Tech News Daily

2026-06-27

MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホットな話題

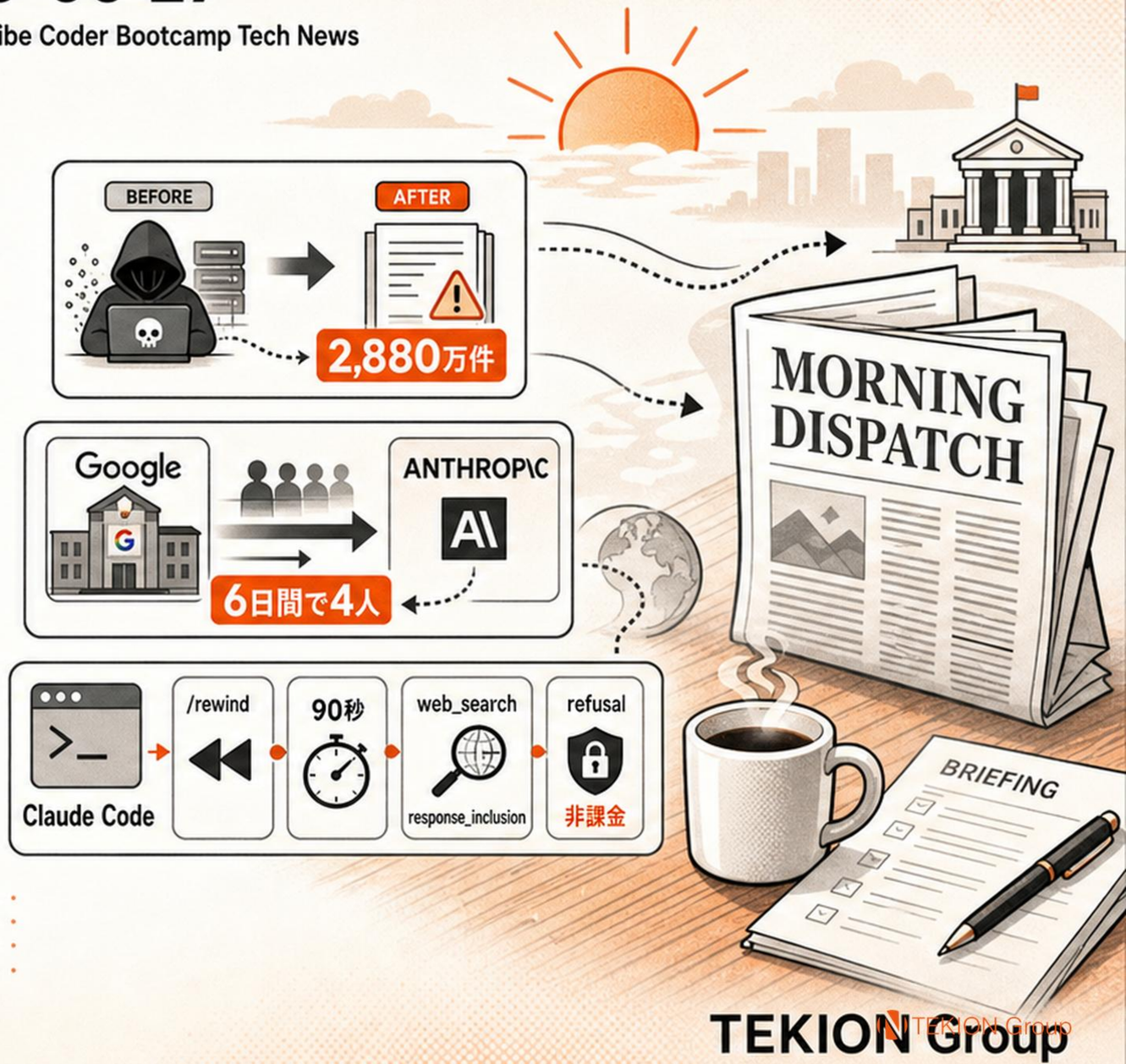
2026-06-27 — Vibe Coder Bootcamp Tech News

1. Anthropic、Alibaba「Qwen」による
過去最大級の蒸留攻撃を上院に告発 —
2,880万件 の不正やり取り、米議会は対中制裁修正案へ

2. Google から Anthropic への
AI 頭脳流出が止まらない —
Gemini の Adler・Pritzel が移籍、**6日間で4人** の連鎖

3. Claude Code & Developer Platform、
6月下旬の実務アップデート群 —
/rewind・**90秒** コード実行の明示・
web_search の response_inclusion・refusal は **非課金** に

4 トピックを整理。



TEKION Group

Tech News Daily
2026-06-27

🔎 Anthropic、Alibaba「Qwen」による過去最大級の蒸留攻撃を上院に告発 — 2,880万件の不正やり取り、米議会は対中制裁修正案へ

Bloomberg / Anthropic
👍 likes

🔍 何が起きた？

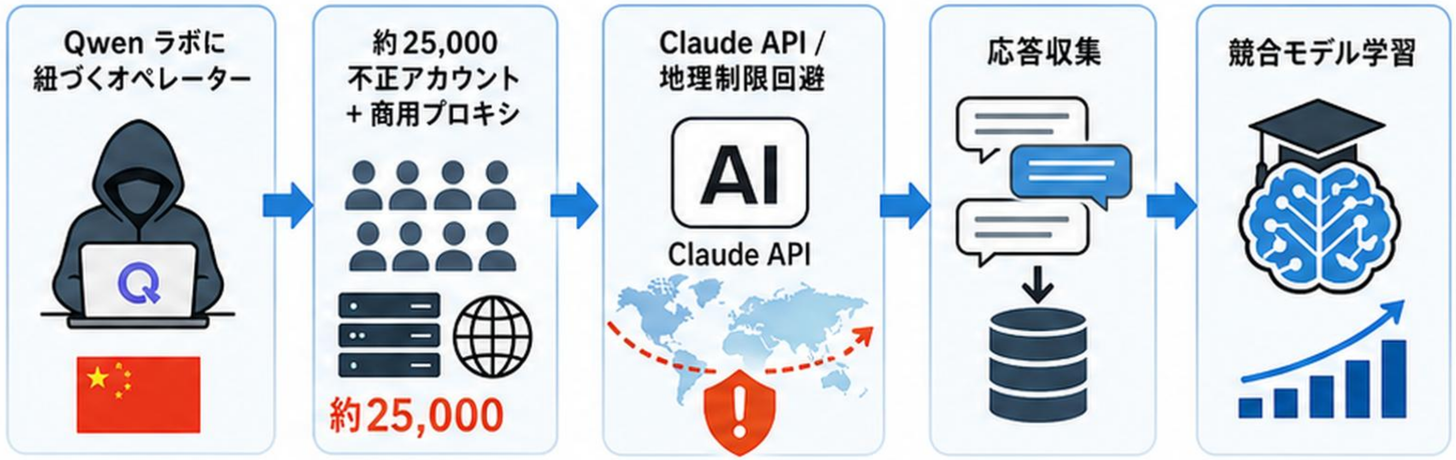
- Anthropic が、Alibaba の Qwen ラボに紐づくオペレーターが Claude に対し「過去最大級の敵対的蒸留(adversarial distillation)攻撃」を行ったと、米上院銀行委員会宛ての6/10付書簡で告発。Bloomberg が6/24に初報。
- 約25,000の不正アカウントと商用プロキシで地理制限を回避し、2026/4/22〜6/5の6週間で約2,880万件のやり取りを生成したとされる。
- 狙われた能力: エージェント推論、ソフトウェア工学、長期タスク遂行。

📌 主な変更点

- **規模:** 約25,000の不正アカウント、商用プロキシ、6週間、約2,880万件。中国エンティティを排除する地理制限を回避。
- **蒸留とは:** フロンティアモデルに大量クエリを投げ応答を収集し、安価な競合モデルの学習に使う手法。R&Dコストを払わず能力を再パッケージする行為。
- **議会の反応:** Hagerty・Andy Kim 両議員が、中国企業を制裁・ブラックリスト化する修正案を必須の国防法案へ。下院でも超党派の関連法案。

💡 なぜ重要？

- **法的シフト:** ToS 違反の枠を超え貿易法・制裁へ。公開APIへの大量クエリ行為の刑事枠組み化には懸念の声も。
- **前史:** 2026/2 に DeepSeek・Moonshot・MiniMax の3ラボで計1,600万件超。4月の OSTP Kratsios メモの警告後に起きた「警告無視」案件。



約 **2,880万件**
不正なやり取り数
(2026/4/22〜6/5)

6週間
攻撃期間
(2026/4/22〜6/5)

約 **25,000アカウント**
不正アカウント数
(+商用プロキシ)

米議会: 制裁・ブラックリスト化修正案

Hagerty・Andy Kim 両議員が、中国企業を制裁・ブラックリスト化する修正案を必須の国防法案へ。下院でも超党派の関連法案が進行中。

関連タイムライン (前史〜初報)

2026/2	2026/4	6/10	6/24
1,600万件超 (3ラボ合計)	OSTP Kratsios メモ (警告)	Anthropic 書簡 (上院宛て)	Bloomberg 初報

bloomberg.com / anthropic.com

TEKION Group
TEKION Group

🔍 Google から Anthropic への AI 頭脳流出が止まらない — Gemini の Adler・Pritzel が移籍、「6日間で4人」の連鎖

何が起きた？

Google の Gemini に主要貢献してきた研究者 Jonas Adler と Alexander Pritzel が Anthropic へ移籍する見込みと Bloomberg が 6/24に報じた。Adler は AI コーディング、Pritzel は事前学習(pretraining)が専門。

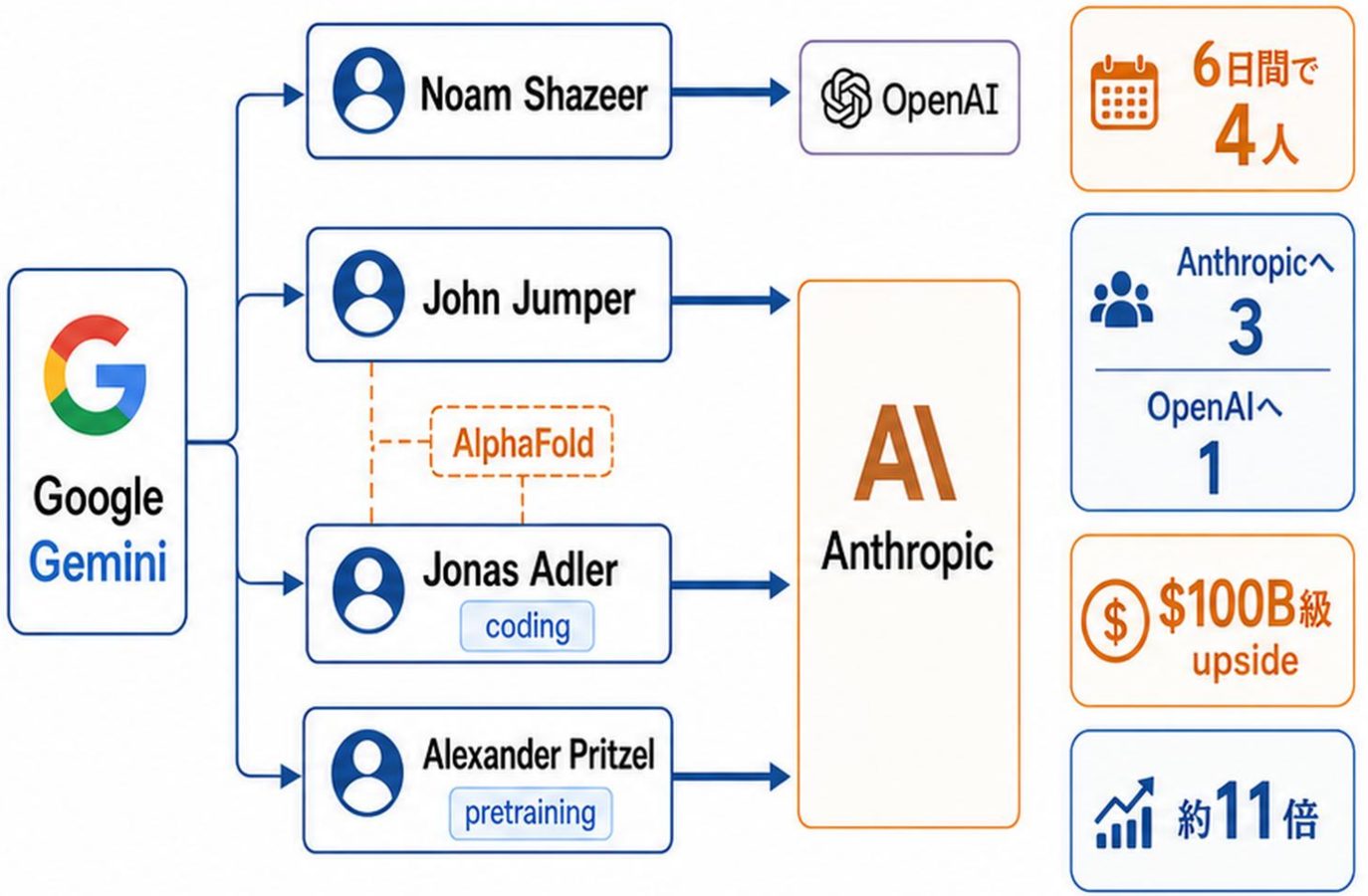
主な変更点

- **Adler:** AI コーディング研究。Cursor / Codex / Claude Code との競争に直結。
- **Pritzel:** pretraining 初期段階を担当。
- **John Jumper との縁:** 2人ともノーベル賞の AlphaFold 研究で Jumper と協働。
- **6日で4人:** Shazeer・Jumper・Adler・Pritzel。全員 Gemini 出身。

なぜ重要？

最大の引力は IPO 前のエクイティ。『Google は給与は出せても上場前の **$100B 級企業の upside は出せない**』。 計算資源配分の対立も背景。SignalFire 2025 分析では DeepMind エンジニアは逆方向の**約11倍** Anthropic へ流れやすい。

Gemini 人材流出マップ



Claude Code & Developer Platform、6月下旬の実務アップデート群 ― /rewind・90秒コード実行の明示・web_search の response_inclusion・refusal は非課金に

1 何が起きた？

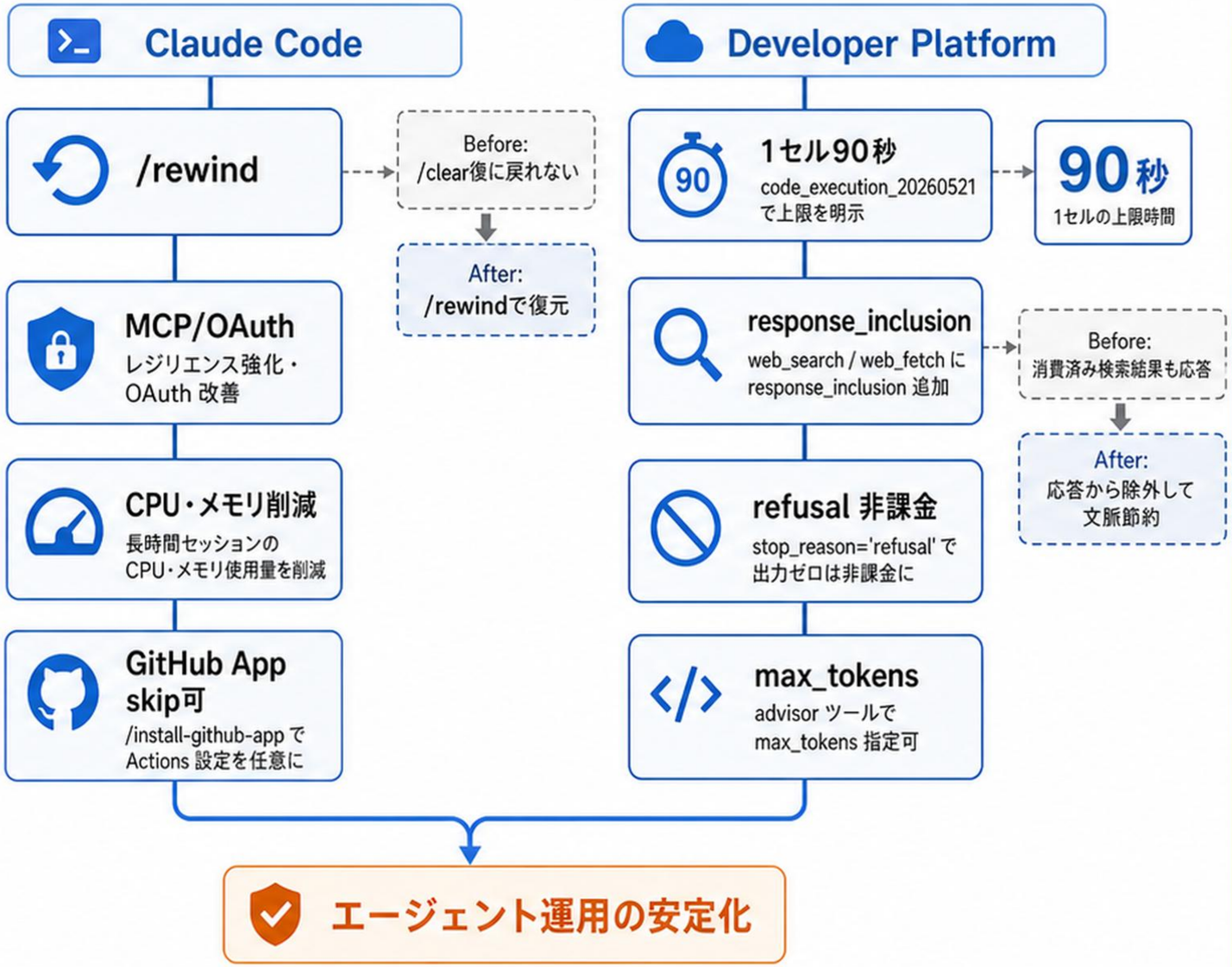
Anthropic が Claude Code 本体と Developer Platform で品質・実務系のアップデートをまとめて投入。Claude Code 側は /clear 前の会話を復元する /rewind や権限・MCP 周りの安定化、長時間セッションの CPU/メモリ削減。API 側は code execution の90秒上限の明示、web_search/web_fetch の応答制御追加、refusal の非課金化など、エージェント運用の細部が改善された。

2 主な変更点

- **Claude Code:** /rewind(/clear 前の会話復元)、バックグラウンドエージェント停止の恒久化、スクロール位置固定、MCP レジリエンス・OAuth 改善、長時間セッションの CPU・メモリ削減
- **/install-github-app:** GitHub Actions ワークフロー設定が任意に(App だけ入れて skip 可能)
- **code execution:** code_execution_20260521 で「1セル90秒」上限をツール説明に明示(beta ヘッダ不要)
- **web search/fetch:** web_search_20260318 / web_fetch_20260318 で response_inclusion 追加。消費済み結果ブロックを応答から落とせる(文脈節約)
- **課金:** stop_reason='refusal' で出力ゼロは非課金に。advisor ツールは max_tokens 指定可

3 なぜ重要？

エージェント運用で効くのは大機能だけでなく、復元・権限・MCP・応答ブロック・課金境界のような細部。長時間運用、検索付きワークフロー、GitHub 連携、拒否時のコスト管理が扱いやすくなる。



TEKION Group
TEKION Group
TEKION Slide Generator v5

Micron × Anthropic、AI インフラ供給で長期提携 — メモリ/ストレージ設計を「フロンティアモデルの要求」に直結、Series H にも出資

1 何が起きた？

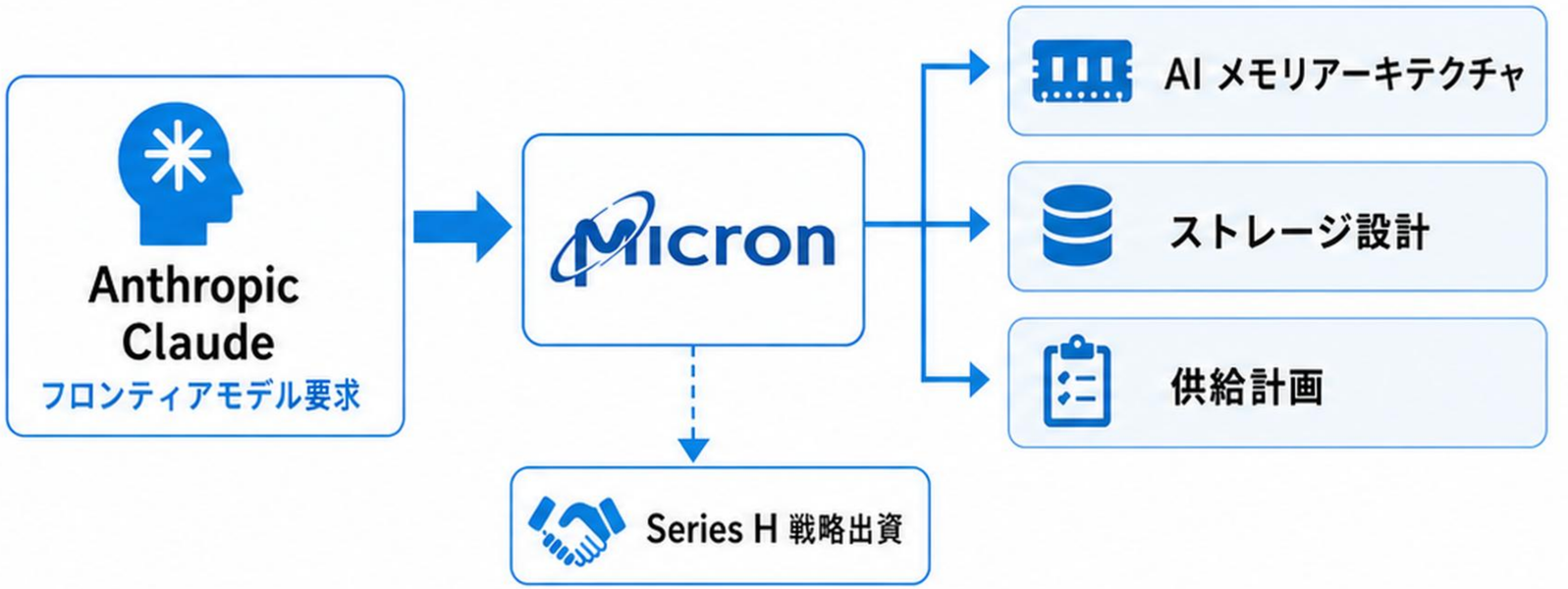
Micron と Anthropic が、AI インフラの供給で提携したと6/22に発表。

2 主な変更点

- AI メモリアーキテクチャ
- ストレージ設計
- 供給計画の連携
- Micron 社内での Claude 活用
- Anthropic への戦略出資

3 なぜ重要？

フロンティアモデルの要求を、インフラの設計・大規模展開に直接結びつける狙い。HBM/メモリ確保がフロンティア競争の制約条件に。



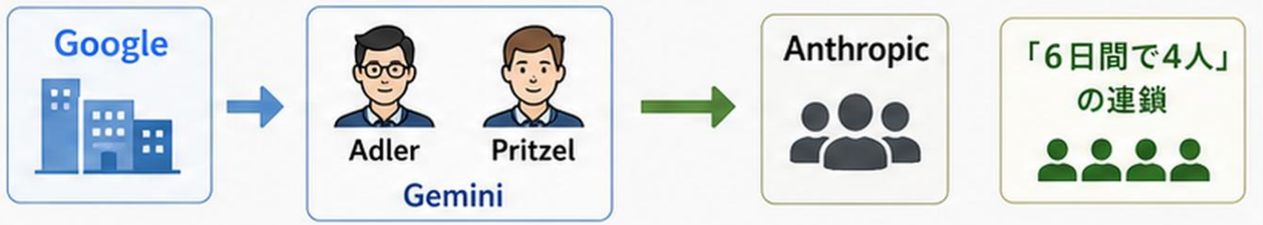
anthropic.com/...

今日のまとめ

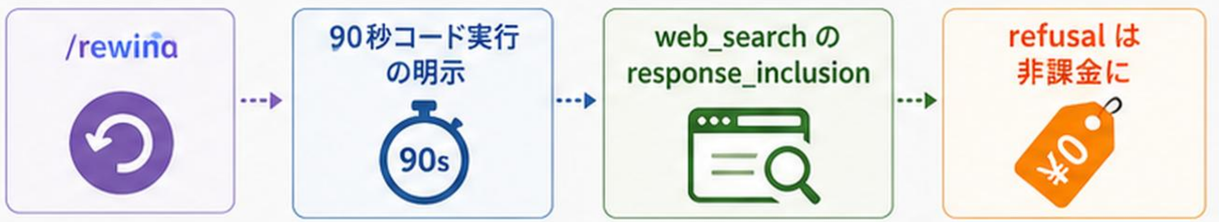
本日のトピック一覧

1 Anthropic、Alibaba「Qwen」による過去最大級の蒸留攻撃を上院に告発 — 2,880万件の不正やり取り、米議会は対中制裁修正案へ

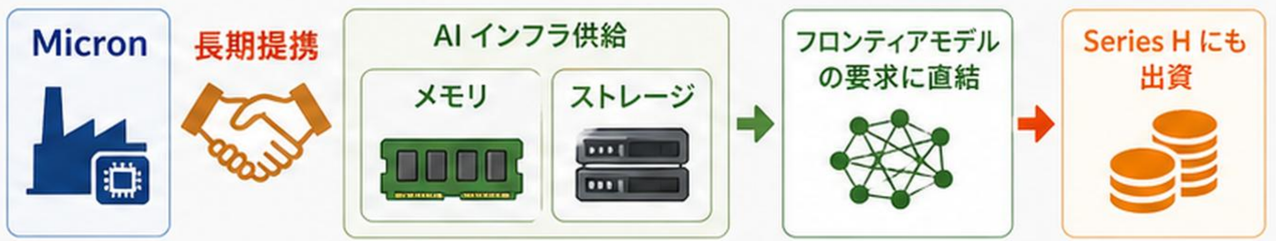
2 Google から Anthropic への AI 頭脳流出が止まらない — Gemini の Adler・Pritzel が移籍、「6日間で4人」の連鎖



3 Claude Code & Developer Platform、6月下旬の実務アップデート群 — /remind・90秒コード実行の明示・web_search の response_inclusion・refusal は非課金に



4 Micron × Anthropic、AI インフラ供給で長期提携 — メモリ/ストレージ設計を「フロンティアモデルの要求」に直結、Series H にも出資



情報ソース（まとめ）　OpenAI　Anthropic　Google

TEKION Group