2023 年 10 月 27 日　全 14 頁

リテール金融での生成 AI 活用と規制動向

日進月歩の技術の活用事例が増える一方、規制の動きも活発化

金融調査部 研究員 森駿介
デジタルソリューション研究開発部 田中誠人

［要約］

- これまで登場しているリテール証券ビジネスに特徴的な生成 AI の活用事例を用途別に分類すると、大きく①営業員等向けの支援ツールとしての利用、②対話型 AI を顧客に直接提供、③コンプライアンスの用途としての利用、に大別できる。
- 米国や EU では、足元の生成 AI 台頭を踏まえる形で、広範なテクノロジーをカバーする規制枠組みが提案されており、リテール金融ビジネスに影響を及ぼす可能性がある。
- また、生成 AI 自体のモデル開発や学習を巡る動きも活発化している。AI モデルの業界・分野特化や国産化、企業固有の情報を活用した専門タスクの実行など、技術は日進月歩であり、活用方法を考える上でも正しい理解が必要である。

１．はじめに

2022 年 11 月の OpenAI 社による ChatGPT の提供開始以降、生成 AI は幅広い業種で注目されている。ビジネスへの応用の可能性を探る動きも活発であり、リテール金融業界も例外ではない。足元でもさらなる活用事例の登場や AI を巡る規制枠組みに係る議論のほか、生成 AI 自体の進化など、引き続き動きが活発となっている。以下では、これらの動向について概観しつつ、リテール金融業界への含意を探っていく。

なお、生成 AI の概要や得意・苦手な機能、2023 年 6 月時点での金融サービスにおける活用状況は「ChatGPT がリテール金融ビジネスに及ぼす影響」（大和総研レポート、2023 年 7 月 6 日付）で既に取り上げているため、併せて参照されたい。

２．リテール証券ビジネスでの生成 AI 活用の最近の動向

リテール証券ビジネスに特徴的な生成 AI の活用方法としては、①営業員やファイナンシャル・アドバイザー（FA）向けの支援ツールとしての利用、②顧客に対話型 AI を直接提供、③コンプライアンスの用途としての利用の三つが挙げられる（図表１）。

図表１　リテール証券ビジネスにおける生成 AI の主な活用事例

			営業員等向け支援	顧客への直接提供	コンプライアンス
米国	ﾓﾙｶﾞﾝ・ｽﾀﾝﾚｰ	2023年3月、GPT-4の試験導入を公表。膨大に蓄積された社内の調査・文書からFAが必要な情報を迅速に見つけ出すことを目標とする。同年9月には、全てのFAがアクセス可能になった。さらに、顧客との面談内容の自動要約・顧客へのメール生成ツールの試験導入も実施中。	✓		
米国	JP ﾓﾙｶﾞﾝ	2023年5月、顧客向けの対話型AIサービス提供を示唆する商標登録を申請。「有価証券・金融商品の選別を行うソフトウェアを組み込んだAIクラウド利用サービス」「顧客のニーズや仕様をもとに、有価証券・金融商品の分析・選別等を行うサービス」といった内容が記載されている。		✓	
米国	ﾓｰﾆﾝｸﾞｽﾀｰ	2023年5月、OpenAIサービスを活用したチャットボット「Mo」のベータ版を自社の複数サービスに搭載すると発表。同社が蓄積してきた投資調査データベースを参照し、IFAや個人投資家などのユーザーからの質問に回答。同年9月には、APIで提供することも発表。	✓	✓	
米国	Orion Advisor Solutions	TAMP（注）である同社は、2023年5月に、FA向けのCRMシステム「Redtail Speak」に、ChatGPTを組み込むと発表。顧客との間の過去のやり取りからメッセージ案を生成する機能を提供。FAは生成された案を採用もしくは再生成・編集することができる。	✓		
米国	Magnifi	フィンテック企業の同社は、FAを介さず取引する個人投資家向けに、対話形式で投資関連の情報を提供するサービスを開始。複数銘柄の株価指標の比較や金融政策の変更がユーザーのポートフォリオに与える影響などについて、文章の生成に加え、理解しやすい図表の表示も行う。		✓	
英国	Aveni	英フィンテック企業の同社は、AI技術を活用したリスク管理ツール「Aveni Detect」を提供。FAと顧客の会話やメール等でのやり取りをモニタリングし、利益相反の発生や不適切な助言などの特定を可能としている模様。2023年6月には、FA向け支援ツール「Aveni Assist」をローンチ。	✓		✓
中国	ｱﾝﾄｸﾞﾙｰﾌﾟ	2023年9月、金融分野に特化した大規模言語モデルに加え、当局から承認を得られ次第、ユーザーに市場分析やポートフォリオ診断、投資家教育などの情報提供を行うツール「支小宝2.0」をAlipayへ導入すると発表。さらに、金融の専門家向けの業務支援ツールも開発中と公表。	✓	✓	
日本	楽天証券	2023年7月、新たなAIチャットサービス「投資AIアシスタント（ベータ版）」の提供を開始。独自開発したAIモデル（特許取得）と、ChatGPTを組み合わせて開発。基本的な投資の知識からユーザーのレベルにあった投資方法、同社が作成したおすすめの記事を回答するサービス。		✓	
日本	400F	2023年5月、個人とお金の専門家をマッチングするサービス「オカネコ」に、ChatGPTを活用した新機能「AIおかねこ」を搭載。ユーザーの家計診断を踏まえたアドバイス生成に加え、ユーザーの質問（NISAやライフプランニングなど）に回答する機能を有している。		✓	
日本	MILIZE	2023年3月、ChatGPTを活用し、LINEでユーザーのお金の質問に回答するサービスを提供開始。営業員・IFA向けの支援ツールとして、顧客ごとにアドバイスや会話の入り口のネタなどをChatGPTを活用して生成するサービス「デジタルアドバイザー」の提供も検討している。	✓	✓	

（注）TAMP（Turnkey Asset Management Platform）は、FA やブローカー・ディーラー等に投資一任サービスなどの機能を提供するプラットフォーマーのこと。
（出所）各種報道・各社資料より大和総研作成

①　営業員等の支援ツール

生成 AI を用いた営業員や FA 向けの支援ツールの主な用途として、社内の専門知へのアクセスの容易化（ナレッジマネジメント）、顧客向けメール・チャットの文案生成、面談前後の顧客情報の整理、顧客との会話・面談内容の生成、などが挙げられる。FA を抱える証券業者に加えて、独立系 FA（IFA）等に投資一任プラットフォームを提供する TAMP（Turnkey Asset Management

Platform）やフィンテック企業など幅広い主体が、このような支援ツールの提供を試みている。

この中でも、先行事例としてモルガン・スタンレーの取り組みが挙げられる。一般に、GPT-4のような汎用的な大規模言語モデル（LLM：Large Language Model）は、必ずしも金融業界に特化した知識や社内独自の情報は学習していない。さらに、誤った情報を回答してしまう「幻覚（ハルシネーション）」の問題もある。そこで、同社はこれまで蓄積してきた約10万件のリサーチレポート・文書等をエンベディング（埋め込み）と呼ばれる手法によりデータベース化した。GPT-4にこれを参照させることで、自社のFAからの質問に迅速に回答するツール「AI @ Morgan Stanley Assistant」を構築している[1]。試験導入に参加したFAから寄せられた質問としては、同社のリサーチに関する内容（例：FFレートの見通し）や事務的な手続き（例：個人退職勘定（IRA）の開設方法）、特定の状況での対応方法（例：顧客の結婚準備に当たって、FAが手助けできる内容）が多かったようだ[2]。

回答精度の向上・維持のために、学習に用いる資料のスコアリング・選別、約400個の決まった質問を投げかけることによる回答精度の定期的な確認、回答を受け取ったFAによるフィードバックなども行っている模様である。

なお、当初は約16,000人のFAのうち数百名を対象とした試験導入だったものの、報道によれば、2023年9月には、全てのFAが同ツールへのアクセスが可能となった。さらに、同社は顧客との面談の内容を自動的に要約し、フォローアップのメールを生成する「Debrief」というツールの試験導入も行っているようだ[3]。

営業員等の支援ツール開発の目的として、「顧客との面談」以外の業務効率化を生成AIにより実現することで、FAにとって最も付加価値の高い「顧客との面談」の時間捻出を掲げる企業が多い。今後は、生成AIに期待されている顧客に合わせたカスタマイズを目的とした活用事例が広がるかが注目される。例えば、米国では、顧客向けにアドバイスすべき内容や優先すべき対応事項をFAに通知するシステム（ネクスト・ベスト・アクション）の活用が進んでいるが、顧客のポートフォリオのリスク分析や顧客とFAとの間のやり取りをもとに、次のアドバイス内容を生成する仕組みをさらに高度化できる可能性があるだろう。

②　顧客への直接提供

フィンテック企業を中心に、LLMが組み込まれたチャットボットを顧客が直接利用することを想定した事例が提供されている。例えば、個人とFP・IFA等との間のマッチングサービスを提供するフィンテック企業の400Fは、家計診断をもとにChatGPTが自動でアドバイスを生成したり、

[1] 汎用的な大規模言語モデルに外部のデータを参照させる手法の詳細については、本稿pp.12-13にて後述。
[2] WealthManagement.com “WealthStack Roundup: AI @ Morgan Stanley Assistant Now Live”（2023年9月21日付）
[3] CNBC “Morgan Stanley kicks off generative AI era on Wall Street with assistant for financial advisors”（2023年9月18日付）

ユーザーの質問に返答したりする機能を提供している。同社は、単にチャットボットにより情報提供するだけでなく、ユーザーからの質問を通じて関心や悩みなど顧客情報を収集する手段としても捉えているようだ[4]。

事例は少ないものの、汎用的な LLM を単に組み込むだけでなく、金融分野の専門的な学習を行ったモデルを活用したツールを顧客に提供する例も出てきている。例えば、2023 年 9 月に中国のアントグループは、金融分野に特化した LLM を開発したことを発表した。学習に当たって、通常のテキスト（1 兆トークン超[5]）や金融関連の資料（数千億トークン）を活用したという。また、金融分野に特化した LLM を搭載した対話型 AI「支小宝 2.0（Zhixiaobao 2.0)」について、当局からの承認が得られ次第、同社のスーパーアプリである Alipay に導入予定であることも発表した。同社によれば、市場分析やポートフォリオ診断、アセット・アロケーションの提案、投資家教育などの機能が提供できるようである[6]。

LLM が組み込まれたチャットボットを顧客向けに提供する事業者はフィンテック企業を中心に増加しているものの、例えば、NISA に関する質問をしても、一般 NISA とつみたて NISA の内容を混同するなど、回答精度が高くない事例も散見される。回答の正確性を確認する営業員等が間に入らない分、顧客に誤った情報を提供する蓋然性は高い。対話型 AI をもとに顧客へ直接情報提供する場合の規制枠組みが固まっていない中で、大手金融機関を中心にまずは社内向けの活用方法を探る事業者は多い。顧客が直接利用する対話型 AI サービスの今後を展望する上では、後述の規制動向に加えて、チャットボットから提供される情報や提案をユーザー側がどの程度受容し信頼するかという点が重要だろう。

③　コンプライアンス業務等の支援ツール

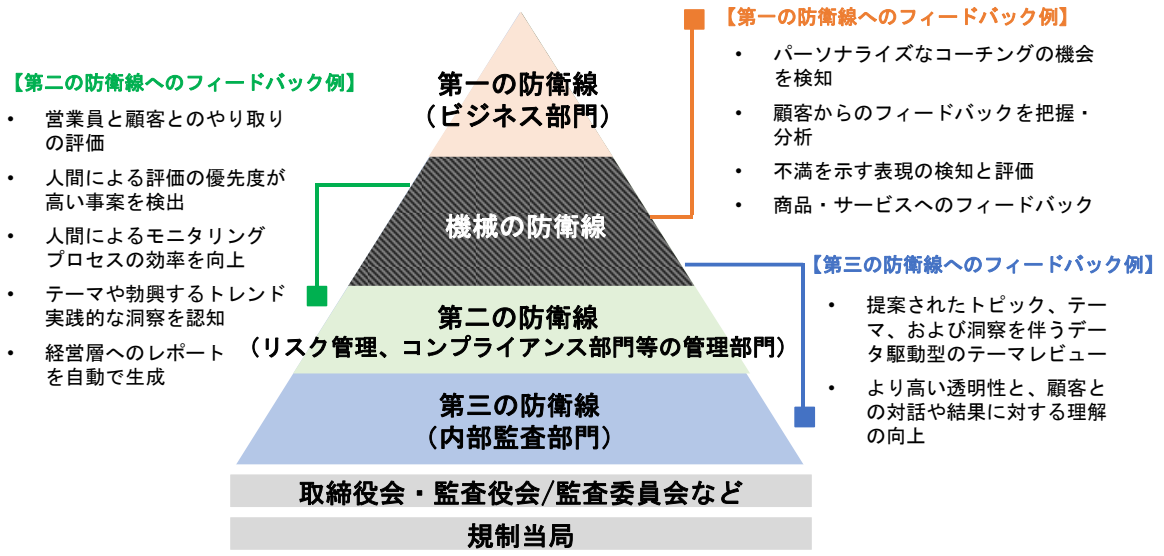
営業員等の販売態勢に関するリスク管理・コンプライアンス管理の観点で生成 AI を用いる例もある。例えば、英国のフィンテック企業である Aveni は、自然言語処理などの AI 技術を用いて、FA と顧客の間の対話をモニタリングするツール「Aveni Detect」を提供している。同ツールは、FA と顧客との会話やメール等での対話内容をトピックや説明・質問すべき項目などの観点から分類することで、利益相反の発生・不適切な助言などの事象やそのようなリスクに直面しやすい顧客を特定し、その情報をビジネス部門・リスク管理やコンプライアンス部門・内部監査部門などと連携することを目的としている。この仕組みについて同社は、内部統制の枠組みである「三つの防衛線（three lines of defence）[7]」になぞらえて、「機械の防衛線（machine

[4] 時事フィナンシャルソリューションズ「『チャット GPT』、金融ガイダンスに強み＝AI と人間が連携し初心者をサポート－400 F の中村 CEO」（2023 年 3 月 22 日付）
[5] トークンとは、単語や文字など意味を持つ単位のこと。
[6] Alizila“Ant Unveils Financial Large Language Model”（2023 年 9 月 11 日付）
[7] 「三つの防衛線」は、リスク管理に関するビジネス部門・管理部門・内部監査部門の機能の整理に用いられる考え方。金融機関がどの機能をどの防衛線の部門・部署が担うかを意識的に整理することを通じて、最適な態勢の構築に役立てるための概念である。

line of defence)」と呼んでいる（図表２）。

特に英国では、金融行為規制機構（FCA：Financial Conduct Authority）が 2023 年 7 月 31 日に導入した Consumer Duty により、金融サービスにおける消費者保護への要請が強まっている。これは、金融事業者が「リテール顧客に対する良いアウトカムをもたらすために行動しなければならない」（1.15、筆者訳（以下翻訳部分同））ことを理念に定める規制枠組みであり、金融サービスから顧客が得られるアウトカム（商品・サービスや価格・価値、顧客の理解、顧客へのサポート）を評価・検証・理解・証明することを求めている。金融事業者にとっては、このアウトカムの評価や証明のためのデータ管理が重要になるが、データポイントの一つとして顧客と FA との対話内容の分析やモニタリングに対するニーズは高まっているとみる向きもある[8]。このような、リテール金融における規制・コンプライアンス対応のためのテクノロジー利用（RegTech）の観点でも、生成 AI の活用可能性は大きいものと思われる。

図表２　AI 技術を用いた内部統制のイメージ



（出所）Chisimdi Nzotta “Why a ‘Machine Line of Defence’ is critical to meeting the FCA’s Consumer Duty”, Aveni Blog（2022 年 7 月 18 日付）を参考に大和総研作成

３．　AI への規制対応に関する議論と金融サービスへの影響

金融サービスでも生成 AI の利用が広がってきたことを受けて、欧米の規制当局からは、AI のリスクや今後の規制対応方針についての言及が散見される（図表３）。この中でリテール金融ビジネスへの影響が大きいとみられる米・SEC（証券取引委員会）の規制案の提案と EU で採択された AI 規則案について、以下の（１）・（２）で概観する。

[8] Chisimdi Nzotta “Why a ‘Machine Line of Defence’ is critical to meeting the FCA’s Consumer Duty”, Aveni Blog（2022 年 7 月 18 日付）

図表３　欧米の規制当局の最近の動向

米国	SEC	2023年7月、ブローカー・ディーラーや投資アドバイザーに対して、幅広いテクノロジーの利用による個人投資家とのやり取りで生じ得る利益相反への対応を義務付ける規則案を公表。
		2023年8月、ゲンスラー議長は、投資アドバイザーはアルゴリズムを用いるか否かに拘わらず、フィデューシャリー・デューティの定める忠実義務に従わなければならないと発言。同年10月には、AIモデルの寡占化が次の金融危機の原因になり得ると発言。
	FINRA	2023年5月、生成AI技術を使用する事業者は、生成された推奨行為が依然としてSECの「最善の利益規則（Reg BI）」の対象となることを認識する必要があると警告。
	CFPB	2023年6月、AIチャットボットに対する苦情が増加しており、顧客からの信頼低下のみならず、法令違反につながる可能性もあると警告するレポートを公表。
		2023年9月、貸し手がAI等をもとに信用供与を拒否する際に、その具体的かつ正確な理由を提供する法的要求に関するガイダンスを公表。
欧州	欧州議会	2023年6月、EU域内で流通するAIについて、リスク分類に応じた対応を要求するAI規則案の修正案を採択。詳細は、欧州委員会・欧州議会・欧州理事会で対話の上で早ければ年内に合意。
	ESMA	2023年8月、半期報告書にて生成AI活用に伴うリスクとして、①誤情報に伴う金融サービスへの信頼低下、②SNSを通じた相場操縦、③AI技術の提供主体の寡占化による依存リスクを指摘。
英国	FCA	2023年7月、チーフ・エグゼクティブのRathi氏は、生成AI利用によりアドバイス・ギャップ解消などイノベーションが期待できると発言。一方で、AIに伴う問題の多くは現行のアウトカムベースの規制枠組みで対応できるものの、問題が生じた際の責任の所在やAI利用に伴う社会的なリスク許容度について議論すべきと指摘。

（出所）各種資料より大和総研作成

（１）米国：SECによる「one-size-fits-all」な規制案

SECは、2023年7月26日に、ブローカー・ディーラー（以下、BD）や投資アドバイザーに対して、テクノロジーを用いた個人投資家とのやり取りで生じ得る利益相反への対応を要請する規制案を公表した[9]。もともと、ミーム株現象[10]の原因の一つとなった投資アプリでの画面表示やゲーミフィケーションのような、個人投資家の関心を過度に引く機能や画面表示などについてSECで規制の議論が進んでいた[11]。

しかし、今回の規制案が対象とするテクノロジーは、投資行動や結果を最適化・予測・案内・指示する技術であり、具体的には「AIや機械学習・深層学習アルゴリズム、ニューラルネットワーク、自然言語処理・LLM（GPT含む）、その他の時系列データやリアルタイムデータ、参照テーブル、相関マトリクスなどを活用する技術など」とされている。技術の進歩やコロナ禍におけるフィンテックの浸透を背景に、足元でさまざまなテクノロジーを応用した金融サービスの事例が増加していることを反映して、非常に幅広い要素が盛り込まれていることがうかがえる。

これらのテクノロジー利用によって、過剰取引や顧客のリスク許容度に見合わない取引などが促されることで、手数料の増加やパフォーマンスの悪化などの弊害が個人投資家に生じる可能性に対して、SECは懸念を示している。生じ得る利益相反の具体例として、過度な取引を促し得る画面表示や機能、事業者の利益を優先するアルゴリズムをもとにした推奨・アドバイスの

[9] SEC “Proposed Rule: Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers”（2023年7月26日付）
[10] ソーシャルメディア上のコミュニティで特定の銘柄が熱烈に注目され、短期的に乱高下した現象。
[11] 詳細は、鳥毛拓馬「SECによる株取引アプリの規制に関わる議論」大和総研レポート（2022年1月21日付）。

生成などが挙げられている。

そして、これらのテクノロジーを利用するBDや投資アドバイザーに対しては、利益相反が生じているか否かを評価させた上で、仮に顧客の利益よりもBD等の利益を優先している場合は、その利益相反を排除もしくは中立化することを義務付けている（図表４）。また、利益相反の有無や対応策の評価プロセスなどについて定めた社内規定の策定や年１回以上の社内規定・対応策のレビューを義務付けている。

もっとも、BDに対しては、既にSECが2019年6月に制定した「最善の利益規則（Reg BI：Regulation Best Interest）」において、リテール顧客に対する推奨に当たって、BDの利益を投資家の利益よりも優先させてはならないという義務が課せられている。BDが最善の利益のために行動したといえるか否かについては、顧客に投資推奨をする際に４つの義務（開示義務、注意義務、利益相反回避義務、コンプライアンス義務）を遵守しているかを事実と状況に基づいて客観的に判断される[12]。しかし、SECは、テクノロジーの急速な進展と金融業界での普及に加え、新たなテクノロジーの利用による利益相反の特定とその対処の難しさやテクノロジーの拡張性などから、現行の規制枠組みを強化する必要性があると主張している。特に、Reg BIなどに従って開示がなされたとしても、データセットの大きさやアルゴリズムの複雑性に伴い、その内容は冗長かつテクニカルとなり、投資家が開示内容を理解するのは困難と指摘している。

図表４　SEC規制案におけるブローカー・ディーラー等への要請

利益相反の排除・中立化
① 規制対象となるテクノロジーについて、投資家とのやり取りでの利用や潜在的な利用を評価し、これに伴う利益相反を特定
② 上記の利益相反によって、投資家よりも事業者の利益が優先されているかを判断
③ 投資家よりも事業者の利益が優先されている利益相反を排除もしくは中立化

社内規定（policies and procedures）の策定
① 投資家とのやり取りにおけるテクノロジーの利用を評価するプロセスの書面による説明
② 利用もしくは潜在的に利用され得るテクノロジーの特徴や利用により生じる利益相反の書面による説明
③ 特定された利益相反が、投資家よりも事業者の利益を優先する結果をもたらしているか否かを判断するプロセスの書面による説明
④ 投資家よりも事業者の利益を優先する結果をもたらすと判断された利益相反の影響を排除、もしくは中立化させる方法を決定するプロセスの書面による説明
⑤ 確立された社内規定とその実施の効果について、年1回以上のレビューおよびレビューの書面による文書化

（出所）SEC “Proposed Rule: Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers”（2023年7月26日付）より大和総研作成

なお、同規制案に対するパブリックコメントにおいて、金融業界からの反発の声が多く寄せられている。例えば、同規制案が規制対象とするテクノロジーや投資家とのやり取りの定義が広範すぎるといった指摘や、既存の規制との重複感があるとの指摘が少なくない。規制の適用により、サービス提供に伴うコンプライアンス・コストが高まり、各種サービスに対する投資家のアクセスが困難になるとの懸念も示されている。また、利益相反の排除・中立化に対応を限るの

[12] 詳細は、鳥毛拓馬「SECのブローカー・ディーラー規制の強化」大和総研レポート（2019年7月2日付）。

ではなく、顧客への開示により潜在的な利益相反への対応を許容することを求める声もある。このほか、各テクノロジーの利用によって生じ得るリスクに応じた規制を課すべきといった主張も見られる。

（２）EU：リスク分類に応じた対応を求めるAI規則案

EUでは、域内で信頼できるAIの利用環境を実現するための規制導入に向けた議論が進められており、金融業界を含め、幅広い業種に影響を及ぼすとみられている。2023年6月に欧州議会本会議において「AI規則」の修正案が採択された。本規則案は、リスクベース・アプローチを採用している。具体的には、AIシステムを①受容できないリスク、②ハイリスク、③限定的なリスク、④最小限のリスクの4つのリスクレベルに分類した上で、そのリスク程度に応じた規制を課している（図表５）。例えば、AIを用いた公的機関等によるソーシャルスコアリングや法執行を目的としたリアルタイムでのリモート生体識別システムは「①受容できないリスク」に分類されており、EUでの利用は禁止されている。

図表５　EUのAI規則案の概要

リスク	AIシステムの例	対応
受容できないリスク	・人々を操作して損害を与えるサブリミナル技術 ・子どもや身体・精神障害のある人の脆弱性の悪用 ・公的機関等によるソーシャルスコアリング ・法執行を目的としたリアルタイムでのリモート生体識別システム	禁止
ハイリスク	・既存のEU法に基づいて第三者適合性評価の対象となる製品等：医療機器、玩具、産業機械、昇降機など ・本規則案のAnnexⅢで定めるもの：生体識別や分類、重要インフラの維持管理、教育・職業訓練、雇用・業績評価、重要な民間サービス・公的サービスへのアクセス、法執行、移住・亡命・国境管理、司法・民主主義プロセスなど	一定要件と事前適合性評価の遵守の下で許可
限定的なリスク	相互にやり取りが生じるチャットボット、感情認識システム・生体認証の分類システム、コンテンツ生成AIなど	透明性の義務のもとで許可
最小限のリスク	その他	規制なし

（注１）本図表は欧州議会が2023年6月に採択した修正案をもとにしており、最終段階で内容が変更される可能性がある点には留意。
（注２）上記のほかに、AIシステム・基盤モデルの提供者にも規制を課している。
（出所）欧州議会　“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS”、欧州議会調査局（EPRS）　“Artificial intelligence act”より大和総研作成

本規則案の主要な規制対象となる「②ハイリスク」には、健康や安全、基本的人権などに深刻な影響を与え得るAIが含まれており、生体識別や重要なインフラの維持管理、教育・雇用、選挙における投票行動といった活用事例が列挙されている。この分類に当てはまるAIシステムに対しては、「リスク管理体制の整備」「データガバナンスの実施」「ログの保存」「技術書の作成・更新」「人による監視」「透明性の確保」「サイバーセキュリティへの対応」といった義務が課されている。また、当該AIシステムの提供者に対しては、品質管理システムの導入やCEマーク

の取得、AI システムの EU 管理下データベースへの事前登録などが義務付けられている。

ハイリスクに含まれ得る金融サービスとしては、生体認証を用いた本人確認のほか、民間サービスや公的サービスからの情報収集をもとにした信用評価や信用スコアを用いた AI レンディングが考えられる。また、欧州保険・企業年金監督機構（EIOPA）は、生命保険・医療保険における特定の AI 利用事例は、ハイリスクとみなされる可能性が高いとの認識を示している[13]。

「③限定的なリスク」には、対話型 AI やコンテンツ生成 AI などが含まれる。例えば、LLM を用いたチャットボットを顧客向けに提供している金融機関については、AI を使用している旨をユーザーに通知するなど透明性に関する義務を負う。

ハイリスクな AI システムの例に金融に関する事項が明示的に列挙されていないこともあり、同規則案において、どの金融サービスがいずれのリスク分類に含まれるか、詳細は不明確な部分も多い。今後は欧州委員会・欧州議会・欧州理事会の三者対話がなされた上で、年内の最終化が目指されている。

（３）小括

以上のように、米国・EU では、金融事業者の AI 利用に大きな影響を与え得る規制案が提案されている。もっとも、仔細に見ると、事業者へ義務付ける内容は異なる。米・SEC における規制案では、顧客よりも金融事業者の利益が優先し得る場合に、テクノロジーの複雑性などから開示のみでは不十分という判断のもと、利益相反の中立化や排除を求めている。一方、EU の場合は、テクノロジーのリスク分類を当局が行った上で、限定的なリスクならば、顧客に対する透明性に関する義務付けに留めている。ハイリスクの場合にリスク低減のための対策を義務付ける点は、SEC の規制案と同様であるものの、EU の規則案の方がリスク管理体制の整備や人による監視など、具体的な対応方法を定めている点で米国とは異なる。

また、共通の論点として、ハルシネーションへの対処や金融サービスでの AI 利用で問題が生じた際の責任の所在、AI 技術の寡占化に伴って生じる金融事業者の依存リスクと金融システムへの影響などが、各国の規制当局から指摘されている。一方で、過度な規制対応はイノベーションを阻害するとの見方も根強い。欧米の中でも、英国は既存の規制枠組みで生成 AI を取り扱う方針が今のところ示されており、金融面でもアドバイス・ギャップ解消やパーソナライズな製品・サービスの提供などのイノベーションを期待する見方が相対的に強く示されている[14]。

日本では、政府の「AI 戦略会議」にて新 AI 事業者ガイドラインの骨子案の策定の動きがある上に、金融業界での生成 AI 開発の利用に関するガイドライン策定に向けた民間の動きはあるものの、金融行政側での目立った動きは現段階では見られていない。もっとも、今後、海外の規制当局の動向を踏まえつつ、日本でも同様の議論が生じる可能性があり、注視すべきだろう。

---

[13] EIOPA “AI in the insurance sector industry adoption and regulatory developments”（2023 年 9 月 13 日付）

[14] 例えば、Nikhil Rathi “Our emerging regulatory approach to Big Tech and Artificial Intelligence”, FCA Website（2023 年 7 月 12 日付）を参照。

４．生成 AI 界隈の動向アップデート

ここまで見てきたような金融業界内での生成 AI を巡る動向だけでなく、生成 AI のモデル開発や学習を巡る動きも活発である。次に、これらの点について、足元の動きを整理したい。

モデル開発を巡る動き

生成 AI には、画像や動画を生成するものもあるが、金融業界内での動きが活発なのはテキスト生成 AI である。まず、テキスト生成 AI の基盤となる LLM の動きを紹介する。

最近の LLM のトレンドは、業界・分野特化と国産化である。一つ目のキーワードである業界・分野特化は、金融や医療等の特定業界やコーディングなど特定の分野に特化した LLM を指す。例えば、ChatGPT の Web サービスには、サービス上で Python コードを生成・実行したり、ファイルをアップロード・ダウンロードしたりできる「Advanced Data Analysis（旧 Code Interpreter)」という機能が追加され、コード実行やデータ分析が強化されている。一方で、ChatGPT などの LLM は極めて汎用的であり優秀なモデルであるが、モデルが巨大であるゆえにその学習や運用には膨大なリソースが必要となることや、特定の分野においては正答率を伸ばす余地があることが指摘されている。

そこで、業界・分野特化型の LLM を開発し、より効率的に運用できるようにして、法人需要を掘り起こす動きがある。例えば、ソフトバンクは独自の LLM の開発に取り組んでいるが、コールセンター業務への導入を念頭に、金融や医療などの専門知識を学習させた特化型として企業向けへの提供を目指すとしている[15]。同社は、LLM の研究開発などを目的とする新会社「SB Intuitions 株式会社」を設立しており、2023 年 8 月より本格的に稼働している[16]。また、米国の大手 IT 企業でも分野特化型の LLM を公開する動きがある。例えば、メタ・プラットフォームズ（旧フェイスブック）は自社開発の最新 LLM「Llama 2」の提供を 2023 年 7 月から開始している[17]が、8 月には Llama 2 をベースに、コーディングに特化した学習データを用いて訓練された「Code Llama」を公開した。Python、C++、Java など主要なプログラミング言語に対応しており、コード生成に関するタスクにおいてはトップレベルのパフォーマンスを示したとされる[18]。

LLM におけるもう一つのキーワードは国産化である。既存の LLM は英語を中心に学習されていることが多いため、他の言語では性能が多少なりとも低下してしまう問題がある。そこで進んでいるのが母国語に強い国産 LLM の開発である。例えば、前述のソフトバンクの LLM も日本語に特化したモデルであるほか、サイバーエージェント、東京工業大学・東北大学・富士通・理化学研究所、NTT、AI inside、NICT（情報通信研究機構)、NEC など大小さまざまな企業等が日本

[15] 日本経済新聞「ソフトバンクが生成 AI 開発　企業に提供、スパコンも整備」（2023 年 6 月 29 日付）
[16] ソフトバンク「国産の大規模言語モデル（LLM）の開発を行う 『SB Intuitions 株式会社』が本格的に稼働」（2023 年 8 月 4 日付）
[17] Meta “Meta and Microsoft Introduce the Next Generation of Llama”（2023 年 7 月 18 日付）
[18] Meta “Introducing Code Llama, a state-of-the-art large language model for coding”（2023 年 8 月 24 日付）

語 LLM の開発を発表している。NEC は、2023 年 7 月に独自の日本語 LLM を開発し、顧客のニーズに合わせて専用ハードウェアやソフトウェア、コンサルティングサービスなどを提供する「NEC Generative AI Service」を開始すると発表した[19]。同社の LLM の特徴は高い日本語能力やモデルの軽量さであり、顧客企業のデータによる個別チューニングも実施するとしている。また、業界横断の動きを見ると、2023 年 6 月、経団連は AI 活用促進に向けた政策提言の中で、日本が（生成 AI 等の）最先端の AI を独自に開発する能力を備えるべきとの提言を行っている[20]ほか、政府の「AI 戦略会議」で座長を務める松尾豊　東京大学大学院工学系研究科教授は日本経済新聞のインタビューにおいて、国内での生成 AI 開発に必要となる設備の整備を「政府がインフラ投資として支援すべきだ」と述べた[21]。インフラ投資という観点では、LLM の開発に必要な GPU サーバー（画像処理などの並列処理を得意とするチップを搭載したサーバー）が取り合いになっており、LLM を開発する国内企業の足かせとなる懸念がある。従って、必要なインフラを国内企業が確保できる環境の整備も重要なことである。ハードウェアとソフトウェアの両面から、LLM や生成 AI の国産化が進むことが期待される。

LLM 以外の動きとしては、生成 AI のマルチモーダル AI 化の動きが見られる。マルチモーダル AI とは、テキスト・画像・音声など、複数の種類のデータを一度に処理する AI のことである。このような AI のモデルは、大規模マルチモーダルモデル（LMM：Large Multimodal Model）などと呼ばれることがある。2023 年 9 月、OpenAI 社は従来のテキスト処理能力に加えて画像処理能力を備えた「GPT-4V（GPT-4 with vision）」を発表した[22]。これに伴い、ChatGPT に画像認識機能と音声会話機能が搭載され、画像の内容に関する会話や、音声でのコミュニケーションができるようになる[23]。また、同時期に、OpenAI 社は画像生成モデルの最新版「DALL·E 3」を発表しており、同年 10 月から ChatGPT でも利用可能になった[24]。ChatGPT の Web サービス上において、ユーザーはテキストでアイデアを伝えるだけで、「DALL·E 3」モデルを用いた高品質な画像を生成することができる。マルチモーダル AI 化によって、生成 AI の活用の幅が広がることが期待される。ビジネスへの応用においては、例えば、画像を含む資料（手順書など）を参照して回答を生成する、といったユースケースが考えられるだろう。

生成 AI の活用を巡る動き

生成 AI をビジネスでどう活用するかという観点について、活用のレベルごとに分けて紹介しよう。図表 6 は、生成 AI のビジネス活用の展開を、三つのレベルに分けて考察したものである。レベル 1 の「汎用タスクの自動化」は、ChatGPT などのサービスを企業で利用できる形態にして単独で利用することによって実現できるものだが、導入の先行事例が増えてきたことや、導入

[19] 日本電気「NEC、日本市場向け生成 AI を開発・提供開始」（2023 年 7 月 6 日付）
[20] 日本経済団体連合会「AI 活用による Society 5.0 for SDGs の実現に向けて」（2023 年 6 月 9 日付）
[21] 日本経済新聞「生成 AI 開発『GAFAM との競争、政府が支援を』 松尾豊氏」（2023 年 6 月 11 日付）
[22] OpenAI “ChatGPT can now see, hear, and speak”（2023 年 9 月 25 日付）
[23] ChatGPT Plus および ChatGPT Enterprise の契約ユーザー向けに順次展開される模様。
[24] OpenAI “DALL·E 3”（2023 年 10 月 18 日閲覧）

を支援するサービスが多数登場したことにより、より容易に実現できるようになっている。

MILIZE、AVILEN、日鉄ソリューションズなど複数の企業が、生成 AI の導入を支援するサービスを提供しており、このようなサービスを利用することで、自社にノウハウがなくても生成 AI を導入することができる[25]。大和総研も「ChatGPT 利用環境構築サービス」を提供しており、自社内や大和証券への導入実績を活かした ChatGPT 利用環境を提供するほか、導入に際して必要となる社内セキュリティ対策や、AI 倫理の策定に関するアドバイザリーも行う[26]。また、2023 年 8 月には、ChatGPT を開発・提供する OpenAI 社自らが企業向けサービス「ChatGPT Enterprise」の一般提供を開始することを発表した。同サービスの入力データは保護され、AI モデルの再学習に利用されないほか、管理者向けの管理コンソール（管理画面）や SSO（シングルサインオン：認証の仕組み）のサポート、使用状況の分析ダッシュボード、共有テンプレートなど、企業向けに適した機能も提供するとしている[27]。

図表６　生成 AI のビジネス活用の展開

	レベル１： 汎用タスクの自動化	レベル２： 専門タスクの自動化	レベル３： アプリケーションとの連携
実現方法	• 生成AIを単体で利用する • 情報漏洩の対策などを施した環境づくりが必要	• 企業固有の情報を生成AIに学習させる、あるいは企業のデータベースなどを参照させる	• 生成AIと他のアプリケーションを連携させる • 業務プロセスを学習させ、一連のタスクを実行
扱う情報	• 一般的な情報 （汎用的な大規模言語モデルを利用）	• 一般的な情報 ＋企業固有の情報 （企業のデータベースなどを参照）	• 一般的な情報 ＋企業固有の情報 （企業のデータベースなどを参照）
実行するタスク	• （一般的な）情報の検索、文章の要約、翻訳など、生成AI単体で実行できるタスク	• （専門的な）情報の検索、文章の要約、翻訳など、生成AI単体で実行できるタスク	• 生成AIが司令塔となり、他のアプリケーションと連携することで実行できるタスク

（出所）森駿介、田中誠人「ChatGPT がリテール金融ビジネスに及ぼす影響」大和総研レポート（2023 年 7 月 6 日付）より抜粋

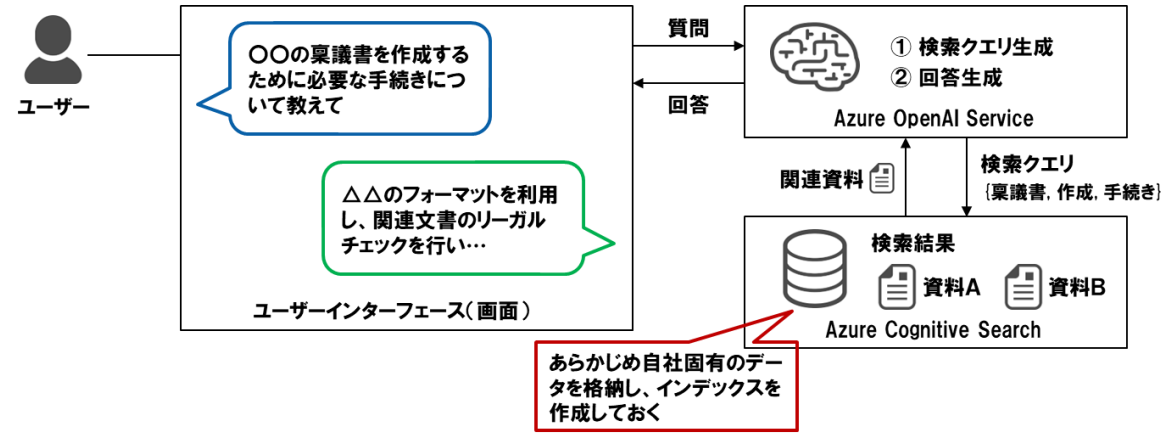
次に、レベル 2 の「専門タスクの自動化」は、生成 AI が企業固有の情報を扱うための方法が複数提案されている状況である。一つは、汎用的な LLM から外部のデータをその都度参照させることで、企業固有の情報を検索できるようにする方法である。これは検索拡張生成（RAG：Retrieval-Augmented Generation）と呼ばれるもので、生成 AI の「知能」自体はそのままに、ユーザーから質問されたときにその都度「知識」を検索し、その情報をもとに回答を生成する。考えられるシステム構成の一つとして、クラウド検索サービスである「Azure Cognitive Search」との組み合わせがある。図表 7 は、この仕組みを実現するためのシステム構成イメージを示している。ユーザーから、稟議書を作成する社内手続きについて質問された生成 AI は、自身がそ

[25] 執筆時点での情報に基づく。サービスの詳細は各社で異なり、社内データの活用等に対応するものもある。
[26] 大和総研「ChatGPT 利用環境構築サービス」（2023 年 9 月 5 日閲覧）
[27] OpenAI “Introducing ChatGPT Enterprise” （2023 年 8 月 28 日付）

の知識を持っていないことから、あらかじめ作成しておいたデータベースに対して検索を行い、関連資料を取得する。その資料の内容をもとに、生成 AI が回答を作成し、ユーザーに対して提示する。これは外部データを参照する方法の一つだが、他にも Python や JavaScript などのプログラミング言語で利用できる「LangChain」というライブラリ（ツール）を用いる方法などがある。LangChain は LLM を活用したサービスを開発する際に役立つもので、外部データの利用のほか、異なるモデルの組み合わせ、プロンプト（AI への指示文）の管理・最適化、複数のプロンプトの実行、複数のツールの組み合わせ、履歴の保持などを比較的容易に実装することができる。

前述の方法は、生成 AI の知能自体には手を加えないものだったが、追加的な学習を行うことによって知能自体をアップデートする方法もあり、「ファインチューニング」と呼ばれる。これまで、主流の LLM がファインチューニングに対応していなかったことから、実用化の場面ではあまり利用されてこなかった。しかし、2023 年 8 月、OpenAI 社が LLM「GPT-3.5 Turbo」をファインチューニングに対応させ、指示に従う能力や出力フォーマットの信頼性の向上など、さまざまなユースケースでモデルの性能を改善できることが明らかになった[28]。また、数多く開発されている国産 LLM は OpenAI 社の GPT などと比較して軽量であり、個別のチューニングを可能にしているものもある。このような状況を踏まえると、今後ファインチューニングがより多く利用されるようになる可能性もある。

図表 7　レベル 2 のシステム構成イメージ



（注）アーキテクチャは一部省略している。
（出所）大和総研作成

レベル 3 の「アプリケーションとの連携」について、企業向けではないものの、生成 AI と外部のアプリケーションを連携する仕組みは既に実装されている。ChatGPT の Web サービス上で利用できるプラグイン機能は一つの例である。例えば、オンライン旅行サイトを展開する Expedia のプラグインを使うと、AI との会話を通して、宿泊施設や航空券の予約などを行うことができる。また、2023 年 9 月に、Amazon Alexa に生成 AI が実装されることが公表された。音声対話

[28] OpenAI “GPT-3.5 Turbo fine-tuning and API updates”（2023 年 8 月 22 日付）

用に最適化された LLM を実装し、効率的なスマートホーム制御などを行うという[29]。

一方で、企業向けとして、業務で利用するという観点では、活用の構想が語られることはあるものの、具体的な情報が出てくることはあまりなく、今後の研究開発の進展が期待される。

５．まとめ

リテール金融業界において、生成 AI の活用を巡る動きは引き続き活発であり、活用事例が多様化しているほか、規制枠組みに係る議論も進んでいる。本稿では、これらの動向について概観し、さらに業界横断的な生成 AI の動向について整理した。最後に、リテール金融業界における活用事例や規制対応と、その背景にある技術的な動向をどのように関連付けて考えるかを示し、本稿のまとめとしたい。

ChatGPT が登場した当初、生成 AI に対して過度な期待が寄せられることが多く、生成 AI は何でもできる「魔法の AI」と捉えられることもあった。しかし、生成 AI にも得手・不得手があり、ビジネスへ応用するためには適切な方法を探る必要があることが意識されるようになってきた。リテール金融業界においては、現状、その活用方法として有力視されているのが、本稿の 2 章で取り上げたような、①営業員等向けの支援ツール、②対話型 AI を顧客に直接提供、③コンプライアンス用途、といった方法である。そして、これらの議論の背景には、生成 AI の技術進歩（AI モデルの進化や、学習方法の高度化を含む）があることを理解することが重要であろう。例えば、営業員等向けの支援ツールの今後の可能性として取り上げた、「顧客のポートフォリオのリスク分析や顧客と FA との間のやり取りをもとに、次のアドバイス内容を生成する仕組みを高度化する」といった活用方法は、4 章で説明した検索拡張生成（RAG）という方法で実現できる可能性がある。さらに一歩踏み込むなら、その活用方法を見越して、LLM が活用できる形で企業固有の情報（資料など）を整備しておくことが、高度化を円滑に進めるために必要となる。このような背景を正しく理解すれば、生成 AI が決して魔法のようなものではなく、技術の蓄積や適切な準備によってもたらされるビジネス上の成果として見えてくるだろう。

また、AI 活用への規制も今後重要となるトピックであり、本稿では米国・EU において金融事業者の AI 利用に大きな影響を与え得る規制案を主に紹介した。日本では規制の議論がそれほど進んでいないものの、金融事業者にとっては、これらの規制に関する議論も参考にしつつ、社内のリスク管理体制やデータガバナンス体制などを検討することが望まれる。

以上のように、リテール金融業界における生成 AI の活用事例と規制動向は、技術的な背景と切っても切れない関係にある。金融事業者においては、これらの状況を包括的に捉え、生成 AI を取り巻く環境の変化をフォローアップしていくことが必要である。さらに、自社の抱える事業や各種業務・それに紐づく作業を洗い出した上で、生成 AI をどのように活用でき得るかを検討していくことが望まれる。

[29] Amazon.com “Amazon previews the future of Alexa with generative AI”（2023 年 9 月 21 日付）