**兵庫県**

**兵庫県生成AI利用ガイドライン**

**付録１　 Q&A集**

[１　利用範囲、利用許可等について 1](#_Toc152678856)

[議会答弁での利用 1](#_Toc152678857)

[所属長の利用許可の考え方 1](#_Toc152678858)

[利用許可簿記録頻度の考え方 1](#_Toc152678859)

[外部サービスでメールアドレス以外の利用登録が必要な場合 1](#_Toc152678860)

[デジタル改革課が提供する有償サービス 1](#_Toc152678861)

[画像生成AIを使う場合 2](#_Toc152678862)

[２　システムの設定について 2](#_Toc152678863)

[入力情報の漏えい対策 2](#_Toc152678864)

[漏えい対策（オプトアウト）が可能なサービス 3](#_Toc152678865)

[３　入力する情報について 3](#_Toc152678866)

[名前や固有名詞をマスキングすれば個人情報に当たらないか 3](#_Toc152678867)

[AIの学習に利用されないにも関わらず、個人情報の入力ができない理由 4](#_Toc152678868)

[将来的に個人情報の入力ができるようになる可能性は 4](#_Toc152678869)

[国の「機密性２」の情報の取扱い 5](#_Toc152678870)

[４　利用場面ごとの留意点について 5](#_Toc152678871)

[会議・打合せの要約時の留意点 5](#_Toc152678872)

[県の内規を要約する際の留意点 6](#_Toc152678873)

[新規施策の壁打ち等に利用する時の留意点 6](#_Toc152678874)

[記者発表資料の作成に利用する場合の留意点 6](#_Toc152678875)

[５　生成物についての留意点 7](#_Toc152678876)

[生成物の修正加工はどの程度行えばよいかの目安 7](#_Toc152678877)

[生成物の内容確認はどの程度行えばよいかの目安 7](#_Toc152678878)

[生成AIシステムを利用した生成物公開時の対応 7](#_Toc152678879)

[ChatGPTを使った場合は内部利用でも表示義務はあるのか 8](#_Toc152678880)

[生成物をそのまま利用する場合に表示必須とした理由 8](#_Toc152678881)

[生成AIシステムを利用した生成物が結果的に第三者の著作物に類似した場合 9](#_Toc152678882)

[６　その他 9](#_Toc152678883)

[委託契約時の留意点 9](#_Toc152678884)

更新履歴

|  |  |  |
| --- | --- | --- |
| 版 | 発行日 | 改訂内容 |
| 第1.0版 | 令和5年10月19日 | 初版発行 |
| 第1.1版 | 令和5年12月18日 | 問タイトルの軽微な修正 |

# １　利用範囲、利用許可等について

## 議会答弁での利用



議会の答弁作成にChatGPTを使用してもよいか。

議会の答弁要旨案の作成は、職員が自ら行うべきものであり、ChatGPT等で得られた文案をそのまま利用するようなことはあってはならない。一方で、得られた文案を職員が責任を持って内容確認、取捨選択、修正加工して利用する前提であれば、最初の下書きにChatGPT等を使用することは差し支えない。

## 所属長の利用許可の考え方

所属長の利用許可について、許可基準のようなものはないか。

許可に当たっては、利用目的が業務に必要なものであることを確認いただきたい（利用許可簿に主な利用目的を記録することとしている。）。

## 利用許可簿記録頻度の考え方

どのような業務に利用する場合でも、利用許可簿の記録は必要か。

どのような業務に利用する場合でも、利用許可簿の記録は必要である。ただし、実際の利用時に逐一許可する以外に、ある程度の期間（例：令和5年10月1日～令和6年3月31日）を定めて、包括的に許可することも想定している。

## 外部サービスでメールアドレス以外の利用登録が必要な場合

外部サービスの利用登録時にメールアドレス以外に電話番号も求められる場合はどのように対応すべきか。

電話番号も求められる場合は、所属の公用携帯電話がある場合はその番号を登録し、公用携帯電話がない場合は、個人の携帯電話番号を登録して差し支えない。

## デジタル改革課が提供する有償サービス

ガイドラインに記載されている「有償サービス」とは具体的に何か。

令和5年10月時点では㈱エクサウィザーズの「exaBase生成AI」のみである。このシステムは指針第18条の2第1号の「運用管理者が利用者を定める生成AIシステム」に該当するため、利用についての所属長の許可は不要となる。

なお、このシステムは指針第18条の2第２号の「安全性が確認されたものとして統括者が許可した生成AIシステム」には該当しないため、情報公開条例第6条に定める非公開情報、個人情報保護法第2条第1項に定める個人情報は入力できない。

## 画像生成AIを使う場合

画像生成AIを使いたい場合はどうすればよいか。

本ガイドラインは指針第18条の2に定める「生成AIシステム」を対象としており、画像生成AIもその中に含まれる。ただし、県の業務における画像生成AIの利用実績がなく、知見を有する職員もいないため、現在のガイドラインは文章生成AIを念頭に置いて記述しており、画像生成AIに関しては内容が不十分な可能性がある。このため、画像生成AIを利用しようとする場合は、情報セキュリティ対策統括者への事前相談、事後報告を行っていただくこととしている。

画像生成AIは既に多くのサービスがリリースされており、今後県の業務での活用が進む可能性がある。ガイドラインに関係の留意事項を盛り込んでいくためにも一定の利用経験が必要であるため、利用を希望する所属は積極的に相談いただきたい。

# ２　システムの設定について

## 入力情報の漏えい対策

ChatGPTは入力した情報を学習すると聞いており、情報漏えいが心配だ。防ぐ方法はないか。

ガイドラインでは、利用許可の対象となるのは、入力データを学習しない設定（オプトアウト）が可能な生成AIシステムに原則限るものとし、職員にはオプトアウトを選択して利用することを求めている。

ChatGPT（WEB版）では以下の2つの方法でオプトアウトを選択できる。

① OpenAIのWEBサイトで示されている利用規約に基づく「オプトアプト申請」

② ChatGPTの「設定」⇒「データコントロール」⇒「チャット履歴無効化設定」

②がオンオフの切り替えで済む簡便な方法であり、令和5年4月28日付事務連絡「ChatGPTの適切な利用について」で②の設定方法を周知している。

なお、入力データが学習に使われることがない場合でもOpenAI等の生成AI事業者が一定期間サーバー内にデータを保持し、可能性は低いとしても、そのデータが利用される懸念は残るため、情報公開条例第6条に定める非公開情報、個人情報保護法第2条第1項に定める個人情報の入力は不可としている。

## 漏えい対策（オプトアウト）が可能なサービス

ChatGPT以外に入力情報が学習に利用されない設定が可能なサービスはあるか。

無償で利用できる生成AIシステムのうち、オプトアウトを選択できるのは、現時点（令和5年10月）ではChatGPTとGoogle Bardのみであり、Microsoft Bing等はオプトアウトの選択ができない。よって、デジタル改革課が導入する有償サービス以外で業務利用が認められるのはChatGPTとGoogle Bardのみとなる。今後オプトアウトが可能な生成AIシステムを確認でき次第、Q＆Aを改定して職員に周知を図りたい。

# ３　入力する情報について

## 名前や固有名詞をマスキングすれば個人情報に当たらないか

氏名や社名は、消去又はマスキングあるいは「A氏」「B社」などの匿名化をすれば、個人情報や法人情報には当たらず、プロンプトに入力可能という理解でよいか。

氏名等の個人情報（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。情報公開条例第6条第1号の対象となる情報とは範囲が異なるため留意すること。）については、情報公開条例第6条に定める非公開情報に当たるか否かに関わらず、入力不可である。

氏名等の消去・マスキングその他の匿名化措置（以下「匿名化」という。）をしても、①それ以外のデータから特定の個人を識別できる場合（例えば、行動特性（例：特技、よく○○に居る）や固有の特徴（例：特徴ある容貌、服装等）から個人を特定できる場合）、②一般的に公開されている情報や県が保有する情報と入力情報とを照合して特定の個人が識別できる場合には、匿名化した情報も個人情報に該当する。入力情報と匿名化前の元データとを照合することで特定の個人を識別できる場合や、対応表を保持している場合も、個人情報に該当することとなるので注意すること。

個人情報や個人の属性に関する情報を匿名化する場合は、単に氏名等を消去・マスキング等すれば個人情報に該当しなくなると安易に考えるのではなく、個人の特定につながらないよう慎重な検討を要する。

また、未だ公開していない会議録を要約させるような場合は、会議録中の氏名等の個人情報や個人の属性に関する情報を、上記の観点から匿名化した上で、さらに個人の特定につながる情報がないかを確認して入力すべきである。そこで得られた生成物において、再度、個人が特定できるようになっていないかを確認することも必要である。

なお、個人・法人の特定ができない場合であっても、条例第6条第1号後段の通常他人に知られたくない情報（犯罪歴、犯罪被害、反省文等）や、条例第6条第2号の法人等の権利、競争上の地位その他正当な利益を害するおそれのあるもの（例：研究中の発明・特許、顧客情報、未発表の著作物（歌詞等））の入力は避けること。

## AIの学習に利用されないにも関わらず、個人情報の入力ができない理由

ChatGPTのオプトアウト設定やAPI連携のシステムを使えばAIの学習に利用されないと聞いているが、このような場合でも個人情報の入力を禁じているのはなぜか。

ガイドラインでは次の２つの観点から個人情報の入力を不可としている。

観点1　個人情報の目的外利用に当たる可能性

地方公共団体は、一部の場合を除き、個人情報を保有するに当たって特定された利用目的以外の目的のために個人情報を利用してはならないこととされている（個人情報保護法第69条第1項）。利用目的以外の目的に利用できる場合は同条第2項各号に定められており、生成AIに個人情報を入力することが同項各号に該当すると認められるための「相当の理由」や「特別の理由」が必要となる。このため、同項各号に該当するかどうかを各所属で慎重に検討する必要があるが、そうした労力をかけてまで個人情報を入力しようとすることは現実的な対応とは言えない。

観点2　生成AI事業者が個人情報を利用する可能性

利用目的のための利用ないしは個人情報保護法第69条第2項による利用目的以外の目的のための利用に該当する場合でも、個人情報の提供を受ける生成AI事業者が、その情報を機械学習に利用しないこと等を十分に確認する必要がある（「生成AIサービスの利用に関する注意喚起等について」R5.6.2個人情報保護委員会）。

ChatGPTのオプトアウト設定やAPI連携のシステム（デジタル改革課で導入する有償サービスはこれに該当）を使えば、入力データが学習に使われることはないが、その場合でもOpenAI等の生成AI事業者が一定期間サーバー内にデータを保持し、可能性は低いとしても、そのデータが利用される懸念は残る。

こうした場合において、必要があると認めるときは事業者に個人情報の適切な管理のために必要な措置を講ずることを求めるものとされている（個人情報保護法第70条）が、生成AI事業者が生成AIサービスの個々の利用者からの要求に応じることは想定しえないことであり、同条に基づく措置要求を行うことは現実的な対応とは言えない。

## 将来的に個人情報の入力ができるようになる可能性は

現在は個人情報の入力が禁じられているが、将来MicrosoftのAzure上に兵庫県独自の環境を構築した場合でも同様か。

MicrosoftのAzure上に県独自の環境を構築した場合は、同社や第三者がサーバー内のデータに一切アクセスできないこと、その他安全管理措置（個人情報保護法第66条）の具備を確認した上で、指針第18条の2第2号の「安全性が確保されたものとして統括者が許可した生成AIシステム」とする見込みである。その場合には、利用目的内の保有個人情報の利用（個人情報保護法第69条第1項）、または利用目的外であっても内部利用であって相当の理由があり、かつ本人等の権利利益を不当に侵害するおそれがない場合（同条第2項第2号）等であれば、個人情報を入力することが可能となる。

## 国の「機密性２」の情報の取扱い

「機密性２」と記された国の文書の情報は入力不可だと思うが、本県の情報公開条例の非公開情報との関係はどう理解すればよいか。また、オンプレミスやMicrosoft Azureの環境であれば「機密性２」でも入力可とする余地があるのではないか。

「政府機関等のサイバーセキュリティ対策のための統一基準」に定める機密性２情報は本県の情報公開条例第6条に定める非公開情報の第６号（事務又は事業に関する情報）に当たる可能性が高いため、収受した国の文書に「機密性２」「取扱注意」等の記載がある場合は、当該文書の情報は入力しないこと。

なお、MicrosoftのAzure上に県独自の環境を構築した場合は、同社や第三者がサーバー内のデータに一切アクセスできないこと、その他安全管理措置（個人情報保護法第66条）の具備を確認した上で、指針第18条の2第2号の「安全性が確保されたものとして統括者が許可した生成AIシステム」とする見込みである。その場合には「機密性２」等の記載がある文書の情報でも入力可とする余地はあるが、国のデジタル社会推進会議幹事会「ChatGPT等の生成AIの業務利用に関する申合せ」における取扱いとの整合を図る必要があるため、同申合せの最新版の内容を事前に十分確認すること。

# ４　利用場面ごとの留意点について

## 会議・打合せの要約時の留意点

議事録の要約に使う場合に留意すべきことはあるか。

要約のために議事録をプロンプトとして生成AIシステムに入力する際に注意が必要である。具体的には、「入力不可の情報」である情報公開条例第6条に定める非公開情報、個人情報保護法第2条第1項に定める個人情報や「入力に注意を要する情報」である職務上知り得た秘密等が議事録に含まれていないかを確認し、そのような情報があれば消去又はマスキングする必要がある。

## 県の内規を要約する際の留意点

一般に公開していない内規を要約等のためにプロンプトとして入力してよいか。

一般に公開していない内規であっても、情報公開条例第6条に定める非公開情報に該当しない部分は、公開請求があれば公開することになるため、非公開情報に該当する部分を除き、必要な場合は入力して差し支えないものと考える。

## 新規施策の壁打ち等に利用する時の留意点

新規施策の検討に利用する場合に特に留意すべきことは何か。また、検討中の新規施策の内容をプロンプトとして入力してもよいか。

新規施策の検討（アイデア出しや壁打ち等）に利用するのは、発想を広げる（思いがけないアイデアを得られる）上でも、バランスを保つ（多様な視点に気付かされる）上でも有効であり、生成AIシステムの効果的な使い方の一つである。

新規施策の検討に生成AIシステムを利用する場合は、その業務の重要性に鑑みて尚更生成物の利用に関する責任は職員の側にあることを認識し、生成物の内容に誤りや偏りがないかを十分確認するとともに、生成物はあくまでも一つの素材に過ぎないという前提で取捨選択、修正加工を行うべきことに留意されたい。

また、検討中の新規施策の内容であっても、ガイドラインに定める「入力不可の情報」「入力に注意を要する情報」を除いては入力しても差し支えない。

## 記者発表資料の作成に利用する場合の留意点

記者発表資料の作成に利用してもよいか。

当然公表前の情報をプロンプトとして入力することになると考えられるが、ガイドラインに定める「入力不可の情報」「入力に注意を要する情報」を除いては入力しても差し支えない。むしろ注意すべきは得られた生成物を利用するときであり、誤った情報が含まれている可能性があるため、正確性、妥当性の十分な確認が必要である。

# ５　生成物についての留意点

## 生成物の修正加工はどの程度行えばよいかの目安

生成物の利用に当たっては、取捨選択、修正加工を行った上で利用するとされているが、どの程度修正加工等を行えばよいのか。

AIによる生成物は、一見もっともらしい内容でも、不正確、不適当な内容を含んでいる可能性があることから、生成物に関する説明責任は生成AIシステムの使用者である職員の側にあることを踏まえ、原則取捨選択、修正加工を行うこととしている。

どの程度修正加工等を行えばよいかの具体的な基準はないが、AIによる生成物はあくまでも一つの素材に過ぎないという前提に立ち、正確性、妥当性の確保に加えて、利用する場面に合った内容にする、簡潔明瞭な内容にするなど、各業務の目的に照らして十分な取捨選択、修正加工を行っていただくようお願いしたい。

## 生成物の内容確認はどの程度行えばよいかの目安

生成物の利用に当たっては、複数の職員で正確性、妥当性を十分確認することとある。確認に際して特に留意すべき事項はあるか。

情報公開条例第6条の「非公開情報」や個人情報保護法第2条第1項の「個人情報」を含んでいないことの確認に加え、ChatGPT等の文章生成AIが一般的に弱いとされている点（主なものは下記）を踏まえた確認を行っていただきたい。

・事実関係の誤り：意味を理解して出力しているわけではないことから、単純な事実関係の誤りを平気で出力するケースがある。

・偏り（偏見）：インターネット上の情報を学習させて作られたものであることから、意図しない偏り（偏見）が含まれている可能性がある。

・計算：一般的に計算は不得意とされているので、数字の取扱いには注意を要する。

・最新情報：ある特定の時点までのインターネット上の情報を学習させて作られたものであることから、最新の情報には疎い。

## 生成AIシステムを利用した生成物公開時の対応

OpenAIは利用規約で、AIによる生成物を公開する際には第三者がAIによる生成物であることを認識できるよう表示することを求めている。OpenAIのサービスを使う際は、AIによる生成物をそのまま利用するのではなく、アイデア出しや壁打ち、文案の下書き等に利用する場合でも、AIによる生成物と表示しないといけないのか。

OpenAIは「共有・公開ポリシー」において、ソーシャルメディアへの投稿時に「コンテンツがAIによって生成されたものであることをユーザーが見逃すことがないように明示する」こと、また、OpenAIのAPIを使用して作成したコンテンツについて「コンテンツの作成におけるAIの役割が示されており、通常の読者が見逃すことがなく、十分に理解できる方法で説明されている」ことを求めている。

このため、OpenAIの生成AIシステムを使用して作成したコンテンツを公開する場合は、生成物をそのまま利用するのではない場合でも、「ChatGPTによる生成物を修正加工して作成」等と表示する必要があると考える。

## ChatGPTを使った場合は内部利用でも表示義務はあるのか

ChatGPTを使って作成したコンテンツを公開する際には、AIを使用して作成したコンテンツであることを明示する必要があるとのことだが、外部に公開せず、内部利用に止まる場合は、明示不要という理解でよいか。

OpenAIが「共有・公開ポリシー」で求めている明示は、人が作成したものと一般の読者・ユーザーが誤認することを防ぐために設けられた規定と考えられ、コンテンツが確実に内部利用に止まる場合にまで明示必須と解する必要はないと考える。

ただし、内部利用に止めると言いながら、結果的に外部に公開される可能性は常にあるため、OpenAIのサービスを使用する場合には、内部利用に止める場合でも、将来外部に公開される可能性を考慮して明示の要否を判断されたい。

## 生成物をそのまま利用する場合に表示必須とした理由

OpenAIのように利用規約で表示義務が課されている場合は仕方ないが、そうでない場合でも、生成物をそのまま利用する場合は「AIにより生成」等と表示しないといけないことにしたのはなぜか。

生成AIの特性から、生成物には不正確、不適当な内容が含まれている可能性が常にあり、あくまでも一つの素材として取り扱うようガイドラインでは規定している。正確性、妥当性を十分確認した結果、生成物をそのまま利用しても差し支えない場合もあるとは思うが、一つの素材に過ぎないという前提に立って取捨選択、修正加工を行う旨を徹底するため、例外的なケースとしてあえて生成物をそのまま利用する場合には、AIによる生成物であることを表示するよう義務付ける規定とした。

## 生成AIシステムを利用した生成物が結果的に第三者の著作物に類似した場合

プロンプトに作者名や作品名を入力したわけでもないのに、生成物が結果的に第三者の著作物に類似してしまった場合でも、著作権の侵害となるか。

著作権侵害は「後発の作品が既存の著作物と同一又は類似していること（類似性）」と「既存の著作物に依拠して複製等がされたこと（依拠性）」の両方の要件を満たすことが必要とされており、このケースでは「依拠性」が認められるかどうかが論点となる。

既存の著作物を知らず、偶然に一致したに過ぎない場合は「依拠性」はないものと考えられるが、裁判例では「既存の著作物に接する機会があったか」「既存の著作物が周知・著名だったか」等が総合的に考慮されることになる点に留意すること。

# ６　その他

## 委託契約時の留意点

「対象となる職員等」において、県から業務委託を受ける外部の事業者に対しては、委託契約書等で生成AIによる生成物を含む成果物の取扱い等について必要な規定を設ける旨の記載があるが、具体的にはどのように記載すればよいか。

　令和5年10月19日付で出納局会計課・企画部情報政策課から発出した通知において、委託契約書及び請書への記載例を示したので、参考にしていただきたい。



兵庫県生成AI利用ガイドライン 付録１ Q＆A集は「クリエイティブ・コモンズ・ライセンス 表示4.0国際」に基づき、出典の表示を条件として自由な二次利用を許諾します。