狭山市生成AI利用ガイドライン

令和8年4月30日 全部改正

1 本ガイドラインの目的

本ガイドラインは、狭山市職員による生成AIの適正な利用を促進するため、狭山市職員が、生成AIシステムを利用する際に遵守・留意すべき事項等を定めるものである。

2 定義

本ガイドラインにおける以下の語句の定義を示す。

語句	定義
生成AI	Generative Artificial Intelligence。文章、画像、音声、プログラム等を生成できるAI（人工知能）およびその技術の総称。
生成AIシステム	生成AIが組み込まれたシステムや生成AIと連携したシステム。
プロンプト	主に対話型生成AIに対して、利用者が入力する指示や命令文またはあらかじめ組み込まれた指示や命令文。
LLM	Large Language Models（大規模言語モデル）。生成AIの一種。膨大なテキストデータと高度なディープラーニング技術を用いて構築された、自然言語処理を行うAIモデル。
RAG	Retrieval-Augmented Generation（検索拡張生成）。生成AIが、あらかじめ用意した文書、狭山市独自で保有するデータベースやweb検索などの外部データを検索し、当該外部データを根拠とした回答を生成すること。
オプトアウト	利用者の入力データやプロンプト及び生成AIシステムの出力結果を学習データとして利用することを拒否する設定。
ハルシネーション	生成AIが事実に基づかない回答を生成すること、またはその生成物。
要機密情報	「狭山市情報セキュリティポリシー」の情報セキュリティ対策基準で定める機密性１または２に該当する情報資産。
管理責任者	企画経営課 行革推進デジタル戦略担当課長
管理担当者	企画経営課　デジタル戦略担当職員
運用管理者	生成AIシステムを利用する所属の長
利用者	生成AIシステムを利用する職員

3 本ガイドラインの対象・利用環境

本ガイドラインの適用対象とする行政機関の範囲は、内部部局、行政委員会、議会事務局及び地方公営企業とする。

本ガイドラインの適用対象とする生成 AI システムは、管理責任者が別表の通り指定するものとし、これらに該当しない生成 AI システムの利用は原則禁止する。なお、指定外の生成 AI システムの利用を希望する場合、事前に管理責任者と協議し、利用環境や取り扱う情報に応じて関係所管を交えた審議の後、利用の可否を判断する。

4 生成 AI システムの利用に係るルール

生成 AI システムを利用する際は、「狭山市情報セキュリティポリシー」とあわせて、以下の（１）利用前のルール及び（２）利用中のルール①、②を遵守すること。また、業務の質や効率の向上を図るため、本ルールの範囲内で生成 AI の積極的な利活用を行うこと。

（１）利用前のルール

ア 生成 AI システムを利用する前には、管理責任者が指定する資料を必ず確認すること。

イ 生成 AI の利用は、様々な便益が期待される一方、要機密情報の流出やハルシネーションなどのリスクがあることを理解すること。

ウ 生成 AI システムごとの利用方法、セキュリティ上の留意点、生成物の精度及びリスクの程度を理解すること。

エ 管理責任者から求めがあった場合、生成 AI システムへの入力データ又はプロンプト、出力結果等を提供する必要がある旨を事前に了解すること。

オ オプトアウト機能を有した生成 AI システムを利用する場合でも、個人情報を含む機密性２の情報資産及び秘密保持契約のもと事業者から秘密保持義務を課されたうえで取得した情報については、生成 AI システムへ入力または学習はしてはならないこと。

（2）利用中のルール

① 入力データ又はプロンプトにおけるルール

ア 生成 AI システムの生成物は、利用者が入力するデータおよびプロンプトの内容と密接に関連しており、これらの入力が生成結果に対して極めて大きな影響を及ぼすことを認識すること。

イ 利用者側の不理解やミスにより生じるリスクがあることを踏まえて、利用目的の範囲内で生成 AI システムを適切に利用すること。

ウ 生成物の正確性を無用に損なうことがないように、生成 AI システムにプロンプトやデータ入力する前に、正確かつ最新のデータであることを利用者自身でチェックすること。

② 生成物利用におけるルール

ア 利用目的に応じて求められる正確性の水準が異なることを意識し、生成 AI システムの出力結果やその情報源を確認すること。

イ 生成 AI システムの出力結果に基づいて行われた判断も説明責任の対象に含まれることに留意すること。

ウ 生成 AI システムの出力結果を業務に利用するか責任を持って判断を行うこと。判断がつかない場合は利用しないこと。

エ 正確性や根拠・事実関係をリスクに応じて必要な範囲内で確認すること。

オ 安全性・公平性・客観性・中立性等に問題がないことを確認し、問題のある表現は必ず加除修正すること。

カ 生成 AI の生成物については、その利用目的や利用範囲に応じて、運用責任者の承認を得ること。

5 生成 AI システム特有のリスクケースへの対応

生成 AI システムは、その特徴から、その出力結果に関して、生成 AI システム特有のリスクケースが発生する可能性がある。以下に、生成 AI システム特有のリスクケースの例を示す。

［例 1］生成 AI が人種・性別・文化等に関する偏見や差別を含む社会的に大きな問題となり得る出力を行った。

［例 2］生成 AI が攻撃的又は危険なコンテンツを生成した。

［例 3］ハルシネーションにより、利用者がその情報を利用したことによって利用者若しくは第三者に不利益を与えた。

［例 4］利用者が生成 AI により既存の作品に類似し、著作権の侵害等の問題が生じる可能性が高いコンテンツを意図せず生成し、利用したことで当該作品に係る権利者等から削除等の申出を受けた。

生成 AI システム特有のリスクケースが発生した場合、重要度・影響の程度等を踏まえ、以下の手順に沿って速やかに適切な対応を行うこと。

（１）検知内容の報告

生成 AI システム特有のリスクケースを検知した者は、ワークフロー「生成 AI システム特有のリスクケースの検知報告フォーム」に必須項目を記載し、管理責任者に報告すること。

「狭山市情報セキュリティポリシー」で定めるセキュリティインシデントに該当する事象を検知した場合は、直ちに同ポリシーで定める手順で報告すること。

（２）対処

生成 AI システム特有のリスクケースを検知した者は、必要に応じ管理責任者の指示を仰ぎながら、業務影響特定・原因特定・暫定対応措置・恒久対応措置等を実施すること。

（３）対応結果の報告

生成 AI システム特有のリスクケースを検知し、しかるべき対応した者は、ワークフロー「生成 AI システム特有のリスクケースの対応報告フォーム」に必須項目を記載し、管理責任者に報告すること。

6 本ガイドラインの変更

本ガイドラインの変更は、生成 AI の技術進展や、AI 法・個人情報保護法の改正等の国におけるルール整備の動向等を踏まえて、適時適切に行う。

以上

別表

生成 AI システム名	利用可能な業務の範囲	入力可能な情報
自治体用 AI ヤマトくん	業務目的での汎用的な利用※1	要機密情報に該当しない情報
QommonsAI	業務目的での汎用的な利用※1	機密性１以下の情報※2

表に掲げる生成 AI システムは、全てオプトアウト機能を有する。

※1 以下①～④に該当する利用に限る

① 文書案の作成及び校正等の補助

② 事務事業案の企画等の補助

③ 各種資料案の作成等の補助

④ 表計算ソフト等における関数やマクロ作成等の補助

※2　機密性の分類は、「狭山市情報セキュリティポリシー」における情報セキュリティ対策基準で定める情報資産の分類を参照