

【東峰村】 生成 AI システム利用ガイドライン

第 1.0 版

令和 8 年 8 月 3 日

東峰村

第1章 本ガイドラインについて

本ガイドラインは、東峰村職員（以下「職員」という。）による生成 AI の適正かつ積極的な利用を促進するとともに、村民や村内事業者に対して、職員がどのようなルールの下で生成 AI を利用するのかを明らかにし、その利用に関する透明性を確保するため、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。

なお、本ガイドラインは職員を対象とするものであるが、この内容が、村民及び村内事業者が生成 AI の適切な利活用について考える際の参考となることも期待する。

第2章 本ガイドラインの対象・利用環境

1 対象とする職員の範囲

本ガイドラインの適用対象とする職員の範囲は、「東峰村セキュリティ基本方針」の「4 適用範囲」で定められた職員の範囲と同様とする。

ただし、学校教育における生成 AI システムの利用その他の分野について、法令、国のガイドライン又は東峰村が別に定める規程等に別段の定めがある場合は、当該定めによるものとする。

2 対象とする生成 AI システム

本ガイドラインの適用対象とする生成 AI システムは、別表に定める「指定生成 AI システム」とする。別表は、セキュリティリスクの観点から職員のみにも周知する。

また、生成 AI システムに入力可能な情報資産の分類は、「東峰村情報セキュリティ対策基準」で定める分類を参照すること。

第3章 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、東峰村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

①生成 AI の基本的な仕組みや特性を理解してから利用すること。

東峰村職員が生成 AI システムを利用する前には、研修資料等を通じて、生成 AI の基本的な仕組み、特性及び留意事項について理解すること。

②特に、生成 AI の使用に伴うリスク・注意点について十分に理解すること。

生成 AI の利用には、業務の効率化や質の向上等の便益が期待される一方で、要機密情報の流出、誤情報の生成、著作権その他の権利の侵害、偏見や差別を含む出力等のリスクがあることを理解すること。

なお、本ガイドラインにおいて「要機密情報」とは、東峰村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機密性 2 以上の情報をいう。以下同じ。

③利用する生成 AI システムの利用方法や制約等を理解すること。

生成 AI システムごとに、利用環境、利用方法、利用条件、入力情報の取扱い、セキュリティ上の留意点、出力の精度及び想定されるリスク等が異なることを理解すること。

④出力結果の利用に伴う説明責任及び利用状況の確認・協力について理解すること。

- ・ ②に示したとおり、生成 AI システムの出力には、誤り、不正確な内容又は不適切な内容が含まれることがあり、その出力を業務に利用することにより、予期せぬ問題が生じる可能性がある。そのため、生成 AI システムの出力を利用して行った業務については、当該出力を利用した職員及びその所属課（室）が、生成 AI システムの利用方法、出力内容の確認方法及び業務上の判断の過程等について、必要に応じて説明できるようにすること。
- ・ また、生成 AI システムの利用に関して問題が生じた場合又は利用状況の確認が必要となった場合は、説明責任を果たし、事実確認や原因究明等を行うため、生成 AI システムを所管する課（室）等が、利用ログ、入力内容、出力内容その他の利用状況に関する情報を確認することがある。この場合、職員は、必要な情報の提供その他の確認に協力する必要があることを、あらかじめ理解すること。

(2) 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の留意事項

不特定多数の利用者に対して提供されるクラウドサービス型の生成 AI システム（ChatGPT 等一般向けの生成 AI システムを含む。）には、無料で利用できるものや、定型約款や規約等への同意のみで利用を開始できるものがあるが、まずは可能な限り「指定生成 AI システム」の利用を検討すること。やむを得ず「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、次の事項に留意し、その必要性や各種リスクへの対策が可能かを十分な検討をすること。

①個人情報・要機密情報の取扱いと各種リスクへの対応に留意すること。

「指定されていない生成 AI システム」については、②以降に示すリスクがあることから、入力情報（プロンプトとして入力する文字情報のほか、添付するファイル、画像、音声等を含む。以下同じ。）に個人情報及び要機密情報を含めてはならない。

また、利用に当たっての設定、利用規約の確認その他の対応は、利用する職員及び所属課（室）の責任において行うこと。ただし、情報セキュリティインシデント又は生成 AI システム特有のリスクケースが発生した場合は、本ガイドライン第 4 章に定めるところにより報告すること。

②入力した情報が学習等に利用される可能性に留意すること。

生成 AI システムへの入力情報は、サービス、利用プラン又は設定によっては、回答の生成以外に、サービスの改善、機械学習その他の目的で利用される可能性がある。

その場合、意図せず情報が漏えいする可能性があるため、入力情報が機械学習等に利用されないこと、機械学習等を停止する設定が適切に行われていること等を十分に確認すること。

③個人情報保護法に違反する可能性に留意すること。

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保護法（平成 15 年法律第 57 号）に違反するおそれがある。

そのため、②に示した学習等に利用される可能性に留意するとともに、①のとおり、入力情報に個人情報を含めてはならない。

④情報が国外で保存又は処理される可能性に留意すること。

生成 AI システムに入力した情報や生成された情報は、国外に設置されたサーバーに保存される場合がある。この場合、現地の法令が適用され、現地政府等による情報の開示要求、検閲、接收その他の措置の対象となる可能性がある。

その場合、意図しない情報の流出等につながるおそれがあるため、①のとおり、入力情報に要機密情報を含めてはならない。

⑤各種機能により情報が保存又は共有される可能性に留意すること。

一般的な生成 AI システムには、会話履歴の保存、過去の会話内容を参照する機能、ファイルの添付、音声・画像の入力、生成内容の共有、外部サービスとの連携、インターネット検索等の機能が備わっている場合がある。

これらの機能を利用することにより、入力した情報が継続して保存されたり、第三者又は外部サービスに送信・共有されたりする可能性がある。また、共有用 URL の発行や公開設定等により、意図せず情報が外部から閲覧可能となるおそれがあることに留意すること。

⑥生成 AI システムごとに利用条件や生成物の取扱いが異なることに留意すること。

生成 AI システムは、システムごと、また、同一のシステムであっても利用プランごとに、業務利用又は商用利用の可否、生成物に関する権利の取扱い、生成物を公開・配布・加工できる範囲、入力情報及び生成物をサービス提供事業者が利用できる範囲、権利侵害等が生じた場合の責任や補償の有無などが異なる。

このため、利用規約その他の利用条件を確認し、予定する利用目的及び利用方法が認められているかに留意すること。

また、サービスの機能、利用規約、プライバシーポリシーその他の利用条件は変更される場合があるため、利用時には最新の内容を確認すること。

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

①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。

- ・ 業務のために利用が認められた生成 AI システムを、職員個人の私的な目的その他の業務目的以外の目的で利用しないこと。
- ・ また、職員の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てはならない。

②入力可能な情報は、指定生成 AI システムごとに確認すること。

入力可能な情報は、別表に定める「指定生成 AI システム一覧」に定める範囲とする。情報資産の分類は「東峰村情報セキュリティ対策基準」で定められている下表のとおり。

分類	分類基準
機密性 3	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産
機密性 2	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表すること前提としない情報資産
機密性 1	機密性 2 又は機密性 3 の情報資産以外の情報資産

入力の可否の判断に迷う場合は、上位の分類として取り扱うか、入力をせず、まずは所属長等に相談すること。また、結果として入力可との判断に至った場合、非特定化处理※¹や仮想例※²で代替する等の対策を講じ、リスクの低減に努めること。

※1 非特定化处理

情報の特定につながる固有の名称や数値、特定の単語や表現・文章等を、無関係又は別の文字列や記号、抽象的・一般的な表現等に置換したり、該当箇所を削除したりすることで、特定化を回避・低減する処理のこと。

※2 仮想例

本質的な構造（課題・目的・制約等）はそのままに、架空の状況・業種・商品等に置き換えた仮想事例のこと。

③文脈や情報の組み合わせ等により特定化につながる可能性に留意すること。

単体で機密性 1 に見える情報でも、複数を組み合わせることで個人等の特定や非公開情報の推測につながる場合があることに留意すること。それが個人情報の場合、単体では個人を識別できない情報でも、個人情報に該当することに留意すること。

④正確かつ最新のデータ入力を行うこと。

不正確な前提情報の入力是不正確な回答につながるため、生成 AI システムに入力する前に、前提が誤っている等の不正確な情報となっていないかを利用者自身でチェックすること。

(2) 生成物利用におけるルール

①不正確な情報や不適切な表現・内容を生成する可能性があることに留意すること。

現在の生成 AI の基盤技術である大規模言語モデル（LLM）とは、膨大な「文字データ（文章やプログラムなど）」を学習し、入力したプロンプトや、それまでに作成された文章に続く「次の単語」を確率的に予測することを繰り返して、「もっともらしい文章」を生成していく仕組みである。その仕組み上、以下のような点に留意する必要がある。

- ・ **ハルシネーション（もっともらしい嘘をつく現象）**：仕組み上、意味を理解して文章を生成しているわけではなく、文脈に続く可能性の高い文章を生成するため、事実とは異なる内容を、正しいことのように出力する場合がある。
- ・ **偏見や差別的回答の可能性**：仕組み上、学習データやインターネット上に存在する偏見や多数派の意見が反映されやすい傾向がある。また、入力者の価値観や入力情報による偏向によって、それらの影響を強く受けた差別的・不公平な内容が出力される可能性がある。
- ・ **情報の鮮度と正確性**：インターネット検索や外部データと連携していない場合、学習を終えた時点までのデータに基づいて出力するため、それ以降の最新情報を反映できない。また、検索機能が有効な状態でも、毎秒更新されるようなリアルタイムの情報や、そもそもインターネット上に公開されていない情報には対応できないこと、検索結果をもとに誤った回答を作る可能性があることに留意すること。
- ・ **個性や感情が伝わらない可能性**：仕組み上、学習した文章から得た表現の傾向やパターンが出力に反映されるため、無難で定型的・機械的な表現になりやすく、固有の個性、表現、感情等が十分に反映されない場合がある。
- ・ **低品質・目的に合わない出力の可能性**：仕組み上、出力内容は、与えられた情報、目的、前提条件、出力形式などによって変化する。必要な情報が不足していたり、目的や指示が曖昧であったりする場合は、体裁は整っていても、具体性、根拠又は検討の深さに欠ける一般的で内容の薄い出力や、目的に合わない内容が出力される可能性がある。
- ・ **生産性や評価を低下させる可能性**：前述までのような不正確、不適切又は内容の薄い生成物を十分に確認せず利用すると、受け取る側に確認や修正の負担を生じさせ、かえって生産性を低下させるだけでなく、発信者や組織全体の評価を損なう可能性がある。

②他者の権利の侵害や炎上リスク、著作権が認められない可能性に留意すること。

生成 AI は、著作物を含むインターネット上の情報も学習しているため、生成される文章やキャッチコピー、コード、イラストやデザイン等において、以下のような点に留意する。

- ・ 既存の著作物に類似したものが生成され、権利を侵害する可能性がある。
同様に、商標権や意匠権、パブリシティ権の侵害につながる可能性がある。

以下の情報は、入力自体が直ちに権利侵害となるものではないが、生成物の利用が各種権利侵害となるおそれがあるため、取扱いに注意すること。

入力情報	侵害の対象	権利侵害の可能性があるケース
著作物（文章やキヤッチコピー、コード、イラストやデザイン等）	著作権	・ 同一・類似する生成物を作成する目的がある場合、入力行為が著作権侵害になる可能性がある。 ・ 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（公開・印刷・配布等）が著作権侵害になる可能性がある。
商標・意匠登録されているロゴやデザイン	商標権 意匠権	・ 故意か偶然（過失の有無）にかかわらず、他社の登録商標と同一・類似のマークを、その指定商品・役務の範囲で商標として使用する行為は商標権侵害になる可能性がある。 ・ また、他社の登録意匠と同一・類似の意匠を業として実施（商用利用を含む）する行為も、同様に意匠権侵害になる可能性がある。 ・ なお、商標権又は意匠権を故意に侵害した場合は、刑事罰の対象となる可能性がある。
著名人の氏名や顔写真	パブリシティ権	・ 生成された氏名や肖像等が特定の著名人と識別でき、かつ専らその顧客吸引力の利用を目的として使用する行為は、パブリシティ権の侵害に該当する可能性がある。

- ・ 著作権的に問題がない生成物であっても、僅かな類似性や品質の問題から炎上に繋がる可能性がある。
- ・ 生成 AI を用いた生成物については、著作権が認められない可能性がある。
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」が認められるか否かについて世界各国でスタンスが異なり、日本においても明確な基準がない状況である。そのため、著作権が必要なものについては、生成 AI を使わない選択肢も含めて事前に検討し、生成 AI を活用する場合は生成物をそのまま利用することはせず、著作物と認められる可能性を高めるために独自の創作的な加工・修正を加えること。また、加工を行う前に、生成物自体が既存の他者の著作物と類似していないかの確認も併せて行うこと。

③起案文書には、必ず生成 AI の利用有無とその利用内容について明示すること。

生成物を利用して作成した文書等について決裁を受けるときは、起案文書に生成 AI を利用した旨を記載する等、意思決定の過程で利用が分かるようにすること。

④生成物は必ず人が確認し、最終判断と説明責任は職員が負うこと。

- ・ ①②のようなリスクがあり、職員による確認が必要なため。

- ・ 行政判断や村民への説明責任は職員にあり、生成 AI の回答は根拠にはならないため。

⑤生成 AI は業務を支援するアシスタントと位置付けて使用すること。

- ・ ①②③のような理由から、生成 AI に判断や説明責任を負わせることはできない。
- ・ より効果的に活用するには、知識・スキルの研鑽が不可欠である。
生成 AI は、誰でもごく短い質問から一定水準の回答を得られる利便性を有する一方、職員が持つ知識、経験、思考力、表現力、判断力を含む総合的な能力が、生成 AI の出力の質や活用範囲に反映される。いわば職員の能力を増幅する道具でもある。これらの能力が高いほど、適切な問いを立て、出力の妥当性を見極めながら、より質の高い成果を効率的に生み出せることにつながるため、生成 AI の普及後も、職員が主体的に知識・スキルを研鑽することの重要性は変わらない。
- ・ 生成 AI への過度な依存による、スキル・思考力の低下に注意する。
生成 AI は便利な道具である一方、思考や判断を過度に委ねると、自ら問いを立て、情報を整理・検証し、試行錯誤しながら結論を導く機会が減少する。こうした状態が続けば、思考力や判断力、表現力、専門的なスキルの低下を招くおそれがある。そのため、生成 AI は思考を代替するものではなく、職員の能力を補い、職員自身の考えを深め、発展させるための道具として、主体的に考える姿勢を保ちながら活用することが重要である。

第 4 章 生成 AI システム特有のリスクケースへの対応

1 生成 AI システム特有のリスクケース

生成 AI システムは、その特徴から、出力結果に関して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。

- ①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。
- ②生成 AI が攻撃的又は危険なコンテンツを生成した。
- ③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。
- ④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。

2 リスクケース発生時の対応

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な対応を行うこと。

(1)検知内容の報告

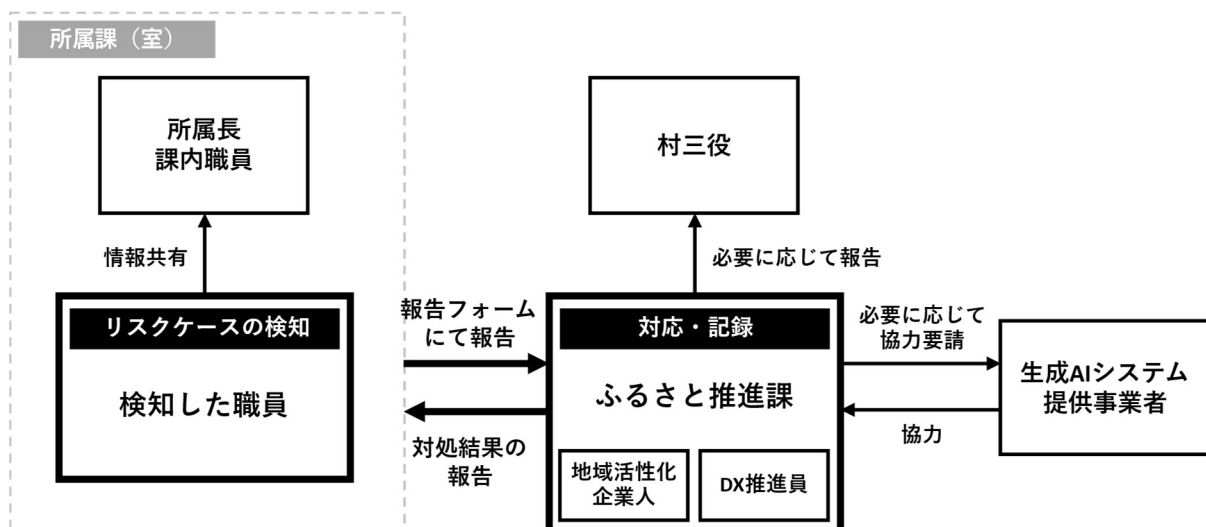
前述のような生成 AI 特有のリスクケースを検知した職員は、所属する職員や所属長と情報を共有するとともに、「生成 AI システム特有のリスクケースの報告フォーム」（様式）等により、ふるさと推進課に報告すること。

(2)対応

報告を受けたふるさと推進課の担当者は、必要に応じて当該生成 AI システム提供事業者へ報告するとともに協力の依頼・要請等を行い、検知した職員と協力して業務影響・原因の特定、暫定対応措置及び恒久対応措置等を実施すること。また、その内容の重要度等必要に応じて、三役に報告すること。

(3)対応結果の記録・共有

対応を行ったふるさと推進課の担当者は、「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）等に対応の内容を記載し、記録を残すこと。また、検知した職員及び関係する職員、報告した三役に情報を共有すること。



第5章 本ガイドラインの変更及び廃止

本ガイドラインの変更及び廃止は、生成 AI の技術進展や、個人情報保護法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。

第 6 章 問い合わせ先

本ガイドラインに関する問い合わせ先は、ふるさと推進課とする。

以上

発行	発行日	改訂内容
第 1.0 版	令和 8 年 8 月 3 日	初版発行