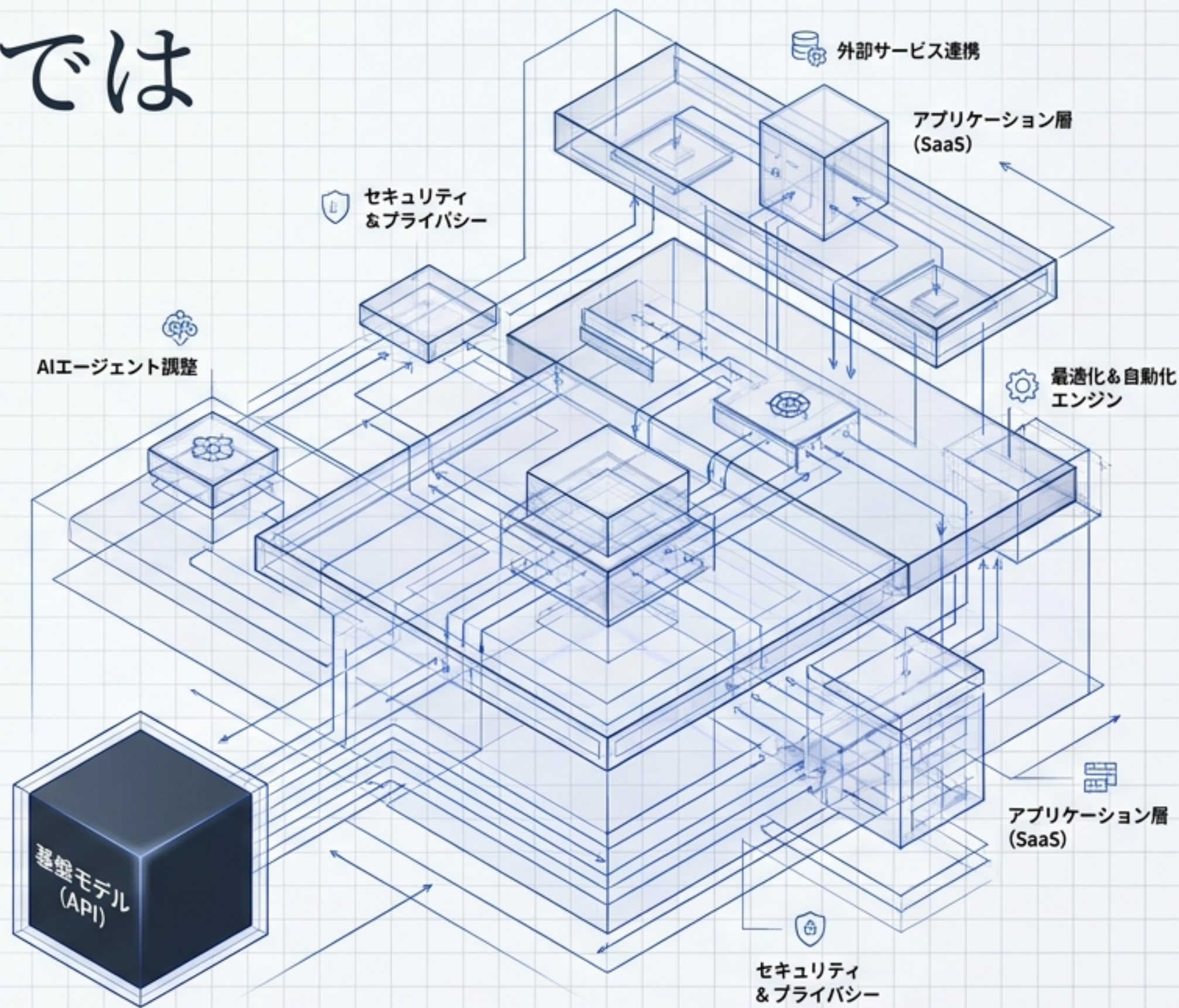


AIの勝負はモデルでは 終わらない

Gensparkが示す 「次のAIサービス」の 競争軸とシステム構造

2026年、基盤モデルは単なる「部品」へと変貌した。真の競争力は、知能の高さそのものではなく、「ユーザーの仕事が終わらせるシステム層」へと移行している。Forbes JAPANの深掘り調査に基づく、次世代SaaSの戦略プレイブック。



「答え」の提供から「仕事の完了」への戦略的移动

2023-2024: AI検索

回答で終わる。Seed \$60M調達。複数モデルを利用。

2025: Super Agentへの転換

Deep ResearchからAI Workspaceへ。非同期の自律行動へシフト。

2026: Workspace 6.0

Voice/Inbox自動化、継続的コンテキスト。モデルのルーティングとコスト効率化を強調。

Insight Badge

Insight: 単なる機能追加ではなく、モデル企業がAPIを閉じるリスクを回避し、「人間・業務」に近い上位レイヤーへ移動する一貫した生存戦略。

企業エージェント市場における爆発的なトラクション



\$2.6B

Valuation (2026年6月 Series B 延長時・Reuters報道)



\$645M

Total Raised



6,400+ 社

Business Clients



\$250M+

ARR (Annual Recurring Revenue)



Disclaimer Box

※顧客数およびARRは監査済み財務情報ではなく、Wen Sangら企業側の自己申告値に基づく。独立検証済み売上高とは区別して評価する必要がある。

むき出しのAPIを「仕事のOS」へ変える4層アーキテクチャ



GenTeam (人間・AI協業)

人間中心のUX、承認フロー、検証UI。プロンプトを書かせない設計。

Suites (実行ツール)

Build / Office / Content。150以上のツールと隔離された実行環境（サンドボックス）。

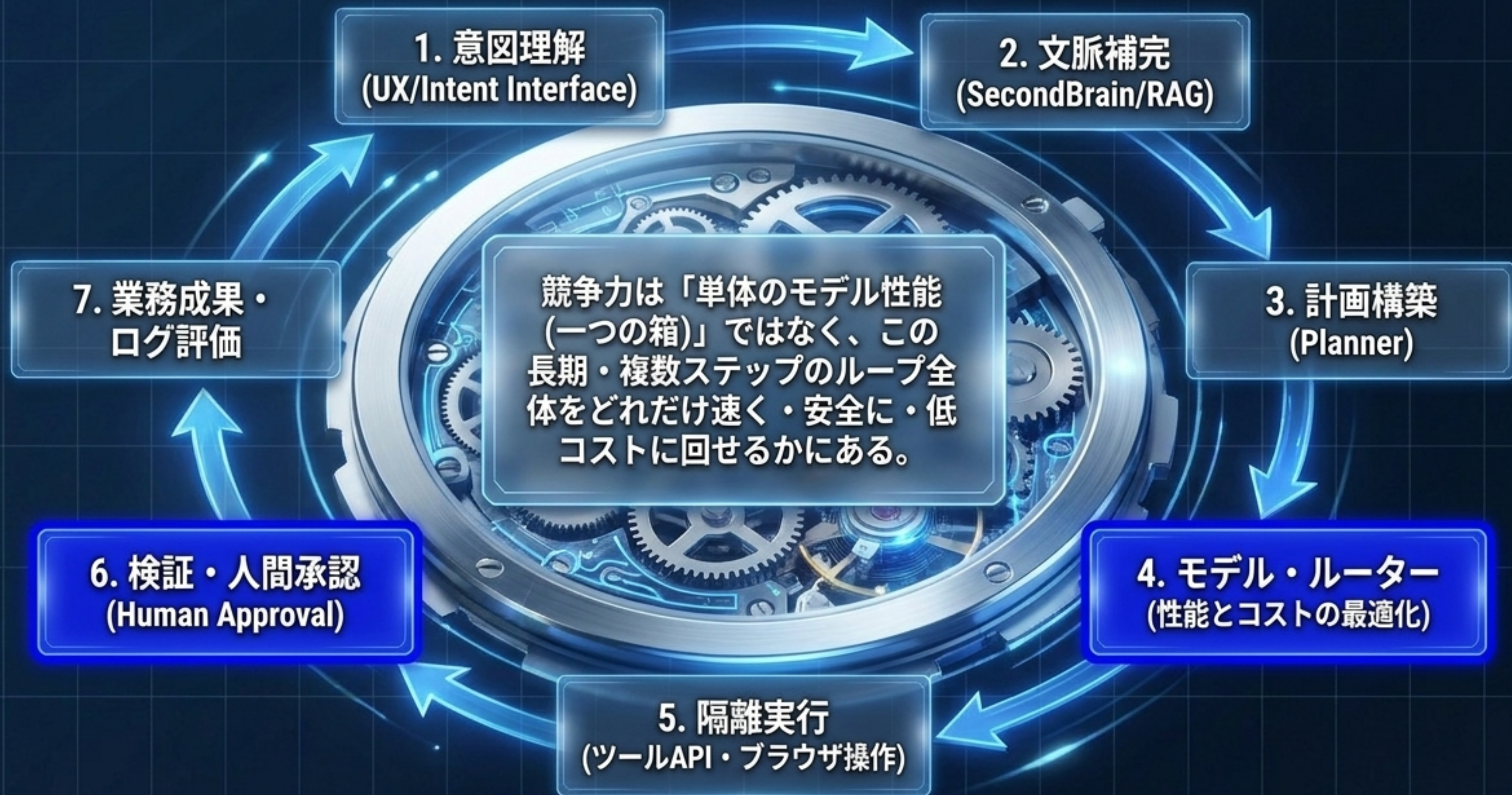
Super Agent (知能・ルーター)

意図理解、プランニング、70以上のモデルの最適なルーティング（高機能/低コスト/専門モデル）。

SecondBrain (文脈・記憶)

メール、会議、チャット、文書の継続的コンテキスト化。「毎回ゼロから説明するAI」からの脱却。

成果を生み出す「自律実行のループ」



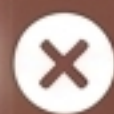
モデル以外の差別化要因と、現実世界の成功・失敗事例



UX / 意図インターフェース



【成功】Panasonic Connectは361万回利用で78.8万時間削減。



【失敗】METR調査：経験豊富な開発者がAIツールを使うと平均19%遅延。



インフラ / 隔離実行



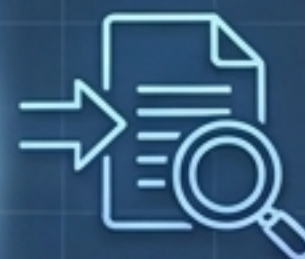
【成功】GensparkはE2Bを利用しコードやウェブ操作を安全にサンドボックス化。



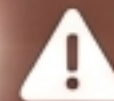
セキュリティ



【リスク】AgentDojoの実証：外部データを通じたプロンプトインジェクションによるエージェントの乗っ取り。



データパイプライン / RAG



【リスク】長い文脈を与えても「Lost in the Middle」問題により検索・QA性能が低下し得る。



運用 / Evals



【リスク】2026年時点でも、Harness（周辺環境）の差だけで長期タスクの成功率に最大18ポイントの差が生じる。



ビジネスモデル

Seat課金だけでは大量Agent利用時の推論原価を吸収できない。Seat + Usage/Creditのハイブリッドが必須。

次世代AIワークスペースの競争マトリクス

	Genspark 6.0	OpenAI ChatGPT Workspace	Microsoft Agent 365	Google Workspace / Gemini	Glean / Notion
マルチモデル対応	◎	△	◎ (partner)	◎	◎
永続的組織コンテキスト	◎	○	◎	◎	◎
自律ツール実行	◎	◎	◎	◎	◎
既存SaaS統合	◎	◎	◎	◎	◎
Agentガバナンス	◎	◎	◎	◎	○

Insight: Gensparkの真の競合はAIスタートアップではなく、仕事のコンテキストとIDを既に握るMicrosoft、Google、Notionなどである。

データ保有者の包囲網と「中立オーケストレーター」の勝機

共存戦略: MS Agent 365
Launch Partner

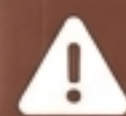
脅威
(Incumbent's Moat)

MicrosoftやGoogleは、最初からメール、文書、予定、ID、権限（Graph）を所有している構造的優位がある。

MSを敵に回さず、エコシステムに乗る（ID/SecurityはMS依存、オーケストレーション特化）。

機動性
(Genspark's Edge)

既存スイートへの忠誠が弱いため、OpenAI、Anthropic、Googleを性能・価格に応じて横断利用できる「マルチクラウド時代のデータ基盤」に近いポジション。



プラットフォーム・リスク: モデル企業によるAPI閉鎖、またはアクセス条件の変更リスク。

経済性の転換：「安さ」から「タスク成功あたりの総費用」へ

旧指標: Cost per Token
(推論単価)

モデル単体の安さを測る。

New KPI: Cost per Successful Task (CPST)

(Model API + Search + Sandbox
+ Human Review + Retry Cost)

成功判定された業務タスク数

Kay Zhu (CTO) の思想: 安いトークンを使っても、ルーティング精度が低く「失敗・再試行・人間の介入」が増えれば、エージェントの総費用は跳ね上がる。長期自律タスクではモデルの単価よりルーティング最適化が命。

「記憶＋行動」がもたらす新たな脅威と権限分離の原則

Threat Expansion: チャットの誤答から、現実世界の誤操作（送金、削除）へとリスクが物理世界へ拡張。

Read権限 $\neq$ Write権限 $\neq$ Send権限 $\neq$ Money-moving権限

AgentDojo Risk

外部ツールから取得した悪意あるデータ（メール等）による間接プロンプトインジェクションでエージェントが乗っ取られるリスク。

Guardrails

高リスク操作（送信・支払）の前には「Human-in-the-loop（人間の承認）」を必須とし、ゼロトラストな実行サンドボックスを構築する。

事業者向け：次世代AIワークスペース構築のロードマップ

Phase 1: 短期 (0-6ヶ月)

予算: 1.5~3億円

RAG、ルーター、サンドボックス、
オフライン評価 (Evals) の構築。
「大量のモデルを載せる」前に、
まず「業務の成功」を機械判定する
評価基盤を作る。

KPI: Task Success >80%

Phase 2: 中期 (6-18ヶ月)

予算: 累計6~15億円

永続コンテキスト、SLA運用、
ルーティングによるコスト削減。

KPI: Cost/Successful Task ▲30~50%

Phase 3: 長期 (18-36ヶ月)

予算: 累計20~50億円

エンタープライズ基盤、国際展開、
コンプライアンス (AI Act等対応)。

Core Advice: 読め・書け・送れを同時に開放しない。段階的な自律性の開放。

投資家向け：次世代AIプロダクトを評価する3つのレンズ



Lens 1: 蓄積される独自資産 (Moat)

モデルがアップデートされても
消えない資産 (Permissioned
Context Graph、評価データ、
修正履歴) があるか？



Lens 2: 実質マージンと成功単価 (Unit Economics)

ARRの伸びだけでなく、推論費
増大に耐えるGross Marginか？
「Cost per Successful Task」は
低減しているか？

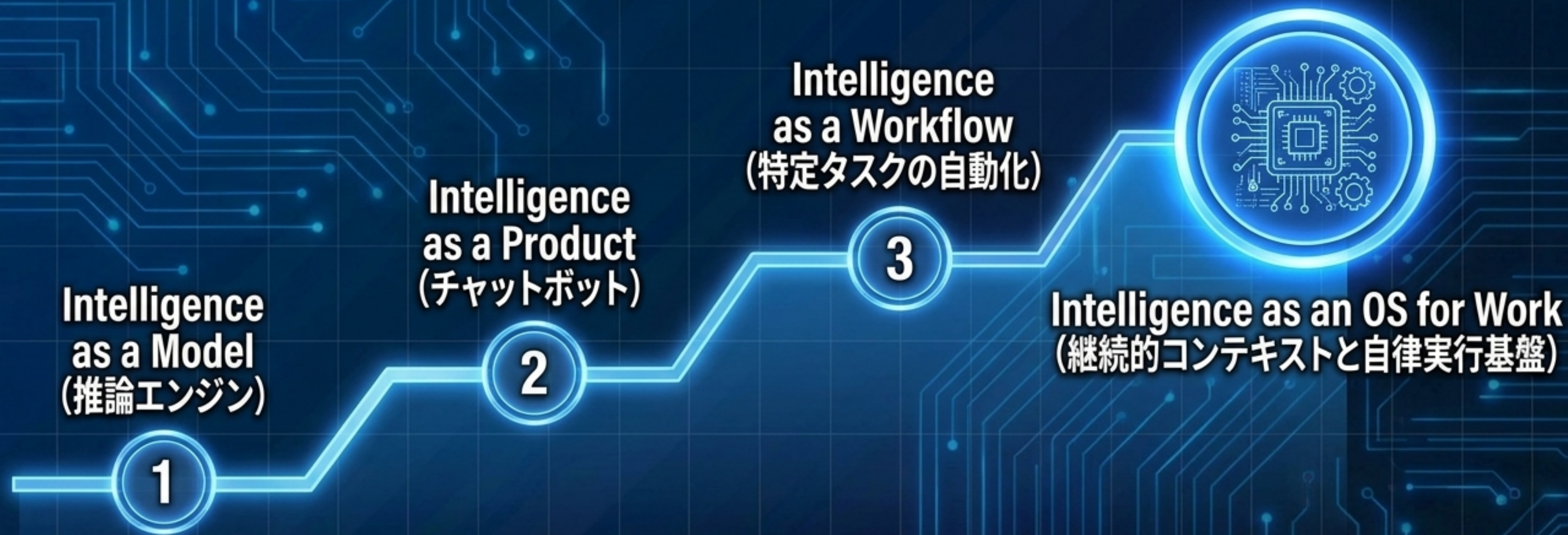


Lens 3: ディストリビューション (Distribution)

既存のSaaSエコシステム
(MS 365等) への組み込みや
流通経路を確保しているか？

Stress Test: DD (デューデリジェンス) では「API価格が2倍になった場合」
「Microsoftが同等機能が無償バンドルした場合」の耐久性をテストせよ。

結論：「モデルの上」に構築される新たな社会技術的システム



Final Thesis: 「AIの勝負はモデルでは終わらない」のではない。モデル競争は続くが、実務上の勝敗を決めるのは、ユーザーの意図から安全な業務成果までを「最小の認知負荷」と「最小のタスク原価」で閉ループ化できる『システム構築力』である。

Appendix & Source Data

Primary Source

Forbes JAPAN: 「AIの勝負はモデルでは終わらない、Genspark創業者が描く『次のAIサービス』の条件」
(2026年8月30日・安井克至)

Key References

- Genspark公式発表: AI Workspace 6.0, The AI Efficiency Frontier
- Reuters: Genspark Series B extension (\$2.6B valuation)
- METR: Task-Completion Time Horizons, 19% slowdown study
- AgentDojo / OWASP: LLM Agents security testing
- NIST AI RMF / 経産省 AI事業者ガイドライン

