TCフォーラム研究報告2021年5号（2021年5月）　©石村耕治

TCフォーラム研究報告2021年5号（2021年5月）

EUの包括的AIシステム規制始動

EUの顔認証情報利用禁止を含むAI（人工知能）規制案を読む

EUのプライバシー侵害AIパンデミック対策ワクチン

～人権が護られてはじめてAI開発・利用はゆるされる

石 村 耕 治

（TC フォーラム共同代表・白鷗大学名誉教授）

≪内容目次≫

●はじめに～人権が護られてはじめて AI 開発・利用はゆるされる
◆GDPR と AI 規制規則との関係
◆ひと目でわかる EU での AI 規制の経緯
◆ひと目でわかるEUのAI規制の仕組み

■第1部　EU の包括的 AI 規制の枠組み
◆ひと目でわかる AI 規制法の枠組み
◆「人間が主役の AI」に向けて EU とアメリカが競争
◆なぜ EU は包括的な AI 規制を実施するのか
～EU は、人間が主役の AI 開発・利用の拠点になる！

■第2部　EU の AI 規制規則案を深読みする
～危ない AI は、逃げられない、逃がさない！！
◆EU の AI 規制規則案のポイント解説
◆4分類の AI 規制規則の仕組み
◆透明性確保：AI システム利用事実の告知義務
◆「禁止される AI 実務」と「高リスク AI システム」
1　禁止される AI 実務/ブラックリスト掲載 AI システム
2　高リスク AI システムへの「ゆりかごから墓場まで方式」規制とは

(1) 高リスク AI システムのプロバイダー/開発者に対する規制
(2) 高リスク AI システムのユーザーに対する規制
(3) 高リスク AI システムの輸入者に対する規制
(4) 高リスク AI システムの販売者に対する規制
(5) 高リスク AI システムのプロバイダー/開発者となるユーザー、輸入者、販売者および第三者
(6) 小括
(7) 限界事例
3 AI システム市販後規制、情報共有、市場監視
(1)プロバイダー/開発者の市販後モニタリグング義務
(2)事故および稼働過誤情報の共有
◆AI 規則(案)の執行体制
◆行動規範に基づく倫理的・自発的協力
◆AI システム規制のガバナンスの仕組み
1 欧州 AI 委員会/AIボードの創設
2 各加盟国のAIシステム規制機関
◆AIシステム規制違反への罰則
1 AI規制規則違反に対する制裁
2 EUの機関・エージェンシー・団体によるAI規制規則違反

■第3部 わが国での危ないAIシステム利用実態
～EUのAI規制からわが国のAI利用ケースを検証する
◆マイナンバーパンデミックを流行らす菅政権
～人権ゼロのデジタル収容所列島化を目指す菅政権
◆顔認証式マイナカード使用オンライン保険資格確認システム
～人権を蝕む顔認証情報のマイナンバー管理制度の裏口導入
◆インドの生体認証式 ID カードから厚労省の悪巧みを読み解く
◆危ない QR コード・顔認証情報使用のマイナカードのスマホ申請
◆問われる東京渋谷区での NINE 依存で顔認証データの利用
◆子どもの学習成績をマイナバーで AI 国家管理
～問われる人格権のポイント評価

●むすびにかえて

【添付資料】
●もっと知りたいEUの統治機構と法制度

●はじめに～人権が護られてはじめて AI 開発・利用はゆるされる

人工知能（AI=Artificial Intelligence）が、目覚ましい発展をとげている。これまで人間にしかできなかった知的な決定を、AI は、情報処理手順（アルゴリズム/algorithm）とデータ（big data）を準備すれば、機械的に遂行できるようにした。こうした知的な決定を人間の介在なしに行うことを、「自動決定（ADM=automated decision making）」、通称で「ADM」と呼ぶ。自動運転自動車が、赤信号を認識して運転を停止することが適例である。視覚認識（visual cognition）仕様の医療機器がガン細胞を探知・発見するのも ADM の利用例である。このように、AI システムや ADM プログラムは、官民にわたりさまざまな分野で活用が広がっている。市場調査、商業サービス、金融サービス、健康医療サービス、政府行政サービス、公共サービスなど多岐にわたる。

今日、先端技術の1つである AI システムや ADM プログラムは市民生活に数えきれなくらいのメリットをもたらしている。

その一方で、AI システムや ADM プログラムに入れるアルゴリズムやデータに偏り（かたより）（偏頗/バイアス/algorithmic bias）があると、不透明で想定外の結果が出たりする[1]。

例えば、課税庁が、AI 税務調査対象者選定システムに、①「疑わしければ課税庁の利益に」のアルゴリズムを入れたとする。逆に、②「疑わしければ、納税者の利益に」のアルゴリズムを入れたとする。①と②では、納税者の同じ申告データを入れても、判定結果に大きな違いが出てくるかもしれない。納税者や税の専門職も、「私はデジタル大嫌い。紙（文書）で何が悪いんだ。AI なんていらない！」と言ってはいられない。「どんとこい AI！」でないと、AI の奴隷にされてしまうかもしれないからだ。AI システムに入れるアルゴリズムについて、課税庁から独立した機関による適正な審査がいる。また、市民・納税者・専門職によるチェックも欠かせない[2]。将来的には、AI システムに入れるアルゴリズムの適否を争う訴訟も多発するに違いない[3]。

これは、ユーザーである政府が、プロバイダーである IT 企業に依頼し開発して AI システムを税務行政サービスに利用するケースである。

そもそも、野放図に AI システムや ADM プログラムを利用してはならない分野もある。AI システムまたは ADM プログラムを、公的機関や民間機関が無差別な人の監視

---

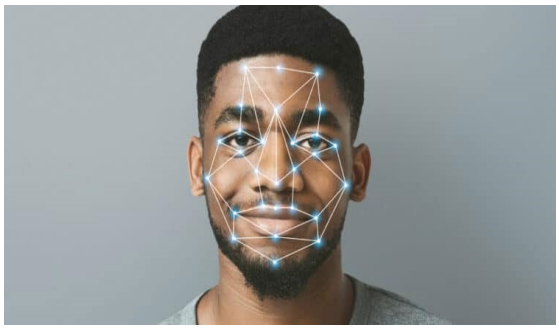
[1] See, Kristin N. Johnson, "Automating the Risk of Bias," 87 Geo. Wash. L. Rev. 1214 (2019) ; Felix Mormann, "Beyond Algorithms: Toward a Normative Theory of Automated Regulation," 62 B.C. L. Rev. 1 (2021); Peter K. Yu, "The Algorithmic Divide and Equality in the Age of Artificial Intelligence," 72 Fla. L. Rev. 331 (2020)

[2] See, Steven Toscher, Daniel Kellerman, "The Impact of Big Data on IRS Civil and Criminal Tax Enforcement," 2-AUG L.A. Law. 14 (2019); See, Michael A. Chichester Jr., Jaclyn R. Giffen, "Recruiting in the Robot Age, 98-JUN Mich. B.J. 34 (2019)

[3] Kimberly A. Houser & Debra Sanders, "The Use of Big Data Analytics by the IRS: Efficient Solutions or the End of Privacy As We knows It?" 9 Vand. J. Ent. & Tech. L. 817 (2017)

や選別に使うケースである。憲法が保障する移動の自由や言論/表現の自由、思想/信条の自由のような市民的自由や人権を侵害につながるからである。

今年 1 月、アメリカのスタンフォード大学の AI 研究機関は、顔認証AIが、70%を超える確率で、SNSの顔写真から政治性向を読み取れるとの研究成果を発表した[4]。



加えて、雇用（採用・勤務評定・契約更新・解雇・昇給など）や教育評価などにも AI システムや ADM プログラムの利用は禁止されるべきであろう。こうした評価に、人種・性別・性的指向などでバイアスのかかったアルゴリズムをインプットして自動決定（ADM）プログラムを使えば、当然、不公正な結果が導き出されるからである。クッキー（cookies）などを使ったターゲティング広告も問題である。自動的に賭博サイトやわいせつ画像の有料サイトへ誘導するなど悪質なものも少なくない。EU では、こうした人権をむしばむ、あるいは人の意思や行動を操作する AI や ADM の利用を禁止する方向である。

最近では、ネット上に流通する有害情報・社会的法益侵害情報、不当投稿・ツイートを自動選別・削除（モデレート）する AI システムも、議論のあるところである。使い方を誤れば、言論/表現の自由をむしばみ、国家や政府に都合の悪い SNS（ソーシャルメディア）への言論・投稿・ツイートを削除（モデレート）するのが当り前の中国型のデジタル監視国家主義とも結びつく。

このように、民主的な価値観に基づく AI システムの使い分け、人間のよるコントロールをどうするかは、デジタル化時代の重い課題である。また、こうしたコントロールを誰が行うか、政府？あるいは民間？を、決めなければならない。つまり、政府規制（法規制）か、自主規制（行動規範/行動指針のよる倫理規制）か、または双方の併用

---

[4] See, Michal Kosinsk, "Facial recognition technology can expose political orientation from naturalistic facial images," Scientific Reports (Jan., 2021)
Facial_recognition_technology_can_expose_political.pdf ; Facial recognition technology can predict a person's political orientation with 72% accuracy
Facial recognition technology can predict a person's political orientation with 72% accuracy (psypost.org)

規制か、の問題もある。AI システム規制手法の基本問題に加え、規制の適用範囲（EU 域外への適用）、透明化を含む法適合性評価やその基準、情報開示、規制違反に対する罰則なども重い課題である。いずれにしろ、“都市計画がないのに EU 域内の次々と家が建つ無法常態に急いでストップをかける”必要がある。

EU（欧州連合）の欧州委員会（European Commission）は、去る（21 年）4 月 21 日に、AI（人工知能）規制をねらいとする規則案（Proposed Regulation on AI/以下「AI 規制規則案」または「規則案」）を公表した [5]。AI 規制規則案の正式名称は、「人工知能に関する統一ルールを定めかつ一定の法律を改正するための規則（Regulation laying down harmonized rules on artificial intelligence and amending certain legislative acts）」である。タイトル I から XII、前文＋85 条と 9 つの別表からなる。通称では、EU「AI 法（Artificial Intelligence Act）」とも呼ばれる。

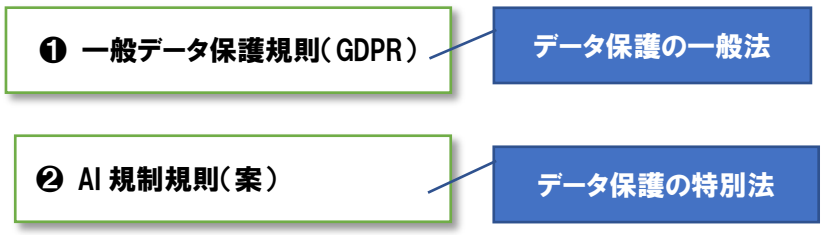
◆GDPR と AI 規制規則との関係

EU は、すでに、ヨーロッパ地域の個人情報保護法ともいえる「一般データ保護規則（GDPR=General Data Protection Regulation）」を採択している。GDPR は、官民双方が規制対象の法律である。EU は、GDPR を、2016 年 5 月 24 日に発効させ、2018 年 5 月 25 日から施行している [6]。

GDPR は、データ保護に関する“一般法”である [7]。これに対して、2021 年4月21日に公表された AI 規制規則案は、AI に規制対象を絞った“特別法”である。したがって、AI 規制規則案が成立・施行され、双方がぶつかる場合には、AI 規制については特別法である AI 規制規則が優先する。

---

[5] Regulation laying down harmonized rules on artificial intelligence and amending certain legislative acts Europe fit for the Digital Age: Artificial Intelligence (europa.eu)
[6] GDPR の邦文での分析について、詳しくは、www.pij-web.net/cnn/CNN-94.pdf
[7] CNN ニューズ 94 号参照 http://www.pij-web.net/cnn/CNN-94.pdf　なお、わが国の個人情報保護委員会による仮邦訳が公表されている。gdpr-provisions-ja.pdf (ppc.go.jp)



EU は、2020 年に、『AI 白書(White Paper on Artificial Intelligence)』[8]を公表している[9]。この AI 白書は、今回の AI 規制規則案は、"GDPR の AI 版"を発布するための草案ともいえる。

一般法である GDPR 22 条では、次のように規定して、個人(データ主体)に対し、ADM プログラム(AI システム)においてもっぱら自動決定の対象とされない権利を保障する。

> 第 22 条 **プロファイリングを含む個人に対する自動化された意思決定**
> 1 データ主体は、当該データ主体に関する法的効果を発生させる、または、当該データ主体に対して同様の重大な影響を及ぼすプロファイリングを含むもっぱら自動化された取扱いに基づいた決定の対象とされない権利を有する。

すなわち、EUにおいて、個人は、人の監視または人が関与しない形で自分のデータが自動処理の対象となることを拒否する権利を保障されている。このことから、例えば、信販事業者が、ローン審査をする場合に、オンラインのアルゴリズムとチャットボット【人工知能(AI)を活用した自動会話プログラム】のみで、消費者の信用格付けをしようとする場合、当該消費者は、これを拒否することができる。

加えて、GDPR13条～15条では、いかなる機関も、ADMプログラム(AIシステム)で、個人の権益に影響を及ぼす決定をするアルゴリズムにデータを挿入する場合には、その処理に先立ち、本人にその旨を通知するように求められる。

◆ひと目でわかる EU での AI 規制の経緯

こうした性格を有するAI規制規則案の公表にいたるまでの経緯は、おおまかに説明すると、次のとおりである。

---

8 commission-white-paper-artificial-intelligence-feb2020_en.pdf (europa.eu)

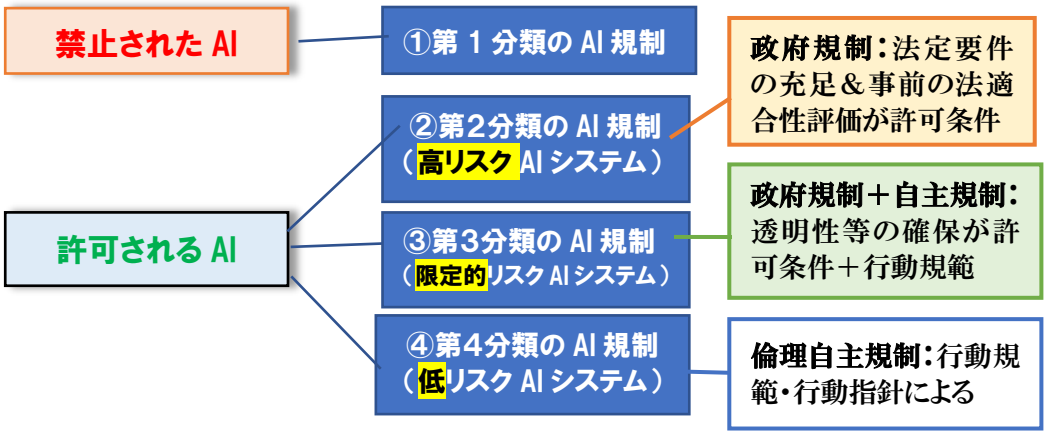
9 わが国の経産省は、「AI 原則の実践の在り方に関する研究会」(旧 AI 社会実践アーキテクチャー検討会) を開催し、EU など諸外国の法制の動きを含め、先端産業の健全な育成に向けて AI システム/ADM プログラムに関する AI ガバナンスのあり方を探っている。本稿の執筆にあたっても参照した。

【図表１】AI規制規則案公表までの主な経緯

年月	主な出来事
2018年4月	欧州委員会が、EU の AI 戦略を各機関に伝達（Communication Artificial Intelligence for Europe）」≪EU は「人間が主役の AI ルール」を定め、AI 投資・開発・利用を促進し、米中などと競争し、世界の AI 市場を主導する。≫
2018年6月	AI専門家グループ（AI HLEG= High-Level Expert Group on AI）設置≪AI倫理ガイドライン草案の検討≫
2019年4月	AI HLEG が「信頼できる AI のための倫理ガイドライン（Ethics guidelines for trustworthy AI）」を策定・公表≪❶AI 倫理原則、❷原則遵守の 7 つの要件、❸チェックリスト≫
2020年2月	欧州委員会が「AI白書（White Paper on Artificial Intelligence）」と「AI・IoT・ロボットに関する安全・賠償責任レポート（Report on the safety and liability implications of AI, the Internet of Things and robotics）」を公表。公開諮問（パブコメ）を実施。
2020年10月	欧州議会が、AI関連の3文書［❶AI・ロボット・関連技術の倫理枠組み（Framework of ethical aspects of AI, robotics and related technologies）、❷AI民事責任体制Civil liability regime for AI］、❸AI知的財産（Intellectual property rights for the development of AI technologies］を採択
2021年4月	欧州委員会が、21日に、AI規制規則案を公表

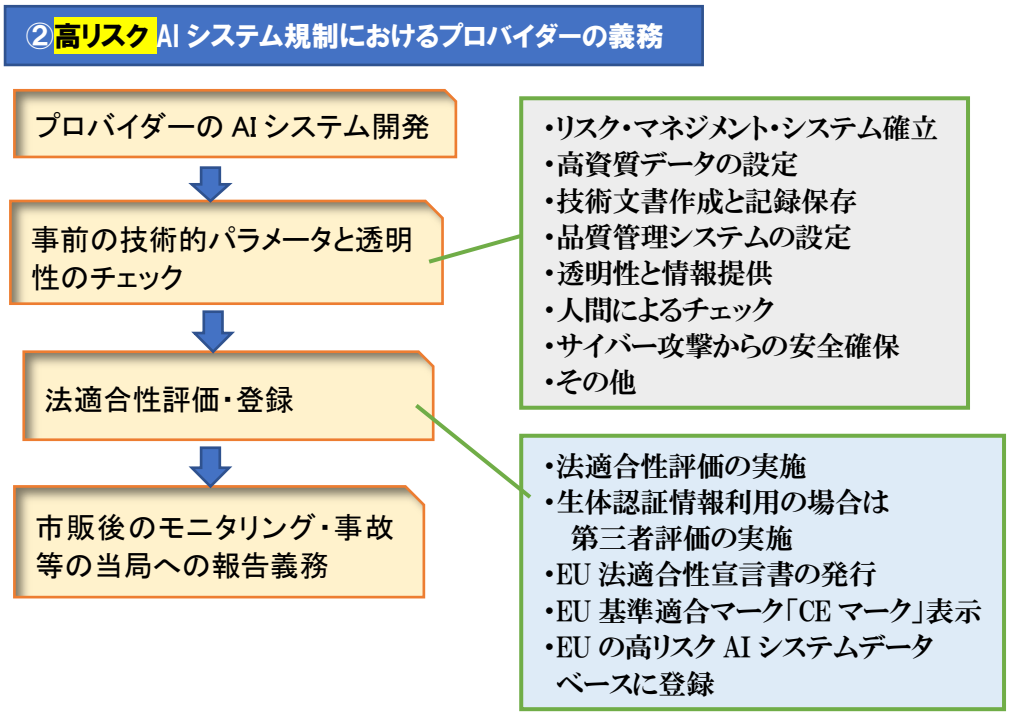
◆ひと目でわかるEUのAI規制の仕組み

この AI 規制規則案では、「AI システム（AI system）」に 4 段階に分けて規制を加える。分類は、リスクベース方式（risk-based approach）、つまり“危険度”順である。4 分類規制の基本的な仕組みは、わかりやすくいえば、次のとおりである。



EU の AI 規制規則案では、②高リスク AI システムに対する政府規制が中核になる。この分類にあてはまる AI システムに対してはライフサイクル（生涯工程）、つまり「ゆりかごから墓場まで方式（cradle-to-grave approach）」」で、さまざまな角度から縛りがかかる。 徹底した規制を実施し、市民の自由や人権保護を先行させるためである。

規制は、プロバイダー（IT 企業）、ユーザー（民間利用者や公的機関）、輸入者や販売者にまで及ぶ。高リスク AI システムの「プロバイダー」の義務を取り上げて、アバウトに説明すると、次のとおりである。



また、④低リスクの AI システムに対しては、政府規制ではなく、業界団体などが自主的に定めた倫理・行動規範・行動指針により自主規制が実施される。そして、③限定的リスク AI システムには、政府規制と自主規制が適用になる。こうした4分類規制の基本的な仕組みをもう少し詳しく読んでみると、次のとおりである。

【図表2】4 分類規制の基本的な仕組みをもう少し詳しく読む

4 分類規制のあらまし

【禁止された AI①】

①第 1 分類の AI 規制：禁止された AI 実務（prohibited AI practices）（規則案 5 条）

❶人間の行動を操作し肉体的または精神的にむしばむ AI システムの利用、❷子どもや障害者を相手の搾取行為への AI システムの利用、❸AI を使ったスコアリングシステム・社会信用ポイント制（social scoring/個人の行動や人格的特性などのデータに基づき、国家が個人の信頼性などを格付けする AI システム）、❹公共空間での無差別な

AI 顔認証監視カメラやライブ遠隔顔認証 AI システムの利用。

【許可される AI②・③・④】

②第 2 分類の AI 規制対象：高リスク AI システム（High-risk AI systems）（規則案 5 条）≪政府規制：法定要件の充足と事前（*ex-ante*）の法適合性評価が許可条件≫

（a）規制対象 AI 製品の安全基準（規則案別表第 2）：産業機械、医療機器など、法により第三者認証対象となるもの。

（b）特定分野の AI システム（規則案別表第 3）

例：❶運輸のような重要な社会インフラへの AI システムの利用、❷AI 手術支援ロボットシステム、❸具体的な事実に対する法の適用のような司法行政などへの AI システムの利用など。

③第 3 分類の AI 規制対象：限定的リスク AI システム（limited risk AI systems）（規則案 52 条）≪政府規制：透明性等の確保が許可条件＋自主規制≫

企業による消費者との対話（chatbots）の解析などへの AI システム利用など。

④第４分類の AI 規制対象：低（極小）リスク AI システム（minimal risk AI systems）（規則案 69 条）≪原則として自主規制/行動規範による倫理規制≫

AI システムを利用したビデオゲーム、e メール・スパム・フィルターなど。

規制方法のあらまし

★これら4分類の AI システムのうち、規制の中核となるのは、②「高リスク AI システム」。高リスク AI システムについては、ライフタイムプロセス（生涯工程）、つまり「ゆりかごから墓場まで方式（cradle-to-grave approach）」で、徹底的に政府規制を実施。

★政府規制は、原則として各加盟国の権限ある当局などが実施。EU の AI 規制の統括組織として、欧州 AI 委員会/AI ボードを新設。EU 共通の AI システムデータベースを新設し危険な AI を集中監視。

★③限定的リスク AI システムについては、プロバイダーが透明性確保などの政府規制に加え、行動規範（Codes of conduct）行動指針による自主規制（倫理・自主規制）。

★低リスク AI システムについては、行動規範（Codes of conduct）行動指針による自主規制（倫理・自主規制）が基本。

★リスクある AI システムには、加盟国の権限ある当局や業界団体から当事者に自主的な是正をとるように指導を実施。

★AI 規制規則違反には罰則。AI システム禁止またはコンプライアンス違反など、その種類や程度に応じて、最大で 3,000 万ユーロ（おおよそ 39 億円）か、企業には世界の売上高の最大6％か、どちらか高い方の過料（規則案 71 条）。また、EU のさまざまな機関やエージェンシー、団体などが AI 規制規則に違反した場合には、欧州データ保護監督官（EDPS=European Data Protection

Supervisor）が過料を科す（第 72 条）

①第 1 分類の AI 規制は、「厳禁される AI 実務（expressly prohibited AI practices）」であり、官民の業務に AI システム（ADM プログラム）を利用してはならない分野である。AI 規制規則案は、公共空間での無差別な AI 顔認証監視カメラやライブ遠隔顔認証 AI システムの利用、スコアリングシステム・社会信用ポイント制などを限定列挙している（規則案 タイトル II、5条）[10]。

②第 2 分類の AI 規制対象は、「高リスク AI システム（High-risk AI systems）」である（規則案 タイトル III、6 条以下）。高リスク AI システムについては原則として利用を解禁する。しかし、その法適合性については市販前またはサービス開始前（*ex ante*）の評価、その後のモニターなど厳しいコンプライアンス義務が課される。

③第 3 分類の AI 規制対象は、「限定的リスク AI システム（limited risk AI systems）」である。限定的リスク AI システムについては、AI 使用にあたり情報処理手順の開示（Algorithmic transparency）などの透明性確保義務が課される。

④第４分類の AI 規制対象は、「低（極小）リスク AI システム（minimal risk AI systems）」である。低リスク AI システムについては、人権に影響が少ないとみて、原則として規制の対象から外している[前記【図表２】参照]。代わりに、欧州委員会（European Commission）などが、AI システムの個々の IT 企業（プロバイダー/開発者）、その業界団体または双方に対して行動規範（Codes of Conduct）を定めるように奨励し、自発的協力を求める仕組みになっている（規則案69条）。

これら4分類の AI システムのうち、規則案で中核となるのは、②「高リスク AI システム」である。高リスク AI システムについて、規則案では、いわゆる「ゆりかごから墓場まで方式（cradle-to-grave approach）」で、徹底的に政府規制を実施する。

なお、AI規制規則違反には、各加盟国の権限ある当局が、AIシステム禁止またはコンプライアンス違反など、その種類や程度に応じて、最大で3,000万ユーロ（おおよそ39億円）か、企業には世界の売上高の最大６%か、どちらか高い方の過料を科す（AI規制規則案タイトルX第71条）。また、EUのさまざまな機関やエージェンシー、団体などがAI規制規則に違反した場合には、欧州データ保護監督官（EDPS=European Data Protection Supervisor）が過料を科す（第72条）。

EU の AI 規制規則案は、EU 域内にいるユーザーを対象に AI システムの販売や AI システムのサービスを提供する IT 企業（プロバイダー/開発者）、とりわけ中小事業者、起業家（startups）に大きな影響が及ぶ。加えて、UE 域外に拠点を置き、EU 市場でビ

[10] AI 規制規則案６条では、「高リスク AI システム（High-risk AI systems）について具体的に定義していない。しかし、規則６条２項関係別表第３において具体例を掲げている。後記【図表５】参照。

ジネスを展開する外国 IT 企業にも多大な影響を及ぼす。EU の AI 規制規則案は、EU 域外にも適用があるからである。

わが国では、法や倫理のよる縛りなくプライバシー/個人情報を糧に、AI システムを使って調理し、利益をあげようとする IT 企業がばっこしている。また、開発された AI システムを使って日常的に人権侵害を繰り返す官民のユーザーも多い。こうした西欧型の民主的な価値観、市民的な自由や人権を後回しにし、利益をむさぼるわが国の IT 企業は、いずれ EU 市場ではビジネスができなくなる。

本稿第 1 部では、EU の包括的な AI 規制規則案の枠組みと包括的な規制を必要としたわけを探る。第 2 部では、EU の包括的な AI 規制を深読みする。そして、第 3 部では、EU の基準を参考にわが国での人権をむしばむ AI システムの利用ケースを点検してみたい。

■第1部　EU の包括的 AI 規制の枠組み

EU の新たな AI 規制規則案は、EU 域内での野放図な AI 利用に包括的な規制を加えることが狙いである。加盟国政府や IT 企業（プロバイダー/開発者）やユーザー（官民の機関）などに対して、AI 技術の利用や提供にあたっては、欧州の民主主義的な価値観、EU 市民の自由や人権を護るように求める。

この規則が正式に通れば、AI システム、とりわけ個別の同意のない顔認証情報システムが人権をむしばむ利用につながらないように、法と倫理の双方の面から厳しい規制がかかる。

◆ひと目でわかる AI 規制法の枠組み

EU の欧州委員会（EC）は、4 月 21 日に AI 規制規則案を公表した。タイトル I から XII、前文＋85 条と 9 つの別表からなる。法と倫理双方の面から多様な規制が盛られている。その目次を邦訳（仮訳）してみると、次のとおりである。

【図表3】AI 規制規則案の目次（仮訳）

前文
タイトル I　**通則**［General provisions］
　第 1 条　趣旨［Subject matter］
　第 2 条　適用範囲［Scope］
　第 3 条　定義［Definitions］
　第 4 条　付則第1への修正［Amendments to Annex I］
タイトル II　**禁止された AI 実務**［Prohibited artificial intelligence practices］

第 5 条
タイトル III　高リスク AI システム[High-risk AI system]
チャプター1　高リスク AI システムの分類[Classification of AI systems as high-risk]
第 6 条　高リスク AI システムの分類ルール[Classification rules of AI systems as high-risk]
第 7 条　付則第3への修正[Amendments to Annex III]
チャプター2　高リスク AI システムの要件[Requirements for AI systems as high-risk]
第 8 条　要件へのコンプライアンス[Compliance with the requirements]
第 9 条　リスク・マネジメント・システム[Risk management system]
第 10 条　データとデータガバナンス[Data and data governance]
第 11 条　技術文書[Technical documentation]
第 12 条　記録保存[Record-keeping]
第 13 条　ユーザーへの透明性確保と情報提供[Transparency and provision of information to users]
第 14 条　人によるチェック[Human oversight]
チャプター3　高リスク AI システムのプロバイダーやユーザーその他の当事者の義務[Obligations of providers and users of high-risk AI systems and other parties]
第 16 条　高リスク AI システムのプロバイダー義務[Obligations of providers of high-risk AI systems]
第 17 条　品質管理システム[Quality management systems]
第 18 条　技術資料作成義務[Obligations to draw up technical documentation]
第 19 条　法適合性評価[Conformity assessment]
第 20 条　自動作成ログ[Automatically generated logs]
第 21 条　是正行為[Corrective actions]
第 22 条　情報通知義務[Duty of information]
第 23 条　権限ある当局への協力[Cooperation with competent authorities]
第 24 条　製品製造者の義務[Obligations of product manufacturers]
第 25 条　授権代理人[Authorised representatives]
第 26 条　輸入者の義務[Obligations of importers]
第 27 条　販売者の義務[Obligations of distributors]
第 28 条　販売者、輸入者、ユーザーその他第三者の義務[Obligations of disributors, importers, users or any other third-party]
第 29 条　高リスク AI システムのユーザーの義務[Obligations of users of high-risk AI systems]
チャプター4　認定当局と認定団体[Notifying authorities and notified bodies]

第 30 条 認定当局[Notifying authorities]
第 31 条 法適合性評価団体への認定申請[Application of a conformity assessment body for notification]
第 32 条 認定手続[Notification procedure]
第 33 条 認定団体[Notified bodies]
第 34 条 認定団体の子団体および下請け[Subsidiaries and subcontracting by notified bodies]
第 35 条 本規則に基づく確認番号と指定された認定団体[Identification numbers and lists of notified bodies designated under this Regulation]
第 36 条 認定の変更[Changes to notifications]
第 37 条 認定団体の適格性にかかる不服申立て[Challenge to the competence of notified bodies]
第 38 条 認定団体との調整[Coordination of notified bodies]
第 39 条 第三国の法適合性評価団体[Conformity assessment of third countries]
チャプター５ 基準、法適合性評価、証明書、登録[Standards, conformity assessment, certificates, registration]
第 40 条 調和した基準[Harmonaised standards]
第 41 条 共通仕様書[Common specification]
第 42 条 一定の要件への適合性の推定[Presumption of conformity with certain requirements]
第 43 条 法適合性評価[Conformity assessment]
第 44 条 証明書[Certificates]
第 45 条 認定団体の決定に対する不服申立て[Appeal against decisions of notified bodies]
第 46 条 認定団体の通知義務[Information obligations of notified bodies]
第 47 条 法適合性評価手続の逸脱[Derogation from conformity assessment procedure]
第 48 条 EU 法適合性宣言書[EU declaration of conformity]
第 49 条 法適合性の EU 基準適合マーク(CE marking of conformity)
第 50 条 文書保存(Document retention)
第 51 条 登録[Registration]
タイトル Ⅳ 一定のシステムへの透明性確保義務[Transparency obligation for certain AI systems]
第 52 条 一定の AI システムへの透明性確保義務[Transparency obligation for certain AI systems]
タイトル Ⅴ 技術革新支援措置[Measures in support of innovations]

第 53 条　サンドボックス AI 規制[AI regulatory sandboxes]
第 54 条　公益用の AI システム開発のために多くの個人データを処理にかかるサンドボックス AI 規制[Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandboxes]
第 55 条　小規模プロバイダーやユーザーのための措置[Measures for small-scale providers and users]
タイトル VI　ガバナンス[Governance]
チャプター1　欧州 AI 委員会/AI ボード[European artificial intelligence board]
第 56 条　欧州 AI 委員会/AI ボードの創設[Establishment of European artificial intelligence board]
第 57 条　AI ボードの構成[Structure of the Board]
第 58 条　AI ボードの業務[Tasks of the Board]
チャプター2　加盟国の権限ある当局[National competent authorities]
第 59 条　加盟国の権限ある当局の指定[Designation of national competent authorities]
タイトル VII　スタンドアロン高リスク AI システム用 EU データベース[EU database systems for stand-alone high-risk systems]
第 60 条　スタンドアロン高リスク AI システム用 EU データベース[EU database systems for stand-alone high-risk systems]
タイトル VIII　市販後のモニタリング、情報共有、市場監視[Post-market monitoring, information sharing, market surveillance]
チャプター1　市販後モニタリング
第 61 条　高リスク AI システムに対するプロバイダーのモニタリングおよび市販後モニタリング計画[Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems]
チャプター2　事故および稼働過誤情報の共有
第 62 条　重大な事故や製造過誤の報告[Reporting of serious incidents and of malfunctioning]
チャプター3　執行[Enforcement]
第 63 条　EU 市場における AI システムの市場監視とコントール[Market surveillance and control of AI systems in the Union market]
第 64 条　データや文書へのアクセス[Access to data and documentation]
第 65 条　加盟国レベルでのリスクのある AI システムへの対応手続[Procedures for dealing with AI systems presenting a risk at national level]
第 66 条　EU 安全手続[Union safeguard procedure]
第 67 条　リスクある基準適合 AI システム[Compliant AI system which present a risk]

第 68 条　正式なコンプライアンス違反[Formal non-compliance]
タイトル IX　行動規範[Codes of conduct]
第 69 条　行動規範[Codes of conduct]
タイトル X　守秘および罰則[Confidentiality and penalties]
第 70 条　守秘[Confidentiality]
第 71 条　罰則[Penalties]
第 72 条　UN の機関、エージェンシーや団体に対する過料[Administrative fines on Union institutions, agencies and bodies]
タイトル XI　権限の委任と小委員会手続[Delegation of power and committee procedure]
第 73 条　委任行使[Exercise of the delegation]
第 74 条　小委員会[Committee procedure]
タイトル XII　最終規定[Final provisions]
≪以下、略、邦訳省略≫

欧州委員会は、2020 年に、『AI 白書(White Paper on Artificial Intelligence)』を公表したことについてはすでにふれた。この白書は、欧州委員会(EC)やそのアドバイザーが AI と人権のあり方について、数年にわたる検討結果を公表したものである。今回公表した AI 規制規則案は、この白書をベースに練り上げられ、正式な規則を制定するためのたたき台となる原案(draft regulation)である。

この AI 規制規則案で、とりわけ注目を浴びたのは、顔認証技術利用の法規制である。公共空間での無差別な AI 顔認証監視カメラの利用やライブ遠隔顔認証 AI システムの利用を原則禁止としている。例外的に認められるとしても、誘拐犯やテロ対策など他者の人身保護が優先する場合に限られる。

◆「人間が主役の AI」に向けて EU とアメリカが競争

AI 規制規則案は、AI 利用について、アクセルとブレーキを装備する法制といえる。すなわち、EU の IT 企業(プロバイダー/開発者)が高い倫理観を持って AI ビジネスを展開できるようにアクセルを踏む。その一方で、デジタル監視国家の中国やプライバシー保護基準が甘いアメリカや日本などの IT 企業(プロバイダー/開発者)の EU での AI ビジネス展開にブレーキをかけるのが狙いである。言い換えると、EU は、「人間が主役」の観点から AI 利用の適正化、健全な発展をはかるためのグローバルなルールつくりを先導する。これにより、人権ファーストで高い倫理観を持ったヨーロッパ IT 企業(プロバイダー/開発者)の競争力強化、AI 世界市場への参入を目指している。

生体認証情報の法規制については、すでにアメリカ・イリノイ州生体認証情報プライバシー法 (BIPA) CNN-99.pdf (pij-web.net)やカリフォルニア州消費者プライバシー

法（CCPA）CNN-98〔完成版〕.indd (pij-web.net)などの法制がある。これらの法制では、規制対象は、原則として民間機関での生体認証情報の利用に限定している。また、とりわけ AI 技術を組み合わせた生体認証情報の利用に焦点を合わせた立法でもない。

バイデン政権誕生後、連邦レベルでの AI 政策論議が活発になってきている。2021 年 3 月12日、第117回連邦議会下院監視と改革委員会の国家安全保障省委員会（U.S. House Committee on Oversight and Reform Subcommittee on National Security）とサイバー・革新的技術・情報システムに関する軍事小委員会（U.S. House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems）とが、人工知能国家安全保障委員会 2021 年報告(2021 Final Report of the National Security Commission on Artificial Intelligence)[11]に関する合同公聴会を開催した。

この公聴会では、小委員会委員長や長老議員、人工知能国家安全保障委員会（NSCAI）委員長、証人から、AI 技術革新が急であることから、人材を集約して研究開発を積極的に推進すべきであるとの主張が目立った。とりわけ、中国やロシアとの軍拡競争に打ち勝つために AI の研究を強力に推進すべきである声が強かった。国家安全保障、軍事問題を専門とする小委員会の公聴会であったのが響いたのであろう。

しかし、同時に、この公聴会で証言した議員や証人からは、AI 技術の誤用、市民的自由や人権侵害を防止するために、テクノデモクラシー（techno-democracy）の構築も重視すべきであるとの意見も相次いだ。その結果、AI 技術の開発・利用にあたっては、民主的な価値観、透明性、強力な監視、説明責任、法令遵守を求めるためのガバナンスの確立が必須である旨のコンセンサスが得られた。加えて、アメリカが主導して価値観を同じくする諸国とテクノデモクラシーの輪を一段と広げる必要があることも確認された [12]。

民主党主導のアメリカ連邦議会での AI 技術の開発・利用の民主的コントロールについての今後の動きには、目が離せない。しかし、アメリカ議会での動きは、いまだ机上の空論の域を出ない。中身の具体的検討はこれからだ。

（public use）

11 https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf
12 https://oversight.house.gov/news/press-releases/oversight-and-armed-services-subcommittees-held-joint-hearing-on-the-final

アメリカのバイデン政権は、中国型のデジタル監視国家体制を痛烈に批判し、“人権尊重を重視する AI 技術の開発・利用、テクノデモクラシーを確立する”政策を明確にすることで、EU と競争する姿勢を強めている。

これに対して、今般の EU の AI 規制規則案は、軍事バランスなどを抜きにした人権ファーストの具体的な実施策である。重みが違う。内容も、生涯不変の究極のプライバシーである生体認証情報の原則利用禁止に加え、高リスク AI システム規制に傾斜した包括策だ。しかも、民間機関のみならず政府機関も含め民官双方に適用される。世界の主要国・地域では初めてのものである。

アメリカのバイデン政権、ホワイトハウス国家安全保障アドバイザーを務めるジェイク・サリバン氏（White House National Security Adviser Jake Sullivan）は、4 月 22 日に、SNS ツイッターで、EU の新 AI 政策に歓迎の意を表した [13]。しかし、EU の AI 政策は、アメリカが想定する AI 政策と大きな隔たりがある。EU の「高リスク」の概念や法適合性評価の基準など、“規制の哲学（regulatory philosophies）”はさまざまな点で異なる。EU とアメリカとの間との間では、GDPR の域外適用や巨大デジタルプラットフォーマーの GAFA の個人情報取扱いなどをめぐり、以前から大きな問題を抱えている。AI 規制規則案の取扱いをめぐり、大西洋両岸協力（trans-Atlantic corporation）の今後が注目される。

◆なぜ EU は包括的な AI 規制を実施するのか ～EU は、人間が主役の AI 開発・利用の拠点になる！

AI の利用は世界で急拡大している。AI 関連の調査・コンサルティング企業である IDC は、2021年2月に、世界 AI 市場に関する調査結果を発表した [14]。2021 年の世界 AI 市場は、ソフトウエア・ハードウエア・サービスを含め 35 兆円規模、2024 年には 59 兆円規模になると予測する。AI システムがとめどもなく広く社会に浸透する様子が伺える。AI が、人類の未来を明るくするとばかり、脚光を浴びる。しかし、AI には「光と影がある」。AI の人権面での危うさも次第にはっきりしてきている。そのなかには、既存の法令で対処するのが難しい課題も少なくない。

EU が AI 規制に踏み切る理由はさまざまある。その1つに、EU が慣れ親しんできた民主国家観に対峙するデジタル監視国家観、スマートシティないしウーブンシティなどと名うったデータ監視都市構想で人格権を軽視するうねり、中国化への懸念がある。

---

13 https://twitter.com/JakeSullivan46/status/1384970668341669891?s=20

14 IDC（International Data Corporation）は、IT や AI など関する調査・分析・コンサルティングを手掛けるグローバルな企業。 IDC Forecasts Improved Growth for Global AI Market in 2021

中国は、すべての一般市民はもちろんのこと、少数民族、ウイグルのジェノサイド（民族浄化策）に AI 顔認証監視カメラ網（天網）などをフル活用し、国際的批判を浴びている。加えて、AI を利用した社会スコアリングシステム（social scoring/個人の行動や人格的特性などに基づき、国家が個人の信頼性などを格付けする社会信用ポイント制。以下「社会信用ポイント制」ともいう。）の活用を広げている。社会信用ポイント制は、国家が国民の行動を監視し餞別する統治ツールとして、市場社会主義モデル、人権ゼロのデジタル監視国家つくりに一役買っている。

こうした中国スタイルの個人情報を無制限に収集・分析し、市民を監視・追跡・選別する社会は EU ではゆるされない。ヨーロッパで共有されてきた民主的な価値観とぶつかるからである。市民の自由や人権を尊重する政治体制とは相いれず、EU としては絶対に容認できない。EU が、AI 規制を急いでいる究極の理由である。

今回の AI 規制規則案は、世界の個人情報保護法制に大きな影響を及ぼした一般データ保護規則（GDPR）の AI 版草案ともいえる。GDPR と同様に、EU でビジネスを展開する IT 企業に対しては、EU 域外にあっても適用になる。このことから、やりたい放題、野放図な生体認証情報技術ビジネスを展開してきたグローバルな IT 企業（プロバイダー/開発者）への影響も極めて大きい。アメリカや日本の名だたる IT 企業（プロバイダー/開発者）も例外でない。EU 市場で AI ビジネスを展開したい IT 企業（プロバイダー/開発者）は、自国でのビジネスモラル、人権に対する姿勢も問われかねない。

EU は、AI には「光と影がある」ことを熟知している。この AI 規制規則案を通じて、人権ファーストで倫理観あるAI開発・利用を主導する意気込みを世界に向けてアナウンスした。

EU の欧州委員会（European Commission）は、行政執行機関である。AI 規制は、この委員会の初の女性委員長を務めるウルズラ・フォン・デア・ライエン（President Ursula von der Leyen）（任期2019年12月1日～2014年10月31日）が、精力的に進める最重要政策の1つである。

ライエン欧州委員会委員長　　（public use）

今回の AI 規制の狙いは、AI が EU の重視する自由や民主主義、人権といったヨーロッパが共有してきた価値観を損なう事態を避けることにある。人が AI にコントロールされるのではなく、人が AI をコントロールする、ずなわち「人間が主役」の原点に立ち返ることにある。

EU 欧州委員会（European Commission）のブレトン（Thierry Breton）コミッショナーはいう。「AI は手段であり、目標ではない（AI is a means, but not an end）」と。

また、欧州委員会（（European Commission））のデジタル時代への欧州適合担当委員のマルグレーテ・ベステアー（Margrethe Vestager）上級副委員長（Executive Vice-President for a Europe fit for the Digital Age）は言明する。「EU市民の安全と基本的人権が、AIによって脅かされれば、我々のルールは介入する」と。

ベステアー上級副委員長（public use）

ちなみに、EU の主要立法としては、「規則（regulation）」と「指令（Directive）」がある。「規則」は、加盟国の国内法に優先して、加盟国の政府や企業、個人に直接適用される。すなわち、加盟国の政府等を直接法的に拘束する。このため、加盟国の国内立法は不要である。一方、「指令」は異なる。付加価値税指令（VAT directive）[15]のように、個々の加盟国に効力を及ぼすには、加盟国の国内立法が必要である［添付資料【図表 E】参照］。

AI 規制規則案（AI 規制法案）は今後、EUの閣僚理事会（European Council）と欧州議会（European Parliament）で審議される。議論を活発化させ、細部にわたり中身の検討を充実させなければならない。これと並行して、公開諮問（public consultation/パブコメ）手続をとり、広く各界から意見を聴取しなければならない。幅広い合意のもとで成立するまでにはかなりの時間を要する。

---

15 付加価値税の共通システムに関する 2006 年 11 月 28 日付理事会指令 2006/112/EC（VAT 指令）（Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax）

■第2部　EU の AI 規制規則案を深読みする
～危ない AI は、逃げられない、逃がさない！！

EU は、今回の AI システム規制規則案を通して、AIやADMに対し、法と倫理の双方の面から包括的な規制に着手した。「危ない AI は、絶対に逃げられない、逃がさない。」をモットーに、法と企業倫理（行動規範）の2つのツールを使い分け規制を実施する。とりわけ、高リスク AI システムについては、EU の AI の法規制を遵守しないと、EU 域内からは完全に排除される。また、組織内対応の不備などを含むコンプライアンス違反に対しては、その程度に応じて厳しい制裁（過料）が課される。現行法制のもとで問題なく流通している AI 製品やサービスであっても、あらたな AI 規制秩序が確立されれば、決して安穏としてはいられない。以下に、EU の AI 規則規制案のポイントを深読みしてみる。

◆EU の AI 規制規則案のポイント解説

（1）AI 規制規則適用の範囲

AI 規制規則の適用対象は、次のとおりである（AI 規制規則案 2 条）。

【図表４】AI 規制規則の適用対象

①AI システムを市場に出すまたはサービス提供する IT 企業、つまりプロバイダー（provider）/開発者（developer）。プロバイダー/開発者は、EU 域内または第三国に所在しているかどうかは問わない[16]。
②EU 域内に所在する AI サービスのユーザー（user）
③製造された AI システムが EU 域内で使用される場合には、第三国に所在する AI システムのプロバイダー/開発者およびユーザー。具体的には、販売者（distributor）および輸入者（importer）。

例えば、AI システムがわが国で開発され、EU 域内のユーザーに提供されるとする。この場合は、わが国のプロバイダー/開発者に対して、EU の AI 規制規則は域外適用（extra-territorial application）になる。

16 ただし、AI 規制規則案は、一定の場合には適用除外となる。例えば、もっぱら軍事目的で開発されかつ利用される AI システムには、適用除外となる（２条３項）。また、第三国の公的機関、EU または加盟国と締結した法執行または司法共助のために国際条約に基づいて関連当局または機関が AI システムを利用する場合には、適用除外となる（２条４項）。

AI 規制規則は、とりわけ国境のないネット/デジタル環境に適用になる。このため、例えば、ユーザーである EU の民間機関や政府機関と AI 技術のプロバイダーである IT 企業とがオンラインで結ばれているとする。この場合にも、IT 企業が地理的に EU 域外に所在していても、この規則は適用になる。すなわち、AI システム規制は、状況に応じて、EU への販売者（distributor）または輸入者(importer)にあたる者にも適用になる（規則案２６条、２７条）。これら規制対象者は、AI 規制規則上のガバナンスおよびコンプライアンスが厳しく問われる。

（2）定義

規制の対象となる「AI システム」は、次のように定義される(規則案 3 条1号)。

【図表５】「AI システム」の定義

①「人工知能システム（AI system）」とは（規則案 3 条 1 号）
本規則案第 3 条 1 号関係別表（Annex）第1に掲げた 1 つ以上の「AI 技術（techniques）および手法（approaches）」により開発され、かっ、一連の与えられた人間が定義した目的、コンテンツ、予測、勧告または相互に状況に影響を与える決定をすることができるソフトウエアである。（規則案 3 条）。
②「AI 技術および手法」とは（規則案 3 条 1 号関係別表第 1）
ⓐ各種機械学習手法（machine learning approaches）
ⓑ各種ロジック・知識ベース手法（logic- and knowledge-based approaches）
ⓒ各種統計的手法（statistical approaches）

（3）欧州委員会の AI 規制の考え方

欧州委員会（European Commission）の AI 規制の考え方や理由は、AI 規制規則（AI 規制法案）の解説メモ（Explanatory Memorandum）に目を通せばわかる。要約すれば、次のとおりである。

AI（人工知能）または AI システムは、多くの利点を持っている。その一方で、この新たなテクノロジーは、ヨーロッパの価値観や基本的人権、民主主義の原則、オープンな社会の展開にとり危険な面も多々みられる。とりわけ、公共空間における生体認証情報の収集やその他大衆監視技術としての AI 利用は、自由でオープンなヨーロッパ社会にとり大きな脅威になっている。このままでは、EU 市民の生存に深く介入し、その危険度も格段に高まる。

EU における AI に対する認識の高まり、幅広いコンセンサスを得て、欧州委員会（European Commission）は、EU 域内で AI は野放しにするのは、自由や人権、民主主義の原則にとり脅威になるとの結論にいたった。そこで、人間不在

の AI システムに対して、その作り方や使い方の危険度に応じて、注意深く歯止め策を講じ、法と法以外の規範（倫理）双方の面から包括的な規制を加えることにした。

新たな AI 規制規則は、リスクベース・アプローチ（risk-based approach）に基づき、AI システムに包括的規制をかけようとするものである。EU が、AI システムの信頼性を確かなものにするための新たなグローバルなルールをつくる。そして、EU はそれを広めていくフロントランナーとして挑戦しようとするものである。いわば、「プライバシー/人格権をむしばむAIパンデミック」にストップをかけるための画期的な“ワクチン”とみてよい。

◆4分類の AI 規制規則の仕組み

法規制は、具体的なAIシステムの開発・利用方法を、そのリスク度に応じて、次のように 4 段階に分類して実施される。その内容をもう少し深読みすると、次のとおりである。

【図表６】 4段階に分類した AI システム規制の仕組み

①禁止される AI 実務（expressly prohibited AI practices）（規則案5条）
❶人間の自由意思基づく行動を操作する AI システム ❷スコアリング/社会信用ポイント制（個人の行動や人格的特性などに基づき、公共機関やその代理機関が個人の信頼性などを格付けする）AI システム ❸公共空間にいる個人を監視するために顔認証情報を利用する AI システム ❹リアルタイムの遠隔顔認証 AI システム
②高リスクな AI システム（high-risk AI systems）（規則案6条以下）
❶運輸のような重要インフラへの AI システムの利用：市民の生命や健康を危険に陥れかねないことが理由 ❷試験の評価のような教育・職業訓練への AI システムの利用：教育や職業訓練コースを受けられるかどうかは応募者の生命にかかわることが理由 ❸手術支援ロボットのような AI システムを利用した製品：人の生命や健康を危険に陥れかねないことが理由 ❹採用の際の履歴書の診断のような雇用や労務管理などへの AI システムの利用：人権がかかわることが理由 ❺融資などの際の信用スコアリング（クレジットスコア）への AI システムの利用：必要不可欠な公的および私的サービスにかかわることが理由 ❻証拠の信頼性評価のような法執行への AI システムの利用：人権がかかわることが理由

❼旅券等の信ぴょう性の証明のような移民・亡命・国境管理への AI システムの利用：人権がかかわることが理由 ❽具体的な事実に対する法の適用のような司法行政などへの AI システムの利用：法の適正手続にかかわることが理由 ➔「ゆりかごから墓場まで方式（cradle-to-grave approach）」による徹底的な規制。AI システムの法適合性について事前チェックの義務化、EU が設置・管理する AI システムデータベースへの登録。プロバイダーへの各種ガバナンス確立の義務化、ユーザーが負う義務の明確化など（29条）。
③限定的リスクの AI システム（limited risk AI systems）
❶企業が消費者との対話（chatbots）の解析などに AI システムを利用している場合など。この場合、原則として消費者はその事実を事前に知らされる権利を有する[17]。 ➔AI システム利用の際の情報開示（Algorithmic transparency）の義務化（規則案 13 条、52条）などの規制はある。しかし、原則は、欧州委員会（European Commission）などが、AI システムの個々のプロバイダー/開発者、その業界団体または双方に対して行動規範（Codes of Conduct）を定めるように奨励し、自発的協力を求める仕組みになっている（規則案69条）。
④低（極小）リスク AI システム（minimal risk AI systems）
上記①・②・③にあてはまらない利用。例えば、AI システムを利用したビデオゲーム、e メール・スパム・フィルターの利用など。大部分の AI システムの利用は、この分類にあてはまる。AI 規制規則案では、この分類にあてはまる AI システムを、EU 市民の権利や安全には大きな影響を及ぼさないとの理由で、法規制の対象から除外している。 代わりに、欧州委員会（European Commission） などが、AI システムの個々のプロバイダー/開発者、その業界団体または双方に対して行動規範（Codes of Conduct）を定めるように奨励し、自発的協力を求める仕組みになっている（規則案69条）。

◆透明性確保：AI システム利用事実の告知義務

EU の AI 規制規則案では、AI システムの透明性を確保するために、一定の場合に、プロバイダーやユーザーに対し受任義務を課している。例えば、AI システムのユーザー（公的機関や民間機関）は、個人（natural persons/自然人）が AI システムを利用し

17 ただし、刑事訴追の対象となる刑事犯罪などが関係する場合は除く（規則案５２条１項）。

ていることをしっかりと認識できないと思われる場合、利用の事実を当該個人に告知しなければならない、と規定する（規則案 タイトル IV 52 条）。

この透明性確保措置により、個人は、その利用状況などから明らかに AI システムが利用されていると理解できる場合を除き、AI システムが利用されていることの告知を受けることができる。ただし、法執行目的での AI システム利用の場合は除かれる。

また、オーディオ（音声）やビデオ（映像）、イメージ（画像）制作に、AI システムを使った人物画像合成の技術、いわゆる「ディープフェイク（deep fakes）」が利用する場合、ユーザーは、そのコンテントを人工的にまたは操作して制作することを開示しなければならない[18]。

AI 規制規則案タイトル IV は、「透明性確保義務（transparency obligations for certain AI systems）」の表題で、次のように規定する。

> ①プロバイダーは、自然人（個人）と相互のやり取りをすることを目的とする AI システムの設計や開発にあたっては、当該自然人がそうした目的を知ることができるようにしなければならない。ただし、利用状況や利用関係からその目的が明らかにわかる場合を除く。この義務は、犯罪行為の摘発、防止、捜査および起訴するために法律により認められている AI システムには課さないものとする。ただし、こうした AI システムが、公衆に対し犯罪行為を報告するように利用される場合は除く。
>
> ②感情認識システム（emotion recognition system）、生体分類システム（biometric categorization system）のユーザーは、その対象となる自然人（個人）に対し、当該システムが作動していることを告知するものとする。この義務は、犯罪行為の摘発、防止、捜査および起訴するために法律により認められている生体分類に使用される AI システムには課さないものとする。
>
> ③画像（イメージ）、音声（オーディオ）または映像（ビデオ）のコンテントを作製または操作する AI システムで、現存する人、物、場所その他の実体または出来事を合成できる、または、本物または実在の人物を不正に合成で（「ディープフェイク（deep fakes）」）できるものがある。この種の AI システムのユーザーは、そのコンテントが合成または操作されていることを開示しなければならない。

[18] わが国でも、アスリートの盗撮画像や映像、女優や特定個人の画像や映像を AI 技術の１つであるデープフェイク【デープラーニング（深層学習）＋フェイク（偽物）】を使って加工したニセ画像を各種サイトで頒布する行為が社会問題となっている。テレビ番組などで放映された画像を基にしたニセ画像については、法執行当局が著作権違反で摘発している。デープフェイク/人物画像合成技術の規制については、芸術作品の作成にも使用されている。このことから、この種の AI 技術の規制は、憲法が保障する表現の自由の視角からも問題になる。

ただし、この種の AI システムが、犯罪行為の摘発、防止、捜査および起訴するために法律により認められている場合、または EU の基本権章典（Charter of Fundamental Rights of the EU）で保障された表現の自由権や芸術・科学の自由権の行使に必要な場合には、第三者の権利や自由の保護を適切にすれば、その限りではない。

④前記①、②および③は、本規則のタイトル III【高リスク AI システム】に規定された要件や義務にはその効力は及ばないものとする。

◆「禁止される AI 実務」と「高リスク AI システム」

以上のように、今回の AI 規制規則案タイトル III では、AI システムを4つに分類して法規制を加える。これらのうち、わかりにくい規制内容について、以下にもう少し深読みしてみる。

1　禁止される AI 実務/ブラックリスト掲載 AI システム

許容されないリスク（unacceptable risk）段階にある厳しく①禁止される AI 実務、つまり俗にいう「ブラックリスト掲載 AI システム（blacklisted AI system）」とは、市民の人権や生存、安全に明確な脅威を与えると考えられる AI システムを指す（規則案タイトル II 5 条）。具体的には、次のような例があげられる。

❶ユーザーの自由意思を巧みにコントロールし、人間の行動を操作するために利用される AI システムがあげられる。具体的には、ゲームや玩具の音声機能で子どもに危険な行動を促すような AI システムの利用は厳禁される。長距離トラック運転者に長時間運転させるために非可聴域の周波数を探し出すためのAIシステムの利用は厳禁される。アルゴリズムを使ってギャンブル依存症の人をその種の広告サイトに誘導する有害な AI システムなども厳禁される。

❷政府が AI を用いて個人データを分析して格付けする「スコアリング（social scoring）」/「社会信用ポイント制」があげられる。すなわち、政府が、AI システムを利用して個人の行動や人格的特性などに基づき、国家が個人の信頼性などを格付けすることは厳禁される。

❸公共空間にいる個人を監視するために顔認証情報を利用する AI システム（ただし、誘拐やテロなど人身保護の場合で裁判所の令状その他の独立した機関の判定に基づくときなどは除く。）があげられる。具体的には、公道上で無差別に顔認証情報により個人を識別する AI 監視カメラシステムなどがあげられ、厳禁される。

❹リアル遠隔顔認証 AI システム

2　高リスク AI システムへの「ゆりかごから墓場まで方式」規制とは

AI 規制規則案の中核となるのが、②高リスク AI システム（high-risk AI systems）に対する規制である（6条以下）。この分類にあてはまる AI システムに対してはライフサイクル（生涯工程）、つまり「ゆりかごから墓場まで方式」で、さまざまな角度から縛りがかかる。 徹底した規制を実施し、市民の自由や人権保護を先行させるためである。

【コラム】AI 規制規則の立ち位置

AI 規制規則は、AI システムに適用される規則である。AI システムは、機械や玩具、エレベーター、装置、医療機器などさまざまな製品に採用されている。また、AI システムは、航空機、自動車、鉄道の安全などの部品として採用されている。こうした製品などに対しては、それぞれの安全性を確保するなどの目的で定められている既存の製品安全基準に関する EU 規則が適用になる。

それぞれの製品などに適用される製品安全基準関係 EU 規則は、“一般法”にあたる。一方、AI 規制規則は、“特別法”にあたる。AI システムに関して双方の規則が重なる場合も想定される。こうした場合には、原則として“特別法”である AI 規制規則が優先して適用になる。

「高リスク AI システム」については、本規則案タイトル III・チャプター2で一般要件を定める。そのうえで、同タイトル・チャプター3以下で、適用対象者別に一般要件うちのどれが、どのように適用になるかを定める。

【図表7】AI 規制の仕方

≪高リスク AI システム法適合性：一般要件≫

第 8 条　要件へのコンプライアンス［Compliance with the requirements］
第 9 条　リスク・マネジメント・システム［Risk management system］
第 10 条　データとデータガバナンス［Data and data governance］
第 11 条　技術文書［Technical documentation］

≪対象者≫

（1）プロバイダー/開発者の場合
（2）ユーザーの場合
（3）輸入者の場合
（4）販売者の場合
（5）その他

紙幅が限られることから、≪高リスク AI システム法適合性：一般要件≫に関する詳しい説明を省き、適用対象別に、一般要件とその他の要件がどのように適用になるのかを、やさしく説明する。

（1）高リスク AI システムのプロバイダー/開発者に対する規制

高リスク AI システム（high-risk AI systems）のプロバイダー/開発者は、次のような規制を受ける(規則案タイトル III、チャプター3)。

【図表８】プロバイダー/開発者に対する規制の仕組み

①技術的パラメータ[外部からいれる値]と透明性

❶リスク・マネジメント・システム：プロバイダー/開発者は、リスク・マネジメント・システムを確立、実施、文書化し、かつ維持しなければならない。この場合においては、AIシステムの予見できるリスクの確認や市場に出した後のモニター制度のような手法を含む。リスク・マネジメント・システムにおいては、各種リスクは、できるだけ AI システムの設計および開発段階で削減または最小化できるようにしなければならない(規則案 16 条 b 号による 9 条の準用)。

❷高資質データの設定：高リスク AI システムは、的確で誤りがなく、完全な高資質データを設定したうえで、訓練、有効性、試行しなければならない。この要件は、適切なデータガバナンスおよびデータマネジメントを通じて充足しなければならない(規則案 17 条による 10 条の準用)。

❸技術文書作成と記録保存：高リスク AI システムの設計は、出てきた結果を追跡しかつ実証できるようにしなければならない。このことから、プロバイダー/開発者は、AI システムが AI 規制規則案を遵守しているかどうかどうかを点検できるように、技術文書（technical documentation）を作成したうえ保存しなければならない(規則案 18 条による 11 条・12 条の準用)。

❹品質管理システム：プロバイダー/開発者は、資質管理システム（quality management system）を設定するように義務づけられる。とりわけ、定期的な規制遵守状況、AI システムの設計対するシステマティックレビュー、技術スタンダードおよび報告制度に関する戦略が求められる。

❺透明性とユーザーに対する情報提供：高リスク AI システムについて、ユーザーは、どのように結果を導き出すことができるのかを理解し、かつコントロールできなければならない。この点について、プロバイダー/開発者は、文書や説明書を準備しなければならない(規則案 13 条)。

❻人間によるチェック：高リスク AI システムは、権限ある自然人のよる効率的な方法でチェック（oversee）できるように設計されていなければならない。この要件は、高リスク AI システムの利用による健康、安全および基本的人権へのリスクを防止するまたは最小化することが狙いである(規則案 14 条)。

❼システムの堅固性、正確性、サイバー攻撃からの安全性：高リスク AI システムは、悪意ある第三者による攻撃や介入に対応できるように、高水準のシステムの堅固性、正確性、サイバー攻撃からの安全性（robustness, accuracy and cybersecurity）を確保できるものでなければならない（規則案 15 条）。

❽授権代理人の指定：プロバイダー/開発者は、EU の域外に所在する場合、有効な書面の形で授権代理人（当該プロバイダー/開発者からの委任を受け EU 域内に所在する自然人または法人）を指定しなければならない（規則案 25 条）。

②法適合性および登録手続

❶法適合性評価：プロバイダー/開発者は、高リスク AI システムが AI 規制規則案の要件を充足している旨を示すための法適合性評価（conformity assessment）を実施しなければならない（規則案 19 条）。プロバイダー/開発者は、AI システムに相当の変更を加える場合には、あらたな法適合性評価を実施しなければならない。高リスク AI システムは、これを遠隔生体認証（remote biometric identification）および公共インフラ網（public infrastructure networks）として利用しようとする場合、第三者遵法評価を受けるものとする。政府機関が発行した証明書は、最大で 5 年間有効とする。遠隔生体認証および公共インフラ網高リスク以外の AI システムについて、プロバイダー/開発者は、自主的な評価を選択し、EU 法適合性宣言書（EU declaration of conformity）を発行することができる。プロバイダー/開発者は、適切な形で継続的に宣言書を更新しなければならない（規則案 48 条）。

❷EU 基準適合マーク（CE marking）：プロバイダー/開発者は、AI システムを EU 域内で自由に作動させるためには、EU 基準適合マーク（CE marking）を見えるところに張り付け、その AI システムが規則を遵守している旨を示さなければならない（規則案 49 条）。

❸登録：AI システムを市場に出すまたはサービスを提供するに先立ち、プロバイダー/開発者は、その AI システムをあらたに設置する旨を、一般に公開されている EU が設ける高リスク AI システムデータベース（EU Database of High-Risk AI Systems）に登録（register）しなければならない（規則案 51 条・60 条）。

③モニタリング

❶市販後モニタリング:プロバイダー/開発者は、市販後モニタリングを実施し、AI システムの性能に関しユーザー等が提供したデータを収集、文書化および分析をしなければならない(規則案 61 条)。
❷報告義務:プロバイダー/開発者は、AI システムの関する重大な事故または機能過誤に加え、重大な受任義務違反を該当する加盟国の権限ある当局に届け出なければならない(規則案 22 条・62 条)。

(2) 高リスク AI システムのユーザーに対する規制

高リスク AI システム(high-risk AI systems)のユーザーは、おおまかにいえば、次のような規制を受ける(規則案 29 条)。

【図表9】ユーザーの義務

高リスク AI システムに対するユーザーの義務:
❶ユーザーは、高リスク AI システムを、プロバイダー/開発者が準備した説明書に基づいて利用し、入力データを管理し、装置の異常をモニターし、かつ、当該 AI システムが自動的に作成したログ(AI の利用状況やデータ通信など履歴や情報)の記録を保存しなければならない。
❷信用機関(credit institutions)による高リスク AI システムの利用については、信用機関を規制する EU 指令(Directive 2013/36/EU)のもとで負う義務の規定を準用する。
❸高リスク AI システムのユーザーは、情報を、他の EU 規則(Regulation(EU) 2016/679 または Directive(EU)2016/680)のもとで求められるデータ保護影響評価(data protection impact assessment)を実施したうえで利用するものとする。

(3) 高リスク AI システムの輸入者に対する規制

高リスク AI システム(high-risk AI systems)の輸入者(importer)は、おおまかにいえば、次のような規制を受ける(規則案 26 条)。

【図表10】輸入者の義務

高リスク AI システムに対する輸入者の義務:輸入者は、高リスク AI システムが市場に出される前にプロバイダー/開発者が実施した法適合性評価手続を護り、準備した技術資料を保存しなければならない。

(4) 高リスク AI システムの販売者に対する規制

高リスク AI システム(high-risk AI systems)の販売者(distributor)は、おおまかにいえば、次のような規制を受ける(規則案 27 条)。

【図表11】販売者の義務

高リスク AI システムに対する販売者の義務:販売者は、高リスク AI システムに法定の EU 基準適合マーク(CE marking)を記し、利用のための法定資料や説明書が添付されていることを確認しなければならない。

（5）高リスク AI システムのプロバイダー/開発者となるユーザー、輸入者、販売者および第三者

高リスク AI システム(high-risk AI systems)のプロバイダー/開発者となるユーザー、輸入者、販売者および第三者は、次のような規制を受ける(規則案 28 条)。

【図表 12】対象者一般に対する義務

高リスク AI システムのプロバイダー/開発者となるユーザー、輸入者、販売者および第三者の義務:いかなる当事者も、次の場合には、プロバイダー/開発者とされ、受任義務を負う。❶高リスク AI システムを、商号や商標をつけて市場に出すまたはサービスを提供する場合、❷すでに市場の出しているまたはサービスを提供している高リスク AI システムの目的に変更を加える場合、または、❸高リスク AI システムに相当の変更を加える場合。これら❶・❷・❸いずれの場合においても、当初のプロバイダー/開発者は、AI 規制規則案のもとでは、もはやプロバイダー/開発者とされない。

（6）小括

すでにふれたように、規則案では、「高リスク AI システム」について、具体的に定義していない。しかし、以上のように、AI システムが高リスクとみなされれば、プロバイダー/開発者は広範な受任義務を負うことになる仕組みになっている。つまり、②高リスク AI システムについては、プロバイダー/開発者には、コンプライアンスチェック、EU が集中管理するデータベースへの登録とか、さまざまな法適合性要件が課される

【図表8】②高リスクが伴う❶～❽のような AI システムについては、市場に出される前に、加盟国政府が指定する権限ある当局(competent authorities)または欧州データ保護管理官(EDPS=European Data Protection Supervisor) による審査を受ける必要がある。 AI 規制規則案では、こうした審査のため、権限ある当局または EDPS に対して、サンドボックス AI 規制(AI regulatory sandboxes)[19]の仕組みを構築するように求める(53条以下)。

19 サンドボックス AI 規制 (AI regulatory sandboxes) とは、外部システムへのアクセスを制限したセキュリティモデルを指す。語源は、「サンドボックス (sandbox/砂場)」に由来し、子どもは砂場の中では遊んでいいが、砂場の外では遊んではならないという制限を課す意味で使われる。

加えて、高リスク AI システムについては、すでにふれたように、プロバイダー/開発者は高度の質の面での厳格な要件を充足する危機管理システム（risk management system）を構築するように求められる（規則案8条、9条）。

一方、AI システムを使うユーザー側も、さまざまな義務を負う。例えば、IT 企業、つまりプロバイダー/開発者が用意した説明書その他の情報を遵守したうえで AI システムを利用するように求められる。また、ユーザーは、個人データ保護評価を実施しなければならない。

（7） 限界事例

どちらの段階の規制にあたるのか、わかりにくい事例もある。例えば、遠隔生体認証 AI システムは禁止、あるいは許容されても高リスクに分類され、厳格な規制に服するように求められる。いずれにしろ、法執行目的で、公共空間にいる個人を無差別に監視するための顔認証情報 AI システムやリアルタイムの遠隔顔認証 AI システムは、EU では厳禁される。

これらは、例外的な利用は認められてはいるものの、きわめて限定的、かつ厳格な条件で認められる。例えば、失踪した子どもの捜索、テロ防止、3年以上に刑罰に対象となる重大犯罪の容疑者の特定などの目的での遠隔生体認証 AI システムを利用するケースなどである（規則案 52 条）。ただし、この場合、裁判所または独立した機関による承認などが必要になる。しかし、禁止か許可かの線引きはあいまいである。

3 AI システム市販後規制、情報共有、市場監視

EU の AI 規制規則案では、AI システムのライフサイクル（生涯の工程）規制を目指している。これまで、「AI システム稼働中の規制」に焦点をあてて、分析・紹介してきた。

以下においては、「AI システム市販後規制」、つまり「市販後モニター・情報共有・市場監視（Post-market monitoring, information sharing, market surveillance）についてふれる（AI 規則案タイトル VIII）。

（1）プロバイダー/開発者の市販後モニタリグング義務

AI 規制規則案は、プロバイダー/開発者に、AI 技術や高リスク AI システムに関する市販後モニタリング・システム（Post-market monitoring system）を確立し、記録文書を残すように求める（規則案 61 条）。つまり、規則案に基づいた仕様でデザインし、かつ実施するように、プロバイダーに求める。

【図表13】プロバイダーの市販後モニタリング義務

プロバイダーのよる市販後モニタリングおよび高リスクAIシステムの対する市販後モニタリング計画

①プロバイダーは、AI技術や高リスクAIシステムの性質に応じた方法で、市販後モニタリング・システムを確立し、文書で記録するものとする。
②市販後モニタリング・システムは、高リスクAIシステムの遂行についてその生涯の工程にわたり、ユーザーが提供したまたはその他の情報源を通して収集したデータを、積極的かつ組織的に収集、記録および分析するものとする。
③市販後モニタリング・システムは、市販後モニタリング計画に基づくものとする。市販後モニタリング計画は、本規則付則IVにいう技術文書の 1 部をなる。欧州委員会は、この計画を施工するための法令を定めるものとする。

（2）事故および稼働過誤情報の共有

高リスクAIシステムのプロバイダーは、基本的人権を保障する EU 法に違反する重大な事故や稼働過誤（serious incidents and of malfunctioning）が発生した場合、15 日以内に、報告書（report）にして発生地を所管する加盟国の市場監視当局に通知する義務を負う（規則案 62 条）。通知をうけた当局は、所定の手続を踏んだうえで、その加盟国で人権問題を所管する公的当局や団体に情報を提供する。

なお、欧州委員会は、本規則施行後 12 か月以内に、この手続に関するガイダンスを作成し、公表することになっている。

◆AI 規則（案）の執行体制

AI 規制規則案の執行（enforcement）、すなわち AI システムに関する市場監視・コンプライアンスについては、EU の製造物市場監視・コンプライアンス規則（Regulation（EU） 2019/1020）[20] に基づいて行われる（規則案チャプター3）。

AIシステムの市場監視やコンプライアンスについては、製品別、サービス利用別になど、様々な角度から包括的に実施される。また、欧州委員会や各加盟国の複数の機関が関与する形になっており、その仕組みは若干複雑である。その概要は、以下のとおりである。

【図表１４】EU 市場での AI システムの監視とコントロールのあらまし

①EU 市場における AI システムの市場監視とコントロール（規則案 63 条）
❶加盟国での執行：各加盟国の監督当局は、管轄する市場の監視活動の結果を定期的に欧州委員会（European Commission）に報告しなければならない。同時に、当該監督当局は、市場監視活動において、競争原則に関する EU 法の適用に関して潜在的に利害があると確認された情報を、遅滞なく、欧州委

[20] Regulation of 20 June 2019 on market surveillance and compliance products） EUR-Lex - 32019R1020 - EN - EUR-Lex (europa.eu)

員会および自国の競争当局報告しなければならない。

❷高リスク AI システムの監視: 高リスク AI システムについては、機械、玩具、エレベーターといったように製品別に、AI 規制規則案別表 II に掲げる準拠規則に基づきそれぞれの市場監視当局が担当する。

❸市販の AI システム:市販の AI システムで、金融機関が使用するまたは金融機関にサービスを提供するものについては、金融機関の監督を担当する権限ある当局が、市場を監視する。

❹法執行目的の AI システム:法執行目的で使われる AI システムは、権限あるデータ保護監督当局、または、法執行・移民・難民を担当する当局の活動を監視する各加盟国の権限ある当局が、市場を監視する。

❺EU 機関が利用する AI システム: EU の機関、団体などが AI システムを利用する場合、欧州データ保護監察官（EDPA=European Data Protection Supervisor）が、市場を監視する。

❻加盟国間の協力体制:AI システムの監視にあたっては、加盟国が協力してその任にあたる。

②データや文書へのアクセス（開示）（規則案 64 条）

❶市場監視当局のデータや資料へのアクセス権の保障:市場監視当局は、プロバイダー/開発者の研修、有効性、試行に関するデータセットについて完全なアクセス（開示）を求めることができる。開示の対象には、リモートアクセスを可能にする API（application programming interfaces）[21]などのツールも含む。

❷ソースコード [22]のアクセス（開示）:高リスク AI システムの法適合性をチェックするに必要な場合に、市場監視当局は、ソースコードのアクセス（開示）を求めることができる。

❸基本的人権保護のためのアクセス（開示）:高リスク AI システムの利用に関して、EU 法が保障する基本的人権を保護するために、監督または執行を担当する各加盟国の公的機関または当局は、自国の管轄権の範囲内で、AI 規制規則案により作成されかつ保存されている資料へのアクセス（開示）を求めることができる。この場合、加盟国の公的機関または当局は、当該アクセス（開

[21] API とは、アプリケーション、ソフトウエア、プログラムをつなぐこと。また、API を公開することとは、ソフトウエアに API という外部とやりとりする窓口を作り、外部アプリとコミュニケーションや連携ができる状態にすることを指す。

[22] コンピュータへの指示やアルゴリズム（情報処理手順）のようにプログラムのもとになる文字列のこと。プログラム言語（プログラミング言語）であらわされる。ソース、ソース・プログラム、原始プログラムなどともいう。ソースコードは知的財産権上の保護の対象となり、重要な企業秘密となる。このため、市販されている一般的なパソコンソフトなどでソースコードが提供されることはほとんどない。ただ、一部のソフトウエアでは改良や修正、再頒布などを目的にオープンソース化されているものもある。

示）に関係する加盟国にその旨を通知するものとする。

❹規制当局の公表：AI 規制規則の施行から 3 か月以内に、各加盟国は、規制を実施する監督当局名などを一般市民がアクセスできるウエブサイトに公表するものとする。各加盟国は、そのリストおよび更新した場合にはそのリストを欧州委員会や他のすべての加盟国に通知するものとする。

❺人権侵害が危惧される AI システムの検査要請：加盟国の公的機関または当局は、基本的人権保護のために前記❸にいう資料にアクセスしたが、EU 法への違反があるかどうか定かではないとする。この場合には、市場監視当局に対して、理由を付して問題の高リスク AI システムを技術的検査するように求めることができる。市場監視当局は、求めがあってから合理的期間内に、公的機関または当局との密接な協力のもとに検査をする。

❻守秘義務：加盟国の公的機関または当局は、前記❸の手続きにおいて入手した情報や資料について守秘義務を負う。

③各加盟国レベルでのリスクある AI システムへの対処手続（規則案 65 条）

❶リスクある AI システム（AI system presenting a risk）と何か：リスクある AI システムとは、健康、安全および基本的人権の保護にリスクのある AI システムを指す。

❷リスク評価と対応：各加盟国の市場監視当局は、AI システムが前記❶にいうリスクある AI システムにあたるとの十分な理由があると考える場合、問題となった AI システムが、AI 規制規則案に規定されたすべての要件や義務を遵守しているかどうかの評価を実施しなければならない。人権保護に関するリスクがある場合、市場監視当局は、その旨を公的機関または当局に通知しなければならない。オペレーター/管理運営者（operators）[23]は、市場監視当局ならびに他の加盟国の公的機関または当局からの必要な協力に応じる。評価過程において、市場監視当局は、AI システムが本規則に規定された要件や義務を遵守していないと判断した場合、遅滞なく当該 AI システムがコンプライアンスに必要な適切な是正措置をとるようにオペレーター/管理運営者に求めるか、または、リスクの性質に応じて、合理的な機関内に、市場から AI システムを回収もしくはリコールするように求める。

❸コンプライアンス違反の通知：市場監視当局は、コンプライアンス違反が、自国内にとどまらないと考える場合には、評価結果とオペレーター/管理運営者に取るように求めた措置を欧州委員会および他の加盟国に通知するものとする。

[23] オペレーター/運営管理者（operators）とは、プロバイダー（provider）ユーザー（user）、授権代理人（authrised representative）、輸入者（importer）、販売者（distributor）を総称する（規則案 3 条 8 号）。

❹オペレーターによる是正措置の域内周知:オペレーター/管理運営者は、問題の AI システムに対して取られたあらゆる適切な是正措置が EU 域内市場に行きわたるようにしなければならない。

❺市場監視当局のよる是正措置:AI システムのオペレーター/管理運営者が、前記❷にいう期間内に十分な是正措置を取らなかった場合、市場監視当局は、その加盟国内市場でその AI システムの利用を禁止または制限する、市場から AI システムを回収もしくはリコールための適切な暫定措置(provisional measure)を講じることができる。こうした措置を講じた場合、市場監視当局は、欧州委員会または他の加盟国にその旨を通知する。

❻加盟国市場監視当局への情報提供:前記❺にいう情報には、手続を開始した加盟国の市場監視当局以外の加盟国の市場監視当局が問題視した法令違反の AI 監視システムの確認に必要な次のような詳細なデータを含むものとする。AI システムの出所、指摘されたコンプライアンス違反とリスクの特徴、加盟国がとった措置の性格や期間、関係するオペレーター/管理運営者との議論など。

❼不同意の場合の通知:手続を開始した加盟国の市場監視当局以外の加盟国の市場監視当局は、遅滞なく、欧州委員会および他の加盟国に、問題の AI システムのコンプライアンス違反に対して取った措置およびその他処分に関する情報、さらには、通知された加盟国の措置に同意しない場合にはその反対を含め、通知するものとする。

❽経過期間後の自動承認:前記❺のいう情報を受け取ってから 3 か月以内に、加盟国が取った暫定措置に対して加盟国または欧州委員会から反対がない場合、その措置は、正式に認められたものとされる。ただし、このことは、製造物市場監視・コンプライアンス規則(Regulation(EU) 2019/1020)18 条の基づき関係人であるオペレーター/管理運営者の手続上の権利行使を妨げるものではない。

❾加盟国による制裁措置:すべての加盟国の市場監視当局は、遅滞なく、自国市場から問題の製品の回収のような適切な制裁措置をとることを認められる。

④EU の安全手続(Union safeguard procedure)(規則案 66 条)

❶市場監視当局に是正措置への異議・協議・評価:前記③❺にいう通知を受け取ってから 3 か月以内に、他の加盟国が取った措置に対する反対がある場合、または、欧州委員会が EU 法に違反する措置であるとみた場合、欧州委員会は、遅滞なく当該加盟国およびオペレーター/管理運営者と協議に入るものとし、かつ、その加盟国が取った措置を評価するものとする。評価の結果、欧州委員会が、前記③❺にいう通知から 9 か月内に、当該加盟国の措置が

正当であるどうかを決定し、かつ、当該決定を関係加盟国に通知するものとする。

❷評価に伴う対応：当該加盟国の措置が正当である場合、すべての加盟国は、違法な AI システムをその市場から回収するに必要な措置を取り、その後欧州委員会に通知するものとする。当該加盟国の措置が正当ではないとされた場合には、関係する加盟国は当該措置を撤回するものとする。

❸統一基準・共通仕様違反の場合：加盟国の措置が正当であるとされ、かつ、AI システムのコンプライアンス違反が本規則 40 条および 41 条にいう統一基準（harmonaised standards）または共通仕様（common specifications）との不具合に起因する場合には、欧州委員会は、EU 規則 2012 年 1025 号（Regulation（EU）1025/2012）[24]11 条に基づく手続を適用するものとする。

⑤リスクある基準適合 AI システム（Complaint AI System which present a risk）（規則案 67 条）

❶AI システムオペレーターによる対応：前記③にいう評価により、加盟国の市場監視当局が、AI システムが本規則のコンプライアンスには順応しているものの、人の健康や安全、基本的人権、その他公益の保護の面でリスクがあると判断した場合、問題の AI システムのオペレーター/管理運営者は、合理的期間内に、AI システムの市場からの回収またはリコールなどにより、リスクを除去するように求められる。

❷是正措置の周知：プロバイダー/開発者またはオペレーター/管理運営者は、問題の AI システムに関して取られたすべての是正措置を、前記❶のもとで加盟国の市場監視当局が定めた期間内に、EU 市場のなかで利用できるようにしなければならない。

❸通知する情報：リスクある AI システムであると判断した加盟国は、その旨をすみやかに欧州委員会および他の加盟国に通知するものとする。通知する情報には、詳細なあらゆるデータを含む。とりわけ、問題ある AI システムを確認するに必要なデータ、AI システムの出所、サプライチェーン、リスクの特徴、加盟国が取った措置や期間など。

❹欧州委員会による評価・対応：欧州委員会は、遅滞なく、加盟国やオペレーター/管理運営者と協議に入り、加盟国が取った措置を評価するものする。評価結果に基づき、欧州委員会は、当該措置が正当化できるかどうか、そして、必要に応じて適切な措置を講じるものとする。

❺欧州委員会による周知：欧州委員会は、決定をした場合、その決定を加盟国に周知する。

⑥正式なコンプライアンス違反（Formal non-compliance）（規則案 68 条）

[24] EUR-Lex - 32012R1025 - EN - EUR-Lex (europa.eu)

❶停止対象となるコンプライアンス違反：加盟国の市場監視当局は、以下のような結論の1つにいたった場合には、当該プロバイダー/開発者に対して当該コンプライアンス違反の解消を求めるものとする。

ⓐAI 規制規則案 49 条の法適合性に関する EU 基準適合マーク（CE marking）を違法に張り付けた場合

ⓑ法適合性に関する EU 基準適合マーク（CE marking）を張り付けていない場合

ⓒEU 法適合性宣言書（EU declaration of conformity）が発行されていない場合

ⓓEU 法適合性宣言書（EU declaration of conformity）が正しく発行されていない場合

ⓔ法適合性評価手続に関係する通知された団体の識別番号が張り付けられていない場合

❷コンプライアンス違反への対応：前記❶に掲げたコンプライアンス違反がある場合、関係加盟国は高リスク AI システムが市場に出回らないように、あらゆる適切な制限または禁止措置をとる、または当該 AI システムを市場からリコールまたは回収するものとする。

◆行動規範に基づく倫理的・自発的協力

AI 規制規則案では、大きく、①禁止された高リスク AI システムと②それ以外の許可される AI システムとに分けて規制を実施する。

そして、後者②の許可される AI システムのうち、とりわけ高リスク AI システム以外の AI システム【つまり、第 3 分類の AI 規制対象の限定的リスク AI システム＋第4分類の AI 規制対象の低（極小）リスク AI システム】については、「行動規範（Codes of Conduct）」【「行動指針」ともいう。】を定め、それを倫理的・自発的に遵守する形で実施する構図になっている。

AI 規制規則案によると、「行動規範」は、EU 当局の後押しのもと、IT 企業、つまり AI システムのプロバイダー/開発者、業界団体、または双方が、利害関係人などの参加を得て、自発的に作成することになっている。

以下に、AI システムに関する「行動規範」について、図説する。

【図表15】AI システムに関する「行動規範」とは

行動規範（Codes of conduct）（69 条）

❶欧州委員会と加盟国は、適正なコンプライアンスを確保することを狙いに行動規範を定め、高リスク AI システム以外の AI システムに対し自発的な適用を奨励しかつ支援する。

❷欧州委員会と欧州 AI 委員会（European Artificial Intelligence Board）は、適正なコンプライアンスを確保することを狙いに行動規範を定め、AI システムの設計や開発における環境の持続可能性、障害者のアクセス可能性、利害関係人の参加および明確な目標を持つ開発チームの多様性、ならびに目標達成を測定するためのキーパフォーマンス・インディケータなどの面で AI システムに対して自発的な適用を奨励する。
❸行動規範は、AI システムの個々のプロバイダー/開発者、その業界団体または双方が起草することができる。この場合、ユーザー、利害関係人やこれらの者を代理する団体の参加を求めることができる。行動規範は、関連性などを考慮して複数の AI システムを対象とすることができる。
❹欧州委員会と欧州 AI 委員会は、行動規範の起草を奨励しかつ促進するために、特別の利害、小規模プロバイダー/開発者のニーズや起業を考慮するものとする。

◆AI システム規制のガバナンスの仕組み

AI システム規制を統括する機関として、EU に「欧州 AI 委員会（European Artificial Intelligence Board）」が設けられる。しかし、AI ガバナンスは、第一次的には、各加盟国主導で行われる。効率的なワンストップ・ショップの仕組み（one-stop-shop mechanism）になってはいない。必ずしも AI システムのオペレーター/運営管理者（プロバイダー・ユーザー・授権代理人、輸入者・販売者）にフレンドリーな仕組みではない、との声もある。最終規則に向けた今後の見直しが注目される。

1 欧州 AI 委員会/AIボードの創設

AI規制規則の執行を監督するために、あらたにAI規制を専門に担当する「欧州AI委員会（European Artificial Intelligence Board/AI委員会/AIボード）」が設けられる（規則56条～58条）。欧州AI委員会（Board）は、各加盟国のデータ保護機関などと協力して新規則の統一的な執行を行う。また、欧州委員会に対して助言と支援を行う。

一方、各加盟国は、国レベルでの規則の遵守状況を監督するために1人以上の権限ある担当管を任命するように求められる。これら担当管は、規則違反に対して過料その他の制裁を科すことができる。これらの制裁は、原則として各加盟国が科す。

【図説16】欧州AI委員会/AIボードの創設

①欧州AI委員会の創設（規則案56条）
❶欧州AI委員会（European Artificial Intelligence Board/以下「AI委員会」、{AIボ

ード}ともいう。」)を創設する。

❷AI委員会は、次のことに関し欧州委員会に助言し、かつ支援する。

ⓐ本規則が適用になる事項に関して、加盟国の監督当局と欧州委員会が効率的な協力ができるようにすること。

ⓑ今規則が適用になる事項に関して域内市場を横断する問題が生じた場合、欧州委員会、加盟国監督当局その他の権限ある当局がガイダンスや分析をする調整および支援を行うこと。

ⓒ本規則の統一的な適用を確保するために加盟国の監督当局と欧州委員会を支援すること。

②AI委員会/AIボードの構成(規則案57条)

❶AI委員会/AIボードは、加盟国の監督当局(その長または高官が代表として参加)と欧州データ保護監督官(European Data Protection Board)で構成される。加盟国の他の当局は、問題がその当局と関連性がある場合には、会議への参加を求めるものとする。

❷AI委員会/AIボードは、その委員の単純多数決で手続規則(rules of procedures)を、欧州委員会の同意を得たうえで、採択する。手続規則には、本規則58条に掲げたAI委員会/AIボードの業務遂行に関するものも含む。AI委員会/AIボードは、特別の問題を検証するために小委員会を立ち上げることができる。

❸AI委員会/AIボードの議長は、欧州委員会が務める。欧州委員会が、会議を招集し、かつ、本規則や手続規則に基づきAIボードの業務執行に関する議題を用意する。欧州委員会が、本規則に基づいてAIボードの活動の事務および分析的な支援を行う。

❹AI委員会/AIボードは、その会合に外部の専門家やオブザーバーの参加を求め、かつ、その活動について知ってもらうために妥当な範囲内で利害関係を有する第三者との意見交換を行うことができる。欧州委員会は、AI委員会/AIボードとEUの諸機関やアドバイザーグループなどとの間で意見交換の促進に務める。

③AI委員会/AIボードの業務(規則案58条)

AI委員会/AIボードは、前記56条2項【①❷】に基づき欧州委員会に助言と支援を行う場合の留意事項は、次のとおりである。

ⓐ加盟国間での専門性にたけた最良の実務慣行を収集しかつ分かち合うこと。

ⓑ加盟国間での統一的な行政実務慣行を推進すること。前記53条にいうサンドボックスAI規制(AI regulatory sandboxes)関連事項を含む。

ⓒ本規則の施行関連事項への見解表明、勧告または投稿を公開すること。

2　各加盟国のAIシステム規制機関

AI規制規則案では、各加盟国は、国レベルでの規則の遵守状況を監督するために１人以上の権限ある担当管を任命するように求める（規則案59条）。

【図説１７】各加盟国のAIシステム規制組織

①本規則を適用するために、各加盟国は、国の権限ある当局（national competent authorities）を創設するまたは指定するものとする。加盟国の権限ある当局は、その活動や業務の客観性および不公平性を確保したうえで組織されるものとする。

②各加盟国は、国の権限ある当局のなかから国の監督当局（national supervisory authority）を指定するものとする。国の監督当局は、加盟国が組織上や行政上の理由で複数の当局を指定する場合を除き、認定当局（notifying authority）および市場監視当局（market surveillance authority）として活動するものとする。

③加盟国は、指定をした場合は、その旨を欧州委員会に通知するものとする。この場合において、複数の当局を指定したときには、その理由を記すものとする。

④加盟国は、国の権限ある当局に対し、本規則に定める業務に必要となる財源と人材を十分の供給するものとする。とくに、国の権限ある当局は、高度のAIテクノロジー、データ、データ計算、人権、健康や安全リスク、各種スタンダードや法的基準に関し資質が高く専門性を有する人員を恒常的に配置ものとする。

⑤加盟国は、国の権限ある当局の財源や人材の状況に関して十分な評価を行ったうえで欧州委員会に年次ベースの報告するものとする。欧州委員会は、その情報を欧州AI委員会（Board）に渡し、審査に付し、必要なに応じて勧告を行うものとする。

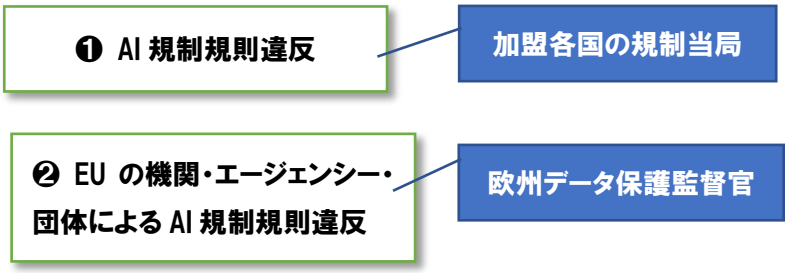
⑥欧州委員会は、各国の権限ある当局間での経験の交換を支援する。

⑦国の権限ある当局は、小規模プロバイダーのことも織り込んだうえで、本規則の執行に関しガイダンスやアドバイスを提供する。国の権限ある当局は、EU法が適用になるAIシステムに関するガイダンスやアドバイスをしようとする場合には、EU法の関する国の権限ある当局が適切な相談に乗るものとする。加盟国は、オペレーター/運営管理者が連絡を取りやすいように、１つの中央コンタクトポイントを設置するものとする。

◆AIシステム規制違反への罰則

AI規制規則違反については、AIシステム禁止またはコンプライアンス違反など、その種類や程度に応じて、各加盟国が、過料その他の制裁/罰則を科す仕組みになっている（AI規制規則案タイトルX第71条）。

また、EUのさまざまな機関やエージェンシー、団体などがAI規制規則に違反した場合には、欧州データ保護監督官（EDPS=European Data Protection Supervisor）が過料を科す仕組みになっている。



1　AI規制規則違反に対する制裁

AI規制規則違反に対する制裁について、例をあげてわかりやすく説明すれば、次のとおりである。

各加盟国の権限ある当局は、禁止されるAI実務、つまり俗にいう「ブラックリスト掲載AIシステム」（規則案タイトルII 5条）を開発し市場に出した、またはサービスを提供した場合、最大で3,000万ユーロ（おおよそ39億円）か、企業には世界の売上高の最大6%か、どちらか高い方の過料を科す。

各加盟国の権限ある当局は、AI規則規制に定める受任義務に違反する場合、最大で2,000万ユーロか、企業には世界の売上高の最大4%か、どちらか高い方の過料を科す。

各加盟国の権限ある当局は、不正確、不完全または虚偽の報告があった場合、最大で1,000万ユーロか、企業には世界の売上高の最大2%か、どちらか高い方の過料を科す。

AI 規制規則案タイトル X 第 71 条は、「罰則（penalties）」の表題で、次のように規定する。

【図表18】AI 規制規則違反に対する罰則

①加盟国は、本規則に規定する文言や条件のコンプライアンス（遵守）を求め、本規則違反に適用するための過料（administrative fines）を含む罰則にかんするツールを定め、かつ、適切で効果的な執行の必要なあらゆる措置を講じるも

のとする。罰則の規定にあたっては、効果的、均等かつ抑止力あるものでなければならない。罰則を科すにあたっては、とりわけ小規模プロバイダーや起業者の利益および経済的支払能力を考慮するものとする。
②加盟国は、ルールや措置およびそれらの修正を行った場合には速やかに欧州委員会に通知するものとする。
③下記のⓐまたはⓑに違反する場合、最大で3,000万ユーロか、違反者が会社の場合には前会計年度における世界の売上高の最大6%か、いずれか高い方の過料を科す。
ⓐ第5条にいう禁止されるAI実務に違反する場合
ⓑAIシステムが第10条【データおよびデータガバナンス】に違反する場合
④本規則のもとでの要件や義務を負うAIシステムで、5条から10条のときを除くコンプライアンス違反の場合には、最大で2,000万ユーロか、違反者が会社の場合には前会計年度における世界の売上高の最大4%か、いずれか高い方の過料を科す。
⑤通知を受けた団体（notified bodies）や加盟国の権限あり当局の求めに応じて提供した情報が不正確、不完全または虚偽的である場合、最大で1,000万ユーロか、違反者が会社の場合には前会計年度における世界の売上高の最大2%か、いずれか高い方の過料を科す。
⑥個々の事例において過料の額を決定する場合、特別な事態に関連するあらゆる状況を勘案し、かつ次のようなことに対し適切な配慮をするものとする。
ⓐ違反と結果の性格、重大さおよび期間
ⓑ同じオペレーター/運営管理者による同じ違反に対して、他の市場監視当局がすでに過料を科しているかどうか
ⓒ違反をしたオペレーター/運営管理者の規模と市場占有率
⑦各加盟国は、自国内に設立された公的当局その他の団体に対して過料を課すことができるかどうか、またはどの程度まで過料を科すかのルールを定めることができる。
⑧他の団体の対する過料に関するルールは、加盟国の法制度に従い、過料は権限ある裁判所によって課される形で適用することができる。加盟国におけるこれらのルールの適用は、同等の効果を有するものとする。

2 EUの機関・エージェンシー・団体によるAI規制規則違反

AI規制規則違反は、EUのさまざまな機関やエージェンシー、団体などがAIシステムを利用する場合にも起こりうる。こうした場合には、欧州データ保護監督官（EDPS=European Data Protection Supervisor）が、これらEUの諸機関などに過料を科

す（AI規制規則案タイトルX第72条）。

制裁について、わかりやすく説明すれば、次のとおりである。

【図表１９】EUの機関のよるAI規制規則違反にEDPSが科す過料の概要

①欧州データ保護監督官（EDPS=European Data Protection Supervisor）は、本規則が適用になるEUの諸機関（institutions）、エージェンシー（agencies）および団体（bodies）に対して過料を科すことができる。過料を科すかどうかやどれだけの額の過料を科すかを決定する場合には、特別な事態に関連するあらゆる状況を勘案し、かつ次のようなことに対し適切な配慮をするものとする。

ⓐ違反と結果の性格、重大さおよび期間

ⓑ同じ問題に関係したEUの機関、エージェンシーまたは団体に対してEDPSが以前に命じた措置の遵守を含む、違反の救済や違反の悪影響を和らげるための欧州データ保護監督官（EDPS）の協力

ⓒEUの機関、エージェンシーまたは団体による同様の以前の違反

②次のような違反には、最大で50万ユーロの過料を科す。

ⓐ第5条にいう禁止されるAI実務にかかるコンプライアンス違反

ⓑ第10条の規定する要件の伴うAIシステムにかかるコンプライアンス違反

③本規則のもとで課される要件や義務を負うAIシステム、ただし第5条から第10条の規定の適用があるものを除く、にかかるコンプライアンス違反には、最大で25万ユーロの過料を科す。

④本条に基づく決定をするにあたり、欧州データ保護監督官（EDPS）は、EDPSが行う手続の対象となるEUの機関、エージェンシーまたは団体に対して違反とされる事項に関し聴聞の機会を与えるものとする。欧州データ保護監督官（EDPS）は、関係当事者が意見を陳述できる状況化においてのみ決定をするものとする。不服については、申立てがある場合、この手続の中で対応するものとする。

⑤関係当事者の防御権は、この手続の中では十分に保護されなければならない。関係当事者は、欧州データ保護監督官（EDPS）のファイルにアクセスする権利を有する。ただし、個人や企業の法的利益を保護するために、個人データまたは企業秘密は対象外とする。

⑥本条において科された過料を収集した基金は、EUの一般会計予算に計上される。

■第3部　わが国での危ないAIシステム利用実態
～EUのAI規制からわが国のAI利用ケースを検証する

◆マイナンバーパンデミックを流行らす菅政権
～人権ゼロのデジタル収容所列島化を目指す菅政権

こうした EU の動きとは対照的なのがわが国である。菅政権は、コロナ禍を緊急時に乗じて“名ばかりデジタル改革”、実質、邪悪な“デジタル収容所列島化”を目指す。人権を後回しにする“デジタル国家総動員体制”づくりしか眼中にない。明らかに EU とは真逆の動きを加速させている。

EU が警鐘を鳴らすように、デジタル化や AI システムは、使い方を誤れば、人権をむしばむ。にもかかわらず、この政権の看板であるデジタル改革関連法のなかに“人権”、“人格権”の文字がまったくない。個人情報保護法制を骨抜きにし、IT 業界の利権を優先し、個人情報を企業に売り渡す。国民をスッポンポンにして、人格権を背番号（マイナンバー）で紐づけて国家監視の枠組みに組み入れる。この政権には、自由や民主主義、人権といった民主国家が共有してきた価値観がまるでない。そもそも自国内で人権を粗末に扱う菅政権は、中国やミャンマーの人権状況などを非難できるわけがない。

菅首相は2021年3月31日の衆院内閣委員会で、マイナンバー制度に関連するこれまでの国費支出が 8,800 億円に上ると説明した。かたや、アメリカは新型コロナワクチン開発に 1 兆円を投じた。アメリカなしではわが国民はワクチンすら受けられない。にもかかわらず、菅政権は、ムダな IT 公共工事に血税をジャブジャブ注ぐのをやめようとしない。「背番号が先か、ワクチンが先か」は、あえて問うまでもないことだ。

「パンデミック」という言葉が流行っている。「パンデミック」の「パン」は“すべて”、「デミア」は“人々”が原義。まさに、菅政権は「マイナンバーパンデミック（背番号感染爆発）」を引き起こす新型コロナウイルスのような存在にみえてくる。

マインバーカード保有が 3 月末時点で全国民の２８％を超え、申請も 4,500 万件弱で３６％超えた、「マイナンバーパンデミック」には貢献したと誇る。だが、これで受けられるデジタル行政サービスなどほとんどない。“デジタル監視国家”、“デジタル収容所列島化”だけが進む。まさに、菅政権の“デジタル国家総動員体制つくり”優先の愚策で、国民のいのちやくらしが大きな犠牲を強いられている。

日の丸ワクチンはつくれない、PCR 検査も徹底しようとしない。効果が不確かな、場当たり的なまん延防止措置や緊急事態宣言を繰り返すだけ。人流をストップさせる思い切ったロックダウンをかけないと、変異種のリバウンドの大波がリバウンドは止められない。この１年間何をしてきたのだろうか。だが、菅政権は、科学軽視で、科学的なデータに基づいた行動（data-driven scientific behavior）ができない。オリバラ開催に固執、やると決めたら一億一心、既定路線には有無をいわせない。コロナウイルスワオーズに、打つ弾（ワクチンや PCR 検査）は満足になし、それでもオールジャパンの精神論（密回避）と竹やり（マスクなど）で切り抜けられると豪語する。「出口戦略」を描けない、ロジスティクス思考を欠き、「インパール」を繰り返す政権だ。科学を軽視し、場当たり政治しかできないこの愚劣な政権には一日も早く退場してもらわないといけない。

コロナパンデミックやアメリカのバイデン政権の誕生で、新自由主義は大きく後退した。にもかかわらず、悲しいことに、わが菅政権は、新自由主義の「自助」の旗を掲げ、コロナ対応そっちのけで、国民の“人権反故”に一心不乱なのである。中国並みのデジタル監視国家つくりしか視野にないのである。人権をまったく語らないデジタル庁など、実質「デジタル［公安調査］庁」以外の何物でもない（CNN ニューズ１０５号参照 http://www.pij-web.net/data/CNN-105.pdf）。コロナパンデミックの最中、デジタル監視法、入管法改悪、高齢者医療負担増額など、いのちとくらしを粗末にする政策を自公など反動的な多数の力で次々と押し切る。

EU の人権尊重の AI ビジネスルールつくりを見る限りでは、人権や IT 倫理に無頓着なわが国が、世界の IT 業界を主導する資格がないことだけは、はっきりしている。全国の医療機関や薬局に顔認証式番号カード使用オンライン保険資格確認システム（M システム）を設置するような公共工事で金儲けし、国民の人権をむしばんで平気な IT 企業は、衰退の軌道を走ることになる時代に入っているのではないか。

EU では、GDPR（一般データ保護規則）で、個別の同意を得ない顔認証情報 AI システムの利用が禁止されている。今般の AI 規制規則案は、EU 域内での野放図な AI 利用に法的規制を加えることが狙いである。加盟国政府や IT 企業（プロバイダー/開発者）やユーザー（官民の機関）などに対して、AI 技術の利用や提供にあたっては、

欧州の民主主義的な価値観、EU 市民の自由や人権を護るように求める。

この規則が正式に通れば、顔認証情報 AI システム、とりわけ、公共空間での無差別な AI 顔認証監視カメラやライブ遠隔顔認証 AI システムの利用、さらには、スコアリングシステム・社会信用ポイント制などは厳禁される（規則案5条）

こうしたEUのAI規制規則案を素材に、わが国での問題の多いAIシステム利用ケースを検証してみる。

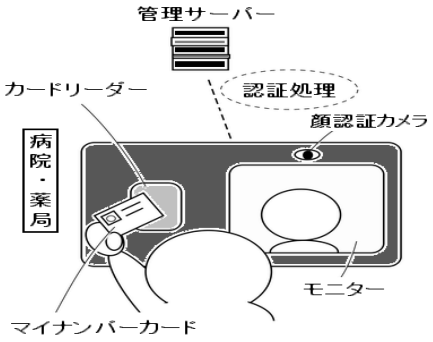
◆顔認証式マイナカード使用オンライン保険資格確認システム ～人権を蝕む顔認証情報のマイナンバー管理制度の裏口導入

政府・厚労省は、かねてから顔認証機能付き IC カードリーダーを使い、患者のマイナバーカード内の IC チップを読み込んでオンライン資格確認を行うシステムつくりを進めてきた。すでに、総額で 1,000 億円を超える国費を投じている。

そして、この 3 月から、全国 22 万ヵ所の医療機関や薬局への顔認証式マイナンバーカード使用オンライン保険資格確認システム（M システム）設置がはじまった。

このシステムでは、医療機関や薬局の窓口にカードリーダーを設置する。そして、原則、患者本人がカードをかざして情報を読みとらせる。保険資格確認用のサーバーで照合するとともに、カードの顔写真で本人確認も行う仕組みだ。

●オンライン顔認証式マイナンバーカード使用保険資格確認システム



しかし、このシステムを使うと、患者は、自分の顔面情報を政府の管理サーバーに提供を半ば強制されることになる。ということは、政府の狙いは、国民全員の顔認証情報の裏口収集しマイナンバーでの監視するために医療機関（Medical institutions）などを総動員することにつながる。

この計画は、公道上の N システムを、あらたに「M システム」として医療機関や薬局にも設けるに等しい。つまり、「マイナンバー（背番号）＋顔（生体）認証情報」を使った国民監視システム」、「M システム」つくりにある、とみてよい。今や全国民の人権/究

極のプライバシーである顔認証情報までもが国家管理される危ない常態にある。

国家に睨まれた市民は、形だけの手続きをとって、医療機関などで裏口収集した顔認証情報を国中の監視カメラ網に垂れ流され、追い回されるのではないか。

わが国の M システムは、EU の GDPR(一般データ保護規則)や今般の AI 規制規則案では、絶対にゆるされない個人データ利用、AI システムにあたる。人権ゼロが当り前の日本政府・厚労省の悪だくみは、あまりにもレベルが低いといわざるをえない。これは、見方を変えれば、民意の低さ、国会議員の人権感覚の悪さにもつながってくる。

生体情報は、生涯不変の情報である。漏れたり、悪用されたら取り返しがつかない。こうした監視ツール、人権侵害ツールを全国 22 万ヵ所に設置するのは、常時国民の基本的人権、プライバシー権を侵害し、憲法違反である。

今のところ、医療機関は、健康保険証に替えて、患者の人権を蝕むオンラインの生体認証式監視カメラシステムを設置するかどうかは任意である。また、カードリーダーを設置したかどうかにかかわらず、これまでどおり健康保険証で診療することができる。21 年 5 月からは、保険証番号でのオンライン資格確認がはじまる。個人情報の詰まったマイナンバーカードを、医療機関が取り扱う必要はなくなる。

ここで、医療機関は、立ち止まって、今一度、政府が進めるオンラインの生体認証式保険資格確認システムの是非を、患者の人権保護の面から、よく考えて欲しい。煮え切らない態度がもどかしい。

◆インドの生体認証式 ID カードから厚労省の悪巧みを読み解く

NECやパナソニックなどわが国の IT 企業(プロバイダー/開発者)は、早くから、このオンライン顔認証式マイナンバーカード使用保険資格認証システムを実用化している。政府・厚労省の悪だくみの裏では、患者(全国民)の究極のセンシティブ情報(人格権)を儲けにつなげようと「IT 利権」がうごめいている。

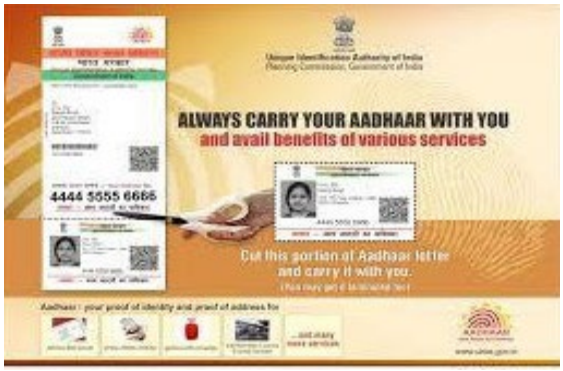
生体認証式背番号カード制といえば、インドの「アーダール(Aadharr)」がある。アーダールでは、国民監視のための生体認証データとしては、本人の顔面＋目の虹彩＋10 本の指の指紋を使う。申請は、原則任意だが、福祉の受給には 12 桁の番号附付き紙カード取得は必須である。申請には、生体情報を含む、次のような個人情報の提出を求められる。

①**身元確認のための個人情報** **【必須】**氏名・住所・生年月日(年齢)・　性別 **【選択】**携帯電話番号・電子メールアドレス
②**生体情報** **【必須】**顔面・2 つの目の虹彩・10 本の指の指紋
③**5 歳以下の子どもの場合**　上記①・②＋両親/保護者の氏名

●インドのアーダール　顔や目の虹彩の採取現場（Public Use）

実は、インドでのアーダール（生体認証式背番号カード制）導入は、日本の IT 企業の協力で実現した制度である。（CNN ニューズ 91 号）http://www.pij-web.net/cnn/CNN-91.pdf。わが厚労省の顔認証データのマイナンバー管理計画は、いわば“日本版アーダール”の裏口導入とみてとれる。

ちなみに、インドのアーダールカードは、プラステック（ラミネート） カードでも、ICカードでもない。わが国のマイナンバー（個人番号）の通知カード（廃止）と同じく紙製。紙製のカードは、各人が自宅や勤め先、ネットカフェなどにある PC（パソコン）などで中央センター（サーバー）にアクセスし、プリンターでプリントアウトできる。IC カードを使っていないのは、インドでは、住所のない人も多いのと、郵便事情が悪く、郵送は難しいからだ。



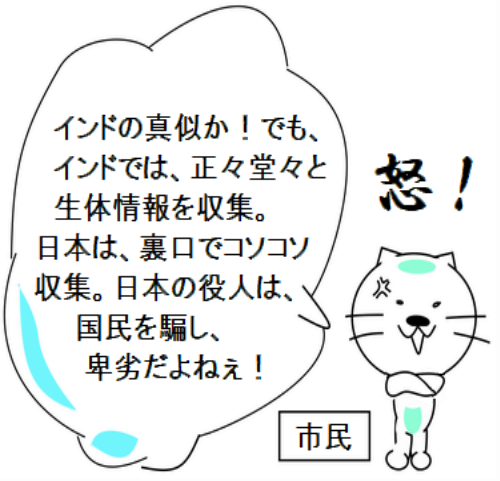
●アーダールカード切り取り使用の PR (public use)

アーダールカードでは、当初バーコードを使っていた。しかし、現在では、QR コードを使っている。QR コードは、日本発の技術である。このことから、このアーダールシステムプログラムには、NEC のような日本 IT 企業が関与していることがわかる。

●アーダールは QR コードが核（Public Use）

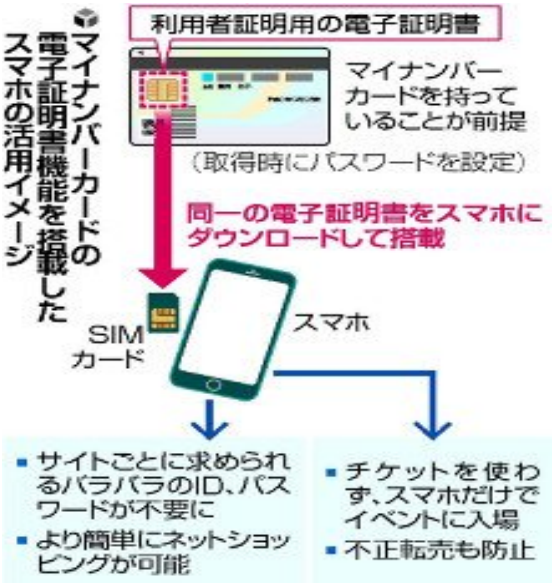
紙製のカードに記載された二次元バー（QR）コードを使ってデータを集積するサーバーと交信・照合し、本人確認をする仕組みだ。本人確認の現場では、指紋と QR コードリーダーを使っている。

インドではやっていいことでも、プライバシーや人権を大事にするように求められるわが国ではやってはいけないことがある。このことを、IT 企業は心しないといけない。政府も同じである。

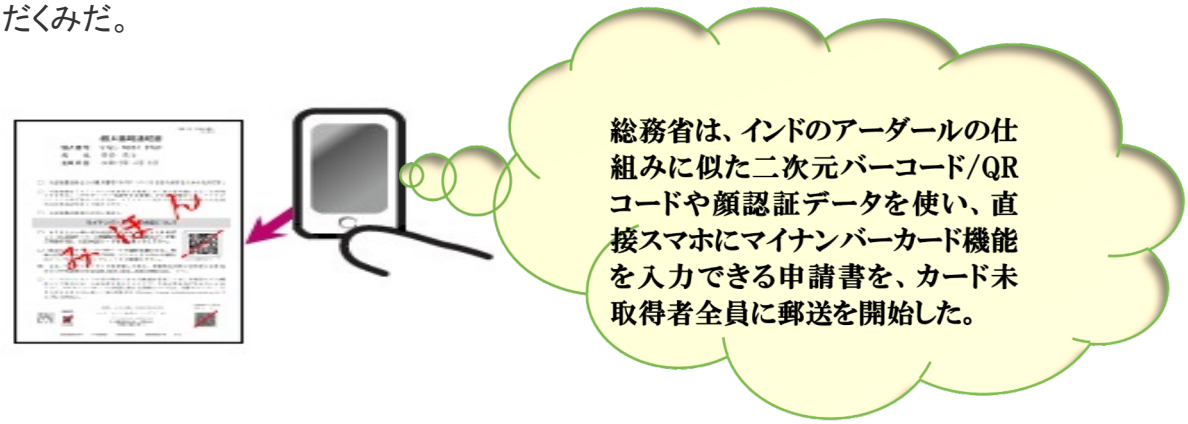


◆危ない QR コード・顔認証情報使用のマイナカードのスマホ申請

国民全員に IC カードの通行手形（国定身分証）を持たせようという政府の悪だくみは、まだまだある。総務省が、J-LIS/ジェイリスをダミーに使って、20 年 11 月末から、マイナンバーカード/マイナ IC カードの未取得者　約 8,000 万人に、スマホ申請書を発送したことだ。コロナ禍で財政逼迫が危惧されるなか、国の役人の悪巧みで、またもや血税の浪費がはじまっている。以前から、国は、下記のようなマイナンバーカードから電子証明書機能をスマホに移転するイメージを公開している。



今度は、QR コード・顔認証情報を使ってマイナンバーカードのスマホ申請を促す悪だくみだ。



この手続では、申請者は、まず、スマホのカメラで交付申請書の QR コードを読み取り、申請用 WEB サイトにアクセスしてメールアドレスを登録する。

顔写真登録

次に、登録されたメールアドレス宛に通知される申請者専用 WEB サイトにアクセスし、スマホのカメラで撮影した顔写真を登録（あらかじめ撮影しなくても操作中に撮影可能。）する。

そして、画面の案内に従い、必要事項を入力し送信すると、登録したメールアドレス宛に申請が完了した旨のメールが届き申請完了する。

「こりゃ、簡単で便利だ」と考える人がいるだろう。「いや、待てよ。国民の顔認証情報

を裏口入手、国家管理が狙いだ」と考える人もいるだろう。

いずれにしろ、EU（欧州連合）などは、生体認証情報を収集するにあたり、事前に本人に利用目的、収集と保存の期間を通知し、個別に同意を得ていること（オプトイン方式）を要件としている。つまり、嫌な人は個別に申し出て収集に協力しなくともよいとするやり方（オプトアウト方式）は違法とされる。わが国は、先進諸国の生体認証のプライバシー保護の作法を学ぶべきである。

○オプトイン方式【参加したい人だけが同意する仕組み】
×オプトアウト方式【参加したくない人は申し出る仕組み】

今般の AI 規制規則案で禁止される AI システムまたは高リスク AI システムの利用にあたるのではないか。ガバナンスゼロの AI システム利用で、文明国失格である。

◆問われる東京渋谷区での NINE 依存で顔認証データの利用

CNN ニューズ104号でも紹介しているように、東京都渋谷区は20年度から住民票の写しや課税証明書などの発行申請をライン/LINEの区公式アカウントで受け付けている。本人確認はスマホを活用したオンラインシステムを活用するほか手数料もライン/LINEで決済し、証明書は自宅に郵送する。渋谷区は、ライン/LINEを活用した住民サービスの拡充を計画している。21年度からは、新たに国民健康保険の申請やオンライン健康相談の受付を始める。サービスを現在の9種類から21年度には15種類に増やすという。

（https://www.city.shibuya.tokyo.jp/kusei/koho/line/line_shinsei.html）。

CNN ニューズ105号ですでにふれたように、とりわけ、渋谷区が採用するスマホ、ライン/LINEのアプリでは、マイナンバーカードなしで本人認証ができるとはいうものの、本人認証には eKYC（electronic Know Your Customer）」という顔認証、生体認証データを使う。生涯不変の生体認証情報の取り扱いについては、慎重を期する必要

がある。軽い気持ちで住民の生体認証情報を官民で分かち合ってはいけない。EU の GDPR（一般データ保護規則）や、今般の AI 規制規則案で禁止される AI システムまたは高リスク AI システムの利用にあたるのではないか。

【図表20】リモートアクセスで使われる認証方式：主要なデータセキュリティ対策

認証方式	導入コスト	利便性	なりすまし対応度	マイナス面
❶固定パスワード	低	高	低	安全度が低い
❷PKI（公開鍵・電子証明書）	中	低	高	運用が煩雑
❸ワンタイムパスワード	高	高	高	コストが割高
❹生体認証	高	高	高	容認度が低い
❺その他（マトリクス認証等）				

さらに、今般のライン/LINE のズサンな個人データ管理実態の発覚は、官民連携、実質民間 IT 企業への丸投げで進める自治体の軽率な“住民データの名ばかり厳正管理”の危うさ、甘さに大きな警鐘を鳴らしている。顔認証データを海外に保存しているとすれば、大きな問題だ。住民の人権保護を置き去りにして、法令遵守、グローバルな個人データ管理水準に達していない民間 IT 企業に依存を強める多くの自治体の危うさが浮き彫りになっている。

顔写真の撮影・アップロードや本人確認書類で本人確認を行う［出所：渋谷区公式 Web サイト］

ただ、総務省（前総務大臣）は、マイナンバーカード搭載の「公開鍵」を使わない渋谷区方式をやめるように渋谷区にコメントを発している。ただ、渋谷区は、総務大臣のコメントを受け入れず、この方式を使い続けている

（https://www.city.shibuya.tokyo.jp/kusei/koho/hodo/message020403.html）。加えて、ライン/LINE はこの件で総務省を相手に裁判を起こしている（https://note.bot-express.com/n/n576bc8f23476）。

もっとも、NTTドコモやヤフー、楽天、メルカリ、日本マクドナルド HD、グーグル、フェイスブックなど国内で利用者が多いアプリの運営IT企業の多くは、国内ユーザーの個人データを海外に移転・保存、海外からのアクセスが可能である。なぜ、対話アプリのライン/LINE だけが集中砲火を浴びたのであるか？総務省にとり、ライン/LINE は役所の言うことをきかない生意気な存在に映っているはずだ。今回の事件は、ライン/LINE に役所の軍門にくだるように暗に促す好機なはずだ。行政指導に加え、個人情報保護委員会のような自称“独立機関”、実質“政府ご用達機関”を動員し、厳しく対処している。この事件については、深読みが要る。過去には、日本年金機構も同じような問題を起こしている。だが、この件では、総務省は静観し、むしろ沈静化するのを待っているような感じであった。

菅政権のデジタル国家総動員体制つくりで、役所にとり、人権に小うるさい外国資本のデジタルプラットフォーマーは使い勝手がよくないはずだ。民族資本のデジタルプラットフォーム事業者であるライン/LINE を手なずけることは大事なはずだ。今回の事件を必要以上にフレームアップすることで、“転向”、“中国スタイルの国家に忠実なプロバイダー役”を期待しているようにもみえた。

いずれにしろ、渋谷区におけるデジタル行政サービスの本人認証に eKYC（electronic Know Your Customer）」というAIシステムのもと生涯不変の顔認証、生体認証データを使うことは、人権に大きなインパクトを与えるものである。この区のトップや現場の担当者に、こうした認識があるのかどうかが問われている。EU の AI 規制の基準によれば、禁止される AI システムの利用または高リスク AI システムの利用にあたるのではないか。とすれば、仮にこの種の顔認証情報の利用がゆるされるとしても、オプトイン方式【参加したい人だけが同意する仕組み】の徹底、顔認証 AI システムの法適合性評価やその評価結果を一般住民が監視で切る仕組みや堅固なガバナンスの確立などが求められる。

◆子どもの学習成績をマイナバーで AI 国家管理 ～問われる人格権のポイント評価

政府は義務教育の対象である小中学生の学習履歴やテストの成績をマイナンバーで紐づけしてオンラインで管理する仕組みづくりをはじめる。2023 年度にも試行開始の方向だ。教育ビッグデータをストックし、指導方法の改善や教育政策の検証に役立てるのが狙いだという。

AI を使ったスコアリングシステム・社会信用ポイント制（social scoring/個人の行動

や人格的特性などに基づき、国家が個人の信頼性などを格付けする AI システム）も最たる例である。EU の AI 規制規則案（5条）で厳禁されるスコアリングシステム・社会信用ポイント制につながるのではないか。

20 年 12 月 1 日に、政府の教育再生実行会議が設けた「デジタル化タスクフォース（TF）」が第 3 回会議を開き、ICT 化に必要な課題次のようにまとめた（https://www.kantei.go.jp/jp/singi/kyouikusaisei/jikkoukaigi_wg/digital_tf/dai3/siryou1.pdf）。

①学習履歴（スタディ・ログ）の活用
②教育ビッグデータの効果的な分析・利活用の推進
③ICT 活用の抜本的拡充に対応した情報基盤のあり方
④デジタル技術による教育手法や学務の高度化・効率化
⑤デジタル化の担い手となる人材育成
⑥その他

これらの課題のうち、①と②を、マイナンバー活用の対象にするようだ。だが、ちょっと待った！である。こうした課題に挑戦するにしても、成績をマイナンバーで紐づけしてオンラインで管理する必要などまったくないはずである。

子どもたちの成績のマイナンバー管理は、極めて重大な人権問題である。マイナンバー管理しないと、子どもたちの学習成績をビッグデータとして AI システムで活用したり、オンライン教育の推進ができないわけではない。そもそも、国家が個人の成績などの個人情報を背番号で一生涯集約管理するなど、民主国家ではやってはいけないことである。マイナンバーを使った子どもの成績の国家管理システム、AI 評価は人権侵害で、憲法違反である。

また、EU の AI 規制規則案によると、禁止される AI システム利用にあたる。先進文化国家を目指すのであれば、こんな愚策は直ちにやめないといけない。恥ずかしい限りである。政府の教育再生実行会議が設けた「デジタル化タスクフォース（TF）」のメンバーに、世界の AI 規制の動き、AI 倫理、AI リテラシーを叩き込むための再教育が要るのではないか。

●むすびにかえて

今般の欧州委員会（European Commission）がまとめた AI 規制規則案（AI 法案）は、たたき台である。今後、EU 理事会（EU Council）や欧州議会（European Parliament）で、中身が精査される。AI 法案については、さまざまな疑問符がついている。とりわけ、バイアスのかかったアルゴリズムの排除、不公正な評価が出た場合その結果を個々の被害者に通知する仕組みや一般市民がチェックする仕組みが未整備であることが指

摘されている。また。市民団体からは、利用が禁止されるはずの AI 顔認証監視カメラやライブ遠隔顔認証 AI システムについて法執行機関への適用除外が広すぎるとの強い批判もある。

EU の AI 規制規則案は、人間不在の IA 開発や AI を使ったデジタル国家主義、市場社会主義の流れにストップをかけることが狙いである。ヨーロッパの民主的な価値観の保全、自由や基本的人権の尊重、民主主義の原則、オープンな社会の保障などがキーワードである。AI システムのプロバイダーもユーザーも、このキーワードを常に復唱しながら、AI の開発・利用を進めようというものである。いわば「人格権をむしばむ AI パンデミック」にストップをかけるための画期的な“ワクチン”にあたるとみてよい。

AI 規制規則案は、EU 域内、あるいは EU 加盟国のみならず、EU 域外（第三国）にありながらも、EU 域内にいるユーザーを対象に AI システムの販売や AI システムのサービスを提供する IT 企業（プロバイダー/開発者）、ユーザーなどにも大きな影響を及ぼす。いわゆる「域外適用（extraterritorial application）」が想定されている。にもかかわらず、AI ガバナンスの仕組みが、各加盟国ベース主導でデザインされ、ワンストップ・ショップ体制（one-stop-shop mechanism）になってはいない。AI システムのオペレーター/運営管理者（プロバイダー・ユーザー・授権代理人。輸入者・販売者）にフレンドリーな仕組みではない、との指摘もある。また、一般法である GDPR（一般データ保護規則）と特別法である AI 規制規則案とのガバナンスやコンプライアンス上の連携を強化すべきである、との声もある [25]。

わが国の現在の政権は、外圧があっても変われない。外圧がなければもっと変われない。まさに、デジタル監視国家主義の中国の政権と似ている。人権をむしばむ「マイナンバーパンデミック」を流行らせ、グローバルの通用しない入管法改正を闇雲に強行する。自由と人権尊重を第一とする憲法にまで触手を伸ばす。この国のガバナンスゼロ、人権反故は当り前の政府や IT 企業の姿勢を改めさせるためには、国際的な経済制裁が要るのかもしれない。家電メーカーの“イメージ”が“売り”のパナソニックなどは、AI ビジネスの核を、人間の大量監視を狙いとする監視カメラ事業から、もっと倫理観ある事業に大きくシフトすべきではないか。EU の AI 規制規則案は、国際水準に到達できないわが国の IT 企業や政府に対してある種の経済制裁として効き目を表すに違いない。

ちなみに、わが国の経団連は、EU の AI 規制について、以前から「イノベーションの阻害要因となる恐れがある」との見解を固守している [26]。

---

[25] See, Mark MacCarthy & Kenneth Propp, “ Machines learn that Brussels writes the Rules: The EU’s New AI regulation,” (May4, 2021, Brooking Institution). https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

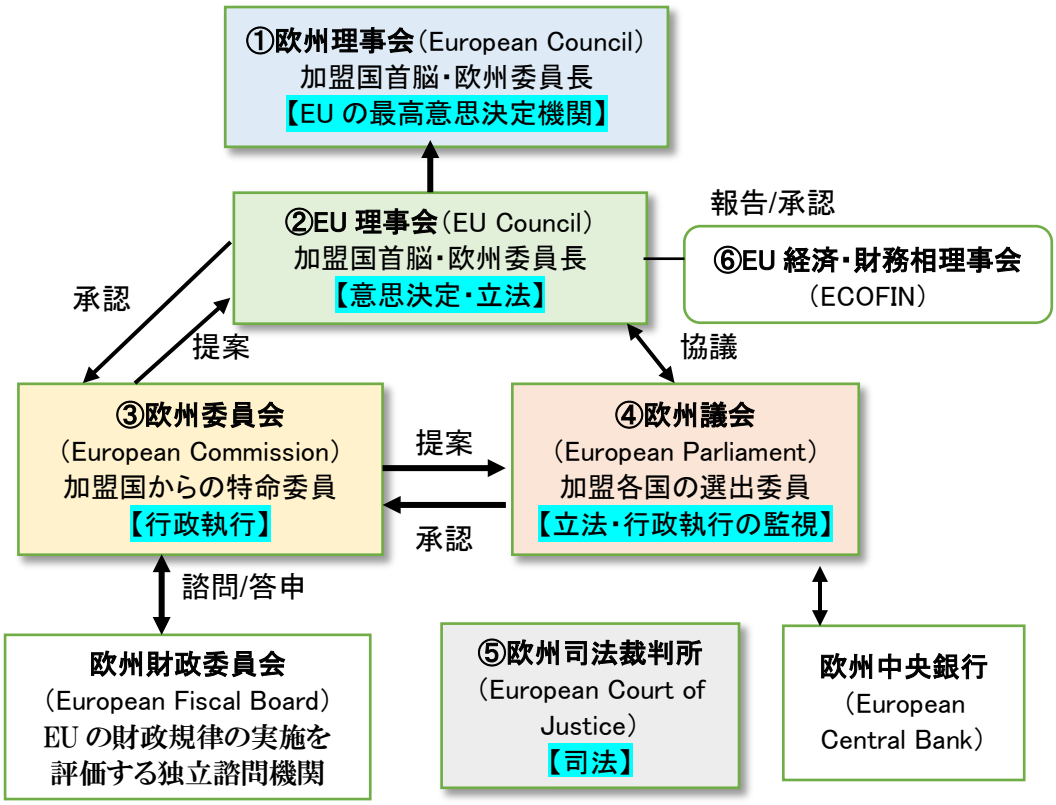
[26] 経団連：欧州委員会“White Paper on Artificial Intelligence:a European approach to excellence and trust”への意見（2020-06-10）(keidanren.or.jp)

【添付資料】

●もっと知りたいEUの統治機構と法制度

わが国は、比較的に厳格な三権分立を採用している。しかし、国家連合であるEUは、必ずしも権力分立がすっきりしているわけではない。EUの統治機構と主な機関（財政関連）を図示すると、次のとおりである。

【図表A】EU/欧州連合（EU=European Union）の統治機構と主要機関（抜粋）



＊EUには、理事会（Council）、議会（Parliament）および委員会（Commission）という機関がある。それぞれのトップはすべて英語で「President」と呼ばれる。駐日欧州連合（EU）代表部 https://eeas.europa.eu/delegations/japan_jaでは、これら3人のPresidentsの日本語を区別し、次のように邦訳（和訳）している。

【図表B】駐日EU代表部の「President」の邦訳方針

・①②理事会（Council）&④議会（Parliament）の President ➡「議長」
・③委員会（Commission）の President ➡「委員長」

＊もちろん、他の邦訳（和訳）も可能

【図表C】EU/欧州連合(EU=European Union)の主要な機関の特質

①欧州理事会(European Council)
EU加盟国の首脳(大統領や首相)、欧州委員会委員長(Commission President)、常任議長を構成員とするEUの最高意思決定機関である。EU首脳会議、EUサミットとも呼ばれる。トップは、欧州理事会議長(European Council President)。 **＊EUの立法機関であるEU理事会(EU Council)や、 EUとは別の機関である欧州評議会(CoE=Council of Europe)と混同しないように注意が必要。**
②EU 理 事 会/欧 州 連 合 理 事 会(Council of the European Union/EU Council)
EU 理事会は、EU の機関である。主な任務は、欧州議会 (EP=Parliament)と共同で立法をすることである。EU 加盟国の政府閣僚級代表(1 人)で構成されている。閣僚理事会とも呼ばれる。政策分野ごとに設置された委員会で活動する。トップは、EU 理事会議長 (President of the EU Council)。 **＊「EU 理事会(EU Council)」は、EU の最高意思決定 機関である「欧州理事会(European Council)」や、 EUとは別の機関である「欧州評議会(CoE=Council of Europe)」と混同しないように注意が必要。**
③欧州委員会(European Commission)
欧州委員会は、EU 基本条約の規定に基づき設置された行政執行機関である。EU 基本条約の守護者として、欧州全体の利益を代表し、法令の立案、政策や法令の執行、国際条約の交渉などを任務とする。「EUの政府、 あるいは内閣」のような存在である。トップは、委員長 (President of the European Commission)である。
④欧州議会(EP=European Parliament)
EPは、EUの立法機関である(ただし、立法権限は、 EU 理 事 会(EU Council)と共有 している。)。 すなわち、条約遂行に必要なEU法の提案は、基本条約に個別に規定されたものを除き、通常、欧州議会 (EP=Parliament)およびEU理事会(EU Council)が 共同で提案・審議・採決する。ほかにEUの行政執行活動を監視する責務を担っている。EPは、欧州市民の利益を代表する機関で、5 年毎の直接選挙で選ばれる議員で構成される。トップは、欧州議会議長(President of the EP)である。
⑤欧州司法裁判所/ECJ(European Court of Justice)
欧州司法裁判所(ECJ)は、EU 基本条約(TEU)およびEU 運営〔機能〕条約(TFEU)に準拠して設立された EU の裁判所である。EU 基本条約(一次法)や EU 法令(二次法)の適切な解釈を通じて、域内でEU法を公平に適用する任務を担っている。①司法裁判所(Court of Justice【法律審裁判所で、一般裁判所または専門裁判所の裁決に対する上訴事件(ただし上訴は法律問題 を争う場合に限られるす)などを管轄する(TFEU 256条1項後段)、②一般裁判所(General Court/事実審)、 ③専門裁判所〔specialised court/EU 公務員審判所 (European Union Civil Service Tribunal)〕の3つの部門からなる。欧州司法裁判所(ECJ)は、欧州共同体設立条約(TEEC)により、

EU 法について排他的に判断する権限が与えられ、統一的な法の適用・解釈を行っている。また、ECJは、先行判決（先決的判決）制度（References for preliminary rulings）（TEEC 267条）に基づき、EU 法と加盟国の国内法との解釈等など各種法律問題に関する鑑定や助言をする権限を有する。競争法関係を含め、欧州委員会（Commission）の 決定を審査するとともに、加盟国の国内裁判所の付託を受けて、EU 法の解釈について先行的判決を下すことができる。加盟国が基本条約（一次法）や二次法 （指令や規則など）に定められている義務を履行しない場合には、欧州委員会（Commission）の求めに応じ、 ECJは、違法状態の認定を行ったり、違法とされた当該加盟国が対応しないときには、高額の罰金を科したりすることによって、各種法令、とくに基本条約の遵守を求めることができる。欧州司法裁判所（ECJ）は、 TEEC 220条に基づき、27人の判事と 8人の法務官で構成される。加えて、事務を統括する事務局長（任期6年、再任可能）を任命している。ルクセンブルグに所在する。現在の正式名称は、CJEU=Court of Justice of the European Union（欧州連合司法裁判所）である。

＊欧州司法裁判所（ECJ）は、欧州評議会（CoE）の人権救済機関欧州人権条約（Convention for the Protection of Human Rights and Fundamental Freedoms） 上の審理を行う欧州人権裁判所（ECtHR=European Court of Human Rights）〔EU評議会（CoE＊）の人権救済機関〕とは別の司法機関である。 混同しないように注意が必要。

＊欧州評議会（CoE=Council of Europe）

欧州評議会（CoE）は、 1949年に設立された人権・デモクラシー・法の支配などについて国際基準を策定・評価する目的でヨーロッパに設立された国際機関である。専門家会議の開催、国際問題に関する勧告や決議の採択、それらのモニタリングなどを責務としている。現在 47か国が参加している。日本もオブザーバー参加している。

1953年発効の欧州人権条約（European Convention on Human Rights）に基づき創設された欧州人権裁判所（ECtHR=European Court of Human Rights）は、欧州評議会（CoE）の機関である。

＊欧州評議会（CoE）は、EU の機関ではない。 EU 理事会（EU Council）や欧州理事会（European Council）などと混同しないように注意が必要。

⑥EU 経 済・ 財 務 相 理 事 会（ECOFIN= Economic and Financial Affairs Council）

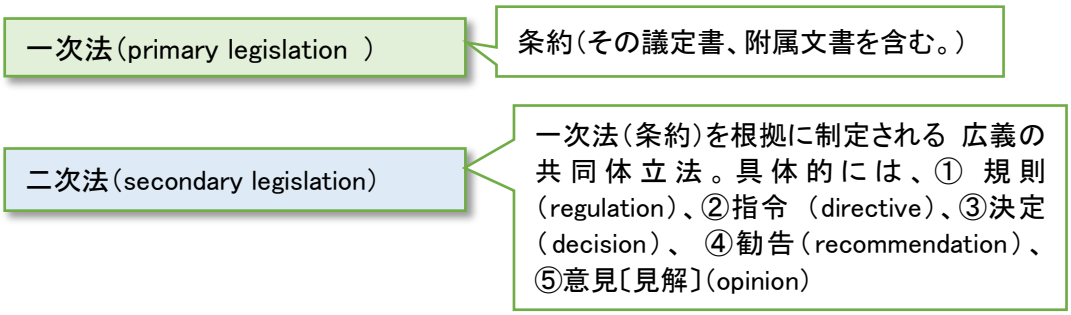
ECOFINは、 EU 加盟国の経済・財務相が出席し、経済政策の調整などを行う閣僚理事会である。毎月定例で開催される。経済サーベイランスに加え、加盟各国の予算政策・財政の監視、金融市場・資金移動、などの諸問題に関する経済政策指針を策定する。また、欧州議会（EP=European Parliament）とともに EUの予 算編成・決定に関与する。

≪EU法とは何か≫

「EU 法とは何か」。英語でいうと、「What is sources of EU law)」。「sources of law」の言葉は、一般に、「法源」と邦訳される。法的拘束力を有する規範(norm)(さらには、法的拘束力のない法形式も含む。)を指す。「EU 法(sources of EU law)」は、「一次法(primary legislation/primary law)」と「二次法(secondary legislation/secondary law)」からなる。 双方をやさしく図にすると、次のとおり＊。

＊詳しくは、石村耕治「Q&A: 現代EU財政法入門塾」JTI税務ニューズ4号参照
988ed1d79a9043157de4814ac2ac2917.pdf (jti-web.net)

【図表 D】EU 法の基本体系



【図表 E】種類の共同体立法(二次法)の違い

①規則(regulation)
EU の「規則」は、加盟国の国内法に優先して、加盟国の政府や企業、個人に直接適用 される。すなわち、加盟国の政府等を直接法的に拘束する。このため、加盟国の国内立法は不要である。2009 年 12 月のリスボン条約によって EC は廃止され、 今まで法の制定ができなかった EU は、法制定が可能な EC の地位を継承した。規則の名称は、複雑である。 やさしくまとめると、次のようになる。 欧州共同体(EC＝European Community)→欧州連合(EU＝European Union)。2009 年末までは、例えば、Regulation(EC)No 1466 /97。2010 年以降は、例えば、Regulation(EU)No 1173/2011 は、加盟国の国内立法が必要である(EU 条約 24 条 3 項・ 10 条 1 項)。つまり、一定期間内(EU 官報掲載後 3 年以内)に加盟国の国内法に置き換えられなければならない。 加盟国には一定の範囲内で立法裁量がある。
②指令(directive)
EU の「指令」は、加盟国政府に対して直接的な法的拘束力があるが、企業や個人には直接適用されない。個々の加盟国に効力を及ぼすには、加盟国の国内立法が必要である(EU 条約 249 条 3 項・10 条 1 項)。すなわち、一定期間内(EU 官報掲載後 3 年以内) に加盟国の国内法に置き換えられなければならない。 加盟国には一定の範囲内で立法裁量がある。

③決定（decision）
EU の「決定」は、特定の加盟国の政府や企業、個人に対して直接適用される。対象となる加盟国の政府等に対して直接的な法的拘束力を及ぼす。性格的には“行政上の処分”とみてとれる。
④勧告（recommendation）
EU の「勧告」は、欧州委員会（Commission）が加盟国の政府や企業、個人などに一定の行為や措置を取ることを期待する旨の表明である。原則として法的拘束力はない。性格的には一種の“行政措置”とみてとれる。
⑤意見〔見解〕（opinion）
EU の「意見〔見解〕」は、 特定のテーマについて欧州委員会（Commission）の意思の表明である。「勧告」と同様、原則として法的拘束力はない。性格的には一種の“行政措置”とみてとれる。

＊TCフォーラム研究報告2021年5号（2021年5月）「EUの包括的AIシステム規制始動」は、あくまでも会員の学習・研究目的での資料であり、内容の正確性や完全性を保証するものではない。したがって、この点について、著者は一切の責任を負わない。読者は、AI法務実務においては、法務専門職のアドバイスを受けるように推奨する。