『AIリスク教本』

日本IBM AI倫理チーム（著）

SBクリエイティブ(2023/12/15)
2,420円

BOOK REVIEW

【感想】

IBM内のAIガバナンスを司るAI倫理委員会に所属するAI倫理チームがまとめた書籍。メンバーはサービス、製造、製品開発、法務等、様々なバックグラウンドを持つ人材で構成されている。IBMは早くからWatsonを展開する等、社外へのAIサービスの提供経験が豊富なAIを積極的に活用してきた企業です。本書は、サービス提供の経験だけでなく、社内外の様々なプロジェクトから得た知見も総合して執筆されています。

本書を読んで、AIを活用する上でのリスクについて大枠からかなり細部まで学べたと感じました。AIを開発する企業はもちろんのこと、活用するだけの多くの中小企業においても、自社が気づいていないだけで多くのリスクが存在します。例えば、コンサルティングをする際、顧客情報をもとにAIからアイデアを得る場合、そのAIにインプットした情報が再学習に活用されるか否かは非常に重要です。もし再学習に活用される場合、顧客情報がAIに取り込まれてしまいます。AIの性質上、一度取り込まれた情報を消すことは不可能です。どのように活用され、どのように公開されるかも全く予測できません。そのため、ある日突然、別のAI利用者に顧客情報が世界中で開示されてしまう可能性もあります。この場合、機密情報を適切に保護していないこととなり、守秘義務違反という法的問題及び信用失墜という社会的問題にもなりかねません。利用するAIがどのような性質のものか、どのように活用すべきか、利用目的に応じてしっかり考慮しなければいけないと改めて思いました。

【以下、引用】

AIリスクは2階建て　法と社会の目が監視

AIリスクは①合法性のレベルのリスクと②社会的受容性のレベルのリスクの大きく2つに分かれます。AIを利用する企業は、行動が法律に違反してしまうリスクに加えて、たとえ法律違反でなくても行動が社会的に受容されないリスクにも配慮しなければなりません。

…

1階部分にあたる合法性のレベルは、AIの共同が法律やそれに類する規制や公的なガイドラインといった「明文化されたルール」に違反することで生じるリスクです。例えば、AIを使用して外部向けに作成した書類に特定の個人を識別できる情報が含まれており、それを公表した結果、プライバシー侵害を問われる、といったケースがそうです。

…

2階部分にあたる社会的受容性のレベルは、法律違反でなくても社会的道徳に反してしまい、その結果として信用を失うリスクです。これは主になにかしらの意味で個人や団体などに損害や、強い不快感、誤解と言った精神的な苦痛を与えてしまう場合と、そのような問題の存在や、その疑いが広く世間に拡散される場合が考えられます。