

DeepSeek-V4.1-Flash-1017

戦略的調査報告

知財業務への破壊的インパクトと地政学リスク評価

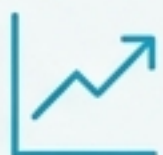
「圧倒的なコストパフォーマンス」と「データ保護の壁」をどう乗り越えるか。日本企業の知財部門が取るべき最適解を提示する。

Date: 2026年10月18日時点

Analysis Engine: Claude Opus 5.5 Intelligence

Target Audience: IP Strategy & IT Executives

Executive Summary: 最新モデル1017は「知財情報の一次処理」を劇的に変えるが、単独での業務完結は極めて危険である。



パラダイムシフト

破壊的低コスト & 高エージェント性能

オフピーク\$0.15/1M入力。コーディング等で Claude Opus 5を凌駕 (DeepSWE 77.0)。



品質の限界

論理推論と日本語の壁

高度な論理推論 (HLE) は上位モデルに劣後。
日本語の不自然さとハルシネーション傾向。



隠れた脅威

データ越境と地政学の板挟み

公式APIは中国法準拠。米国の排除動向と中国の重み輸出管理草案 (10/16) による不確実性。



推奨アクション

ローカル運用+マルチモデル

公式APIへの未公開発明の入力禁止。
オープンウェイト (MIT) のローカル運用と上位モデルとの分業体制の構築。

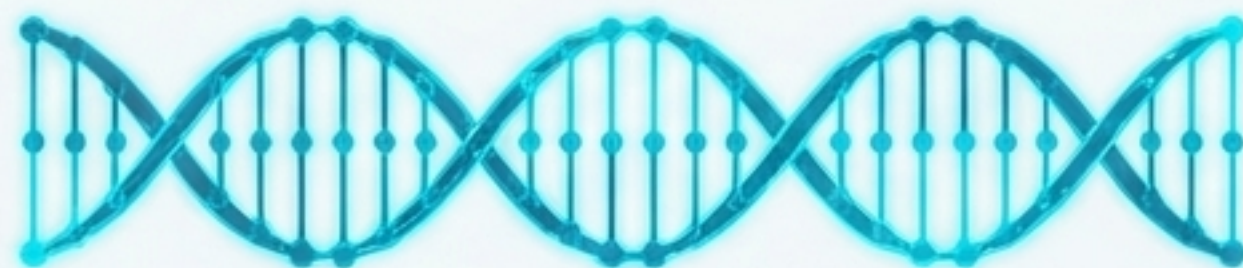
Key Takeaway: 「1017」は新モデルではなく、RLSFによってエージェント性能を極限まで研ぎ澄ませたV4.1-Flashの重み更新版である。

Model Identity: What exactly is 1017?

V4.1-Flash (Sep 10)

- ✓ **Architecture:**
Causal Encoder-Decoder
- ✓ **Context Window:**
100万トークン
- ✓ **License:**
MIT (商用利用可)
- ✓ **Price:** 変更なし

RLSF (自己フィードバック強化学習)

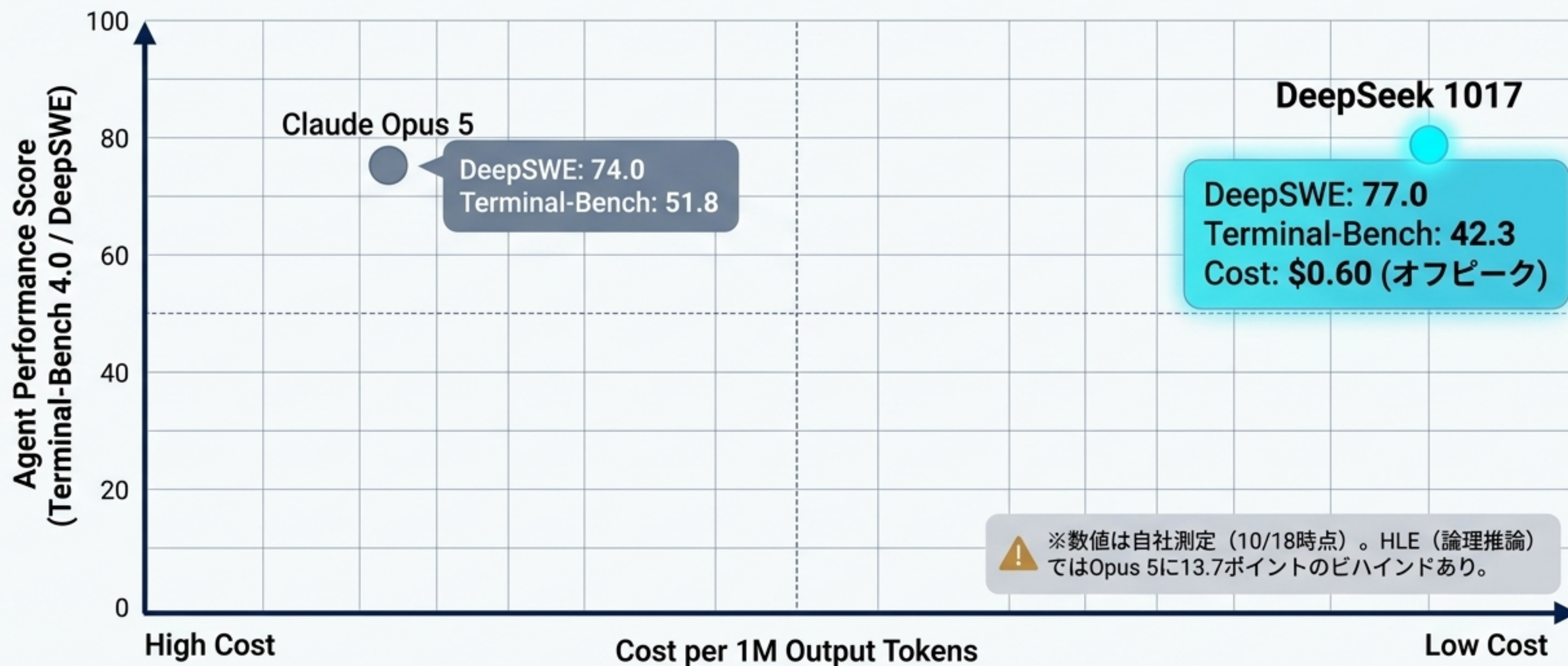


モデル自身の確信度・批評を
報酬とする進化

1017 (Oct 17)

↑ エージェント機能・
タスク完了時間の大幅な向上 (Engram
テーブルの専用化)

Key Takeaway: 同価格帯モデルを置き去りにし、タスクあたりコストを1桁以上引き下げる「異常なコストパフォーマンス」空間に位置する。



Key Takeaway: 「安くて賢い」反面、「知らないことを知らないと言えない」致命的な弱点があり、人間による精査が不可避である。



圧倒的優位性

速度と推論の透明性

- 処理速度・初回応答が速い。
思考過程（CoT）の可視化により、サイバー審査等でブラックボックス化しない。



致命的な欠陥

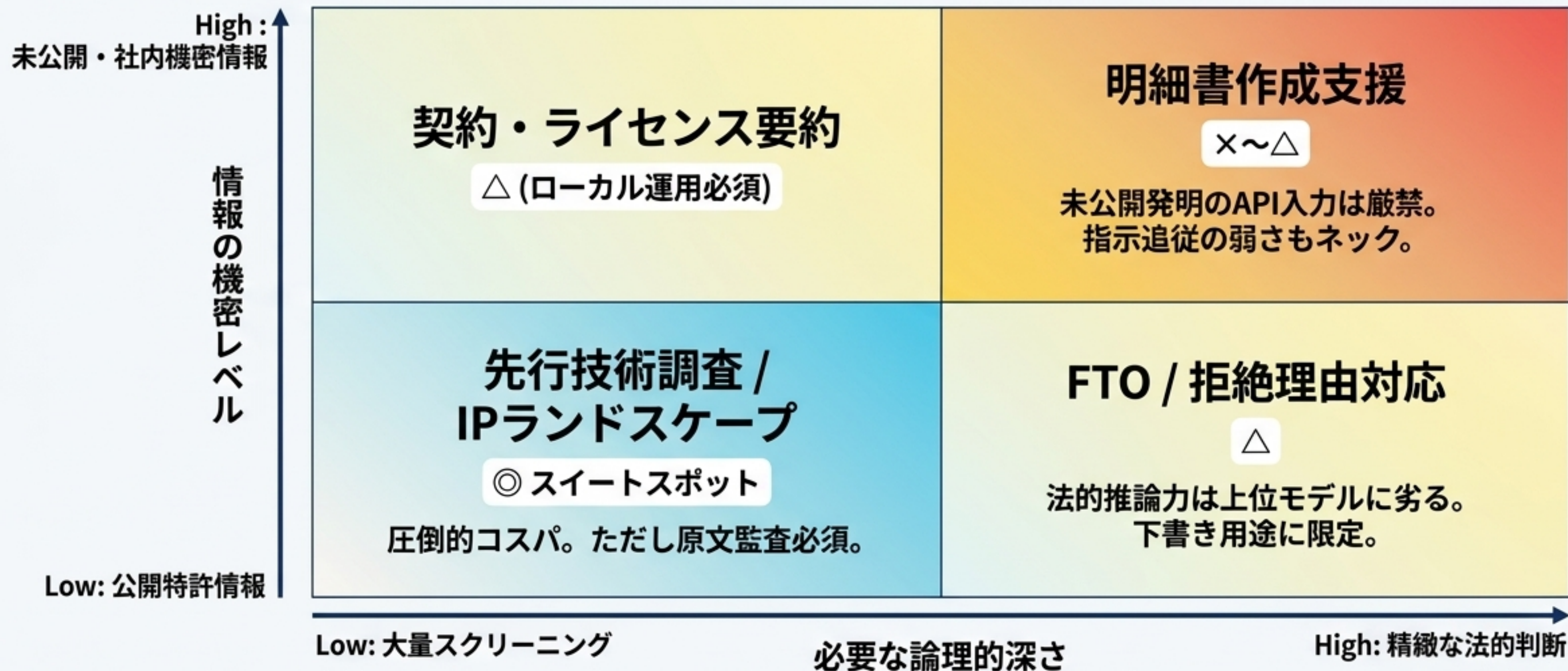
ハルシネーションと日本語の壁

非ハルシネーション率 3.5%

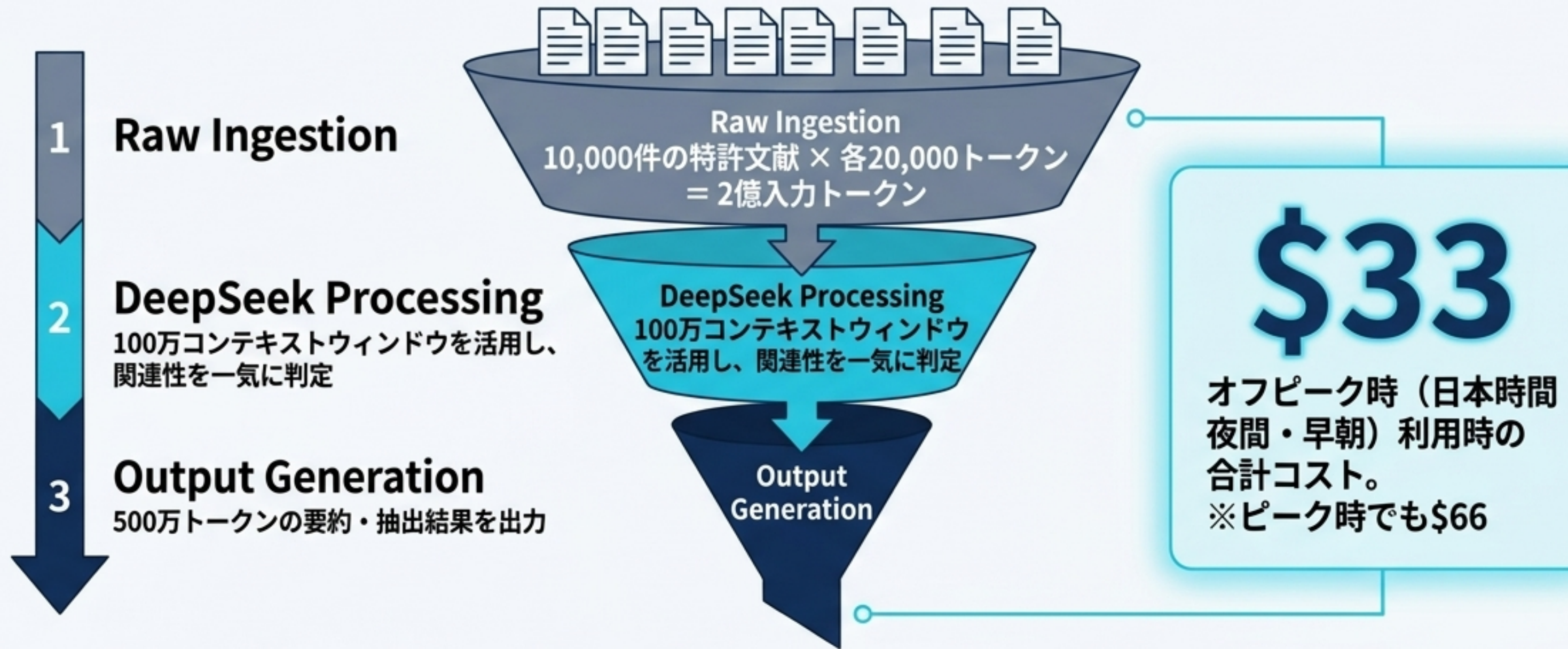
- 日本語の不自然さ（過剰で単調な表現）、JSON Schemaのstrictモード非対応、細かい指示への追従性の低さ。

⚠ 約96.5%の確率で「分からない」と言えず誤答を生成する傾向

Key Takeaway: 100万トークンを活かした「公開情報の大量スクリーニング」がスイートスポット。「明細書作成」はレッドゾーン。

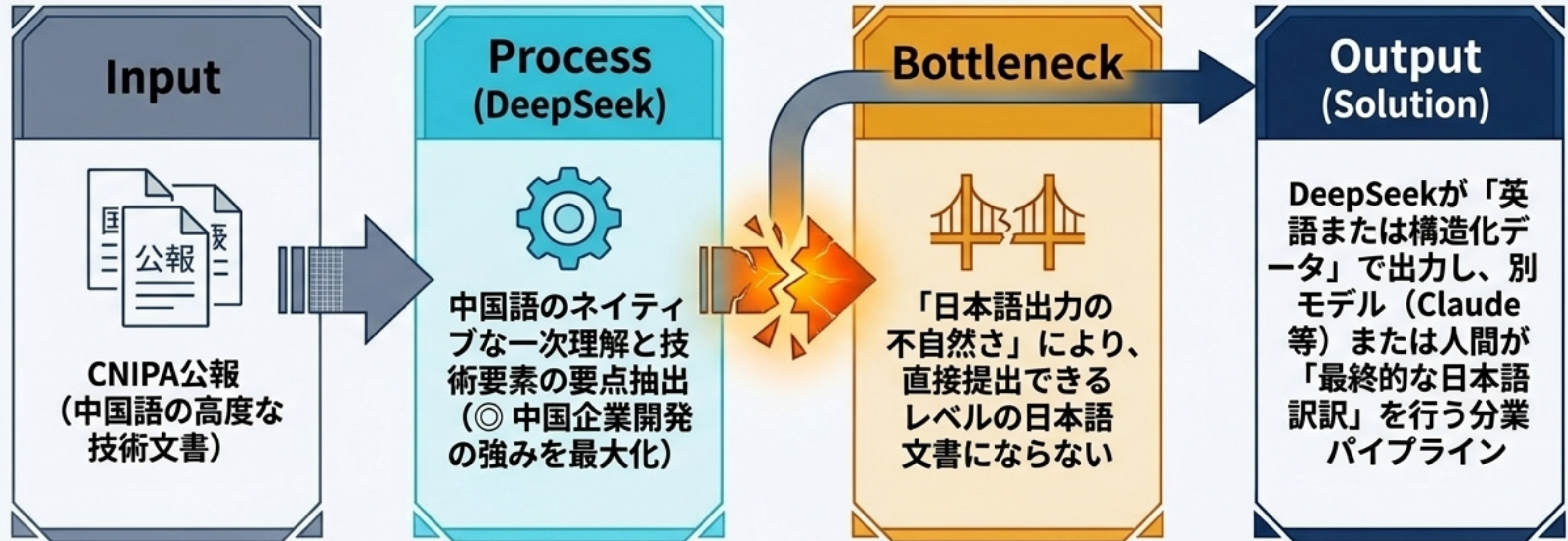


Key Takeaway: 1万件の特許母集団処理が「約33ドル」で完結。 一次スクリーニングのコスト構造が根本から破壊される。



 Risk Mitigation: 記憶に頼った特許番号出力はさせず、必ず「検索DB原文からの根拠段落抽出」をプロンプトで強制すること。

Key Takeaway: CNIPA（中国語公報）の解読能力は圧倒的だが、日本語への最終翻訳は他モデルへのパスが必須となる。



**Key Takeaway: 公式APIへの未公開発明の入力は「公知」リスクを孕む。
保護されたローカル環境での運用が必須である。**

Safe Zone (ローカル運用)



- MITライセンスのオープンウェイト（約510GB）を活用し、社内ネットワークで遮断。
- コーダーシェット公開のブリータに。
- データの越境を物理的に防ぎ、機密情報の漏洩リスクを完全に排除。

Security Firewall

Security Firewall

Danger Zone (外部 API)



- 運営は杭州DeepSeek社。中国本土法準拠、杭州裁判所管轄。
- プライバシーポリシー上、入力データは中国内で収集・保存される。
- 日本国の個人情報保護委員会も中国サーバーへのデータ保存に対し公式に警告を発出（2025年2月）。

結論: 未公開案件や機密性の高い契約書は、左側のSafe Zoneでのみ処理を許可すること。

Key Takeaway: 米国の調達規制と中国の輸出規制の「挟み撃ち」に遭っており、継続利用の保証はない。

Geopolitical Radar Map

西側の排除動向

- NIST/CAISI 警告 (2025/9): 悪意ある要求への応答率94% (米国モデルは8%)。CCPの検閲バイアスを内包。
- 国家レベルの利用禁止: 台湾 (公的機関全面禁止)、豪州・イタリア (利用禁止)。
- 米国の調達規制: 商務省・複数州で政府端末禁止。FY2026国防授權法による国防総省での排除動向。

中国の輸出規制 - East

- 輸出管理草案 (2026/10/16): 学習計算量 10^{26} FLOP以上、または2兆パラメータ以上のモデル重みを輸出管理対象に追加する草案 (11/15締切)。1017は公開済みだが次世代アクセスは極めて不透明。



DeepSeek 1017

戦略的インプリケーション:
現在のオープンウェイト版 (1017) の社内保全を急ぐとともに、単一ベンダーロックインを避けるアーキテクチャが急務。

Key Takeaway: 知財部門のインフラは「公式API（公開情報用）」と「ローカル（機密情報用）」の二段構えが現実的である。

公式API (Official API)

圧倒的な低コスト。
インフラの自社管理
が不要。

データが中国へ渡る。
ピーク時間帯（日本
時間10-13時/15-19
時）は料金が倍額。

用途: 公開特許文献
の大量処理専用。

ローカル運用 (Local / On-Prem)

完全なデータ保護。
未公開の機密情報の
入力が安全に可能。

初期投資大。
8GPU推奨、FP8原版
で約510GB、
2.9bpw量子化版で
約196GBのVRAMリ
ソースを要求。

用途: 未公開案件・
契約書処理の要。

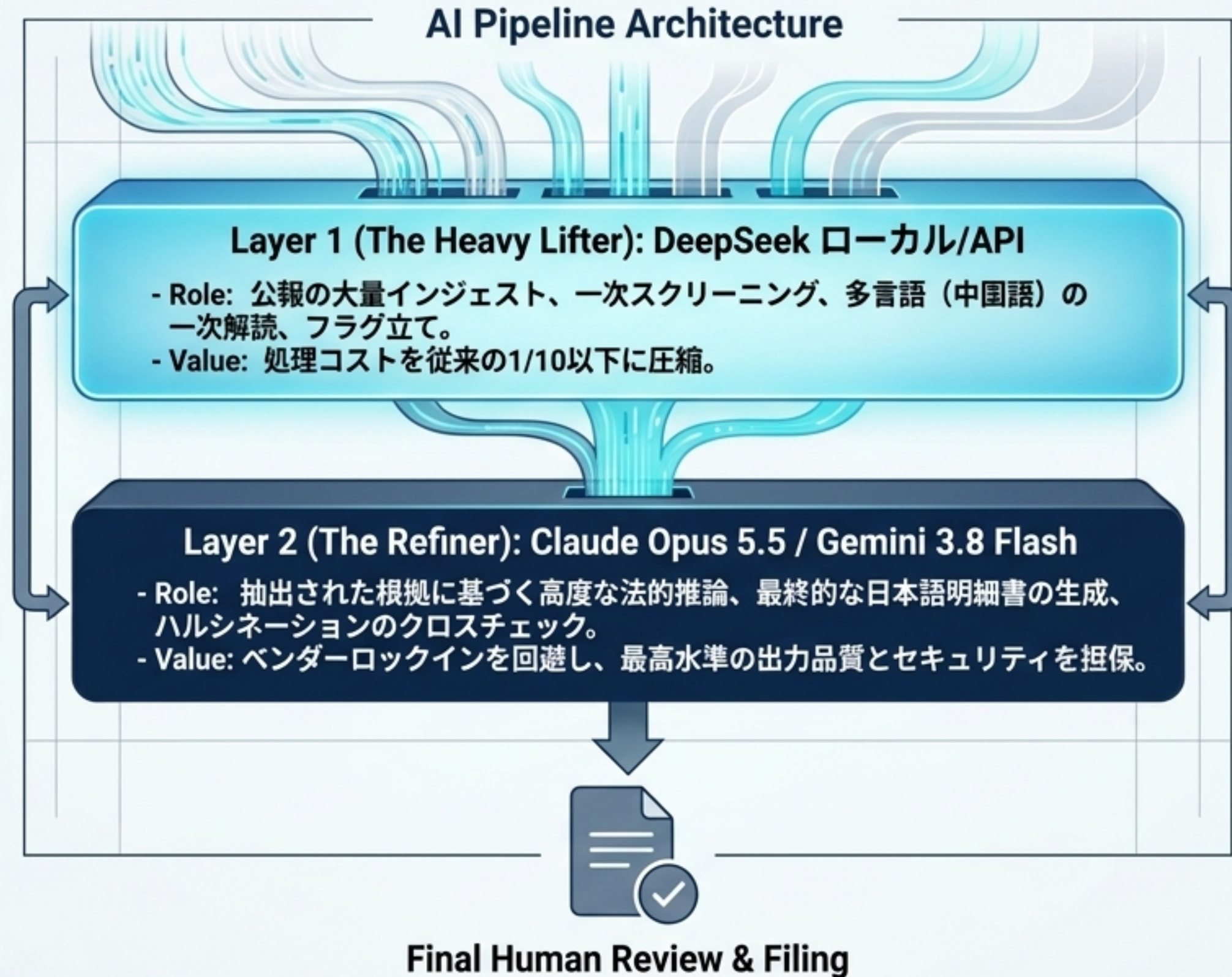
第三者ホスト (Third-Party / OpenRouter)

手軽なアクセスと
API統合。

ルーティング先（
処理国・事業者）の
制御が難しく、コ
ンプライアンス上の
死角になりやすい。

用途: 暫定的な検証
環境に限定。

Key Takeaway: 勝敗を分けるのは単一AIの選定ではなく「適材適所のマルチモデル・ルーティング」アーキテクチャである。



Key Takeaway: 静観する猶予はない。直ちにセキュリティガイドラインを更新し、隔離環境でのPoCへ移行せよ。

Step 1: 即日対応 (Day 1)

ガイドラインの 即時更新



公式APIへの未公開発明・契約書・社内情報の入力を「全面禁止」として通達する。

Step 2: 2～4週間 (Weeks 2-4)

評価セットに よるPoC



過去案件100件を用いた評価セット（スクリーニング・要約等）を作成。ローカル環境または承認済みホストで、1017と上位モデルの精度・費用を比較検証する。

Step 3: 1ヶ月以降 (Month 1+)

エコシステムと 規制の監視



Artificial Analysis等での独立評価スコアの確認。11月1日からのSearch API課金動向と、11月15日締切の中国輸出管理草案の帰趨をモニタリングする。

Key Takeaway: 本レポートはClaude Opus 5.5による一次情報解析に基づくが、未確定の法的・技術的論点が存在する。

Appendix & Caveats

- | | |
|---|--|
| i | 独立評価の不在
1017版の性能数値はDeepSeek自社測定に基づく。第三者機関による速度・ハルシネーション等の厳密な独立評価は10月18日時点で未公表である。 |
| i | ハードウェアと地政学
学習に使用されたチップの詳細は技術報告で非開示。NVIDIA製チップの密輸や米国モデルからの蒸留疑惑については、事実関係が未確定である。 |
| i | 法的解釈の留保
外部AI（API）への未公開発明の入力が「新規性喪失（公知）」にあたるかについては確立した判例がなく、個別具体で専門家（弁理士・弁護士）の判断を要する。 |
| i | 二次情報の取り扱い
8GPU構成要件や非ハルシネーション率（3.5%）など一部のデータは、コミュニティ報告等の二次情報に依拠している。 |