KPMG あずさ監査法人

本邦金融機関のAIガバナンスの在り方

AIの「モデル」としての特定・管理と海外のトレンドを踏まえて

近年、さまざまな業務でAIが活用されるなか、AIリスクの管理態勢（AIガバナンス）の構築が進められている。「攻め」としてのAIの活用のみならずそのリスクを管理する「守り」の整備は、その両方が極めて重要である。現在、あらゆる企業で「攻め」の方策と「守り」の態勢の検討が行われているが、より強固なリスク管理が求められる金融機関は、どのようにAIガバナンスを整備していくべきだろうか。本稿では、AIを「モデル」として整理し、そのリスクを管理する枠組みのなかで態勢を構築している海外のトレンドを取り上げる。そのうえで、本邦金融機関のAIガバナンスの在り方について1つの考え方を示したい。

AIの定義

金融機関業務において、AIが活用されない日はない[1]。AIが活用される領域や業務も多岐にわたっており、チャットボットによるQ&A対応から画像・音声認識、顧客への提案、リスク管理・評価、不正検知・コンプライアンス対応等、業務の効率化から高度化まで、さまざまな用途で活用されている（「攻め」の観点）。

同時に、インプットデータのバイアスやアウトプットのハルシネーション、法的・レピュテーショナルリスク、サードパーティーへの集中リスク、サイバー攻撃などのAI特有のリスクを管理する必要もある（「守り」の観点）。こうしたことを背景に、どのようなAIリスクの管理態勢（AIガバナンス）を構築すべきか、政府や金融機関等で検討が進められている[2]。

そもそも、AIはどのように定義されるのだろうか。各国の政府や民間企業、国際機関等からさまざまな定義が示されており、図表1でAI事業者ガイドラインにおけるAIの定義を取り上げた。米国では、NIST（米国国立標準技術研究所）の定義が有名だろう。欧州ではOECDの定義が一般的であり、FSBのドキュメントでもその定義が採用されている。このようにAIの定義にはさまざまなものが存在するが、これらの定義で共通している点は、「何らかのインプットデータを処理して、アウトプットを出力するもの」という点だろう。

---

1 本稿では従来型AIと生成AIを区別せず、AI全般を取り上げている。従来型AIと生成AIについては、「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」であり「生成AIとは、大規模言語モデル（LLM）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」（金融庁「AIディスカッションペーパー」）の整理が参考になる。

2 AIガバナンスについては、経済産業省「我が国のAIガバナンスの在り方ver.1.1」では、「AIの利活用によって生じるリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる正のインパクトを最大化することを目的とする、ステークホルダーによる技術的、組織的、及び社会的システムの設計及び運用」と定義されている。また、金融庁は2025年に「AIディスカッションペーパー」を公表し、金融機関等のAIガバナンスについて触れている。

© 2025 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

図表1：AIの定義の例

AIシステム

活用の過程を通じて様々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とする（機械、ロボット、クラウドシステム等）。

（中略）

（参考としてOECD AI Principles overviewでは以下のように定義されている）
AIシステムは、明示的又は暗黙的な目的のために推測するマシンベースのシステムである。受け取った入力から、物理環境又は仮想環境に影響を与える可能性のある予測、コンテンツ、推奨、意思決定等の出力を生成する。AIシステムが異なれば、導入後の自律性及び適応性のレベルも異なる

AIモデル（MLモデル）

AIシステムに含まれ、学習データを用いた機械学習によって得られるモデルで、入力データに応じた予測結果を生成する。

出典：総務省 経済産業省「AI事業者ガイドライン（第1.1版）」（https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf）より抜粋

モデルの定義

次に、モデルの定義はどうだろうか。2021年に公表された金融庁の「モデル・リスク管理に関する原則」（以下、金融庁原則）によると、図表2のようなモデルの定義が示されている。古くは、2011年にFRB／OCCが米国におけるガイダンス（SR11-7）においてモデルの定義を示しているが、金融庁原則の定義とほぼ同じである[3]。

図表2：金融庁原則のモデルの定義

「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。モデルには、インプット又はアウトプットの全体又は部分が定性的なものや、インプットが専門的判断に基づくものも含まれる。

出典：金融庁「モデル・リスク管理に関する原則」（https://www.fsa.go.jp/news/r3/ginkou/20211112/pdf_02.pdf）より抜粋

一方で、AIには一般的なモデルにはない特徴も存在する。例えば、AIはアウトプットを出力する過程のなかで、膨大な（非構造）データを用いながら計算処理を自動で行い得る点は特徴の1つである。またAIは、既述のようなインプットデータのバイアスやアウトプットのハルシネーション、法的・レピュテーションリスク、サードパーティーへの集中リスク、サイバー攻撃などの特有のリスクを有していることも重要である。

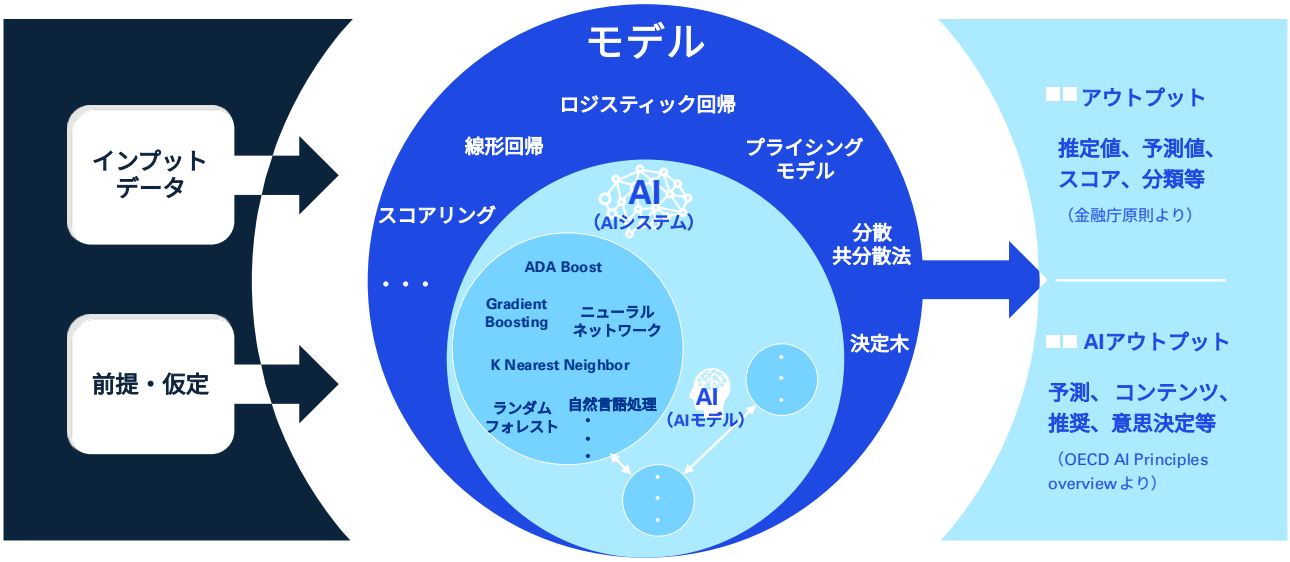
しかしこうした違いはあれど、これまで見てきたAIとモデルの定義からは両者はほぼ同じ定義であり、AIは数あるモデルの手法の1つと捉えれば、広く「モデル」に含まれるという考え方に大きな異論はないものと思われる（図表3）[4]。特に海外の金融機関は、このようなイメージを持っている印象がある。

3 The Fed - Supervisory Letter SR 11-7 on guidance on Model Risk Management -- April 4, 2011

4 本稿では、AIとモデルの定義や手法に着目して包含関係を示した。ほかに、AIとモデルが有するリスクに着目してその共通点から包含関係を整理することも一案である。

© 2025 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

図表3：モデルとAIの関係イメージ



注：あくまでイメージであり、モデルと AI の包含関係にはほかの考え方もあり得る点に留意が必要
出典：KPMG ジャパン作成

ライフサイクル管理

SR11-7の公表以降、米国の金融機関はモデルの管理を徹底している。そのなかで、「AIは（SR11-7のモデルの定義に合致する）モデルである」という考え方があり、米国の金融機関では、「AIはモデルである以上、モデル管理の枠組み（Model Risk Management、以下、MRM）でAIを統制すべき」という捉え方が浸透している。

MRMでは、モデルは次のようなライフサイクルに組み込まれ、管理が行われる。すなわち、1線によって開発された計算処理・手法はモデルの定義に合致し、モデルとして特定され、インベントリー（一覧表）に登録されて管理がスタートする。その後、モデルの使用目的や重要性、複雑性等に応じてモデルのリスクが評価され、2線による検証・承認を経て使用される。モデルが使用される期中もモデルのパフォーマンスがモニタリングされ、再検証を経て継続使用が許可される。こうした一連のライフサイクルを経る点は、AIであれそれ以外のモデルであれ、MRMでは基本的には同じである。

一方、AIについては、従来のMRMのライフサイクル管理では捉え難い論点も存在する。例えば、モデルの特定について、「どこまでのAIをモデルとして特定し、管理すべきか。個人が検索等で使用するAIも管理すべきなのか（すべてのAIを管理することは現実的ではない）」といった論点がある。また、モデルの開発・検証について、「SR11-7などのMRMガイダンスは、AIの開発・検証にフォーカスを当てていない（ため、管理の着眼点が分からない）」といった声も聞かれる[5]。さらに、MRM部署の関与については、「AIはその特性から、MRM部署以外の関与も必要ではないか（MRMだけでは不十分ではないか）」といった論点や「AI任せにせず、最後は人間が関与すべきであり、その枠組みを組み込む必要があるのではないか」といった論点もある。

5 既述の金融庁「AI ディスカッションペーパー」において、金融庁原則の明確化を行うべきといった趣旨のコメントがなされている。

© 2025 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

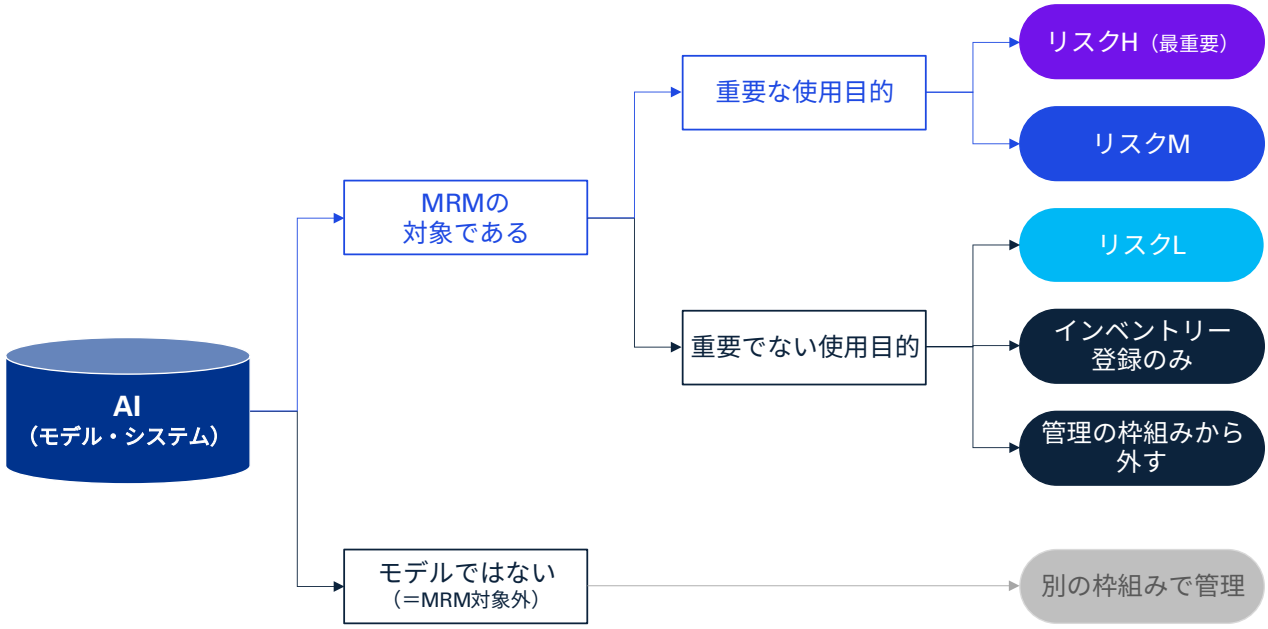
海外のトレンド

しかしこれらのいずれの論点についても、MRMの考え方のなかに答えを見つけることは可能である。

①　モデルの特定

まずモデルの特定については、AIの使用目的や使用者を踏まえて重要ではないAIは、リスクが低い（Low）として管理、またはインベントリー登録に留める、さらには思い切ってMRMの管理の枠組みから外すといった対応が合理的だろう。今後、自社データを学習させた自社専用のAIなどが活用されることでAIの数が膨大になることが想定されるなか、AIの使用目的などに応じて管理のメリハリを付けることは極めて重要である（図表4）。また、自社ではどのようなAIがあり、誰がどのような使用目的でAIを活用しているのか「見える化」を行う意味では、インベントリーへの登録がAIの管理の出発点になる。

図表4：AIの管理における分類の例



出典：KPMG ジャパン作成

②　モデルの開発・検証

またモデルの開発・検証については、SR11-7などで示されている開発・検証の着眼点のなかで、既述のインプットデータのバイアスやアウトプットのハルシネーション等のAI特有のリスクを踏まえて開発・検証を行うことが重要になる[6]。

6 KPMG Trusted AIフレームワーク（https://kpmg.com/jp/ja/home/services/advisory/kpmg-trusted/trusted-ai.html）では、公平性、透明性、説明可能性、説明責任、データインテグリティ、信頼性、セキュリティ、安全性、プライバシー、持続可能性の観点でAIの管理を行うことが重要と指摘しているが、いずれの観点も概ねMRMの枠組みで整理することは可能である。具体的には、①データ、②手法（モデルのコンセプトやロジック）、③テスト（アウトカムアナリシス）、④実装、⑤ガバナンスといった、モデルの開発・検証時に重要になる5項目において、AIのリスク等を特定・評価・コントロールすることになる。例えば、本稿で取り上げたインプットデータのバイアス（上記の観点の公平性に相当）は①で、アウトプットのハルシネーション（信頼性）は②や③で、法的・レピュテーションリスク（プライバシーや安全性）やサードパーティーへの集中リスク（セキュリティや安全性）は⑤で、サイバー攻撃（セキュリティや安全性）は④や⑤などでリスクを評価・低減することが考えられる。ただし、特に生成AIについては、どのように効果的なモデル検証（いわゆるeffective challenge）を行うべきか、MRMで先を行く米国の金融機関でも継続的に議論が行われている。

© 2025 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

③ MRM部署以外の関与

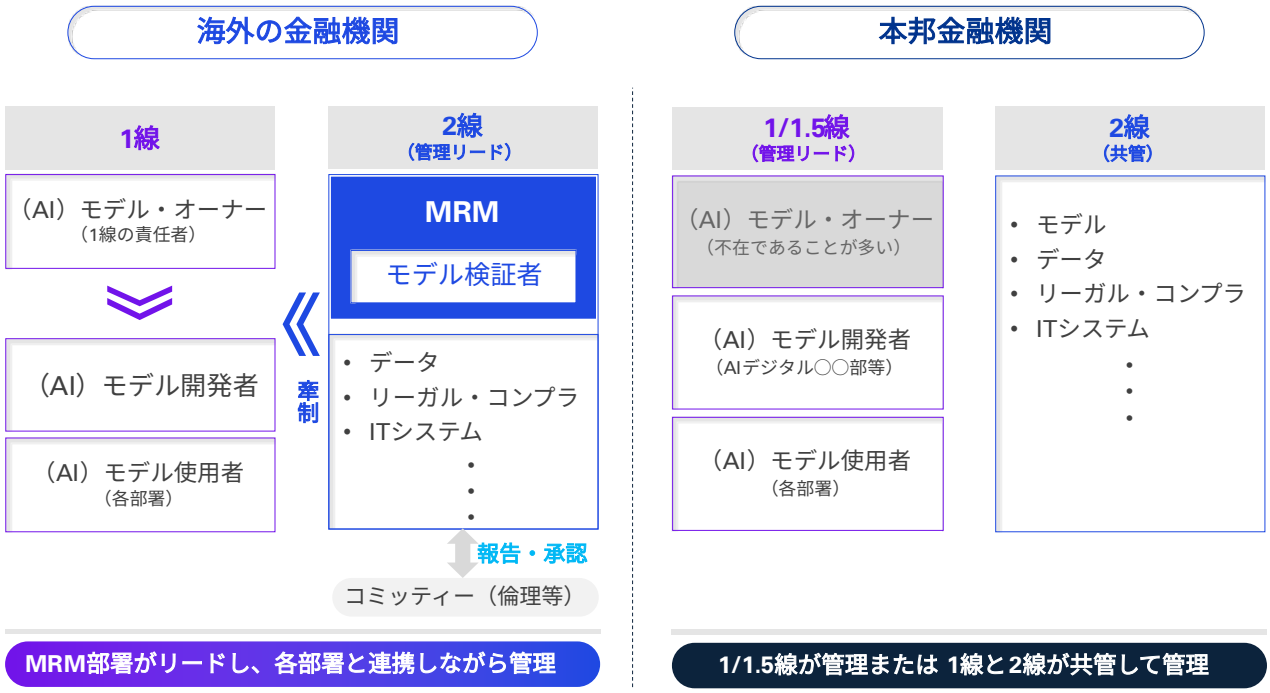
MRM部署以外の関与については、後述のとおりモデルの管理はMRM部署がリードしつつ、AI特有の課題についてはデータやリーガル、コンプライアンス、ITシステム部署等が関与して協働でリスクを管理することが求められる（AIの開発・検証時に、これらの部署を巻き込むことが重要）。AI使用の承認を行うコミッティー（例：AI倫理委員会）の設置・関与も、一案だろう。

④ 人間の関与

最後に、人間の関与については、MRMのガバナンスのなかで、Human in the Loop（人間の関与と是正の枠組み）を組み込むことや既述のコミッティーの設置・関与を行うことで、リスクを低減することが重要である。

以上を踏まえると、海外（特に米国）の金融機関におけるAIガバナンスは、図表5のようなイメージとなる（参考として、後で取り上げる本邦金融機関の態勢のイメージも示している）。米国では、グローバルに重要な金融機関であるG-SIBsレベルから地域金融機関といった規模の大小に関わらず、図表5のような態勢を構築してAIを管理することが一般的である。つまり、MRM部署がAI管理の土台になっている。

図表5：海外の金融機関におけるAIガバナンスのイメージ



出典：KPMG ジャパン作成

本邦金融機関のAIガバナンスの在り方

一方、本邦金融機関では、AIデジタル○○部／AI活用○○部等のAIの1線（1.5線）の部署が管理をリードする流れにあると思われる。

これにはいくつかの要因があるが、例えば「AIをモデルとして捉えていない（モデルではないため、MRMとは別の部署の管理が自然）」といった事情や「AIはモデルと認識しておりMRM部署が管理すべきと考えているが、自社ではMRMが発展途上であるため、現実問題として対応出来ない」といった事情があると思われる。または「AIにMRMを導入すると管理の強度が高まり、AIの活用が進まない（ため、MRM部署の関与はあえて限定的にしている）」という考え方もあるかもしれない。

© 2025 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

しかし、既述の海外のトレンドを踏まえると、本邦金融機関でもAIをモデルとして特定したうえで、何らかの形でMRM部署（やそれに近い機能を持つ部署）の関与を検討する（または関与を増やす）ことは一案だろう。以下では、その場合の1つの考え方を示したい。

① G-SIBsやD-SIBs等の規模の大きな金融機関

まず、金融庁原則の適用対象であるG-SIBsやD-SIBs、それに近い規模の大きな金融機関であれば、自社にある程度のMRM部署が存在することを踏まえて、MRM部署がAIの管理をリードすることを検討してもよいだろう。一方で、MRMを適用すると管理の強度が高まることによって、AIの活用に急ブレーキが掛かることも想定される。まさに「攻め」と「守り」のバランスが重要になるが、例えば図表4で紹介したように、モデルの特定時にAIの使用目的に応じて管理のメリハリを付けることがポイントになるだろう。

② ①以外の金融機関

次に、金融庁原則の適用対象外の中小金融機関については、MRM部署が発展途上または未整備であると考えられる。こうした金融機関では、MRM部署がリードすることは難しく、AIの開発・使用部署（1線や1.5線）が管理を主導することになるだろう。同時に2線（MRM部署やそれに近い機能を持つ部署）の態勢整備を少しずつ行いながら、2線の関与を増やすことも意義があると思われる。どこかの段階で、AIの管理・承認機能を2線に移管することは目指すべき姿かもしれない（ただしMRMを組み込む場合は、既述のとおりバランスを考慮することは必要である）。

③ 事業法人

最後に、金融機関以外の事業法人については「MRM部署を設置する」といったことは難しく、そもそも「AIはモデルである」「モデルを管理する」という発想があまりないものと思われる。従って、事業法人についてはAIの開発・使用部署が管理をリードすることが自然だが、ほかの関連部署との連携は金融機関同様、重要な観点である。なお、事業法人にとっても金融機関のモデル管理やMRMの考え方は有用であるため、活用できる点は参考にしながら態勢を整備すれば、より強固なAIガバナンスを構築できると思われる。

おわりに

本稿では、海外のトレンドを踏まえて本邦金融機関のAIガバナンスの在り方について1つの考え方を示したが、海外のやり方をそのまま取り入れれば良いというわけではない点も事実である。海外に比べて、MRMが発展途上の本邦金融機関ではなおさらである。MRM部署のリソースや負担・スキルも考慮に入れなければならないし、MRMを組み込むことでAIの利用に大幅な制約が掛かることも望ましくないだろう。MRM部署が関与しない場合であっても、MRMのようなライフサイクル管理（の一部）を取り入れる方法も考えられる。本邦金融機関独自のAIガバナンスがあってもよいだろう。

一方で、かつて日本の携帯電話（いわゆる「ガラケー」）がそうであったように、それ自体は優れた機能を持ちながらもトレンド（スマホの隆盛）に乗れなかったがために時代に取り残された例も存在する。本邦金融機関がどのようなAIガバナンスを構築するとしても、グローバルのトレンドやMRMの考え方を参考にしたうえで、あるべき自社の態勢を考えることは重要である。

© 2025 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

なお、これまでMRMを重視してこなかったアジアでも、近年MRMにフォーカスが当たっている。アジアの当局でもモデル管理の重要性が認識されていることもあるが、「AIはモデルであり、MRMで管理すべき」という考え方が浸透してきていることも要因として考えられる。実際、アジアの当局からは、MRMとAIの関連性を整理したガイダンスが公表されている[7]。本邦金融機関には、こうしたグローバルのトレンドも踏まえながら、自社に最適なAIガバナンスを整備することを期待したい。

以上

7 中華人民共和国香港特別行政区（SAR）の当局が「Circular to licensed corporations - Use of generative AI language models」を、シンガポールの当局が「ARTIFICIAL INTELLIGENCE MODEL RISK MANAGEMENT OBSERVATIONS FROM A THEMATIC REVIEW」を公表している。

編集・発行

有限責任 あずさ監査法人
金融統轄事業部　金融アドバイザリー事業部

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査したうえで提案する適切なアドバイスをもとにご判断ください。

© 2025 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.