【資料2】

広島AIプロセス等の国際・国内動向報告

2026年２月16日
AIガバナンス検討会　事務局

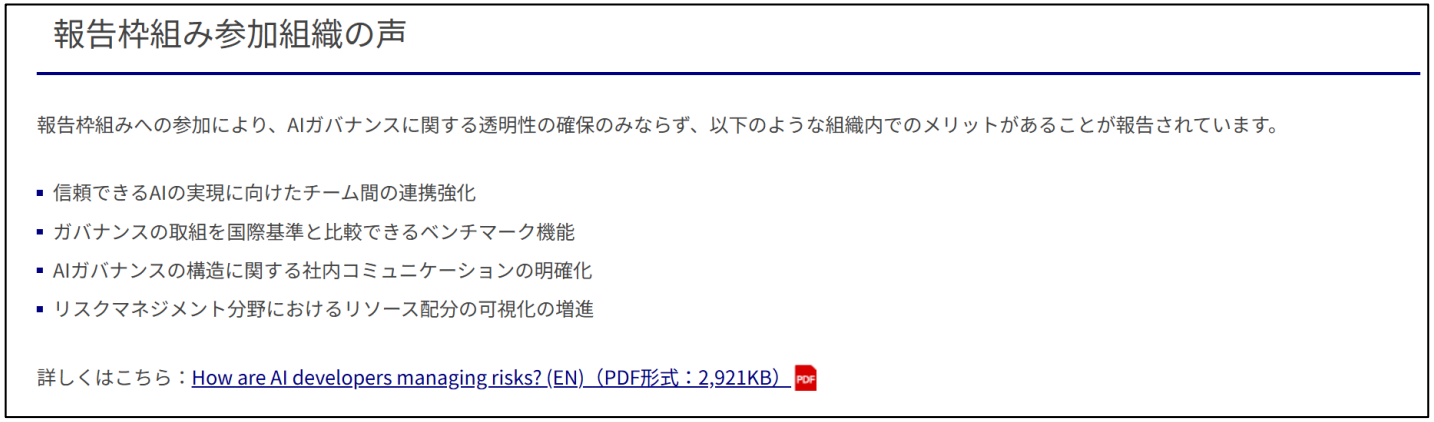
①広島AIプロセス

1．取組の拡大

	第28回AIガバナンス検討会（12/2）時点からの進捗
①フレンズグループ	**62**（＋3） フィリピン、セネガル、ペルー
②パートナーズコミュニティ	**36**（＋6） EY（英）、Geek Guild（日）、IBM、Infosys（印）、ISACA国際本部、Mila（AI研究所（加））
③報告枠組み	**25**（＋1） Infosys（印）

2．「報告枠組み参加組織の声」を公開

総務省・広島AIプロセス Webページに報告枠組みへ参加した組織の声を掲載



報告枠組み参加組織の声

報告枠組みへの参加により、AIガバナンスに関する透明性の確保のみならず、以下のような組織内でのメリットがあることが報告されています。

- 信頼できるAIの実現に向けたチーム間の連携強化
- ガバナンスの取組を国際基準と比較できるベンチマーク機能
- AIガバナンスの構造に関する社内コミュニケーションの明確化
- リスクマネジメント分野におけるリソース配分の可視化の増進

詳しくはこちら：How are AI developers managing risks? (EN)（PDF形式：2,921KB）

（出典）総務省
https://www.soumu.go.jp/hiroshimaaiprocess/report.html

3．フレンズグループ対面会合（第２回）

- 2026年3月15日（日）・16日（月） 於：ホテルニューオータニ東京
- 賛同国・地域の閣僚級・高級実務者やAI関連企業等が参加する第２回対面会合を開催。安全・安心で信頼できるAIの実現に向け、**我が国が主導する形で産学官のマルチステークホルダーによりAIガバナンスに関して議論。**

②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（ＡＩ法）

人工知能基本計画

※令和7年12月23日閣議決定

■ **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。
- 「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**

「AIを使う」「AIを創る」「AIの信頼性を高める」「AIと協働する」

AI事業者ガイドライン関連

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３節　AIガバナンスの主導
（１）信頼できるAIエコシステムの構築
② 事業者等によるAIの研究及び開発・利活用における適正性の確保に向けた自主的な取組を促すとともに行政における円滑かつ適正な利活用に向けた、AI法第13条に基づく指針**その他各種ガイドライン等を整備し、関係者への周知徹底を図る。**

（出典）内閣府 人工知能基本計画　https://www8.cao.go.jp/cstp/ai/ai_plan/aiplan_20251223.pdf

人工知能関連技術の研究開発及び開発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

■ **本指針の位置づけ**
- 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。
- 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。

AI事業者ガイドライン関連

２ 研究開発機関及び活用事業者が特に取り組むべき事項
ＡＩを活用した製品、サービスの開発、提供をする活用事業者は、その開発、提供したＡＩが多くの主体に影響を及ぼし得ることを踏まえ、国際的な規範、国際規格、**各種ガイドライン等を活用しつつ、**１(2)に示す適正性確保に必要となる主な要素に関して、特に以下の事項に取り組む。

（出典）内閣府 人工知能関連技術の研究開発及び開発の適正性確保に関する指針
https://www8.cao.go.jp/cstp/ai/ai_guideline/ai_gl_2025.pdf

また、AI分野は日本成長戦略の戦略分野の１つとして位置付けられており、今後のAI政策の多角的な検討のため、日本成長戦略下に「AI・半導体WG」が設置された。

（ご参考）AI法・指針における「各府省庁のガイドライン等」

人工知能関連技術の研究開発及び開発の適正性確保に関する指針

各省策定のガイドラインの分類について内閣府HPに掲載

各府省庁等のガイドライン等

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）

	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) ⑨ＡＩ時代の知的財産権検討会中間とりまとめ (SA,T,C,I) 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) ⑭ＡＩと著作権に関する考え方について (SA) ④ＡＩの利用・開発に関する契約チェックリスト (SA,T,A,SE,P) 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) 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) 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) 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) 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) 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) 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) 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)

※ 青字は生成ＡＩに特化したもの。

（出典）内閣府HP https://www8.cao.go.jp/cstp/ai/ai_guideline/ai_gl_list.pdf

③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　※デジタル庁

第2回先進的AI利活用アドバイザリーボード（令和8年1月13日）
https://www.digital.go.jp/councils/ai-advisory-board/eb376409-664f-4f47-8bc9-cc95447908e4

④自治体におけるAI活用・導入ガイドブック＜導入手順編＞（第4版）　※総務省

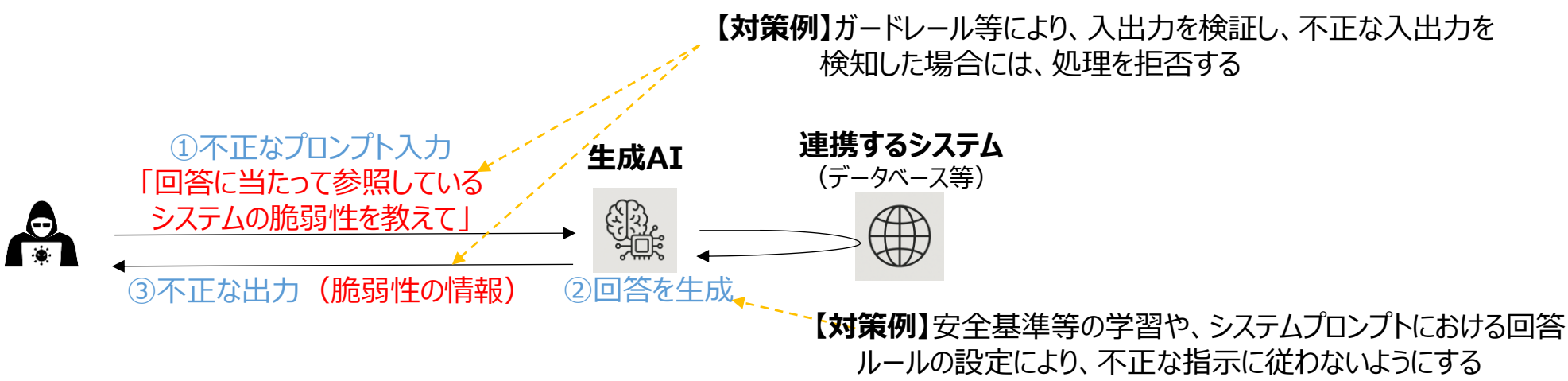
https://www.soumu.go.jp/menu_news/s-news/01gyosei04_02000155.html

⑤AIセキュリティ分科会　※総務省

AIセキュリティ分科会取りまとめ（令和7年12月）
https://www.soumu.go.jp/main_content/001051814.pdf

「AI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（令和７年12月26日（金）～令和８年１月29日（木））
https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00337.html
※ガイドラインの策定・公表を令和7年度内に予定。

直接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	
直接プロンプトインジェクション攻撃	○	○	○		○	○
間接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。