第 1.0 版からの修正箇所について、以下の点を除き、赤字で示したものです。
- 第Ⅳ章内の項目の並び順の変更
- 行間・フォント等を始めとする体裁面の修正

AI ディスカッションペーパー（第 1.1 版）

- 金融分野における AI の健全な利活用の促進に向けた初期的な論点整理 -

2026 年 3 月

金融庁
Financial Services Agency

Ⅰ． はじめに

AI は、これまでもブームと幻滅期を幾度となく繰り返してきたが、生成 AI の加速度的な性能向上等により、ついに社会に広範に実装される段階に到達しつつある。今後、金融を含む産業や国民生活の様々な分野において効率性や利便性を大きく向上させ、国民生活の向上や国民経済の発展に大きく寄与する可能性が指摘されている。金融分野においても、不正検知や市場分析・予測、マーケティングなど従来型 AI の利活用に加え、生成 AI の普及により、一層の業務効率化や顧客体験の向上をもたらすユースケースが登場しつつある。

約 30 年前にインターネットが商用化された時は、通信速度の遅さやセキュリティ、不正利用といった課題があり、インターネットを金融取引に使うことはほとんど考えられなかった。しかし、情報通信技術の発展に伴い、今では金融の中核的な技術の一つとなっている。AI についても、多くの課題に対応していく必要がある一方で、インターネットやクラウドサービスと同様、中長期的には金融業務を支える中核的な技術の一つとなる可能性がある。AI が、将来的に金融サービスの提供の在り方や金融機関等のビジネスモデルを抜本的に変革しうる技術であるとすれば、金融機関等の競争環境が一変する可能性も予見させられる。例えば、専門人材等のリソースが限られる小規模金融機関においても、学習データを用意してモデルを自ら構築する必要がある従来型 AI と異なり、事前学習済の生成 AI は比較的容易に導入が可能である。汎用的な機能を書類作成やシステム開発など様々な業務に活用することにより、人手不足等の課題を克服して大幅な生産性の向上を達成することが期待される。金融機関等においては、現在起こりつつある加速度的な変化を踏まえ、将来を展望した上で、将来のビジネスモデルについて経営レベルで議論していくことが重要である。

一方、我が国においては、生成 AI を悪用した犯罪や偽・誤情報の拡散などのリスクが社会全体で強く意識されている。「現在の規制や法律で AI を安全に利用できると考えている」人の割合が諸外国と比較して顕著に低いなど[1]、積極的な利活用に踏み出せない状況も認められる。このような中、金融分野においても、生成 AI 等の複雑な AI システムの透明性・説明可能性や公平性をどのように担保するか、金融犯罪への悪用リスクや金融システムの安定に与える潜在的影響をどうコントロールするかといった課題が指摘され、リスクや規制面から利活用に躊躇する声も多く聞かれる。

リスクへの対応が重要であることは論を俟たないが、AI はリスクを大きく上回る便益をもたらす可能性が高いとの指摘もあり、技術革新に取り残されて中長期的に良質な金融サービスの提供が困難になる「チャレンジしないリスク」も十分に認識されるべきである。リスクベース・アプローチの下、AI の利用用途に応じて適切にコントロールしつつ、経営陣の主体的な関与の下で顧客利便性や業務効率化の向上に繋がる取組みが着実に進展していくことが望ましい。金融庁としては、金融機関等が AI の利活用に伴うリスクを特定・評価した上で適切に対処し、新たな金融サービスの創出や業務効率化を積極的に実現していくことを期待している。

---

[1] 内閣府「AI 戦略会議・AI 制度研究会　中間とりまとめ」（2025 年 2 月公表）

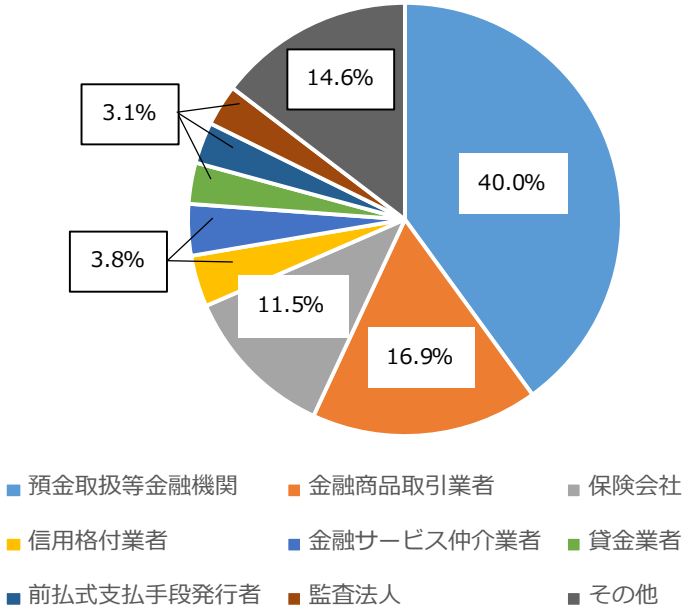
こうした観点から、金融庁としては、金融機関等が AI を活用したチャレンジに安心して取組むことができる環境整備に努めていく。AI に限らず、イノベーションに向けた取組みを進める中で問題が生じた際には、対話等を通じて問題解決に向けて取り組むなど、金融機関等を過度に委縮させることのないように行政対応を行っていく。また、規制の適用関係の明確化等を通じて、セーフハーバーの提供に努めていく。金融庁の基本スタンスは技術中立であり、既存の法令等は AI など特定の技術を利用しているか否かに関わらず適用されることに留意すべきであるが、AI の特性を踏まえて対応が必要な場合は、法令やガイドライン等の見直しを含めて検討していく。AI の急速な技術革新を踏まえると、金融機関等との対話を通じて政策の在り方を柔軟に見極めていくことが重要と考えており、こうした方針に沿って本ディスカッションペーパー（以下、本文書）を策定した。金融庁が先頭に立ち、リスクをコントロールしつつ、我が国の金融分野におけるイノベーションが世界をリードして発展していくことができる環境整備に全力を尽くしていく決意である。

Ⅱ． 本文書の目的・位置づけ

1. 目的・位置づけ

本文書は、モニタリング上の目線や金融機関等に求める具体的対応を示すものではなく、金融庁において 2024 年 10 月 3 日から 11 月 15 日にかけて実施した「金融機関等の AI の活用実態等に関するアンケート調査[2]」や一部の金融機関・ベンダー等へのヒアリング結果、国際的な議論の進展等を踏まえ、金融機関等における従来型 AI 及び生成 AI のユースケースや課題認識、ガバナンス構築に向けた事例などを整理し、今後の対話に向けた初期的な論点及び金融庁としての今後の対応方針を提示するものである。アンケートは、金融分野の幅広い業種に対して実施したものであり、合計 130 社から回答を受領した。うち約４割が預金取扱金融機関で、次いで金融商品取引業者、保険会社がそれぞれ１割強を占め、上記３業態で約７割を占める。

【図表 1 回答先金融機関等の業態別分布グラフ】



任意でのアンケートであり、業態別の回答数にばらつきがあることや、特定の業態に特化した設問ではなく業態間で回答に有意な差は認められなかったことなどから、業態や規模別の詳細な分析はしていない。他方で、自由記載やヒアリングにより頂いた個社からの回答は、個社が特定できない形としつつ数多く掲載した。中小を含む多様な金融機関等の AI 活用状況が把握できるよう、従来型 AI と生成 AI を区分して各種事例や課題を分析している。金融機関等においては各自の置かれた状況を踏まえて、今後の取組みの参考となれば幸いである。

なお、本文書における「従来型 AI」とは、機械学習など、AI にあらかじめデータを与え

[2] 金融庁「金融機関等の AI の活用実態等に関するアンケート調査について」（2024 年 10 月公表）

て「特徴や傾向」を学習させ、入力されたデータに対して回答を得るものを指す（ルールベースのモデルであっても、チャットボットなど、データから複雑なルールを作成してモデルを構築・運用している場合も含む）。また、生成 AI とは、大規模言語モデル（LLM）[3]など膨大なパラメータを有するモデルで、インターネット上のデータやコンテンツ（文章、画像等の非構造化データ）などを学習に使用し、新しい生成物（文書、画像、音声、動画など）を生成する機能を有するものを指す。

また、第Ⅳ章においては様々な課題を指摘しているが、あくまで初期的な分析に基づくものであり、またユースケースや導入方法によってリスクの程度も異なるため、言及された課題に全て対応しなければ AI を導入してはならないといった趣旨で記載したものではない。繰り返しになるが、金融機関等においては、リスクを恐れて過度に委縮することなく、積極的にチャレンジしていくことが期待される。本文書は、本邦金融機関等の現時点でのユースケースやリスク管理の取組みを俯瞰し、中長期的に金融庁の政策や金融機関等における AI ガバナンスの在り方を検討する上での土台として位置づけられるものである。金融庁では、今後、事業者との対話等を通じて論点を深掘りし、本文書の更新や規制の適用関係の明確化等の必要な対応を行っていく考えである。

2. 本文書 1.1 版への改訂の背景

本文書 1.0 版公表後、金融庁では、2025 年 6 月から 12 月にかけて、「金融庁 AI 官民フォーラム」（以下、AI 官民フォーラム）を開催し、AI 利活用の状況、AI に関連するリスクマネジメント・ガバナンスの取組事例、規制の適用関係の明確化を必要とする場面等に関し、情報共有とディスカッションを行った。

その結果、金融機関における AI 利活用は非常に速いペースで進展しており、特に、2024 年 11 月の実態調査の時点ではほとんど行われていなかった顧客向けサービスへの利用について、範囲・条件を絞ったサービス提供又はその検討が行われる段階に至っていることが判明した。また、リスクマネジメント・ガバナンスの手法について、試行錯誤の中で、一定の実務が形成されつつあることが判明した。

これらの進展を踏まえ、本文書 1.0 版に AI 官民フォーラムで得られた知見を基にアップデートを加え、本文書 1.1 版として改訂することとした。

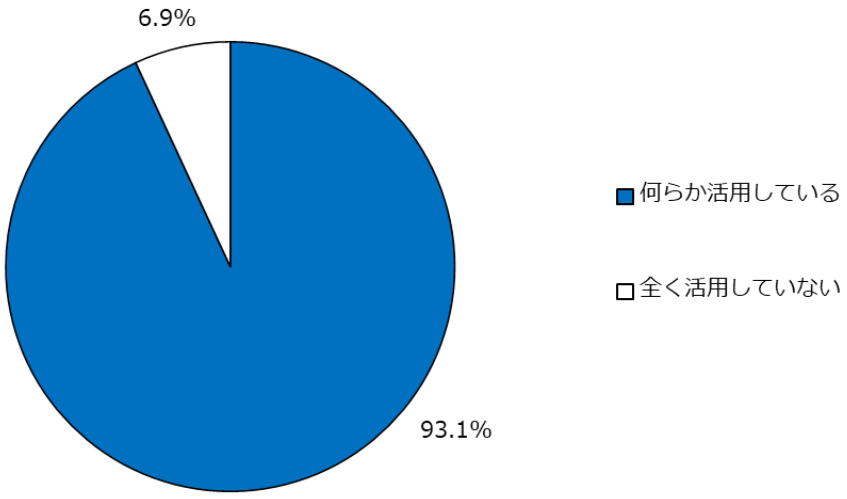
[3] 大規模言語モデル（LLM：Large Language Model）とは、一般に、巨大なデータセットとディープラーニング技術を用いて構築された言語モデルのことを指す。

Ⅲ． 金融分野における AI の活用可能性とユースケース

文書や画像等を含め大量のデータを扱う金融機関等にとって、AI の活用可能性は高い。例えば、顧客のニーズや嗜好が多様化する今、金融機関等は AI の活用により、画一的な金融商品や金融サービスの提供ではなく、取引履歴など顧客にまつわるデータを分析し、一人ひとりに最適化された金融商品を提案することで、顧客本位のサービス提供に繋げていくことができる。また、書類作成など定型的な業務が多い中で、RPA 等と組み合わせてルーティン業務を自動化することで、大幅なコスト削減と業務効率化を実現できる可能性もある。さらに、オルタナティブデータを活用した運用の高度化や市場予測の精緻化など、資産運用分野においても活用余地は大きい。加えて、不正利用の手口も高度化する中で、人手やルールベースでは識別が難しい異常パターンを早期に検知すること等を通じて、リスク管理やコンプライアンスの強化に繋げていくことも可能と考えられる。AI 導入の有無により、デジタル化が進む社会における自社の競争力にも影響が及ぶものと考えられるため、金融機関においては経営陣が主体的に関与して積極的に AI の活用を検討していくべきである。

アンケート回答からは、既に多くの金融機関等で AI の活用が進展していることが明らかとなった。そこで、本章では、従来型 AI と生成 AI に大別した上で、それぞれのユースケース毎の導入状況について整理した。まず、回答先のうち９割以上が従来型 AI または生成 AI を何らか活用していることが判明した。当該結果は本アンケートの回答先に限ったものである点には留意が必要だが、多くの金融機関やフィンテック事業者等が既に相当に AI を導入していることが窺える結果となった[4]。

【図表 2 従来型 AI または生成 AI を活用している先】

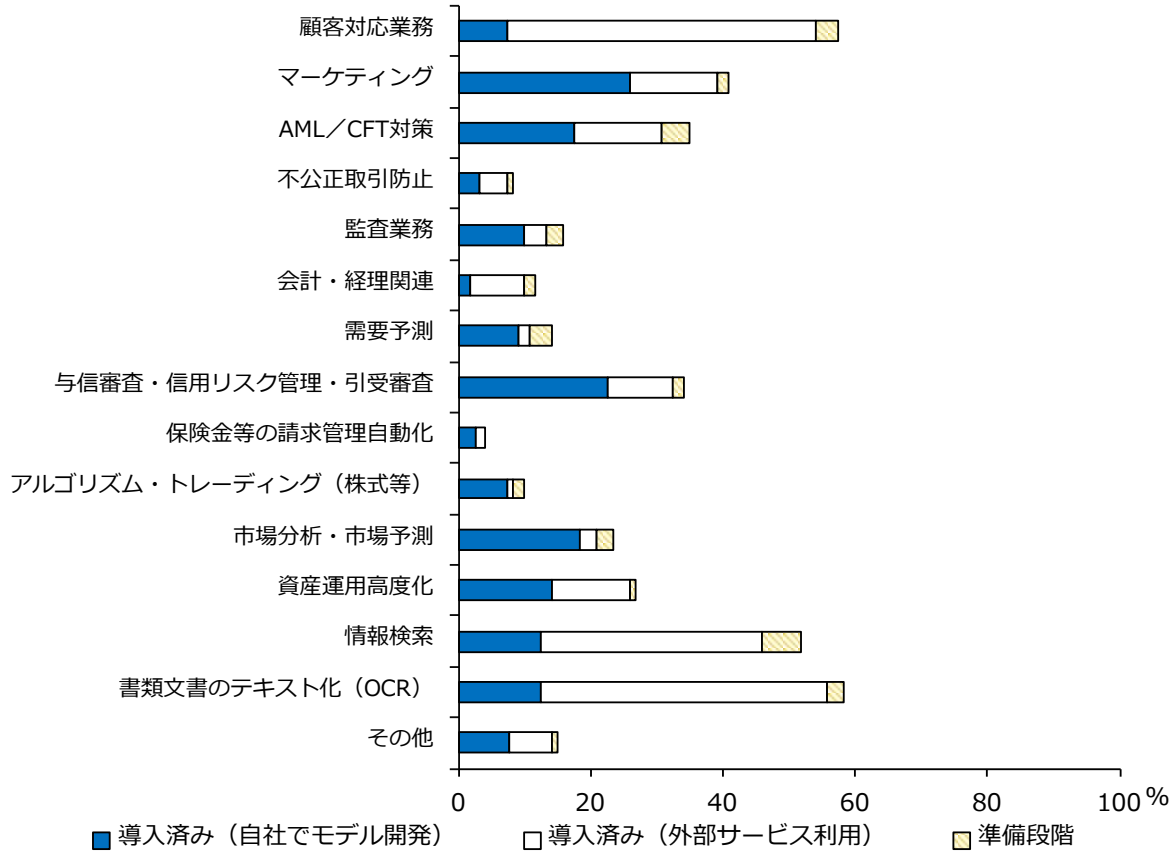


[4] 日本銀行が 2024 年４～５月にかけて預金取扱金融機関等を対象に実施したアンケートにおいても、従来型 AI については既に約６割が利用開始済みで、生成 AI についても約３割が利用開始済みであるほか、試行中を含めると約６割、試行・利用を検討している先を含めると約８割となっており、AI の利用が急速に広まっている結果が示された。
出典：日本銀行「金融機関における生成 AI の利用状況とリスク管理 －アンケート調査結果から－」（2024 年 10 月公表）

1. 従来型 AI の主なユースケース（2024 年実態調査）

「従来型 AI についてのユースケース毎の導入状況」についてのアンケート結果をみると、「書類文書のテキスト化（OCR）」、「顧客対応業務」、「情報検索」、「マーケティング」などを目的とする利用が目立つ結果となった。これらのユースケースを中心に、ヒアリング結果等も参考にしつつ、具体的な活用事例について紹介したい。

【図表 3 従来型 AI のユースケース毎の導入状況】



① 業務効率化

回答先の半数以上が「書類文書のテキスト化（OCR）」や「情報検索」を導入済みであるなど、業務効率化に資する形での活用が広がっていることが明らかとなった。「書類文書のテキスト化（OCR）」については、口座開設時等において顧客から受領した申請書や本人確認書類のデータ化、取引先から手交や FAX で受け取った決算書等のデータ化、PDF 資料のテキスト化といったユースケースが確認された。また、「情報検索」については、社内手続きに関する資料を効率的に検索するための社内向けチャットボットの導入等の事例が見られた。なお、これらのユースケースの導入においては、一部の金融機関等は自社でモデル開発を行っているものの、外部サービスを導入するケースが多くなっている。これは、クラウド会計事業者が自社製品の顧客向けに OCR 機能を提供するなど、他の項目と比較して外部サービスの導入が相対的に容易であることが背景にあると考えられ、他の項目と比較して導入率が高いことの一因となっている。また、導入した外部システムの性能に課題を感じ、生成 AI などと組み合わせた新たな方法の導入を検討している先も存在する。

②　対顧客サービスへの活用

「顧客対応業務」や「マーケティング」など、顧客関連業務への活用も進展している。「顧客対応業務」としては、チャットボットによる照会対応業務での利活用が特に多く確認された。具体的な機能としては、入力された質問項目を解析し、モデルに事前に与えた質問事項に最も類似したものと対応関係にある回答を表示するといったものである。「マーケティング」については、営業職員向けの補助ツールとしての活用（例えば、顧客の年齢・取引状況などを機械学習させ効率的な営業リストを作成、顧客の繁忙期を特定し当該時期には営業活動を行わないようにする等）、人員配置の最適化等を通じた確実な顧客へのサービス提供（例えば、コールセンター業務において、AI で需要予測を行うことにより、必要な時期に必要な人数の配置を実現する等）、アプリを通じた顧客へのパーソナライズド・メッセージの送信といった活用方法が確認された。

③　リスク管理の高度化

「AML/CFT」、「与信審査・信用リスク管理・引受審査」など、コンプライアンスやリスク管理の高度化に向けた取組みにおいても AI が相当に活用されている。「AML/CFT」業務への活用に関してみてみると、取引モニタリング業務等において、過去の取引記録等を教師データとして学習し、検知ルールの高度化への活用を模索している先などが確認された。個社での自社開発では学習データに限りがあり十分な精度が得られず本番利用を見送ったと回答した先もあったが、ルールベースの不正検知システムとの併用を検討する先や、業態を同じくする数社が共同でモデルの開発を行う先、複数の金融機関の AML/CFT データを活用した取引モニタリング及びネームスクリーニング業務の高度化に資するサービスの提供を開始又は提供の準備を進めている先もあり、AML/CFT の高度化に向けた取組みの進展が窺われた。「与信審査・信用リスク管理・引受審査」においては、例えば、顧客のローン返済履歴等を学習させた与信判定モデルや過去の審査判定データを学習させた保証審査モデルを開発・運用している先、購買データ等を活用した与信スコアリングを導入している先、ニュースや SNS を活用した予兆管理を行っている先、延滞率や債務者区分の推定を行っている先などが確認された。これらのモデルの精度は学習データの質や量に依存することになるが、不正検知と比較すると相対的に自社内で多くのヒストリカルデータが蓄積されていることから、AI のみの判断でも比較的高い精度が得られると評価する回答が少なくなかった。

その他、保険金不正請求の検知や監査業務における活用（例：不適切な会計処理の検知、社内メールを AI でスコアリングして不正検知の一助とする）、営業現場におけるコンプライアンス違反の検知（例：金融商品販売時等における応接記録からコンプライアンス違反が疑われるものを抽出）など、コンプライアンスやリスク管理の高度化に向けた様々な用途での AI の活用事例が確認された。

④　市場予測等

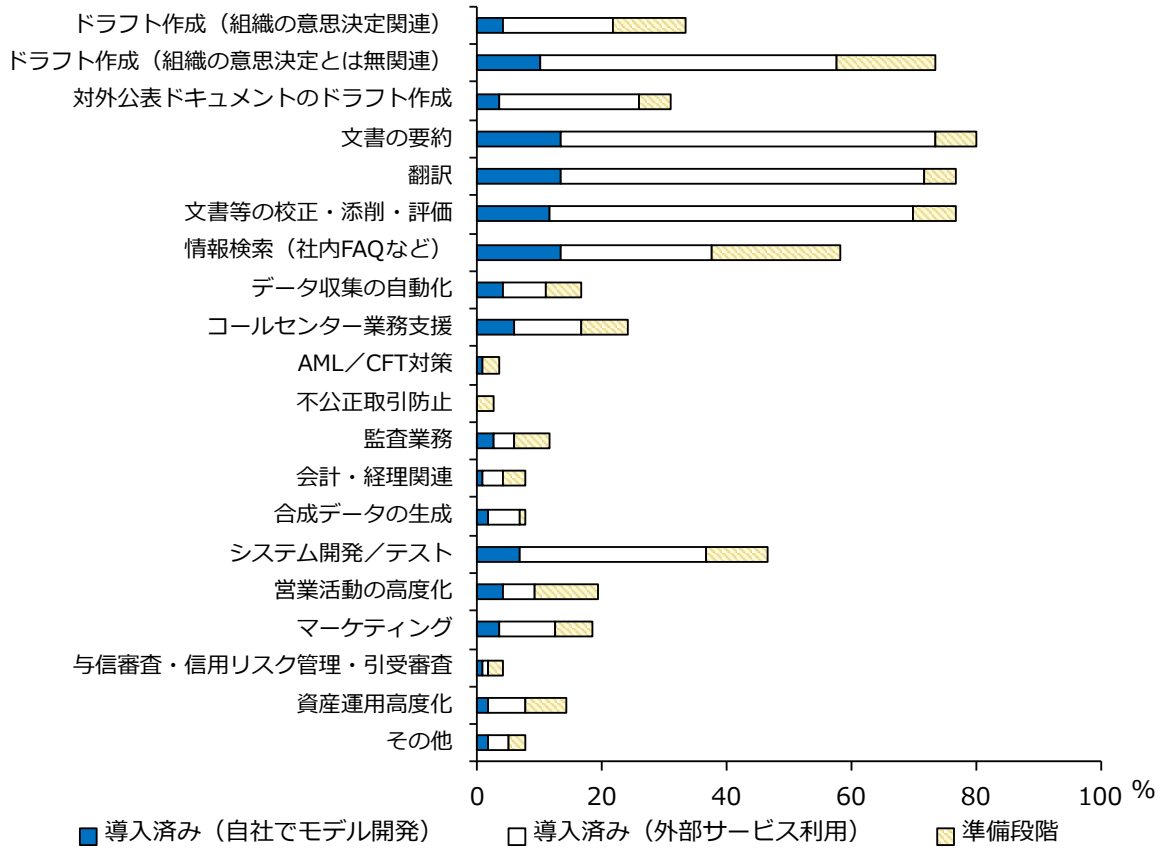
資産運用や証券業務、外国為替取引などの分野で幅広く AI の活用が進展している。具体的には、為替・金利予測、ポートフォリオの最適化、運用戦略の高度化といった用途に加

え、ニュースサイトや SNS の投稿内容を自然言語処理（NLP）で分析し、リアルタイムに市場センチメントを把握するといった事例が代表的である。さらに、衛星画像や地理情報、交通量や企業のサプライチェーン状況など、これまで十分に活用されてこなかったオルタナティブデータを取り込み、財務情報等では把握しにくい先行指標を捉える動きも広がっていることが確認された。

2. 生成 AI の導入状況と主なユースケース（2024 年実態調査）

次に、金融機関等における生成 AI の導入状況と主なユースケースについて、より詳細に分析していく。まず、全般的な導入状況を説明した後に、３つの類型に分けて具体的なユースケースを紹介する。

【図表４ 生成 AI のユースケース毎の導入状況】



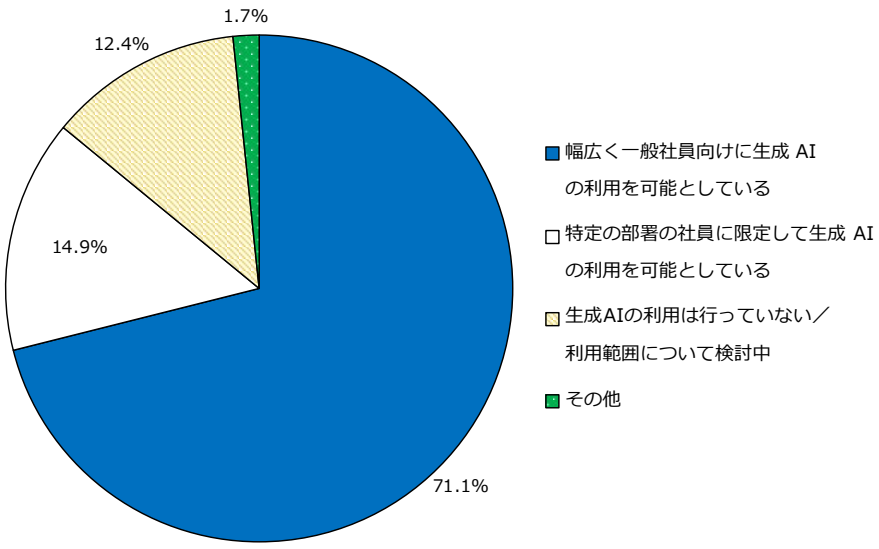
① 生成 AI の利用範囲

生成 AI は従来型 AI とは異なる特性を有し、必然的に金融機関等における活用形態も異なるものになっている。

大きな違いの１つは、生成 AI の汎用性の高さである。特定の用途に応じてモデルが開発・運用されてきた従来型 AI については、デジタル戦略部門や IT システム部門、リスク管理部門などに所属するデータサイエンティストやエンジニアなど、一定の専門知識を持った職員が関与するケースが多い。一方、生成 AI は文書のドラフティングや翻訳・要約など多

くの職員の日常業務を効率化するツールとして活用できる余地があり、既に生成 AI を導入している金融機関等の大半は広範に生成 AI の利活用を認めている。

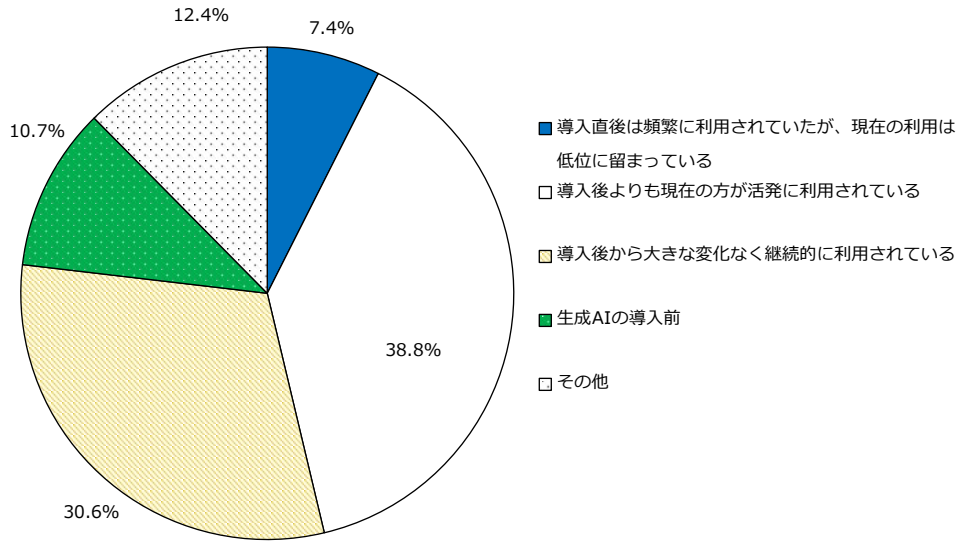
【図表 5 生成 AI の利用状況】



具体的にみると、AI を何らか利用していると回答した先を対象に生成 AI の利用状況について回答を求めたところ、７割以上の先が幅広く一般社員向けに生成 AI の活用を認めていることが確認された。アンケートの回答を詳しくみると、全社員に生成 AI の利用を認めている先、申請制としている先、本社部門に限定して利用を認めている先、生成 AI の種類に応じて異なる利用範囲を設定している先など、投資対効果等の観点も踏まえていくつかの異なるアプローチが確認された。

また、生成 AI 導入後の利用状況については、多くの金融機関等において、導入直後と比較して継続的に利用されているか、現在の方がより活発に利用されているという結果が確認された。カスタマイズ等を行わず汎用の生成 AI を導入しているのみの先も多いが（次節参照）、それでも活発に利用されているのは、生成 AI の金融機関等の業務効率化等への活用可能性の高さを裏付けるものであると考えられる。社員のプロンプト作成能力（生成 AI を効果的に使うための指示や質問を作成する能力）などが障壁となり利用が期待以上に進んでいないと回答した先もあったが、社内勉強会やアイデアコンテストなどの取組みを通じて利活用が広がっていっていると回答した金融機関等が多数確認された。

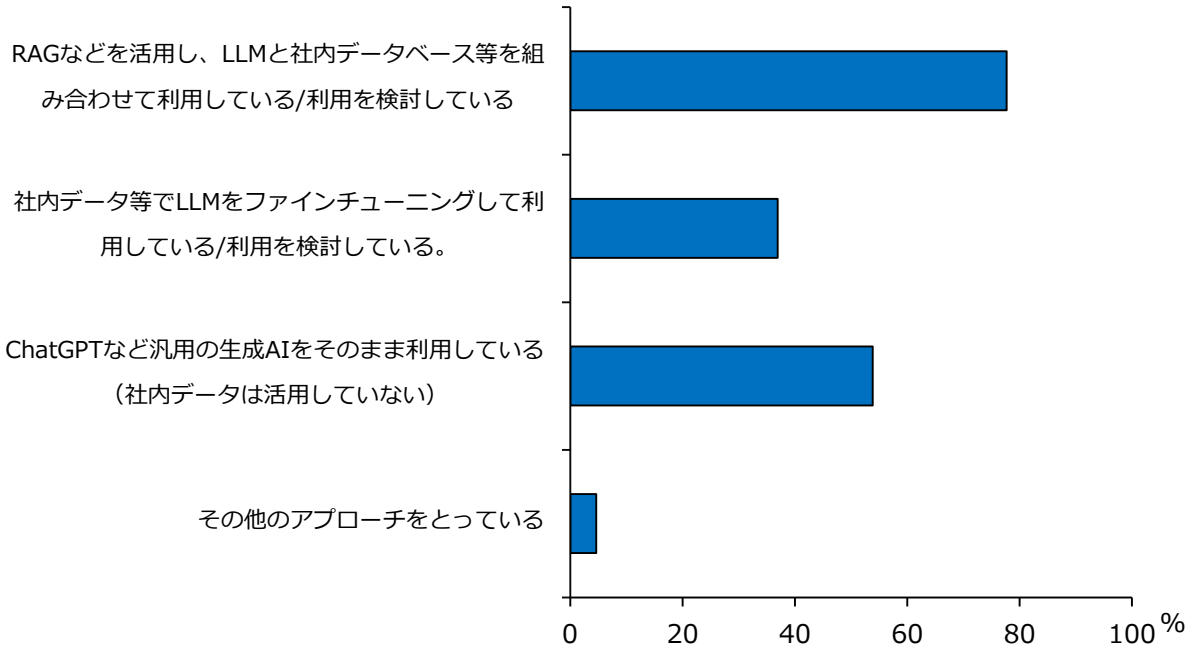
【図表 6 生成 AI 導入後の状況】



② カスタマイズの有無と導入形態

LLM は事前学習済モデルであり、金融機関等は従来型 AI のようにモデルを一から構築する必要がなく、必要最小限の設定で汎用的な機能をすぐに活用することできる。これにより、AI 導入にかかる初期投資や専門スタッフの確保といったハードルが下がる側面があり、アンケートの結果でも、約半数の金融機関等が汎用の生成 AI をそのまま活用しているとの回答が確認された。これらの特性も反映して、従来型 AI よりむしろ生成 AI の方が全般的な導入率が高いとの結果が確認された（例えば、従来型 AI で導入率が高かった顧客対応業務や OCR でも導入率は 6 割未満であるが、文章の要約・翻訳といった生成 AI の汎用的なユースケースは既に 7 割超の金融機関等が導入済）。

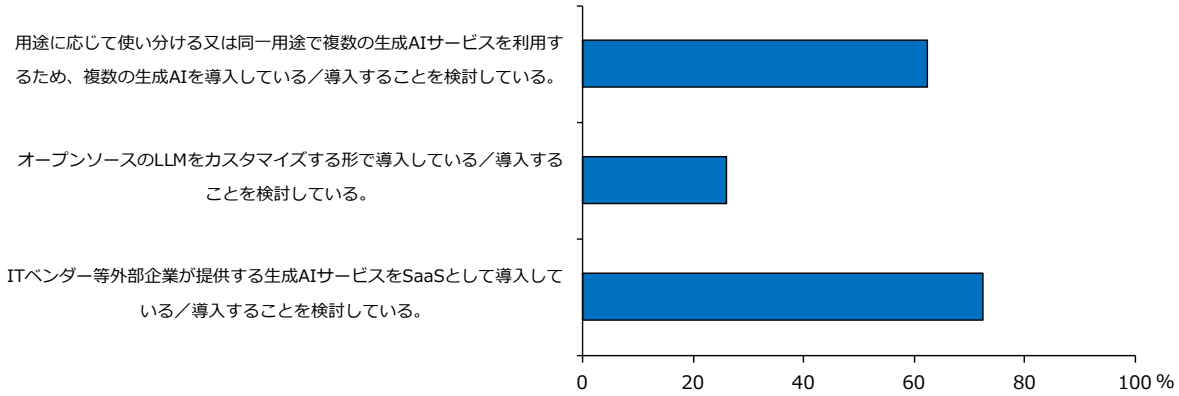
【図表 7 生成 AI の導入形態（カスタマイズの有無）】



その一方で、RAG（Retrieval-Augmented Generation）[5]やファインチューニング[6]により、ベンダーが提供する LLM と社内データベース等を組み合わせて利用または利用を検討している先も多い。従来型 AI と比較すると、マルチモーダル化[7]が進む生成 AI は金融機関等が大量に保有するテキストや画像、またベンダーが提供するオルタナティブデータなどの非構造化データの活用余地を広げており、多くの金融機関等がベンダーやフィンテック事業者、コンサルティング会社等と協働しつつ利活用の可能性を模索していることが確認された。

また、ユースケースに応じて複数の生成 AI を利用する先も多い。例えば、全社員向けの汎用的な生成 AI は大手クラウド事業者が提供する生成 AI サービスを活用しつつ、特定の業務に特化した RAG は内製開発のメイン環境として利用している別の大手クラウド事業者の提供する生成 AI を採用するといった事例が確認された。さらに、LLM にはオープンソースとプロプライエタリの双方のモデルが存在するところ、独自で環境を構築する手間がかかるものの、オープンソースとして提供されている LLM をオンプレミスサーバー内で利用している先や、専用線を通じてプロプライエタリな生成 AI サービスを閉域環境で利用している先なども確認された。また、ベンダーが提供する生成 AI ツールを SaaS として導入している先もあれば、ユーザーインターフェース等を独自で開発する先も存在し、生成 AI の導入形態は一様ではないことが明らかとなった。

【図表 8 生成 AI の導入形態（SaaS での利用等）】



様々な基盤モデルや生成 AI ツールが登場し、また基盤モデルのアップデートや新たな基盤モデルの公開も頻繁に行われる中で、金融機関等は現時点においては一つの導入アプローチにこだわるのではなく、試行的に様々なアプローチで取組んでいる印象である。

---

5 RAG（Retrieval-Augmented Generation,検索拡張生成）とは、一般に、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を指す。

6 この文脈におけるファインチューニングとは、一般に、事前学習済の LLM を特定のデータセットで再学習させてモデルのパラメータ（重み）を微調整することを指す。

7 ここでいうマルチモーダルとは、生成 AI がテキスト・画像・音声・動画などの異なるデータ形式を組み合わせて解析や生成を行うことを指す。

Box 1. 業務特化型モデルの構築に向けた様々なアプローチ

生成 AI は、汎用的な質問に対する回答や文書作成等において高い効率性を発揮する一方、金融機関固有のルールや商品知識、顧客の過去の取引履歴などを踏まえて対応すべきケースにおいては、汎用モデルだけでは十分な精度を得られないことが指摘されている。そこで、RAG やファインチューニングといった技術手法を活用し、業務特化型の生成 AI モデルを構築しようとする動きが進展している。

■ RAG の活用例

RAG とは、LLM と情報検索を組み合わせて応答を生成する手法であり、外部データベースから最新の情報を取得し、モデルの応答に組み込むことで、回答の精度と信頼性の向上を実現しようとするものである。実装にはベクトルデータベースの構築や検索アルゴリズムの最適化が必要だが、モデル自体の再学習が不要な点が利点である。

- ある金融機関では、社内規程や商品パンフレット、顧客向け FAQ などをクラウド上で一元管理し、RAG を用いてこれらの関連情報を取り込んだ上で照会に対する回答を生成するシステムを試行している。

■ ファインチューニングの活用例

ファインチューニングとは特定のデータセットでモデルのパラメータを微調整し、特に出力形式の一貫性を重視する手法である。教師あり学習による微調整のため、応答品質の安定化に寄与するとされる。微調整にあたっては、十分な量と質の学習データと一定の計算コストがかかる。

- ある金融機関では、過去の顧客応対履歴や不正請求データを用いてファインチューニングを実施し、問い合わせ対応チャットボットの回答精度の向上に向けた取組みを進めている。

一方で、LLM をカスタマイズせずに、プロンプトを工夫することで、モデルに業務特化型の応答を促す手法もある。例えば、社内規程や取扱う金融商品の概要をプロンプトに含めて提示することで、カスタマイズなしでも一定の専門性を持った回答が可能になる。また、コンテキスト内学習（In-context Learning）と呼ばれるアプローチでは、プロンプト内に例示や要点をあらかじめ含めることで、モデルが参照しながら回答を生成できるように工夫する。これらの手法は、再学習や外部データベースとの連携を必ずしも伴わないため、導入コストやデータ整備の負担を抑えられるという利点がある。一方で、プロンプトに含める情報が長文になりがちであり、モデルが正確に理解できるよう整理・最適化することが課題となる。

③ ユースケースの３類型

このように、生成 AI の導入は試行錯誤の段階にあるが、例えば以下のような切り口でユースケースを分類することが考えられる。

A) 利活用の目的：業務効率化等の社内利用か、対顧客サービスへの利活用か

B) 汎用／業務特化：汎用の生成 AI を利用するのか、RAG 等を活用した業務特化型の生成 AI を利用するのか

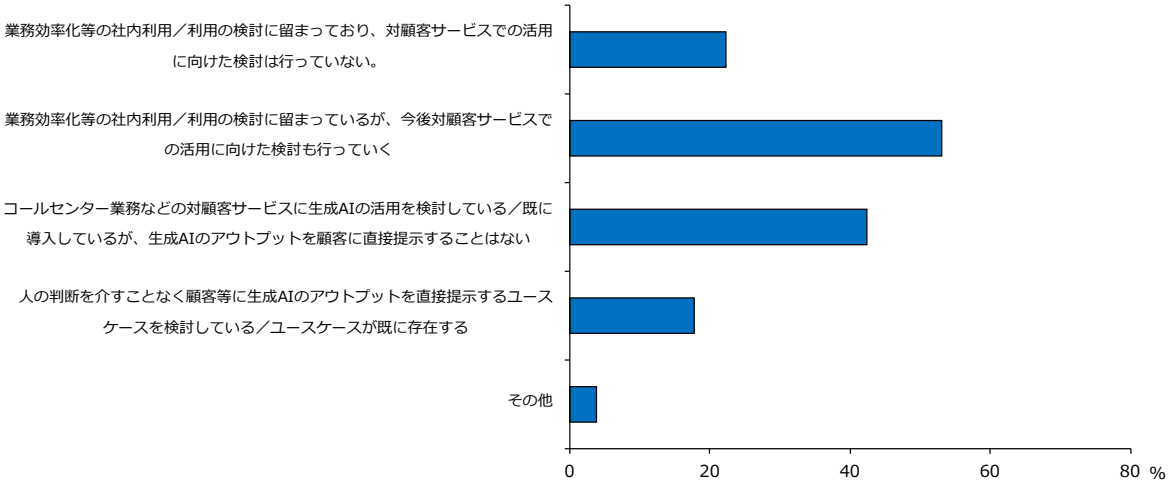
C) 生成物：テキスト等の自然言語か、プログラムコードや画像など自然言語以外のもの

か

本文書においては、A）の切り口に沿って、生成 AI の現段階での主なユースケースを以下の３つに分類して整理することとしたい。

- 社内利用（業務効率化等）
- 対顧客サービスへの間接的な利活用
- 対顧客サービスへの直接的な利活用

【図表 9 生成 AI の対顧客サービスへの活用】



アンケート結果からは、現時点では業務効率化等の社内利用に留まっていると回答した先が多くを占めた。多くの場合、相対的に導入が容易な汎用の生成 AI をまず導入し、文書作成や文書の要約・翻訳・添削といったユースケースから利用を始めている。一方で、現在は社内利用に留まっているが今後対顧客サービスでの活用に向けて検討していくと回答した先も半数以上に上り、新たな金融サービスの創出も視野に、より発展的な活用を目指していく姿勢が多くの金融機関等から窺われた。また、コールセンター業務等の対顧客サービスに生成 AI を導入済の先も相応に存在するが、ハルシネーション等のリスクを考慮して生成 AI のアウトプットを顧客に直接提示することは無く、人の判断を介するユースケースが大半となっていることが確認された。ただし、将来的には技術の進展によりハルシネーション等の課題が緩和されると考える先も存在し、生成 AI のアウトプットを顧客に直接提示するようなユースケースが中長期的に広がっていく可能性もある [8]。

i. 社内利用（業務効率化等）

アンケート結果から、「文書の要約」、「翻訳」、「文書等の校正・添削・評価」の３つのユースケースは既に７割以上の金融機関等が導入済であることが明らかとなった。金融機関等は大量の文書を作成・保有しており、文書関連のユースケースは社内利用において最も一般

[8] 一般社団法人金融データ活用推進協会『金融機関における生成 AI の実務ハンドブック』（2024 年 5 月公表）においては、生成 AI の活用のレベルを３つ（レベル１：社内で ChatGPT 等の生成 AI を個々人が活用、レベル２：RAG の仕組みで社内情報を取り込んで、特定分野のアプリケーションを構築、レベル３：社外のお客さまに生成 AI を使ったサービスを提供）に分類している。

的なものといえる。また、定型的な文書の作成業務に活用する先も多い。具体的な利用例としては、対外公表情報の要約、議事録の作成（オンライン会議等の文字起こし）、外国語（英語以外も含む）の翻訳、誤字脱字の添削などがある。また、文章の作成や翻訳においては、想定される読み手に応じたトーン調整も可能であり、例えば、規制当局向けの文章を作成する際にはフォーマルな文体での文書作成を指示できるなど、その汎用性は既に高いレベルで実現されていることが確認された。その他、新規事業の検討や文書作成の際のアイデア出しとして活用しているとの回答も多くあった。

もう一つの代表的なユースケースが社内 FAQ などの情報検索であり、回答先のうち既に４割程度の先が導入済みであった。従来型 AI でも同様のユースケースは存在するが、汎用の生成 AI を社内専用チャットボットに導入した事例も多く、一部では、RAG を活用することで社内規程等の社内独自のデータも参照した上で回答を生成できる仕様に発展させている。このようなカスタマイズに関しては、社内規程のような社員全員に元々共有されているデータのみならず、会社実務に精通している経験値の高い職員の属人的な知識や知見を見える化を実現する目的での活用も確認された。各社人手不足が意識される中で、ノウハウや暗黙知を若手職員に継承することを目的として積極的に取り組む意義を強調する回答もあった。

また、「システム開発/テスト」など必ずしも自然言語に限らない領域での活用も既に一定程度広がっている。具体的にはプログラミングにおけるコーディングの補助等での利活用が多く聞かれており、一部ヒアリング先からは、当該分野において生成 AI の活用が大きな成果をあげているとの指摘も聞かれるなど、効果的な活用方法として認知されつつある。

Box 2. 生成 AI の社内での幅広い利活用に向けた具体的な取組事例

- 生成 AI を日常的に利用できる環境を社員に提供するため、社内の主要コミュニケーションツールである Slack に愛嬌のある生成 AI アシスタントを常駐させるようにした。業務を補助する実務的な能力を備えつつ、気軽な相談相手としても利用されている。
- 毎回ページを開く必要があるウェブページではなく、コラボレーションツールの中に生成 AI の機能を埋め込み、使い勝手を良くした。リサーチや翻訳、文字起こし等に利用。
- クラウド環境に生成 AI を活用した各種ツールを構築。汎用的な機能だけでなく、社内文書を参照し照会に対する回答案を作成する文書参照 GPT や文書作成アプリから生成 AI を利用可能なアドインを全社で活用している。
- ベンダーが提供するプラットフォーム上で、事務手続きの方法などを対話形式で質問できる生成 AI チャットボットを導入。行内の事務マニュアルに記された内容を AI が要約し、出典とともに回答するもので、専用窓口に電話などで問い合わせる手間を削減。

ii. 対顧客サービスへの間接的な利活用

本分類における代表的なユースケースは、コールセンター業務支援である。今までは必要な人員数をコールセンター部門に配置できずに潜在的な顧客ニーズを取りこぼしていたような場合でも、生成 AI を活用することで、人手を介することなく、かつ的確な回答を行うサービスの提供が最終的には実現可能と指摘する声もある。ただし、現時点では後述のハルシネーション等のリスクを完全に解決することは困難である中、顧客に直接提供されるサービスに活用することは難しいと判断する先が大半であることが確認された。もっとも、コールセンター職員が顧客対応をする際の補助として生成 AI を活用する例は既に広がっており、対顧客サービスへの間接的な生成 AI の利活用は試みられている。こうした活用方法については、既に業務に習熟している職員に追加的にもたらす便益は限定的であるものの、新たに職務に従事する職員にとっては大きな助けとなっているようで、職場全体の離職率低下に大きく寄与しているといった評価も聞かれている。

また、「ドラフト作成（組織の意思決定関連）」や「対外公表ドキュメントの作成」など、顧客に影響を及ぼしうるドキュメント策定業務にも一定の活用が進んでいることも明らかとなった。例えば、過去の稟議書や関連資料を参考に、稟議書のドラフトを行うようなユースケースは複数の金融機関等から挙げられており、稟議書の作成時間の短縮や質の向上といった効果が期待されている。また、稟議書のレビューにも生成 AI が活用されることがある。このようなユースケースにおいても、例えば稟議書は融資判断など顧客に重要な影響を及ぼしうるものであり、人の関与（Human in the loop）を必須とする運用が大半となっていることが確認された。

iii. 対顧客サービスへの直接利用

ハルシネーションのリスクや、生成 AI に関する各金融機関等でのガバナンス体制に関する整理が途上であることを踏まえ、顧客に直接サービスが提供される分野においての生成 AI 利用についてはより保守的に運用している金融機関等が大半である。ただし、一部のフィンテック事業者等においては、ライフプランのアドバイスなど、既に生成 AI のアウトプットを顧客に直接提示するサービスの提供を開始している。

3. AI 利活用の展開

① 顧客向けサービスへの利用

顧客向けサービスへの利用は、2024 年実態調査時点では極めて限定的であったが、その萌芽が見られ始めている。

例えば、AI 官民フォーラムでは、2024 年から 2025 年にかけて、コールセンターにおける一部の顧客対応や営業支援など、顧客と間接的に応対するシステムへの生成 AI の組込みを始めている事例が紹介された。また、2025 年 8 月より、顧客からの問い合わせや住所変更等の手続きに生成 AI を組み合わせたアバターが対応するサービスを開始している事例の

紹介もあった。

昨今の AI の高機能化を踏まえれば、例えば、顧客への資産運用に関する相談対応やコンサルティングなど、より金融サービスの本業に近い領域で生成 AI を直接顧客向けに活用するような高度なサービスを提供する未来も展望される。

② AI エージェント

2025 年は、「AI エージェント元年」とされる。AI エージェントとは、特定の目標を達成するために自律的に行動する AI システムであり、LLM は、その思考や判断を担う「頭脳」として使用される。従来、LLM は、チャットボットとして使用されることが一般的であり、その用途は、テキスト処理やコーディングが中心であったが、AI エージェントに組み込まれることで、幅広い業務に応用できるようになると考えられる。

さらに、AI 官民フォーラムでは、複数の AI エージェントが相互に作用しながら自律的に複数の処理を繰り返し実行できるエージェンティック AI が実現すれば、金融分野の業務における数多くのプロセスを自動化できる可能性があるとの期待感が示された。その上で、今後、AI エージェント／エージェンティック AI を顧客向けサービス等に拡大する動きがみられることや、人手不足に対応する観点からも、AI エージェント／エージェンティック AI の業務への実装を考える必要があることなどが指摘された。

Box 3. 監査業界における AI 活用の概観

- AI ツールの開発・導入は、資本市場で企業の開示情報の信頼性を確保する役割を担う監査業界においても、グローバルレベルで進められている。監査人には、膨大な財務・非財務情報の検索・理解・分析作業が求められる中、AI の活用により、業務効率化やデータ分析の高度化が図られ、監査人が評価・判断を要する業務により注力することが可能となり、監査品質の向上に資することが期待されている。
- 従来型 AI については、取引・仕訳データにおける異常検知や不正リスクの識別・評価、監査の基準や監査業務マニュアルなどの法人内情報の検索、書類文書のテキスト化（OCR）等のツールとして活用されるケースが見られる。一層の効率化・高度化のため、これらのツールに生成 AI も取り入れて導入/試行する例もある。このほか、生成 AI については、傾向として、文書等の要約や翻訳、校正・添削等、監査人を補助するツールの導入/検討が進んでいる。
- 一方、AI 活用の課題に関しては、各監査法人より様々な論点が挙げられているが、特に共通して、学習データの量と質の確保について、データの標準化や不正会計に係るデータ蓄積の不十分さが指摘されている。さらに、生成 AI については、従来型 AI と比べより難化している課題や生成 AI 固有の課題が指摘され、各監査法人において、生成 AI に関する追加的な規程の策定や利用方法の制約など、管理体制の構築に取り組んでいる。課題としては、金融機関同様、特にハルシネーション（Ⅳ-③- ｉ 参照）や出力過程に係る説明可能性の担保の困難さ等が挙げられた。監査法人においては、AI 活用に係るこれらの課題を補う技術の開発・導入やバックテストによる結果の検証など、回答精度や説明可能性を高める工夫を行いながら、ツールの導入/検討を行っている。
- AI の進展が監査品質にもたらす影響については、世界の監査監督当局で構成される国際機関である IFIAR でも議論されている。特に、大手監査法人のネットワークについては、各国の法人のみならず、AI ツールの開発・導入やそのガイドラインの策定を基本的にグローバルレベルで進めており、各国の監査監督当局が協調・協力してモニターしていく必要がある。金融庁では、こうした国際的な議論の動向も踏まえながら、監査法人及び日本公認会計士協会との対話やアカデミアと連携した調査研究を通じて、AI ツールの活用実態や課題を把握し、必要な対応を検討していく。

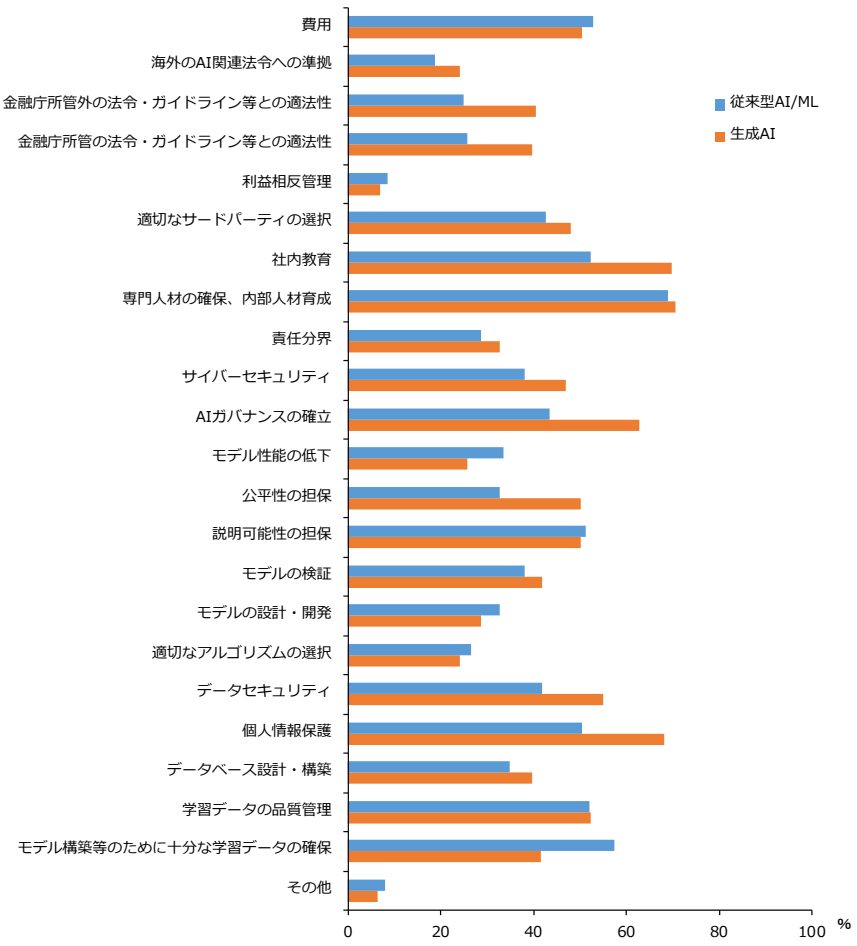
IV.　金融機関等による AI の利活用の促進に向けた初期的な論点整理

本章では、金融機関等へのアンケートやヒアリング、また FSB 等の国際組織を含む国内外での AI を巡る議論を踏まえて、AI 活用に係る主な課題について初期的に整理した。また、これらの課題を克服するための取組みが一部の金融機関等で始まっていることから、具体的な取組事例もあわせて紹介している。更に、AI ガバナンスの構築を通じた AI の健全な利活用の促進に向けた金融庁の今後の対応の方向性について整理した。なお、これらの記載は本文書執筆時点におけるあくまで初期的な分析結果に基づくものであり、金融機関等に対して特定の対応をただちに求めるものではない。

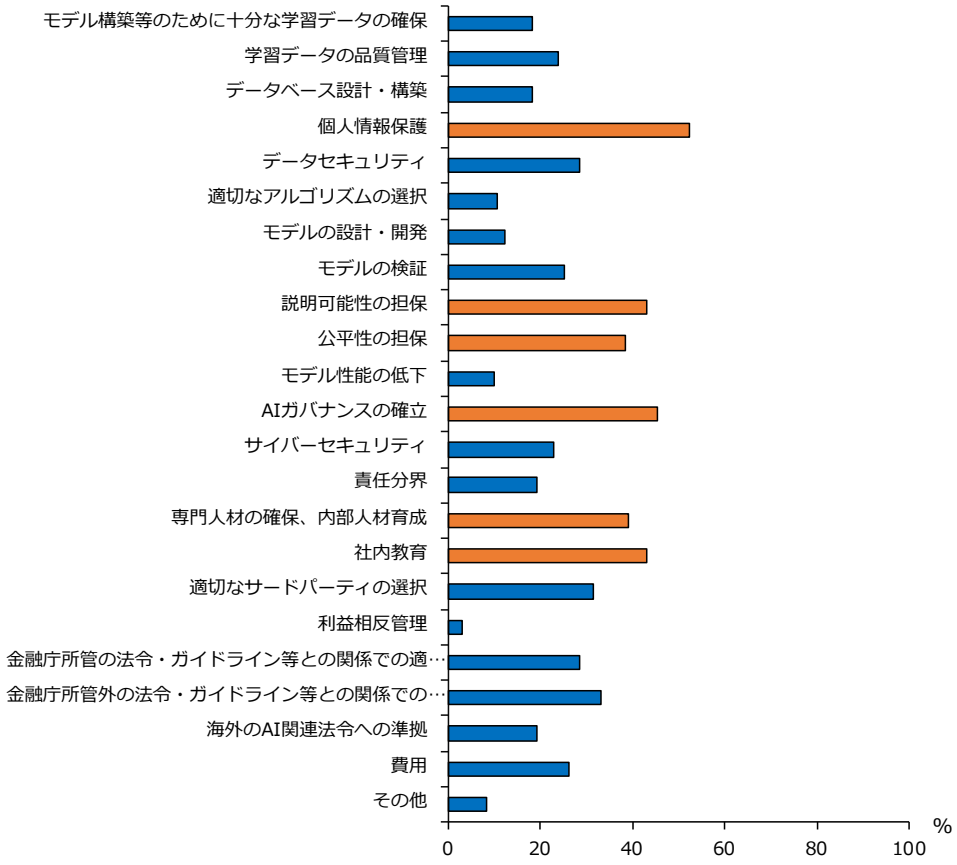
1. 金融機関等の AI 活用に係る主な課題と課題克服に向けた取組事例

従来型 AI と生成 AI の活用に係る課題認識をアンケートで尋ねたところ、データ整備など多くの論点が双方において共通の課題として金融機関等から挙げられた。一方で、例えば AI モデルの出力結果に関する説明可能性の担保など、一部の課題については、生成 AI でより難化しているという声も多く聞かれた。また、ハルシネーションのように、生成 AI 特有の課題も存在している。以下では、全社的な体制に係る課題・取組事例、個々の AI システムに係る課題・取組事例に分けて取り上げる。

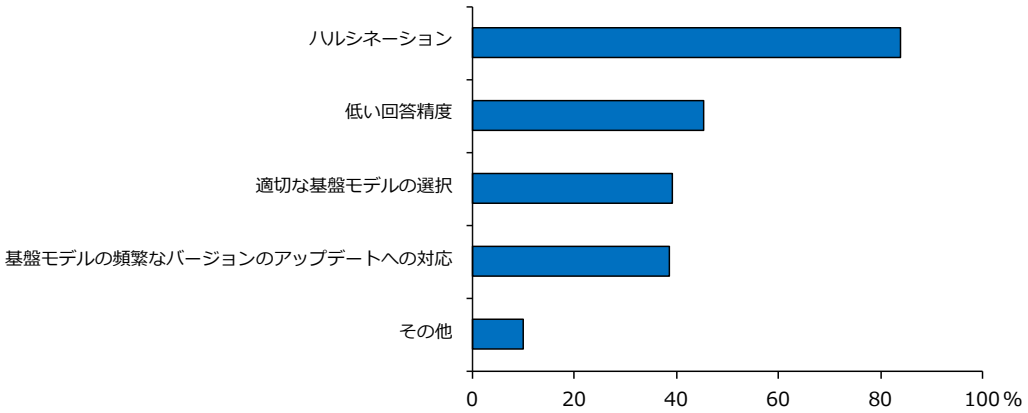
【図表 10 AI の検討・導入・利用時の課題】



【図表 11 生成 AI により難化した課題】



【図表 12 生成 AI に関連する新たな課題】



① 全社的な体制に係る課題・取組事例

i. データ整備・データマネジメント

社会全体のデジタル化の進展や非対面取引の増加、さらには顧客ニーズの多様化等に伴い、金融機関等は業務効率化や新たな金融サービスの創出に向けてデータ利活用の取組みを続けてきた。多くの金融機関等では、クラウドサービスや API を活用したデータ基盤の整備を進めており、フィンテック事業者等の外部事業者との連携を通じたオープンイノベーションも進展している。また、金融機関等のリスク管理、ガバナンス、内部監査の高度化におい

てもデータ活用は重要であり、金融庁としても、オープンイノベーションの推進等に係る法令改正やデータやディスカッションペーパー[9]、モニタリングレポート[10]の公表等を通じて、金融機関等のデータ活用等に関する重要性に言及してきた。こうした中、生成 AI を含む AI の急速な進展と普及は、金融機関等におけるデータの重要性をさらに高めている。前章で一部のユースケースを紹介した通り、社内データ等を学習データや推論検証用データとして活用することで、金融機関等の競争力を向上させる可能性を秘めている。

生成 AI の場合、外部事業者が提供する学習済みの LLM をそのまま利用する場合には、社内データは必ずしも必要ない。しかし、自社の業務プロセスに最適化されていない汎用の生成 AI モデルでは業務効率化等に限界があると考えている先も多く、業務プロセスや顧客ニーズ、ビジネスモデル等に合わせて社内データ等を用いた基盤モデルのカスタマイズの重要性が認識されている。そこで、前章で見たとおり RAG やファインチューニング、コンテキスト内学習等によりカスタマイズを試みている先も多い。

一方で、多くの金融機関等が社内のデータ整備に課題を抱えている。AI のトレーニングやカスタマイズには社内データを含む高品質なデータ基盤を整備する必要があり、特に生成 AI を含む複雑な AI の活用においては、データの質や量の確保、モデルの適切なトレーニング、さらには情報セキュリティや個人情報保護に関する規律の遵守が求められる。しかし、アンケートでも約半数の金融機関等が「モデル構築等のために十分な学習データの確保」や「学習データの品質管理」が課題と回答し、データ整備は道半ばの状況にある。

金融機関等から寄せられたデータ整備に関する主な課題

- RAG での活用など社内データを AI で活用する前提でデータベースが構築されておらず、社内での合意形成やベンダーとの調整など対応に時間とコストがかかる。
- 統合クラウドデータ基盤と他のデータベース間のシームレスな接続が課題。
- データの品質の問題（例：古い社内規程が残っている）により、RAG を試したものの LLM の精度向上に繋がらなかった。
- 法令や社内規程が変更となった場合に学習データの更新が必要であり、その内容の見直しに手間がかかっている。
- 不正案件に関する学習データを集めたいと思っても、実際の不正案件の発生件数が少ないため、自社データだけでは不十分。
- まず Excel ベースの業務プロセスから脱却する必要がある。

これらの課題を克服すべく、AI 活用に適したデータベースの構築と十分な学習データの確保等に向けた取組みが多くの金融機関等で進められている。例えば、社内データを一元的に収集・管理するためのプラットフォームをクラウド上で構築し、顧客管理システムと API で接続することで部門・グループ間でのデータ共有や用途に応じたデータの抽出・分析が行えるようにした先、データへのアクセス制御やデータのバージョン管理を効率的に行うソリ

[9] 例として「金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理　第２版」（2023 年 6 月公表）など。

[10] 例として「金融機関の内部監査の高度化に向けたモニタリングレポート(2024)」（2024 年 9 月公表）など。

ューションを導入した先、OCR や音声認識などによりテキストや音声などの非構造化データを解析している先などが確認された。

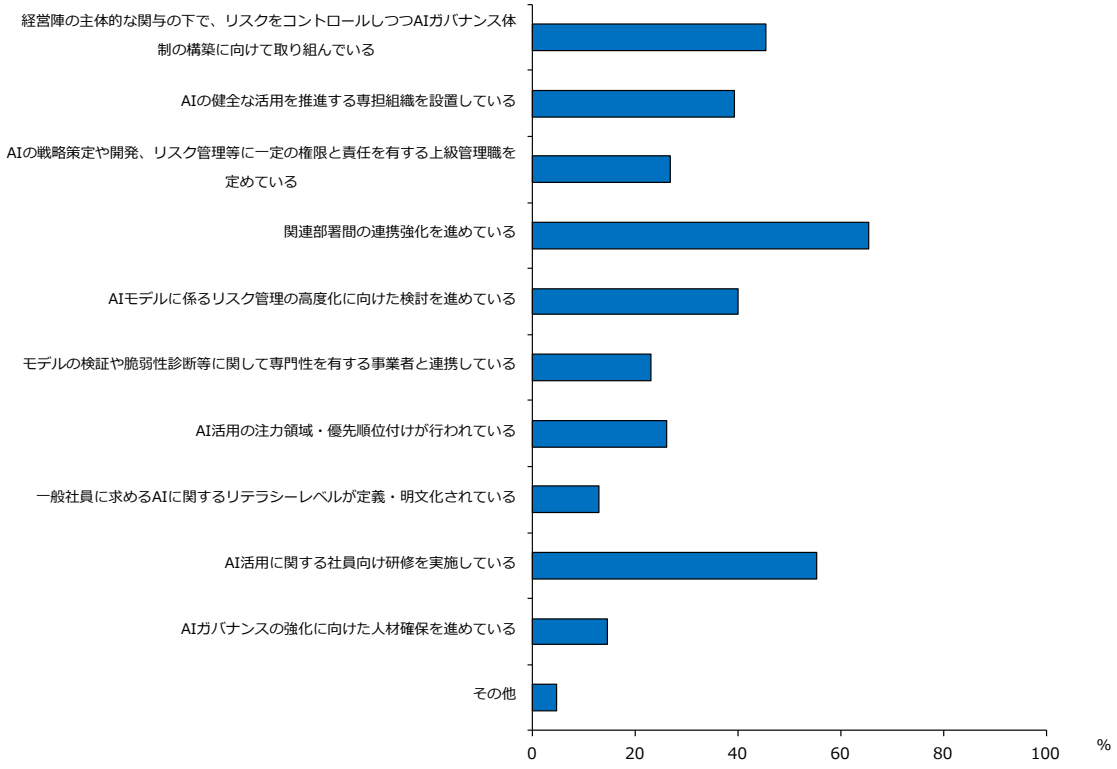
その上で、AI 官民フォーラムでは、まず、AI は“Garbage in, Garbage out”と言われるように、質の高いデータが回答の有用性に直結するため、AI 活用の前提としてのデータ整備の重要性が改めて強調された。そして、データ整備を検討するに際しては、どのような活用方法を念頭に置くのかを意識する必要があり、そうした目的を持たずにデータ整備に取り組むとコストが無駄になりかねないとの指摘がなされた。逆に、組織全体で「何のためのデータか」が理解されていれば、より精度の高いデータ入力が促されるとの指摘があった。また、データ整備に具体的に取り組むに際しては、組織内の様々なデータベースに保存されている情報をデータレイクに集めるべきか、あるいは MCP（Model Context Protocol）などの技術進展を踏まえ個々のデータベースを AI で参照できるようにして運用すべきかを見極めた上で、データマネジメントを設計・運用することの重要性が指摘された。

金融機関等は、AI を活用した業務効率化や金融サービスの高度化等の機会が拡大していることや、自社が保有する非構造化データを含む大量のデータが収益性の向上やビジネスモデルの変革に向けた重要な経営資源になる可能性があることを認識し、セキュリティを確保しつつ、データ活用基盤の整備や API 連携などを重要な経営課題の一つとして検討していく必要がある。

ii. ガバナンスの構築に向けた取組

主に全社的な体制整備に焦点を当てて、ガバナンス構築に向けた取組例を紹介したい。

【図表 13 AI ガバナンスの構築に向けた取組状況】



まず、回答した先の多くが取組んでいるものとして、関連部署間の連携強化等を通じた

AI の推進および管理体制の構築である。具体的な取組事例としては、AI の推進と関連リスクに焦点を当てたガバナンスフォーラムを設置した先や、AI リスク管理に関する規程を策定し責任者や利用者の役割、AI 固有リスクの定義、統制方針などを明文化した上で、システム部門、情報セキュリティ・コンプライアンス部門、モデル・リスク管理部門を横断した管理態勢を検討中の先などがある。

また、AI に関連するリスクが多岐に亘ることから、リスク管理部門など複数部署が協働で案件推進部署と打ち合わせを行いリスク対策状況の把握に努めていると回答した先や、今後の AI 技術の発展や一層の当社内での利活用を見据えて多角的な視点から AI リスクの評価基準の明確化等に努めている先、外部専門家から定期的に国内外のサイバーセキュリティ最新動向の報告を受ける中で AI ガバナンスについても議論していると回答した先などが確認された。

AI 官民フォーラムにおいても、AI 利活用の推進とリスク管理のバランスについて取組事例が共有された。AI は技術進展が非常に速いため、案件の立ち上げのタイミングからシステム部門や管理部門（二線）が連携してアジャイルに取り組むこととしている一方、リスク評価の観点から、事業部門（一線）と管理部門（二線）をはっきり分けるべきかを論点として意識しているとの紹介があった。その上で、管理部門（二線）や内部監査部門（三線）のリスク感性は重要だが、リスクを最初にキャッチするであろう事業部門（一線）のリスク感性を育んでいくことの必要性を指摘する意見もあった。AI 利活用の推進の観点からも、従来はデータサイエンティストなどの専門人材を専門部署に集める体制が一般的だったが、今後はより現場に近い部署で専門人材が実際に手を動かすことが必要との指摘があった。

また、リスクベース・アプローチの重要性が指摘され、社内の業務効率化などのリスクの低い AI 利用については、チェックリストに基づく現場判断に委ねつつ、顧客向けに AI を活用するようなリスクの高い AI 利用については、専門部署で事前審査を行っている事例があった。

さらに、AI 導入後の環境変化を踏まえ、リスク評価や低減策を継続的に点検・見直しし、ライフサイクル全体で適切にリスク管理することの重要性が指摘された。

この他、業界レベルでの知見共有の有用性を指摘する意見があった。各社のデータ活用部門とコンプライアンス部門が揃って意見交換することで、互いのリスク認識を学び合うことができたとの経験も共有された。こうした取組みは、業界全体のリスク対応の高度化につながりうると考えられる。

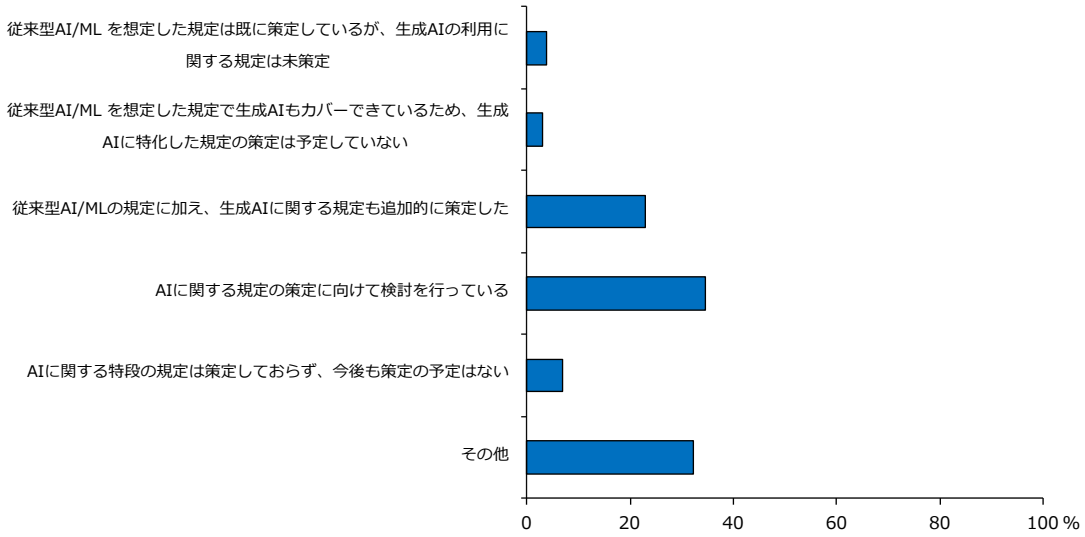
AI ガバナンスについては、攻めと守りのバランスが難しい、生成 AI は汎用性が高くサービスが画一的ではないために統制が難しいなど AI 特有の課題を挙げる先も多く、従前のガバナンス及びリスク管理のフレームワークの適用を基本としつつも、AI の利用範囲拡大と利活用の高度化にあわせ適宜見直すなど、多くの金融機関等が試行錯誤により健全な利活用に向けて検討を行っている様子が窺われた。AI に関する技術進展や社会受容度の変化に応じて AI ガバナンスが目指すゴールも常に変化していくと考えられるため、事前にルールや

手続を固定するのではなく、環境・リスク分析やゴール設定、運用、評価といったサイクルを高速で回していく「アジャイル・ガバナンス」[11]を実践することも一つの重要な考え方である。

iii. AI に関する社内ルール等の策定

従来は、情報セキュリティ管理規程やモデル・リスク管理規程など、既存の社内規程を横断的に適用することで AI に関するリスクをある程度網羅してきた金融機関等が多いが、生成 AI の高度化と普及によって、AI に特化したより具体的かつ柔軟なルール整備を急務とする声が多い。複数の金融機関からは「従来型 AI の利用実績がほとんどなかったため、その規程は策定していなかったが、今般の生成 AI 導入にあわせて新たにルールを設けた」という回答が寄せられている。また別の金融機関では「生成 AI に特化した規程（運用ルール）を策定しているが、従来型 AI を想定した全社的な規程はまだ整備されていない」としつつ、今後の拡大に対応して一本化を図る予定だという。

【図表 14 AI に関する規程等の策定状況】



海外拠点を含むグローバルな大手金融グループでは、生成 AI の登場と急速な浸透を契機に、グローバル全体での AI ガバナンス基本方針や実施基準を新たに制定し、各国の法令やガイドラインに対応する形で実施要領をローカライズする動きもみられる。また、別の金融グループでは「AI ガバナンス指針」を策定・公表した上でグループ各社に徹底を図っている。同グループでは、AI の新サービスを提供する際に、社内で作成したチェックリストを用いて AI ガバナンス指針に合致しているかを確認する運用を導入しており、「まず使ってみる」という姿勢と、倫理的・法的なコンプライアンスを両立させることを目指している。また、別の金融グループでは従来から「企業行動規範」や「モデル・リスク管理規程」を持っていたものの、生成 AI 特有のリスクには対応しきれない可能性があるとして、海外拠点や専門家との連携を通じたセキュリティチェック基準やルール改正に向けた検討を進めている。

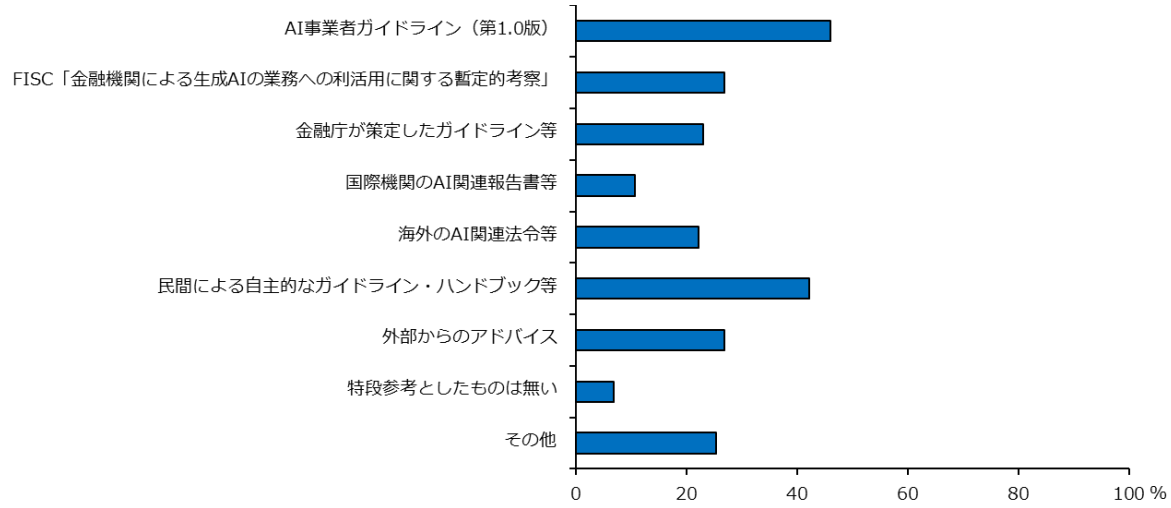
---

[11] アジャイル・ガバナンスについては、「総務省・経済産業省『AI 事業者ガイドライン』第２部　E.AI ガバナンスの構築」を参照。

一方、「既存の枠組みで概ね対応可能」とする声も少なくない。たとえば「AI 専用の規程は設けていないが、情報管理規程等に定めた内容に則って AI を扱っている」というケースや、業務単位で利用範囲を制限し、必要に応じてセキュリティ・コンプライアンス部門の承認を得る運用で足りているとする企業もある。ただし、多くの金融機関等は今後の生成 AI 活用の広がりを見据え、従来の AI を含む包括的なルールやガバナンス体制の検討に着手しており、組織横断的にモデルの全数調査を実施してパイロット的なリスク管理をスタートさせる動きが加速している。

アンケートの選択項目には盛り込んでいなかったものの、従来型 AI の規程に加えて追加的に生成 AI の規程も整備するというよりは、まずは生成 AI の導入・利用に焦点を当てた社内ルールを優先的に整備し、それを発展させて従来型 AI にも適用を広げるアプローチも目立った。

【図表 15 規程等の整備にあたり参考とした文書等】



なお、規程等の整備にあたり参考とした文書等についてみてみると、まず、多くの金融機関等が 2024 年 4 月に経済産業省・総務省から公表された「AI 事業者ガイドライン（第 1.0 版）[12]」を参考にしたと回答した。また、民間団体等による生成 AI 等に関するガイドラインや FISC 公表資料、EU 等の海外 AI 関連法令等も多く参照されており、外部専門家からのアドバイスも含め、金融機関等は様々なアプローチで規程の策定に取り組んでいる。

iv. 専門人材の確保・育成及び社内教育

複雑な AI モデルの開発・運用・管理における専門人材の確保・育成と、AI システムの利用者が増加することに伴う社内教育の必要性を多くの金融機関等が認識している。特に生成 AI においては、利用者が広範囲に及ぶため社内教育の重要性が一層増していると指摘されている。加えて、AI に対する個々人の理解度に差があることや、自分の業務が AI に代替されるのではないかとの不安感から、ユースケースのアイデア出しや部門横断的な協力体制を構築しづらいとの声も多い。

[12] 2025 年 3 月には「AI 事業者ガイドライン（第 1.1 版）」が公表されている。

また、ベンダーを活用して開発や運用を進めた場合、ノウハウや知財が組織内に蓄積されにくく、内部人材の育成が進まない懸念が根強い。データサイエンティストやエンジニアのような専門的人材だけでなく、最適なソリューションを選定し、運用・管理を継続的に行う人材、あるいは現場と IT 部門を橋渡しする役割を担う人材が不足しているといった課題が顕在化している。さらに、生成 AI 特有のハルシネーションや著作権侵害など、新たに考慮すべきリスクが増えたことで、従来の教育コンテンツだけでは十分に対応できない状況に直面しているとの意見も寄せられた。

金融機関等から寄せられた専門人材・社内教育に関する主な課題

- 社内に AI の専門人材が少なく、テーマ設定や分析設計で行き詰まることが多い。
- AI への理解度に個人差があり、ユースケースのアイデア出しが進まない。また、自身の業務が AI によって奪われるのではないかという不安から、積極的な協力を得にくい。
- 生成 AI は従来型 AI に比べて利用者の範囲が広くなるため、社内教育がより重要になると認識しているが、実務レベルでの落とし込みに課題あり。
- 開発等に外部リソースを活用する場合にはそもそも知見や知財が組織内に残らず、内部の人材育成が思うように進まない。

多くの金融機関等が本論点について大きな課題感を抱える中で、アンケートやヒアリングからは、課題解決に向けた様々な取組みが確認できた。まず、専門人材の確保・育成については、副業人材（プロ人材）に AI モデル開発の支援を仰ぎつつ OJT により内部人材育成を図っている先、システムエンジニア出身者などの社内の高スキル人材のリスキリングに取り組んでいる先、新卒専門人材の採用を拡大させている先、AI 活用推進専門チームを設立して専門人材を積極的に採用していく予定とした先などが確認された。また、一般の社員向けの社内教育としては、AI 関連の資格取得支援などの教育施策を実施している先、コールセンター職員向けの実業務に即した AI 活用事例の共有を行っている先、全社員に対して生成 AI のリスクに関する教育プログラムを導入した先などが確認された。より発展的な事例としては、内製での AI 開発・活用に向けてスタートアップとの合弁会社を設立し、グループ内に知見・知財が残る形での開発体制を構築した先も確認された。

これらの個社での取組みに加え、複数の金融機関等が参画する団体等においても人材育成に向けた取組みを行っている。特に小規模金融機関においては単独での知見の向上に限界があるため、先進的な取組みを行っている先からの知見の共有など、業界横断的な取組みが期待される分野である。AI の導入が進む中で、金融機関等に求められる人材も大きく変容していく可能性があり、重要な経営課題の一つと認識して人材育成や社内教育に取り組んでいくことが期待される。

v. 投資対効果

従来型 AI、生成 AI のいずれにおいても、金融機関等からは効果が見通しづらい本分野に関する投資対効果の説明が難しく、社内での合意形成に時間が掛かるとの意見が複数の金融機関から寄せられた。IT 投資管理プロセスの整備の重要性は、AI に限らずシステム全般に

共通する事項である。その一方で、AI システム導入に関する意見として、技術進展が速く導入したシステムが短期間で陳腐化する可能性があること、短期的には効果が限定的でも継続的な学習により精度が向上し中長期的に効果が拡大しうること、AI に対する社会受容の程度や職員の習熟度の変化により導入範囲や効果が変わりうること等の意見も寄せられた。このように、AI システムの導入で得られる効果が変動しうることが、より課題を難化させていると考えられる。また、外部事業者が提供する生成 AI については、多くの場合従量課金であるため、使用頻度によっては制限なくコストが増加していくことに将来にわたる投資対効果の見通しが難しいといった声が聞かれた。

これらの課題に対して、DX についてもみられる対応であるが、ROI（Return On Investment：投資収益率）が見えにくく各部署で予算確保が困難な場合には別途デジタル部門において予算を手当てしている先や、同じような投資を複数の部署が実行しないようにグループ全体で横串を指して案件管理を行っている先などが確認された。将来収益が得られる案件や事業であれば、ROI 等の指標を用いて評価し、進捗状況に応じてリソースの増強やサービスの縮小・撤退を判断する PDCA を回す必要がある。一方で、AI 関連投資のように実証実験（PoC）の段階や中期的な観点で対応が必要な戦略案件は、収益化の目途が立つまでの間、利用者や利用件数などの特性に応じた KPI（定量的指標）を設定して計画対比をモニタリングすることも考えられる。AI 官民フォーラムでは、これまでの DX 案件の KPI としては業務の「削減時間」が代表的だったが、業務プロセスそのものを変革する AI の評価になじまない可能性が指摘された。また、複数の定量指標を複合的に確認する必要性や、指標の測定は短期サイクルで行いつつも、その評価は長期的な時間軸で行うべきとの意見があった。

また、一部の金融機関等からは、数値だけではなく中長期的な投資目的をできるだけ可視化して経営レベルで議論・意思決定を行うことが重要といった意見も寄せられた。AI 官民フォーラムにおいても、試行的な側面がある AI 投資は必ずしも定量的な効果測定になじみにくいことから、AI ツールの利用者数や利用頻度などによる間接的な評価を行う場合が多いものの、経営のアカウンタビリティの観点からも、出来る限り定量的に効果測定する必要性が意識され始めているとの指摘があった。技術進展の速度が極めて速い AI 関連の技術やサービスの導入にあたっては、経営陣の適切な理解と主体的な関与の下で、戦略的に投資判断を行っていくことが重要である。

vi. モデル・リスク管理

AI モデルについても他のモデルと同様、適切にリスク管理を行うことが重要である[13]。その際、モデル・リスク管理に関する原則[14]の「リスクベース・アプローチ」の考えも踏まえると、AI 特有のリスクも含めてモデルに内在するリスクを評価し、その大きさに応じた管理を行うことが適当と考えられる。現状、管理の程度は金融機関により様々であるが、モデル・リスク管理に関する原則に記載のあるモデル・インベントリー管理のような、社内で

---

13 金融庁「金融機関のモデル・リスク管理の高度化に向けたプログレスレポート(2024)」（2024 年 12 月公表）参照
14 金融庁「モデル・リスク管理に関する原則」（2021 年 11 月公表）

利用する重要な AI モデルを一覧で管理するなど、一定のリスク管理態勢を準備することが考えられる。

一方で、多くの金融機関等が AI モデルの検証の困難さに直面している。従来型 AI を活用してきた金融機関等の中には、AI に関するモデル・リスク管理のフレームワークを一定程度整備済みと回答した先もあったが、そのような先であっても、体系的な性能評価指標が確立されていない生成 AI については開発・運用・管理体制の構築に向けてなお取組みの途上にある。生成 AI は、活用の汎用性が極めて高い、学習データに含まれない情報を生成し得る、同じ入力に対して異なる結果が出力されうる、基盤モデルは外部事業者により提供され頻繁にアップデートされるといった、従来型 AI とは大きく異なる特性を有しており、従来と同様の方法では全てのリスクを把握・管理しきれないと捉えている金融機関等もある。一部の金融機関からは、将来的には当局もしくは民間団体によるガイドラインの策定・更新に期待しつつも、当面は金融機関ごとに、潜在的なリスクの類型を整理し、試行錯誤しながら管理せざるを得ないといった声が寄せられた。

また、前述のとおり、AI モデルの推論結果の偏りや説明可能性の担保の困難性といった課題と関連して、モデルの潜在的なリスクを特定してリリース管理や継続的モニタリングに反映する体制の整備が不可欠であると考えている先も存在する。

金融機関等から寄せられた開発・運用・リスク管理に関する主な課題

- 生成 AI はプロンプトが同じでも出力結果が異なることがあるなど、従来の AI モデルとは異なる特性があり、より入念なテストや継続的なモニタリング、緊急対応が必要になる。
- 生成 AI は従来型 AI とは異なり性能の評価方法や評価軸が確立しておらず、また汎用性も高いため、客観性を持って性能検証をすることが難しい。その結果、体系的評価に基づき適切なサードパーティを選定することも現状困難。
- 生成 AI のモデル検証の難しさはインシデント発生時の原因調査や責任分界を明らかにしていくことの難しさにつながり、大規模なインシデント発生時には大きな混乱を生み解決を難化させる可能性があると考える。
- モデルの開発・運用管理について手動対応となっており、工数増加の原因となっている。

生成 AI を含む複雑な AI モデルに対応したモデル・リスク管理の確立に向けた取組みについて、複数の金融機関等から回答が得られた。例えば、AI モデルに適用可能なモデル・リスク管理フレームワークを整備済であり、生成型 AI についても既存のポリシー・手順・管理を継続的に強化して対応しているとした先、複数の専門ベンダーの提供するツールの PoC を行い AI モデルの精度等の検証を進めている先、前提条件・限界・不確実性などを含む AI モデルの方法論を文書化している先、モデル開発者と独立した検証者によって本番適用前の検証や継続的なモデルのパフォーマンス監視を行っている先、業務知見に基づく特徴量の追加等を行いモデルの性能維持に務めている先などが確認された。

また、AI 官民フォーラムでは、AI エージェントの広がりを見越して、現段階から AI エージェントのパフォーマンスの監視、ライフサイクルとコスト管理、インベントリー管理、

権限管理の４つを統合的に管理するプラットフォームの構築を進めているとの事例紹介があった。

上記の通り、AI モデルの管理態勢構築に向けた金融機関等の取組みは様々であり、試行錯誤をしながら検討を行っている状況が伺われた。金融庁では、国内外の AI を巡る議論の進展と AI の利用状況を踏まえつつ、適切なリスク管理が行われているかについて対話を継続していく。

vii. 適切なサードパーティの選択等

AI モデルの開発・運用・管理や生成 AI モデルのカスタマイズ等には高度な知見が求められるため、外部事業者によるソリューションやプラットフォームを活用もしくは活用を検討している金融機関等が多い。例えば、AI 導入支援を行うベンダー・コンサルティング会社や学習データを提供するデータベンダー、クラウド事業者等との連携を通じて、効率的かつ安全な AI 活用環境を構築する動きがみられ、アンケートでも、従来型 AI/生成 AI のいずれにおいても「適切なサードパーティ（外部事業者）の選択」を課題として選択した先が４割強に達した。特に、生成 AI のような複雑な AI においては、金融機関等自身がモデルを開発することは多くの金融機関等にとって現実的ではなく、必然的に外部事業者が提供する基盤モデルを利用することになる。

一方で、外部事業者へ過度に依存することの弊害について指摘する声もあり、自社のビジネス環境や業務プロセス、顧客ニーズ等を踏まえた適切な AI システムを導入するためには、外部事業者との連携においても、金融機関側担当者が AI に関する一定の知見を持っていることが必要である。また、外部事業者の適切なリスク管理も重要である。2024 年 11 月に公表された FSB の報告書[15]では、システミック・リスクを増大させる可能性がある AI 関連の脆弱性としてサードパーティ依存および特定のサービスプロバイダーへの集中を指摘している。

金融機関等から寄せられた外部事業者との連携及びリスク管理に関する主な課題

- 外部サービス利用において、諸所に従来型 AI の技術が組み込まれてきている中、それらについて適切に把握・管理することは難しい。
- システム面だけに限った場合でも、基本設計者からプログラマー、システムの維持管理者など複数の関係者が存在し、それぞれについて内製とするか、外部委託とするか（複数の事業者に委託する可能性もあり）など、個々のプロダクトごとに責任共有範囲を定めて正しく管理する必要がある。
- LLM の完全内製は不可能であるため何らかの外部サービスとの接続を要するが、外部サービスとのセキュアな通信手段の確立は課題。他社との接続点がセキュリティホール化し、社内の機密情報や顧客情報の流出や改竄を防ぐ仕組みを構築する必要がある。

これらの課題に対して、金融機関等においては、既存の外部委託等に係るリスク管理のフレームワークを適用することでセキュリティチェック等を実施しているほか、特定ベンダー

[15] 金融安定理事会（FSB）“The Financial Stability Implications of Artificial Intelligence”（2024 年 11 月公表）

への過度な依存を回避するため、オープンソース基盤を活用してモデル開発を行う例や、ベンダーに社内データ等を提供して AI モデルの開発を委託する際には、モデルの知的財産権が当社に帰属するように契約を定めている例などが確認された。また、大手金融機関を中心に、AI モデル開発・運用・管理の内製化を進める事例も確認された。

生成 AI を含む複雑な AI を利用する際に外部事業者との連携は不可欠であり、新商品・新サービスに係るリスク、システム障害リスク、情報セキュリティリスク（サイバーセキュリティリスクを含む）、経済安全保障上のリスク等の外部事業者との連携に伴うリスクに対応しつつも、自社のニーズを踏まえて適切な連携先を選定する必要がある。

viii. 情報セキュリティ・サイバーセキュリティ

金融機関等の AI の活用に当たっては、情報セキュリティ面やサイバーセキュリティ面でも様々な課題が浮かび上がってきている。一部の金融機関等からは、アンケート等を通じて「セキュリティ関連については既存の IT ガバナンス枠組みで十分対応可能」「AI サービスのアルゴリズムの多様化やリリースサイクルの違いなどの影響は軽微であり既存の業務プロセスの中で点検することで対応可能」といった見解が示された一方で、生成 AI が導入されることにより新たなリスクが発生し得るという認識も根強い。FSB の報告書においては、生成 AI 等の AI が攻撃者の能力を高め、金融セクターに対するサイバー攻撃の可能性と影響を拡大させる可能性が指摘されている。また、米国財務省が 2024 年 3 月に公表した報告書[16]においても、既存のリスク管理原則が金融機関の AI の安全な運用に関するフレームワークを提供すると指摘しつつ、AI 技術の進化はサイバーセキュリティの脅威を増大させ、金融機関はこれまで以上に警戒を強めなければならない状況にあると強調されている。そこで、本節では、特に生成 AI に特有の論点を中心に取り上げたい。

まずは、情報漏洩リスクが挙げられる。前節において個人情報保護の観点でも取り上げたように、金融機関等が生成 AI を活用する際、顧客情報や業務上の重要情報を意図せず外部に漏洩させるリスクが存在する。また、クラウド型 AI サービスと連携する場合、機密情報や顧客情報がサービス提供元に送信される可能性があり、プロンプトや出力内容がベンダー側の学習に利用されるリスクも懸念されている。とりわけ海外にサーバーを置くプラットフォームを用いる場合、データの海外移転の管理も重要な課題である。これらのリスクへの対応として、機密情報や個人情報の入力をシステム上で自動的に制限する仕組み（マスキング等）を検討している先もあるが、完全にブロックできるわけではなく、最終的には従業員教育や運用ルールの徹底に頼らざるを得ないとの意見が寄せられた。

また、プロンプトインジェクションのような攻撃は、AI システムの誤動作や機密情報の漏洩を引き起こす可能性がある。生成 AI によって巧妙なフィッシングメールやなりすましが容易に作成されるだけでなく、AI モデルそのものが攻撃対象となる可能性があり、具体的には、AI モデルの学習データやパラメータを改ざんする「データポイズニング」への警戒や、大量のクエリを投げてモデルの内部構造を推測し、機密情報を引き出す攻撃に対する

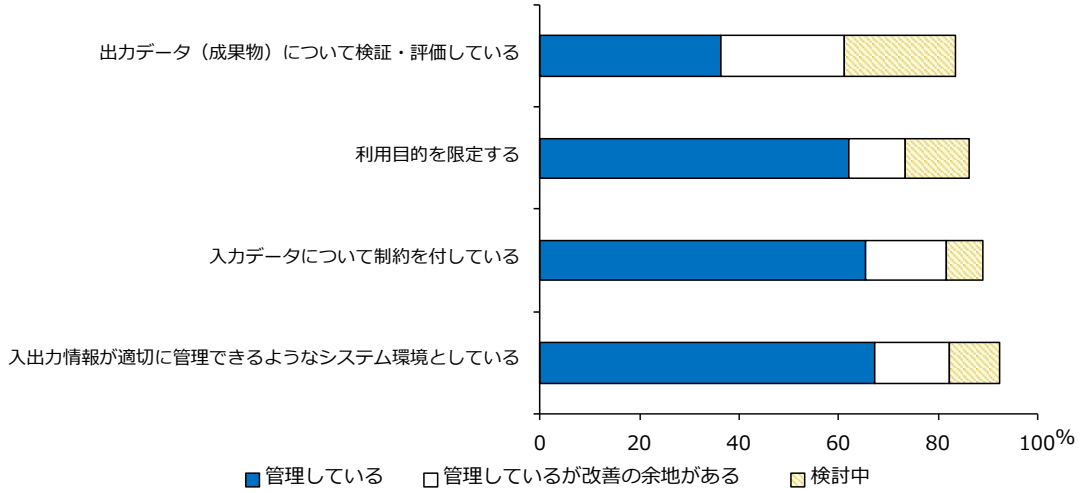
---

[16] U.S. Department of the Treasury “Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector”（2024 年 3 月公表）

検知・防御策が求められている。加えて、FSB 報告書でも、生成 AI がマルウェア開発やなりすまし、ソーシャルエンジニアリング等を支援し、金融の安定性を損なう可能性がある点に懸念が示されている[17]。

一方で、これらの課題への対応も一定程度進展している。例えば、個人情報保護の項目でも触れたように、機密情報のデータ利用は不可とするなど、プロンプトの入力データについて一定の制約を付している先が大半であることが確認された。また、自社専用環境にて生成 AI サービスを導入するなどにより、入出力情報が管理できるシステム環境を構築している先も同様に多数確認された。さらに、出力データの検証・評価に係る仕組み・手法やルールを第 1 線と第 2 線が連携して策定し、企画・開発段階での検証を行うと共に、運用フェーズにおいては人の目とシステムの双方で出力データを常時モニタリングする態勢の構築を検討していると回答した先もあった。

【図表 16 生成 AI 利用に関するコントロール】



このように、多くの金融機関等において一定のガードレールを導入していると考えられるが、「ガードレールを実装しているものの、生成 AI チャットボットへの敵対的入力を完全には阻止できない」といった課題感も共有されている。加えて、AI の広範な普及により、従業員個人や業務部門が組織の許可を得ずに外部の AI サービスを使用する「シャドーIT」の利用が増加する可能性もあり、情報漏洩や不正アクセスなどのセキュリティリスクを増幅させる恐れがある。

総じて、金融機関等が AI を導入・運用する際の情報セキュリティ面の課題は多岐にわたるため、AI モデル固有の脆弱性への継続的なモニタリングといった組織的対応が不可欠であり、今後も生成 AI の普及とともにより高度なセキュリティ手法の整備が求められる。加えて、生成 AI のアウトプットがハルシネーションや著作権侵害に該当しないかをモニタリングする必要がある。こうした多面的なリスクに対応するため、セキュリティ部門だけでなく法務・コンプライアンス部門やモデル・リスク管理部門と連携し、定期的に脆弱性診断やペネトレーションテストを実施する、リスクに応じて内部監査部門による監査を実施するな

[17] なお、公益社団法人金融情報システムセンター（FISC）が 2024 年 9 月に公表した文書においても、情報セキュリティ面に関する課題として、情報漏洩、仕様・設定等、モニタリングの 3 点に関する課題を指摘している。

ど、統合的な対応を講じる必要がある。

一方で、FSB や米国財務省の報告書でも指摘されているように、AI はサイバーセキュリティの強化に資するものでもある。例えば、大量のデータをリアルタイムで分析し、異常なパターンや不正活動を検知することで、攻撃、マルウェア、詐欺等を早期に発見できる。また、AI でインシデント情報を迅速に分析し、適切な対応を行うことができれば、インシデントの影響を最小限に抑え、早期復旧を支援することにも繋がる。他方で、AI の活用に当たっては AI の深い理解と専門知識が必要であり、金融機関等は AI 技術の発展とセキュリティ強化を両立させる戦略を策定し、実践する必要があると考えられる。

ix. 金融犯罪対策

生成 AI の進展により、自然な日本語での文面・音声・映像を生成できるようになったことから、犯罪の手口が巧妙化し、金融機関等やその顧客を取り巻くリスクも拡大する傾向にある[18]。例えば、AI が生成したメールやフィッシングサイトによる詐欺など、これまでも見受けられた手口が巧妙化することに加え、ディープフェイク技術は、特定の人物になりすました偽動画や偽音声等による詐欺行為を容易にし、その影響は甚大となる可能性がある。このほか、偽の証明書類や虚偽の取引情報をあたかも本物のように提示する詐欺行為も想定される。金融機関等における対策という観点からは、従来の KYC 手続や認証システムでは実在の人物との見分けが困難になり、本人確認をすり抜ける可能性が指摘されている。

このように、生成 AI の高度化は、既存の金融犯罪対策では想定していなかった新たな手口を数多く生み出す可能性があり、単に個々の技術対策を導入するだけでは対応しきれない規模の脅威をもたらしかねない。金融機関内部の監査部門やコンプライアンス部門が備えている仕組みや人材も、想定外の速度・巧妙さで繰り返される不正行為に追随できるかどうかが懸念され、結果として金融機関全体の信用や金融システムの安定性を損なうリスクも否定できないことから、金融庁・金融機関等ともに、こうしたリスクにも留意することが重要である。

② 個々の AI システムに係る課題・取組事例

i. 説明可能性の担保

従来型 AI においても、ディープラーニングなどアルゴリズムの複雑さゆえに推論（出力）の根拠を理解・説明することが困難な「ブラックボックス化」の問題は指摘されてきた。与信判断など、その影響（リスク）に照らして重要な判断に AI を用いる場合、当該 AI の性質に応じて、どのようなデータで学習したか、RAG 等を利用する場合どのようなデータを参照したか、どのようなプロンプトが与えられたか、出力結果の記録とモニタリングが機能しているかといった観点から、金融機関自身が判断の合理性を検証・説明できるようにする必要がある。

生成 AI では、従来型 AI と比較してさらに説明可能性の担保が難しいという声が多い。膨

[18] 警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2024 年９月公表）

大なパラメータを用いた複雑な学習プロセスと、テキストや音声、画像などマルチモーダルな入力に応じて動的に出力を生成するという仕組みであり、個々の推論について「なぜその回答になったのか」を明示的に示すことが極めて難しくなる。このため、生成 AI の活用を模索する金融機関等の多くは、説明可能性の欠如という問題への対応が大きな課題となっている。

金融機関等から寄せられた説明可能性に関する主な課題

- ディープラーニング等のモデルを利用すると、結果の出力過程がブラックボックス化してしまい、異常データを検出した際の内部監査上の対応が困難なことがある
- 営業店に AI が推奨した推進先リストを提示しても、なぜ推奨されるかがわからないと優先的に推進してもらえない、利用されなくなってしまうといった可能性がある
- 生成 AI は従来型 AI よりも生成過程がブラックボックス化するため、意図しない形で著作権を侵害してしまうケースや、ハルシネーションによって誤った情報を従業員に提供してしまうリスクに配慮を要する。

生成 AI のような複雑な AI モデルにおいて説明可能性を担保することは容易ではないが、従来型 AI モデルへの対応も含めて、課題解決に向けた一定の取組みが確認された。例えば、外部事業者の AI モデル評価ツールを活用し、与信審査モデルにおいてどのパラメータの寄与度が大きいかを可視化してモデルの妥当性を検証している先、不正リスク検知モデルの説明可能性を向上させる技術を開発中とした先、営業の推進先リストに判定根拠となる列を追加して納得性を担保した上で利用させている先などが確認された。

もっとも、膨大なパラメータを有する生成 AI で完全な説明可能性を確保するのは極めて困難であり、ユースケースに応じて、顧客や社員など関連するステークホルダーの納得感を確保することが重要であると考えられる。納得感には、AI に対する社会受容の程度も影響すると考えられるため、金融機関等においては、AI を利用する際のユースケースやリスク、社会的文脈を踏まえつつ、必要かつ技術的に可能な範囲で情報提供を行っていくことが重要である。

ii. 公平性・バイアス

従来型 AI を顧客向けサービスに利用する場合、十分な学習データが不足する中で学習を行った場合や、利用する学習データ自体が特定の地域や属性に偏った情報を多く含む場合など、学習データやアルゴリズム、さらにはモデルの推論結果に偏りが含まれると、特定の属性を持つ顧客に対して構造的な差別その他の不公平な処遇が行われるリスクが高まる。生成 AI や AI エージェントは、多くの場合、汎用モデルを使用しており、モデル自体に起因する不公平性は相対的に生じにくいが、プロンプトや参照データに起因する不公平性は生じうる。これらの問題は、前節で触れたクレジットスコアリングなどの消費者向けサービスだけでなく、例えば人事評価や採用といった社内業務においても発生し得るため、総体として金融機関等の信用力や社会的責任に影響を及ぼす可能性がある論点といえる。

これらの課題への対応として、外部事業者が提供するモデル評価ツール等を活用してモデ

ルに内在するバイアスを早期に検知し、対処するためのフレームワークを確立することが重要であるとの指摘もある。ただし、具体的にどのような評価指標や監査プロセスを構築すべきかが必ずしも明確ではない中で、バイアス検出ツールが多種多様であり、その正確性や運用コストを見極めるのが難しいといった声も上がっている。そのため、AI モデルのバイアスを早期に検知し、対処するための一貫したフレームワークを確立することが課題となっている。また、過去のデータを学習データとして構築した AI モデルに公平性・バイアスの観点から問題が確認された場合、過去の判断において同様の問題が発生していた可能性があり、これをきっかけに既存のビジネスプロセスの見直しに繋げていく視点も重要である。

iii. ハルシネーション（幻覚）

「ハルシネーション（幻覚）」と呼ばれる、実際のデータに基づかない出力が生成される事象が大きな課題として認識されている。誤った情報を提示したり、信用リスクや法的リスクに直結する回答を誤って生成したりしてしまうと、当該金融機関等の信頼性を損ないかねない。前章で言及したように、ハルシネーションを抑制するために RAG やファインチューニングにより回答精度を高めようと模索している金融機関等が多いが、参照データの整備やモデルの学習データの最新化が不十分だと、ハルシネーションの抑制が難しくなるとの指摘がある。特に、RAG を活用する場合でも、業務設計が適切でないと参照元の選定が不十分となり精度が上がらず、虚偽の出力が排除できないまま運用されるリスクが残ると指摘されている。

さらに、内部利用に加えて、従業員が生成 AI を用いて対外的に回答する際に、誤情報をそのまま伝えてしまうリスクをどのように緩和するかという課題も浮上している。現時点では、システム上での制御だけでなく、利用者の教育やプロンプトの作り方を含めた運用ルールの導入が必要との声もある。

金融機関等から寄せられた主な課題

- ハルシネーションの影響がゼロにはならないことから、人間がチェックするプロセスの導入や生成 AI の不確実性をいかに職員に理解させるかが重要。
- RAG やファインチューニングにおいては、学習データに古い情報が多く混在していると、古い情報の出現回数の方が多いため、ハルシネーションが起きやすい。

顧客向けサービスでの利用など、生成 AI をより発展的に活用しようとする場合においてハルシネーションは避けて通れない課題であり、多くの金融機関において対策が試みられている。典型的には、人間の関与を前提とした業務プロセスの構築で、ハルシネーションがゼロにはならないとの前提の下、生成 AI の導入に当たっては人間によるレビューのプロセスを設定している先が多い。例えば、社員が生成 AI の生成結果をもと顧客や代理店等に回答する場合は、必ず内容の是非を社員が判断してから利用することとしている先などが確認された。また、ハルシネーションを抑制するため、RAG やプロンプトに工夫を行うことにより、根拠となる文書を回答に含めることで根拠の裏付けを確認できるようにしている（検索した結果情報が見つからない場合にはその旨回答させる）先なども確認された。

このように、現時点では RAG などを組み合わせてハルシネーション対策を施した場合でも、人の判断が必要との認識を有している金融機関等が多く、抑制的な利用が中心となっている。他方、人間が誤った判断を行うこともあり、厳密なルールに基づいて動作する従来の AI システムと同様に「AI は絶対に誤ってはならない」といった極めて高精度の要求水準を AI に課すことは適切ではないとも考えられるため、AI に対する社会受容の程度（レピュテーションリスクの大きさ）や技術進展、ユースケース等を考慮し、過度に委縮することなく生成 AI の活用を模索していくことが期待される。金融庁においては、技術進展の動向や国内外の議論等を踏まえ、金融機関等により適切な対応が行われているかについて対話を継続していく。

Box 4. 顧客向けサービスを念頭とするリスク低減に向けた取組事例

これらの課題を認識した上で、AI 官民フォーラムでは、社内の業務効率化にとどまらず、AI を活用した顧客向けサービスの展開を考える金融機関から、リスク低減に向けた取組みの検討状況が共有された。その内容から、具体的に AI をどのように用いるかに応じてリスクの態様や対応は変わりうるが、一定の共通的な目線が形成されつつあることが明らかになった。

- まず、顧客向けサービスへの活用を検討する AI システムの設計と事前のテスト・検証の観点での対応が検討されている。
  例えば、生成内容の不確実性やハルシネーションといった AI の技術的特性に対応するため、システムプロンプトや RAG による回答内容の制御やより高度な LLM の選択、ファインチューニングなどによる対応が具体策として挙げられた。また、特に、投資勧誘に際して「必ず儲かる」といった断定的な判断を示したり、コンプライアンス上不適切な回答を行ったりすることを防止するため、上記に加えて、回答内容にフィルタリングを設けるなどの重層的なガードレールを設定することが検討されている。更に、サービス設計の観点では、特にサービス導入期において、AI が対応するサービスと人間が対応するサービスを利用者が選択できるようにすることや、事務的な手続などから AI の活用を始め、リスクや対応に関する知見を蓄積しながら、金融取引などの中核的な業務にも AI の適用領域を広げていくアプローチを採ることなどが示された。そして、これらの対策が的確に機能しているかをリリース前にしっかりとテスト・検証することが重要となる。
- 次に、顧客への適切な説明・注意喚起の観点である。
  例えば、顧客が生成 AI サービスの利用を開始する前に、以後は生成 AI による回答であることや、生成 AI の特性上誤りが含まれうること等について注意喚起を行うことが挙げられた。また、顧客の理解が不十分なまま AI との対話が進んでしまわないよう、テキストのみならず動画や図解などを用いた直感的に理解しやすい回答を用意することや、予め顧客との対話にいくつかのフェーズを設け、フェーズごとに顧客の理解を確認するステップを踏まない限りは次のフェーズに進まない設計とすることなどが検討例として示された。また、顧客に回答の根拠・情報ソースを明示する設計とすることや、顧客の選択によりいつでも AI 対応から有人対応へ移行できるようにすることも挙げられた。
- また、AI による回答を含む運用状況の記録・モニタリングも共通的な観点として挙げられた。
  例えば、リスクの高い場面を中心に、AI と顧客との会話ログを保存し、不適切な回答がなされていないかのモニタリングと必要な場合に顧客にフォローアップの連絡を行う態勢を整えることが考えられる。また、AI により特定の金融商品に偏った勧誘等を行っていないか等

の客観的な数字を用いた確認・検証や、推奨ロジックの文書化と第三者レビューを通じたモニタリングも考えられる。モニタリングを通じて AI モデルやサービス設計に改善すべき点が見つかれば、適時に改善につなげていく態勢も重要である。

- そして、組織全体としてこれらの対応を行うガバナンスの観点である。
  AI ガバナンスについては本章①でも記載しているが、まず、経営陣を含む全社的な体制の整備と、現場職員に至るリテラシー向上の必要性が指摘された。また、AI の用途等に応じたリスクベースのアプローチが重要であることや、AI のように技術進展が著しく不確実性が高い領域にあっては、事前にルールを設定することは困難であるため、達成すべきゴールを明確化した上で、ライフサイクルを通じてリスクマネジメントを行うアジャイルなガバナンスが必要となることが指摘された。

iv. 個人情報保護

生成 AI により課題が難化したと感じている金融機関等が最も多かったのが個人情報保護であり、AI の開発・運用・管理を行う上で個人情報保護は様々な場面で論点となる。

例えば、2024 年 11 月の実態調査においては、①学習データとして自社の顧客情報を含む個人情報を扱う場合や、②生成 AI の利用時に顧客情報等の個人情報を含むプロンプトを入力する場合の規律の適用関係がわかりにくいとの声がある。さらに、③AI モデルの開発や学習を外部ベンダーに委託する際における規律の適用関係や、④海外にサーバーを置く生成 AI プラットフォームを利用する場合における規律の適用関係についてもわかりにくいとの声があった。

このように、規律の適用関係が明確ではない点を課題として捉えている金融機関が多いが、AI 官民フォーラムでは、専門家から以下のような見解が示された。

①については、AI モデル開発のための学習データとして利用することを利用目的として明示することを要するかが論点となるが、「「個人情報の保護に関する法律についてのガイドライン」に関する Q&A」において、統計データへの加工を行うこと自体を利用目的とする必要はないとされている[19]ことが参考となり、個別事情にはよるものの、AI の開発・学習についても、この Q&A の趣旨に鑑み、利用目的への明記は不要と整理できる場合がありうる。一方、AI の利用（推論）を利用目的として明示すべきかについては、当該取扱いを顧客が合理的に予測・想定できるかが重要なポイントとなる。チャットボットのように顧客が認識可能なものや、従来業務の単なる自動化は、予測・想定可能と評価できる場合が多いと考えられる。

②については、通常、生成 AI サービスは、プロンプトとして入力された顧客情報等の個人情報を用いて分析等の処理を行うことから、生成 AI サービスの提供者を個人データの取扱いの委託先として管理する必要がある。サービスの選定・契約締結に当たっては、金融機

[19] 個人情報保護委員会「「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ」（令和７年７月１日最終改正）2-5。

関が委託に伴って提供する個人データが、当該金融機関の指示なく追加学習に使用されないこと等を確認する必要がある[20]。

③については、AI モデルの開発等を外部委託する場合に、当該開発等に必要な個人データの取扱いを含めて委託する場合には、必要かつ適切な委託先管理が必要である。

④については、いわゆる越境移転規制（個人情報保護法第 28 条第 1 項）は、受領者が「外国にある第三者」である場合に適用されるものであり、サーバー所在地ではなく AI 事業者の所在地を軸に検討することとなる。もっとも、いわゆる基準適合体制（個人情報保護法施行規則第 16 条等）や安全管理措置としての外的環境の把握[21]においては、サーバーの所在地を考慮する必要がある。

これらの課題への対応として、アンケートやヒアリングから確認できた取組みを紹介する。まず、個人情報を生成 AI サービスに入力しないことを徹底するために、個人情報保護委員会からの通達を含めて社内の事務連絡文書にて全職員へ注意喚起している先や、顧客情報の入力をシステムで自動的に制限できないか検討を行っている先などが確認された。また、入力したデータが再学習に使われるのを防ぐために、専用区間を設けてデータが再学習に利用されない環境を構築している先や、外部ベンダーやシステムと連携する際に適切な契約書や覚書を取り交わしてデータの取扱範囲等について明文化している先が認められた。事故やインシデントが発生した場合には速やかにトレースできるようログ管理を徹底している先や、プロンプトの入力内容等の監視運用を効率的かつ正確にできるよう検討していると回答した先もあった。

また、AI 官民フォーラムでは、匿名化・仮名化、秘密計算、連合学習などのプライバシー強化技術（Privacy Enhancing Technologies, PETs）の紹介があった。PETs は、AI の開発及び／又は利用に適用可能なものも多く、AI 利活用に当たって採り得る技術的安全管理措置の一つと考えられる。

金融機関等においては、個人情報保護に係る適切な対応と個人情報を含むデータの効果的な活用の両立が求められており、金融庁としても、継続的な対話を通じて金融機関の取組みの把握を行っていく。なお、個人情報保護法のいわゆる 3 年ごと見直しにおいては、統計作成等、特定の個人との対応関係が排斥された一般的・汎用的な分析結果の獲得と利用のみを目的とした要配慮個人情報の取得等については、統計作成等のみに利用されることが担保されていること等を条件に、同意取得を不要とする改正が検討されている。こうした改正が成立した場合には、金融庁においても、当該改正の趣旨を踏まえて必要な対応を検討する。

v. 規制対応

AI 官民フォーラムでは、AI の活用を考えた際に論点となりうる規制対応上の検討事項が挙げられた。

---

[20] 個人情報保護委員会「生成 AI サービスの利用に関する注意喚起等」（令和 5 年 6 月 2 日公表）。
[21] 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」（令和 7 年 6 月最終改正）10-7

例えば、証券会社が、顧客属性や過去の取引データ等に加えて、顧客との会話データ等を生成 AI にインプットした上で、生成 AI の出力を営業員による営業支援に活用したり、生成 AI が直接顧客に投資商品を推奨するサービスを提供したりすることを想定し、以下のような検討事項が挙げられた。

第 1 に、証券会社がシステム関連の子会社に AI システムの開発を委託する際、顧客との会話データ等を提供する必要があるが、非公開情報の授受規制（金商業等府令第 153 条第 1 項第 7 号）に抵触しないよう、当該会話データ等から非公開情報を事前に除外しておく必要がないかという論点である。

この点に関しては、「電子情報処理組織の保守及び管理を行うために必要な情報を受領し、又は提供する場合」（電子情報処理組織の保守及び管理を行う部門から非公開情報が漏えいしない措置が的確に講じられている場合に限る。）（同号ト）が例外として規定されており、この「電子情報処理組織の保守及び管理」には、システム開発も含むと従前より解釈されているため、必ずしも AI システムの開発に必要な顧客との会話データ等から非公開情報を事前に除外しておく必要はないと考えられる。

第 2 に、顧客との会話データ等には法人関係情報が含まれている可能性が否定できないため、当該会話データ等を分析する者（データサイエンティスト等）にアクセス権限を付与することは法人関係情報の管理態勢として適当かという論点である。

この点に関しては、証券会社は、法令上、「その取り扱う法人関係情報に関する管理又は顧客の有価証券の売買その他の取引等に関する管理について法人関係情報に係る不公正な取引の防止を図るために必要かつ適切な措置」を講じる必要があり（金商業等府令第 123 条第 1 項第 5 号）、また、自主規制規則上、「法人関係部門について、他の部門から物理的に隔離する等、当該法人関係情報が業務上不必要な部門に伝わらないよう管理」すること（日本証券業協会「協会員における法人関係情報の管理態勢の整備に関する規則」第 6 条第 1 項）等が要請されている。

具体的な法人関係情報の管理態勢のあり方については、AI を活用する場合においても、日本証券業協会が示す考え方[22]やこれまでの実務の積み上げなどが引き続き参考になると考えられる。会話データ等を分析する者（データサイエンティスト等）にアクセス権限を付与することをもって直ちに法人関係情報を適切に管理する態勢が整備されていないと判断されるものではないが、管理態勢の適切さは個別具体的な事案に即して実質的に判断する必要があり、まずは、金融機関において AI・データ利活用の目的や態様、情報管理手続等を具体的に特定する必要がある。その上で、今後の AI 活用の進展により AI のユースケースがより明確なものとなり、それに伴って法人関係情報の管理態勢のあり方について AI 特有の論点が具体化されることも見据え、業界内でも、プラクティスの共有や考え方の整理を進めようとする動きが出始めている。

第 3 に、今後、生成 AI ベースのシステムが顧客に直接金融商品の推奨等を行う場合の規

---

22 日本証券業協会「「協会員における法人関係情報の管理態勢の整備に関する規則」に関する考え方」（2022 年 6 月 22 日）

制のあり方についてであるが、金融商品取引法上の行為規制が適用される「勧誘」とは、一般に、金融取引への誘引を目的として特定の利用者を対象として行われる行為と解されており、AI を活用する場合においても同様の考え方が妥当するものと考えられる[23]。AI 活用の「勧誘」への該当性は、個別具体的な事案に即して実質的に判断する必要があり、まずは、金融機関において AI・データ利活用の目的や態様、顧客への働きかけの内容等を具体的に特定する必要がある。その上で、今後の AI 活用の進展により AI のユースケースがより明確なものとなり、それに伴って「勧誘」への該当性についての AI 特有の論点が明らかになった場合には、AI が投資家の判断に与える影響や AI への営業担当者等の関与の度合いなどを踏まえ、具体的な検討を行うことが考えられる。

既存の法令等は AI など特定の技術を利用しているか否かに関わらず適用されるものであるが、証券分野以外においても、AI の活用を考えた際に論点となりうる規制対応上の検討事項については、今後の AI 活用の進展により事業者による具体的な AI のユースケースの特定や論点の深度ある検討が進められ、当局・事業者団体がオープンに対応することにより、個別の論点ごとに解釈や目線の提示、業界レベルでの知見共有やプラクティス形成が進展していくことが期待される。

③　その他の金融システム安定上の論点

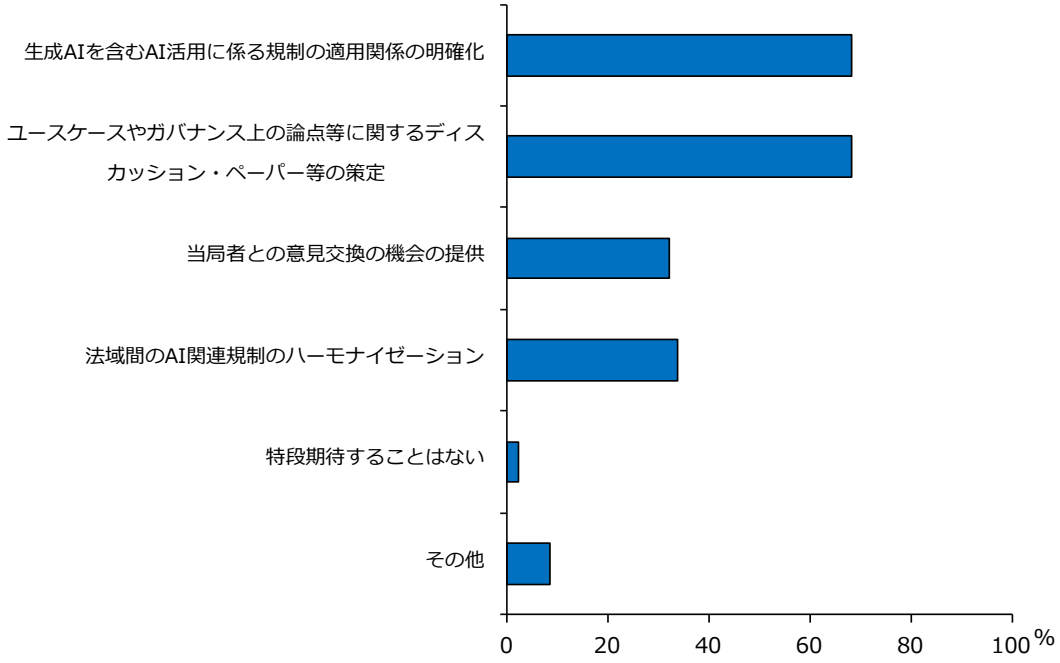
生成 AI など複雑な AI システムがもたらす金融安定への影響についても国際的に議論が進展しており、FSB の報告書においては、具体的な金融安定上のリスクについて言及している。特定のサードパーティへの依存やサイバーセキュリティ、モデル・リスク管理など既に言及した論点に加えて、金融市場の不安定化に繋がるリスクが指摘されており、例としてハーディング（群衆）効果が挙げられる。金融市場における AI の広範な採用は、AI 生成のシグナルに基づいて市場参加者が同様の決定を下す群集行動を引き起こす可能性があり、市場のボラティリティとシステミック・リスクを増幅させる可能性があると指摘されている。また、生成 AI によってフェイクニュースを生成して SNS 等で流布させることで、短期間での取り付け騒ぎや株価急落などを引き起こす可能性があり、市場全体の不安を高めるリスクもある。これらの論点については、今後も FSB 等において検討が進められていく見通しであり、金融庁としても議論に参画し、必要な対応について検討していく。

[23] 「はじめに」に述べたとおり、既存の法令等は AI など特定の技術を利用しているか否かに関わらず適用されることに留意すべきである。

2. 今後の取組みの方向性

本節においては、前節までに整理した論点に加え、アンケートで示された金融庁に対する事業者からの要望や政府全体の AI に関する取組方針、国際的な議論の動向などを踏まえ、金融庁の今後の取組みの方向性及び金融機関等に当面期待する事項について整理した。

【図表 17 金融庁に対する主な要望】



① 金融庁の対応

i. 政府等における直近の対応

我が国では、サイバー空間とフィジカル空間を高度に融合させたシステム（CPS：サイバー・フィジカルシステム）による経済発展と社会的課題の解決を両立する人間中心の社会というコンセプトを実現するため、2019 年 3 月に「人間中心の AI 社会原則」が策定された。その後、AI がもたらすリスクの多様化・増大が進む中で、2023 年 10 月の「広島 AI プロセスに関する G7 首脳声明」も踏まえ、AI の安全安心な活用が促進されるよう、AI ガバナンスの統一的な指針として金融機関を含む事業者（AI 開発者・AI 提供者・AI 利用者）を対象とした「AI 事業者ガイドライン」が 2024 年４月に策定された。

加えて、2024 年８月、AI 戦略会議のもとに「AI 制度研究会」が設置され、「イノベーション促進とリスク対応の両立」と「国際協調」に焦点を当てて具体的な制度・施策の方向性を示した中間とりまとめが 2025 年２月に公表された。「世界で最も AI を開発・活用しやすい国」を目指して政府の司令塔機能の強化や戦略の策定が掲げられているほか、安全性の向上等に向けた取組みの重要性も強調されている。イノベーション促進とリスクへの対応を両立させる観点から、法令とガイドライン等のソフトローを適切に組み合わせ、基本的には事業者の自主性を尊重し、法令による規制は事業者の自主的な努力による対応が期待できないものに限定して対応していくべきこと等が掲げられている。また、一部の金融サービスを含

む国民生活や経済活動の基盤となるインフラやサービス（基盤サービス）等については、引き続き、各業所管省庁が既存の法令あるいはガイドライン等の体系の下で対応すべきであることや、新たなリスクが顕在化し既存の枠組で対応できない場合には、関連する枠組の解釈を明確化した上で、制度の見直しあるいは新たな制度の整備等を含めて検討すべきであること等が示されている。

また、2025 年 5 月には「人工知能関連技術の研究開発及び活用の推進に関する法律」（AI 推進法）が成立し、2025 年 9 月に人工知能戦略本部が設置された。2025 年 12 月には、「人工知能基本計画」（AI 基本計画）及び「人工知能関連技術の研究開発及び活用の適正性確保に関する指針」が決定された。このうち AI 基本計画では、3 つの原則として、イノベーション促進とリスク対応の両立、アジャイルな対応、内外一体での政策推進を掲げるとともに、4 つの基本方針として、AI 利活用の加速的推進、AI 開発力の戦略的強化、AI ガバナンスの主導、AI 社会に向けた継続的変革を掲げている。

金融分野における主な取組みとしては、まず、日本銀行は、2024 年 10 月に「金融機関における生成 AI の利用状況とリスク管理 ―アンケート調査結果から―」（前掲）、2025 年 9 月に「金融機関における生成 AI の利用状況とリスク管理―2025 年度アンケート調査結果から―」を公表し、取引先金融機関に対するアンケートや IT ベンダー・金融機関等との意見交換の内容も踏まえ、金融業界における生成 AI の利用の現状と課題、リスク管理上の論点などを整理している。加えて、金融情報システムセンター（FISC）は、2024 年 9 月に「金融機関による AI の業務への利活用に関する安全対策の観点からの考察」を公表し、当該考察での整理を踏まえ、2025 年 3 月に、「金融機関等コンピュータシステムの安全対策基準・解説書」において AI を対象とする基準項目を追加する改訂を行っている。

ii. 国際的な議論の動向

アンケートで「法域間の AI 関連規制のハーモナイゼーション」を期待する回答が多かったことも踏まえ、ここでは国際組織や主要法域における AI 関連規制動向を概観する。

まず、金融分野における AI の影響については G20 においても高い関心が寄せられており、2024 年 2 月に開催された G20 財務大臣・中央銀行総裁会議においては、AI 等のデジタルイノベーションがもたらす恩恵と脆弱性を理解することの重要性が強調された。G20 からの要請を受けた FSB は、AI の金融安定上のインプリケーションに関する報告書を 2024 年 11 月に公表し、G20 首脳に提出した（前掲）。これは、生成 AI を含む AI の急速な進展と金融セクターにおける AI の利用拡大を踏まえ、2017 年 11 月に公表した FSB の報告書を更新する形で、AI が金融安定に及ぼす潜在的な影響について分析したものである。同報告書においては、今後の取組みとして、基準設定主体（Standard Setting Bodies，SSBs）や各国当局に対して、モニタリングの強化やデータギャップへの対応、既存の規制枠組みの有効性の評価、当局間での連携などを慫慂している。その後、FSB は、2025 年、モニタリングに焦点を当てた報告書を公表した[24]。SSBs の一つである IOSCO（証券監督者国際機

[24] FSB “Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector”（2025 年 10 月公表）

構）は、投資家保護、市場の健全性等の観点から、2025 年 3 月、新たな AI 技術に関する市場参加者の使用事例、潜在的な政策対応を検討する上での問題、リスク、課題をまとめた報告書を公表した[25]。その他の SSBs（BCBS、IAIS、IFIAR 等）においても、AI 関連の議論が進展している。

ここからは、主要法域における AI 関連の取組みについて概説する。まず、EU では、2024 年 6 月、包括的な AI 規制立法である AI 法（EU Artificial Intelligence Act）が成立した。AI 法では、AI システムはそのリスクに応じて分類され、リスクの高い AI システムにはより厳しい要件を適用することとされている。金融機関も AI 法の適用対象とされており、EU ないし加盟国の金融監督当局が、EU の既存の金融サービス法令との整合的な規制の適用・執行を確保することが想定されている。2024 年 6 月から 9 月にかけ、欧州委員会は、既存の金融規制及び AI 法の効果的な実行を目指し、金融サービスにおける AI の利用や影響等について、意見公募を実施した。AI 法制定後、欧州委員会が、禁止行為に関するガイドライン、汎用 AI モデルの提供者に関する行動規範等を採択したほか、欧州保険・企業年金監督局（EIOPA）が保険分野における AI ガバナンスに関する意見書[26]を、欧州銀行監督局（EBA）が銀行分野における AI 法の適用に関する簡易なガイダンス[27]を公表した。EBA は、今後、欧州委員会と協力し、既存法令の適用関係を整理するとしている。一方で、欧州委員会が 2025 年 11 月に公表した法案[28]は、「より簡素で迅速な欧州」の方針に従い、金融機関に適用されるハイリスク AI 規制の施行の延期を提案している。

英国では、政府が、2023 年 3 月にイノベーション促進的な AI 規制へのアプローチに関する白書を公表し、同白書に寄せられた意見に対し、2024 年 2 月に回答書を公表した。これらにおいて、英国政府は、AI がもたらすリスクに対して、現時点では立法によらず、セクター別の規制当局が既存の法律や規制に従い、その権限の範囲内において、安全性を始めとする 5 つの分野横断的な原則の下、プリンシプルベースで対処する方向性を示した。これを踏まえ、2024 年 4 月、イングランド銀行及び健全性規制機構（PRA）、並びに金融行為規制機構（FCA）は、AI 規制に関する戦略的アプローチを公表し、政府が示した方向性を支持するとともに、現在の規制枠組みやアプローチが白書で示された 5 つの原則と整合的であること、金融市場における AI の導入や技術進歩を踏まえ、規制枠組みやアプローチを継続的に見直していくこと、引き続き金融規制当局による国際的な議論に参加していくことなどを表明した。2025 年 1 月、英国政府は、AI 開発・利活用促進に向けた行動計画を公表し、2026 年 1 月までに、AI 開発や人材育成への投資、官民のデータ資産の開放、AI セキュリティインスティテュートの支援、官民における AI 導入等に取り組んだ[29]。金融分野では、金融行為規制機構（FCA）が、同機構の支援と監督の下、金融機関が実環境で AI の導

---

[25] IOSCO “Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges (Consultation Report)”（2025 年 3 月公表）

[26] EIOPA “Opinion on Artificial Intelligence governance and risk management”（2025 年 8 月公表）

[27] EBA “AI Act: implications for the EU banking and payments sector”（2025 年 11 月公表）

[28] “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)”（2025 年 11 月公表）

[29] Department for Science, Innovation and Technology ”AI Opportunities Action Plan: One Year On”（2026 年 1 月公表）

入を安全にテストすることができる「AI ライブテスト」プログラムを実施している。

米国では、金融サービスにおける AI の利用に関する規制は、各金融規制当局が担っており、 AI の利用に関しても、リスク管理やガバナンス等に関する既存の規制が適用されうると指摘されている。財務省は、2024 年 3 月、主として AI 特有のサイバーセキュリティリスクの観点から、金融サービス業における AI の利用状況やリスク管理のベストプラクティスについて示した報告書を公表した。さらに、財務省は、2024 年 12 月、金融サービス部門における AI の利用、機会、及びリスクについて意見公募を行った結果をとりまとめた報告書を公表した。その中で、金融サービス分野における AI の利用について整合的で頑健な基準を促すため各国政府、規制当局、金融サービス部門間の国際的及び国内的な協力を継続すること、関係者が金融サービス分野における AI の利用に関する潜在的なギャップを特定しそれらに対応することや、金融規制当局が既存のリスク管理枠組みの強化に向けた取組みを継続することなどを提言した。2025 年、米国は、AI の安全性に関する大統領令、予測的データ分析に関する SEC 規則案、AI を使用した与信判断に関する CFPB 通達等を撤回し、AI 開発・利活用促進に向けた行動計画を公表した。

シンガポールでは、シンガポール金融管理局（MAS）が、2018 年に AI 及びデータ分析の責任ある展開を促進するため、金融業界と共同で公平性、倫理、説明責任、及び透明性（FEAT）原則を策定した。また、2019 年 11 月、MAS は、国家 AI 戦略の一環として、業界コンソーシアムと協働し、金融機関が AI の利用やデータ分析において FEAT 原則を確保することを支援するための取組み（Veritas Initiative）を開始した。その成果を踏まえ、MAS 及び銀行・テック企業のコンソーシアムは、生成 AI のリスクと機会を調査するプロジェクト（Project MindForge）を立ち上げ、2023 年 11 月には、金融機関の生成 AI 利用に関する包括的なリスク管理枠組みを公表した。さらに、MAS は、金融機関向けに、2024 年 7 月に生成 AI に関連するサイバーリスクに関する情報提供文書を、2024 年 12 月に AI のモデル・リスク管理に関する情報提供文書を公表した。その後、MAS は、2025 年 11 月、金融機関における AI リスクマネジメントに関するガイドライン案を公表している [30]。

香港では、香港金融管理局（HKMA）が、2019 年 11 月、銀行に向けて、AI 利用のリスク管理に関するハイレベルの原則を示す通達を発出した。その中で、AI の利用に関する国際的な規制基準や業界動向の急速な進化を踏まえ、同原則を定期的に見直し、必要に応じて銀行に追加のガイダンスを示すことを表明している。その後の生成 AI の登場を踏まえ、2024 年 8 月、HKMA は Cyberport と共同で生成 AI サンドボックスを立ち上げた。また、同月、HKMA は、銀行に向け、生成 AI の利用に関連する消費者保護についての通達を発出した。証券先物委員会（SFC）も、2024 年 11 月、認可法人に向け、生成 AI を利用するにあたっての監督上の期待を示した通達を発出した。この間、2024 年 10 月、政府の財務事務・庫務局（FSTB）は、金融サービス分野における AI の責任ある導入に関する政策文書を公表した。同文書では、今後、香港政府が、HKMA や SFC ら金融規制当局と緊密に連携し、明確な監督上の枠組みを提供すること、金融規制当局は、AI や国際的なプラクティス

[30] MAS “Consultation Paper on Proposed Guidelines on Artificial Intelligence Risk Management for Financial Institutions”（2025 年 11 月公表）

の進歩に合わせ、既存の規制やガイドラインを継続的に見直し、適宜改定していくことなどを方針として示している。

iii. 金融庁の今後の対応の方向性

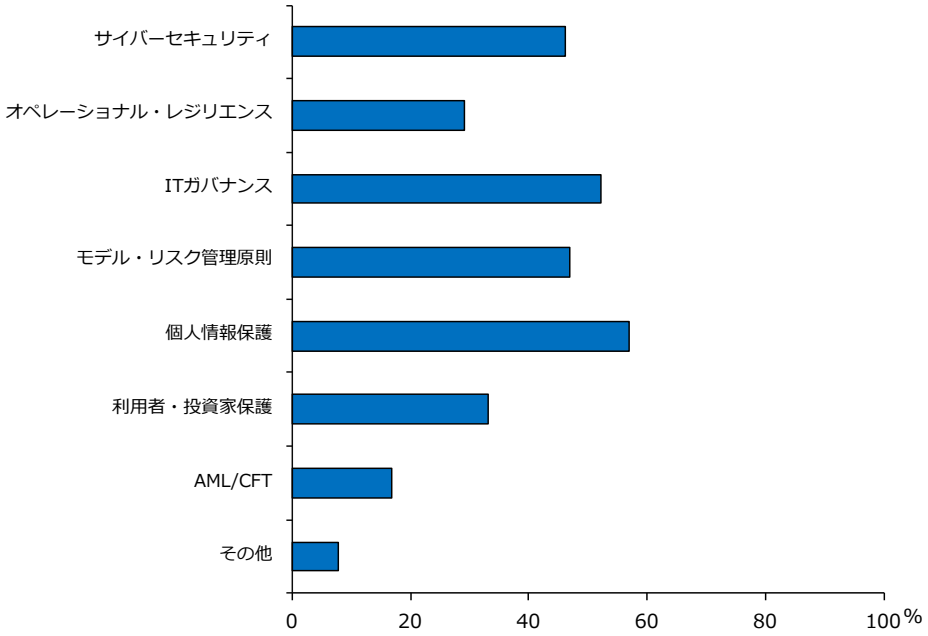
本文書は、金融分野における AI の健全な利活用に向けて、事業者との今後の対話に向けた初期的な論点を提示するものである。よって、法令・ガイドライン等の見直しやモニタリング等に係る詳細な取組方針を示すものではないが、アンケートで AI の利活用に係る規制の適用関係の明確化などを求める回答が多く寄せられたことを踏まえ、初期的な対応の方向性について整理する。

まず、規制の適用の明確化については、個人情報保護、IT ガバナンス、モデル・リスク管理、サイバーセキュリティの順で明確化を求める声が多く、これらの論点については、本章第 1 節において具体的な課題や課題解決に向けた取組事例等について整理・分析した。金融庁では、いずれの論点も、AI 利用の有無に関わらず適用される既存の法令や監督指針、原則、ガイドライン等に沿った対応を金融機関等に促していく。また、AI の利活用に係る相談や照会が金融機関から寄せられた際には、本文書で取り上げた顧客向けサービスを念頭とするリスク低減に向けた取組事例などを参照しながら、リスクマネジメントやガバナンスのあり方等に有益な示唆を与えられるよう対応を行う。

一方で、これまで見てきたように、生成 AI の特性に起因する新たな課題や、生成 AI により対応が難化した課題も存在する。よって、金融機関等との対話等を通じて、AI 活用に係る規制要件が十分明確になっているか、既存の規制・監督上の枠組みでリスクに十分対応できているかといった観点から、今後検証していく。この点、重大な規制上のギャップが特定された場合には、法令上の対応も排除されるものではないが、金融庁では法令による規制は事業者の自主的な努力による対応が期待できないものに限定して対応していくべきとの政府方針を踏まえて、まずは原則やガイドライン等の改定等を検討する。

また、国外事業者による画期的な AI モデルの開発など、国際的な技術・ビジネス動向の把握も重要であることから、金融庁では海外のフィンテック・カンファレンス等に積極的に参加し、AI モデル開発者や大手金融機関、フィンテック事業者等との対話を通じて、活用可能性や潜在的なリスクの特定をフォワード・ルッキングに行っていく。更に、今後 FSB や SSBs 等において国際的な議論が進展していくことが見込まれていることから、金融庁も AI を巡る国際的なルールメイキングに積極的に参画していくとともに、これらが公表する文書等も参考として国内対応を検討していく。

【図表 18 規制の適用関係の明確化等を希望する論点】



なお、規制の適用関係の明確化を支援する枠組みとして、「FinTech サポートデスク」と「FinTech 実証実験ハブ」を紹介したい。FinTech サポートデスクは、様々なイノベーションを伴う事業を営む、または新たな事業を検討中の事業者等からの法令面等に関する相談を一元的に受け付ける窓口であり、2015 年の開設以来、2025 年 12 月までに金融機関やフィンテック事業者等から合計 2,603 件の相談を受け付けている。これまでの相談の中には、投資助言関連サービス、チャットボット、保険業務効率化などの AI の利活用に係るものも含まれており、生成 AI の活用等に関して法令解釈の明確化等を求める場合等に利用できる枠組みである（なお、同デスクは迅速な回答を重視しており書面での回答は行わない。書面での回答を求める場合は、産業競争力強化法に基づくグレーゾーン解消制度の利用等が選択肢となる）。また、FinTech 実証実験ハブは、フィンテック事業者や金融機関等が前例のない実証実験を行う際に、金融庁内に担当チームを組成し、必要に応じて関係省庁とも連携し、イノベーションに向けた実証実験を行うことができるよう支援する枠組みである。法令面での検証結果等を含む実証実験の結果は、金融庁ウェブサイトにおいて公表される。AI 関連の採択案件としては、2018 年 8 月に結果を公表した「人工知能を用いた金融機関のコンプライアンス業務の効率化に向けた実証実験」があり、金融商品販売時において職員の説明内容にコンプライアンス違反がないかのチェック及び応接記録等に含まれる顧客からの苦情等の抽出業務を、AI を活用することで効率化・高度化できるかに関して検証した。

繰り返しになるが、AI の技術革新の進展は極めて速く、現時点において特定の対応に固執することは適当ではない。金融庁としては、上記の方向性に基づいて検討を行いつつも、状況の変化等を鑑みて柔軟に政策対応を行っていく。

その際には、AI 官民フォーラムのような場を通じて、官民の様々な関係者と連携し、AI の技術進展や金融分野での活用状況、リスク管理等に係るプラクティス、更なる活用を考える際の課題等について議論を深めていく。

② 事業者に期待する取組み

i. ビジネスプロセスの見直し

アンケートやベンダーを含めたヒアリングにおいて、AI 導入の効果は既存の業務フローを残置して AI サービスを付加的に採用するだけでは限定的になりやすく、AI の利活用を前提としてビジネスプロセス全体を見直すことが重要との声が多く聞かれた。期待した効果が得られなかった例として、AI サービスのアプリを開くまでの動線が悪く社内データとの連携も不可であるため業務利用が進んでいない事例や、ビジネスプロセス全体の自動化が遅れており AI を十分に利用できない形になっているといった事例が挙げられる。DX 全般に当てはまることだが、ビジネスプロセスの見直しは当該業務に携わる広範な社員に影響が及ぶものであり、AI に最適化する形でプロセスの抜本的な見直しを実現するためには、経営陣を中核にした推進体制や、部門の垣根を越えてシナジー効果が生まれるような組織体制を検討することが重要と考えられる。

AI 官民フォーラムでは、世界中の企業における生成 AI に関する実証実験の 95%が、試験段階から本番稼働に移行できていないことを示す海外のレポート[31]が紹介された。その上で、ビジネスでの利用を目指す上では、汎用的な生成 AI を単に取り入れるのみでは十分な効果は得にくく、用途に応じたカスタマイゼーションや学習、社員が持つ暗黙知の活用などによって AI システムをワークフローに適合させていくとともに、データ整備や社員の AI リテラシーの向上といった社内環境をしっかり整えて現場への落とし込みを徹底していくことの重要性が示唆された。

ii. ユースケースの開拓等に向けた前向きな取組みの後押し

AI の利活用を広げていくためには、当然ながら、各部門で実際に使われる具体的なユースケースが開拓されていく必要がある。この点、いくつかの事例を紹介すると、AI アイデアコンテストの実施、ビジネスインパクトを創出したユースケースの社内報での周知、DX 戦略部門による生成 AI の利用環境構築や事業部門の検討における伴走支援、各部において生成 AI 活用を進める担当を設置、といった取組みが確認された。このような取組みを通じて、PoC の成功事例の集約や人材育成が進展すれば、新たなサービスの創出や業務効率化につながるユースケースが増加し、金融機関等のサービスの高度化に繋がっていくと考えられる。

その上で、AI 官民フォーラムでは、足元では、主に業務の効率化・自動化を図るユースケースが多くみられるが、今後は、AI を活用した既存ビジネスの変革や新規ビジネスの創出など、新たな付加価値の創出に向けた取組みも重要になるとの見解が示された。金融機関ごとに AI 活用の目的は様々であるが、経営トップが先導して、健全な AI の利活用によって業務の効率化・自動化や新たなビジネスの創出を図ろうとする動きを具体的な取組みとして進め、着実に業務プロセスの改善につなげていくことが期待される。

---

[31] MIT NANDA “The GenAI Divide: State of AI in Business 2025”（2025 年 7 月公表）

iii. 経営陣の主体的な関与

これまでの金融機関等との対話では、相対的に AI の利活用に関する経営陣の問題意識が高い先ほど導入が進んでいるといった傾向が窺われた。経営陣が主導して推進体制を整備している例として、CIO 主導の下で AI を利用したシステム開発・社内啓発・リスク管理の体制を構築した上で推進を行っている先や、海外担当役員も含めたグループ横断でのタスクフォースを設置してグループの AI 活用方針・戦略を策定した先、外部有識者を招いてのアドバイザリーカウンシルを開催し、経営トップ自らが専門家の話を聞いて AI 活用推進に取組んでいる先などが確認された。

iv. 業界レベルでの知見共有

AI 官民フォーラムでは、顧客向けサービスを念頭とした AI のリスク評価・低減に関する取組みの検討状況が共有された。AI のように技術進展が早く不確実性が高い分野にあっては、業界レベルで知見を共有することにより、自社の立ち位置や対応の過不足を確認することができ、業界全体のリスク対応の高度化につながりうると考えられる。また、AI の活用に向けた検討が具体化するほど、実務レベルの論点が明確なものとなり、業界レベルで議論を深め、共通の理解を形成していく必要性が高まると考えられる。こうした業界レベルでの知見共有は、健全な AI の利活用に向けたプラクティスを形成する上で重要である。

Box 5. 生成 AI を活用した地域金融機関の DX 化に向けた実証研究事業

AI の利活用は、大手金融機関のみならず、地域金融機関にとっても重要な課題である。

金融庁は、令和 7 年度補正予算に基づき、「生成 AI を活用した地域金融機関の DX 化に向けた実証研究事業」の実施を予定している。本実証研究事業では、地域金融機関による対顧客向けサービス等のユースケースを創出するとともに、当該ユースケースについて、法規制やコンプライアンス等の観点から評価・改善を行い、これらのプロセスを通じて得られた知見を利用方針等として取りまとめて情報提供することで、地域金融機関全体の AI 実装・横展開を支援する予定である。

具体的なユースケースとしては、生成 AI が、顧客からの照会に基づいて、FAQ や各種書類等を検索して回答を生成することや、金融機関職員の指示に基づいて、決算情報等の事業者情報を確認し回答を生成すること等を想定している。

地域金融機関においては、当該情報を参考に、生成 AI を活用し、生産性を向上させることによって、融資や本業支援の強化等の金融仲介機能の一層の発揮、ひいては地域企業・地域経済の活性化に繋げていくことが期待される。

Ⅴ. 金融庁の AI 活用

1. 金融監督当局としての AI 活用の重要性

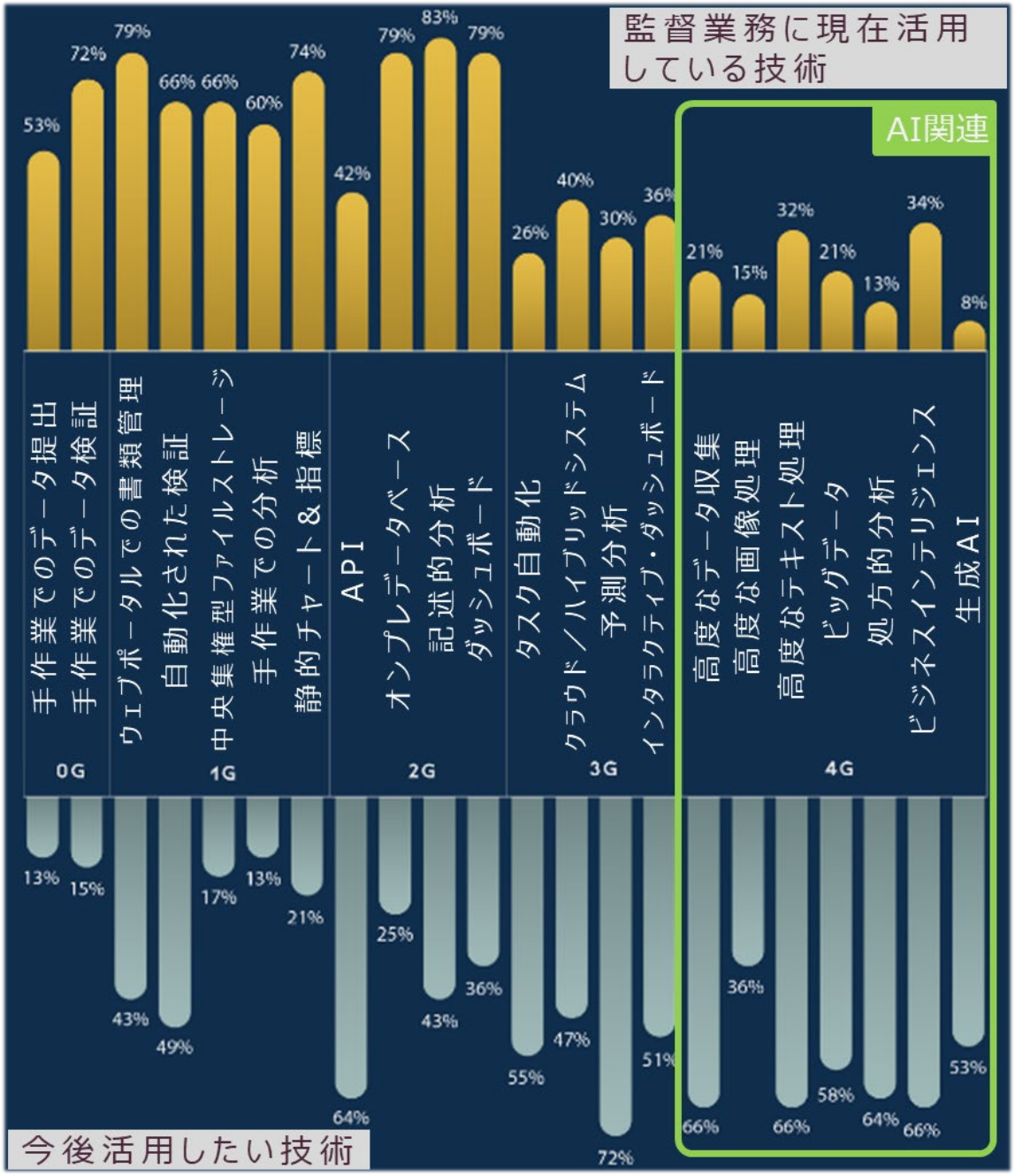
金融機関等のみならず、金融監督当局においてもモニタリングの高度化や業務効率化に向けた AI 等のテクノロジーの活用は極めて大きな課題である。FSB の報告書（前掲）においても、監督責任をより効率的に果たすために当局による AI の導入が進展しており、金融機関に遅れを取らないためにも更にこの傾向が強まる可能性があることを指摘している。世界的に規制監督業務へのテクノロジーの活用（SupTech）は進展しており、ケンブリッジ大 CCAF（Cambridge Centre for Alternative Finance）が 64 の金融監督当局を対象に実施したサーベイ [32]によると、回答した当局のうち 59%が 1 つ以上の SupTech アプリケーションを導入済であり、特に先進国当局では活用が進んでいるとの結果が示されている。

SupTech に活用されている技術のうち、AI 関連技術（テキスト処理、ビッグデータ分析等）の導入は現時点では限定的なものの、多くの当局が今後の活用に高い意欲を示しており、ビッグデータを活用した金融危機の予測や非構造化データ（企業情報、SNS 等）の活用、疑わしい取引や不公正取引の検知など、多岐に亘る領域で AI のモニタリング業務への活用が模索されている。

他方で、これらのテクノロジーを導入に係る主な課題として、AI モデルのトレーニング・検証やデータ／プライバシー保護、ガバナンス・説明責任、データ品質、人材確保等が挙げられている。これらの課題は、前章で取り上げた金融機関等が直面する課題と共通するところも多い。

[32] Cambridge Centre for Alternative Finance “Cambridge SupTech Lab: State of SupTech Report 2023”（2024 年 2 月公表）

【図表 19 金融監督当局の SupTech の導入状況と今後の活用見通し】



2. これまでの金融庁の AI 活用の取組みとより一層の活用に向けて

① データ分析の高度化

金融庁においても、テキスト処理やビッグデータ（高粒度データ）解析等の AI 関連技術の活用を含む、データ利活用の高度化を進めている。特に貸出明細や株式取引データ等の高粒度データの活用により、個別金融機関の経営状況、金融システム全体の脆弱性・強靭性、市場動向等の実態をよりきめ細やかに把握できることから、データの拡充・精度向上とともに、効率的かつ効果的な分析手法の検討を不断に進めている。

金融庁が取り組んだデータ分析事例は、「FSA Analytical Notes―金融庁データ分析事例集―」として随時公表している[33]。2024 年 7 月に公表した「地方銀行における不動産業向け貸出とその債務者区分の動向に関する分析」では、機械学習を活用し、地方銀行の貸出明細データを用いた債務者区分の予測モデル構築を試行し、銀行貸出の中で大きなウェイトを占める不動産業向け貸出の信用リスクに影響を与える要因について示唆を得た。また、同じく 2024 年 7 月に公表した「高速取引行為が市場流動性や市場変動の大きさに与える影響に関する分析」では、株価先物の注文・取引明細データに対してニューラルネットワークの手法を応用することで、高速取引行為（HFT）が市場変動に与える影響を HFT の取引戦略毎に明らかにした。

いわゆる構造化データである貸出明細等の高粒度データ活用のみならず、非構造化データの活用、すなわちテキスト処理の導入にも取り組んでいる。例えば、金融機関のディスクロージャー誌や蓄積された面談議事録等の大部のレポートであっても、テキスト処理の技術を応用することで業態全体や個別金融機関の経営やリスクテイク等に係る特徴を効率的に抽出することが可能となり、こうして得られた情報をモニタリングに従事する職員の専門的知見と組み合わせることで、より効率的かつ効果的に金融機関との対話に臨むことができると考えられる。

このようにデータ利活用の取組を進めていくことは、モニタリング業務の高度化を図る上で重要であるが、AI 技術のモニタリング業務への本格的な導入には、依然として課題も多い。課題の 1 つは、AI モデルの説明責任に係る問題である。学習データの特性や学習方法により AI モデルに偏りが生じる可能性があり、結果の信頼性について検証することにも困難が伴う。 また、情報セキュリティに係る課題も大きい。モニタリング業務に係る情報・データは機密性が高いことから、現状、一般公開されている AI は活用せず完全にクローズドな環境で AI モデル構築を進めている。その他、こうした AI 技術に係る専門的な知見を有する人材の確保・育成にも取り組む必要があり、当該分野の学識経験者を参事に任命し助言を得る等しているが、継続的な人材育成が課題である。いずれも、金融機関等が直面する課題と共通のものが多い。

② 業務効率化

[33] 金融庁「FSA Analytical Notes―金融庁分析事例集―」（2025 年 1 月公表）

また、限られたリソースの中で行政目的を効果的に達成するために、業務効率化に資するAI 活用の取組みも継続・強化している。先に述べたディスクロージャー誌等の大量文書に対するテキスト処理の活用は、モニタリング業務の高度化だけでなく、業務効率化にも直結するものである。金融庁では、情報管理と業務効率化の両立を図りながら、多くの職員がテキスト処理含む効率化ツールを活用できるよう環境整備に努めている。

また、金融庁が設置している自主的な政策提案の枠組みである「政策オープンラボ」のプロジェクトの一つとしても、2018 年には「有価証券報告書等の審査業務等における AI 等利用の検討」を立ち上げており、その中で、有価証券報告書の記載内容の審査を AI 等によって自動で行うことが可能かについて、AI スタートアップ系企業や監査法人など計 20 社の協力を得て、実証実験による検証を行った。検証の結果、今後、十分な開発期間と分析対象データがあれば分析精度が向上する可能性があることや、分析精度の向上には、AI 等による分析結果を人間が解釈してフィードバックを与えるなど、人間と AI 等がそれぞれの得意分野を理解した上で協働していくことが有効である等の示唆が得られた。

③　その他の取組

金融庁は、国際金融センターの実現に向けて、金融庁のみならず、金融業界全体における英語での情報受発信の強化を企図して、国立研究開発法人情報通信研究機構（以下、NICT）と連携し、2022 年 3 月に金融分野の文書を日本語と英語の間で双方向に高精度に翻訳できる AI 翻訳システムを開発した。一般的に金融分野は専門用語が多く、金融機関が業務上取り扱う文書の翻訳については、汎用の AI 翻訳システムでは高精度の結果を得ることは難しい。一方で、一金融機関では十分な教師データを確保することが難しいため、金融に特化した AI 翻訳システムを独自に構築することも困難である。

そこで金融庁は、庁内や業界団体、民間金融機関の対訳データを収集し、それらを NICT に提供することによって、AI の学習に必要なデータ量の確保に努め、当該翻訳エンジンの精度向上に貢献した。その結果、全訳文の 5 割弱が金融専業翻訳者に匹敵する最上位品質となる程度まで精度を高めることに成功した。この AI 翻訳システムは、開発主体である NICT から民間への技術移転が行われることを通じて、幅広い主体が当該技術にアクセス可能となっている。

④　一層の活用の検討

金融庁として、モニタリングの一層の高度化や業務効率化に向けて、生成 AI を含めた AI の活用を推進していく。生成 AI については、生成 AI の業務利用に関する政府全体の申合せ等に沿って、法令照会対応や不公正取引監視の高度化、モニタリング業務に係る文書作成、各種相談照会業務等の領域において活用に向けた検討を進めていく。また、データ分析の高度化においても、課題や目的に応じ AI 含む適切な分析手法を活用することにより、金融システムや金融機関の特徴や傾向を的確に把握し、モニタリングに活かすプロセスを定着させるほか、LLM の活用によるテキストデータからの効果的な情報取得を進めていく。また、金融庁の業務効率化・高度化を目指す政策オープンラボ（組織全体の Tech forming に向け

て）等の枠組みを活用して、AI に知見及び関心を有する若手職員の発掘を始め、人材育成等にも取り組んでいく。

Ⅵ. おわりに

1. 官民ステークホルダーとの連携の重要性

これまで見てきたように、金融機関等と当局の双方における AI 活用が加速度的に進むなかで、課題を克服し AI がもたらす果実を最大限享受するためには、金融業界及び社会全体で連携を強化する意義は大きい。毎月のように LLM がバージョンアップされ、新たな LLM がリリースされるといったスピード感の中で、自社の経営戦略や経営体力、顧客ニーズ等を踏まえて最適な AI の開発・運用・管理を行っていくためには、トレンドのキャッチアップをできる体制や経営陣及び担当者レベルでの知見と経験の蓄積が重要である。

一方で、開発リソースや専門人材が限られる小規模金融機関等においては、個社レベルでの対応が限られ、技術更新のペースに遅れが生じやすい。こうした課題に対応するためには、官民のステークホルダーが連携してユースケースの創出や AI ガバナンスの構築に向けた取組みが有効と考えられる。特に、セキュリティやコンプライアンスなどの非競争領域においては連携の余地が大きく、例えば単一の金融機関では入手困難な多様なデータが複数社間の適切な情報連携によって集約することで、学習データの質と量が向上し、リスク管理の高度化等のために AI の効果を一段と高められる余地が大きい。また、金融機関等が直面している課題の中には、著作権法や競争法上の論点といった金融規制に限らない法令上の論点を伴うため、他省庁との連携も必要となってくる。更に、前述の通り、グローバルで AI 規制が進展している中で、国際的なルールメイキングへの参画も重要である。

これらの観点から、金融庁自身もステークホルダーの一員として、金融分野における健全な AI 利活用を後押ししていく考えである。AI に限らずフィンテック全般に当てはまることだが、技術やビジネスの進展が早い中で適切な環境整備と政策対応を進めていくためには、事業者との対話が欠かせない。そこで、2024 年から金融庁が主催している Japan Fintech Week のような国内外の官民ステークホルダーの対話の機会を今後も継続的に提供し、規制監督の予見可能性を高めつつオープンイノベーションの実現に向けて尽力していく決意である。

2. 本 DP への意見募集

本文書では、金融機関等における AI 活用の現状および課題を整理するとともに、多岐にわたる論点を網羅的に検討した。繰り返しとなるが、本ペーパーの分析は初期段階にすぎず、提示した論点も、技術革新やビジネス環境の変化に伴って大きく変わり得るものである。金融庁としては、今回提示した視点を起点に、今後もステークホルダーとの対話を強化しながら、具体的な施策について柔軟に検討を深めていきたいと考えている。意見やご提案がある場合には、金融庁【ai.survey★fsa.go.jp】（「★」記号を「@」に置き換えてください。）までご連絡いただきたい。