葉山町生成 AI システム利用ガイドライン（Ver1.0）

令和８年３月 24 日

1. 本ガイドラインの目的

本ガイドラインは、葉山町職員による生成 AI の適正な利用を促進するため、葉山町職員が、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. 本ガイドラインの対象・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、「葉山町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における行政機関の範囲と同様とする。
- 本ガイドラインの適用対象とする生成 AI システムは、総務部総務課デジタル推進室（以下、「デジタル推進室」という。）が指定する「exaBase 生成 AI for 自治体」及び「AmiVoice ScribeAssist」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。指定された生成 AI システム以外の利用については、別に定める外部クラウドサービス利用に関するルールに従うものとする。なお、当該ルールが未整備の間は、デジタル推進室への事前相談を要するものとする。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。入力可能な情報における自治体機密性の分類は、「葉山町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とともに、「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和７年３月 28 日改訂）」において示されている、政府機関における対応と整合性を持たせた情報の機密性区分（別紙）を参考として取り扱うものとする。なお、本ガイドラインにおける自治体機密性分類の取扱いは、情報セキュリティポリシー改定までの間の暫定的な運用とする。

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、「葉山町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。

※「「DeepSeek 等の生成 AI の業務利用に関する注意喚起」についての周知」（令和７年２月６日総務省事務連絡)」についても併せて確認されたい。

（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）

- 葉山町職員が生成 AI システムを利用する前には、原則として、デジタル推進室が指定する研修を必ず受講すること。ただし、試行的な利用その他所属長が業務上必要と認めた場合は、この限りではない。また、本ガイドラインにおける研修には、集合研修のほか、動画視聴、資料確認、e ラーニング等を含むものとする。
- 生成 AI の利用は、様々な便益が期待される一方、要機密情報（「葉山町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（生成 AI による便益とリスクについては、「行政の進化と革新のための生成 AI の調達・利用に係るガイドライン」（令和７年５月 27 日デジタル社会推進会議幹事会決定）の「５　生成 AI による便益とリスクを理解した利活用推進」を参照。）。
- 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、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（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。）。
- 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（例：デジタル推進室からの求めに応じて、アクセス可能な状態であれば入力データ又はプロンプト、出力結果、データ提供の手段、形式等を提出する。）。
- 葉山町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てはならないこと。

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：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、デジタル推進室）

- 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）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。

- 不特定多数の利用者に対して提供され、かつ定型約款や規約等への同意のみで利用可能となるクラウドサービス型の生成AIシステムを業務で利用する場合には、原則として、要機密情報を取り扱わないこと。
  要機密情報を取り扱わない場合であっても、不特定多数の利用者に対して提供され、かつ定型約款や規約等への同意のみで利用可能となるクラウドサービス型の生成AIシステムを業務で利用する場合には、「葉山町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の「9. 業務委託と外部サービスの利用（自治体機密性２以上の情報を取り扱わない場合）」に基づき、利用の許可を得ること。
  また、要機密情報を取り扱わない場合であっても、例えば、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収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

- 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。）。
- 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を確認の上、保有個人情報の利用目的のための必要最小限の利用又は提供であることを十分に確認すること（例：生成AIシステムの担当課室が別に定める利用ルールを確認し、問題がないかを判断した上で利用、判断が付かない場合は個人情報を含まないプロンプトとする。）。
- 正確かつ最新のデータ入力を行うこと（例：不正確な回答につながってしまうため、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。）。

② 生成物利用におけるルール

- 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し、生成AIシステムの出力結果を確認すること。

- 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。）。
- 責任を持って生成AIシステム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。）。
- 正確性や根拠・事実関係を必要な範囲内でリスクに応じて確認すること。
- 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。）。
- 葉山町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。
- 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、「葉山町文書取扱規程」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。

- 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若しく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、速やかに別紙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、デジタル推進室に報告すること。特に重大なものを検知した場合には、迅速に AI の利用・リスク管理における責任者（AI 統括責任者（CAIO）等にも報告をすること（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。）。

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、必要に応じデジタル推進室・CAIO 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、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. 本ガイドラインの変更及び廃止

本ガイドラインの変更及び廃止は、CAIO 等の決裁によるものとする。ただし、形式修正等の軽微なものについては、デジタル推進室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、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。

6. 問い合わせ先

本ガイドラインに関する問い合わせ先は、デジタル推進室とする。

以上

（別紙）

機密性の分類、分類基準については、以下の情報資産の例、利用可能なパブリッククラウドサービスの範囲を参考とされたい。

機密性 高 → 低

分類	分類基準	情報資産	パブリッククラウドサービス（※１）の範囲
自治体機密性３A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成23年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	＜例＞ ・「行政文書の管理に関するガイドライン」上の極秘文書、秘文書に相当する文書（統一基準における機密性３情報に相当する情報） ・極秘文書：秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書 秘文書：極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書	「行政文書の管理に関するガイドライン」、統一基準の規定に則って取り扱うものとする（なお、上記ガイドラインにおいては、極秘文書について、インターネットに接続していない電子計算機又は媒体等に保存することが求められている（※２））
自治体機密性３B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	＜例＞ ・データベースや台帳形式になった住民情報を含む個人情報ファイル及びこれに準ずる情報 （住民記録システム、税務システム、国民健康保険システム、生活保護システム、農業委員会台帳システム、貸付金償還システム等に保存される住民の個人情報）	ISMAP登録サービスは利用可（8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要） ※統一基準改定に合わせて、8.3でクラウドサービスの利用について規定
自治体機密性３C	行政事務で取り扱う情報資産のうち、自治体機密性３B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	＜例＞ ・職員としての属性に基づく個人情報 ・オンライン申請の処理等により、システム処理上一時的にインターネット上に保管されるデータ ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格など非公開情報	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３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を前提としていない情報資産	＜例＞ ・政策検討に関する情報	可 （8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要）
自治体機密性１	自治体機密性２又は機密性３の情報資産以外の情報資産	＜例＞ ・将来公表する予定の文書（白書の案等） ・公表された情報	可

注）自治体機密性３C情報については、情報資産単位でのアクセス制御、業務システムログ管理の実施等、β'モデルにおいてインターネット接続系に求められている対策を実施することで、インターネット接続系における取扱いが可能。
※１　クラウド事業者が提供するサーバやネットワークなどのインフラを、仮想化技術により複数のユーザで共用し、個々のユーザが、システムの運用体系を完全に制御することが難しいサービスを想定している。
※２「行政文書の管理に関するガイドライン」（平成23年４月１日内閣総理大臣決定、令和４年２月7日 全部改定）第10 秘密文書等の管理

図表 23　機密性の分類、分類基準の例示

出典：総務省『地方公共団体における情報セキュリティポリシーに関するガイドライン（令和７年３月版）』

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
exaBase生成AI for 自治体	総務課デジタル推進室	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
AmiVoice ScribeAssist（音声認識・議事録作成システム）	総務課文書法制係	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

なお、指定の際に、総務課デジタル推進室において、要機密情報を入力可能な生成AIシステムについては、当該生成AI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葉山町の許可なく監査されないことを確認済みである。