



AIディスカッションペーパー第1.1版の概要と金融法務への示唆

金融庁総合政策局暗号資産・ブロックチェーン・イノベーション参事官室
イノベーション推進室 課長補佐

那須 翔

金融庁では、金融分野における健全なAI利活用の後押しに取り組んでいる。具体的には、2024年10月から11月にかけて、金融機関におけるAI利活用に関する実態調査を行い、2025年3月、「AIディスカッションペーパー」（以下「AIDP」という）を公表した。その後、同年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」という）を開催した。そして、2026年3月、AI官民フォーラムで得られた知見を踏まえ、AIDP第1.1版を公表した。本稿では、これらの取組みの概要と、AIDP第1.1版の金融法務への示唆について解説する。なお、本稿において意見にわたる部分は、いずれも筆者の個人的見解である。

1 金融庁のAI利活用推進に向けた取組み

初めに、冒頭に述べた金融庁のAI利活用推進に向けた取組みについて解説する。

(1) AIディスカッションペーパー第1.0版

AIは、2010年代から、社会を変革し得る技術として注目されてきたが、特に、2022年秋以降のLLM（大規模言語モデル）の性能向上と普及は、AIの民主化をもたらした。もっとも、2024年の時点では、金融機関の実務レベルでは、どのようにAI（特にLLM）を業務に組み込めばよいのか、また組み込んでよいのかについて、様々な考えがあったものと思われる。2025年3月公表のAIDP第1.0版は、このような状況

の中で、金融庁として、金融機関における健全なAI利活用に向けた取組みを後押しするため、AI利活用の実態を調査し、その結果を取りまとめるとともに、AI利活用に向けた初期的な論点整理を行ったものである。その概要は、以下のとおりである。

まず、AI利活用の実態について、従来型AIについては、相当程度普及しており、その主な用途は、業務効率化、顧客サービスへの活用、リスク管理の高度化、市場予測等であった。一方、生成AIも、活用自体は相当程度行われていたものの、その用途は、ドキュメンテーションやコーディングが中心で、顧客向けサービスへの活用はきわめて限定的であった。

次に、AI利活用に向けた課題について、個人情報保護、AIガバナンスの確立、専

門人材の確保・育成、社内教育、データ整備等が主たる課題として挙げられた。

(2) AI官民フォーラム

AI官民フォーラムでは、AIDPで整理した論点について検討を深めるべく、4回にわたり、金融機関のCDOクラスの方、金融機関でAI利活用の実務に従事している方、金融機関にサービスや助言を提供している方等にプレゼンをしていただき、パネルディスカッションを行った。その概要は、以下のとおりである¹。

第1回では、14の業界団体から、各業界におけるAIの活用状況や課題、取組みの方向性等について発表いただいた。第2回では、AIを付加価値創出につなげる上では、各金融機関におけるデータ整備（データマネジメント）が不可欠であるとの認識のもと、金融機関におけるデータ整備についてディスカッションを行った。第3回では、個々のサービスやオペレーションを念頭に、個人情報保護に関する対応や、顧客向けサービスへのAI利活用におけるリスク管理に焦点を当ててディスカッションを行った。第4回では、全社的なガバナンスについてディスカッションを行った。

AIの活用状況については、2024年の実態調査時点では、生成AIの用途は主としてドキュメンテーションとコーディングであったが、2つの変化が明らかになった²。第1は、顧客向けサービスへの活用が検討され始めていることである。現時点で実用化されているものは、事務手続や（典

型的には金融リテラシーに属するような）情報提供を目的としたものが大半だと思われるが、金融機関によっては、将来的にAIが個別の商品について説明・提案することを見据えた検討が進められている旨の紹介があった。第2は、AIエージェントの活用が検討され始めていることである。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をAIエージェントに組み込むことで、より幅広い業務に活用できるようになると考えられる。

2 AIディスカッションペーパー第1.1版の金融法務への示唆

AI官民フォーラムにおける上記の議論を踏まえ、金融庁は、AIDP第1.1版を公表した。改訂点は多岐にわたるが、以下、金融法務への示唆に焦点を当てて解説する。

(1) AIガバナンス体制

AIガバナンスについては、一般論として、以下のことが指摘できると思われる。

第1に、何がリスクか、いい換えればガバナンスのゴールは、AIを使用する場合とそれ以外の場合とで異ならないと思われることである。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（以下「AI推進法」という）3条4項は、AIの適正性確保に関して、「人工知能関連技術の研究開発及び活用は、不正な目的又は不適切な方法で行われた場合には、…国民生活の平穏及び国民の権利利益が害される事態を

1 AI官民フォーラムについては、金融庁ウェブサイトにて資料及び議事要旨を公表している。

2 第2回・第3回AI官民フォーラム議事概要、AIDP第1.1版18～19頁。なお、2025年の調査結果として、日本銀行金融機構局「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—」（2025年9月）も参照。

助長するおそれがある」としており、新たに保護法益を定義するというよりは、既存の法益がAIという新技術の活用場面でも保護されるべきことを述べている³。金融分野においては、この「既存の法益」として、顧客保護、市場の健全性などの法益を考慮する必要があり、第3回AI官民フォーラムでは、主としてこれらの法益やそれを保護するための具体的な対応としてのリスク低減措置が議論されたものと考えられる。

第2に、金融機関がAIガバナンス体制を整備する場合、従前から整備されてきたリスク管理態勢を活用することができることである⁴。AIガバナンスをめぐっては、しばしば、体制整備の重要性が説かれるが、金融機関は、従前から3線モデルに基づくリスク管理態勢を整備してきており、AIに関連するリスク管理についても、これまで培ってきたリスク管理態勢を活かすことができる。第3回・第4回AI官民フォーラムでは、このことを前提に、1線と2線の連携や役割分担が議論された⁵。

第3に、リスクベースアプローチの重要性である⁶。リスク管理とは、リスクを特定・評価し、リスク対応（回避、低減、移

転、保有）を行い、モニタリング・レビューするプロセスであり、どのようなリスク低減措置が適切かは、リスクの内容によって異なる。AIガバナンスをめぐっては、特定の対応、例えば人の関与（human oversight。近時はhuman-in-the-loopという語もしばしば使われる）の重要性が強調されることがあるが、一律に何らかの対応をする必要があるわけではなく⁷、あくまでユースケースごとのリスクに照らして判断すべきと考えられる。なお、個別のAIシステムのリスク管理については、(2)で述べる⁸。

第4に、アジャイルガバナンスの重要性である⁹。AIをめぐりリスクは、技術の進展だけでなく、従業員・顧客のリテラシー、悪意あるアクターの行動等によっても（ポジティブにもネガティブにも）変化し続けていると考えられ、AIシステムの実環境への投入後も継続して、かつ、必ずしも年1回といった伝統的なマネジメントサイクルにとらわれることなく、レビューを実践していくことが必要である。

(2) 個別のAIシステムのリスク管理

第3回AI官民フォーラムでは、顧客向けサービスを念頭に置いたリスク低減措置

3 AI推進法13条の指針として定められた「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」（2025年12月19日人工知能戦略本部決定）も、人間中心、公平性、安全性、透明性、アカウントビリティ、セキュリティ、プライバシー・個人情報保護という、既存の保護法益を確認している。

4 AIDP第1.1版25頁。

5 AIDP第1.1版25頁。

6 AIDP第1.1版25頁。4頁、38頁も参照。

7 AIDP第1.1版25頁～26頁でも、事前にルールや手続を固定する必要はないことを確認している。

8 全社的な体制整備と個別のAIシステムのリスク管理という分類は、AIDPの改訂にあたって採用したものである（AIDP第1.1版21頁）。同様の観点に立つものとして、AIガバナンス協会「AI時代の経営意思決定とガバナンス ～攻めのAIガバナンス実現のための戦略レポート ver. 1.0」は、環境・リスク分析、ゴール設定等の経営レベルの理解・コミットメントが必要になる取組みと、個別のAIシステム単位での評価・対策等の現場での技術的な実装とその結果を踏まえた対応の双方が重要であるとしている。

9 AIDP第1.1版25頁～26頁。

について、銀行、証券、保険の各社から発表いただいた。AIDP第1.1版では、そこで示されたリスク低減措置を、4つの要素に分けて整理している¹⁰。

第1に、サービス提供前におけるAIシステム・サービスの適切な設計とテスト・検証である。ここでは、システムプロンプトやRAGによる回答内容の制御、より高度なLLMの選択、ファインチューニング、(特に断定的判断の提供の防止等のための)ガードレールといった技術的手法のほか、(特に初期段階における)人間による対応のオプションの提供、事務的手続から導入を開始するといったオペレーショナルな手法が挙げられた。技術的手法に比して、オペレーショナルな手法は、相対的にユースケース依存性が強く、手法が確立されていないと思われるが、そのような中で、金融機関における顧客向けサービスというある程度具体的な場面を前提に、一定の取組事例が示されたことは、今後の実務の参考となるとと思われる。

第2に、顧客への適切な説明・注意喚起である。ここでは、生成AIによる回答であって誤りが含まれ得る旨の注意喚起や、(テキストだけでなく)動画や図の併用、顧客の理解度の確認、回答の根拠の明示、人間による対応への移行等が挙げられた。どのような説明が必要かは、顧客の理解力

によるので、どのような顧客に対してAIを使用するか(前記「第1」の要素に関連する)の判断と、顧客に対してどのような説明を行うかは、一体的に判断する必要があると思われる¹¹。

第3に、サービス提供後の運用状況の記録・モニタリングである。ここでは、(特にハイリスクなユースケースや、初期段階における)会話の記録・モニタリング・フォローアップ、特定の商品に偏った勧誘を行っていないか等の客観的指標による検証、推薦ロジックの文書化と第三者レビュー¹²等が挙げられた。これらの手法は、個別の出力というよりは、個別の出力に影響を与える要素や、(個別の出力の総体である)出力全体の傾向をモニタリングの対象として活用するものであり、AIの不確実性への対処法として、今後の実務の参考となるとと思われる。

第4に、これらを支える組織体制である。これについては、2(1)で述べたとおりである。

これらは、顧客向けサービスへのAI活用の初期的段階にある現時点で、今後採り得る選択肢を挙げたものであり、いずれかが必須というわけではなく、また、仮にすべての方策を実施しているとしても、それをもって十分なリスク低減がなされているとは限らないが、少なくとも、現時点で必

10 AIDP第1.1版37頁。

11 なお、本文の議論は、具体的な法的義務を念頭に置いたものではないが、今後、AIを用いて個別の商品について説明しようとする場合には、適合性原則や説明義務との関係について、検討を要する。

12 文脈は異なるが、EUのデジタルサービス法(DSA)は、推薦システム(recommender system)を、オンラインプラットフォーム(SNS・動画共有サイト、オンラインマーケットプレイス等)のビジネスの中核と位置付け(DSA Recital 70)、透明性の確保(DSA27条)、リスク管理(DSA34条、35条)、独立のコンプライアンス機能・監査(DSA37条、41条)、当局に対する説明義務(DSA40条3項)等を定めている。本文の記載は、これと類似の観点に出たものといえる。

要な取組みの検討を進めている金融機関が共通して有している問題意識として、参考になると考えられる。

なお、AIのリスクをめぐっては、説明可能性の欠如、公平性の欠如、ハルシネーション等の課題が指摘されているが、これらは、リスクそれ自体というよりは、AIの技術的特性であり、リスクに影響を与え得る要素と位置付けるのが適切であると思われる¹³。

第3回AI官民フォーラムにおける検討は、このような技術的特性を出発点とするのではなく、具体的なユースケース¹⁴を出発点として、当該ユースケースにおいて配慮すべき法益は何か、AIの技術的特性はそこにどのような影響を与えるかという発想で行われたものと思われ、思考枠組みとしても、参考になるとと思われる。

(3) 個人情報保護法上の論点

個人情報の保護に関する法律（以下「個人情報保護法」という）をめぐっては、2024年の実態調査において、わかりにくいとの意見が多かったことから、第3回AI

官民フォーラムにおいて、専門家にプレゼンいただき、その内容を事務局において整理している¹⁵。その概要は、以下のとおりである。

第1に、金融機関が顧客情報をAIモデルの開発に利用する場合（＝学習データとしての処理）、個人情報保護法ガイドラインQ&A 2-5が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していることが参考になる。一方、AIの利用（＝入力データとしての処理）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であるが¹⁶、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。

第2に、第三者が提供する生成AIサービスに個人データを入力する場合、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¹⁷、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

13 同様に文脈は異なるが、DSA34条は、大規模オンラインプラットフォーム提供者によるリスク評価に関して、1項で、リスクそのものとして、違法コンテンツの拡散、基本権行使に対する否定的影響、市民的言説・選挙プロセス等に対する否定的影響等を挙げた上で、2項で、リスクに影響し得る要素として、レコメンダーシステム、コンテンツモデレーションシステム等を挙げている。リスクそのもの（弊害）とその発生に影響を与える要素の区別という意味で参考になる。

14 例えば、同じAIを使用した製品・サービスでも、自動車と医療機器と投資助言・運用（ロボアドバイザー）と金融商品の販売・勧誘ではリスクが異なる。また、従来型AIとLLMチャットボットと（LLMベースの）AIエージェントでもリスクは異なる。さらに、金融機関が、自らAIモデルを開発するのか、第三者が提供するAIモデルを自らのサービスや業務に組み込むのか、当該AIモデルを（例えばチャットボットのUIで）単に利用するのかによっても、金融機関の責任の範囲は異なり得る。

15 AIDP第1.1版38頁。なお、39頁では、「課題への対応」として、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等の取組みに言及しているが、これらは、あくまで実際にみられた取組みの一例であり、金融庁として推奨する趣旨ではない。

16 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）」（2025年6月最終改正）3-1-1参照。

17 2022年度規制改革ホットライン回答No. 307参照。

選定・契約締結にあたっては、金融機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などを確認する必要がある。

第3に、AIモデルの開発を第三者に委託することに伴って個人データを当該第三者に提供する場合、委託先管理が必要である。

第4に、海外にサーバーを置く生成AIサービスの利用については、越境移転規制は、受領者が「外国にある第三者」である場合に適用されるが、基準適合体制の判断や外的環境の把握においては、サーバー所在地を考慮する必要がある。

また、第3回AI官民フォーラムでは、プライバシー強化技術(Privacy Enhancing Technologies: PETs)についても紹介されたところ、AIDP第1.1版では、PETsには、AIの開発及び(又は)利用に適用可能なものも多く、AI利活用にあたって採り得る技術的安全管理措置の1つと考えられるものとして言及している¹⁸。

なお、以上の内容は、第3回AI官民フォーラムにおけるプレゼンの内容を整理したものであり、金融庁として法的見解を示したのではなく、また、現在行われている個人情報保護法の3年ごと見直しの過程で、解釈又は前提となる法令に変更があり得ることには留意いただきたい。

(4) 金融規制法上の論点

金融規制法上の論点としては、AIDP第1.1版では、第3回AI官民フォーラムにお

ける問題提起を踏まえ、金融商品取引法に関する論点を中心に、現時点での整理を示している¹⁹。その概要は以下のとおりである。

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(金融商品取引業等に関する内閣府令153条1項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はないかについては、必ずしもその必要はないとしている。

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ところ、当該会話データ等を分析する者にアクセス権限を付与することが法人関係情報の管理態勢として適当かについては、当該アクセス権限の付与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とした上で、個別具体的な事案に即して実質的に判断する必要があるとしている。

第3に、今後、LLM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勧誘該当性については、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いう「勧誘」の一般的な解釈を前提に、金融機関においてAI・データ利活用の目的や態様、顧客への働き掛けの内容(特に、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)等を考慮して個別に判断する必要がある旨を述べている。

18 AIDP第1.1版39頁。PETsは様々な技術の総称であり、実際にPETsが有効か、何に対して有効なのかは、個別の場面ごとに判断する必要がある。

19 AIDP第1.1版40頁～41頁。

金融商品取引法の勧誘規制は、人間である営業職員の活動から生じる投資者保護上のリスクを管理するために構築されたものと考えられる。AIが営業職員を代替する場合でも、対処すべき弊害は変わらないが、人とAIの特性の違いに応じて、リスクの内容（≡弊害発生メカニズム）や適切なリスク低減措置は変わり得るのであり²⁰、2(2)で紹介した事例は、リスク管理実務の形成に向けた試みの1つといえる。AIDP第1.1版では、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、AIDP第1.1版で取り上げた取組事例等を参照し、有益な示唆を与えられるよう対応しているところであり²¹、今後、建設的な対話が積み重ねられることが期待される。

3

FSBのAIサウンドプラクティス ペーパー

本稿脱稿後の6月10日、金融安定理事会（FSB）は、“Sound Practices for Responsible Adoption of Artificial Intelligence（AI）：A toolkit for financial institutions”と題する報告書の市中協議版を公表した。本文書は、金融機関による責任あるAI導入を促進するため、あらゆる種類の金融機関を対象とした「サウンドプラクティス」（健全な実務慣行）のツールキットを提供するものである。本文書は、①概説（ユースケース、リスクと課題）、②組織全体のAIガバナンスに関するサウンドプラクティス、③AIライフサ

イクル管理に関するサウンドプラクティスの3部構成となっており、②・③では、12のサウンドプラクティスと、関連する考慮事項が示されている。本ペーパーは、LLM普及後の2026年前半に、従来型AI、生成AI、AIエージェントといった多様なAIを前提に、（筆者を含む）各国の金融規制当局の実務者により、比例性・柔軟性を重視しつつ、新たにドラフトされたものであり、既存の（特に、金融機関向けに調整されておらず、また「生成AI以後」の進展が十分に反映されていない）ガイドライン等を自組織の業務運営や個別のサービス・プロダクトに当てはめようとして苦慮している実務者の参考になり得ると思われる。

なす しょう

2021年3月早稲田大学大学院法務研究科修了。2023年1月TMI総合法律事務所、2024年9月より現職。弁護士、情報処理安全確保支援士、G検定（2024年第4回）合格。現職では、金融商品取引法・資金決済に関する法律等に関する相談対応、各種実証実験の支援、金融分野におけるAI利活用推進、暗号資産交換業等におけるサイバーセキュリティ強化、各種ガイドライン改正等に従事。

20 第3回AI官民フォーラムでは、特に外務員規制に関する問題意識が示されたが、外務員規制は、人間による勧誘に伴うリスクを低減するための制度的措置といえる。

21 AIDP第1.1版46頁。