Tech News Daily

2026-05-13

MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホットな話題

- 🚨 「Mini Shai-Hulud」— TanStack 発の史上最悪級 npm サプライチェーン攻撃が、Claude Code / Mistral AI まで拡大
- Claude Code に「agent view」追加 — 全セッションを 1 ビューで管理する research preview
- Gemini Omni — Google の新動画生成モデル、生成動画内のテキスト整合性が破格

5 トピックを整理。

TEKION Group

「Mini Shai-Hulud」— TanStack 発の史上最悪級 npm サプライチェーン攻撃が、Claude Code / Mistral AI まで拡大

(@IntCyberDigest)

16k+ likes

🔎 何が起きた？

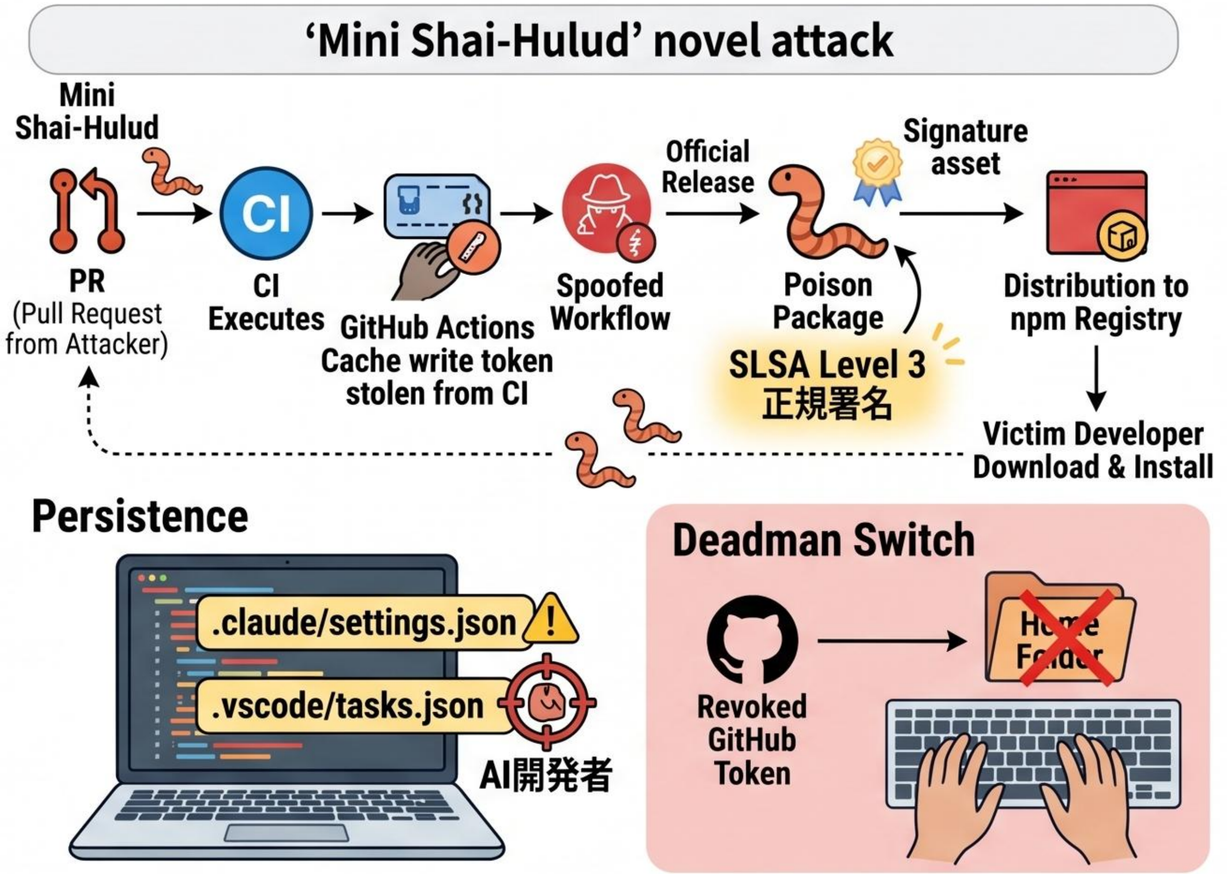
- 5/11〜12、TanStackの公式npmパッケージに毒が混入。攻撃はわずか1日で170+パッケージへ連鎖し「Mini Shai-Hulud」キャンペーンと命名。

📌 主な変更点

- TanStack公式 42パッケージ・84バージョン感染（react-router週1,200万DL）。
- OpenSearch / Mistral AI / UiPath / Guardrails AI / Squawkへ拡散。
- PRのCI経由でGitHub Actions Cacheトークン窃取。SLSA 3級正規署名付きで悪意あるパッケージを公開。
- 被害者の `~/.claude/settings.json` と `~/.vscode/tasks.json` を書き換えて永続化。npm uninstallでも除去不可。AI開発者が最大被害層。

💡 なぜ重要？

- セキュリティクラスタに衝撃。「史上初の有効署名付きnpmワーム」「SLSAも信頼できなくなった」と警鐘。
- 中華圏解説（@AYi_AInotes）：「AI Agent経由の自動インストールが最危険」。日本のシニアエンジニア（@kenn等）も警告。
- 盗んだGitHub token撤回時にhomeディレクトリを丸ごと消し去るデッドマンスイッチ搭載。
- Ryan Carson「今すぐ npm install を止めて全員自査せよ」と緊急呼びかけ。



「今すぐ npm install を止めて全員自査せよ」

- 42 パッケージ/84 バージョン 感染
- 週 1,200万ダウンロード (react-router)
- 170+ 連鎖パッケージ (OpenSearch, Mistral AI 等)

🏷️ Claude Code に「agent view」追加 — 全セッションを 1 ビューで管理する research preview

Anthropic公式

🔍 何が起きた？

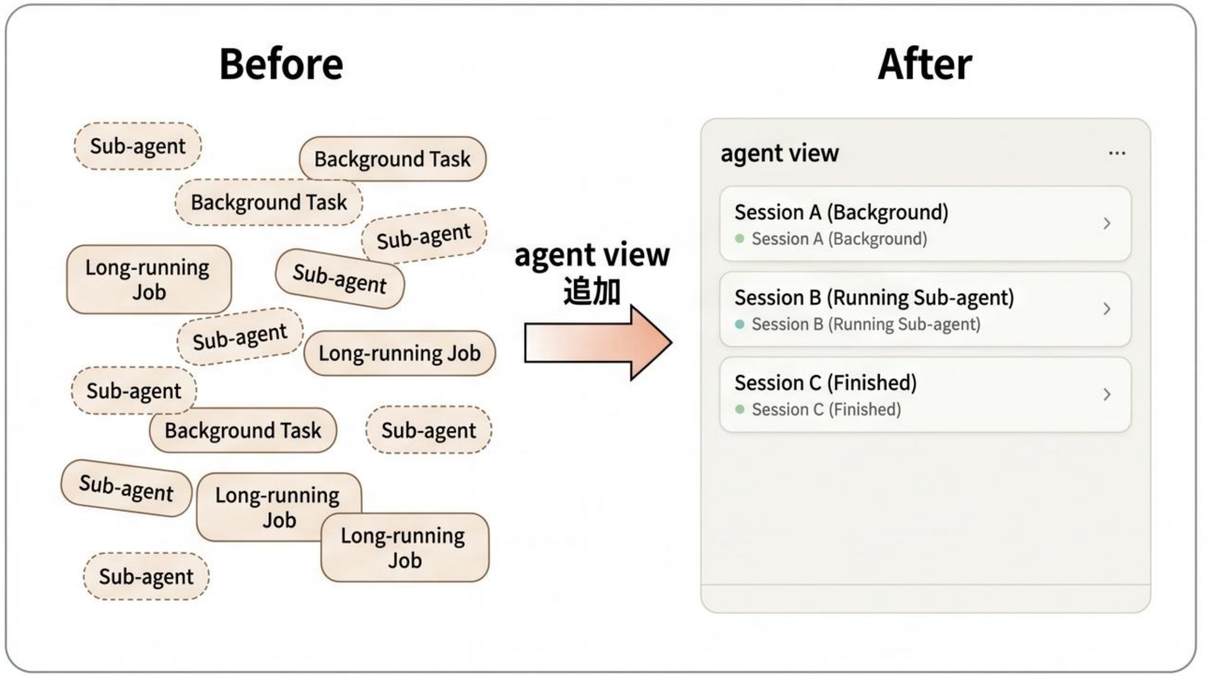
Anthropic が Claude Code 公式アカウントから、新機能 **agent view** の research preview 提供開始を発表。複数の Claude Code セッション（バックグラウンドタスク、並列サブエージェント、長時間ジョブ）を 1 つのリストで横断的に管理できる UI。

📌 主な変更点

- "agent view" として本日 research preview 公開
- 全セッションが 1 つのリストで並ぶ
- バックグラウンド / 並列サブエージェント運用の見える化
- Claude Code 2.1.139 と同時期のリリースで、`/goal` コマンドなど 50 件の CLI 変更も同梱

💡 なぜ重要？

これまで散らばっていた並列実行コンテキストが、ようやく公式 UI で可視化される。



📝 数字ハイライト

50

CLI 変更件数
（/goal コマンド含む）

X での反応

「並列エージェント運用ようやく公式に支援された」
「Vibe Coder Bootcamp で教えるネタが増えた」

Gemini Omni — Google の新動画生成モデル、生成動画内のテキスト整合性が破格

🔍 何が起きた？

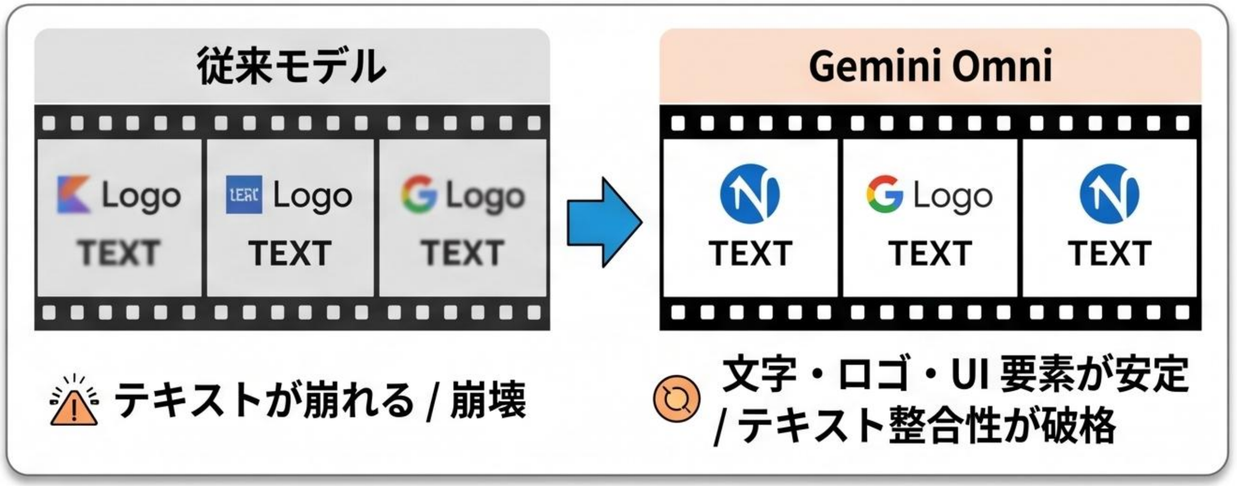
Google Gemini App が新動画生成モデル **Gemini Omni** を公開。chetaslua が最初の出力を共有し「Hollllyyyyy 😳😳 Geminiやりやがった」と評価。

📌 主な変更点 / 特徴

最大のブレイクスルーは **生成動画内のテキスト整合性** で、フレーム間で文字・ロゴ・UI 要素が崩れない。これは Sora2 / Veo3 / Runway 等が苦戦していた領域であり、UI 説明動画やプロモ動画用途で一気に実用域へ。

💡 なぜ重要？ / 波及効果

X 上のクリエイティブ系アカウントが「Sora2 と比べてて文字が崩れない」「ようやくロゴが入れられる」と歓迎。動画モデル戦線が再加熱。Gemini App から発表、@GeminiApp が公式チャンネル。



x.com/GeminiApp/...

Tech News Daily

2026-05-13

Karpathy が指摘した LLM 最大のボトルネックは「テキストという最低帯域幅の出力フォーマット」

Andrej Karpathy公式
Karpathy Tips
1.2K likes

要点

Andrej Karpathy が公開したワンライナー Tips：**クエリ末尾に「structure your response as HTML」と書く**だけで、LLM は見出し・表・リスト・強調を駆使した HTML を返してくれる。ブラウザで開けば、プレーンテキストよりはるかに読みやすい。

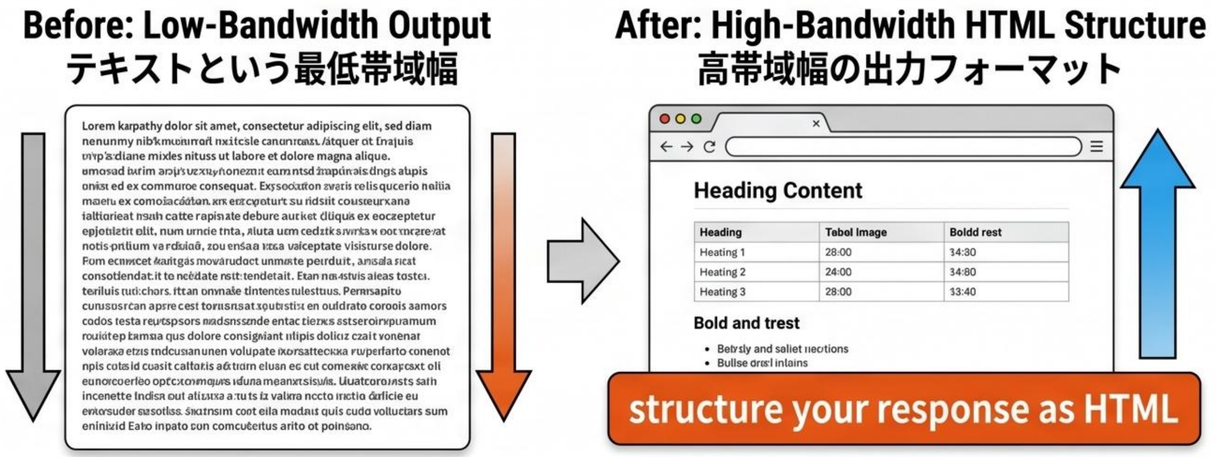
具体的な手法 / 使いどころ

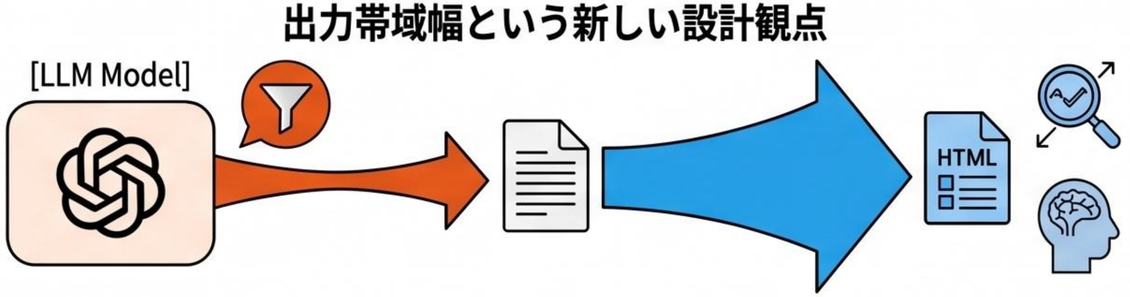
- クエリ末尾に1行「structure your response as HTML」を足すだけ。
- Slack 配信は記法上限あり → HTML レポート別添リンクの設計検討に直結。

なぜ刺さるか / 学び

これに対し @AYi_AInotes が中国語で**「現在の AI 最大のボトルネックはモデルの賢さではなく、テキストという最低帯域幅の出力フォーマット」**と長文展開し、「半年分 AI ワークフローが覆された」と話題に。

みんなより強いモデル・より大きいコンテキストを待っているが、実は**出力チャネルの帯域幅を上げる**ほうが先決という発想転換。プロンプト工学の基本だが見落としていた」というコメント多数。





Xでの反応

@AYi_AInotes「半年分の AI ワークフローが覆された」

日本の AI クラスタ プロンプト工学の基本だが見落としていた」

x.com/OpenAI/...

TEKION Group

🏷️ Agentmemory — Claude Code / Codex / Hermes に「無料で無限メモリ」を付与する OSS が GitHub トレンド入り

GitHub & Community

1.2k

🔍 何が起きた？

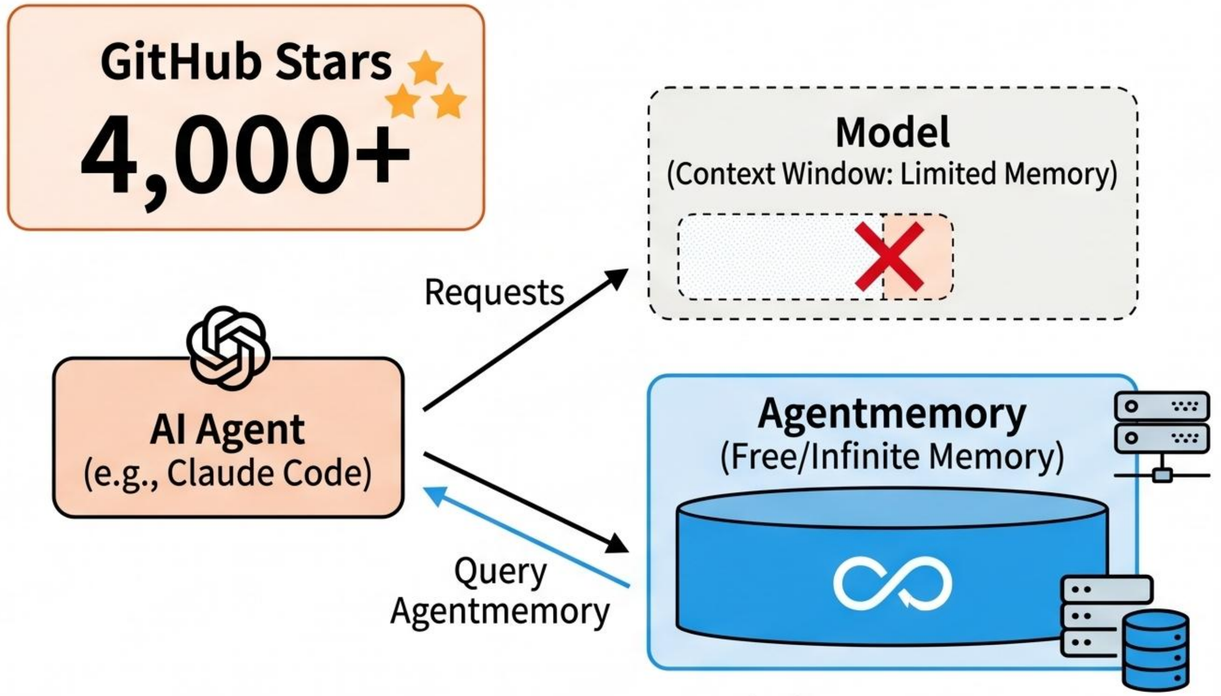
OSS プロジェクト「Agentmemory」が GitHub で急速に注目を集めている。4,000+ stars を獲得しトレンド入り。主要 AI エージェント（Hermes / Claude Code / Codex）に「無料で無限メモリ」を付与する画期的なレイヤとして機能する。

📌 主な機能・特徴

- 反応: GitHub stars 4,000+
- Hermes / Claude Code / Codex に対応
- 完全無料
- ローカル DB 系の長期記憶ストアの可能性が高い

🌱 なぜ重要？

AI エージェントの最大の課題である「コンテキストウィンドウの制約」を回避し、長期記憶をシームレスに統合できる可能性があるため。開発者が自前でメモリ層を構築する手間を省ける点も大きい。



Agentmemory システム概念図

Xでの反応' Quote Card

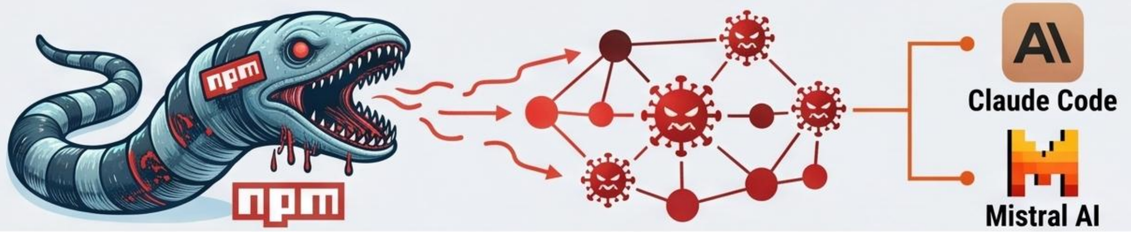
自前で memory レイヤを書いていた人にとって朗報

MCP サーバ形態か、ラッパー CLI かで使い勝手が変わる

本日のトピック一覧

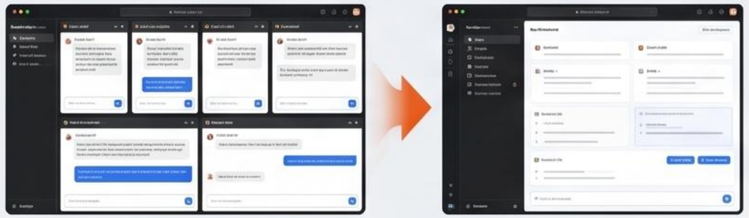
1 Mini Shai-Hulud

Worst-ever npm supply chain attack (TanStack), expanding to Claude Code / Mistral AI



2 Claude Code: 「agent view」

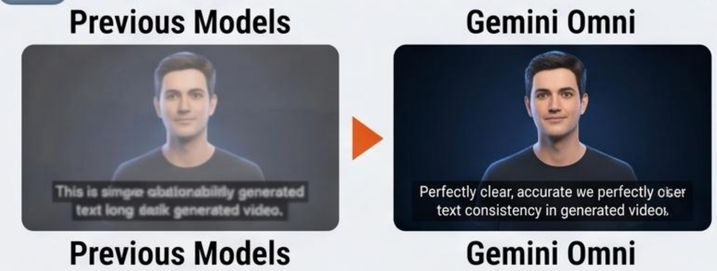
Research preview: Manage all sessions in 1 view



3 Gemini Omni

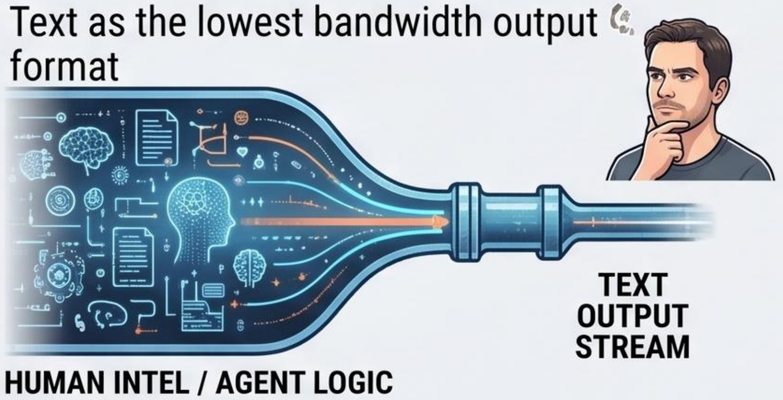
Google's new video generation model: Unprecedented text consistency in generated videos

3 Gemini Omni



4 Karpathy on LLM Bottleneck

Text as the lowest bandwidth output format



5 Agentmemory (OSS)

Free, unlimited memory for Claude Code, Codex, Hermes. GitHub Trending

Source of orgins: Anthropic, Google, Google, Ewatan, Enth, Imptel, Biotornet, Antentmemory...