山本レポート：システム安全性向上―世界の最前線（7）

システム安全と法規制

国立大学法人 名古屋大学
大学院 情報学研究科
教授　山本 修一郎
博士（工学）

今回は、O'Sullivan と Thierer による監督官庁による規制と AI イノベーションについての解説に基づいて、システム安全と法規制の関係について考える。

AI開発の効果とリスク

こういうことを聖トマスアキナスが書いているそうだ。「もし、船長の最も高い目標が、船を守ることなら、永遠に船を港から出さないだろう」

同じことが AI の社会的な導入でも起きるのは間違いない。新たな問題が生まれるからといって新手法の導入を受け入れなければ、新しい AI がもたらす社会的な効果よりも悪い結果になってしまう。

医療画像診断では AI 技術の導入が進んでいる。医師の目では見過ごされる兆候が AI 診断によって摘出できる可能性がある。医師の見落としによって患者が死にいたるという悲劇的な事態を考慮すれば、患者の生命を守るために試験的な技術であっても導入を考慮すべきである。

AI によって新たな社会的リスクが生まれることも事実である。社会的リスクを防ぐためには監督官庁による監視が必要である。以下では、監督官庁による規制の在り方について考える。

規制方針

規制当局の方針には、寛大原則と警告原則の 2 つがある。

◆寛大原則
(permissive policy regime)

◆警告原則
(precautioning principle)

O' Sullivan と Thierer は、米国が AI 開発で成功することができたのは、規制当局が寛大原則による統治を進めたからだとしている。

O' Sullivan と Thierer は、いまのところ、このような AI 開発（AI Development）を米国が主導しているが、ロシアと中国も AI 技術の重要性を認識しており、自国企業に本格的な支援と資金投入を加速している。もし、米国が AI 開発の創造性の支援で遅れるようなことがあれば、AI 開発企業がより創造性を歓迎する国に米国から逃げ出すことになるだろう。

米国はどうすれば先進性を維持できるかについて、O' Sullivan と Thierer は、これまでの米国の成功理由は寛大方針による統治の継続を推奨している。

現在のところ、米国では、AI 技術を監督するような中央機関はなく、異なる当局が既成の規則を個別的に適用している。たとえば、National Highway Transportation Safety Administration (NHTSA) が自動運転車の取り締まりを担当している。この方法は、完全ではないが、規制を制限する効果がある。つまり、AI 開発の統制を包括的ではなく、個別的にとどめておくことで、創造性に対する規制を制限するわけである。

自動運転車

AI が未来社会をどのように、根本的に変革するかを考える典型的な例が自動運転である。無人自動車によって、安全性に対する重大な懸念事項も発生する。面倒な規制と寛大方針との間の緊張関係の例を考える上で自動運転は良い例である。

2017 年 10 月の調査では、米国民の半数以上が無人自動車に乗車することを拒否している。この理由は、自動運転を支えているソフトウェアを信用できないこと、したがって自動運転車が危険になるからである。この調査結果によれば、米国民は自動運転が道路安全性に良い影響を与えると信じていない。30％は交通事故死が増加すると信じている。

しかし、実際には人間による自動車運転では毎年大量の事故死が続いている。たとえば、2016 年に米国では、4 万人が交通事故死している。言い換えれば人間の運転者によって 100 人が毎日死亡している。

一方で、自動運転によって最大 90％の交通事故が削減できる可能

性があると指摘されている。規制上の懸念から無人自動車技術の導入が遅れることによる経費は、毎年必要のない数万人の交通事故死に相当することを意味している。しかし、交通事故の90％が削減できるという可能性にしても推測であって、確実に交通事故の90％を削減できる証拠があるわけではない。段階的な検証が必要である。

謙虚さと遠慮

間違った原則を選択することによる潜在的な経費を算出する必要がある。安全性の法制度化を急ぐのではなく、すべてのリスクを排除することのリスクについて考える必要がある。

O'Sullivan と Thierer らは「人工知能と公的規制」（https://bit.ly/2CqzQBp）で、規制当局がAI技術に対するイノベーションに取り組む規制方針を、以下のようにまとめている。

- 一般原則として、許可を必要としないイノベーションを明確化し、保護すること。
- 参入とイノベーションの障壁を識別して削除すること。
- 発言と説明の自由を保護すること。
- 第三者使用に伴う責任からの免除を維持・拡張すること。
- 課題解決に対して既存の規制と一般法（common law）に従うこと。
- 開発に対する競争反応と保険市場の登場を待機すること。
- 産業界に対して自己規制とベストプラクティスを推進すること。
- 教育と資格認定を推進するとともに、挑戦的課題の解決に向けた社会の成長を許容すること。
- 困難な問題に対して目的に応じた、限定的、法的な対策を採用する。
- 規制方針の判断が厳密な費用対効果分析に合格することを確認するために評価する。

これらの推奨方針を対象領域ごとに具体化する必要がある。たとえば、ソーシャルメディアやコンテンツ統合サービスについては責任の保護が規定されている。これに対して、自動運転に対するソフトウェア開発者の責任問題については議論が継続中である。

また、現在でもソフトウェアのアルゴリズムに欠陥があって、システムに致命的なエラーが生じた場合、消費者を保護するために法律が適用される。AIもソフトウェアであるから、既存の法律が適用されることになる。しかし、機械学習の場合、明確なアルゴリズムによって挙動が規定されるというわけではなく、判断結果がデータに依存するので、挙動をアルゴリズムのように明確に説明できない可能性がある。機械学習では、挙動が教師データに依存するので、教師データの十分性が問題になると思われる。しかし、どれだけの教師データがあれば十分なのかは、問題に依存するので一般的なことは言えない。

基本的に、AI自体は規制対象ではない。しかし、AIの適用によって殺人ロボットや社会的脅威を生むようなAIアプリケーションを作成してしまう可能性がある。したがって、規制当局は、潜在的な脅威をもたらす特定のAIアプリケーションを識別して、これらを監視する必要がある。今後、数多くのAIアプリケーションが開発されることを考えると、潜在的な安全性の脅威について監視するために、開発されたAIアプリケーションに潜在的な脅威がないことを保証する方法を標準化しておき、AIアプリケーションの安全性を保証する必要がある。AI開発自体を規制するのではなく、社会的に導入されるAIアプリケーションの安全性を保証する方法を明確化することが重要になる。

まとめ

上述したことをまとめると以下のとおりである。

- AI開発の創造性は国力の源泉である。
- AI開発の効果を国家レベルで経済的な視点から評価する必要がある。
- 過度な法規制がAIによるイノベーションを阻害する。
- 寛容的な規制の下でAIイノベーションを推進する必要がある。
- 包括的にAI開発を規制すれば、AI開発の創造性が失われる。
- AI開発の創造性を加速する法規制の考え方を整理する必要がある。
- AI開発の安全性を保証する方法が必要である。

【参考】
[1]Andrea O'Sullivan, Adam Thierer, Counterpoint: Regulators should allow the greatest space for AI innovation, November 2018 Communications of the ACM: Volume 61 Issue 12, December 2018

＜システム安全性のことなら下記へ＞
yamamotosui@icts.nagoya-u.ac.jp