NTT DATA

日本銀行　金融高度化センター　創立20周年記念ワークショップ
「デジタル化とわが国の金融の未来」

第3部　プレゼンテーション＆パネルディスカッション
「デジタル技術を活用した金融サービスの安定的な提供について」

生成AI導入に向けた課題とリスク

2025年1月31日

株式会社NTTデータ
執行役員 第三金融事業本部長　　細谷 好志

生成AIに関する倫理、安全性、サステナビリティに関する調査結果

NTT DATA Inc.が5つの地域の34市場に対し生成AI活用効果を調査
12の業界、大企業・経営幹部で生成AI利用の意思決定に影響を持つ2,307人を対象

生成AIの導入に伴う潜在的なセキュリティリスクを懸念している経営幹部の割合
(ただし、大半は生成AIの将来性とROIがリスクを上回ると考えている)

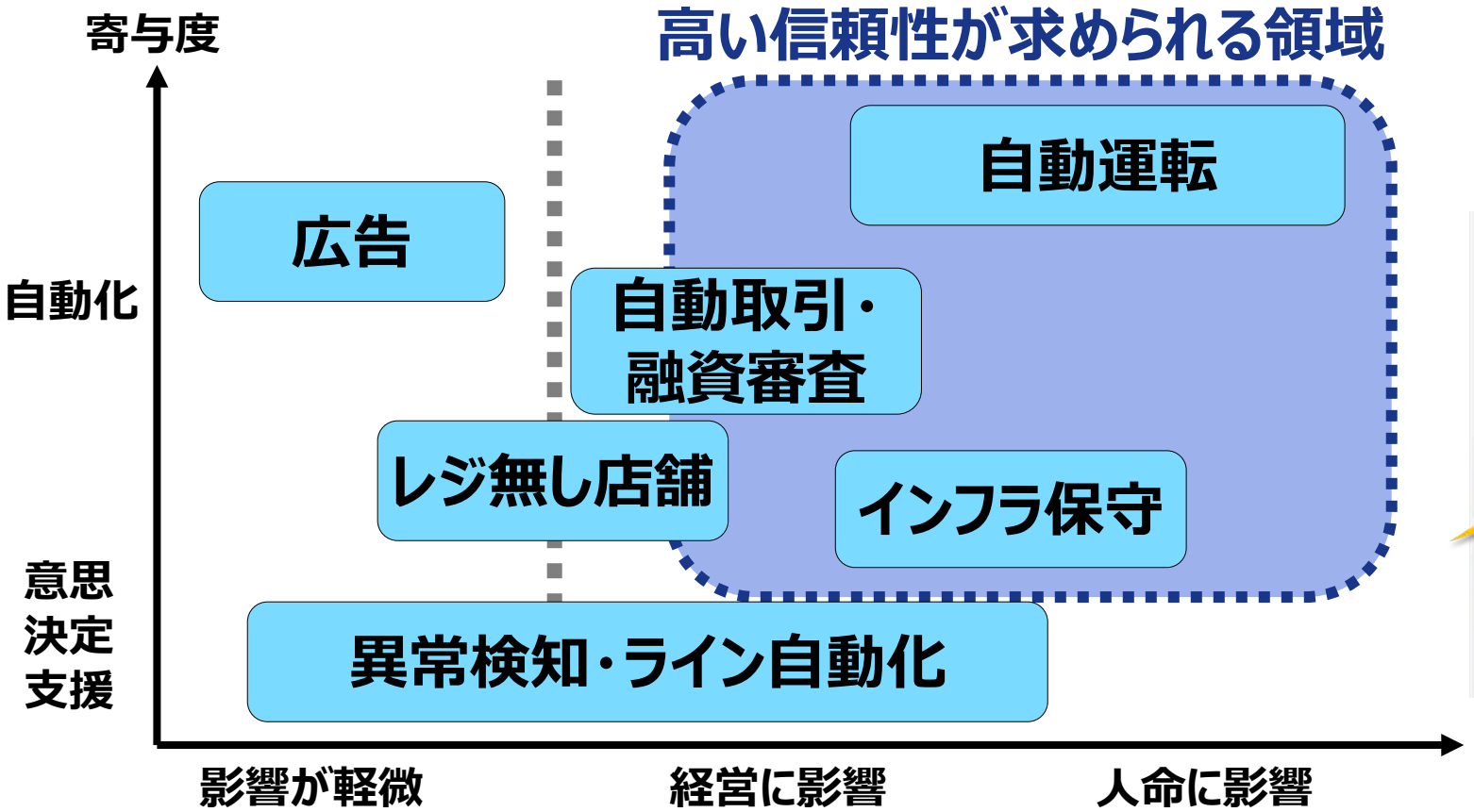
AIに関する政府の規制が不明確で、イノベーションが抑制され生成AIへの投資が妨げられていると答えた回答者の割合

Global GenAI Report　2025年における生成AI活用効果の最大化に向けた道標　Executive summary　2024.12.19　NTT DATA, Inc
https://www.nttdata.com/global/ja/-/media/nttdataglobal-ja/files/news/topics/2024/121902/121902-01.pdf?rev=cca68eb3cf2c4b6ebbaaf3ae9269a184

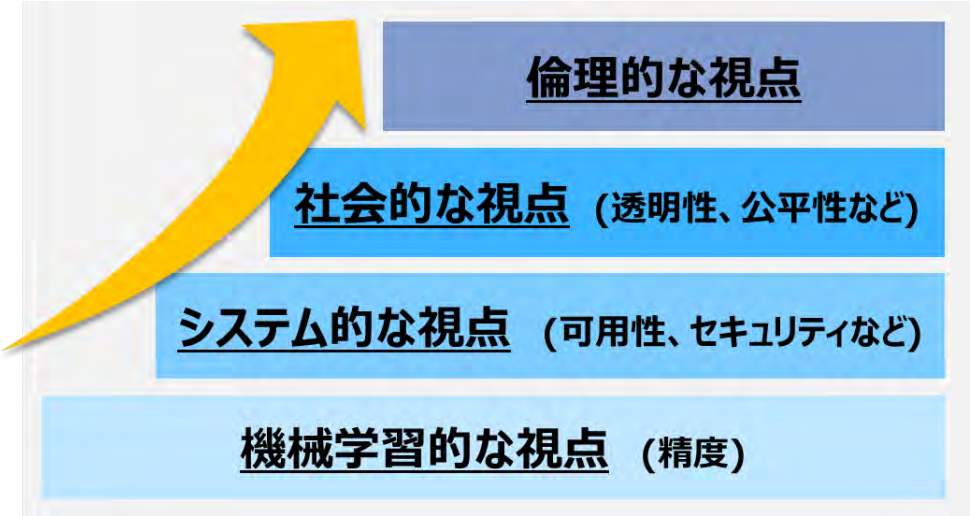
AIの導入にガバナンスが求められつつある背景

信頼性が求められる領域にAI活用が進み、倫理的な視点の評価が重視されている

AI・データ活用の活用範囲の拡大



AI・データ活用の評価視点の変化



従来AI／生成AIの差異

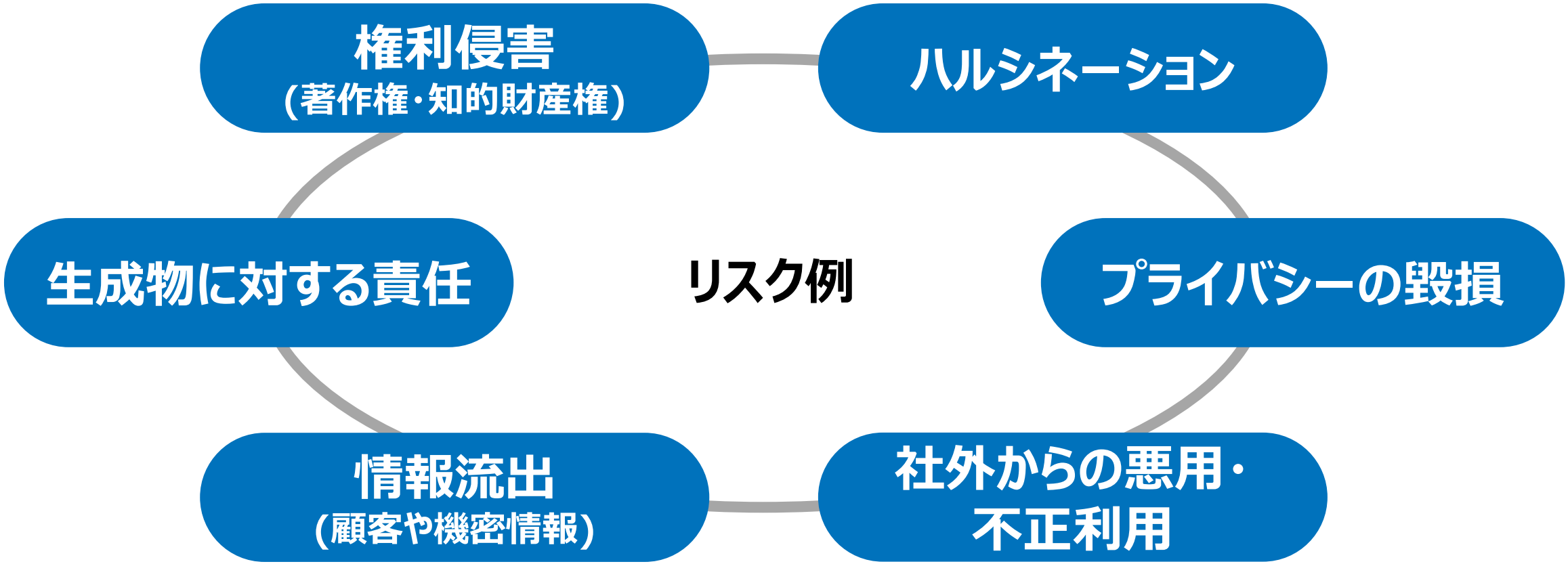
生成AIにより新たなリスクの発生／深刻化が生じ、従前のリスク管理では不十分

従来AI	**特定業務等の定められた行為の自動化**
生成AI	**指示に従いコンテンツ/成果物を生成**

観点	従来AI	生成AI
特徴	目的に沿うデータを学習させ、回答を得る	条件を与えるだけで、**様々な指示に対応可能**
学習	具体的なデータセットで特徴や傾向を学習	**大量の多種多様なデータをもとにして学習**
入力	定められた形式のデータセットを用意して投入	**様々なデータ形式や指示のインプットが可能**
出力	学習データのパターンを元に適切な回答提示	入力した指示に**従い新しいコンテンツを生成する**
利用	データを用意しモデルに読み込ませ回答を得る	**「質問文」形式で利用することが可能**

生成AIが生み出すリスク

生成AIは広範囲に多様な応用が可能で、幅広い効果が期待される一方リスクも拡大



AIに関する主な法制度

日本では現在AIに特化した法律は存在せず、内閣府のAI制度研究会で「イノベーション促進とリスク対応の両立」、「国際協調の推進」等を軸に議論中。AI活用には著作権侵害、個人情報保護、製造物責任等の既存法遵守が必要

法的な視点	日本での法律	法律で規制する事項	必要とされる対応
AI特化の法令	**(なし)**	内閣府AI制度研究会で議論中	法制化後、現在稼働中のシステムでも対応が必要になると思われる
著作権	**著作権法**	-学習データとしての無断利用 -生成物が既存の著作物と類似	文化庁「AIと著作権に関する考え方」の機械学習用途の著作物利用対応
製造物責任	**製造物責任法**	-AIシステムの欠陥による損害	AIが製造物とつながりサイバーフィジカルな製造物責任への対応
個人情報保護	**個人情報保護法**	-個人データの目的外利用 -第三者への提供	生成AIのプロンプト文からの個人情報収集への対応
営業秘密	**不正競争防止法**	-営業秘密や機密情報の流出	生成AI等の利用に従業員が遵守すべきルールを定める等の対応
サイバーセキュリティ	**サイバーセキュリティ基本法**	-金融機関を含む重要インフラ事業者に対して、サイバーセキュリティの確保を義務付け	AI等の新技術を含む周辺状況からの脅威情報の収集と影響評価への対応

AIガバナンスを取り巻く国内外の動向(1)

国際的にAIガバナンスが議論され、国内関連省庁でもルールメイクが活発化

欧州のAI規制法案 （2024年8月発効）	欧州

EU立法機関・欧州議会が**世界初となるAIの包括的な規制法を発効。**25年2月に「受容できないリスクのあるAI」のルール適用開始

総務省、経済産業省 （2024年6月　AI事業者ガイドライン公開）	日本

AIに関するリスクをステークホルダにとって受容可能な水準で管理、そこからもたらされる便益を最大化する**AIガバナンス構築を重要視**

広島AIプロセス （2023年5月～）	G7

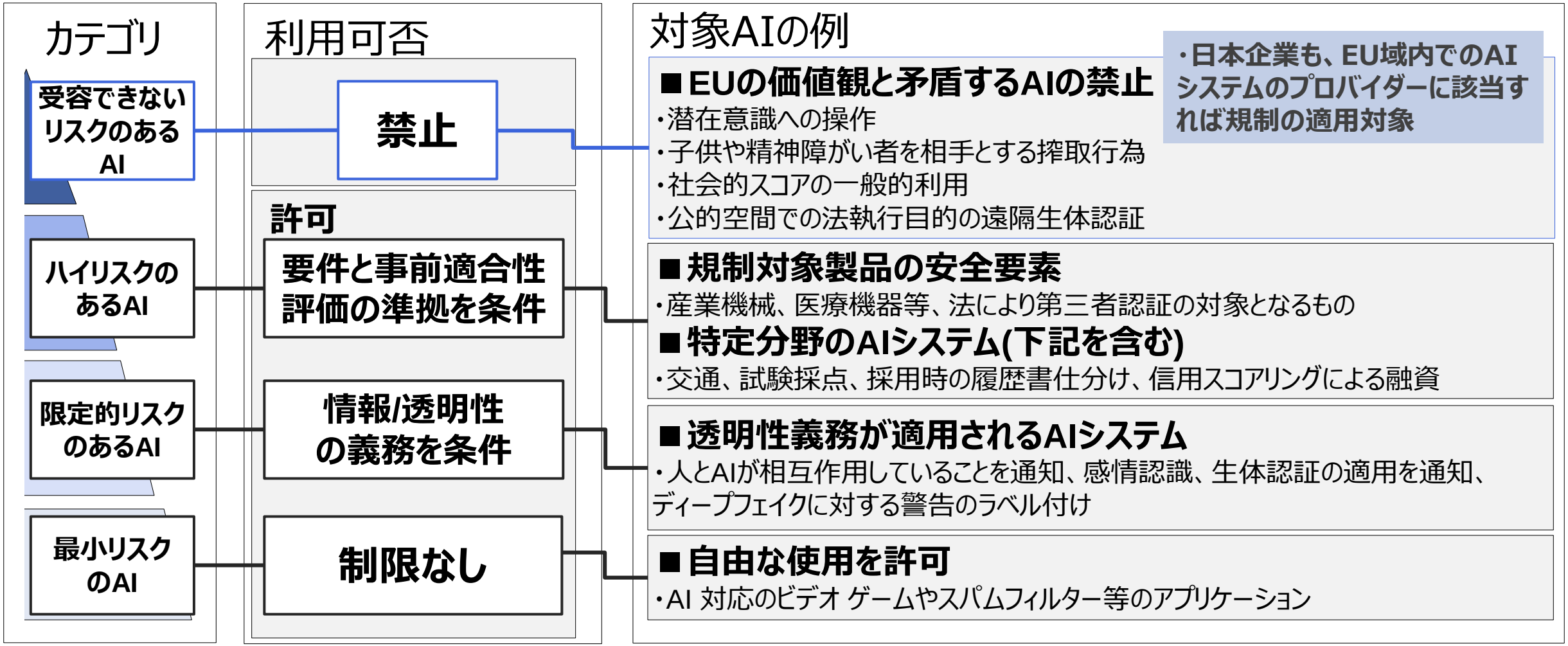
生成AIの活用や開発、規制に関する国際的なルール作りの推進を目的とするG7広島サミット首脳宣言に盛り込まれた新枠組み

金融庁 （2021年「モデル・リスク管理の原則」公表）	日本

金融機関に対するモデル・リスクに関する期待目線を8つの原則ベースで提示

AIガバナンスを取り巻く国内外の動向(2)　欧州のAI規制法

- リスクベースアプローチでAIをリスクの程度でカテゴリ化、それに応じた規制が適用
- 生成AI基盤モデルも、透明性の確保、リスク管理、インシデント監視、広範なテスト義務の規制あり



2021/5/11 経済産業省 「第1回 AI原則の実践の在り方に関する検討会：資料5」を参考に、2024/10/14に更新された
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-aiをの情報を参照しNTTデータにてまとめた

金融機関のAIガバナンス導入の観点

AIの利活用に金融業務特有の問題発生を予見し、様々な対応策が必要

	組織・仕組みにおける対応例
運用指針	・現場での具体的なAIの管理手続きを実現する有効かつ安全な運用指針を提示 ・支店や事務センターでの業務に有効なAIユースケース展開とAI利用ガイドライン策定
セキュリティ	・情報系DBと生成AIの連携やクラウド、オンプレミスともAIシステムのセキュリティ担保 ・利用リスクの想定とデータインジェクション、プロンプトインジェクション等、外部攻撃への対策
体制	・積極的なAI活用の推進とリスクを踏まえたAI統制の役割明確化と定期的モニタリング ・業務支援するAIのニーズ収集と全社的な教育体制整備、現場での人材登用
利用・運用	・インシデントを誘発するAIの誤回答を防止するガードレール整備 ・金融商品広告等で著作権保護や顧客、従業員の個人情報、営業秘密保護対策の浸透 ・AIソフトウェアの最新化、金融業務上の品質維持のための継続的な改善
社会受容	・日本及び海外事業所、サービス需要者を考慮した各地域の政府等の最新規制への対応 ・顧客へのAI利用の透明性の確保と定期的な説明の実施 ・AIにより変化する金融業務に対応する人材への配慮

海外の大手金融機関のAIガバナンスの対応

海外の大手銀行では、AIガバナンスに対して、
人・金・時間といったリソースを相応に投入している

観点	海外大手金融機関のAIガバナンス
運用指針	ガイドラインを制定し、現場レベルの規定に落とし込んでいる
セキュリティ	経営上位層のコミットメントが明確
体制	行内の責任分担が明確
利用・運用	開発とレビューで体制を分ける等、相互牽制が効くようにしている
社会受容	データやモデルの偏りを十分な量でテストしている
	AIモデルのパフォーマンスとコンプライアンス異常のリアルタイム監視を実施
	AIガバナンスの取り組みを銀行の重要な役職がアピールしている

国内金融機関の生成AIのガバナンスに関する取り組み

生成AIの全社普及が進むなか、包括的なAIガバナンスが必要な段階となり、
日本国内では大手金融機関が先行して取り組みを始めている

AIの導入期から全社組織への展開期へ

生成AIのリスクを踏まえた
ガイドラインの策定

↓

ガイドラインに基づき、
ガバナンスの仕組みを
構築しながら適用を図る

生成AI活用ステップの考え方–リスクに応じたレベル分け実施例

FDUAはリスクに応じた活用レベルを設定。 現在、レベル1～２の社内での生成AI活用が中心であるが、技術進展に合わせてレベル３の活用を伺う。

FDUAの活用レベル	生成AI活用のユースケース	ユースケースで考慮すべきリスク
レベル1	社内業務効率化のためのLLMベースのチャットシステム (情報収集、翻訳、文書作成やチェック等、自社データとの連携無し)	・利用者の個人情報や機密情報の流出 ・ハルシネーション、バイアス
レベル2	生成AIを活用した社内の問合せ応対支援 (顧客対応のための社内既定の対策等を含む)	・機密の流出、ハルシネーションを含む回答 ・回答内容に対する顧客への説明責任
	融資審査効率化のための稟議書・取引概要書の自動作成 (行内CRMや公知情報を利用した融資審査書類生成)	・CRMデータの更新漏れ等、不正確な判断 ・生成AIへの過度な依存による業務の不全
レベル3	生成 AI チャットボットによる問合せ対応 (24/365での顧客との直接対応を生成AIが実施)	・機密の流出、ハルシネーション ・プロンプトインジェクションによる意図せぬ動作 ・ユーザーサポートの不足、知的財産の侵害
レベル１～３の組み合わせ	中小企業向け融資申請プロセス効率化 (対話型AIによる融資情報の収集、データ検証や融資承認のサポート)	・融資候補先に関する不正確な情報の生成 ・顧客の懸念への対応 ・セキュリティ事故による影響

一般社団法人金融データ活用推進協会 生成AIWG事務局の「金融機関における生成AIの実務ハンドブック」をもとにNTTデータが作成
https://www.fdua.org/activities/generativeai

金融機関における生成AIの対顧客利用：克服すべき課題

生成AIの対顧客利用には大きな可能性がある一方で、金融機関特有の課題解決が必要。データ、セキュリティ、誤り、規制の4つの観点から、克服すべき課題を整理

データ品質の確保

- 学習に用いるデータの品質が結果に大きく影響
- **金融データの正確性、最新性、代表性担保が重要**
- データのバイアスによる不適切な結果の回避

セキュリティとプライバシーの確保

- 顧客の機密情報や個人情報保護のプライオリティの意思統一
- プロンプトインジェクション等、セキュリティ対策徹底
- 業務上の秘密と説明責任のバランス

誤った結果や判断のリスク対策

- **生成AIによる誤った金融アドバイスや意思決定の可能性の配慮とその対策**
- AIの限界と人間の関与の明確化
  (Human in the loop)

規制対応と内部統制

- **金融規制、法的規制への適合性の確認と対応**
- 社内のAIガバナンスの枠組み構築と内部統制強化
- 生成AIの利用に対する説明可能性と公平性担保

生成AI活用を支えるCoE組織の構築・運営の必要性

**生成AIの利用価値を着実に高め、かつ安全に活用するためには、
社内のリソースと知見を集約する戦略組織が必要となる**

生成AI活用の取り組み課題

戦略
- 生成AI活用の将来像や実行計画の全社浸透の不足

ビジネスプロセス
- 生成AIのユースケース創出に向けた更なる量と質の向上
- 有用な知見の集約と従業員への展開による活動の合理化

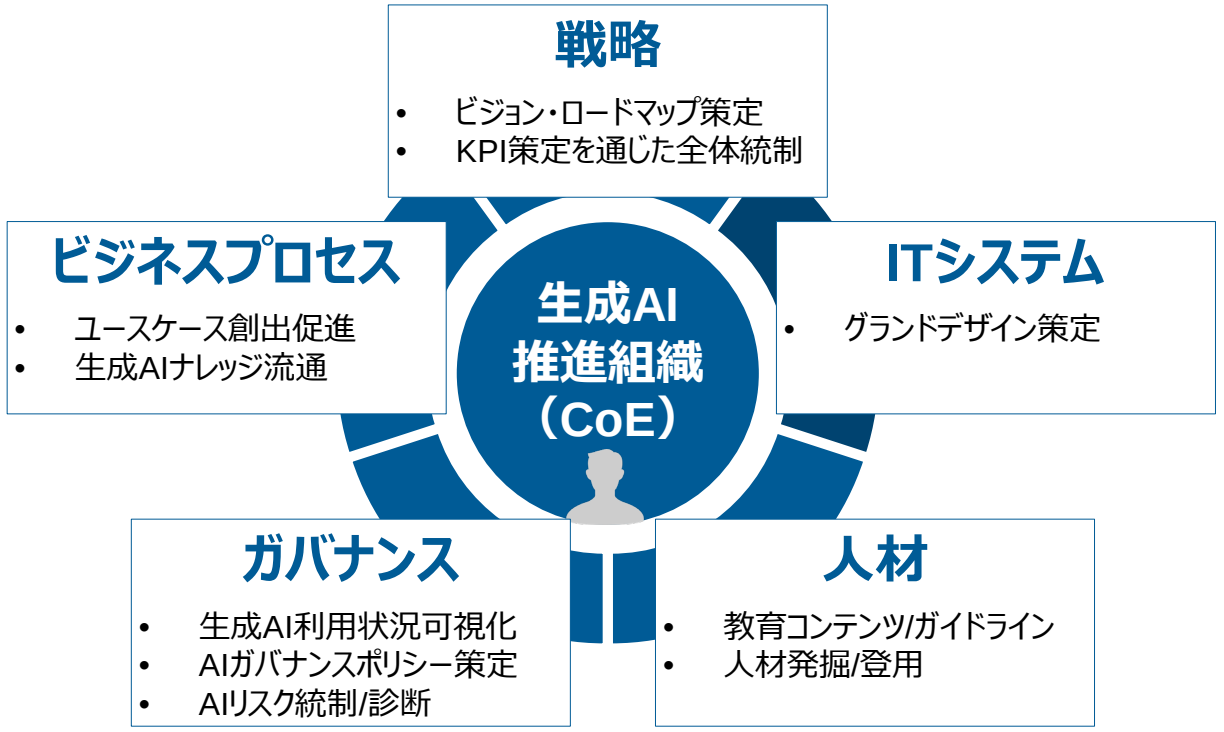
ガバナンス
- 野良AIの撲滅と統制の強化

人材
- 生成AIの利便性向上と安全な活用に向けた指導の徹底

ITシステム
- 活用ユースケースに応じた生成AIシステムの方針の策定
- 検証速度加速に向けた生成AIの共通基盤化の実現

生成AI利活用に向けた推進施策

目的 従業員起点での顧客サービス/業務変革を実行に移すため、**生成AIの普及・活用促進の戦略と実行を集中的に行う**




NTT DATA