

自治体におけるAIの利用に関する ワーキンググループ (第3回)

事務局提出資料

**令和7年4月
総務省**

本ワーキンググループの進め方

1月 23日	第1回WG	・キックオフ（WGの目的、趣旨、進め方など）
3月 5日	第2回WG	・実際のユースケースや自治体への聞取り等を踏まえ、業務効率化等が見込める業務や導入・利用に当たっての課題等を議論
4月 18日	第3回WG	・政府におけるルール策定等の動向等を踏まえつつ、地方公共団体のAI利用に当たっての留意事項やリスク管理等を議論
5月 16日	第4回WG	・政府の取扱い等を踏まえた、AIを利用する上での要機密情報の取り扱いルールについて議論 ・個人情報保護法制関連の検討動向等について報告
6月	第5回WG	・生成AI以外の従来型AI等を活用した自治体業務効率化について議論 ・第4回WGまでの議論を踏まえ、報告書の骨子など、報告書のとりまとめに向けて議論
7月	第6回WG	報告書完成

1. 政府におけるAIに係る動向



人工知能と人権、民主主義及び法の支配に関する欧州評議会枠組条約(仮称)



背景

2025年2月
外務省欧州局政策課

- 2022年4月、欧州評議会の人工知能(AI)に関する委員会において、交渉開始。我が国もオブザーバー国として交渉に参加。
- 2024年5月、欧州評議会閣僚委員会において採択された後、2024年9月から署名開放。
- 2025年2月、我が国及び加はAIアクション・サミット(於:パリ)の機会に署名。2025年2月時点、我が国のほか、11か国(アンドラ、加、ジョージア、アイスランド、イスラエル、モルドバ、モンテネグロ、ノルウェー、サンマリノ、英、米)及びEUが署名済。

(注) 欧州評議会は、1949年に設立された、人権、民主主義及び法の支配の分野で国際社会の基準策定を主導する汎欧州の国際機関。

主な内容

- **目的:** AIシステムのライフサイクルにおける活動(AI活動)が人権、民主主義及び法の支配に合致することを確保する。
- **適用範囲:** 公的機関(代行する民間の者も含む。)のAI活動に適用。その他民間のAI活動による危険性・影響には、条約の規定の適用又はその他の適切な措置のいずれかにより対処(選択した対処の内容は宣言で明示)。国防に関する事項は対象外。
- **AI活動に関する原則:** 人間の尊厳、透明性、監督、責任、平等、無差別、プライバシー・個人情報の保護、信頼性、安全なイノベーション等。
- **危険性・影響評価:** AI活動から生じる人権、民主主義及び法の支配に関する危険性・影響の特定、評価、防止、緩和のための措置を危険性に応じて採用又は維持。
- **人権侵害への実効的な救済:** AIシステムの関連情報の記録、権限のある当局への申立の確保。
- **国際協力:** 条約の目的の実現のための協力、有益な関連情報の交換、人権等に対する危険性防止のための協力。
- **監督の仕組み:** 義務遵守の監督のため、独自かつ公平に役割を果たし、必要な権限・専門知識・資源を備えた仕組みを設置又は指定。

効力の発生

本条約は、5の署名国(欧州評議会の加盟国の少なくとも3か国を含むことを要する。)が、この条約に拘束されることに同意する旨を表明(締結)した日の後3か月の期間が満了する日の属する月の翌月の初日に効力を生ずる。現時点で未発効。

(注) 条約の効力発生後に、締結した署名国については、締結した日の後3か月の期間が満了する日の属する月の翌月の初日に効力が生ずる。

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案（AI法案）の概要

内閣府HP「AI法案概要」から作成

法律の
必要性

日本のAI開発・活用は遅れている。

● 2023年のAIへの民間投資額

1位：米国（約672億ドル） 2位：中国（約78億ドル）
3位：英国（約38億ドル） 12位：日本（約7億ドル）

スタンフォード大学による調査（AI Index Report 2024）

● 生成AIを利用している個人

中国（56%）米国（46%）ドイツ（35%） 日本（9%）

● 生成AIを業務で利用している企業

米国（85%）中国（84%）ドイツ（73%） 日本（47%）

総務省によるアンケート調査（令和6年度版情報通信白書）

多くの国民がAIに対して不安。

● 現在の規制や法律でAIを安全に利用できると思う

中国（74%）ドイツ（39%）米国（30%） 日本（13%）

KPMGによる調査

（Trust in AI : A global study 2023,KPMG）

● AIには規制が必要だと思う

日本（77%） 米国（67%） ドイツ（65%） 中国（56%）

KPMGによる調査

（Trust in AI : A global study 2023,KPMG）

イノベーションを促進しつつ、リスクに対応するため、既存の刑法や個別の業法等に加え、新たな法律が必要。

法案の
概要

目的	国民生活の向上、国民経済の発展
基本理念	経済社会及び安全保障上重要 ➡ 研究開発力の保持、国際競争力の向上 基礎研究から活用まで総合的・計画的に推進 適正な研究開発・活用のため透明性の確保等 国際協力において主導的役割
AI戦略本部	本部長：内閣総理大臣 構成員：全閣僚 関係行政機関等に対して必要な協力を求める
AI基本計画	研究開発・活用の推進のために政府が実施すべき施策の基本的な方針等
基本的施策	研究開発の促進、施設等の整備・共用の促進 人材確保 教育振興 国際的な規範策定への参画 適正性のための国際規範に則した指針の整備 情報収集、権利利益を侵害する事案の分析・対策検討、調査 事業者・国民への指導・助言・情報提供
責務	国、 <u>地方公共団体</u> 、研究開発機関、事業者、国民の <u>責務</u> 関係者間の連携強化 事業者は国等の施策に協力しなければならない
附則	見直し規定（必要な場合は所要の措置）

人工知能関連技術の研究開発及び活用の推進に関する
法律案（第二一七回閣第二九号）（抄）

（地方公共団体の責務）

第五条 地方公共団体は、基本理念にのっとり、人工知能
関連技術の研究開発及び活用の推進に関し、国との適
切な役割分担の下、地方公共団体が実施すべき施策と
して、その地方公共団体の区域の特性を生かした自主
的な施策を策定し、及び実施する責務を有する。

1. AI事業者ガイドラインの令和6年度の更新論点と更新方針

第30回AIネットワーク社会推進会議・
第26回AIガバナンス検討会合同会議資料
(令和7年3月7日)

- ・ 構成員・委員・事業者等からのご意見を踏まえ、令和6年度の更新の論点と更新方針を以下に整理

令和6年度更新論点及び更新方針 一覧

総務省検討会：AIネットワーク社会推進会議・AIガバナンス検討会
経産省検討会：AI事業者ガイドライン検討会

#	更新論点	主なご意見	更新方針
1	AIによるリスクの洗い出し・分類	総務省検討会	リスクの追加・分類・マッピング ✓ AIによる新たなリスク 及び リスクを網羅的に参照する上でのリスク分類を追加 ✓ リスク分類案とガイドラインの「共通の指針」とのマッピングを追加
2	AIの契約に関する留意事項	経産省検討会	開発、提供、利用における契約に関して留意すべき事項の記載 ✓ 「契約モデルや契約当事者の多様化」に関する記載を充実化 ✓ 「開発者・提供者・利用者の間における責任分界」に関する記載を充実化
3	生成AIに関する記載の追加	両検討会	生成AIに関する新たなリスクや留意点の記載 ✓ マルチモーダルな生成AIに関する記載を追加 ✓ RAG導入に関する記載を追加 ✓ プログラムコード生成に関する記載を追加 ✓ AIEージェントに関する記載を追加
4	AIガバナンスに関する事例の充実	両検討会 事業者	AIガバナンスの取組事例の充実化 ✓ 「リスクベース・アプローチ」を実施する上で考慮すべき点を追加 ✓ 「グローバルなAIガバナンスを構築している企業」「中小・スタートアップ企業」「地方自治体」の事例を追加 ✓ AIガバナンスを構築する上での事業者の「人材不足」の課題を追加
5	AIガバナンスの動向等の反映	両検討会	AIガバナンスに関する国内外の最新動向を追記 ✓ AI制度研究会等、国内動向において注視すべき最新状況を追記 ✓ 広島AIプロセスの動向等、国際的な動向において注視すべき最新状況を追記
6	特定単語の整理・見直し	両検討会	AIガバナンスにおいて重要な単語の定義や表現の見直し ✓ 「バイアス」の定義や表現の見直し ✓ 「透明性」の定義や表現の見直し ✓ 「多様性」「包摂性」に関する表現の揺れを修正
7	その他	両検討会	UIの改善 ✓ 目次から該当ページへのリンク

2. 令和6年度の更新内容

2-3. 生成AIに関する記載の追加

第30回AIネットワーク社会推進会議・
第26回AIガバナンス検討会合同会議資料
(令和7年3月7日)

- 生成AIに関する技術の進歩や事業者における導入の進展を踏まえ、マルチモーダルな生成AI、RAG、プログラムコードの生成等に関する記載を拡充する

【更新内容】

① 生成AIによる便益を追加

- ✓「生成AIによる可能性」として、マルチモーダルな生成AI、RAG、プログラムコードの生成、AIエージェントによるリスクの低減やAIそのものの活用範囲の拡大といった便益に関する記載を追加

② 生成AIによるリスクを追加

- ✓環境への負荷、生成物による知的財産権の侵害の可能性といった生成AIの特徴を踏まえ、本編「共通の指針」の「人間中心」「安全性」等における記載を拡充

③ 生成AIに関して配慮すべき事項を追加

- ✓各主体向けに、マルチモーダルな生成AIやRAG、プログラムコードの生成時に配慮すべき事項（RAGにおける参照データの適切な取扱いなど）を整理し記載を追加

【主な更新箇所】

- ✓①別添1. B.AIによる便益／リスク
- ✓②本編第2部 C.共通の指針
- ✓③別添3.AI開発者向け
別添4.AI提供者向け
別添5.AI利用者向け

【更新内容の詳細】

① 生成AIによる便益を追加

生成AIによる可能性⁴⁴⁾

上記に加え、直近では生成AIが台頭している。生成AIはDXへの遅れをとった日本企業の巻き返しの引き金となる可能性も高い。⁴⁴⁾

日本企業の特徴として、良質なOT（Operational Technology）データの蓄積、きめ細やかなサービス及び作業等が挙げられる。これらを従来型のAIを活用することによって実現しようとした場合、組織及び業界横断的なOTデータの活用、それらのサービス、作業等においてAIを活用するためのデータインターフェースの統合、大量のデータの準備、多くのパターンを想定したシナリオ及びケース作り、それらを踏まえた開発等、多くの工数及び専門的な知識が必要であった。ここに生成AIを活用すると、これらのシナリオ及びケース作り自体を自動化でき（自己教師あり学習）、幅広い企業のAI活用を促進することが可能となる。実際に、小売企業のコールセンター及びセールの対応に生成AIで回答並びに資料を作成することにより、生産性を高めている事例もある。また、入力された問い合わせ及び顧客の要望に対し、社内のデータを参照することにより複数のパターンの回答・資料を作成するようなシステムが可能となっている。⁴⁴⁾

さらに、テキスト・音声・画像・動画・センサ情報など、二つ以上の異なるモダリティ（データの種別）から情報を収集し、それらを統合して処理することができる生成AI（以下、マルチモーダルな生成AI）が台頭している。マルチモーダルな生成AIの登場により、医療・創薬・教育・エンターテインメントなどAIの活用範囲が広がることや、推論・分析など生成AI以外の一般的なタスクにおける処理能力も向上すること等が期待されている。⁴⁴⁾

また、RAG（検索拡張生成）の活用も広がっている。LLMによる言語生成に外部情報の検索を組み合わせることによるハルシネーションの抑制、参照する情報源を指定した検索や出力文における参照元の明示等が可能となることによる出力過程・根拠の透明性向上、通常のファインチューニングと異なりモデルの再トレーニングを行うことなく参照するデータソースを追加できることによるコストの低減等が期待されている。⁴⁴⁾

生成AIのプログラムコード生成への活用も進んでいる。低コストかつ迅速なコードの生成が可能となることや、ヒューマンエラーを回避できること、高度な技能・知識がなくてもプログラミングを行えるようになること等が期待されている。⁴⁴⁾

加えて、自律的なAIシステム（以下、AIエージェント）も登場している。従来型のAIや生成AIに比べより高度な効率化や自動化が可能となることで、生産性の向上につながる等が期待されている。⁴⁴⁾

グローバルの激しい競争を勝ち抜くために、生成AIを積極的に取り入れる形でデジタル戦略の見直しを行う等、自身が享受できる便益を正しく理解し、可能性を模索するとともに、積極的な姿勢を持つことが期待される。⁴⁴⁾

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（案）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。

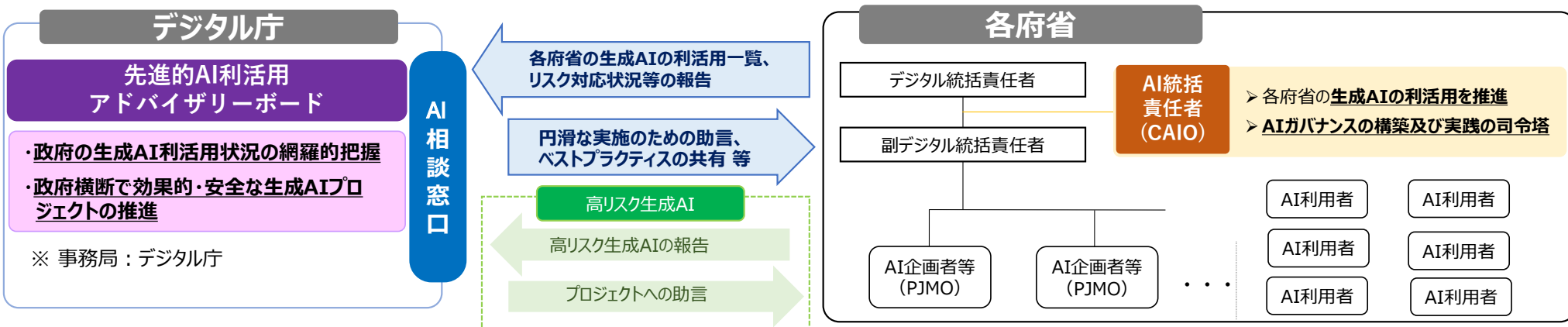
対象：テキスト生成AIを構成要素とするシステム ※特定秘密や安全保障等の機微情報を扱うシステムは対象外

適用開始時期：令和7年5月目途に運用開始。

（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。

- **AI統括責任者（CAIO）は、適切なAIの利用を促進するため、「生成AIシステムの利用ルールひな形」に基づき、**
- ・政府職員等利用者が生成AIシステムの利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
 - ・利用目的の範囲内での利用やAI生成物を利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用に当たって心得るべき事項
 - ・インシデント等発生時の報告窓口への報告
- 等について、**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。**

◆ 府省毎の「生成AIシステム利活用ルール（ひな形）」の構成と概要

（構成）

（概要）

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

- 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
- 不特定多数の利用者に提供され、かつ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型の生成AIサービスは原則として要機密情報を取り扱えないことへの理解
- 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收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

- ① AI統括責任者（CAIO）は、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。
- ② 生成AI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の提供者を中心に、重要度・影響の程度等を踏まえ、適切に対応。**
- ③ **AI統括責任者（CAIO）**は、生成AI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）は各府省に対し必要に応じ、生成AI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**については、**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。**

※生成AIシステム特有のリスクケースとしては以下のようなものが想定される。

＜参考＞ 生成AIシステム特有のリスクケースの例

- ・ 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。

2. 政府の動向を踏まえた、自治体における対応に関する論点

論点①

○ 第2回で紹介した先行団体の取組内容や、第3回で言及された政府におけるAIに関する動向を踏まえ、自治体においてはどのような対応が必要と考えられるか。

例えば、以下については、自治体としてはどのように取り組んでいくべきか。

(例)

- ▶ 自治体における業務効率化等につなげるための取組の推進
- ▶ 従来型AIやRPA等と組み合わせた生成AIの活用
- ▶ 自治体が業務上、生成AIを利用する場合のルール等の整備
- ▶ 自治体が生成AIの適切な利用を進めるために必要な体制の整備
 - ※ 自治体の実情や規模を踏まえ、個別に対応する場合の実効性など
- ▶ 生成AI特有のリスクケースへの対応体制の整備

論点②

- 自治体において、住民利便性の向上や業務効率化の推進につながる**生成AIの利用**や、**論点①で示した対応に取り組むに当たっては、総務省としては、どのような取組をしていくことが必要**と考えられるか。

例えば、以下については、総務省としてはどのように取り組んでいくべきか。

(例)

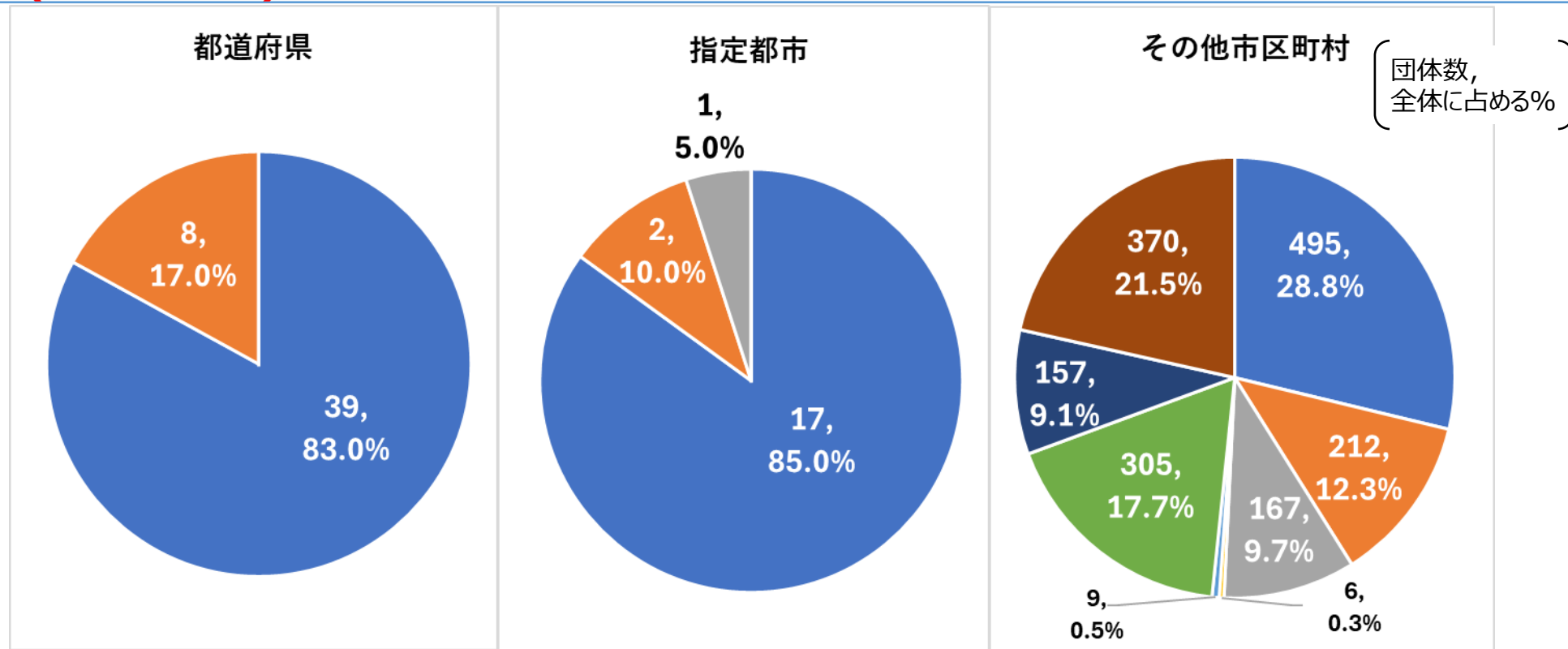
- ▶ 自治体における生成AIのユースケースの提供
- ▶ 機密情報（個人情報を含む）の取り扱いなどの留意事項なども記載した、自治体の生成AIの利用に係るガイドブック等の提供
- ▶ 国の取組に関する情報提供
- ▶ 生成AI特有のリスクケースに関する情報提供と発生・対応状況の横展開
- ▶ 生成AIに係るベストプラクティスの提供

3. 自治体における生成AI導入状況調査 (速報版)(令和6年12月31日現在)

※回答不備等含まれるため、今後集計が修正される可能性があります。

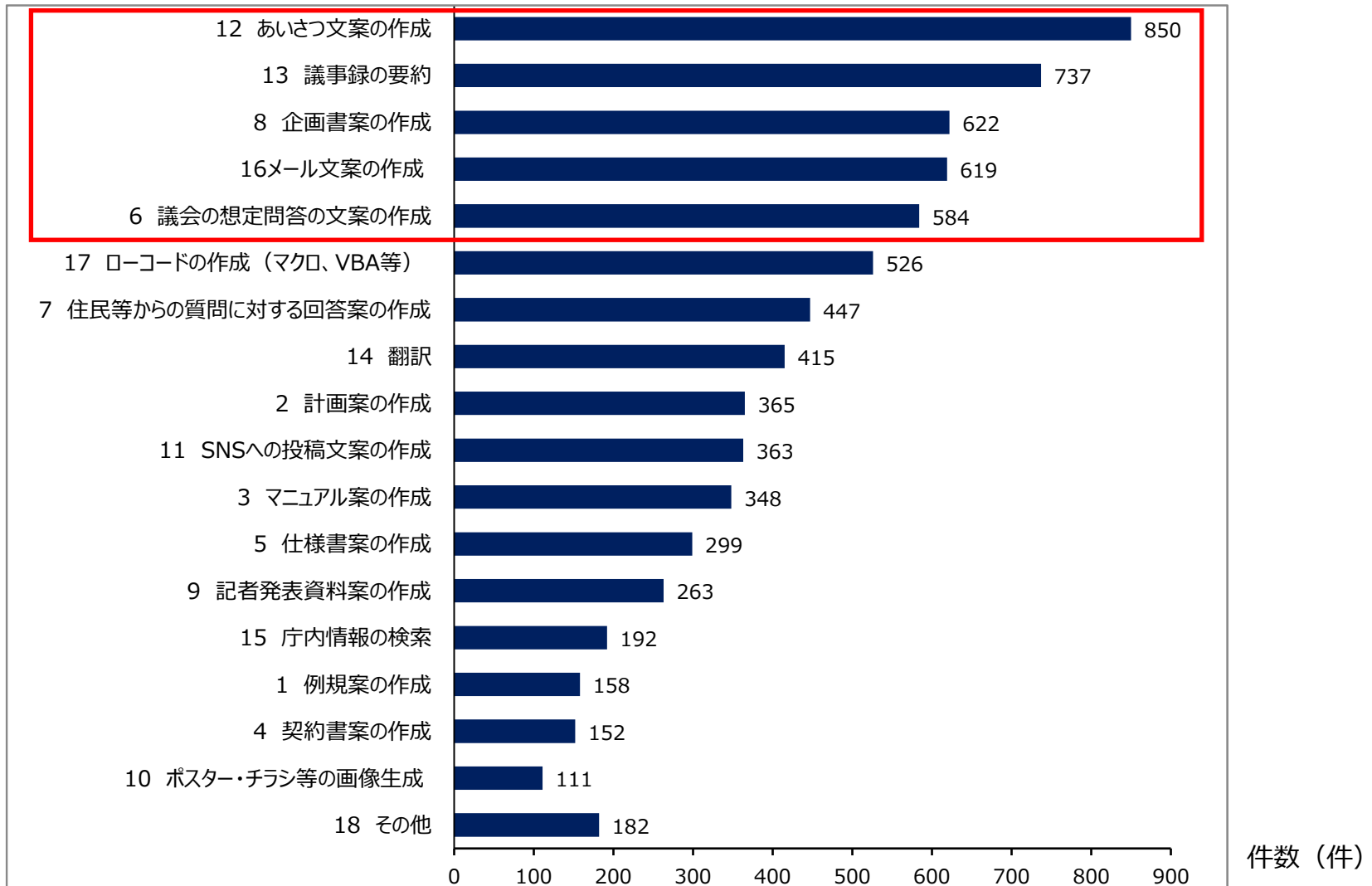
自治体における生成AIの実証実験・導入状況

- 生成AIを導入済みの団体は、都道府県で83.0%、指定都市で85.0%、その他の市区町村で28.8%となった。
- 前回調査（令和5年12月31日現在）と比較し、「導入済」の団体は、**都道府県（前回51%）、指定都市（前回40%）においては大きく増加。その他の市区町村においても、導入済～導入検討中(導入予定あり)の団体**までを含めると全体の50.3%（前回39.5%）と増加し、**過半数となった。**



- 1 導入済
- 2 実証実験中
- 3 導入検討中（導入予定あり）
- 4 導入(実証実験含む)予定はないが、首長レベルで検討している
- 5 導入(実証実験も含む) 予定はないが、幹部レベルで検討している
- 6 導入(実証実験も含む) 予定はないが、担当課レベルで検討している
- 7 導入の検討を行った、または実証実験を実施したが導入には至らなかった
- 8 導入予定もなく、検討もしていない

- 生成AIの活用事例としては、「あいさつ文案の作成」、「議事録の要約」、「企画書案の作成」、「メール文案の作成」「議会の想定問答の作成」が多く、前年度調査（令和5年12月31日現在）から**大きな傾向の変化はみられない。**



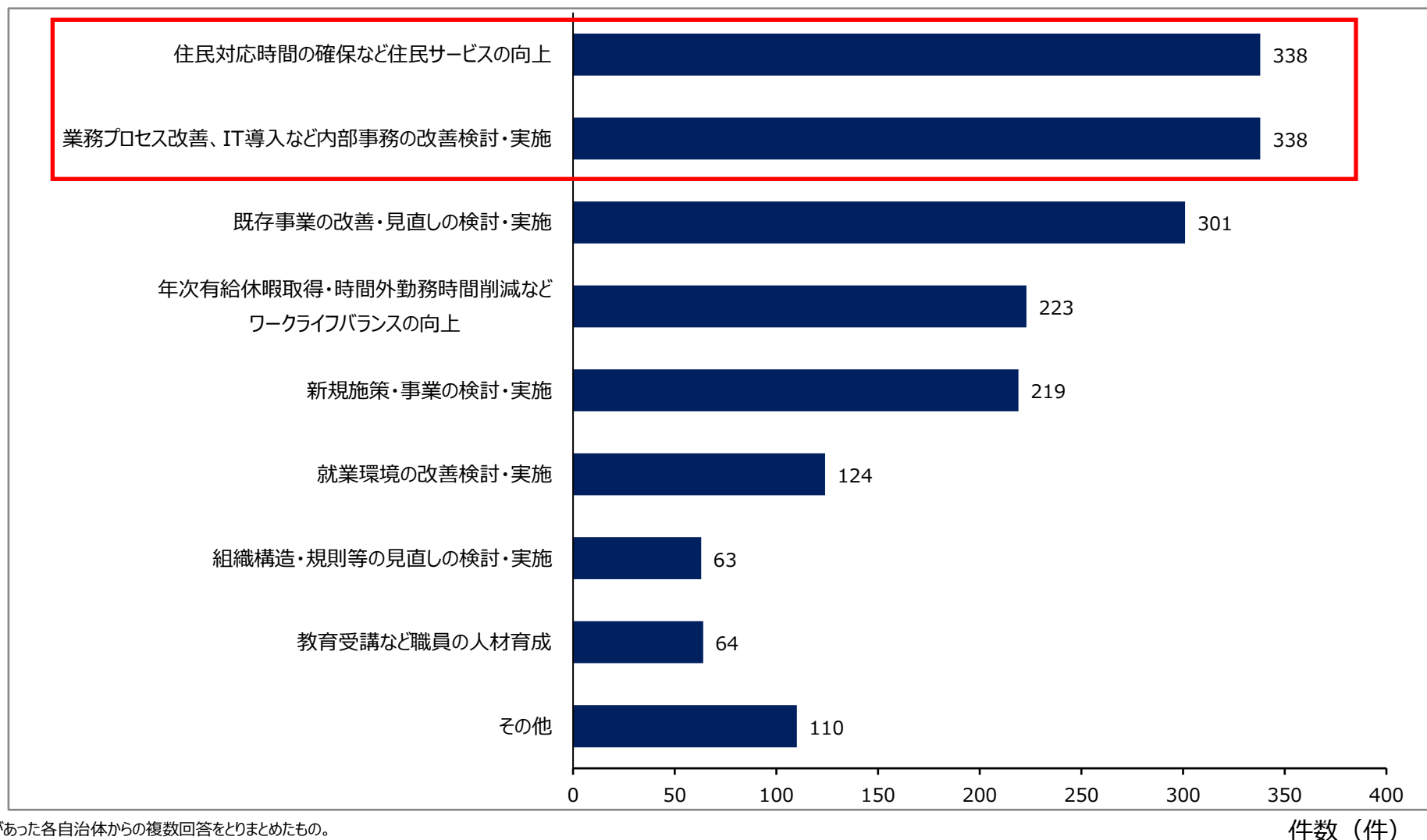
自治体における生成AIの導入効果

- 生成AIの導入効果として、活用事例の多い「あいさつ文案の作成」で1,000時間を超える業務削減効果があったほか、各種活用事例で効果があがっているものの、導入して間もないため効果を検証できていない団体もあった。

活用事例	導入効果	人口規模
議事録の要約	会議録作成において音声からの文字起こし、要約時間を2800時間から1400時間に50%削減できる見込み	4.7万人
計画案の作成 企画書案の作成	企画書・計画書案作成業務の文章作成作業において、一件当たり、1.5時間（約30%）削減	1.8万人
議会の想定問答の文案の作成	議会の答弁書案の修正において、分かりにくい文章について、意図を変えずに新たな文章を作成してもらうことで、修正作業が容易にできた。 想定問答の案を複数提案させた。 5時間の削減×年間質問50件＝250時間	5.7万人
ポスター・チラシ等の画像生成	チラシ等の作成業務の作成の作業において、年間48,333時間を削減（97%減）	10.4万人
ローコードの作成 （マクロ、VBA等）	コード生成による業務時間短縮の実績 775.35時間	9.4万人

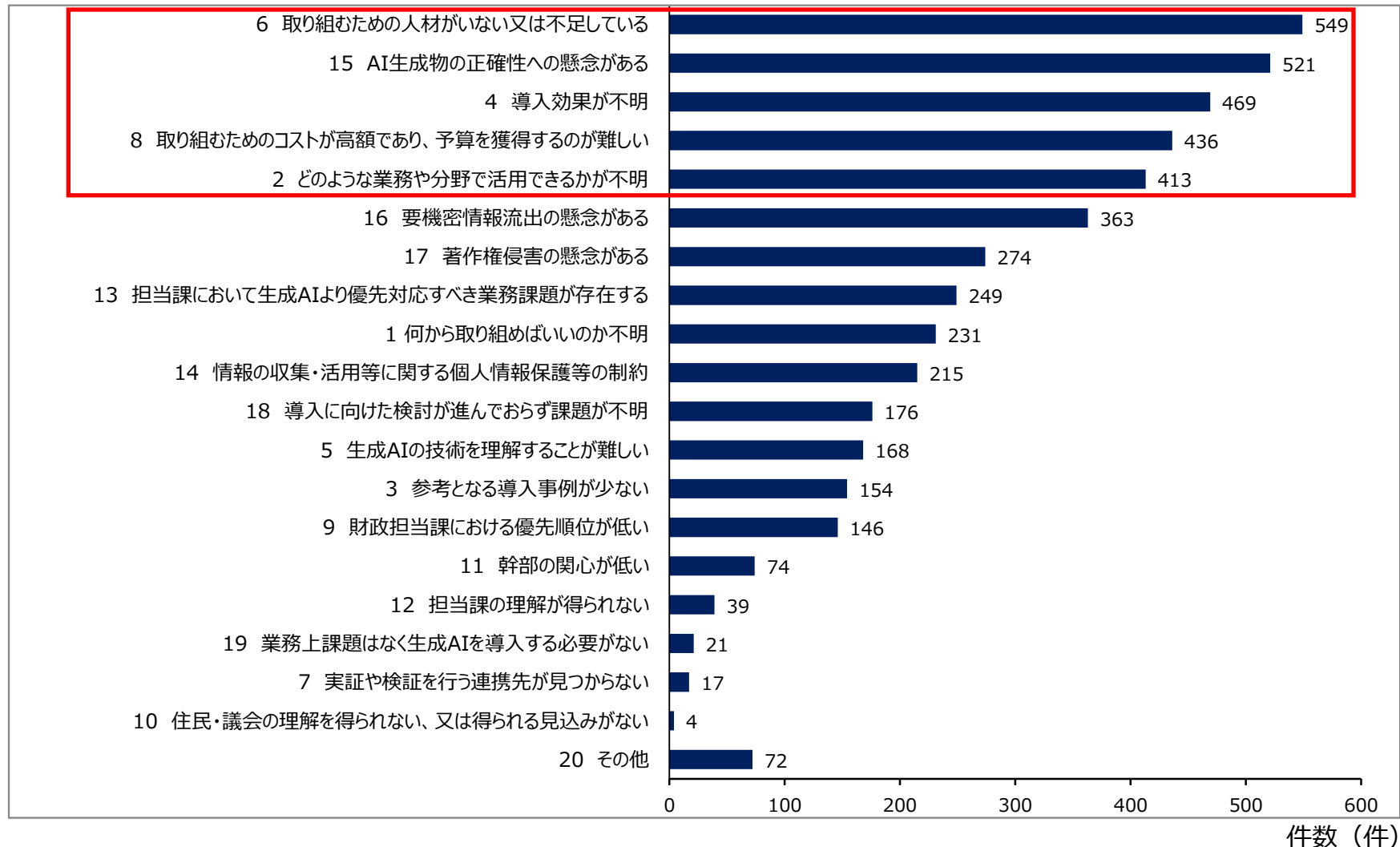
生成AI導入により得られた効果（業務削減時間）の活用方法

- 生成AI導入により得られた効果（業務削減時間）の活用方法は、「住民対応時間の確保など住民サービスの向上」及び「業務プロセス改善、IT導入など内部事務の改善検討・実施」の回答が338件と最も多かった。



生成AIの導入における課題

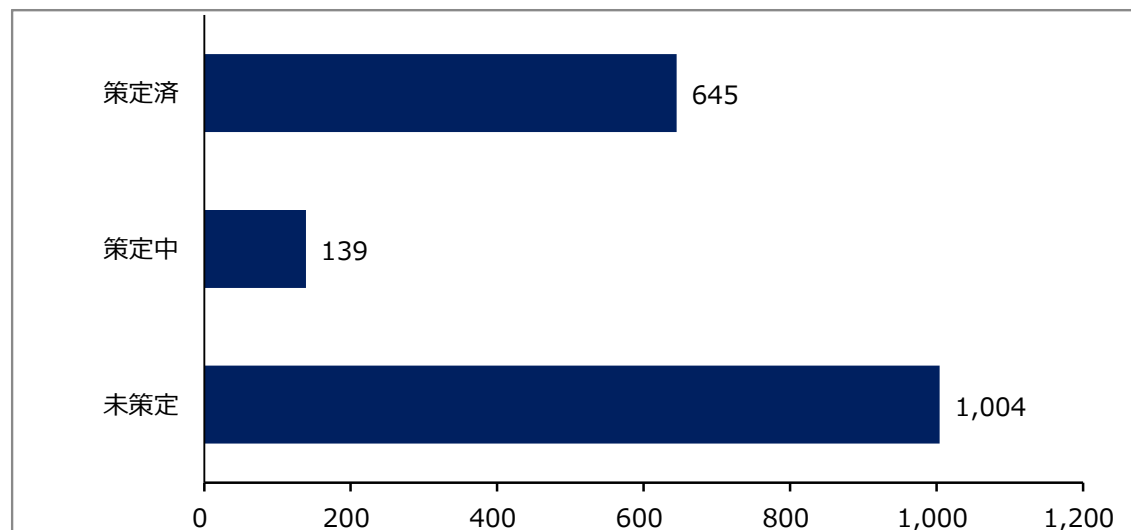
- 生成AIの導入における課題として、人材の確保、信頼性や導入効果、活用可能な業務・分野の理解不足等を挙げている団体が多い。前年度調査（令和5年12月31日現在）から大きな傾向の変化はみられないが、「AI生成物の正確性への懸念がある」「導入効果が不明」という回答数が減り、「取り組むための人材がいらない又は不足している」という回答数が増加したため最多となった。



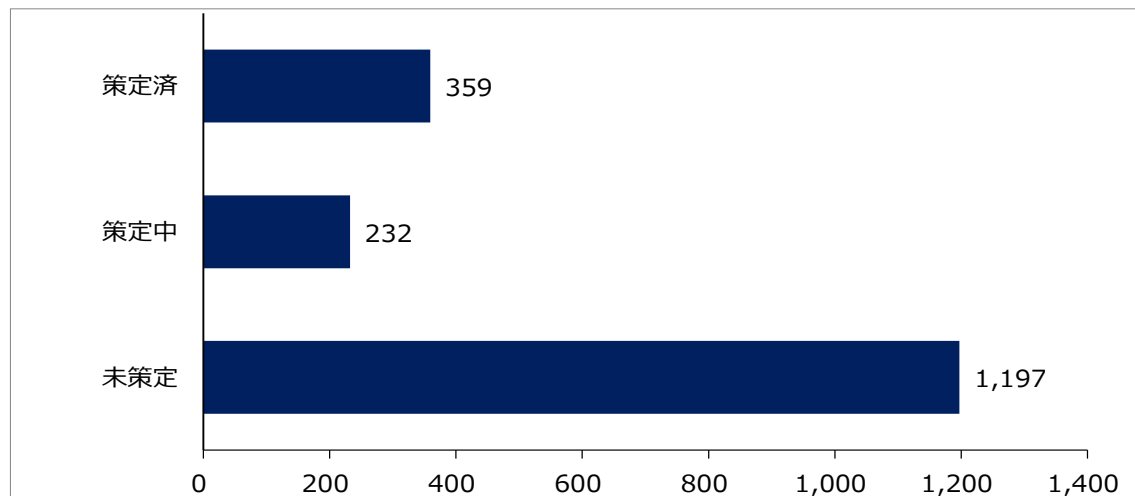
生成A I 利用におけるガイドライン策定状況

- 生成AI利用におけるガイドライン策定状況は、「策定済」は645団体と前回（359団体）と比べて増加したものの、「未策定」が**1,004団体と引き続き最も多い**。

（令和6年12月31日現在）

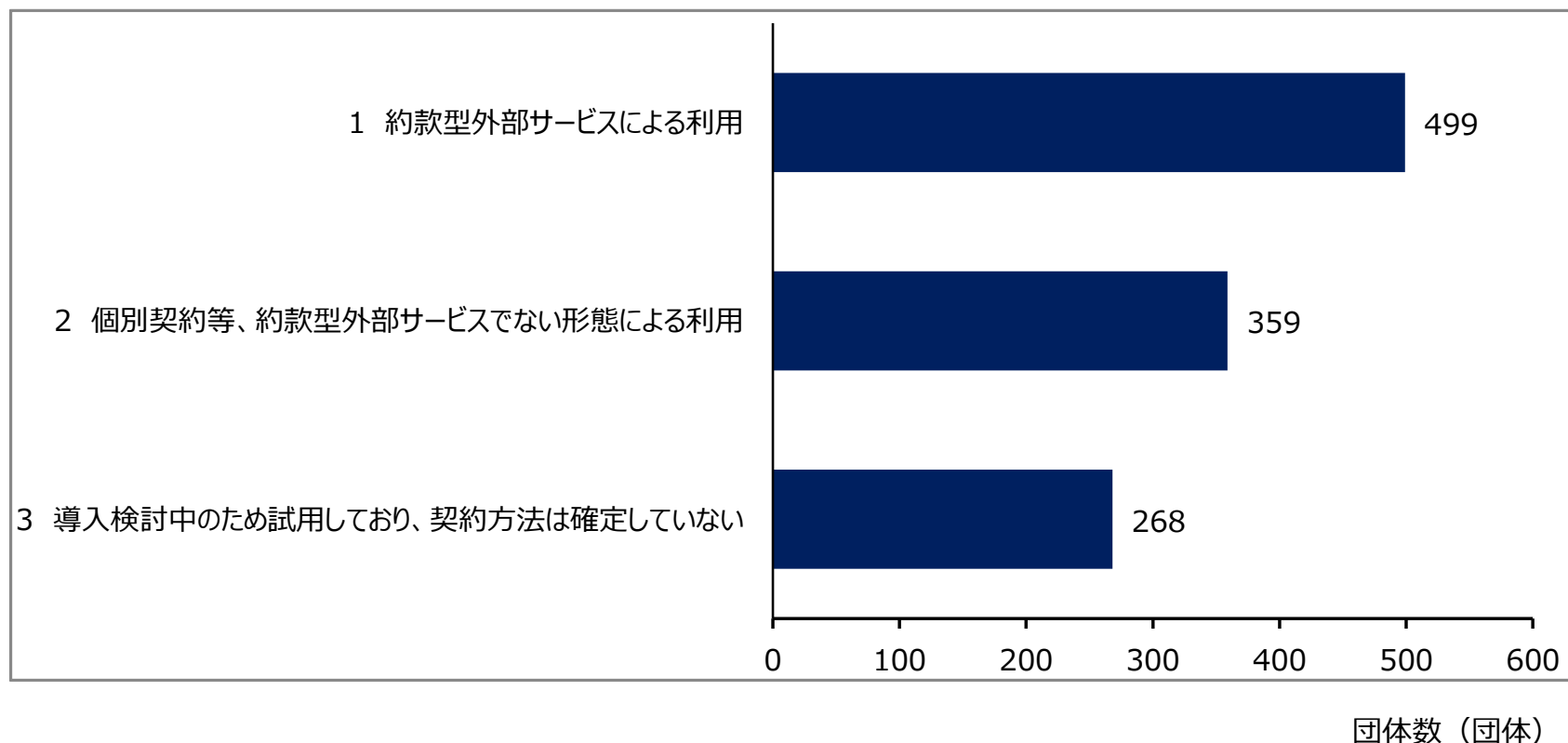


（令和5年12月31日現在）



団体数（団体）

- 導入している生成AIの契約方法は「約款型外部サービスによる利用」が最も多い499団体で、「個別契約等、約款型外部サービスでない形態による利用」は、359団体であった。



※生成A Iを導入済み、実証実験中、導入検討中で生成AIを利用している団体のみ回答。

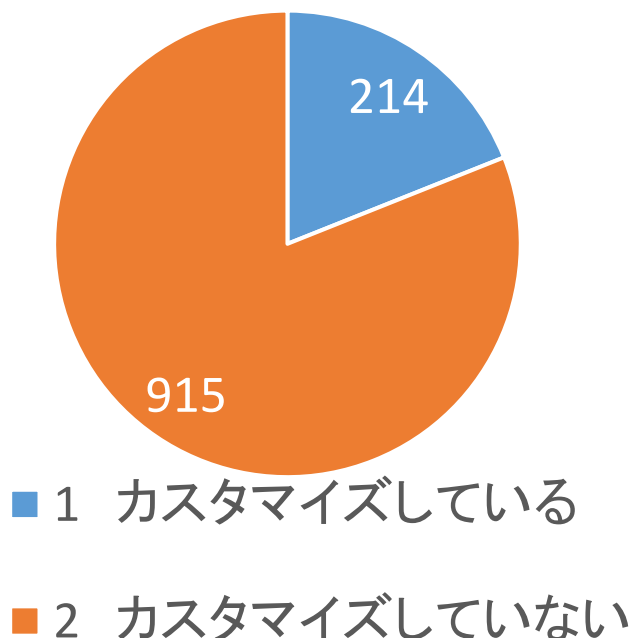
※複数の生成A Iを導入している場合は、生成AIのサービスごとに複数件回答。

※未回答があるため「導入済」「実証実験中」の総数と一致しない。

自治体において導入している（実証実験も含む）生成AIのカスタマイズ

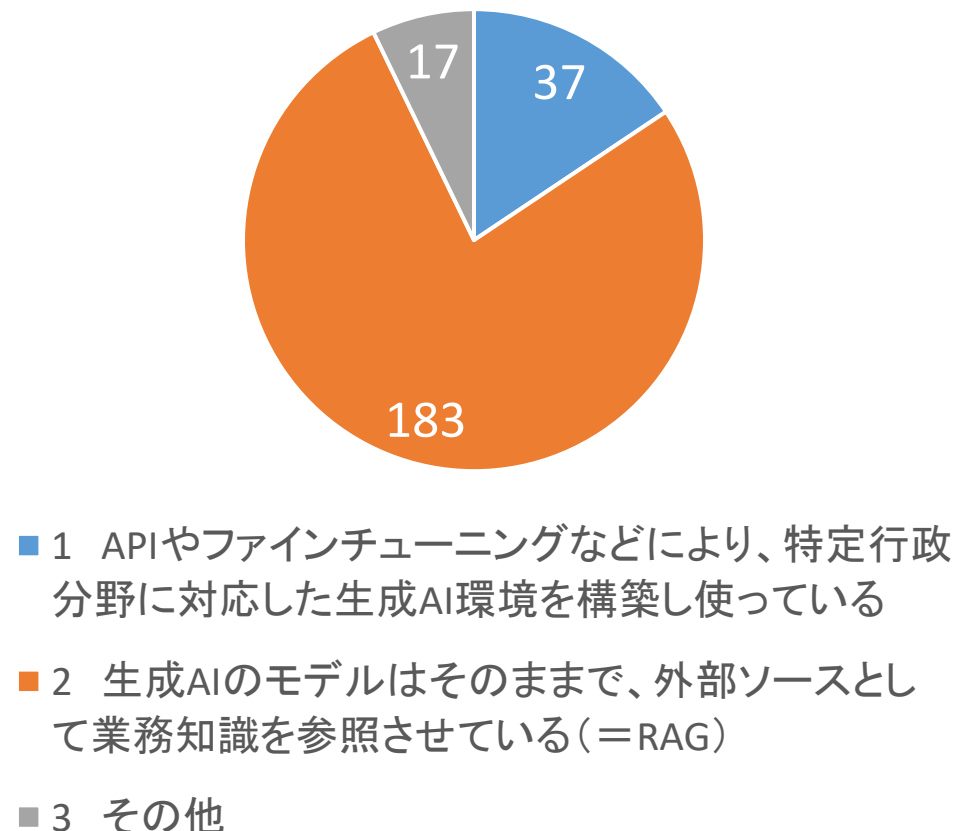
- 導入している生成AIのカスタマイズ状況は、カスタマイズしている団体数が214団体、カスタマイズしていない団体数が915団体であった。
- うち導入しているカスタマイズ方法は、「生成AIのモデルはそのまま、外部ソースとして業務知識を参照させている（＝RAG）」が183件と最も多かった。

カスタマイズ状況（件数）

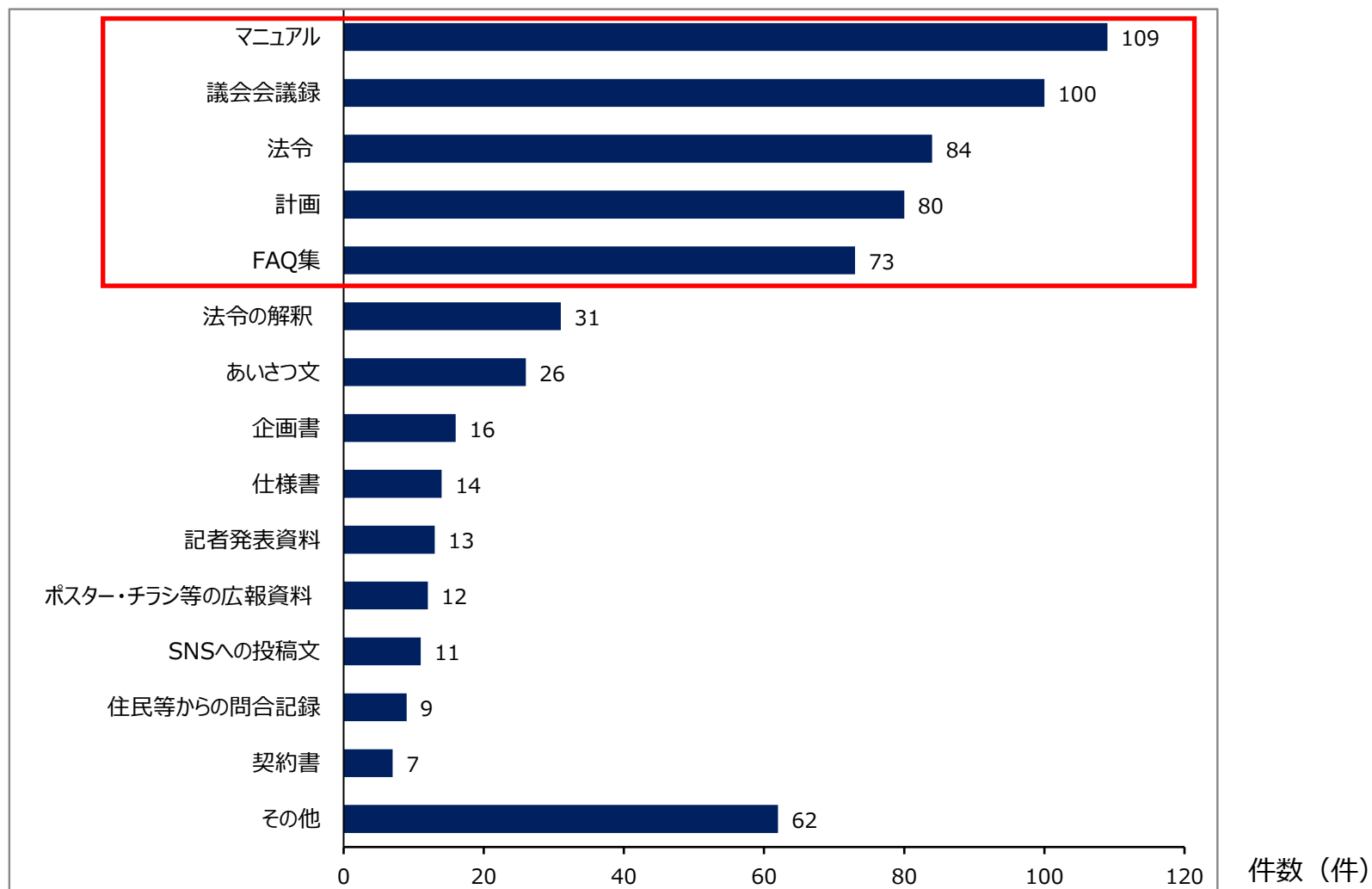


カスタマイズ方法（件数）

件数（件）

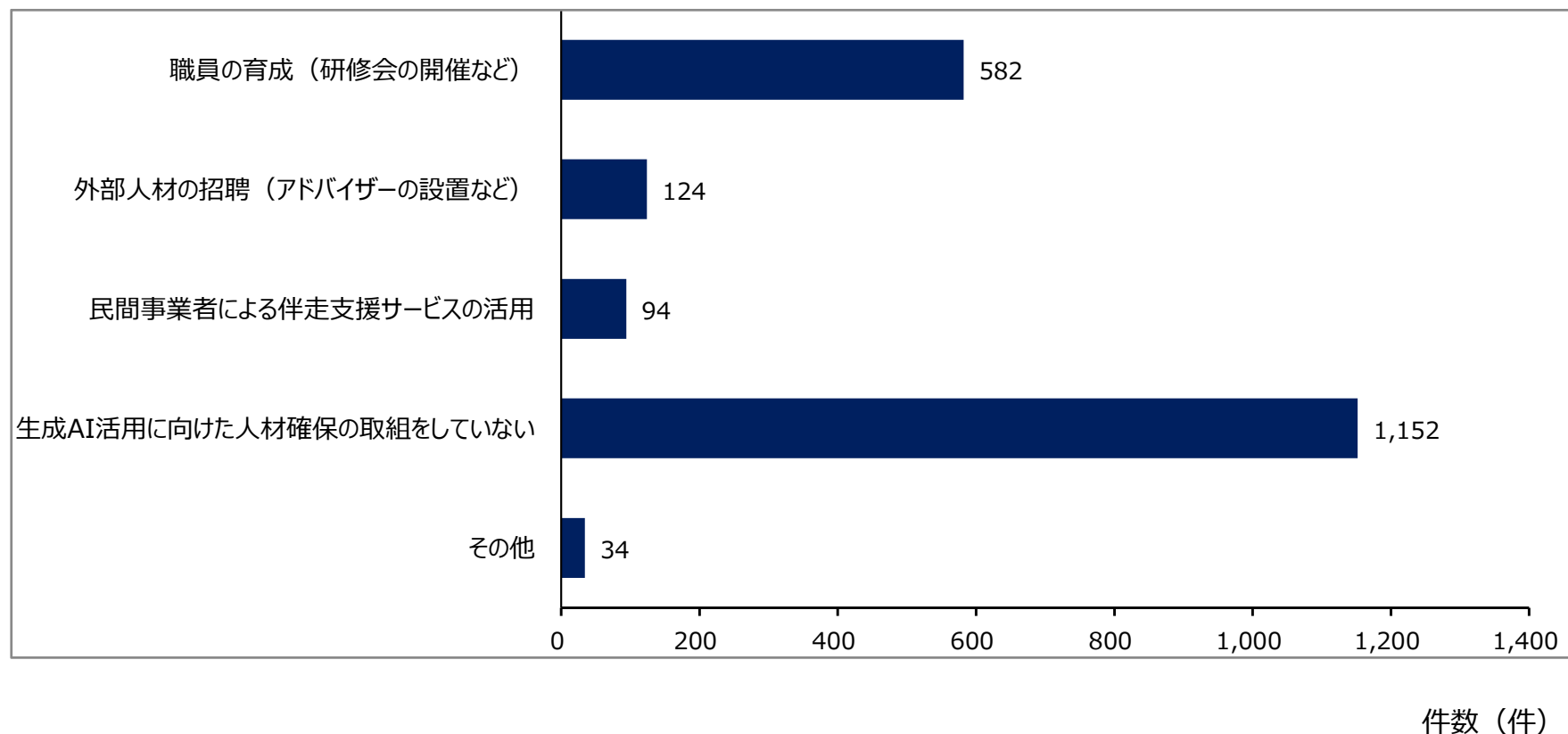


- 生成AIのカスタマイズ対象とした業務知識は、回答の多い順に「マニュアル」、「議会議事録」、「法令」、「FAQ集」となり、これらは70件以上の事例があった。



生成AIの活用に向けた人材確保の取組

- 生成AIの活用に向けた人材確保の取組は、「生成AI活用に向けた人材確保の取組をしていない」が最も多かったものの、実施している取組としては「職員の育成（研修会の開催など）」が最も多かった。



參考資料

第2回WGにおける主な議論内容

①生成AIの利用について

＜主な発言要旨＞

- 生成AIが利用者の求めている回答を高精度で出力するためには、背景情報を適切に入力する必要があるが、その方法が課題ではないか。
- 利用者ごとに有する知見は異なるため、生成物が独創的なアイデアなのか、ハルシネーションなのか、判断がつかない場合も想定されるのではないか。
- RAG等により生成AIに思考の過程を明示させることや分かりやすいUIの導入等により、利用者が求める回答を出力させるために必要な生成AIとのコミュニケーションを取れるようにすることが考えられる。
- フランスの学術論文においては、ヘーゲルの弁証法を用いて論理を構成するケースがあり、これを用いて生成AIを構築すれば、人間の脳の構造に近づくようなところもあるのではないかと感じている。人間の道徳性とAIの道徳性についても研究が進んでいる。信頼性の高いLLMを開発していくうえでも、論理学や哲学的な視点が必要になると感じている。
- 本団体では、開発部門が他団体や民間企業での事例等を調査の上、自団体でも有用と考えられる機能から導入を進めている。
- 生成AIの導入当初は、試しに試ってみるという視点から、庁内における優良事例の収集を行った。開発部門から有用と思われる機能を組み込んでアプリをリリースしているものの、現在、職員が抱えている課題やニーズを収集しており、それらに対応する機能を増やしていきたいと考えている。
- 本団体で活用事例を収集したところ、生成AIを用いてペルソナを作成している例があり、他部署においても有用と考えられたため、横展開を図ったという経緯である。また、ペルソナを作成するにあたっては、本団体の情報は読み込ませていない。一般的な生成AIが学習している情報で、ペルソナを作成している。
- 海外製の生成AIが学習している海外の情報を基にペルソナが作成され、そのペルソナが自治体の施策検討に活用されることで、立案される施策が日本の実情に合わないものとなるリスクもあるかと思う。
- 様々な活用方法を試し、やってみたら上手いといったという柔軟な取扱いを進めることは良いことだと思う。
- 職員が直接プロンプトを入力しなくても生成AIを簡単に活用できる業務用アプリの取組等ノウハウが横展開されることで、自治体における生成AIの活用が加速すると考える。
- 国が一括調達したサービスを各自治体に提供し費用面の課題を解消する、自治体間でナレッジを共有できるプラットフォームを開発する等の取組などが考えられるのではないか。

第2回WGにおける主な議論内容

①生成AIの利用について（続き）

- 本団体においては、議会の答弁案の作成や、ゆるキャラの名前のアイデア出し、Excelの関数やマクロのコードの作成・修正、市民意見への回答、計画書の要約等、様々なシーンで生成AIを活用している。一方で、一定数の職員は生成AIを使っておらず、活用状況が二分化している。より幅広い職員の生成AIの活用につなげるとともに、既に生成AIを活用している職員の更なる活用を促すため、基礎的な研修と応用的な研修に分けて研修を実施する等の工夫を行っている。
- 専門用語が使われる場合、通訳よりも生成AIによる翻訳の方が有用な場合もある。

②要機密情報・個人情報の取り扱いについて

<主な発言要旨>

- 氏名等を黒塗りにしても、元の情報を削除したわけではなく、明らかに元の情報と容易照合可能であって、個人情報に該当する。基礎自治体の持つ情報は、ほとんどが個人情報を含むものであり、また、個人情報の該当性は提供元で判断するため、個人情報を生成AIで取り扱うことを一律に禁止する場合、自治体は生成AIを十分に活用できない。現実的には個人情報を生成AIで取り扱うようにする必要がありと考えている。生成AIを含むSaaS型サービスでも、機密性2以上の情報を取扱うことを前提に検討すべき。
- 本団体では、安全性を確保した上で市長の許可で機密性2以上の入力を可能にする規定を置いている。
- プライベートな領域に格納した庁内ナレッジに基づいて、回答を生成するような、要機密情報が外部に流出しない仕組みであれば、生成AIで個人情報を取扱っても問題は生じないとする。
- 本団体では、既に生成AIアプリを私用のスマホにインストールしている職員も多く、シャドーAIの懸念もあったことから、業務用の生成AIを導入した。
- 非約款型で、入力データが学習に利用されず、十分なセキュリティ対策が講じられている生成AIであれば、機密性の高い情報の取扱いを可能とする余地もあると考える。法律上も、機密性2以上の情報の取扱いが禁止されているものではないと理解している。
- 本団体では、要機密情報の生成AIへの入力ルールの緩和については、国の動向を注視しているところであり、国に先んじた対応をすることまでは進んでいない。高機能なLLMがオープンソースとして公開され、ローカル環境で完結する構成で生成AIを実装できるようになれば、検討を進められる可能性がある。ナレッジを共有できるプラットフォームが整備されると良いのではないかと考える。
- 本団体では、生成AIへの個人情報の入力に係る安全性については、入力データの学習利用の有無、裁判所の管轄国、生成AIに入力されたデータの保存場所等技術的な要件を踏まえて、案件ごとに判断をしている。また、行政処分以外でリスクアセスメントの対象となる「その他市民生活に重大な影響を与えるおそれがあるもの」については、例えば具体的に申し上げると、要綱に基づく給付や、井戸水の水質検査、避難勧告等行政処分には該当しないものであっても、市民生活への影響が大きいものを想定している。

2024年7月以降、AI制度研究会¹⁾を計7回開催。計15の研究者、事業者等からのヒアリングを含む議論、パブリックコメントを経て中間とりまとめを作成。

背景

- AIは我が国の発展に大きく寄与する可能性がある一方、**様々なリスクが顕在化**。
- AIに対する不安の声が多く、諸外国と比べても**開発・活用が進んでいない**との指摘。
 - ▶ AIの透明性など、**適正性を確保し、AIの開発・活用を進める**必要がある。

基本的な考え方

■ イノベーション促進とリスク対応の両立（Ⅱ.3.）

- 研究開発支援、人材育成、データや計算資源の整備などイノベーションの促進
- 法令とガイドライン等の適切な組合せ
- OECD原則、広島AIプロセス国際指針等の共通的な指針等と個別の既存法令の活用



■ 国際協調（Ⅱ.4.）

- AIガバナンスの形成に向けて議論をリード
- 国際整合性・相互運用性の確保



具体的な制度・施策の方向性

■ 全般的な事項（Ⅲ.1.）

- **政府の司令塔機能の強化、戦略の策定**
 - ・ 全体を俯瞰する**司令塔機能強化**
 - ・ AIの安全・安心な研究開発・活用のための**戦略（基本計画）の策定**
- **安全性の向上等**
 - ・ **国による指針（広島AIプロセス準拠）の整備、事業者による協力**
 - ・ **国による調査・情報収集、事業者・国民への指導・助言、情報提供等**

AIの研究開発・実装が最もしやすい国を目指す

速やかな法制度化が必要
世界のモデルになるような制度

■ 政府等による利用（Ⅲ.2.）

- 適正なAI政府調達・利用 等

■ 基盤サービス等における利用（Ⅲ.3.）

- 各業法等による対応 等

1) 官房長官が議長、全閣僚が構成員となっている「統合イノベーション戦略推進会議」の下に「AI戦略会議」を設置。

2) 上記の政策を講じた上で、今後のリスク対応のため引き続き制度の検討を実施すべき。

2. 令和6年度の更新内容

2-3. 生成AIに関する記載の追加

第30回AIネットワーク社会推進会議・
第26回AIガバナンス検討会合同会議資料
(令和7年3月7日)

【更新内容の詳細】

② 生成AIによるリスクを追加

※主たる更新箇所を抜粋して表示

1) 人間中心⁴⁾

各主体は、AIシステム・サービスの開発・提供・利用において、後述する各事項を含む全ての取り組むべき事項が導出される土台として、少なくとも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すべきである。また、AIが人々の能力を拡張し、多様な人々の多様な幸せ（well-being）の追求が可能となるように行動することが重要である。⁴⁾

① 人間の尊厳及び個人の自律⁴⁾

- ◇ AIが活用される際の社会的文脈を踏まえ、人間の尊厳及び個人の自律を尊重する⁴⁾
- ◇ 特に、AIを人間の脳・身体と連携させる場合には、その周辺技術に関する情報を踏まえつつ、諸外国及び研究機関における生命倫理の議論等を参照する⁴⁾

⋮

⑥ 持続可能性の確保⁴⁾

- ◇ AIシステム・サービスの開発・提供・利用において、ライフサイクル全体で、地球環境への影響も検討する（特に、生成AIなど計算量の多いAIシステムにおいては、モデルの軽量化や目的に応じたモデルの使い分け等の対策を講じる）[↓]

2) 安全性⁴⁾

各主体は、AIシステム・サービスの開発・提供・利用を通じ、ステークホルダーの生命・身体・財産に危害を及ぼすことがないようにすべきである。加えて、精神及び環境に危害を及ぼすことがないようにすることが重要である。[↓]

① 人間の生命・身体・財産、精神及び環境への配慮⁴⁾

- ◇ AIシステム・サービスの出力の正確性を含め、要求に対して十分に動作している（信頼性）⁴⁾
- ◇ 様々な状況下でパフォーマンスレベルを維持し、無関係な事象に対して著しく誤った判断を発生させないようにする（堅牢性（robustness））⁴⁾
- ◇ AIの活用又は意図しないAIの動作によって生じる権利侵害の重大性、侵害発生の可能性等、当該AIの性質・用途等に照らし、必要に応じて定期的かつ客観的なモニタリング及び対処も含めて人間がコントロールできる制御可能性を確保する⁴⁾

⋮

② 適正利用⁴⁾

- ◇ 主体のコントロールが及ぶ範囲で本来の目的を逸脱した提供・利用²⁰⁾により危害が発生することを避けるべく、AIシステム・サービスの開発・提供・利用を行う⁴⁾
- ◇ マルチモーダルな生成AIを中心とするAIシステム・サービスの生成物については、比較的容易により精巧な生成物の生成が可能となるため、その精巧さにより誤解や偏見等を助長する可能性があることや、他者の知的財産権等を侵害する可能性があること等にも留意しつつ、その利用に際し人間の判断を介在させる等²¹⁾の対策を講じる²²⁾⁴⁾

⋮

③ 適正学習²³⁾⁴⁾

- ◇ AIシステム・サービスの特性及び用途を踏まえ、学習等に用いるデータの正確性・必要な場合には最新性（データが適切であること）等を確保する⁴⁾
- ◇ 学習等に用いるデータの透明性の確保、法的枠組みの遵守、AIモデルの更新等を合理的な範囲で適切に実施する⁴⁾
- ◇ 権利侵害複製物等の違法なコンテンツ²⁴⁾や情報等を学習データに含めないこと等に留意する²⁵⁾

【更新内容の詳細】

③ 生成AIに関して配慮すべき事項を追加

※主たる更新箇所を抜粋して表示

B. 本編「第 2 部」の「共通の指針」の解説

ここでは、本編「第 5 部 AI 利用者に関する事項」では触れられていないが、本編「第 2 部」の「共通の指針」のうち、AI 利用者にとって特に重要なものについて、具体的な手法を解説する

[本編の記載内容（再掲）] ※ 柱書のみ抜粋

1) 人間中心

各主体は、AI システム・サービスの開発・提供・利用において、後述する各事項を含む全ての取り組むべき事項が導出される土台として、少なくとも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すべきである。また、AI が人々の能力を拡張し、多様な人々の多様な幸せ（well-being）の追求が可能となるように行動することが重要である。

● 「⑥持続可能性の確保」関連

[関連する記載内容]

➤ AI システム・サービスの開発・提供・利用において、ライフサイクル全体で、地球環境への影響も検討する

[具体的な手法]

➤ 目的に応じて環境への影響が小さい軽量なモデルを活用するなど、モデルを適切に使い分ける

[参考文献]

- 総務省「令和 3 年版 情報通信白書」（2021 年 7 月）

<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（案）>

各府省における生成AIリスクの管理のための枠組みの整備

「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」（案）（デジタル庁）を基に事務局において作成

各府省は、**生成AIのリスクを軽減するための方策を把握し、職員種別ごとに適切なリスク対策を実施して調達を行い、利活用を推進。**

※前提として、各種法令や「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」、「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」等既存のガイドラインも遵守することが必要。

各府省の職員の種別

実施すべき生成AIのリスクを軽減するための方策の例

①AI統括責任者

- 各府省内における**AIガバナンスの確保**

- 各府省における**生成AIの利活用ルール（※１）**の策定、**生成AIシステムのリスクケース対応に関わる手順書（※２）**の策定
※１ **ガイドラインにおいてひな形を提示** ※２ **ガイドラインにおいて考え方を提示**

【企画時】・生成AIを使って何を実現・解決したいのか**目的を明確**するとともに、**適切な目標設定**

- 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

※ リスク分析の際、高リスクの可能性のある生成AIシステムについては、AI統括責任者が先進的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。

- デジタル庁が実施する**統括監理の際に、目的、環境・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**

②企画者

（生成AIを企画・調達するチームの職員）

【調達時】・事業者の**AIガバナンス体制や生成AIシステムの安全性等について、調達への応募者に対し求める事項**をガイドライン別紙の**「調達チェックシート」**及び**「契約チェックシート」**を参考に検討し、**仕様書及び契約書に盛り込む。**

- 総合評価方式や企画競争方式を採用する場合、**求める事項について、必要に応じ必須項目又は加点項目として盛り込む**

【リリース前】

- 調達する**生成AI システム・サービスの利活用ルールの策定**

- 受け入れテスト**を実施し、**当初の目標を達成可能な品質が確保されていること、不適切な生成やバイアスの有無をチェック**

③開発者

（事業者へ委託される場合が多いため、開発者に求める事項を、調達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）

④提供者

（AIシステムを提供・運営する職員）

- 適切な目的で 生成AI システム・サービスが利用されているかを**定期的に検証**

- 最新のリスク及びそれに対応するために提供の各工程で留意すべき**最新の動向を確認し、脆弱性への対応等を行うこと**

- サービス規約及びプライバシーポリシーの明示**

⑤利用者（各行政分野において生成AIを利用する職員）

- 各府省における**生成AIシステムの利活用ルール**及び**生成AIシステム・サービスごとの利活用ルールの遵守**

＜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（案）＞ 生成AIのリスク判断をするための高リスク判定シートにおけるリスク判定ロジック

『「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（案）」に対する意見募集について（令和7年3月28日）』公表資料（デジタル庁）より抜粋

C. 要機密情報や個人情報の学習等の有無

- ①機密性2情報または個人情報生成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情報または個人情報を取扱わない
- ④企画時点で未定

B. 生成AI利活用業務の性格

- 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

A. 利用者の範囲・種別

- 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活用（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

D. 出力結果の政府職員による判断を経た利活用

- 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

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

