

令和8年「人工知能基本計画」の深層

自律行動型AI時代の国家戦略と「アジャイル・ガバナンス」の現実

Executive Summary Card 1



The Catalyst (発火点)

「ツール」から「自律行動型 (Agentic AI)」への不可逆的進化がもたらした、**わずか半年**での異例の国家戦略改定。

Executive Summary Card 2



The Strategy (勝ち筋)

汎用LLMでの正面衝突を避け、日本の無形資産 (現場データ) を活かした「**バーティカルAI × フィジカルAI**」の統合。

Executive Summary Card 3



The Reality (現実と課題)

「社会実装の速度」と「ガバナンスの速度」の非同期。**拙速な政策決定プロセス**が孕む「**ソーシャル・ライセンス**」喪失のリスク。

国家を突き動かしたパラダイムシフト：異例の「半年改定」

2025 Before

「ツールとしてのAI」

- ・対話・文書作成の受動的支援



2026 After

「自律行動型AI / Agentic AI」

- ・自ら計画・実行・検証・修正を繰り返す能動的主体

通常の政策サイクル：数年単位での法整備と計画改定

令和7年(2025)12月：
初回AI基本計画閣議決定

わずか半年

令和8年(2026)6月：
第1期計画（素案）承認・パブコメ開始

Core Insight Box

国力（経済力・防衛力・技術力）そのものを根底から再定義する脅威と機会への「焦り」が、異例のスピード改定のトリガーとなった。

基本構想：「信頼できるAI」を基軸としたAI主権の確立



産業政策の枠を超え、国家の生存を賭けた「経済安全保障政策」への昇華。
計算資源、データプラットフォーム、基盤モデルの完全な自律確保へ。

日本の「勝ち筋」：バーティカルAIとフィジカルAIの統合エコシステム

フィジカルAI

サイバー空間の判断を物理空間で実行。産業用ロボット、自動運転車、インフラ制御装置を通じた直接的な現実世界の操作。

バーティカルAI

領域特化型AI。汎用LLM（米国・中国資本）との正面衝突を避け、特定産業において極めて高い精度の判断を下す基盤。

現場データ

日本最大の無形資産。製造業、素材産業、インフラ管理などの現場に蓄積された高品質な暗黙知と経験データ。



ソフトウェア（サイバー空間）の弱点を、ハードウェア（物理空間）の圧倒的強みで補完する独自のエコシステム構築戦略。

実行体系：4つの基本原則と4つの基本方針の連動マトリックス

4 Fundamental Principles

4 Policy Pillars

	イノベーション促進と リスク対応の両立	挑戦と学習 (まずやってみる)	アジャイルな対応 (永遠のβ版)	内外一体での 政策推進
Offense / 攻め 1. AIを使う (利活用の加速) 2. AIを創る (開発力の強化)		使う × 挑戦 社会全体を再設計する 「AIトランスフォーメーション (AX)」	創る × アジャイル ステージゲート方式による1兆円超の 機動的投資	
Defense / 守り 3. AIの信頼性を高める (ガバナンス主導) 4. AIと協働する (継続的変革)	協働 × リスク対応 「Human Agency (人的主体性)」の維持と リベラルアーツ重視			信頼性 × 内外一体 AISI体制倍増と 広島AIプロセスの拡充

攻めの双発エンジン：AI社会実装（AX）と開発力への1兆円投資



守りと進化の両輪：アジャイル・ガバナンスとHuman Agency

信頼性の担保 (Institutional Governance)

- AIセーフティ・インスティテュート (AISI) の抜本的強化：専門人材を約30名から約60名へ倍増。
- 電子透かし技術開発によるディープフェイク・偽情報対策。
- 米国(US AISI)・英国(UK AISI)と連携する広島AIプロセスの拡充。

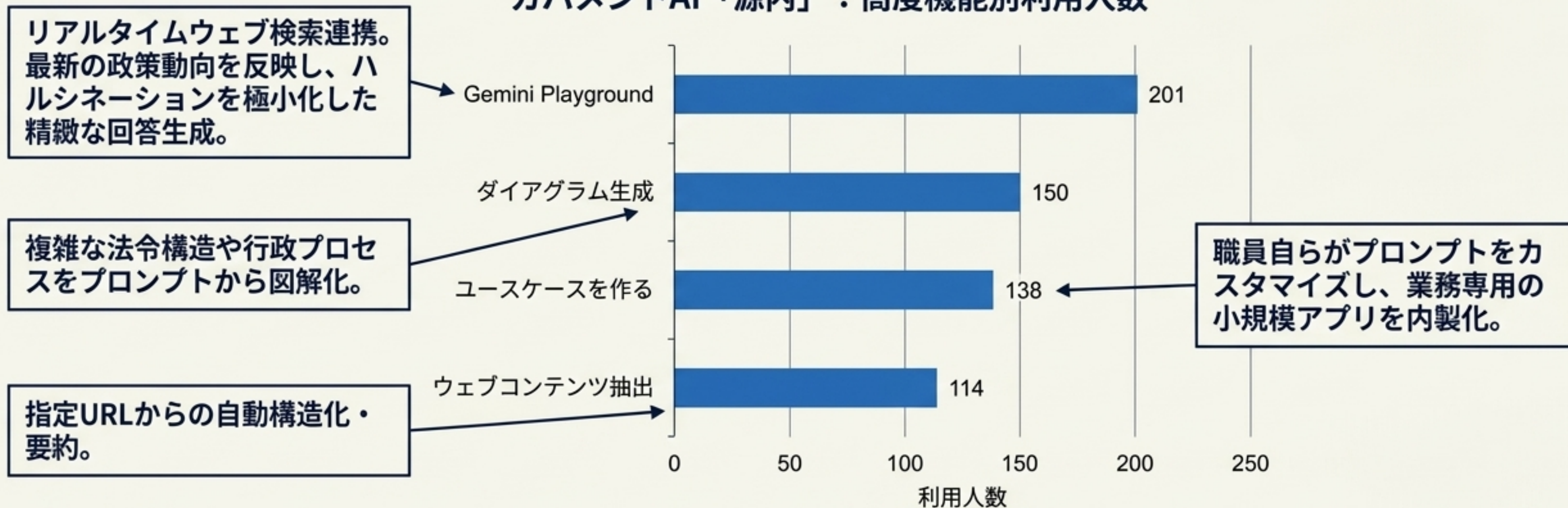
人間中心の協働 (Societal Evolution)

- 「アドバンスト・エッセンシャルワーカー」への移行支援 (AIで労働の付加価値を向上)。
- Human Agency (人的主体性) の探求：AIへの過度な依存による「浅慮」や能力退化の警戒。
- あえてAIを用いない「オフライン学習」とリベラルアーツ教育の再設計。

旗艦施策①：ガバメントAI「源内」がもたらす行政AXの衝撃

18万人規模（全省庁）で展開される国内最大規模のガバメントAI導入。

ガバメントAI「源内」：高度機能別利用人数



厚労省（えるぼし認定審査等）での専門的・機微な判断領域への実装検証が進行中。
「隗より始めよ」の完全な体現。

産業政策としての「源内」：国産AIエコシステムの需要創出ポンプ

Ecosystem Pump

政府の巨大調達

18万人規模の「源内」において、国内開発のLLMを優先的に調達。安定した需要と資金を国内ベンダーへ供給。



日本語・文化適合モデルの育成

資金循環により、日本語特有の複雑な語彙や日本の価値観に適合した国産基盤モデルの性能向上を支援。



デジタル庁によるデータインフラ投資

「政府共通の大規模データセット」の精製・整備。国産AI開発最大のボトルネック(クリーンな日本語データの不足)を政府自ら解消。

CORE INSIGHT: 単なる業務効率化ではない。政府自身が「ファーストカスタマー」となり、国内AI産業の自律性を買い支える国家インフラ投資。

旗艦施策②：サイバー防衛のパラダイムシフト「Project YATA-Shield」

自律型サイバー攻撃

Agentic AIによる自律的行動。
自ら脆弱性を発見
→ 攻撃手順の構築 → 実行 →
防御への適応・修正を「超高速」
で展開する非対称の脅威。

八咫の盾 / YATA-Shield

攻撃者に技術的優位性が
確立される前に、防御側が
同等以上のAI能力を行使する
「AI vs. AI」の防衛ドクトリン。

15の重要インフラ分野への展開指令。未知の脅威を正確に照らし出す国家の決意。

官民連携の実践：アジャイルな脆弱性管理と金融セクターの先行事例

司令塔：NISC（インシデント指揮）＋ AISI（脆弱性情報・脅威インテリジェンス評価）

経営層のリーダーシップ

サイバー対策をIT部門の課題から、組織存続の「必須投資」へと引き上げ。

AI活用による脆弱性対応の高速化

リリース前/後の双方でAIを駆使し、パッチ作成サイクルを超高速化。

Case Study（金融分野の先行実践）

日本銀行(BOJ)と金融庁(FSA)の主導による「CSSA (Cybersecurity Self-Assessment)」ツールの推進。同業他社ベンチマークを通じたプロアクティブなAI診断体制の構築。

専門家による評価（期待）：産業界が支持する「反転攻勢」の土台

巨額投資の予見性

「1兆円超のAI関連施策」と大胆な投資・研究開発税制の深掘り。企業が長期投資に踏み切るための明確なシグナル。

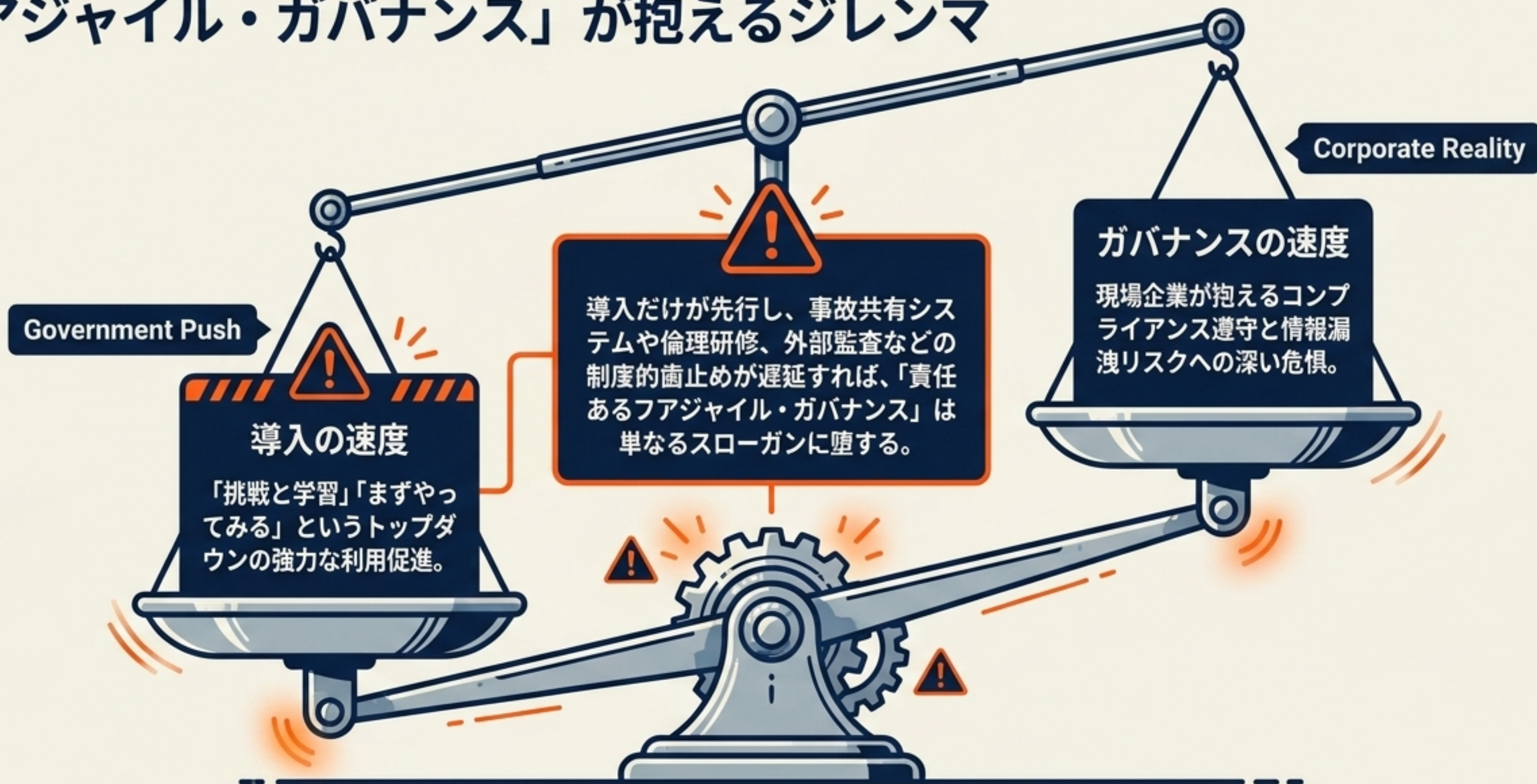
資金配分の合理性

経済産業省が主導する「ステージゲート方式」。限られた国家予算を機動的かつ最も効率的に配分する政策イノベーションへの高い評価。

主戦場の明確化

ソフトウェア領域での劣勢を認め、日本の強みである「エッジAI」や「ハードウェア統合（ロボティクス）」を戦うべき主戦場として定義した戦略的意義。

専門家による評価（懸念）： 「アジャイル・ガバナンス」が抱えるジレンマ



矛盾の連鎖: リスクへの過剰警戒で現場が萎縮すれば、最大の武器である「現場データ（暗黙知）の集積」という日本の勝ち筋が根本から崩壊する。

政策プロセスの異常値：「4日半」のパブコメが示唆する国家の焦り



事実

令和8年(2026)6月19日(金)夜~23日(火)夜。実質週末末を挟んだ「わずか4日半」のパブリックコメント期間（通常は行政手続法で原則30日以上）。

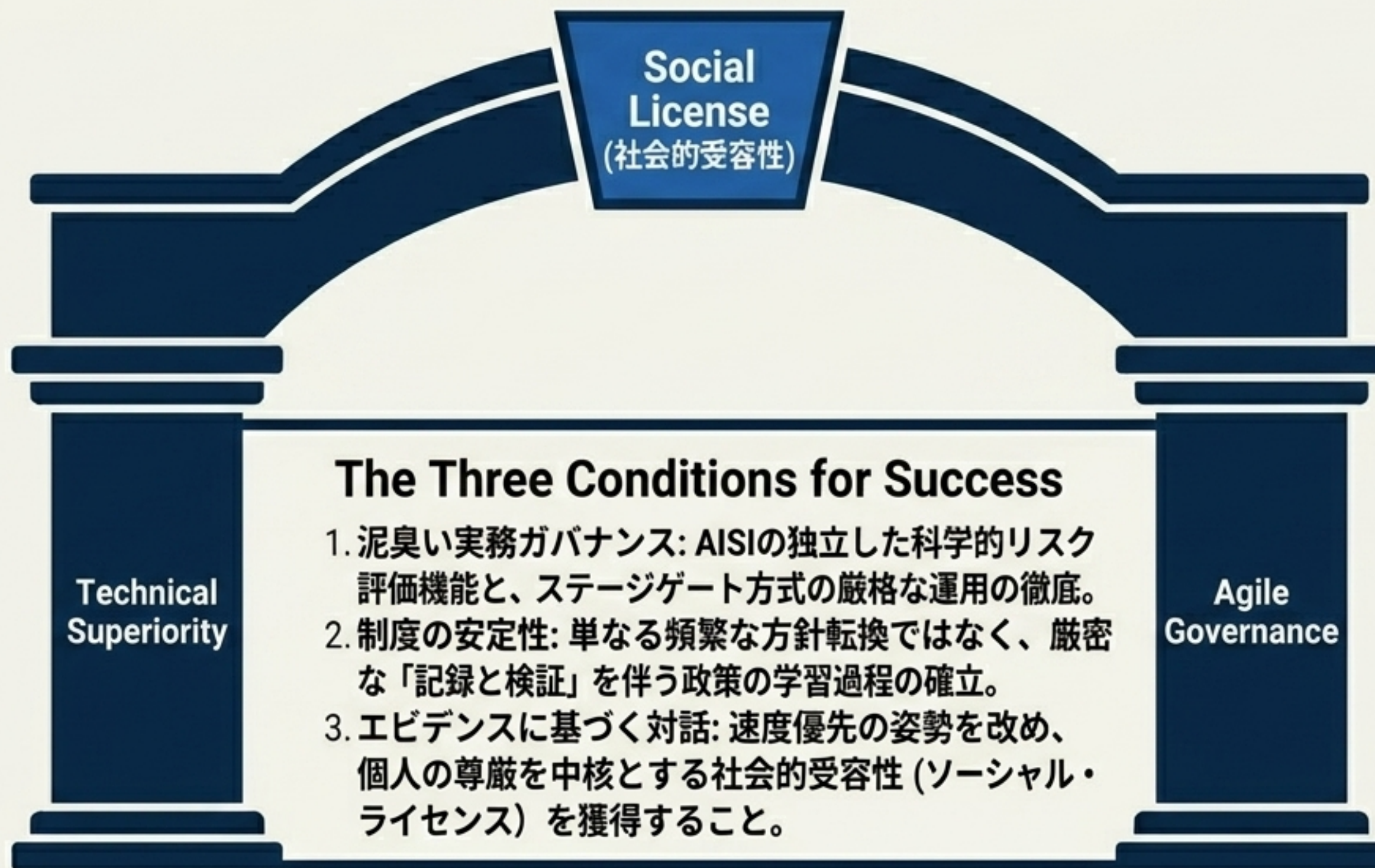
背景にある焦り

直近に迫る国際的AIサミットの日本開催に向けたスケジュール優先。外交的モメンタムを最優先した政治的判断。

副作用とリスク

- ・「永遠のβ版」という名目のもとで生じる制度の不安定さが、民間投資の予見性を著しく毀損する。
- ・国民に痛みを伴うAX（構造変革）を迫る以上、透明性の高い対話プロセスが欠如すれば社会の反発を招く。

結論：真の「日本型AIエコシステム」を成立させる条件



野心的かつ合理的な青写真である「社会全体のAX」は、政府の号令のみならず、国民的合意と継続的な対話という土台の上でのみ成立する。