デジタル社会において人間の自律性と民主主義を守るため、自己情報コントロール権を確保したデジタル社会の制度設計を求める決議

当連合会は、２０１０年の第５３回人権擁護大会において、「デジタル社会における便利さとプライバシー～税・社会保障共通番号制、ライフログ、電子マネー～」と題するシンポジウムを開催した。私たちの行動の足跡がデジタル社会に残ってしまうライフログの実情に迫り、これを利用した行動ターゲティング広告の問題点を指摘し、また当時政府が創設を目指していた共通番号制度の問題点を明らかにしながら、デジタル社会における自己情報コントロール権の実効的な保障を提言した。

それから１２年が経過し、スマートフォンが普及して、ツイッター（Twitter)、フェイスブック（Facebook)、インスタグラム（Instagram）などＳＮＳを利用したり、ユーチューブ（YouTube）等のデジタル動画を視聴したりする頻度が高まるなど、市民の行動は変容を遂げている。行動ターゲティング広告の有効性が周知のものとなり、企業からすると、少ない宣伝コストで従前と同様の売上げが得られるようになっている。

他方で、デジタルプラットフォーマーは、利用者が入力した検索キーワード、閲覧した記事やユーチューブチャンネルの履歴、スマートフォンのＧＰＳ機能をオンにしていることにより蓄積されていく移動履歴など、当の本人では到底覚えておくことの不可能な膨大な情報を記録し、個人の将来の行動を予測するために活用し、収益を上げている。デジタル社会での行動履歴は丸裸と言っても過言ではないほどのプロファイリングに供され、プライバシーの危機を招いている。

私たち自身が、自律的な判断をするために必要な情報アクセスが確保されないといった問題もある。自分と似た興味・関心・意見を持つ利用者が集まるコミュニティが自然と形成され、自分と似た意見ばかりに触れてしまうようになる「エコーチェンバー」現象、自分好みの情報以外の情報が自動的にはじかれてしまう「フィルターバブル」などにより、偏った意見や真実ではない意見に囲まれてしまい、自然な意思形成ができないこともある。２０１６年のアメリカ大統領選挙で、プロファイリングに基づき分類したグループごとにきめ細やかな投票行動の誘導を行って、市民の投票行動に意図的に影響を与えた疑いのあるケンブリッジ・アナリティカ事件も明るみに出ている。一人一人の市民が自己決定するのに十分な情報へのアクセスを確保し、民主主義社会に参加できる制度が必要である。

このような中、２０２１年９月にデジタル庁が発足し、日本の「デジタル社会化」の司令塔として強力な権限を発揮しようとしている。その政策は、データの徹底的

な利活用を図ることを目指し、個人番号カードの全国民への普及、個人番号（マイナンバー）の利活用促進を中心とした計画となっている。個人番号は、当初の税・社会保障の目的とは関連性の乏しい国家行政事務に利用範囲が広がり、個人番号カードを通じた民間事業者におけるデータベースの作成には制限がない。デジタル改革関連６法により個人情報保護法制も改正され、地方自治体による住民のプライバシー保護機能の低下が懸念される。

さらに、日本では、警察による捜査を始めとした顔認証システムの活用が、法律によるルールの策定もなく無限定に広がっている。中国では、約６億台の顔認証機能付きの街頭監視カメラにより、住民全員の個人情報データベースの検索がなされ、信用スコア（個人にひも付く様々なデータを基にＡＩが個人の信用力を評価し、点数化したもの）と連動して人々の行動を監視しているが、このままでは日本も類似した社会となることが危惧される。十分なプライバシーへの配慮を行わないままに顔認証システムを実用化することには重大な問題がある。

情報主体である私たち主権者は、行政機関や民間事業者によってデータを収集・分析・利活用されるただの客体に成り下がり、一人一人の市民の自己決定や自己実現が妨げられ、市民社会全体が萎縮するおそれすらある。

デジタル社会の制度設計にはあらかじめプライバシー保護措置を組み込んでおくことが必要である。その制度設計に市民自身が参加し、その意見を反映させることができなければ、事後的にプライバシー保護を図ることは困難である。

当連合会は、上記の第５３回人権擁護大会において、「『高度情報通信ネットワーク社会』におけるプライバシー権保障システムの実現を求める決議」を採択したところであるが、その後、デジタルプラットフォーマーの活動が著しく広がったこと、政府の主導により、官民を横断するデータの利活用が強く推進されていることを踏まえ、以下のとおり、国に対しデジタル社会において人間の自律性と民主主義を守り、プライバシー権・自己情報コントロール権を確保するための法制度や原則の確立を求める。

１　デジタルプラットフォーマー（プロバイダ、通信事業者を含む）に対する自己情報コントロール権を確立し、民主主義の基盤を崩さないようにするため、以下の内容を含む法律を制定すべきである。

(1) クッキー（Cookie）を始めとした、市民のデジタル社会における行動履歴を同定し得る情報については、事前同意を要件として取得するものとし、同意が得られない場合にもサービスから排除しないこと。

(2) 収集している個人情報のみならず、個人識別可能性のある情報についても、

その種類、利用範囲を明示し、利用結果、第三者提供の結果についての公開を図ること。

(3) 利用者に対して、プロファイリングされない権利、削除権、データポータビリティ権等、ＧＤＰＲ（一般データ保護規則）で規定される諸権利を保障すること。

(4) 収集した情報に対して適用されるＡＩのアルゴリズム（ディープラーニング後のものも含む）及びその適用後のデータ処理について、少なくともその基本構造を公開し、説明すること。

(5) フェイクニュースに対する自主規制ルールの設定と実践を行うとともに、その結果を公開すること。

(6) 信頼性の高い情報、多様な意見との接点の確保が図られるためのアルゴリズムの設定、実践を行うとともに、その結果を公開すること。

2　デジタル社会における市民のプライバシー権・自己情報コントロール権の保障を実質化するため、以下の点を現行法の改正又は新たな法律の制定によって具体化すべきである。

(1) 個人情報の保護に関する法律（個人情報保護法）について、以下の諸点を改正し、プライバシー保護をＧＤＰＲと同水準に引き上げるべきである。

① 収集の必要性・相当性のない個人情報を処理しないこと。

② 他の情報と組み合わせれば個人識別が可能となり得るような個人識別可能性のある情報についても、保護の対象とすること。

③ プロファイリングされない権利、削除権、データポータビリティ権等を保障すること。

④ 個人情報保護委員会について、プライバシー保護に専念する機関とするようその存在目的を設定し直し、調査権限等を充実させて、プライバシー保護機能を強化すること。

(2) 公権力が、自ら又は民間事業者を利用して、市民のデジタルデータを網羅的に収集・検索する方法で監視する行為を禁止すること。

(3) 個人番号や個人番号カードが、行政機関や民間事業者による情報監視の基盤とならないよう、個人番号制度は抜本的な見直しを行うか、個人番号及びマイキーＩＤ等といった個人識別符号の利用範囲の大幅な限定等を行うこと。

(4) 既存の政府の情報収集機関のほか、デジタル庁や警察庁サイバー局の設置等により、公権力による個人情報の収集管理が強化されている状況において、情報機関の監視権限とその行使について、厳格な制限を定め、独立した第三者機

関による監督を制度化すること。

(5) 顔認証システムについて、法律により、官民を問わずその利用を原則禁止とした上で、厳格な設置・運用条件を設定するとともに、その基礎データを供給し得る監視カメラについても厳格な設置・運用条件等に関する要件を明示し、さらに個人情報保護委員会の管理監督下に置くこと。

3　日本のデジタル社会の推進に当たっては、市民のプライバシー権・自己情報コントロール権の保障を実質化するとともに、デジタル政策を民主化するため、政府は、以下の諸点を遵守すべきである。

(1) 市民のプライバシーを最大限保障することを大前提として、同意原則を十分に尊重し、不同意者に不利益を与えないように制度を設計し、その範囲で利便性や効率化等を図ること。

(2) プライバシー影響評価を事前に行った上でその結果を公表し、市民の意見を反映し、あらかじめプライバシー保護に配慮した制度設計を行うこと（プライバシー・バイ・デザイン)。

(3) 行政の効率化を最上位の目標とすることなく、必要なシステムの設計においても、最大限に地方自治を尊重したものとし、また地方自治体レベルでの設計も許容することとし、かつ意思決定に際しては地方自治体の意見を十分に聴取して、これを反映させること。

(4) 市民提案型の制度を採用するとともに、それが実現されるまでの間においても、制度設計について、行政機関、業界側だけでなく、消費者側、市民側の代表者を少なくとも半数程度は参加させ、その意見を反映させること。

(5) オンライン上で生成される個人情報の蓄積・管理、運用に関して、市民自らが個人データの秘匿や共有をコントロールできる仕組みを確立すること。

当連合会は、デジタル社会において人間の自律性と民主主義を守る決意である。

以上のとおり決議する。

２０２２年（令和４年）９月３０日

日　本　弁　護　士　連　合　会

提　案　理　由

第１　２０１０年以後の、自己情報コントロール権を実質化する法制度の課題

当連合会は、２０１０年の第５３回人権擁護大会において、「『高度情報通信ネットワーク社会』におけるプライバシー権保障システムの実現を求める決議」を採択し、以下のとおり、デジタル社会における自己情報コントロール権の実効的な保障を提言した。

１　情報通信技術が進展する中で、自己情報コントロール権を実効的に保障するため、自分の情報が、どのように収集・利用等されるかについて、本人がその目的等を具体的に理解し予測できるような形で事前に告知され、それに基づいた同意ができる仕組みを、法原則として明示すること。

２　その原則を担保するため、情報通信技術の進展にあわせて、明確な個人識別性のないライフログなどの情報にも法規制が及ぶように改めるとともに、極力匿名化を行うことや、目的達成のために不必要な個人情報は収集しないようにするなど、具体的な法原則を明示すること。（※なお、ライフログというのは、２０１０年当時に使用されていた用語であり、総務省のライフログ活用サービスＷＧでは「利用者のネット内外の活動記録（行動履歴）が、パソコンや携帯端末等を通じて取得・蓄積された情報」と定義されている。）

３　国民一人一人に業務分野をこえた共通番号を割り振るなど、個人の自己情報コントロール権を侵害するような「番号制」の導入を行わないこと。

４　大量の個人情報収集システムを構築等する場合は、プライバシーに対する影響評価の実施と結果の公表を義務付け、問題点を回避または緩和するための変更を促す仕組みを構築すること。

５　調査権など十分な機能を有する、行政から独立した第三者機関（プライバシー・コミッショナー）制度を確立し、本人の自己情報コントロール権を補完すること。

しかし、１２年を経過した現在、ＡＩ（「Artificial Intelligence」の頭文字を取ったものであり、人工知能を意味する。普遍的な定義はないが、『令和元年版情報通信白書』（総務省、２０１９年７月）において、ＡＩは「人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている。」と記載されている。）による包括的な人物像の把握（プロファイリング）において重要な意味を持ち、インターネットの閲覧履歴を統合する要となるクッキー（Cookie）等の利用に対する事前同意が、電気通信事業者に対してすら義務付けられず、事業の種類を問わずに事前

同意が求められているＧＤＰＲ（General Data Protection Regulation（一般データ保護規則））との間で、プライバシー保護のレベルが大きく乖離している。このＧＤＰＲは、ＥＵ域内の個人データ保護を規定する法として、２０１６年４月に制定され、２０１８年５月２５日に施行されたもので、ＥＵ加盟国による法制化を要せず、加盟国に同一かつ直接の効力を持つものである。

また、そもそも収集等の必要性のない個人情報の処理を原則として認めないＧＤＰＲとは異なり、個人情報の保護に関する法律（以下「個人情報保護法」という。）においては、収集した個人情報の利用目的・範囲等を明示するという限度で取扱ルールの遵守を求めている。そのため、個人情報保護法の施行以前から判例理論において承認されていた、肖像権･プライバシー権保護のための、同意があるか又は収集の必要性・相当性がなければ利用できないという原則を外れ、利用目的・範囲等を明示すれば、同意や必要性・相当性の有無に関係なく自由に収集等が許されるかのような誤解も見受けられる。

さらに、行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「個人番号法」という。）が２０１３年に成立したが、その後、個人番号の利用範囲は拡大されつつある。

個人番号を含んだ個人情報（特定個人情報）の処理に限定した監督権限を有する第三者機関として創設された個人情報保護委員会は、その後、個人情報保護法の第三者機関として位置付けられた結果、監督権限が、民間分野の個人情報全般、さらには行政機関等の保有する個人情報にまで拡大しているが、なおプライバシー保護のための監督機能が弱いという根本的な問題を抱えている。

したがって、２０１０年当時に必要と考えられていた自己情報コントロール権を実質化するための速やかな法制度の整備が早急に不可欠である。

第２　２０１０年以降のデジタル社会の進展

２０１０年以降、世界中でデジタル社会は更に進化を遂げている。

日本では２０１０年代にスマートフォンが飛躍的に普及し、画像を含めた情報が発信される量は飛躍的に増大した。ツイッター（Twitter）、フェイスブック（Facebook）、インスタグラム（Instagram）などのＳＮＳやユーチューブ（YouTube）等の利用が進んでいる。

デジタル社会では、市民の滞在時間や検索した言葉、閲覧した動画、さらにはスマートフォンを持って移動した全ての移動履歴など、様々な情報が、グーグル（Google LLC）、フェイスブック（現メタ・プラットフォームズ（Meta Platforms, Inc.））、アップル（Apple Inc.）等のデジタルプラットフォーマー（以下「ＤＰ

Ｆ」という。）によって確認・利用され、市民がそのような利用の現状を正確に理解できないままに利活用されている。ここにいうＤＰＦとは、デジタルプラットフォームを運営･提供する事業者を指す。また、デジタルプラットフォームは、概要「多数の者が利用することを予定して電子計算機を用いた情報処理により構築した場であって、当該場において商品、役務又は権利（以下「商品等」という。）を提供しようとする者の当該商品等に係る情報を表示することを常態とするもの…を、多数の者にインターネットその他の高度情報通信ネットワーク…を通じて提供する役務」と定義付けられている（特定デジタルプラットフォームの透明性及び公正性の向上に関する法律第２条第１項柱書)。

インターネット上の行動履歴に基づき解析された趣味嗜好を標的として配信される行動ターゲティング広告により、市民は関心のある商品・サービスにアクセスしやすいという利便性を獲得し、企業は広告費用を削減することができる。ＤＰＦは、大量の市民情報を活用して高収益を上げている。

反面、プロファイリングは、人間にはおよそ不可能な、趣味・嗜好までをも含めた個人像を丸裸にすると言っても過言ではないほどの解析力を持っている。

ＤＰＦが使用しているアルゴリズム（普遍的な定義はないが、デジタル市場における競争政策に関する研究会の報告書『アルゴリズム／ＡＩと競争政策』（２０２１年３月）では「入力を出力に変換する一連の計算手順」と定義されている。）は、利用者の興味・関心に近い意見や動画を次々と勧めるよう設定されているため、一度極端な意見に接すると、科学的根拠がなくても、類似のおびただしい同種意見が次々と表示され（エコーチェンバー（自分が好んだ意見と同種の意見に取り囲まれること))、繰り返し情報に接していくうちに、利用者は確信が深まっていきやすい。翻って、冷静にその科学的根拠を見つめ直す機会、異なる多様な意見に接する機会を失いやすい。新型コロナウイルスワクチンに関して、アメリカ合衆国では「マイクロチップが埋め込まれる」、日本でも「遺伝子が書き換えられる」とのフェイクニュースが席巻し、家族内・社会内での信頼関係の分断が起こったり、２０２０年のアメリカ合衆国大統領選挙でも、投票で不正に票が盗まれたとの情報を信じている市民が今なお相当な割合で存在したりするなど、市民社会を分断する一つの要因ともなっている。自分と異なる意見と接する機会を失わせたり（フィルターバブル)、不正確な情報で取り囲んでしまい、陰謀論による一種の洗脳状態に陥らせたりする弊害事例に対しては、速やかな対策が求められる。

さらには、プロファイリングは民主主義の根幹である投票行動さえも誘導するようになっている。２０１６年に行われたアメリカ合衆国大統領選挙において、

勝者側が利用した選挙コンサルティング会社であるケンブリッジ･アナリティカについては、２０１８年３月、フェイスブックから取得した８７００万人分のプロフィールを基に細かく有権者をターゲティングし、投票行動を左右した疑いが明るみに出た。

ＡＩのアルゴリズムは、いつ、どのようなタイミングでその広告を表示すれば最も効果的かということまで計算し、人の心理を操っている。フェイクや誤解を生む情報も大量に流通させ、異なる意見との接点をブロックするＡＩによる情報管理は、多様な言論を尊重し、熟議を深めていく民主主義の存続を危うくしている。これは、人間の自律性を脅かす、ＡＩによる民主主義に対する危機と言える。

そのため、以下に述べるとおり、２０１０年以降に進展したデジタル社会に対応したプライバシー保護、及び自由で多様な情報流通の確保を通した民主主義の過程の保護のための法整備が必要となっている。

第３　ＤＰＦ向けの規制の必要性と内容

１　プライバシー保護について

デジタル社会においては、個人のあらゆるデータを収集・集積するだけでなく、こうしたデータを基にコンピュータ（ＡＩ）の解析により「パターン」や「相関関係」を引き出し、この「パターン」や「相関関係」をデータベースに適用し、データベース登録者の趣味嗜好、健康状態、心理状態、性格、行動、能力、信用力などを予測し（プロファイリング）、この予測結果を特定の目的のために利用するというサイクルが出来上がっている。その基盤をなしているのがグーグル、アマゾン（Amazon.com,Inc.）、フェイスブック、アップルに代表されるＤＰＦである。

このようなデジタル社会は、私たちの生活に利便性をもたらしているが、他方で、本人の知らないところで個人情報が収集され、寄せ集められた個人情報により本当の自分と一致しないプロファイリングがなされ、自分が自分として扱われる（評価される）という人格的生存が尊重されず、あるいは自分が自律的・主体的に行動する自由を妨げられたり、差別されたりするといった不利益を受ける可能性が生じている。

プライバシー保護は、このような事態を防止し、個人の尊重を実現するためにある。すなわち、プライバシー保護は、私たち一人一人が属性に関係なく、自律した人格的主体として尊重される社会を実現・維持するために必要不可欠なものである。そして、個人情報が無限定に利用されるデジタル社会においてプライバシー保護を実現するためには、本人が個人情報をコントロールできる

仕組みが必要不可欠であり、その意味で現代におけるプライバシー権は自己情報コントロール権を中心に理解されている。

このような考えに基づき、デジタル社会におけるプライバシー保護を実現するためには、以下の法制度が必要である。

(1) ＤＰＦなどの事業者のほか、他人の通信を媒介する電気通信サービスを提供している事業者らをも含む電気通信事業者が、市民のデジタル社会における行動履歴を同一人のものであると識別するための手段がクッキー等である。既に２０１０年の人権擁護大会決議で提言したように、その利用に対して事前同意を必須のものとすることは、市民がデジタル社会におけるプライバシーを確立する大前提のものとして必要不可欠である。また、形式的には事前同意を採用しつつも、同意をしない限りサービスから一切排除する形で同意を事実上強制する運用が一部で行われているが、これは必要性・相当性に欠ける個人情報の利用として適切ではない。この点、ＧＤＰＲは、クッキーのようなそれ自体では個人を識別するものではない情報も個人データとして保護の対象とし（ＧＤＰＲ第４条第１号)、管理者（個人データを取り扱う事業者）がクッキー情報を含む個人データを処理するには本人（データ主体）の同意が必要であることを定め、その同意の条件について厳格に定めている（ＧＤＰＲ第７条)。

すなわち、ＧＤＰＲ第７条は、管理者に本人の同意の存在の立証責任を課し（第１項)、同意の条件として、本人の同意が他の事項を含む書面において与えられる場合には、同意の要請は、分かりやすく容易にアクセスできる形式で明確かつ平易な言葉を用いて、他の事項とは明確に区別される方法で提示されなければならないこと（第２項)、本人はいつでも同意を撤回する権利を有すること（第３項)、同意が自由に与えられたものであるか否かを評価する場合、特にサービス規約を含む契約の履行にとって不要な個人データの処理への同意を条件としているか否かが最大限考慮されなければならないこと（第４項）を定めている。そのため、クッキーに同意しなければウェブサイトを閲覧するなどのサービスを受けられない形での同意の取得は自由な同意とは認められない。また、ＧＤＰＲを具体化・補完した電子プライバシー指令（欧州議会・理事会指令２００２／５８／ＥＣ）では、ウェブ追跡のためのクッキー利用について利用者の同意が必要であると定め（同指令第５条第３項)、インターネットのウェブ・オペレーターが利用者から同意を取得する際に、その同意が真正なものであるというためには、①クッキーが設定されることに関する具体的で特定された情報の提供、②クッキーが

設定される前の事前のタイミングの同意、③利用者の積極的な行為又は能動的な振る舞いによる同意、④自由な選択が必要であるとされている。

日本においても、２０２０年の個人情報保護法改正によって、「個人関連情報」が創設されてクッキー規制が一部導入されたが、例外が多い上、本人同意の条件についてはＧＤＰＲのような厳格な定めになっていない。

したがって、クッキー等の事前同意及び同意が得られない場合もサービスから排除しないことを明記する法制度が必要である。

(2) また、市民がデジタル社会においてサービスを利用することの反面として、自らの個人情報がどの範囲でどのように利用されているのか、特に第三者に対してどのように提供されているのかについて、具体的に把握することは困難になりつつある。自己情報コントロール権を実質化する観点から、自らの閲覧履歴等の利用範囲はある程度具体的にイメージできるように説明を受ける機会がない限り、それに対する有効で実質的な同意を付与することは困難である。

したがって、収集している個人情報のみならず、個人識別可能性のある情報についても、その種類、利用範囲を明示し、利用結果、第三者提供結果についての公開を義務付ける法制度が必要である。

(3) ＧＤＰＲは、個人（データ主体）に対し、管理者が行うプロファイリングについて、異議申立権（中止請求権）を保障している（ＧＤＰＲ第２１条)。また、個人は、プロファイリングを含む自動処理のみによって、自身に法的効果を及ぼす、又はそれと同程度に自身に重大な影響をもたらす決定を下されない権利を有する（ＧＤＰＲ第２２条)。このようなプロファイリングに対する権利保障は、個人の人格的生存の尊重を実現するためには不可欠なものであるが、日本の個人情報保護法にはこれらに対応する規定が存在しない。

また、ＧＤＰＲは、一定の要件の下で、個人データの削除権（忘れられる権利）を保障し、データ管理者は遅滞なく個人データを削除する義務を負うと定めている（ＧＤＰＲ第１７条第１項)。これは、時の経過によりもはや関連性・必要性のなくなった個人データを削除することを保障することで、過去によって現在及び未来が不当に支配されないようにし、もって個人の人格的生存の尊重を実現するものである。これに対して、個人情報保護法では、①目的外利用や不適正利用、不適正取得があった場合や、②事業者が保有個人データを利用する必要がなくなった場合、重大な漏えい事故等が発生した場合、及び本人の権利又は正当な利益が害されるおそれがある場合の利用停止・消去請求権が認められているが、①の場合については事業者は違反を是

正するために必要な限度で利用停止等することを義務付けられているにとどまり、②の場合についても事業者は本人の権利利益の侵害を防止するために必要な限度で利用停止等をすることを義務付けられているにとどまる。また、利用停止等に多額の費用を要する場合等には代替措置で対応することもできるとされており（同法第３５条）、削除権・忘れられる権利が十分に保障されているとは言えない。

なお、裁判例では、民法上の人格権侵害を理由とする検索エンジンに対する検索結果表示の差止めを認めたものがある（さいたま地方裁判所２０１５年１２月２２日決定／判例時報２２８２号８２頁は「忘れられる権利」を認めた）が、最高裁判所２０１７年1月３１日決定は「忘れられる権利」には言及せず、削除の要件もＧＤＰＲのような等価的比較衡量を採用しておらず、厳格に過ぎる（最高裁判所２０２２年6月２４日判決は、犯罪歴のツイートの削除を認めたが、検索結果表示の差止要件を緩和する趣旨ではないと考えられる。）。名古屋地方裁判所２０２２年1月１８日判決は、人格権に基づく妨害排除請求として、無罪判決が確定した元被告人の指紋データ、顔写真データ及びＤＮＡ型データの抹消を命じたが、これを保障する法制度は存在しない。

さらに、ＧＤＰＲは、ある相手に預けていた自己のデータ群を別の相手にそのまま移行させる「データポータビリティの権利」を保障している（ＧＤＰＲ第２０条）。これは、消費者がある事業者（管理者）から受けているサービスを他の事業者（管理者）のサービスに変更することの障壁をなくすものであり、同意の任意性のための重要な前提条件でもある。自己情報コントロール権の一つと位置付けられるが、個人情報保護法にはこれを定めた規定は存在しない。

したがって、利用者に対して、プロファイリングされない権利、個人データ削除権（忘れられる権利）、データポータビリティ権等ＧＤＰＲで認められた諸権利を保障する法制度が必要である。

２　民主主義の確保について

ＤＰＦが提供する業務は、今や多くの市民にとって日常生活の重要な一部を形成している。ニュースその他の情報へのアクセス、市民同士のコミュニケーションなど情報収集あるいは情報発信の場面で、市民はＤＰＦに大きく依存している。主権者として政治に対する的確な判断と意見を形成するためには、市民が多様な情報に接し、意見交換を行うことが重要である。ＤＰＦから得られる情報に偏りがあれば、市民による的確な判断や意見形成もなし得ない。

行動ターゲティング広告の進展に見られるように、事業者は提示する情報と人々の行動パターンをＡＩを通じて学習し、人々の趣味嗜好を単に把握する段階から、積極的に誘導・形成する段階になってきている。人々の購買活動に対するこういった働き掛けが政治的な意見形成に応用されると、主権者の意思形成の歪曲化につながる。民主主義にとって大きな脅威であり、何らかのルール化が必要である。

ＥＵの「デジタルの権利とデジタルの１０年のための原則に関する欧州宣言」（欧州委員会、２０２２年1月２６日）は、「全ての人は、デジタル環境において、十分な情報を得た上で自分自身の選択を行い、健康、安全、基本的権利に対するリスクと害から保護された上で、人工知能の利点を享受できるようになる必要がある」と宣言した上で、アルゴリズムの透明性確保などを規定している（同宣言 III 章)。こういった海外での動きも踏まえ、ＤＰＦは、収集した情報に対して適用されるＡＩのアルゴリズム（ディープラーニング後のものも含む）及びその適用後のデータ処理について、少なくともその基本構造を公開し、説明する必要がある。

フェイクニュース（総務省の解説によれば、フェイクニュースの定義は研究者によって様々であり、嘘やデマ、陰謀論やプロパガンダ、誤情報や偽情報、扇情的なゴシップやディープフェイク、これらの情報がインターネット上を拡散して現実世界に負の影響をもたらす現象がフェイクニュースという言葉で一括りにされているとされる。本決議では、根拠に基づかないため、事実に反していることを前提としつつ、それにもかかわらず広く社会に信用され、強い影響を与える情報の発信を意味する用語として使用する。）は、多様な情報に接する機会を失わせるだけでなく、市民に積極的に偽情報に触れさせて誤導するものであるから、市民による的確な判断や意見形成を損なわせるおそれが大きい。ＳＮＳなどのデジタルプラットフォームサービスは、一般の利用者による情報発信や拡散を容易にするものであり、フェイクニュースの拡散に強い影響力を持つ。そのため、ＤＰＦを対象とした何らかのルール作りが必要である。ただし、表現の自由に対する不当な制約につながるおそれがあるため、何がフェイクニュースに当たるかを国家権力が判断する仕組みは妥当ではない。ＥＵでは、ＤＰＦが行動規範を策定することを求めることを通じて、自主的対応を側面から助長する取組が行われている。日本でも、同様の取組として、ＤＰＦが、自主規制ルールを策定し、それを遵守するとともに、その結果を公表することを内容とする法律を制定すべきである。

ＤＰＦは、機械学習を含むＡＩによるアルゴリズムの活用によって情報の流

通をコントロールしている。自律性の確保及び透明性確保の観点から、どのような考え方に基づいて情報の削除や表示順位を定めているのかなどの公表を求める法律を制定して規制するのが妥当である。

また、デジタル機器を通じてしかニュースに接しない市民が相当の割合に及ぶことを考えると、民主主義の過程における多様な情報流通を確保する観点からは、社会で提起される主要な論争点について、類似の見解の閲覧ばかりを勧めるだけでなく、エビデンスレベルを考慮し、異なる見解も勧めるようなアルゴリズムの設定、実践を行うとともに、その結果を公開することが求められる。

第４　デジタル社会におけるプライバシー保護のために必要な法制度

１　個人情報保護法をＧＤＰＲ並みに

個人情報保護法には、自己の個人情報の開示請求権、訂正請求権、利用停止請求権、同意によらない第三者提供の原則禁止、要配慮個人情報取得の本人事前同意などの規定が置かれ、自己情報に対するコントロールの仕組みが設けられている。これらはできる限り個人情報を本人のコントロール下に置こうという自己情報コントロール権（プライバシー権の一種）の考えに沿うものと理解できる。そして、自己情報コントロール権を具体化する個人情報保護法の背後には、個人を人格的自律の存在として尊重する個人の尊重の理念がある。

もっとも、個人情報保護法の目的を定める第１条には「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」と書かれるにとどまり、憲法的価値、すなわち個人の尊重の理念や自己情報コントロール権の保障が明記されていない。しかも２０１５年改正により、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の」という言葉が冒頭に付けられ、もともと低かったプライバシー保護の目的は、利活用の有用性を十分に考慮した後でしか図られないことになった。

これに対して、ＧＤＰＲは、第１条第２項で「本規則は、自然人の基本的権利及び自由、並びに、特に、自然人の個人データの保護の権利を保護する」と憲法的価値を明記し、それを踏まえた各規定を定めて、自己情報コントロール権の保障を強化している。個人の尊重原理の実現を図るならば、日本の個人情報保護法もＧＤＰＲのような権利保障規定を定めるべきである。欧州委員会は、２０１９年１月２３日に、日本について十分なデータ保護の水準を確保しているとしてＧＤＰＲ第４５条に基づく個人データ越境移転に係る十分性認定を行ったが、この十分性認定をより実効的なものにするためにも、個人情報保護

法においてデータ主体の権利保障規定を充実させるべきである。

具体的には、個人情報保護法に以下の権利保障規定を追加すべきである。

(1) 収集の必要性・相当性のない個人情報を処理しないこと

ＧＤＰＲでは、個人データの処理（ＧＤＰＲ第４条第２号では「自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、個人データ若しくは一群の個人データに実施される業務遂行又は一群の業務遂行」と定義されている。）に関して、以下の原則を定めている。

まず、ＧＤＰＲ第５条では、個人データがどの範囲でどのように処理されているのかについての透明性をデータ主体に確保することが必要であること（透明性の原則）、個人データは管理者が特定され、明示された目的かつ正当な目的のためにのみ収集されなければならず、データが収集された場合には当初の目的と両立することができない方法で追加処理をしてはならないこと（目的制限の原則）、個人データは処理される目的との関連において必要な範囲で適切に、関連性を有し、限定されなければならないこと（データ最小限化の原則）、個人データは正確なものでなければならず、かつ必要に応じ最新の状態にしなければならないこと（正確性の原則）、個人データが処理された目的にとってもはや必要以上にデータ主体が識別できないような形態で保存しなければならないこと（保存制限の原則）、個人データの適切な安全性が確保されるような方法で処理されなければならず、また適切な技術的又は組織的措置を用いなければならないこと（完全性・秘密保持の原則）を定めている。

また、個人データの処理をするためには、法的根拠を証明しなければならない（ＧＤＰＲ第６条第１項）。すなわち、ＧＤＰＲでは、①データ主体による同意、②契約の履行にとって必要な場合、③法的義務の遂行にとって必要な場合、④データ主体又は他の自然人の重要な利益を保護するために必要な場合、⑤公共の利益又は公務の行使において実施される人の遂行に必要な場合、⑥管理者又は第三者の正当な利益の目的にとって必要な場合のいずれかに該当する場合に限り、個人データの処理が認められている。

これに対して、日本の個人情報保護法では、利用目的による制限（同法第１８条）、不適正な利用の禁止（同法第１９条）、適正な取得（同法第２０条）、第三者提供の制限（同法第２７条）といった規定は存在するものの、個人情報の収集・利用等についてＧＤＰＲのような具体的な規律はない。そのため、

個人情報が広範に処理されやすく、不必要な個人情報の処理がなされるおそれがある。

したがって、これを防止すべく個人情報保護法においてもＧＤＰＲのような個人の権利保障に関する規律を定めるべきである。

(2) 他の情報と組み合わせれば個人識別が可能となり得るような個人識別可能性のある情報についても、保護の対象とすること

ＧＤＰＲは、識別された又は識別可能な自然人（データ主体）に関する全ての情報を「個人データ」と定義して保護の対象としている（ＧＤＰＲ第４条第１号)。そして、ある者が識別され得るかどうかを決定するには、データ管理者又は当該人物を識別するための他の人によって用いられるあらゆる可能な合理的手段がとられるべきであるとされている（ＧＤＰＲ前文第２６項)。その結果、他の情報と組み合わせれば個人識別が可能となり得る情報も個人データとして保護の対象となる。

これに対して、個人情報保護法は、個人情報の定義における個人識別性を「他の情報と容易に照合することができ」と定めているため（同法第２条第１項第１号)、他の情報と組み合わせれば個人識別が可能であったとしても、それが「容易に」照合できるものでなければ個人情報として保護の対象にならない。

個人に関するあらゆる情報が氾濫しているデジタル社会においては、ＧＤＰＲのように保護の対象を広く定めるべきである。

(3) プロファイリングされない権利、削除権（忘れられる権利)、データポータビリティ権等を保障すること

前述したとおり、ＧＤＰＲに倣って、個人情報保護法を改正して、利用者に対して、プロファイリングされない権利、個人データ削除権（忘れられる権利)、データポータビリティ権等の諸権利を保障する規定を設けるべきである。

(4) 個人情報保護委員会について、プライバシー保護に専念する機関とするよう、その存在目的を設定し直し、調査権限を充実させて、プライバシー保護機能を強化すること

２０２０年の個人情報保護法改正によって、個人情報保護委員会は行政機関に対する監督権限も持つことになった。しかし、その監督権限は、資料の提出及び説明の要求、実地調査、指導及び助言、勧告、勧告に基づいてとった措置についての報告の要求にとどまるものであって（同法第１５３条～第１５７条)、立入権限を含めた調査権限や是正権限及び助言・認可の権限の

付与を定めたＧＤＰＲと比べて見劣りし、特に行政機関による濫用をチェックするためのものとしては実効的とは言えない。

そもそも、個人情報保護委員会は、「個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報の適正な取扱いの確保を図ること」を任務としており（同法第１２８条）、プライバシー保護に専念する監督機関にはなっていない。しかも、個人番号法第１９条第１７号により、個人情報保護委員会は、規則を制定して特定個人番号の提供先を拡大する権限さえ付与されていることからも明らかなように、個人情報の保護だけではなく、個人情報の利活用を図ることさえもその権限とされている。この点は、「取扱いと関連する自然人の基本的な権利及び自由を保障し」（ＧＤＰＲ第５１条第１項）と、明確にプライバシー保護のための第三者機関として機能が純化されているＧＤＰＲにおける監督機関と異なる。

したがって、個人情報保護委員会は、ＧＤＰＲにおける監督機関のように、プライバシー保護に専念する機関となるようその存在目的を設定し直した上で、調査権限を充実させて、プライバシー保護機能を強化すべきである。

２　公権力による監視の禁止

第２で述べたように、デジタル社会の進展と情報処理技術の進展があいまって、ＤＰＦは、自社が扱う個人データから、利用者の包括的な人物像の把握（プロファイリング）を行うことができるようになっているし、その情報を利用して利用者の消費行動や投票行動まで誘導し得るようになっている。

このような社会において、公権力は、市民に関する膨大で機微な個人データを自ら保有しているところ、公権力がその保有する個人データを利用してプロファイリングを行ったり、又はＤＰＦが収集した個人データを入手してプロファイリングを行ったりすることも可能な状況となっている。

例えば、①公権力は、下記３において述べるように、漏れなく重複しない個人識別番号である個人番号（マイナンバー）に加えて、確実な本人確認情報（氏名、住所等）を保有している上に、それにひも付いた税・社会保障関係の個人データや、レセプト等の医療関係情報なども保有しているから、それらの情報をマッチングしてプロファイリングすることができる。また、②アメリカ合衆国においては、警察がグーグル等に対して、その保有する位置情報を利用して、犯罪現場付近にいた利用者全員の個人情報を「地引網」的に一括請求する捜査手法（ジオフェンス令状）が多用されるようになっている。日本においても、このようなプロファイリングや捜査がなされるならば、市民のプライバシーや移動の自由等は侵害され、萎縮効果により、自由かつ自律的な人格の形成が阻

害され、ひいては自由で自律できる個人を前提とする民主主義の基盤も掘り崩されることとなってしまう。

よって、このような市民監視的な個人データの収集・利用は禁止されなければならない。

3　個人番号、個人番号カードに対する制限

日本に住民登録を有する全国民及び外国人住民には、その個人を一意に識別する個人番号（マイナンバー）が付されており、現在、税・社会保障・防災関係の多くの個人情報が個人番号にひも付けられている。分野を超えた個人識別番号である個人番号（その「前身」である２００２年の「住民票コード」）が付番されるまでは、氏名・住所・生年月日・性別の４情報で、分野別の個人情報を名寄せするしかなかったため、同姓同名・同一生年月日の人物の存在や氏名・住所の変更等により、確実な名寄せができなかったが、現在は個人番号をキーとして名寄せすれば、多くの分野の、生涯を通じた重要な個人情報が漏れなく、かつ他人の情報と間違うことなく収集できることになった。これは、情報の連携や利活用という面では非常に便利であるが、逆にそれらの情報を連携して利用することができる民間事業者や行政機関がその機能を悪用するならば、容易にプロファイリングを行うことができ、個人のプライバシーは丸裸にされ「データ監視社会」を招来することになってしまう。

また、政府は２０２２年度末にはほとんどの国民、外国人住民が個人番号カードを保有する社会の実現を目指して、高額ポイントの付与を含む強力なキャンペーンを行っている。

この個人番号カードは、公的個人認証機能を持っており、同機能を活用して利便性の高いデジタル社会を実現することがうたわれている。しかし、同機能に用いられる発行番号やマイキーＩＤは、個人番号と同じく特定の個人と結び付けられた重複しない個人識別符号であるので、その機能が悪用・濫用されたならば、個人番号の場合と同じく「データ監視社会」を招来することとなる。マイキーＩＤ等にひも付けられる個人情報に制限はなく、マイキーＩＤと連携可能な情報は、質・量ともに、個別分野の個人識別符号とは比較にならないからである。

よって、プライバシー保障の観点から、個人番号制度は抜本的な見直しを行うか、個人番号及びマイキーＩＤ等の個人識別符号の利用範囲の大幅な限定等を行うことが必要である。

4　情報機関に対する法規制

近年、２０１４年１２月１０日から施行されている秘密保護法（特定秘密の

保護に関する法律）や、２０２１年6月１６日に成立した重要施設周辺及び国境離島等における土地等の利用状況の調査及び利用の規制等に関する法律（以下「重要土地等調査規制法」という。）など、国（行政）が個人情報を幅広く収集する権限を認める法律が次々と成立している。しかし、その情報収集の対象や条件は曖昧であり、かつ収集後の情報の保管・利用等の状況はほとんど明らかにされていない。

これらの個人情報を利用しているであろう内閣情報調査室、公安調査庁や警察庁警備局を中核とする公安警察、自衛隊情報保全隊等の活動についての監視システムは存在しない。そのような中、デジタル庁の発足に当たり、デジタル庁本体が内閣に属する機関となり、その長は内閣総理大臣とされたことから、全ての個人情報が内閣総理大臣の下に集中されるおそれがある。これらの情報機関の活動については、その権限に対して法律により限定を行った上で、個人情報保護委員会又はこれとは別個に独立した専門の第三者機関が、職権で、特定秘密や情報機関が集めた情報、デジタル庁が共通仕様化した情報等の中身までをもチェックし、これに対して是正の勧告・命令ができる制度が必要である（当連合会「デジタル改革関連６法についてプライバシー・個人情報保護の観点から、必要な法改正と法の適正な運用を求める意見書」（２０２１年１２月１７日）参照)。

なお、デジタル庁発足後も、政府においては、重要土地等調査規制法に基づく調査情報等が事務局を通じて内閣総理大臣に集中されることとなった。また、２０２２年４月１日施行の改正警察法により、サイバー犯罪に関わる情報収集等のために、警察庁にサイバー局が設置され、関東管区警察局にサイバー特別捜査隊が設けられた。これにより、サイバー犯罪対策の強化を目的としてデジタル化された個人情報が警察庁に集中されることとなる。さらに、経済安全保障推進法（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律）の制定に伴い、官民パートナーシップと称する「協議会」によって、軍事技術につながる特定重要技術の研究開発を政府が一元的に管理・統制するシステム等となるおそれがある。

このように、情報機関の監視権限とその行使について、厳格な制限を定め、独立した第三者機関による監督を制度化することの必要性は一層高まっている。

5　顔認証システム規制

顔は、基本的に隠すことも変更することもできない生体認証の一つとして、指紋やＤＮＡ型情報と共通する性質を持つ。加えて、指紋やＤＮＡ型情報など

とは異なり、監視カメラの前を通るだけで本人が知らないうちに顔認証データを生成することが可能である。他方で、運転免許証に代表されるように、非常に多くの人々をカバーする本人識別のための顔画像データベースが既に存在している。それゆえ、随所に存在する監視カメラ映像と顔認証データを検索・照合することによって個人の移動履歴を把握し、あるいはある人がいつ誰と会っていたのかなどを把握することが可能となる。さらに、他の生体認証とは異なり、顔には表情があるため、その人の感情をＡＩ技術によって読み取り分析することも可能である。こういった技術が進展すれば、人の内心の自由にまで踏み込んだビジネスや捜査手法が今後出てくるおそれがある。そういった手法は、差別を生むおそれがあるだけでなく、誤謬を含む可能性もあり、その場合の弊害が重大であろうことは想像に難くない。

顔認証にはこういった特性があることから、ＧＤＰＲ第９条は、顔認証データを含む生体情報を原則収集禁止としており、欧州評議会も、公共空間における顔認証システムの利用について、警察などの公権力のみならず民間部門も含めて原則禁止している。アメリカ合衆国の複数の州や市などでは、警察による顔認証技術の利用を禁止している。当連合会が２０１２年、２０１６年、２０２１年と繰り返し提言してきたとおり、日本でも重大なプライバシー侵害、あるいは集会結社の自由などの制約にもつながり得る顔認証の利用について、法律により、官民を問わずその利用を原則として禁止した上で、収集、利用及び保存について、利用場面に応じた設置・運用条件（不特定多数者に対する顔認証システムの利用については、特定人に対する顔認証システムと比較して、厳格な設置・運用条件が必須となる）を設定すべきである。加えて、照合・特定用の基礎データの供給源になる監視カメラについても、法律で厳格な設置・運用条件等に関する要件を定めることが求められる。そういった要件の遵守状況を調査し、また必要な是正措置をとるために、官民による顔認証技術及び監視カメラの利用について、個人情報保護委員会に管理監督権限を付与するのが妥当である。

第５　デジタル社会の設計における原則と市民参加

１　同意原則の徹底

政府は、流通するデータの多様化・大容量化が進展し、データの活用が不可欠であることなどを理由として、デジタル改革関連６法案（デジタル社会形成基本法、デジタル庁設置法、デジタル社会の形成を図るための関係法律の整備に関する法律など）を国会に提出し、この法案は２０２１年５月１２日に可決・

成立した。内閣総理大臣をトップとする異例の体制で、強力な権限を有するデジタル庁が司令塔となって、データの利活用推進等を強力に進めていくこととしている。

デジタル・ガバメント実行計画（２０２０年１２月２５日閣議決定）においては、「特にデジタル社会においては行政機関が最大のデータ保有者であり行政自身が国全体の最大のプラットフォーム（Platform of Platforms／System of Systems）となることが産業競争力や社会全体の生産性向上に直結する。このため、国全体の最大のプラットフォームたる行政機関が、そのアーキテクチャを策定し、マイナンバー制度とリンクしたＩＤ体系の整備、ベース・レジストリをはじめとした基盤データの整備、カタログの整備等を行い、民間に対してもオープン化・標準化されたＡＰＩで連動できるオープンなシステムを構築する」とされている。

しかし、デジタル社会の形成の基本的枠組みを明らかにしている「デジタル社会形成基本法」では、個人のプライバシー・個人情報保護を同法の目的に挙げていないなど、データ利活用の推進より上位に置かれるべき価値であるプライバシーの保障がおろそかとなっている。ＥＵのＧＤＰＲのように、まずは市民のデータ保護（プライバシー保護）の権利を保障し、最大限尊重することを大前提とすることが重要である。プライバシーを保障するためには、自己情報コントロール権を保障して、データ主体である本人が、自己の情報がどのような目的に利用等され、それによるリスクはどのようなものであるのかを理解した上で、同意による利用許可を行うという原則を保障することが必要である。

また、同意をしない場合は著しく利便性を損ねるなどの対応を許すならば、事実上同意が強制されることから、そのような対応を許さない規制が必要である。

２　プライバシー影響評価に基づくプライバシー・バイ・デザイン

日本におけるデジタル社会の推進に当たっては、上述のように市民のプライバシーを最大限保障することが大前提とならなければならない。しかし、その実現方法が「同意のみの徹底」となると、形式的に「同意」の過程が増えるのみで、非能率かつプライバシーの保障強化につながらない。プライバシー保障強化の実現のためには、デジタル社会実現のための制度やシステムを構築するに先立ち、同制度・システムによるプライバシーへの影響評価（環境影響評価のプライバシー版）を行うこと、その影響評価に基づき制度・システムの設計段階からプライバシー保障を組み込むこと（プライバシー・バイ・デザイン）、これによりデフォルト（初期設定）の状態でプライバシーが保護されるように

すること（プライバシー・バイ・デフォルト、ＧＤＰＲ第２５条参照）の制度化が必要である。

３　地方自治の尊重

デジタル改革関連６法の中で、個人情報保護法も大幅に改正された。国の行政機関に関する規定を原則としてそのまま地方自治体に適用することとなり、その部分は２０２３年４月から施行されようとしている。

日本では、国に先駆けて地方自治体が個人情報保護制度の整備を進めてきた。上記改正法においても、地方自治体は、区域の特性に応じて、個人情報の適切な取扱いを確保するために必要な施策を策定し、及びこれを実施する責務を有するとされており（同法第５条）、成立時の国会の附帯決議でも、個人情報の適正な取扱いに関して条例を制定する場合には、地方自治の本旨に基づき、最大限尊重すべきことが指摘されている。しかし、実際にはデジタル社会推進による利便性や行政の効率化が強調され、国主導の制度の一元化が進められようとしており、地方自治体における個人情報保護の低下が憂慮されている。

また、デジタル改革関連６法の中で、地方公共団体情報システムの標準化に関する法律が制定され、国主導による行政運営の効率化が推進されようとしている。さらに、スーパーシティ構想と称して、デジタル化推進のために実験的に保護施策を緩和する国家戦略特区の導入が始まろうとしている。

これらの動きは、地方自治体による個人情報保護政策の後退を招くものであり、ひいては憲法の定める地方自治、条例制定権の形骸化につながる。地域の個人情報保護に関わる施策について、地方自治体の方針を尊重するとともに、国の政策決定においても地方自治体の意見を十分に聴取し、決定過程に反映させることが必要である。

４　市民提案、市民参加によるデジタル社会の設計を

個人情報の利活用を図り、利便性や行政の効率化を優先するデジタル社会においては、情報主体である私たち主権者が、行政機関や民間事業者からデータを収集・分析・利活用される客体になってしまい、一人一人の市民の自己決定や自己実現が妨げられ、市民社会全体が委縮するおそれがある。そして、利便性や行政の効率化ばかり優先されることにより、主権者のプライバシー保護は絶えず後方に退く危険もある。そこで、利便性や行政の効率化ばかりが優先され、主権者のプライバシー保護が弱い社会とならないためにも、まず市民が設計に積極的に参加し、その意見が交通や行政・防災・エネルギーなどの都市基盤や市民の暮らしに反映され、改善される仕組みの検討・導入が必要である。

その一つの例として、スペイン・バルセロナ市におけるバルセロナ・コモン

ズによる市政の誕生、そして市民が市政に参加するためのプラットフォーム「Decidim」（カタルーニャ語で「私たちが決める」の意味）が挙げられる。そのプラットフォームでは、オンラインで多様な市民の意見を集め、議論を終結し、政策に結び付けられ、市議会での議論もそのプラットフォーム上でチェックでき、全てのプロセスが可視化されている。Decidimは、バルセロナのほかにも世界中の３０を超える自治体で利用されており、日本では兵庫県加古川市などで導入されている。

また、台湾では、誰もが政治的な提案をインターネットで請願できる「Join」というプラットフォームを導入し、５０００人以上の賛同があれば行政側が取り上げ、検討しなければならない仕組みとなっているなど、画期的な取組が実践されている。

こうした世界各地での取組を参考に、デジタル社会における市民参加型の民主主義の実現に向けた取組を検討し、導入していく必要がある。具体的には、デジタル社会の設計段階においても、市民提案型の制度、つまり市民がプランを描いた上で議会が検討し、採用することのできる仕組みを構築する必要がある。また、そのような制度が実現されるまでの間は、制度設計に際し、行政機関、業界側だけでなく、消費者側、市民側の代表者を少なくとも半数程度は参加させ、その意見を反映させるべきである。

５　データ主権を個人に取り戻す仕組み

もっとも、デジタル技術を活かした市民参加型の仕組みが採用されるだけでは、行政に寄せられた個人情報が集中し、その利便性等からプライバシー保護が後方に退く危険を避ける解決策とはならない。そのため、それと並行して重要になるのがデータ主権を個人に取り戻す仕組みである。

ＥＵでは、ＧＡＦＡ（グーグル、アマゾン、フェイスブック、アップルの総称）の台頭への対抗戦略として、またデジタル社会で個人のプライバシーを保護するための政策として、ＧＤＰＲなどによる規制強化を行い、その延長線上の取組として２０１７年に欧州委員会がＤＥＣＯＤＥ（脱中央集権・市民所有型データエコシステム）プロジェクトを始めた。これは、オンライン上で生成される個人情報の蓄積・管理、運用に関して、市民自らが個人データの秘匿や共有をコントロールできるようにする仕組みである。バルセロナ市も、アムステルダム市と共に実施実験都市として参加しており、近時その報告書が提出された。

さらに、欧州委員会は２０２０年１２月１５日、ＳＮＳ、オンラインマーケットプレイス及びデジタルサービスを対象とした新たな包括的ルールとして、

デジタルサービス法案（ＤＳＡ）及びデジタル市場法案（ＤＭＡ）を公表し、２０２２年７月５日、欧州議会は両法案を承認した。オンライン上での消費者保護、プラットフォームビジネスにおける透明性の確保、プラットフォーム事業者の説明責任の確立等を通じて、公正かつ開かれたデジタル市場を目指すものとされる。

私たちは、これらの新たな試みも参考にして、オンライン上で生成される個人情報の蓄積・管理、運用に関して、市民自らが個人データの秘匿や共有をコントロールできる仕組みを確立することにより、主権者による情報主権が全うされた自律的なデジタル社会の実現を目指すべきである。

第６　結語

当連合会は、２０１０年の第５３回人権擁護大会で「『高度情報通信ネットワーク社会』におけるプライバシー権保障システムの実現を求める決議」を行い、デジタル社会における自己情報コントロール権の実効的な保障を提言し、以降はこの提言に従って活動を続けてきた。

しかし、デジタル社会の進展はその後もいよいよ著しくなっているにもかかわらず、プライバシー保護のための法制度の整備は遅れている。他方で、当連合会が問題点を指摘してきた個人番号制度はますます拡大され、将来のデジタル社会の基盤として今後更に活用されようとしている。

当連合会は、改めて、個人が尊重される民主主義社会の実現のために、プライバシー権・自己情報コントロール権の保障の重要性と、来るべきデジタル社会において市民のための制度設計がなされることが重要であることを確認するとともに、これらの実現を目指し、今後も全力を尽くしていく決意を表明し、上記のとおり決議するものである。