

AIホワイトペーパー 2024 ステージIIにおける新戦略 — 世界—AIフレンドリーな国へ—



生成AIを用いて作成した画像です

2024年4月11日
自由民主党 AIの進化と実装に関するプロジェクトチーム

AIホワイトペーパー2024の骨格



自民党ホワイトペーパー（2023年）：全ての始まり。日本のAIのビッグバン。

提言のほとんどは実現、または実施中。
一方で、この一年の世界と日本の動きは、官民間わず他に例をみない速さで進展。

これからの一年も、誰も具体的に正確な予測ができない「ステージⅡ」

ステージⅡにおける新戦略 — 世界一AIフレンドリーな国へ — 競争力強化と安全性確保の一体的な推進

研究開発、利活用を容易に

安心・安全に

競争力強化

急速な環境変化を味方につける柔軟な対応により
競争力を強化し、イノベーションを創出

研究開発と利活用 一体の競争力強化

利便性の高い新技術の研究開発

研究開発力
の強化

好循環による
競争力強化

AI利活用
の推進

データの増加、AI関連投資の拡大

計算資源等のインフラ高度化

安全性を向上させる
新技術

リスクの最小化
利益の最大化

安全性の確保が
AI利活用、AI研究開発を促進

安全性確保

自発的な対応を基本とする多層的なアプローチ（ソ
フトローと必要最小限のハードロー）により、安全・
安心な利用環境とイノベーションを促す環境を整備

リスクへの対応

リテラシー向上、人材育成
著作権・知財、個人情報への対応等

国際的な連携・協調、国際整合性

AIホワイトペーパー2024 主な提言

第1章 「ステージII」 に臨む日本

ステージIIの戦略 -世界一AIフレンド リーな国へ-

- 「**世界一AIフレンドリーな国**」、すなわち、世界で最もAIに理解があり、AIの研究開発・実装がしやすい国を実現する
- AIによる**国民のリスクを最小化しつつ、利益を最大化**する
- **競争力強化と安全性確保を一体的に推進**する
- 日本は、**広島AIプロセスの実績をベース**に、安心・安全で信頼性のあるAIに関する**国際的なルールメイキングを引き続き主導**する
- **アジア諸国やグローバルサウスとの協調関係を強化**するとともに、**AIの国際共同研究や利活用促進**についても、**世界の中で強いリーダーシップを発揮**する

第2章 AIを活用した 日本の競争力 強化のための 戦略： 急速な環境 変化を味方につける柔軟な 対応

利活用の促進

- **行政における更なる利活用**を進めるため、機密情報の扱い等を踏まえた**ガイドラインを新たに策定**する
- AIリスクに対して、リスクベースで事業者が環境変化に迅速に対応できるよう、「**AI事業者ガイドライン**」を速やかに**策定・公表**するとともに、これを**広く周知徹底**して、各組織による**AIの適切な利活用を促進**する

研究開発力の強化

- **データのAI開発への活用**に向け、政府等保有データの提供スキームの構築や、民間データの活用事例の共有、開発に有用なデータの新たな整備等を実施する
- 自動車・ロボット・材料開発など**日本の強みを活かせる分野**や、医療・金融・農業など**安全保障上も重要な分野**において、AIの開発・利活用をしっかりと進められるよう、**データの収集・整備・更新とAIの開発・利活用の相乗的な取組**を、官民で実施する
- 自由民主党における議論・提言を踏まえつつ、政府は、**AIスタートアップを対象とした支援プログラムを取りまとめる**
- AI for Scienceを含む最先端のAIに係る競争力の飛躍的な強化のため、政府は、**国立研究機関等のデータ基盤を整備**する

インフラの高度化

- 世界一AIフレンドリーな国となるためのデータセンター等のインフラを確保できるよう、政府は、**金融面等での政策的支援**を行い、**必要な民間投資を促す**
- 「**AI橋渡しクラウド（ABCI）**」の**拡充・高度化**や、AI性能も備えた「**富岳**」の**次世代**の整備に着手する

第3章 安全性確保 のための戦略

適切なガバナンス

- **AI事業者ガイドライン等に基づき事業者等が自発的・継続的にリスクを評価し、低減を図ることを日本のAIガバナンスの基本**とする
- 当PTのWG有志による「**責任あるAI推進基本法（仮称）**」の考え方等を踏まえ、政府は、**極めて大きなリスクがあるAIモデルに対し、必要最小限の法的枠組みを整備**する

生成AIを利用した 偽・誤情報対策

- **生成AIを利用した偽・誤情報等**について、制度面も含む**総合的な対策**を今夏を目途にとりまとめる
- **選挙への負の影響に適切に対処**するため、関係事業者は、**ミュンヘン・アコードと同様の取組を日本国内でも実施**する

AIの安全性確保に 向けた更なる取組

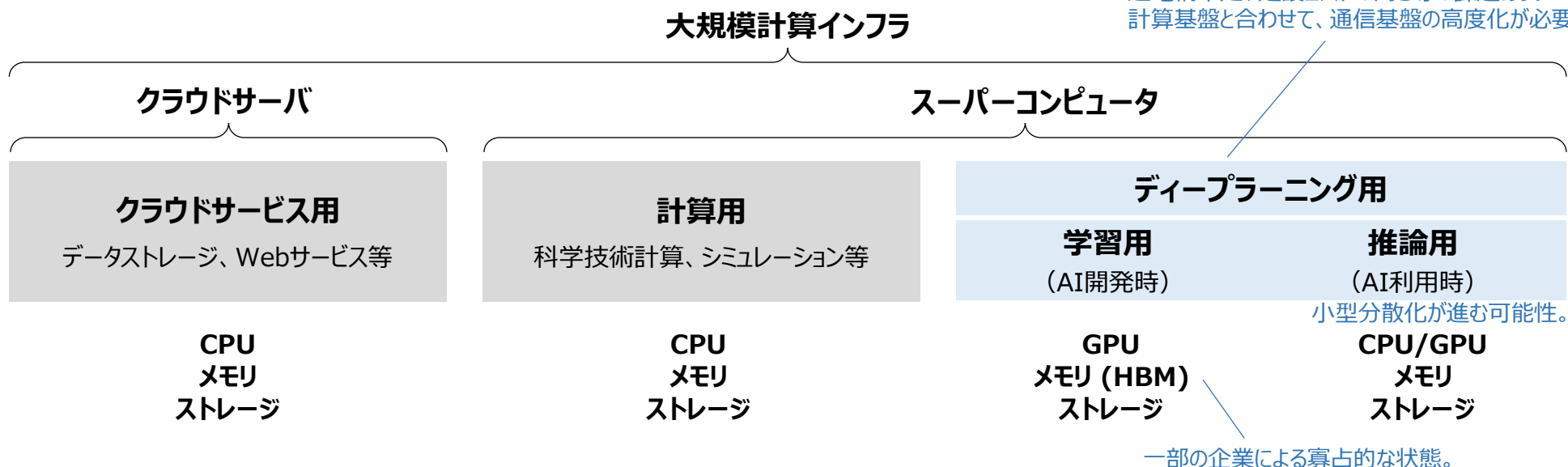
- AIの安全性確保に向けた国際的な協調を図るため、**日本のAISIと諸外国のAISI等のハイレベルのネットワーク**を構築する
- AISIは、AIの安全性評価に関する**我が国の結節点としての役割**を担う

著作権などの知的 財産との関係

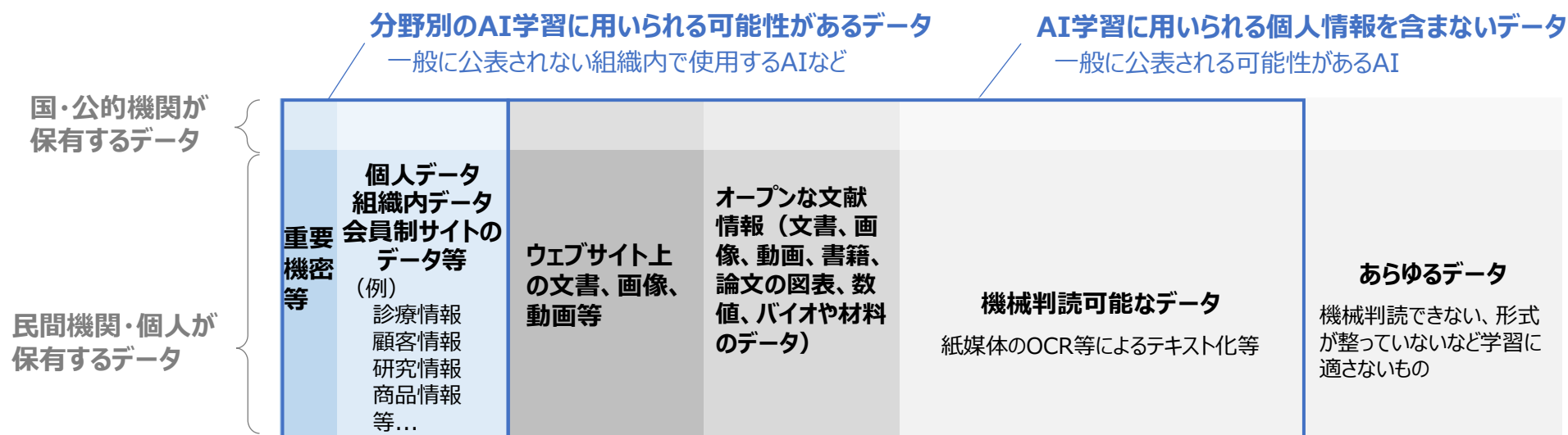
- **著作権などの知的財産権**については、政府はこれらの**権利を尊重**しつつ、AI時代に即した対応を行い、**適切なAI利活用を促進**する

計算資源と学習用データの全体像

計算資源の全体像



学習用データの全体像



(出典) 産業技術総合研究所の資料を基に作成

責任あるAI推進基本法(仮)の骨子

立法趣旨

立法趣旨: 生成AIを含むAIの利活用により基本的人権をはじめとする国民の権利利益が侵害されるリスクを最小化しつつ、AIによるイノベーションを含むAIの健全な発展による利益を最大化するため、安全、安心で信頼できる責任あるAIの設計、開発及び導入並びに人間を中心としたAIの利用を可能とするような、開かれた環境の整備を促進する。

①責任あるAI利活用の促進

国: 官民におけるAIの利活用を推進し、社会課題の解決を目指す

施策例: AIの技術革新を推進する官民パートナーシップの構築・強化

国: AI人材の育成・誘致と研究開発力の強化

施策例: AIの研究開発のための助成金・補助金等交付

国: 先進的AIの安全性に関する研究機関の機能強化

施策例: 今般創設されたAISIの機能強化

③特定AI基盤モデル開発者の体制整備義務(続)

民間: 各事業者又は業界団体が上記の義務内容を具体化する規格や行動規範を制定・公表する

論点

- ✓ EU AI Actの整合規格のように民間にAIの品質担保のための規格策定を委ねるか
- ✓ 利害関係者を含めた議論に基づく具体的な行動規範の制定の可否(例: EUデジタルサービス法では、欧州委員会が利害関係者を招請して行動規範を策定している)
- ✓ 民間機関による認証制度等を設けるべきか

②特定AI基盤モデル開発者の指定

国: 一定の規模・目的のAI基盤モデル開発者を「特定AI基盤モデル開発者」に指定する

論点

- ✓ 「基盤モデル」の「開発者」を規制の対象とする必要性・許容性の整理
- ✓ 「規模」「目的」を何を指標にして評価・区分するか(例: パラメータ数、汎用目的か否か)
- ✓ 指定は一方的に行うか、まず届出をさせるか。一方的に行う場合、指定のための調査権限を国に認めるか
- ✓ 届出すべきであるのに届出しない事業者に制裁するか
- ✓ 適用の地理的範囲(日本で提供されるサービスに「利用」されるモデルに限定するか。)

民間: 届出義務を課す場合は、対象となる事業者は届出を行う

④義務遵守状況の報告義務と監督

国: 特定AI基盤モデル開発者に、定期的に③の義務の遵守状況を国または第三者機関(例: AISI)に報告する義務を課す

論点

- ✓ 国への報告にとどまらず対外的な開示まで求めるか

国及び民間: 国は報告内容に基づき特定AI基盤モデル開発者のモニタリングレビューを行う。国は民間等の利害関係者の意見を聴取することができる

国: 国は評価の結果を公表するとともに、一定の場合には是正を特定AI基盤モデル開発者に求める

国: 特定AI基盤モデル開発者が義務を遵守していない場合やインシデントが発生した場合等に報告徴求や立入検査をできる

③特定AI基盤モデル開発者の体制整備義務

国: 事業者以下に以下の項目を含む体制整備に関する義務を課す

- 特にリスクの高い領域におけるAIについては自社・外部による安全性検証(Red team test等)を行う
- リスク情報を企業・政府間で共有する
- 未公表の重み付けを守るサイバーセキュリティへの投資
- 第三者による脆弱性等の検出と報告
- 生成AIの利用を利用者に通知する仕組みの採用
- AIの能力、限界等の公表
- AIがもたらす社会的リスクの研究推進

⑤罰則等

国: 義務・命令違反に対して課徴金・刑罰を科す

民間: 認証等の取消・一時停止等