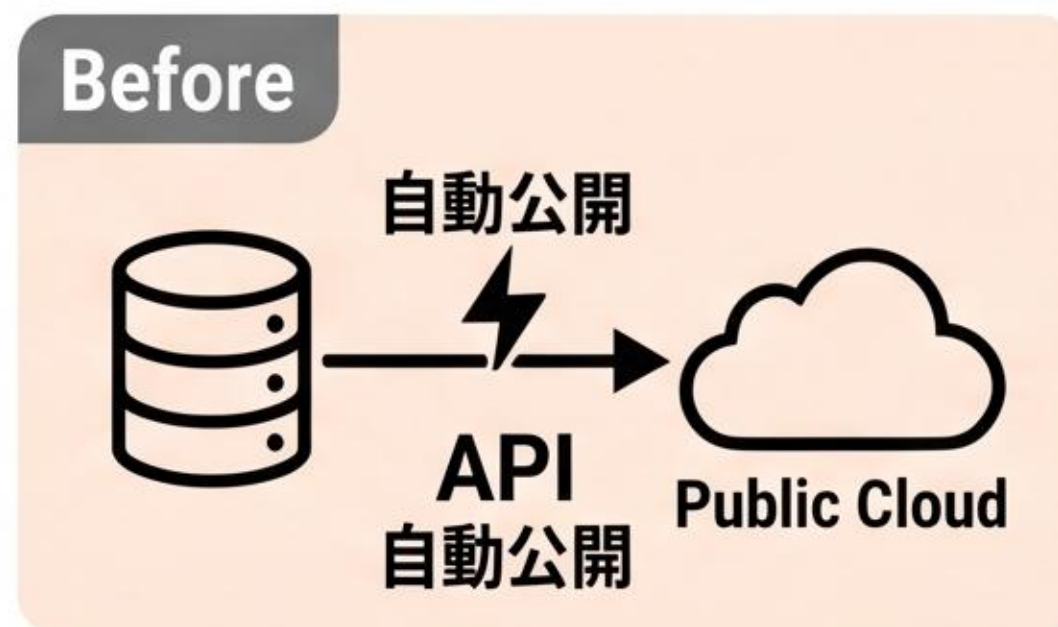




## 今朝のホットな話題

- Supabase が Data API の自動公開を廃止**  
 — 5/30 以降は明示 GRANT 必須
  - Supabase が Database API の自動公開を廃止必ず
  - 自動公開の改造以降→~~4/~~以は明示 GRANT 必須
- OpenAI Codex UX 大改修** — ショートカット完全カスタム化 / Git 操作 10-50x / レビュー画面集約
  - OpenAI Codex → ショートカットを完全カスタム化
  - ショートカットナスタ、Git 操作のベイクルを操作
  - レビュー画面集約 → Git 操作-連弱正が強例で搭載
- Next.js 史上最悪の脆弱性**  
**CVE-2026-44578 (CVSS 8.6)** — 内部 SSRF、認証不要
  - 外部に入力・リーバにが認証される脆弱性を証不要
  - 内内の穴から求める内に続けた脆弱を廻理性



7 トピックを整理。

## 何が起きた？

Supabase は 2026-05-30 以降に作成される新規プロジェクトで、public スキーマに追加された新テーブルを Data API へ自動公開しない方針へ転換する。各テーブル・各ロール (anon / authenticated 等) に対し dashboard または SQL で明示的に GRANT を付与する必要がある。公式ブログと GitHub Discussion #45329 に詳細。

## 主な変更点

- 対象は 5/30 以降に作成される新規プロジェクト、既存プロジェクトには影響なし
- anon / authenticated で別権限が前提のセキュリティモデルへ全面移行
- 「declarative code (diff/grep可能な権限管理)」を公式方針として明示
- RLS が有効でも GRANT がなければ API でテーブルを見れない事故が起きうる
- GitHub Discussion #45329 が一次情報

## なぜ重要？ / Xでの反応

(Pros) セキュリティ向上・IaC準拠

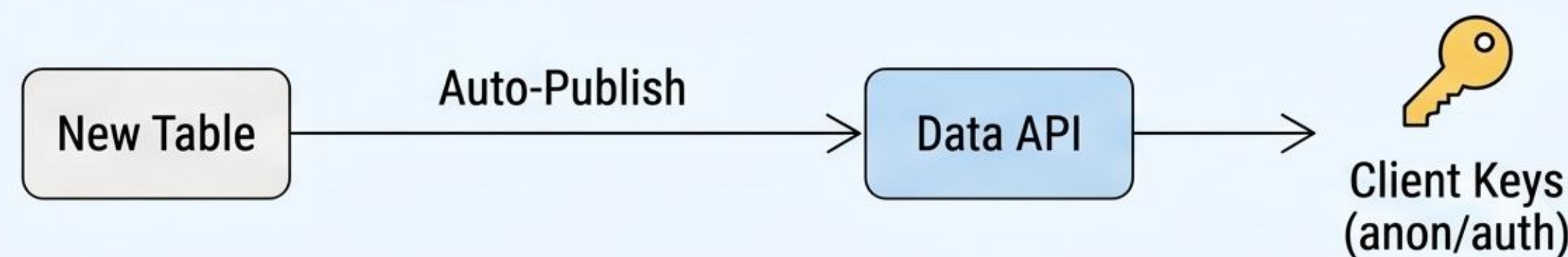
(Cons) 既存ワークフロー影響・セットアップ複雑化

Xでの反応: 「セキュリティ向上は歓迎だが既存ワークフローへの影響が大きい」

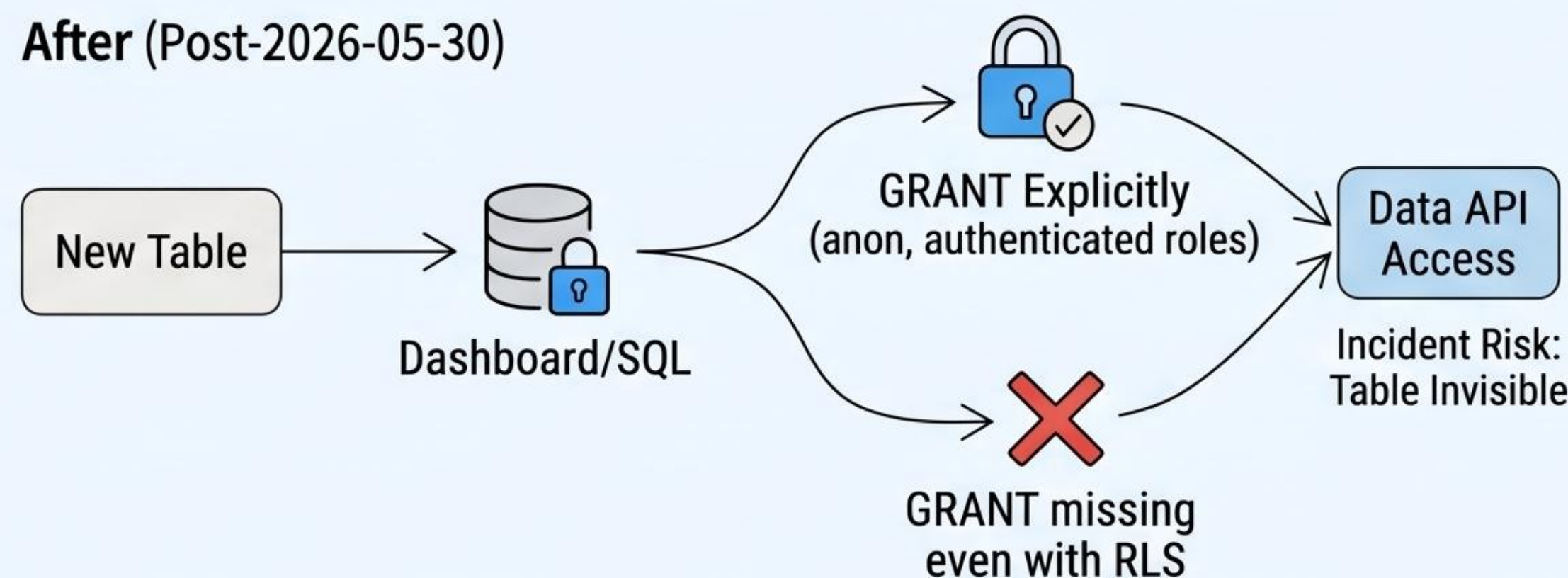
「postgres GRANT を grep/diff できるのは IaC 的に正しい」など賛否両論。

## 旧：Data API 自動公開 vs 新：明示 GRANT 必須 (セキュリティ強化)

Before (Pre-2026-05-30)



After (Post-2026-05-30)



## Xでの反応

「セキュリティ向上は歓迎だが既存ワークフローへの影響が大きい」

「postgres GRANT を grep/diff できるのは IaC 的に正しい」

## 何が起きた？

OpenAI Codex がエンジニア向け UX をまとめて刷新。

## 主な変更点

- キーボードショートカットを設定画面から完全カスタマイズ可
- 大規模リポの Git 操作 10-50× 高速化、ストリーミング系で再レンダ 0 化したパスも
- スレッド切替時の再レンダを ~75% 削減
- Git アクション (commit/push/branch/PR 作成・状態) をレビュー画面に集約
- ローカルサーバー一覧の整理 (フィルタ・sort 記憶・120 秒ごと自動リフレッシュ)

## なぜ重要？

開発者の生産性を劇的に向上させ、レビューや Git 操作をシームレスに行える環境を提供するため。

**Before**

Git 操作  
**10-50× 高速化**  
(10-250/s)

再レンダ 軽減  
**~75% 削減**

**After**

### レビュー画面集約

Git actions

- Git commit
- push
- PR
- .....

Summary

Context

Sources

### ショートカットカスタム

**3** ローカルサーバー一覧  
🔄 120 秒ごと自動更新

「ようやくレビューと git が同じ画面で完結する」  
「スレッド切替がもたつかなくなった」

👍 4.5K  
❤️ 2.2K

# Next.js 史上最悪の脆弱性 CVE-2026-44578 (CVSS 8.6) — 内部 SSRF、認証不要

## 🔍 何が起きた？

Next.js に CVSS 8.6 の **WebSocket SSRF 脆弱性 CVE-2026-44578** が見つかった。認証不要、特殊リクエスト1つで内部サービス・クラウド資格情報・API キー・管理パネルにアクセス可。

## 📌 主な変更点 (points, affect and countermeasure)

- 影響バージョン: 13.4.13+ / 14.x / 15.x / 16.0.0–16.2.4
- 対策バージョン: 15.5.18 / 16.2.6 以上にアップグレード必須。

## 💡 なぜ重要？ (Why it matters)

- 認証不要・単発リクエストで内部サービスへ SSRF
- クラウド資格情報 / API キー / 管理パネルへアクセス可能
- 推計 79,000 self-hosted インスタンスが脆弱状態
- Vercel ホスティングは影響なし。self-hosted は緊急アップグレード必須



! self-hosted  
インスタンス

影響あり  
(脆弱)

▲ Vercel  
ホスティング

安全

数字ハイライトカード

**CVSS 8.6 緊急**

**推計 79,000**

self-hosted インスタンスが脆弱

**82万閲覧**

✕ 引用カード “ ”

「Vercelに載せていてよかった」「self-hostedの本番を急ぎパッチ」緊急対応の動き。警戒レベルが業界横断に。

# Claude 有料プランに月次プログラム利用クレジット — 6/15 開始、Agent SDK / Code / GitHub Actions で利用可

Anthropic公式

12,380 likes

## 🔍 何が起きた？

Anthropic は 2026-06-15 から Claude の有料プランに対し、毎月一定の「プログラム利用専用クレジット」を付与する制度を開始する。

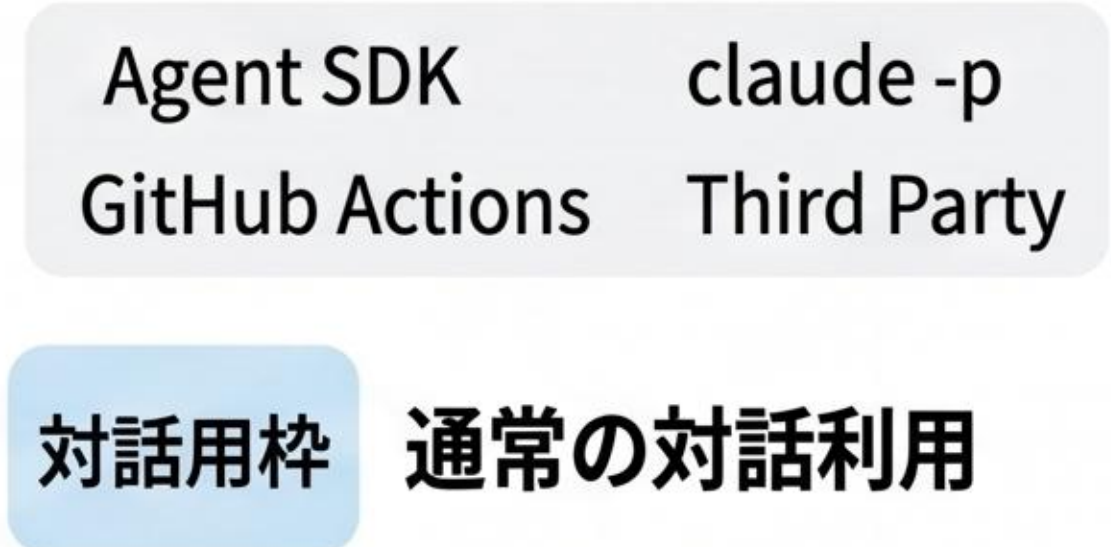
## 📌 主な変更点

- 開始日: 2026-06-15
- 対象: Pro / Max 等の有料プラン
- 利用先: Claude Agent SDK, claude -p, Claude Code, GitHub Actions, サードパーティ
- Claude Code サブスクは同時期に月 \$200 クレジット上限化、従来比 5-10× の実質値上げに相当
- プログラム利用と対話利用を計量分離するモデルへ

## 💡 なぜ重要？

Anthropic公式の発表によると、プログラム利用専用クレジットが新設される。同時期にClaude Codeサブスクは月\$200のクレジット上限計量分離するモデルへの移行である (@weswinder が拡散)。Xでの反応：12,380 likes、990万閲覧。賛否分岐。

従来: 対話・プログラム利用混在    新制度: プログラム専用クレジット



Before (以前)		After (2026-06-15~)		
月 \$200 クレジット上限		月 \$200 クレジット 従来比 5-10× 実質値上げ		
\$200 月クレジット上限	5-10× 実質値上げ相当	2026-06-15 開始日	12,380 likes	990万 閲覧

## Xでの反応



## 📌 Notion 公式 CLI 「ntn」 リリース — ターミナルから Notion API 全機能、Workers 構築・デプロイまで

Notion公式

👍 likes 3.3K

### 🔍 何が起きた？

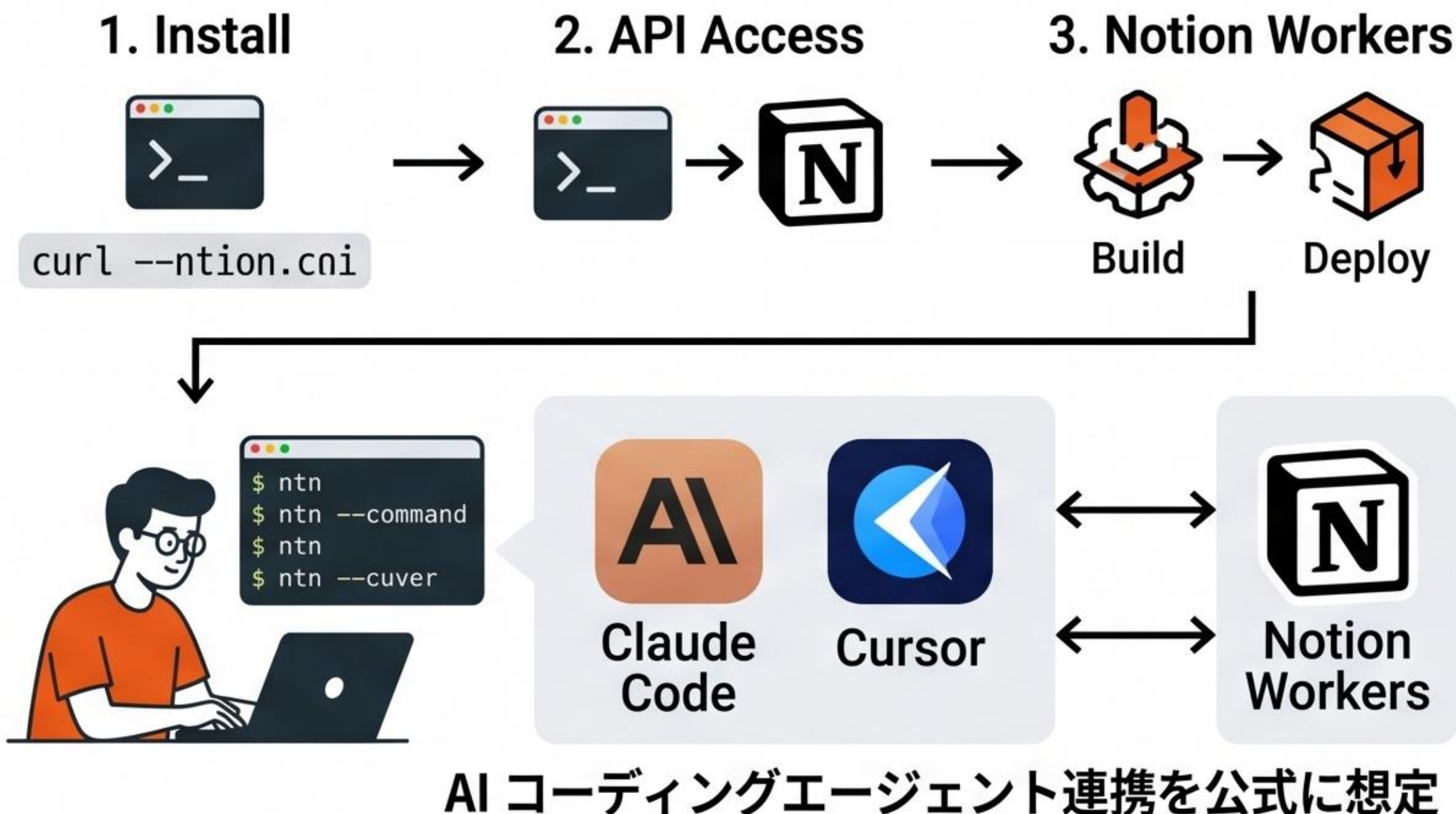
Notion が公式 CLI `ntn` をリリース。ターミナルから Notion API の全機能呼び出せるだけでなく、Notion Workers の構築・デプロイまでカバー。AI コーディングエージェント (Claude Code / Codex / Cursor 等) から直接叩ける設計が強調されている。

### 📌 主な変更点

- インストール: `curl -fsSL https://www.notion.com/cli | bash``
- API 全エンドポイント呼び出し可
- Notion Workers のローカル開発・デプロイ対応
- AI コーディングエージェント連携を公式に想定した設計

### 💡 なぜ重要？

- Notion API の全機能へのアクセスがターミナルで完結する。
- Notion Workers のローカル開発・デプロイが実現。
- AI コーディングエージェントによる Notion 操作が公式に想定されている。



### 数字ハイライト 📊

1.34M+ 閲覧

3.3K+ likes

### 引用カード

Xでの反応

ようやく Notion を CLI で叩ける

Workers のローカル開発が現実的になった

Xでの反応

# 🔍 Hermes Agent (Nous Research) – Grok サブを OAuth 接続 で API key 不要、OSS 自己改善エージェントとして台頭

## 🔍 何が起きた？

Nous Research の OSS 自己改善エージェント「Hermes Agent」が、Grok の OAuth 接続を正式サポート。API キーなしで Grok モデルを直接利用可能に。ローカル/VPS 常駐で長期記憶を持つ。

## 🚩 主な変更点

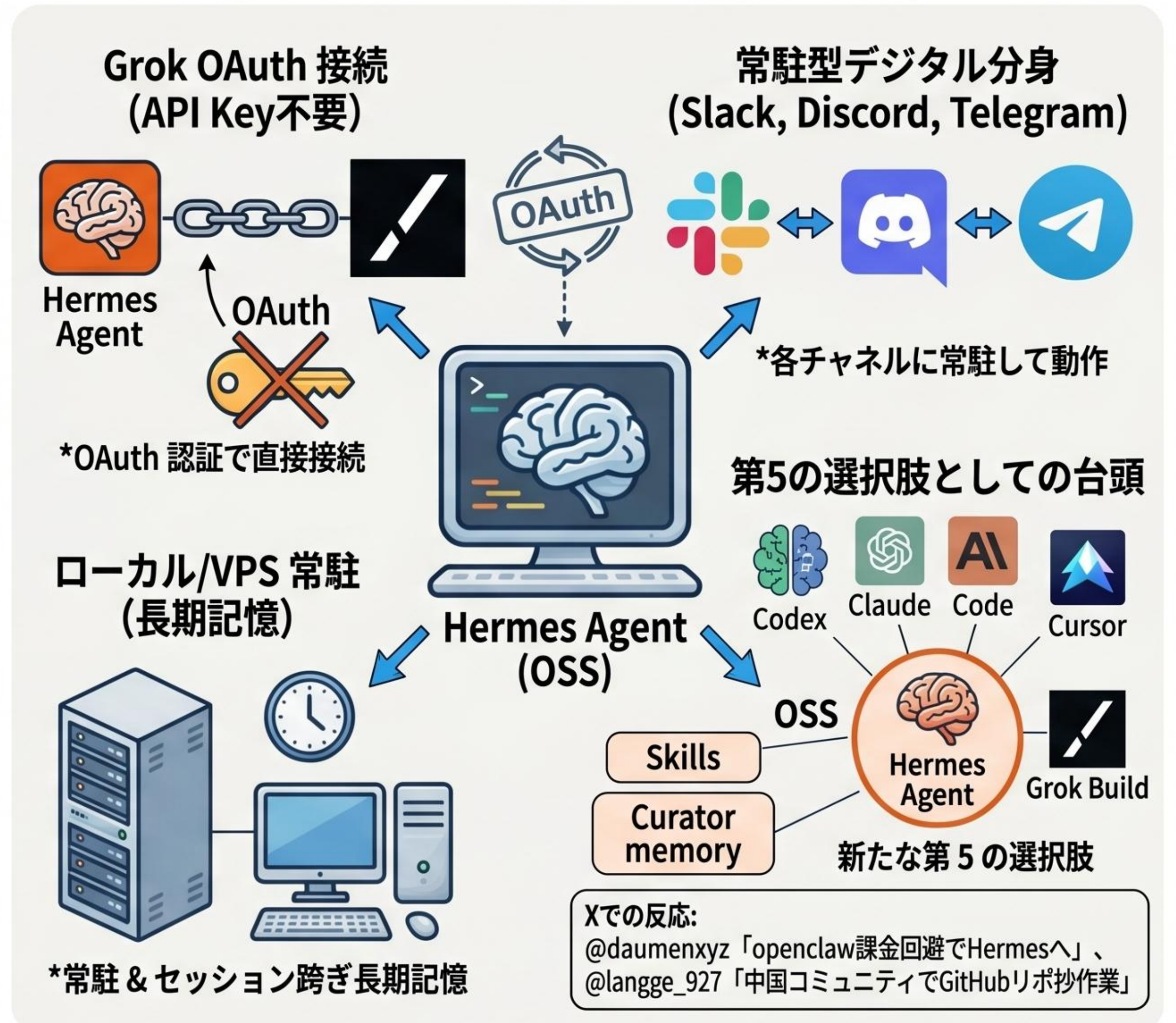
- Grok アカウントを OAuth で接続 → API key 不要で Grok モデルを直接利用
- ローカル/VPS 常駐、セッション跨ぎの長期記憶
- Slack / Discord / Telegram 接続で常駐エージェント化
- OSS なのでカスタマイズ自由 (Skills, Curator memory)
- Codex / Claude Code / Cursor / Grok Build に次ぐ第 5 の選択肢

## 💡 なぜ重要？ / コミュニティの反応

常駐型デジタル分身が可能。Xでは課金回避での切り替え事例や中国コミュニティの動きが報告され、第5の選択肢として注目されている。

Xでの反応:

- 「openclaw のトークン課金がかきつくて Hermes に切り替えた」 (@daumenxyz)
- 「中国コミュニティでは Hermes 周辺の GitHub リポを抄作業の対象に」 (@langge\_927) など実利用が進む。



# Karpathy の「LLM に出力構造を尋ねる」 プロンプト手法 – モデル待ちせずに今日から効く



Andrej Karpathy (X) / AYi\_Alnotes

## 🔑 要点

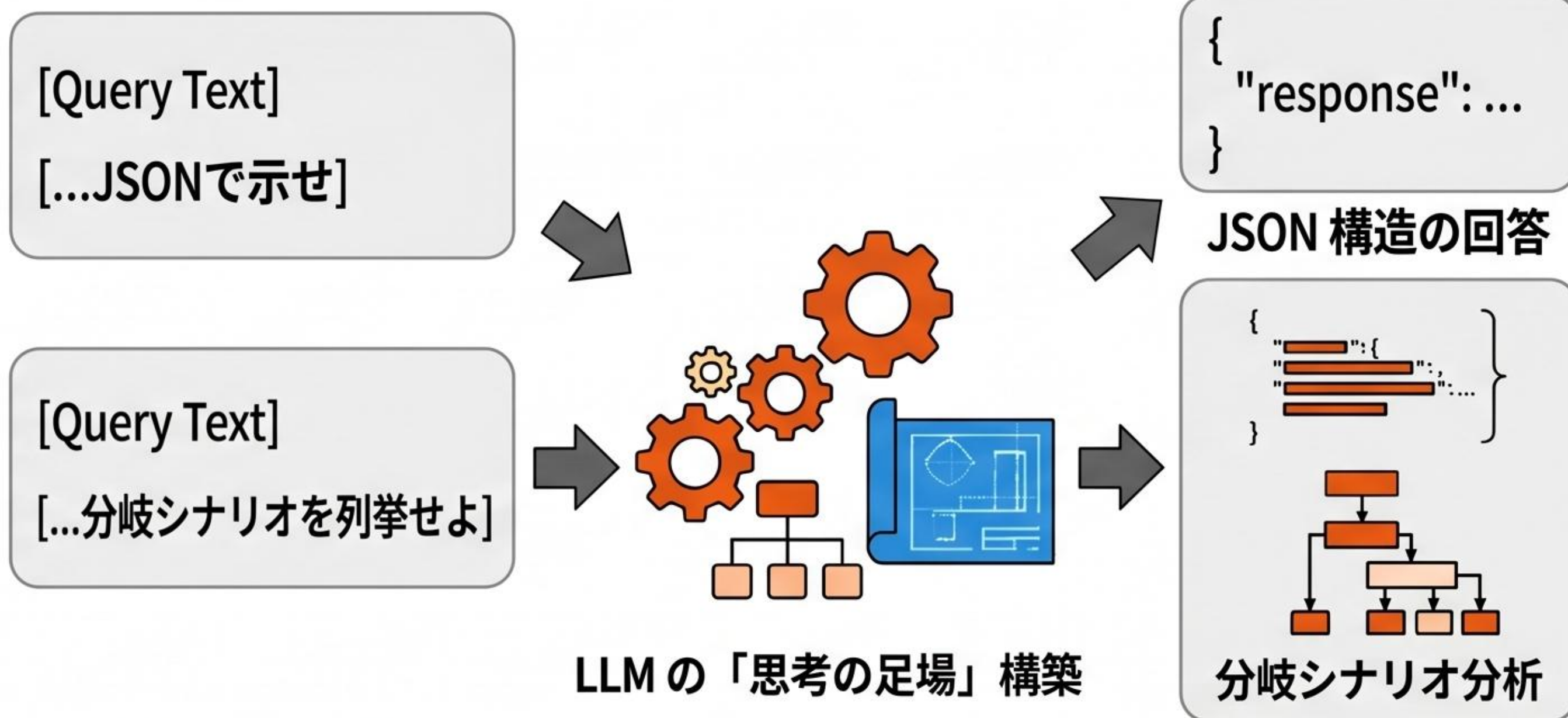
Andrej Karpathy が「クエリの末尾で LLM に『この回答の出力構造を JSON で示せ』『分岐シナリオを列挙してから答えよ』と頼むだけで品質が大きく上がる」と提案。AYi の中国語解説が拡散し、過去半年の AI ワークフロー設計を見直す議論を喚起した。  
Chain-of-Thought / Tree-of-Thoughts と相補的に動く軽量プラクティス。

## 🔧 具体的な手法 / 使いどころ

- テクニック: 質問の末尾に 'structure your answer as ...' / 'list the possible branches' を付ける
- モデル自身に「思考の足場」を作らせる側にコストを支払うアプローチ
- コンテキスト窓やモデル性能向上を待たずに即効性あり
- AYi の中国語解説が拡散

## 🌱 なぜ刺さるか / 学び

- AYi の中国語解説が拡散し、「過去半年の AI ワークフローを覆す」
- ワークフロー設計者に響いており、プロンプトコストとモデル性能向上へのアプローチ見直しの議論を喚起した。



# 本日のトピック一覧

**1 Supabase が Data API の自動公開を廃止**  
5/30 以降は明示 GRANT 必須



**2 OpenAI Codex UX 大改修**  
ショートカット完全カスタム化 / Git 操作 10-50x / レビュー画面集約



**3 Next.js 史上最悪の脆弱性**  
CVE-2026-44578 (CVSS 8.6)  
内部 SSRF、認証不要



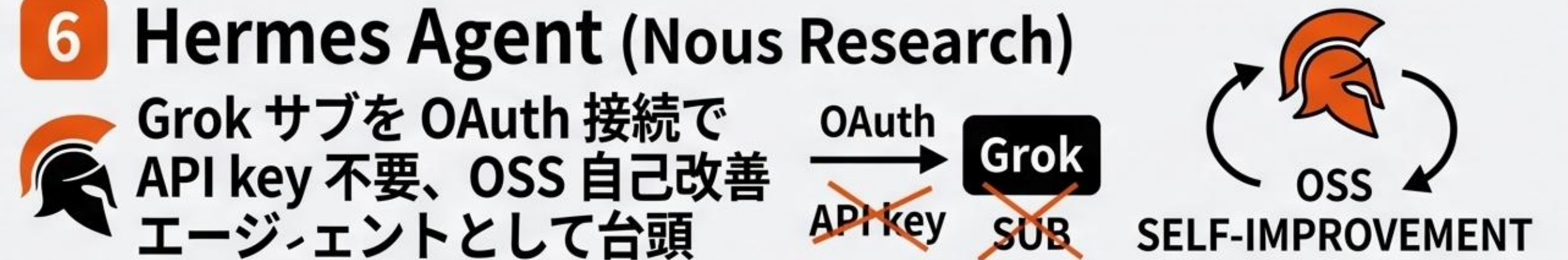
**4 Claude 有料プランに月次プログラム利用クレジット**  
6/15 開始、Agent SDK / Code / GitHub Actions で利用可



**5 Notion 公式 CLI 「ntn」 リリース**  
ターミナルから Notion API 全機能、Workers 構築・デプロイまで



**6 Hermes Agent (Nous Research)**  
Grok サブを OAuth 接続で API key 不要、OSS 自己改善 エージェントとして台頭



**7 Karpathy の「LLM に出力構造を尋ねる」プロンプト手法**  
モデル待ちせずに今日から効く

