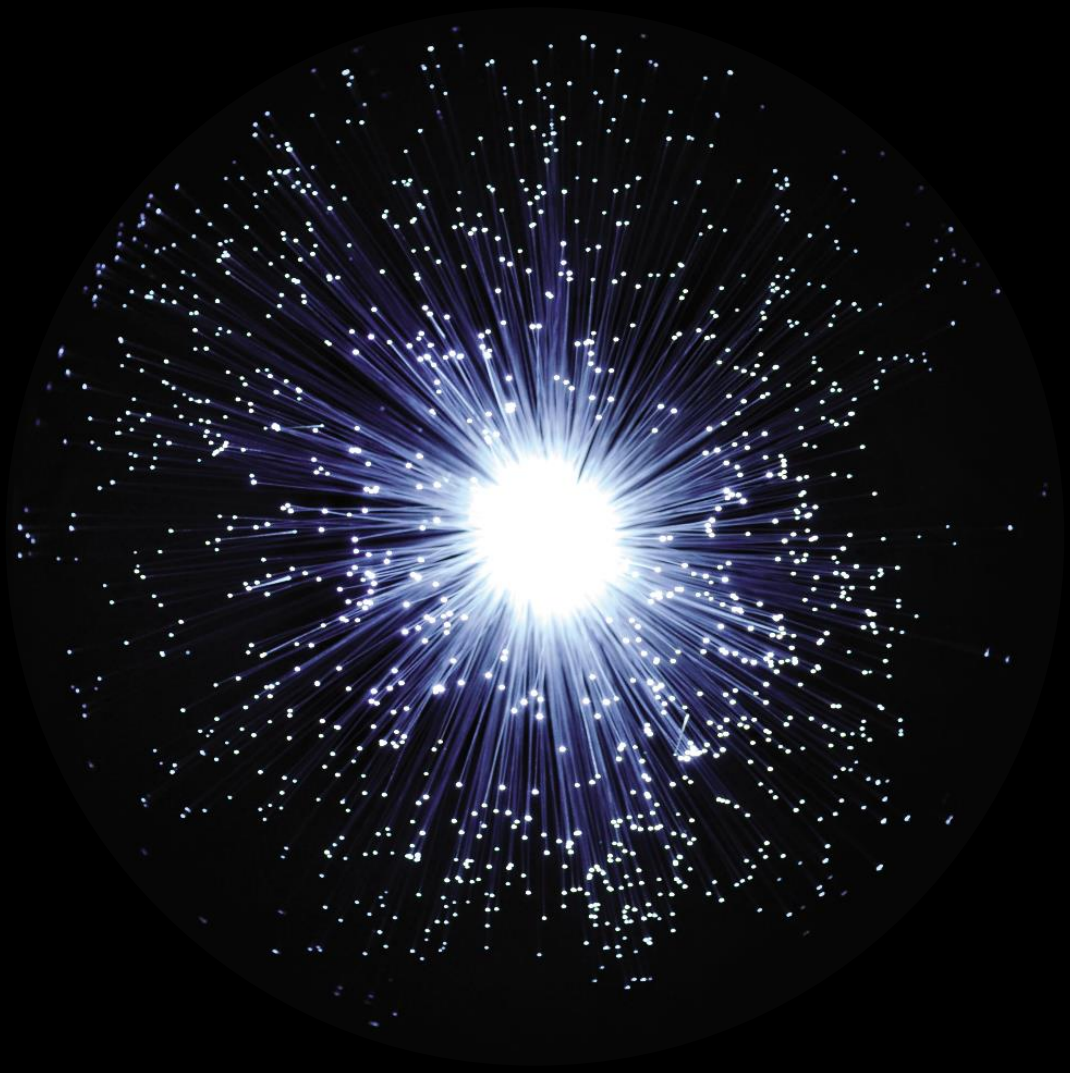
Deloitte.
デロイト トーマツ

トーマツ.



人工知能（AI）とリスクマネジメント

自信をもって革新するために

目次

1. エグゼクティブ・サマリー 01
2. AIの概要 03
3. 金融サービスにおけるAI普及の課題 04
4. リスク管理フレームワークへのAIの組み込み 07
5. 規制当局は何を求めているのだろうか？ 18
6. AIの規制 22
7. まとめ 24

コンタクト、執筆者 25

1. エグゼクティブ・サマリー

人工知能（AI）は新しい概念ではありませんが、金融サービス企業が、関心を寄せ、その可能性を十分に理解し始めたのは最近のことです。

AIは事業効率やコスト効率を向上させるのみならず、顧客満足度の向上につながる戦略的なビジネス改革をも推進することができます。しかし、入手可能なデータの質と量が限られていること、AI固有のリスクに対する理解が不十分であること、企業文化、そして、規制の問題などが、金融サービス企業においてAIを広く活用する上での障壁となっています。

EUや国際的な規制当局もAIに積極的に関心を示しており、AIが金融市場、消費者、そして自身の仕事にもたらす利益を認識している一方で、規制業種におけるAIの使用がもたらす潜在的なリスクや想定外の事象にもますます注意を払っています。

これは、金融業界が近年、顧客の不適正な扱いや市場での不正行為により、相当数の罰金や行政処分を受けていることも重要な要因の一つです。その結果「顧客の平等な扱い」と「市場の整合性」に焦点が当てられ、規制上の観点でAIは比較的、未経験かつ未検証であるため、金融サービス企業はAIソリューションの採用に慎重になっています。

効果的なリスク管理は、イノベーションの阻害要因とはならず、むしろ企業においてAIの活用を成功させるために必要です

これらの障壁を乗り越え、AI導入のメリットを十分に享受し将来的な問題を回避するには、取締役会や上級管理層が、これまでの組織内の利用や今後の活用方法を含めたテクノロジーについての理解を深め、リスクの観点からAIの性質をしっかり把握することが不可欠です。このような意味において、効果的なリスク管理は、イノベーションの阻害要因となるものではなく、企業がAIを活用し成功するために極めて重要な要素となります。

企業にとっての最大の課題は、全く新しい種類のリスクというより、効果的かつタイムリーに特定することが困難な既存のリスクか、これまでに無い形で顕在化するリスクに対処することです

本稿の焦点である後者の点に関して、企業にとっての最大の課題は、全く新しい種類のリスクというより、効果的かつタイムリーに特定することが困難な既存のリスクか、これまでに無い形で顕在化するリスクに対処することです。本稿では既存のリスク管理フレームワーク（RMF: Risk Management Framework）を使い、企業が複雑なAIを活用する際に考慮すべきポイントを解説します。

事前に定義された明確なルールだけではなく、新たなデータから継続的に学習し、複雑な統計的手法に基づいて決定を下すAIにおいては、最終的な意思決定要因の把握が難しくなります。多くの点で、これは組織が人的資源を管理する際に直面する課題と似ています。AIソリューションの進化は、可監査性と追跡可能性を困難にする恐れがあり、またAIソリューションの進化の速度は非常に短い時間内に大規模なエラーを発生させる可能性があります。

企業はRMFライフサイクルの様々な段階（識別・評価・統制・監視）においてリスクを管理するために、その実務を見直し、更新する必要があります。AIソリューションは継続的に進化するものであるため、こういった活動はより短いスパンで、頻繁に行うことが求められます。また、既存のリスクアペタイト・ステートメントも見直す必要があり、RMFの様々な段階で情報を提供するために、例えば「公平性の指針」のような多くの新しい要素を加える必要があるかもしれません。

AIソリューションの進化は、可監査性と追跡可能性を困難にする恐れがあり、AIソリューションの進化の速度は非常に短い時間内に大規模なエラーを発生させる可能性があります

本稿では、シンプルで概念的なRMFを用いて、AIが導くいくつかの課題を抽出し、フレームワークに命を吹き込んでいきます。ここでは、保険会社の保険契約の価格設定を題材として、企業がAIソリューションのモデルリスクを管理する方法を扱います。また、規制当局がAIソリューションにどのように対応しているかを説明し、規制当局の重点分野と期待を示します。最後に、規制当局がAIを規制するための課題と、利用できる選択肢について考察します。

本稿は、AIが既存のリスク管理手法に与える影響と、より広範な規制の背景を理解する出発点となることを目指します。これらの分野を重点的に扱うことで、企業での検討において、より一般的なAI戦略の策定、そしてより具体的なAIのRMFの開発における重要な課題と管理観点を提供することを目的とします。

2. AIの概要

人工知能の概念は、1950年代に研究者たちが機械によって人間の知性を模倣する可能性を最初に考え始めた時に遡ります。しかし、AIが本当の意味で「テイクオフ」したのは2000年代後半で、いくつかの要因が転換点に達した時でした。それは、性能の良いコンピュータの安価な利用、データの量と種類の増加、データへのアクセスの速さ、そして、よりスマートな方法[*1]でデータを分析できる新しい高度なアルゴリズム[*2]の出現といったものです。

AIの定義はひとつではありませんが、大まかに言えば、AIは人間の知性[*3]を必要とする作業を遂行できるコンピュータシステムの理論と開発です。そのようなタスクの例としては、視覚認識、音声認識、不確実性下での意思決定と学習などが挙げられます。

定義の不一致は、少なくとも部分的にはAIそれ自体が技術ではなく、むしろ人間の行動を模倣する技術の集合であるという事実によって説明されるかもしれません。現在金融サービスに関係があり、本稿で言及している主要な技術は次の通りです。

機械学習
明示的なプログラムを与えなくても、データを与えることでコンピュータシステムのパフォーマンスを向上させる機能。機械学習は、データのパターンを自動的に発見し、それを利用して予測を行うプロセスを指す。

音声認識と自然言語処理
人間の発する言葉を人間が行うように理解する能力。例えば、テキストから意味を抽出したり、読みやすく、スタイル的に自然で、文法的に正しいテキストを生成したりすることにより、人間の言語を理解し生成する能力。

ディープラーニング
ディープラーニング・アルゴリズムは、機械学習アルゴリズムの一種であり、音声およびコンピュータ・ビジョンに関連するタスクにおける有効性のため、ますます一般的になっている。これらは複雑な技法であり、各入力がどのように結果をモデル化するか正確に理解することは困難であり、その結果「ブラックボックス」として特徴づけられることが多い。

視覚認識
画像内の物体、シーンおよび動作を識別する機能。コンピュータ・ビジョン技術は、連続的な画像処理操作や技術により、画像解析のタスクを扱い可能な断片に分解する。

金融サービスにおける顧客経験価値の向上
Behaviour and Emotion Analytics Tool（BEAT）は、ディープラーニングと様々な機械学習アルゴリズムにより、音声対話を観察し分析するDeloitteの音声分析プラットフォームです。主に次の3つの機能で構成されます。

1. お客様との音声対話のモニタリング
2. NLP（自然言語処理）を用いたリスクの高い対話の特定
3. 潜在的なマイナス要素（苦情またはコンダクトリスク上の問題など）と対話を対応付け、それが生じる原因の詳細を分析

BEATは、お客様が話した言葉とその言葉のトーンの両方を分析し、機械学習技術を利用してやり取りを分析するアルゴリズムを継続的に開発、強化できるようにすることで、従来の分析手法に比べてより多くの件数を処理することができ、またより高い精度を実現します。

BEATは、30以上の異なる言語と30の異なる行動指標を分析できます。また、特定のリスク要件やユーザーのニーズに合わせてカスタマイズすることも可能です。

*1：Demystifying artificial intelligence - https://www2.deloitte.com/insights/us/en/focus/cognitive-technologies/what-is-cognitive-technology.html
*2：計算またはその他の問題解決操作において、コンピュータが従うべきプロセスまたはルールの集合
*3：https://en.oxforddictionaries.com/definition/artificial_intelligence

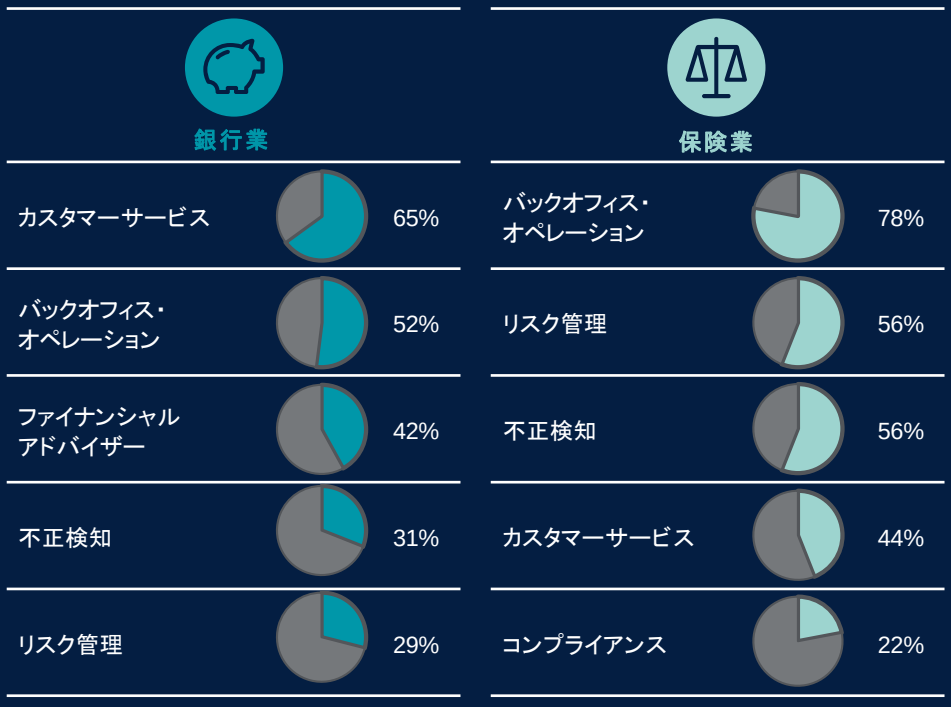
3. 金融サービスにおけるAI普及の課題

2008年の金融危機以来、金融サービス企業は利益率の圧迫を埋め合わせるために、コスト効率を高め、競争力を維持しようと努めてきました。これを達成するために、注目する分野のひとつがテクノロジーであり、ここ数年でAIの利用拡大が検討されています。しかしAIの採用において、ひとつの基準ですべてに対応することはできません。その理由のいくつかを挙げます。

AIが適用されるべき領域についての多様な見解

欧州金融管理協会（EFMA）と共同で実施した3,000人以上の経営幹部を対象とした最近のDeloitteの調査[*4]によると、AIが最大の影響を及ぼすと考えられる活動や機能は、業界によってかなり異なります（図1）。

図1:「開発した人工知能の使用が最も大きな影響を与えるのは、バリュー・チェーンのどの部分ですか。」



また、全体的に見て、金融サービス業におけるAIの採用はまだまだ初期段階にあるとの結論に達しました。調査した企業のうち、40%はAIを組織に導入する方法をまだ模索しており、11%は活動を開始していません。32%の企業だけがAIソリューションを積極的に開発しているという結果でした。

*4：AI and you | Perceptions of Artificial Intelligence from the EMEA financial services industry– https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology/deloitte-cn-tech-ai-and-you-en-170801.pdf

データの不足と品質

AIと他の伝統的なテクノロジーによるソリューションの主な違いのひとつは、後者は事前に定義された明確なルールに則って実行できるタスクが限定されているのに対し、AIアプリケーションはデータを分析してパターンを特定し、それに基づいて決定を下すという点にあります。さらに、AIアプリケーションは、設計時1回限りではなく、提供されたデータから継続的に学習して、時間の経過とともに意思決定の方法を改善するようにプログラムされています。

これは、AIソリューションによって行われるあらゆる意思決定の質が、使用されるデータの質と量に大きく依存することを意味します。品質の高いデータが大量に存在しないという問題は、一般に、AIによる解の適用に対する主要な障壁のひとつです。多くの金融サービス企業において、これはレガシーシステムや部門毎にサイロ化したシステムがいまだ浸透していることが原因であり、データのシームレスな流通が妨げられたり、データの品質に悪影響が及んだりしています。

透明性、説明責任、コンプライアンス（法令遵守）

AIソリューションの中には、最終的な意思決定に複数のブラックボックス化した層が影響を与えるものがあります。ディープラーニングを用いたアプリケーションのような、複雑なAIアプリケーションの場合、金融サービス企業がAIベースの意思決定について、適切性、公平性、組織の価値観やリスクアペタイトとの整合性等、必要なレベルの理解と統制を維持し、根拠を示すことが課題となります。

学習・進化を繰り返し、多くのブラックボックス化した層を含むAIソリューションは、可監査性と追跡可能性を困難にする恐れがあります

これは、組織が人的資源を管理する際に直面する課題と似ています。学習・進化を繰り返し、多くのブラックボックス化した層を含むAIソリューションは、可監査性と追跡可能性を困難にする恐れがあります。さらに、AIソリューションの学習・進化のスピードは、大規模なエラーを急激に発生させる可能性があります。

一部のAIソリューションの不透明性はまた、EUの新しい一般データ保護規則（GDPR）のような特定の規制に関連して実務上の課題を提起します。この規制は特定の状況において、個人情報がどのように使用されているかを説明することや、顧客に重大な影響を与えながら完全に自動化された決定の背後にある前提条件と決定要因について、企業が意味のある説明を提供できるようにすることを要求しています。

AIとその性質の理解

AIは複雑で急速に発展している分野であり、専門家でない人の目から見れば、AIをコントロールすることは難しいことだと映りがちです。さらに、AIの使用は、従来の企業リスクを高めることに加え、リスクを顕在化させる方法を変えたり、組織に新たなリスクをもたらしたりすることさえあります。

金融サービスは高度に規制された業種で、広範で複雑な種類の事業やサービスから構成されており、企業は常に適切なレベルの慎重さを保ち、事業を遂行しなければなりません。しかし、金融業界が経験したコンプライアンス違反や不正行為に対する規制上の罰則の歴史は、規制された活動において比較的未知の技術を採用する際、さらなるレベルの保守主義をもたらしており、これがイノベーションの障壁となる可能性があります。

過度に警戒することは、テクノロジーとその固有のリスクに対する知識や理解の低さに起因します。リスク担当者、コンプライアンス担当者、事業責任者、取締役会メンバー、経営者などの主要なステークホルダーは、AI技術を十分に理解できていると感じない限り、AIを組織内の規制された活動に使用することを承認し、説明責任を負うことをためらいます。ステークホルダーがAIという新しいテクノロジーがもたらすリスクを受け入れるためには、リスクを最小化し、管理監視する方法*5を理解するところまでが必要です。

主要なステークホルダーが個々のAIやAIの集合体への理解に取り組むことは、企業にとっての課題となるでしょう。現実的で受け入れられやすいユースケースを題材に、顧客体験を理解することによって、ステークホルダーはAIの利点だけでなく、何が上手くいかないか、そしてどのようにしてリスクを軽減または管理できるかを理解できます。

人材への影響

AIを採用している組織、特に大規模な組織にとっては、AIがもたらす変革が企業文化や人事戦略にもたらす影響を十分に理解することが不可欠です。そして悪影響に対しては必要な対応を実施することが重要です。

企業にはAIアプリケーションの設計、テスト、管理を支援するために、さらに熟練したエンジニアを必要とするでしょう。現在、このような人材が不足していることと、金融サービス企業のイノベーションに対しての苦手認識が、この問題を難しくする可能性があります。エンジニア採用方法やチャネルを変更する必要があるでしょうし、キャリアパスと、組織への定着・融合・後継者育成の各戦略を策定する必要があります。

既存のスタッフへの影響は、さらに深刻なものになるかもしれません。AIの開発は、パターン認識によって自動化できる仕事の総需要を減らすことが期待されます。人員配置の必要性の減少、または異分野への既存職員の再配置（関連する再トレーニングの考慮も併せて）のような雇用慣行の大きな変更は、職員の士気に影響を及ぼす可能性があり、迅速に対処しなければ、それを望まない職員の離職率の増加につながる可能性があります。

一方で、人員の急激な喪失は、AIアプリケーションに障害が発生した場合、または短期間でシステムを停止しなければならない事態に陥った場合、必要な専門知識を持っていて手作業でプロセスを実行できる熟練スタッフを企業が十分に確保できなくなるという問題を引き起こすでしょう。また、企業の次世代の経営陣の育成にも影響を与える可能性があります。

*5：https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

4. リスク管理フレームワークへのAIの組み込み

AIの採用とイノベーションは、企業のラーニングジャーニーが必要です。AIに関連するすべてのリスクを回避することではなく、そのようなリスクが企業のリスク文化とリスクアペタイトの中で効果的に特定され、管理されていると企業が自信を持つことができるようにプロセスとツールを開発することがその目的です。したがって、恐らく一般的な誤解とは逆で、効果的なリスク管理は、企業のイノベーション能力に重要な役割を果たすことになります。

AIアプリケーションに固有のリスクの性質

AIを管理する上での課題は、まったく新しいタイプのリスクへの対処ではなく、AIソリューションの複雑さと進化の速さを考えれば、従来のリスクを効果的かつタイムリーに特定することが難しくなることや、未知の方法でそれらを明らかにすることだと考えています。したがって、企業はAIを扱うために全く新しいプロセスが必要なわけではありませんが、AIを考慮し、避けがたいギャップを埋めるために既存のプロセスを強化する必要があります。必要なリソースのレベル、および役割と責任への影響の可能性についても対処する必要があります。

企業はAIを扱うために全く新しいプロセスが必要なわけではありませんが、AIを考慮し、避け難いギャップを埋めるために既存のプロセスを強化する必要があります

Deloitte AI Risk Management Frameworkは、AIに関連するリスクとコントロールを特定し、管理するためのメカニズムを提供します。次ページ以降のセクションでは、このフレームワークでカバーされている60を超える網羅的なAIリスクからいくつかの重要な考慮事項を説明しています。これらの考察は一般的な用語で表現されています。リスクのレベルと必要なコントロールは、実際には、ユースケースごと、組織ごとに大きく異なる場合があります。

科学的なマインドセット

AIを採用し発展させるには、科学的なマインドセットを持つ組織と人が必要です。これは製品の最終化までの間に、試行錯誤を行い、失敗のリスクとテストを受け入れることを意味します。外部からの刺激やインプットデータを与え、アウトプットを観察することにより、製品の実現可能性を継続的にテストします。これは本質的には組織全体に「サンドボックス」（ビジネス環境を表す制御され孤立した環境）を作ることを意味します。このマインドの変化は、単にビジネスや機能の責任者だけのものではなく、取締役会や、リスクやコンプライアンス、人事、ITなどのその他の機能を含む、組織のあらゆる分野に関係しています。

3つのディフェンスライン（業務部門、リスク・コンプライアンス部門、内部監査部門）のすべてが関与することが特に重要です。コンプライアンスとコントロールの監督者として、「サンドボックス」へ全部門が参加することは、重要な技術的側面のいくつかを理解し、最初から適切なAIガバナンスとリスク管理の方針を形成するのに役立つでしょう。

企業リスクのカテゴリー	サブカテゴリー（例）	AIソリューションにおける主な考慮事項（例）
モデル	アルゴリズムリスク−バイアス	■ AIの意思決定は、継続的に与えられるデータセットに依存しているため、モデル内に固有のバイアスが生じていても特定することが難しくなります。 ■ 入力データに固有のバイアスがあると、不十分あるいは不適切なアウトプットが出力される可能性があります。 ■ データサイエンティストがバイアスを問題として考慮していないと、バイアスのリスクが最初から適切に対処されない可能性が高くなります。
	アルゴリズムリスク−不正確さ	■ 間違ったアルゴリズムが問題に適用されたり、データの品質が悪かったり、または、最適でないアルゴリズムパラメータが選択されたりすることがあります。
	アルゴリズムリスク−フィードバック	■ AIソリューションは継続的にフィードバックに基づいて学習することができるにも関わらず、不適切なフィードバックが提供され、それが検出されないリスクがある場合は、正確な結果を生み出す能力が損なわれる可能性があります。
	アルゴリズムリスク−誤った使用	■ ビジネスユーザーが複雑なAIモデルを十分に理解しておらず、AIの出力を誤って解釈すると、誤った結論を導く可能性があります。
テクノロジー	情報とサイバーセキュリティ	■ サポートがなく、更新されなくなったオープンソースコンポーネントへ依存することは、セキュリティの脆弱性をもたらす可能性があります。 ■ 複雑なアルゴリズムは、ソリューションがどのように最終的な決定に達したかを理解するのを難しくし、人間または他のシステムにより攻撃を受ける可能性があります。
	変更管理	■ AIソリューションへ学習データを提供する上流システムが変更された場合、その影響を特定することは困難です。これにより、AIとその周辺環境との相互作用において予期せぬ結果が生じる可能性があります。
	ITオペレーション	■ AIアプリケーションがビッグデータを利用していると、場合によって、既存のITインフラが対応できなくなる可能性があり、リスクが増大します（たとえば、ビッグデータを処理できないレガシーシステム等）。
規制とコンプライアンス	データ保護	■ 自動化された意思決定をめぐるデータ主体者の権利を含む、データ保護法（例：GDPR）に関連した侵害のリスクが増加します。
	規制、コンプライアンス	■ 複雑なAIアプリケーション（複雑な意思決定層からなるニューラルネットワークを使ったアプリケーションなど）で意思決定がどのように行われるかを理解し、規制当局に正当性を主張することが困難になります。
実行	文化	■ 実在する、または存在すると錯覚されている規制上および倫理上の懸念によって、大規模なAI導入において文化的な課題が含まれる可能性があります。 ■ 組織内で従来の仕事内容が変化することに関して、組織内で恐怖心や懸念が生じる可能性があります。
	製品の革新	■ 顧客のニーズを満たさない製品が開発されたり（たとえば、AIを使用するためにAIを使用すること）、営業担当者による誤った製品理解に基づいて広範囲にわたって製品が販売されたりする危険性があります。
人物	役割と責任	■ AIライフサイクル全体にわたって、役割、責任、説明責任が明確に定義されていない可能性があるリスクの増大。継続的な関与およびステークホルダー（コンプライアンス、ビジネス、IT、プログラマーなど）からの監視の欠如によって事態が悪化する危険性が高まります。
	採用とスキル	■ 利用されているAIソリューションを理解し、使用し、適切に運用するためのスキルが欠如、もしくは不十分であることはリスクを増大します。 ■ AIに精通した人材が組織へ文化的になじめないときは新たなリスクが生じます。 ■ AIの知識と専門性を備えた少数の人材へ過度に依存する危険性があります。
マーケット		■ マーケットにおける比較的少数の大手サードパーティーAIベンダーへの過度の依存はリスクの集中度を高め、仮にベンダーの一社が事業継続性を失ったり、重大な業務上の事故を起こしたりした場合にはネットワーク効果が発生する可能性があります。 ■ アルゴリズムが特定の変数（例えば株式市場の価格）に過度に敏感である場合、同調的な行動（すなわち、他の市場参加者と同じように行動する傾向）から生じるシステミックリスクが増大します。
サプライヤー		■ 「ブラックボックス」なアルゴリズムを使用すると、損害が発生した場合のAIのベンダー、オペレーターおよびユーザー間の責任が不明確になる可能性があります。 ■ 特に新規および小規模なAIのサードパーティープロバイダーの場合、十分なガバナンス構造と内部統制が整備されていない可能性があり、問題が発生するリスクが高まります。

リスクアペタイト

リスクアペタイトとは、組織が事業遂行のために受け入れ可能なリスクの総量です。リスク管理のプロセスと統制を効果的なものにするためには、AI導入戦略は、最初から全社的なリスクアペタイトと整合している必要があります。

同様に、AI特有の考慮事項に取り組むために、リスクアペタイトを見直す必要もあるかもしれません。AIソリューションの導入によって企業の全体的なリスクアペタイトが変化することはありませんが、その構成要素の相対的なバランスおよびそれらを管理するためのツールと手段は確実に変化します。

AIソリューションは、特定の種類のリスク（モデルリスクなど）を本質的に増減させ、組織の現在と将来の両方のリスクプロファイル（各リスクが有する特徴を表す様々な要素により構成されるものを総称していう）を変化させます。これは、リスクアペタイトをリスクタイプごとに再検討する必要があることを意味します。これには、目標とするリスクレベルだけでなく、そのリスクの効果的な管理と監視をサポートするポリシーと管理指標も同様に再検討することが含まれます。

企業がリスクアペタイトに基づいてAIのユースケースを評価するためには、最初にすべてのケースに適用できる明確で一貫した評価基準を作成する必要があります。例えば、「このAIソリューションは社外に公開するものか」といった質問で、これはAIのユースケースがどのような種類の実行上のリスクを有しているのか判断するのに役立ちます。標準的な質問リストを作成することで、企業はAIの個々のユースケースのレベルでも、全体で集計するレベルでも、どのリスク領域に焦点を当てる必要があるかを理解できます。

リスク管理フレームワークのライフサイクル

詳細や用語は企業によって異なりますが、概念的にはRMFライフサイクルは次の4つの主要なステージで構成されます。

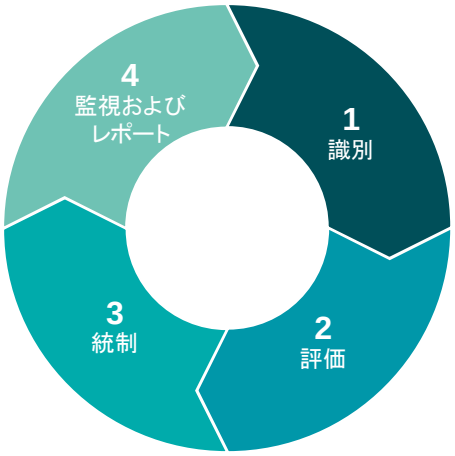
1. **識別**
   組織のビジネス戦略や業務に重大な悪影響を及ぼすリスクを特定することにより、リスク領域の全体像を理解します。また、この段階では、社内外の事業環境や規制環境をモニタリングし、固有のリスク環境の変化を特定し、リスク管理フレームワークが目的に適合しているかを確認します。

2. **評価**
   リスク評価プロセスを定義して組み込み、リスクの影響度を評価します。

3. **統制**
   固有リスクを軽減するための統制の枠組みを組み込み、リスクアペタイトで許容できる水準まで残存リスクを軽減します。

4. **監視およびレポート**
   統制の有効性を測定するための指標、リスク許容閾値および統制有効性に対する実証手続きを含む統制環境について有効性評価方法論を設計します。残存リスクプロファイル、統制環境およびリスク軽減プログラムの状況を、関連するガバナンス会議で報告します。

以下のセクションでは、RMFの各段階におけるAIの考慮事項のうち重要な部分を示し、保険会社の保険契約の価格設定のためのAIソリューションにおいて、企業がモデルリスクを管理する方法の例を示します。



1. 識別

金融サービス企業において、AIの複雑な性質および未成熟な部分は、いくつかのリスクが顕在化する方法およびその規模が徐々に、場合によっては非常に急速に増大する危険性があることを意味します。これは企業にとって、業務遂行と財務安定性の両方の観点から重要な影響が生じる可能性があります（例: 広範囲にわたり誤った製品説明で営業活動が行われるなど）。

そのため、企業はAIユースケースのリスクプロファイルを導入後、モデルの学習と進化に伴い変更が必要かを判断するために定期的な評価を実施する必要があります。

同様に、概念実証（PoC）または社内利用のみを目的として開発されたAIソリューションの使用が広まった場合にも再評価を必要とします。例えば、企業内部で助言を提供することのみを目的として最初に開発されたAIソリューションの使用を外部顧客への提供に拡大する場合、新たなカスタマージャーニーを通して生じるリスクを把握する必要があります。

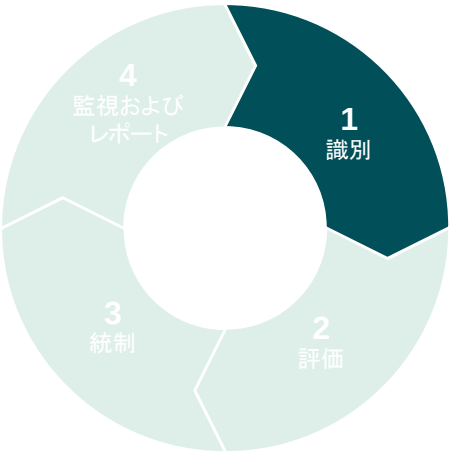
金融サービス企業において、AIの複雑な性質および未成熟な部分は、いくつかのリスクが顕在化する方法およびその規模が徐々に、場合によっては非常に急速に増大する危険性があることを意味します

AIの「定義」も進化し、リスクも進化することは注目に値します。例えば、携帯電話の「定義」と機能が拡大するにつれ、携帯電話に関連するリスクは時間とともに劇的に変化しました。

企業はAIリスクの考慮事項を既存のRMFにどのように統合できるか、またどの程度変更する必要があるかを決定する必要があります。このような考慮事項には、アルゴリズムに偏見（バイアス）が含まれるリスクや、AIがデータセットから因果関係がないにも関わらず相関関係を予測してしまうリスクなど、規制上および倫理的な意味合いの問題が含まれます。これは後の例で説明します。

なお一般的に、複雑で進化し続けるAIのユースケースでは、企業は、リスクを特定するためのガバナンスと方法論を確認し、リスクを特定するためにより包括的で継続的なアプローチを採用する必要があります。AIリスクの識別には、特定のAIユースケースの採用に関連するリスク（リスクプロファイリングアプリケーションに特有のリスクなど）や、より一般的なAIの採用を通じて組織全体に導入されるリスク（たとえば、従業員との関係や企業文化への影響）を含める必要があります。

AIソリューションから生じるリスクを特定するためには、より広範な組織への影響と、それが短期および長期的に組織の人的資源にとって何を意味するのかを考えることが重要です。



例）識別

- リスクプロファイリングAIモデルから生じる重要なリスクのひとつは、アルゴリズムに偏見（バイアス）が含まれるリスクやAIがデータセットから因果関係がないにも関わらず相関関係を予測してしまうAIの特性です。

- たとえば、AIの不動産保険における価格設定モデルでは、不動産の評価にさまざまな非構造化データを使用することができます。そのようなデータは、その地域のリスクプロファイルに1回限りのローカルイベント（カーニバルやデモなど）を取り込むことができます。これには多くのリスクが伴います。第一のリスクは、アルゴリズムが価格設定に使用する意思決定要因としてそのイベントの有無が選択されてしまうことです。です。第二のリスクは、その場所で発生した一時的なイベントがその場所固有の恒久的な要因として価格設定に含まれるようになってしまうリスクがあることです。

- さらに、同じデータが異なるAIモデルで将来使用される可能性があり、他のリスクプロファイルに誤って関連付けられ、影響する可能性があります。例えば、ソーシャルメディアの写真のタグ付け機能が前述のイベントの参加者または見物者と同時に映った写真を本人の同意なく利用することによって、AIモデルが同じ評価データを使用して評価した個人の自動車保険または旅行保険のプロファイルが無関係の別のユーザーに関連付けられ、影響を与える危険性があります。

- この例では、倫理的な考慮事項はもちろんのこと、データ保護、顧客の同意および価格設定の誤りなど、さまざまなリスクが発生します。バイアス、モデル、レピュテーション、規制に関するリスクは企業の新しいリスクではありませんが、AIのユースケースでは、新しい方法やこれまでに無い方法でそれらのリスクが明らかになり、識別がより困難になります。

2. 評価

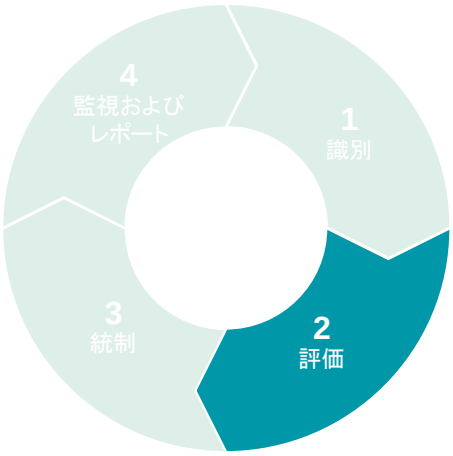
各AIユースケースの開発が始まる前に、リスク評価プロセスが設計され、経営者によって合意されている必要があります。このプロセスは、それぞれのユースケースのリスクに影響する可能性がある主な要因（規制、顧客、財務、またはレピュテーションへの影響）について慎重な検討を促すものでなくてはなりません。例えば、顧客に財務的なアドバイスを提供するAIソリューションに内在するリスクのレベルは、社内のスタッフにITトラブルのシューティングサポートを提供するソリューションのリスクのレベルとは異なります。

既存のリスクアペタイトと評価の枠組みは、AIソリューションが提起する質的な検討事項を包括的にカバーはしていないかもしれません。例えば、AIモデルのバイアスを評価するために、企業は最初に「公平性」などの概念を定義する必要があります。したがって、この文脈では、特に業務遂行とレピュテーションの観点から、公平性などの企業の価値観は、特定のリスクの性質を評価する上で基本的な役割を果たします。

さらに、AIモデルは時間の経過とともに進化する可能性があるため、企業は当初の定義と評価指標ではモデルの意思決定要因に適切に対応できない可能性があることに気付くでしょう。したがって、評価プロセスはより頻繁かつ動的に行われる必要があり、「ボトムアップ」（ユースケース毎）だけでなく「トップダウン」（全体的なリスクアペタイト）でも見直される必要があります。

また、評価プロセスにはビジネス部門の代表者だけでなくAI分野の専門家、テクノロジーリスクやコンプライアンスなどのリスク管理部門も含めた幅広い関係者からの参加と承認を取り付けることも必要です。

最後に、AIのユースケースではアジャイル開発アプローチが一般的ですが、多くのテクノロジー関連のリスク管理フレームワークは従来のウォーターフォールモデルに対応するように設計されています。したがって、従来の技術開発フレームワークを評価するために設計されたプロセス、ポリシー、ガバナンスは、より動的に変える必要があります。少なくとも高リスクのユースケースでは、実際には、開発段階全体にリスク関連部門を毎日関与させていく必要があるかもしれません。これは既存リソースを圧迫する可能性が高いと言えます。



例）評価

- 本保険ソリューションの例では、構造化および非構造化の両方のデータソースを数多く使用するAIソリューションを扱います。静的で識別可能な要因によって価格設定を決定するAIではないソリューションの結果と乖離しすぎることがないかどうかを評価し、差異の理由を理解することが重要です。例えば、商業向け不動産価格ポートフォリオの場合、非AIモデルはその不動産の物理的な特徴とその周辺環境のみを考慮しますが、AIモデルははるかに大きなデータのセットを含めることができます。

- 同様に、あるAIソリューションの価格設定の結果が別のAIソリューションのインプットになるような数多くのモジュールが連携するような環境では、各モジュールの結果は幅広いステークホルダーによって推測された意思決定要因の妥当性により評価されるべきであり、特にそれらが価格設定に影響するリスクと因果関係がないことをレビューして検証します。

- 評価には、モデルの技術的パラメーター（偏りや分類誤差）だけでなく、ビジネスの観点（顧客セグメントごとのポリシーの数など）および運用パラメーター（ポリシーが初期化されてから発行までにかかったスピードなど）も含める必要があります。

3. 統制

管理と検証のプロセスも、より動的である必要があります。実際には、AIソリューションの開発段階と初期データセットのトレーニングをはるかに超えて、AIソリューションの定期的かつ頻繁なテストと監視が必要になる可能性があります。

これにより、従来のテクノロジーソリューションと比較して必要なテストの量が増える可能性があります。組織のリスク評価の枠組みに合わせて、それに整合する各ユースケースの適切な統制レベルを決定するために、リスクベースのアプローチを使用します。

さらに、AIの採用が組織に与える影響は広範囲に及ぶため、関連する統制は複数の領域にまたがる可能性があります（例: 人事、技術、業務など）。このことは、リスク管理のライフサイクルを通じて、幅広いステークホルダーが関与する必要性をさらに重要なものとしています。

システムの利用不可やAIのコントロール不能状態（例えば、非常停止の発動）等の緊急事態において組織が通常の運用に復旧するために、事業継続計画（BCP）を再定義する必要があります。厳しいシナリオにアルゴリズムがどのように対応するか、あるいは非定型の動作が正しいエラーフラグを生成するかどうかを確かめるために、定期的にストレステストを行う必要があります。

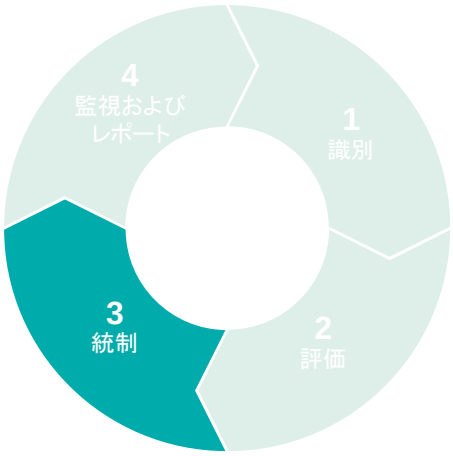
統制プロセスでは、AIがステークホルダー（顧客など）とどのようにやり取りするか、あるいはどのようなタッチポイントがあるかを検討する必要があります。企業にとって特に重要なのは、最初の関与からAIソリューションによって生み出される成果に至るまでのカスタマージャーニーをテストし、早期の段階で異常や異常値を特定し、必要に応じて修正するのに十分な頻度でテストすることです。

同様に、企業はアルゴリズムが事前に定義されたリスクの許容範囲内でアウトプットを生成できない場合（例えば価格が決定できない場合）のために、適切にコントロールされた「人の手による」プロセスも持っておくべきです。十分な信頼をもって案件の価格を決定できない場合は、それを人間に引き渡すべきです。

AIソリューションの開発段階と初期データセットのトレーニングだけではなく、AIソリューション開発の全体で定期的かつ頻繁なテストと監視が必要になる可能性があります

主要な精度評価指標は、学習で用いられたサンプル以外のテストデータにより評価されるよう設計されるべきです（すなわち、テスト担当者は正しい結果だと確認できている全く新しいデータを使用して、AIモデルを実行する）。新しい（または更新された）データセットに対しても、AIソリューションが期待どおりに機能していること、および会社のリスクアペタイトを保証するために、アルゴリズム（特徴量を含む）の頻繁かつ継続的なテストおよび統計分析を本番環境で実施する必要があります。

最後に、モデルのリスクを管理し透明性を高めるための方法のひとつとして、単一のより複雑なアルゴリズムではなく、より狭い範囲のより多数の小さなアルゴリズムを使用して最終的な出力を決定するモジュラーソリューションを構築する方法があります。これにより、推論や意思決定要因の特定が容易になり統制しやすくなります。



例）統制活動

- アルゴリズムは、意思決定要因の様々な結果を理解可能にするように訓練される必要があります。例えば、人工衛星による建物の亀裂の調査を行うための不動産保険価格決定アルゴリズムには、亀裂のある建物の写真だけでなく亀裂のない建物の写真も訓練データとして使用されるべきです。
- 評価のプロセスにおいて、AIを用いない価格設定システムとの差異（正であれ負であれ）が特定された場合、人によるレビューの要件またはその他のモデルによる制約を設定すべきです。
- 保険価格の算定モデルに関する統制は、データだけでなく、アルゴリズムの妥当性、関連性、精度まで含めるべきです。
  - アルゴリズムの精度－前述のように、モデルの精度をチェックするために、アルゴリズムの結果をAIを用いない価格設定システムの結果と比較してチェックする必要があります。さらに、価格設定のために生成されたリスクウェイトについて、アルゴリズムをさまざまなデータソースで学習させて一貫性があることをテストする必要があります。
  - アルゴリズムはモデルが新しいデータに適用されたときに出力が有効であり続けることを保証するために、異なるデータセットで学習され、テストされるべきです。色々な方法論が存在しますが、これを行うひとつの方法は、利用可能なデータセット（例えば過去の保険価格設定データ）を分割し、例えばデータの80%のみを用いてアルゴリズムを訓練し、残りの20%のデータで結果をテストすることで、結果の正確性と公平性を確認します。
  - アルゴリズムが学習データにおいて良好なレベルの精度を有することを確実にし、そして実データが連続的に供給された時に比較的安定したレベルの精度を維持できるよう統制活動が組み込まれるべきです。すなわち、アルゴリズムは、従来の価格設定基準を考慮しながら、可能な限り最良の保険契約の価格を提示することになります。
  - データ表現－異なる期間、異なるデータソースに対して同じアルゴリズムをテストし、データによって発生しているバイアスをチェックします。さらに、偏ったデータをアルゴリズムに入力し、結果がバイアスを反映しうるかどうか確認します。

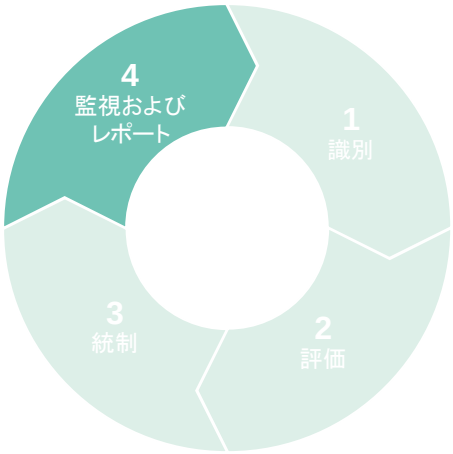
4. 監視とレポート

学習アルゴリズムは絶えず進化しており、モデルが特定のユースケースに合わせて意図した通りに動作していることを確認するため、より動的な監視アプローチが必要です。

さらに、AIソリューションに関連する限界と目標（例：KPI（主要業績評価指標））は、適切性、妥当性、および正確性の観点で、より定期的に監視される必要があります。

モニタリングとレポートは、モデルの技術的パフォーマンスと、それにより達成されたビジネス上および運用上の成果の両方を対象とすべきです。

また、モニタリングの対象にはモデルの設計変更を必要とするすべての法的および規制上の動向や、モデルが利用するデータに間接的に影響を与え、結果に影響を与える外部事象も含める必要があります。AIを用いないモデルもまた、これらの外部動向の影響を受けますが、その場合は意思決定の要因と、その結果への影響は比較的容易に特定できます。AIソリューションにおける意思決定要因は絶えず進化するため、意思決定要因に対する外部事象の影響を特定し、評価し、監視することは困難といえます。



学習アルゴリズムは絶えず進化しており、モデルが特定のユースケースに対して意図した通りに動作していることを確認するため、より動的な監視のアプローチが必要です

例）監視とレポート

- 企業は、アルゴリズムのモニタリングのために明確で正確な成功指標／KPIを定義すべきです。指標には、会社の公正さと差別禁止の方針を含めるべきです。例えば、単純な指標は、サンプル外テストで誰かがあるポリシーにおいて拒否された回数です。テスト中に特定のグループの人々が一貫して拒否された場合、ある程度の偏りがある可能性があります。
- 事前に定義された成功指標でアルゴリズムを評価する必要があります。すなわち、企業は、使用されたアルゴリズムが明白な成果をもたらしたかどうか、および悪影響を打ち消すための明白な措置が取られたかどうかを評価すべきです。
- 関連するスタッフは、保険契約の価格設定モデルの設計に影響を及ぼす可能性のある潜在的な市場や規制の変更を監視する必要があります。例えば、社会的立場の弱い顧客層の公正な扱いを強化する規制は、差別的なアウトプットにつながらないようにするためのアルゴリズムの改正を必要とします。
- 不公平な扱いをされたと考える顧客からの苦情は、アルゴリズムのレビュープロセスに含まれ、必要に応じてアルゴリズムの変更が行われなければなりません。
- モデルの性能にかかる継続的な分析は、人の手を介して行われるべきです。
  - エッジケースの分析・・・ポリシーに関して単に拒否されただけの人と、ポリシーに関して単に承認されただけの人との比較
  - 検証後のモデルへのフィードバック補正
- モデルを供給するデータセットに根本的な変化がないことを保証するために、入力データの分布を分析すべきです。
- ビジネスKPIには、AIモデルとAI以外の価格モデルによる保険料の値、損失率、売上原価および総利益の比較などの指標を含める必要があります。
- 価格の上昇によって特定の顧客グループが大幅に減少することがないように、また、顧客が平等に扱われていないために特定の顧客グループからの利益が大幅に増加しないように、利益とポートフォリオの組み合わせをモニタリングします。
- 運用監視には、AIシステムが保険会社へ出力しているトランザクション量およびAIソリューションがポリシーを出力しているスピードなどを、AIを用いないシステムと比較することなどを含めるべきです。

5. 規制当局は何を求めているのだろうか？

規制産業の企業がAIの利用の影響を理解することは、すでに規制当局と監督当局における議題として社会的に認識されており、それは国際機関、EUや英国当局が発表したスピーチやレポートの数が示しています。

一般的に、AIを採用しようと計画している企業、あるいはすでに利用している企業は、監督者から求められる精査のレベルが今後高まると予想しています。

AIについて規定された一般的な規則はまだありませんが、アルゴリズム取引の使用、内部リスク評価モデルの監督に関する英国のSenior Managers and Certification Regime（SM&CR）のシステムと統制に関する既存のルールは、AIに関するガバナンスとリスク管理に関して、規制当局と監督当局がどのような規制を発する可能性があるかについての良い手がかりとなります。

これらの資料およびクライアントとの私たち自身の経験に基づいて、AIを採用する際に企業が考慮すべきいくつかの重要な規制関連の原則および措置の概要を提示しました。これらの原則の大部分は、アルゴリズム取引の十分に発達した使用事例から導き出されたものです。これら考慮事項が他のAIのユースケースにどの程度当てはまるかは、その性質と複雑さによります。

AIを採用しようと計画している企業、あるいはすでに利用している企業は、監督者からの精査のレベルが今後高まると予想しています

ガバナンス、監督および説明責任

- 監督当局は、企業がRMFを含む堅牢で効果的なガバナンスを実施し、各AIアプリケーションの開発およびそのビジネス全体での継続的な使用において、関連するリスクを特定し、低減し、コントロールすることを期待します。
  RMFは取締役会によって承認されるべきであり、企業はそれぞれのAIアプリケーションがどのように機能し、適用可能な規制要件および企業のリスクアペタイトにどのように準拠しているのかを、監督者に説明できるようになる必要があるでしょう。

- AIは急速に進化するものであり、組織内でAIソリューションの採用は普及していくため、リスクエクスポージャーおよび関連する統制は定期的に見直して、それらが会社のリスクアペタイトと一致しているか確認する必要があります。これには、組織内でのAIの使用範囲、組織内部のAI利用能力、脅威や外部のイベントなどの要因も考慮が必要です。

- 説明責任体制、特に英国のSM&CRに沿って、監督当局は各AIアプリケーションについて明確に所有者を識別し、企業が明確な責任と説明責任を持つことを期待するでしょう。所有者はまた、正確性、公平性、または法令遵守に影響を与える可能性のある関連要因（市場や法規制の変更など）を識別した時には、AIアプリケーションのレビューと見直しを行う責任があります。

- ガバナンス委員会のメンバーは、AIアプリケーションに関連するリスクを理解する訓練が必要であり、品質保証指標を含むテストと承認プロセスを確立し、AIアプリケーションのパフォーマンスを定期的にレビューして、新たな問題を特定すべきです。

- 効果的なAIガバナンスには、組織全体のより広範なステークホルダーを含めます。特に、主要な開発とテストのステージでは、第一、第二、第三のディフェンスラインの関係者に加えて、AI専門家を含めるべきです。

効果的なAIガバナンスには、AIの使用が企業全体に及ぶ可能性のある広範囲な影響を反映して、組織全体からより幅広い一連の利害関係者を含める必要があります

- また、エラーや異常な動作が検出された場合に直ちにアルゴリズムを停止できるようにするため、企業はマニュアルに”kill-switches（停止スイッチ）”や”exit chutes（避難経路）”に関連する手順や統制を文書化する必要があります。また、企業はそのような統制の使用に関するガバナンスプロセスを整備し、これには、事業継続性および変更申請を含める必要があります。

- すべてのAIアルゴリズムは、定期的に再検証される必要があります。このようなレビューの頻度は、アルゴリズムが機能不全に陥った場合に、企業やその顧客、その他の市場参加者がさらされる可能性のあるリスク量によって異なります。レビュー頻度の決定には、アルゴリズムが時間の経過とともに進化、学習する程度と、出力結果に大きな影響を与える重要な要因（例えばマクロ経済指標の変動性等）を考慮に入れるべきです。

制御機能の能力と機能

- 企業は、リスク、コンプライアンス、内部監査チームの各スタッフが、採用された各AIソリューションに関連するリスクを適切に理解するための十分な専門知識を持っているかを確認する必要があります。さらに、所管するビジネス部門に異議を申し立て、必要に応じて、効果的なリスク管理のために追加的な統制を課す権限を与えられるべきです。

- 特にリスクとコンプライアンスの部署は、新しいAIアプリケーションの開発と導入プロセスの重要な段階で関与し、適切なリスクコントロールを確立するためのインプットを提供します。また、それが企業のリスクアペタイトに適合しているかどうかを判断し、潜在的なコンダクトリスクと規制上のリスクに関連する独立したチェックを行います。

- 内部監査部門は、AIのアプリケーションとモデルのレビューが監査計画プロセスの一部であることを確認し、さらに継続的な監視が必要かどうかを検討する必要があります。

文書化と監査証跡

- 企業は、組織を通じて展開されたすべてのAIアプリケーションおよび関連する所有者、ならびに主なコンプライアンスやリスク管理の活動を明確かつ完全に把握している必要があります。

- テストおよび承認プロセスは、AIモデルが実際の環境に実装される必要条件についての明確な説明を含めて文書化されるべきです。

- 同様に、監督当局は特定された問題を監査可能なガイドラインに沿って追跡および管理するためのプロセスが企業に整っていることを期待します。

- 最後に、既存のアルゴリズムに対する変更も明確に文書化されるべきです。企業は、重要な変更となるものを定義し、すべての基準がビジネス全体に一貫して適用されるようにする必要があります。いかなる重要な変更も、厳格に文書化されテストの対象となるべきであり、その範囲は、変更が企業を危険に晒すリスクに見合うものでなければなりません。

規制を受ける企業は、いかなる状況においても、規制上の義務を果たす責任を第三者に委託することはできません

第三者リスクとアウトソーシング

- 規制を受ける企業は、いかなる状況においても、規制上の義務を果たす責任を第三者に委託することはできません。同様に、外部ベンダーによって設計、提供されているAIモデルや関連するリスクコントロールは、導入前に社内で開発されたものと同じ厳格なテストおよび監視を受ける必要があります。

- 企業は、第三者のプロバイダーが開発したAIソリューションが機能しなくなった場合や、プロバイダーがサイバー攻撃の結果などでサービスを提供できなくなった場合に備えて、業務を継続するための効果的な事業継続性の取り決めを設計する必要があります。現在市場に存在する第三者のAIプロバイダーは、スタートアップを含めて少数のため、特に重要です。

AIとGDPR

企業は、AIソリューションを使用して、顧客のニーズに合わせてカスタマイズされたサービスや製品を設計したり、顧客の個々のリスクプロファイルをより効率的に決定するようになってきています。

これらのテクノロジーを活用できるかどうかは、関連する大量の顧客データが利用可能なことが前提となります。GDPRが適用されると、データ保護要件への準拠を維持しながら企業の顧客のデータを使用する能力が求められます。

GDPRは、企業が個人データをどのように利用しているかを消費者が理解し管理するための新たな権利を提供します。ビジネスモデルが顧客の個人データの一括処理に依存している企業（AIソリューションを使用しているかどうかにかかわらず）は、2018年5月までに適切に準備する必要があります*訳者注。これはつまり、監督プログラムが開始された時点で監督当局を満足させることができ、また重要なことは、顧客からの問い合わせに有意義で透明性があり理解しやすい方法で返答できることが求められているということです。

個人に大きな影響を与える決定がAIによって下された場合、GDPRは彼らがその決定に異議を申し立てる権利とその説明を要求する権利を持つことを義務付けます。

（英国の情報コミッショナーElizabeth Denham、下院科学技術委員会への口証、2018年1月*6）

2018年5月のGDPRの施行までに防御可能な状態にするためには、企業は、顧客の個人データを処理するAIアプリケーションのデータプライバシー影響評価を、その進展に合わせて完了する計画を持つ必要があり、必要に応じて、継続的なコンプライアンスを確保するための改善計画を策定する必要があります。

より一般的に言えば、企業はアルゴリズムの説明責任と可監査性の原則を採用すべきです。これらの原則では、アルゴリズムがデータ保護要件に準拠していることを実証するための組織的プロセスと技術的プロセスを整備し、第三者がチェックしレビューできるようにする必要があります。最後に、重要なことですが、企業は、加工に使用されるデータが、使用が合法でありバイアスがないというテストに適合することを保証する必要があります。

規制当局として、フードの下やカーテンの後ろを見て、予測ではどのデータが使用されたか、学習ではどのデータが使用されたか、システムにプログラムされた要因やAIシステムが答えるように訓練された問題設定を確認する必要があります。

（英国情報コミッショナーElizabeth Denham、下院科学技術委員会への口頭証拠、2018年1月）

GDPRでは、企業レベルでも業界レベルでも、データ保護の監督機関との関係を調整する必要があります。つまり、企業は、データ保護の監督機関と定期的に打合せを行い、データプライバシー戦略や、計画されているリスクの高い自動データ処理について議論するために、より構造化され、適切な予算をもつ規制担当チームを設立する必要があるということです。

*6：http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/oral/77536.html

*訳者注：本稿の原文は2018年4月に発行

6. AIの規制

AIの利用が増加することの影響とリスクを理解することは、金融機関だけではなく、規制当局や監督当局にとっても課題です。規制当局や監督当局は、AIがより良いサービスとカスタマイズされたサービスの形で、金融市場の効率性を高め、消費者に利益をもたらすことを認識しています。実際、規制当局や監督当局自身も、自らの仕事でAIを使う方法を模索しています。

しかし、先に述べたように、規制当局は、規制対象企業によるAIの使用がもたらす潜在的なリスクや意図しない結果にもますます注意を払うようになっています。金融の安定性の観点からは、潜在的なネットワーク相乗効果の影響およびサイバーセキュリティが主要な懸念事項の一部です。コンダクトリスクの観点からすると、規制当局は、顧客の不公正な扱いや、不正確なAIモデルに起因する誤販売の可能性、データの処理方法について顧客が理解していないこと、財務上小口の投資家に対する排除が増加していること、脆弱な顧客にとってマイナスの結果となることに留意しています。

企業の場合と同様に、これらのリスクのほとんどは規制当局にとって目新しいものではありません。規制当局がAIや、より一般的な革新的技術に関して直面している課題は、有益な革新と競争を支援し、顧客を保護すること、市場の健全性、そして金融の安定性との間で適切なバランスを見出すことです。

このようなバランスをとることは、新しい技術が発展し採用されるペースと、新たな規制が開発され実行されるスピードが一致しないため特に困難になります。例えば、金融商品取引に関する第2次市場指令（MiFID II）は、金融市場におけるアルゴリズム取引の利用の増加に対処するため、2011年に初めて提案されましたが、適用は7年後の2018年1月でした。

規制当局はこの遅れを意識しており、歴史的には「技術中立性」という原則を採用して、この問題に取り組んできました。つまり、規制活動を行うために使用する技術に関係なく、同じ規制原則が企業に適用されるということです。技術的に中立な規制は、ルールがすぐに時代遅れになるリスクを減らすのに役立ちますが、個々の技術やユースケースに特有のリスクに対処する規制当局の能力を妨げることもあります。

ただし、特定のテクノロジーの使用が体系的に重要になる、またはその可能性がある場合は、規制当局がそのテクノロジーの中立的な立場から脱却する準備をしている兆候がいくつかうかがえます。アルゴリズム取引に関するMiFID IIの規則[*8]はその一例です。

また、規制当局がロボアドバイス[*9]、クラウド[*10,11]へのアウトソーシング、そしてまた最近ではアルゴリズム取引[*12]など、企業に対する期待を明確にするための詳細かつ技術固有のガイダンスを発行するようになっています。

技術的に中立的な規制は、ルールがすぐに時代遅れになるリスクを減らすのに役立ちますが、それはまた個々の技術とユースケースに特有のリスクに対処する規制当局の能力を妨げるかもしれません

*7: https://www.fca.org.uk/mifid-ii/1-overview
*8: http://ec.europa.eu/finance/docs/level-2-measures/mifid-rts-06_en.pdf
*9: https://www.fca.org.uk/publication/consultation/cp17-28.pdf
*10: https://www.eba.europa.eu/-/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions
*11: https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-%E2%80%98cloud%E2%80%99-and-other-third-party-it
*12: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2018/cp518.pdf?la=en&hash=89AB31B883DF430E36387BACCC93F15FC7A75A4A

AIに関しては、規制当局のガイダンスは、企業がリスク管理アプローチに関する監督当局の期待を理解するのに役立つ強力なツールであると考えられます。これにより、統制機関や上級管理職は、イノベーション計画を推進するための自信を深めたり、対処すべき問題を特定したりすることができます。また、よりAIに特化したガイダンスは、監督活動の一貫性を高め、業界全体のコンプライアンスのギャップや残存リスクを特定する能力を高めるため、監督当局自身の作業を容易にします。

課題は、真に効果的であること、すなわち、監督当局が、企業に対して、既存の規制制度をどのように遵守することを期待しているかについて十分な情報を提供するためには、いかなるAIガイダンスも、一般的なものではなく、各ユースケースに特化したものである必要があるという点です。
最近のプルデンシャル規制当局によるアルゴリズム取引に関する監督上の声明で述べられている原則のいくつかは、他のAIアプリケーションに関連していますが、それらの真の力はアルゴリズム取引[*13]活動への特異性にあります。AIのユースケースの幅と複雑さを考えると、規制当局はリスクに基づくアプローチを使用して、自分の限られたリソースに焦点を合わせる場所を慎重に選択する必要があります。規制サンドボックス、Tech Sprints[*14]および業界のラウンドテーブルは、規制当局がそれを効果的に実行できるようにするため、引き続き不可欠です。

規制当局の枠内にあるもうひとつの役割は、対処すべき問題を定義することですが、関連するAI基準と行動規範の策定を業界に求めています。これは、英国の競争市場局が、9つの大手銀行にOpen Application Programme Interfaces規格の開発を求めた際に行ったリテール・バンキング調査の結果と似ています。このようなアプローチは、英国の情報委員会が支持しているように思われます。情報委員会は最近、AIとデータ保護の観点から、業界によって策定され、関連する規制機関によって認証された業界固有の行動規範が、今後進展の可能性が高いと説明しています。

最後に、AIの規制は、単に金融業界にとっての課題ではなく、地理的な境界に限定することもできません。規制当局および監督当局は、国や分野の境界線を乗り越え、新たなリスクに効果的に対処する政策を開発するだけでなく、より広範な公共政策および倫理的懸念に対処するために、幅広い関係者と協力する必要性が増しています。

規制当局の枠内にあるもうひとつのツールは、対処すべき問題を定義することですが、関連するAIガイドラインと行動規範の策定を業界に求めています

*13: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2018/cp518.pdf?la=en&hash=89AB31B883DF430E36387BACCC93F15FC7A75A4A
*14: https://www.fca.org.uk/firms/regtech/techsprints
*15: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/600842/retail-banking-market-investigation-order-2017.pdf
*16: https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2017/algorithms-in-decision-making-17-19

7. まとめ

AIは、より良い顧客サービスを提供し、運用効率と有効性を改善し、競争優位性を獲得するために、多くの金融サービス企業の戦略の中核的な要素となりつつあります。

しかし全体としては、金融サービスでのAIの採用はまだ初期段階にあり、企業は依然として、テクノロジーや個々のビジネスモデル、製品およびサービスにどのユースケースが最も大きな価値をもたらす可能性があるかについて学んでいる段階です。

この学習プロセスの重要な部分は、リスクの観点からAIの影響を理解することにあります。これは、金融業界がいかに広範に規制されているかを考えると、ビジネス上の必要条件であるだけでなく、規制上の必要条件でもあります。

企業にとって重要なのは、これが双方向の学習プロセスであることを認識することです。すなわち、取締役会、上級管理職チーム、事業部門と管理部門はAI対する理解を深める必要があります。一方、AIの専門家は、リスクと規制の観点を理解する必要があります。このように部門横断的なチームを特定し、協働を奨励する金融サービス企業は、AIの利点をよりうまく活用できるでしょう。

この「パートナーシップ」により、企業は、よく知られているリスク（バイアスなど）の顕在化の仕方や実現するスピードと強度において、AIがいくつかの重要な違いをもたらすことを認識することができます。このことは、AIを採用する際、企業はAI特有の考慮事項を既存のRMFにどのように統合するかを慎重に検討する必要があることを意味し、企業の文化とリスクアペタイトによって設定された範囲内でAIに関連するリスクを効果的に特定し管理できるという確信を得ることができます。

規制当局はまた、金融サービスにおけるAI採用の潜在的なリスクと意図しない結果、そして有益なイノベーションと競争の支援と顧客の保護、市場の健全性および財務の安定性との間の正しいバランスを見つけるという課題にますます注意を払う必要があります。場合によっては、現在の技術的中立的立場からの逸脱、または特定のアプリケーションに対するAI標準規格および行動規範の策定を求めて業界と協力することを求めること等が必要です。

我々はまた、AIの規制の課題が金融サービスに特有のものではないことを認識すべきです。AIの広範な利用から生じる長期的な社会的・倫理的意味合い、及び適切な政策対応が何であるべきかについて、産業界と規制当局の双方が協力し、国境を越えた、横断的な議論がなされることを期待します。

企業にとって重要なのは、これが双方向の学習プロセスであることを認識することです。すなわち、取締役会、上級管理職チーム、事業部門と管理部門がAIに対する理解を深める必要があります。一方、AIの専門家は、リスクと規制の観点を理解する必要があります

コンタクト

神津 友武
パートナー
有限責任監査法人トーマツ
Deloitte Analytics
tomotake.kozu@tohmatsu.co.jp

福島 雅宏
パートナー
有限責任監査法人トーマツ
アシュアランス
masahiro.fukushima@tohmatsu.co.jp

染谷 豊浩
ディレクター
有限責任監査法人トーマツ
Deloitte Analytics
toyohiro.sometani@tohmatsu.co.jp

執筆者

Tom Bigham
Director, Risk Advisory
Technology and Digital Risk Management Lead
tbigham@deloitte.co.uk

Valeria Gallo
Manager, Risk Advisory
EMEA Centre for Regulatory Strategy
vgallo@deloitte.co.uk

Suchitra Nair
Director, Risk Advisory
EMEA Centre for Regulatory Strategy
snair@deloitte.co.uk

Michelle Lee
Manager, Risk Advisory
Artificial Intelligence
michellealee@deloitte.co.uk

Sulabh Soral
Director, Consulting
Artificial Intelligence
ssoral@deloitte.co.uk

Tom Mews
Manager, Risk Advisory
Technology and Digital Risk Management
michellealee@deloitte.co.uk

Alan Tua
Director, Risk Advisory
Artificial Intelligence Lead
altua@deloitte.co.uk

Morgane Fouché
Senior Associate, Risk Advisory
EMEA Centre for Regulatory Strategy
mfouche@deloitte.co.uk

Deloitte. トーマツ.

デロイト トーマツ

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームであるデロイト トーマツ合同会社およびそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイトトーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレートソリューション合同会社を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約40都市に約11,000名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイトトーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクアドバイザリー、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスをFortune Global 500®　の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約245,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細はwww.deloitte.com/jp/aboutをご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001