国民 ID 制度とトラスト・フレームワーク

インターネット・アイデンティティとプライバシー保護の観点から

The OpenID® Foundation
Vice Chair
崎村　夏彦（Nat Sakimura）

2010/12/19

For　堀部政男情報法研究会

注：当日のプレゼンテーション資料は、www.sakimura.org にて公開いたします。

【概要】

インターネットでのやりとりが市民の生活に占める割合は年々大きくなっている。

必然的にネット上の人格である「インターネット・アイデンティティ」の重要性もあがってきているが、その性質についてよく理解されないまま現実が進んでしまっているためプライバシー等様々な問題を生んでいる。

本稿では、まずインターネット・アイデンティティの定義、性質からはじめ、プライバシーや情報利用、トラスト・フレームワーク、ガバナンス・フレームワークに関して法学的観点とは別に、(デジタル)アイデンティティ研究の立場から考察する。その上で、2010 年 5 月に IT 戦略本部によって公表された「新たな情報通信技術戦略」で規定された「国民 ID 制度」について検討を行う。

キーワード:アイデンティティ、プライバシー、同意フレームワーク、Governance as a Platform,

アイデンティティ（自我同一性）

人は社会的発達の過程において、多くの他者（集団を含む）と関わり、それらの価値・規範・役割期待などを取得（他者の観点の取得）、それぞれの他者・集団・社会に対する複数の「～としての自分」を獲得する。

例えば，

- 長男（長女）としての自分
- 友人としての自分
- 親としての自分
- 男（女）としての自分
- 会社の一員としての自分
- 日本人としての自分
- ワイン好きな自分
- クラシック音楽好きな自分

などはその典型的な例である。この「～としての自分」あるいは「～として見られたい自分」のことを「アイデンティティ（identity/ID）」と呼ぶ。

> **アイデンティティは相手との関係性（コンテキスト）の中で定義される「～としての自分」「～として見られたい自分」のことである。**

通常我々はこのようなそれぞれの「～としての自分」を意識し、選択しつつ行為し、自らの中でこれらの「～としての自分」を秩序立て統合して自我同一性（ego-identity）を形成している。

プライバシーの尊重

「～としての自分」は、意識的・無意識的に、どのような情報を相手と共有するかを選んでいる[1]。

> **データ・情報の共有は、相手との関係性の中のような、あるコンテキストの中で行われている。**

これは、相手との関係性の価値を高めようとする活動の中で行われている。プライバシーを尊重するということは、この関係性を尊重するということである。

> **プライバシーの尊重とは、ある個人が保とうとしている関係性・コンテキストを尊重することである。**

往々にして、このコンテキストの中からデータ・情報を外に取り出すと、その関係性は阻害される。

たとえば取引先に動物愛護主義者がいたとしよう。その彼女は、毛皮の採取を非人道的だと思っており、毛皮を着る人間に不信感を持っている。一方自分は、プライベートではお気に入りのミンクのコートを持っている。当然このことはその取引先に知られたくはない。しかし、ひょんなことから自分がそのお気に入りのコートを来ている写真が SNS から転載され、取引先に見られてしまって関係性が悪化した。これは、明らかにプライバシーの侵害であろう。

> **あるコンテキストから、本人の同意なしにデータ・情報を取り出し、その関係性を損なうことをプライバシーの侵害という。**

したがって、あるデータ・情報がプライバシーデータだというような主張は成り立たない。例えば、住所情報[2]をとってみよう。自宅でビジネスをしている人にとっては、そのビジネスに伴って住所を広く知ってもらうことはメリットがあり、それを伝えることはプライバシーの侵害にはならない。一方、DV の被害者にとっては、住所を元の夫に知られることは死活問題になる。したがって、住所を公開されることはプライバシーの侵害となる。

> **あるデータ・情報がプライバシー情報であるか否かは、その情報の種類によって規定されるのではなく、その情報が開示・共有されたコンテキストによって規定される。**

現在の日本の個人情報保護法を含む多くの個人情報保護法・条例は、どちらかというとデータ保護法としての側面が強く、プライバシー保護にはなっていないことが多いように思われる。プライバシー保護という側面は、データの種類によって決まる話ではなく、ケースバイケースで判断されなければならないことも多々ある。そのため、紛争

---

1 昨今、ゼロ・プライバシー時代などと言われ、自分の生活や行動をネットに垂れ流す傾向があるが、そういう人にしても多くの場合「放尿・脱糞シーンをネットに流しますか？」と聞かれれば NO と答えるであろう。結局、全部ダダ漏れしていると言っても実際には無意識に選択しているわけで、ゼロ・プライバシーなどではもちろん無いわけである。

2 ここでは簡単化のために、住所＝居所とする。

時にはプライバシーコミッショナーによる裁定のようなものが求められることが多く想定される。諸外国と異なり、日本にはプライバシーコミッショナー制度が無い。今後、プライバシー保護法制の制定と共にコミッショナー制度の制定も求められると言えよう。

プライバシー保護の為には、プライバシー保護法制と、プライバシー・コミッショナー制度の制定が求められる。

同意フレームワーク

したがって、プライバシーを尊重するには、あるデータを別の場所に移そうとするときに本人の同意をとることが必須となる。この同意をとる方法のことを、同意フレームワークという。

> **同意フレームワークとは、情報をあるコンテキストから他のコンテキストに移動する許可を本人から得るための技術的フレームワークのことを指す。**

同意を得る際には、その同意が何を意味しているのかを本人が理解していることが重要である。
この理解が十分でなく、誤解に基づいて同意してしまうことが往々にある。これを錯誤に基づく同意という。同意フレームワークにおいては、その同意が錯誤に基づくものでないことを確認することが重要である。

> **同意を得る際には、本人の理解が得られていることを確認し、それを後に証明できるような形で記録することが重要である。**

逆に言えば、錯誤無効を主張されないためには、どのようなユーザーインターフェイスを持っているべきかということは、同意フレームワークの重要な検討課題である。

> **錯誤無効を産まないようなユーザーインターフェイスは同意フレームワークの重要課題である。**

同意フレームワークの一例としての OpenID®

同意は、対面（口頭）や書面でとることも可能であるが、インターネット上では、コンピュータや携帯電話上のユーザーインターフェイスを通して取得することが有効である。OpenID®は、この同意をとるためのフレームワークとしての一面を持っている。

> OpenID®は、データ提供の同意確認をとるための、フレームワークである。

インターネット上で同意をとり、データを転送するためには、以下のプロセスを経なければならない。

1. 今まさに同意をしようとしているユーザーが、同意を与えうる本人であることの確認（本人確認、「認証」、Authentication）
2. データの内容、転送先、条件の、上記ユーザーによる確認（同意確認、認可、許可、Authorization）
3. データの転送（許可した相手を正しく識別子、その相手だけがうけとれるような形で）[3]（属性転送、Attribute Sharing、Sending Claims）

上記の 1. を「認証」、2. を「許可」と呼ぶことも多い。「OpenID®は認証フレームワークである」としばしば巷間言われるが、これは、上記の 1. に注目した発言である。しかし、OpenID®の本質は、1. 2. 3. すべてを持っていることにある。

OpenID®におけるユーザー同意の流れは以下の図のようになる。

図 1 OpenID®のフロー

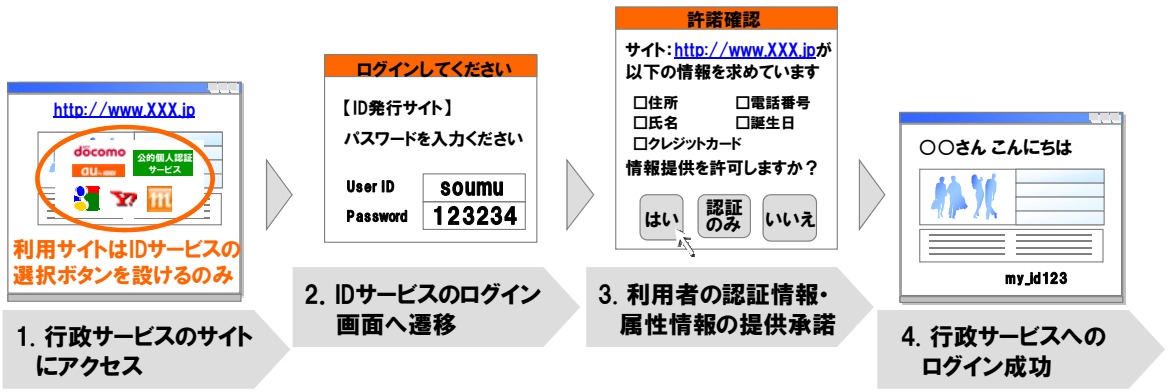


図2,3 は、日本航空において実際に利用されているホテル予約の画面である。これは、OpenID®を使って、ホテル予約に必要な情報を実際に転送するにあたって、ユーザーに同意を求めている画面である。

[3] 相手を正しく識別し、その相手だけが情報をうけとれるようにすることを Audience Restriction という。公開鍵暗号を利用するのが簡便である。

図 2 日本航空における認証画面

図 3 日本航空の OpenID®でのデータ提供同意画面の例

このようにしてデータの提供が行われたさい、誰に、どのような条件で、いつ提供されたのかが記録されるべきで

ある。(個人のレベルではほとんど管理不能であることが分かっている。)図3は、JAL の提供情報管理画面である。

図 4 提供情報管理画面

第三者提供アイデンティティ

OpenID®において、認証を行うサーバーのことを、**Identity Provider (IdP)**ないし、**OpenID® Provider (OP)**という。
IdP は、多くの場合、**属性情報**の提供も行う。
属性情報には「形質」「(狭義の)属性」「嗜好」「関係性」が含まれる。
形質とは、生年月日や性別、眼の色、指紋など、変わらないか、ゆっくりしか変化しないものである。
(狭義の)属性は、形質に比べ変化する速度が早いもので、代表的なものに住所[4]、電話番号、メールアドレスなどの識別子や、位置情報などがある。特殊なところでは、パスワードなども属性情報の一種である。
嗜好は、好きな食べ物、好きな音楽など、好みをあらわすものである。
関係性は、ある店舗の顧客としての関係や、友人関係などがある。昨今話題のソーシャルグラフもこの関係性に含まれる。これらをデジタルに記録しまとめたものが「デジタル・アイデンティティ(Digital Identity)であり、そのうちネットワーク上に存在するもののことを特に「ネットワーク・アイデンティティ(Network Identity)」と呼ぶ。

> **ある存在のデジタル表現した(広義の)属性情報の集まりをデジタル・アイデンティティという。このうち、ネットワーク上に存在するものをネットワーク・アイデンティティと呼ぶ。**

こうした情報を受け取るサーバーのことを、**Relying Party (RP)** という。直訳すれば、依存者である。これは、認証や属性を IdP に「依存」するからこのように呼ばれる。従来型の Web サービスなどでは、RP と IdP は一体であったが、OpenID®のようなシステムでは、これが IdP と RP に分離している。このようなモデルを**「第三者提供アイデンティティ(Third Party Provided Identity)」**という。Third Party Provided Identity の代表例として、OpenID®, SAML, Infocard, Kerberos などがある。

第三者提供アイデンティティ・モデルでは、IdP と呼ばれるサーバーが提供する認証やその他の属性情報を、RP と呼ばれるサーバーが受け取り、何らかのサービスを提供する。IdP と RP が同じ主体に管理されていれば、IdP が提供する情報の信頼度を RP は知っていると言える。しかし、異なる主体が提供している場合、一般的には、IdP が提供する情報がどの程度信頼できるのかを RP が知っているとは言えない。ここに、**情報の非対称性**が存在する。

同様に、RP が受け取った情報を適切に取り扱うと宣言していても、本当にそうかを知ることは、一般的には IdP もユーザー自身も知ることはできない。ここにも情報の非対称性が存在する。情報の非対称性が存在するとき、市場は完全にならず効率的でないため、これを解消ないしは緩和する政策をとることが必要である。

[4]居住地選択の法的および経済上の自由が無い場合、住所はあたかも形質情報であるかのごとき様相を示すが、人口がモビライズされてきている昨今では、住所を形質情報として取り扱うのは適切でない。「基本4情報」といって、住所をあたかも形質情報であるかのごとく扱うのは時代に即しておらず、そのために様々な問題が起きている。

第三者提供アイデンティティのモデルにおいては、ユーザー、IdP、RP 夫々において情報の非対称性が存在し、市場は効率的でない。したがって、この非対称性を緩和する政策が必要である。

この対策として代表的なものが、第三者監査制度である。この制度では、第三者が IdP、RP それぞれについて監査を行ない、その結果を公表することによって、本人申請ベースよりも格段に信頼度を上げるものである。

情報の非対称性の問題を緩和するには、第三者監査とその結果の公表制度を導入することが有用である。

このような監査制度と、次節に述べる契約や紛争解決手段などを備えた体型のことを**「トラスト・フレームワーク」**という。

なお、情報の非対称性の問題の緩和に当たっては、第三者監査制度と共に、「評判情報（Reputation）」の活用が有効である。ここで、評判情報とは、「ある主体がある性質を持っているとする主張の正しさに対する第三者の評価する主観的確率」[5]のことを指す。その意味では、監査結果というのは評判情報の特殊例であると言える。

[5] OASIS Open ORMS TC の定義による。

トラスト・フレームワーク

「第三者提供 ID 情報」の利用を始めると、上記の非対称性の問題に加えて、**責任分界点の決定**とそれを**反映した契約**を結ぶ必要が出てくる。これを個別にやると、対象の主体が N いると、N(N-1)/2 個という膨大な契約が必要になってしまう。これは明らかにスケールしない。これをスケールさせるためには、中心となる契約者一者と契約すれば、全体と契約を行った形になるようにして、必要な契約数を N 個に抑えるべきである。上記の「審査・認定」と、この「統一契約」はセットになるものであり、これを行う者を「トラスト・フレームワーク・プロバイダ」と言う。

> **第三者提供 ID 情報の情報の非対称性、責任分界点の決定、契約のスケーラビリティの課題を解決するための「審査・認定」「統一契約」「紛争解決手段」を備えた枠組みのことをトラスト・フレームワーク、それを第三者として提供する主体のことをトラスト・フレームワーク・プロバイダという。**

これを制度として設置しなければ、ネットワーク上で安心して ID 情報を活用し、経済の発展をはかることは難しい。

> **トラスト・フレームワーク・プロバイダ制度を策定しなければならない。**

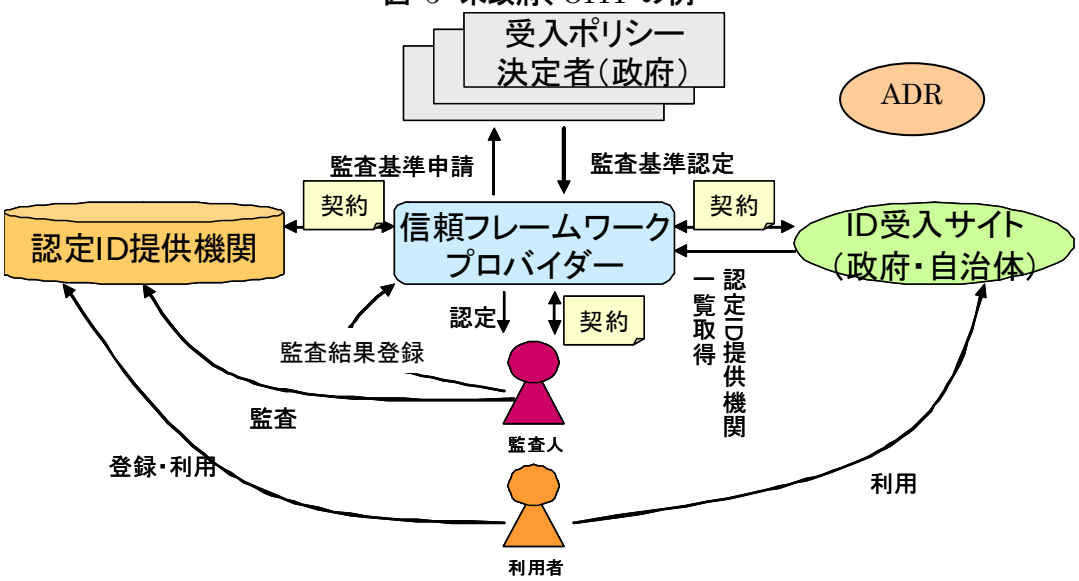
また、この制度のもと、各主体ともに、責任範囲を定め、その範囲での賠償責任があることを認め、実行しなければならない。

> **トラスト・フレームワークで定められた契約に記載された責任分界点に従い、各主体同士で、相互に賠償責任を認め、実行しなければならない。**

このようなトラスト・フレームワークの例としては、米国政府が推進している Open Identity Trust Framework (OITF) がある。具体的な検討の実施にあたっては、ゼロベースで行うよりも、これらの成果を最低限のカスタマイズによって使っていくことが、クロスボーダー時代・クラウド時代には相応しい、「ガラパゴス化・仲間はずれ化」しない方式であると言える。

> **トラスト・フレームワークの検討にあたっては、米政府 OITF の例などを中心に、国際的な流れにできるだけ合致させ、クロスボーダー／クラウド時代に備えるべきである。**

図 5 米政府、OITF の例



（出所）Rundel, et. Al, “The Open Identity Trust Framework (OITF) Model” **をもとに作成**

Governance as a Platform

法律は長年にわたり、社会の基盤をなしてきた。しかし、昨今の急速な技術進化や社会の変化に追随できなくなってきて、社会の基盤たるよりも社会の障害たるケースも散見されるようになってきていると、一部では認識されている。

この原因の一つとして、個別の技術などにあまりにも依存した形で立法が行われていることが多いということがある。たとえば、「印鑑」[6]というものは、日本の法令で多くの場所で用いられているが、現代においては技術的に完全に「危殆化」しており、証明能力は皆無である。にもかかわらず、法令に「印鑑」として指定してあるため、さまざまな課題を産んでしまっている。(そもそも、「印鑑」の定義は何かという問題もあるが。)これは、本来立法時に「印鑑」を用いることによって達成しようとしていた目的を記述し、技術を記述しないことによって回避できた問題である。同様のことは、書証[7]に関しても言える。

こうしたことに鑑み、個別の技術を指定せずに目的ベースで記述し、かつ法や政府の介入を最小化し、法体系をインセンティブスキームを中心としたゲーム論的に再構成しようという考え方も存在する[8]。

一般に、市場が効率的なとき、政府などの介入は資源配分を阻害し、全体の厚生を低下させることが知られている。したがって介入が許されるのは、市場が効率的でなくなる＝市場の失敗が生じている自体ということになる[9]。公平性の観点は、その後である。現代的な法体系を考える際には、こうした考え方も取り入れつつ行われる必要があろう。

6 印鑑の定義はどこでされているのだろうか？
7 書証や書類の定義はどこでされているのだろうか？
8 この考え方は、2010 年 9 月に、Harvard 大学 Berkman Center 主催で Washington D.C. の Cosmos Club で行われた、Governance 2.0 で議論された。いずれにせよ、このあたりのことには、法学者だけでなく、経済学者も入れて議論することが必須であると思われる。
9 厚生経済学の第一基本定理の示唆。そもそも、およそ公共政策にせよ産業政策にせよを考えるに当たって、厚生経済学の基本定理を無視した議論はありえないが、日本の政策立案の現場であまりこれらを聞くことがないのは非常に残念である。

「新たな情報通信技術戦略」と国民 ID 制度

平成22年5月11日、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、本部長：鳩山由紀夫内閣総理大臣）から「新たな情報通信技術戦略」が発表された。国民ID制度はこの中で規定されているものなので、ここから読み解く必要がある。

新たな情報通信技術戦略の構造は以下のようになっている。

図 6 新たな情報通信技術戦略の構造

I. 基本認識
II. 3つの柱と目標
  1. 国民本位の電子行政の実現
  2. 地域の絆の再生
  3. 新市場の創出と国際展開
III. 分野別戦略
  1. 国民本位の電子行政の実現
    (1) 情報通信技術を活用した行政刷新と見える化
      i) 電子行政推進の基本方針を策定
      ii) 行政サービスのオンライン利用に関する計画の策定
      iii) 行政ポータルの抜本的改革と行政サービスへのアクセス向上
      iv) 国民 ID 制度の導入と国民による行政監視の仕組みの整備
      v) 政府の情報システムの統合・集約化
      vi) 全国共通の電子行政サービスの実現
      vii) 「国と地方の協議の場」の活用

ここからまず分かるのは、国民 ID 制度は、国民本位の電子行政の実現の特に行政刷新と見える化のコンテキストで定義されているものであるということである。このあたりが昨今忘れられて、国家戦略室で検討されていた社会保障と税の番号（通称「共通番号」）と混乱した議論が政府内部も含めて展開されているので整理される必要があるのだが、まずはそこに入る前に、基本認識（ビジョン）、3つの柱と目標（大戦略）を見ることにしよう。なぜならば、この路線に乗らない手段はまず今回の議論の対象外となるからだ。

新たな情報通信技術戦略の「基本認識」にみる「ビジョン」

新たな情報通信技術戦略において、「ビジョン」に類するものは「I.基本認識」の中に書かれている。かなり感動的な文章なので、以下に引用する。(下線は筆者による)

> Ⅰ.　基本認識
>
> 情報通信技術革命の本質は情報主権の革命である。政府・提供者が主導する社会から納税者・消費者である国民が主導する社会への転換には、徹底的な情報公開による透明性の向上が必要であり、そのために情報通信技術が果たす役割は大きい。
>
> 国民が主導する社会では、市民レベルでの知識・情報の共有が行われ、新たな「知識情報社会」への転換が実現し、国民の暮らしの質を飛躍的に向上させることができる。
>
> 今回の情報通信技術戦略(IT戦略)は、過去のIT戦略の延長線上にあるのではなく、新たな国民主権の社会を確立するための、非連続な飛躍を支える重点戦略(3本柱)に絞り込んだ戦略である。また、これは、別途策定される新成長戦略と相まって、我が国の持続的成長を支えるべきものでもある。
>
> このため、戦略の実施に当たっては、これまでの関連政策が効果を上げていない原因を徹底的に追求し、IT戦略以外の各政策との連携、関係府省間の連携、政府と自治体との連携、政府と民間との連携等を具体的に進め、新たな国民主権の社会が早期に確立されるよう、国を挙げて、強力に推進する。

(出所)IT 戦略本部　新たな情報通信技術戦略

つまり、こういうことだ。

> 【ビジョン】情報主権革命を通じ、情報主権を政府・提供者から納税者・消費者である国民へ転換、市民レベルでの知識・情報の共有を通じた新たな「知識情報社会」への転換を実現し、国民の暮らしの質を飛躍的に向上させる。

そして、これを実現するための基本的な手段が

> 【戦略】IT の活用による徹底的な情報公開による透明化

国民 ID 制度について考えるとき、上記を常に念頭において置かなければならない。

> 国民 ID 制度は、国民情報主権の確立と、知識情報社会への転換に資するものでなければならない。

国民本位の電子行政の実現

さて、上記の実現のためにどうするかといいうのは、「II. 3つの柱と目標」に「「国民主権」の観点から、まず政府内で情報通信技術革命を徹底し国民本位の電子行政を実現する。」と記載してある。この「国民本位の電子行政の実現」だが、その内容として記載されているのは以下の項目である。

○ 2020 年までに国民が、自宅やオフィス等の行政窓口以外の場所において、国民生活に密接に関係する主要な申請手続や証明書入手を、必要に応じ、週 7 日 24 時間、ワンストップで行えるようにする。この一環として、2013 年までに、コンビニエンスストア、行政機関、郵便局等に設置された行政キオスク端末を通して、国民の 50%以上が、サービスを利用することを可能とする。

○ 2013 年までに政府において、また、2020 年までに 50%以上の地方自治体において、国民が行政を監視し、自己に関する情報をコントロールできる公平で利便性が高い電子行政を、無駄を省き効率的に実現することにより、国民が、行政の見える化や行政刷新を実感できるようにする。

○ 2013 年までに、個人情報の保護に配慮した上で、2次利用可能な形で行政情報を公開し、原則としてすべてインターネットで容易に入手することを可能にし、国民がオープンガバメントを実感できるようにする。

(出所)IT 戦略本部　新たな情報通信技術戦略

そして、そのための重点施策として以下のことが記載されている。

III. 分野別戦略

1.国民本位の電子行政の実現

(1) 情報通信技術を活用した行政刷新と見える化

【重点施策】

○ 行政サービスの中で、利用頻度が高く、週 7 日 24 時間入手できることに よる国民の便益が高いサービス(例:住民票、印鑑証明、戸籍謄抄本等の 各種証明書の入手等)を特定し、それらをオンライン又は民間との連携も 含めてオフライン(例:行政キオスク端末)で利用できるようにする。

○ 社会保障の安心を高め、税と一体的に運用すべく、電子行政の共通基盤として、官民サービスに汎用可能ないわゆる国民 ID 制度の整備を行うとともに、自己に関する情報の活用については、政府及び自治体において、本人が監視・コントロールできる制度及びシステムを整備する。

○ 電子行政推進の実質的な権能を有する司令塔として政府 CIO を設置し、 行政刷新と連携して行政の効率化を推進する。その前提として、これまで の政府による情報通信技術投資の費用対効果を総括し、教訓を整理する。 その教訓にもとづき、上記施策を含め、電子行政の推

進に際しては、費用 対効果が高い領域について集中的に業務の見直し(行政刷新)を行った上 で、共通の情報通信技術基盤の整備を行う。クラウドコンピューティング 等の活用や企業コードの連携等についても、その一環として行う。

(出所)IT 戦略本部 新たな情報通信技術戦略

ようやく「国民 ID 制度」が出てきた。

この(1) 情報通信技術を活用した行政刷新と見える化は前述のとおり、

i) 電子行政推進の基本方針を策定
ii) 行政サービスのオンライン利用に関する計画の策定
iii)行政ポータルの抜本的改革と行政サービスへのアクセス向上
iv)国民 ID 制度の導入と国民による行政監視の仕組みの整備
v)政府の情報システムの統合・集約化
vi)全国共通の電子行政サービスの実現
vii)「国と地方の協議の場」の活用

(出所)IT 戦略本部 新たな情報通信技術戦略

によって行われることになっているわけだが、「国民ID制度」に関しては、この「iv)国民ID制度の導入と国民による行政監視の仕組みの整備」でようやく詳細が語られる。

v)国民 ID 制度の導入と国民による行政監視の仕組みの整備

社会保障・税の共通番号の検討と整合性を図りつつ、個人情報保護を確保し府省・地方自治体間のデータ連携を可能とする電子行政の共通基盤として、2013 年までに国民 ID 制度を導入する。併せて、行政機関による運用やアクセスの状況を監視する第三者機関の創設、公的IC カードの整理・合理化を行う。また、インターネットを通じて利便性の高いサービスを提供するため、民間 ID との連携可能性を検討する。 さらに、各種の行政手続の申請等に際して、既に行政機関が保有している情報については、原則として記載・添付が不要となるよう行政 機関における適切な情報の活用を推進するとともに、行政機関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。【内閣官房、総務省、財務省、文部科学省、厚生労働省、経済 産業省等】

(出所)IT 戦略本部 新たな情報通信技術戦略

上記から以下の「国民 ID 制度の要件」がわかる。

国民 ID 制度の10要件

1. 国民 ID 制度は、政府・提供者が主導する社会から納税者・消費者である国民が主導する社会へと情報主権を逆転させるもので、政府の徹底的な透明化に資するものでなければならない。（基本ポリシー。これに反するものは、以下のいずれに合致しても受け入れられない。）
2. 国民 ID 制度は、官民サービスに汎用可能な制度であり、個人情報保護を確保し府省・地方自治体間のデータ連携を可能とする電子行政の共通基盤である。
3. 国民 ID 制度は、個人情報の保護を徹底するものでなければならない。
4. 国民 ID 制度は、政府及び自治体における自己に関する情報の活用を本人が監視・コントロールできる制度及びシステムでなければならない。
5. 国民 ID 制度の実施にあたっては、行政機関による運用やアクセスの状況を監視する第三者機関の創設しなければならない。
6. 国民 ID 制度の実施にあたっては、公的 IC カードの整理・合理化を行う。
7. 国民 ID 制度の実施にあたっては、インターネットを通じて利便性の高いサービスを提供するため、民間 ID との連携可能性を検討しなければならない。
8. 国民 ID 制度では、各種の行政手続の申請等に際して、既に行政機関が保有している情報については、原則として記載・添付が不要となるよう行政機関における適切な情報の活用を推進しなければならない。
9. 国民 ID 制度では、行政機関が保有する自己に関する情報（アイデンティティ情報）について、国民が内容を確認できる仕組みを整備しなければならない。
10. 国民 ID 制度は2013年までに導入されなければならない。

ここに至るも「国民 ID」なる「番号」は現れてこないことに注意すべきである。巷の報道などでは、「国民 ID」として番号議論が行われているが、ここでは一切論じられていない。逆に述べられているのは、

○ 官民汎用可能なデータ連携基盤
○ 行政監視の仕組みとその一環としての自己情報へのアクセス基盤
○ インターネットからのアクセスに関しては民間 ID との連携を模索する

ということであって、番号やコードなどの識別子は二義的なものである。（存在しないで上記を実現できるならば存在しなくて良い。）

国民 ID 制度の検討

これで、国民 ID 制度を検討する準備が整ったので、以下に順次検討してゆく[10]。

最初に、大前提として、以下を掲げる。

> **厚生経済学の第一基本定理にのっとり、民間に任せられるところはできるだけ民間に任せ、市場の失敗が生じるところだけ政府が介入する。**

また、新たな情報通信技術戦略より、以下も大前提となる。

> **導入される制度は、国民の情報主権を確立するものでなければならない。**

まず、機能面で言うと、国民 ID 制度は官民汎用可能な自己情報（Identity Attributes）のデータ連携基盤である。しかも、先に定義した意味でのプライバシーを徹底しなければならない。

> **国民 ID 制度は官民汎用可能な、プライバシーに配慮した自己情報（Identity Attributes）のデータ連携基盤である。**

上述のように、日本にはプライバシー保護法制は無いから、これを制定するとともに、官民汎用可能にするためには、個人情報保護法もオムニバス方式に転換することが求められる。これは、独立したプライバシー・コミッショナーによって監督されなければならない。

> **個人情報保護法のオムニバス方式への転換とプライバシー保護法制の制定が必要である。その監督機関および ADR 機能としてプライバシー・コミッショナー制度の確立が必要である。**

また、データ連携基盤のネットワークは、官民汎用であるから、インターネットへの接続が前提と考えて良いだろう。実際のデータ連携基盤自体は、大きなデータベースを設けて、そこを皆がアクセスする中央集権モデルと、個々の業務システムが独立して存在し、API[11]提供をしている分散モデルが考えられるが、事前にすべてのデータ項目を予想することは困難であるし、オーソリテーティブなソースは原理的に一箇所にはならない。各所のオーソリテーティブなソースからデータを集めたとしても、その正統性をプライバシーに配慮した形で証明するのは難しい[12]。その上、一箇所に集めてしまうとそこが巨大な攻撃誘引場所になってしまって危険だ。したがって、後者の分散型をとるべき、というかそれしか選択肢は無いだろう。

---

10 以下は、現時点での筆者の仮説であり、今後検証されてゆくべきものである。
11 今からやるなら REST API であろう。
12 ゼロ知識証明を使った u-prove のような技術もあるが、一般化にはまだちょっと早いと思われる。

データの配置モデルは分散型でなければならない。

情報の連携の許可は、法令によるものと本人の同意に基づくものの2種類が必要であろう。法令に基づくもののだけだと、情報の連携に柔軟さを欠く。本人同意に基づくものは、前述の JAL の事例のような形で良いだろう。
一方、法令に基づくものは、許可された取得項目についてプライバシー・コミッショナーが署名をした「情報要求ファイル」に基づいて情報要求をすべきであろう。こうすることによって、個々のシステムが勝手に要求項目を増やすことが出来なくなる。JAL の事例では、要求者が自分で署名したファイルを提出していたが、法令に基づくものは、これにプライバシー・コミッショナーも同時に署名しているような形が良いのではないだろうか。

情報の連携の許可は、法令によるものと本人の同意に基づくものの2種類が必要。前者については、プライバシー・コミッショナーの署名した許可証を必要とするものにする。

データを返す側は、要求した人・システムだけに確実に渡るようにしなければならない。そのためには、要求者の公開鍵で内容を暗号化して送信するのが確実である。公開鍵は、上述の要求ファイルに入れておくのが妥当であろう。

データの転送に際しては、受け取り手の公開鍵を利用して暗号化して送ることによって Audience Restriction するのが妥当である。

また、こうして提供されたデータは、出し手と受け手でスキーマが共有されていることが前提になる。したがって、スキーマの標準化が必要である。これに関しても、今後はクロスボーダーが増えてくることに鑑み、できるだけ国際標準[13]に則り、足りない部分は国際的な標準化の提案を行ってゆくべきである。

データのスキーマは標準化されなければならない。今後のクロスボーダー社会を鑑みると、これは国際標準化されなければならない。

要求する対象の人を特定するには、その識別子が必要だ。これは、情報の要求システムと提供システムが同意した任意の識別子で良いが、地方自治体の現状を鑑みると住民コードなどがよさそうに見える。また、個別の各システムも識別する必要がある。これらの各システムは第三者によって署名されたファイルによって識別されるべきである。識別子だけではなりすましが簡単なので不可である。

識別子は参加者間で同意が取れていれば良いが、その正統性を証明できる形で存在しなければならない。現状では、識別子、公開鍵のセットを信頼された第三者によって署名するのが妥当に思われる。

[13] ISO や ITU-T である必要はない。当面 OASIS Open、IETF, OpenID Foundation などのフォーラム標準で十分であろう。

ユーザーの自己情報アクセスについては、自宅やモバイルからのアクセスと、カウンターやキオスクなどからのアクセスが考えられる。後者については IC カードなどを認証手段(クレデンシャル)に使うことも考えられるが、前者では難しい。実態ベースで考えても、官の配布している公的個人認証は6年で約1%の普及率しか獲得できなかったし、さらにそれの利用は芳しくない。これに鑑みると、諸外国に習い[14]、競争による効率性の実現を勘案し、認定された民間発行になるクレデンシャルを用いたアクセスを提供すべきであろう。

図 7 海外電子政府比較[15]

	エストニア	ベルギー	韓国	オーストリア	デンマーク	スウェーデン	フィンランド	日本
人口(万人)	約134万人	約1,058万人	約4,846万人	約823万人	約551万人	約918万人	約532万人	約1億2,715万人
発行枚数(年)	約105万枚 (2009)	約850万枚 (2008)	約1,790万枚 (2008)	約10万枚 (2007)	約134万枚 (2009)	約230万枚 (2009)	約24万枚 (2009)	約146万枚 (2009)
人口普及率 ＊注1	約80%	約80%	約37%	約1%	約24%	約26%	約5%	約1%
証明書の取得	義務 (15歳以上)	義務 (12歳以上)	任意 (半強制＊注2)	任意	任意	任意	任意	任意
発行機関	民間	行政、民間	民間	行政	民間	民間	行政、民間	行政
導入年	2002年	2003年	1999年	2004年	2003年	2002年	1999年	2004年
証明書格納場所	ICカード、(SIMカード?)	ICカード	ICカード、その他ハードウェア、ソフトウェア証明書	ICカード、ハードウェア証明書	ソフトウェア証明書	ハードウェア・ソフトウェア証明書	ICカード、SIMカード	ICカード
発行方法	対面	対面	対面	対面	対面不要	ハードウェア証明書の場合、対面	対面	対面
電子証明書	署名・認証 各1枚	署名・認証 各1枚	署名・認証兼用	署名用2枚	署名・認証兼用	署名・認証 各1枚	署名・認証 各1枚	署名用1枚

*注1:人口普及率は、人口に占める、発行枚数の割合

(出所:電子政府推進対応 WG 報告書(案))

ユーザーアクセスは、マルチデバイス、マルチロケーション、24時間を前提とすべきである。そのためのクレデンシャルとしては、民間発行のものの利用を推進すべきである。

また、クレデンシャルについては、「大は小を兼ねる」と称し、常に最も強いクレデンシャルを要求する事例が日本ではまま見られるが、これはユーザビリティを削ぐだけでなく、錯誤による重大な同意を行ってしまうことがありえるなど、セキュリティ的にも危険である。我々は普段「実印」「銀行印」「認印」と使い分けているが、常に「実印」を使っていると、認印を必要とする書類の山に、悪意の攻撃者が重大な契約書を紛れ込ませておき、それに実印を押させてしまうというような攻撃がありうる。これは危険であるから、業務のレベルに応じたクレデンシャルをユーザーに提示し選択させるようにすべきである。このレベルを「保証レベル(Level of Assurance)」といい、国際的には4つのレベルに分類することが多い[16]。こうしてレベル分けしてみると、個人が電子政府を利用するに当たっての手

14 そもそも、官発行・官配布のクレデンシャルなど、日本くらいしか無い。このモデルは、皮肉にも現在ロシアなどから注目されているらしい。

15 フィンランドでは、この表のとおり finid の普及には失敗した。現在は3つの銀行が発行する ID を電子政府でも利用しているとのこと。

16 日本においても、平成22年8月31日に同様の趣旨の文書が各府省情報化統括責任者(CIO)連絡会議 から

続はほとんどの場合「認印」かせいぜい「銀行印」レベルであることがわかる[17]。常に最高レベルのクレデンシャルを利用させるのが安全だというのは、責任を利用者側に押し付けることによって、提供者側が安全になるということでしかなく、国民情報主権の基本理念に反する。

クレデンシャルは適切なレベルのものを選択して使用できるようにし、必要以上のレベルのものを要求してはならない。

また、住民基本台帳をもとに最高レベルのクレデンシャルを発行するとしている主張もあるが、これは少なくとも短期的には実施不能である。その理由は:

× 日本においては身元確認が最高レベル(Level 4、実印レベル)で国民全体を網羅したデータベースは存在しない[18]。
× 身元確認プロセス[19]の標準化も行われていない。
× バイオメトリクス情報を取得してカードを大規模に発行するインフラも免許証以外には無い
× 身元確認がもともと済んでいる韓国やドイツでも8年から10年がかりの大事業である。まして、身元確認を含んでだと、ヘタをすると20年がかりの大事業となる。

これらの理由から、

レベル4のクレデンシャルの発行を悉皆的に行うことはあくまで長期的な課題として、短中期的には、別の方策を探らなければならない。

この「エコシステム」の参加者は多数になる。前述のとおり、情報のやり取りには契約ベースのものも含まれることになるので、それぞれの参加者の責任分界を明確化しなければならない。この契約関係をスケールさせるには、トラスト・フレームワークの設置は必須である。また、第三者提供情報の信頼度に関する非対称性を緩和する上でも、トラスト・フレームワークの設置は必須である。

契約関係のスケーラビリティ確保および情報の非対称性の緩和のために、トラスト・フレームワークを設置しなければならない。

「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」として出ている。一般的に参照されるのは、米国 NIST の SP800-63 Rev.1 である。また、ISO/ITU-T においても、X.eaa としての標準化が進んでいる。

[17] 筆者の経験上、海外の政府担当者と話しても、基本的に市民が直接利用する行政手続に高セキュリティなものは無いというのが一般的な意見である。確定申告についても、日本では電子署名を要求しているというと、「なぜ？意味不明」との答えが一般的である。

[18] よく韓国を参照する論があるが、韓国では指紋などの生体情報を含むデータベースが完成していた。そこからスタートしても、人口普及率4割弱にいたるまでに7年を要している。ドイツも同様であるが、eID の配布は10年計画である。日本は前提となるデータベースすら存在しないから、少なくとも10年はかかると考えたほうがよかろう。

[19] ニュージランド政府やカナダ・ブリティッシュコロンビア州の Evidence of Identity Standard (EOI Standard) などを参考にすべきであろう。

また、市民による行政へのアクセスを待つだけでなく、行政から市民に情報他をプッシュする必要があることがままある。このような場合、これまでは郵便制度に根ざす「住所」に大きく依存してきた。たとえば、通知書を送ったり、現金書留を送ったりなどである。しかし、現代では郵便以外にも email や携帯電話など様々な連絡手段が存在しており、市民の立場からしてもそちらのほうが望ましい場合が多い。また、金銭に関しては銀行他の口座のほうが望ましいであろう[20]。これらより、国民 ID 制度では、ユーザーの email、(携帯)電話番号などの電子的連絡手段および銀行口座などの振込み手段を行政に登録する形が望ましいであろう。これらは全国民が持っているわけではないという主張もあろうが、これらを持てない社会的弱者には、行政が責任を持ってこれらを渡すべきであり、何らかの事情で使いたくても使えないという場合には、適切な例外処置をとれば良い。老人には ICT は難しくて使えないなどという議論もされるが、これは90年代にすでに「ウソ」であることが分かっている。このあたりは、ジェロンテクノロジー[21]の専門家と検討すればいくらでも解決策があるはずである。こうして老人などにも通信機能付き端末がとどけられれば、それは「見守り機能としても機能するので、「安全・安心」社会の成立のためには利点が多い。

現在の住所偏重から、email や携帯電話、銀行口座など、より現代に即した手段に転換しなければならない。これらを持てない社会的弱者には、社会保障の一環として、これらを与えるようにすべきである。

ここに述べたことはあくまで議論の出発地点としての仮説である。今後、経済学的、法学的、社会学的、技術的観点から精査されてゆかなければならないことは言うまでもない。

参考文献

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)「新たな情報通信技術戦略」2010 年 5 月
総務省 「電子政府推進対応ワーキンググループ最終報告書(案)」2010 年 10 月
各府省情報化統括責任者(CIO)連絡会議 「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」2010 年 8 月
Rundel, et al., “The Open Identity Trust Framework (OITF) Model”, 2010 年 3 月
Sakimura, et al., “ORMS Reference Model, Use-cases & Requirements”, 2009 年1月
New Zealand The Department of Internal Affairs, “Evidence of Identity Standard”, 2006 年 6 月
Burr, et al., “Electronic Authentication Guideline NIST SP800-63-1”, 2008 年 12 月
Bolten, “E-Authentication Guidance for Federal Agencies OMB M04-04”, 2003 年 12 月

[20] フィンランドでは、政府に対して振込み口座の登録制をとっている。フィンランドの税に占める手数料のたぐいは 0.8%と極めて低額であり、日本でも参考にすべきと思われる。
[21] 高齢者のための生活支援技術