デジタル社会推進標準ガイドライン DS-920

行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン

2026~~2025~~年（令和８~~７~~年）●5~~5~~月●~~27~~日
デジタル社会推進会議幹
事会決定

〔ドキュメントの位置付け〕
Normative
政府情報システムの整備及び管理に関するルールとして遵守する内容を定めたドキュメント

〔キーワード〕
生成 AI、大規模言語モデル（LLM）、政府における生成 AI の利活用方針、AI ガバナンス体制、生成 AI プロジェクト、高リスクな生成 AI、先進的 AI 利活用アドバイザリーボード、AI 統括責任者（CAIO）、生成 AI の調達・利活用に係るリスク管理（企画、調達、開発・運用、利活用、生成 AI システム特有のリスクケースへの対応）

〔概要〕
生成AIの利活用促進とリスク管理を表裏一体で進めるため、政府における生成 AI のガバナンス、各府省庁における調達・利活用時のルールを定めるガイドライン。

改定履歴

改定年月日	改定箇所	改定内容
2025年5月27日	－	・初版作成
2026年XX月XX日	XX	・第XX版作成

目次

1　はじめに

1.1　背景

AI 関連技術は日々発展し、産業におけるイノベーション創出や社会課題の解決に向けた AI の活用が官民で急速に進展している。

こうした中、令和５年のＧ７（議長国：日本）では、安全、安心で信頼できる AI の実現に向け、「高度な AI システムを開発する組織向けの広島プロセス国際指針」[1]、「高度な AI システムを開発する組織向けの広島プロセス国際行動規範」[2]及び「全ての AI 関係者向けの広島プロセス国際指針」[3]が策定されたほか、国連、欧州評議会、OECD 等の多国間の枠組みにおいても、AI ガバナンスに関する議論が活発に行われている。また、諸外国の政府機関等においても、政府内での適切な AI のガバナンスの確保や、リスク管理を行いながら、積極的に AI の活用を進めるためのルール整備が進むなど、着実に環境整備が進められている。

我が国でも、技術、そして、技術を利活用した社会の変化に迅速かつ柔軟に対応するため、事業者等の自発的な取組を支援するための「AI 事業者ガイドライン（第 1.1 版）」（令和７年３月 28 日　総務省　経済産業省。以下「AI 事業者ガイドライン」という。）[4]や、「人工知能関連技術の研究開発及び活用の推進に関する法律（令和７年法律第 53 号）」[5]、同法に基づく「人工知能基本計画」（令和７年 12 月 23 日閣議決定）[6]及び「人工知能関連技術の研究開発及び活用の適正性確保に関する指針」（令和７年 12 月 19 日 人工知能戦略本部決定。以下「AI 指針」という。）[7]を策定するなど、AI の安全・安心な利活用に向けた取

[1] 高度な AI システムを開発する組織向けの広島プロセス国際指針
https://www.mofa.go.jp/files/100573469.pdf
[2] 高度な AI システムを開発する組織向けの広島プロセス国際行動規範
https://www.mofa.go.jp/files/100573472.pdf
[3] 全ての AI 関係者向けの広島プロセス国際指針
https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document03.pdf
[4] AI 事業者ガイドライン（第 1.1 版）
https://www.soumu.go.jp/main_content/001002576.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf
[5] 人工知能関連技術の研究開発及び活用の推進に関する法律
https://laws.e-gov.go.jp/law/507AC0000000053
[6] 人工知能基本計画
https://www8.cao.go.jp/cstp/ai/ai_plan/aiplan_20251223.pdf
[7] 人工知能関連技術の研究開発及び活用の適正性確保に関する指針

組を進めている。

また、「デジタル社会の実現に向けた重点計画」（令和６年６月 21 日閣議決定）[8]においても、AI に関して、生成 AI を含む AI の様々なリスクを抑え、安全・安心な環境を確保しつつ、イノベーションを加速する好循環の形成を図っていくこととされ、イノベーション推進のためにも、ガードレールとなる AI 利活用の安全・安心を確保するためのルールが必要とされたところである。

さらに、各府省庁では、様々な業務への生成 AI の活用の検討が進められるとともに、デジタル庁においては、行政の課題を AI で解決することを目指した「AI アイデアソン・ハッカソン」や生成 AI システムの各種検証事業等を行いながら、ユースケースの発掘や実用化のための試行環境等を用いた検証が進められ、利活用促進に向けた取組も政府全体で進められているところである。

本ガイドラインは、政府の様々な業務への生成 AI[9]の利活用促進とリスク管理を表裏一体で進めるため、政府における AI ガバナンスやベストプラクティスの共有体制、生成 AI の調達・利活用において留意すべきリスク等についての考え方、政府が利活用する生成 AI 全体の機能性や品質及び費用対効果の向上等について、AI 指針をはじめ、AI 事業者ガイドラインや「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群[10]」等既存のガイドライン及び諸外国政府のルールの動向等を踏まえ整理し、国の政府職員~~等~~向けのガイドラインとして示すものである。

1.2　本ガイドラインの位置付け

本ガイドラインは、デジタル社会推進標準ガイドライン群[11]のうち規範として遵守~~順守~~するドキュメントの一つとして位置付けられる。

~~https://www8.cao.go.jp/cstp/ai/ai_guideline/ai_gl_2025.pdf~~https://www8.cao.go.jp/cstp/ai/ai_guideline/ai_gl_2025.pdf

[8] デジタル社会の実現に向けた重点計画
https://www.digital.go.jp/policies/priority-policy-program

[9] 本ガイドラインで対象とする生成 AI は、原則として入力はテキスト及び音声、出力はテキスト、画像又は音声が可能なもの~~テキスト生成 AI~~とする（詳細は「2.2.2 本ガイドラインが対象とする生成 AI」を参照）。

[10] 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群
https://www.cyber.go.jp/policy/group/general/kijun.html~~https://www.nisc.go.jp/policy/group/general/kijun.html~~

[11] デジタル社会推進標準ガイドライン群
https://www.digital.go.jp/resources/standard_guidelines

1.3　用語

本ガイドラインにおける用語は、表１及び本ガイドラインに別段の定めがある場合を除くほか、標準ガイドライン群用語集の例による。

表　1　用語の定義

用語	意味
AI	「AI システム（以下に定義）」自体又は機械学習をするソフトウェア若しくはプログラムを含む抽象的な概念。 （出典：「AI 事業者ガイドライン」P.9）
生成 AI	文章、画像、プログラム等を生成できる AI モデルに基づく AI の総称。 （出典：「AI 事業者ガイドライン」P.10）
AI システム	活用の過程を通じて様々なレベルの自律性をもって動作し学習する機能を有するソフトウェアを要素として含むシステム（機械、ロボット、クラウドシステム等）。 （出典：「AI 事業者ガイドライン」P.9）
生成 AI システム	生成 AI を構成要素とする AI システム。（「AI 事業者ガイドライン」P.9、P.10 に基づき作成）~~本ガイドラインが対象とする生成AIを構成要素とする政府情報システム[12]。~~ ~~（AISI「AI セーフティに関する評価観点ガイド（第1.01版）」P.9に基づき作成）[13]~~
AI モデル	AI システムに含まれ、学習データを用いた機械学習によって得られる、入力データに応じた予測結果を生成するモデル。 （「AI 事業者ガイドライン」P.10 に基づき作成）
生成 AI モデル	文章、画像、プログラム等を生成できる AI モデル。（「AI 事業者ガイドライン」P.10 に基づき作成）
大規模言語モデル（LLM）	文章や単語の出現確率を深層学習モデルとして扱う言語モデルを、非常に大量の訓練データを用いて構築したもの。

~~[12] 政府情報システムの形態は、クラウド又はオンプレミスの形態を問わない。~~
~~[13] AI セーフティに関する評価観点ガイド（第 1.01 版）~~
~~https://aisi.go.jp/assets/pdf/ai_safety_eval_v1.01_ja.pdf~~

用語	意味
	（出典：AIプロダクト品質保証コンソーシアム「AIプロダクト品質保証ガイドライン　2025.04版」P.10-1）[14]
AIガバナンス	AIの利活用によって生じるリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる正のインパクト（便益）を最大化することを目的とする、ステークホルダーによる技術的、組織的、及び社会的システムの設計並びに運用。 （出典：「AI事業者ガイドライン」P.10）
生成AIシステム特有のリスクケース	生成AIシステムの特有のリスクが顕在化した状態又はその可能性を有する兆候や事象が認められる状態のうち、重大な影響を及ぼし得るもの。 （詳細は、「6.7　生成AIシステム特有のリスクケースへの対応」参照）

2　本ガイドラインの目的及び適用対象

2.1　本ガイドラインの目的

~~本ガイドラインは、政府における生成AIの調達・利活用において、~~我が国が平成31年３月に策定した「人間中心のAI社会原則」においては、３つの「基本理念」（「①人間の尊厳が尊重される社会（Dignity）」「②多様な背景を持つ人々が多様な幸せを追求できる社会（Diversity and Inclusion）」「③持続可能な社会（Sustainability）」）が掲げられており、AI指針においては、国が特に取り組むべき事項として、「①AIの積極的かつ先導的な活用によるイノベーションの促進」、「②社会全体におけるAIリテラシーの向上」、「③AIガバナンスの在り方の検討」及び「④行政としてのアカウンタビリティを果たすこと」が定められている。

本ガイドラインは、「人間中心のAI社会原則」の「基本理念」の実現を目指し、AI指針における~~の~~国が特に取り組むべき事項を踏まえた、政府における生成AIの利活用促進のためのガードレールであり、~~本ガイドラインによって、~~政府による生成AIの安心・安全な利活用~~が~~を着実に進展~~し~~させ、以下のような利益を実現することを目指す。

1.　行政目的の効率的・効果的な実現

[14] AIプロダクト品質保証ガイドライン2025.04版
https://www.qa4ai.jp/download/

2. 企画立案能力の向上
3. 情報収集・分析能力の向上
4. 政府が作り出す政策・文書・分析等の質の向上
5. 既存政府情報システムの生成 AI を用いた機能や利便性向上
6. 政府が利活用する生成 AI 全体の機能性や品質及び費用対効果の向上
7. 我が国の AI 分野における国際競争力の向上及び産業の育成
8. AI の安全性の向上及び国際的な相互運用性の確保
9. 政府におけるデータガバナンスの強化

2.2 対象範囲

2.2.1 本ガイドラインが対象とする情報システム

本ガイドラインは、政府情報システムのうち「2.2.2 本ガイドラインが対象とする生成 AI」に記載した生成 AI を構成要素とするシステムに適用するものとする。ただし、特定秘密（特定秘密の保護に関する法律（平成 25 年法律第 108 号）第３条第１項に規定する特定秘密をいう。）、重要経済安保情報（重要経済安保情報の保護及び活用に関する法律（令和６年法律第 27 号）第３条第１項に規定する重要経済安保情報をいう。）又は行政文書の管理に関するガイドライン（内閣総理大臣決定。平成 23 年４月１日）に掲げる秘密文書としての取扱いを要する情報を扱う政府情報システムについては、本ガイドラインの全部を適用対象外とする。また、安全保障、公共の安全・秩序の維持といった機微な情報及び当該情報になり得る情報を扱う政府情報システムについても、本ガイドラインの全部を適用対象外とする。

なお、独立行政法人及び指定法人[15]においても、生成 AI の調達・利活用に当たって、本ガイドラインに準拠した取組を期待する。さらに、地方公共団体においても、必要に応じ、参考とされることを期待する。

2.2.2 本ガイドラインが対象とする生成 AI

本ガイドラインが対象とする生成 AI は、原則として、入力はテキスト及び音声、出力はテキスト、画像又は音声が可能なもの~~大規模言語モデル（LLM）を~~

[15] サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 13 条に規定する「指定法人」を指す。

~~構成要素とするテキスト生成 AI~~[16]とする~~（テキスト及び画像を生成する AI 等については、テキストの生成について対象とする。）~~。

これらを構成要素とする生成 AI システムであって、画像や動画等を入力するもの、~~なお、画像や~~動画等を生成する~~AI~~ もの、より高度なタスクを実行できる~~AI~~ もの（AI エージェント等）~~、その他の AI~~ 等については、政府における利活用状況に鑑み具体的対応事項は定めないが、AI ガバナンスの枠組みの対象とすることとし、具体的には、「4.1　政府全体の AI の利活用促進と AI ガバナンスのための体制構築」及び「4.2　各府省庁における AI ガバナンス体制の整備」並びに「6.7　生成 AI システム特有のリスクケースへの対応」の対象とすることとする（以降、「生成 AI モデル」の語は、本ガイドラインが対象とする生成 AI を構成要素とする生成 AI モデルを、「生成 AI システム」の語は、本ガイドラインが対象とする生成 AI モデルを構成要素とする生成 AI システムを指すものとする。）。

これらを含むその他の AI については、政府等における今後の利活用状況、国内外のルールの整備状況等を踏まえ、必要に応じ、本ガイドラインの~~適用範囲等の~~拡充を検討することとする[17]。

2.2.3　本ガイドラインの対象者

本ガイドラインの対象者は、生成 AI の調達・利活用に関わる政府職員としており、具体的に読者として想定される政府職員の種別は、表２のとおりである。

表　２　本ガイドラインの対象となる政府職員の種別[18]

種別	説明	具体的な政府職員の例
AI 統括責任者	各府省庁における行政の進化と革	「デジタル統括責

[16] ~~本ガイドラインで対象としていないテキスト生成 AI 以外の AI システム・サービスの利用については、AI 事業者ガイドライン（テキスト生成 AI 以外も含む AI 全般を対象）や、本ガイドライン（本ガイドラインがテキスト生成 AI を念頭に記載されていることに留意）も参考にした上で、各府省庁において適切なリスク対応等を実施し、利活用を進めることが望ましい。~~

[17] 本ガイドラインで対象としていない AI システム・サービスの利用については、本ガイドライン（本ガイドラインが生成 AI を念頭に記載されていることに留意）や AI 事業者ガイドライン（AI 全般を対象）等も参考にした上で、各府省庁において適切なリスク対応等を実施し、利活用を進めることが望ましい。

[18] 例えば、共通機能としてデジタル庁が提供するシステムについては、企画者・提供者や利用者が共通機能を提供するデジタル庁と各府省庁にまたがる可能性なども想

種別	説明	具体的な政府職員の例
（CAIO：Chief AI Officer）	新のための生成AI利活用方針を策定・推進し、組織全体の利活用状況とリスク管理等を統括管理する者	任者」又は「副デジタル統括責任者」級の職員
企画者	新たな生成AIの利活用を企画し、業務が生成AIシステムに要求するものを定義し、調達・開発・利活用を推進する者	生成AIの業務における活用を企画・調達する部署・チーム等の政府職員（生成AIシステムに係る業務を所管する部署の政府職員、生成AIシステムを企画・調達する部署の政府職員、PJMO職員等）
開発者	企画に基づき、生成AIモデル・アルゴリズムの開発、データ収集（購入を含む）、前処理、AIモデル学習及び検証を通して生成AIモデル、生成AIモデルのシステム基盤、入出力機能を含む生成AIシステムを構築する者	（開発を内製する場合）左記の生成AIシステムの構築を行う政府職員（PJMO職員等）
提供者	生成AIモデルをアプリケーションや製品~~もしくは~~若しくは既存のシステムや行政の利活用プロセス等に組み込んだサービスとして政府又は国民に提供する者	政府職員又は国民が利活用する生成AIシステムを運営する政府職員（PJMO職員等）
利用者[19]	行政において、生成AIシステムを利活用する者	一般事務や各行政分野において生成AIシステムを利活用する政府職員

定されるが、この場合は、責任分界を明確にした上で、各主体で連携の上、リスク対応等を実施する必要がある。

[19] 利用者は、本ガイドラインの直接の対象者ではないが、本ガイドラインを踏まえて、AI統括責任者（CAIO）によって策定された生成AIの利活用に係るルール及び企画者によって策定された各生成AIシステムにおける利活用ルールを遵守することが求められる（詳細は「6.6　政府における生成AIシステムの利用者の対応事項」参照）。

表 3　本ガイドラインと AI 事業者ガイドラインとの対応関係[20]

本ガイドライン	AI 事業者ガイドライン
AI 統括責任者（CAIO）	経営者を含む事業執行責任者
企画者	AI 開発者又は AI 提供者
開発者	AI 開発者
提供者	AI 提供者
利用者	AI 利用者

※　政府との契約により政府に生成 AI システムを提供等する事業者は本ガイドラインの直接の対象ではなく、上記政府職員である企画者や提供者が調達手続や当該事業者との契約、契約事業者の監督、あるいは生成 AI システム提供事業者との協力を通じて本ガイドラインの遵守~~順守~~や本ガイドラインに基づく取組を確保することとする。

~~2.2.4　本ガイドラインの適用開始時期等について~~

~~本ガイドラインの政府情報システムへの全面適用は、令和８年度以降に調達・利活用を行う生成 AI システムからである（令和８年度事業の令和８年３月末以前の企画や公告等調達手続きを含む）が、令和７年度に調達・利活用を行う生成 AI システムについても、可能な限り本ガイドラインに沿った取組を実施する。~~

~~生成 AI の利活用が、各府省庁で進んでいることも踏まえ、「４　AI の利活用促進と AI ガバナンスの強化及び推進のための体制構築」の取組についても、令和７年度から進めることとする。~~

~~なお、本ガイドラインは、「ChatGPT 等の生成 AI の業務利用に関する申合せ（第２．１版）」による政府における生成 AI の適切な把握等について、リスク管理や利活用の促進と合わせて促進する観点から、その在り方を更に進化させた上で統合したものである。今後は、同申合せに代わり、本ガイドラインを適用し、取組を進める。~~

[20] 政府向けである本ガイドラインと主に民間事業者を対象とした AI 事業者ガイドラインでは、対応関係は一致しない場合がある。

３　政府における生成AIの利活用方針

3.1　政府における生成 AI の利活用方針

生成 AI の政府での利活用は、情報漏えいや不適切な表現の生成などのリスクを伴う一方、様々な事務作業や事務手続の効率化・高度化を実現し、働き方改革や国民サービスの向上等行政の進化と革新を飛躍的に進める可能性がある。加えて、今後、社会全体での安全・安心な AI の活用の推進や日本の AI 分野における国際競争力の向上を実現するためにも、政府において率先して AI の利活用に取り組むことは、極めて重要である。

このため、各府省庁は、生成 AI について、以下に取り組みつつ、積極的に業務での活用を検討することとする。

① 各府省庁は、AI 統括責任者（CAIO）の設置等 AI システム統括監理の体制整備を行うなど、AI ガバナンスの強化に取り組むこと。
⇒「４　AI の利活用促進と AI ガバナンスの強化及び推進のための体制構築」を参照。
② 各府省庁の生成 AI の調達・利活用を行う全ての者は、生成 AI の便益とリスクについて理解すること。
⇒「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。
③ 各府省庁の生成 AI 調達・利活用を行う者は、生成 AI のリスクを軽減するための方策を把握し、それぞれが適切なリスク対策を実施するとともに、生成 AI システムの品質向上や利用方法の工夫による利用効果の増進を図ること。
⇒「６　政府における生成 AI の調達・利活用に係るルール」を参照。

その際、生成 AI の活用を政府全体で着実に進めるため、各府省庁は、内部管理系の業務等リスクが低いと考えられる生成 AI の利活用について、スピード感を持って実装を進める。

また、相対的に高リスクである可能性がある生成 AI の利活用（後述の「3.2 高リスクな生成 AI 利活用の考え方」を参照）であっても、行政の進化や革新をもたらす取組については、適切なリスク対応を行った上で、可能な限り安全かつ効果的な AI プロジェクトとして実施していけるよう、その取組を後押しする。

このため、各府省庁は、行政の進化と革新につながるような生成 AI の利活用を積極的に推進するとともに、当該利活用ケースにあわせたリスク評価を行い、高リスクの可能性がある生成 AI の利活用について、当該プロジェクトの内容、リスク軽減策や運用時を含めた品質確保策等を、「先進的 AI 利活用アドバイザ

リーボード」に報告することとする。「先進的 AI 利活用アドバイザリーボード」は、内外の政府 AI 利活用のベストプラクティス、ルール整備及び生成 AI システムの評価手法の確立等の状況を踏まえた、助言を行うこととする。

さらに、各府省庁は、行政の進化と革新につながるような利用方法の発掘や、各府省庁において利活用する生成 AI 全体の機能性や品質及び費用対効果の向上に努め、必要に応じこれらについて上記「先進的 AI 利活用アドバイザリーボード」の機能や、後述する「AI 相談窓口」の機能を有効活用することとする。

3.2　高リスクな生成 AI 利活用の考え方

各府省庁の AI 統括責任者（CAIO）は、企画者と連携しつつ、利活用ケースにあわせたリスク評価を行い、そのリスクレベル（高リスクの可能性が高いか否か）を適切に判断する。

各府省庁の AI 統括責任者（CAIO）は、企画者と連携しつつ、リスクレベルを判断するにあたり「【別紙１】高リスク判定シート」（以下、「高リスク判定シート」という。）[21]~~を踏まえたうえ~~も参考にした上で、最終判断すること。「高リスク判定シート」は、表４に示すリスク軸に沿ってリスクレベル案を示すものである。

高リスクに該当する可能性が高いと判断した場合には、先進的 AI 利活用アドバイザリーボードに報告を行うこと（※高リスクに該当する可能性が高いと判断しない場合であっても、必要に応じて、デジタル庁又は先進的 AI 利活用アドバイザリーボードに別途相談可能）。

表　４　リスク軸とその考え方

リスク軸	説明	観点
~~B~~A. 生成 AI 利活用業務の性格	~~過失~~生成 AI による生成物の瑕疵（生成 AI が提供する情報の誤り等）が重大な影響を及ぼす可能性のある業務（国民の基本的権利や安全に大きな影響を及ぼす業務、機微な政策分野に関する業務、人間の生命・身体・財産に影響を及ぼす又は法人の事業に重大な影響を及ぼす業	① ~~過失~~生成 AI による生成物の瑕疵が重大な影響を及ぼす可能性のある業務において利活用する ② ~~過失~~生成 AI による生成物の瑕疵が

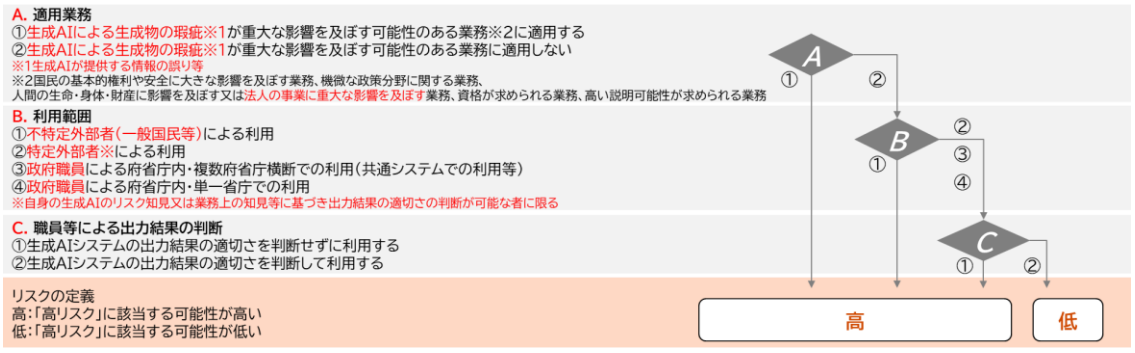
[21] 「高リスク判定シート」は、表４で示した３つのリスク軸に係る設問について、回答するだけで「高リスクに該当する可能性が高い」か「高リスクに該当する可能性が低い」かを簡易的に判定するツール。

リスク軸	説明	観点
	務、資格が求められる業務、高い説明可能性が求められる業務等）において生成 AI を利活用する場合、リスクが高くなると考えられる。	重大な影響を及ぼす可能性のある業務において利活用しない
~~A~~B. 利用者の範囲・種別	~~調達・利活用する~~生成 AI システムの利用者の範囲によってリスクの大きさや影響を与える範囲の大きさが異なる。特に不特定外部者（一般国民等）が利活用する~~国民等が用いるような形で府省庁外で利活用する~~サービスは、政府職員~~等~~による府省庁内での利活用に比べリスクが高いと考えられる。また、政府職員や、外部利用者でも特定の者（地方公共団体や民間企業等）が~~利用される場合などは~~、自身の生成 AI のリスク知見又は業務上の知見等に基づき出力結果の適切さの判断が可能と考えられる~~ことから~~場合については、必ずしも~~府省庁内利用であっても、複数府省庁横断で利活用する場合などはリスクが顕在化した際の影響範囲が大きくなるため、この点を考慮することが必要となる~~リスクが高いものではないと考えられる。	① 不特定外部者（一般国民等）による利用~~国民等による府省庁外利用~~ ② 特定外部者※による利用 ③~~②~~ 政府職員~~等~~による府省庁内・複数府省庁横断での利活用（府省庁共通システムでの利活用等） ④~~③~~ 政府職員~~等~~による府省庁内・単一府省庁での利活用 ※自身の生成 AI のリスク知見又は業務上の知見等に基づき出力結果の適切さの判断が可能な者に限る
~~C. 要機密情報や個人情報の学習等の有無~~	~~生成 AI の利活用においては、学習データやプロンプトに入力するデータに関するリスクが存在する。学習データやプロンプトに入力するデータに要機密情報や個人情報が含まれる場合、リスクが高くなると考えられる。~~	~~① 機密性２情報又は個人情報が生成 AI システムに保存または学習される~~ ~~② 機密性２情報又は個人情報を取り扱うが生成 AI システムに保存及び学習されない~~

リスク軸	説明	観点
		~~③ 機密性２情報又は個人情報を取扱わない~~
~~D~~C. 出力結果の政府職員等による判断を経た利活用	生成 AI の出力結果は必ずしも正しいものとは限らない。そのため、生成 AI システムの出力結果に対して政府職員等が判断せずそのまま利活用するような業務設計をする場合、リスクが高くなると考えられる。	① 生成 AI システムの出力結果の適切さを政府職員等が判断せずに利活用する ② 生成 AI システムの出力結果の適切さを政府職員等が判断して利活用する

なお、「高リスク判定シート」は、回答結果を踏まえ、以下のフローに基づき、高リスクの判定が行われるよう、設定されている（「図 ３　リスク判定ロジック」参照）。

図 ３　リスク判定ロジック



※　~~高~~リスク~~に該当する可能性の高いケース~~判定の例

実際には、~~以下に高リスクに該当する可能性の高いケースを例示する。~~必ずしも表４の~~単一の~~リスク軸~~のみ~~を形式的に適用するに止まらず~~で評価されるものでなく~~、業務生成 AI の具体的な利用の在り方（例：C②の前提として、生成内容の出典が容易に参照可能となっている）等も合わせ、~~て「高リスク判定シ~~

~~ート」に示されるような形で複合~~総合的にリスクレベルを判断~~（後述の「「高リスク判定シート」の見方」も参照）~~することが重要である。

- （例１）生成 AI による生成物の誤りにより、行政手続の結果に影響を与え、法人の事業活動の停止などの大きな影響を与えるような場合（A①→高リスクの可能性あり）
- （例２）サイトに登録した個人が、自らのニーズにマッチした行政サービス等について、生成 AI の検索要約サービスにより対象を絞った上で、具体的な手続ページに誘導されるもの（A②→B②→C②→低リスク）
- （例３）相手のメール内容に応じた返信メールを作成し、政府職員等による確認を経ずに、自動的に返信するもの（A②→B④→C①→高リスク）

~~※「高リスク判定シート」の見方~~

~~「高リスク判定シート」は、上記の４つのリスク軸に係る設問について、回答するだけで「高リスクに該当する可能性が高い」か「高リスクに該当する可能性が低い」かを簡易的に判定するツール（「図　１　【回答前】高リスク判定チェックリスト」、「図　２　【回答後】高リスク判定チェックリスト」参照）。~~

~~図　１　【回答前】高リスク判定チェックリスト~~

記入日	
所属（府省庁/課室等）	
システム名	
記入者名	

リスク判定結果	回答欄を記載ください

■高リスク判定チェックリスト
以下のチェック内容を確認し、企画時点の想定で回答欄を記載ください

観点	チェック内容	選択肢	回答	コメント※自由記述
~~A. 利用者の範囲・種別~~	~~利用範囲は次のいずれでしょうか？~~	①国民等による府省庁外利用 ②政府職員等による府省庁内・複数府省庁横断での利用（共通システムでの利活用等） ③政府職員等による府省庁内・単一府省庁での利活用 ④企画時点で未定		
B. 生成AI利活用業務の性格	利活用業務は次のいずれでしょうか？	①過失が重大な影響を及ぼす可能性のある業務*において利活用する ②過失が重大な影響を及ぼす可能性のある業務において利活用しない ③企画時点で未定 *国民の基本的権利や安全に大きな影響を及ぼす業務、機微な政策分野に関する業務、人間の生命・身体・財産に影響を及ぼす業務、資格が求められる業務、高い説明可能性が求められる業務等		
C. 要機密情報や個人情報の学習等の有無	データおよびその取り扱いは次のいずれでしょうか？	①機密性2情報または個人情報が生成AIシステムに保存または学習される ②機密性2情報または個人情報を取り扱うが生成AIシステムに保存および学習されない ③機密性2情報および個人情報を取扱わない ④企画時点で未定		
D. 出力結果の政府職員による判断を経た利活用	出力結果の利活用に係る運用は次のいずれでしょうか？	①生成AIシステムの出力結果の適切さを判断せずに利活用する ②生成AIシステムの出力結果の適切さを判断して利活用する ③企画時点で未定		

~~図　２　【回答後】高リスク判定チェックリスト~~

記入日	YYYY/MM/DD
所属（府省庁/課室等）	○○庁○○課
システム名	○○○○○○○○
記入者名	○○○○　○○○○

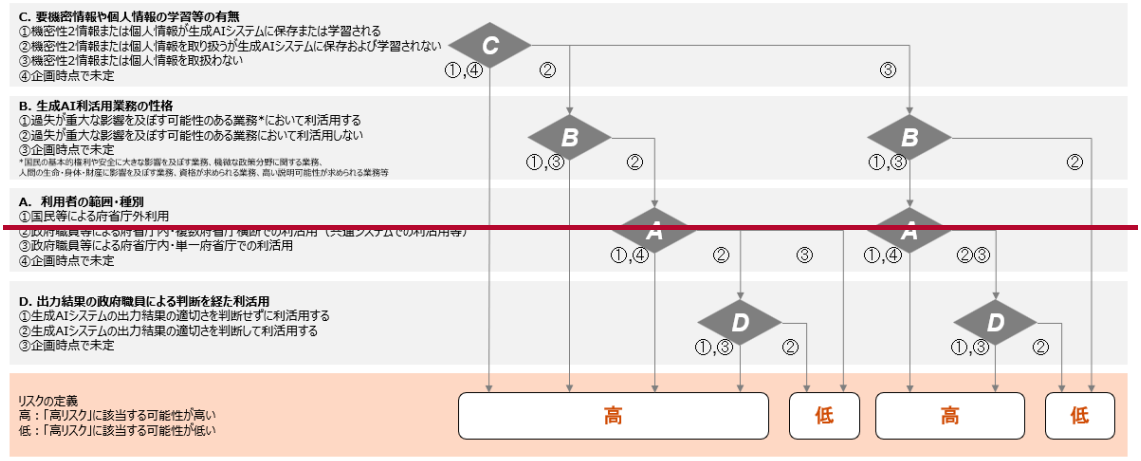
リスク判定結果	高リスクに該当する可能性が低い

■高リスク判定チェックリスト
以下のチェック内容を確認し、企画時点の想定で回答欄を記載ください

観点	チェック内容	選択肢	回答	コメント※自由記述
~~A. 利用者の範囲・種別~~	~~利用範囲は次のいずれでしょうか？~~	①国民等による府省庁外利用 ②政府職員等による府省庁内・複数府省庁横断での利用（共通システムでの利活用等） ③政府職員等による府省庁内・単一府省庁での利活用 ④企画時点で未定	③	○○○○○○○○
B. 生成AI利活用業務の性格	利活用業務は次のいずれでしょうか？	①過失が重大な影響を及ぼす可能性のある業務*において利活用する ②過失が重大な影響を及ぼす可能性のある業務において利活用しない ③企画時点で未定 *国民の基本的権利や安全に大きな影響を及ぼす業務、機微な政策分野に関する業務、人間の生命・身体・財産に影響を及ぼす業務、資格が求められる業務、高い説明可能性が求められる業務等	②	○○○○○○○○
C. 要機密情報や個人情報の学習等の有無	データおよびその取り扱いは次のいずれでしょうか？	①機密性2情報または個人情報が生成AIシステムに保存または学習される ②機密性2情報または個人情報を取り扱うが生成AIシステムに保存および学習されない ③機密性2情報および個人情報を取扱わない ④企画時点で未定	②	○○○○○○○○
D. 出力結果の政府職員による判断を経た利活用	出力結果の利活用に係る運用は次のいずれでしょうか？	①生成AIシステムの出力結果の適切さを判断せずに利活用する ②生成AIシステムの出力結果の適切さを判断して利活用する ③企画時点で未定	②	○○○○○○○○

~~なお、「高リスク判定シート」は、回答結果を踏まえ、以下のフローに基づき、高リスクの判定が行われるよう、設定されている（「図　リスク判定ロジック」参照）。~~

~~図　リスク判定ロジック~~



4　AIの利活用促進とAIガバナンスの強化及び推進のための体制構築

4.1　政府全体の AI の利活用促進と AI ガバナンスのための体制構築

4.1.1　先進的 AI 利活用アドバイザリーボードの開催・AI 相談窓口の運用等

政府横断で効果的・安全な生成 AI プロジェクトの推進を行うため、AI の制度、利活用、リスク管理、サイバーセキュリティ等に高度な知見を有する有識者（民間有識者と政府職員の双方を含み得る）等からなる「先進的AI利活用アドバイザリーボード」を開催し、デジタル庁が事務局機能を担うこととする。

「先進的AI利活用アドバイザリーボード」は、デジタル庁の他、AISI（AIセーフティ・インスティテュート）がアドバイザリーボードの構成員や事務局機能への参画を通じその知見や機能を生かした役割を果たすことによる効果的運営を行う。

「先進的 AI 利活用アドバイザリーボード」は、以下の役割を担う。

- 各府省庁における生成 AI の調達・利活用状況の把握
- 各府省庁の高リスクに該当する可能性の高い生成 AI の調達・利活用に係る評価及びリスク緩和のための助言
- 各府省庁における生成 AI の調達・利活用のベストプラクティスの把握・発信
- 各府省庁で発生した生成 AI システム特有のリスクケースの把握、再発防止のための助言
- 各府省庁における生成 AI の効果的な利活用や、生成 AI システムの機能性や品質及び費用対効果の向上のための助言（AI 利活用について高度な知見や豊富な経験を有する有識者や政府職員のリスト化や紹介の機能を含む。）
- 本ガイドラインの見直しの検討

先進的 AI 利活用アドバイザリーボードは、政府全体の生成 AI 施策の動向やガイドラインの運用状況を踏まえ、関係府省庁等と連携を行いつつガイドラインの見直しを行う。また、デジタル庁は、関係府省庁連絡会議として、「各府省庁 AI 統括責任者（CAIO）連絡会」を開催し、先進的 AI 利活用アドバイザリーボードでの議論等について紹介するとともに、各府省庁における生成 AI の利活用状況や~~各府省庁における~~ガバナンスの状況、生成 AI システムに関する注意喚起等の必要な情報提供を行うこととする。

あわせて、デジタル庁は、各府省庁からの生成AIの調達・利活用や本ガイドラインの運用に関する質問・相談を受け付けることとし、「AI 相談窓口」として運用を行う。

「AI 相談窓口」は、以下のような各府省庁の相談を受け付け、技術的・専門的観点から、機動的に各府省庁による生成 AI の効果的な利活用を実現するために必要な支援・助言を行う。

- ガイドラインの内容に関する問合せ
- 生成AIを活用した行政事務の効率化・行政サービスの高度化等の手法や技術的側面に係る相談
- 高リスクな生成AIに該当するか判断に迷う事案についての相談
- その他、リスク軽減に関して生成AIシステムの企画や調達上留意すべき点についての相談

さらに、デジタル庁の AI 有識者/担当職員等が、デジタル庁が各府省庁に派遣している専門人材とも連携して、各府省庁のプロジェクトにおける生成AI利活用について必要に応じて支援する体制も整えていく。

4.1.2 デジタル庁の統括監理におけるチェック

デジタル庁は、デジタル庁設置法（令和３年法律第36号）第４条第２項第17号に基づく国の情報システムの整備・管理に関する事業の統括監理（一元的なプロジェクト監理）の一環として、各府省庁における生成AIシステムの導入予定、生成AIシステムのリスク対応の状況等について確認を行うとともに、その状況を「先進的AI利活用アドバイザリーボード」に共有する。

4.2 各府省庁における AI ガバナンス体制の整備

4.2.1 各府省庁における AI 統括責任者（CAIO）の設置

各府省庁において生成AIシステム調達契約のチェックを本ガイドラインに基づき行うことを含め、生成 AI システムのライフサイクルを通じた生成 AI システム統括監理の体制整備等を行う。

具体的には、各府省庁は、AI 統括責任者（CAIO）を設置し、各府省庁における、生成AIシステムの企画、行政データの取扱い、調達、利活用、運用、生成 AI システム特有のリスクケース等の状況を一元的に把握し、生成 AI の適切な調達・利活用に係る取組を行う。

AI 統括責任者（CAIO）は、各府省庁における生成 AI の利活用を各府省庁の

業務において積極的に進めるとともに、各府省庁における AI ガバナンスの構築及び実践の司令塔として、生成 AI システム把握、適切なリスク管理の徹底、生成 AI システム特有のリスクケース対応、政府職員の AI リテラシー向上に向けた研修、アドバイザリーボードへの報告の要否の決定等を行う。

AI 統括責任者（CAIO）は、当該組織における総合的・計画的な行政デジタル化の推進を統括する責任者であるデジタル統括責任者の役割のうち、AI 分野に係る役割を担う。このため、AI 統括責任者（CAIO）は、各府省庁における「デジタル統括責任者」又はデジタル統括責任者の業務を補佐する「副デジタル統括責任者」級の政府職員が想定される[22]。

4.2.2　先進的 AI 利活用アドバイザリーボードへの報告

各府省庁の AI 統括責任者（CAIO）は、随時各府省庁内における生成 AI システムの運営状況及び~~行政における生成 AI の~~利活用の状況を一覧的にとりまとめ、その状況を定期的に（四半期に一度程度の頻度を目安とする）「先進的 AI 利活用アドバイザリーボード」へ報告を行うこととする。

また、各府省庁の AI 統括責任者（CAIO）は、企画者と連携しつつ、「３ 政府における生成 AI の利活用方針」のとおり、生成 AI の利活用プロジェクトの企画時において、適切なリスク評価を行い、高リスクの可能性がある生成 AI については、当該プロジェクトの内容・目的、リスク軽減策や運用時を含めた品質確保策等を先進的 AI 利活用アドバイザリーボードへ報告する。

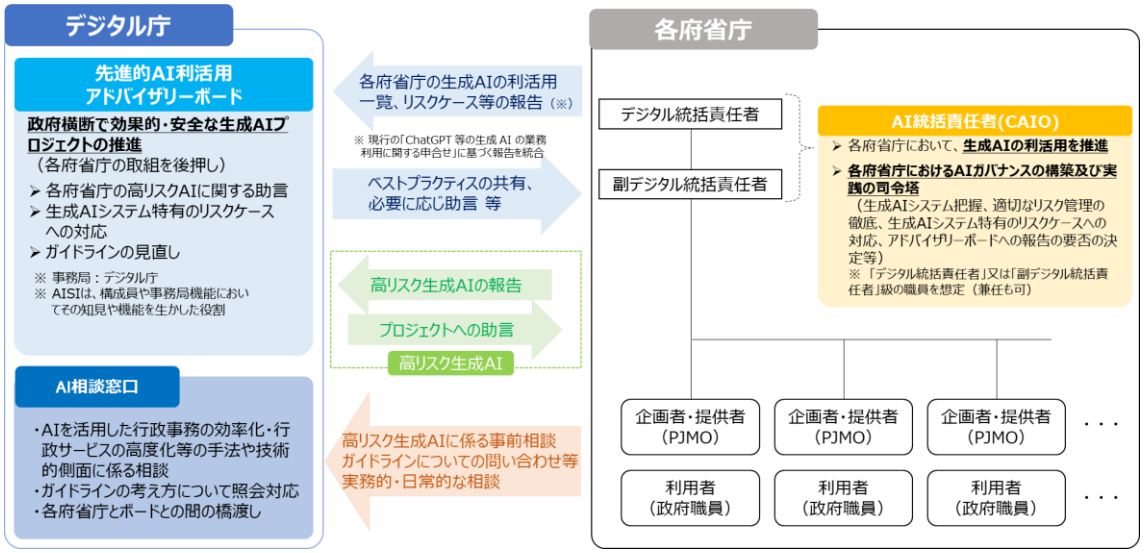
また、プロジェクトの企画時に限らず、構築時、リリース時、運用開始後も含め、事情変化等により高リスクに該当する可能性が生じた場合や、企画時には生成 AI の利活用を認識しておらず、リリース時や構築後に生成 AI の利活用を認識し、かつ、高リスクに該当する可能性が生じた場合にも、先進的 AI 利活用アドバイザリーボードへ報告を行うこととする。

なお、生成 AI の利活用が高リスクに該当するか否かについては、各府省庁においてリスク評価の結果を踏まえて判断（AI 統括責任者（CAIO）が最終決定）することとするが、「先進的 AI 利活用アドバイザリーボード」から求めがあった場合は、各府省庁は当該プロジェクトについて、必要な報告を行うこととする（「図　４　政府の AI 調達・利活用に係るガバナンス体制の概要」参

[22] AI 統括責任者（CAIO）は、各府省庁の「デジタル統括責任者」又は「副デジタル統括責任者」が兼任することも可能。

照）。[23]

図　4　政府の AI 調達・利活用に係るガバナンス体制の概要



[23] リスク判定に情報セキュリティが関わることが想定される場合においては、適宜最高情報セキュリティ責任者（CISO）と連携して協議を行った上で、高リスクかどうかの判断を行う。

５　生成AIによる便益とリスクを理解した利活用推進

5.1　生成 AI の便益

AI 事業者ガイドラインでは、AI の活用による便益~~として~~について、以下のとおり、示されている。

> AI の活用による便益は多岐にわたっており、技術の進展に伴い拡大し続けている。
> AI は各主体において価値を創造するために活用することができる。その結果として以下のことが期待できる。
> - 運営コストの削減
> - 既存事業のイノベーションを加速させる新製品・サービスの創出
> - 組織の変革
>
> さらに、様々な分野（農業、教育、医療、製造、輸送~~、~~等）への応用及び様々な展開モデル（クラウドサービス、オンプレミスシステム、サイバーフィジカルシステム~~、~~等）の活用が考えられる。

政府においても、生成 AI の利活用により、~~表５のような~~このような便益が期待され、こうした便益は、生成 AI の急速な進歩に伴い、更なる拡大が期待される。

各府省庁においては、こうした生成 AI の便益を理解し、今後、積極的に業務への活用を進めていく必要がある。

あわせて、政府での利活用を加速するため、デジタル庁において、各府省庁と連携しながら、実際の業務への活用のユースケースを想定した技術検証や「AI アイデアソン・ハッカソン」等を通じたユースケースの創出にも積極的に取り組む。

~~表　５　政府による生成 AI 利活用により期待される便益の例~~

~~生成 AI 導入目的~~	~~便益の例~~
~~行政目的の効率的・効果的な実現~~	~~指定した内容の文案を作成する目的で活用するケース。生成 AI が生成した文章をもとに、必要に応じて微調整・修正を行うだけで、短時間であいさつ文・メールの作成、文章の要点の作成ができる。~~
	~~複雑で長い文章の要点を短時間で把握する目的で活用するケース（議事録の要約など）。複雑な内容や長い文章でも瞬時に要約できるので、短時間で文章の要点を把握~~

生成 AI 導入目的	便益の例
	できる。
	日本語の文章を英語に翻訳する目的で活用するケース。翻訳にかかる時間が短縮され、再度日本語に翻訳することで正しいかの確認も一定レベルで行うことができる。
企画立案能力の向上	アイデア出しを目的で活用するケース。生成 AI が提示した企画案から、内容を深堀していく方法により、効率的に企画書作成ができる。指定したテーマに関して、新たな気づきや考えの整理ができるので、より企画のイメージがしやすくなる。
情報収集・分析能力の向上	過去事例などの府省庁内の文書調査の目的で活用するケース。作業工数を削減できることで期限超過することなく、問合せ回答が可能となる。
政府が作り出す政策・文書・分析等の質の向上	政府が開催するイベント情報を SNS 向けの記事にする目的で活用するケース。複数の記事のアイデアの提案から、それぞれの良さを取り入れて、より洗練された記事を作成することができる。
	周囲に相談する前に、作成した文章の評価・分析をする目的で活用するケース。上司から指摘される前に一次的に生成 AI による文章確認を行うことができ、報告書の質を高めるための有益なフィードバックを得ることができる。
	提出された報告書について、実効性の観点から課題・対策案を検討する目的で活用するケース。生成 AI による指摘や対策案が具体的かつ多角的で、報告書の質を高めるための有益なフィードバックを得ることができる。
既存政府情報システムの生成 AI を用いた機能や利便性向上	問合せの分類・検索業務において、生成 AI を活用することにより、既存政府情報システムの分類・検索精度の向上が見込める。

5.2 生成 AI によるリスク

AI 事業者ガイドラインでは、一般的な AI のリスクとして、として、以下技

術的リスクや社会的リスク等が例示されているところである。

表 6 AI 事業者ガイドラインにおけるリスクの例

リスクの分類案		AI によるリスク事例とその概要
技術的リスク[24]	学習及び入力段階のリスク	**データ汚染攻撃等の AI システムへの攻撃** 学習データへの不正データ混入、アプリケーション自体を狙ったサイバー攻撃、プロンプトを通した攻撃等のリスクにより、AI の出力が意図的に操作され、悪影響が生じる。
	出力段階のリスク	**バイアスのある出力、差別的出力、一貫性のない出力等** 学習データの偏り等により AI が差別を助長する。
		ハルシネーション等による誤った出力 生成 AI が事実と異なることをもっともらしく回答する。
	事後対応段階のリスク	**ブラックボックス化、判断に関する説明の不足** AI の判断のブラックボックス化により、有事の説明責任を果たせなくなる。また、複雑な機構を持つ AI システムの場合、メンテナンスやトラブルシューティングの難易度が上がる場合がある。
社会的リスク[25]	倫理・法に関するリスク	**個人情報の不適切な取扱い** 適切な同意取得がなく、透明性を欠く個人情報の利用が行われる。
		生命等に関わる事故の発生 自動運転等において、AI の誤動作による大規模な事故リスクが発生する懸念がある。生成 AI で機械等のプログラムコードを生成するケースでは、誤った/非効率なコードによって、パフォーマンスの低下や事故等につながる懸念がある。
		トリアージにおける差別 AI が優先順位を決定する際にバイアスを持つことで、公平性の喪失等が生じる可能性がある。医療場面においては、生命に対する脅威が発生する可能性がある。
		過度な依存 人材採用活動等、重要な意思決定における AI への過度な依存により、企業が説明責任を問われたり批判を受けたりす

[24] 主に AI システム特有のもの。
[25] 既存のリスクが AI においても発生又は AI によって増幅するもの。

リスクの分類案		AIによるリスク事例とその概要
		る懸念がある。また、生成AIを用いたチャットボットとの会話により、利用者が精神的依存状態になる事例も報告されている。
		悪用 詐欺目的でAIが利用される懸念がある。
	経済活動に関するリスク	**知的財産権等の侵害** 生成物による他者の知的財産権等の侵害の可能性がある。複数のアーティストからの集団訴訟事例もある。[26]
		金銭的損失 企業が自社の扱うAIの出力により他者の権利を著しく侵害した場合等において、損害賠償請求など金銭的な責任を問われる懸念がある。
		機密情報の流出 個人情報及び機密情報がプロンプトとして入力され、そのAIからの出力等を通じて流出してしまう懸念がある。特に、外部サービスと内部データを連携する場合は、意図しない重要情報の漏えいや情報の改ざん等に注意が必要となる。
		労働者の失業 AI等の導入により、失業リスクや格差の拡大なども懸念されている。
		データや利益の集中 一部のAI開発者のみにデータや利益が集中する懸念がある。また、少数言語国では自国言語による高性能なAIが存在しないといった懸念がある。
		資格等の侵害 法律又は医療等業法免許及び資格が求められる領域に生成AIを利活用する場合、業法免許及び独占資格等の侵害リスクが存在する。
	情報空間に関するリスク	**偽・誤情報等の流通・拡散** 生成AIによる誤情報、ディープフェイク等による情報操作や世論工作が行われる懸念がある。

[26] 著作権と生成AIとの関係で生じるリスクを低減させる上で、また、自らの権利を保全・行使する上で望ましいと考えられる取組については、「AIと著作権に関するチェックリスト&ガイダンス」（令和6年7月31日文化庁著作権課）にまとめられているため、当該ドキュメントを踏まえ必要な対応を行う。

リスクの分類案		AIによるリスク事例とその概要
		民主主義への悪影響 選挙活動等において、他の候補者の偽・誤情報やディープフェイクの生成・拡散に利活用される懸念がある。
		フィルターバブル及びエコーチェンバー現象 SNS等によるレコメンドにおいて生じる問題であり、自分の見たい情報にのみ囲まれる及び自分と同じような考えばかりが表示される現象により極端な考えの持ち主になる懸念がある。
		多様性・包摂性の喪失 社会の構成員全体が同じ生成AIモデルを同じ用い方で活用した場合、導かれる意見及び回答が画一化し、多様性が失われる懸念がある。また、金融取引において共通したアルゴリズムが用いられることで、市場の不安定性が増すことが懸念されている。
		バイアス等の再生成 生成AIの出力を鵜呑みにする状況が続くことで、既存の情報に含まれる偏見を増幅し、不公平及び差別的な出力が継続・拡大する懸念がある。
	環境に関するリスク	**エネルギー使用量及び環境の負荷** AI開発・利用拡大に伴い大量の電力を使用することで、環境負荷が増大する。

政府における生成AIの調達・利活用においても、上記のようなこうしたリスクに留意することが必要であり、政府として、例えば、以下のようなリスクについても考慮が必要となる。

- 政策に関わる業務に生成AIを活用する際等において、政治的中立性・適正性から逸脱した情報や表現を生成するリスク
- 単一の系統のモデルに依存することによるコスト増やバイアスが定着するリスク
- 利用言語・文化・歴史的背景への考慮が不十分な生成AIの出力を直接利活用することで誤った発信や国益に反する発信を行ってしまうリスク
- 業務に生成AIを利活用することで行政上の判断の根拠等が不明瞭また又は追跡不可能となり、行政過程について国民等への説明責任が果たせないリスク
- ベンダーロックインによる不要なコストの増加のリスク

- 法的拘束力を持つ翻訳や問合せ対応に生成 AI を活用する場合、誤回答によって違法有害情報を流布するリスク
- 生成 AI を用いて出力した画像が、既存の著作物に類似した要素を意図せず含んで出力され、その状態に気付かないまま利用してしまうリスク
- 音声回答機能が、著名な個人の声質や話し方と意図せずに類似してしまうリスク

各府省庁においては、生成 AI の便益のみならず、こうしたリスクがあることにも留意した上で、生成 AI の利活用とリスク管理を表裏一体で進めることが必要である。

6　政府における生成AIの調達・利活用に係るルール

6.1　政府における生成 AI の調達・利活用に係る対応事項の全体像

6.1.1　各種法令・ガイドライン等を踏まえた対応事項

①　生成 AI システムの調達・利活用においても、各種法令や「デジタル社会推進標準ガイドライン」、「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群」、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」、「個人情報の保護に関する法律についてのガイドライン（行政機関等編）」等の政府情報システムに係るガイドラインを遵守することが必要である。

②　本ガイドラインの対象となる生成 AI システムに関して、要機密情報を取り扱うクラウドサービスを調達する場合においては、政府情報システムのためのセキュリティ評価制度（ISMAP：Information system Security Management and Assessment Program）の原則利用の考え方に基づき、原則として ISMAP 等クラウドサービスリスト~~又は ISMAP-LIU クラウドサービスリスト~~から選定した上で[27]、別途、本ガイドラインによる対応を行う必要がある。すなわち、生成 AI システムに特有のリスク等についての必要な対応は本ガイドラインに基づき行うため、ISMAP 等クラウドサービスリスト~~又は ISMAP-LIU クラウドサービスリスト~~から選定したものであっても、本ガイドラインの対応が不要となるものではないことに注意が必要である。

③　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活用する場合には、原則として要機密情報を取り扱うことはできない。また、要機密情報を取り扱わない場合であっても、リスクを考慮した上で利用可能な業

[27] クラウドサービス事業者が、生成 AI モデルを提供する事業者から生成 AI モデルの提供を受け、当該生成 AI モデルの扱うデータに対してセキュリティ管理機能を適用する自らの生成 AI 開発基盤において生成 AI サービスを提供する場合（PaaS に相当）に、当該生成 AI 開発基盤を言明対象範囲に含めて ISMAP に登録したときには、通常は当該生成 AI サービスが取り扱うデータのセキュリティは、ISMAP のセキュリティ要件を満たす状態とみなされる。この場合において、クラウドサービス事業者が生成 AI 開発基盤を言明対象範囲に含めて ISMAP の登録を行う場合には、提供される個々の生成 AI モデルを言明対象範囲に含める必要はない。また、提供される生成 AI モデルは必ずしも ISMAP に登録されている必要はない。

務の範囲をあらかじめ特定し、個々の利用に当たっては、利用手続きに従って、利用目的（業務内容）や利用者の範囲などの企画者からの申請内容を許可権限者[28]が審査した上で利用の可否を決定し、その利用状況について管理することが必要である[29]。

④　政府機関等における生成 AI の業務利用にあたっては、「DeepSeek 等の生成 AI の業務利用に関する注意喚起（令和７年２月６日デジタル社会推進会議幹事会事務局）」[30]を踏まえ、調達行為を伴わない場合であってもサービスの利用によって生ずるリスク（※）を十分認識の上、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」等の趣旨も踏まえ、国家サイバー統括室~~内閣サイバーセキュリティセンター~~の助言を求めた上で、適切に判断することが必要である。

※ 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。

⑤　生成 AI の調達・利活用に関わる政府職員は、AI 事業者ガイドライン「第２部 C. 共通の指針」を踏まえた取組を行う必要がある。

表 7　AI 事業者ガイドライン「第２部 C.共通の指針」の概要

1 人間中心	① 人間の尊厳と個人の自律
	② AI による意思決定・感情の操作等への留意
	③ 偽情報等への対策
	④ 多様性・包摂性の確保
	⑤ 利用者支援
	⑥ 持続可能性の確保
2 安全性	① 人間の生命・身体・財産、精神及び環境への配慮
	② 適正利用
	③ 適正学習
3 公平性	① AI モデルの各構成技術に含まれるバイアスへの配慮

[28] 例外措置の適用の申請を審査し、許可する者を指す。

[29] 「ChatGPT 等の生成 AI の業務利用に関する申合せ（第２．１版）」は廃止し、本ガイドラインを適用し、取組を進めることとしている。

[30] DeepSeek 等の生成 AI の業務利用に関する注意喚起（事務連絡）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/d2a5bbd2-ae8f-450c-adaa-33979181d26a/e7bfeba7/20250206_councils_social-promotion-executive_outline_01.pdf

	② 人間の判断の介在
4 プライバシー保護	① AI システム・サービス全般におけるプライバシーの保護
5 セキュリティ確保	① AI システム・サービスに影響するセキュリティ対策
	② 最新動向への留意
6 透明性	① 検証可能性の確保
	② 関連するステークホルダー
	③ 合理的かつ誠実な対応
	④ 関連するステークホルダーへの説明可能性・解釈可能性の向上
7 アカウンタビリティ	① トレーサビリティの向上
	② 「共通の指針」の対応状況の説明
	③ 責任者の明示
	④ 関係者間の責任の分配
	⑤ ステークホルダーへの具体的な対応
	⑥ 文書化
8 教育・リテラシー	① AI リテラシーの確保（各主体を対象）
	② 教育・リスキリング
	③ ステークホルダーへのフォローアップ
9 公正競争確保	-
10 イノベーション	① オープンイノベーション等の推進
	② 相互接続性・相互運用性への留意
	③ 適切な情報提供

⑥　生成 AI の調達・利活用にあたっては、知的財産権等のリスクに対する対策を踏まえることが必要である。本ガイドラインは、「コンテンツ制作のための生成 AI 利活用ガイドブック」（令和６年７月５日経済産業省）や「AI と著作権に関するチェックリスト&ガイダンス」（令和６年７月 31 日文化庁著作権課）に記載された対策例を踏まえた内容となっているが、詳細を確認する必要がある場合にはこれらを参考に、調達・利活用にあたって適切に判断することが必要である。

⑦　セキュリティ確保の観点では、「AI のセキュリティ確保のための技術的対策に係るガイドライン（案）」（総務省）が、LLM 及び LLM を構成要素に含む AI システムを対象として、「不正操作による機密情報の漏えい、AI システムの意図せぬ変更や停止が生じないような状態」に対する脅威への技術的対策例を示している。AI の性質上、脅威を生じさせる要因等を完全に排除するこ

とは困難であること、単独の対策実施により脅威を生じさせる要因を排除することは困難な場合があることを前提に、企画者・開発者・提供者それぞれが、同ガイドラインが示す技術的対策例も踏まえつつ、できる限り複数の対策を講じるなど適切にリスク対策を行い、リスクを低減することが必要である。同ガイドラインが示す直接プロンプトインジェクション攻撃、間接プロンプトインジェクション攻撃及び DoS 攻撃（サービス拒否攻撃）への主な対策の概観は、表８に示すとおりである。また、【別紙３】調達チェックシート（生成 AI システム用）においては、同ガイドラインが示す技術的対策例も踏まえつつ、セキュリティ確保の評価観点からの対策例を記載している。

表 ８　AI のセキュリティ確保のための技術的対策に係るガイドライン（案）「プロンプトインジェクション攻撃及び DoS 攻撃（サービス拒否攻撃）への主な対策（概観）」[31][32]

<table>
<tr><td rowspan="2"></td><td>AI 開発者における対策</td><td colspan="4">AI 提供者における対策</td></tr>
<tr><td>安全基準等の学習による不正な指示への耐性</td><td>システムプロンプトによる不正な指示への耐</td><td colspan="3">ガードレール等による入出力や外部参照データの検証</td><td>オーケストレータや RAG[33] 等の権限管理</td></tr>
<tr><td></td><td></td><td></td><td>入力プロンプトの検証</td><td>外部参照データの検証</td><td>出力の検証</td><td></td></tr>
</table>

[31] プロンプトインジェクション攻撃とは、生成 AI モデルに細工をした入力を行うことで、不正な出力をさせる攻撃である。ガイドラインにおいて、生成 AI モデルに細工をしたプロンプトを入力することで実施するものを直接プロンプトインジェクション攻撃といい、生成 AI モデルに細工をしたデータを参照させることで実施するものを間接プロンプトインジェクション攻撃という。DoS 攻撃（サービス拒否攻撃）とは、生成 AI モデルに、AI システムが膨大な処理を必要とするプロンプト入力を行うことで、AI システムへの想定以上の計算負荷や経済的な損失を生じさせ、AI システムの応答の遅延・停止を引き起こしたり、サービスの継続性を損なわせたりする攻撃である。

[32] 表８は各攻撃への主な対策を概観するものであり、必ずしも網羅的なものではない。また、空欄となっている箇所については、全く対策が存在しないことを意味するものではない。さらに、各対策については、攻撃の種類等に応じて複数の類型が存在し得る。

[33] Retrieval-Augmented Generation の略であり、外部のデータベースから取得した知識に基づいて LLM に回答を生成させることで、知識に即した回答がなされるようにしたり、ファインチューニングを経ず知識を拡張可能したりする手法（出典：AI プロダクト品質保証コンソーシアム「AI プロダクト品質保証ガイドライン 2025.04 版」P.10-2）

	の向上	性の向上				
直接プロンプトインジェクション攻撃	○	○	○		○	○
間接プロンプトインジェクション攻撃	○	○	○	○	○	○
DoS 攻撃（サービス拒否攻撃）	○	○	○			

6.1.2　本ガイドラインに基づく対応事項

①　生成 AI の調達・利活用に関わる政府職員は、本ガイドラインの「6.2 政府における生成 AI システムの AI 統括責任者（CAIO）の対応事項」、「6.3 政府における生成 AI システムの企画者の対応事項」、「6.4　政府における生成 AI システムの開発者の対応事項」、「6.5　政府における生成 AI システムの提供者の対応事項」、「6.6　政府における生成 AI システムの利用者の対応事項」、「6.7　生成 AI システム特有のリスクケースへの対応」について、それぞれ適切に対応する。

②　ただし、生成 AI システムの導入類型は、様々なパターンが想定される。例えば、主な類型としては、生成 AI システム導入に係る「開発の実施有無」及び「契約の形態」で整理した場合、以下の類型が考えられる。

A：生成 AI システムの個別開発は実施せず、定型約款や規約等への同意によりサービスを利用する。（原則、要機密情報を扱わない想定）
B：生成 AI システムの個別開発は実施せず、定型約款や規約等への同意に加え、個別契約の締結を行う。
C：生成 AI システムの個別開発を実施し、個別契約の締結を行う。

このとき、A に該当するケースにおいては、原則、要機密情報を取り扱わない利用を想定していることから、「6.3.2　生成 AI システムの調達時の対応事項」で規定する「調達チェックシート」及び「契約チェックシート」に基づき、調達仕様書又は契約書において要求事項等を定めることが不要かどうか、「調達チェックシート」及び「契約チェックシート」に記載された内容と矛盾がある約款項目がある等の問題がないか、を確認する必要がある（求めることが必要な要求事項等がある場合には、B 又は C の形で調達を行うことを検討する。）。

加えて、B 又は C に該当するケースにおいても、例えば、以下のような観点を踏まえて、各対応事項について、対策が不十分又は過剰とならないよう、リスクと対策のバランスを考える必要がある。

・概念検証（PoC）段階か、本番開発段階か等のプロジェクトフェーズ
（例えば、概念検証段階で各対応事項を全て実施する場合、対策が過剰となる可能性がある。）
・高リスクの可能性が高い利用か、否か等のリスクレベル
（例えば、高リスクの可能性が高い利用の場合で、ユースケースにあわせた追加の対応が必要となる可能性がある。）
・ユースケースの性格
（例えば、行政内部で大量の文書の検索のために生成 AI システムを利用する場合、基本項目の「有害情報の出力制御」や「偽誤情報の出力・誘導の防止」の要求事項は、不要となる可能性がある。）

このように、生成 AI システムの案件に応じて、上記の導入類型、プロジェクトフェーズ、リスクレベル、ユースケースの性格等を踏まえ、前項（「6.1.2　本ガイドラインに基づく対応事項」の①）については、リスクと対策のバランスを考慮し、各対応事項の要求レベルや一部の要求事項・取決め事項の取捨選択又は拡充を検討する必要がある。

6.2　政府における生成 AI システムの AI 統括責任者（CAIO）の対応事項

6.2.1　各府省庁内向けルールの整備

各府省庁の AI 統括責任者（CAIO）は、①各府省庁内における生成 AI の利活用方針及び②生成 AI システム特有のリスクケース発生時の対応方針を示すため、以下のルールを策定する。なお、当該ルールは、本ガイドラインの改定、生成 AI の最新の動向や利活用状況を踏まえて随時改定することとする。

① 生成 AI システムの利活用ルール

各府省庁において、適切な生成 AI の利活用を促進するため、AI 統括責任者（CAIO）は、「【別紙２】生成 AI システムの利活用ルールひな形」に基づき、以下のような事項に留意して、各府省庁の利用者(政府職員)に向けて生成 AI システムの利活用ルールを策定する。

- ~~政府職員等~~利用者が生成 AI システムの利活用前に最低限理解しておくべき知識や要機密情報の取扱い等の留意事項
- （生成 AI システムごとの利活用ルール等に記載する）利用目的の範囲内での利活用や AI 生成物を利活用した業務に係る説明責任やリスクの回避など~~政府職員による~~利活用に当たって心得るべき事項
- 生成 AI を活用して職務上作成した~~文書~~AI 生成物の取扱い
- 生成 AI 活用時の知的財産権等に係る対策
- 生成 AI システム特有のリスクケース発生時の AI 統括責任者（CAIO）への報告

等

② 生成 AI システム特有のリスクケースへの対応に関わるルール

生成 AI システム特有のリスクケースが起こった場合に備え、生成 AI システム特有のリスクケースへの対応のルールを策定する。

（詳細は、「6.7 生成 AI システム特有のリスクケースへの対応」を参照）

6.2.2 各府省庁内における AI ガバナンスの確保

AI 統括責任者（CAIO）は、以下①、②、及び③を通じて AI ガバナンスの確保に取り組むものとする。

① AI 統括責任者（CAIO）は、各府省庁内における AI ガバナンス体制を整備し、AI ガバナンスを継続して確保する。

（詳細は「4.2 各府省庁における AI ガバナンス体制の整備」参照）

② AI 統括責任者（CAIO）は、本ガイドラインを踏まえたルールの策定・見直し、本ガイドラインや生成 AI システムの利活用ルールの周知、研修（入力データやハルシネーション等に係る注意喚起など）等を通じ、各府省庁において、本ガイドラインを踏まえた生成 AI の調達・利活用が行われるよう、必要な取組を行う。

③ 政府情報システムは、「デジタル社会推進標準ガイドライン」を通じて、各

府省庁 PMO がシステム監査を実施することとしているところ、生成 AI システムに係る監査においては、生成 AI システムの特性上、生成 AI 特有のリスクを認識の上で監査を実施すべきと考えられることから、生成 AI システムに係る上記監査においては、AI 統括責任者（CAIO）も連携して対応し、高リスク生成 AI のリスク軽減策の実施状況をはじめとして、本ガイドラインの記載事項も参考とすることとする。

なお、生成 AI システムの監査の具体的在り方の参考とできるよう、また、各府省庁に知見の共有を行うため、AI 統括責任者（CAIO）は、生成 AI システムの監査において、今後の検討に資すると考えられる監査の指摘事項等があった場合には、先進的 AI 利活用アドバイザリーボードまで共有することが望ましい。

6.3 政府における生成 AI システムの企画者の対応事項

6.3.1 生成 AI システムの企画時の対応事項

生成 AI システムの企画者は、企画時に以下の対応を実施する。生成 AI の便益を最大化するためには、企画時に業務・生成 AI システム両方の知見を用いて検討を進めることが望ましい。そのため、業務知見者と生成 AI システム知見者の両者が連携する体制を構築した上で、生成 AI システムを企画することに努める。

① 企画者は、生成 AI システムを使って何を実現・解決したいのか目的を明確にするとともに、適切な目標設定を行う。

② 企画者は、当該ユースケースを想定した環境・リスク分析を行うとともに、リスクを最小限に抑える方法や運用時を含めた品質確保策等を検討する。

③ 企画者は、生成 AI システムにおいても、「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」に基づき、権限管理を適切に実施する観点から、取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けておくことが求められる[34]。

[34] 生成 AI 固有のリスクとして、当該生成 AI システムが要機密情報又は個人情報を扱う場合で、入力が学習される設定となっている場合に、入力者以外にも漏洩するリスクへの対処が必要となる。

④ 企画者は、「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」に基づき、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの取得及び管理を行う必要がある。生成AIシステムについては、「6.5　政府における生成AI システムの提供者の対応事項」での生成 AI システムの適正利用の確認のため、生成 AI システムへの入力や出力、アクセス履歴等のログの取得及び管理を検討することが求められる。

⑤~~③~~ 企画者は、デジタル庁が実施する統括監理の際に、生成 AI システムの導入予定、リスク分析結果、リスク対応策、行政データの取扱い等について、報告を行う。

⑥~~④~~ 企画者は、高リスクの可能性がある生成 AI システムについては、「4.2.2 先進的 AI 利活用アドバイザリーボードへの報告」のとおり、当該プロジェクト目的、リスク軽減策や運用時を含めた品質確保策等を、AI 統括責任者（CAIO）が先進的 AI 利活用アドバイザリーボードへ報告する際、連携して対応を行う。

⑦~~⑤~~ 今後、政府における生成 AI の利用拡大を見据え、政府機関等における生成 AI システム間のデータ等の連携や府省庁間の共同利用、共同プロジェクトや共通システムの組成等を通じて政府全体としての生成 AI システムの最適化を図る観点は重要である。例えば、ガバメントクラウド等の共通機能上で~~、~~提供される生成 AI システムを積極的に活用することで、費用対効果の向上、セキュリティの確保、業務システムとの連携等を効率的に行うことができる可能性がある。このため、企画者は、新たな生成 AI システムの検討に当たっては、こうした共通機能として提供されたサービスの利活用についても留意する。（※）

※ ガバメントクラウドに関する法律（情報通信技術を活用した行政の推進等に関する法律の一部を改正する法律（令和７年法律第４号））に基づき、国の行政機関等が自らの事務の実施に関連する情報システムの整備を行う場合は、ガバメントクラウドの利活用を検討する義務がある。

生成 AI と組み合わせたシステム整備あるいは更改を検討する際にも、

当該システムをガバメントクラウド上に構築した上でパッケージやツールを活用する形で効率的に生成 AI 環境を確保できないか等について検討することが求められる。

その他、具体的な利活用検討の考え方については、「ガバメントクラウド利用検討の基本的な考え方について」を参照されたい。

6.3.2 生成 AI システムの調達時の対応事項

① 企画者は、「【別紙３】調達チェックシート（生成 AI システム用）」（以下、「調達チェックシート」という。）[35] ~~（※）~~ を参照し、事業者及び調達予定の生成 AI システム等について、調達の応募者に対し求める事項として、調達仕様書に盛り込む。また、企画者は、リスク分析結果等を踏まえ、「調達チェックシート」に記載のない事項についても、必要に応じ追加を検討する。

~~※「調達チェックシート」は、AI 事業者ガイドライン及び AISI が公表している「AI セーフティに関する評価観点ガイド（第 1.01 版）」[36] 等を参考に、生成 AI 納入事業者の AI ガバナンス、適切なインプット・アウトプットやデータの取扱い、偽誤情報の出力防止等を含む生成 AILLM やサービスの品質確保、生成 AI システム特有のリスクケース発生時の適切な対応確保、国民等が利用する場合の適切な取扱確保（生成 AI によるアウトプットであることの表示等）、個人情報や知的財産の保護、セキュリティや説明可能性の確保といった観点から、生成 AI システムの調達時の要求事項や、要求事項を満たすための対策例とその詳細、裏付けとなる情報例を整理している。「調達チェックシート」を参照することで、生成 AI システムの調達時の要点を確認することができるため、~~

[35] 「調達チェックシート」は、AI 事業者ガイドライン及び AISI が公表している「AI セーフティに関する評価観点ガイド（第 1.1 版）」等を参考に、生成 AI 納入事業者の AI ガバナンス、適切なインプット・アウトプットやデータの取扱い、偽誤情報の出力防止等を含む生成 AI やサービスの品質確保、生成 AI システム特有のリスクケース発生時の適切な対応確保、国民等が利用する場合の適切な取扱確保（生成 AI によるアウトプットであることの表示等）、個人情報や知的財産の保護、セキュリティや説明可能性の確保といった観点から、生成 AI システムの調達時の要求事項や、要求事項を満たすための対策例とその詳細、裏付けとなる情報例を整理している。

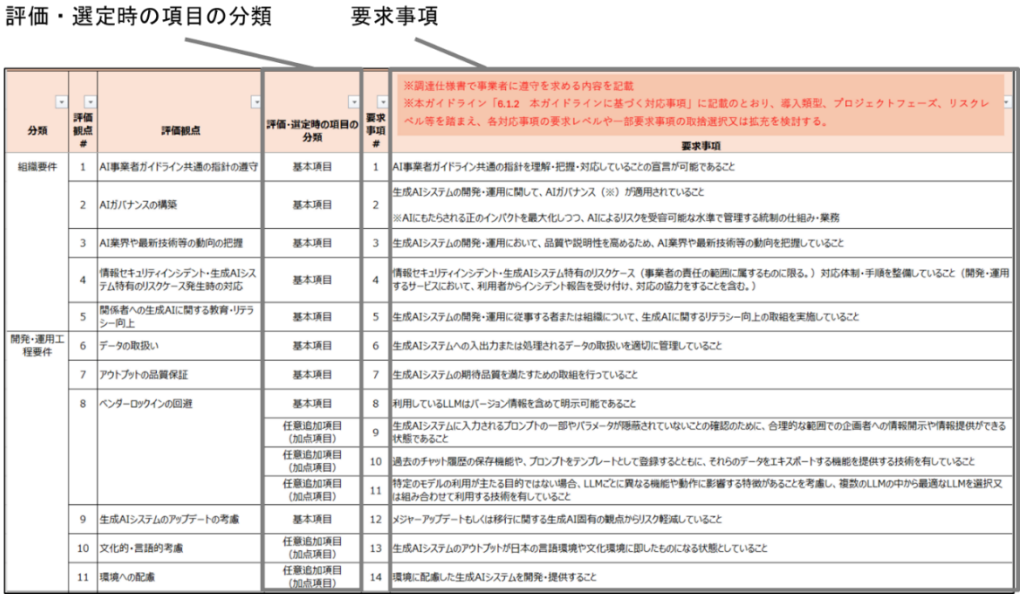
~~[36] 本ガイドラインは、「AI セーフティに関する評価観点ガイド（第 1.01 版）」を参考にしており、最新版「AI セーフティに関する評価観点ガイド（第 1.10 版）」の改定による修正については、今後の本ガイドラインの改定の際に検討する。~~

~~仕様書に盛り込む内容とその裏付けとなる情報を提出させるか、またどのような情報を提出させるかの検討時に参照されたい。なお、「調達チェックシート」は「生成 AI システムの調達」に関して特有の留意すべき項目のみ掲載しているため、あわせて、別途「デジタル・ガバメント推進標準ガイドライン」の内容や、「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の別紙「調達仕様書テンプレート」等を参照し調達仕様書を作成する必要がある。~~

~~※「調達チェックシート」の見方~~

~~（「図 5 「調達チェックシート」の要求事項イメージ」参照）~~

~~図 5 「調達チェックシート」の要求事項イメージ~~



分類	評価観点#	評価観点	評価・選定時の項目の分類	要求事項#	※調達仕様書で事業者に遵守を求める内容を記載 ※本ガイドライン「6.1.2 本ガイドラインに基づく対応事項」に記載のとおり、導入類型、プロジェクトフェーズ、リスクレベル等を踏まえ、各対応事項の要求レベルや一部要求事項の取捨選択又は拡充を検討する。 要求事項
組織要件	1	AI事業者ガイドライン共通の指針の遵守	基本項目	1	AI事業者ガイドライン共通の指針を理解・把握・対応していることの宣言が可能であること
	2	AIガバナンスの構築	基本項目	2	生成AIシステムの開発・運用に関して、AIガバナンス（※）が適用されていること ※AIにもたらされる正のインパクトを最大化しつつ、AIによるリスクを受容可能な水準で管理する統制の仕組み・業務
	3	AI業界や最新技術等の動向の把握	基本項目	3	生成AIシステムの開発・運用において、品質や説明性を高めるため、AI業界や最新技術等の動向を把握していること
	4	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応	基本項目	4	情報セキュリティインシデント・生成AIシステム特有のリスクケース（事業者の責任の範囲に属するものに限る。）対応体制・手順を整備していること（開発・運用するサービスにおいて、利用者からインシデント報告を受け付け、対応の協力をすることを含む。）
	5	関係者への生成AIに関する教育・リテラシー向上	基本項目	5	生成AIシステムの開発・運用に従事する者または組織について、生成AIに関するリテラシー向上の取組を実施していること
開発・運用工程要件	6	データの取扱い	基本項目	6	生成AIシステムへの入出力または処理されるデータの取扱いを適切に管理していること
	7	アウトプットの品質保証	基本項目	7	生成AIシステムの期待品質を満たすための取組を行っていること
	8	ベンダーロックインの回避	基本項目	8	利用しているLLMはバージョン情報を含めて明示可能であること
			任意追加項目（加点項目）	9	生成AIシステムに入力されるプロンプトの一部やパラメータが隠蔽されていないことの確認のために、合理的な範囲での企画者への情報開示や情報提供ができる状態であること
			任意追加項目（加点項目）	10	過去のチャット履歴の保存機能や、プロンプトをテンプレートとして登録するとともに、それらのデータをエキスポートする機能を提供する技術を有していること
			任意追加項目（加点項目）	11	特定のモデルの利用が主たる目的ではない場合、LLMごとに異なる機能や動作に影響する特徴があることを考慮し、複数のLLMの中から最適なLLMを選択又は組み合わせて利用する技術を有していること
	9	生成AIシステムのアップデートの考慮	基本項目	12	メジャーアップデートもしくは移行に関する生成AI固有の観点からリスク軽減していること
	10	文化的・言語的考慮	任意追加項目（加点項目）	13	生成AIシステムのアウトプットが日本の言語環境や文化環境に即したものになる状態としていること
	11	環境への配慮	任意追加項目（加点項目）	14	環境に配慮した生成AIシステムを開発・提供すること

~~「要求事項」のうち、政府機関が調達する生成 AI システムに原則要求すべきと考えられる事項については、「基本項目」として設定している（調達チェックシートの「評価・選定時の項目の分類」列に記載）。~~

~~「基本項目」としている要求事項は、調達時に応募者に求める事項として盛り込むことを原則とする。「任意追加項目（加点項目）」としている要求事項は、必要に応じ考慮した方が良い観点であり、調達の評価項目の加点項目とすることを想定したものである。~~

~~調達チェックシートの参考として、「（参考）要求事項の参考」シートに、要求事項を満たすための対策例である「対策例」と「対策例詳細」、「裏付けとなる情報の例」を記載している。なお、対策例、対策例詳細、裏付けとなる情報の例について、技術動向やビジネス環境等~~

~~の変化を踏まえ、柔軟に記載の更新を検討していく予定である。~~

② 企画者は、総合評価方式や企画競争方式を採用する場合は、こうした要求事項について、必要に応じ評価項目にも反映する。

③ 企画者は、調達する生成 AI システムに関して、生成 AI モデル、アーキテクチャ等の生成 AI システムの特性、生成 AI システムの主要性能指標情報等の情報を取得する。また、リスク分析やリスク対応の検討のために合理的な範囲で、学習に使用されたデータや学習方法、データセットの情報も、取得に努める。

~~③~~④ 国内の生成 AI 事業者等のスタートアップ育成のためには、「公共調達」の活用が重要である。このため、企画者は、生成 AI システムに係る調達においては、「デジタル・スタートアップの公共調達参入機会拡大に向けた情報システムに係る調達における評価制度の実施要領」（令和６年１月 15 日デジタル社会推進会議幹事会決定）に掲げるところにより、デジタル・スタートアップを評価することとする。また、SaaS 型の生成 AI システムや、その導入支援を行う会社のサービスの検討にあたっては、デジタル庁が運営する「デジタルマーケットプレイス」[37]が活用可能である。「デジタルマーケットプレイス」を活用することで、迅速な導入が実現できるほか、中小・スタートアップを含む多様な事業者が公共調達市場にアクセスしやすくなり、公正競争が加速する効果が期待できるため、積極的な活用を検討する。

⑤~~④~~ 企画者は、「【別紙４】契約チェックシート（生成 AI システム用）」（以下、「契約チェックシート」という。）[38] ~~（※）~~を参照し、生成 AI システムの調達において留意すべき事項についても、契約書~~また~~又は調達仕様書に盛り込むことを検討する。また、企画者は、リスク分析結果等を踏まえ、「契約チェックシート」に記載のない事項についても、必要に応じ追加を検討する。

---

[37] デジタルマーケットプレイス　https://www.dmp-official.digital.go.jp/

[38] 「契約チェックシート」は、AI 事業者ガイドライン、経済産業省の「AI の利用・開発に関する契約チェックリスト」及び「AI・データの利用に関する契約ガイドライン」等を参考に、生成 AI システムのインプットに係る権利帰属関係、アウトプットに係る事業者の義務の範囲や知的財産権の帰属関係、生成 AI システム特有のリスクケース発生時の事業者の対応義務の範囲、期待品質の維持、環境への配慮等に係る事業者の対応義務の範囲等について、生成 AI システムの調達における契約時に確認が必要な項目を整理している。

※「契約チェックシート」は、AI 事業者ガイドライン、経済産業省の「AI の利用・開発に関する契約チェックリスト」及び「AI・データの利用に関する契約ガイドライン」等を参考に、生成 AI システムのインプットに係る権利帰属関係、アウトプットに係る事業者の義務の範囲や知的財産権の帰属関係、生成 AI システム特有のリスクケース発生時の事業者の対応義務の範囲、期待品質の維持、環境への配慮等に係る事業者の対応義務の範囲等について、生成 AI システムの調達における契約時に確認が必要な項目を整理している。「契約チェックシート」を参照することで、生成 AI システム調達時の契約において留意すべき要点を確認することができるため、契約書または調達仕様書に盛り込む条項の検討時に参照されたい。なお、契約チェックシートは、「生成 AI システムの調達」に関して契約特有の留意すべき項目のみ記載されている。

※「契約チェックシート」の見方
（「図 6 「契約チェックシート」の取決め事項イメージ」参照）

図 6 「契約チェックシート」の取決め事項イメージ

取り決め事項　　契約に盛り込む条項例　　補足説明

取り決め事項#	契約時の項目	取り決め事項	契約に盛り込む条項内容例	補足説明
1	基本項目	生成AIシステムに係るインプットの取り決め	インプットについて、インプットの定義、インプットの利用目的、インプットの利用条件、インプットの権利帰属に関して定める条項	事業者がインプットを目的に利用できる可能性があるため、契約による規律の対象となるインプットの範囲を定めること。事業者に対して生成AIシステム関連の提供目的以外の目的でインプットを原則として利用・保持しないことを目的外利用禁止義務として定めること（※）。事業者がインプットを利用することを認める場合の利用条件（学習の有無、データの保存方法等）を定めること。事業者がインプットに関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。 ※オプトアウトによって目的外利用を返断することも可能とするが、契約上オプトアウトで目的外利用を返断する対応を取ることを明確にすること。
2	基本項目	生成AIシステムに係るインプットの処理成果の取り決め	インプットの処理成果について、アウトプット以外のもので契約上規律の対象とするものの定義、利用目的、利用条件、権利帰属に関して定める条項	事業者がインプットを目的に利用できる可能性があるため、契約による規律の対象となるインプットの処理成果の範囲を定めること。事業者に対して生成AIシステム関連の提供目的以外の目的でインプットの処理成果を原則として利用・保持しないことを目的外利用禁止義務として定めること。事業者がインプットの処理成果を利用することを認める場合の利用条件（学習の有無、データの保存方法等）を定めること。事業者がインプットの処理成果に関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。
3	基本項目	生成AIシステムに係るアウトプットの取り決め	アウトプットについて、アウトプットの定義、事業者がユーザに対してアウトプットを提供する義務の有無及びその内容、事業者に対してアウトプットに関する一定の保証を定めること、ユーザがアウトプットを第三者に提供することができる場合にその条件を定める、事業者がユーザに対しアウトプットを提供する場合にアウトプットの権利帰属に関して定める条項	契約で規律の対象となるアウトプットとして、アウトプットの定義はユーザのサービス利用目的を十分にカバーできる範囲を定めること、事業者がアウトプットを提供する義務がある場合はユーザのサービス利用目的に照らして、提供条件（提供時期、頻度、登場その他の条件）や提供するアウトプットの内容（性質、量、粒度その他の内容）を定めること。事業者がアウトプットの保証・情報提供義務を負う場合の保証・情報提供の条件を定めること。第三者提供条件（提供先、提供範囲その他の条件）を定めること。ユーザがアウトプットに関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。
4	基本項目	生成AIシステムに係るアウトプットの処理成果の取り決め	アウトプットの処理成果について、契約上規律の対象とするものの定義、ユーザによる外部提供、権利帰属に関して定める条項	契約で規律の対象となるアウトプットの処理結果として、アウトプットの処理結果の定義はユーザのサービス利用目的を十分にカバーできる範囲を定めること、サービス利用目的に照らして外部提供条件（提供先、提供範囲その他の条件）を定めること、知的財産権等一定の権利を取得する場合には権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。
5	基本項目	生成AIシステムに係る契約上の取り決め	事業者が生成AIシステムを完成させる義務を定める条項	請負契約で事業者が生成AIシステムを完成する義務を負う場合、ユーザのサービス利用目的に照らして、どのような完成条件（完成時期、検収条件等）を定めるべきか検討して契約に盛り込むことが望ましい。

契約時に事業者とすり合わせるべき事項として、「取決め事項」を設定している（契約チェックシートの「取決め事項」列に記載）。「取決め事項」は、原則として契約書または調達仕様書に盛り込むことを検討する。

「契約に盛り込む条項内容例」と「補足説明」については、取り決めた事項を契約に盛り込む際の条項内容例とその補足説明であるため、調達する生成 AI システムの特徴や案件の特性、リスク評価結果を踏まえ、取捨選択の上、企画者が必要に応じ契約書または調達仕様書に盛り込むこととする。

コラム：SBIR 制度（Small/Startup Business Innovation Research）

スタートアップ等の支援を目的とした SBIR 制度（Small/Startup Business Innovation Research）[39]がある。

本制度は、スタートアップ等による研究開発を促進し、その成果を円滑に社会実装し、それによって我が国のイノベーション創出を促進するための制度である。

SBIR 制度のもとでは、「特定新技術補助金等」と「指定補助金等」という、２種類の補助金等が交付される。

1）特定新技術補助金等

特定新技術補助金等とは、各府省庁における研究開発の補助金や委託費のうち、研究開発型スタートアップ等を交付対象に含むものを指す。研究開発型スタートアップ等への支出の目標額を設定するとともに、支出の増大を図るための措置を規定している。

2）指定補助金等

指定補助金等とは、上述の特定新技術補助金等のうち、政策ニーズに基づき国が研究開発課題を設定して交付する補助金等のことで、令和３年度の制度改革により新たに創設された。

生成 AI を含む AI の分野においては「スタートアップ」が最先端の知見・技術を有していることが多々ある。

このため、指定補助金等の運用を行う各府省庁は、解決したい政策課題や調達ニーズをトピックとして取りまとめる際に、AI 関連テーマも積極的に検討することが望ましい。

なお、SBIR 制度の特定新技術補助金等の交付先中小企業者等は、政府調達においても、入札参加資格等級、過去の納入実績の有無にかかわらず、基本的に全ての入札への参加が可能となる支援措置も講じられている。

[39] SBIR 制度（Small/Startup Business Innovation Research）
https://www8.cao.go.jp/cstp/openinnovation/sbirseido/sbirseido.html

6.3.3　生成 AI システムの構築・リリース前の準備時の対応事項

生成 AI システムの企画者は、システムのリリース前に以下の取組を実施する。

① 安定的な稼働の確認

- 利用目的・機能を踏まえて、入出力の検証のためのテストシナリオを作成、入出力を検証し、システムが安定して動作すること及び期待品質を満たしているか確認する（※）。
  ~~（~~例えば、以下のような内容や方法が考えられる。~~：~~
  - 個別開発の場合に当該ドメインで禁忌とされる出力をしていないか~~、~~
  - 不適切な生成やバイアス~~の有無~~[人種、民族、性別等の偏見及び差別等の社会的バイアス等]~~を~~が発生していが~~ないか、また、~~
  - 調達時の生成 AI システムに対する仕様書要件を満たしているか
  - レッドチーム等の様々な手法を組み合わせて多様/独立した内外部テスト手段を採用する~~。）~~

※　企画者のみで作成するのが難しい場合には、ユーザーへのヒアリングや開発者等と相談をして作成。国民が使うシステムの場合は、テストとして稼働確認する者~~人~~について国民も含まれる可能性がある。データ（学習データ、テストデータ）の検証~~および~~及び改善対応については、契約上の責任に応じて、必ずしも企画者が実施するものではなく事業者（生成 AI システムのプロバイダー含む）が実施する場合もあり得る。

② 適正利用の促進

- 生成 AI システムごとの利活用ルールや利用方法を整備し、生成 AI システムのユーザー（府省庁内の利用者~~および~~及び生成 AI システムが国民に提供される場合は利用する国民のことをいう。以下同様）に周知する。
  また、特に不特定外部者（一般国民等）による府省庁外利用の場合は、適切な利用規約等を整備し、利用者からの個別の同意を取得する形とすることが望ましい。
  ~~（~~例えば、以下のような内容が考えられる。
  - ~~：~~生成 AI の利用目的・利用範囲、利用可能な生成 AI 環境と活用可能なデータの種別、利用条件・手続き・利用方法、利活用に係る推奨事項・禁止事項、その他生成 AI システムごとの要件に沿ってユーザーに伝えおくべき事項等~~）~~
- ウェブサイト等による行政情報及び機能提供を行う際は、別途「DS-

680.2　ウェブコンテンツガイドライン」[40]の「11　生成 AI 等の利用時の信頼性確保」も参考とする。

- 利用者が高度なタスクを実行できる AI エージェントなどを作成できる生成 AI システムの場合には、出力結果の適切さの判断を行わずにタスクを実行するもの（リスク判定ロジックのＣ①に相当）の作成を制限するか、又は利用者がこれを作成したときには利用開始前に提供者又は AI 統括責任者（CAIO）に報告を求める旨の利活用ルールを整備し、周知する。
- 生成 AI システムに関する重要な情報や生成 AI システムの利活用にあたっての留意点を生成 AI システムのユーザーが理解し易くかつアクセスが容易な方法で提供する。

  （例えば、以下のような内容が考えられる。

  - ：生成 AI の利用目的・利用範囲、適切／不適切な利用、技術的特性、予見可能なリスクとその緩和策、動作状況、受入テストの検証結果、発生した不具合や生成 AI システム特有のリスクケースの内容と対応状況、データ収集ポリシー、学習方法、システムアーキテクチャ、データの処理プロセス、緊急時の連絡先や問合せ窓口等）
- 実際に使用する生成 AI システムの目的・利用方法について、モデル上の制約等を含めて生成 AI システムのユーザーに提供する。

  （例えば、以下のような内容が考えられる。

  - ：データアップロード可否、プロンプトのトークン上限、応答速度等）
- 生成 AI システムのユーザーの情報を収集する可能性がある旨を周知する。

  （例えば、以下のような内容が考えられる。

  - ：利活用状況の適切な監督や説明責任・原因究明を果たすため等に収集するログイン履歴・プロンプトや出力結果等）

6.4　政府における生成 AI システムの開発者の対応事項

政府においては、生成 AI システムの開発は、主に事業者への委託により、実施される場合が多い。このため、開発者に求める事項については、調達への応募者に対し求める事項として、仕様書・契約書に盛り込むこととし、「6.3　政府における生成 AI の企画者の対応事項」として、記載している。

なお、政府職員が自ら生成 AI の開発を行う場合の開発者は、AI 事業者ガイ

[40] DS-680.2 ウェブコンテンツガイドライン
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a02f877e/20250930_web_content_guidelines.pdf

ドライン「第３部　AI 開発者に関する事項」に掲げられた取組を行うこととする。

6.5　政府における生成 AI システムの提供者の対応事項

生成 AI システムの提供者は、システムのリリース後、以下の取組を実施する。

① システムの運用

- 生成 AI システムの出力が期待品質を満たしていること、及び~~および~~不適切な生成やバイアスが発生していないことを監視する。
  ~~（~~例えば、以下のような内容や方法が考えられる。
  - ~~・~~プロンプト・出力結果等の利用ログが取得できる場合にサンプルチェックし、生成 AI システムへの入出力及び判断根拠等を定期的にモニタリングし、判断根拠が偏っていないか、特定の文化背景を基にした出力となっていないか等を確認する~~。~~
  - ~~・~~利用者へのアンケート・利活用実態状況調査で不適切な生成やバイアスが発生していないかを確認する~~。）~~
- 適切な目的で生成 AI システムが利用されていること、~~および~~及び目的外利用がされていないことを定期的に検証する。
  ~~（~~例えば、以下のような内容や方法が考えられる。~~：~~
  - プロンプト・出力結果等の利用ログが取得できる場合にサンプルチェックし、業務と関係のない何らかの出力を期待していると思われる入力をしていないこと等を確認する~~。また、~~
  - 利用者へのアンケート・利活用実態状況調査で利用目的等を調査する~~。）~~
- 生成 AI モデルのメジャーアップデートが実施される場合や追加的な学習を大規模に行った場合には、生成 AI システムの目的・用途及びコストとの関係も考慮しつつ、利用者への提供前に生成 AI システムの出力が期待品質を満たしていること、及び不適切な生成やバイアスが発生していないこと、セキュリティ対策、非機能要件や必要コストの変化等を確認した上で提供を開始する。
- 生成 AI システム及び生成 AI システムが取り扱う情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用する。
- 個人情報の不適切な取扱いや個人情報・要機密情報の流出、プライバシー侵害がないか確認する。
  ~~（~~例えば、以下のような内容や方法が考えられる。~~：~~
  - プロンプト・出力結果等の利用ログが取得できる場合はサンプルチェックを行い、個人情報の目的外利用が疑われるケースが発生していないか、生成 AI システムで想定される入力範囲を超えた要機密情

報が含まれていないか、プライバシー侵害が発生していないかを検知する。

- ◦ また、利用者へのアンケート・利活用実態状況調査で同様の事象が発生していないかを確認する。）

- 生成 AI システムに対する最新のリスク（攻撃手法の多様化など）及びその対応策の動向を確認し、必要な対応を行う。[41]
（例えば、以下のような内容や方法が考えられる：。

- ◦ 情報セキュリティインシデント（JIS Q 27000:2019 における情報セキュリティインシデントをいう。）や生成 AI システム特有のリスクケース事例や開発者のモデルの脆弱性に関するレポート等を定期的に確認し、必要な対応を行う。）

- 生成 AI システムの入出力に関して有用性や問題点などのレビューを行い、必要に応じて、利用者への周知をする。
（例えば、以下のような内容や方法が考えられる。

- ◦ ：生成 AI システムへの入出力及び判断根拠等を確認し、有用性に関する効果的な利用方法、問題点に関する注意喚起等を実施する。

- ◦ また、利用者へのアンケート・利活用実態状況調査で有用性や問題点を共有してもらう。）

- 利用者に対し、知的財産権等に係る対策の取組として、利用規約等を提示するとともに、可能な範囲でモデルにおける知的財産権等の侵害等防止のための仕組みに関する情報提供を行う。

- 提供する生成 AI システムを通じて第三者への権利侵害等が生じていることを認識、又は客観的に認識可能となった場合には、是正等の合理的な措置を講じることが求められ得る。なお、個別具体の事案によっては、認識可能となった時点以降に必要な措置が講じられなかったことが考慮要素となり、責任を問われる可能性が高まる場合があることにも注意が必要である。

- 利用者が高度なタスクを実行できる AI エージェントなどを作成できる生成 AI システムにおいて、出力結果の適切さの判断を行わずにタスクを実行するもの（リスク判定ロジックのＣ①に相当）を作成した場合には、提供者又は AI 統括責任者（CAIO）に報告させることが求められる（提供者が報告を受ける場合においては、AI 統括責任者（CAIO）に報告するこ

[41] 生成 AI システムに対する一般的なセキュリティリスクへの対応の詳細につき、LLM に関しては、AI のセキュリティ確保のための技術的対策に係るガイドライン（案）の「3.4 AI 提供者における対策」や「3.5 AI 開発者・提供者に係るその他の基本的な対策等」、「別添（付属資料）」等、AI 提供時のセキュリティ対策として考えられる対策の内容も確認されたい。

とが求められる）。

② システムの保守

- 必要に応じて、生成 AI モデル改善の判断を事業者に促す。
  （例えば、以下のような内容が考えられる。
  - 生成 AI モデルを構成する各技術要素のバイアスの再評価、評価結果に基づき変化点があった場合等に生成AIモデルの改善を提案する。）
- 「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群」の遵守を前提とし、脆弱性の対応を検討、必要に応じて実施する。
  （例えば、以下のような内容が考えられる。
  - 生成 AI システムのプログラムに内在する脆弱性を検知した場合、パッチ対応・モデル更新等を検討・実施する。）

③ 生成 AI システム特有のリスクケースへの対応

（詳細は「6.7 生成 AI システム特有のリスクケースへの対応」を参照）

6.6 政府における生成 AI システムの利用者の対応事項

利用者は、本ガイドラインを踏まえて策定された、各府省庁における生成 AI システムの利活用ルール（「6.2 政府における生成 AI システムの AI 統括責任者（CAIO）の対応事項」参照）及び各生成 AI システムの利活用ルール（「6.3.3 生成 AI システムの構築・リリース前の準備時の対応事項」参照）を遵守することが求められる。

6.7　生成 AI システム特有のリスクケースへの対応

既に述べたリスクへの対応をすべて行ったとしても、リスクをゼロにすることはできないとの前提のもと、リスクを軽減するための対応と並行して、リスクが顕在化した場合等への対応を各府省庁において準備しておく必要がある。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~~または~~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も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、利活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。
- 音声回答機能が、著名な個人の音声に類似してしまい、本人から停止の申出があった。
- 不自然な表現の画像を生成し不自然であると気付かずに利用し、公開文書等に掲載したことで国民から批判を受けた。
- 音声入力が不正確なことにより、それを元に作成した記録の意味内容が本来と異なるものとなり、重要な記録の正確性が損なわれていることが指摘された。

生成 AI システム特有のリスクケース等への対策として、~~各府省庁の~~政府職員は以下を実施する。

① AI 統括責任者（CAIO）は、本ガイドラインを踏まえ、生成 AI システム特有のリスクケースへの対応手順を整備する。

② 生成 AI システム特有のリスクケースが発生した場合、AI 統括責任者（CAIO）及び生成 AI の提供者が中心となり、重要度・影響の程度等を踏まえ、適切な対応を行う。

③ 政府全体での生成 AI システム特有のリスクケースへの対応能力の向上を目的とし、先進的 AI 利活用アドバイザリーボード（事務局）にて、生成 AI システム特有のリスクケースのナレッジを集約する。このため、AI 統括責任者

（CAIO）は、生成AIシステム特有のリスクケースの発生時及び対応後に先進的AI利活用アドバイザリーボード（事務局）に報告する。先進的AI利活用アドバイザリーボード（事務局）は各府省庁に対し必要に応じ、生成AIシステム特有のリスクケースへの対応にあたっての助言等を行う。

④ 情報セキュリティインシデントと生成AIシステム特有のリスクケース双方の性質を併せ持つインシデントが発生する可能性もある（例：生成AIシステムの学習データがサイバー攻撃者により汚染され、モデルの精度が低下したことにより偏見を含む出力を生成しやすくなる等）。このような状況下においては、情報セキュリティインシデント対応体制、生成AIシステム特有のリスクケースへの対応体制間で適切に連携をする、あるいは双方の専門性を活かして協力して対応する。その際、各府省庁で定められた情報セキュリティインシデント発生時の対処手順に従って対応することが基本となる。

なお、こうした生成AIシステム特有のリスクケース発生時は、必要に応じ、対応に必要なデータについて事業者等から提出を受けることや、必要な監査を実施することについても検討する（これらへの対応が適切になされることを担保するため、生成AIシステムに係る事業者との契約においても、これらへの対応について盛り込むことを検討する。）。

⑤ 生成AIシステムについて、個人情報漏えい事案等が発生した場合は、各府省庁で定められた対応手順に従って適切に対応を行う。このような状況下においては、個人情報保護への対応体制と生成AIシステム特有のリスクケースへの対応体制間で適切に連携をする。

7　今後の進め方

日々技術進歩する生成AIシステムの政府調達・利活用においては、今後想定されていなかったリスクが顕在化する可能性もあることなどから、政府による生成AI調達・利活用ルールについては、随時見直していくこととする。

~~また、政府が調達する画像や動画等の生成AIに係る来歴証明[42]の導入の在り方については、政府における生成AIの利活用の状況、国際的な議論の動向等を踏まえ、引き続き検討を行う。~~

~~更に、政府機関等における生成AIシステム間のデータ等の連携や府省庁間での共同利用、共同プロジェクトや共通システムの組成等を通じた政府全体としての生成AIシステムの最適化の在り方について、令和7年度に検討を行ったうえで、今後のルール見直しに反映させていくこととする。~~

以上

~~[42] コンテンツが誰によって、いつ、どのように作成され、どのような変更が加えられたかを、検証可能な形でコンテンツに付与する技術~~

附則

この決定の内容は、2026 年（令和８年）９月１日から施行する。ただし、「6.2　政府における生成 AI システムの AI 統括責任者（CAIO）の対応事項」については、2026 年（令和８年）６月までに必要な措置を定めるものとし、「2.2.2　本ガイドラインが対象とする生成 AI」の AI ガバナンスの枠組みの対象については、2026 年（令和８年）７月１日から適用するものとする。

記入日	
所属（府省庁/課室等）	
システム名	
記入者名	

別紙１

リスク判定結果	回答欄を記載ください

■高リスク判定チェックリスト

以下のチェック内容を確認し、企画時点の想定で回答欄を記載ください

観点	チェック内容	選択肢	回答	コメント※自由記述
A. 適用業務	適用業務は次のいずれでしょうか？	①生成AIによる生成物の瑕疵※１が重大な影響を及ぼす可能性のある業務※２に適用する ②生成AIによる生成物の瑕疵※１が重大な影響を及ぼす可能性のある業務に適用しない ※１生成AIが提供する情報の誤り等 ※２国民の基本的権利や安全に大きな影響を及ぼす業務、機微な政策分野に関する業務、人間の生命・身体・財産に影響を及ぼす又は法人の事業に重大な影響を及ぼす業務、資格が求められる業務、高い説明可能性が求められる業務		
B. 利用範囲	利用範囲は次のいずれでしょうか？	①不特定外部者（一般国民等）による利用 ②特定外部者※による利用 ③政府職員による府省庁内・複数府省庁横断での利用（共通システムでの利用等） ④政府職員による府省庁内・単一省庁での利用 ※自身の生成AIのリスク知見又は業務上の知見等に基づき出力結果の適切さの判断が可能な者に限る		
C. 職員等による出力結果の判断	出力結果の判断に係る運用は次のいずれでしょうか？	①生成AIシステムの出力結果の適切さを判断せずに利用する ②生成AIシステムの出力結果の適切さを判断して利用する		

※「高リスク判定シート」の見方
「高リスク判定シート」は、以下3つのリスク軸に係る設問について、回答するだけで「高リスクに該当する可能性が高い」か「高リスクに該当する可能性が低い」かを簡易的に判定するツール。判定ロジックは以下のフローに従う

【回答前】

記入日	
所属（府省庁/課室等）	
システム名	
記入者名	

別紙１

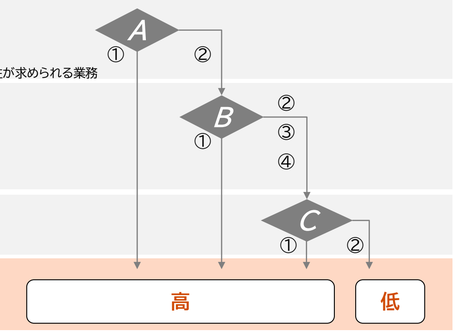
リスク判定結果	回答欄を記載ください

■高リスク判定チェックリスト
以下のチェック内容を確認し、企画時点の想定で回答欄を記載ください

観点	チェック内容	選択肢	回答	コメント※自由記述
A. 適用業務	適用業務は次のいずれでしょうか？	①生成AIによる生成物の瑕疵※１が重大な影響を及ぼす可能性のある業務※２に適用する ②生成AIによる生成物の瑕疵※１が重大な影響を及ぼす可能性のある業務に適用しない ※１生成AIが提供する情報の誤り等 ※２国民の基本的権利や安全に大きな影響を及ぼす業務、機微な政策分野に関する業務、人間の生命・身体・財産に影響を及ぼす又は法人の事業に重大な影響を及ぼす業務、資格が求められる業務、高い説明可能性が求められる業務		
B. 利用範囲	利用範囲は次のいずれでしょうか？	①不特定外部者（一般国民等）による利用 ②特定外部者※による利用 ③政府職員による府省庁内・複数府省庁横断での利用（共通システムでの利用等） ④政府職員による府省庁内・単一省庁での利用 ※自身の生成AIのリスク知見又は業務上の知見等に基づき出力結果の適切さの判断が可能な者に限る		
C. 職員等による出力結果の判断	出力結果の判断に係る運用は次のいずれでしょうか？	①生成AIシステムの出力結果の適切さを判断せずに利用する ②生成AIシステムの出力結果の適切さを判断して利用する		

【判定ロジック】[高]=[高リスクに該当する可能性が高い]、[低]=[高リスクに該当する可能性が低い]

A. 適用業務
①生成AIによる生成物の瑕疵※1が重大な影響を及ぼす可能性のある業務※2に適用する
②生成AIによる生成物の瑕疵※1が重大な影響を及ぼす可能性のある業務に適用しない
※1生成AIが提供する情報の誤り等
※2国民の基本的権利や安全に大きな影響を及ぼす業務、機微な政策分野に関する業務、
人間の生命・身体・財産に影響を及ぼす又は法人の事業に重大な影響を及ぼす業務、資格が求められる業務、高い説明可能性が求められる業務
B. 利用範囲
①不特定外部者(一般国民等)による利用
②特定外部者※による利用
③政府職員による府省庁内・複数府省庁横断での利用(共通システムでの利用等)
④政府職員による府省庁内・単一省庁での利用
※自身の生成AIのリスク知見又は業務上の知見等に基づき出力結果の適切さの判断が可能な者に限る
C. 職員等による出力結果の判断
①生成AIシステムの出力結果の適切さを判断せずに利用する
②生成AIシステムの出力結果の適切さを判断して利用する



リスクの定義
高:「高リスク」に該当する可能性が高い
低:「高リスク」に該当する可能性が低い

【回答後】

記入日	YYYY/MM/DD
所属（府省庁/課室等）	○○庁○○課
システム名	○○○○○○
記入者名	○○　○○

別紙１

リスク判定結果	高リスクに該当する可能性が低い

■高リスク判定チェックリスト
以下のチェック内容を確認し、企画時点の想定で回答欄を記載ください

観点	チェック内容	選択肢	回答	コメント※自由記述
A. 適用業務	適用業務は次のいずれでしょうか？	①生成AIによる生成物の瑕疵※１が重大な影響を及ぼす可能性のある業務※２に適用する ②生成AIによる生成物の瑕疵※１が重大な影響を及ぼす可能性のある業務に適用しない ※１生成AIが提供する情報の誤り等 ※２国民の基本的権利や安全に大きな影響を及ぼす業務、機微な政策分野に関する業務、人間の生命・身体・財産に影響を及ぼす又は法人の事業に重大な影響を及ぼす業務、資格が求められる業務、高い説明可能性が求められる業務	②	
B. 利用範囲	利用範囲は次のいずれでしょうか？	①不特定外部者（一般国民等）による利用 ②特定外部者※による利用 ③政府職員による府省庁内・複数府省庁横断での利用（共通システムでの利用等） ④政府職員による府省庁内・単一省庁での利用 ※自身の生成AIのリスク知見又は業務上の知見等に基づき出力結果の適切さの判断が可能な者に限る	②	
C. 職員等による出力結果の判断	出力結果の判断に係る運用は次のいずれでしょうか？	①生成AIシステムの出力結果の適切さを判断せずに利用する ②生成AIシステムの出力結果の適切さを判断して利用する	②	

別紙2

○○省　生成 AI システム利活用ルール（ひな形 Ver1.10）

令和○年○月○日

1. ルールの目的

本ルールは、○○省職員による生成 AI の適正な利活用を促進するため、「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」等を踏まえ、○○省職員が、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. 生成 AI システムの利活用に係るルール

生成 AI システムを利活用する際は、以下の（１）利活用前のルール※、（２）利活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（事務連絡）」[1]についても併せて確認されたい。

（1）利活用前のルール

- 生成 AI の利活用は、様々な便益が期待される一方、要機密情報の流出やハルシネーション（生成 AI が事実と異なる情報を出力すること）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・利活用に係るガイドライン」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 システムの企画者又は提供者（政府職員又は国民が利活用する生成 AI システムを運営する政府職員。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 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：利活用できる生成 AI の環境、利用条件、ルール、相談先、情報セキュリティインシデント（JIS Q 27000:2019 における情報セキュリティインシデントをいう）・生成 AI システム特有のリスクケース発生時対応等を利活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 システムの提供者に提供する必要がある旨事前に了解すること（例：PJMO（プ

[1] DeepSeek 等の生成 AI の業務利用に関する注意喚起（事務連絡）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/d2a5bbd2-ae8f-450e-adaa-33979181d26a/e7bfeba7/20250206_councils_social-promotion-executive_outline_01.pdf

ロジェクト推進組織のこと。ProJect Management Office の略字）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~~または~~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。）。

- 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（例外として、要機密情報を取扱う場合〇〇省情報セキュリティポリシーに基づき、情報セキュリティ責任者の許可が必要。）。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活用する場合には、〇〇省情報セキュリティポリシーに基づき、利活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。

※「DeepSeek 等の生成 AI の業務利用に関する注意喚起（事務連絡）」[2]についても併せて確認されたい。

（2）利活用中のルール

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、~~生成 AI システムの利用目的の範囲内で、要機密情報や個人情報の入力の可否を含む利用方法を遵守し、当該生成 AI システムを適切に利活用すること（例：生成 AI システムの提供者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 システムを活用する。生成 AI システムの提供者から説明された利用目的範囲外の利活用や禁止されている場合には要機密情報の入力をしない。）。
- 生成 AI システムに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、当該個人情報の利用目的のための必要最小限の利活用又は提供であることを十分に確認すること（例：〇〇省のプライバシーポリシーや生成 AI システムの提供者が定める利活用ルールを確認し、問題がないかを判断したうえで利活用、判断がつ

[2] DeepSeek 等の生成 AI の業務利用に関する注意喚起（事務連絡）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/d2a5bbd2-ae8f-450c-adaa-33979181d26a/e7bfeba7/20250206_councils_social-promotion-executive_outline_01.pdf

~~付~~かない場合は個人情報を含まないプロンプトとする。)。

- 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活用しないこと等を十分に確認すること。
- 正確性が求められる場面では特に、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 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。)。
- プロンプトの入力において、知的財産権等などの侵害等リスクを低減させるよう対策を取ること（表１参照)。既存の著作物への依拠性がないことを説明できるよう、生成に用いたプロンプト等、AI 生成物の生成過程を確認可能な状態にしておくよう努めること。

※知的財産権等のリスクに対する対策例の詳細に関しては、「コンテンツ制作のための生成 AI 利活用ガイドブック」（令和６年７月５日経済産業省）や「AI と著作権に関するチェックリスト＆ガイダンス」（令和６年７月 31 日文化庁著作権課）を確認されたい。

表　１　プロンプト入力段階の知的財産権等の対策の例[3]

場面	対策例
①著作物の利用	他人の著作権と同一・類似の表現が出力されないよう、他人の特定の著作物と関連付けるようなプロンプトを入力しない、自ら創作して手描きしたラフ画など、自らの著作物を読み込ませた上で出力する 等
②登録意匠・登録商標、他人の商品等表示・商品形態の利用	特定の登録意匠・登録商標などと関連するようなプロンプトを入力しない 等

[3] 本表１は、「コンテンツ制作のための生成 AI 利活用ガイドブック」（令和６年７月５日経済産業省）をもとに作成している。なお、生成 AI の利活用場面は様々に想定され、ゆえに発生し得るリスクや検討すべき対応策は利活用場面ごとに様々であり、リスクや対策例は本利活用ルールに記載されたものに限られないため、利活用場面に応じて個別具体的に判断し適切な対策をとること。

③人の肖像の利用	特定の人物と関連するようなプロンプトを入力しない、特定の人物の肖像を含むデータ自体を入力しない 等
④人の声の利用	特定の人物と関連するようなプロンプトを入力しない、特定の人物の声を含むデータ自体を入力しない 等

② AI 生成物利活用におけるルール

- 生成 AI の出力結果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 AI 生成物について説明できることを確かめたうえで業務利活用する。必要に応じて AI 生成物を言い換えて~~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 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、要機密情報を入力、参照又は学習した場合の出力結果の機密性、出力結果に含まれるバイアス、音声文字起こしの固有名詞等の誤りなどに留意して、業務に活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活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修正又は削除~~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。）。
- 生成 AI を活用して職務上作成した文書の取扱いについては、公文書管理法（平成 21 年法律第 66 号）等[4]を踏まえて、適切に管理すること。なお、チャット等の入出力結果についても、組織的に共有を行った場合には行政文書となり得る。
- 生成 AI システム特有のリスクケースのうち特に重大なものを検知した場合に、迅速に AI 統括責任者（CAIO）（xxx@xxx.go.jp）に報告をすること（例：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

[4] 生成 AI を活用して作成した文書の扱いについて、「デジタル技術を用いた行政文書の作成・管理等について」（令和７年２月 14 日 内閣府大臣官房公文書管理課長通知）では、「行政機関の職員が AI を活用して職務上作成した文書（審議会の議事録原案等）は、行政機関において、組織的に用いるものとして保有されれば行政文書になるが、文書の正確性を確保するため、必要な確認を経ることが重要である」とされている。

きな問題となり得る出力を行った。)。

- AI 生成物については著作物性が認められるとは限らないため、著作物として保護が必要な成果物等の作成に生成 AI を利用することは慎重に検討すること。
- AI 生成物（やそれを編集・加工したもの）を利用する上では、既存の著作物の著作権を侵害するものでないこと（特に、既存の著作物と類似したものとなっていないこと等）やその他知的財産権等を侵害するものでないかどうかを必ず確認すること。そのうえで、可能な確認措置（インターネット検索等）を行っていることを適切に説明できるようにしておくことが望ましい。AI 生成物（やそれを編集・加工したもの）に知的財産権等に係るリスクがある場合には、利用（インターネットでの配信、複製物の譲渡等）を避ける、権利者から許諾を得る、類似しないように作成し直した上で利用すること（表２参照)。

表 ２　AI 生成物の利用段階の知的財産権等の対策の例[5]

場面	対策例
①著作物の利用	• 生成 AI を利用しない従来のコンテンツ制作と同様に、AI 生成物（やそれを編集・加工したもの）について、他人の著作物と同一・類似でないかどうかを、インターネット検索等を用いて確認する • 他人の著作物と同一・類似の場合には、利用を避ける、権利者から許諾を得る、類似しないように作成しなおしたうえで利用する 等
②登録意匠・登録商標、他人の商品等表示・商品形態の利用	• 生成 AI を利用しない従来のコンテンツ制作と同様に、AI 生成物（やそれを編集・加工したもの）について、登録意匠・登録商標などと同一・類似でないかどうかを、インターネット検索等により確認する • 登録意匠・登録商標などと同一・類似と考えられる場合には、利用を避ける、権利者から許諾を得る、類似しないように作成しなおしたうえで利用する 等

[5] 本表２は、「コンテンツ制作のための生成 AI 利活用ガイドブック」（令和６年７月５日経済産業省）をもとに作成している。なお、生成 AI の利活用場面は様々に想定され、ゆえに発生し得るリスクや検討すべき対応策は利活用場面ごとに様々であり、リスクや対策例は本利活用ルールに記載されたものに限られないため、利活用場面に応じて個別具体的に判断し適切な対策をとること。

③人の肖像の利用	• 生成 AI を利用しない従来のコンテンツ制作と同様に、AI 生成物（やそれを編集・加工したもの）としての人の肖像を利用するうえでは、特定の人物の肖像との同一性（同定可能性）をインターネット検索等により確認したうえで、肖像権侵害とならないかを検討する。また、顧客吸引力を有する人物の肖像との同一性がある場合は、パブリシティ権侵害とならないかを検討する • 肖像権・パブリシティ権侵害の可能性がある場合は、利用を避ける、権利者から許諾を得る、同定可能性がないように又は権利侵害がないように作成し直したうえで利用する 等
④人の声の利用[6]	• 生成 AI を利用しない従来のコンテンツ制作と同様に、AI 生成物（やそれを編集・加工したもの）としての人の声を利用するうえでは、特定の人物の声との同一性（同定可能性）をインターネット検索等により確認したうえでパブリシティ権侵害とならないかを検討する。 • パブリシティ権侵害の可能性がある場合は、利用を避ける、権利者から許諾を得る、同定可能性がないように又は権利侵害がないように作成し直したうえで利用する 等

3. 問い合わせ先

本ルールに関する問い合わせ先は、〇〇省〇〇担当（yyy@yy.go.jp）とする。

なお、各種生成 AI システムについては、各種生成 AI システム提供者の窓口担当（※生成 AI システムの利活用に係る個別ルールが設けられている場合には、当該ルールに準拠すること）に問い合わせること。

以上

[6] 肖像や声の保護に関しては、不正競争防止法や裁判例における考え方の整理がされている。
経済産業省、2025 年「肖像と声のパブリシティ価値に係る現行の不正競争防止法における考え方の整理について」
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/shozo_koe.pdf

本チェックシートの概要

別紙３

本チェックシートは、生成AIシステムを調達する際に、事業者を評価・選定するための項目を整理したものである。
企画者は生成AIシステムの調達にあたって、調達仕様書を作成する際には、本チェックシートを参考にする。（【別紙４】契約チェックシート（生成AIシステム用）も併せて参考にし、調達仕様書に盛り込むことが適当な場合は、調達仕様書に盛り込む）
ただし、本チェックシートは「生成AIシステムの調達」に関して特有の留意すべき項目のみ掲載しており、別途「デジタル・ガバメント推進標準ガイドライン」の内容や、「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の別紙「調達仕様書テンプレート」等を参照し調達仕様書を作成する必要がある。
なお、本チェックシートでは、「【別紙３】調達チェックシート（生成AIシステム用）」を「調達チェックシート」、「【別紙４】契約チェックシート（生成AIシステム用）」を「契約チェックシート」と表現する。

本チェックシートの構成

■「調達チェックシート」シート

分類	評価観点#	評価観点	評価・選定時の項目の分類	要求事項#	※調達仕様書で事業者に遵守を求める内容を記載 ※本ガイドライン「6.1.2　本ガイドラインに基づく対応事項」に記載のとおり、導入類型、プロジェクトフェーズ、リスクレベル等を踏まえ、各対応事項の要求レベルや一部要求事項の取捨選択又は拡充を検討する。 要求事項
組織要件	1	AI事業者ガイドライン等遵守の契約の遵守	基本項目	1	AI事業者ガイドライン等遵守を契約・実施・可能としていることの証憑が提出できること
	2	AIガバナンスの構築	基本項目	2	生成AIシステムの開発・運用に関して、AIガバナンス（※）が構築されていること ※AIにおける正のインパクトを最大化しつつ、AIによるリスクを受容可能な水準で管理する組織の仕組み・体制
	3	AI開発や運用の注意等の勧告の把握	基本項目	3	生成AIシステムの開発・運用において、政府から提供される、AI開発や運用の技術等の勧告を把握していること
	4	情報セキュリティインシデント（生成AIシステム特有のリスクケース（事業者に責任の範囲に属するもの）に限る。）対応体制・手順を構築していること（例：24時間サービスの違いで、利用者からのインシデント報告を受け付け、即応の協力をすることを含む。）	基本項目	4	情報セキュリティインシデント（生成AIシステム特有のリスクケース（事業者に責任の範囲に属するもの）に限る。）対応体制・手順を構築していること（例：24時間サービスの違いで、利用者からのインシデント報告を受け付け、即応の協力をすることを含む。）
	5	関係者への生成AIに関する教育・リテラシー向上	基本項目	5	生成AIシステムの開発・運用に従事する者または組織において、生成AIに関するリテラシー向上の取組を実施していること
開発・運用工程要件	6	データの取扱い	基本項目	6	生成AIシステムへの入力および学習に使用されるデータの取扱いを適切に管理していること
	7	アウトプットの妥当性検証	基本項目	7	生成AIシステムの運用開始前および定期的な検証を行っていること
	8	ベンダーロックインの回避	基本項目	8	利用している生成AIモデルのバージョン更新を踏まえて契約を結べること
			任意選択項目（追加項目）	9	生成AIシステムに入力されるプロンプトやパラメータが開示されていないことの確認のために、必要に応じ開発・運用への情報提供や情報提供ができる体制であること

A列 分類　C列 評価観点　D列 評価・選定時の項目の分類　F列 要求事項

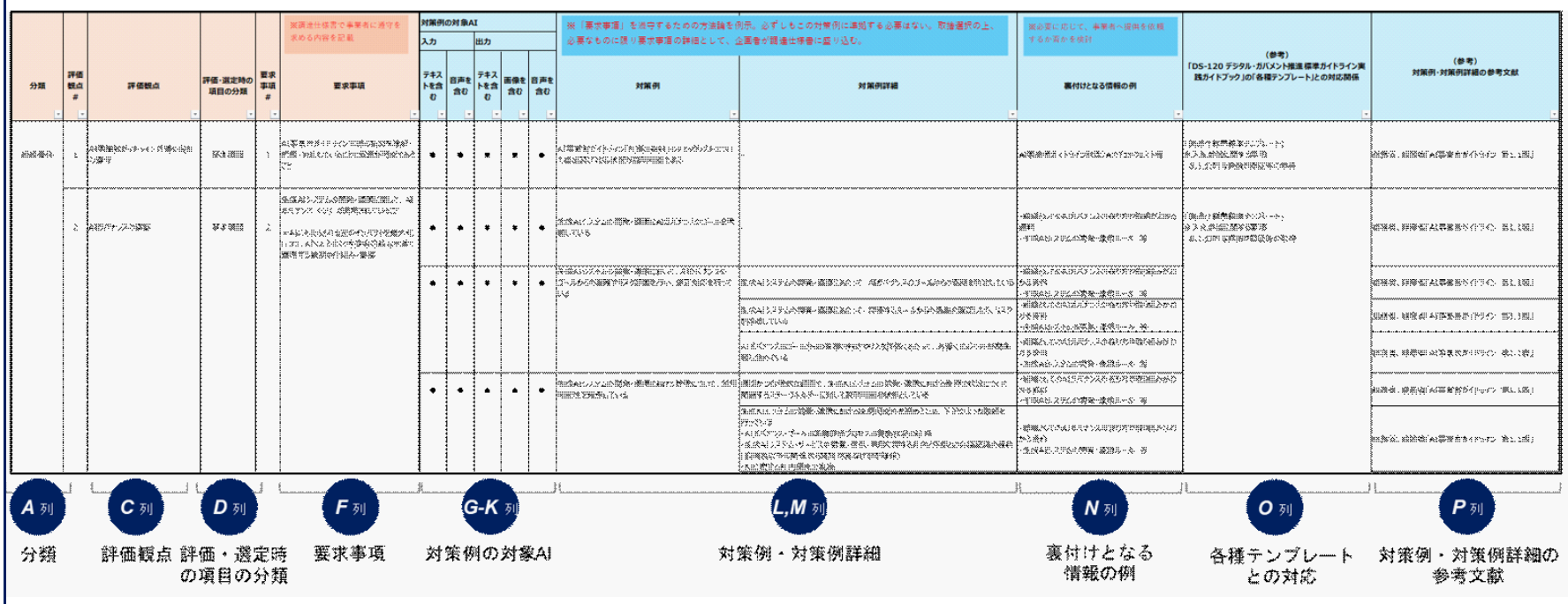
【A列：分類】
事業者を評価する大枠として「組織要件」「開発・運用工程要件」「生成AIシステムの基本機能要件」を定めている。「C列：評価観点」「F列：要求事項」を大別するための列

【C列：評価観点】
要求事項を遵守する目的や観点を記載

【D列：評価・選定時の項目の分類】
原則必須の要求事項を把握するための列。「要求事項」のうち、政府機関が調達する生成AIシステムに原則要求すべきと考えられる事項については、「基本項目」として設定している。~~原則必須とする項目には「基本項目」、~~「基本項目」としている要求事項は、調達時に応募者に求める事項として盛り込むことを原則とする。その条件を満たす場合に原則必須とする項目には「〇〇の場合は適用」と記載している。「任意追加項目（加点項目）」としている要求事項は、必要に応じ考慮した方が良い観点であり、調達の評価項目の加点項目とすることを想定したものである。~~原則必須ではないが考慮した方がよい観点を「任意追加項目（加点項目）」と記載~~

【F列：要求事項】
調達仕様書で事業者に遵守を求める内容を記載。本ガイドライン「6.1.2　本ガイドラインに基づく対応事項」に記載のとおり、導入類型、プロジェクトフェーズ、リスクレベル等を踏まえ、各対応事項の要求レベルや一部要求事項の取捨選択又は拡充を検討する。

■「（参考）要求事項の参考」シート



【A列：分類】
事業者を評価する大枠として「組織要件」「開発・運用工程要件」「生成AIシステムの基本機能要件」を定めている。「C列：評価観点」「F列：要求事項」を大別するための列

【C列：評価観点】
要求事項を遵守する目的や観点を記載

【D列：評価・選定時の項目の分類】
原則必須の要求事項を把握するための列。「要求事項」のうち、政府機関が調達する生成AI システムに原則要求すべきと考えられる事項については、「基本項目」として設定している。~~原則必須とする項目には「基本項目」、~~「基本項目」としている要求事項は、調達時に応募者に求める事項として盛り込むことを原則とする。その条件を満たす場合に原則必須とする項目には「〇〇の場合は適用」と記載している。「任意追加項目（加点項目）」としている要求事項は、必要に応じ考慮した方が良い観点であり、調達の評価項目の加点項目とすることを想定したものである。~~原則必須ではないが考慮した方がよい観点を「任意追加項目（加点項目）」と記載~~

【F列：要求事項】
調達仕様書で事業者に遵守を求める内容を記載。本ガイドライン「6.1.2　本ガイドラインに基づく対応事項」に記載のとおり、導入類型、プロジェクトフェーズ、リスクレベル等を踏まえ、各対応事項の要求レベルや一部要求事項の取捨選択又は拡充を検討する。

【G-K列：対策例の対象AI】
それぞれの対策例が対象とする生成AIを記載。ガイドラインの対象AIであるテキスト・音声入力、テキスト・音声・画像出力AIを対象としフラグ付けしている。

【~~G列・H列~~L列・M列：対策例・対策例詳細】
「F列：要求事項」を遵守するための方法論を例示。必ずしもこの対策例に準拠する必要はない。取捨選択の上、必要なものに限り要求事項の詳細として、企画者が調達仕様書に盛り込む。なお、本情報は企画者のための参考情報であり、調達仕様書に記載された事項に対する対策は事業者により提案されるべきものである。企画者は、調達するAIの特徴を踏まえ、事業者から提案される対策を評価する。

【~~I~~N列：裏付けとなる情報の例】
要求事項を満たしているか否かを判断するための情報を例示。必要に応じて、事業者へ提供を依頼するか否かを検討する。

【~~J~~O列：（参考）「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の「各種テンプレート」との対応関係】
「デジタル・ガバメント推進標準ガイドライン」や「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の別紙「調達仕様書テンプレート」、「要件定義書テンプレートとの対応関係。調達仕様書の作成においては、これらの各種テンプレートを参考とする。

【P列：（参考）対策例・対策例詳細の参考文献】
「L列・M列：対策例・対策例詳細」を作成するにあたり参照した政府機関のガイドライン等を記載。

※対策例、対策例詳細、裏付けとなる情報の例について、技術やビジネス等の変化状況を踏まえ、柔軟に記載の更新を検討していく予定である。

本チェックシートの利用方法

・企画者は、「F列：要求事項」から必要なものを調達仕様書に取り込む。
　※その際、「D列：評価・選定時の項目の分類」を参考にする。「基本項目」は事業者の評価・選定にあたり、原則必須とすることを想定とする項目である。
　※「任意追加項目（加点項目）」は必須ではないが考慮した方が良い観点であり、評価項目に含める場合、加点要素とすることを想定とする項目である。
　※「府省庁外利用の場合は適用」「個人情報を取り扱う場合は適用」等の記載がある要求事項は、当該案件がその条件を満たす場合に原則必須とすることを想定とする項目である。
　※「~~G列・H列~~L列・M列：対策例・対策例詳細」はあくまで例示であり、すべてを満たす必要はなく、また例示している方法以外で遵守されていても問題ない。
　※別途、「デジタル・ガバメント推進標準ガイドライン」が求める「調達仕様書テンプレート」を参照し、政府情報システムの調達に必要な項目も取り込むこと。
・企画者は、事業者へ提供を依頼する情報を「~~X~~N列：裏付けとなる情報の例」を参考に定める。
・企画者は、調達仕様書を候補となる事業者に展開し提案依頼を行う。
・企画者は、事業者の提案・回答をもとに、事業者を評価・選定する。

本チェックシートの対象

本チェックシートは、「2.2.1　本ガイドラインが対象とする情報システム」に記載した政府情報システムのうち、「2.2.2　本ガイドラインが対象とする生成AI」に記載した生成AIを構成要素とするシステムに適用するものとする。

用語の補足

・大規模言語モデル（LLM）：文章や単語の出現確率を深層学習モデルとして扱う言語モデルを、非常に大量の訓練データを用いて構築したもの。（出典：AIプロダクト品質保証コンソーシアム「AIプロダクト品質保証ガイドライン」~~10-1~~P.10-2）
・生成AI：文章、画像、プログラム等を生成できるAIモデルに基づくAIの総称。（出典：「AI事業者ガイドライン」P.10）
・生成AIシステム：~~本ガイドラインが対象とする生成AIを構成要素とする政府情報システム（クラウドサービスも含む）。（AISI「AIセーフティに関する評価観点ガイド（第 1.01 版）」P.9に基づき作成）~~生成AIを構成要素とするAIシステム。（「AI事業者ガイドライン」P.9、P.10に基づき作成）なお、本ガイドラインにおいて、「生成AIシステム」の語は、本ガイドラインが対象とする生成AIモデルを構成要素とする生成AIシステムを指すものとしている。
・生成AIモデル：文章、画像、プログラム等を生成できるAIモデル。（「AI事業者ガイドライン」P.10に基づき作成）なお、本ガイドラインにおいて、「生成AIモデル」の語は、本ガイドラインが対象とする生成AIモデルを構成要素とする生成AIモデルを指すものとしている。
・学習用の生データ：ユーザから事業者に提供された、~~学習時に生成AIシステムにインプット~~生成AIモデルの学習時に活用するためのデータ。
・学習用データ：ユーザから提供された学習用の生データを用いて、事業者による処理・加工等により作成した学習用のデータ。
・情報セキュリティインシデント：JIS Q 27000:2019における情報セキュリティインシデントをいう。
・生成AIシステム特有のリスクケース：生成AIシステムの特有のリスクが顕在化した状態又はその可能性を有する兆候や事象が認められる状態のうち、重大な影響を及ぼし得るもの。

調達チェックシート						（参考）要求事項の参考								
						対策例の対象AI					※「要求事項」を遵守するための方法論を例示。必ずしもこの対策例に準拠する必要はない。取捨選択の上、必要なものに限り要求事項の詳細として、企画者が調達仕様書に盛り込む。		※必要に応じて、事業者へ提供を依頼するか否かを検討		
					※調達仕様書で事業者に遵守を求める内容を記載	入力		出力						（参考） 「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の「各種テンプレート」との対応関係	（参考） 対策例・対策例詳細の参考文献
分類	評価観点#	評価観点	評価・選定時の項目の分類	要求事項#	要求事項	テキストを含む	音声を含む	テキストを含む	画像を含む	音声を含む	対策例	対策例詳細	裏付けとなる情報の例		
組織要件	1	AI事業者ガイドライン共通の指針の遵守	基本項目	1	AI事業者ガイドライン共通の指針を理解・把握・対応していることの宣言が可能であること	●	●	●	●	●	AI事業者ガイドライン「共通の指針」のチェックリストについて提出及び対応状況~~が~~を説明可能~~である~~とする	-	AI事業者ガイドライン別添7Aのチェックリスト等	「調達仕様書標準テンプレート」 8.入札参加に関する事項 8.1.公的な資格や認証等の取得	総務省、経産省「AI事業者ガイドライン　第1.1版」
	2	AIガバナンスの構築	基本項目	2	生成AIシステムの開発・運用に関して、AIガバナンス（※）が適用されていること ※AIにもたらされる正のインパクトを最大化しつつ、AIによるリスクを受容可能な水準で管理する統制の仕組み・業務	●	●	●	●	●	生成AIシステムの開発・運用にAIガバナンスのゴールを考慮~~してい~~する	-	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等	「調達仕様書標準テンプレート」 8.入札参加に関する事項 8.1.公的な資格や認証等の取得	総務省、経産省「AI事業者ガイドライン　第1.1版」
						●	●	●	●	●	生成AIシステムの開発・運用において、AIガバナンスのゴールからの乖離やリスク評価を行い、是正対応を行~~っていな~~う	生成AIシステムの開発・運用にあたって、AIガバナンスのゴールからの乖離を特定~~してい~~する	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
												生成AIシステムの開発・運用にあたって、関連するルールからの逸脱を確認したり、リスクを評価~~してい~~する	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
												AIガバナンスのゴールからの乖離の特定やリスク評価にあたって、必要に応じて外部関係者も含め~~てい~~る	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
						●	●	●	●	●	生成AIシステムの開発・運用における管理について、説明可能性を確保~~してい~~する	適切かつ合理的な範囲で、生成AIシステムの開発・運用における管理の状況について関連するステークホルダーに対して説明可能な状態と~~してい~~する	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
												生成AIシステムの開発・運用における説明可能性を高めるため、下記のような取組を行~~っていな~~う □AIガバナンス・ゴールの乖離評価プロセスの実施状況の記録 □生成AIシステム・サービスの開発・提供・利用に関する社内/外部との会議記録の保持(担当者以外の関係者も閲覧可能な状態を確保) □AIに関する社内研修の実施	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
												生成AIシステムの以下の事項について定められ、ユーザーに適時かつ適切に情報を提供~~してい~~する ・適切/不適切な使用方法等 ・提供する生成AIシステムの技術的特性、安全性確保の仕組み、利用によりもたらす結果より生じる可能性のある予見可能なリスク及びその緩和策等の安全性に関する情報 ・生成AIシステムの学習等による出力又はプログラムの変化の可能性 ・生成AIシステムの動作状況に関する情報、不具合の原因及び対応状況、情報セキュリティインシデント・生成AIシステム特有のリスクケース事例等 ・生成AIシステムの更新を行った場合の更新内容及びその理由の情報 ・生成AIにて学習するデータの収集ポリシー、学習方法、実施体制等 ・サービス規約やプライバシーポリシー ・生成AIシステムの学習等による出力又はプログラムの変化の可能性 ・開発時に想定していない提供・利用により危害が発生することを避けるためのAI開発者が意図する利用範囲 ・生成AIシステムの動作状況に関する情報、不具合の原因及び対応状況	・ユーザーへの説明書や契約書等、事業者のHPや製品パンフレット等で左記項目が含まれた資料 ・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
												乖離評価プロセスの実施状況の記録については、独自に乖離評価のためのチェックリストを作成し、それをもとに確認・記録~~してい~~する	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
						●	●	●	●	●	生成AIシステムの開発・運用における管理について、その管理手法や機能そのものが適切であるか検証を行~~っていな~~う	生成AIシステムの開発・運用における管理が適切に機能しているか否かのモニタリングを行~~っていな~~う	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
												モニタリングの結果をもとに、継続的な改善を実施~~してい~~する	・組織としてのAIガバナンスの在り方や取組がわかる資料 ・生成AIシステムの開発・運用ルール　等		総務省、経産省「AI事業者ガイドライン　第1.1版」
	3	AI業界や最新技術等の動向の把握	基本項目	3	生成AIシステムの開発・運用において、品質や説明性を高めるため、AI業界や最新技術等の動向を把握していること	●	●	●	●	●	生成AIシステムの開発・運用に関係する、業界ガイドラインや法令、最新技術を把握~~してい~~する	産業技術総合研究所の「機械学習品質マネジメントガイドライン」等の標準化に向けた取組を参照~~してい~~する	参照している業界ガイドラインや技術のリスト	「調達仕様書標準テンプレート」 8.入札参加に関する事項 8.1.公的な資格や認証等の取得	総務省、経産省「AI事業者ガイドライン　第1.1版」
												AI関連の研究会や業界団体などへの所属、最新技術の把握、専門家との意見交換等を実施~~してい~~する	加盟しているAI関連の研究会や業界団体リスト		総務省、経産省「AI事業者ガイドライン　第1.1版」
	4	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応	基本項目	4	情報セキュリティインシデント・生成AIシステム特有のリスクケース（事業者の責任の範囲に属するものに限る。）対応体制・手順を整備していること（開発・運用するサービスにおいて、利用者からインシデント報告を受け付け、対応の協力をすることを含む。）	●	●	●	●	●	情報セキュリティインシデント・生成AIシステム特有のリスクケース対応体制・手順を整備~~してい~~する	生成AIシステムの開発・運用時に発生する情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応体制や方針及び計画を策定~~してい~~する	・AIガバナンス関連ルール（情報セキュリティインシデント・生成AIシステム特有のリスクケース対応体制・手順が整備されていることが分かる資料）等	「調達仕様書標準テンプレート」 6.作業の実施に当たっての遵守事項 6.1.機密保持、資料の取扱い 「要件定義書標準テンプレート」 3.非機能要件定義 3.10. 情報セキュリティに関する事項	-
												情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時に備え以下のような体制をあらかじめ整備~~してい~~るかする ・連絡受付窓口の設置 ・プロジェクトに対し責任ある役職者のアサイン ・対応担当者個々の役割分担 ・対応アプローチ・プロセス ・影響を受けるステークホルダーに対して通知するプロセス等	・AIガバナンス関連ルール（情報セキュリティインシデント・生成AIシステム特有のリスクケース対応体制・手順が整備されていることが分かる資料）等		-
						●	●	●	●	●	情報セキュリティインシデント・生成AIシステム特有のリスクケース対応に関する教育や訓練を実施~~してい~~する	生成AIシステムの開発・運用時に発生する情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応方針及び計画について、適宜実践的な予行演習を実施~~してい~~する	・AIガバナンス関連ルール（情報セキュリティインシデント・生成AIシステム特有のリスクケース対応体に関する教育や訓練されていることが分かる資料）等		-
	5	関係者への生成AIに関する教育・リテラシー向上	基本項目	5	生成AIシステムの開発・運用に従事する者~~または~~又は組織について、生成AIに関するリテラシー向上の取組を実施していること	●	●	●	●	●	生成AI開発・運用に従事する者が適切なリテラシー（生成AI関連の技術知識やリスク、倫理等）を具備できるよう、役割に応じた教育や訓練を実施~~してい~~する	-	・AIガバナンス関連ルール（教育・訓練等、AIリテラシーの向上の取組を実施していることが分かる資料）等	「調達仕様書標準テンプレート」 5.作業の実施体制・方法に関する事項 5.2作業要員に求める資格等の要件	総務省、経産省「AI事業者ガイドライン　第1.1版」
開発・運用工程要件	6	データの取扱い	基本項目	6	生成AIシステムへの入出力~~または~~又は処理されるデータの取扱いを適切に管理していること	●	●	●	●	●	プロジェクトの目的に照らし、必要な範囲でインプット（プロンプト、学習用の生データ等）の利用目的や利用条件を定め~~てい~~る	-	事業者によるインプット（プロンプト、学習用の生データ等）の利用目的を定めていることがわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.2.システム方式に関する事項 3.3.システム規模に関する事項 3.10.情報セキュリティに関する事項	経産省「AIの利用・開発に関する契約チェックリスト」
						●	●	●	●	●	プロジェクトの目的に照らし、必要な範囲でインプット（プロンプト、学習用の生データ等）の管理・セキュリティ体制を定めており、問題が生じないよう対策を講じ~~てい~~る	-	インプット（プロンプト、学習用の生データ等）の管理・セキュリティ体制方針がわかる資料等		経産省「AIの利用・開発に関する契約チェックリスト」
						●	●	●	●	●	プロジェクトの目的に照らし、必要な範囲でインプット（プロンプト、学習用の生データ等）の保持期間及び消去を管理しており、問題が生じないよう対策を講じ~~てい~~る	-	インプット（プロンプト、学習用の生データ等）の保持期間及び消去の管理方針がわかる資料等		経産省「AIの利用・開発に関する契約チェックリスト」
						●	●	●	●	●	プロジェクトの目的に照らし、必要な範囲でインプット（プロンプト、学習用の生データ等）の外部提供管理として、生成AIシステムのユーザーに対して提供する義務を定めた上での管理を~~してい~~する	-	インプット（プロンプト、学習用の生データ等）をユーザーに対して提供する義務ををを定めていることがわかる資料等		経産省「AIの利用・開発に関する契約チェックリスト」
						●	●	●	●	●	プロジェクトの目的に照らし、必要な範囲でインプット（プロンプト、学習用の生データ等）の外部提供管理として、第三者提供に関しての管理を~~してい~~する	-	インプット（プロンプト、学習用の生データ等）の第三者提供に関する管理方針がわかる資料等		経産省「AIの利用・開発に関する契約チェックリスト」
						●	●	●	●	●	プロジェクトの目的に照らし、必要な範囲でインプット処理結果（学習用データ、中間生成物、派生的知的財産等）の使用・利用に関しての管理を~~してい~~する	-	インプット処理結果（学習用データ、中間生成物、派生的知的財産等）の使用・利用に関する管理方針がわかる資料等		経産省「AIの利用・開発に関する契約チェックリスト」
						●	●	●	●	●	プロジェクトの目的に照らし、必要な範囲でインプット処理結果（学習用データ、中間生成物、派生的知的財産等）の外部提供に関しての管理を~~してい~~する	-	インプット処理結果（学習用データ、中間生成物、派生的知的財産等）の外部提供に関する管理方針がわかる資料等		経産省「AIの利用・開発に関する契約チェックリスト」
						●	●	●	●	●	プロジェクトの目的に照らし、必要な範囲で学習前・学習全体を通じて、データのアクセスを管理するデータ管理・制限機能の導入検討を行う等、適切な保護措置を実施~~可能である~~する	-	学習前・学習全体を通じて、データの保護措置の方針がわかる資料等		経産省「AIの利用・開発に関する契約チェックリスト」
	7	アウトプットの品質保証	基本項目	7	生成AIシステムの期待品質を満たすための取組を行っていること	●	●	●	●	●	生成AIをチャットで用いる場合、チャットでの利用の期待品質を定め、その基準を満たしているかの測定及び評価を~~してい~~する	-	ベンチマーク~~（JMMLU、JHumanEval、JBBQ等）~~※等を使用した評価基準とその評価内容がわかる資料等 ※一定の信頼性のある評価基準に基づく独自の評価を否定するものではない	「要件定義書標準テンプレート」 3.非機能要件定義 3.12.テストに関する事項 3.17.保守に関する事項	デジタル庁「テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）」
						●	●	●	●	●	生成AIの期待品質を満たしているか、テストケースを用いて評価する。その際テストケースは複数提案する （バッチ処理、情報検索、自然言語からのプログラム作成等）	プロンプトを入力した生成AIの出力を検査することで、生成AIシステムの明示された要求仕様が規定する機能を生成AIモデルが実現可能かを調べている。プロンプトと生成AIモデルの組み合わせを対象とした試行錯誤的な繰り返し（一種のプロトタイピング開発スタイル）を通して、機能要求満足性を評価する	バッチ処理で生成AIを用いる場合、テストケース例とテスト方針がわかる資料等		対策例：デジタル庁「テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）」 対策例詳細：産総研「生成AI品質マネジメントガイドライン　第１版」
						●	●	●	●	●	マーケティング等で実施されるアンケートによる定性的な満足度評価手法を生成AIシステムの機能要求満足性の評価に用いて、機能要求満足性を満たしているか検証する	-	マーケティング等で実施されるアンケートによる定性的な満足度評価手法を生成AIシステムの機能要求満足性の評価に用いて、機能要求満足性を満たしているかの検証方針がわかる資料等		産総研「生成AI品質マネジメントガイドライン　第１版」
						●	●	●	●	●	生成AIシステム出力のサンプリング手法やそのパラメータを指定できる場合、システムプロンプトの設計のための試行錯誤の中で合わせて検討する	-	生成AIシステム出力のサンプリング手法やそのパラメータを指定できる場合、システムプロンプトの設計と合わせて指定する開発方針がわかる資料等		産総研「生成AI品質マネジメントガイドライン　第１版」
						●	●	●	●	●	生成AIシステムの機能要求水準を満たすのに十分な検索精度を確保するよう対策を講じる（多くの場合、想定される問題領域のなるべく多くの範囲で、一定以上の精度が出ることがよいとされる） ※RAGを利用した生成AIシステムのみ本項目の対象	-	生成AIシステムの機能要求水準を満たすのに十分な検索精度を確保するための対策方針がわかる資料等		産総研「生成AI品質マネジメントガイドライン　第１版」

調達チェックシート						（参考）要求事項の参考								
						対策例の対象AI					※「要求事項」を遵守するための方法論を例示。必ずしもこの対策例に準拠する必要はない。取捨選択の上、必要なものに限り要求事項の詳細として、企画者が調達仕様書に盛り込む。		※必要に応じて、事業者へ提供を依頼するか否かを検討		
						入力		出力							
分類	評価観点#	評価観点	評価・選定時の項目の分類	要求事項#	※調達仕様書で事業者に遵守を求める内容を記載 要求事項	テキストを含む	音声を含む	テキストを含む	画像を含む	音声を含む	対策例	対策例詳細	裏付けとなる情報の例	（参考） 「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の「各種テンプレート」との対応関係	（参考） 対策例・対策例詳細の参考文献
	8	ベンダーロックインの回避	基本項目	8	利用している~~LLM~~生成AIモデルはバージョン情報を含めて明示可能であること	●	●	●	●	●	利用可能な~~LLM~~生成AIモデル~~および~~及びそのバージョン情報等の一覧を整理して公開する	-	利用している~~LLM~~生成AIモデルのバージョン情報の開示方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.8.中立性に関する事項 3.11.情報システム稼働環境に関する事項	デジタル庁「テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）」
			任意追加項目（加点項目）	9	生成AIシステムに入力されるプロンプトの一部やパラメータが隠蔽されていないことの確認のために、合理的な範囲での企画者への情報開示や情報提供ができる状態であること	●	●	●	●	●	合理的な範囲での開発・運用時におけるシステムプロンプト等の企画者への情報開示や情報提供が技術的に可能であることを表明し保証する	-	~~LLM~~生成AIシステムに入力されるプロンプトの一部やパラメータが隠蔽されていないことを表明した資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.8.中立性に関する事項 3.10.情報セキュリティに関する事項	デジタル庁「テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）」
			任意追加項目（加点項目）	10	過去のチャット履歴の保存機能や、プロンプトをテンプレートとして登録するとともに、それらのデータをエキスポートする機能を提供する技術を有していること	●	●	●	●	●	過去のチャット履歴の保存機能、プロンプトのテンプレート化機能、それらのエキスポート機能の開発が可能かを表明し保証する	-	過去のチャット履歴の保存機能や、プロンプトをテンプレートとして登録するとともに、それらのデータをエキスポート可能な機能の実装方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 ~~3.8.中立性に関する事項~~ 3.1.ユーザビリティ及びアクセシビリティに関する事項 3.8.中立性に関する事項 3.13.移行に関する事項	デジタル庁「テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）」
			任意追加項目（加点項目）	11	特定のモデルの利用が主たる目的ではない場合、~~LLM~~生成AIモデルごとに異なる機能や動作に影響する特徴があることを考慮し、複数の~~LLM~~生成AIモデルの中から最適な~~LLM~~生成AIモデルを選択又は組み合わせて利用する技術を有していること	●	●	●	●	●	①複数の~~LLM~~生成AIモデルが利用できること、②~~LLM~~生成AIモデルの選択ができること（組み合わせて利用する場合も含む）等の技術を有していることを表明し保証する	-	複数の~~LLM~~生成AIモデルの中から最適な~~LLM~~生成AIモデルを選択又は組み合わせて利用する技術を有している実績が分かる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.8.中立性に関する事項 3.11.情報システム稼働環境に関する事項	-
			基本項目	12	生成AIシステムのアーキテクチャ設計と実装において、ベンダーやシステムの移行の容易性も踏まえた開発や運用が可能であること	●	●	●	●	●	標準化されたインタフェースやプロトコルを活用し、AIコンポーネントを疎結合に設計する	-	標準化されたインタフェースやプロトコルを活用し、AIコンポーネントを疎結合に設計する方法の実現方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.8.中立性に関する事項 3.11.情報システム稼働環境に関する事項	AISI「CAIO設置・AIガバナンス実務マニュアル(案)」
						●	●	●	●	●	モデルやベンダーの切り替えを想定した抽象化レイヤー（アダプタ）を用意し、「出口戦略」をアーキテクチャレベルで組み込む	-	抽象化レイヤー（アダプタ）を用意し、ベンダー変更を想定したアーキテクチャを実現する方法の実現方法がわかる資料等		AISI「CAIO設置・AIガバナンス実務マニュアル(案)」
						●	●	●	●	●	コンポーネントアーキテクチャを、再利用部品である生成AIモデルの置き換えが容易になるようにデザインする	-	コンポーネントアーキテクチャを、再利用部品である生成AIモデルの置き換えが容易になるようにデザインする方法がわかる資料等		産総研「生成AI品質マネジメントガイドライン 第１版」
						●	●	●	●	●	保守性の向上のため、生成AIシステムのコンポーネントをモジュール性を考慮して開発、運用する	生成AIシステムのコンポーネントに明確な役割・責任（Responsibility）を与え、コンポーネントのモジュール性を高める。また、コンポーネントのデザインでは、入出力ポートの定義を明示する	生成AIシステムコンポーネントのモジュール性を高めた開発の方針がわかる資料等		産総研「生成AI品質マネジメントガイドライン 第１版」
												生成AIシステムを構成するアーキテクチャコンポーネントを明示することで、モジュール単位での追加・削除・置き換えに関わる修正性を向上させる	生成AIシステムを構成するアーキテクチャコンポーネントを明示する方法がわかる資料等		産総研「生成AI品質マネジメントガイドライン 第１版」
												システムプロンプトのモジュール性を高める。プロンプトの流れを段落などの観点から構造化し、各々の段落の役割・責任（Responsibility）を明確化する	システムプロンプトのモジュール性を高め、システムプロンプトの保守性を向上させる方法がわかる資料等		産総研「生成AI品質マネジメントガイドライン 第１版」
	9	生成AI~~システム~~モデルのアップデートの考慮	基本項目	1~~2~~3	メジャーアップデートもしくは移行に関する生成AI固有の観点からリスク軽減していること	●	●	●	●	●	~~LLM~~生成AIモデルのメジャーアップデートやモデルの移行前に、移行候補の~~LLM~~生成AIモデルで、アウトプットの品質や安全性等について問題ない性能を検証~~できている~~する	-	~~LLM~~生成AIモデルのアップデート前に、移行候補の~~LLM~~生成AIモデルで、アウトプットの品質や安全性等について問題ない性能かを検証可能とする仕組みの実現方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.16.運用に関する事項 3.17.保守に関する事項	デジタル庁「テキスト生成AI利活用におけるリスクへの対策ガイドブック（α版）」
	10	文化的・言語的考慮	任意追加項目（加点項目）	1~~3~~4	生成AIシステム~~のアウトプット~~が日本の言語環境や文化環境に即した出力が可能であ~~るものになる状態としている~~こと	●	●	●	●	●	日本の言語環境や文化環境を踏まえたアウトプットを出力可能な生成AIシステムを提供~~している~~する	-	日本の言語環境や文化環境に応じた出力結果となっているかの確認方針がわかる資料、開発時に学習データ等で日本の言語環境や文化環境に即したものとなるよう、取組がなされていることがわかる資料、日本語能力を測るベンチマークを活用した評価結果がわかる資料~~（例えば、日本語能力を測るベンチマークとしては、JGLUE（Japanese General Language Understanding Evaluation）、JMMLU（Japanese Massive Multitask Language Understanding Benchmark）等がある。）~~等 ※広く認知された一定の信頼性のある評価基準の使用を否定するものではない	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	-
	11	環境への配慮	任意追加項目（加点項目）	1~~4~~5	環境に配慮した生成AIシステムを開発・提供すること	●	●	●	●	●	電力効率が高い半導体を使用したハードを基に学習されたモデルを利用する等の環境への配慮をした生成AIシステムを提供している又は利用~~している~~する	システムテストに相当するソフトウェアテスティングで、システムが所与の機能仕様を適切に実現していることを検査し時間効率性及び資源効率性を評価する	消費電力等環境性能が優れていることがわかる資料等	「調達仕様書標準テンプレート」 4.作業の実施内容に関する事項 4.17.その他	対策例詳細：産総研「生成AI品質マネジメントガイドライン 第１版」
生成AIシステムの基本機能要件	12	有害情報の出力制御	基本項目	1~~5~~6	テロや犯罪に関する情報や攻撃的な表現など、生成AIシステムによる有害情報の入出力~~を制御制限等を~~していること	●	●	●	●	●	有害情報を入力あるいは想定出力に含むテストデータを入力した際、生成AIシステムの出力に当該情報が含まれない、もしくは出力を拒否できるような仕組みを~~提供する技術を有している~~具備する	サイバー攻撃やテロなどの犯罪、CBRN（Chemical, Biological,Radiological,Nuclear）に利用され得る情報を入力あるいは想定出力に含むテストデータを入力した際、生成AIシステムの出力に有害情報が含まれない、もしくは出力を拒否することができるような仕組みを~~提供する技術を有している~~具備する	サイバー攻撃やテロなどの犯罪、CBRNに利用され得る情報を入力あるいは想定出力に含むテストデータを入力した際、生成AIシステムの出力に有害情報が含まれない、もしくは出力を拒否することができるような仕組みの実現方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												差別表現などエンドユーザーが精神的な被害を受け得る情報を入力あるいは想定出力に含むテストデータを入力した際、生成AIシステムの出力に有害情報が含まれない、もしくは出力を拒否することができるような仕組みを~~提供する技術を有している~~具備する	差別表現などエンドユーザーが精神的な被害を受け得る情報を入力あるいは想定出力に含むテストデータを入力した際、生成AIシステムの出力に有害情報が含まれない、もしくは出力を拒否することができるような仕組みの実現方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	生成AIシステムの出力の有害性スコア（攻撃的であるかどうかなどの有害さを数値で表したもの）の測定及び評価~~をしている~~する	-	生成AIシステムの出力の有害性スコア及びスコアの測定方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	-	●	●	●	テキストの入力に、虚偽の情報や意味不明な内容、複雑な内容が含まれる場合、モデルの挙動が不安定になることがある。そのような入力に対しても、有害な出力を抑制できるような仕組みを具備する	-	画像やテキストの入力に、虚偽の情報や意味不明な内容、複雑な内容が含まれる場合、モデルの挙動が不安定になることがある。そのような入力に対しても、有害な出力を抑制できるような仕組みの実現方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
	13	偽誤情報の出力・誘導の防止	基本項目	1~~6~~7	生成AIシステムによる偽誤情報の出力の防止措置を取っていること	●	●	●	●	●	異なる~~LLM~~生成AIモデルに対し、事実を問う内容の同一のテストデータを入力した際、意味的に同一の内容が出力され、かつ正しい内容となるよう対策を講じ~~てい~~る	-	異なる~~LLM~~生成AIモデルに対し、事実を問う内容の同一のテストデータを入力した結果が記載された資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	偽誤情報の出力防止に関する評価項目のスコアを測定した結果、スコアに問題がないことを確認~~している~~する	生成AIシステムに対するプロンプトと出力データの関連性に係るスコアの測定及び評価~~をしている~~する	生成AIシステムに対するプロンプトと出力データの関連性に係るスコア及びスコアの測定方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												生成AIシステムの出力データとRAGによる検索結果の関連性に係るスコアの測定及び評価~~をしている~~する ※RAGを利用した生成AIシステムのみ本項目の対象	生成AIシステムの出力データとRAGによる検索結果の関連性に係るスコア及びスコアの測定方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												生成AIシステムの出力データとRAGによる検索結果の一貫性に係るスコアの測定及び評価~~をしている~~する ※RAGを利用した生成AIシステムのみ本項目の対象	生成AIシステムの出力データとRAGによる検索結果の一貫性に係るスコア及びスコアの測定方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												正解データとRAGによる検索結果の意味的な一貫性に係るスコアの測定及び評価、~~をしている~~する ※RAGを利用した生成AIシステムのみ本項目の対象	正解データとRAGによる検索結果の意味的な一貫性に係るスコア及びスコアの測定方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												出力にコンテンツ認証がなされる生成AIシステムにおいて、様々なプロンプトを入力した場合でも適切にコンテンツ認証がなされる仕組みを~~提供する技術を有している~~具備する	生成AIシステムへ入力した様々なプロンプトに対し、適切なコンテンツ認証がされることができるような仕組みの実現方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												RAGを利用した生成AIシステムで検索対象となるドキュメントや、評価のために評価者が用意する正解データが、事実に基づいたデータであるかの確認~~ができる状態であるをする~~ ※RAGを利用した生成AIシステムのみ本項目の対象	RAGを利用した生成AIシステムで検索対象となるドキュメントや、評価のために評価者が用意する正解データが、事実に基づいたデータであることを確認した記録等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
			不特定外部者（一般国民等）による府省庁外利用の場合は基本項目として適用	1~~7~~8	エンドユーザー~~に~~対し、生成AIシステムの出力を人間から発せられた情報と区別できるようにすること	●	●	●	●	●	エンドユーザーに対し、生成AIシステムの出力を人間から発せられた情報と区別できるような仕組みを~~提供する技術を有している~~具備する	-	エンドユーザーに対し、生成AIシステムの出力を人間から発せられた情報と区別できるような仕組みの実現方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
			不特定外部者（一般国民等）による府省庁外利用の場合は基本項目として適用	1~~8~~9	生成AIシステムによる、エンドユーザーの意思決定の不当な誘導を防止~~するよう制御等を~~していること	-	-	-	-	-	~~ニュース記事やソーシャルメディアなどにおいて、エンドユーザーが生成AIシステムで出力したコンテンツであることを識別できる仕組みを提供する技術を有している~~	-	~~ニュース記事やソーシャルメディアなどにおいて、エンドユーザーが生成AIシステムで出力したコンテンツであることを識別できる仕組みの実現方法がわかる資料等~~	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	-
						●	●	●	●	●	生成AIシステムの推奨や指示により、エンドユーザーが主観的又は客観的に不利益となる行動に誘導されることがないよう対策を講じ~~てい~~る	-	生成AIシステムの推奨や指示により、エンドユーザーが主観的又は客観的に不利益となる行動に誘導される出力結果になっていないかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	生成AIシステムの出力において、生成AIシステムによる誘導（URLリンク等を含むメッセージ生成など）のオプトイン~~または~~又はオプトアウト手段が出力に含まれる仕組みを~~提供する技術を有している~~具備する	-	生成AIシステムの出力において、生成AIシステムによる誘導のオプトイン~~または~~又はオプトアウト手段が出力に含まれる仕組みの実現方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」

調達チェックシート						（参考）要求事項の参考								
					※調達仕様書で事業者に遵守を求める内容を記載	対策例の対象AI					※「要求事項」を遵守するための方法論を例示。必ずしもこの対策例に準拠する必要はない。取捨選択の上、必要なものに限り要求事項の詳細として、企画者が調達仕様書に盛り込む。		※必要に応じて、事業者へ提供を依頼するか否かを検討	（参考） 「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の「各種テンプレート」との対応関係	（参考） 対策例・対策例詳細の参考文献
						入力		出力							
分類	評価観点#	評価観点	評価・選定時の項目の分類	要求事項#	要求事項	テキストを含む	音声を含む	テキストを含む	画像を含む	音声を含む	対策例	対策例詳細	裏付けとなる情報の例		
	14	公平性と包摂性	不特定外部者（一般国民等）による府省庁外利用の場合は基本項目として適用	~~19~~20	生成AIシステムによる出力に有害なバイアス~~や含まず~~、不当な差別~~のを含まない状態~~と入出力制限等をしていること	●	●	●	●	●	特定のグループ（人種、性別、国籍、年齢、政治的信念、宗教等の多様な背景に関する）に対する有害なバイアスの入力あるいは想定出力に含むテストデータを入力した際、生成AIシステムが回答を拒否できる仕組みを~~提供する技術を有している~~具備する	出力コンテンツに対するフィルター機能を導入し、安全性を損なう情報、想定外のパーソナルデータ漏洩、著作権者の権利侵害に相当する出力、あるいは想定外のバイアスの出力を防ぐようにデザインする	特定のグループ（人種、性別、国籍、年齢、政治的信念、宗教等の多様な背景に関する）に対する有害なバイアスの入力あるいは想定出力に含むテストデータを入力した際、生成AIシステムが回答を拒否することができるような仕組みの実現方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	対策例：AISI「AIセーフティに関する評価観点ガイド（第1.10版）」 対策例詳細：産総研「生成AI品質マネジメントガイドライン 第１版」
						●	●	●	●	●	出力が人の属性に影響されないと想定されるテストデータを入力した際、出力結果が属性による影響を受けないことの対策を講じ~~てい~~る	出力コンテンツに対するフィルター機能を導入し、安全性を損なう情報、想定外のパーソナルデータ漏洩、著作権者の権利侵害に相当する出力、あるいは想定外のバイアスの出力を防ぐようにデザインする	出力が人の属性に影響されないと想定されるテストデータを入力した際、出力結果が属性による影響を受けないことを確認しているテスト方針がわかる資料等		対策例：AISI「AIセーフティに関する評価観点ガイド（第1.10版）」 対策例詳細：産総研「生成AI品質マネジメントガイドライン 第１版」
						●	●	●	●	●	特定のモデルの利用が主たる目的ではない場合、~~LLM~~生成AIモデルごとに異なるイデオロギーやバイアスを持つことがあることを考慮し、複数の~~LLM~~生成AIモデルを利用する~~技術を有している~~	-	複数の~~LLM~~生成AIモデルを利用するシステム設計であることがわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	学習データ、モデルの学習過程において、生成AIシステムに不公正なバイアスがないかを検証する~~手段を有している~~また、生成AIモデルが、法令等に基づき特定の分野における出力制限をかけられている可能性について、整理して提供する	利用目的に応じ、バイアスや出力制限が支障となるかを踏まえ、適切な生成AIを選択する	生成AIシステムの検証プロセス・検証方法が分かる資料、生成AIモデルの提供企業の所在国におけるAIに対する規律や当該生成AIモデルの生成結果のバイアスに対する評価結果等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	出力結果について有害なバイアスが含まれていないか定期的にモニタリング~~してい~~る	-	有害なバイアスが含まれていないか定期的にモニタリングする際の確認観点がわかる資料等		総務省、経産省「AI事業者ガイドライン 第1.1版」
						●	●	-	●	-	特定のカテゴリ（例えば職業）に関わる人物画像の生成を求めた場合に、個人の属性（例えば性別、年齢、人種）に関する偏りのない出力を生成できる仕組みを具備する	-	特定のカテゴリ（例えば職業）に関わる人物画像の生成を求めた場合に、個人の属性（例えば性別、年齢、人種）に関する偏りのない出力を生成することができるような仕組みの実現方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
			基本項目	2~~0~~1	生成AIシステム~~の出力~~が全てのエンドユーザーによって理解しやすい出力となる~~ものである可読性の高い状態としている~~こと	●	●	●	●	●	生成AIシステムの出力の流暢性スコア（出力が文法的に適切かを数値で表したもの）の測定及び評価を~~してい~~る	-	生成AIシステムの出力の流暢性スコア及びスコアの測定方針がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	生成AIシステムの出力の読み易さに関するスコアの測定及び評価を~~してい~~る	-	生成AIシステムの出力の読み易さに関するスコア及びスコアの測定方針がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	生成AIシステムに文法的に不適切なテストデータを入力した場合でも、出力は文法的に適切であり、人間が理解しやすいものとなるよう対策を講じ~~てい~~る	-	生成AIシステムに文法的に不適切なテストデータを入力した場合でも、出力は文法的に適切であり、人間が理解しやすいものとなっているかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
	15	目的外利用への対処	基本項目	2~~1~~2	目的外利用の防止を行い、仮に目的外利用された場合にも~~大きな~~危害・不利益を~~が~~発生~~しにくくなるようもないような状態と~~入出力制限等をしていること	●	●	●	●	●	生成AIシステムに想定ユースケース以外の出力を想定したテストデータが入力された場合でも、エンドユーザーの生命・身体・財産等や各種の権利に危害を生じさせる出力がされない、あるいは、出力を拒否できる仕組みを~~提供する技術を有している~~具備する	-	生成AIシステムに想定ユースケース以外の出力を想定したテストデータが入力された場合でも、エンドユーザーの生命・身体・財産等や各種の権利に危害を生じさせる出力がされない、あるいは、出力を拒否することができるような仕組みの実現方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.10.情報セキュリティに関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	想定された目的の範囲内の生成AIシステムのユースケースにおいて、エンドユーザーの生命・身体・財産等や各種の権利に危害を生じさせる出力がされない、あるいは、出力を拒否できる仕組みを~~提供する技術を有している~~具備する	-	想定された目的の範囲内の生成AIシステムのユースケースにおいて、エンドユーザーの生命・身体・財産等や各種の権利に危害を生じさせる出力がされない、あるいは、出力を拒否することができるような仕組みの実現方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	エンドユーザーが生成AIシステムを安全かつ適正に利用するため、生成AIシステムの利用方法や利用上の留意点、想定利用環境、ガイドライン等が定められ、定期的に更新~~されてい~~る	-	生成AIシステムの利用方法や利用上の留意点、想定利用環境等が記載された資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
	16	個人情報、プライバシー、知的財産等	個人情報を取り扱い、又はプライバシー~~、知的財産を取り扱うの保護が必要な~~場合は基本項目として適用	2~~2~~3	生成AIシステムにお~~いて取得・処理・保存するけ~~る個人情報~~に~~ついてその適切な取扱い~~とが確保されるとともに、知的財産と~~プライバシー~~がの~~保護~~される状態とが図られるよう対策~~していること	●	●	●	●	●	RAGを利用した生成AIシステムを利用し、RAGによる検索先に個人に関する情報が含まれる場合、不適切な個人情報の出力を制御できる仕組みを~~提供する技術を有している~~具備する ※RAGを利用した生成AIシステムのみ本項目の対象	-	RAGを利用した生成AIシステムを利用し、RAGによる検索先に個人に関する情報が含まれる場合、不適切な個人に関する情報の出力を制御する仕組みの実現方法がわかる資料等	「調達仕様書標準テンプレート」 6.作業にあたっての遵守事項 6.3.個人情報等の取扱い 「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	プライバシー侵害を認識した場合等の対処方法について定め~~られてい~~る	-	プライバシー侵害時の対処手順がわかる資料等		-
						●	●	●	●	●	個人情報保護法に準拠して、利用者からデータを収集~~しているする（個人情報保護委員会からの注意喚起参照：https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf）~~	-	個人情報保護法に準拠している旨が分かる資料（ルールや規程、その運用状況の記録等）		-
						●	●	●	●	●	特に国民等外部の者が利用する場合で、個人情報等が入力される可能性があるときには、原則として、利用者の入力情報は当該利用者への回答の生成にのみ利用される仕組みとなるよう確保する	-	個人情報等が入力される可能性がある場合、原則として、利用者の入力情報は当該利用者への回答の生成にのみ利用される仕組みの実装方法がわかる資料等		-
						●	●	●	●	●	生成AIシステムにおいて個人情報を含むパーソナルデータ~~の保護が必要な~~を取り扱う場合、~~生成AIシステムの利用する~~当該データの保護のため~~匿名~~適切な加工等の~~方法~~~~その~~対策を~~具備する~~講じる	-	生成AIシステムにおいて個人情報を含むパーソナルデータ~~の保護が必要な~~を取り扱う場合、~~生成AIシステムの利用する~~当該データの保護のために講じる~~匿名~~適切な加工等の~~方法~~~~その~~対策の実現方法がわかる資料等		産総研「生成AI品質マネジメントガイドライン 第１版」
			生成AIシステムで知的財産等を取り扱う場合は基本項目として適用 ※①著作物の利用、②登録意匠・登録商標、他人の商品等表示・商品形態の利用、③人の肖像の利用、④人の声の利用が主に想定される。	24	生成段階において、知的財産権、肖像権、パブリシティ権の保護が図られるよう対策を講じていること	●	●	●	●	●	モデルにおいて知的財産権等の侵害等防止のための仕組みを具備する	-	知的財産権等の保護のための措置（フィルタリング等）の実現方法がわかる資料	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	経産省「コンテンツ制作のための生成AI利活用ガイドブック」 ※「肖像や声の保護に関しては、不正競争防止法や裁判例における考え方の整理がされている。 経済産業省、2025年 「肖像と声のパブリシティ価値に係る現行の不正競争防止法における考え方の整理について」 https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/shozo_koe.pdf

調達チェックシート						（参考）要求事項の参考								
分類	評価観点#	評価観点	評価・選定時の項目の分類	要求事項#	※調達仕様書で事業者に遵守を求める内容を記載 要求事項	対策例の対象AI 入力 テキストを含む	音声を含む	出力 テキストを含む	画像を含む	音声を含む	※「要求事項」を遵守するための方法論を例示。必ずしもこの対策例に準拠する必要はない。取捨選択の上、必要なものに限り要求事項の詳細として、企画者が調達仕様書に盛り込む。 対策例	対策例詳細	※必要に応じて、事業者へ提供を依頼するか否かを検討 裏付けとなる情報の例	（参考） 「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の「各種テンプレート」との対応関係	（参考） 対策例・対策例詳細の参考文献
			企画・開発において生成AIに学習を行わせる場合は基本項目として適用	25	生成AIシステムの学習段階において、知的財産権等の保護が図られるよう対策を講じていること	●	●	●	●	●	知的財産権等の侵害等防止のため、適切なデータの学習を行う対策を講じる ※生成AIシステムの調達時に調達事業者と連携をして追加学習を行う場合や、政府職員が自ら生成AIの開発を行う場合のみ本項目の対象	外部から学習データの提供を受ける場合、当該データ提供者との契約・利用規約において、提供されるデータを生成AIへの学習用データとして利用することが制限されている場合がある。許諾なく学習データとして用いると契約・利用規約違反となる可能性があるため、契約・利用規約を確認し、データの利用制限の有無や内容をチェックする	データ提供者との契約・利用規約を踏まえての学習を行う際の対応方針がわかる資料等	「要件定義書標準テンプレート」 2.機能要件定義 2.4.データに関する事項 3.非機能要件定義 3.12.データマネジメントに関する事項	経産省「コンテンツ制作のための生成AI利活用ガイドブック」
												学習データをそのまま出力させるような学習方法をとらない	学習データをそのまま出力させない学習方法の実現方法がわかる資料等		文化庁「AIと著作権に関するチェックリスト＆ガイダンス」
												自らが権利を有しておらず、また、著作権で保護された著作物等を学習データとして収集・利用する場合、①契約の締結等の権利者の許諾を得て行われているか、又は②権利者の許諾なく著作権法第30条の４の適用を受けて行われているか確認する。 ②の場合、学習データとしての収集・利用が同条の「非享受目的」要件を満たすか否か、「著作権者の利益を不当に害することとなる場合」に該当しないかを確認する。また、「非享受目的」のみの利用に留め、享受目的あるいは享受目的が併存すると評価される利用はせず、「著作権者の利益を不当に害することとなる場合」に該当するような利用はしない。 ①に関して、例えば以下のような取組が考えられる ・学習データには、著作権者から許諾を得る等権利処理されたデータ（ライセンスの契約等）を利用する ②に関して、「著作権者の利益を不当に害することとなる場合」に該当しないよう、例えば以下のような取組が考えられる ・AI学習データの収集を制限する技術的措置（ID/PWによるアクセス制限や〝robots.txt〟による制限等）を尊重する	学習データの収集・利用等における権利者の許諾の状況の確認と、許諾を得る際の対応方針がわかる資料等 又は、行おうとする学習データの収集・利用等で著作権法30条の4の適用を受けるための確認方針と、そのうえで学習データの利用を「非享受目的」のみに利用する仕組みの実現方法がわかる資料等		文化庁「AIと著作権に関するチェックリスト＆ガイダンス」 経産省「コンテンツ制作のための生成AI利活用ガイドブック」
	17	セキュリティ確保	基本項目	2~~3~~6	生成AIシステム全体の脆弱性に対処し、不正操作による影響~~を防い~~その防止措置を取っていること	●	●	●	●	●	生成AIシステム全体に関するセキュリティ確保の対策を講じる	生成AIシステムに対する攻撃手法は日々新たなものが生まれており、これらのリスクに対応するための仕組みを検討・開発している、また必要に応じて導入することが可能である	最新の攻撃手法に対する対策についての資料等	「要件定義書標準テンプレート」 3.非機能要件定義 ~~3.10.情報セキュリティに関する事項~~ 3.4.性能に関する事項 3.5.信頼性に関する事項 3.10.情報セキュリティに関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												生成AIモデルが意図しない出力を行わないよう、安全基準を事後学習させる	生成AIモデルが意図しない出力を行わないよう、安全基準を事後学習させるための開発方針とその方法が分かる資料等		対策例詳細： 総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
												生成AIモデルが従うべき指示の優先度を定義し、優先度の高い指示（例：システムプロンプト）を常に優先的に処理するよう、生成AIモデルを事後学習させる	生成AIモデルが従うべき指示の優先度を定義し、優先度の高い指示を常に優先的に処理するようにするための開発方針とその方法がわかる資料等		対策例詳細： 総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
												生成AIシステムの意図しない動作の防止のために、オーケストレータの権限等に不備がないことの対策を講じる。生成AIモデルや連携システムを操作するオーケストレータに係る権限を必要最小限とすることで、生成AIモデルが攻撃を受けた場合の被害拡大を抑制する	生成AIモデルや連携システムを操作するオーケストレータに係る権限設定等に不備がないかの確認方法がわかる資料等		対策例：AISI「AIセーフティに関する評価観点ガイド（第1.10版）」 対策例詳細：総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
												入力された要機密情報を参照又は学習する場合、権限を有する者以外の回答の生成に、当該入力された要機密情報が用いられないような仕組みとする	入力された要機密情報を参照又は学習する場合、権限を有する者以外の回答の生成に、当該入力された要機密情報が用いられないような仕組みとする方法がわかる資料等		-
						●	●	●	●	●	生成AIモデルへのプロンプト入力に関するセキュリティ確保の対策を講じる（入力プロンプト全般）	プロンプト内容の有害性を生成AIモデルへの入力前に検知する等、生成AIモデルへの入力前段階での防御策を講じる 例えば、以下のような対策を講じる ・禁止リストを活用したプロンプト検知 ・有害な結果をもたらす可能性のあるコードの実行や生成を促す入力、又は生成AIシステムの利用目的に照らして意図しない出力を生成させる指示がプロンプトに含まれていないか検証し、そのような入力を検知した場合にはプロンプトの一部削除による無害化や、処理の拒否等の措置を講じる ・プロンプトインジェクション等により、生成AIシステムのバックエンドシステムに意図していない操作が行われることがないよう対策する ・実装した生成AIシステムの防御策に関して、プロンプトインジェクションなどにより防御策の回避が可能とならないよう対策する	プロンプト内容の有害性を生成AIモデルへの入力前に検知する等、生成AIモデルへの入力前段階での防御策の実装方針がわかる資料等		対策例詳細： AISI「AIセーフティに関する評価観点ガイド（第1.10版）」 総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
												生成AIシステムが処理困難でコストのかかる複数のテストデータを繰り返し入力した場合でも、生成AIシステムの許容できないパフォーマンス低下やシステムの停止が発生しないよう対策を講じる	生成AIシステムが処理困難でコストのかかる複数のテストデータを繰り返し入力した場合でも、生成AIシステムの許容できないパフォーマンス低下やシステムの停止が発生しないかの確認方法がわかる資料等		対策例詳細：AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												生成AIシステムへの膨大なアクセスによる攻撃を抑制するためのレートリミットを導入する	生成AIシステムのレートリミットの仕組みの実装方法がわかる資料等		対策例詳細：総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
						●	●	●	●	●	生成AIモデルへのプロンプト入力に関するセキュリティ確保の対策を講じる（特に利用者が入力するプロンプト）	生成AIモデルがシステムプロンプトを無視してユーザー入力のみに従うよう生成AIモデルに指示する（いわゆる jail break を試みる）ユーザー入力を無効化するようにシステムプロンプトをデザインする	jail breakを試みるユーザー入力を無効化する仕組みの実現方法がわかる資料等		対策例詳細：産総研「生成AI品質マネジメントガイドライン 第１版」
												生成AIシステムの目的と用途に応じて、ユーザーを認証して、認証を通らないユーザーの利用を拒否することによって、ユーザー入力プロンプトの来歴が明らかになるよう制御する	ユーザーを認証して、認証を通らないユーザーの利用を拒否することによって、ユーザー入力プロンプトの来歴が明らかになるよう制御する仕組みの実現方法がわかる資料等		対策例詳細：産総研「生成AI品質マネジメントガイドライン 第１版」
						●	●	●	●	●	生成AIモデルへのプロンプト入力に関するセキュリティ確保の対策を講じる（システムプロンプト）	システムプロンプトに制約事項やセキュリティ上の注意事項などを設定することで、生成AIモデルが意図しない出力を行わないようにする	システムプロンプトに制約事項やセキュリティ上の注意事項などを設定することで、生成AIモデルが意図しない出力を行わないようにする仕組みを提供する技術の実装方法がわかる資料等		対策例詳細： 総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
												システムプロンプトに出力を意図しない機密情報（例：APIキー）等を直接記述することを避け、生成AIモデルが必要に応じて参照できるよう別個に管理する	システムプロンプトには、出力を意図しない機密情報等を直接記述することを避け、生成AIモデルが必要に応じて参照できるよう別個に管理する対策の対応方針がわかる資料等		対策例詳細： 総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
						●	●	●	●	●	生成AIモデルの出力に関するセキュリティ確保の対策を講じる	生成AIシステムの意図しない動作の防止のための出力の検証機能を具備し、出力を意図しない情報が出力に含まれていないか検証し、検知した場合には応答を拒否する	出力を意図しない情報が出力に含まれていないか検証し、検知した場合には応答を拒否する仕組みの実現方法がわかる資料等		対策例詳細： 総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
												単語の出現確率など、攻撃者に悪用され得る情報を必要に応じて応答から除外することで、モデル抽出攻撃への対策を行う（主にテキスト出力を念頭）	単語の出現確率など、攻撃者に悪用され得る情報を必要に応じて応答から除外することで、モデル抽出攻撃への対策をする仕組みの実現方法がわかる資料等		対策例詳細： 総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
						●	●	●	●	●	生成AIモデルが生成AIモデルの外のデータを参照する場合のセキュリティ確保の対策を講じる	RAGにて要機密情報のように参照権限が設定されている情報を利用する場合、RAG用のデータ及びデータストアへの参照権限をユーザーや役割に応じて適切に設定する（主にテキスト出力を念頭）	RAG用のデータ及びデータストアへの参照権限をユーザーや役割に応じて適切に設定し、不備がないかの確認方法がわかる資料等		対策例詳細： AISI「AIセーフティに関する評価観点ガイド（第1.10版）」 総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
												外部サービスの呼び出しを行うためのプラグインツールを活用する場合、プラグインツールがアクセスする外部サービスやデータベース等の制御を実施する	プラグインツールがアクセスする外部サービスやデータベース等の制御の実現方法がわかる資料等		産総研「生成AI品質マネジメントガイドライン 第１版」
												外部サービスの呼び出しを行うためのプラグインツールを活用する場合、機能の導入前に当該プラグインツールの情報（SBOM 等）を確認し、外部連携としての利用可否を判断する	プラグインツールを導入する場合の、プラグインツールの情報の確認方針がわかる資料等		産総研「生成AI品質マネジメントガイドライン 第１版」
												Webサイトや外部のデータベースなど、外部データを参照する場合には、これらに意図しない出力を行わせる指示が含まれていないか検証し、そのような指示を検知した場合には、処理の拒否等の措置を講じる	Webサイトや外部のデータベースなど、外部データを参照する場合には、これらに意図しない出力を行わせる指示が含まれていないか検証し、そのような指示を検知した場合には、処理を拒否する等の仕組みの実現方法がわかる資料等		総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
												生成AIシステムに、入力プロンプトと外部参照データを明確に区分させ、外部参照データに高い注意を払わせる	生成AIシステムに、入力プロンプトと外部参照データを明確に区分させ、外部参照データに高い注意を払わせる仕組みの実現方法がわかる資料等		総務省「AIのセキュリティ確保のための技術的対策に係るガイドライン（案）」（LLM及びLLMを構成要素に含むAIシステムが対象）
			生成AIシステムに対して高い信頼性が求められる場合は基本項目として適用	27	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生を検知した後、その影響を最小限に抑えつつ、迅速な封じ込めと復旧能力を確保するための対策を講じていること	●	●	●	●	●	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応のために、生成AIシステムの制御性を強化するための仕組みを具備する	改ざんされたモデルの別バージョンや代替モデルへの即時切り替えを実施する	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応方法として、改ざんされたモデルの別バージョンや代替モデルへ即時切替する仕組みの実現方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.4.性能に関する事項 3.5.信頼性に関する事項 3.10.情報セキュリティに関する事項 3.16.運用に関する事項 3.17.保守に関する事項	AISI「AIインシデントレスポンス・アプローチブック」
												混入された悪意のある学習データの局所的な除去や追加学習を実施する	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応方法として、混入された悪意のある学習データの局所的な除去や追加学習等の、生成AIモデルの汚染対策の方針がわかる資料等		AISI「AIインシデントレスポンス・アプローチブック」
												異常時に影響を受けない上位権限を持ち、隔離された制御インタフェースを設置する	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応を想定して、異常時に影響を受けない上位権限を持ち、隔離された制御インターフェースの設置等の対策の実装方針がわかる資料等		AISI「AIインシデントレスポンス・アプローチブック」
			基本項目	2~~4~~8	生成AIシステムの開発の過程を通じて、適切にセキュリティ対策を講じていること	●	●	●	●	●	生成AIシステムの開発の過程を通じて、採用する技術の特性に照らして適切なセキュリティ対策~~技術を有している~~を講じる	-	セキュリティ対策についての資料等	「要件定義書標準テンプレート」 3.非機能要件定義 ~~3.10.情報セキュリティに関する事項~~ 3.4.性能に関する事項 3.5.信頼性に関する事項 3.10.情報セキュリティに関する事項	総務省、経産省「AI事業者ガイドライン 第1.1版」

調達チェックシート						（参考）要求事項の参考								
分類	評価観点#	評価観点	評価・選定時の項目の分類	要求事項#	※調達仕様書で事業者に遵守を求める内容を記載 要求事項	対策例の対象AI 入力 テキストを含む	音声を含む	出力 テキストを含む	画像を含む	音声を含む	※「要求事項」を遵守するための方法論を例示。必ずしもこの対策例に準拠する必要はない。取捨選択の上、必要なものに限り要求事項の詳細として、企画者が調達仕様書に盛り込む。 対策例	対策例詳細	※必要に応じて、事業者へ提供を依頼するか否かを検討 裏付けとなる情報の例	（参考） 「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の「各種テンプレート」との対応関係	（参考） 対策例・対策例詳細の参考文献
	18	説明可能性	基本項目	2~~59~~	出力根拠が技術的に合理的な範囲で確認できる状態と~~する~~よう対策していること	●	●	●	●	●	出力根拠（内部動作やその状態、出典など）が可視化される機能を備える生成AIシステムにおいて様々なテストデータを入力した際、出力根拠が表示される仕組みを~~提供する技術を有している~~具備する	生成AIが出力を生成するために利用した情報を、出力の正当化理由として出力するようにシステムプロンプトをデザインしている。ファイルデータや外部連携コンポーネントからの応答など実行時に選択してプロンプトに組み込む情報については、その来歴を示す情報を添えて組み込んでいる。これと合わせ、システムプロンプトで来歴情報を活用するよう指示している	出力根拠（内部動作やその状態、出典など）が可視化される機能を備える生成AIシステムにおいて様々なテストデータを入力した際、出力根拠が表示される仕組みを提供する技術の実装方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.1.ユーザビリティ及びアクセシビリティに関する事項	対策例：AISI「AIセーフティに関する評価観点ガイド（第1.10版）」 対策例詳細：産総研「生成AI品質マネジメントガイドライン 第１版」
						●	●	●	●	●	段階的な推論を行う生成AIシステムにおいて、出力に至るまでの推論の過程をエンドユーザーに提示することが可能となっているか~~の~~を確認~~するができる状態である~~	-	段階的な推論を行う生成AIシステムにおいて、出力に至るまでの推論の過程をエンドユーザーに提示することが可能となっているかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	生成AIシステムの開発過程、意思決定に影響を与えるデータ収集及びラベリング、使用されたアルゴリズム、生成生成AIシステムのシステムアーキテクチャ、データの処理プロセス等について文書化を行~~っているう~~	-	生成AIシステムの開発過程、意思決定に影響を与えるデータ収集及びラベリング、使用されたアルゴリズム、システムアーキテクトやデータの処理プロセスが文書として管理されていることがわかる資料等 ※文書化した内容について開示するという意味ではない		総務省、経産省「AI事業者ガイドライン 第1.1版」
	19	ロバスト性	基本項目	~~26~~30	生成AIシステムが入力に対して安定した出力を行う~~状態とよう制御等を~~していること	●	●	●	●	●	生成AIシステムに同一のテストデータを複数回入力した際の出力に一貫性があるよう対策を講じ~~ている~~	-	生成AIシステムに同一のテストデータを複数回入力した際の出力に一貫性があるかの確認方法がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.4.性能に関する事項 3.5.信頼性に関する事項 3.9.継続性に関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	生成AIシステムに意味的に類似した複数のテストデータを入力した際、出力に一貫性があるよう対策を講じ~~ている~~	ユーザー入力に揺れがあっても、生成AIシステムが同等なコンテンツを出力するように、その揺れを意味的に吸収するようなシステムプロンプトをデザインする	生成AIシステムに意味的に類似した複数のテストデータを入力した際、出力に一貫性があるかの確認方法がわかる資料等		対策例：AISI「AIセーフティに関する評価観点ガイド（第1.10版）」 対策例詳細：産総研「生成AI品質マネジメントガイドライン 第１版」
						●	●	●	●	●	生成AIシステムに摂動したデータ（誤入力、敵対的プロンプト、文字化けデータ、表記ゆれを含むデータ等）を入力した際も安定動作するよう対策を講じ~~ている~~	ユーザー入力に揺れがあっても、生成AIシステムが同等なコンテンツを出力するように、その揺れを意味的に吸収するようなシステムプロンプトをデザインする	生成AIシステムに摂動したデータ（誤入力、敵対的プロンプト、文字化けデータ、表記ゆれを含むデータ等）を入力した際に安定動作するかの確認方法がわかる資料等		対策例：AISI「AIセーフティに関する評価観点ガイド（第1.10版）」 対策例詳細：産総研「生成AI品質マネジメントガイドライン 第１版」
	20	データ品質	基本項目	~~27~~31	生成AIシステムがアクセスするデータを適切な状態に保~~つために対策し~~ていること	●	●	●	●	●	学習データ、モデルの学習過程において、バイアス（学習データには現れない潜在的なバイアスを含む）が含まれうることに留意し、生成AIシステムに悪影響を及ぼすデータ（事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等）の品質問題が生じていないことの対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータの品質管理として、データの正確性の管理及び、データに問題が生じないよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータの品質管理として、正確性、機密性、完全性の管理方法がわかる資料等	「調達仕様書標準テンプレート」 4.作業の実施内容に関する事項 4.13.データ管理方法 「要件定義書標準テンプレート」 2.~~非~~機能要件定義 2.4.データに関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータの品質管理として、データの破損を防ぐ管理及び、データに問題が生じないよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータの品質管理として、正確性、機密性、完全性の管理方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータに関して、データが文法的に適切であり、人間が理解しやすい内容となるよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータに関して、データが文法的に適切であり、人間が理解しやすい内容となっているかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータに関して、データの分布に人種、性別、国籍、年齢、政治的信念、宗教等による偏りがないよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータに関して、データの分布に人種、性別、国籍、年齢、政治的信念、宗教等による偏りがないかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータに関して、 利用者に対して攻撃的な言葉など、不適切な内容がデータに含まれないよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータに関して、利用者に対して攻撃的な言葉など、不適切な内容がデータに含まれていないかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータに関して、サイバー攻撃やテロ等に利用され得る情報がデータに含まれないよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータに関して、サイバー攻撃やテロ等に利用され得る情報がデータに含まれていないかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータに関して、PETs(Privacy-Enhancing Technologies)などによる措置を行うことで、学習データとしての使用に問題ない状態となっているかの確認~~をするできる状態である~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータに関して、PETs(Privacy-Enhancing Technologies)などによる措置を行うことで、学習データとしての使用に問題ない~~状態となっている~~かの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータの品質管理として、データの構成管理及び、データに問題が生じないよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータの品質管理として、データの構成管理更新方針がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータの品質管理として、アノテーションを自動化する場合、適切に行われるよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータの品質管理として、アノテーションを自動化する場合、適切に行われているかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータの品質管理として、 悪意をもった、あるいは誤動作させるテキスト・プログラム等がデータに含まれないよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータの品質管理として、 悪意をもった、あるいは誤動作させるプログラムがデータに含まれていないかの確認方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等生成AIシステムに影響を及ぼすデータの品質管理として、ツールなどにより、データの来歴管理及び、データに問題が生じないよう対策を講じ~~ている~~	事前学習データ、ファインチューニングやInContext Learning等に向けた学習データやテストデータ等 生成AIシステムに影響を及ぼすデータの品質管理として、データの来歴管理方法がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	訓練データの量と質が十分で、実用的な水準まで学習されているかを検証する	-	訓練データの量と質が十分で、実用的な水準まで学習されているかの検証プロセス・検証方法が分かる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
						●	●	●	●	●	機微情報を含むデータに対して、期待される保護強度を示すデータ加工（データ匿名加工）を施す技術を有していることや、データの利用目的との整合性からデータ匿名加工の方法を選定する	-	-		産総研「生成AI品質マネジメントガイドライン 第１版」
			任意追加項目（加点項目）	~~28~~32	生成AIシステムのアウトプットの高度化としてインプットデータの適切な構造化を行っていること	●	●	●	●	●	アウトプットの精度向上を目的とした、インプットデータの構造化を必要に応じて検討・実施~~可能である~~する	-	アウトプットの精度向上を目的とした、インプットデータの構造化の実現方法がわかる資料等	「要件定義書標準テンプレート」 2.機能要件定義 2.4.データに関する事項	-
	21	検証可能性	基本項目	~~29~~33	生成AIシステムの開発・提供のプロセスを検証可能~~な状態~~としていること	●	●	●	●	●	システムやモデル、データに関する概要や、なりたち、動作についてログや技術仕様等から検証可能~~にするための状態とする~~管理及び、問題が生じないよう対策を講じ~~ている~~	システムやモデル、データに関する概要やなりたち、動作についての検証可能性を確保するため、システムカード、モデルカード、データカードを作成して管理及び、問題が生じないよう対策を講じ~~ている~~	システムやモデル、データに関する概要やなりたち、動作についての検証可能性を確保するための技術仕様書等の管理方針がわかる資料等	「要件定義書標準テンプレート」 3.非機能要件定義 3.16.運用に関する事項 3.17.保守に関する事項	AISI「AIセーフティに関する評価観点ガイド（第1.10版）」
												システムやモデル、データに関する概要やなりたち、動作についての検証可能性を確保するため、生成AIシステムに様々なテストデータを入力した際、適切にデータログが記録されるよう対策を講じ~~ている~~	生成AIシステムに様々なテストデータを入力した際、適切にデータログが記録されているかの確認方針がわかる資料等		AISI「AIセーフティに関する評価観点ガイド（第1.10版）」

調達チェックシート					
分類	評価観点#	評価観点	評価・選定時の項目の分類	要求事項#	※調達仕様書で事業者に遵守を求める内容を記載 ※本ガイドライン「6.1.2　本ガイドラインに基づく対応事項」に記載のとおり、導入類型、プロジェクトフェーズ、リスクレベル等を踏まえ、各対応事項の要求レベルや一部要求事項の取捨選択又は拡充を検討する。 要求事項
組織要件	1	AI事業者ガイドライン共通の指針の遵守	基本項目	1	AI事業者ガイドライン共通の指針を理解・把握・対応していることの宣言が可能であること
	2	AIガバナンスの構築	基本項目	2	生成AIシステムの開発・運用に関して、AIガバナンス（※）が適用されていること ※AIにもたらされる正のインパクトを最大化しつつ、AIによるリスクを受容可能な水準で管理する統制の仕組み・業務
	3	AI業界や最新技術等の動向の把握	基本項目	3	生成AIシステムの開発・運用において、品質や説明性を高めるため、AI業界や最新技術等の動向を把握していること
	4	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生時の対応	基本項目	4	情報セキュリティインシデント・生成AIシステム特有のリスクケース（事業者の責任の範囲に属するものに限る。）対応体制・手順を整備していること（開発・運用するサービスにおいて、利用者からインシデント報告を受け付け、対応の協力をすることを含む。）
	5	関係者への生成AIに関する教育・リテラシー向上	基本項目	5	生成AIシステムの開発・運用に従事する者または組織について、生成AIに関するリテラシー向上の取組を実施していること
開発・運用工程要件	6	データの取扱い	基本項目	6	生成AIシステムへの入出力または処理されるデータの取扱いを適切に管理していること
	7	アウトプットの品質保証	基本項目	7	生成AIシステムの期待品質を満たすための取組を行っていること
	8	ベンダーロックインの回避	基本項目	8	利用している~~LLM~~生成AIモデルはバージョン情報を含めて明示可能であること
			任意追加項目（加点項目）	9	生成AIシステムに入力されるプロンプトの一部やパラメータが隠蔽されていないことの確認のために、合理的な範囲での企画者への情報開示や情報提供ができる状態であること
			任意追加項目（加点項目）	10	過去のチャット履歴の保存機能や、プロンプトをテンプレートとして登録するとともに、それらのデータをエキスポートする機能を提供する技術を有していること
			任意追加項目（加点項目）	11	特定のモデルの利用が主たる目的ではない場合、~~LLM~~生成AIモデルごとに異なる機能や動作に影響する特徴があることを考慮し、複数の~~LLM~~生成AIモデルの中から最適な~~LLM~~生成AIモデルを選択又は組み合わせて利用する技術を有していること
			基本項目	12	生成AIシステムのアーキテクチャ設計と実装において、ベンダーやシステムの移行の容易性も踏まえた開発や運用が可能であること
	9	生成AI~~システム~~モデルのアップデートの考慮	基本項目	1~~2~~3	メジャーアップデートもしくは移行に関する生成AI固有の観点からリスク軽減していること
	10	文化的・言語的考慮	任意追加項目（加点項目）	1~~3~~4	生成AIシステム~~のアウトプット~~が日本の言語環境や文化環境に即した出力が可能である~~ものになる状態としている~~こと
	11	環境への配慮	任意追加項目（加点項目）	1~~4~~5	環境に配慮した生成AIシステムを開発・提供すること
生成AIシステムの基本機能要件	12	有害情報の出力制御	基本項目	1~~5~~6	テロや犯罪に関する情報や攻撃的な表現など、生成AIシステムによる有害情報の入出力~~を制御制限等を~~していること
	13	偽誤情報の出力・誘導の防止	基本項目	1~~6~~7	生成AIシステムによる偽誤情報の出力の防止措置を取っていること
			不特定外部者（一般国民等）による府省庁外利用の場合は基本項目として適用	1~~7~~8	エンドユーザーに対し、生成AIシステムの出力を人間から発せられた情報と区別できるようにすること
			不特定外部者（一般国民等）による府省庁外利用の場合は基本項目として適用	1~~8~~9	生成AIシステムによる、エンドユーザーの意思決定の不当な誘導を防止するよう制御等をしていること
	14	公平性と包摂性	不特定外部者（一般国民等）による府省庁外利用の場合は基本項目として適用	~~1~~920	生成AIシステムによる出力に有害なバイアス~~やを含まず、~~不当な差別~~のを含まない状態と~~入出力制限等をしていること
			基本項目	2~~0~~1	生成AIシステム~~の出力~~が全てのエンドユーザーによって理解しやすい出力となるものである~~可読性の高い状態としている~~こと
	15	目的外利用への対処	基本項目	2~~1~~2	目的外利用の防止を行い、仮に目的外利用された場合にも~~大きな~~危害・不利益~~を~~が発生~~しにくくなるようしないような状態と~~入出力制限等をしていること
	16	個人情報、プライバシー、知的財産	個人情報を取り扱い、又はプライバシー~~知的財産を取り扱うの~~保護が必要な場合は基本項目として適用	2~~2~~3	生成AIシステムにお~~いて取得・処理・保存するける~~個人情報~~のについて~~適切な取扱い~~とが確保されるとともに~~、~~知的財産と~~プライバシーのが保護が図られるよう対策される状態と~~していること
			生成AIシステムで知的財産等を取り扱う場合は基本項目として適用	24	生成段階において、知的財産権、肖像権、パブリシティ権の保護が図られるよう対策を講じていること
			企画・開発において生成AIに学習を行わせる場合は基本項目として適用	25	生成AIシステムの学習段階において、知的財産権の保護が図られるよう対策を講じていること
	17	セキュリティ確保	基本項目	2~~3~~6	生成AIシステム全体の脆弱性に対処し、不正操作による影響~~を防いでの~~防止措置を取っていること
			生成AIシステムに対して高い信頼性が求められる場合は基本項目として適用	27	情報セキュリティインシデント・生成AIシステム特有のリスクケース発生を検知した後、その影響を最小限に抑えつつ、迅速な封じ込めと復旧能力を確保するための対策を講じていること
			基本項目	2~~4~~8	生成AIシステムの開発の過程を通じて、適切にセキュリティ対策を講じていること
	18	説明可能性	基本項目	2~~5~~9	出力根拠が技術的に合理的な範囲で確認できる状態とするよう対策していること
	19	ロバスト性	基本項目	~~26~~30	生成AIシステムが入力に対して安定した出力を行う~~状態とよう制御等を~~していること
	20	データ品質	基本項目	~~27~~31	生成AIシステムがアクセスするデータを適切な状態に保~~っ~~つために対策していること
			任意追加項目（加点項目）	~~28~~32	生成AIシステムのアウトプットの高度化としてインプットデータの適切な構造化を行っていること
	21	検証可能性	基本項目	~~29~~33	生成AIシステムの開発・提供のプロセスを検証可能~~な状態~~としていること

出典：AI事業者ガイドライン「共通の指針」のチェックリスト（全主体向け）より
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_5.pdf

別添7 A

チェックリスト [全主体向け]

令和6年4月19日

本チェックリストは、AI事業者ガイドライン「第2部C.共通の指針」を要約したものです。
事業者に求められる重要な取組事項のチェックにご活用ください
※**高度なAIシステムに関係する事業者**は、
「チェックリスト[別添7 B.高度なAIシステムに関係する事業者向け]」も実施ください

チェック項目

- □ **人間中心**の考え方を基に、憲法が保障する又は国際的に認められた人権を侵すことがないようにしているか？
- □ AIに関わる全ての者の生命・身体・財産、精神及び環境に危害を及ぼすことがないよう**安全性**を確保しているか？
- □ 潜在的なバイアスをなくすよう留意し、それでも回避できないバイアスがあることを認識しつつ、回避できないバイアスが人権及び多様な文化を尊重する**公平性**の観点から許容可能か評価しているか？
- □ **プライバシー**を尊重・保護し、関係法令を遵守しているか？
- □ 不正操作によってAIの振る舞いに意図せぬ変更又は停止が生じることのないように、**セキュリティ**を確保しているか？
- □ **透明性**を確保するために、AI自体やAIシステム・サービスの情報をステークホルダーに対し合理的で技術的に可能な範囲で提供しているか？
- □ データの出所、AIの意思決定等のトレーサビリティに関する情報やリスクへの対応状況等について、関連するステークホルダーに対して合理的な範囲で**アカウンタビリティ**を果たしているか？
- □ **AIガバナンスやプライバシーに関するポリシー**等を策定しているか？

- □ 上記の実現のため、各事業者の状況に応じた**具体的なアプローチは検討**しているか？

検討には**「具体的なアプローチ検討のためのワークシート」**をご活用ください

本チェックシートの概要

別紙４

本チェックシートは、生成AIシステムを調達する際に、契約書に盛り込むことを検討すべき事項を整理したものである。（調達仕様書に盛り込むことが適当な場合は、調達仕様書に盛り込む）
企画者は生成AIシステムの調達にあたって、契約書及び調達仕様書を作成する際には、本チェックシートを参考にする。
ただし、本チェックシートは「生成AIシステムの調達」に関して特有の留意すべき項目のみ掲載しており、各府省庁の契約書等の雛形を参照し契約書を作成する必要がある。
なお、本チェックシートでは、「【別紙４】契約チェックシート（生成AIシステム用）」を「契約チェックシート」と表現する。

本チェックシートの構成

取り決め事項＃	契約時の項目	取り決め事項	契約に盛り込む条項内容例	補足説明
1	基本項目	生成AIシステムに係るインプットに関する取り決め	インプットについて、インプットの定義、インプットの利用目的、インプットの利用条件、インプットの権利帰属に関して定める条項	事業者がインプットを自由に利用できる可能性があるため、契約による規律の対象となるインプットの範囲を定めること。事業者に対して生成AIシステム関連の提供目的以外の目的でインプットを事実上の利用・保持しないことを目的外利用禁止義務として定めること。事業者がインプットを利用することを認める場合の利用条件（学習の有無、データの保存方法等）を定めること（※）、事業者がインプットに関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。 ※オプトアウトにより学習利用の制御を行うことも可能とするが、契約上オプトアウトを行ったデータを学習目的のために利用しない旨を明確にすること。
2	基本項目	生成AIシステムに係るインプットの処理成果に関する取り決め	インプットの処理成果について、アウトプット以外のもので契約上規律の対象とするものの定義、利用目的、利用条件、権利帰属に関して定める条項	事業者がインプットを自由に利用できる可能性があるため、契約による規律の対象となるインプットの処理成果の範囲を定めること。事業者に対して生成AIシステム関連の提供目的以外の目的でインプットの処理成果を事実上の利用・保持しないことを目的外利用禁止義務として定めること。事業者がインプットの処理成果を利用することを認める場合の利用条件（学習の有無、データの保存方法等）を定めること。事業者がインプットの処理成果に関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。 ※RAGコンポーネントに含む場合の処理等は、データベースが成果物となることが一般的であるが、構築するパーサー（RAG用テキストデータに変換するプログラム）、テキスト分割プログラム、ベクトル変換プログラムなどについても、成果物に含めるのか、WebAPI等を通じて機能を提供するのかを検討すること及びその権利帰属や利用方法を、契約に盛り込むことが望ましい。
3	基本項目	生成AIシステムに係るアウトプットに関する取り決め	アウトプットについて、アウトプットの定義、事業者に対してアウトプットに関する一定の保証を求めること、ユーザがアウトプットを第三者に提供することができる場合にその条件やアウトプットの権利帰属に関して定める条項	契約で規律の対象となるアウトプットとして、事業者がアウトプットの保証・情報提供義務を負う場合の保証・情報提供の条件を定めること、第三者提供条件（提供先、提供範囲その他の条件）を定めること、ユーザがアウトプットに関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。
4	基本項目	生成AIシステムに係るアウトプットの処理成果に関する取り決め	アウトプットの処理成果について、契約上規律の対象とするものの定義、ユーザによる外部提供、権利帰属に関して定める条項	契約で規律の対象となるアウトプットの処理成果として、アウトプットの処理成果の定義はユーザのサービス利用目的を十分にカバーできるよう範囲を定めること。サービス利用目的に照らして外部提供条件（提供先、提供範囲その他の条件）を定めること、知的財産権等一定の権利を取得する場合には権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。

【B列：契約時の項目】
取決め事項として、事業者との契約時に考慮を求める項目を「基本項目」と記載。本ガイドライン「6.1.2　本ガイドラインに基づく対応事項」に記載のとおり、導入類型、プロジェクトフェーズ、リスクレベル等を踏まえ、一部の取決め事項の取捨選択又は拡充を検討する。

【C列：取決め事項】
取決め事項として、事業者との契約時に考慮を求める内容を記載。取決め事項は、原則として契約書又は調達仕様書に盛り込むことを検討する。

【D列：契約に盛り込む条項内容例】
「C列：取決め事項」を満たす条項内容例を例示。必ずしもこの対策例に準拠する必要はない。

【E列：補足説明】
「C列：取決め事項」および及び「D列：契約書に盛り込む条項内容例」の補足説明を記載。

※「D列：契約に盛り込む条項内容例」と「E列：補足説明」については、取り決めた事項を契約に盛り込む際の条項内容例とその補足説明であるため、調達する生成AIシステムの特徴や案件の特性、リスク評価結果を踏まえ、取捨選択の上、企画者が必要に応じ契約書又は調達仕様書に盛り込むこととする。

本チェックシートの利用方法

・企画者は、「C列：取決め事項」から必要なものを契約書または又は調達仕様書に取り込む。
※「C列：取決め事項」については、契約書または調達仕様書に盛り込む事項として原則として必須とする項目である。
※「D列：契約書に盛り込む条項内容例」はあくまで例示であり、すべてを満たす必要はなく、また例示している方法以外で遵守されていても問題ない。
※別途、調達時に作成する「要件定義書」や「調達仕様書」等を参照し、政府情報システムの調達に必要な項目も取り込むこと。

本チェックシートの対象

本チェックシートは、「2.2.1　本ガイドラインが対象とする情報システム」に記載した政府情報システムのうち、「2.2.2　本ガイドラインが対象とする生成AI」に記載した生成AIを構成要素とするシステムに適用するものとする。

用語の補足

~~・LLM：文章や単語の出現確率を深層学習モデルとして扱う言語モデルを、非常に大量の訓練データを用いて構築したもの。（出典：AIプロダクト品質保証コンソーシアム「AIプロダクト品質保証ガイドライン」10-1）~~
・生成AI：文章、画像、プログラム等を生成できるAIモデルに基づくAIの総称。（出典：「AI事業者ガイドライン」P.10）
・生成AIシステム：~~本ガイドラインが対象とする生成AIを構成要素とする政府情報システム。（AISI「AIセーフティに関する評価観点ガイド（第 1.01 版）」P.9に基づき作成）~~生成AIを構成要素とするAIシステム。（「AI事業者ガイドライン」P.9、P.10に基づき作成）なお、本ガイドラインにおいて、「生成AIシステム」の語は、本ガイドラインが対象とする生成AIモデルを構成要素とする生成AIシステムを指すものとしている。
・生成AIモデル：文章、画像、プログラム等を生成できるAIモデル。（「AI事業者ガイドライン」P.10に基づき作成）なお、本ガイドラインにおいて、「生成AIモデル」の語は、本ガイドラインが対象とする生成AIを構成要素とする生成AIモデルを指すものとしている。
・ユーザー：本ガイドラインにおいては、生成AIシステムを利用するにあたり関係する政府職員（外部者が生成AIシステムを利用する場合は当該利用者も含む）として、原則として「企画者」「開発者」「提供者」「利用者」を指す。
・学習用の生データ：ユーザーから事業者に提供された、~~学習時に生成AIシステムにインプット~~生成AIモデルの学習時に活用するためのデータ。
・学習用データ：ユーザーから提供された学習用の生データを用いて、事業者による処理・加工等により作成した学習用のデータ。
・インプット：プロンプト、学習用の生データ等。（※インプットの処理成果は含まれない）
・インプットの処理成果：学習用データ、中間生成物、派生的知的財産等。（※インプットに何らかの処理（加工等）を施した無体物を指し、「派生物」、「派生的知的財産」、「派生データ」、「改良成果」等呼ばれることもある。生データに対する学習用データセット等の中間生成物が典型的に想定される。）
・アウトプット：~~AIシステム等の成果物、~~分析結果・コンテンツ等のAI生成物等。（※アウトプットの処理成果は含まれない）
・アウトプットの処理成果：AI関連サービスが出力するコンテンツをユーザーが加工したもの等。（※アウトプットに何らかの処理（加工等）を施した無体物を指し、「派生物」、「派生的知的財産」、「派生データ」、「改良成果」等呼ばれることもある。）
・ノウハウ：AI技術の研究・開発・利活用過程において、事業者又はユーザーが有し若しくは取得する知見、技術、情報等のうち知的財産として該当するもの。（※ノウハウについて、生データの取得や学習に適した生データ加工、学習用プログラムを用いた学習、学習済みモデルの調整、学習履歴、プロンプト履歴等が想定される。）
・情報セキュリティインシデント：JIS Q 27000:2019における情報セキュリティインシデントをいう。
・生成AIシステム特有のリスクケース：生成AIシステムの特有のリスクが顕在化した状態又はその可能性を有する兆候や事象が認められる状態のうち、重大な影響を及ぼし得るもの。

契約チェックシート	※本ガイドライン「6.1.2　本ガイドラインに基づく対応事項」に記載のとおり、導入類型、プロジェクトフェーズ、リスクレベル等を踏まえ、取決め事項の取捨選択又は拡充を検討する。		
取決め事項#	**契約時の項目**	**取決め事項**	**契約に盛り込む条項内容例**	**補足説明**
1	基本項目	生成AIシステムに係るインプット~~の~~に関する取決め	インプットについて、インプットの定義、インプットの利用目的、インプットの利用条件、インプットの権利帰属に関して定める条項	事業者がインプットを自由に利用できる可能性があるため、契約による規律の対象となるインプットの範囲を定めること、事業者に対して生成AIシステム関連の提供目的以外の目的でインプットを原則として利用・保持しないことを目的外利用禁止義務として定めること~~（※）~~、事業者がインプットを利用することを認める場合の利用条件（学習の有無、データの保存方法等）を定めること（※）、事業者がインプットに関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。 ※オプトアウトにより学習利用の制御を行うことも可能とするが、契約上オプトアウトを行ったデータを学習目的のために利用しない旨を明確にすること~~で目的外利用を遮断することも可能とするが、契約上オプトアウトで目的外利用を遮断する対応を取ることを明確とすること~~。
2	基本項目	生成AIシステムに係るインプットの処理成果~~の~~に関する取決め	インプットの処理成果について、アウトプット以外のもので契約上規律の対象とするものの定義、利用目的、利用条件、権利帰属に関して定める条項	事業者がインプットを自由に利用できる可能性があるため、契約による規律の対象となるインプットの処理成果の範囲を定めること、事業者に対して生成AIシステム関連の提供目的以外の目的でインプットの処理成果を原則として利用・保持しないことを目的外利用禁止義務として定めること、事業者がインプットの処理成果を利用することを認める場合の利用条件（学習の有無、データの保存方法等）を定めること、事業者がインプットの処理成果に関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。 ※RAGをコンポーネントに含む場合の納品物は、データベースが成果物となることが一般的であるが、関連するパーサー（RAG用テキストデータに変換するプログラム）、テキスト分割プログラム、ベクトル変換プログラムなどについても、成果物に含めるのか、WebAPI等を通じて機能を提供するのかを検討すること及びその権利帰属や利用方法を契約に盛り込むことが望ましい。
3	基本項目	生成AIシステムに係るアウトプット~~の~~に関する取決め	アウトプットについて、アウトプットの定義、事業者がユーザーに対してアウトプットを提供する義務の有無及びその内容、事業者に対してアウトプットに関する一定の保証を求めること、ユーザーがアウトプットを第三者に提供することができる場合にその条件を定める、事業者がユーザーに対しアウトプットを提供する場合にやアウトプットの権利帰属に関して定める条項	契約で規律の対象となるアウトプットとして、アウトプットの定義はユーザーのサービス利用目的を十分にカバーできるよう範囲を定めること、事業者がアウトプットを提供する義務がある場合にユーザーのサービス利用目的に照らして、提供条件（提供時期、頻度、態様その他の条件）や提供するアウトプットの内容（性質、量、粒度その他の内容）を定めること、事業者がアウトプットの保証・情報提供義務を負う場合の保証・情報提供の条件を定めること、第三者提供条件（提供先、提供範囲その他の条件）を定めること、ユーザーがアウトプットに関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。
4	基本項目	生成AIシステムに係るアウトプットの処理成果~~の~~に関する取決め	アウトプットの処理成果について、契約上規律の対象とするものの定義、ユーザーによる外部提供、権利帰属に関して定める条項	契約で規律の対象となるアウトプットの処理結果成果として、アウトプットの処理結果成果の定義はユーザーのサービス利用目的を十分にカバーできるよう範囲を定めること、サービス利用目的に照らして外部提供条件（提供先、提供範囲その他の条件）を定めること、ユーザーがアウトプットの処理成果に関して知的財産権等一定の権利を取得する場合には権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。
5	基本項目	生成AIシステムに係る契約上の取決め	事業者が生成AIシステムを構築するうえで期待品質を満たすための取組の履行又は完成させる義務を定める条項	~~請負契約で事業者が生成AIシステムを完成する義務を負う場合、ユーザーのサービス利用目的に照らして、どのような完成条件（完成時期、検収条件等）を定めるべきか検討して契約に盛り込むことが望ましい。~~ 期待品質に関する事項を契約に盛り込む前提として、納品物が何かを明確にする必要がある。生成AIシステムの開発の場合、生成AIモデルそのものが納品物でないときには、納品物としてシステムコンポーネント（ユーザーインターフェース・システムプロンプト・ファイルデータベース・ベクトルDB・入力フィルター・出力フィルター・外部連携コンポーネント 等）部分については、明確に特定することが望ましい。 生成AIシステムの期待品質を満たすために契約上、直接期待品質を契約条件に定める形態、又は、品質を確保するために実施すべき取組内容を定める形態があるが、納品物の性質及びその調達の目的を踏まえてどちらの形態を選択するかを検討する必要がある。 生成AIモデルに起因する性能・出力品質については、学習データや基盤モデル等の特性にも左右され、「○○以上の精度」等の成果保証を行うことが困難な場合があるため、その場合には、当該部分は成果保証ではなく、性能改善・品質向上に向けた技術的支援を受ける等の契約形態を取ることが望ましい。 但し、生成AIモデル以外のシステムコンポーネントに関しても、例えば「システムプロンプト構築を目的としたプロンプト設計・評価業務」を考えた際に、設計・評価・チューニングに関する部分は明確に成果物を定義することが困難と考えられるため、取組の履行有無について契約に盛り込むことが望ましく、性能要件を含めない形式としてのシステムプロンプト（指定された構造であり指定の要素が含まれている、トークン長の上限を満たす 等）、プロンプトのテストシナリオ、設定パラメータ群（回答の自由度や出力トークンの上限 等）については請負契約に基づく成果物とすることが考えられる等、その調達の目的を踏まえて契約における成果物の範囲が品質担保可能な範囲内かという点を慎重に検討する必要がある。
6	基本項目	生成AIシステムに係るノウハウの取決め	事業者又はユーザーのノウハウに関して、知的財産（※）として定義し、~~ノウハウの定義、~~ユーザーによる事業者の~~ノウハウの~~利用条件、事業者によるユーザーの~~ノウハウの~~利用条件、~~ノウハウの~~権利帰属に関~~する~~して定める条項 ※発明、考案、意匠、著作物その他の人間の創造的活動により生み出されるもの（発見又は解明がされた自然の法則又は現象であって、産業上の利用可能性があるものを含む。）、及び営業秘密その他の事業活動に有用な技術上又は営業上の情報をいう。	ノウハウの定義に合致しない情報については、適用法令による制限がない限り、事業者がノウハウを自由に利用できる可能性があるため、この条項により契約による規律の対象となるノウハウの範囲やユーザーおよび及び事業者による利用条件（※）、権利帰属等を定めることが望ましい。 ※特に事業者の技術開発や学習目的等のサービス提供目的以外の目的で利用することを許容するか、検討して契約に盛り込むことが望ましい。
7	基本項目	生成AIシステムに係る成果物の取決め	成果物について、成果物の定義、事業者のユーザーに対する成果物の完成義務又は完成条件及びその内容、成果物の権利帰属に関して定める条項	契約で規律の対象となる成果物として、成果物の定義はユーザーのサービス利用目的を十分にカバーできるよう範囲を定めること（※）、事業者が成果物を完成して提供する義務がある場合にユーザーのサービス利用目的に照らして、提供条件（提供時期、頻度、態様その他の条件）や提供する成果物の内容（性質、量、粒度その他の内容）を定めること、ユーザーが成果物に関して知的財産権等一定の権利を取得する場合の権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）を定めることが望ましい。 ※システムプロンプトをコンポーネントに含む場合の納品物は、プロンプトのひな形、プロンプト文及び設定パラメータ群（回答の自由度や出力トークンの上限 等）等が考えられるが、成果物の多様な形態を踏まえて、契約書等で成果物を明確に規定し、契約当事者間で成果物のイメージをあらかじめ共有しておく必要がある。
~~7~~ 8	基本項目	情報セキュリティインシデント・生成AIシステム特有のリスクケースが発生した場合の事業者の対応義務、協力及びその範囲に関する取決め	情報セキュリティインシデント・生成AIシステム特有のリスクケースが発生した場合、事業者に求める対応義務や協力、関係するデータの提供等を求める条項	事業者において発生した情報セキュリティインシデント・生成AIシステム特有のリスクケースによる被害を最小限に食い止めること、また原因を特定するための情報やデータ（具体的には生成AIシステムの学習データやアルゴリズムを含み得る）を政府の求めに応じて合理的な範囲で提供すること、サービスの停止や情報セキュリティインシデント・生成AIシステム特有のリスクケースの原因を特定し、改善措置を講じること、必要に応じ監査を行うこと等について、あらかじめ事業者と合意しておく必要がある。
~~8~~ 9	基本項目	期待品質が満たされなくなった場合等において、そこから生じる被害を最小限に食い止めること及び、原因を特定し改善措置を講じる取決め	生成AIシステムの期待品質が満たされなくなった場合等において、そこから生じる被害を最小限に食い止めること及び、原因を特定し改善措置を講じることを求める条項	生成AIシステムの期待品質が満たされなくなった場合等において、そこから生じる被害を最小限に食い止めること及び、原因を特定し改善措置を講じることについて、あらかじめ事業者と合意しておく必要がある。