AIウォッシングへの監督と金融市場による対応
－米FINRAが示す規制対応に関する検討事項を中心に－

富永　健司

▌要　約▐

1. 米国の金融規制当局は近年、人工知能（AI）を活用しているように見せかけて、顧客を勧誘する行為（AIウォッシング）に対する監視を強めてきた。例えば、米国証券取引委員会（SEC）は2024年3月、AIの活用に関して虚偽で誤解を招く説明をしたとして投資顧問業者のデルフィア及びグローバル・プレディクションズを告発した。
2. 生成AIの活用の進展とAIウォッシングに対する監督強化の流れを受けて、米国における証券会社の自主規制機関であるFINRA（金融取引業規制機構）は2024年6月、会員証券会社に対して、AI関連のアプリケーション導入時における、規制対応に関する検討事項を周知した（規制通知）。FINRAの規制通知は、AI関連のアプリケーションを導入する際に、（1）モデル・リスク管理、（2）データガバナンス、（3）顧客のプライバシー、（4）監督統制システム、等に関連する規制上の義務について遵守を促す内容となっている。
3. SECは、2025年1月20日に第2次トランプ政権が発足するタイミングで、ゲイリー・ゲンスラー委員長の辞任を公表しており、AIウォッシングに対するSECの監督が今後どのように展開していくかは現時点では見通すことが困難な状況である。他方、AIウォッシングに関連する取り組みは、米国だけではなく国際的にも進展が見られる。
4. 国内では金融庁が、データに基づいたより高度な金融サービスの提供や、生成AIを含むAIを活用したモデルの利用が進む中で、その活用に伴って生じるモデル・リスク管理態勢の高度化を金融機関に促している。AIの普及に伴い、金融市場でモデル・リスク管理等への対応が進展することで、AIの活用に関する透明性と信頼性が向上していくのか注目される。

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』2023年秋号。
・齋藤芳充・吉川浩史「米国の自主規制機関 FINRAが進める自己改革の背景と今後の展開」『野村資本市場クォータリー』2018年春号（ウェブサイト版）。

Ⅰ 米国におけるAIウォッシングに対する監督動向

米国の金融規制当局は近年、人工知能（AI）を活用しているように見せかけて、顧客を勧誘する行為（以下、AIウォッシング）に対する監視を強めてきた。

例えば、米国証券取引委員会（SEC）は2024年3月、AIの活用に関して虚偽で誤解を招く説明をしたとして投資顧問業者のデルフィア及びグローバル・プレディクションズを告発した[1]。デルフィアは、2019年から2023年の間、SECへの提出書類・プレスリリース・同社のウェブサイトにおいて、AI関連のサービスを提供する能力がないにも関わらず、「収集したデータによって、AIをより優れたものにし、成長する企業やトレンドを予測し、他の投資家より先に投資を行なう」と主張していた。グローバル・プレディクションズは、2023年にウェブサイト及びソーシャルメディア上で、「初となる規制されたAI関連の金融アドバイザー」と称し、「専門的なAIによる予測を提供する」との虚偽の説明を行っていた。両社は計約40万ドルの罰金の支払いに合意した。

SECは2024年10月にもAIウォッシングに関する告発を投資顧問業者のリマールキャピタル等を対象に行った[2]。さらに、米国では連邦取引委員会（FTC）も、消費者保護の観点からAIウォッシングへの取り締まりを強化している[3]。

生成AIの活用の進展とAIウォッシングに対する監督の強化を受けて、米国における証券会社の自主規制機関であるFINRA（金融取引業規制機構）[4]は2024年6月、会員証券会社に対して、AI関連のアプリケーション導入時における、規制対応に関する検討事項を周知した（以下、規制通知）[5]。

本稿では、FINRAが周知した規制対応に関する検討事項を整理した上で、金融市場におけるAIウォッシングへの対応と注目点について論考する。

Ⅱ FINRAが周知した規制対応に関する検討事項

本章では、（1）FINRAの規制通知の問題意識（2）規制対応に関する検討事項、について示す。

---

1 U.S. Securities and Exchange Commission (SEC), “SEC charges two investment advisers with making false and misleading statements about their use of artificial intelligence,” March 18, 2024.

2 SEC, “SEC charges Rimar Capital Entities and Owner Itai Liptz for defrauding investors by making false and misleading statements about use of artificial intelligence,” October 10, 2024.

3 Federal Trade Commission, “FTC announces crackdown on deceptive AI claims and schemes,” September 25, 2024.

4 FINRAについて、詳しくは、関雄太「新たな自主規制機関FINRAの誕生」『資本市場クォータリー』2007年秋号、齋藤芳充・吉川浩史「米国の自主規制機関 FINRAが進める自己改革の背景と今後の展開」『野村資本市場クォータリー』2018年春号（ウェブサイト版）、を参照。

5 Financial Industry Regulatory Authority (FINRA), “Regulatory Notice 24-09 FINRA reminds members of regulatory obligations when using generative artificial intelligence and large language models,” June 27, 2024; “Finra navigates ‘AI washing’ as firms roll out client-facing gen AI,” *American Banker*, October 14, 2024.

１．FINRA の規制通知の問題意識

FINRA は昨今、（1）生成 AI を含む AI 技術の活用が急速に進展していること、（2）AI ウォッシングに関するリスクが高まっていること、等を踏まえて、AI 関連のアプリケーション導入時の規制上の検討事項を改めて周知した[6]。

FINRA が発出した規制通知は、新たな法的要件や規制要件を課すものではなく、既存の要件について新たな解釈を行うものでもない。むしろ、既存の規制上の義務についての遵守を促す内容となっている。FINRA は規制通知において、会員証券会社が生成 AI 活用を行う際、ビジネスの状況に応じた監督システムを構築し、モデル・リスク管理、顧客プライバシー、データのガバナンス等を含むポリシーや手順を整備していく必要があるとの見解を示した。

２．規制対応に関する検討事項

FINRA の規制通知で参照されている、証券業界と AI に関するレポート[7]においては、AI 関連のアプリケーションを会員証券会社が導入する際に検討すべき事項として、（1）モデル・リスク管理、（2）データガバナンス、（3）顧客のプライバシー、（4）監督統制システム、等が挙げられている（図表 1）[8]。

図表 1　FINRA の規制通知における AI 導入における規制上の主な検討事項

検討事項	内容
モデル・リスク管理	包括的にモデル・リスク管理を実施する場合、モデルに関して、(1)開発・検証、(2)導入、(3)継続的なテスト、(4)監督・管理、の領域について考慮していくこと
データガバナンス	データのガバナンスに関するポリシー及び手順の見直し及び変更について、(1)データのバイアスに関するチェック、(2)データソースの検証、(3)データの統合、(4)データのセキュリティの確保、(5)データの品質に関する指標の活用、を検討していくこと
顧客のプライバシー	AI 関連モデルで使用されるデータ及びアウトプットに関連して、(1)顧客情報及び記録の保護に対応する文書によるポリシー及び手順の整備、(2)これらのポリシー及び手順の維持と、テクノロジーの進展に応じた更新、(3)書面による個人情報盗難防止プログラムの検討・実施、等を行うこと
監督統制システム	AI 関連のアプリケーションを導入する際、(1)部門横断的なテクノロジーガバナンス構造の確立、(2)アプリケーションへの広範なテストの実施、(3)代替計画の作成、(4)人材の登録についての検証、を行うこと

（出所）FINRA, “Artificial Intelligence (AI) in the securities industry,” June 2020.

6 Financial Industry Regulatory Authority (FINRA), “Regulatory Notice 24-09 FINRA reminds members of regulatory obligations when using generative artificial intelligence and large language models,” June 27, 2024.

7 FINRA, “Artificial Intelligence (AI) in the securities industry,” June 2020.

8 この他、追加的に考えられる考慮事項として、サイバーセキュリティ等が挙げられている。

1）モデル・リスク管理

AI 関連のアプリケーションを導入する会員証券会社は、AI 技術がもたらす課題に対処するために、モデル・リスク管理の枠組みを見直し、更新していくことが重要と明記された。包括的なモデル・リスク管理を実施する際には、モデルに関して、（1）開発・検証、（2）導入、（3）継続的なテスト、（4）監督・管理、の領域を考慮する必要があることが示された。

モデルの開発・検証については、モデルの複雑さを考慮に入れた上で、モデルの検証プロセスを更新していくことが重要とされた。これには、入力データのバイアス、アルゴリズムのエラー、パラメータに関するリスクの閾値、アウトプットの説明可能性、等に関連するレビューが含まれている。そして、新しいモデルを導入する際には、既存のモデルと新しいモデルを並行して使用し、新しいモデルが十分に検証された後に既存モデルを新しいモデルに置き換えるべきとされた。

一方、モデルの継続的なテストについては、前例のない市場状況や新しいデータセットを用いたストレステストのシナリオに基づき、継続的なテストの実施を検討することが求められた。AI モデルのデータベース（インベントリー）において、モデルに関するリスク水準に基づいて、適切にモデルを監督・管理することができると言及された。加えて、モデルに関する評価指標を開発し、継続的な監督・報告プロセスを確立することで、モデルの良好なパフォーマンスを維持していくことを考慮すべきとされた。

2）データガバナンス

AI 関連のアプリケーションにおけるデータ関連のリスクに対処するためには、データのガバナンスに関するポリシー及び手順を見直すことが重要とされた。具体的な内容としては、（1）データのバイアスに関するチェック、（2）データソースの検証、（3）データの統合、（4）データのセキュリティの確保、（5）データの品質に関する指標の活用、が挙げられている。

データのバイアスを確認する一例としては、特定のデータを削除してアウトプットへの影響を調べることや、システムを構築・テストするチームを多様なメンバーで構成することが挙げられた。データソースの検証においては、データソースの妥当性及び信頼性を定期的にレビューする必要がある。特にこのことは外部からデータを取得している場合に重要とされた。

一方、複数のデータソースがある場合には、それらを組織内で効率的に取得・統合できるようにすべきと記された。また、データのセキュリティを確保するためには、適切な権限・認証・アクセス制御の手続きを開発・維持・テストする必要があるとされた。機密データについては、暗号化技術を使用することもできる。包括的にデータガバナンスを戦略的に実行するためには、データガバナンスを評価するための指標を活用することが有効と説明されている。

３）顧客のプライバシー

顧客の情報の保護は、会員証券会社にとって重要な責務と明記された。証券業界で使用される AI 関連のアプリケーションの中には、機密性の高い顧客関連データの収集・分析・共有及び顧客行動の監視に関連するものがある。具体的な顧客データとして、（1）個人を特定できる情報の収集・使用及び生体認証、（2）ウェブサイト及びアプリの利用状況、地理空間情報、ソーシャルメディアでの活動、（3）書面・音声・ビデオによるコミュニケーション、が挙げられた。こうしたデータは、企業が顧客の行動や嗜好を知ることに役立つ一方、情報が適切に保護されていない場合、顧客のプライバシーに関する懸念を引き起こす可能性があると言及された。

このような考えの下、証券会社は、AI 関連モデルで使用するデータ及びアウトプットに関連して、顧客のプライバシーの規則を遵守しなければならないとされた。具体的には、（1）顧客情報及び記録の保護に対応する文書によるポリシー及び手順の整備[9]、（2）これらのポリシー及び手順の維持と、テクノロジーの進展に応じた更新[10]、（3）書面による個人情報盗難防止プログラムの検討・実施、等が挙げられた。

４）監督統制システム

FINRA の規則では、監督統制システムに関連して、会員証券会社に対して、AI 技術を基にしたツールやシステムの監督とガバナンスのために、合理的な監督ポリシー及び手順を策定・維持することを求めている[11]。

AI 関連のアプリケーションを導入する際に、監督統制システムの観点から考慮すべき事項としては、（1）部門横断的なテクノロジーガバナンス構造の確立、（2）アプリケーションの広範なテストの実施、（3）代替計画（fallback plans）の策定、（4）人材の登録についての検証、が挙げられた。

金融機関は、AI 関連のアプリケーションの開発・テスト・実装を監視する際には、部門横断的なテクノロジーガバナンス体制を構築することが重要とされた。このような体制を構築することで、様々な分野の知見により、AI の活用に伴うリスク評価を行うことができる。

加えて、新しいツールやアプリケーションについては、様々な段階で広範なテストを行うことで、潜在的なリスクを迅速に特定することができるとされた。また、代替計画を策定することは、AI 関連のアプリケーションに障害が発生した際の事業継続に寄与すると説明された。さらに、FINRA の規則では、アルゴリズム取引戦略の設計・開発や重要な変更に関わる関係者の登録が求められている。

---

9 SEC, “Regulation S-P: Privacy of consumer financial Information and safeguarding consumer information.”

10 FINRA, “Notice to Members 05-49 NASD reminds members of their obligations relating to the protection of customer information,” July 28, 2005.

11 FINRA, “FINRA Rules 2110. Supervision.”

Ⅲ 金融市場におけるAIウォッシング対応をめぐる注目点

FINRAによる規制通知の重要なポイントは、AI導入に関連する規制上の対応事項について、既存の規則の遵守を促している点である。すなわち、AIを導入していく際、既存の規則への影響を慎重に見極めて、必要に応じて適切な修正を行うことが求められている。なお、FINRAは規制通知の中で、将来的に、追加的なガイダンス又は既存の規則の修正を検討する意向を示した。

SECは、2025年1月20日に第2次トランプ政権が発足するタイミングで、ゲイリー・ゲンスラー委員長の辞任を公表しており、AIウォッシングに対するSECの監督が今後どのように展開していくかは現時点では見通すことが困難な状況である[12]。一つの見方として、2025年においては2024年と同様に、既存の規則の遵守を促す形で、AIウォッシングの取り締まりのケースが発生する可能性が指摘されている[13]。

他方、AIウォッシングに関連する取り組みは、米国だけではなく国際的にも進展が見られる。例えば、カナダでは、カナダ証券管理局が2024年12月、AIウォッシングのリスクを念頭に置いて、金融市場におけるAIの活用にカナダの証券法がどのように適用されるかに関する意見募集を開始している[14]。

日本では金融庁が、データに基づいたより高度な金融サービスの提供や、生成AIを含むAIを活用したモデルの利用が進む中で、その活用に伴って生じるモデル・リスク管理態勢の高度化を金融機関に促している。同庁は2024年12月に、2021年に公表した「モデル・リスク管理に関する原則」（図表2）を基に、金融機関のモデル・リスク管理の取り組みを整理し、公表した（以下、プログレスレポート）[15]。

金融庁は、モデル・リスク管理に関する原則公表後のモニタリング結果の中で、AIモデルに関する状況として、「構築したモデル・リスク管理態勢の枠内での管理を進め、又は計画している一方、AI特有のリスクに対応した検証方法等について、各種ガイドライン[16]も参考にしつつ、全ての対象金融機関において模索・検討を進めている」との認識を示している。

生成AIの活用の進展がモデル・リスク管理に与える影響として、モデル・インベントリーの拡大が挙げられる。2023年に国際金融協会（IIF）が発表した調査結果によれば、「今後3年間で、生成AIモデルの増加によりモデル・インベントリーがどの程度拡大することが見込まれるか」との設問に対して、2割以上拡大すると回答した割合が全体の86%に上った[17]。

---

12 SEC, “SEC Chair Gensler to depart agency on January 20,” November 21, 2024.
13 “AI-washing enforcement crackdown set to survive Trump rollbacks,” *Bloomberg*, November 25, 2024.
14 Canada Securities Administrators, “Canadian Securities Administrators issue guidance and consult on use of AI systems in capital markets,” December 5, 2024.
15 金融庁「金融機関のモデル・リスク管理の高度化に向けたプログレスレポート（2024）」2024年12月12日。モデル・リスクは、モデルの誤り又は不適切な使用に基づく意思決定によって悪影響が生じるリスク。
16 例として、2024年4月に総務省・経済産業省が公表した「AI事業者ガイドライン（第1.0版」（同年11月に第1.01版が公表）が挙げられている。
17 IIFがEY（Ernst & Young）と共同で、2023年に世界の金融機関65社を対象に実施（Institute of International Finance, EY, “IIF-EY annual survey report on AI/ML use in financial services,” December 2023）。

図表 2　金融庁が公表したモデル・リスク管理に関する原則

番号	項目	内容
1	ガバナンス	取締役会等及び上級管理職は、モデル・リスクを包括的に管理するための態勢を構築すべきである
2	モデルの特定、インベントリー管理及びリスク格付	金融機関は、管理すべきモデルを特定し、モデル・インベントリーに記録した上で、各モデルに対してリスク格付を付与するべきである
3	モデル開発	金融機関は、適切なモデル開発プロセスを整備すべきである。モデル開発においては、モデル記述書を適切に作成し、モデル・テストを実施すべきである
4	モデル承認	金融機関は、モデル・ライフサイクルのステージ（モデルの使用開始時、重要な変更の発生時、再検証時等）に応じたモデルの内部承認プロセスを有するべきである
5	継続モニタリング	モデルの使用開始後は、モデルが意図したとおりに機能していることを確認するために、第 1 線によって継続的にモニタリングされるべきである
6	モデル検証	第 2 線が担う重要なけん制機能として、金融機関はモデルの独立検証を実施すべきである。独立検証には、モデルの正式な使用開始前の検証、重要な変更時の検証及びモデル使用開始後の再検証が含まれる
7	ベンダー・モデル及び外部リソースの活用	金融機関がベンダー・モデル等や外部リソースを活用する場合、それらのモデル等や外部リソースの活用に対して適切な統制を行うべきである
8	内部監査	内部監査部門は、第 3 線として、モデル・リスク管理態勢の全体的な有効性を評価すべきである

（注）　第 1 の防衛線（第 1 線）は、モデルを所管する又はモデルの開発・使用に直接関係する部門・個人で構成される（モデル・オーナー、モデル開発者、モデル使用者等）。第 2 の防衛線（第 2 線）は、第 1 線に対するけん制を通じてモデル・リスクを管理する部門・個人で構成され、モデル・リスク管理態勢の維持、規程等の遵守状況及びモデル・リスク全体に対する独立した立場からの監視、モデルの独立検証等の役割を担う。第 3 の防衛線（第 3 線）は、内部監査部門で構成され、金融機関のモデル・リスク管理態勢の全体的な有効性を評価する。

（出所）金融庁「モデル・リスク管理に関する原則」2021 年 11 月 12 日

このような状況に鑑みると、生成 AI の活用が進む中で、金融庁が示したモデル・リスク管理に関する原則において、「モデルの特定、インベントリー管理及びリスク格付」の重要性が増していると考えられる。この項目に関する具体的な取り組みとして、プログレスレポートは、（1）モデルの範囲・定義を設定し、社内でモデルに関する認識を統一し、適切な管理を行うこと、（2）フローチャートやチェックリストを活用しながら、グループ内のモデルの全数調査・特定を行うこと、（3）モデルの基本情報やモニタリング、独立検証の実施状況等を一元管理できるモデル・インベントリーの構築と運用を行うこと、（4）影響度（重要性）と複雑性を組み合わせて、モデルに内在するリスクに応じたリスク格付を付与すること、を挙げている。

金融市場において、AI の活用とそのリスク管理を行うにあたって特に重要なのは、（1）バイアスや差別の監視と対処、（2）透明性・解釈可能性の考慮、である。AI の活用を進める際には、データやモデルに関連するバイアスを認識し、その監視を行うことが重要と言える。加えて、当局や顧客とのコミュニケーションを考慮する中で、モデルの精度だけではなく、透明性・解釈可能性を考慮することが求められる。AI の普及に伴い、金融市場でモデル・リスク管理等への対応が進展することで、AI の活用に関する透明性と信頼性が向上していくのか注目される。