一般社団法人新経済連盟
第4回国際動向勉強会

EU・米国・中国におけるAI規制の動きとIT企業に求められる対応

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

大阪大学招聘教授（同大学社会技術共創研究センター）

アメリカ法曹協会（ABA）北東アジア委員会委員長

三部　裕幸

2023年2月24日

目次

1. **EU**及び**米国**の**AI法制**に関する近況、欧米の**類似点・相違点**

2. **中国**の**AI法制**に関する動き

3. **日本**における**AI法制の検討状況**について

1.

EU及び**米国**のAI**法制**に関する近況、欧米の**類似点・相違点**

AIのEU法案と米国法案をここで話す意味

- **EU・米国・カナダ**などの**主要民主主義国**の**AI法案が出揃ってきた**。
- 従来、**日本の一部の人たち**は、**EUに対してはソフトローがいいと主張**してきた。**米国には特段そのような主張は展開してこなかった**。
- **米国**は**EUと連携協調**して進めていて、それぞれの**法案が類似**していることが明確になった。**カナダもしかり**。
- **AI法制度問題**で、**主要民主主義国が同じ方向**を向いている時に、

日本は**同じ方向**を向いて
協調の道を進むのか？

日本は
独自の道を進むのか？

規制は必要？　規制は邪魔？

例えば、**自動運転車**。今のまま自動運転車を商用で販売し、それが**事故を起こし**、歩行者や自転車を**はねた**とします。

新たな規制をかけない（新たな法律を作らない）ならば、その事故は**誰のせいなのか現状ではわからない**ということになります。

「AIには**イノベーションが大事**だ。**規制を掛ければイノベーションを阻害**する。**被害者**は誰のせいか分からない状態を我慢するしかない。**文句があれば、AI開発者、車両販売者、車両運行事業者に順番に訴訟を**かければよい」と皆さんは思うでしょうか？

新たな規制がなければ、自動運転車は社会から受け入れられず、**自動運転車産業**は**すぐに消滅**するでしょう。

規制の要否は

一概に言えることではない

必要な規制もあれば、
邪魔な規制もあり得る

OpenAIのCTOの数日前の談話

- 「AIは**誤用・悪用され得る**ため、この技術の利用を、**どのように統制**（グローバルに、かつ人間の価値と調和するように統制）**するかが課題**となる」
- 「このような課題があることを公に認識されるようにし、コントロールされ責任あるAIにするために、**規制当局や政府の関与が重要**となる。**企業の関与だけでは足りない**」
- （政府の関与によってイノベーションが遅れてしまわないか、規制当局の関与は時期尚早ではないか、との問いに対して）「**関与が早すぎるということはない**。AIの技術が持つことになるインパクトを考えれば、**皆が関与を始めることが非常に重要**だ」

※ 出典：https://time.com/6252404/mira-murati-chatgpt-openai-interview/

※ OpenAIはマイクロソフトが出資者 → **マイクロソフトも同様の意図**だと考えられる。
OpenAIは、**過去3か月**で**1億サブスクライバーを獲得**した気鋭のAIスタートアップ

→ これは優れたAI開発者の当たり前の意向？

→ これは変わったAI開発者の偏った考え？

というようなことを頭において、
EU法案・米国法案の話をお聴きいただきます

EUのAI規則案

- **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**
  - AIの**導入と投資**の促進、AIによる**イノベーション**の**強化**

そのために

- **特徴**（ごく大まかに言えば）

① **統一ルール**が**幅広く適用**される
→ EUとAIの取引をする**日本企業にも適用あり**

② **遵守しない場合**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**市場からの退出**や**リコールなど**があり得る

③ **リスクベースアプローチ**を採用し、AI企業に対応を求める

特徴③について、**以下のページで説明**致します

③ 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

※ EUの価値観とは：
人間の尊厳、自由、民主主義、平等、法の支配、人権の尊重（EU条約2条）
→ **先進民主主義国の法律に既に織り込まれている**

たとえば（大雑把な例）

「許容できないリスク」のあるAI→**禁止**

- **EUの価値観（※）に反する**AI
  - **子ども、障害者などの脆弱性**に付けこみ不利に扱うAI
  - **国が国民に社会スコア付け**して不利に扱うAI
  - **逮捕・起訴の目的**で公共の場で**リアルタイム顔識別**　など

「ハイリスク」のあるAI→**ハードロー**の規制

- **安全に関わる**AI（医療機器、機械、船舶等）
- 主に、**差別・偏見・迫害などにつながりやすい**AI（自然人の生体識別・分類、雇用・入学の決定、貸付けの決定、犯罪・再犯予測など一定の類型）

「限定リスク」のあるAI→**説明**義務のみ、**行動規範が奨励**

- **見聞きする人が「AIではない」と誤解しやすい**AI（チャットボット、ディープフェイク）→AIであると説明
- **感情認識・生体分類**AI　→　システム動作情報の説明

「最小リスク」のAI→**規制なし、行動規範が奨励**

- **上記以外のAI**

どの類型でも、現行のEU法・加盟国法は適用され続けるので注意（AI規則案で改正される点は改正後の規定が適用）

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

ハイリスクAIの義務

- **ハイリスクAI**の場合、下記**「要求事項」**と**「義務」**が発生

- ハイリスクAIの**「要求事項」**
  → **自社**の**ガバナンス**が求められる

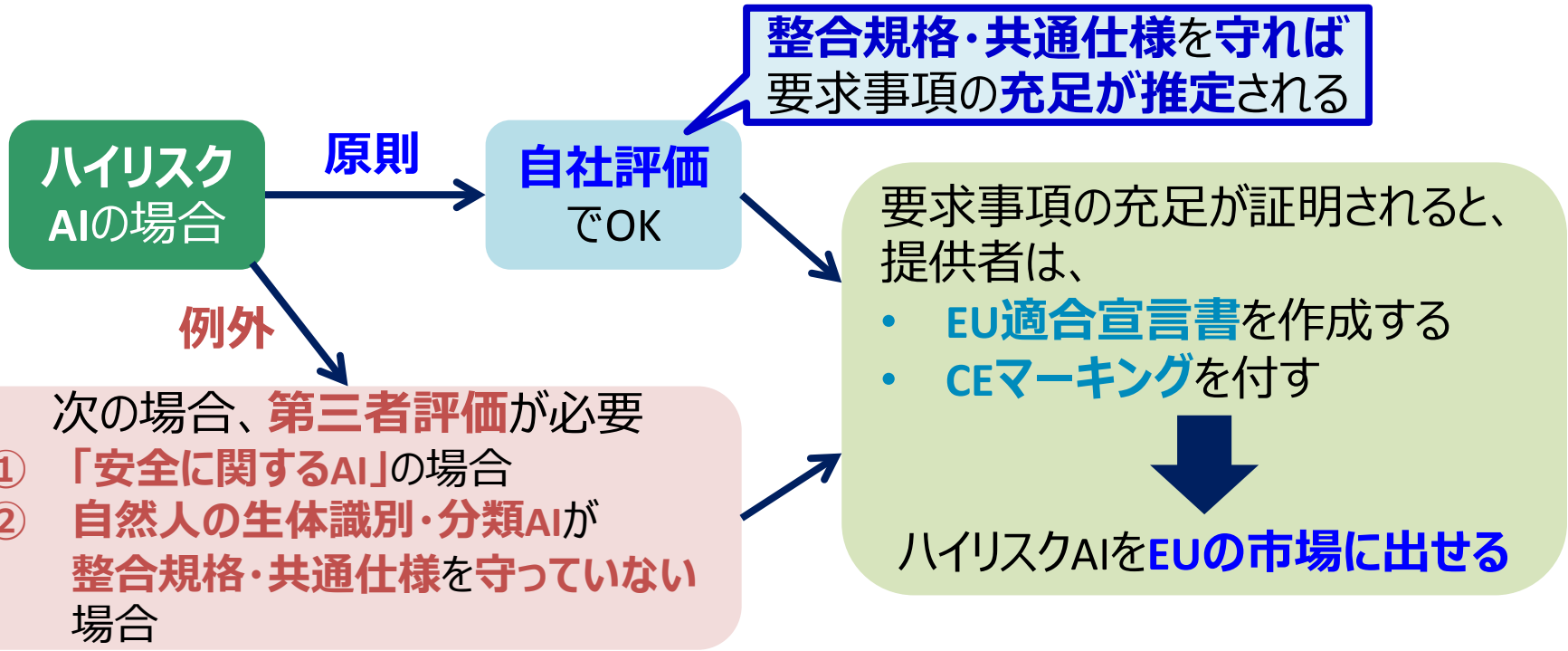
- **各種リスク管理**の対策が必要
  - 管理システムの導入
  - データ・文書・ログの保存
  - 透明性の確保
  - 人間による監査
  - サイバーセキュリティなど

- **提供者等**の**「義務」**
  → **対象者を特定**して**義務を明確化**

- **適合性評価**の**義務が重要**
- 市販化後のモニタリング義務
- 違反の場合の是正義務
- EUに拠点がない場合の**EU代理人選任義務**　など

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）
    - 前ページの**「要求事項」**を**AIシステムが充足**していることを**評価する手続**



従来のEU法・加盟国法と今回のAI規則案

- AI規則案が法制化されなくても、AIが何らか**EU法・加盟国法の規制を受ける**（少なくとも受け得る）点に**変わりはない**
  - **許容できないリスクAI**は**許容されず**、かつ、
  - **ハイリスクAI**は何らかの**規制を受ける公算**が**極めて高い**

一例を挙げれば、**日本企業**が**英国（当時EU）**の**警察に犯罪者と思しき者の顔識別システムを提供**したところ、警察によるそのシステムの利用が**欧州人権条約と英国法に照らして違法**と判断された裁判事例

英国顔認証訴訟に関連して

- もし、**顔識別システム開発当時**、**AI規則が制定されていたら**、
  - 当該日本企業は**警察に売り込むことはなかった**はず。
  - そして、**ハイリスクAI領域で輸出・販売**しようとしたはず。
  - そうすれば、不祥事例ではなく、**成功例になっていたかも**しれない。

↓

- しかしながら、**AI規則がなかったから**、今から考えれば、
  - よりによって警察に売り込み、訴訟を起こされ、**ビジネスは失敗**
  - 「顔識別システムへの人の登録は**本人同意が得られた場合のみ**行う」ことにした。

↓

- **規制がはっきりとあれば**、**チャンスを伸ばすことができた**のに、**規制がなかったばかりに**、**チャンスを逃したのかもしれません**。
- **規制**は、**イノベーションを強化するか、それとも阻害するのか**。
  上記の事例は**「規制は悪」と簡単には言えない事例**だと思います。

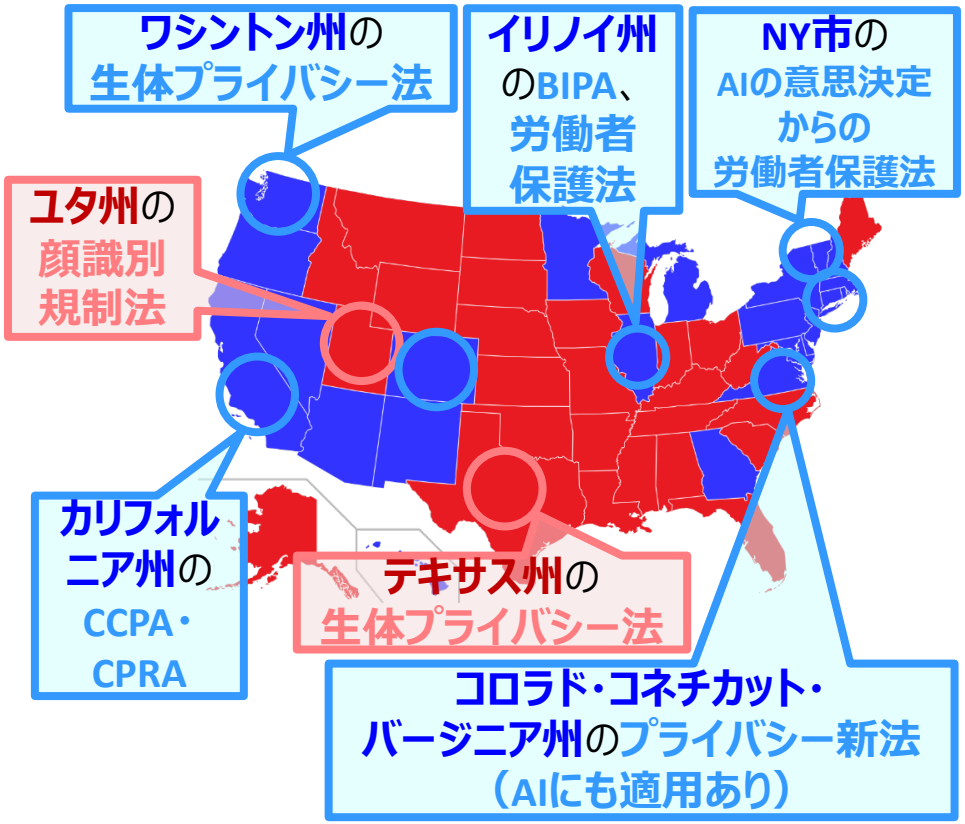
(2) 米国：ハードローへのシフト

米国は、**ソフトロー**と**ハードロー**を**併用**している

- **当初ソフトロー主体**で進んだが、**現況はハードロー**のウェイト増

- **ソフトロー**の例
  - NISTの**AIリスクマネジメントフレームワーク**
  - OSTPの**「AI権利章典の青写真」**

- **ハードロー**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**）案は**超党派**で**可決の見込み**
  - **連邦・州の現行法**
    - **現行法**は**全部AIに適用**（今後のAI新法と矛盾する部分があればAI新法が優先）
    - FTC法、労働法、金融法など
  - **州・自治体の新法**



(3) EUと米国の共通点・相違点

- **相違点**：**AI法制**の**建付け**

- **新たな規制**を導入し**加盟国を拘束**

- **現行法**を**AIに適用**
- 問題点がある場合に**新法**を検討

- **共通点1**
  - **EUでいう「許容できないAI」「ハイリスクAI」**を野放しにはしない**姿勢**などが類似
    → EU・米国は相互に**情報交換と協力を推進**

- 米・EU**貿易技術評議会（TTC）**の「共同ロードマップ」
- **独禁・競争法、労働法などでも連携**

(3) EUと米国の共通点・相違点

- **共通点2**
  - AIビジネスにハードローとソフトローの組合せで対応。なぜ？
    - → **ハードローだけ**でも**ソフトローだけ**でも**うまくいかない**から

ハードローだけ	➡	ハードローだけで、 隙間なくAI対応は困難	➡	**困難**
ソフトローだけ	➡	現行のハードローが 適用される	➡	「ソフトローだけ」 は**あり得ない**

- **共通点3**
  - EU・米国はともに**現行法を存続**させて、**新法と共存**させる
  - **欧米**の**行政**は**共に**、**現行法**が**AIに適用されることを意識**し、**現行法をAIにどう適合させるか**を**検討・公表**している

共通点3（欧米は共に、現行法を存続させて新法と共存させる）の説明

- **米国**では（**あくまで例**） 

連邦取引委員会（FTC）：**消費者保護・雇用・住居・金融**の文脈に影響

- **2020年**、**消費者保護**のため、AIの利用についての**姿勢を示した**
  - 透明性、説明可能性、公平性、健全性、アカウンタビリティを求めた
- **2021年**、**次の法律**のAIへの**適用方針を公表**（原文はより詳細）。**摘発事例**あり
  - FTC法：不公正で詐欺的な行為の禁止 → **バイアスのあるAIなど**が**規制対象**に
  - 公正信用報告法（FCRA）：**雇用・住居確保・借入れ・保険契約など**を**AIが拒否** → **規制**
  - 信用機会平等法（ECOA）：**人種・性別・年齢など**に基づく**AIによる貸付差別** → **禁止**

雇用・労働の文脈：**雇用機会均等委員会（EEOC）**

- **2021年**、**雇用決定AI**の**市民権法遵守**のための**調査イニシアティブ開始**
- **2022年**、AI**雇用差別**が**障害をもつアメリカ人法（ADA）**違反となり得ると表明

金融の文脈

- **2018年**、**証券取引委員会（SEC）**、**投資顧問業法**をロボアドバイザーに適用
- **2021年**、**連邦準備制度理事会（FRB）など5機関**、AIにFCRA・ECOA・公正住宅法（FHA）などの適用があるとし、**AIの利用に関する幅広い情報報告を金融機関に要求**

消費者製品の文脈

- **2021年**、**AI組込み消費者製品の規制権限あり**と公表

ディープフェイクの文脈

- **2020～21年**、**連邦議会**が**国防総省（DoD）**に**ディープフェイクの調査を義務付ける法律等**を可決

共通点3（欧米は共に、現行法を存続させて新法と共存させる）の説明

- **EU**では（**あくまで例**） 

EUのAI規則案自体が、**現行法を検討した結果できたもの**
- **安全に関するAI** → 機械・船舶・医療機器などの**安全に関するEU法令**の適用あり
  → その改正もAI規則案に含まれている
- **GDPR**とも関連

EUでは**他にもAIハードロー**を作る動き → **現行法では足りない**という意識
- **AIの民事責任**について → **AI民事責任指令案**
- **AI学習を含むデータ利活用**について → **データ法案、データガバナンス法**

加盟国レベルでも**AIハードロー**を適用する、又は作る動きがある。**例示するだけでも**：
- **警察**の**監視AIによる個人情報収集・処理**が**違憲**（情報自己決定権の侵害）であるとする**ドイツ**憲法裁判所判決（2023年）
  - **テロ対策に関わる**。EU加盟国でも、おそらく**同様に扱う国とそうでない国がある。そこにも現行法が大きく影響**する
- **自動運転**を適法とするための加盟国法の制定・改正や行政当局の動き
  - ドイツでは2017年・22年にレベル3及び4の自動運転を適法化
  - フランスでは2017年の時点で自動運転における個人情報の取扱いについて当局がガイダンスを公表　など

AI商品・サービスに関して、欧米が法規制で対応しようとするもう一つの理由

- それは、**安全保障上の目的**
  1. **投資審査**と**輸出規制**による**ビッグデータや技術の流出**の**抑止**
  2. **AIコンテンツによる情報操作**により**国の安全保障を脅かすこと**を**禁止**する規制・措置の導入
     - ロシアのウクライナ侵攻時におけるゼレンスキー大統領のディープフェイクがウクライナ国民に虚偽の呼びかけをしたことなどが想起される
  3. 事業者が収集した消費者データの**権威主義的国家**への移転や、それらの国家での処理・保存、あるいは、それらの国々が**消費者データにアクセスすることを許さない**こと
  4. **権威主義的国家で作られる諜報機能のあるAI商品**の**自国市場への流入の阻止**も目的に含まれると考えられる

➡ **全て、日本でも重要**

(4) 小括

- **EUのAI規則案はリスクベースアプローチ**
  - **EUの価値観に背くビジネスはできない・しづらい**
  - 一方で、法制の明確化は**イノベーションを強化する**

- **米国**では、**連邦法**のみならず**州法**も**AIビジネスを規制**
  - **そこで守られる価値**は、**EUの価値観とほぼ同じ**

- **米欧**は、**AIビジネス**に**ハードロー**と**ソフトロー**の**組合せ**で対応する姿勢であり、互いに**情報交換や協働を推進**
  - **ハードロー**：**新法だけでなく、現行法**をAIにどう適合させるかを検討・公表している
  - **安全保障上の目的**でも**具体的な措置に向けて協働**

2.

中国のAI法制に関する動き

ソフトローからハードローの方向へ

- **2021年7月「信頼できる人工知能についての白書」**
  （中国情報通信研究院ほか）
  - **AIのリスク**（セキュリティ、ブラックボックス、バイアス、責任主体の不明確さ、プライバシー）を指摘。**よりよい道筋**とされるものを提示
- **2021年9月「新世代の人工知能倫理規範」**
  （中国科学技術部）
  - **目標**は**AI**を**常に人の制御下に置く**こと。基本的・具体的**倫理要件**を提示

- **2022年4月「人工知能白書2022」（中国情報通信研究院）**
  - AIガバナンスは**ソフトローとハードローのコンビネーション**の局面に入り、**ソフトローからハードローに移行**していると述べる

具体的なハードローの動き

- **インターネット情報サービス**の**アルゴリズムによるリコメンドに関する管理規定**（2022年3月施行）と
- **インターネット情報サービス**の**深層合成の管理規定**（2023年1月施行）
  - **リコメンド活動事業者**や**深層合成**（典型はディープフェイク）**サービス提供者**は、**多様な義務**を負う
    - 安全保障や公益を損わない
    - 違法・虚偽情報を送信しない
    - 合成映像には目立つ位置にマークを付ける
    - 顔や声などの生体情報の深層合成をする場合には、対象者に通知し、同意を得る
    - 世論を操作しない、など
  - **世論属性があり又は社会動員能力がある事業者**は**届出義務**を負う
    - リコメンド管理規定に基づき、アリババ、テンセントなどが届出をした
  - 義務の違反には、**制裁金、行政処分その他の法的責任**が課される
- **他の法律も影響**
  - ネットワーク安全法、データ安全法、個人情報保護法、インターネット情報サービス管理弁法　など

どう評価すべきか

- 一面では、**国民の利益**に資する。また、**安全保障**の方策でもある
  - たとえば、中国ではディープフェイク技術が**違法行為**（一例だが、ある人の顔を勝手に張り付けてセクシー動画を創り出すなど）にも利用される例が多い
  - **国家の安全保障や社会のための規制**という意識も働いている

- **だが、それだけか？**
  - **世論属性があり又は社会動員能力がある事業者**に**届出義務**
    - 被害者保護・安全保障だけならば、そのような義務は必要か？
  - 時限的なものではあるが、リコメンド管理規定の通達（通知）が公表され、5つの主要なタスクを掲げた。その中で、特に**「立入検査」**の意味とは？
    - 「2022年総合的なアルゴリズムガバナンスの特別措置の開始に関する通知」に、自己検証・是正、立入検査、アルゴリズムの情報提出の監視、事業者の責任、期限内の問題の是正が政府側のタスクとして定められている
  - 違反の場合のペナルティには**「治安管理処罰」**が含まれる

小括

- **中国**でのAIビジネスが**ハードロー規制を受ける部分は大きくなる**
  - 現状では少ないが、**ハードローの方向に舵を切った**のは明らか

- **先進民主主義国と似た法令**が、**違う運用をされる可能性**がある
  - **その姿勢**は、**既に施行された法令に現れている**

- 「**中国**であれば**ハードローがなく自由にAIビジネスをさせてくれる**」とは**言えない。状況判断が必要**
  - 仮に明示的な制限がなくても、**データへのガバメントアクセスのリスクなど**の検討を含めて、**ビジネスのステークホルダーの利益に関わる課題がないか**どうかについて**検討が必要**

3.

日本における
AI法制の検討状況

日本の現行法とAI

- AIに関する**現行法上の論点**の**議論自体**、**とても少ない**

日本で現行法が議論されてきた事項の例
（いずれも**一部の事項のみ**）

- **自動走行**
- **自律航行船**
- **金融**
- **AI医療機器**
- **リーガルテック**

AI関連で**優先順位が高いと想定される分野・項目を特定**して**現行法の検討が必要**。例えば

- **交通・建設**
- **金融**全般
- **エネルギー・環境**
- **農業**
- **災害対策**
- **介護**
- **医療**
- **労働**関係
- **教育**
- **通信**
- **スマートシティ**

欧米で議論がなくても、**日本のリスクの高い事項**は**検討が必要**

連合学習・秘密計算などのAI新手法のアウトプットと現行法（個人情報保護法に限らない）**との関係の整理も必要**

個人的な見解

1. 国民が信頼する法制度でないと、後で経済的損失が大きい

就活用ウェブサイト失敗事例や**トロント・スマートシティ失敗事例**などから学べば、

- **国民が信頼する法制度**に沿ってイノベーションを促進することが大切（**イノベーション促進**を**法制度の制定・改正**と**対立させてはいけない**）
- さもないと、**国民や社会**によって**AIビジネス**が**後でひっくり返される（既に事例多数）**
- **規制のない（ソフトローだけの）状態**は、**安全保障上も極めて脆弱**であり、ビジネスにとっても**大混乱のもと**

2. EU・米国に類似した法制度の方が使い勝手がよい

（国内外の**企業や国民、投資家にとって**）

- 類似していれば、**輸出や投資など**が**しやすい**
- 類似していれば、**外国企業や投資家**が**日本に参入しやすい**

3. AI関連で優先順位が高いと想定される分野・項目を特定して前ページの例示のような現行法の検討が必要

- その部分の**分析・対策**が**早急に必要**
- それを、AI企業にやらせようとすると、**各個別企業の負担と時間が甚大**に

企業としては今後どう対応すべきか？

- 少なくとも、**現行法**が**AI事業に適用され続ける**だろう。
- したがって、**ソフトローだけ**で**規制がない**などということは、**あり得ない**。
- 少なくとも、**必要な規制**は**新たに設定**する必要がある。

さもなくば、AI産業が成り立たない。

- **これらを前提**に、**日本のAI企業は少しづつ用意を始める必要**がある

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）

大阪大学招聘教授（社会技術共創研究センター）

アメリカ法曹協会（ABA）北東アジア委員会委員長

Eightでの名刺交換用QRコード

三部　裕幸

電話（直通）：03-5501-2276

Email: hiroyuki.sanbe@aplaw.jp