国立国会図書館 調査及び立法考査局

Research and Legislative Reference Bureau
National Diet Library

論題 Title	EU のデータ保護法制とデジタル立憲主義―AI 規制の憲法的ガバナンス―
他言語論題 Title in other language	Data Protection Law in the EU and the Rise of Digital Constitutionalism: Toward Constitutional Governance of AI Regulation
著者 / 所属 Author(s)	佐藤 太樹（SATO Taiki） / 国立国会図書館調査及び立法考査局　憲法課
雑誌名 Journal	レファレンス（The Reference）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
通号 Number	878
刊行日 Issue Date	2024-2-20
ページ Pages	25-53
ISSN	0034-2912
本文の言語 Language	日本語（Japanese）
摘要 Abstract	EU では、AI やプロファイリング技術の進展を背景として、EU 基本権憲章の憲法的価値に即したデータ保護や AI 規制を目指すデジタル立憲主義が唱えられ、これに沿った法的対応が進んでいる。

EU のデータ保護法制とデジタル立憲主義
―AI 規制の憲法的ガバナンス―

国立国会図書館　調査及び立法考査局
憲法課　佐藤　太樹

目　　次

キーワード：デジタル立憲主義、データ保護法制、プロファイリング規制、GDPR、AI 規則案

要　旨

① 近年 EU（欧州連合）では、データ保護法制（個人データ保護や AI（人工知能）規制）などの分野において、EU 基本権憲章の憲法的価値に即して新しいデジタル政策を立法化する動きが進んでいる。この動向に呼応してヨーロッパの公法学説では、デジタル立憲主義が提唱されている。データ保護法制の文脈においては、デジタル立憲主義は、AI やプロファイリング技術の進展を背景にしながら、人間中心のデジタル化を志向し、憲法的価値に即した個人データ保護や AI 規制を目指す考え方である。

② デジタル立憲主義の議論では、データ保護法制が EU 基本権憲章の基本権を具体化する立法として位置付けられている。EU のデータ保護法制は、プライバシー権の保障を淵源としながらも、プライバシー権の古典的意義（私生活の秘匿）に還元され得ない多様な憲法的価値（情報自己決定権、事業者のアカウンタビリティ、データ取扱いの公正性及びデュー・プロセス）を反映する形で発展してきた。

③ 2016 年制定の GDPR（一般データ保護規則）は、①プロファイリング（様々な個人情報から自動的な取扱いを用いて個人の趣味嗜好（しこう）、健康状態、社会的信用、職業適性などを自動的に予測・分析すること）に伴う過誤や差別的バイアスを規制するために、自動化された意思決定に対するチェック及び異議申立ての権利を保障しているほか、②プロファイリングのプロセスを透明化することで基本権侵害のリスク（アルゴリズムによる差別や人間中心の自己決定原理の毀損）を可視化する仕組みを制度化し、さらに③事業者に対してリスク逓減（risk mitigation）のためのガバナンス規律を義務付けている。

④ 2021 年に公表された AI 規則案による AI 規制においても、GDPR のプロファイリング規制と同じく、憲法的価値に準拠した規制枠組みが採用されている。GDPR の規制と異なる点として、基本権侵害の程度に応じてリスク評価の基準が明文化されるとともに、事業者に対して適合性評価手続などのガバナンス規律を義務付け、事業者に対する監督・統制を強化していることが挙げられる。

はじめに

近年、欧州連合（European Union. 以下「EU」という。）では、データ保護法制（個人データ保護や人工知能（Artificial Intelligence. 以下「AI」という。）規制）などの分野において、EU 基本権憲章（Charter of Fundamental Rights of the European Union. 以下「基本権憲章」という。）(1) の憲法的価値に即して新しいデジタル政策を立法化する動きが進んでいる。この動向に呼応してヨーロッパの公法学では、デジタル立憲主義（digital constitutionalism）が提唱されている。デジタル立憲主義とは、「急速に発展するデジタル技術を扱う私的主体が権力者となりうるデジタル空間に立憲主義の価値を持ち込むことを志向する新たな研究潮流」(2) である。その議論の射程は、表現の自由、個人データ保護、認知過程の自由(3) など多種広範な領域に及ぶ。

本稿は、データ保護法制と憲法との関係性に注目し、デジタル立憲主義の議論内容を検討する。データ保護法制の文脈において、デジタル立憲主義は、AI やプロファイリング（profiling）(4) 技術の進展を背景にしながら、人間中心のデジタル化を志向し、憲法的価値に即した個人データ保護や AI 規制を目指す考え方である。この議論によれば、EU のデータ保護法制は、基本権憲章の憲法的価値を具体化する立法として位置付けられており、かつ、データ保護法制の立法及び解釈は、こうした憲法的価値に即して規律されるべきものとされる。

＊本稿の内容は、令和 5（2023）年 12 月 12 日現在の情報に基づく。インターネット情報の最終アクセス日も、同日である。また、文中で言及する人物の肩書は、当時のものである。

(1) “CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION,” OJ C 326, 2012.10.26, pp.391-407. EUR-Lex Website <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>「この憲章は、…（中略）…とりわけ加盟国に共通する憲法の伝統及び国際法上の義務、人権及び基本的自由の保護のための欧州条約、連合及び欧州評議会の採択した社会憲章並びに EU 司法裁判所及び欧州人権裁判所の判例法から生じる権利を再確認する」（前文）。翻訳として、岡久慶・山口和人訳「欧州連合基本権憲章」『外国の立法』No.211, 2002.2, pp.14-20 を参照。

(2) 山本健人「デジタル立憲主義と憲法学」『情報法制研究』13 号, 2023.5, p.56. 日本の議論動向については、曽我部真裕「社会のデジタル化と憲法」憲法理論研究会編『次世代の課題と憲法学』敬文堂, 2022, pp.33-49; 山本龍彦「近代主権国家とデジタル・プラットフォーム―リヴァイアサン対ビヒモス―」山元一編『講座　立憲主義と憲法学　第 1 巻　憲法の基礎理論』信山社, 2022, pp.147-181; 同「デジタル化と憲法（学）」『自治研究』99 巻 4 号, 2023.4, pp.3-37; 宍戸常寿「憲法と社会のデジタル化についての覚書」『世界』975 号, 2023.11, pp.156-165 を参照。

(3) 「認知過程の自由」とは、神経科学の発展に伴い神経測定及び神経操作を駆使したブレインテックの実装が進みつつある状況の中で、技術促進と規制のバランス確保を目指す自由概念の総称である。生成途上の議論ではあるが、神経科学と法学との横断的な対話を可能にする憲法学説として、近年注目を集めている（小久保智淳「「認知過程の自由」研究序説―神経科学と憲法学―」『法学政治学論究』126 号, 2020.9, pp.375-410.）。さらに、この認知過程の自由は、ケンブリッジ・アナリティカ事件（政治マーケティング企業が、Facebook 利用者のプロフィール等のデータを不当に収集し、各人の心理的傾向を解析した上でこれを選挙戦略に利用した事例）を契機に、デジタル立憲主義とも結び付けて議論されている。例えば、山本龍彦慶應義塾大学教授は、ケンブリッジ・アナリティカ事件に言及した上で、プラットフォーム企業が、AI・アルゴリズムを通じて「人間の内面ないし認知過程に介入・浸透し、これを操縦」できるようになったと指摘し、こうした状況を踏まえて立憲主義の議論をアップデートすべきだと主張している（山本龍彦「デジタル化と憲法（学）」同上, pp.4, 29-30.）。このように、デジタル立憲主義をめぐる議論は、認知過程の自由など新しい学問潮流も取り込みつつ進展している。本稿では、デジタル立憲主義が、データ保護法制の発展を促す原動力として機能してきた側面（理念と制度の連動関係）に注目し、議論動向の整理及び検討を行う。

(4) ここでいうプロファイリングとは、「様々な個人情報から人工知能（Artificial Intelligence: AI）を用いて個人の趣味嗜好、健康状態、社会的信用力、職業適性、内定辞退予測率などを自動的に予測・分析する」技術のことを指し、近年では AI の技術革新を背景に、「ターゲティング広告の配信を目的とした利用を超えて、与信審査や企業の採用活動など、個人の人生を左右しかねない重要場面で、こうした手法が用いられるようになっている」（山本龍彦「「完全自動意思決定」のガバナンス―行為統制型規律からガバナンス統制型規律へ？―」『情報通信政策研究』3 巻 1・2 号, 2019, pp.25-26.）。また、プロファイリング規制や AI 規制を包括的に分析したものとして、福岡真之介ほか編『AI プロファイリングの法律問題―AI 時代の個人情報・プライバシー―』商事法務, 2023 を参照。

第Ⅰ章では、データ保護法制の歴史的沿革を踏まえて、デジタル立憲主義の背景事情やその議論枠組みを明らかにする。

第Ⅱ章では、① 2016 年制定の一般データ保護規則（General Data Protection Regulation. 以下「GDPR」という。）(5)のプロファイリング規制と② 2021 年に欧州委員会（European Commission）が公表した AI 法（Artificial Intelligence Act）案（以下「AI 規則案」という。）(6)の AI 規制に注目する。具体的には、両者の規制がデジタル立憲主義の中でどのように位置付けられているのかを分析し、両者の規制枠組みの中に憲法的価値がどのように組み込まれているのかを明らかにする。まず、GDPR は、①プロファイリングに伴う過誤や差別的バイアスを規制するために、自動化された意思決定に対するチェックと異議申立ての権利を保障しているほか、②プロファイリングのプロセスを透明化することで基本権侵害のリスクを可視化する仕組みを制度化し、さらに③データ管理者（事業者）(7)に対してリスクの逓減のためのガバナンス規律(8)を義務付けている。一方、AI 規則案は、①憲法的価値に準拠したリスク評価の基準を明文化しているほか、②事業者による内発的なリスク逓減（risk mitigation）の取組を促進するようなガバナンス規律の仕組みを強化している(9)。

Ⅰ　デジタル立憲主義とデータ保護法制

1　デジタル立憲主義におけるデータ保護法制の位置付け

本章では、デジタル立憲主義においてデータ保護法制が憲法具体化立法(10)として位置付け

⑸　Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 2016.5.4, pp.1-88. EUR-Lex Website <https://eur-lex.europa.eu/eli/reg/2016/679/oj> 2016 年制定の GDPR は、私企業や公的機関による個人データの取扱いを統一的に規律する一般法であり、EU 加盟国に直接適用される。本稿における GDPR の翻訳については、個人情報保護委員会の仮訳を参考に、一部訳文を変更している。個人情報保護委員会訳「個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則（EU）2016/679（一般データ保護規則）【条文】」<https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf>

⑹　European Commission, “Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts,” COM(2021) 206 final, 2021.4.21. EUR-Lex Website <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206> この案は、法形式としては「規則」（regulation. EU 加盟国に直接適用される。）であるため、本稿では「AI 規則案」と表記する。AI 規則案の翻訳については、総務省 AI ネットワーク社会推進会議の仮訳（三部裕幸訳「「人工知能に関する調和の取れたルールを定める規則の提案」（欧州委員会（2021 年 4 月 21 日））本文・付属書（仮訳）」総務省ウェブサイト <https://www.soumu.go.jp/main_content/000826706.pdf>）を参考に、適宜用字等を変更している。

⑺　データ管理者（controller）とは、「自然人又は法人、公的機関、部局又はその他の組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者」（GDPR 第 4 条 (7)。個人情報保護委員会訳前掲注⑸, pp.3-4.）であり、管理者の代わりに個人データを取扱う処理者（processor）とは区別される（GDPR 第 4 条 (8)）。以下、GDPR を説明する箇所では「データ管理者」と表記し、それ以外の場面では、データ管理者を含めた民間事業者を指す用語として適宜「事業者」と表記する。

⑻　山本龍彦教授は次のように指摘している。GDPR が保障する諸権利の内容や範囲は「いまだ確定的ではなく、また権利侵害行為又は違反行為があっても、これを外部から発見することは非常に困難であるという問題を抱えている。GDPR は、かかる法的不確定性と執行困難性の問題を前提に、事業者自らが行動規範等の策定を通じて不確定性の隙間を埋めたり、データ保護影響評価（DPIA）やアルゴリズム監査といった内部統制システムを整備したりして、想定される違反行為等を未然に防ぐガバナンス体制を構築することを、かかる体制構築の努力と制裁金の免除･軽減とを結び付けることで（明示的なインセンティブ設計）実効的に促している」。（山本　前掲注⑷, p.25.）

⑼　AI の活用に関するガバナンスの在り方を検討したものとして、寺田麻佑「AI とガバナンス―規制等に適する分野，適さない分野―」『情報法制研究』5 号, 2019.5, pp.18-31 を参照。

⑽　デジタル立憲主義を提唱する論者は、EU のデータ保護法制が、基本権憲章の基本権を具体化する立法として位置付けられている点を踏まえた上で（後述本章第 2 節参照）、データ保護法制の中に具体化されるべき憲法的

られている点を分析する。以下、デジタル立憲主義を提唱する論者が、憲法とデータ保護法制をどのように関連付けているのかを概観し、その上で本章の検討課題をより具体的に提示する。

デジタル立憲主義を提唱する論者は、データ保護法制を、憲法的価値に即して解釈すべきだと主張しているが（後述第Ⅱ章参照）、このような解釈論を論証するに当たって、データ保護法制の目的が憲法的価値と密接に結び付いてきた点を強調している。デジタル立憲主義の代表的論者であるエドアルド・セレステ（Edoardo Celeste）氏（ダブリンシティ大学）及びジョバンニ・デ・グレゴリオ（Giovanni De Gregorio）氏（ポルトガル・カトリック大学カトリック・グローバル法科大学院）は、「GDPR は法形式的には憲法的性格を有さないが、機能的視点から見れば憲法に準ずる役割（para-constitutional role）を果たしていると言える。それは AI のアルゴリズムが浸透した社会の文脈の中で、中核的な憲法原理を翻訳し実現するものである」(11)と指摘し、データ保護法制を憲法具体化立法として位置付けている。

デ・グレゴリオ氏は、EU のデータ保護法制が憲法的価値を具体化する立法として形成されてきた点を強調している。同氏によれば、「データ保護法の目的は、データの取扱いに係る透明性やアカウンタビリティを確保しながら個人の自律を保護する点にある」(12)が、この背景には、データ保護法制が憲法具体化立法として位置付けられてきたことが関係している。この点についてデ・グレゴリオ氏は、オーラ・リンスキー（Orla Lynskey）氏（ロンドン・スクール・オブ・エコノミクス）の文献(13)を参照しながら次のように述べている。

> ヨーロッパの枠組みにおける個人データ保護は、テクノロジーの進歩に対応しながら発展してきた比較的新しい権利である。ヨーロッパのデータ保護法は、個人データの取扱いに伴うアカウンタビリティを欠いた権力に由来する脅威に直面する状況の中で、単純な消極的な自由であるプライバシーから積極的な自由である個人データ保護へと移行していったことを証している(14)。

ここでは、データ保護法制の保護法益が、古典的プライバシー権(15)から個人データ保護権へと次第に推移していった経過が指摘され、プライバシー権と個人データ保護権が別個独立の

価値の内容として、基本権憲章の基本権規定の価値理念（人間の尊厳、自己決定、平等、プライバシー）だけではなく、法の支配やデュー・プロセスといった関連した立憲主義的価値も取り上げている（後述本章第 5 節及び第Ⅱ章第 2 節参照）。

⑾ Edoardo Celeste and Giovanni De Gregorio, “Digital Humanism: The Constitutional Message of the GDPR,” *Global Privacy Law Review*, Vol.3 Iss.1, 2022.2, p.5.

⑿ Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge; New York: Cambridge University Press, 2022, p.255.

⒀ Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford: Oxford University Press, 2015.

⒁ De Gregorio, *op.cit.*⑿, p.224.

⒂「プライバシー権は、伝統的には、私生活の平穏の利益と結びつけて理解されてきた（古典的プライバシー権論）。そして、私生活に関する情報をみだりに公開されない権利は、その必須の構成要素とされてきた」（黒澤修一郎「プライバシー権」山本龍彦・横大道聡編著『憲法学の現在地―判例・学説から探究する現代的論点―』日本評論社, 2020, pp.140-141.）。アメリカの憲法学説及び情報法学説では、プライバシー権の中に自己情報コントロール権や構造審査の視点も盛り込むようになっている点につき、山本龍彦『プライバシーの権利を考える』信山社出版, 2017, pp.3-21. 一方、アメリカの学説を参考にしながら、プライバシー権を「適正な自己情報の取扱いを受ける権利」に再構成すべきだと主張する見解として、音無知展『プライバシー権の再構成―自己情報コントロール権から適正な自己情報の取扱いを受ける権利へ―』有斐閣, 2021. このようにアメリカの学説では、プライバシー権の内容を拡張的に理解する方向が目指されてきた一方、EU では、プライバシー権とは別に個人データ保護権の観念が成立し、個人データ保護権の中に情報自己決定権などの多種多様な憲法的法益が読み込まれてきた。

基本権として位置付けられている。こうした理解は、上記引用部分で参照されているリンスキー氏の研究に依拠したものである（後述本章第 4 節（2）参照）。デ・グレゴリオ氏は、データ保護法制が、プライバシー権の古典的価値には還元され得ない多様な憲法的価値（情報自己決定権、事業者のアカウンタビリティ、データ取扱いの公正性及びデュー・プロセス（due process）[16]）を反映する形で発展してきたと指摘している（後述本章第 5 節及び第Ⅱ章第 2 節参照）。

こうして見ると、デジタル立憲主義は、ヨーロッパのデータ保護法制が憲法的価値と密接に関連しながら発展してきた歴史と不可分に結び付いた言説であると言うことができる。以下では、デジタル立憲主義の論者が依拠した先行研究に立ち返りながら、データ保護法制の保護法益（プライバシー権と個人データ保護権の異同）を分析し、デジタル立憲主義の背景事情を明らかにする（後述本章第 2 節～第 4 節参照）。次いでデジタル立憲主義の議論の中で憲法とデータ保護法制がどのように結び付けられているのかを明らかにする（後述本章第 5 節参照）。

2　データ保護法制と基本権

EU では、データ保護法制が基本権を具体化する立法として位置付けられてきた。すなわち、2016 年制定の GDPR は、その第 3 章で列記されたデータ主体（data subject）[17]の諸権利を「個人データ保護の権利」と総称し、これが基本権憲章第 8 条に基礎を置くものであると位置付けている[18]。基本権憲章は 2000 年に制定されたものであるが、第 7 条において私生活の尊重を受ける権利（right to respect for private life）を定める一方、これに加えて第 8 条において個人データ保護権（right to the protection of personal data）を規定している。後者の個人データ保護権は 1995 年のデータ保護指令（Data Protection Directive）[19]を、基本権規定として再構築する目的で制定されたものである。更に遡れば、データ保護指令は、その前文において、データ保護法制が、欧州人権条約（European Convention on Human Rights）[20]やプライバシー権に基礎を置くものであると明記している。データ保護指令の制定当時、欧州人権条約第 8 条は既にプライバシー権の法源として解釈運用されており、また、ヨーロッパ各国においても既に一連のプライバシー法制が整備されつつあった（後述本章第 3 節参照）。

以上、GDPR に至るまでのデータ保護法制の沿革を概観したが、そこから次の点を指摘することができる。すなわち、GDPR で保障されたデータ主体の諸権利は、沿革的には元々プライバシー権にその淵源を持つ規定である。もっとも GDPR は、直接には基本権憲章第 8 条の個人データ保護権に基礎を置くものであり、その限りでは、個人データ保護権が、プライバシー

---

⑯　デュー・プロセスには実体的デュー・プロセスと手続的デュー・プロセスが含まれており、そのうち本稿と関係するのは後者の手続的デュー・プロセスである。手続的デュー・プロセスとは、手続的正義の理念を意味しており、伝統的には通知と聴聞に基づく適正な異議申立ての機会の確保と結び付いてきた（樋口範雄『アメリカ憲法　第 2 版』弘文堂, 2021, pp.270-273, 299-313.）。データ保護法制やデジタル立憲主義の文脈でデュー・プロセスの理念が言及される場合、その場合のデュー・プロセスの意味は、個人データの取扱いの公正性（fairness）や自動化された意思決定に対する異議申立ての機会の確保と結び付いている（後述第Ⅱ章参照）。

⑰　データ主体とは、「識別された自然人又は識別可能な自然人」を指す（GDPR 第 4 条第 1 項。個人情報保護委員会訳　前掲注⑸, p.3.）。

⑱　GDPR 前文第 1 項、第 2 項及び第 4 項

⑲　Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 1995.11.23, pp.31-50. EUR-Lex Website <http://data.europa.eu/eli/dir/1995/46/oj> GDPR 制定時に廃止。前掲注⑸を参照。

⑳　“European Convention on Human Rights.”Council of Europe Website <https://www.echr.coe.int/documents/d/echr/Convention_ENG>

権から徐々に分化していった歴史にも対応している。以下では、データ保護法制を支える憲法的理念の発展と変遷（プライバシー権から個人データ保護権へ）を、データ保護法制の沿革的背景に即して検討する。

3　プライバシー権と個人データ保護権の分化

(1) データ保護法制の誕生とプライバシー権

EU のデータ保護法制はプライバシー権に淵源を持つが、その端緒は、1973 年及び 1974 年の欧州評議会（Council of Europe）[21]の決議にまで遡ることができる。1973 年に欧州評議会は、「民間部門の電子データバンクに対する個人のプライバシー保護に関する決議」（以下「1973 年決議」という。）を採択し、加盟国に対してデータ保護法制を整備するように勧告した[22]。1973 年決議は、「民間部門での電子データバンクの活用によって個人情報の保存・処理・流通の段階で濫用が生ずることを防ぐために、個人を保護するための立法措置が講ぜられるべきである」と述べ、おおむね次のような立法指針を提示した。①「保存された情報が正確でなければならない」（情報の正確性）、②「個人の親密な私生活に関する情報や不公正な差別につながり得る情報は記録されてはならない」（取得禁止情報）、③「情報は保存の目的と適合し関連したものでなければならない」（目的制限）、④各人は「保存されている自己に関する情報や記録の目的を知る権利を有しなければならない」（アクセス権）、⑤不正確な個人情報を訂正し、違法な手段で取得された情報を削除できるような仕組みが整備されなければならない（削除訂正権）。

欧州評議会は翌年の 1974 年に「公的部門の電子データバンクに対する個人のプライバシー保護に関する決議」（以下「1974 年決議」という。）を採択し、おおむね民間部門と同様のデータ保護法制が整備されなければならないと勧告した[23]。1974 年決議では、データ保護法制はプライバシー保護のための制度であると同時に、欧州人権条約第 8 条（私生活の尊重を受ける権利）を保障するための制度として位置付けられている。

これらの欧州評議会の決議と前後してヨーロッパ各国でも 1970 年代に体系的なデータ保護法制の整備が進められた。確かにこれらの法制は各国ごとに独自の憲法的背景を持っていたと言えるが[24]、少なくとも 1970 年代のヨーロッパでは、欧州評議会の決議と同内容の法制が整備され、個人データの保護がプライバシー権の保障と結び付けて捉えられていた。

⑵1 「欧州評議会（Council of Europe）は、人権、民主主義、法の支配の分野で国際社会の基準策定を主導する汎欧州の国際機関として、1949 年フランスのストラスブールに設立され」、主に欧州人権条約を所管している。「欧州評議会（Council of Europe）」外務省ウェブサイト <https://www.mofa.go.jp/mofaj/area/ce/index.html>

⑵2 Council of Europe Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, 1973.9.26.

⑵3 Council of Europe Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, 1974.9.20.

⑵4 例えばドイツでは 1983 年の国勢調査判決（BVerfGE 65,1, Urteil v.15.12.1983. ドイツ憲法判例研究会編『ドイツの憲法判例　第 2 版』信山社出版, 2003, pp.60-66.）によって情報自己決定権（informationelles Selbstbestimmungsrecht）が確立されたが、ボード・ピエロートほかの概説書によると、「それは国家の市民に対する情報に関する対応に関して広く正当化を義務付ける契機となりその結果、包括的な情報・データ保護法が制定され、それは次第に市民相互の関係性をもとらえつつある」という（ボード・ピエロートほか（永田秀樹ほか訳）『現代ドイツ基本権第 2 版』法律文化社, 2019, p.131.（原書名：Bodo Pieroth et al., *Staatsrecht II Grundrechte*, 31. Aufl., Heidelberg: C.F. Müller, 2015.））。なおドイツの情報自己決定権と古典的プライバシー（私生活の秘匿）との関係性について小山剛慶應義塾大学教授は、「情報自己決定権説によれば、単純な個人情報保護は古典的プライバシー権と同じく、人格権の一内容であるが、どちらかが他方に吸収･統合されるのではなく、併存すると解する（二元的構成）」（小山剛「単純個人情報の憲法上の保護」『論究ジュリスト』1 号, 2012.春, p.122.）と指摘している。

例えば、1978 年に「プライバシー立法の比較分析」と題する論文を発表したヨーン・ビング（Jon Bing）氏（オスロ大学）は、ドイツ・フランス・オランダ・スウェーデン・ノルウェーなどのデータ保護法制を比較検討した上で、「特にヨーロッパについては、現在勃興しつつあるプライバシー立法は、1973 年及び 74 年の欧州評議会決議で提示されたガイドラインとおおむね軌を一にするものであった」[25]と指摘し、各国のデータ保護法に共通する内容として、①収集された個人情報が正確でなければならず、収集された情報が利用目的と関連性[26]を持つこと、②一定のセンシティブ情報の取得・利用禁止、③収集された情報の内容及びその利用目的を知る権利、の 3 点を取り上げている[27]。

また、1980 年に経済協力開発機構（Organisation for Economic Co-operation and Development. 以下「OECD」という。）によって採択された理事会勧告「プライバシー保護と個人データの国際流通についてのガイドライン」[28]でも、当時既に加盟国の大半でデータ保護法制が整備されつつあった状況（ヨーロッパではドイツ・フランス・ルクセンブルク・ノルウェー・スウェーデン）に言及した上で、「自動データ処理の発達により個人データに関するプライバシー保護を検討する必要が生じてきた」と説示し、データの取扱いに関して次の 8 つの基本原則が勧告された。すなわち、①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則、である。

プライバシー保護の観点からデータ保護法制を拡充する動きが欧米を中心に活発化する情勢の中で、1980 年に欧州評議会は、「個人データの自動処理に関する個人の保護に関する条約」[29]（以下「第 108 号条約」という。）を採択した。これによって批准国はこの条約の規定を国内法に導入することが義務付けられた。第 108 号条約第 1 条では、「個人データの自動処理に関して本人のプライバシー権（個人データ保護）」を確立することが基本理念として掲げられており、これを受けて条約全体の規定としても、おおむね欧州評議会の 1973 年決議及び 1974 年決議と同一内容の規律が設けられた。

さらに、この第 108 号条約とほぼ同じ内容を引き継いだ EU のデータ保護法として、1995 年にデータ保護指令が制定された。同指令の前文第 11 項では、「個人の権利及び自由の保護、特にプライバシー権の保護の原則に照らして、個人データの自動処理に関する個人の保護に関する 1981 年 1 月 28 日欧州評議会条約［上記第 108 号条約。筆者加筆］に定められていたものに効力を与え、これを増強する」と規定されている。

以上、EU のデータ保護法制の来歴を確認してきた。これらの沿革に照らして見ても、データ保護法制は、プライバシー権の保護に由来するものであったと再確認することができる[30]。

⑵⑸ Jon Bing,“A Comparative Outline of Privacy Legislation,”*Comparative Law Yearbook*, Vol.2, 1978, p.149.

⑵⑹ 関連性の原則を検討するものとして、高木浩光「個人情報保護から個人データ保護へ（6）」『情報法制研究』12 号, 2022.11, pp.49-83; 同「個人情報保護から個人データ保護へ（7）」『情報法制研究』13 号, 2023.5, pp.114-133.

⑵⑺ Bing, *op.cit*.⑵⑸, p.170.

⑵⑻ OECD,“OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,”1980.

⑵⑼ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.108). <https://rm.coe.int/1680078b37>

⑶⓪ “Data Protection.”European Data Protection Supervisor Website <https://edps.europa.eu/data-protection/data-protection_en> 欧州データ保護監視機関（European Data Protection Supervisor）のウェブサイトによると、「人間の尊厳の観念の下では、プライバシーないし私生活の権利、つまり自律的である権利、自己に関する情報をコントロールする権利は重要な役割を果たす」ものであり、この権利は欧州人権条約第 8 条及び基本権憲章第 7 条（双方とも私生活の尊重を受ける権利を定める。）によって保障されている。さらに、基本権憲章第 8 条によって保障された個人データ保護権も、「プライバシー権に由来するものであり、両者は基本的な価値と権利を維持促進するのに仕

(2) プライバシー権と個人データ保護権の分化

もっとも、2000 年に基本権憲章が制定されると、個人データ保護権の独自性と自律性が次第に強調されるようになった。基本権憲章の起草委員会によると、基本権憲章第 7 条（私生活の尊重を受ける権利）が欧州人権条約第 8 条をほぼそのまま引き継いだ条文であるのに対して、基本権憲章第 8 条（個人データ保護権）は、1995 年のデータ保護指令等に基づいて新たに創設された規定であると解説されている(31)。この説明に照らせば、データ保護指令の保障するデータ主体の諸権利は、私生活の尊重を受ける権利とは別の独立した基本権として再構成されたことになる。こうした理解は、データ保護法制を所管する公的機関の見解にも反映されている。例えば、データ保護法制に関する諮問機関であった第 29 条データ保護作業部会（Article 29 Data Protection Working Party(32). 以下「第 29 条作業部会」という。）は、2009 年に次のように指摘している。「個人データの自動処理に関する個人の保護に関する欧州評議会条約（第 108 号条約）は、個人データの保護に関する基本権についてのヨーロッパで最初の法的枠組みであると言える。個人データ保護権は、欧州人権条約第 8 条の私生活の権利と密接に関連しているとはいえ、これと同一ではない。個人データ保護権は、基本権憲章第 8 条における 1 つの自立した基本権として承認されている」(33)。

今日でも、EU の法実務では、プライバシー権と個人データ保護権は、相互に関連しつつも独立した権利として位置付けられている(34)。こうした法実務の現状を背景に、学説では、個人データ保護権がプライバシー権に起源を持つ権利であることを前提にした上で、両者の別個独立性が論じられている。次節では、これらの学説を参考に、個人データ保護権の性格と構造を分析する。

4　プライバシー権・個人データ保護権二元説

(1) デ・ヘルト氏及びグートヴィルト氏の所説

ヨーロッパの情報法学説では、基本権憲章の条文構造に留意した上で、プライバシー権と個人データ保護権の差異が強調されている。例えば、2009 年のポール・デ・ヘルト（Paul De Hert）氏（ブリュッセル自由大学）及びセルジュ・グートヴィルト（Serge Gutwirth）氏（ブリュッセル自由大学）の共著論文では、次のように指摘されている。

> プライバシーは、明らかにデータ保護法の中で中核的位置を占めるものである。しかし、データ保護法を、専らプライバシーの保全に関するものとして捉えるのだとしたら、それは誤りである。データ保護法は多種多様な利益に仕えるものであるが、それらは一定の場合において伝統的なプライバシー構想からは遠く離れたところに存する。親密性志向のプライバシー構想は、データ保護法の条文には余り見いだし得ないものであり、逆にプライ

えている」と説明されている。もっとも、ウェブサイトでは、プライバシー権と個人データ保護権が、相互に関連しつつも、基本権憲章の条文上、別個独立の権利として説明されている。

(31) “Draft Charter of Fundamental Rights of the European Union,” CHARTE 4473/00, 2000.10.11, pp.10-11. European Parliament Website <https://www.europarl.europa.eu/charter/pdf/04473_en.pdf>

(32) 組織及び権限につき、データ保護指令第 29 条及び第 30 条を参照。

(33) Article 29 Data Protection Working Party, “The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data,” WP 168, 2009.12.1, p.5.

(34) 欧州データ保護監視機関のウェブサイト（前掲注(30)）に掲げられたデータ保護法制の解説文を参照。

> バシーをより広い意味で捉えようとしたとしても、それは、目的限定やデータの品質管理ないしセキュリティといったデータ保護法の諸原則を説明することができない[35]。

ここでは、個人データ保護権が、親密性の保全（私生活の秘匿）を核とする古典的プライバシー権とは区別されるべきものとして位置付けられている。つまり、個人データ保護権ないしこれを具体化したデータ保護法制は、古典的プライバシー権のように一定領域に局限された私生活の保護（例えばセンシティブ情報[36]のような「個人の私生活の核心」[37]の保護）に限定されるのではなく、より広く一般に個人データの取扱い全般を規律しており、「個人データの取扱いに対するコントロールや開示、アカウンタビリティや透明性を保障」[38]している。この点について、デ・ヘルト氏及びグートヴィルト氏は、データ保護指令の規定を参照しながら、次のように指摘している。

> 一般的に、個人データ保護は、データが収集されているかどうかに関する一定の情報を受け取る権利、情報に対するアクセス権、必要があればデータを修正してもらう権利、ある特定のデータの取扱いに対して異議を唱える権利といった一連の権利を個人に対して保障している。さらに、これらの法令は一般的に、データ管理者に健全なデータ管理の実装を要請し、次のような一連の義務を課している。つまり、特定の、明確で、正当な目的のために個人データを利用する義務、偶発的ないし不正な情報アクセス又はそうした情報操作に備えてデータ・セキュリティを確保しておく義務、一定の場合につき所定のデータ取扱いを行う前に特定の独立監視機関にこれを通知する義務、である[39]。

ここでは、古典的プライバシーとは区別できる個人データ保護権固有の特徴として、①個人データに対するコントロール手段の確保（権利規定）と②適正なデータ管理を確保するためのデータ管理者の義務が取り上げられている。デ・ヘルト氏及びグートヴィルト氏によれば、古

㉟ P. De Hert and S. Gutwirth,“Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action,”S. Gutwirth et al., eds., *Reinventing Data Protection?* London: Springer, 2009, p.10.

㊱「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの取扱いは、禁止される」（GDPR 第 9 条第 1 項。個人情報保護委員会訳　前掲注⑸, p.12.）。この規定の前身となったのは、データ保護指令第 8 条（特別なカテゴリーのデータの保護）であるが、データ保護指令前文第 34 項及び第 70 項では、特別なカテゴリーのデータが、センシティブ情報と互換的に説明されている。

㊲ De Hert and Gutwirth, *op.cit.*㉟, p.4, n.3.

㊳ S. Gutwirth and P. De Hert,“Regulating Profiling in a Democratic Constitutional State,”M. Hildebrandt and S. Gutwirth, eds., *Profiling the European Citizen: Cross-Disciplinary Perspectives*, New York: Springer, 2008, pp.278-279.

㊴ *ibid*., pp.281-282. なおここで引用されている 2008 年の論文では、主にデータ保護指令の規定を念頭に個人データ保護の基本原則を要約している。そのため以下では、データ保護指令の条文に即して個人データ保護の基本原則を補足した上で、現行法である GDPR との対応関係を示す。まず個人の権利規定について、自己の個人データが取扱いの対象となっている場合にその事実の確認を得るとともに、当該取扱いの目的を通知してもらうよう要求できる権利（アクセス権）につき、データ保護指令第 12 条 (a)（GDPR 第 15 条）を参照。また、個人データの修正及び消去権につき、データ保護指令第 12 条 (b)（GDPR 第 16 条及び第 17 条）を参照。次にデータ管理者の義務規定に関して、目的限定については、データ保護指令第 6 条第 1 項 (b)（GDPR 第 5 条第 1 項 (b)）が、個人データが、「特定され、明確であり、かつ、正当な目的のために収集されるものとし、かつ、その目的に適合しない態様で追加的取扱いをしてはならない」と定める。個人データの取扱いが公正であり、かつ、情報漏えい等のリスクに対して適切な安全性が講じられなければならない点につき、データ保護指令第 6 条第 1 項 (a) 及び第 17 条第 1 項（GDPR 第 5 条第 1 項 (a) 及び同項 (f)）を参照。

典的プライバシー権は、元来「一人で放っておいてもらう権利（right to be let alone）」として観念されてきたものであり(40)、その中核的な内容は、私生活に対する他者からの干渉を排除し、個人の自己決定を他者の視線から遮蔽し、その意味で個人を不可視化すること（opacity of the individual）に本質がある。そのためプライバシー権の典型的な内実は、私事を暴露されることからの自由として伝統的に理解されてきた。これに対してデータ保護法制は、個人データが広範に保存・利用・頒布されている状況を前提に、データ管理者に対して公正性やアカウンタビリティを義務付ける規範として構成されている。こうした規範の中には、個人データのコントロールを確保する権利だけではなく、個人データの取扱いに当たって「平等やデュー・プロセス」(41)を要請する規定など多種多様な内容が含まれる。

(2) リンスキー氏の所説

上記のデ・ヘルト氏及びグートヴィルト氏と同様に、プライバシー権・個人データ保護権二元説を採用する論者としてリンスキー氏がいる。同氏は、デ・ヘルト氏及びグートヴィルト氏の文献を参照しながら、個人データ保護権がプライバシー権と「重なり合いつつも別個」(42)の基本権であるとしている。つまり、両者は、人間の尊厳や個人の自律を保護法益とする点で共通しているが、個人データ保護権は、私生活の秘匿を核とする古典的プライバシー権にはくくり切れない多様な保護法益を内包している。リンスキー氏は、個人データ保護権の多様な保護法益について、その内実を 2 つの観点から説明している。

> 個人データ保護権はプライバシー権より広い範囲の個人データを対象とし、かつ、これに対してより多くのコントロールを個人に保障している。この強化されたコントロールは、…（中略）…2 つの主要目的を促進している。第 1 にそれは、情報自己決定（informational self-determination）を通じて個人の人格権を促進する。第 2 にそれは、個人の自律に消極的な影響を及ぼし得る情報と力の非対称性を縮減する(43)。

ここでは、データ保護法制の仕組みを、情報自己決定権の観点から統一的に把握するための理論的視座が提示されている。リンスキー氏によれば、データ保護法制の中核にあるのは、①情報自己決定権の保障であり、②さらにこの権利を実効的に保障するために、データ管理者に対して、データ主体とデータ管理者との間の情報の非対称性を縮減するための義務が課せられる。以下、2 つの要素を解説する。

（ i ）情報自己決定権

第 1 に、リンスキー氏は、ドイツの国勢調査判決(44)を参照しながら、データ保護法制が、情報自己決定権の理念を具体化していると指摘している。同氏は、情報自己決定権を具体化す

---

(40) De Hert and Gutwirth, *op.cit.*(35), pp.4-5. (citing Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review*, Vol.4 No.5, 1890.12.15, pp.193-220. <https://doi.org/10.2307/1321160>)

(41) *ibid*., p.6.

(42) Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order," *International and Comparative Law Quarterly*, Vol.63 No.3, 2014.7, p.587.

(43) *ibid*., p.597.

(44) ドイツ憲法判例研究会編　前掲注(24)を参照。

る実定法規として、主に忘れられる権利(45)、データポータビリティ権(46)及びデータ主体の同意の 3 点を取り上げている。ここでは、データ主体の同意に関する同氏の説明を紹介しながら、情報自己決定権がデータ保護法制の中核を構成している点を示す。

リンスキー氏によれば、EU ではオプトイン（Opt-in）での同意取得が「優先（preference）」(47)的な法原則として確立しており、それによって「個人データに対する最も強いコントロール」(48)が保障されてきた。

同氏によれば、データ主体が個人データの取扱いに対して同意を与える場合、一般にオプトインかオプトアウト（Opt-out）かの 2 つの同意方式が存在する。オプトアウトは、本人が個人データの取扱いを拒絶する意思表示をした場合にそのデータの取扱いを停止する仕組みのことを指す。この場合、「データ管理者及び処理者に対して個人データを取り扱うためにその許諾を得るような責任を課すというよりも、個人がその許諾を積極的に撤回しなければならないような責任を課すことになる」(49)。これに対してオプトインは、個人データの取扱いに当たってデータ主体の事前の明示的な同意を得なければならない仕組みのことを指し、この場合データ管理者は、取り扱うデータの対象やその利用目的を説明した上でデータ主体の同意を得なければならない。

このように述べた上で、リンスキー氏は、EU のデータ保護法制においてオプトイン方式が原則規定として保障されるに至った沿革に触れつつ、同方式が自己情報のコントロールや自己決定と深く結び付いてきたと主張している。もっとも、同氏の説明では、法制の沿革が詳細に分析されておらず、非ヨーロッパ圏の読者にとっては必ずしも十分な説明とは言えない。そこで以下では、同氏の説明を補足しながら、オプトインに関する法令の変遷を概観しておく。

まず、1995 年のデータ保護指令第 7 条 (a) は、データ取扱いの適法性要件の 1 つとして「データ主体が明確に同意を与えた場合」を定めており、かつ、同指令第 2 条 (h) は、有効な同意の条件として「自由になされた特定のかつ十分に情報を提供された上での意思表示」であることを要すると規定していた。ただし、データ保護指令では、オプトインとオプトアウトのいずれが採用されるべきなのかについて明示的な規定が置かれておらず、同意が要請されるタイミングについて統一的なルールは確立されていなかった。この点、データ主体の同意について大きな転換点となったのは、2009 年に改正された e プライバシー指令（ePrivacy Directive）(50)である。

---

(45) 忘れられる権利とは、「名誉毀損、プライバシー侵害、侮辱に該当する情報について、人格権に基づく個人情報の削除請求」を行う権利の一種であり、特に「インターネット上の情報検索に不可欠なインフラとなった検索サービスとの関連で、検索結果の削除」を求める文脈で議論されている権利である（宇賀克也「「忘れられる権利」について―検索サービス事業者の削除義務に焦点を当てて―」『論究ジュリスト』18 号, 2016.夏, p.24.）。EU では、データ主体の削除権（データ保護指令第 12 条。現行法では GDPR 第 17 条）等を根拠に、自己に関する情報（過去の知られたくない前歴など）を検索エンジン事業者に対して削除するよう求めることができる場合がある。裁判例の検討を含めて、石井夏生利「「忘れられる権利」をめぐる論議の意義」『情報管理』58 巻 4 号, 2015.7, pp.271-285 を参照。

(46) データ主体は、一定の条件の下で、「自己が管理者に対して提供した自己と関係する個人データを、構造化され、一般的に利用され機械可読性のある形式で受け取る権利をもち、また、その個人データの提供を受けた管理者から妨げられることなく、別の管理者に対し、それらの個人データを移行する権利を有する。」（GDPR 第 20 条。個人情報保護委員会訳　前掲注(5), p.25.）

(47) Lynskey, *op.cit.*(13), p.186.

(48) *ibid*., p.187.

(49) *ibid*.

(50) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and

同指令第 5 条第 3 項では、事業者がクッキー(51)等を通じてユーザーの閲覧履歴等の情報を端末機器に保存しアクセスするためには、ユーザーが「明瞭で理解しやすい情報を提供された上で、同意したことを条件」とすることが明記された。「この改正の結果、個人がインターネットを閲覧していたという個人データは、その個人の明確な同意がある場合についてのみクッキーを通じて収集できるようになった」(52)。

次に、同意に関する 2011 年の第 29 条作業部会の見解では、オプトイン方式がデータ保護指令の要請であると説明されている。この見解によれば、e プライバシー指令第 5 条第 3 項は、データ保護指令に沿ったものであり、e プライバシー指令によってクッキー規制について「同意がデータ取扱いの前に提示されなければならない」ものとされた(53)。さらに同様の原理は、一般条項であるデータ保護指令についても当てはまるものと解釈され、「一般的なルールとしてデータ取扱いの開始前に同意が与えられなければならない」と述べられている(54)。同ガイドラインによれば、「同意の観念は伝統的に、データ主体が自己のデータの利用をコントロールの下に置かなければならないという考えと結び付いており、基本権の観点から見て、同意を通じたコントロールは重要な基本理念（important concept）である」(55)とされ、事前の同意は、コントロール権という理念に最も適合的な仕組みであるとされる。

もっとも、2011 年の第 29 条作業部会のガイドラインも述べているように「同意を要求するタイミングはデータ保護指令の中で明記されているわけではない」(56)。これに対して 2016 年に制定された GDPR は、「同意の観念がオプトインを要請していることを明確にしている」(57)。GDPR は前身のデータ保護指令と同様、データ主体の同意をデータ取扱いの適法性要件の 1 つとして位置付けているが、有効な同意が成立するための条件として次のような定義規定を創設している。GDPR 第 4 条第 11 項は、「データ主体の「同意」とは、自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではないデータ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するものを意味する。」（下線部筆者。この部分が新設された文言である。）と規定している。この規定について、2020 年の欧州データ保護会議（European Data Protection Board）のガイドラインは、従前の第 29 条作業部会の見解を踏襲しこれを明文化した規定であると説明した上で、「同意は、それが必要とされる個人データの取扱いをデータ管理者が開始する前に、常に管理者により取得されなければならない」(58)と述べている。

Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 2009.12.18, pp.11-36. EUR-Lex Website <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0136>

(51) クッキー（cookie）とは、「ユーザーが Web サイト閲覧中に入力した値などを、Web サイト側からユーザーのブラウザに一時的に保存する仕組み」であり、そこで保存される情報は、「ログイン情報、サイトの訪問履歴、オンラインショッピングのカートの中身など」である（草野俊彦『見るだけ IT 用語図鑑 278―新入社員、IT に苦手意識を持っている人にも役立つ―』SB クリエイティブ, 2021, p.228.）。

(52) Lynskey, *op.cit.*(13), p.188.

(53) Article 29 Data Protection Working Party,“Opinion 15/2011 on the Definition of Consent,”WP 187, 2011.7.13, p.30.

(54) *ibid*., p.9.

(55) *ibid*., p.8.

(56) *ibid*., p.9.

(57) Lynskey, *op.cit.*(13), p.214.

(58) European Data Protection Board,“Guidelines 05/2020 on consent under Regulation 2016/679,”Version 1.1, 2020.5.13, p.20. 翻訳として、個人情報保護委員会訳『仮日本語訳　規則 2016/679 に基づく同意に関するガイドライン』p.45. <https://www.ppc.go.jp/files/pdf/doui_guideline_v1.1_koushin.pdf> を参照。

（ii）情報の非対称性の縮減

次にデータ保護法制の 2 つ目の特質である、情報の非対称性の縮減という要素を取り上げる。ここでリンスキー氏が問題視している情報の非対称性とは、一般的には「一方の当事者が他方の当事者よりも多くの情報を取り扱っている状況」[59]のことを指し、具体的には、大量の個人データが、データ主体の目の届かない状況の中で、事業者によって集積・解析・利用されている状態を指している。こうした非対称性は、個人の自律に対して次のような悪影響を及ぼすとされる。第 1 に、「情報の非対称性がある場合、個人は、自らのデータが利用されることによって損害が生ずる可能性やその場合の害悪の重大さを認識評価することが困難であるため、個人データの取扱いを認めるべきかどうかについて十分な情報を得た上での選択を行うことが困難となる」[60]。第 2 に、「情報の非対称性の下では、データ取扱いに責任を負う主体を正確に突き止めることが困難であるため、個人は、データの利用の濫用が発生した場合にデータ処理者に対してアカウンタビリティを負わせることが難しくなる」[61]。第 3 に、「こうしたマジックミラー効果は、データをやり取りする関係性の中で個人の立場をぜい弱化し、系統的に個人を不利な立場へと追いやる」[62]。

このように情報の非対称性は、個人の側から見た場合に、個人データの取扱い状況を不透明なままにすることで、データ主体の自己決定や同意を無力化する。リンスキー氏によれば、GDPR はデータ管理者に利用目的等を開示・説明させることによって、情報の非対称性を縮減し、データ主体による主体的な権利行使を担保している[63]。ここで同氏は、同意に関する GDPR の規定を例として次のように説いている。

GDPR はオプトインの原則を規定していることに加えて、有効な同意が成立するための条件として、それが説明を受けた上でのものであることを要求している。この要件は、「データ主体に対し、簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式により、明確かつ平易な文言を用いて」情報提供を行うデータ管理者の義務（GDPR 第 12 条第 1 項）と密接に関連している。データ管理者がデータ主体に対して情報提供すべき内容は、主に①データ管理者の身元、②取扱いの目的、③取得利用されるデータの内容、④個人データの取扱いに自動化された意思決定が介在する場合にはその決定に含まれているロジック等である（GDPR 第 13 条等）。このようにデータ管理者は個人データを取得するに当たって「個人データがどのように利用されるのかについて重要な情報を開示」[64]しなければならず、データ管理者には取扱いの過程を透明化する義務が課せられている。2020 年の欧州データ保護会議のガイドラインでも指摘されているように、「同意の取得に先立ってデータ主体に情報を提供することは、データ主体による、情報に基づく意思決定を可能とし、何について承諾しているかを理解できるように…（中略）…するために不可欠である」[65]。リンスキー氏も同様に、GDPR は「データ管理者に対して、データ主体の諸権利を効果的なものにするような義務を課すことによって、デー

59　Lynskey, *op.cit.*(13), p.211.
60　Lynskey, *op.cit.*(42), pp.592-593.
61　Lynskey, *op.cit.*(13), p.212.
62　*ibid*.
63　リンスキー氏の論文執筆時には GDPR は草案段階であったが、引用されている草案の条文内容はその後正式に採択された GDPR の正文とほぼ同一内容である。そのため後述においては便宜上 GDPR と表記し、正文と草案の内容に異同がある場合にはその旨を特に注記する。
64　Lynskey, *op.cit.*(13), p.214. なお、GDPR で規定する「決定に含まれるロジックに関して意味のある情報」について考察しているものとして、山本　前掲注(4), pp.29-34 を参照。
65　個人情報保護委員会訳　前掲注(58), p.33; European Data Protection Board, *op.cit.*(58), p.15.

タ主体とデータ管理者との情報及び力の非対称性を適正化（adjust）している」[66]と述べている。

このようにリンスキー氏によれば、データ主体とデータ管理者の間にある情報の非対称性は、真意の同意や自己決定を阻害する要因として働くが、データ保護法制は、同意の真正性や自己決定の自律性を維持するためにデータ管理者に対して情報の開示・説明などの義務を課し、データ取扱いの透明性を促進することで情報の非対称性を縮減させている。

(3) 個人データ保護権の構造―2 本柱構造としてのデータ保護法制―

ヨーロッパのデータ保護法制は、私生活の秘匿を中核とする古典的プライバシーの保護を出発点としながらも、次第にそれだけにはとどまらない多様な憲法的価値（情報自己決定権、事業者のアカウンタビリティ、データ取扱いの公正性及びデュー・プロセス）を反映する形で発展してきた。基本権憲章はこうした法発展の歴史（「憲法化プロセス」）を背景に、古典的プライバシー権には還元し得ない諸々の法益を「個人データ保護権」として概括的に保障したものと考えられる。

本節では、個人データ保護権の内実を体系的に把握するために、デ・ヘルト氏及びグートヴィルト氏やリンスキー氏の学説を紹介してきた。これらの学説の共通点としては、憲法化のプロセスを踏まえた上で、プライバシー権と個人データ保護権の別個独立性を強調することが挙げられる。既に見たように、個人データ保護権ないしこれを具体化したデータ保護法制は、①データ主体が主体的に個人データをコントロールするための主観的権利（同意[67]、アクセス権など）を保障すると同時に、②そうした個人の権利行使を担保するためにデータ管理者に開示・説明義務を課している。実際、GDPR の前文第 11 項でも「個人データの実効的な保護は、データ主体の権利並びに個人データを取り扱う者及びその取扱いを決定する者の義務を強化」することに存すると述べられており、データ保護法制における 2 本柱の構造（データ主体の権利規定＋事業者の義務規定）が重視されている[68]。

5　憲法化プロセスとデジタル立憲主義

(1) デジタル立憲主義の背景事情

ここまで、デジタル立憲主義の背景事情を明らかにする趣旨で、EU のデータ保護法制の歴

66　Lynskey, *op.cit.*13, p.214.

67　もっとも GDPR は、個人データの取扱いの適法性を基礎付ける要件として同意以外の要素（例えば、生命に関する利益を保護する場合など）を規定している（第 6 条）。曽我部真裕京都大学教授も、「EU の一般データ保護規則（GDPR）を見ても、前文で「個人データに対するコントロール」の重要性を繰り返し強調しているにもかかわらず、本則では、同意以外の根拠に基づく個人データの取扱いを様々に認めています。つまり、実定法においては、同意不要な場合が、相当な範囲で認められており、自己情報コントロールのうち、自己決定・同意の要素は必ずしも貫徹されていないわけです。」と指摘している（「曽我部真裕＝山本龍彦　対談　自己情報コントロール権のゆくえ」山本龍彦『＜超個人主義＞の逆説―AI 社会への憲法的警句―』弘文堂, 2023, p.169. 関連して、曽我部真裕「憲法上のプライバシー権の構造について」毛利透編『講座　立憲主義と憲法学　第 3 巻　人権Ⅱ』信山社, 2022, pp.7-35; 音無　前掲注15）。この点に関連して、近年日本の憲法学で自己情報コントロール説が批判されている状況の中で、改めて同説の意義を強調するものとして、山本龍彦「自己情報コントロール権について」山本『同』pp.141-164.

68　この点に加えて、基本権憲章第 8 条第 3 項は、データ保護法の遵守状況を監督（control）するための独立機関の設置を定めており、この規定を受けて GDPR 第 6 章は、独立監督機関（independent supervisory authorities）の組織及び権限を規定している。なお、データ保護法の執行について独立の監督機関が要求される根拠としては、①データ保護法の執行に党派的判断が働く誘因が強いため、監督機関が政治的中立性を担保するために組織の独立性を確保する必要があること、②データ保護法の執行及び監督が「専門的で複雑・膨大である上に、個別の権利侵害が直接には認識され難いことから、それを一般の利害関係人が監督し、場合によっては法的救済に訴えることが困難である」こと、が指摘されている（西上治「行政の正統性をめぐる現代的諸問題（1）データ保護法上の監督機関の独立性と民主的正統性」『法律時報』91 巻 8 号, 2019.7, p.91.）。

史的沿革を紹介し、個人データ保護権の構造に関する学説状況を確認してきた。デジタル立憲主義の代表的論者であるデ･グレゴリオ氏も、デ･ヘルト氏及びグートヴィルト氏やリンスキー氏の先行業績に依拠しながら、ヨーロッパのデータ保護法制が、「個人の基本権保障をデータ保護法の指針として位置付けてきた憲法化のプロセスの結果」[69]であったと指摘しており、データ保護法制の歴史的沿革を踏まえた議論を展開している。同氏によれば、EU のデータ保護法制は、「基本権、特に人間の尊厳、比例原則を通じた利益衡量、デュー･プロセス」[70]といった憲法的価値を根拠としながら、個人の自律や情報自己決定権を確保するための諸権利をデータ主体に対して保障し、その一方で事業者に対して「透明性やアカウンタビリティを高めるような手続的な予防策」[71]を義務付けている。

(2) 解釈及び立法指針としてのデジタル立憲主義

このようにデジタル立憲主義の論者は、データ保護法制が憲法具体化立法として形成されてきた歴史に注意を促しているが、このことは、「GDPR を憲法に即して解釈すること（constitutional-oriented interpretation）」[72]や立法論と結び付けて論じられている。つまり、デジタル立憲主義の論者は、データ保護法制が憲法具体化立法として位置付けられてきた点に注目した上で、立法目的である憲法的価値に留意しながら、データ保護法制の解釈論や立法論を展開している。

その際に主に議論されているのは、GDPR のプロファイリング規制と AI 規則案の AI 規制である。次章で検討するように、GDPR や AI 規則案では、プロファイリング技術や AI の進展を背景に、それによって生ずる新しい憲法的課題に対応する規定が設けられており、データ保護法制の憲法化プロセスが継続的に進行している。

Ⅱ　AI 規制の憲法的ガバナンス―GDPR と AI 規則案―

本章では、デジタル立憲主義の議論においてプロファイリング規制や AI 規制がどのように位置付けられているのかを分析する。まず、GDPR におけるプロファイリング規制の趣旨と内容を概観し、プロファイリング規制の憲法的意義を明らかにする（後述本章第 1 節及び第 2 節）。次いで、GDPR のプロファイリング規制と AI 規則案の AI 規制を比較検討し、両者の規制枠組みの中に憲法的価値がどのように組み込まれているのかを分析する（後述本章第 3 節）。

1　GDPR におけるプロファイリング規制

プロファイリングは、「自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好（しこう）、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、

---

[69] De Gregorio, *op.cit.*[12], p.271. なお、憲法化とデジタル立憲主義は次のように区別して論じられることがある。憲法化とは、デジタル空間を憲法的価値に即して設計していくプロセスの実態を指す言葉であるのに対して、デジタル立憲主義とは、そうしたプロセスを支える規範的価値理念それ自体を指す言葉とされる。すなわち、「憲法化は立憲主義の価値を実装するものであるのに対して、立憲主義は、憲法化に内在しつつ、その発展を指導し、これを特徴付けるような原理を供給する」。（Edoardo Celeste, *Digital Constitutionalism*, London: Routledge, 2022, p.78.）

[70] De Gregorio, *ibid*., p.272.

[71] *ibid*., p.218.

[72] *ibid*., p.255.

あらゆる形式の、個人データの自動的な取扱い」のことを指す（GDPR 第 4 条 (4)）[73]。近年では AI の技術革新を背景にプロファイリング技術の予測の精度が高まり[74]、「保険・雇用（人事）・教育・ローンなど、我々の人生における重要な場面でもプロファイリングが用いられるようになってきている」[75]。こうした状況を受けて EU では、プロファイリング等を用いたビッグデータの活用によって「個人の尊厳並びにプライバシー権を含む個人の権利及び自由に対する潜在的な影響」[76]が生じ得ることが懸念され、GDPR において一連のプロファイリング規制が創設された。以下では、第 29 条作業部会が採択した GDPR のガイドライン（以下「GDPR ガイドライン」）[77]を参考にしながら、プロファイリング規制の趣旨と内容を概説する。

(1) プロファイリングに対するチェック及び異議申立ての権利

GDPR は、データ主体に対して「異議を唱える権利（利用停止請求権）」（第 21 条）や「自動化された取扱いのみに基づき重要な決定を下されない権利」（第 22 条）を保障している[78]。まず前者の権利は、プロファイリングを含め、第 6 条第 1 項 (e) 又は (f)[79]に基づく個人データの取扱いに対して異議を述べることができるものである（第 21 条第 1 項）。データ主体がこの権利を行使した場合、データ管理者がやむを得ない正当な理由を示さない限り、当該自動化された取扱いを中止しなければならない。加えて同条第 2 項及び第 3 項は、個人データがダイレクトマーケティングの目的で取り扱われている場合に、データ主体はその取扱いに異議を述べる権利を有すると規定しており、異議が述べられた場合には、その取扱いを中止しなければならないと定めている。

これに対して後者の「自動化された取扱いのみに基づき重要な決定を下されない権利」は、データ主体に対して重大な影響を及ぼす「専ら自動化された取扱いに基づく決定」[80]について、

⑺ 個人情報保護委員会訳　前掲注⑸, p.3.

⑺ GDPR がプロファイリング規制を強化した背景には、AI の技術革新が進んだことによってプロファイリングの精度が高まり、その結果、与信や雇用など様々な場面でプロファイリングが活用されるようになったことが関係している。例えば、第 29 条作業部会が採択した GDPR のガイドラインは、「ビッグデータ解析、AI、機械学習の技術と能力の進歩は、プロファイルの作成と自動化された意思決定を容易にし、個人の権利と自由に大きな影響を与える可能性を有している」と指摘し、プロファイリング規制を強化した理由を、AI の技術革新と結び付けて説明している（Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679," WP 251 rev.0.1, 2018.2.6, p.6. 翻訳として、個人情報保護委員会訳『仮日本語訳　自動化された個人に対する意思決定とプロファイリングに関するガイドライン』p.6. <https://www.ppc.go.jp/files/pdf/profiling_guideline.pdf> を参照）。

⑺ 山本　前掲注⑸, p.263.

⑺ European Data Protection Supervisor, "Opinion 7/2015: Meeting the Challenges of Big Data: A call for transparency, user control, data protection by design and accountability," 2015.11.19, p.7.

⑺ 個人情報保護委員会訳　前掲注⑺; Article 29 Data Protection Working Party, *op.cit.*⑺を参照。

⑺ 両権利を解説する文献として、山本　前掲注⑸, pp.257-277; 石井夏生利『EU データ保護法』勁草書房, 2020, pp.87-96. なお山本龍彦教授は、第 21 条の権利を「異議を唱える権利（中止請求権）」、第 22 条の権利を「自動処理のみに基づき重要な決定を下されない権利」と表記している（山本龍彦「AI と個人の尊重、プライバシー」同編著『AI と憲法』日本経済新聞出版社, 2018, pp.100-105.）。

⑺ GDPR 第 6 条第 1 項は適法な取扱いの条件を列挙している。そのうち (e) は、「公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合」、(f) は、「管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合」である（個人情報保護委員会訳　前掲注⑸, p.9.）。

⑻ 第 22 条の適用対象は、「専ら自動化された取扱いに基づく決定」（下線部筆者）に限定される。GDPR のガイドラインによれば、この「専ら」という語句は、「決定プロセスにおいて人的介入がないことを意味している。管理者は、人間の関与があると装ったとしても、第 22 条の規定を回避できるわけではない。例えば、ある者が自動的に作成されたプロファイルを、結果に対して実際上の影響をもたらさずに、個人に対して日常的に適用し

その決定の対象とされない権利（right not to be subject to a decision based solely on automated processing）である（第 22 条第 1 項）。ただし、①契約の締結又は履行に必要な場合、②データ管理者がそれに服し、かつ、データ主体の権利及び自由並びに正当な利益の安全性を確保するための適切な措置も定める EU 法又は加盟国の国内法によって認められる場合、③データ主体の明示的な同意に基づく場合には、同項の規定は適用されない（同条第 2 項）。もっとも、①及び③の場合については、第 1 項の権利規定が適用されない場合であっても、データ管理者は、「データ主体の権利及び自由並びに正当な利益、少なくとも、管理者の側での人間の関与を得る権利（right to obtain human intervention）、データ主体の見解を表明する権利及び当該決定を争う権利（right to contest）の保護を確保するための適切な措置（suitable measures to safeguard）を実装」しなければならない（同条第 3 項）。

プロファイリングに対するチェック及び異議申立ての権利が規定された趣旨について、GDPR ガイドラインは、プロファイリングに伴う過誤（errors）とバイアス（bias）によって「個人の権利及び自由に大きな影響を与える可能性」(81)を指摘している。具体的には、まず、「もし自動化された意思決定又はプロファイリングのプロセスで使用されるデータが不正確であれば、そこから得られた意思決定やプロファイルは欠陥を持つものとなる。意思決定が、更新されていないデータ、又は外部データの不正確な解釈に基づいて行われるかもしれない。不正確であることは、例えば、誰かの医療、信用又は保険に関わるリスクについての不適切な予測や記述につながるかもしれない」(82)とされ、不正確な予測評価によって個人が重大な不利益を被るリスクが指摘されている。また GDPR ガイドラインでは、「生データが正確に記録されていたとしても、データセットは十分に代表的でないかもしれず、また解析には隠れたバイアスが含まれているかもしれない」とされ、特に「これまでのステレオタイプや社会的差別」が含まれている可能性があると指摘されている(83)。

こうして見ると、GDPR 第 21 条、第 22 条第 1 項及び同条第 3 項は、プロファイリングに伴う過誤や差別的バイアスを規制するために、データ主体に対して、自動化された取扱いに対するチェック及び異議申立ての機会を保障したものと考えられる。つまり、第 21 条は、同条所定の場合につき、プロファイリングを含む個人データの取扱いに対して異議を唱えてその利用を停止することを請求する権利を保障しており、また、第 22 条第 1 項は、専ら自動化された取扱いに基づき重要な決定を下されない権利を保障することで、人間の介入（チェック）によっ

ているならば、それは既に専ら自動化された取扱いに基づく意思決定となる。人間の関与があると資格づけるには、管理者は、決定の監督が形式的なものではなく、意味のあるものであることを確保しなければならない。」（個人情報保護委員会訳　前掲注(74), p.38; Article 29 Data Protection Working Party, *op.cit*.(74), pp.20-21.）

(81)　同上, pp.53, 6; *ibid*., pp.27, 5.

(82)　同上, p.20; *ibid*., p.12. プロファイリングの精度に関連する問題として、過少代表又は過剰代表の問題が指摘されることがある。過少代表又は過剰代表の問題とは、プロファイリングの基になるデータセットに偏りがあるため、そのプロファイリングの精度が低下している状態のことを指し、「たとえば、放漫な食生活を送る者たちが、自身のスコア低下を懸念して飲食記録の提供をしないことで、分析対象となるデータに占める生活習慣病予備軍の割合が実際よりも低下し、判断・決定に影響を与えることなどをいう」。（パーソナルデータ＋α研究会「プロファイリングに関する最終提言案」『NBL』1211 号, 2022.2.1, p.14.）

(83)　個人情報保護委員会訳　前掲注(74), pp.20, 7; *ibid*., pp.12, 5. 例えば、履歴書を審査して応募者をランク付けするシステムで、過去に提出された 10 年間分の履歴書を学習対象としていたところ、技術者は男性からの応募が多数であったため、男性を採用することが望ましいと認識され、履歴書に女性に関する単語（例えば「女性チェス部の部長」）が含まれていると評価が下がる傾向が見られたという事例が報じられている。Jeffrey Dastin「焦点：アマゾンが AI 採用打ち切り、「女性差別」の欠陥露呈で」2018.10.14. ロイターウェブサイト <https://jp.reuters.com/article/amazon-jobs-ai-analysis-idJPKCN1ML0DN> を参照。

て過誤の訂正を求める機会を担保している。次に同条第 3 項は、専ら自動化された取扱いに基づく重要な決定が認められる場合について、当該決定に異議を唱えて争い（challenge）、人間の関与（チェック）を求める権利をデータ主体に保障している(84)。

(2) 透明性の原則

プロファイリングに対するチェック及び異議申立ての権利が的確に行使されるためには、その前提として、データ主体自身がプロファイリングの運用状況（不利益措置の可能性など）を十分に把握している必要がある。GDPR ガイドラインでも、「データ主体は、決定がどのように行われまた何に基づいているかを十分に理解できる場合にのみ、決定に異議を唱え又はその意見を表明できる」(85)と指摘されている。

もっとも、プロファイリングで用いられる AI のアルゴリズムは、大量の学習データの中から統計的に相関関係を検出する点に特徴があり、その複雑な処理過程は人間の知能や直観では捉え難い（AI のブラックボックス問題）(86)。GDPR ガイドラインでも「機械学習の発展と複雑性は、自動化された意思決定プロセス又はプロファイリングがどのように機能するかについての理解を難しくするかもしれない」(87)と指摘されており、プロファイリングの不透明性について懸念が表明されている。

GDPR はプロファイリングの不透明性の問題に対処するために、データ管理者の通知義務を定めている。データ管理者は、①プロファイリングを含めた専ら自動化された意思決定を用いている場合にはその旨の告知をすることはもちろん、②当該決定の「ロジックに関する意味のある情報」、③「当該取扱いのデータ主体への重大性及びデータ主体に及ぼすと想定される帰結」をデータ主体に告知しなければならない（第 13 条第 2 項 (f)）。

この点、GDPR ガイドラインは、「提供される情報は、データ主体にとって意味のあるものでなければならない」と述べ、「管理者は、アルゴリズムの複雑な説明又はアルゴリズムの全ての開示ではなく、データ主体に対して、背景にある論拠、又は決定に至る際に依拠する基準について説明するシンプルな方法を見いだすべきである」と指摘している(88)。

プロファイリングのロジックに係る説明義務の範囲については、現状確立した運用が定着しているわけではなく、学説でも争いがある(89)。もっとも、これらの中では、GDPR ガイドラインの見解と同様、「提供される情報は、データ主体にとって意味のあるものでなければならない」点を強調する学説が注目される。例えば、アンドリュー・セルブスト（Andrew D. Selbst）氏（カリフォルニア大学ロサンゼルス校ロー・スクール）及びジュリア・パウルズ（Julia Powles）氏（西オーストラリア大学）は、「提供される情報が意味のあるものであるかどうか

---

(84) GDPR 前文第 71 項参照。

(85) 個人情報保護委員会訳　前掲注(74), p.53; Article 29 Data Protection Working Party, *op.cit*.(74), p.27.

(86) Andrew D. Selbst and Solon Barocas, "The Intuitive Appeal of Explainable Machines," *Fordham Law Review*, Vol.87 Iss.3, 2018, pp.1085-1139.

(87) 個人情報保護委員会訳　前掲注(74), p.48; Article 29 Data Protection Working Party, *op.cit*.(74), p.25.

(88) 同上; *ibid*.

(89) Sandra Wachter et al., "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law*, Vol.7 Iss.2, 2017.5, pp.76-99 は、事業者の営業の秘密を保全する観点から、GDPR の説明義務の範囲を限定的に解釈すべきだと主張している。著者によれば、データ管理者の説明義務の範囲は、アルゴリズムの一般的な作動法則に限定して解釈されるべきであり、各個人の状況に即した個別具体的な説明は要求されないものと解される。

のテストは、その説明によって初めてデータ主体が実行に移すことができる一定の措置、例えば、GDPR 第 22 条第 3 項における決定に異議を唱え争う権利のような措置との連動性に即して、機能的に理解されなければならない」[90]と指摘している。両氏によれば、「提供される情報は少なくとも、GDPR や人権法規で保障された権利をデータ主体が行使できる程度に意味のあるものでなければならない。一例を挙げると、ある者が自動化された決定の説明を受ける場合、その者は、裁判で差別の主張が行い得るかどうかを判定できるようにその決定を理解する必要がある。こうした解釈は、データの取扱いが合法かつ公正であり、データ主体にとって透明性がなければならないとする GDPR 第 5 条の要件や、理解可能性を重視し、かつ、管理者がデータ主体の権利行使を容易にしなければならないとする GDPR 第 12 条の要件によって支えられている」[91]とされる。

このように、GDPR ガイドラインや学説の見解に照らして見ると、GDPR がプロファイリングのロジックに関してデータ管理者に開示及び説明の義務を課している趣旨は、プロファイリングのプロセスを透明化することで差別的意図やその効果がないかを可視化し、違法なデータの取扱いをあぶり出すことで（違法であれば裁判で是正が命じられる）、データ主体の権利行使の機会を保全する点にあるものと解される。

(3) リスク逓減義務を支えるガバナンス規律

GDPR は、プロファイリングに対するチェック及び異議申立ての権利を保障するだけではなく、アルゴリズムを開発・実装する初期段階からデータ管理者にリスク評価を遂行させ、差別や権利侵害を未然に防止するためのガバナンス体制を構築するようにデータ管理者に義務付けている[92]。GDPR ガイドラインによれば、以下で紹介する条文を念頭に、GDPR は、「プロファイリングのプロセスにおける公正性、非差別性、正確性を確保するための保護措置」[93]を実装することをデータ管理者に要請し、データ管理者のアカウンタビリティを強化するものとされる。

まず、GDPR 第 25 条は、データ保護バイデザイン及びデータ保護バイデフォルト（data protection by design and by default）の原則を定めている。すなわち、同条第 1 項によれば、データ管理者は、データ主体に対する「権利及び自由に対する様々な蓋然性と深刻度のリスクを考慮に入れた上で」、「本規則の要件を満たすものとし、かつ、データ主体の権利を保護するため、取扱いの方法を決定する時点及び取扱いそれ自体の時点の両時点において、データの最小化のような個人データ保護の基本原則を効果的な態様で実装し、その取扱いの中に必要な保護措置を統合するために設計された、仮名化のような、適切な技術的及び組織的措置（appropriate technical and organisational measures）を実装」しなければならない[94]。

GDPR 第 35 条第 1 項は、「自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合」について、データ管理者に対してデータ保護影響評価（data protection impact

---

⑼⓪ Andrew D. Selbst and Julia Powles, “Meaningful Information and the Right to Explanation,” *International Data Privacy Law*, Vol.7 Iss.4, 2017.11, p.236.

⑼① *ibid*.

⑼② GDPR のプロファイリング規制をガバナンス規律と結び付けて理解する視座を提示する文献として以下を参照。Margot E. Kaminski, “Binary Governance: Lessons from the GDPR’s Approach to Algorithmic Accountability,” *Southern California Law Review*, Vol.92, 2019, pp.1529-1616; Margot E. Kaminski and Gianclaudio Malgieri, “Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations,” *International Data Privacy Law*, Vol.11 Iss.2, 2021.4, pp.125-144.

⑼③ 個人情報保護委員会訳　前掲注⑺④, p.26; Article 29 Data Protection Working Party, *op.cit*.⑺④, p.14.

⑼④ 個人情報保護委員会訳　前掲注⑸, p.30.

assessment）の作成を義務付けている。さらに同条第 3 項 (a) は、「プロファイリングを含め、自動的な取扱いに基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を発生させ、又は、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面の体系的かつ広範囲な評価の場合」には、データ保護影響評価の作成が特に求められると定めている(95)。

また、データ管理者によるリスク逓減の取組を外部から監督するための仕組みとして、GDPR 第 51 条は、各加盟国に監督機関の設置を義務付けている。さらにデータ管理者は、データ保護のための適切な技術的及び組織的措置を適切に実装していることを証明するための手段として、GDPR 第 42 条に規定する認証制度(96)を利用することができるとされており、この認証制度によって、データ管理者が積極的にリスク逓減に取り組むためのインセンティブの創出が企図されている(97)。

このように、GDPR では、データ管理者に対してリスク逓減のための取組を義務付ける一連の仕組みが導入されている。

(4) 小括

ここまで見てきたように、GDPR のプロファイリング規制は、①プロファイリングに対するチェック及び異議申立ての権利、②透明性の原則、③リスク逓減義務を支えるガバナンス規律の 3 点によって構成されている。まず GDPR は、プロファイリングに伴う過誤やバイアスを是正するために、データ主体に対してチェック及び異議申立ての権利を保障している。さらに GDPR は、プロファイリングのロジック等をデータ主体に対して開示及び説明する義務をデータ管理者に課している。この規定は、プロファイリングのプロセスを透明化することで差別的意図やその効果がないかを可視化させ、違法なデータの取扱いをあぶり出す機能を持っている。これに加えて GDPR は、プロファイリングによって差別や権利侵害のリスクが発生し得ることを念頭に、データ管理者に対してあらかじめ内発的にリスク逓減に取り組むように義務付けている。具体的にはデータ保護影響評価の作成を義務付けるなどして、データ管理者が事前にリスク逓減に取り組むように求めている。

次節では、これらのプロファイリング規制が、デジタル立憲主義の議論においてどのように位置付けられているのかを分析し、プロファイリング規制の憲法的意義を明らかにする。

2 デジタル立憲主義におけるプロファイリング規制の位置付け

(1) プロファイリング規制と憲法的価値との関係

デジタル立憲主義を主張する論者は、プロファイリング規制の憲法的意義を明らかにすることを通じて、「自動化された意思決定システムを規制する規範の解釈やその将来の発展を指導する基本原則を提示」(98)しようと試みている。例えばセレステ氏及びデ・グレゴリオ氏は、「自動化された意思決定に関する GDPR の枠組みは、一連の基軸となる憲法的価値を維持発展させること、つまり、人間の自律性を維持し、法的確証度を高め、手続的な予防策を与えること

---

(95) 同上, p.40.

(96) 「加盟国、監督機関、欧州データ保護会議及び欧州委員会は、とりわけ、EU レベルにおいて、管理者及び処理者による取扱業務が本規則を遵守することを証明する目的のために、データ保護認証方法、データ保護シール及びデータ保護マークを設けることを奨励しなければならない。」（GDPR 第 42 条第 1 項。同上, p.50.）

(97) 山本　前掲注(4), pp.39-41.

(98) Celeste and De Gregorio, *op.cit.*(11), p.11.

を目指している」[99]と述べ、「自動化された意思決定に関する GDPR の枠組みは、人間の尊厳やデュー・プロセス、法の支配のような憲法的価値と深く結び付いている」[100]と指摘している。以下、両氏の指摘に基づき、プロファイリング規制と憲法的価値との関係性を、具体的に説明する。

（ⅰ）人間の尊厳・平等（人間中心のデジタル化）

AI の技術革新が進展し、量刑判断や与信の決定など多種広範な領域で AI を用いた決定（予測及び評価）の実装が見込まれている。AI による自動化された意思決定は、膨大なデータを迅速かつ一律に処理することができる点で人間よりも効率的であると見られている。しかし、AI などのマシーンも誤り得るのであり、また、AI のアルゴリズムにも差別的バイアスが含まれている可能性がある。そうした過誤や差別のリスクは、人間の尊厳（個人の自律）や平等といった憲法的観点から問題になる[101]。そのため GDPR 第 22 条は、自動化された取扱いのみに基づいた決定を排除することで、人間の関与によって過誤を訂正する可能性を認めている。「第 22 条で規定された自動化された意思決定の禁止は…（中略）…マシーンやプログラマーによる盲目的な差別から免れる権利を反映している」[102]。

（ⅱ）法の支配、透明性、デュー・プロセス

自動化された意思決定が利用される場合についても、GDPR の下では、「全ての個人が、自動化された意思決定の恣意的な利用から保護されるべきだとし、国家に限らず、支配的影響力を持った全てのアクター、とりわけ強力な私企業も憲法的制約に服すべきだとしている」[103]。GDPR 第 13 条は、「自動化された意思決定のロジック」をデータ主体に対して開示・説明しなければならないと規定し、第 15 条は、データ主体のアクセス権を定めている。この規定により「データ管理者は、自動化された意思決定の有無を開示し、そのプロセスに含まれるロジックを説明する義務を負っている」[104]。このことは、個人とデータ管理者との間の「情報の非対称性を均整化し」[105]、データの取扱いの過程を透明化する憲法的意義を持つ。

これに加えて GDPR 第 22 条第 3 項は、専ら自動化された意思決定が適法に適用される場合についても、データ管理者の側での人間の関与を得る権利や、データ主体の見解を表明する権利及び当該決定を争う権利がデータ主体に保障されるべきことを規定している。この規定は、AI などの自動的決定に対するチェック及び異議申立ての機会を保障することで、個人のデュー・プロセスを保障する意義を持っている。

(2) リスク逓減義務を支えるガバナンス規律

デジタル立憲主義の論者であるデ・グレゴリオ氏は、GDPR のプロファイリング規制が、人間の尊厳やデュー・プロセスなどの憲法的価値を促進するための規定として位置付けられている点を踏まえて、「個人データ保護の憲法化の針路（constitutional path）は、…（中略）…

---

(99) *ibid*., p.5.
(100) *ibid*., p.17.
(101) *ibid*., pp.12-14.
(102) *ibid*., pp.13-14.
(103) *ibid*., p.16.
(104) *ibid*., p.15.
(105) *ibid*.

GDPR の登場によって新たな水準に到達している」[106]と指摘している。

もっともデ・グレゴリオ氏は、自動化された意思決定に関する実体規定（権利規定）が新設された点に注目するだけではなく、GDPR においてデータ管理者のリスク逓減義務が強化された点にも注目している。同氏によれば、AI などの自動的決定に対するチェック及び異議申立ての権利の保障（デュー・プロセス）は、データ管理者のリスク逓減義務の規定（GDPR 第 25 条及び第 35 条）と結び付いており、これらの規定によって、AI による権利侵害のリスクを事前に予防するためのガバナンス体制の構築が義務付けられている（本章第 1 節第 3 項参照）[107]。

(3) 小括―解釈論から立法論へ―

デジタル立憲主義は、プロファイリング規制の憲法的意義[108]に注目することで、プロファイリング規制の趣旨や目的を明らかにし、その解釈指針を明示しようと試みている。もっとも、デジタル立憲主義を提唱する論者は、GDPR の解釈論だけではなく、データ保護法制の立法指針も提示しようと試みている。デジタル立憲主義の論者が強調するように、EU のデジタル戦略は基本権憲章に定められた憲法的価値に沿って展開されており、その場合デジタル立憲主義の理念は、憲法的価値に即した法発展を促す原動力として機能している（後述本章第 3 節参照）。

3　デジタル立憲主義と AI 規則案

デジタル立憲主義は、データ保護法制だけではなく、フェイクニュース対策[109]や AI 規制などの EU のデジタル戦略全般を対象としている。そこで本節では、デジタル立憲主義の理念が、デジタル政策の基本指針となっている点を踏まえた上で、GDPR のプロファイリング規制が、AI 規則案によって補完及び強化されている側面を考察する。

(1) デジタル立憲主義とデジタル戦略

近年 EU では、基本権憲章の憲法的価値に即して新しいデジタル政策を立法化する動きが進んでいる[110]。デ・グレゴリオ氏及びピエトロ・ダン（Pietro Dunn）氏（ボローニャ大学）は、

---

[106] Giovanni De Gregorio, “The Rise of Digital Constitutionalism in the European Union,” *International Journal of Constitutional Law*, Vol.19 No.1, 2021.1, p.63.

[107] *ibid*., pp.63-66.

[108] 日本でも山本龍彦教授が、憲法論の観点からプロファイリング規制の必要性を指摘している（比較的最近の著作として、山本龍彦・プラットフォームビジネス研究会「AI と憲法（上）アルゴリズム、プライバシー、デモクラシー」『法律時報』94 巻 5 号, 2022.5, pp.94-102.）。特に日本国憲法第 13 条（個人の尊重）との関係で、同教授は、「個人が、自らの努力や真の能力、自らを取り巻く個別的・具体的状況にかかわらず、人工知能がはじきだした「確率」によって概括的・抽象的・事前的に判断され、人生の重要な機会を奪われ、自律的な生き方を妨げられる」危険性があると述べた上で、「自動化された（人工知能による）確率的な判断のみによって概括的・抽象的に個人を評価・決定することは、「個人の尊重」原理と鋭く矛盾してくるように思われる」と指摘し、GDPR を参考にしながら日本でもプロファイリング規制を導入すべきだと主張している（山本　前掲注[15], p.270.）。

[109] 近年の EU の取組については、南亮一「EU 域内の国民投票運動におけるオンライン広告規制の動向―政治広告の透明性の確保及び偽情報対策の観点から―」国立国会図書館調査及び立法考査局編『諸外国の国民投票運動におけるオンライン広告規制』（調査資料 2022-1-a 基本情報シリーズ 29）国立国会図書館, 2023, pp.129-159. <https://dl.ndl.go.jp/pid/12767880> を参照。

[110] 2023 年に欧州議会等は「デジタル時代におけるデジタル権とデジタル原則に関する欧州宣言」を公表している（European Parliament et al., “European Declaration on Digital Rights and Principles for the Digital Decade,” OJ C 23, 2023.1.23, pp.1-7. EUR-Lex Website <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001>）。宣言の前文では、「デジタル・トランスフォーメーションが人々の生活の全側面に影響を与える」ことを念頭に、EU のデジタル戦略（データ保護、AI 規制、フェイクニュース対策）が、基本権憲章の憲法原則に立脚しながら、「データ保護、差別の禁止、男女平等などの基本権、消費者保護、技術上及びネットワーク上の中立性、信頼性、

「ヨーロッパ的なデジタル立憲主義の視角は、EU のデジタル戦略の将来的発展を理解するための有益な視座を提供し、アルゴリズム社会の課題を憲法的に解決するための示唆を導くものである」(111)と述べ、デジタル立憲主義が、デジタル政策の原動力となっていると指摘している。

既に述べたように、GDPR は、基本権憲章第 8 条の個人データ保護権を強化する目的で制定されたものであり、特にプロファイリング対策が強化されている（本章第 1 節及び第 2 節参照）。GDPR では、「データ管理者及び処理者が個人データを取り扱う際にデータ主体へのリスクを算定するに当たって、基本権の重要性がリスク算定の指針となることが強調されており」、また、「（データ管理者の）アカウンタビリティや、プライバシー権や個人データ保護を水平関係（筆者注：私人間関係）にも拡張する原理が重視されている」(112)。以下で見る AI 規則案についても、基本権憲章の憲法的価値に沿った AI の利活用が目指されており、「憲法によって方向付けられた規制戦略」(113)が採用されている。

(2) AI 規則案の AI 規制

(ⅰ) AI 規則案の経緯

2021 年 4 月 21 日に欧州委員会が公表した AI 規則案は、2023 年 6 月 14 日に欧州議会（European Parliament）の本会議にて賛成多数で採択された(114)。AI 規則案に添付された説明文書（法案趣旨書）によると、包括的な AI 規制の制定を促す契機となったのは、「高リスクと判断されるべき AI アプリケーションを明確に定めることを求める」(115)一連の欧州理事会の勧告であった。そこでは、「基本権との適合性を確保しかつ法的ルールの執行を促進するために、一定の AI システムの不透明性、複雑性、バイアス、一定の予測不可能性及び不十分な自動的動作への対処」(116)が求められていた。

これらの勧告を受けて、AI 規則案は、「人々の健康及び安全又は基本権に対して重大なリスクを生じさせる『高リスク』AI システムを定義するために、リスクに関する確固たる方法論を定め」(117)、リスク逓減のための事業者の義務付けを強化している。以下では、GDPR と関連する部分(118)に限って AI 規則案の AI 規制を紹介する。具体的には、AI 規則案において憲法的

包摂性などの原則を完全に遵守すべきこと」を定めている（前文第 1 項及び第 4 項）。ヨーロッパの公法学説ではこの宣言が「デジタル立憲主義又はデジタル環境の憲法化プロセス」の一環として評価されている点につき、Cristina Cocito and Paul De Hert, “The transformative nature of the EU Declaration on Digital Rights and Principles: Replacing the old paradigm (normative equivalency of rights),” *Computer Law & Security Review*, Vol.50, 2023.9, p.4.

(111) Giovanni De Gregorio and Pietro Dunn, “The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age,” *Common Market Law Review*, Vol.59 No.2, 2022.4, p.500.

(112) *ibid*., p.498.

(113) *ibid*., p.478.

(114) “Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.” European Parliament Website <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html> 本章で紹介するデジタル立憲主義と AI 規則案を論じた論文では、欧州議会の修正案ではなく、欧州委員会の公表した原案を分析対象としているため、本稿でも、欧州委員会の原案を引用している。なお、EU 理事会と欧州議会は 2023 年 12 月 9 日、AI 規則案に関し、暫定合意に達したと公表した。“Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI,” 2023.12.9. European Parliament Website <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>

(115) 三部訳　前掲注(6), p.2; European Commission, *op.cit.*(6), p.2.

(116) 同上; *ibid*.

(117) 同上, p.4; *ibid*., p.3.

(118) AI 規則案の説明文書によると、AI 規則には「横断的な性質」があるとされる（同上, p.4; *ibid*., p.4.）。AI 規則

価値に準拠した規制枠組みが採用されている点を明らかにする。

（ii）AI 規則案の立法目的

AI 規則案に添付された説明文書は、AI 規則案の立法目的を次のように述べ、AI 規則案と憲法的価値との関係性を強調している。すなわち、「特定の特徴（例えば、不透明性、複雑さ、データへの依存、自動的動作など）を持った AI を利用することは、基本権憲章（「憲章」）に規定された多くの基本権に悪影響を及ぼし得る。…（中略）…本提案は、憲章によって保護される次の権利の保護を強化し及び促進する。その権利とは、人間の尊厳に係る権利（第 1 条）、私生活の尊重及び個人データの保護（第 7 条及び第 8 条）、非差別（第 21 条）、並びに女性と男性の平等（第 23 条）である。」(119)

このように、AI 規則案は基本権憲章の憲法的価値を具体化する立法として位置付けられているが、そうした特徴が最も顕著に現れているのが、以下で検討する高リスク AI システムに対する規制枠組みである。

（iii）高リスク AI システムの分類とその規制

AI 規則案は、基本権侵害のリスクの強弱に応じて、①「禁止される AI 実務」（第Ⅱ編）と②「高リスク AI システム」（第Ⅲ編）を類型化している。まず前者の禁止される AI 実務の一例を挙げると、AI 規則案第 5 条第 1 項 (a) は、「その者又は別の者に精神的な又は身体的な害を生じさせ又は生じさせるおそれのある態様でその者の行動を実質的にゆがめるために、その者の意識を超えたサブリミナルな技法(120)を展開する AI システムを市場に置き、サービスを提供し、又は利用すること」を禁止している。

他方、高リスク AI システムの分類及び定義については、AI 規則案附属書（以下「附属書」という。）(121)のうち、附属書Ⅲ等で分野ごとの分類が定義されている（AI 規則案第 6 条第 2 項）。以下、附属書Ⅲと前文の対応関係に注目しながら、高リスク AI システムが、憲法的価値を斟酌（しんしゃく）して分類及び定義されている点を明らかにする（AI 規則案前文第 13 項）。

まず附属書Ⅲ第 1 号は「自然人の生体識別及び分類」を伴うものを、高リスク AI システムとして定めている。この類型の AI は、「不正確な点があると、バイアスのある結果を招き、差別的な効果を生じさせる可能性がある。このことは、それが年齢、民族、性別又は障害に関す

案は、「基本権憲章、並びに個人データ保護、消費者保護、非差別及びジェンダー平等に関する既存の二次 EU 法令」との「整合性」を確保し、その上で「GDPR（規則 (EU) 2016/679）及び法執行指令（指令 (EU) 2016/680）」などの「規則及び指令を補完するもの」であり、それによって「一定の高リスク AI システムの設計、開発及び利用に適用される一連の調和の取れたルール、並びに遠隔生体識別システムの一定の利用に対する制約」を規定するものとされる（同, pp.4-5; *ibid.*）。

(119) 三部訳　前掲注(6), p.13; European Commission, *op.cit.*(6), p.11.

(120) サブリミナル知覚とは、閾下（いきか）知覚とも呼ばれ、「刺激閾あるいは認知閾以下の刺激量を持つ刺激（閾下刺激）により引き起こされる認知の変容の総和を総称」したものを指し、ここで認知閾（いき）とは、「その刺激が何かを正しく認知できる最小刺激量」のことを指す（子安増生ほか監修『現代心理学辞典』有斐閣, 2021, pp.23, 594.）。

(121) “ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS,” COM(2021) 206 final, 2021.4.21. EUR-Lex Website <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF> 翻訳については、三部訳　前掲注(6)を参照。

る場合には特に当てはまる」（AI 規則案前文第 33 項）[122]。

また、附属書Ⅲ第 4 号では、「雇用、労働者管理及び自営業へのアクセス」に用いられる AI であって、採用、昇進、契約関係の終了、業務の割当て、業績評価等に用いられるものを、高リスク AI システムと定めている。この類型の AI は、「将来のキャリアの見通し及び生活に大きな影響を与える可能性があるからであり」、特に「女性、特定の年齢層、障害者、特定の人種的若しくは民族的な出自の人々又は性的指向の人々に対する、差別の歴史的パターンを永続させる可能性がある。また、これらの人々のパフォーマンス及び行動をモニタリングするために利用される AI システムは、データ保護及びプライバシーに係るこれらの人々の権利に影響を与える可能性がある」（AI 規則案前文第 36 項）[123]。

さらに附属書Ⅲ第 5 号では、「重要な民間及び公共のサービス及び給付へのアクセス及びその享受」に関して用いられる AI であって、これらのサービスの受給資格等の審査及び受給者等の信用スコアや与信評価などに用いられるものを、高リスク AI システムと定めている。この類型の AI は、「人種的又は民族的な出自、障害、年齢、性的指向に基づく差別の歴史的パターンを永続させ、又は新たな形態の差別的な影響を生み出す可能性がある」。また、公的機関からのサービス提供の場合には、「社会的な保障、非差別、人間の尊厳又は実効的な救済を受ける権利などこれらの人々の基本権を侵害する可能性がある」（AI 規則案前文第 37 項）[124]。

このように高リスク AI システムの分類及び定義は、健康や安全といった要素だけではなく、非差別やプライバシー、人間の尊厳などの基本権に対する侵害リスクに応じて策定されており、リスク評価の基準の中に憲法的価値が組み込まれている[125]。

次に AI 規則案第Ⅲ編第 2 章は、高リスク AI システムが遵守すべき一連の要件を規定している。当該 AI システムを提供する事業者は、リスク管理システムの構築（第 9 条）、データガバナンスの確保（第 10 条）、同章で定められた要件を遵守していることを証明する技術文書の作成（第 11 条）、AI の動作を自動記録する機能の装備（第 12 条）、AI のアウトプットに関する透明性の確保及び利用者への情報提供（第 13 条）、人間による AI の監視体制を整備し、健康・安全・基本権に対するリスクを防止・最小化すること（第 14 条）、AI の正確性・堅ろう性及びサイバーセキュリティの確保（第 15 条）といった要件を遵守しなければならない。

AI 規則案では、高リスク AI システムを提供する事業者は、当該 AI システムの提供前に、上記要件に対する適合性評価（conformity assessment）手続を経ることを義務付けられている（第 19 条）。適合性評価手続とは、高リスク AI システムに関する AI 規則案第Ⅲ編第 2 章に定める要件が履行されたかを検証するプロセスのことをいう（第 3 条第 20 号）。事業者は、原則として自社内部で適合性評価手続を履践すべきものとされる（第 43 条第 1 項第 1 段落 (a)、同条第 2 項）。また、自社内部で当該手続を行うに当たっては、EU 官報で公表されている AI の整合規格又は欧州委員会の採用する共通仕様を適用していれば、同章に定める要件を遵守していることが推定される（第 40 条、第 41 条）。

このように、AI 規則案において、適合性評価手続は原則として自社内部で行われることが

---

[122] 同上, p.30.
[123] 同上, pp.30-31.
[124] 同上, p.31.
[125] AI 規則案添付の説明文書では、高リスク AI システムの分類を定める AI 規則案第Ⅲ編について、「基本権に対して高いリスクを生じさせる AI システムについての具体的ルールを定める」と説明している（同上, p.15; European Commission, *op.cit.*(6), p.13.）。

想定されている（附属書Ⅵに定める内部コントロールに基づく適合性評価手続）。ただし、整合規格又は共通仕様に準拠していない場合やその他の法令で特段の定めがある場合などについては、附属書Ⅶに定める、第三者認証機関（notified bodies）(126)の関与を伴う、品質管理システムの評価及び技術文書の評価に基づく適合性評価手続が履践されるべきものとされる（第 43 条第 1 項第 2 段落、同条第 3 項）。この場合第三者認証機関は、AI 規則案第Ⅲ編第 2 章に定める要件への適合性を検証・統制する権限を持つ（第 43 条第 3 項第 2 段落）。

（ⅳ）小括

AI 規則案は、プライバシーなどの基本権侵害のリスクの性質に即して高リスク AI システムの分類及び定義を行い、その上で、適合性評価手続を事業者に義務付けることでリスクを事前に逓減ないし軽減させる仕組みが採用されている。その意味で AI 規則案の AI 規制の仕組みは、憲法的価値に準拠した規制枠組み(127)であると言うことができる(128)。

(3) デジタル立憲主義における GDPR と AI 規則案の位置付け

第 1 節第 3 項及び第 4 項で見たように、GDPR は、プロファイリングによって差別やプライバシー侵害が発生し得ることを念頭に、事業者に対してリスク逓減のためのガバナンス規律を義務付けている。具体的には、プロファイリングのロジックを開示・説明させることで、基本権侵害リスクを可視化し、さらに、データ保護影響評価を事業者に義務付けることによって、事業者自身が早期に基本権侵害リスクを検出・発見できるように促している。

したがって、GDPR のプロファイリング規制と AI 規則案の AI 規制は、憲法的価値に準拠したリスク規制の仕組みを採用する点で同一の規律構造を備えている。しかし両者には差異もある。すなわち、AI 規則案は、GDPR に比べて、①リスクの分類及び定義を明確にするとともに②事業者に課すリスク逓減義務を強化し、事業者の裁量を縮減させている点で、GDPR を踏み越える内容を持っている。

まず、①のリスクの分類及び定義の明確化については、AI 規則案は、高リスク AI システムの分類及び定義を行うに当たって、基本権侵害リスクに留意しながら分野や場面ごとに具体的な分類方法を明文化しており、GDPR の包括的なプロファイリング規制に比べてリスクの定義が具体化ないし詳細化されている。次に②の事業者の義務規定については、AI 規則案は、適合性評価手続を導入することで事業者への規制を強化している。加えて、一定の場合には適合性評価手続に第三者認証機関が介在することで事業者に対するモニタリングが強化されてい

---

(126) 第三者認証機関は各国の認証実施機関（notifying authorities）によって認証され、AI システムの提供事業者からは独立して適合性評価の検証及び統制を行う（AI 規則案第 32 条、第 33 条）。

(127) AI 規則案に添付された説明文書は次のように説明している。「第Ⅲ編は、…（中略）…基本権に対して高いリスクを生じさせる AI システムについての具体的ルールを定める。これらの高リスク AI システムは、リスクベース・アプローチに即して、一定の強制的な要件の遵守及び事前の適合性評価手続を条件として、欧州市場に置くことが許容される」（三部訳　前掲注(6), p.15; European Commission, *op.cit.*(6), p.13.）。なお、データ保護法制の文脈におけるリスクベース・アプローチとは、リスクの程度に応じて規制の強度を設定する仕組みのことを指し（Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal Frameworks," WP 218, 2014.5.30; Raphaël Gallert, *The Risk-Based Approach to Data Protection*, Oxford: Oxford University Press, 2020 を参照）、AI 規則案では、許容できない AI、高リスク AI、限定リスク AI の 3 つの区分に応じた規制枠組みが定められている。

(128) 山本健人「EU の AI 規則案とデジタル立憲主義」『IFI Working Paper』13 号, 2023.2. <https://ifi.u-tokyo.ac.jp/wp/wp-content/uploads/2023/02/WP013.pdf> を参照。

る。また、自社内部で適合性評価手続が完結する場合においても、欧州委員会等の公的機関の発行する AI の統一規格（整合規格、共通仕様）への準拠を促すことによって、事業者に対する外部的統制を確保し、事業者のリスク逓減義務を強化している。

このような規律強化の方向性は、デジタル立憲主義の議論の中でも好意的に評価されている。例えばデ・グレゴリオ氏及びダン氏の共著論文では、GDPR がデータ管理者の自主的な取組に依拠したボトムアップ型のプロファイリング規制を採用しているのに対して、AI 規則案は、リスク評価の基準を明文化したトップダウン型の AI 規制を採用していると整理している(129)。すなわち、GDPR ではデータ保護影響評価の仕組みが導入され、「データ管理者は、個人データを取り扱う際にデータ主体の基本権に対するリスクの程度を正確に算定するように要請されており、その評価に基づいて適切なリスク逓減措置を講ずるように要請されていた」(130)ものの、GDPR には「リスクの閾値（いきち）（目安）それ自体は設けられておらず」、「データの取扱いが適法か違法かを判定する二者択一的な論理」は示されていない(131)。そのため GDPR の下で要請されるリスク評価の基準は、「規律密度の粗い、伸縮自在なもの（scalable）」(132)にならざるを得ず、その結果、事業者の裁量判断の余地は大きくなる。しかしリスク評価の基準が曖昧なままでは、「AI システムが本来的に不可解であり透明性を欠く一方、それが（しばしば）不正確で、バイアスを含み、差別的帰結をもたらし得る」(133)といった AI の本質的な問題に対処することはできない。そこで AI 規則案は、リスク評価のための判断基準として、許容できない AI システムの類型を明文化するとともに、「高リスクとされる AI システムの閾値（目安）」(134)を設定している。そうすることで事業者がリスク逓減措置に取り組む際の判断基準を法定化し、「AI システムの使用と機能を直接に規制している」(135)。

おわりに

本稿では、GDPR や AI 規則案を参考にしながら、EU の法制度が基本権憲章の憲法的価値に即して構築されてきた点を明らかにしてきた。データ保護法制は、プライバシー権の保障を淵源としながらも、プライバシー権の古典的意義（私生活の秘匿）に還元され得ない多様な憲法的価値（情報自己決定権、事業者のアカウンタビリティ、データ取扱いの公正性及びデュー・プロセス）を反映する形で発展してきた。

EU ではこのような憲法的文化(136)を背景に、AI による憲法的リスク（アルゴリズムによる差別問題や人間中心の自己決定原理の毀損など）が活発に議論され、プロファイリング規制が立法化されるとともに、AI 規制の立法化についても審議が進んでいる。まず、GDPR は、①プロファイリングに伴う過誤や差別的バイアスを規制するために、自動化された意思決定に対す

(129) De Gregorio and Dunn, *op.cit.*(111), pp.473-500.
(130) *ibid*., p.479.
(131) *ibid*., p.480.
(132) *ibid*.
(133) *ibid*., p.489.
(134) *ibid*., p.490.
(135) *ibid*., p.497.
(136) Woodrow Hartzog and Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection," *Boston College Law Review*, Vol.61 No.5, 2020.5, pp.1687-1761. 同論文によると、「ヨーロッパではプライバシーやデータ保護に関する基本的人権が承認」され、それが GDPR の憲法的基盤になっているのに対して、アメリカではそうした憲法的権利が確立していないものとされる（*ibid*., p.1727.）。

るチェックと異議申立ての権利を保障しているほか、②プロファイリングのプロセスを透明化することで基本権侵害のリスクを可視化する仕組みを制度化し、さらに③事業者に対してリスクの逓減のためのガバナンス規律を義務付けている。次に、AI 規則案は、基本権侵害のリスクに照らして高リスク AI システムの分類を定義するとともに、AI を提供する事業者に対して、適合性評価手続などのガバナンス規律を義務付け、事前のリスク逓減の取組を強化している。

我が国においても、デジタル化の発展に伴い、AI 規制の観点も含めて個人情報保護法制の在り方を見直す必要性が指摘されている(137)。この点、EU のデジタル立憲主義は、憲法と個人情報保護法制の関係性について検討を深めていく契機になると同時に、プライバシー権と個人データ保護権の関係性に関する憲法上の議論を見直す契機にもなると考えられる(138)。

（さとう　たいき）

脱稿後、市川芳治「欧州司法裁 2023 年 7 月 4 日判決の検討―ドイツカルテル庁のデータ収集制限命令を認めた事例―」『ジュリスト』1593 号, 2024.2, pp.20-25 に接し、そこでは、個人データ保護・消費者保護・競争法を三位一体で考察すべき必要性が論じられていた。また、GDPR と AI 規制等の関係については、小向太郎「GDPR と EU のデジタル政策」『同』pp.40-46 に接した。

(137)　デジタル立憲主義に関する日本での議論動向については、前掲注(2)を参照。また、「鈴木正朝＝山本龍彦　対談個人情報保護法制のゆくえ」山本『〈超個人主義〉の逆説』前掲注(67), pp.112-140; 山本龍彦「基調講演　憲法と個人情報保護法制―自己情報コントロール権論の現在―」日本弁護士連合会憲法問題対策本部情報問題対策委員会編『シンポジウム報告書「憲法的価値から考える個人情報保護」（2022 年 8 月 24 日開催）』2022, pp.2-16. <https://www.nichibenren.or.jp/library/pdf/activity/human/constitution_issue/220824_houkokusho.pdf> を参照。

(138)　曽我部真裕教授は、日本国憲法第 13 条の保障するプライバシー権を自己情報コントロール権と解する学説について、次のように指摘している（日本の憲法学説の議論状況については、前掲注(15)及び(67)を参照）。すなわち、個人情報保護法制の規定を見ると、「自己情報のコントロールという要素は、限られた局面でのみ現れるにとどまることから、憲法上のプライバシー権を、「自己情報コントロール権」と呼ぶのは不適切であり、むしろ EU 基本権憲章 8 条 1 項と同様に、「個人情報の保護を求める権利（right to the protection of personal data, droit à la protection des données à caractère personnel）」という呼称が適当だと考えられる」と指摘し、プライバシー権を、EU の個人データ保護権に即して理解すべきとの見解を提示している（曽我部　前掲注(67), pp.11-12.）。この点、EU では、個人データ保護権を具体化するデータ保護法制は、古典的プライバシー権（私生活の秘匿）に限定されない多様な憲法的価値を保障し、情報自己決定権（自己情報コントロール権）もその保障内容の一部分を構成してきた。さらに、データ保護法制は、GDPR の制定以降、ガバナンス規律を含めたプロファイリング規制も規定するに至っており、その保障内容は多様化の傾向を強めている（第Ⅰ章及び第Ⅱ章第 1 節参照）。デジタル立憲主義を含めた EU の議論では、個人データ保護権は、こうした多種多様な規定内容を包摂する役割を果たすと同時に、データ保護法制が多様な憲法的価値に沿って展開されるべきことを要請していると理解されている（第Ⅰ章第 5 節参照）。もっとも、自己情報コントロールの要素をどの程度強く保障すべきかは、一義的に定まっておらず、別途検討の余地があると考えられる。また、宍戸常寿東京大学教授は、「憲法学がそれなりにプライバシー権を論じたにもかかわらず、個人情報保護法制との接点をいまひとつ見出しにくいままであった」と述べている（宍戸常寿「個人情報保護法制―保護と利活用のバランス―」長谷部恭男編『論究憲法　憲法の過去から未来へ』有斐閣, 2017, p.371.）。この点、本稿で検討したデジタル立憲主義は、個人情報保護法制を憲法具体化立法として捉える議論であり、そのため、この議論は、憲法と個人情報保護法制の関係性に関する憲法上の議論に新しい知見を加え得る可能性があると考えられる。