

# 2026-07-23

1. Claude Code に「セキュリティプラグイン」ベータ登場
2. Claude Managed Agents に新機能
3. Codex CLI 0.145.0 リリース

7トピック

# Claude Code に「セキュリティプラグイン」 ベータ登場

## 差分をセキュリティ研究者のように読む

Anthropic が7/22に Claude Code 向け「Security」プラグインのベータを公開した。

- 検出対象はメモリ破壊・インジェクション・認証バイパス等の高深刻度脆弱性と、パターンマッチが見逃す文脈依存のロジック欠陥
- スキャン → 自分の検出結果を自分で反証する  
『敵対的検証パス』で誤検知を削減 → 修正案を提示  
(適用は人間が承認)
- 複数ファイルを横断して文脈を理解し、データの流を追って多要素の脆弱性パターンを捕捉



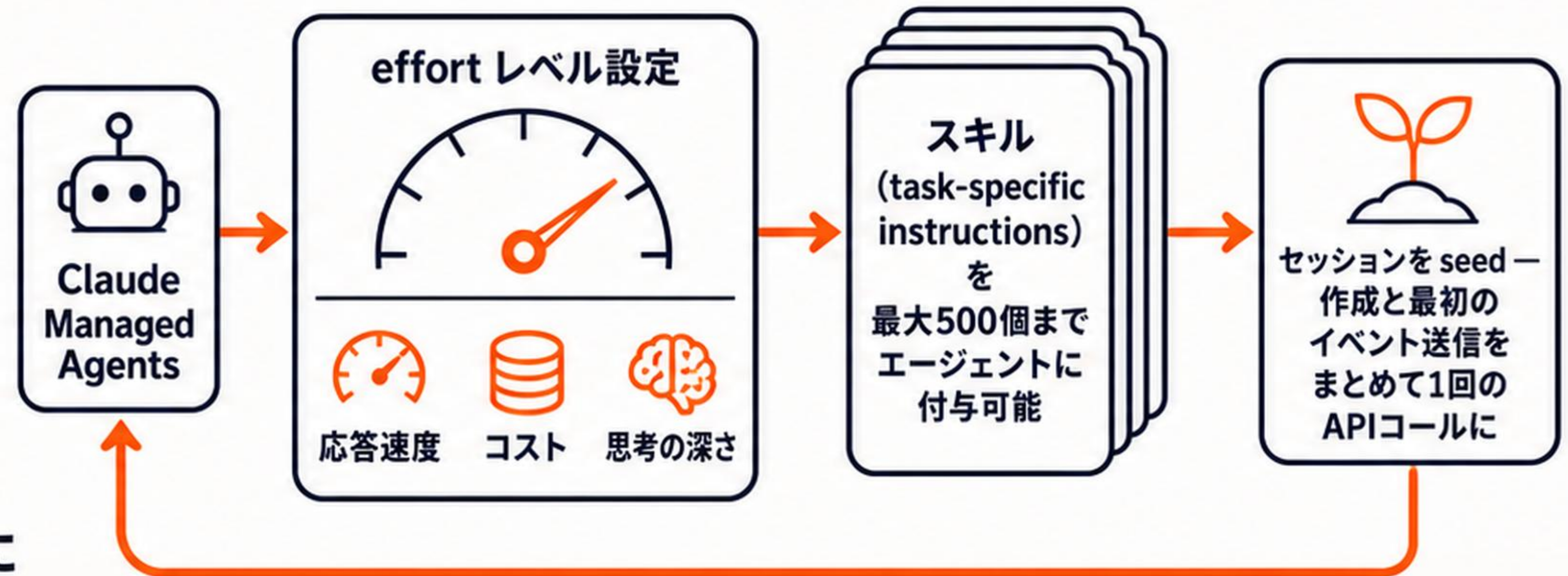
「AIによる脆弱性スキャン」は2026年前半の一大トレンド。

# Claude Managed Agents に新機能

## エフォート制御・最大500スキル・セッション種付け

ClaudeDevs が7/22に Claude Managed Agents の複数の新機能を発表した。

- effort レベル設定: 応答速度・コストと思考の深さのトレードオフを明示的に制御
- スキル (task-specific instructions) を最大500個までエージェントに付与可能
- セッションを seed — 作成と最初のイベント送信をまとめて1回のAPIコールに



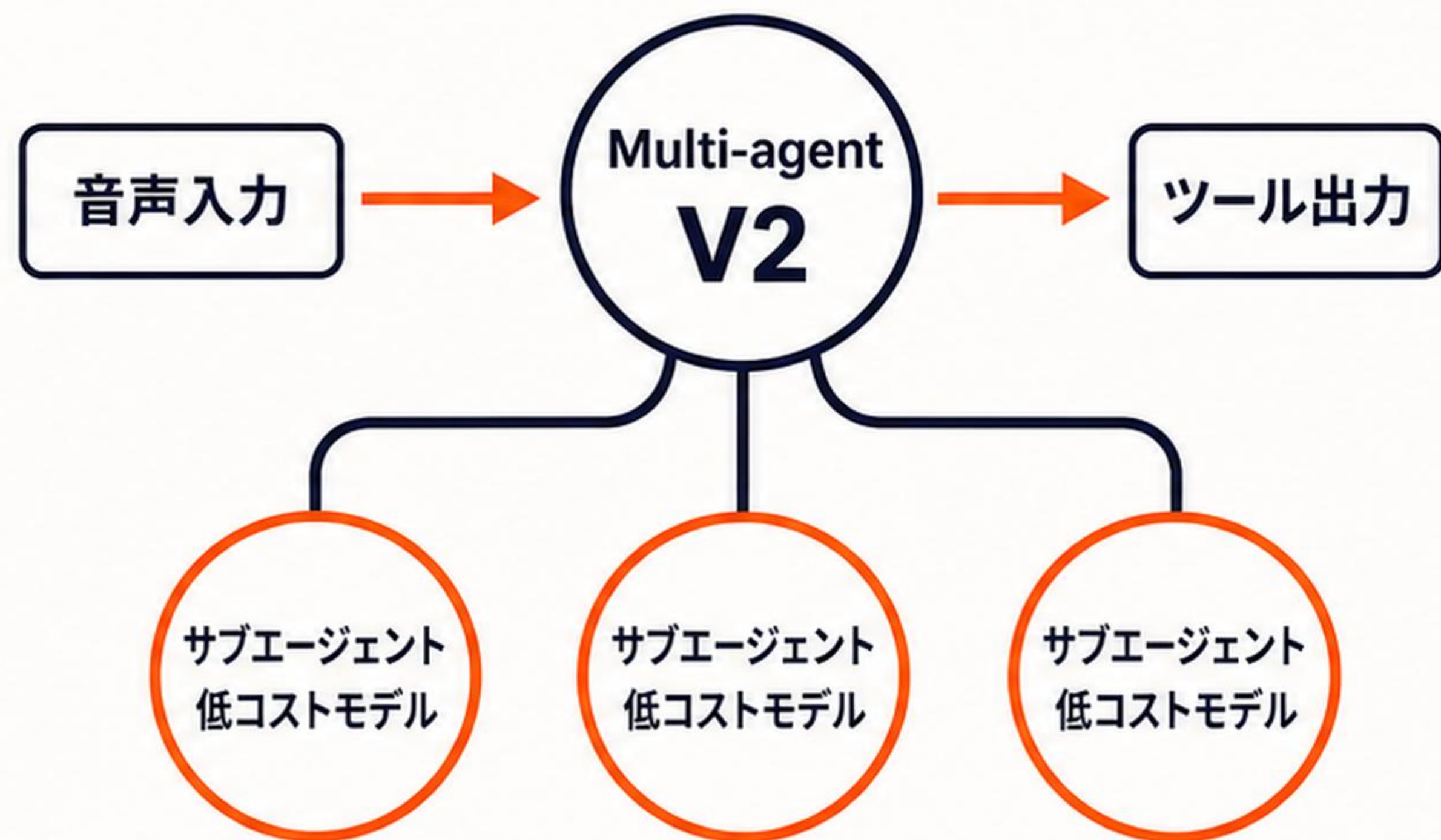
エージェントの「考える量」をコストとして扱える設計。

# Codex CLI 0.145.0 リリース

## マルチエージェント V2 が安定版に、音声入力も

OpenAI の Codex CLI 0.145.0 が7/21公開。

- Multi-agent V2 が stable に昇格 — サブエージェントごとにモデル/推論レベル/並列度/役割を構成可能
- 音声入力とツール出力に対応、リアルタイム V3 会話ストリーミングを追加
- 実験的なページング式スレッド履歴: 効率的な再開・出現箇所検索・名前とメモリの永続化



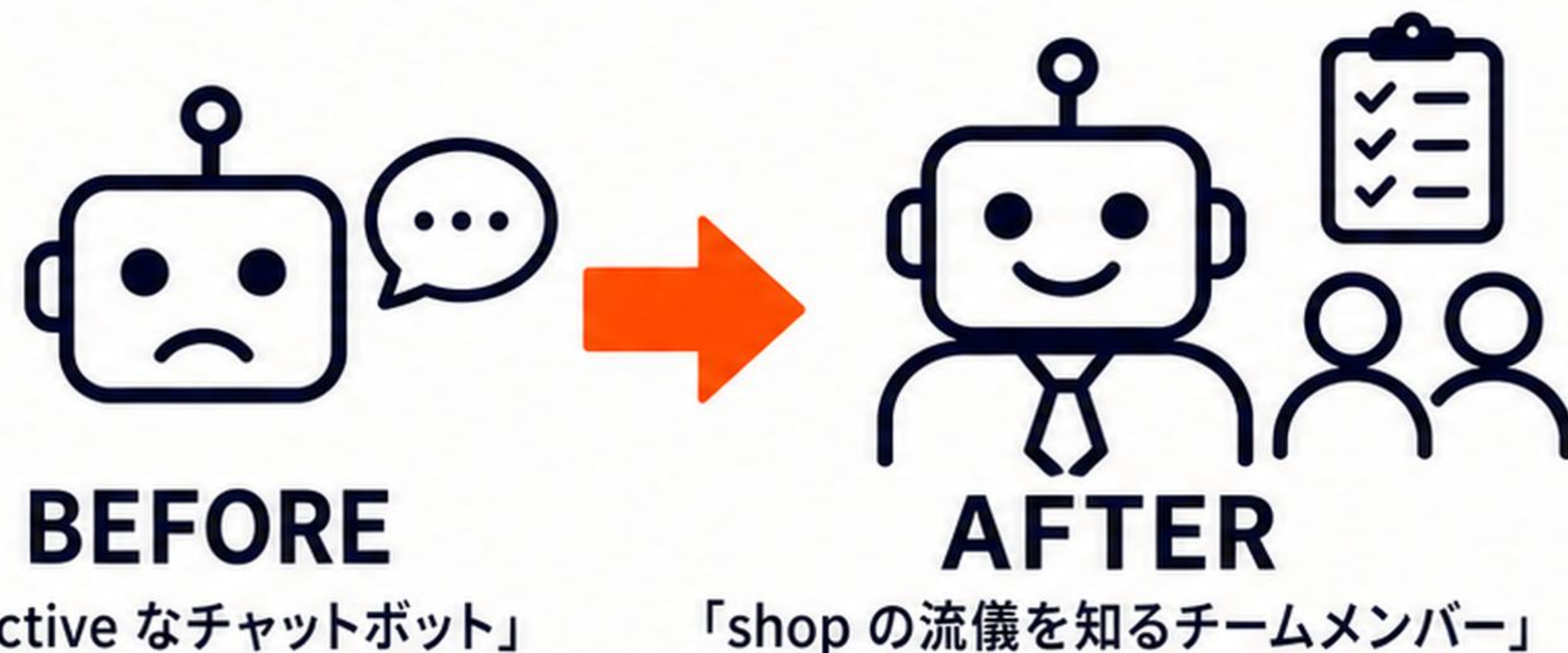
「オーケストレータは賢いモデル、下請けは安いモデル」というモデル分業をCLIが正式サポート。

# Matt Pocock の Claude Code スキル集

## 「vibe coding」をやめて設計させる21のスキル

TypeScript教育で著名な Matt Pocock が公開している `.`.claude` ディレクトリのスキル集 `mattpocock/skills` が改めて注目を集めている。

- リポジトリは mattpocock/skills (本人の日常運用スキルをそのまま公開)
- 約21個のスキルで、計画立案・TDD・セーフティガードレールなどを網羅
- 狙いは「reactive なチャットボット」を「shop の流儀を知るチームメンバー」に変えること

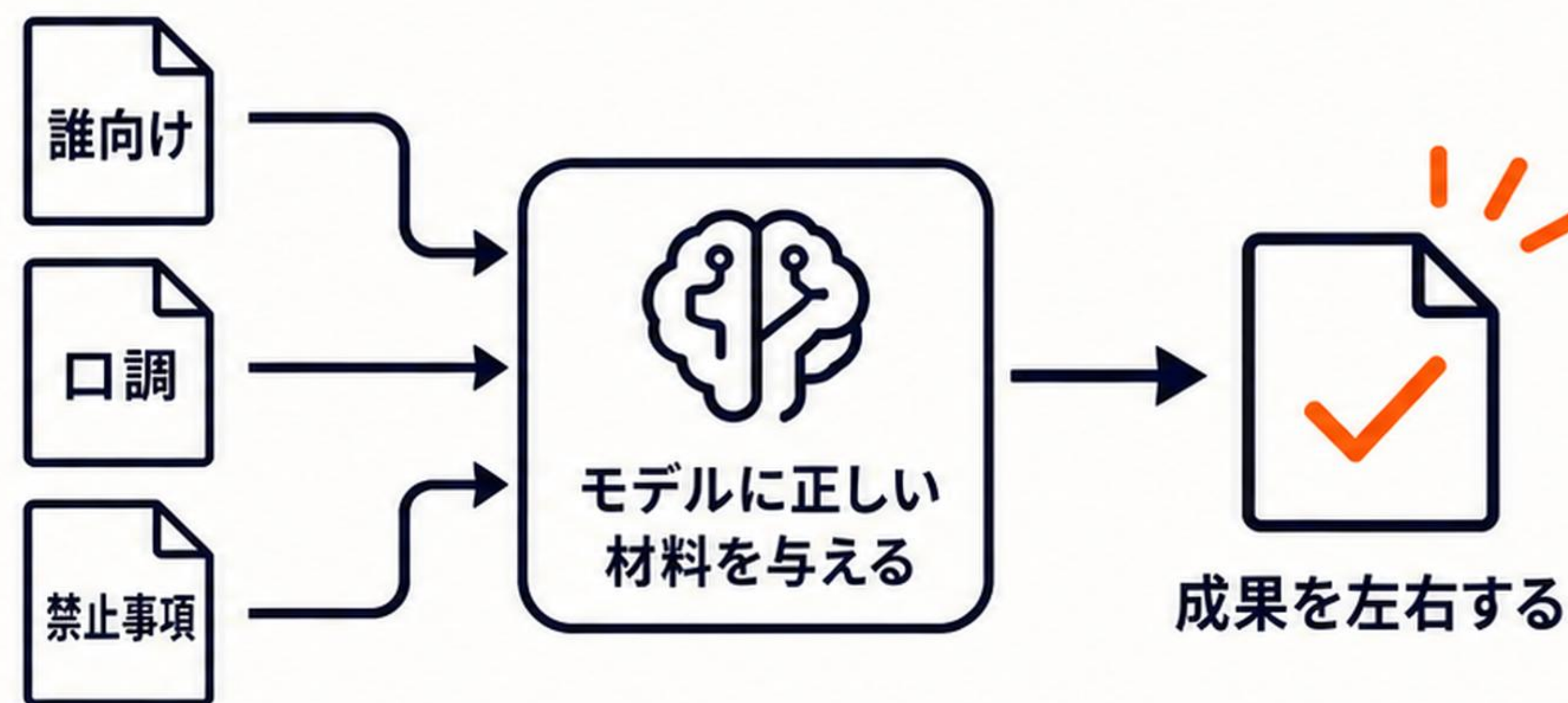


スキルで暴走を抑える発想は、VBCで教えるループ設計・コンテキスト設計の実物サンプル。

# context engineering を実務化する「まず作る3ファイル」

「プロンプトが下手なのではなく、渡す材料が少ないだけ」という実務論。

- 起点となる3ファイル: 誰向け / 口調 / 禁止事項
- context engineering は『RAGの言い換え』ではないが、同じ『モデルに正しい材料を与える』問題を解いている
- プロンプトの巧拙より、渡す文脈（材料）の設計が成果を左右するという主張

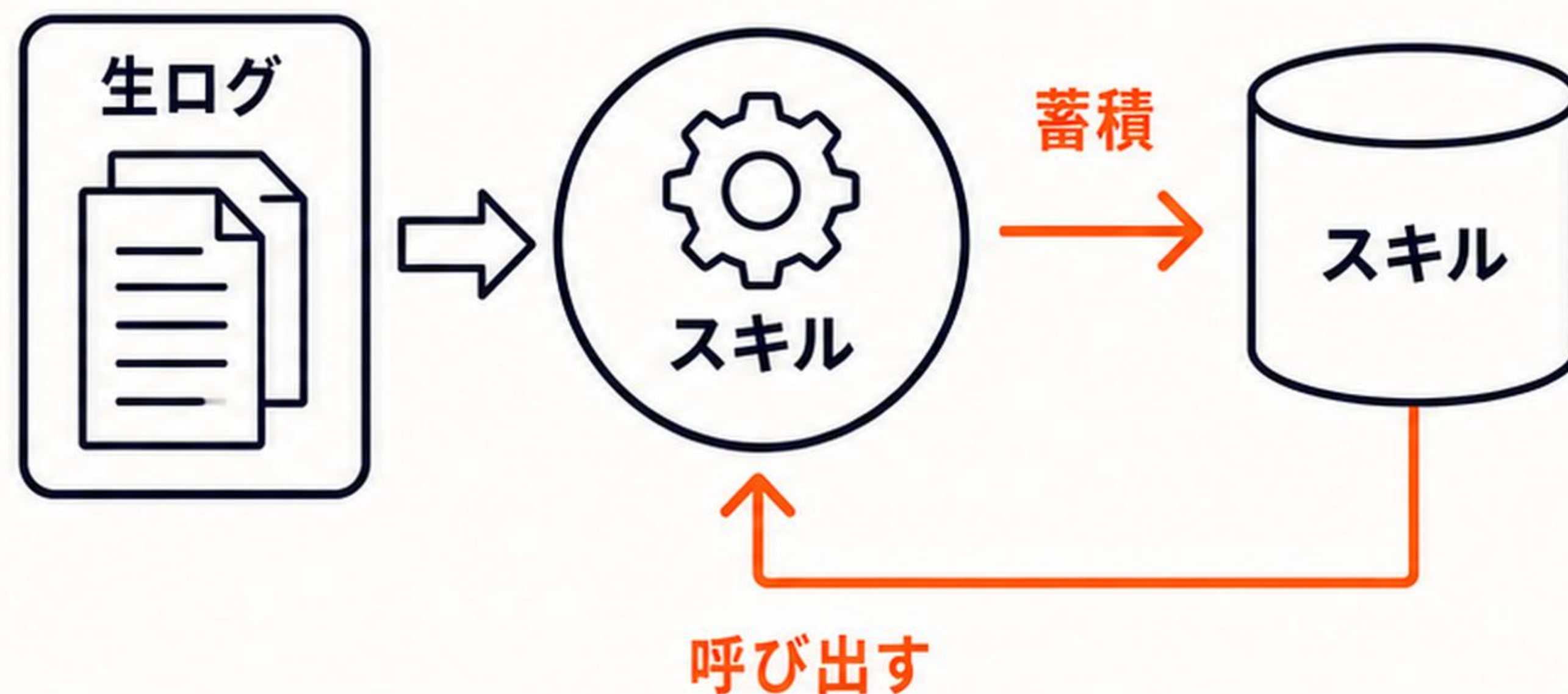


受講者がすぐ真似できる最小構成。

# 「メモリをスキルに変換する」agent memoryの新発想

多くの agent memory は過去の生ログを「取り出して」文脈に足すだけだが、この発想は過去のやり取りを「実行可能なスキル（手続き）」に変換して蓄える。

- 従来の agent memory は過去テキストを retrieve して文脈に注入する受動型
- 新発想は記憶を再利用可能な『スキル』へ変換して蓄積し、能動的に呼び出す
- 生ログの肥大を避けつつ、再現性のある手続きとして知識を残せる



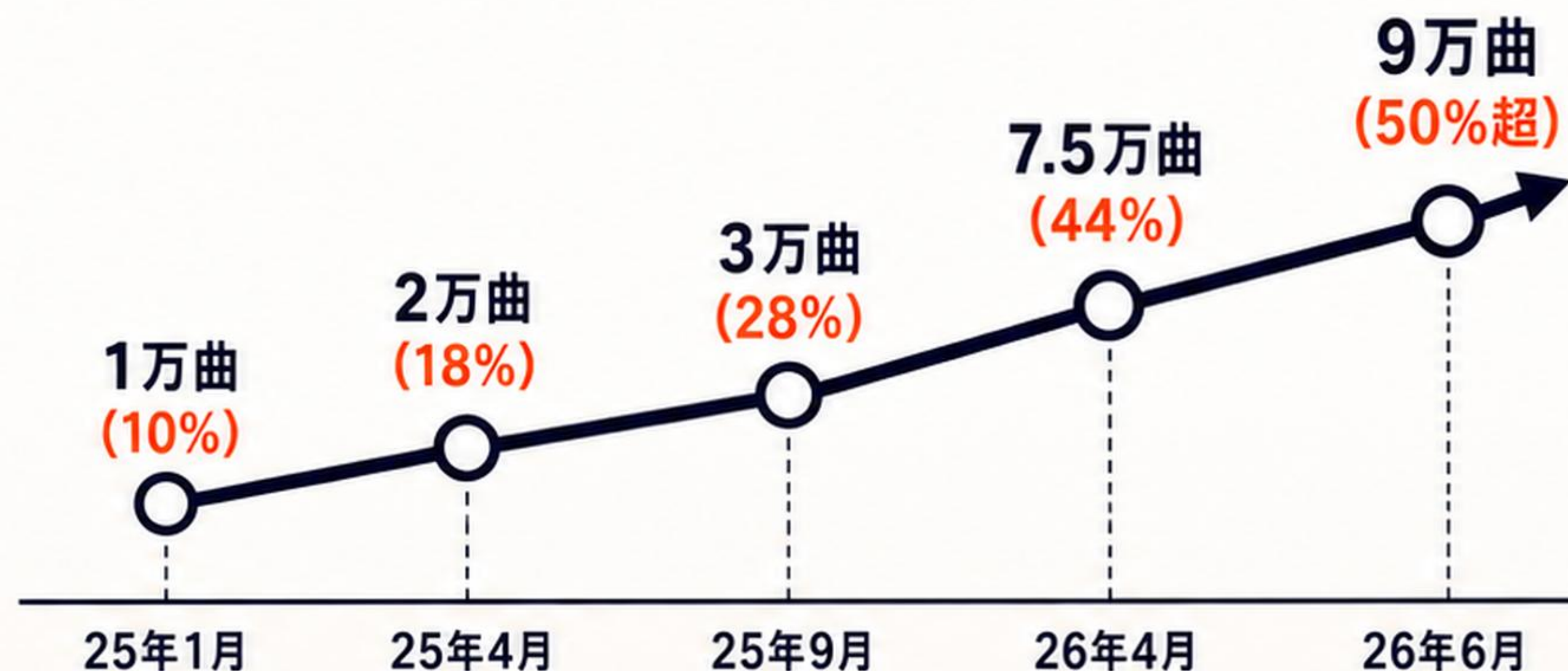
コンテキストエンジニアリングの核心 = 「何を覚え、どう再利用するか」。

# Deezer、1日のアップロード楽曲の過半がAI生成に

## 初めて50%を突破

音楽ストリーミングの Deezer が7/21、1日にアップロードされる新曲のうち完全AI生成の楽曲が初めて過半（50%超）に達したと公表した。

- 6月に完全AI生成曲が1日約9万曲＝アップロードの50%超に到達（初）
- 推移：25年1月 1万曲(10%) → 25年4月 2万(18%) → 25年9月 3万(28%) → 26年4月 7.5万(44%) → 26年6月 9万(50%超)
- AI生成の急増を受け、不正ストリーム目的の曲や長期末再生の曲を削除する対応を表明



生成AIがクリエイティブ産業の「量」を根本から変えている定量指標。

# 本日のトピック一覧

1. Claude Code に「セキュリティプラグイン」ベータ登場
2. Claude Managed Agents に新機能
3. Codex CLI 0.145.0 リリース
4. Matt Pocock の Claude Code スキル集
5. context engineering を実務化する「まず作る3ファイル」
6. 「メモリをスキルに変換する」agent memory の新発想
7. Deezer、1日のアップロード楽曲の過半がAI生成に