

生成 AI の利用に当たってのガイドライン

第 1.2 版

令和 8 年 6 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
第 1.1 版	令和 8 年 5 月 26 日	<ul style="list-style-type: none">・「2 適用範囲」に利用可能な組織を明記・「3 対象サービス」に利用可能な生成 AI サービスを明記・「4 利用制限」を鹿児島県情報セキュリティポリシーに併せて改訂・「6 安全な運用・管理体制」から生成 AI サービスの利用等に関する所属長等の承認等を受けることを条件とする内容を削除
第 1.2 版	令和 8 年 6 月 24 日	<ul style="list-style-type: none">・「, 」を「、」に修正・「5 生成物の利用に際して注意すべき事項」に著作権等の侵害に当たらないかの確認手法を具体化するとともに、生成した画像の取扱い方等を追記。

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

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、以下のとおりとします。

- ・ 知事部局
- ・ 教育委員会
- ・ 選挙管理委員会事務局
- ・ 人事委員会事務局
- ・ 監査委員事務局
- ・ 労働委員会事務局
- ・ 地方公営企業
- ・ 議会事務局

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、以下のとおりとします。

- ・ exaBase 生成 AI for 自治体
- ・ Copilot Chat (Basic)

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。

- (1) 個人情報を含むデータ（自治体機密性 3 に該当するデータ）
- (2) 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 3 に該当するデータ）
- (3) 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

(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。

(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。

生成されたデータの利用に当たっては、そのまま利用することは避け、必ず根拠や裏付けから内容を確認し、必要な加筆・修正をしたものを利用してください。

(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特許情報プラットフォーム (<https://www.j-platpat.inpit.go.jp/>) 等を適宜活用し、所属長の確認のもと行うようにしてください。

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) 生成した画像の取扱い方

生成物を利用する行為が他者の権利を侵害することのないよう注意を払ってもなお、生成した画像については、公開することで著作権等の侵害の指摘を受ける可能性があるため、公開する可能性のある資料には利用しないでください。

また、公開予定のない資料に利用する場合でも、生成した画像であることを第三者が認識できるように、原則として、生成 AI による生成物であることを画像内に表示するとともに、生成した画像ファイルを保存する際は、生成 AI による生成物であることが容易に判別できるように、ファイル名に表記してください。

ただし、やむを得ず、画像内に生成 AI による生成物であることを表示できない場合は、画像が生成 AI による生成物であることを容易に判別できるように、画像の周囲にその旨を表示してください。

なお、公開予定のない資料に利用する際は、(3)の確認手法等を活用し、所属長の確認のもと行うようにしてください。

(5) 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扱いをしてください。

6 安全な運用・管理体制

(1) 生成 AI による生成物の利用に関しては、内容を確認の上、利用の可否を御判断ください。

(2) 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。

(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。