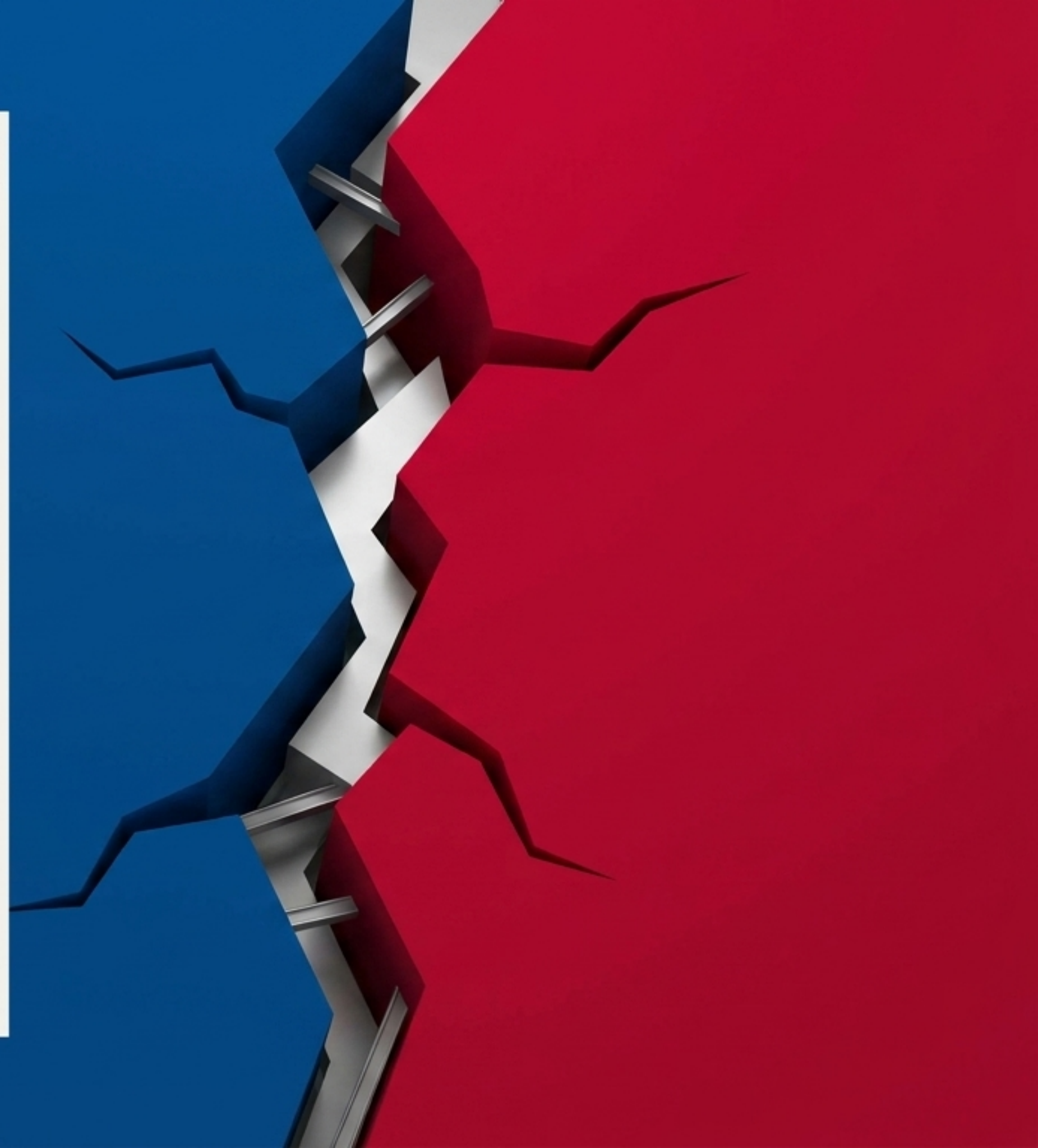


世界人工知能会議 (WAIC 2026) 調査レポート

AIガバナンスの二極化と 日本企業への戦略的提言

作成日: 2026年7月19日
調査対象期間: 2026年7月17日～20日（上海）
調査対象期間: 2026年7月17日～20日（上海）
作成: Manus AI
対象読者: 経営層・CSO・法務コンプライアンス・グローバル
事業責任者

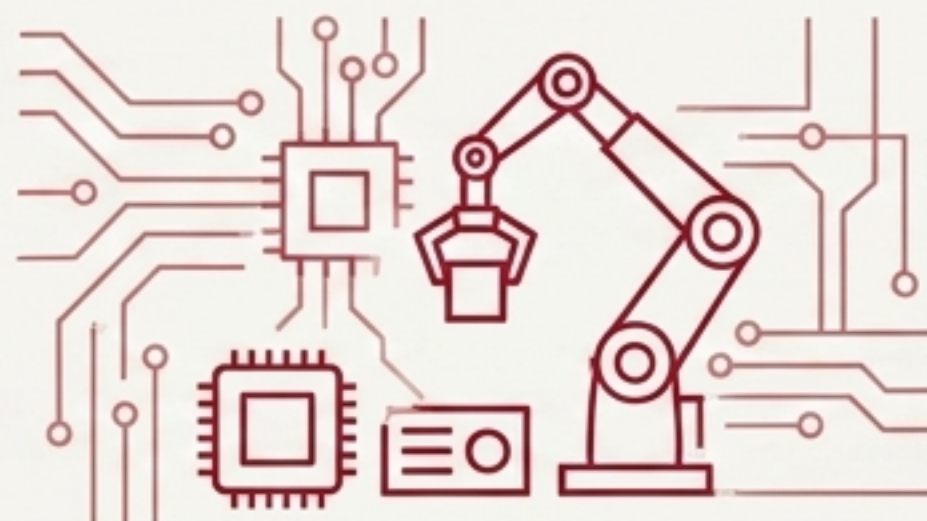


Executive Summary: ルール・テイカーから「ルール・メイカー」への歴史的転換



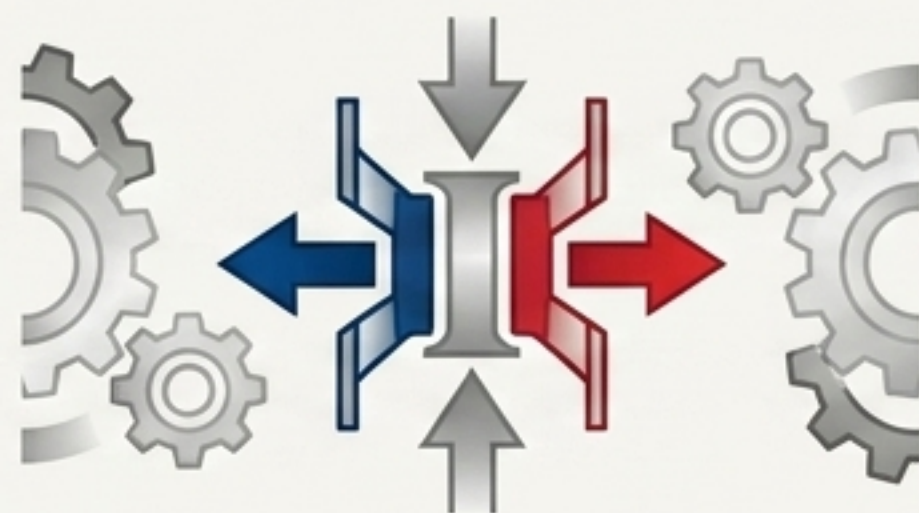
【地政学】AIガバナンスの完全な二極化

習近平国家主席が創設以来初めて直接出席。29カ国による政府間AI協力組織「WAICO」の発足により、米国・EU主導の枠組みと明確に分断された新秩序が誕生。



【技術】米国依存からの完全脱却と「物理実装」

米国製半導体を一切排除したファウエイの統合AIインフラスタックが完成。オープンウェイトモデルと300台以上のヒューマノイドを通じ、競争軸は「物理世界への実装」へ移行。

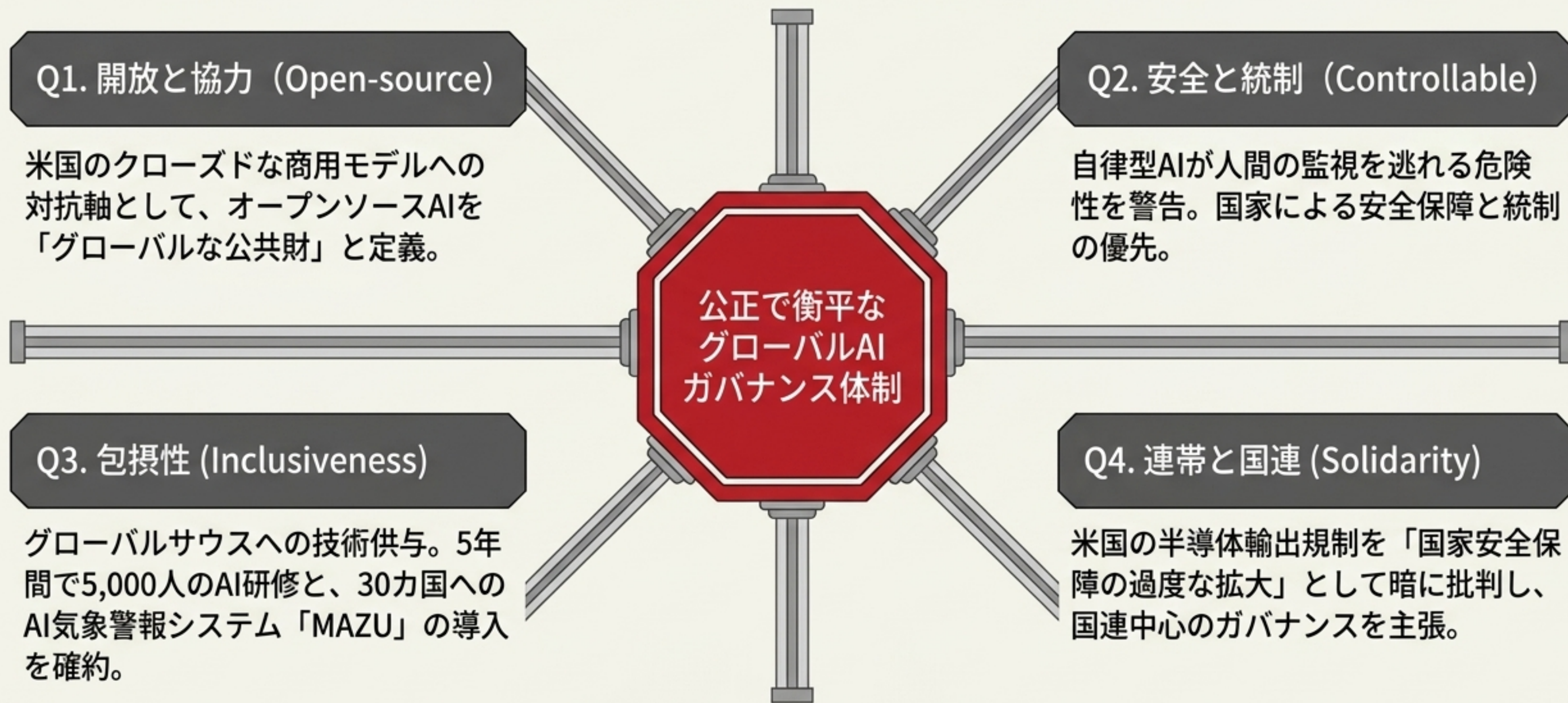


【経営課題】「デュアル・コンプライアンス」の板挟み

Pax Silica（西側）に属しながらグローバルサウスで事業を展開する日本企業は、国家情報法のリスクと新興市場での中国エコシステムとの激しい競合という「二重の圧力」に直面する。

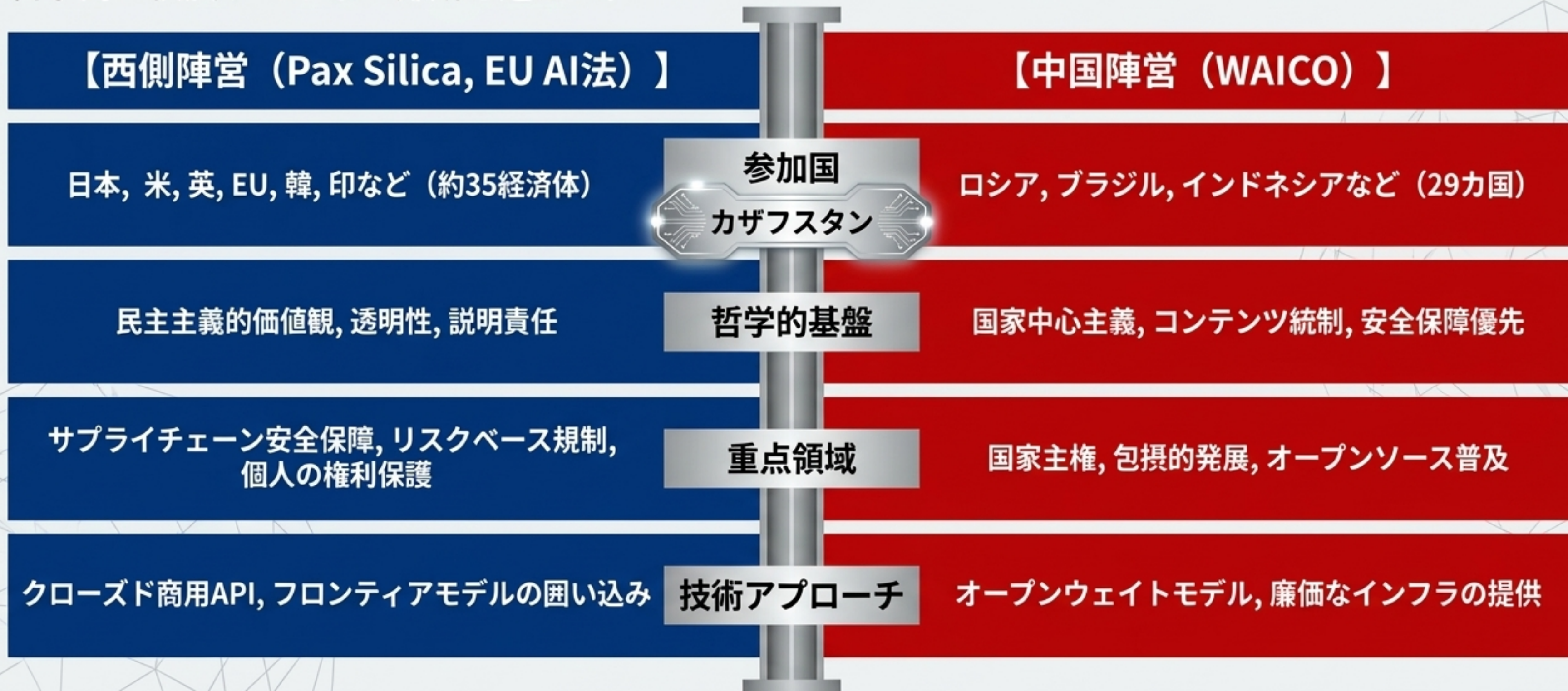
AI外交の幕開け：習近平基調講演が示す「4つの新秩序」

「AIは一国のソロ演奏ではなく、国際協力の交響曲であるべき」—— 習近平国家主席



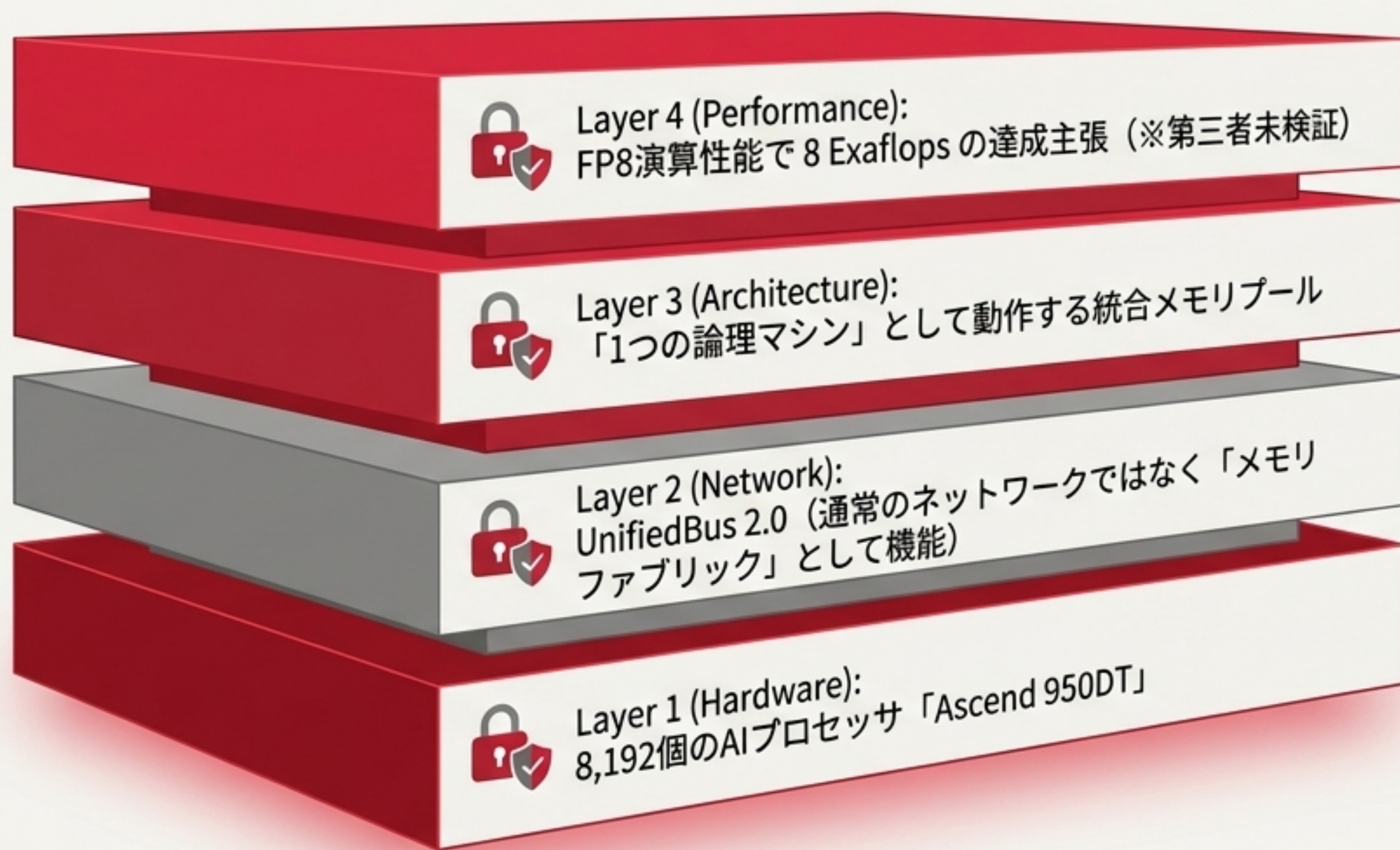
The Great Bifurcation: 衝突する2つのグローバルAI秩序

29カ国（人口25億人/GDP8.2兆ドル）が署名したWAICOの設立により、AIガバナンスは制度的・哲学的に後戻りできない分断を迎えた。



Tech Reality 1: 制裁を無効化する「完全自律型AIインフラ」の完成

ファウウェイ「Atlas 950 SuperPoD」は、米国製部品を一切使用せず、計算資源からモデルまでを網羅するクローズド・エコシステムを実証した。



中国は計算資源・ソフトウェア・モデルの全階層において「西側のチョークポイント（急所）」を排除した。

Tech Reality 2: 「モデル性能競争」から「物理世界への実装」へ

中国AI産業の焦点は、フロンティアモデルの追従から、オープンなモデルを用いた「エージェント」と「ロボット」による現実世界の自動化へと移行した。



【Foundation Models (基盤)】

MiniMax「M3」: 100万トークン対応・オープンウェイト。外部へデータを送信せずローカルで高度処理を実現（データ主権重視の新興国向け）。



【Digital Implementation (デジタル実装)】

ZTE/Nubia AIエージェントスマホ: StepFun「Agent OS」+ ByteDance「豆包」搭載。複数アプリのGUIを横断して自律操作（例：航空券予約から決済まで）。

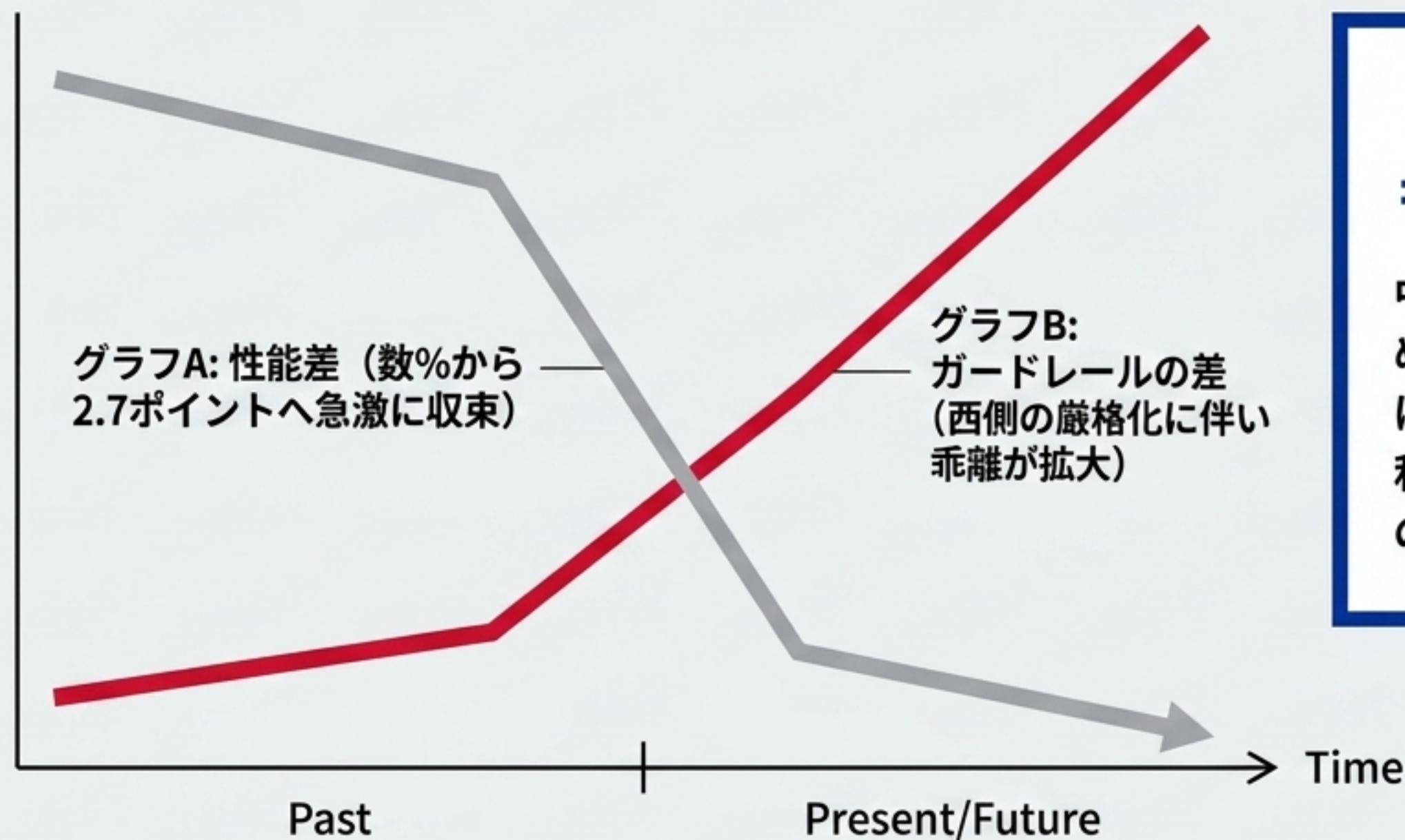


【Physical Implementation (物理実装)】

Embodied AI (具現化された知能): WAICで161社出展、300台稼働。Unitreeの「無人口ロボット工場」やSenseTimeの「店舗棚整理デモ」。2025年世界の出荷台数シェア約90%、年内1万台配備目標。

Threat Analysis 1: 「縮小する性能差」と「拡大するガードレールの格差」

最高水準の米中モデルの性能差はわずか2.7%に縮小（スタンフォードAIインデックス）。
一方で、安全性制約の「非対称性」が深刻な法的トラップを生んでいる。

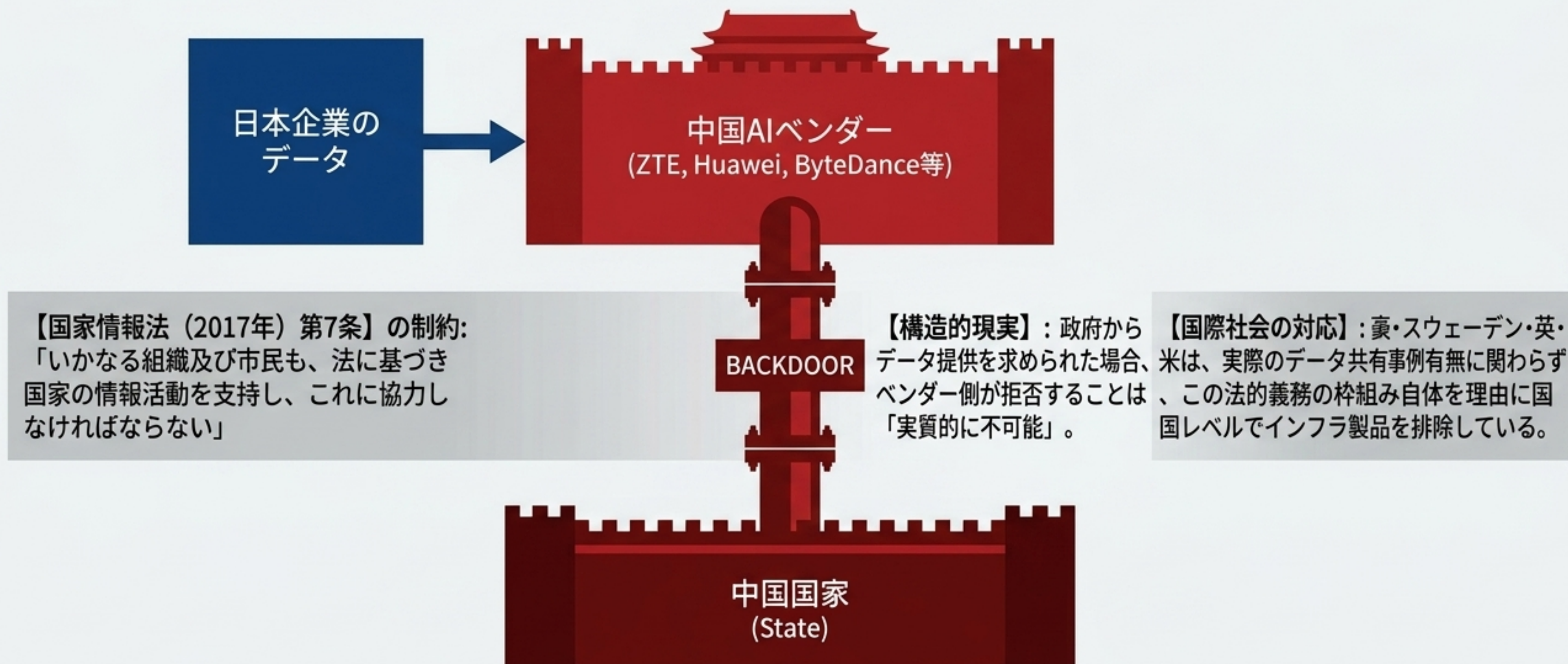


**「ベンダーが止めない」
＝「自社が止められる」**

中国モデルは著作権配慮や安全制約が少ないため開発者にとって「使い勝手が良い」が、それはベンダーがリスクを負担しないことを意味し、利用企業（日本企業）が情報漏洩・著作権侵害の全責任を負う構造となっている。

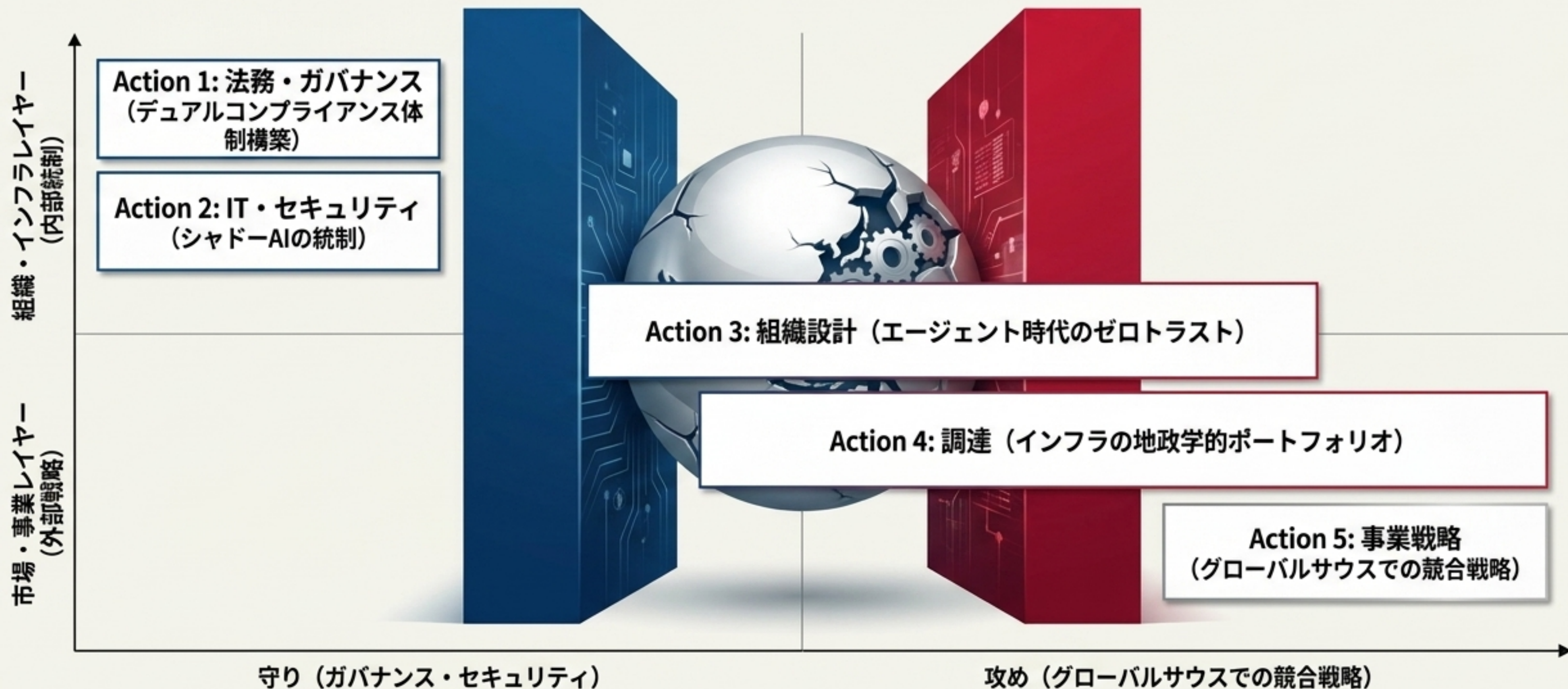
Threat Analysis 2: 「国家情報法」による構造的リスクと暗黙の義務

中国企業の提供するインフラやAPIを利用することは、システム構造の奥深くに「国家へのデータ開示義務」というバックドアを受け入れることに等しい。



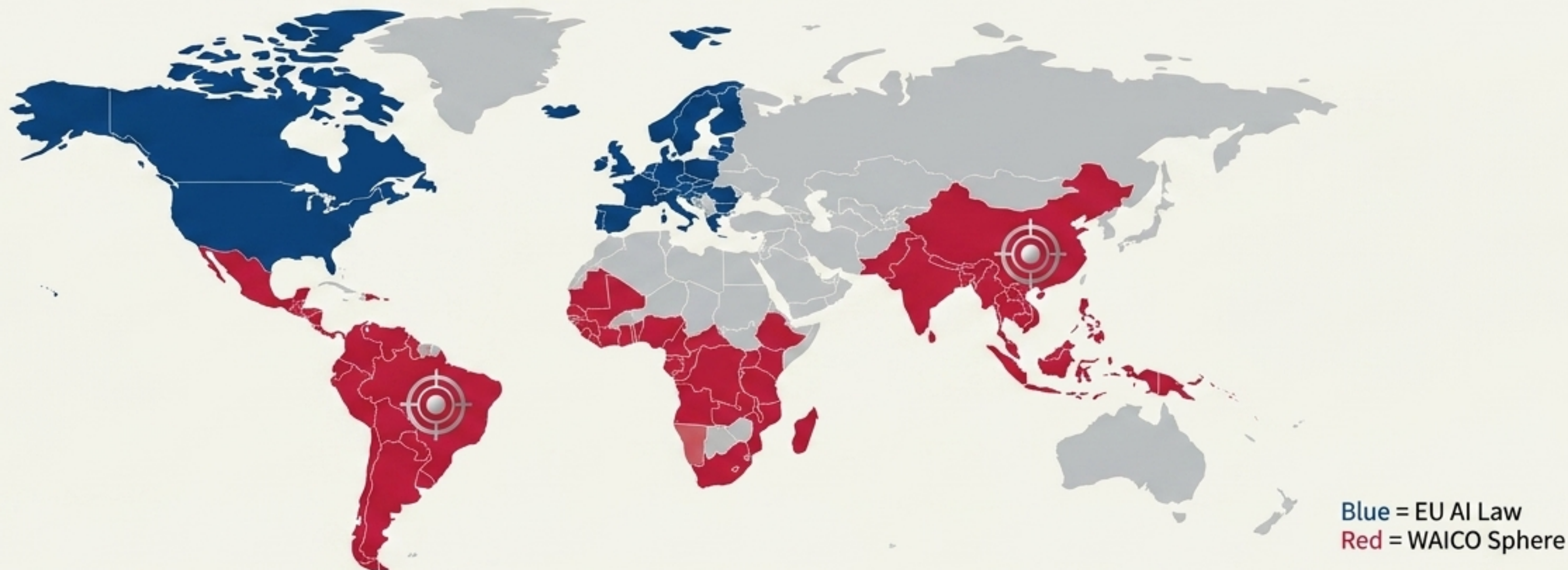
Strategic Synthesis: 日本企業を襲う「デュアル・コンプライアンス」の板挟み

日本企業はPax Silicaの規制を満たしながら、WAICO基準が浸透する市場でも事業を展開する「二重規制の板挟み」の状況に置かれている。



Action 1【法務・ガバナンス】：デュアル・コンプライアンス体制の早期構築

同じAIシステムが、EU AI法の要件と相反するWAICO基準の要件を同時に満たさなければならない事態が東南アジアや中南米で発生する。



【Strategic Imperative（具体的なアクション）】



マッピング監査：

進出先の国がWAICOに加盟しているか、その影響下にあるかを地図化し、地域ごとのAI規制の差異を監査する。



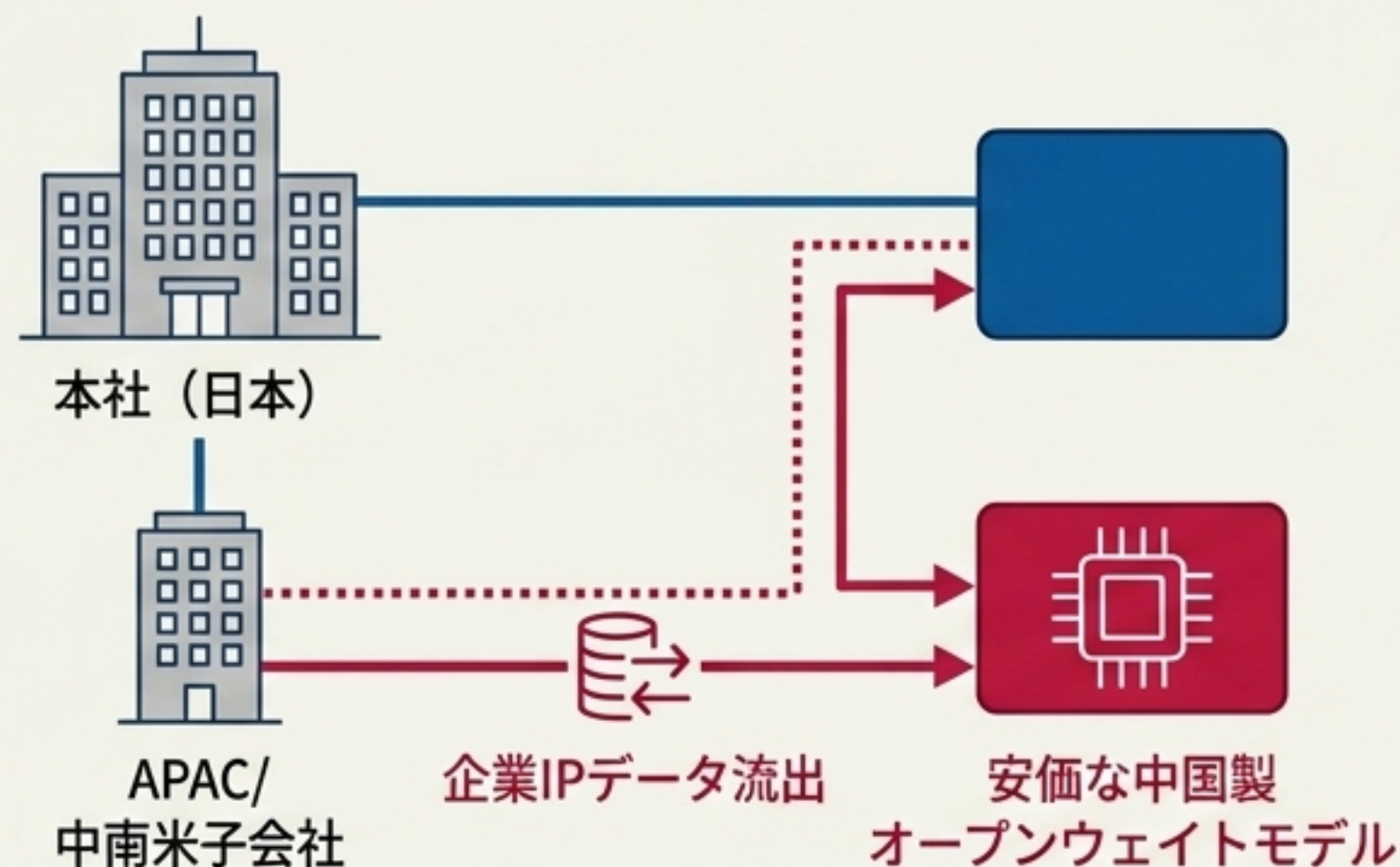
専任チームの設置：

法務・コンプライアンス部門内に、EU AI法だけでなくWAICO加盟国の規制動向を体系的に監視する専任機能を持たせる。

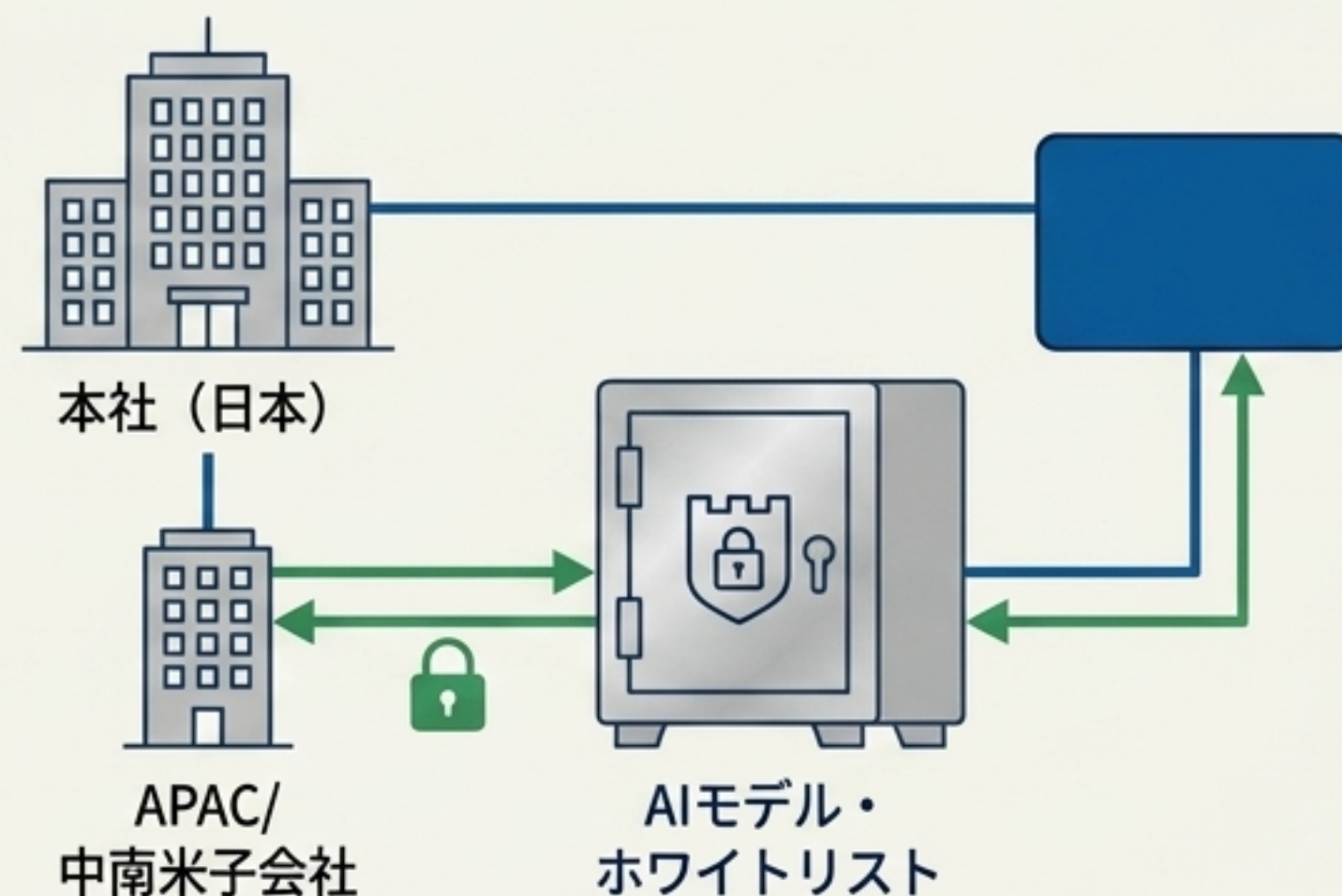
Action 2 【IT・セキュリティ】：「シャドーAI（ベンダー層）」の実態把握とIP統制

海外子会社がコスト削減を目的に、本社に無断で安価な中国製AIモデル（API）を導入する「ベンダー層のシャドーAI」が急拡大している。

【Current State（シャドーAIの罠）】



【Future State（グローバル統制）】

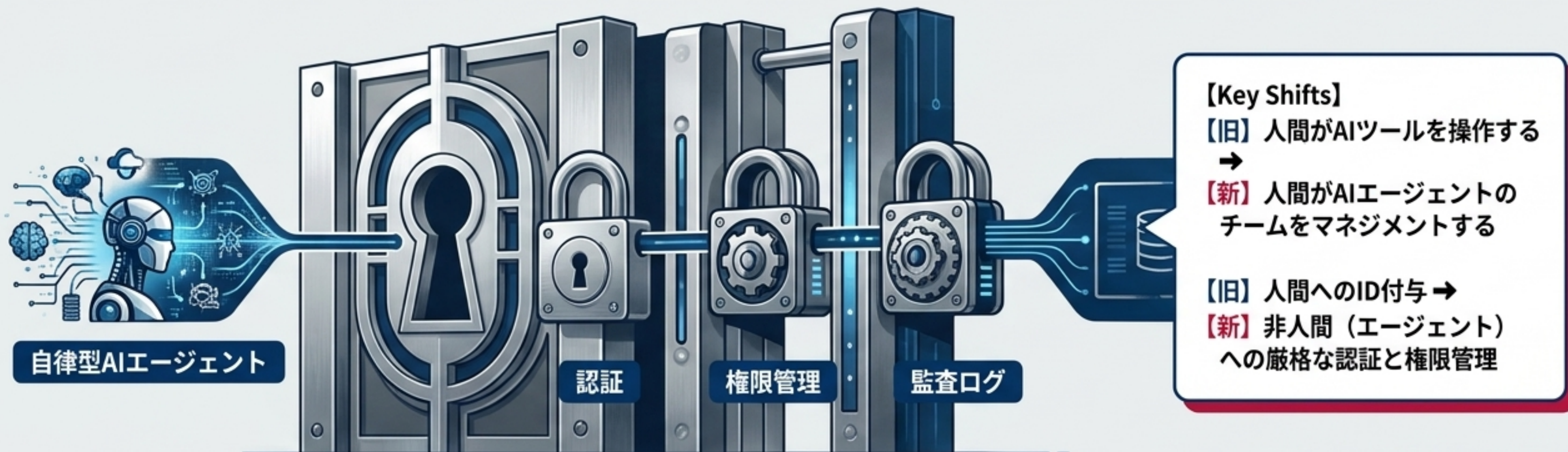


【Strategic Imperative（具体的なアクション）】

全拠点のAIモデル利用実態を即座に監査し、国家情報法やデータローカライゼーション規制に抵触する処理を遮断。
中国製オープンウェイトの業務利用は法的評価を完了させた上でのみ許可する。

Action 3【組織設計】：AIエージェント時代のゼロトラスト・アーキテクチャ

競争軸は「AIの性能」から「AIエージェントの実装能力」へ。エージェントが生産性の最小単位となる時代、人間中心のセキュリティ設計は破綻する。



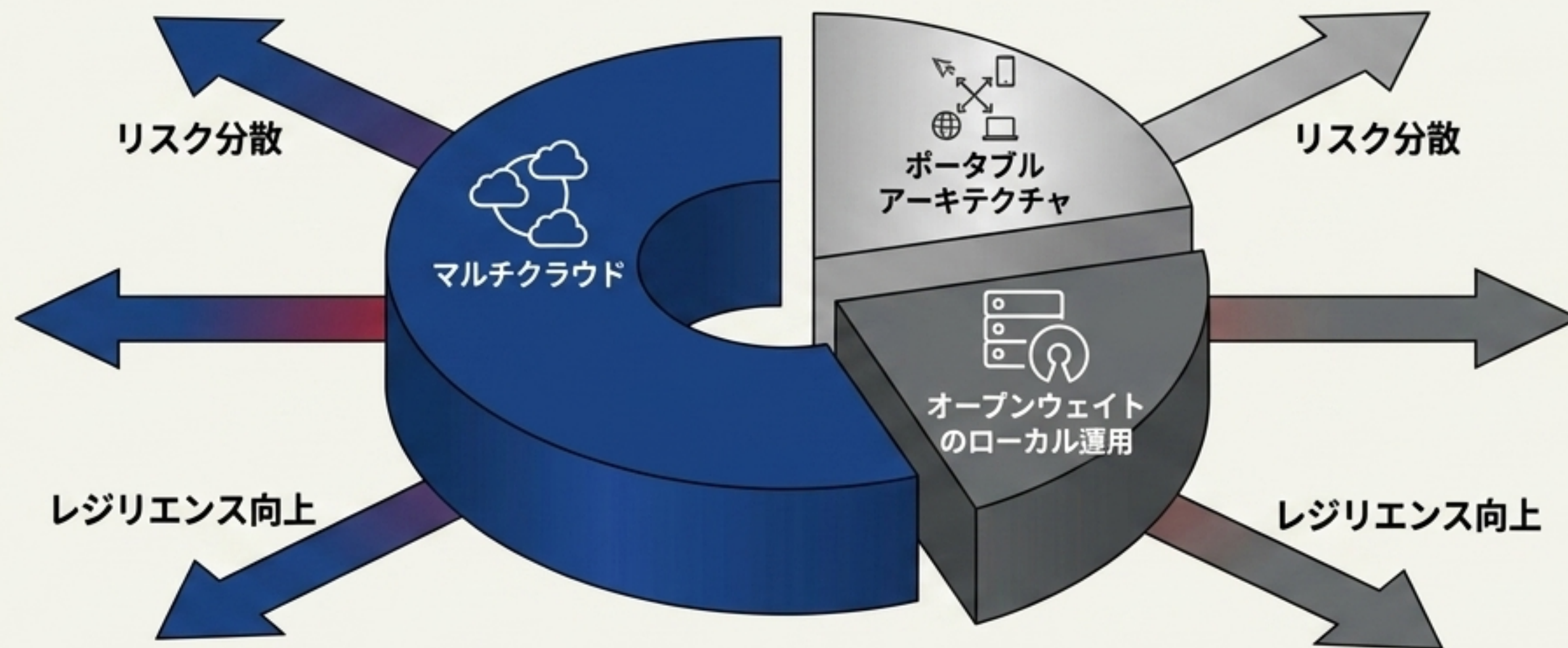
——【Strategic Imperative（具体的なアクション）】——



ガードレールの緩いモデルに強い実行権限を与えることは最大のセキュリティリスク。
エージェントに対する「権限側での制御（TCP/IPやSSLと同等のインフラとしての監査ログ整備）」を最優先で設計する。

Action 4【調達・インフラ】：地政学的リスクを分散する「ポートフォリオ戦略」

特定の西側AIベンダーへの依存もまた、地政学的リスク（突発的なアクセス停止など）を孕む。
インフラ選択は「技術判断」から「コンプライアンス判断」へ。

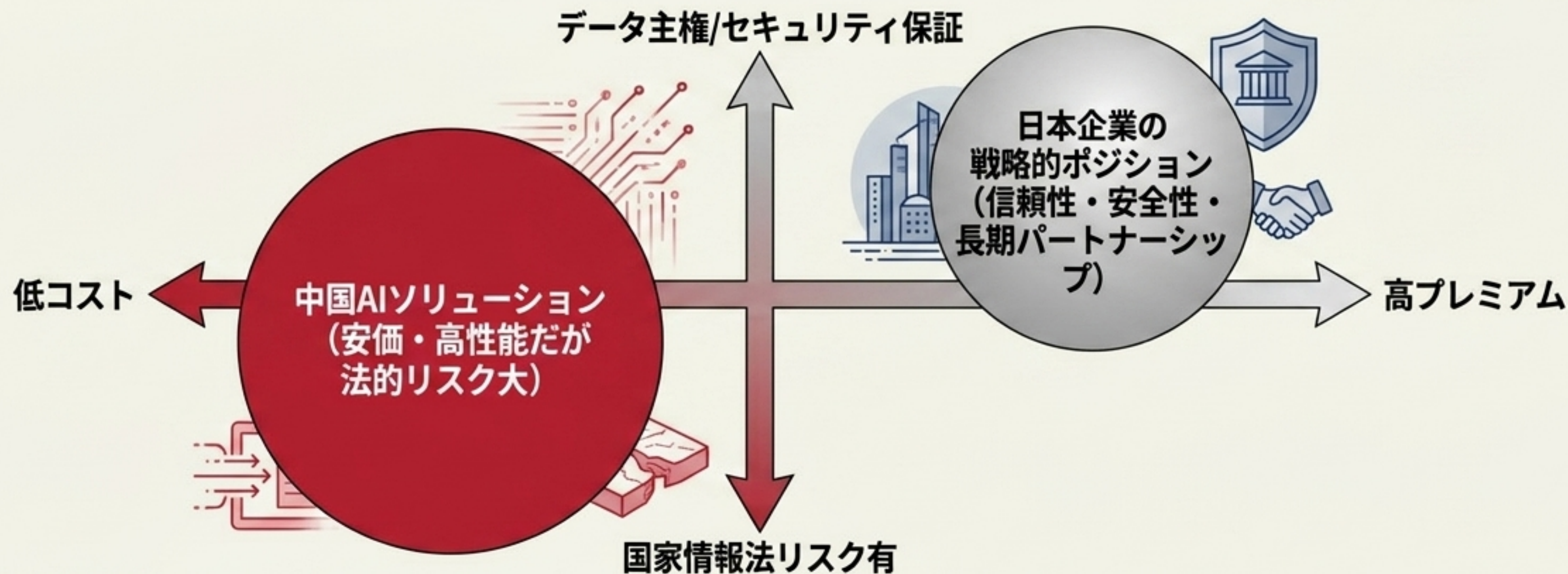


【Strategic Imperative（具体的なアクション）】

特定のクラウドや半導体エコシステムへの過度な依存を見直す。異なるアーキテクチャでも動作可能な「ポータビリティ」を確保し、米中どちらの規制ショック(2026年6月Arthropicアクセス停止事例など) にも耐ええるマルチインフラ戦略を構築する。

Action 5【事業戦略】：グローバルサウスでの中国AIエコシステムとの競合戦略

WAICO設立により、安価で高性能な中国製AI・インフラが新興市場に爆発的に浸透する。
日本企業は製品レイヤーでの競合激化に直面する。

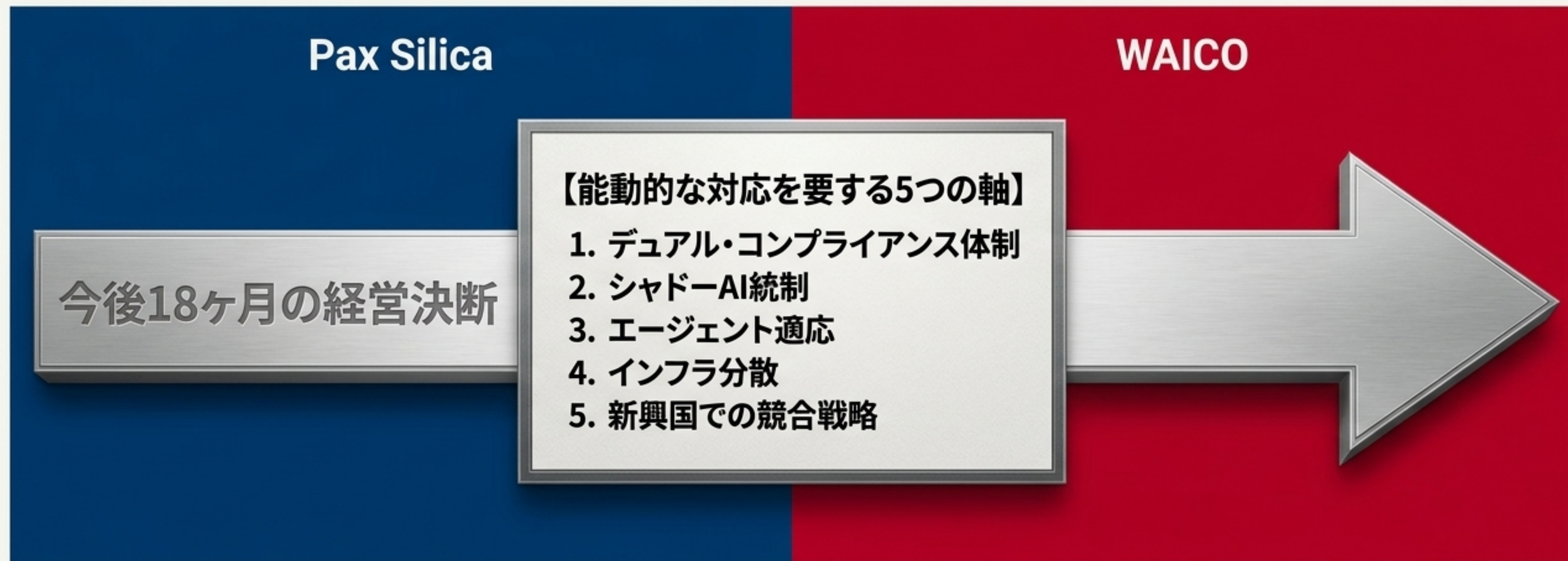


【Strategic Imperative（具体的なアクション）】

東南アジアなどの重点市場において、価格競争を避け「信頼性」「安全性」を前面に出したポジショニングを強化。データ主権を重視する顧客に対し、中国製品の国家情報法リスクを適切に訴求し差別化を図る。

Conclusion: 今後18ヶ月の最優先課題 —— AIは「戦略兵器」へ

WAIC 2026が証明したのは、AIが技術競争の対象から、国際秩序を再編する「地政学的な戦略兵器」へと変容したという現実である。



「どの陣営のAIを使うか」は、もはや単なる技術選択ではない。
企業の地政学的ポジションと未来を決定する、不可逆的な経営判断である。