

デジタル政策アジェンダ

デジタル政策フォーラム

本文書は、デジタル政策フォーラム（DPFJ）におけるデジタル政策を巡る議論に関する問題意識を整理したものである。

膨大なデータという無形資産が旧来の業態や事業領域の枠を越えて自由に流通・連携することにより、社会経済システムを把握するための“画素数”が向上し、より明確な実像を捉えることを可能とするデータ駆動社会が到来し、その流れは今後さらに本格化するものと見込まれる。

そこで、データ駆動社会の特性を改めて整理した上で、データ駆動社会がもたらす社会経済構造の変化に対応するために必要な「デジタルガバナンス」、すなわちデジタル技術を制御するためのルールのあり方に関する論点を提示する。そして、デジタルガバナンスの実効性を確保することで実現する「デジタル主権」の重要性とこれに関連する論点について整理する。

1. データ駆動社会の特性

データ駆動社会を実現していく上で最も重要なのは、データという無形資産が従来の財やサービスと大きく異なる特性を有していることにある。

具体的には、投入物としてのデータは目減りしない非競合性という特徴を持つ。しかもデータが集積することでデータそのものの価値が幾何級数的に増加する規模の経済性（ネットワーク効果）が働く。このため、データ集積の限界費用は限りなくゼロに近づく。こうした特性を有する事業は市場の失敗を招き、寡占状態を生み出す。市場メカニズムが有効に機能することを前提とする競争政策は、市場メカニズムとは相容れないデータという新しい無形資産の特性を反映する試みの途上にある。

市場メカニズムが機能しない状況下において、限られた主体によるデータ集積の様態は大きく2つに分けられる。すなわち、政府統制の強い社会主義国においてデータ集積の主体は国（政府）であり、市場メカニズムを尊重する自由主義国家において

は民間プラットフォーマーである。

(1) 国家がデータ集積の主体である場合

国家がデータ集積の主体になるということは、サイバー空間に国家がどこまで介入することが許容されるのかという議論と密接に関連する。また、デジタル技術そのものが民間利用と軍事利用のデュアルユースの特性を持つため、デジタル技術の軍事利用のあり方が問題になる。

平時から非常時(戦闘行為が行われる状況)に至るまでの変化がシームレスに進むグレーゾーン事態が長く続く状況において、平時のデジタル技術の利用のあり方と非常時のデジタル技術の利用のあり方を明確に区別することが難しく、この状況がデジタル技術を巡るルール策定を困難なものとしている。

例えば、平時においても SNS 等を駆使して偽・誤情報を流布する認知戦によって国内政治体制を不安定化させたり、武力攻撃の前哨戦として重要インフラに対するサイバー攻撃を行うような事案は既に世界各地で散見されている。また、AI 等のデジタル技術が平時のみならず戦時において戦闘行為等に使われるハイブリッド戦争が日常化し、平時と非常時を区分したデジタル技術のガバナンスのあり方が改めて問われている。

こうした中、デジタル技術をどう制御するかという議論は民間の領域にとどまらず、国家が強く関与する安全保障に関連する議論と一体化している。そして、デジタルガバナンスの議論は国連を中心とする国際ルール(法の支配)のあり方と密接に関連している。しかしながら、近年は覇権主義国家が顕著に増加し、自国利益の最大化を第一義とするこれらの国々は国際的なコンセンサスの醸成や一定の許容度をもつ柔軟な合意形成に消極的となってきた。

その結果、サイバー空間における国家の自衛権行使に関する国連専門家会合の議論は 10 年以上かけても合意できていない。また、WTO においてはモノやサービスの越境取引ルールが存在するが、当該ルールの安全保障条項(例えば GATT 第 21 条)を用いて、明確な根拠を示すことなく安全保障を盾に自由貿易を阻害する傾向が強まることも懸念される。

(2) プラットフォーマーがデータ集積の主体である場合

次に、データ集積の主体が民間プラットフォーマーである多くの国においては既に競争政策の見直し議論が進み、プラットフォーマーに対する規制を強化する試みが行われている。例えば、欧州では DSA(デジタルサービス法)や DMA(デジタル市場法)といった法規制によりデジタル関連市場における利用者保護やプラットフォーマーによる市場支配力の濫用を防ぐことが試みられている。

しかし、高水準の法規制が欧州域内のデジタル市場におけるスタートアップ育成の芽を摘む一方、法規制が対象とする米国プラットフォーマーの市場支配力の抑制が実効的な効果を挙げていないことから、規制緩和や産業政策への力点のシフトが模索されるなど、議論の振れ幅は依然として大きい。

(3) データ駆動社会の健全性の確保

言うまでもなく、データが少数のプレーヤーに握られることによりデータ駆動社会の健全性は損なわれる。これは、少数のプレーヤーが独占(寡占)利潤を獲得することで所得の最適配分が失われて富が偏在し、市場競争の欠如から新たな技術やサービスを生み出す活力が損なわれるからである。このため、データ駆動社会の健全性を確保するためには、データの量の増加、質の向上、流通速度の向上の 3 つを実現することが求められる。

この点は AI ガバナンスの問題と密接に関連している。AI は膨大な学習データを言語モデルとして取り込み、当該モデルを使って大量の生成物を生み出す「データ流通の加速化装置」である。この加速化装置が有効に機能することでデータ量が増加するが、ハルシネーションによる偽情報や意図的な誤情報の生成、国家による偽情報の流布を通じた認知戦等、データの質を損なわせる可能性も高まる。また、AI へのアクセスの公平性が確保されないことによりデータ生成の偏在性(少数の者による支配)が生まれ、結果としてデータの流通速度が低下する。

このように、健全なデータ駆動社会を実現するための課題は多い。データ流通を促進するための方策は安全保障政策から競争政策、産業政策、外交政策、消費者政策に至るまで多岐にわたる。デジタル政策の議論は多数の政策領域にまたがる特徴を持つものであり、国や地方自治体だけでなく、技術集団(テックコミュニティ)、大学等研究機関(アカデミア)、市民社会等、幅広いマルチステークホルダー環境を前提とする議論であることが求められる。このため、国際的なデジタルガバナンスの議論の場をどのように設計・運用するかという点についても議論が求められる。

2. デジタルガバナンスの強化

DPFJ では、デジタルガバナンスを 3 つの主要な構成要素、すなわち、データガバナンス、AI ガバナンス、セキュリティガバナンスに分けて議論を深めてきた。そして、この 3 つの要素はますます一体化の様相を見せている。

既に述べたように AI はデータ流通の加速化装置であり、AI 学習用の良質なデータは AI の言語モデルを強化し、優れた AI はデータ駆動社会のエンジンとして機能する。また、AI の重要性が増す中、データのセキュリティ(機密性・完全性・可用性)をどう確保するか、またセキュリティ対策に AI をどのように組み込んで防御の深層化や自動化を実現するかという点が重要な検討課題となる。

デジタルガバナンスを考える上で重要なのは、実現する社会機能を明確にすることにある。特にデータ駆動型社会の到来によって、一人ひとりのニーズに適合したサービス等が提供される「個別化」、AI などにより人手を要しない業務処理を可能とする「自動化」、そして社会全体の解像度があがることによる「最適化」という 3 つの要素を実現する社会機能であると想定する。同時に、AI による無機能的な差別が生じないよう「社会的包摂」の機能も強化する必要がある。

上記の検討に際しては、常に集中と分散のバランスを念頭に置く必要がある。デジタル技術の世界ではインテリジェンスの所在が効率を目指す集中型と自律性を重視する分散型の間を揺れ動いてきた。この集中と分散は二項対立ではなく、適正かつ動的な均衡点が存在する。デジタル技術が進展する中での社会は、常に集中と分散のベストミックスを模索する試行過程であることも重要な留意点である。

(1) データガバナンス

データ駆動社会を実現して「データ力」を発揮させるためには、データの生成・加工・連携・流通等のデータ連携プロセスを共通化する必要がある。その際、AI 駆動型のデータスペースを目指す必要がある。もともとデータスペースはデータ保有者からデータを集める集中型ではなく、データを必要なときだけ連携させる分散型システムであり、ここに AI を実装することで連携力を強化する。

データスペースは、上から下に向かって、アプリサービス層(データ連携のためのコミュニティ)、データ連携層、トラストサービス層の三層構造で捉えられる。この三層構

造の中で、データ連携層は異なる組織・領域間でデータを連携させるためのコネクタを標準化する必要がある。AI を前提としてデータの意味や文脈を理解するデータ連携を目指す場合、当該コネクタについては MCP (Model Context Protocol) 等が共通のインタフェースとなり、AI エージェントを介してデータ連携を実現することが考えられる。

また、データの文脈等を理解する上では推論 AI や無数の RAG を連携させることで精度を高めることが可能になる。特に個人情報等については国産のソブリン AI で取り扱うなど複数の AI をハイブリッド型で組み合わせて利用する AI 活用が必要であり、こうした考え方は、後述するワット・ビット連携等の考え方とも合致する。

さらに、AI 駆動データスペースを実現するには、データ提供者や利用者、AI エージェントに加え、データそのものの真正性を確保するための仕組みが求められる。これがデータスペースの三層構造の基礎部分に位置するトラストサービス層である。このトラストサービス層は AI 駆動型のデータスペースの信頼性の核となるものであり、実装すべき機能等について検討が求められる。

加えて、データ流通の仲介組織、データ流通とデジタル通貨との連携など、データ連携を核とする関連市場拡大に向けての検討まで視野を広げていく必要がある。広範囲に及ぶ AI 駆動型のデータスペースの検討に際しては、DSA (一般社団法人データ社会推進協議会)、JDTF (一般社団法人デジタルトラスト協議会)、RRI (ロボット革命・産業 IoT イニシアティブ協議会) との協業を図る JDSA (Japan Data Space Alliance) として各組織が連携しながら進めていくことが望ましい。

(2) AI ガバナンス

AI ガバナンスを巡る議論は、AI に規制を導入することの是非から始まった。この点、DPFJ は急速な技術革新を阻害しないようソフトローを基本とすることが望ましいと一貫して考えてきた。この考え方を起点に、むしろ社会経済活動において AI の利活用を阻害する規制の見直し、AI 利用のガードレールとして機能させるべき事項(ネガティブリスト)の明確化、AI リテラシー向上のための取り組みなどを強化していく必要がある。同時に、人手不足、孤立、行政サービスの限界が深刻化する中、AI を利用しないことによるリスクの評価も求められる。

また、LLM (大規模言語モデル) の領域において日本の文化や思想、歴史などを踏まえ日本固有の価値観を反映したソブリン AI の構築が重要である。ただし、先行事

例と同様のアプローチによる開発だけでは先行する LLM に肩を並べるのは困難な面もある。このため、AI の多様性を確保する観点から、バーティカル AI など相対的に規模が小さい領域特化型 AI の開発にも力を入れるべきである。また、特定の AI に依存することなく複数(または多数)の AI をハイブリッドで活用できる分散型 AI の仕組みは AI 基盤に関する冗長性の確保等の観点から必要である。同時に、こうした AI の自由な組み合わせを保証するオープンな AI 環境の整備(例えばオープンウェイトの AI の開発・普及)が重要である。

併せて、ソブリン AI のガバナンスとして、自立的に判断し実行する AI エージェントに対する意思反映や契約締結に対する「代理権」などを踏まえた法的権限の整理が必要である。同時に AI エージェントによって発生したトラブルへの個人・法人に対する責任の所在や法的責任の整理なども、現行法を踏まえた整理が必要である。AI エージェントに対して法的権限について整理された場合、AI エージェントそのものがサイバー攻撃の新たなターゲットになることも懸念される。

また、地方分散型のデータセンター(DC)と電源を組み合わせる仕組みを作り、多数の小規模 DC をネットワーク化し、仮想的に大規模 DC として運用したり、大都市部周辺の大規模 DC(学習)と地方分散型の DC(類推)を組み合わせることでデータ伝送の遅延を最小化したり、地方 DC の AI を活用した電力網の更なるスマート化などを一体的に進めるワット・ビット連携を強力に推進すべきである。

さらに、AI の進化により研究開発の進め方も大きく変化しつつあることを踏まえ、国としての研究開発基盤となる AI の開発や共同利用、これを支えるネットワーク基盤の整備、同志国との連携強化なども進める必要がある。

このほか、国における AI を活用した戦闘行為について国際的な議論を進める機運を醸成し、AI 条約(仮称)において非人道的な AI 活用を禁止する方向で考えることも必要である。また、AI が自己修復能力を持つに至った時点でのガードレールのあり方、すなわち AI が超えてはならないレッドラインについて検討する必要がある。これは AI に特に深い関わりを既にもっている若年層の AI リテラシーの議論とも密接に関連する。

特に近年 AI の開発が加速化する中、AI 開発のスピードを緩めるべきという指摘が各方面(特に研究の現場)から出てきている。AI 開発速度のあり方や AI 開発における予見可能性といった問題は AI ガバナンスの最重要課題の一つであり、必要に応じて法規制のあり方について定期的にレビューを行う他、国際的な場における議論を

促す努力も求められる。

(3) セキュリティガバナンス

セキュリティガバナンスについてはAIの進化が大きく影響している。Anthropic社のClaude Mythosの登場以降、AIによって企業システムの脆弱性が多数発見され、セキュリティ対策の量(頻度)の増加と対策の深化が求められるようになっている。特に今後AIエージェントが普及する中、AIエージェントの信頼性や正常稼働の保証など検討すべきリスクが広がり、複数のAIエージェントを介したリスクの拡散(システムリスクの深刻化)も懸念される。このため、官民連携によるAIセキュリティの確保のための枠組みの確立、AI活用による防御対策の自動化に向けた検討、脅威情報の解析を行うスレッドインテリジェンスにおけるAI活用などを進める必要がある。

また、AIが一国の安全保障に密接に関連するようになると、サイバー空間における各国間の攻撃抑止力のバランスが崩れ、AIの優劣が安全保障水準を左右するような事態が生じることも想定される。このため、AIを防衛システムに実装するとしても人間が関与する部分(Man in the loop)をどこまで確保しておけばよいのか、自国の防衛システムにおけるAI能力の情報開示のあり方の検討、AIを前提とした抑止戦略の実効性確保のための国際ルールの検討などを国際的に進めていく必要がある。

さらに、AIの学習データの質の確保、AIを悪用した偽・誤情報の流通による認知戦への対処など、データの真正性を確保するための方策について、表現の自由や報道の自由などの観点から国の関与のあり方も視野に入れつつ、引き続き議論を進める必要がある。

3. デジタル主権の確立に向けて

デジタル主権とは、自国のデジタル資産を主体的に管理するための仕組みであり、「開放性や相互接続性を維持しながら、デジタル分野における重要な選択を自ら行い、自国の法、価値、利益に沿って技術、データ、インフラを統治・利用できる能力」と便宜的に定義される。なお、ここでは国家主権としてのデジタル主権に力点を置いているが、AIの進化に併せて個人の自己主権や地域主権にどのような影響を与えるかについても検討が必要である。

上記のデジタル主権について、より具体的には、自国のデジタル技術を主体的に開発・利用できる「技術主権」、自国のデータに対する管理権を確保する「データ主

権」、自国のデジタルインフラの独立性を確保する「インフラ主権」の 3 つの要素に整理できる。特に、インフラについてはこれまで国土と一体的に整備運用されるものであり、遠隔からインフラにアクセスするという発想はなかった。しかし、第三国による LLM を構成する GPU 基盤へのアクセスをどこまで許容するか等、ネットワーク経由で国家の重要インフラにアクセスするような事態が起きる中、インフラの概念を拡張し、その主権確保について検討することも重要になってきている。

デジタル主権として確保すべき内容は国として守るべき価値として共有される国家理念や文化的背景に依存するものであり、デジタル主権を確保するための OS 部分（基本ルール）に該当するのがデジタルガバナンスである。日本においてはデジタル主権の確立という観点からの議論が欧州と比べて立ち遅れている。デジタル主権を確立するための国家戦略は、産業政策、科学技術政策、競争政策、外交政策、防衛政策等を網羅する相互連関性を持った俯瞰的なものである必要があり、デジタル主権を巡る議論を急ぐ必要がある。

その際、デジタル市場における規制の強度とサイバー空間における国家関与の強度をどう組み合わせるのかという基本方針を明確化することが求められる。日本としては、サイバー空間における国家関与を最小化しつつ、デジタル基盤はデジタル公共財として国の支援の下に官民協同で整備し、当該基盤の API を開放して民間の利用モデルがその上で自由に展開される「官民共創モデル」を一つの叩き台として議論を進める必要がある。その場合、デジタル公共財として国は何を整備支援すべきなのか、どのような支援策（財政支援や標準化など）が求められるかを含め、官民連携による戦略的なアプローチが必要である。

また、デジタル主権を確立するためには、あらためてデジタル社会における国際ルールについて幅広い観点から議論を継続する必要がある。各国の内部において先鋭化する対立の構図を抱えつつ多国間のコンセンサスの醸成に関心を寄せない覇権主義国家が多い「多国間主義なき多極化（multipolarity without multilateralism）」を変革するための努力を続けなければならない。

その際、AI などのデジタル技術が民主主義という普遍的な価値にどのような影響を与えるか検証を継続する必要がある。例えば AI の普及により多様性のある民主的なプロセスによるコンセンサスの形成が困難になる可能性がある一方、デジタル技術を積極的に活用することで全員参加型のデジタル民主主義が実現する可能性も存在する。また、人々の精神世界の柱となっている宗教と AI の関係についても慎重に検証を続ける必要がある。AI はどこまで許容されるのかという検討課題は、宗教あるい

は宗教的倫理が人々に何を与えているのかという根源的な問いかけを照射している。

デジタル政策フォーラムは、デジタル技術を軸とする政策議論の場であるが、こうした議論を他領域にまで拡張し、他の様々な団体・組織と連携しながらデジタル主権を巡る議論をさらに深めていきたい。

なお、本政策アジェンダは今後とも必要に応じて適宜見直していくこととする。なお、本政策アジェンダに係る個別論点(7項目)は以下のとおりである。

(個別論点)

(1) AI 時代のデータ駆動社会の具体像

(主査： 庄司昌彦 武蔵大学社会学部メディア社会学科教授)

「監視資本主義」モデルや「権威国家主義」モデルとは異なる欧州のアプローチに単に準拠せず、国や文化圏、地域社会の多様性を重視して、日本が目指す AI・データ駆動社会の具体像を議論する。問うべきは、抽象的な理念や技術的優位性ではなく、誰の課題を何のために解決し、どのような成果をもたらすかである。国家、市場、地域社会、個人の役割や集中と分散のあり方も、目的、費用、実現可能性に即して考える。

AI の発展により、計算資源、基盤モデル、データ、クラウドの一部の国家や巨大プラットフォーム事業者への集中が進んでいる。すべてを独自に開発・保有するのではなく、国内外の優れた技術を賢く活用しつつ、相互運用性、透明性、選択可能性を確保し、過度な依存を避ける方策を検討する。

また、AI を利用できるかという「アクセスの格差」だけでなく、何を解決すべきかを誰が提起できるのかという「問い立ての格差」にも目を向ける。産業競争力や安全保障に加え、子育て・介護、高齢者や障害のある人、地方などの生活・地域課題、とりわけ「支える人を支える」ための AI について議論する。

あらゆる課題を AI やデジタル技術で解決することは、必要となる時間、費用、制度、運用体制、行動変容、リスク等を考えれば必ずしも現実的ではない。人や制度、アナログな手段と適切に組み合わせ、現場で着実に DX の成果を生み出

すことを重視する。その際、AI を利用するリスクだけでなく、利用しないことで生じるリスクも検討する。また、生成 AI 時代における文化の多様性と制作者・利用者の貢献を尊重し、生活や支援の現場に関わる人々が AI の用途やルール形成に参加できる社会を目指す。

(2) データ駆動社会の基本規律

(主査： 宋戸常寿 東京大学大学院法学政治学研究科教授)

デジタル技術が基盤となる社会における国家と市民社会との関係について検討する。例えば、拡大しているデータ駆動社会のエコシステムと(日本では十分根付いているとはいえない)市民社会のガバナンスをどのように結びつけるかは、今後のデジタル社会を構築していく上での重要な検討課題となる。小さな政府に基づく「アメリカ型」デジタル社会、歴史に根ざした市民社会に基づく「EU 型」デジタル社会、そして権威国家主義による「中露型」デジタル社会との対比を通じて、「日本型」デジタル社会の基本規律の方向性について検討する。

また、ロシアによるウクライナ侵攻以降、グレーゾーン事態(武力行使が行われる前の段階で、自国の主張・要求を強要しようとする試み。平常時と非常時の境目が曖昧で、武力行使前の段階でのサイバー攻撃などが含まれる)を想定した非常時における(国民の)諸権利のあり方について検討を進める。

加えて、政府等の公的主体によるインターネットへの関与のあり方について、「自律・分散・協調」というインターネットの基本精神を踏まえつつ、インターネットガバナンスの観点から多角的に検討する。上記の議論については、国際関係論、安全保障、外交政策などの専門家を迎えて検討を進めるとともに、市民・企業等・政府が緊密に連携する日本型のデジタルトライアングルを念頭に、法執行の確保を含め、地球規模での俯瞰した議論を進める。

(3) データ駆動社会における競争枠組み

(主査： 林秀弥 名古屋大学大学院法学研究科教授)

産業構造のデジタル化によって、リアル空間とサイバー空間の壁を超えてデータや情報を融合・連携しつつ多様なサービスを展開する Cyber Physical System (CPS) がデータ駆動社会の基本になっていく。CPS が実現した社会においては、取得できるデータの大規模・広範囲化のもたらす弊害、AI 等の判断による責任主体の不明確化、巨大プラットフォームによる支配力の行使など様々な課題が

挙げられる一方、こうした変化については市場の革新性を損なわない観点からは事前規制ではなく、アジャイルガバナンスやゴールベースによる法規制の有効性が見込まれるため、これらのアプローチが抱える課題を含め、今後のあり方について議論を進める。

また、競争政策については公正取引委員会における検討は主として BtoB を対象とするものであるが、今後は対消費者取引についても所要の枠組みを検討することが求められることから、こうした問題意識を基に新たな理論枠組みについて検討する。

さらに、プラットフォーマーが自由な競争を阻害しないための責任やグリーンランスフォーメーション(GX)等の公共的課題への対応を促す観点から、競合する企業等が協力しデータ共有などを行うことが有効である一方、こうした行為が競争政策の観点からどう取り扱われるべきか等についても議論を進める。

(4) データ駆動社会における融合型コンテンツ流通

(主査： 内山隆 青山学院大学総合文化政策学部総合文化政策学科教授)

2010 年代後半以降、DAO (Decentralized Autonomous Organization) や Web3、メタバース、生成 AI コンテンツといった技術の展開と推し活やファン・コミュニティなどのユーザー活動の世界規模での拡大はとどまるところを知らない。その鍵となるのが、クリエイター・エコノミーと、国境を越えたグローバル流通市場の普遍化である。

それでも、「メジャーとインディ」、「プロとアマチュア」、「プラットフォームとコンテンツ」という階層構造あるいは垂直的関係そのものは当面変わらずに存在し続けるだろう。ただし、それらの役割や関係性は従前とは大きく変化することが予想されるため、「相互の位相関係」や「クリエイター個々人のキャリアパス」、「デジタル人材育成」、「著作権」というよりは「データの帰属や主権のあり方」などを俯瞰的に見通さないと、メディア/コンテンツ領域は中長期的にみて個々人が人生や生活をかけるに値しない作業領域になりかねない。

これらの認識に基づき、(1)柔軟なコンテンツ制作・流通の実現、(2)伝送路の制約を受けないメディア多様性の確保、(3)グローバルな課題への対応について、制作・流通・利用・消費の全ての観点から、多様なステークホルダーの意見を集約しつつ議論を進める。

(5) データ駆動社会を加速させるルール整備

(主査：生貝直人 一橋大学大学院法学研究科ビジネスロー専攻教授)

デジタル社会のルールとしての“情報法”は、データ・プラットフォーム・AI の影響により、第一期としてのマスメディア環境、第二期としてのインターネット環境に続く、新たな情報環境を前提としたルール形成、いわば第三期情報法とも呼ぶべき議論枠組の必要性に直面している。データ・プラットフォーム・AI がもたらす以下のパラダイムシフトを念頭に、データ駆動社会を加速させるルール整備のあり方を論じる。

データ：情報法は従来、人が生み出す表現(表現の自由論、著作権論)と、人に関わる情報(個人情報・プライバシー論)を主な検討の射程としてきた。しかしデータ駆動社会では、IoT や AI 等の機械が生み出す、非表現・非個人データの重要性が急速に拡大しつつある。EU の Data Act など参照しながら、非表現・非個人データの保護と活用に関わる法制のあり方を我が国でも検討していく必要がある。

プラットフォーム：2000 年前後に各国で確立したプロバイダ責任制限法制は、違法情報流通に対するプラットフォームの事後的責任の調整を主眼としてきた。しかし EU のデジタルサービス法に代表されるように、2020 年以降、プラットフォームの違法・有害情報流通に対する積極的な責務を規律する立法が世界的に拡大している。我が国でも、情報流通プラットフォーム対処法のあり方を含めた継続的な議論が求められる。

AI：2010 年代からのディープラーニング技術を受けプロファイリング・製品安全の論点を中心に拡大した AI 規制論は、2022 年以降の生成 AI の普及により、機械が生み出す情報が主となる情報環境を巡る法のあり方の議論へと拡張した。さらに、2026 年の Mythos 問題以降、人の知性を超えた存在の制御という新たな課題が現実化しつつある中で、我が国でも、国際協調を含むルール形成の議論を本格化させる必要がある。

(6) 分散型 ID による主権確保

(主査：國領二郎 慶應義塾大学名誉教授)

特定の企業や国家による過度に集権的なデータ管理(すなわち他国や個人の

主権侵害)を防ぐ上で注目されるのが、(1)分散型データ管理および(2)分散型ID管理である。

分散型データ管理は、データを単一のサーバーに集中させず、暗号化して複数ノードや個人の手元に分散保管するアプローチを指す。また、これと密接に関わるデータ主権の観点では、自国や自国民にかかわるデータを国外プラットフォームに依存せず自国内で管理する「データローカリゼーション」の議論とも親和性が高い。

分散型ID管理は、自らの秘密鍵をデータ主体(本人)自身の手元(ICカードやスマートフォンのセキュアハードウェアなど)で管理するモデルである。分散型IDは、データが分散保管された状態のままで「誰にアクセス権を与えるか」を本人が直接コントロールすることを可能にし、分散型データ管理の実用性を高める技術といえる。

技術的には、AI エージェントに処理を代行させる際に、アクセス権や実行権限の範囲を細かく制限・付与する場面での活用が期待される。このように大きな可能性を秘めた分散型IDだが、社会実装を進める上では制度や法的基盤の未整備が課題となる。例えば、権利能力を持たないAI エージェントに対して民法上の「代理権」を付与することはできず、法的にはあくまで利用者の「使用者(道具)」として位置づけられる点や、法人の下部組織や担当者が秘密鍵を用いて署名・実行した場合の法的効力の所在などが不透明である。こうした技術の進展に即した政策的・法的な環境整備が求められる。

(7) データ駆動社会におけるサイバーセキュリティ

(主査: 神園雅紀 デロイト トーマツ サイバー合同会社 サイバーセキュリティ先端研究所所長)

インターネットが社会経済基盤の中に占める重要性が高まる中、サイバーセキュリティの確保は経済安全保障に直結する課題として議論されるようになってきており、従来の技術論としてのサイバーセキュリティに止まることなく、ナショナリズム、経済、外交、政治など、様々な視点を取り入れた俯瞰的なサイバーセキュリティ戦略を検討する必要性が急速に高まっている。特に、AI を利用した偽情報によって引き起こされるプロパガンダによる世論の誘導に対しては、喫緊の対策が必要である。

また、データの真正性(integrity)の確保はデータ駆動社会における最重要の

要素となってきた。とりわけデータスペース(データのサプライチェーン)における真正性を確保する仕組みを総括した法制度を検討する必要がある。その際、上述の EU におけるデータガバナンス法やデータ法のようにデータ取次者によるデータ品質確保のための制度(トラストサービス)やデータ流通を促進するための仕組みを盛り込んだ法制度についてデータセキュリティやデータスペースの観点を念頭に置きつつ検討を進める。

上記の他、デジタル社会におけるサイバーセキュリティを巡る新たな課題について整理し、さらにこれらの課題の解決に向けた手段等の社会実装の手法についても検討を進める。

以 上