資料6

安全・安心なAIの実現に向けた取組

2024年9月12日

株式会社三井住友フィナンシャルグループ
常務執行役員
高松 英生

SMBC SUMITOMO MITSUI FINANCIAL GROUP

1．SMBCグループのAI利活用と社内ルール制定の経緯

AIを積極的に利活用する一方、AIにかかるリスクに対し社内ルールを制定

利活用

2014年
コールセンターにおける照会対応業務支援
事前学習させたQ&A集からお客様の問い合わせ内容に対する回答候補をオペレータに提示、迅速かつ正確な回答を実現

2017年
サイバーセキュリティ対策高度化
サイバー攻撃に関して膨大な手口や傾向の情報をAIを活用して分析、対策強化

2020年
マネロン対策業務効率化
疑わしい取引報告にあたり、膨大な顧客取引情報から、AIを活用して効率的に対象を抽出

コールセンターへの高度なAI導入による品質向上
AIエンジンを高度化し、事前学習にかかる時間を1/3に削減し、回答候補の品質を向上

2023年
生成AI活用チャットボット“SMBC-GAI”
生成AIを実用化し、チャットポット形式での活用の他、個別業務での活用に用途を拡大

社内ルール整備

AI導入ガイドライン制定
AI特有のリスクを適切に管理するため、社内のAI開発に関するガイドラインを制定

AI導入・利用ガイドラインへ刷新
AI導入ガイドラインを改定し、生成AIの「利用」に関する留意点を明記

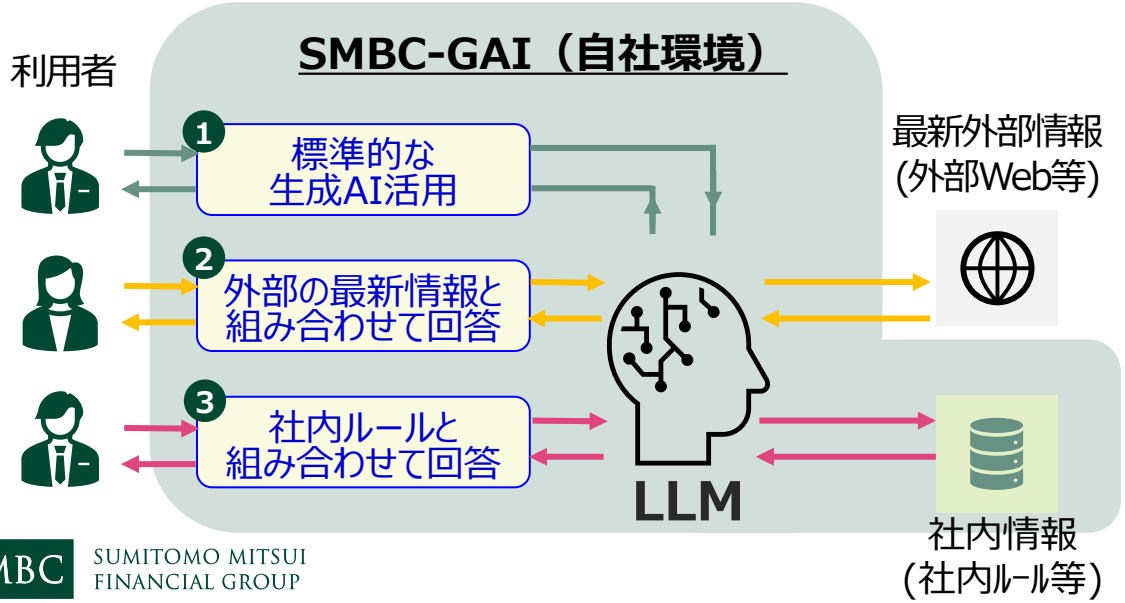
SMBC SUMITOMO MITSUI FINANCIAL GROUP

2．社内生成AI(SMBC-GAI)の概要

社内生成AIシステムを利便性と安全性の両立を考慮して、構築

(1)SMBC-GAI概要

- ✓ SMBC-GAIは、生成AIを活用した情報収集や文書作成等の支援を行うツール
- ✓ SMBCグループ社内専用環境上に構築し、セキュリティ対策や情報管理対策を考慮
- ✓ LLMは最新のAIモデルを搭載し、最新外部情報や社内情報と連携して回答



(2)生成AIの利活用例

- **<u>コールセンターの回答案作成</u>**
  お客さまからの各種照会に対する回答を事前に学習させ、お客さまからのお問合せ時に回答案を即時に作成
- **<u>融資稟議案作成</u>**
  最新の業界動向や過去の稟議書データなどを事前に学習させ、融資稟議書の作成を支援

(3)社内ルール整備

生成AI活用時のリスクを踏まえ、以下について明記の上、徹底

- ✓生成AIの出力結果には誤情報が含まれる可能性があるため、利用責任は利用者自身にあること、及びAI出力結果の妥当性・正確性を利用者が判断すること
- ✓生成AIは著作権を侵害する文章等が出力されるリスクがあり、不適切な利用とならないよう留意すること

SMBC SUMITOMO MITSUI FINANCIAL GROUP

3．社内ルール整備体制

各国法規制の内容・動向を踏まえたルールを整備すべく、関係部署横断でガバナンス強化

Why, What

- 人間中心
- 透明性
- 安全性
- アカウンタビリティ
- 公平性
- 教育・リテラシー
- プライバシー保護
- 公正競争確保
- セキュリティ確保
- イノベーション

Who

安全・安心なAIチーム

- 業務部門
- データ部門
- システム部門
- リスク管理部門

How

ルール	AI事業者ガイドラインに沿ったルールの見直し
プロセス	リスク審査プロセスをAI向けに拡張
ツール	ツールによるAIリスク評価の実施
教育	AIに関する教育コンテンツを拡充

4．AI利活用時の社内審査

AI利活用時の社内審査プロセスを制定し、既存のアセスメントと併せて実施

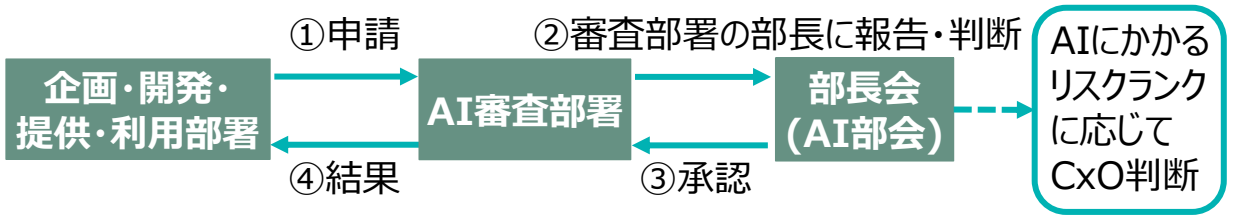
AIによるリスクの指針

指針(*1)	AIによる主なリスク(*2)
人間中心	•バイアスのある結果及び差別的な結果の出力
	•フィルターバブル及びエコチェンバー現象
透明性	•多様性の喪失
	•不適切な個人情報の取り扱い
公平性	•生命・身体・財産の侵害
	•データ汚染攻撃
安全性	•ブラックボックス化、判断に関する説明の要求
	•エネルギー使用量及び環境の負荷
アカウンタビリティ	•機密情報の流出
	•悪用
セキュリティ確保	•ハルシネーション
	•偽情報・誤情報を鵜呑みにすること
プライバシー保護	•著作権との関係
	•資格等との関係
教育・リテラシー	•バイアスの再生成

AIによるリスクの審査の枠組

	枠組み		観点
新規	AI審査	定性判断	•AI固有のリスク（人間中心・安全性・公平性・透明性・アカウンタビリティ）
		定量判断	
既存アセスメント	外部業者取引管理		•業務委託先のAI関連リスク全般
	モデル管理		•モデルリスク（安全性等）
	新種商品・業務		•全般（非対顧商品等は除く）
	セキュリティ基準		•システムリスク(セキュリティ確保・安全性等)
	クラウド審査		
	セキュリティレビュー		
	プライバシー保護		•プライバシー保護

AI審査プロセス



(*1) AI事業者ガイドライン(本冊)
(*2) AI事業者ガイドライン(別冊)

5．AI利活用に関する法令・ガイドラインの整備

- **法令については既に制定されている欧州・米国の内容との整合性を確保**
- **ガイドラインについては「企画者」の視点も明確化**

米州・欧州規制と日本のガイドラインとの差異

地域	法令概要
欧州	法令化（EU AI Act 2024/5） 主として人権侵害、差別・偏見リスクを重大リスクと捉え、センシティブな情報を扱うAIは禁止。高リスクAIに安全性評価等を義務化。影響の大きい汎用AIにはテスト等の報告を義務化。(*1)
米国	法令化（大統領令 2023/10順次） イノベーション促進とリスク対応を目的に、既存法令を活用し、主に経済安全保障の観点から、大規模汎用AIモデル等の開発企業に報告義務。(*1)
日本	法令なし 2024/4、AIのイノベーション及び活用の促進を目的に、関係者による自主的な取組を促すための、AI事業者ガイドラインを制定。

(*1) 内閣府AI政策の現状と制度課題から抜粋

「AI企画者」の定義づけ

役割		説明
AI企画者(*2)	新定義	新たな生成AIサービスの内容を企画し、データ前処理・学習～提供において、戦略・企画時に設定した目的・用途・適用範囲に沿って開発・利用を推進する者
AI開発者	AI事業者ガイドラインで定義済	AIシステムを開発する事業者(AIを研究開発する事業者を含む)
AI提供者	AI事業者ガイドラインで定義済	AIシステムをアプリケーション、製品、既存のシステム、ビジネスプロセス等に組み込んだサービスとして AI利用者（AI Business User）、場合によっては業務外利用者に提供する事業者
AI利用者	AI事業者ガイドラインで定義済	事業活動において、AI システム又は AI サービスを利用する事業者

(*2) FDUA生成AIガイドライン(第1.0版)における定義を引用

SMBC SUMITOMO MITSUI FINANCIAL GROUP