

AI セーフティ ファクトシート 2024

Factsheet of AI Safety in Japan 2024

2025 年 2 月 5 日

AI セーフティ・インスティテュート (AISI) 事務局

目次

| | | |
|-------|--|---|
| 1 | 主要な AI 戦略、アクションプラン、制度 | 1 |
| 1.1 | 原則、戦略 | 1 |
| 1.1.1 | 1) 人間中心の AI 社会原則 (2019 年/統合イノベーション戦略推進会議) | 1 |
| 1.1.1 | 2) 統合イノベーション戦略 2024 (2024 年/内閣府) | 1 |
| 1.2 | 原則や戦略に関する国際合意や主要レポート | 1 |
| 1.2.1 | 1) OECD AI principle (2019 年/OECD) | 1 |
| 1.2.1 | 2) UNESCO Ethics of Artificial Intelligence (2021 年/UNESCO) | 2 |
| 1.2.1 | 3) 広島 AI プロセス (2023 年/G7) | 2 |
| 1.2.1 | 4) Final Report of the High-level Advisory Body on Artificial Intelligence - Governing AI for Humanity (2024 年/国際連合) | 3 |
| 1.2.1 | 5) UN Global Digital Compact (2024 年/国際連合) | 3 |
| 1.3 | 法令 | 3 |
| 1.3.1 | 1) AI 関連法 | 3 |
| 1.3.1 | 2) デジタル関連法 | 4 |
| 1.3.1 | 3) 個人情報・知的財産関連法 | 4 |
| 1.3.1 | 4) 自動運転関係の法令 | 5 |
| 1.3.1 | 5) ドローン関係の法令 | 6 |
| 1.3.1 | 6) 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律 | 6 |
| 1.3.1 | 7) サイバーセキュリティ基本法 | 6 |
| 1.4 | 指針、ガイドライン | 7 |
| 1.4.1 | 1) AI 事業者ガイドライン (2024 年/総務省、経済産業省) | 7 |
| 1.4.1 | 2) AI セーフティに関する評価観点ガイド (2024 年/AISI) | 7 |
| 1.4.1 | 3) AI セーフティに関するレッドチーミング手法ガイド (2024 年/AISI) | 8 |
| 1.4.1 | 4) AI 時代の知的財産権検討会「中間とりまとめ」(2024 年/内閣府知的財産戦略推進事務局) | 8 |
| 1.4.1 | 5) AI と著作権に関する考え方について(2024 年 3 月/文化審議会著作権分科会法制度小委員会) | 8 |
| 1.5 | その他の政府機関の AI 関連ガイドライン | 8 |
| 1.5.1 | 1) 機械学習品質マネジメントガイドライン (2020 年/産業技術総合研究所) | 8 |
| 1.5.1 | 2) 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 (2024 年/文部科学省) | 9 |
| 1.5.1 | 3) コンテンツ制作のための生成 AI 利活用ガイドブック (2024 年/経済産 | |

| | |
|---|----|
| 業省) | 9 |
| 4) テキスト生成 AI 利活用におけるリスクへの対策ガイドブック (α 版) (2024 年/デジタル庁) | 9 |
| 5) 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 (2024 年/厚生労働省) | 9 |
| 6) 農業分野における AI・データに関する契約ガイドライン (2024 年/農林 水産省) | 10 |
| 1.6 民間の主な AI 関連ガイドライン | 10 |
| 1) FUDA 生成 AI ガイドライン (2024 年/一般社団法人金融データ活用推進 協会) | 10 |
| 2) ヘルスケア事業者のための生成 AI 活用ガイド (2024 年/日本デジタル ヘルス・アライアンス) | 10 |
| 3) 医療・ヘルスケア分野における生成 AI 利用ガイドライン (2024 年/非 営利共益法人 医療 AI プラットフォーム技術研究組合) | 11 |
| 2 主要な組織、体制 | 11 |
| 1) AI 戦略本部 | 11 |
| 2) AI セーフティ・インスティテュート (AISI: エイシー) | 11 |
| 3) GPAI 東京専門家支援センター (GPAI: ジーペイ) | 11 |

1 主要なAI戦略、アクションプラン、制度

本ファクトシートは、AI セーフティを検討するにあたり公開された文書や設立された新たな組織および体制を中心に国内外の事実関係を記載したものである。

1.1 原則、戦略

1) 人間中心の AI 社会原則¹ (2019 年/統合イノベーション戦略推進会議)

AI 戦略実行会議の下、AI をより良い形で社会実装し共有するための基本原則を検討し、AI 戦略に反映させることを目的として設置され、原則が策定された。このような考察の下で、特定の技術やシステムが「AI」かを区別するのではなく、広く「高度に複雑な情報システム一般²」がこのような特徴と課題を内包すると捉え、社会に与える影響を議論した上で、AI 社会原則の一つの在り方を提示し、AI の研究開発や社会実装において考慮すべき問題が列挙されている。

2) 統合イノベーション戦略 2024 (2024 年/内閣府)³

「先端科学技術の戦略的な推進」、「知の基盤（研究力）と人材育成の強化」、「イノベーション・エコシステムの形成」の3つの基軸で政策を推進していくとともに、3つの強化方策として、「重要技術に関する統合的な戦略」、「グローバルな視点での連携強化」、「AI 分野の競争力強化と安全・安心の確保」が推進される。

1.2 原則や戦略に関する国際合意や主要レポート

1) OECD AI principle (2019 年/OECD)⁴

OECD AI 原則は、AI に関する初の政府間基準である。人権と民主的価値を尊重する革新的で信頼性の高い AI の推進に貢献してきている。2019 年 5 月に採択され、後述の広島 AI プロセスを踏まえ、2024 年 5 月に改訂された。この原則は、政策立案者と AI 関係者に実用的かつ柔軟な指針を提供する 5 つの価値観に基づく原則と 5 つの加盟国政府等が政策等に反映させるべき勧告で構成さ

¹ <https://www8.cao.go.jp/cstp/ai/aigensoku.pdf>

² この宣言の中では、AI のことを「高度に複雑な情報収集一般」と同一視していく。

³ https://www8.cao.go.jp/cstp/tougosenryaku/togo2024_zentai.pdf

⁴ <https://www.oecd.org/en/topics/ai-principles.html>

れている。

2) UNESCO Ethics of Artificial Intelligence (2021年/UNESCO) ⁵

ユネスコで 2021 年 11 月、AI 倫理に関する世界初のグローバルスタンダードとなる「人工知能の倫理に関する勧告」が採択された。人権と尊厳の保護は勧告の要であり、透明性や公平性といった基本原則の推進を基盤とし、常に AI システムの人間による監視の重要性を念頭に置いている。

3) 広島 AI プロセス (2023 年/G7) ⁶

2023 年 5 月に開催された G7 広島サミットの結果を踏まえ、その急速な発展と普及が国際社会全体の重要な課題となっている生成 AI について議論するために、2023 年 5 月に立ち上げられた。

全ての AI 関係者向けの 広島プロセス国際指針 (2023 年/G7) ⁷

2023 年 10 月に公表された「高度な AI システムを開発する組織向けの広島プロセス国際指針」を基礎として、安全、安心で信頼できる AI の実現に向けて、AI ライフサイクル全体の関係者それぞれが異なる責任を持つという認識の下、同指針の 11 項目を、高度な AI システムの設計、開発、導入、提供及び利用に関わる全ての関係者に適宜適用し得るものとして整理した上で、偽情報の拡散等の AI 固有リスクに関するデジタルリテラシーの向上や脆弱性の検知への協力と情報共有等、利用者に関わる内容が 12 番目の項目として追加されている。

高度な AI システムを開発する組織向けの 広島プロセス国際行動規範 (2023 年/G7) ⁸

高度な AI システムを開発する組織向けの広島プロセス国際行動規範は、高度な AI システムを開発する組織向けの広島プロセス国際指針に基づき、安全、安心で信頼できる AI を世界に普及させることを目的とし、最先端の

⁵ <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>

⁶ <https://www.soumu.go.jp/hiroshimaaiprocess/>

⁷

https://www8.cao.go.jp/cstp/ai/ai_senryaku/7kai/11hiroshimaaipurosesu.pdf

⁸ <https://www.soumu.go.jp/hiroshimaaiprocess/documents.html>

基盤モデル及び生成 AI システムを含む、最も高度な AI システムを開発する組織による行動のための自主的な手引きとして提供される。

国際行動規範の「報告枠組み」に係る合意（2024 年/G7）⁹

「国際行動規範」を自主的に遵守する AI 開発企業等による履行状況を確認するための手法の基本的な運用方法及び質問票に関して、2024 年 12 月に合意された。「国際行動規範」に沿って作成された AI 開発企業等への質問票を OECD の Web サイト上で公開し、企業が回答する。「報告枠組み」の運用開始は、2025 年 2 月以降の予定である。

4) Final Report of the High-level Advisory Body on Artificial Intelligence – Governing AI for Humanity (2024 年/国際連合)¹⁰

国連事務総長直属の「AI に関するハイレベル諮問委員会」の最終報告書「人類のための AI ガバナンス」が 2024 年 9 月に発表された。報告書では、AI の国際ガバナンスの促進に関する提言が記載されている。

5) UN Global Digital Compact (2024 年/国際連合)¹¹

2024 年 9 月 22 日、「未来サミット」の成果文書である「未来のための約束」の附属文書として、すべての人々にとって包摂的かつオープンで持続可能、公平、安全で安心なデジタルの未来を推進するための目的、原則及び行動を定めるグローバル・デジタル・コンパクトが採択された。

1.3 法令

日本は、ガイドラインを中心としたソフトローで AI セーフティが推進されてきた。一方で、法令の必要性、法律を策定する場合の対象や実施事項なども検討されている。

1) AI 関連法

a) AI 制度研究会¹²

2024 年 7 月に法令の必要性を含めた AI 制度のあり方を議論する場として

⁹ https://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000306.html

¹⁰ <https://www.un.org/en/ai-advisory-body>

¹¹ <https://www.un.org/techenvoy/global-digital-compact>

¹² https://www8.cao.go.jp/cstp/ai/ai_kenkyu/ai_kenkyu.html

内閣府に AI 制度研究会が設置された。座長は東京大学大学院工学系研究科の松尾教授で、2024 年 12 月には、中間報告（案）として AI 制度のあり方についての方向性が取りまとめられた。

2) デジタル関連法

a) デジタル社会形成基本法¹³

デジタル社会の形成が、我が国の国際競争力の強化及び国民の利便性の向上に資するとともに、急速な少子高齢化の進展への対応その他の我が国が直面する課題を解決する上で極めて重要であることに鑑み、デジタル社会の形成に関する施策を迅速かつ重点的に推進し、もって我が国経済の持続的かつ健全な発展と国民の幸福な生活の実現に寄与するため、デジタル社会の形成に関し、基本理念及び施策の策定に係る基本方針、国、地方公共団体及び事業者の責務、デジタル庁の設置並びに重点計画の作成について定められた。

b) デジタル原則に照らした規制の一括見直しプラン¹⁴

我が国がデジタル化を図っていく上での指針となるべき「構造改革のためのデジタル原則」を策定し、当該原則に適合したデジタル社会の実現を目指して、各府省庁とも連携し、構造改革に取り組んでいく計画が示された。

3) 個人情報・知的財産関連法

a) 個人情報保護法等¹⁵

個人情報の有用性に配慮しながら、個人の権利や利益を守ることを目的とした法律である。この法律は、デジタル社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関

¹³ <https://laws.e-gov.go.jp/law/503AC0000000035>

¹⁴ https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_re_sources/cb5865d2-8031-4595-8930-8761fb6bbe10/e3650360/20220603_meeting_administrative_research_outline_07.pdf

¹⁵ <https://www.ppc.go.jp/personalinfo/>

し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにし、個人情報を取り扱う事業者及び行政機関等についてこれらの特性に応じて遵守すべき義務等を定めるとともに、個人情報保護委員会を設置することにより、行政機関等の事務及び事業の適正かつ円滑な運営を図り、並びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とされる。

b) 知的財産に関する法令

特許法¹⁶：発明の保護及び利用を図ることにより、発明を奨励し、もつて産業の発達に寄与することを目的とされる。

著作権法¹⁷：著作物並びに実演、レコード、放送及び有線放送に関し著作者の権利及びこれに隣接する権利を定め、これらの文化的所産の公正な利用に留意しつつ、著作者等の権利の保護を図り、もつて文化の発展に寄与することを目的としている。

商標法¹⁸：商標を保護することにより、商標の使用をする者の業務上の信用の維持を図り、もつて産業の発達に寄与し、あわせて需要者の利益を保護することを目的とされる。

意匠法¹⁹：意匠の保護及び利用を図ることにより、意匠の創作を奨励し、もつて産業の発達に寄与することを目的とされる。

不正競争防止法²⁰：事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もつて国民経済の健全な発展に寄与することを目的とされる。

4) 自動運転関係の法令

道路交通法²¹：道路における危険を防止し、その他交通の安全と円滑を

¹⁶ <https://laws.e-gov.go.jp/law/334AC0000000121>

¹⁷ <https://laws.e-gov.go.jp/law/345AC0000000048>

¹⁸ <https://laws.e-gov.go.jp/law/334AC0000000127>

¹⁹ <https://laws.e-gov.go.jp/law/334AC0000000125>

²⁰ <https://laws.e-gov.go.jp/law/405AC0000000047>

²¹ <https://laws.e-gov.go.jp/law/335AC0000000105>

図り、及び道路の交通に起因する障害の防止に資することを目的とした法令。

道路運送車両法²²：道路運送車両に関し、所有権についての公証等を行い、並びに安全性の確保及び公害の防止その他の環境の保全並びに整備についての技術の向上を図り、併せて自動車の整備事業の健全な発達に資することにより、公共の福祉を増進することを目的とされる。

5) ドローン関係の法令

航空法²³：航空機の航行の安全、航空機による運送事業などの秩序の確立を目的とする法令。航空機の航行の安全及び航空機の航行に起因する障害の防止を図るための方法を定め、航空機を運航して営む事業の適正かつ合理的な運営を確保して輸送の安全を確保するとともにその利用者の利便の増進を図り、並びに航空の脱炭素化を推進するための措置を講じ、あわせて無人航空機の飛行における遵守事項等を定めてその飛行の安全の確保を図ることにより、航空の発達を図り、もつて公共の福祉を増進することを目的とされる。

航空法その他、小型無人機等禁止法、道路交通法、民法、電波法、都道府県の条例等によって規制される。

6) 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律²⁴

特定電気通信による情報の流通によって権利の侵害があった場合について、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示を請求する権利について定めるとともに、発信者情報開示命令事件に関する裁判手続に関し必要な事項を定める目的とする法令。

7) サイバーセキュリティ基本法²⁵

我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事

²² <https://laws.e-gov.go.jp/law/326AC0000000185>

²³ <https://laws.e-gov.go.jp/law/327AC0000000231>

²⁴ <https://laws.e-gov.go.jp/law/413AC0000000137>

²⁵ <https://laws.e-gov.go.jp/law/426AC1000000104>

項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、同法と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とされる。

サイバー基本法その他、刑法、不正アクセス行為の禁止等に関する法律等によって規制される。

1.4 指針、ガイドライン

1) AI 事業者ガイドライン（2024年/総務省、経済産業省）²⁶

AIの安全安心な活用が促進されるよう、我が国におけるAIガバナンスの統一的な指針が2024年4月に示されている。これにより、様々な事業活動においてAIを活用する者が、国際的な動向及びステークホルダーの懸念を踏まえたAIのリスクを正しく認識し、必要となる対策をAIのライフサイクル全体で自主的に実行できるように後押しし、互いに関係者と連携しながら「共通の指針」と各主体に重要となる事項及びAIガバナンスを実践することを通して、イノベーションの促進とライフサイクルにわたるリスクの緩和を両立する枠組みを、積極的に共創していくことを目指している。

2) AI セーフティ²⁷に関する評価観点ガイド（2024年/AISI）

AIシステムの開発や提供に携わる者がAIセーフティ評価を実施する際に参照できる基本的な考え方を提示している。本書の作成に際しては、日本においてAIを活用する事業者が適切にAIを活用するための指針を示す「AI事業者ガイドライン」を参考としている。

²⁶ <https://www.meti.go.jp/press/2024/04/20240419004/20240419004-1.pdf>

²⁷ 人間中心の考え方をもとに、AI活用に伴う社会的リスクを低減させるための安全性・公平性、個人情報等の不適正な利用等を防止するためのプライバシー保護、AIシステムの脆弱性等や外部からの攻撃等のリスクに対応するためのセキュリティ確保、システムの検証可能性を確保し適切な情報提供を行うための透明性が保たれた状態

3) AI セーフティに関するレッドチーミング手法ガイド (2024 年/AISI) ²⁸

AI システムの開発や提供に携わる者が対象の AI システムに施したリスクへの対策を、攻撃者 (AI システムの悪用や破壊を意図する者) の視点から評価するためのレッドチーミング手法に関する基本的な考慮事項を示している。

4) AI 時代の知的財産権検討会「中間とりまとめ」²⁹ (2024 年/内閣府知的財産戦略推進事務局)

「AI 時代の知的財産権検討会 中間とりまとめ」(2024 年 5 月) は、生成 AI と知的財産権の関係についてガイドラインとしての役割を果たす資料である。「中間とりまとめ」のポイントを、権利者の視点から紹介、解説した「権利者のための手引き³⁰」が 2024 年 11 月に公表されている。

5) AI と著作権に関する考え方について³¹ (2024 年 3 月/文化審議会著作権分科会法制度小委員会)

生成 AI と著作権の関係についてクリエイターや AI 開発事業者等の懸念の払拭に向け、文化審議会著作権分科会法制度小委員会において議論し、現行の著作権法における考え方を整理したものである。また、本文書の内容を踏まえ、関係当事者の立場ごとにわかりやすくまとめた「AI と著作権に関するチェックリスト&ガイダンス」が 2024 年 7 月に文化庁より公表されている。

1.5 その他の政府機関の AI 関連ガイドライン

1) 機械学習品質マネジメントガイドライン (2020 年/産業技術総合研究所) ³²

本ガイドラインは、機械学習を利用したシステム、特にその中に含まれる機械学習で実装されたソフトウェアコンポーネント (機械学習要素) の品質

²⁸ https://www.ipa.go.jp/digital/ai/begoj90000004szb-att/ai_safety_rt_v1.00_ja.pdf

²⁹ https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2024/0528_ai.pdf

³⁰ https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2024/2411_tebiki.pdf

³¹ <https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html>

³² <https://www.digiarc.aist.go.jp/publication/aigq/>

に関する基準と達成目標を定めることにより、企業が自ら構築した AI を利用するシステムの品質を測定し向上させ、また AI の誤判断による事故や経済損失などを減少させる一助となることを目的とされたものである。2020 年の初版以降、2023 年 12 月に日本語第 4 版、2023 年 1 月に英語第 3 版が公開されている。

2) 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³³ (2024 年/文部科学省)

2024 年 12 月に発行された本ガイドラインは、教職員や教育委員会等の学校教育関係者を主たる読み手として、学校現場における生成 AI の適切な利活用を実現するための参考資料となるよう、利活用に当たっての基本的な考え方や押さえるべきポイントをまとめたものである。生成 AI の概要、基本的な考え方を示した上で、学校現場において押さえておくべきポイントとして、利活用する場面や主体に応じた留意点について、現時点の知見が基に可能な限り具体的に示されている。

3) コンテンツ制作のための生成 AI 利活用ガイドブック³⁴ (2024 年/経済産業省)

2024 年 7 月に発行された本文書は、生成 AI を利用したコンテンツ制作の企画・検討や、利用する生成 AI サービスの選択、リーガルチェック、さらに生成 AI の利用に関する社内ガイドラインの作成などへの活用が推奨される。

4) テキスト生成 AI 利活用におけるリスクへの対策ガイドブック (α 版)³⁵ (2024 年/デジタル庁)

2024 年 6 月に発行された本文書には、広島 AI プロセスや AI 事業者ガイドラインを踏まえ、行政業務において生成 AI を用いる際の指針として、生成 AI の中でもテキスト生成 AI とその利活用に焦点を当て、政府調達において考慮する点について、より具体的なリスクと対策が記載されている。

5) 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 (2024

³³ https://www.mext.go.jp/content/20241226-mxt_shuukyo02-000030823_001.pdf

³⁴

https://www.meti.go.jp/policy/mono_info_service/contents/aiguidebook.html

³⁵ <https://www.digital.go.jp/resources/generalitve-ai-guidebook>

年/厚生労働省)³⁶

民間企業等と共同で AI を活用した医療機器の研究開発等を実施するにあたり、個人情報保護法の下、医療機関等において診療で得られ、既に保管されている医療情報を利活用する際の法的・技術的な取扱いについて示している。医療情報は、一般的に、個人情報保護法上の個人データに該当する上、同法上の要配慮個人情報にも該当し、極めて機微な性質を有していることから、個人情報保護法で規定する仮名加工情報を作成し、運用するにあたって不可欠である実践的な指針として、また、医療情報の利活用に対する社会的な信頼の確保に貢献することを目的としている。

6) 農業分野における AI・データに関する契約ガイドライン (2024 年/農林水産省)³⁷

農業関係者等（農業関係者、農業指導普及員等）が持つノウハウ等を活用して、AI などを利用したシステムやサービスに反映させたり、あるいはノウハウを含むデータを用いて、システムやサービスを利用したりする場合の取決めに関する留意事項や条項例が示されている。また、スマート農業全般で用いられることが想定される農業関係者が持つデータについて、その利活用のために研究機関や企業等、プラットフォーム事業者などに提供する際の農業関係者の利益を配慮した条項例や留意事項が示されたものである。

1.6 民間の主な AI 関連ガイドライン

1) FUDA 生成 AI ガイドライン (2024 年/一般社団法人金融データ活用推進協会)³⁸

生成 AI 独自の特徴とリスクの整理に加え、金融機関において生成 AI の利活用を推進するために実践的ルールを作る上で留意すべき AI 原則および法規制まで網羅的に取りまとめ解説されたものである。

2) ヘルスケア事業者のための生成 AI 活用ガイド³⁹ (2024 年/日本デジタルヘルス・アライアンス)

本ガイドにおいては、まずはヘルスケア領域で最も広く活用されていると考えられる文章（テキスト）生成 AI を対象とされる。なお、本ガイドは今

³⁶ <https://www.mhlw.go.jp/content/001310044.pdf>

³⁷ <https://www.maff.go.jp/j/kanbo/tizai/brand/keiyaku.html>

³⁸ <https://www.fdua.org/activities/generativeai>

³⁹ <https://www.jri.co.jp/page.jsp?id=107056>

後技術やサービスの進展を踏まえて随時アップデートを行う予定とされている。

3) 医療・ヘルスケア分野における生成 AI 利用ガイドライン⁴⁰ (2024 年/非営利 共益法人 医療 AI プラットフォーム技術研究組合)

生成 AI の医療現場における利用にともなうリスクと対策を示し、医療現場における生成 AI の導入と利用を促進することを目的としている。本ガイドラインは、医療機関・薬局等で生成 AI を利用する人、もしくは生成 AI の開発に携わる人を対象読者として想定されている。

2 主要な組織、体制

1) AI 戦略本部⁴¹

2024 年 12 月 26 日に AI 制度研究会によって公表された『中間とりまとめ (案)』に対する議論を踏まえ、石破総理より全閣僚からなる『AI 戦略本部』の設置が指示された。各省庁や自治体において、インフラなどにおける AI の導入実態を把握し、ガイドラインの見直しなどの対応が進められていく。

2) AI セーフティ・インスティテュート⁴² (AISI : エイシー)

2024 年 2 月に 10 府省、5 政府系機関が共同して AI セーフティ・インスティテュートを設立した。AISI は政府の AI セーフティに関する取り組みを支援する機関である。また、幅広く情報収集をしていることから、日本国内における AI セーフティに関する情報のハブとなる役割が期待されている。さらに AI セーフティに関しては国際的な取り組みが非常に速いスピードで進む中で、国際的な場への参加と貢献を期待されている。

3) GPAI 東京専門家支援センター⁴³ (GPAI : ジーペイ)

2024 年 7 月に GPAI (THE GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE) 東京専門家支援センターが設立された。AI に関する優先課題に取り組む産業界、市民社会、政府、国際機関、学界の専門家による研究やプロジェクトの

⁴⁰ https://haip-cip.org/assets/documents/nr_20241002_02.pdf

⁴¹ <https://www.kantei.go.jp/jp/103/actions/202412/26ai.html>

⁴² <https://aisi.go.jp/>

⁴³ <https://www2.nict.go.jp/gpai-tokyo-esc/>

運営・管理を支援する機関である。