03

リスク管理 1

AIと金融安定政策 ―海外の金融当局の政策対応動向―

金融機関による生成AIの利用は急速に拡大している。金融機関共通のAIモデルやクラウドへの依存・集中が、金融システムの脆弱性となる。日本の金融当局も、AIを金融システムに対するリスク要因として捉え、モニタリングとシナリオ分析態勢を迅速に整備する必要がある。

すでに幅広い分野でAIの活用が進んでいる

日本銀行の調査[1]によると、金融機関による生成AIの利用は試行を含め9割に達しており、大手行から第二地銀まで幅広い業態に拡大している。用途も、社内業務の効率化にとどまらず、融資稟議書の作成、与信審査・信用リスク管理、営業支援などへ広がりつつある。

金融庁が2024年に実施したアンケート調査とその後の知見を基に2026年3月に公表したディスカッションペーパー[2]も、RAG（Retrieval-Augmented Generation）によるLLMと社内データベースの連携や、社内データを用いたファインチューニングなど、金融機関が保有データをAIに組み込む動きを紹介している。生成AIは、単なる業務効率化ツールから、意思決定や金融サービスの提供を支えるシステムへ移行しつつある。

金融システム全体にもたらすリスクとして認識

こうした動きを受けて、各国の金融当局もAIがもたらすリスクの把握に乗り出している。金融安定理事会（FSB）は2024年の報告書[3]で、AIが金融システムにもたらし得る脆弱性として、第三者事業者への依存・集中、市場参加者の行動の相関、サイバーリスク、モデルリスク、データ品質やガバナンス上の問題を挙げた。

生成AIは、クラウド、半導体・計算資源、事前学習済みモデルなどへの外部依存が生じやすい。同一モデルの利用は判断や取引行動を同質化させ、市場変動を増幅する可能性がある。AIによる攻撃能力の高度化や、共通サービスの障害が複数の金融機関に同時に波及するリスクもある。

同報告書は、第三者事業者への依存と集中に注視し、①重要性：金融機関が生成AIを利用する業務がどの程度不可欠か（critical service）、②集中度：どの程度の金融機関が同一の第三者事業者に集中しているか（concentration）、③代替可能性：金融機関が他のサービスへ切り替えることができるか（substitutability）、④金融システム全体への影響・強靭性：障害時にも金融システムが機能を維持・回復できるか（systemic relevance of third-party dependencies）という4つの観点から状況を把握することが重要だと整理している。

あわせて、データギャップの解消、監視能力の向上、既存の規制・監督枠組みの点検、当局間の情報共有と国際連携を推奨している。

監視からシステムワイドな対応へ

欧州システミックリスク理事会（ESRB）の諮問科学委員会（ASC）も2025年12月の報告書[4]において、AIの利用や提供の集中、類似モデルへの依存、意思決定の高速化、過度な依存や相互連関を通じて、AIに伴うリスクが金融システム全体に波及し、システミックリスクを増幅・変容させる可能性があると指摘した。

さらに2026年6月には、フロンティアAIモデル（FAIMs）に起因するシステミックなサイバーリスクに関する正式な警告（ESRB/2026/3）を採択した。同警告は、FAIMsが金融インフラの基盤となるICT環境を脅かし、システミックな影響を及ぼすサイバーインシデントの発生可能性と深刻度を高めると指摘している。その

野村総合研究所　金融ITイノベーション事業本部 事業企画室 ©2026 Nomura Research Institute, Ltd. All rights reserved.

NOTE

1) 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」(2026年8月)。
2) 金融庁「AIディスカッションペーパー（第1.1版）」(2026年3月)。
3) FSB, "The Financial Stability Implications of Artificial Intelligence," November 2024
4) ESRB, "Advisory Scientific Committee, Artificial intelligence and systemic risk," December 2025
5) Bank of England, "Financial Stability Report," July 2026
6) Bank of England, "Frontier AI and the question of governance," September 2026

上で、関係当局に対し、それぞれの権限・所管の範囲内で、こうした懸念を監督・オーバーサイト業務および政策上の方針に反映させるよう求めている。AIをマクロプルーデンス政策の対象として明示した点で、FSBの国際的整理を具体的な政策対応へ進めた事例といえる。

また、英中銀のイングランド銀行は、2026年7月の金融安定報告書[5]において、フロンティアAIの急速な能力向上が金融システムのサイバー・オペレーショナルリスクを増幅し、システミックなサイバーイベントにつながる可能性を指摘するとともに、複数金融機関や共通のテクノロジー・サプライチェーンにまたがる相関的な障害などを含むシナリオを検討、AIシナリオをサイバー・オペレーショナル・テストに組み込む作業を進めている。9月のベイリー総裁のインサイト[6]では、金融機関によるAI導入前後の厳格なモデルテストを通じて、まず、中央銀行がシステム全体のリスクを理解、検証し、信頼できる介入ポイントを確立することが必要だとしている。

海外の対応は、単に「AI利用を監視する」段階から、AIを金融システムへのシステミックなストレス要因として捉え、金融機関や共通するAI・ICT基盤への依存・集中を踏まえて、シナリオ分析、モニタリング、テスト、監督上の対応を強化する段階へ進みつつある。

日本も早急に金融安定政策への実装を

日本では、金融庁と日本銀行が生成AIの利用状況を調査しており、オペレーショナル・レジリエンスや第三者リスク管理の枠組みの高度化も進む。他方、AIモデル、クラウド、計算基盤を含む依存関係を、金融システム横断的に定量把握する仕組みは、なお発展途上にある。

金融庁、日本銀行、関係省庁は、第一に、利用金融機関数、重要業務の依存度、集中度、代替可能性、切替え・復旧時間などのモニタリング項目を整備し、ヒートマップの提示や警戒閾値の設定によって、リスクを可視化すべきである。第三者事業者については、経済安全保障推進法、サイバーセキュリティ政策、重要インフラ政策等との重複・補完関係を整理したうえで、金融システム安定の観点から監視を追加する必要がある。

第二に、蓄積したデータを用いて、共通AI・ICTサービスの停止やAIを利用した同時多発的なサイバー攻撃を想定するシナリオ分析を重ね、銀行、証券、保険、決済・市場インフラから実体経済に至る波及メカニズムを特定すべきである。その成果を踏まえ、システムワイドなストレステストやマクロプルーデンス措置への接続を検討することが望ましい。

第三に、AI関連ショックは波及が迅速かつ広範になり得る。政府・金融当局は、金融システム全体の損失を最小化するため、対象業務やAIサービスの一時停止を含む緊急措置について、発動要件、法的根拠、権限分担、解除手続、国際連携をあらかじめ検討すべきである。

これらの対応は、AI利用による生産性向上や国際競争力を損なわないよう、リスクに応じて比例的に設計する必要がある。同時に、依存先の多くがグローバル事業者であることを踏まえ、FSB等を通じて国際的に歩調を合わせることが不可欠である。

Writer's Profile



石川 純子 Junko Ishikawa
金融イノベーション研究部
グループ・マネージャー
専門はマクロ経済分析、中央銀行の政策
focus@nri.co.jp