04

リスク管理 2

経済安全保障下における金融機関のAIガバナンス

Mythosショック以降、AIを用いたサイバー脆弱性対策が急速に進展している。従来求められたハルシネーションや情報漏洩への対応にとどまらず、今後、経済安全保障というリスク評価が不可欠となる。とりわけ注意を要するのはAIモデルの輸出管理規制を踏まえたガバナンスの構築である。

モデル・リスク管理によるAIガバナンス

「Mythosショック」を契機としたサイバーセキュリティの脆弱性評価への活用が進む一方、負の側面として、AIそのものがサイバー攻撃の実行主体となり得る脅威も認識されるようになった。

こうした中、金融庁は2026年3月に『AIディスカッションペーパー』を改訂・公表した。同資料は、金融機関に対するアンケート調査およびヒアリングに基づき、AIの活用事例や課題認識を取りまとめたものである。金融機関の実務におけるAIの利用は、日常業務の効率化をはじめ、与信審査やマネー・ローンダリングおよびテロ資金供与対策（AML/CFT）など多岐にわたるユースケースが存在する。同資料においてAIガバナンスの構築に向けた取り組みも紹介されており、「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」と、当局のガバナンス構築への関心の高さを示している。

生成AIの技術進化は極めて急速であり、金融機関における利用者としてのAIガバナンスの考え方も流動的な状況にあるが、欧米主要国においては、AIガバナンスを「モデル・リスク管理（MRM）」の枠組みに含めて捉えることが一般的である。これは、モデルが一般に「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」と定義され、生成AIを含む広範なAIの挙動がこの枠組みに合致するためである。

具体的な制度の例としては、バーゼル銀行監督委員会（BCBS）が2024年5月に公表した報告書『金融のデジタル化（Digitalisation of finance）』、米国財務省の報告書『金融サービスにおける人工知能（Artificial Intelligence in Financial Services）』等が挙げられ、いずれもモデル・リスク管理の枠組みを基本としている。もっとも、米国連邦準備制度理事会（FRB）等が2026年4月に発出した監督指針『SR Letter 26-2（モデル・リスク管理に関する監督ガイダンス）』においては、AIが急速な発展途上にあり発展形態が定まっていない現状に鑑み、規制枠組みへの性急な規定を一旦見送り、個別金融機関による自律的なガバナンス判断に委ねる姿勢をとっている。

このように、欧米においてはAIガバナンスの必要性が認識され、モデル・リスク管理に包含させるというコンセンサスがある一方で、米国の例にもある通り、技術の急激な進化を背景に、業界として一律のガバナンスが確立されているわけではない。しかしながら、AI活用がAI以外の一般的なモデル（財務・時価評価モデル、信用リスク・与信管理モデル等）に進む現状に鑑みれば、AIを既存のモデル・リスク管理と切り離して考えることは実務上も困難である。

AIガバナンスに欠かせない輸出管理

金融庁が2021年11月に公表した「モデル・リスク管理に関する原則」では、「3つの防衛線」を含む重要な概念と8つの原則が示されている。

この原則は、「特定のモデルのカテゴリーに限定せず、

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.

広範なモデルを対象」としており、AIガバナンスも対象となると考えられる。仮にAIガバナンスをこの枠組みに沿って実践する場合、AIモデルごとに挙動の特性が異なる点を踏まえると、AIモデルを使った一般的なモデル（財務・時価評価モデル、信用リスク・与信管理モデル等）のみならずAIモデル単体も対象に含める必要がある。

例えば、「3つの防衛線」の管理部署には「モデル承認（原則4）」の役割が求められる。AIモデルを審査・承認するにあたっては、明確な基準が存在しない現状において、経産省・総務省による『AI事業者ガイドライン』や、AIの安全性確保に取り組む機関AISIの『AIセーフティに関する評価観点ガイド』が重要な参考となる。

さらに、この審査・承認においては、AIが実質安全保障や国防のいわゆるデュアルユースであることから、これまで金融機関では意識してこなかった輸出管理の観点が不可欠となることに留意する必要がある。

AIモデルの開発・進化は現在、米国と中国が中心であり、両国の緊張関係を背景に、AI関連技術、ソフトウェア、ハードウェアが米国輸出管理規制の対象となっている。米国輸出管理規制は、米国製品や技術を介する形で法域外の日本にも適用される。詳しくは割愛するが、仮に国内の金融機関が米国から取引禁止企業として指定された場合、米国製品の利用が不可能となるなどの致命的な事業リスクが生じるため、日本の金融機関にとっても同規制への準拠は避けては通れない。

詳しくは、個別の技術、ハードウェア、ソフトウェアの種類を確認する必要があるが、具体的にはNVIDIA製のような高機能のGPUや各種AIモデルの特定国への輸出が制限されている。また、技術、ソフトウェアについては、実際に物理的な輸出を規制するだけでは十分ではないとして、現在、下院は通過し、上院で審議中のRemote Access Security Actでは、リモートアクセスも輸出と同等にみなすことが検討されている。本法案の可決の時期等は未定ではあるが、実質的にはすでに、リモートアクセスも輸出と同等とみなされていると考えてよい。

その場合、実際にハードウェア、技術、ソフトウェアの物理的な移動を伴わなくとも、米国の指定対象国に拠点をおく企業、あるいはそうした国に実質的株主を持つ日本企業から、日本に設置されたAIへアクセスすること自体が輸出規制の対象となる可能性がある。

こうした法制度やリスクへの備えとして、米国の各種AIモデルのライセンス規約では、米国の輸出規制を広めに解釈して、利用可能な国が限定列挙されている。したがって、「モデル承認（原則4）」では、該当するAIモデルの利用範囲に、上記に該当するグループ会社、委託先（再委託先含む）が含まれていないかを確認し、それを担保するようなセキュリティ設定を講じる必要がある。

もっとも、金融機関の既存のモデル管理部署が輸出管理から高度なセキュリティ設定の妥当性までを一手に審査することは現実的でない。関係部署による会議体の設置や、外部リソースの活用など組織横断的な態勢を構築した上で、モデル・リスク管理態勢の中にAIガバナンスを適切に組み込んでいくことが求められる。

Writer's Profile



堤 順 Jun Tsutsumi
金融ITイノベーション事業本部
シニアチーフ研究員
専門は金融向けGRC
focus@nri.co.jp