資料3
議会報告資料

草津市　文章生成 AI
利活用ガイドライン（案）

令和6年　月

草津市

目次

Ⅰ　はじめに

1　生成 AI とは

生成 AI(または生成系 AI)とは、「Generative AI:ジェネレーティブAI」とも呼ばれ、入力された情報に基づき、新たな文章、画像等を生成できるAIです。

（代表的な生成 AI の例）

文章生成 AI	入力された文章等に基づき、新たな文章を生成
画像生成 AI	入力された文章等に基づき、新たな画像を生成
動画生成 AI	入力された文章等に基づき、新たな動画を生成
音声生成 AI	入力された文章等に基づき、新たな音声を生成

2　ガイドラインの目的

令和3年3月に策定した「草津市行政経営改革プラン」では、行政経営の課題を解決するための「改革に向けた実施計画（アクション・プラン）」に「行政運営の効率化（情報化推進計画に基づく取組の推進）」を掲げ、先端技術の活用を推進しています。

生成AIについては、自治体や企業での利用が急速に広がる中、本市においても導入の可能性を検証するため、実証実験を行い、活用の有効性を確認したところです。

一方で、入力したデータが AI に学習され、利用されるといった情報漏洩のリスク、事実とは異なる不正確な回答を生成するリスク、知的財産権等をはじめとする他者の権利を侵害するリスクなど、様々な危険性が指摘されています。

本ガイドラインは、こうした危険性を回避しながら、生成 AI を効果的・効率的に活用するため、草津市情報セキュリティポリシーに基づき、職員が遵守すべき事項を示すものです。

3 ガイドラインの対象範囲

(1)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「文章生成AI(以下『生成AI』という。)」とします。また、生成 AI がバックグラウンドで動作するサービス(文章の要約機能を提供するサービスなど)、生成 AI と連携して動作するプログラムもガイドラインの対象とします。

なお、生成 AI の利用に当たっては、申請許可の実施手順の遵守、入力情報がAIの学習に利用されない一定のセキュリティが担保されたシステムの導入等、草津市情報セキュリティポリシーに基づく適正な対応が必要です。

(2)対象者

本ガイドラインの対象者は、「草津市情報セキュリティポリシー」の適用範囲に掲げる全ての職員等とします。

Ⅱ　利活用に当たって

1　生成 AI のリスク

生成 AI は、行政事務の様々な場面に活用できる可能性がある一方で、様々なリスクが潜んでおり、適切に利用するために、そのリスクについて十分に理解する必要があります。

①　情報漏洩

入力したデータ等が AI に学習されることで、第三者の回答に利用されるなど、外部に流出するおそれがあります。

②　回答の不正確性

生成された情報については、虚偽や偏りのある意見等の不正確な情報を含む可能性があります。生成 AI については、「ある単語の次に続く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するため、虚偽の内容を回答するおそれがあります。

また、インターネット上の情報を学習していることが多く、回答に偏りが生じるおそれや、最新の情報を学習していないことで、誤った回答をしてしまうおそれもあります。

③　知的財産権等の権利の侵害

生成 AI がインターネット上から学習した情報の中には、著作権・商標権・意匠権等の知的財産権として法律上保護されているものがあり、生成物によっては、これらの権利を侵害するおそれがあります。

（参考）代表的な知的財産権

著作権	著作物（思想または感情を創作的に表現したものであって、文芸、学術、美術または音楽の範囲に属するもの）を保護。
商標権	商標（商品・サービスを区別するために使用するマーク・ネーミング等）を保護。
意匠権	意匠（独創的で美感を有する物品の形状、模様、色彩等のデザイン等）を保護。

④　個人の権利の侵害

生成ＡＩは、個人に関する誤った情報を生成する可能性があり、誤った個人情報を利用・提供する行為は、個人情報保護法違反や、名誉毀損・信用毀損等に該当するおそれがあります。

また、人権侵害にも留意が必要です。生成 AI は、インターネットから多くの情報を収集し、学習しています。インターネット上では、SNS 等において、他人への誹謗中傷や侮辱、プライバシーの侵害、いじめ、特定の民族や国籍の人々を排斥する差別的言動、部落差別等を助長するような投稿など、人権に関わる様々な問題が発生しており、これらの内容が生成AIの回答に含まれるおそれがあります。

一人ひとりの職員が人権を基調とする行政の担い手であるという認識のもと、生成 AI を利用する必要があります。

２　禁止事項

前述のリスクを踏まえ、生成 AI の利用に当たっては、以下に示す事項を禁止します。

①　個人情報・機密情報の入力

入力した個人情報・機密情報（※）が生成 AI に学習され、外部へ流出するリスクを避けるため、個人情報・機密情報の入力はしないでください。複数の情報の組合せにより個人情報・機密情報となるおそれがありますので、十分に注意してください。

また、個人情報等の収集を目的として利用しないでください。生成される情報は虚偽の内容を含むことがあり、個人情報保護法違反や名誉毀損・信用毀損等の個人の権利の侵害につながるおそれがあります。

個人情報・機密情報の入力を避けるために、質問を一般化・抽象化することが重要です。ただし、複数の情報を組み合わせることにより個人が特定できる場合等は、個人情報・機密情報に該当しますので、注意してください。

※機密情報とは、草津市情報セキュリティポリシーにおける「機密性２」以上の情報を指します。

（参考）機密性による情報資産の分類　※草津市情報セキュリティポリシーから引用

分類	分類基準	取扱制限
機密性3	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する情報資産	・私物パソコンでの作業禁止（機密性3の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の外部記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・外部記録媒体の施錠可能な場所への保管
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は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性1	機密性2又は機密性3の情報資産以外の情報資産	―

（参考）不適切な利用と許容される利用の例

不適切な利用例	許容される利用例
○○さん（個人の氏名）からの以下の問合わせに対する回答を作成してください。	市民からの以下の問合わせに対する回答を作成してください。
○○氏の住所を教えてください。	※個人情報の収集はいかなる場合でも認められません。
草津市において計画している△△△の設置（未公開の情報）について、懸案事項を挙げてください。	地方自治体（または市町村）において△△△を設置する場合の懸案事項を挙げてください。

② 加筆・修正を加えない状態での利用

生成された情報は、不正確な情報や偏りのある意見、他者の権利を侵害する情報等を含むおそれがあるため、そのまま利用せず、あくまでも補助的なツールとして、必ず職員による確認を行い、加筆・修正の上、利用するようにしてください。

③ 業務目的以外の利用

業務目的以外の利用については、厳に慎んでください。

3 利用用途

(1)推奨する利用用途

生成 AI の活用により効果が見込まれる利用用途例については、下記のとおりです。

① 文章案の作成

入力した情報に基づき、文章案を作成することができます。

（想定される用途）

メールの文面、挨拶文、資料作成の補助

② 文章の要約

指定した字数・形式で要約文を作成することができます。

（想定される用途）

国・県からの通知文、議事録等の要約

③ 文章の校正

既存の文章について、誤字、脱字、句読点の誤り等のチェック・修正や文章表現の調整を行うことができます。

④ 文章の翻訳

様々な言語で文章の翻訳を行うことができます。

⑤ アイデア出し

指定したテーマ・条件に基づき、幅広い視点からアイデア出しを行うことができます。

（想定される用途）

企画・施策の立案、アンケートの項目出し等の補助

⑥　Excel の関数、VBA 等

関数やマクロのコード等を作成することができます。

（2）活用のポイント

①　質問を明確にする

生成物の目的（挨拶文、プレスリリース、企画提案資料等）、対象（職員向け、児童向け等）、役割（〇〇課の職員、市長等）、その他前提条件等を指示として与えることで、回答精度の向上につながります。

②　繰り返し質問する

一問一答で完璧な回答を求めるのではなく、追加の情報を与えることにより回答精度の向上につながります。

（3）推奨しない利用用途

生成 AI は、「ある単語の次に続く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するため、虚偽の内容を回答するおそれがあります。

また、学習したデータを基に生成するため、学習元のデータが最新のものではない場合、不正確な情報を含むおそれがあります。

このことから、以下に示すような「事実の確認」を利用用途とすることは推奨しません。

①　インターネット検索の代替としての利用

事実の確認・情報収集等のため、インターネット検索の代替としての利用は避けてください。

②　専門性の高い情報の確認

法律の解釈等の専門性が高い情報については、特に情報の正確性が求められます。

不正確な情報が含まれることにより、判断を誤るリスクがあることから、専門性の高い情報の確認については、専門家に確認することなどとし、生成AIの利用は避けてください。

Ⅲ　その他

その他留意事項等

(1)　問題発生時の対応

生成 AI の利用に当たって、情報セキュリティに関わる問題(個人情報・機密情報の漏洩、虚偽・不適切な表現を含む生成物の公表等)が発生した場合は、直ちに草津市情報セキュリティポリシーに基づき、必要な措置を講じてください。

(参考)情報セキュリティインシデントの報告　※草津市情報セキュリティポリシーから引用

(1)庁内での情報セキュリティインシデントの報告

①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口(情報政策担当課)に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③情報セキュリティ管理者は、当該情報セキュリティインシデントについて、CISO 及び情報セキュリティ責任者に報告しなければならない。

(2)住民等外部からの情報セキュリティインシデントの報告

①職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口(情報政策担当課)に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じて CISO 及び情報セキュリティ責任者に報告しなければならない。

(2)　ガイドラインの改定等

生成 AI を取り巻く環境については、日々変化している状況です。

本ガイドラインについても、今後、国・社会等の動向を注視しながら、運用の中で生じた課題等に対応するため、必要に応じて見直しを行います。

草津市　総合政策部　経営戦略課
〒525-8588　滋賀県草津市草津三丁目 13 番 30 号
電話：077-561-6544(直通)
FAX：077-561-2489
E-mail：keiei@city.kusatsu.lg.jp