金 融 研 究

2026 年 1 月 / 第 45 巻 第 1 号

日本銀行金融研究所

金 融 研 究

2026 年 1 月 / 第 45 巻 第 1 号

目　次

日本銀行金融研究所

第 25 回
情報セキュリティ・シンポジウム「金融分野におけるセキュリティの潮流 CITECS 設立 20 周年記念」の模様

1. はじめに

日本銀行金融研究所・情報技術研究センター（Center for Information Technology Studies: CITECS）は、設立 20 周年を記念して、2025 年 3 月 6 日、「金融分野におけるセキュリティの潮流」をテーマとした第 25 回情報セキュリティ・シンポジウムを開催した。

近年、インターネットやスマートフォンなど情報通信技術の急速な普及を背景に、フィンテックと言われる金融サービスと情報通信技術を結びつけたさまざまな革新的な動きがみられている。さらには、人工知能（artificial intelligence: AI）技術の急速な進展が金融サービスに新たな可能性をもたらそうとしている。

一方、こうした変化に伴い、新たなセキュリティ面での課題も顕在化している。CITECS では、金融分野におけるセキュリティ面での課題への対応を研究面から支援すべく、これまでさまざまな調査研究を行ってきた。そこで、本シンポジウムでは、CITECS における情報セキュリティ研究の 20 年を振り返るとともに、近年関心が高まっている、量子耐性を有するシステム、AI、デジタル決済といったテーマについて講演と対談を行い、今後のセキュリティ対策について考察を行った。

当日は、金融機関やフィンテック企業などの実務家、システム開発・運用に携わる技術者、研究者など約 200 名がオンラインで参加した。本稿では、以下に示したプログラムに沿って、講演と対談の概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

1 文中の講演者やパネリストの所属および肩書きは、シンポジウム開催時点のものである。また、本稿において示された意見はすべて発言者個人に属し、その所属する組織の公式見解を示すものではない。また、本シンポジウムでの講演の資料等については、日本銀行金融研究所のサイト（https://www.imes.boj.or.jp/jp/conference/citecs/25sympo/25sec_sympo.html）を参照されたい。

【第 25 回情報セキュリティ・シンポジウムのプログラム】

- 基調講演「情報技術研究センター（CITECS）20 年のあゆみ」
  金融研究所情報技術研究センター長　鈴木淳人
- 講演「金融高度化センターの活動―高度化センター 20 周年 WS の内容を中心に―」
  金融機構局金融高度化センター長　須藤　直
- 講演「量子耐性を有するシステムの実現に向けた金融分野での取組み」
  金融研究所参事役　宇根正志
- 講演×対談「AI がもたらすリスクに対するセキュリティ」
  金融研究所情報技術研究センター企画役　菅　和聖
  情報セキュリティ大学院大学教授　大塚　玲
- 講演×対談「さまざまな決済スキームとそのセキュリティ」
  金融研究所情報技術研究センター企画役　田村裕子
  筑波大学システム情報系教授　面　和成
- 講演「金融分野における今後のセキュリティ対策―シンポジウム総括を兼ねて―」
  京都大学公共政策大学院教授　岩下直行

2.　基調講演「情報技術研究センター（CITECS）20 年のあゆみ」

鈴木は、この 20 年を振り返り、CITECS の設立経緯やこれまでの研究活動等について、次のとおり講演した。

(1)　CITECS の設立経緯

日本銀行は、1980 年代から暗号技術・情報セキュリティについて研究を行ってきた。1988 年に稼動した日銀ネットに共通鍵暗号 DES（Data Encryption Standard）を搭載したこともあり、当初はユーザの視点から暗号アルゴリズムの安全性について研究を行っていた。その後、インターネットの普及を背景に、調査研究の対象を理論研究から応用に広げ、金融サービスのセキュリティ対策全般について検討を行うこととなった。例えば、1999 年に開催した第 2 回情報セキュリティ・シンポジウムでは、キャッシュカード取引のセキュリティが低下していることを指摘し、より安全性の高い方式への移行を推奨していた。

しかしながら、金融業界における対応は進まず、2000 年代中盤には、偽造キャッシュカードを用いた預金の不正引出しが社会問題となった。そのため、日本銀行

は、情報セキュリティに関する研究体制の強化とより積極的な情報発信を企図して、2005 年 4 月に CITECS を設立することとした。CITECS は、金融界・学界・IT 実務家間の架け橋となり、ひいては金融業界における情報システムの技術革新に貢献していくことを目標に活動を開始した。

(2) CITECS の活動

CITECS では、金融業界が情報化社会において直面する新たな課題について調査研究を行っており、その内容を論文等として公表してきた。また、情報セキュリティ・セミナーや情報セキュリティ・シンポジウムの開催を通して、最新の研究動向などについて情報発信を行ってきた。

情報処理推進機構が 20 年前に公表した「情報セキュリティ 10 大脅威」には Web アプリケーションの脆弱性による情報漏洩、マルウェアによる情報漏洩、フィッシング詐欺が挙げられており、いまもなお脅威として認識されているものが少なくない。このように情報セキュリティにかかる課題には、変わらないものと新しいものが混在しており、その調査研究には知見の蓄積と知識の吸収が必要となる。実際、1998 年に開催した第 1 回情報セキュリティ・シンポジウムでは、電子マネー、暗号アルゴリズムの移行、公開鍵暗号の安全性などを取り上げており、これらはいまも CITECS における主テーマとなっている。

CITECS における研究テーマは幅広く、暗号理論、決済・電子現金、認証・生体認証、人工物メトリクス、暗号アルゴリズム移行、ハードウェア、ブロックチェーン、AI セキュリティ・セーフティなどがある。本日は、このうち、暗号アルゴリズムの移行、AI セキュリティ・セーフティ、決済・電子現金を取り上げ、それぞれに関する最新の研究内容について研究スタッフから紹介する。

イ. 暗号アルゴリズムの移行

暗号アルゴリズムの移行にかかる課題整理は、古くて新しい研究領域であり、過去の知見のもとに常に新しい課題への対応が必要とされている。約 30 年前には、共通鍵暗号である DES の安全性低下を受け、AES（Advanced Encryption Standard）への移行に向けた検討が行われた。また、2005 年頃には、当時広く利用されていた鍵長を 1,024 ビットとする RSA 暗号などが十分な安全性をもたなくなることが指摘され、2010 年に向けて暗号アルゴリズムの移行が進められた。移行対象は共通鍵暗号、公開鍵暗号、ハッシュ関数であり影響範囲が広かったことから、移行にかかる問題は暗号アルゴリズムの 2010 年問題とも呼ばれた。さらに、現在は量子コンピュータによるリスク対応について検討が必要となってきており、本日は、従

来の暗号から耐量子計算機暗号（post-quantum cryptography: PQC）への移行に向けた課題等について整理した内容を紹介する。

ロ．AI セキュリティ

AI セキュリティは、まったく新しい研究領域である。近年の AI 技術の急速な発展を受け、そのセキュリティについての研究の重要性も高まっている。一般的に AI 技術の進化が知られるようになったのは、おそらく、囲碁 AI である AlphaGo[2] がプロ棋士に勝利した 2015 年頃であるように思う。CITECS ではその頃から AI がもたらすリスクに対するセキュリティについて研究を開始してきた。近年は生成 AI の台頭により、セキュリティ研究の重要性が増していることから、今後も高い関心をもって研究活動を行っていく予定である。

ハ．決済・電子現金

決済・電子現金は、古くて新しい研究領域とまったく新しい研究領域の組み合わせである。CITECS 設立前より、金融研究所では電子現金に関する研究を行っており、金融研究所から公表した情報技術分野の第 1 号論文も電子現金に関するものであった。当時は世界各国でデジタル決済に関する実証実験が盛んに行われた時期であり、金融研究所も民間企業とともに研究開発を行っていた。本日は、古くて新しい研究内容として、電子現金について再検討した内容を報告する。

また、2008 年以降は、スマートフォンの普及によりデジタル決済の形態が大きく変化したほか、ビットコインの登場によりブロックチェーン技術が注目を集めた。こうした分野は比較的新しい研究領域であり、最新の研究動向をフォローしながらそのセキュリティについて検討していくことが重要であろう。

3. 講演「金融高度化センターの活動について ―高度化センター 20 周年 WS の内容を中心に―」

須藤は、2025 年 1 月に開催された金融高度化センター 20 周年ワークショップの内容、および、金融機関におけるデジタル技術の実装に向けた課題について、次のとおり講演した。

2 AlphaGo は、Google Inc. の登録商標である。

(1) 金融高度化センターについて

金融高度化センターは、金融機関における先進的な金融技術や金融仲介機能の向上のための取組状況等に関する調査・研究・公表、セミナーやワークショップの開催を通じた金融機関との対話を行っている部署である。こうした活動を通じて、金融機関が金融仲介機能をより有効に発揮していく取組みを支援している。2005 年に、日本銀行におけるプルーデンス政策を、それまでの危機管理重視から、金融システムの安定を確保しつつ、公正な競争を通じて金融の高度化を支援する方向へ切り替えるという方針のもとで設立され、CITECS と同じく 2025 年に 20 周年を迎える。

(2) わが国におけるデジタル技術の進展

この 20 年で、デジタル技術は大きく発展し、金融分野においてもデジタル技術の活用が広がってきている。こうしたなか、金融高度化センターでは、2025 年 1 月、デジタル化とわが国の金融の未来と題したワークショップを開催した。デジタル技術を活用しながらどのように金融サービスを効率化・高度化できるのか、また、デジタル技術を活用しながらどのように金融サービスをこれまでどおり安定的に提供できるのかという論点について、講演とパネル・ディスカッションを行った。当日の講演資料は、日本銀行のホームページに掲載している[3]。

イ. デジタル技術活用に伴うメリットとリスクの認識

デジタル化にかかる便益については、大規模データと高い計算能力の組み合わせによる便益と、大規模言語モデルの活用のもとで人とコンピュータ、あるいは人と人との対話が変化することによる便益の 2 つがあるように思われる。この結果、個々の顧客ニーズに即した付加価値の高い金融サービスを、より幅広くかつタイムリーに提供できるようになる可能性がある。もっとも、デジタル化の進展に伴い、リスクも拡大している可能性があることには留意が必要である。例えば、2010 年のフラッシュ・クラッシュは、高速・高頻度取引などのアルゴリズム取引が市場の振幅を大きくした可能性がある事例として知られている。

便益に関するデジタル化の最適なペースは、自社の態勢をみながら自分で選べる一方、リスクに関するデジタル化の最適なペースは、自社の外側でどのようなペースでデジタル化が進むかという点にも影響を受ける。そのため、外のペースが思っ

3 https://www.boj.or.jp/finsys/c_aft/aft250213a.htm

ていたよりも速く、例えば、不正行為が急に高度化してしまうような場合には、これまで提供できていた付加価値の提供が難しくなる可能性もある。

ロ．デジタル技術と生産性

生成 AI が生産性に与える経路については、人が従事している業務を AI に委ねるという労働力の代替である「自動化」と、労働者の生産性を高める「支援」という 2 つがあると指摘されることがある。金融については、自動化されうる業務と支援されうる業務の双方の割合が高いとする調査報告もあり、生成 AI の影響が大きい業種であるとみられる。

先行き 10 年における労働生産性の伸び率の見通しについては、年率 0.05％程度から 1％を超えるものまで、さまざまな見方が示されている。こうした見通しの違いの要因の 1 つは、生成 AI によって被支援業務がどう変化するかといった評価の違いによるものであり、業務への実装の巧拙によって労働生産性への影響が異なるものになる可能性も示唆している。

(3) わが国におけるデジタル技術の進展

金融機関が、メリットとリスクのバランスを取り、かつ、デジタル技術の実装を着実に生産性の上昇につなげるには、①業務の見直し、②リスク統制、③人材育成、④関係者の協調などがある。これらは社内リソースの配分にかかる課題となるため、経営トップによるコミットメントが必要になる。

主要国の労働生産性を比較すると、日本の生産性はやや伸び悩んでいる。特に、1990 年代以降の成長率の鈍化が顕著である。こうした生産性の違いを生む背景としては、資本ストックの量などに加え、技術を使いこなせているかという点も重要であると考えられる。デジタル技術の進歩と、今後の実装がこうした状況を大きく打開するかどうかは非常に重要な論点であり、金融高度化センターとして高い関心をもっている。今後も、金融技術やリスク管理手法の高度化という観点から有益な情報を発信していきたい。

4. 講演「量子耐性を有するシステムの実現に向けた金融分野での取組み」

宇根は、PQC への移行に向けた金融分野での取り組みについて、次のように講演した。

(1) PQC 移行対応の特徴

これまでの 20 年間において、金融分野では、サービス提供環境が大きく変化した。ネットワークで結ばれる対象システムが拡大したほか、ステークホルダーも大きく多様化が進んだ。こうした環境のもとで、安全で信頼される金融サービスを提供するには、暗号技術が必要不可欠である。RSA や楕円曲線暗号などの現在主流となっている公開鍵暗号技術は、暗号解読が可能な性能を有する量子コンピュータ（cryptographically relevant quantum computer: CRQC）によって効率的に解読できることが知られており、金融分野では CRQC によるリスクへの対応について検討が進められている。

CRQC の実現時期については、専門家の間でも意見が分かれており、不確実性が極めて大きい。外部機関によるアンケート調査によれば、現在広く使用されている RSA 暗号（鍵サイズ 2,048 ビット）を 1 時間で解読できる CRQC について、その実現の可能性が 5 割以上となる時期が 2039 年までと回答した有識者は約 6 割であったほか、2044 年までと回答した有識者は約 9 割であった。これまでは、コンピュータの計算処理能力の向上スピードを予測して、暗号鍵のサイズを伸長するという対応を行うことが可能であったが、CRQC によるリスクが顕現化する時期の見通しは非常に難しいというのが実情となっている。

PQC への暗号移行がこれまでより難しいとの見方が多いが、その理由の 1 つに、対応すべき範囲が不透明であることが挙げられる。対応方針や責任分担などの調整を要するステークホルダーが多く、対応に時間がかかることが懸念されている。また、脅威が顕現化する時期が不透明であることにより、いつまでに対応すべきかといったタイムラインが未確定であることも課題の 1 つとなっている。さらに、実装技術が十分に成熟していないことから、移行対応後に脆弱性が見つかるリスクも懸念されている。これらの課題を考慮すれば、PQC 移行にかかる検討には早期に着手することが必要であるといえる。

(2) PQC 対応をめぐるこれまでの動き

イ. 海外のセキュリティ当局の動き

米国は、2035 年までに CRQC にかかるリスクを最小化させる方針を掲げている。現在、2035 年末までに、既存の連邦政府標準暗号（公開鍵暗号）の使用を禁止する方針についてパブリックコメントが公表されている。また、国立標準技術研究所は数年前から PQC の標準化作業を進めており、2024 年夏、複数のアルゴリズムが標準化された。

EU では、欧州委員会が加盟国のセキュリティ当局に対して、PQC 移行のロードマップを 2026 年 4 月までに策定するよう勧告している。また、加盟 18 カ国のセキュリティ当局は連名で、PQC 移行に向けた検討の早期着手を推奨するステートメントを公表した。

ロ. 実装に向けた動き

実サービスへの実装も始まっている。一部のウェブ・ブラウザの鍵共有プロトコルに PQC が実装されているほか、メッセージング・アプリやテレビ会議システムにおける鍵共有プロトコルにも PQC が導入されている。また、PQC を搭載した IC チップが開発され、第三者によるセキュリティ評価の結果が公表されている。そのほか、IC カードに搭載する IC チップなどのセキュリティ・エレメントに関して、PQC を組み込んだ技術仕様の標準化の検討も開始されている。

ハ. 金融分野における主な動き

金融分野においては、欧米の金融当局や金融コミュニティより、さまざまな調査報告やステートメントが発表されている。わが国を含む主な金融分野の動きは以下のとおりである。

2022 年 11 月	米国金融分野におけるセキュリティ技術の標準化を担う ASC X9 が、量子コンピュータによるリスクに関する調査報告を公表。
2023 年 3 月	セキュリティ・インシデントの情報共有などの共助の取組みを行う FS-ISAC がリスク対策に関する調査報告を公表。
2023 年 6 月	中央銀行のコミュニティ（国際決済銀行・仏中銀・独連銀）が、共同プロジェクト「Leap」の報告書を公表。Leap は、仏中銀と独連銀間で VPN（Virtual Private Network）を構築し、既存暗号と PQC のハイブリッドで通信するもの。
2023 年 11 月	イギリスの銀行協会（UK Finance）が、リスク・シナリオや対応方針に関する報告書を公表。
2024 年 1 月	世界経済フォーラムが、リスク対応における連携（民間部門と当局、国家間）の重要性に関する提言を公表。
2024 年 2 月	シンガポール金融管理局が、量子コンピュータによるリスクへの対応を金融機関に勧告。
2024 年 9 月	クレジットカード取引の国際的な決済技術の標準を策定する EMVCo が、リスク対応のポジション・ステートメントを公表。

2024 年 9 月	G7 のサイバー・エキスパート・グループが、リスク対応に関する提言を公表。
2024 年 10 月	FS-ISAC が、暗号アジリティ[4] の重要性と方法論のガイダンスを発表。
2024 年 11 月	預金取扱金融機関の耐量子計算機暗号への対応に関する検討会（PQC 検討会。事務局：金融庁）が報告書を公表。
2024 年 11 月	仏中銀・シンガポール金融管理局が、共同プロジェクト（メールへの PQC 実装）の報告書を公表。
2025 年 2 月	欧州域内の金融業界における PQC 移行の課題を検討するフォーラム Quantum Safe Financial Forum がリスク対応の推奨事項を公表。

わが国では、2024 年 11 月に、金融庁が事務局となって同年 7 月から 3 回にわたって開催された PQC 検討会による報告書が公表された[5]。同報告書では、PQC 移行対応において経営層が認識・対処すべき事項として、リーダーシップの発揮、および全社的な施策としての対応方針の策定を挙げている。また、PQC を使用可能にするタイミングに関して、優先度の高いシステムについては 2030 年代半ばとしているほか、海外の規制動向にも留意してタイミングを設定すべきであるとしている。移行に向けた事前準備として、暗号利用箇所やアルゴリズムの棚卸し、リスク評価、優先順位付けを挙げたうえで、これらへの早期着手を推奨している。また、IT ベンダーや金融インフラ提供事業者、フィンテック企業、政府当局、他の重要インフラ事業者といった多様なステークホルダーとの連携が重要であるとしている。

(3) PQC 対応にかかる今後の課題

CRQC によるリスクを取り巻く環境は今後も変化しうる。量子コンピュータの開発進捗状況、暗号の解読アルゴリズムに関する研究の進展、海外における規制動向をフォローしながら対応を進めていくことが求められる。また、PQC を搭載したソフトウェアやハードウェアを実装した後で、それらにおいて脆弱性が発見されるリスクもある。PQC 実装における脆弱性に備えた体制整備も必要となろう。

金融機関においては、まず、PQC 移行に向けた体制を整備することが必要である。具体的には、量子コンピュータや PQC に関する情報の収集、社内での PQC 対応の必要性に関する啓発活動、ステークホルダーとの調整、暗号使用箇所の調査と

4 暗号アジリティとは、別のアルゴリズムに入れ替えやすい特性を指す。
5 https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf

使用状況に関する情報の収集・管理体制（暗号インベントリ）の整備、リスク評価、他の金融機関や重要インフラ事業者との連携などが挙げられる。

次に、PQC 移行のロードマップの策定が求められる。わが国では、金融 ISAC において、金融業界としてのロードマップのひな形が検討されている。各金融機関は、このひな形を参照するかたちで、自社の事情に合致したロードマップを作成するという流れとなろう。また、こうした作業を通じて PQC 移行における課題を洗い出すとともに、それらを必要に応じてステークホルダーと共有し連携して対応することが重要である。長期的には、今回と同様に、暗号アルゴリズムの移行が将来必要となりうる点を踏まえ、暗号移行に柔軟かつ効率的に対応できるシステム・アーキテクチャを検討することが望ましい。

欧米では、業界団体やコミュニティによる検討や提言が活発化している。わが国でも、PQC 検討会の報告書を参照するなどして、各金融機関において検討が活発化することを期待したい。

5. 講演「AI がもたらすリスクに対するセキュリティ」

菅は、AI の研究開発動向を概観したうえで、AI がもたらす脅威とセキュリティ・リスク、対策の動向について、次のとおり講演した。

(1) AI の研究開発動向

AI のリスクを論じる際には、これをもたらす技術との対応関係を把握しておく必要がある。AI に対応する最も広い技術のクラスは機械学習であり、機械学習には多層のニューラル・ネットワーク・モデルを用いる深層学習が含まれる。そのうち、動画像や音声、テキストなどのコンテンツを出力するものが生成 AI である[6]。さらに、生成 AI の中に、汎用人工知能（artificial general intelligence: AGI）が含まれる。AGI は、人間のように広範な知識をもち、多様なタスクを処理し、思考する AI を指す概念である。10 年前には、AGI の到来は近未来に予見されないとの見方が大勢であったが、今日の最先端の生成 AI は、すでに AGI の領域に到達している。

これまで AI は、①諸分野の知を統合する方向、②情報処理とエネルギー消費の効率を高める方向に発展してきた。とくに、②の方向性は、単なるエネルギー節約

6 生成 AI は、必ずしも深層学習モデルである必要はないが、事実上、深層学習モデルに包含されると言ってよい。

を超えて、推論能力や汎化能力といった知性の獲得に本質的な役割を果たしたとみている。今後は、言語や動画などを統合処理するマルチ・モーダル化、推論能力の深化、自律的に行動するエージェント化によって、AI は現実世界の広範なタスクを処理できるようになり、用途が拡大していくと見込まれる。これに伴い、AI が社会にもたらす脅威も変化していくため、AI セキュリティの研究の重要性は高まっていくだろう。

(2) 深層学習モデルによる自然言語処理を可能にした技術進歩

第 3 次人工知能ブームのきっかけは、画像認識のコンペティションにおいて、畳み込みニューラル・ネットワークが従来の機械学習手法を大きく上回る性能を達成したことである。もっとも、この時点では、複雑な構造をもたない画像データであれば深層学習モデルで処理できるが、意味や文法などの複雑な構造をもつ自然言語はうまく処理できないだろうとの見方が一般的であった。

現在では、さまざまな工夫の積み重ねにより、自然言語処理が可能となっている。代表的なものには、注意機構と呼ばれるモデル・アーキテクチャの工夫がある。注意機構とは、文の中で重要性の高い部分に自動的に大きな重みを割り当てる仕組みを指す。注意機構以外にも幾つかの重要な工夫があり、その多くは 2013 年に開発された Word2Vec と呼ばれるモデルの登場時点で既に提唱されていた。1 つ目の工夫は、データ構造である。Word2Vec は、単語を高次元のベクトル空間に埋め込む。このとき、ベクトル空間において「queen」−「woman」+「man」=「king」といった意味の演算が概ね成立することから、ベクトル空間への埋め込みの有用性が注目を集めた。2 つ目は、文章生成のアルゴリズムである。コンピュータによる文章生成メカニズムを、意味や文法を捨象して、確率的なプロセスによる単語列の生成に単純化してとらえた。3 つ目は、訓練データである。Word2Vec は、ある単語の出現確率を、周辺にある単語群から推定する CBOW（continuous bag of words）という手法で推定した。これは、現代的には、自己教師あり学習と位置付けられる。大規模言語モデルでは、言語データの集合の一部を削り、その部分を周辺の文章から予測する「穴埋め問題」を大量に解くことで自己教師あり学習を行う。

(3) AI セキュリティ

AI セキュリティの研究分野は、① AI システムを守る、② AI を攻撃に悪用する、③ AI を防御に活用する、という 3 つの目的に分かれる。ここでは、①に焦点を当てて説明を行う。

イ．AIのセキュリティ・リスクの特徴

一般的な情報システムの脆弱性対応では、脆弱性のある部位を特定して修正することで、脆弱性の解消を行う。ここでの脆弱性のある部位とは、プログラム・ソースコードや設定ファイルなどの不具合（バグ）である。これに対し、深層学習モデルは、何億個ものモデル・パラメータの組み合わせで機能が発現しているため、機能の一部に不具合があっても、その原因となるパラメータを特定することは困難である。また、パラメータを特定できても、その数値を変更することで不具合を解消できるとは限らない。一般的な情報システムとは異なり、局所的な対応では機能の不具合が解消できない点が、深層学習モデルのセキュリティ・リスクの特徴である。

また、大規模言語モデルは、自己教師あり学習によって確率予測の精度を高めるという原理に基づいているため、リスクをゼロにすることも不可能である。セキュリティ・リスクに対処するには、モデルの頑健性向上などの技術的対応に加えて、サプライチェーン管理や利用者教育といった非技術的対応も合わせて必要になる。

ロ．失敗によるリスクの分類

深層学習モデルのセキュリティ・リスクを包括的に捉えるには、脆弱性という原因ではなく、モデルによって生じる不都合な事態、すなわち失敗を分類することが合理的と考えられる。その大まかな分類としては、セキュリティ、セーフティ、サプライチェーン・リスクがある。

（イ） セキュリティ

セキュリティは、悪意のある攻撃者がいるもとでの安全性を指す。例えば、敵対的サンプル攻撃は、入力データに微小なノイズを付加することにより、誤った出力データを誘発するものである。また、大規模言語モデルには、有害情報やプライバシー情報を出力しないように制限がかけられているが、プロンプト（入力文）の工夫により、この安全装置を巧みに回避するジェイル・ブレイク攻撃がある。ジェイル・ブレイク攻撃では、システム・プロンプトを無視するよう指示するプロンプトや、善良な目的を装うプロンプトが悪用される。バックドア攻撃は、条件付きで発動する不正な機能を機械学習モデルに埋め込む攻撃である。不正な機能は、攻撃者が定めた特徴（トリガー）を入力データが有している場合にのみ発動するため、通常は気が付きにくい。この攻撃は、機械学習モデルや訓練データを外部から調達する場合に脅威となるため、サプライチェーン・リスクとの関係が深い。

（ロ） セーフティ

セーフティは攻撃者がいないもとで安全を確保するものであり、モデル性能の不足のほか、倫理への適合性の問題がある。後者は、出力データがプライバシー保護

や差別などの倫理規範に抵触するリスクを指す。倫理規範は地域や文化によって異なるうえ、時代や利用目的によっても異なりうる。したがって、AI サービスを提供する事業者は、利用状況に応じて適切な対応がとれていることを、継続的に確認していくことが望ましい。

（ハ） サプライチェーン・リスク

サプライチェーン・リスクは、訓練データやモデルの社外からの調達、業務委託によって生じるリスクである。対応策を考慮する際には、セキュリティやセーフティにかかるリスクとあわせて評価する必要がある。

ハ. セキュリティ・リスクへの対策とまとめ

AI を安全に利用する対策アプローチとして、AI 自体の安全性の向上、AI に対する攻撃への対処、外部から調達した AI の検査、外部装置によるフェール・セーフな仕組みの導入、サプライチェーンまたは業務委託先の管理、利用者教育やリスク・コミュニケーションに分類できる。

最先端の AI は、すでに AGI の領域に到達しているが、その登場から間もない。今後は社会において AGI の活用が進み、その副作用も顕在化していくとみられる。その対処を考えるうえで、AI セキュリティの研究の重要性も高まっていくと思われる。

(4) 対談

人工知能学会傘下に設立された「安全性とセキュリティ研究会（SIG-SEC）」について、菅は、まず、設立発起人である大塚教授に立ち上げの経緯について尋ねた。大塚は、これまで、AI 研究者が研究する安全性は主に AI セーフティであり、サイバーセキュリティ研究者が研究する安全性は AI セキュリティであるという大まかな棲み分けがなされていた経緯を説明したうえで、AI 研究者とセキュリティ研究者の両者の知見を融合させていく必要があるという問題意識から SIG-SEC を設立したと説明した。そのうえで、両者の専門的知見から AI セーフティと AI セキュリティに関する研究を深めていきたいと説明した。

続いて、菅は、AGI の出現でサイバー攻撃と防御がどのように変化するかを問うた。大塚は、オープンソース・ソフトウェアにおいて、セキュリティ・パッチからエクスプロイト・コード[7] を生成する際に AI を悪用する研究事例を紹介し、マルウェアの作成が高度化、効率化する可能性を示唆した。サイバー防御に関しては、

7 ソフトウェアの脆弱性を悪用した不正な動作を再現するために作成されたスクリプトやプログラム。

DEF CON[8] において、AI のみでシステムの脆弱性を自動的に発見および修復するコンテストが 2 年がかりで開催されていることを紹介したうえで、こうしたコンテストで活用される手法から有益な示唆が得られると指摘した。

さらに、菅は、AGI を超えた超知能（Artificial Super Intelligence: ASI）のリスクをどのように考慮すべきかを尋ねた。大塚は、AI がメイン・タスクを達成するために、人間にとって有害なサブ・タスクを設定するリスクがあることを指摘した。例えば、コーヒーを淹れるタスクを課された AI が、コーヒー・メーカーの電源を抜こうとする人物がいたときに、目的達成のために当該人物を排除するという下位の目標を立ててしまうことがありうる。ASI のような人知を超えた AI であれば、人間の予測がつかない解決策を思いつき、思わぬリスクをもたらしうると述べた。

6. 講演「さまざまな決済スキームとそのセキュリティ」

田村は、デジタル決済に関する研究開発の経緯について紹介するとともに、決済スキームのセキュリティについて、次のとおり講演した。

(1) デジタル決済に関する研究の勃興

デジタル決済に関する研究は 1980 年代に遡る。インターネットや家庭用パソコンの普及、IC カードの実用化を背景に、デジタル決済に関する研究開発が盛んに行われた。こうした研究開発は、クレジットカードなどのアナログ処理で行われていた決済手段をデジタル化するものと、現金を代替する手段をデジタル技術で実現することを企図したものがあった。

金融研究所では、1990 年代より、現金を代替する手段である「電子現金」について研究を行っていた。電子現金は、現金の電子化を目指したものであり、現金に見立てた電子データのやり取りによって決済を完了させる方式をいう。具体的には、銀行から引き出した電子現金を IC カードに格納し、それをショッピングや個人間送金に利用するという運用が想定されていた。電子現金に関する実証実験も複数行われており、非対面決済を想定した「インターネットキャッシュ」と、主に対面決済を主とした「スーパーキャッシュ」と呼ばれる実証実験はその代表例である。

8 DEF CON は、毎年ラスベガスで開催されている大規模なセキュリティ・カンファレンス。企業や政府機関のセキュリティ研究者やハッカーが集まり、ハッキングの講演やハンズオン、Capture The Flag コンテストなどが開催される。

スーパーキャッシュの実証実験は、24 の金融機関、約 1000 の店舗、約 2.2 万人のユーザの協力を得て、大規模に実施されたと記録が残っている。実証実験の結果を踏まえて、普及に向けての課題などが整理されたが、その後は非接触 IC カードを利用した決済サービスが登場したことなどもあり、電子現金に関する検討は一旦収束した。

(2) 台帳を使用しない決済方式

現在、われわれが使っているキャッシュレス決済の多くは、サービス事業者が決済を仲介するものである。つまり、サービス事業者が台帳に決済内容を書き込むことにより決済が完了する。政府はキャッシュレス比率の最終目標を 8 割としており、今後のキャッシュレス決済のさらなる普及を見据えれば、サーバやネットワークの障害といった決済に及ぼしうる影響について、より一層の考慮が必要になってくると思われる。

電子現金における送金処理は、サーバを介さずユーザ 2 者間でのデータ通信に閉じるものであることから、サーバやネットワーク障害、あるいは、サーバの処理性能への依存度の面からは、優位な可能性があるといえる。そのほか、電子データそのものに価値を持たせたものであることから、例えば、電子現金にプログラム機能を持たせるといった応用も考えられる。この点、電子現金スキームは、決済に閉じない発展の可能性を秘めた技術であるとみている。

(3) 電子現金の基本構成

電子現金の基本スキームでは、電子現金を発行するサービス事業者のほか、サービス事業者とは独立した組織として認証機関を想定する。ユーザは認証機関に対してユーザ登録を行い、電子現金の送受信に使う鍵ペアに対する証明書の発行を受ける。ユーザはサービス事業者から発行された電子現金をインターネット、あるいは、近距離無線通信を通して別のユーザに送ることができる。電子現金は転々流通が可能であり、最終的にサービス事業者にすべて還流させることで二重使用チェックを行うというシンプルな構成となっている。

電子現金の偽造・改ざん対策は、サービス事業者によるデジタル署名によって実現される。電子現金の送受信は、電子現金の移転履歴とセットで行われ、その移転履歴には、電子現金の保有者に関する情報が記載される。これにより、正当な保有者以外のユーザが複製して使用することができないよう対策が講じられている。例えば、ユーザ A からユーザ B に電子現金を送信する際、A は移転履歴に B の公開

鍵に関する情報を記載してデジタル署名を付与する。B は、移転履歴を検証することで、A が自分宛てに送信したものであることを確認することができるほか、1 つ前の移転履歴をみることで、同電子現金が過去に A に送金されたものであることを確認できる。移転履歴の更新に使用するデジタル署名用の秘密鍵については、本人であっても不正な使い方ができないようセキュリティ対策を講じておくことが必要であるが、中長期的観点からは、セキュリティ機能の安全性が低下する可能性についても考慮が必要である。電子現金スキームには、事後的な二重使用検知機能が付与されており、還流してきた電子現金のなかに同じシリアルナンバーをもつものが存在した場合、それぞれの移転履歴を比較することで二重使用者を特定できるようになっている。

(4) 電子現金の実機検証

今般、現行技術で電子現金を実装した場合、どの程度のユーザビリティを確保しうるか再検討を行った。電子現金の送受信処理についてボトルネックとなるのは、送金ユーザ側で行われる移転履歴更新にかかる時間と、データの通信時間である。そこで、現行のスマートフォンを用いて実機検証を行ったところ、100 枚の電子現金の送受信にかかるトータル時間を 230 ミリ秒（0.23 秒）と概算することができ、既存の非接触 IC カードによる決済手段とほぼ同程度の時間で送受信できることがわかった。もっとも、電子現金の場合には、送金先の選択や送金額の入力といったスマートフォンでのアプリ操作が必要となるが、実用可能性は低くないとの結果が得られたといえる。

そのほか、更なる効率化やプライバシー強化の方法についても検討を行っており、詳しい内容をディスカッション・ペーパーにまとめている[9]。なお、今回の実機検証は技術的な観点からの検証を目的としたものであり、法律や制度、実運用等、社会実装に向けた実現可能性は検討の対象外である。

(5) 決済スキームのセキュリティ

オンラインでのクレジットカード決済、インターネットバンキング、コード決済といった既存の決済サービスは、台帳ですべての取引を管理している。そのため、不正な取引については、サービス事業者が検知できるようになっている。これらの

9 田村ほか、「台帳を用いない決済方式に関する技術面からの一考察」、『金融研究』第 44 巻第 3 号、日本銀行金融研究所、2025 年、79～136 頁

サービスでは、サーバ側でアカウント管理しており、アカウントにログインした者が正しいユーザであるということを前提としていることが多い。こうしたログインにはパスワードを用いるものが多いため、人の脆弱性を突いてパスワードを特定しようとする攻撃への対策が非常に重要となる。フィッシング詐欺はその一例であり、正しくユーザ認証を行うことの難しさが顕著となっていることを表している。

また、暗号資産については、台帳ですべての取引が管理されているという点は既存の決済サービスと同じであるほか、不正な取引もブロックチェーン参加者によって排除される。暗号資産取引は、デジタル署名を付与したトランザクションデータの記録によって行われるものであることから、不正送金を防止するには、正当なユーザだけが秘密鍵を用いた署名を生成できるような仕組みが必要となる。実際、秘密鍵を安全に保管するためのウォレットと呼ばれるデバイスが多く登場している。

これに対し、電子現金には、取引を記録する台帳はないが、他人の電子現金を複製して使用しようとした場合には、電子現金の受信側でこれを検知することができる。しかしながら、送信者が過去に使用した電子現金を再度使用するような二重使用については、受信側で検知することができない。そのため、電子現金スキームでは、サービス事業者が還流した電子現金を事後的にチェックすることとしている。なりすまし対策については、暗号資産と同様、電子現金送信時に生成するデジタル署名用の秘密鍵を安全に保管することが重要となる。そのため、電子現金の実装を考えるにあたっては、暗号資産分野で先行しているセキュリティ対策の事例が参考になろう。

(6) 対談

まず、面から、デジタル決済等に使用するデジタル・ウォレットの種類とそのセキュリティについて説明が行われた。デジタル・ウォレットとは、一般に、重要なデジタルデータを保管するデバイスを指し、暗号資産取引に使用するウォレット、個人情報などを管理する ID 管理ウォレットなどがある。このうち、暗号資産ウォレットは、一般に、ホット・ウォレットとコールド・ウォレットに分類され、コールド・ウォレットの方が安全であるといわれている。しかしながら、これらはデバイスが常時インターネットに接続した状態か否かで分類したものに過ぎず、コールド・ウォレットであっても、暗号資産の取引時にインターネットに接続されれば、ホット・ウォレットと同様のリスクが生じると指摘された。

これに対して、田村は、PC 等がマルウェアに感染した場合のリスクについて尋ねた。面は、マルウェアによるリスクとして、送金先の改ざんにより暗号資産が意

図しない先に送金されてしまう可能性を指摘した。ブロックチェーンに書き込まれた取引は取り消すことができないため、送金内容をモニタで人間が最終確認するなど、マルウェアに感染したとしても安全に取引できるようにするという考えが重要であるとの見方を示した。

また、面は、マイナンバーカードに搭載される暗号アルゴリズムが 2026 年を目途に ECDSA（Elliptic Curve Digital Signature Algorithm）に移行することを受け、ECDSA を使用している暗号資産用のウォレットとしてマイナンバーカードを応用できる可能性を指摘した。もっとも、デジタル署名用の鍵ペアはマイナンバーカードごとに固定であるため、これをそのまま暗号資産取引に使用すると、異なる取引が同一ユーザによるものであるという情報が露呈することでプライバシーの問題が生じる可能性があると指摘した。

これに関連して、田村は、電子現金においても同様の課題があることを紹介し、取引用の鍵ペアを都度生成することで取引の関連付けを切断するとともに、ゼロ知識証明を使用して、認証機関に登録を行った正しいユーザであることを証明する方法を紹介した。

7. 講演「金融分野における今後のセキュリティ対策―シンポジウム総括を兼ねて―」

岩下[10] は、シンポジウムの総括を兼ねて、CITECS における課題や今後の活動への期待について述べたうえで、金融分野における今後のセキュリティ対策について、次のとおり講演した。

(1) シンポジウムの総括

本日のシンポジウムでは、CITECS における 20 年の活動を振り返るとともに、現在のセキュリティ上の課題が整理され、金融分野のセキュリティ対策を考えるうえで大変有益なものとなった。PQC 移行については、金融機関のセキュリティ関係者の間では話題になっているものの、必ずしも正しい情報が共有されていないとも感じており、今回のような客観的かつ正確な情報発信は非常に重要である。また、AI セキュリティについては、生成 AI の台頭に伴うセキュリティ・リスク、倫理的

10 岩下教授は、日本銀行において金融分野における情報セキュリティ技術の研究に従事し、CITECS の初代センター長を務めた。

課題、金融業界が直面する新たな課題について多くの洞察が得られた。生成 AI の仕組みを理解することは容易ではないものの、その活用にあたっては、仕組みを理解したうえでリスクを認識しておくことが必要との示唆が得られた。また、決済スキームのセキュリティに関する講演では電子現金に関する検討結果が紹介された。近年、ステーブルコインと呼ばれる暗号資産が注目を集めているが、技術への理解が乏しいユーザの参加が増えてきているのも事実であり、電子現金スキームの再検討から得られる知見をもとに理解を深めていってほしいと思う。

(2) 金融機関に必要な対応

金融機関が直面する状況はそれぞれに異なり、脅威の確度も一概に断定できるものではない。そのため、金融機関には、常に最新の情報をアップデートして、自らが知る範囲を最大限に拡大しながら、適時適切に最善の決断を下すことが求められる。そのためには、技術研究者と金融機関実務家とをつなぐ結節点のような存在が必要であり、それこそが CITECS なのであろうと思う。

(3) セキュリティとセイフティ

日本において「安全」という言葉は、セキュリティ（Security）とセイフティ（Safety）の両方を含む。インターネットが普及する以前は、外部からの脅威に対する「セキュリティ」はあまり重要ではなかった。実際、金融情報システムセンターによる安全対策基準においては、不慮の事故やバグによるシステム停止への対策を、「セイフティ」の意味で安全対策と呼んでいたが、世界中の端末がインターネットでつながったことにより、セキュリティの重要性は徐々に増していった。

わが国の金融機関は、長きにわたってインターネットから切り離すことで、社内システムのセキュリティを確保するという考え方を採用していたが、最近ではインターネットとフルに接続したうえで、しっかりシステムの安全性を確保する「サイバーハイジーン[11]」という考え方に移行しつつある。

(4) CITECS に期待する役割

CITECS の活動は、単なる技術研究にとどまらず、社会的インパクトや社会実装、

11 マルウェア感染などを予防し、IT 環境を健康・健全に維持する衛生（ハイジーン）管理のことをいう。

標準化、法規制との関わりを通じて金融分野におけるイノベーションを支えてきた。今後も、未知の技術やリスクへの挑戦を続け、金融分野の情報セキュリティの未来を切り開いていくことを期待したい。

そのためには、まず、①基盤技術の検証が必要である。どの技術が金融分野のセキュリティを支える基盤となるかを評価し、短期的な流行に惑わされることなく長期的な視点で検討することが求められる。そのうえで、②結節点としての機能を持ち合わせてほしい。研究者、技術者、実務家をつなぎ、単なる技術研究ではなく、実際に使われる技術に育てていくといった役割を担うことが求められよう。また、③技術の受容プロセスの支援も必要である。「何の役に立つのか？」という疑問が持たれる段階から研究し、十分な検討を経て、社会に受け入れられる道筋をつくっていくという取組みを期待したい。

(5) CITECS の今後の課題

CITECS における今後の課題は、①既存技術の維持と継承である。安全であることが当たり前になると、安全対策のための技術が適切に維持・継承されないリスクがある。CITECS にとっては、コモディティ化した技術をどう支えていくかが課題となろう。2 つ目の課題は、②新しい技術領域への挑戦である。CITECS には、未来の基盤技術を発掘し、既存の枠組みでは捉えられないリスクを先取りする力を備えてほしい。3 つ目は、③社会実装のギャップを埋めることであり、技術的な正しさだけでなく、実際に使われる技術としての現実的な道筋をつくることである。

安全であることが当然の世界において、CITECS が果たすべき役割は、研究・技術・実務の間に生じるズレを調整し、先を見据えて動くことにあると思う。未来を予測するのではなく、変化に適応し、技術の受容プロセスを支える役割こそを、CITECS の強みとしていってほしい。

金融機関における AI 利用に伴う私法上のリスクと管理

金融機関における AI の利用を巡る法律問題研究会

要　旨

本稿は、日本銀行金融研究所が設置した「金融機関における AI の利用を巡る法律問題研究会」（メンバー〈50 音順、敬称略〉：井上聡、加毛明、神作裕之、神田秀樹〈座長〉、宍戸常寿、事務局：日本銀行金融研究所）の報告書である。

Artificial Intelligence（人工知能。以下、「AI」という。）技術の急速な進展とともに、AI の利用に対する期待も高まりを見せている。金融分野でも、さまざまなデータを利用した AI の導入が進んでいる。そこで、本報告書では、金融機関の AI 利用を巡る法的な課題を明らかにすることを目的として、AI の利用に伴う法的リスクとその管理のあり方について分析を行った。

主な指摘事項は次のとおりである。（i）AI モデルまたはシステムの開発・導入等の局面については、金融機関が AI 開発者・AI 提供者に対する契約責任を追及する場合の問題点と望ましい契約上の定めについて検討を行った。（ii）金融機関が AI を用いたサービスを顧客に提供する局面については、顧客に対する金融機関の責任の内容を確認し、一定の場合にはあらかじめ AI 利用にかかる契約を顧客との間で締結する必要があることを指摘した。（iii）組織内部のリスク管理の局面については、AI の利用に伴うリスク管理の必要性と取締役の AI ガバナンス体制構築義務を前提に具体的なリスク管理のあり方を示した。

AI は技術の進展が非常に速く、法的リスクについても不断の見直しを行っていく必要性が高い。本報告書で示した視点を契機として、金融機関における AI の利用にかかわる利害関係者が法的リスクにどのように対応していくべきかという観点での議論が深まっていくことが期待される。

本報告書の内容や意見は、日本銀行の公式見解を示すものではない。

1. はじめに

Artificial Intelligence（人工知能。以下、「AI」という。）[1] 技術の急速な進展とともに、AI の利用に対する期待も高まりを見せている。金融分野では、これまでもさまざまなデータを利用した AI の導入が進められてきており[2]、近年では、生成 AI の導入に向けた検討が進んでいる[3]。

一方で、AI に関するルールについては、特定の領域における限定的な規制を除き、法的拘束力のある横断的な規制には各国で慎重な姿勢がとられてきた。そうした中、欧州では 2024 年 5 月に AI Act[4] が制定され、わが国でも 2025 年 5 月に「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」が国会で成立したところである。

わが国では、生成 AI を含む AI のリスクを踏まえ、安全で安心な環境を確保しながらイノベーションを促進させるため、ソフトローによる AI リスク対応がなされてきた。2024 年 4 月に公表された「AI 事業者ガイドライン」（総務省・経済産業省［2025］）は、AI に関するシステムのライフサイクルにおける役割を基準として、AI に関する事業活動を担う主体を大別し、共通の指針と主体ごとの重要事項、事業者が構築すべき AI ガバナンスの基本モデルを示している。

本報告書は、金融機関の AI 利用を巡る法的な課題を明らかにすることを目的として、AI 利用に伴う法的論点を抽出し、それに対する解釈論または立法論による解決可能性の検討を試みる。AI は技術の進展が非常に速いため、法的論点についても不断に見直しを行っていく必要があるが、AI に関するシステムのライフサイクルにおいて、どの部分に、どのようなルールが必要かを見定めるうえでも、現行

1 AI システム（活用の過程を通じてさまざまなレベルの自律性をもって動作し学習する機能を有するソフトウェアを要素として含むシステム）自体または機械学習をするソフトウェアもしくはプログラムを含む抽象的な概念との定義による。総務省・経済産業省［2025］9 頁。

2 Crisanto *et al.* [2024] p. 3. アルゴリズム・AI の利用を巡る法律問題研究会［2019］でも、アルゴリズム・AI による投資判断を提供する業者を前提としてではあるが、損害発生時の責任分担等について分析を行っている。

3 日本銀行金融機構局［2024］は、2024 年 4 月から 5 月にかけて実施した金融機関における生成 AI の利用に関するアンケート調査結果を公表しており、当該時点では約 3 割の先が生成 AI を既に利用しているほか、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 割であった。また、現時点では、わが国金融機関の AI モデルの利用は、構想段階または初期段階であるが、技術進歩のスピードを踏まえると、今後より広範に、金融業における中核的な業務でも利用される可能性が高い。金融庁［2024］2 頁。

4 正式名称は、Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

法のもとで、AI の利用にかかわる利害関係者が対応しうる法的問題であるかを検討しておく意義がある。

本報告書は、こうした問題意識のもと、日本銀行金融研究所に 2025 年 2 月に設けられた「金融機関における AI の利用を巡る法律問題研究会」における議論を事務局の責任において取りまとめたものである。なお、本報告書において意見にわたる部分は、日本銀行または金融研究所の公式見解を示すものではない。

「金融機関における AI の利用を巡る法律問題研究会」メンバー

（五十音順、敬称略、2025 年 5 月末時点）

井上　　聡　弁護士（長島・大野・常松法律事務所パートナー）
加毛　　明　東京大学大学院法学政治学研究科教授
神作　裕之　学習院大学法学部教授
（座長）神田　秀樹　東京大学名誉教授
宍戸　常寿　東京大学大学院法学政治学研究科教授
（事務局）
渡辺　真吾　日本銀行金融研究所長
鈴木　淳人　前日本銀行金融研究所参事役
河野真一郎　日本銀行金融研究所制度基盤研究課長
兒玉　啓宗　日本銀行金融研究所法制度研究グループ長
山本　慶子　日本銀行金融研究所企画役補佐
大島あゆみ　日本銀行金融研究所企画役補佐
石岡　佑太　日本銀行金融研究所
小川　紘一　日本銀行金融研究所（田辺総合法律事務所弁護士）

本報告書の構成は、次のとおりである。2 節において本報告書の検討対象とする法的論点と金融機関における AI の利用態様について確認を行う。3〜5 節において、AI の利用に伴う法的リスクとその管理のあり方を分析する。最後に、6 節において、以上の検討の結果を総括する。

2. 検討の対象

(1) 法的論点

イ. 私法上の論点

金融機関における AI 利用に関連する法的論点は多岐にわたるが[5]、本報告書では、金融機関における AI 利用が進展するにつれ、より、中心的かつ重要な法的論点になると考えられる利害関係者間の責任の所在という私法上の論点、すなわち、AI が不正確な情報を生成し、それが損害発生につながる場合、誰が何を根拠に誰に対して責任追及しうるかという問題[6] を議論する。

上記以外の主な論点として、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下、「個人情報保護法」という。）上の論点[7]、知的財産法上の論点[8] や競争法上の論点[9] 等を挙げることができるが、これらについては、すでに検討が進められている[10]。

なお、本報告書では、生成 AI[11] を含めた AI 一般を検討の対象とする。AI とりわけ生成 AI に関する技術が著しく発展し、金融分野を含めて広く利用されつつある中、AI 技術が抱える問題であるブラックボックス問題、バイアス問題、ハルシネー

5 AI のもたらしうるリスクの例と関係する主要法令を整理したものとして、AI 戦略会議・AI 制度研究会［2025］8～9 頁がある。

6 AI システムの開発、提供、利用にかかわるすべての主体間での責任分担を明確にすることが必要との指摘がなされているほか（金融データ活用推進協会［2024］77～79 頁）、AI に関する責任を分析したものとして、福岡［2020］148～162 頁。法と経済学の見地から、AI の利用によって発生した事故についての責任と法規整のあり方を検討したものとして森田［2017］がある。

7 例えば、学習データの提供やプロンプト入力、生成される情報等が、第三者提供や情報漏洩に該当しうる可能性等が考えられる。

8 例えば、データを学習し、コンテンツを生成する際に著作権またはそれ以外の知的財産権等の侵害が生じる可能性等が考えられる。

9 例えば、大規模言語モデル（Large Language Model: LLM）開発には莫大なコストがかかるため、ビッグ・テック企業の寡占状態にあるところ、各事業者が同一の AI を利用する場合には、価格設定にあたり事業者間で合意がなくても、AI の並行利用による協調的行為として私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号）上禁止されるカルテルに該当しうる可能性等が考えられる。

10 個人情報保護法上の論点に関しては、個人情報保護委員会による注意喚起がなされているほか（https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/）、知的財産法上の論点に関しては文化審議会著作権分科会法制度小委員会［2024］、AI 時代の知的財産権検討会［2024］がある。競争法上の論点に関しては、公正取引委員会より、ディスカッションペーパー（公正取引委員会［2024］）や実態調査を踏まえた報告書（公正取引委員会［2025］）が公表されている。

11 文章、画像、プログラム等を生成できる AI モデルに基づく AI の総称との定義による。総務省・経済産業省［2025］10 頁。Bank for International Settlements [2024] p. 94. も、Generative AI とは、自然言語のプロンプトからテキスト、画像、音楽等のコンテンツを生成できる AI を指すと定義している。

ション問題等（BOX 参照）[12] は、いずれも機械学習や深層学習の技術に起因しているため、これらを包含的に検討することが適当と考えられる。

BOX: AI 技術が抱える問題

（ブラックボックス問題）

機械学習、とりわけ深層学習による判定は高精度であるが、なぜそう判定したのか、人間に理解可能なかたちで理由を説明するものではない。深層学習の判定結果は、多層ニューラルネットワーク中のリンクの重みに基づいたものであり、その複雑な処理に基づいた判定根拠を人間が理解することは困難であるため、深層学習はブラックボックスといわれる。

ブラックボックスには、上記のように、モデルの内部構造や意思決定プロセスの解釈の困難性に関する問題のほか、データとプロセスの履歴や追跡（トレーサビリティ）の困難性が問題になることもある。また、確率モデルに基づくため、どのような条件でどのような結果が得られるかを 100％予測したり保証したりできないことが問題になることもある。

（バイアス問題）

機械学習の判定結果は、学習データ（訓練データ）の傾向を反映するため、学習データにバイアスが含まれていると、判定結果にもバイアスが反映される。学習データに差別的な内容が含まれる場合は、AI の出力結果にも反映される可能性がある。

（ハルシネーション問題）

生成 AI は、深層学習による確率モデルに基づき、自然でもっともらしい応答を返してくるが、ウソや架空の出来事をあたかも事実であるかのような回答を生成する（ハルシネーション）問題が伴いうる。

ロ．責任の所在を前提としたリスク管理の必要性

金融機関を含む事業者は、AI 技術によってもたらされるビジネスチャンスやリスク――AI が組織内でどのように利用され、どのような価値を生み出しているか、また、それに伴うリスクがどのように管理、軽減されているかを、十分に理解する必要がある。AI 利用に伴うリスクを踏まえ、組織としてどのようなリスク管理が必要かという AI ガバナンス構築の必要性は、金融機関にとどまらず AI を利用しようとする事業者一般に広く認識されているものの、現状は、事業者レベル、自主団

12 国立研究開発法人科学技術振興機構研究開発戦略センター［2023］19 頁、同［2024］9、14 頁、同［2025］15、122 頁。

体レベルで、AIポリシー、管理ルール、利用ルールの策定または検討がなされているにとどまっている[13]。

会社法のもとでは、取締役について、組織内におけるAIガバナンスを構築する責任、すなわちAIガバナンス体制構築義務が、内部統制システム構築義務[14]の一内容として求められると考えられるが、その具体的な内容は明らかではない。本報告書で検討の対象となる私法上の論点すなわちAIの利用に伴う法的リスクを踏まえ、組織として、どのようなリスク管理をしていくか自体も、重要な法的論点の1つといえる。

(2) 金融機関におけるAIの利用態様

現時点での金融機関におけるAIの利用実態[15]を踏まえると、総務省・経済産業省［2025］（AI事業者ガイドライン）を前提に、次の3つの類型に整理することが考えられる（図1参照）[16]。

まず、①汎用的AIサービス利用型である。これは、事業者A（AI利用者[17]）が事業者C（AI開発者[18]・AI提供者[19]）の提供する汎用的AIサービスを利用する類型である。事業者Aが汎用的AIモデルをシステムに組み込んだサービスを利用するケースであるが、当該サービスに事業者Aが自らシステム開発を行うケースも含まれる。

次に、②カスタマイズ型である。これは、事業者C（AI開発者・AI提供者）の開発・提供する汎用的AIサービスを利用する事業者B（AI利用者）がAI提供者となって事業者A（AI利用者）向けに改良・調整し、事業者Aが利用する類型である。この類型には、事業者Aが事業者Bに対してAIサービスの改良・調整を

13 AIガバナンス協会AIガバナンス実装ワーキンググループ［2024］では、AIガバナンスの民間での自主取組みを進めるハブとして蓄積された知見がまとめられている。

14 神田［2025］258頁。田中［2025a］292頁。藤田［2019］376頁。最一判平成21年7月9日裁判集民231号241頁。

15 例えば、金融庁［2025］14〜15頁。

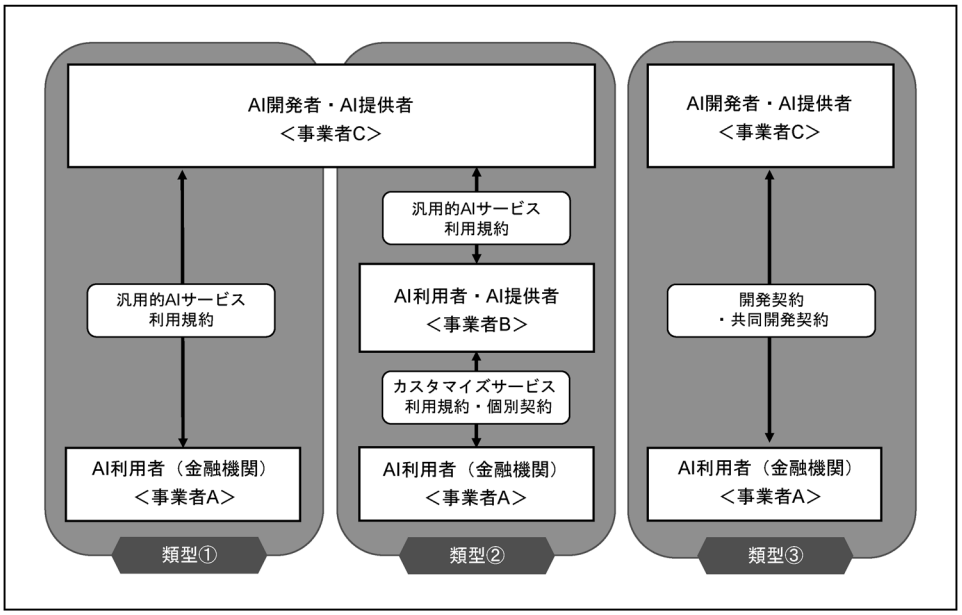
16 経済産業省［2025］7〜8頁。

17 他者が実装したAIシステムをサービスに組み込み、AIサービスとして利用する者、または提供されているAIサービスを利用する者。AI戦略会議・AI制度研究会［2025］5頁。総務省・経済産業省［2025］は、事業活動において、AIシステムまたはAIサービスを利用する事業者をいうとしており、業務外利用者（事業活動以外でAIを利用する者またはAIを直接事業で利用せずにAIシステム・サービスの便益を享受する、場合によっては損失を被る者）は対象としていない。

18 データ収集やモデル学習、そのほかモデルのシステム基盤構築や入出力機能等の開発を行う者。AI戦略会議・AI制度研究会［2025］5頁。総務省・経済産業省［2025］5頁もほぼ同旨。

19 既存または新規システムにAIを組み込み、サービスに利用可能な状態でAIシステムを提供する者、またはAIの組込みからAIサービスの提供まで実施する者。AI戦略会議・AI制度研究会［2025］5頁。総務省・経済産業省［2025］5頁もほぼ同旨。

図１　３つの類型における契約関係の整理



（経済産業省［2025］をもとに作成）

内容とするシステム開発を依頼するケースや、事業者 A の依頼を前提とせずに事業者 B が自ら開発した付加的な機能を組み合わせた AI サービスを提供するケースがある。類型②のカスタマイズには、追加学習、ファインチューニング、Retrieval Augmented Generation（検索拡張生成。以下、「RAG」という。）[20] 等が含まれる。

最後に、③新規開発型である。これは、事業者 A（AI 利用者）が事業者 C（AI 開発者・AI 提供者）と提携して独自の AI モデルまたはシステムを開発・利用する類型である。AI の開発を手掛ける事業者 C に対し、より業務に特化したモデル・システム開発を依頼するケースといえる。

続いて、これらの類型における契約関係を確認する[21]。

まず、類型①においては、汎用的 AI モデルそのものの開発を行い、それを組み込んだサービスを提供する事業者 C（AI 開発者・AI 提供者）に対して、当該サービスを利用しようとする事業者 A（AI 利用者）がモデルの開発を直接依頼することは想定されず（開発契約は締結されない）、事業者 C と事業者 A との間には、利

20 ユーザからの入力（プロンプト）を生成 AI に渡す前に別途用意した外部知識ベース（専門知識や社内情報等）から検索し、プロンプトだけでなく検索結果から抽出した情報もあわせて生成 AI に渡して応答を生成させるものであり、よりカスタマイズされた応答が可能になるため、ハルシネーション抑制効果も見込まれている。国立研究開発法人科学技術振興機構研究開発戦略センター［2024］47 頁。

21 経済産業省［2025］7〜9 頁も同旨。

用規約に基づく合意が存在する。場合によっては、当該利用規約に基づく契約関係に加えて、事業者 C が提供する導入支援等のサービス提供契約が存在しうる。

次に、類型②においては、2 つの契約関係が存在する。1 つは、類型①の契約関係、すなわち汎用的な AI サービスを提供する事業者 C と当該 AI サービスを利用する事業者 B との間の契約関係であり、もう 1 つは、当該事業者 B が上記とは別の AI サービスの提供者となって当該 AI サービスを利用する事業者 A との間で締結する契約関係である。以下では、前者の契約関係は、類型①の契約関係（利用規約に基づく合意等）と同様であることを前提として、後者の契約関係については、AI サービスの提供者である事業者 B が用意する利用規約に基づく合意が存在する場合と、個別に締結される契約が存在する場合がありうることを前提として、検討を行う。

最後に、類型③においては、事業者 C（AI 開発者・AI 提供者）と事業者 A（AI 利用者）との間で開発契約または共同開発契約が締結されることになる。

以下では、AI の利用に伴う法的リスクを分析する目的から、金融機関の AI 開発者・AI 提供者に対する責任追及（3 節参照）と、AI を用いたサービスを提供する局面における金融機関の責任（4 節参照）について分析を行い、金融機関の AI ガバナンス体制構築義務の内容、とくに具体的なリスク管理のあり方について検討を行う（5 節参照）。

3. 金融機関の AI 開発者・AI 提供者に対する責任追及

金融機関が利用する AI モデルまたはシステムにおいて、AI が生成した不正確な情報に基づく意思決定または自動処理によって、金融機関が顧客または第三者に対する損害賠償責任を負担する可能性や、期待されていた収益機会を逸する可能性がある。

例えば、金融機関が AI モデルまたはシステムを用いたサービスをその顧客（事業者のみならず、預金者等の個人を含む。以下、「AI 顧客」という。）に提供していたところ、AI が生成した不正確な情報に基づく自動処理がなされ、AI 顧客に対する損害賠償責任を金融機関が負担する場合を考える。このとき、金融機関は、当該 AI モデルまたはシステムを開発・提供した者に対し、いかなる請求を行うことができるか。金融機関と AI 開発者・AI 提供者との間の契約に基づく責任追及の可能性を検討しておくことによって（本節（1）および（2）参照）、AI の開発・導入の局面における法的リスクが明確になると同時に、あらかじめ締結しておくことが望ましい契約内容の明確化につながると考えられる（本節（3）参照）。

なお、金融機関における AI の利用態様は、2 節（2）のとおり、①汎用的 AI サー

ビス利用型、②カスタマイズ型、③新規開発型があることから、必要に応じてそれらに言及する。

(1) 契約の類型に基づく分析

システム・ソフトウェアの開発委託にかかる契約については、請負契約（民法 632 条）または準委任契約（同法 656 条・643 条）が選択されるのが一般的である[22、23]。請負契約のもとでは、開発者は完成義務（同法 632 条）を負うほか、合意した仕様どおりにシステムやソフトウェアが動作しない場合には、当該動作不良の原因について契約不適合責任（同法 559 条・562 条～565 条、636 条）を問われうる。これに対し、準委任契約のもとでは、開発者は善管注意義務（同法 644 条）を負い、当該義務違反を理由とする債務不履行責任を問われる可能性がある。

AI 開発においても同様であり、仮に、請負契約であることが契約上明らかであれば、AI 開発者・AI 提供者には完成義務が認められ、契約不適合責任が問題となりうるほか、準委任契約であっても債務不履行責任が問題となりうる[24]。

もっとも、民法上の典型契約に関する規定は、当事者間の合意がない場合に適用されるものにすぎず、当事者の合意次第では、請負契約や準委任契約に当てはまらない場合もありうる。AI 開発者・AI 提供者の債務の内容を確定するうえでは、契約によって求められる成果の内容や水準が重要な論点となると考えられる[25]。そこで、以下では、AI 開発者・AI 提供者と金融機関との契約の内容について分析を行うこととする。

(2) 契約の内容に基づく分析

イ. 性能保証条項の有無

（イ） 性能保証の可否

AI システムを構成する AI モデル部分に関しては、完全な性能を想定できず、とりわけ未知のデータを前提とした性能保証は困難であるとの指摘もある一方[26]、評価用データを前提として契約当事者が性能保証を合意できる場合も存在してい

22 システム開発について、森・濱田松本法律事務所ほか［2022］23～25 頁。多くの場合、当事者間で契約形態について意見が対立するため、実務上は、準委任型・請負型の折衷的な契約形態（成果完成を報酬支払の基準とする準委任型）がとられる場合が少なくないとされる。中崎［2024］393 頁。

23 ソフトウェア開発について、東京地方裁判所プラクティス委員会第二小委員会［2011］5 頁。

24 経済産業省［2025］31 頁。

25 経済産業省［2025］31 頁。

26 経済産業省［2018］18～22、33～34 頁。従来型のソフトウェアでは、開発段階で取り扱われなかっ

る[27]。性能保証がある場合、AI 開発者・AI 提供者は、合意された性能を実現する義務を負い、保証された性能が実現されない場合には債務不履行責任を負うことになる（契約が全体として準委任契約と性質決定される場合でも、性能保証の合意については、このように解される）。性能保証に関する合意は、金融機関による AI 開発者・AI 提供者の責任追及を容易にする一方で、AI 開発者・AI 提供者にとっても、性能保証とりわけ評価指標に関する合意をしておくことにより、自らの責任範囲を明確化することができる。

もっとも、類型①または②で典型的なように、AI モデルまたはシステムでは完全な性能を想定できない場合があり、そうした状況下にあっては、AI 開発者・AI 提供者が明示的に積極的な性能保証を行うことは困難と考えられる（むしろ、後述のとおり、性能に起因した損害賠償責任についての免除や制限が契約上定められている例がある。本節（2）ロ．参照）。ただし、当事者間で仕様および性能についての明示的な合意がない場合であっても、当事者意思の合理的解釈により、本来あるべき状態としての仕様および性能を確定することができれば、それによることが考えられる[28]。

（ロ） カスタマイズと性能保証

金融機関は、汎用的 AI サービスをそのまま利用する場合もあるが（類型①）、何らかのカスタマイズがなされたものを利用する場合がある。類型①を前提として自らカスタマイズする場合のほか、類型②の場合がこれに相当する[29]。

さらに、類型②には、カスタマイズを行う事業者（以下、「カスタマイズ事業者」という。）が、自ら汎用的 AI サービスをもとにカスタマイズを行い、それに基づく AI サービスを広く提供するもの（類型②-1）と、特定の顧客の依頼に基づくカスタマイズを行い、当該顧客に提供するものがある（類型②-2）。類型②-1 におけるカスタマイズは、特定の顧客の依頼に基づくものではなく、開発委託関係はないことから、AI 利用者に対する性能保証が合意されることは想定しがたい[30]。一方、類型②-2 は、特定の顧客の依頼に基づくカスタマイズであり、開発委託関係があること

た未知のデータの処理についても、事前に一定の性能保証を行うことができる場合があるが、AI モデルに関しては、学習用データセット以外の未知のデータに対しての挙動が不明確とされている。

27 実務的な解決策としては、評価用データを入力した場合の性能保証条項を置くことがあげられている。影島［2020］22 頁。現に性能保証があるケースも存在しているといわれている。

28 東京地方裁判所プラクティス委員会第二小委員会［2011］16 頁。ソフトウェア開発についての分析ではあるが、例えば、要件定義書・基本設計書に特段明示されていないが、本来ならば必要なはずの機能がないため、現状のシステムでは業務に支障がある場合が挙げられている。

29 金融庁［2025］14～15 頁。類型③については、汎用的 AI サービスを前提としていないという違いはあるが、そもそも、顧客の依頼に応じた開発委託はカスタマイズが前提となっており、カスタマイズ部分についての別個の性能保証の合意を観念する必要はない。

30 もっとも、追加的に、顧客の依頼に基づくカスタマイズがなされるケースも観念しうるが、その場合の帰結は類型②-2 に準じることになる。

から、性能保証の合意がある場合やカスタマイズ事業者が完成義務を負っていると解される場合もありうると考えられる。

類型②-1 または類型②-2 で性能保証に関する合意がない場合であっても、カスタマイズ事業者たる AI 開発者・AI 提供者が、AI サービスの提供契約（準委任契約）に基づく善管注意義務[31] 違反を根拠に債務不履行責任を負う可能性はあると考えられる。AI のモデルまたはシステム開発に即していうと、AI 開発者・AI 提供者は、AI 開発の専門家（ベンダ）として一般的に要求される平均的な注意義務を負い、平均的な AI 開発の専門家（ベンダ）であれば適切に処理できるであろうことを行わなければ、善管注意義務違反を問われうると解される。例えば、カスタマイズ事業者によるカスタマイズ部分が原因で不正確な情報が生成された場合には、その善管注意義務違反が問題となりうると考えられる[32]。ただし、金融機関が、カスタマイズ事業者が平均的なベンダの注意義務を尽くしていたか否かを立証することは、通常は容易ではないと考えられる[33]。

類型②の深刻な問題は、カスタマイズ事業者が実装したカスタマイズ部分と、基盤となっている AI モデルのいずれが原因となって不正確な情報が生成されたかが明らかではない場合に生じる。カスタマイズ事業者は、基盤となっている AI モデルに起因する不具合・リスクをコントロールできる地位にない。したがって、カスタマイズ事業者の完成義務が認められうる範囲としても、善管注意義務の及ぶ範囲としても、カスタマイズ部分に限定するのが相当であると考えられる。こうしたもとでは、少なくとも、カスタマイズ部分に起因して問題が生じていることが立証できなければ、金融機関によるカスタマイズ事業者に対する債務不履行責任の追及は困難となろう。また、原因を技術的に立証できるとしても、コスト等の面で対応が難しいことも考えられる。

ロ. 免責条項等の有無

AI 開発者・AI 提供者は、AI が不正確な情報を生成した場合に備え、あらかじめ責任を免除する条項（以下、「免責条項」という。）や、責任を制限する条項（以下、「責任制限条項」という。）を契約に設けておくことがある。

具体的には、類型①の場合では、AI 開発者・AI 提供者が定める約款において、

31 善管注意義務とは、債務者の職業・地位・知識等において一般的に要求される平均人の注意義務であり、各具体的場合の取引の通念に従い、相当と認められる人がなすべき注意を行う義務をいう。幾代・広中［1989］225 頁〔中川高男〕。

32 RAG を実装した AI モデルまたはシステムにおけるハルシネーションの定義について、確立されたものはないが、出力内容が提供されたデータに基づいているか否か、およびそれが事実に基づく正しい情報かどうかという点で判断する方法がある。Magesh *et al.* [2025] pp. 220–222.

33 例えば、カスタマイズ事業者が実装した RAG を原因とする不正確性が生じた場合には、AI 利用者が RAG のデータや AI モデルを入手し、これらをもとに不正確性の原因を検証することが考えられる。もっとも、実装されているデータ自体はカスタマイズ事業者が作成していること、通常それらの収集は容易ではないうえ、検証には技術的な困難が伴うことが想定される。

AIの回答の不正確性に対するAI開発者・AI提供者の免責条項や責任制限条項が定められている例がみられる[34]。また、類型①のAI開発者・AI提供者は、国外事業者であることが多く、その約款において外国法が準拠法選択されているところ、当該免責条項等の無効を争うとしても、その法的不確実性は高い。

類型②の場合にも、類型①と同様、カスタマイズ事業者の免責が定められている例がある。わが国では、企業間取引の免責条項の有効性が争われた裁判例は少ないものの、まず、事業者の全面的な免責を認める契約条項は、当該事業者に故意または重過失があったとしても、その免責を認める結果となり、当事者の衡平を著しく害するため、その有効性に疑義が生じうると考えられる[35]。さらに、事業者に故意または重過失[36]のない場合すなわち軽過失の場合に生じた損害の全部を免責する条項は、取引態様によっては無効とされたり（民法90条）[37]、民法上の定型約款の不当条項に該当すれば、みなし合意の適用除外となる（同法548条の2第2項）可能性がある[38]。

ハ. 運用保守・アップデートの有無

AIモデルまたはシステムを利用していた際に生じた不正確な情報が、AIモデルの学習やカスタマイズに用いたデータの陳腐化によるものであった場合には、性能保証の合意がなされていたとしても、合意当時のデータに基づいた出力である以上、性能保証条項に基づいた対応を求めることはできないと解される蓋然性が高い。その結果、AI開発者・AI提供者に対する契約責任の追及可能性は、もっぱら善管注意義務を基準とすることになると考えられる。

本節（2）イ.（ロ）のとおり、善管注意義務に基づく責任追及には限界があることを踏まえればAI開発者・AI提供者が提供するサービス内容の質の維持または運用保守という観点からは、AI開発者・AI提供者がデータやモデルのアップデート

34 例えば、現状の技術水準および汎用的AIモデルを前提としてではあるが、AIによる出力には、その性能等に起因する誤りが含まれる可能性があり、ベンダは、当該AIによる出力結果の誤りに関連または起因して生じたユーザの損害について一切の責任を負わない旨の免責条項がおかれる例がみられる。

35 郵便業務従事者の書留郵便物についての損害賠償責任を免除または制限した郵便法（昭和22年法律第165号）の規定について、最大判平成14年9月11日民集56巻7号1439頁、ホテルの宿泊客の損害賠償義務の範囲制限を定める宿泊約款について、最二小判平成15年2月28日裁判集民209号143頁。

36 判例では、重過失とは、ほとんど故意に近い著しい注意欠如の状態（結果の予見が可能でありかつ容易であること、結果の回避が可能でありかつ容易であること）であるとされている。例えば、東京地判平成21年12月4日判タ1322号149頁（ジェイコム株式誤発注事件）。

37 例えば、レンタルサーバの障害によって顧客のデータ等が消失したことが問題となった裁判例についてであるが、顧客について十分な保証が受けられるだろうと期待する程度に高額な利用料が設定されている場合や、障害が生じうることが想定しにくい場合等が無効となりうる例として挙げられている。嶋寺・細川・小林［2020］136頁。

38 嶋寺・細川・小林［2020］136頁。

等の早急な対応を図ることが望ましい。開発契約の内容によっては、AI モデルまたはシステムの保守等を行う義務が認められる場合もあると考えられる。

この点、類型①から③のいずれについても、AI モデルまたはシステムの運用に関する継続的な契約関係が存在する場合がある[39]。AI モデルまたはシステムの運用に関する継続的な契約関係が存在し、かつ、開発契約締結の時点で AI モデルまたはシステムに生じうるリスク分析が技術その他の制約により十分に実施できない場合には、開発契約単体でリスク調整を行うのではなく、その後に締結される契約で段階的に調整することで、より実態に即したリスク分配が可能になりうる旨の指摘がなされている[40]。

こうしたリスク分配を図る観点では、例えば、運用に関する契約において、AI 開発者・AI 提供者には、モデルやデータのアップデートを行う努力義務、モデルの不具合（不正確な情報の生成）を発見したときには直ちにその内容を通知し、遅滞なく不具合に対応する義務を定め、AI 利用者である金融機関には不具合やアップデートに関連する情報を発見したときに AI 開発者・AI 提供者に通知する義務を定めておくことが有用であると考えられる。

あるいは、AI モデルまたはシステムの開発契約に、ベンダ（AI 開発者・AI 提供者）とユーザたる金融機関（AI 利用者）の双方にプロジェクト・マネジメント義務および協力義務をあらかじめ規定しておくことも考えられる。すなわち、システム開発契約では、ユーザ側のニーズに合わせたシステム開発が完成するか不確実な性質があることから、ベンダにプロジェクト・マネジメント義務を、ユーザに協力義務を措定することが裁判例で認められている[41]。AI の開発においても、AI 開発者・AI 提供者について、AI モデルまたはシステム開発に続き、そのモデルまたはシステムの適正な稼動を管理する義務が認められると解される余地があり[42]、契約上も明らかにしておくことが考えられる。AI 利用者についても、協力義務の一環として、AI モデルまたはシステムを適正に利用する義務や、AI モデルまたはシステムの不具合を発見したときには、直ちにその内容を通知する義務、不具合の解決に向けて協力を行う義務を定めることが考えられる。

39 AI モデルまたはシステム開発においては、システム・ソフトウェア開発でも採用されることのある多段階開発方式（開発工程をいくつかに区分し、複数の個別契約を締結する方式）が想定されており、そうした工程のなかには、追加学習を含む運用・保守段階も想定されている。経済産業省［2018］33、43〜44 頁、古川ほか［2021］239 頁。

40 経済産業省［2025］32 頁。

41 東京地判平成 16 年 3 月 10 日判タ 1211 号 129 頁、東京高判平成 25 年 9 月 26 日金判 1428 号 16 頁（スルガ銀行事件控訴審判決）。プロジェクト・マネジメント義務は、準委任契約においては、ベンダが負う善管注意義務の一内容と位置付けられている。西本［2020］158 頁。

42 松尾・西村［2022］462 頁は、プロジェクト・マネジメント義務に基づき、ベンダとしては、ユーザが提供したデータを漫然と学習用システムに投入するだけではなく、開発のスケジュールや内容等について役割分担に沿って必要な働きかけを行うべきであり、それを怠っていると義務違反が認められる可能性があると指摘している。

AIモデルまたはシステムの開発においても、このようなプロジェクト・マネジメント義務および協力義務を認めることで、不正確性が問題となる事象が見つかった場合には、互いに協力をして対応を図ることが、AIモデルまたはシステムの適正な運用のために不可欠な要素になると考えられる。また、このような義務をあらかじめ明確にしておくことで、カスタマイズのために用いたデータやアップデートに用いたデータにかかる情報提供を、プロジェクト・マネジメント義務の一環としてベンダが行うことにつながり、AI利用者による善管注意義務違反にかかる立証が容易になるほか、そもそも善管注意義務違反を抑止する効果があると考えられる。

(3) 望ましい契約上の定め

本節（2）でみた法的不確実性の発生を回避する観点から望ましい契約上の定めとしては、まず、契約責任の成立範囲をあらかじめ明らかにしておく観点からは、性能保証、あるいは、それが難しい場合であっても具体的な評価指標をAIモデルまたはシステムの開発契約で定めておくことが考えられる。これには、AI開発者・AI提供者においても、自らのリスクを明らかにできる利点がある。

次に、運用の段階については、運用に関する契約や開発契約に基づくプロジェクト・マネジメント義務または協力義務の内容として、不具合発生時の連絡および対応義務、アップデートの範囲および期間、未知のデータに対する不具合についても継続運用のなかで対応を図るといった双方の協力義務（契約による柔軟な解決）を規定することが考えられる[43]。

以上の指摘事項は、事前に契約交渉の可能性がある場合（類型②-2または類型③）を前提としたものであるが、実際には利用約款が準備されている等の事前の交渉可能性がない場合（類型①または類型②-1）も多い。その場合には、以下の事項に留意すべきと考えられる。

まず、AI利用者である金融機関による契約責任の追及可能性が小さくなる点である。解釈上、本来あるべき状態としての仕様および性能が確定できれば、それに至らない履行内容については債務不履行責任を問いうるが、その確定には開発実務の定着が必要となり、一定程度の年月の経過が必要と考えられる。また、善管注意義務違反の立証が可能な限り、債務不履行責任を追及できる可能性はあるとしても、およそ立証が不可能なケースや免責条項が有効なケースも考えられる。

こうした状況下での利用については、必然的に自己責任のもとで行わなければな

43 以上のような契約上の定めは、AIシステム自体が備えるべき性能や構造に関する要件（プロダクト要件）やAIシステムを開発・運用する事業者が遵守すべき要件（マネジメント要件）を当事者間で自主的に定める試みであるとも解しうる。プロダクト要件とマネジメント要件の組み合わせによるAI規制のアプローチ等を紹介するものとして、羽深［2024］91～92頁。

らない場面が多くなる。したがって、ハルシネーションの発生を検知し、対応できる利用体制の整備が重要となる。また、開発後のアップデートについても、AI 開発者・AI 提供者による事後的なフォローアップが想定されない場合には、自ら主体的に管理を行っていく必要がある。したがって、アップデートの必要性の確認、不具合の発生状況に関するモニタリング等を通じて、問題発生を検知しうる利用体制の整備が重要となる。これらは金融機関内部における体制整備の問題であり、ガバナンスがより重要な課題となる（5 節参照）。

仮にこうした契約上の問題に起因して、社会に便益をもたらしうる AI の利用、普及が制約される事態が生じるようであれば、AI 開発者・AI 提供者に対する情報提供義務や立証責任のあり方に関する立法的な手当てを検討する余地がある。

4. AI 顧客に対する金融機関の責任

以下では、金融機関が、AI を利用したサービスを AI 顧客に提供している局面における金融機関の責任、すなわち、AI の不正確性等に起因した損害が AI 顧客に発生した場合、金融機関はどのような責任を負う可能性があるかについて分析を行う。

現在、検討または導入されている金融機関の AI のユースケースは、AI の生成した情報をもとに金融機関（の従業員）が意思決定を行う例が大半であるとされる[44]（以下、「支援型」という。）。こうした AI の利用は、金融機関が AI の生成した情報をもとに何らかの行為（作為または不作為）をなすことを意味しており、その結果、AI 顧客に何らかの損害が発生した場合には、その損害発生の原因となった行為の主体である金融機関の責任の問題となる。このほか、金融機関（の従業員）による意思決定を介さずに、AI が自律的に判断・決定を行い、AI 顧客にサービスを提供する形態も想定しうる（以下、「自律型」という。）[45]。こうした AI の利用形態[46]のもとで AI 顧客に何らかの損害が発生した場合にも、サービスの提供主体である金融機関の責任の問題となると考えられる。現時点で自律型のユースケースは極めて限定的とみられるが、支援型とあわせて検討することで、両者のリスクの相違について考察する。

44 例えば、金融庁［2025］17 頁。

45 金融庁［2025］17 頁では、こうしたユースケースの存在が示されている。

46 このほか、AI 利用のユースケースに関しては、自律型のサービスを提供すると同時に、人によるサービスという代替手段も提供するケース等がある。例えば、基本的には自律型サービスを提供するが、人による応対を希望する顧客には支援型を提供しているケースがこれに該当する。この場合には、完全な自律型には該当せず、支援型と同一の帰結となる。

(1) 支援型のAI利用における金融機関の責任

銀行業務における支援型のAI利用は、外部照会業務や融資審査業務において既に存在している。こうしたAI利用は、従来、人間が対応していた事務処理を効率化するためのものであり、コンピュータ・システムが用いられる場合と機能的には同等といえる。したがって、AIが利用されているからといって、サービス提供主体が金融機関であることに変わりはなく、また、金融機関の顧客に対する債務の内容に影響を与えるものではないと考えられる。

代表的な例として、まず、預金者に対する外部照会業務については、金融機関は預金契約[47]を前提として預金者からの照会に正確に回答する債務を負っているところ、AIの判断を参照しながら預金者からの照会対応を行うとしても（例えば、キャッシュカードの紛失に伴う利用の一時停止や再発行手続にかかる照会への対応）、正確に回答するという債務の内容に変化は生じない。そして、外部照会に対する回答を行うに当たってAIの判断を参照しても、上記債務の履行の有無（正確な手続を案内したか否か等）は客観的に判定可能である。ここでは金融機関が適切に債務を履行したかどうかだけが問題になるのであって、AIがなぜそうした判断を行ったのかということは問題とならない。よって、外部照会業務において支援的にAIが利用され、例えば、不正確な回答によりキャッシュカードの利用停止が遅延し、不正利用が発生した場合の金融機関の債務不履行は明らかであるといえる。

次に、融資審査業務については、そもそも諾成的金銭消費貸借契約（民法587条の2）は、書面または電磁的記録によって、貸主が借主に金銭を引き渡すことを約し、借主が同額の金銭の返還を約することをもって成立することから、融資審査の時点では、書面等によって金融機関は、何ら金銭の引渡しを約していないため、諾成的金銭消費貸借契約は成立しておらず、融資申請者に対して貸す債務は負っていない[48]。それゆえ、AIにより稟議書案を作成したり、金融機関が審査の過程でAIの判断を参照したりしたとしても、そのことのみによって、金融機関の融資申請者に対する債務不履行責任が生じるわけではない。

さらに、支援的にAIを用いるということは、最終的な意思決定を従来どおり人が行うことを意味する。融資審査業務における支援型のAI利用においても、AIの判断は、融資審査における参照情報のひとつにすぎず、人による最終的な意思決定に基づく従来の業務と本質的な違いはないと解される。同様のことは、融資謝絶が

47 預金契約については、神田・森田・神作［2016］85～87頁。

48 この点、契約準備段階における信義則上の注意義務違反を理由として、貸主たる金融機関に融資義務が肯定されることがある。谷口・五十嵐［2006］108～143頁〔潮見佳男〕。ただし、支援型のAIの利用があるという事実のみから、取引を開始し契約準備段階に入った者として信義則の支配する緊密な関係に立つ（最三判昭和59年9月18日裁判集民142号311頁）と評価されるわけではないと考えられる。

なされる場合についても妥当する。融資謝絶については、監督指針に基づき、これまでの取引関係や、顧客の知識、経験、財産の状況および取引を行う目的に応じ、可能な範囲で、融資謝絶の理由等を説明する態勢の整備が求められている[49]。その際にも、AI の判断はあくまでも融資謝絶という最終的な意思決定を導くうえでの参照情報であって、融資謝絶の理由等が適切に提示されている以上、融資謝絶の対応に影響はないと考えられる。

以上によれば、融資審査業務において支援的に AI が利用された場合において、例えば、融資申請者が適切な時期に資金を用意できず、ビジネス機会を失い融資があれば得られるはずであった収益を得られなかったとしても、金融機関に貸す債務はないため契約責任は成立せず、また融資謝絶に妥当な理由がある限り不法行為責任も成立しないことになる[50]。

なお、以上のような支援的な AI 利用は、各局面における銀行業務について従来から認められる金融機関の債務を必然的に変更させるものではなく、AI を利用したサービス提供を行うための個別の契約締結は必ずしも必要ではないと考えられる[51]。

(2) 自律型の AI 利用における金融機関の責任

自律型としての AI 利用も、業務の効率化のためにコンピュータ・システムが用いられることは支援型と同様であるが、AI の判断が人間の判断を介すことなく金融機関の行為となる点で違いがある。もっとも、自律型であるからといってサービスを提供する主体が金融機関であることには変わりはないほか[52]、既存の業務に関

49 金融庁「中小・地域金融機関向けの総合的な監督指針」「II-3 業務の適切性」（https://www.fsa.go.jp/common/law/guide/chusho/02b.html）参照。

50 なお、金融機関について融資審査を公正に行うという信義則上の義務が認められ、仮に AI の生成する情報に不公正なバイアスが含まれていた場合には、そうした AI を利用した融資審査は当該義務に違反する可能性がある。もっとも、従前と同様、人の意思決定をもとに融資審査がなされる限りは、当該義務の遵守は疑いがないといえる（これに対し、自律型については後掲注 54 参照）。

51 むしろ、以上のような局面で AI の利用を理由とした責任制限条項が契約に定められている場合には、その有効性が問題になりうると解される。ただし、一般論として、責任制限条項とあわせて、対価を低く設定したサービスが提供されることが契約内容となる場合には、当該条項の有効性が認められる余地がある（東京地判平成 21 年 5 月 20 日判タ 1308 号 260 頁）。このほか、従来のサービスよりもリスクが高いもののそれを利用することのベネフィットが顧客にあり、それについて十分な説明を受け、責任制限条項とあわせて合意している場合も同様と考えられる。以上は自律型についても同様にあてはまる。

52 これに対し、AI を「意図を持たないエージェント」として扱う提案（Ayres and Balkin [2024]）では、AI を利用して事業をする主体をプリンシパル（本人）、AI をエージェント（代理人）とみなしてエージェントの行為についてプリンシパルに責任を負わせるエージェンシー法理の適用が認められる旨指摘されており、その前提として AI に過失を認めることとしている（同論文を紹介したものとして

して金融機関が顧客に対し負っている本質的な債務の内容に影響を与えないのは支援型と同じであると考えられる。

例えば、外部照会業務を AI が自律的に行うケースを想定してみる。AI が預金者からの照会に対して自律的に回答し、さらに送金やキャッシュカードの再発行手続等を行うというケースである。そうした AI の利用形態であっても、預金者からの照会に正確に回答するという金融機関の債務の内容は変わらない。また、AI が回答または手続の実行を自動執行しても、その債務の履行の有無（照会に対する回答または手続の自動執行が正確になされているか等）も明らかであり、AI がなぜそうした判断を行ったのかは債務不履行の事実を判定するうえで問題とならない。

また、融資審査・実行までを AI が自律的に行うケースを想定してみても、本節（1）と同様、金融機関は融資申請者に対して貸す債務を負ってはいないなか、AI によって融資謝絶が行われたとしても、監督指針上で求められる程度の判断の妥当性の説明[53]が求められるにとどまる[54]。

もっとも、自律的な AI 利用のうち、金融機関の債務の内容に判断および裁量の要素が含まれており、AI の判断がそれを代替する利用形態では、AI の判断の妥当性が論点となる。例えば、債権管理を AI が自律的に行うケースを想定してみる。金融機関がコミットメントライン契約[55]に基づく貸す債務を負っているとする[56]。このとき、AI の判断により、貸付が実行されず、その結果、AI 顧客に投資機会の逸失や資金繰り悪化による倒産といった損害が発生する事態が生じたとする。前提となっている金融機関の貸す債務には、貸付の実行や中止に関する判断および裁量が含まれているところ[57]、AI の不作為が契約に沿った対応であるのかの評価は客観的に明らかではなく、AI の判断の妥当性が問題となる場合もある。より具体的には、AI の判断によって損害を被ったとする AI 顧客が、金融機関の債務不履行（AI の判断が妥当ではなかったことや利用している AI のリスク管理が不十分であったために不正確な判断がなされたこと等）の存在を主張・立証する責任を負うのに対

田中［2025b］）。本研究会は AI を法的主体としては扱わず、もっぱら AI を利用している主体の過失の問題として扱っている。同様の立場として、福岡［2020］148 頁。

53 説明すべき内容については、前掲注 49 に対応する本文参照。

54 仮に、AI の生成した判断の根底に不公正なバイアスが含まれていた場合には、融資審査を公正に行うという信義則上の義務に違反しうる余地がある。

55 コミットメントライン契約とは、一般に、あらかじめ約定した期間、極度額、融資条件等の範囲内であれば、取引先がいつでも融資を受けることができる枠（クレジットライン）を設定し、金融機関は融資の申出に応じて融資を行うことを約し、取引先はこれに対し手数料を支払うことを約する契約をいう。神田・森田・神作［2016］151 頁。

56 コミットメントライン契約は、融資契約そのものではなく、融資枠を設定する契約であり、個々の融資自体は別途の意思表示により個別に金銭消費貸借契約が成立するとされている。借主のみが有する予約完結権行使により金銭消費貸借契約が成立することになる。神田・森田・神作［2016］151 頁。

57 例えば、日本ローン債権市場協会の推奨のコミットメントライン契約書（https://www.jsla.org/wp-content/uploads/legacy/2005/3120190626125732.doc?d=1）では、6 条において貸付前提条件が定められており、貸付人にはさまざまな指標の充足性について一定の判断が求められている。

して、金融機関の側において、当該債務不履行が自らの責めに帰すべき事由によるものではないこと（十分なリスク管理体制を構築・運用していたこと）を主張・立証する責任を負うことになるものと考えられる。

こうした紛争の発生を予防するためには、金融機関の判断または裁量を AI に代替させることによって、従来と異なるリスクが生じるのであれば[58]、AI を用いるベネフィットのある金融機関が、AI 顧客に対して、そのリスクを十分に説明し、AI による判断に服することの合意（AI サービス利用契約）を求める必要があると考えられる。AI 顧客においても、AI を利用したサービスの提供を受けることに伴うリスクを認識し、それを上回るベネフィットがあると判断する場合には、そうした契約に合意する合理性があると考えられる[59]。現状、契約における金融機関の判断の妥当性が金融機関に対する顧客の信頼によって成り立っているとすれば、AI が人間の判断に代替することはただちに受容されがたい可能性がある。上述した顧客に対する説明は、金融機関に対する信頼を要素とする債務を、AI の判断に依存する債務へと変化させるうえでも重要な役割を担うと考えられる。

自律型の AI によるサービスを受けることにリスクが伴い、その十分な理解が必要な場合等に、代替手段の提供なく自律型の利用のみを促すことは、AI 顧客の利益を害する可能性があると考えられる。このような AI サービスを提供するに当たっては、金融機関は、代替手段を用意することや、AI の利用に際していわゆる適合性の原則に相当する配慮を行うこと等が考えられる。顧客が AI の利用に伴うベネフィットのほかにデメリットおよびリスクを甘受する可能性があるならば、事前にその説明が必要と考えられ、適合性の原則のように、その顧客の知識および経験に応じた取引または勧誘が望ましいといえる。

なお、AI によるサービスの提供に伴って発生しうるリスクは、顧客のみならず、金融機関にも影響を与えるものである。このため、金融機関と AI 顧客の間で適切なリスク分配を図る観点から、AI サービス利用契約によって金融機関には合理的な範囲で免責が認められる必要があると考えられる。現状、金融機関はその社会的な役割から、法令、各種指針に基づいて高い水準の義務が課される場面も多い。付加価値を有する効率的な AI サービスが実装されていくためには、金融機関に認め

58 債務を履行するに当たって金融機関の判断および裁量が認められている場合、それを人間が行うことと AI が代替することのリスクの違いは必ずしも明らかではない。この点、AI の提供するサービスが、人間の提供するサービスと同程度のリスクしかもたらさないにもかかわらず、人間が提供する場合よりも厳格な規制が課されるならば、AI による技術革新を阻害することになると指摘されている。田中［2025b］93 頁。また、AI 固有の問題ではなく既存の規制に内在していた問題が AI の利用によって浮き彫りになったことを指摘する見解もある。羽深［2024］86〜87 頁。

59 例えば、金融機関が、あらかじめ定めた分散ルール等の運用基準の範囲内で AI が一任運用をするというファンドラップ・サービスを提供する場合については、顧客において、運用基準が守られている限り金融機関に責任追及ができないというリスクはあるとしても、手数料が低く設定されるというベネフィットがあれば、そうしたサービス提供を望むとも考えられる。

られる免責範囲は重要な論点になると考えられる。

(3) 不法行為責任の追及における法的問題

金融機関と AI 顧客の間で AI の不正確性等に起因して損害が発生した場合には、それが債務の本旨に従った履行に該当しない事実は明らかであるため、基本的には契約に基づく責任追及がなされると考えられる。もっとも、不法行為が問題となる場面もありうる。例えば、自律型の AI を用いた融資審査において、AI の判断に不公正なバイアスが反映されていた場合には、融資審査を公正に行うという信義則上の義務に違反しうる[60]。この場合、金融機関と AI 顧客の間には融資契約関係はないとしても、信義則上の義務違反に基づく不法行為責任を追及することが考えられる。

問題は、AI 顧客において、AI が生成した判断の根底に不公正なバイアスが含まれていたことを立証できるかという点である[61]。こうした事例では、AI がなぜそのように判断したのかという理由の説明は難しく（AI のブラックボックス問題）、判断に至った過程を事後的に検証することも難しい（AI のトレーサビリティの問題）という特質が影響することになる。また、こうした特質に伴い、金融機関の過失（予見可能性）の存在も AI 顧客が立証するのは困難と解される。

さらに、AI 顧客は、金融機関が利用していた AI を開発した AI 開発者に対して不法行為責任を追及することも考えられるが、上記の立証の問題は同様に該当する[62]。

なお、不法行為責任の立証負担（過失の立証）を緩和する特別法としては製造物責任法（平成 6 年法律第 85 号）がある。AI 開発者に対する製造物責任の追及については、(i) 現行の製造物責任法における「製造物」には、純然たるソフトウェアとしての AI モデルは含まれないと解されること[63]、(ii) ブラックボックス化、複雑化している AI の欠陥の存在を、被害者が立証することは困難であること等から、同法に基づいて AI 開発者の製造物責任を追及することは事実上不可能と考えられ

60 前掲注 50、54 およびそれらに対応する本文参照。

61 不法行為責任の成立には、①加害者に故意または過失があること、②損害が発生していること、③他人の権利を侵害していること（違法性があること）、④加害行為と損害との間に因果関係があることが必要であり（民法 709 条）、いずれについても、不法行為責任を追及する被害者である AI 顧客が立証責任を負う。

62 福岡［2020］158 頁、同［2023］32 頁。被害者が、AI の利用状況を知らない開発者に予見可能性があったことを立証するのは容易ではないこと、AI が開発者の想定外のふるまいをした場合には予見可能性があったことを立証することは容易ではないことが指摘されている。

63 例えば、経済産業省［2018］34～35 頁。製造物責任法における「製造物」とは、「製造又は加工された動産」と定義されており（同法 2 条 1 項）、動産は民法上有体物に限定されている（民法 86 条 2 項、85 条）。プログラムのみの AI は製造物に該当しないと解するものとして、福岡［2020］156～157 頁。

る。以上のような帰結に問題があるとするならば、立法による対応が検討されるべきと考えられる[64]。

5. 組織内部におけるリスク管理

金融機関を含む事業者は、組織における AI の利用を決定すると同時に AI 利用に伴うリスク管理を行う必要がある。取締役には、内部統制システム構築義務の一内容として AI ガバナンス体制構築義務が認められ、AI の利用における組織内の最終的な責任を負うと解される。今後はどのようなリスクに対して、どのような管理を行うべきかをより具体的に検討していく必要がある。

以下では、金融機関に求められる AI ガバナンス体制構築義務の内容を考察したうえで、同義務が遵守されるために必要なリスク管理のあり方を検討する。

(1) AI ガバナンス体制構築義務

金融機関に求められる AI ガバナンス体制構築義務の内容については、確立した見解があるわけではない。そこで、同義務の前提となっている内部統制システムと、金融庁が公表している「モデル・リスク管理に関する原則」（以下、「MRM 原則」という。）[65] を手掛かりにその内容を検討する。

イ. 内部統制システムとしての AI ガバナンス

AI ガバナンス体制は内部統制システムの一部であることから、前者に求められる水準を後者と同様に考えるならば、①不適切な行為が行われた時点において、②通常想定されるリスクにつき、③同業他社並の水準で構築する必要がある[66]。もっとも、AI については技術の進展が速く、①や②については、AI ガバナンス体制を構築した後も不断の見直しを行うことが、③については、とくにグローバルに展開する金融機関においては国内に限らず海外同業他社並の水準を意識することが求め

64 欧州では、AI Act の制定と並行して、AI の利用に伴う損害賠償制度の見直しも進められており、2024 年 10 月には製造物責任指令の改正法（Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC）が成立した。同指令では、AI 技術への対応として、損害概念、製造物等の定義、欠陥概念の見直し等が行われている。製造物責任指令の改正案を紹介した文献として、角田・戸田［2022］、福岡［2023］、小塚［2024］、De Luca [2025] がある。

65 https://www.fsa.go.jp/news/r3/ginkou/20211112/pdf_02.pdf

66 中村［2017］126 頁。

られると考えられる。

なお、AI ガバナンス体制の構築・運用に当たっては、内部統制システムの場合と同様、取締役に一定の裁量が認められると解されるが、経営判断原則[67] が適用されるかについては明らかではない。とくに、金融機関については、判例上[68]、その高い公益性から同原則の適用余地は限定的なものとされており、AI ガバナンス体制の内容についても同原則が適用されない可能性がある点には留意が必要である。

ロ. MRM 原則

金融機関の AI ガバナンス体制の内容を検討するに当たっては、金融庁が 2021 年に公表した MRM 原則を参考とすることができる。同原則は、金融システム上重要な金融機関を対象として、モデルの利用に当たって考慮すべき原則を定めたものであり、対象とされるモデルの定義には、AI モデルが含まれるとされている[69]。

まず、MRM 原則では、モデル・リスクとは、モデルの誤りまたは不適切な使用に基づく意思決定によって悪影響が生じるリスクをいい、より具体的には、①意図した用途（モデルの目的）に照らしてモデルに根本的な誤りがあり、不正確なアウトプットを出力する場合、②モデルが不適切に使用されている場合（想定した範囲外での使用や、モデルの限界を超える使用を含む。）に発現しうるものとされている。同原則におけるモデル・リスクには、AI の不正確性（ハルシネーション等）が含まれると考えられる。

そして、モデル・リスク管理に当たっては、①他のリスク管理と同様、「3 つの防衛線」[70] に基づく組織構成のあり方や、役割・責任の割当て等による実効的なけん

67 取締役が会社の事業活動に関する決定（いわゆる経営判断）を行う際には裁量が認められ、その判断の過程、内容に著しく不合理な点がない限り、取締役としての善管注意義務に違反するものではないと解されている（経営判断原則）。最一判平成 22 年 7 月 15 日裁判集民 234 号 225 頁（アパマンショップホールディングス事件）。

68 最三小決平成 21 年 11 月 9 日刑集 63 巻 9 号 1117 頁（旧北海道拓殖銀行事件）。

69 同原則でいうモデルとは、定量的な手法（複数の定量的な手法によって構成される手法を含む。）であって、理論や仮定に基づきインプット・データを処理し、アウトプット（推定値、予測値、スコア、分類等）を出力するものをいうとされる。MRM 原則 5 頁。この定義に AI モデルが含まれることについては、金融庁［2024］5 頁。

また、モデルは、金融商品のプライシングや価値評価、リスク計測（信用リスク、市場リスク、オペレーショナル・リスク等）において広く使用されてきたが、近年、その利用範囲が拡大しているほか（マネー・ローンダリング等対策、不正検知、アルゴリズム取引等の領域）、コンピュータの計算能力の向上や、機械学習・AI の手法の深化といった技術革新の成果を活用したモデルも多くなっていると指摘されている。MRM 原則 2〜3 頁。

70 MRM 原則 6 頁。MRM 原則では、3 つの防衛線とは、以下のように説明されている。すなわち、第 1 の防衛線（第 1 線）は、モデルを所管するまたはモデルの開発・使用に直接関係する部門・個人で構成され（モデル・オーナー、モデル開発者、モデル使用者等）、第 2 の防衛線（第 2 線）は、第 1 線に対するけん制を通じてモデル・リスクを管理する部門・個人で構成され、モデル・リスク管理態勢の維持、規程等の遵守状況およびモデル・リスク全体に対する独立した立場からの監視等の役割を担う。第 3 の防衛線（第 3 線）は、内部監査部門で構成され、金融機関のモデル・リスク管理態勢の全

制の確保[71]、②モデル・ライフサイクル[72] に応じた実効的なけん制の確保、③リスク・ベース・アプローチ[73] によるリスク管理の実効性確保が重要であるとされている。3 つの防衛線のほかに、取締役会等や上級管理職、モデル・リスクの関連会議体が果たす役割も重要とされている。金融機関のモデル・リスク管理体制の構築およびモデル・リスク管理に関する最終責任は、基本的には取締役等にあるが、取締役等が管理態勢の構築を行うことは現実的ではなく、その権限と実行は、チーフ・リスク・オフィサー（CRO）といった上級管理職やモデル・リスクの関連会議体に委譲されることが一般的である[74]。

このような MRM 原則のもとでは、リスク・ベース・アプローチによるリスク管理、すなわち AI の利用方法や態様に応じたリスク評価を行い、そのリスクに応じた実効的なけん制の確保の必要性と、AI 特有のリスクの考慮の必要性が導かれる[75]。

より具体的には、予期せぬリスクの事後的な顕在化や運用中の精度の変動に備えられるように、継続的、定期的なモニタリング等による実効的なけん制の仕組みを構築することが考えられる。その際には、リスクの大きさに応じて AI を利用したシステムの精度を定期的にモニタリングする体制や、定期的なサンプリング調査を行う体制を設けること等が考えられる。複数の部門で異なる AI を利用する場合には、全体的な統制を 3 線モデルで管理する必要性が高いといえる。

そのうえで、AI 特有のリスク、すなわち、ハルシネーションやバイアスの存在を前提としたリスク管理については別途考慮が必要である。そうしたリスクを前提に、人の意思決定を介在させる体制を構築することは、AI ガバナンス体制構築義務遵守の一態様といえる。他方で、ハルシネーションが存在するからといって、すべての利用に際し、ただちに人の意思決定を介在させること、すなわち、支援型しか利用すべきではないという帰結までにはならないと考えられる[76]。ここでも、リ

体的な有効性を評価するとされる。

71 MRM 原則に基づき 3 線モデルを構築している先は、その管理対象に生成 AI を含めることが推奨されている。金融データ活用推進協会［2024］115 頁。

72 モデルの特定、リスク格付けの付与、開発、使用、変更、使用停止等のモデルが経る一連の流れと定義される。MRM 原則 6 頁。

73 モデル・リスク管理におけるリスク・ベース・アプローチとは、金融機関がモデルに内在するリスクを評価し、評価結果に基づいてリスクを管理することと定義されている。MRM 原則 7 頁。

74 取締役等は、第 2 線のモデル・リスク管理部門からモデル・リスク管理の状況について報告を受け、必要に応じて改善事項等を指示し、その実行を監督することが主な役割になる。田中・曽我部［2024］21 頁。

75 金融機関が利用する 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り、その際には「リスク・ベース・アプローチ」の考えを踏まえ、モデルに内在するリスクの評価、その大きさに応じた管理を行うことが適当であるが、その評価においては AI 特有のリスクを十分に考慮することが重要であると指摘されている。金融庁［2024］22 頁。

76 顧客対応型の生成 AI の利用に金融機関が慎重となっている理由としては、リスク・エクスポージャーの増加（誤ったアドバイスや商品の提供の可能性等）、関連する規制要件を満たすために必要

スク・ベース・アプローチに基づき、常に人の意思決定を介在させるのではなく、モニタリングおよびAIの精度評価を行う体制とすることも、AIガバナンス体制構築義務の内容と認められると解される。

この点、人間の尊厳や個人の尊重という観点から、AIを人の意思決定に代替させるべきではないという価値判断もありうるところ、顧客にオプト・アウトの機会を提供することが有効な対応となる場合もありうる。

(2) AIガバナンスのもとでのリスク管理

以上を踏まえ、AIガバナンス体制構築義務が遵守されるために必要なリスク管理のあり方を検討する。なお、以下の検討は管理方法の一試案であり、これに限られるものではない。

まず、AIが組織内で広く利用されていく前提として、AIのリスクに関する社内教育を徹底し、それに資する社内ルールを整備する必要がある。より重要度が高まる事項としては、専門部署によるリスクの定性的・定量的な評価、リスク・レベルに応じたCxO（各領域の最高責任者）による関与体制の整備が挙げられる。

次に、支援型でのAI利用については、人の意思決定の介在を前提としていることがリスクの顕在化の抑止対策になっている。したがって、社内教育の浸透を条件として、従来のリスク管理体制枠組みのなかで相応のリスク軽減措置がとられていると評価できれば、AIガバナンス体制構築義務の遵守がなされていると解することができる。

これに対し、自律型については、事前の対応として、想定されるリスクの特定とその大きさの評価を行い、リスクの大きさに応じた頻度でのモニタリング、とくにモデルやデータのアップデートの要否の検討を実施する必要がある。事後の対応、すなわち、リスクが顕在化した場合の対応としては、顧客による異議申立権の付与、事後的な問題解明機会の提供が考えられ、そのためには検証可能なシステムの設計の確保といった整備をリスクの大きさに応じて行うことが考えられる。

より具体的にみると、AIの利用に伴うリスクの種類としては、顧客に対する金銭的損害、金融機関における損失の発生、レピュテーションの毀損等が考えられる。AIを貸出業務、債権管理業務、外部照会業務、不正送金検知業務に用いるケースでは、サービス提供先が顧客であるため、顧客に金銭的損害が生じうる。また、AIを貸出業務および債権管理業務で用いるケースや、資金運用業務で用いるケースで

な高い障壁（モデルの結果を検証する等）、企業独自の内部リスク管理ポリシー、モデルの結果が間違っている場合に最終的に責任を負う当事者の明確さの欠如、生成AIと対話することに対する消費者の信頼の欠如、サード・パーティのモデル・プロバイダーへの過度な依存に対する危惧が挙げられている。Crisanto *et al.* [2024] p. 12.

は、金融機関自らに損失が発生しうる。このほか、AI の利用が不適切な結果を発生させているとして、当該金融機関のレピュテーションが毀損するケースも考えられる。

顧客に生じる金銭的損害については、生じうる規模に応じたモニタリングと、不正確な自動執行がされた後に速やかにその是正を図りうるよう、顧客に対して異議申立ての機会を付与することや、問題を解明する機会を提供すること（検証可能なシステムに基づく調査の実施と説明の提供）、損害の補填を行う準備を行うことが、適切なリスク管理であると考えられる。

AI のもたらすリスクが、金融機関における損失やレピュテーションの毀損に留まる場合には、リスクの大きさに応じたモニタリングの頻度および内容を選択し、適当なタイミングでのモデルの見直しを行うことが適切なリスク管理であると考えられる。なお、金融機関のレピュテーションの毀損を防ぐ観点からは、AI で利用しているデータやモデル、および AI の利用にかかる透明性や公平性を確保し、自らの説明責任を果たすことが重要であり、そのためには AI による判断の説明可能性を確保する体制を確保および公表していくことが有益であると考えられる。

また、外部環境の変化が激しく、AI の判断の前提となるデータやモデルがその時点の水準からみて陳腐化しやすい業務で AI を利用するケースがある[77]。このような業務に自律型 AI を用いる場合には、外部環境の変化を適時適切に反映した AI を利用する必要性が高く、データやモデルのアップデートの要否を定期的に確認する必要がある。

6. おわりに

本報告書では、金融機関における AI の利用に伴う法的リスクを明らかにするために、3 つの局面、すなわち、AI モデルまたはシステムの開発・導入、AI を用いたサービス提供、組織内部でのリスク管理を取り上げ、分析を行った。

第 1 の開発・導入の局面については、金融機関が利用する AI モデルまたはシステムにおいて、AI の生成した不正確な情報に起因した損害が発生した場合に、AI 開発者・AI 提供者に対して契約責任を追及するうえでの法的帰結を確認した。現状、契約で性能保証がなされている場合や、AI 開発者・AI 提供者の善管注意義務違反が明らかな場合を除き、AI 開発者・AI 提供者の債務不履行責任の追及は難しいこと、そうした現状のもとでは運用・保守における協力的な関係の構築が重要な

77 そのときどきの金融経済情勢を反映する必要のある資金運用業務や貸出業務、日々進歩する不正手口に対処する必要のある不正送金検知業務がこれにあたる。参照するサービス内容が変化しうるという意味では、外部照会業務もこれに含まれよう。

意味を有することを指摘した。

第 2 のサービス提供の局面については、金融機関が AI を用いたサービスを提供している顧客に AI の不正確性に基づく損害が発生した場合の金融機関の責任の内容を確認した。AI の利用形態が従来の債務の内容に変更を及ぼさないものである限り、金融機関の責任にも変容がないことを確認した。ただし、AI の判断が、金融機関の判断または裁量に代替するものであり、それが債務の内容にかかわる利用形態である場合には、AI の利用についてあらかじめ当事者間で契約を締結しておく必要性が高いことを指摘した。

第 3 の組織内部のリスク管理の局面については、AI の利用に伴うリスク管理の必要性と取締役の AI ガバナンス体制構築義務を前提に、具体的なリスク管理のあり方を示した。具体的な AI ガバナンス水準の内容や、AI の利用に伴うリスク評価とけん制の確保のためにとくに留意すべき点として、複数の AI 利用時における社内の全体的な統制の確保、社内教育、事前や事後の対応策の整備を指摘したほか、とくに、グローバルに展開する金融機関については、AI ガバナンス水準として海外同業他社を比較対象に求めるべきことも指摘した。

以上のうち、とくに第 1 の局面については、AI の開発を阻害しないためには AI 開発者・AI 提供者における責任を過大なものとしないことが必要であるが、AI 利用者が AI により生じた損害をすべて負担することになる帰結も適当ではない。現状では、当事者が契約において何も定めていないと民法の規定から導かれる責任に関する帰結が必ずしも明確とはいえない場合が少なくないという問題が存在すると考えられる。このため、あらかじめ、契約において、責任の範囲を明確化しておくこと、とくに可能な限り性能保証の範囲を明らかにしておくことが望ましいと考えられる。

今後の課題としては、当該分野は技術の進展が非常に速いため、法的論点についての見直しも不断に行っていく必要があるほか、海外準拠法に基づく AI 開発者・AI 提供者に対する責任追及については海外の動向を注視していく必要があること等が挙げられる。

参考文献

アルゴリズム・AI の利用を巡る法律問題研究会、「投資判断におけるアルゴリズム・AI の利用と法的責任」、『金融研究』第 38 巻第 2 号、日本銀行金融研究所、2019 年、1〜44 頁

幾代　通・広中俊雄編、『新版　注釈民法（16）　債権（7)』、有斐閣、1989 年

影島広泰、「金融機関が AI を活用する際の法的留意点」、『銀行法務 21』852 号、2020 年、20〜27 頁

神田秀樹、『会社法（第 27 版)』、弘文堂、2025 年

———・森田宏樹・神作裕之編、『金融法概説』、有斐閣、2016 年

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)」、金融庁、2024 年（https://www.fsa.go.jp/news/r6/ginkou/20241212/20241212_1.pdf、2025 年 6 月 6 日）

———、「AI ディスカッションペーパー（第 1.0 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―」、金融庁、2025 年（https://www.fsa.go.jp/news/r6/sonota/20250304/aidp.pdf、2025 年 6 月 6 日）

金融データ活用推進協会、『金融生成 AI ガイドライン』、外為印刷、2024 年

経済産業省、「AI・データの利用に関する契約ガイドライン―AI 編―」、経済産業省、2018 年（https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20180615001-3.pdf、2025 年 6 月 6 日）

———、「AI の利用・開発に関する契約チェックリスト」、経済産業省、2025 年（https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20250218003-ar.pdf、2025 年 6 月 6 日）

公正取引委員会、「生成 AI を巡る競争（ディスカッションペーパー)」、公正取引委員会、2024 年（https://www.jftc.go.jp/houdou/pressrelease/2024/oct/241002_generativeai_02.pdf、2025 年 6 月 6 日）

———、「生成 AI に関する実態調査報告書 ver.1.0」、公正取引委員会、2025 年（https://www.jftc.go.jp/houdou/pressrelease/2025/jun/250606_generativeai02.pdf、2025 年 6 月 6 日）

国立研究開発法人科学技術振興機構研究開発戦略センター、「人工知能研究の新潮流 2〜基盤モデル・生成 AI のインパクト〜」、CRDS-FY2023-RR-02、国立研究開発法人科学技術振興機構、2023 年（https://www.jst.go.jp/crds/pdf/2023/RR/CRDS-FY2023-RR-02.pdf、2025 年 6 月 6 日）

———、「戦略プロポーザル　次世代 AI モデルの研究開発」、CRDS-FY2023-SP-03、国立研究開発法人科学技術振興機構、2024 年（https://www.jst.go.jp/crds/pdf/2023/SP/CRDS-FY2023-SP-03.pdf、2025 年 6 月 6 日）

———、「人工知能研究の新潮流 2025〜基盤モデル・生成 AI のインパクトと課

題～」、国立研究開発法人科学技術振興機構、CRDS-FY2024-RR-07、2025 年（https://www.jst.go.jp/crds/pdf/2024/RR/CRDS-FY2024-RR-07.pdf、2025 年 6 月 6 日）
小塚荘一郎、「AI 製品に対応した EU の製造物責任ディレクティヴ改正」、『情報法制研究』15 号、2024 年、37～49 頁
嶋寺　基・細川慈子・小林直弥、『約款の基本と実践』、商事法務、2020 年
総務省・経済産業省、「AI 事業者ガイドライン（第 1.1 版）」、総務省・経済産業省、2025 年（https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf、2025 年 6 月 6 日）
田中康浩・曽我部淳編著、『詳解　金融機関のためのモデル・リスク管理』、中央経済社、2024 年
田中　亘、『会社法　第 5 版』、東京大学出版会、2025 年 a
———、「金融サービスにおける AI 利用に対する法規制について―same rule 原則は新たな法規制を要求するか―」、『証券経済研究』129 号、2025 年 b、91～107 頁
谷口知平・五十嵐清編、『新版　注釈民法（13）　債権（4）　〔補訂版〕』、有斐閣、2006 年
角田龍哉・戸田　相、「AI 責任指令案・製造物責任指令改正案の公表及び日本企業への影響」、西村あさひ法律事務所ヨーロッパニューズレター、西村あさひ法律事務所、2022 年（https://www.nishimura.com/sites/default/files/images/newsletter_221004_europe.pdf、2025 年 6 月 6 日）
東京地方裁判所プラクティス委員会第二小委員会、「ソフトウェア開発関係訴訟の手引」、『判例タイムズ』1349 号、2011 年、4～27 頁
中崎　尚、『生成 AI 法務・ガバナンス――未来を形作る規範』、商事法務、2024 年
中村直人編著、『コンプライアンス・内部統制ハンドブック』、商事法務、2017 年
西本　強、『ユーザを成功に導く AI 開発契約』、商事法務、2020 年
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―アンケート調査結果から―」、金融システムレポート別冊シリーズ、日本銀行、2024 年（https://www.boj.or.jp/research/brp/fsr/data/fsrb241021-1.pdf、2025 年 6 月 6 日）
羽深宏樹、「『AI 規制論』のコペルニクス的転回――現代の一般的規制モデルの構築に向けて――」、『東京大学法科大学院ローレビュー』19 号、2024 年、85～106 頁
福岡真之介、『AI の法律』、商事法務、2020 年
———、「AI と民事責任・製造物責任――EU の AI 責任指令案・製造物責任指令改正案を踏まえて」、『NBL』1237 号、2023 年、28～33 頁
藤田友敬、「取締役会の監督機能と取締役の監視義務・内部統制システム構築義務」、尾崎安央・川島いづみ・若林泰伸編『上村達男先生古稀記念　公開会社法と資本市場の法理』、商事法務、2019 年、357～383 頁

古川直裕・渡邊道生穂編著・柴山吉報・木村菜生子、『Q&A　AI の法務と倫理』、中央経済社、2021 年

文化審議会著作権分科会法制度小委員会、「AI と著作権に関する考え方について」、文化庁、2024 年（https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf、2025 年 6 月 6 日）

松尾剛行・西村友海、『紛争解決のためのシステム開発法務―AI・アジャイル・パッケージ開発等のトラブル対応』、法律文化社、2022 年

森田　果、「AI の法規整をめぐる基本的な考え方」、RIETI Discussion Paper Series 17-J-011、独立行政法人経済産業研究所、2017 年（https://www.rieti.go.jp/jp/publications/dp/17j011.pdf、2025 年 6 月 6 日）

森・濱田松本法律事務所編・飯田耕一郎・田中浩之・渡邉　峻、『企業訴訟実務問題シリーズ　システム開発訴訟（第 2 版）』、中央経済社、2022 年

AI ガバナンス協会 AI ガバナンス実装ワーキンググループ、「AI ガバナンスの実装状況に関するワーキングペーパー～横断的な視点からみる、企業取組の諸相」、AI ガバナンス協会、2024 年（https://www.ai-governance.jp/blog/implement-wp-240807、2025 年 6 月 6 日）

AI 時代の知的財産権検討会、「AI 時代の知的財産権検討会中間とりまとめ」、内閣府、2024 年（https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2024/0528_ai.pdf、2025 年 6 月 6 日）

AI 戦略会議・AI 制度研究会、「中間とりまとめ」、内閣府、2025 年（https://www8.cao.go.jp/cstp/ai/interim_report.pdf、2025 年 6 月 6 日）

Ayres, Ian and Jack M. Balkin, “The Law of AI is the Law of Risky Agents Without Intentions,” *University of Chicago Law Review Online,* 11/27/24, 2024 (https://lawreview.uchicago.edu/sites/default/files/2024-11/Ayres_Balkin_Law%20of%20Risky%20Agents.pdf、2025 年 6 月 6 日).

Bank for International Settlements, “BIS Annual Economic Report June 2024,” Bank for International Settlements, 2024 (https://www.bis.org/publ/arpdf/ar2024e.pdf、2025 年 6 月 6 日).

Crisanto, Juan Carlos, Cris Benson Leuterio, Jermy Prenio, and Jeffery Young, “Regulating AI in the Financial Sector: Recent Developments and Main Challenges,” FSI Insights on Policy Implementation, No.63, Financial Stability Institute, 2024 (https://www.bis.org/fsi/publ/insights63.pdf、2025 年 6 月 6 日).

De Luca, Stefano, “Revised Product Liability Directive,” European Parliament, 2025 (https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf、2025 年 6 月 6 日).

Magesh, Varun, Faiz Surani, Matthew Dahl, Mirac Suzgun, Christopher D. Manning,

Daniel E. Ho, “Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools,” Journal of Empirical Legal Studies, Vol.22(2), 2025, pp. 216–242 (https://dho.stanford.edu/wp-content/uploads/Legal_RAG_Hallucinations.pdf、2025 年 6 月 6 日).

金融研究所の概要

金融研究所（Institute for Monetary and Economic Studies, IMES）は 1982 年 10 月に日本銀行創立百周年を記念して、日本銀行の内部組織の 1 つとして設立されました。その主な目的は、(1) 金融経済の理論、制度、歴史に関する基礎的な研究の充実を図り、日本銀行の政策の適切な運営に役立てること、(2) 学界等との交流を促進すること、(3) 外部の研究活動の便宜に資する各種情報、資料等を公に提供することです。

主な活動

研究活動

・金融経済の基本的問題に関する理論・実証的研究。
・金融関連の制度基盤（法律・会計・中央銀行制度等）に関する研究。
・金融関連の情報技術に関する研究。
・金融経済の歴史に関する研究。
・金融経済に関する歴史的資料の収集・保存・公開（アーカイブ・貨幣博物館）。

顧問および客員研究員の招へい

・国内外の有力学者若干名に研究所顧問（非常勤）を委嘱し、研究所の運営、研究活動の進め方、内外学界との交流等に関する助言を受けています。
・国内外より学者数名を客員研究員として招へいし、研究活動の強化を図っています。

会議の開催

・海外中央銀行、国際機関の研究者や内外の著名学者を交えた会議を開催。
・外部の研究者、専門家を交えた研究会、セミナー等を適宜開催。

刊行物の発行

金融研究、Monetary and Economic Studies、IMES Discussion Paper Series、日本銀行の機能と業務、国際コンファランス議事録等を公刊（刊行物の一覧は後掲）。

貨幣博物館

国内を中心とした貴重な貨幣や貨幣にかかわる資料を貨幣博物館に展示するとともに、貨幣に関する歴史資料をホームページ等で公開（博物館の案内は後掲）。

歴史的公文（歴史的文書）の公開

日本銀行に関連する歴史的資料のうち、歴史的価値を有するものについて、日本銀行金融研究所アーカイブで保管・整理し、一般に公開（アーカイブの案内は後掲）。

研究の委託

人員面、資料面の制約等から所内での研究が困難なテーマについて外部の学者等に研究を委託。

主な刊行物

金融研究

邦文機関誌、年 4 回程度発行。金融研究所の研究論文や各種ワークショップの模様、研究会報告等を公表。

Monetary and Economic Studies

英文機関誌。『金融研究』と同様、金融研究所の研究論文等を公表（『金融研究』掲載論文の英訳のほか、英文オリジナル論文を含む）。

IMES Discussion Paper Series（E-Series：英語版、J-Series：日本語版）

金融研究所スタッフおよび外部研究者による研究成果の未定稿を随時公表。学界、金融機関、関係者等から、広くコメントを求めることを目的としている。

国際コンファランス議事録

- *Growth, Integration, and Monetary Policy in East Asia*（*Monetary and Economic Studies*、Vol. 25、No. S-1、2007年）
- *Financial Markets and the Real Economy in a Low Interest Rate Environment*（*Monetary and Economic Studies*、Vol. 24、No. S-1、2006年）
- *Incentive Mechanisms for Economic Policymakers*（*Monetary and Economic Studies*、Vol. 23、No. S-1、2005年）
- *Challenges for Sustained Economic Growth under Changing Economic, Social, and International Environments*（*Monetary and Economic Studies*、Vol. 22、No. S-1、2004年）
- *Exchange Rate Regimes in the 21st Century*（*Monetary and Economic Studies*、Vol. 20、No. S-1、2002年）
- *The Role of Monetary Policy under Low Inflation: Deflationary Shocks and Policy Responses*（*Monetary and Economic Studies*、Vol. 19、No. S-1、2001年）
- *Monetary Policy in a World of Knowledge-Based Growth, Quality Change and Uncertain Measurement*（Palgrave、2001年）
- *Towards More Effective Monetary Policy*（Macmillan Press、1997年）
- *Financial Stability in a Changing Environment*（Macmillan Press、1995年）
- *Price Stabilization in the 1990s: Domestic and International Policy Requirements*（Macmillan Press、1993年）
- *The Evolution of the International Monetary System: How Can Efficiency and Stability Be Attained ?*（University of Tokyo Press、1990年）
- *Toward a World of Economic Stability: Optimal Monetary Framework and Policy*（University of Tokyo Press、1988年）
- *Financial Innovation and Monetary Policy: Asia and the West*（University of Tokyo Press、1986年）
- *Monetary Policy in Our Times*（MIT Press、1985年）

なお、2008 年以降に開催された国際コンファランスについては、議事要旨等を *Monetary and Economic Studies* に所収。

日本銀行の機能と業務（有斐閣、2011 年発行）
　日本銀行がどのような役割・機能を担い、また、これを果たすため、どのような業務を行っているのかについて、網羅的かつ具体的に解説。

貨幣博物館 常設展示図録（ときわ総合サービス、2017 年発行）
　貨幣博物館の展示資料を紹介した図録です。

日本銀行金融研究所（IMES）
〒103-8660 東京都中央区日本橋本石町 2-1-1
TEL：03-3279-1111、FAX：03-3510-1265
E-mail：imes.journals-info@boj.or.jp
ホームページ：https://www.imes.boj.or.jp

資料公開サービス

以下の資料公開サービスを行っておりますので、ご利用下さい。

(1) 貨幣博物館の公開

2015年11月、貨幣博物館はリニューアルオープンしました。日本の貨幣を中心に、和同開珎や大判・小判の実物、貨幣に関する絵画など、貴重な資料を多数展示するとともに、所蔵資料を貨幣博物館ホームページ等で一般に公開しています。20名以上の団体で見学を希望される場合は予め電話でご連絡下さい。

開館時間：9時30分～16時30分（入館は16時まで）
休 館 日：月曜日（ただし祝休日は開館）
年末年始（12月29日～1月4日）
※最新の情報は下記の当館ホームページで
お知らせいたしますので、ご確認下さい。
貨幣博物館ホームページ：https://www.imes.boj.or.jp/cm/
〈連絡先〉金融研究所　貨幣博物館
TEL：03-3277-3037（直通）

(2) 日本銀行が保有する歴史的公文（歴史的文書）の公開

金融研究所では、日本銀行に関連する歴史的資料のうち、歴史的価値を有するものについて保管・整理し、一般に公開しています。閲覧をご希望の方は、当館ホームページ掲載の目録で検索のうえ、予めメール・電話にてご連絡下さい。

歴史的公文の目録：https://www.imes.boj.or.jp/archives/hozon.html
〈連絡先〉金融研究所　アーカイブ
E-mail：imes.archives@boj.or.jp
TEL：03-3277-2151（直通）

金　融　研　究（第 45 巻 第 1 号）
ISSN 2759–5099
2026 年 1 月 20 日　発行
日本銀行金融研究所長
編集兼発行者　渡 辺 真 吾
発　行　所　日本銀行 金融研究所
郵便番号 103–8660
東京都中央区日本橋本石町 2–1–1
電　話：（03）3279–1111（大代表）
国際文献社
本誌に関する照会は、日本銀行金融研究所までお寄せ下さい。