基礎研レポート

EU の AI 規則(1/4)

―総論、定義、禁止される AI の行為

保険研究部 専務取締役 研究理事　松澤　登
(03)3512-1866　matuzawa@nli-research.co.jp

1――はじめに

EU の AI 規則（(EU) 2024/1689。以下、本規則）は当初案が 2021 年 4 月 21 日に欧州委員会により公表された。その後、欧州委員会、EU 理事会、欧州議会の間で非公式交渉が行われていた。

2023 年 12 月 9 日、3 者間での非公式交渉で本規則の修正案が合意された。最終的には 2024 年 6 月 13 日に本規則が正式に EU ジャーナル（日本の官報に該当）に掲載され、同年 8 月 1 日に発効した。

本稿では本規則を解説することを目的とするが、内容が多岐にわたるため、4 回のシリーズ物としたい。本稿は全 4 回のうちの 1 回目である。

まず、本規則の目的であるが、「域内市場の機能を向上させ、人間中心の信頼できる人工知能（AI）の導入を促進することである。同時に、域内における AI システムの有害な影響に対して、健康、安全、民主主義、法の支配、環境保護など、憲章に謳われている基本的権利の高水準の保護を確保し、イノベーションを支援することである」とする(1 条 1 項、下線筆者、以下同じ)。

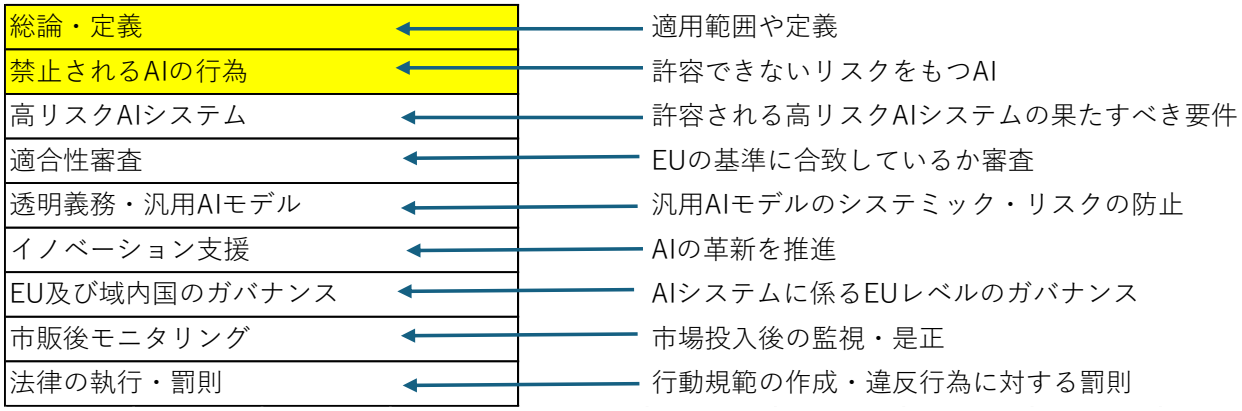
すなわち、「民主主義、法の支配、環境の保護を含む、健康、安全、欧州憲章に明記されている基本的権利を高水準で保護しつつ、技術革新を促進する」（本規則の前文（以下、前文という）1）ところに本規則の目的がある。前文は規則の制定理由についてさらに「域内市場における AI の開発、使用、普及を促進すると同時に、健康や安全といった公共の利益や、民主主義、法の支配、環境保護など、域内法で認められ保護されている基本的権利の保護といった公共の利益を高いレベルで守るためには、AI に関する調和された規制を定めた域内の法的枠組みが必要である」(前文 8)とする。

解説にあたっては、全条文を解説するのではなく、筆者が重要と考えた条文のみ取り上げた。また取り上げた条文であっても読者の理解のため、一部を省略したり、わかりやすい表現に意味の変わらない範囲で修正したりしているので、あらかじめお断りしておく。解説にあたっては、前文を引用することを中心に、条文の意図を明らかにする方法をとる。

なお、レポートが全 4 回にわたることから、本規則のどこを解説しているかを示すため、図表（下

記図表 1）をそれぞれの個所で表記する。

【図表 1】本規則で解説する部分の全体像

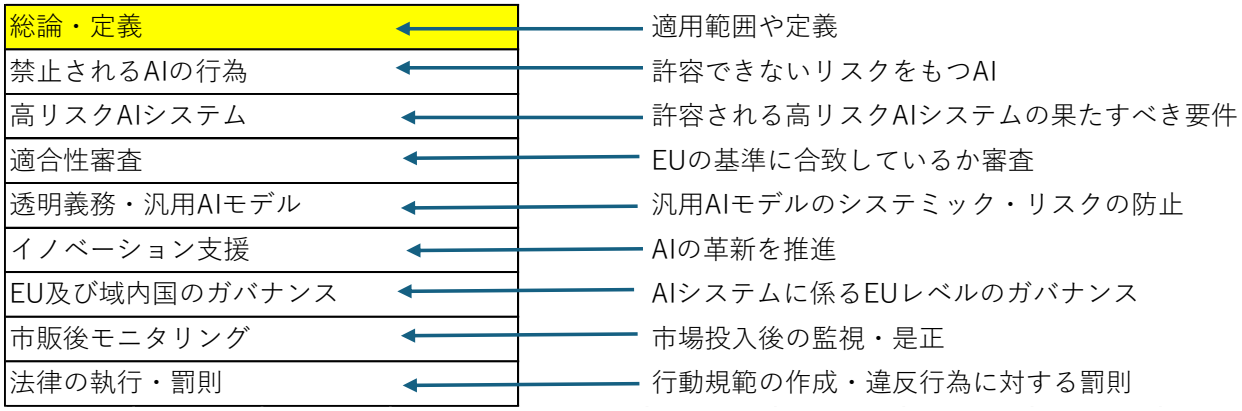


本稿では色塗りの部分、すなわち「総論・定義」「禁止される AI の行為」を解説する。

2――総論

本項は総論部分についてであり、本規則の適用範囲、適用除外、定義等について解説する（図表 2）。

【図表 2】本項 2 の解説部分（色付き部分）



1｜本規則の適用範囲

本規則が適用される主体は、主には「提供者」「配備者」である。具体的には主に以下の通りである（2 条 1 項）。

(a) AI システムそのものを市場投入し、AI システムのサービスを開始し、または汎用 AI モデル[1]を市場投入する提供者(provider)。これらの提供者が域内に設立されたかどうか、所在しているかどうか、第三国に所在しているかどうかを問わない。

[1] 汎用 AI モデルは AI システムの一分類であるが、特別な規定が適用されるため、本条では AI システムとは別に掲げられている。なお、モデルという用語とシステムという用語の相違だが、AI モデルを一要素として組み込んだものが AI システムと呼ばれる。

(b)域内に事業所(place of establishment)を持つか、または域内に（本部が）所在する、AI システムの配備者(deployer)。
(c) その AI システムによって出力されたアウトプットが域内で使用がされている、 第三国に事業所を置くか、または第三国に所在する AI システムの提供者および配備者
(d)AI システムの輸入・販売業者
(e)製品メーカーであって自社の製品とともに、自社の名称または商標の下で、AI システムを市場に出したり、サービスを開始したりする者
(f)EU 域内に設立されていない提供者の認定代理人
(g)EU 域内に所在する被害者
　この適用範囲の条文を理解するには、AI システム、汎用 AI モデル、提供者、配備者などの定義を確認しなければならないが、それは次項で解説する。

2｜若干の定義

(1)AI システム　まず、AI システムという用語であるが、これは本規則を理解するための基本となる概念である。AI システムとは、さまざまなレベルで自律的に動作するように設計され、配備後に新たな状況に適応することができる機械ベースのシステムであって、かつ、明示的または暗黙的な目的のために、予測、コンテンツ、推奨、または決定（これらは物理的または仮想的な環境に影響を与える）などの出力をどのように生成するかを、受け取った入力から推論するもの(3 条 1 項)というものである。
　（注記）この条文はほぼ直訳している。この条文を読んでも即座に AI システムが何かを理解することは難しいが、前文によれば、AI システムの主要な特徴は推論能力であるとする。この推論能力とは、「物理的・仮想的環境に影響を与えることができる予測、コンテンツ、推奨、決定などの出力を得るプロセスのことであり、入力やデータからモデルやアルゴリズム、あるいはその両方を導き出す AI システムの能力」（前文 12）のことであるとする。要するに与えられた情報から物事の答えを導き出す人間の脳のような働きをするシステムを AI システムと呼ぶということになる。なお、AI システムの定義は世界的に定まったものはないようであり、たとえば日本の AI 事業者ガイドラインでは、AI システムは「活用の過程を通じて様々なレベルの自立性をもって動作し学習する機能を有するソフトウェアを要素として含むシステムとする」とされている。推論能力には触れておらず、これだけを見ても AI を定義する難しさがわかる。

(2)汎用 AI モデル　汎用 AI モデルとは、AI モデルであって、大規模な自律監視のもとで大量のデータで自己学習する場合を含み、有意な汎用性を示し、広範で明確なタスクを適切に実行することができるものを指す（3 条 63 項）と定義されている。
　（注記）これまでは、たとえば囲碁の AI ソフトや自動車の自動運転 AI のように、特定の目的に対して、特定のタスク（仕事）を実行する AI であったが、ここでいう汎用 AI モデルとは人間のようにあらゆる種類（「有意な汎用性」「広範で明確なタスク」）のタスクをこなすことができるというものである。

汎用AIモデルにはChatGPTのような生成AIが該当する可能性があるが、詳細は第3回レポートを参照のこと。

(3)提供者　提供者とは、自然人もしくは法人、公的機関、代理店またはその他の団体であって、AIシステムまたは汎用AIモデルを開発し、あるいはAIシステムまたは汎用AIモデルを他者に開発させて自己の名称・商標の下でAIシステムを市場に投入しまたはAIシステムを稼働させる者を意味する(3条3項)と定義されている。

（注記）要するに提供者は、自社でAIシステムを開発したかどうかを問わず、AIシステムを自社の名義で市場に投入しサービスを提供またはAIシステムを稼働させる者を指す。

(4)配備者　配備者とは、自然人または法人、公的機関、代理店またはその他の団体が、自身の権限に基づきAIシステムを使用する者を意味する。 ただし、AIシステムが個人的な非職業活動の過程で使用される場合は除かれる(3条4項)

（注記）配備者とはAIシステムのユーザーである。ただし、業務上で利用するものでなければならない。したがって生成AIを個人として私的に利用している場合には本規制の適用はない。他方、会社（あるいは個人事業主）として生成AIを業務上導入している場合は配備者に該当する。

(5)輸入業者　輸入業者とは第三国に設立された自然人または法人の名称または商標を付したAIシステムを域内市場に流通させる、域内に所在または設立された自然人または法人を意味する。
(注記)EU域外で開発流通するAIシステムは原則として本規制の対象外だが、そのAIシステムをEU域内市場に流通させる事業者は輸入業者として本規則の対象となる。

3｜本規則から除外されるもの

本規則から適用除外されるものとしては以下がある。
(1)付属書ⅠB(次項、図表3参照)に掲げる民間航空の安全性に関する規則、農業用車両に関する規則、二輪、三輪、四輪車両に関する規則など、8種類のEU規則・指令の適用のある製品にかかわるAIシステムであって、高リスクAIシステム(6条1項)に該当するものについては、本規則は一部の規定を除き、適用除外されることとなっている（2条2項)。

これらのAIシステムに具体的に適用されるのは6条1項(高リスクAIシステムの分類ルール)、102条から109条である。102条から109条の内容としては、先述8種類のEU規則・指令を改定して、本規則のⅢ章2節(8条～15条、高リスクAIシステムの要件)の規定を踏まえ、高リスクAIシステムの要件に関する規定を導入すべきことを定めている。
(注記)付属書IBにあげられた8種類のEU規則・指令が適用される製品については、本規則を直接適用するのではなく、本規則の高リスクAIシステムに係る規定と同様の内容をそれらの8種類のEU規則の中に規律を導入することで、同様の規律が適用されることとされている。

【図表 3】付属書ⅠB に掲げる規則

民間航空安全分野における規則
二輪車、三輪車、四輪車の認可と市場監視に関する規則
農業・林業用車両の承認と市場監視に関する規則
船舶機器に関する指令
鉄道システムの相互運用性に関する指令
自動車及びトレーラー、自動車を対象とするシステム、部品及び個別技術ユニットの承認及び市場監視に関する規則
自動車及びトレーラー、自動車を対象とするシステム、部品及び個別技術ユニットの安全性および車両乗員・交通弱者の保護に関する型式承認要件に関する規則
民間航空分野における共通規則および欧州連合航空安全機関の設立に関する規則

(2)軍事、防衛、国家安全保障の目的のみに使用される AI システム(同条 3 項)

(注記) 軍事・防衛目的に関する AI システムは、本規則から適用除外されている。このように除外されている理由としては、前文において「欧州連合条約(THE TREATY ON EUROPEAN UNION、TEU)4 条 2 項(加盟国の国家安全責任)によって、また、TEUⅤ章 2 節によってカバーされる加盟国および EU 共通の防衛政策の特殊性によって(適用除外が)正当化される」。また、「国家安全保障の目的に関しては、国家安全保障が TEU 第 4 条第 2 項に従って加盟国が唯一の責任主体であり続けるという事実と、国家安全保障活動の特定の性質と運用上の必要性、およびそれらの活動に適用される特定の国内規則の両方によって、(AI 規則からの)除外が正当化される」(前文 24)とする(カッコ内は筆者追記)。国家安全保障あるいは軍事という側面にあっては、人権保障が最大限に尊重される一般的な AI システム規制には本質的に馴染まず、その構築や監視の責任は国家に存在すると位置づけられている。

(3)第 3 国の公的機関または 2 条 1 項に該当する国際機関であって、これら機関が EU または加盟国との間で法施行や司法協力のために国際協調又は協定を締結することにより利用される AI システム[2](同条 4 項)

(注記) 欧州域外国や EU 以外の国際機関が、EU や加盟国と協調して利用する AI システムについては本規則の適用が除外されている。すなわち前文において「情報および証拠の交換を行う外国のパートナーとの既存の取決めおよび将来の協力のための特別な必要性を考慮し、第三国の公的機関および国際機関が EU または加盟国との法執行および司法協力のために EU レベルまたは国内レベルで締結された協力または国際協定の枠内で行動する場合には、当該第三国または国際機関が個人の基本的権利および自由の保護に関して適切な保護措置を提供することを条件として」(前文 22)本規則を適用しないこととされている。なお、EU 内の国家機関、公的団体などが単独あるいは共同で利用する AI システムには本規則の適用がある(前文 23)。

[2] ただし、基礎的な人権尊重と個人の自由を保証する十分な措置が講じられていることが必要(同項)。

(4) 科学的研究開発のみを目的として特別に開発され、使用される AI システムまたは AI モデル（その出力を含む）（同条 6 項）

（注記）純粋な科学研究目的の AI システムについては本規則の範囲外である。前文において「本規則は、イノベーションを支援し、科学の自由を尊重するものであり、研究開発活動を損なうものであってはならない。したがって、科学的な研究開発のみを目的として特別に開発され、使用されるようになった AI システムやモデルを、この規則の適用範囲から除外する」（前文 25）とされている。純粋な研究目的の AI システムは、市場投入されない限り、具体的な人権侵害の可能性が想定されないうえ、AI システムの進歩を促進する理由により本規則から除外されているものと考えられる。

(5) AI システムまたは AI モデルが新規販売または実用化される前の研究、試験または開発活動(同条 8 項)

（注記）前文に該当する記述はないが、研究開発段階にある AI システムが適用除外なのは上記(4)と同様の理由があるからだろう。なお、研究開発段階にある AI システムを実験する制度として、規制のサンドボックス制度等が設けられている。規制のサンドボックス制度については本規則 57 条以下（4 回目のレポートで解説予定）に規定がある。

(6) 純粋に個人的な非事業活動の過程で AI システムを使用する自然人である配備者（同条 10 項）

（注記）業務外の目的で個人が AI を利用する場合には本規則の適用はない。日本の事業者 AI ガイドラインでも AI 利用者は「事業活動において、AI システム又は AI サービスを利用する事業者」と定義されており、本規則と同様の立場をとっている。

(7) フリーおよびオープンソースのライセンスでリリースされた AI システム（同条 12 項）

（注記）このような AI システムが適用除外になる理由について前文に特段の説明はない。なお、「汎用 AI モデル以外のフリーでオープンソースのツール、サービス、プロセス、または AI コンポーネントの開発者は、AI バリューチェーンに沿った情報共有を加速させ、EU における信頼できる AI システムの促進を可能にする方法として、モデルカード[3]など、広く採用されている文書化の慣行を実施するよう奨励されるべきである」（前文 89）とある。フリー・オープンライセンス AI については、明確な規定はないものの、AI システムの技術仕様等を文書化するように努めることが奨励されている。

4｜リテラシー

AI システムの提供者および配備者は、技術的知識、経験、教育および訓練、ならびに AI システムが使用される文脈を考慮し、AI システムを利用する人を考慮し、そのスタッフおよびその代理として AI システムの操作および使用に対処するその他の人の十分な AI リテラシーを、最善の範囲で確保するための措置を講じなければならない(4 条)。

（注記)前文では「基本的権利、健康および安全を保護し、民主的な管理を可能にしながら、AI シス

[3] モデルカードとは AI システムの学習データセットや学習プロセス、偏向等について解説した文書である。

テムから最大の利益を得るために、AI システムに関して十分な情報に基づいた意思決定を行うために必要な知識を、AI システムの提供者、配備者、および影響を受ける人々に与えるべきである」（前文20）とする。AI システムに起因する悪影響を避けるとともに、AI システムからから最大利益を得るために、AI リテラシーは必須と位置付けられている。本条はこのうち、特に AI システムを操作する人のリテラシーを高めるための措置について規定している。

3――禁止される AI の行為

本項で取り扱う部分は禁止される AI の行為であり、下記図表 4 の色付き部分である。人の権利や安全へのリスクが高すぎて許容できない AI システムの行為は禁止される（5 条）。

【図表 4】本項 3 の解説部分（色付き部分）

総論・定義	適用範囲や定義
禁止されるAIの行為	許容できないリスクをもつAI
高リスクAIシステム	許容される高リスクAIシステムの果たすべき要件
適合性審査	EUの基準に合致しているか審査
透明義務・汎用AIモデル	汎用AIモデルのシステミック・リスクの防止
イノベーション支援	AIの革新を推進
EU及び域内国のガバナンス	AIシステムに係るEUレベルのガバナンス
市販後モニタリング	市場投入後の監視・是正
法律の執行・罰則	行動規範の作成・違反行為に対する罰則

1｜禁止される行為

(1) サブリミナル技術を使用するシステム：人の意識を超えたサブリミナル的な技法、または意図的に操作的もしくは欺瞞的な技法を展開する AI システムを市場に投入、稼働させること、または使用すること、並びにその目的または効果が、十分な情報に基づいた意思決定を行う能力を著しく損なわせることにより、人または人の集団の行動を実質的に歪め、その人、他の人または人の集団に重大な損害を与えるか、または与える可能性が合理的に高い意思決定を行わせること（5 条 1 項(a)）は禁止される。

（注記）前文では AI を利用した操作技術により、「身体的、心理的健康または経済的利益に対して十分に重要な悪影響を及ぼすような重大な危害が発生する可能性があり、人間の行動を実質的に歪めることを目的とする、またはそのような効果を持つ特定の AI システムを市場に出すこと、稼働させること、または使用することは、特に危険であり、禁止されるべきである」（前文 29）とする。このような危険は脳と機械を接続する技術や仮想現実で特に起こりやすいと同前文では指摘している。AI システムにより人間の自由な思考を不当に歪める行為は禁じられる。

(2) こどもや障がい者等を搾取する AI システム：自然人またはその年齢、障がいまたは特定の社会的もしくは経済的状況に起因する特定の集団の脆弱性を悪用する AI システムであって、その人の行動

を重大に歪曲させる目的または効果があり、そのことで、その人または他の人に重大な損害を与えるか、または与える可能性が合理的に高いものを、市場投入すること、サービスを開始すること、または使用すること（同項（b））は禁止される。
（注記）前文では「AI システムは、年齢、障がい、または極度の貧困状態にある人、民族的もしくは宗教的マイノリティなど、（中略）人または特定のグループの脆弱性を悪用する可能性がある」（前文29）とする。たとえば高齢者など社会的に脆弱性があると認められる層に対して、AI を利用して高リスク金融商品の販売を促進するなどの危険も想定される。

(3) ソーシャルスコアリング：以下（図表 5）のような影響をもたらす結果となる、社会的行動又は既知，推論若しくは予測される個人的若しくは人格的特徴に基づいて，一定期間にわたり自然人又は集団の評価又は分類のために AI システムを市場投入すること，稼働させること又は使用すること（同項(c)）は禁止される。

【図表 5】禁止されるソーシャルスコアリング

(i)データが元々生成または収集された文脈とは無関係な社会的文脈において、特定の自然人または集団に対して不利益または不利な扱いをすること
(ii)特定の自然人または集団に対して、その社会的行動や重大性に不当または不釣り合いな不利益または不利な扱いをすること

（注記）前文では「公的または私的主体による自然人の社会的採点を提供する制度は、差別的な結果や特定の集団の排除につながる可能性がある。これらは、尊厳と非差別の権利、平等と正義の価値を侵害する可能性がある」とし、そして「そのような AI システムから得られる社会的スコアは、データが元々生成または収集された文脈とは無関係な社会的文脈において、自然人またはそのグループ全体を不利に扱うことにつながる可能性がある」（前文 30）とする。
　たとえば、中国には芝麻信用（ジーマ信用）という企業があって、この企業の信用スコアの高低でビザ申請や図書館の利用などに影響が出るといったことがある[4]。このようなシステムはこの規定に抵触する可能性が高いと考えられる。

(4) 予測取締システム：自然人が罪を犯すリスクを評価又は予測するために，自然人のプロファイリング又はその人格的特徴及び特性の評価のみに基づき，自然人のリスク評価を行うための AI システムを市場に投入すること，この特定の目的のために使用すること，又は使用すること（同項(d)）は禁止される。
（注記）前文では「無罪の推定に基づき、EU 域内の自然人は常に実際の行動に基づいて判断されるべきである。国籍、出生地、居住地、子供の数、借金の額、車の種類など、その人のプロファイリング

[4] 大野雄裕「個人信用スコアとその規範」季刊個人金融 2023 冬号　https://www.yu-cho-f.jp/wp-content/uploads/2023winter_articles01.pdf　参照。

や性格的特徴、特性のみに基づいてAIが予測した行動のみによって、その人が犯罪行為に関与しているという客観的に検証可能な事実に基づく合理的な疑いがないのにも関わらず、人間による評価なしに判断されるべきでは決してない」（前文 42）とする。その人のプロファイリングによって罪を犯す可能性が高いとAIが判断した場合に予防的に取り締まるAIシステムを禁止するものである。つまり実際に発生した犯罪事実に基づかない予測取締システムは禁止される。これは映画[5]のような話であるが、一部の権威主義的国家では実現している可能性がある。

(5)生体データの無差別収集：インターネットや CCTV（監視カメラ）映像から顔画像を無制限に収集し、顔認識データベースを作成または拡張するAIシステムを使用すること(同項(e))は禁止される。
（注記）前文では「インターネットやCCTVの映像から顔画像を無制限にスクレイピング（＝データの余分な部分を削除し、抽象化されたデータにすること）して顔認識データベースを作成・拡大するAIシステムを市場に投入したり、そのような特定の目的のために使用したりすることは、集団監視の感覚を助長し、プライバシーの権利を含む基本的権利の重大な侵害につながる可能性があるため、禁止されるべきである」（前文(43)）とする。たとえば犯罪が行われた現場を監視カメラでとらえたケースで、事前に収集した顔画面データと照合して犯人を割り出すことが考えられる。一見、合理的なようにも思えるが、一般大衆の顔データを取締目的でデータベース化することは政治体制や為政者次第で一般大衆のデモ抑圧や不当逮捕などの表現の自由に対する大きな脅威になる。したがって禁止されるべきである。これも一部の権威主義的国家では実現している可能性がある。

(6)感情認識システム：職場や教育施設内での自然人の感情を推測するためのAI システムを市場に出すこと，この特定の目的のために使用すること（同項(f)）は禁止される。ただし、医療及び安全確保目的であるものは許容される。
（注記）前文では「感情の表現は文化や状況によって、また一個人であってもかなり異なるため、感情を識別または推論することを目的とした AI システムの科学的根拠には深刻な懸念がある。このようなシステムの主な欠点として、信頼性の低さ、特異性の欠如、一般化可能性の低さが挙げられる。したがって、AI システムが自然人の生体データに基づいて感情や意図を特定または推論することは、差別的な結果をもたらし、関係者の権利と自由を侵害する可能性がある」（前文 44）とする。感情認識システムとは、たとえばコールセンターのシステムにおいて顧客の感情を判断し、顧客の口調を柔らかく加工するなど、職員による対応の支援を行うようなAIシステムが既に実現している。このようなAIシステムは安全確保とも言い難く、本規則では文言上は禁止対象になりそうである。ただ、このようなAIシステムの目的に問題があるとも思われないが、どうであろうか。

(7)機微な特徴を利用した生体分類システム：人種、政治的意見、労働組合員、宗教的または哲学的信条、性生活または性的指向を推測または推論するために、生体データに基づいて個々の自然人を分類

[5] マイノリティ・リポートという映画があり、純粋にはAIシステムではないが、罪を犯すことを予見してその者を事前に拘束するというシステムを持つ社会でのストーリーとなっている。

する生体分類システムを市場に投入すること、また、このような目的のために使用すること(同項(g))は禁止される。

(注記) 前文でも条文と同様に「個人の政治的意見、労働組合員、宗教的または哲学的信条、人種、性生活または性的指向を推測または推論するために、個人の顔や指紋などの自然人の生体データに基づく生体分類システムは禁止されるべきである」(前文 30) と記載されている。たとえば特定の政治的意見を有する人の生体データを収集・分析し、この結果に基づいて特定個人の政治的意見を推論するものである[6]。このような行為は非常に差別的であり、また民主主義や個人の尊厳に悪影響を及ぼすことは明らかであることから、禁止される。

(8) リアルタイム遠隔生体識別システム：法執行の目的で、公共のアクセス可能な空間において「リアルタイム」の遠隔生体識別システムを使用することは禁止される。ただし、その使用が次のいずれかの目的(図表 6)で厳格に必要性がある場合を除く (同項(h))。

【図表 6】リアルタイム遠隔生体識別システムが許容されるケース

(i)拉致、人身売買、性的搾取の被害者、行方不明者の捜索
(ii)自然人の生命または身体の安全に対する具体的、実質的かつ差し迫った脅威、または真正かつ現在もしくは真正かつ予見可能なテロ攻撃の脅威の防止
(iii)付属書Ⅱ (テロや誘拐、殺人などの犯罪が列挙されている。図表は省略) で言及されている犯罪であって、当該加盟国において少なくとも 4 年以上の拘禁刑又は拘禁命令により処罰される犯罪について、犯罪捜査若しくは訴追を行い、又は刑事罰を執行する目的で、罪を犯したと疑われる者を特定又は識別すること

(注記) ここで生体識別システムとは自然人の身体的、生理的または行動的特徴に関連する特定の技術的処理から生ずる個人データを、以前に提供された個人データと比較して自然人の身元を 1 対 1 で検証するシステム(3 条 34 項、36 項)をいう。

そして、リアルタイム遠隔生体識別システムとは、自然人の生体データを参照データベースに含まれる生体データと比較することにより、自然人の積極的な関与なしに、リアルタイムかつ遠隔で、自然人を識別することを目的とする AI システム (3 条 41 項、42 項) を意味する。

前文では「法執行の目的で、公的にアクセス可能な空間における自然人の『リアルタイムの』遠隔生体識別のための AI システムの使用は、国民の大部分の私生活に影響を及ぼし、常に監視されているという感覚を呼び起こし、集会の自由やその他の基本的権利の行使を間接的に阻害する可能性がある」(前文 32) とする。したがって、「法執行の目的でこれらのシステムを使用することは、網羅的に列挙され、狭く定義された状況において、その重要性がリスクを上回る実質的な公共の利益を達成するために厳密に必要である場合を除き、禁止される」(前文 33) としている。条文の定める通り、禁止原

[6] AI がどの程度利用されたかは定かではないが、ケンブリッジ・アナリティカ社が大統領選にあたって、Facebook ユーザーの情報をもとに、特定候補に投票するよう誘導することが行われた。現時点での AI システムではより高度な操作が行われしまう危険がある。

則についての例外が定められている。この点についての具体的な取り扱いは次項参照。

2｜リアルタイム遠隔生体識別システムが許容されるケース

(1)上記1｜の(8)（リアルタイム遠隔生体識別システム）が法執行において許容されるのは、特定の個人に合致することを確認することに限られ、かつ以下の要素（図表 7）に配慮しなければならない(5条2項)。

【図表7】リアルタイム遠隔生体識別システムで考慮すべき要素

(a)使用により引き起こされる状況の性格、特にAIシステムが利用されないとしたときの弊害発生の可能性と大きさ
(b)システムを利用した場合の関連するすべての人の権利と自由に対する影響、特に影響の深刻さ、可能性、大きさ

以上に加え、法執行機関(law enforcement authority)が基本的権利影響評価(27条、次回レポートで解説予定)を完了し、EUのデータベースに登録(49条、3回目のレポートで解説予定)することが求められる。

そして、人に不利な法的効果をもたらす決定はリアルタイム遠隔生体識別システムの出力のみに基づいてはならない。

（注記）前文では、「法執行の目的で『リアルタイムの』遠隔生体識別のためのAIシステムの使用は、例外的に認められる。そのような状況とは、行方不明者を含む特定の犯罪被害者の捜索、自然人の生命または身体の安全に対する特定の脅威、テロ攻撃、本規則の付属書に記載された犯罪の加害者または容疑者の位置特定または特定を含む」（前文33）とする。

これは捜査のために監視カメラとAIシステムを組み合わせた容疑者の所在確認が可能かどうかという問題である。捜査にあたっては、幅広いエリアでの一般大衆の生体情報の確認が行われることとなる。そうすると一般人のプライバシー保護の要請と犯罪の容疑者確保という要請との利害衝突が発生する場面が生ずる。このような利害の衝突を上述のように登録や法執行機関の影響評価という手順を踏ませることで調整可能にしている。

上記に加え、司法当局の事前許可を得ること(5条3項)、市場監視当局および国内データ保護当局へ通知すべきこと（同条4項)、加盟国は捜査目的のリアルタイム遠隔生体識別に係る立法を行うべきこと（同条5項)、市場監視当局等からの欧州委員会への年次報告を行うこと（同条6項)、欧州委員会は年次報告を行うこと（同条7項）などが定められている。

4――小括

本稿で取り扱ったのは、AI規則案の前半、すなわち①AI規則の適用範囲および適用除外、②各種の

定義、③禁止されるAIシステムの行為である。

ここで特に注目したいのが③禁止されるAIシステムの行為である(5条1項)。AI規則が、法令であるがゆえに、一定の行為を禁止することができる。日本のAI事業者ガイドラインはガイドラインに過ぎないので、弊害が大きい行為でも禁止することができない[7]という相違がある。日本でAI規制法の制定が急がれる理由の一つであろう。

EU域内において、もしAIシステム提供者等が本規制に違反した場合は、35百万ユーロまたは前会計年度の全世界の年間売上高の7%以下のいずれか高い方の罰金が科される(99条3項、4回目レポートで解説予定)。

禁止される行為は類型的に人権侵害の程度が高いものであり、1)人の意識や感情に干渉するシステム(サブリミナル技術を使用するシステム、こどもや障がい者等を搾取するシステム、感情認識システム)、2)人を監視し、分類するシステム(ソーシャルスコアリング、予測取締システム、生体データの無差別取集、機微な特徴を利用した生体分類システム、リアルタイム遠隔生体識別システム)である。

上記1)は、本質的に自由であるべき人の内心の自由を歪めるものであり、どのような理由においても正当化できないものと判断される。また、上記2)は、人の行為や動向を監視し、結果次第でその人に不利益をもたらす可能性が高いものであり、ディストピアである監視社会をもたらす可能性がある。この場合、人の自由に大きな制約をもたらすことになり、やはりAIシステムの利用は正当化できない。禁止されるべき行為がこれだけなのか、あるいは過剰規制に該当する部分が存在するかは明らかではないが、今後、本規則の運用に伴って修正が加えられるのだろう。

次回(2回目)は、高リスクAIシステムについて述べる。

[7] 実際に日本のAI事業者ガイドラインには禁止規定は存在しない。