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（概要）

2025/5

デジタル庁
Digital Agency

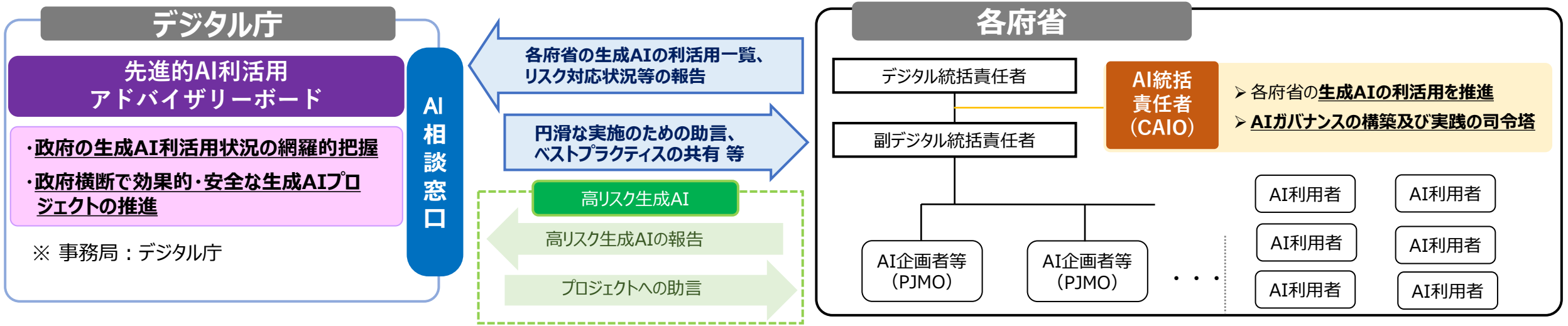
行政の進化と革新のための生成AIの調達・利活用に係るガイドラインのポイント

（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。　※サプライチェーンリスクも考慮
- 各府省に新たに設置する**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**。



（３）生成AIの調達・利活用ルール

※　各府省生成AIシステムの①AI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。

（参考１） 別添各シート（高リスク判定シート、調達チェックシート、契約チェックシート）について

１．高リスクAIの判定についての参考とする判定軸（高リスク判定シート）

４つの観点を勘案し、
アドバイザリーボードに助言を求めるべきか各省において判定

A.生成AIシステム利用者の範囲・種別（国民か政府職員か等）、 B.生成AI利用業務の性格、
C.機密情報や個人情報の学習等の有無、 D.出力結果の職員による判断を経る利用か否か

２．調達・契約時のチェック項目について（調達チェックシート、契約チェックシート）

（１）調達チェックシート

生成AIを調達する際に**事業者への要求事項**として、**仕様書等に盛り込むべき項目を整理**

ガバナンス項目

①AI事業者ガイドライン共通の指針の遵守　②AIガバナンス（AIのメリットを最大化しつつ、リスクを統制する体制）の構築
③生成AIシステムの品質向上のため、AI業界や最新技術等の動向を把握する
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手順の整備
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の生成AIに関する教育・リテラシー向上

開発・運用プロセス要件項目

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の適切な管理
⑦生成AIシステムの期待品質を満たすための取組
⑧ベンダーロックインの回避　⑨生成AIシステムのアップデートの考慮
⑩文化的・言語的考慮　⑪環境への配慮

生成AIシステムの要件項目

⑫有害情報の出力制御措置　⑬偽誤情報の出力・誘導の防止措置
⑭公平性と包摂性の確保（バイアスや差別を含む出力の抑止措置）　⑮目的外利用の防止
⑯個人情報、プライバシー、知的財産に関する適切な取扱　⑰セキュリティの確保
⑱説明可能性の確保　⑲ロバスト性（出力の安定性）　⑳学習データ品質　㉑検証可能性

（２）契約チェックシート

生成AIを調達する際に**契約書で取り決めるべき項目を整理**

- 生成AIシステムに係るインプットの取り決め（学習の有無、データの保存方法等）
- 生成AIシステムに係るアウトプットの取り決め（アウトプットに関する一定の保証、アウトプットの権利帰属）
- 生成AIを含むインシデントが発生した場合の事業者の対応義務及びその範囲に関する取り決め
  （被害を最小限に食い止めるため、また、原因を特定するための情報やデータの提供を含む）　等

※チェックシートの内容の適用項目や適用方法については、個別の生成AIシステムの調達形態やリスクレベルに応じて、AI相談窓口とも連携しつつ各府省において判断。

（参考２）「生成AIシステムの利活用ルール」について

１．府省毎の利活用ルール

- **各府省のAI統括責任者（CAIO）**が、適切なAIの利活用を促進するため、**「生成AIシステムの利活用ルールひな形」に基づき、各府省の利用者（職員）に向けて生成AIの利活用ルールを策定・周知。**

２．生成AIシステム毎のルール

- **企画者**が、**システム毎に、利用目的をはじめ、利活用に係るルールを策定し、各システムの利用者（職員・国民等）に周知。**

◆1. 府省毎の生成AIシステム利活用ルールの「ひな形」の構成と概要

（構成）

1．ルールの目的

2．生成AIシステムの利用に係るルール

（１）利用前のルール

（２）利用中のルール

① 入力データ又はプロンプトにおけるルール

② 生成物利用におけるルール

3．問い合わせ先

（概要）

- 生成AIの**リスク**についての理解
- 生成AIシステムへの**入力結果や出力結果**が**必要に応じシステム側に提供**されることの理解
- **約款型クラウドサービス**は**原則として要機密情報を扱えない**ことの理解
- **国外サーバを利用**する生成AIの場合に現地政府による**データの検閲や接収を受ける可能性**があることの理解

- 生成AIシステムの**利用目的の範囲内での利用**
- 生成AIシステム毎の**個人情報の取り扱いについての留意**
- 正確かつ最新のデータの入力

- 生成AIの**出力に基づいて行われた判断**についての**説明責任**についての理解
- 出力結果に**含まれうるバイアスを踏まえて**業務に出力結果を活用すること
- 出力結果の**正確性や根拠、事実関係等を必要に応じ確認**すること
- （第三者の著作権等の侵害の有無を含め）**安全性・公平性、客観性、中立性**に問題がある出力でないかを確認し、問題点は必ず加除修正の上で利用すること
- リスクケースやその兆候を検知した場合の**迅速な各府省報告窓口への報告**