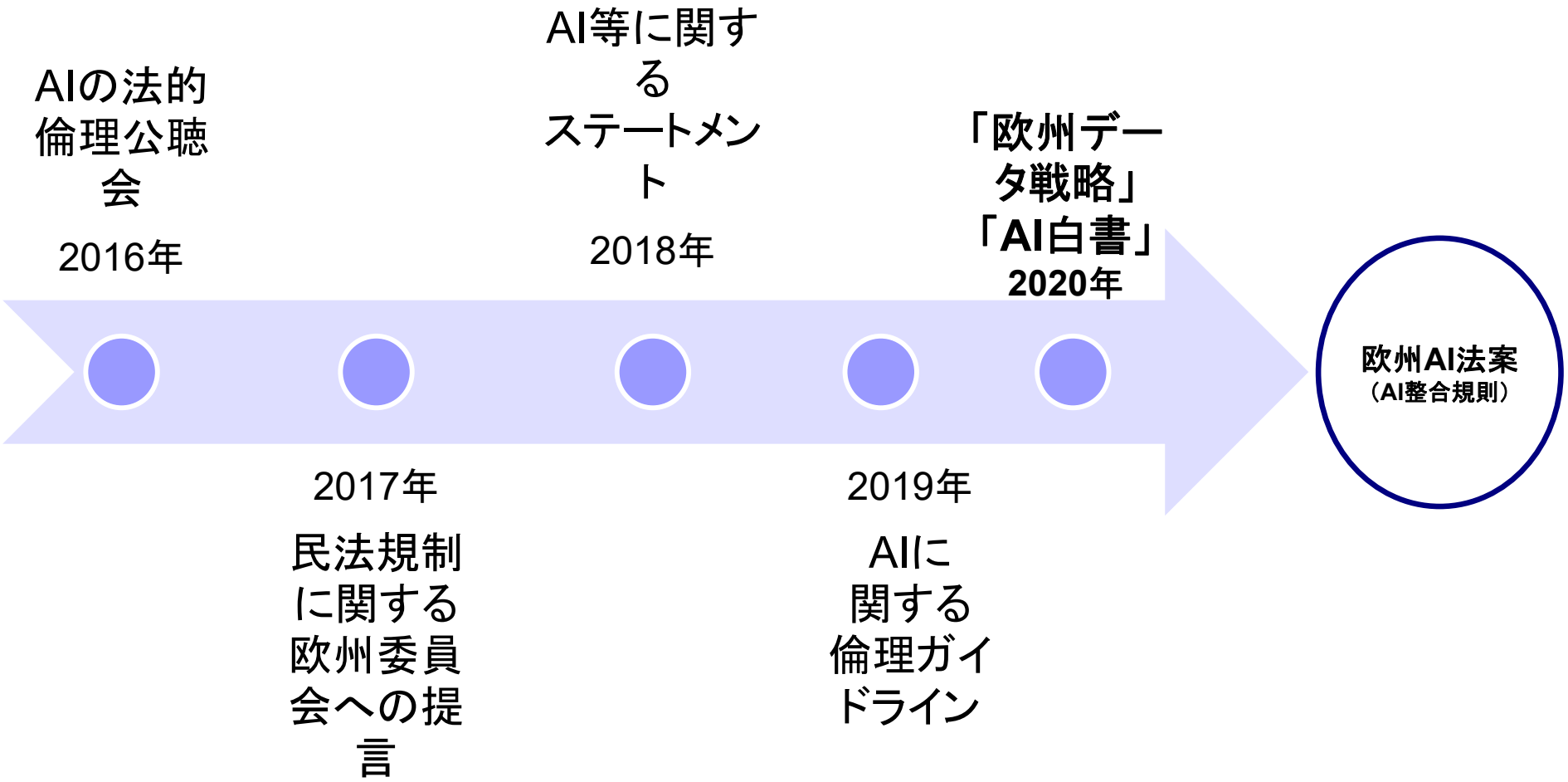
日米欧のAI規制方針の相違と方向性

慶應義塾大学　総合政策学部　教授
新保 史生

欧州AI政策の概要



1. EUのロボロー・ガイドライン(2014年9月)

- Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics, FP7-SCIENCE-IN-SOCIETY-2011-1, Project No.: 289092(報告書作成費用:149万7966ユーロ)
- ロボットをめぐる法的課題の体系的な検討を試みた最初の取り組み
- 体系的なガイドラインの提示には至らず、具体的な問題を手がかりに検討に着手せざるを得なかったとしている

具体的な検討課題

- ①ロボット(ドローンなど文字通りのロボット)
- ②自動運転(自動操縦)
- ③モビルスーツ・義足等(装着型、ウェアラブル)
- ④手術・遠隔地・宇宙(リモート操作、遠隔地対応)
- ⑤医療、介護、福祉(医療等分野)
- ⑥災害・レジリエンス

法的課題について

- ①健康、安全、環境、利用者保護のための規制(安心・安全な利用環境の保護)
- ②法的責任 製造物責任(物の製造物責任、情報の製造物責任は認められるか)
- ③知的財産(ロボットそのもの、ロボットが創作したもの)
- ④プライバシー
- ⑤権利能力(エージェント)

ＥＵにおけるAI規制に向けた検討の系譜

欧州連合「犯罪予防、調査、犯罪捜査目的若しくは犯罪訴追手続又は刑事罰の執行のための主務執行機関による個人データの処理に関する自然人の保護及び当該データの自由な移動並びに欧州議会枠組決定2008/977 / JHAの撤回に関する欧州議会及び欧州理事会2016年4月27日指令2016/680」（2016）

- (European Union (2016) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA)

欧州評議会議員会議、欧州議会勧告2102（2017）「技術的収束、人工知能及び人権」(2017)

- (Council of Europe, Parliamentary Assembly, Recommendation 2102 (2017) 1, Tech-nological convergence, artificial intelligence and human rights)

欧州連合、欧州委員会「人工知能（AI）コミュニケーションに関する調整計画」

- (European Union, European Commission (2018) Coordinated plan on Artificial Intelligence (AI) Communication)

欧州委員会「欧州委員会から欧州議会、欧州理事会、欧州理事会、欧州経済社会委員会及び欧州人工知能地域委員会への連絡事項」(2018)

- (European Commission (2018) Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe)

欧州評議会「個人データの処理に関する個人保護のための近代化条約」（2018）

- Council of Europe,Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data)

欧州連合「AI、ロボット、自律型システムに関するステートメント」(2018)

- (European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and ‘Autonomous’ Systems, Brussels, 9 March 2018)

欧州評議会、欧州司法制度効率化委員会「司法制度における人工知能の利用に関する欧州倫理憲章」（2018年）

- (Council of Europe, European Commission for the Efficiency of Justice (2018) European Ethical Charter on the use of artificial intelligence in judicial systems)

欧州評議会議員会議「アルゴリズムによる正義についての勧告提案：警察及び刑事司法制度における人工知能の役割」（2018）

- (Council of Europe, Parliamentary Assembly (2018) Motion for a recommendation about Justice by algorithm . the role of artificial intelligence in policing and criminal justice systems)

欧州連合、欧州委員会の人工知能に関する高等専門家グループ「信頼できるAIに関する倫理ガイドライン」（2019）

- (European Union, European Commission’s High-Level Expert Group on Artificial Intelligence, Ethics guidelines for trustworthy AI)

欧州委員会「AI白書」

- WHITE PAPER On Artificial Intelligence -A European approach to excellence and trust, 19.2.2020 COM(2020) 65 final

EU「AI、ロボット、自律型システムに関するステートメント」

(European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and 'Autonomous'Systems, Brussels, 9 March 2018)

概要

- 人工知能、ロボット技術及びいわゆる「自律型」の技術進歩
  - 道徳に係る問題について、喫緊に対応が必要であり、かつ、複雑な問題を提起
- 倫理的、社会的および法的な課題に対する答えを見つけこと
  - 異なるイニシアチブのパッチワークとして共通の利益を求める方向性を示すこと
- 集合的、広範囲、包括的な検討と対話の必要性を強調
  - 社会を組織する上で求められる価値観、社会においてテクノロジーが果たすべき役割に焦点を当てた対話が必要

本文書の目的

- 共通の国際的な倫理的及び法的枠組みの構築を目指す取り組みへの着手を示すもの
  - 人工知能、ロボット技術、「自律」システムの設計、製造、使用および管理が対象
- 基本的な倫理原則を提案
  - EUの各条約及びEU基本権憲章に定められた価値観に基づくもの

EU「AI、ロボット、自律型システムに関するステートメント」が示す主な課題

（1）安全性、セキュリティ、危害の防止及びリスクの軽減に関する問題

- 相互接続されたAIと「自律型」のデバイスを使用する世界を安全かつ安全にするための方策

（2）人間の道徳的責任についての問題

- 高度なAIとロボットの構成要素を備え、動的で複雑な社会技術システムについて、道徳的な問題について検討する組織は？
- 道徳的責任の帰属先、不都合な結果についても責任分配
- 「管理の共有(shared control)」や人間とスマートマシンとの関係について検討することは意義があるか
- 道徳的「緩衝領域(crumple zones)」として、人間は「自律的な」装置のエコシステムの一部でしかないのか

（3）ガバナンス、規制、設計、開発、検査、監視、テスト及び認証に関する問題

- 個人や社会の福祉に役立つように、そして社会をこの技術に対して安全にするために、私たちの制度や法律はどのように再設計されるべきか？

（4）上記の問題の基調となる制度、政策及び価値観に関する意思決定を含む民主的な意思決定の問題

- プロファイリング、マイクロターゲティングを可能にする機械学習、ビッグデータ、行動科学の組み合わせに基づく高度なナッジング技術の使用により市民がどの程度恩恵を受けるのかについて確認するための調査。商業的又は政治的な目的に応じた選択アーキテクチャの調整および操作。

（5）AIと「自律型」システムの説明可能性と透明性についての問題

EUのステートメントの検討において参照されている資料

IEEE's(Institute of Electrical and Electronics Engineers) policy paper on ‘Ethically Aligned Design’

- http://standards.ieee.org/news/2016/ethically_aligned_design.html

ITU's (International Telecommunication Union) Global Summit ‘AI for Good’

- https://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx

ACM's (Association for Computing Machinery) work on the issue, including a major AAAI/ACM ‘Conference on AI, Ethics, and Society’in summer 2017

- http://www.aies-conference.com/

IBM, Microsoft and Google's DeepMind have established their own ethic codes on AI and joined forces in creating broad initiatives such as the ‘Partnership on AI’in 2018

- https://www.partnershiponai.org/

OpenAI’7

- https://openai.com/

Asilomar AI Principles

- https://futureoflife.org/ai-principles/

The Forum on the Socially Responsible Development of Artificial Intelligence held by the University of Montreal in November 2017, 'Declaration for a Responsible Development of Artificial Intelligence’ has been developed. It is now publicly accessible on an online platform where all sectors of society are invited to comment on the text.

- http://nouvelles.umontreal.ca/en/article/2017/11/03/montreal-declaration-for-aresponsible-development-of-artificial-intelligence/

- (a)人間の尊厳 (Human dignity)
- (b)自治 (Autonomy)
- (c)責任 (Responsibility)
- (d)正義、公平及び相互依存(Justice, equity, and solidarity)
- (e)民主主義 (Democracy)
- (f)法の支配と説明責任 (Rule of law and accountability)
- (g)安全性、安全性、身体的及び精神的完全性(Security, safety, bodily and mental integrity)
- (h)データ保護とプライバシー(Data protection and privacy)
- (i)持続可能性 (Sustainability)

欧州委員会「AI白書」(2020)

構成

- ①現行のEUにおけるAIをめぐる政策的な枠組み
- ②欧州における具体的な政策(投資や技能向上及び中小企業対策)
- ③AIシステム開発に必要なデータ利用のあり方
- ④将来的な欧州における法規制に向けた主な論点
- ⑤ステークホルダーの貢献と政策立案

規制の枠組みの方向性

- 新たな分野におけるイノベーションの促進を前提とした規制であるとともに、欧州における価値や原則を尊重した上での技術開発を目指すもの
- AIの利用に伴う新たな可能性とともに生ずるリスクについて、現行のEUの法規制の枠組みの範囲内ですべての問題をカバーしきれていないとともに、効果的な規制の方法について検討
- 現行のEU加盟国の法的枠組みを踏まえた上で、欧州企業が最大限の利益を享受できるようにバランスが取れた規制の枠組みを検討することが必要

中核となる要素

- ①基本的権利に対するリスク(具体的には差別やプライバシーおよびデータ保護の観点からの問題)
- ②安全及び法的責任をめぐるリスク

AI白書が示すEUにおける法的枠組みの検討事項

①基本的権利の観点からの問題として、EU基本権憲章は民間部門のみが関わる問題については適用がないことや、雇用、社会保障、教育、公的サービスなどの特定の分野にしか適用されないこと

②製造物の観点からの問題として、EUの製造物責任に関する法令は製造物に対しては適用されるがサービスには適用されないこと。具体的には、ヘルスサービス、金融サービス、運送サービスにおいてAIが用いられる場合の問題

③AIの研究開発における責任主体の不明確さとして、規制が適用されるのは開発者が製造者である場合に限られること

④製造物の性質の変化として、製造物にAIが組み込まれることによって従来不要であったアップデートがソフトウェア同様に必要になるといった製造物の性質の変化に伴う問題

⑤新たなリスクの出現について、新たな安全性の観点からのリスクが出現する可能性があること

⑥法執行の困難性について、透明性を担保することが困難であるため自動化された意思決定における差別の有無について証明することが法執行機関にとっては困難であること

AI白書が示す法的義務として検討すべき項目

①開発者に対する説明責任と透明性の確保

②利用者に対する透明性の確保と情報提供

③AIシステムのリスク軽減のための設計原則

④AIの学習データの質と多様性の確保

⑤開発者に対するリスクアセスメントの実施とリスク軽減のための措置

⑥自動化された意思決定に対する人間による関与方法の検討

⑦製造物について追加で必要な安全対策

EUの規制力

- 遠藤乾･鈴木一人編『EUの規制力』日本経済評論社(2012)。

ブリュッセル効果

- Anu Bradford, *The Brussels Effect,* Northwestern University Law Review, Vol. 107, No. 1, 2012 (Columbia Law and Economics Working Paper No. 533, 27 Apr 2016 Last revised: 6 May 2016)。

新保史生「EU新AI整合規則提案にみるAI規制戦略の構造・意図とブリュッセル効果の威力」ビジネス法務2021年8月号PP. 188-193(2021)

(1)利用規制
- 人工知能の使用行為禁止事項(5条)

(2)高リスクAIIに関する義務
- 高リスクAIの分類及び対象リスト(6条・7条)
- 高リスクAIの要件(8-15条)
- プロバイダ等の義務(16-29条)

(3)適合性評価
- 通知機関(30-39条)
- 適合性評価等(40-51条)

(4)透明性要件
- 特定のAIシステムに対する透明性(52条)
- 行動規範の策定(69条)

(6)ガバナンス
- 欧州人工知能委員会の設置等(56-59条)

(7)監督及び法執行
- 高リスクAIに関するデータベース(60条)
- 市販後のモニタリング(61条)
- インシデント報告義務(62条)
- 法執行(63-68条)
- 罰則・制裁金(71-72条)

①経済的・社会的利益
- AIはあらゆる産業や社会活動において経済的・社会的に多大な利益をもたらす可能性
- AIの利用によって、社会的・環境的に有益な結果をもたらし企業や欧州経済に重要な競争力を提供
- 気候変動、環境と健康、公共部門、金融、モビリティ、家政学、農業など、影響の大きい分野で特に必要

②個人や社会への新たなリスク
- AIの社会経済的利益をもたらす要素や技術は、個人や社会に新たなリスクや負の影響をもたらすこともある
- AIは人々のためのツールであり、人間の幸福度を高めることを究極の目的として、社会に貢献する力となるべき

③EUの価値観、基本的権利の保障
- EUの技術的リーダーシップを維持し、EUの価値観、基本的権利、原則に従って開発・機能する新技術からEU市民が恩恵を受けることができるようにすることは、EUの利益となる

④信頼のエコシステム構築(政治的背景)
- AIの導入を促進し新技術の利用に関連するリスクに対処するため、信頼できるAIのための法的枠組みを提案すること
- EUが安全で信頼できる倫理的なAIシステムの開発と利用において世界的な主導権を獲得するという政治目的

① EU市場に投入され利用されるAIシステムの安全規制を、基本的権利とEUの価値を保護する既存の法令に基づき実施すること

② AIへの投資とイノベーション促進

③ 基本的権利の保障と安全性確保のためAIシステムへのガバナンスと効果的な法執行

④ 信頼できるAIにより単一市場の発展を促進し市場の断片化を防ぐこと

(a) EUにおいてAIシステムを上市、サービス開始及び利用するための整合規則

(b) 特定のAI利用禁止行為

(c) 高リスクAIシステムに関する要求事項及び義務

(d) 自然人との対話を目的としたAIシステム、感情認識システム、生体情報分類システム、画像・音声・映像コンテンツの生成又は処理を目的としたAIシステムの透明性に関するルールの整合性確保

(e) 市場のモニタリングと監視

EUのAI規制法体系（将来的な）

AI法案
（整合規則提案）

機械規則提案

AI法的責任
指令案

データ法案

EUのAI法案

欧州委員会案
人工知能に関する整合規則（人工知能法）の制定及び
関係法令の改正に関する欧州議会及び理事会の規則提案

欧州議会採択案
欧州議会が2023年6月14日に採択した人工知能に関する整合規則（人工知能法）の制定
及び域内の関連法令の改正に関する欧州議会及び理事会の規則提案に関する修正案

EUのAI法案の名称について

2021年4月21日に公表されたEUのAI法案の名称の原題文

- 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

2023年6月14日の欧州議会採択版

- Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

欧州委員会が提出した規則提案

- 「人工知能に関する整合規則（人工知能法）の制定及び関係法令の改正に関する欧州議会及び理事会の規則提案」（略称：AI整合規則提案）と訳出

欧州議会採択案

- 「欧州議会が2023年6月14日に採択した人工知能に関する整合規則（人工知能法）の制定及び域内の関連法令の改正に関する欧州議会及び理事会の規則提案に関する修正案」と訳出

「人工知能に関する調和の取れたルールを定める規則の提案」と訳している場合も多い

- EUのAI法案が「整合規格」を核とする「整合規則」の法定を目指しているという趣旨を理解し、整合規則の目的と意図を把握する上で、EUのAI法案の条文訳
- 夏井高人「人工知能に関する整合化された規定を定め、欧州連合の一定の立法行為を改正する欧州議会及び理事会の規則（人工知能法）の提案（COM/2021/206 final）」法と情報雑誌6巻5号（2021年11月）を参照しその内容について適切に理解することが必要

AIに関するEUの新たな規則提案

- Europearn Commission, Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final, 2021/0106 (COD)

- Europearn Commission
  - 欧州委員会
- Proposal for a Regulation
  - 規則提案
- The European Parliament and of the Council
  - 欧州議会及び理事会
- Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)
  - 人工知能に関する整合規則（人工知能法）の制定
- Amending Certain Union Legislative Acts
  - 関係するEU法令の改正

新保 訳

欧州委員会「人工知能に関する整合規則（人工知能法）の制定及び関係法令の改正に関する欧州議会及び理事会の規則提案」

「人工知能に関する整合規則（人工知能法）の制定及び関係法令の改正に関する欧州議会及び理事会の規則提案」の目的　（2021年4月21日公表）

- AIシステムのリスクに応じた利用規制

- 従来からEU市場に上市する製品の製造者や輸入者等に課されている製品安全規制同様の義務を

  高リスクに分類されるAIシステムにも拡充してCEマーキングの対象とするもの

- 適合性評価及び第三者認証制度の構築に基づく

  AIシステムの管理

2-1　提案の背景

①経済的・社会的利益

- AIはあらゆる産業や社会活動において経済的・社会的に多大な利益をもたらす可能性
- AIの利用によって、社会的・環境的に有益な結果をもたらし企業や欧州経済に重要な競争力を提供
- 気候変動、環境と健康、公共部門、金融、モビリティ、家政学、農業など、影響の大きい分野で特に必要

②個人や社会への新たなリスク

- AIの社会経済的利益をもたらす要素や技術は、個人や社会に新たなリスクや負の影響をもたらすこともある
- AIは人々のためのツールであり、人間の幸福度を高めることを究極の目的として、社会に貢献する力となるべき

③EUの価値観、基本的権利の保障

- EUの技術的リーダーシップを維持し、EUの価値観、基本的権利、原則に従って開発・機能する新技術からEU市民が恩恵を受けることができるようにすることは、EUの利益となる

④信頼のエコシステム構築（政治的背景）

- AIの導入を促進し新技術の利用に関連するリスクに対処するため、信頼できるAIのための法的枠組みを提案すること
- EUが安全で信頼できる倫理的なAIシステムの開発と利用において世界的な主導権を獲得するという政治目的

2-2　意図

① EU市場に投入され利用されるAIシステムの安全規制を、基本的権利とEUの価値を保護する既存の法令に基づき実施すること

② AIへの投資とイノベーション促進

③ 基本的権利の保障と安全性確保のためAIシステムへのガバナンスと効果的な法執行

④ 信頼できるAIにより単一市場の発展を促進し市場の断片化を防ぐこと

EUの2021年度調整計画に示されているAI関係戦略の背景

(Coordinated Plan on Artificial Intelligence 2021 Review, ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Fostering a European approach to Artificial Intelligence, Brussels, 21.4.2021 COM(2021) 205 final)

新たな法的枠組みは、既存の法令に基づく加盟国レベルでのガバナンスシステムと、欧州人工知能委員会（EAIB）の設置によるEUレベルでの協力の双方の取り組みによって実現

2-3　AI整合規則提案1条が示す目的及び対象

(a)　EUにおいてAIシステムを上市、サービス開始及び利用するための整合規則

(b)　特定のAI利用禁止行為

(c)　高リスクAIシステムに関する要求事項及び義務

(d)　自然人との対話を目的としたAIシステム、感情認識システム、生体情報分類システム、画像・音声・映像コンテンツの生成又は処理を目的としたAIシステムの透明性に関するルールの整合性確保

(e)　市場のモニタリングと監視

2-4　AI整合規則提案の根幹となる目的

「高リスクAIシステム」をEU市場に上市及び利用可能状態にするにあたって
遵守しなければならない手続的義務を新たに課すこと

事前規制

①適合性評価 → ②適合宣言書への署名 → ③CEマーキング

①AIデータベースへの登録 → ②市販後のモニタリング → ③インシデント報告義務

事後規制

機械指令が機械規則に改正されるなど関係法令を整備する目的

整合規則提案の射程

- AIシステムの安全リスク一般

機械規則の目的

- 機械一般において用いられるAIシステムの安全を総合的に保証すること

3　AI整合規則提案の構造

(1)利用規制

- 人工知能の使用行為禁止事項(5条)

(2)高リスクAIに関する義務

- 高リスクAIの分類及び対象リスト(6条・7条)
- 高リスクAIシステムのマネジメントシステム要求事項(8-15条)
- 高リスクAIシステムのプロバイダ(生成AIを含む)及びデプロイヤ(実装者)等の義務(16-29条)

(3)適合性評価

- 通知機関(30-39条)
- 適合性評価等(40-51条)

(4)透明性要件

- 特定のAIシステムに対する透明性(52条)
- 行動規範の策定(69条)

(6)イノベーション促進施策

- AI規制サンドボックス、小規模事業者・ユーザ支援等(53-55条)

(7)ガバナンス

- 欧州人工知能委員会の設置等(56-59条)

(8)監督及び法執行

- 高リスクAIに関するデータベース(60条)
- 市販後のモニタリング(61条)
- インシデント報告義務(62条)
- 法執行(63-68条)
- 罰則・制裁金(71-72条)

4　AIシステムのリスク分類

四段階のリスクに分類

①受容できないリスク

- 利用禁止AI（5条）

②高リスク

- 高リスクAI（6条）

③限定的なリスク

- 特定のAI（52条）

④低リスク又はリスク無し

- 低リスクAI
- 無リスクAI（69条）

人工知能の利用禁止行為（5条）

5条1項

(a)サブリミナル技術による人の行動を歪める利用

(b)弱い立場にある者の脆弱性につけ込む利用

(c)公的機関による社会的スコアリング

(d)法執行目的での公共の場におけるリアルタイム遠隔生体識別システムの利用

（5条2項乃至4項で利用する場合の例外を厳格に限定）

6　高リスクAIに係る義務

高リスクAIの分類及び対象リスト（6条・7条）
高リスクAIの要件（8-15条）
プロバイダ等の義務（16-29条）

高リスクAI

「附属書 II」に記載されている製品安全規制の対象となるAIシステム

かつ

(a)安全構成要素において用いられるAIシステム

(b)安全構成要素として用いられるAIシステムを含む製品として第三者適合性評価を受ける義務があるもの

上記二つの要件を満たす場合

①機械、②玩具、③海洋レクリエーション船舶、④リフト、⑤爆発性雰囲気装置、⑥無線機器、⑦圧力機器、⑧索道設備、⑨個人用保護具、⑩ガス燃焼機器、⑪医療機器、⑫体外診断用医療機器：（6条1項）

2条2項により、以下は適用除外　→　84条の評価・見直し条項が適用される

①民間航空、②マイクロカー、③農業・林業用トラクター、④船舶用機器、⑤鉄道システム
⑥自動車及びトレーラー等、⑦無人航空機：附属書 IIのB

６条１項の対象（附属書 IIのA）

- 1. 機械指令（2006/42/EC指令）
- 2. 玩具安全指令（2009/48/EC指令）
- 3. 海洋レクリエーション船舶指令（2013/53/EU指令）
- 4. リフト指令（2014/33/EU指令）
- 5. 爆発性雰囲気装置及び保護システム指令（2014/34/EU指令）
- 6. 無線機器指令（2014/53/EU指令）
- 7. 圧力機器指令（2014/68/EU指令）
- 8. 索道設備規則（(EU) 2016/424規則）
- 9. 個人用保護具規則（(EU) 2016/425規則)
- 10. ガス燃焼機器規則（(EU) 2016/426規則）
- 11. 医療機器規則（(EU) 2017/745規則）
- 12. 体外診断用医療機器規則（Regulation (EU) 2017/746規則）

６条１項の対象の詳細（附属書 IIのB）（現時点では義務規定の適用なし）

2条2項により附属書 II B（航空機、車両、船舶等）は、現時点では適用外

84条の評価・見直し条項が適用される

- 1. 民間航空安全規則（ (EC) 300/2008規則）
- 2. 二輪・三輪及び四輪マイクロカー規則（(EU) No 168/2013規則）
- 3. 農業用及び林業用トラクター規則（ (EU) No 167/2013規則）
- 4. 船舶用機器指令（2014/90/EU指令）
- 5. 鉄道システム相互運用性指令（Directive (EU) 2016/797指令）
- 6-1. 自動車及びトレーラー等システム規則（(EU) 2018/858規則）
- 6-2. 自動車及びトレーラー等型式認証規則（(EU) 2019/2144規則）
- 7. 無人航空機規則（ (EU) 2018/1139規則）

６　高リスクAIに係る義務

附属書IIIが規定する分野におけるAIシステムの利用も高リスクとしており、高リスクAIシステムがもたらす危害または悪影響のリスクに応じて欧州委員会が見直しを実施（７条）

６条２項（附属書Ⅲ）

- １.　自然人の生体識別及び分類
- ２.　重要インフラの管理・運用
- ３.　教育及び職業訓練
- ４.　雇用、労働者管理、自営業へのアクセス
- ５.　必要不可欠な民間サービスや公共サービス
- 使用することを目的としたAIシステム。
- ６.　法執行
- ７.　移民、亡命、国境管理
- ８.　司法行政及び民主主義プロセス

7　高リスクAIシステムのマネジメントシステム要求事項（8-15条）

リスクマネジメントシステムの構築、実施、文書化、維持をライフサイクル全体を通して実行される継続的な見直し改善手続から構成されるPDCAサイクルに基づくマネジメントシステム要求事項

8～15条が定める要求事項

①リスクマネジメントシステムの構築

②適切なデータガバナンス

③技術文書

④記録保持

⑤透明性及び利用者への情報提供

⑥人的監視

⑦正確性、堅牢性及びサイバーセキュリティ要件

高リスクAIシステムのプロバイダ（生成AIを含む）及びデプロイヤ（実装者）等の義務

①リスクマネジメントシステム要求事項を満たすこと

②品質マネジメントシステムの構築

さらに、以下の事項が定められている。

③技術文書の作成

④適合性評価の実施

⑤自動ログの生成

⑥是正処置

⑦情報提供義務

⑧主務当局との協力

⑨製造者の義務

⑩権限のある代表者の設置

⑪輸入者の義務

⑫ディストリビュータの義務

⑬ディストリビュータ、輸入者、利用者又はその他の第三者の義務

⑭高リスクAIシステム利用者の義務

９　適合性評価

第三者認証機関（Notified Body（NB））（30-39条）

- 各加盟国は、適合性評価のための第三者認証機関を設置する。
- その他、認証機関の要件等が規定されている。

適合性評価等（40-51条）

- 第43条の適合性評価手順に基づくNBによる認証制度
- CEマーキングの後に、第43条に定められた適合性評価手順に責任を有する第三者認証機関の識別番号を記載

適合性の推定

- 整合規格が存在する場合：整合規格を満たしていれば、要件適合が推定。既存の安全規制の延長線上（40条）

整合規格不存在の場合：欧州委員会が共通仕様を策定

- 共通仕様を満たしていれば、要件に適合していることが推定される（41条）

附属書 IIIの遠隔生体識別システムの適合性評価

- 整合規格又は共通仕様を「適用する」場合は、NBの関与のもと、①内部統制、②品質管理システムの評価、③技術文書の評価に基づく適合性評価手順を実施
- 整合規格又は共通仕様を「適用しない」場合、NBの関与のもと、①品質管理、②技術文書を提出
- 附属書 IIIの遠隔生体認証以外は、内部統制
- 附属書 IIのA記載の場合は、各法令（各規則や指令）に基づく適合性評価の実施

特定のAIシステムに対する透明性（52条）

行動規範の策定（69条）

- 特定のAIシステムに対する透明性確保義務は、高リスクAIだけでなく、低リスクのAIにも適用される
- 自然人とのやりとりが発生するAIシステムのプロバイダーは、AIとやりとりしていることがわかるように知らせる
- 感情認識、カテゴリー形成機能によって個人情報を処理する場合は、本人にその旨を知らせる
- 本物と見間違ってしまう程度に実際の人、物、場所等に類似する画像、音声、映像を生成するAIシステムを使用する者は、その旨を開示

11　イノベーション促進施策

AI規制サンドボックス、小規模事業者・ユーザー支援等（53-55条）

12　ガバナンス

欧州人工知能委員会の設置等（56-59条）

- European Artificial Intelligence Board（EAIB)の設置
- 各国の監視当局の代表、欧州データ保護監督官から構成され、欧州委員会が議長を務める。
- 加盟国の監視当局間の協調、新しい課題への対応に関する調整、AI規則の一貫した適用のための支援

高リスクAIに関するデータベース（60条）

市販後のモニタリング（61条）

インシデント報告義務（62条）

- プロバイダーはモニタリングシステムを設置し、文書化し、積極的かつ体系的にユーザー等からの情報を収集・分析
- ハイリスクAIシステムのプロバイダーは、加盟国当局に対して、法令に反する重大なインシデント等を報告
- ハイリスクAIシステムのプロバイダーは、重大な法令違反の場合は、15日以内に報告
- 重大なインシデントについては、インシデントとAIの関係の判明後速やかに報告

法執行(63-68条)

- 各加盟国監視当局は市場監視結果を定期的に欧州委員会に報告する
- 各加盟国監視当局は、学習データ等へのアクセスが認められる。合理的な場合には、ソースコードへのアクセスも認容

適合性評価等(40-51条)

- 第43条の適合性評価手順に基づくNBによる認証制度
- CEマーキングの後に、第43条に定められた適合性評価手順に責任を有する第三者認証機関の識別番号を記載

罰則・制裁金(71-72条)

- 罰則規定は、各加盟国が制定5条(利用規制)違反及びデータガバナンス要件に対する違反の場合
  - 4千万ユーロ(当初案は3千万)又は全世界の年間総売上の7%(当初案は6%)が上限の制裁金
- その他の違反の場合
  - 2千万ユーロ又は全世界の年間総売上の4%が上限の制裁金

一般データ保護規則（GDPR）との比較

個人情報保護制度の国際関係

OECD

プライバシー・ガイドライン(2013年改正)

越境協力勧告 /セキュリティ勧告等

GPA(旧プライバシーコミッショナー会議)

- データ保護機関としての参加基準
- 法的基礎、自主性及び独立性、国際基準との整合性、適正な機能
- 2017年9月の香港会議において日本は正式メンバーに

GPEN(Global Privacy Enforcement Network)

OECD加盟国間で国境を越えて個人情報保護への取り組みを行うネットワーク

欧州評議会条約第108号(1981)

及び同追加議定書 (2001)(個人データの自動処理に係る個人の保護に関する条約)

日本

個人情報保護法

行政機関等個人情報保護法

米国

個 別 法

EU

EU・米国データプライバシー枠組み(DPF)
2023年7月10日

一般データ保護規則(GDPR)

(2016年5月4日公布、5月24日施行、2018年5月25日適用開始)

①個人の基本的権利としてのプライバシー保護
②自由な意思に基づき、情報が与えられた上での明示的な同意(忘れられる権利、訂正・消去権、アクセス権、プロファイリング)
③いかなる状況や取扱者に対しても適用できる基本的原則
④技術中立性を保った上での新技術へ対応(プライバシー・バイ・デザインやプライバシー・バイ・デフォルト)
⑤実効性ある個人情報保護のための対策(利用目的の制限、データ管理者の責任、データ保護影響評価、セキュリティ侵害通知、データ保護のためのマーク(シール)制度の整備)
⑥断片的な対応の防止や法的確実性の確保(EU加盟各国の監督機関への個別承認が不要、規則違反は最大2千万ユーロ又は全世界での年間総売上高の4%の課徴金)
⑦基本原則に基づく法執行
⑧域外適用や第三国への安全なデータ移転

個情法24条指定
GDPR45条十分性決定
2019年1月23日

標準契約条項(SCC)
拘束力を有する企業の内部規程(BCR)

APPA(Asia Pacific Privacy Authorities)

プライバシー・フレームワーク

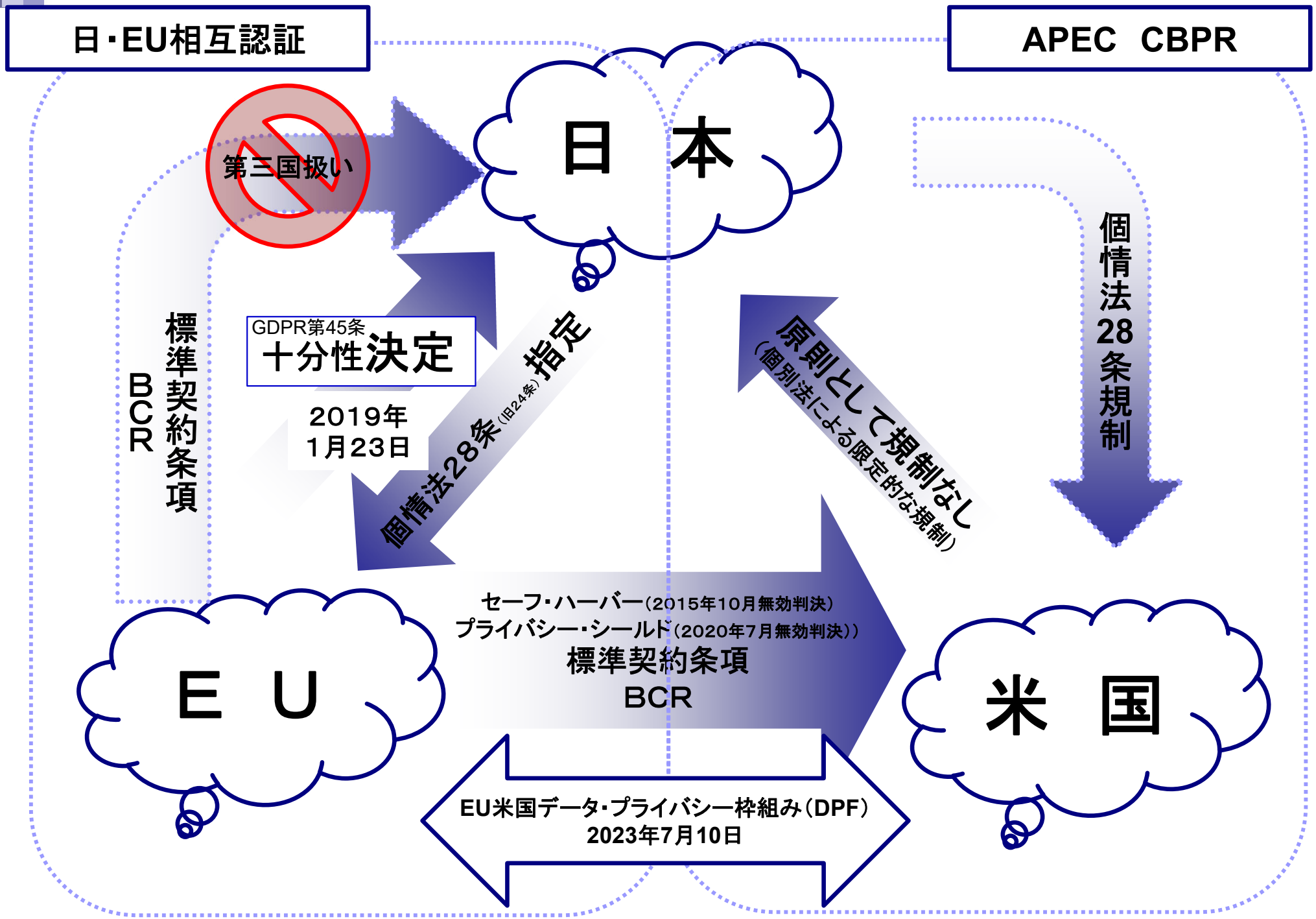
越境プライバシー・ルール(CBPR)

越境執行協力協定(CPEA)

個人情報の漏えい等が国境を越えて発生した場合などに対応可能な越境執行協力の枠組み

APEC

個人データの移転をめぐる国際的な制度



General Data Protection Regulation

- 正式名称、「一般データ保護規則（個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則）」
- 2016年5月24日に施行、2018年5月25日からEU加盟国への適用開始
- EUの個人情報保護制度は、個人の基本的権利として個人データを保護する特徴を有する制度
  - 1993年11月1日に欧州連合条約（マーストリヒト条約）が発効し欧州連合（EU）が発足
    - 欧州域内で国ごとに異なる法制度（規制）のレベルを一定にするための取り組み
    - 個人データ保護のための取り組みは、「個人データ保護95/46/EC指令」(1995)が端緒

European Union（欧州連合）一般データ保護規則（GDPR）の検討過程

1995年：「EU個人データ保護指令」の採択

1998年：同履行期限

2009年：EU個人データ保護指令の見直しに関する検討開始

2010年11月：見直しの基本的方向性に関する文書公表

2012年1月25日：「EU個人データ保護規則」案の公表

2012年～：理事会及び議会で審議

2013年10月21日欧州議会市民的自由・司法・内務委員会(LIBE)採択

個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則（**一般データ保護規則**）

規則の特徴

①EU域内における規制の単一化・簡素化
- 国内法制化の不要な「規則」に変更
- 一つの国からの承認を得れば、他国の当局からの承認は不要
- データ保護当局間の調査協力のメカニズム

②より強固な個人データ保護ルールの整備

事業者
- プライバシー・バイ・デザインの原則
- 個人データ漏えい時の通知義務

個　人
- 消去権（忘れてもらう権利）
- プロファイリングへの異議を申し立てる権利
- データ・ポータビリティの権利
- 同意の明示（オプト・イン原則）

③データ保護に関するグローバルな課題への対応

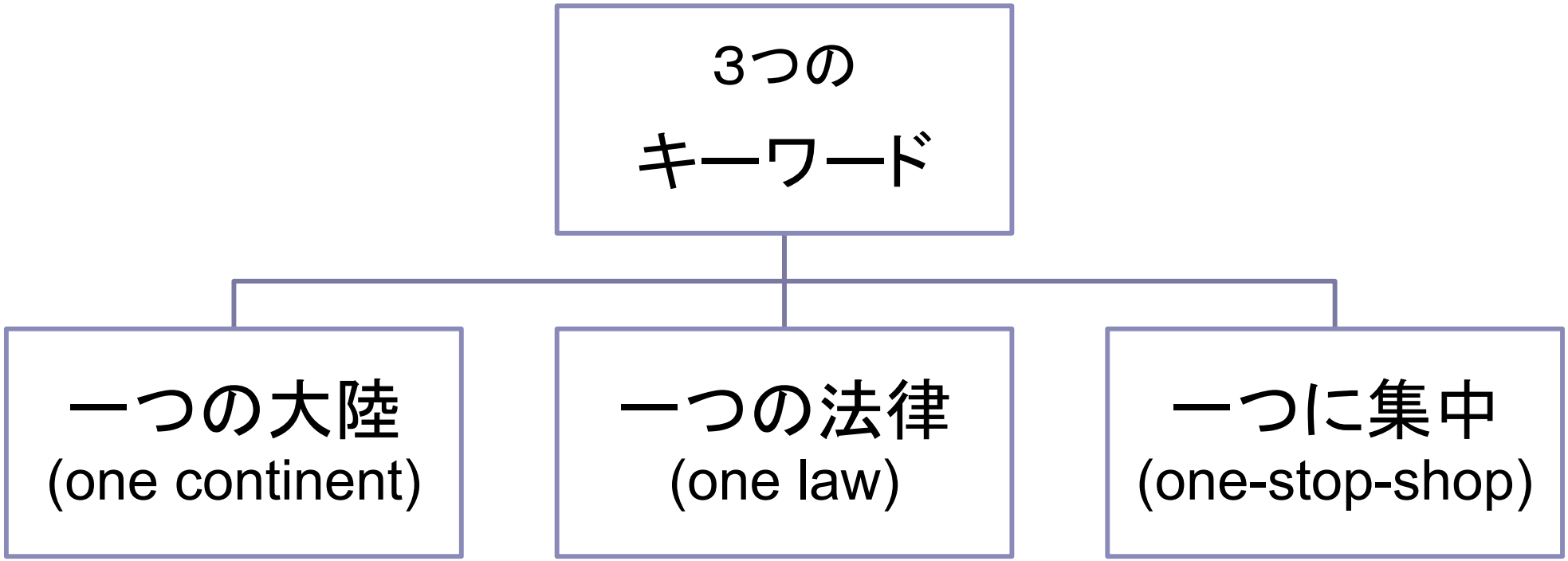
- **規則とは？（指令と規則の違い）**
  - **規則 (Regulation)、指令 (Directive)**
  - **決定 (Decision)、勧告 (Recommendation)**

□　指令とは、EU加盟国に対して示された提案を、国内法へ転換することを義務づける効力を有するもの
□　その効力は、EU域外の国に直接影響を及ぼすものではないが、各国の国内法の規定によっては間接的に域外の国にも影響が及ぶことがある
□　各国で法制度が異なることから、欧州域内における法制度（規制）の基準を統一化すことが必要なため、そのために必要な一定の枠組みや基準を明確に示し、各国がそれを履行する際の要求事項を定めたもの

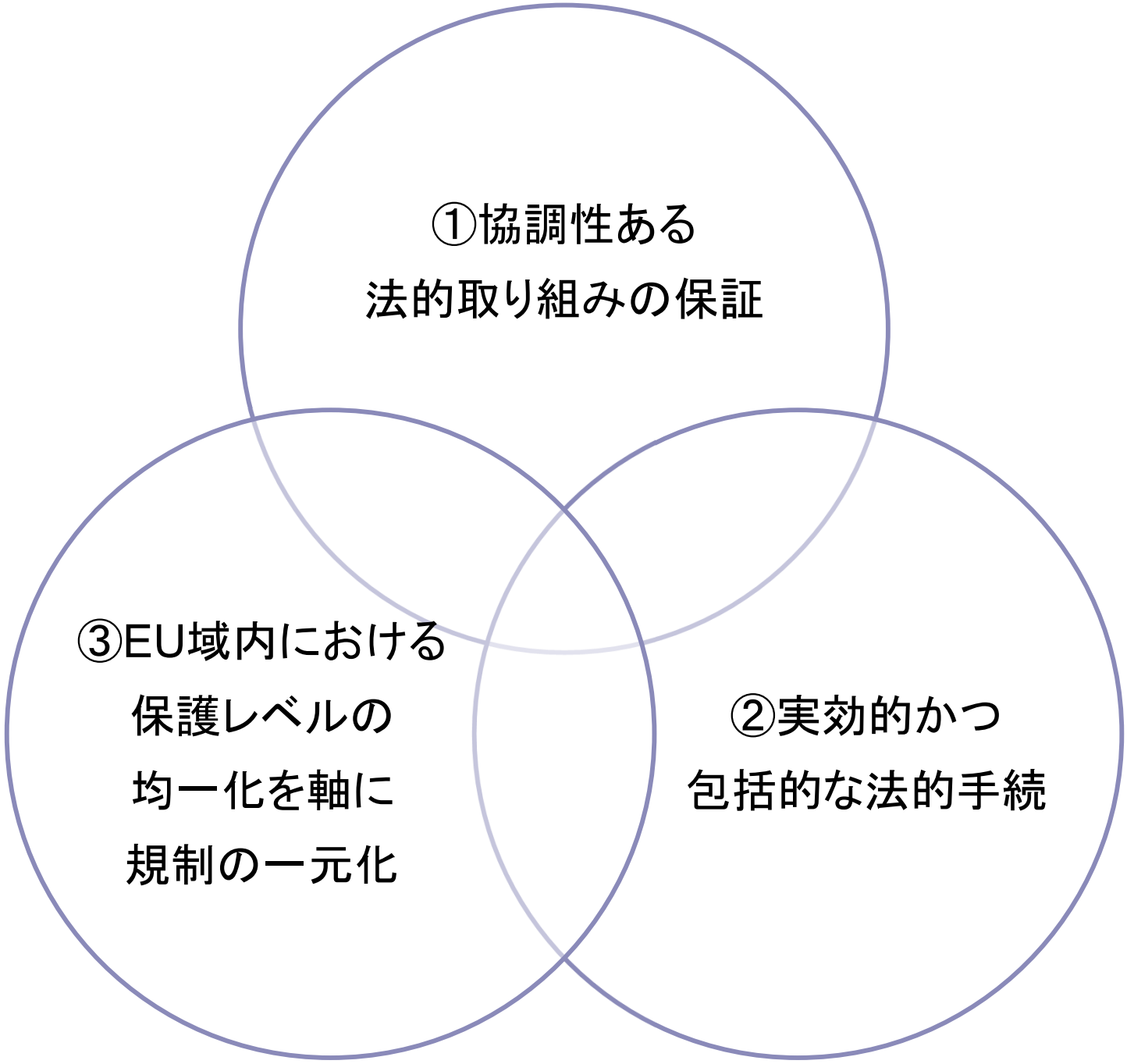
- 検討過程における議論
  - 2009年から検討を開始し、「忘れてもらう権利」や「プライバシー・バイ・デザイン」などの新たな取り組みの導入の必要性について議論
  - 2011年には、規則案が非公式に公表されて各国による水面下の検討・交渉が行われる
  - EU加盟各国から寄せられた意見（コメント）は、約3000件
  - 意見に基づき2013年3月までにとりまとめが行われる予定が、2013年5月29日まで延期（この段階で、ベルギー、チェコ、デンマーク、エストニア、ハンガリー、スウェーデン、スロベニア、イギリスの8カ国（EU加盟国は27カ国）が反対意見を表明）

一般データ保護規則　（ＧＤＰＲ）の特徴

（個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則）



GDPRの３つの目標


①協調性ある
法的取り組みの保証
③EU域内における
保護レベルの
均一化を軸に
規制の一元化
②実効的かつ
包括的な法的手続

GDPR制定の主たる目的（４つの目的）

①包括的な取り組みの充実

②個人の権利保障の強化

③域内市場の一層の活性化及びデータ保護ルールの執行の向上

④グローバル化への対応強化

GDPRの８つの主なポイント

①個人の基本的権利としてのプライバシー保護

②自由な意思に基づき、情報が与えられた上での明示的な同意（忘れられる権利、訂正・消去権、アクセス権、プロファイリング）

③いかなる状況や取扱者に対しても適用できる基本的な原則

④技術中立性を保った上での新技術へ対応（プライバシー・バイ・デザインやプライバシー・バイ・デフォルト）

⑤実効性ある個人情報保護のための対策（利用目的の制限、データ管理者の責任、データ保護影響評価、セキュリティ侵害通知、データ保護のためのマーク（シール）制度の整備）

⑥断片的な対応の防止や法的確実性の確保（EU加盟各国の監督機関への個別承認が不要、規則違反に対し最大2000万ユーロ又は全世界での年間総売上高の4%の制裁金）

⑦基本原則に基づく法執行

⑧域外適用や第三国への安全なデータ移転

GDPRが定める越境データ移転に関する制度

十分性の判定に基づく移転 （45条）

適切な安全性確保措置による移転 （46条）

特例 (49条）

欧州人工知能委員会

（EAIB：European Artificial Intelligence Board）の設置（56-59条）

- EAIBは、各国の監督機関の代表及び欧州データ保護監督官から構成され、欧州委員会が議長を務める
- この仕組みは、GDPRに基づいて設置されている欧州データ保護会議（EDPB：European Data Protection Board）と同じ位置づけにある組織
  - EDPBも、EU加盟国のデータ保護機関の代表及び欧州データ保護監察機関（EDPS：European Data Protection Supervisor）の代表によって構成される
- GDPRの統一的な適用を及びデータ保護機関間の効果的な協力を促進することが目的
- AI規制におけるEAIBもデータ保護におけるEDPBと同様の役割を担うことになる

GDPR（個人データ）

- 規則違反に対し最大2千万ユーロ又は全世界での年間総売上高の4%の制裁金

AI法（データガバナンス）

- 罰則規定（71-72条）は各加盟国が定めることになる
- 利用規制違反（5条）及びデータガバナンス要件違反
- 4千万ユーロ又は全世界の年間総売上の7%の制裁金
- データガバナンス以外のその他の違反の場合
- 2千万ユーロ又は全世界の年間総売上の4%が上限（GDPRと同じ）

安全、安心、信頼できる人工知能に関する大統領令
（2023年10月30日）

Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, October 30, 2023

米国の大統領令

安全、安心、信頼できる人工知能に関する大統領令（2023年10月30日）

• Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, October 30, 2023

① AI安全保障のための新たな基準

② アメリカ国民のプライバシー保護

③ 公平性の確保と権利保障

④ 消費者、患者、学生のための取り組み

⑤ 労働者の支援

⑥ イノベーションと競争の促進

⑦ 国外におけるアメリカのリーダーシップの推進

⑧ 政府による責任ある効果的なAI活用の確保

AI安全保障のための新たな基準

大統領令は、AIの進歩に伴うリスクに対処し、米国民を保護するために必要な措置を指示するもの

大統領令が最初に示している項目は、AIの能力向上に伴う米国民の安全とセキュリティに対する影響の増大に鑑み、当該大統領令により、AIシステムの潜在的リスクから米国民を保護するために必要と考えられる以下の措置

①AIシステムの安全性に関する開示義務

②AI安全基準の開発

③AIによる危険な生命科学試料の使用リスク対策

④AIによる詐欺と欺瞞からの保護

⑤高度なサイバーセキュリティプログラムの確立

⑥国家安全保障メモランダムの開発命令

⑦米国の国防及び情報機関によるAIの安全かつ倫理的・効果的な使用の保証

アメリカ国民のプライバシー保護

適切な保護措置がなければ、AIは米国民のプライバシーを危険に晒す可能性があるとの考えに基づき、AIによるプライバシーリスクに対処し、特に子供を含むすべての米国民のプライバシーを保護するために、超党派のデータプライバシー法案の可決を議会に求めると共に、大統領が関連する措置を指示

AIは個人データの抽出、識別、悪用を容易にするだけでなく、AIシステムの学習にデータを使用する企業によって、プライバシー保護のインセンティブも高まることを指摘し、米国民のプライバシーをAIがもたらすリスクを含めて適切に保護するために、以下の措置の実施を指示

①プライバシー保護技術の開発と使用の加速

②プライバシー保護研究と技術的対策の強化

③組織による情報の収集と利用に対する評価とプライバシー保護指針の強化

④プライバシー保護技術の有効性評価ガイドラインの開発

これらの措置は、最先端AI技術を利用したプライバシー保護技術の開発と使用を加速させ、プライバシー保護研究と技術的対策を強化することに焦点を当てている。また、連邦政府機関による個人を特定可能なデータを含む商用情報の取得と利用方法を評価し、AIリスクに対応するためのプライバシー保護指針を強化し、プライバシー保護関係技術の有効性を評価するためのガイドラインを開発することで、米国民のデータ保護を進めることを目指している。

公平性の確保と権利保障

AIの誤用が正義、医療、住宅分野での差別やバイアスを引き起こす可能性に対処するため、AI権利章典の草案を公表し、アルゴリズム差別に対抗する大統領令を発行

さらに、AIが公平性と公民権の保護に貢献するよう、大統領が追加の措置を指示

①差別の助長を抑止するためのAIアルゴリズムの使用ガイドラインの提供

②アルゴリズムによる差別への対応

③刑事司法システム全体の公正性の確保

消費者、患者、学生のための取り組み

AIが消費者に実質的な利益をもたらす可能性がある反面、AIは米国民を傷つけたり、誤解を招いたり、その他の形式で害を与えるリスクも高める

消費者を保護しつつ、AIが米国民の生活を向上させることを確実にするため、大統領は以下の措置を指示

①ヘルスケアにおけるAIの責任ある使用の促進と安価な救命薬の開発

②教育におけるAIの活用

AIが消費者に利益をもたらす一方で、米国人に対する危害を及ぼすリスクもあることに言及

消費者を保護するための措置として、ヘルスケアにおけるAIの責任ある使用の促進と安全プログラムの設立、教育分野でのAIの活用を支援するリソースの作成を実施することが目的

労働者の支援

AIは米国の雇用と職場に変化をもたらしており、生産性向上の可能性と同時に、職場における監視の増加、偏見、雇用転換といった危険もあることを指摘

これらのリスクを緩和するために労働者の団体交渉能力の支援と全員が利用可能な職業訓練と開発への投資を行うための措置を実施

AIによる労働者への影響を軽減し、利益を最大化するための原則とベストプラクティスの開発

労働者の過少報酬や不公平な職務評価を防ぐための指針として機能させることが目的

AIが労働市場に与える影響を分析するレポートの作成

雇用の変革に直面する労働者への連邦政府による支援を強化するために取り得る手段を研究することを強調

イノベーションと競争の促進

米国がAIの革新を既に先導していることと、米国で最初の資金調達を行ったAIスタートアップの数が、G7各国を合わせた数よりも多いことを指摘

大統領令を通じて、イノベーションと競争を継続してリードするための措置が講じられることを強調

①国策としてのAI研究の促進

②公平でオープンな競争的なAIエコシステムの推進

③高度な技能を有する移民と非移民の能力の拡大

米国政府によるAI研究リソースの試験運用を通じて全米でのAI研究を促進

重要な分野での研究のための補助金の拡大

小規模開発者や起業家への支援によって公平で競争的なAIエコシステムを推進

高度な技能を持つ移民や非移民が米国で学び、働くためのビザ基準を合理化すること

国外におけるアメリカのリーダーシップの推進

AIに関連する課題と機会が世界的なものであることから、バイデン・ハリス政権が世界中で安全で信頼性のあるAIの展開と使用を支援するために他国との協力を続けることを強調

その達成のために大統領が取るべき措置を指示

①AIに関する二国間、多国間、マルチステークホルダーの関与の拡大

②国際パートナーと標準化機関における重要なAI標準の開発と実装の加速

③安全かつ責務を果たし、権利を尊重したAIの開発と海外展開の推進

AIに関する国際協力を拡大し、AIの利点を活用しリスクを管理するための国際的枠組みの確立を国務省が主導

国際パートナーと協力してAI標準の開発と実装を加速

持続可能な開発や重要インフラの保護などのグローバルな課題に対処するために、海外でのAIの安全で責任ある開発と展開を促進すること

政府による責任ある効果的なAI活用の確保

AIが規制、統治、福祉の分配を拡大し、コスト削減と政府システムのセキュリティ強化に貢献する一方で、差別や不安全な決定などのリスクをもたらす可能性があることを指摘

これらのリスクを回避し、政府によるAIの責任ある展開と連邦AIインフラの近代化を進めるための措置を指示

①政府機関によるAI使用のためのガイダンスの発行

②AI製品とサービスの迅速で効率的な調達支援

③AI専門家の迅速な採用の加速

AIの利用に関する明確な基準を含むガイダンスの発行

AI製品とサービスの迅速かつ効率的な調達支援及びAI専門家の迅速な採用を加速するための政府全体の取り組み

AIの責任ある使用と展開を支援し、政府の効率性を高めることを目指すもの

ＡＩ規正論

新保史生「AI規正論」情報通信政策研究第7巻第1号

新AI規制試案の構成

①AIシステムの研究開発から利用、販売及びサービスの提供にあたって必要な「ルール（規制）」を定めること

②その遵守について自主的な取り組みを尊重

③販売やサービス提供において「事実上の強制規格」として機能する「ルール（整合規格・技術標準・要求事項）」を導入

④それを計画、実施、評価及び改善するためのマネジメントシステム規格を制定

⑤これらの仕組みを規律するための根拠を法定

⑥「AI規正委員会（仮称）」を設置

⑦「日本版AIシステム適合性評価制度」を中核とするAI規制構想

AI規制構想の目的

専ら自主的な規律に期待するソフトローの検討を試行錯誤し続ける施策からの転換

反対意見が根強い規制（実質的な禁止事項の法定等）の導入に伴うハードローへの抵抗感の払拭

これまで検討がなされてきた原則・指針やガイドライン等をめぐる議論からは発想を転換した取り組みを模索することが目的

当該目的を達成するため

規範の遵守を自主性に委ねハードローによる規制を行わない法規制回避論からの脱却

国際的な動向を踏まえたAI規制の「最適化(optimisation)」

AIの研究開発・利用における将来的なAI規制政策に資する方策

新たなAI規制の制度設計試案

1.1.　AI規正論とは

- AI時代に向けて必要なAIの安全・安心な利用のための管理及び規制の方策として、
  新たな「AI規正論」を展開することが目的

今後、世の中で広く用いられ日常生活における
システムやサービスを制覇することになるAI

↓

その管理やガバナンス等の規制の主導権を握ること

↓

今後のAI時代におけるAI政策の覇権を獲得

日常的に利用されるAIに求められるのは 安全と信頼性が確保され安心して使うことができること

EU

EUは域内のAI規制の整合化を図るための整合規則をAI法案を提案

同法に基づいて定められる整合規格に準拠した高リスクAIに製品安全規制同様のCEマークを付す制度の構築を目指している（CEマーキング）

輸入から販売に至るまでのEU市場への上市規制を設ける制度の整備を進めている

日本

日本にも電気や電子製品の様々な整合規格やJIS規格・ISO規格・IEC規格との整合標準が存在

企業の法令遵守における取り組みと整合規格の位置づけ

マネジメントシステム規格の導入実績も豊富

- 品質、環境、労働安全衛生などのISO規格
- JIS Q 15001を用いたプライバシーマーク
- JIS Q 27001（ISO/IEC 27001）を用いたISMS（情報セキュリティマネジメントシステム）等

EUがAI法の制定によりAI統治(governance)のための制度として構築を目指している安全規制の枠組み

事実上の強制規格（法律に基づく義務）

日本版のAI整合規格の策定と整合性確認基準及び手続に基づく適合性評価制度

当該制度を整備し展開することが可能か検討を試みる

新保ビジョンを実際に達成する上での選択肢

(a) EUが目指している整合規格の整備に係る整合標準策定に向けた取り組みに歩調を合わせること

- EUの制度との相互運用性を確保する国内規格をわが国おいても導入する方法（ISO規格とJIS規格の関係と考えるとよい）

(b)我が国独自の技術基準として日本版のAI整合規格を策定すること

- AIシステムの製造・開発、輸入、販売又はサービス提供を行う事業者に当該規格に基づく技術基準適合義務を課すこと
- 適合証明の表示を義務づけ（PSEマークを想定）
- 適合証明の取得に必要なマネジメントシステム規格を新たに設けること

後者の(b)の選択肢で進めたい

- いわゆる「ブリュッセル効果」への闘いを挑むもの
- 我が国の政策立案の中心地である霞ヶ関から「カスミガセキ効果（仮称）」を今後AI関連政策分野で発揮できるかどうかは不明
- 既に整合規格の根拠となるISO規格の検討も進んでいることから現実は厳しい

新保ビジョンの方針

新保ビジョンにより示す提案は我が国におけるAI規制をめぐる議論や検討過程においてこれまで俎上に載ったことがないもの

最初から諦めて(a) EUへの追従を図るのではなく、(b)AI整合規格をわが国独自の基準として制定する施策を目指す

①産業標準化法に基づく新たな「AIマネジメントシステム規格（仮称）」を制定

②電気用品安全法の改正によりPSEマークをAIシステム適合証明に活用する方法又は日本版AI法の制定によるAI整合規格の根拠となる法整備を実施

「日本版のAIシステム適合性評価制度」の構築に向けた提案

1.3.　着想の背景

EUがAI法案（AI整合規則提案）においてAI管理のための制度として構築を目指している製品安全規制に基づく法的枠組みである適合性評価制度

わが国においても導入が可能ではないかという問題意識に基づくもの

適合性評価制度を新興技術規制において用いる着想は、ムーンショット研究開発プロジェクト目標1研究開発プロジェクト「アバターを安全かつ信頼して利用できる社会の実現」の提案に依拠するもの

サイバネティック・アバター（CA）を安全かつ信頼して利用できるCA基盤の構築

CA操作者の認証技術

CA認証技術

CA公証

遠隔操作者が法律に基づいてCAを公的に使用できることを証明・認証

自律型ロボットを将来的に社会で受け入れるために共通の認識として必要な原則の策定が必要との着想

- 2015年10月11日に開催した「ロボット法学会設立準備研究会」において「ロボット法　新8原則（新保試案）」を公表
- あくまで将来的なロボット共生社会に向けて求められる基本となる原則を考案したにすぎない

AIブームとともに原則や指針策定の機運が社会的に高まる

- AI原則を単なる非拘束的な原則として活用を求める段階から、基本法の整備による法令事項としての組み込みや法定公表事項としての位置づけに移行することを検討してよいのではないかとの考えを公表
- 非拘束的な原則の有効性に疑問を呈しつつも、具体的な規制の在り方について方向性を見出すことができない状況が続いていた
- 規制の方向性を明確に表明することができる段階に至ったと考えている

ロボット・ロー・バイ・デザイン（仮称）（Robot Law by Design）

ロボット法の理念･概念

アイザック･アシモフのSF小説（I, Robot, Isaac Asimov）
「**ロボット工学の三原則**」(Three Laws of Robotics)

第1条
ロボットは人間に危害を加えてはならない。また、その危険を看過することによって、人間に危害を及ぼしてはならない。

第2条
ロボットは人間にあたえられた命令に服従しなければならない。ただし、あたえられた命令が、第1条に反する場合は、この限りでない。

第3条
ロボットは、前掲第1条および第2条に反するおそれのないかぎり、自己をまもらなければならない。

——『ロボット工学ハンドブック』第56版、西暦2058年

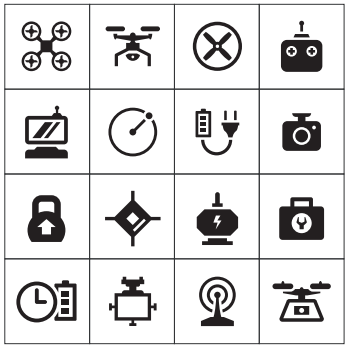
ロボット法原則
(The Robot Law Principles)

- ①人間第一の原則 Humanity First
- ②命令服従の原則 Obedience to Order
- ③秘密保持の原則 Secrecy
- ④利用制限の原則 Use Limitation
- ⑤安全保護の原則 Security Safeguards
- ⑥公開･透明性の原則 Openness & Transparency
- ⑦個人参加の原則 Individual Participation
- ⑧責任の原則 Accountability

半世紀以上前にアシモフが生み出した「思想」であって、「法」や「規範」ではない。

ロボット法　新8原則（新保試案）
New Eight Principles of Laws of Robotics
(Tentative Proposal by Dr.Shimpo)

OECDプライバシー8原則を参考に
シンギュラリティ（技術的特異点）も見据えて



新保史生「何故に『ロボット法』なのか」ロボット法学会設立準備研究会(2015年10月11日）報告資料(2015)

2.1. AI・ロボット政策の端緒

ロボットの利用をめぐる基本政策

- 「ロボット新戦略（Japan's Robot Strategy—ビジョン・戦略・アクションプラン）」
  2015年2月10日（日本経済再生本部決定）
  - 本戦略はAIブーム前の戦略であるためAIに関する言及はない
  - 従来の産業用ロボットにとどまらず、ロボットの概念を広く柔軟に捉えるもの
  - ロボット革命の実現に向けた戦略の三本柱を提示

①世界のロボットイノベーション拠点－ロボット創出力の抜本的強化

②世界一のロボット利活用社会

③世界をリードするロボット新時代への戦略

重点的に取り組むべき技術課題としてのAI

- 総合科学技術・イノベーション会議「第５期科学技術基本計画」2016年1月22日閣議決定

基本計画の内容

- Society5.0実現には人工知能技術が重要な役割を担うこと
- 科学技術イノベーションと社会との関係深化の重要性
  - そのために倫理的・法制度的・社会的取組を行うべき
- 「超スマート社会」の実現に向けた共通基盤技術や人材の強化
- AI等の重点的に取り組むべき技術課題等を明確にし、関係府省の連携をはかり戦略的に研究開発を推進することを明示

その後、AI・ロボット関係の様々な施策が立案されることとなった

2016年時点の第５期科学技術基本計画前後のＡＩ・ロボット関係政策

【各府省による取り組み状況】

- 内閣府
  - 人工知能と人間社会に関する懇談会
- 内閣官房
  - 自動運転に係る制度整備大綱サブワーキングチーム
  - 知的財産推進計画2017（データ・人工知能（AI）の利活用促進による産業競争力強化に向けた知財制度の構築）
- 総務省
  - AIネットワーク社会推進会議（AI開発ガイドライン案）
  - 情報通信審議会陸上無線通信委員会（ITS Connect）
- 経済産業省
  - ロボット産業をめぐる政策全般
  - 自動走行ビジネス検討会（国土交通省とともに）
- 警察庁
  - 自動走行の制度的課題等に関する調査検討委員会（自動走行システムに関する公道実証実験のためのガイドライン2016）
- 国土交通省
  - 航空法の一部改正法（無人航空機の飛行ルール）
  - 次世代社会インフラ用ロボット開発・導入検討会
  - オートパイロットシステムに関する検討会
- 人工知能技術戦略会議
  - 日本経済再生本部決定（2016年4月12日）により設置（「未来投資に向けた官民対話」人工知能の研究開発目標）

  と産業化のロードマップを策定
- 文部科学省
  - AIPプロジェクト（人工知能／ビッグデータ／IoT／サイバーセキュリティ統合プロジェクト）

検討の成果・実証

自動走行

・自動走行システムに関する公道実証実験のためのガイドライン2016

航空法の改正（2015年12月10日施行）

（1）無人航空機の飛行にあたり許可を必要とする空域
（2）無人航空機の飛行の方法
（3）事故や災害時の公共機関等による捜索・救助等の場合の適用除外

● 無人航空機一般に対する規制
・飛行禁止空域の設定
・夜間飛行禁止
・目視による常時監視
　重量が200g未満の無人航空機は規制対象外

人工知能

・AI研究開発8原則(G7情報通信相会合：2016年4月)
・国際的な議論のためのAI開発ガイドライン案（2017年7月28日）

構造改革特区

つくばモビリティロボット実験特区
羽田空港ロボット実験特区
豊田市立ち乗り型パーソナルモビリティ実験特区
けいはんな学研都市知的特区
福岡市ロボット開発・実証実験特区
さがみロボット産業特区
鳥取発次世代社会モデル創造特区

国家戦略特区

完全自動走行に向けた国家戦略特区プロジェクト（神奈川県、仙台市、名古屋市）

AIに関する政策立案を検討する主な会議

(1)イノベーション政策強化推進のための有識者会議
「AI戦略」（AI戦略実行会議）

(2)AIステアリングコミティー

(3)新AI戦略検討会議

(4)AI戦略会議（イノベーション政策強化推進のための有識者会議）2023年5月11日に発足

(5)AI戦略チーム（関係省庁連携）

2.4. 法規制回避論の功罪

今後のAI規制のあり方を考えるにあたっては、我が国のAI政策における**法規制回避論の功罪**を省察すべきである。

法規制回避論の効用

- EUや米国をはじめとする諸外国におけるAI規制の取り組みに対し、我が国同様に自主的な取り組みを尊重する米国の取り組みと同調することによるメリット

法規制回避論の弊害

- ブリュッセル効果を発揮しつつあるEUの取り組みを傍観することにより、AI規制への乗り遅れが顕著（日本国内において制度の内容は詳細に調査し精査している）
- 米国における自主的な取り組みは大統領令や法規制に基づく強制的な取り組みへ移行（米国が規制に舵を切っていることについて日本国内における認識の遅れ）

→ **日本だけが法規制によらない自主規制に依拠し続けることの妥当性に疑問を持つべき段階に来ている**

日本の法規制回避論の問題は、原則やガイドラインの策定及び公表段階において意識はされてきたものの、政府における取り組みとしては法的拘束力を前面に打ち出すことが難しいがゆえに、結果的にその妥協案としての折衷論によるしかなかったことはやむを得なかったといえよう

「肯定論」又は「否定論」の両極と「折衷論」

- 規制の必要性を認識
- 法規制としてのいわゆるハードローによる規制ではない
- 事業者や民間団体等による純粋な自主的な規律でもない
- 政府の検討会が定めたガイドライン等による取り組みを推進する「折衷論」

OECDで「AIに関する理事会勧告」(2019年5月22日）が採択された後は、我が国からの提案も踏まえて国際機関において原則策定にまで至った達成感とAIブームの終息が重なり、次のステップに必要な本来の「規制論」に向けた検討が停滞

2.5. AI規制に向けた研究や検討で後塵を拝しつつある要因

我が国におけるAI規制に関する議論の遅れを指摘する意見が見受けられるようになりつつあるものの、**国内における検討や議論は諸外国に先駆けて精緻な取り組みがなされてきた**ことを再認識すべき

将来的なAIやロボットの研究開発及び利用における規制に向けて、統一的かつイノベーションの促進に資するために必要な共通認識として、「原則」策定の必要性を提唱し、国際的な議論を先行してきたことは明らか

にもかかわらず、AIの研究開発だけでなく、**AI「規制」に向けた研究や検討においても周回遅れになりつつあるのはなぜか**

国内外のガイドラインの紹介、各国の法制度の詳細な調査や国際動向の把握、AIに関する法的諸課題の検討などに関する論考は数多く公表されているにもかかわらず、日本のAI規制の方向性やそのための戦略を具体的に示している論考が見当たらない

① 規制・禁止同視論

- 「規制」を「禁止」と同義に議論
- イノベーションの促進への仮想・架空の懸念（実際には阻害されるイノベーションそのものが存在していない）
- 緩和する規制が存在しないにもかかわらず規制緩和を主張する見解

② 規制の不存在の反射としての躊躇

- 規制されていないので「実施できない」という不合理な理屈（本来は規制されていないので実施して何ら問題ないはず）
- 新たな技術開発やサービスの提供にあたっての「規制の不存在」による事業展開や利用への躊躇

③ 責任転嫁論

- 技術開発や利用の遅れを法整備の不備（規制の不存在としての）を理由に言い訳をしているとしか思えない指摘

④ 法と倫理の混同

- 法と倫理を区別せずAIをめぐる法的課題を一緒くたに倫理的課題にしてしまい、情報倫理で情報法に関する課題をすべて論じようとしていた時代を彷彿させるもの

⑤ 取り越し苦労的な懸念先行論

- まずは懸念やリスクに関する問題を先行して議論し、振り返ってみるといずれの懸念も単なる杞憂と帰してしまっている指摘
- リスク「認識」ではなく単なるリスク「例示」による自己満足的な議論により本来のリスク認識が達成できていない
- 抽象的で中途半端なディストピア的議論。AIについての抽象的畏怖に基づく浅薄なリスク論
- AIによる人類駆逐懸念やラッダイト運動的排斥主張

⑥ クリックベイト的論文

- AIによる問題に関する議論と謳っていながら、その内実は単なる情報システムの高度化への懸念論でしかない論考（DX推進を謳いながら実際には基幹系刷新にすぎず現行システムの再構成を売り込んでいるようなもの）
- タイトルにAIと冠しているためAIに関する論考かと思いきや無関係の内容で、まるでクリックベイトのような欺瞞的なものや、AとIという文字列から成る空想の産物に関する内容
- 電子法人格(electronic person)に関する議論がいつの間にかAI基本的人権論に飛躍しているもの

⑦ 検討事項の断片的抽出・認識・評価による弊害

- 単に思いついた課題から議論をはじめる断片的な検討事項の抽出・認識を行う指摘の弊害
- 新たな技術の利用に伴い議論される法的課題として、まずは、知的財産やプライバシー関係の問題からとりあえず議論をはじめる傾向 → 真に検討すべき論点の欠落が生じ中途半端な楽観論により議論が収束してしまうこと
- なぜその原則が必要なのか理由を説明できないにもかかわらず、単に流行に遅れんとせんがために、適当にピックアップした原則を提示しているだけの指針
- AI・ロボットに関する法的課題を産業用ロボットの延長でしか考えていない場合

AI規制をめぐる研究や議論の仕方における問題を意識し

建設的なAI規制に向けた議論を進めることが必要ではないか

AI法案の欧州議会採択案第40条（新設規定）

- 「欧州標準化規則」10条に基づく標準化要請に関する規定の追加

- 欧州委員会はAI法案が定める適合性評価制度の実施に必要な整合規格の策定に向けて必要な要求事項の標準化に向けた取り組みに着手

- 本要請案はAI法案の制定後に発効するため、標準化要請が具体化するのはAI法制定後

4.1. AI整合規格の標準化要請案（草案）の名称、根拠及び目的

安全で信頼できるAIを支援するための欧州標準化機関への標準化要請案（草案）

根拠：AI整合規則提案（AI法案）

- 高リスクAIの適合性評価制度を構築するため、欧州標準化規則第12条に基づいて10分野の整合規格を策定するために必要な標準化要求を決定することが目的
- 安全で信頼できる人工知能システムを支援するために、欧州規格又は欧州標準化規格類の策定を要請する意図
- 「欧州標準化のための2022年次統合作業計画」に関する欧州委員会通知C(2022) 546の附属文書内の「標準化戦略に関して欧州委員会が設定した標準化緊急課題」と題する表63番目の項目記載事項に基づくもの

整合規格を策定する実施機関

- 欧州標準化委員会（CEN）及び欧州電気標準化委員会（CENELEC）
- 欧州の標準化機関の一つである欧州電気通信標準化機構（ETSI）については、セキュリティなど特定の事項に関して既に本文書通知前の段階において作業に着手しているとともに、特定の専門知識を有していることから、作業計画の作成中にCENおよびCENELECがETSIと協議し、これらの事項に関してETSIの貢献を認めるための方法を確認することが適切であるとしている

草案において示されている国際標準化の効果

- 信頼できるAI（trustowrthy AI）という共通のビジョンを世界中に定着させるのに役立つこと
- AIを搭載した製品やサービスに関連して起こりうる技術的障壁を取り除き貿易を促進すること
- 規則(EU) No 1025/2012（欧州標準化規則）の第10条1項に基づく要求事項を定め、本要請に基づく欧州規格及び欧州標準化規格類( )の起草にあたっての確認項目として以下の要求事項を定めることを目的としている

4. 2.　国際標準化の効果

草案において示されている国際標準化の効果

- 信頼できるAI（trustowrthy AI）という共通のビジョンを世界中に定着させるのに役立つこと
- AIを搭載した製品やサービスに関連して起こりうる技術的障壁を取り除き貿易を促進すること

規則(EU) No 1025/2012（欧州標準化規則）の第10条1項に基づく要求事項

①AI分野における欧州委員会の政策目標を考慮すること

②EUのデジタル主権を強化すること

③AIへの投資と技術革新を促進し、EU市場の競争力と成長を促進すること

④EUの価値と利益に合致するAI分野の標準化に関する国際協力を強化すること

政策目標に含まれる事項

- (a)EU内で上市又は使用されるAIシステムが安全であること
- (b)EU基本権条約が定める基本的権利を遵守し、EUの価値を十分に尊重した使用がなされること

4. 3.　標準化要請

標準化要請案（草案）第1条

- **欧州標準化委員会（CEN）**及び**欧州電気標準化委員会（CENELEC）**に対し、安全で信頼できるAIを支援するため、附属書Iの表1に記載された新規の**欧州規格又は欧州標準化規格類**を起草するよう要請する。
- 第1項に基づいて策定される欧州規格又は欧州標準化規格類は、附属書IIが規定する要求事項を満たさなければならない。

標準化要請案（草案）第2条1項

- CEN及びCENELECは，附属書Iが記載するすべての規格、担当TB及び要請された標準化活動の実施期限を示す業務計画を作成しなければならない。
- EUの中小企業及び市民社会組織の効果的な参加を確保し、基本的権利の分野で関連する専門知識を収集するために実施される行動を含む。附属文書第1項の作業計画の作成にあたっては、CEN 及び CENELEC は、欧州電気通信標準化機構（ETSI）と協議し，以下の要素に対する ETSI の貢献を確保するための方法を検討し合意するものとする。

【作業計画で定める実施事項】

- (a) 附属書Iの表1の8に基づく**欧州規格及び欧州標準化規格類の策定**
- (b) 附属書 I の表 1 において列挙されている欧州規格及び欧州標準化規格類のうち、同表の 8 に言及されているもの以外のものについては、**セキュリティ評価及び統合を実施すること**
- (c) 附属書 II の第 1 章に基づく**ETSIが実施可能な手続及び仕様の策定及び精緻化**

草案第2条2項 （ETSIが実施すべき事項について）

- ETSIが実施可能な貢献の方法及びその範囲に関する記述は、第1項において示されている作業計画の下に記載されなければならない。
- CEN、CENELEC及びETSIが、前項が定めるETSIが実施可能な貢献について合意できない場合、作業計画にはその理由を記載しなければならない。
- ETSIが実施可能な貢献は、第1条に基づく要請の実行に対するCEN及びCENELECの責任並びに附属書IIIに規定された欧州規格および欧州標準化規格類に対する要求事項を損なうものであってはならない。

草案第2条3項 （CEN 及び CENELECが実施すべき事項について）

- CEN及びCENELECは，第1条に基づく標準化要請が欧州委員会に採択されてから4 か月後以内に作業計画を欧州委員会に提出しなければならない。CEN 及びCENELEC は、共同作業計画の修正を欧州委員会に通知しなければならない。

草案第2条4項

- CEN及びCENELECは、欧州委員会に対し、全体的なプロジェクト計画へのアクセスを提供しなければならない。

草案第3条 （標準化の実施期限）

- ①第1条の標準化要請の実施について、第2条の作業計画の実施の進捗状況を6ヶ月ごとに欧州委員会に報告すること
- ②第1条の標準化要請が採択されてから10ヶ月以内に、最初の共同半期報告書を欧州委員会に提出すること
- ③2025年1月31日までに欧州委員会に共同最終報告書を提出すること
- ④附属書Ⅰに定める期限及び要請の実施に関する重大な懸念事項があれば、すみやかに欧州委員会に報告すること
- ⑤第1項乃至第3項に基づく報告書は、EUの中小企業、市民社会組織の適切な関与及び関係者からの情報収集について、その計画及び実施内容に関する証跡を含めなければならない

10項目の要求事項

① AIシステムのリスク管理システム (Risk management system for AI systems)

② データとデータガバナンス (Data and data governance)

③ ログ機能による記録管理 (Record keeping through logging capabilities)

④ ユーザへの透明性と情報提供 (Transparency and information to the users)

⑤ 人間による監督 (Human oversight)

⑥ AIシステムの精度仕様 (Accuracy specifications for AI systems)

⑦ AIシステムの堅牢性に関する仕様 (Robustness specifications for AI systems)

⑧ AIシステムのサイバーセキュリティ仕様 (Cybersecurity specifications for AI systems)

⑨ 市販後モニタリング・プロセスを含む、AIシステム・プロバイダーのための品質マネジメントシステム (Quality management system for providers of

⑩ AIシステムの適合性評価 (Conformity assessment for AI systems)

AI関係の国際標準

- ISO/IEC JTC 1/SC 42において検討
- 標準化の動向
  （2023年10月時点で20件が公表済み、32件が検討中）

1. ISO/IEC TS 4213:2022 (**Assessment of machine learning classification performance**)
2. ISO/IEC 8183:2023 (**Data life cycle framework**)
3. ISO/IEC 20546:2019 (**Big data — Overview and vocabulary**)
4. ISO/IEC TR 20547-1:2020 (Big data reference architecture — Part 1: **Framework and application process**)
5. ISO/IEC TR 20547-2:2018 (Big data reference architecture — Part 2: **Use cases and derived requirements**)
6. ISO/IEC 20547-3:2020 (Big data reference architecture — Part 3: **Reference architecture**)
7. ISO/IEC TR 20547-5:2018 (Big data reference architecture — Part 5: **Standards roadmap**)
8. ISO/IEC 22989:2022 (**Artificial intelligence concepts and terminology**)
9. ISO/IEC 23053:2022 (**Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)**)
10. ISO/IEC 23894:2023 (**Guidance on risk management**)
11. ISO/IEC TR 24027:2021 (**Bias in AI systems and AI aided decision making**)
12. ISO/IEC TR 24028:2020 (**Overview of trustworthiness in artificial intelligence**)
13. ISO/IEC TR 24029-1:2021 (**Assessment of the robustness of neural networks — Part 1: Overview**)
14. ISO/IEC 24029-2:2023 (**— Part 2: Methodology for the use of formal methods**)
15. ISO/IEC TR 24030:2021 (Artificial intelligence (AI) — **Use cases**)
16. ISO/IEC TR 24368:2022 (**Overview of ethical and societal concerns**)
17. ISO/IEC TR 24372:2021 (Artificial intelligence (AI) — **Overview of computational approaches for AI systems**)
18. ISO/IEC 24668:2022 (**Process management framework for big data analytics**)
19. ISO/IEC 25059:2023 (Software engineering — **Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems**)
20. ISO/IEC 38507:2022 (Governance of IT — **Governance implications of the use of artificial intelligence by organizations**).

検討中の国際標準

- 1. ISO/IEC DIS 5259-1 (Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples)
- 2. ISO/IEC DIS 5259-2 (Data quality for analytics and machine learning (ML) — Part 2: Data quality measures)
- 3. ISO/IEC DIS 5259-3 (Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines)
- 4. ISO/IEC DIS 5259-4 (Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework)
- 5. ISO/IEC CD 5259-5 (Data quality for analytics and machine learning (ML) — Part 5: Data quality governance)
- 6. ISO/IEC CD TR 5259-6 (Data quality for analytics and machine learning (ML) — Part 6: Visualization framework for data quality)
- 7. ISO/IEC FDIS 5338 (Information technology — AI system life cycle processes)
- 8. ISO/IEC FDIS 5339 (Information technology — Guidance for AI applications)
- 9. ISO/IEC DIS 5392 (Information technology — Reference architecture of knowledge engineering)
- 10. ISO/IEC DTR 5469 (Functional safety and AI systems)
- 11. ISO/IEC CD TS 6254 (Information technology — Objectives and approaches for explainability of ML models and AI systems)
- 12. ISO/IEC CD TS 8200 (Information technology — Controllability of automated artificial intelligence systems)
- 13. ISO/IEC DTS 12791 (Information technology — Treatment of unwanted bias in classification and regression machine learning tasks)
- 14. ISO/IEC CD 12792 (Information technology — Transparency taxonomy of AI systems)
- 15. ISO/IEC AWI TS 17847 (Information technology — Verification and validation analysis of AI systems)
- 16. ISO/IEC CD TR 17903 (Information technology — Overview of machine learning computing devices)

検討中の国際標準

- 16. ISO/IEC CD TR 17903 (Information technology — Overview of machine learning computing devices)
- 17. ISO/IEC AWI TR 18988 (Application of AI technologies in health informatics)
- 18. ISO/IEC AWI TR 20226 (Information technology — Environmental sustainability aspects of AI systems)
- 19. ISO/IEC AWI TR 21221 (Information technology – Artificial intelligence – Beneficial AI systems)
- 20. ISO/IEC AWI TS 22440 (Functional safety and AI systems — Requirements)
- 21. ISO/IEC AWI TS 22443 (Information technology — Guidance on addressing societal concerns and ethical considerations)
- 22. ISO/IEC AWI 24029-3 (Assessment of the robustness of neural networks — Part 3: Methodology for the use of statistical methods)
- 23. ISO/IEC CD TR 24030 (Information technology — Use cases)
- 24. ISO/IEC DTS 25058 (Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of artificial intelligence (AI) systems)
- 25. ISO/IEC AWI TS 29119-11 (Software and systems engineering — Software testing — Part 11: Testing of AI systems)
- 26. ISO/IEC FDIS 42001 (Information technology — Management system)
- 27. ISO/IEC CD 42005 (Information technology — AI system impact assessment)
- 28. ISO/IEC DIS 42006 (Information technology — Requirements for bodies providing audit and certification of artificial intelligence management systems)
- 29. ISO/IEC AWI 42102 (Information technology — Taxonomy of AI system methods and capabilities)
- 30. ISO/IEC AWI TR 42103 (Information technology — Overview of synthetic data in the context of AI systems)
- 31. ISO/IEC AWI 42105 (Information technology — Guidance for human oversight of AI systems)
- 32. ISO/IEC AWI TR 42106 (Information technology — Overview of differentiated benchmarking of AI system quality characteristics).

6.1. DFFT（信頼性のある自由なデータ流通）との制度的な整合性の確保

- AIシステム適合性評価制度を構築した場合、AIシステムの輸入、販売又はサービス提供を行う事業者に対する直接的な規制となる
- 非関税障壁にあたるとの指摘を受ける可能性についても考慮が必要
- DFFT（信頼性のある自由なデータ流通）との制度的な整合性の確保が重要

DFFT（データ・フリー・フロー・ウィズ・トラスト）

IT総合戦略本部「デジタル時代の新たなIT政策大綱」（2019年6月7日決定）

- 「プライバシーやセキュリティ・知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指す」というコンセプトを掲げ
- 「DFFT（信頼性のある自由なデータ流通）のコンセプトに基づく「国際データ流通網」を広げていくことを目的として、より多くの国との間で、デジタル貿易ルールの形成等を促進することが求められる」とし
- 当該目的を達するため、「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画」（2019年6月14日閣議決定）が策定された

G20茨城つくば貿易・デジタル経済大臣会合（令和元年６月８日及び９日）

- DFFTはG20全体で合意され、信頼につながる各国の法的枠組みは相互に接続可能なものであるべきことが確認された
- その後、2019 年のG20大阪首脳宣言、2021年の「DFFTへの協力に向けたG7ロードマップ」、2022 年の「DFFT促進のためのG7 アクションプラン」と着実に取り組みがなされている

情報の自由な流通と保護を基調とするデータ保護制度の整備

OECDプライバシーガイドライン（1980年制定2023年改正）

- 1980年にOECDプライバシーガイドラインが制定され、OECD加盟国相互における個人データの自由な流通と保護を目的とする基本理念が共有され培われてきたもの

個人情報保護法第1条

- 「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」
- 個人情報の適正な「利用」と「保護」のバランスのもとで個人情報を取り扱う事業者の遵守すべき義務を定めている。

DFFTに基づく「国際データ流通網」の拡大を目的として、多国間のデジタル貿易ルールの形成の促進を目指す施策

- 「デジタル貿易に関する日本国とアメリカ合衆国との間の協定（略称：日米デジタル貿易協定）」（令和2年1月1日）」
- 「日英包括的経済連携協定（EPA）」(令和3年3月26日)」
- 「TPP11（環太平洋パートナーシップに関する包括的及び先進的な協定）」

6.2. DFFT及びデータガバナンスとAI規制の両立

G7広島サミット「閣僚宣言：G7 デジタル・技術大臣会合（2023年4月30日）」

- DFFT及びデータガバナンス
  - 「越境データ流通及び信頼性のあるデータの自由な流通の促進」
- AI原則や信頼できるAIに関する施策
  - 「責任あるAIとAI ガバナンスの推進」

両者の項目は分かれている

DFFTの枠組みは、AIシステム適合性評価制度にも適用できる

DFFTを実現するための国際的なトラスト基盤の構築は、「標準化」と「認定・認証」により達成されるもの

適合性評価制度と目標も構成も一致

適合性評価制度におけるデータ・ガバナンスについてはDFFTの枠組みに基づく管理方策を提案することが可能と考えられる

DFFTとAIガバナンスに向けた取り組みは統合されておらず別個の施策として並行している

この併存を解消し一体化させることで、日本の強みであるDFFTの一層の促進を図りつつ、AIガバナンスに向けた取り組みについてDFFTを礎として展開することができる

6.3.　地政学的観点からのAI規制

DFFTは、データ管理を一定の域内に限定する「データローカライゼーション」と対照的な概念として提唱されたもの

各国のAI戦略との関係

- 米国のAI規制に向けた取り組み（大統領令からAI規制法）
- EUにおけるAI規制に向けた取り組み
- 中国などのアジア諸国との関係における経済安全保障の観点からの検討

新たな先端技術であるAIなどの機微技術管理は、経済安全保障の枠組みにおいて保護する方針も示されている

我が国においても、国際情勢の複雑化、社会経済構造の変化等により、安全保障の裾野が経済分野に急速に拡大している

背景及び経緯

国際情勢の複雑化、社会経済構造の変化等により、安全保障の裾野が経済分野に急速に拡大する中、国家・国民の安全を経済面から確保するための取組を強化・推進

令和3年10月：経済安全保障担当大臣の任命

我が国の経済安全保障を推進するための法案の策定を岸田内閣において表明

令和3年11月：第１回経済安全保障推進会議の開催

内閣官房に経済安全保障法制準備室を設置（令和4年2月にかけて、経済安全保障法制に関する有識者会議の開催：分野別検討会合を含め16回の会合で議論）

経済安全保障法制に関する提言の提出

「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案」

第208回国会に提出：　令和4年5月11日に成立、同月18日に公布

安全保障の確保に関する経済施策として４つの制度を創設

①重要物資の安定的な供給の確保

②基幹インフラ役務の安定的な提供の確保

③先端的な重要技術の開発支援

④特許出願の非公開

7. 「安心」に関する基準を定立すべき

「安心」は、「安全」と「信頼性」の両者が確保されることによって実現する

AIの信頼性と安全確保と品質保証に関する日本国内におけるガイドライン

- 石油コンビナート等災害防止3省連絡会議（経済産業省、総務省消防庁、厚生労働省）「プラント保安分野AI信頼性評価ガイドライン第2版」(2021年3月)
- 国立研究開発法人 産業技術総合研究所「機械学習品質マネジメントガイドライン第1版」(2020/06/30)
- AIプロダクト品質保証コンソーシアム「AIプロダクト品質保証ガイドライン 2022.07版」

8.　日本版AIシステム適合性評価制度構築にあたって必要な構成要素

定義

⓪規制対象となるAIシステムの定義

- 日本版AIシステム適合性評価制度を検討するにあたっては、まずは根拠法において**規制対象となるAIシステムの定義が必要**
  - EUの場合は高リスクAIを対象としていることから我が国においてもその対象範囲を定める必要がある

組織

①適合性評価の実施機関

手続

②AIシステム適合性評価制度における実施機関による審査、評価及び認証手続

規格

③規制対象となるAIシステムの研究開発、利用、販売、サービス提供に係るマネジメントシステム規格

表示

④AIシステム適合性評価制度に基づく認定を受けたことを示すマーク制度又はシールプログラム

⓪規制対象となるAIシステムの定義

JIS X 22989:2023（情報技術―人工知能―人工知能の概念及び用語）

- AIシステム
  - 人間が定義した所与の目標の集合に対して、コンテンツ、予測、推奨、意思決定などの出力を生成する工学的システム

AIの概念及び用語の定義にすぎない

JIS Q 31000：2019 (ISO 31000：2018)「リスクマネジメント－指針」「6.3.4 リスク基準の決定」においてもリスク基準の度合いは明記されていない

日本版AIシステム適合性評価制度におけるリスク分類案

（禁止対象となるAIシステムの法定は避けるべきではないか？）

高リスクAI → 低リスクAI

大リスクAI → 中リスクAI → 小リスクAI

①適合性評価の実施機関

JIS Q 17021-1：2015 (ISO/IEC 17021-1：2015)「適合性評価-マネジメントシステムの審査及び認証を行う機関に対する要求事項-第1部：要求事項」による適合性評価の実施は可能か？

- 日本国内には様々な認証機関が存在するが、製品安全規制とデータ管理のいずれの枠組みから実施機関の設置を検討するのかにより、指定される認証機関及びその評価手続は異なる
- 民間認証によって事実上の強制規格としてのAIシステム適合性評価制度を実現することは困難である

認証機関の設置及び審査は、AI規正委員会（仮称）の所掌とすべき

JIS Q 17011：2018 (ISO/IEC 17011：2017)

「適合性評価 – 適合性評価機関の認定を行う機関に対する要求事項」

- JIS Q 17011の対象となる適合性評価機関は、試験所・校正機関・製品認証機関
- JIS Q 17025「試験所及び校正機関の能力に関する一般要求事項」
- JIS Q 17034「標準物質生産者の能力に関する一般要求事項」
- JIS Q 17065「適合性評価―製品、サービス及びプロセスの認証を行う機関に対する一般要求事項」

AIシステム適合性評価制度の実施に用いるためJIS Q 17065を改定

or

AIの適合性評価制度に特化したマネジメントシステム規格の新設

「AIマネジメントシステム規格（仮称）」の制定を検討

- 根拠法：産業標準化法
- 目的：AIシステム適合性評価制度に関するマネジメントシステム認証

留意事項

（1）マネジメントシステム規格の共通基本構造を定めているISO/IEC専門業務用指針 補足指針2023年（第3版）の附属書SLと、EUのAI法案の高リスクAIに係るマネジメントシステムの内容を比較すると附属書SLとは不整合であることを踏まえて日本版の規格を策定すること

- 我が国においてAIシステム適合性評価制度におけるマネジメントシステム規格を策定する際に附属書SLとの整合性を確保した要求事項で構成する規格を策定することで、国際標準としてのAIシステム適合性評価制度を提案することが可能になる
- ただし、AIに関する国際標準の検討は、2017年にISO/IEC JTC1/SC42が設置され、①AIガバナンス、②基礎的標準、③データ、④信頼性、⑤ユースケースと応用、⑥計算アプローチと計算的特徴の6つのWGにおける検討が進んでいる
- ISO/IEC FDIS 42001 (Information technology - Artificial intelligence - Management system)が今後策定されると当該規格はJIS化される予定であることから、国内規格の検討よりも国際標準の策定のほうが先行するため、マネジメントシステム規格とともに認証規格についても、ISOが策定するAI国際標準規格をJIS化する方向が現実的

（2）これまで検討がなされてきたガイドラインや指針等に定められている「原則」をはじめ、AIの研究開発から利用において留意すべき実体的な利益の保護のための規定は、マネジメントシステム規格の「附属書」として編入することが可能

- AIシステム適合性評価制度における手続的な義務とともに、精緻な議論がなされてきた個人の権利利益保護や原則の遵守を基本理念とする制度の構築を目指すべき

電気用品安全法に基づく**PSEマーク**の活用（案）

- ただし、当該マークの対象は「電気製品」
- EUのAI法案のCEマークと対比すると、EUの機械指令（機械規則提案）に対応する部分については整合するものの、「AIサービス」への適用については課題が残る
- AIシステムをネットワークに接続する場合は、端末機器の技術基準適合認定と無線通信については技術基準適合証明を取得する必要がある

法整備の方向性

(a)**電気用品安全法の改正**によりPSEマークをAIシステム適合証明に活用する方法を検討し、既存の「技術基準適合認定・証明 」は現行法の枠組みで対応

(b)**日本版のAI新法を制定**し規制対象のAIの定義を定めるとともに、整合規格への適合から表示（マーク制度）に至る義務を法定し、整備法において適合認定・証明手続を一括して定めるハネ改正を実施

(c)**産業標準化法を根拠**とする「AIマネジメントシステム規格（仮称）」の認証制度に基づく新たなマーク制度を創設

8.　AI規正委員会（仮称）の設置提案

日本版AIシステム適合性評価制度を機能させること

民間部門及び公的部門におけるAI利用について監督すること

国家行政組織法第三条に基づくいわゆる三条機関（委員会）を想定

- EUのAI法案が定める欧州人工知能委員会(EAIB)に対応する機関の設置が必要
- 「欧州評議会AI条約」も監督機関の設置義務を求めるはず
  - 欧州評議会個人データの自動処理に係る条約（条約第108号）が「監督機関の設置」を締約国に求める内容であったことに鑑みると、「欧州評議会AI条約」の目的も同様の方向性になることは自明であろう（CoEの発想は同じはず）
- 事業者側が実施するマネジメントシステム構築・運用指針である「AIシステムマネジメント規格」を産業標準化法に基づいて制定する場合
  - 当該規格への適合性の審査基準は、行政手続法5条の審査基準及び同12条の処分基準に基づいて、AI規正委員会が整合規格を策定し要求事項を定めるべき

認証部門はAI規正委員会に設置すべき

AIシステム適合性評価制度を機能させるための認証制度については、民間組織による認証制度は国際的な相互認証を実現する上で支障となることがある

AI規正委員会に認証部門を設け、事実上の強制規格として実施することが望ましい

- 同様の趣旨について、個人情報保護法の3年毎見直しにおいて、民間認証である「プライバシーマーク制度」を個人情報保護委員会に認証部門を設置して実施すべきであるという見解を述べた
- その趣旨は、国際的な個人情報保護の枠組みにおいてJIS Q 15001を国際標準として機能させ、さらにEUの一般データ保護規則(GDPR)42条のシールプログラムとの相互認証を実現することにあった
- GDPRに基づくシールプログラムとの相互認証については、その協議に向けた兆候はあったものの、日本国内におけるシールプログラム（マーク制度）の実施が民間組織によるものであることから、現在に至るまで実現には至っていない

AI技術に特化した委員会ではない体制も視野に入れる必要がある

重要・新興技術（Critical and Emerging Technologies(CET)）に係る米国の戦略と歩調を合わせ、「重要・新興技術委員会」とすることも考えられる

例えば、米国が進めている8分野

- 通信・ネットワーク技術
- 半導体
- AI・機械学習
- バイオテクノロジー
- 測位・航法・タイミング（PNT）サービス
- デジタルアイデンティティ・インフラ
- 分散台帳技術
- クリーンエネルギー発電と蓄電
- 量子情報技術

まとめ

非拘束的なガイドラインを軸とする自主的な規律に基づく我が国における取り組みに対し

(a)法規制回避論からの脱却

(b)AI規制の最適化

(c)日本「発or初」の
新たなAI規制政策の立案

日本のAI規制政策の隘路を認識するために

非拘束的なガイドラインに基づく自主的な規律は

- 自主的（自発的）に賛同する組織に対する取り組みを推進する上での指針となるため有効

規制の根拠となる法令が存在しない状況

- 準則や法解釈の指針としてのガイドラインではなくガイダンス的な機能を発揮しているにすぎない

AIシステムの開発・販売・提供を行う組織

- EUの適合性評価制度に強制的に従わざるを得なくなる
- 日本企業としても、AIシステムを開発し販売を企図する場合にEU市場を放棄するわけにはいかない
- 事実上の世界標準として機能するEUの適合性評価制度に準拠した対応を迫られる
- 法令遵守意識が高い日本企業は、忠実にその制度に準拠するための取り組みを進める
- 強制的に遵守せざるを得ない規格や制度への準拠については従順に対応し単にそれらの規制に盲従するしかない状況を、AI規制への対応においては見直さなければならない

法規制を回避し自主的な規律の推進を掲げた政策を継続し、国際動向を注視していながら気が付くと国際的には法規制に舵を切った政策が主流になった時、AI政策分野での日本の凋落を見守るしかない状況に陥るおそれがある

本研究は、JSTムーンショット型研究開発事業JPMJMS2215の支援を受けたものである。