三田市生成 AI の利用ガイドライン

令和６年１月制定

１　目的

生成 AI は、業務効率の改善や新しいアイデア出し等に役立つ反面、入力したデータがバックグラウンドで学習され、第三者の回答に利用される可能性がある等、情報が他者に漏洩・拡散されるリスクがある。また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恐れがある。

本ガイドラインは、三田市情報セキュリティポリシー（第２章９　外部サービスの利用）に基づき、三田市職員が業務で ChatGPT 等の生成 AI(以下「生成 AI」という。)を利用することに関して、遵守すべき事項を定めるとともに、本市の業務における生成 AI 利用に関するルールを示すことで、個人情報などの市民の権利、財産を守ることを前提に生成 AI を利用することを目的として解説するものである。

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、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、質問その他の電子計算機に対する指令に応じて当該知的機能の活用により得られた結果を自動的に回答するよう作成されたプログラムとする。

また三田市職員が業務で利用可能な生成AIは、次のとおりである。

○ 株式会社トラストバンクが提供する「LoGo AIアシスタントbot版」

○ その他所属長及び情報セキュリティ所管課長の許可を得たもの

３　本ガイドラインの構成

生成AIは、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」という構造である。このことから、本ガイドラインでは次の観点から構成する。

○ 生成AIの利用が禁止される事項

○ データの入力に際して注意すべき事項

○ 生成物の利用に際して注意すべき事項

４　生成 AI の利用が禁止される事項

生成AIは入力等を行った内容をデータとして蓄積・学習することが考えられるため、情報保護の観点から三田市情報公開条例第7条各号に定める非公開情報に該当するような、以下の直接的な内容を含めた生成AIの利用を禁止する。

○ 個人情報及び特定個人情報

○ 守秘義務を課されている情報

○ 法人その他の団体に関する情報で漏洩することにより当該団体の利益を害するおそれのある情報

○ 漏えいした場合、行政に対する信頼を著しく害するおそれのある情報

○ その他、三田市情報公開条例第7条に定める非公開情報に該当する情報

5　データの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るが、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、特に注意すること。

5-1　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ないが、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こと。

5-2　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ないが、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るため、生成されたものを利用する場合は十分に調査を実施すること。

5-3　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ないが、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するため注意すること。

5-4　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こと。

5-5　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こと。

5-6　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こと。

6　生成物を利用するに際して注意すべき事項

6-1　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る。

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る。

6-2　誰かの既存の権利を侵害する可能性

○ 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る。そのため、次の留意事項を遵守すること。

・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。

○ 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こと。

○ 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ないこと。

6-3　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こと。

6-4　生成 AI による生成物であることの表示

生成AIのサービスポリシーにおいて表示の義務がない場合においても、AI による生成物を取捨選択、修正加工を行わずにそのまま利用する場合は、「生成AI により生成」「生成AI による生成物をそのまま掲載」等と表示すること。

7　その他

7-1 問題発生時

生成AIの利用において情報セキュリティに関わる問題が発生した場合は、直ちに所属長及び情報セキュリティ所管課長に報告し、必要な措置を講じること。

7-2　ガイドラインの改定等

生成AI は進化の途上にある新しい技術である。本ガイドラインも、生成AI の開発状況に応じて、あるいは職員から寄せられた疑義や業務利用を進める中で生じた新たな課題、さらには職員の利用実態に照らして生じ得ると想定される課題に適時対応するため、逐次改定を行う。

以上