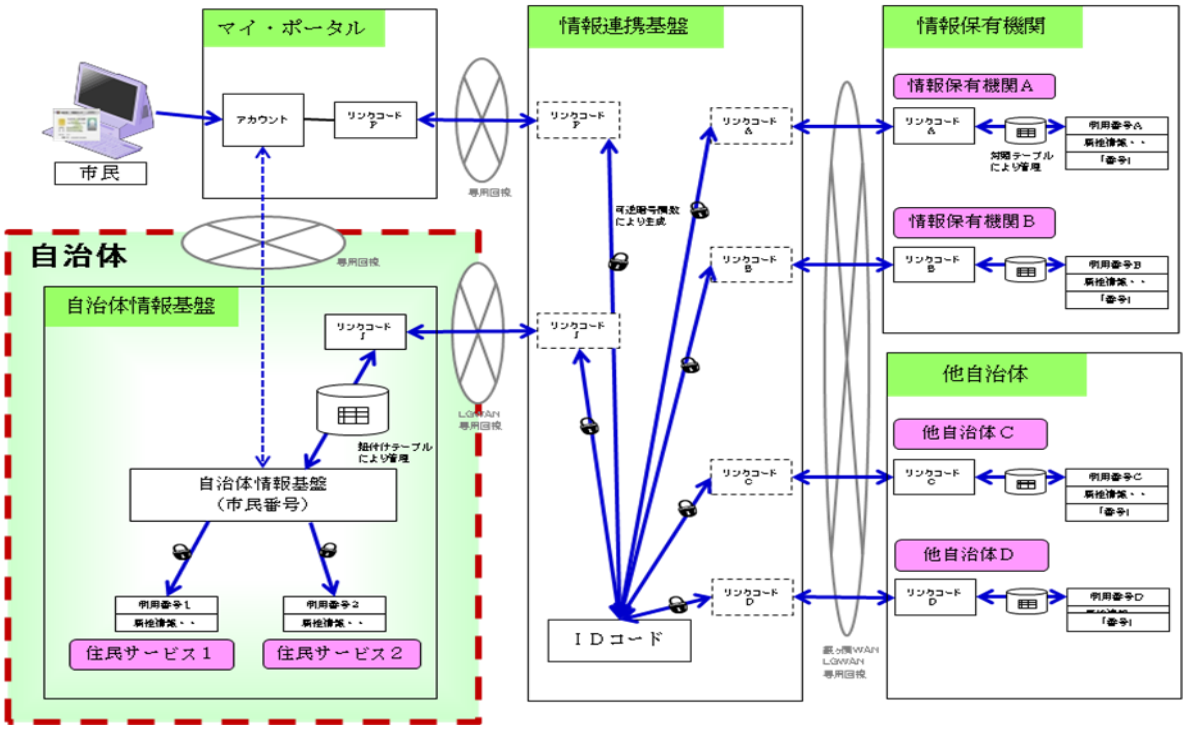


図６－２　自治体のシステムを含めた「国民 ID 制度」

自治体では、住民サービス１や２の様な各々の住民サービスは別々の利用番号でサービスを提供している。4.1 節で説明した様に、自治体と情報提供ネットワークシステムとの連携はリンクコード J にて行われる。このリンクコード J は ID コードから可逆暗号関数を用いて生成される。自治体では、各々の住民サービスとこのリンクコード J を紐付けしておく必要がある

が、サービス毎に各々の利用番号と対照テーブルを作成するには膨大な時間と経費がかかる。

通常、自治体では市民に市民番号を付番し、住民サービスの業務処理を行っている。この市民番号は市民に知らせない番号であり、自治体の業務を円滑に行うための整理番号として、各々の利用番号が紐付けされている。この市民番号とリンクコードJの対照テーブルを作成することで、全ての住民サービスと連携が取れることとなる。

図６－３に、現状のシステムで行った場合の、リンクコードJの取得と市民番号との対照テーブルの作成方法を示す。

ただし、市民番号は個人情報の分散管理の原則より、住民票コードと紐付けされていないとしている。

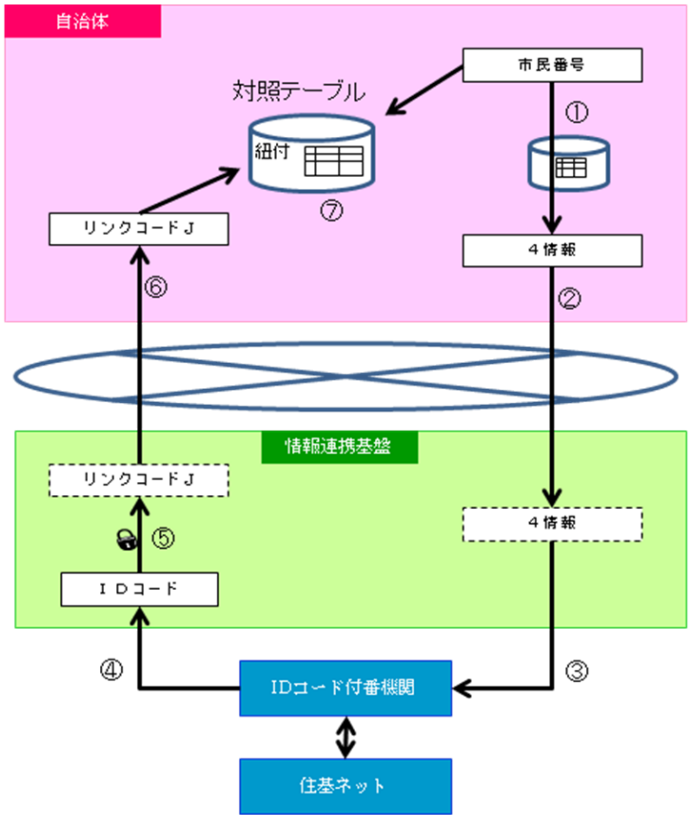


図６－３　現状のシステムでのリンクコードJの取得と対照テーブルの作成

取得方法は以下のようになる。

① 自治体は、対象となる市民番号に紐づいた4情報を抽出。

② 自治体から情報提供ネットワークシステムに対して、4 情報を提示し、リンクコード J を要求。

③ 情報提供ネットワークシステムは ID コード付番機関に対して、自治体から受け取った 4 情報を提示し、ID コードを要求。

④ ID コード付番機関は、情報提供ネットワークシステムに 4 情報に対応した ID コードを提供。

⑤ 情報提供ネットワークシステムは ID コード付番機関から提供された ID コードを可逆暗号関数により、リンクコード J を生成。

⑥ 情報提供ネットワークシステムは、自治体に対しリンクコード J を提供。

⑦ 自治体は市民番号とリンクコード J を紐付ける。

以上のような手続きにより、市民番号とリンクコード J の対照テーブルを作成することが出来る。VRICS を用い、市民番号の付番を検討することで、より簡単な自治体の情報基盤を作成することが可能となる。

図６－４に VRICS を用いて自治体システムを構築した場合の「国民 ID 制度」の構成図を示す。

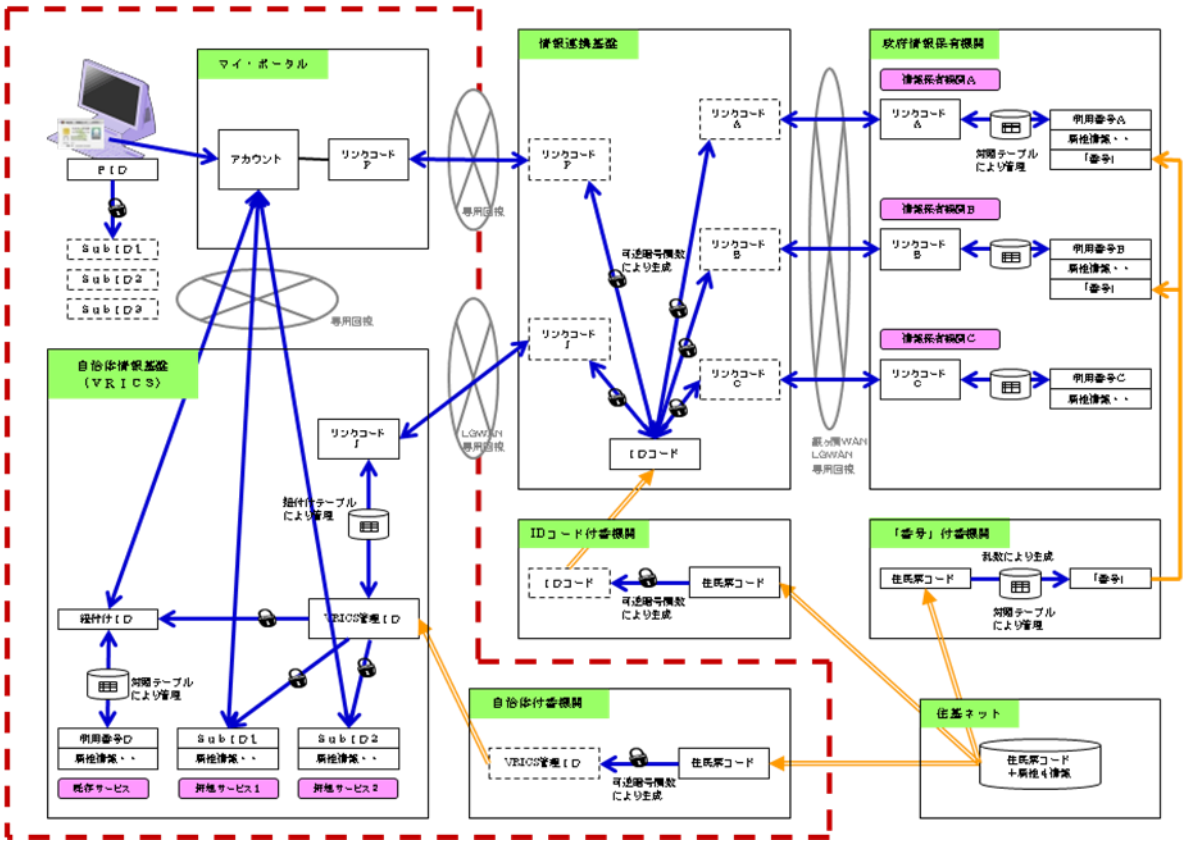


図６－４　VRICS を用いて自治体システムを構築した場合

ここでは、各番号やコードの付番を含めて図示した。自治体には新たに VRICS 管理 ID を付番する機関を設けている。VRICS 管理 ID は現在自治体で使用されている市民番号に代わるものである。VRICS 管理 ID に市民番号を使用することも考えられるが、新しい市民の登録の度、市民番号を台帳管理しなければならなく、新たな住民サービスが増える度に、市民番号と新た

な利用番号との紐付け作業が必要となる。将来の拡張性と、将来の手間を考えると VRICS 管理 ID に市民番号を使用することは適切でない。市民番号として VRICS 管理 ID を新たに作ることを薦める。現在使用している市民番号とは、対照テーブルなどで紐付けも可能であり、業務上の過渡期や既存システムの運用において問題はないが、将来は VRICS 管理 ID を市民番号とすることで、システムの統合が図れ、業務の効率化が進むこととなる。

VRICS 管理 ID の作成方法は、自治体の付番機関にて、住民票コードから可逆暗号関数にて生成することにしている。このことにより、情報提供ネットワークシステムから取得するリンクコード J との紐付けが容易となる。この場合の VRICS 管理 ID とリンクコード J との参照テーブルの作成方法を図６－５に示す。

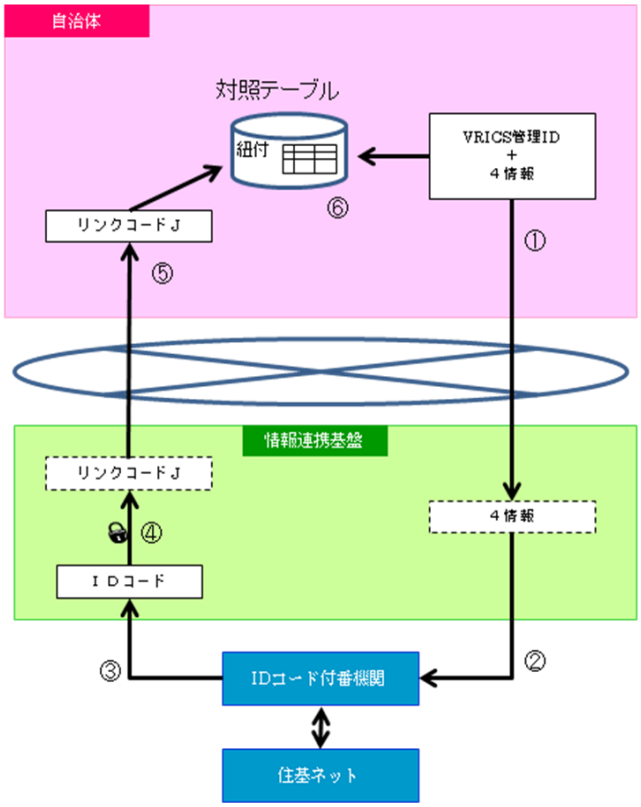


図６－５　VRICS 管理 ID とリンクコード J の参照テーブルの作成

① 自治体は、対象となる VRICS 管理 ID の中から４情報を取り出し、情報提供ネットワークシステムに対し４情報を提示し、リンクコード J を要求。

② 情報提供ネットワークシステムは ID コード付番機関に対して、自治体から受け取った４情報を提示し、ID コードを要求。

③ ID コード付番機関は、情報提供ネットワークシステムに４情報に対応した ID コードを提供。

④ 情報提供ネットワークシステムはIDコード付番機関から提供されたIDコードを可逆暗号関数により、リンクコードJを生成。

⑤ 情報提供ネットワークシステムは、自治体に対しリンクコードJを提供。

⑥ 自治体はVRICS管理IDとリンクコードJを紐付ける。

また、既存する利用番号とVRICS管理IDの紐付け方法を図６－６に示す。

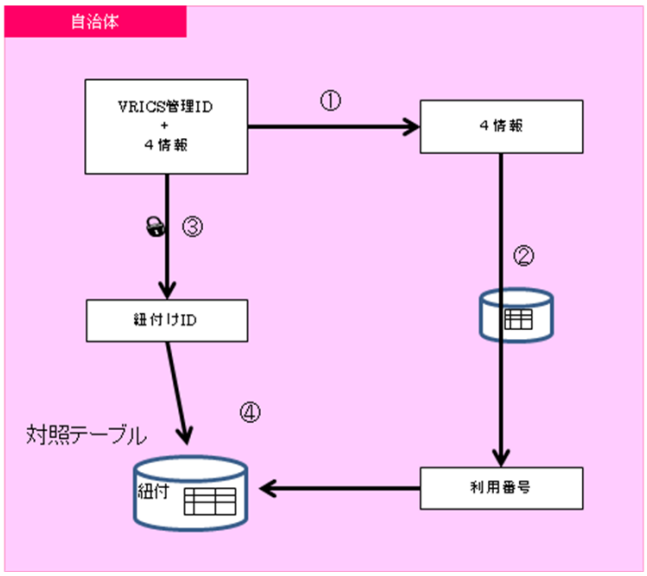


図６－６　既存する利用番号とVRICS管理IDの紐付け

① 対象となるVRICS管理IDの中から４情報を取り出す。

② 利用番号の対照テーブルを用いて利用番号を抽出。

③ VRICS管理IDから、紐付けIDを生成。

④ 紐付けIDと利用番号を紐付ける。

このようにすることで、既存サービスがVRICSの基盤上で利用できることとなる。

6.3　自治体マイ・ポータル

4.2 節では国が用意するマイ・ポータルについて説明した。ここで、情報提供ネットワークシステムでは法定業務のみを取り扱うことより、このマイ・ポータルの「閲覧」・「申請」・「通知」の機能についても法定業務に限定された利用となっていることも説明した。

しかし、自治体においては、法定業務ではない住民サービスも多くあり、住民の福祉に利用されている。今後さらに住民サービスの充実を行う上で、マイ・ポータルの存在は大きい。このため、法定業務以外も扱う自治体独自のマイ・ポータルが必要とされる。このマイ・ポータ

ルは、国のマイ・ポータルとは異なり、住民の生活に溶け込むべきものでなくてはならない。一方、社会保障分野においても、医療情報など個人向けに情報を閲覧できるようにする動きもある。この場合も、法定業務以外であるため、情報提供ネットワークシステムを通らない方法で社会保障マイ・ポータルを開設する必要がある。

図６－７に各々のマイ・ポータルとそれに繋がる情報基盤について図示する。

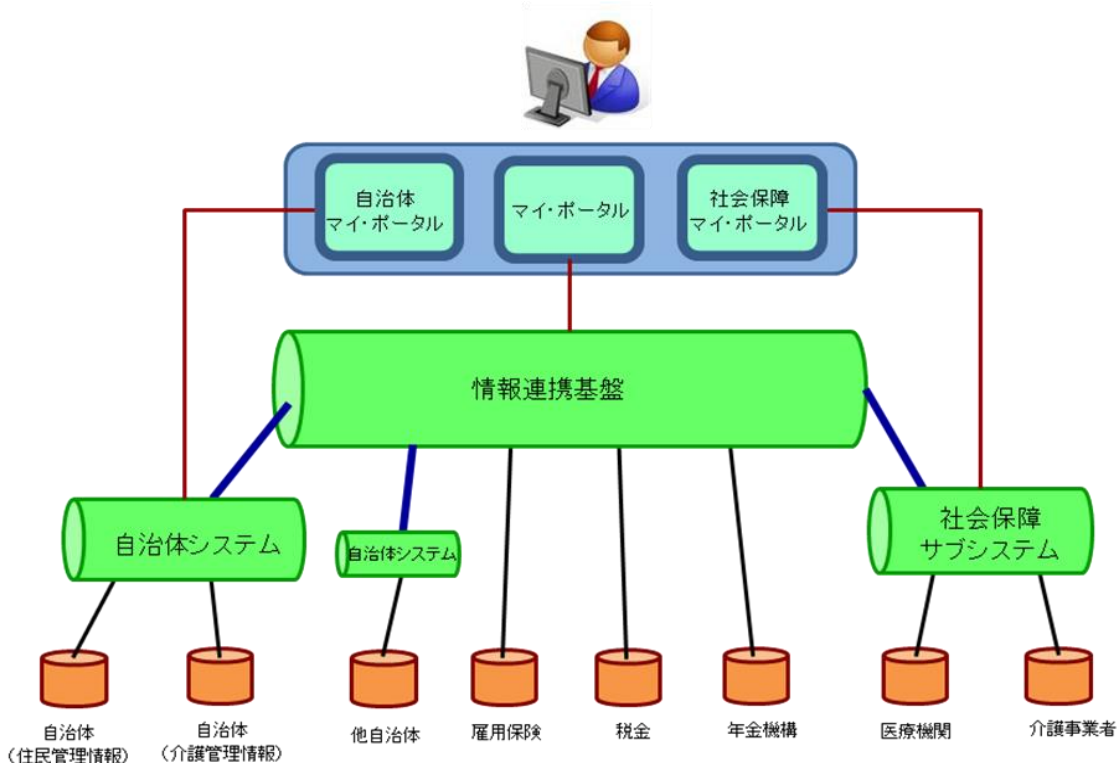


図６－７　マイ・ポータルと情報基盤

情報提供ネットワークシステムには各自治体のシステム、社会保障サブシステムが接続されており、その他国の情報保有機関が繋がっている。マイ・ポータル（国のマイ・ポータル）は、情報提供ネットワークシステムに繋がっており、法定手続きの「閲覧」、「申請」、「通知」の機能と情報連携のログを確認することが出来る。自治体の住民サービスのため、自治体システムに自治体マイ・ポータルが繋がっており、法定業務以外の社会保障（医療等）のために社会保障マイ・ポータルが社会保障サブシステムに繋がることになる。つまり、住民にとって、マイ・ポータルは複数存在することになる。住民サービスとしては、これらの全てのマイ・ポータルを集合させたものとして住民に提供すべきであり、常に住民が使用する自治体マイ・ポータルを窓口とし、これらのマイ・ポータルにログインできるような仕組みが適切である。

また、自治体マイ・ポータルはセキュリティを確保するためにも、VRICS の 1 つのアプリケーションとしての位置づけであることが望ましい。つまり、VRICS の 1 つの SubID に対応してサービスされるべきものである。

6.4　市民カード

VRICS を利用するためには、VRICS 仕様の IC カードが必要となる。一方で、「国民 ID 制度」では、4.3 節で説明した様に、住基カードを改良して使用することにしている。

実際に住民サービスのカードとして利用するためには、利用範囲の狭い住基カードではなく、多目的に市民サービスをカバーしたカード、すなわち市民カードが必要となる。自治体の情報基盤に VRICS を用いた場合にも、「国民 ID 制度」に対応した市民カードとする必要がある。この市民カードを実現するには、住基カードに VRICS 用のアプレットを搭載する方法と、VRICS 仕様の市民カードに公的個人認証を搭載する 2 つの方法が考えられる。各々の方法と、課題について以下に検討する。

6.4.1　住基カードに VRICS 用のアプレットを搭載する方法

住基カードに VRICS 用のアプレットを搭載することにより、「国民 ID 制度」や住基ネットの全ての応用が利用できることとなる。しかし、住基カードに別アプリを載せるためには、法令の変更が必要となる。加えて、住基カードのメモリ容量に余裕が必要となる。以下に特長・利点と、搭載するための条件・課題をまとめる。

（特長・利点）

1．　全ての機能を満足

住基カードに VRICS 用のアプレットを搭載することにより、現在住基カードでサポートされているアプリケーションが全て使用できることとなる。さらに、「社会保障・税の番号制度」で検討されている、保険証として利用など、住基カードの機能アップに基づいた新しい応用についても、サポートされることとなる。

（搭載するための条件・課題）

1．　法令の改正

住基カードに VRICS 用のアプレットを搭載するためには、法令を変更する必要がある。通常市町村が定めたアプリケーションを搭載できるとしているが、今回「社会保障・税の番号制度」の関係で、住基カードに関する法律に搭載アプリがどの程度許されるかは不明である。更に、市町村での条例変更も伴う。

2．　IC カード容量

住基カードに VRICS 用のアプレットを搭載するだけの容量が必要となる。このためには、住基カードに十分メモリ余裕がある IC カードが採用される必要がある。この採

用を決定する機関は、総務省であり、IC カードを申請するメーカは住基カードだけの応用を検討していると考えられるため、十分なメモリ容量を確保した IC カードが準備される可能性は低いと考えられる。

3． VRICS アプリの搭載方法

住基カードの発行時に、同じように自治体窓口で VRICS 用のアプレットを搭載する必要がある。搭載アプリは事前に住基カードに搭載しておくのか、その場で希望を聞いて搭載するのかなど、発行方法を時間や法的手続きなどを検討する必要がある。

4． IC カード OS

住基カードのアプレットと VRICS 用のアプレットを同じ IC カード上で動作させるためには、IC カード OS を住基カードに合わせる必要がある。次期住基カードの仕様では、Global Platform（GP）が採用される公算が大きく、VRICS 用のアプレットもこの Global Platform（GP）上で動作するようにしておく必要がある。

5． 時期

現状の住基カードは「国民 ID 制度」に対応している訳ではない。現在の政府の計画では、当初 2014 年 6 月より配布することになっているが、未だ不明瞭であり遅延することが予想される。どちらにせよ、この時期まで住民にカードを配布出来ないこととなり、IC カードを使った住民サービスはそれ以降となってしまう。住基カードが「国民 ID 制度」に対応するまで、どのように住民サービスを行っていくか別途検討が必要となる。

6． 運用

住基カードに VRICS 用のアプレットを搭載するため、住基カードに合わせた運用が必要となる。例えば、有効期間やカード仕様の変更なども、住基カードに合わせる必要がある。

7． 紛失時の手続き

本来、住基カードであるため、紛失時は住基カードの紛失・再発行の手続きを行う必要があり、VRICS の特長である迅速な再発行の長所が失われる。これを補うためには、一時的な住基カードを用いない VRICS サービスなどを検討し、カード紛失時の迅速な対応を確保する必要がある。

以上のように、住基カードに VRICS 用のアプレットを搭載することが出来れば、機能面では満足できるが、法律面や政府の計画の不確定さや、住基カードに関する制限から、解決すべ

き課題は多く、融通面や確実面に欠けるものと言える。

6.4.2　VRICS 仕様の市民カードに公的個人認証を搭載する方法

VRICS 仕様の市民カードに公的個人認証を搭載することにより、マイ・ポータル（政府のマイ・ポータル）にアクセスすることが可能となる。さらに、e-TAX 等の公的個人認証を使った電子政府アプリケーションの利用も可能となる。しかし、印鑑証明、証明書自動交付や図書館利用などの従来の住基カードのアプリケーションがそのまま使用できる訳ではない。これらのアプリケーションをVRICSにて再構築する必要がある。加えて、社会保障分野で券面情報に「社会保障・税の共通番号」を入れ、目視による「番号」のチェックの機能が果たせなくなる。以下に特長・利点と、搭載するための条件・課題をまとめる。

（特長・利点）

1．　法令の改正が不要

市民カードとして発行するため、住基カードに関する法令に従う必要が無くなり、市町村の条例により発行が可能となる。

2．　市民カードとしての導入

政府の計画に左右されることなく、住基カードの計画とは関係せず、いつの時点でも発行が可能である。また、有効期限や運用についても、自治体独自で決定することが出来る。

3．　容易な発行と停止

市民カードの発行方法についても、自治体で自由に決定でき、発行数量や発行費用などを検討し、発行スキームを決定することが出来る。

（搭載するための条件・課題）

1．　保険証への対応

住基カードを使用しないことになれば、住基カードでサポートされている、また今後サービスをする予定のサービスの全てがサポートできる訳ではない。現状使用されている印鑑証明、証明書自動交付や図書館利用などのサービスは、VRICS にて比較的簡単に再構築は可能である。

しかし、今後計画されている「社会保障・税の番号制度」で 1 つのテーマである保険証に対応するためには、この市民カードを正規の保険証として使用する厚生労働省や保険組合からの認定が必要となる。「社会保障・税番号大綱」では、「保険証機能を券面に「番号」を記載した１枚の IC カードに一元化し、IC カードの提示により、年金手帳、医療保険証、介護保険証等を提示したものとみなすこととすることで、利用者の利便性の向

上を図ることができる。」と記載されている。これは、保険証として使用するためには、券面に「社会保障・税の共通番号（マイナンバー）」を記載する必要があることを示しており、市民カードにどのような手順をとって記載していくかを別途検討しなければならない。

2． IC カード容量

VRICS カードを市民カードとして発行し、そこに公的個人認証を載せるためには、あらかじめ IC カードに、公的個人認証が載せられるだけ領域を確保しておく必要がある。

3． 公的個人認証の搭載条件

公的個人認証を住基カード以外に搭載するためには、その IC カードが、法律で決まっている公的個人認証の搭載条件を満足する必要がある。

公的個人認証の搭載条件は、「電子署名に係る地方公共団体の認証業務に関する法律施行規則」[18]、および「認証業務及びこれに附帯する業務の実施に関する技術的基準」[19]において定義されている。

・電子署名に係る地方公共団体の認証業務に関する法律施行規則」では、

第八条 電磁的記録媒体は、住民基本台帳カードその他の半導体集積回路を一体として組み込んだカード（住所地市町村長の使用に係る電子計算機の操作により利用者署名符号及び利用者署名検証符号を安全かつ確実に記録できるものに限る。）であって、総務大臣が定める技術的基準を満たすものとする」[18]

となっている。

・その技術基準については、「認証業務及びこれに附帯する業務の実施に関する技術的基準」において、

第六条 利用者署名符号及び利用者署名検証符号を記録する電磁的記録媒体は、次に掲げる要件を満たすものとする。

一 電磁的記録媒体が住民基本台帳カードの場合にあっては、公的個人認証サービス利用領域（住民基本台帳カードに関する技術的基準（平成十五年総務省告示第三百九十二号）第１の７に規定する公的個人認証サービス利用領域をいう。）に利用者署名符号及び利用者署名検証符号、電子証明書並びに暗証番号を記録することが可能であること。

二 住民基本台帳カード以外の電磁的記録媒体にあっては、次の要件のすべてを満たすこと。

イ 半導体集積回路上に公的個人認証サービスアプリケーション（住民基本台帳カードに関する技術的基準第１の６に規定する公的個人認証サービ

スアプリケーションをいう。）のための専用の領域を有すること。

ロ イに規定する領域に利用者署名符号及び利用者署名検証符号、電子証明書並びに暗証番号を記録することが可能であること。

ハ イに規定する領域とそれ以外の領域は、電磁的記録媒体の内部でそれぞれ独立し、イに規定する領域以外の領域に搭載されているアプリケーションに係るシステムが、イに規定する領域に情報を記録し、又は当該領域に記録された情報を読み取ることができない仕組みを保持すること。

三 受付窓口端末及び鍵ペア生成装置との間で乱数等を送受信することにより、当該鍵ペア生成装置及び受付窓口端末が正当なものであることを確認するための必要な機能を有すること。

四 前条第六号の規定により暗号化されて送信された利用者署名符号を復号するために必要な機能を有すること。

五 利用者署名符号の電磁的記録媒体の外部からの読み取りを防止するために必要な機能を有すること。[19]

と、定められている。

一般的に、IC カードは CC 認証（Common Criteria）のあるものを採用する必要がある。また、公的個人認証を搭載する専用領域を確保し、他のアプリからアクセスできないようにしたものが必要である。これら搭載には、財団法人・地方自治情報センター（LASDEC）から情報を得、承認を取る必要がある。

4． 住基カードの発行

自治体が独自に市民カードとして発行した場合、国のカードとして住基カードも発行する必要がある。この場合、自治体は IC カードを住民に 2 枚ずつ発行しなければならなく、費用や手間が 2 重となってしまう。自治体の手間と費用を削減する方法を検討する必要がある。

2つの方法を列挙したが、双方に解決しなければならない課題がある。しかし、住基カードに VRICS 用のアプレットを搭載する方法には、法律面や政府の計画、住基カードに関する制限などの、制御困難な要素が多く、見通しが不明であり、自由度に欠ける。また、住基カードに VRICS 用のアプレットを搭載することにより、「現在住基カードでサポートされているアプリケーションが全て使用できることとなる。」と説明したが、住基カードに個別アプリを搭載し、利用している自治体は殆どなく、そのアプリケーションは極めて少ない。

VRICS 仕様の市民カードに公的個人認証を搭載する方法では、住基カードが備えようとするアプリケーションの全てを取り込むことは出来ないと言う欠点はあるものの、課題のほとんどは技術的に解決できるものである。

また、現状でも保険証は別カードで用意されており、このサービスは 2018 年以降スタートとの計画があり、保険証の機能を市民カードに盛り込むだけのために、大きな労力を払うことが良いかどうかを検討する必要がある。

第７章　まとめ

第１章～第４章において、現在検討されている「国民 ID 制度」と「社会保障・税の番号制度」について、制度の内容、その構築方法、および自治体に求められる仕組みを説明した。また、６章において VRICS での実現方法を説明した。本章では、まとめとして、自治体向けのシステム要件をまとめる。

7.1　システム

自治体で構築すべきシステム構成図を図７－１に示す。自治体の認証基盤として VRICS を用い、政府の情報提供ネットワークシステムとリンクコード J を使って認証連携する仕組みである。また、マイ・ポータルにおいては、自治体のマイ・ポータル、政府のマイ・ポータル、およびその他情報保有機関のマイ・ポータルという複合した構造となっており、政府のマイ・ポータルはリンクコード P でリンクされているが政府が用意するものと考えられる。

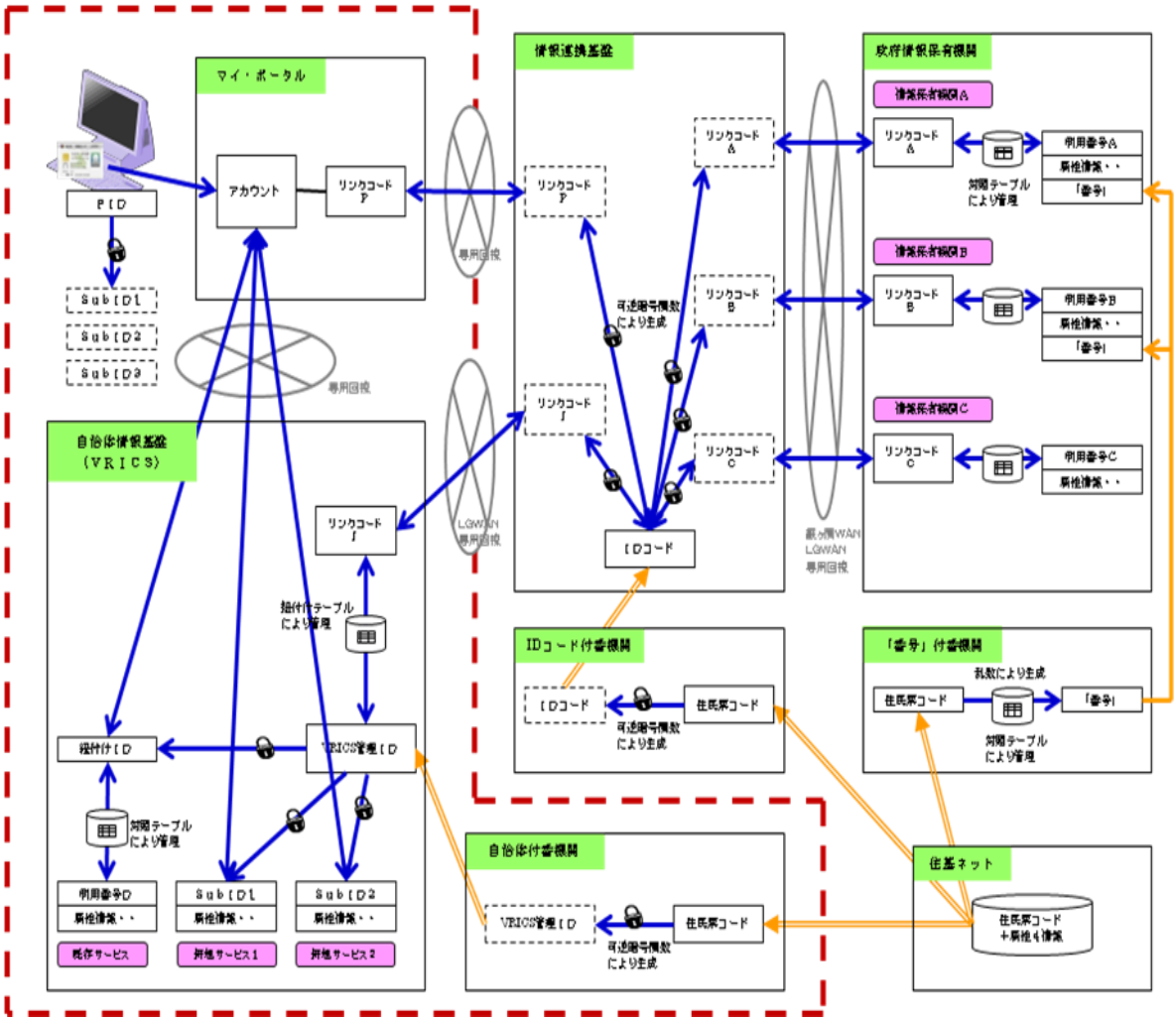


図７－１　VRICS を用いて自治体システムを構築した場合

（図６－４再掲載）

7.2　コード生成

7.1 節で示したシステムを構築する場合のコードの生成方法と各種番号のリンク方法を以下に示す。図７－２に VRICS 管理 ID の生成方法を示す。

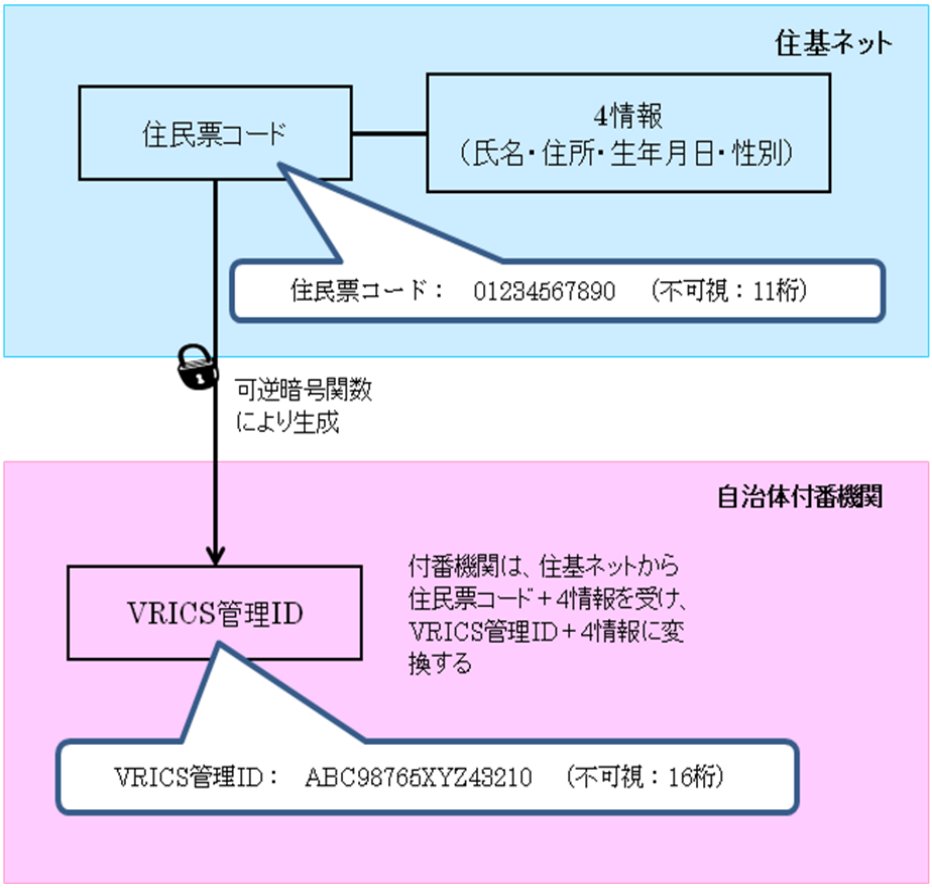


図７－２　VRICS 管理 ID の生成方法

自治体の認証基盤の基本となる VRICS 管理 ID 生成については、住民票コードより可逆暗号にて作成する方法が良い。詳細については 6.2 節で説明しているが、政府が用意する情報提供ネットワークシステムのリンクコードと紐づけるのに容易となるためである。将来は、現在自治体において使用している住民番号に代わり、VRICS 管理 ID を利用していくことを強く推薦したい。ここで説明したコード生成の方法は、ほんの一例であって、この方法以外にも考えられるが、現在考えられている情報提供ネットワークシステムの内容においては、現時点ではこの方法が効率的であると考えられる。

また、図７－３に VRICS 管理 ID とリンクコードの紐付け方法、図７－４に VRICS 管理 ID と住民番号との紐付け方法を示す。

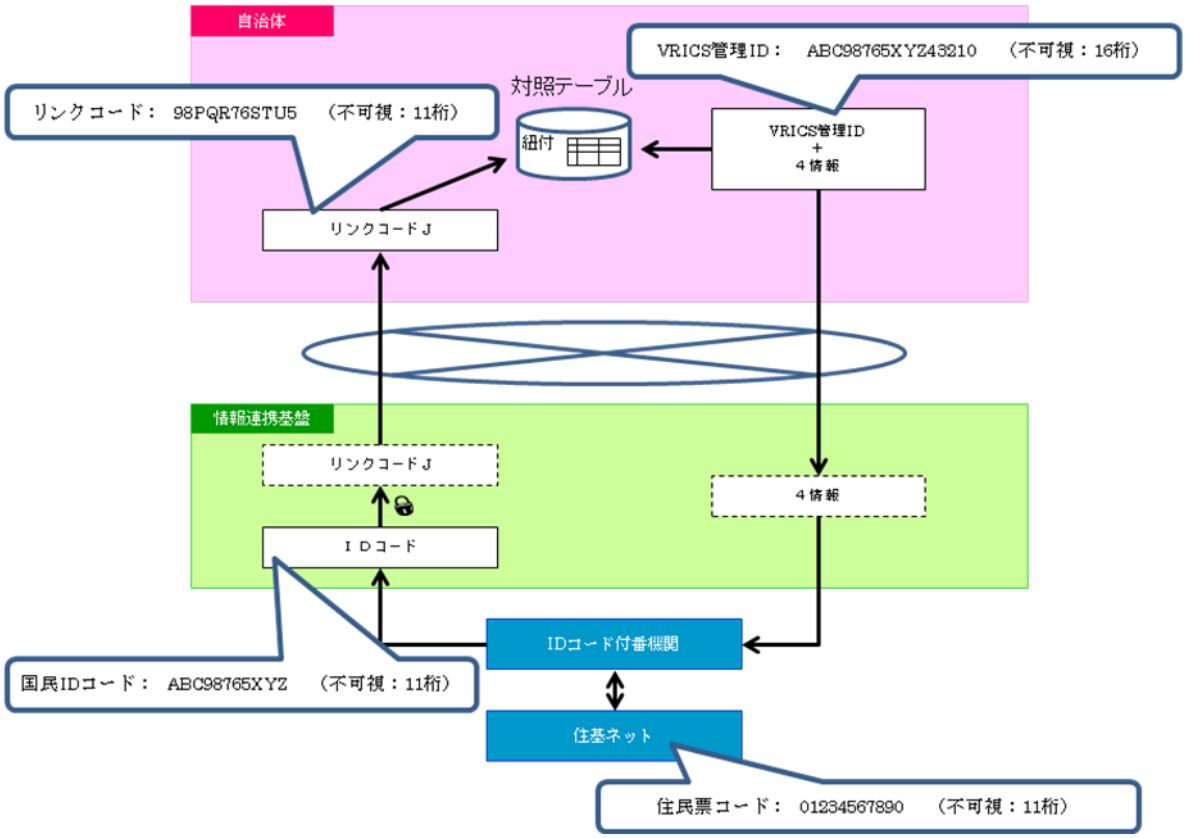


図７－３　VRICS 管理 ID とリンクコードの紐付け方法

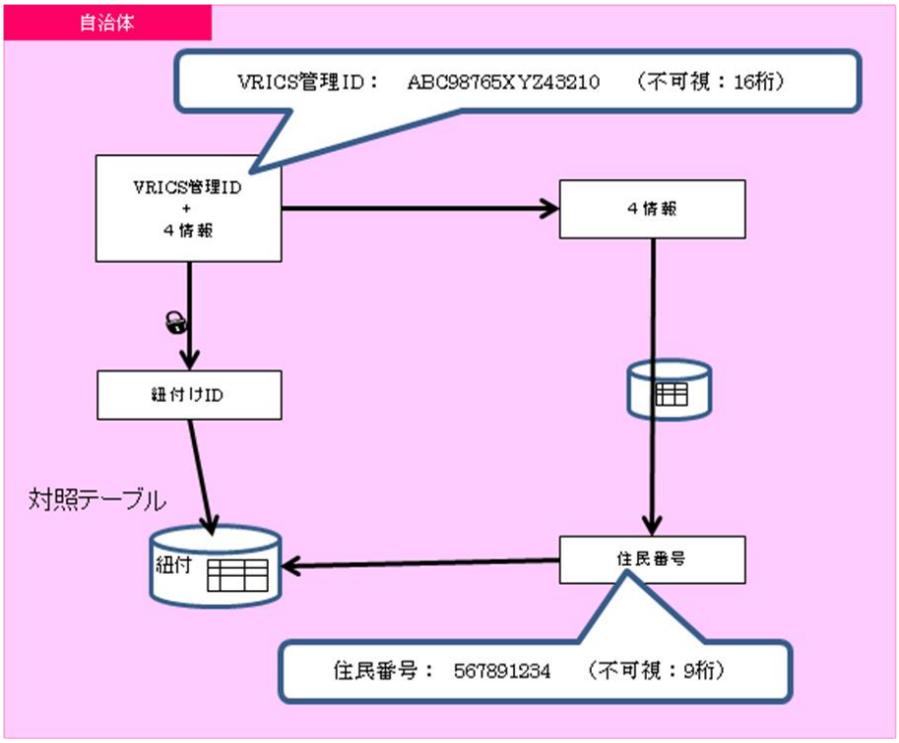


図７－４　VRICS 管理 ID と住民番号との紐付け方法

これらのリンク方法においても、ここに示したものは一例である。理論上では、図７－５や図７－６に示すように、VRICS 管理 ID を逆変換し、住民票コードに戻し、紐付け出来れば、更に容易なリンク方法となるが、現行の法律では住民票コードで名寄せを行ってはいけないとのことになっているため、4 情報を使わざるを得ない。もし、住民票コードが利用できるならば、図７－５や図７－６に様な方法が望ましい。

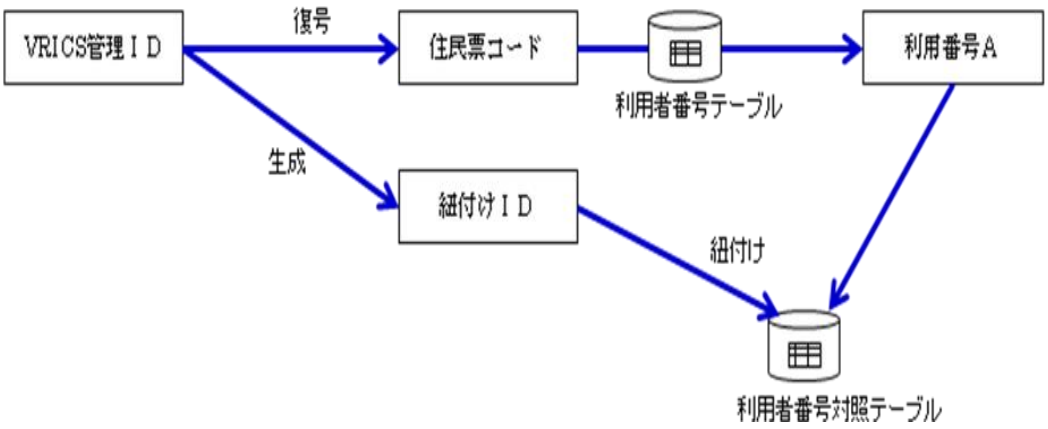


図７－５　住民票コードによる VRICS 管理 ID とリンクコードの紐付け方法

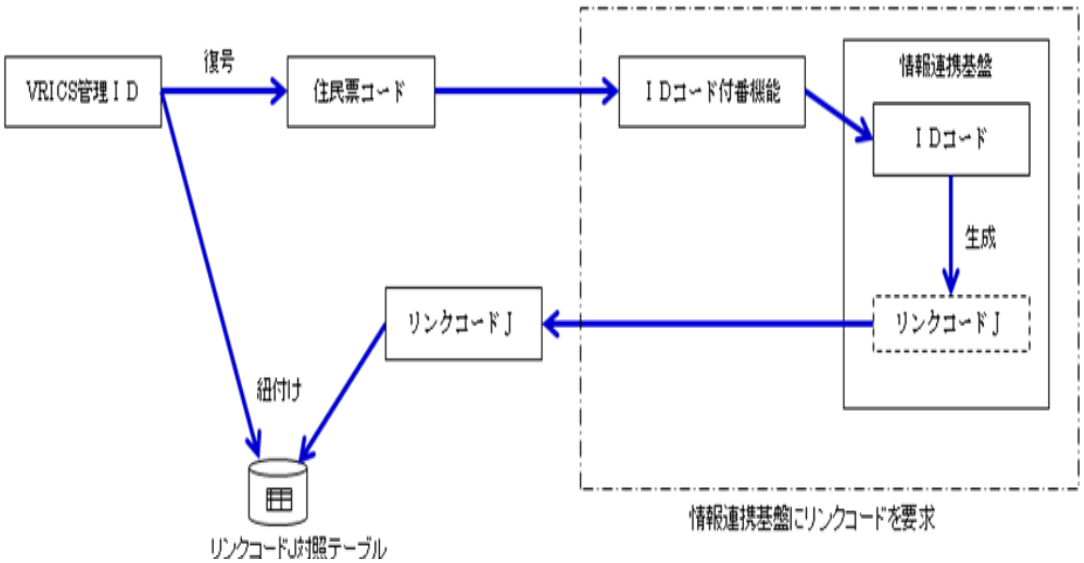


図７－６　住民票コードによる VRICS 管理 ID と住民番号との紐付け方法

つまり、現行法においては、図７－３と図７－４を使用することになる。

7.3　マイ・ポータル

マイ・ポータルについては、政府が提供するマイ・ポータルとは別に、自治体のマイ・ポータルを作る必要がある。マイ・ポータルは、情報提供ネットワークシステムに付随して提供されるマイ・ポータル（この章では政府マイ・ポータルと仮称する。）と情報保有機関が独自に提供するマイ・ポータル（この章では省庁マイ・ポータルと仮称する。）と自治体が提供するマイ・ポータル（この章では自治体マイ・ポータルと仮称する。）が提供される可能性がある。6.3節においてこの点に触れ、説明した。図６－７にイメージ図を再掲載する。

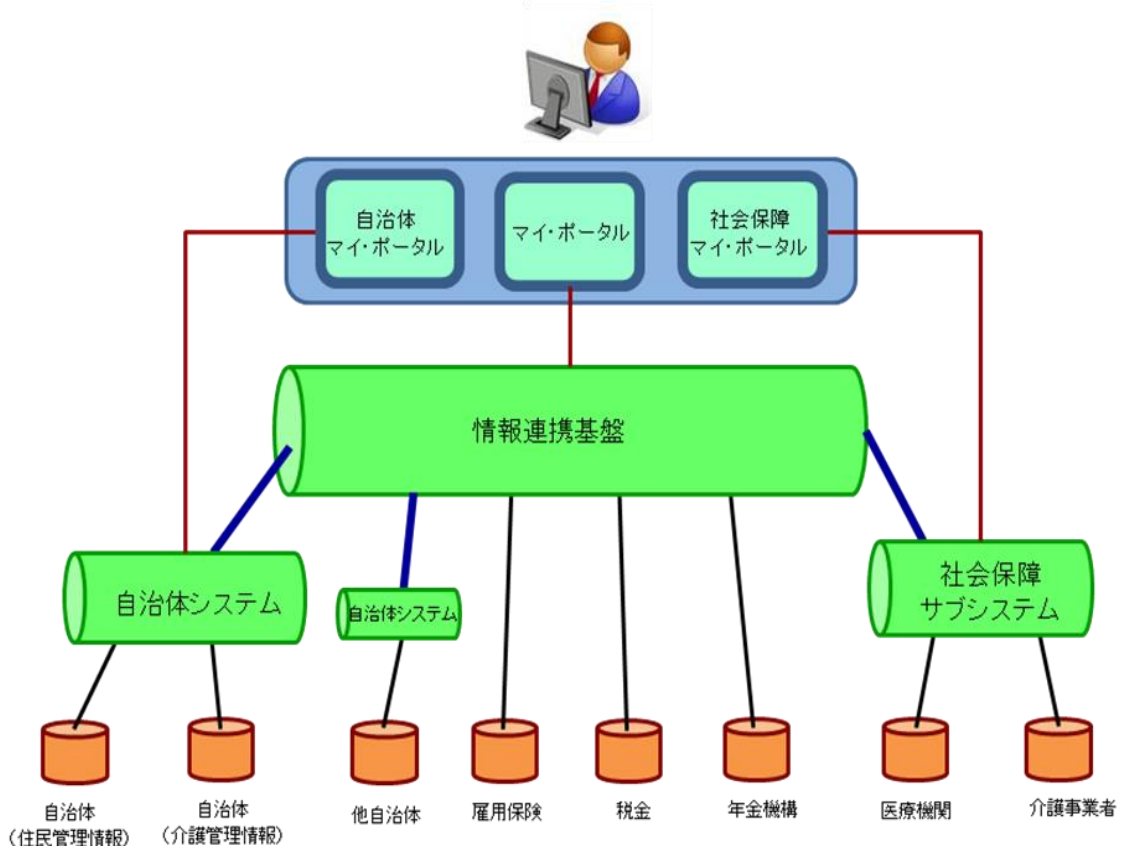


図７－７　マイ・ポータルのイメージ

（図６－７再掲載）

図７－７において、図中の自治体マイ・ポータルはここで言う自治体マイ・ポータルを、図中のマイ・ポータルは政府マイ・ポータルを、社会保障マイ・ポータルは省庁マイ・ポータルと言う位置付けにある。さらに、様々な情報保有機関からも他の省庁マイ・ポータルが作成されることも考えられる。

このような状況において、日常住民が使うマイ・ポータルが住民サービスの一番の窓口になけ

ればならないことを考えれば、自治体マイ・ポータルがその責任を果たさなければならない。図７－８にマイ・ポータルのイメージ図を示す。

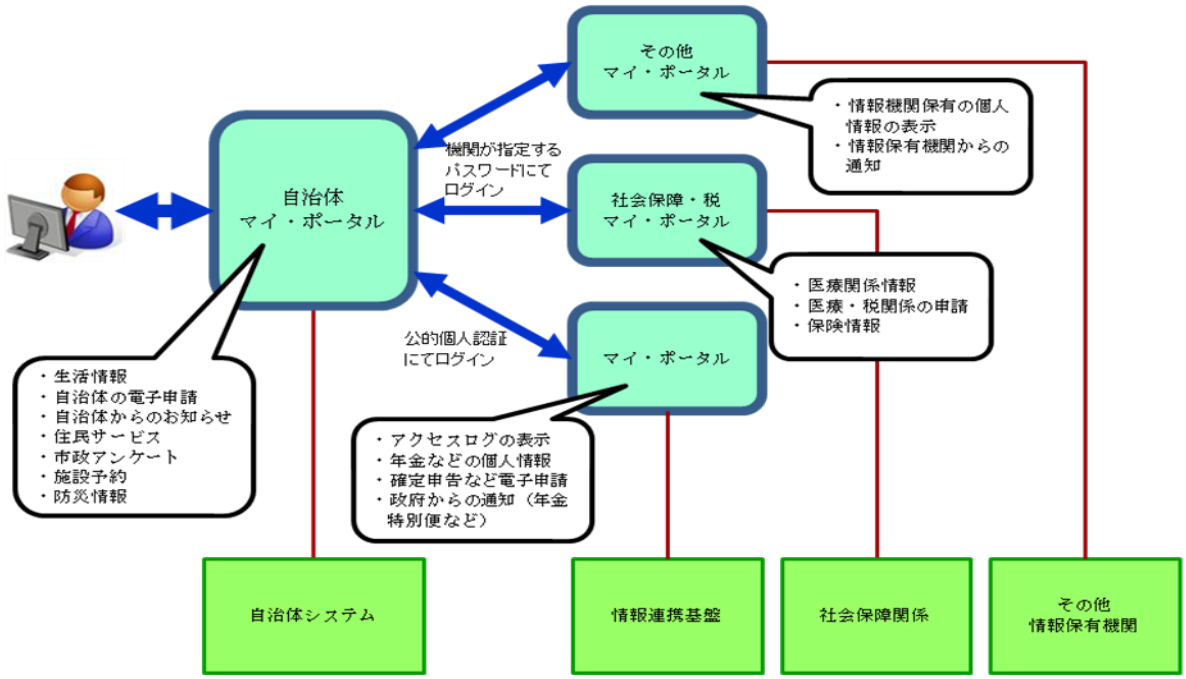


図７－８　マイ・ポータルのイメージ

また、自治体の認証システムが VRICS にて構築される場合、自治体マイ・ポータルは、VRICS の 1 つのアプリケーションとして作成されるべきと考える。この自治体マイ・ポータルへのログインは、その住民サービスごとにその機密性を考慮しながら、住民カードによる個人認証やパスワードによるログインなど、住民が利用し易いログイン方法を採用する必要がある。

7.4　IC カード

「番号制度」に用いる IC カードは、住基カードを改良して利用するとされている。　この前提で考えれば、VRICS を用いた自治体の住民カードとして考えられる方式としては、5.4 節で示した、住基カードに VRICS 用のアプレットを搭載する方法（6.4.1 節で説明）、及び VRICS 仕様の市民カードに公的個人認証を搭載する方法（6.4.2 節で説明）のいずれかの方法を採用することになる。

現状の「大綱」に示されている内容と政府の検討を分析すれば、2015 年より開始する「番号制度」においては、当初保険証や年金手帳の機能は搭載されず、IC カードは希望者のみの配布とされる方向にある。また、情報提供ネットワークシステムも法定業務と規定され、IC カードが利用される第 1 の目的であるマイ・ポータルの当面の利用方法は、アクセスログの閲覧だけ

であり、IC カードやそれに搭載する公的個人認証の必要性も大きくないと言えよう。端的に言えば、当初は IC カードすなわち、「番号制度」用に改良された住基カードは、再びタンスカードと化してしまうとも言えかねない。このような状況を鑑みれば、VRICS 仕様の市民カードを先行して配布し、この市民カードに公的個人認証を搭載する方法、つまり 6.4.2 節で説明した方法がより確実なアプローチであると考えられる。

あとがき

現在のところ､情報提供ネットワークシステムの技術的内容は平成 23 年 7 月に内閣官房の情報連携基盤技術ワーキンググループで取りまとめられた「中間とりまとめ」［20］が最終となっている。その後、ここでまとめられた技術仕様をもとに実証実験のためのシステムを構築すべく細部の仕様検討が進められている段階である。

また、国会に提出された「マイナンバー法」では、「情報連携基盤」を「提供ネットワークシステム」、「IC カード：マイカード」を「個人番号カード」と名称が変更された。更に、マイナンバーは｢地方公共団体情報システム機構（機構の設立法案を国会に提出中：LASDEC を解体し再設立）｣にて付番されることが明記され、用途は年金、雇用保険、ハローワーク事務、医療保険、福祉分野、税務分野に加え、被災者生活再建支度金の給付が加えられた。

本考察の中では、「国民 ID 制度」と「社会保障・税の番号制度」の中心的役割を行う情報提供ネットワークシステムと VRICS を自治体の情報基盤として利用した場合の接続について説明してきたが、現在国会に提出中の法案においては、情報提供ネットワークシステムの用途は限定されており、自治体が独自の目的で利用することは許されていない。政府では、民間などでも利用できるように 2018 年を目途に利用範囲の拡大を含めた番号法の改正を計画している。もし、行政以外の住民サービス、自治体間での行政連携、災害のためのバックアップとしてこの仕組みが利用できるようになれば、更に「国民 ID 制度」と「社会保障・税の番号制度」の必要性や、情報提供ネットワークシステムの有効性が発揮できるのではないかと考える。このためには、現在政府で検討している情報提供ネットワークシステムに自由度を取り入れ、拡張性のあるものとしなければならない。同時に、自治体として、住民サービスや地域社会の社会情報基盤の在り方を政府に提案し、政府の仕組みが住民生活に最大限に有効活用できるようすべきである。また、この社会情報基盤として九州大学が開発した VRICS、またその思想やアプローチなどが利用されることを期待する。

参考文献

１．政府・与党社会保障改革検討本部,「社会保障・税の番号制度についての基本方針」,H23,1,31

２．社会保障・税に関わる番号制度に関する事務検討会「社会保障・税番号要項」,H23,4,28

３．政府・与党社会保障改革検討本部,「社会保障・税番号大綱」,H23,6,30

４．内閣官房、情報連携基盤技術WG（第２回）資料３「社会保障・税に関わる番号制度及び国民ＩＤ制度における情報連携基盤技術の骨格案（その１）」,H23,3,4

５．内閣官房、情報連携基盤技術WG（第４回）資料２－２「社会保障・税に関わる番号制度及び国民ＩＤ制度における情報連携基盤技術の骨格案（その２）修正案 」,H23,4,12

６．浜崎 陽一郎, 安浦 寛人, 「PIDを用いた安全な社会システムの構想」, 九州大学大学院システム情報科学紀要, Vol. 7, No. 2, pp. 139-148, Sep. 2002

７．社会保障制度審議会,「社会保障制度に関する勧告」, S25, 10, 16

８．平成２０年３月６日最高裁第１小法廷判決（民集６２巻３号６６５ 頁),「 住基ネットとプライヴァシー 判決」

９．菅野康子,立石尋太郎,花村健一,「情報セキュリティ読本」,独立行政法人 情報処理推進機構,実教出版株式会社,2004,10,16

１０． ISO/IEC 27002:2005 “Code of practice for information security management”

１１． 日本貿易振興機構,財団法人ニューメディア開発協会, シャープ株式会社, 日本電気株式会社「カンボジア政府セキュア通信および政府公的カードにおけるガイドライン」, 経済産業省平成19年度貿易投資円滑化支援事業報告書,H20,3,31

１２． 河本敏夫,「国民ID制度」日経BPガバメントテクノロジー 2010年秋号 pp.25-29

１３． 大山永昭, 内閣官房、情報連携基盤技術WG（第６回）資料３－１「情報連携基盤システムとマイポータルの在り方」,H23,6,30

１４． NPO 日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ「2009年情報セキュリティインシデントに関する調査報告書」,H22,7,1

１５． 日本貿易振興機構,ニューメディア開発協会,九州大学,シャープ株式会社,「貿易投資円滑化支援事業(実証事業)バングラデシュにおける社会基盤確立に向けたマイクロクレジットの電子化に関わる実証実験報告書」,日本貿易振興機構, 2010年２月

１６． 浜崎 陽一郎, 安浦 寛人, 「PIDを用いた安全な社会システムの構想」, マルチメディア, 分散, 協調とモバイル（DICOMO2002）シンポジウム, Jul. 2002

１７． 野原 康伸, 浜崎 陽一郎, 萩原 大輔, 井上 創造, 安浦 寛人, 「PIDを用いた社会システムにおける認証プロトコルの安全性評価」, マルチメディア, 分散, 協調とモバイル（DICOMO2003）シンポジウム, pp.753-756, Jun. 2003

１８．　総務省,「電子署名に係る地方公共団体の認証業務に関する法律施行規則」,H15,9,29
１９．　総務省,「認証業務及びこれに付帯する業務の実施に関する技術的基準」,H15,12,3
２０．　内閣官房,情報連携基盤技術ワーキンググループ,「中間とりまとめ」, H23,7,28