

生成AIの利用に関する基本的な考え方(案)

この資料はA Iの技術的仕様を説明するものではなく、使用にあたっての基本的な考え方について整理したものである。
また、本資料の内容は、情報セキュリティ規程および個人情報保護規程に従って運用されるものとする。

1 背景

近年、画像生成や文章生成を含む生成A Iの利用が急速に拡大しており、著作権、内容の正確性、成果物の責任範囲等に関する課題が各所で指摘されている。

特に画像・文書の生成においては、利用者側の理解不足が原因となり、トラブルや誤解が生じる事例も見受けられる。

本資料は、行政内部における生成A Iの適切な利用を図るにあたり、基礎的な考え方を整理するものである。

2 生成AIと従来の制作依頼との類似性

生成A Iによる成果物の生成は、画家の工房や文筆家の事務所等に制作を依頼する事と類似している点が多い。絵の制作を例とした場合、以下のような流れが共通している。

- (1) 依頼者が内容を指定し、工房が試作（必要に応じ複数案）を提示する。
- (2) 内容の指定がない部分については、工房が過去に修得した技術や作例を基に絵柄・要素等を判断し、依頼内容に沿うと考えられる形で制作する。
- (3) 指定がある場合はその内容に沿って制作するが、精度向上のため追加説明を必要とすることがある。
- (4) キャラクター等の特定要素を指定する場合、依頼者が資料（ラフ等）を提供し、それを基に制作が行われる。
- (5) 成果物に対して依頼者が瑕疵（間違いや権利侵害など）がないかを確認（検収）し、問題なければ受領する。

生成A Iも同様に、指示内容に応じて成果物を生成し、指定のない部分は学習データの傾向に基づいて補完するなど同様のプロセスを持ち、生成物に対しては利用者が瑕疵がないかを確認の上で使用する必要がある事も同じである。

3 生成AI利用における利用者側の課題

生成A Iの仕組みが理解されないまま利用されることにより、次のような誤認や問題が発生する可能性がある。

- ・ A Iの生成物を「自身の能力の拡大」や「才能の獲得」と誤認すること
- ・ A Iが自律的に判断しているかのように扱うこと
- ・ 生成物を確認せず、そのまま提出・公開すること

これらは、著作権侵害、誤情報の拡散、成果物の品質低下等の重大なトラブルにつながるおそれがあるため、厳に注意が必要である。

4 利用者が理解すべき基本的な考え方

生成A Iの利用にあたり、利用者は以下について必ず理解しておく必要がある。

- (1) 生成A Iを利用することは、あくまでも外部に制作を依頼していることと同様であること。
- (2) 生成A Iは、画家や文筆家と異なり、意図の理解・説明、違法性の判断等を行うことができないこと。
- (3) 生成された成果物を提出・公開する際の最終責任は、A Iではなく利用者本人にあること。
- (4) 生成A Iの利用にあたっては、外部への依頼の場合に機密情報が漏れないよう厳しく情報を制限するのと同じく、入力するデータの取り扱いにも注意を要すること。

これらの理解が欠ける場合、利用者側・A Iシステム側の双方に望ましくない結果をもたらす可能性がある。

5 まとめ

生成A Iは行政事務の効率化等に寄与する一方、適切な理解のないまま利用すると、法令遵守、情報管理、品質確保の面で問題が生じる可能性がある。

生成A Iを活用する際には、利用者が最終責任を負うという原則を徹底し、成果物の確認、権利関係の配慮、内容の正確性の確保等を行うことが不可欠である。

(補足)

生成AIの抱える問題

- ・A Iが学習したデータセットには無断使用のデータ群が含まれている可能性がある事。
- ・人間の思考プロセスとは異なり、A Iは求められた正解に最も近くなるよう、学習したデータから合成している事。

この二つを同時に内包しているため、工房などであれば注意を払うはずの著作権問題やハルシネーション（事実と異なる内容をもっともらしく生成してしまう現象）の出力といった問題が発生しやすく、使用者が生成物をよりシビアにチェックする事が求められる現状にある。

生成AIが市場に与える問題

生成A Iは工房などの制作速度とは比較にならないほど早く大量に生成物を出力して市場を歪めるおそれのあることが指摘されており、識別するためにA I生成物であることを示すマーキング（透かしなど）をデータに自動的に内包させるといった改善の余地がある状況である。

生成AIと人間の関係

注意しなければならないのは、生成A I自体は人間のように思考しているのではなく、正解に近くなるようデータを組み合わせたり形を変えたりしているのであり、生成A Iの学習に必要なデータは依然

として人間の創造したものが求められているという事である。

つまり、生成A Iはあくまでも人間を補佐するものであり、成果物を得るための技能などバックグラウンドストーリーと言えるものは今も人間の手の中にあり続けているという事を忘れずに、生成A Iと向き合う事が重要である。

(参考資料)

1. 行政における生成AI活用の最新指針

- ・行政の進化と革新のための生成A I の調達・利活用に係るガイドライン（デジタル庁）

<https://www.digital.go.jp/news/3579c42d-b11c-4756-b66e-3d3e35175623>

※ 行政事務における適切な利用とリスク管理

- ・自治体におけるA I 活用・導入ガイドブック（総務省）

https://www.soumu.go.jp/menu_news/s-news/01gyosei04_02000155.html

※ 自治体向けの具体的なひな形や、ハルシネーションへの留意事項を含む

2. 著作権と権利侵害に関する法的解釈について

- ・令和5年度 著作権セミナー「A I と著作権」資料（文化庁）

<https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html>

※ 著作権侵害の判断基準、創作的寄与（人間がどこまで関与したか）の考え方について

- ・都立学校生成A I 利活用ガイドライン（東京都）

https://shintosei.metro.tokyo.lg.jp/post_lp07_250512/

※ 権利侵害を避けるための具体的な行動ルール、教育現場の視点での留意点について

3. AIの透明性と識別性について

- ・A I 戦略会議 資料（内閣府 広島A I プロセス関連）

https://www8.cao.go.jp/cstp/ai/ai_senryaku/ai_senryaku.html

※ 国際的な枠組み（広島A I プロセス）に基づくA I 生成コンテンツの識別の重要性についての議論を含む

4. 利用者が理解すべき基本的な考え方

- ・初等中等教育段階における生成A I の利活用に関するガイドライン（文部科学省 資料）

https://www.mext.go.jp/content/20241226-mxt_shuukyo02-000030823_001.pdf

※ A I は意図を理解しているわけではないという点や、情報の真偽確認の徹底を含む

- ・テキスト生成A I の導入・運用ガイドライン（IPA 独立行政法人 情報処理推進機構 中核人材育成プログ

ラム)

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/generative-ai-guideline.html

※ 生成A I の活用、リスク管理などについて

5. 生成AIと人間の関係性(大規模言語モデルの仕組み)について

- ・大規模言語モデル (LLM) の光と影 (国立国会図書館 調査及び立法考査局 資料)

<https://dl.ndl.go.jp/view/prepareDownload?itemId=info:ndljp/pid/14102350>

- ・大規模言語モデルの現状と今後 (内閣府 消費者委員会 消費者をエンパワーするデジタル技術に関する専門調査会 資料)

https://www.cao.go.jp/consumer/kabusoshiki/digital_technology/doc/007_240910_shiryoul.pdf