加賀市　行政事務における生成 AI・ChatGPT 活用

プライバシー影響評価　実施書

令和５年５月３１日

加賀市 イノベーション推進部

はじめに

本実施書は、「加賀市　行政事務における生成 AI・ChatGPT 活用」に対するプライバシー影響評価の実施内容について記載するものです。

プライバシー影響評価とは

プライバシー影響評価（PIA：Privacy Impact Assessment）は、プライバシー情報を取り扱う事業において、潜在的なプライバシーへの影響をアセスメントする手段であり、事業を始める前に、プライバシーリスク、プライバシー保護や情報セキュリティに関する対策等について“評価”を行い、リスクの回避や低減を行うものです。

※本実施書の対象となる市の行政事務における ChatGPT 活用では、個人情報やプライバシー情報を扱いませんが、これまで使用してこなかった新たなテクノロジーを利用することに対し、市民の理解を得るために、PIA を実施しました。

目次

1. 事業

1.1　事業目的

事業の目的について、説明してください。

加賀市は、少子高齢化が進む中、現在、人口の減少が続き、人手不足や地域活力の低下といった新たな問題が起き始めています。一方で、現在、第 4 次産業革命と呼ばれている中、AI や IoT、ロボットなどの先端技術は、予想を超えるスピードで進展しており、近い将来にはこれらの技術が私たちの生活の困りごとに対応し、また、企業の生産性を更に高めていくと言われています。

そのような中、本市では、先端技術の社会実装やデータを広く活用することによって、市民生活の質の向上や経済の発展を図る、デジタルトランスフォーメーション（以降、DX）を推進しております。市の行政事務・サービスにおいても、デジタル技術を活用することで、業務の効率化や住民サービスの向上など、様々な効果が生まれます。

また、近年、生成 AI（人工知能）の ChatGPT が急速に普及しており、自治体においても ChatGPT の活用事例が報告されております。本市においても、ChatGPT を活用することで、DX 推進を加速させていきます。

＜ChatGPT とは＞

ChatGPT とは、自然言語処理技術の一つで、人工知能を用いて自然な会話を行うことができるシステムのことです。

- GPT（Generative Pre-trained Transformer）と呼ばれる技術を用いて、大量のテキストデータ（ウェブ上の文章や書籍、ニュース記事、SNS の投稿など）を学習し、そのデータから自然な文章を生成できる。
- 人間との会話を通じて情報を収集し、問題を解決することができる（例えば、スマートフォンの音声アシスタントや、ネット上のチャットボットなど）。
- ChatGPT（GPT3.5）は 2022 年 11 月に公開された。今後、ますます高度化し、より高度な機能を持つようになることが期待されている。

1.2　事業の実施理由

事業を実施する理由について、説明してください。

自治体の行政事務・サービスに ChatGPT を活用することにより、業務の効率化や住民サービスの向上など、様々な効果が期待できます。

加賀市においても、これらの効果を享受するため、行政事務において ChatGPT を導入し、業務効率化を図るとともに、今後、活用できる領域を評価・検討していきます。

1.3　PIA の実施理由

事業で PIA が必要な理由について、説明してください。

市の行政事務に ChatGPT を活用することは、業務効率化など、様々な効果が期待できます。一方で、生成 AI といった、これまで使用してこなかった新たなテクノロジーを利用することに対し、市民の不安も生じます。

このため、市の行政事務における ChatGPT 活用に対して、リスクを分析し、適切な手段を講ずるとともに、市民の理解を得るために、プライバシー影響評価を実施します。

1.4　事業内容

事業の実施内容について、説明してください。

ChatGPT は、公開情報を扱う（機密情報や個人情報を扱わない）行政事務で活用します。例えば、以下のような業務で利用します。

- 情報収集（業務上のインターネット検索同様)、情報分析
- 文書作成の支援（仕様書(フレーム)の作成など）
- 政策提案のサポート（アイディア出しなど）

1.5　事業根拠

事業の根拠（利益を根拠づけるデータまたは研究）について、説明してください。

ChatGPT を活用した効果（業務効率化など）に関して、実際に ChatGPT を導入した企業の事例などが報告されています。ChatGPT の導入による業務効率化の効果は、企業や業種、導入方法などによって異なるため、数値的な効果を一概に示すことはできませんが、チャットボット、調査・分析、文書の要約などの活用事例が報告されています。

1.6　事業関連性

事業が部局の役割や取組にどのように関連しているか、説明してください。

加賀市役所は、イノベーション推進部を中心に、ChatGPT の全庁活用を推進しています。イノベーション推進部は、地域・行政デジタル化などのイノベーション施策を所管するとともに、全部局のデジタル関連施策を統括しています。

1.7　事業体制

事業に関与する団体・組織、事業者について、説明してください。

ChatGPT 活用に関与する市の組織は、以下の通りです。

＜イノベーション推進部＞

・ ChatGPT 利用環境、利用ルール・ガイドラインなどの提供

＜全部局＞

・ ChatGPT の活用

2. 法令、ポリシー

2.1　法令

事業に係る法令、システムによる情報収集を許可する具体的な法的根拠は何ですか。

以下の ChatGPT に係る総務省の事務連絡を踏まえ対応します。ChatGPT を活用する行政事務では、機密情報や個人情報を扱いません。

＜事務連絡＞

・ ChatGPT 等の生成 AI の業務利用について(令和 5 年 5 月 8 日)（総務省）
https://www.soumu.go.jp/main_content/000879561.pdf

2.2　ポリシー

システムの利用者と運用者に必要なポリシー（方針・ルール）と遵守を確保するための施策について、説明してください。

ChatGPT 活用は、加賀市情報セキュリティポリシー(*1)を遵守します。

また、「生成 AI の利用ガイドライン（日本ディープラーニング協会)」(*2)を参考に利用ルール・ガイドラインを制定しました。利用ルールのポイントは、以下の通りです。

＜利用ルール＞

・ ChatGPT には機密情報、個人情報、プライバシー情報は入力しないこと。
・ ChatGPT から個人情報、プライバシー情報を取得しないこと。
・ ChatGPT の結果（回答）は正確な情報ではない場合があることを認識し、また結果（回答）の理由や根拠を精査したうえで利用すること。

(*1) https://www1.g-reiki.net/kaga/reiki_honbun/r287RG00000058.html
(*2) https://www.jdla.org/document/?utm_source=direct&utm_medium=event

2.3　利用条件

事業で導入するシステムの利用条件がある場合、それらを説明（列挙）してください。

ChatGPT の利用は、情報セキュリティを考慮し、利用環境は以下の条件を満たす必要があります。

＜利用環境＞

・ ChatGPT の利用者の入力情報を学習データとして使用させないこと。

2.4　利用管理

事業で導入するシステムの利用前に必要な手続きと管理者について、説明してください。

ChatGPT の「2.3 利用条件」に従った利用環境の設定を利用前に実施します。

2.5　研修

事業で導入するシステムの利用に必要な研修について、説明してください。

市の職員は、定期的に情報セキュリティ研修を受講しています。

また、ChatGPT 利用について説明会を実施し ChatGPT の利用ルールや利用方法などを周知します。

3. データ収集

3.1　収集データ

事業で収集される情報の詳細について、説明してください。

ChatGPT に収集される市のデータはありません。
なお、ChatGPT は、ウェブ上の文章や書籍、ニュース記事、SNS の投稿といった大量のテキストデータから学習します。

3.2　データ収集方法

＜対象外＞

事業で不適切なデータ収集を最小限にするために、どのような方法で収集しますか。

対象外

3.3　データ収集装置

事業でデータを収集する物理的な機器（カメラや音声記録装置等）はありますか。
物理的な機器がある場合、情報収集について、常時収集中である旨の掲示を行っていますか。使用中であることを示すマークは何ですか。その所有者と連絡先を把握するために、どのような標識が使用されていますか。

対象外

4. データ利用

4.1　データ利用

事業で収集されたデータは、どのように利用しますか。

ChatGPT に収集される市のデータはありません。
なお、ChatGPT では、学習された大量のテキストデータから AI が回答します。

4.2　データアクセス

事業で収集されたデータには、誰がどのようにアクセスしますか。

ChatGPT に収集される市のデータはありません。
なお、ChatGPT は、ウェブブラウザから ChatGPT にログインして利用します。

4.3　他組織・事業者のアクセス

＜対象外＞

事業を市に代わり他組織や事業者が運営・利用する場合、アクセス方法・適用規約（該当する覚書、契約書等）に関して記載してください。

対象外

4.4　アクセス理由

事業でシステムや収集データへのアクセスは、どのような理由で許可されますか。

ChatGPT は、市の公開情報を扱う（機密情報や個人情報を扱わない）行政事務で利用します。

5. データ保存

5.1　データ保存

事業で保存したデータは、どのように安全性を確保しますか。

ChatGPT に保存される市のデータはありません。

＜対象外＞

5.2　データ正確性

事業でシステムが収集・保存した情報の正確性をどのように確認しますか。

対象外

5.3　データ開示・訂正

事業で個人からのデータ開示・訂正請求に対する手順について、説明してください。

対象外

5.4　データ管理責任

事業でデータ保持要件の遵守する責任を負うのは、どの部局ですか。

対象外

6. データ削除

6.1　データ削除

事業のデータの削除、その監査について、説明してください。

ChatGPT に保存される市のデータはありません（データ削除もありません）。

＜対象外＞

6.2　データ削除（例外）

不正や誤って収集されたデータを破棄するためには、どのような措置をとりますか。

対象外

7. データ共有

7.1　データ共有

市内外のどのような団体や組織とデータを共有しますか。

ChatGPT に保存される市のデータはありません（データ共有もありません）。

＜対象外＞

7.2　データ共有の必要性

なぜデータ共有が必要なのですか。

対象外

7.3　市管理外データの利用

市管理外データの利用に制約はありますか。

はい☐　　いいえ☐　　市管理外データの利用はありません☒

6.3.1 「はい」 と答えた場合は、これらの制限を確実に遵守するための部門の手順とポリシーのコピーを提供してください

対象外

7.4　データ共有の審査

事業において、情報共有契約、覚書(MOU)、情報の新たな利用目的、新たなデータ共有の相手からのシステムへのアクセス等を審査し、承認されていますか。

はい☐　　いいえ☐　　新たなデータ共有はありません☒

6.4.1 データ共有契約の審査と更新のプロセスを説明してください

対象外

8. システム

8.1　システム

事業で導入するシステムについて、説明してください。

ChatGPT の利用において、導入するシステムはありません。ChatGPT は、ウェブブラウザから ChatGPT にログインして利用します。

8.2　関連システム

事業で導入するシステムと関連するシステムについて、説明してください。

なし

8.3　システム導入計画

事業のシステム導入計画について、説明してください（いつ、どのように、誰により導入または利用されますか。また、システムがいつ導入され、利用されるのかを決定するのは誰ですか）。

ChatGPT 活用は、2023 年 4 月から加賀市 イノベーション推進部で先行導入し、2023 年 5 月から全庁展開します。

8.4　システム利用頻度

事業で導入するシステムは、どのくらいの頻度で利用されますか。

ChatGPT は、市の公開情報を扱う（機密情報や個人情報を扱わない）行政事務において、日々利用します。

8.5　システム永続性

事業で導入するシステムの永続性について、説明してください。

ChatGPT 活用の終了時期は、今のところ定めていませんが、ChatGPT を含む生成 AI の動向によって検討します。

9. リスクと対策

9.1　プライバシーリスクと対策

事業で収集されたプライバシー情報について、特定されたリスク（危険が生じる可能性）と対策を記述し、各リスクについてどのように軽減されたか、説明してください。

ChatGPT の利用における、想定されるプライバシーリスクと対策は、以下の通りです。

＜想定されるプライバシーリスク＞

（利用者の入力情報によるプライバシーリスク）

- ChatGPT は、利用者が入力した情報を元に自動的に回答を生成するため、入力された情報が学習され、他者の回答に利用される可能性があります。

（回答の内容によるプライバシーリスク）

- ChatGPT が生成した回答が、個人情報を誤用する可能性があります。例えば、回答に含まれる個人情報が不正確であった場合、その情報を誤用する恐れがあります。

＜プライバシーリスクの対策＞

（利用ルール）

- ChatGPT には機密情報、個人情報、プライバシー情報を入力しない。
- ChatGPT から個人情報、プライバシー情報を取得しない。

（利用環境）

- 利用者の入力情報を学習データとして使用しない環境とする。

9.2　セキュリティリスクと対策

事業で導入するシステムのセキュリティリスクと対策を記述し、各リスク（危険が生じる可能性）についてどのように軽減されたか、説明してください。

ChatGPT の利用における、セキュリティリスクに対する対策は、下表の通りです。

リスク	リスク説明	対策
機密性の侵害	機密情報が漏洩する	「9.1 プライバシーリスクと対策」と同じ
完全性の侵害	保管情報が改ざんされる	ChatGPT に市のデータを保管しない
可用性の侵害	サービスが利用できない	高いサービス継続性が必要となる業務には利用しない

9.3　その他リスク

事業でその他に考えられるリスクはありますか。プライバシー侵害やプライバシー情報の悪用が疑われる点はありますか（例えば、予想外の個人への情報プッシュ配信等）。

その他に考えられるリスクとして、利用ルールに従わないケースが考えられます。この対策として、職員向けの情報セキュリティ教育の開催、情報セキュリティ・セルフチェックの実施、端末の操作ログ取得を行います。なお、個人情報は、別の閉じられたネットワーク環境で管理しているため、プライバシー侵害やプライバシー情報の悪用が疑われる点はありません。

10. 監査

10.1 監査

事業で情報を保護するためにどのような監査を実施していますか。

加賀市は、情報セキュリティマネジメントの仕組みを構築しており、定期的に内部監査を実施します。ChatGPT の利用についても監査対象とします。

10.2 監査証跡保護

事業で監査証跡(参照ログ、変更ログ等)に、どのような保護手段が導入されていますか。

加賀市は、端末の操作ログをログ管理システムで収集・管理しています。