

宝塚市生成 AI 利用ガイドライン

令和 6 年 (2024 年) 3 月

宝塚市

目次

第 1 本ガイドラインの目的	1
第 2 本ガイドラインの対象	1
1 対象となる生成 AI システム	1
2 対象となる職員等	1
第 3 生成 AI を利用する際の基本事項	2
1 事前に所属長の許可を得ること	2
2 留意事項	2
3 適切な生成物を得るための工夫が必須であること	2
第 4 データの入力に際して留意すべき事項	3
1 入力不可の情報	3
(1) 宝塚市情報公開条例第 7 条の非公開情報	3
2 入力に注意を要する情報	4
(1) 職務上知り得た秘密	4
(2) 第三者が著作権を有しているデータ(他者が作成した文章等)	4
(3) 登録商標・意匠(ロゴ・デザイン等)	4
(4) 著名人の氏名や肖像	4
第 5 生成物の利用に際して留意すべき事項	5
1 内容の正確性を確認し、修正加工すること	5
2 AI による生成物であることの表示	5
3 その他の留意事項	5
(1) 生成物の内容には誤りや偏りが含まれている可能性がある	5
(2) 生成物を利用する行為が他者の権利を侵害する可能性がある	6
(3) 生成物に著作権が発生しない可能性がある	7
(4) 生成物を営利目的で利用できない可能性がある	7
(5) 個々の生成 AI システムの利用規約上の制限を確認する	7
第 6 生成 AI の効果的な使用方法	7
(1) 具体的に指示する	7
(2) 質問を重ねる	7
(3) 生成 AI が理解しやすい構成にする	8
(4) 生成 AI に役割を与える	8
(5) 情報の検索や計算には不向きであることを理解する	8
第 7 その他	8
1 問題発生時の対応	8
2 ガイドラインの改訂等	8

第 1 本ガイドラインの目的

生成 AI は、画像や音楽、文章など様々なデータを学習し、新しいコンテンツを生成することができる AI です。従来の AI は与えられたデータの分析や予測ができますが、生成 AI では与えられたデータから新しい情報や作品を創ることができるため、よりクリエイティブな分野での活用が期待されています。

生成 AI は、有効に活用すれば、業務の効率化や生産性の向上、市民サービスの向上につながる可能性がある一方で、入力された内容を学習し、その内容を利用して生成する可能性があるため、情報漏洩に繋がるおそれがあります。また、著作権の侵害や回答が正確でない可能性もあります。業務で活用する際は、その特性を理解し、正しく利用することが重要です。そのため、市の業務で使用する際のガイドラインを作成しました。

第 2 本ガイドラインの対象

1 対象となる生成 AI システム

生成 AI を用いた情報システム（無償で提供される外部サービスを含む。以下「生成 AI システム」という。）を対象とします。文章等の生成機能と他の機能を組み合わせた情報システム（例：音声から文字起こしを行う会議録作成支援システムに生成 AI による要約機能を組み合わせたもの）も対象となるので留意してください。

なお、本ガイドラインは、文章生成 AI システムを念頭に置いて記載していることから、画像、動画、音声、音楽等を生成するものについては、内容が不十分な可能性があります。画像等の生成 AI システムを導入する際は、情報セキュリティ対策、著作権、商標権等に十分留意してください。

2 対象となる職員等

生成 AI システムを利用しようとするすべての職員を対象とします。

市から業務委託を受ける外部の事業者および市の指定管理者に対しても本ガイドラインに沿った対応を求めることとします。生成 AI による生成物を含む成果物の取扱い等について別紙の「生成 AI の利用に関する特記事項」を事業者および指定管理者に遵守させてください。

第3 生成 AI を利用する際の基本事項

1 事前に所属長の許可を得ること

職員が外部サービスとして無償で提供される生成 AI システムを業務で利用する場合は、事前に所属長の許可を得ること。所属長は、職員にガイドラインが定める留意事項を十分確認させてください。

なお、利用許可の対象となるのは、入力データを学習しない設定（オプトアウト）が可能な生成 AI システムに限るものを原則とします。職員は、オプトアウトを選択して利用すること。

また、外部サービスでメールアドレスによる利用登録が要求される場合は、職場電子メールアドレスで行い、利用するにあたりアカウント等の作成が必要になる場合の認証情報の取り扱いについては、市情報セキュリティポリシー「共通実施手順（認証情報管理編）」を参照してください。

有償で導入した生成 AI システムの利用については、当該システムを所管するセキュリティ責任者の指示に従うこと。

2 留意事項

生成 AI システムを利用する際は、他の情報システムの利用の際と同様、次の各号に掲げる行為を禁止しています。

- (1) 業務に関連しない目的で情報システムを利用すること。
- (2) 法令又は公序良俗に反した利用を行うこと。
- (3) 他の利用者又は第三者の著作権、人権及びプライバシーを侵害するおそれのある利用を行うこと。
- (4) 情報の改ざん、き損及び滅失並びに虚偽の情報提供を行うこと。
- (5) 通信を阻害する行為及び情報資産に損害又は不利益を及ぼす利用を行うこと。

また、生成 AI システムは基本的に「ユーザーがデータを入力し、AI が処理を行い、ユーザーが生成物を得る」ものであることから、個別の留意すべき事項については、「データの入力」と「生成物の利用」の 2 つの側面に分けて次章以降で示します。

「第 4 データの入力に際して留意すべき事項」

「第 5 生成物の利用に際して留意すべき事項」

3 適切な生成物を得るための工夫が必須であること

生成 AI システムに入力する指示や条件を含むテキストのことを「プロンプト」といいます。生成物の質は入力するプロンプトの質に依存することから、生成 AI システムの利用時は、具体的に指示する、質問を重ねる等、適切な生成物を得るための工夫が必須です。

詳しくは「第 6 生成 AI の効果的な使用方法」を参照してください。

第4 データの入力に際して留意すべき事項

1 入力不可の情報

(1) 宝塚市情報公開条例第7条の非公開情報

個別に契約するなど、情報セキュリティが担保されたものを除き、ChatGPT のような、約款による外部サービス（民間企業等が不特定多数のユーザーに対して同一条件で提供するサービス）については、入力内容が漏洩・多目的利用されない保証がありません。このため、宝塚市情報公開条例第7条に規定する非公開情報を入力しないこと。

生成 AI システムについては、入力した内容が学習に利用され、他の利用者に表示される可能性も指摘されているため、特に留意すること。生成 AI に限らず、情報セキュリティが担保されていないインターネット上のサービス・システムに非公開情報を入力することはできません。

【参考】宝塚市情報公開条例第7条で定める非公開情報一覧

号数	非公開理由	
第1号	個人に関する情報	<ul style="list-style-type: none"> ・特定の個人を識別することができるもの（他の情報と照合することにより、特定の個人を識別することができることとなるものを含む） ・特定の個人を識別することはできないが、公にすることにより、なお個人の権利利益を害するおそれがあるもの
第2号	法人等に関する情報	<ul style="list-style-type: none"> ・法人等又は事業を営む個人の権利、競争上の地位その他正当な利益を害するおそれがあるもの
第3号	公共の安全等に関する情報	<ul style="list-style-type: none"> ・人の生命若しくは身体に危険を及ぼすもの ・犯罪を誘発し、その他公共の安全と秩序を維持する上で支障が生じるおそれがあるもの
第4号	法令秘等に関する情報	<ul style="list-style-type: none"> ・法令又は他の条例により公にしない旨を定めているもの
第5号	市の内部又は国等との間における審議、検討又は協議に関する情報	<ul style="list-style-type: none"> ・率直な意見の交換若しくは意思決定の中立性が不当に損なわれるおそれ又は特定の者に不当に利益を与え若しくは不利益を及ぼすおそれがあるもの
第6号	事務又は事業に関する情報	<ul style="list-style-type: none"> ・事務又は事業の適正な遂行に著しい支障を及ぼすおそれがあるもの

※詳しくは、宝塚市情報公開条例及び「情報公開条例解説」を参照のこと。

2 入力に注意を要する情報

(1) 職務上知り得た秘密

職務上知り得た秘密を生成 AI システムに入力する行為は、第三者である生成 AI 提供事業者
にその秘密を漏洩する行為となり、地方公務員法第 34 条に違反する可能性があるため、注意す
ること。

(2) 第三者が著作権を有しているデータ(他者が作成した文章等)

単に生成 AI システムに他者の著作物を入力するだけの行為は、「著作物に表現された思想又
は感情の享受を目的としない利用」に当たるため、原則として著作権侵害に該当しない(著作権
法第 30 条の 4)。また、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
者の著作物を利用する行為も、同規定により、原則として著作権侵害に該当しないと考えられる。
ただし、他者が著作権を有する著作物と生成物が類似している場合は、当該生成物の利用が著
作権侵害に当たる可能性があるため注意すること。

※生成 AI システムでは入力するプロンプトの質が出力の質を左右することから、プロンプトを工夫することで出力の質
を高める手法(=プロンプトエンジニアリング)に注目が集まり、盛んに研究されている。

(3) 登録商標・意匠(ロゴ・デザイン等)

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 システムに入力することは商標権・
意匠権の侵害に該当しない。一方で、他者の登録商標・意匠と類似する商標・意匠を営利目的で
利用する行為は、商標権・意匠権の侵害に該当する可能性がある。著作権については、既存の著
作物と類似する生成物が偶然生成された場合、当該生成物を利用(公開等)しても著作権侵害に
該当しない余地があるが、商標・意匠については類似の生成物が偶然生成された場合であって
も、当該生成物を営利目的で利用すると商標権侵害・意匠権侵害に該当する可能性がある。この
ため、ロゴ・デザイン等を入力する時点では登録商標・意匠の調査の必要性は乏しいが、生成物を
利用する場合には調査が必要である。

(4) 著名人の氏名や肖像

著名人の氏名や肖像(顔写真等)を生成 AI システムに入力する行為は、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ないと考えられるが、著名人の氏名や肖像を含む生成物を
営利目的で利用する行為はパブリシティ権の侵害に該当する可能性があるため注意すること。

第 5 生成物の利用に際して留意すべき事項

1 内容の正確性を確認し、修正加工すること

生成 AI による生成物は、一見もっともらしい内容であっても、不正確、不適切な内容を含んでいる可能性があります。また、生成物に関する説明責任や生成物の利用に関する責任は生成 AI の利用者側にあり、利用者には生成物が最終的に公開されても支障のない内容であることを担保する責務があります。このため、生成物の利用に当たっては、複数の職員で正確性、妥当性を十分確認すること。また、生成物をそのまま利用することは避け、原則として修正加工を行った上で利用すること。特に市民への応答や、市民が直接利用するサービスには、生成物をそのまま利用しないこと。

2 AI による生成物であることの表示

生成 AI システムの利用規約（例えば OpenAI）では、AI による生成物をあたかも人が作成したものであるかのように表示することを禁じたり、AI による生成物であることを第三者が認識できるように表示したりする義務を課すものがあります。AI による生成物を利用する場合は、こうした義務の有無を確認し、利用規約に沿った対応をすること。

なお、利用規約において表示の義務がない場合でも、AI による生成物の修正加工を行わずにそのまま利用する場合は、「〇〇AI による生成」「〇〇AI による生成物をそのまま掲載」等と表示すること。

【参考】ChatGPT の利用規約は OpenAI の利用規約類を参照 (<https://openai.com/policies>)

3 その他の留意事項

(1) 生成物の内容には誤りや偏りが含まれている可能性がある

生成 AI には次のような限界があることを認識し、生成物の内容を過信せず、必ず根拠や事実関係を複数の職員で確認した上で利用すること。

ア 内容の誤り

文章生成 AI の基盤となる大規模言語モデル (LLM: Large Language Model) の原理は、「ある単語の次に用いられる可能性が確率的に高い単語」を出力することで、もっともらしい文章を生成する点にあります。ある単語の次に用いられる確率の高い単語がその文脈の中で常に適切な単語であるとは限らず、文章生成 AI が意味を理解して出力しているわけでもないため、生成物には常に誤りが含まれている可能性があります。

また、生成 AI は通常ある特定の時点までのインターネット上の情報を学習させて作成されており、学習した時点以降の事柄には回答できないか、誤った回答をする可能性が高いため、最新の事柄に関する生成物には注意が必要です。

イ 偏り

生成 AI は通常インターネット上の情報を学習させて作成されているため、生成物に意図しない偏りが含まれている可能性があります。その偏りに気づかないまま生成物を利用することにより、個人や集団を不当に差別することになるおそれがあります。

ウ 法的判断、医学的判断など

法的判断を含む事項は弁護士法との関係で、健康状態及び治療に関する判断を含む事項は医師法との関係で問題となる可能性があります。

また、行政の重大な意思決定に関する事項については、生成AIシステムの利用規約上、利用が禁じられている例が多いことも踏まえ、これらの事項を含む生成物の利用は避けること。

(2) 生成物を利用する行為が他者の権利を侵害する可能性がある

ア 著作権侵害

生成物が既存の著作物と同一又は類似している場合は、生成物を利用（複製、配信等）する行為が著作権侵害に該当する可能性があるため、以下の事項に留意すること。

- ・特定の作者の著作物のみを学習させた特化型生成 AI は使用しないこと
- ・プロンプトに既存の著作物の作者名、作品名を入力しないこと
- ・生成物を公開する場合は、生成物自体を検索サービスに入力してテキスト・画像検索するなどして、既存の著作物と類似していないか事前に調査すること

イ 商標権侵害等

生成したキャッチコピー等を営利目的で使う行為は、他者が権利を持つ登録商標権や登録意匠権を侵害する可能性があるため、生成物が既存の著作物に類似していないかの調査に加えて、特許情報プラットフォーム（J-PlatPat）を活用するなどして、登録商標・登録意匠の調査を事前に行うこと。

ウ 名誉毀損等

生成 AI は人に関する誤った情報を生成する可能性があります。特定の人に関する情報を生成し利用すれば、名誉棄損や信用棄損、個人情報保護法違反に該当する可能性があるため、そのような行為は行わないこと。

(3) 生成物に著作権が発生しない可能性がある

生成物に著作権が認められるかどうかは、人の創作的な関与があったかどうかによります。業務の目的により、利用する生成物に著作権を発生させる必要がある場合は、生成物の全部又は一部を用いて加工編集するといった、人による明確な創作行為を介在させるようにすること。

(4) 生成物を営利目的で利用できない可能性がある

例えば OpenAI の利用規約では生成物の利用には特に制限がない旨が記されているが、サービスによっては生成物を営利目的で利用できない可能性があるため、生成 AI システムの利用規約を確認すること。

(5) 個々の生成 AI システムの利用規約上の制限を確認する

生成 AI システムごとに提供者が定めた利用規約があります。サービスによっては、本ガイドラインとは異なる規定も含めて、利用規約で独自の制限を設けている可能性があるため、それぞれの利用規約を確認すること。

【参考】ChatGPT の利用規約は OpenAI の利用規約類を参照 (<https://openai.com/policies>)

第 6 生成 AI の効果的な使用方法

生成 AI は、文書作成（要約、言い換え、翻訳、文案作成）やアイデア出し（企画、提案）に有効ですが、生成物の質は入力するプロンプトの質に依存します。生成 AI システムから適切な回答を引き出すため、下記の要点を参考にプロンプトを工夫しましょう。

(1) 具体的に指示する

生成 AI システムに対する指示は、具体的に行う方がよい。単に求める結果だけを記すのではなく、回答の条件や期待する回答のイメージをできるだけ具体的に記すのが望ましい。

悪い例) 「以下の文章を要約して」

良い例) 「以下の文章を 100 字以内で小学生でもわかるように要約して」

(2) 質問を重ねる

一度のプロンプトで適切な回答を引き出せなくても、「もっと具体的に教えて」「それはどういう意味ですか」など追加の質問を行うことで回答の精度を上げることができます。二度、三度と質問を重ねることが重要です。

(3) 生成 AI が理解しやすい構成にする

単なる文章ではなく、命令文と条件を分けて記述するなど、生成 AI が理解しやすい構成にすることで回答の精度を上げることができます。例えば「#命令文」や「#条件」のように記号「#（シャープ）」を付してまず項目名を記す、個々の条件は箇条書きにするなどが効果的とされています。

(4) 生成 AI に役割を与える

立場や目的・背景をはっきりさせたり、出力形式を指定したりするなど、生成 AI に役割を与えることで回答の精度を上げることができます。

(5) 情報の検索や計算には不向きであることを理解する

生成 AI が学習している情報は通常、ある特定の時点までのインターネット上の情報であるため、最新の情報を検索することには向いていません。また、複雑な計算は間違える場合があります。生成 AI の特徴を知ることによって効果的に業務に活用することができます。

第 7 その他

1 問題発生時の対応

生成 AI システムの利用において情報セキュリティに関わる問題（例：不適切な使用方法が発覚、不適切な表現を含む生成物を公表）が発生した場合は、直ちに情報セキュリティ責任者（所属長）に報告し、必要な措置を講じること。

2 ガイドラインの改訂等

生成 AI は進化の速度が著しい技術です。生成 AI の性能や業務利用を進める上で生じた課題等に対応するため、逐次改訂を行います。

委託業務に係る特記仕様書

【生成 AI の利用に関する特記事項】

第1 委託事業者（受注者及び受注者から業務の一部を再委託された事業者を含む。以下「乙」という。）及び乙の作業要員は、委託事務を処理するに当たり、生成 AI（人工的な方法により学習、推論、判断等の知的機能を備え、かつ、質問その他のコンピュータに対する入力情報に応じて当該知的機能の活用により得られた文章、画像、音声等の結果を自動的に出力するよう作成されたプログラム及び当該プログラムと連携して動作するプログラムをいう。以下同じ。）を利用する場合は、委託事務の処理の過程において第三者の知的財産権その他一切の権利を侵害し、又は成果物が第三者の知的財産権その他一切の権利を侵害しないように対応しなければならない。

第2 乙は、委託事務を処理するに当たり、生成 AI を利用する場合には、委託事務の処理に関して知り得た秘密及び個人情報を生成 AI に入力してはならず、生成 AI の出力結果を確認し、必要に応じて修正した上で成果物として発注者に提出しなければならない。

指定管理業務に係る特記仕様書

【生成 AI の利用に関する特記事項】

第1 指定管理者（以下「乙」という。）及び乙の作業要員は、指定管理業務を実施するに当たり、生成 AI（人工的な方法により学習、推論、判断等の知的機能を備え、かつ、質問その他のコンピュータに対する入力情報に応じて当該知的機能の活用により得られた文章、画像、音声等の結果を自動的に出力するよう作成されたプログラム及び当該プログラムと連携して動作するプログラムをいう。以下同じ。）を利用する場合は、指定管理業務の実施の過程において第三者の知的財産権その他一切の権利を侵害し、又は成果物が第三者の知的財産権その他一切の権利を侵害しないように対応しなければならない。

第2 乙は、指定管理業務を実施するに当たり、生成 AI を利用する場合には、指定管理業務の実施に関して知り得た秘密及び個人情報を生成 AI に入力してはならず、生成 AI の出力結果を確認し、必要に応じて修正した上で成果物として市に提出しなければならない。

更新履歴

版	発行日	改定内容
第 1 版	令和6年(2024年)3月1日	初版発行

(本ガイドラインに関する問い合わせ先)

生成 AI の活用全般に関すること 生成 AI 研究 WG

生成 AI を活用した業務効率化に関すること 経営改革推進課、総務課
 情報セキュリティに関すること 情報政策課

非公開情報、例規等に関すること 総務課

このガイドラインは次の著作物を改変して利用しています。兵庫県生成AI利用ガイドライン(本文) 第 1.1 版および同付録

I Q&A集