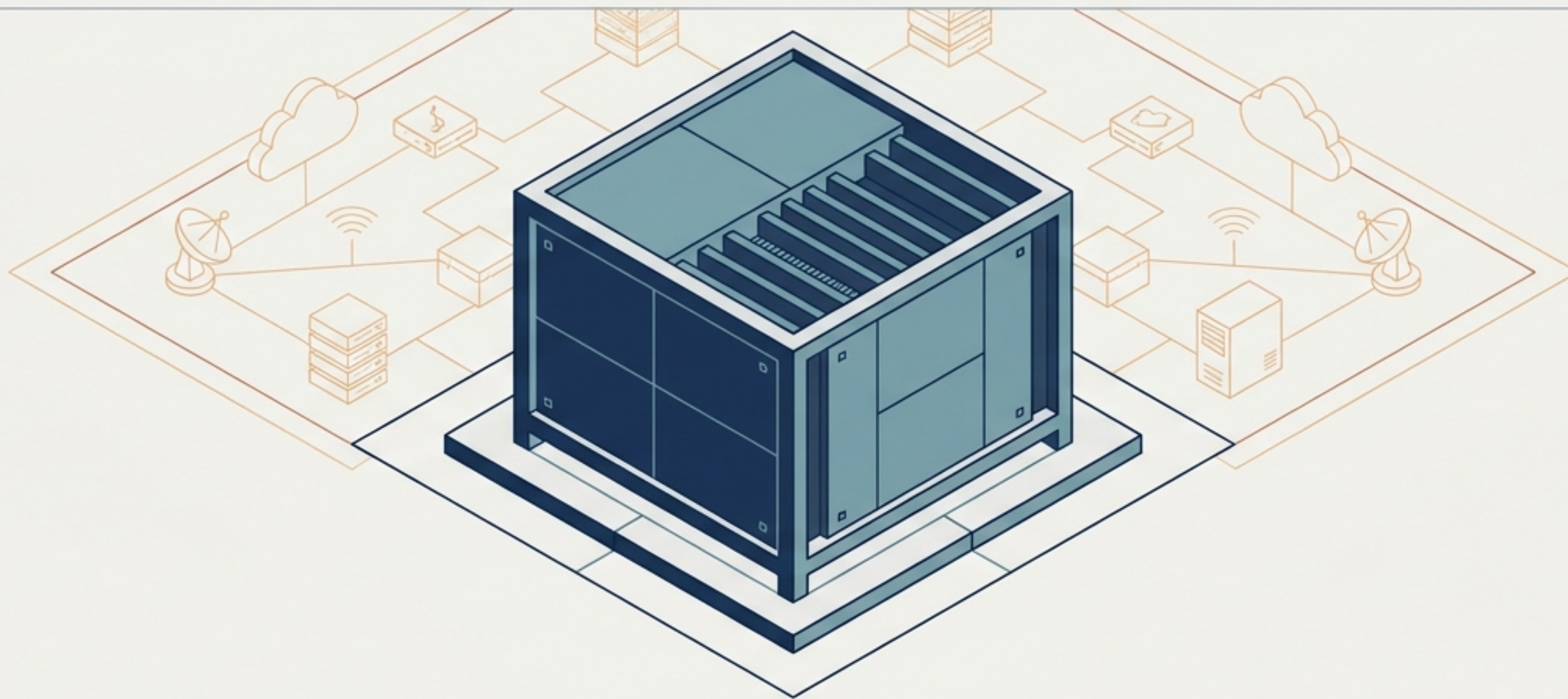


ローカルAIエージェント「Portable Computer」 知財部門への導入可能性分析

クラウドAIの構造的課題を克服する新アーキテクチャの評価と導入シナリオ



対象モデル: Perplexity x NVIDIA (2026年8月25日発表) | 作成日: 2026年8月30日

評価結論：条件付きで導入可能性は高い

条件付きGO

出願前発明や営業秘密など、クラウドAIでは構造的に困難だった領域をローカル処理でカバーできる点が本質的な価値である。



1. 統制設計

クラウドエスカレーション
時の承認ワークフローと
送信基準の明文化



2. 精度実証

日本語特許文書（明細書・
公報等）での公開ベンチ
マーク不在を補うPoC



3. ポリシー整合

ベースモデル（Qwen）に
起因する社内の中国系モデ
ルポリシーとの整合審査

結論: 現時点では管理機能等が未成熟な初期版であるため、PoC起点の段階導入が合理的。

知財部門における生成AIの「構造的パラドックス」

極めて機密性の高いテキスト
処理が知財業務の中核

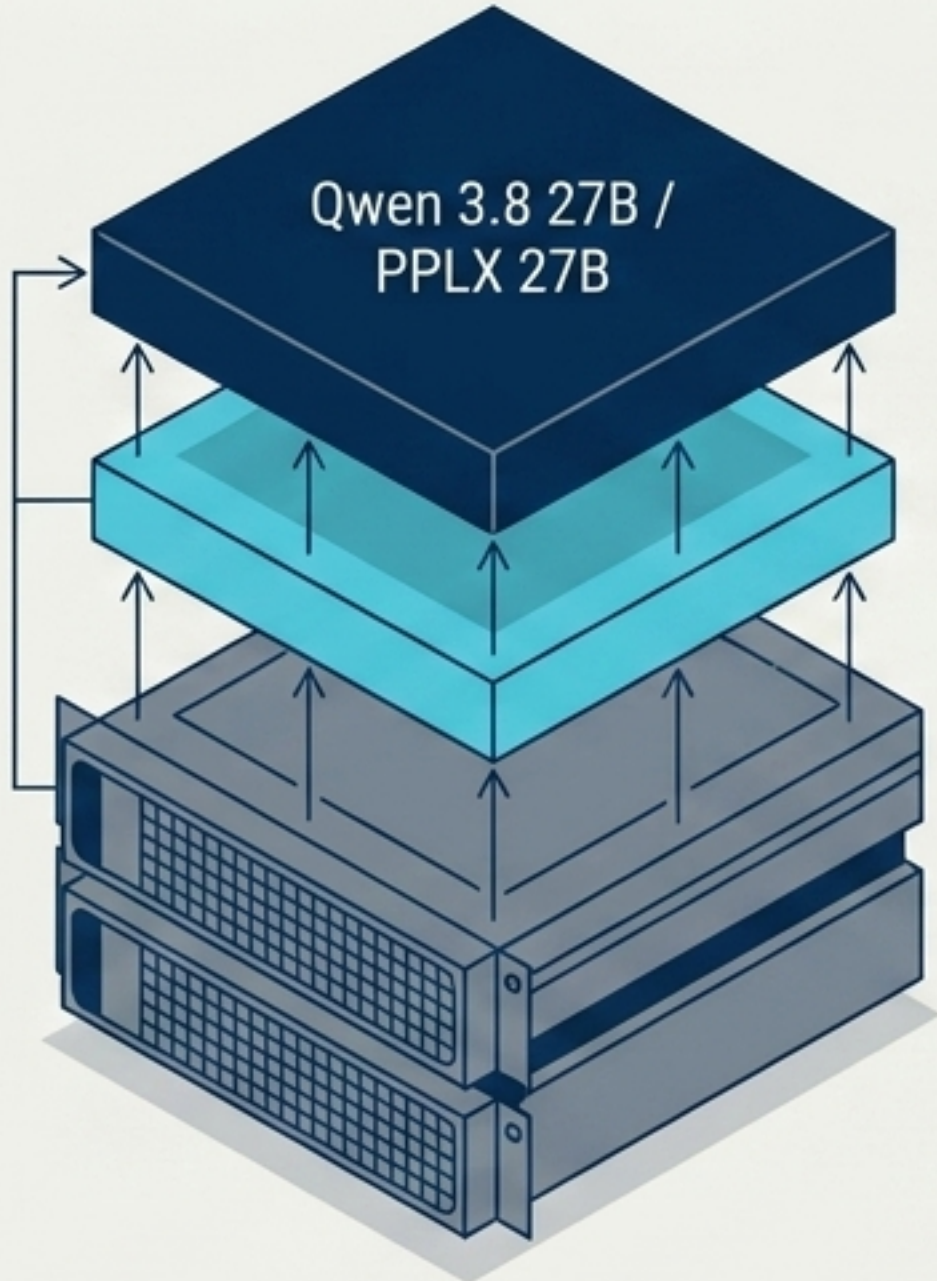
出願前発明、営業秘密、未公開特
許、NDA対象文書など

既存の高性能クラウドLLM
は、これらの重要データに
適用できない

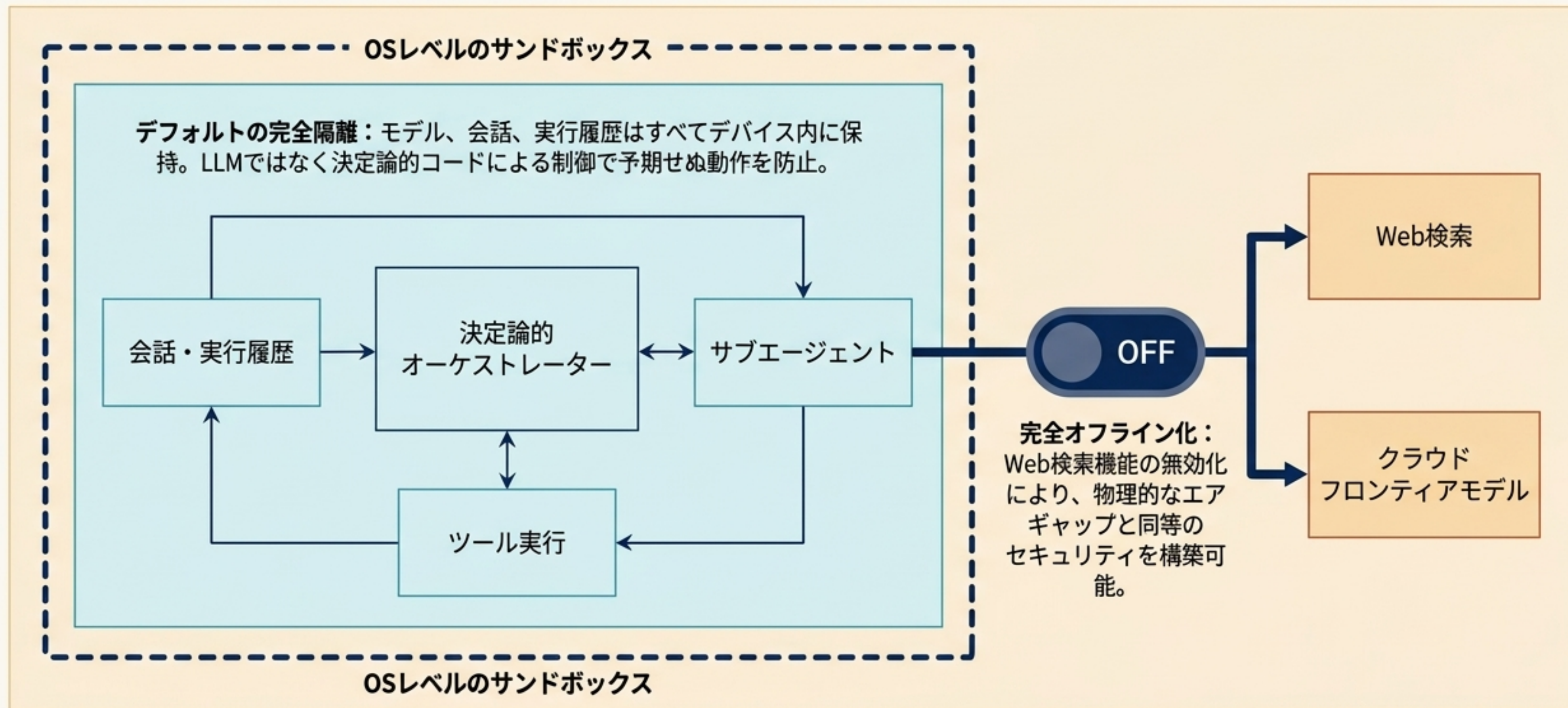
法的・セキュリティリスクの壁
第三者（クラウド事業者）へのデータ
送信に伴う「新規性喪失リスク」およ
び「秘密管理性の喪失リスク」

パラダイムシフト：「Portable Computer」の全体像

Perplexityエージェント基盤の完全ローカル版（NVIDIA共同開発）。ランタイム全体がユーザー環境で動作。

 Qwen 3.8 27B / PPLX 27B Perplexity OS / Orchestrator NVIDIA DGX Spark / RTX GPU	<table><tr><td>対応モデル</td><td>Qwen 3.8 27B / PPLX 27B (NVIDIA Nemotron 3.5 Lightning 近日追加予定)</td></tr><tr><td>対応ハードウェア</td><td>NVIDIA DGX Spark (128GBメモリ) または RTX GPU搭載機 (VRAM 24GB以上)</td></tr><tr><td>対応OS</td><td>現状 Linux (DGX OS/Ubuntu) のみ。 ※Windowsは2026年9月対応予定</td></tr><tr><td>コスト構造</td><td>ローカル処理はトークン消費ゼロ (クラウド処理のみクレジット消費)</td></tr></table>	対応モデル	Qwen 3.8 27B / PPLX 27B (NVIDIA Nemotron 3.5 Lightning 近日追加予定)	対応ハードウェア	NVIDIA DGX Spark (128GBメモリ) または RTX GPU搭載機 (VRAM 24GB以上)	対応OS	現状 Linux (DGX OS/Ubuntu) のみ。 ※Windowsは2026年9月対応予定	コスト構造	ローカル処理はトークン消費ゼロ (クラウド処理のみクレジット消費)
対応モデル	Qwen 3.8 27B / PPLX 27B (NVIDIA Nemotron 3.5 Lightning 近日追加予定)								
対応ハードウェア	NVIDIA DGX Spark (128GBメモリ) または RTX GPU搭載機 (VRAM 24GB以上)								
対応OS	現状 Linux (DGX OS/Ubuntu) のみ。 ※Windowsは2026年9月対応予定								
コスト構造	ローカル処理はトークン消費ゼロ (クラウド処理のみクレジット消費)								

アーキテクチャの優位性：OSレベルの「セキュア・サンドボックス」

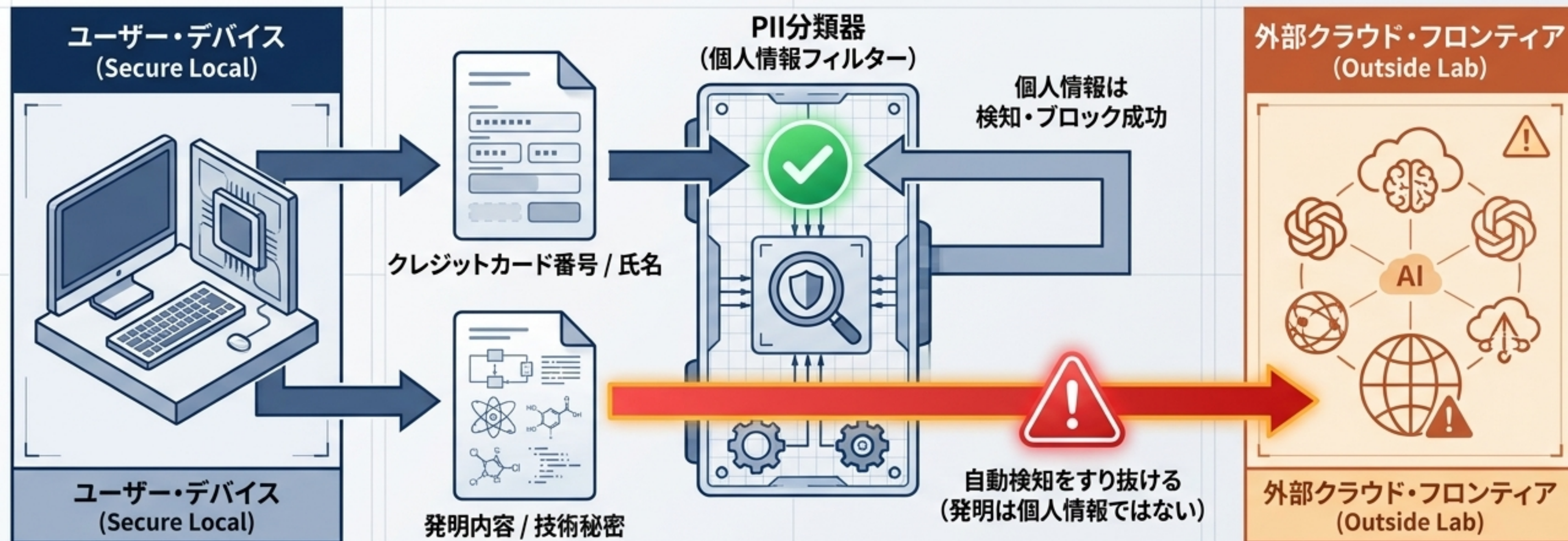


法的・ガバナンス基準との適合性比較

	従来のクラウドAI	Portable Computer (ローカル)
弁理士会 ガイドライン (2025年4月)	外部事業者への入力は「第三者への開示」。守秘義務違反・新規性喪失のリスク。 	【根本解消】 デバイス内で完結するため、構造的に「第三者への開示」が発生しない。 
経産省 営業秘密管理指針 (令和7年3月改訂)	外部AI提供事業者での学習利用により「秘密管理性」が否定される恐れ。 	【根本解消】 自社の「管理単位内」での利用として整理可能。アクセス制御・ログ整備により秘密管理性を維持。 

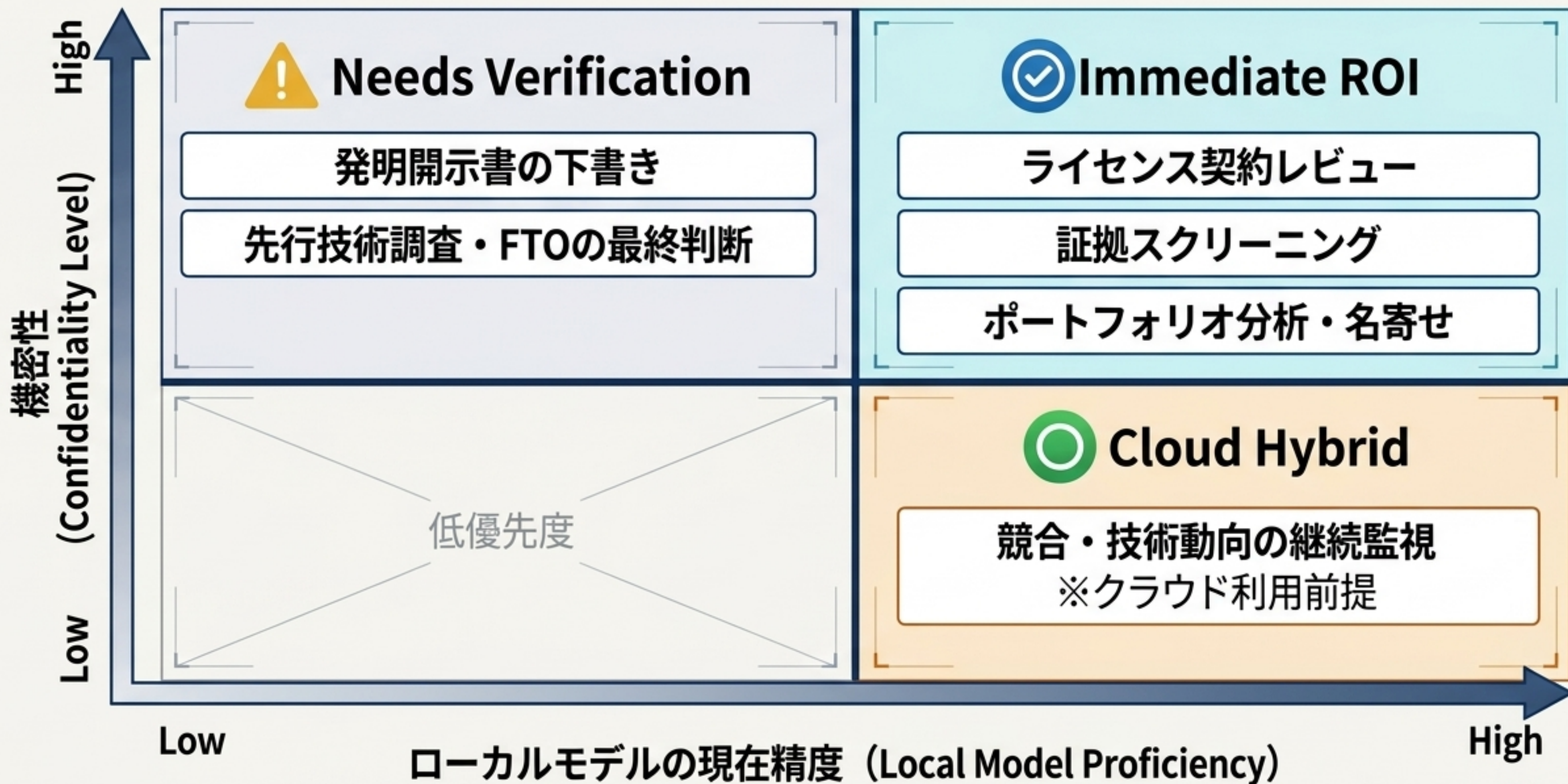
境界線のリスク：クラウドエスケーレーション機能の落とし穴

15種以上のフロンティアモデル（クラウド）への相談・Web検索へのエスケーレーション機能における注意点



対策：システム（自動検知）に依存せず、技術秘密の送出を防止する社内運用ルールと「手動の承認ワークフロー」の確立が不可欠。

知財業務別 適性・導入優先度ダッシュボード



Immediate Wins (🎯) : 導入効果が最も高い領域

契約・コンプライアンス領域



NDA下の機密文書、未公開特許文書をセキュアに処理。ベンチマーク (Contracts, evidence) でも極めて高い適性を示す。外部流出リスクゼロでの高度な分析が可能。

ポートフォリオのバッチ処理 (分類・名寄せ)



トークン非消費の強み:
大量の特許ポートフォリオデータのクレンジングや記録照合において、API課金コストを気にせず無限にバッチ処理が可能。
「Data, finance, procurement」タスクで絶大な費用対効果を発揮。

要検証領域 (○ / △)：初期版特有のボトルネック



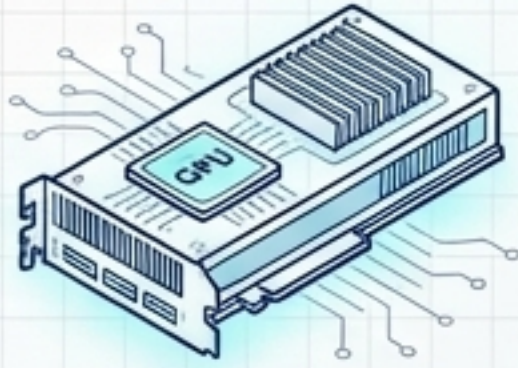
Issue 1: 日本語特許特有の文言理解 (○)

請求項の独特な表現や明細書の記述作法に対する PPLX 27B の精度は未知数。(先行事例：コニカミノルタの Azure OpenAI 基盤自社アプリ等との性能比較が PoC で必須)

Issue 2: 公報・図面の構造解析能力 (△)

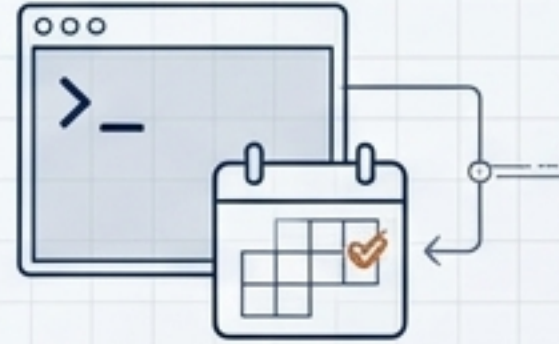
文書理解 (ParseBench-100) において、文字認識は堅調だが、レイアウト理解 (16.2%) が極めて弱い。複雑な段組や図面参照符号の構造理解には現状適さない可能性が高い。

ITインフラ・運用における3つの障壁



ハードウェア要件とコスト

DGX Sparkは国内約70万～110万円。RTX搭載機でも24GB超のVRAMが必須であり、既存の一般業務PCの転用はほぼ不可能。



Windows対応の遅れ

現状Linuxのみ。知財部門の標準環境（Windows/Office）への本格展開は、2026年9月予定のWindows版リリースを待つ必要がある。

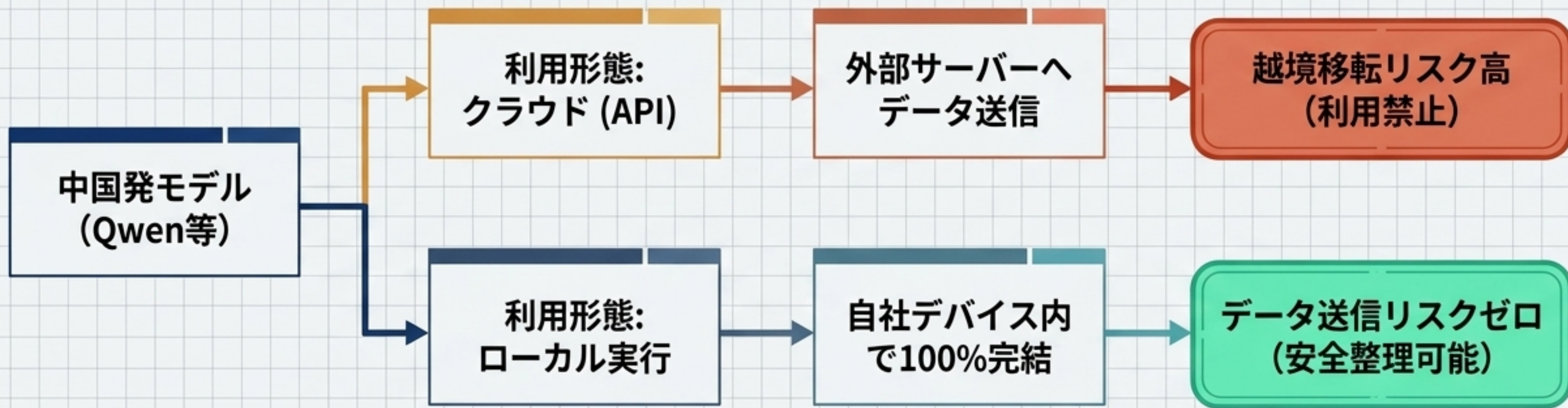


管理機能 (ITガバナンス) の欠如

SSO、管理者コンソール、監査ログ機能が未実装。営業秘密の「秘密管理性」立証に必要なアクセスログ等は自社で手動構築が必要。

ポリシーのジレンマ解消：「中国系モデル」規制への対応

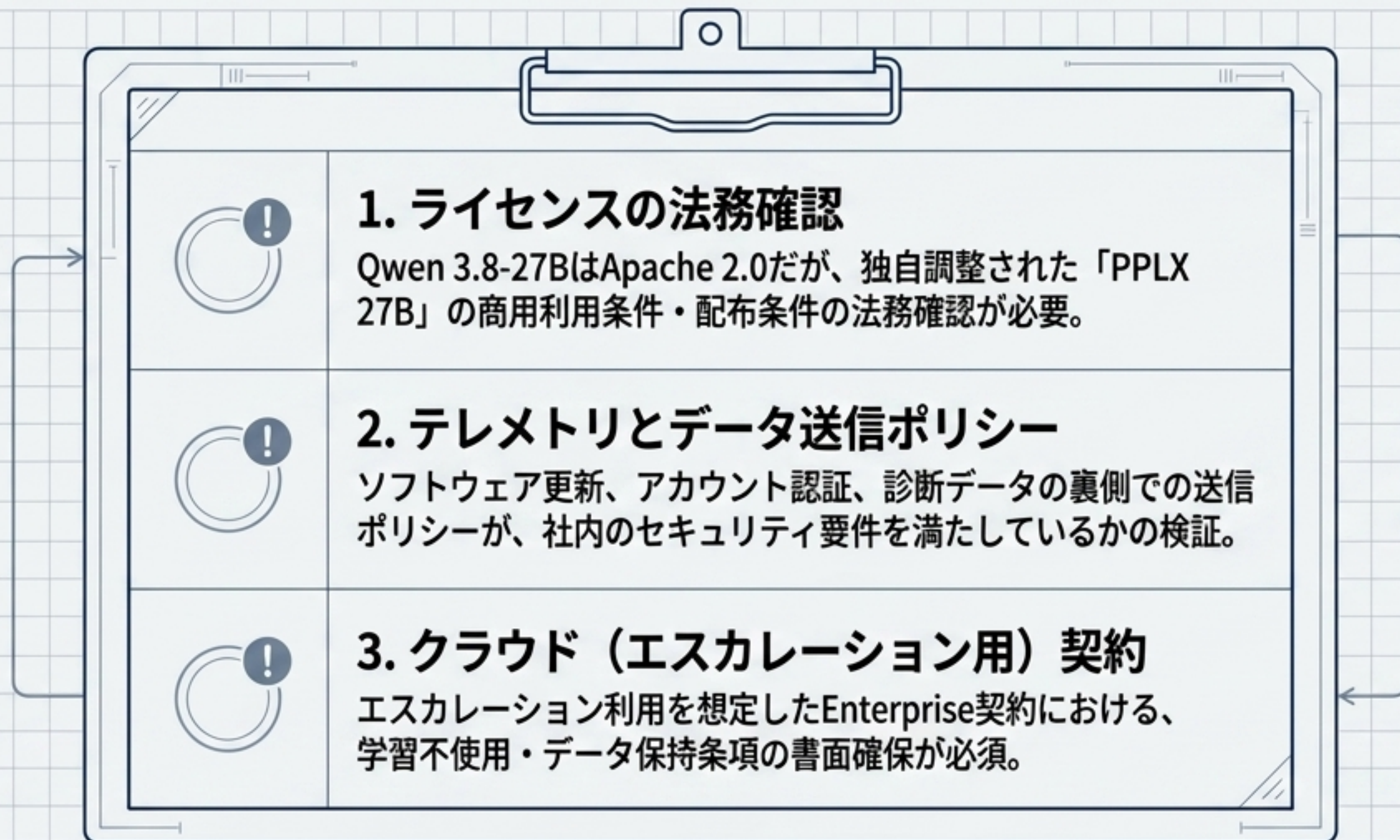
トヨタ・ソフトバンク等でのDeepSeek業務利用禁止事例により、「Qwen」ベースであることへの社内懸念が予想される。



The Argument: 政府・企業の主たる懸念は「外国サーバーへのデータ送信」。オープンウェイトモデルの完全ローカル実行は、構造的にデータ送信リスクを排除できるため、別枠での安全整理が可能（※みずほ、ライオン等でのQwen採用実績あり）。

ベンダーロックインと商用ライセンスの確認事項

純粋なOSS運用ではなく、Perplexityの有料サブスクリプションと専用ソフトウェアに依存する「ベンダー管理型ローカル」である点に注意。



リスクを最小化する3段階の導入シナリオ

Windows版リリース
(2026年9月予定)



Phase 1: PoC (0~3か月)

- DGX Spark 1台導入
- 公開情報処理（競合監視）に限定
- 最重要課題：日本語特許文書の精度ベンチマーク構築

Phase 2: 限定機密業務（3~6か月）

- Web検索を無効化（エアギャップ運用）
- NDA契約レビュー、大量バッチ処理（ポートフォリオ棚卸し）を開始
- 操作ログの自社運用ルールの確立

Phase 3: 部門展開（6か月～）

- 【Windows対応・管理機能実装後】
- クラウドエスケーレーションの厳密な社内規程を整備した上で、知財部門全体へスケール

ステークホルダー向け Go/No-Go 最終判断チェックリスト

- ☐ 1. 社内AIポリシーにおいて、中国発オープンウェイトモデルのローカル実行を許容できるか？
- ☐ 2. PPLX 27Bのライセンス条件および診断データの取り扱い規定は法務的に受容可能か？
- ☐ 3. エスカレーション利用に備え、学習不使用・データ保持を担保するEnterprise契約を締結できるか？
- ☐ 4. 「クラウドへ送信してはいけない情報」の基準とエスカレーション承認ワークフローを社内規程化できるか？
- ☐ 5. 「秘密管理性」を法的に立証するためのアクセス制御とログ取得を、自社運用でカバーできるか？
- ☐ 6. 日本語特許文書（明細書・請求項）に対するPoCの合否判定ライン（精度基準）が定義されているか？