

志賀町 生成 AI の利用ガイドライン

第 1.0 版 2023 年 7 月 制定

1 本ガイドラインの目的

本ガイドラインは、職員が町の業務で ChatGPT などの生成 AI を利用する際に注意すべき事項を解説したものです。

生成 AI は、業務効率の改善や新しいアイデア出しなどに役立つ反面、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。本ガイドラインをよく読んでいただき、生成 AI を上手に利用してください。

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。それ以外の生成 AI の利用を希望する場合にはデジタル情報課にお問い合わせください。

3 生成 AI の利用が禁止される用途

当町では以下の用途・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

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。

そのため、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（送信）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、以下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。

(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 を利用して生成物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商用利用する行為はパブリシティ権侵害に該当しますので注意してください。

(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きますので、ChatGPT に個人情報（氏名・住所等）を入力する場合、当該個人情報により特定される本人の同意を取得する必要があります。そのような同意取得は現実的ではありませんので、個人情報を入力しないでください。

(5) 他社から秘密保持義務を課されて開示された秘密情報

外部事業者が提供する生成 AI に、他社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) 自組織の機密情報

機密情報を生成 AI に入力する行為は何らかの法令に違反するということはありませんが、生成 AI の処理内容や規約の内容によっては当該機密情報が法律上保護されなくなったり特許出願ができなくなったりしてしまうリスクがありますので、入力しないでください。

6 生成物を利用するに際して注意すべき事項

(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 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既存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商品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りますので、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) 生成物を商用利用できない可能性がある

生成 AI により生成した生成物をビジネスで利用する場合、当該生成物を商用利用できるかが問題となります。

この論点は、利用する生成 AI の利用規約により結論が左右されますが、ChatGPT の場合、生成物の利用に制限がないことが利用規約に明記されているので、この点は問題になりません。

(5) 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 を利用する場合、以下の点に注意してください。

Usage Policies (<https://openai.com/policies/usage-policies>) で、「Adult content, adult industries, and dating apps（アダルトコンテンツ、アダルト産業、出会い系アプリ）」
「Engaging in the unauthorized practice of law, or offering tailored legal advice without a qualified person reviewing the information（許可なく法律実務を行うこと、または資格のある人が情報をレビューしないままに特定の法的助言を提供すること）」などの具体的禁止項目が定められています。

また、医療、金融、法律業界、ニュース生成、ニュース要約など、消費者向けにコンテンツを作成して提供する場合には、AI が使用されていることとその潜在的な限界を知らせる免責事項をユーザに提供する必要があることも同ポリシーには明記されています。

さらに、関連ポリシー上は、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。】

以上