

中国製フロンティアLLM： エンタープライズ実装設計図

米中性能差の消失と、データ分類に基づく
「ポートフォリオ&ルーティング」戦略の完全体系

調査基準日: 2026年7月19日 | 対象モデル: Kimi K3, GLM-5.2,
Qwen3.7 Max, DeepSeek V4 Pro | 経営・調達・実装判断向け

結論：全面採用か全面排除かではなく、最適ルーティングへ



「追いつき」は事実

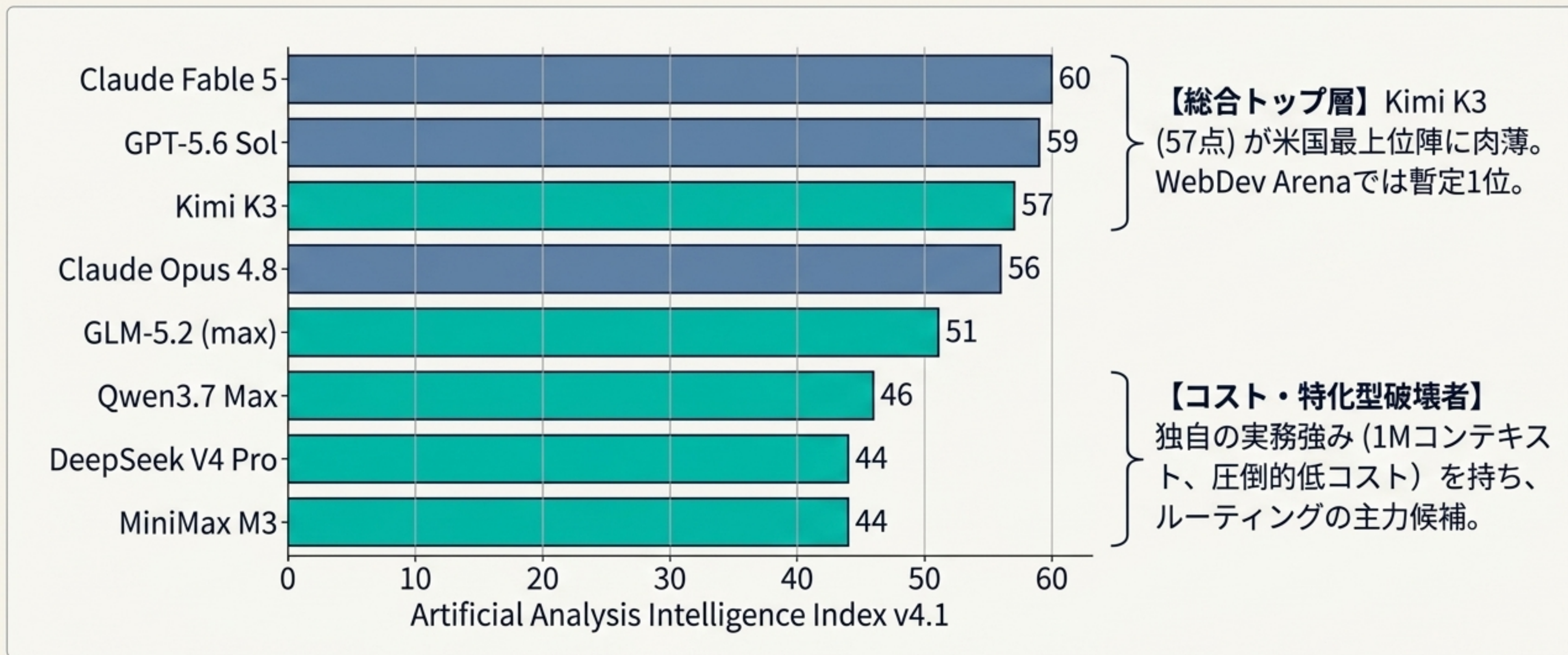
トップモデル間の性能差は2.7%に縮小（Stanford AI Index）。Kimi K3等の登場により、米国系最上位と「ほぼ同じ競技場」に到達。



国籍ではなく「経路」で制御する

単一モデルへの依存を脱却。データ分類（公開・機密）、提供経路（API・自社基盤）、用途別の複線型ポートフォリオを構築する。

フロンティアの密集：トップ3はわずか「3点差」に



米国製に追いついたのか？ 4つの問いで分解する



公開ベンチマークで近いか？
[概ね Yes]

トップ差2.7%。候補外にする合理性は薄れた。



特定タスクで首位か？
特定タスク 首位か？ [すでに Yes]

Kimi K3のWebDev、GLM-5.2の長期コード。用途別ルーティングが有利。



総合UX・信頼性も同等か？ [まだ No]

思考履歴の不安定さ、NIST評価でのサイバー課題の遅れ。
人間による検証が必須。



持続的な全面首位か？ [未証明]

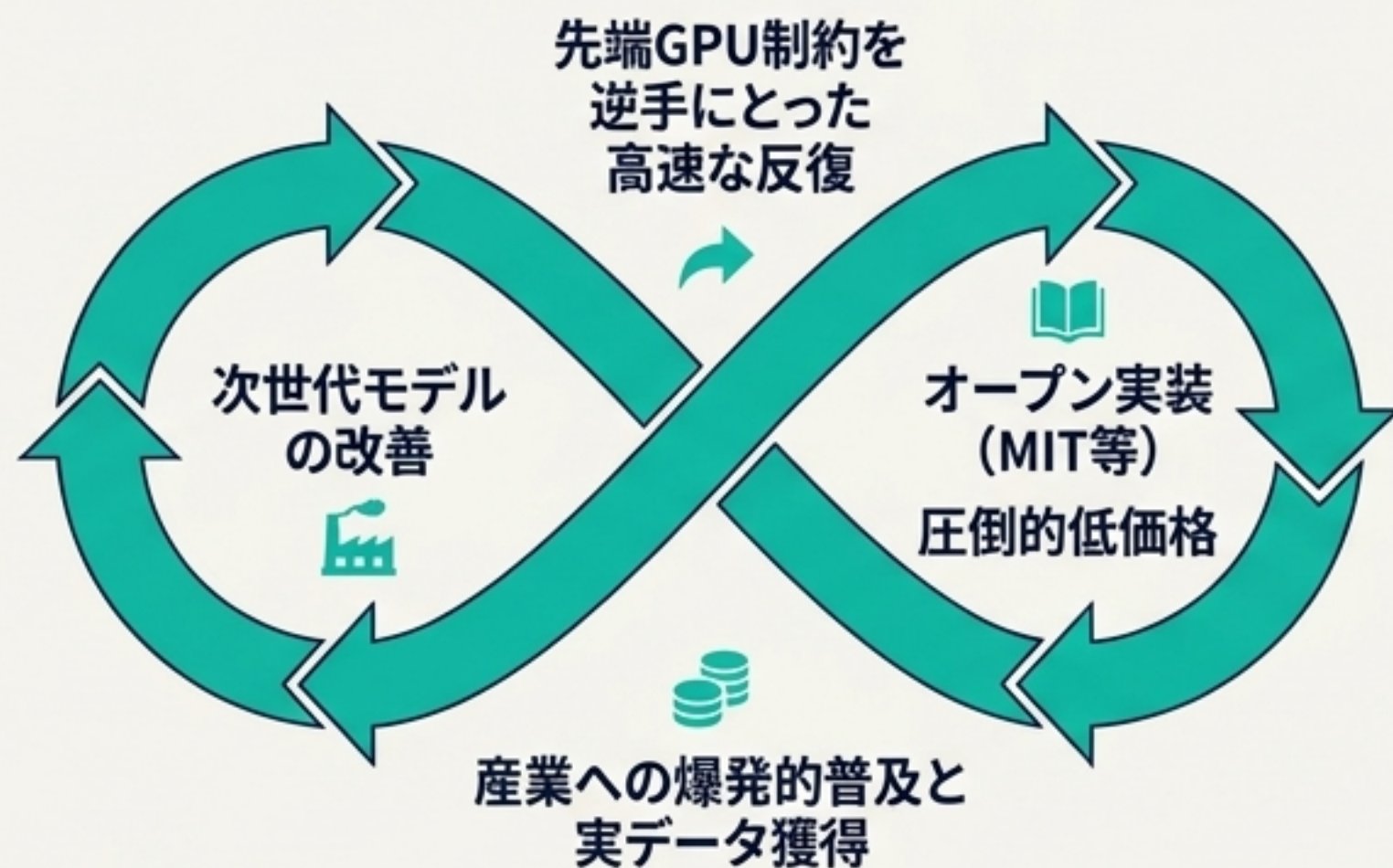
数週単位で首位が交代する「回転するフロンティア」。
ロックイン回避が絶対条件。

主要4モデルの企業向けプロファイリング

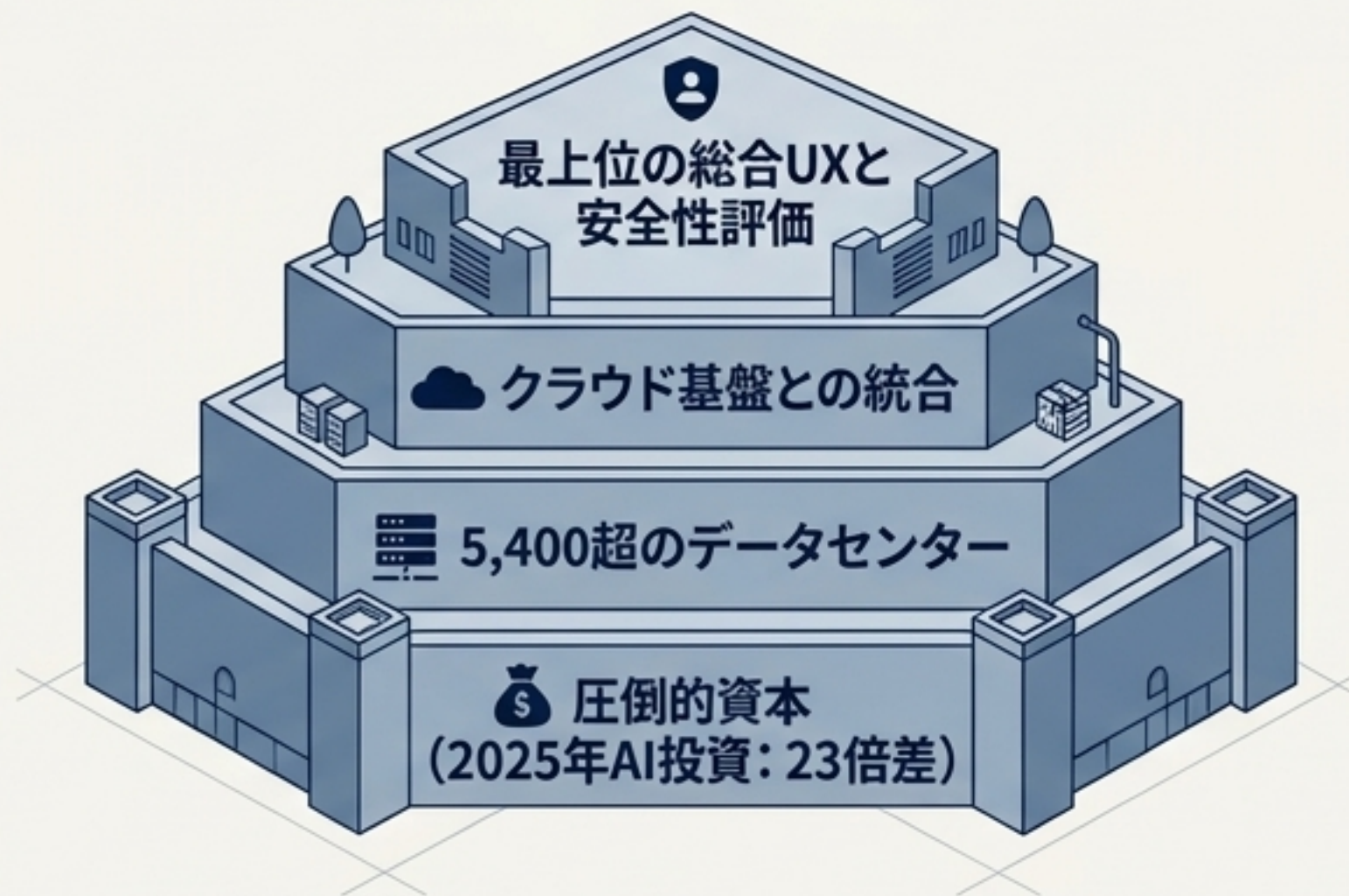
	Kimi K3	GLM-5.2 (max)	Qwen3.7 Max	DeepSeek V4 Pro
 Specs	2.8T/16 active (API). 1Mコンテキスト。	約750B/40B active (MIT オープン重み)。	非公表 (独自モデル/API)。	1.6T/49B active (MIT オープン重み)。
 Strengths	中国勢最強の総合性能 (AA 57)。資料作成・ フロントエンド設計。	長期コード監査、自社 専用基盤での高い統制 力。	高速(200 token/s)、 ツール呼び出し、オフ イス自動化。	圧倒的な費用効率。一 次処理やバッチ推論の ルータ要員として最適。
 Risks	技術報告/重みが未公 開(7/19時点)。過度な 先回りの癖。	非常に冗長。巨大モデ ルゆえの自社配備 (GPU)負担が重い。	重み非公開。"Global scope"と"国内保存"を 契約上区別すること。	直営SaaSは中国内保存。 NIST評価でサイバー/推 論に弱点(約8ヶ月遅れ)。

「モデル単体」の競争から、「普及ループ」対「インフラの濠」へ

普及ループ（中国勢の戦略）



資本と計算資源の濠（米国のエコシステム）



2026-27年は「回転するフロンティア」。
単独王者は不在であり、供給国を分けた二重化が必須。

複雑性：圧倒的コスト効率に潜む 「ギザギザの知能」とデータリスク



DeepSeek V4 Pro (The Reward)

AA v4.1 Score 44

\$0.43/MTok

安価な「弱モデル」ではなく、大量の一次処理を担う強力なエンジン。



NIST CAISI & Privacy (The Risk)

NIST Evaluation Gap:

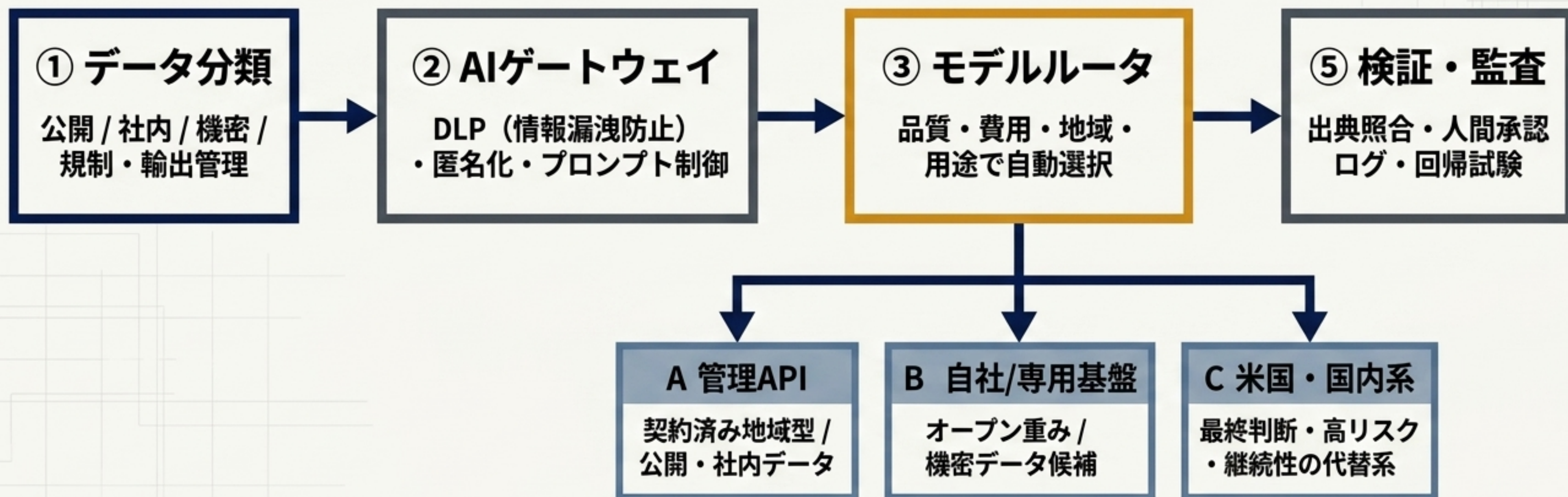
NIST評価: 数学は強いが、サイバー(32%)、ARC-AGI-2(46%)で米国上位に約8ヶ月遅れ。

Privacy Warning:

直営SaaSのプライバシーポリシーは「中国で直接収集・処理・保存」と明記。機密入力厳禁。

【結論】 安さだけで直営SaaSを使うのは危険。保護された「経路」での実装が必要。

エンタープライズ向け推奨アーキテクチャ： 「AIゲートウェイとルータ」



禁止線：承認のない消費者向けSaaSへ
個人情報・営業秘密・未公開発明を入力しない。

データ分類と提供経路のマトリックス

4x4 Data Governance Heat-Map Matrix				
	①直営SaaS	②契約済み企業API	③地域型第三者	④自社/専用隔離基盤
1. 公開 (Public/Web)	利用可。出力検証 必須。			
2. 社内 (Internal/Anonymous)	原則不可。	SSO/DLP/学習不使 用の確認で可。		
3. 機密 (Confidential/Source Code/M&A)				隔離、最小権限、 版固定で可。
4. 規制・限定 (PII/Export Control)	全外部LLM原則禁止。案件別の専用環境と法務承認。			

用途別ルーティング： 適材適所のポートフォリオ戦略

Task Assignment

大量の安価な 一次処理

- 候補 (Candidates):
DeepSeek V4 Pro
(難問は上位へ転送)
- 条件 (Conditions):
公開・匿名化データ、
または地域型提供。

長期コード・ 大規模リポジトリ

- 候補 (Candidates):
GLM-5.2 max
(代替: **Kimi K3**)
- 条件 (Conditions):
社内基準、コミット
権限の明示。

高速なオフィス・ ツール連携

- 候補 (Candidates):
Qwen3.7 Max
(代替: 米国・国内系)
- 条件 (Conditions):
処理地域(DPA)、
スナップショット固
定の確認。

高リスクの 最終判断

- 候補 (人間 + 米国
系/国内系企業基盤
(中国系は反対意見・
探索として利用)
- 条件 (Conditions):
自動確定の禁止、
一次資料と二重承認
の必須化。

調達・法務のゲートチェック：最低限確認すべき重要項目

管轄・データフロー

- 契約主体、準拠法、紛争解決国はどこか？
- データ処理・保存・バックアップの「物理的リージョン」は？
- 再委託先・下請先の開示と変更通知はあるか？

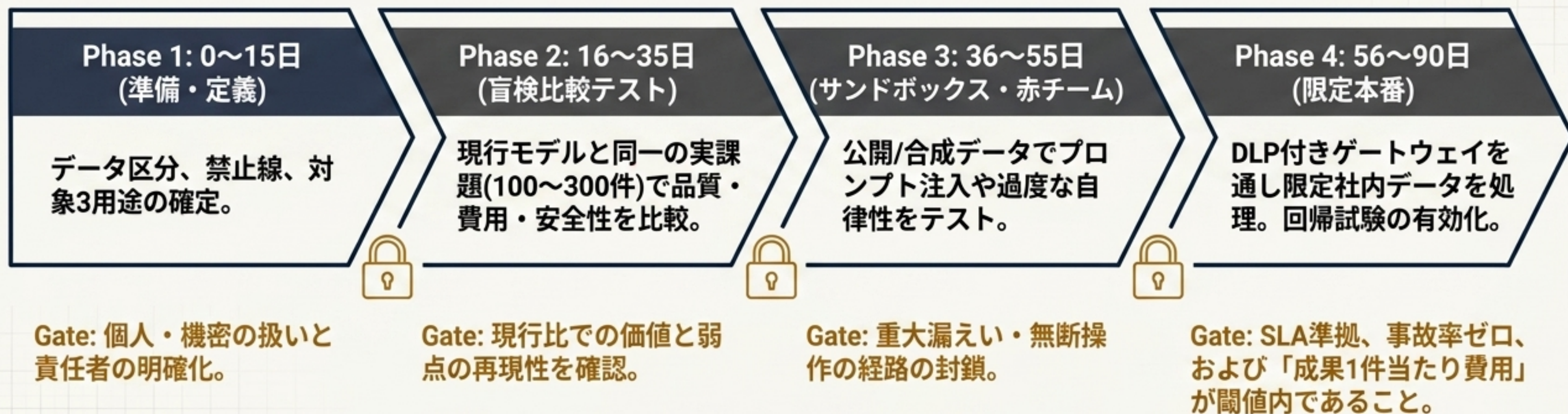
セキュリティ・権利

- 入力/出力の「学習不使用」が明示されているか？
- テナント分離、暗号化、鍵管理の主体は誰か？
- オープン重みの場合、脆弱性対応やSBOMは提供されるか？

運用・継続性

- モデルIDとスナップショットの固定は可能か？
- 輸出規制・制裁・地政学リスクによるサービス停止の補償は？
- 契約終了時のデータ返却
・ 完全削除証明は出るか？

90日導入ロードマップ：安全な限定本番へのステップ



最善の選択は「無条件に避ける」ことではなく、「用途別に勝者を変えられる運用能力」を自社に持つこと。