別紙２

生成 AI システムの利活用ルール

2026 年 4 月

１　本ルールの目的

本ルールは、愛知県職員による生成 AI の適正な利用を促進するため、「生成 AI の調達・利活用に係るガイドライン」（以下「ガイドライン」という。）等を踏まえ、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　本ルールの対象

- 本ルールの適用対象とする組織の範囲は、ガイドラインに定める適用範囲における組織の範囲と同様とする。
- 本ルールの適用対象とする生成 AI システムは、別表のとおり。なお、入力可能な情報における情報資産の分類は、「愛知県情報セキュリティポリシー」における情報資産の分類を参照すること。

３　生成 AI システムの利活用に係るルール

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

（１） 利活用前のルール

- 本ルールが対象とする生成 AI は、愛知県情報セキュリティポリシーにおける外部サービスにあたることから、生成 AI の利用にあたっては、同セキュリティポリシーをはじめとしたルールを遵守すること。
- 職員が生成 AI システムを利用する前には、デジタル戦略課が指定する研修を必ず受講すること。
- 生成 AI の利用は、様々な活用方策がある一方、情報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し、生成物をそのまま用いることはしないこと。
- 生成 AI システムを所管する所属（別表に定める「所属」をいう。）から説明された利用方法、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すること。（例：利用できる生成 AI システムの環境、利用規約、利用条件、ルール、相談先、情報セキュリティインシデント、生成 AI システム特有のリスクケース発生時対応等を利活用前に理解しておく。）
- 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 システムを所管する所属に提供する必要がある旨を事前に了解すること。

- 職員は、私用デバイスへ私的にインストールした生成 AI に職務上知り得た情報を入力しないこと。
- その他デジタル戦略課及び生成 AI システムを所管する所属の指示に従うこと。

（2） 利活用中のルール

ア 入力データ又はプロンプトにおけるルール

- 愛知県情報セキュリティポリシーに規定する重要性Ａ※以上に該当する情報を生成 AI に入力することは、原則禁止とする。

※重要性ＡＡＡ：秘密を要する情報資産のうち、極めて機密性が高い情報資産
重要性ＡＡ：秘密を要する情報資産のうち、特に機密性・完全性・可用性が高い情報資産
重要性Ａ：秘密を要する情報資産
重要性Ｂ：重要性Ａ以上又は重要性Ｃ以外の情報資産
重要性Ｃ：直ちに一般に公表することを前提としている情報資産

- 個人情報については、単体では個人を識別できない情報であっても、他の情報と照合することで個人を識別できるものは、個人情報に該当する点に注意すること。
- 利用者自身の理解不足や過失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 システムを所管する所属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 システムを所管する所属から説明された利用目的範囲外の利用をしない）。

イ 生成物利活用におけるルール

（ア）生成物の内容に誤りが含まれているおそれがある。

- 生成 AI の基盤技術である大規模言語モデル（LLM）の原理は、「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、もっともらしい文章を作成していくものである。そのため、その内容には誤りが含まれていることを念頭に置き、必ず事実検証（ファクトチェック）を行うこと。
- 生成 AI は、インターネット上の情報を基に学習していることが多いため、生成される回答は、多数派の意見が重視され、少数派の意見が反映されにくい傾向にある。そのため、回答には差別・偏見等のバイアスが含まれていることを念頭に置き、その回答に基づいて判断することによって個人及び集団を不当に差別してしまうことのないよう注意すること。

（イ）AI に判断を委ね、責任を負わせることはできない。

- 生成 AI は、あくまで補助的なツールに過ぎないため、業務における検討・判断の責任は職員にあることを理解して利用すること。
- 生成物又は派生物（生成物を参考に作成したコンテンツ）を外部に公表する際は、県が説明責任を負うことを踏まえ、適切に判断すること。
- 生成 AI への過度な依存は、学習・成長の機会を奪いかねない。そのため、これまで業務を通じて自然に身についていた能力（例：行政文書の作成や校正、文書の読み解き等、政策立案において求められる知識・技能）を職員が獲得できなくなるおそれがあることから、業務や成果物の質を向上させるために生成 AI を利用するのであって、職員は自ら考え判断することをこれまでどおり意識すること。

（ウ）生成物を利用する行為が他者の権利を侵害するおそれがある。

〇著作権侵害

- 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該当するおそれがある。そのため、次の内容を遵守すること。
  - 特定の作者や作家の作品のみを学習させた特化型 AI は利用しない。
  - プロンプトに既存著作物、作家名、作品の名称を入力しない。
  - 特に生成物を「利用」（配信・公開等）する場合には、生成物が既存著作物に類似しないかの調査を行うようにする。

〇商標権・意匠権侵害

- AI を利用して生成した画像や文章を販売活動や広告宣伝などに使う行為は、他者が保有する登録商標権や登録意匠権を侵害するおそれがあるため、生成物が既存著作物に類似しないかの調査に加えて、登録商標・登録意匠の調査を行うようにすること。

〇誤った個人情報・名誉毀損等

- 生成 AI は、個人に関する誤った情報を生成するおそれがあることが知られている。誤った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（法第 19 条・第 20 条）違反や、名誉毀損・信用毀損に該当する可能性があるため、必ず事実検証を行うようにすること。

（エ） 生成物について著作権が発生しない可能性がある。

- 生成物の著作権については、生成 AI を利用しての創作活動に人間の「創作的寄与」があるか否かによって結論が分かれ、著作権が発生しない場合がある。
- 生成物の著作権が発生しない場合、当該生成物は第三者による濫用を防止することができず、自らの創作物として権利の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可能性があるため、留意すること。

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存在する可能性がある。以下に、生成 AI システム特有のリスクケースの例を示す。

- 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。
- 生成 AI が攻撃的、又は危険なコンテンツを生成した。
- 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、又は第三者に不利益を与えた。
- 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、利活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。

（１）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場合は、生成 AI システムを所管する所属に伝え、生成 AI システムを所管する所属は「生成 AI システム特有のリスクケースの報告フォーム」（様式）により、デジタル戦略課に報告すること。

（２）対処

生成 AI システムを所管する所属は、必要に応じて、当該生成 AI システム提供事業者等へ協力を依頼するとともに、デジタル戦略課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。

（３）対応結果の報告

生成 AI システムを所管する所属は、対処した内容について、「生成 AI システム特有のリスクケースの報告フォーム」（様式）により、デジタル戦略課へ報告すること。

５　問い合わせ先

本ルールに関する問い合わせ先は、デジタル戦略課戦略企画グループとする。

以上

別表

生成 AI システム名	所属	利用者	利用可能な業務の範囲	入力可能な情報	備考
具体的な生成 AI システムのサービス名	△△課	△△課に所属する職員	××業務目的での利用	重要性Ｂ以下の情報	