

# 2026-08-26

---

1. Next.js が8月のセキュリティ更新を1日前倒しで公開
2. Claude の記憶がチャットと Cowork で1つになった
3. Vercel Connect が正式提供に

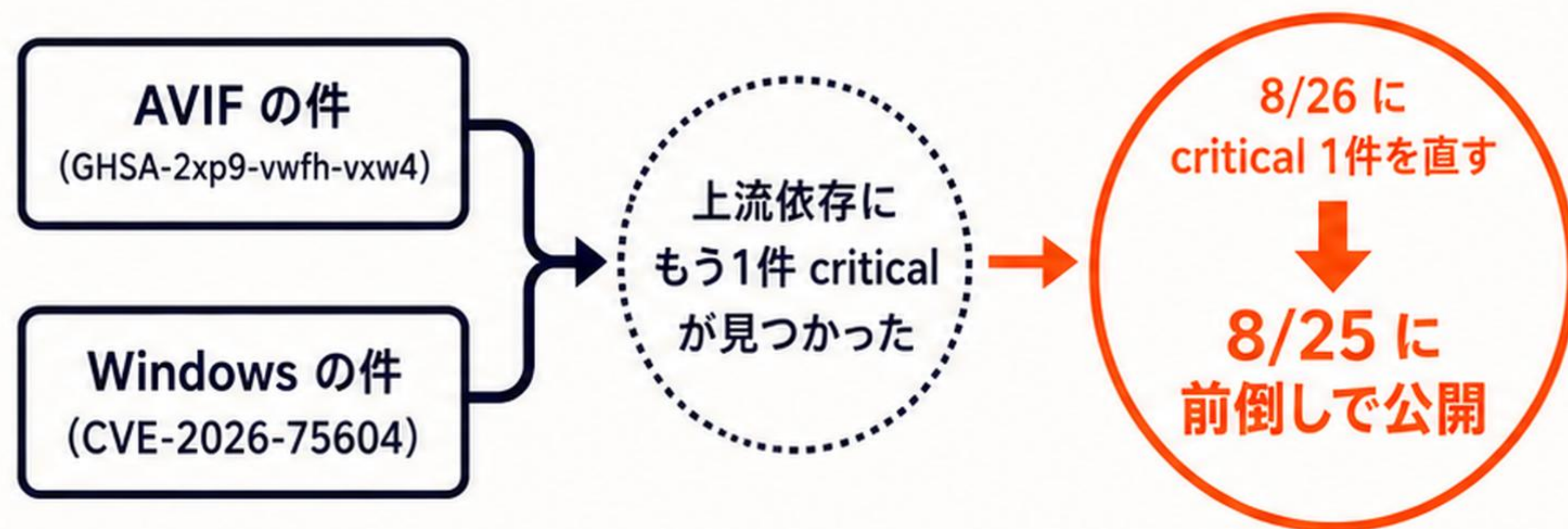
8トピック

# Next.js が8月のセキュリティ更新を1日前倒して公開

## 認証不要のリモートコード実行が2件

8/20 に「8/26 に critical 1件を直す」と予告されていた Next.js のセキュリティリリースが、上流依存にもう1件 critical が見つかったため 8/25 に前倒して公開された。

- AVIF の件 (GHSA-2xp9-vwfh-vxw4) : `sharp` が使う libheif の欠陥で、攻撃者が用意した AVIF 画像を Next.js...
- Windows の件 (CVE-2026-75604) : Pages Router と App Router を併用し Cache Components...
- Linux と macOS は Windows の件の影響を受けない



バイブコーディングで作ったアプリの多くが Next.js を土台にしている。

# Claude の記憶がチャットと Cowork で1つになった

## 会話中に書き込む方式へ

Anthropic が 8/25、Claude のチャットと Claude Cowork の記憶を同一のものに統合した。

- チャットで覚えたことが Cowork にも、Cowork で覚えたことがチャットにも反映される
- ただし記憶が共有されるのは Cowork がクラウドで動いているときだけ。手元の PC でローカル実行している...
- 記憶の作られ方が変更。会話中にトピックを追加するので「締め切りが9月に動いた」と言えば次の会話ではもう知っている



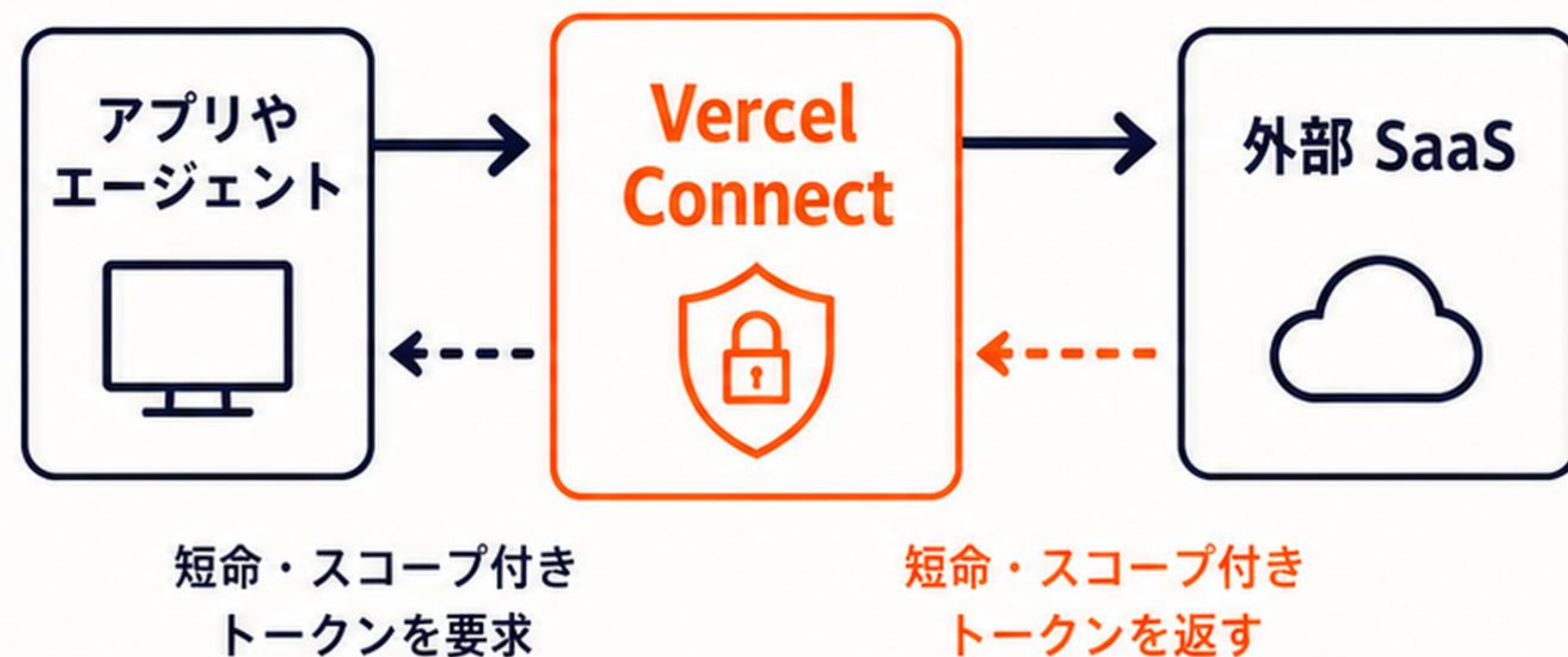
エージェントに毎回同じ前提を貼り直す作業がそのまま消える。

# Vercel Connect が正式提供に

## エージェントに長期シークレットを持たせない接続層

アプリやエージェントから外部 SaaS に安全につなぐための層「Vercel Connect」が 8/25 に GA になった。

- 100以上のプリセットコネクタ（Notion、Workday など）。マネージドコネクタとして Slack / GitHub / Linear /...
- 長期シークレットを保存せず、実行時に短命・スコープ付きトークンを要求する方式。承認が要る場面では認可フローが自動で走る
- アプリ単位の権限とユーザー委任の権限を切り替えられる。エージェントには read-only など絞ったスコープだけを渡せる



エージェントに外部サービスを触らせるとき一番危ないのは、全権限の API キーをコードや環境変数に置いたまま渡すやり方だ。

# CodeRabbit が Cursor 用プラグインを公開

## レビュー用サブエージェントと承認付き autofix

コードレビュー SaaS の CodeRabbit が 8/25、Cursor 向けの公式プラグインを公開した。

- ``code-reviewer`` サブエージェントが同梱。  
メインの Agent が作業を続けている裏で、  
レビューを別コンテキストで走らせられる
- 呼び出しは自然文（「Review my code」）  
でもコマンド（``/coderabbit-review uncommitted``）でも可
- 導入は Cursor Marketplace から入れるか、  
Cursor 内で ``/add-plugin coderabbit``。  
初回に CodeRabbit CLI...



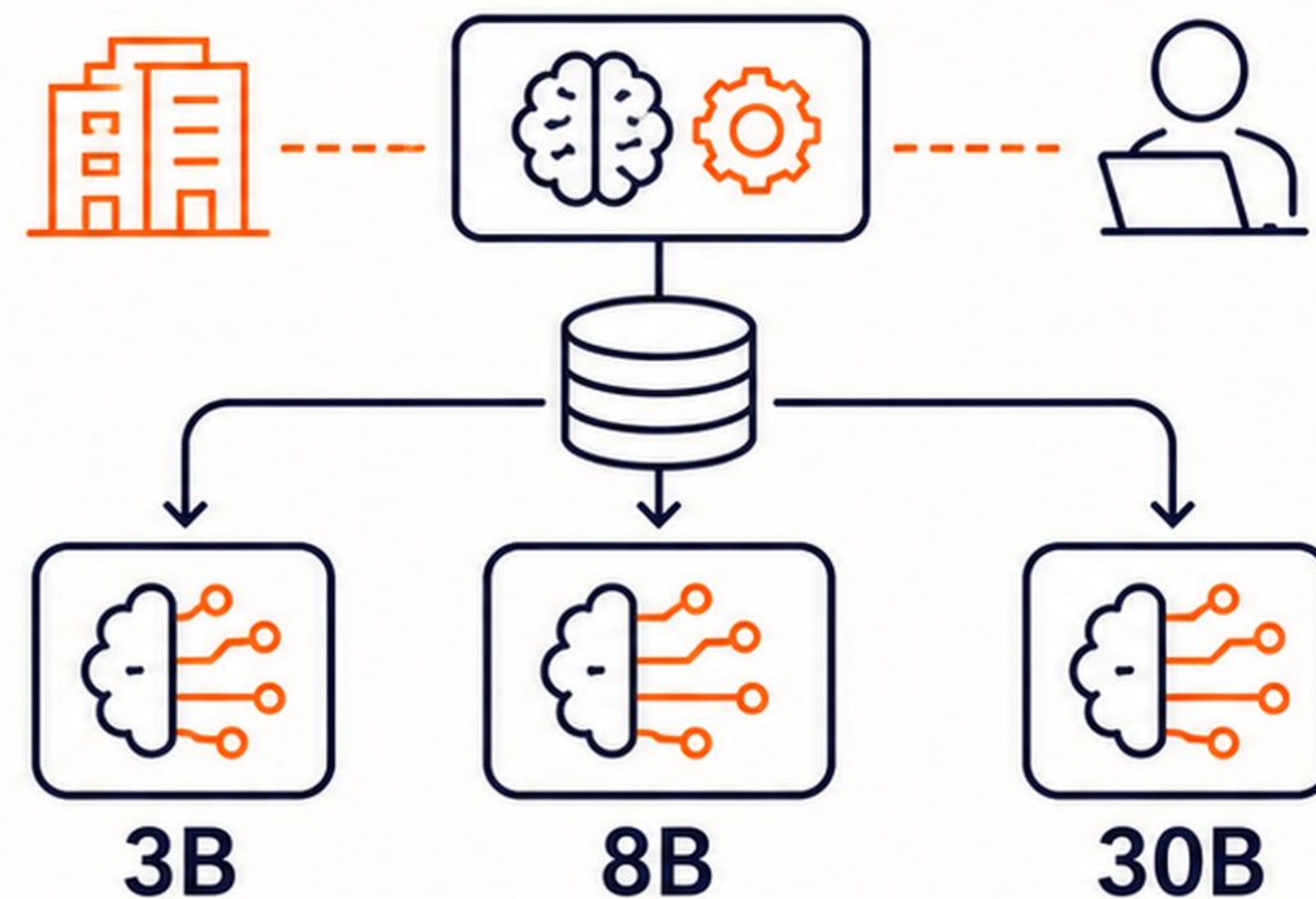
書いた本人と同じエージェントにレビューさせても甘くなる。

# IBM が Granite 4.2 を公開

## Apache 2.0、3B/8B/30B、思考モードの切り替え付き

IBM が 8/25、企業向けエージェントを想定した推論モデル群 Granite 4.2 を 3B / 8B / 30B の3サイズで公開した。

- ライセンスは Apache 2.0。ダウンロード・ファインチューニング・商用投入に制限がない
- Ollama 上のダウンロード量は 3b が 2.2GB・8b が 5.3GB・30b が 18GB。コンテキストは 128K
- `enable\_thinking` と `reasoning\_effort` で思考の深さを制御できる…



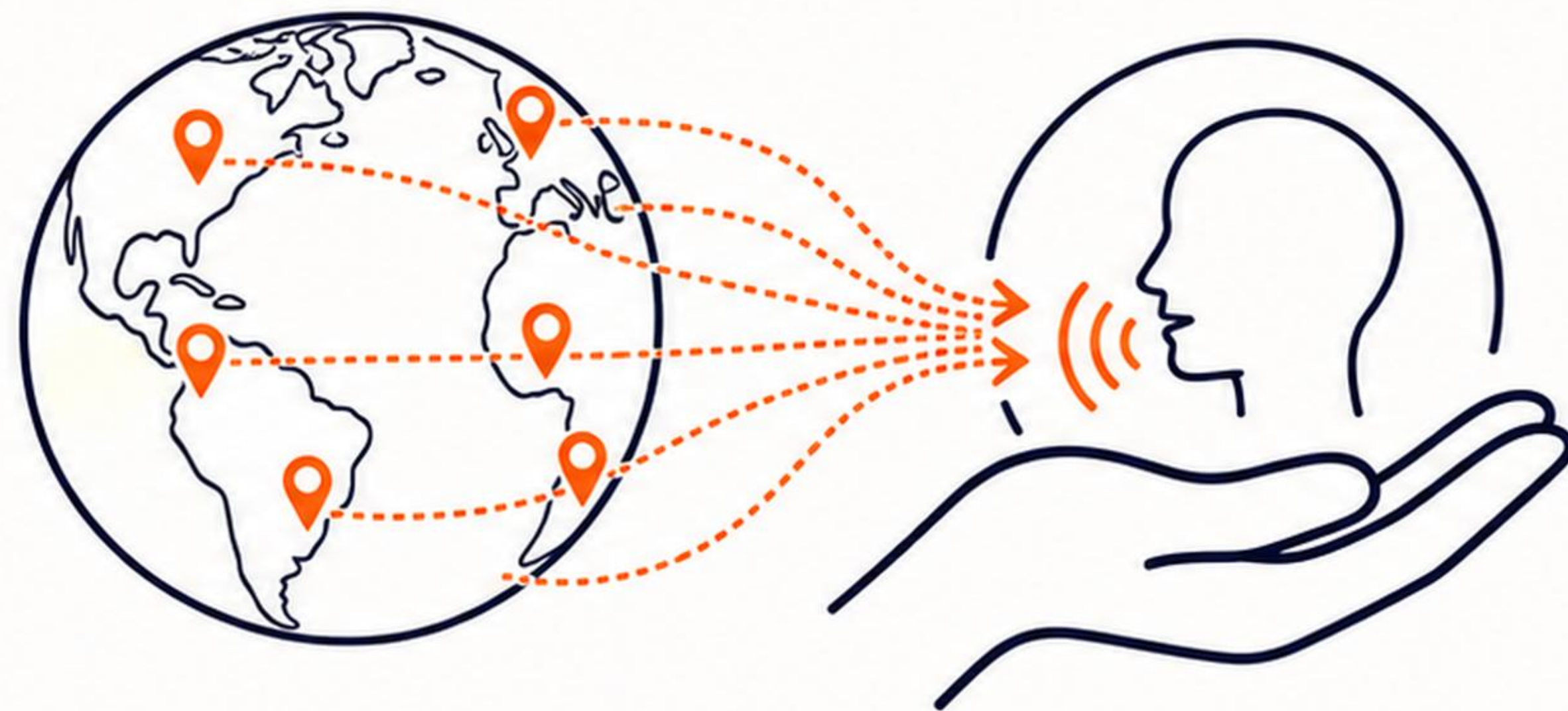
ローカルで動くサイズ（8B なら 5.3GB）でツール呼び出しと思考モードが最初から入っていて、Apache 2.0 なので商用利用に制限がない。

# OpenAI Build Week の受賞作が発表

## 186カ国・約4.7万人・8,000プロジェクト

OpenAI が8日間かけて開催した世界規模のハッカソン「Build Week」の受賞作が 8/25 に公開された。

- 規模は186カ国・約47,000ビルダー・8,000プロジェクト超・8日間。デジタル7件と対面60件のコミュニティイベントを併催した
- Apps for Your Life: 1位 Second Voice（発話支援）、2位 AirBridge for Windows（PCの音声をAppleデバイスへ流す）
- Work & Productivity: 1位 veTriage（獣医のトリアージ支援）、2位 Pulse（心停止時の対応補助）



受賞作の顔ぶれが巨大な技術デモではなく、獣医のトリアージ、ベトナム語の声調、発話支援といった具体的な誰かの困りごとに寄っている。

# Hugging Face が130億ドル超での買収交渉と報道

## 相手は不明、成立もしていない

Business Insider が週末に、オープンソース AI のハブである Hugging Face が130億ドル以上での買収について交渉していると報じた。

- 報道元は Business Insider。TechCrunch は「相手が誰かは不明」「合意には至っていない」と明記している
- 直近の資金調達は2023年、ポストマネー45億ドル。Salesforce Ventures がリードし Alphabet・GV・IBM Ventures が参加した
- 2026年前半に NVIDIA から企業価値70億ドルでの5億ドル出資提案があったが断っている



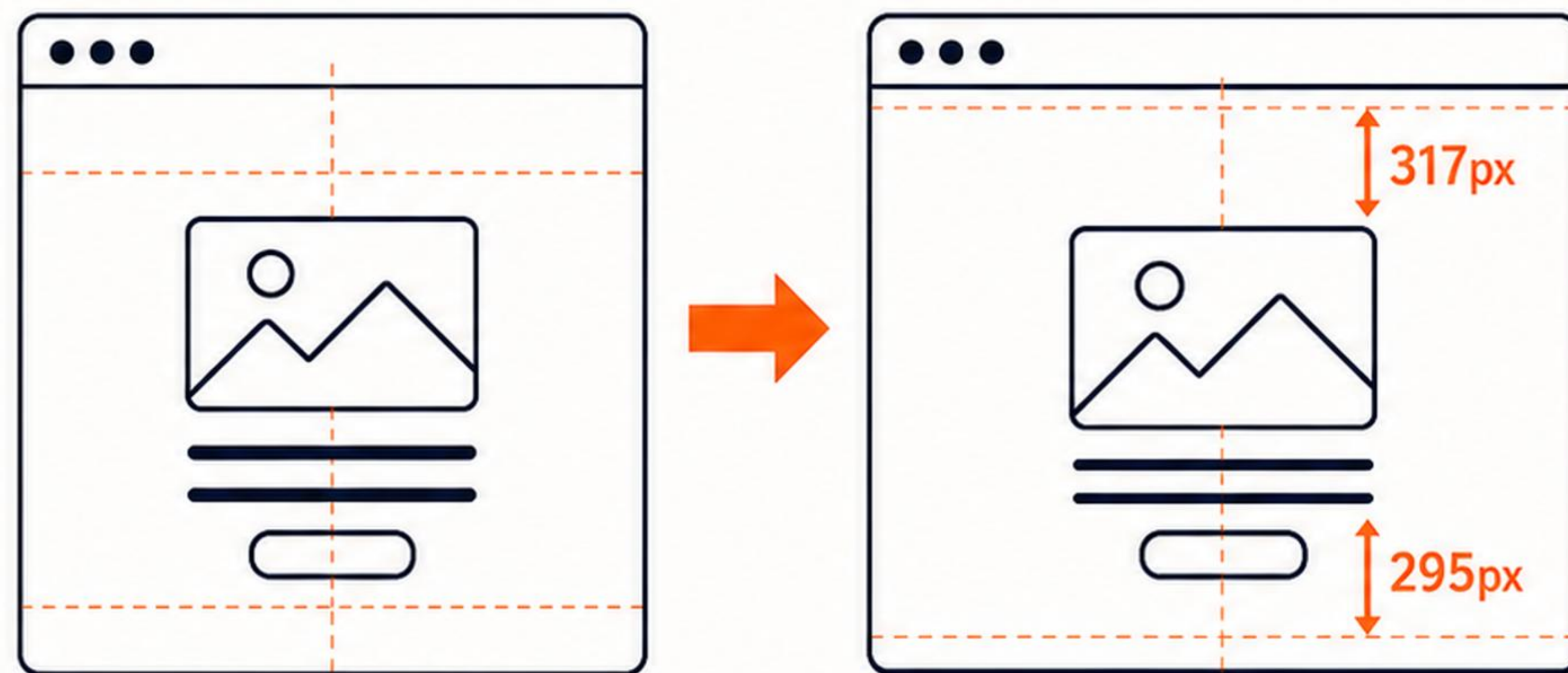
モデルを落とす先、データセットを探す先、Ollama や各種ツールが裏で叩いている先はほぼ全部 Hugging Face だ。

# 〈知見〉AI が出す UI が「なんとなく惜しい」理由

## 数字の中央と目で見た中央は違う

サイバーエージェントのクリエイティブディレクター・原佑一氏による29枚のスライド。

- 上下のマージンが同じ数値だと、下にズレて見える。「上方距離過大の錯視…」
- 実例として Ameba ブログ20周年サイトでは上下マージンを 317px / 295px と非対称にして視覚的な中央を取っている
- 同じ色でも面積が変わると違う色に見える。面積が大きいほど明るく、あるいは暗く極端に見える…



AI に UI を作らせると、数値上はきれいに揃っているのに「なんか惜しい」ものが出てくる。

# 本日のトピックス一覧

---

1. Next.js が8月のセキュリティ更新を1日前倒しで公開
2. Claude の記憶がチャットと Cowork で1つになった
3. Vercel Connect が正式提供に
4. CodeRabbit が Cursor 用プラグインを公開
5. IBM が Granite 4.2 を公開
6. OpenAI Build Week の受賞作が発表
7. Hugging Face が130億ドル超での買収交渉と報道
8. 〈知見〉AI が出す UI が「なんとなく惜しい」理由