NEWS

Tech
News
Daily

2026.05.01

MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホットな話題

1. **Gemini CLI v0.40.0**
   — tiered memory + 自動 skill 生成
2. **Anthropic claude-jupiter-v1-p**
   — 次世代 Claude を red team で実機テスト開始
3. **Anthropic Science Blog**
   — Claude が「専門家でも詰まる」生物学難問の 30% を解く

5 トピックを整理。

TEKION Group

Source: URL / noterebools.com / Design Instructions

Topic 1: Gemini CLI v0.40.0 — tiered memory + 自動 skill 生成

Gemini CLI (公式)

🔍 何が起きた？

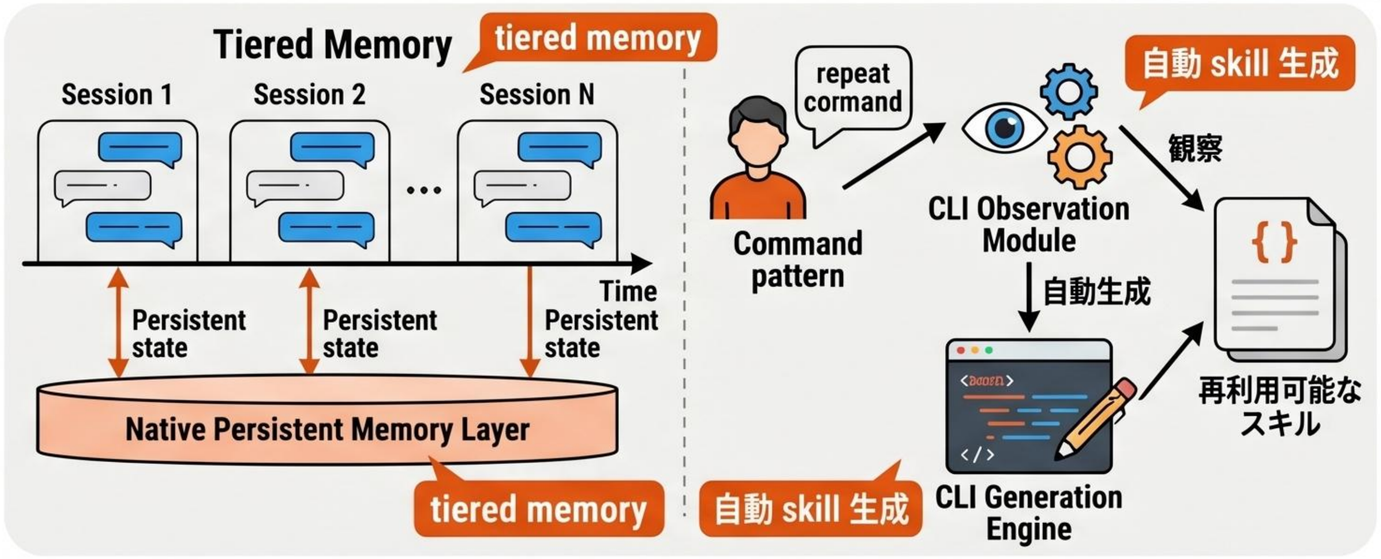
@geminicliが「v0.40.0」リリース。tiered memoryと自動skill生成機能をGoogle CLIにネイティブ実装。

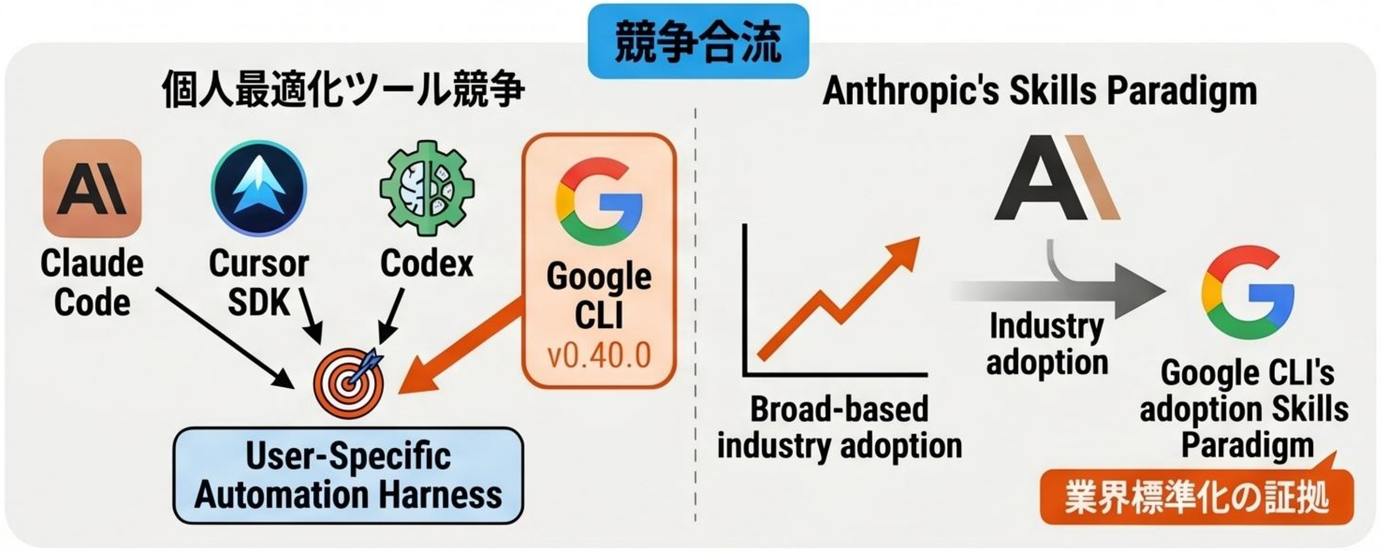
📌 主な変更点

- **tiered memory:** 会話セッションをまたく記憶レイヤーをCLIがネイティブに保持。
- **自動 skill 生成:** ユーザー操作パターンを観察し、CLI自身が再利用可能なskillを記述。
- **公式告知:** Gemini CLIチームによるv0.40.0の発表。

💡 なぜ重要？

- **競争合流:** Google CLIがClaude Code, Cursor SDK, Codexと並ぶ「ハーネスの個人最適化」競争へ本格合流。
- **業界標準化の証拠:** Anthropicの「skills思想」が業界デフォルトに近づいている追加証拠。





Topic 2: Anthropic claude-jupiter-v1-p — 次世代 Claude を red team で実機テスト開始

🔍 何が起きた？

@testingcatalog によるリーク情報。Anthropicの未発表の次世代 Claude モデルが実機テストに入ったことがが判明。

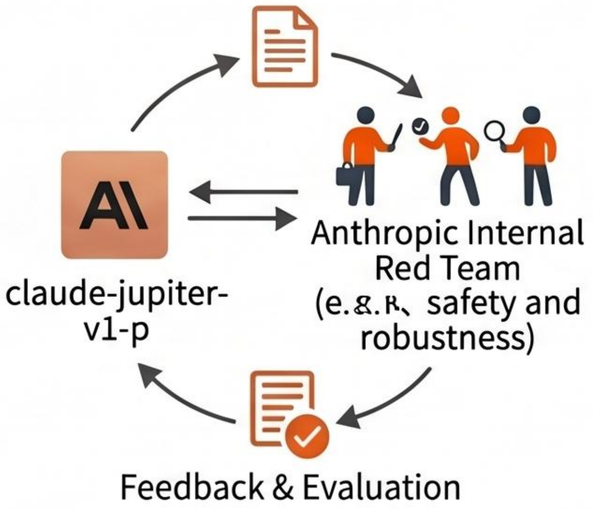
📌 主なポイント

- **モデル名:** `claude-jupiter-v1-p` (preview suffix)
- **状態:** `Anthropic 内部 red team´による評価中
- **情報源の信頼度:** `TestingCatalog は過去のリーク実績あり、そこそこ高い

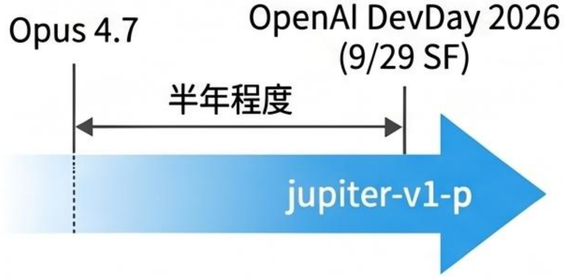
💡 リリースの可能性とタイミング

- **開発サイクル:** Opus 4.7から`半年程度`のスパンで次期Claude系モデルが来る可能性。
- **戦略的リリース:** OpenAI DevDay 2026（`9/29 SF）の前後で Anthropic がぶつけてくるシナリオも視野。

内部評価 (Red Team) フロー



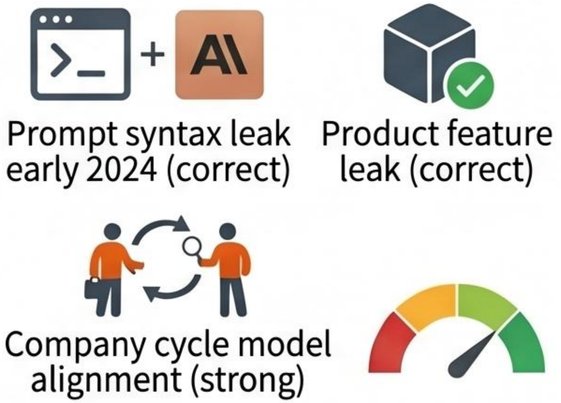
リリース予想タイムライン



リーク元の信頼度

モデル名: `jupiter-v1-p`
公開日: 2026-04-30
開発サイクル: `半年程度`
対抗イベント: OpenAI DevDay

リーク情報の信頼度 (TestingCatalog)



Tech News Daily

2026.04.30

Topic 3: Anthropic Science Blog — Claude が「専門家でも詰まる」生物学難問の 30% を解く

Anthropic公式

512 likes

🔬 研究の核心

最新 Claude が実バイオデータベースの生物学難問に取り組む。専門家が詰まった難問を含め、高い正答率を達成。

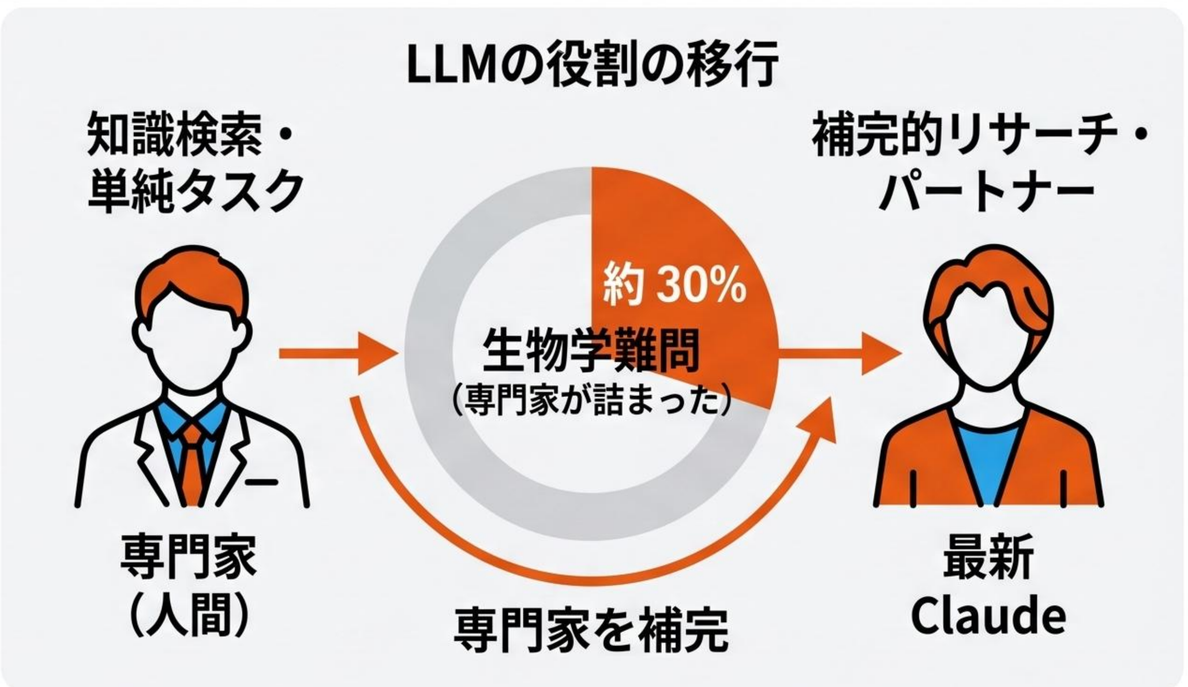
📊 主な知見

- 問題数: 99（実バイオデータベース）
- 専門家が詰まった問題: 23 / 99
- 最新 Claude の正答率: 詰まった 23 問のうち約 30%、その他もほぼ全問正答
- 一次情報: Anthropic 公式 Science Blog（X で告知）

🎯 含意

why-it-matters: LLM の役割が「知識検索」から「専門家を補完するリサーチ・パートナー」へと移行することを示す具体的な証拠。

問題数	専門家が詰まった	Claudeの正答率
99	23 / 99	約 30%
（実バイオデータベース）		（詰まった23問）



Source: x.com/AnthropicAI/...

TEKION Group

Topic 4: Google Gemini CLI に RCE 級脆弱性 — CLI 型 AI ツールのセキュリティ警鐘

🔍 何が起きた？

Gemini CLIにおいて、ホストシステム上で任意コマンドを実行可能にする『**リモートコード実行　（RCE）級脆弱性**』を発見。CLI型AIツール全体のセキュリティに警鐘を鳴らす事態となっている。

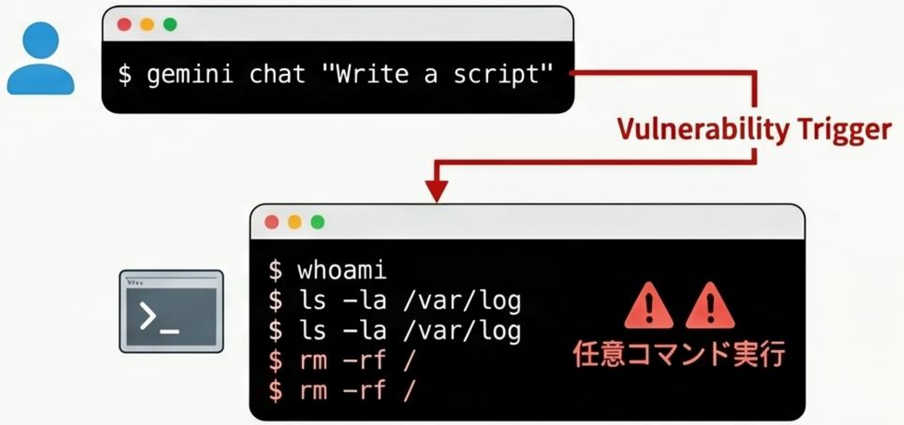
📌 主なポイント

- **影響:** Gemini CLI のホスト上で任意コマンド実行が可能
- **一次情報:** 元ソースリンク先の脆弱性レポート本文
- **Cursor 案件との地続き:** 4/28 の Cursor PocketOS インシデント（volume delete を本番 DB に実行）と地続きの文脈にある問題

💡 なぜ重要？

VBC / TekionがCLI型のAIツールをビジネス利用に入れる場合、**最小権限・専用ユーザー・コンテナ分離**を運用前提に格上げする必要がある。業界全体へ『**CLI内サンドボックス**』仕様標準化の圧力が高まる。

Google Gemini CLI RCE 脆弱性概念図



CLI型AIツールのセキュリティ警鐘と対策

Topic 5: Cursor SDK ローンチ — Cursor のランタイム/ハーネス/モデルでエージェントを構築可能に

🔎 何が起きた？

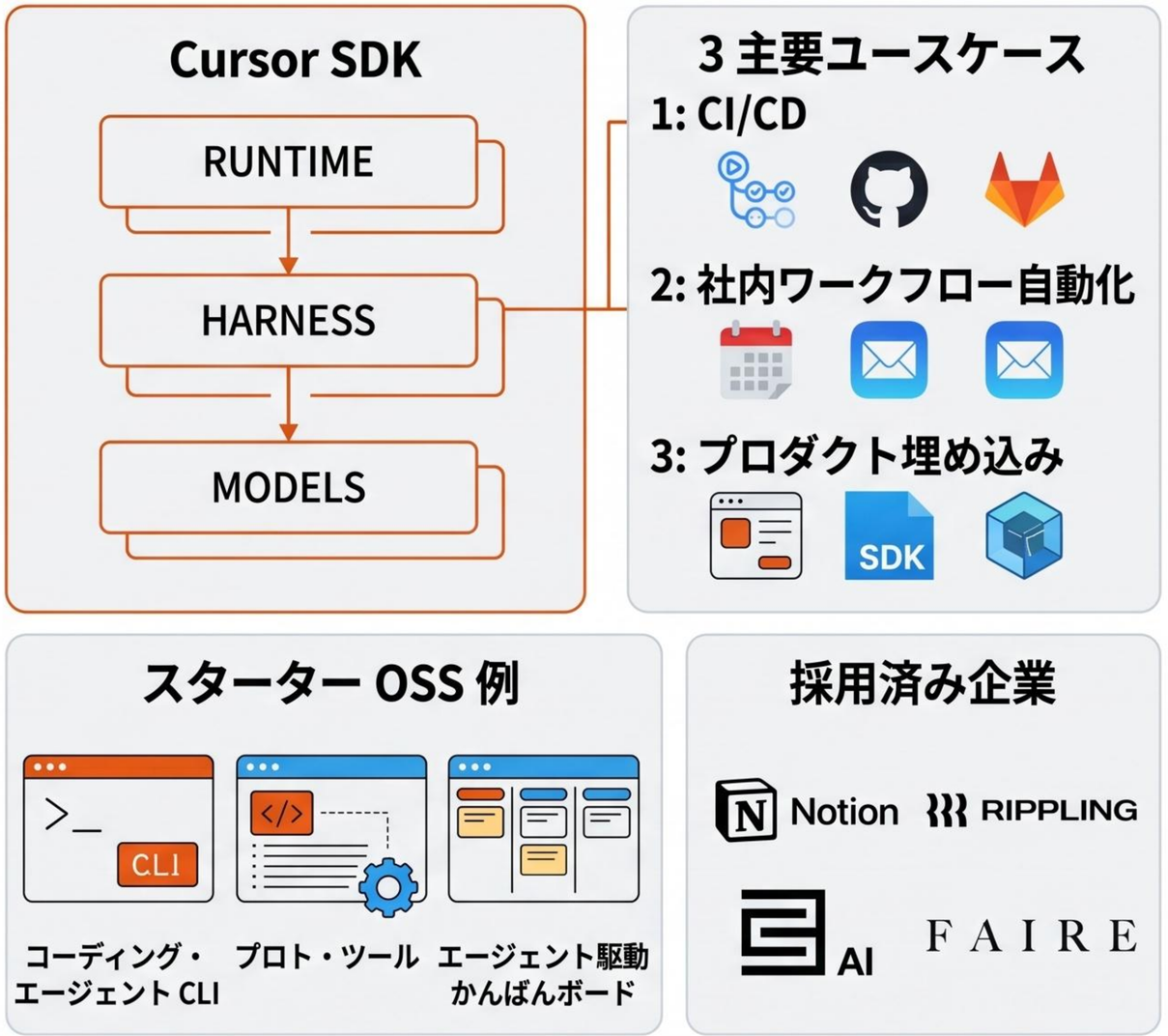
Cursorが、IDE体験を支える runtime + harness + models をSDKとして提供開始。コーディング・エージェントトの構築が容易に。

📌 主な変更点

- CursorのIDE技術をSDK化。
- 3ユースケース: CI/CD ／ 社内ワークフロー自動化 ／ プロダクト埋め込み。
- ローカル / Cursor クラウドを選択可能。
- スターターOSS: コーディング・エージェント CLI、プロト・ツール、エージェント駆動かんばんボード。
- 採用済み: Rippling, Notion, C3 AI, Faire.

💡 なぜ重要？

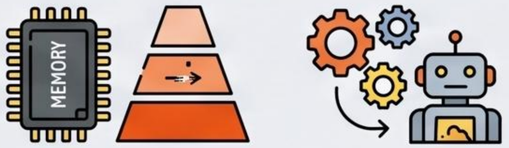
AIによるコーディング自動化が開発インフラとして定着。 企業独自のツール構築を加速。



本日のトピック一覧

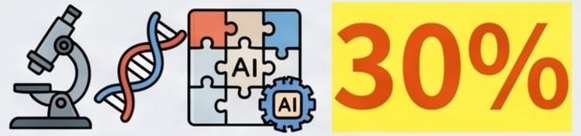
今日のまとめ

1. **Gemini CLI v0.40.0** — tiered memory + 自動 skill 生成



2. **Anthropic claude-jupiter-v1-p** —
次世代 Claude を red team で実機テスト開始

3. **Anthropic Science Blog** —
Claude が「専門家でも詰まる」生物学難問の 30% を解く



4. **Google Gemini CLI に RCE 級脆弱性** —
CLI 型 AI ツールのセキュリティ警鐘

5. **Cursor SDK ローンチ** —
Cursor のランタイム/ハーネス/モデルでエージェントを構築可能に

出典一覧のサマリ

TEKION Group