# 国産AI基盤モデル新会社「日本AI基盤モデル開発」

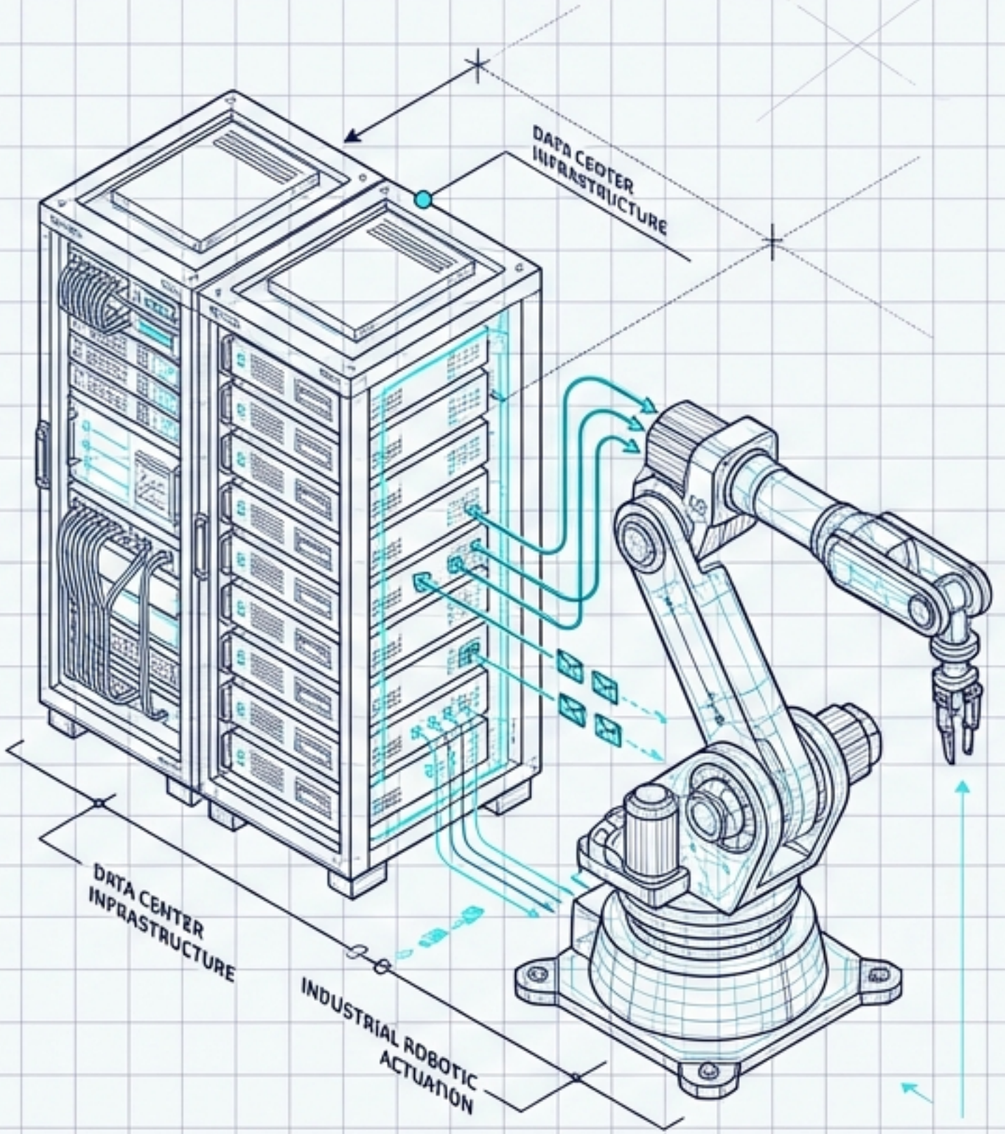
## 深掘り分析と戦略的解剖 (Strategic Anatomy & Deep Dive)

— フィジカルAI実現に向けたエコシステム・技術・ガバナンスの全貌 —

[TARGET]:
経営層・戦略部門・政策担当者向け
Executive Strategic Briefing

[DATE]:
2026-04-13

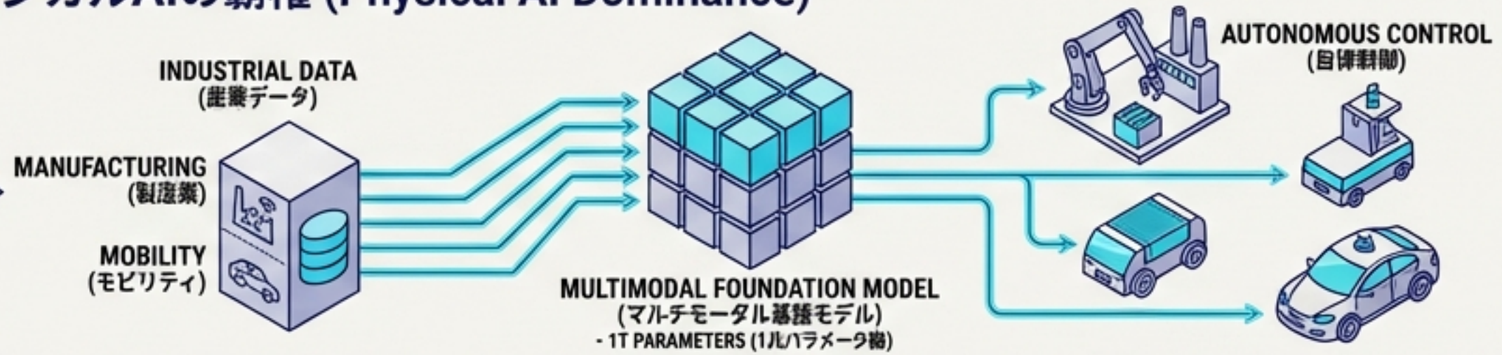
[CLASSIFICATION]:
分析レポート



# THE GOAL (目的と射程) – フィジカルAIの覇権 (Physical AI Dominance)

## CONCEPTUAL FRAMEWORK (概念フレームワーク)

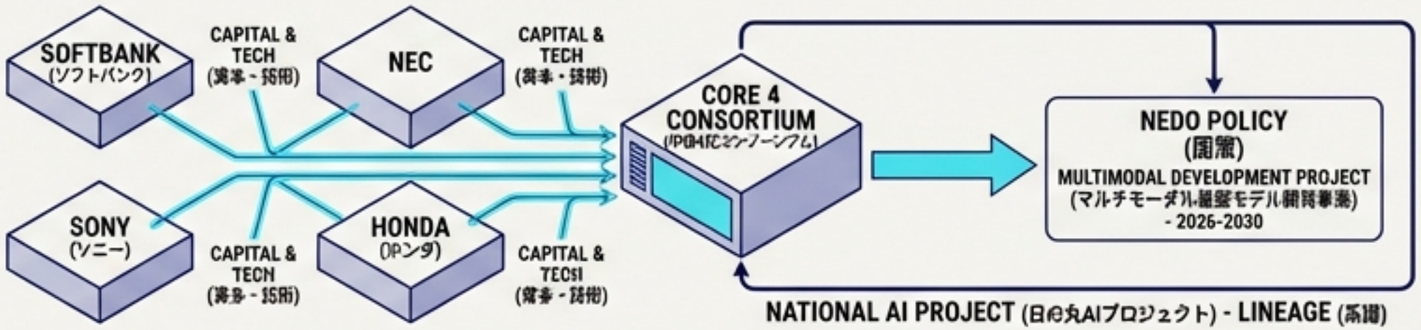
単なる国産ChatGPTの構築ではない。製造業・モビリティ領域の「現場データ（産業データ）」を活用し、ロボットや設備を自律制御するマルチモーダル基盤モデル（1兆パラメータ級）の構築と一気通貫の実装を狙う。




# THE BACKING (推進エンジン) – 中核4社 × 国策

## STRATEGIC ALLIANCE (戦略的提携)

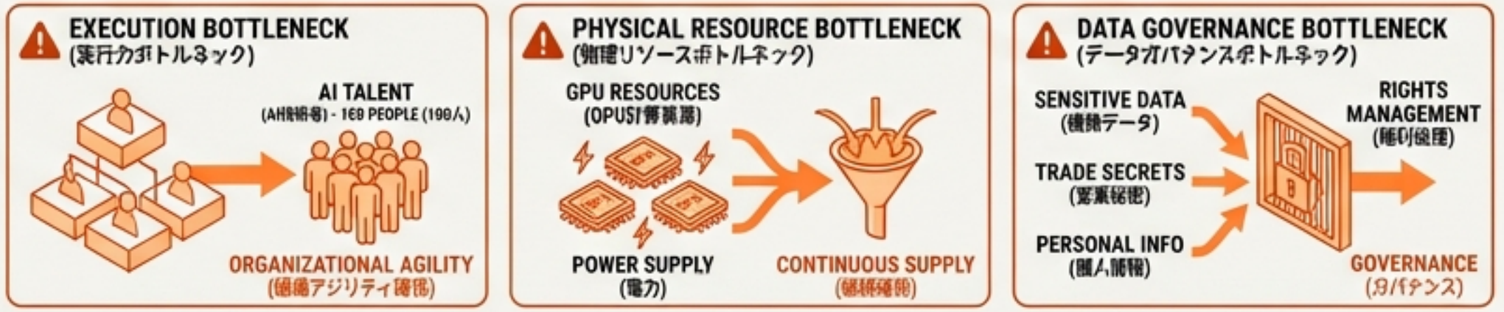
ソフトバンク、NEC、ソニー、ホンダ（各十数%出資）による資本と技術の結集。さらに、NEDOの2026～2030年度「マルチモーダル基盤モデル開発事業」への参画を前提とした、実質的な「日の丸AIプロジェクト」の系譜。

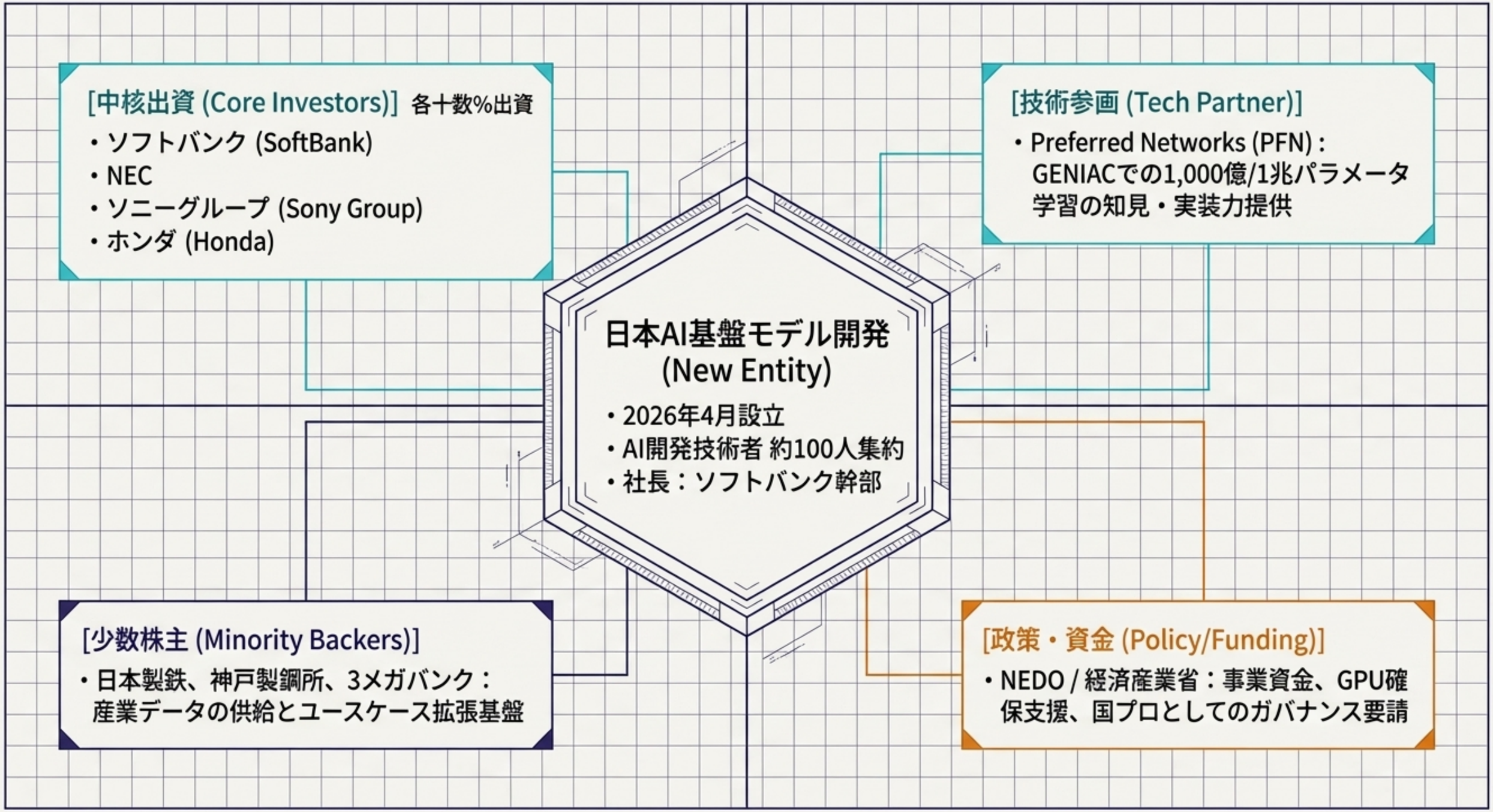



# THE CHALLENGE (成功の阻害要因) – 実行力と物理的制約 (Execution & Physical Limits)

## CRITICAL BOTTLENECKS (重大なボトルネック)

AI技術者約100人の組織集約とアジリティ確保。さらに、膨大なGPU計算資源・電力の継続確保と、機微な産業データ（営業秘密・個人情報）の適切な処理・ガバナンスが最大のボトルネックとなる。




[中核出資 (Core Investors)] 各十数%出資
・ソフトバンク (SoftBank)
・NEC
・ソニーグループ (Sony Group)
・ホンダ (Honda)
[技術参画 (Tech Partner)]
・Preferred Networks (PFN) :
GENIACでの1,000億/1兆パラメータ
学習の知見・実装力提供
日本AI基盤モデル開発
(New Entity)
・2026年4月設立
・AI開発技術者 約100人集約
・社長：ソフトバンク幹部
[少数株主 (Minority Backers)]
・日本製鉄、神戸製鋼所、3メガバンク：
産業データの供給とユースケース拡張基盤
[政策・資金 (Policy/Funding)]
・NEDO / 経済産業省：事業資金、GPU確
保支援、国プロとしてのガバナンス要請

## SOFTBANK（インフラ・データ）

- 想定役割：
  基盤モデル構築の主導
- 戦略資産：
  国産生成AI「Sarashina」運用ノウハウ、国内データセンター網
- 独自強み：
  差分プライバシー・合成データ活用の実装経験

## NEC（エンタープライズ・安全）

- 想定役割：
  基盤モデル構築の主導
- 戦略資産：
  特化型LLM「cotomi」、エンタープライズAI運用知見
- 独自強み：
  AIガードレール設計、学習データの法令順守・ガバナンス設計

## SONY（センシング・認識）

- 想定役割：
  自動運転・ロボット等への実装（認識層）
- 戦略資産：
  「Sony AI」の研究基盤、イメージング＆センシング技術
- 独自強み：
  物理世界をデータ化するマルチモーダル直結のセンサー・映像系R&D

## HONDA（モビリティ・エッジ）

- 想定役割：
  自動運転・ロボット等への実装（物理制御層）
- 戦略資産：
  レベル3自動運転技術、ロボティクスR&D
- 独自強み：
  安全要件の極めて厳しい「実機×実環境データ」と制御経験

**フルスタック・フィジカルAI（Full-Stack Physical AI）**

[Corporate Track]

2026/04: [Corporate]
新会社「日本AI基盤モデル開発」設立報道。公募要件への適合体制を構築。

[NEDO Policy Track]

2026/03: [NEDO]
「マルチモーダル基盤モデル開発事業」公募開始。言語偏重から実空間・マルチモーダルへの政策シフト。

2026/04/22: [NEDO]
公募締切。データ・計算資源の確保計画の提示が必須。

2026/06-08: [NEDO]
採択決定および契約締結。

2027以降: [NEDO]
毎年度のステージゲート評価。価。(進捗による軌道修正・打切りリスク)

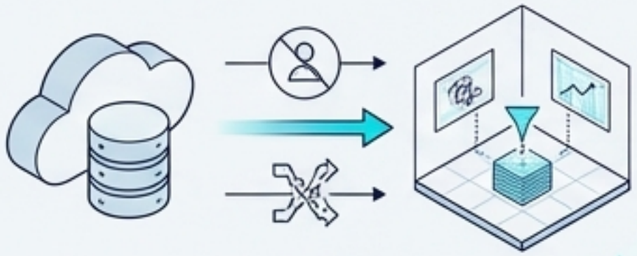
2029/03: [NEDO中間目標]
論理推論・合成データ生成/供給の基盤確立。

2031/03: [NEDO最終目標]
物理特性等の実空間情報を統合した論理推論の実現(フィジカルAIの完成)。

**戦略的含意 (Strategic Implication):**

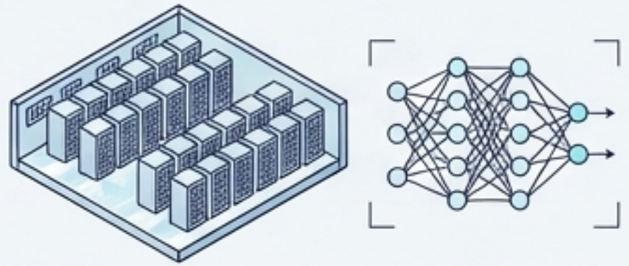
「長期一括」の予算ではない。初期の1〜2年でGPU稼働とデータ収集の"実績"を示せなければ、ステージゲートで脱落するシビアな設計。

## DATA REFINEMENT (匿名化・合成)



・SoftBank / NEC：収集した機微データを安全にクラウドへ。差分プライバシー技術による匿名化と、シミュレーション空間での「合成データ（Synthetic Data）」への変換。

## SOVEREIGN COMPUTE (国内基盤学習)



・SoftBank / PFN：国内データセンターの巨大GPUクラスターで、マルチモーダル基盤モデルへ学習。1兆パラメータ級の論理推論能力を獲得。

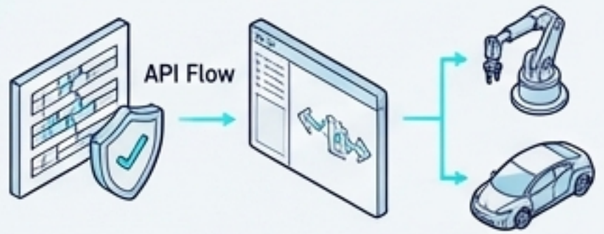
# The Moat：ハードウェア裏打ち型の主権データ

（言語モデルのようなWebクローリング競争ではなく、物理デバイスを持つ企業連合だけが回せる閉鎖的・高純度なデータループ）

## PHYSICAL WORLD (実世界・エッジ)

・Honda / Sony: センサー群、自動運転車両、工場ロボットから「実機・環境データ」を絶えず収集。

## SECURE ACTUATION (制御と実装)




・NEC / Honda: エンタープライズ水準のガードレール（cotomiの知見）を通過した安全な重み/APIを、再び現場のロボット・自動運転のエッジ推論へ還元し、自律制御を実行。

## 許諾済み公開データ (Public & Licensed)

特性：日本語テキスト、一般技術文書、規格、安全手順等。

処理：著作権・ライセンス整理済み。直接モデルの事前学習に投入。

## 企業提供データ (Enterprise Restricted)

特性：工場ログ、保全履歴、CAD/CAEデータ、走行環境データ。

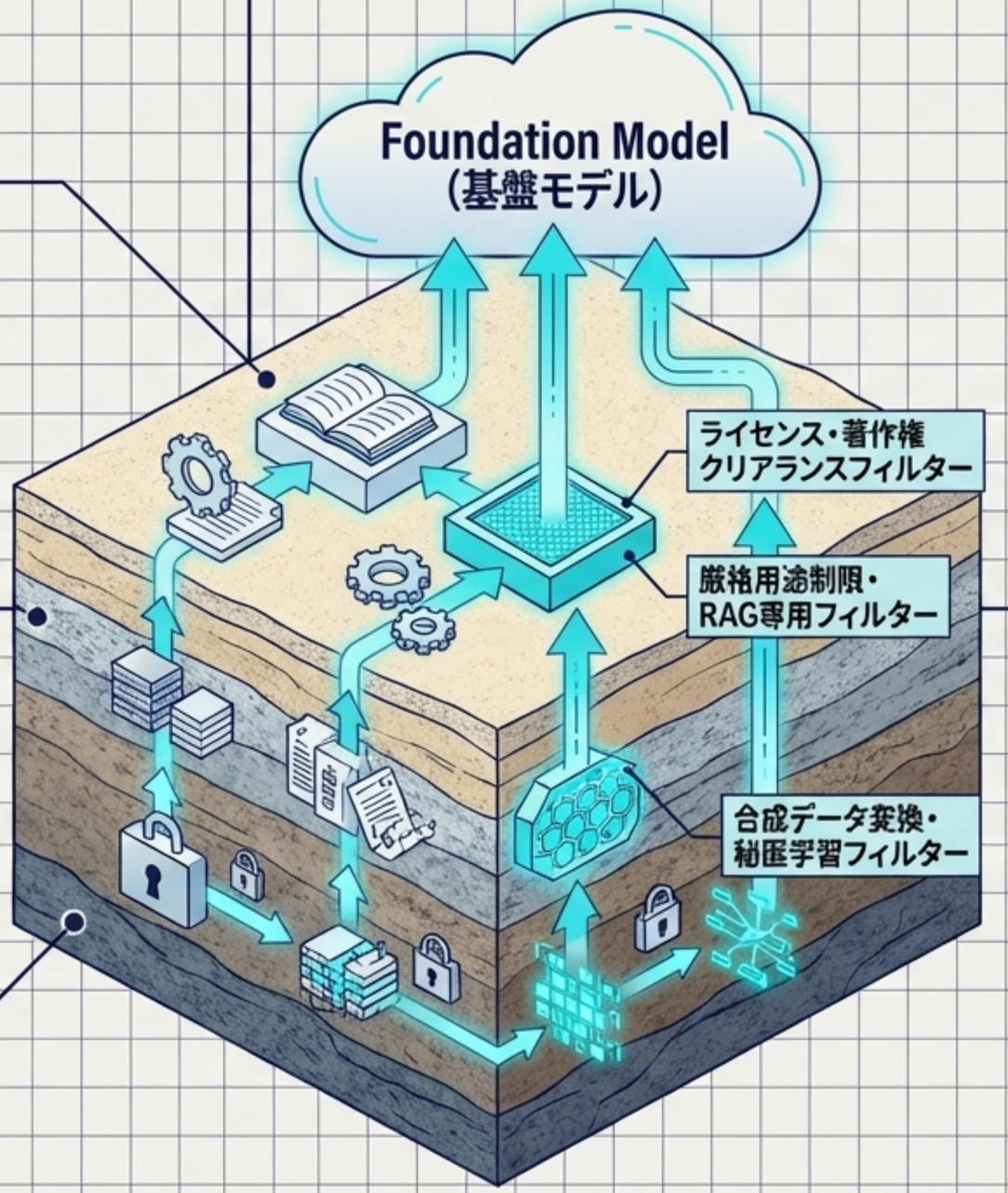
処理：契約により「用途・保管・再配布」を厳密に制限。特化型モデルのファインチューニングやRAG（検索拡張生成）で活用し、ベースモデルの重みには混入させない。

## 秘匿前提データ (Highly Secret / Regulated)

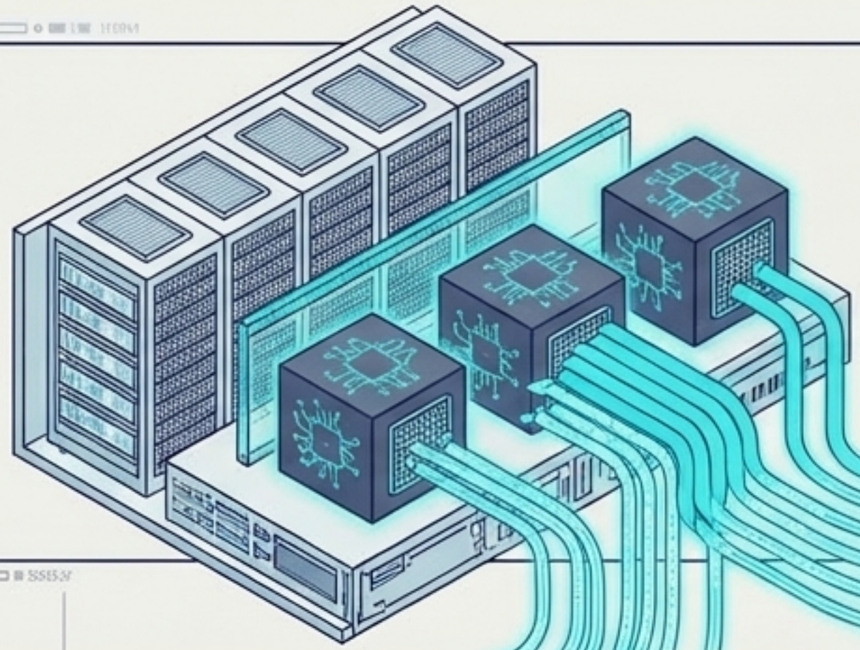
（秘匿）秘匿前提・データ (Highly Secret / Regulated)

特性：作業員の映像・音声（個人情報）、極めて機密性の高い営業秘密データ。

処理：外部持ち出し厳禁。エッジ側での秘匿学習や、ソフトバンクの差分プライバシー技術を用いて「合成データ (Synthetic Data)」へ変換してから学習層へ引き上げる。




**致命的リスク:**
この分離設計を誤り、企業秘密がモデルの「コア」モデルの「重み」に混入した場合、モデルの公開や他社提供が不可能になる（後戻り不能の汚染）。

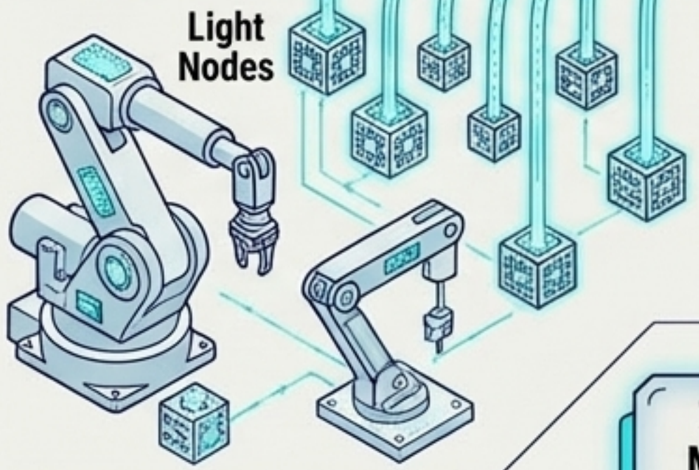


Heavy Nodes

## Heavy Cloud Inference（重い推論）

**国内クラウド / HPC基盤**

- 役割：モデルの設計・計画・学習・高度な統合論理推論。
- 制約：膨大な電力とGPUを消費。データ主権のため国内立地が必須。
- 用途：シミュレーション、合成データ生成、全体最適化計画。



Light Nodes

## Light Edge Inference（軽い推論）

**エッジ / オンプレミス基盤**

- 役割：実時間での物理制御・認識・対話・監視。
- 制約：極低レイテンシ要件（ミリ秒単位）、ネットワーク切断時も停止が許されない絶対的な可用性（自動運転等）。
- 用途：車載ECU、ロボット制御器、工場内専用サーバーでの推論。

フィジカルAIの運用において、「クラウド一択」は成立しない。
MoE（Mixture-of-Experts）や蒸留（Distillation）技術を用い、
エッジデバイスに搭載可能な軽量・高効率モデルの派生が不可欠。

MAX OPEN
(最大公開)

STRICTLY CLOSED
(完全非公開)

## Max Open
(最大公開)

研究成果とエコシステム基盤

- 学習レシピ、評価ベンチマーク手法、データ生成手法。
- 目的: NEDOの「成果の公開」要件を満たし、国内のAIエコシステム（研究者・開発者）を育成する。

## Tiered / Gated Access
(段階的・制限付き提供)

学習済みモデルの重み (Model Weights)

- 小〜中規模の派生モデルは広範な事業者に提供。
- 1兆パラメータ級の最大モデルは、監査・契約・利用制限を伴う限定提供（APIベース等）。

## Strictly Closed
(完全非公開)

産業用生データ (Raw Industrial Data)

- 参加企業から提供された生データそのものは原則非公開。
- 代替策: データ仕様書、匿名化手順、および生成された「合成データ」を公開することで、透明性と機密性を両立。

## 高信頼・安全運用マネージド (Managed Services)

収益性タッグ

収益性：高マージン（継続的ARR）
概要： NECの知見を活かしたAIガードレール、MLOps（継続的学習・運用）、セキュリティ監査、および法令対応を含めたエンタープライズ向けの包括的運用サービス。

## 産業特化型実装支援 (Implementation)

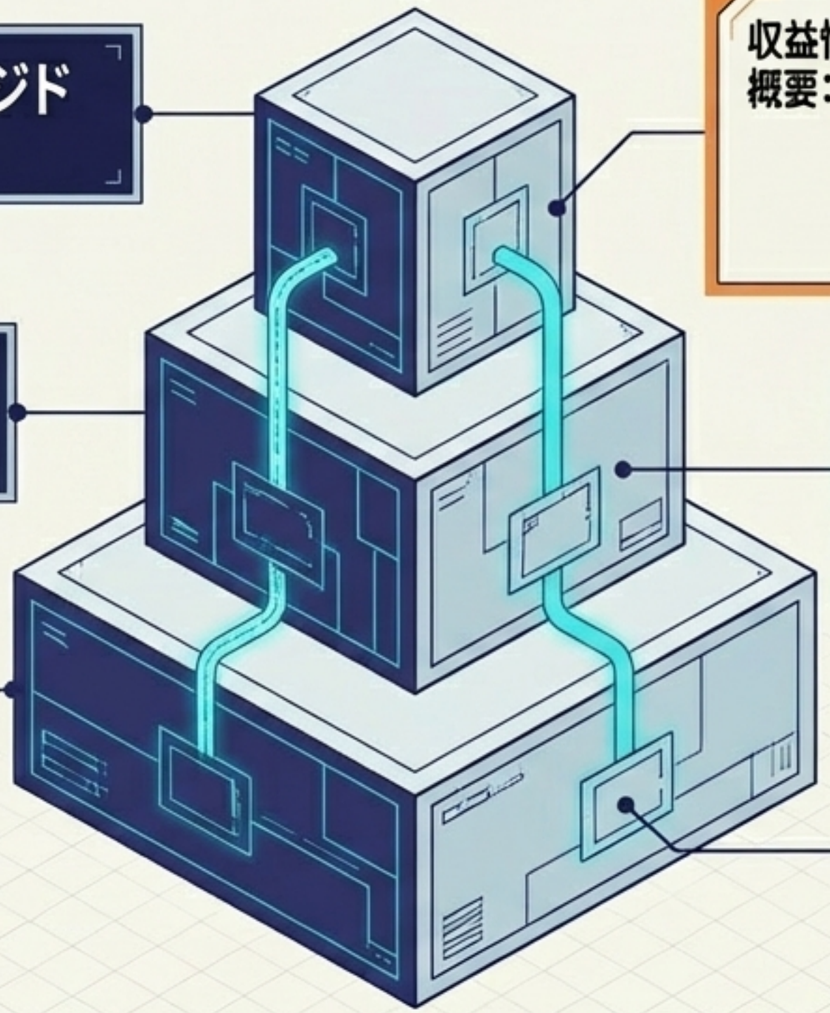
収益性タッグ

収益性：中〜高マージン
概要：出資企業（Honda, Sony等）および外部企業に対する、自動運転・工場制御・ロボティクス向け特化モデルの開発・チューニング支援。

## 基盤モデルAPI提供 (Enabler)

収益性タッグ

収益性：低〜中マージン
概要：「国内事業者への学習済みモデル提供」という国プロ要件を満たすための普及層。エコシステムを形成し、API経由で推論機能を提供。



**マネタイズの中心は、モデル自体の販売ではなく、「安全な運用」と「産業別への繋ぎ込み（SI・マネージド）」に置かれる。**

## 知財と優先権のバランス
(IP Rights & Exclusivity)

**課題**

学習データ由来の権利が重みに混入した場合の責任分界界点。出資企業（自社実装）の「優先権」と、国プロ要件である「広い提供」の矛盾。

**対策**

追加出資や再委託が増えることを見据えた、初期段階での厳密なライセンス規定とクリーンルーム設計。

## サプライチェーン統制
(Supply Chain & GPU Limits)

**課題**

汎用基盤モデル市場は「**海外の貿易管理規制の域外適用（米国の対中半導体規制など）**」に直接左右される。

**対策**

クラウド・半導体のサプライヤー契約における**越境リスクの排除**。AI版SCM（調達・保守・更新の供給網設計）の確立。

## グローバル法規制対応
(Global Regulatory Compliance)

**課題**

個人情報保護委員会(PPC)や経産省ガイドラインへの対応。対応。さらに、欧州で発効した「**EU AI Act**」。

**対策**

日本企業がEU域内で「**高リスク用途**（重要インフラ、安全関連、ロボット制御等）」にAIを展開する場合、モデル提供者として**適合証明**が必須となる。

Sovereign / Domestic Focus

Global Broad Tech

## Domestic Enterprise IT
（国内エンタープライズAI）

- 富士通(Takane)、ストックマーク(100B LLM)
- 企業内文書、日本語特化の業務効率化。

## 日本AI基盤モデル開発

- 「主権データ × フィジカルAI」
- PFNの技術力(GENIAC)と、出資社の製造・物理デバイス網を独占的に結びつけ、米中巨大資本との直接対決を避ける特異点。

## US Tech Giants
（米ビッグテック）

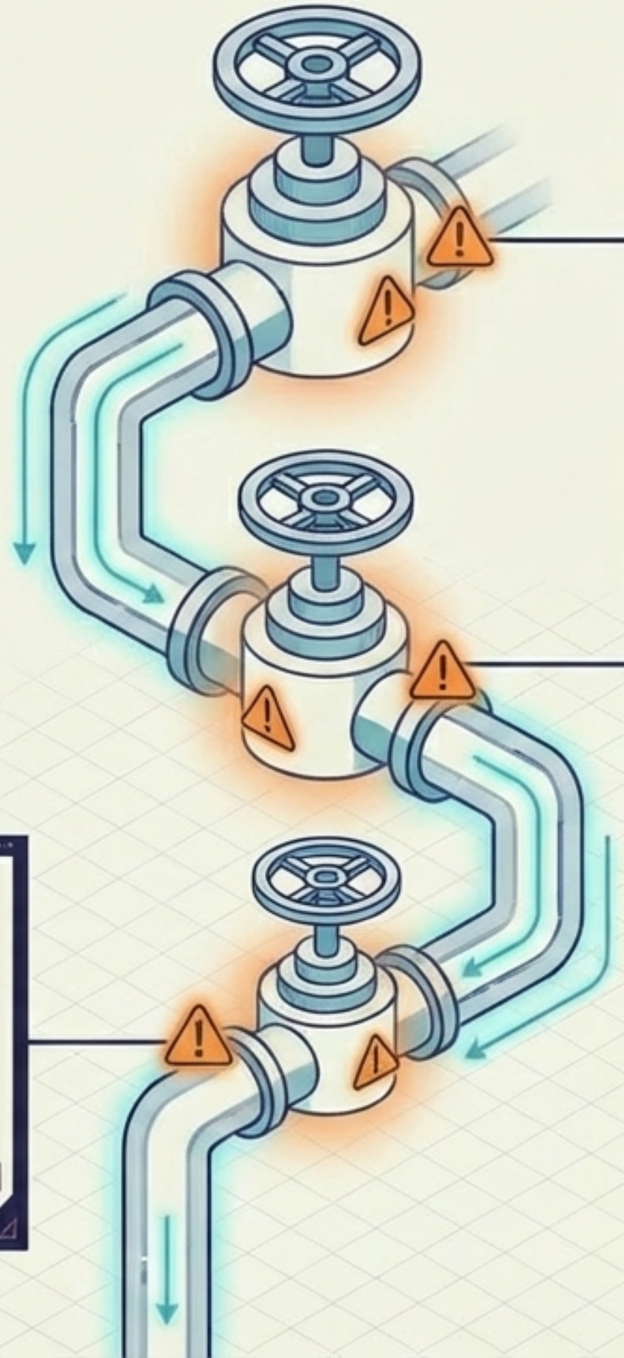
- OpenAI, Google, Anthropic
- 圧倒的な資金力と汎用Webデータ。

## Global Autonomy
（グローバル自律制御勢）

- Tesla, Nvidia (Isaac)
- ロボティクスと自動運転の垂直統合。

Digital / Cyber Focus

Physical / Industrial Focus



## 計算資源と電力
(Compute & Power Limit)

- 現状：1兆パラメータ級の学習には数万基の最新GPUと、それを支えるデータセンター・電力・冷却設備が必要。
- リスク：国内単独での調達難航。資金ショート、または学習速度の低下による相対的陳腐化。

## データガバナンスと権利
(Data Rights Clearance)

- 現状：産業データには営業秘密や個人情報が複雑に絡む。
- リスク：契約処理の遅れ。データ提供企業が「自社ノウハウの流出」を恐れて高品質な実データの提供を渋る「構想倒れ」化。

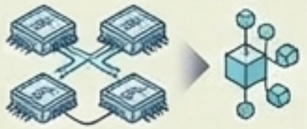
## 組織アジリティと人材
(Talent Consolidation)

- 現状：各社から集められた約100人の高度技術者による混成組織。
- リスク：出身母体の異なる技術者の間で、意思決定ラインや評価制度が不明確になり、開発スピードが米中のスタートアップに劣後する。

## YEAR 1: 2027（短期）

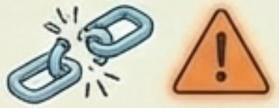
Milestone:
NEDO採択・
モデルα版提示

**Success (上):**



パートナー企業でのPoC開始。GPU安定稼働。

**Failure (下):**



資源確保遅れによる構想倒れ。

**[Real KPIs]**

- GPU稼働率
- 産業別データ契約締結件数
- 安全評価パイプライン整備有無

## YEAR 3: 2029（中期）

Milestone:
マルチモーダル能力
実証（NEDO中間目標）

**Success (上):**

合成データの供給能力確立。派生モデルの国内エコシステム循環。

**Failure (下):**

ベンチマークで他社に埋没。提供形態が曖昧でエコシステム不成立。

**[Real KPIs]**

- 合成データ供給能力
- 推論コスト（円/1k tokens）
- 重大インシデント件数

## YEAR 5: 2031（長期）

Milestone:
実空間統合推論
（NEDO最終目標）

**Success (上):**

複数産業での自律制御実現。海外（EU等）への高信頼モデル輸出。

**Failure (下):**

維持費（GPU/電力）が重荷となり事業縮小。

**[Real KPIs]**

- 継続収益（ARR）
- 省電力化指標（推論電力/性能）
- 導入企業の生産性改善実測値

# STAKEHOLDER ACTION GRID: 構造化された推奨事項 (Structured Recommendations)

Blueprint for Coordinated Execution & Risk Mitigation.

## STAKEHOLDER 1: 出資コンソーシアム (The Consortium)

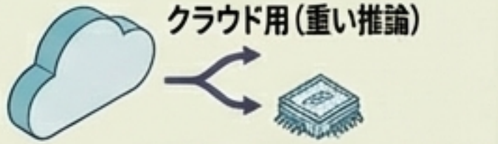
【優先度:高】

### データ契約の「仕組み化」 (最初の90日)

個別案件ごとの権利交渉を廃し、「再配布条件・知財帰属・合成データ変換プロセス」を標準テンプレート化する。知財侵害のクリアがNEDO審査の絶対条件。

【優先度:中】

### 推論製品の二層設計

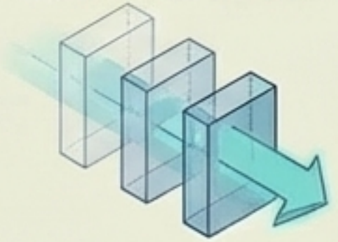



最大モデル一本勝負を避け、体系を早期設計し、電力コストを抑制する。

## STAKEHOLDER 2: 政策・政府 (Government / NEDO)

【優先度:高】

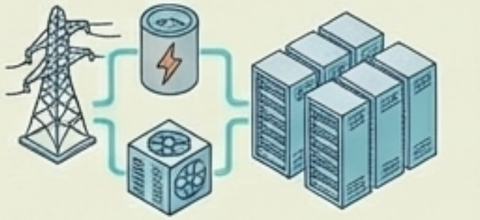
### 評価基盤の先回り整備



マルチモーダル・実機統合における「安全・省電力の標準ベンチマーク」を官民で策定し、ステージゲート評価の基準を透明化する。

【優先度:中】

### 調達とGXの連動支援



GPU調達を単なる設備投資ではなく国家ボトルネックと位置づけ、再エネ・冷却技術と連動した省エネ運用を支援要件化する。

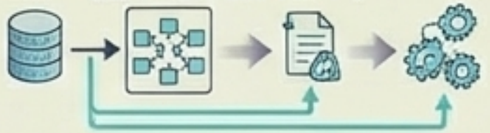
## STAKEHOLDER 3: 研究・学術機関 (Academia)

【優先度:高】

### 合成データと失敗モードの検証

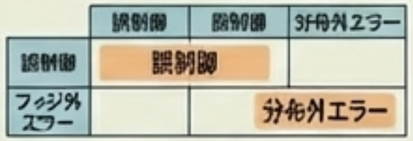
産業データ不足を補う「合成データ」の品質保証(偏り・再識別リスク)を学術検証する。

### 合成データ品質保証 (偏り・再識別リスク)



産業データ不足を補う「合成データ」の品質保証(偏り・再識別リスク)を学術検証する。

### フィジカルAI特有の「失敗モード」テスト体系




誤制御・分布外エラー等、フィジカルAI特有の「失敗モード」テスト体系を構築する。