次世代のシステム監査研究プロジェクト報告
ーシステム監査の視点から見る生成AIー

- Generative AI considered from a perspective of System Audit -

2024年6月14日

次世代のシステム監査研究プロジェクト

主　査：荒牧　裕一
（かなざわ食マネジメント専門職大学）

研究会メンバー（アイウエオ順）

【主　査】　荒牧　裕一（かなざわ食マネジメント専門職大学）

【副主査】　浦上　豊蔵（たつの市）

【メンバー】栗山　孝祐（株式会社スターシステム）
小林　和子（Monad Consulting）
雜賀　努　（株式会社ニイタカ）
原　善一郎（原善一郎技術士事務所）
深瀬　仁　（パナソニックコネクト株式会社）
福永　栄一（大阪成蹊短期大学）
松田　貴典（大阪成蹊大学、大阪公立大学大学院）
吉田　博一（システム監査技術者）

【ISACA大阪支部】
板倉 寛和　藤井 みゆき　松井 亮宏　松浦 潤　森下 貴博

本研究プロジェクトについて

- 情報システムの基盤に関わる新たな技術の登場・普及と、新たな制度の導入に伴い、システム監査の位置付けや監査の方法についても新たな視点が求められるようになっている。
- 本研究PJは、関西および中部地区のメンバーにより、このようなシステム監査を取り巻く環境の変化への対応を研究し情報共有を図っている。
- プロジェクト５年目の取り組みとして、主に生成AIの活用事例やガイドラインに関する研究に取り組んできた。それらを踏まえて、生成AIの活用におけるシステム監査の視点からの留意点について、現時点における中間的なとりまとめの報告を行う。

活動実績

（2023年5月~2024年5月）

2023-2024年の活動実績（１）

【第27回（発表：深瀬　仁）】
・日 時： 2023年5月17日
・テーマ：**「対話型AIの活用について」**
・内 容：対話型AI（生成型AI）について、勤務先での活用の体験談の発表があり、それを踏まえて、意見交換をした。

【第28回（共同研究）】
・日 時： 2023年7月6日
・テーマ：**「新システム監査基準ガイドラインについて(1)」**

【第29回（共同研究）】
・日 時： 2023年9月13日
・テーマ：**「新システム監査基準ガイドラインについて(2)」**
・内 容：新しいシステム監査基準とガイドラインについて、内容の共有と意見交換を行った。

2023-2024年の活動実績（２）

【第30回（共同研究）】
・日 時： 2023年10月18日
・テーマ：**「AI利用のガイドラインについて(1)」**
・内 容：東京都デジタルサービス局やディープラーニング協会（JDLA）等が公表しているAI利用のガイドラインや新聞記事を基に、意見交換を行った。

【第31回（発表：松田　貴典）】
・日 時： 2023年12月5日
・テーマ：**「AI利用のガイドラインについて(2)」**
・内 容：各種団体のガイドラインを元に、「生成ＡI活用のガイドライン項目とそのポイント」をまとめ、意見交換を行った。

2023-2024年の活動実績（３）

【第30回（発表：深瀬　仁）】
・日 時： 2024年1月17日
・テーマ：**「AI利用のガイドラインについて(3)」**
・内 容：昨年5月の発表の続きとして、発表者の勤務先でのガイドラインの説明と活用の体験談の発表があり、それを踏まえて意見交換を行った。

【第31回（発表：深瀬 仁）】
・日 時： 2024年2月27日
・テーマ：**「AI利用のガイドラインについて(4)」**
・内 容：前回の研究会の内容の続きと、1/15に公表された文化庁の「ＡＩと著作権に関する考え方」素案についての意見交換を行った。

2023-2024年の活動実績（４）

【第32回（発表：荒牧 裕一）】
・日 時： 2024年3月27日
・テーマ：**「AIと著作権について」**
・内 容：1/15・2/29に公表された文化庁の「ＡＩと著作権に関する考え方」素案に基づいて、AIと著作権についての問題整理と法解釈の方向性について発表が行われ、意見交換を行った。

【第33回（発表：松田 貴典）】
・日 時： 2024年4月23日
・テーマ：**「システム監査の視点から見る生成AI(1)」**
・内 容：著作権法の概要、および、内閣府・文化庁の資料を基に、生成AIと著作権に関する論点整理を行い、それに基づいた意見交換を行った。

2023-2024年の活動実績（５）

【第34回（発表：板倉 寛和）】

・日 時： 2024年5月21日

・テーマ：**「システム監査の視点から見る生成AI(2)」**

・内 容：3月、4月の研究会で行った、AIと著作権との関係に関する発表を踏まえた意見交換の続きを実施し、積み残しとなった論点について討議した。

また、著作権以外の知的財産権との関係についても問題提起された。

企業でのAI活用について
（1月~2月研究会を踏まえて）

利用の注意事項

1. 回答が正しいとは限らない。最後は人が判断する。

2. 参考情報として扱う。

3. 情報は最新ではない。

4. 公開情報からしか回答しない。社内情報は非対応。

5. 英語の方が正確な回答が返ってくる。

３つの課題と解決策

１．自社固有の質問には回答できない。
→企業データを活用できるシステムを構築する。

２．回答の正確性を担保できない。
→回答の引用元を表示することで検証可能にする。

３．最新の公開情報は回答できない。
→検索エンジンと連携することで最新の情報にも対応する。

AI利用のガイドラインについて
（10月~2月研究会を踏まえて）

ガイドライン項目例（１）

１．生成AIについて

生成AIの活用は、その特性を認識し正しい利用をすること。あらゆる分野に有効とは限らず、不向きな分野もある。事前に十分に認識して活用することを明記する。

２．利用環境

利用する生成AIと安全な利用環境を共通基盤として整備し、その情報を明記する。

３．リスク（リスクについて注意喚起等）

・情報漏洩につながるリスクや不正確な回答が個人情報漏洩、機密情報漏洩を誘因
・法的侵害のリスクの認識（著作権法、不正競争防止法、商標法、民法、刑法等）

ガイドライン項目例（２）

４．利用方法とルール

・プロンプトエンジアリングを習得して、より質の高い回答を得る

・顧客の個人情報の利用・入力
　顧客の許可如何に関わらず個人情報の入力を禁止

・既存の著作物に類似する文章の生成の禁止
　「似せて文章を生成してください」等の入力禁止

・登録商標・意匠（ロゴやデザイン）の入力で生成された生成物を活用する場合の調査

・他社から秘密保持義務を課されて開示された秘密情報の入力禁止

ガイドライン項目例（３）

５．文章生成AIが生成した回答の根拠や裏付けの確認
（公開や配信の前に）

６．生成AIのポリシー上の制限や公開時の表示、注意事項等

７．一定の専門知識や自分なりの問題意識とともに、真偽を判断する能力の指導と育成を図る。
最終的には自己判断する責任があることを明記する。

生成AIの活用分野

（1）適した分野

①文書作成の補助

要約、言い換え、翻訳 文案作成 等

②アイデア出し

考えの整理（壁打ち）

事業企画におけるペルソナ分析

デジタルツールの活用案提示等

③ローコード等の生成

マクロ、VBA（Visual Basic for Applications ）等の生成

（2）不向きな分野（現時点）

①検索

最新情報、正確性が必要な情報 等の検索

②数学的な計算等

生成AIの活用におけるリスク

①公開された環境で利用すると、入力内容が学習データとして保存されるなど、情報漏洩につながる。
→「opt out機能」を利用する。

②プロンプトに機密情報や未公開情報を入力すると、情報漏洩につながるリスクがある。
→機密情報や未公開情報を扱う部署での活用に特別の対策が必要。

③不正確性な回答、情報漏洩、著作権侵害等、
→生成AIが生成した回答の根拠や裏付けを必ず確認することが重要である。

AIと著作権について
（3月~5月研究会を踏まえて）

著作権侵害防止に対するAI各社の対応

・Adobe社

自社の生成AIサービス、Fireflyのコンテンツに関しては100%ライセンス取得したものである、と保証した上で、著作権侵害の訴訟が起きた際にはその補償もする。（2023年6月）

・マイクロソフト社

ChatGPT／CoPilotの使用に対して著作権侵害の保護を保障する。（2023年9月）

・Google社

自社のAIサービス（Vertex AI, Duet AI）のコンテンツに関する外部からの訴訟の保護をする。（2023年10月）

・IBM

自社のGraniteをはじめとしたAIサービスに関する著作権の保護を発表。IBMのデータに関しては、そのソースを公開していて、誰でもレビュー可能であると主張（2023年10月）

留意点（私見）①

①開発・学習段階

事業者側の対応が進み、事業者レベルでの著作権問題はクリアされつつある。

（1）自社独自の学習を行わない場合

・対応済みの生成AIのみが使用されるような運用ルール作り

（2）自社独自の学習を行う場合

・使用データと著作権の関係の事前確認
→問題がある場合には利用制限

・プロンプト入力を学習させる場合の対応

・学習させたデータの記録の保存

・侵害が後日判明した場合は、学習前に戻す方法の確保

留意点（私見）②

②生成段階

対応済みの生成AIを使用しても、生成の方法次第では著作権侵害の恐れがある。

・既存の著作物の類似物の生成を意図するプロンプト入力等を禁止する必要
→プロンプト入力の記録のチェック

・検索拡張生成（RAG）等の利用への対応
→指示・入力に用いられたデータに含まれる著作物と共通した創作的表現が出力されないようフィルタリングする技術的措置が取られているかどうか
（パブコメ対応145番）

生成AIによる生成物が、利用者の著作物として認められない可能性がある。

・プロンプト入力だけでは著作物として認められない可能性大
→人の手による創作的な加工
→生成物がプログラムである場合の対応は？

③利用段階

生成物の譲渡や公衆送信（SNSへの掲載等）時には、著作権侵害の恐れがある。

・「著作権者の利益を不当に害さない」かどうかの確認

・特に、有料譲渡、インターネットでの公開には、注意が必要
→「既存著作物との高度な類似性」の最終チェック

AIに関する他の論点

AIに関する他の論点（１）

（1）公開時の表示

ChatGPT など OpenAI 社のサービスを利用して生成されたコンテンツを公開する際には、「使用に関するポリシー」において、AIを利用した生成物であることを明示することなどが定められている。

また出力時には、手動/自動提供などの提供手段にかかわらず、「AI が生成した物であること」及び、「生成物の内容に虚偽が含まれている可能性があること」をユーザに表示する。

ただし、生成物そのものを、顧客情報を含めた第三者には提供せず、第三者に提供する書類などを作成するために生成物を参照する場合は、上記に言及した表示は必要ない。

AIに関する他の論点（３）

（２）ハルシネーション（Hallucination：幻覚）対策

・「もっともらしいウソ」すなわち、事実とは異なる内容や文脈と無関係な内容が生成されることである。

・ハルシネーションが発生する原因としては、生成AIでは、大規模言語モデル（LLM：Large Language Models））に基づいて、ある単語や文章の次にくる単語や文章を推測して、確率的にそれらしい回答を生成するが、このプロセスは完全ではなく、AIが誤った情報を生成したり、生成したデータに偏りや誤りを含む可能性がある。

　また、言語モデルはある単語に対し次に続く確率が高い単語を予測するものであり、正しい情報を出力することを目的として訓練されていないこと等が挙げられる。

（参考文献：「ハルシネーション」 用語解説 野村総合研究所(NRI)）

AIに関する他の論点（２）

（３）偽情報・フェイクニュース対策

・生成AIによって生成されたかどうかを判定するソフトの開発

・インターネット上の情報発信者を第三者機関が認証する「OP（Originator Profile）技術」の活用

（２）（３）について、

【４つの原則（日本ファクトチェックセンター：古田大輔編集長）】
①情報の発信元の身元をチェックすること。
②他者から誤りが指摘されていないか調べること。
③報道機関や公的機関の情報と照合すること。
④情報ソースから正確に引用しているか確認すること。
（出典：偽ニュースから身を守る最新事例と対策の4原則- 日本経済新聞(nikkei.com)）

今後の活動について

・関西および中部地区のメンバーにより、Zoom開催を中心に研究会を開催していく。

・引き続き新技術や新制度のほか、タイムリーな事件・事項を取り上げ、システム監査の観点から検討する。

・特に、生成型AIについては、現在進行形であり、今後も取り上げて研究対象としたい。

・また、システム監査基準やガイドラインについても、その内容をより深く理解・研究していきたい。

参考文献・資料

・パナソニック ホールディングスHP
「パナソニック コネクトのAIアシスタントサービス「ConnectAI」を自社特化AIへと深化」
https://news.panasonic.com/jp/press/jn230628-2，最終閲覧日2024年6月3日

・松田貴典「生成ＡI活用のガイドライン項目とそのポイント」2023年12月5日
（「次世代のシステム監査研究PJ発表資料」）

・松田貴典「生成ＡＩの活用と課題－ChatGPTを中心に課題と対策－」
2024年2月27日（「次世代のシステム監査研究PJ発表資料」）

・文部科学省 初等中等教育局編 「初等中等教育段階における 生成AIの利用に関する暫定的なガイドライン」
2023年7月4日

・サイダス社 「生成AIの利用ガイドライン_第1版」2023年5月公開

・一般社団法人日本ディープラーニング協会」「生成AIの利用ガイドライン」2023年5月1日

・文化庁文化審議会著作権分科会法制度小委員会 「AIと著作権に関する考え方について（素案）（令和6年2月29日時点版）」2024年

・荒牧裕一「AIと著作権について－著作権法第30条の4の解説を中心に－」2024年3月27日（「次世代のシステム監査研究PJ発表資料」）

ご清聴ありがとうございました。