



大河原町生成AⅠ利用ガイドライン



大 河 原 町

令和8年1月

目次

1. はじめに	3
1.1 目的	
1.2 位置づけと基本原則	
1.3 適用範囲	
1.4 対象とする生成 AI	
1.5 用語の定義	
2. 生成 AI の利用に関する基本方針	4
2.1 利活用の推進	
2.2 リスク管理との両立	
3. 生成 AI の利用ルール	4
3.1 利用する AI ツールについて	
3.2 データ入力・プロンプト作成時の注意事項	
3.2.1 情報の機密性分類と取扱い	
3.2.2 機密性情報の取扱いにおける非特定化措置	
3.2.3 プロンプト作成上の注意	
3.3 生成 AI 利用時の注意事項	
3.3.1 生成物の信頼性とファクトチェック	
3.3.2 権利侵害（著作権、商標権、意匠権、プライバシー権等）	
3.3.3 生成物の権利の帰属と保護	
3.3.4 商用利用の制限	
3.3.5 生成 AI 提供事業者のポリシー・利用規約の遵守	
3.3.6 業務外利用の禁止	
3.3.7 判断と責任の所在、説明責任	
3.3.8 感情に配慮が必要な文書の扱い	
3.3.9 バイアスと公平性への配慮	
3.3.10 セキュリティ（不正利用、インシデント対応等）	
3.3.11 ID/パスワードの管理	
3.4 リスク評価と高リスク AI への対応	
3.4.1 リスク評価の実施	
3.4.2 高リスク AI と判断された場合の対応	
4. 生成 AI の活用	9
4.1 生成 AI を活用した行政業務の効率化	
4.1.1 文書作成等の自動化・支援	
4.1.2 町民対応のチャットボット導入・運用	

4.1.3	広報資料・コンテンツ作成支援	
4.2	生成 AI による政策立案・推進の支援	
4.2.1	データ分析に基づく政策立案のサポート	
4.2.2	過去の事例・知見の抽出・分析サポート	
4.3	生成 AI とデータベース・外部システム連携	
4.3.1	自治体固有データベース等との連携（RAG 等）	
4.3.2	リアルタイムデータ等の活用	
4.4	生成 AI による住民参加・協働の促進	
4.4.1	住民意見の集約・分析サポート	
4.4.2	アンケート・対話型コンテンツ作成と集計・分析サポート	
4.5	先進・他自治体事例の活用と効果測定	
4.5.1	先進・他自治体等の成功・失敗事例の紹介と分析	
4.5.2	導入後の効果測定と評価・改善（PDCA）	
4.6	高度な AI 活用への展望（AI エージェント等）	
5.	ガバナンス体制	11
5.1	推進・管理体制（AI 統括責任者(CAIO)相当職、相談窓口）	
5.2	人材育成・研修（リテラシー向上、倫理研修）	
6.	ガイドラインの見直し	11

1. はじめに

1.1 目的

本ガイドラインは、大河原町（以下「本町」という。）のセキュリティポリシーに基づき、かつ国の定める「人間中心の AI 社会原則」及び関連ガイドラインの趣旨を踏まえ、職員が業務で生成 AI を利用する際に遵守すべき事項を示すものです。生成 AI は業務効率の向上や創造的なアイデアの提供に役立ちますが、不適切な使用により法令違反や権利侵害、情報漏洩、差別助長等のリスクが生じる可能性もあります。本ガイドラインは、リスク管理と利活用促進を表裏一体で進めることを目的とし、職員が安全かつ効果的に生成 AI を活用するための指針となります。本ガイドラインを熟読し、その趣旨を理解した上で、生成 AI を活用してください。

1.2 位置づけと基本原則

本ガイドラインは、本町における生成 AI の利用に関するルールとして、全職員が遵守すべきものです。生成 AI の利活用にあたっては、以下の基本原則を尊重します。

- **人間中心:** AI は人間の幸福と尊厳を尊重し、支援するために利用します。
- **安全性:** AI の利用が個人や社会に危害を及ぼさないよう、安全確保に努めます。
- **公平性:** AI の利用において、差別や偏見を生じさせないよう、公平性の確保に努めます。
- **プライバシー保護:** 個人のプライバシー権を尊重し、関連法令等を遵守します。
- **セキュリティ確保:** 不正アクセス、情報漏洩等の脅威から情報を保護します。
- **透明性:** AI の利用状況や判断プロセスについて、可能な範囲で説明可能性を確保します。
- **アカウントビリティ（説明責任）:** AI の利用に関する判断と結果について、説明責任を果たせるようにします。

1.3 適用範囲

本ガイドラインは、町長、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、議会事務局、及び地方公営企業の職員（会計年度任用職員、派遣職員等を含む）に適用されます。

利用にあたり職員に利用 ID とパスワードを付与します。

1.4 対象とする生成 AI

本ガイドラインは、主として大規模言語モデル（LLM）を構成要素とするテキスト生成 AI を対象とします。画像、動画、音声等を生成する AI や、より高度なタスクを実行する AI（AI エージェント等）については、今後の技術動向や利用状況を踏まえ、必要に応じて本ガイドラインの改訂や別途の指針を検討します。

1.5 用語の定義

- **生成 AI(Generative AI):** テキスト、画像、音声、プログラムコード等の様々なコンテンツやアイデアを生成できる AI。
- **AI モデル:** 入力データに応じた予測結果等を生成する AI システムの中核部分。
- **大規模言語モデル (LLM):** 大量のテキストデータでトレーニングされた、人間のような自然な文章を生成・理解する能力を持つ AI モデル。

- **AI ガバナンス:** AI の利活用によって生じるリスクを管理し、便益を最大化することを目的とする、技術的、組織的、及び社会的システムの設計並びに運用。
- **プロンプト:** 生成 AI に対して、処理や応答を指示するために与えるテキスト（指示文・命令文）等の入力。
- **ハルシネーション:** 生成 AI が、事実に基づかない、もっともらしい虚偽の情報を生成する現象。
- **機密性情報:** 本町の情報セキュリティポリシーで定める機密性の高い情報。国の区分における「機密性 2 情報」等に相当する情報を含む。
- **個人情報:** 個人情報の保護に関する法律に規定される個人情報。
- **約款型外部サービス:** 不特定多数の利用者に対して提供され、画一的な約款や規約等への同意のみで利用可能となる外部の AI サービス。
- **個別契約サービス:** 本町として個別に契約を締結し、データの取扱い、セキュリティ要件等が明確化された AI サービス。
- **非特定化措置:** 匿名化、置換対応、マスキング等、情報の特定につながる要素を排除・低減するための処理。

2. 生成 AI の利用に関する基本方針

2.1 利活用の推進

本町は、行政サービスの向上、業務効率化、政策立案能力の強化等に資するため、本ガイドラインに基づき、生成 AI の積極的な利活用を推進します。職員が、創造性を発揮し、新たな価値創出のために生成 AI を活用します。

2.2 リスク管理との両立

生成 AI の利活用にあたっては、情報漏洩、権利侵害、差別助長、不確実な情報等のリスクを十分に認識し、本ガイドラインに示すルールを遵守することで、これらのリスクを低減し、安全な利用を確保します。利活用の推進とリスク管理は表裏一体であり、バランスの取れた運用を目指します。

3. 生成 AI の利用ルール

3.1 利用する AI ツールについて

本町では、ポリミル社提供の QommonsAI（コモンズ AI）、日本 DX 地域創生応援団提供の公務員専用 AI マサルくんを公式の生成 AI ツールとして利用します。

なお、ChatGPT や Bing Chat などの約款型外部サービス（特にコンシューマー向けサービスや国外にサーバを持つサービス）に関しては、情報セキュリティポリシーに基づき、データ越境リスク、現地法令によるアクセス・差押えリスク、利用規約上の制約等を考慮し、生成 AI を主目的として業務データを入力する行為は原則禁止とします。検索エンジンの検索結果に AI による要約が含まれる場合は例外としますが、情報の取り扱いに関する管理・監査、説明責任の観点から、能動的な利用は避けてください。例外的に外部サービスを利用する必要がある場合は、リスク評価、契約内容等の詳細な資料を付して総括情報セキュリティ責任者に協議を行ってください。

3.2 データ入力・プロンプト作成時の注意事項

3.2.1 情報の重要度分類と取扱い

生成 AI にデータを入力する際には、本町の情報セキュリティポリシー等に定められた機密性による情報資産の分類に応じて、その取扱いを判断する必要があります。機密性分類は、情報が漏えいした場合の影響レベルに応じて定められており、主な分類と基本的な考え方は以下の通りです。（※詳細な定義や具体的な情報の分類は、大河原町情報セキュリティポリシーを参照のこと）

- **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:** 行政情報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を前提としていない情報資産。
- **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。

【機密性レベルごとの入力ルール】

生成 AI へのデータ入力可否は、情報の機密性分類に応じて、以下の点を考慮し、適切な対応をとってください。

1. 機密性 3 情報:

- 漏洩時の影響が極めて甚大であるため、原則として生成 AI への入力は避けるべき情報です。
- 非特定化措置を施してもなおリスクが高いと考えられるため、利用は想定していません。

2. 機密性 2 情報:

- 漏洩時の影響を考慮し、注意深い取り扱いが必要な情報です。
- 約款型外部サービスへの入力は原則禁止とします。
- 個別契約を締結し、ISMAP 登録サービス相当以上のセキュリティ対策（例：アクセス制御、データの暗号化、国内データセンター利用、監査ログ取得等）が講じられているサービスを利用する場合、「非特定化措置」を実施することを前提とし、業務上の必要性に応じて利用してください。

3. 機密性 1 情報:

- 個別契約サービスであれば、比較的安全に利用可能です。意図しない情報が含まれないか確認することを推奨します。
- 約款型外部サービスへの入力は原則禁止です。

【非特定化措置の重要性と実施責任】

上記ルールにおいて、機密性の高い情報を扱う際の鍵となるのが「非特定化措置」です。これらの措置を適切かつ徹底的に行うことで、情報漏洩リスクを大幅に低減し、生成 AI 活用の可能性を広げることができます。

ただし、非特定化措置が完全であることを保証するものではありません。文脈から情報が推測される可能性等も考慮し、措置の実施後もリスクが残存することを認識し、入力の必要性を慎重に判断し

てください。

具体的な非特定化措置の方法は、3.2.2 を参照してください。

【補足事項】

- 上記ルールは最低限の基準であり、各部署の判断でより厳格なルールを適用することは可能です。
- 機密性情報を入力する場合は、常に 3.2.2 に定める対策を講じ、リスクを最小化してください。
- 判断に迷う場合は、必ず政策企画課デジタル政策推進室に相談してください。

3.2.2 機密性情報の取扱いにおける非特定化措置

前項（3.2.1）で述べたように、機密性の高い情報を生成 AI で扱う場合は、情報漏洩等のリスクを最小限に抑えるため、非特定化措置が不可欠です。機密性の高い情報（機密性 2）を入力する際には、以下の対策を複数組み合わせるなど、情報の特定につながる要素を排除することが、安全な利用の前提となります。

【実施すべき非特定化措置】

- **匿名化:** 個人名、組織名、役職名、地名、固有の製品名などを、意味のない記号（例：A 氏、X 社、Y 部署、Z 市）や一般的な名称（例：担当者、関係機関）に置き換えます。置き換えパターンは推測されないように注意し、対応表等は作成しないか、作成する場合は厳重に管理します。
- **置換対応:** 文書内で繰り返し出現する特定の機密情報（例：特定のプロジェクトコード、未公開の数値データ）を、一時的な記号（例：[Project-X]、[CONFIDENTIAL-1]）に置き換えます。処理後に正確に元に戻せるよう、置換箇所と元の内容の対応関係を安全な方法で管理し、復元後は速やかに対応情報を破棄します。
- **マスキング:** 日付の一部（例：202X 年 X 月）、住所の一部（例：〇〇市△△）、金額の桁数（例：〇〇〇万円）など、完全には削除できないが特定性を下げたい情報を「*****」や「〇〇」で覆い隠します。ただし、他の情報と組み合わせることで推測が可能にならないか、十分に注意が必要です。

【非特定化措置実施上の注意点】

- **措置の徹底:** 一部の情報だけを処理しても、他の情報から推測できれば意味がありません。文脈全体を考慮し、特定につながる可能性のある要素を網羅的に処理してください。
- **組み合わせの有効性:** 単一の措置よりも、匿名化とマスキング、置換対応と匿名化などを組み合わせることで、より安全性が高まります。
- **作業プロセス記録:** どのような非特定化措置を施したか、作業プロセスを記録しておくことが望ましいです。

3.2.3 プロンプト作成上の注意

プロンプトを作成する際は、以下の点に注意してください。

- 入力禁止・制限付き許可に該当する情報（個人情報、機密情報等）をプロンプト自体に含めない。

- 具体的すぎる内部情報（未公開の計画、人事情報等）を含めない。
- 誤解を招くような曖昧な表現や、攻撃的・差別的な表現を避ける。

3.3 生成 AI 利用時の注意事項

3.3.1 生成物の信頼性とファクトチェック

生成 AI は、確率的に文章等を生成するため、内容に虚偽（ハルシネーション）が含まれる可能性があります。生成された情報を鵜呑みにせず、必ず利用者自身の責任において事実確認（ファクトチェック）を行ってください。特に、統計データ、法令、専門知識、歴史的事実等に関する情報は、必ず信頼できる情報源（公式文書、専門家の監修記事等）で裏付けを取ってください。複数の AI で確認する、出典を確認する等の対策も有効です。

3.3.2 権利侵害（著作権、商標権、意匠権、プライバシー権等）

生成されたコンテンツが、既存の著作物、商標、意匠、あるいは個人のプライバシー権や肖像権（パブリシティ権含む）等を侵害する可能性があります。以下の点に注意し、関連法令（著作権法、商標法、意匠法、個人情報保護法等）及び文化庁「AI と著作権に関する考え方について」等を遵守してください。

- 特定の作者や作品のみを学習させた特化型 AI の利用は慎重に行う。
- プロンプトに既存の著作物名、作家名、ブランド名、個人名等を安易に入力しない。
- 生成物を公開・利用（複製・配信・翻案等）する際は、既存の権利（特に著作権、商標権、意匠権）を侵害していないか、事前に調査・確認する。特に、生成された画像や音楽、キャッチコピー等の利用には注意が必要です。登録商標・意匠の調査も必要に応じて実施してください。
- 個人に関する情報（特に非公開情報や評価に関する情報）を生成・利用する場合は、プライバシー侵害や名誉毀損にあたらないか十分に注意する。

3.3.3 生成物の権利の帰属と保護

AI が生成したコンテンツには、著作権が発生しない可能性があります（人間の創作的寄与が認められない場合等）。そのまま利用した場合、第三者による模倣を防げない可能性があります。本町として権利を確保したい制作物（例：広報キャラクター、シンボルマーク等）に AI を利用する場合は、AI による生成物を素材としつつ、職員が十分に創作的な修正・加筆を行うことで、著作物性を確保するように努めてください。あるいは、権利関係が明確な契約に基づき外部に委託することを検討してください。

3.3.4 商用利用の制限

生成 AI サービスによっては、生成物の商用利用が制限されている場合があります。利用規約を必ず確認し、許可されている範囲で利用してください。

3.3.5 生成 AI 提供事業者のポリシー・利用規約の遵守

各生成 AI サービスには、法令とは別に独自の利用規約やポリシー（禁止事項、利用目的の制限、AI 生成物であることの表示義務等）が定められています。これらを十分に確認し、遵守してください。

3.3.6 業務外利用の禁止

生成 AI は、本町の業務目的に限り使用し、私的な目的や業務外での利用は禁止とします。

3.3.7 判断と責任の所在、説明責任

生成 AI はあくまで補助的なツールであり、業務における最終的な判断とそれに伴う責任は職員自身にあります。AI が提供する情報は、本町や地域の個別具体的な状況を完全に理解しているわけではありません。AI の出力を鵜呑みにせず、必ず人間が内容を精査し、判断を行ってください。特に重要な意思決定や外部に影響を与える可能性のある業務においては、AI の利用状況や判断プロセスを記録に残し、説明責任を果たせるようにしておくことが望ましいです。

3.3.8 感情に配慮が必要な文書の扱い

追悼文、お見舞い状、謝罪文など、人間の感情に深く関わる文書や、高度な配慮を要する文書の作成に生成 AI を使用する際は、必ず人間が表現のニュアンスや適切性を十分に吟味し、必要に応じて加筆・修正を行ってください。

3.3.9 バイアスと公平性への配慮

生成 AI は、学習データに含まれる社会的・歴史的なバイアスを反映・増幅する可能性があります。生成された内容に、特定の属性（人種、性別、年齢、宗教、出身地、障害の有無等）に対する偏見や差別的な表現が含まれていないか、常に注意を払い、多様な視点から確認してください。問題がある表現を発見した場合は、利用せず、修正してください。AI の利用が、行政サービスの公平性を損なうことがないように努めてください。

3.3.10 セキュリティ（不正利用、インシデント対応等）

生成 AI の利用においては、以下のようなセキュリティリスクにも注意が必要です。

- **不正利用:** 悪意のあるプロンプト（プロンプトインジェクション等）により、AI が意図しない動作をする可能性があります。不審な挙動が見られた場合は利用を中止し、速やかに所属長及び政策企画課デジタル政策推進室に報告してください。
- **マルウェア感染:** 生成 AI を騙るフィッシングサイトや、生成されたコードにマルウェアが含まれる可能性も考慮し、不審なリンクやファイルを開かないように注意してください。
- **インシデント発生時の対応:** AI 利用中に情報漏洩や不正アクセス等のインシデントが発生した場合、またはその疑いがある場合は、速やかに所属長及び政策企画課デジタル政策推進室に報告してください。

3.3.11 ID/パスワードの管理

生成 AI サービスの利用に必要な ID 及びパスワードは、本町の情報セキュリティポリシーに基づき、以下の点を遵守し厳重に管理してください。

- ID・パスワードを紙に記録して PC に貼り付けたり、安易にアクセスできる場所に保管しない。
- パスワードは他人に教えない、共有しない。
- パスワードは十分な長さや複雑性（英大文字、小文字、数字、記号の組み合わせ等）を持たせる。

3.4 リスク評価と高リスク AI への対応

3.4.1 リスク評価の実施

生成 AI を新たな業務やシステムに導入し、既存業務での利用方法を大幅に変更する場合は、その利用目的、影響範囲、取り扱う情報の種類、利用者の範囲、判断プロセス等を考慮し、リスク評価を実施することが推奨されます。評価にあたっては、以下の点を考慮してください。

- **影響の大きさ:** 利用結果が町民の権利や安全、財産に重大な影響を与える可能性はないか。
- **利用者の範囲:** 不特定多数の町民が利用するか、特定の職員のみか。
- **情報の機微性:** 個人情報（特に要配慮個人情報）や機密情報を取り扱うか。
- **判断プロセス:** AI の出力のみに基づいて自動的に判断が行われるか、人間による最終確認・判断が介在するか。
- **公平性:** 特定の属性を持つ人々に不利益を与えるバイアスが生じるリスクはないか。

3.4.2 高リスク AI と判断された場合の対応

リスク評価の結果、「高リスク」な利用（例：町民の評価や選考に利用する、重要なインフラ制御に関わる等）に該当すると判断された場合、またはその可能性がある場合は、原則利用を禁止します。

4. 生成 AI の活用

生成 AI は、適切に利用すれば、行政運営の様々な側面で有効活用できる可能性があります。以下に活用例を示しますが、これらに限定されるものではありません。活用にあたっては、常に本ガイドラインの利用ルールを遵守してください。

4.1 生成 AI を活用した行政業務の効率化

4.1.1 文書作成等の自動化・支援

報告書、議事録、通知文、メール文面等の定型的な文書作成の迅速化、文章の要約、校正、翻訳、ブレインストーミングによるアイデア出し等を支援し、職員の負担を軽減します。

4.1.2 町民対応のチャットボット導入・運用

町民からの定型的な問い合わせに対して、24時間365日対応可能なチャットボットを導入・運用し、町民サービスの利便性向上と職員の対応負荷軽減を図ります。ただし、回答精度の確保、個人情報保護、エスカレーション体制の整備が不可欠です。

4.1.3 広報資料・コンテンツ作成支援

広報誌、ウェブサイト、SNS 等で使用する文章（キャッチコピー含む）やデザイン案の作成、多言語対応などを支援し、より魅力的で効果的な情報発信をサポートします。著作権・肖像権等には充分注意が必要です。

4.2 生成 AI による政策立案・推進の支援

4.2.1 データ分析に基づく政策立案のサポート

過去のデータや統計データを分析し、傾向把握、将来予測、政策効果のシミュレーション等を支援することで、客観的根拠に基づく政策立案をサポートします。データの可視化も支援します。ただし、分析結果の解釈と最終判断は人間が行います。

4.2.2 過去の事例・知見の抽出・分析サポート

膨大な量の文書（過去の政策文書、審議会議事録、研究報告書、他自治体事例等）から、関連性の高い情報、成功・失敗要因、教訓等を効率的に抽出し、分析することを支援します。

4.3 生成 AI とデータベース・外部システム連携

4.3.1 自治体固有データベース等との連携（RAG 等）

生成 AI を本町固有のデータベースや文書管理システムと連携させ、庁内情報に基づいた、より正確で状況に即した回答生成（RAG: Retrieval-Augmented Generation 等の技術を活用）を可能にします。情報セキュリティとアクセス権限管理の徹底が前提となります。

4.3.2 リアルタイムデータ等の活用

リアルタイムで収集されるデータ（気象情報、交通情報、センサーデータ等）を生成 AI が分析・活用し、現状把握や予測の精度を高め、即時対応が求められる課題（災害対応、イベント運営等）への対応力を向上させます。

4.4 生成 AI による市民参加・協働の促進

4.4.1 市民意見の集約・分析サポート

パブリックコメントやアンケート等で寄せられた大量の町民意見を、AI がトピックやキーワード、賛否、感情（ポジティブ/ネガティブ）等に基づいて自動的に分類・整理・要約し、分析作業を効率化・高度化します。多言語意見の翻訳も支援します。

4.4.2 アンケート・対話型コンテンツ作成と集計・分析サポート

政策課題等に関するアンケートの質問項目作成支援、オンライン対話型コンテンツ（意見交換ボット等）の作成支援、回答データの自動集計・可視化・分析支援等により、効果的な住民参加・意見収集をサポートします。

4.5 先進・他自治体事例の活用と効果測定

4.5.1 先進・他自治体等の成功・失敗事例の紹介と分析

生成 AI を導入・活用している他の自治体や民間企業等の事例（成功事例、失敗事例、課題、効果等）を調査・分析し、本町における導入検討や改善の参考にします。

4.5.2 導入後の効果測定と評価・改善（PDCA）

生成 AI の導入効果（業務時間削減効果、市民満足度向上、コスト削減等）を定量・定性的に測定・評価し、その結果に基づいて利用方法の改善や対象業務の拡大等を検討する PDCA サイクルを回します。

4.6 高度な AI 活用への展望（AI エージェント等）

将来的には、より自律的にタスクを実行できる AI エージェント等の活用も視野に入れ、技術動向を注視しつつ、さらなる行政の高度化・効率化に向けた検討を進めます。その際は、本ガイドラインの見直しや新たなルールの策定を行います。

5. ガバナンス体制

生成 AI の利活用を適切に推進し、リスクを効果的に管理するため、以下のガバナンス体制を整備・運用します。

5.1 推進・管理体制（AI 統括責任者(CAIO)相当職、相談窓口）

本町における生成 AI の利活用に関する方針策定、リスク評価基準の設定、庁内ルールの整備・周知、高リスク AI 利用の検討、インシデント対応の統括等を担う責任者を明確に定めます。

また、職員が生成 AI の利用に関して技術的・倫理的な疑問や懸念を気軽に相談できる窓口を設置します。

5.2 人材育成・研修（リテラシー向上、倫理研修）

全職員を対象に、生成 AI の基本的な仕組み、メリット、リスク、本ガイドラインの内容、倫理的な配慮事項等に関するリテラシー向上のための研修を定期的実施します。また、AI を積極的に活用する部署や管理者層に対しては、より専門的な研修や事例共有の機会を提供します。

6. ガイドラインの見直し

本ガイドラインは、生成 AI を取り巻く技術の急速な進展、新たなリスクや課題の顕在化、利活用の進展状況、関連する法令や国のガイドラインの改定等を踏まえ、定期的または必要に応じて見直し、改訂を行います。