尾張旭市 生成AI利用ガイドライン（試行用）

試行第1.0版　令和5年8月8日制定

1. 本ガイドラインの目的

本ガイドラインは、職員が市の業務において生成AI（特にOpenAIのChatGPT）の利用に関する基本的な方針を定めるものです。

生成AIは業務効率の改善や新しいアイデア出しに役立つ一方で、入力するデータの内容や生成物の利用方法によっては法令に違反したり、他者の権利を侵害したりする可能性があります。本ガイドラインは、これらの問題を避けるための注意事項を解説します。

なお、当ガイドラインは、利用する生成AIの利用規約の改正や、社会の動向、世論等の変化を踏まえ、随時見直しを行います。

2. 本ガイドラインが対象とする生成AI

本ガイドラインが対象とする生成AIは、OpenAI社が提供するChatGPTです。

> 生成AIとは、入力文字に応答してテキスト、画像、または他のメディアを生成することができる人工知能システムのこと。主な生成AIは以下のとおり。
> ・ChatGPT、BingAI、Bard、Midjourney、Stable Diffusion等

3. 生成AIの利用が禁止される用途

本市では、以下の用途・業務での生成AIの利用を禁止します。

(1)行政サービスの公平性、透明性を確保できない業務

(2)機密情報、個人情報、プライバシー情報を扱う業務

> 主な生成AIの用途
> ・文章（議事録）の要約、翻訳又は平易に書き改めること。
> ・文書（あいさつ文、メールまたはホームページ等）の文面を作成すること。
> ・文章を校正、改善すること。
> ・公開されている情報や文章を表などに整理すること。
> ・着想を得る、又はアイデアを発展させること。
> ・エクセルの関数やマクロ等のプログラムを作成又は修正すること。
> ・その他、業務の効率化や行政サービスの向上に資するもの。

4. 本ガイドラインの構成

生成AIは、いずれのサービスも基本的に「ユーザーが何らかのデータを入力して何らかの処理（保管、解析、生成、学習、再提供等）が行われ、その結果（生成物）を得る」という構造です。

本ガイドラインは以下の2つのパートから構成されています。

▼　データ入力に際して注意すべき事項

▼　生成物を利用するに際して注意すべき事項

5. データ入力に際して注意すべき事項

生成AIに入力するデータは多種多様なものが含まれますが、知的財産権の処理の必要性や法規制の遵守という観点からは、特定の種類のデータを入力する場合、特に注意が必要です。

(1)第三者が著作権を有しているデータ（他人が作成した文章等）

単に生成AIに他人の著作物を入力するだけの行為は著作権侵害に該当しません。もっとも、生成されたデータが入力したデータや既存のデータ（著作物）と同一・類似している場合は、当該生成物の利用が当該著作物の著作権侵害になる可能性もありますので注意してください。具体的には「6（2）生成物を利用する行為が誰かの既存の権利を侵害する可能性がある 」の部分を参照してください。

また、ファインチューニング（微調整）による独自モデルの作成や、いわゆるプロンプトエンジニアリング※のために他者著作物を利用することについても原則として著作権侵害に該当しないと考えられます。

※プロンプトエンジニアリングとは、AIに対して適切な質問や指示を与えることで、より望ましい結果を引き出す技術です。

(2)登録商標・意匠（ロゴやデザイン）

商標や意匠として登録されているロゴ・デザイン等を生成 AI に入力することは商標権侵害や意匠権侵害に該当しません。

もっとも、この点は著作物と同様、あくまで「入力行為」に関するものである点に注意が必要です。故意に、あるいは偶然生成された、他者の登録商標・意匠と同一・類似の商標・意匠を商用利用する行為は商標権侵害や意匠権侵害に該当します。

すなわち、生成AIにロゴやデザインを入力する際には登録商標・意匠の調査の必要性は乏しいですが、生成物を利用する場合には調査が必要です。

(3)著名人の顔写真や氏名

著名人の顔写真や氏名を生成 AI に入力する行為は、当該著名人が有しているパブリシティ権※の侵害には該当しません。

ただし、生成AIを利用して生成された著名人の氏名、肖像等については、それらの氏名や肖像等を利用する行為はパブリシティ権侵害に該当する場合がありますので注意してください。

※パブリシティ権とは、有名人や著名人が、自己の氏名や肖像などについて、対価を得て第三者に専属的に使用させ得る権利のことです。

(4)個人情報

ChatGPTにおいては入力したデータがOpenAI社のモデルの学習に利用されることになっているため、個人情報を入力しないでください。

(5)他者から機密保持義務を課されて開示された機密情報

外部事業者が提供する生成 AI に、他者との間で秘密保持契約（NDA）などを締結して取得した秘密情報を入力する行為は、生成 AI 提供者という「第三者」に秘密情報を「開示」することになるため、NDA に反する可能性があります 。

そのため、そのような秘密情報は入力しないでください。

(6)機密情報

ChatGPT に機密情報を入力しないでください。

（尾張旭市情報セキュリティ対策基準の機密性２以上の情報は入力しない。）

6. 生成物を利用するに際して注意すべき事項

生成 AI からの生成物が、既存の著作物と同一・類似している場合は、当該生成物の利用が当該著作物の著作権侵害になる可能性もあります。そのため、生成物をそのまま利用することは極力避け、できるだけ加筆・修正するようにします。

(1)生成物の内容に虚偽が含まれている可能性がある。

大規模言語モデル（LLM）の原理は 、「ある単語の次に用いられる可能性が確率的に最も高い単語」を出力することで、もっともらしい文章を作成していくものです。書かれている内容には虚偽が含まれている可能性があります。

生成 AI は学習データにないことは答えられません。例えば、ChatGPT は 2021 年 9 月までのデータで学習したため、それ以降の事項については答えられないか誤った回答をします。そのため、学習データの範囲をきちんと確認してください。

生成 AI のこのような限界を知り、その生成物の内容を盲信せず、必ず根拠や裏付けを自ら確認するようにしてください。

(2)生成物を利用する行為が、誰かの権利を侵害する可能性がある。

① 著作権侵害

生成 AI からの生成物が、既存の著作物と同一・類似している場合は、当該生成物を利用（複製や配信等）する行為が著作権侵害に該当する可能性があります。

そのため、以下の留意事項を遵守してください。

・特定の作者や作家の作品のみを学習させた特化型 AI は利用しないでください。

・プロンプトに既存著作物、作家名、作品の名称を入力しないようにしてください。

・特に生成物を「利用」（配信・公開等）する場合には、生成物が既存著作物に類似しないかの調査を行うようにしてください。

② 商標権・意匠権侵害

画像生成 AI を利用して生成した画像や、文章生成 AI を利用して生成したキャッチコピーなどを製品のロゴや広告宣伝などに使う行為は、他者が権利を持っている登録商標権や登録意匠権を侵害する可能性がありますので、生成物が既存著作物に類似しないかの調査に加えて、登録商標・登録意匠の調査を行うようにしてください。

③ 虚偽の個人情報・名誉毀損等

ChatGPT などは、個人に関する虚偽の情報を生成する可能性があることが知られています。虚偽の個人情報を生成して利用・提供する行為は、個人情報保護法違反（法19 条、20 条違反）や、名誉毀損・信用毀損に該当する可能性がありますので、そのような行為は行わないでください。

(3)生成物について著作権が発生しない可能性がある。

仮に生成物に著作権が発生していないとすると、当該生成物は基本的に第三者に模倣され放題ということになりますので、自らの創作物として権利の保護を必要とする個人や組織にとっては大きな問題となります。

この論点については、生成 AI を利用しての創作活動に人間の「創作的寄与」があるか否かによって結論が分かれますので、生成物をそのまま利用することは極力避け、できるだけ加筆・修正するようにしてください。

(4)生成 AI のポリシー上の制限に注意する。

生成 AI においては、これまで説明してきたリスク（主として法令上の制限）以外にも、サービスのポリシー上独自の制限を設けていることがあります。

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、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ます。

【補足事項】

このガイドラインの作成に当たっては、一般社団法人日本ディープラーニング協会作成の「生成 AI の利用ガイドライン第１版」（令和５年５月公開）を参考にしています。