

CHINA AI 2026: 中国AIフルスタック 競争の現実と日本企業への戦略提言

WAIC 2026 調査報告書 (GPT-5.6 Sol)

対象会期: 2026年7月17日ー20日

調査基準日: 2026年7月19日

対象読者: 取締役会・経営会議メンバー / CIO / CDO

WAIC 2026最大のシグナル：「代替フルスタック」の完成

過去

チャットとモデル規模の競争



現在

実行と完遂のフルスタック競争



出展1,100社超

(最低値比37.5%増)

世界初公開300件超

(同3倍以上)

展示面積10万m²超

(ハードウェアと工程統合の拡大)

日本企業にとって、無視するリスクは高い一方、無条件に依存するリスクも同じく高い。

取締役会・経営会議で直ちに決断すべき5つの事項

01. 責任体制

推奨:
90日限定の横断
タスクフォース設置
(事業・IT・法務)



放置リスク:
技術評価と契約・
安全判断の分断

02. モデル方針

推奨:
マルチモデル方式
への移行
(用途ごとの切替)



放置リスク:
単一ベンダーへの
ロックイン・
供給遮断

03. データ境界

推奨:
機密度3段階と
越境・学習利用
ルールの定義



放置リスク:
営業秘密・
規制データの流出

04. 実証投資

推奨:
公開/合成データに
限る隔離PoCを
100日以内に実施



放置リスク:
機会損失、または
現場での
無秩序な導入

05. フィジカルAI

推奨:
デモ性能ではなく
「稼働率・安全・
TCO」を量産ゲートに



放置リスク:
見栄えの良い
実証デモが
量産投資に化ける

会場が示した「6層の競争」構造



国際ルール (WAICO等)

競争の本質：誰の価値観・規格が新興国で使われるか

市場・シナリオ (57シナリオ)

競争の本質：実需要とデータの循環

アプリ / エージェント (DuMate等)

競争の本質：会話ではなく業務完遂と権限監査

フィジカルAI (EVライン等)

競争の本質：安全・稼働率・工程統合

基盤モデル (Kimi K3等)

競争の本質：性能・価格・オープン性

算力・インフラ (Atlas 950)

競争の本質：相互接続・統一メモリ・供給耐性

[Layer 2 & 4] 基盤モデルとエージェント：Kimi K3の現在地

展示シグナル（モデルの実力）



圧倒的な規模

2.8兆パラメータ
100万トークン文脈入力



ベンチマーク上位

独立評価 Vals 総合2位
WebDev Arena 暫定1位



破壊的価格

出力15ドル/1Mトークン
(最高位群に比べ圧倒的競争力)

既知の制約と現実の壁



「条件付き」のオープン

API提供が中心。重み、学習データ由来、
商用制限は未検証



幻覚率の悪化

K2.6の39%からK3で51%へ悪化したとの
第三者評価 (Artificial Analysis)



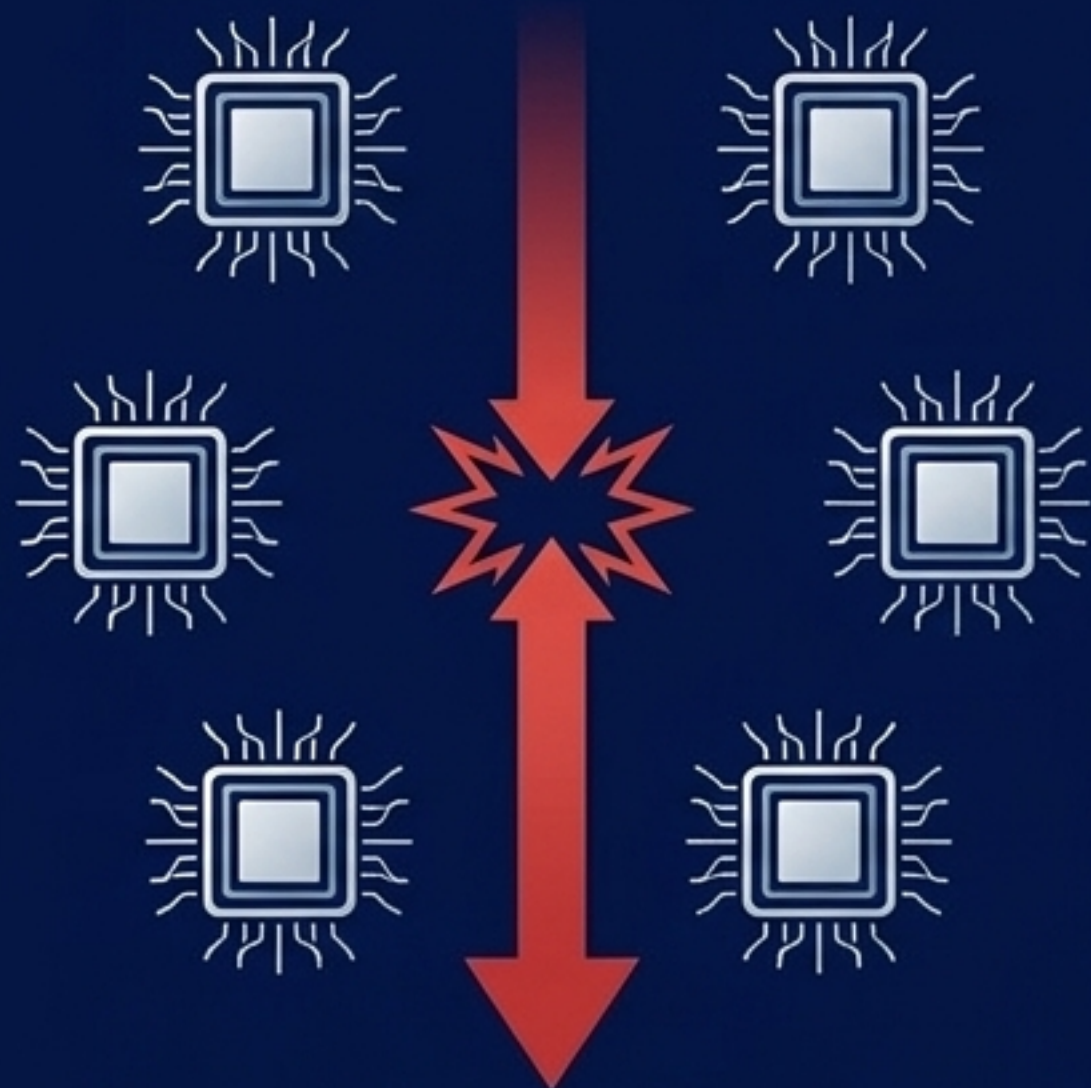
自律エージェントの壁

最上位米国モデルとのUX差。
過剰な自律判断の危険性

結論: 安価な二番手と侮るべきではないが、機密データの投入や完全オープン化の過信は禁物。

[Layer 1] 国産計算基盤：チップ単体から「超ノード」への移行

旧来の単一チップ競争



単一チップの演算性能
(FLOPS)への依存
(半導体規制によるボトルネック)

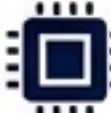
現在のシステムレベル競争 - 超ノード



統一メモリアドレス空間

ハードウェア単体の不足を、
相互接続とソフトウェア層で補う

Huawei Atlas 950 SuperPoDの主張

 1,024基のAscendプロセッサを単一システム化

 FP8で1 EFLOPS
の演算力

 256TBの
統一メモリアドレス空間

 CANN(1,244万行超)
によるソフトウェア生態系

 ※多くは企業発表値であり
独立検証が必要

[Layer 3] フィジカルAI：ショー（展示）から工程（量産）へのギャップ

ユースケース	展示シグナル (What they show)	量産前の必須KPI (What we need)
Case 1: EV部品の自律操作	視覚・触覚を備えたロボットが、未定義の部品を把持・ねじ締め	サイクルタイム、部品ばらつき耐性、停止からの自動復帰
Case 2: スマート薬局の統合	異メーカー3機を同一具身モデルで同時制御し、ランダム受注を処理	誤在庫率、薬機法・個人情報監査、新規機種追加の工数
Case 3: ロボット間協働作業	6機が15時間にわたり、タスクを自律的に配分して協働組立	人間の介入回数、MTBF（平均故障間隔）、タスク再計画時間



警告: 24時間操業はデモとは異なる。

「見栄えの良い実証」ではなく、TCOと安全証明を量産ゲートにせよ。

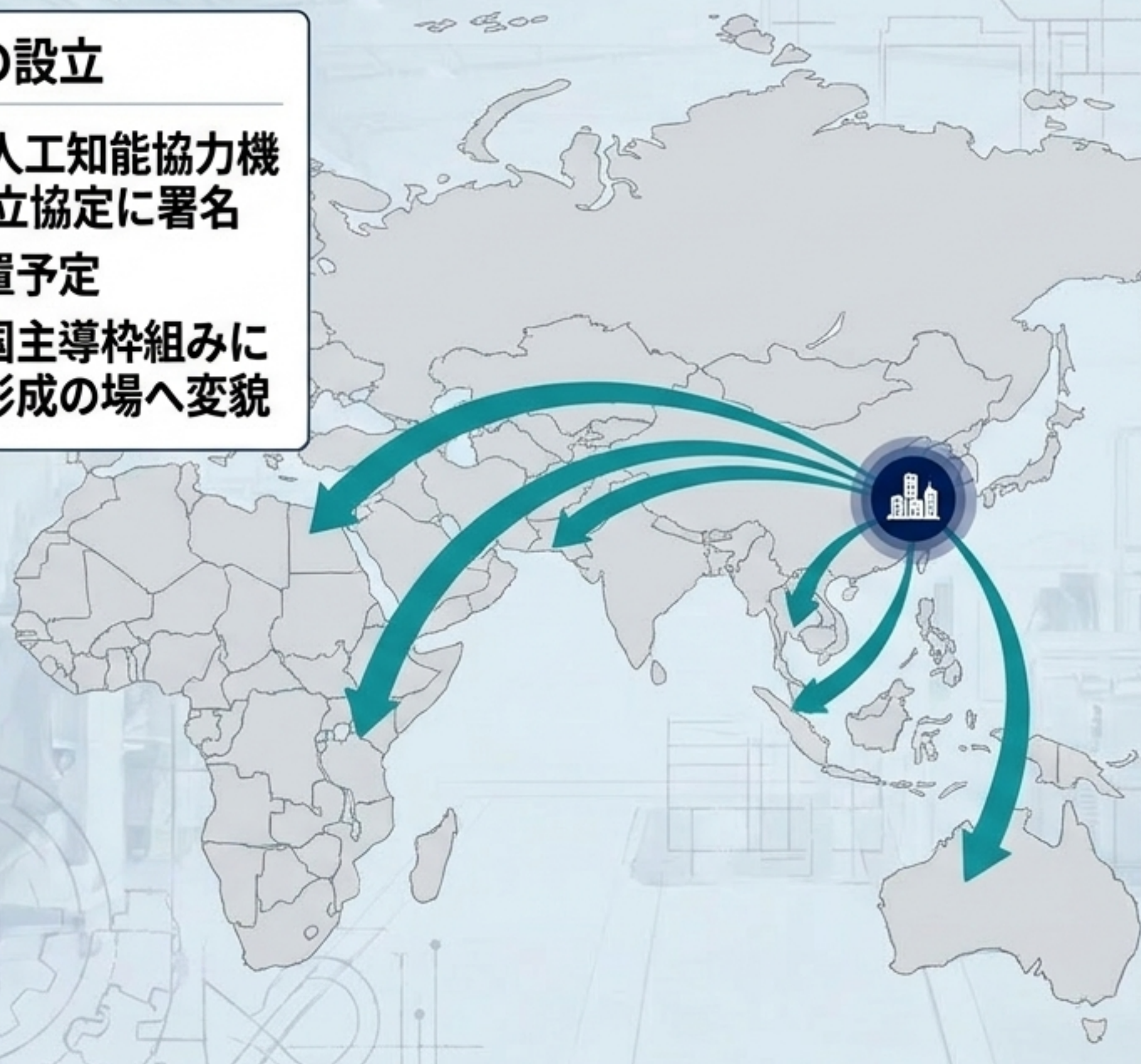
[Layer 6] 国際ルール形成：技術会議から地政学の間（WAICO）へ

WAICOの設立

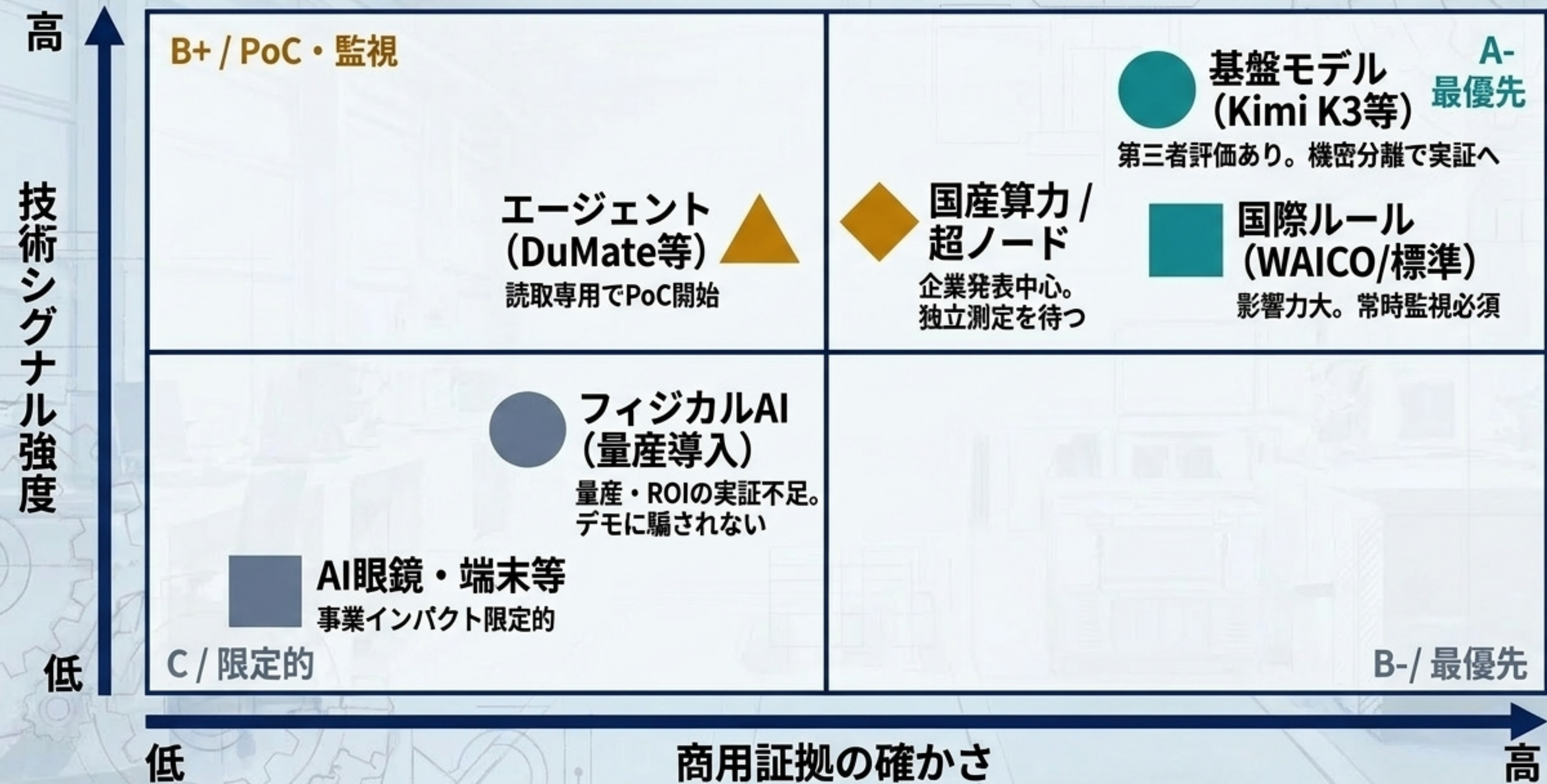
- 29か国が「世界人工知能協力機構 (WAICO)」設立協定に署名
- 本部：上海に設置予定
- 技術会議が、米国主導枠組みに対抗するルール形成の間へ変貌

⚠ 日本企業への影響

- 調達要件の書き換え：
新興国市場での標準規格
や監査要件が中国主導に
なるリスク
- システム分断：
グローバルサプライチェーン
におけるAI標準の二重化
- アクション：
ISO/IECとWAICOの差分
を常時監視し、製品設計へ
反映せよ



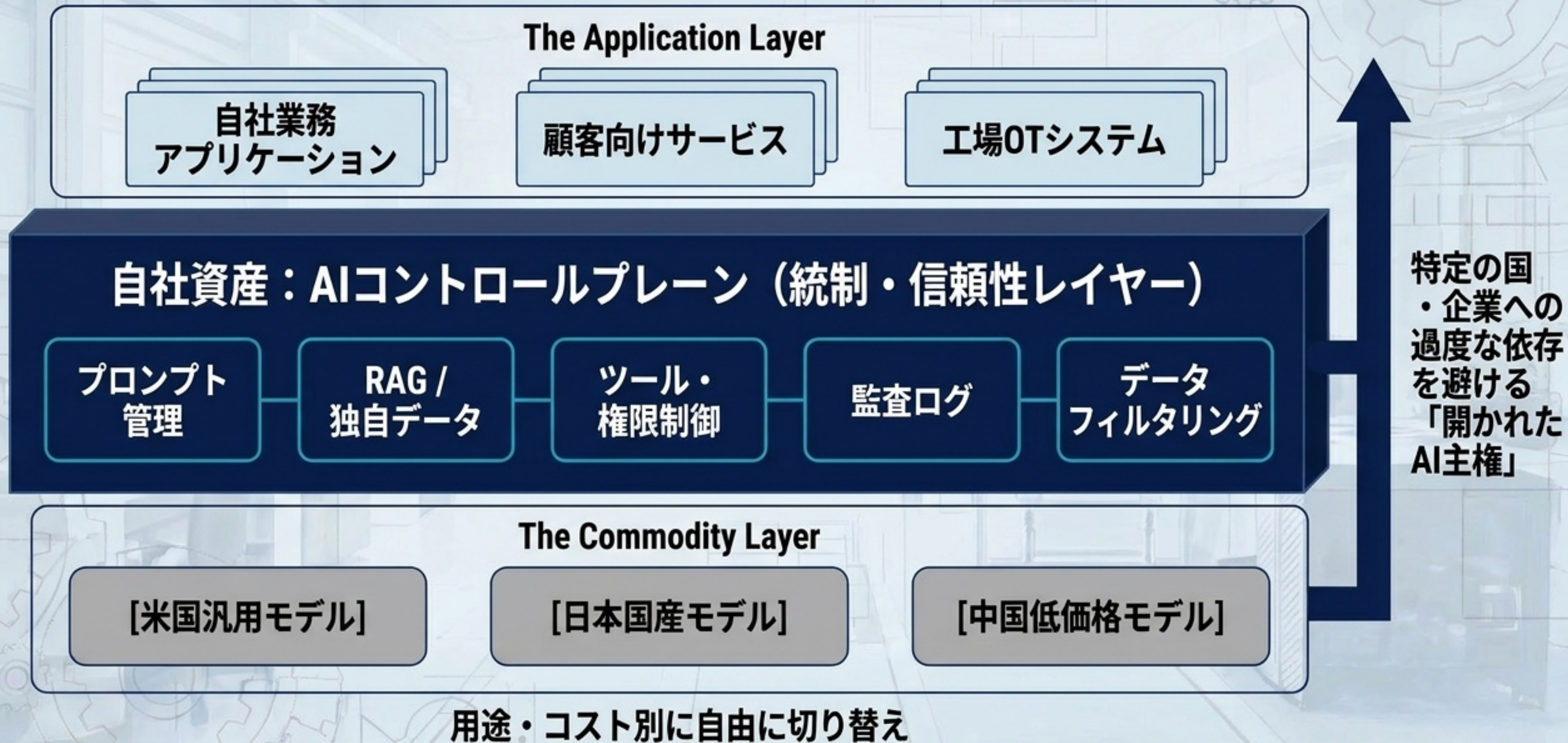
技術成熟度・事業化レディネスマトリクス



産業別インパクトと脅威アセスメント

対象産業	機会（機会領域）	脅威（想定リスク）	優先対応策（アクション）
製造・自動車	視覚/触覚の統合、工程エージェント、予兆保全	中国製ソフト/ロボットによる現場データの囲い込み	OT安全の確保、共通API化、現場データ権利の死守
機械・ロボット	日本の精密機械、安全保証、保守網の優位性発揮	汎用ヒューマノイドによるハードウェアのコモディティ化	モデル非依存の「信頼性レイヤー」の製品化とパッケージ化
ソフトウェア・BPO	低価格モデルを活用した業務の徹底的な自動化	コーディング/事務エージェントによる工数売上の圧縮	成果課金への移行、エージェント統制製品の開発
金融・保険	高度な検索、審査補助、不正検知の効率化	越境データ問題、説明責任、エージェントの誤取引	読取専用の徹底、二重承認ルール、全ログの監査

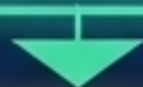
日本企業の勝ち筋：「AIコントロールプレーン（統制層）」の構築



ガバナンス実装：データ境界と最小権限制御

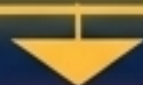
Green（公開データ / 合成データ）

- 条件: 外部API利用可。
- 必須アクション: ログ保存期間、学習利用条件（オプトアウト）の事前確認。



Amber（社内限定 / 低機密）

- 条件: 原則は企業テナントまたは私有環境。
- 必須アクション: 学習利用の完全禁止。データの最小化とマスキング。出力の人間によるレビュー。



Red（営業秘密 / 個人情報 / 規制データ）

- 条件: 外部APIへの送信を一切禁止。
- 必須アクション: 承認済みの国内閉域網、または完全隔離環境でのみ処理。法務・輸出管理の個別判定。

エージェント制御の絶対原則: 既定は「読取専用（Read-only）」。書込・データ送信・本番環境の変更・OT（設備）制御を実行する場合は、必ず「人の都度承認（Human-in-the-loop）」を必須とする。

ネットワーク実行指針：「ローカル最適化＋グローバル分離」

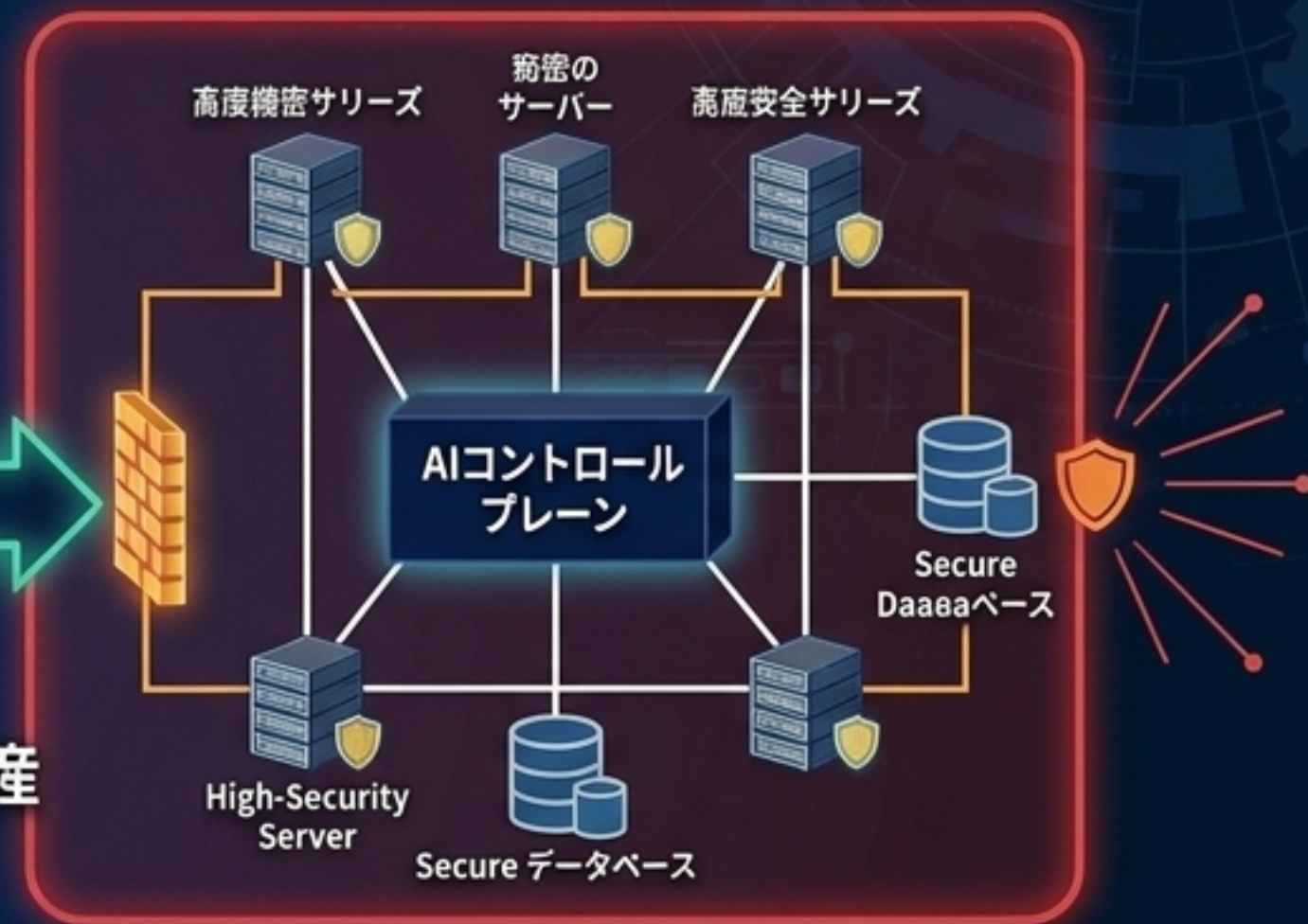
中国子会社網 - ローカル最適化



本社へ戻すデータは
「集計・匿名化」のみに限定

設計情報やグローバル学習資産
との混在を物理的に防ぐ

グローバル中核網 - 日本本社



- 中国モデルをローカルで運用。現地の言語・規制・プラットフォーム要件に適合。
- 顧客データ、改善データ、管理者権限はこの区画内に完全保持。

- 高度機密データ（営業秘密、未公開特許、グローバル顧客情報）を隔離管理。
- 日米の信頼できるモデルを利用した統制基盤。

経営陣が推進する「100日アクションプラン」



経営ダッシュボードとモニタリングKPI



売上寄与額、処理時間削減、再作業率



ポリシー違反数、越権行為、セキュリティインシデント



最大ベンダー依存比率、特定国モデルへの依存率



FTO（侵害予防調査）完了率、確保したデータ権利数



国際委員会参加数、調達要件への反映件数



MTBF（平均故障間隔）、稼働率、人間の介入率

「過小評価しない。過信しない。比較評価する。機密を分離する。
切替可能にする。現場KPIで量産を決める。標準形成へ入る。」