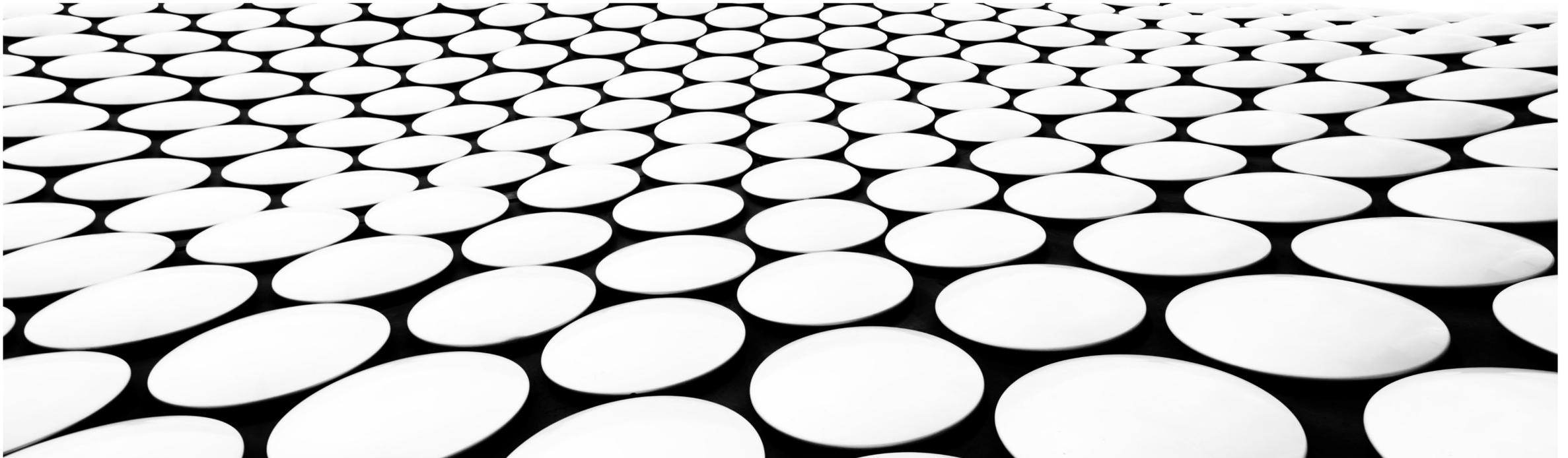


「AIとシステム監査」研究プロジェクト報告

2024年6月14日

黒澤兵夫

(TAKE国際技術士研究所)



コンテンツ

1. 活動メンバー
2. 活動状況
3. 参考文献
- 4.
5. AIの最近の情報
6. AI 事業者ガイドライン
7. AIガバナンス
8. AI開発者
9. AI提供者
10. AI利用者
11. AI契約
12. 今後の展開

1. 体制

	名称	所属
主査	稲垣 隆一	弁護士
副主査	黒澤 兵夫	TAKE国際技術士研究所
	荒添 美穂	
	芳仲 宏	「法とシステム監査研究」プロジェクト

2. 活動状況 月に一回ペース 平日 18:30 開始 約1時間30分程度

回数	開催日	場所	内容
第1回	11月13日	オンライン会議	AI要件とシステム監査の今後の進め方等
第2回	12月21日	オンライン会議	最近のAI/生成AIの動向等
第3回	2月19日	オンライン会議	AI/生成AIの教育と利活用について
第4回	3月6日	オンライン会議	AI/生成AIによる映画プロダクトについて
第5回	5月8日	オンライン会議	AIのガバナンスについて（ディスカッション）
第6回	6月5日	オンライン会議	研究大会発表 AIとシステム監査について（ディスカッション）

4. 参考文献

No	書名・資料名	著者	発行期日	備考
1	システム監査基準	経済産業省	2018年4月20日	
2	システム管理基準	経済産業省	2018年4月20日	
3	システム監査基準（改定版）	経済産業省	2023年4月26日	
4	システム管理基準（改定版）	経済産業省	2023年4月26日	
5	AI・データの利用に関する契約ガイドライン -AI編-	経済産業省	2018年6月	
6	GOVERNANCE INNOVATION Ver.2 アジャイル・ガバナンスのデザインと実装に向けて	経済産業省	2021年7月	
7	我が国のAIガバナンスの在り方Ver.1.1	経済産業省	2021年7月9日	
8	AI原則実践のためのガバナンス・ガイドライン Ver.1.1	経済産業省	2022年1月28日	
9	デジタルガバナンスコード2.0	経済産業省	2022年9月13日	
10	生成AIの利用ガイドライン	JDLA	2023年5月	
11	<u>AIプロダクト品質保証ガイドライン（QA4AIガイドライン）</u>	QA4AI	2022年7月20日	
12	機械学習品質マネジメントガイドライン（AIQMガ	産業技術総合研		

4. 参考文献

No	書名・資料名	著者	発行年月日	出版社	参照名
1	システム管理規準	経済産業省	2018年4月20日		経産省①
2	AI・データの利用に関する契約ガイドライン－AI編－	経済産業省	2018年6月		経産省②
3	GOVERNANCE INNOVATION Ver.2 アジャイル・ガバナンスのデザインと実装に向けて	経済産業省	2021年7月		経産省③
4	我が国のAIガバナンスの在り方 Ver. 1.1	経済産業省	2021年7月9日		経産省④
5	AI原則実践のための ガバナンス・ガイドライン Ver. 1.1	経済産業省	2022年1月28日		経産省⑤
6	AI時代における監査の取り組み とポイント	ISACA東京支部 稲垣 敦夫	2019年10月8日		ISACA⑥
7	AIシステムの監査 ～監査実施 モデル ポイント・プロセス～	ISACA東京支部 阿古島 隆	2020年7月3日		ISACA⑦
8	「AIを監査する…」 ～ビジ ネスにAIを活用するITCへの提 言～	企業内ITC・ITガバナンス研究会 (久住 昭之/坂本 徳明/瀬戸 昭彦/滝 沢 康/千枝 和行/古川 正紀/牧田 一雄 /山崎 直和)	2020年3月31日		ITC⑧
9	持続可能な開発のためのITとAI のガバナンスと評価	第3回SWIM研究会 小倉 博行(日本 大学) / 原田 要之助(情報セキュリ ティ大学院大学) / 馬奈木 俊介(九 州大学)	2020年11月28日		SWIM⑨
10	企業ITに人工知能を生かす	アビームコンサルティング	2019年6月24日	日経BP	7P-6⑩

AIの最近の情報

- **AI法規制、検討開始へ＝戦略会議で決定**
5/22 政府政府のAI戦略会議（座長・松尾豊東大大学院教授）、生成AI（人工知能）の開発事業者らに対する法規制の検討を今年の夏にも始める方針
- AIに関し「核軍縮、核軍備管理に対してリスクと（活用する）機会の両面」があり「核兵器国、非核兵器国を含む多層的なマルチステークホルダー（複数の利害関係者）の対話、協力の構築が重要」
5/21～22 第4回国際賢人会議
- **EU、世界初のAI規制法成立＝全面施行は26年の見込み**
5/21 欧州連合（EU）理事会、人工知能（AI）の開発や利用に関する規制法案を承認、同法が成立。規制の全面的な実施は2026年見通し
- **AI向けパソコン展開＝作業振り返り機能も一歩MS**
5/20人工知能（AI）利用に最適なパソコンを6月に発売と発表。最先端の半導体などにより、処理性能を最大20倍向上。その日の作業を振り返って確認できる「リコール」など、AIを活用した新機能の搭載
- 経済産業省と総務省は、生成AIの普及を始めとする近年の技術の急激な変化等に対応すべく、有識者等と議論を重ね、関連する既存のガイドラインを統合・アップデートし「**AI事業者ガイドライン（第1.0版）**」
4/19 「AI事業者ガイドライン（第1.0版）」を取りまとめ

政府政府のA I 戦略会議「AI規制に関する基本方針」

- 大規模なAI開発事業者を対象に、情報開示を求める制度の必要性
基本方針：競争力の確保と国民生活の向上「便益の最大化とともにリスクは可能な限り低減化」
リスク：①人権侵害②安全保障・犯罪増加③知的財産権の侵害
法的制の必要性：リスクの高いAIや人権侵害・犯罪につながり得るAIに対し必要
偽情報対策：コンテンツに出所や来歴情報を付与する技術の普及（OPオリジネータープロフィールの活用）
- AI創作物 発明者は「人」

” オープンなAI” 実現に残る課題 なかなか標準化が進まない背景

- ベンダーがモデルの仕組みを明らかにしていないため、情報不足による混乱が起こり、それを解消するために企業は努力するが空回りしている。新しい技術であるAIの分野では、企業にとっての価値とリスクが明確になっていない。（**Open source tops list of tech developers trust (CIO Dive)**）
- 目標は、アーキテクチャの設計図やフレームワーク、評価基準を作成することであり、これにより企業は生成AIシステムのパフォーマンスや機能、信頼性、企業レベルでの即応性を評価できる。

GPT-4o 「自然な会話」

- 応答速度と使い勝手（**UI : User Interface**）の向上
- ネイティブなマルチモーダル（多メディア対応）機能
- 感情を理解し表現することで人間に近づく（擬人化（anthropomorphization））

知性の原点は「生成コンテンツ」が創り出せない「ゆらぎ」 (FLUCTUATION)

[HTTPS://MIU.ISMEDIA.JP/R/C.DO?2E7C_MO_3ZL_SDS](https://miu.ismedia.jp/r/c.do?2E7C_MO_3ZL_SDS)

- 「揺らぎ成分」変化の部分だけを取り出して、私たち人間を含め動物の知覚や脳は、鋭敏に反応、記憶・記銘し、判断・行動の参考になっている
- 逆に、ワンパターンのノイズをヒトは記憶しない
- ヒトは「微細」な「変化分」の「微分」を認識・記銘し、記憶、判断の根拠とする
- 「AIが生成した音声コンテンツ」は、「均一な成分」が特徴的で、緩急の変化など「ゆらぎ」の成分は乏しい
- 「ソルフェージュ」という教科では、児童生徒が聴音しやすいよう「ソルフェ弾き」と言われる、ある種の「歪み」、音楽のなかに「ゆらぎ」を導入することで、音が聴き取りやすいよう、工夫して聴音課題を実施（東京藝術大学）
- 明確に表現するため、必須不可欠な「ゆらぎ」、細かく「不均一」な音楽の音階を意味している
- ヒトの反射的な知覚反応に根ざしつつ、余計な屁理屈を混ぜ込むことなしに、音楽の本質を言葉を超えて聴き手に伝える確かな**叡知**、**方法**（メトード = methode）
- 音のシグナルに鋭敏
- AIはこうした海馬の「ダイナミックな学習」（時空間学習則）ではなく、**言語や静止画像などの「静的な学習」**（ヘブの学習則）しか用いていない

グーグルマップに悪評、口コミ投稿削除命じる 大阪地裁

判決は5月31日付。

- インターネット上の地図サービス「グーグルマップ」上の口コミで一方向的に悪評を投稿されたとして、兵庫県内で眼科医院を運営する医療法人が損害賠償と投稿の削除を求めた訴訟の判決が3日までに大阪地裁であった。山中耕一裁判官は名誉毀損を認定し、投稿者に200万円の賠償と削除を命じた。判決は5月31日付。
- 判決によると、原告は兵庫県尼崎市で眼科医院を運営する医療法人「秀明会」。被告は大阪府内に住む女性で、遅くとも2021年11月までに同眼科について「レーシック手術は左目だけで勝手に右目はレンズを入れられていた。最悪」「何も症状もないのに、勝手に一重まぶたにされた」といった内容の口コミをグーグルマップに投稿した。
- 山中裁判官は判決理由で「患者から適切に承諾を得ることなく、勝手に医療行為をするとの印象を一般の閲覧者に与える」と指摘。名誉を毀損し、投稿により原告の社会的評価が低下したと認められるとして、投稿の削除を命じた。
- グーグルマップでは、地図上に表示される対象をクリックすると名称や住所、営業時間などの情報を確認できる。口コミの内容や5点満点の「評点」を投稿・閲覧することができ、飲食店などでも同様の機能を利用できる。
- こうしたグーグルマップの機能を巡っては、投稿された不当な口コミが削除されずに利益が侵害されたとして、全国の医師や歯科医師らが4月、米グーグルに計約140万円の損害賠償を求めて東京地裁に提訴した。
- 今回のケースでは、口コミが匿名で投稿されていたことから、原告側は21年11月、米グーグルに発信者情報の開示を求め提訴。その後、開示を命じる大阪高裁判決が確定し、23年9月に投稿者の氏名や住所が明らかにされた。

AI 事業者ガイドライン (総務省・経済産業省 第 1.0 版 令和 6 年 4 月 19 日)

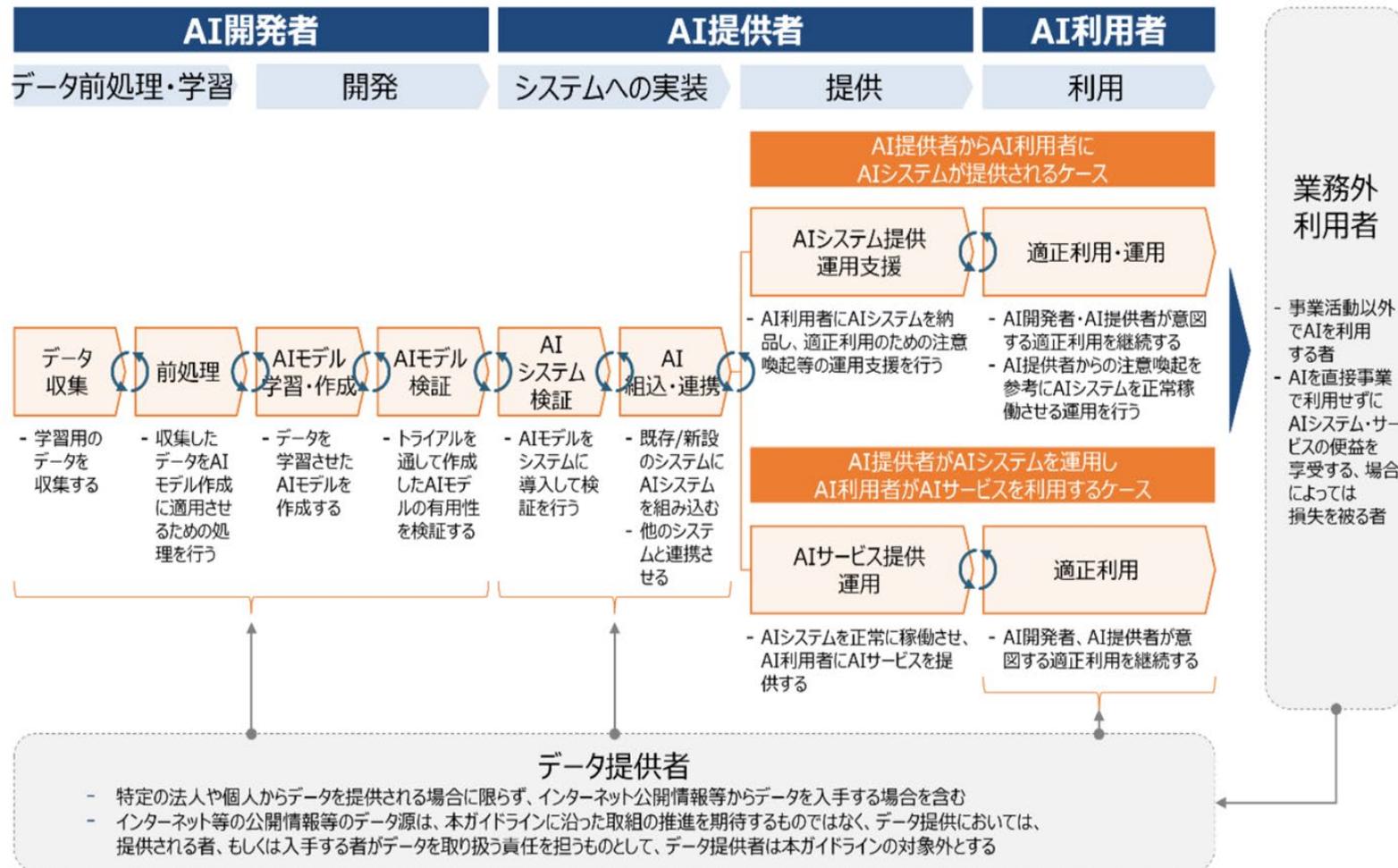
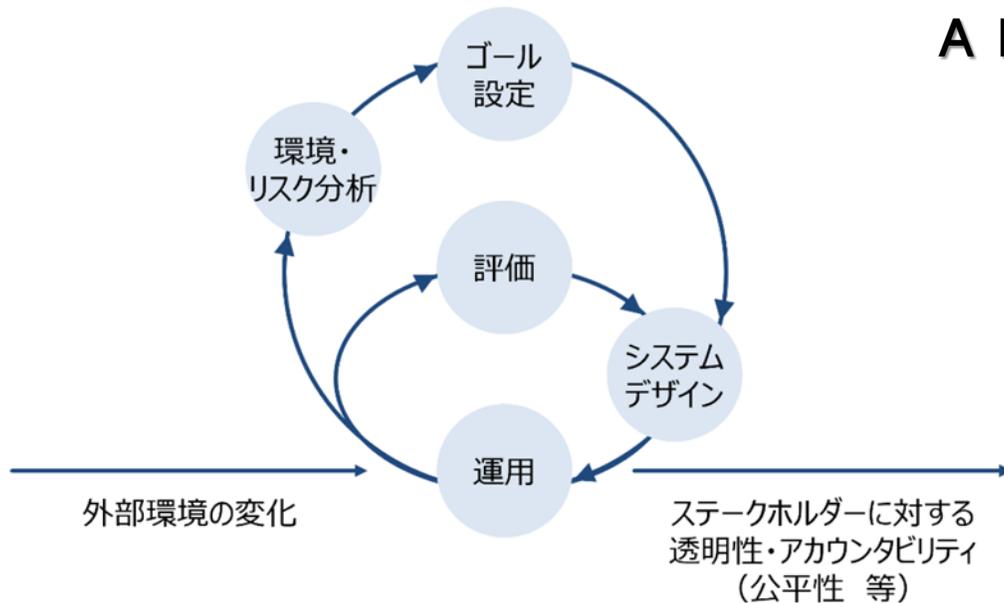


図 3. 一般的な AI 活用の流れにおける主体の対応

AI事業者ガイドライン案



AIガバナンス

1. 環境・リスク分析
2. AIガバナンス・ゴールの設定
3. AIマネジメント・システムの設計・運用
4. 評価、継続的改善
5. 外部環境の変化を踏まえた環境・リスク分析

A I 開発者に関する事項

データ前処理時・学習時

- ・適切なデータの学習
- ・データに含まれるバイアスへの配慮

A I 開発時

- ・人間の生命・身体・財産、精神及び環境に配慮した開発
- ・適正利用に資する開発
- ・A I モデルのアルゴリズム等に含まれるバイアスへの配慮
- ・セキュリティ対策のための仕組みの導入
- ・検証可能性の確保

AI開発後

- ・最新動向への留意
- ・関連するステークホルダーへの情報提供
- ・AI提供者への「共通の指針」の対応状況の説明
- ・開発関連情報の文書化

A I 提供者に関する事項

A I システム実装時

- ・人間の生命・身体・財産、精神及び環境に配慮したリスク対策
- ・適正利用に資する提供
- ・A I システム・サービスの構成やデータに含まれるバイアスへの配慮
- ・プライバシー保護のための仕組みや対策の導入
- ・セキュリティ対策のための仕組みの導入
- ・システムアーキテクチャ等の文書化

AIシステム・サービス提供後

- ・適正利用に資する提供
- ・プライバシー侵害への対策
- ・脆弱性への対応
- ・関連するステークホルダーへの情報提供
- ・AI利用者への「共通の指針」の対応状況の説明
- ・サービス規約等の文書化

A I 利用者に関する事項（A I システム・サービス利用時）

安全を考慮した適正利用

入力データ、プロンプトに含まれるバイアスへの配慮

個人情報の不適切入力とプライバシー侵害への対策

セキュリティ対策の実施

関連するステークホルダーへの情報提供および説明

AIガバナンス

- A I の開発者、利用者である企業・組織には、ガイドラインを実施するための仕組みの構築（A I ガバナンス）が求められる
- A I ガバナンスは、企業・組織自身についてのガバナンス（コーポレートガバナンス）のほか、サプライチェーンについてのガバナンス（AI契約ガバナンス）も必要とされる

AIとシステム監査



有識者会議「AI制度研究会」（仮称）（2024.6.5 読売、）

- 新たな規制の検討
- G7「広島AIプロセス」 ⇒ 安全性の高いAIの実現に向けえた国際連携



おわり