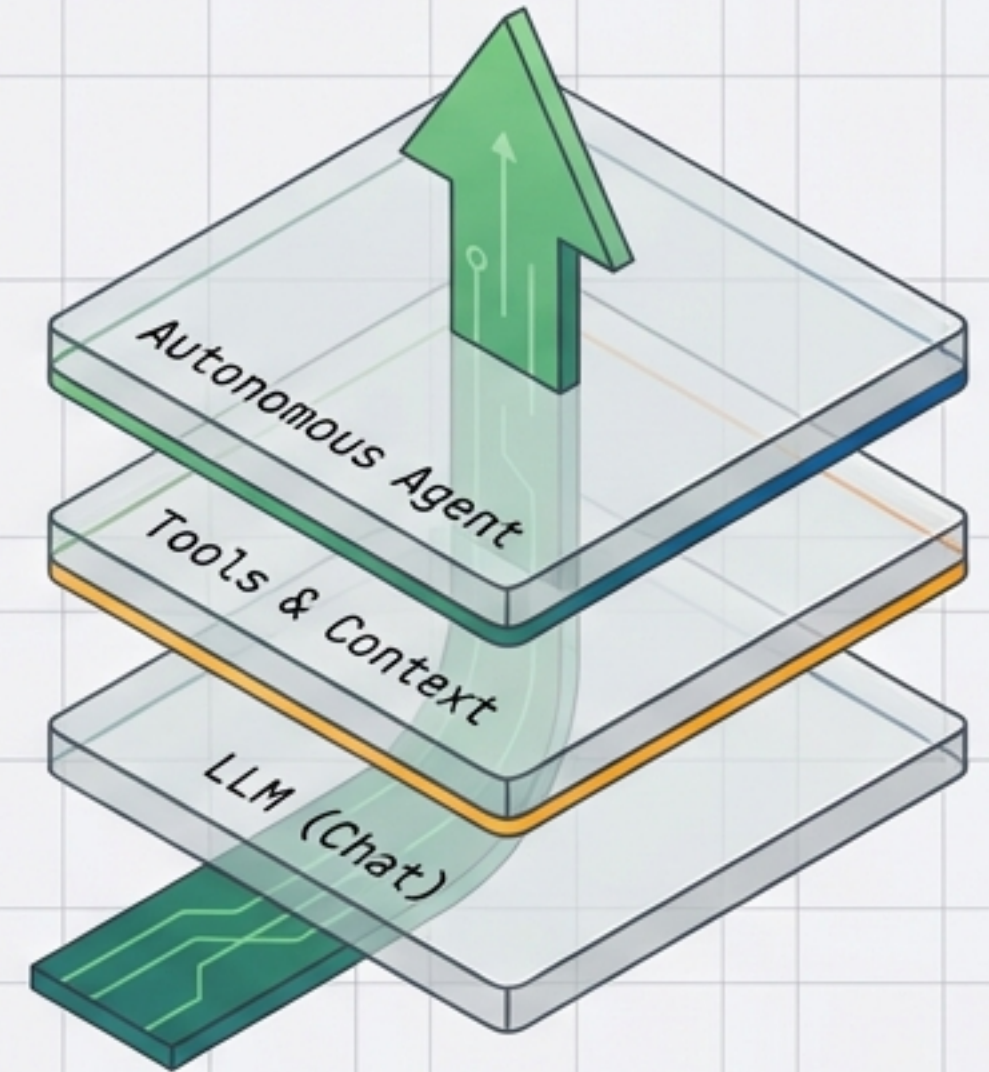


チャットボットから 「自律エージェント」の 時代へ

技術的探求と社会実装の摩擦レポート



ENGINEERING

MitchellhのAGENTS.md
ClaudeによるCコンパイラ構築

FRONTIER

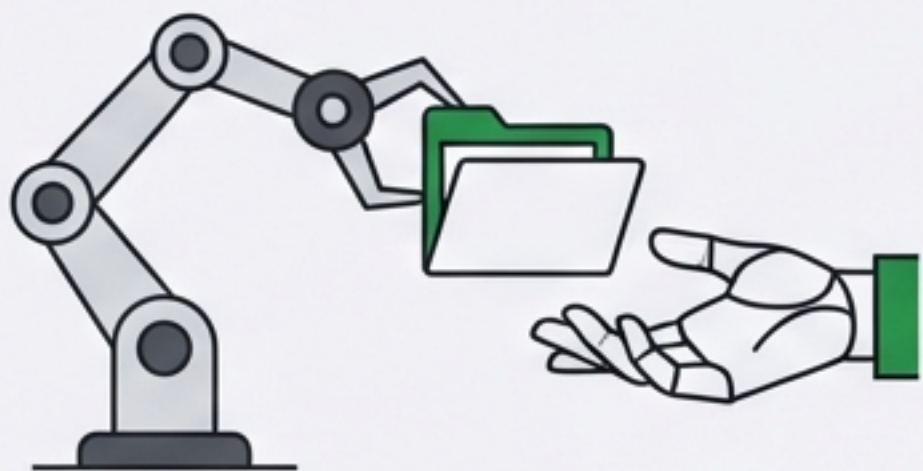
Waymo「世界モデル」Genie 3
3D LiDAR生成

SOCIETY

NY州AI開示義務法案
インドのデータ労働者
CapEx \$6,600億の波紋

DEV SHIFT

開発の転換点

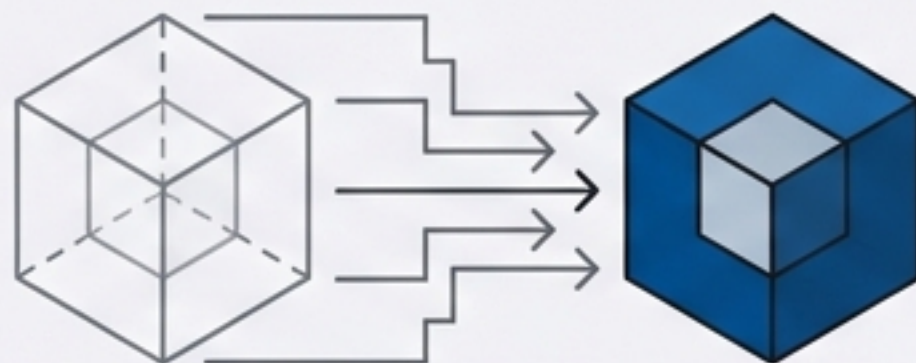


AI活用の主戦場は「対話」から「自律エージェント (Agent Teams)」へ移行。

HashiCorp創業者Mitchellhは「エージェントこそ価値の源泉」と断言。Anthropicは16並列インスタンスでCコンパイラを構築し、人間が仕様を書けば実装はAIが担う未来を示唆。

TECH BOUNDARY

物理とデジタルの融合



世界モデルと大規模並列処理が、物理シミュレーションの限界を突破。

Waymoの新世界モデルは2D動画から「3D LiDAR」データを生成し、竜巻や飛び出しなどのレアケースを検証可能に。

SOCIETAL FRICTION

社会実装の摩擦



技術進化に対し、規制・倫理・市場の揺り戻しが加速。

NY州で「AI開示義務法案」提出
NY州で「AI開示義務法案」提出 (Prop 65化の懸念)。Amazon等の株価急落は、2026年予測6,600億ドルに達するCapExへの収益化懸念を反映。

ENGINEERING THE FUTURE: MITCHELL HASHIMOTO'S MANIFESTO

AGENTS.md

Project Rules

- ALWAYS check existing tests before modifying code.
- Use the specific logging format defined in [/lib/logger](#).
- **Context**: This is a high-performance distributed system.

指示書 (Context) をコードとして管理する

「チャットボットは価値の源泉ではない。エージェント（実行能力）こそが鍵だ」

- **AGENTS.md**：プロジェクト固有の指示書。繰り返し発生するミスを防ぐため、ルールを明文化する（READMEのAI版）。
- **Warm Start**（常時稼働）：作業時間の20%をAIに任せ、翌日のリサーチやトリアージを完了させておく。
- **Deep Thought**：即答ではなく、30分かけて思考させる「遅い」モデルを戦略的に使う。

TAKEAWAY: 最初の失敗で諦めず、「摩擦を乗り越える」までツールを習熟させた者だけが、真の委任（Delegation）に到達できる。

CASE STUDY: CLAUDE OPUS 4.6 BUILDING A C COMPILER

10万行のコードを「Agent Teams」は自律的に記述できるか？

Scale

16

Parallel Instances

Volume

100,000

Lines of Rust

Sessions

2,000

Sessions

Cost

\$20,000

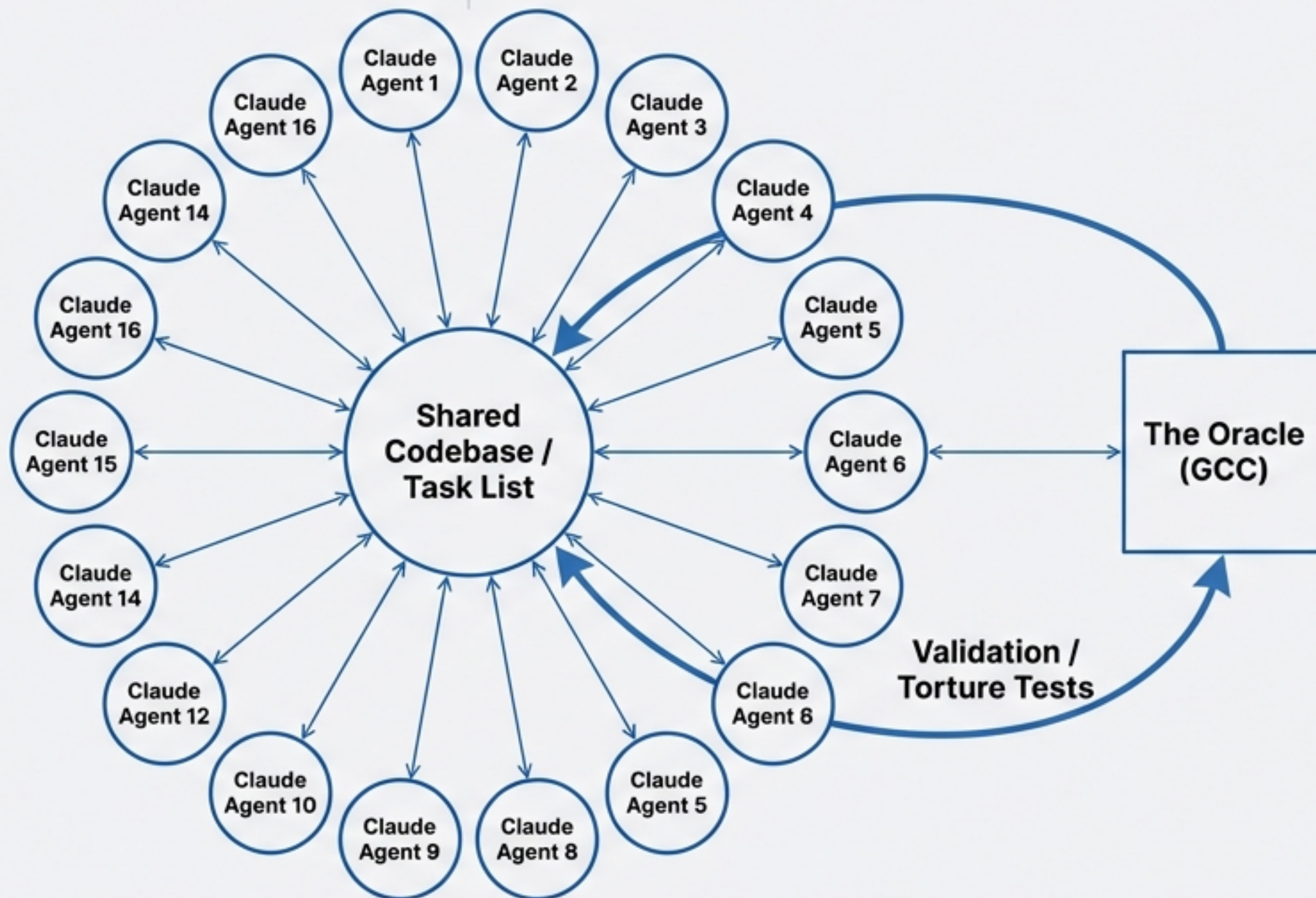
API Spend

Result

Linux 6.9

Build Success

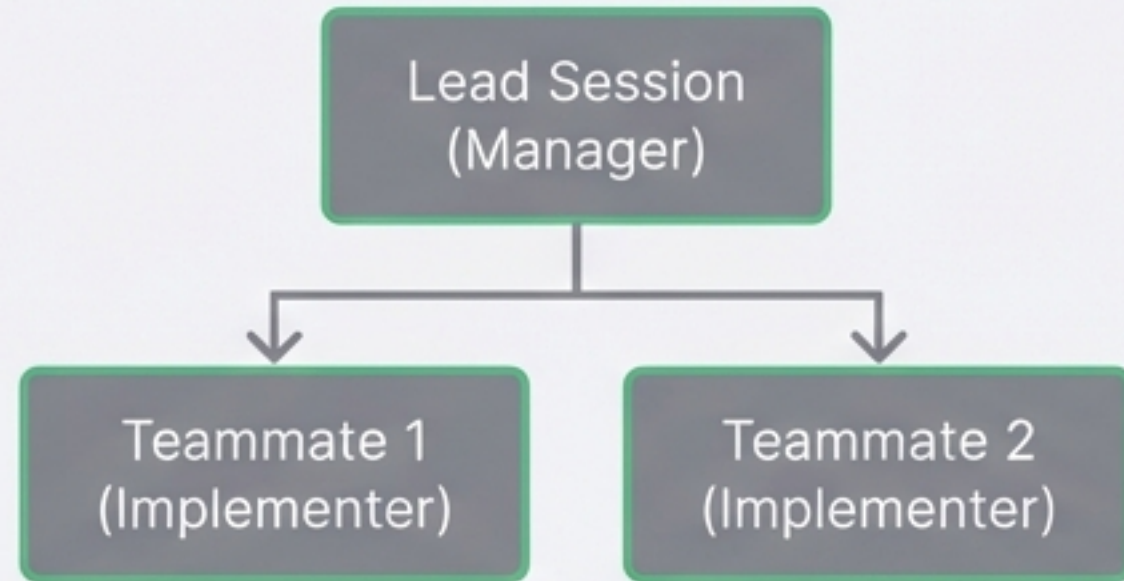
(x86/ARM/RISC-V)



KEY INSIGHT: 「テストファースト」が必須。GCCという強力なオラクル（正解）があったからこそ、マルチエージェントでの自律デバッグが可能になった。

SYNTHESIS: THE REALITY OF AGENT TEAMS

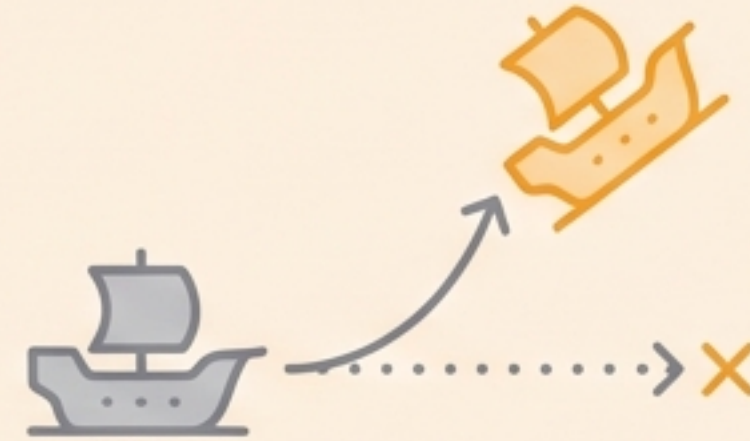
THE NEW STANDARD (Claude Code)



Lead + Teammates: 公式機能として実装。リードがタスクを分配し、チームメイトが並列実装を行う。

Delegate Mode: リードを調整役に特化させ、実装を強制的に委任する。

THE COUNTERPOINT (Critique)



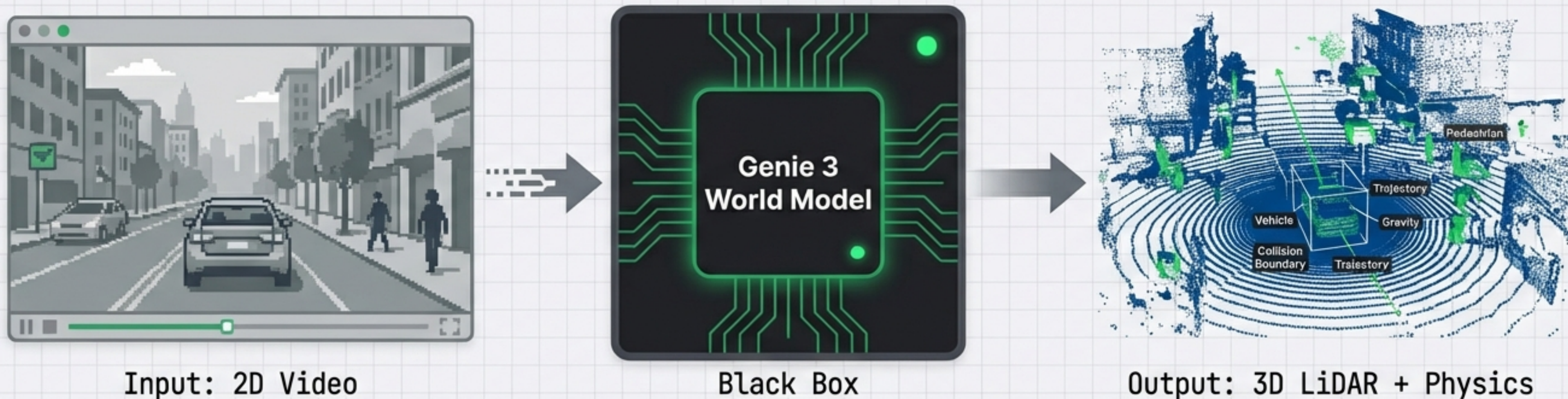
LLM is not a Compiler: 自然言語の仕様（「メモ帳アプリを作って」）は曖昧すぎて、数十億通りの実装を許容してしまう。

Drift Risk: 人間が詳細を理解しないまま「Accept All」を続けると、ソフトウェアは所有者の意図から漂流 (Drift) する。

ACTIONABLE ADVICE: 並列化可能で正解が明確なタスク（テスト生成、ドキュメント）から始めよ。複雑な依存関係はまだ人間の領域。

EXPANDING REALITY: WAYMO'S WORLD MODEL

実走行データの限界を「生成」で突破する (Powered by Genie 3)



Simulating the Rare



竜巻、洪水、飛び出しなど、実データ収集が困難な「レアイベント」を自然言語プロンプトで生成・検証。

Critical View



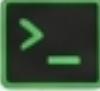


Physics Fidelity: 生成されたシミュレーションは物理法則を完全に守っている保証はない。(例: 2025年SF停電時のWaymo停止事例との乖離)

REGULATORY FRICTION: NY FAIR NEWS ACT

カリフォルニア (Prop 65) 化する「AI開示義務」のリスク

 AI GENERATED

-  **1. Disclosure**
「実質的にAIで作成・編集」されたコンテンツへのラベル義務。
-  **2. Human Review**
公開前に人間がレビューを行う義務。
-  **3. Protection**
AIによる記者情報源へのアクセス制限と、雇用保護。

BUSINESS IMPLICATION

「実質的に (Substantially)」の定義が曖昧。軽微な編集でも対象になるリスクがある。

Action Item: 法案成立を待たず、自社の「AI利用ポリシー (どの段階でAIを使ったか)」を記録するワークフローを整備せよ。

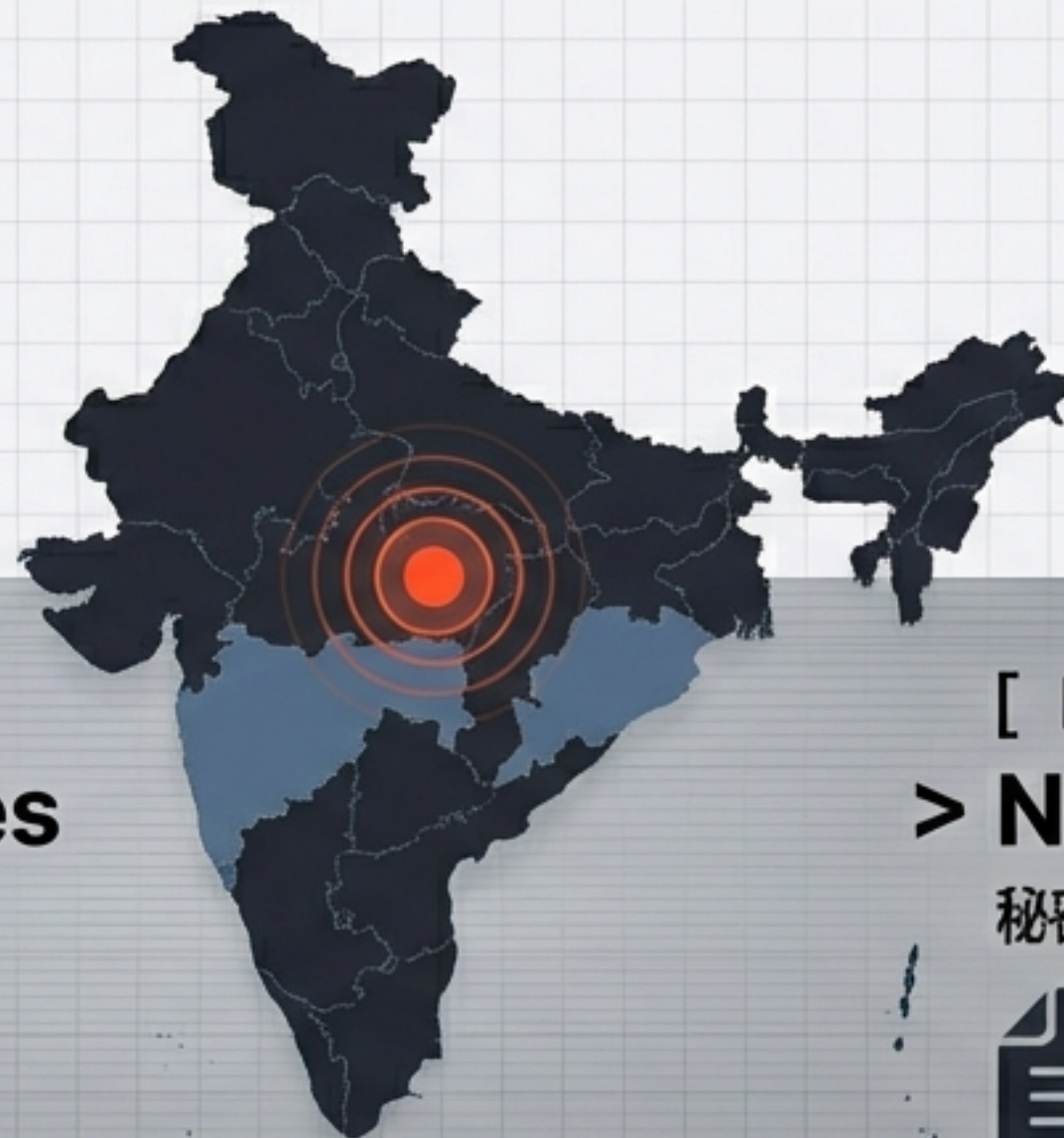
THE HUMAN INFRASTRUCTURE

High-Tech Models vs. The Hidden Workforce

> AI PERFORMANCE

99%  **SUCCESS RATE**

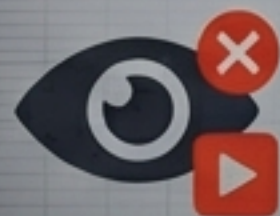
High-accuracy content moderation powered by advanced algorithms.



[WORKLOAD]

> 1日800本

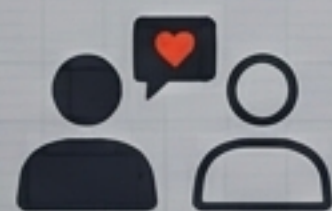
暴力的・性的動画の視聴ノルマ。



[SUPPORT]

> 2 / 8 Companies

心理カウンセリング提供率。



[MECHANISM]

> NDA Isolation

秘密保持契約による社会的孤立。

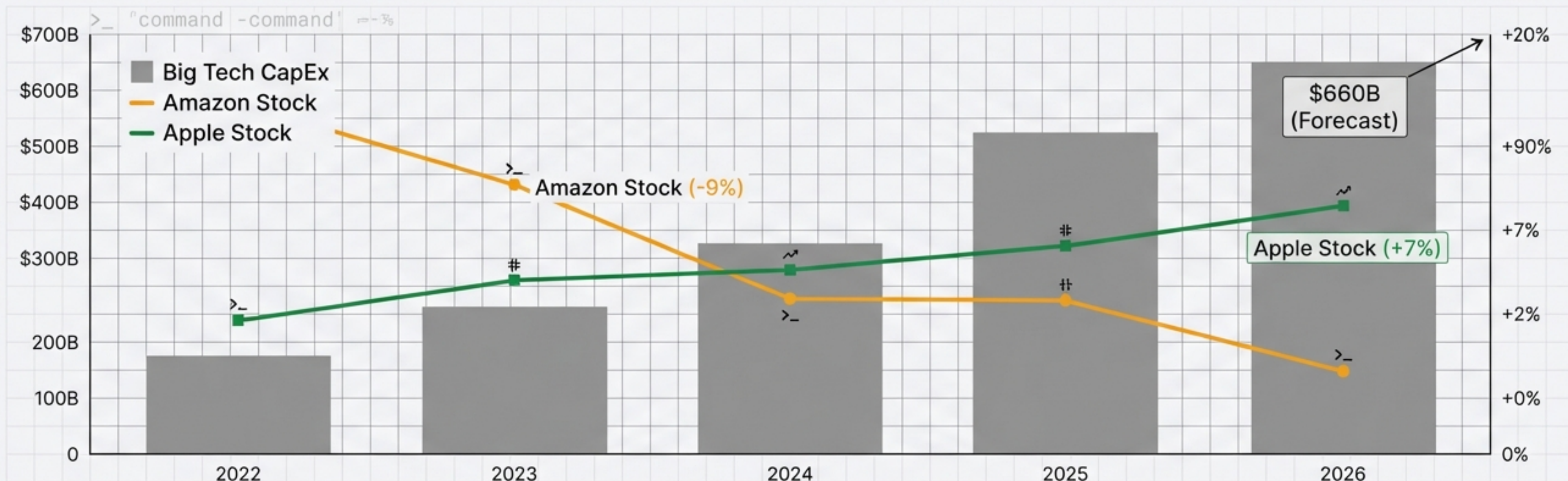


> ETHICAL SUPPLY CHAIN

AIのパフォーマンスは、適切なケアを受けられない労働者の精神的コストの上に成り立っている。企業はサプライチェーンの倫理的責任を問われるフェーズに入った。

MARKET WATCH: THE \$1 TRILLION QUESTION

膨張するCapEx（設備投資）と、見えない収益化への不安



>_ Modern Developer Terminal

MARKET REACTION

Amazon, Microsoft, Nvidia等で週間時価総額が合計1兆ドル減少。

>_

BUSINESS IMPLICATION

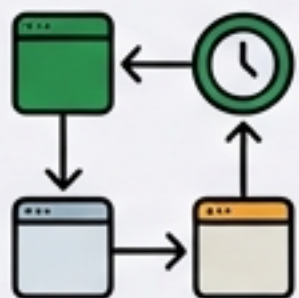
市場は「AIの性能向上」だけでは満足せず、「具体的な収益（ROI）」を厳しく問い始めている。OracleとOpenAIの大型契約さえリスク要因と見なされる局面へ。

>_

STRATEGIC DIRECTIVE: NEXT STEPS

OVERCOME THE FRICTION (摩擦を乗り越えろ)

Try: Experiment with Teams



ClaudeのAgent Teams (または類似ツール) で、テスト生成やドキュメント整備など「並列化可能」なタスクから委任を試す。

Adopt: Warm Starts



作業の20%をAIエージェントに任せ、翌日のリサーチやトリアージを完了させる習慣を作る。

Prepare: Transparency



NY法案をベンチマークとし、自社コンテンツのAI利用履歴 (Provenance) を管理し始める。

Watch: Monitor CapEx



AIバブル崩壊の予兆か、実需への調整か。Big Techの投資対効果のニュースを注視せよ。