経済産業省

日本のAI産業競争力確保とAIセーフティ

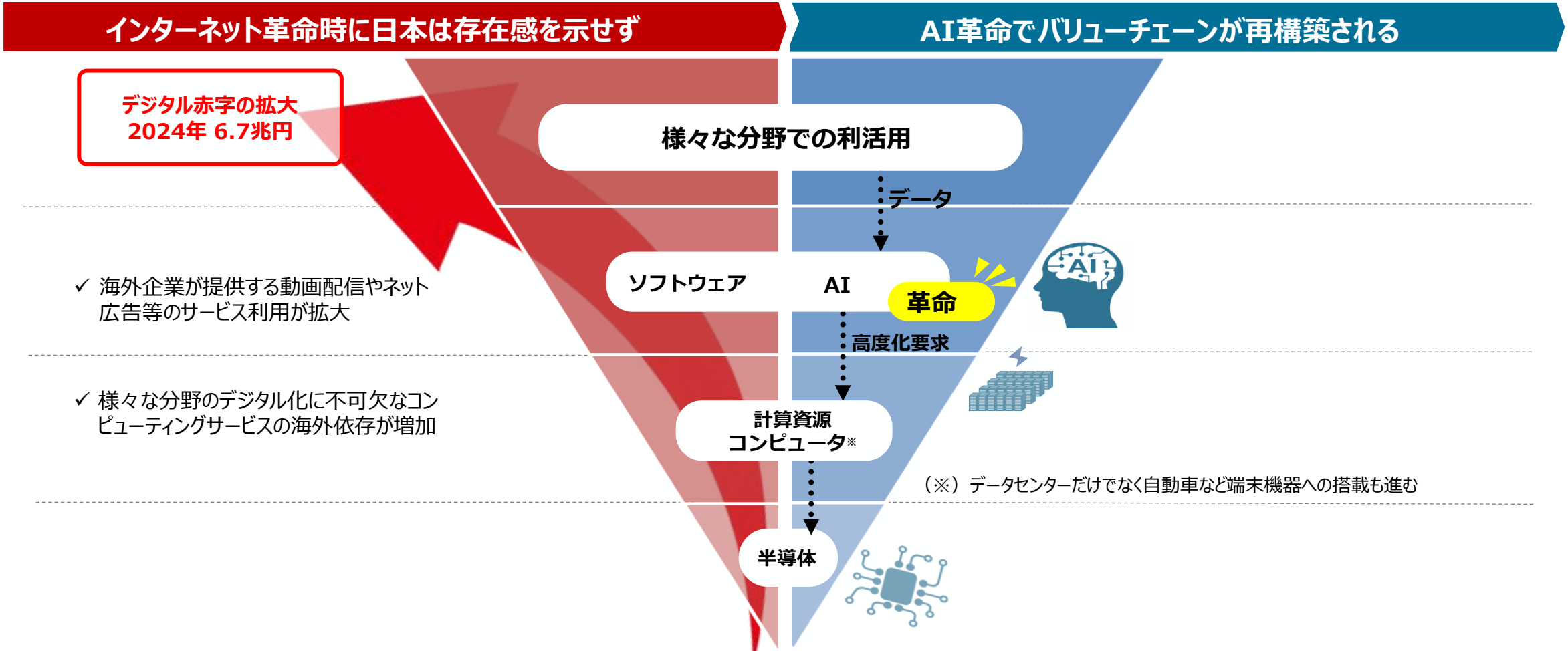
2025年10月29日

商務情報政策局 情報産業課 AI産業戦略室

鶴岡　譽

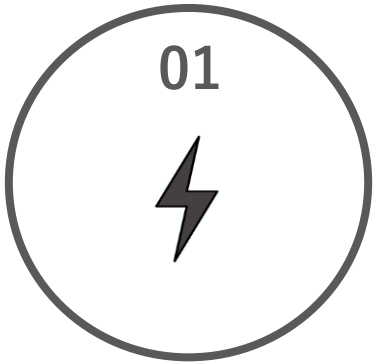
AI革命を契機としたデジタル分野の競争力確保に向けて

- 20世紀末のインターネット革命で存在感を示せなかった日本は、いまデジタル赤字の拡大に直面。
- AI革命が生じる中、全面的な海外依存が進めば、デジタル赤字は更に拡大するおそれ。
  逆に、価値創造が再構築される中、競争力を確保できるチャンス。



GENIAC ～Generative AI Accelerator Challenge～

- **生成AIについて、エンジニアリング能力の向上を図る**とともに、専門データの確保やユースケースを踏まえた付加価値を創出し、**社会実装を目指すプログラム**。2024年2月から実施。

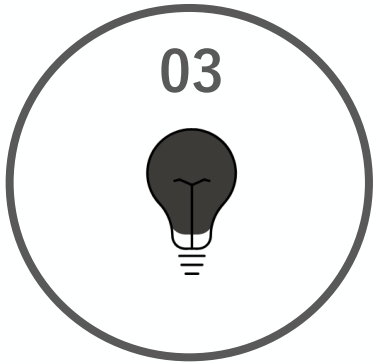


計算資源

生成AIのコア技術である基盤モデルを開発する上で必要な計算資源の調達を支援する。

データ

ユーザーなどデータ保有者との連携を促進し、データの利活用を支援する。



ナレッジ

イベント等を通じて国内外の開発者同士や様々な関係者との交流を支援する。

GENIACサイト：https://www.meti.go.jp/policy/mono_info_service/geniac/index.html

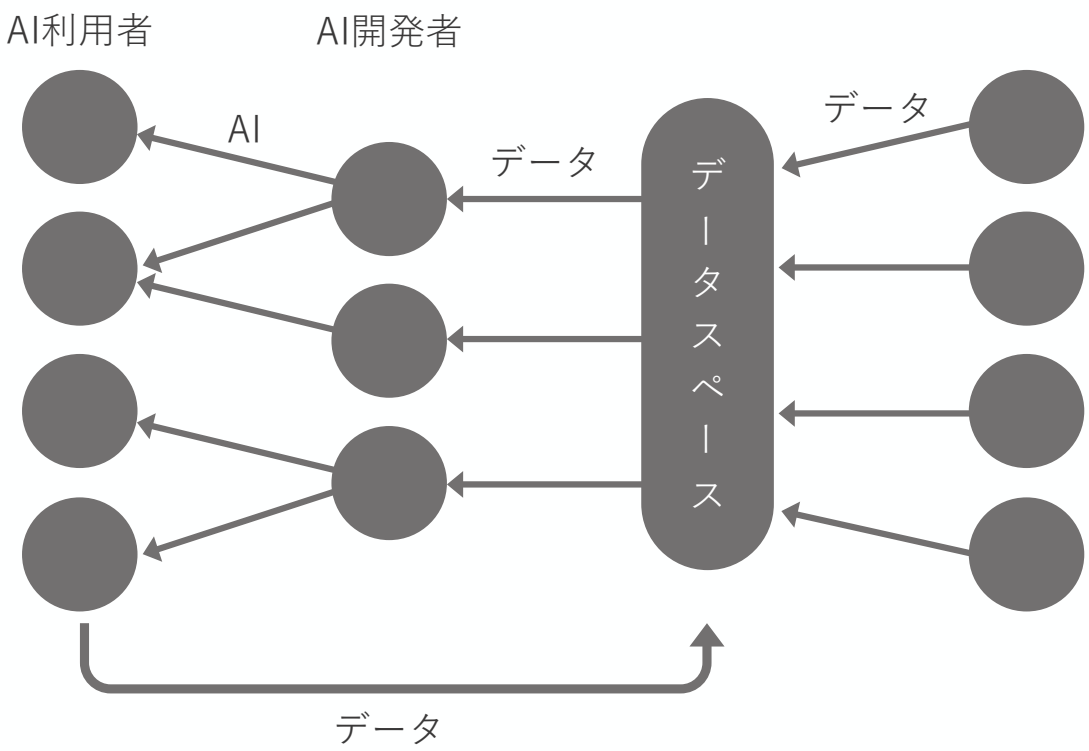
基盤モデル開発のための計算資源の調達支援

- 1期目では、開発ノウハウ等の公開を重視して支援し、大規模言語モデル開発に関する日本としての基礎体力作りを行った。300名超が開発を経験。世界レベルの成果も。
- 2期目では、マルチモーダル化や推論の効率化、領域特化など、社会実装を重視した基盤モデルの開発を支援。
- 現在、3期目の開発を支援中。ユーザーと連携した実証を推奨。

	1期目	2期目	3期目
目的	• 生成AI基盤モデル開発者の基礎体力作り	← • 社会実装を見据えた基盤モデル開発 →	
補助率	• 定額（中小企業・スタートアップ等） • 1/2（大企業）	← • 2/3（中小企業・スタートアップ等） • 1/2（大企業） →	
対象経費	• 計算資源（Google Cloud、Microsoft Azure）の利用料	← • 計算資源の利用料 ※計算資源提供者は問わない • データ整備に必要な費用 →	
事業期間	• 2024/2/15～2024/8/15（6ヶ月）	• 2024/10/18～2025/4/30（うち6ヶ月）	• 2025/8/1～2026/2/28（うち6ヶ月）

データを起点にしたエコシステム作り

- 様々なデータ提供者に対する適正な利益分配や、信頼性の高いデータ流通等を確保することにより、特定の領域におけるデータを次々と収集し、活用を促すデータスペースを構築する取組を支援する。
- これにより、データを起点にしたエコシステムのモデル事例を創出する。



実施者と収集データ

SoftBank	ソフトバンク株式会社	コールセンター等の音声・言語データ
safie	セーフィー株式会社	店舗や建設現場等のカメラ映像データ
AIRoA AI Robot Association	一般社団法人AIロボット協会	ロボット動作データ
VISUAL BANK	Visual Bank株式会社	キャラクター・背景等の作画データ
HEMILLIONS	株式会社HEMILLIONS	医療画像データ
Preferred Networks	株式会社Preferred Networks	都市・建築空間の3Dデータ

GENIACコミュニティ

基盤モデル開発者

ABEJA
sakana.ai
NII 大学共同利用機関法人 情報・システム研究機構 国立情報学研究所 National Institute of Informatics
Stockmark
Preferred Networks
TURING
松尾・岩澤研究室 Matsuo-Iwasawa Lab UTokyo
Kotoba Technologies
ELYZA
FUJITSU
AIdeaLab Innovate through AI
AiHUB
AI inside
EQUES
NABLAS
SYNTHETICGESTALT
woven by TOYOTA
KARAKURI
JAMSTEC
DATAGRID
Humanome Lab
FUTURE
RICOH imagine. change.
ubitus
Deepreneur
DIREAVA
エアリオン Airion
NRI
PRECISION
ONESTRUCTION
zen intelligence
Nishika
NexaScience
Alivexis Delivering the future of medicines
sansan
Degas
SDio
Rakuten

アプリケーション開発企業

データスペース構築者

SoftBank
safie
AIRoA AI Robot Association
VISUAL BANK
HEMILLIONS
Preferred Networks

ユーザー企業

- 製造業
- 素材・化学・医薬品
- 消費財・小売・流通・金融
- インフラ・運輸
- エンタメ・教育

計算資源提供者

金融機関、投資会社、CVC

生成AIアプリケーションの開発促進のための懸賞金コンテスト

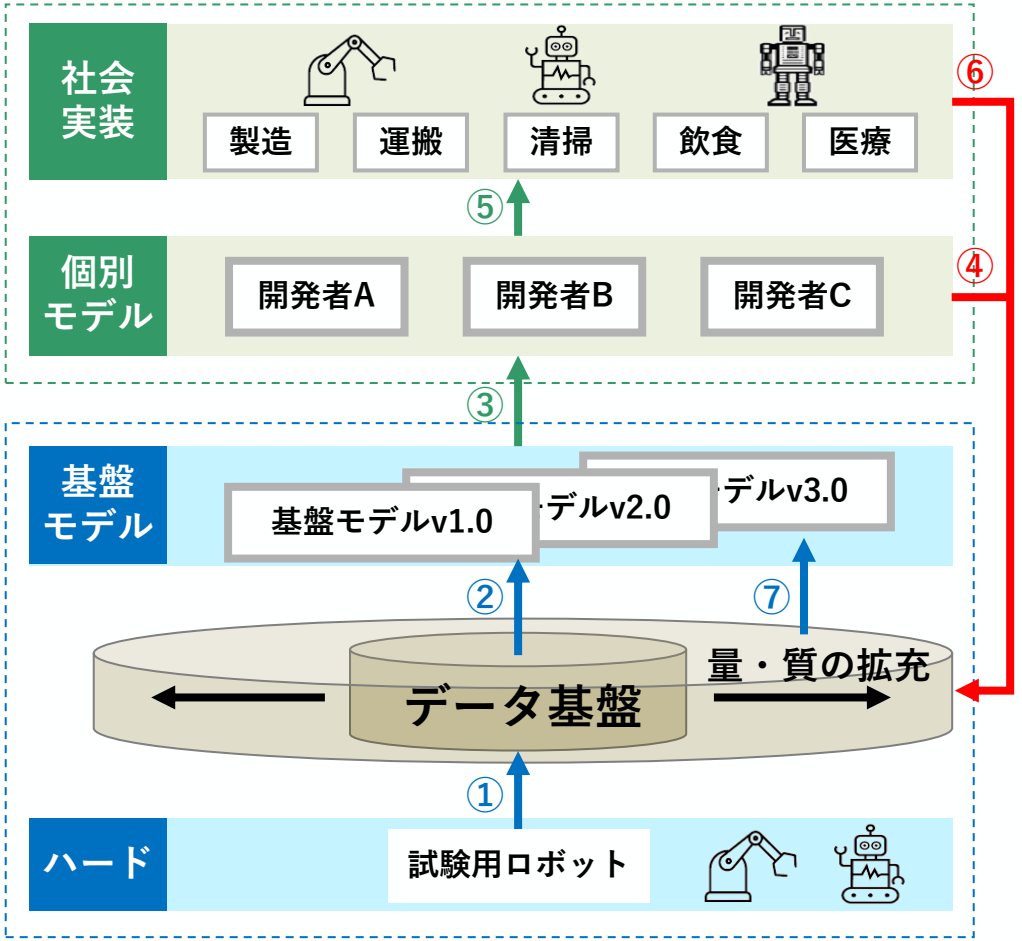
- 下記テーマにおける具体的なニーズに基づき開発・検証・申請された生成AIアプリケーションについて、審査を行い、成果に応じた懸賞金を授与する。
- 様々な地域や業種における幅広い事業者の参画を促し、生成AIの開発・社会実装を促進する。

	テーマ	懸賞金総額	スケジュール
民	**国産基盤モデル等を活用した社会課題解決AIエージェント開発** **（Ⅰ. 製造業の暗黙知の形式知化／Ⅱ. カスタマーサポートの生産性向上）** ● ユーザーが主体となり申請（AI開発者やSIerと組んだ申請も可能）、ユーザーの変革につながる検証成果を審査	3.5億円	• 9月末：エントリー〆 • ～12月末：エントリー企業の応募〆 • 来年1月～3月末：審査
官	**官公庁等における審査業務等の効率化に資する生成AI開発** ● 特許審査業務をモデルとし、情報探索等を効率化するAIを開発、その性能を審査	2.1億円	• 12月上旬：応募〆 • 来年1月～3月末：審査
安全性	**生成AIの安全性確保に向けたリスク探索及びリスク低減技術の開発** ● AIのリスクや対応策をセットで提案、評価手法の妥当性や波及効果を審査	2.2億円	• 7月末：トライアル審査応募〆 • 10月9日：トライアル審査結果公表 • 12月下旬：応募〆（※トライアル審査申請企業以外も応募可能） • 来年1月～3月末：審査

GENIAC-PRIZEサイト：https://geniac-prize.nedo.go.jp/

フィジカルAIの開発促進

- フィジカル分野の基盤モデルにより、従来は難しかった汎用・自律的なロボットの動作が可能に。米中では、プロプライエタリにデータを蓄積し、基盤モデルを開発する動きが加速。
- 日本では、オープンなデータ基盤の成長を加速させることにより、基盤モデルの開発や社会実装を促進する。



⑥創出されたデータをデータ基盤に還元

⑤個別モデルを組み込み、社会実装

④モデル・データ利用時に一定以上のデータをデータ基盤に還元

③基盤モデルを元に個別モデルを開発

国内外の多様なプレイヤーの参画を促進
⇒各事業者による開発を支援

⑦新たに得られるデータで基盤モデルの性能を向上

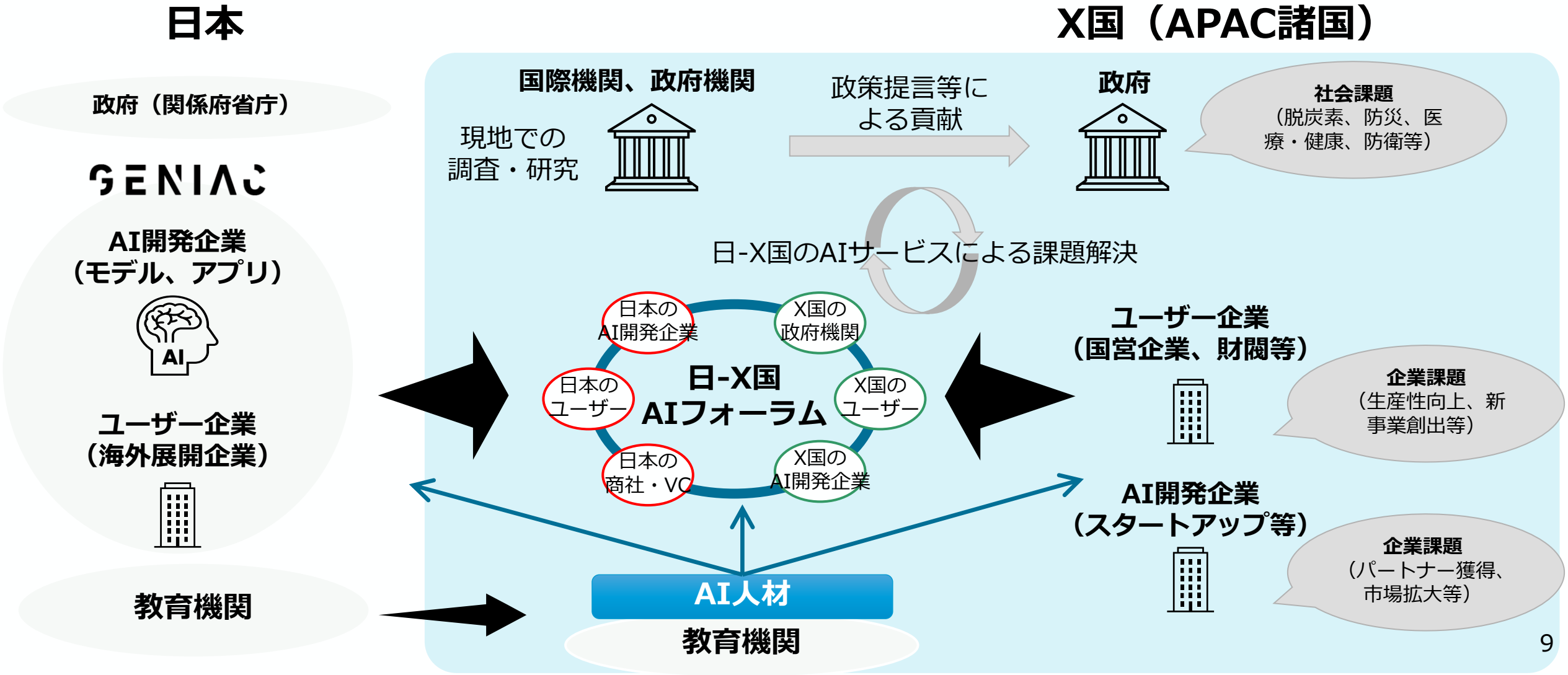
②データ基盤のデータを用いてフィジカル分野の基盤モデルを開発

①圧倒的に不足するフィジカル分野のデータ収集

AIRoA
AI Robot Association
一般社団法人AIロボット協会の活動を支援

海外展開支援：日-X国 AIエコシステムの構築

- 特に成長著しく地理的に近い**アジア・太平洋地域への展開を促進**するため、各国ごとの人材育成から開発・利用のエコシステム作りに貢献していく基本姿勢が重要。相手国とのAIフォーラムを開催しながら、**面的なネットワーキングの構築・深化**を図っていく。



ASEAN関連首脳会議での高市総理発言

- １０月２６日、高市新総理が総理大臣就任後、初の外国訪問先としてマレーシアを訪れ、ASEAN関連首脳会議に出席。
- 日本として、国際的なAIガバナンスを構築し、AIを活用したイノベーションを促進していくことにも言及。

ASEAN関連首脳会議出席に際しての寄稿（抜粋）10/26

デジタルの分野では、**AIには経済・社会を大きく変革し発展させる高い潜在力**があります。日本は、「安全、安心で信頼できるAI」を推し進め、**国際的なAIガバナンスの構築**や**AIを活用したイノベーションを促進**していきます。

日ASEAN首脳会議での高市総理発言（抜粋）10/26

日本は新たに「日ASEAN・AI共創イニシアティブ」の立ち上げを提案する。モデル開発、人材育成、ソリューションの共創などを通じ、**安全、安心で信頼できるAIエコシステムを共に構築**していきたい。
AI、量子、半導体等の最先端分野で、国際共同研究や研究者の交流を強化していく。

ASEAN首脳と高市総理の写真撮影

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）の概要

法律の必要性	日本のAI開発・活用は遅れている。 多くの国民がAIに対して不安。 **イノベーションを促進しつつ、リスクに対応するため、既存の刑法や個別の業法等に加え、新たな法律が必要。**	
法律の概要	**目的**	**国民生活**の向上、**国民経済**の発展
	基本理念	経済社会及び**安全保障上重要** ➡ 研究開発力の保持、**国際競争力**の向上 基礎研究から活用まで総合的・計画的に推進 **適正な研究開発・活用**のため**透明性**の確保等　　**国際協力において主導的役割**
	AI戦略本部	**本部長：内閣総理大臣　構成員：全閣僚**　　関係行政機関等に対して必要な協力を求める
	AI基本計画	研究開発・活用の推進のために**政府が実施すべき施策の基本的な方針**等
	基本的施策	**研究開発**の推進、**施設等の整備・共用**の促進　　**人材確保、教育振興** **国際的な規範策定**への参画　　**適正性**のための**国際規範に即した指針**の整備 **情報収集**、権利利益を侵害する**事案の分析・対策検討、調査** **事業者等への指導・助言・情報提供**
	責務	国、地方公共団体、研究開発機関、事業者、国民の責務、関係者間の連携強化 **事業者は国等の施策に協力しなければならない**
	附則	**見直し規定**（必要な場合は所要の措置）
世界のモデルとなる法制度を構築	**国際指針に則り、イノベーション促進とリスク対応を両立。最もAIを開発・活用しやすい国へ。**	

AI事業者ガイドライン：概要

- 「AIに関する暫定的な論点整理」（2023年5月、AI戦略会議）を踏まえ、総務省及び経済産業省において検討を行い、2024年4月に**「AI事業者ガイドライン（第1.0版）」を策定・公表**（第8回AI戦略会議に報告した上で、同日、公表）。最新の動向等を踏まえ、その後も引き続き更新中（**2025年3月に第1.1版に更新**）
- 既存のガイドラインを統合・アップデートするとともに、広島AIプロセスの成果を含む国際的な動向等を反映。**共通の指針**を示しつつ、**AI開発者、提供者、利用者ごとに取り組むべき事項**を整理
- 本ガイドラインを活用し、事業者が**適切なAIガバナンスを構築**する等、**自主的に取り組む**ことが重要

AI開発者・提供者・利用者の共通の指針

- 各主体は、法の支配、人権、民主主義、多様性、公平公正な社会を尊重するようAIシステム・サービスを開発・提供・利用し、**関連法令及びAIに係る個別分野の既存法令等を遵守**
- 各主体が取り組むべき**10個の指針**（**①人間中心、②安全性、③公平性、④プライバシー保護、⑤セキュリティ確保、⑥透明性、⑦アカウンタビリティ、⑧教育・リテラシー、⑨公正競争確保、⑩イノベーション**）を記載
- 高度なAIシステムに関係する事業者は、**広島AIプロセス国際指針**を遵守　等

AI開発者に関する事項

- **安全に利用可能なAIの使い方**について明確な方針・ガイダンスを設定
- **適切なデータで学習**し、個人情報、知的財産権やバイアス等に配慮
- 開発するAIについて、適切に関連するステークホルダーに**情報提供**
- **イノベーションの機会創造**への貢献に期待　等

AI提供者に関する事項

- AI開発者が設定した範囲でAIを活用し、AIシステム・サービスの**利用上の留意点**を正しく定める
- AIシステム・サービスやデータに含まれる**バイアスやプライバシー侵害等への配慮**、脆弱性への対策を実施
- 提供するAIシステム・サービスについて、適切に関連するステークホルダーに**情報提供**　等

AI利用者に関する事項

- AI提供者が定めた利用上の留意点を遵守して、**AI提供者が設計において想定した範囲内**でAIシステム・サービスを利用
- 入出力データやプロンプトに含まれるバイアスやプライバシー侵害等への配慮
- 利用状況や障害情報等を、可能な範囲で関連するステークホルダーに説明　等

AIセーフティ・インスティテュート（AISI)

- 2023年11月の**AI安全性サミット**を契機に「AI安全性」をキーワードにガバナンスの深掘りに関する議論が進む。
- 2024年2月、独立行政法人情報処理推進機構（IPA）に、**AIセーフティ・インスティテュート**を設置。
- 国内外の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キング**を進めるとともに、**AISIの安全性評価能力を確立しながら、安全性評価のためのガイダンスの作成等**を目指す。

日本のAISIの概要

- **業務**
  - **安全性評価に係る調査、基準等の作成**
  - **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AISI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、内閣サイバーセキュリティセンター、警察庁、デジタル庁、総務省、外務省、文科省、経済産業省、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**

村上明子所長

2024年2月１日、内閣府・IPAから内定発表。**2月14日就任**

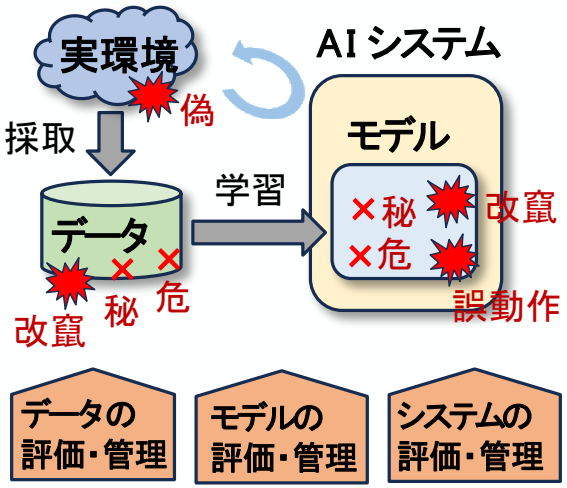
- 1999年　日本アイ・ビー・エム株式会社 東京基礎研究所　入社
- 2022年　**損害保険ジャパン株式会社 執行役員CDO**（Chief Digital Officer）**DX推進部長**（現職）
- 京都大学防災研究所客員講師（兼職）

産総研におけるAIセーフティの研究開発

- AISIを中心とした取組の中で、産総研においても、日本が強みを持つフィジカル分野の知見も活かしたAIセーフティの研究開発を加速し、その成果を元に基準を策定するとともに、国際標準の形成も主導していく。

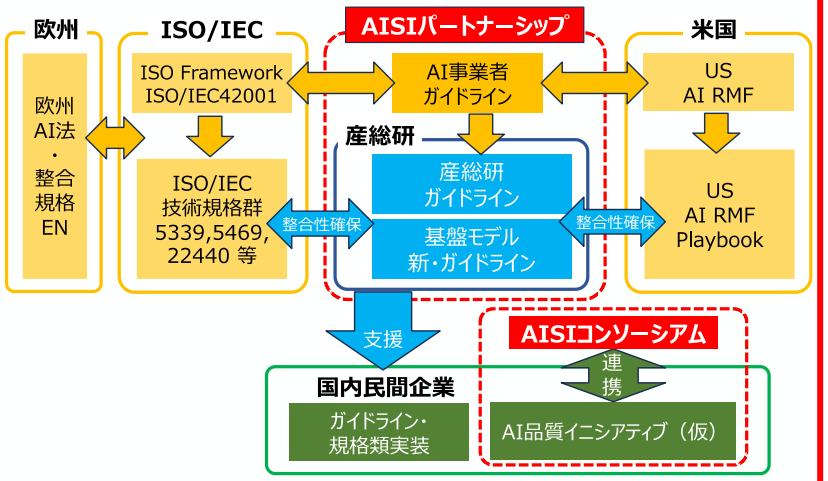
①AIセーフティ評価・管理基盤技術開発

- **AIに対する個別の攻撃や防御手法の研究は盛んだが、安全性の評価・管理技術が体系的に確立していない。**
- **このため、データ、モデル、システムそれぞれのレイヤーにおいて、それぞれの課題を踏まえ、リスクベースアプローチの基になる安全性を評価するためのソフトウェアツールやベンチマークデータを開発する。**



③AIセーフティ基準・ガイダンス作成と標準化活動

- **①や②の成果を基に、AIセーフティ基準・ガイダンスを作成する。**
- **関係する事業者を巻き込みながら、AIセーフティ基準・ガイダンスの社会実装・普及を促進する。**
- **あわせて、ISO/IECにおける標準化活動と国際連携も行う。**



②応用領域別AIセーフティ評価・実装技術開発

- **サイバー空間とフィジカル空間をつなぐ応用領域(暮らし支援、協働ロボット、スマートシティ)に特有のリスクに対応するためのAIセーフティ評価・実装技術を開発する。**

暮らし支援

プライバシー情報を適切に扱うAIを開発するため、介護見守りAIをモデルケースとして、デジタルツインを用いて生活事故環境を再現する技術を開発する。

協働ロボット

AIロボットが予想外な動き等により人をケガさせないよう、模擬的な環境下で、複数のAIロボットが相互に連携して人と協調した作業を安全にできる技術を開発する。

スマートシティ

通信断で人による遠隔操作・制御不可になっても、安全・安心に動作する自律性の高いAIロボットの開発のため、屋内外のシームレスなデジタルツインを実現する技術を用いたロボットの統合運用管制システムを開発する。

AIセーフティの取組強化 ～AISIを中核とした標準化活動～

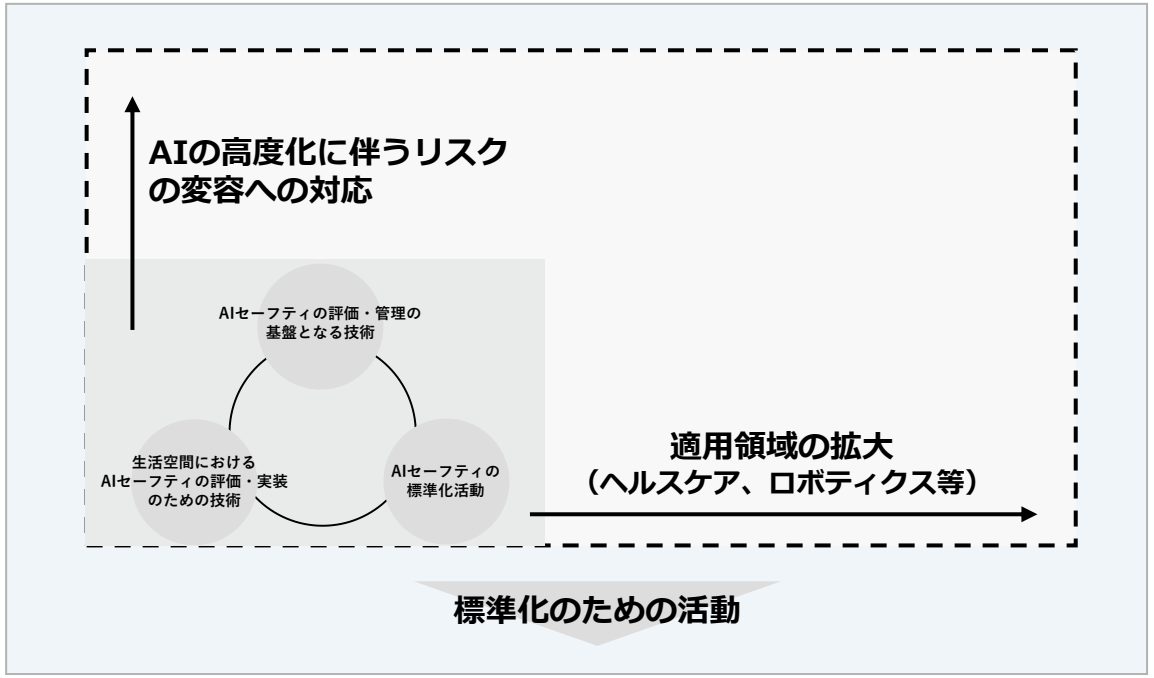
- AISIは、これまでの取組を発展させ、ドキュメントの策定や国際連携に加え、**汎用／分野別のAIセーフティ評価環境の構築**等を目指す。
- その際、経産省としては、国研等のアセットも活用しながら、**主に技術面からAISIを支援**する。

AISIの取組方針

- 最新の動向を反映した「評価観点ガイド」「レッドチーミング手法ガイド」の改訂
- 汎用的なAIセーフティ評価環境（自動レッドチーミングツール、データセットなど）の構築
- 分野別（ヘルスケア、ロボティクス、データ品質、適合性評価等）の取組（分野別AIセーフティ評価に関するドキュメント、評価シナリオ、データセット等の策定）
- AIセキュリティに対する取組（AIシステムに対する特有の攻撃手法の調査、AIセキュリティインシデントの分類体系の検討）
- 国際連携の強化　等

技術面からの貢献

国研等を活用した取組



イノベーション促進とリスク対応を両立。
最もAIを開発・活用しやすい国へ