生成 AI の利用に当たってのガイドライン

第 1.0 版

令　和　６　年　３　月

鹿児島県総合政策部デジタル推進課

改訂履歴

版数	策定（改訂）日	内容
第 0.1 版	令和５年９月８日	試行利用ガイドラインを策定
第 1.0 版	令和６年３月 27 日	試行利用ガイドラインを改定し，本運用ガイドラインとして第 1.0 版を策定

生成 AI の利用に当たってのガイドライン　目次

１　目　的.....4

２　適用範囲.....4

３　対象サービス.....4

４　利用制限.....4

５　生成物の利用に際して注意すべき事項 5

６　安全な運用・管理体制.....6

（付録）

・　生成 AI の活用に向けて（解説動画）

・　文章生成 AI 活用事例集

・　ChatGPT の利用方法

・　公務員業務専用 ChatGPT「マサルくん」の利用について

・　県庁 LAN ワークフローシステムによる生成 AI 利用承認

1　目　的

本ガイドラインは，職員が業務で生成 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，鹿児島県情報セキュリティポリシーの適用範囲と同様とします。

（参考）鹿児島県情報セキュリティポリシー
第１章 情報セキュリティ基本方針
４ 適用範囲
⑴ 行政機関の範囲
本基本方針が適用される行政機関は，知事部局，出納局，各種委員会事務局，各教育機関，警察本部（警察学校及び各警察署を含む。），県立病院局，工業用水道部及び議会事務局とする。

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文章生成 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（デジタル推進課長）が別途指定します。

4　利用制限

生成 AI の利用に当たり入力したデータが，AI 学習のため二次利用される場合や，システム運営事業者が不正利用の監視等のため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。

⑴　個人情報を含むデータ（機密性３に該当するデータ）

⑵　秘密文書に相当する機密性を要するデータ（機密性３に該当するデータ）

⑶　秘密文書に相当する機密性はないが，直ちに一般に公表することを前提としていない情報を含むデータ（機密性２に該当するデータ）

⑷　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

5　生成物の利用に際して注意すべき事項

⑴　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。

⑵　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。

⑶　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

⑷　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。

⑸　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⑴から⑷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

⑴　生成 AI を利用する場合は，年度毎に，県庁 LAN ワークフローシステムにより，情報セキュリティ管理者(各所属長)の承認を受けてください。

⑵　生成 AI の利用に関しては，情報セキュリティ管理者(各所属長)で内容を確認の上，利用の可否を御判断ください。

⑶　万一，情報流出が発生した場合は，「情報流出時対処マニュアル」に基づき対応してください。

⑷　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。