行方市生成 AI の利用ガイドライン

第 1.0 版 令和 6 年 3 月 19 日制定
行方市総務部資産経営課 DX 推進室

1 はじめに

本ガイドラインは、職員が業務遂行のために ChatGPT などの生成 AI を利用する際に注意すべき事項をまとめたものです。

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おそれがあるため、このガイドラインの内容を十分に理解したうえで、生成 AI を適正に利用してください。

なお、本ガイドラインにおいて「生成AI」とは、自然言語による対話形式で入力した情報に対して、AIが新たなデータを生成して出力する「約款による外部のサービス*1」のことをいいます。

*1 不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスのこと。

2 対象とする生成 AI

職員が業務において利用できる生成AIは、以下のとおりとします。

〇一般社団法人デジタル田園都市国家構想応援団「公務員専用 AI マサル」

〇その他 統括情報セキュリティ責任者及び情報政策担当課長の許可を得たもの

3 用途

生成 AI の用途は、次に掲げるものとします。

(1) 文章の要約、翻訳または平易に書き改めるもの
(2) 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もの
(3) 文章を校正、改善するもの
(4) 公開されている情報や文章を表等に整理するもの
(5) 着想を得るまたはアイデアを発展させるもの
(6) 表計算ソフトで関数やマクロ等を作成または修正するもの
(7) 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 生成 AI の利用を禁止する事項

以下の用途・業務での生成 AI の利用を禁止します。

(1) 個人情報、特定個人情報（個人番号を含む個人情報）、その他個人を特定できる情報を取り扱う業務
(2) 機密情報を取り扱う業務
(3) 未決定事項や公表すべきでない内容

（4）意図的な悪用や攻撃行為、迷惑行為を助長する内容

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、以下の類型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）

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が、生成されたデータについて、入力したデータや既存のデータ（著作物）と同一・類似している場合には、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るため十分に精査する必要があります。

（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が、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する可能性があります。

（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が、生成 AI を利用して生成された著名人の氏名、肖像等を利用する行為はパブリシティ権の侵害に該当します。

（4）個人情報

生成 AI に個人情報にあたる情報を入力することは禁止されていることから、入力する際にはそのような情報がないかを十分に確認する必要があります。

（5）機密情報

本市の機密性の高い情報を生成 AI に入力する行為は禁止されていることから、入力する際にはそのような情報がないかを十分に確認する必要があります。

（6）他者から秘密保持義務を課されて開示された秘密情報

生成 AI に、他者から秘密保持義務を課されて開示された秘密情報（以下、「秘密情報」という。）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り、秘密保持義務違反につながることから、入力する際にはそのような情報がないかを十分に確認する必要があります。

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

大規模言語モデル（LLM）の基本的な原理は、「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あるため、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。このような仕組みをもつ生成 AI の利用にあたり、その生成物の内容を過信せず、必ず根拠や裏付けを自ら確認する必要があります。

（2）誰かの既存の権利を侵害する可能性

〇著作権侵害

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、公開等）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、次の留意事項を遵守してください。

・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すること。

・生成物を利用する場合には、生成物が既存著作物に類似しないかの調査を実施すること。

〇商標権・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等を商品ロゴや広告宣伝等に使う行為は、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恐れがあるため、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・登録意匠の調査をする必要があります。

〇虚偽の個人情報・名誉毀損等

生成 AI 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から、虚偽の個人情報を生成して利用・提供する行為は、個人情報保護に関する法律や、名誉毀損・信用毀損に該当する可能性があるため、そのような生成文書を利用してはいけません。

（3）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及びルール等（主として法令上の制限）以外にも、サービスのポリシー上、サービス提供者が独自の制限を設けていることがあるため、その制限に抵触しないように利用する必要があります。

7 利用の停止

生成AIの利用規約等の変更や新たなリスクの発生等が認められた場合は、統括情報セキュリティ責任者は、利用の停止を決定し、その旨を職員に周知します。

8 その他

本ガイドラインは、生成AIの機能や環境、利用状況や変化に合わせ、適宜見直しを行います。

以上