2024/10/17 発行

CNN ニューズ No.119

プライバシー
インターナショナル
ジャパン（PIJ）
国民背番号問題検討
市民ネットワーク
Citizens Network Against
National ID Numbers（CNN）

Privacy International Japan
PIJ
Privacy NGO™

季刊発行
年４回刊

巻頭言 どう克服する多言語での税務支援問題

先進各国は、移民の積極的な受入れに必死である。資質の高い移民は奪い合いになっている。人口減対策、国内の労働力や消費力拡大が、国の将来を左右するからである。わが国の人口は、全都道府県で減少、外国人 299 万人が下支えし、人口減を食い止めている。税金をジャブジャブ注ぎ込んでの〝産めよ増やせよ〟の政策は限界にきている。

アメリカ、カナダ、オーストラリアなどでは、移民の自発的納税協力を多言語で支援する仕組みが整っている。ドイツでは、税理士会が、移民の増加に伴い、国内での自発的納税協力促進に積極的だ。移民の出身国の税理士会と相互協定を結び「外国人税務専門職の認証」をし、移民に対する母国語での税務支援サービス態勢を整えている。会費バク食い親善大好きの日税連幹部にも学びになる視点だ。

アメリカの連邦課税庁（IRS ／内国歳入庁）は、納税者権利憲章を出し、「納税者が主役」の税務行政を進める旨アナウンスしている。納税者権利憲章に沿い、納税者からの苦情に積極的に対応している。IRS 内に、納税者からの苦情に対応する独立した「納税者権利擁護官」という組織を設け、納税者権利擁護官サービス（TAS）を展開している。TAS は、全米に支部を置き、2,200 ～ 300 人のスタッフがいる。また、おおよそ 170 の言語で税務支援する態勢を整えている。

さらに、TAS は、全米の法科大学院やボランティアの協力を得て開設する低所得納税者相談所（LITC）で多言語での訟務支援をしている。加えて、ボランティア所得税援助（VITA) プログラム、高齢者向け税務相談（TCE) プログラムなど、民間ボランティアの参加を得たさまざまな税務支援サービスを提供している。

ところが、わが国の税界では、外国出身の納税者への多言語税務相談、申告支援の必要性に対する意識は希薄である。島国根性丸出しで、「外来者は、日本語を学べ！　日本文化を学べ！」の大合唱。国粋主義に近い発想から解脱（げだつ）できていない。

国税庁も、税務支援の多言語サービスには沈黙している。だが、多言語での税務支援の整備は待ったなしである。税理士会をはじめとした税務専門職団体も真摯な対応を考えないといけない。自分らで対応できないなら、税理士法を改正し、税務相談と税務書類の作成業務を有償独占化すべきだ。そして、外国語で支援できる個人や市民団体、さらには AI などによる無償の税務支援に扉を大きく開かないといけない。ところが「税理士業務は無償独占で、俺たち以外は他人の税務にタッチするのは違法だ。やるならお縄頂戴でやれ！」のスタンスである。この４月から非税理士等による税務相談停止命令制度が動き出した。税理士以外の税務支援を認める「臨税」も萎む傾向にある。まさに時代を逆走する動きが続く。

税務の無償独占、政府規制にあぐらをかき、排外主義に徹していると、この国の申告納税制度は確実に危なくなる。この国の多言語での税務支援強化にむけた新たな政策が求められている。

２０２４年　１０月１７日
PIJ 代表　石 村 耕 治

時代遅れのマイナカードとマイナ保険証の一体化策

― スマイナカード、マイナ保険証を持つ持たないは自由！！ ―

石 村 耕 治 （PIJ代表・白鷗大学名誉教授）

政府はマイナカードと保険証の一体化を強引に進める。今年の12月2日には，従来の健康保険証は廃止される。代わって、新たな資格証明書を発行・送付することが決まっている。政府のマイナカードと保険証の一体化策は問題だらけで、各界から不安の声はあがっている。現行の健康保険証の存続を求める声は大きくなる一方である。デジタル弱者保護の観点から、各地の弁護士会や市民団体は、「現行の健康保険証を廃止してマイナンバーカードの取得を義務化することに反対する」集会を開き、反対声明が相次ぐ。スマホなどモバイル端末が主流で、時代遅れになってしまったマイナカードとマイナ保険証の一体化策の問題点を検証する。

（CNNニューズ編集局）

≪紙の健康保険証はいつまで使えるのか？各自治体のアナウンスメント≫

紙の健康保険証はいつか廃止されるが、廃止後は医療機関での診察をどのように受ければよいのか？保険者により、その取扱いは異なる。国民健康保険証（市区町村が加入する後期高齢者医療広域連合が交付する後期高齢者医療被保険者証を含む。以下同じ。）については、一般に、マイナ保険証を持つ被保険者を含め、プッシュ型（個別申請なし）で交付することになっている。

≪紙の保険証はいつ廃止されるのか？≫

紙の保険証は、12月2日に廃止される。 とはいっても、廃止とは「新たな保険証の発行を廃止する」だけなので、紙の保険証も有効期限まで継続して利用できる。2024年8月1日に交付される国民健康保険証は、2025年7月31日までが有効期限になる（取扱いは自治体により異なる）。

≪紙の保険証が廃止された後はどうなるのか？≫

紙の保険証が廃止された後は、マイナ保険証を持っているかどうかで受診方法が異なる。 保険証とマイナンバーカードが一体化されている人は、マイナ保険証を活用して診察を受けることができる。マイナ保険証を持っている人には、「資格情報のお知らせ」が届く。一方、マイナ保険証を持っていない人は、医療機関で受診ができなくなる。こうした不便を避けるため、各保険者は、被保険者に「資格確認書」を送付する。被保険者は、資格確認書を提示すれば、これまでどおり医療機関で診察できる。資格確認書の有効期間は、5年以内で保険者が設定する。

≪各自治体のアナウンスメント≫

- **神奈川県横浜市**

  横浜市は、2024年12月2日に紙の国民健康保険証の新規発行を廃止するとホームページ上でアナウンス済み。 マイナ保険証がない人には、個別に資格確認書を発送する予定。2025年7月中に、すべての被保険者に「資格確認書」または「資格情報のお知らせ」を発送する。

- **埼玉県さいたま市**

  さいたま市は、2024年12月2日に紙の国民健康保険証の新規発行を廃止するとホームページ上でアナウンス済み。廃止日より前に交付された紙の国民健康保険証は、2025年7月31日まで有効。2024年12月2日以降、マイナ保険証を保有していない人には、本人の申請がなくとも「資格確認書」が交付され、引き続き、医療を受けることができる。

- **東京都足立区**

  東京都足立区では、2024年12月2日に紙の国民健康保険証の新規発行を廃止するとホームページ上でアナウンス済み。 廃止日より前に交付された紙の保険証は、2025年9

月 30 日まで有効。 廃止日以降にマイナ保険証が利用できない人には「資格確認書」を交付。 資格確認書の発送は、2024 年 12 月と 2025 年 10 月に予定。

- **愛知県名古屋市**

  名古屋市でも、2024 年 12 月 2 日に紙の国民健康保険証の新規発行を廃止するとホームページ上でアナウンス済み。 廃止後、マイナ保険証を持っていない人は、資格確認書を提示して診療を受ける。資格確認書の発送は紙の国民健康保険証の有効期限である 2025 年 7 月 31 日までに発送。資格確認書を発行の申請手続きは不要。

- **大阪府大阪市**

  大阪市は、2024 年 12 月 2 日に紙の保険証の新規発行を廃止するとホームページ上でアナウンス済み。マイナ保険証がない人には、個別に資格確認書を発送する。資格確認書の発送は、2024 年 12 月を予定。

≪私学共済／日本私立学校振興・共済事業団のアナウンスメント≫

加入者証・加入者被扶養者証（任意継続を含む）は、2024 年 12 月 1 日に廃止される。加入者証等廃止に伴い、原則的にはマイナンバーカードにより医療機関等にかかることになる。マイナンバーカードを持っていない、持っていても保険証利用登録をしていない人には、申請により「資格確認書」を交付する。

◆問われるマイナカードとマイナ保険証の一体化政策

国家が国民全員に唯一無二の国民背番号であるマイナンバーを振り、官製の IC カード（マイナカード）を持たせるのは、国民を国家がデータ監視することが狙いである。マイナンバーやマイナカードで税や社会保障などを含め国民をトータルにデータ監視するのは、権威主義国家につながるという見方がある。昨今の DX 化（データ＋デジタル技術ファースト）は、悪用すれば、自由と人権を大事にする民主国家も、いともたやすく権威主義国家に改造できる。仮に効率性追求のためにマイナンバーやマイナカードの利用が避けられないとしても、民主主義国家であるためには、国民のデータ監視の法的限界が明らかにされないといけない。わが国では、政府も国民も、あえていえば医療界も、法的限界を厳しく問うことを躊躇し、人権を後回しにしてきたのではないか。このことが、現在のデータ収容所列島化にストップをかけられない状況を生んでいるのではないか。

◆国民皆保険制度を餌食にした政策

政府は、「マイナカードパンデミック」の拡散に、誰も逃げられない国民皆保険制度を餌食にした。政府は紙の保険証の「廃止」に先立って、まず保険医療機関と保険薬局をターゲットにした。2023（令和 5）年 4 月から保険医療機関・薬局におけるシステム導入を義務化した。このために、保険医療機関及び保険医療養担当規則を「改正」し、これに違反した保険医療機関を保険指定の取り消しにできるようにした。このシステム導入を拒んだ医療機関は、最悪の場合、保険指定取消しもあり得る。

ただ当初は、仮にすべての保険医療機関にシステムが導入されたとしても、国民は、現行の健康保険証が使えなくなるわけではなかった。この段階では、あくまでも医療機関側に「マイナ保険証」に対応するよう求めるものであった。

ところが、政府は、マイナカードを実質国民全員に持たせる政策に方向転換した。2023 年の通常国会で、健康保険法などを改正し、現行の保険証廃止を 2024 年秋に期限を定めた。その結果、国民はこれまでの健康保険証でも問題なく使い続けることができなくなった。これが昨今のマイナ保険証トラブル発生の原因である。

◆プッシュ型「資格確認証」発行は血税の無駄遣い

医療サービスの現場にも、DX 化の大波が押し寄せている。DX 化にはさまざまなメリットがある。だが、大波を乗り切るのは至難である。人口の高齢化もあり、医療サービスの利用者のみならず提供する側にも「デジタルデバイド（情報技術格差）」、デジタル弱者が多いからである。加えて、デジタル投資が至難な医療サービス提供者もいる。こうした医療現場の実情に背を向けて、いきなり紙の健康保険証を廃止し、IC 仕様のマイナ保険証カードに一体化する政策の強行は乱暴すぎる。国民の異論・反論が想定以上に強くなったのは当り前だ。

その後、政府は、マイナ保険証トラブルへの対

応策をアナウンスした。その内容は、マイナカードと健康保険証との一体化計画は改めない。現行の健康保険証を計画どおり 2024 年秋までに廃止しマイナ保険証にする基本は堅持する。その一方で、資格確認証を最長 5 年間、交付するというもの。国民健康保険などの場合は、一般に、プッシュ型（個別申請なし）で交付。一方、私学共済や協会けんぽなど保険者によっては、被保険者による申請が必要。いずれにしろ、マイナ保険証を持っていても、資格確認証も交付してもらえる。

政府は、言い訳しないで、紙またはプラスチックカードの現行健康保険証を存続させることで一件落着にすれば、マイナ保険証トラブルに対する国民の抵抗も少なかったはずだ。にもかかわらず、政府は、その道を歩もうとしなかった。資格確認証の発行という新たな血税の浪費につながる政策を選択した。資格確認証の発行という懐柔策で、国民の納得が得られたかどうかは疑問である。

マイナカードとマイナ保険証の一体化策は、災害時、停電時、サイバー攻撃時にその弱点を露呈する。一歩誤れば、安心・安全に医療サービスを受ける態勢を崩壊に導く。憲法 25 条の生存権保障の観点から、高齢者などを含むデジタル弱者が、紙媒体で行政や医療機関の窓口にアクセスするのは当然の権利である。いずれにしろ、マイナカードを持つか持たないかは任意である。

◆マイナカードには 2 種類のマイナンバーが入っている

マイナカードには、実は 2 種類のマイナンバーが入っている。1 つは、①対面／オフライン／目視で本人確認に使う 12 桁の個人番号である。もう 1 つは、②ネット／オンライン／デジタル空間で本人確認に使う「デジタルマイナンバー」である。

ひとくちに、目に見えないデジタル ID といっても、官製のもの［公開鍵／ JPKI 方式］と民間のもの［ID ＋パスワード方式］がある。

●マイナ IC カードは「官製の対面用リアル ID ＋官製のデジタル ID」兼用

対面で使うリアル ID	デジタル ID
目に見える空間の本人確認で使う ID	目に見えないネット空間の本人確認に使う ID

【官製のリアル＆デジタル兼用 ID ／マイナ IC カード】

★実は「官製のデジタル ID」と「民間のデジタル ID」の 2 つがある

①官製のデジタル ID
わが国の場合は、「公開鍵式 [JPKI ／電子証明書] の暗号」を IC カードのチップに格納した官製の共通デジタル ID、いわゆる「デジタルマイナンバー」
②民間のデジタル ID
民間のデジタル ID プロバイダーが開発した「ID ＋パスワード方式」、「ID ＋パスワード＋ワンタイムパスワード方式」仕様のデジタル ID

政府の方針では、できるだけ民間のオンライン取引の本人確認にも、民間のデジタル ID に代えて官製のデジタルマイナンバー／ JPKI を使わせさせようとしている。民間の取引データも国家が管理できる権威主義国家の仕組みを拡張しようと画策しているからだ。今の政府の方針だと、医療機関の診療予約、アマゾンからのネット購入やホテル予約の際の本人確認にもマイナカードを使わないといけなくなるかも知れない。誤解を恐れずにいえば、政府は、デジタル ID 政策で「NHK だけで、民放は認めない」方向を目指しているようにも見える。行き過ぎると、市場主義国家のデジタル ID 政策ではなくなる。民間活力を削ぐ。

◆官製の IC カード不要は世界の流れ

世界の流れは、行政へのアクセスは、対面／リアルではなく、「オンライン／デジタルが原則」になりつつある。だが、他の G7 諸国では、オンラインアクセスに、もはやマイナカードのような官製の IC カードを使っておらず、発行もしていない。モバイル端末（スマホやタブレット）全盛の時代だからである。官製の IC カード発行自体が時代遅れでガラパゴス化してしまったのだ。

わが国でも、政府はあわててマイナカード機能のスマホ搭載に舵を切り出した。ただ、他の諸国では、IC カード機能は、ネット上の公式アプリストア（Apple Store、Google Play）にアクセスし、アプリをダウンロードし、それを開いて、画面を見

ながら、自分の基本情報その他必要情報を入力する。自分用のデジタルIDを生成し、認証されれば、それをスマホに直接搭載する仕組みだ。ところが、わが国では、それができない。マイナカードを取得し、スマホで読み取る時代遅れのやり方だ。マイナカードの発行を止め、公式アプリストアからマイナアプリを搭載するやり方に変えないといけない。

今日、災害時にはスマホ持参で避難するのが常識だ。マイナカード持参の避難者は少ない。じきにマイナ保険証はスマホ搭載が標準になるはずだ。こうした流れに抗し、政府は、血税を使って官製のマイナカードを発行し続けている。新型のマイナカードを発行するとまで言っている。これは、明らかにモバイル端末ファーストの時代に逆行する。そのうち、政府は、医療機関や薬局に、持ち出し費用はガマンしろの姿勢で、新型のマイナカードやスマホ掲載のマイナ保険証に対応できる新たなマイナ機能読取機の設置を押し付けてくるはずだ。

政府は、「医療機関などに関所を設けて官が発行したリアルの通行手形（マイナカード）で監視する仕組み」は「日本モデル」だ。「国民に、対面／リアルでも、オンラインでも、官が、すべての国民のIDを支配・管理するのが正義だ」と言うのかも知れない。だが、こんな理の通らない呪術で国民をマインドコントロールしようとするのは不健全そのものだ。権威主義国家の発想である。

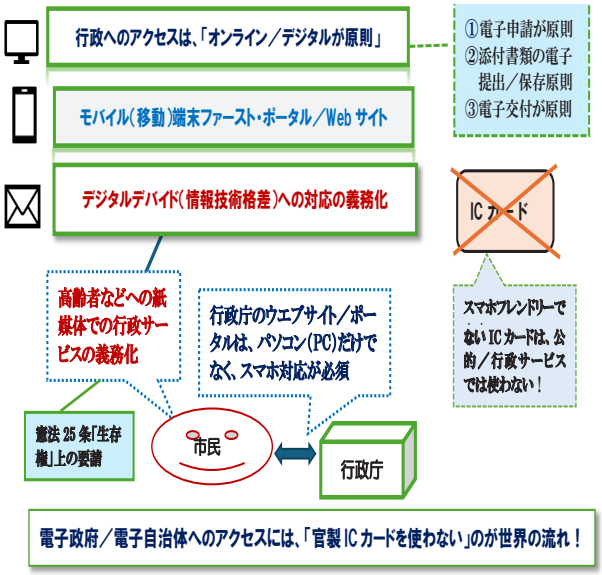
◆国民を常時監視する「Mシステム」の国民監視が要る

マイナ保険証と顔認証（顔パス）データとを使って保険証資格確認をするネットワークの仕組みは、国家による国民の顔認証データの集中監視につながる。データ監視国家の構想である。国中の路上に張り巡らされたNシステム（自動車ナンバー自動読取システム）の医療分野版、いわば新たな「Mシステム（medical surveillance system）」の創設と見てよい。Mシステムが一人歩きしないように、逆に、国民がMシステムを監視できる仕組みつくりが急がれる。

◆本人同意のない顔パス利用は人権侵害

国民が、医療機関や薬局などを訪れマイナ保険証と顔パスシステムを使うとする。これにより、本人のはっきりした同意なしに生涯不変の生体データ（顔面データ）の提供を半ば強要されることになる。このやり方は、個人情報保護の基本原則とぶつかる。EU（欧州連合）をはじめとした民主主義国家では、センシティブ（機微）な生涯不変の生体データの利用を、人権保護の観点から厳しく制限する。ユーザーから明確な同意を得ない限り顔認証データを入手してはならないとする「オプトイン方式」を採用する。また、アメリカでは、人種差別その他の人権侵害につながるとして、顔パスの自由な利用を禁止する方向にある。

●世界の流れ～モバイル端末で行政などにアクセスする国民の権利保障



マイナカードとマイナ保険証の一体化に賛成しない団体は多い。しかし、あらたなMシステム、顔認証ネットワークシステムによる位置確認が危険なデータ収容所列島化構想につながり人権侵害である、との認識がいまだ薄い。

医療機関や薬局で収集・管理される顔認証データがどのように扱われるのか、透明性、公開性が問われる。国中の医療機関や薬局に生体認証式監視カメラを設置しても、悪いことをしていなければ怖がることはないでは済まされない。

やましいことをした人は安心して医療機関で治療を受ける権利はない、といった流儀は危険だ。医療機関を治安機関に変身させるのは、権威主義国家の発想で、民主主義国家の発想ではない。

◆マイナ保険証の危険な使われ方への対応が要る

国家によるマイナ保険証の危険な使われ方にもっと警戒しないといけない。逃げられない国民皆保険制度、マイナ保険証と顔パスを核としたMシステムで収集・管理した国民の健医療データ・

健康データを、国家が自動徴兵、国民総動員などに利用することが危惧されるからだ。この国では、行政追従大好きの政治が主流で、国民は、政府のマイナ保険証の危険な使われ方からプライバシーや人権を護る政治や政党活動を期待するのが難しい。政権が交代しても、行政追従大好きの政治の流れを変えるのは至難だ。

マイナ保険証を使った国民の医療データ・健康データを、国家から独立した管理に移す仕組みの確立を急がないといけない。外国からの大規模なサイバー攻撃に備え、国民の医療データ・健康データの信頼できる他国へのバックアップも急がないといけない。医療界には、自由と人権を基軸とする憲法をベースに、マイナ保険証の危険な使われ方に法的セーフガードを構築し、DX 化・IT を利活用した効率的な医療サービスの実現と、国民の医療・健康プライバシーと民主主義の価値を大事にする責任ある行動が期待される。

最新のプライバシーニューズ

各地であぶり出される恐ろしき公権力濫用県政

CNNニューズ編集局

●兵庫県の公益通報制度は〝盗聴器〟？

ドイツのナチス政権下、その後の東ドイツでは、市民が赦しを乞うに訪れた教会懺悔室は盗聴器だらけだった。こんなこと、独裁国家、権威主義国家では常識としても、民主主義国家では赦されない。

公益通報者保護法は、報道機関なども通報窓口として定め、一定の要件のもとで通報者への不利益な取り扱いを禁じている。斎藤元彦・兵庫県前知事は、自身のパワハラ行為などの告発者捜しに公益通報制度を悪用していたことがわかった。

兵庫県のように公益通報制度を〝盗聴器〟のように扱う実務は、民主主義国家にはなじまない。県の百条委員会で参考人として意見を述べた山口利昭弁護士は批判した。「文書の存在を知った直後に、誰がどんな目的で書いたのか探索するというのはありえない。法令違反だ」と。斎藤氏のような資質の人物は、やはり民主主義を大事にしないといけない組織のトップにはふさわしくない。権力を持つとおごり高ぶり、市民や弱者をいたぶるような感覚の人物は、政策を練る仕事をする前に、自らの再教育が必要だ。任意取得のはずのマイナ保険証を強いる御仁や、介護施設や保育園などで弱い入所者や入園者をいたぶる人物も同様である。

●岐阜県警の市民情報の違法収集・横流しは違憲・違法

岐阜県警大垣署が、岐阜県大垣市での風力発電施設建設に反対する地元の寺の住職ら市民の学齢や病歴、過去の市民運動暦などの個人情報を中部電力子会社「シーテック」に垂れ流ししていた。

この事実をオープンにしたのは、朝日新聞名古屋本社版 2014 年 7 月 24 日のスクープ記事である。この記事では、県警大垣署警備課とシーテックが、複数回にわたり協議した内容の議事録が詳報された。

2016 年 12 月、名指しされた市民 4 人が原告となり、岐阜地裁に提訴した。警察が目を付けた特定個人の情報を集め、第三者に提供するのはプライバシーや思想・信条の自由、表現の自由を侵害するというのが提訴の理由だ。

岐阜地裁は、2022 年 2 月に、判決をくだした。警察の行為は、プライバシー情報を積極的かつ意図的に提供したのは悪質であるとした。220 万円の賠償を命じた。一方、情報収集の違法性は認めなかった。理由は、警察は、万一に備えて情報収集の必要性があったからだという。原告市民は、名古屋高裁に控訴した。

名古屋高裁は、2024 年 9 月 13 日に判決をくだした。情報収集の違憲性、違法性を指摘して一審岐阜地裁判決を変更し、一部の抹消を命じた。賠償額についても情報収集が警察官の裁量権を逸脱しており、プライバシー侵害は明らかだとして原告請求を認容した。賠償額も、一審から倍増の計 440 万円とした。

今年 8 月、名古屋高裁は、無罪判決が確定した男性が捜査時に採取された指紋や DNA 型を警察庁のデータベースから抹消するよう求めた訴訟で、データの抹消を命じた 1 審判決を支持する判決を言い渡した。この判決も今回の判決を書いたのも、名古屋高裁の長谷川恭弘裁判長である。今回の判決を下した 9 月 13 日が同裁判長の退職日。警察当局による行き過ぎた情報収集活動を立て続けにとがめた形で裁判官の仕事を終えることになった。

公安警察の行き過ぎた情報収集・配付を厳しく批判した名古屋高裁判決を、原告の市民側は「望みうる中で最高の判決」と高く評価した。

岐阜県警を実質的にマネージしている警察庁（国）は、名古屋高裁の判決には納得しまい。今後、最高裁で争われるのではないか。

鹿児島県警の事例もいまだ記憶に新しい。各地であぶり出される恐ろしき公権力濫用県政をとがめるには、やはり市民のパワーが要る。

≪ 2024 年 9 月 13 日 名古屋高裁判決の要旨は 33 頁≫

石村 PIJ 代表に CNN ニューズ編集局が聞く！！

オーストラリアの 2024 年デジタル ID 法を読む(下)

Q&A：オーストラリアのスマホ直接搭載デジタル ID

― デジタル ID はスマホ直接搭載が世界の流れ ―

石 村 耕 治 （PIJ代表・白鷗大学名誉教授）

≪コンテンツ≫

■ PLS ／税務専門職電子申告サービスとは何か

（Q）わが国では日税連が独自の電子申告フラットフォームを構築し、認証制度、税理士用電子証明書を格納した IC カードを発行している。この日税連の電子申告フラットフォームを使って税理士はクライアントの電子申告ができる。オーストラリアの税務専門職の場合はどうなのか？

（A）オーストラリアにも、ATO（国税庁）と各税務専門職をリンクする「Practitioner Lodgment Service（PLS）／税務専門職電子申告サービス)」という名のプラットフォーム（ポータル）がある。以前から税務専門職と課税庁（ATO）とをリンクする「Electronic Lodgment Service（ELS）／電子申告サービス」という名のプラットフォーム（ポータル）があった。ELSは、原則として、2017年4月1日からPLSに取って代わられた。

企業や個人が、税理士（RTA=Registered Tax Agent）登録した公会計士（CA・CPAなど)、BASエージェント（記帳・法定資料作成士 ／ Business Activity Statement（BAS）Agent）のような税務専門職に、所得税や消費税（GST=Goods and Services Tax）の申告書や源泉所得税（PAYG withholding）関係の法定資料（証票や支払調書）などの作成を依頼したとする。この場合、税務専門職は、PLSプラットフォームを介して、標準事業報告(SBR=Standard Business Reporting）仕様のソフトウエアを使い、リアルタイムで、課税庁（ATO）に電子申告やデータの提出、電子申請ができる。

ちなみに、SBRソフトウエア［商品名：Software Assistant, Tax Assistantなど］は、民間のソフトウエア開発事業者が税務専門職界やATOとタイアップして開発したもので、有償である。各専門職は、ソフトウエアIT企業にSBR仕様のソフトウエアを注文し、購入する必要がある。

■豪州では本人申告ではスマホ申告が主流

（Q）オーストラリアでは、正規の給与所得者を含め、免税点を超える納税者は、原則として全員確定申告する仕組みで個人はスマホによる電子申告が主流ということだが？

（A）法人事業者など複雑な確定申告をしないといけない納税者もいる。一方で、オーストラリアには、わが国にあるような年末調整（ the-end-of-adjustment procedure）の仕組みはない。このため、給与所得者／サラリードワーカーも確定申告しないといけない。年金受給者などの場合も、一般に申告内容はそれほど複雑ではない。このため、通常、サラリードワーカーや年金受給者、ギグワーカーなどは電子納税申告（myTax）をする。今日、個人所得税では90％を超えている。しかも、その多くはスマホ申告である。

すでにふれたように、2020年3月に、オーストラリアの電子政府ポータル【マイガブ／myGov】やデジタルID【マイガブID／myGovID】は、スマホフレンドリー方式（スマートデバイス・ファースト）に全面移行した。マイガブID／myGovIDは二段階認証／二要素認証を基本とするツールである。納税者が、電子納税申告（e-file）をするとする。この場合、スマホを使い、連邦・州・準州の多くのオンライン行政サービスを束ねハブとなっている電子政府ポータルマイガブ／myGovにログインする。そして、次に、国税庁（ATO）のWebサイトをログインして手続を進めることになる。

■「デジタルID問題」の日豪比較

（Q）日本から見ると、オーストラリアはいまだ第一次産業や第二次産業中心の国のようなイメージが強い。ところが、デジタル化、電子政府デザイン、デジタルIDなどの面では、日本と比べものにならないくらい先を行っているようにも感じるが？

（A）率直にいえば、デジタル化で、日本は世界の流れから遅れ過ぎた。オーストラリアのデジタル化が特に進んでいるわけではない。オーストラリアは広大な国土を持つ。かつては、広大な国土を持つことの長短があった。近年は、短所の多くをデジタル化でカバーする政策をとっているように見える。言い方を変えると、天然資源のない日本は、このままデジタル化に遅れをとって行くと、国力が落ち、円安なども手伝って、転落して行くのではないかと思う。

わが国でとりわけデジタル化が遅れているのは「官」、「行政」、「政治」の分野である。加えて、文系の高等教育分野でのデジタル対応もいまだ明るさが見えない。

今回は、「デジタルID」とは何かについて議論している。この点について、基礎的な話をしたい。アマゾン（Amazon）は多国籍のデジタルプラットフォーム企業である。アマゾンのWebサイトを閲覧して欲しい本を見つけ、プラットフォームに出店している販売業者からその本を買う契約をするとする。その場合、購入者の本人確認／身元確認をしないといけない。自治体のWebサイト／ホームページ（HP）を閲覧し、オンラインで子供の保育園の入園申込をするとする。この場合も、申込者の本人確認をしないといけない。

このように、官民を問わず、オンライン取引、オンライン申請・申請をする際に本人確認に使うツール（道具）を「デジタル ID」という。Web サイトにログインしてオンライン取引やオンライン申請をする際には、何らかのデジタル ID が必要なわけである。

現実には、多くの人たちが「デジタル ID」とかの意味をよく知らないまま、民間の取引に頻繁に使っているのではないか。一方、行政事務でのオンライン申請・申告はかなり遅れて始まった。このため、オンライン申請でデジタル ID を使うといわれてもピンとこない人が多いのではないか。役所の窓口に出向いて、健康保険証や運転免許証など本人確認できるカードを持参して申請・申告をする、あるいはそれらのコピーを同封して郵送で申請・申告をするのが常識であった。

しかし、インターネット（ネット）という便利なツール（道具）ができた。で、ネットでオンライン申請・申告をするときには、デジタル ID が必要になる。目に見える現実空間では、運転免許証や旅券のような対面（face-to-face）用の物理的 ID（physical ID）、リアル ID（real ID）を使えるが、ネット空間では使えないからである。つまり、ネット空間で使う身分証明書／本人確認証がデジタル ID といえる。民におけるネット取引に加え、官におけるネット申請・申告の急激な拡大とともに、デジタル ID の重要性が増している。

デジタル ID には、民間のものと官製のものがある。わが国やオーストラリアでは、法定の行政事務についてオンライン申請・申告する場合には、官製のデジタル ID を使うことになっている。一方、アメリカでは、それぞれの行政機関が公開入札で民間のデジタルプロバイダー（デジタル ID を開発・販売する IT 企業）のデジタル ID を採用し、オンライン申請・申告でそれぞれの Web サイトにログインする際に、ユーザーにそのデジタル ID を利用するように求めている。アメリカは市場主義ファーストの国である。官製の共通デジタル ID をあらゆる行政機関、さらには民間機関利用にエスカレートさせる政策で、国民を納得させるのは難しい。官製の共通デジタル ID の採用や拡大利用など、権威主義国家がすることだと考える国民性からくるのかも知れない。

わが国の場合は、マイナ IC カードに格納された公開鍵（JPKI ／電子証明書）式の官製の共通デジタル ID を使わないといけない。パソコン（PC）が全盛の時代には、IC カードリーダーを PC に接続し、マイナ IC カードに装備された官製のデジタル ID［公開鍵（JPKI ／電子証明書)］を読み取るのでも、あまり問題にならなかった。

しかし、世の中は、いつの間にかスマホ全盛の時代になってしまった。わが国でも人口の 90％近くがスマホを持っている。法定の行政事務のオンライン申請・申告は、着実にスマホでする時代に入ってきているわけである。行政サービスにおけるオンライン申請・申告の際にはデジタル ID が必須である。ところが、わが国では、ユーザーに対して、〝民間のデジタル ID を使うのはご法度。官製の共通デジタル ID を使え！〟と強要しているわけである。つまり、スマホで行政の申請・申告をする場合にも、マイナ IC カードに入っている官製のデジタル ID［公開鍵（JPKI ／電子証明書)］を使えというわけである。〝マイナ IC カードを持たない人は、行政事務のオンライン申請・申告する資格はない！〟の姿勢なわけである。

一方、オーストラリアの電子政府（myGov）ポータルは、スマホフレンドリーなモデルである。IC カードは使わない。連邦政府は、日本とは違って、スマホ全盛時代に合わなくなってしまった共通番号 IC カードのような官製の IC カードを発行していない。

オーストラリアで、市民がオンライン申請・申告のために連邦や州の電子政府（myGov）ポータルに束ねられた各種行政機関の Web サイトにログインしてオンライン申請・申告をするとする。その際には、ネット上のアプリストアから官製のデジタル ID であるマイガブ ID ／ myGovID をスマホやタブレットのようなモバイル（移動）端末にダウンロードし、自分のデジタル ID を生成・インストールして使う仕組みになっている。

■ネットから官製デジタル ID を入手直接スマホに装備

（Q）ということは、オーストラリアでは、日本のようなマイナ IC カードに入っている官製のデジタル ID［公開鍵（JPKI ／電子証明書)］を読み取る面倒な作業は要らないわけだ。オーストラリアは、官製のデジタルアプリ（App）を、ネット上の公式アプリストアからインストールできるのに、なぜ、日本は、IC カードからスマホへデジタル ID を読み取るような時代遅れのことをやっているのたろうか？

（A）このことについては、総務省やデジタル庁に聞いて欲しい。ともかく、スマホファーストの時代だ。幼児などを除くわが国人口の 9 割近くがスマホを持つ時代である。今や IC カード機能はスマホに格納・装備するのが世界の常識になりつつある。ポイントを撒き餌にスマホに不具合なマイナカードを持てと急かすやり方は、どうかしている。解せない。スマホに IC カード機能を読み取る作業は至難である。ネット上のアプリストアからダウンロードしてスマホにマイナ機能を直接装備すれば簡単である。マイナカードはその役割を終えつつあるといえる。

この国の役人が主導する一連の「マイナカードインパール作戦」には大きな疑問符が付く。しかし、彼らも、モバイルファースト／スマホファースト時代の激流に逆らった「マイナカードパンデミック」、「マイナカード継続はヤバイ！」と悟ったのではないか？

最近になって、彼らは、この愚策を覆い隠そうと必死になってきた。「今が潮時だ！」ということで、この 3 月、政府は、「マイナカードの全機能をスマホに搭載できるようにする」マイナンバー法などの改正案を国会に提出した（デジタル社会形成基本法等の一部改正法案（digital.go.jp）。国会での政治とカネも問題への至近の対応を見てもわかるように、国会は〝現金、アナログ記録が大好きな議員〟だらけだ。こんな国会では、まともな議論しないままこの法案は通るのではないか。

マイナンバーカードの全機能のスマホ搭載といっても、大きく 3 つのモデルがある。

【表 21】マイナンバーカードの全機能のスマホ搭載モデル

★マイナンバーカードの全機能のスマホ搭載には 3 つのモデルがある。

① IC カードを取得させたうえでスマホに読み取らせるモデル

② IC カードの取得なしにすべてアプリストアから入手しスマホに直接装備するモデル

③ IC カードを取得させ、アプリストアからスマホ用デジタル ID を入手すると同時に、他の IC カード券面事項を読み取らせるモデル

わが国は、最も複雑な③の方式の採用を模索している。しかし、③の方式は、操作が複雑、ユーザーフレンドリーではなく、一般の市民・納税者がデジタル ID（JPKI　App）などをインストールするのが至難である。

① IC カードを取得させたうえでスマホに読み取らせるモデルは、読み取り作業の面でも極めて面倒である。② IC カードの取得を要らなくしてアプリストアからスマホに直接装備できるモデルにしないといけない。つまり、電子政府・電子自治体は、スマホファーストの時代にマッチしたデザインでないといけない。マイナ IC カードの発行は、思い切ってもうやめる時期に来ている。

マイナカードの IC チップに備わっている機能として、①カードの画像データ、②カード面の記載事項の文字データ、③カード保有者用の官製共通デジタル ID ／公開鍵式［JPKI ／電子証明書］の暗号の 3 つがある。現在、グーグル社のアンドロイドスマホのような一部機種では、③公開鍵式［JPKI ／電子証明書］の機能だけは使える。この法改正で、残りの①②の機能もスマホで使えるようになるのかは定かではない。

もし、①・②・③すべての機能をスマホに格納できることになれば、実質的にマイナカードがスマホのなかに入っているのと同じになる。EU 諸国のように、マイナ IC カードの携行は要らなくなる。もちろん、越えないといけないハードルは高いように見える。

わが国のスマホは、アップル社の iPhone の市場占有率が 7 割強だ。iPhone では、マイナ IC カードに装備されている公開鍵（JPKI ／電子証明書）式の官製の共通デジタル ID 読み取りできない機種が多い。

問題は、政官産がスクラムを組み莫大な血税を垂れ流しても、「マイナカードは時代遅れ、マイナ機能はスマホ装備に変えて 1 件落着、誰も責任をとらない！」のでいいのか？が問われている。マイナカードパンデミックで浪費された巨額の血税は国民・納税者の汗の結晶である。

■スマホ全盛時代のデジタル ID 入手方法

（Q）まず、更新の必要なマイナ IC カードは廃止にして、官製の共通デジタル ID をネット上のアプリストアから直接ダウンロードできるようにして、血税の無駄使いを止めないといけないのではないか？

（A）民間企業の Web サイトでは、ログインの際に、通例、「ID ＋パスワード」式のデジタル ID が使われる。アプリストアから民間企業の Web サイトを選び出して閲覧し、取引する際には、「ID

コラム 6　わが国での官製デジタル ID などのスマホ搭載の操作方法

わが国では、デジタル社会形成基本法などを改正し、官製のデジタル ID（JPKI）などを格納したマイナ IC カードの内容をスマホにインストール（搭載）する方向である。行政手続等にかかるユーザーなどの利便性の向上、行政運営の簡素化・効率化が狙いだという。

そこで、政府が構想するわが国での官製デジタル ID などのスマホ搭載の操作方法を点検して見る。

◆マイナ IC カードアプリ（App）の概要

アプリ（App）	用途・機能	アクセスコントロール
①JPKI-App（公的個人認証 App）	・署名用電子証明書の電子申請に利用	暗唱番号（6～16 桁の英数字）
	・利用者証明用電子証明書は、マイナポータル等へのログインなどに利用	暗唱番号（4 桁の数字）
②券面 App	・対面での券面記載情報の改ざん検知 ・対面での本人確認の証跡として画像情報の利用 ＊記録する情報：表面情報：4 基本情報＋顔写真画像 裏面情報：個人番号の画像	○個人番号を利用できる者：個人番号 12 桁により表と裏の券面情報を確認 ○個人番号を利用できない者：生年月日 6 桁＋有効期限西暦部分 4 桁＋セキュリティコード 4 桁により表の券面情報のみ確認
③券面事項入力補助 App	・個人番号や 4 基本情報を確認（対面・非対面）し、テキストデータをして利用することも可能 ＊記録・利用する情報：❶個人番号や 4 基本情報、それらの電子署名データ、❷個人番号およびそれらの電子署名データ、❸4 情報とそれらの電子署名データ 個人番号については、法認された事務でのみ利用可能	❶については、暗唱番号（4 桁の数字） ❷については、個人番号 12 桁 ＊これにより、券面目視により個人番号のマニュアル入力のケースで正誤チェックが可能 ❸については、生年月日 6 桁＋有効期限西暦部分 4 桁＋セキュリティコード 4 桁 ＊個人番号を読みだせない仕方とすることで、暗唱番号（4 桁の数字）を使うことも可能
④住基 App	・住民票コードを記録 ・住基ネット事務のために住民票コードをテキストデータとして利用可能	暗唱番号（4 桁の数字）

＊暗証番号（4 桁の数字）については統一設定も可能。ただし、生年月日やセキュリティコードなどと同一は不適切

◆煩雑過ぎるマイナンバーカード機能のスマホ搭載の操作

現時点では、Android 端末スマホだけが NFC 機能を使いマイナンバーカードの読取り可能である。iOS 端末スマホ（iPhone）は読取りができず、いつ可能になるかも未定である。

マイナンバーカード機能のスマホ搭載は、フェーズ 1 から 4 までの操作が必要ある。つまり、フェーズ 1［アプリ準備］、フェーズ 2［アプレット準備］、フェーズ 3［初期設定］、フェーズ 4［サービス利用・証明書管理］までの操作が必要である。

公式アプリストアの利用はフェーズ 1 の段階のみ。アプリストア（Google Play）からスマホ用アプリ、スマホにインストールする。次いで、自己のマイナカードから、NFC（or Felica）機能を使い、JPKI デジタル ID を読み取るなどの操作をする【詳しくは、［資料］ 総務省／マイナンバーカードの機能のスマートフォン搭載等に関する検討会「第 1 次とりまとめ（案）～電子証明書のスマートフォン搭載の実現に向けて（2020（令和 2）年 12 月 25 日）」（https://www.soumu.go.jp/main_content/000725415.pdf）19 頁～20 頁参照】

すでにふれたように、世界の流れは、官製の IC カードにデジタル ID を格納する方式はやめている。官製のデジタル ID を格納した IC カードは発行せずに、直接公式アプリストア（Google Play、Apple Store）から、デジタル ID を、スマホにインストールする方式を採用。例えば、オーストラリア。マイナ IC カードを廃止し、スマホのみで、JPKI-App（官製デジタル ID／官製デジタルマイナンバー）、券面 App、券面事項入力補助 App、住基 App をインストールするには、大胆な簡素化が必要だ。いまのままでは、手続が煩雑すぎる。本当に行政手続等にかかるユーザーなどの利便性の向上、行政運営の簡素化・効率化が狙いなのかどうか大きな疑問符がつく。

＋パスワード」＋TMS（テキストメッセージシステム）を通じて送られてくるlinking Code／security code（ワンタイムパスワード）を、スクリーン画面の「Linked Service」欄に貼り付けるなどの手続で完了する。

ところが、わが国の電子政府・電子自治体（マイナポータル）を介した税の電子申告や社会保障サービスのオンライン申請では、ログインの際に、官製のデジタルIDである〝電子証明書／PKI／公開鍵〟（以下「PKI（公開鍵）」、「JPKI」ともいう。）が必須だ。［唯一個人所得税の電子申告にだけ、例外的に「ID＋パスワード」式のデジタルIDの利用が許されている。しかし、この場合も、公式アプリストアから電子申告アプリを入手することはできず、最寄の税務署へ届け出て「ログインID＋パスワード」の配付を受けないといけない。］

官製のデジタルID（JPKI）は、個人向けにはマイナンバーICカードに格納されて配付される。このことから、マイナICカードを取得しないと、官製のデジタルID（JPKI）は入手できない。玉突きで、マイナICカード取得に「ノー」の市民は、電子政府（e-Gov）ポータルを通じたネット申請・申告もできない。

わが国では、政府が、住民全員にマイナICカードを持つようにさせて、通行手形のように、国民監視ツールとして使おうとしている。マイナICカードを持ち歩かない人は「非国民」か「外国代理人（スパイ）」と敵視する国つくりをめざしてきたわけである。マイナンバー制度をデザインしている役人は、こうした「警察国家」の呪縛から脱却できていないのではないか。

しかし、多くの諸国では、対面用の身分証明書（ID）も、デジタルIDもすべてスマホに装備させる政策に舵を切ってきている。もう、政府が官製のICカードを発行する時代にはなくなってきている。日本政府の人権意識が問われている。

すでにふれたように、わが国の場合、オーストラリアなどとは異なり、ネット上のアプリストアから官製の共通デジタルIDアプリをスマホにインストールするのはできない。

マイナICカードには、対面用のIDに加え、公開鍵（JPKI／電子証明書）式の官製の共通デジタルIDが装備されている。このことから、官製のICカードから官製の共通デジタルIDをスマホやパソコン（PC）などに読み取る作業をしないといけない。

一方、オーストラリアは、官製の共通ICカードは発行していない。その代わり、行政上のオンライン申請・申告の必須の官製のデジタルIDはネット上のアプリストアから自分のスマホにインストールするモデルを採用している。

スマホのような移動／モバイル端末全盛の時代である。ところが、わが国の各種電子政府・電子自治体ポータル「マイナポータル」は、パソコン（PC）＋マイナICカード＋ICカードリーダーの3点セットの旧式モデルなわけだ。スマホフレンドリーな電子政府・電子自治体モデルに刷新しないといけないのである。でないと、利便性が悪すぎて、行政のオンラインサービス利用は遅々として進まないのははっきりしている。

■民間のデジタルIDの相互利用

（Q）わが国でも、行政サービスのオンライン申請・申告に、官製のデジタルID（JPKI）だけでなく、民間活力をいかし、信頼できる水準のものであれば民間のデジタルIDも並行して使えるようにすべきではないか？

（A）その辺も早急に検討しないといけない課題である。仮にマイナICカードを取得していたとしても、スマホで電子政府・電子自治体（e-Gov.）／マイナポータルにログインしてオンライン申請・申告をするのは容易ではない。わが国のマイナポータルサイトは、「簡素」、「利便性」などはほぼ皆無に近いデザインである。原因は、マイナICカードの格納された官製のデジタルID（JPKI）をスマホに読み取らないといけないことにある。しかも、アンドロイド系スマホでは読み取りできるが、アップル系スマホではほとんど読み取りができない。

わが国では、この問題を解消し、電子政府・電子自治体（e-Gov）をもっと市民に身近な存在にしないといけない。そのためには、まず、電子政府・電子自治体（e-Gov）ポータル（マイナポータル）を、スマホフレンドリーにする必要がある。つまり、マイナICカードがなくとも、電子政府・電子自治体の申請・申告ポータルにログインできるようにしないといけない。そのためには、官製のデジタルID（JPKI）を止め、「ログインID＋パスワード」式のデジタルIDを採用するのも一案である。これには異論もあり得る。「ログインID＋パスワード」式（2段階式）のデジタルIDでは安全性の不安が残る、官大好派で、官製のデ

ジタル ID（JPKI ／公開鍵）を引き続き利用したい、というファンもいると思う。そういう声に応えるには、すでにふれたように、官製のデジタル ID（JPKI）を、ネット上のアプリストアから直接スマホに格納できるようにすべきでないか。

いずれにしろ、諸外国では、PKI（公開鍵）の技術仕様のデジタル ID を採用していても、物理的な IC カードに格納するやり方を止めてきている。とくに新たにデジタル ID を導入する国では、デジタル ID を物理的 IC カードに格納する方式の採用には消極的だ。スマホ全盛時代逆行するからである。それに、IC カード紛失に伴うプライバシー漏洩などの危険を避けないといけないからだ。

オーストラリアでは、2020 年に新たなデジタル ID【マイガブ ID ／ myGovID】を採用しました。しかし、わが国のマイナンバー IC カードのような時代遅れの「ハコモノ」は使っていない。これはすでにふれたように、スマホ全盛の時代であることを考えてのことである。こうしたツールはすべて、ネット上のアプリストアからスマホに直接格納（インストール）する方式を採っている。

オーストラリアは、わが国と同様に、電子政府（マイガブ／ myGov）ポータルにログインする際に、ユーザーの官製デジタル ID を利用させている。しかし、ユーザーフレンドリーではない官製の IC カードは発行していない。

それに、わが国のスマホは、アップル社の iPhone の市場占有率が 7 割強だ。アップル系スマホでは、マイナ IC カードから官製のデジタル ID の読取りはほとんどできない。しかし、マイナンバー制度をデザインしている役人は、頭が固いのか、発想の転換ができない。

市民（ユーザー）がオンライン申請・申告で行政の Web サイトにログインする場合には、アップルワオーレット（Apple Wallet）のような一定の基準を満たした民間のデジタル ID も、官製のデジタル ID と同じように使えるようにすればいいわけである。役人は、〝官尊民卑〟の呪縛から自らを開放すれば、解決の糸口が見えてくる。

わが国のガラパゴス化した電子政府・電子自治体（e-Gov）／マイナポータルを、モバイルデバイスに優しい（フレンドリー）に改造するのは急務であり、道を踏み外さない正しい改造が要る。このためには、他国のモデルと比較検討が欠かせない。

■どんなデジタル ID の管理モデルがあるのか？

（Q）現在、一般に採用されているデジタル ID の発行・管理の方式には、「集中管理モデル」と「連邦管理モデル」がある。ほかに、「自己主権型アイデンティティ（SSI）モデル」があるといわれる。この辺について、どう違うのか？

（A）オーストラリアの官製デジタル ID である myGovID は、連邦サービス庁（Services Australia）、国税庁（ATO）、財務省（DOF）共管の「連邦政府デジタル ID システム（AGDIS=Australian Government Digital ID System）」の枠組みのなかで、ユーザーの求めに応じて任意申請で交付される仕組みである。ユーザーは、ネット上のアプリストアから myGovID アプリを自分のスマホやパソコン（PC）にインストールする仕組みになっている。

一般に採用されているデジタル ID の方式には、①セントライズト（集中）モデルと、②（centralized model）と②フェデレーテッド（連邦）モデルがある。

【表 22】デジタル ID の管理モデルとは

①セントライズト（集中）型モデル（centralized model）
ユーザーの ID 情報は各サービス提供主体が個別に管理し、ユーザーはサービスごとに発行された ID で各 Web サイトサービスにログイン／アクセスする方式
②フェデレーテッド（連邦）モデル（federated model）
ユーザーの ID 情報は外部の主体に預けて管理し、ユーザーはその主体が発行した ID を使用して、連携している複数の Web サイトサービスにログイン／アクセスする方式
③自己主権型アイデンティティ・モデル（SSI=self-sovereign identity model）
ユーザーの ID 情報は外部の主体に預けずに、ユーザー自身が管理する方法

ただ、日本も、アメリカも、EU も、デジタル ID は、官製デジタル ID（プラットフォーム）を使うか　あるいは民間のデジタル ID（プラットフォーム）を使うかの違いはあるものの、「外部に預けて」管理する方式である。こうした管理方式のデジタル ID は、「フェデレーテッド（連邦）モデル・デジタル ID」あるいは「サイロモデル・

デジタルID」と呼ばれる。

もう少し分かりやすくいうと、消費者（ユーザー）が、オンラインで官民のWebサイトにログインしてサービスを利用するとする。この場合、ユーザーは、アカウント名やパスワードを登録し、サービスする側からデジタルIDを発行してもらって利用するやり方が主流である。こうしたデジタルIDは、発行者であるプラットフォーム企業や政府（あるいは官製の公的機関）が中央集権的に管理している。発行者によるデジタルIDの中央集権的な管理により、ユーザーは「発行者にお任せコース」を選ぶことになり、ユーザーは自分で自身の個人情報を管理する必要がない。また、ユーザーが自分のパスワードを忘れても、発行者に照会できる。発行者による中央集権的に管理は、お任せコース大好きなユーザーにとっては、利便性が良いともいえる。

ところが、このフェデレーテッド（連邦）モデルでは、プラットフォーム企業や政府プラットフォーム（ポータルサイト）が、ユーザーの大量の個人情報を蓄積・分析、ユーザーの知らないところで目的外利用されるなど深刻な問題になっている。

デジタルIDは、機微情報（sensitive information）に紐付けられることがある。このため、プライバシーや人権の侵害、デジタルIDを使ったデータ監視社会つくり［データ収容所列島化］などへの心配も高まっている。中国政府が採用する社会信用システム（social credit system）、つまり政府が収集したデータに基づいて、全国民をランク付けし、各人の『信用度』をスコア化するデジタルシステム導入は最たる例である。

こうした心配に対応するために考えられるモデルが、「自己主権型アイデンティティ（SSI=self-sovereign identity）」である。このSSIモデルは、デジタルIDをプラットフォームに預けない方式である。つまり、SSIモデルでは、管理主体は存在せず、ユーザーである個人が自身のデジタルIDを管理するデザインである。言いかえると、SSIモデルでは、サービス提供者は、第三者（プラットフォーマー）を介さないで、ユーザーに個人データを要求し、ユーザーは直接、サービス提供者にデータを送信する。

SSI（自己主権型デジタルID）モデルでは、「個人は、管理主体に依存することなく、自分の個人情報を管理・保存をし、あらゆる自己決定権をもつべきであるとの考え方」、「個人情報の自己コントロール権（the right to control personal

コラム 7　SSI（自己主権型ID）モデルの成り立ち

自己主権型アイデンティティ（SSI=self-sovereign identity model）モデルは、2000年代初めに提唱され出した。SSIについて最もよく知られているのは、2016年に、データセキュリティ専門家のクリス・アレン（Christohpher Allen）が公表した「自己主権型アイデンティティへの道（The Path to Self-Sovereign Identity）」の考え方である（The Path to Self-Sovereign Identity - CoinDesk）。アレンは、このなかで、「SSIの10原則（10 Principles of SSI）」を打ち立てた。その骨子は、次のとおりである。

①存在（existence）
ユーザーは独立した存在である。

②コントロール（control）
ユーザーは自分で自身のIDを管理でき、最終的な権限を有する。

③アクセス（access）
ユーザーは、自分のIDと紐づくすべてのデータに常に容易にアクセスできる。

④透明性（transparency）
IDを管理・更新するシステムとアルゴリズム（情報処理手順）に透明性が確保されている。

⑤持続性（persistence）
IDはユーザーが望む限り存続できること。

⑥持ち運びできること（portability）
ユーザーの権利利益ファーストとし、IDはサービス間で持ち運びができること。

⑦相互運用性（interoperability）
IDはできるだけ幅広く利用できること。

⑧同意（consent）
データは、ユーザーが同意する場合に限り利用できる。

⑨最小化（minimalization）
ユーザーへのデータの求めは最小限とし、かつ、最大限のプライバシー保護をはかること。

⑩保護（protection）
ネットワーク内の需要よりも、常に個人の自由と権利ファーストとすること。

SSI（自己主権型ID）モデルは、ユーザーは自分のデジタルIDを自己責任で管理し、提供先を選択する仕組みである。「お任せコース」大好きなユーザーが多い国では、ユーザー自身の責任が重くなることも織り込んでSSIモデルを評価する必要がある。

information)」の保障がベースにある。

自己情報コントロール権とは、伝統的なプライバシー権を進化（深化）させた考え方だ。プライバシー権は、伝統的には「一人にしてもらう権利(right to be let alone)」という考え方がベースだ。しかし、情報化が格段に進んだデジタル社会で、個人に対して「一人にしてもらう権利」を保障するのは難しい。このことから、代わりに「個人情報の自己コントロール権」を認めることで人権を護ろうというわけだ。「情報上のプライバシー権（informational privacy rights)」とも呼ばれる。

ちなみに、オーストラリアの連邦政府デジタル ID システム（AGDIS）は、②フェデレーテッド（連邦）モデルである。したがって、ユーザーである市民の ID 情報は、特定の主体(オーストラリア政府デジタル ID プロバイダー(Australian Government’s Digital ID provider)／myGovID）が管理し、ユーザーはその主体が発行した ID（マイガブ ID ／ myGovID）を使って、連携している連邦・州・準州の複数の行政機関の Web サイトサービスにログイン／アクセスできる仕組みになっている。国営のデジタル ID プロバイダーである AGDIS は、なんの縛りもなければ、ユーザーがどのような行政機関の Web サイトにログインし、どのようなサービスを受けたか追跡し、情報を収集・蓄積することもできる。権威主義国家観に基づく AGDIS の運営・管理が心配される。権威主義国家である中国政府が採用する社会信用システム（social credit system)、つまり政府が官製のデジタル ID を使って収集したデータに基づいて、全国民をランク付けし、各人の『信用度』をスコア化するデジタルシステム導入もあることが危惧される。

この点、国営のデジタル ID プロバイダーである AGDIS は、デジタル ID（myGovID）のユーザー、つまりオーストラリア市民が、どのような行政機関の Web サイトにログインしサービスを受けたのかを追跡するのを厳禁されている。これは、オーストラリア政府の AGDIS の運営・管理における基本的なプライバシー保護ルールである。

日本では、官製の共通デジタル ID である公開鍵式［JPKI ／電子証明書］を、法定の行政サービスだけでなく、民間分野にも汎用／拡大利用しようという方向である。にもかかわらず、オーストラリアと異なり、デジタル ID である公開鍵式

コラム 8　自己情報コントロール権を盛り込んだ世界の法制事例

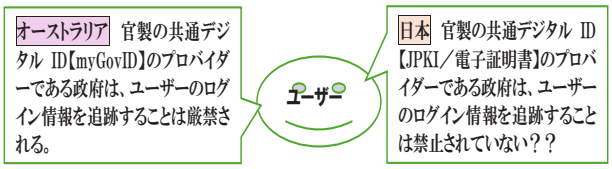
自己情報コントロール権を盛り込んだプライバシー法制事例をあげると、つぎのとおりである。

◆ EU（欧州連合）一般データ保護規則（GDPR）

EU では、2018 年 5 月に、一般データ保護規則（GDPR=General Data Protection Regulation）を施行した。GDPR は、「個人の情報に関する決定権はその個人が持つべきである（the right to control personal information)」という考えに基づき、①企業のデータ管理者（controller）の義務の強化、②本人の同意があいまいな形でのクッキーなどを使った個人情報大量集積、ビッグデータ利用に対する規制強化、③企業や公的機関の滞留する個人データや、ネット上のプライシー侵害・誹謗中傷個人情報を削除してもらう権利（忘れられる権利／ right to be forgotten）（削除権）の法認、④自分の個人データが企業のダイレクトマーケティング（DM）に利用されることを拒否する権利（right to object direct marketing）の法認、⑤不正確な自己データの訂正を求める権利、いわゆるプロファイリングを含む自動処理による個人に関する決定の対象とならない権利（Automated individual decisions)、⑥ EU 域外の第三国・地域への個人データ移転の規制、⑦データ保護規則の EU 域外企業への適用、規則違反に対する巨額の過料などからなる。（詳しくは、「【Q&A】「EU の一般データ保護規則（GDPR）とは何か」CNN ニューズ 94 号（CNN-94.pdf（pij-web.net）8 頁以下参照）

◆カリフォルニア州消費者プライバシー法

アメリカのカリフォルニア州で は、消費者プライバシー法（CCPA=California Consumer Privacy Act）を制定し、2020 年に施行した。CCPA は、消費者のプライバシー保護を徹底した法律である。「カリフォルニア版 GDPR（California’s GDPR)」との呼び名もあるほどだ。個人情報（PI=personal information）を広く定義し、削除権（right of deletion）や自己情報を第三者に譲渡することを拒否する(opt-out)権利、消費者が権利行使をしたことを理由に差別されない権利（right to be free of discrimination）などを法認した。（詳しくは、「カリフォルニア州消費者プライバシー法を読む」CNN ニューズ 98 号（CNN-98〔完成版〕.indd（pij-web.net）11 頁以下参照）



［JPKI ／電子証明書］のユーザーが、どのような行政機関の Web サイトにログインしサービスを受けたのかを追跡するのを法律で厳禁していない。

日本でも、官製の共通デジタル ID プロバイダーである国は、国民の官製の共通デジタル ID である公開鍵式［JPKI ／電子証明書］利用歴の収集を厳禁し国民のプライバシーを守る姿勢を明確にすべきである。この場合、郵便法や民間事業者による信書の送達に関する法律などに盛られた信書の秘密の保護等に関する規定などを参考とするのも一案である。国民の官製の共通デジタル ID である公開鍵式［JPKI ／電子証明書］の利用歴の収集を禁止する規定を設けないといけない。

■ブロックチェーン技術を使ったデジタル ID とは

（Q）ブロックチェーン技術を使った SSI モデルのデジタル ID が注目されているが、その理由を教えて欲しい。

（A）SSI（自己主権型デジタル ID）モデルは、ブロックチェーン（分散台帳／暗号資産）技術との相性がよいといわれる。このことから、ブロックチェーン技術を実用化した次世代型デジタル ID、官または民のプラットフォーマーのいないデジタル ID として注目を浴びている。とりわけ、ブロックチェーン技術自体は、データの安全やプライバシー保護の観点からの評価が高いからだ。

ブロックチェーン技術（blockchain technology）とは、ネットワーク上にある端末同士を直接接続して（peer-to-peer network）、取引記録を暗号技術で分散して処理・管理するデータベース／プラットフォームである。さまざまなモデルがあるが、一般に、仲介者（intermediary）がいないモデルである。つまり、仲介者がいないことから、ブロックチェーン技術は、）SSI（自己主権型デジタル ID）と相性がよいとされるわけである。

もっとも、ブロックチェーン技術そのものは、暗号通貨（cryptographic currency）や付加価値税（VAT ／ GST）課税の際に仕入税額控除に使うデジタルインボイス（digital invoice）など、さまざまな利用が想定されている。したがって、デジタル ID への利用だけを想定したものではない。税務面では、デジタルインボイスだけでなく、納税申告データを、ブロックチェーン技術を応用したプラットフォームを介して流通させようという検討も進められている。

現在のブロックチェーン技術を使わないデジタル ID では、各ユーザーは、各機関の Web サービスを受ける度に違うログイン ID とパスワードを使わないといけない。この結果、デジタル ID 情報は、仲介者であるさまざまなプラットフォーム企業に集中管理・蓄積される。各ユーザーは自分のデジタル ID を自己コントロールすることは難しい。ユーザーは、自分が提供した個人情報が、仲介者（プラットフォーマー）に、目的外利用される、あるいはデータ漏洩があっても、ユーザーが直接ストップをかけることは至難である。

こうした問題を避けたい。信頼できる官民のあらゆる Web サイトで同じ ID でログインできる「単一デジタル ID システム（a single digital ID system）」あるいは「官営のデジタル ID システム（government-based digital ID system）」があれば、そこに〝お任せ〟する。その方が、利便性が高く、ユーザーフレンドリーだ、と思う人も少なくないと思う。

まさに、わが国の官製のデジタル ID（JPKI）や、オーストラリアの官製の myGovID が適例だ。つまり、こうした単一あるいは官製（官営）のデジタル ID は、〝国家は悪いことをしない〟、〝デジタル ID の本性は利便・コンビニ〟という〝性善説〟あるいは〝信仰〟をベースにつくられた仕組みといえる。

しかし、こうした単一あるいは官製（官営）のデジタル ID システムでは、仲介役を演じる国家が、ユーザーである市民がどのような Web サイトにログインし、どのようなサービスを受けたか追跡できる。膨大な個人情報を収集・蓄積して、市民を AI（人工知能）で分析・監視できる。〝デジタル ID の本性は利便・コンビニ〟の信仰は、〝迷信〟かも知れない？なぜならば、人権を尊重する政体が持続するとは限らないからだ。

デジタル ID の本性は〝個人情報の監視〟と見る〝性悪説〟にも一理ある。単一あるいは官製（官営）のデジタル ID システムは、権威主義国家つくりにはうってつけの凶器に大化けするからだ。単一あるいは官製（官営）のデジタル ID システムの評価には、国民のデータ監視は当り前の考えを丸出しにした独裁政体が出現する可能性も織り

込まないといけない。単一あるいは官製（官営）のデジタルIDを使ったデータ監視社会つくり、「データ収容所列島化／デストピア（暗黒郷）構想」の〝悪夢〟が消えないからだ。

この点、SSI（自己主権型デジタルID）モデルのブロックチェーン技術を使ったデジタルIDシステム（block-chain-based digital ID system）は、デジタルID情報の集中管理も必要がなく、データセキュリティやプライバシー保護に資する。

デジタルIDについて、いずれは、ブロックチェーン技術を応用した自己主権型アイデンティティ（SSI）モデルが主流になるとの見方もある（詳しくは、「Q&A：デジタルIDとは何か」CNNニューズ113号27頁以下参照）。

しかし、ブロックチェーン技術を応用したSSIモデルは、極めて複雑な仕組みである。また、ひとくちにブロックチェーン技術といっても、さまざまなタイプがある。ブロックチェーンのような新技術の汎用は、とりわけデジタル技術に精通していないユーザーには重荷になる。つまり、運用効率性（operational efficiencies）が問われる。どれくらいのコスト負担になるのかも未知数である。この新技術の信頼性（trust）や透明性（transparency）、持続可能性（sustainability／persistence）も問われる。加えて、仮に税務行政などにブロックチェーン技術を応用したSSIモデルを採用するとなると、公的ブロックチェーンインフラ（public blockchain infrastructure）の構築も重い政策課題となる。もともと、ブロックチェーン技術自体、既成のガバナンスや政府規制を嫌う、自由な発想に基づく新技術だからである。ブロックチェーン技術を応用したSSIモデルの採用では、相互運用性（interoperability）の確保や標準化（standardization）も至難な課題である［See, Orly Mazur, 〝Can Blockchain Revolutionize Tax Administration?〟, 127 Penn St.L.Rev.115（2022）; Charles J.Delmotte, 〝Toward a Blockchain-Driven Tax System,〟, 43 Va. Tax Rev.37（2023）］。

■豪での信頼できるデジタルID制度確立の動き

（Q）オーストラリアのデジタルID制度の最近までの流れを、もう少し詳しく教えて欲しい。

（A）急激なデジタル（DX）化には、専門職界でも大きな戸惑いがある。このことから、こうした動きに後ろ向きになるのも理解できる。しかし、次の世代のことも考え、日本が経済的に沈没しないようにするには、デジタル化の恩恵も評価しないといけない。その場合、何よりも、安心・安全、かつ人権ファーストのデジタルIDが必要だと思う。

オーストラリア政府は、デジタル化の大波を受けて、電子政府／myGovポータルサイト／政府プラットフォームの構築に力を入れてきた。とくにその核となるデジタルIDの問題にも取り組んできた。

わが国では、「デジタルID」について、マイナンバー制度に反対している人たちも、賛成している人たちも、よく理解できていない。「デジタル共通番号」というと、逆に「マイナンバーとどう違うのか？」と質問される。役人は、いかに、市民を取り残し、デジタル化をいかに自分らに都合のよい方向に使うかが優先している。言い換えると、政府広報がいかにいい加減なのが実感できる。

オーストラリアの電子政府／myGovポータルサイトの経緯については、すでに詳しくふれている。ですから、ここでは、デジタルID／myGovIDの最近までの動きについてふれて見る（tdif_02_overview_-_release_4.8_-_finance_1.pdf（digitalidentity.gov.au））。

■GovPass／ガブパス計画

オーストラリア政府は、2017年に「GovPass／ガブパス」と名付けた「デジタルID国家戦略」を公表した。連邦政府のデジタルトランスフォーメーション庁（DTA=Digital Transformation Agency）が立てた計画である。GovPass／ガブパスに盛られた計画は、デジタルIDに関する政策の策定、システム設計、技術開発など多岐にわたる。GovPass／ガブパス計画のアウトラインは、次頁（**【表23】**）のとおりである。

■信頼できるデジタルID制度とは

（Q）オーストラリア政府の信頼できるデジタルIDの枠組み（TDIF=Trusted Digital Identity Framework）について、もう少し詳しく説明して欲しい。

（A）GovPass／ガブパスは、連邦デジタルトランスフォーメーション庁（DTA）が主導する計画である。この計画における最も重要な目標の1つ

【表 23】GovPass ／ガブパス計画の推移

・2017 年～	GovPass ／ガブパス計画への連邦予算計上。
・2019 年～	試行開始
・2020 年 3 月～	生体認証デジタル ID 試行開始
・2020 年 5 月	民間のデジタル ID プロバイダーの参加。信頼できるデジタル ID の枠組み（TDIF=Trusted Digital Identity Framework）を改訂し、民間デジタル ID プロバイダーが GovPass ／ガブパスに参加するための認証を受けることを承認
・2024 年 5 月	デジタル ID 法成立。信頼できるデジタル ID 枠組み（TDIF）に法的典拠を与える

は、行政 Web サイトや民間企業の Web サイトを利用する個人や企業に対して、簡単で、安全かつ安心してログイン（サインイン）できる信頼できるデジタル ID を提供する仕組みづくりにある。このため、オーストラリアにおける「信頼できるデジタル ID の枠組み（TDIF=Trusted Digital Identity Framework）」を確立することにある。

TDIF の対象となるのは、官民双方のデジタル ID である。これまで、連邦サービス省（Services Australia）が所管する連邦政府デジタル ID システム（AGDIS=Australian Government Digital ID System ）の中でネット交付されているマイガブ ID ／ myGovID について点検してきた。TDIF の対象となるのは、マイガブ ID ／ myGovID はじめとした他の官製のデジタル ID も含む。加えて、民間の数多くのデジタル ID プロバイダー（IT 企業）が提供するデジタル ID も含まれる。

オーストラリア政府は、信頼できるデジタル ID の枠組み（TDIF）を確立するために、次のようなデジタル ID の指導原則（Guiding principles）を掲げている。

【表 24】デジタル ＩＤの指導原則（Guiding principles）

①ユーザー中心（User centric）

❶デジタルサービスにアクセスすることが、簡易、便利、簡単、安全かつ信頼できるものであること。❷個人は、認証された政府または民間の認証されたプロバイダーからデジタル ID を生成することを選択できること。❸個人は、本人および事業上のデジタル ID を複数の ID サービスプロバイダーを利用することができること。

②任意性と透明性（Voluntary and transparent）

❶個人が参加するかどうかを選択すること（つまり、オプトイン方式）。❷個人が自己のデジタル ID を簡単かつ直接コントロールできること。❸クレデンシャル情報（credential）の利用記録は、認証プロバイダーにより安全に保存され、かつ、信頼できるデジタル ID 枠組み（TDIF=Trusted Digital Identity Framework）のもとで権限行使ができる者が容易にアクセスできるようにすること。

③サービス提供の要点（Service delivery focused）

❶認証プロバイダーは、ユーザーが行政または民間のデジタルサービスにアクセスするときに選択と便宜を提供すること。❷費用はどの利用者にとっても中立であること。❸民間部門の利用を促すビジネスモデルであること。

④プライバシー向上（Privacy enhancing）

❶認証プロバイダーがユーザーの個人情報の収集および開示は、当該ユーザーの明示の同意を得ると同時に、プライバシー保護法や善良なプライバシー慣行（good privacy practices）に従う場合にのみ許される。❷認証プロバイダーは、あらゆる個人情報に対してプライバシー促進技術、ポリシーおよびプロセスを適用すること。❸ユーザーは、自己の個人情報がどのように利用されかつ保護されるのかインフォームド・アンダスタンディングできること。❹利用者は自己の個人情報の開示を求めかつ管理し、誤りの訂正を求めかつ同意を撤回できること。❺ ID エクスチェンジプロバイダー（Identity Exchange provider）は、ID サービスプロバイダー（Identity Service Providers）、アトリビュートサービスプロバイダー（Attribute Service Providers）またはリライングパーティ【Relying Party ／本人確認結果を利用してユーザーに対してサービス提供を行う主体】に対して単一の ID を発行しないこと。❻個人情報に関する単一のクレデンシャル情報（credential）または集中管理型（centralised）のデータベースをつくらないこと。

⑤官民連携（Collaborative）

積極的な官民部門の連携および広範なコミュニティ連会は、行政と企業がそれぞれの強みと専門性の発揮につながるであろうこと。

⑥相互運用性（Interoperable）

❶他のトラストフレームワークならびに内外の ID サービスとの協力を促進すること。❷認証プロバイダーとリライングパーティのニーズを拡大しかつ調整すること。

⑦適応性（Adaptable）

❶テクノロジーやビジネスモデルにおける柔軟性や革新を推進すること。❷信頼できるデジタル

ID 枠組み（TDIF）は、コミュニティの期待、ビジネス、法律および社会のニーズの変化に即した展開ができるように柔軟であること。❸信頼できるデジタル ID 枠組み（TDIF）は、低価値から高価値の情報交換、およびペンネームのものから完全に証明された情報まで、安全な情報交換を保障すること。

⑧安全・弾力性（Secure and resilient）

❶認証プロバイダーは、厳格な政府の安全保障基準に適合すること。❷同様の要件を民間機関や行政機関に適用すること。❸認証プロバイダーやリライングパーティは、サイバーセキュリティへの脅威や危険を確認し、かつ、積極的管理すること。❹効果的な不正管理統制を実施しかつ継続すること。

■ TDIF で認証の対象となるデジタル ID プロバイダーの種類と機関／企業とは

（Q）オーストラリアには、デジタル ID を発行する行政機関や民間機関（企業）【デジタル ID プロバイダー】は、政府の「信頼できるデジタル ID の枠組み（TDIF）」のなかで、認証（accreditation）を受けられる仕組みがある。これはわが国にはない仕組みだ。デジタル ID プロバイダーが TDIF で認証を受けられる仕組みについて教えて欲しい。

（A）オーストラリア政府の「信頼できるデジタル ID の枠組み（TDIF）」では、認証の対象となる行政機関や企業（2024 年デジタル ID 法では双方を一括して「entity」と表記している。ここでは「機関」と邦訳しておく。「実体」という邦訳も可能だ。）を、次の４つのカテゴリーにわけている。それぞれのプロバイダーが、どのようなサービス（業務）を遂行するのかも含めて、簡潔に説明を加えて見る。

【表 25】認証対象となるデジタル ID プロバイダーの種類

●属性サービスプロバイダー（Attribute Service Providers）

属性サービスプロバイダーは、オーストラリア国税庁（ATO）や、連邦サービス省（Services Australia）のような、サービス利用者の氏名や生年月日のような属性情報を保有している機関を指す。属性サービスプロバイダーは、「信頼できる当事者（Relaying Party）」判断する場合に本人であると証明するサービスを提供する認証された機関である。例えば、ATO は、認証された属性サービスプロバイダーとして、個人とビジネスとの間の関係を電子的に証明・認証するプラットフォーム「RAM=Relationship Authorisation Manager（RAM）」（電子的な【関係性認証システム】）を運営している。

●クレデンシャルサービスプロバイダー（Credential Service Providers）

クレデンシャルサービスプロバイダーは、正当なユーザーであることを証する、ユーザーネーム＋パスワード、ワンタイムパスワード、生体データなどを管理し、かつ、これらのデータを提供するサービスをする機関である。ID サービスプロバイダー（IdP）も、クレデンシャルサービスを行うことができる。

●ID エクスチェンジプロバイダー（Identity Exchanges Providers）

ID エクスチェンジプロバイダーとは、本人属性を安全に流通させるために管理・調整するサービスをする機関である。連邦サービス省（Services Australia）があてはまる。同省は、ID フェデレーション（ID Federation）のメンバー間での ID の流通を管理・調整する業務を担っている。

●ID サービスプロバイダー（IdP=Identity Service Providers）

各種オンラインサービスの利用に際し個人のアイデンティティ（本人確認）証明する認証された行政機関、非政府機関、民間機関が、「IdP（ID サービスプロバイダー）」にあたる。個々のサービスで求められる保証強度により、ユーザーは、俗に 100 ポイント身元確認チェックといわれる基準に基づき適切なポイントを満たす身元確認資料や経歴を提示するように求められる。ID サービスプロバイダー（IdP）は、ユーザーがデジタル ID を入手する条件として生体認証を求める場合もある。オーストラリア国税庁（ATO）は、myGovID のデジタル ID サービスでは、認証された ID サービスプロバイダー（IdP）である。また、オーストラリア郵便（Australia Post）も、認証された IdP 機関である。マスターカード（Mastercard）も、民間機関であるが、ID サービスプロバイダー（IdP）として認証された機関である。

●本人確認を求めた公的機関や民間企業（Relying parties）

■認証デジタル ID プロバイダーになる申請手続

（Q）認証デジタルプロバイダーの認証を受けるには、官民の機関はそれぞれ任意の申請が必要であるが、申請手続について教えて欲しい。

（A）デジタル ID のプロバイダーである官民の機関は、申請に基づいて認証（accreditation）を受けることになる。各機関は、申請に先立ち、機関のサービス内容や業種【ID プロバイダー、クレデンシャルプロバイダー、属性プロバイダー、ID エクスチェンジプロバイダー】の詳細について、オンラ

インで連邦財務省の認証担当者と事前の打ち合わせ（pre-engagement meeting）をするように求められる。その後、正式な申請手続に進むことになる。信頼できるデジタル ID の枠組み（TDIF）のなかでの認証されたプロバイダーになるには、一般に、次のような要件を満たすように求められる。

【表 26】一般的な認証要件とは

アクセシビリティ（accessibility）およびユーザビリティ（usability）
ユーザーは自身の ID に紐づくすべてのデータを常に容易に入手できるようになっているかどうか。
プライバシーの保護（privacy protection）
ユーザーの ID に関するプライバシーがしっかりと保護されるようになっているかどうか。
安全および不正制御（security and fraud control）
ユーザーの ID の安全と不正利用の制御・取締りができるようになっているかどうか。
危機管理（risk management）
ユーザーの ID の危機管理を徹底できるかどうか。
技術的清廉性（technical integrity）など
常にユーザーの ID に関する技術の向上に努める態勢ができているかどうか。

認証する場合の具体的な手続や細目については、次の資料を参照して欲しい（https://www.digitalidentity.gov.au/tdifdocs）。

最終手続として、すべての申請機関は、財務省との間で、TDIF 上の義務で遵守することを約する「認証ガバナンス協定（accreditation governance agreement）」を締結することになる（ TDIF 03 Accreditation Process.）。

申請機関であるプロバイダーは、いったん認証を受けると、年次報告を含む、TDIF 上の義務の遵守状況を継続的に開示するように求められる（TDIF 07 Maintain Accreditation）。

■認証デジタル ID プロバイダーになった機関

（Q）デジタル ID の認証を受けた行政機関や民間企業の認証状況を教えて欲しい。

（A）認証デジタル ID プロバイダーになった機関については、Web サイトで閲覧できる（Trusted Digital Identity Framework（TDIF）| Digital Identity）。この Web サイトを参考にして、認証デジタル ID プロバイダーになった機関と認証された機関がどのようなタイプのプロバイダーサービスを提供するのか、以下に図（**【表 27】・【表 28】**）にして、簡潔に紹介して見る。

■ TDIF 制度を刷新するデジタル ID 法の経緯

（Q）オーストラリア政府は、最近、信頼できるデジタル ID 枠組み（TDIF）の構築に向けて、デジタル ID 法案（Digital ID Bill）を連邦議会に提出し、成立したとのことだが、どのような立法目的、内容の法律なのか。

（A）2023 年 11 月 30 日に、連邦議会上院経済法制委員会（Economics Legislation Committee）に、デジタル ID 法案（Digital

【表 27】政府のデジタル ID システムを担当する認証された機関

認証された機関	サービス名称	業種	サービス内容	認証日
ATO（国税庁）【事業者番号／ABN：51 824 753 556】	myGovID	ID プロバイダー（IdP）	・再利用可能なデジタル ID ・モバイル対応 ・IP 1 ・PI 2 ・IP 3 ・生体認証対応	2019 年 5 月 30 日 IP3 および生体認証対応については 2021 年 8 月 30 日に認証
		クレデンシャルプロバイダー	・モバイル対応 ・CL 2 ・Multi-Factor Crypto Software	2019 年 5 月 30 日
	RAM	属性プロバイダー	Business Authorisation Attributes	2019 年 6 月 20 日
連邦サービス庁 Services Australia【事業者番号／ABN：90 794 605 008】	Exchange	エクスチェンジプロバイダー	認証された機関と信頼できる当事者との紐づけ支援	2019 年 5 月 13 日
	RAM	属性プロバイダー	myGov LinkID attributes	2021 年 8 月 25 日

【表 28】政府のデジタル ID システム外でサービスをする認証された機関

認証された機関	サービス名称	業種	サービス内容	認証日
オーストラリア郵便公社【事業者番号／ABN：28 864 970 579】	myGovID	ID プロバイダー (IdP) クレデンシャルプロバイダー	・再利用可能なデジタル ID ・モバイル対応 ・その他	2019 年 5 月 17 日
ID バース（IDVerse）、OCR Labs Pty ltd 社の商標【事業者番号／ABN：20 603823 274】	IDKit	ID プロバイダー (IdP)	・One-off verification ・モバイル対応 ・IP1 Plus ・IP2 ・IP2 Plus ・IP3 ・生体認証対応	2021 年 7 月 8 日 生体認証対応については 2022 年 3 月 7 日に認証
マスターカード (Mastercard)【事業者番号／ABN：95 108 603 345】	ID	ID プロバイダー (IdP)	・再利用可能なデジタル ID ・モバイル対応 ・IP1 Plus	2022 年 7 月 21 日
		クレデンシャルプロバイダー	・モバイル対応 ・Multi-Factor Crypto Software ・CL2 ・生体認証対応	2019 年 5 月 13 日
		エクスチェンジプロバイダー	・エクスチェンジサービス	2022 年 6 月 10 日
eftpos デジタル ID Pty Ltd 社【事業者番号／ABN：80 648 970 101】	ConnectID Exchange services	エクスチェンジプロバイダー	・再利用可能なデジタル ID ・モバイル対応 ・IP1、IP1 Plus、IP	2023 年 10 月 20 日
Makesure Consulting Pty Ltd 社【事業者番号／ABN：35 168 163 666】	RatifyID	ID プロバイダー (IdP)	・モバイル対応 ・CL2 ・その他	2023 年 10 月 20 日

ID Bill 2023）が上程された（Digital ID Bill 2023-Parliament of Australia（aph.gov.au））。この法案は、オーストラリアにおけるデジタル ID に関する包括的な法的枠組みを構築するためのデジタル ID 基本法である。認証制度を敷いて、現在オーストラリアで使われている政府および民間のデジタル ID サービスを安全かつ簡素で、ユーザーである個人や企業にもっとフレンドリーなものにすることが狙いである。

デジタル ID 法は、官製のデジタル ID である myGovID を所管する ATO（国税庁）や連邦サービス省（Services Australia）などの行政機関（government agencies）のみならず、デジタル ID を提供するに民間 IT 企業（private sector service providers）も、任意の形で認証を受けることができる。「デジタル ID サービスプロバイダー（digital ID service providers）」、「属性プロバイダー（attribute providers）」などのカテゴリーに分けて認証する。

これら認証を受けたデジタル ID プロバイダーには、ユーザーのプライバシー保護の徹底など質管理（QC）やガバナンス向上のための義務が課される。任意のデジタル ID プロバイダーの認証制度（voluntary accreditation scheme）ではあるが、できるだけ多くのプロバイダーが、連邦政府デジタル ID システム（AGDIS=Australian Government Digital ID System ）に参加するように推奨されている。

近年、オーストラリアでは、市民や企業が、ATO やセンターリンク、myGovID をかたったスキャム／詐欺メール、サイバー犯罪の急増に悩まされている。myGovID キャムメールは、フィッシング詐欺や本物そっくりの偽装されたウエブサイトに誘導し、そこで ID やパスワード、クレジットカード（クレカ）情報などを含むセンシティブ（機微）な個人情報を入力させて、それらの情報を盗み出すことを狙いとしている。

こうした一連のデジタル ID 制度改革、とりわけ「デジタル ID にかかる認証制度」を稼働されることにより、サイバー犯罪に対処できるオーストラリアにおける「信頼あるデジタル ID 枠組み（TDIF=Trusted Digital Identity Framework）」

を刷新し、サイバーセキュリティを堅固なものにしようというものである。

デジタルID法案（Digital ID Bill 2023）は、2023年11月30日に、連邦議会上院経済法制委員会に上程されてから、慎重に審議された。この法案には、人権団体や右派政党などから批判がでた。「権威主義国家の電子監視ツールの合法化、実質的な強制利用でないか」、「中国政府が採用する社会信用システム（social credit system）、つまり政府が収集したデータに基づいて、全国民をランク付けし、各人の『信用度』をスコア化するデジタルシステム導入につながる。」など。

現在のアルバニージー首相率いる労働党政権は、2024年4月3日に、2024年デジタルID法案（Digital ID Bill 2024）として、連邦議会上院通過に成功し、連邦議会下院に送られた。同法案は、同年5月16日に連邦議会下院を通過し、成立した。

デジタルID法の経緯を簡潔の一覧にすると、次のとおりである。

【表29】デジタルID法の経緯

法案PC（パブリック・コンサルテーション）手続
2023年デジタルID法案原案（Draft Digital Identity Bill 2023）に対し、意見公募（2023年9月29日～2023年10月10日）
法案の上院への上程
法案を、2023年11月30日連邦議会上院経済法制委員会に付託し、2024年2月28日までに審査のうえ報告書提出を求めた。2024年1月19日に報告書を提出
法案の上下両院通過
法案は、2024年3月27日に、連邦議会上院を通過。下院(House of Representatives)に送致。・法案の下院通過・成立　法案は2024年5月16日に連邦議会下院を通過、成立した。

■ 2024年デジタルID法の概要

（Q）2024年デジタルID法案（Digital ID Bill 2024）は、2024年5月16日に成立したが、どのような立法目的、内容の法律なのか？まず、デジタルID法の建て付けがどうなっているのかを教えて欲しい。

（A）2024年デジタルID法は、10の章、170を超える条文からなる法律である。10の章（Chapter）＋節（Part）＋款（Division）＋目（Subdivision）は、そのタイトルだけを邦訳して紹介すると、次のとおりである。

【表30】2024年デジタルID法の骨子

第1章（Chapter1）　総則
　第1節（Part1）　通則
　第2節　解釈
第2章　認証（Accreditation）
　第1節　総則
　第2節　認証
　　第1款（Division1）認証の申請
　　第2款　認証
　　第3款　認証の変更、停止及び取消
　　第4款　認証に関する大臣の指示
　　第5款　認証規則
　　第6款　認証に関する雑則
第3章　プライバシー（Privacy）
　第1節　総則
　第2節　プライバシー
　　第1款　1988年プライバシー法との関係
　　第2款　追加的プライバシー保護措置
第4章　連邦政府デジタルIDシステム
(Australian Government Digital ID System)
　第1節　総則
　第2節　連邦政府デジタルIDシステム
　　第1款　連邦政府デジタルIDシステム
　　第2款　連邦政府デジタルIDシステムへの参加
　　第3款　参加承認の変更、停止及び取消
　　第4款　参加に関する大臣の指示
　　第5款　連邦政府デジタルIDシステムに関する雑則
　第3節　責任と救済の枠組み
　　第1款　参加機関の責任
　　第2款　制定法上の制約
　　第3款　救済の枠組み
第5章　デジタルID規制官
(Digital ID Regulator)
　第1節　総則
　第2節　デジタルID規制官
第6章　システム管理者
(System Administrator)
　第1節　総則
　第2節　システム管理者
第7章　デジタルIDデータスタンダード
(Digital ID Data Standards)
　第1節　総則
　第2節　デジタルIDデータスタンダード
　第3節　デジタルIDデータスタンダード担当官
　　第1款　デジタルIDデータスタンダード担当官の設置及び職権
　第2節　デジタルIDデータスタンダード担当官の任免

（Q）2024 年デジタル ID 法の建てつけはどうなっているのか紹介して欲しい。

（A） 経済・社会の DX 化が加速している。いずれの先進国においても、デジタル ID の安全性を確保し、デジタル ID のユーザー・消費者である市民・納税者のデジタル ID にかかるプライバシー保護を徹底することが、重い政策課題となっている。

オーストラリアは、信頼できるデジタル ID の枠組み（TDIF=Trusted Digital Identity Framework）」を構築しようということで、ユーザー・消費者保護の視点から、デジタル ID 法を制定し、法的対応をした国の１つである。

【表 31】デジタル ID 法の立法理由

①既存の任意の認証制度 (voluntary accreditation scheme）の整備をすること。
②連邦政府のデジタル ID システム（AGDIS=Australian Digital ID System）の展開に法的根拠を付与すること。
③ユーザーのプライバシーおよび消費者保護を強化すること。
④デジタル ID のガバナンスを強化すること。

2024 年デジタル ID 法は、オーストラリア国内でデジタル ID サービスにアクセスする市民・納税者（ユーザー）のプライバシー保護、データの安全性および利便性を推進し、かつ、デジタル ID の利用を通じて経済発展に寄与することを目的とする。こうした目的を達成するために、デジタル ID 法は、各種デジタル ID サービスプロバイダーである機関（entity）を対象とした既存の任意の認証制度（voluntary accreditation scheme）を強化し、かつ、連邦政府のデジタル ID システム（AGDIS=Australian Government Digital ID System）の展開に備えて法的根拠を与えるものである。すなわち、デジタル ID のデータセキュリティを確保し、ユーザーのプライバシーを保護するため、オーストラリア政府が、デジタル ID サービスプロバイダーである官民の機関に対する認証制度を整備し、認証された機関に、連邦政府デジタル ID システム（AGDIS）への自由な参加を求める仕組みである。

デジタル ID 法は、デジタル ID 規則（Digital ID Rules）や認証規則（Accreditation Rules）がセットになっている。デジタル ID 規則や認証規則はデジタル ID 法の枠内で制定される法令であり、必要に応じて改定される。

【表 32】デジタル ID 認証にかかる法的根拠

①デジタル ID 法（Digital ID　Act）
②デジタル ID 規則（Digital　ID　Rules）
③認証規則（Accreditation Rules）

認証サービス（業務）は、デジタル ID 規制官 (Digital ID Regulator）［当面は、連邦競争・消費者委員会（Australian Competition and Consumer Commission)］が担当する。認証サービスについては、本法の枠内で制定された認証規則（Accreditation Rules）が法的根拠になる。デジタル ID 規制官は、任意の申請に基づき、認証規則に規定する種類のサービスを提供するもしくは提供を予定するの機関を、認証規則に従って、属性サービスプロバイダー（Attributes Service Provider)、ID エクスチェンジプロバイダー（ID Extension Provider)、ID サービスプロバイダー (ID Service Provider）として認証する。認証された機関には、これまでの連邦プライバシー法上の保護義務に加え、デジタル ID 法および認証規則に基づいてさらに一定の保護義務が課され、制裁が伴う形でそれらの義務を遵守するように求められる。具体的には、サイバー犯罪および不正事

故報告、データローカライゼーション＊の責任および罰則などの規定が適用になる。

＊「データローカライゼーション（data localization）」とは、〝越境データ規制〟、すなわちネット上のサービスについて、物理的なサーバーや、個人や企業のデータすべてその個人等が居住する国内に存在しなければならないという考え方である。

オーストラリアにおいて、個人のユーザーがオンラインで行政サービスにアクセスする場合、官製のデジタルIDである「マイガブID／myGovID」を使う必要がある。しかし、myGovIDの利用は、あくまでも「任意（voluntary）」であることを基本とする。認証されたデジタルIDプロバイダーである官民の機関は、この基本を守らないといけない。

連邦政府デジタルIDシステム（AGDIS）に参加を望む官民の機関は、参加に先立ち認証を受ける必要がある。

2024年デジタルID法の特徴をまとめてみると、次のとおりである。

◆任意の認証制度の確立

この法律は、各種デジタルIDサービスプロバイダー向けの任意の認証制度を規律する。この認証制度は、経済全般に展開され、かつ、信頼あるデジタルIDの枠組み（TDIF）からの学びを取り入れて構築される。TDIFに対する大きな変更点は、執行体制の強化にある。認証を受けたサービスプロバイダーの非違行為に対しては民事罰を課す。

・サービスプロバイダーは、次の3つ、つまり、①IDサービスプロバイダー（IdP=Identity service providers）、②属性サービスプロバイダー（Attribute service providers）、③IDエスチェンジプロバイダー（Identity exchange provider）のタイプに分けて認証される。新たなテクノロジーに対応するために、他のタイプのサービスプロバイダーも認証規則（Accreditation Rules）の定めに従い認証することができる。

・認証要件は、デジタルID法および認証規則（Accreditation Rules）で定める。認証規則は、IDの認証ランク、プライバシー、安全性、アクセシビリティ（accessibility）およびユーザビリティ（usability）などテクニカルな細目について規定する法令である。

・認証制度は任意であるが、機関はいったん認証を受けると、1988年連邦プライバシーが求める保護措置の水準を超える厳しいプライバシー保護措置を遵守しないといけなくなる。これらの保護措置のなかで重要なのは、単一の識別子（single identifier）の利用の禁止、マーケティング利用向けの情報開示の禁止、生体情報その他の個人情報の収集・利用・開示の制限である。連邦議会のオンブズパースンである情報コミッショナー（Information Commissioner）が、これらの保護措置の実施を監視し、かつ、違反を制裁する権限を有する。

◆連邦政府デジタルIDシステム

この法律は、連邦政府デジタルIDシステム（AGDIS=Australian Government Digital ID System）の国全体への段階的拡大を認める。様々なデジタルIDを公的部門と民間部門の機関の間でのデジタルIDを相互にまたは共同で利用することの促進につながる。

連邦政府デジタルIDシステム（AGDIS）は、現在、連邦のIDサービスプロバイダー（myGovID）、属性プロバイダー（RAM=Relationship Authorisation Manager【電子的な関係性認証システム】およびIDエクスチェンジプロバイダー（連邦サービス省が所管）が母体となっている。連邦、州、準州のいくつかの機関は、AGDISに参加し、信頼できる当事者（relying party）として、myGovIDないしRAM【電子的な関係性認証システム】を使って個人や企業に対するオンラインサービスを提供している。

AGDISの段階的な拡大は、次のようなフェイズで進められる。

・**フェイズ1および2**　デジタルIDプロバイダーおよび属性プロバイダーの相互利用を連邦・州・準州のサービスに拡大する。

・**フェイズ3**　逐次、政府デジタルIDおよび政府属性プロバイダーの利用を民間部門のサービスに拡大する。

・**フェイズ4**　民間のデジタルIDおよび民間の属性プロバイダーの利用を一定の政府（行政）サービスに拡大する。

AIDIS内で展開される各種デジタルIDプロバイダーは認証を受けなければならず、さらに厳しい規制の対象となる。これら追加される規制は、信頼できる当事者（relying parties）に対しても適用になる。

デジタルID法は、連邦政府デジタルIDシステム（AGDIS）に参加を望む機関に対してより厳しい受忍義務を課している。例えば、AGDIS内（とりわけ行政サービスにアクセス）では、個人に対する各種デジタルIDの利用は、原則として任意でなければならない。また、サイバーおよび不正事故報告、データローカライゼーション、責任および罰則に関する特別の要件がデジタルID法やデジタルID規則に定められている。

◆トラストマーク（Trustmarks）

デジタルID法は、国民の信頼を確立するためのデジタルIDの透明化策を規定している。デジタルID法案とデジタルID規則は、認証を受けたデジタルIDのサービスプロバイダーにトラストマークの使用を認める。法案は、規制官（Regulator）に対して、デジタルIDを提供する企業が、サービスプロバイダーであること、および認証プロバイダーであること、ならびにAGDISに参加する信頼できる当事者であることが分かるように公的記録を保存するように求める。

◆連邦デジタルID規制官（Australian Digital ID Regulator）

デジタルID法は、認証制度とAGDISのガバナンスを確立する。このため、独立した連邦デジタルID規制官（当初はACCC=Australian Competition and Consumer Commission／連邦競争・消費者委員会とする。）を創設する。この規制官は、認証業務、AGDISへの参加の承認、および法令上のプライバシー以外の事項の遵守状況の執行にあたる。

・本法は、デジタルID規制官に業務について定める。
・サービスオーストラリアは、AGDISの安全・清廉性・および執行に関する業務を担う。
・本法は、データ基準担当（Data Standards Chair）の任命について定める。当該担当は、AGDISの運営および認証制度を支援する技術的な基準を開発する。

◆民事制裁および規制権限（Civil penalties and certain enforcement powers）

デジタルID法は、規制官が法令遵守を求めることに役立つように、民事制裁および一定の規制権限について規定する。本法は、規制官に一連の是正権限を与える。それらは、信頼できるプロバイダーである認証資格またはAGDISへの参加資格の停止もしくは取消前に、質問検査する権限、救済命令を出す権限、執行可能な合意書の発行にまで及ぶ。

・デジタルID法は、この法律のプライバシー保護措置違反は、1988年連邦プライバシー法に定めるプライバシーの侵害にあたることを明確に規定する。このことから、連邦議会のオンブズパースンである情報コミッショナー（Information Commissioner）は、プライバシー法のもとでデジタルIDに関してその権限を行使しかつ制裁規定を適用することを可能にする。

◆所管大臣の権限（Powers of Minister）

デジタルID法は、担当大臣の一定の権限について規定する。それらは、法令制定権限、認証およびAGDIS参加に関し国家安全保障を理由とする規制官への命令の発出、データ基準担当（Data Standards Chair）の任命、および大臣の裁量に基づく諮問機関の設置などである。デジタルID法に添付された修正案（Transitional and Consequential Amendments）は、この修正案に基づき制定される法令を基に、現在認証を受けAGDIS参加しているデジタルIDプロバイダー企業が新たな制度に移行する際の手続について規定する。

≪資料：2024年デジタルID法概要の邦訳（仮訳）≫

2024年デジタルID法は、各章ごとに、その章の建て付け（概要）を説明する規定を置いている。そこで、[資料]として、各章の概要を邦訳（仮訳）しておく。

【表33】資料：2024年デジタルID法概要の邦訳（仮訳）

第1章（総則）

第4条（第1章の概要）

本法は、デジタルIDサービスを提供する機関（entity）に対する認証制度を確立する。デジタルID規制官［連邦競争・消費者委員会（Australian Competition and Consumer Commission）］は、申請に基づき、一定の種類の機関を、認証された属性サービスプロバイダー、認証されたIDエクスチェンジプロバイダー、認証されたIDサービスプロバイダー、または、認証規則に規定する種類のサービスを提供するもしくは提供を予定している機関を、認証するものとする。

認証された機関は、認証されたサービスを提供する場合、プライバシー保護措置を遵守しなけれ

ばならない。これらの保護措置は、1988 年連邦プライバシー法に規定する保護措置に加重する形を取る。認証された機関は、プライバシー保護措置に違反した場合には、民事制裁の対象となる。

デジタル ID 規制官は、連邦政府デジタル ID システム（AGDIS=Australian Government Digital ID System）を監督しかつ維持する。一定の種類の認証された機関は、デジタル ID 規制官に対し、このシステムへの参加を申請できる。加えて、一定の種類の信頼できる当事者も、このシステムへの参加承認を求めて申請をすることができる。信頼できる当事者は、承認を得ると、参加する信頼できる当事者（participating relying parties）と呼ばれる。システム管理者（System Administrator）は、連邦政府デジタル ID システム（AGDIS）に参加する機関を支援し、かつ、連邦政府デジタル ID システム（AGDIS）に利用を管理するなどの職責を担う。

デジタル ID データスタンダード担当官（Digital ID Data Standards Chair）は、連邦政府デジタル ID システム（AGDIS）に参加する機関の技術的統合要件を含む、さまざまな事項について、認証規則（Accreditation Rules）またはデジタル ID 規則（Digital ID Rules）、認証に関する技術、データもしくはデザインのスタンダードにより求められる場合には、デジタル ID データスタンダードを作成する。

デジタル ID 規則は、認証された機関や参加する信頼できる当事者が使用するまたは使用が義務づけられるマーク、シンボル、ロゴ、デザイン（以下「デジタル ID トラストマーク」という。）を設定するものとする。

デジタル ID 規制官は、デジタル ID 認証機関登録簿（Digital ID Accredited Entities Register）や連邦政府デジタル ID システム登録簿（AGDIS Register）を創設しかつ維持しなければならない。

デジタル ID 規制官およびインフォメーションコミッショナーは、認証された機関その他の機関に対する執行行為を行う。デジタル ID 規制官は、連邦政府デジタル ID システム（AGDIS）での認証や参加に関する指示を与える、または、機関に対して法令遵守評価をするように求めるまたは情報もしくは資料を提出するように求めることができる。加えて、システム管理者は、連邦政府デジタル ID システム登録簿（AGDIS Register）への参加に関して機関に対して指示を与え、かつ、機関に対して情報または資料を提供するように求めることができる。

連邦政府デジタル ID システム（AGDIS）への参加が承認されたかつて認証された機関または現在認証されている機関は、記録保存義務を負い、かつ、当該機関が所有もしくは占有する情報を破棄または非識別化（de-identity）を求められる。機関は、本法のもとで受けた処分の本案について不服審査請求できる。

第 2 章（認証）

第 13 条第 2 章の概要）

デジタル ID 規制官は、申請に基づき、一定の種類の機関を、認証された属性サービスプロバイダー、認証された ID エクスチェンジプロバイダー、認証された ID サービスプロバイダー、または、認証規則に規定する種類のサービスを提供するもしくは提供を予定している機関を、認証するものとする。機関は、認証を受けるには要件を充たすように求められる。課させる要件は、本法によるものと、デジタル ID 規則（Digital ID Rules）または認証規則（Accreditation Rules）によるものがある。要件は、認証された機関が提供するサービスに関するもの、サービスの提供方法、および機関が収集または開示することが認められる個人の限定された属性の種類などについてである。

機関の認証に関してデジタル ID 規制官が課す要件およびその機関の認証自体が、変更または取消の対象となる。また、認証は停止の対象となる。所管大臣は、安全上の理由があり、必要と思われる場合に、デジタル ID 規制官に対して指示することができる。デジタル ID 規制官はその指示に従わなければならない。

認証された機関は、個人のデジタル ID について停止の求めがあった場合、停止しなければならず、かつ、認証されたサービスのアクセシビリティ（accessibility）およびユーザビリティ（usability）の要件を遵守しなければならない。

第 3 章（プライバシー）

第 32 条（第 3 章の概要）

認証された機関は、認証されたサービスを提供する場合、プライバシー保護措置を順守しなければならない。これらの保護措置は、1988 年連邦プライバシー法に規定する保護措置に加重する形を取る。

認証された機関は、政治的見解または人種的起源のような個人の属性の収集をすることによりプライバシー保護措置に違反した場合には、民事制裁の対象となる。個人の生体認証情報の収集、利用または開示に関する制限があり、かつ、行動のオンライン追跡のためにデータプロファイリングは禁止される。

第 4 章（連邦政府デジタル ID システム（AGDIS））

第 57 条（第 4 章の概要）

連邦政府デジタル ID システム（AGDIS）は、デジタル ID 規制官に監督されかつ維持される。連邦政府デジタル ID システム（AGDIS）に参加するには、機関は、認証された機関または信頼できる当事者でありかつデジタル ID 規制官から

AGDIS への参加の承認を得ていることなど一定の基準を充たさなければならない。

一定の種類の認証された機関および信頼できる当事者のみがデジタル ID 規制官に参加申請ができ、かつ、デジタル ID 規制官の承認を得るには、特定された基準を充たさなければならない。信頼できる当事者は、承認を得た場合には、参加する信頼できる当事者（participating relying parties）と呼ばれる。

機関は、連邦政府デジタル ID システム（AGDIS）に参加する承認を得るには要件を充たすように求められる。課させる要件は、本法によるものと、デジタル ID 規制官またはデジタル ID 規則（Digital ID Rules）によるものがある。要件は、機関が収集もしくは開示が認められる、または禁止される個人の属性の種類にかかわることなどである。

デジタル ID 規制官が機関の参加申請承認にあたり課す要件およびその機関自体の承認にかかる要件は、変更または取消の対象となる。また、承認は停止の対象になる。

所管大臣は、安全上の理由があり、必要と思われる場合に、連邦政府デジタル ID システム（AGDIS）への機関の参加承認に関してデジタル ID 規制官に対して指示することができる。デジタル ID 規制官はその指示に従わなければならない。

参加する信頼できる当事者は、サービスの提供もしくはサービスへのアクセスの条件として、個人に対してデジタル ID の装備または利用を求めてはならない。ただし、当該信頼できる当事者がデジタル ID 規制官から適用除外とする旨の承認を受けている場合などは別である。

デジタル ID 規則には、次に関する規定を置くものとする。

第 a 項　連邦政府デジタル ID システム（AGDIS）に関して生じたまたは合理的に生じたと推認される出来事を通知かつ管理すること。

第 b 項　相互運用性（interoperability）の関する要件

第 c 項　連邦政府デジタル ID システム（AGDIS）内で提供される認証された機関の認証サービスに関して生じる出来事にかかる救済枠組み

連邦政府デジタル ID システム（AGDIS）に参加する機関の間で拘束力のある制定法上の契約を締結するものとする。当該契約の当事者となる機関は、その制定法上の契約違反の結果として損害または損失を被ったもしくは被る怖れがある場合には、連邦巡回・家庭裁判所（第 2 部）に訴えることができる。

第 5 章（デジタル ID 規制官）

第 89 条（第 5 章の概要）

デジタル ID 規制官は、連邦競争・消費者委員会（Australian Competition and Consumer Commission）が担う。デジタル ID 規制官は、本法の遵守の推進や本法に関するプライバシー事項についてインフォメーションコミッショナーに諮問することなどの義務を行う。

第 6 章（システム管理者）

第 93 条（第 6 章の概要）

システム管理者は、連邦政府デジタル ID システム（AGDIS）に参加する機関を支援することや連邦政府デジタル ID システム（AGDIS）のアベイラビリティ（availability）を管理することなど職務を担う。

所管大臣は、システム管理者の職務の遂行または権限行使に関してシステム管理者に対して一般的な指示をすることができる。

第 7 章（デジタル ID データスタンダード）

第 98 条（第 7 章の概要）

デジタル ID データスタンダード担当官（Digital ID Data Standards Chair）は、連邦政府デジタル ID データスタンダードの技術的統合要件を含む、さまざまな事項について、認証規則またはデジタル ID 規則、認証に関する技術、データもしくはデザインのスタンダードにより求められる場合には、デジタル ID データスタンダードを作成する。

デジタル ID データスタンダードの制定、修正または廃止に先立ち、デジタル ID データスタンダード担当官は所管大臣等に諮問し、パブリックコメントを徴収しなければならない。

所管大臣は、デジタル ID データスタンダード担当官に対して担当官の職務や権限行使に関して一般的な指示を出すことができる。

第 8 章（トラストマークおよび登録簿）

第 116 条（第 8 章の概要）

デジタル ID 規則は、認証された機関や参加する信頼できる当事者が使用するまたは使用が義務づけられるマーク、シンボル、ロゴ、デザイン（以下「デジタル ID トラストマーク」という。）を設定するものとする。

機関は、次の場合に、民事制裁を受ける。

第 a 号　機関が、デジタル ID トラストマークを使用し、かつ、デジタル ID 規則がその機関に使用を認めていない場合

第 b 号　機関が、デジタル ID 規則に定めるところに従いデジタル ID トラストマークを掲示するように求めれているのにもかかわらずそれに従っていない場合

デジタル ID 規制官は、デジタル ID 認証機関登録簿（Digital ID Accredited Entities Register）を創設し、かつ、そこに過去に認証された機関ま

たは認証される機関の登録を維持しなければならない。

デジタル ID 規制官は、連邦政府デジタル ID システム登録簿（AGDIS Register）を創設し、かつ、連邦政府デジタル ID システムに参加を承認された機関の登録を維持しなければならない。

第 9 章（管理）
第 122 条（第 9 章の概要）

デジタル ID 規制官やインフォメーションコミッショナーは、認証された機関その他の機関が民事制裁規定に違反する場合、権利侵害通告の発出、裁判所に金銭罰命令の発出もしくは差止命令などを求めるなどして、当該機関に対して執行行為を取ることができる。

デジタル ID 規制官は、認証および連邦政府デジタル ID システム（AGDIS）への参加に関係する機関に指示することができる。加えて、指示は、連邦政府デジタル ID システム（AGDIS）の清廉性または遂行を確保するために発出することができる。こうした指示は、システム管理者にも発出することができる。

デジタル ID 規制官は、認証された機関が本法に違反しているまたは違反するかもしれないと合理的に推認できる場合に、当該機関に改善の指示を発出するまたは認証を停止することができる。

デジタル ID 規制官は、認証された機関に関し、当該機関が本法を遵守しているかどうかを判断する、または、サイバー安全事件もしくはデジタル ID 詐欺事件が発生するまたは発生したと推認できると判断する場合などに、当該機関に対して法令遵守評価（compliance assessment）を実施するように求めることができる。

デジタル ID 規制官またはシステム管理者は、一定に状況のもとでは、機関に対して情報の提供または資料の提出を求めることができる。

認証された機関で連邦政府デジタル ID システム（AGDIS）への参加の承認を得たまたは得ている場合、当該機関は、記録保存義務を負い、かつ、当該機関が所有または占有する一定の情報を破棄または非識別化するように求められる。

機関は、本法のもとで行われた処分の本案につき不服申立てすることができる。

本法のもとでの申請をするには、一定の条件を充たさなければならない。

デジタル ID 規則に、本法のもとで申請する者に対してデジタル ID 規制官等が課す手数料に関する規定を置くことができる。

認証された機関が連邦政府デジタル ID システム（AGDIS）に関して提供される認証サービスにかかる手数料を課すには、拘束力のあるデジタル ID 規則によらなければならない。

第 10 章（雑則）
第 149 条（第 10 章の概要）

所管大臣は、本法のもとで生じる問題に関し、次の者に助言するために諮問委員会（advisory committee）を置くことができる。

第 a 号　所管大臣
第 b 号　長官
第 c 号　デジタル ID データスタンダード担当官（Digital ID Data Standards Chair）

本法のもとで職務の遂行または権限の行使の過程もしくは目的で情報を入手し、かつその情報を利用または開示した場合、その者は処罰される。ただし、いくつかの適用除外がある。

本章は、次のような事務的性格の事項についても規定する。

第 a 号　デジタル ID 規制官、インフォメーションコミッショナー、法執行機関、強制執行機関および連邦警察（AFP=Australian Federal Police）担当大臣、および、
第 b 号　委任（delegations）
第 c 号　規則制定権限（rule-making powers）

■官製デジタル ID と民間デジタル ID との互換性の課題

（Q）最適なデジタル ID は、安心・安全で人権にもやさしいツールで、しかも、デジタル ID の多様性が保障されないといけないと思うが、オーストラリアのデジタル ID 法のスタンスはどうなのか？

（A）わが国では、官のデジタル ID（JPKI）と民間のデジタル ID とを分断し、官のデジタル ID である JPKI を民間にも拡大して利用させようという政策である。官製のデジタル ID（JPKI）サービス［法令等で本人確認について定めのあるサービス］と民間のデジタル ID サービス［法令等で本人確認について定めのないサービス］との相互利用（互換性）を促進しようとしていない。言い方をかえると、「NHK ファーストで、民放は別物」と見るような考え方である［記事「民間事業者向けデジタル本人確認ガイドライン」CNN ニューズ 113 号 47 頁以下（CNN-113.pdf（pij-web.net）参照］。

わが国でのこのようなデジタル ID の法的分類

◆日本でのデジタル ID の法的分類

①法令等で本人確認について定めのあるサービス
②法令等で本人確認について定めのないサービス

は、〝官民のデジタル ID プロバイダーやユーザーの分断（divide）〟、〝官尊民卑〟につながっている。官製デジタル ID の優越的地位を認めるのは、民主主義や人権が後退し、官民のデジタル ID の権威主義的な運用が心配される。ユーザー（市民・納税者）ファーストの信頼できるデジタル ID の確立には、流れを変えないといけない。官民のデジタル ID プロバイダーを同じ土俵で競わせて、最適なデジタル ID を採用しようという政策に変えないといけない。

わが国は、〝憲法には人権規定を置いているけれども、政府はこの憲法はどこか他の国の憲法でなはないか？〟といった感じの国情にある。こうした国柄もあってか、官製のデジタル ID（JKPI）のユーザーを使うのは市民・納税者の義務であるといったスタンスである。官製のデジタル ID（JKPI）のユーザーを〝権利主体〟と見る思考を欠いている。

この点、オーストラリアはどうなのであろうか？

オーストラリアも、連邦政府がさまざまな行政機関の Web サイトの接続ハブとなる「マイガブ／ myGov」という名前で電子政府ポータルサイトを構築している。市民・納税者（ユーザー）がそのポータルの紐づけされた各種行政機関にオンライン申請・申告でログインするには、官製のデジタル ID である myGovID を利用しないといけない。このことから、わが国のマイナポータルと似たデザインである。

オーストラリアは、イギリスの植民地であったこともあり、ヨーロッパ諸国の影響が強い国である。ただ、イギリスの労働者階級が大挙して入植してきた歴史もあり、イギリスのような「階級社会（class society）」ではない。無尽蔵にある天然資源などを輸出し、福祉国家財政を支える、また政治的には公務員が多くして雇用を支えるような社民主義的思考が強い。以前は、高等教育機関は官立だけで、私立大学はなかった。言いかえると、アメリカのような「民間ファースト」のような国情にはないが、私立大学も増え市場主義が浸透しつつあるといえる。わが国のような「官尊民卑」のような風土にはないものの、友人の研究者に聞いても、官製のデジタル ID である myGovID に対してはさほど違和感がないようである。これに対して、アメリカのデジタル ID 政策は、それぞれの行政機関が、Apple Wallet とか、id.me のような民間のデジタル ID プロバイダーが開発したデジタル ID を、公開入札で採用するという市場主義が基本である。このことから、アメリカでは、連邦が、国全体をカバーする電子政府（e-Gov）ポータルサイトを構築し、連邦や諸州の機関を紐づけ、官製のデジタル ID の利用を強制するような権威主義国家的な仕組みに賛同が得られる可能性は限りなく低い。

オーストラリアは、アメリカとは大きく異なり、かなり官依存の強い市民を抱える国である。アメリカのような「デジタル ID で市場競争をするのがベスト」という認識は弱い。

とはいっても、電子政府（e-Gov）プラット

コラム 9　アメリカの全米規模で信頼できるデジタル ID インフラ検討の動き

アメリカではいずれの分野でも市場主義が徹底されている。デジタル ID プロバイダー業務（サービス）についても、民間 IT 企業（vendor）が担うべきであるとする考えが支配的である。行政分野の Web サイトを含め、デジタル ID サービスは、ほぼ全面的に民間の IT 企業（デジタルプラットフォーマー）に依存する体制が続いている。「民間活力（private action）」を優先する資本主義の本場ならではの姿ともいえる。ただ、この結果、必ずしも、信頼できるデジタル ID 基盤（インフラ）が確立できていないとの声もある。

アメリカには、わが国のマイナポータルやオーストラリアのマイガブ／ myGovID ポータルのような官営の電子政府ポータル（e-Gov）がない。アメリカでもネット空間に連邦・州・地方団体が提供する各種行政サービス Web サイトのユーザーに利便性の高い接続ハブ（nodal hub）［ネットワーク接続拠点］となる電子政府（e-Gov）プラットフォーム／ポータルサイト／ Web ポータルを構築すべきである、という声はある。しかし、政府機関（官）がトータルにデジタル ID プロバイダー業務を行うことには、概して消極的である。中央集権的なデジタル「権威主義国家」につながりかねないという嫌悪感が強いからである。

アメリカ連邦議会では、これまで、幾度も、連邦電子政府ポータルサイト（e-Gov）を構築する提案や、全米をカバーするデジタル ID を導入する提案が消えてはまた現れるということを繰り返してきた。

とはいうものの、近年、少し違った動きも見られる。2020 年から世界的な感染爆発（パンデミック）にいたった新型コロナウイルス禍

（COVID-19 Crysis）が契機である。コロナ禍では、各地で外出禁止令が出され、民間のネットショッピングのみならず、福祉や公的給付についても各種行政ウエブサイトにログインしてへのオンライン申請・申告するケースが急増した。この背景には、連邦議会が急きょ、ケアーズ法（CARES Act=Coronavirus Aid, Relief, and Economic Security Act ／コロナウイルス支援・救済・経済安定法）を制定し、緊急の各種給付金支給を決めたこともある。ところが、スキャムメールを使った詐欺取引だけでなく、各種公的給付の不正受給もうなぎ登りとなった。2021 年の雇用（失業）保険金の不正受給額１つ取って見ても、約 360 億ドルにも達した（See, Greg Iacurci, "Scammers Have Taken $36 Billion in Fraudulent Unemployment Payments from American Workers," CNBC, January 5, 2021; Waldo Jaquith, "Americans Need a Digital Identity System, Stat!," 15 Community Development INNOVATION REVIEW (Aug. 19, 2021))。

不正受給の急増は、個人を一意に特定・本人確認できる全米で統一的に使える信頼できるデジタル ID インフラ（基盤）がないからではないか？オンラインの行政サービスには、的確な ID クレデンシャル【credentials: 正当なユーザーであることを証する、ユーザーネーム＋パスワード、ワンタイムパスワード、運転免許証や旅券のような行政機関が発行した証票その他の証拠など。「クレデンシャル（credential)」は、「資格証明書」、「資格証票」などの邦訳がある。】や ID 属性【attributes: 氏名・住所・生年月日・性別（基本４情報）など】に基づき、安心・安全にオンライン上で本人確認ができるデジタル ID インフラ確立が必須とする声が高まった。連邦省庁の役人からは、連邦や諸州・地方団体の行政当局が民間のデジタル ID プロバイダーに過度に依存すること（problems with privatized digital identity）に対する疑問も投げかけられた。加えて、研究者などからも、個人情報の漏洩やオンライン上のスキャム（詐欺）防止にも強い、安全かつ効率的・利便性の高いデジタル ID インフラがないことが、コロナ禍での多額の給付金不正受給クライシスにつながったとの指摘があった（See, Usman Ahmed, et al., "The U.S. Digital Identity Crisis," The Regulatory Review (Apr. 29, 2021))。

不正受給のひどさが市民の間でも話題になり、「なぜデジタル ID は重要なのか（Why Digital ID matters)」の認識が共有されはじめた。連邦省庁や研究者は、各個人のクレデンシャル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る本人の権利や義務を証明できる安心・安全なインフラ（基盤）確立プランを提唱している。いずれの提案にも共通するのは、非中央集権的な官民にわたる複数のサービス間で持ち歩き、共通して利用可能（Portability）な官民連携のデータセキュリティやプライバシー保護が完璧な建て付けのデジタル ID の確立である。1936 年に対面／オフライン用として導入された社会保障番号（SSN=Social Security Number）以外のツールを使った官民のオンライン取引で安心・安全な個人認証インフラの構築が目標とされている。

ただ、アメリカは、行政主導ではなく、政治主導の国である。わが国のような、行政が、「名ばかり審議会」などを濫設して政策を主導することを、政治が赦さない国情にある。どのような提案（政）を実現するにしろ、政治主導が必要になる。

連邦議会からも、デジタル ID 問題で機を見るに敏な動きがあり、全米で統一的に使えるさまざまなデジタル ID インフラ整備の提案が出てきている。

2020 年９月には、連邦議会に、民主・共和両党の議員から超党派の「2020 年デジタル ID 改善法（Improving Digital Identity Act of 2020)」（下院法案 8215 号）が、議会下院に提出された。次のような建て付けの法案である。

◆ 2020 年デジタル ID 改善法（案）の骨子

①行政（連邦・州・地方団体等）・民間分野で相互運用可能なデジタル ID の確立に向けて共同で検討を行うタスクフォース（作業部会）を創設すること。
②タスクフォースは、米国国立標準技術研究所（NIST-Institute of Standard and Technology）が作ったデジタル ID 基準やさまざまな現在使われている ID を点検し、運転免許証、旅券、出生証明書など含むデジタル ID クレデンシャルの統一化の検討を行うこと。
③連邦国土安全保障省（DHS）は、諸州が、米国国立標準技術研究所（NIST）のデジタル ID 基準に従ったデジタル ID 制度を確立する際の補助金プログラムを確立すること。

2020 年デジタル ID 改善法は、成立には至らなかった。しかし、翌 2021 年 6 月に、連邦議会上院に提出された「2021 年デジタル ID 改善法（Improving Digital Identity Act of 2021 ／上院法案 4528 号」が提出された。このデジタル ID 改善法（案）は、カーステン・シネマ上院議員（Senator Kyrsten Sinema ／アリゾナ州選出／当初民主党所属、現在無所属）が、連邦議会上院に提出した。次のような建て付けの法案である。

◆ 2021 年デジタル ID 改善法（案）の骨子

≪目的≫
連邦や諸州などが発行する運転免許証、電子旅券（e-Passports)、社会保障用認

証、出生証明書なども含む現行の対面用証票（credentials）のデジタル版を連邦・諸州の協力により開発推進することにより、対面用とオンライン（非対面用）のクレデンシャル［ユーザーネーム＋パスワード、ワンタイムパスワードその他の識別子（identifier)］の安全性を確保するため、連邦、諸州、地方団体などからの代表で構成されるタスクフォース（作業組織）を創設すること。

≪骨子≫

デジタル ID 改善法案の内容骨子は、次のとおりである。

①タスクフォース／作業部会の創設（Task Force Creation）

アメリカでのデジタル ID 問題を点検する「デジタル ID 改善タスクフォース（Improving Digital Identity Task Force）（作業部会）を、大統領府（EOP= the Executive Office of the President）に設置する。タスクフォースは、国土安全保障省（DHS）長官、財務省長官など連邦政府の高官、諸州や地方団体出身者（6人)、非政府出身の専門家（5 人）などの委員からなる。

座長（Director）は、必要に応じてワーキンググループ（WG）を組織・開催できる。タスクフォースは、本法施行から 3 年以内に作業を終了する。本法施行から 180 日以内に中間報告書を作成し、終了前 6 か月以内に勧告を含む最終報告書を作成し、大統領および議会の所管の委員会に報告をし、一般に公開する。

②プライバシーと安全の確保（Privacy and Security）

タスクフォースは、プライバシーと安全（privacy and security）を保護する方法に焦点をあてて検討する。

③相互運用性（Interoperability）

技術の進歩の沿う形で絶え間ない検討を行い、移動（モバイル対応）方式の本人確認とデジタル ID の仕組みとの相互運用性を確かなものにすること。

④不正防止（Fraud Prevention）

連邦議会の政府検査院（GAO）が、デジタル ID の利用拡大の結果、なりすまし犯罪からの消費者保護や不正申請を含む詐欺の防止によりどれくらいの被害減少につながるのかなどを評価した報告書を連邦議会に提出すること。

2021 年（下院法案 4258 号）と同じ内容の法案は、2022 年（上院法案 4528 号)、2023 年（上院法案 844 号）にも連邦議会に提出されている。

＊　　＊　　＊

連邦議会に提出されたデジタル ID 改善法（案）は、連邦や州の行政トップが集まり、官民にわたる複数のサービス間で持ち歩き、共通して利用可能（Portability）な官民連携のデータセキュリティやプライバシー保護が完璧なデジタル ID の仕組みの確立に向けて検討を進めようというのが狙いである。言いかえると、連邦電子政府ポータルサイト（e-Gov）にあらゆる官民の Web サイトを紐づけする中央集権的なデジタル ID インフラ（接続ハブ）の構築を目指したものではない。アメリカでは、国民のプライバシーをトータルに国家が管理する「権威主義国家」、「役人が主役」の政体につながりかねない提案は、広く受け容れられる可能性は少ない。

デジタル ID 改善法（案）は、あくまでも官民連携で個人のプライバシーを保護し、安心・安全かつ信頼できるデジタル ID（Digital Identity）インフラ確立の〝検討〟を求めるだけの内容である。安心・安全にオンライン上で本人確認ができる具体的なデジタル ID インフラのデザインなどはまったく盛り込まれていない。

アメリカでは、政治家が、わが国のマイナンバー制度のような、対面用の国民総背番号制＋官製の中央集権的なデジタル ID インフラ構築を推進する、あるいは市場主義や「民間活力（private action)」を否定するような主張をすることは、政治生命を危うくする。連邦や諸州・地方団体の行政当局がデジタル〝ID プロバイダー業務を過度の民間に依存していることが諸悪の根源だ！〟などと唱え、〝官による国民のデータの直接管理も必要！〟に大きく踏み込むことはご法度である。だからと行って、デジタル ID 改善法（案）のような、腑抜けな建て付けの議員立法には大きな疑問符がつく。民間抜きで、連邦や州の行政トップが集まってデジタル ID のあり方を検討しても、最適な結論や幅広い支持は得られないのではないか。

＊　　＊　　＊

ちなみに、現在、アメリカでは、各行政機関は、ユーザーがオンライン申請・申告でそれぞれの Web サイトにログインする際のデジタル ID として、民間デジタル ID プロバイダー（ベンダー）が開発したデジタル ID を、入札などで公共調達して使っている。❶アメリカ大手 IT のレキシスネキシス（LexisNexis）社の Login.Gov ／ログイン・ドット・ガブ、❷アイデー・ドット・ミー（ID.me）社の ID.me ／アイデー・ドット・ミー、❸アップル社の Apple Wallet ／アップルワオーレットなどのデジタル ID が採用されている。これらはいずれも、モバイル、スマートデバイス（スマホやタブレット）対応で、IC カードを使わないデジタル ID である。わが国のように、官製のデジタル ID（JPKI）がバッコし、民間のデジタル ID が居場所を失い隅に追いやられるのは、イノベーションを阻害しかねないことを肝に銘じておくべきである［詳しくは、「Q&A: デジタル ID とは何か！」CNN ニューズ 113 号 CNN-113.pdf（pij-web.net)］。

フォーム向け個人用デジタルID市場に、一定の基準を満たした民間IT事業者（an accredited private sector provider）を参入させようとする動きがないわけではない。つまり、官製のmyGovIDアプリなどに加え、民間のデジタルIDでも、電子政府（e-Gov）プラットフォームにアクセス・ログインできるようにしていこうという動きがないわけではない。2024年デジタルID法は、ユーザーが安心・安全にオンライン上で本人確認ができる信頼できるデジタルIDの枠組み（TDIF=Trusted Digital Identity Framework）」を構築しようということで、消費者保護の視点から制定された。この法律は、デジタルIDに関する認証制度（accreditation scheme）を構築し、官民のデジタルIDプロバイダー（public and private sector digital ID providers）の任意の参加を促し、安心・安全確保の観点から〝質管理〟をしようというものだ。段階的ではあるが、官製のデジタルID（myGovID）の民間利用の拡大に加え民間のデジタルIDの官（行政）Webサイトでの利用拡大も視野に入れている。つまり、認証された官製のデジタルIDと認証された民間のデジタルIDの相互利用（互換性）を拡大する政策に舵を切ったように見える。

オーストラリアの2024年デジタルID法は、一種の官民のデジタルID市場つくりのための法律ともいえる。

オーストラリアは、わが国とは異なり、個人が行政機関へのオンライン申請・申告の際に民間のデジタルIDを使うのは絶対禁止という閉鎖的なデジタルID政策を改善する方向を目指しているように見える。

驚くことに、わが国では、東京都渋谷区が住民票などのオンライン申請に民間のデジタルIDを使おうとしたら、総務省は、官製のデジタルID（JPKI）以外はご法度だとして、法令まで改正してストップをかけた。

このストップ措置を司法（東京地裁）までがお墨付きを与えた。行政追従の消極司法は市場主義感覚ゼロである。加えて、役人依存の政治は、権威主義国家のデジタルID政策に異論を唱える見識を持ち合わせていない［「デジタルID（デジタル本人確認）とマイナ保険証」CNNニューズ115号11頁【コラム】CNN-115.pdf（pij-web.net）参照］。

■むすびにかえて
～人権弾圧用の凶器にもなる官製デジタルID

（Q）わが国でも、オーストラリアと同様に、官製のデジタルIDだけでなく、信頼できる水準のものであれば民間のデジタルIDも、オンラインでの行政申請・申告でも並行して使えるようにすべきではないか？

（A）デジタルIDは、機微情報（sensitive information）との紐づけが伴う。このため、プライバシーや人権の侵害、デジタルIDを使ったデータ監視社会つくり［データ収容所列島化］などへの心配が絶えない。とりわけ、官製の共通デジタルID、単一IDプロバイダーへの過度の依存は、権威主義国家つくりのツールになる可能性がある。中国が最たる例だ。

官民のさまざまなデジタルIDが互換して利用でき、それにより市民の自由や権利を守れる民主主義国家に最適なデジタルID政策が不可欠である。1つの官製のデジタルIDに依存するのは、危険だ。特定のIDプロバイダーへの依存度を下げるためには、官民のデジタルプロバイダー間での競争が状態をつくる必要がある。

連邦政府は久しく、オーストラリアにおける「信頼できるデジタルIDの枠組み（TDIF=Trusted Digital Identity Framework）」を確立するための努力を重ねてきた。しかし、データセキュリティを確保し、個人データやプライバシーを保護するための基本法制が整備されていなかった。そこで、今般のデジタルID法（Digital ID Act 2024）では、官民の各種デジタルIDを評価・認証する仕組みをつくった。

ただ、国が官民の各種デジタルIDを評価・認証しお墨付きを与える仕組みには常に危うさが伴う。官がお墨付きを与える仕組みは、そもそも西欧型の民主政体が維持できてはじめてこうした仕組みはうまく機能することを忘れてはならない。独裁体制の国、あるいは国が分断している政情にある場合、デジタルIDは、敵対勢力の抑圧のツールに使われる危険性が避けられない。

オーストラリアの2024年デジタルID法には、人権団体や右派政党などから批判の声があがった。「官製のデジタルIDであるmyGovIDを権威主義国家の電子監視ツールとして合法化し、実質的な強制利用につながるのではないか？」、「中国政府が採用する社会信用システム（social credit system）、つまり政府が収集したデータに基づい

て、全国民をランク付けし、各人の『信用度』をスコア化する AI を駆使したデジタル ID システム導入につながるのではないか？」などだ［Labor’s Digital ID Bill Forced Through Senate Without Debate - The Daily Declaration ／ Digital ID laws - Pauline Hanson’s One Nation］。

人権団体「ヒューマン・ライツ・ウオッチ／Human Rights Watch」は、次のような衝撃的な報告をしている。

【表 34】アフガンでタリバンの手に落ち、凶器と化したデジタル ID システム

アメリカのよるアフガニスタンでのタリバン政権の壊滅、そして占領が続いた。この当時、西側諸国は、アフガン国内にさまざまな生体認証式デジタル ID システムを持ち込んだ。日本もアフガン支援に参加、警察官の訓練などを狙いに、デジタル ID システムを使っていた。バイデン政権の政策変更により、米軍はアフガンから急きょ撤収することになった。米軍や西側機関は、撤収時に、これらのデジタル ID システムは完全破壊しきれなかった。このため、多くはタリバン政権の手に落ちた。タリバン政権は、これらのデジタル ID システムを旧政権や占領軍への協力者の追跡・発見に活用し、闇の処刑などが多発している。こうしたアフガンの実情からもわかるように、整然と個人を識別管理する生体認証式デジタル ID システムは、使い方によっては、人権クライシス（危機）を拡大する危険な凶器になることを教えてくれる［See, New Evidence that Biometric Data Systems Imperil Afghans：Taliban Now Control Systems with Sensitive Personal Information (March 30, 2022) New Evidence that Biometric Data Systems Imperil Afghans | Human Rights Watch (hrw.org)］。

デジタル ID システムのあり方は、まさに、政変、占領など「国家・国民安全保障」や「持続的な民主国家体制の確保」など危機管理の視点も織り込んで考えないといけない。平和ぼけした能天気な政策は許されない。単一の官製の生体認証式デジタル ID システムを整然とした形で利活用を官民にエスカレートさせることは、状況によっては取り返しのつかない危険が伴うことを理解しないといけない。官製（官営）のデジタル ID システムで、民主主義が後退し、人権侵害が当り前の権威主義国家が世界中に蔓延することは誰も望まない。

【資料】2024 年 9 月 13 日 名古屋高裁判決の要旨

＜県警の行為は違憲・違法＞　※記事は 6 頁参照

憲法は、個人情報の収集および保有がみだりにされない自由も保障していると解すべきである。これらが侵害された場合に、損害賠償請求ができるのはもちろんのこと、保有している情報の抹消なども具体的な権利として認められる。

県警による個人情報の取得、保有および利用は、著しく社会的相当性を欠き、恣意的な運用が行われていた。県はこれを改めようとはせず、一般的、抽象的な公共の安全と秩序維持を唱えて擁護しようとするばかりである。警察組織内部での自浄作用は全く機能していない。

県は大規模かつ無秩序な「大衆運動」が展開する危険性を秘めているなどと主張する。加えて、県警が行った情報収集活動にも必要性は認められるなどと主張する。しかし、市民運動やその萌芽の段階にあるものを際限なく危険視して情報収集し、監視を続けることが憲法による集会、結社、表現の自由の保障に反することは明らかで失当というほかない。

原告らが行ってきたこれまでの活動を見ても、何ら犯罪性や、公共の安全や秩序に対する危険性は認められない。原告らは適法かつ平穏な方法によって活動していると認められる。風力発電事業に対する反対運動が広がったとしても、公共の安全や秩序の維持が損なわれる可能性は全くうかがわれない。

県の主張は市民運動一般に対する誤った理解に基づく独自の見解と言わざるを得ない。原告らのメーリングリストの内容を県警や中部電力子会社シーテックが入手することは、メーリングリストがそこに含まれる限られた者の通信手段であり、外部に公開されていないことからすると、憲法の保障する通信の秘密を害する行為であると認められる。情報を入手する手段において違憲、違法と言わざるを得ない。

原告らはいずれも県警から違法に個人情報を収集、保有された上、シーテックに違法かつ意図的に個人情報を提供されたことで多大な精神的苦痛を被った。原告に支払われるべき慰謝料額は請求額である１００万円を下らず、弁護士費用についても１０万円を下らない。

＜結論＞

県警の収集、提供行為の違法性について１審判決を一部変更し、原告らの損害賠償請求をいずれも請求通り認容し、県の控訴を棄却する。提供情報に基づいて事業者が作成した議事録の記載から特定できる情報の抹消について、県に対する請求を認容し、国に対する請求を棄却する。

≪刑事司法にＡＩ判定が活用されるようになる？≫
AI 刑事手続とプライバシー・人権保護（3）

― アルゴリズム（情報処理手順）の判断による刑事手続の透明性・公平性 ―

コメンテーター　清 水 晴 生 （白鷗大学教授）

【内容目次】

4　AI 刑事手続の各局面（承前）

（13）　AI 刑事手続と量刑

被告人による犯罪事実の存在が認定された後、刑の量定においては現在、裁判所の過去の量刑データが参照されていることはよく知られている。罪種、被害の程度、共犯者の有無、前科の有無等を入力して結果が出力されると思われる。どのような要素を入力するかによって結果が変わってくることから、どのような要素を入力内容に含めて裁判員に参照させるかといったことも、裁判員裁判の前の公判前整理手続において争われると聞く。

同じように、その量刑データをディープラーニングさせた AI に個別の判断を任せる場合でも、いかなるプロンプト（入力内容）を用いるかが問題となる。そうすると、結局はどういうプロンプトが入力されるべきかも AI が判断しなければならないことになり、そのためにはさらに事案の争点、証拠調べの必要性の判断なども AI が判断すべきことになる。AI にいろいろやらせることはできても、それをどこまで任せるのかの判断も必要になる。

そしてそれ以前にやはり、刑事手続 AI のディープラーニングにおいてどういった要素（特徴量。feature value）を用いるべきかについても別途問題になる。これもさらに AI に設計させることもできようが、そうすると完全に AI による司法の支配ということになり、憲法を書き換えなければならない。

現実的には現在の量刑データのシステムに加えて、例えば裁判員裁判の効率的運営の参考資料として、同種事案においてどの程度の証人尋問がなされたかといったデータを示させるといったことは考えられる。

以上のように量刑の判断とは、いってみれば何を・どこまでを審判対象とし、どのような証拠を採用して取り調べるかといった事実認定を踏まえた結論だ。一見、量刑こそ過去の事例との間の相対評価により結論を導き出せるとの意味で AI に適合しやすいように思えるが、よく考えてみると

その判断の前提となる事実認定と直結している以上、量刑だけを AI に判断させるというのはシステムとして難しさがある。

またビッグデータをディープラーニングさせた AI に被告人の再犯確率を予測させ、量刑上参考にするという利用方法も考えられる。確かに事案・罪種によって再犯可能性が高いといわれるものがあり、実際薬物犯罪などは再犯者が多い傾向にある。使用罪などは被害者なき犯罪ともいわれ、直接の被害者を認識しにくいところが再犯が抑止されない理由ともいえる。逆に性犯罪はいわれるほど再犯の多い犯罪ではないともいえる。性犯罪のかなりの部分が顔見知りの間で起こるものであることが、その理由とも考えられる。

しかしそのような全体的な傾向を踏まえることは裁判官でも難しくはない。これを超えて、犯人の性格、境遇・生い立ち、年齢や体格、人間関係などといった事情をプロンプトとして、どこまで確定的な再犯予測が可能か。このような未来予測はいくら AI でも簡単ではない。AI といっても所詮その設計や作成は人間が行うのであり、何が再犯の可能性を高め、どんな要素がそれを下げるかの考慮も結局人間の考えを踏まえざるをえない。AI がそれ以外の要素を発見するかもしれないが、それを了解し採用できるかどうかも人間にかかっている。

同じ環境下に置かれたままの者による再犯予測など、そもそも AI に任せるまでもない。結局量刑における再犯予測を AI に委ねたとしても、その根拠が不明（ブラックボックス）な厳罰化に至ったりすることにもなりかねない。ならばむしろ、いかなる出口支援、いかなる更生保護がその受刑者の更生にとって有用か、そのためのリソースがどこにどのようにあるかといった内容こそを AI に学ばせまた判断させることの方が、AI の使い方として理に適いずっと意味がある。

（14） AI 刑事手続とダイバージョン

ダイバージョン（diversion ディバージョン）とは、わき道・分岐という意味で、ここでは刑事処分の多様性・多様化のことだ。最も基本的な刑事処分として刑罰がある。しかし実際には反則切符のような行政罰で代えることも行われている。広い意味では示談による解決なども含む。いわゆる ADR（裁判外紛争処理。Alternative Dispute Resolution）もダイバージョンの代表的なものの一つ。刑事手続特有のダイバージョンとしては、警察限りでの微罪処分や起訴猶予（不起訴処分のうち、罪体はあるが起訴価値に乏しい場合）もこれにあたる。他方で少年法に基づく少年審判や医療観察法による強制入院・通院決定も、当事者の属性に基づくダイバージョン処分といえる。

これらは限りある刑事司法リソースの効率的運用や、必要以上に重い刑罰を科したり前科をつけることなしに、本人の変化や自覚、あるいは社会的リソース（家族や会社など）も最大限活用して処罰と同等以上の実質を上げることを目的に用いられる。

日本は受刑者が年々減り、各地の刑務所が閉鎖されてきている。それでもなお有効性の検証もないまま刑事施設に収容し、大した手当もなく釈放して再犯が繰り返され、受刑者の 5 割前後が再犯者というのが常態だ。ようやく 2025 年 6 月 1 日から懲役・禁錮を再編統合した拘禁刑が施行される。拘禁刑では「改善更生を図るため、必要な作業を行わせ、又は必要な指導を行うことができる」（刑法 12 条 3 項）とされ、より積極的に、計画的かつ組織的な再犯予防の取り組みが刑事施設の中で行われることになっている。

このように犯罪の処理といっても様々な出口がありうる。当事者の性格・環境、病態、前科・前歴と罪種、年齢や事案の特性、受け入れる側の社会内リソースの多寡や種類などを特徴量とした AI により、具体的事案に最適なダイバージョン処理の判断を導き出すことは実現可能だ。

それは例えば起訴・不起訴の判断や、裁判の量刑とも結びついてくるという意味では、刑事裁判手続の一部をなす。ただダイバージョンを積極的に活用する方向でのハイパーパラメータチューニングがなされる限りでは、より軽い処分を導くという点で不利益を課すことには原則ならないといえる。もっとも罰金刑や短期拘禁刑の代わりに長期の強制入院処分にするというような例外的な場合もある。また少年法上の保護観察とするか 20 歳になるのを待って罰金刑とするかなど、一概にはいえない場合もある。

人口も受刑者も減る中、法務省の余剰リソースはより効果的な再犯予防・再社会化へと向けられつつある。ただし刑罰を超えるダイバージョン処分が過剰な予防拘禁・保安処分化する恐れもある。ダイバージョン処分のバリエー

ションやそれぞれの中身について詳しくない裁判官の判断を補いつつ、その処分内容の適正さが客観的に検証・担保される形でなら、AI は刑事手続におけるダイバージョンの進展に資するところがありえよう。

（15） AI 刑事手続と更生プログラム

これまでの懲役・禁錮という刑罰は、犯罪者を一旦社会から隔離し、犯した罪に応じた不自由・不利益を正義として科し、その不自由・不利益を味わったことで再犯を忌避させ予防を期すという素朴な発想による。更生緊急保護といった出所後のサポートもあるにはあったが期間も限られ、最近になりようやく社会復帰・再統合による再犯率低下を目指す入口支援・出口支援が本格的に検討・試行されるようになってきた。それは特に、これまでなかなか有機的な連係を取れてこなかった司法と福祉の協働を必要とし、地域社会内にどのような福祉リソースがあり、それを活用できるかを司法特に検察が把握し、これを積極的に活用できるかにかかっている。

他方で施設内処遇に関しては、各地に開設された官民共同運営に係る PFI 刑務所を始めとして、新たな試みもなされてきたものの、それは一部にとどまってきた。薬物事犯に関しても各行刑施設内で限定的に依存回復のための取り組みはなされてきたものの十分ではなく、2020 年になって札幌市東区の札幌刑務支所に「女子依存症回復支援センター」が開設され、いっそう本格的な取り組みも始められつつある。

本来個々人に見合った更生プログラムの作成には、経験を積んだ精神保健福祉士ほかソーシャルワーカーの関与が必須だ。過去の経歴の把握・分析を踏まえて、本人や関係者からも十分を聞き取りをしてその特徴・病態を把握した上で、実績のあるプログラムと最新のプログラムの双方をうまく勘案し、適切な期間の実施が計画されなければならない。またその実施においても、適宜の変更を加えつつ、粘り強くサポートを続けることが必要だ。

そう考えると、これらの取り組みに AI によるサポートを加えるとしても、それはおそらくかなり限られた、補完的なものにとどまることになる。同じ依存症患者といってもその依存に至る背景や、依存の中身・程度も様々だ。それに加え各自の性格・環境も様々であり、それらは汲み尽くせない部分もあるから、単純に AI に答えを求めそれを信頼すれば良いとはならない。

他方、全国の刑事施設全てで十分な専門家（社会福祉士などの福祉専門官）の確保が困難なことも想像される。そうした場合に、従来からあるアセスメントツールに加え（あるいはそれらと統合して）、刑務官らによる更生プログラム実施を補うという形では、むしろ経験豊かな専門家のエッセンスが相当程度適切にアルゴリズム化された AI の役立つ余地がありうる。

（16） AI 刑事手続と仮釈放

刑法の厳罰化の流れの中、早期に仮釈放で出てくることへの感情的な反発が広がり、再犯との関係の検証もろくにされないまま、自由刑の長期化、仮釈放の厳格化が進められた。実際には仮釈放が認められる方が受刑態度が良いはずだ。もちろん受刑態度の良さと再犯率との相関も明らかではない。しかし、真面目にやってもやらなくても同じように出所するなら、真面目に取り組むモチベーションもないことになる。その意味において仮釈放の運用は行刑の意味・効果を高めうる。

確かに刑期は犯罪の重さに比例する（応報刑主義）が、刑罰の中身に再犯予防の意味を期待する（特別予防論）以上、漫然と受刑者を社会から長く隔絶することで満足することはできない。長期の拘禁は当然、再社会化をむしろ阻害する副作用を伴う。

しかももし仮釈放がなければ、満期出所した者はその時点から強制力のある関わりとは無縁になり、自ら求めない限り、更生保護や NPO との繋がりの用意もない。家族も前科者とは関わりたくないとなると、社会の中でまた一から居場所を確保しなければならず、再社会化へのハードルは高くなる。つまり仮釈放に義務づけられる保護観察（更生保護法 40 条）期間が短くなるほど、元受刑者は社会に一人放り出され、よるべなく再び罪を犯し、また収容されることを繰り返してしまう。

現在、刑期の長期化・仮釈放の厳格化によるこうした不都合（世論に迎合したツケ）を補正するため、法改正により判決時点で保護観察付き一部執行猶予を

言い渡し、始めから保護観察期間を確保することが可能になった（刑法 27 条の 3。薬物使用者一部執行猶予法 3 条により薬物使用ではさらに厚く認められる）。前述した出口支援（更生保護法 82 条以下の特別調整が中心となる）の取り組みと組み合わされることで、長期間切り離されていた社会へポンと放り出されて「立ち直れ」と自己責任を強いられるばかりでない、再犯予防のために連係していくシステムが構築されることを期待したい。

仮釈放自体の判断は、受刑期間中の態度、問題行動の多寡、罪種・刑期等を踏まえ、公平な基準によって判断されると思われるから、AI に判断させることも容易であろうが、それが何としても必要というほどではなかろう。

むしろ仮釈放に伴う居住地、身元引受人、受け入れ先となる民間の更生保護施設・自立準備ホームや国（法務省）運営の自立更生促進センター、勤務先、あるいは学校・フリースクール、家族との関係の調整、仮釈放中の特別遵守事項の内容などから、そのほか福祉的支援に係る地域生活定着支援センターへの接続、更生支援計画の作成に至るまで、仮釈放に伴う出口支援のあり方を決めるために、各種リソースについてのデータを網羅し、過去事例のサンプルを学習している AI が、ある程度の更生支援マップのようなものを作成するということは考えられる。各被支援者の個性や個別の事情をプロンプトとして入力することで、社会リソースを十分に活用した更生支援の道筋が描き出されるならば、それは保護観察を中心とした再犯予防・社会復帰の取り組みにとっての一つの重要な手引きとなる可能性がある。

（17）　AI 刑事手続と少年法上の保護処分

少年による犯罪・非行事件では、重大事件で刑事裁判となるものを除けば、家庭裁判所の調査・審判により処理される。そこでは刑罰の代わりに保護処分の決定がなされるが、実際にはむしろ不処分や審判不開始の決定が多い。これは無罪放免の扱いになるというより、少年事件が全件送致主義を掲げて小さな非行も見逃さないという姿勢を取っていることや、調査・捜査の過程での警察官や家裁調査官による働きかけと調整により一定の問題解決が図られていることを意味する。

このように少年法では保護処分のみならず、むしろそれまでの調査や審判の過程での少年への働きかけを通し、自覚や立ち直りを促すこと（保護的措置）が重視される。この考え方は保護主義や教育主義と呼ばれ、少年法の手続全体に及ぶ。そのため少年法は刑訴法の採る厳格な適正手続をある程度犠牲にして（非形式主義）でも、こうした働きかけ（ケースワーク機能）に重点を置き、これを活かす制度を採っている。この姿勢は少年審判や調査のみならず、警察の街頭での補導を始めとする少年警察活動（少年警察活動規則 3 条）から、少年に対する勾留・取調べの場面（少年法 17 条）、ひいては少年の刑事事件でさえ求められる（少年法 45 条 5 号ただし書き、48 条、55 条、61 条など）。

こうした少年事件におけるケースワーク機能が十分発揮されるには、非行事実のみならず、少年自身の素質や背景に対する十分かつ科学的な調査と理解が必要だ。

いってみれば保護処分の決定前の段階にこそ、少年法上重要なケースワーク機能の発揮される場面がある。AI がこれらや保護処分決定に関わるとすれば、どのようなことが考えられるか。

保護処分を決定する上では、大きく非行事実と社会調査（少年自身の資質や環境に関するもの）の内容が関わる。このうち非行事実に関するもの、つまり警察・検察が調べた内容に関しては、例えば非行事実や犯罪の種類（性犯罪か薬物か窃盗か、集団犯罪か、ぐ犯かなど）、非行歴、年齢、性別などがある。これらは一定の定型性があるから、AI のアルゴリズムの特徴量として設定することができそうだ。

他方、家裁調査官による社会調査の内容としては、少年の生い立ち、家庭環境、素質･気質、交友･交際関係、行状・生活態度などの具体的で詳細な内容が含まれる。

両者を踏まえた上で、具体的にどのような保護処分が有効かが判断される。さらにはそれに加え、いかなる環境調整が必要かも示される場合がある（少年法 24 条 2 項、64 条 5 項）。

あるいは不処分・審判不開始とする場合でも、例えば監督者・保護者との具体的な関係を踏まえて、どのような監督や保護が期待できるか。学校その他関係機関の理解・協力をどの程度得られるかも検討される。少年への働きかけや、こうした環境調整といった保護的措置は手続を通して一貫してなされる。

このような少年の社会調査を踏まえた処分・不処分決定とその内容は、ケースワーク機能という言葉が示すとおり、個々の少年の特徴・特性や個

別の環境を踏まえたものとなる。その点で、犯罪事実の重さが重視される刑事裁判と異なる。

家裁の裁判官は経験が少ない場合も多く、また一人での裁判も多いため、AI が機能しうる余地はないではない。だがそれはむしろ AI を参考にするというより、AI に頼ることになりかねない。さらに個々の少年の様子をしっかり観察するという少年審判の基本・ケースワーク機能がおろそかになる恐れもある。

画一的処理に必ずしもなじまず、また公平性以上に事案の特殊性を十分加味すべき少年審判において、AI 利用は限定的であるべきだ。

（18） AI 刑事手続と裁判員裁判

裁判員は法律の素人であり、事実認定の素人だ。だからその部分を AI が補ってくれれば有用にも思える。しかし裁判員は素人であるがゆえ、AI が示した判断を批判的に吟味することが難しい。ましてその専門性や科学性に過度に幻惑されかねない。それは素人の素直な感覚を裁判に導入した意味そのものを失わせる。

むしろ裁判員裁判に AI を導入するならば、裁判員に偏見を抱かせないような取調べの録画方法の検討や、弁護人立会を前提とした取調べ・調書作成のあり方の改善、より良い評議の進め方の検討などにこれを活かし、硬直化しがちな現状を変えるのに役立てるべきだ。

（19） AI 刑事手続と弁護活動

刑事弁護人の中には、刑事弁護の経験や技術が未熟だったり、あるいは始めから刑事弁護の意義を限定的に捉えて検察や裁判所の意向を安易に受け入れるような弁護をする者もいると聞く。依頼人の意見や考えに十分耳を傾けない不適切な弁護活動は、被疑者・被告人の不利益のみならず、刑事裁判の公平・適正そのものを脅かす。

法律に素人の被疑者・被告人自身が、自分を弁護するのにどのような活動が必要かを知るサポートのための AI があるのは望ましい。あるいは自分になされている弁護活動に関するセカンドオピニオンを AI から得られれば、不適切弁護の被害者となるのを防げるかもしれない。

弁護人も知り合いの弁護士から弁護活動のアドバイスを受けられるだろうが、経験も相談相手も限られる場合、AI 刑事弁護人のアドバイスを聞けるのは有効となる。ひいては依頼者のメリットにもなりうる。

犯罪類型や事件類型により、検察官がどのような主張をしがちであり、どの裁判体のどの裁判官がいかなる判断傾向を有しているか、過去の同種事案で採られた弁護方針やその有効性など、現在でも考慮されている内容につき AI が整理して示すなら、それは迅速・有効な弁護活動に役立つかもしれない。

もちろんそれらは弁護人自身が弁護技術を身につけ経験を積み重ねるための手立てであり、AI に任せきりにするのを許すものであってはならない。

5　EU 規則案と刑事手続

（1）EU 規則案とリスクベース・アプローチ

ここまで見てきたような AI 刑事手続に関する懸念は、2024 年 2 月 2 日に欧州議会と欧州理事会（EU 首脳会議。最高意思決定機関）とが合意に至った AI 規則案（https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf）でも共有されている（以下、三部裕幸弁護士による労作であろう仮訳を参照した。https://www.aplawjapan.com/publications/20220725 なお同サイトにある「概要」がわかりやすい）。

EU 規則は EU 指令と異なり国内法の整備を要せず直接適用される。また AI 規則案は域外適用も定める（2 条 1 項（a）。上掲規則案 94 頁、仮訳 44 頁以下）。

AI 規則案は特に「禁じられる AI 利用」（5 条。規則案 106 頁以下、仮訳 49 頁以下）と「ハイリスク分類の AI システム」（6 条。規則案 111 頁以下、仮訳 53 頁以下）とを分ける。

AI 利用が禁じられる場合として規則 5 条 1 項（d）は、「法執行目的での、公共空間におけるリアルタイム遠隔生体識別システムの利用」を挙げる。ただし例外として、国内法に基づく厳格な必要性・相当性（比例性）の司法審査等を条件に、（i）拉致、人身売買、性的搾取の特定された被害者等に限定した捜索、（ii）現実的で差し迫った人身の安全への特定の脅威や現実的に差し迫りまた予測可能なテロ攻撃の脅威の阻止、（iii）加盟国

において長期４年以上の拘禁に係る罪の被疑者の発見・捜査、起訴、刑の執行、といった必要のある場合が挙げられている（規則案 107 頁）。

禁じられる AI 利用（規則案５条）
法執行目的での、公共空間におけるリアルタイム遠隔生体識別システムの利用（規則５条１項 (d)）
司法審査を前提とした例外
(i) 拉致、人身売買、性的搾取の特定された被害者等に限定した捜索 (ii) 現実的で差し迫った人身の安全への特定の脅威や現実的に差し迫りまた予測可能なテロ攻撃の脅威の阻止 (iii) 加盟国において長期４年以上の拘禁に係る罪の被疑者の発見・捜査、起訴、刑の執行

他方「ハイリスク分類の AI システム」に含まれる場合（6 条２項）が、規則案末尾に掲げられた付属書Ⅲ（annex Ⅲ）に示され、そこには「6. 関係する EU 法ないし国内法下で許される法執行」に使用される AI と、「8. 司法や民主的プロセスの運営」に使用される AI がある（規則案 249 頁以下、仮訳 107 頁以下）。

まず「6. 関係する EU 法ないし国内法下で許される法執行」で用いられる AI として、(a) ある人が犯罪の加害者ないし被害者になるリスクを評価するために各種法執行機関が用いようとする AI システム、(b) 各種法執行機関が嘘発見器やそれに類するツールとして用いようとする AI システム、(d) 各種法執行機関が捜査や訴追の過程で証拠の信用性を評価するために用いようとする AI システム、(e) 各種法執行機関が、EU 刑事法執行指令（2016/680 LED=Law Enforcement Directive）３条（4）で定義されるプロファイリングに基づく場合に限らず犯罪や再犯を犯すリスクを評価したり、あるいは人の人格的特性・特徴や前科・前歴を評価するために用いようとする AI システム、(f) 各種法執行機関が、犯罪の検知、捜査、訴追の過程で EU 刑事法執行指令３条（4）で定義されるプロファイリングのために用いようとする AI システム、が挙げられている。なお (c) はディープフェイク検出に係るもの、(g) は犯罪の分析に係るものを定めていたようだがなくなっている（仮訳 107 頁）。EU 刑事法執行指令については、横田明美「EU 刑事司法指令のドイツにおける国内法化と十分性認定 ――監督機関に着目して――」情報法制研究９号（2021）92 頁以下も参照。

また「8. 司法や民主的プロセスの運営」で用いられる AI のうち司法に関するものとしては、「司法当局などが具体的事案において事実や法律を取調べ、解釈し、適用するのに、またはその他の紛争解決上同様のことをするのに用いようとする AI システム」が挙げられている（規則案 251 頁、仮訳 107 頁）。

ハイリスク AI に含まれる場合（規則案６条２項）
関係する EU 法ないし国内法下で許される法執行に使用される AI（付属書Ⅲの 6）
司法審査を前提とした例外
(a) ある人が犯罪の加害者ないし被害者になるリスクを評価するために各種法執行機関が用いようとする AI システム (b) 各種法執行機関が嘘発見器やそれに類するツールとして用いようとする AI システム (d) 各種法執行機関が捜査や訴追の過程で証拠の信用性を評価するために用いようとする AI システム (e) 各種法執行機関が、EU 刑事法執行指令（2016/680 LED=Law Enforcement Directive）３条（4）で定義されるプロファイリングに基づく場合に限らず犯罪や再犯を犯すリスクを評価したり、あるいは人の人格的特性・特徴や前科・前歴を評価するために用いようとする AI システム (f) 各種法執行機関が、犯罪の検知、捜査、訴追の過程で EU 刑事法執行指令３条（4）で定義されるプロファイリングのために用いようとする AI システム
司法や民主的プロセスの運営」に使用される AI（付属書Ⅲの 8）
司法当局などが具体的事案において事実や法律を取調べ、解釈し、適用するのに、またはその他の紛争解決上同様のことをするのに用いようとする AI システム

そして「ハイリスク分類の AI システム」については、９条以下に定められた諸要件が遵守されると共に、その AI 技術の意図・目的や技術水準の概略が明らかにされなければならないとされる（8 条。規則案 115 頁、仮訳 53 頁）。

９条以下に定められた遵守すべき要件としては、❶ AI システムが健康や安全等に与えうるリスクの特定・分析や推定・評価に適し、またそれらの低減・除去が保障されるべき「リスク管理システム」の構築・実施・維持・記録・性能テストなど（9 条）、❷システム開発における適

切な「データ管理」（10 条）、❸「技術文書」の作成・提供（11 条）、❹ログ（作動履歴）の「保持」（12 条）、❺「透明性とシステム利用者への情報提供」、アクセサビリティ（13 条）、❻「人的監視」・モニタリング、決定補助 AI に自然と依存化する傾向（「自動化バイアス」）の確認（14 条）、❼設計・開発における適正な「正確性、堅牢性（robustness）、安全性（cybersecurity）」、動作上の耐性（resilient）（15 条）、があり、ハイリスク AI の提供者はこれら要件の遵守や品質管理システムの導入が義務づけられ（16 条）、輸入者や販売者にも提供者による遵守を確認する義務が課される（26、27 条）。

ハイリスク AI の要件（規則案 8 条）

❶ AI システムが健康や安全等に与えうるリスクの特定・分析や推定・評価に適し、またそれらの低減・除去が保障されるべき「リスク管理システム」の構築・実施・維持・記録・性能テストなど（9 条）
❷システム開発における適切な「データ管理」（10 条）
❸「技術文書」の作成・提供（11 条）
❹ログ（作動履歴）の「保持」（12 条）
❺「透明性とシステム利用者への情報提供」、アクセサビリティ（13 条）
❻「人的監視」・モニタリング、決定補助 AI に自然と依存化する傾向（「自動化バイアス」）の確認（14 条）
❼設計・開発における適正な「正確性、堅牢性（robustness）、安全性（cybersecurity）」、動作上の耐性（resilient）（15 条）、

※ハイリスク AI の提供者はこれら要件の遵守や品質管理システムの導入が義務づけられ（16 条）、輸入者や販売者にも提供者による遵守を確認する義務が課される（26、27 条）

（2）EU 規則案と刑事手続原則

上に見てきた AI 法たる EU 規則案も、禁じられる AI として公共空間でのリアルタイム遠隔生体識別、つまり常時監視を挙げ、特定可能な生命・身体への現実的脅威のある場合のみを例外としている。それは必要性・比例性の厳格な司法審査の法定を要求しているから、当然国内法上令状主義の下に置かれなければならない。

他方で捜査当局が捜査・訴追、証拠評価において、また司法当局が法の解釈適用や事実認定において援用する AI はハイリスク AI として、いわばアルゴリズムの透明性やログ（作動履歴）の検証可能性が確保されれば利用できそうだ。

少なくともアルゴリズムの透明性やログの検証可能性の保障は、AI の利用上不可欠だ。特に自由・人権への制限を伴う刑事司法での利用ではそれらは最低限の条件であり、そのことが AI 規則案でも明示されたのは重要だ。

たとえそれらが保障されたとしても、AI のアルゴリズムはブラックボックス問題から不可避であり、捜査・司法当局は説明責任を果たせない恐れがある。これまでもただでさえ被疑者・被告人の人権を「嫌疑がある」というだけで軽視してきたのがわが国の刑事司法だ。AI 利用がその責任さえもブラックボックスに押し付け回避する手段とならないためには、徹底的な透明性・情報開示・設計運用への参画が不可欠だ。

今後各国当局がそれぞれの社会状況の中で導入を進めていくことになろう。日本は刑事人権保障の後進国として、他国の有意義な取り組みを真摯に取り入れる態度が求められる。またこの点を注視していくことが必要だ。（続く）

編集及び発行人

プライバシー・インターナショナル・ジャパン（PIJ）
東京都豊島区西池袋3－25－15 IB ビル10F　〒 171-0021
Tel/Fax：03-3985-4590　**E メール**：wagatsuma@pij-web.net
編集・発行人　中村克己
Published by
Privacy International Japan（**PIJ**）
IB Bldg. 10F,3-25-15 Nishi-ikebukuro
Toshima-ku, Tokyo, 171-0021,Japan
President Koji ISHIMURA
Tel/Fax +81-3-3985-4590
http://www.pij-web.net
2024.10.17 発行 CNN ニューズ No.119

入会のご案内

季刊・CNN ニューズは、**PIJ** の会員（年間費 1 万円）の方にだけお送りしています。入会は **PIJ** の口座にお振込み下さい。

郵便振込口座番号
00140－4－169829
ピー・アイ・ジェー（**PIJ**）

NetWork のつぶやき

・時代は、スマホファースト！　IC カードを使わない電子政府モデルが世界の趨勢。マイナカードとマイナ保険証の一体化は時代遅れの愚策！　「マイナ保険証パンデミック」はご免だ！　血税のムダ遣いはもう止めないと！　（N）