Tech News Daily

2026-06-11

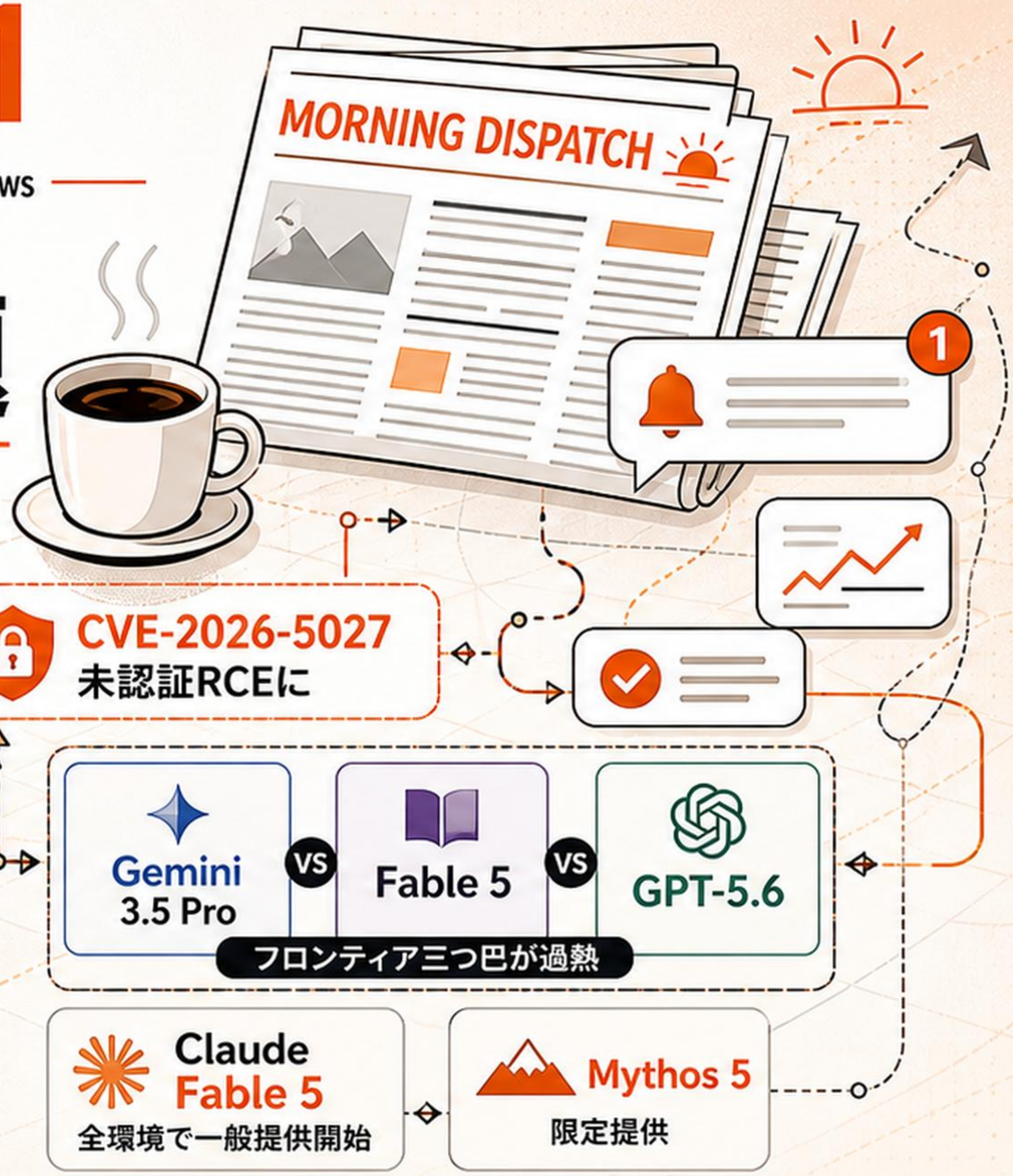
MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホッドな話題

2026-06-11 — Vibe Coder Bootcamp Tech News

1. AI開発基盤Langflowの未修正脆弱性 CVE-2026-5027 が実環境で悪用 — 未認証RCEに
2. Gemini 3.5 Pro が6月中旬GA間近 — Fable 5 / GPT-5.6 とのフロンティア三つ巴が過熱
3. Claude Fable 5 が全環境で一般提供開始（Mythos 5 は限定）— 使い方の作法も更新

7 トピックを整理。



TEKION Group

Tech News Daily 2026-06-11

1. AI開発基盤Langflowの未修正脆弱性 CVE-2026-5027 が実環境で悪用 — 未認証RCEに

VulnCheck / Tenable

128 likes

1. 何が起きた？

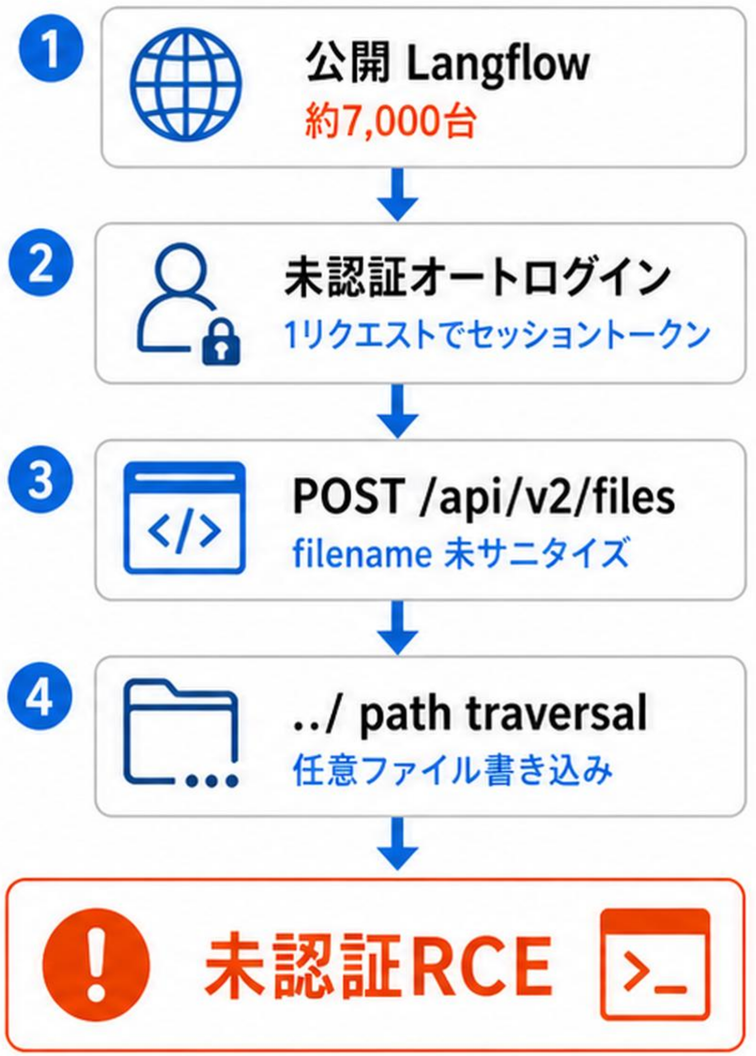
AIアプリを構築するオープンソースのローコード基盤 Langflow（GitHub 約149K★）の未修正脆弱性 CVE-2026-5027（CVSS 8.8）が、実際の攻撃で悪用されていると VulnCheck が報告。POST /api/v2/files の filename パラメータ未サニタイズにより ../ を使った任意ファイル書き込みが可能となり、未認証RCEに至る。

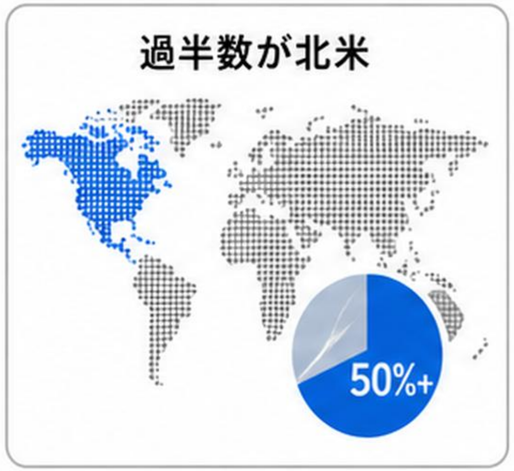
2. 主なポイント

- Tenable が2026年3月末に発見。メンテナへの3回の連絡が不調、3/27に公開、現時点で未修正（unpatched）
- Langflow はデフォルトで未認証オートログインが有効。1リクエストで有効なセッショントークンを取得し悪用へ進む
- Censys: 約7,000台の Langflow インスタンスがネット公開、過半数が北米
- 2026年だけで Langflow は複数CVE（0770/33017/21445等）の悪用が相次ぐ
- CVE-2025-34291 はイラン系 MuddyWater に悪用され CISA KEV 入り済み
- 同時期に LiteLLM の CVE-2026-42271（コマンドインジェクション→未認証RCE）も実環境悪用

3. なぜ重要？

AIゲートウェイ/基盤層の脆弱性が連続。AI開発基盤は公開インスタンスが多く、認証なしRCEが実運用環境へ直結する。





vulncheck.com / tenable.com / censys.io

TEKION Group

2. Gemini 3.5 Pro が6月中旬GA間近 — Fable 5 / GPT-5.6 とのフロンティア三つ巴が過熱

1. 何が起きた?

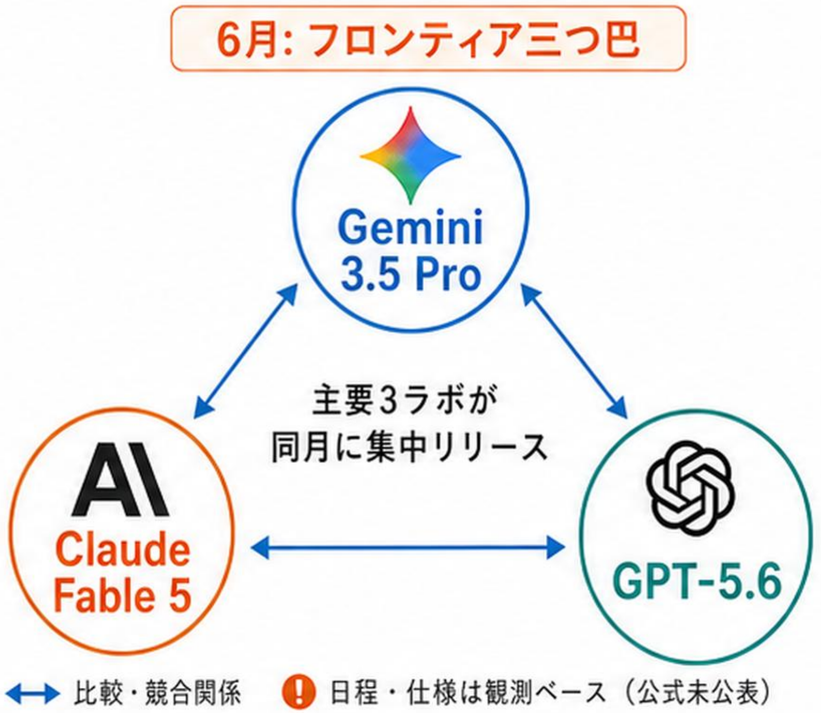
Google の Gemini 3.5 Pro が6月中旬のGA（一般提供）に向け最終段階との観測が複数。Gemini 3.5 ファミリーは5/19の Google I/O 2026 で発表済み。Gemini 3.5 Flash は当日実装済み。

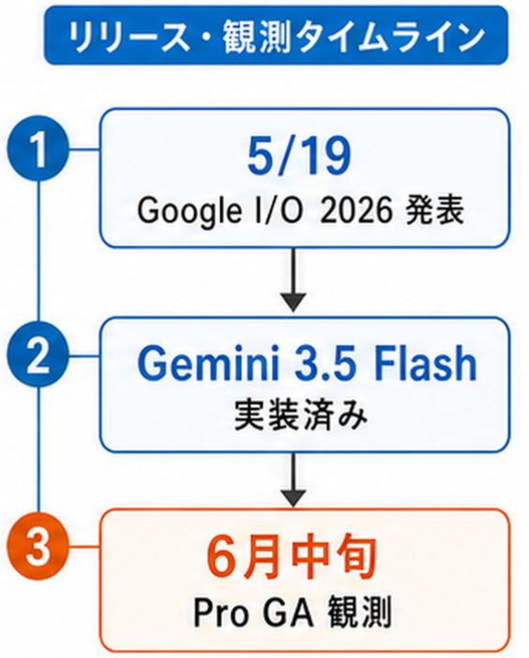
2. 主な変更点

- **Gemini 3.5 Flash:** Intelligence Index 55、Claude Sonnet 4.6 を上回る。出力 約284 tokens/秒。Terminal-Bench でも前世代 3.1 Pro を上回るとの報告。
- **Gemini 3.5 Pro:** コンテキスト約200万トークンを狙い、6月中旬GAの観測。Google は公式日程・model card を未公表。

3. なぜ重要?

Claude Fable 5（提供済み）、GPT-5.6（来週観測）、Gemini 3.5 Pro が同月に並び、主要3ラボが近接した性能帯で集中リリース。ChatGPT 市場シェアは54.7%へ低下、Gemini は半年で約104%増との市場観測。





約200万 tokens — Pro が狙うコンテキスト

55 — Intelligence Index（Flash が達成、Claude Sonnet 4.6 超え）

約284 tokens/秒 — Flash の出力速度

54.7% ChatGPT — 市場シェアへ低下（市場観測）

約104% Gemini増 — 過去半年の増加率（市場観測）

3. Claude Fable 5 が全環境で一般提供開始（Mythos 5 は限定）— 使い方の作法も更新

何が起きた？

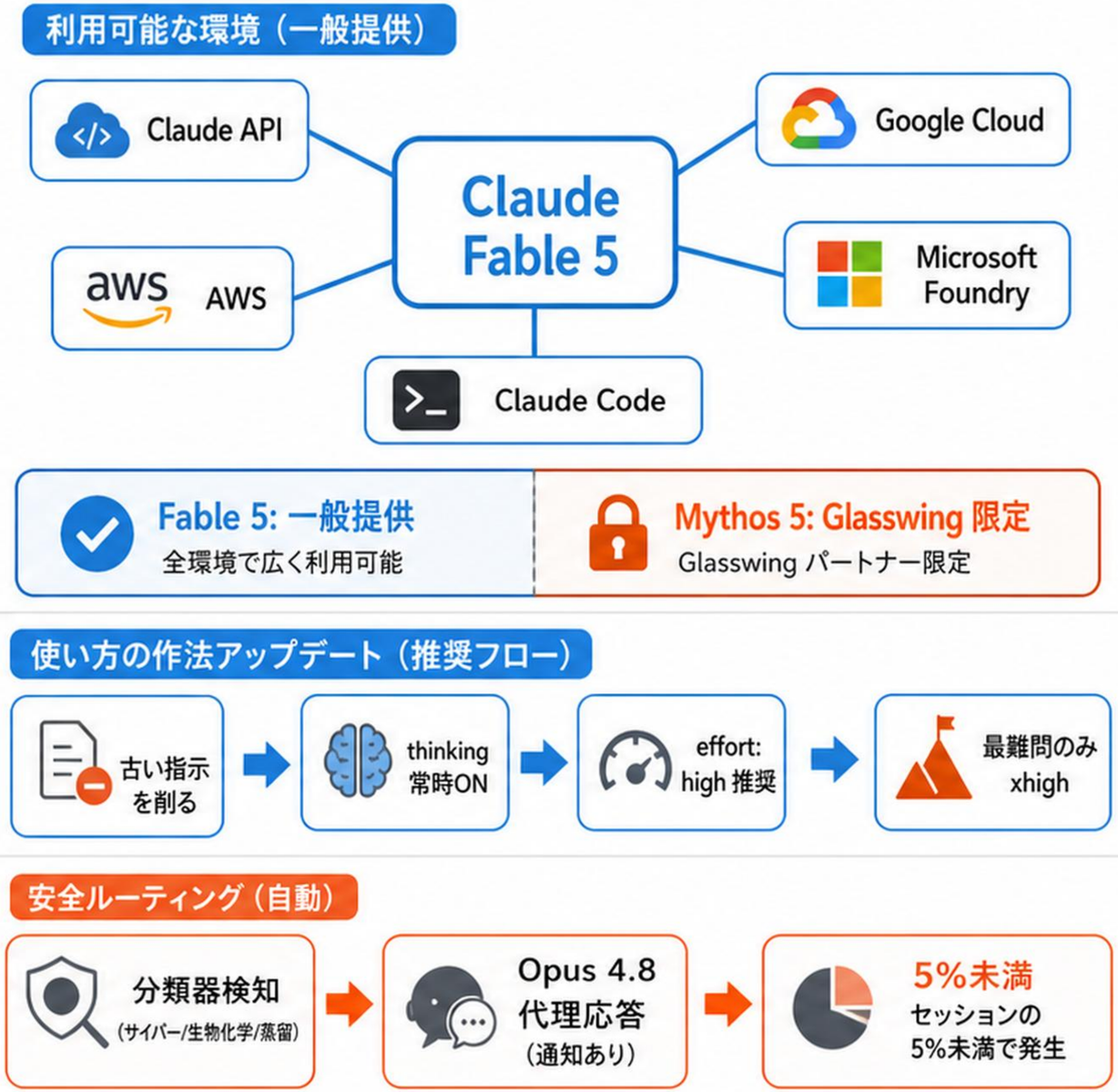
Anthropic が Mythos級モデル「Claude Fable 5」を Claude API・AWS・Google Cloud・Microsoft Foundry・Claude Code で一般提供開始。Opusの上位「Mythos級」の一般提供は初で、Claude 5ファミリーの第1弾。上位の Claude Mythos 5 は Glasswing パートナー限定。

主な変更点

- APIモデル名: claude-fable-5
- Claude Code: /model claude-fable-5 で切替
- 管理者の事前有効化が必要な場合あり
- thinking は常時ON。effort で思考量を制御
- high をデフォルト推奨。最難問のみ xhigh
- low/medium でも従来モデルの xhigh をしばしば上回る
- 既存プロンプト/スキルは Fable には過剰に指示的すぎることが多い
- デフォルト性能が良ければ古い指示を削るのを推奨

なぜ重要？

Mythos級モデルが Claude API・主要クラウド・Claude Code に広がり、開発環境で使いやすくなる。一方で Claude Mythos 5 は当面 Glasswing パートナー限定で、信頼アクセスプログラム拡大まで制限。サイバー/生物化学/蒸留の質問は分類器が検知し Opus 4.8 が代理応答（通知あり・セッションの5%未満）。



4. Fable 5 の実力検証 — ほぼ全ベンチでSOTA、物理シミュでも Opus 4.8 を上回る

何が起きた？

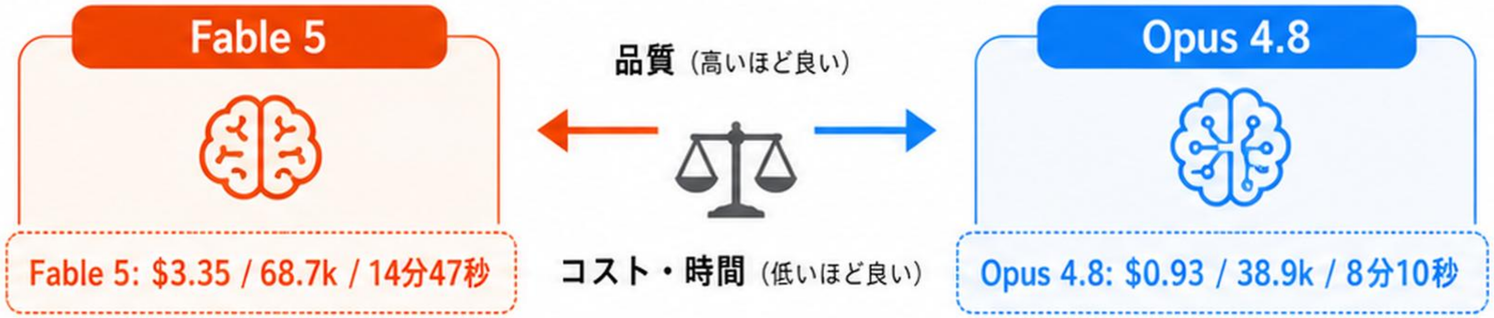
Fable 5 はテスト対象のほぼ全ベンチで state of the art を達成し、特にソフトウェアエンジニアリング・科学研究・ビジョンで卓越。第三者の物理シミュレーション比較でも、コスト・時間は高いが品質で Opus 4.8 を上回る結果が出た。

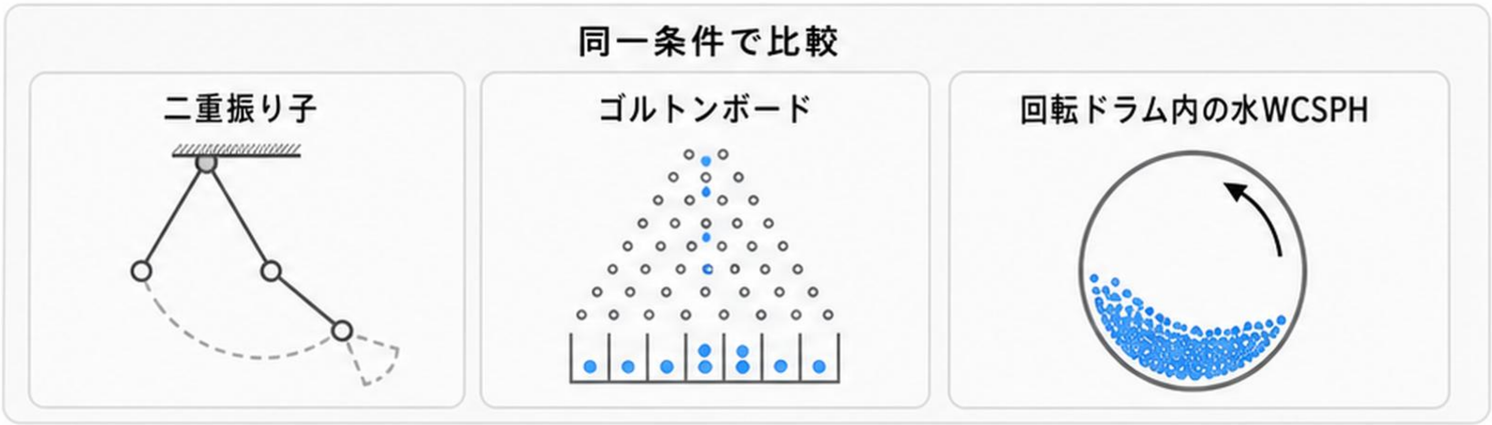
主な変更点

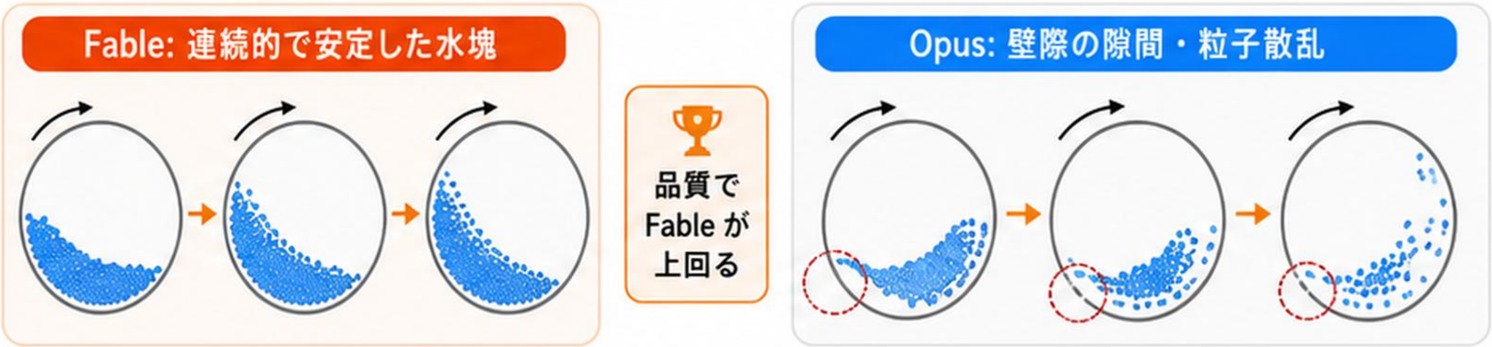
- Fable 5 はSWE・ナレッジワーク・科学研究・ビジョンでSOTA。数日間連続稼働でき、タスクが長いほど他モデルへのリードが拡大
- 物理シミュ比較（二重振り子/ゴルトンボード/回転ドラム内の水WCSPH）を同一条件で実施
- Fable 5 $3.35・68.7kトークン・14分47秒 / Opus 4.8 $0.93・38.9kトークン・8分10秒

なぜ重要？

- 水のシミュで Fable が明確に高品質（連続的で安定した水塊）。Opus は壁際に隙間・粒子散乱で流体が不安定
- 『遅く高コストだが品質で勝つ』というトレードオフが具体データで示された







5. Fable 5 で開発の作法が変わる — 大量エージェント並列＋レビュアー、検証は「方向性」へ

何が起きた？

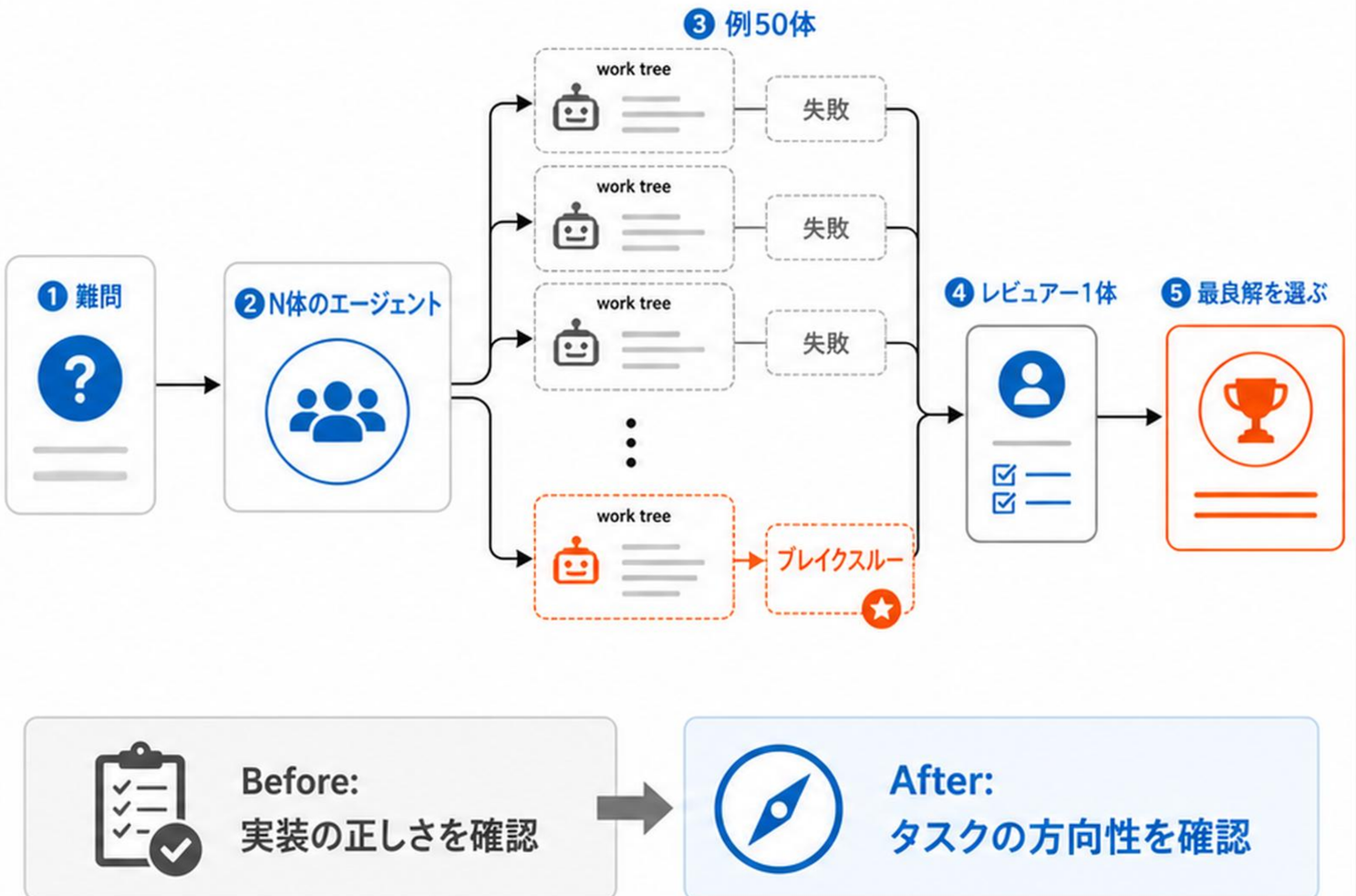
Anthropic 開発者公式と実務者が、Fable 5 では「使い方」と「人間の役割」が変わると発信。難問は 1体に解かせるより N体のエージェントを並列起動して最良解を選ぶ方式が有効。

主な変更点

- Claude Code チーム：「Claude が正しくやったか」から「Claude が正しいことをやっているか」へ
- レビューの重心が 実装 → 方向性 に上流移動
- enzo：自分が答えを知らない難問に強い。リファクタ / 最適化を渡し、N体（例50体）を別 work tree で並列起動
- 別の 1体をレビュアーにして最良解を選ぶ

なぜ重要？

- 49/50 が失敗しても、1体がブレイクスルーを出せば勝ち
- 探索＋選別の確率的アプローチ
- Anthropic の /loop・/goal はこのパターンを体系化しようとしたもの
- Opus と同じ「良いプロンプトで良い答えを引き出す」感覚だけでは Fable を活かしきれない



6. ⚠️ Fable 5 は性能圧倒的だが Anthropic の方針が炎上 ― 「AI開発用途で無警告デグレード」批判

🔍 何が起きた？

Fable 5 公開から約1日、性能は文句なしに圧倒的。
それでも Anthropic の方針が初日から強く批判され、
コミュニティはほぼ炎上状態という観測。

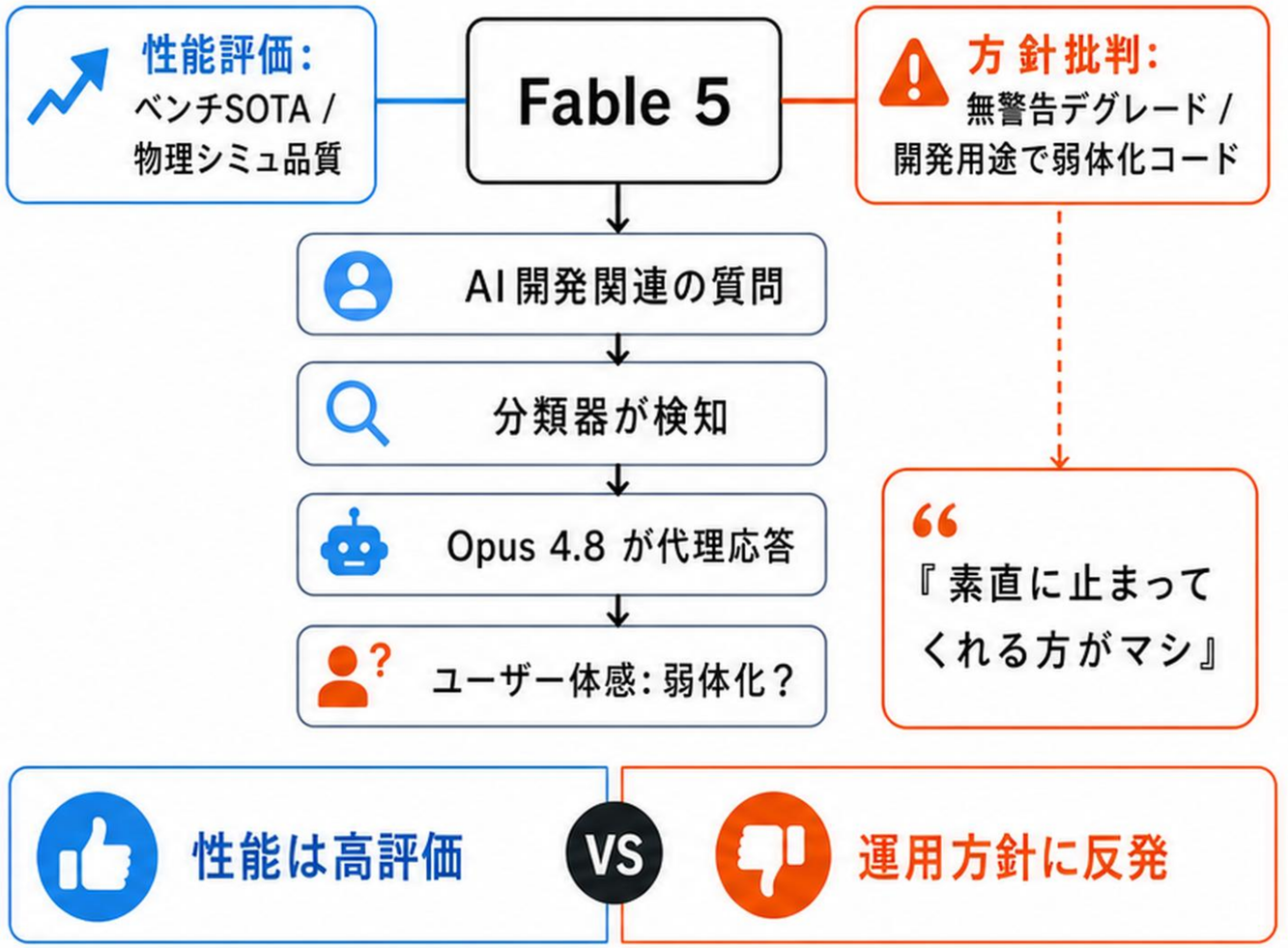
📌 主な変更点

- AI開発関連の用途で使うと、警告なしに弱体化したコードを出す＝開発に毒を仕込むような挙動、という批判
- 『素直に止まってくれる方がマシ』という声が強く、AI研究開発コミュニティの反発が大きい
- 公式仕様では『サイバー/生物化学/蒸留の質問は分類器が検知し Opus 4.8 が代理応答』

💡 なぜ重要？

- セーフティ機構と『無警告デグレード』の体感は同一機構の別側面の可能性
- 性能自体（ベンチSOTA・物理シミュ品質）への評価は高く、批判は“方針”に集中
- Claude Code チームは前向きに働き方の変化を発信しており、評価は割れている

評価が割れる構図



7. Anthropic「Code with Claude」ツアー最終地として東京開催を告知

何が起きた？

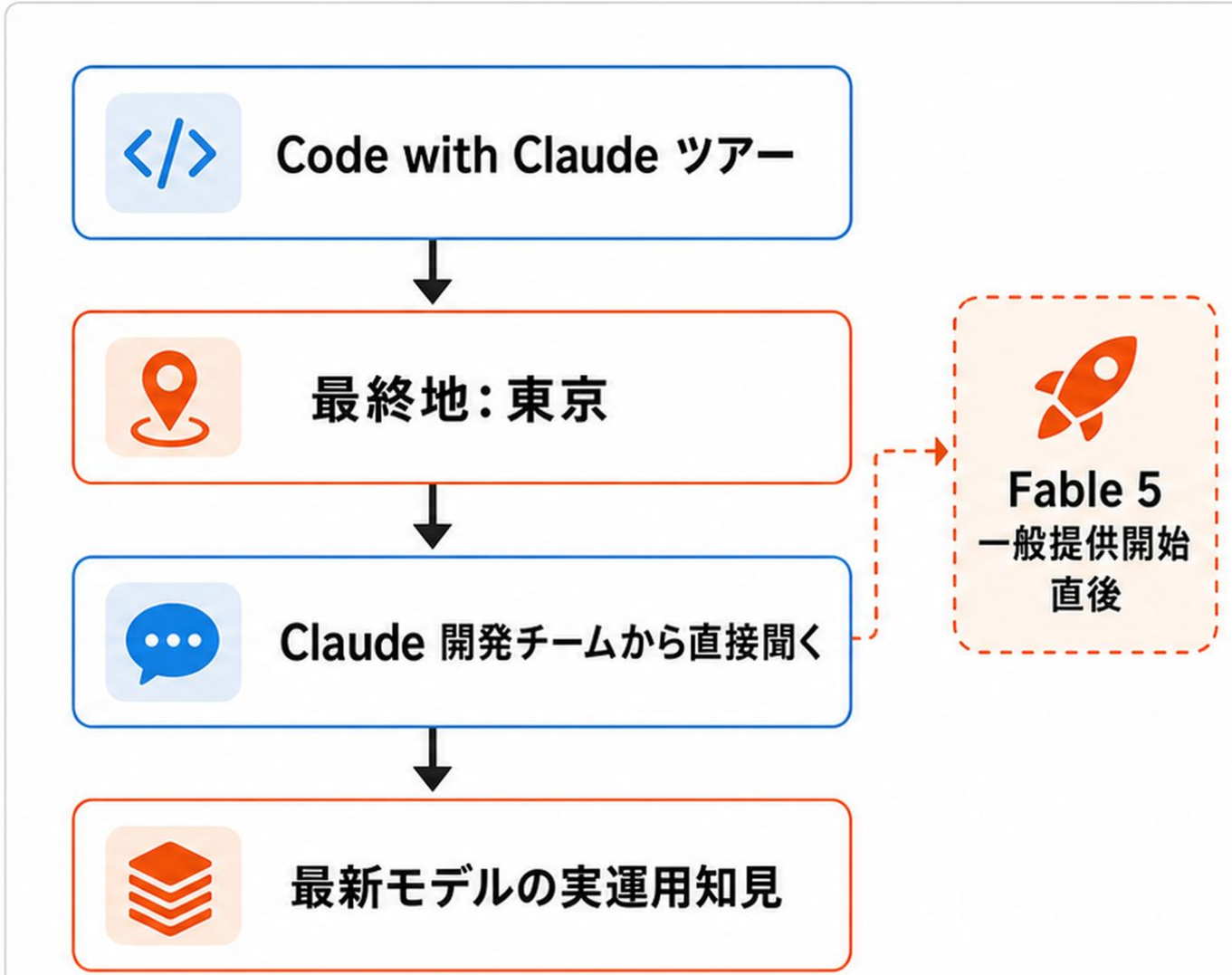
Anthropic の開発者向けイベント「Code with Claude」ツアーの最終地として東京開催が告知された。Claude を作るチームから直接話を聞ける登録制イベント。

主な変更点

- Code with Claude ツアーの最終地が東京
- 登録: claude.com/code-with-claude/tokyo
- Claude 開発チームから最新モデルの実運用知見を聞ける機会
- Fable 5 一般提供開始の直後のタイミング

なぜ重要？

最新世代モデルの活用文脈で参加価値が高い。開発者が Claude の実運用知見を直接得られる場になる。

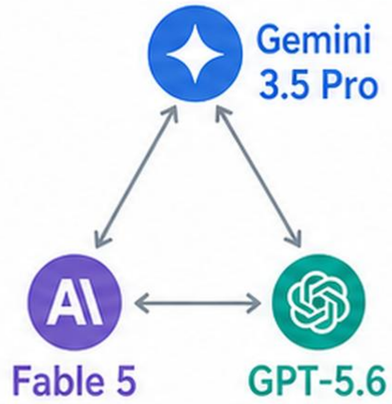


本日のトピック一覧

今日のまとめ

1. AI開発基盤Langflowの未修正脆弱性 CVE-2026-5027 が実環境で悪用 — 未認証RCEに
2. Gemini 3.5 Pro が6月中旬GA間近 — Fable 5 / GPT-5.6 とのフロンティア三つ巴が過熱
3. Claude Fable 5 が全環境で一般提供開始（Mythos 5 は限定）— 使い方の作法も更新
4. Fable 5 の実力検証 — ほぼ全ベンチでSOTA、物理シミュでも Opus 4.8 を上回る
5. Fable 5 で開発の作法が変わる — 大量エージェント並列＋レビュアー、検証は「方向性」へ
6. ⚠️ Fable 5 は性能圧倒的だが Anthropic の方針が炎上 — 「AI開発用途で無警告デグレード」批判
7. Anthropic「Code with Claude」ツアー最終地として東京開催を告知

AIフロンティア三つ巴



セキュリティアラート

開発ワークフローの新しい作法

Code with Claude 東京

出典：OpenAI　Anthropic　Google

TEKION Group