

第2回 AI 社会実装ガイド・ワーキンググループ 議事概要

2020年9月3日 9:30-11:30

- 用語や対象の定義・想定について、認識に齟齬が生じないようにするべき
 - ガイドにおいて、「AI」とはなにを指しているのか。どのような想定・シチュエーションなのかを明示しておく必要がある。
 - 会社における、「AI ガバナンス」と「DX ガバナンス」をどのような関係とするか。DX に関する検討は多くの企業で進んでいる。AI ガバナンスの構築が転用できる要素がある。
- 導入側となる企業を想定し、実運用における論点を把握し、対応をしておくべき
 - ガイドの活用において、導入企業である各社のポリシーとの関係をどう定義するか。各社のポリシーがなかった場合、AI 原則がそのまま適用されてしまうのか。
 - 実際にガイドを適用する企業が、ひとつの組織体だけで AI に関連するサービスを開発するだけでなく、複数企業が開発・運用するというケースも想定すべきではないか。リスクオーナーが誰なのかという観点になる。
 - 日本企業の特徴として、現場、コーポレート、内部監査という部門がある。ここで、責任を第2線としてしまうことが多い。PoC 担当チームが意思決定に入ると記載されているが、マネジメントレイヤがリスクの高い段階ではサポートしていくべき、との指摘があってもよい。
- 運用におけるリスクマネジメントを、どのように提示していくか
 - ガイドにおける「リスク」とはなにか。プロセスのなかでリスクを最小化するという考え方が必要。運用保守をするなかで、プロセスとしてリスクを最小化していくことが不可避ではないか。
 - 運用のリスクマネジメントは重要。運用の仕方として、走りながらリスクアセスメントするというアプローチは危険である。試しながら品質を上げていくなれば、最初の人に伴走するとか、ものの作り方をリスクベースで変えていく、最初は慎重にやっていくと良い、ということを記述するとよい。
 - リスクとは、問題が生じた際のハザードの大きさと、発生可能性をかけたものである。ハザードは人間への害と考える。最終的なリスクはなにかと考えると、プライバシーやセキュリティである。それを防ぐツールとして、AI ガバナンスやリテラシーが。本検討は、AI というツールから見ているという認識である。
- リスクオーナーシップをどのように記述していくか
 - AI の導入においては、企業によってレベル感の違いがあるはずである。事業規模や重要性によって扱いは違う。2、3 パターンで分けてはどうか。例えば人間が介在するのであれば、そこにチェック機能が生まれる。
 - 会社にまたがるリスクの分配の問題がおきてくる。ベンダに開発を任せた場合、例えばそれが小さなスタートアップだとしても、ガバナンスを求めないといけなくなってしまう。

- リスクレベルによって変わるというのもその通り。社内体制で細かく書かれているものは、リスク評価のあたりから、開発体制の重さにあわせていけるとよい。
- 社内体制の構築については、AI 導入者・運用者、開発・実装・運用でステークホルダーが多くなか会話をして進めていく。認識を一致させる必要があると書いてあるが、その際に参考になる具体的な記載があってもよいのではないか。
- リスクオーナーシップは重要と認識しているが、産総研のガイドラインには記載されていない。協調するようにと記載することは重要。

● **ガイドラインでは、データガバナンスに関する記述が中核になるのではないか**

- AI を機械学習ベースのもと仮に定義するとすれば、それはデータの品質をコントロールすることに限りなく近い。データに関する記述を書くべきではないか。
- ガイドラインの記述の大半はデータに関するものになるのではないか。
- データに関する記述は難しい。産総研のガイドラインでは細かく言及していない。「データ」という言葉が独り歩きしてしまうので、製品ベースできちんとリスクアプローチをすることとしている。

● **企業がガイドラインを活用するインセンティブを高める仕掛けが必要である**

- 企業がガイドラインを活用するインセンティブを高めるためには、こうしたルールを遵守することで、良かったとか、沿っていないために大変なことになったという、実例を示すとよいのではないか。
- ガバナンスイノベーションでは、ガイドラインへのコミットをどう促すかについて考えている。規制を破った際に即座に罰則となるとコミットされないものになる。一方で、コミットをしていなくても、結果として損害があれば刑事罰がかかるとなる。しかし、事前にコミットをしていれば罰則が軽減される、という形でないといけないと思っている。事後的な調査の原因究明に協力する等で緩和をしたり、コミットのあるうえで、事前に想定できなかった事案は致し方なしとするなどが考えられる。

● **読み手の受け取り方について、どこまで考慮ができるか**

- 本領域では、IT 系スタートアップと、これまでの安全安心を大事にしてきたような大企業では、読み方が変わってくる。走りながらリスクを最小化しようとしたとき、スタートアップはほんとうにリスクのあるものをローンチしてしまう。なにかイメージが湧くような事例をもとに一般論を提示しなければ、読み手によって大きく受け取り方が変わる。