# デジタル時代の社会基盤「デジタルID」

調査部　主任研究員　野村　敦子

目　　次

## 要　約

1．デジタルIDについての定義は様々あるが、デジタルの世界で使われる身分証明の方法と位置付けることができる。インターネットやスマートフォンの普及に伴い、官民のサービスのデジタル化・オンライン化が進展するなか、オンライン上で本人を特定し、安全かつ簡便に取引を行うための手段として、デジタルIDが不可欠となっている。また、個人を一意に識別可能なデジタルIDにより、金融や医療、教育などの公共サービスを広く社会に行き届かせることが可能であり、社会包摂を進めるためのツールとしても重要性が高まっている。その一方で、デジタルIDは機微情報に紐付けられる可能性があることから、プライバシーや人権の侵害、IDを通じた監視社会の到来などに対する懸念も膨らんでいる。

こうした状況下、世界各国ではデジタルIDの導入が進められており、世界銀行によれば、2014年現在、197カ国中148カ国が何らかの形で公的なデジタルIDを導入している。このうち、わが国の参考になる先進国の事例として、民間のIDスキームを活用するスウェーデン、政府が主導するシンガポール、基礎的な基盤（識別子）が未整備のため試行錯誤するイギリスの3カ国を事例として取り上げた。

2．スウェーデンでは、銀行業界のコンソーシアムにより開発されたBank IDが公共サービスでも使われており、普及率は80％を超える。高い普及率の背景には、公共調達の手続きによりデジタルIDを選定する仕組みがあること、IDの識別子となる個人識別番号が官民の様々なサービスで既に利用されていること、国民のデジタルリテラシーや政府に対する信頼が高いこと、などスウェーデン固有の事情が指摘できる。Bank IDは、日常的に利用する銀行のデジタルIDが統一され、公共サービスでも利用できることや、スマートフォンアプリが導入されていることなどから、利用者にとって利便性が高く、対応するサービスも増加するという好循環が生まれている。一方で、①単一IDプロバイダーへの過度の依存はリスク、②イノベーションや品質、価格面での競争が不在、③移民や銀行口座のない個人などが排除、などの問題点が指摘されている。そこで政府に対し、国民IDカードにデジタルIDの機能を搭載することが提案されている。

3．シンガポールは、スウェーデンとは対照的に、国が主導してNDI（国家デジタル認証）と呼ぶ官民共通のデジタルIDスキームの開発・普及を推進している。NDIは、識別子となる個人登録番号（NRIC番号）と既存の公的認証システム「SingPass」、個人情報の登録・利用の一元化サービス「MyInfo」を基盤とし、市民が単一のデジタルIDで官民のサービスを利用できる共通認証プラットフォームの構築を目指すプロジェクトである。NDIイニシアチブの一環として、2018年にスマートフォンの生体認証を利用するSingPass Mobileが始まり、2019年には公的身分証明書（NRICカード）を見せなくても本人確認と必要な個人情報を提供可能とするSG Verifyが導入された。企業は、独自のインフラやシステムを構築しなくても、政府が提供するNDIの共通APIや各種ツールを使って認証基盤を導入することが可能となり、コスト削減や安全性の強化に繋がる。一方で、中央集権型のシステムであるためトラブルが発生すると機能不全となる事態や、民間企業の採用が想定通りに進むか、といった課題がある。

4．イギリスでは、2000年代に入ってテロ対策や犯罪予防等の観点から、厳格に本人確認できる手段として国民IDカードの導入が議論された。2006年にはIDカード法が成立したものの、費用対効果やプライバシー侵害等が問題視され、政権交代とともに同法は廃止された。この代替策として、2016年に公共サービスの共通認証プラットフォーム「GOV.UK Verify（Verify）」が導入された。オンラインで公共サービスを利用するにあたり、政府の認定を受けた複数のIDプロバイダーのなかから、利用者自身が使用する認証サービスを選択する仕組みである。もっとも、Verifyは当初の計画通りには普及が進んでいない。その理由として、ユーザーエクスペリエンスが不十分であることや、関係する省庁が必ずしも協力的ではないこと、民間サービスプロバイダーの求める要件を満たすものではないことなどが指摘されている。政府は、2019年に省庁横断的にデジタルIDを推進する組織を設置し、Verifyに代わる新たなデジタルIDの在り方を検討している。もっとも、識別子となる統一的な国民番号がないことが課題として指摘されている。

5．各国の事例を見ると、デジタルID導入の経緯や制度の枠組みは、それぞれの歴史や社会の成り立ち、政府と国民の関係性などが深く影響しており、取り組む内容や発展経路は異なっている。もっとも、各国ともに、デジタルの世界で個人が主張する本人であることや正当な資格・権利を有することを証明するためには、信頼性の高いデジタルIDスキームの構築が不可欠との認識に立つ。その実現に向けて、以下の課題への対応―①技術面（デジタルIDシステム自体）の課題：セキュリティの強化、識別子の存在、ユーザビリティの実現と、安全性・利便性のバランスの確保、②社会的な課題：プライバシーの保護と社会包摂の追求、身元検証者と利用者（国民）との間の信頼関係の構築、③運用上の課題：国民生活に密着したサービスでの利用、そのための官民間はもとより政府内、民間内での協力体制の整備―が求められる。

6．先行する国の事例を見ても、デジタルIDへの取り組みは未だ模索が続いている状態といえるが、情報のデジタル化が経済・社会で進展する中、デジタルIDへの対応は民間企業も政府・公共機関も避けて通れない。わが国でも、デジタル化の便益を社会全体で広く享受できるように、共通デジタルIDスキームの在り方について、今こそ政府がリーダーシップをとって関係者と広く議論することが求められているといえよう。その際には、先行する各国の事例を踏まえ、①共通デジタルIDスキームに向けた政府・民間の関係者間での対話と協調、②積極的な情報の公開とリテラシー教育の推進、③先端技術のデジタルIDへの応用の研究、④これらについて責任をもって推進する組織の設置、について検討していく必要がある。

## １．はじめに

データ駆動型社会の構築に向けた取り組みが、国内外で活発化している。民間企業はもとより政府・行政機関においても、データの利活用によるサービスの効率化や質の向上が模索されている。

データの利活用や、これに基づくデジタルサービスの実現を進めるうえで、「デジタルID」は不可欠の機能である。デジタルの世界において個人を一意に識別するとともに、その権利や資格の正当性等を確認し、ネットワークへの接続やオンライン上での各種手続き・取引、自己に関するデータへのアクセス・共有・利用などを可能にする。そこで、IDの真正性や信頼性を国が保証し、官民のサービスで利用可能とするデジタルIDスキームの整備が各国で進められている。もっとも、不正利用・情報漏洩などのリスクや、政府による国民監視・管理の強化などの懸念から、国レベルで共通のデジタルIDを導入することに対し、多くの国で国民の抵抗感が強い。

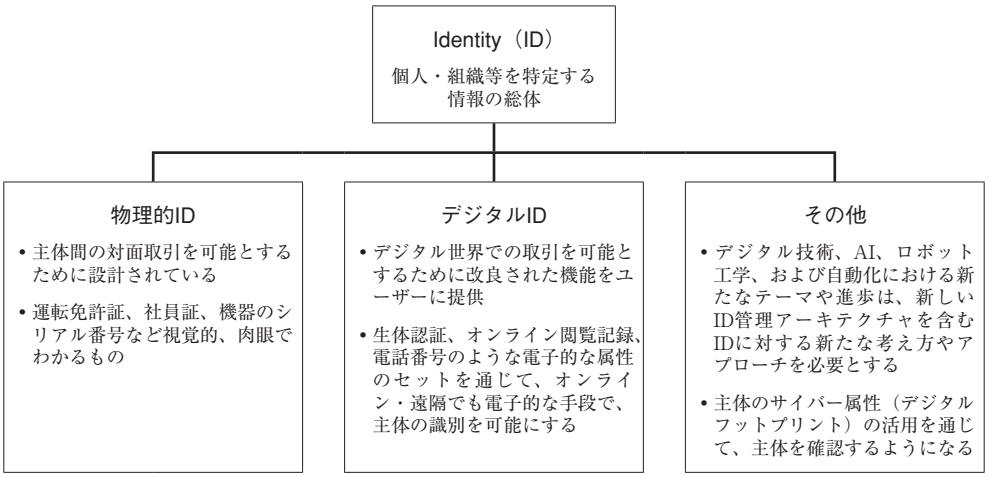
わが国で2016年に始まったマイナンバー（個人番号制度）も、デジタルIDとして分類することが可能である。しかしながら、現状では取り扱うことができる情報や分野が、法的にもシステム的にも制限されており、国民の個人番号制度に対する根強い不信感や誤解も重なって、普及は進んでいない。このため、官民の広範な分野でデジタルIDとしての利用が期待されているものの、実際の活用は困難な状況にある。現状、わが国には公共サービスでも民間サービスでも利用できる共通のデジタルIDが存在しないため、サービスごとに様々なデジタルIDが林立することになり、消費者は多くのデジタルIDを管理しなければならず、かえって不便が生じている。このままでは、本来、各種サービスのデジタル化で実現されるはずの便益を享受できない恐れがある。

本稿では、官民のデジタルサービスの共通認証基盤としてデジタルIDの導入・活用を進めている国について比較検討を行い、デジタルIDを国民の納得を得ながら普及・定着させていくための課題について考察する。まず、第２章でデジタルIDの定義や意義について整理する。第３章では、ヨーロッパやアジアでデジタルIDが導入されている代表的な事例を取り上げる。導入されている国の多くが政府主導で開発されたものであるが、なかにはスウェーデンのように民間の認証システムが採用されている事例もあり、わが国の参考になると考えられる。第４章ではまとめとして、デジタルIDの課題を整理し、今後の経済・社会の便益に繋げるための方策について考察する。

## ２．デジタルIDとはなにか

実社会において、自分が主張する人物であることを証明するために、運転免許証やパスポートなど、公的機関が発行する物理的な身分証明（物理的なID）が使われる。これと同様に、コンピュータやインターネットなどで、アクセスしている人物が確かに本人であり、当該システムを使う権利や資格を有することを証明するために、IDやパスワード、生体認証などが使われる。このように、デジタルの世界で使われる身分証明の方法がデジタルIDである（図表１）。ここでは、官民におけるサービスのデジタル化の広がりとともに、これを支えるインフラとして重要性を増すデジタルIDについて整理した。

（図表１）IDの分類




（資料）World Economic Forum “Identity in a Digital World - A new chapter in the social contract” 2018を一部加筆

(1) デジタルIDの概要

ID（Identity、身元識別情報）とは、「ある状況で個人やグループ、組織・企業を特定する情報の総体」である（高橋［2009］）。サービスや製品の購入、申請や手続きなどを行う際に、申し出た者（認証要求者）が確かに主張する本人であることを確認し、その利用資格や権利に応じたサービス等を提供するための手段としてIDが使用される。IDは、識別子（Identifiers）、クレデンシャル（Credentials）、属性（Attributes）の３要素からなる（図表２）。

実社会における対面取引の際、わが国では、サービス等の利用者は運転免許証やパスポートなど政府や公的機関によって発行された写真付の公的書類を個人の身分証明として提示する。サービス等の提供者側は、提示された運転免許証等に記載されている氏名や生年月日、顔写真、免許証番号等を照合するなどにより本人確認をする。運転免許証等は、対象者を識別するための情報を記録した物理的なIDといえ、公的機関が発行していることで信頼度も高い。これを所有・提示することで対象者が本人であることを証明でき（注１）、金融機関での口座開設や携帯電話の契約など、重要な取引が可能となる。

（図表２）IDの３要素

| 構成要素 | 機　能 | 主な例 |
|---|---|---|
| 識別子<br>（Identifiers） | IDを識別するための情報 | アカウント名、メールアドレス、保険証番号、運転免許証番号、社員番号、学生番号、電話番号など |
| クレデンシャル<br>（Credentials） | ある情報内容の正当性を示すための情報 | 正当な利用者であることを示すワンタイム・パスワード、国籍を示す電子パスポート、電子証明書、印鑑、生体情報など |
| 属性<br>（Attributes） | IDを特徴付ける情報 | 個人：氏名、住所、生年月日、所属、役職、信用情報、生体情報、人間関係、銀行口座番号<br>企業：代表者名、所在地、ロゴ、定款、格付け情報、東証コードなど |

（資料）高橋健司「アイデンティティ管理の現状と今後」電子情報通信学会誌Vol.92 No.4、2009年、伊藤宏樹「クラウドにおけるアイデンティティ管理の課題」情報処理Vol.51 No.12、2010年12月

これと同様に、デジタルIDはデジタルの世界で本人を特定するための情報の総体といえる。デジタルIDについては様々な定義がなされているが、例えば世界銀行（World Bank［2018］）は、「電子的に取得・保存された、主体（個人や企業、組織）を一意に識別する属性やクレデンシャル（認証情報）のセット」としている（図表３、注２）。そこで、本稿ではデジタルIDは、主にデジタルの世界での取引において、「申し出た者（認証要求者）が確かに主張する本人」であり、取引等が「当該本人が行っている行為であること」を確認・証明するための情報ならびにシステム（注３）と位置付けることとする。

（図表３）デジタルIDの定義

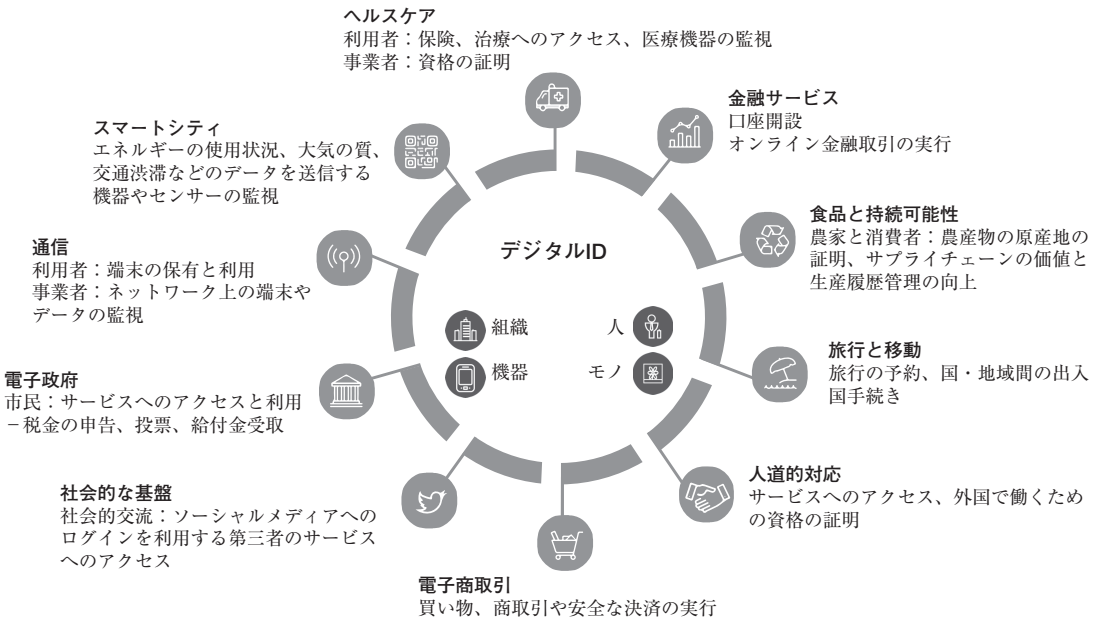
| 機　関 | 定　義 |
|---|---|
| 世界銀行 | 個人を一意に識別する電子的に取得・保存された属性及び／又はクレデンシャルのセット。 |
| ITU（国際通信連合） | 一つ又は複数の主体をコンテクストのなかで十分に区別できるようにする一つ以上の属性の形式で、主体をデジタルで表現したもの。 |
| EU（欧州連合） | 電子的IDとは、自分が言っているとおりの者であることを電子的に証明する方法であり、それによってサービスへのアクセスが可能になる。IDは、主体（市民、企業、行政）を他のものと区別できる。 |
| GSMアソシエーション | 電子的に取得・保存された識別属性の集合で、経歴データ（例･氏名、年齢、性別、住所）と生体データ（例･指紋、虹彩、顔写真）を含み、与えられたコンテクストの中で個人を一意的にあらわし、電子取引で使われる。 |
| OIX | 主体が誰であるかを証明するために、個人を特定できるデータのセット。信頼のレベルに応じて、個人の身元確認の必要がある（ウェブサイトへのアクセスに必要な認証のレベルは、支払いや家の購入に必要なレベルとは異なる）。通常、デジタルサービスへのアクセスには個人のIDだけでなく、属性（年齢、住所、信用格付、在留資格など）も必要。 |
| 情報処理推進機構（IPA） | デジタル情報として統一的に管理されたアイデンティティ情報（アイデンティティ情報は、エンティティ＜主体：属性を管理する単位＞についての属性情報の集合）。 |

（資料）World Bank and GPIF “G20 Digital Identity Onboarding”, ITU “Digital Identity Roadmap Guide”, GSMA “Digital identities - Advancing digital societies in Asia Pacific” June 2018, EU “Electronic Identities - a brief introduction” 2007、Open Identity Exchange（OIX）“Digital Identity: The cost of doing nothing” 2018, 情報処理推進機構「アイデンティティ管理技術解説」2013年１月

デジタルIDを構成する要素のうち、識別子は集合の中からある主体を他と識別したり同定するために付される文字列、数字、符号などであり、個人番号や免許証番号などがある。属性情報は、本人を特徴づける情報であり、生年月日や身長など固有のもの、健康記録や取引履歴など蓄積されたものなどがある。またクレデンシャル（認証情報）は、個人・組織等の主体（認証要求者）が確かに関連する情報（身元識別情報や属性情報、利用資格、権利等）の持ち主であることを証明するための情報で、特定のサービスやアプリにアクセス・利用する際のパスワードや生体認証などがそれに当たる（前掲図表２）。デジタルIDでは、これらの情報がデジタルデータにより表現されている。

デジタルIDの発行・利用が増大している背景として、インターネットやスマートフォンの普及に伴い、官民のサービスのデジタル化・オンライン化が進展していることが挙げられる（図表４）。デジタルサービスを提供する際の顧客・利用者の本人確認手続き（KYC：Know Your Customer）を、オンライン上で安全かつ簡便に行うための手段として、デジタルIDが必要とされる。例えば、エストニアではオンライン上のサービス（例：公共サービスやインターネットバンキングなど）を利用する場合には、利用者はPCのカードリーダーに自分の国民IDカード（eIDカード）を差し込んでパスワードの入力を行い、サービス提供者側でアクセスした者が主張する本人であると確認されれば、各種手続きや取引を行うことができる。eIDカードのICチップに格納された電子証明書を使う（政府の公的認証サービスが

（図表４）日常生活で広く使用されるデジタルID




（資料）WorldEconomic Forum “Identity in a Digital World - A new chapter in the social contract” September 2018

介在する）ので、単にホームページ上でID（利用者番号）とパスワードを入力するより安全性が高いとされる。デジタルIDの発行者は、エストニアのように政府である場合のほか、専門のIDプロバイダーや銀行、通信事業者などが自社のデジタルサービス提供と同時に独自のIDのプロバイダーとなっているケースもある。本稿では、多様なデジタルIDのなかでも、国が公的な本人確認・認証手段としてその真正性や信頼性を保証しているデジタルIDを対象とする。

わが国では、政府（市区町村）がICチップ搭載のマイナンバーカードを発行しているが、実社会でカードを物理的IDとして身分証明に使うことができ、かつ、パソコンのカードリーダーに差し込んでオンラインで確定申告を行うなどデジタルIDとしても使うことができる。前述のエストニアのように、政府が発行する公的なデジタルIDを銀行口座取引など民間サービスに利用できるところもあれば、それとは逆で、スウェーデンのように民間のデジタルIDを使って公共サービスにアクセス可能としているところもある。

さらに、最近ではカードなどの物理的なIDを使わなくても、スマートフォンのアプリや生体認証などの電子的な手段で本人の認証が完結できる方式への移行が世界的に進んでいる。運転免許証などのように偽造が可能な物理的なIDに比べ、デジタルIDの方がより厳格に本人を確認できるということで、デジタルの世界ばかりでなく、実社会の本人確認手段（例えば、建物の入退館や病院の受付、デバイスへのアクセス、キャッシュレス決済など）としても、IDカードに代わり顔や虹彩、指紋などの生体認証が使われるなど、応用範囲は大きく広がっている。

オランダのデジタルID関連企業であるGemalto（ジェムアルト）は、2018年から2020年にかけてのデジタルIDの主要な動向について、①モバイル化が一段と進展、②セキュリティと信頼に対する需要が増大、③スマートシティへのシフトが加速、④デジタルIDシステムに対する公共の監視を求める声が

増加、⑤国民IDカードや電子ID計画、国民IDイニシアチブや実装がさらに増加、の５点を指摘している（注４）。官民のサービスのデジタル化の進展や本人確認の厳格化が求められる中で、デジタルIDへの取り組みが加速すると見ている。

(2) デジタルIDに対する期待

それでは、デジタルIDにはどのようなメリットがあるのであろうか。

第１に、各種デジタルサービスの利用時に、安全・簡便に本人性や有する権利・資格の正当性を証明できることが挙げられる。とくに最近のデジタルIDは、生体認証等を使うことにより、従来のパスワードのみの認証より安全性が高まっている。加えて、デジタルIDは相手によって必要な属性情報だけを提供する仕組みとすることが可能であり、対面での本人確認時に、カード不要のデジタルIDと生体認証を使えば、運転免許証などの物理的なIDのようにカードに記載されているすべての個人情報を相手に見せる必要がない（図表５）。さらには、個人を一意に特定できるので、当該個人に関連するデータを分野横断的に収集・連携させたり、分析することにより、これまでにない多様なサービスを実現することが可能になる。例えば、エストニアではeIDと個人の属性情報や健康情報が紐付けられており、運転免許更新時に必要な健康診断のデータが道路交通局に送られ、申請人（運転者）と行政職員双方の手間やコストが削減されている。また、引越しの際にはオンラインで住所変更をすれば、役所や電気・ガスなど関連する公的機関の手続きも基本的に一度で完了する。デンマークにおいても、デジタルID（通称NemID）を基盤として、中央政府・地方自治体双方の行政サービスの一元化窓口（国民のポータルサイト「Borger.dk」）が実現しており、デジタルIDと口座番号の紐付けにより、公共機関からの給付金等の支払いが全て専用口座（NemKonto）に振り込まれる仕組みとなっている。デジタルサービスとデジタルIDが両輪となって普及・活用が進むことにより、サービスの利便性や生活の質の向上、透明性の確保、社会的課題の解決などに繋がることが期待される。

第２に、デジタルIDは社会包摂の手段としても注目されている。途上国では、戸籍・住民登録のような人口台帳が未整備のため、従来、本人確認をすることが困難であった。世界銀行によれば、推定10億人が基本的な身分証明情報であるIDを持たない。そのため、これらの人々は医療や教育、福祉、金

（図表５）デジタルIDで実現する世界の例

エラは、さまざまな方法でデジタルIDを採用しています。彼女はバーで、自分の名前、住所、生年月日など不必要な情報までさらしてしまう運転免許証を見せる必要がなく、「利用するのに十分な年齢」であることを証明するために、デジタルIDを使います。彼女は、社員証の代わりに自分のデジタルIDを使ってオフィスビルに入り、処方薬をオンラインで注文します。一方で、彼女はデジタルIDを使用して、ロイヤルティプログラムやポイントサービスに参加したり、雑誌や動画配信サービスに会員登録したり、ソーシャルメディアのプロフィールを作成したり、お気に入りの音楽を共有することもできます。エラは、デジタルIDをどこで使用するか、どのデータを誰に提供するかを自分で決めます。

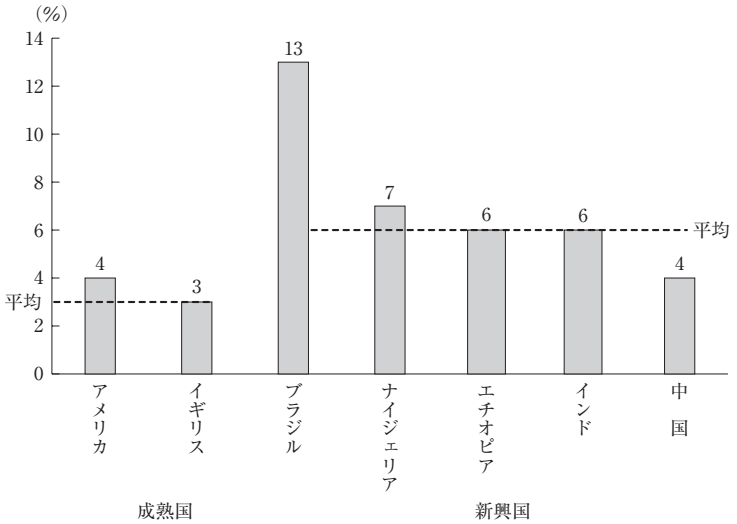
（資料）Mastercard “Digital Identity: Restoring Trust in a Digital World” March 2019を一部加筆修正

融サービス等を受ける機会から排除されている。このような背景から、法的身分証明としてのIDの提供は国連のSDGs（持続的な開発目標）のターゲットの一つ（16.9）とされている（注５）。

このような課題について、本人固有の生体認証等を使用するデジタルIDを導入することにより、個人を一意に識別することが可能となり、社会包摂を進めるツールになると考えられる。インドでは、2009年に「アドハー（Aadhaar、基礎という意味）」と呼ぶ生体認証（指紋・顔・虹彩）を使ったデジタルID制度（注６）が導入された。アドハーの登録は任意であるにもかかわらず、全人口の90％超に当たる12.5億人（2020年１月17日現在）が登録している（注７）。その理由として、国民はアドハー登録時に国民識別番号（アドハー番号）と紐付けされた銀行口座を開設でき、社会保障給付金や補助金を当該口座で受け取ることができるようになったことが大きいと指摘されている。政府にとっても、補助金等の対象となる低所得者を正確に把握し、効率的に支払いができるようになり、不正行為が大きく減少するという効果が得られている。ナイジェリアでは、デジタルID（注８）の導入により、実際には存在しないのに給料が支払われている62,000人の幽霊公務員が排除され、年間10億ドルの節約に繋がったほか、投票者の認証により二重投票が阻止され、選挙の透明性が確保されるようになった（世界銀行［2016］）。このように、途上国においても本人確認・認証手段としてデジタルIDが市民に遍く付与されることにより、金融サービスはもとより、教育、医療、年金等の公共サービスを広く社会に行き届かせることが可能になり、社会包摂や経済成長に貢献する可能性が認められる。

世界銀行［2016］は、「インドやパキスタンには、高所得の北アメリカ諸国よりも高度なデジタル式身元証明システムがあり、これはこのような技術が『リープフロッギング』効果をもたらす可能性を示唆している」と指摘している。マッキンゼー・グローバル・インスティテュートは、デジタルIDの導入を通じ、2030年には先進国でGDPの３％、新興国では６％に相当する経済価値を獲得すると予測している（McKinsey Global Institute［2019］、図表６）。

（図表６）デジタルIDの高水準での導入による経済価値の増加
（2030年、GDP比）

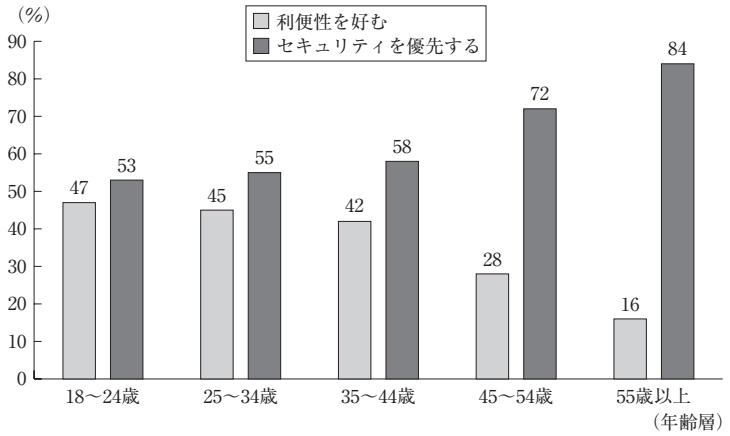



（資料）McKinsey Global Institute “Digital Identification: A Key to Inclusive Growth” January 2019

(3) デジタルIDに対する懸念

デジタル経済社会の進展に伴い、あるいは社会的課題の解決に向けて、デジタルIDの普及はこれから一段と進むことが予測されている。その一方で、デジタルIDには個人の属性情報が含まれ、センシティブ情報に紐付けられる可能性があることから、懸念も膨らんでいる。具体的には、IDへの不正アクセスや不正使用、IDと紐付いた個人情報の流出、それに伴うプライバシーや人権の侵害、IDを通じた監視社会の到来などである。IBMの調査によれば、特に年齢が高い層ほど、IDの利便性よりもセキュリティを重視する傾向にある（図表７）。例えば、世界でも先進的なデジタルIDと見做されているエストニアのeIDに関しては、2017年８月にIDカードのチップに潜在的なセキュリティリスクがあることが明らかになり、対応を余儀なくされた（注９）。あるいは、アメリカの巨大プラットフォーマーによるデータ寡占が問題視されているが、ユーザーがサービス利用時に登録・使用するIDに、属性情報のみならず嗜好や行動なども含む様々な情報が紐付けられ収集されており、本人が知らないところでそうしたデータが使われていることがある。

（図表７）認証方法の利便性と安全性とどちらを重視するか



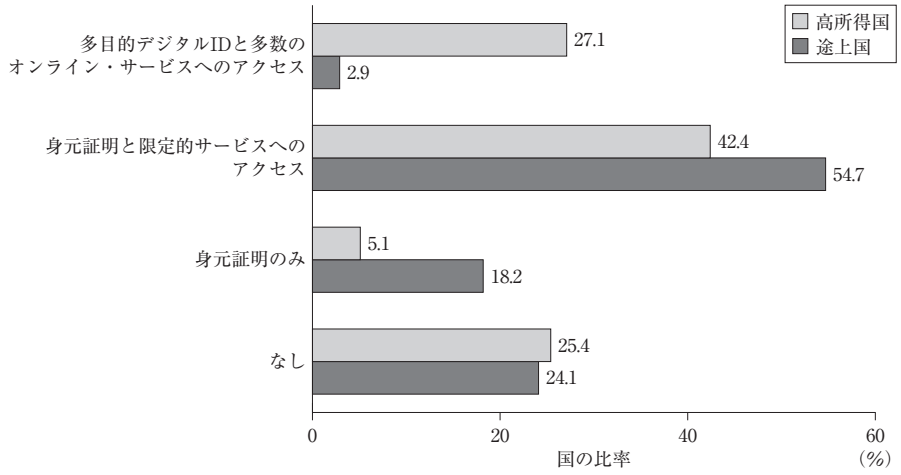

（資料）IBM “IBM Security: Future of Identity Study”
（注１）「安全性が低くても10秒節約になる認証方法を使う」または「利便性のために安全を引き換えにはしない」から選択。
（注２）アメリカ、EU、アジア太平洋（オーストラリア、インド、シンガポール）の成人約4,000人からの回答。

また、「デジタル技術は専制体制にとって統制を維持しながらサービス提供を改善する機会を提供してくれている」（世界銀行［2016］）という意見がある。政府が発行するIDをもとに国民の様々な情報を収集し、監視を強めているというものである。実際に、中国では政府が社会信用システム「全国信用信息共享平台」（注10）の構築を進めており、国民ID（身分証番号）と結びつけて、個々人の信用度を測定・可視化するツールとして用いられている。インドでは、アドハー制度はプライバシー権を侵害しており憲法違反であるとの申し立てが相次いでなされている（注11）。フランスでも、内務省が主導する「Alicem（アリセム）」と呼ぶデジタルIDに顔認証を導入するプロジェクトに対し、データ規制当局からEU規制に違反するとして最高行政裁判所に異議が申し立てられている（注12）。

デジタルIDにはこうした懸念があるものの、セキュリティを過度に重視すると、デジタルIDの本来の利点である利便性や効率性が損なわれることになり、導入しても使われないものとなってしまう恐れがある。デジタルIDの導入と運用に当たっては、その活用の公益性や利便性・生活の質の向上といったメリットと、プライバシー保護やセキュリティ確保とのバランスをいかに両立するかが重要な課題となる。

なお、世界銀行によれば、2014年現在、世界197カ国のうち148カ国が何らかの形のデジタルIDを導入しているが、多くの国で身元証明ならびに2～3の機能に限定されている（世界銀行［2016］）。オンライン・オフラインの多様なサービスに共通で使える多目的型のデジタルIDプラットフォームが整備されている国は、高所得国で27.1%、途上国は2.9%にとどまる（図表8）。また、49カ国はいかなる種類のデジタルIDも導入していない。

（図表8）デジタルIDシステムの機能




（資料）世界銀行（翻訳：田村勝省）「世界開発報告2016　デジタル化がもたらす恩恵」一灯舎（原文：「World Development Report 2016: DIGITAL DIVIDENDS」The International Bank for Reconstruction and Development/The World Bank）

（注1）電子商取引推進協議会 認証・公証WG「証明書利用形態に関する考察」2002年3月（https://www.jipdec.or.jp/archives/publications/J0004138）。

（注2）なお、IoT（モノのインターネット）ではインターネットに繋がれたモノを特定する必要がある。したがって、デジタルIDを利用する対象はヒトに限らず、国や企業、組織、機械やデバイス、サービスなど多岐にわたる。本稿は、そのなかでもとくに個人を識別するためのIDに焦点を当てている。

（注3）Open Identity Exchange（OIX）［2018］は、本人を確認・認証するためのシステムを「デジタルIDスキーム」と呼び、「デジタルIDスキームは、個人が製品またはサービスにアクセス可能とするために、サードパーティと共有する必要がある個人の属性情報を明らかにする（unlocked）組織間の合意である」としている。

（注4）Gemalto “Digital identity trends - 5 forces that are shaping 2020”（https://www.gemalto.com/govt/identity/digital-identity-services/trends）。

（注5）この目標を達成するために、国連は2017年6月にNGO、民間企業と連携して「ID2020」プロジェクトに取り組むことを発表した。ブロックチェーンや生体認証を活用した非中央集権型のデジタルIDシステムの構築を目指している。

（注6）AadhaarはUIDAI（インド固有識別番号庁）が運営しており、インドの全居住者を対象に12桁の国民識別番号が付番されるほか、氏名、生年月日、住所といった基本情報や、顔写真、10指の指紋、目の虹彩が登録される。

（注7）インド政府ホームページ（https://uidai.gov.in/aadhaar_dashboard/registrar.php）。

（注８）認証機能付のICカードでマスターカードが発行。
（注９）e-estonia “What we learned from the eID card security risk?” May 2018（https://e-estonia.com/card-security-risk/）による。エストニア政府は、これに対応するため、脆弱なチップを搭載したカードの電子証明書の停止と更新を行った。また、同様にスペインでは1,700万枚のカードの取り消しを余儀なくされた。
（注10）企業版の「国家企業信用情報公示システム（国家企**业**信用信息公示系**统**）」も存在。
（注11）2017年８月に最高裁で「プライバシーは憲法で保障される権利」とする判決が出され、2018年９月の最高裁判決により民間企業が本人確認に使用してはならないとされた。もっとも、2018年９月の判決ではアドハー制度自体は合憲との判断がなされた。さらに、2019年７月には修正アドハー法が成立し、民間企業は本人同意のもと本人確認にアドハーを利用することが法的に認められることとなった（岩崎［2019a］）。
（注12）Helene Fouquet “France Set to Roll Out Nationwide Facial Recognition ID Program” Bloomberg（2019年10月３日付）による。

## ３．デジタルIDの導入事例

世界の多くの国では、国民ID番号や社会保障番号など基礎的なID番号のインフラを導入、あるいは整備を進めている。各国は、この番号制度をデジタルIDスキーム導入の基盤とし、官民のサービスを効率的・効果的に提供することを目指している。もっとも、アプローチ方法は国によって異なる（図表９）。そこで、わが国の参考とするため、先進国を対象にデジタルIDの整備状況を概観する。ここでは、①民間のIDスキームを活用するスウェーデン、②政府によるIDスキーム構築と民間への開放に取り組むシンガポール、③基礎的なIDインフラが未整備のため試行錯誤するイギリスの事例を取り上げ、わが国への示唆を探る。

（図表９）主なデジタルIDの事例

| 類　型 | 国 | 名　称 | 備　考 | 国民ID番号 |
|---|---|---|---|---|
| 政府主導・中央集権型 | シンガポール | NDI（National Digital Identity） | 既存の認証システム等が基盤（認証SingPass／個人情報MyInfo） | NRIC（National Registration Identity Card）番号 |
| | インド | Aadhaar Authentication | Aadhaar eKYC（個人情報照会）と連動 | Aadhaar |
| | エストニア | e-identity | 民間企業（銀行と通信会社が設立したSKID）が基盤技術開発 | PIC（Personal Identification Code） |
| 官民協調・連合型 | スウェーデン | Bank ID | 銀行コンソーシアムが開発、公共調達でIDプロバイダーを複数選定（他にFreja eID+、Telia等） | PIN（personnummer、Personal Identity Number） |
| | イギリス | GOV.UK Verify | 民間IDプロバイダーを複数選定 | なし |

（資料）各種資料を基に、日本総合研究所作成
（注）World Bank Group et al.［2016］によれば、政府主導・中央集権型、官民協調・連合型は以下の通り分類。
政府主導・中央集権型
- 個人のID属性が１つまたは複数の政府所有データベースに保存され、国発行のIDが公共部門と民間部門の全てまたはほとんどのデジタル取引の基盤として機能。
- 公的IDは、銀行や携帯電話の資格情報など、他のデジタルIDを検証するための基盤として使用可能。

官民協調・連合型
- 市民は複数の信頼できるIDプロバイダー（銀行、携帯電話事業者など）から自由に選択、これらの資格情報を使用して、IDハブまたはゲートウェイを介して広範な公共・民間デジタルサービスにアクセス。
- 政府が身元確認の公式基盤を提供し、民間企業がデジタルIDプロバイダーとしての役割。
- 公的機関も信頼できるIDプロバイダーであり、政府はIDフレームワークと承認プロバイダーの定義と規制において中心的な役割。

### (1) 民間のIDスキームの活用：スウェーデンの「BankID」

#### A．Bank IDの概要

スウェーデンでは、民間部門・公共部門ともにデジタルIDを発行できるとされているが、その中で

も最も普及しているのが、2003年に導入されたBank IDである（図表10）。

Bank IDは、2002年に大手銀行のコンソーシアムが設立した「Finansiell ID-Teknik BID AB」（注13）により開発され、2003年に導入された。スウェーデン政府（国税庁）が全市民に付番する個人識別番号（PIN：Personal Identification Number／Personnummer）と氏名、電子証明書（認証用・署名用、注14）を統合したもので、銀行口座と紐付けされている。当初はパソコンのハードディスクやUSBメモリを差し込み使用するファイル形式（Bank ID on file）であったが、2005年にICチップ搭載のスマートカード（Bank ID on card）が発行され、2010年にはスマートフォンやタブレット端末で利用できるMobile Bank IDが導入された（当初はSIM、2011年からモバイルアプリに移行）。Bank IDは、パスポート、運転免許証などの物理的な身分証明書に匹敵する電子身分証明書であり、Bank IDで作成された電子署名は物理的な署名と同等の法的拘束力があるとされる。

スウェーデンでは、デジタルガバメントの取り組みが進んでおり、行政サービスのほとんどがオンラインで利用可能である。オンラインで各種申請や手続きを行う際の本人認証手段として、民間が開発したBank IDが利用されている。なかでも、国税庁や社会保障庁がいち早く、2003年にBank IDを採用した。2005年には、銀行のインターネットバンキングにアクセスする際の共通のデジタルIDとして、Bank IDの利用が開始した。導入当初は普及が進まなかった（2003年の利用者数10万人、2005年50万人）ものの、2009年に国税庁がBank IDを使った電子申告に対し、優遇税制措置を適用したことが普及のきっかけとなった（注15）。さらに、2010年にモバイルBank IDが導入され利便性が高まり、2012年にはモバイルP2P決済サービス「スウィッシュ（Swish）」の認証手段にBank IDが使われたことで、一気に利用が広がった（Citi［2019］）。

（図表10）Bank IDの概要

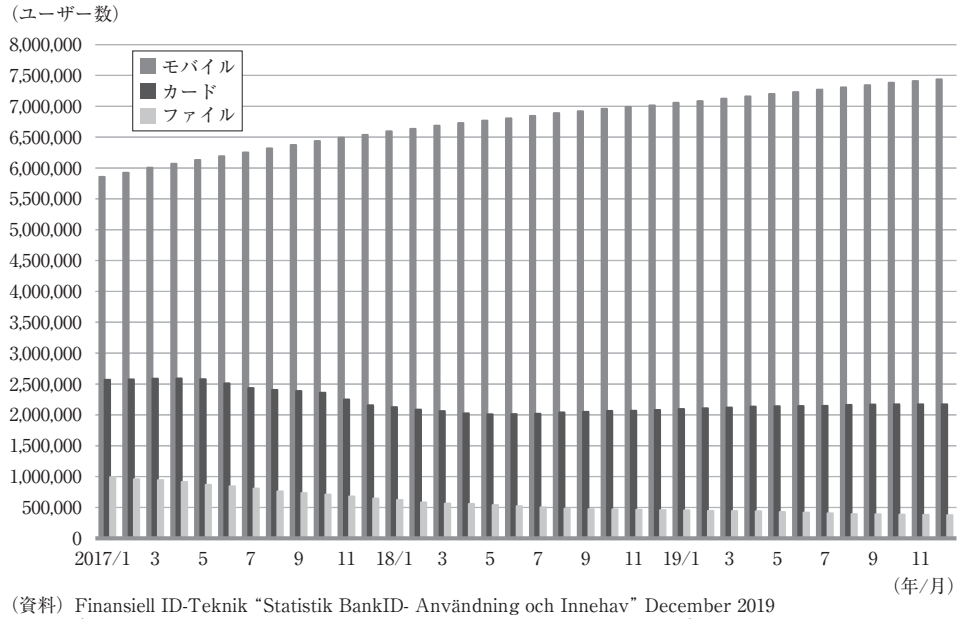
| | |
|---|---|
| 導　入 | 2003年（1999年のEUの電子署名指令が契機） |
| 開発者 | Finansiell ID-Teknik BID AB（2002年設立、銀行７行が出資） |
| 利用者 | 820万人（人口普及率80%超）／年間の利用件数・累計41億件（2019年）<br>スウェーデンの全銀行（11行）が認証システムとしてBank IDを採用 |
| 対象者 | スウェーデンの銀行口座の保有者<br>（スウェーデンでは個人識別番号を持つ者でないと口座開設ができない） |
| 概　要 | ・個人識別番号と氏名、電子証明書（認証用・署名用 ）を統合したもの<br>・パスポート、運転免許証などの物理的な身分証明書に匹敵する電子身分証明書、かつ、作成された電子署名は物理的な署名と同等の法的拘束力を有する |
| 保有形態<br>（全保有者に占める割合・重複あり） | ファイル形式：USBまたはコンピュータのファイル（4.9%）<br>カード形式：ICチップ搭載カード（26.8%）<br>モバイル形式：モバイルアプリ（95.7%） |
| 利用可能サービス | 公共サービス：確定申告、各種行政手続、病院関連の手続きなど<br>民間サービス：銀行取引、決済サービス、電子商取引、ポイントサービスなど |

（資料）Finansiell ID-Teknik BID AB “Statistik BankID- Användning och Innehav” December 2019, インタビュー調査等を基に日本総合研究所作成

現在、Bank IDは電子納税申告などの公共サービスのほか、民間では銀行取引、保険手続き、ポイントサービス、駐車場の利用などで使用されている。官民の様々なサービスにおいて日常的に利用可能であることから、国民の80%以上に普及している。2019年末時点で820万人がBank IDを保有しており、内訳はモバイルBank IDが95.7%、カードタイプは26.8%、ファイルタイプは4.9%である（重複あり、

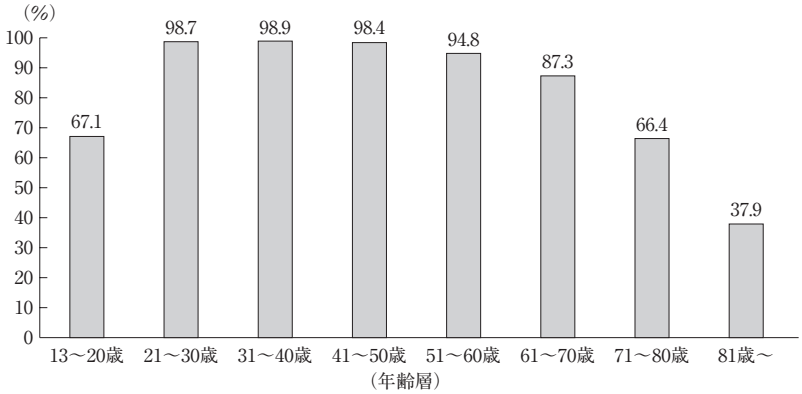
図表11)。年代別に見ると、20代から60代までの 9 割以上がBank IDを保有しており、81歳以上でも 4 割近くが利用している（図表12)。また、2019年における使用件数（ログインと電子署名）は41億件（月 3 億件以上）で、97%がモバイルBank IDによるものである。インターネットおよびモバイルバンキングでの利用が53.8%と最も多く、公共サービスでの利用は6.9%となっている（図表13)。なお、カードタイプのBank IDは一部銀行が発行してきたが、モバイルBank IDへの移行が進んでいるため、今後の新規発行・更新は縮小・廃止していく方針である。

（図表11）Bank IDのユーザー数の推移（2017年 1 月～2019年11月）



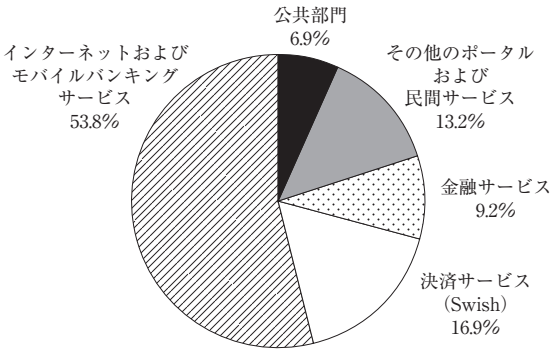

（資料）Finansiell ID-Teknik “Statistik BankID- Användning och Innehav” December 2019
（https://www.bankid.com/assets/bankid/stats/2019/statistik-2019-12.pdf）

（図表12）年代別Bank IDの保有率（2019年11月）




（資料）Finansiell ID-Teknik “Statistik BankID- Användning och Innehav” December 2019
（注）スマートカード、コンピュータ、携帯電話、タブレット端末のいずれかでBank IDを保有する者の割合。

（図表13）Bank IDの利用の内訳




（資料）Finansiell ID-Teknik“Statistik BankID- Användning och Innehav”December 2019
（注）2019年９月（第３四半期）時点。

B．共通デジタルID普及の背景

スウェーデンでは、共通デジタルIDとしてBank IDが広く普及している。その背景には、①公共調達の手続きにより公共部門のサービスに使用するデジタルIDを選定していること、②官民の様々なサービスで個人識別番号（PIN）が必要とされ、番号の使用が当然のこととして普及していること、③国民のデジタルリテラシーや政府に対する信頼が高いこと、などスウェーデン特有の事情がある。

第１点目として、スウェーデンでは公共調達の手続きにより、電子政府のオンライン申告や申請手続きに使用するデジタルIDを選定している。後述のシンガポールのように、中央政府自身が開発・発行するデジタルIDが導入されているわけではない。スウェーデンでは公共部門及び民間部門がデジタルIDを発行できるとされているものの、政府は市場で既に使用されているデジタルIDを導入することで、自前で開発する時間やコストを削減でき、より安全で利便性や費用対効果の高い技術を導入できるとの考えに立つ。スウェーデン政府のデジタル政府局（DIGG：Myndigheten för digital förvaltning＜Agency for Digital Government＞、注16）が、公共部門の電子サービス向けのデジタルIDと電子署名の促進や調整の役割を担っており、選定や利用料の決定等を行っている。DIGGは目標として、①誰もが使いやすく安全なデジタルIDを利用できること、②デジタルサービスにおいて、簡単かつ安全にデジタルIDと電子署名を利用できること、③公共部門におけるデジタルIDおよび電子署名の使用に対する費用対効果が高いこと、を掲げている。

初回の2004年６月の入札では、①銀行コンソーシアムのBank IDのほか、②ノルデア銀行、③大手通信会社のテリアソネラ・スウェーデン、④コンピュータ会社のステリアが、ID発行者として選定された（注17）。現在は、①Bank ID、②デジタルセキュリティ会社Verisec（Freja e ID+：アプリを提供）、③ICカードベンダーのジェムアルト（AB Svenska Passとして国税庁のIDカードに使用）が政府の認定プロバイダー（個人向け）となっている。

第２点目として、スウェーデンでは1947年に個人識別番号（PIN）が導入され、個人の本人確認や様々な情報の管理に使われており、公的機関ばかりでなく民間事業者もサービスの手続き時などにPINを要求するなど、PINの利用が国民にとって当然のことと受け入れられていることがある。スウェーデ

ンでは、すべての国民は国税庁により出生時に10桁（生年月日６桁と個人ごとに異なる４桁で構成）の番号が割り振られている（注18）。そして、利用目的に正当性が認められれば、PINの利用について本人の同意は不要とされており、民間企業でもPINを利用することができる。そこで、例えば、銀行口座の開設、携帯電話の契約、医療機関の診察、不動産の売買・賃貸契約、確定申告、パスポートや運転免許証の申請などの手続きを行う際、PINが必要とされる。このように、日常生活のなかでPINが必要となる場面が多く、国民のPIN使用に対する抵抗感もそれほど強くないことから、デジタルIDにPINやそれに付随する情報が紐付けられることに対する受容性も高い。

第３点目として、ICTインフラが整備されており市民のデジタルリテラシーが高いことが挙げられる。スウェーデンでは、1998年の「家庭用PC改革」を通じて、勤務する企業から家庭用パソコンのリースを受けたことで、インターネットの利用率が高く、オンラインサービスでのデジタルIDの利用が浸透している。DIGGによれば（注19）、人口の98%がインターネットを利用しており、10歳以下の子供のインターネット利用は87%にのぼる。また、人口の92%がスマートフォンを保有している。そして、90%以上がインターネットバンキングを利用している。

加えて、政府における透明性確保に対する意識の高さや、そうした政府に対する国民の信頼と理解、といったスウェーデン社会の特性も指摘できる。スウェーデンは、世界で最初に情報公開制度（プレス自由法）が成立した国でもある。政府は、高福祉国家を成立させるためには国民の高負担に対する理解が不可欠であるとして、情報公開と公平な手続きを徹底し、国民の信頼を得てきた。

政府に対する高い信頼を背景として、政府による個人情報の管理に対しても、国民はあまり抵抗がない。スウェーデンでは、センシティブ情報は厳格に守られるべきであるものの、PINや氏名、住所、生年月日はセンシティブ情報ではなく、国民が権利を正当に行使するためにはそうした情報を提供する義務があると考えられている（注20）。そして、住民登録法（Population Registration Act）のもと、PIN、氏名、住所、出生地、国籍、市民権の有無など、当該個人に関する様々な情報が住民登録簿（Population Register）に登録されている（注21）。民間企業は、自社の顧客の情報をPINで管理可能であるほか、民間利用に供する目的で設立されたSPAR（Statens personadressregister、情報登録庁・国税庁傘下の独立機関）を通じて有料で氏名・住所等の情報を入手することができる（注22）。

なお、公的機関における個人情報の取り扱いの適正性については、独立機関のデータ検査院（Datainspektionens、Data Inspection Board）が監督するとともに、希望者に対しては公的機関の保有する自己に関する情報を毎年提供し、官庁間や官から民への情報提供ルールが法令で規定されているなど、透明性の高い仕組みが構築されている（渡辺［2010］）。

### C．Bank IDの利点と課題

スウェーデンでは、国民が日常的に利用する銀行のデジタルIDが「Bank ID」に統一され、さらに公共サービスを利用する際のデジタルIDとして採用されたことが、その普及に大きく寄与していると考えられる。銀行業界が、共通のデジタルIDの開発に取り組んだ背景には、1999年12月にEU電子署名指令が成立し、電子署名の法的な効力の承認と制度化を加盟各国に求めたことがある。それまでは、各銀行でそれぞれ独自のIDを発行していたものの、本人の身元確認や電子署名などのセキュリティは競争

領域ではなく協調領域とすることが最善であり、競争は、より良いサービスや商品で行えば良いという考え方に変わった（注23）。また、そもそも銀行は金銭や資産、個人の機微情報を取り扱うことから厳しい規制を遵守しており、その信頼性も官民共通IDのプロバイダーとしての強みとなった。大手銀行の中で、ノルデア銀行は最後までBank IDに参加していなかったが、2011年にBank IDに参加することを決めた（完全な移行は2015年）。同銀行のマネージャーは「Bank IDへの加入により、すでに他の銀行のBank IDを保有する一部顧客との契約を失ったものの、この時点で参加していなかったら、モバイルソリューションが提供できずにもっと多くの顧客を失っていただろう」と述べている（注24）。インターネットバンキングで使用するデジタルIDの共通化が進められ、公共サービスにも採用されたことで、普及が大きく後押しされた。Bank IDの普及が進むことで、他のデジタルサービスでも利用されるようになり、さらに普及が進むという好循環がもたらされている。ちなみに、Bank ID利用者が行う取引の半数以上がインターネットバンキングである（前掲図表13）。

一方で、Bank IDがスウェーデンのデジタルID市場で圧倒的なシェアを占めている点について、問題視する意見もある。①一つのIDプロバイダーへの過度の依存は、デジタルエコシステムにとって脅威、②競争がないことがイノベーションや製品の品質の向上、価格などに影響、③移民や銀行口座のない個人などすべての市民をカバーしていないこと、などが指摘されている（注25）。DIGGも、現状では、Bank IDを提供するルールは銀行により決定されており、市民の選択の自由を保障する「選定システム（Electoral System）」が十分に機能していないこと（注26）、クロスボーダーの人の流れに対応できていないことなどを憂慮している（注27）。

そこで、現在、政府はすべての市民が利用可能な公共部門のデジタルIDの在り方を模索している。EUでは、2019年 6 月に新しい規則（2019/1157）が採択され、加盟国はEU市民に対し安全性が強化されたIDカードまたはパスポートの発行が求められることとなった。スウェーデンでは物理的なIDとしての身分証明カードとしては、主に運転免許証が代替として使われているほか、カードタイプのBank ID、警察が発行する国民IDカード（EU域内のパスポートとしても使用可能）、国税庁が発行するIDカードなど複数存在する。政府は運転免許証に関して、本来運転の資格を有していることを証明するものであり、有効期間も長いことから、身分証明書として使用することは望ましくないと考えている。他のIDカードについても、発行主体が複数あり、身分証明書としての有効性や真正性の確認が難しいことや、偽造が増加していることなどが問題点として指摘されている。加えて、これらのIDカードは国民に保有・携行の義務はなく、有料であることや、ICチップを搭載しているものの限られた公共サービスでしか使えないことなどから、普及は進んでいない（注28）。

こうした課題を解決することを目的として、国の調査委員会から報告書が発表され、政府に対し、統一的かつ堅牢なデジタルIDの機能を搭載した国民IDカード（発行者は警察）、ならびに、これを規制する法律の導入が提案された（注29）。提案内容として、国民IDカードは13歳以上のスウェーデン人・居住者を対象とし、ICチップを搭載しており、デジタルIDとして、またEU域内のパスポートとしても使用できることや、本人確認を確実なものとするために、生体認証情報（指紋と顔）を登録すること、2022年1月の発行などが示された。もっとも、政府がこの報告書に従うかどうかの決定は、現在まで下されていない（注30）。また、提案されている国民IDカードは有料で保有は任意であることや、Bank

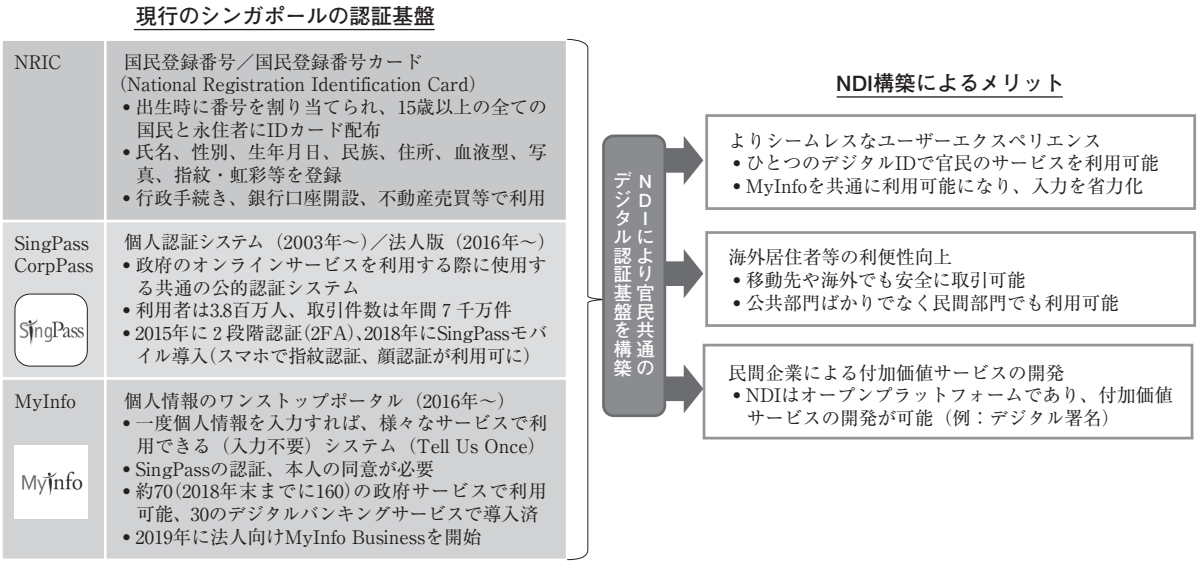
IDのように広範なサービスへの利用がすぐに実現できるわけではないので、導入されたとしても普及するかどうかは不透明である。

(2) 公的なIDスキームの民間への開放：シンガポールの「National Digital Identity（NDI）」

A．NDIの概要

シンガポールは、現在、スマートネイションイニチアチブを遂行している。その重要戦略分野の一つが、NDI（National Digital Identity、国家デジタル認証）である。NDIは、国民が政府や民間のデジタルサービスを利用する際に使用する共通のデジタルIDスキームであり、2020年の運用開始を目標としている。推進主体は、政府のデジタル化を推進する政府技術庁（GovTech：Government Technology Agency）である。シンガポールでは、2003年に「SingPass（Singapore Personal Access）」と呼ばれる個人向け公的認証システムを開始しており、NDIはこの「SingPass」と、2016年に導入された個人情報の登録・利用の一元化サービス「MyInfo」を基盤としている（図表14）。

（図表14）シンガポールのNDIの概要




（資料）スマートネイションホームページを参考に日本総合研究所作成

SingPassは、政府機関のサイト毎にばらばらであった認証方法の統一を目的として導入された共通認証システムである。シンガポールでは、イギリス統治下の1948年に不法移民の排除を目的として、国民登録番号制度が導入されている。出生時に９桁からなる番号が割り当てられ、15歳以上のシンガポール居住者には国民登録番号カード（NRIC：National Registration Identification Card）が配布される。SingPassは、この国民登録番号（NRIC番号）とパスワードを使って、各種行政サービスをオンラインで利用できる仕組みである。なお、セキュリティ強化のために、2015年に２段階認証（2FA：Two-factor Authentication）が導入されている（2016年に完全移行）。

SingPassの取得は任意であり、利用の際には申請が必要とされる。また、外国人はNRIC番号の代わ

りにFIN（Foreign Identification Number）と呼ばれる外国人向けのID番号を使って、SingPassの一部機能を利用できる。2019年９月現在のSingPassの利用者数は380万人、SingPassを利用した取引件数は年7,000万件を超える規模に達している。60を超える政府機関ならびに一部民間企業で、SingPassを利用可能なサービスは300を超える（注31）。

もう一つの基盤とされているMyInfoは、行政サービスの利用時に一度個人情報を登録すれば、他のサービス利用時に当該情報が自動的に入力される（Tell Us Once）サービスである。政府機関毎・利用サービス毎に何度も同じ情報を入力する手間が省け、いわば「個人情報の収納庫」ともいえる機能である。2016年に導入され、2017年には銀行の口座開設やクレジットカード申請時にもMyInfoを使うことができるようになった。政府のNDI戦略を推進するGovTech（政府技術庁）によれば、MyInfoの利用により、ユーザーはオンライン手続きの入力に必要な時間を80％短縮できるということである。

なお、法人に関しては、2016年開始のCorpPassと2018年開始のMyInfo Businessがあり、行政手続きのほぼすべてでCorpPassが利用できるようになっている。

NDIはこの２つの基盤を拡張し、市民が単一のデジタルIDを利用して、公共サービスでも民間サービスでも利用できる共通の認証プラットフォームを構築しようとするプロジェクトである。利用者は、デジタルサービスごとに複数のユーザー名やパスワードを使い分けたり、パスワードを記憶する必要がなくなる。政府はNDIイニシアチブの一環として、2018年10月に、スマートフォンの指紋認証や顔認証を利用でき、パスワードが不要となる「SingPass Mobile」を導入している。このモバイルアプリは、すでに20万人以上が利用している。SingPass Mobileは、海外に居住するシンガポール国民も利用可能であるなど、メリットが大きい。

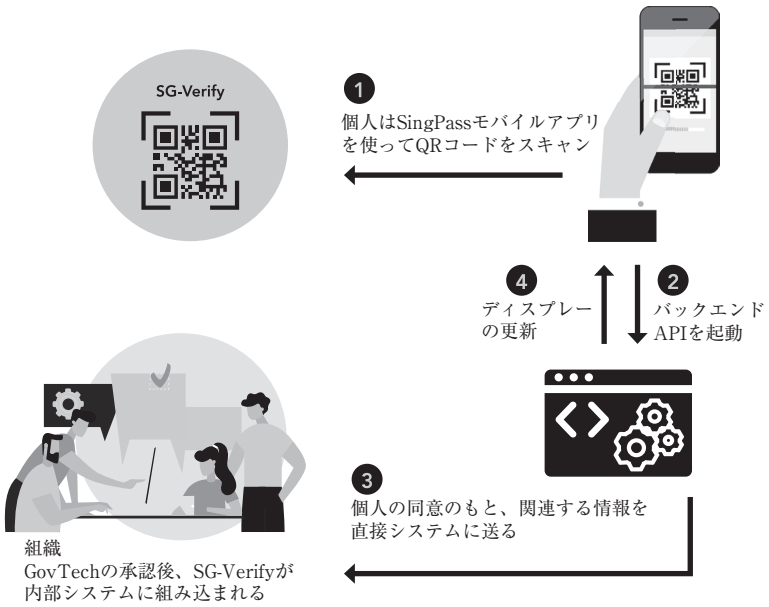
Ｂ．NDIの民間サービスへの展開

政府は、NDIの第二段階として、2019年12月に「SG Verify」を開始した。個人が、SingPass Mobileのアプリを使用して組織から提供されたQRコードをスキャンすると、本人確認と手続き等に必要な個人情報を提供できるサービスである（図表15）。個人は、物理的な身分証明カードを提示したり、個人情報をいちいち入力する必要がない。また、当該組織にどのデータが提供されるかがアプリで通知され、個人の同意がある場合にのみ情報が共有される。

SG Verify導入の背景として、シンガポールでは2019年９月に個人データ保護法が改正され、定められた例外を除き、民間組織によるNRIC（個人識別番号）の収集、使用、保管、開示が原則禁止となったことがある。NRICの番号やカードを代替する手段として、SG Verifyが利用されることになる。SG Verifyを本人確認手段として使う必要がある組織などは、GovTechに申請して使用可能となる。政府は、ユースケースとして、①病院やオフィスへの来訪者の身元確認、②銀行の店頭や通信事業者の販売店での本人確認、③クレジットカードの契約や公共料金の口座開設、などの事例を例示している。

このように、企業は独自のインフラやシステムを構築しなくても、政府が提供するNDIの共通APIや各種ツールを使って認証基盤を導入することが可能となり、コストの削減や安全性の強化に繋がる。GovTechは、民間事業者によるNDIの利用拡大に取り組んでおり、配車アプリのGrabやオンラインマーケットプレイスのCarousellなどが既に身元や個人情報を確認するツールとして導入している。オ

（図表15）SG-Verifyの概要




（資料）Personal Data Protection Commission Singapore（PDPC）“Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers” 2019

ンラインサービスの事業者にとってNDIは、ユーザーの本人性を正確に検証でき、偽アカウントや詐欺などの不正防止策としても有効であると評価されている（注32）。

C．NDIの利点と課題

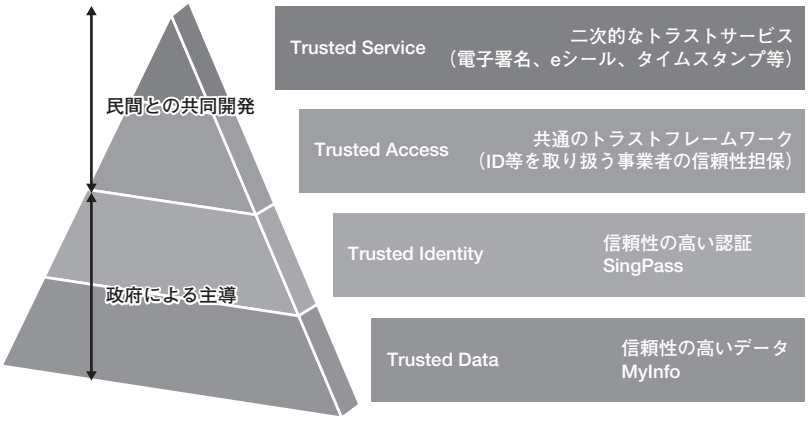
政府のNDI担当責任者であるKwok Quek Sin氏は、シンガポールにはもともとNRICという信頼性の高いID制度があったことが、デジタルIDの基盤としても機能したと評価している。加えて、SingPassの登場と政府サービスのオンライン化の時期が重なったことも大きい。政府機関ごとにシステムが分断されることなく、統一的な認証システムとしてSingPassが利用されることになった。

また、NDIに物理的なカードとしてのNRICを活用することは考えられていない。Kwok Quek Sin氏は、物理的カードに依存したシステムは、①カードのチップを数年ごとに交換する必要がありコストが高くつく、②カードに保存されているデータへのアクセスのために、カードリーダーを使用しなくてはならずユーザーフレンドリーではない、といったデメリットを指摘している（注33）。シンガポールはモバイル普及率が150%であることから、カードにICチップを搭載するのではなく、モバイル方式に移行させる方が普及を進めやすいという事情もある。なお、当初のSingPassは、政府のデジタルサービスを利用する際の認証としてIDとパスワードを入力する単純なもので、ユーザーがパスワードを忘れることや不正アクセスが頻発することが課題であったので、現行のSingPass Mobileではパスワード入力は行わないシステムへの移行が図られている（注34）。シンガポールの場合には、スウェーデン政府に対するデジタルIDの機能を搭載した国民IDカードの提案とは逆に、物理的ID（NRICカード）とデジタルID（NDI）の分離を図っているといえよう。

NDIのメリットは、上記の課題を克服できることばかりでない。MyInfoを通じて、個人が政府の保有する自分のデータをどのように使用したいか、民間部門との取引においてもそれらのデータをどのように使用するか、自分自身でコントロールできる点が挙げられる。

シンガポール政府は、NDIを通じて（ユーザーの同意のもと）信頼性の高いIDとデータを提供する基盤構築を主導し、民間部門と協力してトラストフレームワークやトラストサービスを提供する「ユニバーサルトラストレイヤー」の実現を目指している（図表16）。

（図表16）シンガポールNDI Stackの概念




（資料）GovTechホームページ（https://www.tech.gov.sg/products-and-services/myinfo-for-private-sector/）を基に日本総合研究所作成

一方で、NDIの核となるSingPassやMyInfoは中央集権型であるため、そのことから生じるリスクがある。認証システムが十分に堅牢でないと、トラブルが発生した場合に、政府サービスが一斉に停止してしまう事態が想定される。2018年２月ならびに11月には、ソフトウェアのバグなどにより機能停止する事態が発生し、一部のマレーシア労働者が、オンラインで労働許可を処理できず、帰国しなければならなかったり、企業が従業員の中央準備基金を期日までに提出できず、罰金を科せられることになった（注35）。

もう一つの課題として、民間企業が共通のデジタルIDスキームとしてNDIを採用する動きが進むかどうかということがある。MyInfoに関しては、多くの民間企業がAPIを通じて、個人の同意のもと必要なデータを入手する手段として活用している。しかしながら、例えばシンガポールの大手銀行はスウェーデンとは異なり、それぞれ独自の認証システムを使っており、現状では、政府のSingPassで使われているOneKeyのような認証トークンを共通で使おうとする動きがない（注36）。政府としても、NDIを採用するかどうかはそれぞれの民間企業の決定に委ねる方針である。

### （3）統一的なIDが確立できていない国の動向：イギリスの「GOV.UK Verify」

#### A．国民IDカード導入の頓挫

イギリスでは、第二次世界大戦時に、非常時下ということでIDカードが導入されたが、戦後の1952

年に廃止された。1990年代半ば頃から、再び国民IDカード導入が議論されるようになった。さらに2000年代に入って、アメリカでの同時多発テロの発生や、個人情報の盗用・偽造による公共サービスの不正受給などが問題となり、個人を正確に本人であると確認する手段の必要性が高まった。その当時、EUやアメリカにおいてパスポートへのICチップ搭載と生体認証情報の登録が進められており、これに対応する意味合いもあった。

2006年３月に、労働党政権によりIDカード法（Identity Card Act 2006）が成立した。同法は、イギリスに在住する16歳以上の個人について、生体認証を含む個人情報を国民ID登録簿（NIR：National Identity Register）に登録し、個人にID登録番号（National Identity Register Number）を付与するとともに、これに基づくIDカードを発行するというものであった（図表17）。2008年11月には外国人（EEA域外）向けの滞在許可として生体認証IDカード（BPR：Biometric residence permit）が発行され、2009年11月にはマンチェスターで先行して一部住民向けIDカードが発行された。しかしながら、システム構築にかかる費用対効果が不透明であったこと（注37）や、政府による管理・監視社会に対する強い危機感、個人情報流出に対する懸念などもあり、2010年に同制度に反対してきた保守党・自由党の連立政権が成立したことで、IDカード法は廃止となった（ただし、外国人向けBPRのみ2007年イギリス国境法および2009年国境・市民権・移民法の規定に基づき制度として残った）。

（図表17）イギリスのIDカード法の概要

| | |
|---|---|
| 名　称 | IDカード法（Identity Cards Act 2006） |
| 成　立 | 2006年３月成立、2009年11月にIDカード発行開始 |
| 廃　止 | 2010年５月の政権交代、12月のID文書法制定に伴い2011年１月に廃止 |
| 目　的 | ・国家安全保障、犯罪の防止及び探知（なりすまし防止、テロ対策）<br>・出入国管理、不法就労・不法雇用の取締りの強化<br>・効率的・効果的な公共サービスの提供 |
| 対　象 | ・連合王国内に３カ月以上居住する16歳以上の者（外国人を含む） |
| 概　要 | ・個人情報（氏名、住所等）と生体情報（指紋や顔写真等）を個人情報のデータベース・国民ID登録簿（National Identity Register）に登録し、それに基づきIDカードを発行<br>・当初は、指定書類（パスポート）の発行や更新に付随したNIR登録とカード発行を想定<br>・当初の取得は任意、その後法制化によりNIRへの登録とIDカードの保有の義務付けを予定 |
| 利用場面 | ・身分証明書ならびにEU域内のパスポートとして利用<br>・民間サービス利用時の本人証明として利用（銀行、郵便・宅配、ビデオレンタル、固定・携帯電話、旅行・航空、大学、オンラインショップ、不動産賃貸、レンタカーなど） |
| 登録情報 | ・氏名、生年月日、出生地、国籍、性別、在留資格、住所、身元確認に利用できる身体的特徴（生体認証情報を含む）、身元確認目的で割り振られた国民ID登録番号及びそれに関連した書類（※）、その他自発的に提供された情報<br>※国民保険番号、パスポート番号、運転免許証番号、番号の有効期間など<br>※人種、政治思想、宗教、健康状態、性的ライフスタイル、犯罪歴に関するものを含めてはならない |
| 議　論 | ・ロンドン・スクール・オブ・エコノミクスの委員会報告書（2005年６月）は、IDカード制度の効果（身元情報の偽造・窃盗の防止、電子商取引市場の発展）を認めつつも、テロ防止の目的の達成、費用対効果、制度の複雑さ、技術的な安全性、公共の信頼性などで問題があると指摘<br>・そのほか、市民的自由の侵害、政府による大量・多岐にわたる個人情報の収集により管理・監視社会、制度を監視する管理官の独立性に対する疑問などの問題点が提起された |

（資料）国際社会経済研究所「国家情報システム（国民ID）に関する調査研究報告書―英国、フランス、イタリア等における番号制度の現状－」2011年３月を基に日本総合研究所作成

B．GOV.UK Verifyを巡る動向

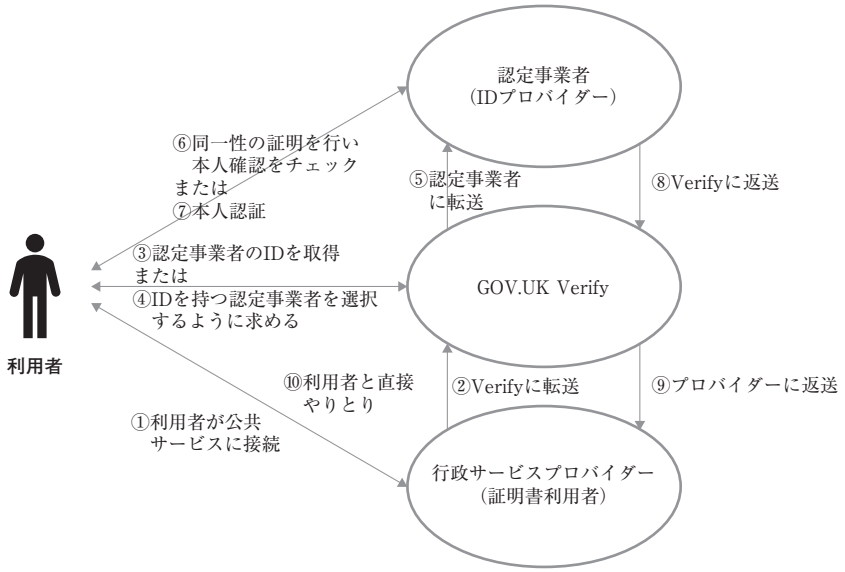
a．GOV.UK Verifyの概要

この代替策として、2011年に“Identity Assurance Service”プロジェクトが発表された。銀行や郵

便局、スーパーマーケットなど民間企業が発行するIDを、公共サービスにアクセスする際の本人認証手段として活用するというものである。具体的には、各政府機関が提供するサービスを利用する際に、共通プラットフォーム「GOV.UK Verify（以下Verify）」を通じて、民間事業者の認証を受ける仕組みで、利用者は政府の認定を受けた複数の事業者（IDプロバイダー）の中から自分が利用する事業者の選択・登録を行う（図表18）。

当初は、ユニバーサルクレジット（低所得層向け給付制度）での活用を目的として、雇用年金省が開発に従事していたが、その後、政府横断的なデジタルサービスを担うGDS（Government Digital Service）が主導し、名称もGOV.UK Verify（以下、Verify）に変更された。2014年２月にプライベートβ版、10月にパブリックβ版がリリースされ、2016年５月に本格運用を開始した。

（図表18）GOV.UK Verifyの仕組み




（資料）Edgar A. Whitley［2018］

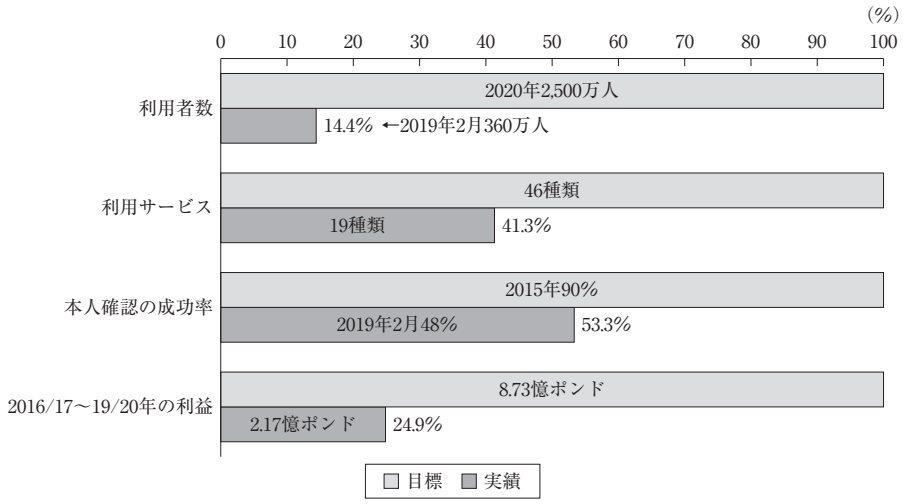
イギリス政府は、民間IDプロバイダーを使用する理由として、①ユーザー自身がIDプロバイダーの選択や使用の中止を判断可能、②集中化されたIDのデータベース構築が不要、③単一サービスでないことによるセキュリティの強化、④民間事業者間の競争による市場の発展、⑤民間事業者により利用可能な技術を最大限に活用、の５点を挙げている。

Verifyを通じて、税金の払い戻しの請求や運転免許の記録の確認など、16種類の公共サービスが利用可能である（2020年１月現在）。イギリス政府は、政府の全てのデジタルサービスへのアクセスに利用されるとともに、医療・社会サービスや民間セクターへと広範に活用されることを期待していた。認定事業者は、バークレイズ（銀行）、デジデンティティ（オランダのソフトウェア企業）、エクスペリアン（アイルランドの信用情報・データ分析企業）、ポストオフィス（郵便局）、セキュアアイデンティティ（IDプロバイダー・モルフォのサービス）の５社である（2019年９月現在）。また、利用者数は2020年１月時点で約600万人である（注38）。

ｂ．顕在化した課題

Verifyは、市民が公的サービスを利用する際に、自分が選択した民間のIDプロバイダーを利用可能とする野心的な試みであるものの、成功していないと評価されている。イギリス政府は、当初2012年にVerifyの本格運用を開始する計画であったが、実際には2016年にずれ込んだ。また、GDSは2016年の事業開始時に、2020年までにGOV.UK Verifyの利用者数2,500万人、利用可能な政府サービス46種類とする目標を設定した。しかしながら、会計検査院（NAO：National Audit Office）の調査（注39）によれば、2019年２月時点での利用者数は360万人で一人当たりの取引数は平均2.5、利用可能なサービスはβ版も含め19種類にとどまる（図表19）。しかも、19種類のうち11種類は他のオンラインシステムを使用してアクセス可能であり、Verifyを使おうというインセンティブとしては不十分である。一部サービスでは認証手続きの手動での処理が想定よりも多く生じ、コスト増加要因ともなっている（注40）。デジタルIDを利用するために行うプロバイダーにおける本人確認の成功率は、2015年に90%を達成すると予測されたが、2019年２月時点で48%であった。認証の設定ができないために、途中で脱落している利用者も多い。

（図表19）GOV.UK Verifyの目標（2016年）と実績（2019年２月）




（資料）National Audit Office “Investigation into Verify” March 2019

GDSは、2016年から2020年の間にVerifyは8.73億ポンド（約1,250億円）の利益（費用は2.12億ポンド／約303億円）を得ると推計し、2018年３月には自己資金で運営できるようになり、政府資金が必要なくなるとしていた。しかしながら、そのような利益を実現することはできず、見込まれる利益は４分の１の2.17億ポンド（約310億円）に修正された（前掲図表19）。

このように、現状は当初の計画に遠く及ばず、認定事業者（IDプロバイダー）の７社のうちGBグループ（サービス名：シチズンセーフ）とロイヤルメールが政府との契約の更新を止めた。政府は、2018年10月に残りの５社と引き続き契約を締結したものの、期間は18カ月であり、民間部門による自立を促すために2020年３月で資金提供を停止すると発表している（注41）。このため、バークレイズ、エクス

ペリアン、セキュアアイデンティティは、Verifyからの撤退を表明している（注42）。

Verifyの普及率が低い理由として、手続きに想定以上の時間がかかるなどユーザーエクスペリエンス（UX）が不十分であることや、関係する省庁が必ずしも協力的ではないこと（注43）、などが挙げられている。また、Verifyの利用対象となっている政府サービスがNAOの調査当時で19種類しかなく、それらの多くはVerifyがなくても利用できるため、登録のインセンティブとなっていない（現在利用できるサービスはさらに減少）。実際、調査当時に登録されていた360万アカウントにおいても取引の利用率が低いこと（一人当たり平均2.5件）が問題視されている。このため、NAOからVerifyの廃止が提言された。

C．今後のデジタルID政策を巡る議論

イギリスではVerifyの普及が進まない一方で、ID等を不正利用するなりすましの被害が急増しており、デジタル経済・社会の進展とともに安全性の高いデジタルID導入の必要性が高まっている（注44）。デジタルIDが必要とされる局面が増えるにつれ、これを利用する市場の拡大が予測されており、新たな成長分野におけるイギリスの国際競争力を確保する観点からも、デジタルIDの開発は政府の産業政策上の重要課題ともされている。

こうした状況下、2019年 6 月にデジタル文化・メディア・スポーツ省（DCMS）と内閣府により「Digital Identity Unit（DIU）」が組成された。DIUは、公共部門と民間部門の間の相互協力の促進や、相互運用が可能な標準や仕様の策定をミッションとし、デジタルIDの利害関係者から意見を集約し、個人データ保護法に準拠した信頼性の高いデジタルIDシステムの構築に向け、新たなプログラムを検討中である。

DIUでは、取り組みの優先順位として、①デジタルIDの追跡と利用を容易にするための標準化を支援、②民間部門・公共部門のサービス全体でデジタルIDが機能するように支援、③政府のデータのよりよい活用、④デジタルID市場の信頼醸成を支援、を挙げている。もっとも、これまでの経緯もあり、中央集権的な国民登録データベースやIDカードシステムの構築は行わない方針である。2019年 7 月には、政府がデジタルIDの開発と安全な使用をどのように支援していくべきか、国民に広く意見を求めるコンサルテーションペーパーを発表している。また、2020年 4 月から約 1 年間の予定で、政府が保有するパスポートのデータを利用して、民間企業がサービス（クレジットカードの申し込みなど）の利用者の本人確認（HMパスポートオフィスのデータベースと照合して確認）を行う「Document Checking Service（DCS）」のパイロットプロジェクトに取り組む予定である（注45）。

一方で、イギリスには依然として、デジタルIDの基盤で識別子となる統一的な国民番号の枠組みが不在である。下院科学技術委員会は、単一の一意の識別子としての国民番号について一部機能に対する懸念はあるものの、政府は一貫性のある本人確認の価値を認識し、国民的議論を推進すべきと提言している。同報告書は、「単一の一意の識別子は、政府のサービスの効率と透明性を変えることができる」としており、単一の一意の識別子としてeIDを導入しているエストニアの事例を挙げ、（政府機関の）誰が、いつ、どのような目的でどの種類の個人情報にアクセスしたかについて、情報の所有者は正確に知る権利があり、国民的な議論を通じて確認すべきだとしている（注46）。

（注13）出資は、Danske Bank、Handelsbanken、Ikano Bank、Länsförsäkringar Bank、SEB、Skandiabanken、Swedbankの７行。
（注14）認証用は、ウェブサイトなどにアクセスした人物や組織が本人であることを確認するために用いる。署名用は、インターネットなどで申請や手続き等を行うときに文書の作成者の身元や文書の真正性を証明し、成りすましや改竄を防ぐ。
（注15）Finansiell ID-Teknik BID ABのKenneth Tessem氏へのインタビューによる（2020年１月14日実施）。
（注16）デジタルIDを所管するスウェーデン電子ID委員会（Swedish e-Identification Board）は、2018年に設立されたDIGGの一部門となった。
（注17）Nordén［2007］。このうち、②のノルデア銀行は2015年にBank IDと統合した。また③のテリアソネラは、2010年のモバイルIDの開発に関与している。政府や地方自治体はBank ID等デジタルIDプロバイダーに対し、利用者数と利用状況に応じて使用料を支払っている。なお、テリアのデジタルIDは、2017年秋以降は入手できず、既に発行されたものは有効期限までとされている（DIGGホームページによる）。
（注18）６桁の数字と４桁の数字の間はマイナス（－）で繋がれており、100歳を超えるとプラス（＋）になる。また、外国人は、１年以上滞在する場合に住民登録により個人識別番号が付与される。
（注19）Lotta Hämäläinen, Roger Fagerud, Sven-Erik Ceedigh“The Swedish eID system”による。
（注20）出口治明「社会変革の起爆剤になり得るマイナンバー制：スウェーデンの事例を虚心坦懐に学ぶべき」ダイヤモンドオンライン、2013年４月16日付。また、総務省資料によれば、「スウェーデン憲法では、公文書の情報開示原則（Principle of Public Access to Official Documents）が定められており、原則として、公的機関が持つ公文書は全て公開されるべきもの。住民登録データベースにある情報もその例外ではない。ただし、本人又はその近い親類に危害が及ぶおそれがあると思われる場合には、情報を非公開とすることができる」（総務省「諸外国における住民登録制度について」http://www.soumu.go.jp/main_sosiki/kenkyu/daityo_eturan/pdf/j_daityo_eturan06_s01.pdf）。
（注21）住民登録は、もともと16世紀より教会が行っていた経緯がある。1947年にはPINが導入され、1960年代にはコンピュータで管理されるようになり、納税者番号としても利用されるようになった。1991年には、住民登録業務の所管が教会から国税庁に移管された。
（注22）総務省の資料によれば、「大量の情報提供向けにSPARというデータベースが作られており、そこからの情報提供については、例えば銀行の場合には、①PIN、②氏名、③住所、④配偶者、⑤過去３年間の記録となっており、また、DM（ダイレクトメール）の場合には、①氏名、②住所となっている。ただし、DMに関しては、住民からオプトアウト（拒否の選択）の申し出があった場合は、当該住民に関する情報の開示はしない」（総務省「諸外国における住民登録制度について」http://www.soumu.go.jp/main_sosiki/kenkyu/daityo_eturan/pdf/j_daityo_eturan06_s01.pdf）。
　また、「誰でも手数料を支払いさえすれば、SPARからの情報を取得できるというわけではなく、情報提供先の企業等がSPARの情報を提供することに対して妥当であるかどうかを、法律や個人情報保護法等に照らし合わせて審査したうえで情報提供が行われる」（東京税理士会国際部［2012］）。
（注23）Finansiell ID-Teknik BID ABのKenneth Tessem氏へのインタビューによる（2020年１月14日実施）。
（注24）Finextra“Banks have been the catalyst for Nordic digital identity success”April 9, 2019（https://www.finextra.com/newsarticle/33655/banks-have-been-the-catalyst-for-nordic-digital-identity-success）。
（注25）DNB Markets“VERISEC -David and Goliath”September 2019（https://www.verisec.com/sv/wp-content/uploads/sites/2/2019/09/Verisec-sponsored-reserach-Initiation-of-coverage-David-and-Goliath-final-20190903.pdf）、OECD［2018］など。
（注26）DIGGは、①選定システム（Electoral System）：市民が使用するデジタルIDを制御できること、②連合アーキテクチャ（Federated Architecture）：複数のプロバイダーにより提供されていること、③Quality Mark（品質マーク）：政府が品質を保証する「Svensk e-legitimation」を付与していること、をデジタルIDの基本的な枠組みとしている。品質マークを取得しているのは、AB SvenskaとFreja eID+であり、Bank IDは申請中である。
（注27）DIGGのLotta Hämäläinen氏、Roger Fagerud氏へのインタビューによる（2020年１月14日実施）。
（注28）Hans Graux, Jarkko Majava“eID Interoperability for PEGS: Analysis and Assessment of similarities and differences - Impact on eID interoperability”November 2007（https://ec.europa.eu/idabc/servlets/Doc0939.pdf?id=29618）。
（注29）スウェーデン政府公式報告書（“Ett säkert statligt ID-kort - med e-legitimation”2019）。
（注30）スウェーデン法務省2019年３月27日付プレスリリース（https://www.regeringen.se/pressmeddelanden/2019/03/utredning-foreslar-nytt-statligt-id-kort-och-e-legitimation/）。
（注31）GovTechのNDIの責任者であるKwok Quek Sin氏の記事“Inside Singapore's National Digital Identity programme”TechRadar, September 3, 2019による。（https://www.techradar.com/news/inside-singapores-national-digital-identity-programme）。
（注32）Yip Wai Yee“Online marketplace Carousell users can now verify their identities using MyInfo”The Straits Times, July 2, 2019（https://www.straitstimes.com/business/companies-markets/carousell-adopts-singapore-government-service-myinfo-to-combat-fraud）。
（注33）Cristina Lago“Inside Singapore's National Digital Identity programme”August 16, 2019（https://www.cio.com/article/3432144/inside-singapore-s-national-digital-identity-programme.html）。
（注34）SingPassは、段階的に２要素認証（2FA）／ワンタイムパスワード、モバイルSingPass（パスワードは不要で生体認証また

はパスコード）へとセキュリティが強化されてきた。その間、物理的なカードでアクセスするようなシステムは構築されなかった。

（注35）Irene Tham“SingPass, CorpPass system failure fixed; SingPass Mobile fully restored on Friday”The Straits Times, November 29, 2018（https://www.straitstimes.com/tech/singpass-mobile-unavailable-restoration-in-progress-govtech）。

（注36）Irene Tham“The new system, which will build on existing SingPass, is likely to be in place in three years”The Straits Times, August 2017（https://www.straitstimes.com/tech/new-digital-identity-system-in-the-works）。

（注37）当初政府は、IDカード導入にかかるコストを10年間で55億ポンドとしていたが、ロンドン・スクールオブエコノミクス（LSE）の報告書では、最低106億ポンド・最高192億ポンド（中間値145億ポンド）に上ると試算された。また、スペインで発生した列車爆破事件などのテロ事件を国民IDカードで防止することは不可能であることが各方面から指摘された（岡久［2004］）。

（注38）Elizabeth Marsh-Rowbotham氏・Caroline France氏（Department for Digital, Culture, Media and Sports）へのインタビューによる（2020年１月10日実施）。

（注39）National Audit Office“Investigation into Verify”March 2019（https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify.pdf）。

（注40）労働年金省は、手動での検証に係る支出が今後10年間で約4,000万ポンドになると予想。

（注41）政府の資金支援は、利用者一人当たり20ポンドと推測されている（https://www.governmentcomputing.com/identity/news/commercial-concerns-push-two-idps-away-verify-heads-towards-private-sector-delivery）。

（注42）2019年８月23日付ComputerWeekly.com,の記事による（https://www.computerweekly.com/news/252469110/Three-more-identity-providers-to-withdraw-from-troubled-Govuk-Verify-programme）。

（注43）例えば、歳入関税庁はVerifyと重複する独自の認証サービス「Government Gateway」を運用しており、NHS Englandやスコットランド政府も独自のIDシステムの開発に取り組む（Bryan Glick“GDS loses digital identity policy to DCMS”June 11, 2018：https://www.computerweekly.com/news/252442712/GDS-loses-digital-identity-policy-to-DCMS）。

（注44）例えば、EUではeIDAS（電子ID保証制度、2014年７月制定）規則への対応の義務化（2018年９月）に伴い、域内のデジタル取引でeIDASの基準を満たすデジタルID等が求められるようになるなど、デジタルIDを利用する市場が一段と拡大すると予想されている。

（注45）“The Document Checking Service pilot scheme”October 2019（https://www.gov.uk/guidance/apply-for-the-document-checking-service-pilot-scheme）。民間事業者は顧客の本人確認のために、パスポート番号、氏名、生年月日、有効期限をGDS経由でHMPOに送信し、有効かどうかを「はい」または「いいえ」で返信することで、パスポートの有効性＝本人確認を行う仕組み。一回ごとに50ポンドを利用企業が負担（参加企業は、最低でも5,000回利用することとされている）。

（注46）The House of Commons Science and Technology Committee“Digital Government”July 2019（https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1455/145505.htm）。なお、報告書でアラン・チューリング研究所のヘレン・マーゲッツ博士は、「イギリスが抱える重要な問題は一意のデジタル識別子（Single unique identifiers）の欠如」であると指摘している。一方、Open Data Instituteのピーター・ウェルス氏は、ある特定部門が目的と関係のないものも含め全てのデータにアクセスできる可能性は望ましくないとし、（個人に関係する情報を束ねることが可能な）単一の一意の識別子には注意を要すると述べており、識者の間でも議論は分かれている。

## ４．デジタルIDの課題と今後の展望

前章では、デジタルIDへの取り組みについて代表的な事例を見てきたが、導入の経緯や制度の枠組みは、それぞれの国の歴史や社会の成り立ち、政府と国民との関係性などが深く影響しており、取り組み内容・発展経路も異なっている。もっとも、各国ともにデジタルID整備の必要性に対する認識は強く、安全性と利便性の両立やデジタルIDに対する国民の信頼の確保といった課題に直面している。ここでは、各国の取り組み事例を基に共通する課題について整理するとともに、デジタルIDを経済社会の便益に繋げるためにどのような取り組みが求められるのか、わが国への示唆を探る。

### （1）共通デジタルIDの導入に向けた課題

デジタルの世界で、個人が主張する本人であることや正当な資格・権利を有することを証明するためには、信頼性の高いデジタルIDの仕組みを構築することが不可欠である。その実現に向けては、Ａ．技

術的な（デジタルIDシステム自体の）課題、B．社会的な課題、C．運用上の課題、への対応が求められる。それらは以下の通りである。

A．技術面（デジタルIDシステム自体）の課題

第1に、セキュリティの強化が挙げられる。先に述べたように、エストニアでは2017年にデジタルIDカードのICチップの脆弱性が問題となり、発行済みeIDカード約80万枚がリスクに晒されることとなった。エストニアの場合、eIDカードの更新にコストと手間がかかったものの、大きな被害や深刻な影響を出さずに済んだことは不幸中の幸いであったといえる。デジタルIDやこれに紐づく個人情報が流出すれば、大変な混乱に陥るであろうことは想像に難くない。シンガポールの事例では、セキュリティの問題ではないものの認証システムのソフトウェアの不具合により、これに依拠する公共サービスが機能不全の状態に陥り、不利益を被る人や企業が出ることとなった。

第2に、個人を一意に特定する識別子の存在である。官民のサービスで共通に使えるようにするためには、唯一性とともに普遍性や永続性が求められ、信頼性の高い主体により統一的に付与されていることが望ましい。スウェーデンやシンガポールでは、全国民・居住者に付番される個人識別番号（PIN）や国民登録番号（NRIC番号）があり、これをデジタルIDの識別子として使うことで、オンライン上でも個人を一意に特定できている。一方、イギリスの場合には、国民保険番号（NINO、NI番号）や国民医療制度番号（NHS番号）など分野別に複数の番号制度はあるものの、全国民・居住者をカバーできるものはなく、先に述べたようにデジタルIDスキームを構築する際の課題として指摘されている。

第3に、利用者にとってのユーザビリティの実現が重要である。イギリスの場合、ユーザーエクスペリエンス（UX）が不十分であったため、利用者の半数近くがデジタルIDの取得まで至らずに途中脱落することとなった。このことは、普及が進まなかった要因の一つとして指摘されている。一方、スウェーデンやシンガポールでは、カードやファイルタイプより使い勝手がいいモバイルタイプのデジタルIDが登場したことで、普及が拡大している。

なお、安全性と利便性という二つの課題は、トレードオフの関係にある。すなわち、官民共通で使うことができるデジタルIDを導入するに当たり、安全性の高い堅牢なシステムとすることが大前提であるが、これを重視するあまり使い勝手が悪いものになると、結果としてユーザーに使われないものになってしまう恐れがある。したがって、安全性と利便性のバランスをいかに確保するか、技術面と制度面の両輪での対応が強く求められている（注47）。

B．社会的な課題

社会的な課題としては、特に重要と考えられるのが第2章で述べたプライバシーの保護であるが、もう一つの課題として社会包摂への配慮が指摘できる。サービス毎に事業者が設定するデジタルIDであれば、そのサービスの利用者に限定されていてもよいのであろうが、国民・居住者が自分の身分証明として、また公共サービスへのアクセス手段として用いるのであれば、希望する者全員が利用できるものとしなければならない。スウェーデンでは、Bank IDの利用対象者が限定されていることが問題視されており、統一的な国民ID（物理的IDにデジタルIDの機能を搭載したもの）の導入が提案されている。

利用者の包摂という観点では、デジタルデバイドにも配慮する必要がある。デジタルIDを使用できるデバイスの保有・利用が所得や能力により差を生むことになれば、デジタルサービスやそれに伴う便益から排除される者が出てくることになるからである。

なお、社会的課題に関連する重要な示唆として、利用者（国民）と「身元検証者」（国や民間IDプロバイダー）との信頼関係の構築が指摘できる。スウェーデンでは、国やデジタルIDの身元検証者の一つである銀行（Bank IDの発行元）に対する国民の信頼が高く、国が個人識別番号（PIN）を本人確認のための識別子として官民の様々なサービスに使用することについても抵抗がないことは先に述べた通りである。適切な情報公開により、デジタルIDの導入が納税申告の簡便化ばかりでなく、税負担の透明性・公正性に繋がっていると国民が理解しており、高い税率に対しても充実した福祉として国民にきちんと還元されていると納得している。シンガポールも同様に、政府に対する国民の信頼は高い。これとは逆に、イギリスでは2006年IDカード法に対する政府の説明や公開情報に対する不信感が重なり、その後の廃案に繋がった。その後、Verifyを導入したものの、技術仕様や使い勝手が満足の得られるものではなく、また身元検証者であるデジタルIDプロバイダーに対する信頼性も政府が認定していたとしても不十分であったこと、政府が設定した目標が楽観的過ぎたことなどから、これを利用する国民・サービスプロバイダー（公共機関・民間企業）との信頼関係を構築することに失敗している（注48）。

C．運用上の課題

実際のデジタルIDの運用に当たっては、利用者にとって公共サービスばかりでなく民間サービスでも使え、利便性や効率性の実現など、直接的・間接的な利益がもたらされることが重要である。そのためには、利用者である国民の生活に密着したサービスがデジタル化され、多方面で共通のデジタルIDを利用できることが、利用の動機づけとしても望ましい。スウェーデンの場合には、日常的に使用する銀行のデジタルIDが業界で統一され、他の公共サービスや民間サービスでも共通に利用できることが普及の拡大に繋がった。シンガポールはこれとは逆のアプローチではあるが、公共サービスで利用するデジタルIDが個人情報のデータベースとリンクしており、共通APIの公開を通じて民間サービスでも利用できる共通プラットフォームとすることで普及を推進し、国民の利便性を高めようとしている。

これらの事例から得られる示唆は、デジタルIDを用いて個人の身元確認をしようとする官民のデジタルIDプロバイダー、サービスプロバイダーの協力体制の整備であり、広く関係者を巻き込んでいく必要がある。イギリスでは、政府内で省庁の足並みが揃わず、それぞれが既存の独自の認証システムを使い続けており、GOV.UK Verifyを公共サービスの共通IDとすることができていない。また、民間セクターのなかでは銀行業界による採用が期待されていたが、実際には銀行業界が遵守すべきAML（アンチマネーロンダリング）等の要件の解釈と適合していないとみなされ、使用が困難とされている（注49）。GOV.UK Verify導入に当たり主導してきたGDSにおいて、関係する省庁や民間セクターとの協力体制を整備する取り組みが不足していたことによるものと考えられる。

民間側の問題もある。初期のスウェーデンのBank IDで一部銀行に見られたように、多くの企業は自社の保有する顧客情報等を自社内に囲い込もうと考え、デジタルIDに関しても競合他社と協調して取り組もうとせずに自社のみに閉じたものとしがちである。しかし、それでは利用者の利便性や効率性に

繋がるものとはならない。スウェーデンの事例では、業界内でデジタルIDを協調領域と捉えることで一致し、その結果としてより広範な利用者をデジタルサービスに取り込むことができ、各社のコスト削減や利用者の利便性向上、新たな付加価値サービスの提供などの便益に繋がっている。

(2) デジタルIDを経済社会の便益に繋げるために

第2章で述べたように、デジタルIDにはメリットとデメリットが存在する。もっとも、情報のデジタル化が経済・社会で進展する中、デジタルIDへの対応は、民間企業も政府・公共機関も避けて通れない。このため、先に見た各国の事例でもメリットを具現化しつつデメリットを縮小・解消していくために様々な試みがなされている。こうした点でデジタルIDへの取り組みは未だ模索が続いている状態といえるが、デジタル化の便益を社会全体で広く享受できるように、わが国でも共通のデジタルIDスキームの在り方について、政府のリーダーシップのもと関係者と広く議論していく必要があると考えられる。その際には、先行する事例を踏まえ、以下の点も含めて検討していくことが求められよう。すなわち、共通のデジタルIDスキームに向けた、①政府と民間の対話と協調、②積極的な情報の公開とリテラシー教育、③先端技術のデジタルIDへの応用、④これらについて責任をもって推進する組織の設置、である。

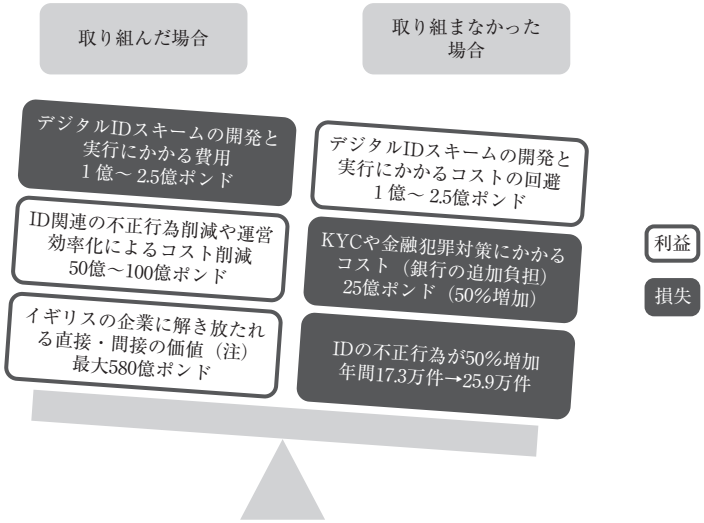
第1に、まずはデジタルIDの推進者でありサービスプロバイダーとなる政府・地方自治体や民間セクターにおいて、共通のデジタルIDスキーム構築に向けた対話と協調が求められる。

イギリスの事例のように、政府の一部門だけでデジタルIDの導入を検討しても、これを導入する政府の他部門や民間企業（サービスプロバイダー）、利用者である市民にとっては不十分な仕様となる可能性がある。また、政府内や地方自治体、民間企業の足並みが揃わないと、依然としてバラバラのIDが林立することになり、利用者に不便を強いることになる。関係者の対話や議論を通じて、シンガポールのような公的デジタルIDへの統一を図るのか、あるいはスウェーデンのような官民連合型（Federated）とするのか、といった官民共通のデジタルIDのフレームワークや、デジタルIDに必要とされる要件、標準化や相互運用性、ルールの設定（注50）、工程表などの検討を進めていく必要がある。

第2に、利用者となる市民や民間企業等に対し、共通デジタルIDスキームに関する適切な説明や情報公開が必要である。その際には、デジタルIDの共通化や導入による利便性や効率化などの効用について訴えるばかりでなく、「何もしないことのリスクやコスト」、「導入したことによる効果」について、数値まできちんと示す必要があろう。例えば、Open Identity Exchange（OIX）［2018］はイギリスにおけるデジタルIDへの取り組みの有無について、具体的な数字で利益や損失を示しており参考になる（図表20）。もっとも、イギリスのVerifyでGDSが示したように現実的でない楽観的な数値ばかりを示す普及計画は批判の対象となり、逆に利用者の信頼を失うことになる。提供する情報は透明性の高いものとし、説明責任を果たす必要がある。世界銀行［2016］の分析によれば、政府の説明責任が強い国ほど広くデジタル技術を導入している。

また、情報公開・説明責任に加えて、デジタルIDや個人情報・パーソナルデータの取り扱いやリスクに関するリテラシー教育も求められる。シンガポールでは、政府のほか民間企業や市民団体が、高齢者向けにスマートフォンなどのデバイスの操作やセキュリティに関するトレーニングコース・ワークシ

（図表20）イギリスにおけるデジタルIDの取り組みの有無の比較
（2021年の時点）




（資料）OIX［2018］
（注）潜在的な価値創造には、デジタル経済におけるより広範なイノベーションへの触媒としてのデジタルIDが含まれる。

ョップを開催している。利用者である市民が、利用方法ばかりでなく、デジタルIDや自分のデータに関する正しい知識を習得できる場の設定が必要になると考えられる。

第3に、デジタルIDの分野における生体認証やブロックチェーン、APIなど先端技術の活用について研究を進める必要がある。例えば、顔や指紋などの生体情報は、既にスマートフォンやパソコンでデバイスにアクセスするための暗号鍵として利用されている。そこで、シンガポールでは既存のデジタルIDとデバイス、デバイスに登録された生体認証とを組み合わせることにより、本人確認の精度を上げていくことや、将来的には高度化された生体認証のみでカードやスマートフォンのような物理的な媒体を不要とする可能性も考えられている。わが国においては、特に災害時の被災者や救急搬送された患者の本人確認について、デバイスを用いなくても可能とすることは効果を発揮すると考えられる（注51）。そのほか、デジタルIDを社会インフラとして共通に活用できる基盤を作るためにAPIの取り組みを進めていく必要があろう。シンガポールでは、NDIに関連する共通APIが次々に開発・公開されている。既にわが国でも、マイナポータルと民間サービスの連携を促進させるためにマイナポータルAPIが提供されているが、さらなる拡充が求められる。また、デジタルIDのセキュリティや信頼性を高めるうえで、ブロックチェーンの技術の活用を検討することも重要になってこよう。

第4に、共通デジタルIDスキームの構築について責任をもって推進する組織の設置が必要になると考えられる。先行する事例の多くで、政府内にデジタルIDを担当する専門組織が設置されている。イギリスでは、政府のデジタル化をGDSが担当していたものの、関連省庁に対する権限を有さず、Verifyの普及が計画通りに進まなかったため、新たに省庁横断的な組織が設置された。わが国では、デジタルIDに関する検討会や研究会が散発的に設置されてきたものの、正面から共通デジタルIDスキームについて論じるものではなく、省庁横断的な常設組織でもない（注52）。共通のデジタルIDスキームの具体

的な検討や推進について責任を負う組織の設置が必要ではなかろうか。

なお、イギリスのOIX［2018］によれば、政府は「ファシリテータ」としての役割を果たすべきとしており、シンガポールでも政府は「プラットフォーム」としての位置づけにある。わが国においても、政府は官民共通のデジタルIDスキーム構築に向けたファシリテータとして関係者の対話と協調を促すとともに、相互運用性の確保やAPIなどのプラットフォーム機能を提供する役割を果たすことが望まれる。

（注47）このソリューションの一つとして、ブロックチェーンの活用が模索されている。例えばエストニアでは、データ交換基盤のX-RoadにスタートアップのGardtimeが開発したKSI（Keyless Signature Infrastructure）ブロックチェーンと呼ばれる独自の技術を導入し、データの完全性を検証している。

（注48）Jerry Fishenden “Implementing a 21st century approach to digital identity” Computer Weekly, 2020年1月8日付（https://www.computerweekly.com/opinion/Implementing-a-21st-century-approach-to-digital-identity）。

（注49）Open Identity Exchange（OIX）［2018］。

（注50）デジタルIDの運用ルールの制定、ルールを逸脱した場合や盗難・情報漏洩など不正行為に関する罰則規定などに加えて、誰が共通番号を付与するのか、提示されたIDや属性情報の真正性、デジタルIDスキームの安全性やデジタルIDプロバイダー、これを利用するサービスプロバイダーの信頼性などを誰がどのように担保するのかなども、重要な検討事項である。

（注51）なお、例えば指紋を認証に用いると表現する場合、「①全ての個人の指紋情報を、あらかじめデータベースに登録し、各個人を識別するIDとして活用する、②希望する個人が、あらかじめ自ら指紋情報を登録し、本人しか持ち得ない秘密の暗号鍵として活用する」の2通りのケースが考えられることに留意を要する（総務省「Society 5.0を見据えた個人認証基盤の在り方について（報告）」2018年6月、https://www.soumu.go.jp/main_content/000560721.pdf）。特に、前者の場合には利用者の抵抗感が強いと考えられることから、プライバシーに配慮しつつ、どのような生体情報をどのような認証で用いるのか、その認証を用いる手続きや取引に求められる本人確認の厳格性との関係なども考慮しながら検討する必要がある。

（注52）法人については、経済産業省の進める法人共通認証基盤がある。

## 5．おわりに

現行のデジタルサービスの多くが、依然としてユーザー名とパスワードによる認証に依存している。不正アクセス等では、こうした脆弱なシステムでパスワードが漏洩し、さらには同一のパスワードが使いまわしされているために、被害が拡大しているケースが多い。金銭や資産、医療、プライバシー関連などの重要な情報をやり取りするデジタルサービスでは、より堅牢なデジタルIDの導入が求められている。世界経済フォーラム（WEF）によれば、「デジタル化が進んでいる国では、政府がデジタルIDを導入していない国に比べ、金融機関に対するハッカー攻撃が少ない」ことなどが示されているという（注53）。本稿では、共通のデジタルIDが導入されていないため対象としなかったが、アメリカにおいても財務省から（特に金融取引における安全性や効率性確保のために）「Digital Legal Identity」の実現が提言されている（注54）。

デジタルIDには、①認証と、②データの紐付けによる属性情報へのアクセス・共有・連携の二つの機能がある。このうち、②については、官民の部門間・組織間を越えたデータの紐付け・連携等に対し、政府による監視・管理や情報漏洩に対する国民の抵抗感や不安が強く、法律面やシステム面でも様々な障壁が存在している。そこで、まずは本稿でも述べた信頼性・安全性の高い官民共通の公的認証基盤としてデジタルIDを定着させていくことが考えられる。官民共通の認証基盤としてデジタルIDの普及を進めるにあたり、シンガポールの「MyInfo」のように、申請や手続きなどを行う際に認証と連携して必要な個人情報が本人同意のもと自動的に入力される仕組み（Once Only）や、公的認証基盤を使った場合の手数料の減免措置など、デジタルIDの使用を利便性や負担軽減に繋げることが効果的と考えら

れる。その前提として、サービス提供側の業務フローや処理プロセスなどについて、デジタルIDに対応した徹底的な見直し（＝デジタルガバメントやデジタル変革の推進）が官民双方に求められる。その際には、「情報は誰のものか」の原則を明示し、徹底する必要がある。すなわち、基本的には国民の情報は国民自身のものとする考え方（注55）のもと、国民にとっての便益が最大になるように、共通デジタルIDスキームの設計ならびに業務の改革を進めていくことが肝要である。

（注53）Henrik Hvid Jensen「デジタル化で犯罪を撲滅する３つの方法」World Economic Forum、2019年11月28日（https://jp.weforum.org/agenda/2019/11/dejitaru-de-wo-suru3tsuno/）。
（注54）アメリカ財務省が提言する「Digital Legal Identity」は、特性や属性に基づき個人を一意に特定・本人確認でき、法律によって認められ、本人の権利や義務を証明する。実現に向けて、複数のサービス間で共通に利用可能（Portability）なシステムとし、官民のパートナーシップを強化する必要性が指摘されている（水口［2019］、Steven T. Mnuchin, Craig S. Phillips “A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation - Report to President Donald J. Trump” U.S. Department of the Treasury, July 2018）。
（注55）個人が「自分の情報を自分でコントロールする」という仕組みや考え方に関しては、拙著「個人起点のデータ流通システムの形成に向けて－イギリスのmidataの取り組みから得られる示唆」（JRIレビュー Vol.9,No.70、2019年８月）を参照されたい。

### 補論：共通デジタルIDとしてのわが国のマイナンバー制度

わが国でも共通のデジタルIDスキームの確立が望まれる中、公的な主体が保証するデジタルIDとしてマイナンバーカードの公的個人認証サービスを活用し、「ネットで完結する本人確認」の実現が期待されている（注56）。マイナンバーそのものは、マイナンバー法の見直しや個人情報保護への配慮、システムの改修などが必要とされ、現状では法や条例で定められた分野以外の活用はできないなど様々な問題を抱えており、解決には相応の時間がかかると考えられる（図表21）。しかしながら、まずは本人確認手段としてのマイナンバーカードの機能を利用することで、以下（1）で述べるメリットを享受できるものと考えられる。その利用に向けては、マイナンバーにかかる法制度やシステムの段階的な見直しとともに、（2）で述べる①物理的な手段への依存、②極めて高い番号の秘匿性、③デジタルバイデフォルトの不徹底、といった課題解決に取り組む必要があろう。

#### （1）マイナンバーカード利用のメリット

マイナンバーカードの公的個人認証機能をデジタルIDとしての利用を進めることで、以下の通り、オンライン・オフラインの双方でのより厳格な本人確認、官民のサービスのワンストップ化などが実現できる。

第１に、マイナンバーカードは物理的な身分証明書として認められているが、公的機関による証明ということで本人確認書類としての信用度が高い。そして、マイナンバーカードの公的個人認証サービスは、オンライン上での単なるIDとパスワードを使った認証手段に比べ、なりすましなどのリスクを低減できる。さらに、対面でカード提示の際にICチップの情報（電子証明書の所持情報=本人しか持ちえない情報）を読み取って本人と突合することで、本人確認の精度を向上させることが技術的に可能である。

また、現行の対面での本人確認手続きでは、本人確認書類の提出を求めるのはサービスの利用開始時

（図表21）マイナンバーをデジタルIDとして用いる際の問題点

| | 課　題 | 考えられる対応策 | 時間軸 |
|---|---|---|---|
| 国　民 | 番号が決して人に知られてはならない（という誤解）、カードをなくすと危険ではないかという懸念 | 番号が表示されているカードを持ち歩かなくても済むソリューション開発<br>⇒番号未記載の子カードの発行、モバイルID（アプリ）の開発 | 短　期 |
| | 情報を国に収集・把握されるのではないかと言う漠然とした不安 | 情報は個人のものという認識を、情報を受け取る側（行政、企業等）に徹底、その観点からサービス・業務等を見直し（Privacy by Design） | 中長期 |
| 行　政 | 法律で情報連携に制約<br>（例：税金の情報は地方税法22条で本人同意がないと移動できない） | 国民生活にとって必要とされるものから段階的に法律を改正、又は、法律の解釈を整理することが必要 | 中長期 |
| | 組織や権限が縦割りのため、一体化・情報連携が困難（例：運転免許証やパスポートとの一体化、戸籍謄本（注１）が情報連携の対象外など） | 同上<br>業務そのものの見直しを徹底（物理的な証書や書類を廃止、情報のやりとりは全てデジタルで行う方向） | 中　期 |
| | マイナンバーのシステムが使いにくく、情報連携より紙の提出の方が便利な場合がある | 例：住基ネットのシステムとの併存<br>⇒統合する方向で検討する必要<br>業務や法律の見直しが必要 | 中　期 |
| 民間企業 | 金融、通信、流通（、医療）など、それぞれの事業者が独自のデジタルIDをすでに導入 | 公的個人認証基盤の有効性、安全性の周知、事業者にメリットのある仕組みや措置の検討（例：マイナポータルから本人の指示やAPI接続により基本４情報（注２）などを入手できる仕組、民間の個人認証や事務手続きで必要となる印鑑の代わりに公的個人認証の活用を推進） | 中　期 |
| | マイナンバーカードの空き領域を活用する場合、ユーザーがICチップの書き換え手続きを行う必要 | カード形態ではなく、モバイル形態にするなど | 中　期 |
| | 利用者である国民に対し、取得や利用が義務とされていないため、取り組みが進まない（例：銀行口座についてマイナンバーの告知、カードの取得など） | 個々の事例について慎重に検討 | 中長期 |
| その他 | データの共通化（例：外字のコードや字形の統一） | 代替文字利用に対する理解促進と標準化の推進（デジタルガバメントや官民データ活用とも関係） | 中長期 |

（資料）つくば市政策イノベーション部情報政策課・家中賢作氏、日本電気(株)デジタル・ガバメント推進本部長・小松正人氏などにヒアリング
（注１）戸籍法の改正により、戸籍データとマイナンバーが連携する予定（2023年度）。
（注２）基本４情報とは、氏名、住所、性別、生年月日。

のみがほとんどで、その後は更新されないため、住所変更などが追跡できていないことが多い。マイナンバーカードは数年ごとに更新されるので、そうした情報の変動の有無を定期的に確認でき情報の鮮度を保てるメリットがある。将来的に、マイナンバーの異動情報とリンクされることになれば、自動的な更新も展望できる。このように、本人確認の厳格性や長期にわたり継続的な確認が必要な場合には、マイナンバーカードを利用することが有用と考えられる。

第２に、マイナポータルは政府が運営する国民向けオンラインサービスのポータルサイトで、マイナンバーカードでログインする仕組みであるが、このサイトでは公的サービスだけでなく、民間サービスの利用も可能とすることが想定されている。そこで、例えば引っ越しの手続きについて、地方自治体ばかりでなく、銀行や電気・ガス・水道等の住所変更の手続きを一元的に行えるようにすることが検討されている。それ以外にも、公的手続きと、それに連動する支払いを、同一画面で行うことなどが可能になると考えられる。

### (2) マイナンバーカードをデジタルIDとして用いるための課題

もっとも、利用の観点から見ると、現行のマイナンバーカードは、①物理的な手段への依存、②番号

の秘匿性、③デジタルバイデフォルトの不徹底、などが普及や利活用の阻害要因になっていると考えられる。

第1に、世界的にデジタルIDは物理的なカードから、モバイルや生体情報との組み合わせなど電子的な手段に移行しており、カードのような物理的な手段の形態だけでよいのか検討を要する。そもそも、わが国のマイナンバーカードは券面に番号が記載されている一方で、その番号をむやみに人に見せたりコピーさせてはいけないこととされており、人々が取得や携行はやめたほうがいいと考える逆インセンティブになっている。また、カード形態での利用は、カードリーダー（注57）とパソコンを必要とするため、どこでもいつでも公的個人認証サービスを使えるわけではない。まずは、わが国で既に世帯普及率約8割・個人で6割を超える（令和元年版情報通信白書）スマートフォン上で、デジタルIDとして使えるようにしていく必要があろう。

第2に、マイナンバーについて正しく理解されていないために、カードが取得されず、利用が進まない側面がある。とくに、カードに番号を表示していることが取得されない・使われない要因となっているのであれば、そもそも番号を表示しないことも検討に値するのではなかろうか。一つには、番号を表示しないサブカードの発行がある。もう一つには、シンガポールのSG Verifyのように、利用者の意思（生体認証や二段階認証による承認）のもとスマートフォンから必要な情報を読み取らせる方法が考えられる。また、現状ICチップ内には表面情報（住所・氏名・生年月日・性別の4情報＋顔写真）と裏面情報（個人番号）の画像データが記録されているので、提示を求める機関に対してはICチップの読み取りにより確認させる方法もあろう。なお、諸外国のなかにはエストニアやスウェーデンのように、番号そのものには意味がなく、日本のように自分の個人番号は絶対に秘密にしなければならないとする必要がないところも多い。

第3に、そもそも普及が進まないのはマイナンバーやマイナンバーカードの問題ばかりでなく、政府・地方自治体等によるデジタルサービスの供給体制にあると考えられる。依然として、マイナンバーの紙での提出やマイナンバーと紙の申請書との併用など、行政手続き等のデジタル化が進んでいないことによる問題も散見される。公的個人認証サービスでデジタルサービスが使われることを前提として、紙や印鑑の徹底的な廃止、ならびにマイナンバーカード所有者は住民票や印鑑証明書の添付を原則不要にすることを、まずは政府内、そして地方自治体において推進していくことが求められる。

なお、日本の場合、国民が政府による情報の管理に対する抵抗感が強いことがマイナンバー・マイナンバーカードの普及の阻害要因として指摘されることが多いが、それ以外にも、「住民管理行政における戸籍制度の安定的な地位が確立し、その管理体制の下で行政領域ごとに番号制度が形成」されたため、新たに導入されたマイナンバー制度とそれに付随するデジタルIDやデジタルサービスのメリットが十分に感じられるものではないことも普及の妨げになっているとの指摘がある（羅［2019］）。

以上でみてきたように、マイナンバーはデジタルIDの機能を持つものの、現行の関連法制度やシステム構成のままで、「個人を一意に識別できるID」として官民共通で使うにはまだ制約が多い。デジタルIDとして、将来のデータ連携を進めるためには、法制度やシステム、取扱い体制などの継続的な見直しが求められる。

（注56）なお、わが国をはじめ各国では、オフライン・オンライン双方ともにデジタルによる厳格な本人確認の実現が目指されている。例えば、国民IDカードやパスポート等に搭載されているICチップを、オンラインのみならず役所や銀行の窓口などの対面における本人確認にも利用するというものである。

（注57）なお、マイナンバーカードの読み取り対応をしているスマートフォンが登場しており、パソコンとブルートゥース接続してカードリーダー代わりに利用できるようになっている。もっとも、パソコン利用が前提とされているため、その携帯が必要とされる。また、マイナポータルについては、スマートフォン用アプリがリリースされている。

謝辞：本論文の補論作成に当たり、つくば市政策イノベーション部情報政策課・家中賢作氏、日本電気株式会社デジタル・ガバメント推進本部長・小松正人氏、同マネージャー 古屋晶子氏より、多くの貴重な示唆や助言をいただきました。厚く御礼申し上げます。

（2020. 3. 4）

## 参考文献

・岩崎薫里［2019a］.「India Stack：インドのデジタル化促進策にみる日本のマイナンバー制度への示唆」環太平洋ビジネス情報 RIM 2019 Vol.19 No.75、日本総合研究所、2019年11月
・淵田康之［2019］.「デジタル時代の世界と日本」野村資本市場クォータリー2019年夏号、野村資本市場研究所、2019年 8 月
・野村敦子［2019］.「シンガポールのスマートネイション戦略」リサーチ・レポート No.2019-009 、日本総合研究所、2019年 8 月
・岩崎薫里［2019b］.「デジタル社会基盤としてのマイナンバー制度のフル活用に向けて：まずはマイナンバーカード普及を」ビューポイント No.2019-017、日本総合研究所、2019年 7 月
・羅芝賢［2019］.「番号を作る権力－日本における番号制度の成立と展開」東京大学出版会、2019年 3 月
・各府省情報化統括責任者（CIO）連絡会議決定［2019］.「行政手続きにおけるオンラインによる本人確認の手法に関するガイドライン」2019年 2 月
・総務省［2018］.「Society 5.0を見据えた個人認証基盤の在り方について（報告）」2018年 6 月
・今井秀紀［2018］.「スウェーデンにおける住民登録番号制度を利用した大規模データベースの活用について―その 2 」社会薬学Vol.37 No.1 2018
・今井秀紀［2017］.「スウェーデンにおける住民登録番号制度を利用した大規模データベースの活用について―その 1 」社会薬学Vol.36 No.2 2017
・吉元利行［2017］.「キャッシュレス先進国の実情と課題―現金を使用せずに生活できる国スウェーデン―」CCR第 6 号、日本クレジット協会、2017年 3 月
・金貝［2016］.「先進諸国の医療ICT推進の最新動向―スウェーデンとエストニアの事例を中心に―」SciREX-WP-2016-#04、政策研究大学院大学、2016年 8 月
・世界銀行（翻訳：田村勝省）［2016］.「世界開発報告2016　デジタル化がもたらす恩恵」一灯舎（原文：「World Development Report 2016: DIGITAL DIVIDENDS」The International Bank for Reconstruction and Development/The World Bank）、2016年

・CLAIRシンガポール事務所［2015］.「シンガポール国民や外国人居住者への登録番号制度について～入国管理庁（ICA）、労働省（MOM）、情報通信開発庁（IDA）に訪問～」CLAIRメールマガジン2015年 7 月号
・国際大学グローバル・コミュニケーション・センター［2012］.「諸外国における国民ID制度の現状等に関する調査研究報告書」総務省、2012年 4 月
・東京税理士会 国際部［2012］.「2012年スウェーデン社会保障・税共通番号制度等研修視察報告書」2012年
・湯元健治［2011］.「共通番号制度導入への道筋―スウェーデンの実例に学ぶ利便性の高い番号利用を―」Business & Economic Review、日本総合研究所、2011年 9 月
・宮下紘（代表研究者）［2011］.「個人情報保護の執行制度に関する比較法的考察」電気通信普及財団研究調査報告書第27号、電気通信普及財団、2011年 9 月
・国際社会経済研究所［2011］.「国家情報システム（国民ID）に関する調査研究報告書―英国、フランス、イタリア等における番号制度の現状―」2011年 3 月
・渡辺周［2010］.「番号制度等に関するスウェーデン・オーストリア・ドイツの視察報告」2010年 5 月
・情報通信政策研究所［2010］.「IDビジネスの現状と課題に関する調査研究」総務省、2010年 4 月
・高橋健司［2009］.「アイデンティティ管理の現状と今後」『電子情報通信学会誌』92巻 4 号（2009年 4 月）
・岡久慶［2006］.「英国2006年IDカード法」外国の立法230、国立国会図書館調査及び立法考査局、2006年11月
・電子商取引推進協議会 認証・公証WG［2002］.「証明書利用形態に関する考察」2002年 3 月
・Citi［2019］.“The Age of Consent: The Case for Federated Bank ID” August 2019.
・OECD［2019］.“Digital Government Review of Sweden – Towards a Data-driven Public Sector” May 2019.
・Eloïse Margrethe Langaker, Heidi Gjersø Thaulow, Frank Wunderlich, Kim Catherin Kasch［2019］.“Federated e-IDs as a value driver in the banking sector based on experience from Nordic markets” Arkwright, April 2019.
・Open Identity Exchange（OIX）［2018］.“Digital Identity in the UK: The cost of doing nothing” April 2018.
・OECD［2018］.“OECD Reviews of Digital Transformation: Going Digital in Sweden” June 2018.
・Annie Göransson［2018］.“Electronic Identification as an Enabling or Obstructive force – The general public’s use and reflections on the Swedish e-ID” Linnaeus University, June 2018.
・McKinsey Global Institute（Author : Olivia White et al.）［2019］.“Digital identification: a key to inclusive growth” McKinsey Global Institute, April 2019.
・World Bank Group［2018］.“G20 Digital Identity Onboarding” January 2018.
・Edgar A. Whitley［2018］.“Trusted digital identity provision: GOV.UK Verify’s federated approach” CGD Policy Paper 131, Center for Global Development, November 2018.

・Ben Eaton, Jonas Hedman, and Rony Medaglia [2017]. “Three Different Ways to Skin a Cat: Financialization in the Emergence of National e-ID Solutions” Journal of Information Technology, 33(1), 70- 83.2017.
・World Bank Group, GSMA, Secure Identity Alliance [2016]. “Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation” July 2016.
・PBLQ（Dutch Institute for Public Administration）[2015]. “International Comparison eID Means” April 2015.
・Anna Nordén [2007]. “National Profile Sweden” IDABC, European Commission, 2007.
・https://govdata360.worldbank.org/subtopics/h21acc114
・DIGG E-legitimationホームページ
（https://www.elegnamnden.se/inenglish.4.4498694515fe27cdbcf13d.html）.
・Bank IDホームページ（https://www.bankid.com/en/）.
・シンガポールSmart Nationホームページ（https://www.smartnation.sg/）.
・シンガポールGovTechホームページ（https://www.tech.gov.sg/）.
・GOV.UKホームページ（https://www.gov.uk/）.