

City of Kita

北区文章生成AIガイドライン

令和7年3月
DX推進担当課

1章 生成AIと文章生成AI

生成AIとは……………P3

文章生成AIとは……………P4

2章 北区におけるガイドライン

利用上のルール……………P6

（ルール1） 安全性が確保された、庁内共通の文章生成AIを利用すること……………P7

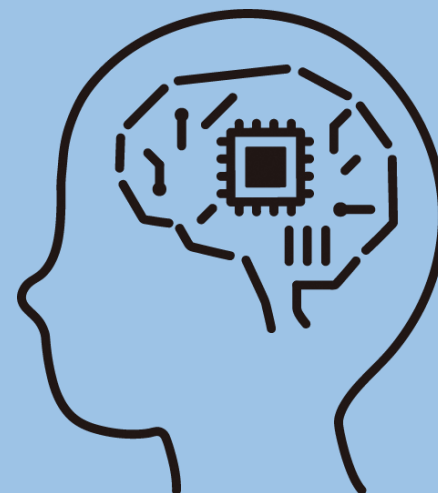
（ルール2） 個人情報等、機密性の高い情報の入力を行わないこと……………P8

（ルール3） 著作権等、他者の権利を侵害するような情報の入力を行わないこと……………P9

（ルール4） 文章生成AIが作成した回答の根拠や裏付けを必ず確認し、修正を行うこと…P10

1章

生成AIと文章生成AI

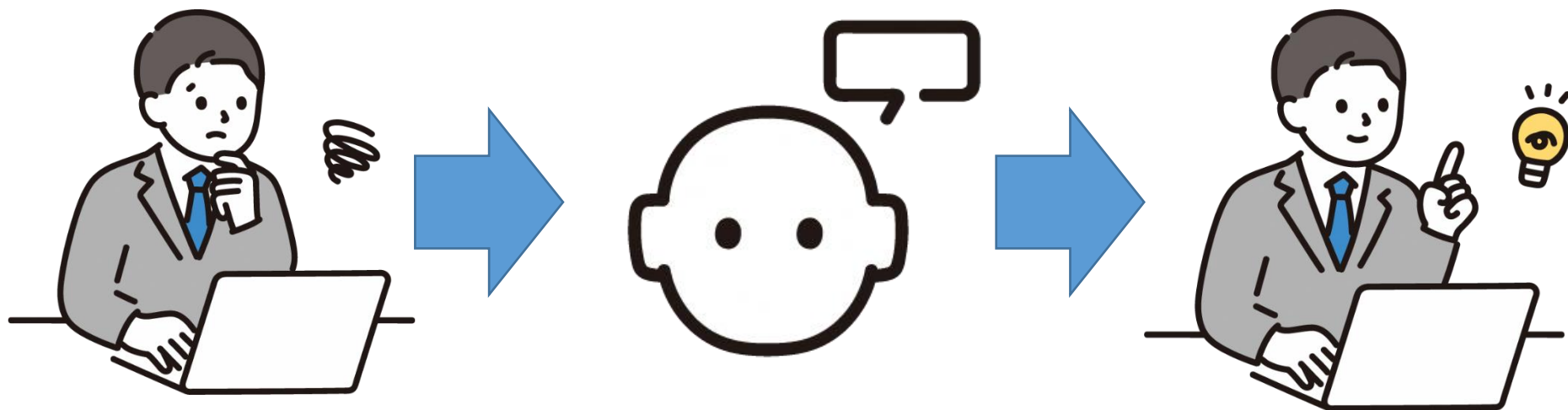


1章では、生成AIと文章生成AIの概要について紹介します。

これまではAIがデータを基礎とした結果を予測し、人間が具体的な対応策を生み出してきました。しかし最近では、AIは驚くべき速さで進化を遂げ、生成AIという新しい技術に注目が集まっています。

生成AIとは、AIに対して指示・命令文(**プロンプト**と言います)を与え、文章やイラスト・音声などを生成することができる人工知能の一つで、人間の業務・作業をサポートするツールとして活用が期待されています。

また生成AIの中でも、文章生成AIは**対話形式**でプロンプト（指示・命令文）に対して応答する点が、これまでのAIとは異なることに注目が集まっています。



■ 文章生成AIとは

文章生成AIとは、ユーザーの様々な質問や命令に対して、高度な返事をしてくれるAIのことです。その仕組みとしては、利用者がプロンプト(指示・命令文)を入力すると、その内容や文脈を読み取り、確率的にありそうな続きの文字を続けていくというものです。

よって文章生成AIは真の知性ではなく、あくまで学習したデータから「**回答として一番相応しい（確率が高い）であろう内容**」を引っ張ってきて、それらしい回答を生成します。

その特徴から、**情報漏洩や回答の不正確性、著作権侵害**など、様々な問題が指摘されています。区の業務での活用においては、特にこうしたリスクへの対応が必要です。



2章

北区におけるガイドライン



2章では、北区におけるガイドライン・利用上のルールについてご説明します。

利用上のルール

文章生成AIを利用する際のルールは以下の4点です。

ルール 1

安全性が確保された、庁内共通の文章生成AIを利用すること

ルール 2

個人情報等、機密性の高い情報の入力を行わないこと

ルール 3

著作権等、他者の権利を侵害するような情報の入力を行わないこと

ルール 4

文章生成AIが作成した回答の根拠や裏付けを必ず確認し、
修正を行うこと

1 安全性が確保された、庁内共通の文章生成AIを利用すること

文章生成AIを利用することで発生するリスクを職員の皆さん自身が理解し、ルールを守って利用することが重要です。

安全性が確保された庁内共通の文章生成AIを利用すること

庁内共通の文章生成AIは安全性が確保されたLGWAN対応サービスであり、入力内容が学習データとして利用されることはありません。

一方、インターネット上の公開された環境で文章生成AIを利用すると、入力内容が学習データとして保存されるなど、情報漏洩につながるリスクがあります。

私物端末を使って業務内容を入力せず、安全性が確保された、庁内共通の文章生成AIを利用してください。

2 個人情報等、機密性の高い情報の入力を行わないこと

文章生成AIは外部サービスに該当し、セキュリティ対策はサービス提供者に依存します。そのため機密情報や未公開情報の入力を行ってしまうと、万が一の場合、情報漏洩につながるリスクがあります。

個人情報等、機密性の高い情報の入力を行わないこと

分類	セキュリティポリシー上の分類	情報資産の例
入力不可	機密性3 情報資産のうち、秘密文書に相当する機密性を要するもの 個人番号（マイナンバー）を含む情報	個人情報（基幹系内で管理している住民情報など）、 特定個人情報、パスワード、ネットワーク情報、 セキュリティ情報など
	機密性2 情報資産のうち、秘密文書に相当するほどの機密性はないが、 すぐには一般に公表することを前提としていないもの	未発表の計画書、見積書、 個人情報※ など
	機密性1 機密性2及び3の情報資産以外の情報資産	カタログ、ひな型、記入要領など

※ 個人情報は内容により機密性2と3に分類されますが、いずれの場合も入力を行わないでください。

3 著作権等、他者の権利を侵害するような情報の入力を行わないこと

単に他人の既存の著作物や作品の名称等を入力するだけの行為は、必ずしも著作権侵害に該当するとは限りません。ただし、AIによる生成物が既存の著作物と**同一・類似している場合**当該生成物の利用が著作権侵害になる可能性もあります。

第三者が著作権等の知的財産権を有する情報の入力を行わないこと

「アニメ〇〇の登場人物△△の定番フレーズを用いたキャッチコピーを考えてください」といった、著作権等の知的財産権が第三者にある情報が含まれたプロンプト（指示・命令文）の入力を行わないでください。

虚偽の個人情報・名誉毀損にあたる情報の入力を行わないこと

文章生成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、そのような情報の入力を行わないでください。

4 文章生成AIが作成した回答の根拠や裏付けを必ず確認し、修正を行うこと

文章生成AIは情報の真偽を判断する能力がなく、提供する回答の情報が常に最新であるとは限りません。

文章生成AI が生成した回答の根拠や裏付けを、必ず自ら確認すること

生成AIは業務執行にあたっての単なる補助的なツールに過ぎないことを前提として、生成した回答の根拠や裏付けを自らが確認し、業務において生成物の使用の検討・判断を必ず行ってください。

生成物の未修正利用の禁止

文章生成AIは、国や北区の最新状況、詳細情報をすべて網羅的に把握しているものではない前提のもと、できあがった生成物の内容をそのまま利用しないでください。特に区民の方々の感情に寄り添う必要がある追悼文等では、生成物をそのまま利用することは控えてください。

必要に応じて「生成AIにより作成」と記載することで、生成された文章がAIによるものか、人間によるものかを読み手に伝えることも大切です。

文章生成AIは自治体職員の業務のあり方を大きく変える可能性を秘めている一方、その特性をよく理解し、**正しく利用**することが大切です。

そのためにも実際に文章生成AIというツールを使ってみて、ツールについて深く知ることが重要です。

まずは**簡単なプロンプト(指示・命令文)**の入力から始め、徐々にコツをつかんでいきましょう！