流山市生成AI利用ガイドライン概要

1　本ガイドラインの目的

本ガイドラインは、職員等が業務で生成AI（注１）を利用する際に注意すべき事項を定めるものである。

生成AIは、業務効率の改善や新しいアイデア創出等に有効となる反面、入力するデータの内容や生成物の利用方法によっては、情報が他者に漏洩し拡散される、法令に違反する、他者の権利を侵害する可能性がある。

そこで、本ガイドラインを確認のうえ、生成AIを利用することとする。

2　本ガイドラインの対象

本ガイドラインは、ChatGPT（注２）、LoGoAIアシスタント（注３）、QommonsAI（注４）を対象とする。

3　本ガイドラインの適用範囲

本ガイドラインは、職員が業務において生成AIを利用する場合に適用される。

4　生成AIの用途

本市では、生成AIの用途を次に掲げるものとする。

（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）エクセルの関数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

5　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の利用を禁止する。

（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）市内部での情報共有に留める内容

（５）意図的な悪用や攻撃行為、迷惑行為を助長する内容

（６）著作権に関する内容

6　生成AIを利用・構築する場合の手続き

（１）生成AIを利用する場合

職員は利用する生成AIが受けている許可対象となっているシステム及び入力可能な情報を確認したうえで適切に使用すること。

利用にあたり、本ガイドラインを確認し、内容をよく理解のうえ適切に使用すること。

（２）生成AIを構築（外部サービスの利用を含む）する場合

生成AIを含むシステムを構築する場合は、入力情報が許可なくモデルの学習に利用されないことやシステムを提供する事業者による監査等に用いられないこと等について、情報セキュリティ管理者である各課室等の所属長の審査・許可を受けること。

7　データ入力に際して注意すべき事項

7．1　個人情報

生成AIにおいては入力したデータがAIモデルの学習に利用される場合があるため、ChatGPT等の生成AIに個人情報（顧客氏名・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る。

そのような同意取得は現実的ではないため、個人情報の入力は禁止する。

７．２　他機関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、他機関との間で秘密保持契約（NDA:Non-Disclosure Agreement）（注５）等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る。

そのため、そのような秘密情報の入力は禁止する。

７．３　自組織の機密情報

流山市情報セキュリティポリシーで規定している「機密性２」（行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要しないが、直ちに一般公表することを前提としていない情報資産）以上の情報の入力を禁止する。

また、自組織内の機密情報（ノウハウ等）については、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る、特許出願ができなくなるリスクがあるため、入力を禁止する。

８　生成物を利用するに際して注意すべき事項

８．１　判断の責任は人間である職員自身にある

業務における検討・判断の責任は人間である各職員にあり、生成 AI は業務執行にあたっての単なる補助的なツールに過ぎない。

各職員が適切に生成 AI の活用範囲を判断し、自らの責任の下に利用すること。

生成 AI は本市の状況、各地域の状況の詳細を把握しているものではない。

また、生成 AI の出力には、虚偽や偏りのある意見等を含む可能性がある。

生成 AI は、インターネット上の情報を基に学習していることが多いため、生成される回答は多数派の意見が尊重され、少数派の意見が反映されにくい傾向にある。

そのため、返答においては差別・偏見等のバイアスが含まれている可能性があり、その回答に基づいた判断をしてしまうことによって個人及び集団が不当に差別されないよう注意すること。

また、学習データの起点が古い場合、社会情勢や社会情勢等の変化に対応できず、必ずしも目指すべき社会を実現するための回答を得られるわけではない。

そのことを十分に認識し、業務遂行（政策決定や市民からの相談に対する回答等）に当該出力をそのまま用いることはしないこと。

生成 AI は、追悼文等受け取る方の感情に寄り添う必要がある文章にそのまま用いることはしないこと。

８．２　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:Large Language Model）（注６）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ある。

書かれている内容には虚偽が含まれている可能性がある。

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、裏付けや事実を自ら確認すること。

８．３　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る。

そのため、以下の留意事項を遵守する。

・特定の作者や作家の作品のみを学習させたことが判明した場合は利用しない。
・プロンプト（注７）に既存著作物、作家名、作品の名称を入力しない。

・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。

（２）商標権・意匠権侵害

生成 AI を利用して生成したキャッチコピー等を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可能性があるため、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・登録意匠の調査を行う。

（３）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。

虚偽の個人情報を生成して利用・提供する行為は、個人情報の保護に関する法律違反（第 19 条、第 20 条違反）や名誉毀損・信用毀損に該当する可能性があるため、そのような行為は行わない。

８．４　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、上記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ため、注意する。

また、関連ポリシー上は、生成 AI 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等が定められているため、生成物を加工せずにそのまま利用する場合や一部に引用した場合は、「【生成 AI 名】により作成」と資料中に明記し、利用したチャット内容を記録しておく。

９　生成 AI の利用における問題の報告と利用の停止

生成 AI の利用で問題が発生した場合は、直ちに情報セキュリティ管理者である各課室等の所属長及び情報政策部門に報告し、必要な措置を実施するものとする。

また、生成 AI の利用規約の変更、新たなリスクの発生等が認められた場合、情報政策部門は、一時的な利用の停止を決定し、その旨を職員に通知するものとする。

10　用語解説

（注１）生成 AI

あらかじめ学習したデータをもとに、画像・文章・音楽・デザイン等を新たに作成する人工知能（AI）の総称

（注２）ChatGPT

OpenAI 社によって開発された、自然言語処理技術を活用し人工知能が自然な会話を行うことができるシステム

（注３）LoGoAI アシスタント

株式会社トラストバンクが提供する自治体向けビジネスチャット「LoGo チャット」で対話型 AI を利用できる自治体専用の生成 AI サービス

（注４）QommonsAI

Polimill 株式会社社が提供する自治体業務に特化した生成 AI サービス

（注５）秘密保持契約（NDA:Non-Disclosure Agreement）

商談や取引等を通じて開示される秘密情報について、本来の目的外での使用や第三者への開示・漏えいを防止するために締結するもの

（注６）大規模言語モデル（LLM:Large Language Model）

大量のテキストデータを使用して学習した自然言語処理のモデル

（注７）プロンプト

記号を用いて画面上にコマンド入力位置を表示するもの