# ChatGPT 等の生成 AI の利用ガイドライン

第 1.0 版

第 1.0 版：令和５年６月１９日

千葉県デジタル改革推進局デジタル推進課作成

本ガイドラインは、まずは**内部資料の作成等に限った試用**として、各所属の職員の皆さんが千葉県情報セキュリティポリシーの範囲内で、業務上 ChatGPT などの生成 AI を利用する際に注意すべき事項を定めたものです。

生成 AI は、業務効率の改善や新しいアイデア出しなどに役立つ一方で、入力するデータの内容や生成物の利用方法によっては法令に違反したり、他者の権利を侵害したりする可能性があります。本ガイドラインの内容を十分に理解した上で、生成 AI を上手に利用してください。

また、利用する生成 AI の仕様や、業務の性質、内容等により、このガイドラインで判断できないことがありましたら、デジタル推進課に確認するなどして、適正な利用が図られるよう努めてください。

なお、このガイドラインの作成に当たっては、一般社団法人日本ディープラーニング協会作成の「生成 AI の利用ガイドライン第１版」（2023 年５月公開）を参考にしています。今後も、本格利用に向け、社会動向等を踏まえ随時見直しを行っていきます。

**＜利用に当たっての注意事項＞**

**Ⅰ　データ入力に際しての注意事項**

（１）入力内容を学習内容に反映しない設定をした上で利用すること。

（２）個人情報、機密情報、法令や契約等により非公開とされている情報をはじめ機密性２以上の情報を入力しないこと（当該情報の入力は禁止）。

（３）県の業務だとわかるような聞き方をしないこと。

**Ⅱ　生成物の利用に際して注意事項**

（１）利用は内部資料に限ることとし、外部向けの資料等には使わないこと。

（２）得られた回答を鵜呑みにせず、根拠等をしっかり確認すること。

（３）得られた回答をそのまま使用せず、権利侵害等となっていないかをしっかり確認すること。

（４）資料作成等の際に生成 AI から得られた回答を利用した場合は、資料中に明記すること（例：【生成 AI 名】により作成）

**Ⅲ　その他**

（１）問題が発生した場合は、直ちに所属長に報告すること。

## Ⅰ　データ入力に際しての注意事項

**（１）入力内容を学習内容に反映しない設定をした上で利用すること。**

ChatGPT 等の生成 AI の標準設定では、生成 AI とのやりとりの「チャット履歴」が、AI で応答の生成をするためのデータとして利用される可能性があり、個人情報や機密情報の情報漏洩のリスクが考えられます。

そのため、生成物を利用するに当たっては、システム上可能な場合、入力内容を学習内容に反映しない設定をした上で利用してください。

**（２）個人情報、機密情報、法令や契約等により非公開とされている情報をはじめ機密性２以上の情報を入力しないこと（当該情報の入力は禁止）。**

生成 AI の利用に当たっては、（１）のとおり、入力内容を学習内容に反映しない設定をした上で利用することとしていますが、そのような設定を行った場合でも、生成 AI に入力するデータには、個人情報、機密情報、法令や契約等により非公開とされている情報や、直ちに一般公表することを前提としていない情報を入力することは禁止します。

※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を要しないが、直ちに一般公表することを前提としていない情報資産（千葉県情報セキュリティ対策基準「６ 情報資産の分類と管理」）

※ 幹部レク結果の要約、策定中の計画の概要版の作成など、政策形成過程の情報等については利用しないよう注意してください。

**（３）県の業務だとわかるような聞き方をしないこと。**

生成 AI の利用に当たっては、（１）のとおり、入力内容を学習内容に反映しない設定をした上で利用することとしていますが、そのような設定を行った場合でも、生成 AI に入力するデータには、県の業務だとわかるような聞き方をせず、抽象化した聞き方にするようにしてください。

（よくない例）千葉県庁で生成 AI を業務利用する際の課題を１０個教えてください。
（望ましい例）都道府県レベルの自治体で生成 AI を業務利用する際の課題を１０個教えてください。

## Ⅱ　生成物の利用に際して注意事項

**（１）利用は内部資料に限ることとし、外部向けの資料等には使わないこと。**

生成 AI の利用に関し、使い方や懸念点等についての確認がまだ必要であるため、生成 AI の生成物利用にあたっては、内部資料にのみ使ってください。

**（２）得られた回答を鵜呑みにせず、根拠等をしっかり確認すること。**

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り、書かれている内容には虚偽が含まれている可能性があります。

そのため、生成物を利用するにあたっては、必ず根拠や裏付けを確認するようにしてください。

※Bing では、チャットでの回答時に根拠が表示されます。

※AI はフェイク情報も学習して回答してしまうことがあるので確認が重要です。

**（３）得られた回答をそのまま使用せず、権利侵害等となっていないかをしっかり確認すること。**

生成物が、既存の著作物と同一・類似している場合は、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可能性があります。

また、生成 AI を利用して生成したキャッチコピーなどを宣伝などに使う行為は、他者が権利を持っている登録商標権や登録意匠権を侵害する可能性があります。

上記を踏まえ、生成物を利用するにあたっては、必ず著作権侵害、商標権・意匠権侵害など、権利侵害となっていないかを職員で確認するようにしてください。

**（４）資料作成等の際に生成 AI から得られた回答を利用した場合は、資料中に明記すること（例：【生成 AI 名】により作成）**

（１）、（２）のとおり、生成 AI の利用にあたっては、根拠や裏付け、権利侵害がないかなどを確認する必要がありますが、業務で利用した際、将来的に、問題がなかったかの確認することが必要になる場面もあり得るため、生成物を加工せずにそのまま利用する場合や一部に引用した場合は、「【生成 AI 名】により作成」と資料中に明記し、利用したチャット内容を記録しておくようにしてください。

## Ⅲ　その他

**（１）問題が発生した場合は、直ちに所属長に報告すること。**

問題が発生した場合は、直ちに所属長に報告し、必要な措置を実施するようにしてください。また、デジタル推進課にも情報を共有するようにしてください。