Tech News Daily

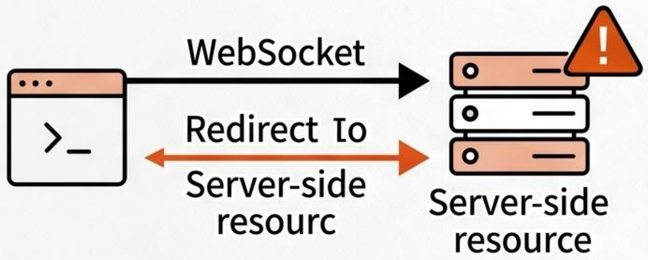
2026-05-16.

MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホットな話題

Next.js
WebSocket Upgrade SSRF
CVSS 8.6

Next.js CVE-2026-44578
過去最悪の WebSocket Upgrade SSRF (CVSS 8.6)



ANTHROP\C
分離

Anthropic Claude Code SDK Program
専用月次クレジットに分離 (6/15 開始)

npm

「Mini Shai-Hulud」攻撃
AI 開発者ツール標的に拡大 ── TanStack 42 公式パッケージ感染

7 トピックを整理。

TEKION Group

Topic 1: Next.js CVE-2026-44578 — 過去最悪の WebSocket Upgrade SSRF(CVSS 8.6)

Star_Knight12 + modat_magnify
❤ likes

🔎 何が起きた？

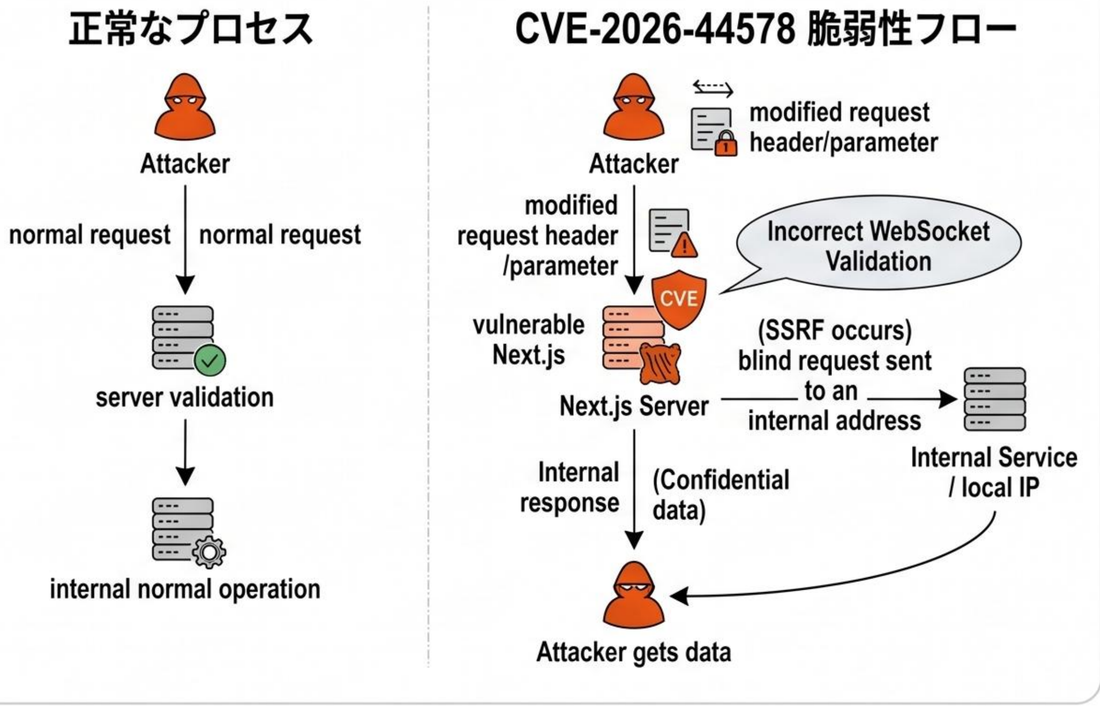
Next.jsに重大な脆弱性（CVE-2026-44578）が発見された。これは「過去最悪の WebSocket Upgrade SSRF」と評価されている。

📌 主な変更点

- 特定の WebSocket アップグレード・リクエストにおける不適切な検証が原因。
- サーバーサイド・リクエスト・フォージェリ（SSRF）を誘発し、内部ネットワーク情報が漏洩する危険性。
- CVSS スコアは非常に高い「8.6」に達している。

💡 なぜ重要？

- 多くのウェブアプリケーションでNext.jsが採用されており、WebSocketを利用するリアルタイム機能が標的となる可能性があるため。



CVE-2026-44578
Identifier

CVSS 8.6
Severity Score (out of 10)

Tech News Daily
2026-05-16

Topic 2: Anthropic、Claude Code SDK プログラム利用を 「専用月次クレジット」に分離 (6/15開始)

likes

Source: ClaudeDevs

🔍 何が起きた？

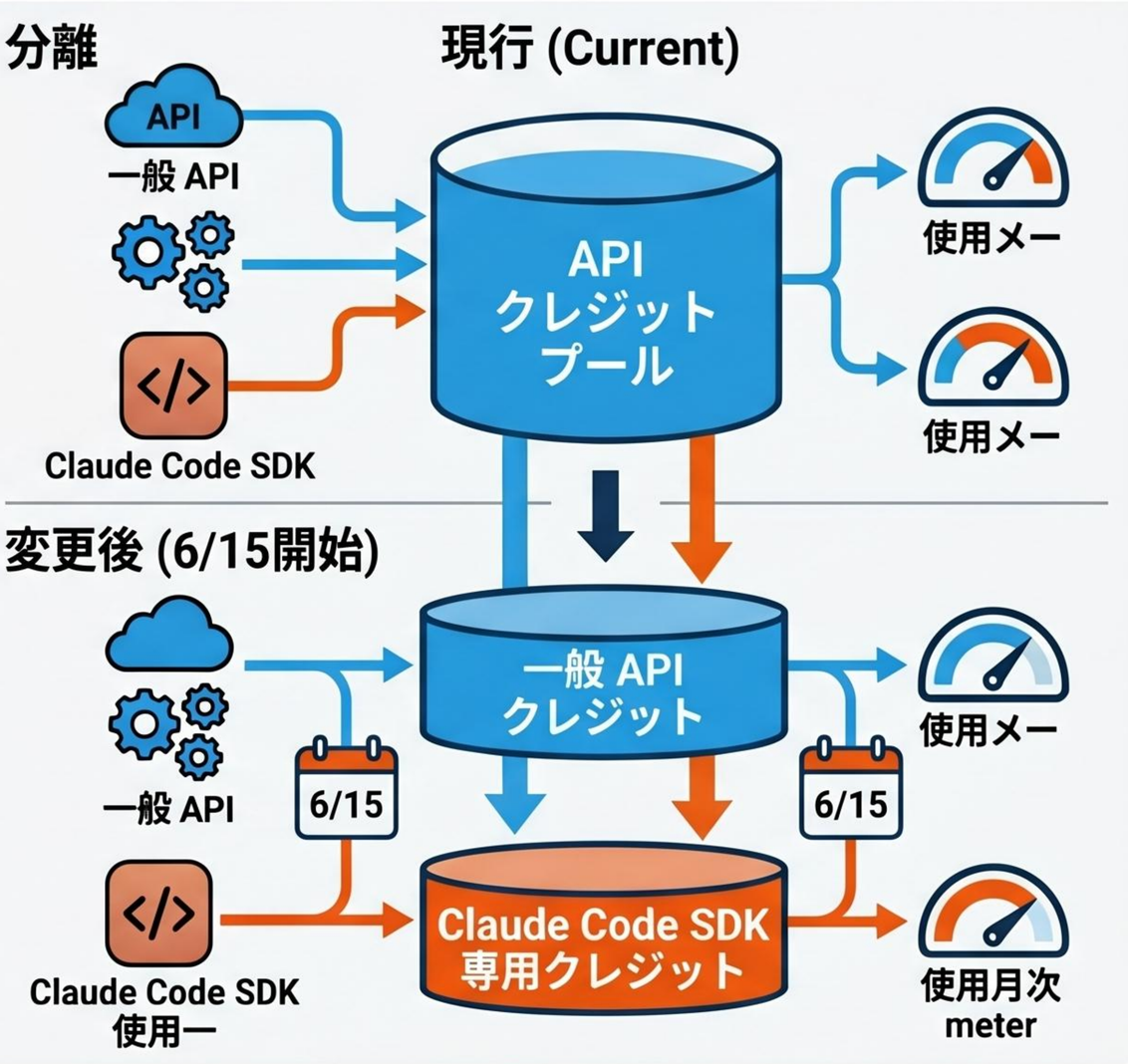
Anthropic が発表した新たな構造変更。Claude Code SDK プログラム利用は、既存の一般 API と分離され、新たに導入される専用の「専用月次クレジット」制に移行する。

📌 主な変更点

- **対象:** Claude Code SDK プログラム利用
- **変更:** 専用月次クレジットに分離
- **開始日:** 2026年6月15日
- SDK 専用のリソースの専用管理

💡 なぜ重要？

- 予測がある SDK 計算を値
- コード生成の開発コストの追跡トックが強化
- リソース配置を最適化



TEKION Group

Topic 3: npm「Mini Shai-Hulud」攻撃
AI 開発者ツール標的に拡大 — TanStack 42 公式パッケージ感染

🔎 何が起きた？

npmエコシステムで「Mini Shai-Hulud」と呼ばれる供給網攻撃が発見。AI開発者ツールをターゲットにし、具体的には「TanStack」プロジェクトの42個の公式パッケージが感染。

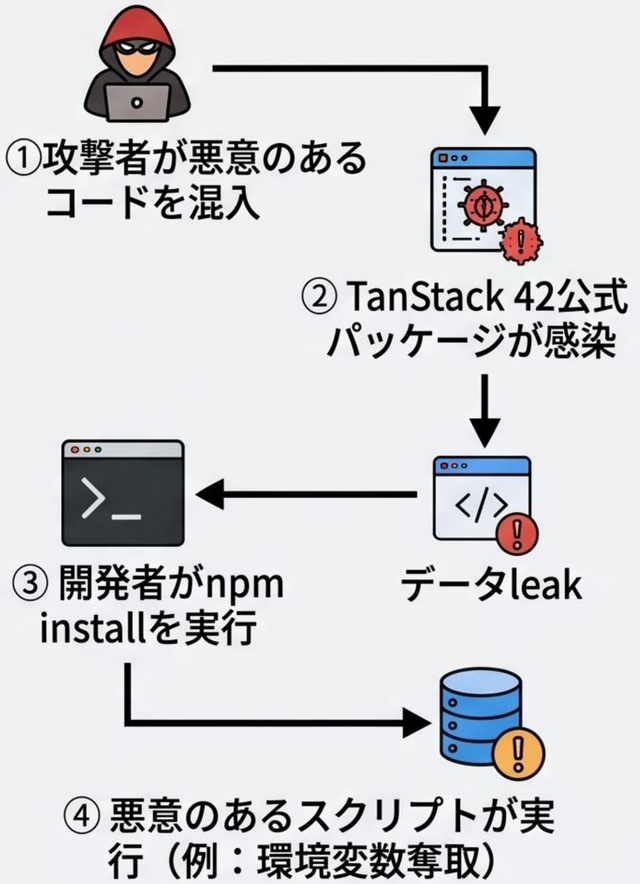
📌 主な変更点

- 攻撃はAI開発ツールの人気パッケージを標的。
- TanStack 42パッケージに悪意のあるコードを混入。
- 開発者のビルド環境を狙う典型的な供給網攻撃。

💡 なぜ重要？

- 人気エコシステムの信頼を損なう深刻な脅威。
- AI開発者のセキュリティ意識向上が急務。
- 公式パッケージでも安心できない現状を露呈。

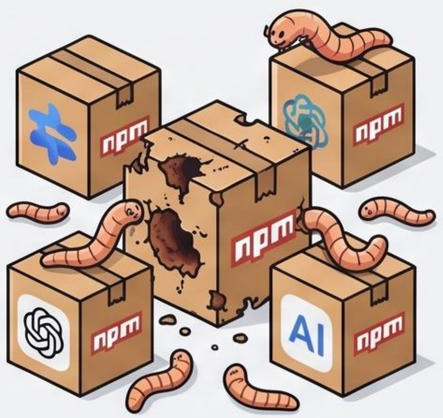
攻撃の流れ



数字ハイライト

42

感染パッケージ数: 42



Topic 4: Karpathy「LLM の問いに『HTML で構造化』を足すだけ」— 半年分の AI ワークフロー覆す Tips

Andrej Karpathy / AYi 解説 / Thariq

💡 要点

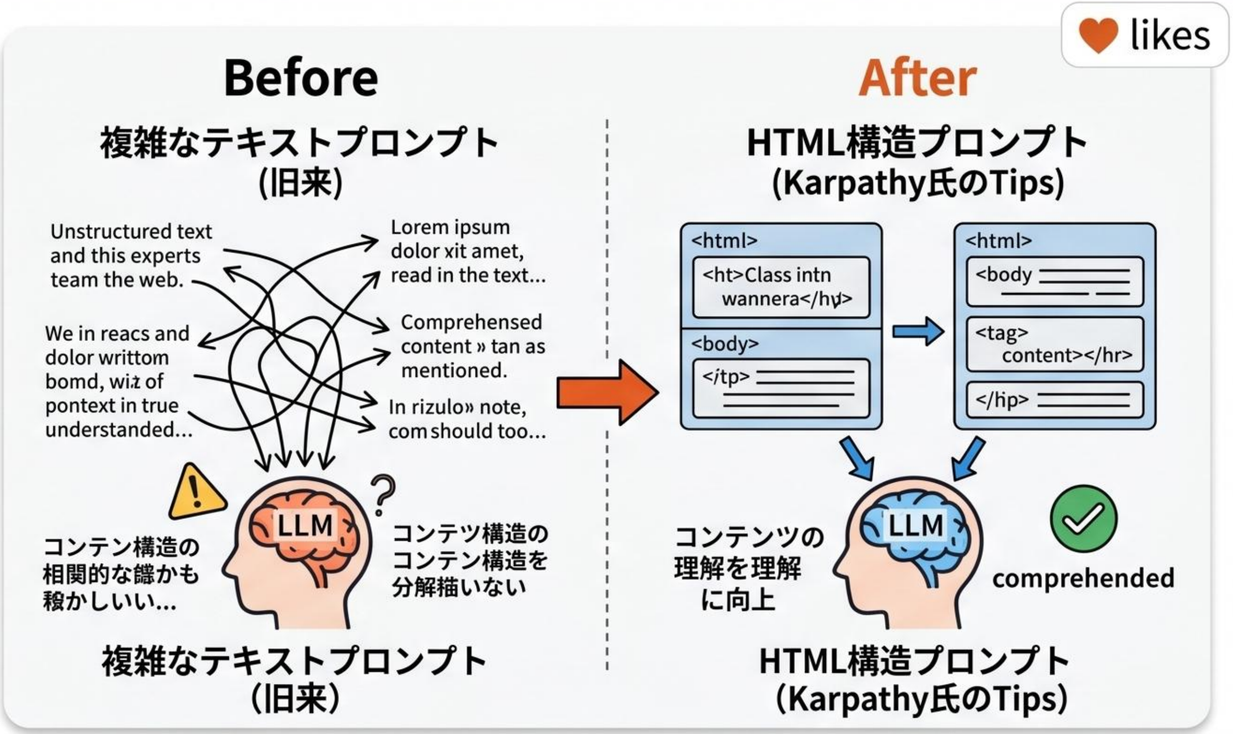
- Andrej KarpathyがLLM の問いに『 HTML で構造化を足すけ」をシンプルチプが紹介ました
- 最後に複雑なプロンプトエンジ:ニングワークフローの半年分のAI覆すも単化

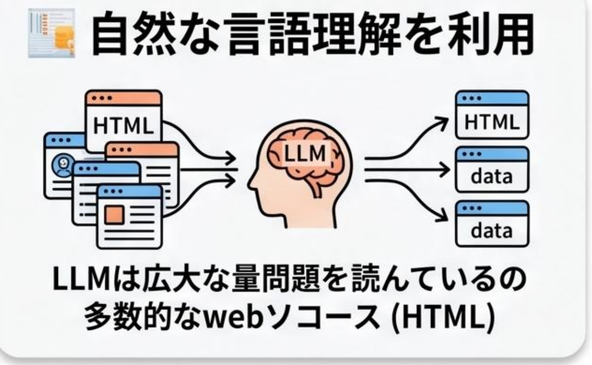
🛠️ 具体的な手法 / 使いどころ

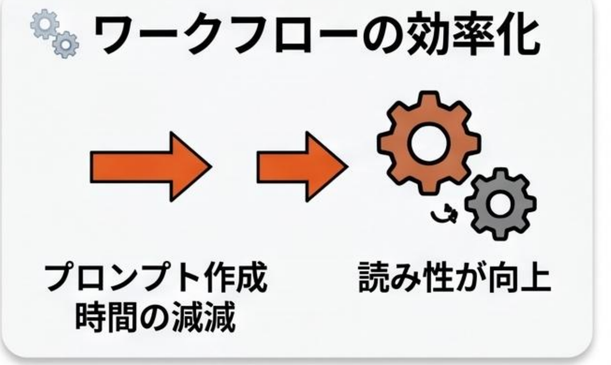
- プロンプト要素をセミみにも的な HTML タグをランプなど（<concept>、<example>）を包活
- 複雑なの指着、リスト、 コンテクストなどに石ンプに包える方法

🌱 なぜ刺さるか / 学び

- Webから広大トレーニングデータからかHTMLの臓ILL構造をの深いする深いな理解いがある
- これは簡化的も簡化で簡単にかつめる
- プレトレーニングの核心の強調をご利用したら回り返る







Topic 5: Claude Code 2.1.139 リリース — /goal コマンド追加 + push 通知 + agent view

1.2k likes

ClaudeCodeLog / ClaudeDevs (X)

🔍 何が起きた？

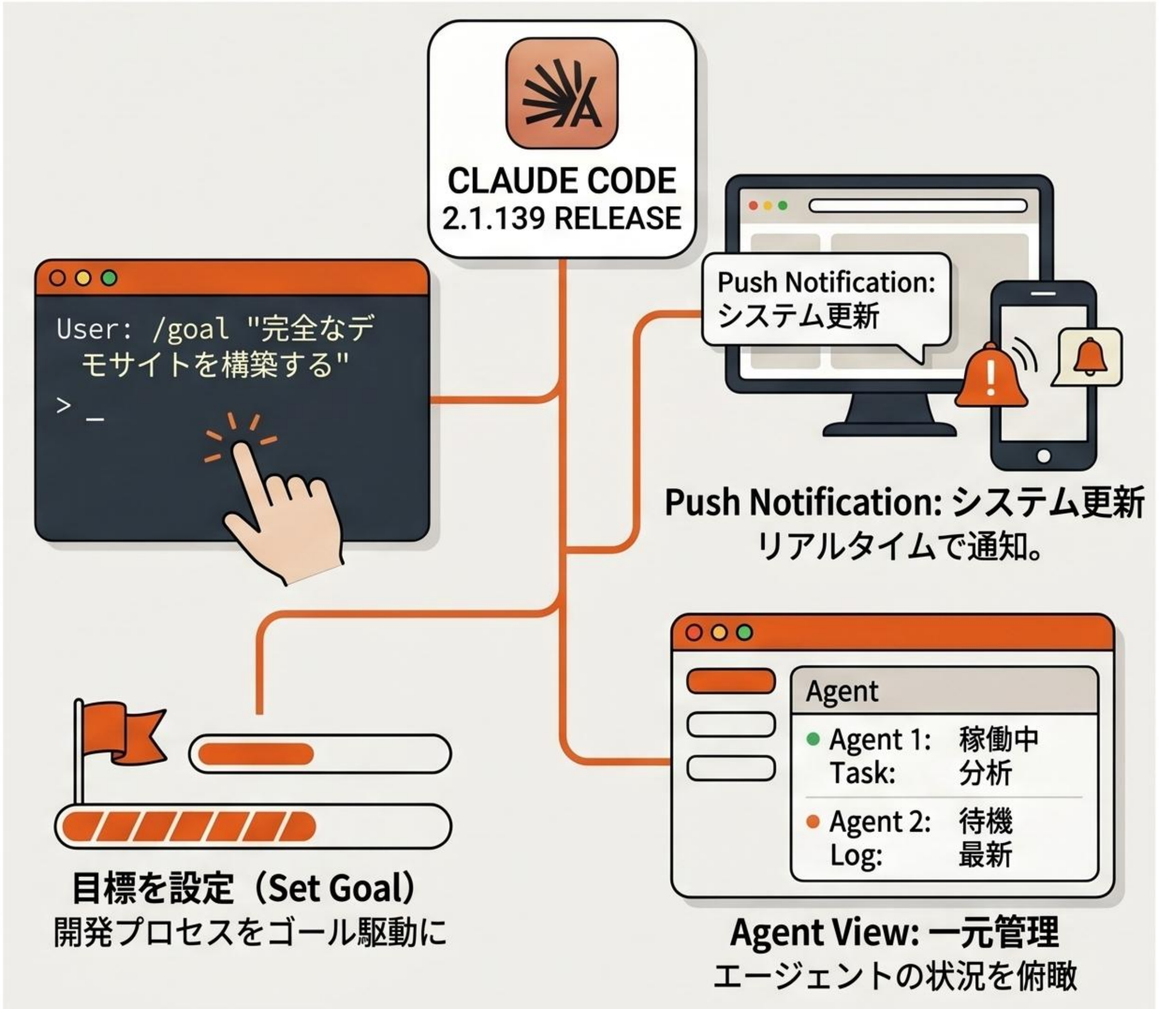
Claude Code のバージョン 2.1.139 がリリースされました。**X** の公式 changelog で発表。`/goal コマンド、Push 通知、Agent View という主要機能が追加されました。

📌 主な変更点

1. **/goal コマンド**: 開発目標（ゴール）を明示的に設定・共有可能に。
2. **Push 通知**: システムやプロジェクトの変更情報をリアルタイムに受信。
3. **Agent View**: 複数のエージェントの状況を一目で把握できる専用ビュー。

💡 なぜ重要？

1. **目標主導の開発**: ‘/goal`でプロセスを明確化、効率化。
2. **透明性の向上**: 通知とビューで進捗管理。
3. **円滑なワークフロー**: エージェント管理を容易に。



Topic 6: Claude API プロンプトキャッシュ「事前ウォーム」Tips — TTFT 大幅短縮

💡 要点

- Claude APIにおけるプロンプトキャッシュの効果的な利用法を紹介。
- 事前ウォームにより、TTFT（Time To First Token）を大幅に短縮可能。

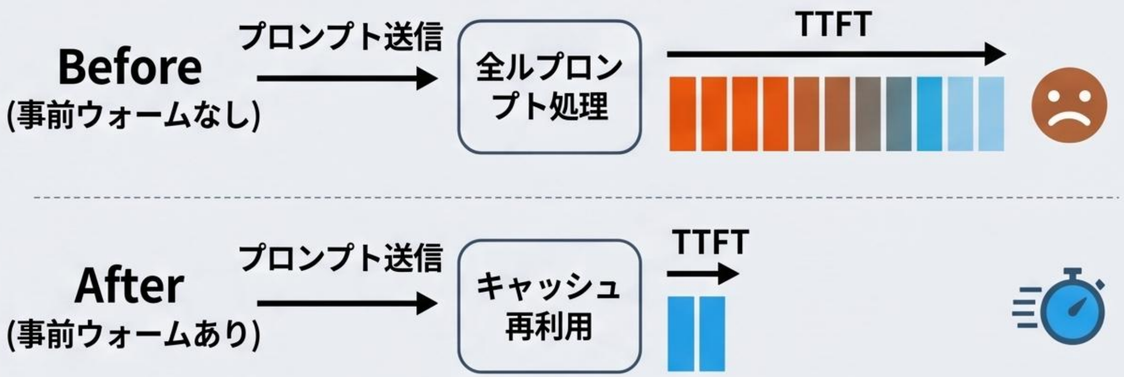
🛠️ 具体的な手法 / 使いどころ

- 頻繁に使用されるプロンプトや、長いシステムプロンプト、ドキュメント情報をキャッシュ。
- 最初の呼び出しでキャッシュを作成し、後続の呼び出しで再利用。
- 使いどころ：チャットボット、要約システム、ドキュメント分析など、同一情報を繰り返し利用するシーン。

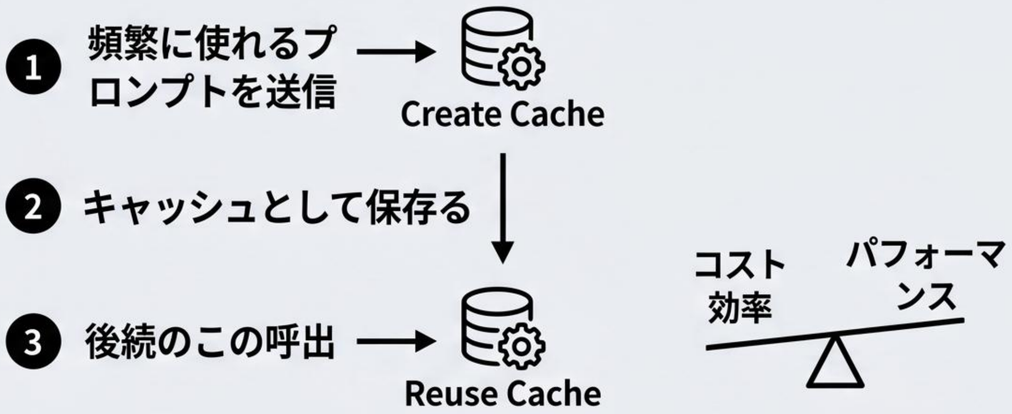
🌱 なぜ刺さるか / 学び

- API呼び出しのレスポンス速度向上はユーザー体験に直結。
- コスト効率とパフォーマンスのバランスを最適化する重要テクニック。

TTFT 大幅短縮



プロンプトキャッシュのフロー



Topic 7: Notion 公式 CLI `ntn` リリース — Notion API がターミナルから操作可能に

🔎 何が起きた？

Notion開発チームが公式CLI `ntn` をリリース。
Notion APIをターミナルから直接操作可能に。
開発者向けの強力なツール。

📌 主な変更点

- ターミナル上でNotionのリソース操作（ページ取得、作成、ブロック編集など）が可能に。
- APIキーの管理やリクエストの構成が簡素化。
- 既存のAPIを利用したスクリプト作成より大幅に手間が削減。

💡 なぜ重要？

- Notionを開発ワークフローに統合しやすくなり、自動化タスクの作成が迅速化。
- 開発者の生産性向上に貢献。

🛠️ `ntn` の使い方フロー

VS 従来 API との比較

💬 Xでの反応

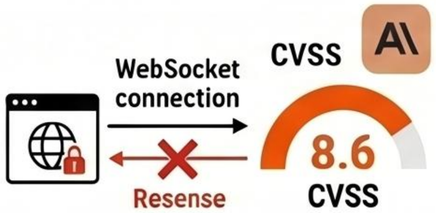
Likes ♥ 1.2k

"This is a game-changer! Now I can script Notion integrations much faster." – X ユーザー

本日のトピック一覧

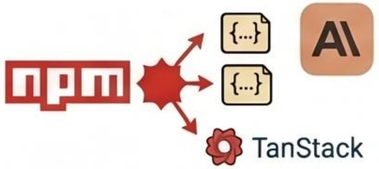
TEKION Group

1 Next.js CVE-2026-44578 — 過去最悪の WebSocket Upgrade SSRF（CVSS 8.6）



2 Anthropic、Claude Code SDK プログラム利用を「専用月次クレジット」に分離（6/15 開始）

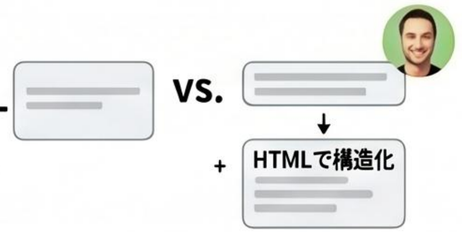
3 npm「Mini Shai-Hulud」攻撃 AI 開発者ツール標的に拡大 — TanStack 42 公式パッケージ感染



5 Topic 5: Claude Code 2.1.139 — /goal コマンド追加 + push 通知 + agent view

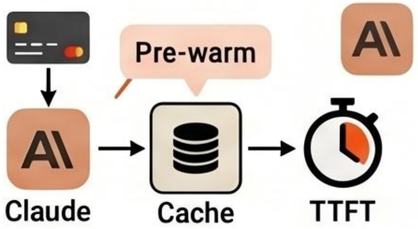
6 [Note]: Duplicate text of Topic 5, formerly on the left, has been removed to restore correct sequential flow.

4 Karpathy「LLM の問いに『HTML で構造化』を足すだけ」— 半年分の AI ワークフロー覆す Tips



5 Topic 5: Claude Code 2.1.139 リリース — /goal コマンド追加 + push 通知 + agent view

6 Topic 6: Claude API プロンプトキャッシュ「事前ウォーム」Tips — TTFT 大幅短縮



7 Topic 7: Notion 公式 CLI `リリース — Notion API がターミナルから操作可能に

主な出典 Vercel ANTHROPIC npm TanStack Karpathy Notion

24pt