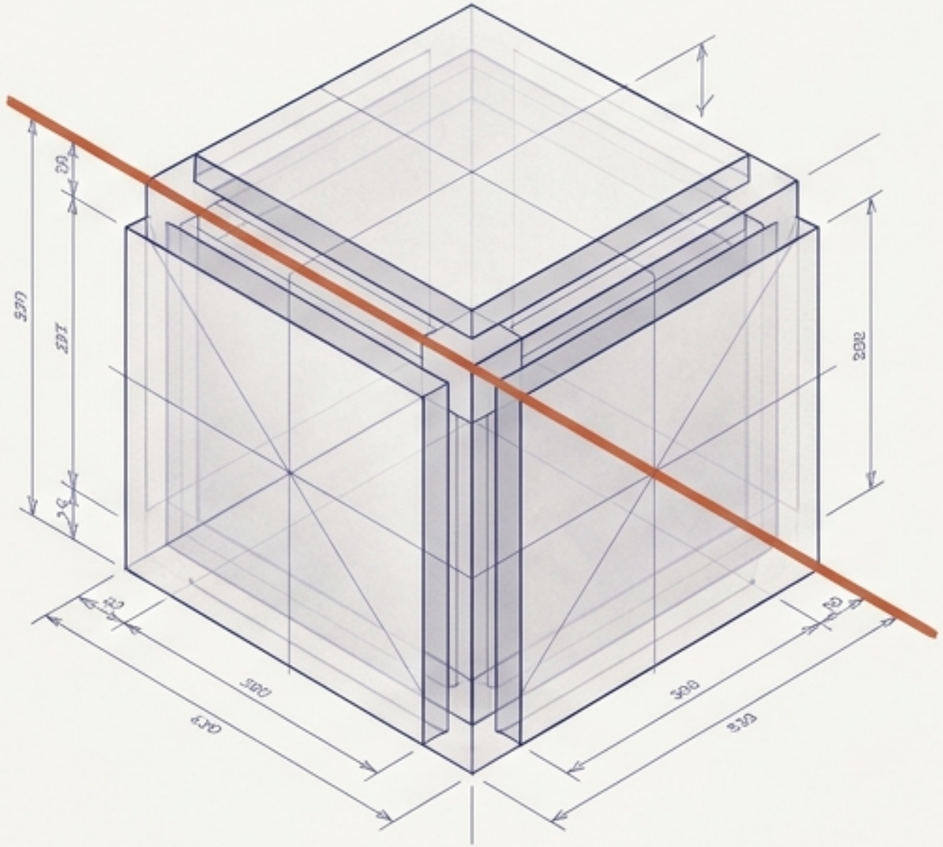
Target:	Enterprise IT & Strategy
Status:	Due Diligence Briefing
Date:	As of May 3, 2026

Intelligence Dossier: Manus AI

エージェントAIの技術実体、性能評価、および地政学的リスクのデューデリジェンス



実行能力は本物だが、法的安定性が崩壊している

Manusは高度な「実行レイヤー」として実在し、半構造化業務を自動化する強力な機能を持つ。しかし、Metaによる買収と中国当局の介入により、法的・地政学的な運用リスクが極めて高い状態にある。

技術・性能

既存のフロンティアモデルを束ねる「Action Engine」。リサーチやアプリ構築に強いが、実取引の確実性には課題が残る。

地政学・資本

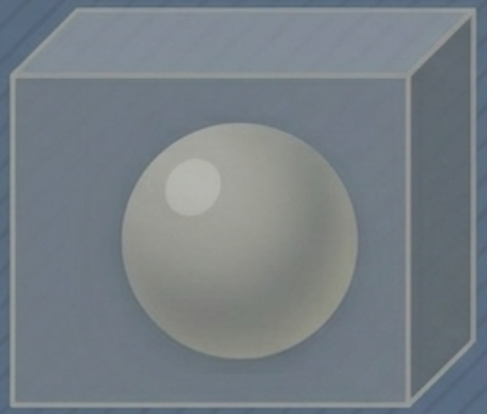
2025年12月にMetaが買収発表後、中国当局（NDRC）が審査・巻き戻し命令を発動。実務統合と法的不安定性が混在。

セキュリティ

独立VMによる隔離（Zero Trust）は評価できるが、認証済みブラウザ操作の「被害半径（Blast Radius）」とデータ学習オプトアウトの契約確認が必須。

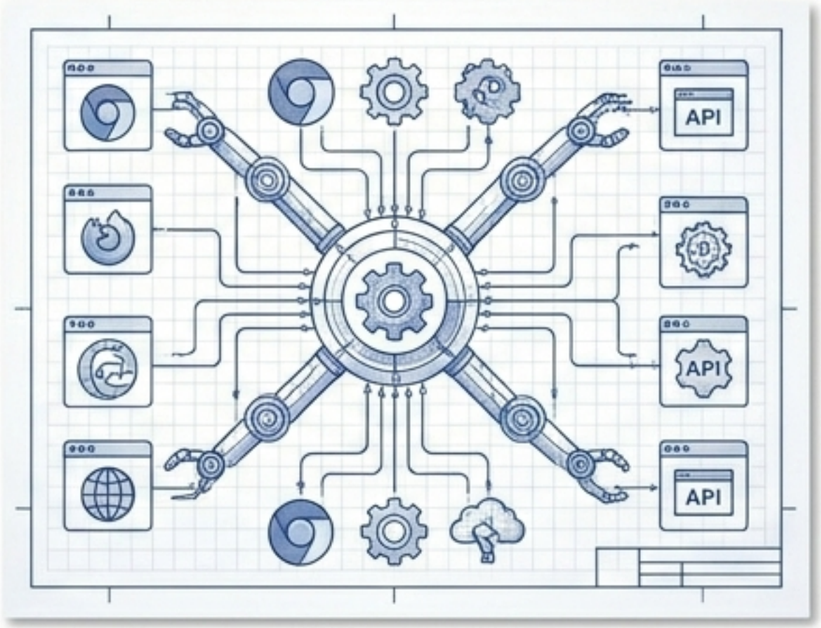
認識のギャップ: 「何」を評価すべきか

「単一の最強基盤モデル」



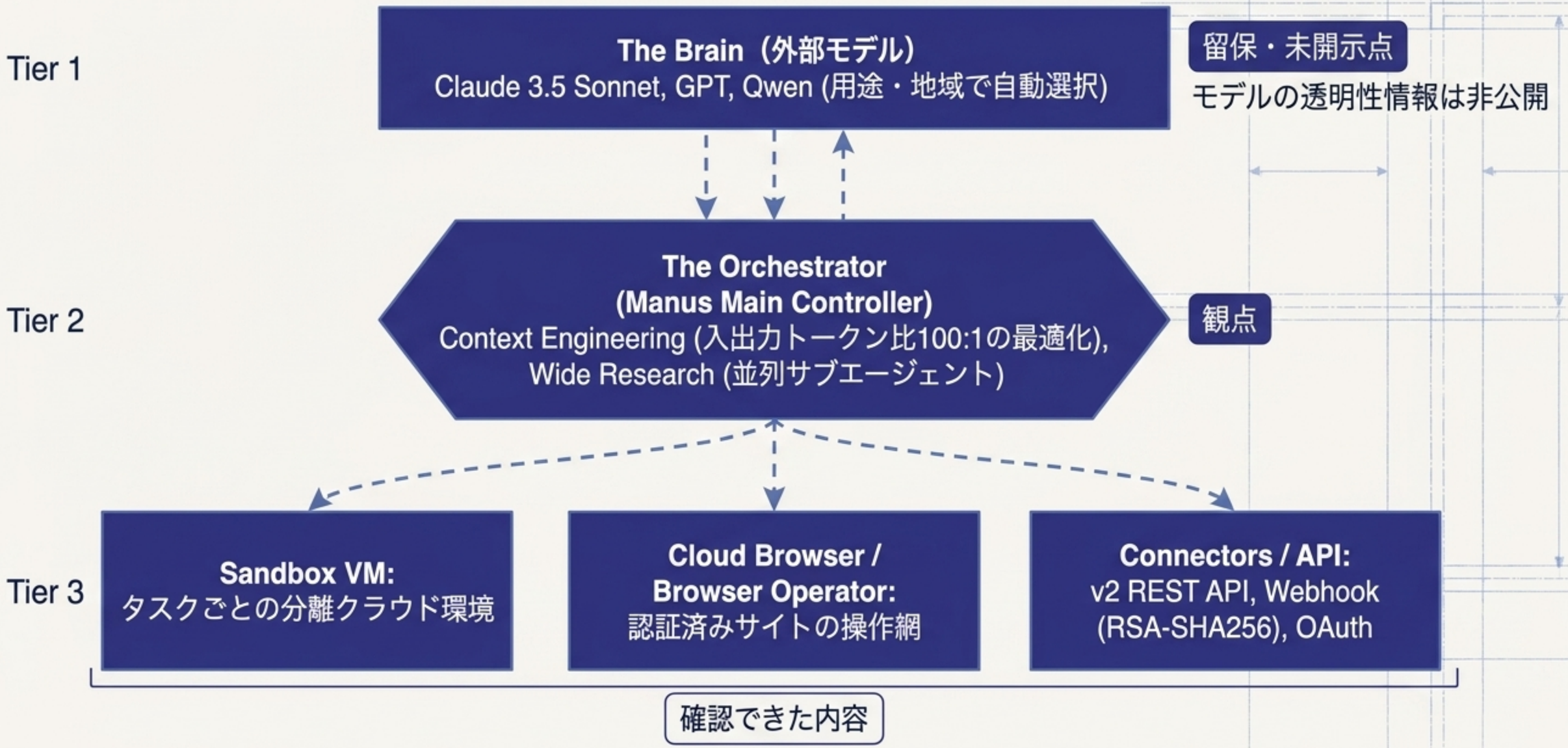
市場の誤解：独自の巨大エンドツーエンドモデルを学習させたDeepSeekの次なる存在。モデルの透明性やパラメータ数が評価の軸となる。

「最強の手足を持つオーケストレーター」



技術的現実：複数の外部モデル（Claude, GPT, Qwen）の能力を引き出す「Context Engineering」を採用。自らを「Action Engine」と定義し、評価の軸は「タスクを完了させる実行力」にある。

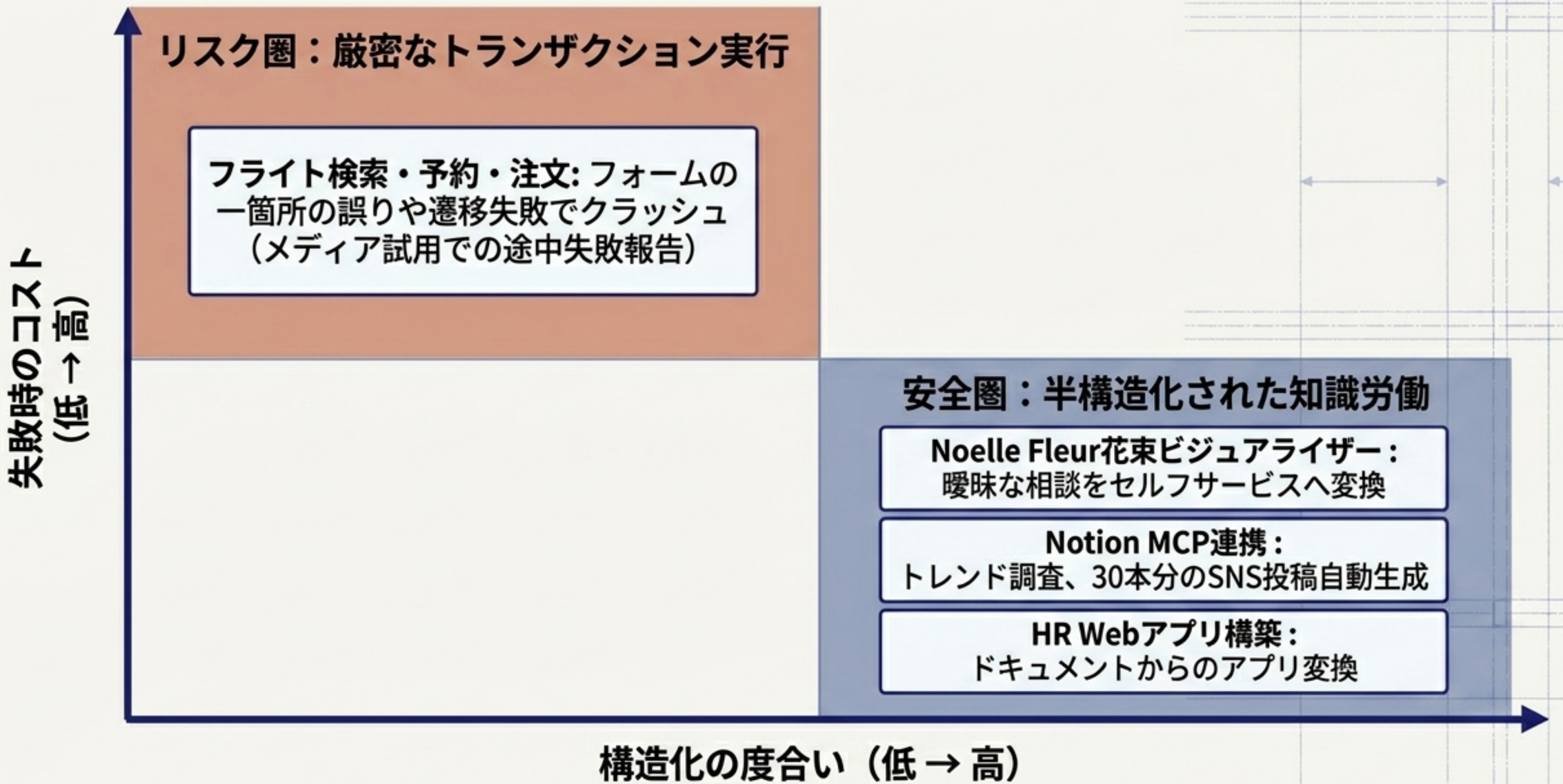
アーキテクチャの解剖図：Action Engineの仕組み



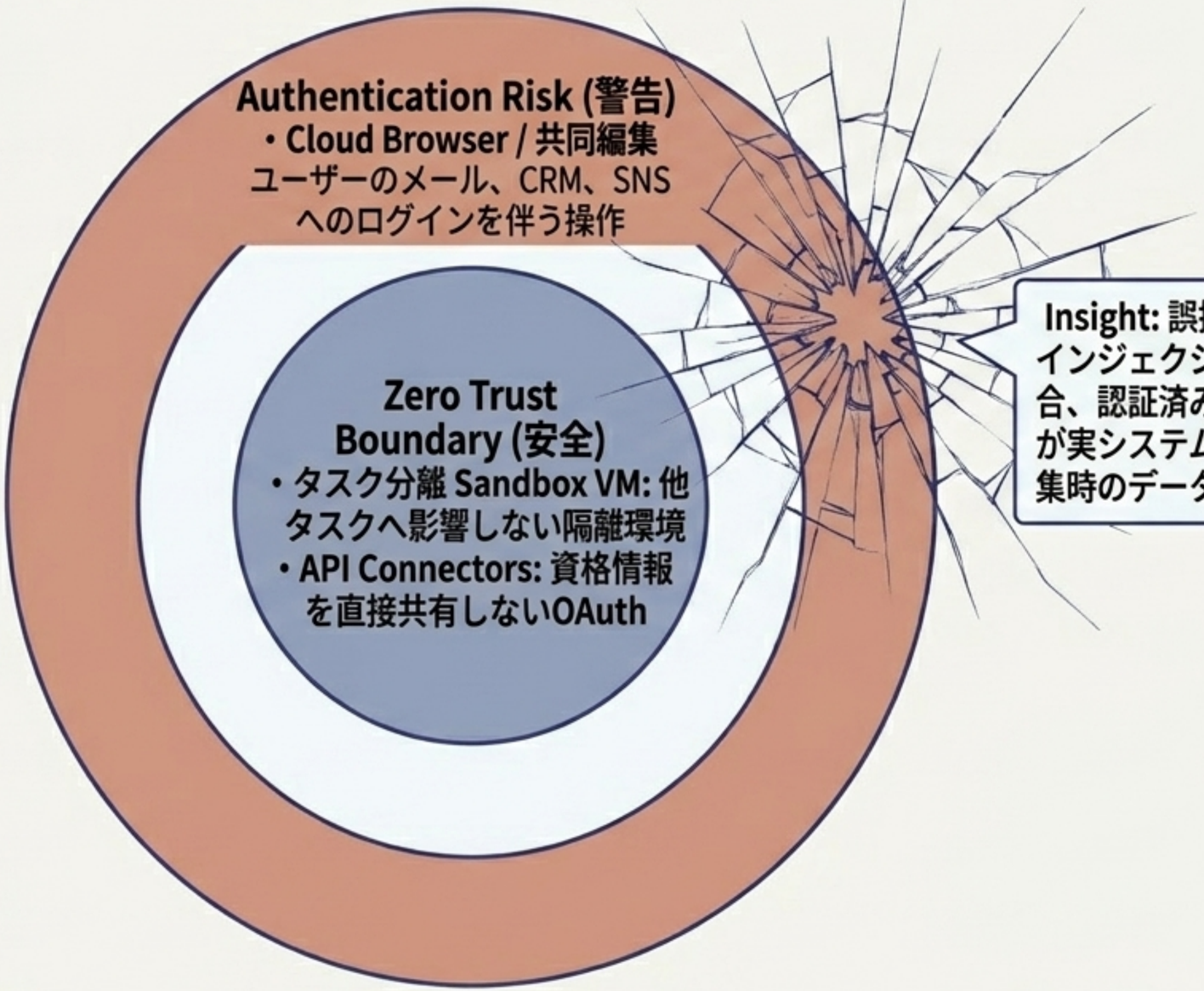
パフォーマンス検証：「主張」と「現実」のギャップ

評価軸	会社側の主張 (Claim) vs. 独立検証・反証 (Reality)	総合判定 (Verdict)
外部ベンチマーク	会社側はGAIAでOpenAI Deep Research/Assistant系より優位だと主張。東京イベントでも約10%優位を説明。	△ 独立再現性が弱い
	現在確認できる独立公開の検証済みGAIA掲載ではManusが見当たらない。	
内部評価	1.6 Maxは二重盲検テストで満足度が19.2%改善。	△ 客観性に限界
	あくまで社内評価であり、第三者の再現検証はない。	
品質保証の透明性	並列サブエージェントで幻覚を減らす設計。	△ 監査指標不足
	幻覚率低下の独立監査値は未公開。	

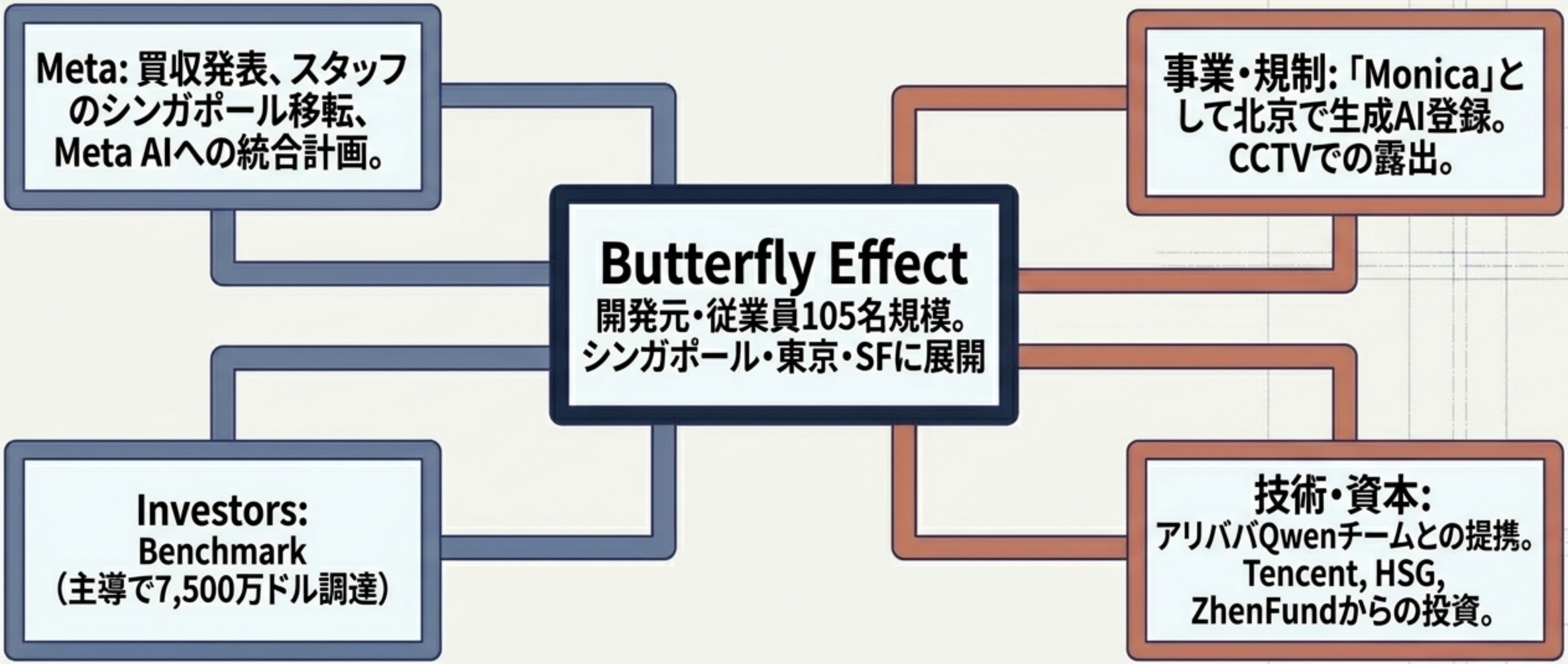
導入適性ヒートマップ：得意領域とリスク領域



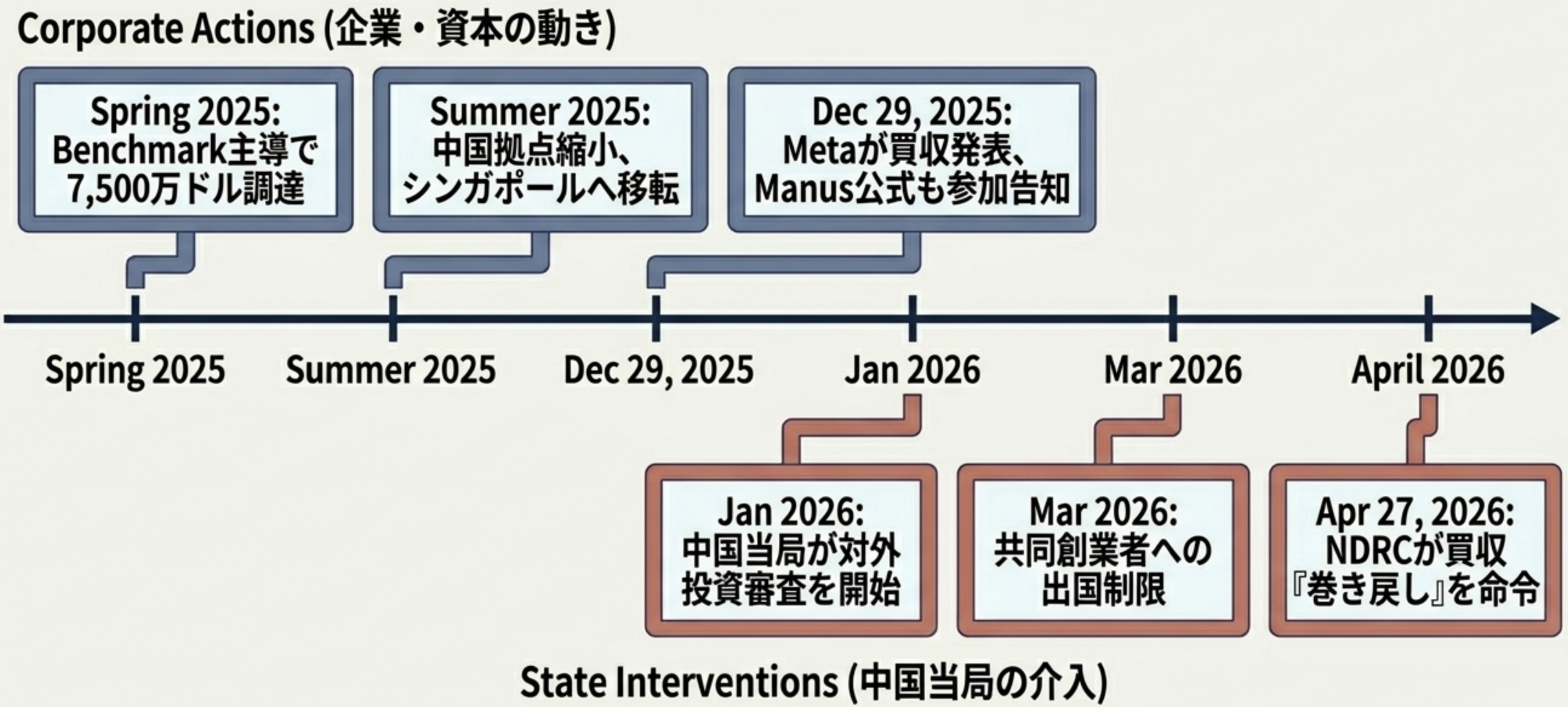
セキュリティ境界と「被害半径（Blast Radius）」



地政学と資本の複雑なレイヤー（China Nexus）



地政学的な綱引き：買収から「巻き戻し」までのタイムライン



データガバナンス：「統制」と「共有」の境界線を引く

確認された事実：規制と政策の統制

- 中国当局による取引審査と巻き戻し命令の行使
- 国内向け（Monica）の当局への登録と認可

結論: 強い政策支配力と規制権限の下にあることは「事実」である。

確認されていない事象：データ共有の実態

- 中国政府への直接的なユーザーデータの共有証拠（なし）
- 政府による直接的な企業保有の証拠（なし）

結論: 「統制下にあること」と「実データが抜かれていること」は別の命題である。

Action Required: 企業利用時はTeamプランの「Data Training Opt-Out」の契約上の法的意味の精査が必須。

戦略的シンセシス：大国間のオーケストレーション戦争

> 「技術的には強力なオーケストレーターだが、戦略的には国家間のオーケストレーションの『対象』に陥っている。」

The Value (価値)

Manusの真価は、特定の賢いモデルを作ることではなく、「長い実行経路を太く繋ぐ」実行レイヤーとしての成熟度にある。

The Flaw (致命的欠陥)

最大の弱点はAIの性能ではなく「法的な安定性の崩壊」。Metaへの統合プロセスと中国への知財・人的な巻き戻しリスクが衝突している。

アクションプラン：企業導入に向けた4つの監査ステップ

1 技術監査（データフローと学習利用）

モデルルーティング、保存先、サブプロセッサー一覧、Data Training Opt-O-Outの設定を文書で確認。

2 用途制限（PoCのスコープ定義）

予約・注文などの高リスクな自律実行は避け、まずは「半構造化された知識労働（調査・資料生成）」に限定。

3 地政学・法務デューデリジェンス

Meta買収巻き戻しの影響、China nexus、知財移転、輸出入規制の確認を、通常のSaaS導入審査よりも厳格に実施。

4 プライバシー設計（Zero Trustの徹底）

Cloud Browserの認証済み操作は最小権限アカウントに限定し、秘密情報を含むSandboxタスクでの共同編集機能を無効化。