データ主権を確保した生成AI活用の条件

生成AIは、汎用的な業務への活用からより付加価値の高い業務への応用を検討するフェーズに移った。このフェーズでは金融機関が保有する独自のデータを活用し、生成AIを特定の業務に最適化する必要がある。今後、学習データのデータ主権を確保した生成AIの活用が求められる。

最適化された生成AI活用へのニーズ

生成AIの存在が一般的になり、生成AIを手軽に利用できるAIサービスが登場している。ただし、金融ビジネスにおけるAI活用については、現状、情報収集や問い合わせチャットボット、会議の要約といった汎用性の高いスキルで処理できるタスクに限られている。

金融ビジネスの専門業務に生成AIを活用するには、金融機関が保有するデータを使い生成AIをその業務に最適化する必要がある。例えば、過去の顧客応対履歴を活用した営業支援、過去の取引データや自社のチェック基準を用いたコンプライアンスチェック、事務フローや手順を学習した事務支援などが対象となろう。

実際、金融機関が保有する営業秘密や個人情報を含むクローズドなデータを生成AIに活用するニーズが高まっており、生成AIを特定の業務に最適化する技術も進展している。

問われるデータ主権

ただし、金融機関のクローズドなデータを生成AIに活用する際には「データ主権」への懸念が生じる。データ主権とは、データを国内で確保し、自国の規制やルールのもとで、データの所有権やアクセス権、トレーサビリティなどの安全を確保する考え方である。生成AIが金融機関のデータを学習する際、データ保護のためのデータ主権の考え方を排除することはできない。

データ主権はデータを処理・保存する国や地域の法律に強く依存する。データ越境移転に関する規制が国や地域によって異なり、データの現地保管を義務付ける国も存在する。最近では経済安全保障やデジタル赤字などの観点からも自国でデータ管理体制を強化する動きがみられる。

生成AIの効果を最大限に引き出すためには、営業秘密や個人情報を含むデータのリスク管理が重要であり、生成AI時代ではそのデータ主権の重要性が今後さらに増すだろう。

データ主権を確保した生成AI活用に向けて

データ主権を確保しながら生成AIを活用するには、大きく3つの要件がある。

まず、データの管理と生成AIの学習・推論を日本国内に設置したデータセンター内で完結させる必要がある。日本の法律のもとで管理し、海外の法律・規制の影響を受けないようにするためである。また、生成AIで学習・推論するためには膨大なコンピューティングリソースが必要であり、日本国内のデータセンターにGPUなどのリソースを備えることが求められる。

つぎに、営業秘密や個人情報を含むデータを取り扱うために高度なガバナンスとセキュリティが求められる。もともと金融では、ガバナンスとセキュリティに関する要件が多く、監査対応も厳しい。そこに加えて生成AI固有のハルシネーションや著作権の問題等に対応する必要がある。また、ガバナンス・セキュリティといってもその範囲は広く、データセンター等の施設・電源に係るものから、ネットワーク、ハードウェア、OS、ミドルウェア、アプリケーション、データまで全体を統合したリスク管理が必要である。生成AIの活用においてこれらを運

NOTE

1) Retrieval-Augmented Generationの略。大規模言語モデル（LLM）によるテキスト生成に、外部情報の検索を組み合わせることで、回答精度を向上させる技術のこと。事実に基づかない情報を生成する現象（ハルシネーション）を抑制する効果などが期待されている。
2) サービス提供者などが自社データセンター内に専用のパブリッククラウドを設置し、自社統制下で運用する活用形態。
3) 総務省令和6年版情報通信白書 https://www.soumu.go.jp/johotsusintokei/whitepaper/r06.html

用するためには、高度なガバナンス体制が必須となる。

最後に、特定の業務に最適化された生成AIの構築環境が必要となる。金融機関の場合、日本の金融制度の理解や社内特有の業務フロー・ルール、顧客情報を学習・参照できる生成AIが必要である。

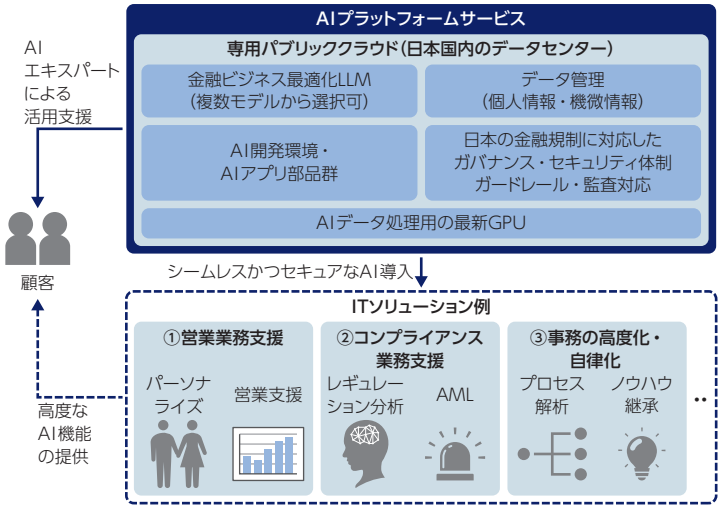
最近では、生成AIのモデルは多様化しており、モデルごとに得意な領域が異なる。生成AIを特定の業務へ最適化するRAG[1]などの手法に適したモデルも登場している。いくつかある生成AIの中から、高付加価値な業務を最適化するのに適した生成AIモデルを選択・利用することは重要な要件となる。

AIプラットフォームサービス

いまの生成AI活用事例では、機能とコンピューティングリソースが豊富な海外のパブリッククラウドサービスが利用されることが多い。しかし、前述の3つの要件を満たすためには、データセンターやGPUのハード面、ガバナンス・セキュリティやAIモデルの知見を有した人材確保が必要であり、それを個社で確保することは困難である。

このため、今後は新しい選択肢の一つとしてデータの置き場所がより明確な専用パブリッククラウド[2]を共同利用するAIプラットフォームサービスが台頭するのではないかと考える（図表）。このサービスでは、ハードウェア、ソフトウェアだけでなく、AIガバナンス・セキュリティへの対応・運用やAIエキスパートによる活用支援もサービスに含まれる。専用パブリッククラウドによるデータ主権の確保とパブリッククラウドの利便性を両立し、共同利用によってデータセンターやGPU等のコスト負担の軽減と高度な技術面・運用面でのAI活用ノウハウを享受できることがメリットだ。

図表　AIプラットフォームサービスイメージ図



（出所）野村総合研究所

総務省の調査によると、企業における生成AIの活用は、諸外国に比べると日本は大きく遅れている[3]。セキュリティリスクや著作権の侵害、人材不足等に対する懸念の声が大きい。このデータ主権を確保したAIプラットフォームサービスが提供されれば、これらの懸念が解消し、より高付加価値な業務への生成AIの活用が進む可能性がある。

Writer's Profile

村尾 将和 Masakazu Murao
金融プロセスイノベーション推進部
エキスパートシステムコンサルタント
専門はリテール金融
focus@nri.co.jp