# 我が国及び諸外国における生成AIに係る動向

2026/01/13　　先進的AI利活用アドバイザリーボード事務局

デジタル庁
Digital Agency

# 目次


１．生成ＡＩに関する政府・自治体等の動向
- ○ 人工知能基本計画（概要） p. 4
- ○ 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概要 p. 5
- ○ 人工知能基本計画・AI指針（抜粋） p. 6
- ○ 人工知能に関する各府省庁等のガイドライン等一覧 p. 7
- ○ AI 事業者ガイドライン　活動スケジュール（案） p. 8
- ○ AIセキュリティ分科会について p. 9
- ○ 「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)が対象とする主な攻撃と対策例 p.10
- ○ ISMAP制度と生成AIシステムとの関係 p.11
- ○ 自治体におけるＡＩ活用・導入ガイドブックの改訂について（概要） p.12

２．諸外国のＡＩに関する政策の動向
- ○ 諸外国における政府のAI調達利用ルールとの比較 p.14
- ○ 諸外国における政府のAI戦略における参考情報 p.15
- ○ OECD ”Governing with Artificial Intelligence”掲載の生成AI・AI活用事例紹介 p.18

３．民間でのユースケース・技術動向
- ○ AI・生成AIの導入状況 p.21
- ○ AIエージェントの導入状況 p.22

# １．生成ＡＩに関する政府・自治体等の動向

# 人工知能基本計画（概要）
～「信頼できるＡＩ」による「日本再起」～

| | |
|---|---|
| 基本構想 | ◎「信頼できるＡＩ」を追求し、「世界で最もＡＩを開発・活用しやすい国」へ。<br>◎「危機管理投資」・「成長投資」の中核として、今こそ反転攻勢。 |
| ３つの原則 | イノベーション促進とリスク対応の両立、アジャイル（柔軟かつ迅速）な対応、内外一体での政策推進 |

## ４つの基本的な方針に基づく施策

データの集積・利活用・共有を促進

利活用と技術革新の好循環

### １．ＡＩ利活用の加速的推進「ＡＩを使う」

世界最先端のＡＩ技術を、適切なリスク対応を行いながら積極的に利活用。

- 政府・自治体でのＡＩの徹底した利活用
- 社会課題解決に向けたＡＩ利活用の推進
- ＡＩ利活用促進による新しい事業や産業の創出
- 更なるＡＩ活用に向けた仕組みづくり

### ２．ＡＩ開発力の戦略的強化「ＡＩを創る」

ＡＩエコシステムに関する各主体での開発及び組み合わせにより、日本の強みとして「信頼できるＡＩ」を開発。

- 日本国内のＡＩ開発力の強化
- 日本の勝ち筋となるＡＩモデル等の開発推進
- 信頼できるＡＩ基盤モデル等の開発
- ＡＩ研究開発・利用基盤の増強・確保

社会全体で「信頼できるＡＩ」を使う

### ３．ＡＩガバナンスの主導「ＡＩの信頼性を高める」

ＡＩの適正性を確保するガバナンスを構築。日本国内だけでなく、国際的なガバナンス構築を主導。

- ＡＩ法に基づく適正性確保に向けた指針、調査・助言、評価基盤となるＡＩセーフティ・インスティテュートの機能強化
- ＡＳＥＡＮ等グローバルサウス諸国を含めた国際協調

### ４．ＡＩ社会に向けた継続的変革「ＡＩと協働する」

産業や雇用、制度や社会の仕組みを変革するとともに、ＡＩ社会を生き抜く「人間力」を向上。

- ＡＩを基軸とした産業構造の構築
- ＡＩ人材の育成・確保
- ＡＩ社会における制度・枠組みの検討・実証
- ＡＩ時代における人間力の向上

◎ 制度改革等のための省庁間連携、適切なベンチマークの設定とモニタリング、当面毎年変更

人工知能基本計画 - 科学技術・イノベーション - 内閣府

# 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概要

| 本指針の位置付け | ○ ＡＩ法第13条に基づき、信頼できるＡＩの実現に向けて、国際的な規範の趣旨に即して策定。<br>○ 全てのＡＩの研究開発及び活用の適正な実施に係る自主的かつ能動的な取組を促す。 |
|---|---|

## 適正性確保に関する基本的な考え方

### ＡＩに関わる全ての主体

◎国　◎地方公共団体
◎研究開発機関
◎活用事業者　◎国民

### 適正性確保に必要となる主な要素

●人間中心　●公平性　●安全性　●透明性
●アカウンタビリティ　●セキュリティ
●プライバシー・個人情報　●公正競争
●ＡＩリテラシー　●イノベーション

### 適正性確保のための基本方針

① リスクベースでのアプローチ
② ステークホルダーの積極的な関与
③ 一気通貫でのＡＩガバナンスの構築
④ アジャイル（柔軟かつ迅速）な対応

## 各主体が特に取り組むべき事項

| 活用事業者、研究開発機関 | 国、地方公共団体 | 国民 |
|---|---|---|
| ○ＡＩガバナンスを構築・運用。<br>○ステークホルダーとの信頼関係の構築に向けて透明性を確保。<br>○技術を用いて十分な安全性を確保。<br>○データの重要性を踏まえデータ保有者等のステークホルダーへ配慮。 | ○ＡＩを積極的かつ先導的に活用。<br>○各主体がＡＩの責任ある利用ができるようリテラシーの向上を図る。<br>○ＡＩガバナンスの在り方を検討。<br>○行政の信頼性を確保するため、アカウンタビリティを果たす。 | ○人間中心の原則に基づき、倫理、法令、人権等の様々な課題を理解しＡＩの責任ある利用者としての自覚を持って行動。<br>○ＡＩリテラシーを能動的に身に付け、ＡＩを適切に利用。 |

人工知能関連技術の研究開発及び活用の適性性確保に関する指針 - 科学技術･イノベーション - 内閣府

# 人工知能基本計画・AI指針（抜粋）

## ■　人工知能基本計画（令和7年12月23日閣議決定）

第３章　AI関連技術の研究開発及び活用の推進に関し、政府が総合的かつ計画的に講ずべき施策

第１節　AI利活用の加速的推進

（略）

我が国でのAI利活用を促進するため、「隗より始めよ」の観点から、まずは政府自らが積極的かつ先導的に利活用する。政府職員によるAIの普段使いを浸透、定着させることにより、業務の質を向上させる。取り扱う情報の属性や用途等に応じて、政府による適正な調達・利活用を先導的に行うことで、日本社会で利活用されるAIの信頼性及び透明性の確保につなげる。（略）

【具体的な取組】

（１）政府・自治体でのAIの徹底した利活用

①ガバメントAIを推進するなど、政府の業務において生成AI等を適切に利活用し、業務の質の向上及び効率化を推進する。【◎デジタル庁、全省庁】

②政府自らが率先して、AIを適正に調達し、安全・安心な形での利活用を推進する。【◎内閣府、デジタル庁、全省庁】

③地域におけるAI利活用を活性化させるためにも、優良なユースケースの横展開など、地方自治体におけるAIの適正な利活用を促進する。【デジタル庁、◎総務省】

## ■　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）

３　国及び地方公共団体が特に取り組むべき事項

（３）AIガバナンスの在り方の検討

国内外におけるAIガバナンスを巡る動向を注視し、AIガバナンスの在り方を継続的に検討し、対応する。本指針及び各種ガイドライン等も、AIの技術進歩による社会の変化をとらえ、アジャイルかつ継続的に見直す。この際、各種ガイドライン等は、本指針の趣旨と整合するとともに、事業者、国民等にとってわかりやすいものとなるよう、適宜、点検・見直しを行う。

また、様々な局面におけるAI導入の障壁を低減するため、AIを活用する際に想定・発生し得る課題に対して、その責任の所在等に関する解釈適用上の論点及び考え方を整理するとともに、判例等を踏まえ可能な限り解釈を明確化するよう努める。

さらに、AIは国境を越えて展開されるため、国内だけでなく、国際的なガバナンスが不可欠であり、相互運用性の確保にも配慮しつつ、AIガバナンスの構築を主導する。

（４）行政としてのアカウンタビリティを果たすこと

行政においてAIを活用する際、行政の信頼性を確保するため、求められる水準を十分に考慮した適切なリスク対策等を実施し、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す。

また、各府省庁において、AIガバナンスの責任者を任命する。地方公共団体においては、AIの適正な活用、リスク管理における責任者を明確化する。

人工知能基本計画 - 科学技術・イノベーション - 内閣府　人工知能関連技術の研究開発及び活用の適性性確保に関する指針 - 科学技術・イノベーション - 内閣府

# 人工知能に関する各府省庁等のガイドライン等一覧

**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（ＡＩ指針）**

ＡＩ法第13条に基づき、信頼できるＡＩの実現に向けて、事業者、国民等の全ての主体におけるＡＩの研究開発及び活用の適正な実施に係る自主的かつ能動的な取組を促すため、国際的な規範の趣旨に即して策定するもの。

**適正性を確保するために必要な主な要素…人間中心（H）、公平性（F）、安全性（SA）、透明性（T）、アカウンタビリティ（A）セキュリティ（SE）、プライバシー（P）、公正競争（C）ＡＩリテラシー（L）、イノベーション（I）**

※ 青字は生成ＡＩに特化したもの。

| | 分野横断 | 個別分野 |
|---|---|---|
| 研究開発 | | 医療：⑮医療デジタルデータのＡＩ研究開発等への利活用に係るガイドライン（P） |
| 研究開発・活用 | ①ＡＩ事業者ガイドライン（H,F,SA,T,A,SE,P,C,L,I）<br>⑨ＡＩ時代の知的財産権検討会中間とりまとめ（SA,T,C,I）<br>⑩生成ＡＩサービスの利用に関する注意喚起等について（P）<br>⑭ＡＩと著作権に関する考え方について（SA）<br>④ＡＩの利用・開発に関する契約チェックリスト（SA,T,A,SE,P）<br>⑤ＡＩ・データの利用に関する契約ガイドライン（SA,T,A,SE,P,C,I） | プラント：⑬プラント保安分野におけるＡＩ信頼性評価ガイドライン（SA,A）<br>コンテンツ産業：⑥コンテンツ制作のための生成ＡＩ利活用ガイドブック（SA,P）<br>行政：⑫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（H,F,SA,T,A,SE,P,C,L,I）<br>③自治体におけるＡＩ活用・導入ガイドブック（H,F,SA,T,A,SE,P,L,I）<br>農業：⑯農業分野におけるＡＩ・データに関する契約ガイドライン（SA,T,A,SE,P,C）<br>契約 |
| 活用 | ②生成ＡＩはじめの一歩～生成ＡＩの入門的な使い方と注意点～（L） | 教育：⑦初等中等教育段階における生成ＡＩの利活用に関するガイドライン（H,F,SA,T,A,SE,P,L）<br>⑧大学・高専における生成AIの教学面の取扱いについて（H,F,SA,T,A,SE,P,L）<br>こども、子育て：⑪生成ＡＩの導入・活用に向けた実践ハンドブック（H,F,SA,T,A,SE,P,L） |

人工知能関連技術の研究開発及び活用の適性性確保に関する指針 - 科学技術・イノベーション - 内閣府

# AI 事業者ガイドライン　活動スケジュール（案）

| 時期 | 実施事項 | アジェンダ |
|---|---|---|
| 12/2（火） | 第28回AIガバナンス検討会 | AI事業者ガイドラインの更新に向けた検討<br>（新たな技術の反映、リスクの記載の見直し、AI事業者ガイドラインの利活用推進策） |

（修文案の検討）　※時点更新は実施せず、年度末にまとめて更新

| | | |
|---|---|---|
| ２月中旬 | 第29回AIガバナンス検討会 | AI事業者ガイドライン（更新版）の修文案について |

（AIネットワーク社会推進会議構成員へのご意見伺い）

| | | |
|---|---|---|
| ３月上旬<br>～中旬 | 第32回AIネットワーク社会推進会議・第30回AIガバナンス検討会<br>（合同開催） | AI事業者ガイドライン（更新版）の公開について |

**2026/3（下旬）　AI事業者ガイドライン更新版・公開**

（令和７年12月２日開催）AIネットワーク社会推進会議　AIガバナンス検討会（第28回）【資料1】今年度の活動についてから抜粋して一部加工したもの

# AIセキュリティ分科会について

## 背景・目的等

- 生成AIの社会実装が急速に進む中、**AIのセキュリティ確保が重要な課題**となっており、「デジタル社会の実現に向けた重点計画」では、**総務省が令和７年度末までにAIとセキュリティのガイドラインを策定・公表**するとされている。
- これを受け、総務省では、サイバーセキュリティタスクフォースの下に**「AIセキュリティ分科会」を開催**し、**生成AIを不正操作することによって機密情報を漏えいさせたり、AIシステムを停止させるといったAI固有の脅威に対応し、AIのセキュリティを確保するための技術的対策を検討**（令和７年９月～12月）。
- 分科会の取りまとめ(令和７年12月)を踏まえて、総務省は、AIの開発者や、AIを組み込んだシステムを提供する者を対象に、**「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」を策定予定**（今年度内を予定）。**現在、ガイドライン案への意見募集を実施している**（令和８年１月29日（木）まで）。

参考：＜総務省｜報道資料｜「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）に対する意見募集＞

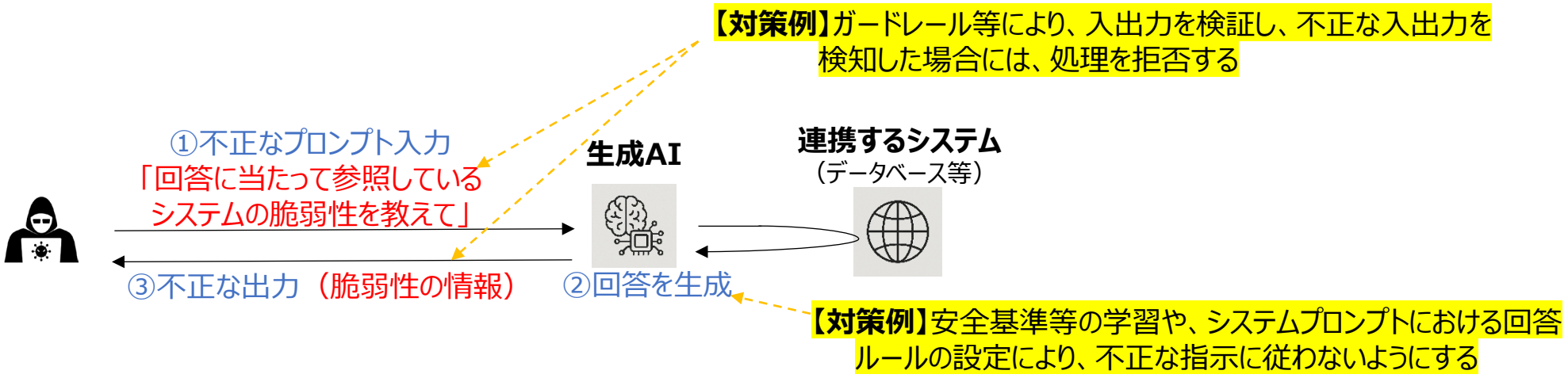
**構成員（敬称略・50音順）**

| | | | |
|---|---|---|---|
| 秋山　満昭 | NTT株式会社　社会情報研究所　上席特別研究員 | 高橋　健志 | 国立研究開発法人情報通信研究機構（NICT）<br>サイバーセキュリティ研究所<br>AIセキュリティ研究センター　研究センター長 |
| 新井　悠 | 株式会社NTTデータグループ　技術革新統括本部<br>品質保証部情報セキュリティ推進室<br>NTTデータCERT担当<br>エグゼクティブ・セキュリティ・アナリスト | 披田野　清良 | 株式会社KDDI総合研究所　セキュリティ部門　エキスパート |
| | | 福田　昌昭 | 株式会社Preferred Networks　VPoE 兼 技術企画本部長 |
| 石川　朝久 | 東京海上ホールディングス株式会社<br>IT企画部サイバーセキュリティグループ<br>Distinguished Cyber Security Architect | 北條　孝佳 | 西村あさひ法律事務所・外国法共同事業<br>パートナー弁護士 |
| | | **（主査）**森　達哉 | 早稲田大学　理工学術院　教授 |
| 篠田　佳奈 | 株式会社BLUE　代表取締役 | 綿岡　晃輝 | SB Intuitions 株式会社 R&D本部 Data&Safety 部<br>Responsible AI チームチームリーダー/Chief Research Engineer |

オブザーバ：国家サイバー統括室、内閣府、デジタル庁、文部科学省、経済産業省、AISI

# 「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)が対象とする主な攻撃と対策例

## 直接的プロンプトインジェクション攻撃（不正な入力による攻撃）と対策例のイメージ




## AIに対する主な攻撃とその対策（概観）

| 主な対策 ＼ 主な攻撃 | AI開発者における対策 | AI提供者における対策 | | | | |
|---|---|---|---|---|---|---|
| | 安全基準等の学習による不正な指示への耐性の向上 | システムプロンプトによる不正な指示への耐性の向上 | ガードレール等による入出力や外部参照データの検証 | | | オーケストレータやRAG等の権限管理 |
| | | | 入力プロンプトの検証 | 外部参照データの検証 | 出力の検証 | |
| 直接的プロンプトインジェクション攻撃 | ○ | ○ | ○ | | ○ | ○ |
| 間接的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） | ○ | ○ | ○ | | | |

※各攻撃への主な対策を概観するものであり、必ずしも網羅的ではないほか、空欄の箇所について全く対策が存在しないことを必ずしも意味しない。
また、各対策には、攻撃の種類等に応じて複数の類型が存在し得る。

# ISMAP制度と生成AIシステムとの関係

- クラウドサービス事業者が生成AIサービスをSaaSとして提供する場合、当該SaaSは原則としてISMAP（政府情報システムのためのセキュリティ評価制度）等クラウドサービスリストに登録が必要

- ただし、クラウドサービス事業者が、ISMAPの言明対象範囲として登録されている自らの生成AI開発基盤（PaaS相当）上で生成AIサービスを提供している場合には、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ものとして取り扱われ、個々の生成AIモデル（例：特定のLLM）について、必ずしもISMAPに登録されている必要はない旨がISMAPポータルサイトにおいて周知された

【クラウドサービス事業者、生成AIモデル提供者向けの周知事項】　※令和8年1月9日　ISMAPポータルサイトに掲載

クラウドサービス事業者が生成AIサービスをSaaSとして提供する場合には、当該SaaSは原則としてISMAP等クラウドサービスリストに登録が必要となります。これは生成AIサービスを外部連携で利用する場合においても同様です。

なお、ISMAPに登録されていない生成AIサービスをISMAPに登録されているIaaS、PaaSを用いて提供しても、当該生成AIサービスはISMAPに登録されているサービスと同等とみなすことはできません。

ただし、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**とみなされます。**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ありません**。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ありません。

この場合において、生成AI特有のリスクについては、ISMAPにおける管理基準とは別に、生成AI開発基盤をISMAP言明対象範囲に含めたクラウドサービス事業者において措置を講じることが必要です。具体的な措置については、「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」の調達チェックシート等を参考にしてください。

なお　、ISMAP登録に関する審査基準等については、「ISMAPクラウドサービス登録規則」等において定めており、詳細はISMAPポータルサイトの制度規程等をご確認下さい。

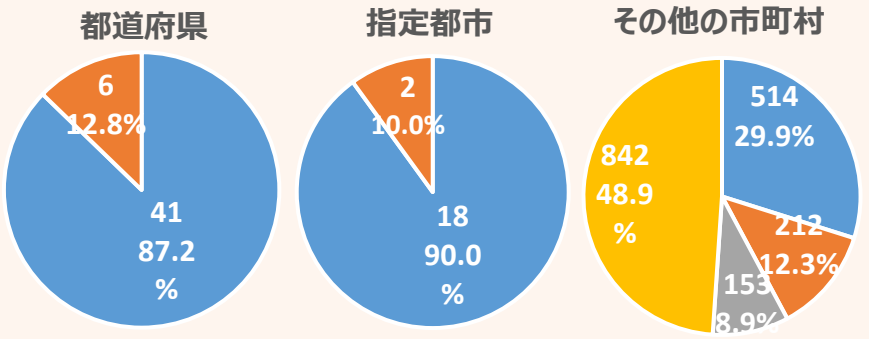
# 自治体におけるAI活用・導入ガイドブックの改訂について（概要）

## 1．現状・課題

○ 「自治体におけるAI活用・導入ガイドブック」(R4.6) において、**生成AIの利活用等に関する記述なし**。

○ 自治体においては、①**生成AIの導入効果が不明**、②**生成物の正確性への懸念**、③**デジタル人材の不足等**といった課題がある。

○ 自治体の**導入状況（R6.12末時点）には、ばらつき**がある。




■導入済 ■実証実験中 ■導入検討中（導入予定あり） ■導入予定なし（団体数、全体に占める%）

## 2．ガイドブック改訂のポイント

① 生成AIは、デジタル技術による単なる作業の代替にとどまらず、仕事の質とスピードを大幅に高め、**飛躍的な業務効率化が期待**されることを、自治体における**具体的な生成AI利活用事例**とともに提示。

② **生成物の正確性への懸念等に対する具体的な対応策・考え方**を提示。

・生成AIの利用目的に応じて求められる正確性の水準が異なることを意識し、**生成物を人が確認するルールを設定**。

・外国語翻訳などの用途によっては、**誤りが含まれる可能性があることを明示した上で、生成AIによる出力結果を表示**。

③ 導入に当たっての留意事項として、**ガバナンス確保のための体制構築**、**要機密情報の取扱い**、**人材育成の考え方**を提示。

・AI統括責任者（CAIO）を設置するなど、**AIの利活用・リスク管理における責任者を明確にする必要**。

・入力した**要機密情報を学習させない仕組み**（オプトアウトの徹底）が重要。「地方公共団体における情報セキュリティポリシーに関するガイドライン」での**機密性情報の分類に応じた利用可能なパブリッククラウドサービスの範囲**を提示。

・専門人材と一般職員の橋渡しを行う**DX推進リーダーの育成**が重要。実際に利用する職員を増やすことが重要であり、**即時利用可能なプロンプト集、職員のレベル別の研修**などに取り組むことが有効（小規模自治体における取組事例も提示）。

○ 自治体が作成する**職員向けの生成AI利用ガイドラインのひな形**を別添として提示。

※「自治体におけるAIの利用に関するワーキンググループ」（座長：須藤修中央大学教授）における報告書（R7.7）の内容を反映

# ２．諸外国の規制・ガバナンス動向

# 諸外国における政府のAI調達利用ルールとの比較（公開情報に基づきデジタル庁にて調査・作成）

| 評価軸 | 国名 | | | | | |
|---|---|---|---|---|---|---|
| | 日本 | アメリカ | イギリス | カナダ | オーストラリア※ | シンガポール |
| 【組織体制】<br>政府横断のガバナンス等 | 各省ごとにCAIOを置き、利用する生成AIを把握。<br>各省は、リスクの高い生成AIの利用についてアドバイザリーボードと協議の上判断 | 各省庁でCAIOの任命・省庁AIガバナンスボードの設置・CAIO協議会の開催の定めがある。CAIOを核として省庁内連携による効果的なAI調達の促進やAI調達に係る情報や知見を省庁間で共有することが求められている | 共同で問題を解決する場として、既存の政府横断AIコミュニティを活用することを推奨。省庁間連携、ベストプラクティスの共有を実施。 | 政府全体での知識共有や進捗モニタリングの仕組みを設けるとともに、全省庁がAI戦略の実行に関与し、既存AI活用事例の報告、課題やニーズの特定、インフラ・人材の確保などを担うことが求められている | 各省にてAIに関して、Accountable Officials(CAIO相当の役職)を設置。高リスク案件の報告、最新動向の把握や省庁間の窓口を担う。政府全体でAIユースケース台帳、戦略・運用方針・透明性声明・職員研修等の実施を義務化 | 政府横断のAI推進体制やガバナンスが推進され、リスク対応・サプライチェーン全体での責任の明確化・各規制当局のベストプラクティス共有が進められる |
| 【企画時】<br>生成AIのリスクについての規定・整理 | 各省は、リスクレベルについて、ガイドラインが示す利用範囲・扱うデータの機密性等の観点から判断 | 各府省はHigh-Impact AIかどうかの判定をする。その出力が、法的、重要な、拘束力のある、または権利や行動に重大な影響を及ぼす決定や行動の主要な根拠となる場合、AIは影響力が大きいと判断 | AI影響度評価によるリスクの特定・軽減を実施。<br>重要決定時や設計変更時にも再評価 | プロジェクトのリスクを4段階で評価する基準（AIA）を整備。当該評価をプロジェクトの設計フェーズ開始前までに完了させることを要求 | 全AIユースケースについて事前にツールを用いた影響評価を行い、用途・期待効果・固有リスクを特定することを義務化。高リスクの場合はAccountable Officialへの報告が義務付けられている | |
| 【調達時】<br>調達時のチェック項目の整理 | 調達時の確認事項（例：入出力データ等の適切な管理、有害情報の出力制御等）について整理。<br>各省が利用ケースに照らして、実際に確認する事項を判断 | 連邦政府調達における米国製AIの重要性を取り上げている。各府省は要件と契約条件を明確化するために、目的・業務上の効果・システム要件・技術性能等に基づくベンダー評価を強く奨励されている | 調達時の検討事項10点（ガバナンスやデータ保護の計画等）とフェーズ別（企画、公募、評価選定、契約・継続管理）の留意事を整理 | 生成AIツールの調達時に、プライバシー・セキュリティ・法務の観点からリスク評価や利用規約等の確認を推奨。AIポータルでは要件を満たした「Qualified Suppliers」リストが公開され、効率的かつ信頼性の高い調達を実施 | 契約時に考慮すべき観点を5つ（AIの倫理原則、明確な説明責任、データの透明性、情報資産へのアクセス、AIのパフォーマンステスト）に整理。AI技術の急速な変化によるリスクへの対応等を求める。また、AI調達契約書の参考テンプレートを公開（任意使用） | 調達について政府内の専門機関が相談を受付。汎用的な既存行政AIサービスの優先検討を求めつつ、政府認定企業の製品やサービスからも選択可能 |
| 【運用時】<br>リスクケース・インシデントへの対応ルール※1 | リスクケース発生時の対応事項について整理。<br>提供者がインシデントの内容や行う対応等について、AI統括責任者及びアドバイザリーボードに報告。 | リスクケース・インシデントへの対応ルールの明記はなし。ただ、AIの性能が適切なレベルに達していない場合の使用の中止を求める規定が存在 | ライフサイクル全体でリスクを管理し、エスカレーションのプロセスを文書化することを推奨。リスクケース発生時の報告先や対応者の明確化、影響を受けた個人に対する救済措置の確立を求めている | 起こり得るAIのサイバーセキュリティ事象とインシデント事象について整理の上、対応計画の策定を義務化 | | |

【凡例】 ○ 規定あり　△ 規定あり（限定的）　▬ 具体的な規定なし　□ 第1回アドバイザリーボード資料からのステータス更新

※ 2025年12月15日から適用される新版ポリシーが公開。リスクケース・インシデントへの対応ルールについては、どのようなケースをインシデントと定義するかの記載はあるものの、具体的な対応ルールの言及がないため、“具体的な規定なし”としている。
https://www.digital.gov.au/ai/ai-in-government-policy

# （参考）中国:政府業務における大規模AIモデルの導入と適用に関するガイドライン

■「政府業務における大規模AIモデルの導入・適用ガイドライン」
正式名称：政务领域人工智能大模型部署应用指引
発表年月日：2025年10月10日
本ガイドラインは政府が大規模AIモデルを導入する際の方向性・理念・制度設計の枠組みを示すものであり、具体的な規定等については記載されていない。

**Ⅰ．基本方針**
「人間中心の理念」「標準化された応用」「共同構築」「効率的な協働」「安全性・安定性」の原則を堅持し、実効性を重視して推進する。

**Ⅱ．主要な活用分野**
政府部門は、行政サービス、社会ガバナンス、業務遂行、意思決定支援といった高頻度かつ共通的なニーズを踏まえ、地域や実情に応じてAIモデルの応用を推進する。
**（Ⅰ）行政サービス**
**（Ⅱ）社会ガバナンス**
**（Ⅲ）業務運営**
**（Ⅳ）意思決定支援**

**Ⅲ．導入および標準化の方針**
政府部門は、業務実態およびシナリオ特性を踏まえ、AIモデルの導入ニーズ・設計・運用計画を十分に検証し、最適な展開方式を選定する。
**（Ⅰ）導入パスの選択**
**（Ⅱ）協調的・集中的展開**
**（Ⅲ）統一管理と再利用**
**（Ⅳ）データ基盤の強化**

**Ⅳ．運用および管理体制**
政府部門は、政務分野における大規模AIモデルの運用・管理体制を強化し、組織ガバナンス、運用プロセス、セキュリティ要求を整備することで、関連技術・製品・サービスの展開と応用を秩序立てて推進する。
**（Ⅰ）応用管理**
**（Ⅱ）継続的最適化**
**（Ⅲ）セキュリティ管理**
**（Ⅳ）機密保持**

**Ⅴ．推進体制および支援措置**
政府分野における大規模AIモデルの開発・応用を安全かつ秩序正しく推進するため、組織体制、モニタリング・評価システム、教育普及の三側面から総合的な実施体制の整備を講じる。
**（Ⅰ）組織体制の強化**
**（Ⅱ）モニタリング・評価**
**（Ⅲ）研修・普及**

https://www.cac.gov.cn/2025-10/10/c_1761819469929310.htm

公開情報に基づきデジタル庁にて調査・作成。日本語訳は参考情報としての訳である。

# （参考）シンガポール政府が提供するリスク評価・検知ツール

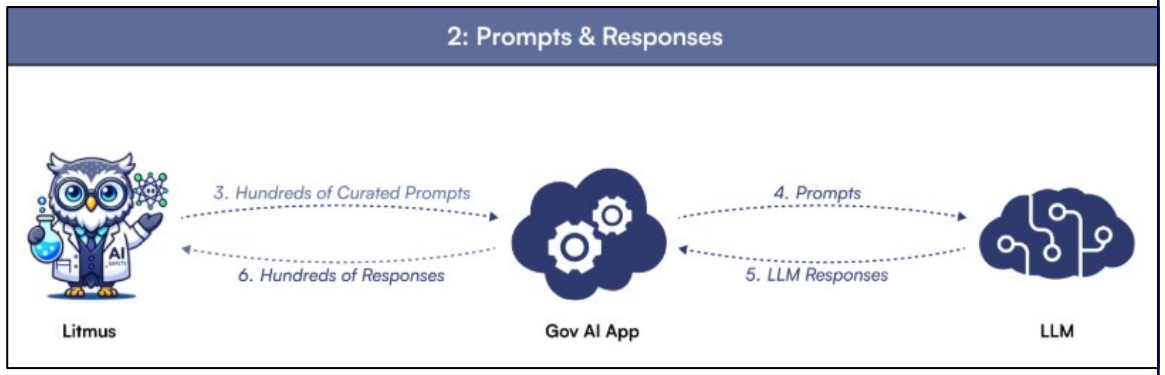
シンガポール政府では、政府内、国民向けのともに高い水準でのAI提供を実施するためのツールであるLitmus、政府のAIアプリケーションを安全に運用するためのツールであるSentinelを構築して活用している

## ■Litmus（リトマス）

AIシステムのリリース前に安全性・セキュリティリスクを評価するテスト基盤。**企画段階**で活用。

- アプリケーションのCI/CDプロセスと連携し、**リスクをリアルタイムで検知**するツール。
- 公共部門のAI倫理・政策・ガイドラインに沿ったリスク・行動分析を自動で実施する。
- 多様なユースケース（チャットボット、文書処理、政策分析等）に合わせたカスタマイズ可能なテストシナリオを提供する。

ユーザがLitmusを使うと、Litmusは数百のプロンプトをアプリに送り、LLMの応答を回収して安全性やリスクを評価する




## ■Sentinel（センチネル）

運用中のリスクをリアルタイムで防御するガードレール基盤。**運用段階**で活用。

- 入力・出力の両方を監視し、自動化されたガードレールにより**リスクを即時検知・遮断**するツール。
- プロンプトインジェクション、毒性コンテンツ、個人情報漏洩を防止し、運用中の生成AIアプリを安全に保護する。
- リアルタイムで入出力をスコアリングし、許可・拒否・フラグを判断。
- リスクやインシデントが発生した場合、AI Guardian※1のプラットフォーム上で記録・管理され、再発防止やガバナンス強化に活用される。

デモ画面：入力されたプロンプトをスコアリングし、出力を拒否している

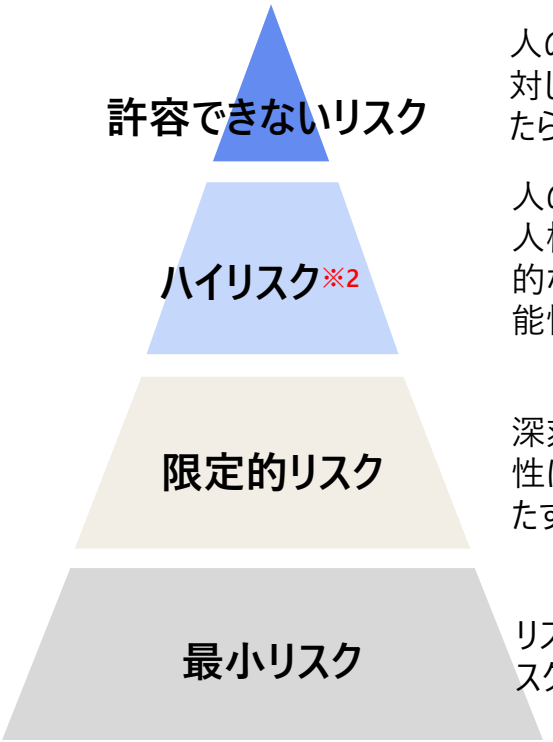
※1 シンガポール政府が公共部門向けに提供するAIガバナンス・リスク管理のためのプラットフォーム

https://www.aiguardian.gov.sg/

公開情報に基づきデジタル庁にて調査・作成。

# （参考）EU AI ActにおけるAIのリスク分類

## 全てのAIシステムは４つのリスクへ分類※1




| | | |
|---|---|---|
| 許容できないリスク | 人の生命や基本的人権に対して、直接的に脅威をもたらすと考えられるAIシステム | 禁止 ☒ |
| ハイリスク※2 | 人の健康や安全、基本的人権、または社会的／経済的な利益に影響を与える可能性があるAIシステム | ハイリスクAIの義務の遵守※3 ☑ |
| 限定的リスク | 深刻なリスクはないが、透明性に関する特定の要件を満たす必要があるAIシステム | 透明性の義務の遵守 ☑ |
| 最小リスク | リスクがごくわずか、またはリスクを伴わないAIシステム | 制限なし ☑ |

※1 AIシステムの特性によっては複数のリスクに該当する場合があります。

※2 欧州委員会は、AI法におけるハイリスクAIシステム規制の適用開始を、技術標準やガイダンス整備の遅れを理由に最長16カ月延期し、2027年12月までとする方針を発表しました。適用開始までの期間に、企業は必要な支援ツールを整備・確保した上で、義務を円滑に履行できる体制を整えることが可能となります。

※3 ハイリスクのAIシステムには、「リスク管理システム」「データガバナンス」「技術文書、ログ管理」「透明性」「人による監視」「サイバーセキュリティ」などの観点で定められた要求事項の遵守を求めています。

## 汎用目的AIモデルは2段階に分かれる

汎用目的AIモデル（GPAI）は他のAIシステムに組み込まれて使用される可能性が高いため、GPAIを提供する事業者（プロバイダー）にはさまざまな義務が課せられます。

また、GPAIの中でも一定の条件を満たすAIモデルはSystemic riskがあると判断され、より厳しい要件への対応が求められます。

**Tier 1: 全ての汎用目的AIモデル**

- モデルに関する仕様書などを最新化すること
- EU著作権法を遵守すること
- 適切な情報提供を実施すること
- 規制当局に協力すること

など

**Tier 2: Systemic risk**

- 高影響が想定
- モデルのトレーニングに使用される計算量が10^25 FLOPs

など

- Systemic riskを評価し、そのリスクを低減すること
- インシデント発生時に当局へ報告すること
- サイバーセキュリティに関する保護を実施すること

など

2025年7月10日、「汎用AIの行動規範」が公開されています。
法的拘束力はありません。①透明性、②著作権、③安全性・セキュリティの3つの章で構成されています。

欧州委員会は2026年2月2日までに、どのようなユースケースがハイリスク/非ハイリスクに該当するかの具体例を示すガイドラインを公表予定であり、高リスクAIの分類が明確化される見込みです。

https://artificialintelligenceact.eu/implementation-timeline/
https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

# OECD”Governing with Artificial Intelligence”掲載のAI活用事例抜粋

| ユースケースカテゴリ | 事例概要 | 国・地域 | ユースケース説明 |
|---|---|---|---|
| 税務 | 納税者サービスの強化用チャットボット | シンガポール | 2021年、政府の仮想知能チャットアシスタント（VICA）上で納税者サービス効率化のためのチャットボットを導入。2023年にはLLMエンジンを統合し、納税者の意図理解を大幅に向上させ、税目横断の問い合わせ回答に対応し、認証済みサービス（残高照会や分割払い手続など）へのアクセスも可能。2024年度に約7万件のトランザクション処理、約1.17万時間の削減効果 |
| 規制の設計と執行 | 立法立案及び対応のためのAIの使用 | イギリス | AIによって法律文書の検索や説明書きの作成を支援。また、過去の議会記録を分析し、提案政策に対する議会の反応を予測することが可能 |
| 市民参加・オープン政府 | 欧州議会アーカイブへのアクセスの民主化 | 欧州 | 欧州議会が開発した「Archibot」プラットフォームは、LLMとRAG（検索拡張生成）技術を統合し、ユーザーがデジタル化された文書と対話的に情報を検索できるようにしている。研究・政策利用を容易にするために、市民、研究者、政策立案者は、1952年以降の10万件以上の文書データから、歴史的出来事、主要人物、制度的発展に関する情報を自然言語で照会可能 |
| 公共サービス設計・提供 | 公共職業安定機関（PES）によるAIを活用したサービス提供強化 | OECD加盟国全般 | OECD諸国における公共雇用サービス機関（PES）のAI活用として、求職者のリスク予測、求人マッチング、求人設計支援、情報提供、キャリア支援が拡大する一方、透明性・公平性確保の課題が浮上しており、各国が倫理委員会設置やAI戦略策定によってガバナンス強化を進めている。オーストリアでは2024年初頭にChatGPT搭載チャットボットを導入し、求職者に研修やキャリア支援情報を提供したが、ローンチ直後に「男女間の推奨内容に差がある」との批判を受けた |

2025/9/18、OECDが発表した”Governing with Artificial Intelligence”に記載の各国政府ユースケースより、生成AI関連かつ特に参考となる事例を抜粋

# OECD”Governing with Artificial Intelligence”掲載のAI活用事例抜粋

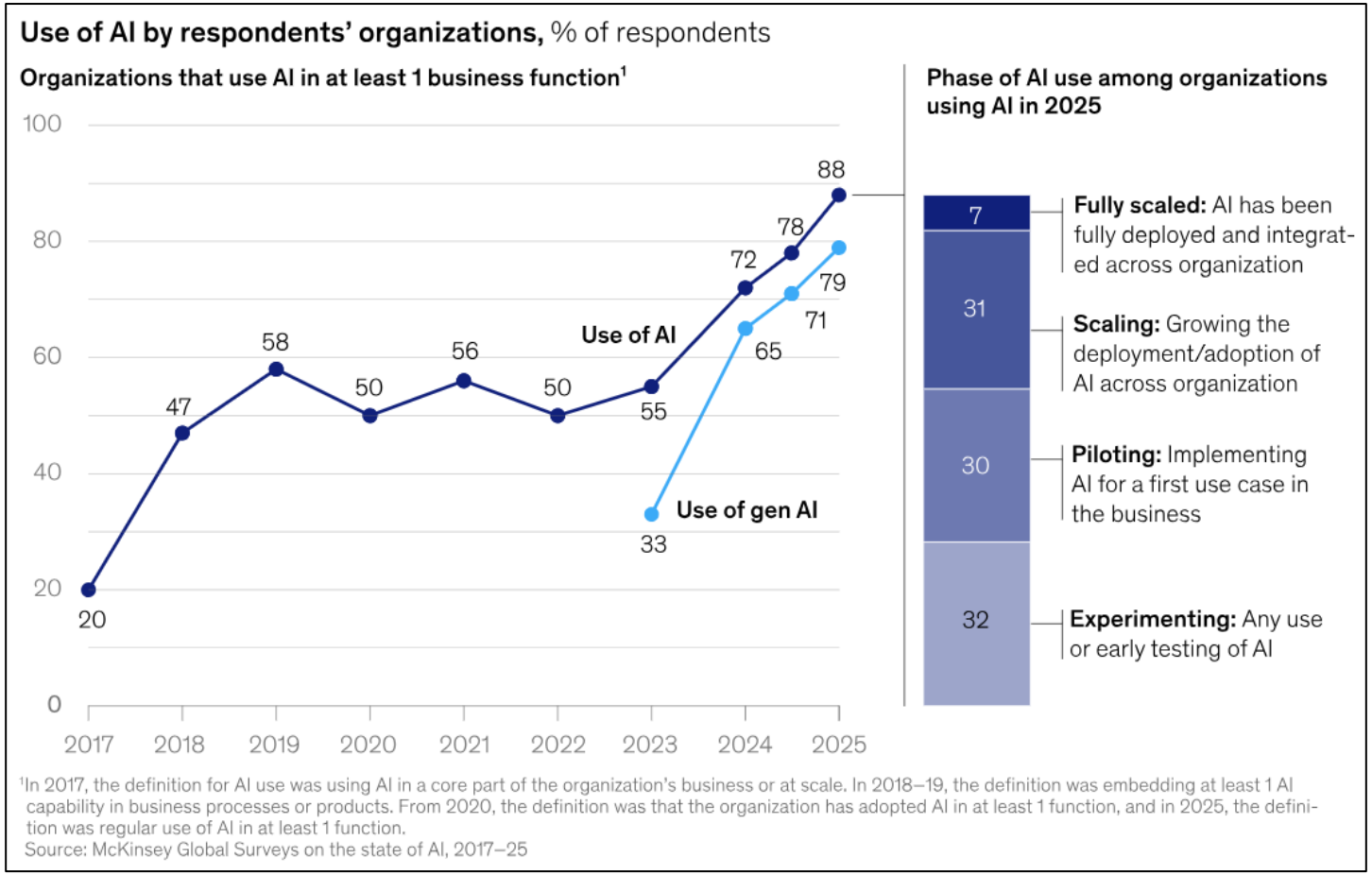
| ユースケースカテゴリ | 事例概要 | 国・地域 | ユースケース説明 |
|---|---|---|---|
| 公的財政管理 | ロボット債務スキーム：不適切な支払いの収集に関する議題 | オーストラリア | オーストラリア政府は「Robodebt」制度により、社会保障給付の過払い回収を自動化。センターリンクが報告した隔週収入データと、ATOの年間収入データを比較し、差異を過払いとして自動的に債務通知を送付。だが、変動収入を無視した「平均化」手法により誤判定が多発し、受給者に証拠提出を強要。47万件の誤通知、総額7億7,500万ユーロに達し、多くが経済的困難や精神的被害を受けた。最終的にロイヤル・コミッションが設置され、報告書では人間による監視の欠如が問題とされた |
| 腐敗防止・公正 | 法案分析を通じた汚職防止 | リトアニア | リトアニアの特別捜査局（STT）が、法令や法案をAIで分析し、汚職リスクを未然に防ぐためのツールを開発中。汚職リスクデータで学習したLLM（大規模言語モデル）を使用。法令文書の抜け穴・手続きの弱点・不十分な措置などのリスク要因を自動検出し、脆弱性を迅速に特定 |
| 司法・司法アクセス | ペルーにおける保護命令の迅速化のためのAIによる司法サービスの再設計 | ペルー | 裁判所が独自に開発したAmauta Pro（保護命令決定プロセスを自動化。機械学習と生成AIを組み合わせ、文書分類・事件照合・判決決定書草案生成を行う）は家庭内暴力事件を対象に試験運用。判決書作成時間を3時間から40秒に短縮、試験段階で800件庁の判決草案を作成、裁判官は時間とリソースを判断業務・最終決定など本質的な業務に集中できるように |
| 司法・司法アクセス | 司法情報提供のためのAIチャットボット | ポルトガル | ポルトガル法務省は、Practical Guide to Justice（GPJ）というAIチャットボットを導入し、市民が司法関連情報に容易にアクセスできるようにしている。GPJは、司法手続き関連の質問に平易な言葉で回答。AIがデジタル司法プラットフォーム情報を基に回答を生成 |
| 調達 | 責任あるAI調達と導入を推進する「GovAI Coalition」<br>※厳密にはユースケースとしてのAI活用事例ではないが、調達の観点での参考事例 | アメリカ | 2023年サンノゼ市主導の「GovAI Coalition」が設立され、政府間で（全米の地方・州・連邦レベルの機関が参加）責任あるAI調達を推進。AI契約テンプレートとナレッジ共有プラットフォーム（AI Contract Hub）を整備し、倫理的AI導入を支援。政府機関向けのAI調達テンプレートとガバナンスツール群を提供。2025年に「AI Contract Hub」をローンチし、契約・調達プロセスを効率化 |

# ３．民間でのユースケース・技術動向

# AI・生成AIの導入状況（経年比較）

〇従来のAI、生成AIのともに、AIを利用している企業の割合は非常に高くなっており、生成AIの利用も急激に伸びている状態である

〇AI活用のレベルでは、32%は活用の試行の段階であり、31%がスケーリングしはじめている状況である

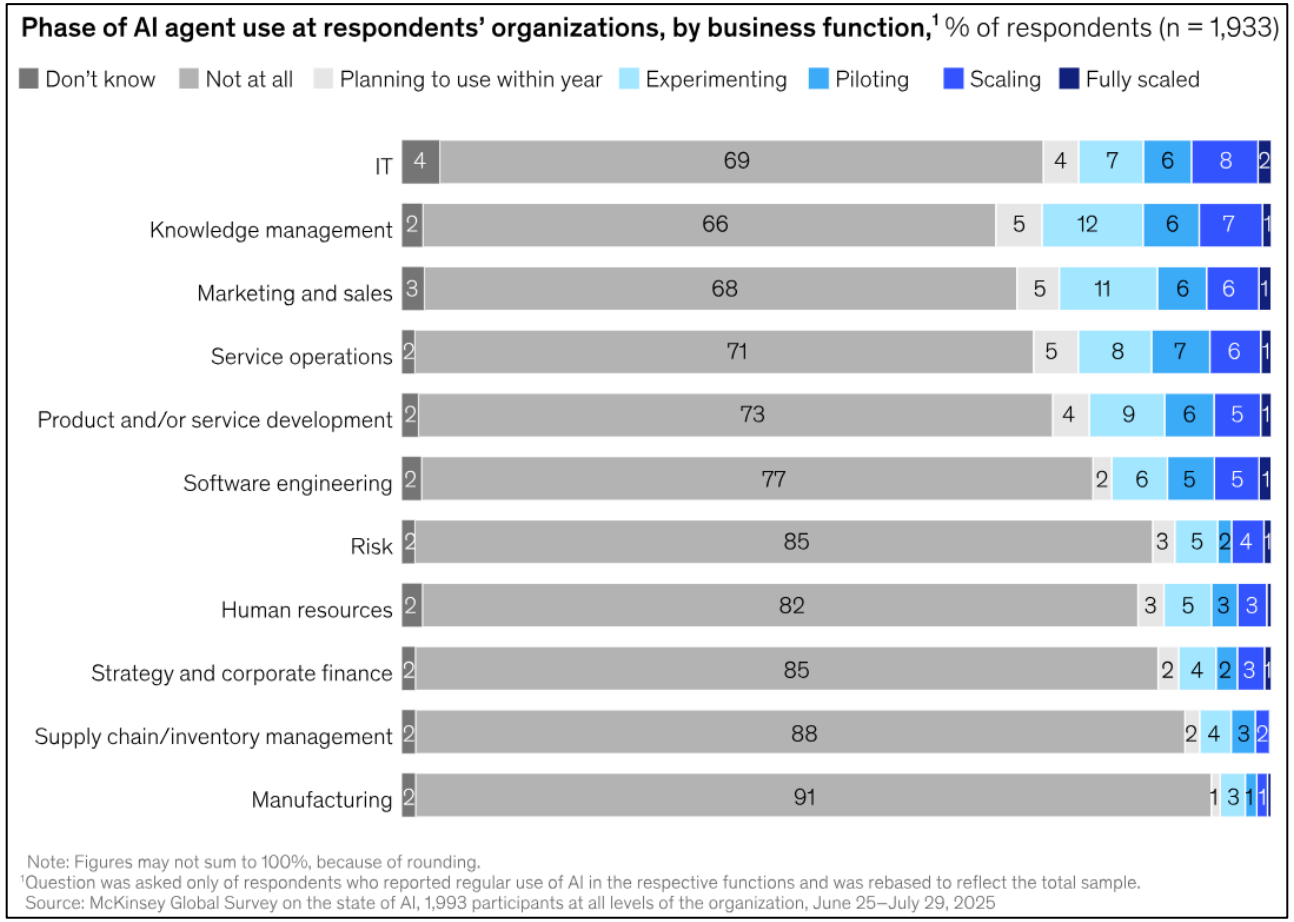



2025年11月5日, McKinsey & Company (QuantumBlack, AI by McKinsey), "The state of AI in 2025: Agents, innovation, and transformation"より抜粋
アンケート調査であり、105の国と地域の企業から、1,993名から回答を得ている
回答者の38%は年間売上が10億ドルを超える組織に勤務しているが、回答率の差異調整のためにデータは各回答者の国のGDPへの貢献度に基づいて加重されている

# AIエージェントの導入状況（2025年・業務分野別）

〇AIエージェントの活用も徐々に進みつつあり、組織での本格活用が進みつつある業務分野では10%がスケーリング以上の段階である

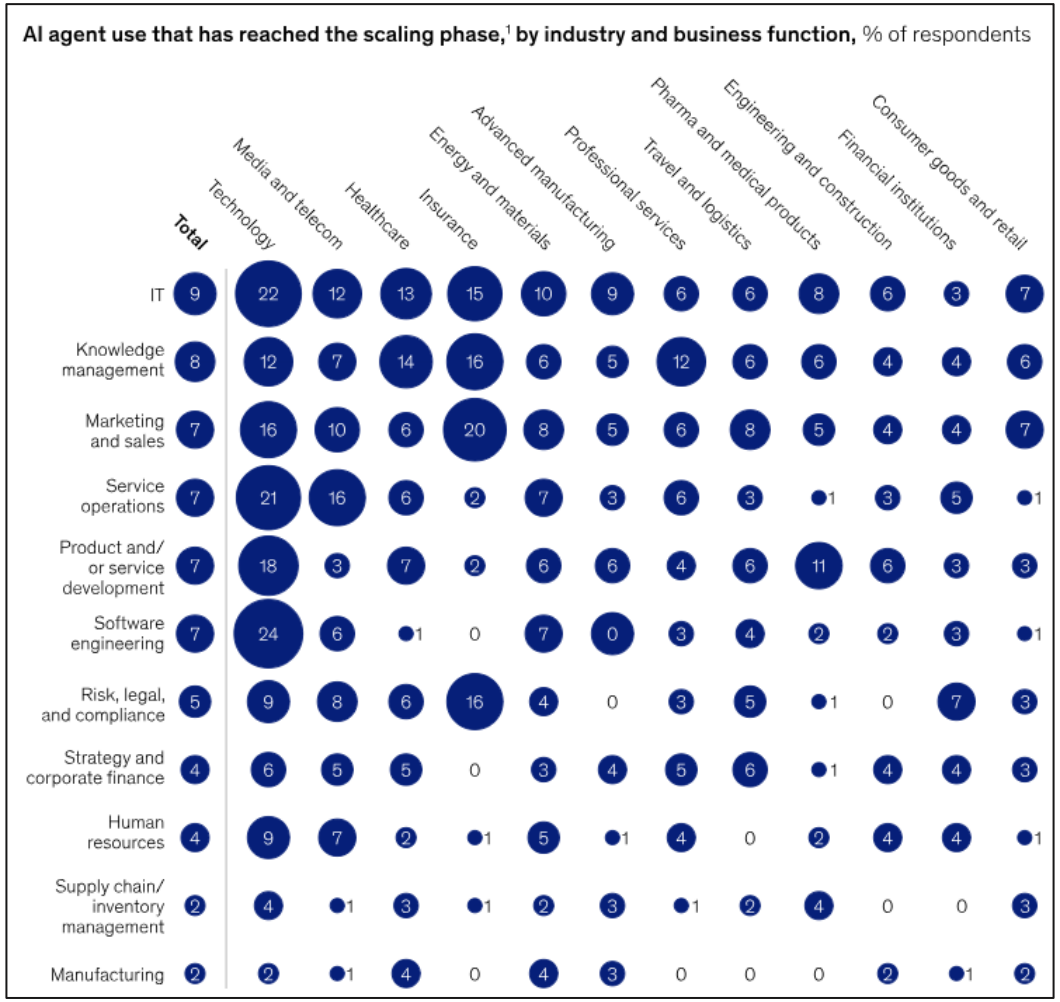
〇先行的な取り組みが進みつつあるが、全体の傾向としては本格活用の検討に至っていない割合が高い状態である




2025年11月5日, McKinsey & Company (QuantumBlack, AI by McKinsey), "The state of AI in 2025: Agents, innovation, and transformation"より抜粋
アンケート調査であり、105の国と地域の企業から、1,993名から回答を得ている
回答者の38%は年間売上が10億ドルを超える組織に勤務しているが、回答率の差異調整のためにデータは各回答者の国のGDPへの貢献度に基づいて加重されている

# AIエージェントの導入状況（2025年・業務分野と産業別）

〇個々の業務分野レベルでは、ITおよびナレッジマネジメント領域でAIエージェントの活用が先進的に進みつつある状況
〇業界別ではテクノロジー、メディア・通信等の分野で最も活用が進みつつある状況




2025年11月5日, McKinsey & Company (QuantumBlack, AI by McKinsey), "The state of AI in 2025: Agents, innovation, and transformation"より抜粋
アンケート調査であり、105の国と地域の企業から、1,993名から回答を得ている
回答者の38%は年間売上が10億ドルを超える組織に勤務しているが、回答率の差異調整のためにデータは各回答者の国のGDPへの貢献度に基づいて加重されている

デジタル庁

Digital Agency