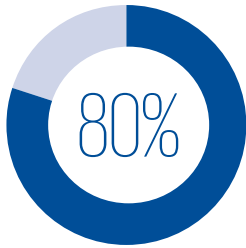




AI コンプライアンスを コントロールする

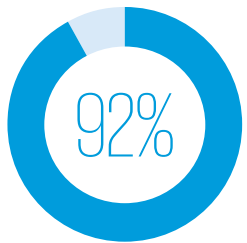
ファイナンシャルサービス
規制上の課題

金融業界が人工知能 (AI) システムと アドバンスド・アナリティクスの採用を加速させており、 規制上およびコンプライアンス上の新たな課題が生じています。



のリスク専門家が、AIに関するガバナンスの適切さに確信がもてないと述べました。

—120人以上のリスク専門家を対象に
KPMGが実施した調査



の企業がデータとアナリティクスの信頼性に疑問を感じ、評判への影響を懸念しています。

—KPMGの最近のレポート
Guardians of Trust



の企業だけが、コンプライアンス自動化への明確に定義された全社戦略を策定しています。

—KPMG Compliance
Automation Survey 2018

企業はAIを通じて明確に、オペレーションおよびコンプライアンスのプロセスと分析に関する効率性および実効性を、進化し続けるデータとモデル・トランスフォーメーションによって高め得るチャンスを手にかけています。一方AIは、ガバナンスおよびコントロールにおいて、現状および将来にわたって、対応しなければならない規制およびコンプライアンス上の課題（既存の規制とAIのみを対象とした規制の両方）を有しています。

加えて、多くの金融機関はアドバンスド・アナリティクスおよびAI関連の技術利用の迅速な展開や拡大に関して、第三者ベンダーに依存しており、それがまた、ガバナンスおよびアカウントビリティの領域で新たな問題とリスクを生じさせています。

米国の規制当局は、特に、AIの利用が消費者にアクセスおよび利便性の拡大をもたらし、オペレーション効率化、リスク検知、正確性向上をもたらす限りにおいては、「責任ある」AI利用の進展を妨げたくはないと表明しています。米国の規制当局は主に監督に重点を置いており、AIに関する公共政策はテクノロジーの発展よりも遅れています。一部のケースでは、規制当局が業界と協力して、AIおよび関連テクノロジーの「変革の加速」を支援する一方で、引き続き安全性、健全性、消費者保護に重点を置いています。アドバンスド・アナリティクスとAIソリューションがもたらす固有のリスクを評価するために、現在、規制当局は、既存の法令がシステムのアウトプットを評価するためのパラメータの定義や、「ガードレール」の設定を検討しています。これによって、また、規制当局の高い期待がすでに向けられている領域にかかわるAIソリューションに規制当局の関心が集中しています（次ページの図をご参照ください）。

本稿では、規制当局の高い期待がすでに向けられている領域における、ビジネス推進のドライバーと企業が取り得るアクションを概説します。

AIシステムおよびアドバンスト・アナリティクスに関する規制およびコンプライアンス上の課題



AIは、フィンテック・ソリューションと新興テクノロジーといった、より広いカテゴリーのなかの一分野です。世界的には、規制当局や監督当局がフィンテック関連リスクへの具体的な対応を講じ始めており、国際基準や原則の策定、国内規則および指針のいっそうの詳細化や規定の追加、監督上の優先順位の変更などが進められています。しかし、AIに関しては依然として、次のような課題があります。

AIとは何か? 人工知能とは、一般的に知的生物とかかわる業務を遂行できるテクノロジーです。AIの鍵となる要素は一般的に、知覚、学習、推測、推論などを含みます。

AIはRPAではない。 RPA（ロボティック・プロセス・オートメーション）とは、以前は人間が行っていた業務をハードコード／設定されたソフトウェアによって自動化するアドバンスト・オートメーションを指します。このプロセスは、人間がコードを変更しない限り、同一のプロセスのままです。



不揃いな規制



AIを含むフィンテックの発展により、さらなる規制、あるいはより詳細な規制が必要となる可能性のある新たな領域が継続的に注目を集めています。さらに、ますます増大する金融およびそれ以外のデータを収集・共有する全体的傾向により、さまざまな活動主体が設立されています。

規制当局および監督当局は、国内および国際的にデータの収集、保存、共有、使用に関して適切なフレームワークが導入されているかどうかを議論しています。しかし、公共政策は新たなテクノロジーの開発および展開に対して、遅れをとっています。大手金融機関は、少なくとも最初は、金融サービスセクターに参入した、多くの非金融企業やスタートアップ企業と異なる種の規制や監督を受けることになります。時間の経過とともに、これらの違いは解消されるかもしれません。現在のところ、金融サービスに限定されない規制を含め、AIに影響を及ぼす規制活動が州、連邦、世界の法域に導入されており、ノンバンクの監督や金融安定化、オペレーショナル・レジリエンス、サイバーセキュリティ、消費者保護に対応しています。

見通しとして、制定された規制および監督は、具体的活動をどこに置くかを含めて、企業戦略やビジネスモデルに影響を及ぼす可能性があります。

ドライバー

- テクノロジーの急速な進展により、金融商品およびサービスに関するアクセスと提供チャネルの再構築がもたらされる。
- 公共政策は新たなテクノロジーの進展に遅れをとっている。
- 連邦、州、海外法域は独立に活動。非金融サービスの規制当局も含め、複数の規制当局がデータ、テクノロジー、テクノロジー・プロバイダーに対する管轄権を有する可能性がある。

アクション

- **既存の「予備規制」を適用**：既存の法令を来るべきAIに対する予備的規制として認識する。
- **他の規制、方針、原則を考察**：AIに関連し得る将来のパラメータの事例として、他法域における政策や規制を考察する。
- **規制改正を監視**：AIに適用される新たな法令その他の要件を特定する。

規制対象分野：公共政策はテクノロジーの発展に遅れをとっています。規制当局は既存の規制要件が「ガードレール」となることを期待していません。州、連邦、グローバルのレベルでは規制要件が異なります。

カリフォルニア州「消費者プライバシー法」、EU「一般データ保護規則 (GDPR)」、ニューヨーク州金融サービス局 (NY DFS)「サイバーセキュリティ規則」、「国家サイバー戦略」、米国通貨監督庁 (OCC)「フィンテック・チャーター」、ノンバンクに関する米国財務省報告書、SECレギュレーションSPおよびS-ID、米国金融取引業規制機構 (FINRA)「サイバーセキュリティ慣行に関する報告書—2018年」



規制当局の見解

一般的には、AIを用いて提供される商品の規制へのアプローチは、(中略) リスク面の評価により情報が提供されるべきです。

リスクが既存の規制体制の範囲内にある場合は、(中略) 政策議論は既存の規制がすでに十分にそのリスクに対応しているか、あるいはAIが加わったことでそれらの規制を変える必要があるかということから始めなければなりません。

— 大統領府国家科学技術会議 (NSTC)
「人工知能の未来に備えて」(2016年10月)

米国のAIへの取組みの一環として、連邦政府当局もまた、新たなAI利用を統治するための規制およびそれ以外のアプローチを模索し、公衆の信認の構築に努めることになるでしょう。この目的のために、ホワイトハウスは(中略) 規制当局およびその他の利害関係者と協力し、プライバシー、市民の自由権、アメリカの価値観を尊重しながらも、イノベーションを推進するAIテクノロジーに関する指針を策定していきます。

— 大統領副補佐官マイケル・クラツィオス、
2019年2月11日の「人工知能における米国の
リーダーシップ維持に関する大統領令」に続く
Wired.comの論説 (2019年2月11日)





リスクガバナンス・コントロール



規制および監督当局は、企業が全社にわたるリスクを特定、管理、測定、コントロールするとともに、これを効果的に行うための適切な資源、スキル、専門性を持つという中核的リスクガバナンスの能力に対して、新しいテクノロジーがどのような影響を及ぼすかに注目しています。

企業には、強力な変更管理能力を持つことが期待されるでしょう。また、リスクガバナンスのフレームワーク（たとえば、企業、戦略、評判）とともに、サード・パーティ・リスク管理（必要に応じた外部依存度の調整）やIT / データガバナンス（テクノロジーリスクとモデルリスクの検証を含む）のフレームワーク、AIソリューションを管理するスキルを持つ人材、明確なアカウントビリティも必要です。

ドライバー

- 規制の中心は倫理とコンダクト、消費者保護、評判リスク、戦略リスクである。
- サード・パーティおよび外部データソースへの依存が高まっている。

アクション

- **プログラム・ガバナンス部門の設立**：AI関連の方針を含むべく既存方針の見直しおよび修正を監督する。ガバナンス部門には、リスクおよびコンプライアンスからの代表者を含めるべきである。
- **リスク低減へのコントロールの確立**：AIリスク・プログラムを既存のリスク管理プログラムに整合させる。
- **リスク管理プログラムの統合**：業績ベースの領域、リスク機能、規律全体にわたり、サード・パーティ・リスク管理を統合する。
- **AIの独立評価を実施**：独立評価を実施し、プログラム・スポンサー、経営陣、その他の利害関係者がAIプログラムの結果および成果を評価できるようにする。

規制対象分野：モデルリスク管理、サード・パーティ・リレーションシップ、外部委託リスク、オーナーシップ / アカウントビリティ、デジタルレイバー、ノンバンク規制 / 監督、取締役会による監督 / リスク・アベタイト

“

規制当局の見解

私たちの監督対象である大多数の銀行は、AIを駆使するプロセスを活用するために、ノンバンク・ベンダーの専門性、データ、既成のAIツールに依存せざるを得ないでしょう。

モデルリスク管理に関する連邦準備理事会の指針は、AIのような複雑なアルゴリズムを含むモデルの開発、実装、使用を通じて、埋め込まれる重要な分析の安全性と健全性が重要だと強調しています。また、当該モデルの開発、実装、使用と無関係な、バイアスのない、無資格の個人の「第二の目」による、モデルへの「効果的な異論」も強調しています。

— 連邦準備制度理事会理事、ラエル・ブレイナード
「金融サービスにおける人工知能について何を学ぶか」
(2018年11月13日)

”



データ・プライバシー



企業は既存のデータ保護要件を満たすことを求められる一方で、フィンテックの発展により、データ・プライバシー、セキュリティ、保護に関する金融サービス規制当局およびより一般的なデータ保護監督当局の考え方が根本的に変わる可能性に対して、プロアクティブなアプローチをとる必要もあります。加えて、データ漏洩事件が注目を集めるなか、現在、こうした問題を懸念する数百万人の顧客が自分たちの個人情報を、よりしっかりと管理（その収集、使用、保持に関して）できる方法を求めており、企業は規制要件とは独立に、オプトインおよびオプトアウトの手続きや収集するデータの範囲、アクセス方法、誰がどのように使用し共有するかに関する方針を再考するよう迫られています。

AIに関しては、データ・プライバシーおよびデータ・セキュリティへの公衆の意識の高まりにより、AI利用のための大規模かつ、または広範囲のデータセットの使用が困難になる可能性があり、データ使用が制限されたり、機械学習に影響が及んだりする可能性があります。金融機関は使用するデータセットのソースおよび内容を理解し、その使用に影響を与え得るアクセス、共有および制限にかかわる潜在的リスクを評価しなければなりません（たとえば、モデル検証、引受業務、公正貸付、販売慣行）。

ドライバー

- **利用可能なデジタル・データの増大**：フィンテック・アプリおよびデータ・アグリゲータの役割が増大している。
- 高度に相互接続した金融システム
- データ保護に関する消費者の意識／期待の高まり

アクション

- **AIの結果および判断を導出するのに使用されるデータおよびアルゴリズムに関するガバナンスの確立**：システムの学習に使用されるデータが安全に保存され、適時に読み出せるようにする。
- **アカウントビリティの確立**：AIのためのデータ管理者を設置し、コンプライアンスを証明できるようにする。
- **データ保護リスクの包括的評価を遂行**：個人情報を取得／処理するためのAIの必要性、潜在的リスク、導入したプロセスを理解する。必要性がない場合は、高リスクのデータをAIの使用から除く。

規制対象分野：データ・プライバシー、アクセスを含むデータ・セキュリティ、国際ルール、法域横断的取り決め

カリフォルニア州「消費者プライバシー法」、「グラムリーチブライリー法 (GLBA)」、「公正信用報告法 (FCRA)」、「米国連邦取引委員会 (FTC) 法」、「EU-米国間プライバシーシールド」、EU「一般データ保護規則 (GDPR)」



規制当局の見解

2020年までにデジタル・データの生成量は、2009年の40倍以上の水準になると予想されます。

消費者はある程度、安全性よりも利便性を選ぶことに慣れる必要がありますが、それでも個人情報と金融データの保護に関して主要金融機関への期待はなくならないでしょう。

— 米国財務省報告

「経済的機会を創出する金融システム、ノンバンク金融、フィンテック、イノベーション」

(2018年7月)





コンプライアンス・プロセス



新しいテクノロジーはリスクを呼び込むことがあります。金融機関や規制当局がより早期にリスクを特定し、低減するのを助けることもできます。AIおよび自動化は、コンプライアンス上の課題——コンダクト／カルチャー、データ・プライバシー、金融犯罪、消費者金融、取引および投資、データ保持のような領域における「リアルタイム」のコンプライアンス・リスク管理および報告を含む——にデジタル変革をもたらす可能性があります。

AIツールはより速く網羅的で正確なモニタリングとテストの実施を促し、従業員を反復的で「低価値」な業務から解放し、専門的判断と専門的知識を必要とする高価値の活動に集中できるようになります。しかし、一部のAIツールの不透明性は、規制当局や消費者に対してAIの結果を説明することを困難にし、コンプライアンス・リスクを増大させるかもしれません。取締役会および経営陣はこれらのリスクを特定し、効果的に管理するために、自社で使用するフィンテックの用途を十分に認識かつ理解する必要があり、規制当局は、これを確保することに重点を置く規則、および指針を設定するようになっています。

ドライバー

- 「リアルタイム」のコンプライアンスおよびリスク管理への期待
- 市場競争の激化とオペレーション・コスト削減への圧力の高まり
- オペレーションおよび事業部門横断的なリスク管理とコントロール

アクション

- **リスクおよびコンプライアンスの戦略目標への組み込み**：戦略的優先事項として、法令対応・規制対応の一環として、適切なリスク管理とコンプライアンスを位置付ける。
- **AIの開発プロセスにコンプライアンスを統合**：開発に先立ち、また開発を通じて、将来のプロセスに関する規制およびコンプライアンス要件を理解する。
- **規制変更を継続的に監視**：AIプログラムおよびソリューションのレベルで適用される、対象規制の変更を継続的に監視し特定する。

規制対象分野：取締役会の監督／リスク・アペタイト、取引監視、ミスコンダクト、BSA/AML関連報告、消費者／投資家関連法、変更管理、リスク評価／優先順位付け

取締役会および経営陣のためのFRB指針、FinCEN CDDルール、BSA/AML、消費者法



規制当局の見解

一群の規則をデジタル化して、データをリアルタイムで利用、処理、分析する能力は、いわゆる「アジャイル規制」の適用の可能性を大いに高めています。

機械はますます多くの経済上の業務や機能を引き受けることになるので、これらの機械が法令を必ず遵守することを確保するためのルールに沿って、プログラムされる必要があります。

— 商品先物取引委員会 (CFTC) 会長、クリストファー・ジャンカルロ
「量的規制：デジタル時代における効果的市場規制」
(2018年11月7日)





信用管理



金融機関は信用度の評価、バックテスト・モデル、市場分析、取引最適化などさまざまな用途にAIを使用しています。特に信用スコアリングモデルにおけるAIの利用は、債権者がより正確にリスクをモデリングし、価格を設定できるという債権者にとっての利点（それにより、消費者に対しても信用へのアクセスが拡大する）と、「説明できない」信用判断、学習バイアス、その他の公正貸付および消費者コンプライアンス・リスクに由来する潜在的リスクという点で、業界と規制当局の注目を集めました。

規制を受ける大部分の金融機関は、ノンバンク・ベンダーを通じてAI駆動のリソースにアクセスしており、サード・パーティ依存リスク、市場集中リスク（特定のベンダーが規模の経済を通じて独占し始めているため）、類似／同一データソースへの過度の依存リスクが増大しています。

ドライバー

- 消費者にとって信用へのアクセスが拡大
- 広範な非構造データセットの入手可能性／適用
- 監督当局の優先順位の特定

アクション

- **AIの与信判断の理解**：バイアスのない判断だと証明できるように、厳格な基準と指針に基づいて与信判断を支援するAIを点検する。
- **AIの結果とトレンド分析を監視**：AIが実行するトレンド分析に対する、より十分な精査。
- **変わりつつある規制要件の遵守**：信用管理の支援に使用されるAIが、会計基準と規制要件に加えられる変更に従っていることを証明する。

規制対象分野：相互接続性、サード・パーティ・テクノロジーへの過度の依存、AIラーニング手法の監査可能性、信用スコアリングモデルの独立性

レバレッジド・ローンに関する各当局の指針、米国財務会計基準審議会（FASB）の現在予想信用損失（CECL）、ファニーメイ／フレディマック基準、金融安定理事会（FSB）「金利指標改革」

66

規制当局の見解

AIは膨大な量のデータの迅速な分析を可能にします。その結果、特定の個人に関する信用リスク評価のコストを下げ、企業が信用リスクを測定できる個人の数を増やす方向で、広範な信用情報を扱うことのできる信用スコアリング方針を策定できるようになります。

機械学習を使用して信用スコアを割り当てて与信判断を行う場合、意義申し立てがあった場合、一般的に消費者、監査人、監督当局に信用スコアと与信判断結果を説明することはより難しくなります。

加えて、オンライン上の行動やこれまで利用されなかった金融情報のような新たな代替データソースの利用が、与信判断にバイアスを持ち込む可能性があるという議論もあります。

— 金融安定理事会（FSB）
「金融サービスにおける人工知能および機械学習」
(2017年11月)

99



サイバーセキュリティ



サイバーセキュリティ・アナリティクスが、発生前にサイバー攻撃を予想するのに役立つように、機械学習やディープラーニング（深層学習）のようなAI技術は、それなしには見付けられなかったかもしれない弱点を浮き彫りにすることができます。

しかし、AIの使用はまた、サード・パーティ・テクノロジーへの過度の依存や市場およびシステムの相互接続性の高まり、AIにより力を増して市場機能を操作しようとするサイバー脅威／サイバー犯罪などを通じて、新たなサイバーリスクをもたらすことがあります。規制当局はガバナンス、リスク分析、評価、コントロール（アクセス管理、情報セキュリティ、モニタリング、テスト、情報共有）、事案対応に重点を置いています。

ドライバー

- デジタルデータの増大、ますます高度になるテクノロジー
- 金融システムの高度な相互接続性
- 多くの革新的テクノロジー資源に対する消費者のアクセスニーズ
- サード・パーティ・プロバイダーやデータへの依存度の高まり

アクション

- **AIの開発プロセス全体に対してサイバーセキュリティを検討：**AIの安全な保護や機能不全を起こしたAIからの保護を含め、開発プロセス全般においてサイバーセキュリティを検討する。
- **方針およびリスク・アペタイトと一貫性のあるAIの開発：**第三者の利用やデータ交換を含め、サイバーセキュリティに関するリスクおよび活動を管理する。
- **AIテクノロジーに関するエンドツーエンドの方針、基準、役割、責任を確立：**AIテクノロジーの方針や基準を通じて、テクノロジーの重要要素を統治する。

規制対象分野：レジリエンス（適合可能なツール）、サード・パーティ・データ・セキュリティおよびデータ・プライバシー

「国家サイバー戦略」、米国国立標準技術研究所 (NIST) 「サイバーセキュリティ・フレームワーク」、SECガイダンスおよびレギュレーションS-PおよびS-ID、ニューヨーク州金融サービス局 (NY DFS) 「サイバーセキュリティ規則」、SECレギュレーションSPおよびS-ID、米国金融取引業規制機構 (FINRA) 「サイバーセキュリティ慣行に関する報告書—2018年」



規制当局の見解

AIの構成要素が幅広く利用可能であるということは、フィッシング詐欺師や不正行為者が最高クラスのテクノロジーにアクセスして、強力かつ実行可能なAIツールを構築できることを意味しています。

監督当局がこれらの脅威に対抗するために、同等に強力かつ実行可能なツールを求めるであろうことは明らかでしょう。

— 連邦準備制度理事会理事、ラエル・ブレynaード
「金融サービスにおける人工知能について何を学ぶか」
(2018年11月13日)





倫理とコンダクト



金融機関は、従業員、サード・パーティ、提携先／関連企業による不正行為を効果的に監視し低減することを期待されています。組織の倫理および価値観をAIシステムに組み込むのは、難しいことかもしれません。しかし規制当局は、消費者のデータ・プライバシーや商品適合性、販売／取引慣行にかかわるバイアス、公正さ、正確性、不正などを探すのに、従来型のオペレーションに使用するのと同じレンズを使って、AIの結果を評価することになるでしょう。AIシステムは分析の訓練に使用したデータにも、また、システムを強化するツールやアルゴリズムにも依存しています。

ドライバー

- 監督当局は、企業は従業員、サード・パーティ、提携先／関連企業による不正行為のリスクを管理しなければならないことを期待している。
- 消費者保護重視
- 不正行為がもたらし得る非金融リスク（評判、戦略、不正）への意識の高まり

アクション

- **AIの倫理および行動規範の策定**：倫理原則と行動規範を策定し、AIにも適用できるようにし、報告や告発の手続きを定めるようにする。指針は企業の目的と全社的倫理および規範と一貫制を持たせなければならない。
- **AIの倫理とコンダクトに関する研修の確立**：AIのエンドユーザーだけでなく、AIシステム設計者、開発者、リスク管理者、AIプログラムに関与するその他の利害関係者に対しても、倫理とコンダクト研修を実施する。

規制対象分野：行動規範、利益相反、適合性／フィデューシャリー・デューティー、マーケット・ミスコンダクト、取引監視およびモニタリング
取締役会および経営陣のためのFRB指針、SECレギュレーションBI、SEC「ビジネス行動規則」



規制当局の見解

機械学習に基づき特定された詐欺や不正行為の兆候は、それだけで強制執行の根拠とすることはできませんし、また、そうするべきではありません。

(中略) 機械学習の技術進展が、市場での不正行為の兆候を監視する我々の能力をこれまで高めてきましたし、これからも高めていくでしょうが、AIを未来の市場規制者と考えるのは時期尚早です。

科学はまだその段階に至っていません。現在使われている最先端の機械学習のテクノロジーは、人間の行動をこれまでにないやり方で模倣することができますが、機械による高度な推論はまだ漠然とした願望にとどまっています。

— スコット・バーゲス「リスク評価におけるビッグデータ、機械学習、AIの役割：規制当局の見解」
(2017年6月17日)





消費者保護



消費者金融保護の第1の目的は、すべての消費者にとって金融サービスと市場がより公平となるようにすることです。「信用状態が見えない」あるいは信用履歴が限定されている消費者に対し、代替データや機械学習のアルゴリズムを使用する信用スコアリングモデルを通じて、金融商品やサービスへのアクセスを拡大するなど、AIはこの目的にさまざまな方法で貢献できます。同様に、AIモデルにおけるパターンの検知により、消費者の苦情における異常値・特徴値を特定し、新たなリスク発生の可能性を予測できます。

しかし、広範なデータセットと機械学習の不透明性は、データ・プライバシーや公正貸付、信用報告、販売慣行、取引活動に関して消費者および個人投資家保護の観点から、意図しない結果や説明できない結果を持ち込む可能性もあり、企業のレピュテーションリスクと戦略リスクを高めています。消費者は自分の取引データや個人を特定できるデータの使用について、理解した上で同意することがますます重要となっています。規制当局は、消費者の意識向上のために透明性と開示をいっそう求めています。

ドライバー

- 統合され、パーソナライズされた製品およびサービスを消費者は求めている。
- 個人データの管理を消費者は求めている。
- 人口動態変化により、デジタル製品への移行が進んでいる。

アクション

- **AIソリューションの結果のモニタリング**：データアナリティクス、監査証跡、および経営陣のレビューによって、AIがパフォーマンスおよびビジネスの要件を満たしているかを検討する。
- **公正でバイアスのない取り扱いを証明**：AIの判断と結果に関して、固有のバイアスがないことを十分な審査、調査、探求を行って証明する。
- **消費者に影響を及ぼすAIは潜在的高リスク**：直接的または間接的に消費者に影響を及ぼすAIを、強化された監視と、より頻繁な評価にかけるべき潜在的高リスクとみなす。

規制対象分野：不正・欺瞞的な行為または慣行 (UDAP) / 不正・欺瞞的・濫用的な行為または慣行 (UDAAP)、差別的効果、均等信用供与法 (ECOA) / 公正貸付、データ・プライバシー

「グラムリーチブライリー法 (GLBA)」、「公正信用報告法 (FCRA)」、カリフォルニア州「消費者プライバシー法」、消費者法、米国障害者法、SECレギュレーションBI (最善の利益)、SECレギュレーションSP、「米国連邦取引委員会 (FTC) 法」



規制当局の見解

AIは自動化されており、人間の直接的介入にあまり依存しないという理由だけで、AIのアプローチにバイアスがかからないと思い込むべきではありません。

アルゴリズムとモデルは、その開発者の目的と観点、さらにAI訓練に用いられたデータが反映されます。その結果、AIツールは、このようにして作られた「社会」自体がはらむバイアスを反映または「学習」し得るのです。

— 連邦準備制度理事会理事、ラエル・ブレynaード
「金融サービスにおける人工知能について何を学ぶか」
(2018年11月13日)





金融犯罪



デジタルトランスフォーメーションは、金融犯罪関連のコンプライアンスの取組み全般にわたる変革を求めており、そのなかには、さまざまな金融犯罪、および顧客デューデリジェンスや取引モニタリング・報告などの領域におけるプロセスの自動化に関連するデータアナリティクス／予測的アナリティクスも含まれます。マネー・ローンダリング対策の分析の多くは事後に行われ、豊富な情報が集められますが、疑わしい取引として当局報告に足る有用な情報はほんのわずかです。このため資源を集中させることができず、有用な情報から注意がそらされる可能性があります。AIを予測的アナリティクスに使用すれば、各顧客に関して、何が特殊または異常な活動で、何が通常の予想される活動を対比することで、より理解でき、組織はどこに注意を向ければよいか、よりわかるようになります。また、この新たなテクノロジーは、どの情報を収集すれば法の執行に最も役立つか、顧客行動をより確実に予測するのに役立つかを企業が理解するのを助けます。

ドライバー

- デジタルデータの増大とテクノロジー・プロバイダーの増加：イノベーションの競争
- 規制当局による精査：高まるサード・パーティへの依存度
- コスト圧力：オペレーションおよび事業部門横断的なリスク管理とコントロール

アクション

- **既存の金融犯罪ツールに対してAIをテスト**：既存モデルに対してAIのパフォーマンスをテストする。マネー・ローンダリング分析と不正分析の任意のサブセットに対し頻繁にテストと検証を行い、AI駆動形システムが特定のグループを不当に取り扱っていないことを確認する。
- **AIが意図どおりに機能している証拠の提出**：AIが意図どおりに作動しているという証拠を提出し、AIおよびガバナンス構造によってもたらされるギャップと新たなリスクを特定する能力を維持する。

規制対象分野：BSA/AMLコンプライアンス（リスクの特定、疑わしい取引報告（SAR）、顧客デューデリジェンス、顧客受入れ）、資源の共有、共同契約

BSA/AML、金融犯罪捜査網（FinCEN）「顧客デューデリジェンス（CDD）ルール」、イノベーションに関する各当局の指針、ニューヨーク州金融サービス局（NY DFS）「取引モニタリング規則」、米国金融取引業規制機構（FINRA）規則3310



規制当局の見解

人工知能や機械学習のような新しいテクノロジーは、コンプライアンスのコストを削減し、同時にマネー・ローンダリングやテロリスト資金供与のリスクをよりよく管理するためのよりよい戦略を、あらゆる規模の銀行に提供できます。

一連邦預金保険公社（FDIC） 総裁、
エレナ・マクウィリアムズ

疑わしい活動を特定するための、リスクプロファイルに見合ったアプローチという点で、一部の銀行はますます洗練度を高めています。たとえば、複雑で戦略的な不法収益に関する脆弱性や脅威を特定するための、革新的な金融情報専門部署を設立、または強化するなどの取組みです。また、自らの銀行BSA/AMLのコンプライアンス・プログラムに適用できる人工知能およびデジタル・アイデンティティ・テクノロジーを用いた実験を行っている銀行もあります。（中略）規制当局はこの種の革新的アプローチを歓迎しています。

- 「マネー・ローンダリングおよびテロリストへの資金供与と戦う革新的取組みについての共同声明」（2018年12月3日）





資本および流動性



大企業は資本、流動性、信用リスク、取引先リレーションシップをより統合的な方法で測定する能力に、引き続き投資するものと予想されます。これにより、より頻繁かつ効果的な報告プロセスが可能となります。大企業はAIソリューションを使用して、資本最適化の効率性、正確性、速度を高めるとともに、バックテストおよびモデル検証（特にストレステストとオペレーショナルリスクに関連するもの）を行っています。

AIソリューションは、サード・パーティ（AIテクノロジーを提供／実施するプロバイダー）への依存の高まり、他の金融機関との相互接続性（テクノロジーおよびデータセットを通じて）、市場（テクノロジーおよびデータセットを通じて）とシステム、信用集中（機械学習／データのバイアスの結果）、意図しないモデルの判断／結果（機械学習の不透明性や人間の専門性の喪失による）などを通じて、金融機関のリスクプロファイルおよびビジネスモデルと関連するキャピタルリスクおよび流動性リスクを増大させるかもしれません。AIは巨大な非構造データセットを解析できますが、企業は時間の経過とともに、AIシステムの訓練に使用されたデータとその判断が、引き続き十分に質の高いものであるという保証や説明をすることが難しくなる可能性があります。

ドライバー

- 重要性、タクソミー、リエージを含むデータ・マネジメント要件
- ストレステストを含む資本および流動性に関する要件のためのモデル管理

アクション

- **AI判断プロセスの文書化**：資本および流動性に関する規制遵守を確保できるよう、AI判断の監査証跡を提供する能力を維持する。
- **資本および流動性に関するツールの結果をテスト**：関連するすべての複数モデルを通して、AIの処理結果と分析を対比し評価する。
- **データの質の評価**：分析に使用するデータが、その質に関する要件を遵守していることを確認する。

規制対象分野：資本最適化、資本構造、流動性の脆弱さ、システミックリスク（相互接続性、代替性／依存性、ビジネスモデルの複雑性）

1株当たり利益（EPS）、ストレス資本バッファー、FRB/OCC/FDIC「資本ルール」、包括的資本分析レビュー（CCAR）、流動性カバレッジ比率（LCR）、安定調達比率（NSFR）、単一カウンターパーティーの与信制限（SCCL）、現在予想信用損失（CECL）、米商品先物取引委員会（CFTC）およびSEC「スワップディーラーのための資本および証拠金規則」、米国金融取引業規制機構（FINRA）協会員宛広報（NTM）15-33「流動性リスク管理慣行のガイダンス」



規制当局の見解

これらの種類のモデルは、信用にアクセスできる者や投資ポートフォリオの管理方法の決定など、ますます価値の高まる判断への使用に配置されるため、現在、アカウントビリティの維持への疑問が根本的問題となっています。

モデルの不透明性は、特に広範な市場にストレスがかかるときに、監督当局やこれらのモデルの使用者がリスクを監視し、それらの相互作用の仕方を理解することが難しいという問題を引き起こす可能性があります。

— 米国財務省報告

「経済的機会を創出する金融システム、ノンバンク金融、フィンテック、イノベーション」

(2018年7月)



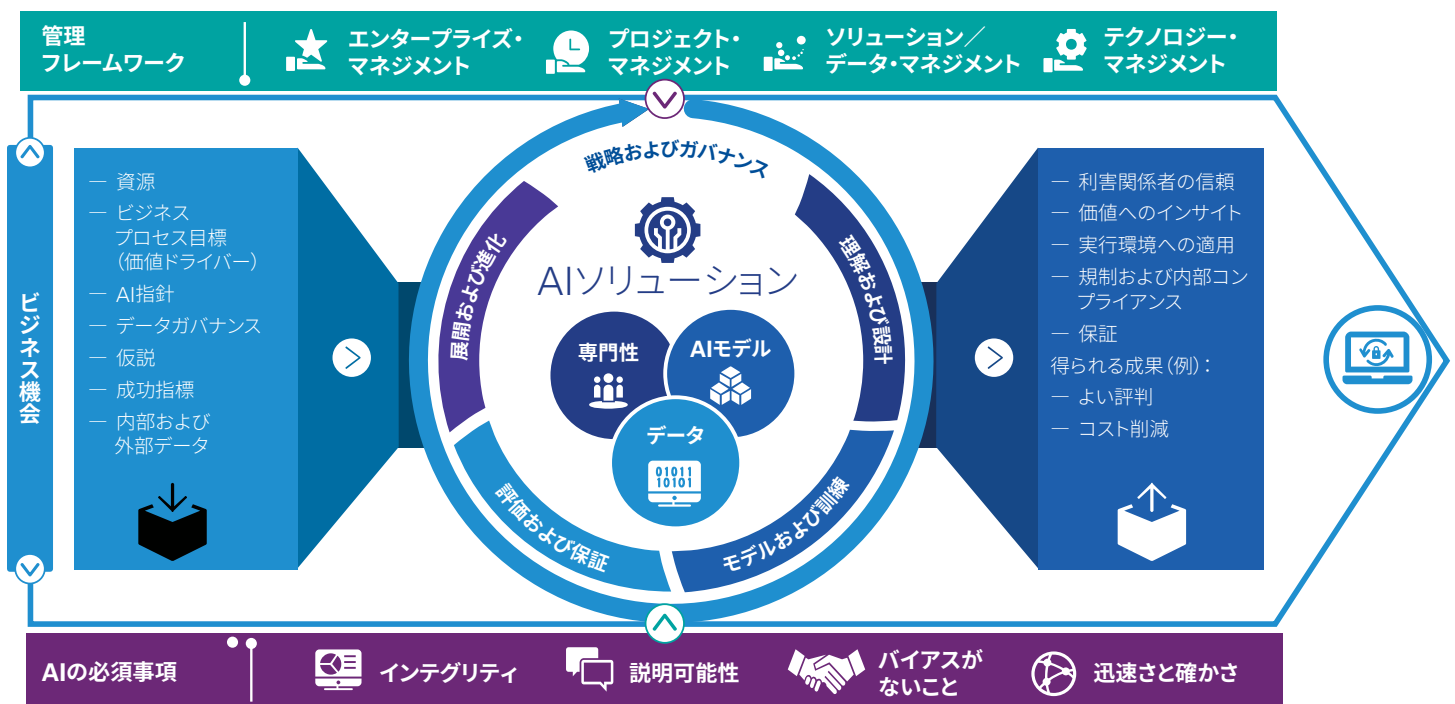
AIをコントロールするためのフレームワーク

変化のスピードは、特にAIでは加速していくでしょう。これらの新しいテクノロジーの潜在的価値への期待は大きいのですが、一部にはこのテクノロジーに対して、長期的にそのリスクを管理しコントロールを行使する人間の能力に疑念を感じ、恐れすら表明する人々も存在します。彼らは、「コントロール速度」(単一あるいは一連のコントロール操作の速度)が「リスク速度」(リスクが重大化する速度)についていけるのか、疑問を呈しています。人間はAIシステムを効果的に監視かつ管理するために、その結果を反復または検証しながら、AIの機械学習の速度と同じペースで進んでいけるのでしょうか。最悪のシナリオは、人間の関与と専門性が失われ、誰もがプロセスがどのように作動するのかわからず、結果を評価または修正する専門性を持つ者が存在しなくなるというものです。

AIの新たなリスクが、新たなコントロール方法を必要としています。

KPMGのAI in Controlは、ますます発展するAIシステムの実装と関連するリスクを企業がプロアクティブに検討するのを支援するために開発された、リスクおよびコントロールのフレームワークです。機械学習を含むAIソリューションのためのこのフレームワークは、エンタープライズ・マネジメント、プロジェクト・マネジメント、ソリューション/データ・マネジメント、テクノロジー・マネジメントの4分野にわたるリスク管理とコントロールを対象とします。企業が次のようなAIソリューションを構築するのを支援するように設計されています。

- インテグリティ (信頼できるデータ、アナリティクス、結果)
- 説明可能性 (どのように判断がなされ、新たに学習され、これに関連して何が変わるのか)
- バイアスのないこと (データおよび分析が網羅的かつ規制要件を満たしている)
- 迅速さと確かさ (多様なランタイム、プロバイダー、フレームワーク間での相互運用可能性、アプリやプロセスによる消費可能性、害や悪意ある攻撃からの安全性が保証されたモデル) を備えたAIソリューション



KPMG調査 発見事項の抜粋

自動化を追求する上位4つの理由



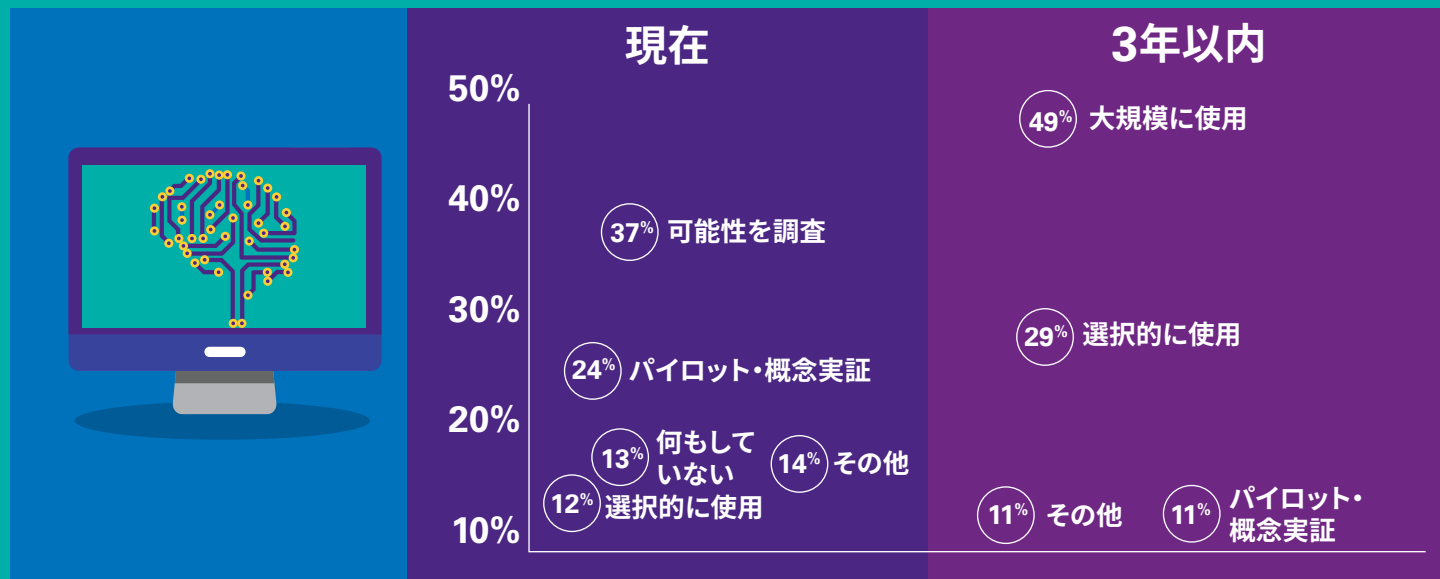
出典：自動化を通じた革新的コンプライアンス（業界横断）

期待は高いが準備不足

KPMGの調査の結論では、企業はインテリジェント・オートメーション (IA) の潜在的価値を認識しているものの、AIテクノロジーの使用への移行はなかなか進まず、ソフトウェア・ロボットの配備はまだ初期段階にあります。

それでも、AIの広範な採用計画が明らかとなっています。回答企業の3分の2近くがロボティック・プロセス・オートメーション (RPA) の今後3年以内の完全導入計画に言及していました。他の18%は選択的に使用すると述べています。コグニティブ・オートメーションに関しては、半数近くが3年以内にこれらのアプローチを大規模に使用する予定だと述べています。また、29%がコグニティブ・オートメーションの能力に選択的に依存すると述べ、約10%が予備プロジェクトと概念実証を開始すると述べています。

コグニティブ・オートメーションの使用（現在と3年以内）



出典：Ready, set, fail? Avoiding setbacks in the intelligent automation race. KPMGの調査による発見事項、2018年。

Contact us

home.kpmg/jp/regtech
regtech@jp.kpmg.com

山崎 千春
あずさ監査法人
マネージング・ディレクター
E: chiharu.yamazaki@jp.kpmg.com

東海林 正賢
KPMGコンサルティング
フィンテック・イノベーション部 部長 ディレクター
E: masayori.shoji@jp.kpmg.com

Amy Matsuo
Principal and National Lead
Regulatory Insights
T: 919-664-7302
E: amatsuo@kpmg.com

Deborah Bailey
Managing Director
Operations and Compliance Risk
T: 212-954-8097
E: dpbailey@kpmg.com

Charles Jacco
Principal
Cyber Security
T: 212-954-1949
E: cjacco@kpmg.com

Michael Lamberth
Partner
Operations and Compliance Risk
T: 804-241-2795
E: mlamberth@kpmg.com

大塚 卓美
あずさ監査法人
シニアマネジャー
E: takumi.otsuka@jp.kpmg.com

津田 圭司
KPMGコンサルティング
ディレクター
E: keiji.tsuda@jp.kpmg.com

Adam Levy
Managing Director
Risk Analytics
T: 312-665-2928
E: adamlevy@kpmg.com

Orson Lucas
Managing Director
Cyber Security
T: 813-301-2025
E: olucas@kpmg.com

Frank Manahan
Managing Director
Risk Analytics
T: 212-954-3660
E: fjmanahan@kpmg.com

Bill Meehan
Managing Director
Operations and Compliance Risk
T: 212-954-1870
E: billmeehan@kpmg.com

Teresa Pesce
Principal
Forensic
T: 212-872-6272
E: tpesce@kpmg.com

Todd Semanco
Partner
Operations and Compliance Risk
T: 412-232-1601
E: tsemanco@kpmg.com

Steve Stein
Principal
Cyber Security
T: 312-665-3181
E: ssstein@kpmg.com

Tracy While
Principal
Operations and Compliance Risk
T: 212-954-2691
E: twhile@kpmg.com

本リーフレットで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはあずさ監査法人までお問い合わせください。

home.kpmg/jp/socialmedia



本冊子は、KPMG米国が2019年5月に発行した「AI | Compliance in control: Financial services regulatory challenges」を翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

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上で提案する適切なアドバイスをもとにご判断ください。

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 853528

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Japan. 19-1041

The KPMG name and logo are registered trademarks or trademarks of KPMG International.