Local-First / Hybrid Pipeline

Enterprise Readiness Assessment

September 2026

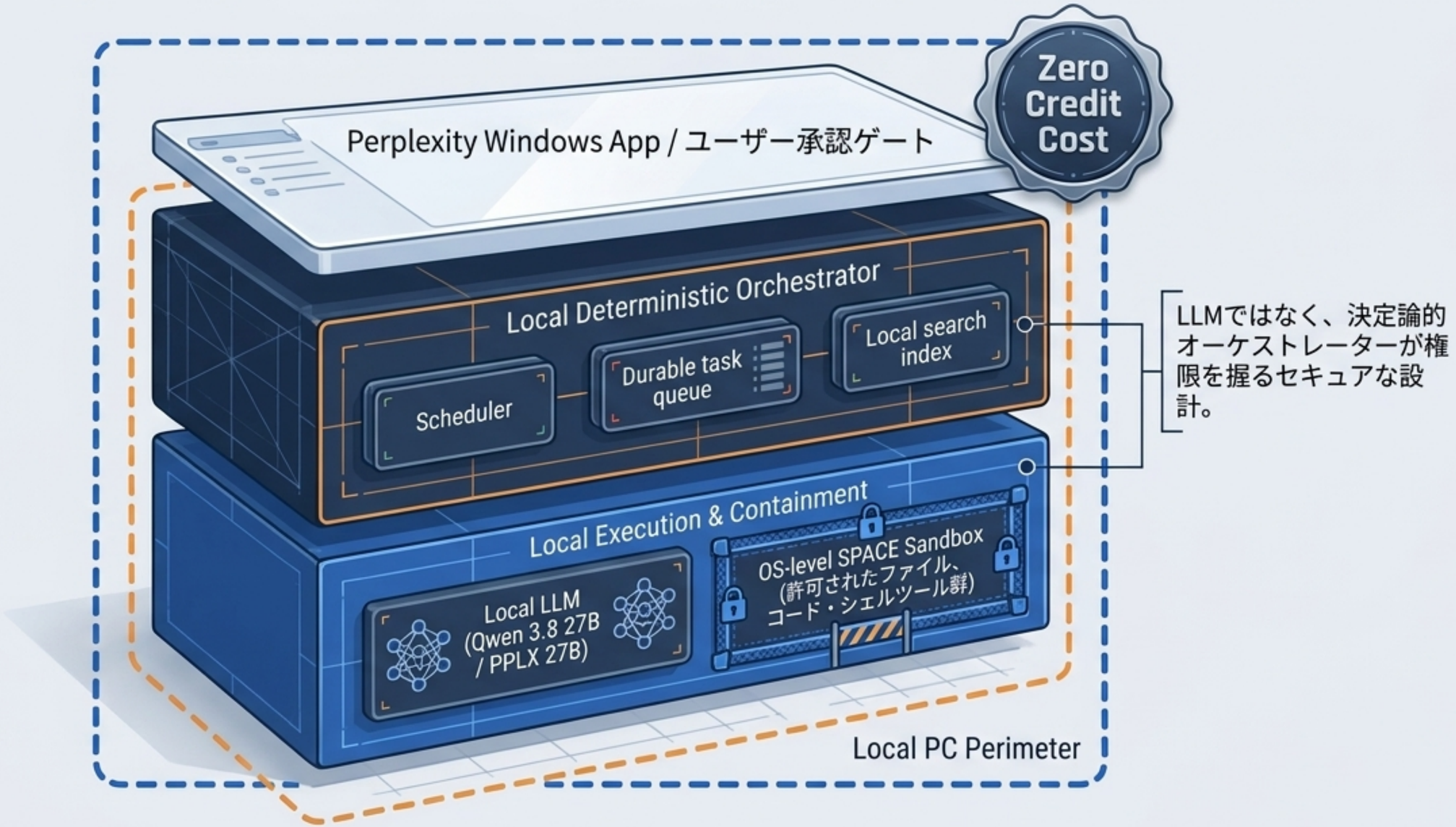
Perplexity Portable Computer 徹底解剖

ローカルAIエージェントの実態、セキュリティ要件、ライセンスリスク、本番導入へのロードマップを完全解明。

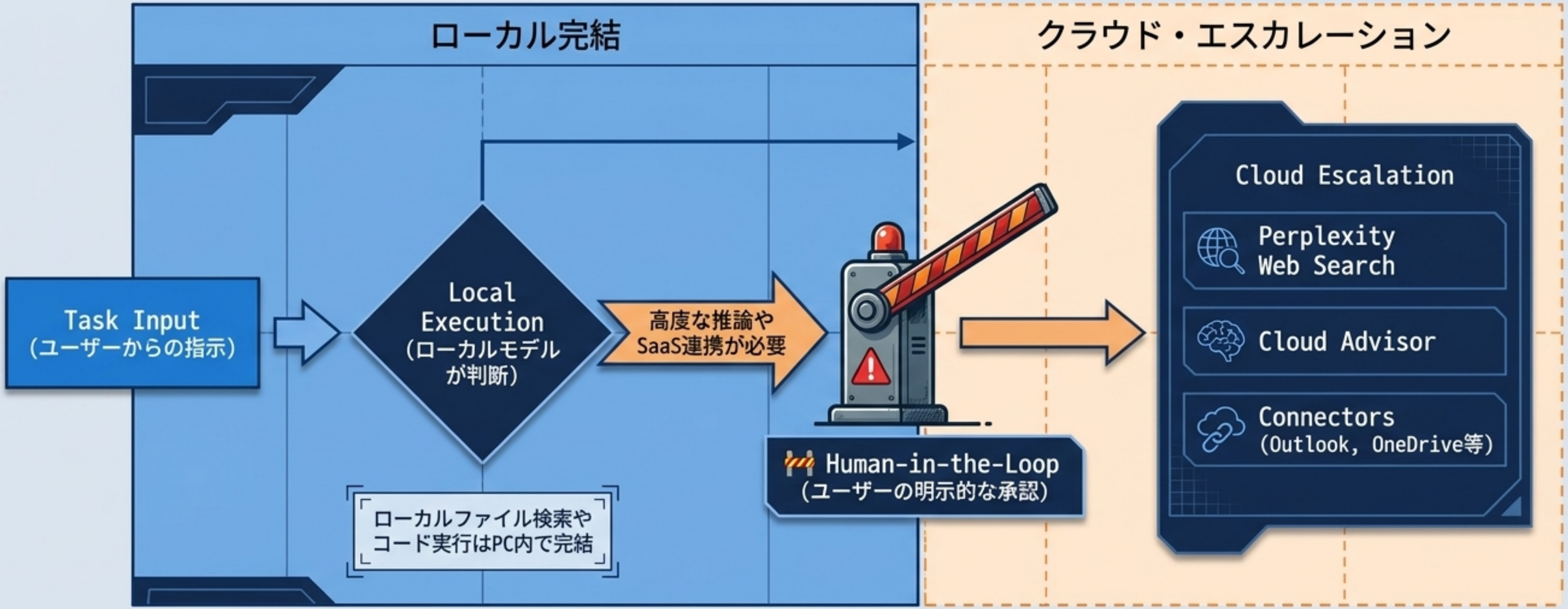
Local-First / Hybrid Pipeline

強力なローカル完結能力と未公開仕様が混在する初期リリース

ローカルAIの定義を拡張するエージェント・アーキテクチャ



デフォルトはローカル完結、難題のみクラウドへ委譲するハイブリッド経路



⚠ アーキテクチャの要：Cloud Advisorはファイル権限を直接持たず、ローカルオーケストレーターから送られたコンテキストに対して「テキストの助言」のみを返す安全な分離構造。

24GB VRAMの壁と、運用を阻む「見えない仕様」

The Knowns (決定事項)

NVIDIA RTX / RTX PRO

24GB+ VRAM

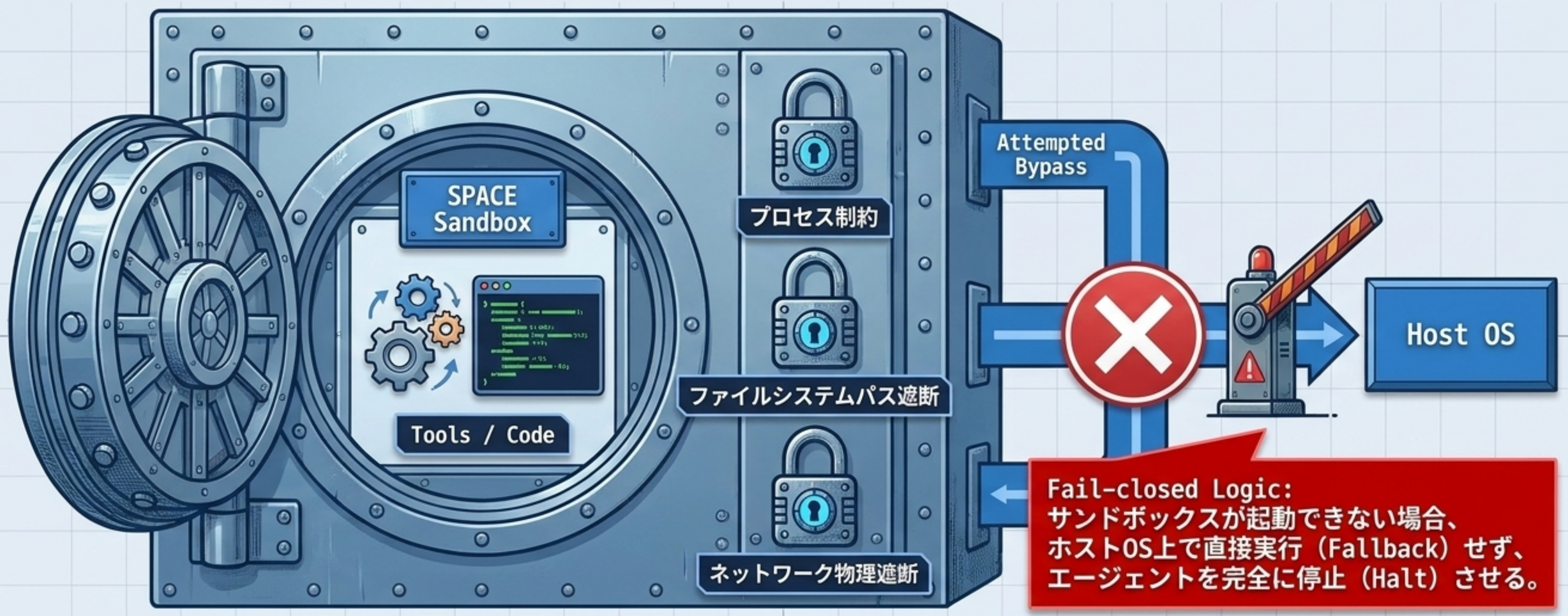
```
PS C:\> Get-WmiObject Win32_VideoController | Select-Object Name,
    @{Name='VRAM (GB)'; Expression={($_.AdapterRAM / 1GB).
   .ToString('F2')}}

Name                VRAM (GB)
----                ---------
NVIDIA RTX A6000        48.00
```

The Unknowns (ブラックボックス)

?	CPU最低要件
?	システムRAM
?	SSD空き容量
?	最低Windowsビルド
?	モデル保存パス
?	llama.cpp / CUDAの正確なバージョン
?	公開SBOM

依存関係や更新ポリシーが不明なため、標準PCイメージの設計や脆弱性管理（LTS）が極めて困難。

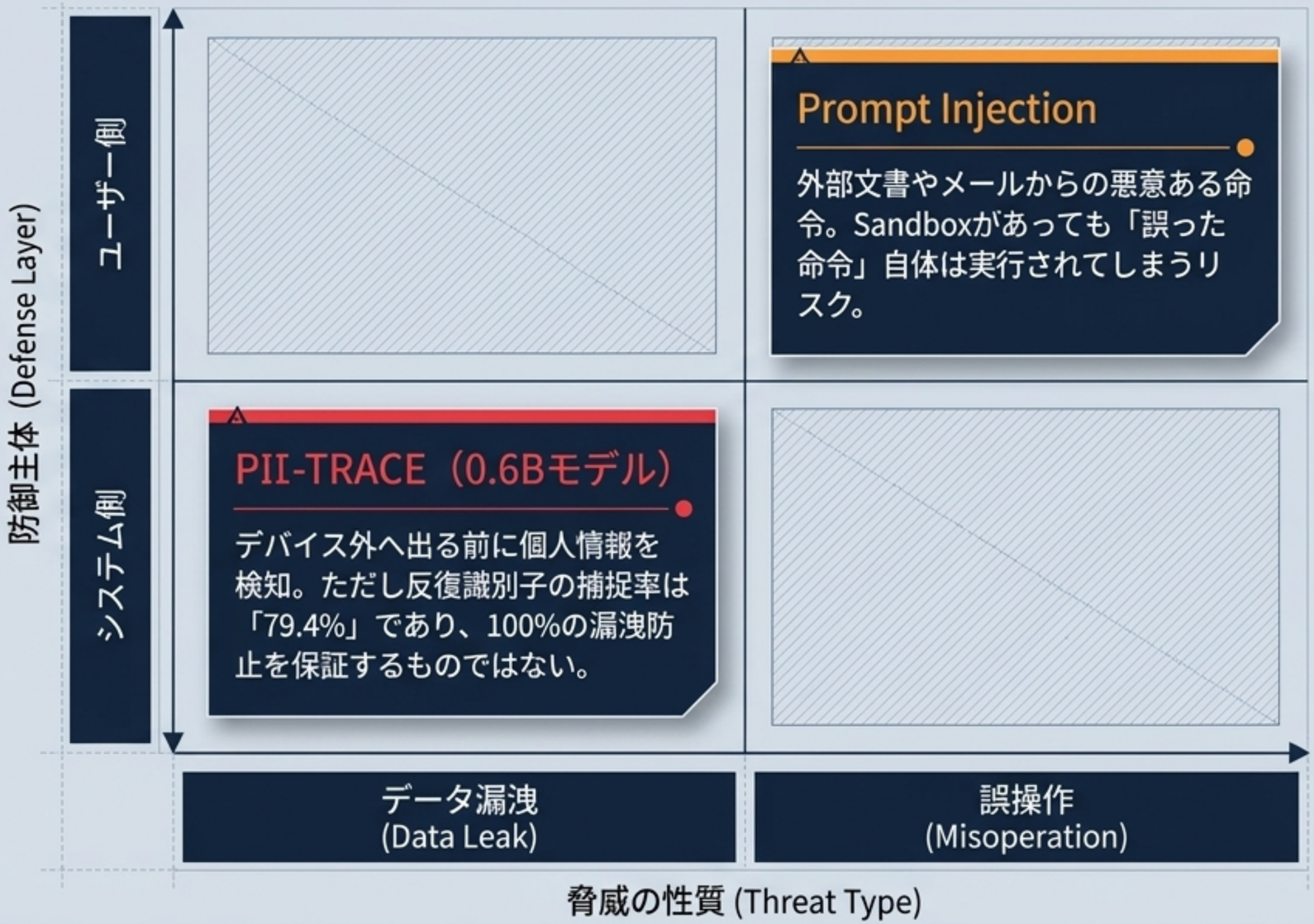
競合OSSを凌駕する強制的サンドボックスとFail-closed設計



比較：OpenClaw等のOSSはデフォルトでホスト実行（Sandbox設定は任意）であるのに対し、
Perplexityは「常時有効・設定不要」であり企業向けとして極めて優秀。

Editorial Mission Control

DLP技術の限界と、規約が突きつける「監督責任」



Enterprise Agentic Specific Terms（規約抜粋）

「AIが間違った操作をするリスクはSandboxでは消せない。アクセス権管理とアクションの承認・監督はユーザー（顧客）の責任である。」

個人版の業務利用は法務リスク。本番導入はEnterpriseプラン一択

個人向け Pro / Max

$20~$200/月

⚠ **ステータス:** 業務利用不可

⚠ **規約:** 「個人の非営利目的に限定」「営利目的での悪用禁止」

⚠ **データ保護:** 第三者LLM利用時の入力データ保護の明示的な確約なし。

Enterprise Pro / Max

$40~$325/月

✓ **ステータス:** 本番導入推奨

✓ **規約:** 「顧客の事業目的のための利用を明示的に許可」

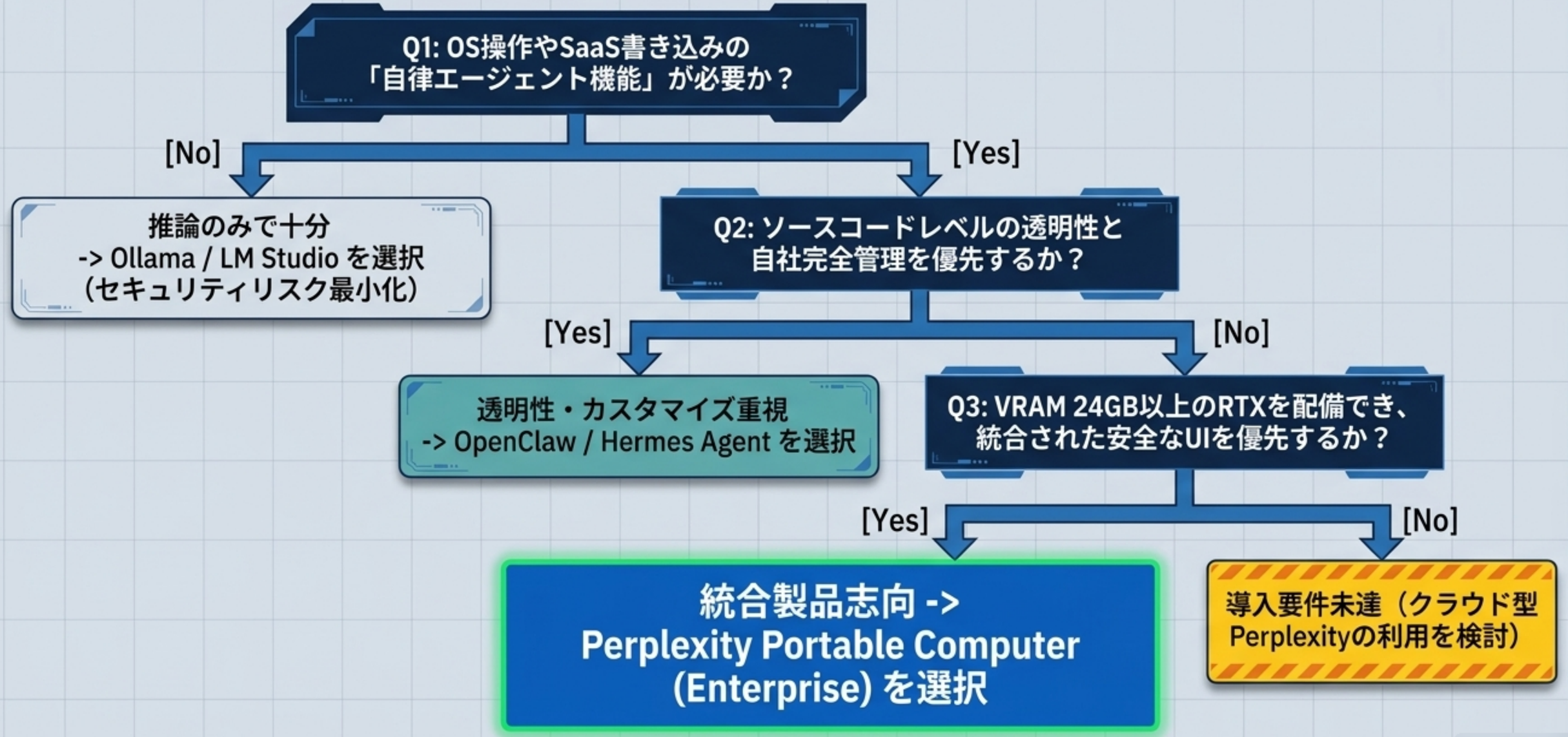
✓ **データ保護:** SOC 2 Type II準拠。エンタープライズデータをモデル学習から完全に除外（Training Exclusion）。

ローカルAIエージェント製品 比較マトリックス

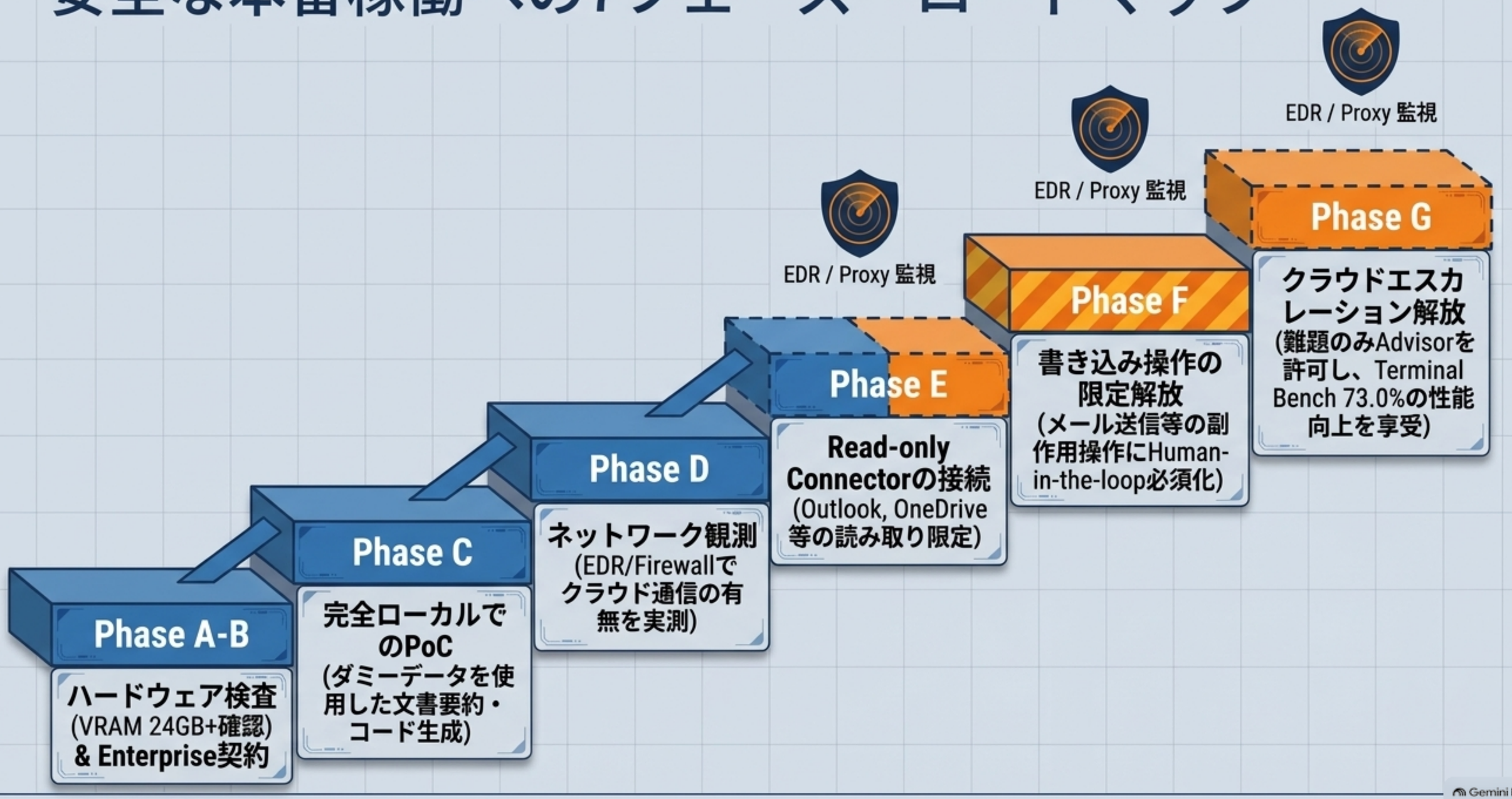
製品形態	自律エージェント機能	Sandboxの強制力	UI / CLI	価格と運用
Perplexity Portable Computer	○	強制 / Fail-closed	Windows GUI	$20/月～ (Enterprise必須)
Hermes Agent (Nous Research)	○	任意設定	Terminal / Desktop	無料OSS (カスタマイズ要)
OpenClaw	○	なし / Host実行	TUI / UI / CLI	本体無料 (攻撃面広い)
LM Studio Bionic	推論中心	製品による	GUI中心	無料から
Ollama	なし (ランタイムのみ)	Agent側に依存	CLI / API	無料

結論：統合UIと強制的Sandboxによる「セキュア・デフォルト」はPerplexityの圧倒的強みだが、透明性（OSS）では劣る。

組織のニーズ別・最適アプローチの選択



安全な本番稼働への7フェーズ・ロードマップ



ガバナンス・アズ・コード：組織が監査すべきポリシー要件

シャドーIT防止:
個人版の業務利用をシステム的に禁止。

```yaml
# portable-computer-governance.yaml
policy_name: "Enterprise Baseline"
deployment_tier: enterprise
compliance:
  web_search: deny_by_default
  local_access:
    deny_roots:
      - /etc/passwd
      - ~/.ssh
  data_egress:
    github:
      write_requires_human_approval: true
```

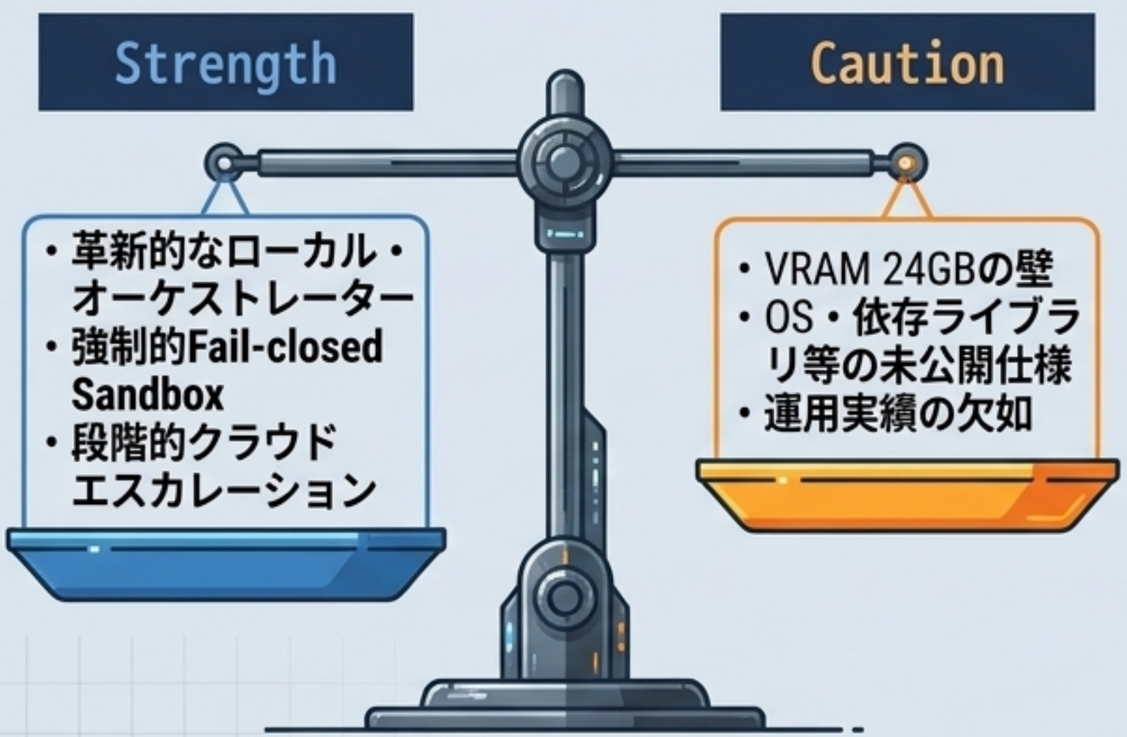
デフォルト遮断:
クラウド送信を初期状態で遮断し、明示的な承認を要求。

物理的アクセス禁止:
SSHキーやクレデンシャル等、機密フォルダへのアクセスをOSレベルで遮断。

Human-in-the-loop:
GitHub等への書き込み操作に対し、必ず人間の承認を介在させる。

⚠ ※現時点ではUI設定のみだが、企業としてはこのレベルの宣言的ポリシー監査が実務上不可欠である。 ⚠

最終評価と本番導入前チェックリスト



結論: ローカルファースト基盤として極めて優秀だが、エンタープライズ運用仕様はまだ発展途上。

本番導入前チェックリスト

- ☐ 業務利用としてのEnterprise Pro/Max契約確認
- ☐ VRAM 24GB以上のNVIDIA RTX/RTX PRO端末の確保
- ☐ Prompt Injectionを前提とした外部入力の**Untrusted**扱いルール策定
- ☐ EDR/Firewallによるクラウド通信の事前観測
- ☐ Canary（少数グループ）から本番への段階的アップデート体制構築