特別研究

生成AIの活用とガバナンス上の留意点

2022年11月にChatGPTが公開されて以降、地域金融機関においても生成AIの積極的な活用が進められている。しかし生成AIからの出力内容の精度が低いことや、AIガバナンス態勢構築が取組み途上であるなど課題も多い。本稿では生成AIが業務効率化・高度化につながるための活用とガバナンス上の留意点を解説する。

KPMG／あずさ監査法人 金融統轄事業部 金融アドバイザリー事業部　ディレクター　秋場　良太

❶ 生成AIの急速な進歩

筆者は、生成AIは18世紀後半から始まった「産業革命」に匹敵するインパクトを現代にもたらすと考えている。OpenAI社が22年11月にChatGPT（注1）を公表して以降、GoogleやMeta等も生成AIの開発を進め、各社の生成AIの性能についても数年で劇的な進化を遂げている（図表1参照）。

そして、22～23年時点では主にテキスト情報のやり取りが主であったが、24年に入り画像や音声にも対応できるようになり、いわゆる「マルチモーダルAI（注2）」の開発が進んでいる。24年5月に公表された「GPT-4o」は、あたかも人間と会話しているように音声同士で人間とAIの間で会話ができるようになった（注3）。24年9月に公表された「OpenAI-o1」は、大規模自然言語モデルが苦手とされる数学・科学分野にも強い能力を有するといわれており、生成AIは僅か2年という短期間で従来の常識を覆す進化を遂げている。

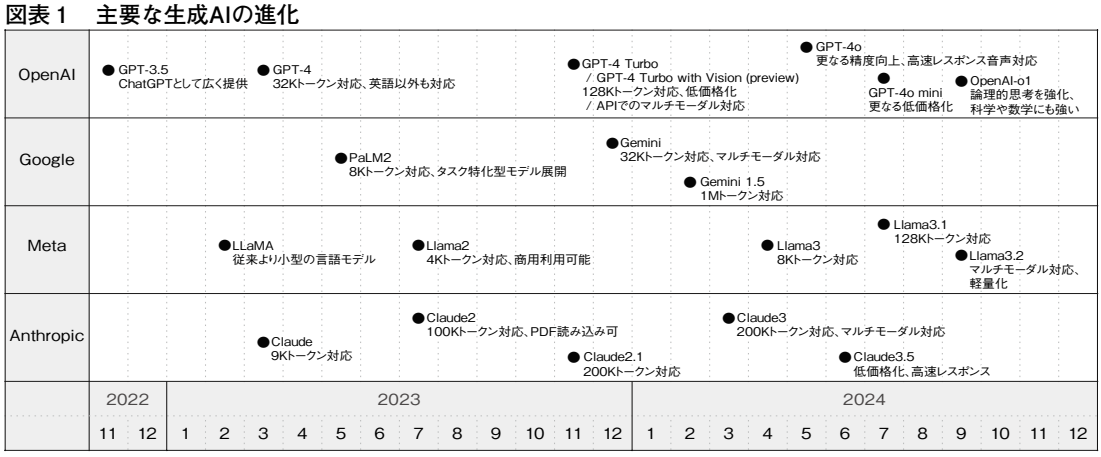
❷ 金融機関における生成AI活用の現在地

(1) 現状の概観

筆者が多くの金融機関に対する生成AIの導入に係る支援やAIガバナンス態勢構築の支援を通じて理解した、金融機関における生成AI活用の現状を述べる。

金融機関の多くは、最初の段階としてチャット形式

図表1　主要な生成AIの進化



出所：各社のホームページなどから筆者作成

の生成ＡＩをセキュアに活用できる環境を用意し、多くの社員によるチャット形式の生成ＡＩの利用を促す取組みである。これと同時並行的に、システム企画やＤＸ推進部署が全社的な旗振り役となって、想定される多くのユースケースから優先的に取り組むべきものを選定し、そのユースケースの実務適用を見据えて、ＰｏＣ（注4）の実施などを進めるというのが典型的である。

大手金融機関では、既に具体的なユースケースの洗い出しと優先順位付けを完了させて、実装に向けたＰｏＣを全社的に推進しているようである（一部ユースケースでは既に実務適用が完了しているものもある）。生成ＡＩは様々なリスクを内包するため、生成ＡＩの活用推進と同時並行的に、自社のＡＩガバナンス態勢の構築・高度化にも取り組んでいる。

一方、地域金融機関においては取組みにバラツキがあると感じている。大手金融機関と同様に有益なユースケースに対して実装に向けた取り組みを推進する機関と、全社的にチャット形式の生成ＡＩを利用できるようにしたものの個別のユースケースへの生成ＡＩ活用は取組み途上の機関、これから生成ＡＩの活用を検討する機関の３パターンに類型化される。ただし生成ＡＩに関するリスク・ガバナンス態勢構築に関しては、多くの地域金融機関が取組み途上であると筆者は理解している。各金融機関は具体的にどのようなユースケースを検討しているかについて、代表的な事例を紹介したい。

⑵　社内問い合わせ業務の効率化

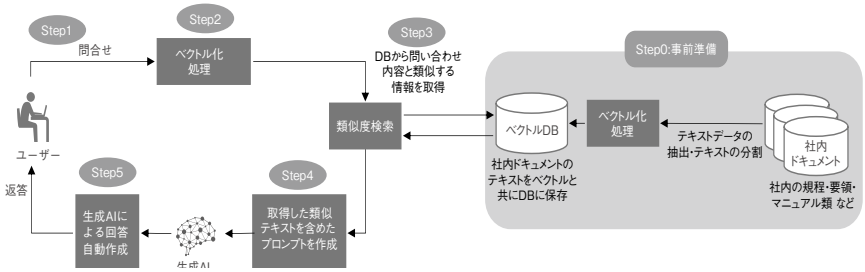
個別のユースケースを検討している多くの金融機関は、様々な部署で発生している社内問い合わせ業務に、生成ＡＩを活用して効率化を目指す取組みを行っている。

例えば営業店においてＡＭＬ関連の事務手続きの方法やルールを、本部担当者に問い合わせすることや、各部署が経理・財務部署の担当者に経理・財務に関する問い合わせをすること等が当てはまる。こうした社内で発生する問い合わせにおいて、直接担当者に問い合わせるのではなく、まずは生成ＡＩにチャット形式で問い合わせ、生成ＡＩが自動で回答を出力することで、多くの問い合わせを自動で処理することを目指すものである。各部署からの問い合わせに対応していた時間が大幅に削減されるため、本部職員は自らの本来業務に注力することができる。生成ＡＩは質問に対する回答を生成するのは得意であることや、本ユースケースは業務効率化の効果が高いことから、多くの金融機関内で検討が進んでいるテーマである。このユースケースを実現するためにはＲＡＧ（ＲｅｔｒｉｅｖａｌＡｕｇｍｅｎｔｅｄＧｅｎｅｒａｔｉｏｎ：検索拡張生成、「ラグ」と読む、以下ＲＡＧ）と呼ばれる技術を用いるのが一般的だ（次頁図表２参照）。

ＲＡＧは、事前準備として社内に存在する規程やマニュアル類をベクトル化と呼ばれるテキスト情報をＡＩでも理解可能な数値情報に変換する処理を実施した後、そのデータを「ベクトルＤＢ」と呼ばれるデータベースに格納しておく。そしてＳｔｅｐ１にて、ユーザーが聞きたいことをチャット画面に問い合わせ、Ｓｔｅｐ２としてその内容をベクトル化処理しておく。Ｓｔｅｐ３にて問い合わせ内容と類似した社内データを検索技術を用いて特定し、Ｓｔｅｐ

4でStep1の問い合わせ内容と特定された社内情報を含めたプロンプト（注5）を作成し、それを生成AIに入力する。最終段階として入力されたプロンプトに基づいて生成AIが回答を自動生成して、ユーザーがその内容を受け取る一連の仕組みである。

図表2　RAGの仕組み（簡略化した記載）



出所：著者作成

このRAGを用いることで、生成AIが知り得ない社内の情報に基づいた回答の生成が可能となるため、社内問い合わせ業務を効率化できる。

(2)　稟議書のドラフト作成

次に多いケースとしては稟議書のドラフト作成である。金融機関内には多くの稟議書が存在する。典型例としては融資稟議書であろう。こうした稟議書をRAGの仕組みを活用して一部分だけでも生成AIによるドラフト自動生成が実現できれば、稟議に関する業務が効率化されたり、若手職員がベテラン職員と同レベルの稟議書作成が実現できたりするのである（標準化の実現）。

(3)　文書レビューの自動化・効率化

最後に紹介する事例は、「文書レビューの自動化・効率化」である。

例えば営業部門やリスク管理部門などの部署は、システム投資に関する要望書をシステム部署に提出し、その内容をシステム部署の担当者がレビュー・内容確認を実施し、不足している観点の追記や修正等のやり取りを行う業務が存在する。似たようなやり取りとしては、営業店から審査部署に提出された融資稟議書に対し審査担当者がレビューを行う業務がある。こうした文書レビューについても、生成AIに事前にレビュー観点をプロンプトなどに記載しておくことでレビュー観点毎に自動で評価結果を出力することが可能となる。

金融機関内では、こうした文書のレビュー・内容確認・修正対応が多く発生しているため、効率化効果の大きい領域であると考えている。生成AIの活用を検討するにあたり、要約や翻訳、コンピュータソースコード自動生成などのユースケースは多くの金融機関で検討されているものの、「文書レビュー」について検討している金融機関は多くはないと認識している。このレビューを自動化・効率化することは生成AIの得意とする内容であるため、有望なユースケースの一つと評価している。なお、このユースケースにもRAGが用いられる。

❸　生成AI活用上の課題

金融機関において生成AIの活用やリスク・ガバナンス面における検討が進展するにつれ、課題も具体的に明らかになっている（次頁図表3参照）。

(1)　適切なカスタマイズをしないと「PoC倒れ」も

次頁図表3は、生成AIの

実務適用を進める上で必要な「活用方針」、「システム構成」、「データ」および「リスク・ガバナンス」の各段階で主な課題を「PoC・一部社内業務適用」と「本格展開」のフェーズ毎に整理した。

図表３　生成AIの活用やガバナンス面における主な課題

領域毎の主な課題	PoC・一部社内業務適用	本格展開
活用方針	・有望なユースケースの洗い出し、ユースケースの優先順位付け ・PoC実施のための方法・評価方法の検討 ・PoC実施後の実務適用判定	・生成AI活用を前提とした業務フローの変更とそれに伴う既存規程類の修正 ・本格展開に向けたシステム実装、導入済みの生成AIソリューションの活用
システム構成	・RAGの検索精度の向上、ベクトルDBの構成検討 ・活用する生成AIモデルの検討（アップデート対応含む）	・ハルシネーションやプロンプトインジェクションへの対応 ・ガードレール設計（入出力の監視と不適切な入出力の防止） ・生成AIモデルの追加学習やバージョン管理
データ	・必要なテキスト情報の収集・整理・体系化 ・文書化されていない暗黙知の形式知化 ・図表や画像の解読	・非構造化データも含めたデータガバナンス・データマネジメント構築とその運用設計 ・継続的なデータのアップデート
リスク・ガバナンス	・生成AIの利用のための社内利用ガイドラインの策定 ・セキュリティーやプライバシー、著作権への対応 ・国内外のAI規制・AIガイドラインの主要要件整理とその対応	・本格展開のためのリスク評価方法の確立 ・生成AIの利活用を過度に制限しない組織設計・ガバナンス態勢整備 ・生成AIのリスク評価・監視システムの実装

出所：著者作成

今から生成ＡＩの活用を検討していく金融機関にとっては、ユースケースの洗い出しやユースケースの優先順位付け、ＰｏＣテーマの選定などが課題になる。ＰｏＣテーマが定まったとしても、ＲＡＧを実施するためには社内ドキュメントの収集・整理・体系化が必要であり、この対応は非常に手間のかかる作業となる。無事にＰｏＣの実施までこぎ着けたとしても、いわゆる「ＰｏＣ倒れ」に陥っている金融機関が一定程度存在する。

その要因としては、「ＲＡＧの検索精度が低い」理由で実務展開に至らずＰｏＣ倒れになっているのである。現在生成ＡＩをクイックかつ安価に利用できるスターターキットや生成ＡＩパッケージ製品が存在している。

これらの製品は、社内のドキュメントの特性を踏まえたカスタマイズを実施しなくてもＲＡＧを活用したユースケースへの適用が実現できる。社内ドキュメントのチャンク分け（注6）やベクトル化方法の工夫、ベクトルＤＢを社内文書体系に沿った構成にする等のカスタマイズを実施しないでパッケージ製品を使った場合、生成ＡＩからの出力内容の精度や正確性が低いため、ＰｏＣ倒れになってしまう。

もちろん、社内ドキュメントのフォーマットが多種多様でテキスト情報だけでなく図表や画像が多用されたデータである場合でも正確性が低くなる場合があるが、マルチエージェント（注7）やマルチモーダルの技術を使えばある程度解決できるため、しっかりとしたカスタマイズが生成ＡＩの実務適用には必須である。

(2)　本格展開のためのシステム実装

ＰｏＣ実施後、生成ＡＩを実務に本格展開するフェーズでは、生成ＡＩ活用を前提とした業務フローの設計や、本格展開のためのシステム実装が必要と考えられる。

さらに、ハルシネーション（注8）やプロンプトインジェクション（注9）への対応や個人情報の入力の抑止のため、生成ＡＩシステムに対する入出力の監視と不適切な入出力の防止のためのガードレール設計も重要となる。

また生成ＡＩ活用は「データがあって始めて成立する」ため、非構造化データを含めたデータマネジメント態勢構築とその運用設計もポイントとなる。

(3) ガバナンス上の留意点

生成ＡＩ活用上の課題の最後として、生成ＡＩのリスク・ガバナンスの観点について説明する。生成ＡＩは既述の通りハルシネーションの問題やプロンプトインジェクション、個人情報漏洩などのリスクが存在する。そのため、多くの従業員が生成ＡＩを扱う状況にある場合（単純なチャット形式の生成ＡＩの利用も該当する）には、従業員向けのガイドラインを策定し、当該内容をしっかりと従業員に説明することが生成ＡＩガバナンスの第一歩であろう。

次に、生成ＡＩの個別ユースケースを本格展開する前までには、生成ＡＩシステムに対するリスク評価方法を確立の上、金融庁の「モデル・リスク管理に関する原則（注10）」（以下、金融庁原則）で述べられている３つの防衛線、モデル・ライフサイクル、リスクベース・アプローチという概念を理解しＡＩモデル・リスク管理のためのガバナンス態勢構築を進めることが望ましい。

ただし、金融庁原則で記載されている内容をそのまま地域金融機関に適用するのは、過度な対応になる懸念がある。さらに生成ＡＩを積極的に活用して効率化や高度化を促進したいものの、金融庁原則を鵜呑みにすると管理負荷が高いことと、機動的なモデルの変更やＲＡＧの各要素の改善が阻害される恐れもある。そのため「攻め」と「守り」に鑑みたバランスあるガバナンス態勢構築が肝要である。組織設計としては、ＡＩモデルを利用するモデルオーナー（モデルリスク管理上の１線）とそのリスクを統括するモデル・リスク管理上の２線、そして内部監査部による監査という３つの防衛線の組織設計は基本である。ただし１線と２線をどの部署・部門が担当し、各部門の役割分担については各金融機関の人的リソース等の実態を考慮した設計が求められる。

生成ＡＩのライフサイクル管理プロセスの構想や設計も必要である。ＡＩモデルは一般的に、ＡＩモデルの開発、使用前検証、使用後の継続モニタリングと再検証、ＡＩモデルの改善という一連のプロセスが存在する。そしてこのライフサイクル管理の対象はもちろんＡＩモデルが対象であるものの、生成ＡＩシステム内にあるどの機能をモデルと定義するのか、定義されたモデルに対して管理プロセスを適用するのであるが、生成ＡＩは技術的な進歩が著しく、ＲＡＧの仕組みも日々アップデートしていくものなので、これらのどの範囲を一連の管理プロセスにのせるのかは、ＡＩ活用が過度に制限されないような工夫をする必要がある。特に１線による継続モニタリングとして、どの程度の深度でリスク評価をするか。ハルシネーションなどの生成ＡＩ固有リスクに対し、どのように評価・モニタリングするか。そして１線による継続モニタリングに対し、２線による検証・承認をどのように行うのかの設計も重要である。現在、生成ＡＩに対する評価方法は確立された手法が存在する訳ではない。そのため生成ＡＩシステムが対象としている内容に応じて、リスクベース・アプローチの基本概念の下、あくまで生成ＡＩの積極的な活用が円滑に進むような管理プロセスを設計することが大切である。

❹ 真のＤＸ実現のために

大手金融機関や地域金融機関によらず、多くの生成ＡＩ

ユースケースが、既存の業務フローの一部効率化に留まっているのが現状である。それでも、生成ＡＩから獲得できる効果が大きいため、従来は実現が困難であった領域にも効率化は進むであろう。

しかし、真のＤＸがそれらの取組みで実現するかといえば「否」である。ＤＸはデジタル技術を用い既存の業務やビジネスの変革を行い、顧客起点の価値創出を実現することを意図している。この「真のＤＸ」実現のためには、筆者は３つのキーワードが要諦になると考えている。

１つ目のキーワードは「パーソナライズ」である。生成ＡＩは入力される情報に応じた個別の出力を行うことが可能である。マスリテール向けの営業においては従業員が個別に渉外活動を行うことが困難であったものの、生成ＡＩとデジタルチャネルを用いることで、個客のニーズに応じた接客や提案等のサービス提供が実現可能となるであろう。

２つ目は「ＣＸＯサポート」である。ＣＥＯやＣＩＯ、ＣＲＯなどのＣＸＯ機能に対して生成ＡＩを活用することで、多くの管理コストを削減すると同時に、ＣＸＯが本来担うべき機能に対し新たな提案やサポートを提供する活用方法である。

最後は「リアルタイムモニタリング」である。２線による統制・モニタリングや３線による監査は、多くの人的リソースが投入されているものの、特定の時点におけるモニタリングとなっているのが実態である。生成ＡＩを活用すればリアルタイムモニタリングが実現すると同時に、モニタリングの質も高いレベルで行えるであろう。

生成ＡＩは、今後大きなインパクトを産業界に与えるであろう。24年のノーベル物理学賞と化学賞ともにＡＩ研究家に送られることになった（注11）。ＡＩは科学の発展をも加速させているのである。今後数年間のＡＩに対する取組み深度によって、各金融機関の競争優位性は大きく変動することは、もはや自明であろう。

なお、本稿で述べた意見は筆者の個人的見解である

※　※　※

（注１）ＯｐｅｎＡＩ ＯｐＣｏ，ＬＬＣの商標登録である。

（注２）テキストや音声、画像、動画など複数の異なる種類のデータをまとめて扱うことができるＡＩ。

（注３）https://www.youtube.com/watch?v=DQacCB9tDaw

（注４）「Ｐｒｏｏｆ ｏｆ Ｃｏｎｃｅｐｔ」の略で、「概念実証」を意味する。新しい技術やシステム・サービスを導入する前段階で、その実現可能性を確認するための検証作業を指す。

（注５）ユーザーが生成ＡＩシステムのユーザーインターフェースを通じて入力する生成ＡＩに対する指示や質問。

（注６）ＲＡＧの参照元となるベクトルＤＢを作成する前に、予め社内テキストをＡＩが読み込めるように分割しておく処理。

（注７）複数の生成ＡＩが役割に応じて自動的に動作することで、従来よりも複雑なタスクをこなしたり、正確性の高い出力を実現するための技術。

（注８）生成ＡＩが事実とは異なる不正確な内容を出力する現象を指す。

（注９）巧みなプロンプトを入力することで、差別や倫理違反、犯罪につながる情報を出力できたり、生成ＡＩが学習済みの個人情報などの機密情報を抜き取ったりする行為。

（注10）https://www.fsa.go.jp/news/r3/ginkou/20211112/pdf_02.pdf

（注11）https://www.kva.se/en/prizes/nobel-prizes/