

委託業務における生成 AI 利用の禁止事項

藤崎町が発注する委託業務において、生成 AI の利用は業務の効率化や高度化に寄与することが期待される一方、その技術的特性から、これまでにない法的・技術的なリスクを伴います。経済産業省の指針においても、生成 AI への不適切なインプットによる機密情報の漏洩や個人情報の流出、アウトプット（生成物）に含まれる不正確な情報の拡散や第三者の知的財産権（著作権等）の侵害といったリスクが明確に指摘されています。本町が締結する契約においては、受注者は「善管注意義務」を負い、委託業務の実施について第三者に損害を及ぼしたときは、受注者がその損害を賠償しなければならないとされています。そのため、受託者が業務遂行に当たって生成 AI を利用する場合は、生成 AI の特性による不確実性を十分に認識し、「人の目による適切な評価・確認」を徹底するなど、行政の適正性と住民の信頼を確保するための高度な注意義務が求められます。これらを踏まえ、業務の公共性と機密性を維持し、適正な履行を確保するために、委託業務における生成 AI 利用に際して遵守すべき禁止事項を次のとおり定めます。

受託者は、本事項を遵守するとともに、利用するサービスの利用規約の変更状況等を随時管理・把握するなど、適切な管理体制を構築しなければなりません。

1 入力データが AI 学習に利用される生成 AI サービスの利用禁止

オプトアウト設定（学習不許可設定）ができないサービスや、入力データがベンダの AI 学習・サービス改善に利用される仕様のサービス（一般的な無料の約款型サービスなど）の利用を禁止します。

2 個人データ・個人情報の無断入力 of 禁止

本人の同意を得ていない個人データ及び適切な委託関係が結ばれていない個人情報を含むプロンプトの入力を一切禁止します。

3 第三者の著作物や秘密保持義務のある情報の無断入力 of 禁止

第三者が知的財産権（著作権など）を有しているデータや、他者との間で外部提供禁止の秘密保持義務を負っている情報を、適切な許諾や権利制限規定の適用なくインプットとして利用することを禁止します。

4 人による確認（ファクトチェック・権利侵害確認）を経ない成果物の納品禁止

生成 AI が出力したテキストや画像を、委託業者側での適切な「人の目による評価・確認」を経ずに、そのまま納品することを禁止します。

5 セキュリティ水準が低く、ログ保存に対応していないサービスの利用禁止

自治体業務で求める機密水準を満たさないセキュリティ強度のサービスや、第三者認証（ISO/IEC 27001 等）や適切なシステム構成図等の資料で安全性が確認できない生成 AI サービスの利用を禁止します。

6 利用規約の変更状況を管理・把握していない状態での利用禁止

委託業者が、利用している生成 AI サービスの利用規約及びその変更状況を随時確認・管理できる体制を整えていない状態での利用を禁止します。