欧州の証券監督当局が注視する証券市場における AI リスク
－ESMA による調査分析結果と今後のリスク対応の論点－

江夏　あかね

▌要　約▐

1. 人工知能（AI）が世界で急速に発展・普及が進む中、各国・地域の証券監督当局が証券市場における AI の潜在的なリスクへの対応を進めている。2023 年に入って、（1）欧州連合（EU）では、欧州証券市場監督局（ESMA）が 2 月に EU の証券市場の AI リスクに関する調査分析結果、（2）米国では、米国証券取引委員会（SEC）が 7 月にブローカー・ディーラー等に対して、AI 等の予測データ分析を利用する際に生じ得る利益相反への対応を義務付ける規則案、をそれぞれ公表した。
2. ESMA による EU の証券市場の AI リスクに関する調査分析結果では、証券市場参加者や各取引プロセスの観点から AI の利用状況を調査し、5 つの潜在リスク（説明可能性、集中・相互連関・システミックリスク、アルゴリズム・バイアス、オペレーショナル・リスク及びデータの質とモデル・リスク）を特定した。ただし、「AI の開発を監視し、関連する重大なリスクを分析した上で、これらが十分に理解され、考慮されるようにする」として、厳格な規制の導入といった結論は導き出さなかった。
3. 世界の証券市場で今後、ますます AI 利用が進んでいくと想定される中、証券市場における AI リスクへの対応をめぐる主な論点としては、（1）各国・地域における証券監督当局や国際組織等による取り組み、（2）リスク管理・ガバナンス体制の拡充、が挙げられる。
4. 特に、リスク管理・ガバナンス体制は、AI リスク対応に向けて新たな仕組みを構築するより、既存の体制を継続的に見直し、AI の利活用にも耐えうるような形に拡充していくことが多いと推察される。

野村資本市場研究所　関連論文等

・橋口達「予測データ分析や AI の利活用に関する規制強化を図る米国 SEC 規則案―金融事業者と投資家間の利益相反への対応―」『野村資本市場クォータリー』第 27 巻第 2 号（2023 年秋号）。
・関雄太・佐藤広大・ラクマン ベディ グンタ「機械学習型人工知能とビッグデータの結合がもたらす金融サービス業の変化」『野村資本市場クォータリー』第 19 巻第 4 号（2016 年春号）。
・佐藤広大「人工知能・ビッグデータを活用した資産運用への期待と課題」『野村資本市場クォータリー』第 20 巻第 4 号（2017 年春号）。

Ⅰ 証券市場で利用が進む AI と潜在的なリスクへの着目

人工知能（AI）[1]は近年、ビックデータの発展、データストレージ容量の増加、計算機の処理能力向上等を背景に、世界で急速に発展・普及が進んでいる。金融資本市場にとっても、AI の導入は、コスト削減、生産性向上、顧客に提供するサービスや商品の質の向上や多様化等のメリットが期待される[2]。そのような中、（1）ポートフォリオ・マネージャーの約 3 割がアルゴリズム取引[3]に何らかの AI 技術を、約 1 割が投資戦略に機械学習（ML）[4]を利用、（2）世界の金融機関の約 8 割が、AI が短期的に金融サービス業界全体で不可欠なビジネスドライバーになるとみている、などのサーベイ調査結果[5]が示唆するように、存在感が高まっているところである。

一方で、証券市場における AI のリスクが顕在化する事例も出現している。例えば、2023 年 5 月に AI が米国国防総省の近くで大きな黒煙が上がっていることを示す偽造画像を生成し、ソーシャルメディア上で拡散されたことを背景に、ニューヨーク株式市場のダウ平均株価が一時的に 100 ドル以上下落する等の混乱を招いたとの報道[6]があったことは記憶に新しい。

このような状況下、証券監督者国際機構（IOSCO）が 2021 年 9 月に市場仲介者及び資産運用会社による AI 及び ML の利用を証券監督当局が規制監督する際に役立つガイダンス[7]（後掲図表 5）を公表したことも後押しする形で、各国・地域の当局が証券市場における AI の潜在的なリスクへの対応を進めている。2023 年に入って、（1）欧州連合（EU）では、欧州証券市場監督局（ESMA）が 2 月に EU の証券市場の AI リスクに関する調査分析結果、（2）米国では、米国証券取引委員会（SEC）が 7 月にブローカー・ディーラーと投資顧問に対して、AI 等の予測データ分析[8]を利用する際に生じ得る利益相反への対応

---

1 AI に関する確立された定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている。（総務省「令和元年版　情報通信白書」2019 年 7 月）

2 Organisation for Economic Co-operation and Development, “AI in Business and Finance,” OECD Business and Finance Outlook 2021, September 24, 2021.

3 アルゴリズム取引は、コンピューターシステムが株価や出来高などに応じて、自動的に株式売買注文のタイミングや数量を決めて注文を繰り返す取引。

4 ML は、コンピュータ（機械）がデータから自動で学習し、データの背景にあるルールやパターンを発見する方法。

5 CFA Institute, “AI Pioneers in Investment Management” 2019; Cambridge Center for Alternative Finance and World Economic Forum, “Transforming Paradigm: A Global AI in Financial Services Survey,” January 2020.

6 「“米国防総省近くで爆発”　偽画像拡散 株価一時下落する騒動に」『日本放送協会』2023 年 5 月 23 日、「米国防総省付近で爆発との AI 偽造画像が拡散、米株下げる場面も」『ブルームバーグ』2023 年 5 月 23 日。

7 International Organization of Securities Commission, “The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers: Final Report.” September 2021.

8 予測データ分析は、大規模なデータセットから推論を引き出し、仮説のないデータマイニングと帰納的推論に依拠してパターンを発見し、将来の結果を予測するもの。（U.S. Securities and Exchange Commission, “17 CFR Parts 240 and 275 [Release Nos. 34-97990; IA-6353; File No. S7-12-23] RIN 3235-AN00; 3235-AN14 Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker Dealers and Investment Advisers,” July 26, 2023）

を義務付ける規則案[9]（後掲図表 6）、をそれぞれ公表した[10]。

本稿では、欧州のESMAによる調査分析結果に焦点を当て、ポイントを考察した上で、証券市場における AI リスクへの対応に向けた今後の論点を考察する。

Ⅱ ESMA による EU 証券市場の AI リスクに関する調査分析結果

EU では、欧州委員会が 2020 年 9 月に採択した「デジタルファイナンス戦略」の優先事項として、金融セクターへの AI 導入促進を掲げる一方、2018 年頃より欧州監督機構（ESAs）[11]が AI の発展に伴う潜在的な影響について検討を進める等の動きが見られている（図表 1 参照）。そのような中、ESMA が 2023 年 2 月、「EU の証券市場における AI」と題した論文を公表した。

同論文は、（1）証券市場参加者による AI の利活用実態、（2）各取引プロセスにおける AI の利活用状況、（3）信用格付会社や議決権行使助言会社による AI の利活用状況、（4）AI 利活用に伴う潜在的なリスク、に関する調査・分析を行った上で、（5）ESMA として EU の証券市場における AI リスクに規制監督の観点からどのように対処するのかを検討した結果を示している。なお、同論文には、AI に関する基礎的な概念の説明も併せて示されている（図表 2 参照）。

図表 1　EU における金融市場の AI をめぐる主な動き

時期	詳細
2018 年 3 月	欧州監督機構（ESAs）の合同委員会、ビックデータに関する報告書を公表。AI とビックデータの発展可能性等に関する論点も提示
2020 年 9 月	欧州委員会、「デジタルファイナンス戦略」を採択。優先事項として、金融セクターへの AI 導入推進を掲げる
2021 年 4 月	欧州委員会、AI 規制法案を含む政策パッケージを公表
2021 年 6 月	欧州保険・企業年金監督機構（EIOPA）、欧州保険セクターを対象とした AI ガバナンス原則を公表
2021 年 11 月	欧州銀行監督機構（EBA）、内部格付手法（IRB）の機械学習に関するディスカッションペーパーを公表
2023 年 2 月	ESMA、「EU の証券市場における AI」と題した論文を公表
2023 年 6 月	欧州議会、AI 規制案を採択

（出所）European Securities and Markets Authority, “Artificial Intelligence in EU Securities Markets,” February 1, 2023、各種資料、より野村資本市場研究所作成

9　詳細については、橋口達「予測データ分析や AI の利活用に関する規制強化を図る米国 SEC 規則案―金融事業者と投資家間の利益相反への対応―」『野村資本市場クォータリー』第 27 巻第 2 号（2023 年秋号）、を参照されたい。

10　European Securities and Markets Authority, “Artificial Intelligence in EU Securities Markets,” February 1, 2023; U.S. Securities and Exchange Commission, “SEC Proposes New Requirements to Address Risks to Investors from Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers,” July 26, 2023.

11　ESAs には、欧州銀行監督機構（EBA）、ESMA 及び欧州保険・年金監督機構（EIOPA）が含まれる。

図表 2　ESMA による AI に関する基礎的な概念の説明（抜粋）

概念	説明
AI	対話する環境に影響を与えるコンテンツ、予測、推奨事項、決定等の出力を生成できるソフトウェア(注 1)
ML	アルゴリズムと統計モデルを利用してデータのパターンを分析し、推論を引き出すことで、明示的な指示に従わずに学習し、適応できるシステム
自然言語処理(NLP)	テキストや話し言葉を処理し、その意味を理解する AI の一分野
教師あり学習	ラベル付けされたデータでトレーニングされる ML モデル。以前の入力データと以前の結果（ラベルを表す）の両方から学習し、ラベルのない新しい入力データに基づいて結果を予測する
教師なし学習	ラベルのない入力に対してのみトレーニングされる ML モデル。アルゴリズムは同様の特性に基づいてクラスター（集合体）を形成する。アルゴリズムは、トレーニングデータにラベルを付けるための事前の人間の介入なしにデータを分類する
強化学習	ML の一種であり、モデルが報酬関数(注 2)を最大化する最適な方法を学習すること
ディープラーニング	複数の層からなるニューラルネットワーク(注 3)に基づく ML 手法。ディープラーニングは、教師あり学習、教師なし学習、または強化学習タスクに適用可能

（注）　1. 本説明は、欧州委員会が 2021 年 4 月に公表した AI 規制法案に基づく。
2. 本論文には、報酬関数に関する説明はないが、一般的に良い結果につながるアクションを実行した際に、正のフィードバックとして報酬を提供する関数を指す。
3. 本論文には、ニューラルネットワークに関する説明はないが、一般的に人間の脳の神経回路の構造を数学的に表現する手法を指す。

（出所）European Securities and Markets Authority, “Artificial Intelligence in EU Securities Markets,” February 1, 2023、各種資料、より野村資本市場研究所作成

1．証券市場参加者による AI の利活用実態

本論文では、主な証券市場参加者として、資産運用会社、ロボアドバイザー[12]及びサービス提供者が取り上げられている。

資産運用会社が運用する EU 域内において販売可能とされる投資信託（UCITS）[13]のうち、投資戦略に明示的に AI の利活用を謳っている銘柄は 2021 年末時点で、本数全体の 0.2%未満、運用資産残高（AUM）全体の約 0.03%に留まっていると指摘された。資産運用会社における AI の利活用への関心は高い一方で、明示的に宣伝することに消極的である主な背景として、意思決定プロセスの限定的な部分のみでの利活用の実態、技術や知識の障壁のみならず、一部の顧客による AI のブラックボックス問題[14]への懸念が挙げられた。加えて、AI の利活用を公表しているファンドとそれ以外のファンドのパフォーマンスやコストに大きな差がなかったとの分析も示された（図表 3 参照）。

[12] 本論文で、ロボアドバイザーは、投資家のリスク選好度に合わせて最適なポーフォリオを作成するコンピュータープログラムで自動化されたポートフォリオ・マネージャーと定義付けられている。

[13] EU の譲渡可能証券の集団投資事業（UCITS）指令に準拠した投資信託。

[14] AI におけるブラックボックス問題について、ML では、膨大なデータの学習結果を用いた帰納的な処理過程を経て判定結果を得るため、どのようにしてその判定結果に至ったのかを明確に説明することが一般的に困難であることを指す。（新エネルギー・産業技術総合開発機構 産業技術総合開発機構 技術戦略研究センター（TSC）「人工知能分野の技術戦略策定に向けて―社会実装推進のために―」『TSC Foresight』第 114 号、2023 年 7 月）

図表 3　AI の利活用を公表しているファンドとそれ以外のファンドのパフォーマンス比較（%）

項目	AI の利活用を公表しているファンド	それ以外のファンド
リターン	0.30	0.26
アルファ	0.17	0.23
総経費率（TER）	1.33	1.43

（注）　リターンは 2019 年 11 月から 2022 年 10 月までの平均。アルファは、テクニカル指標ベンチマークを参照して月次で算出。TER は 2022 年 10 月の平均。

（出所）European Securities and Markets Authority, “Artificial Intelligence in EU Securities Markets,” February 1, 2023、より野村資本市場研究所作成

また、調査対象となった業界幹部らは、AI は現状で人間が監視しない限り自律的な意思決定を行うことはできないが、AI と人間の判断と組み合わせることで最良の結果が導き出されるとの期待をもって見ており、ソリューションの開発に向けて注力しているとの実態が紹介された。

ロボアドバイザーについては、大部分が投資ホライズン（投資期間）やリスク許容度といった顧客に関する情報に基づく比較的シンプルなアルゴリズム（データ処理手順）に基づき運営されているとされた。現状でロボアドバイザーが AI を駆使していない主な背景として、（1）個々の顧客の情報を拡充したアルゴリズムに基づいても伝統的なポートフォリオ理論に基づくパフォーマンスの改善が保証されるわけではないこと、（2）EU 一般データ保護規則（GDPR）[15]に基づき、顧客に影響を与え得るアルゴリズムの決定に関連するロジックについて顧客が問い合わせる権限が与えられており、対応が煩雑になる可能性があること、が挙げられた。

一方、サービスプロバイダーについては、機関投資家に対して、ポートフォリオ管理、リスク管理、コンプライアンス関連のサービスを提供する AI ネイティブのテクノロジー企業が出現している旨が紹介された。特に、コンプライアンス関連では、データの異常検知やファンド目論見書等の法的文書の自動作成といった機能を担っており、いわゆるレグテック[16]を将来的に変革させる可能性があると指摘された。

２．各取引プロセスにおける AI の利活用状況

本論文では、取引プロセスを（1）取引執行前、（2）取引執行時、（3）取引執行後に分けて、AI の利活用状況を紹介している（図表 4 参照）。

取引執行前について、投資家等が価格のシグナルを分析し、投資機会を特定する際に AI モデルを活用していると説明された。投資の意思決定と実施の両方を行うアルゴリズム取引戦略の一部となることもある。自己勘定取引を行う業者は、ML モデルを活用する

[15] EU 一般データ保護規則（GDPR）は、個人データやプライバシーの保護に関する規定であり、2018 年 5 月に施行された。詳細については、板津直孝「サステナビリティ課題としての個人データ保護」『野村サステナビリティクォータリー』第 1 巻第 2 号（2020 年夏号）、を参照されたい。

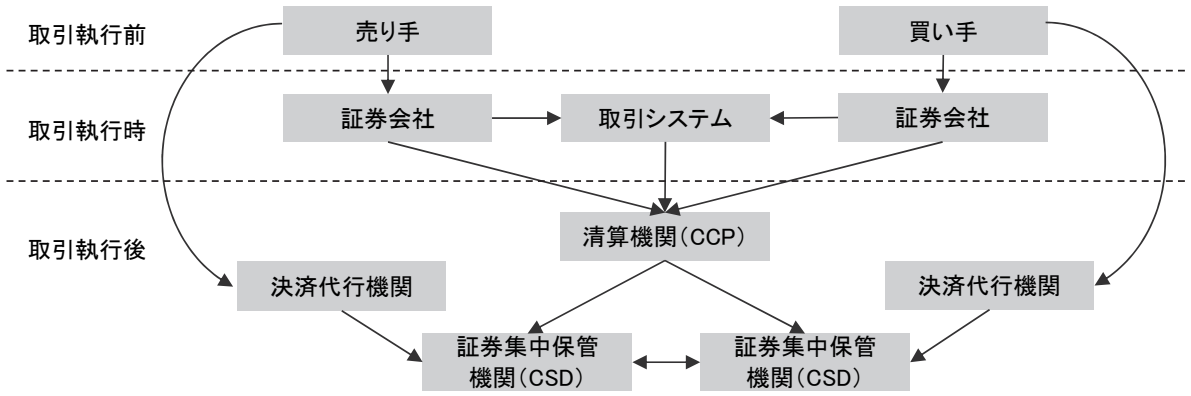
[16] レグテックは、規制とテクノロジーを合わせた造語で、AI、ビックデータ分析、ブロックチェーン等のテクノロジーを活用して、規制やコンプライアンスへの対応を効率的に行う仕組み。

ことが多いが、現状は教師あり学習（学習データに正解を与えた状態で学習させる手法）が主流で、強化学習（AI が試行錯誤しながら価値を最大化するような選択を学習する手法）については試行しているケースもあると紹介された。また、機会学習が活用されるアセットクラスは、株式、先物、外国為替といったタイムリーなデータが利用可能な流動性を有する金融商品が中心と説明された。

取引執行時について、一部の証券会社や大手バイサイド投資家等が、より良いメタオーダー[17]を実施すべく、異なる取引所、時間に最適に分割して実行する ML モデルを開発している旨が紹介された。この用途における ML モデルでは、強化学習が適しているとされた。その一方で、注文を実行する組織以外はデータを保有せず、限られた情報で訓練された ML モデルが開発されるため、モデルの有効性が確保できないといった課題も指摘された。

取引執行後については、一部の証券集中保管機関（CSD）やブローカーが、取引が決済されない可能性を予測し、証券を最適に配分するために ML モデルを活用していると紹介された。しかし、大部分の清算機関（CCP）や CSD は、AI を活用しても限られた付加価値しかないとの考えの下、AI を広く活用している状態ではないとも説明された。

図表 4　取引プロセスの構成



（出所）European Securities and Markets Authority, “Artificial Intelligence in EU Securities Markets,” February 1, 2023、より野村資本市場研究所作成

３．信用格付会社や議決権行使助言会社による AI の利活用状況

信用格付会社については、情報収集や信用格付評価等の一部で AI を利活用する傾向があるが、EU に拠点を置く信用格付会社全てが信用格付評価プロセスの自動化のために AI を導入することは当面ないとの意向を示した旨が紹介されている。加えて、多くの信用格付会社が AI の実装に関する規制がどのように導入されるか見通すことができないため、AI に大規模に投資する段階に至っていないと説明された。

[17] メタオーダーは、大規模な売買注文を小口に分割し、段階的に実行する手法。

一方、議決権行使助言会社では、機関投資家にリサーチやデータを提供したり、株主総会における投票に関する推奨を提供するために利用する情報を収集、合成、処理するために、AI を利活用しているとの実態が紹介された。

４．AI 利活用に伴う潜在的なリスク

本論文では、証券市場における AI 利活用に伴う潜在的なリスクとして、（1）説明可能性、（2）集中・相互連関・システミックリスク、（3）アルゴリズム・バイアス、（4）オペレーショナル・リスク、（5）データの質とモデル・リスク、が挙げられた。

１）説明可能性

説明可能性は、狭義にはアルゴリズムの動作を技術的かつ客観的に理解すること、広義には与えられた AI モデルが人間によって解釈・理解可能であることを指している。本論文では、AI モデルの説明可能性の欠如は、モデルのパフォーマンスやリスク管理に悪影響を及ぼす可能性があると説明された。

２）集中・相互連関・システミックリスク

AI システムの開発は資源集約的で、テクノロジー、データ、インフラ、人材に投資するための財務基盤を有する一部の大規模な資産運用会社に集中し得るとのリスクが取り上げられた。また、特定のサービス提供者が寡占している実態を踏まえ、集中リスクやシステム等の相互接続性のリスクがデジタル金融サービス部門に広範に及ぶ可能性があると指摘された。

一方、AI ツールの利用が少数のサービス提供者に集中することを通じて、アルゴリズム取引の文脈で、群集行動、投資戦略の収束、ショック時のボラティリティを悪化させる連鎖反応を誘発し、システミックリスクを引き起こす可能性があるとの説明も記された。

３）アルゴリズム・バイアス

アルゴリズム・バイアスは、一般的に偏りのあるデータを AI に学習させてしまうことで、公平性のない偏った結果を算出してしまうことを指す。本論文では、顧客の個人データの利用が融資や信用供与、消費者金融等のビジネスを担う銀行や保険のアプリケーションと比較して、資産運用や証券市場における AI モデルのアルゴリズムが差別的な結果につながるリスクは少ない可能性があると指摘している。その一方で、対象とする過去のデータの内容によっては、資産アロケーションモデルの結果を歪める可能性があり、最適でない結果をもたらしたり、金融市場の健全性を脅かすこともあり得ると説明された。

４）オペレーショナル・リスク

AI モデルを体系的に利用する場合、不適切な内部統制プロセスや、サイバーセキュリティリスクのような外部事象を通じて、オペレーショナル・リスクが高まる可能性があると説明されている。

５）データの質とモデル・リスク

IOSCO が 2021 年 9 月に公表したガイダンス（後掲図表 5 参照）にも取り上げられたように、学習段階で利用されるデータの質が AI や ML の成果とパフォーマンスに重大な影響を与え得ると記された。加えて、AI ツールの実効性は、データの質に大きく依存しており、質が悪くノイズが多いデータは信頼性の低いモデルを容易に生み出すと指摘された。

本論文では、これら 5 つのリスクをめぐり、さらに監視する必要があるとした上で、適切なガバナンスとプロセスの監視が、相応部分を軽減するのに効果的であることが証明される可能性があるとの考えが示された。

５．ESMA による AI リスクに対する規制監督のスタンス

ESMA は、今般の調査分析結果に基づき、「AI の開発を監視し、関連する重大なリスクを分析した上で、これらが十分に理解され、考慮されるようにする」と結論付け、本論文で厳格な規制の導入等は示さなかった。

その背景として、AI の利活用は増えているものの、技術的制約、顧客の選好、規制の不確実性等により、ビジネスプロセスの迅速かつ破壊的な見直しにつながっておらず、証券市場における AI の利活用に関するリスクは重要だが、現時点では限定的との見方を挙げた。ただし、（1）重要なビジネスや意思決定プロセスを大幅に高速化し、より複雑化し、透明性を低下させる可能性がある、（2）将来的に AI ベースのモデルが投資や取引で成功するようになれば、AI システムが少数の大手企業に集中するといったリスクが顕在化する可能性がある、（3）現状で AI や ML を実装している企業において、既存のガバナンスと監視体制に依存し、専門のコンプライアンス担当者を雇用していない傾向にある、といった懸念も示した。

その上で、ESMA は、AI 技術の提供者とエンドユーザー双方の説明責任及び責任を明確化する適切なガバナンスの枠組みが必要と指摘した。同時に、多くの市場参加者が依然として AI の利用に対して警戒感を抱いており、AI の効果的かつ信頼できる利用のための明確な枠組みが将来的に導入される見込みであることを歓迎しているとの実情も紹介された。

Ⅲ 今後の論点

ESMAによるEUの証券市場のAIリスクに関する調査分析結果では、証券市場参加者や各取引プロセスの観点からAIの利用状況を調査し、5つの潜在リスク（説明可能性、集中・相互連関・システミックリスク、アルゴリズム・バイアス、オペレーショナル・リスク及びデータの質とモデル・リスク）を特定した。ただし、「AIの開発を監視し、関連する重大なリスクを分析した上で、これらが十分に理解され、考慮されるようにする」として、厳格な規制の導入といった結論は導き出さなかった。

世界の証券市場で今後、ますますAIの利活用が進んでいくと想定される中、証券業界におけるAIリスクへの対応をめぐる主な論点としては、（1）各国・地域における証券監督当局や国際組織等による取り組み、（2）リスク管理・ガバナンス体制の拡充、が挙げられる。

1点目について、前述のSECが2023年7月に公表したブローカー・ディーラー等による予測データ分析の利用に伴う利益相反に関する規則案は、利益相反に焦点を当てた内容になっているが、例えば、前述のIOSCOによる2021年9月のガイダンスとほぼ同時期に、経済協力開発機構（OECD）や国際通貨基金（IMF）が金融分野におけるAI利用に関して、包括的なアプローチでリスクの特定や政策・規制の考慮事項等を提示している（図表5～図表8参照）。ESMA、IOSCO、OECD及びIMFが取り上げた潜在的なリスクは大部分で共通しているものの、例えば、IOSCOによるアウトソーシング、OECDによる雇用とスキル、IMFによるサイバーセキュリティ、といった特有の項目もある。

普及や進展のペースを踏まえると、今後もAIが世界の証券市場における重要な論点の1つであり続ける可能性は高い。そのため、証券市場関係者は、各国・地域における証券監督当局や国際組織等による取り組みを注視し、自らの組織運営の適切なあり方を考えるきっかけにすることが大切と言える。

2点目について、ESMAの論文でも紹介されたように、AIは証券取引プロセスの随所で利活用されている。AIリスク対応に向けて新たにリスク管理・ガバナンス体制を構築するというより、既存の体制を見直し、AIの利活用にも耐えうるような仕組みに拡充していくことが多いと推察される。加えて、AIの発展が続く見通しであることを踏まえると、体制の見直し及び対応は一過性のものではなく、定期的かつ重大な事象が自社のみならず業界で起きた場合等のタイミングで継続的に行う必要があると言える。

Ⅳ 参考資料

図表 5　IOSCO：市場仲介者と資産運用会社による AI 及び ML の利用に関するガイダンス（概要）

潜在的なリスク・弊害	
項目	詳細
ガバナンスと監視	AI と ML を導入しているほとんどの企業が、AI と ML の技術開発と社内での利用を承認し、監督するにあたって、既存のガバナンスと監督体制に依存している。特定の AI と ML のリスクを管理するために、新たな手順を求めたり、既存の手順を修正したりする必要性を認識している企業はほとんどない
アルゴリズムの開発、テスト、継続的なモニタリング	企業は、AI や ML を利用しているか従来のアルゴリズムを利用しているかに関わらず、堅牢で理解可能な開発及びテストのフレームワークを導入することが重要である
データの質とバイアス	AI と ML のパフォーマンスは、特にモデル構築時において、データセットの質の影響を大きく受ける。データセット内の学習バイアスは、アルゴリズムによって行われる決定に影響を与える場合があり、差別的な決定及び市場参加者に対して望ましくない結果をもたらす可能性がある
透明性と説明可能性	AI と ML の効率的な利用と導入には、正確であるのみならず、企業、市場のカウンターパーティ、顧客、規制当局が理解できるアルゴリズムが必要である。仮に、結果が十分に説明できない場合、リスクが生じる可能性がある。企業が AI や ML を利用する際の透明性を高めることは、AI や ML の利用に対する国民の理解と信頼を向上させる可能性がある。しかし、その一方で、過度な透明性は、混乱を招いたり、個人がモデルを悪用したり操作したりする機会を生み出す可能性がある。一部の ML モデルは、結果の背後にある理由が明確ではなく、「ブラックボックス」と言われる
アウトソーシング	AI と ML ソリューションのための外部プロバイダーの利用は、特定のプロバイダーへの集中を招いたり、データのプライバシー、サイバーセキュリティ、運用上のリスクに関する懸念を引き起こす可能性がある。これらのリスクは、AI や ML の利用に特有のものではなく、適切かつ効果的なアウトソーシングプロセスを通じて軽減できることに留意すべきである
倫理上の懸念	AI と ML の文脈において、モデルが特定の社会的バイアスを発生させ、望ましくない結果を推奨する可能性がある場合、倫理的な懸念が生じ得る。アルゴリズム・モデルが市場機能においてますます重要な役割を果たすようになる中で、企業と従業員によって倫理的配慮がどのように満たされ続けるのかという論点もある
措置	
1. 規制当局は、AI と ML の開発、検証、監視、制御の監督を担当する上級管理職を企業に義務付けることを検討すべきである。これには、明確な説明責任を伴う、文書化された内部ガバナンスの枠組みが含まれる	
2. 規制当局は、企業に対し、AI と ML 技術の成果を継続的に検証するために、アルゴリズムを適切に検証及び監視するように求めるべきである	
3. 規制当局は、企業が利用する AI と ML の管理を開発、検証、展開、監視、監督するための十分なスキル、専門知識、経験を企業に要求すべきである	
4. 規制当局は、企業に対して、パフォーマンスの監視や監督を含めて、第三者プロバイダーとの関係を管理するように求めるべきである	
5. 規制当局は、企業が AI と ML の利用についてどの程度の情報開示を求めるかを検討すべきである	
6. 規制当局は、AI と ML のパフォーマンスに影響を与え得るデータが、バイアスを防ぐのに十分な品質であり、基礎がしっかりとしたものであることを確保するため、AI と ML の適切な管理を企業に義務付けることを検討すべきである	

（出所）International Organization of Securities Commission, “The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers: Final Report,” September 2021、より野村資本市場研究所作成

図表 6　SEC：予測データ分析の利用に伴う利益相反に関する規則案（抜粋）

SEC は、ブローカー・ディーラーや投資顧問による投資家との対応における予測データ分析の利用に関連する特定の利益相反に対処するため、新たな規則案を公表した。規則案では、以下を義務付けている

- ブローカー・ディーラーや投資顧問は、投資家に対応する際に対象テクノロジーを利用することにより、投資家の利益よりも企業またはその関連者の利益を優先するような、利益相反の影響を排除または中立化する必要がある
- 対象となる技術を利用して投資家と対応するブローカー・ディーラーや投資顧問は、規則案の違反を防止（投資顧問の場合）若しくは遵守を達成（ブローカー・ディーラーの場合）するために合理的に設計されたポリシーと手順を文書化する必要がある
- 利益相反に関する規則案に関連する記録の管理

（出所）U.S. Securities and Exchange Commission, “Fact Sheet: Conflicts of Interest and Predictive Data Analytics,” July 26, 2023、各種資料、より野村資本市場研究所作成

図表 7　OECD：金融分野における AI 導入によるリスク・課題及び政策の考慮事項

リスク・課題

項目	詳細
データ管理	AI を活用したアプリケーションにおけるデータの不適切な利用は、AI 技術を利用する企業に対して重要な非財務リスクをもたらし得る。このようなリスクは、データの真実性、プライバシーと機密性、公平性の考慮、潜在的な集中、より広範な競争問題に関連する
バイアスと差別	AI アルゴリズムは、利用方法によっては、金融サービスにおけるバイアスや不公正や扱い、差別を回避するのに役立つ。意図しないバイアスと差別のリスクは、データの誤用と ML モデルの不適切なデータの利用に関連している
説明可能性	AI ベースのモデルの本質的な複雑さに加え、市場参加者が知的財産を保護するために AI モデルのメカニズムを意図的に隠蔽することもある。その場合、説明可能性の欠如を招くこともある
モデルの堅牢性とレジリエンス（回復力）	テールイベント(注 1)を含むデータセットで ML モデルを訓練しなければ、金融システムに重大な脆弱性をもたらし、予測されない危機の際にモデルの信頼性を弱めるとともに、AI を市場環境が安定している時のみに利用可能なツールとなってしまう
AI システムのガバナンスと説明責任	顧客のために意図した成果が AI 技術を活用して得られるかの評価とともに、ガバナンスの仕組みを組み込む必要がある。AI システムを開発、導入、利用する組織はその適切な機能について責任を負うべき
雇用とスキル	金融業界における AI と ML の普及は市場参加者と政策当局者双方にとって、雇用上の課題やスキルアップの必要性を浮き彫りにする可能性

政策の考慮事項

- 金融機関によるデータガバナンスの改善に重点を置いた政策を強化し、金融における AI のユースケース(注 2)全体で消費者保護を強化する
- 意図しないバイアスや差別のリスクを克服するために役立つ慣行を促進する
- ファイナンスにおける AI 技術の利用が顧客の成果に影響を与え得る場合には、開示要件を検討する
- AI モデルのガバナンス及び説明責任メカニズムを強化する
- 企業が AI モデルの堅牢性とレジリエンスに関する信頼性を担保するための要件を検討する
- AI モデルの適切なトレーニング、厳密な検証のためのフレームワークの導入または強化を検討する
- AI モデルのレジリエンスを向上させるため、継続的な監視と検証を促進する
- 融資のようなユースケースの意思決定において、人間の優位性確保に重きを置く
- 技術の進歩に遅れないようにリソースを投入し、研究とともに、金融市場参加者及び政策立案者のスキル向上に投資する
- 既存の規制の適用が、技術の革新的な要素に関する新たなリスクへの対処に十分であるか否かを含め、国内及び国際レベルで政策立案者と産業界との間の学術的な対話を促進する
- AI への信頼性を間接的に醸成するため、金融業界の AI 利用を監督する

（注）　1. テールイベントは、稀にしか発生しないが、一旦発生するとその影響が極めて大きい事象。
　　2. ユースケースは、利用者から見たシステムの利用場面。

（出所）Organisation for Economic Co-operation and Development, “AI in Business and Finance,” OECD Business and Finance Outlook 2021, September 24, 2021、より野村資本市場研究所作成

図表 8　IMF：金融分野における AI／ML 導入によるリスクとポリシーに関する考慮事項

項目	詳細
埋め込みバイアス （embedded bias）	・ 埋め込みバイアスとは、特定の個人または個人のグループを組織的かつ不当に差別し、他の人を優遇するコンピューターシステムのことである ・ バイアスは、(1)システムのトレーニングに利用されるデータが不完全か、代表的なものでないこと、(2)データがこれまで根付いてきた偏見を支持すること、等が要因で生じ得る ・ AI／ML に埋め込まれたバイアスの問題に対する政策対応は、アプリケーションのガバナンスと倫理的利用のためのより広範な枠組みを開発し、展開することによって進めることができる
「ブラックボックス」の解除：説明可能性と複雑性	・ ML モデルは、ユーザーが直接説明できないため、ブラックボックスと呼ばれることが多く、ML の意思決定の適切性を検証することを困難にする可能性がある ・ 偏ったデータ、不適切なモデリング手法、誤った意思決定などの脆弱性を組織にもたらし、組織の堅牢性に対する信頼を損なう可能性がある ・ AI／ML にはモデリングプロセスの異なる段階、個々の予測や全体的なモデル動作の説明などの異なる目的に関連する様々なレベルの説明可能性がある。異なるレベルの説明可能性に関するリスクを管理するための適切な枠組みと戦略を構築する規制ガイダンスが金融セクターに必要である
サイバーセキュリティ	・ AI／ML の導入は、サイバー脅威の範囲を拡大し、新たな特有のサイバーリスクをもたらす。攻撃者は、AI や ML アルゴリズムを悪用すべく、ライフサイクルのある段階でデータを操作する。このような操作により、攻撃者は検出されることを回避し、AI や ML に誤った判断や情報の抽出を促すことができる ・ AI／ML に対する具体的なサイバー脅威は、(1)データポイズニング攻撃（トレーニング・データセットに特別なサンプルを追加することによって、トレーニング段階で ML アルゴリズムに影響を与える）、(2)入力攻撃（捜査中にデータ入力に混乱をもたらし、AI システムを誤解させる）、(3)モデル抽出・反転攻撃（トレーニングでの入力データやモデルの回復を試み、特定のデータがトレーニングに含まれているか否か確認する）、に大別される ・ AI／ML のサイバー脅威は金融セクターの完全性と信頼を毀損する可能性があり、システミックリスクを引き起こす可能性がある。金融セクターにおけるサイバーセキュリティ要件に関する規制の範囲は、AI／ML 特有のサイバー脅威に対応すべく、拡大される可能性がある
データプライバシー	・ AI／ML は、新たな固有のプライバシー問題をもたらす。例えば、AI／ML には推論によって匿名化されたデータのマスキングを解除する機能を有するほか、データが利用された後にトレーニングセット内の個人に関する情報を記憶する可能性があり、機密データが直接または推論によって漏洩する可能性がある ・ AI／ML システムと関連するデータソースが、関連するマネーロンダリング対策やテロ資金対策の要件と共に、強化されたプライバシー基準に準拠することを要求する法的及び規制の枠組みを適切に更新する必要がある
堅牢性	・ 金融セクターの AI／ML システムは、比較的安定して信頼性の高いシグナルを生成するデータ環境で良好なパフォーマンスを発揮してきたが、急激な構造変化の時期にはそれが急速に変化する可能性がある ・ 慎重な監視を強化し、意図しない結果を回避するために、AI／ML システムの開発のための新しいガバナンスフレームワークが必要である
金融安定性への影響	・ 金融セクターにおける AI／ML システムの広範な展開は変革をもたらすものであり、金融安定性への影響はまだ十分に評価されていない ・ AI／ML 主導の金融システムの完全性と安全性に対する国民の信頼を損なう可能性や、システミックリスクの新たな発生源と伝達経路をもたらす可能性がある ・ AI／ML の急速な進化は、様々な規制対応につながっており、一部の法域は包括的なアプローチをとっているが、他の法域はガバナンスに関する既存の規制で新たな問題に対処するのに十分と結論付けている

（出所）International Monetary Fund, “Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance,” October 22, 2021、より野村資本市場研究所作成