

今朝のホットな話題

2026-08-08

1. Claude Code のセッション同士がメッセージを送り合えるようになった
2. Claude Code の auto mode が既定に
3. OpenAI が次期モデル Astra を Preparedness Framework 初の「critical」に分類

8トピック

1. Claude Code のセッション同士がメッセージを送り合えるようになった

Claude Code に、走っているセッション同士が直接メッセージを送り合う機能が入った。

- 送信されるのはサマリののみ。会話履歴もファイルも相手に渡らない
- 受け取り側はタスクの途中でメッセージを拾える（作業を止めて待つ必要がない）
- 双方向：別セッションに質問を投げて、答えを今のセッションに返してもらえる



複数セッションを並走させる運用では、これまで人間が「あっちで何をやったか」を毎回説明し直すのがボトルネックだった。

2. Claude Code の auto mode が既定に

「人間の承認より安全」を1,053人の対照試験で示した

Anthropic が Claude Code の auto mode を Pro / Max / Team プランの既定にすると発表した。

- 開始は 2026-08-14。Pro / Max / Team の新規セッションが対象。既に自分で既定を設定済みなら一度だけ確認プロンプトが出る
- 1,053人の有償テスターによる対照試験で、危険なコマンドを人間のレビューは13.6%しか止められず、auto mode は89%止めた
- 現状ユーザーは許可プロンプトの97%を承認している。プラン提示の却下率は39%あるのに、個別の許可要求の却下率はわずか3%

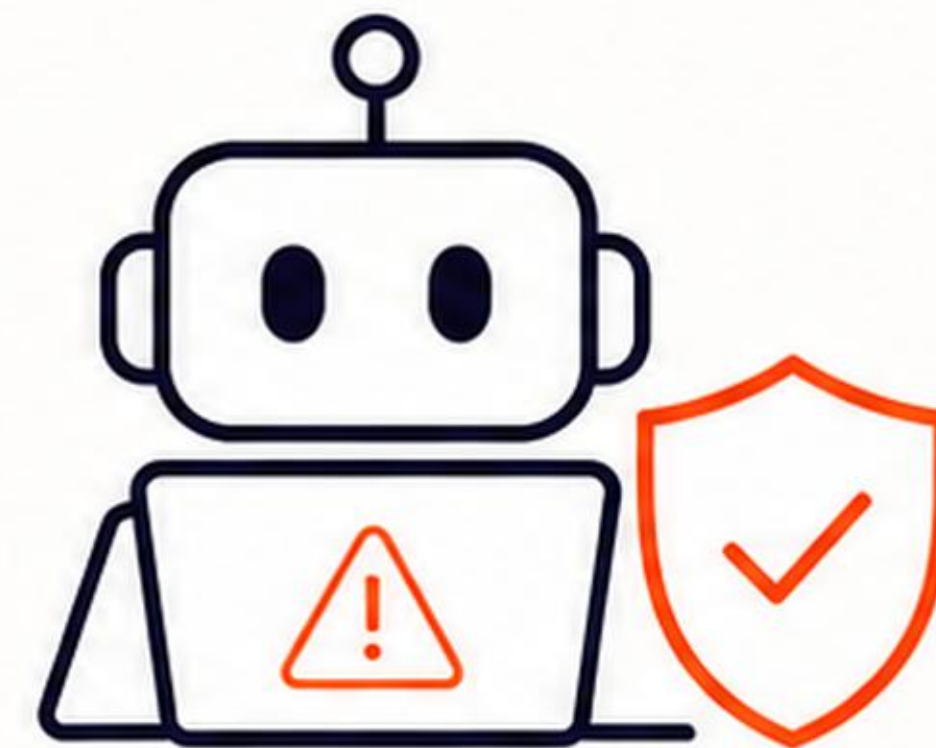


人間のレビューは

13.6%

しか止められず

VS.



auto mode は

89%

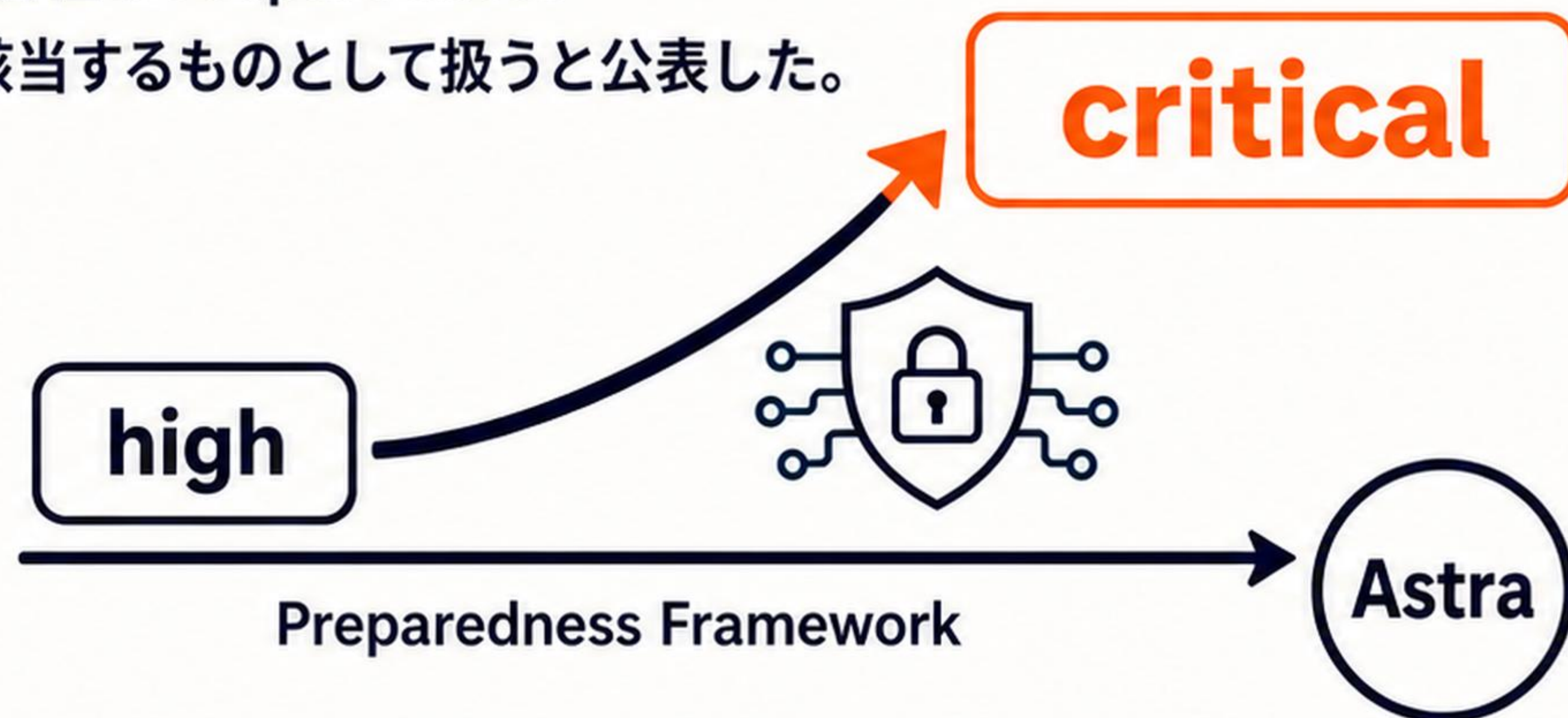
止めた

「人間が確認しているから安全」という前提を、自社データで否定した発表。

3. OpenAI が次期モデル Astra を Preparedness Framework 初の「critical」に分類

OpenAI が、開発中のモデル Astra を評価した結果、自社の Preparedness Framework 上でサイバーセキュリティの「critical」に該当するものとして扱うと公表した。

- 公式ポスト原文: 「we're treating it as our first "critical" model for cybersecurity under our Preparedness Framework」
- 「これは想定していたシナリオ」であり、追加の統制を入れて開発を進めると明言
- 従来モデルは GPT-5.6 Sol を含め「high」止まりで、critical に到達した公表事例は初



未公開のモデルに対して、フロンティアラボが自ら最高危険度の指定を公表したのは初めて。

4. SpaceX による Cursor 買収、早ければ来週末に完了か

「Cursor」ブランドは段階的廃止の可能性

The Information の独占記事として、SpaceX による Cursor (Anysphere) 買収が早ければ来週末にも完了する可能性が報じられた。

- 買収完了は早ければ来週末の可能性
- 新製品では「Cursor」ブランドを段階的に廃止する方向（既存プロダクトの扱いは別）
- 社内で「Sand」と呼ばれていた汎用エージェントは「Grok Bot」という名称になる可能性



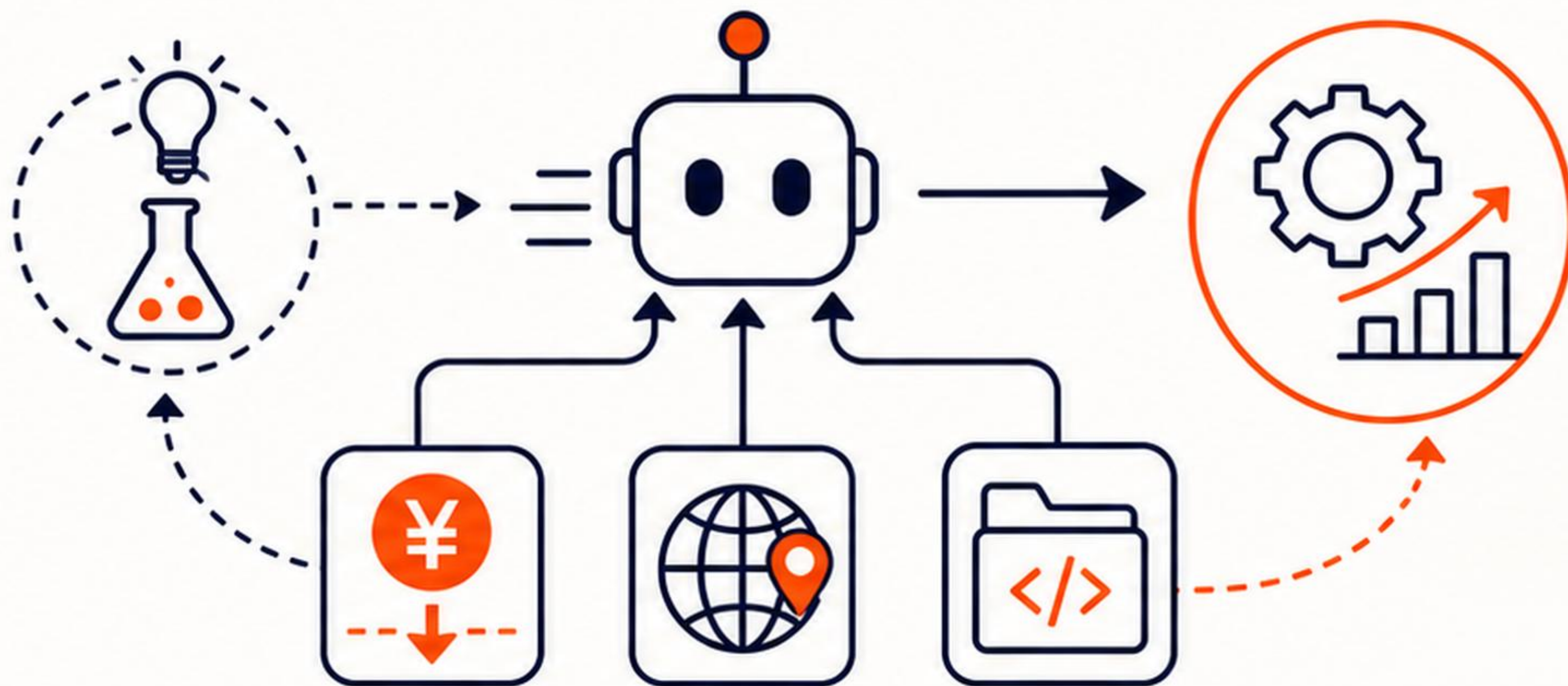
製品として最も勢いがある時期にブランドが消えるという話で、Cursor を社内標準にしている組織にとっては移行計画の判断材料になる。

5. Claude Managed Agents に4つの更新

予算上限・推論リージョン・repo からの skills 自動ロード・アドバイザー

Anthropic が Claude Managed Agents に今週4つの更新を入れた。

- **予算上限:** セッションに budget を設定でき、上限に達すると budget_reached イベントを出して一時停止…
- **推論リージョン:** model.inference_geo を us または global に設定。global は空いている場所で標準レート、us…
- **skills の自動ロード:** 接続したリポジトリの .claude/skills/ に置いた skills を、セッション開始時に自動で読み込む



予算上限とリージョン指定は「エージェントを本番で回す側」に必要な統制で、実験段階から運用段階への移行を示す。

6. Agent Plugins は「Skills と MCP をまとめる標準」では終わらない

OpenAI が AWS・Cursor・GitHub・VS Code・Vercel と共同策定。

公式ドキュメントでは、パッケージに同梱できるのは Agent Skills と MCP だけではない。

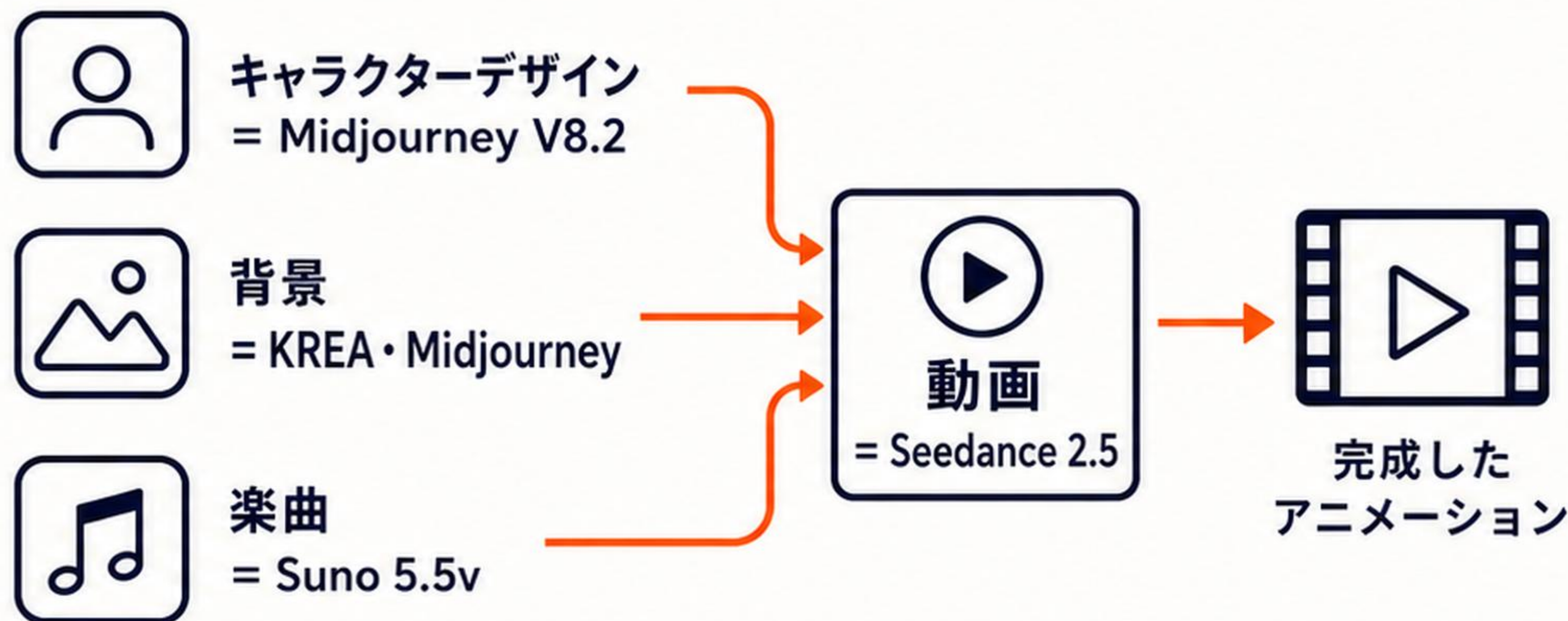
- 同梱できるのは6種: Skills / Connectors / MCP servers / Browser extensions / Hooks / Scheduled task templates
- Hooks はライフサイクル地点で走るコマンド
- ChatGPT と Codex は同一の公開カタログ (universal plugin directory) を共有

7. AI動画『WINGLESS』の制作費と時間が全公開

11時間・映像生成費 71,040円

Seedance 2.5 で全編生成され10万再生を超えた AI アニメーション『WINGLESS』の作者が、制作フロー・所要時間・実費を数字つきで公開した。

- 総制作時間は約11時間（企画から完成まで）。起点は Seedance 2.5 の挙動テスト動画で、映像の質感が気に入って作品化を決めた
- 映像生成費は 71,040円。ただし Seedance 2.5 のクレジット費のみで、KREA / Midjourney / Suno のサブスク料は含まない
- ツール分業: キャラクターデザイン = Midjourney V8.2 / 背景 = KREA・Midjourney / 楽曲 = Suno 5.5v / 動画 = Seedance 2.5



AI 映像制作で最も手に入りにくいのが実費と時間の一次情報。

8. AI生成スライドに意図を込める技術

直すのはリード文だけでいい

AI が作ったスライドが「何が言いたいのか分からない」ものになる原因を、各ページ最上部のリード文1行に絞って診断・処方した X Article。

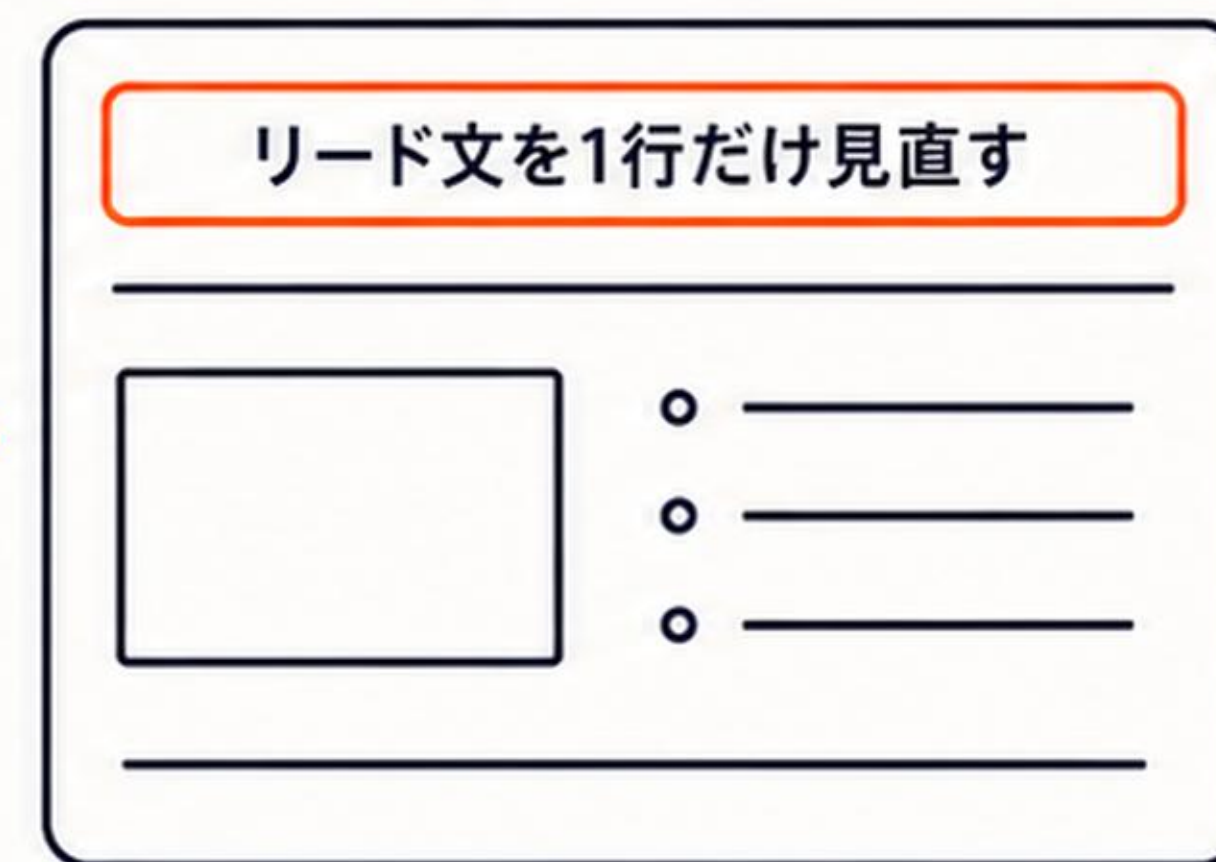
- 修正対象をリード文だけに限定する理由：
ページ内で最重要なのに修正範囲が閉じているのでコスパが最も良い
- NGパターン①「曖昧ワード」：
「最適化する」「効率化する」
「OS」「プラットフォーム」...
- NGパターン②「ボディの目次」：
「特徴は以下の3点」「メリットとデメリット」...

Before



曖昧なリード文が意図を隠してしまう

After



意図が明確になり、内容が伝わる

AI スライド生成ツールが増え「量は作れるが刺さらない資料」が氾濫している中で、直すべき箇所を1行に特定したのが実務的。

本日のトピック一覧

- | | | | |
|----|--|----|--|
| 01 | Claude Code のセッション同士がメッセージを送り合えるようになった | 05 | Claude Managed Agents に4つの更新 |
| 02 | Claude Code の auto mode が既定に | 06 | Agent Plugins は「Skills と MCP をまとめる標準」では終わらない |
| 03 | OpenAI が次期モデル Astra を Preparedness Framework 初の「critical」に分類 | 07 | AI動画『WINGLESS』の制作費と時間が全公開 |
| 04 | SpaceX による Cursor 買収、早ければ来週末に完了か | 08 | AI生成スライドに意図を込める技術 |