2023/05/26
第 2 回 AI 戦略会議用資料

法制度の観点を中心とした論点整理ペーパー（岡田）

■　リスクとそれに応じた規制手法の在り方

・　生成 AI に関して語られる論点の中には従来から提起されていた議論の延長線上にあるものも多い。何が「AI」や「『生成』AI」に特有の課題かを峻別し、既存の法制度・ガイドラインや体制で対処できるか否かを確認し、できない場合は対応を検討すべきである。不必要で過度な規制や政府による監視は好ましくない一方で、真に必要な場合であれば適切な規制が求められる。

・　リスクへの対応に対しては、ハード・ローとソフト・ローの二者択一の議論は生産性を欠いており、両者のメリットやデメリットを勘案しつつ、適切なバランスの下で効果的な規律の在り方を検討すべきである。ハード・ローであっても、適切な内容の規制であれば、個人の権利保護に加え、ビジネスの予見性を高める側面もあり、様々なステークホルダーにとってメリットとなり得るため、検討対象から排除すべきではない。一方で、変化が激しい分野では規制は陳腐化し易い、あるいは、イノベーションを阻害するという面もある。したがって、ソフト・ローの手法も活用し、技術の進化や用途の拡大に応じてタイムリーかつ柔軟にアップデートするという発想もやはり重要である。

・　仮に何らかの規制を導入する場合、対処すべきリスクの性質に応じて、以下のような観点を考慮する必要がある。
　①　既存法の守備範囲の領域なのか、AI 特別法を制定すべき領域なのか
　②　リスクベースアプローチを採る場合、何が「リスクの高い」AI なのか
　③　立場（開発者、提供者、利用者等）に応じた検討
　④　ルール・ベースと、プリンシプル・ベースのような発想をどう組み合わせるか
　⑤　単純な行為規制を超えた、事業者の主体的なガバナンスを促進する仕組み
　⑥　国際的なルールメイキング（規制手法、規格等）との整合性
　⑦　いかに実効性のあるエンフォースメントにより法遵守を担保するか（海外企業への域外適用や執行手法を含む）

・　あまりに抽象的・観念的な議論ではなく、技術面での正しい知識や事業者の行動原理を理解した上で、各論点につき具体的な政策効果を意識した、地に足のついた議論をする必要がある。例えば、「透明性」の論点を例にとっても、
　①　どのような利用場面において、どの程度の透明性を求めるかは、悩ましい問題である（例：営業秘密や悪用問題から、一般にアルゴリズム開示は困難）。
　②　「メード・ウィズ AI」といった表示義務についても、実効性をどう担保するの

か考える必要がある。見破るのは困難であり単にアングラ化を助長するだけではないか、様々な表現が混ざっていく過程でいずれ分離しトレースできなくなるのではないか、という問題意識。

■ 規制緩和の観点

・ AI と法制度をめぐっては、リスクに対応する規制という観点とは別に、新たなビジネスチャンスを活かす環境を整備するための規制緩和という観点も、より一層重要となる。AI 新時代への臨機応変な規制適応として、現行の規制緩和手続のスピードと使い勝手を向上させ、事業者が既存の規制に委縮せず新規事業にチャレンジできる環境を整備・発展させていくことも、政策立案に際して意識すべきである。

■ プライバシーの問題

・ 現行法が硬直的な規律となっていないか、という問題意識（AI 新時代において規制すべきものが規制されず、逆に規制緩和してもよい規制が残ったままとなっているのではないか。他方で個情法により対処すべき領域の線引きや、改正した場合の AI 以外への波及効果にも留意しつつ要検討）

例１）個人データの第三者提供において画一的に適用される本人同意原則（「個人データ」（データベース性）、「提供」（クラウド例外）、「委託」などの解釈操作や、「同意」概念の緩やかな解釈によって結論の妥当性を図ることの限界？）

例２）公開情報に要配慮個人情報が含まれてしまう場合の取得規制

例３）生成 AI のアウトプットに不正確な個人情報が含まれる場合における対処の必要性

・ プリンシプル・ベースに基づき、規制や執行の不備を埋めるとともに、事業者の自発的なガバナンスを促すことはできるか、という問題意識

例１）正確性の原則

例２）最小性の原則

例３）データ保護バイデフォルト、データ保護バイデザインの原則

例４）プライバシー影響評価

■ 知的財産権（特に著作権）の問題

・ 近時の一連の改正を経た著作権法の発想自体は、イノベーションと権利保護のバ

ランスの観点からも、原則として妥当なように思われる。それを前提として、以下のような点については要検討。

① 現行法が意図した政策効果を達成できているか、という問題意識（「機械学習天国」と言われながら、日本で AI 産業が後れる一方で逆に海外 AI 企業の発展を助長し、日本のコンテンツ産業が打撃を受けるだけ、という結果になっていないか）

② 濫用的な使用を防ぐという観点から、現行法の解釈としてガイドライン等で明確にすべき解釈問題はあるか（但し、最終的には司法判断の問題であり、位置づけの曖昧なガイドラインに頼りすぎることには課題も残る）

③ 個別の侵害・非侵害とは別の次元の解決手段として、コンテンツホルダーに対価還元できるようなフレームワークの導入の是非（但し、著作権法の守備範囲なのかという問題はある。また、既存の補償金制度における様々な課題や教訓もあり、このような手法がはたして適切なのか、慎重な検討が必要）