第１回　AI等の健全な利活用の推進に関する研究会

資料２－２

事務局参考資料
金融分野のAI利活用における課題や対応策に関する国際機関等の報告書

2026年11月24日

金融庁
Financial Services Agency, the Japanese Government

金融分野のAI利活用における課題や対応策に関する国際機関等の主な報告書

公表日	組織	タイトル
2024年10月22日	IMF	人工知能の発展が資本市場に与える影響 “Advances in Artificial Intelligence: Implications for Capital Market Activities”（GFSR Chapter3）
2025年４月９日	BoE	金融安定性の観点から見る金融システムにおける人工知能 “Financial Stability in Focus: Artificial intelligence in the financial system”
2025年10月10日	FSB	金融セクターにおけるAI導入と関連する脆弱性の監視 “Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector”
2026年４月23日	IMF	AIエージェントがもたらす決済の変革 “How Agentic AI Will Reshape Payments”
2026年５月25日	IOSCO	資本市場におけるAI利用に関する監督ツールキット “Supervisory Toolkit for AI Use in Capital Markets”
2026年10月７日	Europol	量子コンピューティングと暗号資産 “Quantum Computing and Cryptocurrencies”
2026年10月７日	MAS	AIリスク管理に関するガイドライン “Guidelines on Artificial Intelligence Risk Management”
2026年10月15日	FSB	AIの責任ある導入に関する健全な実務慣行に係る報告書 “Sound Practices for Responsible Adoption of Artificial Intelligence (AI): Final report”
2026年10月15日	HKMA	人工知能の責任ある導入 “Responsible Adoption of Artificial Intelligence”
2026年10月28日	CFTC	CFTC Frontier Forum（Michael S. Selig 委員長発言）
2026年11月４日	OCC	銀行によるスーパーインテリジェンスの利用に関する監督フレームワーク “OCC Supervisory Framework on Bank Use of Super Intelligence”

IMF「人工知能の発展が資本市場に与える影響」（2024年10月）
GFSR Chapter3 “Advances in Artificial Intelligence: Implications for Capital Market Activities”

- 国際通貨基金（IMF）は、2024年10月22日に、国際金融安定報告書（GFSR）を公表。第3章において、**人工知能の発展が資本市場に与える影響**について言及し、市場参加者や規制当局へのアウトリーチから得られた洞察と新たな分析に基づき、**新技術の広範な採用から生じ得る利益とリスク**を説明の上、政策対応を提案。

リスク	具体的なリスクの内容	主な政策対応
市場ストレス時における市場スピードとボラティリティの上昇	• AIモデルは、特に市場のストレス時に群衆行動をとり、類似した判断を行うことで、**市場の変動を増幅させる金融安定上のリスクをもたらす**可能性がある。市場に負のショックが生じた場合には、複数のモデルが同時に安全資産へポートフォリオを再配分し、**投げ売りの連鎖を生じさせるおそれ**がある。 • 前例のない事象が発生した場合には、AIモデルが理解困難な結果を出力し、又は停止することで、**人間が大量の取引について意思決定及び処理を行う必要が生じる可能性**がある。	• AIによる急速な価格変動が生じ得ることを踏まえ、**サーキットブレーカーの適切な設定及び証拠金慣行の見直し**を実施すること。
不透明性の高まりと監視上の課題	• AIの利用拡大により、市場形成や投資活動がヘッジファンド、自己勘定取引会社その他の**ノンバンク金融機関（NBFI）へさらに移行する可能性**がある。 • AIモデルが複数の資産クラス、地域及び市場にまたがって投資判断を行うことで、市場参加者間の相互作用や相関関係が複雑化し、その**実態が把握しにくくなるおそれ**がある。 • このため、異なる投資家やトレーダーが利用するAIモデルが相互にどのような影響を及ぼし合うか不透明となり、**金融システム全体のモニタリングがより困難になる**可能性がある。	• NBFIを含む大口トレーダーの活動について、**モニタリング及びデータ収集を強化**すること。 • 規制対象事業者に対し、**データ、モデル及び技術インフラの相互依存関係に係るリスクマッピングを求める**ことにより、当該依存関係に対応すること。
少数のAIサービス提供者への依存に伴うオペレーショナルリスク	• AIモデル及び関連するITサービスは、支配的な計算能力と確立された大規模言語モデルを有する少数の事業者に集中している。資本市場活動がこれらのモデルに過度に依存した場合、当該事業者の機能停止や障害が、**清算機関等の重要な金融市場インフラの機能不全に類似した市場ストレスを生じさせる**おそれがある。	• 規制対象事業者に対し、データ、モデル及び技術インフラへの依存関係に関するリスクマッピングを求めることにより、当該依存関係に対応すること。特に、**少数の第三者AIサービス提供者への依存関係及び集中リスクを把握**すること。
市場操作及びサイバーリスクの増大	• AIの高度化に伴い、詐欺、偽情報及びディープフェイクがより巧妙化し、**悪意ある主体によって金融市場や資産価格の操作に利用される可能性**がある。 • データの完全性及び機密性が損なわれることで、**AIモデルが最適でない取引・投資判断を行うおそれ**がある。	• AIモデル及び関連するデータの**ガバナンス並びに健全性を強化**すること。 • AIの利用に伴う不正行為、市場操作及びサイバーリスクに対応するための**監視能力を向上**させること。

BoE「金融安定性の観点から見る金融システムにおける人工知能」（2025年4月）

“Financial Stability in Focus: Artificial intelligence in the financial system”

- イングランド銀行（BoE）は、2025年4月9日に、「金融安定性の観点から見る金融システムにおける人工知能」を公表。金融機関のAI利活用の進展がもたらし得る金融安定上のリスクについて、**銀行及び保険会社の中核的な金融意思決定におけるAI利用の拡大**、**金融市場におけるAI利用の拡大**、**AIサービス提供者に関するオペレーショナル・リスク**、及び**変化する外部のサイバー脅威環境**の4つの領域に焦点を当てて指摘。

■ **銀行及び保険会社の中核的な金融意思決定におけるAI利用の拡大**

銀行及び保険会社は、それぞれ信用供与及び保険引受に関する中核的な事業上の意思決定へAIの利用を一層組み込んでいく可能性が高い。特に、AIモデルがエージェント機能においてますます利用されるようになるにつれて、既存の規制枠組みが、個社レベルの統制とともに、AIに起因するミクロ（個別金融機関）のリスクを十分に抑制することが重要となる。

多数の金融機関が同一のオープンソースのモデル構成要素またはデータライブラリに依存している場合、重大な未知の誤りまたはバイアスにより、多くの金融機関が特定のリスクを誤って見積もり、その結果、**与信の値付けを誤り不適切な配分を行う可能性**がある。このような脆弱性が最終的に顕在化した場合、複数のシステム上重要な企業が損失を負い、**実体経済への信用供与の引き締め、または信認の喪失を通じた金融システム全体への波及**につながり得る。

サービスの利用可否及び価格設定に関する中核的な意思決定がAIモデルに依存するシナリオの下では、偏った、または誤って調整されたデータもしくはモデルが、**消費者による金融商品へのアクセス等に直接影響**を及ぼす可能性がある。

■ **金融市場におけるAI利用の拡大**

市場参加者は、より高度なAIベースの分析を中核的な取引及び投資活動に組み込んでいく可能性が高い。未知のデータまたはモデルの欠陥により、市場参加者のエクスポージャーが誤って測定または解釈され、結果として**市場のストレス事象に耐えるための財務上の強靭性が不足**する可能性がある。また、AIモデルが、歴史的に前例のないショックなどの**極端な事象**や、予測の前提を置くことが難しい**不確実な状況への対応は、特に困難**となり得る。

AI主導の取引・投資戦略は、市場参加者が相関したポジションを取る傾向を強め得る。**高度なAI取引モデルがより大きな自律性をもって行動するよう導入されるシナリオ**では、**高度なAI取引モデルが、他社の取引戦略の弱点を特定して利用し、相場変動を引き起こし、または増幅させる**可能性がある。もう一つのリスク要因は、そのようなモデルが、**共謀またはその他の形態の相場操縦を容易にする**可能性である。一部のAIモデルがマルチエージェント環境で動的に学習する能力を有すること及びモデル出力の説明可能性を巡る課題を踏まえると、このような有害な行動は、人間の管理者の意図または認識なしに生じる可能性がある。

■ **AIサービス提供者に関するオペレーショナル・リスク**

多くのAI導入において、金融機関はベンダー提供のAIモデルに依存している。特定のサービスを少数のサービス提供者に依存する場合、特に代替サービスの提供者への迅速な移行が難しい場合には、**AIサービス提供者の障害がシステミック・リスクにつながる**可能性がある。

外部サービス提供者に関連する深刻な業務障害は、金融システムへの影響が重大である場合、金融安定上の問題につながり得る。

官民連携により、AIの導入に伴うリスクを管理するための「責任共有モデル」の策定が進められている。このモデルでは、AIの導入形態に応じて、外部サービス提供者と利用金融機関のいずれがデータ管理の責任を負うかなどを整理する。

■ **変化する外部のサイバー脅威環境**

サイバー攻撃は多くの金融機関が直面する重大なリスク要因であり、AIは、**悪意ある主体にとって新たな攻撃手段**となり得る。攻撃者によるAIの利用は、金融システムに対するサイバー攻撃の成功可能性を高め、従来よりも高度かつ大規模な攻撃を可能にするおそれがある。金融機関自身によるAI利用も、第三者提供者のソフトウェアまたはハードウェアを巡る脆弱性を通じて、攻撃者に新たな侵入・攻撃機会を与える可能性がある。より長期的には、サイバー攻撃者が、**今後発展する量子コンピューティング技術をAIと組み合わせる可能性**について、技術進展を踏まえて継続的にモニタリングする必要がある。

FSB「金融セクターにおけるAI導入と関連する脆弱性の監視」（2025年10月）①

“Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector”

- 金融安定理事会（FSB）は、「AIの金融安定上のインプリケーションに関する報告書」（2024年11月公表）で特定されたAI利用に伴う金融セクターの脆弱性を踏まえ、2025年10月に、**当局が金融機関によるAIの導入状況をモニタリングし関連する脆弱性を評価するための手法**について検討した「金融セクターにおけるAI導入と関連する脆弱性の監視に関する報告書」を公表。
- 多くの当局がAIのユースケースとその利点・脆弱性に対する理解を深めつつある一方で、AIに関連する**金融安定上の脆弱性に対するモニタリングの枠組みは依然として初期段階にある**ことや、**AIの共通定義の欠如や法域間の比較可能性の困難さ**等を課題として指摘しつつ、各国当局の取組事例等を踏まえ、モニタリングにおける考慮事項や潜在的な指標を特定した上で、各法域・FSB・基準設定主体（SSBs）が今後考慮すべき事項を提示。

主な指摘事項

■ データ収集における考慮事項

①脆弱性との関連性、②代表性、③関連する基準及び分類法との整合性、④適時性、⑤負担への配慮、に留意してAI関連のデータを収集すべき。

■ モニタリングにおける考慮事項

①AIサービスの重要性、②集中（特定のAIサービス提供者への依存）、③代替可能性、④サードパーティ依存が金融システム全体に及ぼす影響、を考慮すべき。

■ 潜在的な指標

金融セクターにおけるAIの導入状況に関する直接・代替指標（例：AIを活用する金融機関の割合や、その代替指標としての金融機関内のAI関連職種の動向）に加え、個別リスク（サードパーティ依存・集中、市場相関、サイバー、モデル・リスク、AIを用いた詐欺・偽情報）をモニタリングするための指標など、監視当局において利用可能な潜在的指標を特定。

各法域及びFSB・SSBsにとっての考慮事項

■ 各法域

- 考慮事項を踏まえたモニタリング手法の強化。
  - 特定された指標を踏まえた、脆弱性の監視と評価を目的とした指標の正式化
  - 金融機関に対する監督上の関与強化を通じた、定量指標の特定が困難な脆弱性に関する知見の獲得
  - AIツールの活用
  - AI事業者その他関連する事業者との連携

■ FSB・SSBs：

- 情報・知見・好事例の共有に資するクロスボーダー協力の促進。
- 実行可能な範囲での分類法や指標の整合性の向上。
- 継続的なAIの進展のモニタリング、及び残るデータギャップへの対応。

FSB「金融セクターにおけるAI導入と関連する脆弱性の監視」（2025年10月）②

“Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector”

脆弱性監視のためのモニタリング指標

AI導入	• 金融セクターにおける**AIユースケースのインベントリ**（金融活動（取引、貸付、保険、決済など）、**AIの種類**（生成型、エージェント型など）、**重要度**（コアビジネスライン、重要業務、低リスクの内部プロセスなど）） • ユースケース及び**AIモデルの種類並びに金融機関の規模別に見たAIを利用する金融機関の割合** • 金融機関の類型別に見た**AI導入パターンに関する定性データ**（業界アウトリーチや公開情報から得られる定性指標） • 直接的なデータ収集が困難な場合に利用可能な代理指標 – 金融機関の**AI関連特許出願** – 金融機関内の**AI関連職種の動向** – AI投資の代理指標としての**技術・研究開発（R&D）支出**
サードパーティへの依存とサービスプロバイダーの集中	• 金融機関が利用するAIアプリケーションのうち、**サードパーティが提供するものの割合** • サードパーティAIサービスプロバイダーが提供するサービスに影響を与える**重大なサイバー・運用インシデントの当局への通知** • 金融機関から収集したデータ・情報に基づく、**重要なAIサービスとサービスプロバイダーの登録簿** • 単一または密接に関連する**AIサービスプロバイダーが支援する重要なAIサービスの数** • サードパーティのAIサービスが重要な業務を支援する、**グローバルまたは国内のシステム上重要な金融機関の数** • 広く使用されるAIサービスの**相対的なコストとパフォーマンス**
市場相関	• 広く使用される**事前学習済みモデル**、**その特徴（モデル分類等）**、及び/または**学習データソースのそれぞれを利用する金融機関の数** • **特定のユースケースにおけるAI導入と、資産価格のボラティリティまたは資本市場の各セグメントにおける相関**との関連性を示す分析指標 • 主要市場におけるAIモデルの自律性の程度に関する情報（AIによる**自動取引戦略、与信判断及び資産配分に関する市場慣行や動向**）
サイバー	• 金融セクターを標的とするAIに関連する**サイバー攻撃の件数** • AIに関連する**内部でのサイバーインシデントの件数** • **サードパーティにおけるAIに関連するインシデントの件数** • **サイバー防御のためのAIユースケース**
モデルリスク・データ品質・ガバナンス	• 金融機関のモデルインベントリにおける**AIモデルの割合** • **AIモデル・リスク管理及びガバナンスに関する監督上の指摘事項の動向** • AIシステムにおける**自動意思決定の程度**（ヒューマン・イン・ザ・ループの活用状況）
AI主導の金融詐欺と偽情報	• **AI主導の金融詐欺の件数**（ディープフェイク、合成アイデンティティ、不正請求など） • **偽情報キャンペーン**（AIが生成した偽情報の拡散状況及び市場の安定性への潜在的影響） • AI関連の詐欺及び偽情報に関連する**顧客からの苦情**の報告

IMF「AIエージェントがもたらす決済の変革」（2026年4月）
“How Agentic AI Will Reshape Payments”

- 国際通貨基金（IMF）は、2026年4月23日に、エージェンティックAIが決済システムに与える影響を整理したIMF Noteを公表。決済の起点が“click-to-pay”（人間による明示的指図）から“decide-to-pay”（AIエージェントを介した意思決定）へと移行しつつあるとの問題意識のもと、確率論的推論を行うAIエージェントの判断と決定論的な要件を持つ決済インフラを両立させるため、3層の機能分離を含む論点を提示。

AIエージェント決済の3層モデル

■ 決済プロセスを3層で整理する概念的フレームワークを提示。AIエージェントによる確率論的な判断と、決定論的な承認・決済実行を機能分離する設計の重要性を示すとともに、当面はLayer1及びLayer2を中心にAIエージェントの利活用が進展すると整理。

Layer 1	意図形成・オーケストレーション	AIエージェントが利用者の目的や制約を解釈し、検索・比較・交渉・計画立案・マルチステップの調整を行う層。
Layer 2	統制・承認	委任条件、本人真正性、上限金額、利用条件、AML/CFT、制裁スクリーニング等に基づき、承認可否を決定論的ルールで判断する層。
Layer 3	決済・ファイナリティ	RTGS（即時グロス決済）、カードネットワーク、即時決済網、CBDC（中央銀行デジタル通貨）、DLT（分散型台帳技術）等において、最終的な実行と法的ファイナリティを担う層。

AIエージェント決済に伴うリスク

指図ギャップ	利用者による広範な委任やAIエージェントによる個別指図を伴わない決済実行による意図しない支払の発生
判断の不透明性	説明・検証が困難なモデル設計や決済フローへのAIの組込みによる、意思決定の検証困難化
高速な支払実行	高速での支払実行最適化や決済事業者の取引速度・流量制御の不足による、エラーの急速な拡大と取消不能な資金流出の発生
承認プロセスの追跡困難化	十分な監査可能性を欠く委任ベースの承認への依存による、利用者の意図や同意の証明困難化
取引責任の不明確化	利用者・決済事業者・決済システム運営者がAIの自律的判断を前提としない旧来の責任枠組みに依拠することによる、不正・誤決済時の損失負担の不明確化
サービス提供者の責任範囲	AIモデルやプラットフォーム提供者の欠陥・自律的挙動に対する契約・規制上の責任枠組みが不明確であることによる、責任の所在の曖昧化
行動の同調	AIエージェントの行動が同調することによる、市場ボラティリティの増幅
流動性ストレス・決済混雑	AIエージェントの決済・流動性の最適化や決済事業者の制約不備による、日中流動性需要の増加及び決済経路の混雑を通じた決済システムの能力・効率性の低下
サイバーセキュリティリスク	外部ツール及びAPIとの連携拡大や不十分なアクセス制御・ガバナンスによる、認証情報の窃取や不正な決済指図の誘発
ファイナリティを伴わないDLT決済	法令上・制度上の決済ファイナリティが明確に認められていないDLT基盤の導入による、決済の取消・巻戻しの発生
規制上の盲点	技術変化に対する規制枠組みの遅れやKYA（Know Your Agent）・越境プラットフォームへの監督欠如

IOSCO「資本市場におけるAI利用に関する監督ツールキット」（2026年5月）
“Supervisory Toolkit for AI Use in Capital Markets”

- 証券監督者国際機構（IOSCO）は、2026年5月25日に、「資本市場におけるAI利用に関する監督ツールキット」の最終報告書を公表。規制当局に対して、事業者が使用するAIシステムの監督を支援するための実践的なツールキットを提示。

ガバナンス及びリスク管理

取締役会または統治機関による監督	• 取締役会はAI利用の戦略目標とリスク選好を設定し、AIに関する方針・手続を定めているか。AIシステムについて定期的な経営情報の報告を受けているか。
上級管理職の責任	• 上級管理職はAI関連のガバナンス、リスク管理方針、手続を有効に実施し、その有効性を定期的にレビューする責任を負っているか。
AIリスク管理の枠組み、方針及び手続	• AIリスク管理枠組みを実施し、ハルシネーション、説明可能性・透明性、利益相反、バイアス等の主なリスク要因を取り込んでいるか。 • 適切な人間による監督方法と介入基準を定め、自動化バイアスを防いでいるか。end to endのライフサイクル統制を運用しているか。
データ・ガバナンス	• AIが利用するデータが目的に照らして正確性、完全性、代表性、適時性かつ関連性を有することを確保しているか。 • AI利用において適切なデータ収集、準備及び保守を行っているか。
高度なAIシステムのリスク管理	• 特にリスクが高いAIシステムを明確化・理解し、リスクに応じて管理や監督を行っているか。
AIモデルの検証、テスト及び監視	• リスクの重要度に比例した評価・テストを行っているか。モデルドリフト、敵対的攻撃、データポイズニング、新たな規制要件等、変化するAI固有のリスクを特定・評価しているか。 • 利用目的・リスクに応じた公平性指標を設定し、AIのライフサイクルを通じて差別的な結果を監視しているか。
AIシステムの統制及び人間による監督	• 人間・AIの役割分担及びAIシステムの監督に関する役割や責任を定義・区別する方針や手続があるか。
研修及びAIリテラシー	• 取締役会、上級管理職、開発者、検証者、フロント部門、コンプライアンス部門等に役割別研修を提供しAIリテラシー向上に努めているか。

記録保存及び報告

AIライフサイクル全体の管理に関する文書化	• 設計・計画、データ収集・処理、アーキテクチャ・モデル選択、構築、学習、テスト・検証、導入、運用、変更、監視、アルゴリズム、廃止計画等、全段階を包括的に文書化しているか。
AIに関する事業目的の文書化	• 期待便益、リスク、戦略整合性を含めAI導入の事業目的を明確に文書化しているか。
AI生成結果の文書化	• 投資者・市場に影響するユースケースのAI生成結果を保存しているか。
AI出力の説明可能性の文書化	• 意思決定の論理や推論を含め、AIが出力を生成する方法を説明する記録を保存しているか。
AIを利用する商品・サービスに関するインシデント記録	• インシデントにAI利用が含まれたかを記録・報告する方針・手続があるか。業務障害、不正行為、セキュリティ侵害、根本原因、是正措置の詳細記録を保持しているか。
報告	• 監督当局に対し、適切な頻度で適時かつ十分な報告を行っているか。

第三者及び外部委託リスク管理

リスクに応じた統制の評価	• 外部製品の採用、開発及び導入統制に関する方針・手続があり、リスク重要性に照らし十分か。 • 第三者AI製品・サービスのテストに自社データ・ユースケースを使っているか。第三者の更新・変更通知を受け、影響を評価する手続を含んでいるか。
透明性の確保	• 第三者のAI提供者による主要なリスクへの対応について、十分に情報が提供されているか。情報が不十分な場合、追加テストや人間による監督の強化等の補完措置を講じているか。
公平性に関するデューデリジェンス	• 第三者AIの利用により生じる結果の公平性について自社が引き続き責任を負うことを認識し、提供者による公平性確保の取組についてデューデリジェンスを実施しているか。
サプライチェーン・リスク評価	• 主要な第三者・オープンソースAIモデル、データセット、依存要素について、モデル来歴、学習データ完全性、既知脆弱性を含むサプライチェーン評価・検証を行っているか。
集中リスク	• 主要な外部サービス提供者への過度な依存に伴う集中リスクを評価しているか。共通インフラ・クラウド等の間接依存を考慮しているか。
コンティンジェンシープラン	• 特に高リスク用途について、第三者AIの障害、予期せぬ挙動、ベンダー支援終了に対応する強固な計画があるか。
法的枠組み及び説明責任	• 性能保証、データ保護、監査権、AI導入通知・事前同意等を含む契約により期待・責任を明確にしているか。
能力開発	• 第三者AIの調達、開発、導入、利用に関わる職員の認識・能力を高めているか。
複雑なAI製品の利用	• 利用実績の少ない、より複雑な外部のAI製品・サービスに対する評価を強化しているか。

開示

商品・サービスにおけるAI利用の顧客向け開示	• AIシステムの性能、限界及び適合性に関する重要情報を含め、AIシステムがどのように機能するかを明確に説明しているか。
AIガバナンス及び戦略の開示	• 取締役会・上級管理職の監督、ガバナンス・リスク管理枠組み、役割・責任を公表することとしているか。
開示及び同意	• 自社・第三者AIが顧客の権利、口座へのアクセスまたはプライバシーに影響する場合、顧客にその旨を知らせ、明示的な同意を得るかオプトアウトの機会を提供しているか。
誤解を招く表示・説明の特定	• 届出書類、報告書、広告、ウェブサイトまたはSNSにおけるAIに関する表示・説明が、不正確、虚偽、曖昧または誤解を招いていないか。 • 当該主張を公平かつ正確に裏付けられているか。

Europol「量子コンピューティングと暗号資産」（2026年10月）①
“Quantum Computing and Cryptocurrencies”

- 欧州刑事警察機構（Europol）は、2026年10月７日に「量子コンピューティングと暗号資産」を公表。量子コンピューティングが暗号資産に及ぼす影響について、ブロックチェーンの基盤となるハッシュ関数は量子攻撃に対して比較的高い耐性を有する一方、**公開鍵暗号を用いるウォレットでは秘密鍵の導出による資産流出リスク**があると指摘。その上で、**ウォレットのセキュリティ強化**、**耐量子計算機暗号への段階的な移行**、**分散型ネットワークにおける移行上の課題**及び**政策当局等に求められる対応**を整理。

■ 量子コンピューティングによる暗号技術への影響

現時点では、既存の公開鍵暗号を破るのに十分な性能と耐障害性を備えた量子コンピュータは存在せず、その実現時期にも不確実性がある一方、中長期的に実現する可能性があることを踏まえ、**暗号資産へのリスクを事前に評価し、移行に備える必要**がある。

ショアのアルゴリズム(注1)により、ウェブ通信（TLS）やブロックチェーン上の署名等の幅広い領域で用いられている**RSAや楕円曲線暗号などの公開鍵暗号が破られると、公開情報からの秘密鍵の導出、デジタル署名の偽造及び暗号化通信の解読が可能となる**おそれがある。

グローバーのアルゴリズム(注2)により、保存データや通信の保護に用いられる対称鍵暗号や、トランザクション・ブロックの識別、ブロック間の連結及びプルーフ・オブ・ワーク等に用いられるハッシュ関数への総当たり攻撃が高速化し、これらの暗号技術の安全性が低下する。一方で、公開鍵暗号とは異なり、鍵長又はハッシュ長の拡大によって影響を緩和することは可能である。

■ 暗号資産における主要なリスク

プルーフ・オブ・ワーク（PoW）及びプルーフ・オブ・ステーク（PoS）では、ブロックの連結や完全性の維持に関し、量子攻撃に対して比較的高い耐性を有するハッシュ関数が使用されており、量子コンピューティングによって直ちにブロックチェーン自体の完全性が損なわれるわけではない。

暗号資産の所有は秘密鍵によって管理され、取引については秘密鍵による署名と公開鍵による検証が行われるため、**十分な性能を持つ量子コンピュータによって公開鍵から秘密鍵を導出できるようになれば、攻撃者が正当な保有者の承認を得ずに資産を移転することが可能となる。**

分散型の暗号資産システムには、侵害された鍵を失効させ、又は耐量子計算機暗号への移行を強制する中央管理者が存在しないため、移行には開発者、マイナー、ノード運営者及び利用者等による合意形成が必要となる。このため、移行が適切に計画・実行されなければ、**量子攻撃に対して脆弱なウォレットが長期間にわたり残存する**おそれがある。

（注１）ショアのアルゴリズム：公開鍵暗号の安全性の基礎となる素因数分解問題及び離散対数問題を、量子コンピュータによって効率的に解くアルゴリズム。
（注２）グローバーのアルゴリズム： 共通鍵暗号や暗号学的ハッシュ関数に対する総当たり探索を、量子コンピュータによって高速化するアルゴリズム。

Europol「量子コンピューティングと暗号資産」（2026年10月）②
“Quantum Computing and Cryptocurrencies”

■ **主な対策**

1. **既存の仕組みを活用した段階的な対策**
   アカウント抽象化、スマートコントラクトウォレット、ゼロ知識証明及びアドレスの定期的な変更により公開鍵の露出を抑え、マルチシグを活用し単一の公開鍵への依存を軽減する。**既に公開鍵が露出しているウォレットを事後的に安全化する暗号学的な手段はないため、量子コンピュータによる攻撃が可能になる前に新しいウォレットへ資産を移転する必要**がある。

2. **耐量子計算機暗号への移行**
   米国国立標準技術研究所（NIST）が標準化したCRYSTALS-Kyber（鍵カプセル化）やCRYSTALS-Dilithium（デジタル署名）などの耐量子計算機暗号へ移行する。**耐量子計算機暗号は古典コンピュータ上で利用できるため、現時点で最も実現可能性の高い長期的対策**とされている。ただし、**従来方式より署名データが大きくなる**場合があり、ブロック容量、手数料、処理速度及びウォレットの互換性への影響が課題となる。

3. **量子技術を利用したセキュリティの強化**
   量子鍵配送（QKD）を利用すれば、理想的な条件下では、盗聴による量子状態の変化を検知する通信経路の構築は可能である。しかし、通信距離、費用、設備及び拡張性に制約があり、量子ブロックチェーンや量子暗号資産も現時点では実験段階にある。このため、短期から中期においては、量子技術そのものよりも、古典コンピュータ上で動作する耐量子計算機暗号への移行を優先すべきとしている。

■ **移行上の課題**

耐量子計算機暗号への移行には、プロトコルの変更とウォレットの更新が必要となり、既存のハードウェアウォレットが新たな仕様と互換性を持たない場合には、ハードウェアの更新も必要となる。特にビットコインでは、既存の未使用トランザクション出力（UTXO）も新たな方式へ移行する必要があり、そのためのトランザクションが通常の取引に利用可能なブロック容量や取引時間に影響を及ぼす。また、UTXOの量子リスクは台帳上の保存方法によって異なり、一時的な公開鍵が取引の承認まで露出する形式では、短時間で公開鍵から秘密鍵を導出して資産を奪う「ジャストインタイム量子攻撃」が想定される。

■ **政策提言**

- **量子コンピューティングの開発状況と技術的限界について、最新情報を継続的に提供**する。
- 耐量子計算機暗号及びその他の量子耐性を持つプロトコルへの移行に関する議論を優先し、**幅広い関係者と移行時期を検討**する。
- 欧州委員会を中心に、研究機関、民間企業、加盟国及び欧州連合（EU）関係機関が参加する共同作業部会を設置し、政策決定者向けの評価を定期的に作成する。
- 中央銀行デジタル通貨（CBDC）の開発状況とブロックチェーンの安全性への影響を監視し、量子コンピューティングに対する脆弱性を評価する。

■ **関係主体に求められる対応**

- 政策当局・規制当局：**耐量子計算機暗号の導入に関する明確な指針を策定**し、量子耐性を有する対策に関する**業界内の連携を促進**する。
- ブロックチェーンプロジェクト：**中核プロトコルへの耐量子計算機暗号の統合**を進め、ウォレット提供者が変更を実装するためのリソースを提供する。
- ウォレット提供者：耐量子計算機暗号に対応したウォレットの試験・導入を開始し、**量子耐性を有する暗号技術のリスクと利点を利用者に説明**する。
- 利用者：量子コンピューティングによる脅威の動向を把握し、**量子耐性を有するウォレットが利用可能になった段階で、資産を能動的に移行**する。

MAS「AIリスク管理に関するガイドライン」（2026年10月）
“Guidelines on Artificial Intelligence Risk Management”

- シンガポール金融管理局（MAS）は、2026年10月7日、金融機関による責任あるAIの導入を支援するため、「AIリスクに関する管理ガイドライン」を公表した。本ガイドラインは、2025年11月に公表されたガイドライン案への市中協議を踏まえ、**AIリスク管理に関する監督上の期待**を最終化したものであり、2027年10月から段階的に適用される。
- 金融機関に対して、**AIリスクに関する明確な責任及び監督態勢の確立**、**AIライフサイクル全体を通じたリスク管理**、**第三者AIの利用に伴うリスク管理**等を、**リスクに応じた比例的な方法**で実施することを求める。
- また、MASは、**AIエージェントについて、2027年に追加的なガイダンスの必要性に関する意見募集を金融機関等を対象に実施する予定**である。

■ ガイドライン本文は、第1節「導入」、第2節「適用」、第3節「AIの監督」、第4節「主要なAIリスク管理システム・方針・手順」、第5節「AIライフサイクル管理」、及び第6節「AIに関する能力・体制」の計6節で構成される（第4～6節の小項目については右図参照）。

■ これに対し、プレスリリースは主要な期待を以下の4点に整理。

✓ 監督体制の強化と責任の明確化
取締役会はAI利用の方針、管理枠組み及びリスク許容度を定め、上級経営陣はその実施、責任分担及び必要な資源の確保を担う。

✓ AIライフサイクル全体を通じたリスク管理
AI利用の特定、整備及びリスク評価を行い、開発・導入時にはデータ管理、人的監督、試験及び独立したレビュー等を実施する。導入後も継続的な監視、再検証及び変更管理を行い、必要な人材・技術基盤を整備する。

✓ 第三者AIの利用に伴うリスク管理
第三者が提供するAIについても、利用する金融機関が責任を負う。利用場面に即した検証や追加試験等を行い、残余リスクが許容範囲に収まらない場合は、利用の制限・停止又は提供者の変更を検討する。

✓ リスクに応じた比例的な適用
管理の範囲と厳格さは、AI利用の影響、複雑性、依存度及び自律性等に応じて調整する。低リスクの用途においても、責任者の明確化、利用ルールの策定、職員教育及び定期的な見直し等、一定の管理措置が求められる。

第4節　主要なAIリスク管理の体制・方針・手続
AIの特定（組織内で利用されているAIを一貫した基準により特定）
AIインベントリ
AIリスクの重要度評価（業務の性質及びモデルから生じるリスクに基づき評価）
第5節　AIライフサイクルの管理策
データ管理
透明性と説明可能性
公正性
人による監督
第三者AIの管理
選定（ファインチューニングなどの技法も含まれる）
評価とテスト
技術リスクとサイバーセキュリティリスク
再現可能性と監査可能性（AIの開発プロセス全体の文書化）
導入前レビュー
導入後のモニタリングとレビュー
変更管理（運用中のAIに対する変更の管理）
第6節　AIの利用に必要な能力と体制
AIリスク管理能力（AIに関わる人材の知識・技能を確保し、資源を配分）
AIの技術基盤（AIの安定的な利用に必要なシステムや計算資源を整備）

FSB「AIの責任ある導入に関する健全な実務慣行に係る報告書」（2026年10月）①

“Sound Practices for Responsible Adoption of Artificial Intelligence (AI): Final report”

- 金融安定理事会（FSB）は、2026年10月15日、当局が金融機関による責任あるAI導入を促進するため、**健全な実務慣行に係るツールキットを提供**することを目的とし、**「AIの責任ある導入に関する健全な実務慣行に係る報告書」**を公表。
- 報告書では、金融機関による責任あるAI導入を促進するため、組織全体のAIガバナンスや、AIライフサイクルにおける包括的なリスク管理枠組みに関して、**12の健全な実務慣行（Sound Practices）を提示**している。

組織全体のAIガバナンス

1. **戦略的な方針と監督**：取締役会及び上級管理職は、AIの導入及びガバナンスが、金融機関のビジネスモデル、リスクアペタイト及び戦略と整合していることを確保。
2. **ガバナンス及び説明責任**：責任あるAI導入を可能とするガバナンスモデルを選択し、明確な役割や責任を指定。
3. **リスク管理枠組みへのAI統合とAI利用に係る効果的な文書化**：AIリスクに効果的に対応可能なリスク管理枠組みを採用するとともに、AI利用・重要性及びリスク評価に係る文書化プロセスをリスク管理枠組みに組み込む。
4. **組織の適応力**：AIの進化に合わせて、監督体制、ガバナンス、リスク管理の実務及び組織能力を継続的に見直し、適応・改善する。

AIライフサイクルにおけるリスク管理

5. **重要性とリスク評価**：AIユースケースの企画・導入段階から継続的に、その重要性とリスクを体系的に評価。
6. **選定プロセス**：AIモデル又はシステムを選定する際、業務上の目的・運用上・技術上の要件や、AIユースケースの重要性・リスクを考慮。
7. **データガバナンス**：AIの学習、テスト、及び利用に用いるデータが目的に適合したものとなるよう、適切なデータガバナンスを確立。
8. **説明可能性と透明性**：適切かつ実行可能な場合には、より説明可能性の高いAIを採用、又は代替的な統制措置を検討。また、ステークホルダーごとのニーズに応じた適切な透明性を確保。
9. **パフォーマンス管理**：AIユースケースの重要性・リスクに応じて、パフォーマンスを評価し、導入後も継続的にモニタリングを実施。
10. **人による監督**：AIユースケースの重要性、リスク、自律性、複雑性、説明可能性に応じ、適切かつ効果的に人による監督を実施。
11. **サイバー・ICTリスク管理**：AIに関連するサイバー・ICTリスクを管理。必要に応じて、リスクシナリオのテスト等への組込み、関連情報の共有、またAIツールの活用を実施。
12. **サードパーティAIリスク管理**：パフォーマンス、透明性、データ品質、サプライチェーンリスク、集中リスク及び事業継続性に重点を置き、AIに関する第三者依存に伴うリスクを適切に管理。

FSB「AIの責任ある導入に関する健全な実務慣行に係る報告書」（2026年10月）②

“Sound Practices for Responsible Adoption of Artificial Intelligence (AI): Final report”

主なケーススタディ

	実務慣行	課題	対応策
AI戦略に対応した人材・能力開発	1. 戦略的な方針と監督	• AIの活用による価値を測定するための適切な指標の設定。	• 生産性向上、コスト削減及び職員能力向上等について具体的な目標の設定。 • 取締役・上級管理職向け研修や職員向けAIリテラシー向上施策の実施。
官民連携を通じたAIリスク管理手法の整備	4. 組織の適応力	• AI技術、関連リスク及び監督上の期待が急速に変化するため、**一金融機関の知見だけでは対応が困難**。	• 官民コンソーシアム及び規制サンドボックスを通じて、AIの機会とリスクを把握し、**実務指針の策定及び監督上の知見の蓄積**を実施。
リテール融資における機械学習	8. 説明可能性と透明性	• AIが利用する変数が、消費者向けの融資判断で使用が禁止されている属性と相関し、**融資判断に差別その他のバイアスをもたらす**可能性。	• 使用が禁止されている属性との相関が認められた特徴量は、それ自体の使用が禁止されていない場合でも、データセットから除外。
保険金請求処理におけるLLM（大規模言語モデル）	8. 説明可能性と透明性	• 大規模言語モデルによるハルシネーションの発生原因及び抑制方法の特定。	• 既存の保険情報を用いた**検索拡張生成（RAG）の導入**。
保険金請求処理におけるAIエージェント	10. 人による監督	• 試験中のAIエージェントによる、権限のないデータベースやシステムへのアクセス及び**データファイルの削除**。	• 権限付与及びアクセス管理の強化。 • 人によるログの抜取り確認。

HKMA「人工知能の責任ある導入」（2026年10月）
“Responsible Adoption of Artificial Intelligence”

- 香港金融管理局（HKMA）は、2026年10月15日、金融機関による責任あるAI導入を促進するための枠組みとして、「人工知能の責任ある導入に関する監督ガイダンス」を改訂。責任あるAI導入に重要な3つの要素として、**説明責任（Accountability）**、**強靭性（Resilience）**、**信頼（Trust）**を提示（頭文字を合わせて“ART”）。
- また、生成AIサンドボックス（第2期）から得られた実務的知見や好事例をまとめた報告書、及びエージェント型AIの発展を見据えたガバナンス体制に関する予備的な検討事項を示した「エージェント型AIのガバナンスに関するコンセプトノート」も公表。

監督上の期待

A. 説明責任（Accountability）

1. 取締役会及び上級管理職は、効果的な戦略及びガバナンス態勢を定めることを通じて、AI導入について説明責任を負う。
2. 導入する各ユースケースに責任者を割り当て、AIが生成した結果に対する効果的な人間の監督を確保する。
3. 導入が承認されたAIユースケースの最新の台帳を維持し、台帳に含まれないソリューションの利用を制限する。

R. 強靭性（Resilience）

4. ユースケースの重要性及びリスクに見合った方法でAIの導入を管理する。
5. 効果的なリスク管理フレームワークを導入し、AIの特定のニーズに対応する。
6. AIユースケースを安全かつ責任ある方法で継続的に提供するため、人材を含む十分な資源及び専門性を確保する。

T. 信頼（Trust）

7. AIが生成した出力（行動も含む）について、出力内容の品質を保証し、説明する責任を負う。
8. AIユースケースについて、社内外の関係者に対して適切な説明可能性及び透明性を確保する。
9. AI導入が倫理的であり、顧客を公正に取り扱うことを確保する。

エージェント型AIのガバナンスに関する予備的な検討事項

(a) 意図に基づく説明責任

AIエージェントの行為は、与えられた指示やビジネス目標についての当該エージェントの解釈によって駆動されるため、ガバナンス態勢において、**エージェントの行為と、その基礎となるビジネス上の意図との明確なつながりを確立する必要**が生じ得る。

(b) 重要なAIエージェントの可視性

効果的なガバナンスは、エージェント型AIシステムについて**十分な可視性が確保されている**ことに依存する。これは、重要なビジネス機能を遂行するエージェント、高度な自律性を有するエージェント、機微データや重要なシステムにアクセスできるエージェントにとって、特に重要となり得る。金融機関が導入した**重要なAIエージェントについて、業界レベルの登録制度を設ける可能性**についても検討する。

(c) 人間による監視と介入

エージェント型AIは高速で行動し、相互に関連する行為を実行する場合があるため、**適切な監視及び人間による監督の重要性**を浮き彫りにする。監督の水準は、エージェントが実施する活動の性質や潜在的な影響によって異なり得る。そのアプローチは、「human in the loop」から「human on the loop」へと移行しつつある。

(d) 運用上の境界と安全対策

AIエージェントは、許可されたツール、システム、データ等の**明確に定められた境界の中で動作すべき**である。明確な運用上の境界は、エージェント型AIの利用における顧客及び社会の信頼を維持するために不可欠である。

CFTC Frontier Forum（2026年10月）

- 米商品先物取引委員会（CFTC）のMichael S. Selig委員長は、2026年10月28日、Frontier Forumの冒頭挨拶において、「スーパーインテリジェンス（SI）」及びSIエージェントがデリバティブ市場に与える機会及び課題並びに規制・監督の方向性について言及した。**AIによるリスク管理や市場監視の高度化が期待される**一方、相関した取引行動及び取引の高速化並びに**SIエージェントの規制上の位置付け及び責任の所在が課題になる**と指摘した。

金融市場への影響

■ **機会**

- 大量の市場情報を迅速かつ正確に処理し、高度な分析に要する費用を低下させることにより、**投資判断及びリスク管理の高度化**並びに**小規模な市場参加者への利用拡大**に寄与する可能性。
- 高度な分析に要する費用を低下させ、**小規模な市場参加者による高度な分析・リスク管理手法の利用を促進**する可能性。
- 市場価格を左右する情報や異なる市場の相互関係の把握を通じて、**価格発見機能を向上**させる可能性。
- 取引所による不審な取引の特定、清算機関による損失リスクの監視及び規制当局による不正行為の検知を高度化する可能性。

■ **課題**

- SIエージェントが**市場環境に対して想定外の反応を示す**可能性。
- 類似するモデルを利用するシステムが、**相関した取引行動を生じさせる**可能性。
- 自律的な取引の高速化により、**市場監視及びリスク管理が困難となる**可能性。
- SIエージェントが利用者に代わって取引を行う場合、**開発者に対する規制適用、問題発生時の責任及び取引の帰属主体が不明確となる**可能性。

規制・監督の方向性

- SIエージェントへの規制の適用について、**当該エージェントが果たす機能**、**支配の主体**及び**取引の経済的実態**を踏まえて判断。
- SIエージェントが誰のために取引を行っているかを確認するため、顧客確認（KYC）に相当する**「Know Your Agent（KYA）」の必要性**を提起。
- 技術革新を促進しつつ、市場の競争力、公正性及び強靱性を確保する観点から、**SI及び自律的な取引の進展を踏まえて規制の在り方**を検討。

OCC「銀行によるスーパーインテリジェンスの利用に関する監督フレームワーク」（2026年11月）①
“OCC Supervisory Framework on Bank Use of Super Intelligence”

- 米国通貨監督庁（OCC）は、2026年11月４日、「スーパーインテリジェンス（SI）」及び自律的に行動する「エージェント型SI」の銀行による利用について、**リスクベースで評価するための監督上の枠組み**を公表。
- SIが既存のオペレーショナル・リスク、コンプライアンス・リスク及び信用リスク等に及ぼす影響を、**銀行の既存のリスク管理態勢の中で管理する考え方**を採用し、**事後的な是正の可否、自律性並びに顧客、金融機関及び市場への影響**を踏まえ、リスクに応じた管理策を講じる考え方を示している。

6本の柱と16の構成要素

■ 既存のリスク管理態勢の中でSIの利用に伴うリスクを管理するため、**主要な監督上の考慮事項**として、**6本の柱**と、これらに対応する**16の構成要素**からなるフレームワークを提示。

■ 技術や利用事例の進展及び監督上の理解の深化に応じて**継続的に見直される「生きた文書」と位置付け。**

柱	定義	構成要素
目的（Purpose）	SIシステム（エージェント）に実行を許可する行為を定める	• 目的及び利用範囲の明確な定義
リスク（Risk）	SIシステム（エージェント）による出力・行為が目的に適合しない場合の影響を評価する。	• リスク分類及び重要度評価
統制（Control）	SIシステム（エージェント）による権限のない行為、不適切な行為または安全でない行為を防止するための統制を特定する。	• Human-in-the-Loop / Human-on-the-Loopによる統制 • モデル・リスク管理の拡張的適用 • データガバナンス • プライバシー • コンプライアンス・法令遵守 • サイバーセキュリティ
管理・監視（Oversight）	SIシステム（エージェント）を監視する主体と、その利用について説明責任を負う主体を定める。	• Human-in-the-Loop / Human-on-the-Loopによる統制 • ガバナンス・説明責任 性能の継続的モニタリング • 報告・透明性
レジリエンス（Resilience）	重要な業務プロセスを継続しながら、SIシステム（エージェント）の障害検知、封じ込め、復旧及び是正を行うための銀行の態勢を対象とする。	• オペレーショナル・レジリエンス • サイバーセキュリティ
保証（Assurance）	SIシステム（エージェント）に対する統制が継続的に有効に機能していることを示す証拠を提供する。	• サードパーティーリスク • テスト • 文書化・監査可能性 • 内部監査・独立した立場からの検証

サイバーセキュリティ

キーコンセプト

- 6つの柱のうち、「統制（Control）」と「レジリエンス（Resilience）」の双方に位置づけられた構成要素。
- SIシステムは、**サイバー攻撃の標的**となるだけでなく、**攻撃の速度、規模又は手法の高度化を助長する手段として悪用**される可能性があることを踏まえ、サイバーセキュリティ管理の対象を、**SIシステムのライフサイクル全体とその基盤にまで広げる**ことが考えられる。

検討事項

- プロンプトインジェクション・ジェイルブレイク

  悪意のある入力や誤解を招く入力により、従来型のネットワーク侵入を伴わずに、**システムの動作が変更**されたり、制限が回避されたり、**SIエージェントが接続先のツールを不正に使用**したりする可能性。
- データポイズニング・モデルポイズニング

  学習、ファインチューニング、検証済み情報源又はフィードバックに用いるデータが改ざんされることにより、導入後には検知が困難な**望ましくない動作がモデルに組み込まれる**可能性。
- モデル抽出・データ漏えい

  反復的な照会や悪意のある入力を通じて、**モデルの動作が推測**されたり、**学習データに含まれる機微情報や機密情報が取得**される可能性。
- ツールの利用及び過度な権限付与

  SIエージェントに広範な認証情報や権限を付与した場合、外部から不正に操作されることにより、**不適切な処理が高速かつ連続的に実行**される可能性。
- SIエージェントのID及び利用管理

  SIエージェントのID、認証情報、操作記録及びデータ利用を**高度なアクセス権限を持つユーザーに準じて厳格に管理**。