北九州市立大学法政論集第 50 巻第1・2合併号(2022 年 10 月)抜刷

論　　説

EUにおけるAI規制の動向
――ドイツの視点から――

水　野　陽　一

北九州市立大学法政論集第 50 巻第 1・2 合併号（2022 年 10 月）

論　　説

EU における AI 規制の動向
－ドイツの視点から

水　野　陽　一*

はじめに

人工知能（AI）の実装は、われわれの生活の様々な場面で現実のものとなっており、それを意識するしないとを問わず人々はその恩恵を享受している。AI は人間の暮らしを豊かにする一方、対象とする個人に対して軽視できない侵害を与えることがあり、とりわけ生体認証技術に関わるものについては活発な議論が行われている。その中でも、顔認証システムの市場は、今後大きな成長が見込まれており、顔認証技術の利用拡大が世界的に大きな話題となっている。顔認証システムは、公共の安全のためにもその有用性が認められているが、その普及に際して生じ得るプライバシー侵害の性質、エラーの起こりやすさなどから、特定の層に対する差別、データ保護やプライバシーに対する権利の侵害など、基本権に関する懸念があ

＊本学法学部准教授

ることも指摘されている。このような事態に対処するため、EU はすでに基本権憲章、EU データ保護一般規則(GDPR)、刑事訴追におけるデータ保護に関する指令などの厳格な規則を採用しており、これは既に顔認証技術の制限、統制に適用されている。しかしながら、AI に関する技術的発展は、これら諸規則の立法当時の予想を上回るスピードで進行している。その結果、現行の EU の法的枠組みは、既に顔認証技術に関わる基本権についての懸念に適切に対処するには十分ではなく、顔認証技術の利用に関して看過し得ない問題点が存在するとされる(1)。このような現状において、現行 EU 法の積極的な解釈によっても基本権保障を行うことはできず法的な不確実性と混乱を完全に解消するとは困難であるとの認識から(2)、2021 年 4 月 21 日、AI の新たな規制案（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）が示された(3)。これは、広範囲な監視につながる可能性がある顔認証を含む生体認証技術の利用を制限、適切に統制

(1) 例えば、*Martin,* NVwZ 2022, 31-32.

(2) EU は 2018 年のヨーロッパ AI 戦略の公表以後、信頼できる AI 開発のために多くの取り組みを行なっている。特に 2020 年の AI 白書において、欧州における AI の明確なビジョンとして、卓越性と信頼のためのエコシステムを掲げており、これは新しい AI 規制案の基礎となっている。白書には「人工知能、モノのインターネット、ロボティクスの安全性と責任に関する報告書」が添付され、現行の AI に関する製品安全法制には、特に機械指令(Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006)を通じて対処すべき多くのギャップがあることが明らかにされていた。

機械指令の目的は、すべての加盟国で市場に出ることが予定されているまたは現在既に稼働する機械に共通の安全レベルを保証し、「加盟国は指令に準拠した機械の自国内での上市や稼働を禁止すること及び制限、妨害をしてはならない」として EU 内での移動の自由を確保することである。

(3) 全文は、以下の URL を参照。https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri = CELEX:52021PC0206&from = DE

することを目的とする。新しい規制案では、データ保護や差別防止に関する既存のルールに加え、EU における AI 利用について新しいルールを導入、特にその利用が「高」リスクか「低」リスクかを区別することが提案されている。顔認証技術の多くは、利用自体が禁止されるか、厳しい要件の対象となる「高リスク」のシステムとみなされることが予想される。

以下では、ヨーロッパ委員会が示す新しい AI 規制の枠組みを概観し、これが EU 加盟国においてどのような意義を有するのかについてドイツにおける議論を参考に考察する。EU における AI 規制の枠組みは、現時点でも世界的にみて相当に厳格なものであると考えられる。EU ではこれを更に発展させることで、AI 規制に関する世界的なイニシアティブを取ることを目論んでおり、これはわが国の AI に関するガバナンスの議論にとっても多大な影響があると思われる(4)。顔認証技術の利用範囲は世界的に拡大を続けているが、同時に国家による監視に対する懸念も高まっている。しかしながら、日本、ヨーロッパ以外でも、米国や中国などにおいてさえ、顔認証技術に関する拘束力のあるルールがほとんど存在しないことがこの懸念を一層深刻なものとしている(5)。

(4) EU データ保護一般規則(GDPR)は、EU 域外へのデータ移転の際にも EU 域内と同等のデータ保護基準の徹底を求めており、この一点だけをみても EU における新しい AI 規制のあり方はわが国にとって大きな影響がある。この点につき、拙稿「刑事手続における AI 実装と個人情報保護に関する諸問題--刑事捜査・訴追機関の情報収集・処理に関するものを中心に」北九州市立大学法政論集 47 巻 (1・2 号) 77 頁以下参照（2019 年)。

(5) Madiega, Regulating facial recognition in the EU, European Parliamentary Research Service, 2021 pp.41.

このヨーロッパ議会の有識者による報告書は、https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf から入手した。

１．EU における AI 規制の動向

(1)　EU 憲法とデータ保護

AI を利用した個人情報の処理は、通常、EU 基本権憲章第 8 条に基づくデータ保護の権利、情報自己決定権および 7 条に基づくプライバシーの権利への侵害を伴うことになる。EU 基本権憲章 52 条 1 項によれば、プライバシーに関わる基本権に対する侵害、制限を伴う行動は、比例原則に基づきその可否が決せられることになるが、EU 基本権憲章は、データ保護に関する原則を示すものではあってもその具体的な枠組みを決定するものではない。EU におけるデータ保護の方向性及び具体的内容について、下位法としての GDPR 及び EU 指令である刑事訴追に関するデータ保護指令を参照しなければならない(6)。これらの規定から、EU におけるデータ保護について、以下の要請が満たされなければならないことがわかる。

(2)　EU データ保護法からの要請(7)

①合法性、信頼性、透明性の原則

個人データ処理は、同意または法的根拠（同意の留保を伴う禁止）が存在する場合に限り合法である(8)。法的根拠は明確に策定され、データ処理の目的が明確にされなければならない。信頼性の原則は、「公正な処理」を

(6)　*Id.* at 12.

(7)　EU 法からの要請について、*Bauer/Gogoll/Zuber,* ANALYSEN UND STUDIEN Gesichtserkennung Ein Diskussionsbeitrag zur Regulierung der Technologie, bidt – Bayerisches Forschungsinstitut für Digitale Transformation, 2021, S.21-25.を参照した。このバイエルン・デジタルトランスフォーメーション研究所による報告書は以下の URL から入手した。https://www.bidt.digital/wp-content/uploads/
2021/11/bidt_Analysen-Studien_Gesichtserkennung.pdf

(8)　データ保護法では、許可を留保した上での禁止の原則が適用される。つまり、個人データの処理（収集、保存、開示）は、当初は禁止されており、法的根拠を必要とする。この文脈で最も重要な規定は、GDPR の第 6 条である。

要求し、特に対象者の同意は自発的に行われたものでなければならない。透明性の原則は、データ処理対象者が、どのような個人データが誰によって、どのような目的で、どのくらいの期間処理されるか、この点に関してどのような権利が存在し、これらの権利をどのように行使できるかについて、分かりやすく明確な方法で知らされることを要求する。データ保護に関する司法と内政分野における EU 指令の領域では、刑事訴追や安全保障のために秘密捜査が必要であるため、透明性の原則は適用されない。しかし、関係者が権利を行使できるようにするために、事後的に当該捜査について告知されなければならない。

②目的制限の原則

個人データの収集は、明確かつあらかじめ定められた正当な目的のためにのみ許容され、その処理も原則として当初の目的に限定される。しかしながら、例外的に他の目的のためにデータ処理を行うことが許される場合もある。

③データ最小化の原則

個人データの処理は、その必要性が認められる場合にのみ許される。対象者に与える影響がより低いかつ、適切な手段がある場合は、当該個人データの処理に必要性は認められない。また、データ処理の強度は、その目的に比例していなければならない。

④正確性の原則

個人データは正確でなければならない。データ管理者はこれを自ら確認しなければならない

⑤保存制限の原則

個人データは、処理の目的に必要な期間を超えて保存されてはならない。

⑥個人データの完全性・機密性

個人データは、その安全性が十分に保証される方法で処理されなければならない。したがって、不正または違法な処理、偶発的な損失、破壊または損害がないことを保証するために、技術的および組織的な措置を講じなければならない。

⑦データ保護影響評価

特にリスクの高いデータ処理業務については、データ保護影響評価を実施する必要がある。これは、当該データ処理が、EU 基本権憲章はもちろん、GDPR、刑事訴追におけるデータ保護指令、EU 加盟国内のデータ保護法の規定を満たすものであるかを検証する目的で行われる。それでもなお高いリスクが残る場合、データ保護監督機関に申告し、必要であればデータ処理を停止しなければならない。

(3) ヨーロッパ委員会による信頼できる AI システム構築のための新しい規則の提案[9]

①リスクベースアプローチの採用

以上のように、EU におけるデータ保護は、EU 基本権憲章に基づく GDPR 及び刑事訴追におけるデータ保護指令においてある程度具体化されているが、AI を用いた個人データの処理の性質を考えると、未だにその規制内容が基本権保障にとって十分ではないという。このような批判を受けて、ヨーロッパ委員会は新しい AI 規制案を示した。このヨーロッパ委員会の提案は、EU で使用される AI システムが安全、透明、倫理的、公平で、人間のコントロール下にあることを保証するための新しい規則の構築を目的とする。これは、将来的にも有効な AI の定義に基づき、すべての

(9) 本提案について、以下の URL より英語版とドイツ語版の文書を入手し、概観、検討した。https://eur-lex.europa.eu/legal-content/DE/TXT/?uri = CELEX%3A52021PC0206

加盟国で直接かつ共通に適用される。AI システムにはリスクが存在していることを前提としたリスクベースアプローチを採用し、リスクに応じた AI の分類が行われる。

② AI の利用が認められない場合

信頼できる AI システムの構築のために、AI のリスク分類が行われるが、人間の安全、生活、権利を明らかに脅かすような場合、そもそも AI の利用自体が認められないこともある。EU 市民にとって明らかに脅威となるもの、例えば、政府によるソーシャル・スコアリング、市民に対する点数付などがこれに当たるだろう(10)。また、子どもを危険な行為に誘う音声アシスタント付き玩具など、人間にとって明らかに脅威であることが明白な場面での AI の利用は、いかなる条件のもとでも禁止されることになる。また、後述のように公的機関による顔認証技術を用いたリアルタイム監視は、一部の例外を除き原則として禁止されることになる。

③高リスク AI と低リスク AI の分類

ⅰ．高リスク AI

以下のような場面で AI が用いられる際に、その利用が高リスクであるとされることになる。例えば、市民の生命や健康が危険にさらされる可能性のある重要インフラ、特に交通インフラの運用に AI を用いる場合がこれにあたる。また、教育または職業訓練で、個人の教育および職業への評価が影響を受ける可能性がある場合、その生活に多大な影響を与える可能性があることから、このような場面での AI 利用も高リスクとなる。更に、製品の安全性に関わる部分、例えばロボット支援手術のための AI アプリケーションなどは、個人の生命、身体への影響が大きいことから当然に高リスクとなる。この他、採用プロセスで履歴書を評価するソフトウェアな

(10) 草案によると、これらの規則に違反した者は、最高 3000 万ユーロまたは全世界の年間売上高の 6%（いずれか高い方）の罰金を科されることが予想される。

ど雇用、人材管理、自営業への評価に関わるもの、個人への融資を決定する信用スコアリングに用いるなど重要な民間および公共サービスに関わるもの、旅行書類の真偽確認等、移民、亡命、国境管理に関係するものなども AI 利用に高いリスクがある典型であるとされている。この他、具体的事実への法の適用など司法の運営に AI が関わる場合も高リスクであるとされており、その中でも刑事捜査・訴追はその性質上、常に個人の基本権を侵害する可能性を有するため、特に注意を要すべき類型であるといえる。被疑者の特定はもちろん、証拠評価の場面でもその真実性等を判断するために AI が利用される場面が想定される。

以上示した類型に代表されるすべてのシステムは、公表、発売前だけでなく、システムが使用される全ての期間を通じて厳密にチェックされる。これは、リスクと差別的な結果を最小化するために、高品質のデータセットをシステムに供給すること、結果のトレーサビリティを可能にする操作のロギング等を通じて行われる。また、監督機関がその準拠性を評価できるように、システムおよびその目的について必要なすべての情報を記載した詳細な文書の提出が求められる。ユーザーに対する明確かつ適切な情報提供、リスクを最小化するための適切な人的管理、高いレベルの堅牢性、安全性、正確性の確保が必要となる。

高リスクに分類される AI 利用の中でも、あらゆるタイプの遠隔生体認証システムは、特に高いリスクを伴い実装、利用に際して厳しい要求がされる。まず、刑事訴追等、法執行を目的とした公共空間でのリアルタイムの使用は原則禁止とされる。その例外は厳密に定義され、規制される（行方不明の子供を捜索するため、具体的かつ差し迫ったテロの脅威を回避するため、あるいは重大な犯罪の犯人や被疑者・被告人を検知、追跡、特定、起訴するために絶対必要な場合などの条件が必要となる）。このような利用は、加盟国の司法当局またはその他の独立した機関の認可・許可を必要とし、時間的、地理的範囲および検索されるデータベースに関して合理的かつ必要な制限を受けることになる。

ii. 限定的なリスクが認められる AI

以上示した類型ほどの危険はないが、一部の AI システムには、その利用の際に危険性が認められる場合がある。例えば、チャットボット[11]のような AI システムについては、最低限の透明性確保義務が適用され、対話するユーザーが十分な情報を得た上で意思決定できるようにする必要がある。チャットボットは、透明性保持義務の対象となる AI であり、ユーザーには自分が機械を相手にしていることを認識し、アプリケーションを使い続けるかどうかを十分な情報に基づいて判断できる機会が認められなければならない。

iii. 低リスク AI

AI を搭載したゲームやスパムフィルターなどのアプリケーションは、低リスク AI に分類され、特別な制限なく利用できる。これらの AI 利用の場合には、市民の自由や安全保障に与えるリスクはほとんどないため、ヨーロッパ委員会の示す新しい AI 規制案の対象にはならない。

(4) 小括

GDPR に代表される EU におけるデータ保護法制は、その内容、実効性、EU 加盟国以外に与える波及的効果の大きさから、世界的に見ても個人の権利保障をその中核とするモデルとして大きな影響力を有していると思われる。しかしながら、現行 EU 法の枠組みでさえ、個人のプライバシー権

---

(11) 「チャットボット（Chatbot）」とは、「チャット」と「ボット」を組み合わせた言葉で、自動的に会話を行うプログラムを意味する。ここでは特に、人工知能により、統計的に正解する可能性の高い回答を選ぶチャットボットが問題となり、これは会話ログを自動的に学習し、正答率や会話の精度を上げていく仕組みを有している。

ユーザーがこれを利用する際に、不正に誘導され望まない回答をすることにないように、適切な情報提供等が行われる必要がある。

チャットボットについて、https://www.jbsvc.co.jp/useful/ai/what-is-chatbot.html を参照した。

及びデータの保護にとって必ずしも十分なものではないとの評価がされた。

今後、人工知能に対するヨーロッパのアプローチと機械指令に関するヨーロッパ委員会の提案は、欧州議会による立法手続を経て採択されることになろう。欧州議会による規制案の採択がされれば、EU 全域に直接適用されることになる。これと並行して、ヨーロッパ委員会は、調整計画で発表された措置の実施に向けて加盟国と引き続き協力するとしており、各加盟国は対応を求められることになる。その後 EU 加盟国は、国内法制化によって EU 法に合致した AI 規制の整備を進めることになる。

２．EU 加盟国における AI 規制の法的枠組み
―ドイツにおける議論を参考に―

⑴　ドイツにおける法的規制の前提

ドイツにおいて、顔認証をはじめとする AI に関する技術的信頼性のあるシステムの構築は、憲法上の比例原則を担保するために必要であるとされる。信頼性の認められるシステムの構築が行われない場合、憲法上の要請を損なう危険性が指摘され、特に平等原則等との関係で問題を生じるとされている[12]。

⑵　民間企業に課される義務

民間企業には、技術的信頼性のあるシステムを構築する義務があると考えられる。これはシステム等の提供先との契約上の相互的な注意義務によって生ずることが考えられ、契約外のことであっても危険回避義務[13]（Verkehrssicherungspflicht）から信頼性の認められるシステム開発が求められる。当該義務の不履行については、生じた損害等についての責めを

⑿　*Bauer/Gogoll/Zuber* Fn(7), 19.

⒀　危険源を生み出し、または有する者は、他者への被害を防止するために必要かつ合理的な予防措置（安全対策）を講じる義務を負う。

負うことになりうる。ここで注意しなければならないのは、技術的に信頼できるシステムであっても、法律的に許されるとは限らないということである。顔認証システム等、AI アプリケーションを使用する者は、技術的な問題とは別に憲法とデータ保護法の求める要件を満たさなければならない(14)。

(3) ドイツ憲法上の要請

①情報自己決定権(15)

連邦憲法裁判所は、1983 年にいわゆる国勢調査判決(Volkszählungsurteil)(16)で、一般的人格権の表出として情報自己決定権を確立した。これは、個人の生活に関わる事実をいつ、どのような範囲で開示するかについて、個人が自ら決定する権利を保障し、個人データの無制限の収集、保存、使用、開示から国民を保護するものである。それ故、対象者の同意がある場合、または侵害の法的根拠があり、それが比例的で、規範の確実性と規範の明確性の原則に準拠し、十分な組織的・手続的保護措置を備えている場合に限り、立法者によって情報自己決定権に対する侵害が許される。AI による個人データの処理は、全て情報自己決定権に対する制限、侵害となるため、以下の要件を備えた場合に初めてその利用が認められることになる(17)。

②比例原則

正統・正当な目的を追及しておりかつ、目的達成にとって適当であり、また利益を保護するのに必要以上に踏み込まず、狭義の意味で比例的であれば、当該侵害は比例的であるといえる。

---

(14) *Bauer/Gogoll/Zuber* Fn.(7), 20.

(15) ドイツにおける情報自己決定権に関する議論について、玉蟲由樹『人間の尊厳保障の法理―人間の尊厳条項の規範的意義と動態』281 頁以下（尚学社、2013 年）を参照した。

(16) BVerfGE 65,1.

(17) 以下の具体的な要件について、*Bauer/Gogoll/Zuber* Fn.(7), 21.

狭義の比例性とは以下のようにまとめられる。目的は手段を正当化するものではなく、むしろ侵害の程度は、それを正当化する根拠の重さに対して不釣り合いであってはならない。

③規範の確実性と明確性の要請

これは、民主的正統性が認められる立法府自らが重要な決定を行うこと、行政活動の統制と制限を確保するためのものである。例えば、連邦憲法裁判所は、ビデオ監視について、その影響が広範囲に及ぶこと法的根拠が欠如することから、基本権に対する非常に集中的な侵害であるため、データ保護法の一般条項はビデオ監視の適切な統制には曖昧すぎると考えている(18)。近年では公共空間での顔認証を原則禁止とする意見がドイツ国内で有力であり、少なくとも現状では個別法による統制が求められている。

④組織的・手続的な予防措置

これは、濫用の可能性を排除することを目的とする。

これには、データ管理者がデータ処理についてデータ対象者に通知する義務、および保存されたデータに関する情報を提供する義務が含まれる。また、目的を達成するために必要でないデータは収集されてはならず、事後的に必要ではなくなったデータは削除されなければならない。

データ利用の範囲は、原則として法的に認められた当初のデータ収集目的に限定される。さらに、独立したデータ保護監督担当者によるモニタリングが求められる。

さらに、高度なデータセキュリティ（例えば、「データの分離保管、高度な暗号化、二重管理原則などを用いた安全なアクセス体制、監査証明付きログイン」）が必要な場合がある。高度なデータセキュリティーの枠組みとして、裁判所による審査、裁判官留保もこれに含まれる場合がある。

(18) BVerfG NVwZ 2007, 688 (690 f.)

(4) ドイツにおける AI 規制の今後の展望

①ヨーロッパ委員会の示した新しい AI 規制案に対する対応[19]

2022 年 3 月 16 日、第 6 回連邦議会デジタル委員会において、AI に関する EU 規制の交渉状況に関する連邦政府の報告書が取り扱われた。ここでは、ヨーロッパ委員会の示す提案に対して、ヨーロッパ共通の価値観が定義され、AI 拠点としてのヨーロッパが強化されれば法的確実性が生まれるという規制の目的を歓迎したとされている。

法確実性の拠り所となるべき規制案を作成することの目的は、規制を通じて信頼のできる技術を創造することで、新しい技術とうまく付き合う方法を見出すことであるとされる。これまで GDPR と刑事訴追におけるデータ保護指令が担ってきた EU 域内の単一市場の発展と効果的な刑事訴追のための共同について、新たなヨーロッパ委員会の提案に従い更なる発展が見込まれるとしている。

ヨーロッパ委員会の示す新たな提案の特徴である、AI のリスク分類について、「許容できない」、「高い」、「低い」、「最小」の 4 つの定義がされているが、重要なのは「高い」リスクを有する AI 規制のあり方を議論することであるという認識が示されている。このカテゴリーには、当然、顔認証を含む生体認証システムが入る。刑事法分野で重要となるのは、「公共スペースでの生体認証による監視は行わない」ということが確認されたことであろう。公共空間での生体認証による監視、バイオメトリクス遠隔認証は、ヨーロッパ委員会提案に基けば、テロ攻撃対策、ヨーロッパ逮捕状で指名手配されている犯人の追跡、子供の捜索などの目的のために国内法で許可される可能性があるが、ドイツにおいてこれに否定的な意見が優勢である。他国に比して、ドイツがこの分野での AI の利用にやや慎重な姿勢を見せるのは、刑事法分野における AI 利用が、他の分野に比して、個人に

---

⑲ ドイツの対応について、ドイツ連邦議会のホームページを参照した。
https://www.bundestag.de/dokumente/textarchiv/2022/kw11-pa-digitales-kuenstliche-intelligenz-883942

対して与える影響がより過大なものとなる事実を重要視していること、技術的な不確実性が残ることなどがあると思われる。ドイツ連邦司法省は、ヨーロッパ委員会が AI 利用の全範囲にわたって規制案を示したことはその顕著な功績であるとする一方、刑事捜査・訴追機関等、治安当局のための独立した章を設けることが有用であるとの見方も示している[20]。高リスクな AI 利用の中でも、警察利用の際のリスクは対象者に与える影響の大きさなどを考慮した場合、更にもう一段階高いレベルにあると考えられることから、このようなドイツの認識には妥当性がある

⑸ 小括

ヨーロッパ委員会による新しい AI 規制案に対するドイツの反応は、概ね好意的なものといって良い。特に、顔認証を含む生体認証技術に関する AI 利用については、EU の示す提案よりも高い水準での規制が行われる可能性が高い。EU におけるデータ保護の原則として、個人に対して情報自己決定権が認められることを前提とすることからも、EU のデータ保護政策に対してドイツの与える影響を注視していく必要がある。

おわりに

本稿において、EU における AI 規制の最新の動向を概観し、若干の検討を行った。これまでも EU は、個人の権利保障を主軸としたデータ保護法制の整備を進めることにより、データ保護の領域において世界的にイニシアティブをとってきたように思われる。ヨーロッパ域内で示されるデータ保護や AI 規制の枠組みは、個人のプライバシー権保障の観点から既に相当高水準ものであるように見えるが、EU ではこれを一段進めて個人の権

---

⑳ 刑事法関係の議論について、拙稿「顔認証技術を用いた捜査手法に対する規制方法--EU、ドイツにおける議論を参考に」北九州市立大学法政論集 49 (1・2 号)85-108 頁 2021 年参照。

利保障水準の更なる底上げを狙っているように思える。本稿で検討したヨーロッパ委員会の新しい AI 規制案では、AI 利用にリスクが存在することを前提としたリスクベースアプローチが採用され、適切なリスク分類によって個人が AI システムによって不当に損なわれないようより一層の配慮を各ステークホルダーに求めている。これに対するわが国の反応は、経済界を中心に概ね好意的であるように思われるが(21)、厳格な AI 規制は個人の保護にとっては有効である反面、AI 自体の発展を阻むものであるとの危惧が見て取れる。EU の新しい AI 規制案は、とりわけ生体認証技術の利用には厳しい条件を課すものとなっており、民間企業の利用はもちろん、警察利用など公共の利用目的であってもフリーハンドによる利用を認めない。EU 加盟国であるドイツ国内においては、原則として公共の場所での顔認証システムを利用した行動監視が原則禁止される見込みであり、今後、刑事捜査・訴追の分野においても刑事訴訟法を中心とした顔認証に関する個別法が設けられることになろう。

わが国において、AI の発展を促すルールづくりに関して、ソフトローによる統制を中心としたアジャイル・ガバナンスが注目されている(22)。これは、可能な限りステークホルダー間での対話に基づく柔軟なルールの構築を目指すものであり、刻一刻と変化する AI 開発を取り巻く環境を考慮した場合、AI アルゴリズムの発展にとっては有益な部分が多いように思われる。しかしながら、AI システムの社会、個人に与える影響の大きさを考えると、ソフトロー的なゆるい規制では個人の保護にとって十分な対応が

---

(21) EU の新しい AI 規制案に対するわが国の反応として、日本経済団体連合会の「欧州 AI 規制法案に対する意見」等がある。https://www.keidanren.or.jp/policy/2021/069.html

わが国において、データ保護や AI 規制に関して、民間企業の方がその対応に積極的な印象がある。これは、AI が実装されたシステムが炎上した場合、企業価値を大きく損なうかもしれないという危機感からくるものであるように思われる。

(22) アジャイル・ガバナンスについて、例えば経済産業省「アジャイル・ガバナンスの概要と現状」を参照。https://www.meti.go.jp/press/2021/03/20220303003/20220303003-1.pdf

困難となる場面も想定される。このような事態に対処するために、ヨーロッパ委員会の示す AI のリスク分類の指標はわが国の AI に関するガバナンスを検討する際に有益である。高リスクな類型の規制はハードロー的な規制を、その他類型の統制には、対話を中心としたステークホルダー間の自主的な対応を軸とした運用といった対応が考えられる。

AI の警察利用は、高リスクな AI 利用の典型である。しなしながら、わが国において AI を用いた生体認証技術の警察利用には、成文法による制限が事実上存在しない現状にあり(23)、AI システムによって個人の基本権が不当に損なわれないように適切なルール作りが急がれる。AI の警察利用には、高リスクの中の高リスクが存在しており、その利用が認められるためには刑事訴訟法及びそれに準じた個別法による統制を行える法整備を通じた体制づくりを進めなければならない。

(23)　わが国における現状について、拙稿・前掲註(20)・100 頁以下参照。

Reprinted from

KITAKYUSHU SHIRITSU DAIGAKU HOU-SEI RONSHU

Journal of Law and Political Science. Vol. L No. 1/2

October 2022

Tendenz in der KI-Regulierung in der EU

Aus der deutschen Perspektive

MIZUNO Yoichi