狭山市生成ＡＩ利用ガイドライン

第一版　令和５年８月２９日　市長決裁

膨大な学習データに基づき文章や画像等を作成する生成ＡＩは、社会にイノベーションを引き起こす力を持つ技術として、飛躍的な発展と爆発的な利用拡大を遂げており、日常生活のみならず、企業や公共団体においても業務効率化とサービス向上に向けて活用が進んでいる。

しかし、その一方で、生成ＡＩによって生成された文章等（以下、「生成物」という。）には、虚偽情報の蔓延や第三者の権利侵害、機密情報の漏洩等の懸念・リスクも確認されていることから、業務で生成ＡＩを利用する上では、これらの懸念・リスクを正しく理解し、あくまでも業務の補助的な利用にとどめ、生成物をそのまま使用するのではなく、最終的には職員が確認し判断することが求められる。

以上を狭山市職員の共通認識として共有し、生成ＡＩを適切かつ安全に利用するため「狭山市生成ＡＩ利用ガイドライン」（以下、「本ガイドライン」という。）を定める。

１　目的

本ガイドラインは、本市職員が業務効率化や市民サービス向上のために生成ＡＩを業務において利用するにあたり、生成ＡＩの安全な利用と生成物の適切な取扱いを確保するために必要な事項を定めるものである。

２　定義

本ガイドラインにおいて「生成ＡＩ（※1)」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（※2)」のことをいう。

（※1)「ジェネレーティブＡＩ（Generative AI)」とも呼ばれるＡＩ（人工知能）の一種であり、楽曲や画像、動画、プログラムのコード、文章など生成する。生成ＡＩはＡＩが自ら答えを探して学習する「ディープラーニング（深層学習)」を用いて構築された機械学習モデルである。

（※2）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。

３　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、入力情報を学習データとして利用しないよう設定できる（以下、「オプトアウト（※3)」という。）ものに限る。なお、当面の間、利用時に自動的にオプトアウトが設定される一般社団法人デジタル田園都市国家構想応援団（※4）が提供する「行政用ＣｈａｔＧＰＴマサルくん３．５」のみを対象とする。

（※3）製品やサービスを通じた個人データの第三者への提供を、本人の希望に応じて停止すること。生成ＡＩに入力された情報は、ＡＩの学習のために利用されることがあり、オプトアウ

トをしていない場合、万が一機密情報等を生成ＡＩに入力してしまった場合、ＡＩが知識として蓄え、第三者に漏洩してしまうリスクがある。

（※4）デジタル田園都市国家構想の実現に不可欠な官民連携を目的に自治体や法人会員等が自主的に結集して組織した団体。

4　用途

本市では、以下の用途において生成ＡＩを利用できるものとする。

(1) 文書案の作成や校正等を行う際の補助的手段
(2) 事務事業案の企画等を行う際の補助的手段
(3) 各種資料案の作成等を行う際の補助的手段
(4) 表計算ソフトで関数やマクロ等を作成する際の補助的手段

5　利用における遵守事項

職員が業務において生成ＡＩを利用する場合は、次に掲げる事項を遵守すること。

(1) チャットオフ（チャット履歴を残さないこと）及びオプトアウトを必ず設定すること。
(2) 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補助的ツールに過ぎないことを理解した上で、各職員が適切な利用を判断し、自らの責任の下に利用すること。

6　情報の入力における遵守事項

情報の入力にあたっては、上記第５(1)のとおり、チャットオフ及びオプトアウトの設定をした上で利用することとしているが、その設定下においても、情報保護や法規制遵守の観点から、以下のデータについては入力を禁止する。

(1) 狭山市セキュリティポリシー第２章２(２)アに掲げる重要性分類Ⅰ（個人情報及び業務上必要とする最小限の者のみが扱う情報）に属する情報及び重要性分類Ⅱ（公開することを予定していない情報）に属する情報の入力
(2) 事業者等から秘密保持義務を課された上で取得した秘密情報の入力
(3) 非公開情報や公開前情報の入力

7　生成物の利用における遵守事項

職員が生成物を業務に利用する場合は、次に掲げる事項を遵守すること。

(1) 生成ＡＩ 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繋ぎ合わせる」という原理に基づいて“もっともらしい”文章を作成しているため、生成物の内容には虚偽が含まれている可能性があることから、生成物の内容について必ず根拠や裏付けを確認すること。
(2) 生成物の内容について、倫理的に問題がないこと、著作権や商標権などの第三者の権利を侵害していないこと、第三者の生命・身体・財産に危害を及ぼすことがないこと等を必ず複数の職員で確認すること。

(3) 生成物はあくまでも参考として利用することとし、生成物の内容に対しては原則として加筆又は修正を行うこと。

８　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、情報セキュリティ責任者（情報政策課長）は、利用の停止を決定し、その旨を職員に周知する。

９　その他

本ガイドラインは、生成ＡＩの機能や環境、利用等の状況や変化に合わせ、適宜見直しを行う。

附則

本ガイドラインは、令和５年９月１日から施行する。