

「実世界ネイティブ AI」という賭け

——日本は AI 主権を確立できるのか、新たな依存を生むのか—— 政策ブリーフ

詳細版「『実世界ネイティブ AI』という賭け」の要約版

発行日：2026 年 7 月 22 日 発行元：一般財団法人日本危機管理研究所

問題の所在

2026 年 7 月、ソフトバンク・ソニー・NEC・ホンダ中核の新会社 Noetra が、NVIDIA の GPU 約 27,500 基を用いた国家規模の AI 計算基盤構築を発表した。経産省・NEDO は 5 年で総額 1 兆円規模とされる支援を行う（この金額は政府一次資料には明記がなく、報道の一致に基づく）。本稿は、この「国産 AI」計画が、データ・モデル・計算資源・電力/制度という 4 層のどこまで日本の主権が及ぶ実質を伴っているかを、一次資料に基づき検証する。

図 1 AI 主権の四層評価フレームワーク

AI 主権の四層評価フレームワーク（提案）

「国産 AI か否か」の二択ではなく、4 つの軸で主権の実質を評価する

評価軸	問うべき問い	Noetra の 現状評価
① データ・モデル主権	どのようなデータで学習し、 モデルをどこで開発しているか	国内に実質あり
② 重み・運用主権	学習済みの重みを誰が管理し、 公開時のリスクを誰が制御するか	要検証
③ 計算資源主権	学習・推論を実行する ハードウェアを誰が供給するか	海外依存
④ 電力・制度主権	計算基盤を支える電力・制度を 自国で規律できているか	制度上の空白

※本フレームワークは Noetra に限らず、他国の主権 AI 政策の評価にも適用可能な一般的分析枠組みとして提示する。

「国産 AI か否か」の二択ではなく、4 つの軸で主権の実質を評価する（詳細版第 8 章）

本稿における各軸の現在地

① データ・モデル主権	どのようなデータで学習し、モデルをどこで開発しているか	実質あり
② 重み・運用主権	学習済みの重みを誰が管理し、公開リスクを誰が制御するか	要検証
③ 計算資源主権	学習・推論を実行するハードウェアを誰が供給するか	海外依存
④ 電力・制度主権	計算基盤を支える電力・制度を自国で規律できているか	空白確定

※本フレームワークは Noetra に限らず、他国の主権 AI 政策の評価にも適用可能な一般的分析枠組みとして提示する（詳細版第 2～7 章）

現状評価

Noetraの「国産AI」は、データ層・モデル層では国内に実質があるが、計算基盤（GPU/CPU）は完全に米NVIDIA製に依存する。さらに、経済安全保障推進法の基幹インフラ16分野にはデータセンターに相当する分野が存在せず、この空白は2026年7月17日に閉会した第221回国会でも埋まらなかった——データセキュリティに関する規律は法案に盛り込まれず「次なる課題」とされたことが、参議院の公式調査資料で確認できる。EU（NIS2指令）・米国（CISA）は、いずれもデータセンターを重要インフラとして明示的に位置づけており、日本はこの点で異なる制度設計になっている。なお、4層すべてを満たしうる国として中国・ロシアの2カ国による予備的検証を行ったところ、権威主義体制であっても計算資源主権（半導体自給）までは完全には満たせないことが分かった。民主主義国にとって現実的な優先順位は、4層の一挙な統制ではなく、基幹インフラ制度の対象範囲を漸進的に拡張することにある。

提言

- **提言①** 自律ロボット制御AIに対する、OT/ICS領域を含めた安全性検証・レッドチーミングの標準的な枠組みを、業界横断で整備する。
- **提言②** 秘匿性の高いデータで学習したモデルを公開する際の、反転攻撃耐性評価・署名検証等を含む技術的ガイドラインを、公開前に整備する。
- **提言③** データセンター・AI計算基盤を、基幹インフラ制度上どう位置づけるか（インフラ指定型かデータ保護型か）の方向性を、次の法改正サイクルを待たず早期に確定する。
- **提言④** 特定国・特定企業への計算資源依存を緩和するため、供給網の多元化や国内代替技術の育成を、中長期的な政策課題として位置づける。

本ブリーフの位置づけ

本ブリーフは、Noetraの投資規模の国際比較（仏・サウジ・印・英・韓・独・加）、フィジカルAIの物理セキュリティ、モデル重み公開のリスク、半導体供給網、基幹インフラ制度の日欧米比較に加え、四層フレームワークが「4層すべてを満たしうる国」として中国・ロシアにも当てはまるかを検証した詳細版の要約である。中国・ロシアは、投資規模の比較対象国とは異なり、フレームワークの妥当性・限界を検証するための別個の参照点として扱っている。詳細版では、各提言の根拠となる一次資料とその検証過程を明示している。