生成 AI の利用ガイドライン（第１版）

1 本ガイドラインの目的

本ガイドラインは，職員が業務で生成AIを利用する際に注意すべき事項を解説したものです。生成AIは，業務効率の改善や新しいアイデア出しなどに役立つ反面，入力するデータの内容や生成物の利用方法によっては法令に違反したり，他者の権利を侵害したりする可能性があります。本ガイドラインをよく読んでいただき，生成AIを上手に利用してください。

2-1 本ガイドラインが対象とする生成AI

本ガイドラインが対象とする生成AIは，OpenAI社が提供する「ChatGPT」，及びデジタル田園都市国家構想応援団が提供する「マサルくん」（以下「対象生成ＡＩ等」という。）を原則とします。

これら以外の生成AIの利用を行う場合は，必ずDX・行革推進室と事前に協議してください。

2-2 本ガイドラインが対象とする職員

庁内で，対象生成ＡＩ等を使用する本市職員とします。

なお，個人利用でアカウントを取得している職員が，当該基盤を用いて業務利用を行う場合についても，本ガイドラインの対象として含むこととします。

【解説】

生成AIは当該AIサービスの構造や処理内容によって法的リスクが異なります。そのため，業務のために生成AIの利用を許可する場合には，ホワイトリスト方式（利用してよいサービスを特定した上で列挙する方式）で指定することを原則とします。

利用する生成AI の仕様や、業務の性質、内容等により、このガイドラインで判断できないことがありましたら、DX・行革推進室や関係する機関に確認するなどして、地方自治体として適正な利用が図られるよう努めてください。

2-３ 対象生成AI等の利用承認

庁内で，対象生成ＡＩ等を利用しようとする職員は，その利用目的を明確にし，情報管理責任者（DX・行革推進室課長）の利用承認を得てから利用するものとします。

なお， 使用状況についても定期的に報告を行い，業務から逸脱した利用や情報漏えいの防止に努めてください。

【解説】

組織の承認を得ずに職員等がAIサービスを利用する，いわゆる「シャドーAI」は

誰がどのように使用しているかなどの管理ができなくなり，機密情報の漏えい等のリスクを高めることになります。事前に責任者の承認を得ることにより，利用の目的や内容が適切なものであるかチェックし，また利用状況を定期的にすることが重要です。

3 禁止する用途

本市では以下の用途・業務での生成AIの利用を禁止します。

（1）鹿嶋市電子情報セキュリティに関する規則（平成１５年規則第４９号）第９条に規定するセキュリティ分類Ⅰ類及びⅡ類に該当する情報含む内容を入力すること。

（2）対外的な資料や外部への回答を作成する場合，文書のすべてを生成AIから得られた情報をそのまま転載すること。

（3）ChatGPTの学習機能設定をオンにして業務利用すること。

【解説】

生成AIを利用する機関によっては，特定の用途での利用を禁止したい場合もあると思われます。たとえば，東京大学が2023年4月3日に公表した「生成系AI(ChatGPT，BingAI，Bard，Midjourney，Stable Diffusion等)について」においては「本学では学位やレポートについては，学生本人が作成することを前提としておりますので，生成系AIのみを用いてこれらを作成することはできません。」とされています。そのような場合は，ガイドラインにおいて一定の用途での利用を禁止することが考えられます。

鹿嶋市では，「３ 禁止する用途」にある個人情報や機密性の高い情報を入力すること，外向けの資料作成の際などに生成AIから出力された情報を加工せずにすべて転載すること，ChatGPTの学習機能をオンにして利用（※）することを禁止します。

※マサルくんは基盤上，ＡＰＩ使用のため入力情報等を学習する機能はありませんが，ChatGPTは標準で入出力情報を学習する機能を有しており，その学習機能をオフにするためには，個別のオプトアウト申請を行う必要があります。

4 本ガイドラインの構成

対象生成AI等は，いずれのサービスも基本的に「ユーザーが何らかのデータを入力して各種処理（保管，解析，生成，学習，再提供等）が行われ，その結果（生成物）を得る」という構造です。

そのため，本ガイドラインは以下の2つのパートから構成されています。

▼ データ入力に際して注意すべき事項

▼ 生成物を利用するに際して注意すべき事項

5 データ入力に際して注意すべき事項

対象生成AI等に入力（送信）するデータは多種多様なものが含まれますが，知的財産権法規制の遵守という観点からは，以下の類型のデータを入力する場合，特に注意が必要です。

（1） 第三者が著作権を有しているデータ（他人が作成した文章等）

単に対象生成AI等に他人の著作物を入力するだけの行為は著作権侵害に該当しません。

もっとも，生成されたデータが入力したデータや既存のデータ（著作物）と同一・類似している場合は，当該生成物の利用が当該著作物の著作権侵害になる可能性もありますので注意してください。具体的には「6（2）生成物を利用する行為が誰かの既存の権利を侵害する可能性がある」の部分を参照してください。

また，ファインチューニング（あるデータセットを使って事前学習（Pre-training）した訓練済みモデルの一部もしくは全体を，別のデータセットを使って再トレーニングすることで，新しいタスク向けに機械学習モデルのパラメーターを微調整すること。）による独自モデルの作成や，いわゆるプロンプトエンジニアリングのために他者著作物を利用することについても原則として著作権侵害に該当しないと考えられます。

【解説】

単に生成AIに他人の著作物を入力するだけの行為は，著作権法30条の4の「情報解析」の非享受利用に該当すると思われますので，著作権侵害のリスクはかなり低いと思われます。

また，ユーザーがファインチューニングによる独自モデル作成に際して他者著作物を利用する行為についても同様の理由で著作権侵害のリスクは低いでしょう。

さらに，いわゆるプロンプトエンジニアリングのために，ユーザーが自社サーバ内や生成AIサービス事業者のサーバ内に他人の著作物を蓄積する行為を行うことも考えられます。

プロンプトエンジニアリングとは，具体的には，生成AIにおいてより精度の高い出力を生成させるために，ユーザーの入力（プロンプト）を補完したり加工したりする行為をいいますので，当該行為自体が「情報解析」「非享受利用」に該当する，あるいは生成AIにおける出力の生成（これも「情報解析」「非享受利用」に該当すると思われます。）に「必要と認められる限度」の行為として，著作権法30条の4により適法ではないかと考えられます。

ただし「必要と認められる限度」でしか利用は認められませんので，たとえば「プロンプトエンジニアリングのためにサーバ内に他人の著作物を蓄積」しつつ，同時に「当該著作物をデータベース化して人間が参照したり読んだりすることができる」のであれば「必要と認められる限度」を超えていますので，30条の4は適用されず著作権侵害に該当すると思われます。

（2） 登録商標・意匠（ロゴやデザイン）

商標や意匠として登録されているロゴ・デザイン等を対象生成AI等に入力することは商標権侵害や意匠権侵害に該当しません。

もっとも，この点は著作物と同様，あくまで「入力行為」に関するものである点に注意が必要です。故意に，あるいは偶然生成された，他者の登録商標・意匠と同一・類似の商標・意匠を商用利用する行為は商標権侵害や意匠権侵害に該当します。

すなわち，対象生成AI等にロゴやデザインを入力する際には登録商標・意匠の調査の必要性は乏しいですが，生成物を利用する場合には調査が必要です。

（3） 著名人の顔写真や氏名

著名人の顔写真や氏名を対象生成AI等に入力する行為は，当該著名人が有しているパブリシティ権の侵害には該当しません。

ただし，対象生成AI等を利用して生成された著名人の氏名，肖像等については，それらの氏名や肖像等を商用利用する行為はパブリシティ権侵害に該当しますので注意してください。

（4） 個人情報

ChatGPTにおいては入力したデータがOpenAI社のモデルの学習に利用されることになっていますので，ChatGPTに個人情報（顧客氏名・住所等）を入力する場合，当該個人情報により特定される本人の同意を取得すれば認められるケースなども想定はされるところですが，そのような同意取得は現実的ではありませんので，個人情報の入力は禁止とします。

なお，学習機能をオフにするオプトアウト申請をしたChatGPT，ＡＰＩ使用のマサルくん，いずれのサービスについても対象生成AI等は学習機能を有していない状態になりますが，入力情報等は一定期間外部サーバに保管されることとなることから，学習機能の有無にかかわらず，個人情報の入力は一律禁止とします。

【解説】

個人情報を対象生成AI等に入力する行為が適法か否かは，当該生成AI内でのデータの取扱や，当該サービス提供者が外国にある事業者なのかによっても結論が分かれ，非常に複雑です。

たとえば，ChatGPTにおいては，オプトアウト申請により学習機能をオフにしたり，データ管理機能の追加により，対話履歴をオフに設定することで，学習に使われないようユーザーが管理できるようになっていますが，いずれも外部サービスの利用となること，また，使用に際して個人情報を入力しなくても活用は可能な基盤であることから，本ガイドラインでは一律個人情報の入力を禁止することとしています。

（5） 他社から秘密保持義務を課されて開示された秘密情報

外部事業者が提供する対象生成AI等に，他社との間で秘密保持契約（NDA）などを締結して取得した秘密情報を入力する行為は，生成AI提供者という「第三者」に秘密情報を「開示」することになるため，NDA に反する可能性があります。
そのため，そのような秘密情報は入力しないでください。

【解説】

生成AI提供者が入力データに監視目的での限定されたアクセスしかしない，あるいは一切アクセス・保存しない場合において，組織が秘密情報の利用目的として定められている目的のために生成AIに秘密情報を入力（プロンプトエンジニアリングのために利用することも含む。）して分析・生成する行為については，NDA に違反しないでしょう。一方，大規模言語モデル（LLM）の多くは入力データが学習に利用されますので，NDA違反を構成する可能性が高いと思われます。たとえオプトアウト申請をして学習機能をオフにしていても，将来のバージョンアップなどで変更されることもあるため，本ガイドラインでは一律入力を禁止しています。

（6） 自組織の機密情報

組織内の機密情報（ノウハウ等）を対象生成AI等に入力する行為は何らかの法令に違反するということはありませんが，対象生成AI等の処理内容や規約の内容によっては当該機密情報が法律上保護されなくなったり特許出願ができなくなったりしてしまうリスクがありますので，入力しないでください。

（7）差別用語や倫理に反する表現が含まれていないか確認する

対象生成AI等からの応答内容には，差別につながったり，倫理に反する内容が含まれている場合があります。
そのため，生成AI から出力された情報を利用したり，外部に発信する際は，複数の職員で，その内容の一部が切り取られても問題がないかどうかを含め，厳重にチェックすることが重要です。

【解説】

このようなチェック，判断は，法令の規定はもとより社会通念等も踏まえて，様々な角度から行うことが重要であると考えられます。

対象生成AI等の生成物については，地方自治体が取り扱う情報としてふさわしいものであるか，グループ内や所属内，さらには関係機関を含めて，十分に議論を尽くすようにしてください。

6 生成物を利用するに際して注意すべき事項

（1）生成物の内容に虚偽が含まれている可能性がある

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す。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。

生成AIのこのような限界を知り，その生成物の内容を盲信せず，必ず根拠や裏付けを自ら確認するなどして正確性を保ってください。また，回答の正確性や信頼性については自己責任で判断する必要があることを念頭においてください。

（2）生成物を利用する行為が誰かの既存の権利を侵害する可能性がある

① 著作権侵害

対象生成AI等からの生成物が，既存の著作物と同一・類似している場合は，当該生成物を利用（複製や配信等）する行為が著作権侵害に該当する可能性があります。

そのため，以下の留意事項を遵守してください。

・特定の作者や作家の作品のみを学習させた特化型AIは利用しないでください。

・プロンプトに既存著作物，作家名，作品の名称を入力しないようにしてください。

・特に生成物を「利用」（配信・公開等）する場合には，生成物が既存著作物に類似しないかの調査を行うようにしてください。

② 商標権・意匠権侵害

画像生成AIを利用して生成した画像や，文章生成AIを利用して生成したキャッチコピーなどを商品ロゴや広告宣伝などに使う行為は，他者が権利を持っている登録商標権や登録意匠権を侵害する可能性がありますので，生成物が既存著作物に類似しないかの調査に加えて，登録商標・登録意匠の調査を行うようにしてください。

③ 虚偽の個人情報・名誉毀損等

ChatGPTなどは，個人に関する虚偽の情報を生成する可能性があることが知られています。虚偽の個人情報を生成して利用・提供する行為は，個人情報保護法違反（法19 条，20 条違反）や，名誉毀損・信用毀損に該当する可能性がありますので，そのような行為は行わないでください。

【解説】

対象生成AI等からの生成物が既存の著作物と同一・類似している場合は，当該生成物を利用（複製や配信等）する行為が著作権侵害に該当する可能性があります。

もっとも，どのような場合に著作権侵害に該当するかは明確な基準が存在しない状況です。

そこで，本ガイドラインでは保守的に考え，著作権侵害に繋がる可能性のある行

為（「特定の作者や作家の作品のみを学習させた特化型AIを利用する行為」「プロンプトに既存著作物，作家名，作品の名称を入力する行為」）を禁止し，生成物を配信・公開等する場合には，生成物が既存著作物に類似しないかの調査を行うよう義務づけています。

（3）生成物について著作権が発生しない可能性がある

仮に生成物に著作権が発生していないとすると，当該生成物は基本的に第三者に模倣され放題ということになりますので，自らの創作物として権利の保護を必要とする個人や組織にとっては大きな問題となります。

この論点については，対象生成AI等を利用しての創作活動に人間の「創作的寄与」があるか否かによって結論が分かれますので，生成物をそのまま利用することは極力避け，できるだけ加筆・修正するようにしてください。

【解説】

① 画像生成AIの場合

画像生成AIの場合であれば，自分の意図通りに高画質の画像を生成するために，①詳細かつ長いプロンプトを入力して画像を生成した場合，②プロンプト自体の長さや構成要素を複数回試行錯誤する場合，③同じプロンプトを何度も入力して複数の画像を生成し，その中から好みの画像をピックアップする場合，④自動生成された画像に人間がさらに加筆・修正をした場合などは「創作的寄与」があるとして，それらの行為を行った人間を著作者として著作権が発生することになるでしょう。

② 文章生成AIの場合

対象生成ＡＩ等のような文章生成AIには様々な用途がありますが，文章生成AIのユーザーが何らかの指示をして，何らかのリサーチ結果，アイデアや回答を得た場合，出力テキストにはユーザーの創作意図と創作的寄与は通常はありませんので，文章生成AIによる出力テキストには著作権は発生しないということになるでしょう。

文章生成AIから，よりよい出力を引き出すために，質問（入力）の仕方のヒントやプロンプト文例がたくさん公開されていますが，ユーザーが質問をするにあたってそれらの文例を駆使したとしても，出力テキストに対するユーザーの創作意図と創作的寄与が認められることはないように思います。

したがって，ユーザーが文章生成AIに指示をして，何らかのリサーチ結果，アイデアや回答を得た場合，それらの出力には著作権が発生しない，ということになりそうです。

（4） 生成物を商用利用できない可能性がある

対象生成AI等により生成した生成物をビジネスで利用する場合，当該生成物を商用利用できるかが問題となります。

この論点は，利用する生成AIの利用規約により結論が左右されますが，ChatGPTの場合，生成物の利用に制限がないことが利用規約に明記されているので，この点は問題になりません。

【解説】

本ガイドラインではChatGPTを主たる例に挙げて言及していますが，たとえば，画像生成AIであるMidjourneyの場合，無料会員が生成した画像の著作権はいったん無料会員にAI生成物の著作権が帰属した後，Midjourneyに当該著作権が移転し，その上で，Midjourneyは，当該AI生成物を創作した無料会員に対して，CC4.0NCの下，ライセンスをすることになっています。

つまり，無料会員は当該AI生成物を商用利用することはできません。

（5）対象生成AI等のポリシー上の制限に注意する

対象生成AI等においては，これまで説明してきたリスク（主として法令上の制限）以外にも，サービスのポリシー上独自の制限を設けていることがありますので注意してください。

【解説】

① ChatGPTを利用する場合，以下の点に注意してください。

Usage Policies（https://openAI.com/policies/usage-policies）で，「Adult content, adultindustries, and dating apps（アダルトコンテンツ，アダルト産業，出会い系アプリ）」「Engaging in the unauthorized practice of law, or offering tailored legal advice without a qualified person reviewing the information（許可なく法律実務を行うこと，または資格のある人が情報をレビューしないままに特定の法的助言を提供すること）」などの具体的禁止項目が定められています。

また，医療，金融，法律業界，ニュース生成，ニュース要約など，消費者向けにコンテンツを作成して提供する場合には，AIが使用されていることとその潜在的な限界を知らせる免責事項をユーザーに提供する必要があることも同ポリシーには明記されています。

さらに，関連ポリシー上は，ChatGPTなどOpenAI社のサービスを利用して生成されたコンテンツを公開する際には，AIを利用した生成物であることを明示することなどが定められています。

② マサルくんの利用上の注意（※令和5年10月現在のサイト掲載情報を転載）

・行政DXをリードしている１９１自治体、８６社で構成する「一般社団法人デジタル田園都市国家構想応援団」の会員で利用しているもので、API費用は当応援団が各自の会費から支払っていますが、非会員の方も無料で利用可能です。

・現時点では、バージョンアップを繰り返している開発テストの状態です。

ChatGPTの回答等に責任は持ちませんので、自己責任でテスト利用してください。

サーバーが込み入ってエラーが出た時は、後ほど、再度、ご利用ください。

・機密事項や個人情報は入れないようにして、利用してください。
・自治体のAI活用が注目される中で、ChatGPTリリース後の自治体初のAI導入の公募は東京都でした。東京都技術審査委員会が、日本全国のAI企業、IT企業の中から技術審査で選んだのは、東武トップツアーズ株式会社です。この行政DX「マサルくん」も東武トップツアーズのITエンジニアチームが作っているため、試行錯誤の成果を東京都や他自治体のAI技術の革新に役立てる事をご理解ください。また、デジ田応援団の各自治体・各社との行政AIの利活用の研究会にも使います。

（6）チャットの内容を記録・保管する

生成AI を利用したチャットの内容は，将来，何らかの証拠等として必要になることも想定されることから，回答結果の原文や画像，イラスト等を業務で利用する場合はその根拠として，出力された内容を必ず記録・保管しましょう。また，文書や資料の作成，データの収集・分析に利用した場合には，生成AI を利用した旨を記録しておくことも重要です。

【解説】
生成AI は，公開されてから日の浅いサービス（技術）であり，今後，様々な議論を経て開発や利用のルールが確立されていくものと考えられます。将来，どのような問題が起こるか，現時点では予想できないことから，生成された文章等を業務で利用する場合は，その履歴を記録・保管してください。
同様の理由から，職員がAI の生成物を利用する場合には，コピーライトのように文書や資料の枠外に「【生成AI 名】により生成」と明示するようにしましょう。

（参考）
機密性の高い情報とは、一律に定義できるものではなく、状況に応じて個別具体に区分するケースもあるものと考えられます。以下に代表的なものを例示します。

（機密性の高い情報の例） ○ 個人情報（特定の個人を識別できる情報（※），住民の税情報，職員個人に関する情報など） ○ 企業・団体・他自治体等から入手した未（非）公開の情報（企業等の経営や雇用，事業計画，財務・税務に関する情報，企業等の知的財産や商品・サービスに関する情報，企画競争入札に係るプレゼンテーション資料，その他公にすることにより企業等の利益を害するおそれがある情報，担当者の氏名・メールアドレスなど） ○ 公にすることにより意思決定に影響を及ぼすおそれや，市民に混乱を生じさせるおそれ，特定の者に利益又は不利益を及ぼすおそれ，その他事務事業の適正な遂行に支障を来すおそれがある情報（確定前・公表前の予算案・人事案・計画

案・条例案，外部に発出する文書の素案，議会答弁案，入札公告前の調達情報など）

※ 個人情報に該当する情報

・ 個人情報保護法において「個人情報」とは，生存する個人に関する情報で，氏名，生年月日，住所，顔写真などにより特定の個人を識別できる情報をいいます。これには，他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものも含まれます。例えば，生年月日や電話番号などは，それ単体では特定の個人を識別できないような情報ですが，氏名などと組み合わせることで特定の個人を識別できるため，個人情報に該当する場合があります。

また，メールアドレスについてもユーザー名やドメイン名から特定の個人を識別することができる場合は，それ自体が単体で，個人情報に該当します。

・ このほか，番号，記号，符号などで，その情報単体から特定の個人を識別できる情報で，政令・規則で定められたものを「個人識別符号」といい，個人識別符号が含まれる情報は個人情報となります。例えば，次のようなものです。

（1）身体の一部の特徴を電子処理のために変換した符号で，顔認証データ，指紋認証データ，虹彩，声紋，歩行の態様，手指の静脈，掌紋などのデータがあります。

（2）サービス利用や書類において利用者ごとに割り振られる符号で，パスポート番号，基礎年金番号，運転免許証番号，住民票コード，マイナンバー，保険者番号などがあります。

（出典：政府広報オンライン）

策定　令和５年１２月１４日
DX・行革推進室／ChatGPT 利活用検証ワーキングチーム