

# 自民党AI・WEB 3 小委員会提言等 を踏まえた対応（AISIの機能強化、 AIサミットについて）

# I. AISIについて

## (1) 人工知能戦略本部 高市総理ご指示 (抄)

AIセーフティ・インスティテュートの抜本的強化です。AIの安全性に対する不安が高まる中、英国並みの200人体制を目指して、小野田大臣と赤澤経済産業大臣は、全省庁、産学から人材を集結させ、AIセキュリティに万全を期してください。

## (2) 自民党AI・web3小委員会提言 (抄)

我が国のAIに関するイノベーションの促進とリスク管理を両立させるためには、「信頼できるAI」の利活用及び開発の中核となるAIセーフティ・インスティテュート(AISI)の抜本的な機能強化を行わなければならない。AIモデルの技術的評価、広範な適正性に係る評価、セキュリティ面での対策を実行できる体制の構築を行う必要がある。

(中略)

1. 政府は、英国のAISIをベンチマークに、質・量ともにAISIの人員・体制強化を図ること。まずは令和7年度補正予算を的確に執行し、早急に現行の30名から陣容を拡充し、60名体制を目指すこと。
2. AIはあらゆる行政分野に関係しており、各省庁でAI安全性やAIセキュリティの専門家の育成が必要不可欠である。そこで、全省庁がAISIに出向者を出すこと。特にデジタル政策に関係する省庁については複数名出すこと。
3. AISIが自らの権能で国内外の有能なAI関連の専門家を柔軟に雇用できるよう、国家公務員より高額かつ柔軟な年俸支出も可能となるようにすること。
4. AISIの拡充する業務の適切な執行と常勤常駐含めた体制整備及びそのための財政基盤を確保するため、AI政策の司令塔である内閣府がAISI業務の共管省庁となること、また内閣府及び経済産業省から運営費交付金を安定的に支出すること。

# AIセーフティ・インスティテュート (AISI) について

- 国際的にAIガバナンスの重要性が高まる中、**AI安全性サミット**（2023年11月、英国）を契機に「**AI安全性**」を具現化するための議論が進み、英・米はAIセーフティ・インスティテュートを設置。
- 我が国も第7回AI戦略会議（2023年12月）における**岸田元総理からの指示を踏まえ、2024年2月に日本のAIセーフティ・インスティテュート（所長：村上明子氏）を設置。**
- AI安全性の知見のハブとして、**国内外の関係機関とのネットワークを強化中。AISIの安全性の評価能力を確立しながら、安全性評価のための基準、ガイダンスを作成。**

## エイシー 日本のAISIの概要

名 称

(日本語) AIセーフティ・インスティテュート  
(英 語) Japan AI Safety Institute (略称 J-AISI)

業務内容

- 安全性評価に係る調査、基準等の検討
- 安全性評価の実施手法に関する検討
- 他国の関係機関（英米のAI Safety Institute等）との国際連携に関する業務

関係機関

内閣府、国家安全保障局、国家サイバー統括室、警察庁、デジタル庁、総務省、外務省、文科省、厚労省、農水省、経産省、国交省、防衛省

情報通信研究機構、理化学研究所、国立情報学研究所、産業技術総合研究所、情報処理推進機構

主要な実績

**AIセーフティに関する評価観点ガイド、レッドチーミング手法ガイド等の公開。AISI国際ネットワーク(米・EU等の主要国AISI関連機関10カ国が参加)に参加し、AIの共同テストに関するトラックをリード。**







村上 明子

**(AIセーフティ・インスティテュート所長)  
(SOMPOホールディングス株式会社  
執行役員常務 グループChief Data  
Officer)**

2024年、AIの安全性と信頼性を専門的かつ中立な立場で検証する公的な第三者機関であるAIセーフティ・インスティテュート(AISI)の設立に伴い所長に就任。

# 主要国AISI関連機関の動向：「セキュリティ」や「標準」に重点

-  ● 2025年2月14日、**英国**AISIはAI Security Institute に改名。  
**AI安全性(AIモデルの透明性、堅牢性、信頼性等)に係る取組からセキュリティ(サイバー・化学攻撃等への活用の可能性、犯罪への活用の評価等)によりシフト。**  
防衛科学技術研究所等とも連携。
-  ● 2025年6月3日、**米国**AISIはCAISI (Center for AI Standards and Innovation) に改名。  
これまでの**AI安全性に係る取組から、より競争力強化 (イノベーション促進) と国家安全保障に重点をおいた取組にフォーカス。**具体的には、  
①**セキュリティ評価機能の強化・拡充 (敵対国のAIシステム評価、バックドア対策等)**、  
②**外国の脅威への対処 (競争力評価、外国製AIシステム採用状況調査等)**。  
米国は、日本や韓国との間でMOUを結び、業界標準の開発等を推進。
-  ● 2025年7月26日、**中国**は、上海での世界人工知能大会で、AIへのユニバーサルアクセスが多くの国で確保されることの重要性を説く中で、グローバル・サウスへの支援を表明。  
**中国主導で、A I を安全かつ包摂的に活用するための国際組織の創設を提唱。**  
(参考) 同国サイバーセキュリティ法を改正し、AI等の新技術のサイバーセキュリティへの活用 (AIによる攻撃を想定しAIによる防御を実施) を追加予定。
-  ● 2025年7月30日、**英国AISI及び加AISIは、30億円規模の基金を設け、急速な進化を遂げるAIが、人間の価値観や倫理観に沿って行動するよう管理・制御するための研究開発を、多国間の官民連携で実施する「Alignment Project」の開始を表明。**

# 日本AISIと米国アンソロピック社の協力について

## 1. 令和7年10月29日に、アンソロピック社のダリア・アモデイCEOは、高市総理大臣を表敬訪問。

小野田内閣府特命担当大臣（人工知能戦略）が同席し、MoCに基づきAISI村上所長も同席。

高市総理は以下について発言。

「日本における信頼できるA Iの実現に向けて、安全に関するA I S I（エイシー）との協力、政府での活用、スタートアップ支援で協力いただけることに感謝。是非、日本での開発拠点等更なる投資に期待したい。」



## 2. 同日、AISIと米国アンソロピック社はAIの評価に関する協力覚書(MoC)を締結し、以下

について協力。

(主な協力内容)

- AIモデル評価に関する情報やベストプラクティスの共有
- AIモデルの能力やリスクを評価するためのツールやベンチマークの開発
- AI分野の動向や将来の技術開発に関する意見交換



# アンソロピック 脅威インテリジェンス・ブリーフィング

(2025.11「初めて報告されたAI主導型サイバー諜報活動の阻止」)

- **Claude** (アンソロピック社の生成AI)を活用したサイバー攻撃が複数報告。攻撃手法が驚異的なスピードで大きく進化。人間の関与が10~20%に留まり、**AIが自律的にサイバー攻撃するフェーズへ**。
- **技術や資金の少ない攻撃者でも、大規模かつ効率的なサイバー攻撃が可能**に。
- **AIは防御にも不可欠**。検知技術の向上や安全対策の強化がますます重要に。

【AIを活用したサイバー攻撃の進化状況】

## 2025年3月

- 英国拠点の脅威アクターがClaudeを活用し、**技術力不足を補い、ノーコードでランサムウェアを開発**。
- ダークウェブで高度なマルウェアを流通・販売 (\$400~1,200)。

## 2025年5月

- ロシア語を話すサイバー犯罪者がClaude Code (アンソロピック社のAIEージェント型コーディング支援ツール) を使い、国内外の17の標的に対して**大規模な恐喝を実施**。(要求額: ビットコインで \$75,000~500,000)
- Claude Codeが大規模な偵察、認証情報等の収集、ネットワーク侵入を自動化。

## 2025年9月

- 中国政府支援グループがClaude Codeを使い、**自律型サイバー攻撃エージェントを構築**。Claudeをオーケストレーションシステムとして用い、複雑な多段階攻撃を個別の技術タスク(脆弱性スキャン、認証情報の検証、データ抽出、横展開等)に分解することで、悪用検知が非常に困難に。
- **サイバーキルチェーン全体(脆弱性発見、侵入、自律的分析、横展開、権限昇格、情報流出)を概ねAIが自律的に実行**。

# 日本AISIの現状に対する評価

## 1. 職員数・予算規模




- **人員・予算が潤沢でない**ため、企業向けのA I 安全性に係るガイドのみを作成・提供。  
例：AI安全性に関する評価観点ガイドやレッドチーム（攻撃者側の目線でAI脆弱性を発見する手法）ガイド等

## 2. 活動内容

- 主要国AISIのように、技術評価のR&Dリソース・体制が十分になく、自らAI評価ツールを作ったり、評価することができていない。  
注：他国AISIでは専用テストベッド・計算資源を準備、フロンティアAIモデルの事前評価を実施。
- 日本の国研にはAI安全性の知見・ノウハウが存在も、AISIがこれら国研の司令塔にはなれていない。現在は、パートナー協定を結んでいる国研（NICT、産総研、NII、理研、IPA等）の成果を活用するのみ(注)。最近、民間企業への外注を開始。  
例1：NIIが日本語LLMの出力の安全性・適正性向上のためのデータセットの作成等を実施、それをAISIの名で各国に提供  
例2：NEC等に外注して、AIが有害な情報を出力しないか等を自動で評価できるツールを開発、AISIの名で公開
- **国家安全保障やサイバーセキュリティの観点から、AIの意図的な誤動作や思想誘導等の評価や、バックドアがないか等の分析は行っていない。**

# 日本AISI機能強化の必要性

- AIが社会に与える影響が拡大するなかで、その**安全性と信頼性を専門的かつ中立的な立場で検証する「公的な第三者機関」であるAISIが必要不可欠に。**
- 2023年11月、英国でのAI安全性サミットを契機に、英・米がそれぞれ国内にAISIを設立。日本も、**2024年2月に日本AISIをIPAに設置。AISI国際ネットワークを形成。**
- **日本AISIの予算、人員は英米に比べて圧倒的に少ない。**  
国際ルール形成主導に向け、**産官学の人材、知見、資金を糾合して機能を強化する必要。**

|        |  <b>日本</b><br>AI Safety Institute                |  <b>英国</b><br>AI Security Institute   |  <b>米国</b><br>Center for AI Standards and Innovation  |
|--------|---|--|--|
| 設立     | 2024年2月   | 2023年11月   | 2024年2月（25年6月にCAISIへ改名）  |
| 所管     | 経済産業省・デジタルIPA（情報処理推進機構）内  | 科学・イノベーション・技術省   | 商務省（NIST内）   |
| 所長     | 村上明子  | Adam Beaumont  | Austin Mayron  |
| 職員数・予算 | <b>31人（併任含む*）</b><br>令和6年補正：3.8億円<br>* IPAや理研からの併任  | <b>約200名人以上*（うち専門家は90人）（目標300人）</b><br>初期予算：£1億（約200億円）<br><small>*2025年9月時点、大学教授、元Google、元Open AI等トップ人材を採用<br/>*トップAIモデルへの特権アクセス及びコンピューティングへの優先的アクセス</small>            | <b>30人程度（目標80人）**</b><br>2024年度：予算\$1000万（約15億円）<br><small>**2024年時点情報</small>   |
| 役割     | <ul style="list-style-type: none"> <li>AI事業者ガイドラインの策定支援、米国ガイドラインとの相互比較を実施。</li> <li>評価観点ガイド、レッドチーミング手法ガイドなど実務ドキュメント作成。</li> </ul> | <ul style="list-style-type: none"> <li>フロンティアモデルの評価ベンチマークとテストプラットフォーム構築。</li> <li>AI安全性・セキュリティの最新研究の白書の発行。</li> <li>米国AISIとの共同テスト、カナダAISIとの協力などAISIネットワークのハブ。</li> </ul> | <ul style="list-style-type: none"> <li>OpenAI・Anthropic等との間で、フロンティアモデルの事前評価（プレリリース・テスト）協定。</li> <li>モデル評価・リスク管理の技術スタンダードを策定。</li> <li>Google、Microsoft、Anthropic等200社超を巻き込んだ共同研究。</li> </ul> |

# AISI関係府省庁連絡会議連絡会議非公式会合での議論（R7.5～7月）

令和7年7月11日 内閣府・経済産業省

AISIの安定的・持続的な運営体制の確立に向けた今後の展開について

「AIセーフティ・インスティテュート（AISI）」は、令和6年2月に、岸田総理（当時）の指示を踏まえ、内閣府をはじめとする関係府省庁の協力の下、経済産業省所管の情報処理推進機構（IPA）に設置された。その後、関係府省庁等の依頼にも応じながら、我が国のAIセーフティ/ガバナンスの中心的な機関として、活動を実施してきている。

民間企業や各府省庁等におけるAIの利活用が一層見込まれる中、我が国のAIセーフティの確保に向けてAISIの取組が一層重要になることから、安定的・持続的なAISIの運営体制の確立やこのための資源の確保が重要になってきている。

そこで、経済産業省（IPA所管省庁）からの依頼に基づき、内閣府は、本年6月5日に、「AISI関係府省庁等連絡会議関連・非公式課長級会合」を開催し、AISIの運営に係る12府省庁の課長級職員を中心にAISI運営経費の分担に係る意見交換を実施した。

その結果、各省庁より、以下のような意見があった（詳細は別紙を参照）。

- ✓ AISIの活動については、関連する全府省庁で支えるべき。
- ✓ AISIの運営経費については、安定的・持続的な運営体制の確保に向け、「所管している経済産業省や、新たに設置されるAI戦略本部の事務局となる内閣府が支えるべき」、または、「AI政策の指令塔である内閣府が関係府省庁を取りまとめて検討すべき」という意見もあり。
- ✓ 関係府省庁による分担を検討する場合は、分担省庁の範囲、各省庁の分担額、経費の負担方法等について、整理・検討が必要。
- ✓ 各省庁の調整に時間を要することから、令和8年度要求では暫定的・臨時的措置を検討し、令和9年度要求に向けて時間をかけて関係省庁で議論・合意を行うべき。

関係府省庁からのこういったご意見を受け、令和8年度におけるAISI運営経費については、関係府省庁からの運営経費以外の支援も引き続き募りつつ、AISIが設置されているIPAを所管する経済産業省と、AI戦略本部の事務局となる内閣府において、暫定的・臨時的に予算要求を行うこととする。そのうえで、AISIの安定的・持続的な運営体制の確立に向けて、引き続き検討を進める。その際、以下の点に留意する。

- ① AISIの設置経緯に鑑みれば、AISIの活動に必要な運営経費を特定の府省庁のみに依存し続けるものではなく、中長期的には、経費負担に賛同する関係府省庁も含めて分担することも考えられる。
- ② AISIの活動に必要な運営経費を各府省庁から支出する場合には、関係府省庁が負担すべき明確な理由が必要となる。
- ③ ②に加え、実際に分担するに当たっての要検討事項<sup>※</sup>もあり、関係する府省庁間で丁寧な議論・調整が必要である。

- ④ なお、令和9年度予算要求のみならず、令和8年度要求の観点からも、AI法に基づく新体制でAISIの安定的・持続的な運営体制の確保策の検討を早期に開始し、本年冬頃を目途に一定の方向性を固めていく。

※今後のAISIの中長期計画及びそれに必要な人件費等の確認、各府省庁におけるAISI活動の関係度合いや今般のAI法の成立による関係府省庁の増加を踏まえたAISI運営経費を支える各府省庁の範囲、AISI運営経費確保に向けた各府省庁の事業を踏まえた支援方法（予算支援、職員等の派遣で対応、別事業で支援など）、支援開始時期等

（別紙）

## 第1回 AISI 関係府省庁等連絡会議関連・非公式課長級会合 を踏まえた各府省庁からのご意見の概要

- ✓ AISI の活動については関連する全府省庁で支えるべき。
- ✓ AISI の運営経費については、「所管している省庁である経済産業省と新たに設置される AI 戦略本部の事務局となる内閣府で負担すべき」または、「安定的・継続的な確保に向けて、AI 政策の指令塔である内閣府が関係府省庁を取りまとめて検討すべき」
- ✓ 関係府省庁による分担を検討する場合は、以下の事項についても整理・検討が必要。
  - ① AI 法により関係省庁が増加（現在の AISI 関係府省庁等連絡会議のメンバーは 13 府省庁）することを踏まえた AISI 運営経費の分担省庁の範囲
  - ② AISI からの受益内容を踏まえた 1 省庁あたりの負担額の検討
  - ③ 各省庁からの予算の支出方法の検討（AIS I 運営の中核となる省庁からの支出の検討、枠貸しや補助金、役務契約、別事業の取組や関連職員等の出向・派遣で代用等）
- ✓ また、各府省庁の官房会計課への一報や経費負担に係る根拠の整理を含めたうえで依頼等の手続きも必要であり、特に関係府省庁が負担する明確な理由が必要となる。
- ✓ こういった事項の整理・検討や関係者の了解を取るための手続きに非常に時間を要することが予想され、令和 8 年度概算要求額の決定までに、全府省庁間で調整を完了させることは困難ではないか。
- ✓ このことから、令和 8 年度概算要求にあたっては、暫定的・臨時的な措置として、例えば、以下の取組を実施してはどうか。
  - ① AI 法により内閣府の所掌事務が変更されることを踏まえて、内閣府が主担当して予算要求。
  - ② 各府省庁の職員等を AISI に一時的に派遣・出向させることや、別事業からの AISI への支出策を検討しつつ、内閣府で要求できない府省庁分をまとめて予算要求。
- ✓ そのうえで時間をかけて議論・合意を行い、令和 9 年度要求に間に合うようにさせるべきである。

# 令和7年度補正予算（計：88億円）を活用したAISIの機能強化

AISIが自ら評価ツールを開発、我が国で活用されるAIについて、**セーフティのみならず、セキュリティの観点を含めて分析・評価する能力を持つ。**

(AI評価手法の構築、専用テストベッド・計算資源の整備等)

## 【具体策】

- **AIによるサイバー攻撃への対応**を含めてAISIの既存活動のアップデート
- 日本語に関する出力データの安全性確認を中心に**AI評価手法を開発し**、民間 企業等に提供
- **AIエージェントに係る安全評価ガイドライン**や、適正性を評価するためのチェックツールを開発・提供。
- **産総研とともに、人との協働ロボット等の安全性に係る研究開発、ガイドラインの策定、更に国際標準化に向けた検討を実施。**
- **国内外の民間企業等が開発したAI（フロンティアAIやAIエージェント、フィジカルAI）の安全性・セキュリティを事前に評価**するための調査

# AISIの機能強化に係る今後の主な予定

## 1. 短期的な取組予定

- 内閣府は、R7補正予算をAISIの活動予算として、経済産業省に移し替え（1月30日）、その後、経済産業省はIPAに交付
- 経済産業省（IPA）は、AISIで高額かつ柔軟な年俸支出が可能にできるよう給与体系や各種運用規程の調整
- AISIは、各省庁に出向をお願いしたい人材の人数・特性（独立行政法人の職員含む）を検討。

## 2. 中長期的な取組予定

- 内閣府は、経済産業省や、関係省庁と協力しつつ、中長期的に安定的な財源を確保するための方策の検討（内閣府がAISI業務の共管省庁となることに向けた法改正の調整含む）

# Ⅱ. AIサミットについて

## (1) 人工知能戦略本部 高市総理ご指示 (抄)

信頼できるA Iを世界とともに創りあげるため、『AIサミット』を可能な限り早期に日本で開催すべく、関係省庁を挙げて、取組を進めてください。

## (2) 自民党AI・web3小委員会提言 (抄)

A I S Iを軸とした日本として安全性やセキュリティ確保に係る国際ネットワークをグローバルサウスを含めて構築し、AIサミットの日本での早期に開催も行うことで、日本の「信頼できるA I」を世界に広げていく。

(中略)

5. AIサミットの日本での早期開催を検討すること。

# AIガバナンスを巡る国際動向

## G7及びOECD

**G7広島サミットにて、日本が広島AIプロセス提唱**

安全、安心で信頼できる高度なAIシステムの普及を目的とした初の国際的政策枠組みとして「**広島AIプロセス包括的政策枠組み**」がG7首脳で承認

広島AIプロセスのアウトリーチとして、**広島AIプロセス・フレンズ・グループ創設**

OECD閣僚理事会 生成AIに関するサイドイベントの実施、**OECD AI原則の改定**

広島AIプロセス・フレンズ・グループの初の対面会合が開催

広島AIプロセスに即した指針の整備を規定した**AI法が公布**

(2023.5)

(2023.12)

(2024.5)

(2025.2)

(2025.6)

## AIサミット及びAISI

**AIサミット**  
AI安全性サミット (英国で開催)

**AISI**   
「AI安全性」を具現化するための議論が進み、英・米はAI Safety Instituteを設置

**AIサミット**  
AIソウル・サミット (英・韓共催)

**AISI**   
日本のAI Safety Instituteを設置

**AIサミット**  
AIアクションサミット (仏で開催)

**AISI**   
英国AISIの名称がAI Security Instituteに変更

**AIサミット**  
AIインパクトサミット (印で開催予定)

**AISI**   
米国AISIの名称がthe Center for AI Standards and Innovation (CAISI)に変更

(2023.11)

(2024.2)

(2024.5)

(2025.2)

(2025.6)

(2026.2※予定)

# これまでのAIサミット

- **AI安全性サミット（2023年11月、於：英国ブレッチリー）**：英国（スナク首相（当時））が主催。首脳会合には、岸田総理（当時）がオンライン参加。閣僚会合には、小森総務政務官（当時）が対面参加。我が国を含む29か国がブレッチリー宣言を採択。英国は、同国のAIセーフティ・インスティテュート（AISI）設置を表明。
- **AIソウル・サミット（2024年5月、於：韓国ソウル）**：韓国（尹大統領（当時））及び英国（スナク首相（当時））が共催。オンライン開催となった首脳会合に、岸田総理（当時）はビデオメッセージを送付。閣僚会合には、西田総務政務官が対面参加。我が国を含む27か国がソウル宣言を採択。
- **AIアクション・サミット（2025年2月、於：フランス・パリ）**：フランス（マクロン大統領）が主催、インド（モディ首相）が共同議長。（対面出席しか認められなかったため、）日本からは松本外務政務官（当時）が政府を代表して対面出席。ヴァンス米副大統領、フォン・デア・ライエン欧州委員会委員長を始めとする約90の各国政府代表、約20の国際機関代表及び主要企業の代表が出席。成果文書となる「人類と地球のための包摂的で持続可能なAIに関する声明」が発出（我が国を含む64か国・地域が賛同、米英は反対）。

# 各AIサミットへの政府代表出席者※1 (G7、EU、印、韓、中)

【凡例】◎:首脳・首脳級、○:閣僚、△:閣僚級 (事務方幹部を含む)

|      | ①英国開催<br>2023年11月              | ②韓国開催※2<br>2024年5月    | ③フランス開催<br>2025年2月 |
|------|--------------------------------|-----------------------|--------------------|
| 英国   | ◎ 首相                           | ○ 科学・イノベーション・技術担当相    | ○ 科学・イノベーション・技術担当相 |
| 米国   | ◎ 副大統領                         | △ 重要・振興技術担当副特使        | ◎ 副大統領             |
| フランス | ○ 経済・財務・産業・デジタル主権相             | △ 開発・国際連携担当<br>国務長官   | ◎ 大統領              |
| カナダ  | ○ イノベーション・科学・産業相               | △ イノベーション・科学・産業省 副次官補 | ◎ 首相               |
| イタリア | ◎ 首相                           | △ 閣僚級                 | ○ 企業・メイドインイタリアー相   |
| ドイツ  | ◎ 副首相兼 経済・気候保護大臣、<br>デジタル・交通大臣 | △ デジタル・交通省<br>国家次官    | ◎ 首相               |
| EU   | ◎ 欧州委員会<br>委員長                 | △ 欧州委員                | ◎ 欧州委員会<br>委員長     |
| インド  | ○ 電子・情報技術<br>担当相               | △ 電子・情報技術省<br>次官補     | ◎ 首相               |
| 韓国   | ○ 科学技術情報通信<br>部長官              | ◎ 大統領                 | ○ 科学技術情報通信<br>部長官  |
| 中国   | △ 科学技術部副部長                     | 閣僚以上の出席なし             | ◎ 国務院副総理           |
| 日本   | △ 総務大臣政務官                      | △ 総務大臣政務官             | △ 外務大臣政務官          |

※1) 対面での出席状況

※2) 韓国開催では、首脳会合をオンラインで、閣僚会合を対面で実施する形態がとられた

# インド・A I インプクト・サミット

## 日程・場所

- ◆ 2026年2月19日～20日
- ◆ インド（ニューデリー）



## 概要

- ◆ 人間、地球、発展の3本柱のもと、7つのテーマ（人材、多様性、安全で信頼できるA I、レジリエンス、科学、A I 資源の公平な利用、公共の利益）について議論。
- ◆ モディ首相が基調演説。石破総理も招待されている（本年8月の日印首脳共同声明に記載）

### 【背景】

- ◆ インド政府は、A I 国家戦略を策定し、ヘルスケア、農業、教育、スマートシティ、交通・輸送に焦点を当て、社会課題の解決のためにA I を活用することを掲げており、インドで実現した解決策を発展途上国・新興経済圏で展開することを目指すなど、A I 政策に精力的に取り組んでいる。
- ◆ 同共同声明では、日印A I 協カイニシアティブ（J A I）を立ち上げ、A I に関する相互補完的な協力を推進し、A I を活用した経済社会課題への解決策を共創することを目指す。

## 開催実績

- ◆ 2023年11月 A I 安全性サミット（英国ブレッチリー）…29カ国等による共同宣言
- ◆ 2024年5月 A I ソウル・サミット（ソウル）… 27カ国等による閣僚声明
- ◆ 2025年2月 A I アクション・サミット（パリ）… 63カ国等による宣言文書

# AIを巡る国際動向と日本の役割

非規制  
輸出促進



- 2025年7月、「AI競争に勝つ：アメリカのAI行動計画」を発表。①AIイノベーションの加速、②AIインフラの整備、③国際的な外交・安全保障での主導の3本柱で構成する包括的国家戦略。
- オープンソース・オープンウェイトAI支援や、イノベーション促進と米国発モデルの国際標準化（AIスタック輸出、オープン化）を重視。データセンターや半導体製造施設の建設を加速してAIインフラを整備し、規模の経済達成を目指す。

自主的対応  
の促進  
(ソフトロー)



- 2023年G7議長国下で「広島AIプロセス」を立上げ、安全・安心で信頼できるAIを実現するためのルール作りを推進。「国際指針」と「国際行動規範」を含む「包括的政策枠組」を策定。
- 「国際行動規範」の実施に向け、2025年2月からAI開発者による遵守状況のための報告枠組をOECDが運用開始。フレンズグループを通じて理念の共有を進め、参加国・地域が56に拡大。
- 2025年5月にAI法が成立し、イノベーション促進とリスク対応のバランスを追求。2025年目途でAI基本計画及び適正性確保のための指針を策定予定。

リスク対応  
の法規制  
(ハードロー)



- 基本的人権の保護を重視。欧州AI法に基づく規制（リスクの程度によりAIを4つに分類し、それに応じて禁止事項や義務を規定）と並行して、イノベーションも推進。
- 2025年4月、欧州委員会は、欧州がAIの世界的リーダーとなることを目的として「AI大陸行動計画」を発表。①AIデータ・インフラ構築、②高品質データへのアクセス拡大、③イノベーション促進と戦略分野導入加速、④AI人材強化、⑤規制遵守の促進・簡素化の5つの柱から構成。

国家管理



- 2024年9月、国連の「グローバル・デジタル・コンパクト（GDC）」のビジョン実現のための「AIに係る能力構築に関する国際協力に向けたフレンズグループ」を立上げ。
- 2025年7月、世界AI大会を開催。「AIグローバルガバナンス行動計画」を発表。「世界AI協力組織」（本部：上海）の設立を提唱。
- 「行動計画」では、国連の下でのガバナンス・メカニズムの設立等を含む13項目が盛り込まれ、国際協力の重視を強調。
- 2025年8月、「『AI+』行動のさらなる実施に関する意見」を発表。2035年までの三段階目標を掲げ、AIを社会・経済全域に深く融合し新質生産力と智能社会を育成する行動提言。

# AIサミットの日本開催に係る今後の主な予定

- インド開催（本年2月）の次としては、スイスが2027年に開催する旨、表明済
- 日本として、**2028年以降の開催に向けて、内外で調整を進める。インドサミットでの他国の開催希望等に係る情報収集を基に、具体化に向けて検討を開始予定**

注：他にも、開催検討中の国ありとの情報も

## （主な検討事項）

### 1. 開催の目的・意義、期待される効果

#### □ 目的・意義

- ✓ AIは今や国力を左右する技術として世界的な開発競争が激化し、特に米中間における覇権争いが顕在化
- ✓ かかる状況下、日本が「世界で最もAIを開発・活用しやすい国」を実現していくためには、日本がAIサミット議長国として、国際社会においてリーダーシップを発揮し、プレゼンスを発揮することは極めて重要

#### □ 期待される効果

- ✓ AI協力や政府間・産学官間の連携強化、広島AIプロセス（HAIP）の普及・拡大を通じて、国際社会における日本のプレゼンスを強化することで、信頼できるAIエコシステムの構築に向けて国際的な議論を主導
- ✓ AIサミット開催を機に、内外からの民間の参画を確保しつつ、企業や人材、投資マネーを海外から呼び込み、日本の勝ち筋となりうるAI分野（フィジカルAI、Vertical AI、AI for Science 等）への投資促進による開発力強化、新たな市場・イノベーションの創出等を通じ、日本経済を活性化させる
- ✓ サミット開催を通じて、国民のAIに対する関心の喚起や理解促進を図ることで、国民のAIの利活用の促進・定着の機会とする

## (主な検討事項 (続き) )

以下の項目については、検討具体化の過程で精査・調整していく。

### 2. 予算・財源 (内閣府)

- ✓ 総費用見積もり (警備、施設、交通、宿泊、人件費、広報等)
- ✓ 予算・財源の確保

### 3. 議題・コンテンツ・イベント (内閣府、総務省、経産省、外務省、デジタル庁、関係省庁)

- ✓ 取り上げるべき議題やコンテンツの設定、優先順位付け
- ✓ メインイベント、サイドイベント等、各イベントの概要と位置づけ

### 4. 開催地・時期 (内閣府)

- ✓ 開催都市の選定 (インフラ、アクセス、国際会議の開催実績等)
- ✓ 開催時期の決定 (国際イベントや国内政治日程との重複回避)

### 5. 参加者 (内閣府、総務省、経産省、外務省、他)

- ✓ 招待する国や国際機関の範囲、基準、参加者レベルの決定
- ✓ 国内産業界との連携 (国内外の民間企業をどこまで呼ぶか等)

# 參考資料

# 人工知能戦略本部 総理ご指示 (2025.12.19)

- A I は、産業競争力や安全保障に直結。信頼できる A I による日本再起を実現するため、以下を指示 (以下、抜粋)
- 第一に、『ガバメント A I 源内』の徹底活用です。2026年5月から10万人以上の政府の職員が活用できるようになります。A I 源内の活用により、創造的に業務を行い、国民の皆様へ信頼できる A I の意義を示してください。
  - **第二に、A I セーフティ・インスティテュートの抜本的強化**です。A I の安全性に対する不安が高まる中、**英国並みの200人体制を目指して**、小野田大臣と赤澤経済産業大臣は、**全省庁、産学から人材を集結させ、A I セキュリティに万全を期してください**。
  - 第三に、A I ロボットを始めとしたフィジカル A I に不可欠な信頼できる国産の汎用基盤モデルの開発です。赤澤経済産業大臣は、質の高い産業データを日本の競争力の中核に位置づけ、意欲ある企業としっかりと連携し、開発を進めてください。
  - 第四に、信頼できる A I による社会課題を解決できるサービスの開発・導入です。今般の経済対策で、4000億円以上の A I 関連施策を措置したところです。これらを活用して、地域や中小企業の成長戦略を実現するとともに、世界各国にサービスを展開してください。
  - **第五に、信頼できる A I を世界とともに創りあげるため、『A I サミット』を可能な限り早期に日本で開催**すべく、関係省庁を挙げて、取組を進めてください。
  - 第六に、信頼できる A I を創る官民投資を日本成長戦略における危機管理投資として、力強く推進してください。政府としては、投資の予見性を高めるため、当面、1兆円超を A I 関連施策の推進に投資してまいります。また、大胆な投資促進税制を創設し、研究開発税制を深堀りします。これらの政府のコミットを、それぞれが所管する企業の皆様と共有し、政府の取組に呼応していただき A I 投資を強力に推進してください。
  - 結びに、A I をめぐる動向の変化は非常に速いです。小野田大臣は、今回の計画に基づく、官民の取組を直ちに実施するとともに、来年の夏を目指して、投資目標、制度改革、人づくり、データ戦略などを含む官民投資ロードマップを盛り込む形で、『A I 基本計画』を更に充実させてください。以上です。

# 自民党デジタル社会推進本部 AI・web3小委員会提言(R7.12.19) ～A I セーフティ・インスティテュート (A I S I) の機能強化に係る緊急提言～

我が国のA Iに関するイノベーションの促進とリスク管理を両立させるためには、「信頼できるA I」の利活用及び開発の中核となる**A I セーフティ・インスティテュート (A I S I) の抜本的な機能強化**を行わなければならない。**A I モデルの技術的評価、広範な適正性に係る評価、セキュリティ面での対策を実行できる体制の構築**を行う必要がある。

このA I S Iの機能拡充及び機能強化においては、政府を挙げた取り組みが必要であり、特に以下の二つの目標を早急に達成しなければならない。

まず、**世界のA I 開発事業者から、フロンティアモデルの発表、提供に先立ち、事前評価の実施を委託される機関**となる。当面は他の独立行政法人や民間機関等との連携の下、将来的には自ら、技術評価能力の強化とそのための研究開発基盤を構築する。世界の主要開発事業者との協力協定を積極的に締結する。

また、**顕在化する「A Iによるサイバー攻撃とA Iによる防御」に対応できるよう、諸外国のA I S Iや内外の関係機関と連携しサイバーセキュリティの評価機能を強化**する。サイバーセキュリティに関する専門人材をはじめ人的基盤を強化する。

A I S Iを軸とした日本として安全性やセキュリティ確保に係る国際ネットワークをグローバルサウスを含めて構築し、AIサミットの日本での早期に開催も行うことで、日本の「信頼できるA I」を世界に広げていく。

そこで、A I・w e b 3小委員会・デジタル社会推進本部として、A I S Iの機能強化について、下記のとおり緊急提言する。

# 自民党デジタル社会推進本部 AI・web3小委員会提言(R7.12.19) ～A I セーフティ・インスティテュート (A I S I) の機能強化に係る緊急提言～

1. 政府は、英国のA I S Iをベンチマークに、質・量ともにA I S Iの人員・体制強化を図ること。まずは令和7年度補正予算を的確に執行し、早急に現行の30名から陣容を拡充し、60名体制を目指すこと。
2. A I はあらゆる行政分野に関係しており、各省庁でA I 安全性やA I セキュリティの専門家の育成が必要不可欠である。そこで、全省庁がA I S Iに出向者を出すこと。特にデジタル政策に関係する省庁については複数名出すこと。
3. A I S I が自らの権能で国内外の有能なA I 関連の専門家を柔軟に雇用できるよう、国家公務員より高額かつ柔軟な年俸支出も可能となるようにすること。
4. A I S I の拡充する業務の適切な執行と常勤常駐含めた体制整備及びそのための財政基盤を確保するため、A I 政策の司令塔である内閣府がA I S I 業務の共管省庁となること、また内閣府及び経済産業省から運営費交付金を安定的に支出すること。
5. A I サミットの日本での早期開催を検討すること。