

情報通信法学研究会  
令和4年度AI分科会第2回

# EUのAI規則案の概要

— 欧米のその他の動きや日本への示唆とともに

渥美坂井法律事務所・外国法共同事業  
弁護士・ニューヨーク州弁護士

大阪大学招へい教授（同大学社会技術共創研究センター）

三部 裕幸



# 【本題の前に】AI規則案の全文和訳のご紹介

- 総務省ウェブページにて掲載

- 総務省からの委託により私が作成したAI規則案の全文和訳が、同省「AIネットワーク社会推進会議」ウェブページで公表されていますので、ご参考になればと思います。
- [https://www.soumu.go.jp/main\\_content/000826706.pdf](https://www.soumu.go.jp/main_content/000826706.pdf)



1.

---

# AI規則案の目的と リスクベースアプローチ

# AI規則案の目的と特徴

- **目的**（ごく大まかに言えば）
  - AIの**リスク**（健康、安全、基本権などへのリスク）**に対処する**
  - AIの**導入**、AIへの**投資**、AIによる**イノベーション**を**強化**する

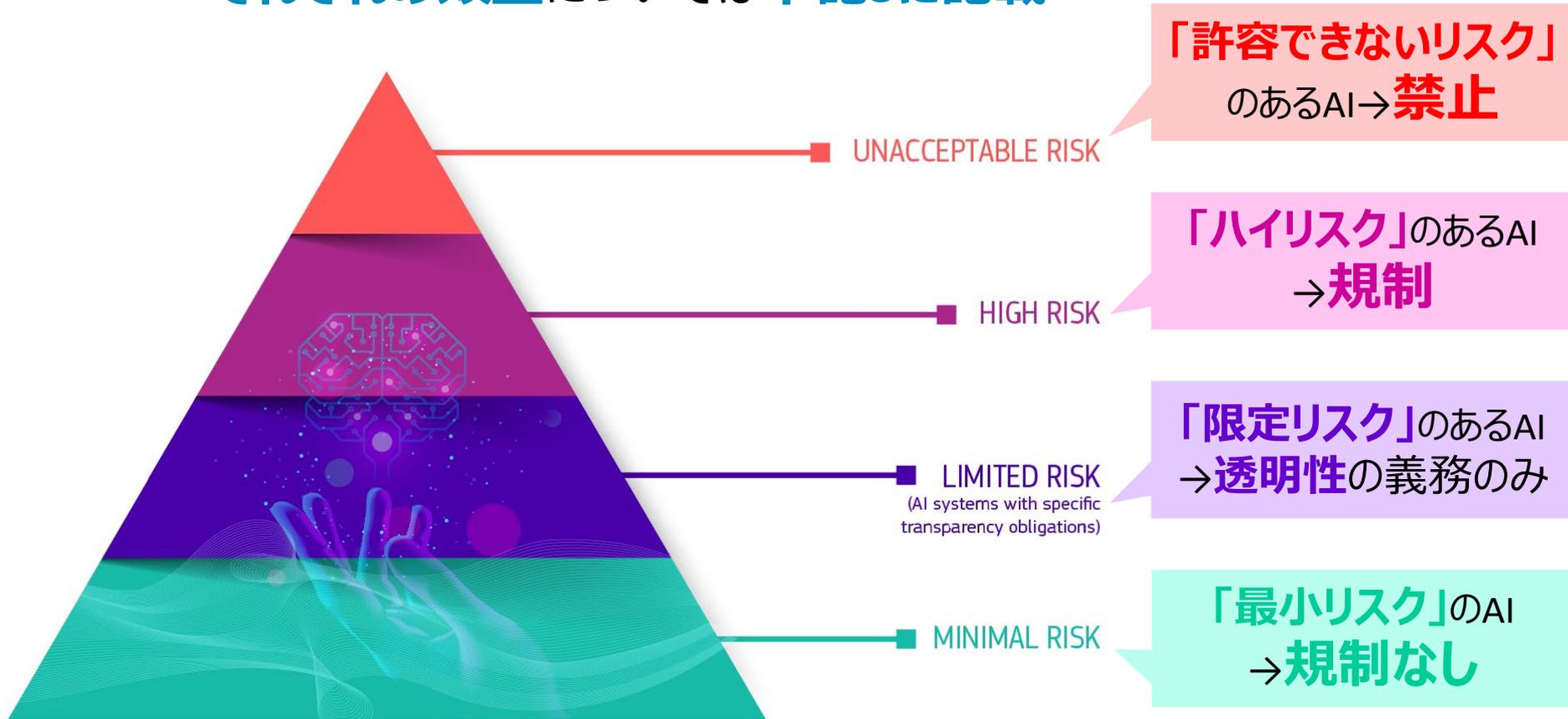
そのために

- **特徴**（ごく大まかに言えば）
  - ① **リスクベースアプローチ**を採用
  - ② **統一ルール**が幅広く**適用**される（**日本にも適用あり**）
  - ③ **遵守しない場合**の**リスク**が**大きい**

①を次のページと下記3で、②③を下記2で説明致します

# 最大の特徴：「リスクベースアプローチ」

- リスクに応じて、規制内容を変える
  - それぞれの**類型**については下記3に記載



(図の出典) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

# 2.

---

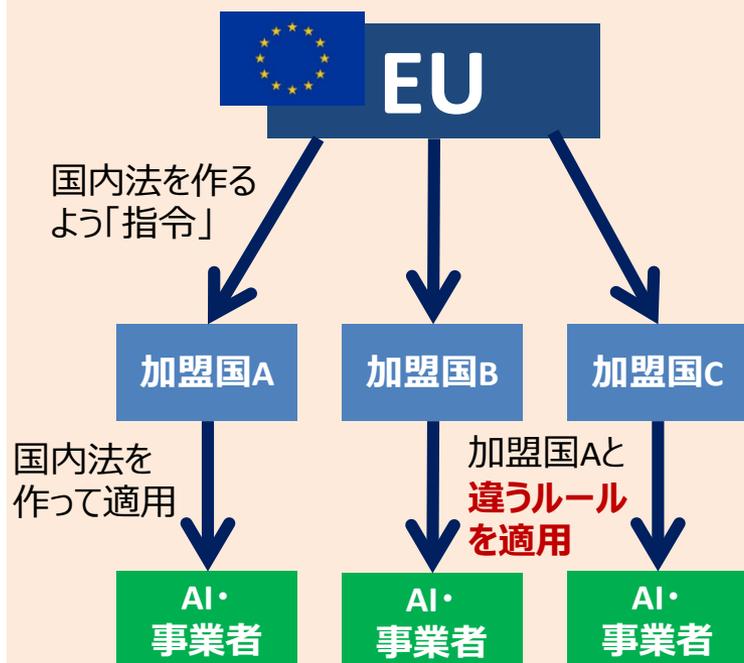
## AI規則案の幅広い適用と 違反した場合のリスクの大きさ

# 「規則」 (Regulation) → 統一ルール<sup>①</sup>の直接適用

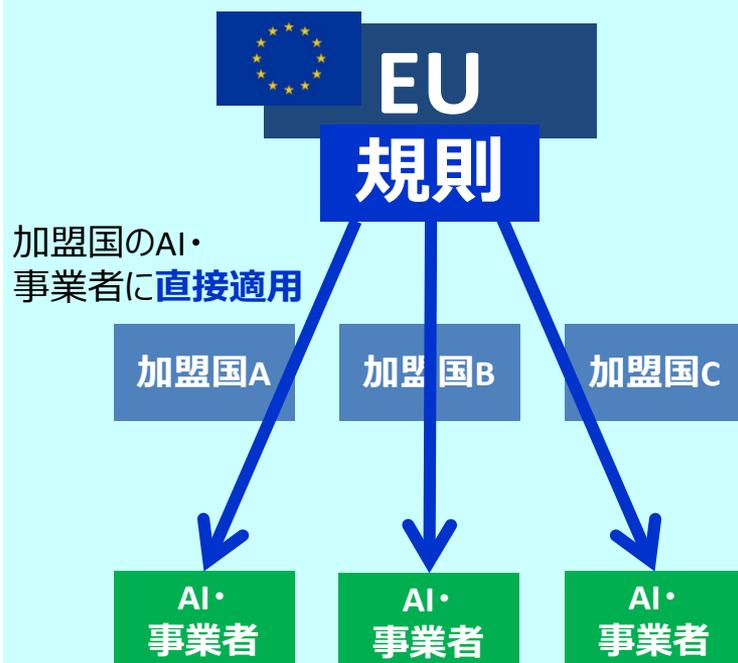
- AI規則案は「規則」 → 加盟国に統一ルールが直接適用される
  - 加盟国ごとに国内法化が必要 (※) となる「指令」 (directive) と異なり、EU全体で統一したルールを作ることができる

(※) AI規則案でも加盟国ごとに国内ルールが必要な部分はあるが、加盟国が国内実施の措置を担う「指令」とは異なる

「指令」の場合：EU内でルールがバラバラ。  
EU市場でAIを流通させにくい



「規則」の場合：EU統一ルールが適用。  
市場でAIを流通させやすい



# 域外適用 → 日本にも適用される

- 大まかに言えば、**EU所在の者をターゲットにAIシステム・サービスを提供すれば日本にも適用される**（2条1項(a)号※）

（※）正確には、EUにおいてAIシステムを市場に置き又はサービスを提供した提供者（など）に適用される。



- AIの**アウトプットのみ**が**EUで利用**される場合にも**適用される**（同項(c)号、前文(11)項）。例えば
  - ① **EU域内の事業者**が、**EU域外のAI事業者と契約**をして**AIシステムのアウトプットを提供させる**場合であって、
  - ② その**アウトプット**が**EU域内の自然人に影響する**場合

# 適用対象となる「AIシステム」

- 次の**二つの要件を満たすもの**（3条1項）
  1. **付属書の技法及びアプローチ**で開発された**ソフトウェア**
    - 「ディープラーニングを含む様々な方法を用いた.....**機械学習によるアプローチ**」
    - 「知識表現、帰納（論理）プログラミング.....を含む**論理ベース及び知識ベースのアプローチ**」
    - 「**統計的アプローチ**」など
  2. **人間が定めた一定の一連の目的**のために、当該ソフトウェアが相互作用する環境に影響を与える**コンテンツ、予測、推奨又は決定などのアウトプットを生成**することができるもの



- **かなり範囲が広い。ソフトウェアの利用が  
思わぬところで適用対象とならないかどうか注意が必要**

# 違反した場合のリスクが大きい

- 違反すると**巨額の制裁金**が課され得る
  - **最大で3,000万ユーロ（約40億円）**か**全世界売上高の6%**のうち**どちらか高い金額**（71条）
- 違反すると**EUでビジネスができなくなるおそれ**もある
  - 一定の違反や、基本権にリスクが生じ得る場合などに、適切な対応をしないと、**AIシステムの市場からの取下げ**や**リコール**などの**是正措置**を**公的な機関から義務付けられる可能性がある**（65～68条）

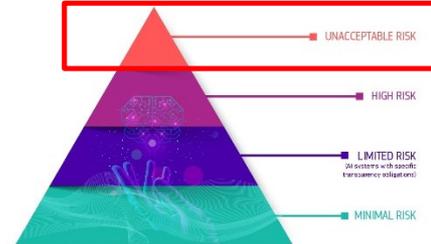
The background features a complex, abstract pattern of glowing blue lines that flow and curve across the frame, creating a sense of dynamic movement and depth. The lines vary in opacity and brightness, set against a darker blue gradient background.

3.

---

# リスクに応じた規制の概要

# 許容できないリスクのあるAIシステム



## • 四つの類型 (5条1項)

### サブリミナルな技法

精神的・身体的な害を生じさせる態様で**対象者などの行動を実質的に歪める**ため、対象者の意識を超えた**サブリミナルな技法**を展開

### 脆弱性を利用

精神的・身体的な害を生じさせる態様で年齢・障害などによるグループ（子ども、障害者など）の**脆弱性を利用**

### 公的機関のソーシャルスコアリング

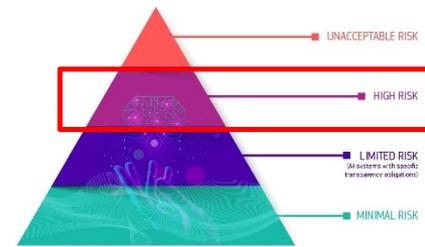
自然人の信頼性評価や分類のため**公的機関がソーシャルスコア**を使い、自然人に**害や不利な取扱い**などが発生

法執行を目的とした**公にアクセスできる場所**における「リアルタイム」**遠隔生体識別システム**（例外を除く）



# 禁止

# ハイリスクAIとは



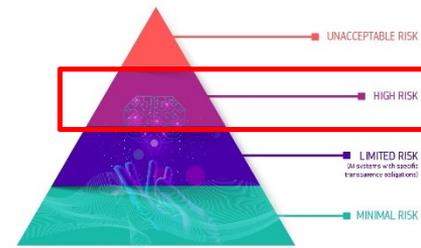
- **付属書II型**（下記）・**III型**（次頁）に該当するAIシステムは**ハイリスク**（6条1項・2項）

## – **付属書II型（安全型）**： **次の二つの要件**を満たすもの

- 付属書IIの法令の対象製品の**セーフティコンポーネント**としての使用が意図されているか、それ自体が**付属書IIの法令の対象**となる
  - 機械、玩具、娯楽用船舶、昇降機、医療機器などの法令
- 同法令によって**第三者による適合性評価が必要**となる

➡ **規制がかかる**

（※）「付属書II型・III型」や「安全型・スタンドアロン型」は、筆者が便宜上そのように表現しているだけであり、EUの正式な表現ではない。



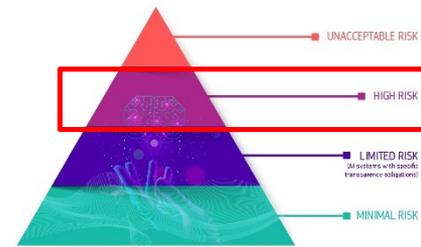
## – 付属書III型（スタンドアロン型）： 一定の分野＋一定の利用

「一定の分野」	「一定の利用」の例（あくまで例）
自然人の生体識別・分類	民間企業による自然人の遠隔生体識別
重要なインフラの管理・運営	交通管理、電気水道ガスのセーフティコンポーネントとして使用
教育・職業訓練	入学の決定、割当て、学生の評価、入試の評価
雇用、労働者管理、自営業へのアクセス	面接での評価、昇進や労務契約終了の決定、パフォーマンスや行動のモニタリング・評価
重要な民間・公共のサービス及び給付へのアクセス及びその享受	公的扶助の給付やサービスを受ける自然人の適格性を評価、自然人のクレジットスコアを確立
法執行	ポリグラフとして使用、プロファイリングで犯罪・再犯予測
移民、難民等の庇護及び国境管理	難民等の庇護・査証・居住許可の申請の検討支援
司法の運営及び民主的なプロセス	司法機関の事実・法律の調査や解釈、事実への法適用の支援

➡ **規制がかかる**

(※) 「付属書II型・III型」や「安全型・スタンドアロン型」は、筆者が便宜上そのように表現しているだけであり、EUの正式な表現ではない。

# ハイリスクAIの義務



## 付属書II型・III型の場合

### • ハイリスクAIシステムの要件 (第III編第2章)

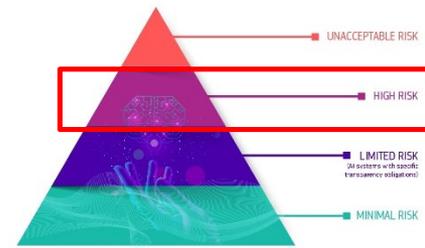
- リスクマネジメントシステム
- データとデータガバナンス
- 技術文書の要件
- 記録の保持
- 透明性・情報提供
- 人間による監視
- 正確性、頑健性及びサイバーセキュリティ

### • 提供者等の義務 (第III編第3章)

- 品質管理システム
- 適合性評価を受ける義務
- 自動生成ログの維持義務
- 是正措置・情報提供義務
- EU代理人選任義務 など
- 販売者、輸入者、利用者その他の第三者にも一定の義務あり

(※) 「付属書II型・III型」や「安全型・スタンドアロン型」は、筆者が便宜上そのように表現しているだけであり、EUの正式な表現ではない。

# ハイリスクAIの義務



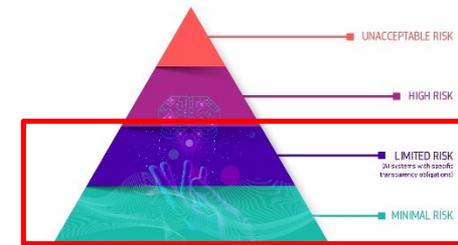
## ハイリスクAIの適合性評価

- 提供者は**事前に適合性評価手続**を経なければならない（19条）
- **原則**として**自社で評価**すればよい（43条1項1号(a)、2項）
  - しかも**整合規格・共通仕様を守れば要件遵守が推定される**（40条、41条）
- **例外**として、次の場合には**第三者評価**が必要
  - **付属書II型（安全型）**の場合（43条3項。**付属書IIの法令**に基づく**第三者評価**）
  - **自然人の生体識別・分類AI**が**整合規格・共通仕様を守っていない**場合（43条1項第2段落）
- 要件遵守が証明された場合、提供者は、**EU適合宣言書**を作成し、また、適合性の**CEマーキング**を付す（19条、48条、49条）

## 付属書III型のデータベース登録義務など、他にも義務がある

（※）「付属書II型・III型」や「安全型・スタンドアロン型」は、筆者が便宜上そのように表現しているだけであり、EUの正式な表現ではない。

# 限定リスク・最小リスクAIについて



- **限定リスクAIの透明性の義務**（52条）。例として：

## チャットボット

（など自然人と相互作用するAI）  
→ AIシステムと相互作用していると**自然人に知らせる義務**

**ディープフェイク**の場合  
→ コンテンツが**人工的に生成・操作されたものであることを明らかにする義務**

- **行動規範の奨励**（69条）

- 上記「**ハイリスクAIシステムの要件**」（第III編第2章）を、限定・最小リスクAIシステムにも**任意に適用することを促す**
- AIシステムの**提供者やその団体が作る**ことが想定されている。**利用者・ステークホルダーやその団体が参加して作るケースもあり得る**と想定されている

The background features a complex, abstract pattern of glowing blue lines that flow and curve across the frame, creating a sense of motion and depth. The lines vary in opacity and thickness, with some appearing as bright, sharp streaks and others as softer, more ethereal trails. The overall color palette is a range of blues, from deep, dark tones to bright, vibrant highlights.

4.

---

# イノベーション支援

# — 以下の手段で、イノベーション支援を図る —

- AIの**規制のサンドボックス制度**
  - 革新的なAIシステムが市場に置かれる前に、限定的な期間、**開発・試験・検証を促進するための制御された環境**を提供
  - **他の目的で適法に収集された個人データを、サンドボックス内の一定のAIのために利用**することを、**制限付きで認める**
  - **小規模提供者等に、サンドボックスへの優先アクセス**
- 具体的な**意識向上のための活動**
- **小規模提供者等**の問合せに応じる**専用チャネル**の設置など

The background is a vibrant blue with a complex, abstract pattern of overlapping, flowing lines that create a sense of movement and depth. The lines vary in thickness and opacity, creating a layered effect. The overall color palette is monochromatic, ranging from deep navy to bright cyan.

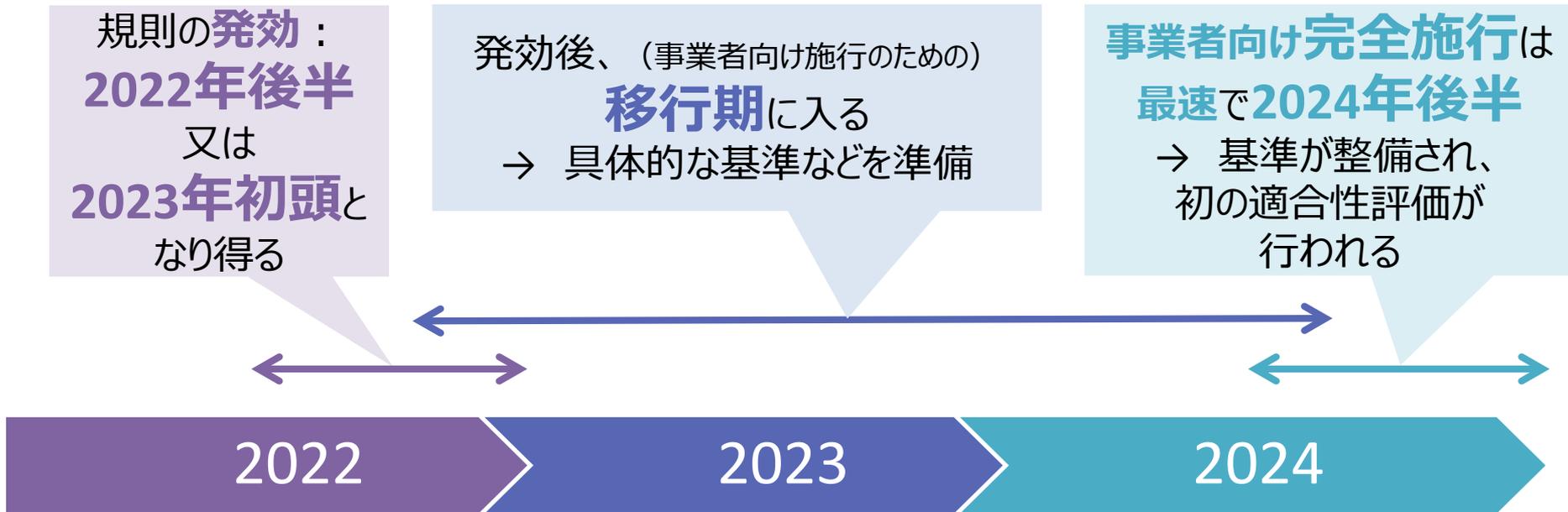
5.

---

# 施行スケジュール

# 施行スケジュール

- 欧州委員会は、以下のスケジュールを目指している



- 実際には少し遅くなるかもしれない。しかし、何年も遅れるとは見込まれない（発効は2023年？）

(欧州委員会が目指すスケジュールの出典)

<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> のNext steps欄

6.

---

EU・欧州のその他の動き、  
米国の動き、  
日本への示唆

# AI規則案の現状

- AI規則案の現状

- 欧州議会・EU理事会がそれぞれ検討中

- 2022年10月12日現在公表されている修正案は、欧州議会の法務委員会とEU理事会がそれぞれ9月に公表したものが最新

- 三者対話（trilogue）に入るよりも前の段階

- 論点の例

- AIシステムの定義

- 適用除外

- 許容されないAIの範囲

- ハイリスクAIの義務 など

# — AI規則案は、実はビジネスに有利な面がある —

- **原案の以下の点はビジネスに有利**と考えられる  
(もちろん、**今後の修正で変更されるかどうかの注視は必要**だが)
  - **加盟国ごとの対応をしなくてよい**
  - 各リスクのあるAIごとに見ても、
    - **許容されないAIの範囲がそれほど広くない**
    - **ハイリスクAIのルールには標準化などの議論**が取り込まれそう。  
しかも、ハイリスクAIの**適合性評価は原則自社**でできる
    - **限定リスクAI**というだけであれば**規制はほとんどかからない**
      - たとえばディープフェイクの悪用問題にも強い規制を課していない
  - **イノベーション支援策**が盛り込まれている



- 企業は、**自社にとっての有利・不利を見極める**ことが大切
  - **ハイリスクAIの基準などの整備**に加わるほうが得か？

# EU・欧州の他の動き（例）

- ソフトローの動きの例
  - 信頼できるAIのための倫理ガイドラインと、それに基づく企業の自主的な対応
- ハードローの動きの例
  - EUのAI民事責任指令（AILD）案
    - 2022年9月28日、欧州委員会、「人工知能の非契約民事責任ルールを採択する指令の提案」を公表
  - 欧州評議会のAI条約構想
  - AIの利活用に対するGDPRの適用 など

# 米国の動き（例）

- **EUとの連携**
  - 貿易技術評議会（TTC）
- **ソフトローの動きの例**
  - NISTのAIリスクマネジメントフレームワーク（現在はドラフト段階）
  - OSTPの「AI権利章典の青写真」
    - ソフトローでありつつ、ハードローを視野に入れて企業に対応を促している
- **ハードローの動きの例**
  - **連邦議会提出法案**
    - 特にアメリカのデータプライバシー及び保護法（ADPPA）案、アルゴリズムアカウントビリティ法案
  - **既存の連邦法**
    - FTC法、労働法（EEOC公表物）、金融法（Fintech、ロボアドバイザー）など
  - **州法・自治体の法律**
  - **訴訟事例**

# 欧米の動きをみると

- ソフトローとハードローの**組合せで対応**している。なぜ？



- ① **ハードローだけの対応**は（適切か否か以前に）**できない**
  - 既存の現行法を全てAI法に置き換えることなど現状できるわけがない
- ② **ソフトローだけ**で進めることも**できない**
  - 「ソフトローだけ」= 規制がない状態、ではない
  - 「ソフトローだけ」= **既存の現行法が足枷**になる状態
    - 民法も刑法も業法もその他の法律も適用される
    - それら既存の現行法のほとんどは、AIの出現を想定していない
    - レベル4の自動運転のためには道交法改正が必要だった。同様の法改正や解釈の明確化が必要な論点が、未だ手つかずのまま多く残されている
- ③ **現行法がAIにも適用**される → **欧米の行政はそのことを意識し、現行法がAIにどう適用されるかを検討・公表**している

# 民主主義国の動きとして

- ソフトローとハードローの**組合せに収斂**する可能性が高い
  - 各国・各法域の違いは、単に**規制手法の違い**にすぎない
  - 法の背景をなす**基本的な理念**は既に**各国で共有**されている
  - **米欧**はTTCなどで**連携**。行政も**ディスカッション**を深めている

# 日本（の企業）への示唆

- 国内外のAIハードロー・ソフトローについて、タイムリーに情報を追いつつ、自社ビジネスにどう関わるかを先入観なく評価することが大切
  - 自社に有利に活用できるのではないか
  - 不利な面や違法・炎上等のリスクがあるとしたらどのように対策できるのか



- EUのAI規則案についても、上記のように自社ビジネスへの影響を評価することが大切
  - 日本の企業に一律に有利又は不利ということではない
  - 個社ごとに、有利不利や対応が必要な点の検討が必要

# 日本（の企業）への示唆

- ソフトローとハードローは、二者択一ではない
  - 実際、欧米はAIについてソフトローとハードローを併用している
  - ソフトローとハードローは、両方必要
    - ソフトローに対応したガバナンスがあつてこそ、ビジネスへの信頼を得られる
    - ハードロー（の明確化）をしなければビジネスが後で違法とされるリスク
- 「AIに関し法律ができる」と現行法よりも規制が上乗せされるからソフトローがよい」は、誤解である場合が多々ある
  - ハードロー＝現行法の改正をしないとできないAIビジネスが多い
  - 今でもできるAIビジネスでも、法律を変えればやりやすくなり得る

# 渥美坂井法律事務所・外国法共同事業

パートナー 弁護士・ニューヨーク州弁護士  
(第二東京弁護士会所属)

大阪大学招へい教授 (社会技術共創研究センター)

## 三部 裕幸

電話 (直通) : 03-5501-2276

Email: hiroyuki.sanbe@aplaw.jp

本資料、及び本資料を用いて私が述べた事項は、私が所属する法律事務所、又は私や当該法律事務所が所属・活動する団体等における見解を述べたものではありません。

Eightでの名刺交換用QRコード

