【講演レポート】

当日寄せられたご質問と回答

独立行政法人情報処理推進機構　デジタル基盤センター長
AI セーフティ・インスティテュート 副所長・事務局長
平本　健二氏

Q：グローバルな AI 標準化作業の場では産業技術総合研究所（AIST）が積極的に活動していますが、AISI の活動との関係性や協業部分をお教えください。

A：AISI は 10 府省庁+5 つの独立行政法人と連携しており、AIST とも今後の関係性について頻繁に打合せを行っています。例えば、標準はそれだけではなかなか普及しないので、ツールや実証の機会、より実践的なガイドラインなどへのニーズへの対応等で協力し、日本としてワンチームでリソースを最大活用する方策を考えていきたいと思っています。
また、今回セミナーに参加され標準化に関心を持たれた方にも、ぜひ活動に参加していただきたいと思っています。標準化と AI セーフティは表裏一体で、AISI の活動は実務的なところに近いものなので、人材のボリュームゾーンを増やしていきたいと思っています。

Q：AI リスクと Computor/System のリスクに区別はありますか？

A：区別はほとんどないと思います。従来のコンピュータリスクと同様の対応が取れる部分は多くあります。一方で、AI の特殊性として、例えば生成画像で顔認証が通るか等の技術的要素はあるので、アドオンする部分はあると思います。
AISI 事務局が IPA に設置された理由の 1 つとして、IPA にすでにセキュリティセンターがあり、そこでの調査で AI に関する情報等も取り扱っていたということもあり、併任しているメンバーもいます。

Q：欧米日でリスクに対する考え方が違う事があるという説明がありましたが、ハーモナイズできていないこと自体のリスクは大きいのではないでしょうか？

A：各国とのハーモナイズはかなりできています。欧米はじめ各国と対話を重ねるなかで調整も行っているので、ソフト・ローかハード・ローかといった違いは若干あるものの、内容的には大きな差異はないのでリスクはほぼないと考えています。

Q：AI リスクの科学技術リスクも視野に入っていますか？

A：汎用 AI のリスク（暴走や技術的限界等）ということであれば、メディアからも多く問い合わせがありますが、現時点ではまだそこまでは視野に入っていません。文献調査等でリスク自体は把握していますが、具体的なアクションには至っていません。今は、まずは本当に基本的な部分について抑える必要があるので、米国も日本もリスクマネジメントにフォーカスしてガイドライン等を策定しています。将来的には、対応が必要だという認識はあります。

Q：日本では AI によって雇用が奪われるリスクについてあまり議論がなされていないという話がありましたが、なぜ日本ではあまり議論されていないのでしょうか。

A：EU 等は失業率が非常に高いため、それに直結する形で AI による雇用リスクが語られています。一方で、日本はすでに労働力不足に悩まされており、単純作業等は AI に担ってもらう必要があるといった話も出ています。現在の日本の失業率では、大量失業によって社会不安に陥るという状況ではないので、それよりも会社の機密情報を生成 AI に入れて漏えいしたり AI の誤情報により判断を誤るといった基本的なリスクへの対処が議論されています。

Q：例えば、自社内で AI にデータを学習させてそれを自社内で活用する場合などにおいて、一般事業者が AI 利用者だけでなく AI 提供者としても規制を受ける可能性はあるでしょうか。

A：現段階では、そもそも規制が必要かどうかという議論を行っているので、その先の具体的な部分までは議論されていません。一般的には、法律で規制する場合もありますが、第三者認証や自己点検の際のガイドラインやチェックリストを自社内で使用して自主的に確認するということも当然ありえます。また AI 原則には立場に関わらず人間の倫理としての対応のあり方が書かれているので、それらを参考に適応していくことが望ましいと思います。

Q：ソフト・ローで業界ガイドラインを定めた場合、遵守しない企業に対しては指導や警告が必要になると思いますが、AISI が企業に指導を出すスキームになるのでしょうか？あるいは現行法での所轄省庁が行うことになるのでしょうか？

A：基本的に、AISI が何らかについて指導することは想定していません。警告したり規制をすることはこれまでの業法の中で所管省庁が対応し、AISI は事例収集の過程で新たなリスク等が想定された際にチェックリストに反映させるなど情報の取りまとめを行う役割になります。
また、認定に関する質問も多くいただきますが、現在は、認定するとすればプロダクトに対してなのか組織なのか、自己認定か第三者によるものなのかといった議論を行おうとしている段階です。さらに認定に関しては賛否両論あるので、企業の方のご意見や規制の検討状況をもとに考えていくことになると思います。

本内容は、2024 年 7 月 22 日に開催された JIPDEC セミナー「AI 規制について　欧米の動向と日本の状況」での主なご質問と回答を取りまとめたものです。