

『ゼロマイナ』から『ウイズマイナ』の時代をどう闘い抜くか？

巻頭言

政官主導のマイナパンデミックを止めるには やはりオールジャパンの新党が要る！！

世界を見渡すと、デジタル化で、いまや物理的なICカードはお荷物になりつつある。モバイルアプリを活用した「デジタルID」に代替わりしているからだ。ガラパゴス化したマイナICカードは、対面での国民監視ツールの役割しかない。アナログの凶器になる前に廃止しないとイケない。改良型のマイナICカードの発行も要らない。国の役人の悪巧みそのもの、デジタル化の失敗を公言するようなものだ。世界の笑いものになる。

名ばかり三権分立、行政追従の消極司法で、3月9日に、最高裁は市民のマイナ違憲の訴えを上告不受理で退け、「合憲」のお墨付きまで与えた。司法は、やはり「国家権力」なのだ。ずっとこんな裁判闘争はいい加減にして欲しいと願っていた。最高裁が「合憲」と判断するのがわかっているのに最後まで突っ走る。まさに「外部不経済」である。反マイナでサステナブル（持続可能）な闘いを望む者には迷惑である。「合憲」、「違憲」をはっきりさせないで闘う賢さを欠いていたのではないか。

この国のトップは、国民の声を聴く気がない御仁である。マイナパンデミック、原発再稼働、防衛増税も、突然アナウンスされる。

◆ 主な記事 ◆

- ・ 巻頭言～やはりオールジャパンの新党が要る！！
- ・ Q & A：デジタルIDとは何か
- ・ NYU 報告書を読む
- ・ チャットジプティ（ChatGPT）と税理士の相談業務

近隣の専制国家並みの政策決定の作法だ。そして、いまや立法府も大勢は、「悪いことしていなければ、マイカードでの国民監視でも怖がることはない」のトーンである。

もはや「ゼロマイナ」では闘えない。「ウイズマイナ」で、デジタルも総動員し、マイナが人権に踏み込まないように賢く闘わないとイケない。マイナパンデミック、マイナカード取得で監視社会は当り前の集団ノイローゼと、どう闘うのかが問われている。

住基ネット反対のときには、左右を問わず大物の政治家や有名人をたてた運動を展開できた。巧みな戦略があった。しかし、現在のマイナ要らない運動は「ゼロマイナ」のムシロ旗闘争しかできていない。求心力も今一つである。

マイナ要らない運動にはマイナパンデミックを撲滅する新たなチーム力が要る。オールジャパンのシングルイシュー（単一争点）新党を立ち上げて、人権侵害的なマイナパンデミック拡散にストップをかける道を探らないとイケない。ムシロ旗闘争や大本営発表の解説も大事ではある。だが、それだけでは絶滅危惧種になる。どの運動も、しぶとく加え、したたかな戦略で駆け出す行動がいる。

マイナ要らない運動に栄光あれ！！

わが国の人権エコシステムを欠く危ないマイナ IC カード

Q & A : デジタル ID とは何か !

世界で加速するモバイル化、IC カードに頼らないデジタル ID が主流 2023 年、豪・加・米に続き、英も IC カードなし方式を選択

石村 耕治 (PIJ 代表・白鷗大学名誉教授)

《コンテンツ》

【ポイント解説】

■はじめに

- ◆本人確認とは何か
- ◆デジタル ID とは何か
- ◆デジタル ID を取り巻く諸課題とは
- ◆わが国のデジタル ID とは
- ◆頓挫した東京渋谷区での民間活力を生かした個人向けデジタル ID
- ◆アメリカで採用するデジタル ID とは

- ◆アメリカで問われたデジタル ID 「デザインの不正義」
- ◆アメリカで問題化した顔認証式「ID.me」
- ◆EU ではブロックチェーン技術活用のデジタル ID 検討も
- ◆2023 年、イギリスも IC カードを使わない新デジタル ID 採用
- ◆個人用デジタル ID に人権エコシステムをどうデザインするのか？
- むすび

【ポイント解説】

デジタル化 (DX) の嵐が吹き荒れている。社会、経済のあらゆる部門で DX の影響は避けられない。こうしたなか、「デジタル ID (digital identity)」のあり方が注目を浴びている。

もっとも、「デジタル ID ?」と言われれば、戸惑う人も少なくないかも知れない。私たちは、常日頃、スマホのアプリやパソコン (PC) のソフトを使っている。この際に「アカウント ID」と「パスワード」などを入力する。これが、「デジタル ID」である。「ID / アイデイ (identification)」は英語で、日本語では「本人確認」、「身分証明書」とかいう意味である。

「デジタル ID」とは、インターネット (ネット) / デジタル / オンライン空間で本人確認 (身元確認 + 本人認証) に使う ID である。パソコン (PC) またはスマホを使って、インターネットで、政府・公共機関 (国や自治体その他の公的機関など) や民間機関 (会社その他の企業や私的機関など) のさまざまなウェブサイト (ホームページ / デジタルプラットフォーム / ポータルサイトなど言い方はさまざま。) にリモート (遠隔) アクセス / ロ

グインする際の ID を指す。

インターネットのないリアル (対面) / 紙 (文書) だけの時代が長く続いた。この時代には、「ID (本人確認)」は紙のカードとか、プラスチックカードが使われてきた。こうした本人確認証は、リアル (現実 / 対面) で使われることから「リアル ID」と呼ばれる。インターネットが発達した今日でも、対面での本人確認には「リアル ID」が欠かせない。一方で、ネット / デジタル / オンライン業務は急拡大でゴールのないレースのようなありさまだ。当然、本人確認での「デジタル ID」の重要性を増す。なりすましその他さまざまなネット / サイバー犯罪の防止にも、「デジタル ID」は必須アイテムだ。

◆さまざまな「デジタル ID」がある

「デジタル ID」は、大きく 2 つにわかれる。1 つは「個人用」である。もう 1 つは「個人以外 (企業 / 団体) 用」である。個人用のデジタル ID と言っても、技術仕様 / デザインはさまざまである。実用化されて、一般化しているものは、次のとおりだ。

個人用デジタル ID として実用化された技術仕様

① (アカウント) ID・パスワード式、② PKI (公開鍵・電子証明書・電子署名) 式、③ 生体認証 (顔・虹彩・指紋など) 式、④ 二次限バーコード (2D barcode / 商品名: QR コード) [マトリック] や⑤ ワンタイムパスワード式 [マトリック] がある。他に、実用化されていない⑥ ブロックチェーン (暗号資産) 式がある。

マイナカード (マイナンバーカード / 個人番号カード) は、①リアル (対面) での本人確認用の ID (リアル ID) と、②非対面では①・②・④ (+③) の技術仕様を使ったデジタル ID を兼ねた物理的 IC カードだ。

住民票の写しが欲しいとする。以前は市町村役場に出かけて行って、対面で申請する、あるいは郵送で申請するしかなかった。しかし、デジタルシフト / デジタル化が急激に進み、今日では、インターネットを使いパソコン (PC) やスマホなどから市町村のウェブサイトログイン / アクセスしオンライン申請ができる。

また、電気やガス、上下水道代その他の公共料金の支払 / 銀行口座引落領収書、クレジットカードの利用額明細書なども、以前は紙 / 文書で通知を受けていた。しかし、今日では、デジタル / ネットでの通知・閲覧が当たり前になってきている。

スマホで、アプリを使って電気料金やクレジット利用明細を見たいとする。その場合、クレジット会社のウェブサイト (ホームページ / デジタルプラットフォーム / ポータルサイト) にリモート (遠隔) アクセス / ログインすることになる。その際には、アカウント ID とパスワード (2 段階認証) を入れるか、さらにはネットワーク暗唱番号ないし Q&A 操作 (3 段階認証) をしないといけない。これが、まさに① ID・パスワード式のデジタル ID だ。人によっては、アカウント ID・パスワードなどが憶え切れないということで、顔認証技術仕様 (FaceID / FRT) を使うことになる。これが、③ 生体認証 [顔面 (顔パス)・虹彩・指紋 (タッチ ID) など] 式のデジタル ID だ。

今日ではデータセキュリティを高めるために、①+②、②+③、①+②+③、①+②+④、①+②+③+④を組合せ、バージョンアップされたデジタル ID もある。

◆マイナ IC カードはなぜ嫌われ者なのか？

マイナ IC カードは、デジタル時代の申し子のように見える。また、リアル ID とデジタル ID

兼用で、最も効率的な ID のようにも見える。政府によるプロパガンダ・マインドコントロールは一見成功しているようにも見える。ところが、必ずしも好感度が高くなく、嫌われ者である。「マイナパンデミック」とやゆされる。それには、いくつかの原因がある。主なものをあげると、次のとおりである。

マイナ IC カード、好感度が低く、嫌われ者となっている理由

①	デジタル ID には、いくつかの技術仕様がある。わが国は、個人用のデジタル ID を、マイナンバー (背番号) を記載した物理的な IC カードに② PKI (公開鍵・電子証明書・電子署名) 技術仕様を格納する人権ストレスの強い (人権エコシステムを欠く) モデルを選択している。また、マイナシステム (国民総背番号制) では、① (アカウント) ID・パスワード式、② PKI (公開鍵・電子証明書・電子署名) 式、③ 生体認証 (顔面認証) 式、④ 二次限バーコード (QR コード) [マトリック] の監視技術を総動員した人権ストレスが高いデザインとなっている。一方、個人以外 (企業 / 団体) 用デジタル ID は、必ずしも法人番号などとは紐づかない自由な技術仕様を選択できる。個人用のデジタル ID は、国民監視ファースト、「人権エコシステム」を欠いたデザインになっており、民主主義国家の価値観とぶつかる。
②	わが国のマイナ IC カードを使った「リアル ID とデジタル ID 兼用」のモデルでは、オフライン (対面) とオンライン (遠隔) 双方で使えて便利、とする見方もある。だが、紛失すると、リアル ID としての表記されたプライバシーが駄々洩れになる。また、ID として第三者に提供する自己データを限定・コントロールする権利を行使できない。この権利を保障するには、欧米の例にならい、物理的な IC カードに頼らないデジタル ID [モバイル ID アプリ] を選択しないといけない。
③	政府は、`公定 / 実質国定`、`官製`の個人用デジタル ID を格納した「マイナ IC カード」の利用を無原則に民間取引に広げる画策をしている。自由な資本主義・市場主義のルールとぶつかる。また、国民には、「国の役人がつるんで横並び、官が主役」のデジタル ID 政策のように映る。権威主義国家の悪臭がし、民主主義国家には似合わない。どの技術仕様のデジタル ID を選択するかは、個人も個人以外 (企業 / 団体) も、自由とすべきである。
④	国家によるマイナ IC カード取得の強要、健康保険証・介護保険証として利用させる政策は、

④	<p>「国内パスポート (inner passport)」化につながり、マイナ IC カードを携行していない人は「非国民」とする「分断政策 (decoupling)」につながる。こうした差別的な権威主義国家づくりは止めないといけない。リアル (対面) ID としては、運転免許証、パスポートなどさまざまな選択を認める政策を維持するのが、民主主義国家の基本である。IC カードのモバイル化の流れが強まっており、西欧型民主主義を採る諸国では、民間活力を生かし、国民番号 (ID) カードなど公定/実質国定の IC カードに頼らないデジタル ID [モバイルアプリ] を導入している。国の役人が検討している新型のマイナ IC カードは時代の流れを読めない愚策であり、かつ血税の無駄遣いでもある。人権ストレスの強いマイナ IC カード自体、これを廃止すべきである。</p>
⑤	<p>「人権エコシステム」がデザインされていない個人用のデジタル ID は、単なるデジタル空間における本人確認目的・社会サービス目的のツール (道具) であることを超えて、国家による濫用・悪用で人権弾圧の凶器/デジタルトラップ (罠) にもなる。わが国のマイナ IC カード (IC カード式デジタル ID) の健康保険証併用による国民医療・健康情報の国家管理・自動徴兵選別。中国のデジタル ID を使った社会信用スコア制度 (social credits system) の構築・人間選別は典型的な悪例である。</p>
⑥	<p>国家は、デジタル ID が人権侵害装置になることを防ぎ、かつデジタル ID に人権エコシステムを確立するために、①プライバシー最優先の技術仕様 (privacy-first by design)、②データ収集の最小化 (data minimization)、③分散化 (decentralization)、④同意/任意 (consent)、⑤アクセス制限 (limited access)、⑥IC カードなし (without a national identity IC card) / モバイルアプリ (mobile app) 利用、⑦第三者への自己データ提供の自己コントロール権 (right of digital self-determination / self-sovereign) などの原則を遵守したうえでデジタル ID をデザインしないとけない。しかし、わが国にマイナシステムではこうした原則が守られていない。国民監視ファーストのデザインである。</p>

◆公定/実質国定デジタル ID で民業圧迫？

例えば、住民が住民票の写しをオンライン申請とする。それで、ネットで市町村のウェブサイトログイン/アクセスとする。この場合、住民は、さまざまあるデジタル ID のなかから最

も使い勝手のよいものを選んでもいいはずだ。ところが、マイナンバー IC カードに格納された② PKI (公開鍵・電子証明書・電子署名) 式のものしか使えないことになっている。つまり、国の役人が、国や自治体のウェブサイトログインの際の個人用のデジタル ID として、民間 IT 企業が開発し、自治体や住民が選んだものを使うのは罷りならぬとし、法律で縛りをかけているからだ。おおかたの自治体も、横並び大好きである。「国は地方体にもっと効率的な独自のデジタル ID を使わせろ!」、「民業圧迫だ!」などの声をあげる意欲は見られない。たとえ不合理だとわかって、国の役人を付度する。ところが元気な自治体もある。

◆総務省に潰された東京渋谷区での民間活力を生かした個人向けデジタル ID

民間のスタートアップ、IT 企業である東京都港区にある Bot Express 社は、LinePay のアプリをベースにデジタル ID を開発・販売している。

東京都渋谷区は、2020 年 4 月から、Bot Express 社とタックルを組んで同社のデジタル ID を使って、住民が住民票のオンライン申請をしたうえで住民票の郵送を受けられる制度を始めた。つまり、マイナンバー IC カードに格納された② PKI (公開鍵・電子証明書・電子署名) 式のデジタル ID を使わない方式での住民票のオンライン申請を受け付け始めたわけである。元気のある自治体だ。

渋谷区のこの新システムは、① ID・パスワード式をベースに、スマホで撮影した③顔写真付き身分証とスマホのカメラで写した本人の容貌を送信、AI (人工知能) がそれらを照合する技術仕様だ。本人と確認されれば、区が住民票の写しを後日郵送する手順になっている。

AI による判別がつかなかった場合には、自治体職員が目視で確認する。そして OK であれば住民票を郵便で提供することになっている。金融機関で顧客が口座開設の際に利用する際に、オンラインで身元確認を完結する「eKYC (electronic Know Your Customer)」と呼ばれる技術仕様と同じだ。

ちなみに、eKYC 方式のデジタル ID は、犯収法 (犯罪による収益の移転防止に関する法律) でも使われている。つまり、マネー・ローンダリングやテロ資金供与防止を目的として、特定の事業者が取引する際の本人確認等でも認められている。eKYC 式のデジタル ID は、法認されたデー

タセキュリティの確かなものだ。

東京都渋谷区は2020年4月に、Bot Express社のデジタルIDを導入し、同区のウェブサイトのログインに利用できるようにし、住民票のオンライン申請をできるようにした。しかし、開始直後、総務省が「待った！」をかけた。

総務省は、2020年4月3日に、全国の市町村への「技術的助言」として、事実上同サービスを採用しないよう求める通知をした。住民票の交付には厳格な本人確認が必要であり、マイナンバーカードに搭載した②PKI（公開鍵・電子証明書・電子署名）よりも性能が劣るeKYCの採用は「適切でない。」というのが理由だ。しかし、eKYCは、すでにふれたように、犯収法で法認された技術仕様である。携帯電話移転防止法、古物営業法などでのオンライン上の本人確認で、適正な技術仕様として法認されている。

総務省は、2021年9月には、この通知にあわせて、住民票の写しの交付に関連する省令を改正した。これにより、住民票のオンライン申請のウェブサイトへのログインの際の本人確認には、マイナンバーICカードに搭載された②PKI式のデジタルIDしか認められないことになった。総務省は、民間IT企業のデジタルIDを使った渋谷区のオンライン申請は法令違反とするとの規定を設けたわけだ。「悪法も法なり」の手法で、同社のデジタルIDの自治体への販売を停止に追い込んだのである。

Bot Express社は、総務省の画策により、他の自治体へのサービス展開ができなくなった。そこで、2020年9月10日に、同社は、総務省（国）の通知は違法であるとして、東京地裁に提訴した。東京地裁は、昨年末（2022年12月8日）によりやく判断をくださった。判決では、LINE申請では偽造された本人確認書類でも審査を通過する可能性があるとした上で、「不正の手段がひとたび確立されれば住民基本台帳制度の根幹への信頼が揺らぐことになりかねない」と指摘した。総務省が通知した厳格な本人確認は、行政のIT化を推進するデジタル手続法とも整合するとした（東京地判令和4年12月8日判決・東京地判令和4年（行ウ）第344号）。

東京地裁は、行政追従の消極的司法の姿を露わにする判断をくだし、原告IT企業の訴えを認めなかった。2023年3月9日、最高裁が、市民のマイナンバー違憲の訴えについて上告不受理、マイナは合憲の判断をしたのと同じスタンスである。

スマホ全盛時代に入り、アメリカやオーストラリア、イギリスなどでは、デジタルIDには、①ID・パスワード式ないし①+③顔認証（顔パス）併用式の技術仕様を採用している。マイナカードのような利便性の悪い物理的なICカードに頼るデザインのデジタルIDは採用していない。②PKI（公開鍵・電子証明書・電子署名）式でなくとも、他の技術仕様のデジタルIDでも、十分に安心・安全だからである。むしろ②PKI（公開鍵・電子証明書・電子署名）でない技術仕様のデジタルIDの方が、簡素・安心・安全・安価である。とりわけモバイルスイカなどに慣れたデジタルネイティブ、スマホネイティブにはユーザーフレンドリー（利用者優先）である。いまさらICカードは時代遅れである。

東京地裁で判決を下した裁判官は、こうした事実を知らないのであろうか。あるいは、単なる事なかれ主義なのだろうか。

総務省のやり方や時代感覚には大きな疑問がつく。同時に、裁判所の判断にも、「官尊民卑そのもの」、「民業圧迫に加担している」などの厳しい批判が渦巻いている。

もちろん、東京都渋谷区が採用したBot Express社の③顔認証（顔パス）式のデジタルIDが最良の選択とは思えない点もある。アメリカなどでは、③顔認証（顔パス）式デジタルIDは、人種差別など人権侵害を引き起こすとの厳しい声もあるからだ。

ちなみに、わが国の個人（所得税）の電子申告（e-Tax）では、国税庁のポータルサイト（ウェブサイト）へログインの際のデジタルIDとして、②PKI（公開鍵・電子証明書・電子署名）式に代えて、①ID・パスワード式の選択も可能となっている。マイナカードが普及するまでの暫定措置としているものの、①ID・パスワード式の方が確実にユーザーフレンドリーである。いまや①ID・パスワード式かそのバージョンアップ版が世界標準である。にもかかわらず、初期設定などがIT素人には煩雑過ぎる②PKI（公開鍵・電子証明書・電子署名）式を強要しているわけだ。国の役人のふるまいにはあきれられる。

◆アメリカの個人向けデジタルIDとは？

アメリカでは、官民とも、個人向けデジタルIDには、①ID・パスワード式、ないし①+③顔認証（顔パス）併用式を採用している。②PKI（公

開鍵・電子証明書・電子署名) 技術を使ったデジタル ID を採用しようとする動きはまったくない。IC カードやカードリーダーが必要な②PKI 式は、ガラパゴス化した過去の技術、というのが大勢の見方だ。スマホ全盛時代に入り、将来を見据えて考えれば、IC カードの選択はない。むしろ③顔認証(顔パス) 技術(FRT) 利用に傾斜する傾向が伺える。加えて、データセキュリティ(データ安全)、デジタル ID として④ブロックチェーン(暗号資産) 技術を実用化しようという動きすらある。

アメリカで個人用のデジタル ID に②PKI (公開鍵・電子証明書・電子署名) 技術の利用が敬遠されるのは、初期設定などが IT 素人には煩雑過ぎ、むしろ簡素な方式が好まれることによる。また、モバイル化の流れ、IC カード(国民番号カード) に頼らないデジタル ID が世界で加速していることがある。

◆民間活力を生かしたのアメリカのデジタル ID

いずれにしろ、アメリカは、市場主義を大事にする国である。同国では、わが国のような②PKI (公開鍵・電子証明書・電子署名) 式の公定/実質国定の個人用デジタル ID をマイナンバー IC カード格納して配り、官民の垣根を越えてより包括的(オムニバス) に使わせようという不気味な政策は、絶対にコンセンサスが得られない。市民には、「民間活力を死滅させる」、「全体主義」、「民業圧迫」以外の何物でもないと映るからだ。

今、アメリカでは、連邦や州行政機関では、個人用には①アカウント ID・パスワードの技術仕様をベースにした ID.me(アイデー・ドット・ミー) という民間のスタートアップ IT 企業が開発・販売しているデジタル ID [モバイル ID アプリ] が幅広い支持を得ている。

ID.me は、ログインには、①アカウント ID・パスワード、複数のアナログ身元確認証の写しデータ、さらには③スマホないしパソコンのウェブカメラを使って自撮りした写真画像(selfie image) の提出を求めるデザインだ。有人ビデオ(動画) チャット【Video Chat / インターネットを通じてお互いの映像を見ながら、リアルタイムにコミュニケーション・会話ができるサービス】の利用も可能だ。若いデジタルネイティブ、スマホネイティブ層には大人気だ。

ところが、2022 年に入ってから、ID.me 社が

開発・販売するデジタル ID サービスに、連邦議会民主共和両党の議員から茶々が入った。同社のデジタル ID は人権エコシステムを欠いているのではないかというのだ。写真画像(selfie image)、顔認証(顔パス) 地術(FRT) を使っているのが社会的・経済的に弱い立場にある人たちの人権にマイナスに作用しているというのである。

こうした批判・指摘を受けて、連邦課税庁(IRS) は、電子申告やオンライン申請などで同庁のウェブサイトへのログインには、ID.me 社の①アカウント ID・パスワードの技術仕様は引き続き利用しているものの、スマホないしパソコンのウェブカメラを使った自撮りした写真画像(selfie image) の提出、顔認証(顔パス) 地術(FRT) の利用を一時停止した。

一般に、アメリカでは、監視カメラやデジタル ID などに、生涯不変の生体認証情報技術を活用することには否定的な考えが強い。IRS はいまだ世論や連邦議会の動向を注視している。2023 年 4 月末を期限とする 2022 年分の連邦個人所得税の電子確定申告(e-file) がすでに始まった。

にもかかわらず、IRS は、オンライン申告のデジタル ID として、ID.me を継続して使うのか、他社のデジタル ID、Login.gov に代えるのかも含め、2023 年 3 月にいたっても、新たな方針を出していない。

◆EU ではブロックチェーン技術活用のデジタル ID 検討も

EU(欧州連合) は、個人用のデジタル ID として、久しく IC カードに頼る②PKI (公開鍵・電子証明書・電子署名) 式を採用してきた。しかし、いまや時代は、スマホ全盛である。商業 IC カードのモバイル化の流れも止まらない。モバイル化が急激に高まったことが、IC カードには逆風で、マイナスに働く。デジタル ID [モバイルアプリ] は、スマホに直接格納する、あるいは④ブロックチェーン技術を実用化したデジタル ID への転換の検討を始めた。

2017 年にエストニアの国民総背番号(マイナ) システムがサイバー攻撃を受け、IC チップ管理機能が不全になった。人口約 133 万人の都市国家エストニアで、約 75 万の IC カードが利用不能となり、正常化に当局は多大な時間を費やした。わが国の役所寄りのマスメディアなどが持ち上げる IC カードを使ったエストニアの国民総背

番号システムは、例外と脆弱だった。これを機に、エストニア政府も、② PKI 技術を格納した IC カードを使った既存の中央集約管理システムを、分割管理型のデジタル ID の仕組みに移行した。さらに⑥ ブロックチェーン技術の実用化も検討し始めた。ここでも、モバイル化の激流のなか、IC カードにデジタル ID を入れるモデルには逆風で、スマホにモバイル ID アプリを入れる方向に大きく舵を切っている。

◆ デジタル ID のデザイン不正義とは？

「デジタル ID」は、安全対策（データセキュリティ）を二重旗に、不正義なデザイン・技術仕様を選択すれば人権侵害ツールに悪用できる。国民監視用の国内パスポート、健康保険証データの自動徴兵選別、社会保障給付対象選別、信用スコア制度（social credit system）への悪用が適例だ。

このことは、「デジタル ID」のデザイン・技術仕様の選択に対する国民監視は重い課題であることを教えてくれる。国民監視が行き届かないと、唯我独尊の国の役人の横暴を止められなくなる。公定／実質国定の技術仕様のデジタル ID はたちまち国民をデータ監視する「凶器」に変貌する。

アメリカの研究者は、ユーザー（国民）が、デジタル ID の「デザイン不正義（design injustice）」をゆるさないとする姿勢を保つことが大事だ、と強調する。また、デジタル ID のデザインに人権エコシステムをどのように組み込むべきかをもっと真剣に考えないといけない、と警鐘を鳴らす。とはいえ、「デザイン不正義（design injustice）」の言葉は、「外部不経済（external diseconomies）」の言葉などと同様に、一般の人たちにはなじみが薄いのが現実だ。

この島国の庶民は概して英語が不得手、外国のデジタル ID について直接学ぶ機会は限られる。国の役人が「② PKI 公開鍵・電子証明書・電子署名」式以外のデジタル ID はありえない。この方式のデジタル ID を格納するマイナ IC カードは必須！の呪文を唱えれば、たちまちマインドコントロールされてしまう。久しく挙国一致で束ねられてきた庶民の呪縛を解くのは容易ではない。

国の役人にとり、個人用のデジタル ID は、ウェブサイトへの単なるリモートアクセス／ログインのツールではない。彼らには最強の国民監視用ツールなのだ。彼らに「お任せ」では、マイナ IC カード、デジタル ID は、「デザインの不正義」詰

め放題になる。ところが、この不正義にストップをかけようとする研究者もほとんどいない。役人に取り込まれてしまっているからだ。加えて、マイナパンデミック退治に懸命な個人や団体も概して勉強不足だ。

結果、② PKI（公開鍵・電子証明書・電子署名）式のガラパゴス化したマイナ IC カードに異論を唱える研究者や市民団体の方が絶滅危惧種になってしまっている。しかし、これでは、世界から取り残される。IC カードのモバイル化の流れが急激だからである。いまやデジタル ID も、モバイルアプリの技術仕様が世界水準だ。モバイルアプリを使ったデジタル ID では、ユーザー（利用者）が第三者に自己データ提供する際に自由意思で提供データの選択／限定ができる。結果、提供データを自己コントロールできる権利（right of digital self-determination）が保障される。

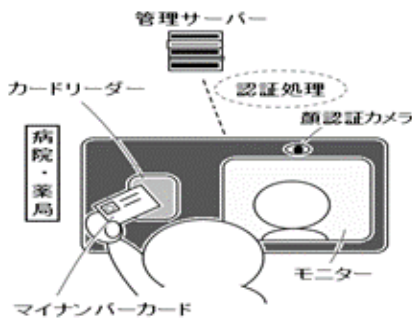
◆ やはり「マイ国党」が必要だ！！

マイナパンデミックにストップをかける運動をする個人や団体は、「デジタル ID とは何か」、とりわけ「個人用デジタル ID」についてももっともっと深掘りして欲しい。でないと、国の役人がやろうとしている悪巧みがよく見えてこないからである。

わが国は、オフライン（対面）とオンライン（遠隔）の双方で使える「リアル ID」＋「デジタル ID」の仕組みづくりをしているようにも見える。しかし、IC カードに格納しないとイケない PKY（公開鍵）式のデジタル ID を採用することで、国民監視 ID カード制（マイナ IC カード制）を敷こうとする悪巧みも格納（秘密に）されてしまっている。国や自治体がオンラインで提供できるサービスはそんなにない。その結果、マイナ IC カードは使う機会は限られる。だから、ただ放っておいては、国の役人が画策する国民監視 ID カードにはならない。

そこで、悪巧みに長けた国の役人は、考えた。悪国民皆保険制度で逃げ切れないマイナ保険証とマイナ IC カードを合体させよう。そうすれば、国民全員が、常時携行せざるを得なくなる。逃げられない国内パスポート（内国人登録証）にできる、と。

マイナ保険証で保険資格確認をするシステム [マイナ保険証資格確認オンラインシステム (M システム)] を医療機関や薬局などに設置する。患者は、マイナ IC カード背番号（マイナバー）と顔認証（顔パス／生体認証）で本人確認をする。



これで、国民の移動の自由を監視する仕組みである「顔認証+背番号カード式自動改札システム」が

できあがる。まさに、車輛のナンバーから追跡するNシステムに匹敵するのが「Mシステム」である。Mシステムは、国民全員の医療/健康データを、国家が管理し、平和憲法をないがしろにしかねない。自動徴兵システム、自動赤紙発行装置に変貌するのではないかと？

Mシステムは、①対面で使う物理的ICカードと、②非対面で使う場合には①（アカウント）ID・パスワード式、②PKI（公開鍵・電子証明書・電子署名）式、③生体認証（顔・虹彩・指紋など）式、④二次限バーコード（QRコード）[マトリックス]の技術仕様を総動員し、まさに「人権エコシステム」を欠いた極悪の個人用デジタルIDの典型である。国の役人がデザインの不正義・悪巧みであり出したこの監視ツールへの反対の大合唱もしばみがちである。肝心の医療界はあきらめ顔だ。国の役人の高笑いが聞こえてくる。

最高裁は、2023年3月9日、市民のマイナ違憲の訴えを上告不受理で退け、「合憲」のお墨付きまで与えた。最高裁は、名ばかり三権分立、行政追従の消極司法の顔を露わにした。司法は、やはり「国家権力」なのだ。「三権分立」は、国家権力を3つに分割してデザインしているだけである。司法が、独立して権力を行使してくれるはず、との「夢」をいただくのもわからないでもない。こうした市民感覚は確かに大事である。だが、マイナは「民事」ではない。「諫早」などと同じで、国家の統治が絡んでくる。司法が「柔」な判断をするはずがない、国家権力がむき出しになる。マンマーや中国などの司法と同じ顔になる。

ずっとマイナ違憲裁判闘争はいい加減にして欲しいと願っていた。最高裁が「合憲」と判断するのがわかっているのに最後まで突っ走る。反マイナでサステナブル（持続可能）な闘いを望む者には迷惑である。身勝手なカミカゼ戦法は時代に合わない。「合憲」「違憲」をはっきりさせないで賢く闘う戦略を採って欲しかった。今の最高裁に自衛隊は違憲か合憲か問うたらどうだろう。ためら

いなく合憲と言うかも知れない。「高度の政治性を有するので司法審査になじまない」（統治行為論）などと柔な説教はしないのではないかと。何事にも深読みが要る。

いまや立法府も「悪いことをしていなければ、マイナカードで国民監視されても怖がることはない」のトーンである。もはや「ゼロマイナ」のムシロ旗作戦では聞えない。

もちろん、ネットを使って危ない国策を評論する、街頭でのムシロ旗をあげたマイナパンデミック撲滅運動も大事である。しかし、シングルイシュー（単一争点）の「マイ国党（マイナパンデミックから国民を守る政党）」（仮称）を立ち上げ、マイナパンデミック撲滅に向けて賢く戦わないといけぬ。マイナ要らない運動にはマイナパンデミックを撲滅する新たなチーム力が要る。国会や自治体議会へ議員を送る軌道をスタートアップさせないといけぬ。リーダーシップが問われている。

このままでは、全国民がデジタルIDで●●の穴まで監視される超データ監視国家、データ収容所列島が誕生してしまう。若いカップルは、ますます子どもを産まない選択を強めるかも知れない。

◆現在の政治状況では何が起こるかわからない

政府は、マイナICカードを持たせる大政翼賛的なPRを展開している。「マイナICカードはデジタル化（DX）に必須の道具（ツール）だ」。「政府・公的機関へのオンラインアクセスにはマイナICカードを使った②PKI（公開鍵・電子証明書・電子署名）式のデジタルIDしかない」等々。こうしたフェイクで、国民をマインドコントロールし、³集团的ノイローゼ、に陥れている。国民全員に国内パスポートを常時携行させ、もっと邪悪なデータ監視国家をつくらうとしている。国の役人の悪巧みは、エスカレートする一方だ。

国や担当大臣などが、マイナカードというIC仕様の赤紙配付を、マイナポイントと地方交付税で操り、国民や自治体をあおっている。これに、あたかも戦時下のようにマスメディアが協力しているのも異様だ。マイナカードを持ち歩かない人は「国賊」だ。³国賊一家、には本来無料のはずの給食費などを有料にする。こんな総動員大好き、前時代的な自治体首長も現れる始末だ。山本一太郎群馬県知事や河村たかし名古屋市長など、保守良識派は、「どうかしている？」と見て、こうした首長の蛮行を糾弾している。

そもそも、マイナンバーは、現在国民民主党にいる古川元久議員らが旧民主党時代の旗振りをした愚策だ。彼らの構想は、いまやこの国を確実に権威主義国家に転落させている。責任は重い。

◆愚策のエスカレート：新型マイナカード配付計画

国の役人は懲りない。②PKI（公開鍵・電子証明書・電子署名）式の公定／実質国定の個人用デジタルIDをマイナンバーICカードに格納して配り、官民の垣根を越えてより包括的（オムニバス）に使わせようという不気味な政策を広げている。現在のマイナカードは、カードの表面に顔写真や氏名、住所、性別、生年月日（属性情報）が記載されている。しかし、こうした情報は内蔵されているICチップにも含まれている。諸外国では、モバイルIDアプリで、自分の個人情報が丸裸にならないように、本人の意思でストップをかけられるような仕組みが標準になりつつある。

しかし、国の役人は、こうした声には耳を貸そうとしない。政府は、2026年を視野に、新型のICカード導入を検討し出した。新仕様では、個人情報を見られたくない、または性別を載せたくないなどといった声にも配慮して、カードの表面に、こうした情報を載せないことを検討している。また、18歳以上の場合、「発行から10回目の誕生日まで」とされているカードの有効期限についても見直すとのことだ。

だが、国の役人は、ICカードのモバイル化の流れにいつまでそっぽを向いているつもりなのだろうか。わが国が、デジタルIDで、ICカードを使わない世界の流れの「抵抗勢力」になるのはみっともない。時代遅れのPKI（公開鍵・電子証明書・電子署名）式のデジタルIDに固執し、血税の垂れ流しを続けるのは止めないといけない。

◆急がれる人権エコシステムを盛り込んだデジタルIDの確立

わが国が、デジタル化（DX）の波を悪用し、中国のような専制主義国家を志向するのはいただけない。世界の民主国家陣営から相手にされなくなる。国の役人は確信犯であるとしても、民主国家でのデジタルIDのあり方について、政治家や自治体首長などのリスクリング（学び直し）が急務である。

コロナ禍を契機に、デジタルシフトは急激に進

んでいる。だが、デジタル化（DX）に悪乗りしたマイナICカードは、デジタルで人権エコシステムを破壊する（Digital disruption of human rights）邪悪なツールである！デジタル全体主義はご免である。西欧型民主主義国家を目指すとうたった憲法を持つこの国において、人権エコシステムを盛り込んだデジタルIDづくりは急務である。

Q & A : デジタル ID とは何か！

■はじめに

パソコン（PC）やスマホを使い、インターネットを使って遠隔（リモート）／オンラインでやり取りする空間／世界を、「デジタル空間／デジタルスペース」といいます。「サイバースペース／電脳空間」または「オンライン空間」ともいいます。これらの言葉は、ほぼ同じ意味と考えてよいでしょう。目に見えない（非対面の）「ネット空間」と言った方が分かりやすいかも知れません。（以下、「デジタル」、「オンライン」、「ネット」、「非対面」の言葉を同じに扱います。）

一方、対面、アナログでやり取りをする空間を「現実空間（real space）」、「リアル空間」といいます。（以下、「リアル」、「対面」、「アナログ」の言葉を同じに扱います。）

急激なデジタルシフト（Digital shift）が起きています。数年前まではリアル／対面／アナログが当たり前でした。ところが、コロナパンデミック（Covid 19）がグローバルに拡散して以降、デジタル／オンライン／ネット／非対面への急激なシフトが起きました。もちろん、デジタルシフトには、光と影があります。

デジタル化についていけない「デジタルデバイド（情報技術格差）」を抱える、あるいは「デジタルリテラシー（デジタルについて適切に理解し、自ら活用できる力／知見）」が十分でない市民・企業・教育機関・専門職などがたくさんいます。放置してはなりません。差別を助長する、あるいはついていけない個人や企業などがゾンビ化するからです。オンライン／デジタル化を強める納税手続や各種社会保障給付申請などではとりわけです。生存にかかわってきます。リスクリング（学び直し）の機会を保障することが大事です。同時に、リスクリングが至難な層への高配も忘れてはなりません。

小学校でのデジタル教育がエスカレートしてい

ます。大学その他の高等教育機関によるデータサイエンス（情報学）、デジタル関連学部・学科の新設ラッシュです。政府は東京 23 区の大学定員増、デジタル分野の学部・学科だけは例外的に認めるとの方針を打ち出しました。いずれ、小さいころからネットゲームの親しみ、スマートフォン（スマホ）、パソコン（PC）を駆使し暮らしてきた「デジタルネイティブ」、「スマホネイティブ」が社会の中核を占める時代がくるはずで

数年前に、関東圏のある大学の教室でリアル／対面／アナログの授業をしていたときの話です。4 月の最初の授業の日のことでした。年次の税制改正を織り込んだ改訂版の税法の教科書の発行が後追い、月末になるため、教科書を持っていない学生がほとんどでした。そこで、おおよそ 100 人位の受講生を前に、「パソコン（PC）やタブレット端末を持っている人は持参してきてください。教室のスクリーンに加え、ネットにアップし、学内 Wi-Fi を使い授業概要を教室内で各自の PC で受信できるようにします・・・」とアナウンスしました。次回の授業で、教室に PC を持参できた学生は 1 割程度。その後、教科書を使った完全なリアル／対面／アナログの授業に戻りました。ただ、学期末の授業アンケートには、「私は法学部に法律を学びにきたのだ。情報学部情報学、パソコンの使い方を学びに来たのではないのだ。先生は、何を勘違いしているのだ・・・！」といった類の「怒り、呪いの声」、多数のブーイングが寄せられました。

しかし、その後すぐに、コロナ禍を契機に文系は一気にオンライン／遠隔授業一辺倒になりました。その大学は、ハコモノ投資一辺倒から、巨額の IT 投資をし、いわば「通信教育中心」に大変身。大学も確実に IT 投資が勝敗を決める時代に入っているのです。ハコモノ投資一辺倒では勝負にならなくなっています。

あの当時ブーイングした法学部出の学生たちは、昨今の急激なデジタルシフトについていけているかどうか案じています。

同じころ、関東圏のある国立大学で大学院の授業を担当していました。授業は英語で、受講生もすべて留学生で、英語もデジタルもともにネイティブ、コロナ禍に対応したオンライン／遠隔開講は問題なしでした。ところが、大学当局から、大学の予算が限られるので、「今年度から非常勤教員は、Zoom の配信ツールを割当、利用できないことになった」との通知を受けました。「傭兵（非

常勤教員）には武器を供給しない。自前で武器や弾を調達して闘え！！」の指令です。

こんなデジタル差別に、私は大ブーイング。ところが、それを何とも思わない（できない？）、「丸で他人事」の正規雇用の教職員集団は、馬耳東風の姿勢でした。どこかの権威主義国家のような感じも・・・しましたが。ウクライナ戦争を見ても、とにかく「デジタルに強くないと闘いにならない！」のが現実です。

デジタルシフトの流れを重くとらえることは大事です。「デジタルなど●●くらえ！」を合言葉に、「デジタルデバインド（情報技術格差）」を権利として主張する、ネオラダイト運動（新たな機械打ち壊し運動／デジタル粉碎運動）をするのが正論なのか？再考の余地がありそうです。「どんとこい、デジタル！」の勢いがないと、仕事も社会活動などへの参加も困難になりかねません。

もちろん、あらゆる新しいものには独自の危険性があります。これまでなかった新たな脆弱性を生み出す可能性もあります。人権エコシステムに大きなインパクトを及ぼすデジタルシステムやインフラの構築（デザイン）をゆるしてはならないのは当たり前です。本題に戻ります。

◆ 「本人確認」とは何か

— 「本人確認」って何なのでしょう？「身元確認」、「本人認証」とはどう違うのでしょうか？やさしく説明してください。

「本人確認」、「身元確認」、「本人認証」といった言葉は、必ずしも、はっきりと区別されないで使われています。混乱がありますが、専門家の間では、一応、①本人確認＝②身元確認＋③本人認証といった形で区別して使われています。また、本人確認、本人確認証／カードは、一般に「ID／アイデイ」と呼ばれます。

「本人確認」は、これまでのリアル／対面／アナログの世界でも日常茶飯事に行われてきました。警察官に車を止められて「免許証を拝見させてください。」と言われて、対面で本人確認するのは、リアル／対面／アナログの世界、眼に見える世界での話です。

そこで、ここでは、まず、「リアル／対面／アナログ」と「デジタル／オンライン／ネット／非対面」に共通する「個人の本人確認をする場合のベーシックな仕組み（イロハ）」について、ふれておきます。

【表 1】個人の本人確認をする場合のベーシックな仕組み

<p>ひとくちに「本人確認」といっても、「個人（自然人）」と「個人以外（企業／団体）」とは異なります。個人（individual / natural person）の場合は、通例、次のようになります。</p>	
① 本人確認	<p>英語では「authorization」と言います。 ①本人確認は、以下の②身元確認と③当人認証を併せて行うことで完了します。</p>
② 身元確認	<p>英語では、「identification / identity proofing / identity verification / KYC=Know Your Customer」などといいます。②身元確認とは、①本人確認をする際に、氏名や住所、生年月日など「属性情報（attributes）」で本人確認をすることです。日本では、身元確認を、戸籍や住民票で行って来ました。例えば、運転免許証の発行や更新に住民票が必要なのは、確かに日本に居住しているという身元を確認するためです。アメリカなどでは、公共料金の支払領収書や第三者が身元確認をしたうえで契約した契約書情報などを身元確認に利用しています。</p>
③ 当人認証	<p>英語では「authentication」と言います。「本人認証」とも邦訳されます。③当人認証とは、当人しか知り得ないもしくは他人は知らない情報（ID やパスワード、秘密の質問など）、または当人だけの身体的もしくは生態的な（顔面／指紋／目の虹彩などの）特徴をもとに、所持する人が本人であると推測することです。例えば、運転免許証を所持している人の顔が免許証のある写真と同じか見比べることで、この免許証を所持する人は当人である」と確認することができます。最近話題になっているマイナンバー（国民背番号／個人番号）カードは、アナログ／対面の世界では、運転免許証と同じ機能を持ちます。</p>

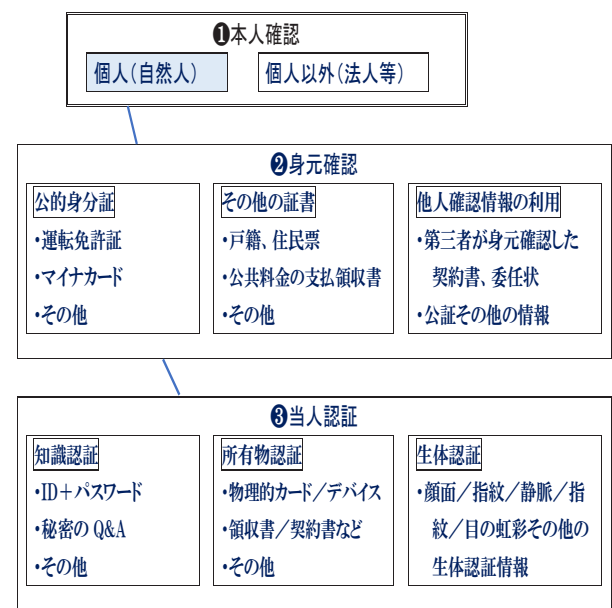
もう少し分かりやすく、図説すると、【表 2】のような感じです。

◆デジタル ID とは何か？

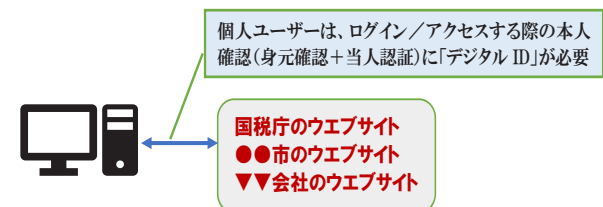
一 最近、よく「デジタル ID」という言葉を見聞きます。「デジタル ID」は、アナログ ID / リアル ID と、どう違うのでしょうか？

「デジタル ID」は、大きく「個人用」と「個人以外（企業／団体）用」に分けることができます。ここでは個人用について話します。個人用の「デ

【表 2】「本人確認」の仕組みをチャートで確認する



ジタル ID」とは、個人ユーザー（利用者）が、インターネットとパソコン（PC）またはスマホを使って、官民の機関のウェブサイト（ホームページ／デジタルプラットフォーム／ポータルサイト）にリモート（遠隔）アクセス／ログインする際に、①本人確認（②身元確認＋当人認証）するのに必要なツールを指します。



以前は、住民票の写しが欲しい場合には、市町村役場に出かけて行って、対面（リアル）で申請するのが常でした。もちろん、郵送での申請もできます。しかし、デジタルシフト／デジタル化が急激に進み、今日では、パソコンやスマホなどからオンライン（非対面）申請ができます。

また、電気やガス、上下水道代その他の公共料金の支払／銀行口座引落領収書、クレジットカードの利用額明細書なども、以前は紙／文書で通知を受けていました。しかし、今日では、デジタル／ネットでの通知が当たり前になってきています。

スマホで、アプリを使ってクレジット利用明細を見るとします。その場合、クレジット会社のウェブサイト（ホームページ／デジタルプラットフォーム／ポータルサイト）にアクセス／ログインするときには、ID とパスワード（2 段階認証）

を入れるか、さらにはネットワーク暗唱番号（3段階認証）をしないといけません。また、人によっては、ID やパスワードなどを覚え切れないということで、顔認証／顔パス（FaceID／FRT）技術を使うことになります。これが、まさに「デジタル ID（digital identity）」です。

ちなみに、住民票の写しのオンライン申請で、市町村のウェブサイトログインする場合のデジタル ID としては、法律で、マイナンバー IC カードに格納された PKI（公開鍵・電子証明書・電子署名）以外は使えない、ことになっています。民間 IT 企業がデザインした「ID + パスワード」式のデジタル ID は使えないとしています。官尊民卑、民業圧迫ではないか？との批判があります。後に詳しくふれます。

デジタル ID については、個人用のものが注目されています。しかし、個人以外用のデジタル ID も重要です。

一 確認させてください。「デジタル ID」といっても、さまざまな方式があるのですか？

そうです。「デジタル ID」は官民のウェブサイト（デジタルプラットフォーム、ポータルサイト）にリモート（遠隔）アクセス／ログインをする際に、なりすまし犯罪などを防ぐための本人認証（authentication）には必要なツールです。これは、個人用か個人以外（企業／団体）用かを問いません。データセキュリティ対策に使われる主な本人認証のための技術仕様とその特徴をおおまかにリストにして見ると、次のとおりです。

【図表 3】 デジタル ID づくりのデータセキュリティ対策で採用できる技術仕様

技術仕様	導入コスト	利便性	なりすまし対応度	マイナス面
① ID・パスワード	低	高	低	安全度が低い
② PKI（公開鍵・電子証明書）	中	低	高	運用が複雑
③ 生体認証（顔・虹彩・指紋など）	高	高	高	容認度が低い
④ 二次元コード	高	高	高	PC 対応に難あり
⑤ ワンタイムパスワード	高	高	高	コストが割高
⑥ ブロックチェーン	—	—	高	技術開発途上

わが国では、現在、国・自治体をはじめとした官のセクターでの個人向けデジタル ID の技術仕様としては、② PKI（公開鍵・電子証明書・電子署名）が使われています。ですから、国税庁のウェブサイト（デジタルプラットフォーム／ポータルサイト）である KSK システムにリモートアクセス／ログインする際のデジタル ID、データセキュリティ対策には、マイナ IC カードや税理士会の電子申告用 IC カードに格納された② PKI（公開鍵・電子証明書・電子署名）が使われているわけです。

一方、民間の金融機関のネットバンキングで、銀行のウェブサイト（デジタルプラットフォーム／ポータルサイト）に預金者がリモートアクセスする際のセキュリティ対策でのデジタル ID としては、⑤ ワンタイムパスワードが使われています。信販（クレジット）会社のウェブサイト（デジタルプラットフォーム／ポータルサイト）にスマホでリモートアクセス／ログインし、アプリを使ってクレジット利用明細を見るときには、どうでしょうか？デジタル ID として、①（アカウント）ID とパスワード（2 段階認証）を入れるか、人によっては、ID やパスワードを覚え切れないということで③ 生体認証【顔（顔パス）認証（FaceID）】機能を使うことになります。

わが国は、② PKI（公開鍵・電子証明書・電子署名）式の個人用公定／実質国定のデジタル ID をマイナンバー IC カードに格納して配り、オンライン／オフライン・官／民の垣根を越えてより包括的（オムニバス）に使わせようという不気味な政策を続けています。

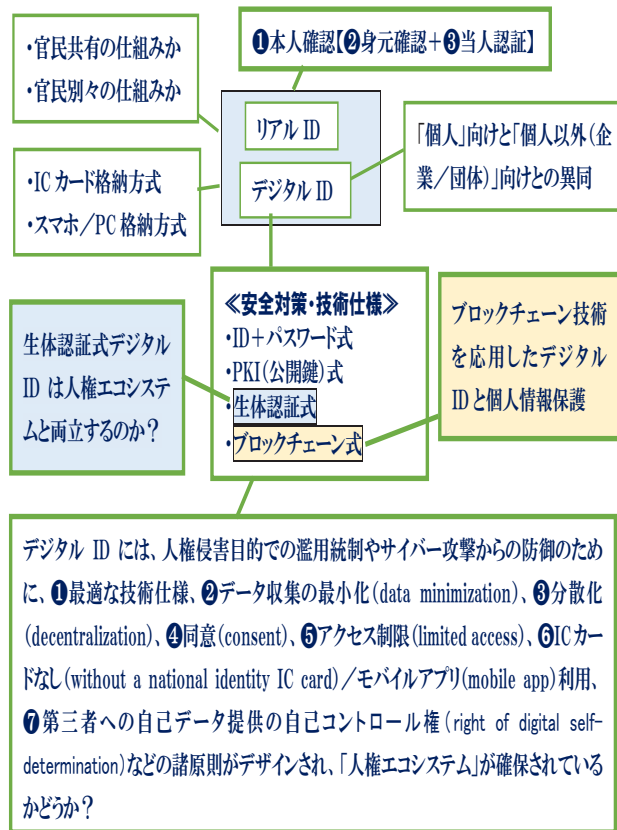
また、政府の計画では、個人用デジタル ID である② PKI（公開鍵・電子証明書）を、あらゆる行政分野に加え、民間セクターでの利用を拡大していく方針です。これは、裏返せば、マイナ IC カードで個人のあらゆる情報をデジタルで集約管理し、国家が監視できる体制の確立を目指していることになります。

◆ デジタル ID を取り巻く諸課題とは

デジタル ID を取り巻く課題はさまざまです。おおまかにまとめて見ると、【表 4】 のとおりです。

一 デジタル ID は、なりすまし犯罪対策には必須のツールのようにも見えます。それにもかかわらず、わが国では、PKI（公開鍵・電子証明書）が格納されたデジタル ID であるマイナ IC カードが

【表4】 デジタル ID を取り巻く諸課題



悪者扱いされています。なぜなのでしょう?

デジタル ID は、本来、ウェブサイト（デジタルプラットフォーム／ポータルサイト）に安全にアクセス／ログインする際の当人認証（authentication）のツールなはずですが、しかし、デザイン／技術仕様の選択の仕方によっては、他のさまざまな邪悪な目的に使うことができます。言いかえると、正義に資するデザインの仕方／最適な技術仕様の選択が行われないと、デジタル ID は、安全対策（ネットセキュリティ）に使うこともできるし、人権弾圧のための「凶器／デジタルトラップ（罠）」にもなり得るわけです。まさに、デジタル ID に、人権エコシステムがデザインされているかどうかと問われるところです。デジタル ID を選ぶとします。この場合には、個人用には、人権に最もインパクト（影響）の少ない技術仕様を選ぶ必要があります。

ネットセキュリティ（安全対策）と名打ったわが国の PKI（公開鍵・電子証明書・電子署名）式のデジタル ID を装ったマイナ IC カードは、個人が、オンライン（非対面）／オフライン（対面）申請の際の当人認証ツールとして使われるだけではありません。マイナ IC カードは、安全対策（データセキュリティ）を「偽旗／ニセ旗」に、不正義なデザイン・技術仕様を選択すれば人権侵害ツ

ルに悪用できます。国民監視用の国内パスポート、健康保険証データの自動徴兵選別、社会保障給付対象選別、信用スコア制度（social credit system）などへの悪用が適例です。

「デジタル ID の危険は使われ方」が問われます。アメリカの学者は、デジタル ID の「デザインの不正義（design injustice）」と呼んでいます。個人用のデジタル ID は、いかに「効率性」に役立つとしても、人権エコシステム（human rights ecosystem）が確保されないと「凶器（weapon）」になります。デジタル ID が、地球上に全体主義をまき散らすツール／凶器になることはゆるぎのないのです。

「デザインの不正義（design injustice）」という言葉は、「外部不経済（external diseconomies）」のような言葉と同様に、一般にはなじみが薄いかも知れません。

◆わが国のデジタル ID とは

ー IC 仕様のマイナンバーカード／マイナカードは、さまざまある「デジタル ID」の 1 つなのですね？

すでにふれたように、リアル／対面／アナログ／オフラインでやり取りをする空間を「現実空間／リアル空間（real／physical sphere）」といいます。現実空間での物理的な身元確認（physical identification）のための公的身分証を「リアル ID」とも呼びます。個人用のリアル ID としては、久しく運転免許証、健康保険証、介護保険証などが使われてきました。

2003 年からは、対面（リアル／オフライン）と非対面（オンライン）双方に対応できる「住基カード（住民基本台帳カード）」が導入されました。これは、一種のデジタル ID といえます。IC カードの PKI（公開鍵・電子証明書・電子署名）の技術仕様が格納されオンライン（ネット）とオフライン（対面）とで使えるデザインでした。しかし、「デジタルシフト」の大波が起きず、普及せず、廃止されました。その後 2016 年からはマイナンバー（個人番号）カード（マイナカード）が交付されました。

わが国では、例えば、個人が所得税の電子申告（e-Tax）をする際には、原則としてマイナカードが必要です。つまり、納税者が自宅のパソコン（PC）から国税庁のデジタルプラットフォーム／ポータルサイトである国税総合管理（KSK）シス

テムにリモート（遠隔）アクセス／ログインするとします。この場合には、その納税者（本人）のマイナ IC カードが必要です。

一方、税理士に代理人申告をお願いするとします。この場合には、代理人となった顧問税理士は、税理士会発行の IC カードを使って国税庁のウェブサイト／KSK システム（デジタルプラットフォーム／ポータルサイト）にアクセス／ログインし、ゲート（門）を通過することになります。マイナ IC カードや税理士会が発行する税理士用電子申告用 IC カードには、PKI（公開鍵・電子証明書・電子署名）の技術仕様を使った本人認証（authentication）の仕組み、つまり「デジタル ID」が格納されています。

税理士に頼むほど難しい計算も要らないので、自分で電子申告（本人申告）をします。しかし、マイナ IC カードの取得には抵抗があり、いまだ持っていないとします。このままでは、国税庁の KSK システムにログインできません。ログインの際の本人認証では、② PKI（公開鍵・電子証明書・電子署名）式の技術仕様の利用を原則としているからです。しかし、これでは、個人所得税の電子申告は進みません。

そこで、国税庁は、納税者が望めば、特例として、①（アカウント）ID・パスワード式の技術仕様だけのデジタル ID の利用を認めています。つまり、② PKI（公開鍵・電子証明書・電子署名）という本人認証（authentication）の仕組みを使わなくともいい、としています。ただし、最寄りの税務署で対面確認を受け必要な届出が必要です。マ

イナ IC カードが普及するまでの特例としています。

マイナカードの場合、IC カード面には、12桁の背番号が記載されています。この番号は、リアル／対面／アナログ／オフラインで本人を監視するには役立ちます。しかし、デジタル／オンライン／ネット／非対面／遠隔での本人確認、とりわけ本人認証には、もっと精巧なデジタル ID が必要です。安全対策（ネットセキュリティ）、すなわち、ネット犯罪、ハッカー対策、なりすまし（identity theft）などへの対策が要るからです。

デジタル ID には、① ID + パスワードの技術仕様を使うモデル／デザインから、データの暗号化／復号化ができる② PKI（公開鍵・電子証明書・電子署名）の技術仕様を使うモデル／デザイン、さらに高度なブロックチェーン（暗号資産）のようなハイテクな技術仕様を使うモデル／デザインが考えられます。

デジタル ID は、ユーザー（利用者）が、インターネットを通じて、官民を問わずさまざまな機関のウェブサイト（デジタルプラットフォーム／ポータルサイト）にリモート（遠隔）アクセス／ログインし、ゲート（門）を通過するために必要なツール（道具）です。

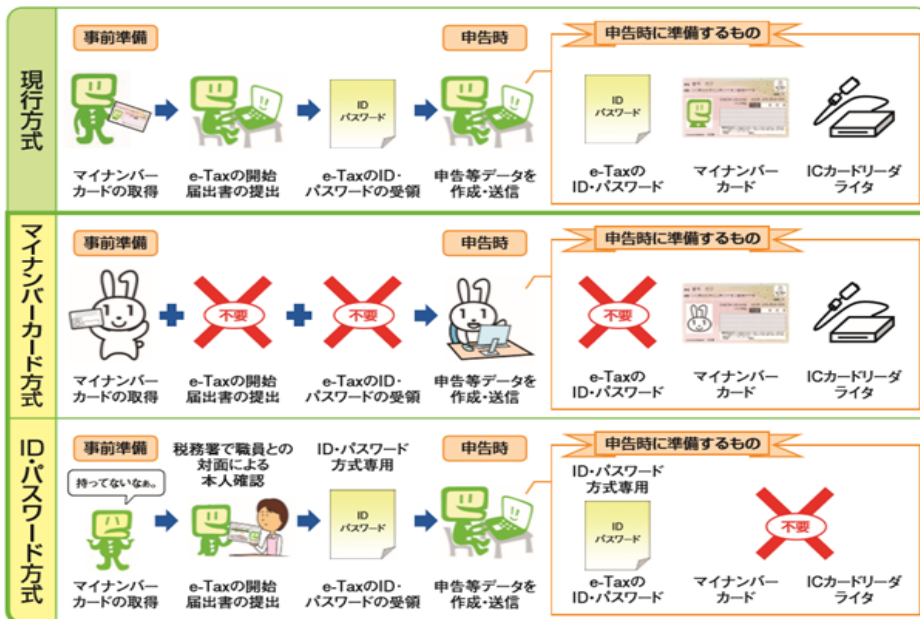
デジタル ID を、わが国のように IC カードに格納するモデル／デザインか、アメリカやオーストラリアなどのように IC カードを使わないで、ネットを通じてモバイル ID アプリを取得するモデル／デザインかは、国によって異なります。

現在のマイナカードは、カードの表面に顔写真や氏名・住所・性別・生年月日など（属性情報）が

記載されています。リアル ID として、オンラインに加えてオフライン（対面）でも使えるようにするためです。しかし、こうした情報は内蔵されている IC チップにも含まれています。IC カードは、紛失・悪用の可能性があり、プライバシー保護やなりすまし犯罪対策などでは大きな問題があります。

そこで、政府は 2026 年を視野に、新しいカードの導入を検討しています。新仕様では、個人情報を見られたくない、ま

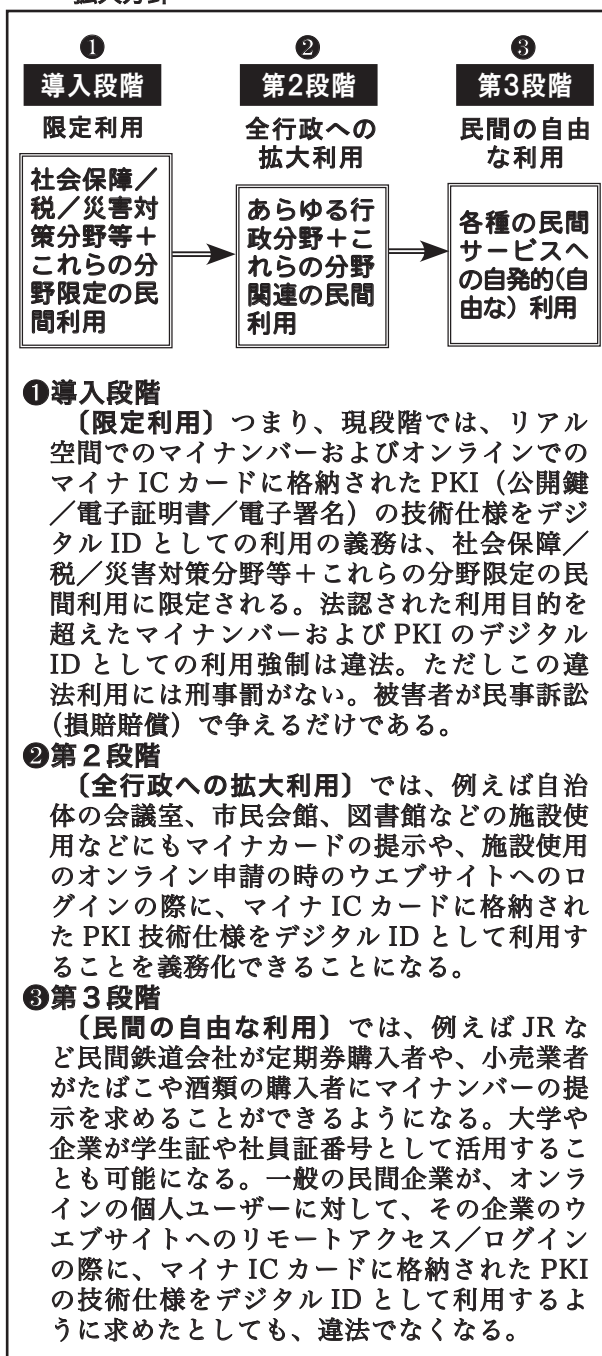
【表 5】 所得税の電子申告では 2 つのデジタル ID の選択が可能



たは性別を載せたくないなどといった声にも配慮して、カードの表面に、こうした情報を載せないことが検討されています。また、18歳以上の場合、「発行から10回目の誕生日まで」とされているカードの有効期限についても見直すことが想定されています。

しかし、諸外国では、物理的なICカードにPKIの技術仕様のデジタルIDを格納する方式を採っていません。また、新たにデジタルIDを導入する国でも、デジタルIDを物理的ICカードに格納する方式の採用を止めています。ICカード紛失に伴うプライバシー漏洩などの危険性を回

【表6】政府のマイナンバー／PKI式デジタルIDの利用拡大方針



避し、さらにはスマホなどモバイル端末の普及でICカードに頼らない、モバイルIDアプリを使う動きが加速しているからです。

デジタルIDは、いまや①アカウントID・パスワードをベースに③生体認証〔顔面（顔パス）・指紋（タッチID）〕の技術仕様を加えた方式が世界標準です。モバイルIDアプリを使えば、ユーザーが自分の個人情報が丸裸にならないように、本人の意思でデータ利用に制限をかけられるようになります。日本の国の役人が構想する自称「新型(?)」のICカードは時代遅れ（旧式）なのではないでしょうか？国の役人は、ガラパゴス化したデジタルIDの技術仕様に固執し、血税の垂れ流しを続けようとしているようにしか見えません。

モバイル化の嵐が吹きまくり、アメリカ、イギリス、オーストラリアなどの諸国で見られるように、物理的な国民背番号ICカードに頼らない個人用のデジタルIDがグローバルな流れです。わが国のマイナカードのようなICカードへの依存、利用分野の拡大は、国民の徹底監視には悪用できますが、見方によっては時代遅れの愚策に映るわけです。

わが国では、国の役人が主導して、国民をリアル（対面）とデジタル（非対面）双方で監視できる包括的（オムニバス）なツールのマイナICカードの取得を強要しています。「デジタルID」の意味などそっちのけです。まともな説明もしないのです。担当大臣のファンティックな姿を見ると、どこか全体主義に猛進する権威主義国家のトップに似ています。時代の流れへの順応、発想の転換、ができないのです。ポイントの人参で大衆をマインドコントロールし、国民を集団的なノイローゼ常態にしています。こうやって、過去にも、国民を悲惨な敗戦まで導いて行ったのでしょうか。

◆頓挫した東京渋谷区での民間活力を生かした個人向けデジタルID

一 東京都渋谷区では、民間IT企業が開発した個人用デジタルIDを使った簡便な住民票のオンライン申請の仕組みを導入したのに、国が待ったをかけ、潰してしまったそうです。もう少し詳しく教えてください。

マイナンバーICカード（マイナICカード）を使ったオンライン申請は、スマホなどオンライン端末では、使い勝手が悪いわけです。そこで、東京都渋谷区は、2022年1月から、住民が、住民票の写しや印鑑証明書、納税証明書をオンライ

ン申請し、同区のウェブサイト／ポータルサイトにログイン／アクセスする際に、デジタル ID として民間 IT 企業が開発した ID・パスワードをベースに LINE Pay の顔認証（顔パス）の技術仕様を加味した公的個人認証サービス [モバイル ID アプリ] を利用することにしました (https://app.box.com/s/z9uc3ezb7d2htz2v vm7e3yio04buog0f)。しかし、国が「待った！」をかけたのです (https://www.soumu.go.jp/main_content/000681028.pdf)。

総務省は、住民が住民票のオンライン申請で、市町村のウェブサイトログインの際のデジタル ID としては、マイナ IC カードに格納された PKI（公開鍵・電子証明書・電子署名）以外の技術仕様を使うのは罷りならぬ、ということです。

2020 年 9 月 10 日に、東京都渋谷区にデジタル ID サービスを提供していた民間 IT 企業（株式会社 Bot Express）は、国（総務省）を相手に

「ラインを用いたオンラインの請求サービス適法確認」を裁判所に求めて裁判を起こしました。勇気ある元気なスタートアップ企業です (https://app.box.com/s/hbcw665urwsaas3w6wr582 j08e56ema7)。

東京地裁は、2022 年 2 月 8 日に、行政追従の消極的司法の姿を露わにした判断をくだし、原告 IT 企業の訴えを認めませんでした（東京地判令和 4 年 12 月 8 日判決・東京地判令和 4 年（行ウ）第 344 号）。

◆アメリカで採用するデジタル ID とは

一 アメリカのデジタル ID の特徴は、個人用や個人以外（企業／団体）用のデジタル ID として、官民双方の部門とも、日本でマイナ IC カードに格納されて使われている PKI（公開鍵・電子証明書）の技術仕様をデジタル ID に採用していない

コラム

官尊民卑、市場主義を知らない総務省横やり＋消極司法で潰された東京渋谷区独自の民間デジタル ID 利用プラン

東京都港区にある Bot Express 社が LinePay のアプリをベースに新たなデジタル ID を開発・販売しました。同社のデジタル ID では、スマホで撮影した顔写真付き身分証とスマホのカメラで写した本人の容貌を送信、AI（人工知能）がそれらを照合し、本人と確認できれば住民票の写しを後日、区が郵送する手順になっています。AI による判別がつかなかった場合は区の職員が目視で確認して、住民票を提供することになっています。金融機関で顧客が口座開設の際に利用するなど、オンラインで身元確認が完結する「eKYC (electronic Know Your Customer)」という技術仕様と同じです。ちなみに、こうした技術仕様のデジタル ID は、モバイル時代の今日では世界基準です。欧米諸国では常識です。

東京都渋谷区は、2020 年 4 月に、同社のデジタル ID を導入し、同区のウェブサイトログイン利用できるようにし、住民票のオンライン申請を始めました。しかし、同サービスの開始直後、総務省が「待った！」をかけました。

総務省は、2020 年 4 月 3 日に、全国の市町村への「技術的助言」として、事実上同様のサービスを採用しないよう求める通知をしました。住民票の交付には厳格な本人確認が必要であり、マイナンバーカードに搭載した PKI（公開鍵・電子証明書・電子署名）の技術仕様よりも性能が劣る eKYC の採用は「適切でない」というのが理由です。

総務省は、2021 年 9 月には、この通知にあわせて、住民票の写しの交付に関連する省令（住民基本台帳の一部の写しの閲覧並びに住民票の写し等及び除票の写し等の交付に関する省令の一部を改正する省令）を改正しました。これにより、オンライン申請のウェブサイトへのログインの際の本人認証には、マイナンバー IC カードに搭載された PKI 式のデジタル ID しか認められないとしました。民間 IT 企業のデジタル ID を使った渋谷区のオンライン申請は法令違反とする規定を設け、同社のデジタル ID の自治体への売込みを停止に追い込んだわけです。Bot Express 社は、総務省の画策により、他の自治体へのサービス展開が事実上できなくなりました。そこで、2020 年 9 月 10 日に、同社は、総務省（国）の通知は違法であるとして、東京地裁に提訴しました（総務省提訴のお知らせ | Bot Express (bot-express.com)）。

東京地裁は、2022 年 12 月 8 日の判決で、LINE 申請では偽造された本人確認書類でも審査を通過する可能性があるとしたうえで、「不正の手段がひとたび確立されれば住民基本台帳制度の根幹への信頼が揺らぐことになりかねない」と指摘しました。厳格な本人確認は、行政の IT 化を推進するデジタル手法とも整合するとししました（東京地判令和 4 年 12 月 8 日判決・東京地判令和 4 年（行ウ）第 344 号）。

ようです。それでは、アメリカのデジタル ID は、官民双方の部門でのデジタル ID としては、どのような技術仕様を採用しているのでしょうか？

アメリカのデジタル ID で使われている技術仕様は、「(アカウント) ID・パスワード式」あるいは「ID・パスワード+生体認証式」です。これらをベースとしたバージョンアップ方式です。もう少し分かりやすくいえば、先ほど紹介した東京都渋谷区が住民票のオンライン申請で導入したデジタル ID [モバイル ID アプリ] を活用した方式です。

先般、知合いの IT 法務専門のアメリカ人弁護士と配信ツール Skype でオンライントークをしました。その際に「東京地裁が、行政機関が提供する一定のサービスへのオンライン申請では、公定/実質国定の PKI (公開鍵・電子証明書) 式のデジタル ID 以外の利用が罷りならぬ」として、「民間デジタル ID を使うのは違法とした!」と伝えました。そうしたら、「日本の司法は権威主義国家の司法のようですね」と驚いていました。そういわれて見れば、「民間活力、民主導の資本主義」を知らない、官尊民卑の司法の姿が浮き彫りになってきます。わが国でも、弁護士を体験しないと裁判官に任官されないアメリカ司法のデザインを採り入れないと、民間活力を知らずに、行政追従の消極司法が続くのではないかと危惧します。

わが国は、② PKI (公開鍵・電子証明書・電子署名) 式の公定/実質国定の個人用デジタル ID を物理的なマイナンバー IC カードに格納して配り、オンライン/オフライン・官/民の垣根を越えてより包括的 (オムニバス) に使わせようという監視資本主義につながるような不気味な政策を続けています。

連邦議会にも、「アメリカでも官民共通の個人用デジタル ID が必要ではないか?」という声もあります。しかし、PKI (公開鍵・電子証明書) 式のデジタル ID を格納し、国民総背番号 IC カード (National ID / IC カード) を持たせるようなモデルには幅広い支持が得られる可能性はまったくありません。自由権、人権を大事にする国柄です。人権エコシステムを欠き、全体主義、権威主義国家に通じるツール (道具) はご免だ、となるわけです。

データセキュリティの高いデジタル ID が要るとしても、アメリカでは、公定/実質国定、官製の仕組みではコンセンサスが得られません。「民業圧迫だ!」、「官尊民卑そのもの!」、「民間活力を使え!」の大合唱になるわけです。

— アメリカでは、デジタル ID 「デザインの不正義 (design injustice)」が問われていることですが、どういうことでしょうか? もう少し、IT 弱者にもわかるように、説明してください。

アメリカには、1935 年に導入されたアナログの社会保障番号 (SSN=Social Security Number) があります。また、SSN を申請した人には、「紙」製の社会保障番号カード (SSN card) が発行されています。これは、「リアル ID」です。



(public use)

この SSN カードは、電子申告 (e-File) その他電子申請の際に課税庁 (IRS) など連邦政府 (行政) 機関のウェブ

サイト (デジタルプラットフォーム/ポータルサイト) にリモートアクセス/ログインする際に、デジタル ID としては使えません。

ですから、アメリカでは、電子申請などで各種行政機関のウェブサイト (デジタルプラットフォーム/ポータルサイト) にリモートアクセス/ログインするには久しく、アカウント ID とパスワード (2 段階認証)、さらにはネットワーク暗証番号または Q&A (3 段階認証) などを使ってきました。

— アメリカの 9 ケタの社会保障番号とわが国の 12 ケタの個人番号とはどう違うのでしょうか？

アメリカの 9 ケタ社会保障番号と日本の 12 ケタの個人番号 (マイナンバー) の利用について、大きな違いが現れるのは、行政機関相互間での情報連携 (データマッチング / data matching) のときです。わが国では、住基ネット訴訟最高裁判決 (2008 [平成 20] 年 3 月 6 日判決・民集 62 卷 3 号 665 頁) の影響もあり、行政機関のデジタルプラットフォーム (ポータルサイト) 相互間では、情報連携に、直接個人番号 (マイナンバー) を使っていません。個人番号から組成された符号 (暗号) を使っています。これに対して、アメリカの行政機関のデジタルプラットフォーム (ポータルサイト) 間での情報連携には、直接、社会保障番号が使われています。

マイナンバーを問う争訟などでは、個人番号は、リアル ID としての使われ方と、符号化されデジタル ID としての使われ方がある点を憶えておくことは大事です。この違いを織り込んで論理構成

し、手続を進める必要があります。

— もう一度確認します。アメリカでは、例えば連邦の個人所得税の電子申告／オンライン申告や各州での失業保険（雇用保険）のオンライン申請に、ユーザーは、IC カードに格納された公開鍵（PKI）式のデジタル ID を使っていないのですか？

先ほども少しふれたところです。アメリカでは、個人用のデジタル ID には公開鍵（PKI）の技術仕様を使っていません。それから、連邦（国）は、わが国のような物理的なマイナ IC カードを発行するようなことはしていません。スマホ全盛時代に、カードリーダー必須の IC カードに頼るデジタル ID 政策はありません。ひとことでいえば「愚策」です。

例えば連邦個人所得税の確定申告を電子申告（e-file）、オンライン申告するとします。この場合、わが国のマイナンバー（個人番号）や法人番号に相応する社会保障番号（SSN = social security number）や雇用主番号（EIN = employer identification number）を電子ファイルに記載することになります。しかしすでにふれたように、個人の社会保障番号（SSN）カードは紙製です。アナログ時代のツール（道具）です。IC カードではないので、公開鍵（PKI）のような技術仕様のデジタル ID を格納することはできません。

わが国のような国の傘下にある公的機関（地方公共団体情報システム機構／略称 J-LIS）が、公開鍵を格納する IC カードを全国民に対して発行するのは、権威主義国家のデジタル中央集権的な構想みたいなものです。民主主義・市場主義・分権主義を重視するアメリカでは、到底受け入れられません。

それに、国家が物理的な IC カードを国民全員に配付する発想も、明らかに時代遅れだからです。スマホ全盛時代に入り、物理的な IC カードがガラパゴス化するのは目に見えています。これは、商業 IC カードのモバイル化の流れを見れば一目瞭然です。血税の無駄遣いです。仮に PKI（公開鍵）式のデジタル ID を採用するにしても、スマホに直接格納の方が安心・安全なわけです。カード面に個人情報が入った盛りの物理的な IC カードは紛失・悪用の危険があります。

こうした危ないカードは、国定身分証明書として国民全員に持たせるのは、あらゆる国民データを一元監視する権威主義国家づくりには便利でしょう。そのうち、警察官が IC カードリーダーを持って街中を徘徊し出すでしょう。実質全国民に GPS を装着させるに等しいわけで、マイナカー

ドが見つからないと、お使いにも出られない社会が待っています。

日本の国の役人は、わが国が他国から侵略を受け、こうした整然と管理された膨大な国民データが敵の手に渡ったらどうなるのかなど、地政学リスクには考えが及ばないのでしょうか。平和ボケし、「ポイントの人参の方が大事！」で空騒ぎするレベルの国家と国民なわけです。私は、ミサイルよりも、マイナシステム／デジタルプラットフォームに「国家安全保障」と「人権エコシステム」をどう組み込むかが、もっと大事だと思います。しかし、大半の国民も政治家も、未来を読む力が育っていないのです。先の敗戦では、占領軍の実働部隊が民主政体を維持する国からやってきたことが、不幸中の幸い、のようにも見えます。

— わが国トップのアップル社 CEO へのマイナカードスマホ搭載懇願の愚！

アップル社のティム・クック CEO が来日し、2022 年 12 月 16 日に、岸田首相を表敬訪問しました。その際、首相は、アップル社のスマホに、マイナカードに入れている公定／実質国定の PKI（公開鍵）式のデジタル ID を直接格納できるようにしてほしいと懇願した、と報道されました（<https://jp.reuters.com/article/kishida-apple-idJPKBN2T0059>）。

しかし、CEO は即答を避けたようです。背景には、アメリカでは官製（国定）の PKI（公開鍵）方式のデジタル ID をスマホに格納するデザインをすんなりと許容できる環境にないことがあります。これは、最近、ツイッター社やメタ（フェイスブック）社など巨大 IT 企業が SNS（交流サイト）向けのデジタル ID を有料発行する政策を発表しています。ここに、アップル社の CEO が明確な回答を避けたヒントがありそうです。

また、すでにふれたように、総務省は、2020 年 9 月に、東京都渋谷区が住民票のオンライン申請システムに、民間 IT 企業（Bot Express）が開発した公定／実質国定の PKY ではない技術仕様を個人用デジタル ID に採用することに異論を唱えました。その後法令改正をし、同区が民間スタートアップ企業とタッグを組んで始めた獨創性に富んだオンライン申請システムを潰してしまいました。国のやり方は、権威主義国家の発想です。市場主義、民主主義の価値観にそぐわないやり方です。もちろん「名ばかり地方自治で当り前」の姿勢でバッコする国の役人に、交付税で首根っこ

をつかまれ、国の言いなりの数多くのひ弱な自治体の側にも問題がありそうですが。ここにも、アップル社の CEO が明確な回答を避けたもう 1 つのヒントがありそうです。

いずれにしろ、このような民間 IT 企業が開発・販売する独創性に富んだ個人向けデジタル ID の利用を、一部業務にしろ国家のすべての政府・公共ポータルサイト／ウェブサイトで排除してしまうことは解せません。デジタル ID は、本来、ウェブサイトに安全にアクセス／ログインする際の本人認証 (authentication) のツールなはずです。いろいろな技術仕様のデジタル ID があり、民間活力を生かし、切磋琢磨できて当たり前なわけです。

アップル社 CEO は、むしろ「日本政府は、公定／実質国定のデジタル ID ではなく、アップル社など民間 IT 企業が開発したデジタル ID を積極的に活用すべきだ!」、「民業圧迫だ!」と感じたのではないのでしょうか。何事についても役人主導の役所社会主義に毒され、市場主義・民主主義の価値観を共有できていないこの国のトップの発言に驚いているかも知れません。

◆アメリカで問われたデジタル ID 「デザインの不正義」

ー アメリカのコロナ禍対策支援金給付は、オンライン申請が原則だったようですが?

まず、アメリカのコロナ禍対策支援金のオンライン申請手続よりも、アメリカでの個人に対するコロナ禍対策支援金の基本について少し話したいと思います。

トランプ政権下で、連邦議会は、新型コロナウイルス感染症関連緊急事態経済対策で、巨額の財政支出をしました。2022 年 3 月から 4 月末 (第 1 弾～第 4 弾) までだけで、あわせて 5 兆ドル (当時の換算で 500 兆円) 規模に達しました。

第 3 弾 (Phase3) の新型コロナウイルス感染症支援・救済・経済安定化法 (CARES Act=Coronavirus Aid, Relief, and Economic Security Act / 通称「ケアーズ法」は、2022 年 3 月 27 日に成立しました。

ケアーズ法では、個人向けに、【表 7】のような給付措置が講じられました。

ケアーズ法で、世帯支援給付金 (わが国の特別定額給付金に相当) の支給事務は、連邦課税庁 (IRS) が担当しました。

IRS は、連邦所得税を毎年確定申告をしている

【表 7】主な個人向けコロナ禍対策支援金給付措置

失業保険増額給付への財政支出 (2,500 億ドル (当時の換算率で約 25 兆円)) 【一部わが国の休業支援金に相当】

《休業支援金の概要》

各州の失業保険給付に加え、別途、連邦から週あたり 600 ドル (6 万円) を、最長 4 カ月間、加算給付。また、失業保険の受取期間を 13 週間に延長する。さらに、通常では失業保険給付を受けられないフリーランサーや雇用類似の働き方をするギグワーカーなど、いわゆる「名ばかり個人事業者」、「一人親方」も支給対象に織り込む。

《給付申請手続の概要》

失業保険 (UI) 事務は連邦と州との共管。アメリカの失業保険制度は、連邦の社会保障法 3 章 [失業補償行政についての州への補助] と連邦失業保険税法 (FUTA tax =Federal Unemployment Tax Act) を典拠に、州の失業保険法に基づいて運営されている。管理運営主体は、連邦労働省と各州の職業安定機関である。財務省は、連邦課税庁 (IRS=Internal Revenue Service /内国歳入庁) を通じて社会保障税連邦失業保険税法 (FUTA tax) を徴収する事務を担当している。FUTA tax は雇用主に課税される。年間給与総額 7,000 ドルまでに対し 0.6% (州失業保険税を払っている場合。払っていない場合は 6.0%)。コロナ禍対策休業支援金は、各州の職業安定機関に対するオンライン申請が原則。

世帯支援 (Economic Impact Payment / Individual Recovery Rebates in the CARES Act) (3,010 億ドル (当時の換算率で、約 30 兆 1,000 億円)) 【わが国の特別定額給付金に相当】

《世帯支援の概要》

個人に 1,200 ドル (12 万円) [夫婦に 2,400 ドル (24 万円)、子供 1 人につき 500 ドル (5 万円)] の現金支払い [ただし、単身で年収 75,000 ドル (750 万円) / 夫婦で年収 150,000 ドル (1,500 万円) 以上の場合は減額調整あり]。

《給付申請手続の概要》

連邦財務省の外局である内国歳入庁 (IRS / 連邦課税庁) が事務を所管。2019 年度の確定申告 (2020 年 4 月 15 日 / コロナ特例で 7 月 15 日まで延長) を終えていない場合で、その間に子供が生まれているときには、受給者 / 納税者は、2020 年度の確定申告で調整する。IRS は、受給者 / 納税者が、2018 年度、2019 年度の確定申告している場合には、その情報に基づいて審査して、受給者 / 納税者の銀行口座に振込か、または銀行口座を利用して納税または還付請求していないときには小切手を郵送する。一方、課税所得がないために確定申告をしていない人は、受給にあたり IRS の公式ウェブサイト (HP (Non-Filers:

Enter Payment Info Here <https://tinyurl.com/sz91387>)でオンライン申請が必要。支援金は課税対象。

人は、納税者の社会保障番号 (SSN) その他個人情報情報を把握しています。ですから、IRS は自動的に世帯支援給付金の銀行口座振込や小切手送金ができます。しかし、所得がなく確定申告をしていない低所得者は、IRS への受給申請が必要になります。この場合は、オンライン申請が原則です。

つまり、世帯支援給付金に関するオンライン申請は、所得がなく納税申告をしていない人たちに限られたわけです。そして、オンライン申請での本人確認では、民間の IT 企業・ID.me 社が開発したデジタル ID の利用を求めました。

一 アメリカの連邦課税庁 (IRS) が、本人確認 (個人用) のデジタル ID に採用した民間 IT 企業が開発した「ID・me」について教えてください。

デジタル ID はデータセキュリティ対策上必要不可欠なツールです。ただ、すでにふれたように、本人認証の技術仕様／デザインはいろいろです。主なものでも、① ID + パスワード、② PKI (公開鍵・電子証明書・電子署名)、③ 生体認証 (顔・虹彩・指紋など)、または①+②、①+③、①+②+③などのアラカルトがあります。

アメリカでは、政府・公共機関がオンラインサービスで使うデジタル ID の技術仕様選びでは久しく、活発に議論されてきました。デジタル ID の導入では民間 IT 企業の活力を最大限に生かすことでは各界は一致しました。しかし、デジタル ID の「デザイン」、つまりどのような技術仕様を採用するかでは、「コンセンサス」、着地、ができていません。

玉突きで、連邦課税庁 (IRS=Internal Revenue Service / 内国歳入庁) でも、どのデジタル ID (技術仕様) を採用するのか、その決定が遅々として進んでいませんでした。納税者が電子申告 (e-file) などで、自分ら IRS のウェブサイト (デジタルプラットフォーム / ポータルサイト) にオンライン / リモートアクセス / ログインする際にデータセキュリティ (安全) を確保するために必要なデジタル ID の決定がずっとできないでいたわけです。

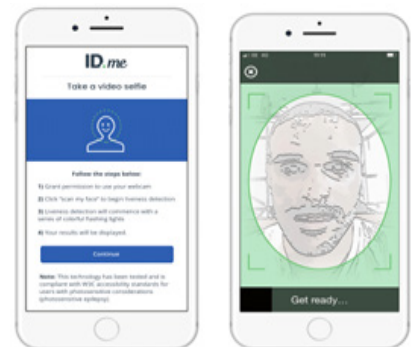
そうしているうちに、他人の社会保障番号 (SSN) を悪用したなりすまし還付申告が日に日に深刻になっていきました。連邦政府は、民間 IT 企業が開発・販売する Login.Gov / ログイン・ドット・ガブという商標のデジタル ID の採用を薦めていました。しかし、Login.Gov の評判は今一つでした。

2021 年になって、ようやく IRS は独自で決断しました。IRS が採用したのは、民間 IT 企業が開発した「ID.me (アイデー・ドット・ミー)」という商標のデジタル ID [モバイル ID アプリ] です。ID.me は、アカウント ID・パスワードなどをベースに、本人認証に顔面認証 (顔パス) 式を採用したモデル / デザインです。いわゆる「eKYC (electronic Know Your Customer)」と同じ技術仕様をベースにしたものです。

ID.me のデジタル ID では、ユーザーは、アカウントを開く段階で、ログインには、アカウント ID やパスワードなどに加え、次のうち、複数 (2~3) のアナログ身元確認証の写しデータを入力します。

- ① 各州が発行する運転免許証をはじめとした連邦または各州の政府発行の写真付き身元証明書、
- ② 旅券、③ 出生証明書、④ 所得税の源泉徴収票 (Form W-2)、⑤ 社会保障カード、⑥ 退役軍員健康保険証、⑦ 国土安全保障省信頼できる旅行者カード、⑧ スマートフォン自撮り動画、⑨ 光熱費請求書、⑩ 保険請求書、⑪ 電話代請求書、⑫ ID.me 従業者との動画面接記録

加えて、スマホやパソコン (PC) のウェブカメラを使って自撮りした写真画像 (selfie image) の提出を求めるデザインです。



(public use)

ちなみに、オンライン申請者が、ID.me のデジタル ID を使って IRS のウェブサイトログインしたとします。この場合、申請者がログインの際に提出した各種自撮り写真 / 顔認証 (顔パス) データは、ログインに成功してから 24 時間以内に、また、ビデオチャット動画データは、ログイン成功から 30 日以内に、消去されています (IRS-When will my selfie, video and biometric data be deleted?-ID.me Help Center)。

◆アメリカで問題化した顔パス認証式「ID.me」

一 わが国では、「米国では、アメリカ版マイナンバー (個人番号) である社会保障番号 (SSN) を

駆使して各種のコロナ対策支援金の給付はスムーズに行われた」と報道されました。問題はなかったのでしょうか？

わが国のメディアによっては、「アメリカでは、アメリカ版マイナンバーである社会保障番号 (SSN) があつたから各種のコロナ対策支援金の給付は混乱なく、スムーズに進んだ。」と報道しました。しかし、これは、オンライン申請の仕組みを良く調べない、あるいは知らないでの報道です。明らかにフェイクニュース (偽情報) です。

失業保険 (UI=unemployment insurance) の一環として各州が支給した「休業支援金」や連邦課税庁 (IRS) が給付事務を担当した「特別定額給付金」では混乱を極めました。

コロナ禍対策での休業支援金や特別定額給付金は、感染対策もあり、オンライン申請が原則でした。州当局や連邦課税庁 (IRS) などのウェブサイト (デジタルプラットフォーム/ポータルサイト) にはオンライン申請が殺到しました。

ところが、各州の当局や IRS は、リモートアクセス時の本人認証 (authentication) に、民間 IT 企業が開発したデジタル ID である顔認証 (顔パス) 式の「ID.me」を採用していたことがアダとなりました。誤認証、長時間の応答不能など、殺到する本人認証に ID.me システムが適切に対応できなかつたのが原因でした。州当局のウェブサイトへのログインに成功するには、何日も要した申請者が大量に出ました。

IRS も、ウェブサイト独自の「ID.me ヘルプセンター」を立ち上げ、押し寄せるカスタマーに対応を急ぎました (IRS & ID.me-ID.me Help Center)。

【表 8】アメリカの民間の 2 大デジタル ID プロバイダー

<p>① ID.me / アイデー・ドット・ミー 【ID.me 社】</p> <p>ID.me の創設者、ブレイク・ホール (Blake Hall) CEO [最高経営責任者] は、米陸軍の元特殊部隊所属。特殊部隊で同僚だったマシュー・トンプソン (Matthew Thompson) と共同で、2010 年に、ID.me の前身であるトループスワップ (TroopSwap) 社を設立した。この会社は、除隊者向けの電子商取引 (EC) サイト。退役軍人であることを認証したユーザーに対し、提携業者が割引販売をするアフィリエイト・マーケティングを展開。その後、社名を ID.me に変更。政府・公共機関のウェブサイト (デジタルプラットフォーム/ポータルサイト) にオンラインでリモートアクセス/ログインする際のデジタル ID の開発、</p>

生体認証・動画チャット技術を活用した個人の本人認証 (authentication / authentic ID) に特化したサービスを展開。民間企業のウェブサイトにも幅広く利用されている Google やフェイスブックのワンクリック・ログインなどとは差別化。ID.me 社 [モバイル ID アプリ] のユーザー数は 3,900 万人で、ARR (年間経常収益) は 6,500 万ドルを超える。アメリカでもっとも注目されているユニコーン企業【時価総額が 10 億ドル以上で、株式未公開 (未上場) のベンチャー企業] の 1 つである。ID.me 社の評価額は、法人向けのデジタル ID サービス (IDaaS=Identity as a Service) を提供するオクタ (Okta) 社の時価総額に比べるといまだ小さい。

② Login.Gov / ログイン・ドット・ガブ 【レキシスネキシス (LexisNexis) 社】

アメリカ大手 IT のレキシスネキシス (LexisNexis) 社は、2017 年に、政府機関が立ち上げたウェブサイト (デジタルプラットフォーム/ポータルサイト) にオンラインでリモートアクセス/ログインする際のデジタル ID [モバイル ID アプリ] を開発、個人の本人認証事業を開始。連邦総務庁 (GSA=General Services Administration) は、2017 年 12 月に、政府/公共機関向けデジタル ID [モバイル ID アプリ] の開発・導入で、レキシスネキシス (LexisNexis) 社を含む 2 つの IT 企業との間で、3400 万ドルの契約を交わした。

レキシスネキシス (LexisNexis) 社が開発した Login.Gov / ログイン・ドット・ガブ [モバイル ID アプリ] の方式は、アカウント ID + パスワード式 + 顔パス (顔認証)。

政府のウェブサイトには、ユーザーの氏名や電話番号、身分証明書の画像で本人のアカウントにログインするデザインである。

ー アメリカの個人用デジタル ID としては「ID.me」より選択はないのでしょうか？

すでにふれたように、ID.me の顔認証の技術仕様 (FRT) を使ったデジタル ID が大きな問題になったのは、2022 年にいたってからのことです。コロナ禍対策の失業保険 (UI) の一環として各州が支給した「休業支援金」や連邦課税庁 (IRS) が所管した「特別定額給付金」のオンライン申請が急増したことが原因です。ID.me 社が、急増するリモートアクセス/ログイン申請者の本人認証に迅速かつ適切な対応ができなかつたことがきっかけでした。

オンライン申請は、コロナ感染対策の給付金の迅速な処理で即戦力になるはずでした。しかし、その期待は大きく外れたのです。

アメリカでは、連邦総務庁 (GSA=General

Services Administration) は、個人がオンライン申請で、連邦政府／公共機関のウェブサイト（デジタルプラットフォーム／ポータルサイト）にログインする際のデジタル ID [モバイル ID アプリ] を用意しています。連邦総務庁（GSA）は、デジタル ID として、「Login.gov」を指定しています。現在、連邦社会保障庁（SSA=Social Security Administration）をはじめとした 20 程度の連邦政府・公共機関が採用しています。

Login.gov は、IT 企業 LexisNexis Risk Solutions が開発した①アカウント ID + パスワード式をベースに②自撮り写真 [顔認識 (顔パス) 技術 (FRT)] でユーザーのアカウントを認証できる仕組みです。ID.me 社のデジタル ID とほぼ同じ技術仕様です。しかし、Login.gov のデジタル ID では、世論や議会の動きを注視し、現在②自撮り写真 [顔認識 (顔パス) 技術 (FRT)] を使っていません。

連邦総務庁（GSA）の長官は、2021 年現在で 3,000 万人のユーザーが Login.gov のアカウントを持っており、政府・公共機関での Login.gov のデジタル ID の導入が進めば、さらにその数は増えるだろうと語っています。

しかし、連邦や諸州の主な政府・公共機関は、Login.gov のデジタル ID の採用には消極的です。理由は、ID.me より利便性が劣る、と見ているからです。

Login.gov のデジタル ID [モバイル ID アプリ] は、パソコン (PC) があり、英語が話せることを前提にデザインされています。つまり、ある程度のデジタルリテラシーがある人たちを標準にデザインされているわけです。このため、デジタルデバイスや英語の問題を抱える社会的・経済的に弱い立場にある人たちがパソコン (PC) が不得手だが、スマホは得意のスマホネイティブには評判が今一つなのです。

【表 9】アメリカのデジタルデバイス/デジタルリテラシー「水準」を理解する。

アメリカ人の：

- ① 20% がスマホを持っていない。
- ② 25% 自宅にブロードバンド / Wi-Fi がつながついていない。
- ③ スマホもパソコン (PC) も持ってない人が、他人のスマホもしくはパソコン (PC)、または公共施設のパソコン (PC) を使った場合には、本人認証 (authentication) ができず、個人情報も漏れ漏れになる。

[E.A. Vogels, Digital divide persists even as Americans with lower incomes make gains in Tech adoption, Pew Rsch. Ctr. (June 22, 2021)]

一 求められる誰にも使い勝手のよいデジタル ID

アメリカのみならず多くの国々でも、政府・公共サービスを利用する際に、その機関のウェブサイトログインするデジタル ID [モバイル ID アプリ] としては、ID.me と類似したデザインを採用しています。いわば、デジタル ID の国際標準です。すでにふれたわが国の東京都渋谷区にデジタル ID サービスを提供していた IT 企業 (株式会社 Bot Express) のデジタル ID [モバイル ID アプリ] も、ID.me と類似したデザインです。国際的なセキュリティ基準は、米国立標準技術研究所 (NIST) が定める基準をほぼ満たしています。

本人確認の仕組みは、インターネットやアプリを使えない人たち、あるいはこれらを使いたくない人たち向けにオフライン (対面) でも利用できる方法を提供する必要があります。アメリカは、広大な国土で英語を母国語としない大量の移民を抱える国です。誰一人取り残されない、人に優しいデジタル化、オンライン (デジタル / ネット) サービスも利用できるように政策を練るのは大変な作業になります。まさに、「言うは易く行うは難し」です。

例えば、連邦課税庁 (IRS) のような政府機関のウェブサイトのユーザー (利用者) の規模は、巨大 IT 企業 (Tech Giants) のユーザーの数に匹敵します。

ID.me 社は、ネット上に支援センター (Help Center) を開設しています。ユーザーは、有人ビデオ (動画) チャットで、配置されたビデオ通話担当者 (Video Chat Agent) 【同社では「Trusted Referee」と呼ぶ】と対話することもできます。

加えて、インターネット接続ができないデジタルデバイス (情報技術格差) のある人たち向けに、対面 (オフライン) で本人確認ができるようになっています。ID.me 社によると、同社が開設する対面で本人確認できる場所 (対面登録所) は全米 650 か所あるということです。この数でも、広大な国土にしては、少なすぎるわけです。

一 連邦課税庁 (IRS) のその後

コロナパンデミックのさなか、2022 年 3 月に成立したコロナ禍救済をねらいとした連邦のケアーズ法では、連邦課税庁 (IRS / 内国歳入庁) が、世帯支援金 (わが国の特別定額給付金に相当) 支給事務を担当しました。納税申告や還付申告している人は、IRS に世帯支援金の申請をしなくとも、自動的に金融口座振込ないし小切手が郵送されます。しかし低所得で無申告の人は、IRS にオンライン申

請をしないと、この世帯支援金をもらえません。

オンライン申請では、IRS は、同庁のウェブサイト にログインする際のデジタル ID [モバイル ID アプリ] として ID.me を採用しました。広く連邦政府が採用するとしているレキシスネクシス (LexisNexis) 社が開発を手掛けている Login.gov のデジタル ID [モバイル ID アプリ] を採用しませんでした。理由は、Login.gov のデジタル ID では自撮り写真 [顔認識 (顔パス) 技術 (FRT)] の利用を避けており、IRS はネットセキュリティに今一つ自信を持ってなかったからです。

一方、IRS が採用した ID.me のデジタル ID では、本人認証で自撮り写真 [顔認識 (顔パス) 技術 (FRT)] を使っています。ネットセキュリティのレベルは高いのですが、このことが原因で、逆に人権団体や連邦議会議員から厳しい批判を浴びました。

批判を受けて、ID.me 社は、デジタル ID で、アカウント ID + パスワード方式の基本は継続しましたが、自撮り写真 [顔認識 (顔パス) 技術 (FRT)] の使用を暫定的に止めました。デジタル申請者は、顔パス (顔認証) に代えて、有人ビデオ (動画) チャットで済ますことができることにしました。(ただ、ID.me 社の幹部によると、IRS のオンライン申請には、有人ビデオ (動画) チャットは使っていないとのことですが…) どちらが正しいかは定かではありません。いずれにしろ、2023 年にいたっても IRS のオンライン申請における顔認証 (顔パス) 技術の暫定停止はいまだ解かれていません。

連邦のケアーズ法による個人向けコロナ禍対策支援金給付では、不正給付申請防止が重い課題でした。2023 年 2 月 8 日に、連邦政府検査院 (GAO=Government Accounting Office) は、コロナ対策の一環として各州の失業保険給付当局が所管した失業保険増額給付 (わが国の休業支援金に相当) で、少なくとも 600 億ドルもの不正受給があった旨の見積を公表し、改善を求めました (Unemployment Insurance: DOL Needs to Address Substantial Pandemic UI Fraud and Reduce Persistent Risks | U.S. GAO)。

ただ、この報告では、給付金のオンライン申請に、ID.me 社のデジタル ID を使ったことで、不正受給が増加したのか、減少したのかは、明らかにしていません。

一 アメリカの連邦や州の政府・公共機関は、今回のコロナ対策「休業支援金」、「特別定額給付金」

のオンライン申請の体験を通じて、「人権エコシステム」を組み込んだうえで、迅速な給付と不正受給防止の双方に資するデジタル ID を、どうデザインしたらよいかで、苦悩していると聞きますが？

今日、アメリカでは、連邦や諸州のさまざまな政府・公共機関が、各種行政サービスその他の公共サービスの提供で、対面 (オフライン) 申請からオンライン (ネット) 申請) に大きく舵を切っています。

これは、国土が広大なアメリカでは、コストパフォーマンスを考えると、対面/オフライン/アナログで本人確認できる数多くの場所 (リアルのコタクトポイント) の設定が難しい事情があるからです。また、働いても貧しい人たち (the working poor) をはじめとした社会的弱者に、迅速に必要なサービスを提供するには、オンライン申請にした方がフレンドリー (優しい) という読みもあります。

オンライン (ネット) 申請では、住民・納税者は、パソコン (PC) やタブレット端末、スマホを使って、必要な機関のウェブサイト にアクセス/ログインすることになります。この場合、ウェブサイト へのアクセス/ログインには、まず本人確認 (身元確認+本人認証) 手続きをしなければなりません。

これまでは、ID + パスワードで本人確認をするような比較的簡素な技術仕様が採られてきました。しかし、サイバー犯罪、すなわち、なりすまし (identity theft) やハッカーが横行するようになり、本人確認を厳格にしなければならなくなりました。正確かつ効率的な「デジタル ID」の必要性です。

わが国のように国や国が操る機関が全国共通の官製のデジタル ID を【マイナ IC カードに PKY / 公開鍵 / 電子証明書を格納する形で】導入するのも一案です。しかし、アメリカでは、こんな官主導の政策は支持されません。専制主義国家のような仕組みを嫌う国民性があるからかも知れません。いずれにしろ、わが国のように「何をするにも国の役人がつるんで、横並びで」の発想は、アメリカの民主主義では好まれないのです。

多くの連邦や州の機関は、効率的なデジタル ID として、勢いのある民間 IT 企業 (ID.me 社) が開発した顔認証 (顔パス) 方式の「ID.me」の導入を進めました。現在、ID.me 社のデジタル ID への需要が旺盛です。このことがアダとなり、逆に、個人向けのデジタル ID 市場での寡占化やそれに伴うイノベーションの停滞が心配されるところです。いずれにしろ、連邦や州の機関は「効

率的なデジタル ID で効率的な行政サービス」が合言葉です。ところが、そうはいかなかったのです。

原因は、政府・公共機関のサービス、とりわけ今回のコロナ禍対策の各種給付金では、オンライン申請者に社会的・経済的に弱い立場の人たちが多く、しかも、デジタルデバイド（情報技術格差）問題を抱えた人も多かったからです。

[See, Michele E. Gilman, 'Me, Myself, and My Digital Double: Extending Sara Green's Stealing (Identity) from the Poor to Challenge of Identity Verification,' 106 Minn. L. Rev. Headnotes 301 (Spring, 2022)]

大規模災害などの場合は、コロナ禍の事例とは異なり、通信インフラが被害を受けます。通常のオンライン申請は機能しない可能性もあります。逆に、オフライン（対面）申請、あるいは本人確認を柔軟にしたオンライン申請が必要になるかも知れません。まさに、細緻な「人権エコシステム」を組み込んだ迅速な救済に向けたオンライン申請に必要なデジタル ID のあり方が問われます。

◆ EU ではブロックチェーン技術活用のデジタル ID 検討も

一 欧州連合 (EU) の、デジタル ID の法的枠組みについて教えてください。

わが国は、② PKI（公開鍵・電子証明書・電子署名）式の公定／実質国定の個人用デジタル ID をマイナンバー IC カードに格納して配り、オンライン／オフライン・官／民の垣根を越えてより包括的（オムニバス）に使わせようという監視資本主義につながるような不気味な政策を続けています。こうしたデジタル ID の政策は、EU を参考にしたデザインともいわれています。

EU は、デジタル ID として、久しく② PKI（公開鍵）の技術仕様を採用してきました。しかし、時代は、スマホ全盛です。商業 IC カードでもモバイル化の流れは止まりません。デジタル ID は、スマホに直接格納する[「モバイル・デジタル ID (mobile digital ID)」／「デジタルウォレット (digital wallet)」]、あるいは④ ブロックチェーン技術を実用化したデジタル ID への転換の検討を始めました。

2017 年にエストニアの国民総背番号システムがサイバー攻撃を受け、IC チップ管理機能が不全になったことも 1 つの契機となったのです。人口約 133 万人弱の都市国家エストニアで、約 75 万の IC カードが利用不能となり、正常化に当局

は多大な時間を費やしました。わが国の政府系マスメディアなどが持ち上げる IC カードを使ったエストニアの国民総背番号システムは、以外と脆弱だったのです。

これを機に、エストニア政府も、サイバー攻撃からの対応を重視し、② PKI 技術を格納した IC カードを使った既存の中央集約管理システムを、ブロックチェーン技術を実用化し分割管理型のデジタル ID の仕組みに移行することも検討し始めました。

EU のデジタル ID は、「EU 市場内取引の電子認証およびトラストサービスに関する規則 (Regulation on electronic identification and trust services for electronic transactions in the internal market)、通称「イーアイダス規則 (eIDAS regulation / EU 規則 No 910 / 2014)」に拠っています。イーアイダス (eIDAS) 規則は 2014 年に成立し、2016 年 7 月より施行されました。イーアイダス (eIDAS) 規則は、1999 年に施行された電子署名に関する指令 (eSignature Directive 1999 / 93 / EC) に置き換わるものです。EU 全域にわたる電子署名の法的枠組みと、電子署名、タイムスタンプ、e シールなどを含む新たに定義された「トラストサービス」の範囲を定めています。EU 加盟国内における電子取引に関する信頼性やセキュリティを保護するために設けられた法的規則です。

ちなみに、EU の「指令 (directive)」と「規則 (regulation)」の違いを憶えておいてください。「指令 (directive)」は、加盟各国が国内法を制定して始めてその国で効力を有します。これに対して、「規則 (regulation)」は、各加盟国の国内法の制定の有無とは関係なく、直接 EU 全域に適用になります。

一 2021 年に、EU は新しいデジタル ID の構想を提案したようですが？

2021 年 5 月 28 日に、EU の執行機関である欧州委員会 (EC) は、「信頼ありかつ安全な欧州 e-ID 規則 (A trusted and secure European e-ID Regulation)」の制定を提案しました (<https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation>)。この提案は、新たなデジタル ID を構想し、EU での導入を目指したものです。

まず、この 2021 年デジタル ID 規則 (e-ID Regulation) が提案された背景を少し説明します。

DX 時代に対応しようということで、EU の欧

州委員会 (EC=European Commission) は「2030 デジタルコンパス：あなた方のデジタル 10 年 (2030 Digital Compass : Your Digital Decade)」をアナウンスしました [2030 DIGITAL COMPASS: YOUR DIGITAL DECADE | Futurium (europa.eu)]。

このなかで、欧州デジタル ID の確立などを含めた構想を明らかにしました。例えば、2030 年までに、すべての主要な公共サービスをオンラインで利用できるようにしよう、すべての EU 市民が電子カルテにアクセスできるようにしよう、80% の EU 市民がデジタル ID を使用できるようにしよう。こうした目標が盛り込まれています。

この構想は、2014 年に成立し、2016 年 7 月より施行されたイーアイダス (eIDAS) 規則を基礎としています。このイーアイダス (eIDAS) 規則は、EU 域内での加盟国の国境を越えた電子認証、ウェブサイト認証基盤 (インフラ) の確立を目的とするものです。すでに EU 市民のおおよそ 60% がこの恩恵を受けています。

しかし、イーアイダス (eIDAS) では、各加盟国がデジタル ID を開発し、他の加盟国のものと相互利用できるようにすることは目標とされていませんでした。これが原因で、各国間で格差や齟齬が生じていました。今回の構想・提案は、現行の枠組みを改良し、その恩恵を公的機関のみならず民間企業やモバイル利用にまで拡大することを狙っています [See, Peeter Vihma, The (bumpy) road to European Digital Identity (Sep.21,2022)]。

— 2021 年デジタル ID 規則 (e-ID Regulation) で提案されたデジタル ID とは、こういった特徴のものなのでしょうか？

2021 年デジタル ID 規則 (e-ID Regulation) で、欧州委員会 (EC) は、EU のすべての市民、居住者、企業が利用できるオムニバスな欧州デジタル ID の枠組みを提案しました。市民は、スマートフォン (スマホ) 画面にタッチするだけで、欧州デジタル ID ウォレット (EDIW=European Digital Identity Wallet) [モバイルアプリ] から自分の身元を証明し、電子データを共有することができるようにしよう。欧州市民は、EU 全域で認識される各国のデジタル ID を使ってオンラインサービスにアクセスできるようにしよう。アマゾンをはじめとした一定規模以上のプラットフォームには、年齢証明などで、ユーザーの求めに応じて欧州デジタル ID ウォレット (EDIW)

の利用ができるような対応を求めよう。欧州デジタル ID ウォレット (EDIW) の利用自体は、任意、常にユーザーが選択できるようにしよう。こうした提案が盛り込まれています。

— IC カードは使わないのですか？

IC カードは使いません。当然、欧州デジタル ID は、時代の流れを見据えて、スマホに格納できるモバイル化したデジタル ID [モバイルアプリ] です。わが国の時代の流れを読もうとしない国の役人が提案している新型の (フェイク? ガラパゴス化した?) 物理的な IC カードは使わないデザインです。

一方、わが国では、ポイントの人参でゾンビ化したマイナ IC カードを配っている集団ノイローゼの光景です。本当に日本の将来が心配になります。物理的な IC カードがないとスマホにデジタル ID を「写経」、できないデザインは明かに時代遅れです。いまやモバイル ID アプリを直接スマホに格納できるデザインが国際基準です。

政府の「日本は技術立法を目指す！」はフェイク、ニセ旗作戦に見えてしまいます。

— で、欧州のデジタル ID は、こういった使い方ができるのですか？

デジタル ID 規則 (e-ID Regulation) によると、各加盟国は、市民や企業に、求めがあれば、欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] を提供し、公的デジタル ID を他の個人属性 (運転免許証、卒業証書、銀行口座など) の証明と結びつけることができるようになります。欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] は、加盟国が承認すれば、政府・公的機関の各種プラットフォーム (ウェブサイト/ポータルサイト) のみならず、民間企業のプラットフォームにアクセス/ログインする際のデジタル ID として使うことができます。

新しい欧州デジタル ID ウォレット [モバイルアプリ] により、すべての EU 市民は、統一したデジタル ID の利用が可能になります。さまざまなデジタル ID を使う煩雑さを回避することができます。また、個人データを必要以上に共有したりすることなく、オンラインサービスにアクセスできるようになります。このソリューションでは、各ユーザー自身がどの個人データを提供し相手方と共有するかの決定することができるようになります。

欧州デジタル ID は、EU 市民の域内でも自由

な移動を促進すると見られています。フランス人がドイツで家を借りるあるいは職に就くとします。この場合の本人確認が容易になります。また、コンビニで酒類を買うとします。その際には、厳密には年齢確認だけが必要になります。欧州デジタル ID は、物理的な IC カードはなく、モバイルアプリとしてスマホに格納されます。ですから、年齢だけを提示することも可能になります。他の個人情報は相手方に見せないこともできます。自分の情報をどれだけ、誰と、何の目的で共有するかは、自分で決める、自己コントロールすることができるわけです。

このように、EU 市民は、民間機関との取引において、個人データの保護面で高レベルの保護を期待できます。加えて、政府・公共機関の納税申告書の提出など国や自治体とのやりとりや、EU 内の大学に入学する際に公的な身分証明書、としての利用なども検討されています。欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] は、空港でのチェックインからレンタカーの利用まで、あらゆるサービスにデータを保存・利用できるなどの事例が示されています。ただし、その利用はあくまでも消費者の選択に委ねられます。これは、欧州デジタル ID / 欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] 構想は個人情報の自己コントロール権は保障されているデザインだとはいうものの、懐疑的な声もあるからです。トータルな監視につながるとして、こうした構想に異論を唱える EU 市民に配慮するためです。確かに捜索令状があれば、各国政府当局は、該当者の欧州デジタル ID ウォレット (EDIW) の中身を調べることもできるわけです。「悪いことしなければ怖がることはない」の論理だけでは納得しない EU 市民も少なくないと思います。(それに、スマホなどモバイル端末を持たない人は、デジタル ID を利用できないわけですから、当然、任意とならざるを得ません。)

手短かにまとめると、欧州デジタル ID / 欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] は、次のような特徴を持っているといえます。

【表 10】 欧州デジタル ID / 欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] の特徴

<p>①利用を希望する個人や企業は誰でも利用できる</p> <p>欧州デジタル ID / 欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] の利用は任意です。希望する EU 市民、EU 域内の居住者、EU 域内の企業は、誰でも利用できます。</p>

②官民のオンライン取引で幅広く利用できる

欧州デジタル ID / 欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] の利用は任意です。希望する EU 市民、EU 域内の居住者、EU 域内の企業は、誰でも利用できます。

③提供する個人データを自己コントロールできる

欧州デジタル ID / 欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] では、ユーザー(利用者)は自分の ID、データ、および証明書のどの部分を第三者と共有するかを選択でき、共有状況を追跡することもできます。ユーザー自身が第三者に提供するデータを自己コントロールすることで、共有する必要のある情報のみが共有できるようになります。モバイルアプリで、自分の個人情報が丸裸にならないように、本人の意思でストップをかけられるようにする。

いずれにしろ、ユーザーが第三者に提供するデータを自らコントロールしながら利便性を享受するデザインは、グローバルな流れです。人権エコシステムを組み込んだデジタル ID であることの最低の基準になっています。

一 欧州デジタル ID / 欧州デジタルウォレットの構想は実現しそうなのでしょうか？

EU の欧州委員会 (EC) は、欧州デジタル ID / 欧州デジタル ID ウォレット (EDIW) [モバイルアプリ] の構想をできるだけ早く実現させようとしています。

欧州委員会 (EC) は、加盟国に対し、2022 年 9 月までに共通のツールボックスを確立することになっています。このツールボックスには、技術的なアーキテクチャー、標準、ベストプラクティスのガイドラインなどが含まれます。

2022 年 10 月から合意されたツールボックスを公開し、パイロットプロジェクトが開始されているはずで。

それから、欧州委員会 (EC) は、立法プロセスと並行して、欧州デジタル ID / 欧州デジタル ID ウォレット (EDIW) の技術的面で加盟国や民間企業と協力を推進していきます。欧州委員会 (EC) は、デジタル欧州プログラムを通じて、各加盟国に対して欧州デジタル ID 枠組みへの参加を支援することになっています。多くの加盟国は、検討に前向きです。

一 アメリカと EU との競争問題もあるように感じますが？

確かに、EU は、アメリカの巨大 IT 企業 (Tech Giants)、GAF A などと競争できるような EU 独自の個人・企業共用のデジタル ID (eID solution) の開発を目標にしています。また、「プライバシー」と「利便性」という 2 つの利益のバランスをどう保つか慎重に検討を進めています。デジタル ID は、デザインの仕方を誤れば国民総背番号制につながります。また、官製の臭いの強いオムニバスのデジタル ID / デジタル ID ウォレット構想では、民間活力を奪うという指摘もあります。

EU では、アメリカを「新自由主義の国」と見て、官依存の方がベターとする考え方も広く支持されています。EU を離れたイギリスの行方も気になるところです。

EU には、デジタル ID / 欧州デジタル ID ウォレットのあり方でも、北米・コモンロー諸国とは別の道を行くべきだとする意見も強いところです [EU, Commission proposes a trusted and secure Digital Identity for all Europeans (Feb.1, 2021)]。

コラム

新たなデジタル ID の管理方法とデジタル ID ウォレット (EDIW, e-ID wallet)

現在のデジタル ID の管理方法は、「外部に預ける」が主流です。ところが、個人のアイデンティティ (ID) は、その個人自らがコントロールすべきであるとする考え方があります。「自己主権型アイデンティティ (SSI=Self sovereign Identity)」と呼びます。

個人情報 の 自己コントロール権と重ねてイメージすると、分かりやすいのではないのでしょうか。

デジタル ID について、例えばわが国では、個人以外、つまり「企業 / 団体」は、どの方式を選ぶかは選択ができます。ところが、個人はそれができません。個人は、国や自治体の一定のポータルサイトへのログインには、公的 / 実質国定の PKI (公開鍵・電子証明書) 方式以外のデジタル ID の使用は罷りならぬ! となっています。裁判所までこのおかしい規制にお墨付きを与えています。

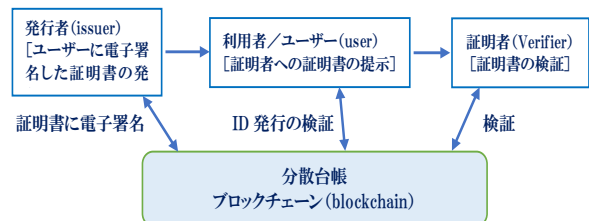
23 年のマイナンバー改正法で、今後は法改正をしなくも役人の舌先三寸でこの公定 / 実質国定のデジタル ID の利用範囲を強制できるようになります。まさに「止まらない、止められないマイナバンデミック」なわけです。なぜ個人だけが PKI (公開鍵) 以外の他の方式のデジタル ID の選択ができないのか、大きな疑問符がつくわけです。しかも、国は、国民に対して、公定 / 実質国定のデジタル ID の入った IC カードまで半ば強制しているわけです。モバイル化が進み、IC カードは時代遅れになってきているにもかかわらずです。解せません。

アメリカは、デジタル ID については、個人用も、企業用も、PKI (公開鍵・電子証明書) 式を採用していません。わが国のような公定 / 実質国定のデジタル ID を IC カードに入れて利用を強制するような政策はとっていません。コンセンサスが得られません。動機が不純だ、行き過ぎた監視資本主義だとして嫌われます。ですから、個人・企業双方とも、デジタル ID として、IC カードが要らない民間 IT 企業が開発したアカウント ID + パス

ワード (+FRT)、eKYC を採用しています。EU も、今後でき上る予定の欧州仕様のデジタル ID [モバイルアプリ] の利用を、市民や企業に促していますが、あくまでも任意です。しかも、IC カードは使わず、モバイルデバイス、スマホに入れて使えるデザインです。イギリスもそうです。

ただ、日本も、アメリカも、EU も、デジタル ID は、公的なデジタル 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」管理する方法です。こうした管理方式のデジタル ID は、「サイロ型デジタル ID」とか、「フェデレーション型デジタル ID」と呼ばれます。これに対して、「自己主権型アイデンティティ (SSI)」では、デジタル ID を官または民のプラットフォームに預けない方式です。

つまり、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 を管理するというデザインです。ブロックチェーン (分散台帳 / 暗号資産) 技術を実用化した次世代型デジタル ID は、官または民のプラットフォームのいない、自己主権型アイデンティティ (SSI) が主流になるとの見方もあります。



それから「デジタル ID ウォレット (EDIW, e-ID wallet)」[モバイルアプリ] ですが、「電子 ID 財布」とも直訳できます。デジタル ID ウォレットは、「個人データ保存 (PDS) アプリ (personal data store app)」、「モバイル・ウォレット・アプリ (mobile wallet app)」とも呼ばれます。ス

マホなどにこのアプリをインストールして、その中に入れたデジタル ID と紐づけしてさまざまな電子データ【銀行口座・納税・住民登録変更・公共サービス・国家資格・学歴など】を連携させて保存・活用しようというものです。

EU などでは、デジタル ID ウォレットを「官」主導で進めようとしています。一方、アメリカやイギリスなどでは、アップル・ウォレット (Apple Wallet) のように、「民」主導で進めようとしています。

一方で、デジタル ID ウォレットを、管理者 (プラットフォーム / ID プロバイダー) のいない、ブロックチェーン (分散台帳 / 暗号資産) 技術を活用した自己主権型アイデンティティ (SSI) を使ってデザインし実現しようとする動きが強まっています。

国の役人が何から何まで口をはさむのが日本で

す。国民を自立・一人にさせておこうとしないのです。この国では、「自己主権型アイデンティティ」ではなく、政府主導で「情報銀行」という第三者預託型のデジタル ID と紐づけ / 電子データ連携モデルを探っています。何となく「第三者」と聞くと、プライバシーが護られるような響きがあります。しかし、「情報銀行」にアクセス / ログインする際の個人のデジタル ID に公定 / 実質国定の PKI (公開鍵) (マイナンバーから組成された識別子) の利用しか認めないとすると、国はいつでも覗き見ができます。こんなプライバシー公有化の構想に賛成する人はいるのでしょうか? 「情報銀行」構想は、デザイン不正義、人権エコシステムを欠いたデジタル ID の典型的な使われ方につながりかねません。[Adrian Doerk, Digital Identity Wallet: A place for your self-sovereign identity (Jun 20, 2021)]

◆ 2023 年、イギリスも IC カードを使わない新デジタル ID 採用

— 「Brexit」を旗印に、EU (欧州連合) から離脱したイギリス (UK) では、デジタル ID でも、独自路線を走ろうとしているのでしょうか?

イギリスは、2021 年 1 月 1 日に、EU から離脱しました。デジタル ID でも、EU とは独自の道を行くことになりました。離脱前から、イギリスでは、かねてから信頼できるデジタル ID の確立は重要な政策課題になっていました。

ただ、2006 年にブレア首相に率いられた労働党政権が生体認証方式の国民背番号カードを導入しました。ところが、国民からの大ブーイングでした。政権交代で誕生した保守・自由連立政権は、即、国民背番号カードを廃止しました【CNN ニュース 62 号 CNN-62 (HP) .qxp (pij-web.net)】。

イギリス政界では、この経験がトラウマになっています。現在の保守党政権も、国民背番号カードから一歩距離を置いてデジタル ID を考えようというスタンスにあるわけです。

もちろん、イギリスも、デジタル ID やデジタル ID ウォレットをデザインする場合には、モバイル化の波を避けてとおることはできません。デジタルデバイド (情報技術格差) に悩む市民だけでなく、スマホネイティブにも納得のいくデザインが求められます。

— EU 離脱をしたイギリス政府の「物理的な IC カード離脱宣言」

イギリス政府のマット・ワーマン (Matt Warman) デジタルインフラ担当大臣が、2023 年 1 月 1 日に「イギリスのデジタル ID と属性の信頼できる枠組み (UK digital identity and attributes trust framework)」と題する政策方針 (Policy paper) を出しました。ここでは、改めて、「国民背番号カード (わが国のマイナンバーカードに相当) に頼らない (without the need for a national identity card)」デザインのデジタル ID を目指すと宣言しました。

言いかえると、わが国のような、② PKI (公開鍵・電子証明書・電子署名) 方式の公定 / 実質国定の個人用デジタル ID を物理的な IC カード (マイナカード) に格納して配り、オンライン / オフライン・官民の垣根を越えてより包括的 (オムニバス) に使わせようという監視資本主義につながるような不気味な政策は取らないとしたわけです。

つまり、イギリスは、わが国のような国民に不評で未来志向を欠く物理的なマイナ IC カードを使わない信頼できるデジタル ID 制度を導入すると公約したわけです。

— イギリスのデジタル ID は未来志向のモデルなのでしょうか?

モバイル化が急激に進み、スマホネイティブ世代がますます社会の中核を占めるようになりつつあります。スマホに不具合な IC カード自体が絶滅危惧種になりつつあります。

イギリスも事情は同じです。ユーザー (利用者) がアナログの IC カードを見せて、サービスを提供する事業者が、カードに記載された写真とユー

ザーの容姿を目視で確認するのは、リアル（対面）のサービスでは可能です。しかし、スマホを使ってデジタル／オンライン（遠隔）でサービスを受けるためにウェブサイト（デジタルプラットフォーム／ポータル）にログインする際に IC カードは不都合です。

ですから、イギリス政府が、デジタル化だけでなくモバイル化時代を見据えて、改めて物理的な国民背番号 IC カードに頼らない（without the need for a national identity card）「デザインのデジタル ID [モバイル ID アプリ] の確立を目指したわけです。これは、未来志向と見ることができます。すでにふれたように、実は、EU でも、モバイルデバイス（スマホなど）の普及を見据えて、スマホなどに直接 ID データ [スマホアプリ] を入れ、物理的な IC カードへ格納することは止めています。

ー イギリスだけでなく、アメリカやオーストラリアなども、物理的な国民背番号 IC カード、わが国のようなマイナンバー IC カードに否定的ですが。

イギリスだけでなく、オーストラリアでも大掛かりな国民 ID カード導入計画がありました。「オーストラリアカード (Australia Card)」というネーミングで計画が進められました。1984 年に提案されましたが、国民から猛反対にあい、87 年に廃案になりました [詳しくは CNN ニュース 57 号 参照 <http://www.pij-web.net/cnn/CNN-57.pdf>]。アメリカやカナダなどを含め、「コモンロー諸国 (英米法系諸国)」では、国民背番号制にはアレルギーが強く、プライバシー保護を大事にしたいという国民性が強いように思います。権威主義国家につながる仕組みは絶対に嫌だ、になるわけです。運転免許証や健康保険証など特定の公的サービス用の物理的な個人 ID があり、対面での本人確認にはこれを使えば十分、となるわけです。あえて公定／実質国定のデジタル ID を物理的な IC カードに格納し持ち歩かせる必要はない、となるわけです。血税の無駄遣いで、国民の不人気にもつながります。デジタル ID は、モバイル ID アプリでやり取りすれば済むことです。

いずれにしろ、利便性の高いマルチ／オムニバスなデジタル ID [モバイル ID アプリ] をデザインするにしても、民間活力を生かす、血税をムダに使わないようにしようということになるわけです。

ー イギリスは、デジタル ID では、これまでも試行錯誤を繰り返しているようです。英デジタル庁は、「Gov.UK Verify」、通称で「バリファイ」というデジタル ID をつくったようですが？

2011 年 4 月に、イギリス政府は、内閣府 (Cabinet Office) にデジタル庁 (GDS=Government Digital Service) を設けました。デジタル庁は、新たなデジタル ID 制度の構築を目指しました。イギリスのデジタル庁が目指すのは、わが国のようなオンライン（非対面）／オフライン（対面）双方に共通の ID ではありません。オンラインに限った、個人／個人以外（団体）双方に提供するデジタル ID です。しかも、物理的な IC カードに頼らない仕組みです。

イギリスのデジタル ID は、2016 年 5 月に、正式に稼働しました。「GOV.UK Verify (Verify)」、通称で「ベリファイ (Verify)」と呼ばれます。このデジタル ID は、民間活力、競争原理を生かした仕組みになっています。つまり、本人確認業務は、民間 IT 企業 [認定 ID サービス事業者 (identity providers, certified companies)] に委託されており、ユーザー（利用者）は、デジタル ID アカウントの発行を申し込む際に、認定事業者一覧から好きな業者を選べる仕組みになっています。

この民間活力を生かした政策で、政府は、次のようなメリットを期待できるとしています。

【表 11】民間活力を生かした政策のメリット

- | |
|---|
| <ul style="list-style-type: none"> ①各認定事業者は、標準規格内で自由にベストな本人確認の技術仕様を選択できる。 ②政府は集中化した巨大なデータベースを構築する必要がなく、デジタル ID を分散管理でき、データセキュリティにも資する。 ③競争によりデジタル ID サービスの向上が期待できる。 ④ユーザー（利用者）に自主的な業者選択権が保障される。 |
|---|

バリファイ (GOV.UK Verify) のデジタル ID は、2019 年に民間機関のウェブサイトへのログイン／アクセスにも利用できるようになるまで、もともとは政府／公共機関のウェブサイト（デジタルプラットフォーム／ポータル）へのログイン／アクセス用につくられたインフラでした。

ユーザー（利用者）は、バリファイ (GOV.UK Verify) にオンラインで申請し、好きな認定事業者を選んで、デジタル ID アカウントの発行を受

けることができます。無料です。デジタル ID アカウントの発行には、メールアドレスやパスワードを登録し、氏名・生年月日・スマホ電話番号・住所・写真付きの運転免許証ないしパスポートなどのデータを入力し、Q&A、銀行口座にオンライン署名をするなどの方法で本人確認が必要です。受注した事業者は、運転免許証やパスポートなどについては、所管の当局に照会をし、結果の連絡をもらうことになります。

ユーザー（利用者）は、初回のアカウント設定手続を完了した後は、バリファイ（GOV.UK Verify）のロゴのあるオンラインサービスにアクセスし、自分がアカウントを開設・デジタル ID を保存した事業者に到達できれば、本人確認ができます。

いずれにしろ、ユーザー（利用者）はアカウントを開設・デジタル ID の発行が受けられれば、それを使って政府／公共機関のウェブサイト（デジタルプラットフォーム／ポータル）にログインできます。2019年時点では、バリファイ（GOV.UK Verify）のデジタル ID は、所得税や年金の確認、運転免許証情報の表示など40程のサービスに対応しています。

バリファイ（GOV.UK Verify）を利用するかどうかは、任意、あくまでも利用者の自由意思に委ねられています。利用者が自主的にアカウント登録することではじめて利用できることになります。政府は、「デジタル庁の役割は、あくまでもイギリスのプライバシー法に即したデジタル ID 制度を構築することであり、新たな国民背番号制や住民登録のようなシステムを稼働させることではない。」と宣言しています。[Moving forward our work on identity assurance-Government Digital Service (blog.gov.uk)]

ー バリファイ（GOV.UK Verify）は、情報の機密密度に応じて、サービスを差別化しているとのことですが？

バリファイ（GOV.UK Verify）のデジタル ID は、常に最高レベルの正確性を求めなくともよいという考え方に基づいて、セキュリティレベルに応じて4段階に差別化されています。認証レベルによって利用できるサービスが異なります。例えば、一番低いレベルの「LOA1」は、機密情報に関わらない情報の閲覧などアクセス／ログインの際に利用する認証です。より厳密なサービスへのログイン／アクセスには、「LOA2」「LOA3」

と認証レベルが上がっていきます。

ー しかし、バリファイ（GOV.UK Verify）は、利用が伸び悩み、大幅に見直しされるそうですが？

バリファイ（GOV.UK Verify）の利用は伸び悩んでいました。政府は、2016年のバリファイ開始時に、2020年までに利用者数2,500万人を見積もっていました。しかし、2019年2月時点での利用者数は14.4%／360万人程度でした。会計検査院（NAO=National Audit Office）も、利用が低迷するのは、バリファイ（GOV.UK Verify）は、必ずしもユーザーフレンドリーなデザインになっていないのではないかと苦言を呈しました。

イギリスには、ユニバーサルクレジット（給付つき税額控除）という働いても貧しい人たち（the working poor）向けの税制があります。会計検査院（NAO）の検査によると、申請対象者の70%がバリファイ（GOV.UK Verify）のデジタル ID を使って課税庁（HMRC）のポータルサイトへのログイン／アクセスを試みたものの、実際にログイン／アクセスできたのは、そのうちに38%に過ぎませんでした [NAO, Investigation on verify (March 5, 2019) Investigation into Verify - National Audit Office (NAO) press release Investigation into Verify (Summary) (nao.org.uk)].

ユーザー（利用者）がデジタル ID アカウントの発行を申し込もうと認定事業者一覧から好きな業者を選んでトライをしたものの、設定でうまくできず、途中であきらめたケースも少なくなかったのではないかと、思います。とりわけ、多くの政府・公共サービスは社会的・経済的に弱い立場にある人たちと深く関係してきます。こうした人たちは、デジタルデバイド（情報技術格差）問題を抱えていることも少なくありません。バリファイ（GOV.UK Verify）のアカウントを立ち上げる入口の手続に戸惑い、狙いのポータルサイトのログインまでたどり着けなかったケースも多いものと見られます。

また、バリファイ（GOV.UK Verify）のデジタル ID が使える政府・公共サービスの数が限られていること（40程度）もマイナスに働いているのではないかと思います。

ロイヤルメール（郵便局）を始めとした主要な認定事業者の撤退も相次ぎました。

内閣府は、2018年10月に、バリファイ (GOV.UK Verify) を、2020年3月末で終了するとアナウンスしました。しかし、コロナパンデミックの混乱を受けて、その後さらに3年間利用が延長されました。

ー バリファイ (GOV.UK Verify) のデジタル ID 見直し開始

イギリス政府は、2019年6月に、デジタル・文化・メディア・スポーツ省 (DCMS= Department for Digital, Culture, Media and Sport) が、バリファイ (GOV.UK Verify) の見直しに着手することをアナウンスしました。デジタル ID システム (プラットフォーム) を官民が共通で利用できるデジタルインフラにする方針を明らかにしました。このため、内閣府に「デジタル ID 作業班 (DIU=Digital Identity Unit)」が設置されました。

DIU は、バリファイ (GOV.UK Verify) のデジタル ID の運用をもっと民間に開放し、民間活力を生かし、もっと使い勝手のよいデジタル ID の利用・再利用に向けたシステム開発を進め、現行のデジタル ID を再生する方針を明らかにしました。

しかし、2021年3月に、内閣府 (Cabinet Office) のトップである官房長官 (Parliamentary Secretary) は、突如、バリファイ (GOV.UK Verify) は死に体 (dead in the water) であり、新規のデジタル ID に舵を切りたい、と話しました。新たなデジタル ID 政策が確定するまでは、バリファイ (GOV.UK Verify) に代えて、「One Login」 (Gov.UK One Login)、通称「ワンログイン」をデジタル ID として使う、としました。[British Government-once again-aims for 'one login for government' (diginomica.com)]. [*ちなみに、このワンログイン (Gov.UK One Login) 方式では、イギリス政府／公共機関の各種サービスを受けるために各機関のポータルへログイン／アクセスするには、各ユーザー (利用者) の①アカウント ID (eメールアドレス) + ②パスワード + ③本人確認・2種類身元確認 (verification) / 本人認証 (authentication) [生体認証 (顔・指紋)、身元認証 (公務員証・軍人証等) または知識認証 (ワンタイムコード・バックアップコード等) のいずれかのうち2つ] を入力することになります。]

ー 2023年4月から、新たなデジタル ID [モバイル ID アプリ] が使われることになるようですが、どんなデザインなのでしょうか？

イギリス政府は、新たなデジタル ID を確定し、2023年4月1日から稼働させる方向で、急ピッチで準備を進めています。したがって、2023年3月末までは、バリファイ (GOV.UK Verify) に代わり、ワンログイン (Gov.UK One Login) を、指定された政府／公共機関のポータル／ウェブサイトへアクセス／ログインする際のデジタル ID [モバイル ID アプリ] として使い続けることとなります。

昨年 (2022年) 夏、とくに年末、そして今年 (2023年) の1月から、あわただしい動きが見られました。政府が出したデジタル ID の改革案は、次のように2本建てになっています。

今年2月末まで、法案に対するパブリックコメント (public consultation / 公開諮問) を求めました。3月中の法案を仕上げ、議会上程し、成立をはかるスケジュールです。

【表 12】 イギリスの新たなデジタル ID の特質

- ① デジタル経済法 (Digital Economy Act 2017) の改正法案 [One Login 導入法案]: ①個人が、政府・公共機関のポータルサイトにログインする際のデジタル ID [gov.UK One Login] [モバイル ID アプリ] の標準化、②個人が、オンライン／オフライン (対面) 双方での本人確認手続で、自己情報の利用制限・コントロール権を保障された形での利用可、③政府・公共機関は、そのデジタル ID で個人+世帯に関する機関相互間での情報連携が可能【主な対象は個人と政府・公共機関 (GtoC)】
- ② データ保護・デジタル情報法 (Data Protection and Digital Information Bill) 改正法案 [民間部門での信頼できるデジタル ID 利用促進法案] 【主な対象は個人と民間機関など (BtoC、BtoB、CtoC、GtoB)、オプトイン方式】

ー どういう仕組みのデジタル ID なのでしょうか？

現時点では法案が成立していません。詳しく説明するには、もう少し時間が欲しいところです。現在、デジタル庁 (DGS) が、民間 IT 企業 (Deloitte、Experian) と共同でデジタル ID デザインについて詰めの作業を続けています。

誤解を恐れずにアバウトにいいます。個人が、政府・公共部門が提供するサービスに、オンライ

ン／ネットで申告・申請するとします。この場合には、まず公営のデジタル ID プラットフォームで、モバイルアプリを使って、自分のデジタル ID アカウント [ID・パスワードをベースとした方式] を開設することになります。

ID アカウント／デジタル ID ができると、その ID を使って、目当ての機関のウェブサイト（デジタルプラットフォーム／ポータル）にログイン／アクセスすることになります。

このデジタル ID は政府・公共部門に共通して使えます。また、政府・公共機関は、このデジタル ID を使って法令の範囲内で情報連携（data sharing）／データ照合（data matching）することが認められています。

このことから、個人が、課税庁（HMRC=His Majesty's Revenue and Customs／歳入・関税庁）や労働・年金省（DWP=Department for Work and Pensions）のような国の機関や各地の自治体（local councils）に設置されたウェブサイト（デジタルプラットフォーム／ポータル）にアクセスする場合、加えて、これらの機関が機関相互での情報連携をする場合には、このデジタル ID を使うことになります。

イギリス保守党は、物理的な国民背番号カード（national ID card）は導入しないというのが公約です。デジタル ID 導入を装ってオフライン（リアル空間／対面）でも個人の監視に使える公定／実質国定の「箱／容器」・「カード」を導入するのは人権侵害につながりかねないという考え方を堅持しています。

現在、イギリスの国政は保守党が担当しています。ですから、今回のデジタル ID では、国民が嫌がるデジタル ID を格納するための物理的な IC カードだけは絶対に導入しない、というのがギリギリの政策選択のように見えます。

しかし、政府は、このデジタル ID を、政府／公共機関の間での情報連携／データ照合の際にキーとして使うとしています。もちろんキーとして使う場合には、法認された透明なルールによることになっています。法令では、情報主体に不服申立権を認めるなど民主的な手続が保障されています。一応、法的手続の体裁は整っています。しかし、情報連携／データ照合自体に異論もあるわけです。

すでにふれたように、イギリスでは、かつて労働党政権が導入した汎用の生体認証式国民総背番号制／カード制が、政権交代で廃止されま

した。こうしたこともあり、各個人の国民背番号（unique national ID number）を識別子（identifier）に使った各種政府・公共機関相互での効率的な情報連携（data sharing）・データ照合が難しい状態が続いているわけです。

今回の標準化されたデジタル ID の導入が実現すれば、各個人のデジタル ID ないしデジタル ID から組成された符号を使い、これまで滞っていた情報連携・データ照合を一気に進められる、との読みがあると思います。この構想を推進する役人には、まさに願ったりかなったりなわけです。

今回のイギリスのデジタル ID 導入案にはこうした巧妙なマジックが隠されていることを忘れてはなりません。ただ、こうした点を差し引いても、モバイル化の流れの「抵抗勢力」となって、人権ストレスの一番高い物理的なマイナ IC カード（国民背番号 ID カード）を国民に強要する日本のデジタル ID 政策よりは、ベターかも知れません。

— もう一方の個人と民間機関との間で、オンライン取引、ネット契約する場合などで使うデジタル ID [モバイルアプリ] については、どうなのでしょう？

イギリスは、ユーザー／消費者や民間機関（企業／団体）は、民間取引（BtoC／BtoB）などでは、信頼できる技術仕様のデジタル ID を自由に選択して利用できるという政策です。ただ、ユーザー／消費者が信頼できる技術仕様のデジタル ID を選択できるようにとのことで、政府が「デジタル ID と属性の信頼できる枠組み（UK digital identity and attributes trust framework）」を構築し、裏支え（信用保証）するという政策です。一定の標準を充たす民間の IT 事業者に対してこの枠組みへの参加を促し、ユーザー（個人）は、信頼マーク事業者一覧から選択し、デジタル ID アカウントを設定できます。各個人は、この信頼マークの仕組みを信頼（トラスト）し、利用するか利用しないかは、全く自由です。将来的には、信頼マーク事業者による IDaaS（アイダース）サービスの提供なども計画しているようです。[* IDaaS（アイダース）とは、「Identity as a Service」の略称であり、クラウド経由で ID 認証、ID パスワード管理、シングルサインオン（SSO）、アクセス制御を提供するサービスです。]

【表 13】 デジタル ID と属性の信頼できる枠組み (2023 年 1 月 26 日公表)

1.Ministerial foreword	1 デジタルインフラ大臣序文
2.Feedback received and updates	2 フィードバックと最新情報
3.Introduction	3 はじめに
4.What are digital identities	4 デジタル ID とは何か
5.What are attributes	5 属性とは何か
6.What the UK digital identity and attributes trust framework does	6 イギリスのデジタル ID と属性の信頼枠組みが行うこと
7.What you get from adopting trust-marked digital identities and attributes	7 信頼マークを付けたデジタル ID と属性を採用することで得られるもの
8.Benefits for users	8 ユーザーにとってのメリット
9.Who runs the trust framework	9 誰が信頼枠組みを運営するか
10.How organisations participate in the trust framework	10 企業が信頼枠組みに参加する方法
11.Rules for identity service providers	11 ID サービス事業者のためのルール
12.Rules for attribute service providers	12 属性サービス事業者のためのルール
13.Rules for all identity and attribute service providers	13 すべての ID・属性サービス事業者のためのルール
14.Rules for orchestration service providers	14 オーケストレーションサービス事業者のためのルール
15.Rules for all identity, attribute and orchestration service providers	15 ID・属性・オーケストレーションサービス事業者共通のルール
16.Table of standards, guidance and legislation	16 標準、ガイダンスおよび立法の表
Glossary of terms and definitions	用語集と定義

ー イギリスのデジタルウォレット (e-ID wallet) のデザインはどうなのでしょう？

イギリスのデジタル ID ウォレット (e-ID wallet) [モバイルアプリ] のデザインも、EU のデジタル ID ウォレット (EDIW) [モバイルアプリ] のデザインと同様に、現時点では細部についていまだ定かではありません。ただ、双方とも、国や EU が安全で信頼できる枠組みを構築しようという点では似通っています。[See, Policy paper : UK digital identity and attributes trust framework alpha v1 (0.1) (Updated 11 January 2023) ; Sophia Waterfields, 'UK government plans digital identity law change to support One Login rollout,' Tech Monitor (January 6, 2023) ; Sophia

Waterfield, 'Public buy-in will be needed to implement UK's Digital Identity Trust Framework,' Tech Monitor (Feb. 1, 2023) ; News, Digital ID Aims to Simplify Brits' Use of Public Services (Jan. 10, 2023)]。

◆個人用デジタル ID に人権エコシステムをどうデザインするのか？

ー もう一度大事なところを復習させてください。近年、「人権エコシステム」という言葉をよく耳にします。デジタル ID に人権エコシステムをデザイン (組み込む) には、どのような課題を解決しないといけないのでしょうか？

エコシステム (ecosystem) とは英語で「生態系」を意味します。もともと生物学で使われていた言葉です。同じ領域で暮らしている生物が、相互に依存し合って生きている状態を指します。自然界では、生物は 1 つの種のみでは生きられません。大気や気候、土壌と言った環境から栄養を吸収している微生物、それを捕食する虫、さらにその虫を捕食する動物などの循環系のなかに相互依存して生きています。こうした生態系を維持する関係を「エコシステム」と呼びます。

デジタルシフトが急激に進むなか、「基本的人権としてのデジタル ID (Digital ID as a basic human right)」を探る動きも活発化しています (World Economic Forum, 4 principles for securing the digital identity ecosystem (Mar. 18, 2021) 4 principles for securing the digital identity ecosystem | World Economic Forum (weforum.org))

デジタル ID は、本来、ウェブサイト (デジタルプラットフォーム/ポータルサイト) に安全にアクセス/ログインする際の本人認証 (authentication) ツールのはずです。デジタル ID は、各国の憲法の人権条項、世界人権宣言や国際人権基準などの国際基準をベースに、正義に資するデザインでなければなりません。

人とテクノロジーがグローバルに交差する場で、世界中の人々に悪影響が及ばない技術仕様であることが求められます。データプライバシー、サイバーセキュリティ、デジタルデバイド、デジタルリテラシー、人種やジェンダー、年齢差別などからの点検・評価に耐えうる水準でないといけないわけです。

ところが、デジタル ID は、安全対策 (データセキュリティ) を「偽旗/ニセ旗」に、不正義な

技術仕様／デザインを選択すれば人権侵害ツールに悪用できます。国民監視用の国内パスポート、健康保険証データの自動徴兵選別、社会保障給付対象選別、信用スコア制度 (social credit system) への悪用が適例です。[*この辺は、CNNニュース本号(113号)別稿／報告書レビュー：NYU 報告書『人権をむしばむ世銀のデジタル ID プロジェクト』を読む をご覧ください。]

それに、デジタル ID は、常に最高レベルの正確性を求めなくともよいわけです。ユーザーが利用するサービスのレベルに応じて、段階を設けて差別化する必要があります。でないと、ユーザーが人権への恐怖を感じてしまいます。

わが国のマイナシステム (国民総背番号制) では、データセキュリティ (安全) を口実に、あらゆる技術仕様を総動員し、デジタル監視トラップ (罠) 化したデジタル ID の利用を一律に強要しています。IT 技術、小型化したスマート技術に悪乗りし、国民をスマートに超監視する、国の役人の悪巧みです。

一 わが国では、反マイナの市民団体は、「ゼロマイナ」一辺倒で、「人権エコシステムを織り込んだデジタル ID」については、深く考えていない、展望なしに見えますが？

指摘のようにその辺が問われている点です。それに、人権エコシステムを内装するにしても、わが国のデジタル ID のデザインは最悪なわけです。土台が腐っています。

わが国では、人権エコシステムを欠く「マイナ IC カード」(national identity IC card system) を悪用した、国民をデータ監視するシステムの拡大利用で、マイナパンデミックが止まりません。物理的なマイナ IC カードには、各人に国民背番号 (マイナンバー / unique individual ID number) や写真、氏名・住所など各種の属性が記載され、PKY (公開鍵) 技術仕様のデジタル ID も格納されています。一定の公共サービスのオンライン事務では PKY (公開鍵) 技術仕様のデジタル ID が強制されます。しかも、その強要を際限なく拡大しようとしています。

政府は、この物理的なマイナ IC カードと国民皆保険制度 (overall national health insurance scheme) で逃げ切れない健康保険証 (health insurance card) とを合体させたマイナ保険証で資格確認するオンラインシステム (通称「M システム」) を稼働させました。M システムでは、

【表 14】わが国の腐った国民総背番号制の土台

<p>①マイナ IC カード</p> <p>オフライン (対面) とオンライン (非対面 / ネット) 双方で使える IC カード。IC カードの表面には各人の背番号 (12 ケタ) + 属性情報 (氏名・生年月日など) や顔写真が搭載され、オフライン (対面) で面通し / 本人確認に使える。一方、IC カードには公定 / 実質国定の PKI (公開鍵・電子証明書・電子署名) 式のデジタル ID が格納され、一定の公共サービスのオンライン事務には、この PKI 技術仕様のデジタル ID の利用が強制される。</p>
<p>②マイナシステム (国民総背番号制)</p> <p>① (アカウント) ID・パスワード式、② PKI (公開鍵・電子証明書・電子署名) 式、③ 生体認証 (顔・虹彩・指紋など) 式、④ 二次限バーコード (QR コード) [マトリック] の監視技術を総動員したシステム。「デザイン正義」はゼロ。</p>
<p>③マイナ保険証資格確認オンラインシステム (M システム)</p> <p>マイナ IC カードと国民皆保険制度で逃げ切れない健康保険証とを合体させたマイナ保険証と、③ 生体認証 (顔パス) 技術 (FRT) とを使って資格確認するオンラインシステム。マイナ保険証確認オンラインシステムは、車輛のナンバーから追跡する N システム (自動車ナンバー自動読取システム) に匹敵し、いわば「M システム」。M システムは、データ収容所列島化を目指し、国家が、マイナ保険証を国内パスポートとして使い、国民の「移動の自由」をデータ監視する全国的な自動改札、カスミ網のような「デジタルトラップ (罠)」</p>

マイナ保険証という名の国内パスポート (内国人登録証) を国民全員に携行させ、医療機関や薬局などに設置された患者の資格確認ポイントで、顔認証 (顔パス) 技術 (FRC) まで動員し、本人確認の手法でデータ監視を徹底します。

実質は、顔認証技術 (FRT) + 背番号付き IC カードを使った国民の「移動の自由」を国家がトータルに監視する全国的な自動改札、カスミ網のような「デジタルトラップ (罠)」です。

わが国のオフライン / オンライン兼用のマイナ IC カードに格納された「デジタル ID」は、「人権を語るのはご法度！」を合言葉にデザインされたものです。国の役人・彼らに紐づいた研究者・シンクタンク・IT 企業などからなる産官学の「護送船団」、「日本株式会社」が悪知恵を出し合って完成させた極めて人権ストレスの強い仕組みです。まさに、プライバシーを反故にする権威主義国家

のデザインです。

折しも、政府は2023年3月3日に、保釈中の刑事被告人らの逃亡を防ぐため、刑事訴訟法などの改正案を閣議決定しました。海外逃亡の恐れがある場合、裁判所が衛星利用測位システム (GPS) 端末の装着を命令できるようになります。この新制度は、成立後の公布から5年以内に開始する予定です。Mシステムは、保釈中の刑事被告人らへのGPS装着と同様に、善良な市民に対して国内パスポートとしてマイナカードの持ち歩きを事実上強制します。国家が、病院や薬局で市民の位置情報を監視できるようにする国の役人の悪巧みです。Mシステムは「生活に欠かせない効率的なインフラだ！」は嘘っぱちです。

このデジタルトラップ (罠) を使ったMシステムで、全国の医療機関や薬局などを「監視技術の人体実験場」のように扱うのはゆるされません。

ところが、残念なことに、Mシステムの「裏の顔」に気づいている人は余りいないのです。ですから、この権威主義国家のデザインに対する批判は弱いわけです。これが、監視されることに慣れ切ってしまった庶民の実像かも知れません。しかし、このような人権エコシステムを欠いた、デザインの不正義丸出しのMシステムを立ち上げておいて、わが国が民主主義国家を標榜するのにはムリがあります。

いずれにしろ、わが国は、対面で「リアルID」として使う公定／実質国定のICカードPKY (公開鍵) を仕込んで非対面でも使える「デジタルID」に衣替えしたIDを、オンライン／オフライン双方でエスカレートして使わせようという政策です。この政策には「人権」のキーワードがすっぽり抜けているわけです。

グローバルに見ると、公営／実質国営のデジタルプラットフォーム (DFP)、マイナポータルのような中央集権的なデジタルIDシステム自体が人権侵害装置そのものだ、という厳しい批判があります。世界の人権団体や研究者から、こうしたデジタルIDの導入・活用は、民主主義国家における人権エコシステム保障の観点からゆるされないという声が高まっています。地政学やデータセキュリティの面でも危うさが指摘されています。

インドは、中央集権的な生体認証式デジタルIDシステム (アドハー／Aadhaar) を導入しています (詳しくは、CNN ニュース 91 号参照 <http://www.pij-web.net/cnn/CNN-91.pdf>)。しかし、何度もサイバー攻撃、ハッカー攻撃にあ

い、大量の国民データが漏洩する問題を引き起こしています。それから、2017年には、エストニアの公営のデジタルIDカードシステム／デジタルプラットフォーム (DFP) がサイバー攻撃を受け、ICチップ管理機能が不全になりました。当時の人口の半分以上、おおよそ75万人のデジタルIDカードの利用停止に追い込まれました。

デジタルIDに「正義 (justice)」を導入するには、ブロックチェーン (暗号資産) のような技術仕様を実用化したデジタルIDをデザインしないといけない時代に入っています。また、オーストラリア、アメリカ、イギリス、カナダなどを見ても、デジタルIDを、物理的なICカードに格納し、持ち歩かせる方式はとっていません。交通系のスマホスイカに見られるように、商業ICカードもモバイル化が時流だからです。スマホやパソコン (PC)、タブレット端末に直接、正義にかなう技術仕様のデジタルID [モバイルIDアプリ] を格納するやり方に切り替わっています。

また、アメリカ、カナダなど北米でも、民間のIT企業が構築したデジタルプラットフォーム (DPF) を使ってデジタルID [モバイルIDアプリ] を提供する方向にあります。官が個人向けの中央集権的なデジタルIDシステム／プラットフォームを構築し、公定／実質国定のデジタルIDの利用を強制するやり方は止めにしているわけです。

一 アメリカは顔認証 (顔パス) 技術 (FRT) のデジタルID利用に賛否が割れてますが？

そうですね、① (アカウント) ID・パスワードだけでは、簡易な技術仕様なのですが、なりすましその他のサイバー攻撃・犯罪を完全に防げないのも事実です。どうしても、顔面のような生涯不変の生体情報を活用しようとなるわけです。一方で、顔認証 (顔パス) 技術 (FRT) のデジタルIDでは、「有色人種の認識の精度が低い」といった問題が出てきます。

生体認証式デジタルIDについては2つの大きなグローバルなトレンド (流れ) があります (次頁【表15】)。

繰り返しますが、わが国では、顔認証 (顔パス) 方式の「マイナ保険証資格確認オンラインシステム」(Mシステム) の導入です。これに対する政党・政治家の反応、人権感覚が鈍いわけです。大方の市民や市民団体も、生涯不変の生体認証情報の利用／公有に対する危機意識が薄く、大きな声をあげないわけです。「経済社会のデジタルシフトに

【表 15】生体認証式デジタル ID のトレンド

①生体認証式デジタル ID を推進する流れ
中国に代表されるように、国家資本主義、デジタル監視権威主義国家の視点から、デジタル ID を、国民監視に積極的な利用拡大を促進
②生体認証式デジタル ID にストップをかける流れ
アメリカ、イギリスに代表されるように、自由な資本主義、民主主義国家の視点から、人権保護を優先し、デジタル ID の国民監視への利用を禁止

伴うハイテクな仕組みであり問題があるとは思えない？」、とする肯定的な意見すらあるわけです。しかし、わが国のマイナ保険証資格確認オンラインシステム（M システム）では、例えば患者が医療機関や薬局など提供した顔認証（顔パス）データの保存／消去はどうなっているのでしょうか？まったく、初歩的な基準すら誰にでもわかるように公開されていません。厚化粧に隠された人権ゼロのマイナや M システムの素顔が見えてきます。

これは、対岸のアメリカの実情と比べてみればわかります。アメリカのデジタル ID では、わが国とは真逆で、IC カードに頼る PKI（公開鍵・電子証明書・電子署名）の技術仕様は論外ですし、顔認証（顔パス）の技術仕様の利用すら制限・停止する方向にあるわけです。

国家がデジタル政策の一環として、個人用のデジタル ID の技術仕様／デザインを選ぶとします。この場合、憲法で基本的な人権を保障している国では、人権に最もストレスの少ない方式を選ばなければなりません。ところが、わが国は、国の役人が、国民に有無を言わずに、人権に最もインパクト（影響）の大きいデジタル ID の技術仕様／デザインを選ぶ、あるいはあらゆる監視技術仕様を総動員して、国民に重い人権ストレスを強要しているわけです。この問題でバッコする国の役人は、国民のデータ監視の徹底しか眼中にないわけです。

彼らは、「PKI（公開鍵）方式のデジタル ID では、「それ格納する IC カードが必要だ。これで、オンライン（遠隔）だけでなくオフライン（対面）でも国民監視ができる。一石二鳥だ。顔認証（FRT）もテンコ盛りにし、完璧な国民監視システムだ」と氣勢を上げているわけです。しかし、司法は、彼ら国の役人／行政の氣勢に押されてしまうのです。

最高裁は、2023 年 3 月 9 日、市民のマイナ違憲の訴えを上告不受理で退け、「合憲」のお墨付きまで与えました。最高裁は、名ばかり三権分立、

行政追従の消極司法の顔を露わにしたわけです。司法は、やはり「国家権力」なのです。「三権分立」は、国家権力を 3 つに分割してデザインしているだけなのです。司法が、独立して権力を行使してくれるとの「夢」をいただくのもわからないでもありません。こうした市民感覚は大事です。しかし、マイナは「民事」ではないわけです。「諫早」などと同じで、国家の統治が絡んできます。司法が「柔」な判断をするはずはなく、国家権力がむき出しになるのです。ミャンマーや中国などの司法と同じ顔になります。

ずっとマイナ違憲裁判闘争はいい加減にして欲しいと願っていました。最高裁が「合憲」と判断するのがわかっているのに最後まで突っ走るわけです。まさに「外部不経済」で、サステナブル（持続可能）な闘いを望む者には迷惑です。「合憲」「違憲」をはっきりさせないで闘う賢さを欠いている感じを受けます。

反マイナの市民団体は、相変わらず「ゼロマイナ」のムシロ旗作戦、大本営発表の解説に終始している感じです。もちろん、ムシロ旗作戦も大事です。しかし、ただ、それだけでは絶滅危惧種になります。理論武装して「ウイズマイナ」時代を見据えた闘いができていない感じがします。新たなチーム力がないと国の役人や行政追従の司法と対峙するのは至難です。どの運動も、しぶとさに加え、したたかな戦略で駆け出す行動が要ります。

政治は与野党を含め大勢は、デジタルデバインドで、この面での人権感覚は希薄です。このままでは、わが国は、お隣の権威主義国家を超える名だたるデータ監視国家の仲間入りするのは必至です。

わが国の名だたる IT 企業は、グローバルサウス諸国に、こうした人権エコシステムを欠いた技術仕様のデジタル ID システムを輸出し続けています。ビジネスの人権デュー・ディリジェンス（Human Rights Due Diligence／人権 DD）が厳しく問われる時代です。ビジネスも政治も、口先だけで「デモクラシー万歳！」を叫び、内実は「何をやっても儲かればいい」では済まないのです。真に民主主義国家を標榜するのであれば、デジタル ID でも「人権ファースト」を貫き、切磋琢磨し、グローバル市場で開花しないといけません。

— 今回はかなり難しい点も含め、「デジタル ID」についてかなり深く勉強できました。モバイル全盛時代にマイナ IC カードを配るのは、世界の流れから隔絶したガラパゴス日本の愚策であることがよくわかりました。ありがとうございました。

報告書レビュー

NYU 報告書『人権をむしばむ世界銀行のデジタル ID プロジェクト批判』を読む

《 評 者 》 石 村 耕 治

ニューヨーク大学 (NYU) ロースクール、人権とグローバル正義センター、デジタル福祉国家と人権プロジェクト報告書『地獄に向けたデジタル道の舗装：デジタル ID のグローバルネットワーク構築における世銀の役割入門』(2022年6月) https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf

Paving a Digital Road to Hell?

A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID
Digital Welfare State and Human Rights Project
Center for Human Rights and Global Justice
NYU School of Law
June, 2022



世界各国には、戸籍 (family registration system)、個人籍 (individual birth/marriage/death registration system) のようなさまざまな民事籍 (civil registration system) がある。こうした伝統的な民事籍制度は、出生、婚姻、死亡その他の身分関係を証明するのに役立つ。民事籍制度に問題がないわけではない。しかし、少なくとも無国籍者をなくすには役立つ。これは、ミャンマーのロヒンギヤの人たちのように、居住する国の国籍も法認されない例を見れば一目瞭然である。

こうした伝統的な民事籍制度に、唯一無二 (ユニーク) な個人番号/背番号 (unique personal identity number) をつけた管理が世界に広がっている。背番号に加え、顔写真や氏名・住所などの属性データをカードや証票 (紙製の運転免許証や旅券) に入れ、本人確認に使う仕組みは「リアル ID/対面 ID (real identity)」とも呼ばれる。一方で、経済社会のデジタル化 (digital

economy/digitalization) が急速に進み、ネット空間/オンライン空間/非対面で流通するユニークな本人確認が主流になりつつある。いわゆる「デジタル ID」である。デジタル ID は、公的機関やサービス提供事業者が発行する唯一無二の電子版の ID である。デジタル ID は今や、モバイルアプリを使ったものが世界標準だ。

デジタル ID は、本来、ウェブサイト (デジタルプラットフォーム/ポータルサイト) に安全にアクセス/ログインする際の本人認証 (authentication) ツールのはずである。しかし、デジタル ID は、安全対策 (データセキュリティ) を「ニセ旗」に、不正義な技術仕様/デザインを選択すれば、人権侵害ツールに悪用できる。国民監視用の国内パスポート、健康保険証データの自動徴兵選別、社会保障給付対象選別、信用スコア制度 (social credit system) への悪用が適例だ。

わが国では、紙製の運転免許証や旅券は、地方公安委員会や外務省によって本人確認書類が「名

義人本人のものであることに間違いなし」と証明される。一方、デジタル ID は、事前に本人情報を登録の上発行され、通信を利用して、発行機関が証明する仕組みである。わが国のマイナンバー／マイナンバー IC カードは、住民登録情報をベースとしたつくりだ。対面で使う物理的な「リアル ID」を継ぎ足し、非対面でも使える「デジタル ID」に衣替え、本人確認をする仕組みといえる。

経済社会のデジタルシフトが急激に進むなか、世界中の政府や地域がデジタル ID の導入に懸命に取り組んでいる。デジタル ID には、背番号や属性情報に加え、生体認証（顔面、指紋、目の虹彩など）を使うケースも少なくない。しかし、デジタル ID は、それが持続可能（サステナブル）な利用ができ、かつ人権を侵害しない、人権ストレスの少ないデザイン／技術仕様のものでないといけない。

アメリカのワシントン D.C. に本部を置く世界銀行（World Bank/ 通称「世銀」）は、グローバルサウス（Global South）* のデジタル ID システム導入・拡大を支援するためのプログラムを組み、推進してきている。About Us | Identification for Development (worldbank.org)

* グローバルサウスとは、「途上国 (developing countries)」と同様の意味で用いられる言葉。アフリカ、ラテンアメリカ、アジアの新興国 (upcoming countries) などがあてはまる。国際連合 (UN) は、77 の国と中国をグローバルサウスに分類している。対義語として、経済的に豊かである先進諸国 (developed countries) を「グローバルノース (Global North)」と呼ぶ。グローバル正義 (global justice) とは、グローバルサウスとグローバルノースが共に手を携え、地球的なジャスティス (正義) を実現しようという考え方である。

さまざまな国際機関は、事あるごとに、グローバルサウスの経済的な発展、人権の保護にはデジタル ID の導入／確立が必要不可欠であるかのように説いてきた。世銀もそうした国際機関の 1 つである。

「経済的 ID (economic identity)」と名打って、デジタル ID は、持続可能な開発目標／SDGs (sustainable development goals) の必須アイテムであるかのように語られてもいる。

2013 年に、インドは、眼球の虹彩などで本人確認をする生体認証式のデジタル ID である「アドハー (Aadhaar)」を導入した。同年、世銀総裁は、「アドハーは貧困キラー (poverty killer)」であると称賛した。2014 年の世銀と国際通貨基金 (IMF) の年次総会で、世銀副総裁は、「本人



目の虹彩の採取現場 (Public Use)



アドハーカード切り取り使用の PR (Public Use)

確認 (ID) なしには、尊厳も権利保護も不可能である (Neither dignity nor rights are possible without an identity)」旨のアナウンスをした。

その後、世銀は、「開発のための ID 実施指針 (ID4D / Identification for Development Initiative)」を出し、財政支援と紐づけし、生体認証式デジタル ID 実証実験へのグローバルサウス諸国の参加を促した。世銀は、35 カ国へ 15 兆米ドルを超える財政支援を行った。しかし、世銀が称賛したインドのアドハーのような生体認証式デジタル ID モデルは、グローバルな人権エコシステム (global human rights ecosystem) に対するインパクトが大きい。

もちろん、グローバルサウス諸国の多くは、すでに民事籍制度を持っている。にもかかわらず、リアル ID を導入していない国もある。一方で、しっかりした民事籍制度すらない国もある。人権保護レベルもまちまちである。西欧型民主主義を志向していない国も少なくない。デジタルシフトが急激に進むなか、多様な国々を束ねて人権エコシステムを織り込んだ「基本的人権としてのデジタル ID (Digital ID as a basic human right)」を探る動きも活発だ (World Economic Forum, 4 principles for securing the digital identity ecosystem (Mar. 18, 2021) 4 principles for securing the digital identity ecosystem | World Economic Forum (weforum.org))。

インドのアドハー【生体認証式デジタル ID プラットフォーム】の運用実態 (詳しくは、CNN ニュース 91 号参照 <http://www.pij-web.net/cnn/CNN-91.pdf>)

- 2013年に導入。政府の固有ID庁 (UIDAI= Unique Identification Authority of India) が管理・運営。この人権にインパクトが大きいとして世界の人権活動家や人権団体から批判されているアドハーシステムの構築には、わが国のIT企業・NECが技術支援をした (NECが生体認証システムを提供しているインドのアドハープログラムの登録者数が10億人を突破 (2016年10月12日): プレスリリース | NEC)。
- ①(アカウント)ID・パスワード、②生体認証(顔・虹彩・指紋など)式、③二次限バーコード(2D barcode / 商品名: QRコード) [マトリック]式の技術仕様を使い、国民1人ひとりに固有のIDを発行。住所がない人も多く、郵便事情も悪いので、物理的なICカードを発行したり、郵送していない。
- 2023年2月9日現在: ①登録人数(enrolment) 1,362,325,017、②認証件数(authentication) 86,992,816,983、③デジタル本人確認(eKYC=eKnow Your Customer) 14,218,394,633 Aadhaar

Dashboard (uidai.gov.in)【当初は①と②だけ、③は継ぎ足し】

- アドハーは、何度もサイバー攻撃を受け、ハッキングで国民情報が度々大量に漏洩した。データセキュリティが甘く、議会は後追いでプライバシー保護立法を行った。インドの人権団体や識者、マスメディアは、「アドハーは人権エコシステムを欠く」と批判を強めている。

■アドハーカード(レター)のサンプル(Public use)



問題は、生体認証式のデジタルIDである。西欧型民主国家でも問題が山積している。とりわけ権威主義国家では人権弾圧ツールと化すおそれ強い。にもかかわらず、世銀が、グローバルサウス諸国をじっばひとからげに扱う。一律に生体認証式デジタルIDを強要する。これでは、デジタルジャスティス(digital justice)とぶつかるのは当たり前だ。

ニューヨーク大学(NYU)ロースクールに組織された「人権とグローバル正義センター」は、デジタル福祉国家と人権プロジェクトを組み、世銀の「開発のためのID(ID4D)実施指針」(ID4D Initiative)を検証した。そして、2022年6月に、報告書『地獄に向けたデジタル道の舗装: デジタルIDのグローバルネットワーク構築における世銀の役割入門』(A4 103頁)を作成、世界に向けて公表した。

このNYU報告書では、世銀のデジタルID拡散計画を徹底的に批判した。監視資本主義(surveillance capitalism)を助長し、人権侵害の効率化(efficiency of human rights violations)を促進していることなど「暗黒部

(dark side)」、「不正義(injustice)」を指摘した。

ID4D実施指針は、単なる1私企業の企画でない。人権リスクの高い計画ではあるが、グローバルな知名度もある国際機関によるものである。世銀が鼻先にぶらさげた人參でグローバルサウスに怒涛の流れが生まれたとしても、止めるのは至難である。この報告書でも、グローバルサウス諸国の「真贋が問われる」と吐露している。

世銀の危険なデジタルIDモデル、デジタルIDプラットフォームの拡散にストップをかけるように訴えている。そのためには、世界各国の人権団体、専門職、ジャーナリストや人権活動家など、幅広いステークホルダーがタイアップするように求めている。加えて、この課題で、グローバルな人権エコシステムづくりに向けてグローバルサウスとグローバルノースの団結を訴えている。

このNYU報告書は、グローバルサウス諸国に中央集権的な生体認証式のデジタルID構築を奨める世銀の「開発のためのID(ID4D)実施指針」(ID4D Initiative)が、グローバルな人権エコシステムに大きな障害となる、と警鐘を鳴らした啓蒙書である。デジタルIDは不要であるとか、新

●わが国の人権エコシステムを欠く危ない国民総背番号制の仕組み

<p>①マイナ IC カード</p> <p>オフライン（対面）とオンライン（非対面／ネット）双方で使える IC カード。IC カードの表面には各人の背番号（12ケタ）＋属性情報（氏名・生年月日など）や顔写真が搭載され、オフライン（対面）で面通し／本人確認に使える。一方、IC カードには公定／実質国定の PKI（公開鍵・電子証明書・電子署名）式のデジタル ID が格納され、一定の公共サービスのオンライン事務には、この PKI 技術仕様のデジタル ID の利用が強制される。</p>
<p>②マイナシステム（国民総背番号制）</p> <p>①（アカウント）ID・パスワード式、② PKI（公開鍵・電子証明書・電子署名）式、③生体認証（顔・虹彩・指紋など）式、④二次限バーコード（QR コード）[マトリック] の監視技術を総動員したシステム</p>
<p>③マイナ保険証資格確認オンラインシステム（M システム）</p> <p>マイナ IC カードと国民皆保険制度（overall national health insurance scheme）で逃げ切れない健康保険証（health insurance card）とを合体させたマイナ保険証と、③生体認証（顔パス）技術（FRT）とを使って資格確認するオンラインシステム。マイナ保険証確認オンラインシステムは、車輛のナンバーから追跡する N システム（自動車ナンバー自動読取システム）に匹敵し、いわば「M システム」ともいえる。</p>

たな分権的なブロックチェーン（暗号資産）技術を実用化しデジタル ID を採用すべきであると、具体的を示したものではない。

この NYU 報告書での指摘事項は、日本の①マイナ IC カードを使った②マイナシステム（国民総背番号制）や③マイナ保険証資格確認オンラインシステム（M システム）にもあてはまる。決して他山の石ではない。

日本では、人権エコシステムを欠く「マイナ IC カード」（national identity IC card system）を悪用した、国民をデータ監視するシステムの拡大利用で、*「マイナパンデミック」* が止まらない。物理的なマイナ IC カードには、各人に国民背番号（マイナンバー／unique individual ID number）や写真、氏名・住所など各種の属性が記載され、PKY（公開鍵）技術仕様のデジタル ID も格納されている。一定の公共サービスのオンライン事務では PKY（公開鍵）技術仕様のデジタル ID が強制される。

日本政府は、この物理的なマイナ IC カードと国民皆保険制度（overall national health insurance scheme）で逃げ切れない健康保険証（health insurance card）とを合体させたマイナ保険証で資格確認するオンラインシステム（通称「M システム」）を稼働させた。M システムでは、マイナ保険証という名の国内パスポート（内国人登録証）を国民全員に携行させ、医療機関や薬局などに設置された患者の資格確認ポイントで、顔認証（顔パス）技術（FRC）まで動員し、本人確認の手法でデータ監視を徹底する。

実質は、顔認証技術（FRT）＋背番号付き IC カードを使った国民の「移動の自由」を国家が監視する全国的な自動改札、カスミ網のような「デジタルトラップ（罫）」である。産官学の「日本株式会社」が悪知恵を出し合って完成させた極めて人権ストレスの強い極悪の仕組みである。人権リスクではインドのアドハーをはるかに超える。実質、保釈中の刑事被告人らへの GPS（衛星利用測位システム）装着に等しい、と見る向きもある。プライバシーを反故にする M システムは民主主義国家にはなじまない。

私たちは、島国意識を丸出しではいけない。もっとグローバルな流れを学ばないといけない。そして、わが国での「*マイナパンデミック*」の「化けの皮」をはがさないといけない。加えて、わが国 IT 企業が海外で行っている事業活動に対する適正な人権 DD（デューデリジェンス）評価をしないと、グローバルサウス諸国で蔓延する人権エコシステムを欠いた生体認証式のデジタル ID にストップがかからなくなる。「儲かるのなら何をやっても赦される！」ではいけない。「人権」、「民主主義」を貫き、切磋琢磨し、グローバル市場で開花しないと、いけない。

この NYU 報告書は、わが国の人権エコシステムを欠いたマイナ IC カードシステム（国民総背番号制）への警鐘／外圧でもある。

最近、アメリカの大学のプライバシー法専攻で日本語が堪能な研究者からコンタクトがあった。日本のマイナ IC カードシステムは人権エコシステムを欠いているとのことで意見の一致を見た。プライバシー・インターナショナル・ジャパン（PIJ）の『CNN ニュース』の愛読者だという。もっと日本の実情を、世界に向けて「英語で発信して欲しい」との注文があった。日本語という地域言語が、日本のデジタル ID の「不正義（injustice）」や「暗黒部（dark side）」を覆い隠していると指摘する。紛れもない事実である。

Q & A 「デジタル刑事法学／ローテック (LawTech)」 デジタル空間での罪刑法定主義、人権①

— デジタル刑事法の市民目線での監視のあり方 —

コメンテーター 清水晴生 (白鷗大学教授)

デジタル技術が生活を便利にするだけでなく、今やインフラをなす時代が変わっている。それは民間のみならず、いよいよ公共サービスの領域にも広がってきた。

マイナンバー制度はデジタルと相性が良いだろう。あたかもパスワードを打ち込むようにパソコンに憶えさせておけば、気軽に様々なネット上のサービスを受けられるかもしれない。そうした多用途での利用を見越して、いよいよ義務化に打って出ること、人気のない政権はなんとか官僚の支持を得ようとしているとも伝え聞く。

◎ しかしマイナンバーをパソコンに打ち込む行為は、書類にマイナンバーを書きこむ行為とは実は大きく異なっている。書類が宅配伝票のようにカーボン紙をはさんだ体裁になっていれば、2枚目が手元に残り、3枚目は業者が持って帰ると想像がつく。

しかしパソコンに打ち込んだマイナンバーが、いま見ているサイトだけで利用される保証はどこにもない。じつはサイトポリシーやサイトのプライバシーポリシーという、ページの一番下のリンクから説明を見に行くと、「ここで得られた情報は100ぐらいのほかのサイトでも使うのでよろしく。」などと書いてある。書いてあればまだ親切なほうで、ろくに書いてないサイトのほうが多い。

つまりデジタル空間というのは、裏で便利にやっていますよという裏側が見えないようになっている。そこで先回りして処理してくれるから、表面的には一見便利だ。しかしどんな処理をしているのかは表からはわからない。知らないうちに望まないサービスまで進めてくれたり、勝手にあなたにあった広告を表示してくれたりまでする。

これが公共サービスだったらどうだろう。病院でマイナンバーを使えば、親切にも

(!?)病院にかかる金があるなら税金を先に払ってくださいと、求めてもないのに勝手に書類を送りつけてくるかもしれない。

◎ つまりデジタル空間は便利でおせっかいで、そして監視ツールであり、その中身はブラックボックスなのだ。われわれは普段からインターネットを使っているが、見ているページを一体どこのだれが作ったかも、誰が運営しているサーバーを経由しているかも、ろくに知らないまま自分の情報を無意識のうちにあちこちに渡しているのだ。

逆にいえば、情報を知らないうちに盗られているのだ。

◎ これからますます公共サービスのデジタル化が進む。それは公共サービスのあらゆる部門で進むが、それは知らないうちに、思っている以上の情報をとられるシステムが構築されていくということだ。

いま司法・裁判の世界で進んでいるのもこれと同じ性格を持たないわけにはいかない。便利さの裏側で、必ずプライバシー情報という大きな代償・対価が支払われている。そしてマイナンバーのように便利さをうたって拡大されたデジタル空間に対しては、もはや自分が支払っている代償がその便利さに見合うものかどうかをチェックできる余地はなくなっている。もういりませんといっても、いったん差し出したデジタルデータのプライバシー情報は無限にコピーされ、もうどこに行ったかもわからない状態になる。それは公共機関のクラウドサーバー上に保管されて、個人情報込みのビッグデータとして、付番された国民を数字一つで特定して、モニター上でその移動も行動も、何を買ったか、どこに行ったかまで手に取るようにわかるようになる。

◎ こうした便利監視ツールを、今度は裁判で

も使おうというのが監視役（国）の新たなアイデアだ。

法律や裁判の世界は、デジタルとはもともと相性はよくないように思える。なぜならデジタルは日進月歩の世界であるのに対して、法律や裁判は安定さを求める傾向があるからだ。しかも法律や裁判はルールに関わるから、いいかげんであることが許されない。デジタルは複雑すぎてその影響を切り切れないところがあり、その分不安定だ。だから確実さを求める司法の世界にデジタルがなじむには時間がかかってきた。

◎ デジタルの不安定さを心配する世代のあとに、デジタルの不安定さが気にならない世代が登場してきた。生まれたときからデジタル空間の中で育ってきたデジタルネイティブ世代は、デジタルの不安定さを過度に心配する態度を、ただイライラして見てきた。そしてそれはあまりにコストをかけすぎていると感じ始めた。お金がかかるだけじゃなく、時間も無駄にしている。確かに、手紙を書いて送って届くのと、電子メールが届くのとでは雲泥の差だ。

◎ デジタルはコストをカットできる。そしてその裏側には情報監視・取得のブラックボックスがある。うわべの便利さやコスト・ベネフィットだけを期待すれば、それはエサに釣られる魚のようなものだ。デジタルと裁判、デジタルと法律の関係も、この両面を確認しながら理解しなければならない。

デジタル技術の活用は民事裁判が先行しつつあるが、刑事裁判での利用も検討され始めた。司法・裁判は国が主催するもので、基本的には民間のものではない。選挙を前提とした国会とも違い、民主的要素がもともと薄い。しかし法律というルールが作られても、それを実際に適用するのは裁判所の仕事だ。これが国びいきで運用されれば、いくら法律が民主的に作られても、現実はお役所のやり放題になる。だからどんな法律が作られ、どんな裁判が行われるかについても、市民はしっかりと監視しなければならない。選挙で落とせないのでおさらだ。

◎ デジタルが中身のわからないブラックボックスだと述べた。それを今度は裁判に使おうというのだ。国は自分たちの使い勝手の良いインフラを作ってしまうと、あとはそれに合わせざるを得なくなる。国が勝手に仕様を決

めてよいだろうか。その運用に民間が加わらなくてよいだろうか。

◎ 刑事裁判は国（検察）と私人との対決だ。その対決のフィールドを国側（検察・法務省）が握って、その中身は国側しか知らないということになる。ずっと国側のホームゲームをするようなものだ。

◎ 戦前の刑事裁判がまさにこれだった。職権主義というシステムで、裁判所に任せておけば万事大丈夫といった考え方で、捜査も証拠も裁判も全部裁判所が主催する。つまり裁判所が捜査して、起訴して、裁くという茶番のようなものだ。しかし実際には検察が主導権を握って、裁判所を背後からコントロールしてしまう。これでは有罪の結論は始まる前から決まっただけで、裁判などセレモニーでしかなくなる。

◎ 刑事裁判がブラックボックス化するというのはそれほどおそろしいことだ。国は現在でも、国家機密や個人情報保護を理由に情報を隠し、他方でビッグデータやマイナンバーは民間にばらまこうとしている。安全といいながら頻繁に情報は流出し、そのたびに「悪用された形跡は今のところありません」という頼りないコメントだけが残される。

本当に刑事裁判のデジタル化を民主化させなくてよいだろうか。権威主義的なお役所裁判のデジタル版を目をつむって手放しに信頼して任せてしまっただけで本当に大丈夫だろうか。

◎ だからこそ、市民目線での監視・コントロールが制度としても我々の意識としても不可欠だ。そのポイントは次の三本柱に集約できる。

- ・法律の裏づけ
- ・データ保護、プライバシー保護（守秘義務やシステムの制度設計）
- ・透明性、説明責任、情報開示

◎ 刑事裁判のデジタル化が権威主義国家化への一丁目一番地とならないために、民主主義国家のままでいられるかの試金石だと考え、市民目線でのコントロールをリアル空間以上に効かせなければならない。それはデジタルネイティブにも、デジタルリテラシーを欠く人にも、その双方に課され、託された役割である。

刑法は、被害者が生命、身体、自由、財産の安全を損なわれないために、その人権を守っているという側面がある。

ただし同時に他方では、刑法に違反する行為をすれば刑罰が科され、懲役刑や罰金刑という自由・人権に対する制約が及ぶことになる。それは正当なもので、正義でもある。しかし刑法が国により悪用された場合を考えてみたらどうだろうか。そんなことはありえない？いや、戦争が始まればそうもいっていらなくなる。戦争をしてなくても、そんな国は周りを見渡せば五万とある。日本でも、当時の安倍総理の演説から法律の根拠なく警察により排除されるなど、法が公務員によって守られないケースはいくらでもある。

したがって刑罰により自由・人権を制約する刑法が、治安を守る正義の法だとばかりもいってられないのだ。逆に刑法は、むしろ刑罰を科せる場合を限定した、治安・司法当局者をルールで縛りつけるための法律だと考えなければならない。そしてこのルールをはみ出した法適用がないように、市民は監視しなければならない。

この要請が特に強く必要となるのが、デジタル空間での刑法の適用だ。というのも現行の刑法はなんと明治40年にできた法律だ。その後デジタル社会に合わせた法改正を何度か行っているが、それも頻繁なものではない。つまり、まだ車もそれほど走ってない時代の刑法を、デジタル全盛の今の時代でも大事に使い続けているのである。

つまり、日進月歩のデジタル空間での動きに対応し切れていない刑法を無理やりに今の現実に適用しようとするから、そこには法律との間に大きな隙間が生まれる。刑法で許された範囲を大きく超えて、裁判所が自ら立法者となって刑法を適用しているおそれが大きいのだ。これでは法律の意味がない。裁判所が勝手に法律を創造していないかも、市民はしっかりと監視しなければならない。監視することが多くて大変だ。でも事は個人の自由・人権に関わることだから、大変ともいってられないのだ。

◎ そしてこの刑法を適用し、刑罰を科すプロセスを定めるのが、刑事訴訟法だ。実は裁判の手続きを定める刑事訴訟法の方が、はるかに自由・人権との関わりが大きい。

ここで裁判の手続きといっても、それは裁判のための証拠を集める捜査段階から問題になる。無理やりに取調べで強引に作り出された自白調書や、令状もないのにガサ入れして、本当にそこで見つけたかどうか分からないような証拠物、令状に記載されてもいない物まで押収したり、そもそも令状のチェックが

緩すぎるなど。捜査がいいかげんであれば即冤罪につながる。冤罪は再審を請求している事件だけで起きているわけではない。泣き寝入りしている事件も多いだろう。なぜなら冤罪を追及するためには、強大な国家権力相手に、金も時間も労力もたっぶりかけて、名誉回復とわずかな賠償金を求めて闘わなければならないからだ。相手は税金が原資だから金に糸目はないし、裁判所も同じ国家機関の警察・検察にやたらにやさしい。裁判所は警察・検察の集める証拠がなければ裁判にならないもんだから、捜査当局への信頼には絶大なものがある。

◎ 捜査が終わった後も、怪しい証拠が裁判に使われていないかなど、冤罪への落とし穴はいくらでもある。捏造された証拠も大歓迎の裁判所なら、どんなに頑張っても裁判に勝つことはできない。噂とか伝え聞いた話まで証拠にしたり、検察官が勝手に創作した自白調書を裁判官が信じ切ってしまうなら、公平な裁判とは名ばかりの、有罪確立99.9%を誇るためだけの裁判劇場が上演されるだけのことになる。

◎ デジタル技術が捜査や裁判に入り込んでくるとき、その便利さとは裏腹に、ディープフェイクよろしく、その証拠の映像や音声の本物かどうかを確認することははるかに難しくなる。

またデジタル技術はリモートでの対面を可能にするが、それがリアルでの対面の一部を代替することはできても、大きな差があることもまた疑いのないところだ。特に相手の心情・様子は、目の前にいれば自然と伝わってくるものだが、遠隔の映像や音声では十分ではなからう。落ち着かない態度で証言しているのか、声に若干の不安感が感じられるかなど、憲法が保障した公判廷での証人審問権・反対尋問権(憲法37条2項)はだてではない。

デジタルがあたりまえの社会においては、そこで起こる犯罪に適用される刑法もこれに対応した姿に形を変える場面が少なくない。それでも、刑法が刑罰を科し、自由・人権を制約するためのルールである以上、その基本原則を変更することはできない。刑法には罪刑法定主義(criminal legality principle)という基本原則がある。

詳細は後述するが、デジタル空間で罪刑法定主義がどのように展開するかを検討する必要があ

る。なぜならそれはリアル空間を前提とした刑法を想定外のケースにあてはめるものであるという時点で、すでに立法者の想定・授権の範囲を超えた勝手な刑法の適用である可能性が高いからである。

AI、ビッグデータの捜査・裁判での利用についても検討しておく必要がある。すでに捜査技術にも数々のデジタル技術が取り入れられてきている。ビッグデータを基にしたAIは効率性を高めるには有用だが、過度に信頼されれば、例外の存在を捨象して、偏った判断が示されることにもなりうる。

そして自動運転技術と同様に、その責任の所在がどこ、誰にあるのかがわかりにくくなる。ビッグデータの担当者に問題があったのか、プログラマーの組んだプログラムに問題があったのか、それともAIを利用する側の捜査関係者や司法当局者の問題なのか。デジタル技術のブラックボックスの中身は、捜査や裁判の責任の所在まで見えづらくしてしまう問題がある。

デジタルと法と人権の関係は、それ自体としては無色のものかもしれない。ただ逆にそれだけに、警察・検察といった捜査・訴追機関がこれを自分たちに有利に、便利に使おうとすれば、それは問題点の指摘や批判を難しくする、デジタルだから信頼性が高いなどという目くらましのブラックボックスになることは必須だ。

犯罪捜査・刑事司法のデジタル化はまさにこれからだ。偏った既成事実化を見過ごすことなく、①しっかりと法的な裏付けを繰り返し求め、②データ保護・プライバシー保護の原則を確かなものにし、③その収集・保管・利用・評価の全過程について、完全な透明性と説明責任の十分な確保を明確なものとする。こういったことが原則として絶対的に必要とされなければならない。

では全4回にわたって少しくわしく見ていこう。

【内容目次】

- Q1 デジタル空間と刑事法
 - Q1-1 デジタル空間と刑法
 - Q1-2 デジタル空間と特別刑法
 - Q1-3 デジタル空間と刑訴法（以上、本号）
 - Q1-4 デジタル空間と少年法
- Q2 デジタル空間と刑事法学
- Q3 デジタル空間と罪刑法定主義
- Q4 デジタル空間と罪刑法定主義の応用
- Q5 デジタル空間と刑事人権
- Q6 デジタル空間と少年法改正

Q1 デジタル空間と刑事法の関わり の概要とは？

A デジタル空間の特徴としては、それが使い慣れたものであったとしても、ユーザーはその具体的な内容を細部までは知りえないことにあります。自分の情報がどう扱われているかを知る権利が認められつつある中で、デジタル空間では事実上、それとは逆行する事態が進展しています。それはビッグデータの活用という美名のもとで、十分な説明も透明性も中で情報が横取りされ、集積され、リスクに対する説明も責任の所在も明らかでないまま、便利さだけが謳い上げられています。

刑事法は人権に直結する内容を定めた法律です。何が犯罪とされ、どのような捜査や裁判の過程を経て不利益・拘束・刑罰を受けるかは、すべて明らかにされ、透明性と適正さ、外部からの監視が機能する状態で進められなければなりません。裁判官によるチェック、被疑者・被告人・弁護人による監視とチェック、検証作業に耐えるデジタル証拠の開示とその収集過程の記録とが必要です。不透明な手続とは本来相容れないものです。

今のままでさえ、容疑者は逮捕され拘束されれば、弁護人以外とは会うことも禁じられ、留置施設の中でどのような取調べが行われているかは外からは見えません。取調べの可視化といっても、すべての取調べで行われているわけでもなく、容疑者が観念したあとから録画が始まったなら、その適否を判断しようもないのです。

デジタル技術は、その詳細の透明性が確保されず、改変・複製が容易で、そして改変・複製されたことの外部からの検証も必ずしも容易でないなど、これまで現物は一つしか存在しないという証拠の考え方とは大きくずれることになります。それは証拠の信用性の評価と大きく関わります。

これまでのリアルな捜査や証拠の場合以上に、デジタルな捜査や証拠に関しては、それがどのような法的裏付けや裁判官のチェックの下に収集され、どのような保管・

デジタルの便利さを支えるデータ処理。それってじつは知らない間に情報を渡してる？



市民

もしそれが犯罪捜査なら、黙秘権や自己情報プライバシー権は？

鑑定の過程を経て、その内容がどのようなものだったかを時系列であとから全て検証できるように逐一記録する万全の管理体制が確保されなければなりません。

そしてそれはいつでも被疑者・被告人・弁護人サイドからの利用の申し出に応えられるものである必要があります。

Q1-1 デジタル空間と刑法との関わりとは？

A デジタル空間の拡大は、刑法上の犯罪行為もまたその中で行われる時代を生み出しています。もはや泥棒や強盗は目なし帽をかぶってコンビニや銀行に押し込む必要はありません。資産家の子供を誘拐する必要もありません。大企業のサイトから個人情報のデータを盗み出して、それを人質に多大な身代金を受け取ればよくなりました。

他人の名誉を毀損するにも、手元のスマホを操作するだけでいつでも簡単に行えるようになりました。

一方で、リアル空間を想定して作られた刑法をそのまま適用できるかが問題になることも少なくありません。例えばごく仲間うちだけでやりとりするLINEで誰かを侮辱した場合、「公然と侮辱した」という犯罪成立要件にあてはまるでしょうか。

偽名を用いてアダルトサイトを利用したら「虚偽の情報」によるコンピューター詐欺罪が成立するでしょうか。

離婚した妻のスマホに追跡アプリを無断でインストールして居場所を常時把握していたら、ストーカー行為防止法の「つきまとい」にあたるでしょうか。

こうした事例はいずれも、法律ができたときには想定されていなかったものです。法律はもちろんすべてを予想して作ることはできませんが、およそ想定外のケースにまであてはめることは、特に刑法では重要な問題となります。なぜなら刑法は処罰範囲をできる限り明確に、一意に定めることで、処罰されない



自由な領域も同時に定めなければ、市民の自由な行動を必要以上に規制することになってしまうからです。

デジタル空間の規制と自由の線引きを立法者が考えてもいなかった以上、本来は今の国会が時代に見合った新たな規定を立法すればよい話です。それをせずに後追いで裁判所が有罪としてしまうのでは、とても自由を保障するという役割を刑法が果たしているとはいえません。不利益を被るのはいつも、線引きが明らかでない中で現代を生きなければならない市民です。

Q1-2 デジタル空間と特別刑法との関わりとは？

A いわゆる刑法典上の犯罪とは異なり、刑法典以外の法令の中に規定されている罰則規定のことを特別刑法と呼びます。デジタル空間での行為を新たに処罰する規定が置かれる場合があり、例えば著作権法119条3項には著作権侵害コンテンツの違法ダウンロードを罰する規定があります。

そのほかにも、出会い系サイト規制法（正式名「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」）や、迷惑メール防止法（正式名「特定電子メールの送信の適正化等に関する法律」）などの中にも罰則規定が置かれています。

このようにデジタル空間での新しい現象に即応した特別法（特別刑法）が置かれた場合には、その適用範囲は比較的明確です。しかしこれもまたデジタル空間を規制する法律の宿命で、新しいプラットフォームが登場したり、新しいトレンドが次々に登場する流れの速いデジタル空間では、すぐに古くなり、あるいは現状に適合しなくなりがちです。ただこれらの法律は対象とする範囲も明確な分、改正もしやすいという特徴があります。

他方でこうした法律が罰則規定を設けても、その実効性の検証が十分に行われているかについては疑問の余地があります。違法ダウンロードを規制する法律が本当にデジタル著作権保護に有効に機能したのかどうか。業界はむしろサブスクリプション等の利用機会の拡大によって、違法コンテンツや海賊版の流通に対抗しているように見えます。

刑法や刑罰はそれが人権・自由を制約するも

のであるがゆえに、適正な捜査と適正な裁判手続とによって、厳密な検討を時間をかけて行う必要があります。つまり刑法で罰則規定を設けても、それを一人一人に適用するのに多大な労力を必要とするわけです。

デジタル空間は時間の流れの速い世界です。流行り廃りも忙しく、特別刑法といってもいちいちの対応には困難を伴う場合があります。かといって手続の厳密さを犠牲にすれば元も子もありません。刑法が万能でないのはデジタル空間に限った話ではありません。リアルでもデジタルでも、刑法が改正されれば問題が解決するなどということはめったにありません。

変化の速いデジタル空間への刑法の適用の場面では、それが後追いのこじつけの法適用になっていないか、無理なあてはめがなされていないかを十分チェックする必要があります。

Q1-3 デジタル空間と刑事訴訟法との関わりについて?

A 事件が発生し、それが発覚すると、軽微な事案でなければ捜査が開始されます。刑事事件と刑事訴訟法の関わり自体はここから始まりますが、警察の日頃の活動はこれにとどまらず、犯罪が発生する前から様々なデータを各地で集めていることは有名です。Nシステムや指紋・DNAデータの集積など、その法的根拠の疑わしいものがいくつもあります。犯罪も起きていないのにデータを集めるというのは、ただの監視活動でプライバシー侵害の最たるものです。

捜査とは事件が起きて初めて開始され、その起訴価値を見極め、起訴する場合には公判・有罪を支えるための証拠を発見・収集するための捜査機関の活動です。事件が社会の中で発生する以上、デジタル空間の広がった社会の中で起こる事件もまたデジタル要素を帯びてきます。つまり犯罪の痕跡がデジタル空間に残り、それが刑事裁判の証拠とされるわけです。したがって捜査機関の捜査もデジタル空間へと及ぶことになります。

刑事訴訟法も戦前の刑訴法を受け継ぎながら、戦後間もなくして作られた法律ですので、もともとはデジタル空間を想定していません。「物」を集める活動には、当然それが存在する場所という物理的制約がかかり、また同種のものが複数作られていたとしてもそれ自体は唯一のもの

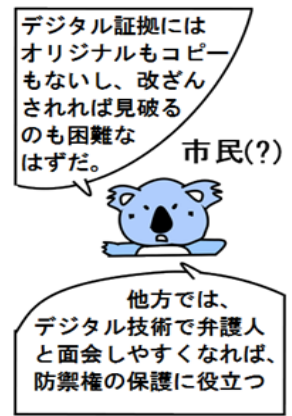
だということができません。しかしデジタルデータは複製されれば、両者はまったく同じもので区別が付きません。それが存在することの証明力も相対化されざるをえなくなる場合があるということです。

普通に生活するだけでもあちこちに行動の痕跡を残さざるをえない現代のデジタル社会の中では、そこに残ったデータが容疑者の絞り込みに利用されます。容疑者の身柄は一つですから、証拠隠滅や逃亡のおそれがあると拘束されます。この間、容疑者は自ら身の潔白を明らかにするための証拠や証人を集める活動が不可能となりますから、外部で代わりに行動できる弁護人が必要となってきます。弁護人は法律や裁判の専門家ですが、事件や依頼人のことは何もわかりませんから、頻繁に連絡をとる必要があります。弁護人が容疑者と面会し打ち合わせることを接見といいます。法曹過疎の地域ではとりわけ遠隔地までの接見が困難となる場合があります。こうした場面ではデジタル技術によるリモート接見といったニーズが存在しています。

そして身柄を拘束されていると否とに関わらず、容疑者や参考人が取調べを受ける際に、録音・録画がなされデータが作成される場合があります。これを裁判で証拠とする場合にも、リアルな証拠物とは異なる問題がありますし、そもそもどのような証拠として扱えるかという問題もあります。

リモート接見も取調べの録画も、デジタル化以前からやろうと思えば可能なはずでした(電話接見、録音テープでの録音)が、デジタル技術の高度化と汎用化が、リアルとの等価的な代替を可能とするようになってきて、その活用を検討せざるをえない状況も招来されたということになるでしょう。

そしていよいよ法廷での裁判手続になると、証人を取り調べるという過程で、事件の関係者が被告人の前では話しづらいとして別室で証言するという手続も用意されており、これをビデオリンク方式といいます。証人の証言にどの程度の信用性があるかというのは、物証の乏しい



多くの事件において決定的な意味を持ちます。ですから証人の尋問のしかたにデジタル技術が加わるというのは、ただ便利だというのを超えた意味を持ってきます。

また刑事裁判との関係に加えて最後に、裁判のあとの話にも触れておきます。近年犯罪数は年々減り続けています。他方で再び何かしらの犯罪を犯してしまうという再犯の割合は逆に増えています。そこにはとりわけ様々な障害や病気の存在のあることが指摘されています。警察や検察は組織維持のために犯罪は減っても凶悪事件は増えているようなことをいい続けてきましたが、さすがにその作戦もあきらめたようです。今度はようやく再犯を減らす、更生だとい

い出しました。犯罪の背後に家庭環境や障害や依存が多く存在する以上、再犯をしないで更生するというのを本人の自覚にすべて委ねるとするのは無理なことです。そのための支援を起訴前の段階（入口支援）と裁判後や出所の段階（出口支援）とで充実させる取り組みが始まっていますが、未だ十分ではありません。そこには警察・検察、裁判所、刑事収容施設、保護観察所といった関係機関の連携が不十分なままだという原因があります。対象者について調べられ・集められたデータをどのように共有することが可能で、どのように活用して連携をとるかといった重要な問題も残されています。（次号に続く）

紹介<<人権の香りがしない民間デジタルIDガイドライン>>

民間事業者向けデジタル本人確認ガイドライン

「https://www.openid.or.jp/news/kyc_guideline_v1.0.pdf
オープンIDファウンデーション・ジャパン [2023年3月]

(CNNニュース編集部)

「民間事業者向けデジタル本人確認ガイドライン（第1.0版）」（以下「民間デジタルIDガイドライン」ともいう。）が公表された。「デジタル本人確認」とは、「デジタルID」のことだ。民間団体（一社）のOpenIDファウンデーション・ジャパンの手によるものである。

デジタル化の大波で、「対面（オフライン）サービス」に加え、リモートの「オンラインサービス」も加速的に増えている。このため、「本人確認」は、対面（オフライン）サービスのみならず、オンラインサービスでも重みを増している。

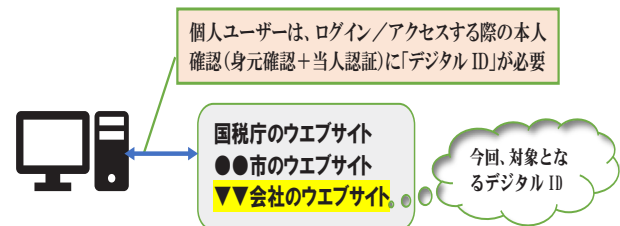
オンラインサービスでは、ユーザー（利用者）が政府／公共機関や民間機関のウェブサイト（ポータルサイト／デジタルプラットフォーム）にアクセス／ログインする際には、デジタルでの本人確認手続が必要になる。サイトの安全や、なりすましその他のサイバー犯罪を防ぐためである。

わが国のオンラインサービスでの本人確認（デジタルID）は、大きく次の2つに分けられる。

デジタルIDの分類

- 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

■オンラインアクセス／ログインのイメージ



①「法令等で本人確認について定めのあるサービス」では、個人の本人確認の対象となるサービス申請の手法、使用するデジタルIDなどについて法令に定められている。一般に、PKI（公開鍵・電子署名・電子証明書）が格納されたマイナICカードの利用が強制される。言いかえると、デジタルIDサービスを提供する民間IT企業が独自にデザインした「ID＋パスワード」式のような技術仕様のデジタルIDは自由に使えない。官尊民

卑、民業圧迫ではないか？との批判も根強い。裁判でも争われた。ガイドラインづくりでは、この裁判で闘った元気のあるスタートアップのIT企業も仲間に入れた方がいい。

とりわけ、マイナICカードは、国の役人の悪巧みで、人権侵害ツール／デジタルトラップ（監視の罠）としての使われ方をしている。安全対策（データセキュリティ）を「偽旗／ニセ旗」に、わざと不正義なデザイン・技術仕様を選んでいるのは明かだ。これは、国家によるマイナICカード取得の強要、健康保険証・介護保険証として利用させる政策、「国内パスポート（inner passport）」に使わせようとする画策を見ればよくわかる。それに、ICカードを使わないモバイルIDアプリが世界標準になっている。このことも悪いシナリオ選りを行っている証になる。ガラパゴス化したマイナICカードは、血税の無駄遣いの傷をさらに広げる。物理的なICカードがないとスマホにデジタルIDを「写経」、できないデザインは明かに時代遅れだからである。

個人用デジタルIDとして実用化された技術仕様

①（アカウント）ID・パスワード式、②PKI（公開鍵・電子証明書・電子署名）式、③生体認証（顔・虹彩・指紋など）式、④二次限バーコード（2D barcode / 商品名：QRコード）[マトリック] や⑤ワンタイムパスワード式 [マトリック] がある。他に、実用化されていない⑥ブロックチェーン（暗号資産）式がある。

②「法令等で本人確認について定めのないサービス」において、個人や企業は、デジタルID、つまり「デジタル本人確認の技術仕様」の自由な選択が認められている。市場主義を原則とする経済社会においては、ある意味では当然だ。公権力が法令で、「デジタル本人確認の技術仕様」の自由な選択を縛るのは、権威主義国家につながりかねないからだ。

国の役人は、個人用のデジタルIDは、ウェブサイトへの単なるリモートアクセス／ログインのツールにしておきたくない。デザインの仕方次第で、最強の国民監視用ツールに転用できると読んでいる。事実、国の役人に「お任せ」の結果、マイナICカード、デジタルIDは、「デザインの不正義」詰め放題になってしまった。

「デジタルID」のデザイン・技術仕様を選択に対する国民、民間企業による監視は重い課題である。国民監視が行き届かないと、唯我独尊の国の

役人の横暴を止められなくなる。公定／実質国定の技術仕様のデジタルIDはたちまち国民をデータ監視する「デジタルトラップ（監視の罠）」に変貌する。

わが国は、G7で、唯一LGBT立法に否定的な国だ。納税者憲章でも同じだ。民間デジタルIDサービスでも、世界の笑いものなっけはいけない。今回の民間の動きは注目に値する。

確かに、横断的な民間ガイドラインもない実情では、デジタルIDサービスを提供する業界での混乱も生じる。例えば、消費者がネット／オンラインで酒類を購入するとする。消費者であるユーザーがネット販売事業者のプラットフォーム／HPにログインし、本人確認をする際には、「年齢」が重要なチェックポイントになる。年齢（生年月日）を除き氏名その他の多様な個人情報を、第三者であるネット販売事業者に提供する必要がない。KYC（Know Your Customer）のような金融機関などと同等の厳格な本人確認は不要だ。消費者にとってもネット販売事業者にとっても「過剰」になる。なぜならば、KYCは、犯罪を防ぐためにサービス利用者の身元を知ることが狙いだからである。

「過剰」は百害あって一利なしである。ということで、いまや、第三者への自己データ提供の自己コントロール権（right of digital self-determination/self-sovereign）の原則を遵守が国際標準だ。つまり、消費者／ユーザーは、自己のプライバシー権を優先させ、ネット販売事業者に最低限の個人情報を提供し、不要な個人情報を提供しない権利があるとされる。

だが、「法令等で本人確認について定めのないサービス」を提供するIT企業にとっては、適正水準の本人確認技術を提供しているのかどうかを判断するのは難しい。何らかのガイドラインがあった方が判断しやすい。とりわけ、ネット販売事業者が、マイナポータルが提供する背番号その他大量の個人情報を提供する厳格な本人確認サービスを活用するのでは、消費者／ユーザー離れにつながりかねない。それに、民間のデジタルIDサービスを提供する企業にとっても「過剰」は望むところでない。

そこで、OpenID ファウンデーション・ジャパンが音頭を取り、有志の民間事業者を集めてタスクフォース（作業部会）を設置し、デジタル庁の協力も得て、この民間デジタルIDガイドラインを策定したとのことだ。

PoentID Japan の民間デジタル ID ガイドラインの概要

- ①本人確認の導入・選択に必要な基礎知識
- ②本人確認手法の特徴の整理
- ③マイナ I C カードや本人確認を巡る最新動向等の紹介
- ④その他

この民間デジタル ID ガイドラインは、ガイドブックと指針の2つの性格を持ち合わせているとのことだ。民間事業者の目的、ニーズに合わせて利用を促し、デジタル ID を導入する際の抛りどころにして欲しいというわけだ。この民間デジタル ID ガイドラインがあることで、デジタル本人確認の理解・普及が拡大し、安心・安全なデジタル社会の実現が期待できるという。

国の役人(目付/めつけ)が何から何まで口をはさむのがこの国の慣わしだ。国民や企業を自立・一人にさせておこうとしないのである。こうした状況を付度したのであろう。このガイドライン作成では、デジタル庁の目付が名を連ねている。

残念ながら、この民間デジタル ID ガイドラインには「人権」の香りがしない。IT 産業界主導とはいうものの、「人権 DD / デューデリジェンス」の言葉が見当たらない。「人権を語るのはご法度！」を合言葉に作成されたからだろう。国の目付・彼らに紐づいたシンクタンク・IT 企業・研究者などからなる産官の「護送船団」、「日本株式会社」が人権エコシステムを迂回して完成させた、

限りなく人権ゼロの内容である。

しかし、人権の香りのしない「日の丸のデジタル ID」のガイドラインでは、世界から疑いの目を向けられるのではないか。このガイドラインで、わが国に、まだ民間活力がある「証」にはなるかどうかは疑わしい？見方によっては、プライバシーを反故にする権威主義国家の目付を付度して、あるいは目付が敷いたルール上でつくられたガイドラインのようにも見える。ある意味では、この「国のかたち」がよくわかるつくりのガイドラインではある。

OpenID ファウンデーション・ジャパンは、アメリカの OpenID ファウンデーションの子団体だという。だが、少しうさん臭さが付きまとう。アメリカでは、公民双方セクターで、デジタル ID として、民間のモバイル ID アプリが使われている。わが国のような国民が嫌がる IC カードに公定/実質国定のデジタル ID を格納して配ったりはしていない。子団体は、国際標準の「人権 DD」を掲げ、虚偽なくアメリカの実情を日本国内でしっかり紹介したうえで発信しないとイケない。でないと、民主主義国家を標榜するアメリカの親団体に誤解されるのではないか？人権に背を向けて「ジャパナイズ (Japanized)」してはいけない。人権ファーストで「アメリカナイズ (Americanized)」を目指した方がいい。わが国の IT 企業は、「何をやっても儲かればいい！」のビジネスモデルをそろそろ卒業しないとイケない。

【最新のデジタル化の動向】 石村代表に聞く！！

Q&A : チャットジブティ (ChatGPT) と税理士の相談業務の行方

(CNN ニュース編集局)

【読者からの質問 (Q)】 「ChatGPT」(チャットジブティ) に恐怖を憶えました。NHK の AI 囲碁将棋放映をゲームみたいに軽く見てました。3月10日に、NHK「クロ現」で開発者のインタビューをみました。良いことを述べ立ててましたが・・・。IT 化どころか、税理士の頭脳は要らない。オペレーターがいれば十分。「AI ヒットラーによる人間支配。悪魔が産まれた、建設亡き破滅・・・」。そんな風に考えてしまうのですが、どうなんですか？

【回答 (A)】 アメリカのスタートアップ IT 企業、オープン AI 社 (OpenAI) の CEO が来日し、同社が開発した「チャットジブティ (ChatGPT)」を PR していました。対話型の AI (人工知能) のチャットジブティを試して見ました。確かにスゴイ威力です。当然、税理士業務、とりわけ判断業務に大きな影響を及ぼすでしょう。

いま、各大学では、学生のレポート提出で、チャットジブティ対応、パクリ対策で、てんやわんやです。私のようなレベルの低い研究者に比べ

ると、チャットジプティの方が迅速かつ正確です・・・(笑)。

東大学長が、4月12日に、東京都千代田区にある武道館で開かれた入学式の式辞でチャットジプティにふれた、と報道されています。「学生に主体的に活用してもらいたいとか?」。ただ、教員の研究でも文系では創造性に欠ける駄文だらけ。なのに、若い学生にどの程度の責任あるチャットジプティの利用を期待できるかは未知数です。

以前、若い教員が、「配布」と「配付」の違いがしっかりしない文書を書いてきました。注意したのですが、違いについて、本人がわかっていないのです。「配布」は一般に広くまくことです。「頒布」とも書きます。一方、「配付」は、会議など特定者に配ることです。で、今回、双方の違いについて、チャットジプティに質問してみました。上記と同じような的確な回答が数秒で即返ってきました(;´Д`)トホホ!!

私は、現在、カナダの税務行政について論文を書いています。不明な箇所は、英語で、マイクロソフトエッジ、チャットジプティに質問してみました。カナダの大学の紀要とかのデータ入手は至難です。しかし、カナダ歳入庁 (CRA) の法令解釈や解釈通達などの所在、専門職団体の意見などについては、データを即入手できます。アクセス先の URL、www も表示されます。ついでに、知合いにカナダの旧友の先生のことを尋ねてみました。「(邦訳) ●●先生の生存は確認できませんでした。しかし、近年、次のような著書を出しています。」の回答。アクセス先の URL、www も表示されます。

もともと、大学の紀要や専門誌などは、各種シンクタンクのアーカイブス、LexisNexs 社のような企業が運営する有料のデータベースに入らないと、ダメですね。チャットジプティだけでは、とても、売り物のなるような質にはなりません。

それに、英語が国際公用語化している時代です。にもかかわらず、わが国では、英語で文献を読めない研究者も少なくありません。むしろ、そうした研究者が増えてきています。チャットジプティの回答内容に「フェイク」あるいは「ミステイク」が含まれる可能性は大いにあります。ですから、チャットジプティを使いこなすには、専門知識をもって判断し直す必要があるのは当たり前です。しかし、原文を英語で読めない人に「判断」を求めると自体、所詮ムリなわけです。

【問 (Q)】 税理士は概して、「税務のデジタル化など●●くらえ」の態度です。電帳法 (電子帳簿保存法)、デジタルインボイスなどが目白押しです。こうした状況で、チャットジプティ (ChatGPT) のような、対話型の生成 AI が競争相手になってきても、生き残れるのでしょうか?

【回答 (A)】 税理士は、リスクリング (学び直し) に励めば、少なくとも IT 技術者として生き残れます。

2023年3月に発表された ChatGPT-4 [GPT-4] は、最新型の生成 AI です。GPT-3.5 から GPT-4 に進化したことで、GPT-3.5 と違って有料 (20ドル/月額約 2,500円) です。

相続税に関する税務処理について、チャットジプティに質問してみても、GPT-4 では、ほとんど誤りはありません。用語の使いこなしなどには少々違和感もありますが・・・。

数年後には、税務相談生成 AI は、格段に進化/深化するでしょう。これまでの10年を1年と考えてください。まだ、特定・個別事例をインプットしても、回答は曖昧です。しかし、納税者が的確な情報を入力すると、相続税額まで自動的に計算できる税理士にとって「悪夢」の時代はすぐそこです。デジタル型超高速度社会です。

現在でも、課税庁は、所得税を対象に記入済み申告制度 (pre-filling tax return system) の導入に動いています。いずれは、資産課税や消費課税を含め幅広い種類の税金で、税理士レスの申告が常識になるかも知れません。ただ、すべてを自動化できるのかはわかりません。

税理士業務のうち、税務相談は、チャットジプティや税務専門職用の生成 AI などの方が優れてくると思います。将来的には、税理士法上の「税務相談業務」は、名称独占、とせざるを得ないでしょう。

一方、税務データの作成業務や税務のデジタル代理は、税理士法上の独占業務として残る? と思います。税務調査も、オンラインのビデオチャット (映像対話) を使う時代になるでしょう。

【問 (Q)】 税務調査のオンライン化、ビデオチャット (映像対話) の利用で、調査手法はどう変わってくるのでしょうか?

【回答 (A)】 そうなると、税務調査の録音・録画は当たり前になります。税務調査時に、税務調査官に録音・録画すると告げると、調査を打ち切って

帰署してしまう、という税務実務は、通用しなくなります。当然、これまでの税務調査実務は大きく変わります。

アメリカやオーストラリアなど多くの先進諸国では、オフライン／リアルの税務調査ではオーディオ録音は常識になっています。今後、オンラインのビデオチャット（映像対話）を使った税務調査が普遍化すれば、調査の録音・録画をデータで保存する実務は広く一般化すると思います。そして、保存された調査の録音・録画データをAIで分析するという方向に進むと思います。

【問 (Q)】 課税庁が、税務調査結果をAI分析にかける方向に進むのでしょうか？

【回答 (A)】 税務調査のデジタル化、調査結果のAI分析は、最も重い課題です。今回は、深くふれませんが。AIにインプット（入力）されるアルゴリズム（情報処理手順）次第では、分析結果に大きな違いが出てきます。つまり、AIに、「疑わしきは納税者の利益に」の考え方を入力すると、「疑わしきは課税庁の利益に」の考え方をいれるのでは、結果に大きな違いが出てきます。ですから、税務当局によるアルゴリズムを使い方を、納税者を、どう「監視」、どう「評価」するのが重い課題になります。

名古屋税理士会がドイツの税理士会を訪問し、税務のデジタル化について話し合ったそうです。その際に、ドイツ側が、「課税庁が税務AIにインプットするアルゴリズムをどのように透明化するのが重い課題だ」と指摘したそうです。ところが、日本側は「デジタル化など●●くらい」の態度ですから、何を言っているのか理解できなかったそうです。参加していたITに強い税理士の方は、「わが国の税理士はデジタル化についてはゾンビ集団だなあ・・・」と実感したとのことでした。

チャットジプティ (ChatGPT) でも同じです。税理士によっては、「使えない、使いたくない」が当り前の態度で、「紙様、万歳！」です。これでは、絶滅危惧種になるのは防げないわけです。転落は避けられません。

もっとも、もう少しすると、小さいときからデジタル／ネット環境で育ってきた「デジタルネイティブ」が社会の中核を占める時代がきます。デジタル当り前の税務専門職が救世主になるのでしょうか。世代交代でうまくいくと思います。

デジタル時代においては、モバイルファースト

で行政サービスを受ける市民／国民の権利を保障するのが世界の流れ（国際標準）となっています。このことも頭に叩き込んで、税務専門職業務をすることが大事です。

【問 (Q)】 2023年3月28日に税理士法改正が成立しました。この改正で、「非税理士等による税務相談停止命令制度」が設けられました【詳しくは、TCフォーラム意見書【2023年3月1日（3月3日微訂正）】 | 納税者権利憲章をつくる会 / TCフォーラム (tc-forum.net)】。税理士でない者が繰り返して税務相談をした場合、財政当局がストップを命令できる制度です。これは、どうとらえたらよいのでしょうか？

■ 税理士等でない者に対する税務相談停止命令制度のつくり

要件
①税理士等（税理士・税理士法人）でない者が
②税務相談を行った場合、
③更に反復して税務相談が行われることにより、
④不正に国税・地方税の賦課・徴収を免れさせる又は還付を受けさせることにより、納税義務の適正な実現に重大な影響を及ぼすことを防止するために、
⑤財務大臣が緊急に措置を取る必要があると認めるときに、
⑥国税庁長官が、⑤のための調査する必要性があると認めるときは、相談を行った者への報告徴収、または国税庁・税務署職員による質問・検査を実施
⑦財務大臣が停止等必要な措置の命令（停止命令） +停止命令の官報による公告／インターネットへの公表 +公告は相当と認める期間はおおむね3年間 +停止命令違反は1年以下の懲役又は100万円以下の罰金 +質問検査等拒否または虚偽答弁等は、30万円以下の罰金

【回答 (A)】 税理士業務「無償独占、ルールを悪用した、当局による税理士のワグネル化／傭兵化策です。時代遅れの役人の悪巧みのように見えます。当局は、リアル／オフラインばかりか、ネット／オンラインで脱税指南し、税理士法違反でカネを稼いでいる連中を退治する武器を用意するための改正だと豪語しています。どうでしょうか？「チャットジプティは、税理士等でない者で、繰

返し税務相談をしている。税理士法違反で、納税義務の適正な実現に重大な影響を及ぼす」とみることもできます。当局は、無茶を承知で、停止命令を出してみたらいいと思います。

この国に、マイクロソフトの後ろ盾にグローバルな事業展開をしているオープン AI 社のチャットジプティを叩ける国力はないわけです。叩いたら、「日本は `word、を使うな！」で反撃されたらどうしますか？（日本は「一太郎」で頑張れる??）

【問 (Q)】 マイクロソフトの強敵、グーグル (Google) も対話式 AI を開発しているのでしょうか？

【回答 (A)】 OpenAI + マイクロソフト陣営の動きに対して、検索エンジンとしてシェア No.1 のグーグル (Google) は、「バード (Bard)」と呼ばれる対話型 AI を発表し、対抗する構えです。グーグルバード (Google Bard) はこれまでの検索方法とは違って、人と会話するような文章で AI に質問をすることができ、AI がビッグデータを使つて的確で、ナチュラルな回答をしてくれるのが特徴、といわれています。

グーグルは、2023 年 3 月 21 日に、アメリカとイギリスでバード (Bard) の実験版を公開しました。米英のユーザーはグーグルバード (Google Bard) を利用することができます。日本版については、いつ開始されるのか明らかではありません。

ほかにも、続々と、対話式 AI が出現してくると思います。中国も、権威主義国家観に基づく対話式 AI の開発に着手しています。指導者に関する質問には回答が出てこないなど、民主主義国家観に基づく対話式 AI とは一味違うつくりのようです。

ちなみに、チャットジプティ (ChatGPT) を開発したオープン AI 社は、23 年 4 月に入ってから、「バグ報奨金プログラム (Bug Bounty Program)」を始めました。チャットジプティ (ChatGPT) の脆弱性 (bug) を発見し、通報した人には、重大性と影響度に応じて 200 ドル (2 万 7000 円) ~ 2 万ドル (270 万円) の報奨金を支払うというものです。市民参加を得て、チャットジプティ (ChatGPT) の清廉性を高めるためです。

【問 (Q)】 税務や法律などの専門職は、デジタル化、チャットジプティのような対話型の AI の展開とどう折り合いをつけたらよいのでしょうか？

【回答 (A)】 御心のままにです。逃げられないのです。税務のデジタル化の大波は、新たな産業革命なのです。機械打ち壊し (ラダイト) 運動をしても、生き残れません・・・(-_-;)!! いずれにしろ、ガラ系の専門職としての生存は至難です。「どんとこいデジタル化！」で、しかも IT 投資をケチらないことです。ケチると生き残れません。それに、IT / デジタルに弱い税理士は、徹底した「リスキング (学び直し)」、「リハビリ」が要ります。もちろん、額に汗して糧を得られる健康な職種に転じるのも一案です。

なぜならば、AI 専門家がいうには、今般のチャットジプティ (ChatGPT) のような対話式 AI の出現は、「ホワイトカラーのほぼすべての業種に何らかの影響を及ぼす可能性が高い」からです。

こんな回答を書いているのは本当に疲れます (-_-;)。もうほとんどチャットジプティ (ChatGPT) か、生身の人間なのかわからなくなります (笑)。止めにしましょう。

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 <i>Published by</i>
	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 2023.5.4 発行 CNN ニュース No.113

入会のご案内
季刊・CNN ニュースは、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 のつばやき
・「デジタル ID とは何か！」で未来が読めた。世界は「モバイル ID アプリ」が主流で、マイナ IC カードは、人権ストレスも高く、絶滅危惧種だ。「ガラパゴス日本」は売りにならない。変化に機敏になり、血税の垂流しの愚策を即やめよう。 (N)