

五條市生成 AI システム利用ガイドライン (Ver1.0)

令和8年9月25日 策定

五條市

五條市生成 AI システム利用ガイドライン

令和8年9月25日

1. 目的

本ガイドラインは、情報セキュリティリスクを最小化し、個人情報保護、システムの安全性・信頼性を確保しながら、五條市職員(以下、「職員」という。)による生成 AI の適正な利用を促進するため、職員が生成 AI システムを利用する際に遵守・留意すべき事項等を定めるものである。

2. 適用範囲・対象・利用環境

本ガイドラインの適用対象とする行政機関の範囲は、「五條市情報セキュリティポリシー」における情報セキュリティ基本方針に定める適用範囲と同様とする。

本ガイドラインの適用対象とする生成 AI システムは、別表のとおりとし、これらに該当しない生成 AI システムの利用は禁止する。なお、指定されていない生成 AI システムの利用を希望する場合は、各担当課室から情報政策担当課に対し、当該システムの指定を届け出るものとする。

また、生成 AI システムごとに、担当課室、利用者、利用可能な業務の範囲及び入力可能な情報を、別表のとおり定めることとし、入力可能な情報における自治体機密性の分類は、「五條市情報セキュリティポリシー」における情報セキュリティ対策基準で定める情報資産の分類を参照するものとする。

3. 生成 AI システムの利用に係るルール

生成 AI システムを利用する際は、「五條市情報セキュリティポリシー」等とあわせて、以下の(1)利用前のルール及び(2)利用中のルールを遵守すること。

(1)利用前のルール

①前提として理解しておくべき事項(対象:全職員)

(ア)職員が生成 AI システムを利用する際は、情報政策担当課が指定する研修を受講すること。

(イ)生成 AI の利用の際は、要機密情報(「五條市情報セキュリティポリシー」における情報セキュリティ対策基準に定める自治体機密性2以上の情報をいう。以下同じ。)の流出やハルシネーションなどのリスクがあることを理解すること。

- (ウ)生成 AI システムの担当課室(別表に定める「担当課室」をいう。以下同じ。)から説明された利用方法、生成 AI システムの環境、利用規約、利用条件、ルール、セキュリティ上の留意点、生成 AI システムの出力についての精度及びリスクの程度を理解しておくこと。また、情報セキュリティインシデント(望まない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。)、生成 AI システム特有のリスクケース発生時対応等を利用前に理解しておくこと。
- (エ)生成 AI システムへの入力結果及び出力結果は、必要に応じて生成 AI システムの担当課室に提供する必要がある旨を事前に了解すること。また、提供にあたっては情報政策担当課又は担当課室からの求めに応じて、データ提供の手段・形式等について調整するものとする。

②個人情報や要機密情報の取扱いについて留意すべき事項

(対象:別表に指定されていない生成 AI システムの利用を希望する課室、担当課室、情報政策担当課)

- (ア)行政機関等が、生成 AI システムに保有個人情報を含むプロンプト(指示)を入力し、当該保有個人情報が当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、当該行政機関等は個人情報の保護に関する法律(平成 15 年法律第 57 号)の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、当該生成 AI システムを提供する事業者が、当該保有個人情報を機械学習に利用しないこと等を十分に確認すること。
- (イ)要機密情報を取り扱わない場合であっても、国外にサーバ装置を設置している場合は、現地の法令が適用され、現地の政府等による検閲や接收を受ける可能性があることに留意すること。

(2)利用中のルール

①入力データ又はプロンプトにおけるルール

- (ア)利用者側の不理解やミスにより生じるリスクがあることを踏まえて、利用目的の範囲内で生成 AI システムを適切に利用すること(例:生成 AI システムの担当課室から説明された利用方法や必要に応じてマニュアルと照らしつつ、生成 AI システムを利用する。生成 AI システムの担当課室から説明された利用目的範囲外の利用をしない。))。

- (イ)生成 AI システムにプロンプトを入力する場合には、事前に当該生成 AI システムへの入力の可否について別表を確認の上、情報を必要最小限の利用又は提供にとどめること。

②生成物利用におけるルール

- (ア)利用目的に応じて求められる正確性の水準が異なることを意識すること(例:庁内での会議資料に使う簡単なイラスト(低リスク)や庁外向け印刷物に大きく掲載されるキャッチコピー(高リスク)まで、必要度に合わせた正確性が必要となるため、他者の権利(著作権等)を侵害していないか等、作成者の目で出力結果について確認を行う。))。
- (イ)生成 AI システムの出力に基づいて行われた判断も説明責任の対象に含まれることに留意すること(例:利用者自身が生成物について説明できることを確かめた上で業務利用する。必要に応じて生成物を換言して、自身で説明できる表現にする。))。
- (ウ)責任を持つての出力結果の業務への利用判断を行うこと(例:入力データ又はプロンプト、出力結果に含まれるバイアス等に留意して、業務に利用して問題ないかを利用者が判断する。判断に迷う場合は利用しないこととする。))。
- (エ)正確性や根拠・事実関係をリスクに応じて確認すること。
- (オ)安全性・公平性・客観性・中立性等に問題がないことを確認し、問題のある表現は必ず加除修正すること(例:差別用語や倫理に反する表現が含まれていないこと、著作権等第三者の権利を侵害していないこと、第三者の生命・身体・財産等に危害や悪影響を及ぼすことがないこと等を確認する。))。
- (カ)本市が業務を委託する外部事業者に対しては、当該委託業務の成果物に生成 AI システムによる生成物が含まれる場合の取扱い等について、委託契約書等に必要な規定を定めることなどにより、受託業務の遂行に当たって本ガイドラインに沿った対応を求めること。
- (キ)生成 AI システムを利用して職務上作成した文書の取扱いについては、「五條市文書編さん保存規程」等を踏まえて、適切に管理すること。

4. 生成 AI システム特有のリスクケースへの対応

生成 AI システムは、その特徴から、その出力結果に関して、生成 AI システム特有のリスクケースが発生する可能性がある。以下に、生成 AI システム特有のリスクケースの例を示す。

- (ア)生成 AI が人種・性別・文化等に関する偏見や差別を含む社会的に大きな問題となり得る出力を行った。

- (イ)生成 AI が攻撃的又は危険なコンテンツを生成した。
- (ウ)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利用者若しくは第三者に不利益を与えた。
- (エ)利用者が生成 AI により既存の作品に類似し、著作権の侵害等の問題が生じる可能性が高いコンテンツを意図せず生成し、利用したことで当該作品に係る権利者等から削除等の申出を受けた。

生成 AI システム特有のリスクケースが発生した場合、重要度・影響の程度等を踏まえ、以下の手順に沿って速やかに適切な対応を行うこと。

(ア)検知内容の報告

生成 AI システム特有のリスクケースを検知した者は、別紙1「生成 AI システム特有のリスクケースの報告フォーム」の「報告者(生成 AI システムの担当課室・職員等)が記載する欄」の必須項目を記載し、情報政策担当課に報告すること。特に重大なものを検知した場合には、迅速に本市の情報セキュリティにおける責任者である、最高情報セキュリティ責任者(CISO)に報告をすること(例:生成 AI システムが人種・性別・文化等に関する偏見や差別を含む、社会的に大きな問題となり得る出力を行った、など)。

(イ)対処

生成 AI システム特有のリスクケースを検知した者は、必要に応じ情報政策担当課等の指示を仰ぎながら、業務影響特定・原因特定・暫定対応措置・恒久対応措置等を実施すること。

(ウ)対応結果の報告

生成 AI システム特有のリスクケースを検知した者は、別紙1「生成 AI システム特有のリスクケースの報告フォーム」の「報告者(生成 AI システムの担当課室・職員等)が記載する欄」に対処の内容を記載し、「(ア)検知内容の報告」と同様に報告すること。その際、何度も繰り返して上記の特有のリスクケースが再現される場合は、必要に応じて当該生成 AI システム提供事業者等への依頼・要請等を実施すること。

5. 本ガイドラインの定期的な見直し

本ガイドラインの変更は、五條市情報セキュリティ委員会等の決裁によるものとする。ただし、ガイドラインの軽微な変更、別表内のシステムの軽微な変更については、情報政策担当課長の決裁によるものとする。

本ガイドラインの変更は、生成 AI の技術進展や技術動向、脅威環境の変化に応じ、個人情報保護に関する法律の改正等の国におけるルール整備の動向等を踏まえて、適時適切に行う。

6 遵守と違反

五條市情報セキュリティポリシー及び本ガイドラインの違反者に対しては、懲戒処分その他の措置を講じることがある。違反事実を把握した場合は、直ちに所属長及び情報政策担当課へ報告すること。

7. 問い合わせ先

本ガイドラインに関する問い合わせ先は、情報政策担当課とする。なお、各種生成 AI システムについては、各種生成 AI システムの担当課室の窓口担当に問い合わせること。

（※生成 AI システムの利用に係る個別ルールが設けられている場合には、当該ルールに準拠すること。）

別表

生成 AI システム名	担当課室	利用者	利用可能な業務の範囲	入力可能な情報
①QommonsAI (行政用 AI システム)	資産管理課 デジタル推進室	適用対象となる行政機関に所属する全職員	業務目的での汎用的な利用	自治体機密性2以下の情報
②調達インフォ (仕様書作成支援・仕様書チェック等の AI 機能)	契約検査課	適用対象となる行政機関に所属する全職員	入札・契約等の業務目的での汎用的な利用	自治体機密性2以下の情報
③Ami Voice ProVoXT(会議録システム内部のクラウド型 AI 機能)	資産管理課 デジタル推進室 議会事務局	適用対象となる行政機関に所属する全職員	会議録等作成	自治体機密性3B 以下の情報
④NARA AI (県専用環境生成 AI) ※共同利用実証中	資産管理課 デジタル推進室	適用対象となる行政機関に所属する全職員	業務目的での汎用的な利用	自治体機密性2以下の情報

※上記自治体機密性3B 以下、2以下を入力できる生成 AI システムについては、指定の際に、各担当課において、システムを提供する事業者によって入力データが機械学習に利用されないこと及び許可なく監査されないこと等を確認済みである。