

「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 改定案に対するご意見及びその考え方

デジタル庁

1.実施期間

令和8年3月18日(水)～4月8日(水) 21日間

2.意見提出数

合計:172件

(1)法人・団体: 9法人・団体(25件) (「3.意見提出者」に記載)

(2)個人:147件

3.意見提出者

(一社)AIガバナンス協会、(株)グラファー、Cell Dynamics(同)、(株)セールスフォース・ジャパン、日本電気(株)、(株)Box Japan、(株)Preferred Networks、富士通(株)、楽天グループ(株)

※法人・団体と事務局で判断できるもの以外のご意見は個人としてカウントしておりますので、ご了承ください。

※50音順

大項目	中項目	小項目	累計数
A. ガイドラインの内容に直接関係するご意見とその考え方	ガイドライン本紙	1.1 背景	2
		1.3 用語	1
		2.1 本ガイドラインの目的	1
		2.2.2 本ガイドラインが対象とする生成AI	3
		2.2.3 本ガイドラインの対象者	2
		3.1 政府における生成AIの利活用方針	1
		3.2 高リスクな生成AI利活用の考え方	20
		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	1
		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	2
		4.2.2 先進的AI利活用アドバイザリーボードへの報告	1
		5.1 生成AIの便益	3
		5.2 生成AIによるリスク	2
		6.1.1 各種法令・ガイドライン等を踏まえた対応事項	20
		6.1.2 本ガイドラインに基づく対応事項	6
		6.3 政府における生成AIシステムの企画者の対応事項	1
		6.3.1 生成AIシステムの企画時の対応事項	2
		6.3.2 生成AIシステムの調達時の対応事項	6
		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	1
		6.5 政府における生成AIシステムの提供者の対応事項	4
		6.7 生成AIシステム特有のリスクケースへの対応	2

※中項目のガイドライン本紙に係る記載において、見出しが記載されていない章については該当する意見がなかった章である。

※本表については、提出された意見の内容を踏まえて意見内容のマッピングを実施しているため、提出意見数の合計と一致するものではない。

大項目	中項目	小項目	累計数
A. ガイドラインの内容に直接関係するご意見とその考え方	ガイドライン本紙	7 今後の進め方	4
		附則	3
	別紙2 生成AI利活用ルールひな形	別紙2 生成AI利活用ルールひな形	6
	別紙3 調達チェックシート	別紙3 調達チェックシート 全般	3
		別紙3 調達チェックシート 生成AIシステムの基本機能要件全般	3
		別紙3 調達チェックシート 要求事項#7	2
		別紙3 調達チェックシート 要求事項#11	1
		別紙3 調達チェックシート 要求事項#12	5
		別紙3 調達チェックシート 要求事項#13	1
		別紙3 調達チェックシート 要求事項#20	2
		別紙3 調達チェックシート 要求事項#23	1
		別紙3 調達チェックシート 要求事項#24	3
		別紙3 調達チェックシート 要求事項#25	5
		別紙3 調達チェックシート 要求事項#26	3
		別紙3 調達チェックシート 要求事項#27	3
		別紙3 調達チェックシート 要求事項#29	2
		別紙3 調達チェックシート 要求事項#30	1
	別紙4 契約チェックシート	別紙4 契約チェックシート 取決め事項#1	2
		別紙4 契約チェックシート 取決め事項#2	1
		別紙4 契約チェックシート 取決め事項#5	2

※中項目のガイドライン本紙及び別紙に係る記載において、見出しが記載されていない章については該当する意見がなかった章・項目である。

※本表については、提出された意見の内容を踏まえて意見内容のマッピングを実施しているため、提出意見数の合計と一致するものではない。

大項目	中項目	小項目	累計数
A. ガイドラインの内容に直接関係するご意見とその考え方	別紙4 契約チェックシート	別紙4 契約チェックシート 取決め事項#6	1
		別紙4 契約チェックシート 取決め事項#8	2
	ガイドライン全体	全体的な方針に賛成	2
		全体的な方針に反対	19
		全体的な方針に反対(リスクに着目した反対意見)	18
		本ガイドライン全体の改善提案	10
		本ガイドライン全体への意見	3
B. A以外で多く寄せられたご意見とその考え方	国産の生成AIの開発を支援すべき		1
	(生成)AI反対の意見		12
	生成AIによる不利益への懸念		8
	学習・開発時のデータ等に関するご意見		13
	AI関連の政府の政策、法規制の在り方に対する意見		32
	環境への負荷に関する意見		3
	パブコメ実施期間・実施方法等に対する意見		2

※中項目のガイドライン本紙及び別紙に係る記載において、見出しが記載されていない章については該当する意見がなかった章・項目である。
 ※本表については、提出された意見の内容を踏まえて意見内容のマッピングを実施しているため、提出意見数の合計と一致するものではない。

A. ガイドライン案の内容に直接関係する ご意見とその考え方

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

1.1 背景

P1の1.1背景の3段落目中「人口知能関連技術の研究開発及び活用の推進に関する法律」、「人口知能基本計画」、「人口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」の法律番号、閣議決定の括弧書きがカギ括弧内と外にそれぞれ記載されているが、平仄が合っていないのではないか。法令の規定でもないため法律名の補足情報として法律番号もカギ括弧の外に出して記載しても問題無いように思われるが如何。(法令の規定であっても初出の箇所に法律番号を付しているが、この法律番号も法律名として取り扱っているわけではない。)【個人】

ご意見のとおり修正いたします。

1.1 背景

冒頭の背景から本ガイドラインに至るまでの整理が甘い。そもそもこうしたガイドラインでは逐条列記したうえで、このガイドラインはどのような位置付けであると説明するのが筋なのに、単に遵守するドキュメントと一文である。さらには整理が甘いことにより、例えば広島AIプロセスといった、国際的な規範との整合性の関係も見えづらくなっている。他国が定めたのを追うのは任意であるが、せめて本邦が国際的に打ち出したものくらいは本ドキュメントでも位置づけと関係性を触れるべきと考える。【個人】

ご意見として承ります。本ガイドラインは、広島AIプロセスを含む国際的な議論を踏まえて検討された「AI事業者ガイドライン」を踏まえて整理したものです。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

1.3 用語

並列に定義されているAI／AIモデル／生成AI／生成AIモデル／LLM／AIシステムは「AIシステム」に集約し、相関を明確に示してその違いを説明すべきである。また「ステークホルダー」は2.2.3項に沿って最終受益者等として具体化し、行政実務での適用を明確にすべきである。【個人】

原案では、各用語の相互関係が分かるよう、他の用語の定義を参照しつつ整理しているため、原案のとおりとさせていただきます。

なお、「2.2.2 本ガイドラインが対象とする生成AI」以降では、本ガイドラインの対象となる生成AIモデルを構成要素として含む生成AIシステムを指すものとして、主として「生成AIシステム」の語を用い、必要に応じて他の用語も用いています。

また、「ステークホルダー」は最終受益者に限定されないため、原案のとおりとさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

2.1 本ガイドラインの目的

国際的な相互運用とありますが、重要な情報を外国政府や事業者とやりとりする可能性があるということですか？（直接のやり取りは無いかと思いますが、利用家庭のうちに情報を入力する行為があるためにそのように感じました。）【個人】

ガイドラインの相互運用性と、個別具体の情報のやりとりは別個の問題であり、関連はございません。

2.2.2 本ガイドラインが対象とする生成AI

・公正証書PDFや地図画像、災害動画等、マルチモーダル技術は行政実務で利用されており、生成AIの入力に既に含めて然るべき段階と考えるべきである。【個人】
・本ガイドラインが対象とする生成AIのうち、何故動画生成AIだけ外されているのか、理解できない。かなり批判が噴出した生成AIだったと記憶しているが。【個人】

画像や動画等を入力するもの、動画等を生成するもの、より高度なタスクを実行できるもの（AIエージェント等）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ております。

これらの生成AIを対象とするガイドラインの
スコープ拡大は、今後の検討事項とさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

2.2.2 本ガイドラインが対象とする生成AI

本ガイドラインの対象外であるAIエージェントについて、各府省のリスク評価による判断で利用可能と明記された点を歓迎します。一方で、真にAIエージェント実装を本格化させその便益を得るためには、ガイドラインによる指針がやはり不可欠と考えられます。そのため、次回の改定で本ガイドラインの対象に含むことを視野に入れて、民間との意見交換含めてご検討をさらに加速していただくことを希望します。

実際に民間では、ガードレール等のビルトイン且つカスタマイズ可能なリスク低減・管理機能を前提に、AIエージェントの利活用が進んでおります。更に弊社含む様々な企業が行政ニーズに特化したサービスを提供しており、海外の公共機関での活用も徐々に進んでいるところです。今後のご検討において最新の安全な行政向けAIエージェントサービスの調査（ヒアリングや実証等）が必要な場合、民間からも喜んで協力させていただきます。【セールスフォース・ジャパン】

AIエージェントに係る今後の運用・改定の検討にあたって参考とさせていただきます。

2.2.3 本ガイドラインの対象者

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改定案のp6.7の本ガイドラインの対象者に関して、開発者のデータ収集とありますが、その収集されるデータの権利者は、どのような扱いになるのでしょうか？【個人】

開発者が収集したデータの権利関係の観点については、「別紙3 調達チェックシート」も踏まえて、法令・契約等に従い整理することとしております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

2.2.3 本ガイドラインの対象者

「※ 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や本ガイドラインに基づく取組を確保することとする。」

じゃあ責任はまるまる国にあると考えていいのか？開発企業のやらかしは、国が賠償を負うということでした承したと理解する。【個人】

当該記載は、本ガイドラインの適用対象者を整理するものであり、国が一律に全責任を負う趣旨ではありません。責任の有無・範囲は個別案件ごとの契約により取り決められ、問題が起きた場合の責任は個別事案に応じ、関連法令に基づき判断されます。

3.1 政府における生成AIの利活用方針

冒頭は従来のIT一般の利用利益に留まり、生成AI特有の実利が不明確である。従来のITが演繹的なルール処理に基づくのに対し、生成AIは帰納的推論により多様な文脈を踏まえた応答生成が可能である。この特性は職員の効率化にとどまらず、多様な国民の状況に応じた個別化された行政サービスを実現し、行政への信頼向上にも資することを明記すべきである。【個人】

生成AIの便益については、「5.1 生成AIの便益」にて整理しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

3.2 高リスクな生成AI利活用の考え方

- ・表4リスク軸とその考え方＞旧項目「C.要機密情報や個人情報の学習等の有無」(削除)(P.11)および、図 リスク判定ロジック(P.15)当該箇所は削除すべきではなく、個別に記載が必要、あるいは更新が必要な内容と考えられます。【個人】
- ・p11の表にある斜線の引かれたCの部分に関しては、リスクとは考えていないのでしょうか？【個人】
- ・p11表4で削除されているcの項目に示されている問題は、現在も解決していない。なぜ削除したのか説明を求める。【個人】
- ・なぜ個人情報関連項目をまるごと削除したのかわからない。個人情報の取り扱いは明らかに高リスクであり、最新の注意を払うべきものであるからして、本来ならここは「生成AIに個人情報は一切入力してはならない」と記載するべきではないのか。【個人】
- ・要機密情報や個人情報の学習が消されているが、個人情報を学習させるというのはリスク軸のAに該当する。【個人】
- ・リスクについて「要機密情報や個人情報の学習等の有無」の項目が消されていましたがもってのほかです。全ての企業、すべての国民が、知られたくない情報を漏洩・利用されるリスクを背負うことになります。【個人】
- ・C 要機密情報や個人情報の学習等の有無について、なぜ削除してあるのか分かりません。現在でも例えば企業が写真をユーザーにアップロードさせ、AIで加工する企画などが、責任をユーザーに持たせる形で横行しています。入力内容が画像であれ文字列であれ、リスクがあることを無かったかのように扱うのはやめてください。【個人】
- ・本ガイドラインのP11の表4リスク軸とその考え方内、C要機密情報や個人情報の学習等の有無の「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。」も高リスクに分類されるべきであり、生成AI、入力や学習をさせるべきではありません。【個人】

初版におけるリスク判定ロジックの「C.対象データ」については、政府情報システムは情報セキュリティ統一基準に基づく情報の格付に応じたアクセス制御を行うことに加え、要機密情報が入力・学習等される場合を想定した生成AIシステム特有のリスク対策を必須の実施事項とすることとし、リスク判定ロジックからは外すこととしました。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

3.2 高リスクな生成AI利活用の考え方

・p11の政府職員や、外部利用者でも特定の者（地方公共団体や民間企業等）が自身の生成 AIの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場合、と書かれていますがどのように判断が可能であると判断するのでしょうか？【個人】

・「自身の生成AIの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」とあるが、判断が可能であるとの判断は誰がどうやって決めるのか。の高さに反して基準が極めて曖昧に思う。【個人】

リスク軸とその考え方は、CAIOによる最終判断の参考となる考え方を整理したものです。リスクレベルについては、各府省庁のCAIOが企画者と連携しつつ、ユースケースに応じた評価を行い、そのレベルを適切に判断することを前提としております。

その上で、「自身の生成AIの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」であるかについては、利用者の生成AIに関する知見や、当該業務等に関する知識・経験の有無等を踏まえて、判断することを想定しております。例えば、当該組織において生成AIに関する研修等を受講している者や業務に継続的に従事している者等が想定されます。

3.2 高リスクな生成AI利活用の考え方

AIエージェントが自律的にタスクを実行する際、動的プロンプトへの依存のみならず、バージョン管理されたポリシーに基づく動作を必須とすべきです。これによりCAIOは高リスク業務（リスク軸A-1）における自律的判断の瑕疵を事前に抑制し、行政法に準拠した一貫性のある制御と説明責任の履行が可能となります。【Cell Dynamics 合同会社】

ご意見として承ります。AIエージェントに係る今後の運用・改定の検討にあたって参考とさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

3.2 高リスクな生成AI利活用の考え方

・高リスク判定シートは職員の判断の有無のみで高低を分類しており、2024年にハーバード大学のDanielle Allenらが指摘する複雑なリスクの過度な単純化や形式的運用による誤った安心感に該当する懸念がある。行政実務のリスクは判断の有無だけでなく、影響範囲、データの機微性、利用者特性、外部依存度等に依存するため、更に多面的な評価軸を検討すべきである。

【個人】

別紙1高リスク判定シートでは、ガイドライン本紙「3.2 高リスクな生成AI利活用の考え方」に記載しているとおり、出力結果の政府職員等による判断の他、生成AI利活用業務の性格や生成AIシステムの利用範囲も踏まえてリスクレベルを判断することとしております。

3.2 高リスクな生成AI利活用の考え方

・本改定案において、高リスク判定ロジックを見直し、適用業務・利用範囲・職員等による出力結果の判断を基軸として整理した点は妥当と考えます。特に、AIエージェント等について、出力結果の適切さを人が十分に判断しない運用の影響が未知数であることを踏まえ、高リスク側に寄せて扱う方向性は適切です。その上で、3.2には「高リスク」と判定された後の追加的取扱いとして、運用開始後の継続監査、ログ保存、判断根拠の追跡可能性、異常兆候発生時の停止又は縮退運転条件を明記することを提案します。高リスク判定は入口管理として重要ですが、実際の事故や不適切運用は運用段階で顕在化することが多いため、高リスク案件については、導入時評価だけでなく、運用中に監査可能な状態を維持することまで制度要件化すべきと考えます。【個人】

・政府職員や、特定の外部利用者（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）が利用する場合で、生成内容の出典が容易に参照可能な場合について、高リスクの可能性が低いとする考え方に賛同します。

今後、安全に利用するための技術のさらなる進展や利用者等の知見の蓄積も踏まえて定期的にリスク判定シートが見直されることを期待します。【セールスフォース・ジャパン】

今後の運用・改定の検討にあたって参考とさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

3.2 高リスクな生成AI利活用の考え方

・そもそも高リスクな生成AI利活用のケースが存在する時点で、国民の生活に直結する行政の業務に使用すること自体がおかしく、高リスクな使用方法であると判断されうる事例において生成AIを使用することは不適當である。

高リスクな使用方法である可能性が生じた時点で、その使用方法是差し止めるとガイドラインに明記するべきである。そもそも、各人の生成AIの使用についてレベルを判断すること自体が管理者の負担を増加させる要因であり、簡単に言えば余計な仕事を増やしていることに他ならない。

場合によって判断させるのではなく、一律に、しかも厳格にセーフラインを引き、そのラインを超える場合は一律使用を禁止するぐらい厳しい規律を設けるべきである。このガイドラインを作成した担当者は国民の生活を担っている自覚があるのか、甚だ疑問である。【個人】

生成AIの利活用にあたってはリスクが伴いますが、本ガイドラインは生成AI利活用推進のためのガードレールであり、生成AIの安心・安全な利活用を着実に進展させ、利益の実現を目指すものです。

高リスクの可能性が高い生成AIの利活用であっても、先進的AI利活用アドバイザリーボードの助言やAI相談窓口への相談等も活用しながら、適切な軽減措置を講じることにより、リスクを軽減しつつ、生成AIの利活用推進を可能とすることとしております。

・「出力結果の適切さを判断せずに利用する」AIエージェント等の判定を高リスクに一本化し、「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」も同様の整理とされている。しかし「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適用しない」軽微な自動返信メールを作成・送信するものまで高リスクとすることは、AIエージェント等の利活用を過度に委縮させるおそれがある。適用業務や利用範囲等に照らして総合的に低であると判断できるものは例外的に低と判定できる仕組みを設けるべき。【楽天グループ】

ご意見として承ります。今後の運用・改定の検討にあたって参考とさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

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
・アドバイザリーボードとCAIOが連携しながら、最終的にはCAIOが高かどう
か判断する。ということと理解しています。行政機関が扱う情報の性質上、
アドバイザリーボードとCAIO間での意見交換の往復が日常的に起こること
になるかと思いますが、この運用の仕方は現実的ですか？
各部署に必ず一人はアドバイザリーボードとして選出されるような人材がい
ないと、まっとうに業務を遂行していくのは難しいと考えます。
また、生成AI利用の等の研修を行うこととありますが、これは定期的に行う
ことを必須とする必要があると感じます。【個人】

高リスクの可能性のある生成AIシステム
については、先進的AI利活用アドバイ
ザリーボードに報告される仕組みとしており、
その過程を踏まえてCAIOがユースケ
ースのリスクレベルを判断することとしてお
ります。
研修については、ガイドラインに基づき、
各府省庁においてCAIOが実施することと
しております。

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
・アドバイザリーボードについて どのような人が構成員として選定されま
すか？デジタル庁HPなどどこでも構いませんが、構成員の名前や来歴、選定
基準などを国民すべてが閲覧できる場所への明示を求めます。【個人】

先進的AI利活用アドバイザリーボードの
構成員名簿(※)は、デジタル庁のホーム
ページにて公開しております。構成員は、
AIの制度、利活用、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)等から選定しております。

※[先進的AI利活用アドバイザリーボ
ード構成員名簿](#)

ガイドライン本紙

提出された主なコメント

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
・クラウドの生成AIシステム(ChatGPT等)など一般に知られる生成AIシステムは、インターネット上のコンテンツを収集しているとされており、かつ入力においても「オプトアウト」が標準・無償で設定されていないことがあり、個人情報や知的財産(コンテンツ)の流出について懸念をしています。こうした侵害について、内部通報や外部意見・通報窓口の設置を要望します。また、通報があった内容について、可能であれば個別、最低でも月例での対応状況を報告することにより、適切な知的財産の管理がなされることを強く希望します。【個人】

ご意見に対する考え方

生成AIシステムに係るインプット及びインプットの処理結果に関しては、別紙4契約チェックシートを活用した取決めによる対策を実施することとしております。

個人情報や知的財産権等の保護は、ガイドライン本文や別紙3調達チェックシート、別紙2利活用ルールひな形に基づき作成された各府省庁における利活用ルール等で対策することとしております。通報については、ご意見として承ります。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

4.2.2 先進的AI利活用アドバイザリーボードへの報告

本改定案において、各府省庁のAI統括責任者（CAIO）が、生成AIシステムの運営状況及び行政における生成AI利活用状況を定期的に取りまとめ、四半期に一度程度を目安としてアドバイザリーボードへ報告する仕組みを設けた点は高く評価します。その上で、報告事項について、単なる案件一覧や運用状況にとどめず、少なくとも以下を共通様式で含めることを提案します。

1. 高リスク判定の理由
2. 実施した軽減策
3. 発生したインシデント又はヒヤリハット
4. 停止・縮退運転を行った有無と判断理由
5. 監査で確認された是正事項
6. 他府省庁でも再利用可能な知見

アドバイザリーボード報告を横断学習の基盤として機能させるには、報告内容の標準化と、監査結果・停止判断を含む実運用知見の共有が重要です。これにより、政府全体でのAIガバナンス水準の底上げが可能になると考えます。【個人】

各府省庁からの生成AIシステムの定期報告や生成AIシステム特有のリスクケースの報告については、先進的AI利活用アドバイザリーボード（事務局）において知見を集積し、「各府省庁AI統括責任者（CAIO）連絡会」を通じた情報共有に活用するとともに、必要に応じガイドライン改定に際しての参考とすることとしております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

5 生成AIによる便益とリスクを理解した利活用推進

・P20以降の『表5 便益の例』およびP22以降の『表6 リスクの例』について。こちらについても、両方の例題を削除したのは何故か？特にリスクに関しては、不利益を回避するためにも具体例を挙げるべきであるが、経産省としては不利益を回避する意思がないのか？上記の削除により、機密情報入力を促しかねない危険を覚えるが、そのような意図があるのか？【個人】

・p20.21の便益の例、p22からp24のリスクの例に関して、すべて斜線が引かれています。具体例は出さないのでしょうか？【個人】

初版における「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」及び「表6 AI 事業者ガイドラインにおけるリスクの例」は、本ガイドラインのスリム化の一環で削除いたしました。本改定にて削除した便益及びリスクの例は、全て「AI事業者ガイドライン」からの引用であり、「AI事業者ガイドライン」においては、AIによる便益や一般的なAIのリスクが整理されています。

なお、本文では「AI事業者ガイドライン」にも言及する形で政府のAI調達・利活用において留意すべきリスクの例を引き続き記載しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

5.1 生成AIの便益

表5で削除された便益例は、利活用ルールひな形を用いて各府省が自らの業務に即して実践的に整理できるよう別紙2の中に残すべきである。【個人】

初版における「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」は、全て「AI事業者ガイドライン」の記載を整理したものであり、本文を総則的な記載に整理する観点から削除いたしました。別紙2は利活用ルールのひな形であり、便益の例を盛り込むことはその趣旨に照らして適当ではないと考えられるため、原案のとおりとさせていただきます。

5.1 生成AIの便益

P20の5.1生成AIの便益の2段落目中「政府においても、…『このような』便益…」と記載されているが、その直上のハコを指しているのであれば『このような』ではなく『上記のような』と指し示す方が一般的な記載ぶりではないか。【個人】

当該箇所は、直上のAI事業者ガイドラインの記載の抜粋を指し示す意図はなく、政府においても、生成AIの利活用による便益が期待される旨を示す記載でしたが、ご意見を踏まえて、「政府においても、生成AIの利活用による便益が期待され、こうした便益は…」と修正いたします。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

5.2 生成AIによるリスク

・「AI事業者ガイドラインにおけるリスクの例」の項目を削除するのはなぜでしょうか？

【個人】

・生成AIによるリスクのほとんどに取り消し線が引かれているが、そのリスクは無くなったと考えているのか。少なくとも現時点で自分の目線から見える生成AIのリスクは決して減っては居ないと感じている。【個人】

・表6の内容についても、生成AIのリスクを理解する上で重要な情報である。削除すべきでは無い。【個人】

・生成AIのリスク例を削除している理由が分かりません。昨今は生成AIによる予測していなかった損害の報道もあり、企業側も使用を躊躇することが多いと聞きました。こうやって例示されまとまっていると、見る側もわかりやすく、企業側も参考にしやすい表や解説だと思います。この表をつかわないのはもったいないと思います。削除はせず、そのままガイドラインに載せていただきたいと思います。【個人】

・AI事業者ガイドラインにおけるリスクの例が全て消されているが、これは事業者が守るのではなく、府省庁職員が守るガイドラインなので消したという意味でよろしいか。全て重要なリスクだが。【個人】

初版における「表6 AI事業者ガイドラインにおけるリスクの例」は、本ガイドラインのスリム化の一環で削除いたしました。本改定にて削除した表は、全て「AI事業者ガイドライン」の記載を整理したものであり、「AI事業者ガイドライン」においては、一般的なAIのリスクが整理されています。

なお、本文では「AI事業者ガイドライン」にも言及する形で政府のAI調達・利活用において留意すべきリスクの例を引き続き記載しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

5.2 生成AIによるリスク

・今回の改定案で、旧案に含まれていた「知的財産権の侵害」「労働者の失業」「偽情報の拡散」「民主主義への悪影響」、さらには「環境負荷(電力消費)」といった、現代社会が直面している極めて重要なリスク項目が大幅に削られていることに、強い憤りと不信感を抱きます。行政がAIを導入・推進するにあたり、以下の懸念を「なかったこと」にすることは断じて許されません。【個人】

・リスクの具体例を消す意図が分かりません。現在の国会議員ですらハルシネーションの存在を知らないように見えたり、AIが出力するものが間違っていないと思いつているように見えます。政府内で利用するなら、まず正しい知識とリスク管理について周知してください。【個人】

・具体例を意図的に削除することは、制度の柔軟性を確保する側面がある一方で、結果として「責任回避的な効果を持つ設計」になっていると評価せざるを得ない。【個人】

・IT知識を問わず幅広く国民に利用を促す行政サービスにLLMを組み込む上では、最終利用者のリスク許容度や本人確認・年齢制限等の利用制限の設計視点を踏まえ、これらのリスクを本項で整理して検討すべきである。【個人】

初版における「表6 AI事業者ガイドラインにおけるリスクの例」は、本ガイドラインのスリム化の一環で削除いたしました。本改定にて削除した表は、全て「AI事業者ガイドライン」の記載を整理したものであり、「AI事業者ガイドライン」においては、一般的なAIのリスクが整理されています。

なお、本文では「AI事業者ガイドライン」にも言及する形で政府のAI調達・利活用において留意すべきリスクの例を引き続き記載しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

5.2 生成AIによるリスク

・「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」の部分には、テキストに関するリスク留意が抜けている。テキストにも著作権があることを軽視していると取られかねないと言える。【個人】

・「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」について、以下の修正を提案します。提案:「生成 AI を用いて出力したコンテンツ(※)が」(※注釈で「文章、画像、動画、プログラム等、知的財産権により保護されるもの」等の記載を追記)【個人】

理由:「6.7.生成 AI システム特有のリスクケースへの対応」にも記載があることは承知していますが、対象とする生成AIを文章、画像等に限らず定義していることから、広範な分野を扱う汎用生成AIに相当するものを想定していると認識しています。これらは実際に商標に酷似したロゴなど「頻繁に学習したコンテンツ」を出力することがあり、「実際にどのような出力がされることがあるか」の知識は、専門職(知的財産系の制作者や法務担当者)相当の十分な知識が必要であると考えます。【個人】

・リスク例示の7ポツ目(生成AIによって出力した画像がで始まる部分)について、画像のみ列挙されているが、文章および個人情報情報を追加すべき。【個人】

・リスクの例示として、テキストデータや書籍、記事といったものに係るリスクの記載がないように思われます。想定されるリスクを事前に多く周知する事が必要であると考えられるため、テキストデータや書籍、記事に関しても記載されるべきであると思われます。【個人】

ご意見を踏まえ、「**画像等の出力結果**が、既存の著作物に類似した要素を含んで出力され、その状態に気付かないまま利用してしまうリスク」と修正いたします。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

5.2 生成AIによるリスク

p.24にて政府における生成 AI の調達・利活用における複数のリスクが例示されている。その中でも以下のようなリスクについては実際に起こってはならないものである。

- ・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
- ・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

実際に上記のような問題が起きた時、AI 統括責任者(CAIO)がどのような責任を果たすのかが気になる。

また、どうすればこうした問題の発生を避けることができるかについて正しい知識を持ったものがAI 統括責任者(CAIO)を担うべきである。そのため選定基準も客観的にその役職を担う資格ありといえるような基準が設定されているべきである。

【個人】

生成AIシステム特有のリスクケースが発生した場合、各府省庁において整備されたリスクケースへの対応手順に従い、「6.7 生成AIシステム特有のリスクケースへの対応」に記載されているとおり、CAIO及び生成AIシステムの提供者が中心となり、重要度・影響の程度等を踏まえ、適切な対応を行うこととしております。各府省庁は、リスクケースの発生時及び対応後に先進的AI活用アドバイザリーボード(事務局)に報告することとしております。

また、各府省庁のCAIOは、「デジタル統括責任者」又は「副デジタル統括責任者」級の職員が担うこととしております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

5.2 生成AIによるリスク

- ・生成AIの開発段階・学習段階でのリスク評価に殆ど言及していないことも改善すべきである。現状のほとんどの画像、音声、テキスト生成AIは、開発過程で用いられたデータセットに著作権や肖像権を侵害する画像、音声、テキスト、もしくは違法な現場を撮影した写真等が多数含まれている。また、派生的なモデルを作成する上で、上記のようなデータを(他人の権利物であると知った上で)使用することもある。当ガイドラインでも言及されているが「既存の著作物」や「個人の声質や話し方」に類似した出力を生成AIが返す理由は、著作物や個人の音声を無断学習しているからに他ならない。学習データと同様の形式で出力する生成AIにおいて、学習データとしての権利物の使用は著作権法における「享受」目的の使用と考えられ、同法30条の4で示される「利用」には当たらないと思われる。以上から、学習段階での他者の権利侵害リスクを重視し、ガイドラインに明記すべきである。【個人】
- ・現行の生成AI全般の学習元データが違法性のある内容(海賊版著作物、児童ポルノ等)を含むこと、生成AIの利活用にあたっては学習データの透明性と適法性が確保されたものを選択することを明記すべき。【個人】

ご指摘の知的財産権等の侵害等のリスクに対しては、生成AIシステムの調達段階は別紙3調達チェックシート、利用段階は別紙2利活用ルールひな形に対応事項を記載しております。

別紙3調達チェックシートでは、「評価・選定時の分類」に当てはまる場合は、学習段階、生成段階に関する要求事項を踏まえて調達を実施することとしております。

別紙2利活用ルールひな形においては、生成AIシステムの利活用時の知的財産権等に係る対策を整理し、プロンプト入力段階及びAI生成物の利用段階におけるルール・対策例を記載しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

5.2 生成AIによるリスク

・「5.2 生成AIによるリスク」で認識されているリスクはすべて国民の不利益、財産の損失、さらには生命にも関わる可能性があるもので看過できるものではありません。【個人】

・ユースケースばかり語り、個人情報が個々人の財産であり、人権が擁護するものであるという認識が欠けています。リスクは実際に起きた被害であり今後起こる被害です。規制緩和はリスクを、被害を増やすのみです。行政にとっては一件の報告であっても、被害者本人にとっては一生かかっても取り戻すことのできない財産の喪失等の被害になります。GDPRのような個人情報を人権として、それを擁護するのならともかく、AIのような人権侵害を助長するものに対して、規制を緩和するなど言語道断です。憲法が保障する権利の侵害です。【個人】

生成AIの利活用にあたってはリスクが伴いますが、本ガイドラインは生成AI利活用推進のためのガードレールであり、生成AIの安心・安全な利活用を着実に進展させ、利益の実現を目指すものです。

高リスクの可能性が高い生成AIの利活用であっても、先進的AI利活用アドバイザリーボードの助言やAI相談窓口への相談等も活用しながら、適切な軽減措置を講じることにより、リスクを軽減しつつ、生成AIの利活用推進を可能とすることとしております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.1.1 各種法令・ガイドライン等を踏まえた対応事項

・「※ 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收を受ける可能性がある」ということは、他国に国内の府省庁及び国民の個人情報公開するということか。他国への機密事項の漏洩、内政干渉の可能性があるのに、このガイドラインを作っただけで十分だと考えているのか。【個人】

当該記載は、政府職員による生成AIの業務利用にあたっての国外サーバ利用時のリスクを注意喚起するものであり、個人情報や機密情報の公開を許容する趣旨ではありません。「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、不特定多数向けの定型約款等への同意のみで利用可能なクラウドサービスでは、原則として要機密情報を取り扱えないこととされております。

6.1.1 各種法令・ガイドライン等を踏まえた対応事項

■原文：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收を受ける可能性がある。

■変更案：…検閲や接收を受ける可能性がある。ただし、API経由での利用かつデータが学習に利用されない（ゼロデータ保持等の）規約が担保されている場合は、当該リスクを低減できるものとして評価する。

■意見理由：外国製のクラウド型LLMを利用する場合、サーバが国外にあることは避けられません。検閲や接收のリスクのみが強調されると、外国製LLMを利用したサービスの導入障壁となるため、データ非保持（ゼロデータリテンション）契約等によるリスク低減効果も併記すべきです。【グラファー】

政府機関として生成AIの利活用にあたって留意すべきリスクであるため、原案のままとさせていただきます。また、「学習に利用されない」規約等については、契約チェックシートの取決め事項#1にて、学習の有無を利用条件として定めることを補足説明として記載しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.1.1 各種法令・ガイドライン等を踏まえた対応事項

・ISMAPはクラウド基盤のセキュリティ管理を対象とする制度で生成AI固有のリスクを評価する枠組みではなく、その安全性評価として十分でない上、事業者の参入を不必要に制限するおそれがあり削除すべきである。【個人】

ISMAPは、政府のクラウドサービス調達において必要なセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とする制度です。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、別途本ガイドラインによる対応を求めています。ISMAPでは生成AI固有のリスクを評価するものではなく、その点は本ガイドラインに基づき対応することとしています。

要機密情報を取り扱うクラウドサービスとして生成AIシステムを調達する場合には、政府情報システムのためのセキュリティ評価制度（ISMAP）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から選定した上で、別途本ガイドラインによる対応を行う必要があります。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.1.1 各種法令・ガイドライン等を踏まえた対応事項

・政府調達セキュリティ評価をクリアしたクラウドサービス一覧においては、ISMAPクラウドサービスリストとISMAP—LIUクラウドサービスリストのみであるところ、今般の改訂で『等』を用いる趣旨如何。あえてISMAP—LIUクラウドサービスリストを記載しないこととする改訂を行う必要性が理解できないため、特段の事情が無いのであれば初版のままとしておくべきではないか。【個人】

・行政向けにサービスを提供する際、基盤として利用する個々の最新生成AIモデル(LLM等)が全てISMAPに個別登録されるのを待つ必要がなくなります。SaaS事業者が最新技術を迅速かつ柔軟に行政へ提供しやすくなり、ビジネス上非常に追い風となります。【グラファー】

ご意見として承ります。今後の運用・改定の検討にあたって参考とさせていただきます。

6.1.1 各種法令・ガイドライン等を踏まえた対応事項

・■原文: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。

■変更案:…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(追記:ただし、API利用等のサービス形態によりシステムプロバイダ側で一元的に対策が講じられている場合等、単独の対策で十分なリスク低減が図られると評価される場合はこの限りではない。)、リスクを低減することが必要である。」

■意見理由:「複数の対策」が必須であるかのように読めるため、API提供者(OpenAI等)のセキュリティ機能で既に十分な防御が担保されている場合であっても、SaaS事業者側で無駄な多重防御(開発・運用コストの増大)を強いられるリスクがあります。実質的なリスク低減が図れていれば柔軟な対応を認めるべきです。【グラファー】

当該記載は、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を前提にしたものであり、そうでないと評価される場合に複数の対策を講じることを求めるものではありません。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.1.2 本ガイドラインに基づく対応事項

「導入類型…(中略)…ユースケースの性格等を踏まえ、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」という内容には同意しつつ、当該リスクレベルやユースケースに応じて、望ましい取捨選択や拡充を判定するための補助となる事例拡充を要望する。
また、現状では高リスクか否かのみ区別されているところ、必要に応じてリスクレベルをより詳細に分割し、同リスクレベルに応じて採るべき要求事項・取決め事項を明確化することを検討いただきたい。【AIガバナンス協会】

今後、各府省庁の事例が蓄積された段階で、アドバイザリーボード等を通じての共有を検討しております。

また、「リスクレベルに応じて取るべき要求事項・取決め事項を明確化すること」について、要求事項及び取決め事項は個別具体の案件ごとに項目の取捨選択や拡充を行う前提としており、一律で項目の選定基準を設けることはしていません。リスクレベルの詳細な分割については、各府省庁における利活用実態を踏まえ、今後の検討の参考とさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.3.1 生成AIシステムの企画時の対応事項

「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、入力者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。」と書かれていますが、要機密情報及び個人情報が生成AIに学習された場合や漏洩した場合、意図せぬところで国民の生活が脅かされる可能性があります。要機密情報及び個人情報は生成AIに学習させない、生成AI上で扱わないようにしてください。【個人】

要機密情報や個人情報を取り扱う場合の対応事項は、ガイドライン本文や別紙3調達チェックシート、別紙4契約チェックシート、別紙2利活用ルールひな形に基づき作成された各府省庁における利活用ルール等に対応事項を記載しております。

要機密情報や個人情報の学習の要否はユースケースの特性を踏まえ検討しつつ、別紙4契約チェックシートにて、生成AIシステムに係るインプット及びインプットの処理結果に関する取決め事項を設け、学習の有無等の取決めも踏まえ、調達に係る契約を実施することとしています。

その上で、ガイドライン本紙においては、アクセス制御機能の適切な運用、必要なログの取得及び管理等を求めています。

別紙3調達チェックシートでは、「評価・選定時の分類」に当てはまる場合は、「生成AIシステムにおける個人情報の適切な取扱いと、プライバシーの保護が図られるよう対策していること」を踏まえて調達を実施するほか、説明可能性や検証可能性等の評価観点と要求事項も設け、総合的に対策することとしています。

別紙2利活用ルールひな形においては、生成AIシステムの利活用時の個人情報の取扱いに係る対策を整理し、利用者に対して要機密情報や個人情報の入力の可否を含む利用方法の遵守を求めています。

先進的AI利活用アドバイザリーボードの助言やAI相談窓口への相談等も活用しながら、適切な軽減措置を講じることにより、リスクを軽減しつつ、生成AIの利活用推進を可能とすることとしております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.3.1 生成AIシステムの企画時の対応事項

■原文：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。

■変更案：…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SaaS等のクラウドサービスが標準機能として提供可能な範囲、又は別途合意したデータ保管期間・コストの範囲内で検討することが求められる。

■意見理由：SaaSとして多数の行政機関にサービスを提供する際、すべてのプロンプト入出力やアクセスログを無期限あるいはシステム仕様外の形式で保存・管理することを要求されると、莫大なストレージコストが発生します。システムの標準仕様に基づく「合理的な範囲」での対応に限定できるよう、歯止めが必要です。【グラフナー】

「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」の記載と平仄を合わせ、ご意見の趣旨も踏まえ、「ログの取得及び管理を適切に行う必要がある」と修正いたします。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.3.2 生成AIシステムの調達時の対応事項

・P.41では、企画者がモデルやアーキテクチャ等の特性、主要な性能指標に加え、「合理的な範囲」で学習データ、学習方法、データセットに関する情報の取得に努める旨が記載されています。一方、学習データの詳細やセキュリティ関連情報は、提供者にとって競争上の機微情報に該当する場合も多く、必ずしも開示・取得が可能でないケースも想定されます。そのため、取得が困難な場合の考え方や整理について、一定の補足があると判断しやすくなると考えます。【日本電気】

・特に海外事業者が提供する基盤モデルを利用する場合、学習データ、データセット、学習方法等の情報の一部は営業秘密等の理由から開示されず、調達事業者を通じても取得できない可能性がある。「プライバシー及び営業秘密へ配慮しつつ、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、」と追記いただくことを検討いただきたい。

(参照)AI事業者ガイドライン・別添

開発者からステークホルダーに対する情報提供に関する記載(103頁)【AIガバナンス協会】

・■原文: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。

■変更案:…合理的な範囲で、基盤モデル提供者が一般公開しているホワイトペーパーやシステムカード等の範囲内で、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。

■意見理由:OpenAIやAnthropic等の外国製クラウドLLM(API)を利用するSaaS事業者にとって、基盤モデル自体の学習データや詳細なアルゴリズムはブラックボックスであり、それを政府に開示することは物理的に不可能です。情報提供の範囲を「API提供者が公開している範囲」に限定しないと、要件を満たせないリスクがあります。【グラフナー】

事業者にとって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の開示・取得が困難である可能性を踏まえ、「合理的な範囲で～取得に努める」という記載にしておりますが、リスク分析やリスク対応の検討のために取得の必要性がある場合が想定されることから、原案のとおりとさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.3.2 生成AIシステムの調達時の対応事項

生成 AI 事業者等のスタートアップ育成・公正競争加速に係る記載に関連して、生成AI利用環境「源内」に係る政府内での取組み、及び事業者との関わりについて言及いただくことを検討いただきたい。【AIガバナンス協会】

今回のガイドライン改定においては、全体の構造のスリム化の観点から、政府のAIの調達・利活用に必要な一般的事項に限って記載することとしております。

ガイドライン本紙

提出された主なコメント

6.3.2 生成AIシステムの調達時の対応事項

本改定案において、企画者が調達チェックシートを参照し、必要事項を調達仕様書に盛り込み、さらにリスク分析結果を踏まえて追加事項も検討することとした点は妥当です。

その上で、調達仕様書に盛り込むべき最低要件として、以下をより明確に例示することを提案します。

1. 入出力ログ及び主要な処理履歴の保存可能性
2. 事後監査に必要な情報の抽出可能性
3. インシデント発生時の封じ込め・停止対応手順
4. モデル変更、設定変更、外部接続変更時の記録保持
5. 高リスク案件における説明可能性・検証可能性の担保
6. 契約期間中の監査対応義務

生成AIは導入後に運用条件や接続先の変化によってリスクが増大し得るため、調達段階で監査可能性と停止可能性を契約要件として確保しておくことが重要です。価格や性能のみではなく、運用統制と事後検証に耐える設計を求めるべきと考えます。【個人】

ご意見に対する考え方

ご指摘の観点は、本文及び別紙3調達チェックシート、別紙4契約チェックシートに対応事項を記載しております。

本文において、6.2.2でシステム監査の対応、6.3.1で入力・出力・アクセス履歴等のログの取得及び管理、6.5で利用ログの確認や目的外利用・情報流出の検証、6.7でリスクケース発生時に必要な監査や対応について記載しております。

別紙3調達チェックシートでは、要求事項#29において「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」、要求事項#33において、「生成AIシステムの開発・提供のプロセスを検証可能としていること」を求めており、説明可能性及び検証可能性の確保に係る評価観点を盛り込んでいます。また、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、要求事項#27において「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」を求めています。

別紙4契約チェックシートでは、取決め事項#8において「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」、取決め事項#9において「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」を記載しており、生成AIシステムによるインシデントやリスクケース等を踏まえた契約を実施することとしています。

したがって、ログ保存、監査、封じ込め・停止対応、説明可能性・検証可能性といった観点は既にガイドラインで記載しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.3.2 生成AIシステムの調達時の対応事項

■原文：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…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」が活用可能である。

■意見理由：従来の重厚長大なシステム調達（入札・プロポーザル）を経ずに、デジタル庁の「デジタルマーケットプレイス（DMP）」を活用した迅速なSaaS導入が推奨されています。これにより、グラファー社のような事業者が自治体や省庁へプロダクトを導入する際のリードタイムと営業コストが劇的に下がるため、非常に強力な追い風となります。【グラファー】

賛成のご意見として承ります。

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

■原文：データ（学習データ、テストデータ）の検証およ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。

■変更案：…事業者が実施する場合もあり得る。（ただし、RAG等において行政機関等が自ら用意・入力した外部データの正確性や権利侵害の有無等に関する検証責任は、原則としてデータ提供元である企画者（行政側）が負うものとする。）

■意見理由：RAG（検索拡張生成）を用いたSaaSを提供する際、行政側がアップロードしたPDFやドキュメントに不正確な情報や著作権侵害が含まれていた場合、SaaS事業者側でその「データの中身」まで検証・改善することは不可能です。データ自体の品質・適法性の責任は行政側（企画者）にあることを明確に切り分けないと、事業者が不測の責任を負うリスクがあります。【グラファー】

ご指摘のような意味合いを持たせることを意図するものではないため、趣旨を明確化する観点から、「データ（学習データ、テストデータ）の検証及び改善対応については、契約の規定に応じて、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」と修正いたします。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.5 政府における生成AIシステムの提供者の対応事項

提供者の対応事項における期待品質及びアクセス制御について
生成AIモデルのメジャーアップデート等に際し、「期待品質」を満たしていることを確認する旨が示されていますが、その基準が必ずしも明確ではありません。提供者が自主的に設定する品質を指すのか、調達時に発注者が要求する品質を指すのかが読み取りにくく、要件次第では対応が難しい場合も考えられます。
また、アクセス制御についても、「アクセスを許可する主体」や「確実に制限される」状態の具体像が明確ではありません。調達要件として設定される場合には、実務を踏まえた内容が示されることが望ましいと考えます。【日本電気】

契約チェックシート取決め事項#5で示されているとおり、「期待品質」は一律の基準ではなく、生成AIシステムの目的・用途・コスト等を踏まえ個別案件ごとに調達仕様書・契約で具体化される前提としております。
また、アクセス制御は、「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、取り扱う情報の格付及び取扱制限等に従い設定することとしております。

6.5 政府における生成AIシステムの提供者の対応事項

システムの運用における「メジャーアップデート」や「追加的な学習を大規模に行った場合」の該当性について、具体的な事例や判断基準等を可能な範囲で示していただきたい。【AIガバナンス協会】

当該記載に対して具体例や判断基準を示した場合、限定的な記載に見えかねないため原案のとおりとさせていただきます。

6.5 政府における生成AIシステムの提供者の対応事項

提供者には利用者が構築したワークフローについてシステム上可能な範囲での利用状況・ログ等の情報を求めつつ、利用者の報告受け・管理については提供者を経由せず「企画者」や各府省庁内の「AI統括責任者(CAIO)」に一元化することで、効果的に適正利用の推進が可能と考えられます。
なお、プラットフォーム型の生成AIシステムを提供する事業者にとって、利用者が構築したワークフローが「出力結果の適切さの判断を全く行わない高度な自律型エージェント」に該当するかどうかを、適時かつ網羅的に検知することは技術的・実務的に困難な場合があります。【セールスフォース・ジャパン】

「提供者又はAI統括責任者(CAIO)」としており、必ずしも提供者を経由することとしていないため、原案のとおりとさせていただきます。
後段のご意見については、今後の運用・改定の検討にあたって参考とさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.5 政府における生成AIシステムの提供者の対応事項

■原文：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…等を確認した上で提供を開始する。

■変更案：…考慮しつつ、事業者の制御可能な範囲において（サードパーティ製基盤モデルを利用する場合は、当該プロバイダの仕様変更等の実態を踏まえつつ）、利用者への提供前に…等を可能な限り確認した上で提供を開始する。

■意見理由：クラウド型の外国製LLMを利用している場合、プロバイダ側の都合で予告なくモデルが更新されたり、旧モデルが強制的に廃止されたりすることがあります。「提供前の完全な確認」を事業者の絶対的な義務とされると、API提供者側の都合による変更で契約違反に問われるリスクがあり、物理的に対応困難です。【グラフナー】

ご指摘の課題があることを踏まえ、「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」と記載しており、また、重要な生成AIシステムに関しては事業者の制御可能な範囲も超えて対応を求めるケースもあり得るため、原案のとおりとさせていただきます。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

6.7 生成AIシステム特有のリスクケースへの対応

P45の6.7生成AIシステム特有のリスクケースへの対応の1段落目中の最後のポツにおいて「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、…」との記載があるが、音声入力が不正確なことを「基因」として意味内容を異にしたということを企図した記載であれば、『基に』とするのが適切ではないか。【個人】

ご意見のとおり修正いたします。

6.7 生成AIシステム特有のリスクケースへの対応

45ページ目の「6.7 生成 AI システム特有のリスクケースへの対応」において挙げられた例はいずれも生成AIが実用に足らないことを示していると思います。
生成AIはハルシネーションなど誤情報を含め不適切な出力をすることは仕様上避けられません。人間が最終チェックを行いこうしたリスクを防ぐ想定での推進の検討と推察しますが、実際問題こうしたチェックの労力は生成AIがもたらす効率を上回り労働意欲を削ぐという研究があります。また正確なチェックには高度な専門性や判断力が必要となるのに反して、生成AIによる省力化は逆にそうした優れた人材の育成の機会を奪います。今回の資料の膨大な修正削除は推進ありきでリスクを軽視しており、長期的に見て国全体の利益を大きく損ねることにつながると思います。

生成AIの利用の推進ではなく、まず人材育成と人材を大切にする環境を整えてください。
例に挙げられた失敗は、物事を最低限判断できるプロフェッショナルがいれば起きなかったことであり、生成AI導入による人材削減は生成AIのリスクを防ぐ人材の減少という悪循環を産みます。

どうか生成AIの推進について、真に活用したいならば長期的な目線を持って世界の動向を汲んだ慎重な計画を実行してください。【個人】

ご意見として承ります。
今回のガイドライン改定においては、全体の構造のスリム化の観点から、政府のAIの調達・利活用に必要な一般的事項に限って記載することとしております。

なお、本文では「AI事業者ガイドライン」にも言及する形で政府のAI調達・利活用において留意すべきリスクの例を引き続き記載しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

7 今後の進め方

「活用がより進んだ段階で反映を検討」とする方針は適切でない。設計調達段階での国際標準準拠が最もコスト効率よく安全を確保できる。既稼働システムへの遡及的対応は著しく困難であり、国際的にISO/IEC 42001準拠設計が標準化しつつある中での先送りは相互運用性において遅れをとるリスクがある。2027年度改定において高リスク用途への準拠要件化を明示するとともに、2026年度中に本ガイドラインとISO/IEC 42001の対応表を参考資料として公開を求める。【個人】

今後の運用・改定の検討にあたって参考とさせていただきます。

7 今後の進め方

・『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』

上記の文面を削除しているが、経産省としては、来歴証明を重要視しないということか？【個人】

・「来歴証明」の文言削除に関して。断固として「ふざけるな」と申し上げる。「来歴証明」こそがシステムの透明性を担保する唯一のものであることをまったくこれっぽっちも理解していない。あるいは「有耶無耶にしたい」思惑しか感じられない。【個人】

・（来歴証明に関する）点を消してガイドラインの改訂をしないでください。生成AIが結果を出力するために使われたデータがどこの何のデータに由来するのかを証明することは、生成AIを使う際に非常に重要なことです。国際的にも、データの透明性の確保が重要であるという意見が多数です。ブラックボックス状態から出力された生成AIのデータは信頼に値しません。来歴証明の導入は必要不可欠で、その在り方にも十分な検討が必要です。この点をガイドラインから削除しないでください。【個人】

ご指摘の来歴管理に関する観点は、別紙3調達チェックシートにおいて反映しております。具体的には、説明可能性確保のための対策例として、要求事項#29において「ファイルデータや外部連携コンポーネントからの応答等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」と記載しております。

また、要求事項#31においても、「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、ツール等により、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る」ことを、データ品質に係る対策例詳細として記載しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

附則

P48の附則について、『ただし、』と用いているが『なお、』とするのが適切ではないか。例えば、「新訂 ワークブック法制執務 第2版」の問74(P195)において「ただし書は、本文の文章に対する例外を規定するための立法技術として用いられるのが通例であり」と示されているところ、本附則のただし書は本文の「施行」の例外となる施行を規定しているものではなく、適用関係について規定しているため、ただし書を用いるのは不適切ではないか。(法令では、通常、施行日と異なる適用をする場合には、施行日の規定とは別途適用関係に関する経過措置を設けることとしており、施行日のただし書においては、本文の施行日と異なる施行日を定めている。)【個人】

ご意見のとおり修正いたします。

附則

P48の附則について、「2026年(令和8年)9月1日から」、「2026年(令和8年)6月まで」、「2026年(令和8年)7月1日から」とそれぞれ時期についての規定がされているが、「2026年(令和8年)6月まで」のみ日付まで特定していないのは並びが取れていないのではないか。【個人】

ご意見のとおり修正いたします。

附則

P48の附則について、初版では附則を設けていないところ、今般、附則を設けることとしたのは何を意図したものか。また、今回の改訂の仕方では初版の制定附則を改訂により追加するような形式となっているように読めるが、問題無いのか。【個人】

ガイドラインの適用開始時期等の附則事項をより分かりやすく示すため、今回の改定から附則を設けております。また、附則の「この決定」は、表紙にあるとおり、「令和8年〇月〇日(今回の改定日時) デジタル社会推進会議幹事会決定」を指しております。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

別紙2 生成AI利活用ルールひな形

・著作物の利用に自ら創作して手描きをしたラフ等を読み込ませることが対策例であることが説明されていますが、現状の生成AIは著作者の許諾無く読み込ませて他者の知財を利用し変換している時点で全く適切ではありません。国民の声を反映しているとは考えられません。【個人】

・既存の著作権物を侵害するものか否かを確認することとあるが、そもそも現状大手中小問わずごく一部を除くほぼ全ての生成AIサービスはベースの学習に用いた著作物データ群を非公開としており、頑なに公開したがない姿勢を鑑みるにおよそ権利的に問題のある未許諾のデータを取り込んでいると見て相違ないだろう。(中略)真にAIの利活用を勧めたいのであれば問題を抱えた生成AIは一時的に一律利用不可とし、潜在的リスクを排除した自国の物のみで運用していくべきだ。【個人】

・“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”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くても、「城の前で愛を誓う男女」としても、ディズニー風のイラストが出力された例がある。これは、特定の登録意匠や登録商標でも同じである。生成AIは学習量とタグに基づいて出力されてくるからである。【個人】

・どのような生成の仕方であれ、生成物には必ず「生成AIによる出力物」ということを明示しなさい(出所明示義務)。著作物だと認められる認められないに関わらず、分からないのであれば著作権法に則り、そうすべきだ。【個人】

知的財産権等の侵害等の対策については、ガイドライン全体で対応事項を記載としておりますが、別紙2利活用ルールひな形においては、プロンプト入力段階・AI生成物の利用段階の双方で対応することとしています。

AI生成物の利用段階の対策では、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としています。

生成AIによる出力物であることの明示については、別紙3調達チェックシートの要求事項#18で「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」を設けており、生成AIシステムからの出力であることを表示することを必要に応じて検討する仕組みとしています。

ガイドライン本紙

提出された主なコメント

ご意見に対する考え方

別紙2 生成AI利活用ルールひな形

- ・調達時や契約時のチェックシートが整備されているのと同様に、政府職員等が利活用の場面で確認すべき事項をまとめたチェックシートを整備し、情報漏洩、偽・誤情報の出力、知的財産権の侵害といったリスクの種類に応じて各段階で確認すべき点等を示すべき。【楽天グループ】
- ・AI開発又は事業者には他人の著作権と同一・類似の表現や他人の特定の著作物と関連づけられるように、その他人の名称と紐づけている隠語を生成AIシステムに組み込んでいると思われるケースが確認されています。その事を鑑みても、特定の登録意匠や登録商標、特定の人物についても隠語として今後紐づけられる可能性が考えられるために前述に述べたケースも併せ、活用ルールに隠語を含むプロンプトを入力しないといった記載が必要であると思われます。【個人】

今後の運用・改定の検討にあたって参考とさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 全般

調達チェックシートに示されている「偽・誤情報の出力防止措置」「エンドユーザーの意思決定の不当な誘導の防止」「公平性及び包摂性（バイアス検証情報の提供）」は重要な観点である一方、運用的な制約を踏まえると、完全性の担保が難しい場合も想定されます。リスクに応じた考え方で整理されることが望ましいと考えます。【日本電気】

調達チェックシートの要求事項は「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」としており、個別具体の案件に応じた整理が行われる前提としております。

別紙3 調達チェックシート 全般

Human-in-the-Loopの設計要件の明示を求む。
「人間が確認する手順がある」とことと「人間が判断している」ことは同義ではない。調達チェックシートにおいて、1処理の判断類型（人間が最終判断・人間確認後AIが実行・AIが自律実行）の明示、2AIの出力根拠・不確実性・代替案を人間が理解できる形式で提示する要件、3担当者が当該業務の判断能力を維持するための定期的措置の調達計画への組み込み、4AIによる判断・介入ログの保存と改善への活用を調達要件に含めることを求める。2026年公表のScience誌掲載研究（Cheng et al., eaec8352）は、AIへの過度な依存が人間の判断感受性を低下させることを実証しており、行政組織において組織的な判断能力低下につながりうる。【個人】

ご指摘の観点については、高リスク判定シートで政府職員等による出力結果の判断有無を行わない場合には高リスクの判定となる判定フローを設けており、リスク軽減措置を具体化する必要があることを明らかにしております。また、本ガイドラインにおいては、利用者による確認、ログ取得・管理、研修等を求めており、ガイドライン全般にて対応しております。

別紙3 調達チェックシート 全般

庁内で既に利用されている製品やサービスにおいて、本チェックシートのテスト運用を実施し、実現可能性や運用可能性を確認したうえで、本運用に移行いただきたいです。【グラファー】

今回改定を行うガイドライン2.0版は、令和8年9月1日からの全面適用を予定しており、以降生成AIシステムの調達等において適用することとしております。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 生成AIシステムの基本機能要件全般

出典明記・知的財産保護の義務強化(6.5、別紙3 #24・#29): 要求事項#24 (IP保護)と#29(説明可能性)は相補的であり、出典の自動付与はその両方を同時に充足します。高リスクシステムについては、調達チェックシートにプロバナンス機構の実装を明示的に要件化し、アドバイザリーボード報告(4.2.2)に反映することを提案します。【Cell Dynamics合同会社】

知的財産権等の侵害等の対策、説明可能性の確保に関しては、方法として共通する対策も想定されるところですが、リスク対策の内容やレベル等は各ユースケースを踏まえて検討する必要があるため、評価観点をそれぞれ設け、各ユースケース毎に判断する形としております。

別紙3 調達チェックシート 生成AIシステムの基本機能要件全般

調達チェックシートの技術的整合性の確保

調達チェックシートの要求事項16・20・22において、「有害情報・バイアス・目的外利用に関する入出力制限」が基本要件として記載されておりますが、「入力の制限」という表現は技術的に正確ではないと考えます。生成AIシステムは入力データの内容が有害か否かをAI処理前に自動判定・遮断することは一般に困難であり、入力制限を基本要件として課すことは実装上の混乱を招くおそれがございます。

要求事項の趣旨が「有害な出力を防ぐこと」にあるならば、「生成AIシステムによる有害情報の処理および出力制限」と表現を改めることが適切と考えます。また要求事項20の「不当な差別の入出力」という表現は日本語として不自然であり、「不当な差別を含む情報の処理および出力制限」への修正を求めます。

加えて、P26注釈27において、サードパーティのAIモデルを利用しつつ自社セキュリティ基盤でサービスを提供する形態を「PaaSに相当」と限定しておりますが、同様の構成はSaaSにおいても存在いたします。「PaaSおよび一部のSaaS」と修正することで、実態に即した記述となると考えます。【Box Japan】

結果として生成AIシステムの出力において有害情報やバイアス等が制限されていればよいという考え方を踏まえて、要求事項#16及び#20を以下のとおり修正いたします。

- ・要求事項#16:「テロや犯罪に関する情報や攻撃的な表現等、有害情報の出力制限等をしていること」
- ・要求事項#20:「有害なバイアスや、不当な差別の出力制限等をしていること」

なお、要求事項#22につきましては、目的外の入力の制限も要求事項の範囲内に含まれることから、原案のとおりとさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 生成AIシステムの基本機能要件全般

■項目名:

13 偽誤情報の出力・誘導の防止

14 公平性と包摂性

15 目的外利用への対処

■意見理由:事業者が個別に開発をして納品を行うものについては開示可能な場合がございますが、広く利用されるクラウドサービス型では実装している機能に対して事業者内部の情報となるものは開示することは難しいと思います。事業者側で開示できる情報がない場合の説明可能な余地を残していただきたいです。【グラフアー】

各対策例の「裏付けとなる情報の例」は、要求事項を満たしているか否かを判断するための情報の一例を示したものであり、必ずしも開示・提出を求める記載ではありません。そのため、原案のとおりとさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#7

■原文:ベンチマーク※等を使用した評価基準とその評価内容がわかる資料等
■変更案:合理的な範囲で、ベンチマーク…
■意見理由:事業者が個別に開発をして納品を行うものについては開示可能な場合がございしますが、広く利用されるクラウドサービス型では実装している機能に対する品質の測定や評価方法は事業者内部の情報となるため開示することは難しいと思います。事業者側で開示できる情報がない場合の説明可能な余地を残していただきたいです。【グラファー】

当該記載は、裏付けとなる情報の例を示したものであり、必ずしも提出を求める記載ではありません。そのため、原案のとおりとさせていただきます。

別紙3 調達チェックシート 要求事項#7

■原文: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
■変更案:…場合、合理的な範囲でテストケース例と…
■意見理由:事業者が個別に開発をして納品を行うものについては開示可能な場合がございしますが、広く利用されるクラウドサービス型では実装している機能に対するテストやテスト方針は事業者内部の情報となるため開示することは難しいと思います。事業者側で開示できる情報がない場合の説明可能な余地を残していただきたいです。【グラファー】

当該記載は、裏付けとなる情報の例を示したものであり、必ずしも提出を求める記載ではありません。そのため、原案のとおりとさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#11

対象文章：特定のモデルの利用が主たる目的ではない場合、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、複数の生成AIモデルを利用する

提言：複数の生成AIモデルの利用導入は、安定性・公平性の確保と適切なコストのバランスに考慮した最適なモデルごとにライセンス費用や運用保守費用が発生し、システム全体のコスト増加や開発期間の長期化につながる可能性があります。特に、不特定多数の利用者が利用するシステムにおいて、この条件を必須とすることは、費用対効果の観点から現実的ではないケースも想定されます。

複数の生成AIモデルを利用する想定される具体的なユースケース（例：異なるモデルで生成された結果を比較検証する、特定のタスクには専門性の高いモデルを使い分ける、特定のモデルの出力にバイアスが見られた場合に別のモデルで補完するなど）を明確に示していただくとともに、以下のような修正を提案します。

一律の必須化の見直し：「原則として複数の生成AIモデルの利用を推奨する」といった表現に留め、必須とせず、各府省庁がリスクとコストを考慮して判断できる余地を残す。

加点項目としての位置づけ：複数の生成AIモデルを利用する技術を有することを評価する際、コスト増や複雑性に見合う便益が期待できる場合に加点対象とするなど、柔軟なインセンティブ設計を行う。

利用想定 の明確化：複数の生成AIモデルを利用する際の具体的な活用シナリオ（例えば、モデルAで一次生成を行い、モデルBで内容の検証や別の観点からの追加情報を得るなど）をガイドライン内で示していただくことで、各府省庁が導入を検討する上での参考となると考えます。これにより、過度なコスト負担を避けつつ、リスクと便益のバランスを考慮した最適なAIシステム調達を促すことができると考えます。【富士通】

調達チェックシートの「対策例」及び「対策例詳細」は、要求事項を遵守するための対策の例示であり、この対策例を採用することを必須とするものではありません。

当該記載は、要求事項そのものではなく対策例として示しているものであり、一律に複数モデル利用を求める趣旨ではありません。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#12

ベンダーロックイン回避のためのレイヤーの推奨(別紙3 #12): 行政ポリシーロジックを特定AIモデルから分離するレイヤーの導入を、要求事項#12の具体的実装指針として推奨すべきです。これによりモデル更新・ベンダー変更時にも政府のデータ主権とポリシーの継続性を確保した円滑な移行が可能となります。【Cell Dynamics 合同会社】

今後の運用・改定の検討にあたって参考とさせていただきます。

なお、レイヤー(アダプタ)の用意については、要求事項#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」の対策例の1つとして例示しております。

別紙3 調達チェックシート 要求事項#12

改定案に賛成します。その上で、国民向け又は高い信頼性が求められる生成AIシステムでは、要求事項をより実装可能な形で明確化していただきたいです。

第一に、ベンダーロックイン回避については、理念だけでなく、モデル切替、履歴・テンプレート・評価ログのエクスポート、標準的なAPI・データ形式での移行可能性を確認事項として明示していただきたいです。【個人】

ベンダーロックイン回避については、別紙3調達チェックシートの評価観点#8において、モデル切り替え、履歴・テンプレートのエクスポート、標準的なインタフェースを通じた移行容易性に関する内容を、対策例・対策例詳細を新たに追加しております。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#12

アーキテクチャの柔軟性(要求事項12)が基本項目に設定されています。特定のLLMモデルへの依存(ロックイン)を避けることは重要ですが、AIモデルの置き換えを全てにおいて必須要件とした場合、LLMの特性に連動して設計されたセキュリティガードレールや信頼性の機能が提供困難になる／低下する可能性もあります。各省庁がニーズ・用途に応じて柔軟に調達要件を設計できるよう、本項目は任意追加項目(加点項目)とされることを提言します。【セールスフォース・ジャパン】

要求事項#12はモデルの置き換え自体を義務付けるものではなく、移行容易性も踏まえた設計・運用を求める趣旨であるため、原案のとおりとさせていただきます。

別紙3 調達チェックシート 要求事項#12

単純なテキスト生成を行う大規模言語モデル(LLM)のAPI利用であればモデルの切り替えは比較的容易ですが、高度なタスクを実行するAIエージェントは、特定のオーケストレータやツール連携機構(RAG機能、外部API連携機能等)と特定のLLMの特性が密結合して最適化されているケースが一般的です。仮にこの要件がAIエージェントにも一律に求められた場合にはシステム全体のパフォーマンス低下や高度な自律実行機能の喪失を招く恐れもあります。各省庁がAIエージェントシステムを導入する際、または今後ガイドラインにおいてAIエージェントをカバーする場合は、エージェント型システムについてはモデル単体ではなく「システム全体としての機能要件」を重視しつつ、アーキテクチャの性質に応じて「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」など弾力的な運用を実施できることを期待します。【セールスフォース・ジャパン】

AIエージェントに係る今後の運用・改定の検討にあたって参考とさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#12

提言:レイヤー(アダプタ)は、ベンダーロックイン回避やシステム移行の容易性を高める上で重要な要素であります。しかしながら、これらの導入はシステム構築における初期コストや開発期間の増加を伴う場合があります、すべてのAIシステム調達において一律に基本項目とすることは、プロジェクトの規模や特性によっては過剰な要件となり効率的なシステム構築を阻害する懸念があります。

例えば、以下のようなケースでは、柔軟な対応が望ましいと考えます。

- ・小規模なPoCや限定的な利用: 費用対効果の観点から、将来的な拡張性よりも早期の導入やコスト抑制が優先される場合があります。
 - ・特定のベンダー製品に特化したシステム: レイヤーの導入が困難な場合や、その効果が薄い場合があります。
- 従って、レイヤー(アダプタ)の導入については、その必要性和導入におけるトレードオフを考慮し、リスクレベルやプロジェクトの特性に応じた評価を可能とするため、「基本項目」ではなく「加点項目」として評価することをご検討いただきたく存じます。これにより、各府省庁が実情に合わせた最適なAIシステムを選択できるようになり、より効率的かつ柔軟なAI利活用を促進できると考えます。【富士通】

調達チェックシートの「対策例」及び「対策例詳細」は、要求事項を遵守するための対策の例示であり、この対策例を採用することを必須とするものではありません。

当該記載は、要求事項そのものではなく、ベンダーロックイン回避のための対策例として示しているものであり、一律にレイヤー(アダプタ)の用意を求める趣旨ではありません。

別紙3 調達チェックシート 要求事項#13

また、要求事項13(生成AIモデルのメジャーアップデート前の検証)についても、同様の理由により、外部モデルを利用する事業者にとっては対応が困難な場合があると考えられることから、システム側での検証・評価プロセスの整備をもって代替的に充足できる旨を明確化することが望ましい。【Preferred Networks】

ご意見を踏まえ、当該対策例を「生成AIモデルのメジャーアップデートやモデルの移行時に、生成AIシステムの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する」と修正いたします。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#20

対象文章: 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

提言: AIモデルにおける不公正なバイアスの検証や法令等に基づく出力制限への対応は、AIシステムの公平性・適切性を確保する上で極めて重要であると認識しております。ファインチューニングを行わない既成のAIモデル（特にデジタル庁が認定または推奨する国内LLMや広く利用されている著名なLLM）を利用する場合、これらの対応はAI事業者ガイドラインにおけるAI開発者が留意すべき事項と考えます。

したがって、これらの既成AIモデルをファインチューニングせずに利用するケースにおいては、個別の調達ごとに毎回、バイアスの検証や出力制限の確認を求めることは、調達・提供双方にとって過度な負担となり、効率性を損なう可能性があります。つきましては、以下のようなご提案をいたします。

・デジタル庁認定/推奨モデルの優遇: デジタル庁が事前にその公平性や出力制限に関する事項を一定レベルで確認・認定したAIモデルについては、個別の調達における詳細な調査・確認を一部免除または簡略化する方策を検討。

・情報提供の活用: AI事業者が提供するAIモデルの説明書やサービス規約等に、バイアス検証や出力制限に関する情報が記載されている場合、それを活用することで個別の確認作業を効率化できることを明記する。これにより、各府省庁は安心安全な既成AIモデルを利活用できるようになり、調達プロセス全体の効率化に寄与すると考えます。【富士通】

当該対策例に係る要求事項は、不特定外部者（一般国民等）による府省庁外利用の場合に基本項目として適用するものであり、事前学習モデルをそのまま利用するケースであっても、生成AIシステムの利用範囲に応じた確認を行うことは重要であるため、原案のとおりとさせていただきます。

また、「AI事業者が提供するAIモデルの説明書やサービス規約等に、バイアス検証や出力制限に関する情報が記載されている場合、それを活用することで個別の確認作業を効率化できることを明記する」とご意見をいただいている部分については、裏付けとなる情報の例として、「生成AIシステムの検証プロセス・検証方法が分かる資料」と記載しており、ご記載いただいた情報提供の方法は、これに該当する想定です。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#20

対象文章: 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

提言: 特定の職業やカテゴリに関する人物画像を生成する際に、性別、年齢、人種などの属性におけるバイアスを軽減し、多様な出力を実現する仕組みは重要です。しかしながら、現在多くの生成AIモデルがそのための技術開発を進めておりますが、現実のデータに基づいて学習を行うという性質上、完全に偏りのない(バイアス・フリーな)出力を保証することは技術的に極めて困難であると認識しております。したがって、ガイドラインにおいて「偏りのない出力を生成できる仕組みを具備する」ことを求める際には、以下の点を明確にすることを提言します。

・「軽減」への表現の変更: 「完全に偏りのない出力を保証する」から、「過度な偏りを軽減した出力を目指すこと」へ、技術的な現実解を踏まえた表現への修正を提言します。【富士通】

調達チェックシートの「対策例」及び「対策例詳細」は、要求事項を遵守するための対策の例示であり、この対策例を採用することを必須とするものではありません。

当該記載は、要求事項そのものではなく対策例として示しているものであり、完全にバイアス・フリーな出力保証を求める趣旨ではありません。また、「完全に偏りのない出力を保証する」という表現は用いておらず、「偏りのない出力を生成できる仕組みを具備する」という表現を用いております。

別紙3 調達チェックシート 要求事項#23

個人情報・知的財産等については、利用者入力が当該利用者への回答生成に限定されることを既定とし、二次利用や学習利用は原則として明示同意を前提にしたいです。【個人】

今後の運用・改定の検討にあたって参考とさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#24

■原文:

- ・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。
- ・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。

■変更案: 生成AIシステムの学習段階・生成段階において、知的財産権、肖像権、パブリシティ権等の保護が図られるよう事業者の制御可能な範囲において合理的な対策(例: 基盤モデルの利用規約の確認、オプトアウトへの対応、システムプロンプトによる出力制御等)を講じていること

■意見理由: 生成AIの技術的特性上、事前学習データの完全な権利非侵害や、生成物が既存著作物と一切類似しないことをシステム提供者が100%保証することは不可能です。過度なコンプライアンスを避けるため「事業者が制御可能な合理的な範囲」に限定する記載が不可欠です。【グラファー】

当該要求事項は「図られるよう対策を講じていること」を求めるものであり、「システム提供者が100%保証すること」を求めるものではありません。

また、当該要求事項は、政府による調達・開発の過程で事後学習を行う場合の学習段階と生成段階、それぞれの段階での知的財産権等の侵害等対策の要求事項を設けるものであり、要求事項を合わせて1つとすることは構造上困難となります。

以上より、原案のとおりとさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#24

・調達チェックシート要求事項24について、「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」の対策例として、「モデルにおいて知的財産権等の侵害防止のための仕組みを具備する」とされている。しかしながら、生成AIシステム提供者のうち、外部の生成AIモデル(API等)を利用する事業者にとっては、当該モデル自体の仕様はコントロールの範囲外であるため、当該対策例のみをもって要件充足の可否を判断することは適切でない場合がある。このため、生成AIシステム側において同等の保護措置(出力フィルタリング、利用規約上の制限、侵害発生時の対応手順の整備等)が講じられている場合も対策例として明示することが望ましい。【Preferred Networks】

・本要求事項は、生成段階における知的財産権・肖像権・パブリシティ権の保護を求めるものです。しかし対策例は「知的財産権等の侵害等防止のための仕組みを具備する」ととどまっています。

何をもって仕組みが機能していると判断するか、基準が示されていません。ベンダーが自己申告により要件を満たしたとする場合、行政側には客観的に検証する手段がありません。著作物を制作するクリエイターの立場から見ると、保護の実態が不透明なままです。

裏付けとなる情報の例として、類似性判定ツールによるテスト結果や第三者評価の概要の提出を求めることを追加すべきではないでしょうか。【個人】

ご意見を踏まえ、当該対策例を「生成AIシステム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」と修正いたします。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#25

生成AIシステムの開発者・提供者とデータ提供者間で契約締結され、守秘義務により政府職員による契約の直接確認が困難なケースも想定されるため、「契約・利用規約を確認し、又は調達事業者において確認させ、データの利用制限の有無や内容をチェックする」とし、政府職員に代えて調達事業者が確認することを許容するよう追記いただくことを検討いただきたい。【AIガバナンス協会】

契約・利用規約の確認主体は個別案件の契約関係や実務に応じて整理されるものであり、原案でも調達事業者を通じた対応を排除していないため、原案のとおりとさせていただきます。

別紙3 調達チェックシート 要求事項#25

調達チェックシートの要求事項#25の例で「※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」とする文言があるが、これは不適切である。
知的財産権等の侵害等防止を目的として適切なデータの学習を行う対策を講じることを要求するのであれば、生成AIシステムのベースを作る際にこれまで事業者が用いた学習データについても知的財産権等の侵害等防止のための対策（例えば、使用してはいけないデータを学習に用いていないか）が取られていることを証明してもらう必要があるからである。【個人】

ご指摘の箇所は、あくまで要求事項を遵守するための対策例に関する注記です。他方、事業者が用いた学習データ等の情報については、本紙「6.3.2 生成AIシステムの調達時の対応事項」にて、「企画者は、（中略）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」としております。なお、ご指摘箇所の記載は、別紙3調達チェックシートの構造を踏まえ、「評価・選定時の項目の分類」の記載で充足することから、削除いたしました。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#25

・「対策例詳細」では、「AI学習データの収集を制限する技術的措置」の例示に限らず、権利者による「AI学習禁止」「無断利用禁止」「転載禁止」等の意思表示や利用条件を遵守することを明記すべきです。

このことは、著作権法第30条の4における「著作権者の利益を不当に害することとなる場合」の規定や、文化庁の「未管理著作物裁定制度」とも関連し、「著作物等の利用における、権利者による意思表示や利用条件の遵守の原則」を遵守することを意味しており、重要です。【個人】

・本要求事項は、生成AIの学習段階における知的財産権保護を求めるものです。しかし適用対象が「企画・開発において生成AIに学習を行わせる場合」に限定されています。

政府調達の多くは、既存の基盤モデルをそのまま利用する形態です。この場合、ベンダーが使用した学習データの権利処理状況は問われません。クリエイターの著作物が無断で学習されたモデルであっても、調達要件を満たすことになります。

知財保護の実効性を確保するため、既存モデルを調達する場合にも、学習データの権利処理状況の概要説明をベンダーに求めることを基本項目として追加すべきではないでしょうか。【個人】

・是非対策の適用範囲を拡大してもらいたい。(中略)学習データの正当性が不明のままでは、国が採用するのは一納税者として到底納得できません。歴任のデジタル大臣に税金を返して欲しいくらいです。

生成AIに費やす予算があれば、まずは学習データを築き上げたクリエイターの支援や、「著作物が学習されない自由」と「学習元への還元体制」の確立を国として乗り出す方が急務ではないだろうか。【個人】

ご指摘の点については、要求事項#24において、「生成段階における知的財産権、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」を、生成AIシステムで知的財産権等を取り扱う場合の基本項目として設けています。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#26

・■項目名: 17.セキュリティ確保: 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

■原文: 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。

■変更案: …生成AIモデルを事後学習させる。又は、サードパーティ製基盤モデルを利用する場合等において、システムプロンプトによる指示の厳格化や、外部の入力フィルタリング機構等の代替手段により同等のセキュリティ水準を確保する。

■意見理由: クラウドAPIを利用してSaaSを提供する事業者にとって、基盤モデル自体に「事後学習(ファインチューニング等)」を施すことは仕様上不可能、もしくは莫大なコストがかかります。これを要件の対策例としてそのまま求められると要件を満たせないケースもありうるため、API利用者として実施可能な代替手段(プロンプト制御やガードレール等)を許容する記述が必要です。【グラファー】

調達チェックシートの「対策例」及び「対策例詳細」は、要求事項を遵守するための対策の例示であり、この対策例を採用することを必須とするものではありません。このため、原案のとおりとさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#26

・■項目名: 17. セキュリティ確保: 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

■原文: 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。

■変更案: …など、外部データを参照する場合には、事業者の技術的・経済的に合理的な範囲において、これらに意図しない出力…

■意見理由: RAG(検索拡張生成)などで外部Webサイト等を動的に参照する際、取得したすべてのテキストに対して間接プロンプトインジェクションの完全な検証をリアルタイムで行うことは、システムのレスポンスタイムの著しい悪化と処理コスト(LLMによる二重チェックなど)の増大を招きます。SaaSとしてのUXとビジネスモデルを損なうため、「合理的な範囲」という制約が必要です。【グラファー】

調達チェックシートの「対策例」及び「対策例詳細」は、要求事項を遵守するための対策の例示であり、この対策例を採用することを必須とするものではありません。このため、原案のとおりとさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

別紙3 調達チェックシート 要求事項#26
セキュリティ確保については、プロンプトインジェクション、RAG、外部Web/DB参照、オーケストレータ権限を明示的な対象に含め、入力プロンプト・システムプロンプト・外部参照データの分離、悪性指示の検知時の処理拒否、最小権限、出力検証を必須に近い形で整理していただきたいです。【個人】

ご意見に対する考え方

ご指摘の点は、別紙3調達チェックシートの要求事項#26において、基本項目（原則必須とする項目）の対策例詳細として以下のとおり整理しています。

プロンプト入力に関するセキュリティ確保については、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に、「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」こととしています。

生成AIモデルが外部データを参照する場合のセキュリティ確保については、「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」ことや、「Webサイトや外部のデータベース等、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」こととしており、RAGや外部のデータ参照時の参照権限の管理や、意図しない出力を行わせる指示の拒否に関する観点を盛り込んでいます。

オーケストレータの権限管理等については、「権限等に不備がないことの対策を講じる」ことや、「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」こととしています。

出力の検証については、「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」こととしています。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#27

・■原文:

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。
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。

■変更案:(追記)ただし、サードパーティ製モデル等で自社での直接制御が困難な場合は、当該APIの利用停止、別プロバイダへの切り替え、又はシステムプロンプトの修正等の運用対処による迅速な封じ込めをもってこれに代えることができる。

■意見理由:万が一プロバイダ側でモデル改ざんや学習データの汚染が起きた場合、SaaS事業者側で「悪意あるデータの局所的な除去」や「即時の代替モデルへの切り替え」を内部的に行うことは物理的に不可能です。API利用の実態に即し、サービスの一時停止や代替APIへの切り替えといった運用ベースの封じ込め策を正当な対策として明記すべきです。【グラファー】

・他社製の基盤モデルを利用して開発・提供される生成AIシステムに関しては、学習データやアルゴリズムの詳細は提供事業者の開示されないことが一般的であるため、「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」や「混入された悪意のある学習データの局所的な除去」は技術的・構造的に不可能。よって、提供事業者の立場で合理的に実施可能な代替措置等を講じることができれば対策例を満たす旨を明記すべき。【楽天グループ】

要求事項#27は、生成AIシステムに対して高い信頼性が求められる場合に基本項目として適用される要求事項であることから、原案のとおりとさせていただきます。

別紙3 調達チェックシート

提出された主なコメント

別紙3 調達チェックシート 要求事項#27

インシデント対応については、迅速な封じ込めと復旧能力を実効化するため、検知、封じ込め、切戻し、復旧、利用者周知の手順と目標時間を要求事項又は必須付属資料として明記していただきたいです。

以上により、説明可能性、移行可能性、安全性が高まり、行政における生成AIの信頼できる調達・利活用に資すると考えます。【個人】

ご意見に対する考え方

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は、あらかじめ事業者と合意しておく事項として、別紙4契約チェックシートの取決め事項#8の補足説明にて以下のとおり記載しております。

「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。」

別紙3 調達チェックシート

提出された主なコメント

別紙3 調達チェックシート 要求事項#29

高リスク業務における説明可能性指標の実装強化(6.3.1、6.7、別紙3 #29): 要求事項#29は適切に規定されていますが、リスク軸A-1に該当するシステムについては、ログ取得に留まらず、AIが出力を導いた統計的・論理的根拠を示す具体的指標の提出を調達要件とし、先進的AI利活用アドバイザリーボードへの報告(4.2.2)への明示的な反映を求めます。【Cell Dynamics 合同会社】

ご意見に対する考え方

本ガイドラインにおいては、「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)を踏まえ「2.1 本ガイドラインの目的」にて国が特に取り組むべき事項として「④行政としてのアカウンタビリティを果たすこと」等をガイドラインの冒頭で記載しております。政府における生成AIの調達・利活用においては、これらの指針に則り各案件が進められることとなります。

具体的には、別紙1の高リスク判定シートを参考にCAIOが高リスクと判断した案件やその可能性が高い生成AIシステムは、アドバイザリーボードへの報告や、必要に応じてアドバイザリーボードでのリスク緩和のための助言等の対象となるものです。また、別紙2利活用ルールAI生成物利活用におけるルールにて、生成AIの出力結果に基づいて行う判断も政府職員の説明責任の対象に含まれることを留意することとしており、生成AIの出力結果をそのまま使うのではなく、職員の判断を踏まえて使うこととしています。

本ガイドラインに基づく以上のような取組みにより、生成AIの利活用において、可能な限り判断の根拠等が不明瞭にならないよう国民へのアカウンタビリティを果たせるよう、取り組んでまいります。

別紙3 調達チェックシート

提出された主なコメント

ご意見に対する考え方

別紙3 調達チェックシート 要求事項#29

「出力結果が技術的に合理的な範囲で確認できる状態にする」ことが基本項目とされているが、RAGにおける引用元提示等の手法を除き、生成AIが出力生成に利用した情報の詳細を特定・提示することは、現時点では一般的な実装としては限定的である。したがって、要求水準や具体例については、現実的な技術水準を踏まえた整理が必要と考える。【Preferred Networks】

「合理的な範囲で確認できる状態と対策していること」としており、情報の詳細な特定・提示を必ずしも求めるものではないため、原案のとおりとさせていただきます。

別紙3 調達チェックシート 要求事項#30

■項目名: 19. ロバスト性

■原文: 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

■変更案: 生成AIシステムが入力に対して完全に同一出力を保証はせず、不適切な回答を低減する程度での安定した出力を行う状態とよう制御等をしていること

■意見理由: LLM(生成AI)の技術的特性上、入力に対して「常に同じ安定した結果」を返すこと(決定論的な挙動)は原理的に不可能です。これを「基本項目」として厳格に求められると、わずかな出力の揺らぎが「要件違反(債務不履行)」として扱われるリスクがあり、AIの不確実性を事業者が全て被る形になってしまうため、前提条件(免責事項)の明記が必須です。【グラファー】

当該要求事項は、完全に同一出力を保証することを求める記載ではありません。このため、原案のとおりとさせていただきます。

別紙4 契約チェックシート

提出された主なコメント

ご意見に対する考え方

別紙4 契約チェックシート 取決め事項#1

契約チェックシート取決め事項1における「オプトアウトにより学習利用の制御を可能とする」との記載について、政府利用の生成AIシステムにおいてオプトアウト方式を許容する場合、利用者が能動的に拒否の意思表示をしない限り学習利用が行われる可能性があり、個人情報保護法上の利用目的の範囲外での利用や、行政事務に係る機密情報・機微情報の意図しない学習利用につながるリスクが生じ得る。政府調達においては、情報管理上の要請から、原則としてオプトイン方式（明示的な同意がない限り学習利用を行わない）を採用し、オプトアウト方式は許容しないことが望ましいと考える。【Preferred Networks】

ご意見を踏まえて、「※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」を削除いたします。

別紙4 契約チェックシート 取決め事項#1

■原文：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。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。
■意見理由：行政機関のデータを扱う際、「学習への利用禁止（目的外利用の禁止）」が求められますが、OpenAI等の外部APIの「オプトアウト機能」を用いることでこの要件を満たせることがガイドライン上でも明確化されました。これにより、「完全閉域網やローカルLLMでなければならない」という極端な要求を退け、APIを活用したSaaSモデルの正当性が担保されます。【グラファー】

ご指摘の箇所は、オプトアウト方式を前提に一定の提供形態を許容する趣旨に読まれ得ること、また、学習利用の可否や目的外利用の禁止は個別案件の要件等を踏まえて契約で整理すべき事項であることから、削除いたしました。

別紙4 契約チェックシート

提出された主なコメント

ご意見に対する考え方

別紙4 契約チェックシート 取決め事項#2

■原文: ※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。

■意見理由: 独自に開発・チューニングした高度なパーサーやテキスト分割・ベクトル化のプログラムは、当社にとっては技術資産になりうるものです。これらを「納品」するのではなく、「WebAPI等を通じた機能提供 (SaaS形態)」として契約できること、及び権利帰属を事業者に残せる余地が明記された点は、自社の知的財産を保護する上で極めて肯定的に捉えています。【グラファー】

賛成のご意見として承ります。

別紙4 契約チェックシート 取決め事項#5

■意見の方針: 賛成

■原文: 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、「〇〇以上の精度」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。

■意見理由: LLMの確率的性質上、「100%の精度保証」を行うことは技術的に困難です。準委任等の柔軟な契約形態が推奨されることで、事業者が過度な瑕疵担保責任 (契約不適合責任) を負うリスクが適正化され、積極的な提案を行いやすくなります。【グラファー】

別紙4 契約チェックシート

提出された主なコメント

ご意見に対する考え方

別紙4 契約チェックシート 取決め事項#5

■意見の方針: 賛成

■原文: 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…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

■意見理由: プロンプトエンジニアリングや精度チューニングは、LLMの性質上「必ず100%意図通りに動く」という確約が困難です。この部分を「性能要件を含めない」形式や「取組の履行有無(準委任型)」として契約できることがガイドラインで明記されたことは、不確実なAIの挙動に対する過度な責任を回避でき、事業者として肯定的に捉えています。【グラファー】

賛成のご意見として承ります。

別紙4 契約チェックシート

提出された主なコメント

ご意見に対する考え方

別紙4 契約チェックシート 取決め事項#6

契約チェックシート取決め事項6の「生成AIシステムに係るノウハウの取決め」について、「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」とあるが、そもそも事業者によるノウハウの利用制限の必要性和範囲については、現時点では整理が十分とは言えないように思われる。政府活用を通じて蓄積されたノウハウは、行政サービスの向上や生成AIサービス全般の技術発展に資するものであり、適切な範囲において積極的に活用されるべきと考える。

なお、個人情報・機密情報等の機微な内容を含む場合は別途適用法令や秘密保持義務により保護されることから、それらの範囲外の事項、すなわち適用法令による制限、秘密保持義務、及び取決め事項1のインプットの利用制限等の範囲外については、原則として事業者が自由に利用できるものとすることが望ましい。末尾の注記において「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」とされているが、上記の通り原則を「自由利用」とし、制限事項を明示的に列挙する構成とする方が、事業者の予見可能性及び制度の透明性の観点から適切と考える。【Preferred Networks】

ノウハウについては、各案件における定義を明確にした上で「事業者が自由に利用できるものとする」かどうかも含め、その利用条件や権利帰属等を定める条項を契約に盛り込むことを検討すべきことを示す趣旨で、別紙4 契約チェックシート取決め事項#6にて「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。」と記載しているものです。

取決め事項#1におけるインプットの利用制限等の範囲外について、事業者によるノウハウの自由利用を原則とすることにつきましては、ご意見として承ります。

別紙4 契約チェックシート

提出された主なコメント

ご意見に対する考え方

別紙4 契約チェックシート 取決め事項#8

・■原文: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…について、あらかじめ事業者と合意しておく必要がある。

■変更案:…、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に関し、事業者が権利を保有し開示可能な範囲、又はサードパーティの基盤モデル提供者が公開している情報の範囲を含み得る)を政府の求めに応じて…

■意見理由:外部API(OpenAI等)を利用する想定で考えた場合、基盤モデル自体のアルゴリズムや事前学習データを保持・開示する権限がありません。「提供不可能な機密情報の開示」を契約上義務付けられるリスクとして解釈されかねず、提供可能な範囲を限定すべきです。【グラファー】

・「(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」という点について、情報やデータの提供に関し、「提供事業者が自ら保有・管理し、提供可能な範囲に限る」旨を追記いただきたい。他社製の基盤モデルを利用している場合、学習データやアルゴリズムの詳細は提供事業者に開示されないことが多いためである。また仮に事業者自らが保有・管理する情報等であっても、それが営業秘密等に該当する場合は合理的な代替手段(概要の説明や限定条件を付した上での開示等)で足りる旨も明確にすべき。【楽天グループ】

当該記載は、取り決めた事項を契約に盛り込む際の条項内容例に対する補足説明であり、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情報の提供を事業者に一律に要求するものではありません。当該記載は、ご指摘の点も考慮して、取決めを踏まえて「政府の求めに応じて合理的な範囲で提供すること」としているため、原案のとおりとさせていただきます。

ガイドライン全体

提出された主なコメント

ご意見に対する考え方

全体的な方針案に賛成

・本改訂については、政府内外における生成AIの利用実態を踏まえ、ガイドラインを拡充するとともに、各種リスクへの対応として記載内容を充実させるという全体の方向性に賛同いたします。【日本電気】

・本改定案は、生成AIの急速な技術的发展及びその利活用の拡大という状況を踏まえ、政府調達における円滑な運用の確保に資するとともに、想定される論点及び必要な対策の網羅性を高めるものであり、総論として支持する。もっとも、生成AIの適用領域や利用形態は多様であり、求められるリスク水準や対応の程度も案件ごとに大きく異なる。このため、すべての調達案件において一律の対応を求めるのではなく、各案件の目的、利用範囲、リスク特性等に応じて、必要な要件を選択的に適用できる柔軟な運用が確保されることが重要である。運用にあたっては、過度に画一的・形式的な適用とならないよう配慮しつつ、実務に即した弾力的な運用がなされることを期待する。【Preferred Networks】

賛成のご意見として承ります。

全体的な方針に反対

・個人情報や機密情報を取り扱うAIを政府で取り扱うべきではない。【個人】

・AIの利活用のせいでかえって余計な業務が増えるのではないか。【個人】

・「生成AIの利用によって業務の効率化を図ったが、実際には労働時間が増加した」との報告がすでに多数あり、疑問に思う。果たして生成AIが抱える多数のリスクを上回るほどのメリットや成果があるだろうか。

本案では基盤データセットの権利侵害や環境への負荷など、使い方の工夫程度では対応できない根本的な問題も多く抱えている点を無視しているように思う。【個人】

生成AIの利活用にあたってはリスクが伴いますが、本ガイドラインは生成AI利活用推進のためのガードレールであり、生成AIの安心・安全な利活用を着実に進展させ、利益の実現を目指すものです。

ガイドライン全体

提出された主なコメント

全体的な方針に反対(リスクに着目した反対意見)

- ・AIというリスクのあるシステムを政府で使うべきではない。【個人】
- ・AI活用によるリスクや不利益をより一層取り上げるべき。【個人】
- ・生成AIのリスク・危険性に関する記述が不明瞭及び、対策が曖昧かつ非積極的と思われる箇所が見られる為、撤廃を前提とした再考を提案させていただきます。【個人】
- ・「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」という項目がある時点で論外である。そもそもそんな可能性があるような生成AIの調達、利活用は一律禁止するようガイドラインに明記すべきだ。【個人】

ご意見に対する考え方

生成AIの利活用にあたってはリスクが伴いますが、本ガイドラインは生成AI利活用推進のためのガードレールであり、生成AIの安心・安全な利活用を着実に進展させ、利益の実現を目指すものです。

高リスクの可能性が高い生成AIの利活用であっても、先進的AI利活用アドバイザリーボードの助言やAI相談窓口への相談等も活用しながら、適切な軽減措置を講じることにより、リスクを軽減しつつ、生成AIの利活用推進を可能とすることとしております。

ガイドライン全体

提出された主なコメント

ご意見に対する考え方

本ガイドライン全体への意見

全体として「等」と「など」が混在しているがどのような整理に基づいて書き分けているのか。【個人】

ご意見を踏まえ、「など」と記載した箇所を「等」に修正いたします。

本ガイドライン全体への意見

3. 先進的AI利活用アドバイザリーボードにおけるリスク判断の蓄積に敬意を表します。先般第2回アドバイザリーボード(令和8年1月13日)にて公開された具体的な審査観点は、官民双方が効果的に利活用を検討する際の重要な指針となりました。検討の予見可能性を高めるため、今後も継続的に審査事例を公表いただくことを希望します。特にガバメントAI等において最も先進的に利活用を推進される官庁の一つであるデジタル庁の先進的実証におけるリスク判断等についても、引き続きタイムリーに情報を公開しつつ進めていただくことを期待します。【セールスフォース・ジャパン】

今後の運用・改定の検討にあたって参考とさせていただきます。

本ガイドライン全体への意見

P45「6.7 生成 AI システム特有のリスクケースへの対応」や別紙2のP5「表 2 AI 生成物の利用段階の知的財産権等の対策の例」において、画像や音声といったもののみが著作物として扱われており、書籍の本文や小説等の文章を著作物として扱っていないように受け取れる。画像や音声、動画と同様に文章にも著作権は発生するため不適切である。【個人】

ご意見を踏まえ、「**画像等の出力結果**」が、既存の著作物に類似した要素を含んで出力され、その状態に気付かないまま利用してしまうリスク」に修正いたします。

ガイドライン全体

提出された主なコメント

ご意見に対する考え方

ガイドライン全体への改善提案

・今後のガイドライン改定にあたっては、既に検討項目として示されており、将来的に民間企業の活用が進むと考えられる外部認証や既存の評価・認証スキーム等との関係性や、これらを組み合わせた活用の考え方についても明示いただくことで、民間企業の参入促進や円滑な対応につながるものと考えます。【日本電気】

・ISO42001取得事業者の説明負担軽減については、同規格の活用がより進んだ段階で反映を検討する方向と承知しております。本規格の普及はAIサービスのさらなる安全性確保に直結し、政府調達ガイドラインへの反映はその強力な後押しとなります。弊社は既に同規格を取得しており、今後、制度設計に向けた事業者ヒアリング等を実施される場合は喜んで協力させていただきます。【セールスフォース・ジャパン】

外部認証の活用は継続検討事項としており、今後の運用・改定の検討にあたって参考とさせていただきます。

ガイドライン全体への改善提案

プロンプトの入力ログ、出力ログを保存しておくことを義務化しなさい。重大な瑕疵があったとき、問題点を遡って確認することができなくなる。責任逃れの言い訳として利用されてしまう恐れがある。【個人】

ログについては、本紙「6.3.1 生成AIシステムの企画時の対応事項」において、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適切に行うこととしております。さらに、別紙2の利活用ルールひな形でも、入力結果及び出力結果は必要に応じて提供者に提供する必要がある旨を記載しています。したがって、重大な瑕疵等が生じた場合に事後確認を可能とする観点からは、原案に盛り込まれているため、原案のとおりとさせていただきます。

ガイドライン全体

提出された主なコメント

ご意見に対する考え方

ガイドライン全体への改善提案

AIの位置付けと統治・調達設計の抜本的見直し

現行ガイドライン案では、生成AIは一貫して「ツール」または「システム」として整理されておりますが、この前提自体を見直す必要があると考えます。AIエージェントの急速な進展を踏まえると、AIはもはや人間が操作する受動的なツールではなく、業務を自律的に担う「主体（リソース）」としての性質を強めております。用語定義（2.2.2）および利活用方針（3.1、5章）において、AIを「業務の一部を担う主体」として明示的に再定義されることを求めます。

この再定義は、ガバナンス設計にも直結いたします。現行案はCAIOを中心とした統治構造を想定しておりますが、AIが業務主体となる環境では、人材・組織マネジメントとの統合が不可欠であり、CAIO単独の管理では限界があります。CHROや各事業部門と連携した統合的マネジメントの枠組みを6.2および4.2.1に明示いただくことを要望します。

同様に、調達設計（6.3.2）においても、AIを「個別システム」として切り出す現行の発想を改め、人的リソースとAIを統合したコスト設計・全体最適の観点で調達方針に組み込むことが必要と考えます。

さらに、AI利活用の実効性を高めるためには、AI-Readyな情報環境の整備が前提となります。6章の利活用ルールにはデータ管理の記述はあるものの、コンテンツ構造やメタデータ設計の視点が欠落しております。AIが業務文脈を正確に把握し、適切に機能するためには、メタデータ設計を含むコンテキスト実装の方針を利活用ルールの前提として明記いただくことを求めます。

【Box Japan】

AIエージェントに係る今後の運用・改定の検討にあたって参考とさせていただきます。

ガイドライン全体

提出された主なコメント

ご意見に対する考え方

ガイドライン全体への改善提案

- ・AIエージェント等を本ガイドラインの対象に含めるのであれば、具体的対応事項を今後の検討に委ねるだけでなく、少なくとも最低限の統制原則を本文に明記すべきと考えます。具体的には、1.権限範囲の明確化、2.人による介入・停止可能性の確保、3.重要な処理・判断過程のログ確保、4.モデルの大幅更新や追加学習時の再評価、5.外部サービス接続時のリスク見直し、を基本原則として示すことが望ましいと考えます。【個人】
- ・AIエージェントへの判断制限要件の明示を求む。【個人】
- ・一定の行政事務における生成AI活用を原則とする運用を明確化すべき。【個人】
- ・本改定案においては、生成AIの出力について「人間による確認」を前提とした運用が中心に設計されているが、この前提のみでは生成AIの利活用による効率化効果は限定的であり、今後の利活用拡大において持続困難となる可能性がある。現状において、生成AIの出力が不確実性を含むことから人間による検証が必要である点は理解できるが、すべての出力に対して人間が個別に確認を行う構造は、業務負荷の観点からスケーラビリティに課題がある。このため、現行の「人間による全面的確認」を前提とした運用に加え、検証依存からの段階的な脱却を見据えた制度設計の方向性をガイドラインにおいて明確に示す必要がある。(中略)単なる運用上の注意喚起ではなく、出力の信頼性を制御するための技術的要件を制度として明確化することが不可欠である。【個人】
- ・別紙等の様式は紙やスプレッドシートではなく、JSON等の機械可読形式で提出可能とすることで、行政内部の再利用性・検証可能性・効率性に配慮すべきである。【個人】
- ・対象とする生成AIについて「原則として、入力テキスト及び音声、出力はテキスト、画像又は音声が可能なもの」と記載があります。一般に「コンテンツの利用」というのは、商用のコンテンツについては利用権料(ライセンス料)によって、コンテンツ制作を行う事業者・個人事業主が提供するものであり、この指摘箇所において注釈程度でも記載がなされるべきであると考えます。【個人】

ご意見として承ります。

B. A以外で多く寄せられたご意見と
その考え方

提出された主なコメント	ご意見に対する考え方
(生成)AI反対の意見 ・生成AIの利用そのものを支持しない。【個人】 ・権利侵害の可能性があるAIは使用しないでほしい。【個人】	
生成AIによる不利益への懸念 ・生成AIのリスクや悪影響に対する懸念(著作権侵害、個人情報漏えい、AIへの過度な依存等)がある。【個人】 ・生成AIの出力結果に対する懸念(公平性の欠如、行政文書等の質の低下等)がある。【個人】	生成AIの利活用にあたってはリスクが伴いますが、本ガイドラインは生成AI利活用推進のためのガードレールであり、生成AIの安心・安全な利活用を着実に進展させ、利益の実現を目指すものです。
AI関連の政府の政策、法規制の在り方に対する意見 ・生成AIに対する法規制や罰則を速やかに整備すべき。【個人】 ・生成AIの利用を禁止又は強く制限すべき。【個人】 ・個人情報・著作権・人権その他の国民への影響に配慮すべき。【個人】 ・AIの透明性・責任の所在・識別可能性を確保すべき。【個人】 ・AIに関するガイドラインに散乱しており、国民や企業としてはどれを参照すればよいかわからず、また、拘束力のないガイドラインであれば参照・考慮する必要がないものと軽視される可能性がある。全体の整合性を図った上で、真に参照すべきガイドラインを絞った上で、公表して頂きたい。【個人】 ・昨今の生成AIを取り巻く議論は結論ありきでリスクを軽視しており、倫理的に正しい行為とは到底思えません。推進と規制の平等な議論の活性化を望みます。本邦もプリンシプル・コードをはじめとするルールを策定していること存じ上げていますがその内容の実効性に疑問を感じざる負えません。より踏み込んだ欧米・そして世界基準のルールの策定を望みます。【個人】	高リスクの可能性が高い生成AIの利活用であっても、先進的AI利活用アドバイザリーボードの助言やAI相談窓口への相談等も活用しながら、適切な軽減措置を講じることにより、リスクを軽減しつつ、生成AIの利活用推進を可能とすることとしております。

提出された主なコメント	ご意見に対する考え方
AI関連の政府の政策、法規制の在り方に対する意見 生成AIによる高度な住民サービスの提供の実現には、住民データあるいは民間データ利活用において個人情報保護の制約や同意取得の手続き等の課題を解決する必要があります。実効的なデータ利活用のためには、参照されるデータの種類や所在、権利関係（オーナーシップ）の整備が重要であり、以下の3点について生成AIの調達・実装戦略と連動した検討を提言します。 - データ戦略の策定: 参照元となるデータの所在と権利関係を整理した戦略的な整備 - 適正な利活用ルール of 構築: 時代に即したデータの利活用基準を策定し、既存の規制や枠組みも必要に応じて再検討 - オンライン同意取得の仕組み化: Web等を活用した簡便かつ透明性の高い同意取得（デジタル・コンセント）の推進 【セールスフォース・ジャパン】	ご意見として承ります。

提出された主なコメント	ご意見に対する考え方
学習・開発時のデータ等に関するご意見 ・権利上の問題が解決されたクリーンな学習データ・生成AIモデルを求める。【個人】 ・学習データの透明性・説明可能性を確保すべき。【個人】 ・生成AIに個人情報や著作物等を本人の同意なく読み込ませるのはやめてください。【個人】 ・日本人の個人情報を売る為のサービスのようなシステムに自分や家族の個人情報をとられたくありません。【個人】 ・画像生成を利用するにしても、無断盗用のデータではなく、同意した人物からの学習を元にしたデータを作してほしい。【個人】	個人情報や知的財産権等の保護は、ガイドライン本文や別紙3調達チェックシート、別紙4契約チェックシート、別紙2利活用ルールひな形に基づき作成された各府省庁における利活用ルール等に対応事項を記載しております。 別紙3調達チェックシートでは、「評価・選定時の分類」に当てはまる場合は、学習段階、生成段階に関する要求事項を踏まえて調達を実施するほか、説明可能性や検証可能性等の評価観点と要求事項も設け、総合的に対策することとしています。 別紙4契約チェックシートでは、生成AIシステムが扱うデータ等の取決めを踏まえて調達に係る契約を実施することとしています。 別紙2利活用ルールひな形においては、生成AIシステムの利活用時の知的財産権等に係る対策を整理し、プロンプト入力段階及びAI生成物の利用段階におけるルール・対策例を記載しています。 また、政府内限りの参考資料ではありますが、国民向け生成AIシステム利用規約作成時の留意事項も作成し、国民向け生成AIシステムの提供に際しての利用規約による同意取得の観点も確認することとしています。

提出された主なコメント	ご意見に対する考え方
環境への負荷に関する意見 ・生成AIは水・電気といった資源を無尽蔵に消費し人々の生活を圧迫する「公害」と成り果てていたり、そのシステムのもつ悪質性が広く警戒され、強い規制の方向が潮流となっている中、まるで逆進するように「違法性の塊である生成AIを利活用しよう」などという方針を検討すること自体、著しく国益を害するものであり、「いまずぐ検討そのものをやめるべき」であります。【個人】 ・生成AIは環境に対するリスクも非常に大きいと報じられています。生成AIの稼働に必要なデータセンターの維持には大規模なエネルギー・資源の消費にとどまらず、常時サイバー攻撃や紛争発生時に狙われる危険がつきまといます。【個人】 ・資源を消費し過ぎる問題は特に深刻に感じます。私の地域でも水が不足していますが、生成AIは人が使う水資源まで消費したり地球温暖化に大きく寄与するのではないのでしょうか。【個人】	ご意見として承ります。今後の運用・改定の検討にあたって参考とさせていただきます。 なお、別紙3調達チェックシートでは任意追加項目として「環境に配慮した生成AIシステムを開発・提供すること」を要求事項として設けております。
国産の生成AIの開発を支援すべき ・「国内での、政府主導の透明性の高い生成AIモデルの作成」を強く求めますがどうですか。金銭的な負担は大きいですが、本ガイドラインで示されるリスクのほとんどをかなり低減できます。行政府が示してきたこれまでの生成AIモデルの業務への利用による便益を鑑みれば十分検討するに値すると思います。【個人】	本ガイドラインの見直しに直接関係するご意見ではないため、参考として承ります。

提出された主なコメント	ご意見に対する考え方
パブリック・コメント実施期間に対する意見 ・資料が赤書きや訂正線(取り消し線)ばかりで非常に読みづらく、内容が整理されていないため要点が全くもってわかりにくい。このような杜撰な資料で議論を進めているデジタル庁は、本件に関心を持って意見を提出する国民を馬鹿にしていると強く感じる。生成AIの利活用を推進しようとしている行政府(デジタル庁)自身が、デジタルツールを使いこなせず、まともな資料一つ作れない状況では、先行きに不安しかない。提出期限が午前10時という設定も、労働者である国民の事情を何一つ考慮しておらず、配慮に欠ける。【個人】 ・文章内で打消し線が多用されておりどの内容が適用範囲なのか視認性、可読性がとても低い。パブリックコメント制度は障害に関わらず広く国民へ意見を募る為のものである、それらを考慮した上で作成された資料とは思えない。【個人】	今後の運用・改定の検討にあたって参考とさせていただきます。