



2026知財・情報フェアに見る、知財特化AIの現在地と未来設計図

ローカルLLMと外部接続（MCP）が交錯する会場から読み解く、AI導入のパラダイムシフト

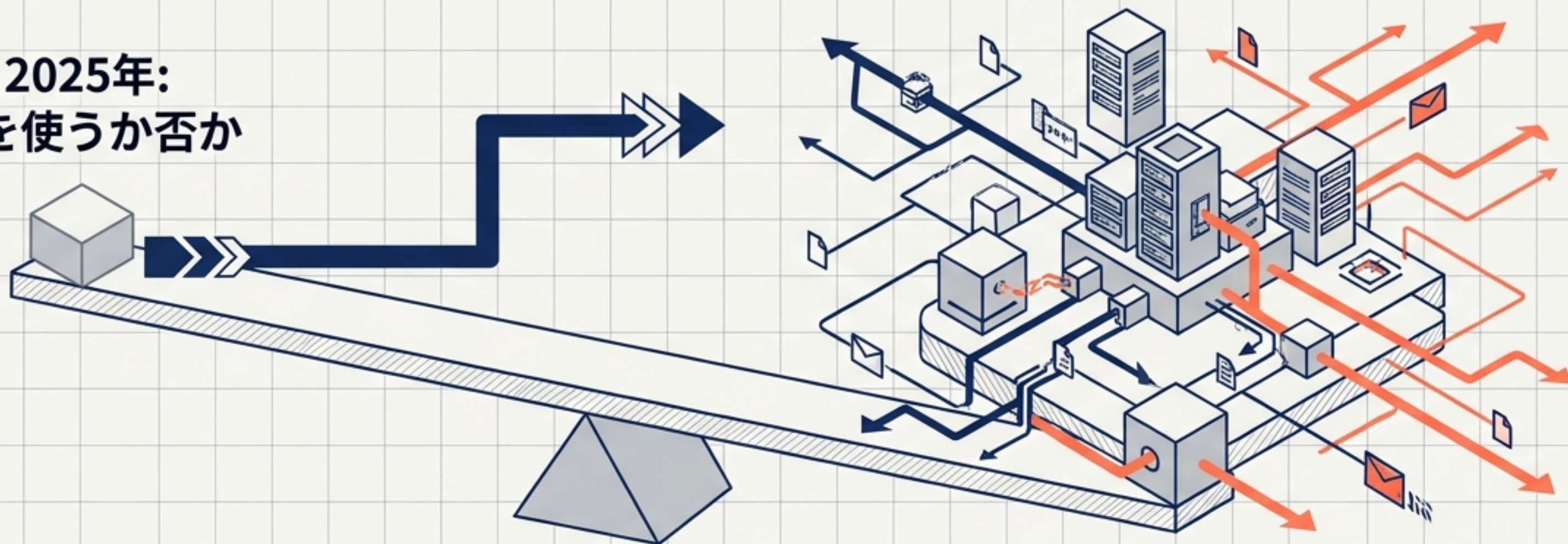


わずか1年で劇的に進化した「問い」のレイヤー

来場者数: 8,634名
プレゼン数: 108テーマ

2026年: どのAIを、どこで、どう接続するか

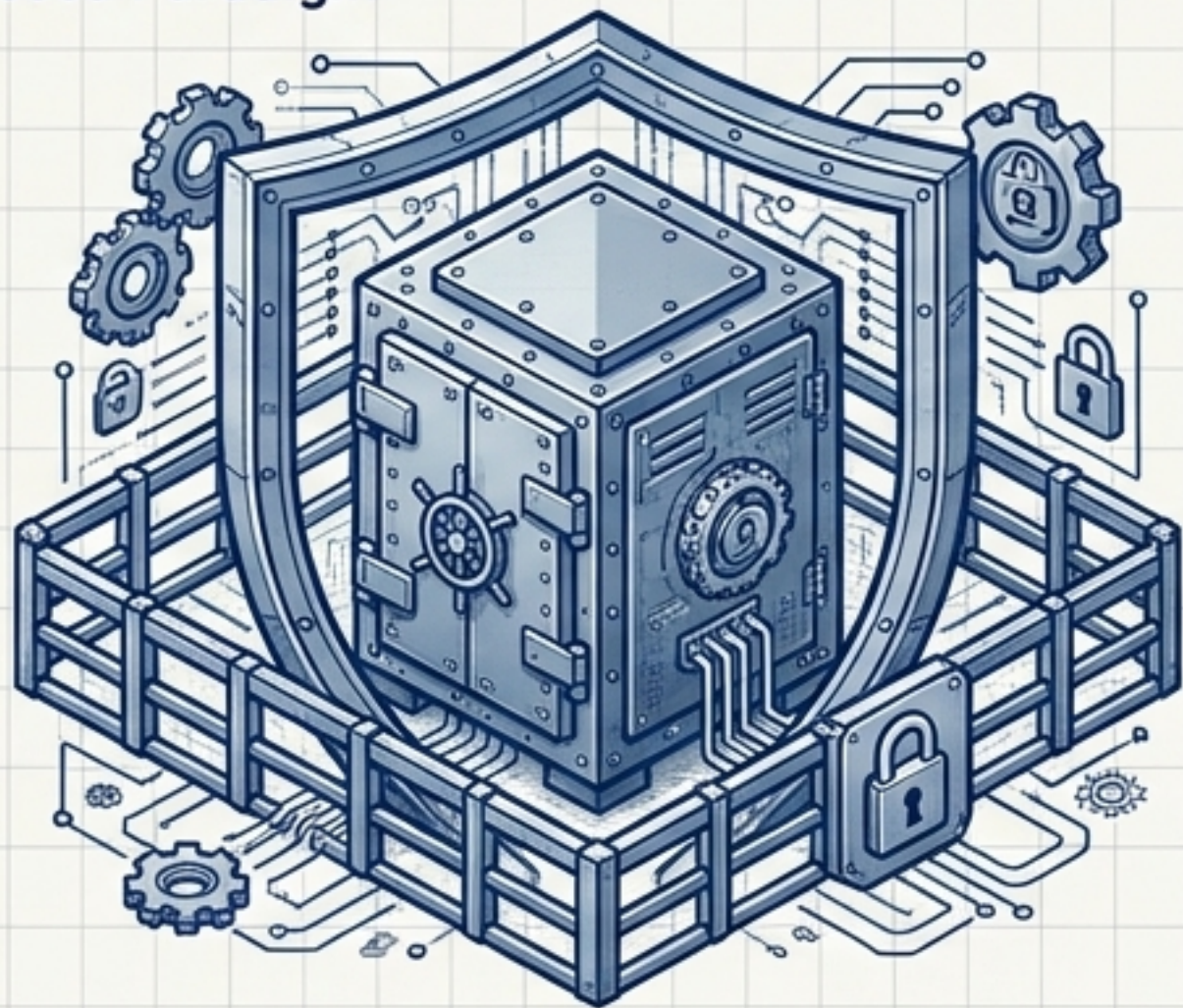
2025年:
AIを使うか否か



2026年の知財・情報フェアは、AI活用が単なるツール導入から
「システムアーキテクチャ設計」の段階へ突入したことを明確に証明した。

会場を二分した、相反する「2つの巨大な潮流」

The Closed Paradigm



「閉じるAI」

完全オフライン / ローカルLLM

The Open Paradigm



「開くAI」

公開LLMへのMCP直接連携

機密保護を至上命題とする「ローカル化」と、公開情報への直接アクセスを
至上命題とする「MCP連携」の並立が今年の特徴である。

[Thesis] なぜ今、「ローカルLLM」がプレゼンの主役となったのか



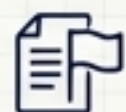
日本弁理士会ガイドライン

秘密情報の第三者プラットフォーム入力
による守秘義務違反・新規性喪失リスク



特許庁 AIビジョン

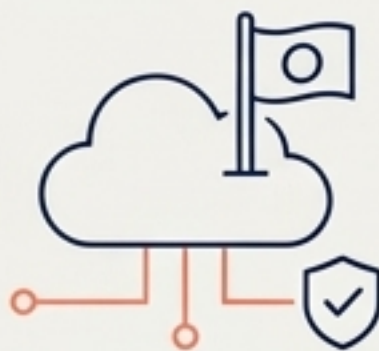
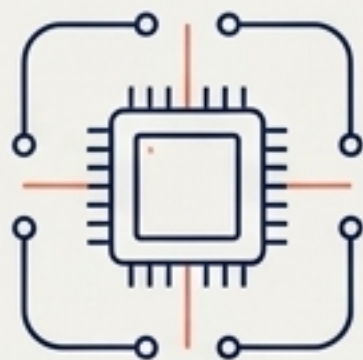
機密情報漏洩防止と
「人間中心・検証可能性」の原則



政府 (GENIAC等)

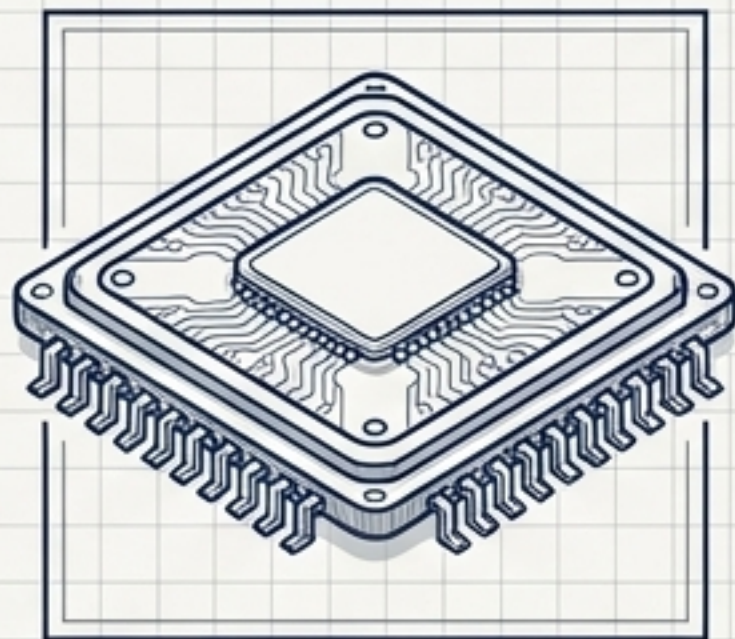
国産LLM振興策による「国内閉鎖
環境」への公的な正統性付与

「ローカル」という言葉の解像度を上げる：4つの技術類型



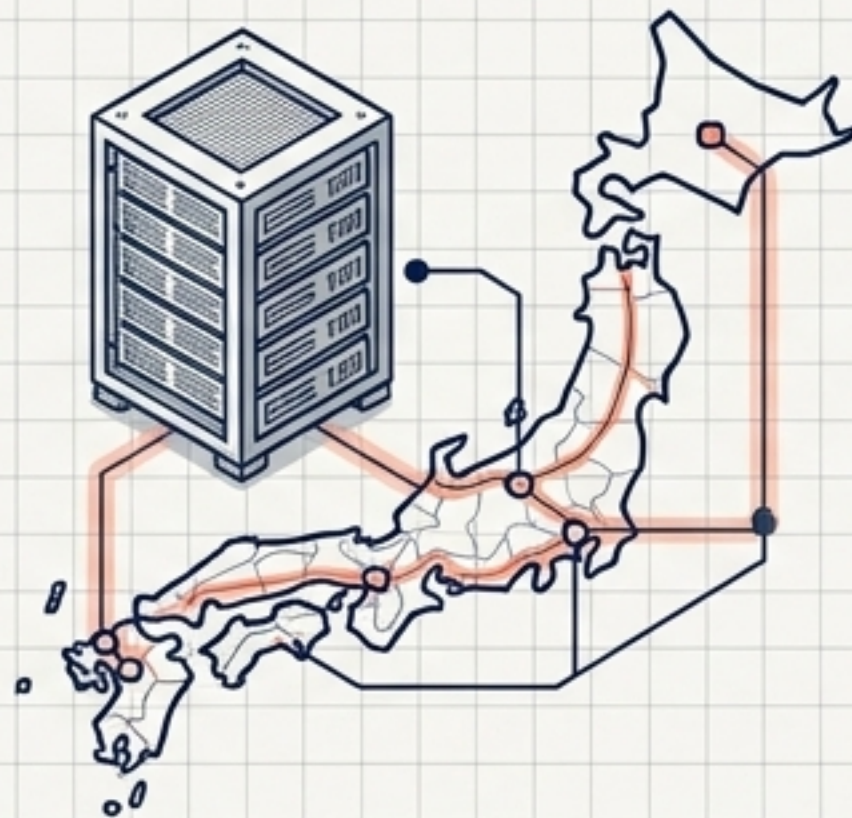
	(A) 完全オフライン型	(B) 国内ソブリン型	(C) 閉域クラウド型	(D) 特許特化独自モデル
推論環境	PC / イントラ完結	国内データセンター	自社契約クラウド	未開示 / オンプレ
基盤モデル	小規模・CPU駆動	オープンウェイト	商用API	特許特化の継続学習
外部通信	完全遮断	MCP連携あり	VPC等による論理遮断	不使用（プロトタイプ時）
出展企業例	アイビーリサーチ	GMO知財AI	サマリア等のオプション	Patentfield

「閉じる」最前線：アプローチの多様化



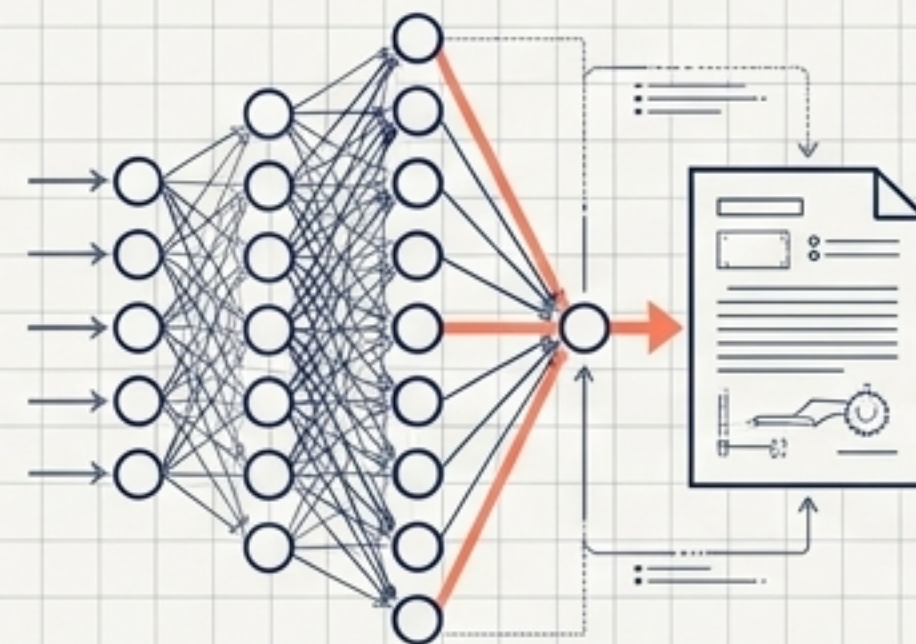
アイビーリサーチ

- CPU駆動のオフライン実用化
- GPU不要のPC単体動作
- 審査済み公報特化学習+RAG
- 外部通信を完全遮断



GMO知財AI

- オープンモデル×国内ベアメタル
- 国内GPUクラウド上でGemma 4稼働
- 商用API同等のプライベート空間
- MCPによるデータ連携基盤



Patentfield

- 1,000億トークンの特化学習
- GENIAC技術新規賞モデル
- プロンプトレス推論の実現
- 外部API不使用のローカル構成

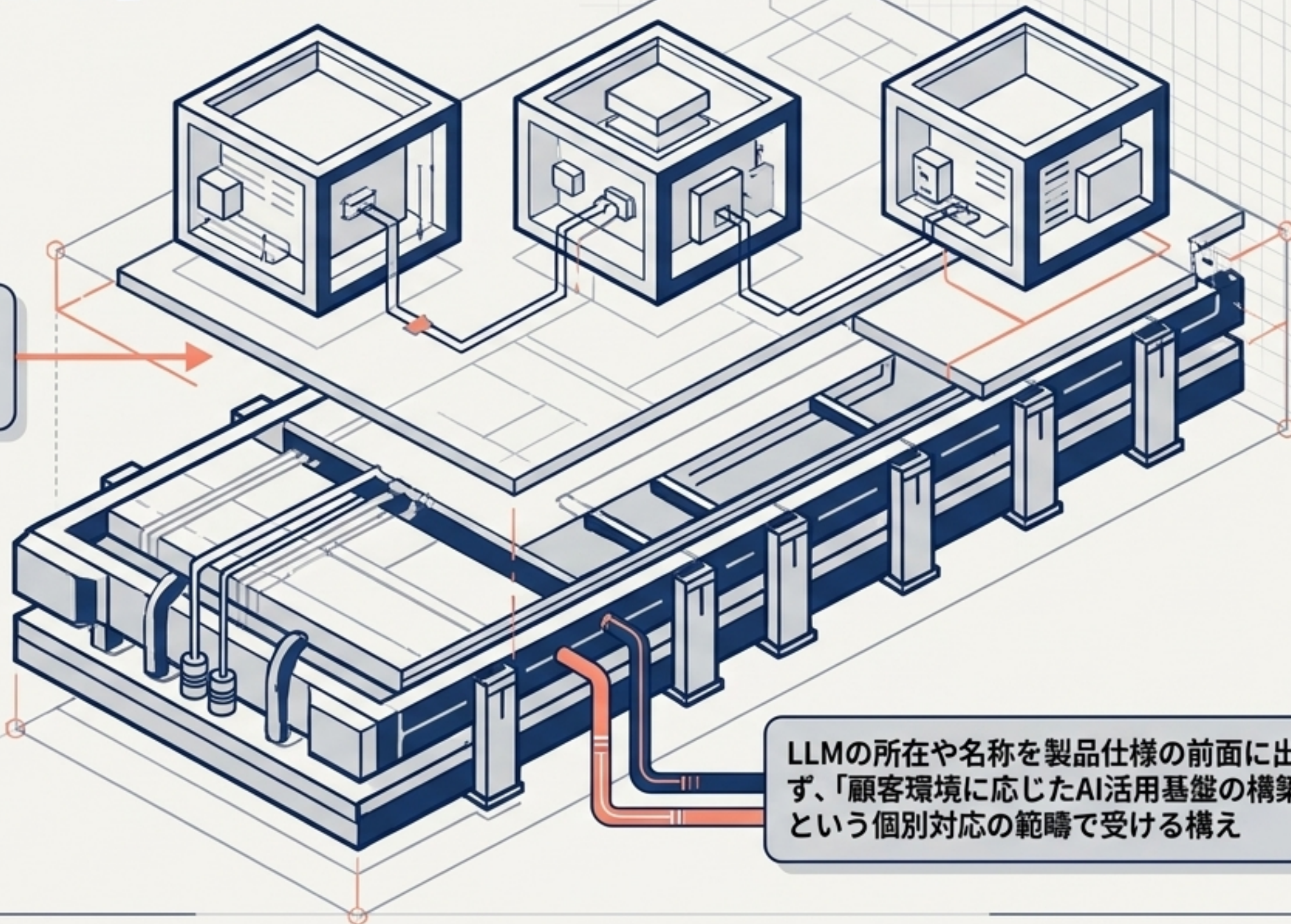
巨大Slerの静かなる対比： 「製品」か「基盤構築」か

ベンチャー / 海外勢の アプローチ

「完全オフライン」「オンプレミス」を
製品のコアバリュー・差別化要因とし
て前面に訴求（パッケージ製品化）

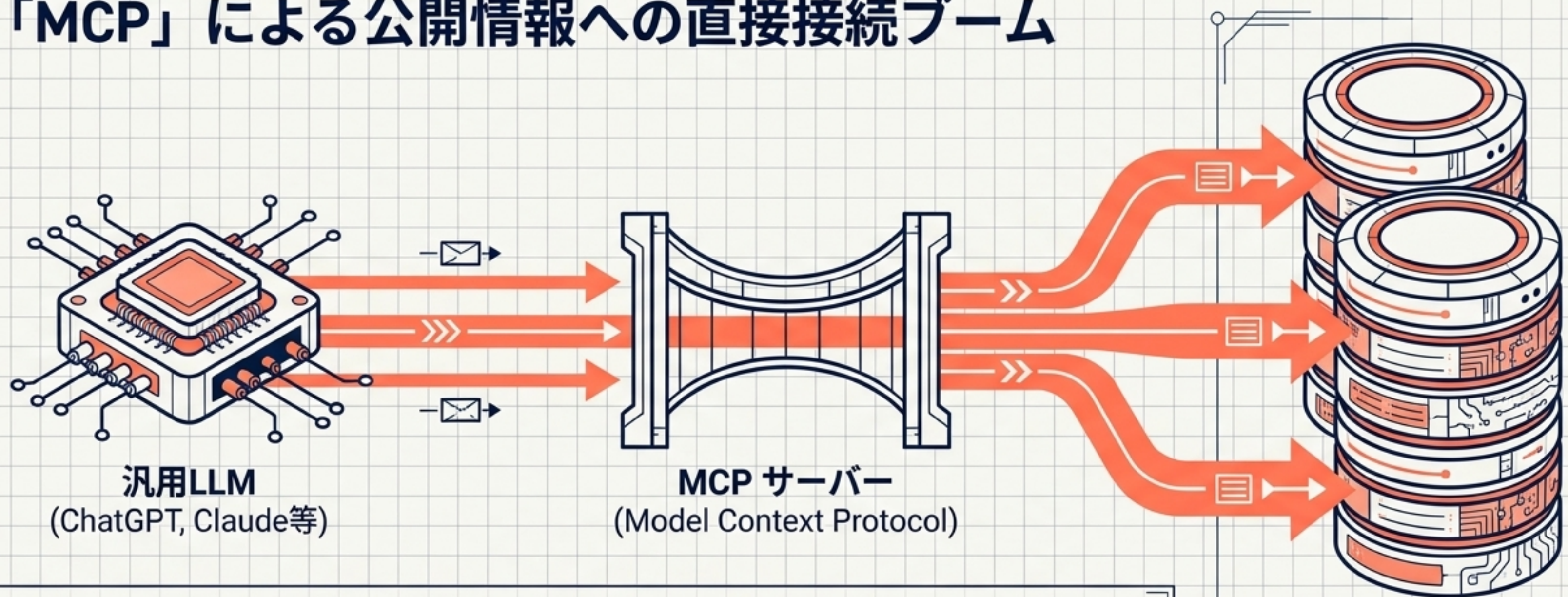
大手Slerのアプローチ (日立, 東芝, NTTデータ等)

LLMの所在や名称を製品仕様の前面に出さ
ず、「顧客環境に応じたAI活用基盤の構築」
という個別対応の範疇で受ける構え



[Antithesis]

「MCP」による公開情報への直接接続ブーム



- ・ローカルの対極にある、API経由で特許DBを直接叩く「開く」アプローチ
- ・サマリア、AI Samurai、Patsnapなど主要ベンダーが相次いで対応を発表
- ・専門知識を汎用AIに直接引き渡す仕組みが、調査・分析工程で急速に標準化

「開く」ことの代償：MCPのトロイの木馬リスク

Alert



社内ネットワーク（機密情報）



発明の着想 / 検索クエリ



パブリックLLM空間

【脆弱性の本質】

検索対象が「公開公報」であっても、入力する「**自社の検索クエリ**」は**極秘の未公開情報**である。

【UK IPKatの警告】

汎用LLMプロバイダーはMCPサーバー側のデータ保護を保証しない。
守秘契約のない接続は、接続は、営業秘密の管理義務を損なう恐れがある。

【ガバナンスの急務】

便利な接続が広がるほど、**社内規程による境界線の設定が不可欠**になる。

[Synthesis] 工程の特性が生み出した「自然発生的な棲み分け」

上流工程：Local / Closed（未公開情報）

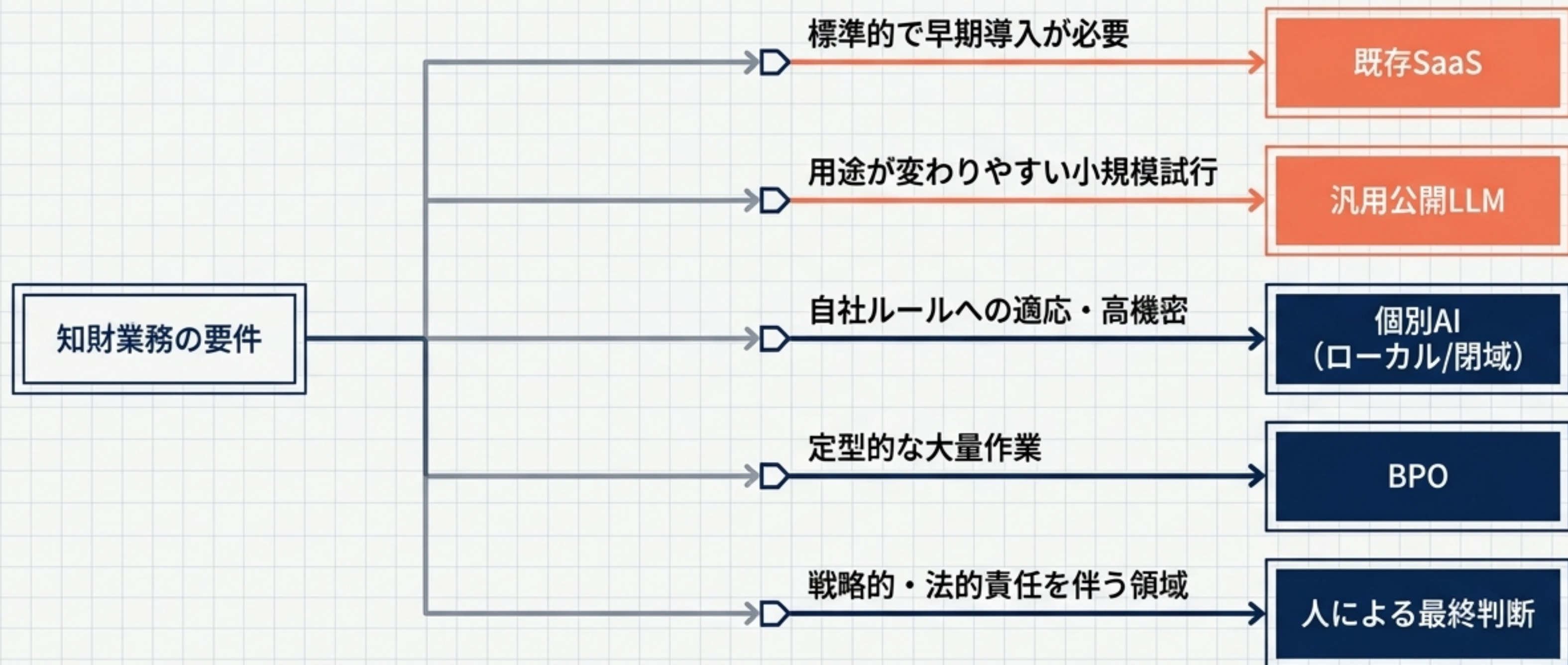
下流工程：MCP / Open（公開公報）



機密保護が絶対条件。
完全ローカル・閉域クラウドへ
の需要が集中。

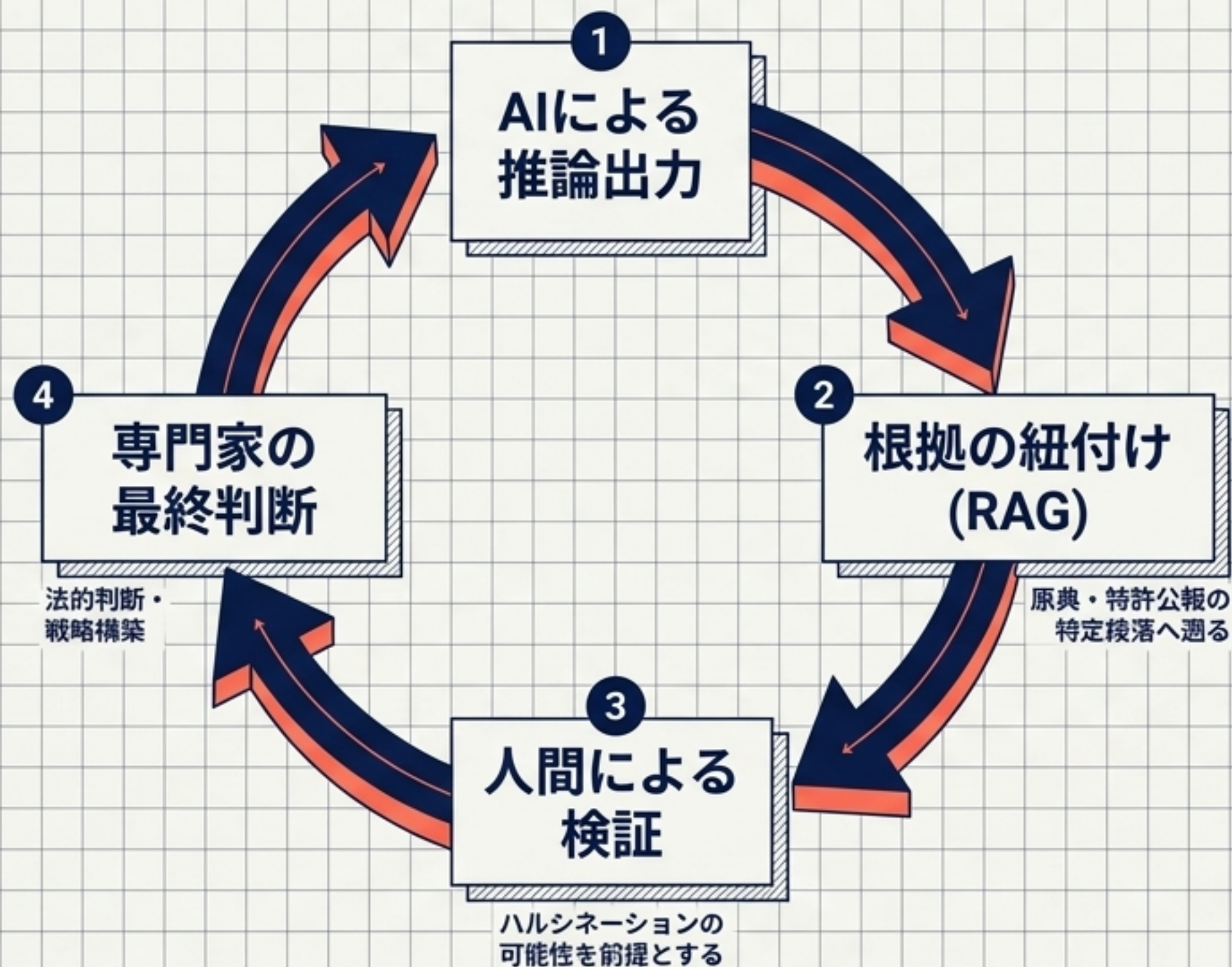
汎用LLMの高い推論能力と
MCPの外部DB連携メリット
がリスクを上回る。

新たなパラダイム：「使い分け」のポートフォリオ設計



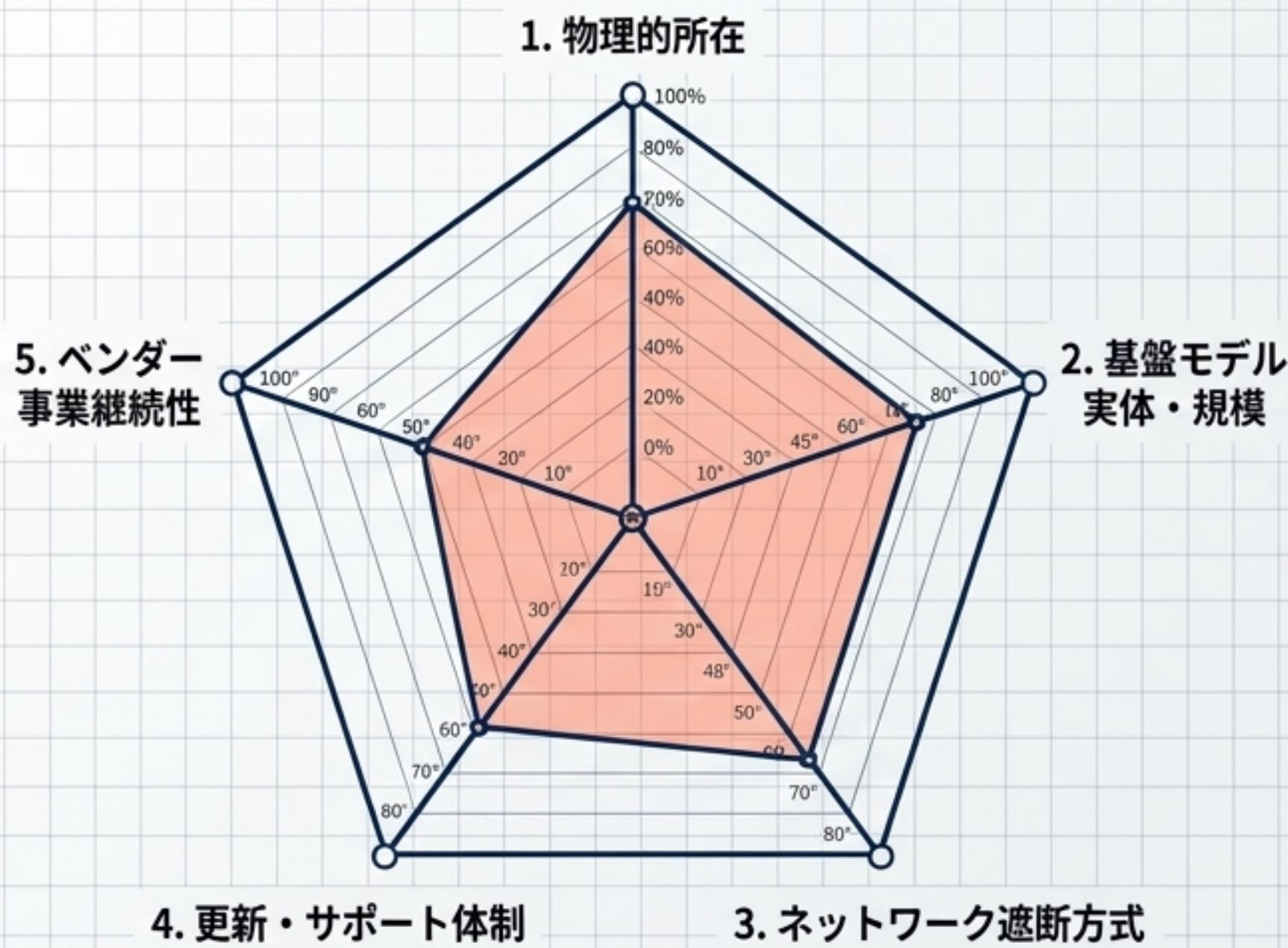
AIDAO等が提唱する「万能なAIはない」という成熟した視点。
業務ごとの棚卸しと、複数ツールのハイブリッド設計こそが知財DXの最適解。

所在を問わない絶対条件： 「検証可能なAI」とHuman in the Loop



IPCCの講演や特許庁「JPO AIビジョン」が示す通り、AIの出力を鵜呑みにしないプロセス設計が必須。「ローカルクラウドか」以前に、AIの限界を認知に、AIの限界を認知し、人が根拠を検証できる設計できる設計（プロセスの可視化）が不可欠である。

導入に向けた「5つの確認事項」 (ベンダー監査チェックリスト)



1. 推論環境の物理的所在

ユーザーPCか、社内サーバーか、国内DCか、海外クラウドか？



2. 基盤モデルの実体と規模

国産か、オープンウェイトか、商用APIか？パラメーター規模は？



3. ネットワーク遮断の方式

物理的な遮断（スタンドアロン）か、論理的な遮断（VPC）か？



4. モデル更新とサポート体制

基盤モデルの陳腐化に対し、誰がどのようにアップデートを担うか？



5. ベンダーの事業継続性

スタートアップや小規模企業への過度な依存リスクをどう担保するか？

2027年に向けた展望と、 未解決のジレンマ

2027

性能ギャップのジレンマ

保有可能なローカルGPUの限界と、最先端商用モデルの間の性能差を実務でどこまで許容できるか。

運用規程のアップデート

ローカル環境整備と同時に、社内情報のMCP経由での持ち出しを禁ずるガバナンス体制の構築が急務。

第3の道：特許特化SLM

汎用モデルではなく、小規模でも特定タスクに特化させた言語モデル（SLM）をオンプレ稼働させるアプローチの拡大。

知財部門が踏み出すべき、 次世代への3つのアクション

01

業務棚卸しと設計

AIを単に「導入する」段階から脱却し、機密性と定型性に基づき、全知財業務のポートフォリオ（Local / Open / SaaS / 人）を構築せよ。

02

ベンダー解像度向上

「ローカル」「オンプレ」のバズワードに惑わされず、5つの監査確認事項を用いて技術的実体と事業継続性をシビアに見極めよ。

03

エコシステム統制

自社内にとどまらず、委託先の特許事務所を含めた情報の受け渡し経路全体のセキュリティとガバナンス・ガイドラインを再構築せよ。