デジタル ID 時代の世界と日本

淵田　康之

▌要　約▐

1. デジタル情報を用いて自分の身分を証明するデジタル ID（Identification、身分証明）の重要性が高まっている。デジタル ID は、円滑なサービス提供に寄与するのみならず、アナログな身分証明よりも精度の高い本人認証につながりうる。
2. デジタル ID の整備は、SDGs（Sustainable Development Goals、持続可能な開発目標）の実現や AML/CFT（Anti-Money Laundering and Counter Financing of Terrorism、マネーロンダリング防止とテロ資金対策）の強化という観点からも、不可欠である。
3. 公的 ID 制度においても、デジタル ID への対応が進展しているが、その仕組みは発展途上であり、国によって様々な試みがなされている。ペルー、インド、エストニア、英国などの仕組みは、それぞれ、他国においても参考になる特徴がある。
4. 現時点では、ネット上の多くの取引において、本人確認はパスワード入力に依存し、カード決済もカード情報の入力のみで済むことが多い。これに対して、EU などでは SCA（Strong Customer Authentication、厳格な本人認証）を義務付ける動きがある。
5. わが国においては、公的 ID としてマイナンバーカードが導入されたが、未だ普及率は低く、そのデジタル ID への活用も途上である。アナログな身分証明や、昔ながらのパスワードやカード情報入力などに依存することの弊害も目立っている。デジタル ID を巡る世界の状況を踏まえた対応が求められる。

I　デジタル ID の意義

経済・社会のデジタル化が進展するなか、人々がネットにアクセスし、様々なサービスを享受し、また決済などの金融取引を行う機会が飛躍的に増大している。このため、ネット上で自分の身分を証明するデジタル ID の重要性が高まっている。

デジタル ID とは、電子的に取得（capture）され保管（store）された attributes（本人の属性）や credentials（本人であることを証明する認証情報、資格情報）であり、他人と区別して本人を特定（identify）するものである。

デジタル ID は、ネット取引において不可欠であるだけではなく、店頭での本人確認や入場者チェックなど、リアルな場面でも活用される。従来、写真や印鑑の目視など、アナログな形で行われていた身分証明に比べ、生体情報やネット上の様々なデータを活用することで、身分証明の精度の向上につながりうる。

今日、ID の整備は SDGs（Sustainable Development Goals、持続可能な開発目標）においても目指されている。デジタル ID の導入・普及は、SDGs 実現のためにも意義がある。

ID 制度が不十分であれば、AML/CFT（Anti-Money Laundering and Counter Financing of Terrorism、マネーロンダリング防止とテロ資金対策）の観点から、円滑な金融サービスの提供が困難となる。これは金融インクルージョンに反し、SDGs にも逆行する。デジタル ID が整備されれば、AML/CFT に則った形で、FinTech などの金融サービスも提供しやすくなる。

現時点では、ネット上の多くの取引において、本人確認はパスワード入力に依存し、カード決済もカード情報の入力のみで済むことが多い。この結果、様々な問題も生じている。そこで、EU などでは SCA（Strong Customer Authentication、厳格な本人認証）を義務付ける動きがある。

わが国は、公的 ID としてマイナンバーカードを導入したが、その普及は途上であり、デジタル ID への活用も進展していない。アナログな ID 認証や昔ながらのパスワード入力、カード情報入力などに依存することが依然として多く、各種の弊害も目立っていることから、デジタル ID を巡る世界の状況を踏まえた対応が求められる。

Ⅱ SDGs と ID

SDGs は、2015 年 9 月の国連サミットで採択された。17 のゴールと 169 のターゲットで構成されており、国連加盟 193 か国が、2016 年から 2030 年までの 15 年間で達成することを目指している。

SDGs のターゲット 16.9 に「2030 年までに、全ての人々に出生登録を含む法的な身分証明（legal identity）を提供する」と掲げられており、ID の整備は SDGs において求められている。

2018 年時点で、世界のおよそ 10 億人が、公的な ID を持たないと推計されている[1]。ID が無ければ、社会保障や教育の機会にも恵まれず、金融へのアクセスも困難である。このため ID の整備は、それ自体が SDGs のターゲットとして掲げられているのみならず、SDGs の他のゴールやターゲットを達成する上でも不可欠である（図表 1）。

[1] http://id4d.worldbank.org/global-dataset

図表 1　ID と SDGs

Target 16.9：2030年までに、全ての人々に出生登録を含む法的な身分証明を提供する

- **金融へのアクセス**
  - ✓ 所有権の証明 (Goal 1 & Target 1.4)
  - ✓ 銀行取引のKYCルールの充足 (Goal 1 & Target 1.4)
  - ✓ 信用情報機関向けのユニークなID (Target 8.3 & Target 1.4)
  - ✓ 送金コストの低減 (Target 10c)
- **ジェンダー平等**
  - ✓ 経済・社会活動への完全な参加 (Goal 5)
  - ✓ 金融分野のジェンダーギャップの是正 (Target 5a)
- **ベイシック・サービスへのアクセス**
  - ✓ 就学や受験の登録 (Goal 4)
  - ✓ 予防接種率の向上 (Goal 3 & Target 3.3)
  - ✓ 健康保険のためのユニークなID (Target 3.8)
  - ✓ 結核、HIV/AIDS治療の生体認証による追跡 (Target 3.3)
  - ✓ 医療データの登録: 乳幼児死亡率の低下(Target 3.2)
- **子供の保護**
  - ✓ 年齢の証明：児童労働の撲滅 (Target 8.7)
  - ✓ 年齢の証明：児童婚の根絶 (Target 5.3)
- **労働の機会**
  - ✓ 雇用の取引コストの削減 (Goal 8 & Target 8.5)
  - ✓ 秩序ある、安全な移住の促進 (Goal 10 & Target 10.7)
- **社会保障（扶助・補助）**
  - ✓ 支払のターゲティング、タイムリネス、コスト効率性の改善 (Goal 1 & Target 1.3)
  - ✓ 透明性の向上とリーケージ（受給対象者以外による中間搾取）の削減のためのユニークなID (Target 1.3)
  - ✓ 緊急的支援の迅速かつ効率的な実行 (Target 1.5)
  - ✓ 燃料補助の改革：価格補助から金銭支給へ(Target 12c)
- **公務員給与の管理**
  - ✓ ゴースト・ワーカーの排除、歳出のムダの削減 (Goal 16 & Target 16.5)
- **徴税**
  - ✓ 共通のIDにより税の捕捉率向上 (Target 17.1)
- **クリーンな選挙**
  - ✓ ユニークなIDによる選挙権者の登録 (Target 16.7)

（出所）Alan Gelb and Anna Diofasi Metz, *Identification Revolution: Can Digital ID be Harnessed for Development?*, Center for Global Development, 2018.　より野村資本市場研究所作成

Ⅲ AML/CFT と ID

1．FATF 勧告における CDD

適切な ID の仕組みの存在は、世界が目指すもう一つの重要課題である AML/CFT[2]の観点からも不可欠である。FATF[3]が 1990 年に最初に発表した 40 の勧告（第一次勧告）においても、顧客の ID 確認は重要な柱となっていたが[4]、2003 年の FATF 勧告改訂で、CDD（Customer Due Diligence）という精緻な枠組みが導入された。この内容は、最新版である 2012 年勧告の勧告 10 に引き継がれている。勧告 10 には、9 ページに及ぶ interpretive note も付されており、この分野は FATF 勧告の中でも、もっとも包括的で詳細に論じられているところである。

[2] CFT（Counter Financing of Terrorism）は、CTF（Counter Terrorism Financing）と表現されることもある。

[3] 1989 年のアルシュ・サミットを受け、マネーロンダリング問題に対応すべく設立された政府間組織。Financial Action Task Force on Money Laundering の略。「マネーロンダリングに関する 40 の勧告」は、1990 年に提示された。2001 年には、テロリズム・ファイナンス関する 8 つの特別勧告も策定された。2012 年、これまでのマネーロンダリングに関する勧告とテロリズム・ファイナンスに関する特別勧告が統合され、新たな「40 の勧告」が提示された。

[4] 「金融機関は匿名や偽名口座を受け入れないこと、そして顧客と取引関係を構築するにあたり、あるいは取引を行うにあたり、随時ないし常時、公的ないし他の信頼できる ID 文書をベースに顧客を identify し、また identity を記録しなければならない」というのが、当初の勧告の記述である。

勧告 10 によれば、金融機関[5]は、(i)顧客と取引を行う関係となる場合、(ii)15000 ドル（ないしユーロ）超の取引を行う場合、及び電信送金を行う場合、(iii)マネーロンダリングやテロリスト・ファイナンシングの疑いがある場合、(iv)過去に入手した顧客の ID データの正確性、適切性に疑いを持つとき、CDD を実施しなければならない。

CDD の詳細は、各国の法律で規定され、実行されるが、FATF 勧告でまず求められていることは、「顧客を identify し、その identity を信頼できる、かつ独立した原資料（source documents）、データ、情報を用いて、verify すること[6]」である。

２．金融インクルージョンとのバランス

このように FATF 勧告は CDD を要求しているが、この手続きが厳格に過ぎれば、SDGs に反しかねない。特に、ID を保有しない人々が世界には多いという現状の下では、AML/CFT を徹底すればするほど、こうした人々がますます金融サービスから遠ざけられることとなる。

FATF としても、その目的とする所は、正規の金融取引の促進であるため、手続きの厳格さ故に、非正規の金融取引が蔓延することは望ましくなく、金融インクルージョンの推進は、FATF の立場と整合的である。

そこで 2010 年 6 月、FATF は金融インクルージョンをアジェンダの一つに位置づけ、2011 年にガイダンスを公表している。その後、FATF 勧告の 2012 年改訂で、リスクベースト・アプローチが導入されたことなどを踏まえ、新たなバージョンが 2013 年に公表されている。

リスクベースト・アプローチでは、リスクの懸念が大きくない場合など、一定の条件の下で簡易な CDD の適用が可能とされる。この点を活用することにより、金融インクルージョンとの両立が各国で工夫されるようになっている。2017 年 11 月には、CDD に関する各国の新たな動向などを踏まえた補足的なガイダンスも発表されている[7]。

FATF 勧告は、ID データ（国民 ID カードやパスポートなど身分を証明する情報）や ID エレメント（identifiers、生年月日、性別、勤務先、住所など身分の証明に関わる要素）として何を求め、どう verify すべきかについて、具体的には規定していない[8]。2013 年及

---

[5] 預金取扱金融機関の他、各種の金融業務を営む者が含まれる。この他、FATF 勧告は、指定非金融業者及び職業専門家（designated non-financial businesses and professions, DNFBPs）も対象としている。

[6] identify とは、顧客が誰であるかという情報を顧客から入手すること、例えば顧客から顧客本人を特定する身分証明情報の提示を受けることである。verify とはこの情報を、信頼できる、独立した原資料、データ、情報に基づき、確かにこの顧客が本人であることを示しているか否かを検証することである。例えば顧客の提示する身分証明情報が、情報を提示する顧客本人のものであることを、身分証明情報を発行した機関の元データと照合する、あるいは身分証明情報に格納された生体情報を、顧客の生体情報と照合するなどして、その一致を確認することである。identify は多くの人から一人を特定すること、verify はその一人が、登録されている本人であるかどうかを、データを照合することにより検証すること、という説明もされる。

[7] FATF Guidance, “Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion,” November 2017.

[8] 各国の金融機関側の対応については、各国の金融当局がガイダンス等を出している他、バーゼル委員会もガイダンスを取りまとめている。

び 2017 年の FATF によるガイダンスは、各国の事例を紹介しつつ、留意点をまとめたものであり、個々の手法にお墨付きを与えるものではない。

多くの国で、一定金額以下の預金口座、引出しや送金の頻度や金額に制限のある口座などに関し、簡易な CDD を可能としている例がある他、次に示すように新たなテクノロジーを活用することにより、AML/CFT の要請を満たしつつ、金融インクルージョンを推進する工夫も登場している。

３．テクノロジーの活用

特に重要なテクノロジーとなるのが、デジタル ID であり、モバイルや生体認証テクノロジーの活用もカギとなっている。

まずモバイルを活用し、銀行口座を持てない人々でも送金など一定の金融取引が可能となる仕組みが、急速に普及している。またモバイル・バンキングに限定した新たな制度を導入し、人々の銀行へのアクセスを促進する国も増えている。これらモバイル中心のサービスの場合でも、銀行店舗ではなくノンバンクがエージェントとなることで、現金の預け入れや引出しにも不便がないよう工夫がされている場合が多い。そして金額や取引頻度に制限を設けることにより、簡易な CDD が採用される。

こうしたモバイル金融取引の場合、ID 認証[9]、すなわち ID の提示やその確認も、紙などアナログの身分証明証を利用するのでは不便である。デジタル ID が導入され、ID そのものや ID 認証に必要な情報が電子的に管理され、電子的に本人認証ができれば、店舗を持たないモバイルバンクなどでも口座開設や取引時における CDD を円滑に行いうる（e-ID や e-KYC とも呼ばれる[10]）。

モバイルの普及は、デジタルな ID 認証にも重要な役割を果たしている。すなわち、インターネット取引におき、電話回線を通じて認証コードを送信し、サイト上でその入力を求める、あるいは SIM カードに国民 ID 情報等を格納し、デジタルな ID 認証に利用する事例がある[11]。

また生体情報が ID として利用される例が増えているが、生体認証データを電子的に管理することにより、デジタル ID 認証が金融取引にも活用されるようになっている。この

---

[9] 一般に、本人を identify し、その identity を verify するプロセス全体を「認証」、英語では authentication と呼ぶ。このうち、verify すること、すなわち verification については「検証」と訳されることもある。なお、身分証明書などが偽造や無効ではないことを確認すること（本人との一致の確認ではない）は、validation と呼ばれることが多い。

[10] なお KYC（Know-Your-Customer）という用語は、1990 年代頃より普及しているが、FATF 勧告では用いられておらず、その定義は統一されていない。

[11] 例えばスウェーデンの BankID は、2003 年に銀行界が導入したデジタル ID であり、国民の大半がモバイル上で認証や電子署名に利用している。通常のモバイル・バンキングやモバイル送金として有名な Swish など金融取引のみならず、政府機関など公的サービスの認証にも利用されている。BankID 自体は銀行界が運営しているが、BankID、銀行口座、モバイル契約は、同国の個人識別番号（personnummer）と紐づけられている。利用の際は、銀行口座開設時に登録した BankID のパスワードの入力やモバイルの生体認証により認証を行う。BankID による電子署名は、スウェーデン及び EU において法的効力が与えられている。ノルウェーも BankID を導入している。

点で、最も壮大な仕組みを実現させたのが、次章で示すインドの事例である。

金融インクルージョンにおいて、こうしたイノベーションが果たす役割は、G20 でも重視されており、規制上も留意すべきとされている[12]。FATF も、上述のガイダンスに加え、プリペイドカードやモバイルなどを活用した新たな決済サービスが、金融インクルージョンに重要な役割を果たすとして、ガイダンスを公表している[13]。同ガイダンスでは、AML/CFT の規制が、これらのサービス、及び今後の新たな商品の発展を制約すべきでないとも指摘している。

最近の動きとしては、世界銀行グループなどが G20 に向けた報告書におき、デジタル ID を通じて、金融インクルージョンと AML/CFT を実現していく方策について整理している[14]。例えば、各国におけるモバイルや生体認証の活用が紹介されている。

FATF も、近年、FinTech 及び RegTech（テクノロジーの規制分野への応用）に関するフォーラムを開催している他、デジタル ID と CDD に関する新たなガイダンスを準備している[15]。

Ⅳ 先進的 ID の事例

１．様々な ID へのアプローチ

今日、各国の公的 ID においても、デジタル ID への対応が進展しているが、そのアプローチは様々である。まず既存の ID 自体、その目的や登録、発行、管理のあり方において、様々な形態がある。公的な ID としては、多くの国において、出生登録や住民登録、婚姻届など、ライフイベントに応じた登録の仕組みや証明書の発行の仕組みがある。また運転免許や徴税、選挙など、特定の行政目的に応じた証明書発行・管理の仕組みもある。

ただし、これらの登録が、対象とすべき人々を十分カバーできていない国や、二重登録や記録の消失など管理が不十分な国もある、またこれら各種の ID データが異なる当局によって独立して管理され、相互の連携や統合的な管理が実現していない国もある。

また ID を用いて各種のサービスを利用する方法も、様々な形態がある。ユーザーがアナログな ID カードを提示し、サービス提供者がカードに掲載された写真と ID 保有者の容貌を目視で確認するという伝統的な方法から、ID カード保有者が入力するパスワードや生体情報を、中央データベースやカードの IC チップに格納された情報と照合して verify し、認証するという方法もある。後者が、デジタル ID としての活用例である。

本章では、先進的 ID 事例としてペルー、インド、エストニア、英国の事例を紹介する[16]。

[12] G20, “Principles for Innovative Financial Inclusion,” G20 Toronto Summit, June 27, 2010.

[13] FATF, “Guidance for a Risk-Based Approach: Prepaid Card, Mobile Payments and Internet-based Payment Services,” June 2013.

[14] World Bank Group, GPFI, “G20 Digital Identity Onboarding,” January 2018.

[15] FATF, “FATF Report to G20 Leaders’ Summit,” November 2018.

[16] 本章の記述は、主に Alan Gelb and Anna Diofasi Metz, *Identification Revolution: Can Digital ID be Harnessed for Development ?,* Center for Global Development, 2018 に依拠している。

図表 2　先進的 ID 事例

国名	背景	運営主体	公的IDの提供	生体認証による登録	生体情報による認証	認証の方法	e-ID（リモートアクセス）	カバレッジ
ペルー	国家再建、社会・開発プログラム	RENIEC（独立行政法人）	○	○	普及途上	IDカードの写真。e-IDカードではカード内の生体情報との照合による認証が可能	普及途上	3000万人（人口の99%）
エストニア	国家建設・行政管理、サービス提供の効率性	Information System Authority（警察及び国境警備組織との協調）	○	○	×	PINとIDカード内のデジタル証明書（あるいはモバイルのSIM情報）との照合による認証	○	120万人（15歳以上人口の94%）
インド	補助金改革、金融インクルージョン、経済のデジタル化	UIDAI（独立行政法人）	○	○	○	中央機関で管理された生体情報との照合による認証	○	11億人(成人人口の98%)
英国（GOV. UK Verify）	公共サービスへのオンライン・アクセスの利便性、効率性向上	GDS（政府機関）が公認民間ID提供者と協調	×	×	×	官民のレジストリーを用い、証明機関が認証情報を提供	○	95万人（成人人口の2%）

（出所）Alan Gelb and Anna Diofasi Metz, *Identification Revolution: Can Digital ID be Harnessed for Development?*, Center for Global Development, 2018.　より野村資本市場研究所作成

ID システムは、SDGs への問題意識が高い途上国の方が、プライバシーへの配慮から ID のあり方を巡る議論の多い先進国よりも発展しているケースが多い。ペルー、インドの事例は、その代表と言える。

エストニアは、先進国の範疇に入るが、国策としてデジタル化に注力しているユニークな国家であり、ID システムも、プライバシー保護に配慮しつつ、革新的な仕組みを導入している。

先進国のなかでも、英国、米国、オーストラリアなど、コモンロー諸国においては、国民 ID カードの導入も実現していないケースが見られる。これは、プライバシーの観点から国民の反発が強いことに加え、既に社会保障番号や運転免許証など、特定用途向けの公的 ID の仕組みが存在しているためである。これら functional ID により、相当程度のニーズは満たされており、さらなるコストをかけて新たな仕組みを作ろうという動きになりにくい。こうしたなかで英国は、複数の民間企業に本人確認作業を担わせるという新たなアプローチを採用した点で注目される。

図表 2 は、いくつかの観点からこれら 4 か国の仕組みを比較したものである。

２．ペルー

ペルーにおいては、内戦時に過去の公的記録の多くが失われたこともあり、国民の ID 登録は国家の優先課題として推進された。この任務は 1993 年に設立された RENIEC（Registro Nacional de Identificación y Estado Civil、英語では The National Registry of Identification and Civil Status）という、省庁や政治からの独立性が憲法で保障された機関が担っている。RENIEC は、教会以上に国民に信頼されている組織とされる。

ID カードには、写真、生年月日等が記載されている。通常、本人確認には ID カードの写真と本人との一致を確認するという、伝統的な方法が用いられている。ID カードが有効なものであるかは、中央データベースとの照合でチェックできる。

正式の ID カードは、18 歳で取得が義務付けられているが、産院で生まれた時点でほぼ自動的に、産院に付属する登録事務所で出生登録（住民登録）が行われ、子供用の国民 ID が付与される。写真と足型も記録される。

近年、e-ID カードも発行されるようになり、生体情報によるリアルタイム認証も可能となった。e-ID カードの IC チップには 10 本の指の指紋情報が格納されており、各種サービス利用時に、利用しようとする人の実際の指紋と、カードに格納された指紋情報との間での verification が行われる。電子署名の機能もある。

同国の ID サービスは、世界で最も統合された[17]ものの一つであり、ほぼ全ての政府サービスに利用され、また民間の商業サービスにおける本人確認にも広く利用されている。例えば不動産取引において、公証人は取引参加者全ての ID を、RENIEC のデータと照らして確認することが義務付けられている。

制度運営コストの 7 割は、ID 発行や認証サービス提供の手数料によって賄われている。貧困地区や僻地の住民の ID 登録などは、コストがかかるが、不足部分は政府が補助している。

３．インド

インドでは、出生登録や住民登録の仕組みが発展途上であり、ID が無いために政府の補助や教育を受けられず、また銀行口座の開設などが出来ない人が多かった。各種補助金の中間搾取も問題となっていた。そこで、2006 年 5 月に採択されたナショナル e ガバナンス・プランの下、中央データベースに、生体情報を用いた国民 ID を登録する、Aadhaar（アドハー）という仕組みを導入した。

この仕組みの導入・運営を担うのが 2009 年 1 月に設立された UIDAI（Unique Identification Authority of India）という組織である。閣僚委員会レベルの組織で、初代会長にはインフォシスの元 CEO が就任した。

10 本の手の指の指紋、虹彩、さらに顔のデジタル・スキャンデータが登録される。成人の登録率はほぼ 100%であり、最近は 5 歳の子供にまで登録対象が広がっている。顔写真と 12 桁の番号が付されたカードは存在するが、IC チップなどは搭載されておらず、厳格性を求められない非公式の本人確認に利用される程度である。正式の本人確認は、リーダーで生体情報を読取り、これを中央データベースと照合することによって行われる。

オンライン上での認証サービスも、様々な政府機関のサービス向けに提供されている他、銀行口座開設や銀行取引の際の本人確認などにも利用されている。指紋読取り機能のある micro-ATMs という小型の決済及び銀行取引用端末が、商店などに広く導入されており、現金引出しの際などは、このデバイスで指紋認証することで、店員より現金を受け取るこ

[17] まず出生登録や住民登録、死亡届などが、ほぼ確実に行われている。これらのデータは地方自治体によって管理されているが、RENIEC とのデータ連携が確立しており、国民 ID 登録が徹底されている。そして選挙権、教育、医療、公的給付などの資格管理は、国民 ID 番号とリンクする形で実現している。

とができる。プラスチック・カードやモバイルも使わず、生体認証のみで決済が可能な仕組み（Aadhaar Pay）も導入されている[18]。

この他、電子署名機能や、本人がある機関に保管された自分のデータを、セキュリティが厳格に管理された形で他の機関に提出できる DigiLocker という仕組みも導入されている。これは、大学における自分の学業成績を、就職希望先の企業に送付する場合などに利用される。

インドの ID の仕組みは、10 億人を超える国民を対象としており規模の経済が働くこと、コストのかかるスマートカード（IC チップ搭載カード）を採用していないこと、システムや機器に必要とされる要件を明確に示した上で、納入業者を競わせていることなどから、ID 一件の登録コストが 1.16 ドルと、諸外国に例を見ない低コストでの運営が実現しているという。

４．エストニア

エストニアは、e-ID のパイオニアと称されている。2002 年に物理的 ID カードを導入し、今日、2000 以上の官民のオンライン上のサービスへのアクセスが、デジタル ID を通じて可能となっている。

ID カード取得は強制であり、登録の際には名前、生年月日、性別、住所、国籍などの情報の他、顔と手の指全ての指紋のデータが登録される。ただし生体情報は、二重登録を避けるために用いられており、認証には使われない。

ID カードには、11 桁の番号が付されている他、本人確認用と電子署名用の二種類のデジタル証明書が格納されている。前者は、ID カードを保有している人が入力する最低 4 桁の PIN が、ID カード内の記録と一致した場合、保有者が本人であることを示すものであり、後者は、ID カード保有者が入力する最低 5 桁の PIN と、ID カード内の記録が一致した場合、本人として正式の署名をデジタルで行える仕組みである。このように、エストニアの仕組みは、中央データベースとの照合ではなく、カードの証明書と入力された PIN の照合によって、本人確認や電子署名を行う方式である。

エストニアの国民は、2007 年以降、この物理的 ID カードとスマートカード・リーダーを用い、自分のコンピュータを用い、様々なオンライン・サービス利用の際に、必要な本人確認を行い、また電子署名を行うことができる。近年は、物理的 ID カードではなく、デジタル ID にリンクした SIM カードや専用アプリの利用により、モバイルのみでサービスの享受が完結するようになっている。

カードは本人確認と電子署名のみに用いられ、それ以外の機能はない。サービス提供に必要なデータは、ほぼ分権的に管理されている。すなわち、政府機関や民間機関は、カードを通じた本人確認ができれば、11 桁の番号を用い、必要なデータを管理する機関のデータベースにアクセスし、サービスを提供する。

[18] 淵田康之『キャッシュフリー経済』2017 年、日本経済新聞出版社。

各機関のデータベース間のシェアリングを可能とするネットワークが、X-Road と呼ばれる堅固なセキュリティで守られた仕組みである。どの機関が、どの機関のデータをリクエストしたかは、タイムスタンプされ、またどこにどのデータがなぜ保管されているかを含め、国民は知ることができる。

エストニアでは、1990 年代半ば、官民の複数の機関の業務に従事していた一民間人が、各機関の大量の個人情報を統合した「スーパーデータベース」を作成し、外部に販売するという事件が発生した。この結果、個人データの集中的管理への懸念が強まり、データを分権的に管理し、X-Road を用いて必要に応じてシェアすることとした上で、全体の管理状況や利用状況を国民が随時確認できる仕組みとしたのである。

５．英国

英国には国民 ID カードのような、国が管理する統一的な個人 ID の仕組みは存在しない。2000 年代半ばに、生体認証を用いた ID カードを導入し、データを中央で集中的に管理することが構想されたが、国民の反発が強かったこともあり、2010 年に成立した保守党と自民党の連立政権が、同構想を撤回した経緯がある。

その後、2011 年 4 月に、政府のデジタルサービスの拠点として Government Digital Service（GDS）が内閣府に設置されたことを契機に、各種のオンライン・サービス利用時の本人確認を目的とした、新たな ID システム構築の検討がスタートした。

2 年間のベータ版の運営を経て、2016 年 5 月に正式稼働したオンライン・サービス向け新 ID システム、GOV.UK Verify は、国の機関が既に導入している出生証明書、運転免許証、パスポートなどの ID や証明書を基礎としつつ、それ以外の利用可能な各種データを活用して、本人確認の精度を高めるアプローチを採用している。この確認作業を特定の民間企業に担わせる点も、英国の仕組みのユニークな点である[19]。以下、具体例で示そう[20]。

まず政府の各種オンライン・サービス、例えば、「オンライン確定申告」のサイトにアクセスすると、サイン・インを求められる。従来利用されてきた Government Gateway という本人確認の仕組みを使ったサイン・インも選択できるが、この場合、ユーザーに郵送されるアクティベーション・コードを入力する必要があるため、利用開始までに一週間もかかる場合もある。これに対して、GOV.UK Verify の場合、初回に 10 分から 15 分程度かけて以下の手続を済ませれば、サービスの利用をスタートできる。

まず GOV.UK Verify の利用を選択し、「GOV.UK Verify の利用は初めて」を選択すると、認定 ID サービス・プロバイダー（identity providers や certified companies と呼ばれる）

[19] このように民間の ID 認証の仕組みを、公的にも利用する事例としては、注 11 で示したスウェーデンの BankID がある。ただしスウェーデンは税務当局が発行する個人識別番号が、税、社会保障、医療、その他あらゆる場面で幅広く利用されており、同番号に紐づける形で銀行口座の開設やモバイル契約が行われ、これらを前提に BankID によるデジタルな ID 認証が利用可能となっている。

[20] Gelb and Diofasi Metz（2018）及び Edgar A. Whitley, “Trusted Digital Identity Provision: GOV.UK Verify’s Federated Approach,” *CGD Policy Paper* 131, Center for Global Development, November 2018 参照。

の一覧が表示される。認定 ID サービス・プロバイダーは、2019 年 6 月末時点で、Barclays、Digidentity、Experian、Post Office、SecureIdentity の 5 社である。各社は、政府が設定したセキュリティ基準を満たす企業であり、利用は無料であること、これら企業の既存の顧客である必要はないことなどの点も示される。

次にユーザーは、現在、顔写真付きの運転免許証を所持しているか、英国のパスポートを所持しているか、他の国が発行した ID 書類（パスポート、ID カード、運転免許証）を所持しているか、という質問に答える。続いて、モバイルやタブレットを所持しているか、アプリをインストールできるか、という質問に答える。

このような質問に対するユーザーの回答内容に応じ、先述の 5 社の中から、当該ユーザーに対して本人確認サービスを提供可能な認定 ID サービス・プロバイダー名が表示される。複数の候補がある場合、ユーザーはそこから一社を選択する。メールアドレスやパスワードを登録し、生年月日やモバイル電話番号、住所などの情報を入力することで、同社に ID アカウントを開設できる。

この際、運転免許証やパスポートなど本人確認文書の情報も入力するが、認定 ID サービス・プロバイダーは、入力された情報について、それら文書を管理する当局（Driver and Vehicle Licencing Agency やパスポート・オフィス）に照会する。認定サービス・プロバイダーは、当局の文書に直接アクセスできないため、当局側からは、情報が当局の情報と一致するかどうかという、照会結果のみの連絡を受ける。

以上の基本的な ID 情報の一致が確認されると、さらに銀行口座やカード情報など追加的な情報や、直近の口座残高など本人しか知りえないような情報なども確認することで、本人確認の精度を高める。

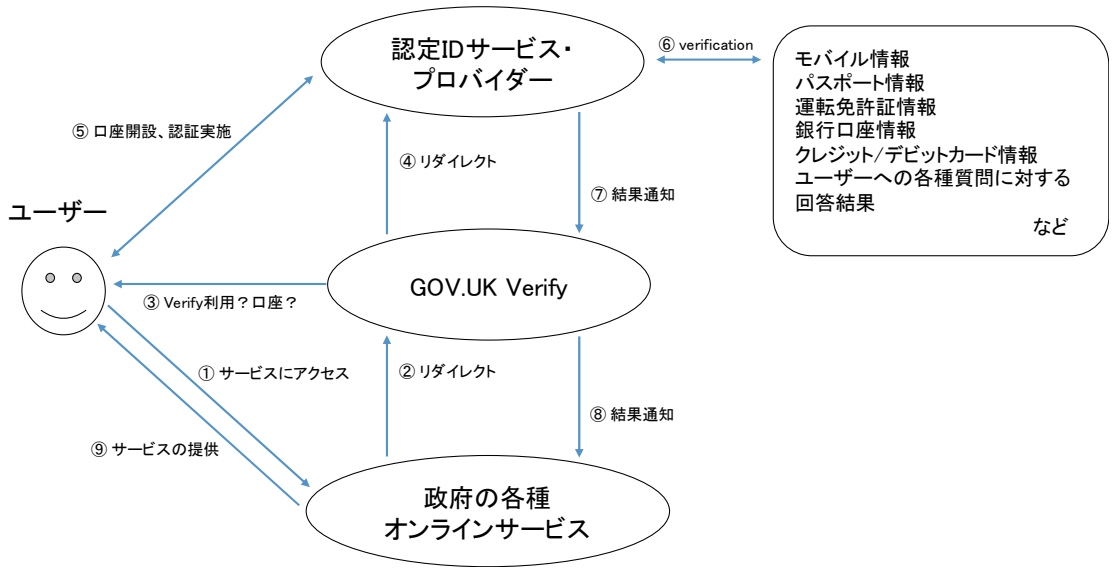
上記が初回の手続きであり、二回目以降は、GOV.UK Verify のロゴのあるオンライン・サービスにアクセスすると、認定 ID サービス・プロバイダーのリストが表示され、そこから自分がアカウントを開設しているプロバイダーを選択してログインすることにより、本人であることが確認され、ユーザーは当該サービスを利用できるのである（図表 3）[21]。

2019 年 6 月末時点で、自動車免許の申込、確定申告、年金の確認・受給申込など、16 のサービスにおいて GOV.UK Verify による認証が利用可能となっている。現状、GOV.UK Verify を採用しているのは公的サービスのみであるが、将来的には民間のネットサービスにも利用を開放することが展望されている。

以上に示したように、これらサービスの提供者は、自らの仕組みで本人確認するのではなく、本人が上記の初回登録時に選択した認定 ID サービス・プロバイダーが行う本人確認の結果に依拠するのである。サービス提供者には、サービスにアクセスしようとしているユーザーが本人であるかどうかを検証した結果だけが、認定 ID サービス・プロバイダーから通知される。運転免許証やパスポートに記載された情報、その他、認定 ID サー

[21] 認定 ID サービス・プロバイダーは、初回登録時の verification だけではなく、ユーザーがサイン・インするごと、及び定期的に、一定の確認作業を行う。認定 ID サービス・プロバイダーに対しては、ID 認証が成功した件数に応じて報酬が支払われる。

図表 3　GOV.UK Verify におけるデータ・フロー



（出所）Whitley（2018）を参考に野村資本市場研究所作成

ビス・プロバイダーが本人確認作業に利用した情報は、サービス提供者には一切伝わらない。どのような情報を利用したかも、通知されないのである[22]。

GOV.UK Verify は、最高レベルの正確性を常に追求しなくても良いという発想で運営されている。すなわち、ユーザーがアクセスしようとしているサービスによって、要求される正確性のレベル（アシュアランスのレベル）は異なって良いという立場である。具体的には、4 段階のレベルを設定し、レベルに応じて、認定 ID サービス・プロバイダーが実施する検証作業の厳格さが変化する。

制度の運営にあたっては、インドのアドハー同様、認定 ID サービス・プロバイダーなど、制度に関与する者に要求される技術的要件（パラメーター）を注意深く定義し、またパフォーマンス・データを公開している。さらに民間のボランティア団体である、Privacy and Consumer Advisory Group が定めた Identity Assurance Principles を遵守した運営がなされている。

６．ID のプリンシプル

以上の事例からもわかるように、各国において ID に対するアプローチは様々であり、あるべき ID 制度とはどのようなものであるか、確立した答があるわけではない。

[22] 現在、オーストラリアも Gov.UK Verify と似たデジタル ID の仕組みを導入しつつある。ただし ID プロバイダーは、現状、民間企業ではなく、Australian Taxation Office が運営する myGovID という仕組みのみである。自分の顔の自撮り画像を、政府が管理する本人のパスポート写真のデータと即座に照合する Face Verification Service を活用する点も注目される。なお同国では既に、Australia Post が運営する Digital ID という仕組みもあり、大手信用金庫や Travelex など民間サービスにも利用されている。同国も過去（1985 年及び 2006 年）、国民 ID カード導入が構想されたものの、批判が強く実現しなかった経緯がある。

ID 整備の重要性は、途上国支援に関わる世界の様々な開発援助機関においても認識され、多くのプロジェクトに資金が投じられ、様々な ID の仕組みが試されてきた経緯がある。しかし国によっては ID が差別に使われる事態が生じたり、限定的な用途の ID 制度がいくつも導入された上、十分普及しなかったり、独自の認証テクノロジーを持つ特定の IT ベンダーが業務を独占し続ける事例も生じるなど、様々な教訓が蓄積されてきた。

そこで、あるべき ID 制度として一つの確立したモデルは無いとしても、過去の様々な教訓を踏まえると、ID 制度が共通に満たすべき要素があると考えられるようになった。これをまとめたのが、2017 年に世界銀行グループ等が発表した「持続的な成長のための ID に関するプリンシプル：デジタル時代に向けて」である（図表 4）[23]。同プリンシプルは、世界の主要な開発援助機関によって支持されている。

こうした個々の国々の ID 制度のあり方だけではなく、デジタル取引の時代に通用するグローバルな ID のあり方を巡る議論もある。人々が国境を超えて、様々なネットサービスにアクセスし、取引や決済を行う時代となっているが、国の違い、サービスの違い、さらにはデバイスの違いなどに応じ、その都度、様々な ID 認証を求められる。ID 認証を経なければ、誰とコミュニケーションしているのかわからないから、これはやむを得ない。

しかしこの煩雑なプロセスは、顧客体験（デジタル・エクスペリアンスとも表現される）の質を低下させ、また随所で求められるままに入力した各種の個人情報が、どこでどのように管理されているのか、という懸念も生じさせている。

そこで、デジタル ID に焦点を当てたプリンシプルも提案されている。図表 5 は、2019 年 3 月にマスターカードが発表したプリンシプルである[24]。大手カードブランドは、国境を超えた決済認証ネットワークを運営しており、今後、こうした強みがデジタル ID サービス全般に活かされていくことも展望されよう。

図表 4　持続的な成長のための ID に関するプリンシプル：デジタル時代に向けて

インクルージョン：ユニバーサルカバレッジとアクセシビリティ	
	1. 出生から死亡まで、個人をユニバーサルにカバー。差別のない仕組み
	2. アクセスや利用の障害をなくす、情報やテクノロジーの利用可能性についても不公平をなくす
デザイン：ロバスト、セキュア、レスポンシブで、サステイナブルであること	
	3. ロバスト（ユニークでセキュア、そして正確）なIDを確立
	4. インターオペラブルで様々なユーザーのニーズに即応するプラットフォームを構築
	5. オープン・スタンダードの導入。ベンダーとテクノロジーに関する中立性を確保
	6. ユーザーのプライバシーとコントロールを、システムデザインによって保護
	7. 財政的、また運営的なサステイナビリティをアクセシビリティに妥協せず計画
ガバナンス：プライバシー保護、利用者の権利の保護を通じて信頼を構築	
	8. データプライバシー、セキュリティ及びユーザーの権利を、包括的な法規制フレームワークを通じて安全に守る
	9. 明確な制度的権限とアカウンタビリティを確立
	10. 独立した監視及び苦情対応の仕組みを通じ、法的および信頼のフレームワークを実現

（出所）世界銀行、Center for Global Development（2017）より野村資本市場研究所作成

[23] World Bank Group and Center for Global Development, “Principles on Identification for Sustainable Development: Toward the Digital Age,” 2017.

[24] Mastercard, *Restoring Trust in a Digital World*, March 2019.

図表 5　デジタル ID のプリンシプル

Inclusion	全ての人がデジタルIDの権利を持つ
Ownership	IDと個人データを所有するのは本人である
Simplicity	個人にとって自分のデジタルIDの利用は簡潔で直感的であるべき
Confidentiality	個人は自分のデジタルID情報をプライベートなものとする権利を持つ
Consent	デジタルIDは、本人の明確な同意、あるいは法による許可がなければ、利用されたりシェアされることはない
Transparancy	個人は自分のデジタルIDデータが、どのように利用されシェアされたかを理解する権利を持つ
Security & Integrity	個人のデジタルIDとデジタルIDを伴う取引は、最高基準のセキュリティとインテグリティの下で管理されなければならない
Data Rights	個人は自分のIDデータにアクセスし、これを修正し、削除する権利を持つ。またそれらの権利が侵害された場合、不服申立の権利を持つ
Fair Use	個人のIDデータは、正当かつ公正、そして非差別的な目的にのみ利用される
Choice	個人はデジタルIDプロバイダーを選択できるべきである。またオプトアウトする権利を持つべきである

（出所）Mastercard, *Restoring Trust in a Digital World*, March 2019. より野村資本市場研究所作成

V 欧州の SCA

1．SCA とは

ID とその認証が最も重要となる局面の一つとして、決済がある。個人がオンライン上で電子決済を行う機会も急増しているが、それとともに決済に係るトラブルも増大している。

そこで近年、中国、EU、マレーシア、メキシコなどでは[25]、取引の実行や、センシティブな支払いデータへのアクセスなどにおいて、SCA（Strong Customer Authentication、厳密な本人認証）を法的に義務付ける動きがある。以下では、2019 年 9 月 14 日に施行が予定されている、EU の SCA について紹介する。

EU における SCA の導入は、2015 年に制定された改正決済サービス指令（Payment Services Directive 2、PSD2）において要請されたものである。決済サービス指令は、銀行や電子マネー会社、その他決済関連業者を決済サービス・プロバイダーとして横断的に位置づけ、共通の利用者保護の枠組みなどを規定すると同時に、個々の業者のリスク等に応じた財務基準などを設定したものである。PSD2 は 2007 年に制定された最初の指令を改訂したもので、新たなタイプの FinTech の決済関連業者の規定や、電子マネー会社に対する

[25] World Bank Group, GPFI, “G20 Digital Identity Onboarding,” January 2018.

規制緩和を盛り込んだことで知られるが、同時に SCA のような利用者保護の充実も図られている。

SCA の規定は、PSD2 の 97 条に定められ、(a)ユーザーがオンラインで決済口座にアクセスする際、(b)電子決済を行う場合、(c)決済関連の不正が生じうるリモート環境チャネルを通じて何らかのアクションを行う場合に、加盟国の決済サービス・プロバイダーは SCA を適用しなければならないとしている。

さらにユーザーが電子決済を行う場合、ユーザーの認証の際に、取引金額と支払先に関連付けた固有の要素を用いなければならない、としている。これは後述するダイナミック・リンキング（dynamic linking）の要請である。

また 98 条におき、EBA が ECB との協力の下、全てのステークホルダーと協議して、SCA の要件や適用除外の規定などを定める Regulatory Technical Standards（RTS）の案を、2017 年 1 月までに策定し欧州委員会に提出することが求められた。その後、RTS は 2017 年 11 月に制定されている。

２．多要素認証の要請

RTS において、決済サービス・プロバイダーには、2 つ以上の要素を用いた認証が求められることとなった。認証に用いられる要素は、Knowledge、すなわちユーザーしか知らないもの（ユーザーのみが知りうるパスワードや暗証番号、秘密の質問への回答など）、Possession、すなわちユーザーが保有するもの（ユーザーのみが利用している携帯電話に送付したコード、あるいは本人に配布したトークンに表示されたワンタイムパスワードなどを決済サイトに入力してもらうことで、携帯電話やトークンの持ち主であるユーザーによる取引であることを確認するなど）、Inherence、すなわちユーザーにもともと備わっているもの（指紋や顔など、生体情報）、という 3 種類に分類することができるが、SCA はこのうち 2 つ以上を用いるべきとしたのである。

例えばこのうちの一つが他人に不正に入手されることによって、他の要素も他人が提供できる情報となるようでは、いくら複数の要素が用いられても意味がない。それぞれの要素が独立していることも求められる[26]。

[26] 従来、オンラインなどリモート環境における取引では、カード番号や有効期限、セキュリティ・コード、氏名などの情報でカード決済を可能となる場合が多かった。しかしこれらの情報では、カードの有効性は識別できても、その決済をしようとしている者がカード会員本人かの識別はできない。そこで、カード業界では、決済時にカード会社のサイトが表示され、そこにあらかじめカード会員が設定した（あるいはカード会社が送信した）パスワード入力を要求することで本人認証をする仕組み、「3D セキュア」が考案され、利用されつつある。しかし追加的に手間がかかるため取引を中止するユーザーが少なくない（いわゆる「かご落ち率」が高い）こと、別画面が立ち上がるためフィッシングサイトへの誘導と誤解される場合があること、パソコンでの取引を前提にデザインされていることなどが、普及の障害となっていた。そこで 2016 年に、「3D セキュア 2.0」という新たなバージョンが発表されている。同バージョンは、生体認証にも対応し、また別画面が立ち上がる仕組みではなくなり、モバイルでの利用にも適応している。なお 3D セキュアのバージョン 1.0.2 の段階で、既に SCA の要件は満たされている。

３．ダイナミック・リンキング

こうした 2 要素認証、あるいは多要素認証は、今日、既に普及しつつあるが、欧州の SCA においては、同時にダイナミック・リンキングと呼ばれる仕組みの採用が要請されている。これは、支払者が支払う金額と支払相手を確認し特定すると、この情報を固有のコード（authentication code）で管理することにより、支払者が、意図しない金額や意図しない相手への支払いを行う事態を避けるためのものである。

具体的には、RTS におき、支払者に対して支払う金額と支払相手が通知されていること、そして支払者が支払いを実行するに当たり、支払う金額と支払先に固有の認証コードを生成し、この同一のコードによる注文のみ受け入れることが求められている。金額や支払先が変更されると、当該認証コードは無効となる。

４．施行延期を求める動き

RTS において SCA の施行期限は、2019 年 9 月 14 日と規定されている。しかし施行期限が迫るにつれ、期限までにこの規定をクリアできる認証の仕組みを導入できない電子商取引サイトが少なくないとの指摘がされ、懸念が広がっている。

欧州の銀行界は、25～30%の電子商取引サイトでは対応が間に合わず、オンライン決済が出来なくなり、大きな混乱が生じるとして、欧州委員会や European Banking Authority に施行延期を求めた[27]。同様の指摘は、電子商取引業界や決済サービス業界からも生じた。

2019 年 6 月 21 日、このような動きに対して EBA は、例外的に各国の監督当局が、関係者と調整を続けることを認めた。この例外措置の適用を受けるためには、決済サービス・プロバイダーは、規制遵守への移行プランを策定し、当局の承認を得た上で、迅速に実行する必要がある。これら業者に対する最終期限は、2019 年後半に発表するとしている[28]。

Ⅵ わが国への示唆

１．様々な課題

１）SDGs

SDGs は途上国のみを対象としたものではなく、先進国においても達成に向けて努力すべき部分は少なくない。ID についても、多くの先進国において、ターゲット 16.9 に掲げられた法的な ID は存在しても、第Ⅲ章で紹介した先進的な途上国の事例

[27] Nicholas Megaw, “Banks warn EU rules will scupper a quarter of online payment,” *Financial Times*, June 12, 2019.
[28] EBA のプレスリリース、”EBA publishes an Opinion on the elements of strong customer authentication under PSD2,” June 21, 2019 参照。

と比べて、有効に機能していない場合も多い。このことは、図表 1 で示されるように、SDGs の他のゴールやターゲットの実現にも支障をきたすことを意味する。

この点は、わが国も無縁ではない。マイナンバーカードが導入されたが、まだ普及途上であり、身分証明は、相当程度、運転免許証、健康保険証、パスポートなどの functional ID に依存している。また生体認証の利用は限定的であり、運転免許証を本人確認に使う場合など、顔写真と本人の顔の目視による一致に頼る場合も多い。健康保険証など、顔写真を伴わない ID も多い。

このため例えば、クレジットカードなどを送付した簡易書留郵便の不在票を郵便受けから盗み、郵便局で偽の運転免許証や健康保険証を用いて郵便物を受領し、他人名義のカードを不正利用する組織的犯罪も増加しているという[29]。

また、やはり証明書を偽造するなどして、他人の土地を売却する契約を結び、多額の資金を詐取する事件が後を絶たない。このような事態は、わが国において所有権の証明という、SDGs の Goal 1、Target 1.4 に関わる問題が生じていることを意味する。

一方、本人が死去しているにも関わらず、年金が払われ続け、遺族などの生活費となるという年金不正受給問題のような、社会保障のターゲティング（SDGs の Target 1.3）に関わる問題も生じている。

この他、災害時など、各種の身分証明書を保持しない者が多数発生する一方、本人を特定した上で、その個別のニーズに対応することが急務となる局面も発生しうる。また高齢化が進むなか、従来の方法では本人確認が困難な人々が増えていくことも考えられる。

２）AML/CFT

一方、AML/CFT については、わが国は 2008 年の第 3 次相互審査において厳しい評価を受け、2014 年 6 月には、その後の改善も十分ではないとの警告を受けた経緯がある。勧告の「不履行（Non Compliant）」とされた分野の一つが CDD であり、個人 ID に関しては、金融機関が依拠することのできる本人確認書類の質が不明確であり、写真やユニークな ID 番号が付与されていない ID 文書でも口座開設が可能となっている点が問題視された。

その後、犯罪収益移転防止法（犯収法）が二度にわたり改正され、取引時確認の厳格化が図られてきた。本人確認書類については、2016 年 10 月 1 日より、顔写真のない本人確認書類（健康保険証、国民年金手帳、児童扶養手当証書、母子健康手帳など）を使用する場合は、提示に加えて、その他の書類の提示や転送不要郵便等の送付等の二次的確認が必要とされることとなった。

非対面取引の場合は、本人確認書類またはその写しを顧客が送付し、金融機関は本人確認書類に記載の住所に取引関係文書を転送不要郵便等で送付することされていた。しかしこの点は、FinTech の金融サービスが台頭し、デジタル ID の活用により、モ

[29] 日本経済新聞、2019 年 7 月 2 日掲載記事参照。

バイル等で口座開設を迅速に完了可能となっている世界の潮流に反する規定として批判されてきた[30]。

そこで、2018 年 11 月 30 日の犯収法の施行規則改正で、①身分証明証撮影と容貌撮影、②身分証明証の IC チップ読取りと容貌撮影、③身分証明証の IC チップ読取りと銀行・クレジットカード口座照合や銀行振込確認という、3 つの手法の採用も認められ、ネット上で本人確認手続きを完結させることが可能となった[31]。

2019 年は、FATF の第 4 次対日相互審査が実施される年でもあり、以上のような取組みを含め、わが国の AML/CFT 対応のあり方が再検証されることとなる。

3）SCA

SCA については、わが国の場合、カード業界や個々の決済サービス・プロバイダーにおける自主的な取組みはみられるが、欧州などにおけるような法律レベルでの義務付けの動きは本格化していない。昨今、新たなキャッシュレス決済サービスも登場しているが、これらのサービスも含め、わが国の多くの決済サービスは、クレジットカードの番号、有効期限、セキュリティなどの入力のみで支払い可能なものが多い。

2．展望

わが国において ID を巡る問題が生じてきた一つの背景は、国民に幅広く利用される ID カードや ID 番号が長年存在しなかった点にあろう。マイナンバーの利用やマイナンバーカードの交付は、2016 年 1 月に始まったばかりであり、マイナンバーカードの普及率も、2019 年 4 月 1 日時点で 13%程度に留まる。カードを保有していても、身分証明書として利用できない、利用しないケースも多い[32]。

マイナンバーカードは、利用者証明用と電子署名用の二つの電子証明書が格納されており、デジタル ID としても利用可能であるが[33]、マイナンバーカード自体が普及していないことに加え、デジタル ID としての利用にあたっては、カードリーダーの入手やパソコンのセットアップなどが必要なこともあり、利用は進んでいない。

現在、わが国では、マイナンバーカードの普及拡大に向けた対応が、各種進展しつつあ

[30] 増島雅和「FinTech 時代の本人確認はどうあるべきか（前編）、（後編）」https://startupinnovators.jp/blog/、2017 年 4 月 23 日及び 5 月 19 日掲載記事参照。

[31] 従来の本人確認書類 1 点の送付と転送不要郵便の利用は、2020 年 4 月より認められなくなる。転送不要郵便を用いたい場合は、①身分証の撮影と転送不要郵便、②IC チップ読取りと転送不要郵便、③本人確認書類の原本の送付と転送不要郵便、④本人確認書類 2 点の送付と転送不要郵便のいずれかが必要となる。

[32] 運転免許証や健康保険証と異なり、「番号」（識別子）を記録できない点が一つのネックとなっているという。保有者も、マイナンバーに紐づけられた様々な情報が漏洩する事態を懸念し、カードの携行を避ける場合が多い。

[33] 公的個人認証サービス。

るが[34]、本稿で見てきたように、国民 ID カードなどに頼らないデジタル ID 認証の仕組みを国が推進している英国のような例もある。一方、途上国も含め、モバイルや生体認証の活用の動きも活発となるなど、世界の ID を巡る状況は、日進月歩と言える。

わが国もこのような変化に柔軟に対応していくとともに、ID のプリンシプルに示されるようなグローバルな基本原則にも留意しつつ、ID 制度やデジタル ID を進化させていくことが望まれる。

[34] 2019 年 6 月 4 日に開催されたデジタル・ガバメント閣僚会議において、「マイナンバーカードの普及とマイナンバーの利活用の促進に関する方針」が策定された。2020 年には、消費税増税対策として、マイナンバーカードに自治体ポイントを付与する制度が実施される予定である。また 2019 年 6 月に成立した改正健康保険法を受け、2021 年 3 月より、マイナンバーカードを健康保険証として利用する仕組みの本格運用が始まる。なお 2017 年 11 月より、マイナポータルがスタートし、マイナンバーカードを使ってログインすることで、一部の行政サービスの利用手続きや個人情報の利用履歴の確認などが可能となっている。