

Perplexity「Portable Computer」検証ドシエ

汎用ローカルAIの過大評価に対する技術的制約・法的リスクと日本企業への実装要件

DATE: 2026.08.30



世間の認識 (Myth)

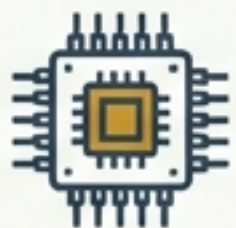
「一般のPCで動く画期的な汎用ローカルAIエージェントが、完全無料でリリースされた。」



冷徹な現実 (Reality)

「**NVIDIAの専用高額ハードウェア**（DGX Spark等）を前提とした、検証フェーズの**限定的製品**である。」

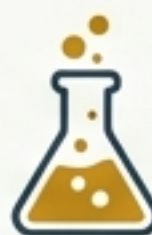
Key Findings



1台数千ドルのハードウェア投資が必須要件（一般的なノートPCは不可）。

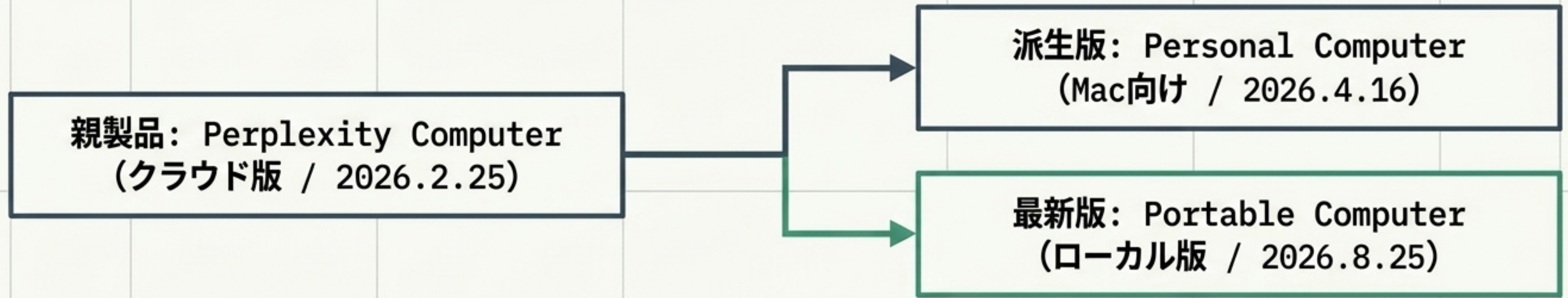


ローカル処理分は**無料**だが、真価を発揮するクラウドモデルへのエスカレーションは「**従量課金**」。

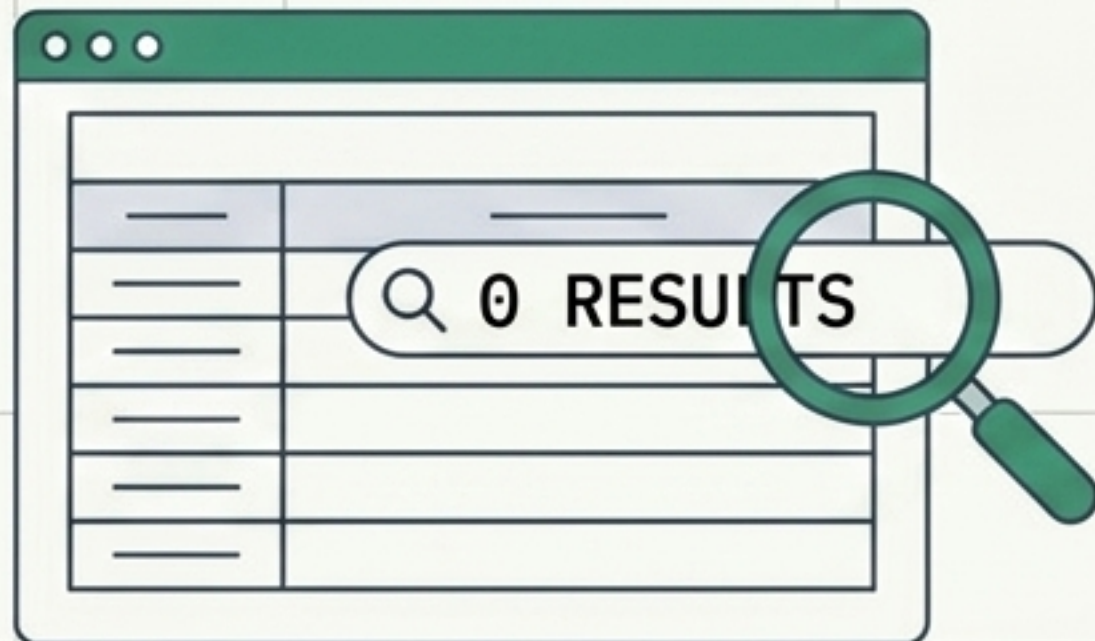


現時点では**全社導入のフェーズ**になく、**限定的な「1台のPoC評価」**に留めるべき。

製品の系譜 (Lineage)



「一般名称」採用の裏事情



- 「Portable Computer」という名称について、米国商標出願の形跡はない（2026年8月時点）。
- 過去に雑誌名「PORTABLE COMPUTER」等が識別力欠如（総称的）として扱われた判例と整合する。
- 代替策として、同社は2026年7月にスローガン「EVERYTHING IS COMPUTER」を商標出願し、ブランド保護の軸足を移している。

技術アーキテクチャ（フルスタック・オンデバイスの解剖）

クラウド・エスカレーション層（Cloud Layer）

- 15 以上のフロンティアモデル（※従量課金）
- アドバイザーモデル（テキスト助言のみ・直接アクセス不可）

防御ゲート



PII分類器による事前チェック
& ユーザー承認の強制

OSレベルサンドボックス内でコード実行

ローカル実行層（Local Layer）

LLM: Qwen 3.8 27B
/ PPLX 27B

音声認識: NVIDIA
Nemotron 3.5 ASR

エンジン: vLLM推論,
エージェントハーネス,
ツールルーター

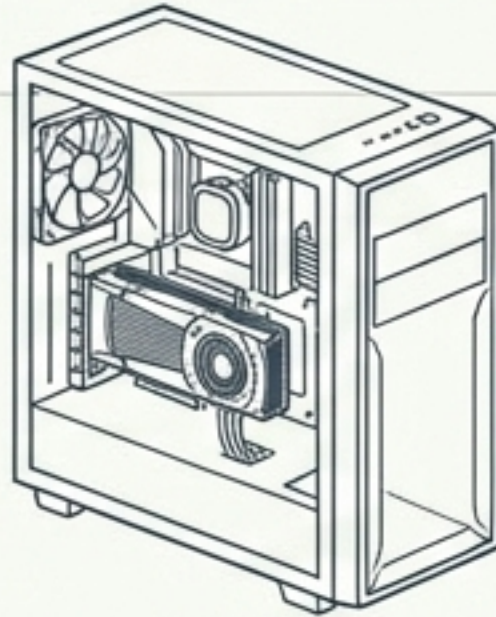
ハードウェア要件と導入障壁（コスト分析）

一般的なノートPC (Windows / Mac)



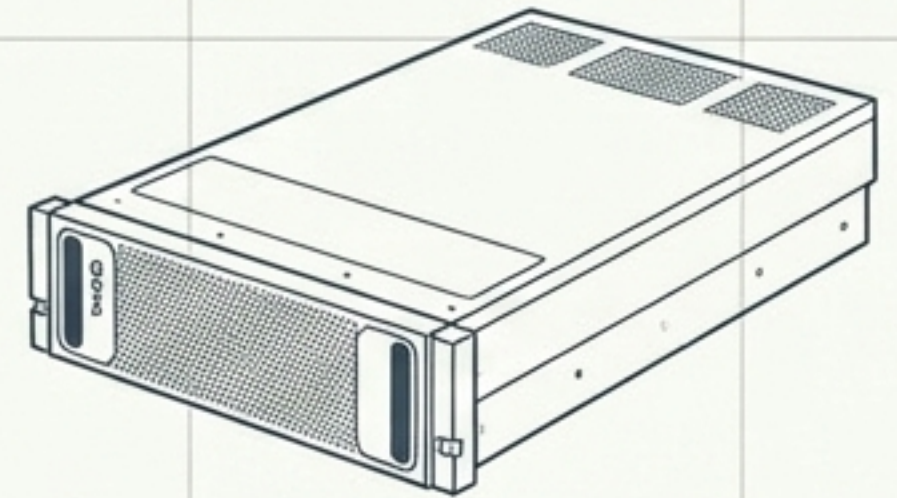
現状未対応。Windows対応は
2026年9月予定、Apple
Siliconはロードマップ上未定。

ハイエンドLinux機 (Ubuntu / DGX OS)



VRAM 24GB以上のNVIDIA
RTX GPUが必須。旧型RTX
3090でも単体で\$1,500超の
追加投資が必要。

NVIDIA DGX Spark (推奨環境)



GB10 Grace Blackwell, 20コアArm CPU, 128GB統合メモリ。
初期コスト(MSRP): \$4,699
(約70万円強)。これが普及に向
けた最大の物理的障壁。

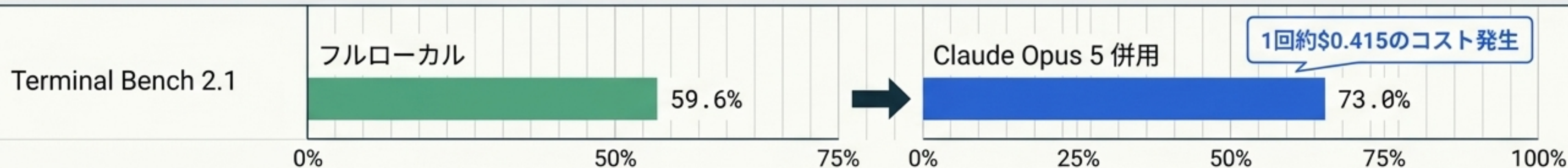
パフォーマンス評価（自社ベンチマークの読み解き）

⚠ 本データはすべてPerplexityの「自社公表値」であり、第三者検証は未了。

1. 知識作業・ブラウジング（健闘）



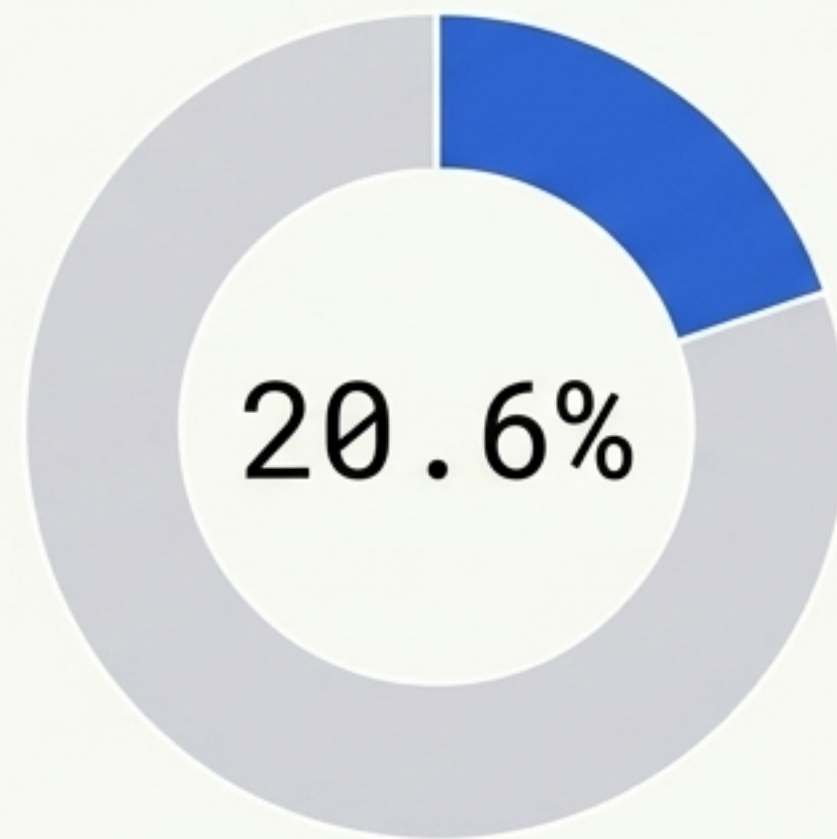
2. コーディング・複雑タスク（クラウド依存）



競合マトリクス（コンピュータ操作エージェントの現在地）

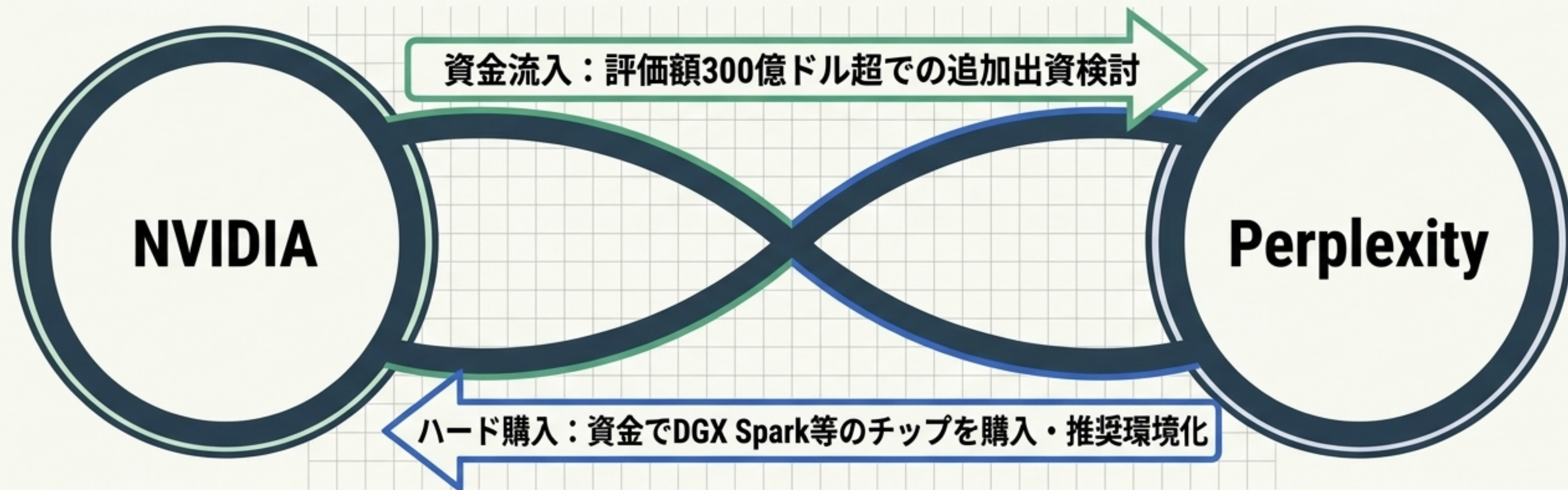
クラウド実行 (Cloud)	ブラウザ特化 (Browser)	Anthropic (Claude for Chrome) Google (Gemini Auto Browse)	OpenAI (ChatGPT Work) Microsoft (Copilot Cowork)
			Perplexity Portable Computer（唯一の切り口）
ローカル実行 (Local)	OS/アプリ横断 (OS-Wide)		

分野全体の未成熟さ



学術ベンチマーク「OSWorld 2.0」における最高性能の完全達成率はわずか20.6%。「完全オンデバイス」は革新的だが、エージェント技術自体が未完成な実験段階である。

NVIDIAとの「循環型」エコシステム (The Circular Dependency)



ビジネスインパクト

Perplexityの年換算売上は約2.5億ドルから7.5億ドル超へ急拡大。Jensen Huang CEO自身がPerplexityを常用。

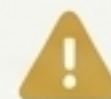
強固な成長エンジンである一方、「特定ハードウェアへのロックイン」という批判的視点も存在する。

セキュリティ・アーキテクチャと残存リスク

過去の教訓：2025年、Cometブラウザにて間接プロンプトインジェクション等の脆弱性が実証され、機微データ窃取リスクが露呈。



プロンプトインジェクション / CometJacking



残存する本質的リスク：
防御壁は構築されたが、エージェントが「シェルコマンド実行権限」を持つ以上、突破リスクはゼロにならない。

リーガル・バトルマップ（著作権・利用規約係争）

Cloudflare (2025.08)

争点：robots.txtを無視したステルススクロール。検証済みボット一覧から削除措置。

Amazon (2025.11 提訴)

争点：エージェント経由の無断購買（CFAA違反）。

⚠ ステータス：第9巡回控訴裁が「ユーザーの指示で動くエージェントはユーザー自身である」として差止を取消。法理確定の途上。

New York Times / Chicago Tribune (2025.12 提訴)

争点：無断学習・アクセスに伴う著作権および商標侵害。



知財（IP）戦略の空白地帯

商標（Trademark）の空白



「COMET」等で出願拒絶の過去あり。

「Portable Computer」は出願自体が存在しない（一般名詞化による識別力の欠如の推認）。

特許（Patent）の不在



Perplexity自身に帰属するAIエージェント、ローカル推論の登録特許・公開出願は**ゼロ**。

類似特許（Agentic orchestration等）は、他社RPAベンダーが先行して仮出願済み。



企業への警鐘: 自社でエージェントを組む際は、Perplexityではなく**サードパーティ**に対する**FTO（実施の自由）調査**が不可欠。

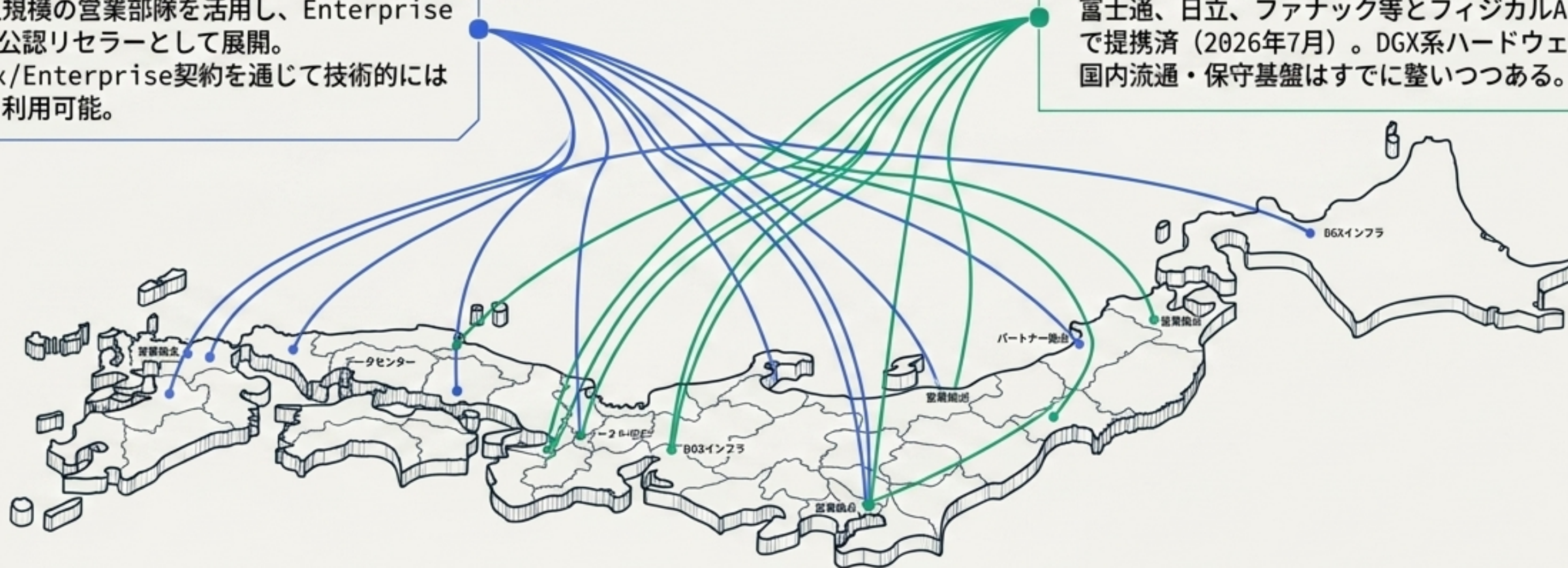
日本市場での展開とエコシステム

SoftBankによるエンタープライズ再販網

7,000人規模の営業部隊を活用し、Enterprise Proの初公認リセラーとして展開。
Pro/Max/Enterprise契約を通じて技術的には日本でも利用可能。

NVIDIAの国内インフラ基盤構築

富士通、日立、ファナック等とフィジカルAI分野で提携済（2026年7月）。DGX系ハードウェアの国内流通・保守基盤はすでに整いつつある。



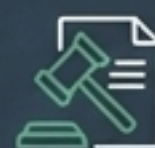
導入に向けた外堀（営業網・インフラ保守）はすでに埋まりつつある現状。

企業内部門別アクション・マトリクス



IT / セキュリティ部門

- ☐ OSレベルのサンドボックス設定と有効性検証
- ☐ クラウドエスカレーション時の承認フロー確立
- ☐ Enterprise契約における「学習からの除外（オプトアウト）」の確認



知財 / 法務部門

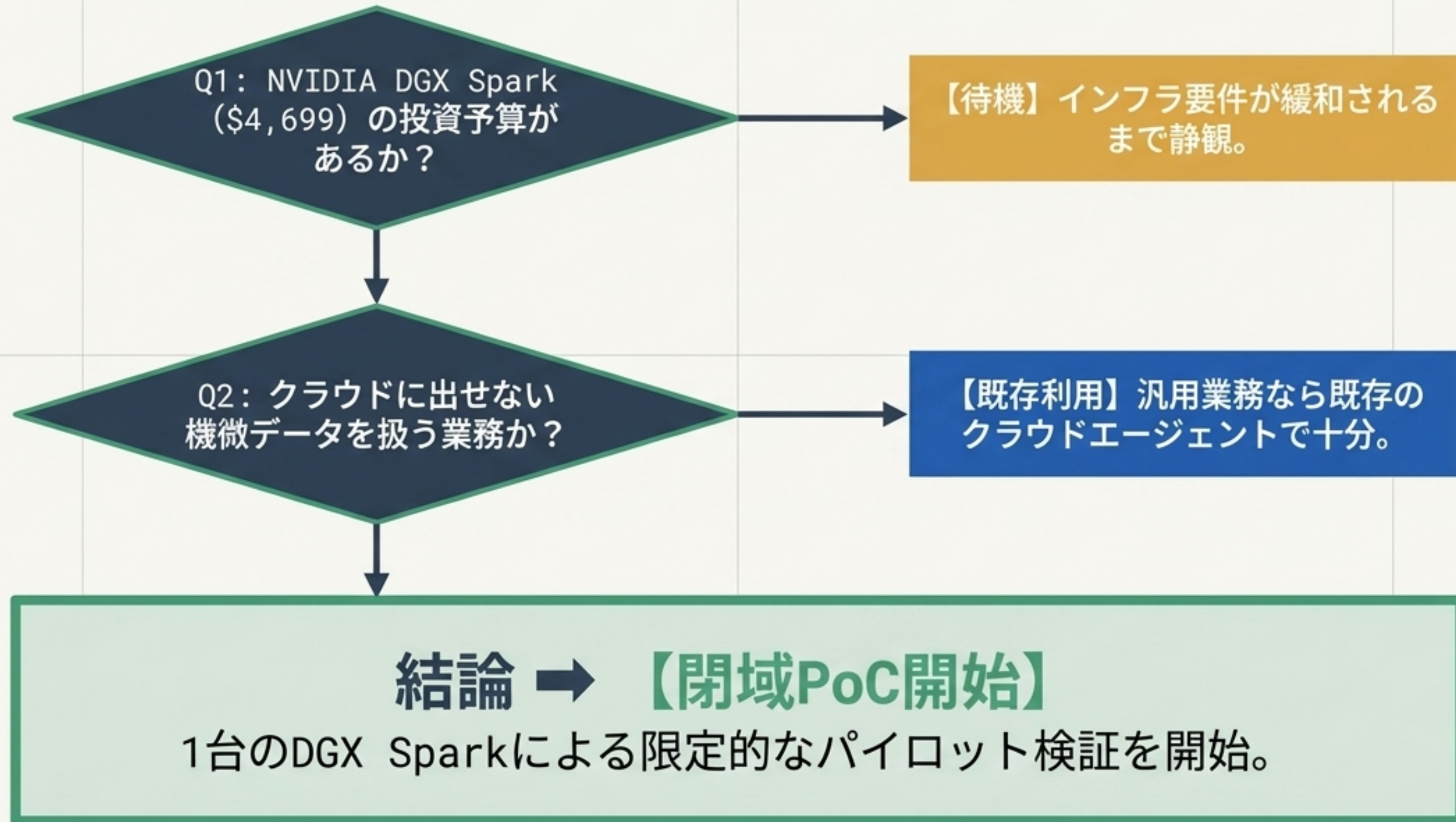
- ☐ 自社実装時のFTO（特許実施の自由）調査
- ☐ 外部サイトの利用規約（robots.txt等）への抵触リスク評価



事業 / 戦略部門

- ☐ ROI算出（DGX投資・従量課金 vs 業務効率化リターン）
- ☐ 金融・医療等、閉域環境が必須な機微ユースケースの選定

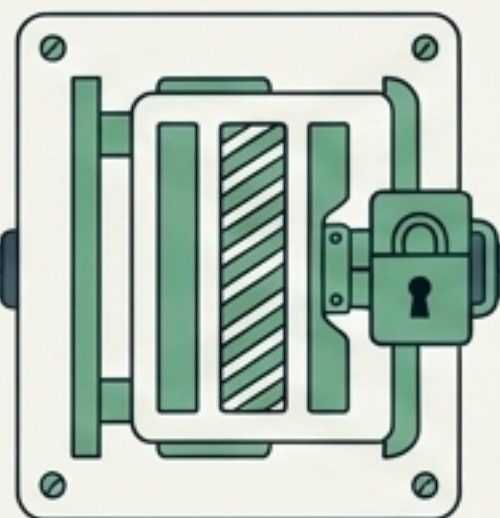
最終判定フロー（今すぐ導入すべきか？）



今はまだ「実験室のエンジン」。全社導入の機が熟すのは、これら3つのゲートが開いた時である。

ロードマップ：判断を変える「3つの閾値」

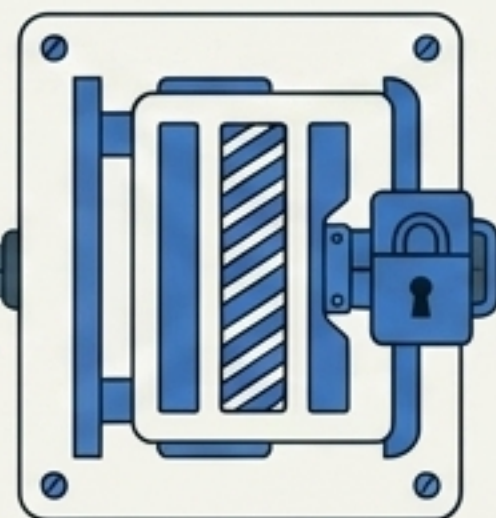
インフラの民主化



2026年9月予定のWindows対応、およびApple Silicon対応による高額ハードウェア要件の緩和。

GATE 1: HARDWARE/OS

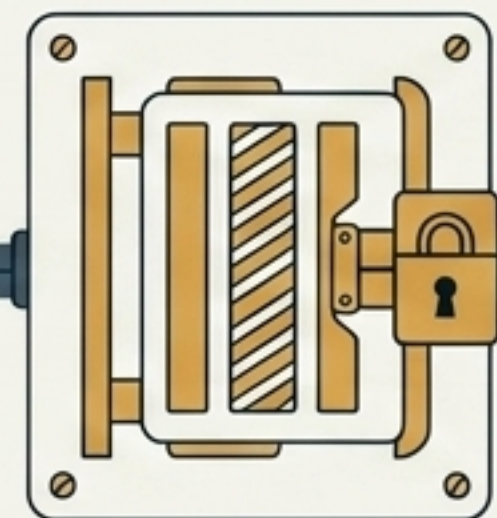
第三者検証の登場



自社公表値ではない、独立機関による客観的ベンチマークとセキュリティ監査の完了。

GATE 2: VALIDATION/AUDIT

法的判例の確定



AmazonやNYTとの訴訟により、「エージェントの挙動＝ユーザーの法的責任」という法理が確定すること。

GATE 3: LEGAL/LIABILITY