奄美市生成AIの利用に当たってのガイドライン

第1.0版

令和7年3月

鹿児島県奄美市デジタル戦略課

生成AIの利用に当たってのガイドライン 目次

版	発行日	改定内容
第 1.0 版	令和7年3月1日	初版発行

1.目的

本ガイドラインは，奄美市職員及び奄美市会計年度任用職員（以下、「職員」という）が業務で生成AIを利用するに当たり遵守すべき事項をまとめたものです。
生成AIは，様々な事務作業や事務手続等に役立てられる反面，入力するデータの内容や生成されたデータの利用によって，個人情報や機密情報の漏えいや法令違反，他者の権利侵害となる可能性があります。
生成AIはあくまで業務効率化のための補助的なツールであり，業務における検討・判断の責任は，職員自身にあることを認識し，自らの知識・専門性にもとづき，最終的な判断を行うなど，本ガイドラインを理解しセキュリティ対策を行い適切に利用してください。

2.適用範囲

本ガイドラインが対象とする組織は，市長部局、各種委員会事務局、議会事務局、上下水道部とします。

3.対象サービス

本ガイドラインが対象とする生成AIは，大規模言語モデルを利用した生成AIとし，「入力データがAIの学習に利用されない設定」が可能であるなど，セキュリティが担保されたサービスとします。
具体的なサービスは，統括情報セキュリティ責任者（商工観光情報部長）が別途指定します。

4.利用制限

入力データがAIの学習に利用されない設定を用いた場合でも，システム運営事業者が不正利用の監視等のためユーザーが入力したデータを一定期間保存する場合があります。このため，以下に該当するデータを生成AI利用のため入力することを禁止します。

（1）秘密文書に相当する機密性を要するデータ（自治体機密性3Aに該当するデータ）

（2）個人情報を含むデータ（自治体機密性3Bに該当するデータ）

（3）基本的に公表することを前提としていない情報（自治体機密性3Cに該当するデータ）

（4）自治体機密性3に相当する機密性は要しないが、直ちに一般公表することを前提としていない情報（自治体機密性2に該当するデータ）

（5）自治体機密性2以上に該当するデータを使用する場合は、匿名化等により自治体機密性1相当の情報資産へ加工、または情報セキュリティ管理者の承認を得なければならない。

（6）第三者が著作権や登録商標，意匠（ロゴやデザイン）を有するデータ

●機密性についての格付の定義

格付の区分	分類の基準
自治体機密性3	A 秘密文書（極秘文書、秘文書）
	B 漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報（住民記録システム、税務システム等に保存されている住民の個人情報）
	C 自治体機密性3B以上に相当する機密性は要しないが、基本的に公表することを前提としていない情報（職員の属性に基づく個人情報、入札予定価格）
自治体機密性2	自治体機密性3に相当する機密性は要しないが、直ちに一般公表することを前提としていない情報（政策検討に関する情報　等）
自治体機密性1	行政事務で取り扱う情報のうち、自治体機密性2以上に相当する機密性を要しない情報

5.生成物の利用に際して注意すべき事項

（1）生成AIに適さない利用

生成AIは，学習したデータを元にユーザーの指示に従って，文章の作成や要約，翻訳，アイデアなどを生成しますが，常に最新の情報を学習しているものではないため，検索としての利用には適していません。検索にはGoogleやYahooなどの検索サービスを利用してください。

また、ChatGPT等の生成AIは主にテキストデータを基に学習しているため、数値計算や複雑な数学的問題は苦手であり、計算目的での利用は適しません。

（2）内容の確認

文章を生成する生成AIの基盤となる大規模言語モデル（LLM）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り，書かれている内容には虚偽が含まれている可能性があります。

また，生成AI はインターネット上の情報をもとに学習しているため，学習したデータに差別・偏見等の偏りが含まれていた場合，生成物にもその偏りが反映される可能性が考えられます。
生成されたデータについては，必ず根拠や裏付けから内容を確認した上で利用してください。

（3）著作権等の侵害
生成されたデータが，第三者が著作権や商標権，意匠権（以下「著作権等」という。）を有するものと同一，又は類似している場合は，当該生成物の利用が著作権等の侵害に当たる可能性があります。特に以下の利用に関しては，著作権等の侵害に当たらないか十分に確認をしてください。

（ア）　特定の作者や作家の作品を学習させた特化型AIの利用
（イ）　入力するデータに著作物や作家名，作品名等を入力した利用
（ウ）　生成AIで生成したキャッチコピー等の利用

（4）虚偽の個人情報・名誉毀損等
生成AIの特性上，生成されたデータに虚偽の個人情報が含まれる場合があります。このようなデータを利用した場合，個人情報保護法違反や名誉毀損等に該当する可能性があります。利用に当たっては慎重な取り扱いをしてください。

（5）最終的な確認
生成されたデータの利用に当たっては，そのまま利用することは避け，上記（1）から（4）の確認を行い，必要な加筆・修正をしたものを利用してください。 加筆・修正しないで利用する場合は，必ず「**生成AIの回答を利用**」等を付記してください。

6.安全な運用・管理体制

（1）業務において生成AI利用する際は，情報セキュリティ管理者（各所属長）で内容を確認の上，利用の可否を判断してください。

（2）万一，情報流出が発生した場合は，「インシデント発生時の連絡フロー」に基づき対応してください。

（3）本ガイドラインは，今後の運用状況などを踏まえて，随時見直しを行います。