資料1

AI制度研究会発表資料

株式会社ABEJA　法務チーム　古川直裕

2024年9月10日

デジタルプラットフォーム事業

ABEJA Platformを核に、「トランスフォーメーション領域」で顧客のDXを推進し、
「オペレーション領域」で様々なシステムを汎用的な仕組み・サービスとして提供するデジタルプラットフォーム事業を展開

ABEJA PLATFORM

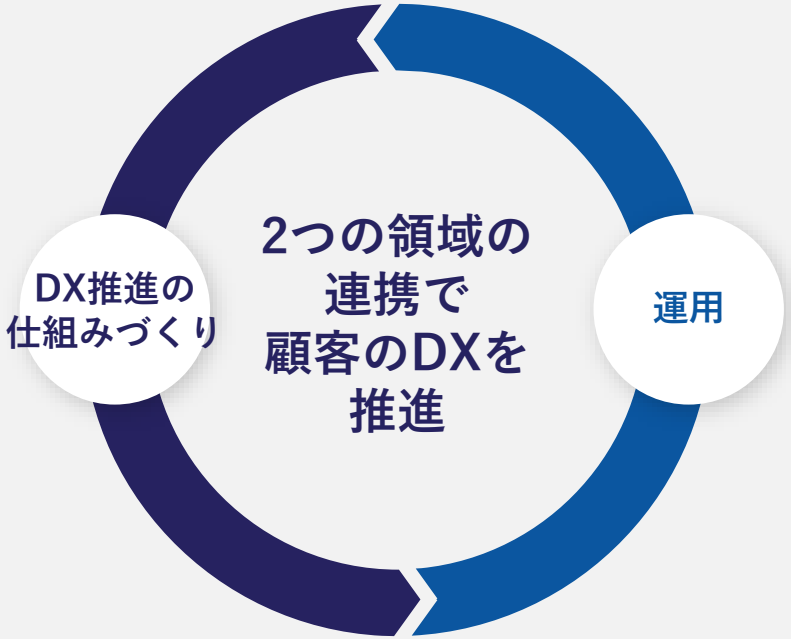
DXの実行に必要な、データの生成・収集・加工・分析、AIモデリングまでの
プロセスを提供し、継続的、安定的な運用を行う、ソフトウェア群

トランスフォーメーション領域

企業のDXニーズに対応した
プロフェッショナルサービスを提供

- DX推進に向けたコンサルティング
- ビジネスプロセスにABEJA Platformを導入、AIシステムの構築
- DXを推進する人材育成

フロー収益



オペレーション領域

ABEJA Platformを利用して
顧客が業務推進

- 店舗の動線分析システム
- 来店者推定システム
- 画像判定システム
- 属性推定システム　など

ストック収益

発表者について

- 3つの業務を担当
  AI関係の契約処理、法律相談といった法務業務を担当
  社内のAIリスクマネジメント業務を担当
  AIリスクマネジメントコンサルティングを担当
- Global Partnership on AI専門会員
- 日本ディープラーニング協会人材育成委員会G部会委員
- AI法研究会設立者・代表
- AIのリスクに関する書籍多数

AIのリスクの捉え方

- ユースケースから離れてリスクを考えることはできない
- 例えば生成AIの誤情報というリスクも、その意味はユースケースに依存する
  例：映画レコメンドでの誤情報（「タイタニック 2」推薦）
  　　医療マニュアルでの誤情報
- 現在日本で導入が進んでいるのは、個別ユースケースを想定したLLMの導入などであり、ユースケースごとのリスク管理こそが重要

個別リスク対策のための法規制

- ユースケースごと、つまり個別法における規制が重要
  ソフトローと既存法の併用
- 個別法規制は、通常は「AI規制」の形をとらない
  例：採用における男女差別
  　　選挙における虚偽情報の流布
- EUのような禁止や一定の手法を強制するのは不適切

個別リスク規制のために

- 採用の雇用機会均等法など現行法でそれなりにそろっている
  → AIにも適用があるという当たり前のことを明確化する
  日本は規制がないという誤解にも対応できる
  おそらく日本の足りていないところ
- 結局重要なのは人の問題
- ユースケースごとのリスクを的確に把握する人が少ない
  例：誤情報の意味をユースケースごとに考える人が少ない
- リスク把握人材の育成とリスク検討実施例の公表

技術への規制

- 生成AI技術に対する規制の議論が存在している
  例：レッドチーミングの実施、ウォーターマーキングの実施
- 個別ユースケースごとの規制とは異なる技術規制の形になっている
- 根拠は汎用性、ただし汎用性のあるAIは以前から存在
  例：顔認識、翻訳
- 技術への規制は行うべきではなく、ユースケース規制で対応すべき
  技術進歩が速く、また対応方法もよく分かっていない
- よく見られる「大型の生成AI」への「一定の措置」の実施を求める考えは・・・

大規模モデルへの規制

- 一定規模（学習に必要なコンピューター資源やパラメータの数）以上の大規模なモデルだけを規制するというのは、大規模なモデルを開発・利活用するインセンティブを損なう
  例：規制がかからないように強引にギリギリに小さくする
- モデル効率化・小型化の要請は重要ではあるが、結局2017年頃からずっと言われてきており、実際にはモデルは大型化している現実
- 最先端に対する挑戦を阻害する

求める一定の措置

- 一定の措置の実施を求められても、実施事項が不明
  共同規制といっても・・・
- ウォーターマーキングやレッドチーミングのような標準や規格が決まっていない事項の実施を求められても、実施できない。
  また、そもそも実効性も不明。
- ノウハウがあるのは海外の大規模AI開発者くらい
- IT産業が下請け構造になっており、AI開発において中小の下請けが多い日本で、同じことを求められても実施できない
- ユースケースに応じ様々な方法によるリスク低減を探るのが現実的
- また、リスク制御に重要そうな手法の調査と標準化

情報開示による対応

- 基盤モデルに関する規制として情報開示が存在する
- 上流開発者による下流への情報提供（透明性）は重要だが、開示した情報をどう使うのか検討のないままの情報開示に関する考えが多い印象
- 例として、性能の開示など
  テスト用データにおける性能と個別ユーザーごとの現実環境での性能は異なる。また、テスト用データにおける性能を開示されてそれが現実的にどういう影響があるか分析できる生成AI利用者がいるのか？
- 学習用データの開示も・・・
- 重要なのは、テスト導入して影響を検討し、徐々に適用を広げていく
  安全な導入プロセスのプロトコル化
- もう一つはモデル間の競争

現状

- そもそも規制を議論するだけの日本における実情の把握ができているのか？
- できていないのなら、事実関係の把握に努めるべき
- 報告義務や国の調査権限に関する立法を行うべき
- 高度なAIに対する規制を行う前に、やるべきことはたくさんある。

その他

- 念のためアメリカの動向を紹介する
- アメリカは法規制に向かっているという誤情報が多いが、事実は異なる。法的義務が生じているのは報告義務のみ
- 以下に、アメリカでの実務担当者の声を紹介する
  「大統領令は法律ではない」
  「大統領令は各省庁に対して指示を与えており、各省庁はガイダンスなどを作っている」
  「ニューヨーク市の採用AIに関する法律はうまく動いていない」