Vol.2021-EIP-92 No.13
2021/6/8

EU における 2021 年 AI 利用規則案にみる AI リスクと法規制の枠組み

寺田麻佑[13] 板倉陽一郎[23]

欧州委員会が 2021 年 4 月 21 日に発表した，AI の利用に関する規則案は，AI に関する世界初の包括的な法的規則となる見込みの案である．AI 採用の際に顔認証の仕組みを取り入れるのであれば，事前に当局による審査が必要となるといった規則提案や，各種規定に違反した場合の高額な罰金案がその内容となっている．また，AI のリスクの高さが 4 段階に分けられており，その分類によって，EU による評価が必要かどうかが変わる仕組みとなっている．本論考は，AI のリスクの分類やその規制について，どのような形で法規制を行おうとしているのか，AI 規則案の内容と日本へのインパクトも含めて検討を行うものである．

Draft AI Regulations 2021 in the EU and its Framework for AI Risk and Regulation

MAYU TERADA[13] YOICHIRO ITAKURA[23]

The European Commission's draft regulations on the usage of AI, announced April 21, 2021, are expected to become the world's first comprehensive legal rule on AI. The proposals include proposed rules that would require prior regulatory approval if facial recognition was to be incorporated into AI-powered recruitment, and proposed hefty fines for breaches of provisions. There are also four levels of AI risk, each of which may or may not require EU assessments. The purpose of this study is to examine how laws and regulations on the classification and regulation of AI risks are to be implemented, including the content of the proposed AI rules and their impact on Japan.

1. 問題の所在：EU における AI 規制の課題

欧州委員会が 2021 年 4 月 21 日に発表した AI の利用に関する規則案は，AI に関する世界初の，ソフトローではなくハードローによる規制枠組みとなる可能性がある．

この AI に関する世界初の包括的な法的規則となる見込みの案は，これまでにも検討の方向性がリークされるなどしていたところ，具体的には，AI 採用の際に顔認証の仕組みを取り入れるのであれば，事前に当局による審査が必要となるといった規則を提案することや，各種規定に違反した場合の高額な罰金案がその内容となっている．

また，AI のリスクの高さが 4 段階に分けられており，その分類によって，EU による評価が必要であるかどうかが変わる仕組みとなっているとのことである．

欧州委員会は，AI のリスクに対処し，欧州が世界で主導的な役割を担うことを定めた，AI に関する初の法的枠組みを提案している[1].

ここにみえる EU の規制強化は，法規制として日本にも大きなインパクトを与えるものである．

そこで，本論考においては，AI のリスクの分類やその規制について，どのような形で法規制を行おうとしているのか，AI 規則案の内容と日本へのインパクトも含めて検討を行う．

2. AI 規制法案 2021 の具体的内容

EU による AI 規則へのアプローチの提案」 (規則案) は，2020 年 2 月に発表された欧州委員会による，AI の 「ハイリスク」 アプリケーションに関するホワイトペーパー（白書）を受けたものである．

本 AI 規制案は，全体として，AI 技術の（危険な）使用を規制し，そのことによって偏見や差別を防止しようとするものである．また，企業による AI の使用については，と個人のニーズや基本的権利とのバランスをとることを求めている．また，AI 技術がもたらしうる，様々な複雑な問題にも対応しようとしている．このような規制と同時に，しかし，AI の利用と発展を促進しようともしている規制と説明されている．

EU による AI 規則案は，特定の目的のために人工知能を使用することについて，たとえばその AI を，その他の，特定の調査やテロリズムなどのために利用するなどといった他の分野での使用を規制することを禁止するものでもある．本 AI 法案には，規則違反に対する重大な罰則も盛り込まれ

1 国際基督教大学教養学部上級准教授
Senior Associate Professor of Law, College of Liberal Arts, International Christian University
2 弁護士・ひかり総合法律事務所
Attorney at Law, Hikari Sogoh Law Offices
3 理化学研究所革新知能統合研究センター（AIP）
RIKEN AIP

ており，世界の年間売上高の 6%または 3000 万ユーロのいずれか大きい方までの課徴金が課される可能性がある．

2.1 AI 規制法案の具体的目標

包括的な EU における AI 規則案の目的は，AI の利活用が人々の生活やビジネスに大きな影響を及ぼすことにかんがみ，「EU 市場に投入され，利用される AI システムが安全であり，基本的権利と EU の価値に関する既存の法律を尊重することを確保すること．AI への投資とイノベーションを促進する法的確実性を確保すること．そして，AI システムに適用される基本的権利と安全要件に関する現行法のガバナンスと効果的な執行を強化すること，そして，合法的かつ安全で信頼できる AI アプリケーションのための単一市場の開発を促進し，市場の断片化を防ぐこと．」にあると説明されている[2].

2.2 AI 法（仮称）と他の政策領域との整合性

今回の AI 法（仮称）は，AI の発展と利用に関する AI 白書が目標とするパッケージの一部えあり，デジタル世代となる予定の次の特に 10 年間を支える重要な柱となる予定とされる[3].

AI駆動型イノベーションが目指されるこのAI法(仮称)は，EU の他の，データガバナンス法やオープンデータ規則や，その他 EU のデータ戦略などと歩調を合わせるものであるとも説明されている[4].

そのため，今回の AI 法は，これまでにすでに発表されており，高リスクな AI システムがすでに使われているか，これから使われる可能性の高い分野の規制とも整合性を持つものである[5].

2.3 専門家会合に基づく提案であること

今回の AI 法の提案は，加盟各国と EU 市民，NGO やビジネス・社会関係上の法人や学術団体などによる AI に関するハイレベル専門家会合（High-Level Expert Group on AI : HLEG）の提案に基づいている．この HLEG は，52 人の専門家から構成され，欧州委員会に AI 戦略について提案を重ね，2019 年 4 月には，欧州委員会は，この HLEG の信頼できる AI に関する提案の中心的な構成提案要素を支持し，それ以降も検討を続けてきた．そして，AI 白書も発表され，さらに多くのステークホルダーなどとの検討を経てインパクトアセスメントも行われた．

2.4 インパクトアセスメント

2020 年 12 月 16 日に行われた規制検討会合は否定的な見解を示したが，その後，実質的な内容の変更などを経て，2021 年 3 月 21 日の規制検討会合においては，規則案への肯定的な見解となったと説明されている．

そのなかにおいては，とくに，本規則案が課す規制が EU の基本権憲章に定める基本権に抵触しないかということも具体的に検討され，いくつか欧州市民の経済活動の自由を侵害する可能性がある点についても，比例原則に照らして適合的である（基本権を侵害しない）と分析された．

2.5 背景となっている AI 白書

欧州の AI 白書は，AI システムの利用において EU は世界をリードする存在になるべきであるとして，市民の価値観と権利を尊重した AI 開発における信頼性と優越性を実現するための政策オプションを示している．

AI 白書は，AI システムが複雑かつリスクを包含することに鑑み，信頼構築のために EU がこれまでに形成してきた消費者保護や競争ルール，GDPR といった個人データ保護のルールに加えて，高リスクの AI に関するルールの導入が必要であると提案したものである[6].

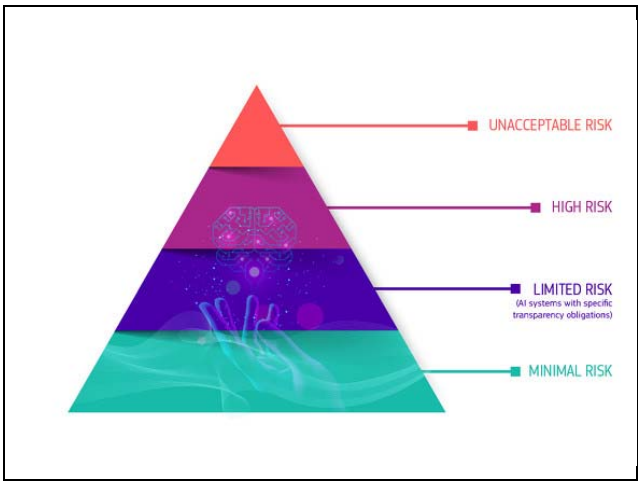
3. AI のリスク別の規制

3.1 AI 法（規制枠組み規則）におけるリスク別の規制

本 AI 法の核心的内容は，AI を利用する際の基本的人権や安全性を確保するために，AI に関する利用者の信頼を確保するための法的安定性のために，AI システムをリスク別に，特に以下の 4 つのリスクに分けて規制するものである．

すなわち，容認できないリスク，高リスク，制約されたリスク，最低限のリスクの 4 つである．

（参考図：AI 法における 4 つのリスク）



3.2 リスクごとの規制—容認できないリスク

１の容認できないリスクについては，サブリミナル（潜在意識に作用する）技術の利用や，政府が個人の信用力を書く付けする社会信用システムを運用すること，法の執行目的に利用することも含めた，顔認証などを含めた遠隔生体認証技術を公共の場において利用すること，といった，EU の基本的権利（人権）に反する AI システムの利用が該当するとされた．

これらの容認できないリスクにかかわる AI システムの利用は禁止されることとなる．

3.3 高リスク—適合性評価手続きの義務化

雇用場面や，教育場面，そして医療場面や法の執行などの分野における重大な利益に関係する可能性の高い意思決

定や，重要なインフラストラクチャー，生体認証で用いられる AI といった AI システムは高リスクに分類され，規制の対象となる．

こういった高リスクなことに関係するシステムに AI を利用する提供事業者は，AI システムの提供を開始する前に，規則案が規定する適合性評価手続をとることが義務化される．

また，AI システムを高リスク分野において利用しはじめたのちも，リスクや品質の管理を定期的に実施する必要があるとされた．

3.4 制約されたリスクと最低限のリスク

これらについては，規制の対象外となり，新たな義務は現状では検討されていないが，自動応答（AI チャットボット）プログラムなどについては，人とかかわる部分があるため，AI システムが「利用されている」といったことを利用者に開示する必要があるといった義務が課される．

3.5 義務の主体と違反の制裁

義務の履行主体は各加盟国となり，監督をおこなう．そして，事業者が違反した場合には，最大 3000 万ユーロもしくは，全世界における前年度の総売上高の 6 パーセントまでの制裁金が課される（課徴金）．

3.6 リスクベースアプローチ

これらは，リスクベースアプローチであり，AI システムを具体的に検討し，義務をそれぞれ検証しながら適用するものである[7].

4. 欧州産業界からの AI 規制法案への危惧表明

4.1 いち早く出された懸念表明

AI 規制枠組み規則案については，すでに EU の産業界から，企業の負担が増加することに関する懸念が表明されている．

なお，リスクベースアプローチについては否定的な声はなく，歓迎するとしているが，企業の負担が増え，その結果，イノベーションが阻害されるとしている．

具体的には，たとえば，デジタルヨーロッパ（情報通信技術（ICT）関連の産業団体）は，GDPR と同様に，中小企業やスタートアップ企業の負担が増大することを懸念し，迅速さが求められる AI ソフトウェアが適合性評価の対象となったことへの懸念を表明している[8].

また，欧州の機械電気電子金属加工産業連盟（Orgalim）も，AI システムとはいったい何を指すのか定義をより明確化すること，産業用 AI は高リスクとみなされないことを保証することを求めること，そして，適合性評価の義務化は企業の負担を増やし，安全性を高めることには必ずしもつながらないのではないのかという懸念を発表している[9].

4.2 財政支援を求める声明

欧州家庭用電気機器産業協会は（APPLiA）が開催した会議においては，AI の定義を明確化・共通化することが重要であることや，IoT イノベーション・アライアンス（AIOTI）とともに，AI の研究開発への財政支援の拡大が必要であるとの意見が出された[10].

5. 禁止される AI 利用形態と生体認証

AI の利用のなかでも，大規模な監視システムや，差別につながる可能性の高い，商業目的も含めた社会的なスコアリングシステムへの AI の利用は禁止される方向での提案がなされている．

また，人間の行動うや意思決定，意見を有害な方向へ操るために設計された AI システムは禁止され，個人データを利用し，人や集団の潜在的な弱みにつけこむような有害な予測を利用する AI のシステムも禁止されることとなる．

6. 高リスクな AI システム

6.1 加盟国政府における認証機関による審査

公共の場を含めた顔認証技術の利用については，公認された機関の関与を通じることによって，より厳格な適合性評価手順を踏む必要があると提案されている．

認証評価手続きにおいては，認証機関は定められた目的でシステムを利用する際の誤差によって生じる危険（とりわけ年齢，民族，性別，または障害等に関するもの）の頻度とその重大度を考慮する必要があり，その他，特に民主的プロセスへの参加や市民参加，さらには参照データベース内の人々のインクルージョンに関する手段，必要性，および比例について，その社会的影響を考慮しなければならない，と提案されている[11].

なお，高リスクな AI システムについては，下記が明記されている[12].

> ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)
> High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:
> 1. Biometric identification and categorisation of natural persons:
> (a) AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons;
> 2. Management and operation of critical infrastructure:
> (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.
> 3. Education and vocational training:
> (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
> (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and

for assessing participants in tests commonly required for admission to educational institutions.
4. Employment, workers management and access to self-employment:
(a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.
5. Access to and enjoyment of essential private services and public services and benefits:
(a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;
(c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.
6. Law enforcement:
(a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
(b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
EN 5 EN
(c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);
(d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;
(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;
(f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;
(g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.
7. Migration, asylum and border control management:
(a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
(b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;
(c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;
(d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.
8. Administration of justice and democratic processes:
(a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

6.2 適合性評価の実施の頻度について

適合性評価は，AI システムの変更があった場合や，内容の変更があった場合は，その都度受けなければならない．

すなわち，AI 法（AI 規則）への準拠に影響しかねない変更が AI システムに生じた場合や，AI システムの利用目的に変更が生じた場合には，新たに適合性評価を実施することが適切であるとされている．

また，市場に出された，あるいは運用を開始した後にも AI が「学習」を続ける（機能の実行方法を自動的に適応する）といった形のシステムについては，その AI のアルゴリズムおよびパフォーマンスに生じた変化の度合いに鑑み，適宜の段階において，すでに受けた適合性評価において評価しつくされていないと考えられる場合に，新たに AI システムの適合性評価を実施する必要があるとされる．

6.3 適合性マークの付与の可能性

AI 法に準拠する企業には，適合性評価を受けたという証

拠（根拠）となる，認証評価マーク（適合性マーク）が付与される．

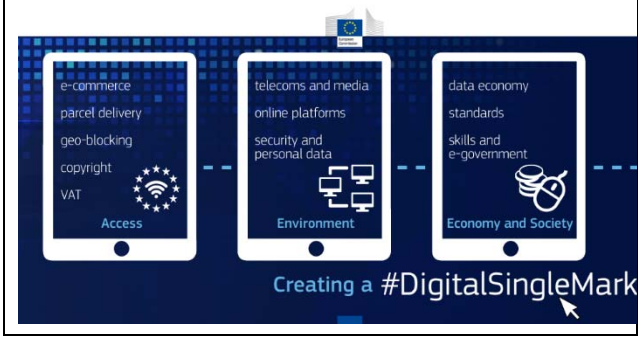
このマークがあることによって，利用者（ユーザ）の信頼を獲得することもでき，また，EU のデジタル単一市場全体で摩擦のないサービスを提供できると提案されている．

すなわち，特に高リスクの AI システムを EU 内で自由に利用するには，適合性評価認証結果を証明するマークを取得して AI 法との適合を示す必要があることとなる．

EU 加盟国は本規則で定められた要件に準拠する AI システムの市場展開または運用を妨げる障害を作るような形で法整備をしてはならないし，法執行の妨げとなる運用をしてはならないとされる．

7. デジタル単一市場戦略のなかの AI 法

欧州におけるデジタル単一市場戦略は，欧州全域における消費者と企業に対するデジタル商品やサービスのよりよいアクセスと，デジタルネットワークと革新的なサービスに関する適切な条件や競争環境を整備すること，そして，デジタル経済の成長力の最大化を目指すことという三つの柱から成り立っている．



（デジタル単一市場の 3 本の柱に関する図）

この AI 法も，デジタル市場戦略の中に位置づけられ，AI システムをデジタルシステムの中でハーモナイズさせてうまく活用することを意図しているものである．

デジタル分野における AI 法も加えた形での EU のリーダーシップは以下のような図で説明されている13.

8. おわりに

本 AI 法案は，まだ提案されている途中のものであり，これから修正される可能性も高いものである．

しかし，実際に GDPR のように施行されることとなると，域外適用をおこなうことを明言していることも含め，日本への影響も大きなものとなるものと考えられる．

具体的には，課徴金としての制裁金が EU 市場とかかわる AI システム利用企業にとって大きな障害となる可能性がある．

また，それぞれ認証評価を高リスク AI についてはとらなければいけないと義務付けされることについても，企業にとっては大きな負担となる．

EU にとってのリスク分類が，どのくらい世界基準となるのか，今後の検討が進められていくこととなるものと考えられるが，日本においても AI 利活用の基準の詳細化をおこなうとともに，EU の基準に対して意見表明をするなどの積極的な関わりを行っていく必要があるものと考えられる．

参考文献

[1] See, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence (2021 年 5 月 6 日最終閲覧，以下同じ)
[2] EUROPEAN COMMISSION Brussels, 21.4.2021 COM(2021) 206 final 2021/0106 (COD) , 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, p.3.
[3] *Ibid,* p.5.
[4] See, proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.
[5] Above note 2, p.9.
[6] EUROPEAN COMMISSION, Brussels, 19.2.2020, COM(2020) 65 final, WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
[7] Above note 2, p.38－54.
[8] New AI rules must be streamlined for Europe to become a global innovation hub – DIGITALEUROPE, https://www.digitaleurope.org/news/new-ai-rules-must-be-streamlined-for-europe-to-become-a-global-innovation-hub/.
[9] European Regulation on Artificial Intelligence – Orgalim calls for legal clarity and workability, Orgalim, https://orgalim.eu/news/european-regulation-artificial-intelligence-orgalim-calls-legal-clarity-and-workability.
[10] The EU race towards AI: striking a balance between safety and innovation - APPLiA - Home Appliance Europe, https://www.applia-europe.eu/topics/living-the-connected-home/387-the-eu-race-towards-ai-striking-a-balance-between-safety-and-innovation.
[11] Above note 2, p.38－54.
[12] COM(2021) 206 final.
[13] COM（2021）205final, p.37.