

# 松戸市職員生成 AI 利活用ルール

第三版 令和8年6月12日 策定

松戸市総務部 DX 推進課

## 第1章 はじめに

### 1 前提

1 - 1 本ガイドラインは、「ChatGPT 等の生成 AI の業務利用について」（令和5年5月8日付け事務連絡、総務省自治行政局デジタル基盤推進室通知）及び「生成 AI の利用ガイドライン」（令和5年5月1日、一般社団法人日本ディープラーニング協会（※1）公開）及び、「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」（令和7年5月27日、デジタル社会推進会議幹事会（※2）決定）を参考に作成をしたものである。

1 - 2 松戸市が用いる生成 AI は、「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和8年3月版）」（※3）における外部サービスに該当し、松戸市情報セキュリティポリシー（平成19年11月26日施行）におけるマイナンバー利用事務系、LGWAN 接続系及びインターネット接続系によるシステムやサービスとは異なる。

### 2 社会の動向

近年、ChatGPT などの生成 AI（※4）が急速に普及し、日常生活において、多くの人々が活用を始めている。それと同時に、多くの企業では、業務の効率化や生産性の向上に向けた活用の他、顧客対応の自動化が進められている。こうした新しい技術を積極的に利用していくことは、効率的に業務を遂行し、人的資産を軽減する上でも、大変重要なものであり、今後、多くの地方自治体で市民サービスの向上や業務の効率化を強力に推進するための活用が進んでいくものと考えられる。

### 3 目的

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、第三者の権利を侵害したりする可能性がある。本ガイドラインは、職員が各業務において生成 AI を利用及び提供する際に注意すべき事項を示し、適切な制限により、活用を可能とするものである。

## 第2章 松戸市職員生成 AI の利用について

### 1 本ガイドラインの対象範囲

#### 1-1 サービスの対象

(1) 本ガイドラインの対象とする生成 AI は、以下のとおり。

- ①OpenAI 社が提供する「ChatGPT」(※5)
- ②㈱アイネスが提供する「生成 AI 総合案内チャットボット」(※6)

#### 【解説】1 本ガイドラインの対象範囲 1-1 (1)

今後、他社等から提供される生成 AI の普及がさらに進むようでしたら、対象範囲の拡大も検討していきます。

(2) 現時点において、ChatGPT のバージョンは、無償版と有償版がリリースされており、バージョンにより利用可能な機能や費用が異なる。本ガイドラインにおいては、無償版を対象とする。

#### 【解説】1 本ガイドラインの対象範囲 1-1 (2)

無償版と有償版の主な相違点

項目	機能	処理性能	利用上限	サポート
無償版	標準	標準	制限あり	なし
有償版	高性能	高速	制限緩和	あり

(3) 現時点において、生成 AI 総合案内チャットボットに用いられている生成 AI モデルは、Anthropic 社(※7) が提供する Claude Haiku (※8) であり、バージョンは2025年10月に発表された Claude Haiku 4.5 を対象とする。(現時点では、Claude はその他4つのモデルがリリースされているが、当生成 AI チャットボットでは、Claude Haiku を利用している。)

#### 【解説】1 本ガイドラインの対象範囲 1-1 (3)

Claude のモデル比較

モデル	特徴	主な用途	適したユーザ
Fable	最高性能・複雑タスク	長期エージェント・戦略立案	研究開発者・エンジニア
Mythos	創作特化・物語生成	文体模倣、小説、脚本	クリエイター、作家
Opus	高度な推論力	研究、複雑な分析	プログラマー・研究者
Sonnet	バランス重視	日常業務、コーディング	ビジネスユーザ、学習者
Haiku	速度重視・低価格	チャット、リアルタイム 応答、低コスト運用	一般ユーザ

## 1 - 2 対象者と対象端末

本ガイドラインの対象者は、市長部局をはじめとし、全職員とする。

また、対象端末については、原則として次世代型職員用パソコン及び情報系の公用パソコンとする。

<参考> 正規職員数：約4,000名（令和8年4月1日現在）

会計年度職員数：約2,400名（令和8年4月1日現在）

情報系端末台数：約990台（令和7年度情報機器等の使用状況に関する調査より）

次世代型職員用パソコン台数：約2,500台

## 2 生成AIの機能

### 2 - 1 ChatGPTの機能

#### (1) 基本情報

OpenAI 社が開発した会話型 AI（※9）サービスであり、大規模言語モデルがベースとなっている。人間と同様に自然な会話を生成・理解し、精度が高く、2023年現在で、質問対応、対話生成、アイデアのブレインストーミング（※10）、プログラミングコードの生成、オリジナルストーリー作成など、様々なタスクに対応していることから、急速に社会全体で利用が広がっている。

#### (2) 活用方法

本市職員は以下に掲げる業務において活用できるものとする。

- ① 内部事務及び事務事業の企画立案等の工程における情報収集等
- ② 行政サービスの案内等をする際の補助的手段
- ③ 住民等にわかりやすい文章作成の補助的手段
- ④ 文章の校正や、表を作成する際の補助的手段
- ⑤ 業務の進め方の助言としての活用
- ⑥ Excel 関数等を作成する際の補助的手段
- ⑦ その他、事務的作業の確認、助言、補助等

なお、生成物に疑義が発生した場合には、詳細な前提条件や例示を加えるほか、同じ質問を繰り返し行うなど質問を工夫し、より効果的に活用をすること。

#### 【解説】2 - 1 (2) 活用方法

ChatGPT は業務中の下記において、地方自治体でも効果的に活用できると考えています。

- ①内部事務及び事務事業の企画立案等の工程における情報収集等

例)・新規事業における他市・企業などの事例や実績の調査

・ 予算要求時の資料作成、新規事業企画書の作成に伴う情報収集

- ・対象となる事業を請け負う、又は、使用できる物件を持つ事業者の調査（対象業務、実績等）

#### ②行政サービスの案内等をする際の補助的手段

- 例) ・行政サービス利用時に必要な書類や申請条件等の参考リスト作成や説明のための参考情報として利用
- ・市民からの電話や来庁の問い合わせ時に、参考情報としてグーグル等インターネット検索をする代替として利用

#### ③住民等に分かりやすい文章作成の補助的手段

- 例) ・問い合わせメールや投書などの返答の下書き
- ・事業者とのメールやり取りなどの下書き
- ・事業者や市民へのお知らせ、アンケートを行う際等の下書き
- ・ホームページ作成の下書き
- ・課内等の説明文書の下書き

#### ④文章の校正や、表を作成する際の補助的手段

- 例) ・③で作成した文書の漢字や誤字・脱字の確認
- ・庁内外に掲示する文書の校正や、複数の事案をより分かりやすい表で示したい時など
- ・調べたいこと案件（例：専門用語）等の解説

#### ⑤業務の進め方の助言としての活用

- 例) ・課題の解決方法の提供や、成果や達成度の指標例の提示など
- ・業務の実施手段や作業項目出しの参考
- ・業務を行っている中での疑問などの深堀
- ・業務におけるアイデア出し

#### ⑥Excel 関数等を作成する際の補助的手段

- 例) ・Excel 関数利用時に、最適な計算式の提供など
- ・予算、決算等の財務情報資料作成
- ・執行額の集計
- ・アンケートの集計や分析

詳細な前提条件や例示を加えたり、同じ質問を繰り返し行うことで、生成物の精度を高めたり、なぜそのような回答をしたのかの説明をさせることで、生成物の根拠を明確にするなど、より効果的な活用が見込めます。

## 2 - 2 生成 AI 総合案内チャットボットの機能

### (1) 基本情報

利用者からの様々な質問に対し、生成 AI が自ら考え、的確な回答を行う。  
インターネット上に公開されている松戸市公式ホームページの情報を生成 AI が学習し、幅広く、正確に、意図を汲んだ創造性のある回答が可能。  
活用している生成 AI モデルは Anthropic 社が開発した Claude Haiku である。  
会話型 AI サービスであり、大規模言語モデル(LLM)がベースとなっている。長文理解・要約・ビジネス文書作成に高い精度を発揮することが特徴。多言語能力にも優れ、自然な会話での応答が可能であることから、世界中で爆発的に普及している。

### (2) 活用方法

生成 AI 総合案内チャットボットは、以下に掲げる業務において活用できるものとする。

なお、市民への提供という観点については、第3章にて後述する。

- ① 内部事務及び事務事業の企画立案等の工程における情報収集等
- ② 行政サービスの案内等をする際の補助的手段
- ③ 住民等にわかりやすい文章作成の補助的手段
- ④ 文章の校正や、表を作成する際の補助的手段
- ⑤ その他、事務的作業の確認、助言、補助等

#### 【解説】 2 - 2 (2) 活用方法

生成 AI 総合案内チャットボットは業務中の下記において、地方自治体でも効果的に活用できると考えています。

##### (1) 内部事務及び事務事業の企画立案等の工程における情報収集等

- 例)・新規事業における他市・企業などの事例や実績の調査  
・予算要求時の資料作成、新規事業企画書の作成に伴う情報収集

##### (2) 行政サービスの案内等をする際の補助的手段

- 例)・行政サービス利用時に必要な書類や申請条件等の参考リスト作成や説明のための参考情報として利用  
・市民からの電話や来庁の問い合わせ時に、参考情報としてグーグル等インターネット検索をする代替として利用

##### (3) 住民等に分かりやすい文章作成の補助的手段

例)・問い合わせメールや投書などの返答の参考情報

- ・事業者とのメールやり取りなどの参考情報
- ・事業者や市民へのお知らせ、アンケートを行う際等の参考情報
- ・ホームページ作成の参考情報
- ・課内等の説明文書の参考情報

(4) 文章の校正や、表を作成する際の補助的手段

例)・庁内外に掲示する文書や、複数の事案をより分かりやすく整理して示したい時など

### 3 現状の問題・課題

#### 3 - 1 ChatGPT の活用における課題

- (1) インターネット上の情報を集めての回答となり、誤った内容でも自然な文章で作成されるため間違いに気付きにくく、偽情報が拡散する恐れがある。(正確性は人の目による判断が必要となる。)
- (2) 利用者の宗教や思想等に左右される回答が含まれており、かつ、人間による倫理的観点でのチェックが漏れた場合、その文章を業務利用すると、市民からの信用を失う恐れがある。
- (3) 職員が入力した情報が利用され、個人情報・機密情報を拡散される恐れがある。
- (4) OpenAI 社の利用規約に、サービス向上(サービスの開発及び改善)のため、コンテンツに利用する旨の記載があり、職員が入力した情報が今後の学習等に利用される恐れがある。

#### 【解説】3 現状の問題・課題 (4)

OpenAI 社の利用規約に、サービス向上の為のコンテンツ利用の記述があります。

規約の主な内容としては、ユーザ ID 及びパスワードの管理、利用料金及び支払方法、ユーザに対する禁止事項や、利用制限及び登録抹消となっています。

- (5) インターネット上の情報を集めての回答となるため、生成物を利用した職員が意図せず権利侵害(著作権等)を犯している恐れがある。
- (6) 自動応答のためのツールであり、人間と同様の思考力や判断力は備わっていないため、不適切な発言や犯罪等に利用される恐れがある。

(7) 職員が ChatGPT を利用することで、業務上の資料等を AI に作成させることが可能となり、作業を全面的に代替させる恐れがある。

(8) ChatGPT を利用する所属と利用しない所属によって、業務の方法や業務にかかる時間に大きな差が生まれる恐れがある。

### 3 - 2 生成 AI 総合案内チャットボットの活用における課題

(1) 生成 AI の性質上、一定のランダム性が含まれるため、質問方法や状況、条件により、必ずしも正しくない回答や最新でない回答となる場合がある。

(2) 利用するネットワーク環境の状況によっては質問を送信後、回答まで15秒前後要する。回答速度の向上が求められる。

## 4 利用方法及び制限

生成 AI は、いずれのサービスも基本的に「ユーザが何らかのデータを入力して、何らかの処理（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」という構造となっている。そのため、「3 現状の問題・課題」の対策を含め、適切に利用するため、職員が生成 AI に入力する情報に応じて、本ガイドラインにより利用の可否を定める。

なお、職員が生成 AI を業務で利用する場合は、原則として所属長の許可を得た上で、業務を遂行するための補助的ツールとして利用すること。

また、「5 職員がデータを入力する際の注意事項」に抵触する可能性がある場合には、必ず入力する内容を所属長に確認の上、利用すること。

### 【解説】4 利用方法及び制限

生成 AI のサービス形態は、政府統一基準における「不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービス」に該当します。組織の承認を得ずに職員が外部サービスを利用することは、規程に反していることに加え、誰がどのように使用しているかなどの管理が出来ず、情報漏えい等のリスクを高める可能性があります。

## 5 職員がデータを入力する際の注意事項

5 - 1 職員が入力する情報は、生成 AI 内にデータが保存され、又は一般に公開されても問題がないと判断したものだけに留めること。

また、知的財産権の必要性や法規制の順守という観点から、下記データの入力を

禁止する。

- (1) 松戸市情報セキュリティポリシーに定める機密性3及び機密性2(※11)の情報の入力

**【解説】5 職員がデータを入力する際の注意事項 5-1(1)**

民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、セキュリティ対策やデータの取扱いなどについて機関等への特別な扱いを求めることができない場合が多いため、機密性2及び機密性3以上の情報の入力を禁止します。

機密性2情報とは、行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏洩により、国民の権利が侵害され又は行政事務の遂行に支障を及ぼす恐れがある情報となります。

例) 職員情報や事業者名を含む執行情報、及び契約情報等、職員だけが知り得る状態を確保する情報等。

(職員のうち特定の職員だけが知り得る状態を確保する必要がある情報を含む。)

機密性3情報とは、行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報となります。

例) 住基情報や税情報などの特定個人情報(マイナンバーと紐付けられる情報)や個人に関する情報(特定の個人を識別することが出来る情報や、公にすることにより、個人の権利利益を害するおそれがある情報)等。

- (2) 事業者等から秘密保持義務を課されて開示された秘密情報の入力

**【解説】5 職員がデータを入力するに際の注意事項 5-1(2)**

事業者との間で秘密保持契約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という「第三者」に秘密情報を「開示」することとなり、秘密保持契約に反するため、禁止します。

例) 企業内の体制や個人の連絡先、秘密としている実績等

契約相手方の業務上の秘密情報や特許、営業戦略、製品情報、技術情報、顧客リスト等、特定の企業や個人にとって秘密にしておく必要がある情報等。

- (3) 非公開情報や公開前情報の入力

**【解説】5 職員がデータを入力する際の注意事項 5-1(3)**

「3 現状の問題・課題」に記載のとおり、職員が入力した情報が拡散される恐れがある

ため、業務等に関する情報で非公開や公開前の情報の入力には禁止します。

例) 非公開情報とは、マニュアル・手順書・業務プロセス等、第三者によって不正に利用される可能性のある情報等。

5 - 2 既存の著作物に類似した生成物が提供される可能性があり、意図しない「ライセンス違反 (※12)」や「権利侵害 (※13)」があることを認識して利用すること。また、以下の著作物・登録商標など第三者が権利を保有しているデータを入力する場合は、特に注意すること。

**【解説】5 職員がデータを入力する際の注意事項 5 - 2**

データを入力することで、著作物・登録商標など、第三者の権利を侵害することはありませんが、以下(1)～(3)に記載のリスクを理解して、十分に注意して利用する必要があります。

(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)

生成 AI 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ない。

ただし、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があるため、注意すること。具体的には後述の「6-2 職員が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」を参照すること。

(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・デザイン等を生成 AI に入力することは、商標権侵害や意匠権侵害には該当しない。

ただし、「(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)」と同様、「入力行為」に関するものであるため、「故意に、あるいは偶然生成された、他社登録商標と同一・類似の商標を『使用』する行為」については、商標権侵害となる。

そのため、職員が生成 AI の生成物を業務に利用する場合には商標登録・意匠の確認を行うこと。

(3) 著名人の氏名

著名人の氏名等を生成 AI に入力する行為は、パブリシティ権侵害 (※14) には該当しない。

ただし、生成 AI を利用して生成された著名人の氏名等については、それらの氏名等を商標利用する行為はパブリシティ権侵害に該当するため、注意をする

こと。

## 6 職員が生成物を利用する際の注意事項

### 6 - 1 生成物の内容に虚偽が含まれている可能性がある

本市が利用する生成 AI は大規模言語モデルのため、「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、自然な文章を作成している。

そのため、生成された内容には虚偽が含まれている可能性がある。

生成物の内容は、正確で信頼できる情報源と照合し、必ず根拠や裏付けを確認すること。また、生成物が事実と異なる場合は修正の上、所属長の責任で利用すること。

#### 【解説】6 職員が生成物を利用する際の注意事項 6 - 1

「3 現状の問題・課題」3-1に記載のとおり、正確性は人の目による判断が必要になります。

### 6 - 2 職員が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

#### 【解説】6 職員が生成物を利用する際の注意事項 6 - 2

データ入力とは異なり、入力して得た結果の生成物の利用等においては、著作物・登録商標など第三者の権利を侵害となる恐れがあるため、以下(1)～(3)について必ず確認を行う必要があります。

#### (1) 著作権侵害

生成 AI 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当たる可能性がある。そのため、職員が生成物を利用する際は、生成物が既存著作物に類似しないかの確認を行うこと。

#### (2) 商標権・意匠権侵害

ChatGPT の生成物をキャッチコピーやロゴ、広告宣伝などに使う行為は、第三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るため、職員が生成物を利用する際は、既存著作物に類似しないかの調査に加えて、登録商標・登録意匠の確認を行うこと。また、データ出典元に十分に確認を行うこと。

#### (3) 虚偽の個人情報・名誉毀損等

生成 AI は、個人に関する虚偽の情報を生成する可能性がある。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や名誉毀損・信用毀損に

該当する可能性があるため、そのような行為は行わないこと。

### 6 - 3 生成物について著作権が発生しない可能性がある場合

仮に生成物に著作権が発生していない場合、当該生成物は基本的に不特定多数の第三者に模倣されている状況となり、自らの創造物として権利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る。そのため、生成物をそのまま利用することは極力避け、出来る限り、加筆・修正すること。

### 6 - 4 サービスのポリシー上の制限に注意する

生成 AI 利用する場合は、独自に策定された制限やポリシー、利用規約を必ず確認の上、その内容を遵守し、リスクを十分に把握したうえで利用すること。

#### 【解説】 6 職員が生成物を利用する際の注意事項 6 - 4

治療・処置の方法といった医療情報で、特に命に関わる問題やトリアージなどの制限・禁止事項や、個人情報の入力や、緊急時の使用、回答の利用等に関する制限・禁止事項が設けられております。

### 6 - 5 生成物利用の責任所在を明確にする

生成されたコンテンツをそのまま提供する場合には、必要に応じて下記例を参考の上、データの出典元や、生成 AI が作成したものであることを明記し、内容については参考程度にする断りを、適宜記載すること。

【例】「本コンテンツは ChatGPT によって生成されております。本コンテンツの情報を利用の際は、必ず利用者様ご自身で、内容をご確認ください。」など

### 6 - 6 リスクケース検知時の報告

生成 AI が事実と異なる情報を出力し（ハルシネーション）、利用者がその情報を利用したことによって、市民等の第三者に不利益を与えた、などの生成 AI システム特有の重大なリスクケースを検知した場合、迅速に最高情報セキュリティ責任者（副市長）、情報セキュリティ統括管理者（総務部長）及び情報セキュリティ管理者（各部長）に報告をすること。

## 7 利用手順

### 7 - 1 ChatGPT の利用手順

#### (1) 説明会の参加

ChatGPT の利用を希望する所属は、定期的に行われる説明会に参加すること。

## (2) アカウント及び利用者の申請

ChatGPT のアカウント及び利用者を適正に管理するため、利用を希望する所属は、【様式1】 ChatGPT アカウント及び利用申請書に記入の上、申請を行うこと。  
また、人事異動等により利用者に変更が生じた場合も、同様に申請を行うこと。  
なお、申請内容に応じ、情報系ネットワーク及び情報系端末を管理する DX 推進課 DX 推進課（以下、DX 推進課 DX 推進課という。）が利用可否の連絡を行うものとする。

## (3) 申請の承認及び研修の受講

DX 推進課の承認後、利用申請者は別途開催する関連事業者による研修を受講すること。

## (4) アカウントの作成

ChatGPT のアカウントは、各所属のメールアドレスを使用して作成すること。  
また、アカウント作成時には登録したメールアドレス宛に認証コードが送付されるため、メールを受信できる環境で作業を行うこと。

## (5) 活用方法の管理と周知

効果的な活用方法を共有し、管理するため、【様式2】 ChatGPT 活用方法報告書を提出すること。  
提供された情報については庁内へ、DX 推進課より適宜周知を行う。

## (6) 利用における責任の所在及び問題発生時の対応

ChatGPT は、本ガイドラインに基づき所属長の責任において利用すること。  
また、所属長は、その所掌する所属において、ChatGPT の利用に起因とする問題が発生した場合、又は、問題発生のおそれがある場合には、【様式3 ChatGPT 障害発生報告書に 記入の上、松戸市情報セキュリティポリシーに定めるところの最高情報セキュリティ責任者（副市長）、情報セキュリティ統括管理者（総務部長）及び情報セキュリティ管理者（各部長）へ速やかに報告を行い、指示を仰がなければならない。

## 7 - 2 生成 AI 総合案内チャットボットの利用手順

### (1) アクセス方法

アカウント作成や利用申請等は不要。松戸市公式ホームページのトップ画面左下に常時表示されるアイコンや、SKYDIV Desktop Client ランチャー内のメニュー、あるいはホームページ内のリンクからアクセスすること。

## (2) 活用方法の管理と周知

利用にあたり、効果的な活用方法が確認できた場合は、庁内にて共有し、管理するため、【様式4】生成 AI 総合案内チャットボット活用事例報告書を提出すること。提供された情報については庁内へ、DX 推進課より適宜周知を行う。

## (3) 利用における責任の所在及び問題発生時の対応

生成 AI 総合案内チャットボットは、本ガイドラインに基づき所属長の責任において利用すること。

また、所属長は、その所掌する所属において、生成 AI 総合案内チャットボットの利用に起因とする問題が発生した場合、又は、問題発生のおそれがある場合には、松戸市情報セキュリティポリシーに定めるところの最高情報セキュリティ責任者（副市長）、情報セキュリティ統括管理者（総務部長）及び情報セキュリティ管理者（各部長）へ速やかに報告を行い、指示を仰がなければならない。

【解説】 7 利用手順 7-1 (6)、7-2 (3)

松戸市情報セキュリティポリシーP11

情報セキュリティ実施責任者の役割・権限 4 を参照しています。

### 第3章 松戸市職員の生成 AI 提供について

#### 1 生成 AI 提供者としての対応事項

本市は、生成 AI 総合案内チャットボット等の生成 AI システムを住民等へ適正な提供を行うにあたり、「行政の進化と革新のための生成 AI 調達・利活用に係るガイドライン」等を踏まえ、以下 1 - 1 ~ 1 - 3 を遵守・留意しなければならない。

##### 1 - 1 システムの運用

###### (1) 品質

出力結果が期待品質を満たしていること、および不適切な生成やバイアスが発生していないことを監視するため、利用ログからサンプルチェックし、生成 AI システムへの入出力及び判断根拠等を定期的にモニタリングし、判断根拠が偏っていないか、特定の文化背景を基にした出力となっていないか等を確認すること。

###### (2) 目的外利用の検証

適切な目的で生成 AI システムが利用されていること、および目的外利用がされていないことを定期的に検証するため、利用ログからサンプルチェックし、業務と関係のない何らかの出力を期待していると思われる入力をしていないこと等を確認すること。

###### (3) 個人情報の入力

個人情報の不適切な取扱いや個人情報・要機密情報の流出、プライバシー侵害がないか確認するため、利用ログからサンプルチェックを行い、個人情報の目的外利用が疑われるケースが発生していないか、当生成 AI システムで要機密情報が入力されていないか、プライバシー侵害が発生していないかを確認すること。

###### (4) 最新動向の確認

Claude Haiku に対する最新のリスク（攻撃手法の多様化など）及びその対応策の動向や、情報セキュリティインシデント（JIS Q 27000:2019 における情報セキュリティインシデントをいう。）、リスクケース事例、開発者のモデルの脆弱性に関するレポート等確認し、必要に応じ適切な対応を行うこと。

###### (5) 有用性・問題点の周知

生成 AI システムの入出力に関して有用性や問題点などのレビューを行い、必要に応じて、利用者への周知をすること。

出力及び判断根拠等を確認し、有用性に関する効果的な利用方法、問題点に関する注意喚起等を実施する。

## 1 - 2 システムの保守

### (1) 改善対応

必要に応じて、生成 AI モデル改善の判断を事業者に促し、生成 AI モデルを構成する各技術要素のバイアスの再評価、評価結果に基づき変化点があった場合等に生成 AI モデルの改善を提案すること。

### (2) 脆弱性対応

「政府機関等のサイバーセキュリティ対策のための統一基準群」の遵守を前提とし、脆弱性の対応を検討、必要に応じて実施し、生成 AI システムのプログラムに内在する脆弱性を検知した場合、パッチ対応・モデル更新等を検討すること。

## 1 - 3 入力された情報の取扱い

(1) 利用者により、本生成 AI に入力された内容及び利用状況は、回答の生成、サービスの品質向上、不具合対応、不正利用防止、利用状況の分析のため以外に利用しないこと。

(2) 本生成 AI の導入委託事業者との間では、入力内容を本生成 AI の提供目的以外に利用しないこと、適切な安全管理措置を講じること等を契約又はサービス仕様により確認すること。

(3) 入力内容及びログは、松戸市が定める期間保存し、保存期間経過後、適切な方法により削除すること。

## 第4章 問い合わせ

本ルールに関する問い合わせ先は、松戸市総務部 DX 推進課 (047-366-7399) とする。

## 第5章 附則

本ガイドラインは、ChatGPT および生成 AI 総合案内チャットボットの機能、環境、活用等の状況や変化に合わせ、適宜見直しを行うこととする。

## ■用語解説

### (※1) 一般社団法人日本ディープラーニング協会

ディープラーニングを中心とする技術による日本の産業競争力の向上を目指し、ディープラーニングを事業の核とする企業及び有識者が中心となって、産業活用促進、人材育成、公的機関や産業への提言、国際連携、社会との対話など、産業の健全な発展のために必要な活動を行っている。

(ディープラーニングとは、人工知能技術の中の機械学習技術の一つ。人間の手を使わず、コンピュータが自動的に大量のデータの中から希望する特徴を発見する技術を指す。)

### (※2) デジタル社会推進会議幹事会

デジタル社会推進会議は、デジタル庁設置法第14条に基づき設置された、政府のデジタル政策を統括する最高レベルの会議体。議長は内閣総理大臣で、行政のデジタル化やデータ利活用など国家的課題を省庁横断で推進している。実務的な検討や省庁間調整は下部組織である幹事会(議長:デジタル監)が担い、重点計画の策定や施策の具体化を行っている。

### (※3) 「地方公共団体における情報セキュリティポリシーに関するガイドライン(令和8年3月版)」

総務省が各地方公共団体向けに情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したガイドライン。

### (※4) 生成 AI

あらかじめ学習したデータをもとに、画像・文章・音楽・デザインなどを新たに作成する人工知能(AI)の総称。

### (※5) OpenAI 社が提供する「ChatGPT」

OpenAI 社は、営利法人 OpenAI LP とその親会社である非営利法人 OpenAI Inc. からなるアメリカの人工知能(AI)の開発を行っている企業。

ChatGPT の正式名称は Chat Generative Pre-trained Transformer という。

### (※6) (株)アイネスが提供する「生成 AI 総合案内チャットボット」

株式会社アイネスは、東京都中央区に本社を置く独立系システムインテグレーター。本市では、平成19年度からオープンシステムとして、税・国保・福祉関連システムを同社にて導入、保守、運用を行っている。同社が提供する「生成 AI 総合案内チャットボット」は、市民の生活に役立つ情報を提供し、行政サービスの効率化を図ることを目的として開発された。

案内チャットボット」は、市民からの様々な質問に、的確な回答を行うことができるチャットボットシステム。インターネット上に公開されている松戸市公式ホームページの情報を生成 AI が学習することにより、幅広く、正確に、意図を汲んだ創造性のある回答が可能。令和8年6月12日より稼働。

(※7) Anthropic 社

AI の安全性を最優先にすることを理念に掲げて設立された、アメリカの先進的 AI 研究・開発企業。

(※8) Claude Haiku

Claude は、AI 特有の不自然な会話表現が少なく、文脈理解と要約・分類に適した生成 AI モデル。その中でも Claude Haiku-4.5 は最も低コストかつ応答速度が早く、リアルタイムでの応答が必要なチャットボットに向いている。

(※9) 会話型 AI

会話型人工知能 (AI) とは、ユーザと対話する事ができる、チャットボットや仮想エージェントなどの技術。これらの技術は大容量データ、機械学習、自然言語処理を使用し、発話やテキスト入力を認識し、複数の言語の間で翻訳・通訳を行うなどして、人間の意思疎通を模倣する事が可能。

(※10)ブレインストーミング

集団でアイデアを出し合うことで互いに刺激しあい、その場で想像的な発想を生むことを目的とした会議手法の一つ。

(※11) 機密性2

別紙参照のこと。

(※12) ライセンス違反

ソフトウェアの提供元が定めた方法でソフトウェアを利用しないこと。代表的な例は、有料のソフトウェアライセンスを購入や課金することなく利用すること。

(※13) 権利侵害

この場合の権利侵害は知的財産権に関するもの。知的財産権は、人の幅広い知的創造活動について、その創作者に独占的に搜索を利用する権利を与えるものだが、そうした権利を無視して模倣品や海賊版を作成する行為や、無断で搜索や商用などを利用する行為。

(※14) パブリシティ権侵害

パブリシティ権とは有名人や著名人が、自己の氏名や肖像等が、商品の販売等を促進する顧客吸引力を有する場合、対価を得て第三者に排他的に使用することができる権利であり、パブリシティ権侵害とは、無断で有名人や著名人の氏名や肖像等を利用すること。

## 松戸市情報セキュリティポリシー第5 情報資産の分類と管理方法

## 機密性による情報資産の分類

分類	分類基準	取扱制限	ChatGPT上での 入力可否
3	<ul style="list-style-type: none"> <li>・松戸市情報公開条例第7条に規定する非開示情報のうち、特定の職員等又は組織など、業務上必要とする最小限の者のみが扱う情報</li> <li>・特定個人情報(マイナンバーと紐付けられる情報)</li> </ul>	分類2に掲げる対策のほか、以下に掲げる事項 <ul style="list-style-type: none"> <li>・暗号化やパスワード設定</li> </ul> 特定個人情報においては、上記に掲げる対策のほか、以下に掲げる事項 <ul style="list-style-type: none"> <li>・法令で定める以外の事務での取り扱い禁止</li> <li>・インターネットに接続したコンピュータへの作成・保管・複製</li> </ul>	×
2	松戸市情報公開条例第7条に規定する非開示情報のうち、上記以外の情報資産	<ul style="list-style-type: none"> <li>・許可された者以外による閲覧</li> <li>・適切なネットワーク回線の選択</li> <li>・必要以上の複製及び配布禁止</li> <li>・情報資産の送信・運搬・提供時における暗号化、パスワード設定、鍵付ケースへの格納等</li> <li>・電磁的記録媒体の施錠可能な場所への保管</li> <li>・復元不可能な処理を施しての廃棄</li> </ul>	×
1	上記以外の情報資産		○

【様式1】

令和 年 月 日

DX推進課長

所 属 \_\_\_\_\_  
所属長 \_\_\_\_\_  
担当者 \_\_\_\_\_  
連絡先 \_\_\_\_\_

### ChatGPT アカウント及び利用申請書

提出日	
アカウント	
利用用途	

利用者情報			
No.	mアカウント	氏名	申請区分
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
補足			

※利用可否につきましては、以下に記入の上、返信させていただきます。

DX推進課使用欄	
----------	--

【様式2】

令和 年 月 日

D X 推進課長

所 属

所属長

担当者

連絡先

## ChatGPT活用方法報告書

提出日	
業務名	
ChatGPT利用前の 運用方法	
ChatGPT利用時の 運用方法	
効果	※定量的な要素も含めてご報告下さい。

【様式3】

令和 年 月 日

D X 推進課長

所 属

所属長

担当者

連絡先

## ChatGPT 障害発生報告書

発生日時	
経緯	
原因	
今後の対応と見通し	
備考	

## 松戸市生成AI総合案内チャットボット活用事例報告書

No.	所属名	班、係名	関連事業・業務名	活用方法(どのような場面で、誰が、どのように)	想定活用頻度	担当者 氏名	外線・内線
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							