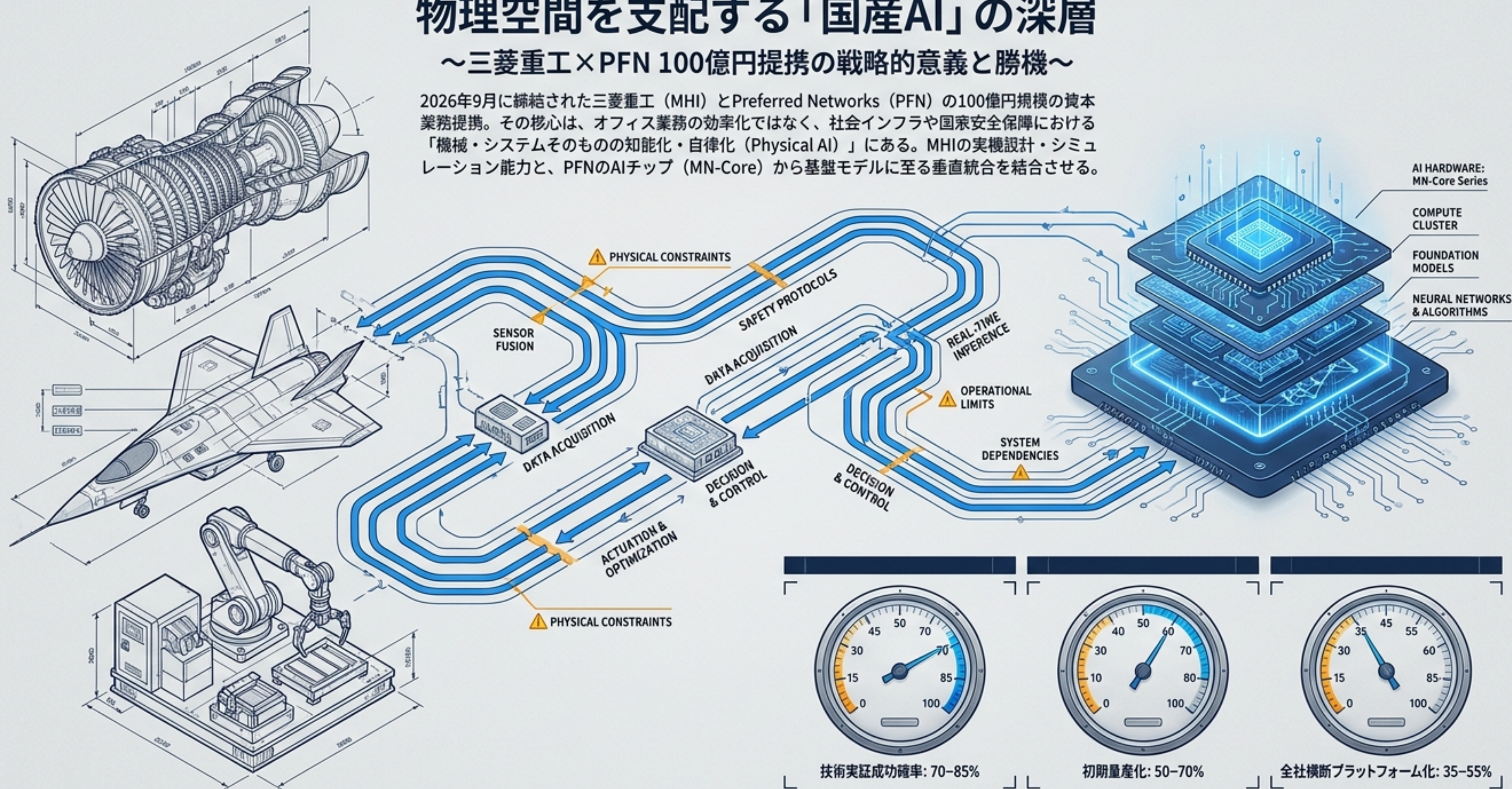


物理空間を支配する「国産AI」の深層

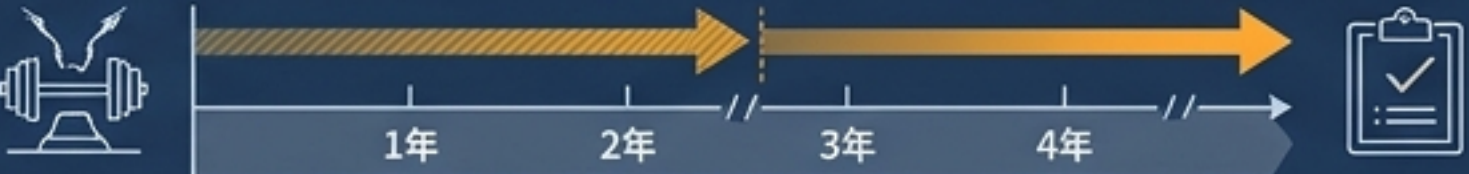
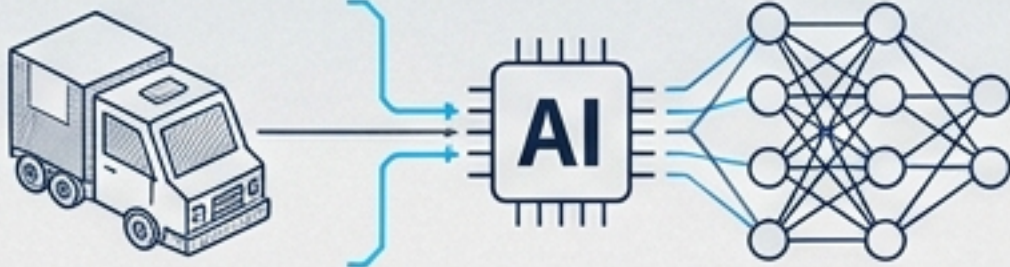
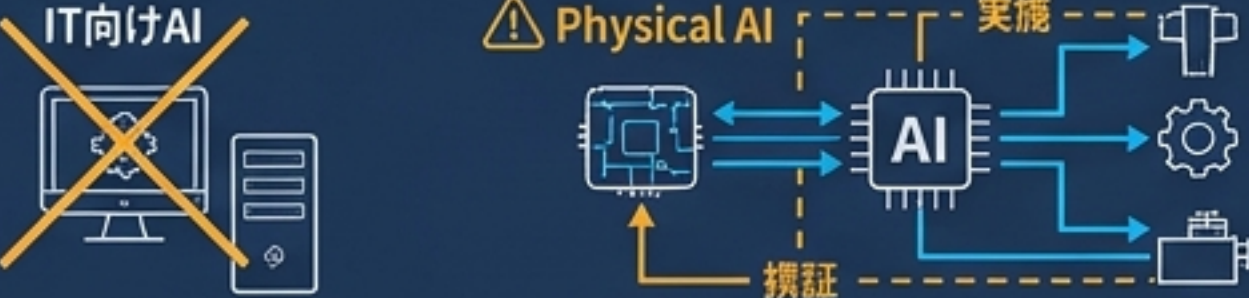
～三菱重工×PFN 100億円提携の戦略的意義と勝機～

2026年9月に締結された三菱重工（MHI）とPreferred Networks（PFN）の100億円規模の資本業務提携。その核心は、オフィス業務の効率化ではなく、社会インフラや国家安全保障における「機械・システムそのものの知能化・自律化（Physical AI）」にある。MHIの実機設計・シミュレーション能力と、PFNのAIチップ（MN-Core）から基盤モデルに至る垂直統合を結合させる。



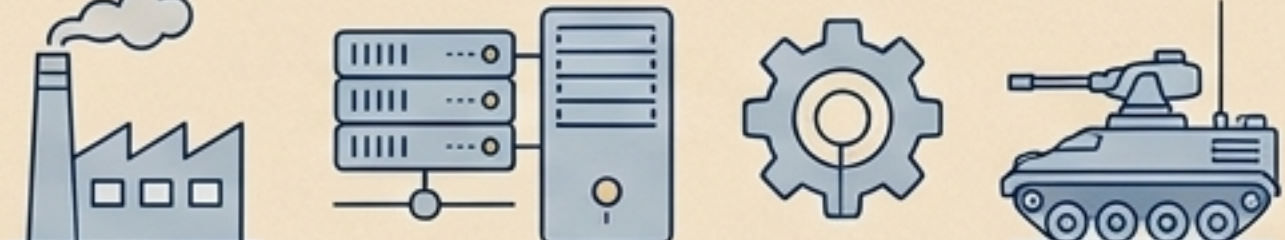
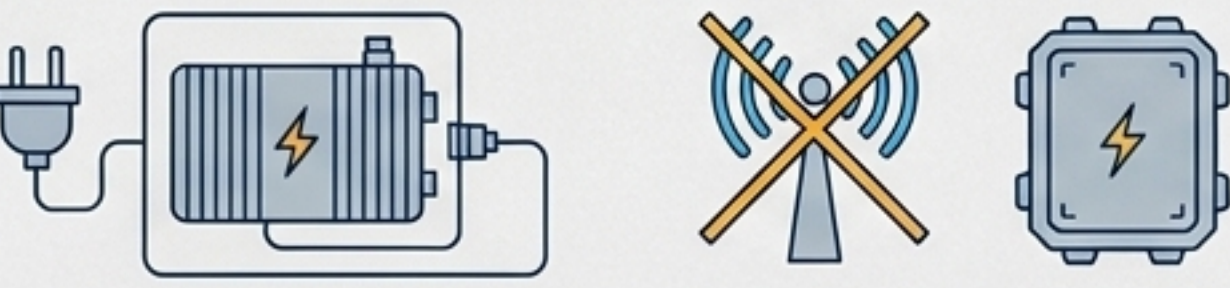
ニュースリリースの表層と、未公開データに潜む実態

2026年6月の基本合意から9月の100億円出資へとフェーズが進んだが、多くの重要指標はベールに包まれている。
100億円は「出資額」であり、R&D予算の規模や最初のターゲット製品は未だ公開されていない。

		ファーブ (公式 PR)	ディープ (専門家評価)
対象分野		社会インフラ、国家安全保障	⚠ エネルギー、輸送、防衛へ波及可能。個別製品は未公表。 
出資・予算		MHIからPFNへ100億円出資 	⚠ R&D予算とは別。持株比率や経営関与度は不明。 
契約期間		未公開 	⚠ ミッションクリティカル製品の性質上、実態は長期（複数年）必至。 
技術目的		機械・システムの知能化・自律化 	⚠ 「IT向けAI」ではなく、実機と直結する「Physical AI」の構築。 

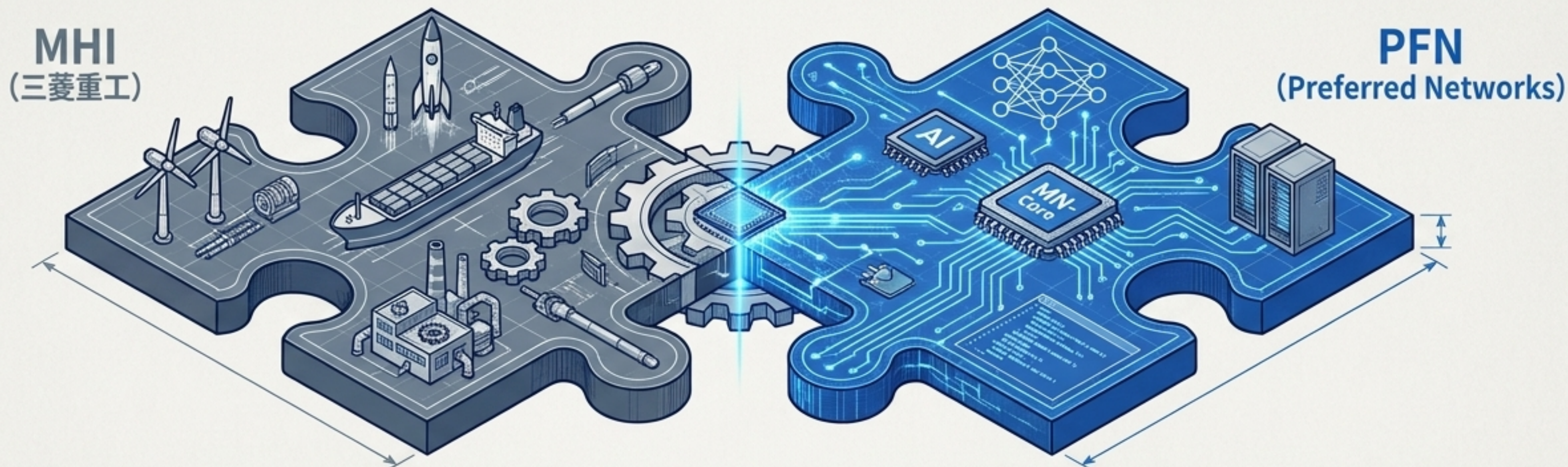
なぜChatGPTはタービンを制御できないのか:「IT向けAI」と「Physical AI」の断絶

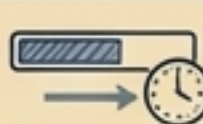
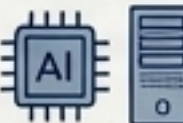
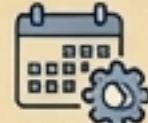
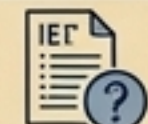
クラウド上の情報系AIと、現場の物理機器を動かす制御系AIでは、要求される技術要件の次元が異なる。
物理システムでは、一度の推論遅延や誤判断が致命的な事故（フェイル）に直結する。

	IT向けAI (Information-based AI)	Physical AI (Mission-critical AI)
		
レイテンシ (遅延)	 平均レイテンシで許容される	 Worst-case latency (最悪実行時間) の保証が必須。 締切超過は「故障」とみなされる。
フェイルセーフ	 リトライ可能、 回答のやり直し 	 致命的事故。フォールバックと 安全側への遷移設計が必要。 
モデルの 更新頻度	 高頻度 (継続学習) 	 厳格な変更管理と段階的再認証を経た 「凍結・認証済みモデル」。
実行環境	大規模クラウド/データセンター 	閉域オンプレミス、機上・エッジ推論、通信断耐性。 

相互補完のパズル：重エプライムとフルスタックAIの結合

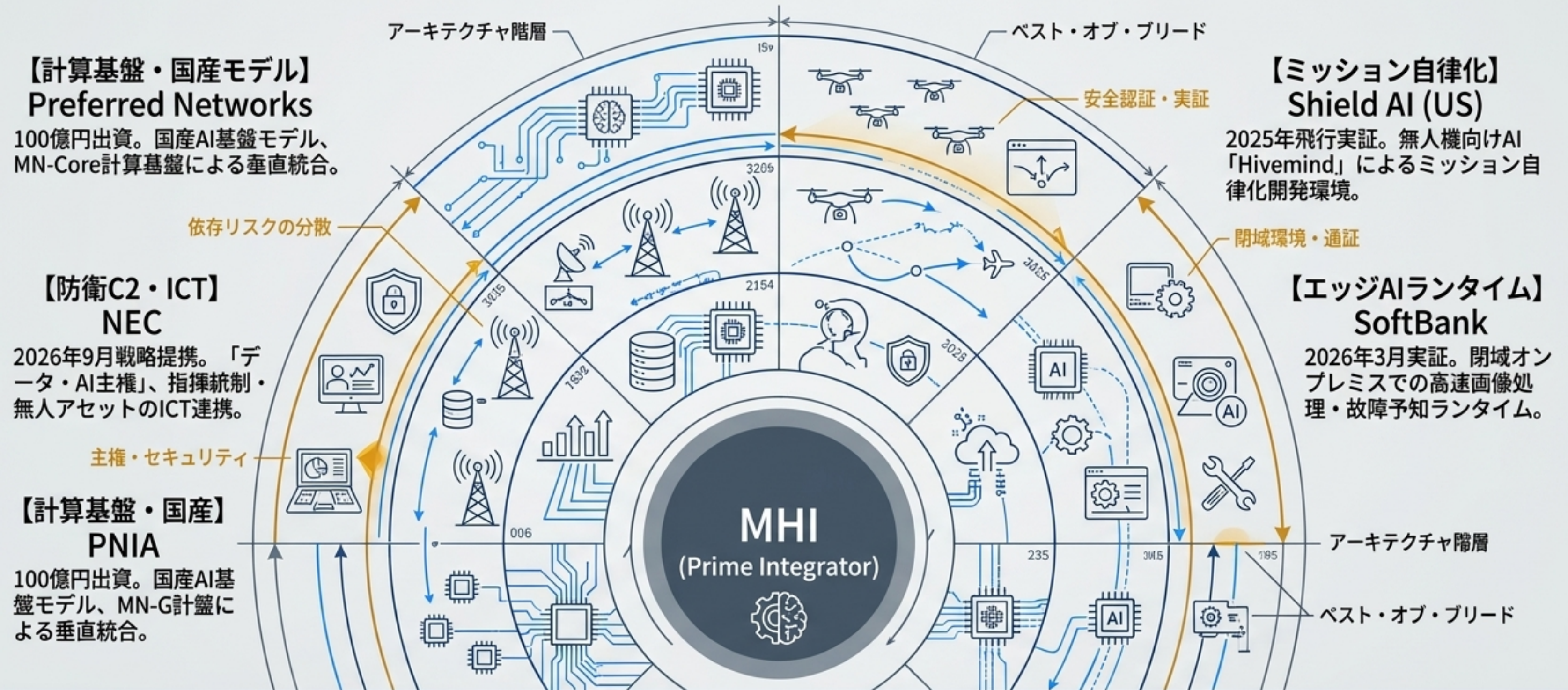
MHIにとってPFNは単なるソフトウェアベンダーではなく、半導体からモデルまでを自給できる戦略的パートナーである。
一方で、PFN単独ではミッションクリティカル特有の「数十年にわたる品質保証」には耐えられない。



MHI		PFN	
【強み・提供価値】	【弱み・課題】	【強み・提供価値】	【弱み・課題】
・実機設計、制御技術、シミュレーション (デジタルツイン)  ・現場の実世界データ  ・安全性要求・認証への深い理解 	・先端AIモデル・AI半導体の短周期での更新能力  ・ソフトウェア中心の開発能力  ・ソフトウェア中心の開発速度 	・MN-Core等のAIチップ、自社スーパーコンピュータ  ・基盤モデル (PLaMo)、産業AIの実装経験  ・フルスタックでの垂直統合 	・重工業レベルの長期間 (数十年) の製品保守  ・IEC 61508等の機能安全認証の取得ノウハウ  ・大規模な24時間フィールドサービス体制 

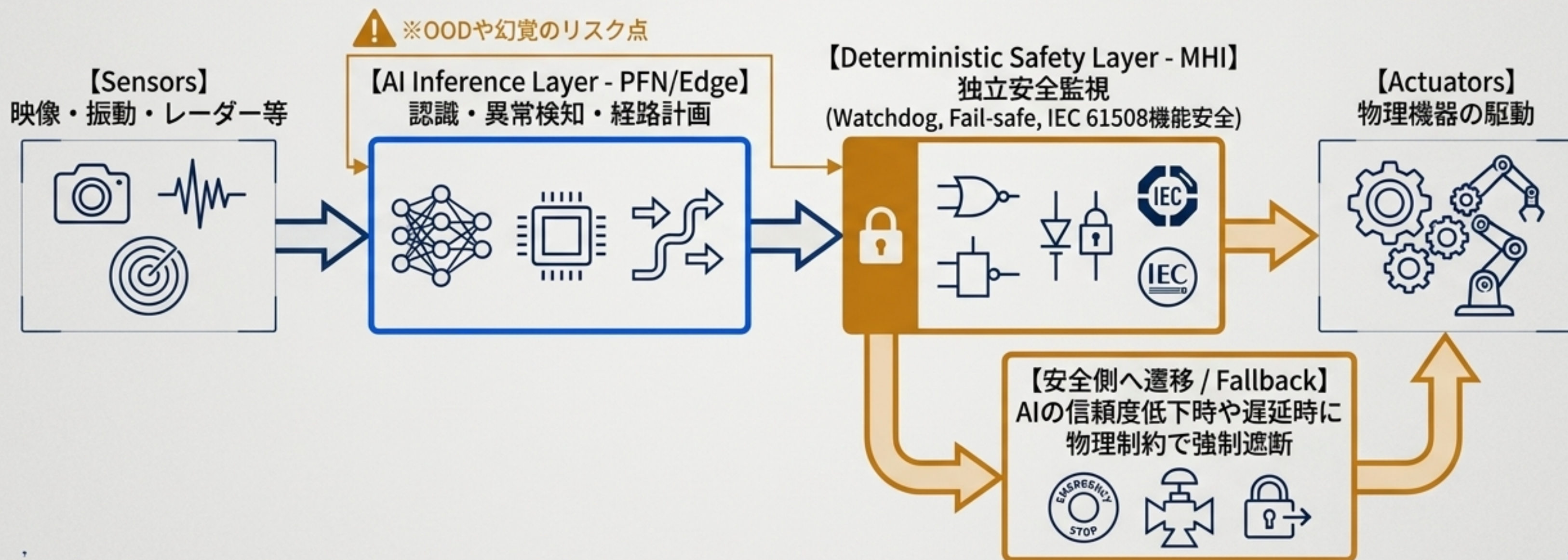
1社依存への拒絶：MHIが構築する「複数レイヤー型AI・自律化エコシステム」

MHIの動きを俯瞰すると、PFNとの独占的な提携ではないことがわかる。2025年～2026年にかけて、用途ごとに最適なパートナー（ベスト・オブ・ブリード）を配置し、ベンダーロックインを回避する複層的なアーキテクチャを形成している。



アーキテクチャの絶対原則：AIを「直接制御」に入れない多層防御

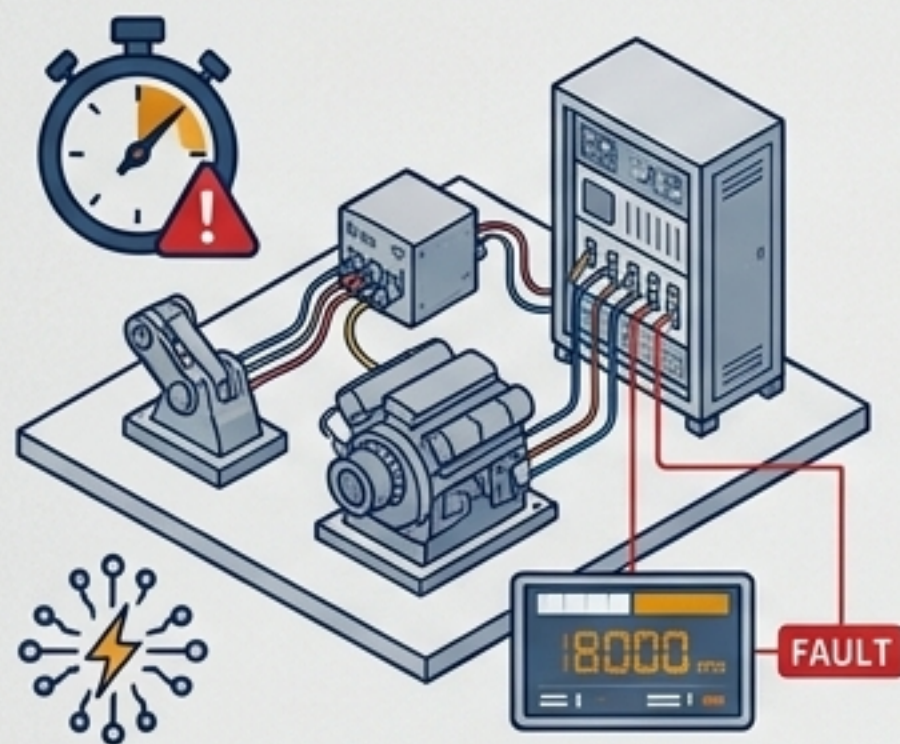
生成AIの持つ非決定性（幻覚や確率的揺らぎ）を物理空間に持ち込むには、AIの推論結果を無条件に信じない「決定論的な安全関所」が不可欠である。AIが認識・計画を行っても、最終的な実行許可は物理制約の枠内に限定される。



ミッションクリティカルAIを阻む「検証と認証」の壁

通常のAIベンチマークでは現場の安全性は証明できない。特に、継続的に賢くなる「AIの学習プロセス」と、変更を許さない「安全認証制度」の根本的な衝突（パラドックス）をどう解決するかが、商用化速度の分水嶺となる。

Pillar 1: リアルタイム性の限界テスト



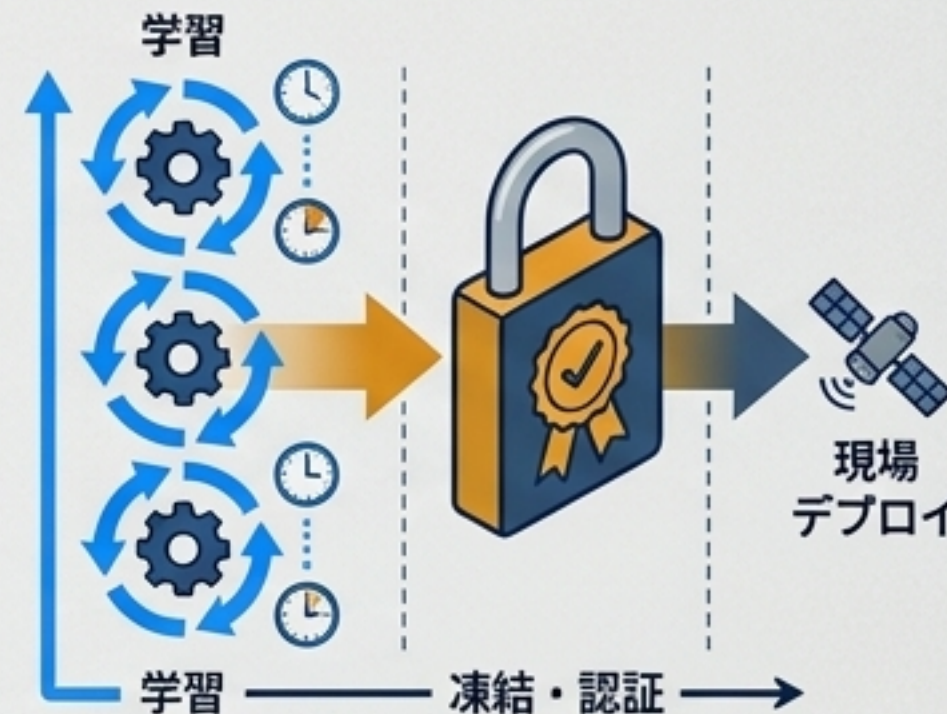
HIL (Hardware-in-the-Loop) 評価による Fault Injection (故障注入)。AIの平均応答ではなく、絶対的な『最悪応答時間』を測定し、遅延を故障として扱う。

Pillar 2: 稀少事象（OOD）の網羅



極端な破損や悪天候の事故データは現実には存在しない。MHIが誇るデジタルツイン・シミュレーションを活用し、合成データによる網羅的テスト環境を構築する。

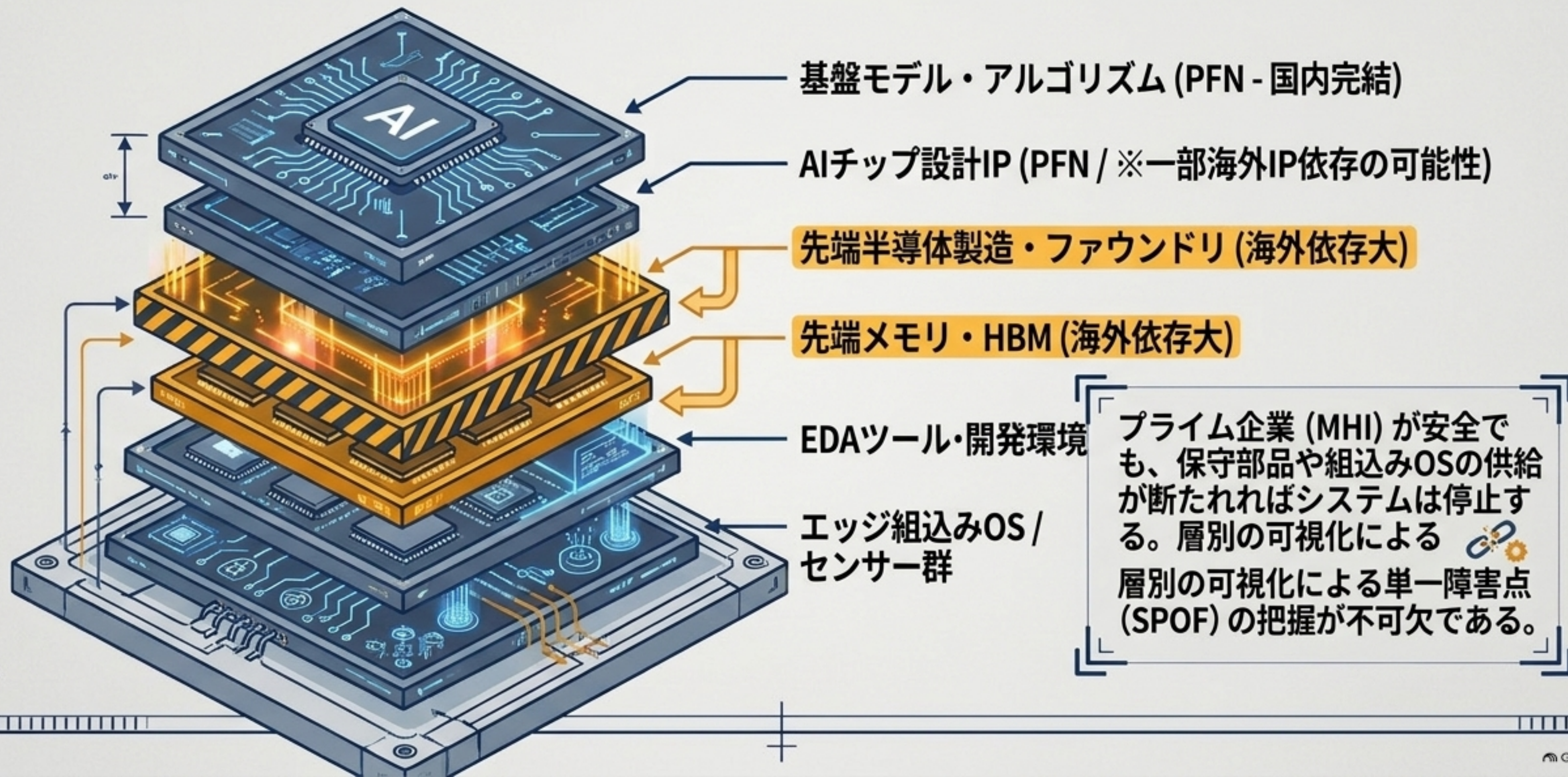
Pillar 3: 【パラドックス】 ⚠ 継続学習 vs 認証 ⚠



AIは毎週モデルを更新したいが、航空・防衛の安全認証は『変更』のたびに根拠の再提出を求める。
解決策として、開発環境で学習を回し、現場へは『凍結された認証済みモデル (Frozen Model)』を段階的にデプロイする手法が必須となる。

「国産AI」の錯覚：サプライチェーンに潜む単一障害点（SPOF）

経済安全保障推進法や外為法の観点から見れば、PFN製AIチップを採用しただけで完全な「データ・AI主権」が達成されるわけではない。深層のハードウェアスタックには、依然として国外依存の急所が存在する。



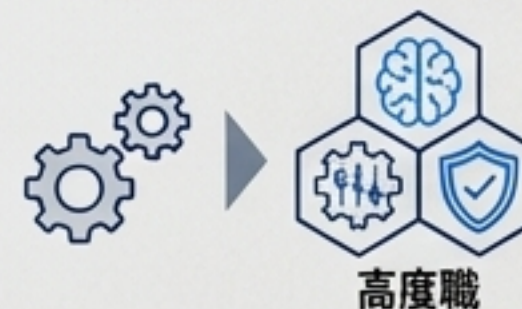
事業化ロードマップ：「Safety-MLOps」市場の誕生と労働力の変容

ミッションクリティカル市場は消費者向けAIより調達サイクルが長く、最先端モデルを作っただけでは直ちに売上にはならない。最初の成果は非破壊的領域から始まり、徐々に高度な自律制御へと移行する。



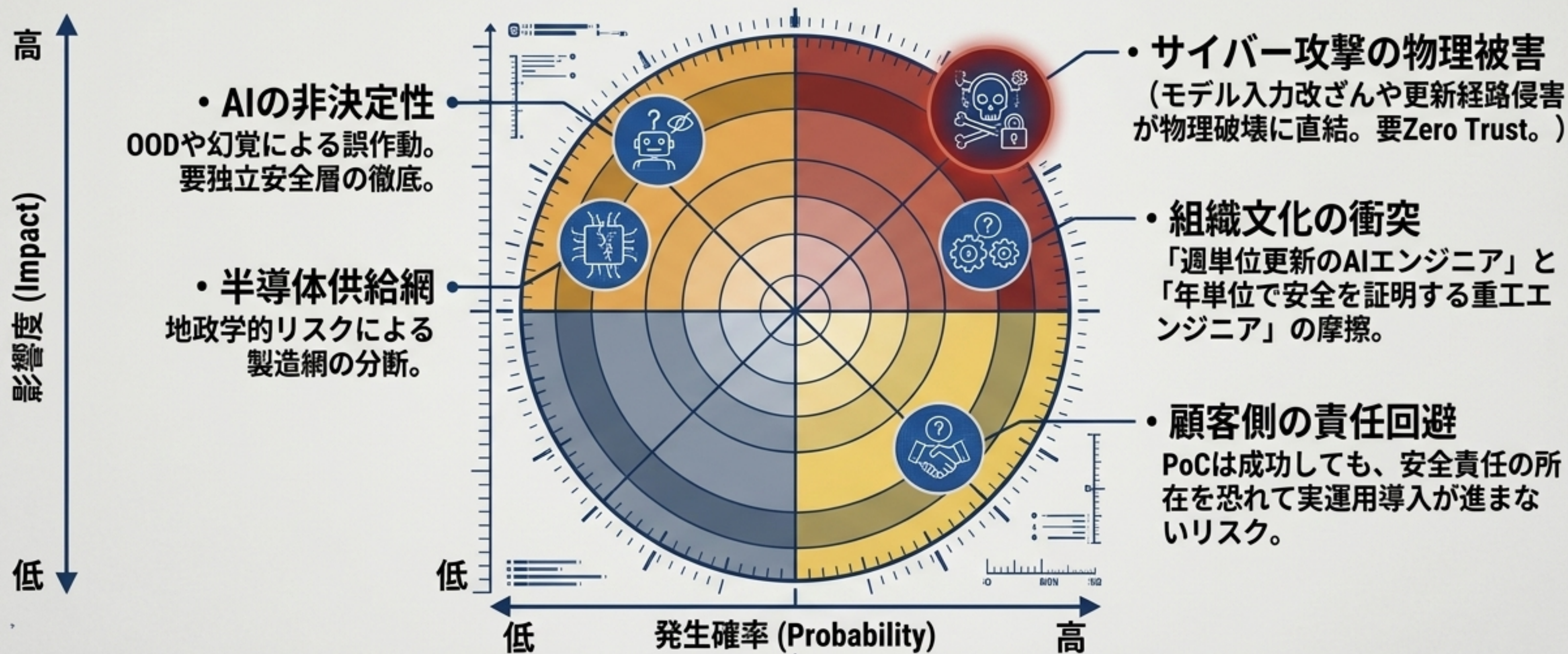
【労働力の変容】

雇用は奪われるのではなく「シフト」する。
単純監視業務は減るが、AI・制御工学・安全解析を横断する「高度職（AI＋機械＋安全）」の需要が爆発する。



リスク・レーダー：プロジェクトを頓挫させる潜在的脅威

技術的な概念実証の成功確率が高い。しかし、量産化とプラットフォーム化を阻むのはAIの精度そのものよりも、サイバーセキュリティ、認証遅延、そして組織文化の衝突である。



戦略提言：MHIとPFNが直視すべき「次の打ち手」

100億円の資本提携を具体的な産業価値に変換するためには、リソースの分散を避け、地味だが確実な「安全検証プロセス」の強化に投資を集中させる必要がある。

【MHIへの提言 (The Integrator)】

- ✓ 「全製品のAI化」を焦らず、2〜3件の**確実な灯台案件**（予知保全等）にリソースを集中せよ。
- ✓ 製品ごとにAI基盤を乱立させず、共通エッジAIランタイム、**安全監視インターフェース**、証拠ログなどの「**全社共通資産**」を構築せよ。

【PFNへの提言 (The AI Provider)】

- ✓ 資金を「**モデル巨大化・パラメータ競争**」だけに溶かしてはならない。
- ✓ ミッションクリティカル市場の勝負所である、**確定的レイテンシ**の保証、長期供給体制、認証資料自動生成といった「**Safety/Assurance Engineering**」へ投資せよ。

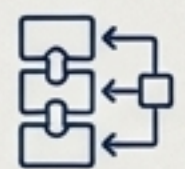
産業エコシステムへの提言と結論：実装競争は今、始まった

日本のソブリンAI政策の真の勝機は、基礎的なLLM開発競争に追従することではなく、「AIを物理空間に安全に組み込む枠組み」を世界に先駆けて構築することにある。

【政府・産業界への提言】



- 補助金でモデル競争をするのではなく、HIL/シミュレーション試験環境や安全ケース基準といった「検証・保証基盤」を公共財として整備せよ。



- PFN/MHIを閉じた垂直統合にせず、センサー、サイバーセキュリティ、RTOS企業が参加できるモジュール性の高いインターフェースを作れ。

『勝負の分かれ目は「国産LLMを作れるか」ではない。
「AIを、停止できない物理システムに、**認証可能な形で組み込めるか**」である。
100億円の出資は完成ではなく、**日本発・ミッションクリティカルAI真実尋、
日本発・ミッションクリティカルAI実装競争の号砲に過ぎない。**』