資料２－２

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について

2025/10/9　デジタル庁

デジタル庁
Digital Agency

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ポイント

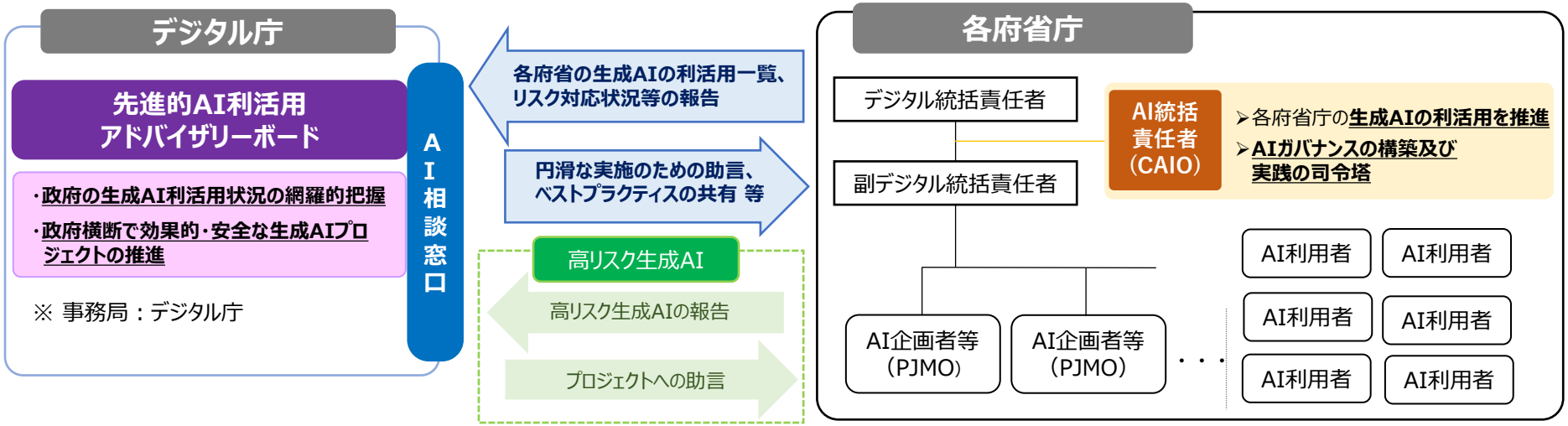
（１）ガイドラインの目的・枠組み等

目的：**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AIの推進・ガバナンス・調達・利活用のあり方**を定めるもの。
対象：**テキスト生成AIを構成要素とするシステム**　※特定秘密や安全保障等の機微情報を扱うシステムは対象外
適用開始時期：**令和７年５月に運用開始**。

（２）政府における生成AIの推進・ガバナンス体制の構築

- 比較的**高リスクとなる可能性がある生成AIの利用**であっても、**先進的AI利活用アドバイザリーボード**の各府省への助言や**相談窓口**等の仕組みを通じ、**安全かつ効果的AIプロジェクトとしての実施をサポート**し、先進的生成AIの利活用を促進。
- 各府省庁に新たに設置する**AI統括責任者（CAIO）**が、**生成AIの利活用を把握・推進、ガバナンス、リスク管理を総括**。

※サプライチェーンリスクも考慮



（３）生成AIの調達・利活用ルール

※ 各府省庁生成AIシステムの①**AI統括責任者（CAIO）**、②**企画者**、③**提供者**、④**利用者等**毎にルールを規定

- AI統括責任者（CAIO）は、各府省の利用者（職員）に向けて**生成AIの利用ルール**を策定。
- 企画者・提供者は、本ガイドラインの**「調達チェックシート」**及び**「契約チェックシート」**を参考にして仕様書作成や事業者との契約等を行うことにより安全かつ品質の高い生成AIシステムの調達を確保。運用開始後も適切な利用や安全性や品質の確保を定期的に検証。
- 提供者及び利用者は**リスクケースが生じた場合、適切に各府省庁AI統括責任者（CAIO）に報告し、提供者が必要な対応を実施**。先進的AI利活用アドバイザリーボードは各ケースの報告を受け、必要に応じ再発防止策等を検討。

先進的AI利活用アドバイザリーボードについて

○ 政府横断で効果的・安全な生成AIプロジェクトを推進するため、デジタル社会推進会議議長決定（2025年６月12日）により、「先進的AI活用アドバイザリーボード」が設置（事務局デジタル庁）。
○ 各府省庁から生成AIの調達・利活用状況の報告を受けつつ、官民のベストプラクティスの共有、ガイドラインの更なる改定を検討するとともに、WGを開催し、高リスクAIへのリスク緩和策等の助言を実施予定。
○ 年度内に３回程度開催の上、１回目のガイドライン改定を検討。

１．目的

政府横断で効果的・安全な生成AIプロジェクトの推進のため、以下の役割を担う。
①各府省庁における生成AIの調達・利活用状況の把握、②各府省庁における高リスクAIやリスクケース等への助言、
③各府省庁におけるAI利活用のベストプラクティスの共有、 ④各府省庁における生成AIの効果的な利活用等に関する助言、
⑤ガイドラインの見直しの検討　等

２．構成員

大柴 行人	（一社）AIガバナンス協会　代表理事	鳥澤　健太郎	NICT　フェロー
岡田 幸彦	筑波大学　システム情報系／ 高等研究院人工知能科学センター　教授	永沼 美保	（一社）日本経済団体連合会　デジタルエコノミー推進委員会企画部会国際戦略WG　主査
門林 雄基	奈良先端科学技術大学院大学 教授	生田目　雅史	東京海上ホールディングス 専務執行役員
北村 弘	IPA　デジタル基盤センター　エキスパート	湯淺 墾道	明治大学専門職大学院　教授
柴山 吉報	（一社）日本ディープラーニング協会 弁護士	吉永 京子	慶應義塾大学大学院　特任准教授

３．R7開催スケジュール(案)

第１回（9/18）　ガイドライン充実に関する論点案、運営要領、各府省庁利活用状況報告　等
第２回　　ガイドライン改定方針案、各府省庁生成AIシステム報告、各府省庁利活用状況報告　等
第３回　　ガイドライン改定案、各府省庁利活用状況報告　等

このほか、WGを随時開催し、必要に応じてアドバイザリーボードに報告予定

政府AI調達・利活用ガイドラインの充実に向けた論点候補

政府調達ガイドラインについて見直しの観点を第一回のアドバイザリーボードで議論いただいたところ。
他の関係ガイドラインの議論を踏まえた記述の追加についても見直しの観点の一つ。

＜ガイドラインの課題と充実に向けた論点候補＞

Ⅰ　政府内外の利用実態等を踏まえたガイドラインの拡充
Ⅱ　生成AIのリスクに対応する記載の見直し・充実
Ⅲ　チェックリストのupdateやベストプラクティスの充実
Ⅳ　現行ガイドラインで記述が不足している他の制度等の記述の追加

ガイドラインの関連領域における既存制度や法令との概念整理が求められていると考えているところ。
以下のような内容について検討を行うこととしてはどうか。

＜セキュリティ関係＞
- ISMAP制度とクラウドサービス上で実装される生成AIについての見解が問われるケースが多く、パブコメでも意見として接到。
- 総務省においてAIセキュリティに関する分科会が開催、AIに対する脅威への技術的対策のガイドライン策定を予定。

→ ＜論点候補案＞
- クラウドサービス基盤としてのセキュリティの他、生成AIを用いることに起因するセキュリティ対策について、関係する制度及びガイドラインも踏まえつつ必要な見直しを行うべきではないか。

＜知的財産関係＞
- チェックシートの知的財産関係の要求事項において、対策例・対策例の具体例を明示できていない。

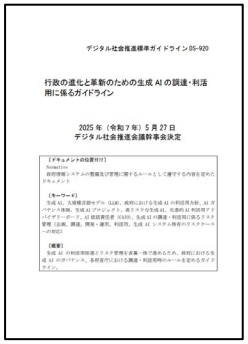
→ ＜論点候補案＞
- 調達チェックシート等について、「コンテンツ制作のための生成AI利活用ガイドブック」や「AI時代の知的財産権検討会中間とりまとめ」等も踏まえた記載を追加すべきではないか。

＜既存のAIシステムガイドラインとのレファレンス＞
- 「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こととされている。
- AIマネジメントシステムの国際規格であるISO/IEC 42001等との対応関係が未整理。

→ ＜論点候補案＞
- 評価観点ガイドは、画像を取り扱う生成AI利用の評価観点が追記されているため、Ⅰ課題②と連動して、修正を検討すべきではないか 。
- AI関係の規格標準の動向を踏まえ、要求事項との対応関係を整理し、調達時の事業者の説明負担を軽減すべきではないか。

※その他、AI調達・利活用に関係しうる法令・ガイドライン等の見直しがあった場合、本ガイドラインにおいても見直すべき事項が無いか必要に応じて検討を行う。

ガイドラインの構成


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

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

ガイドライン本紙

政府のAI利活用におけるガバナンスや基本的な考え方、AI利活用各フェーズにおける対応事項の概要等を記載

別紙1 高リスク判定シート

参照推奨

ガイドライン本紙で記載する4つのリスク軸に係る設問に回答することで、「高リスクに該当する可能性が高い」かそうでないかを簡易的に判定するツール

別紙2 生成AIシステムの利用ルールひな形

参照必須

各府省庁において、AI統括責任者（CAIO）が各府省庁の利用者(政府職員)に向けて策定する生成AIシステムの利活用ルールのひな形

別紙3 調達チェックシート（生成AIシステム用）

参照必須

生成AIシステムの調達時に、事業者及び調達予定の生成AIシステム等について、調達の応募者に求める事項として調達仕様書に盛り込む事項を企画者が参考とするサポートツール

別紙4 契約チェックシート（生成AIシステム用）

参照必須

生成AIシステムの調達において留意すべき事項を、契約書または調達仕様書に盛り込む際に企画者が参考とするサポートツール

調達チェックシートにおけるAIセキュリティ関係の要求事項①

No	要求事項	対策例	対策例詳細	裏付けとなる情報の例
・ ・	・・・・	・・・・	・・・・	・・・・
23	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いること	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ている		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
		プロンプトインジェクションなどにより生成AIシステムの防御策の回避が可能ではないか、また、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を講じている		プロンプトインジェクションなどにより生成AIシステムの防御策の回避が可能ではないか、また、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かの確認方法がわかる資料等
		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

「（参考）要求事項の参考」シートより、一例を抜粋

調達チェックシートにおけるAIセキュリティ関係の要求事項②

No	要求事項	対策例	対策例詳細	裏付けとなる情報の例
・ ・ ・	・・・・	・・・・	・・・・	・・・・
23	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いること	RAGを利用した生成AIシステムにおいて、要機密情報が出力されないよう、RAGによる検索先のアクセス権限の設定等に不備がないことの対策を講じている ※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システムにおいて、要機密情報が出力されないよう、RAGによる検索先のアクセス権限の設定等に不備がないかの確認方法がわかる資料等
		禁止リストを活用したプロンプト検知など、生成AIシステムへの入力段階での防御策を提供する技術を有している		禁止リストを活用したプロンプト検知など、生成AIシステムへの入力段階での防御策の実装方法がわかる資料等
24	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		セキュリティ対策についての資料等

政府調達ガイドラインにおいても、調達仕様としてAIセキュリティ関係の要求事項については盛り込んでいるものの、対策例の詳細について、どのような技術・対策があるかについて具体的に示せていないところ。

「（参考）要求事項の参考」シートより、一例を抜粋

（参考）ガイドラインの見直しに関する記述

2.2.2 本ガイドラインが対象とする生成AI

（略）

なお、画像や動画等を生成するAI、より高度なタスクを実行できるAI（AIエ ージェント等）、その他のAIについては、政府等における利活用状況、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。

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

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。

6.3.2 生成AIシステムの調達時の対応事項

「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）」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LLM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。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。

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。

政府調達ガイドラインについては、AIの利活用動向や他の関係ガイドラインの改定・運用状況を踏まえつつ見直しを行うこととしており、貴分科会における議論も参考にさせていただきたい。

（参考）高リスクの考え方

ガイドラインでは4つの軸でリスクが高いかどうかを考える

リスク軸	リスクの考え方
A. 利用する人や範囲の広さ	誰が使うのか、どのような立場で使うのか。国民向けか省内に閉じるのか、範囲が広いほどリスクが増す
B. 利用の目的や性質	どのような業務目的で活用するのか。人間の生命・身体・財産に影響を及ぼす業務など、ミスが重大になる場面ではリスクが高まる
C. 学習データや個人情報の扱い	機密性の高い情報（個人情報・秘密情報など）を学習させるかどうか。そうしたデータを使うほど慎重な管理が必要となる
D. 出力結果のチェック	生成AIが出力した内容を必ず人間がチェックするのか。チェックがなければ誤情報や不適切な内容がそのまま使われてしまう可能性がある