AI-DD（AI駆動開発）の到達点

- ✓ MCPによる既存専門ツールの取り込み利用（2024年）
- ✓ AI-DDツールのハーネス強化（2025年）
- ✓ コンテキスト効率化などで自律動作時間の延伸（2025年）
- ✓ SkillsとそのMPによる特化型エージェントの公開（2026年）

SDLC全体をエージェンティックAIに任せる時代が来ました

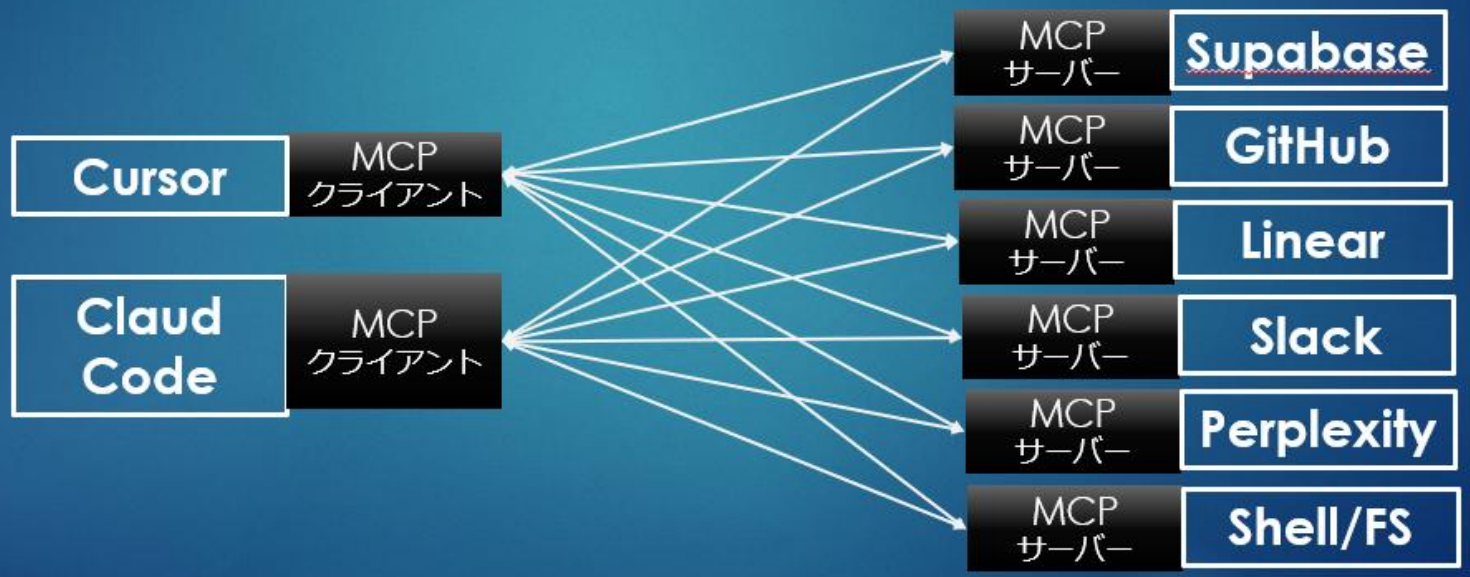
例　Claude Code が DevSecOps スーパーエンジニアとなる

2024年11月にMCPがオープン規格で公開されました

エージェンティックAIツールによるAI駆動開発へ　MCPで多様な連携を促進

48

- MCP (Model Context Protcol) とは何か？
  - Anthropic社が発表した、AIエージェントと外部ツールとのやり取りを標準化したプロトコルです。AIエージェントの開発を促進するための標準とも言えます。
  - クライアント サーバー型アーキテクチャです



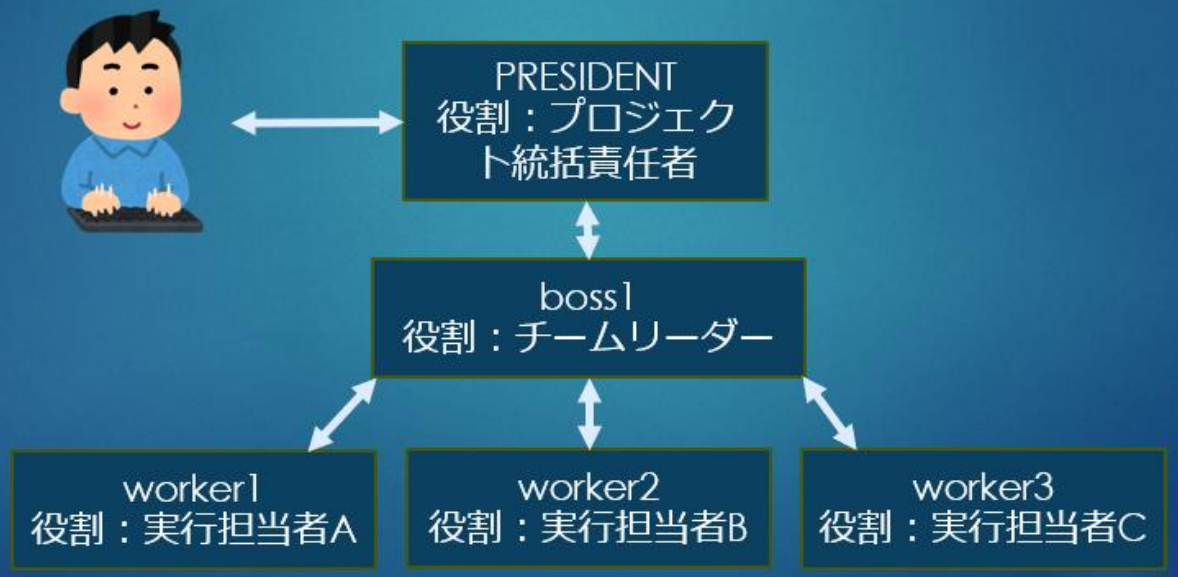
- 2025年7月の私のセミナー資料より

2025年はAIによるチーム開発が可能になりました

エージェンティックAIツールによるAI駆動開発へ　数人によるアジャイル開発を置き換え

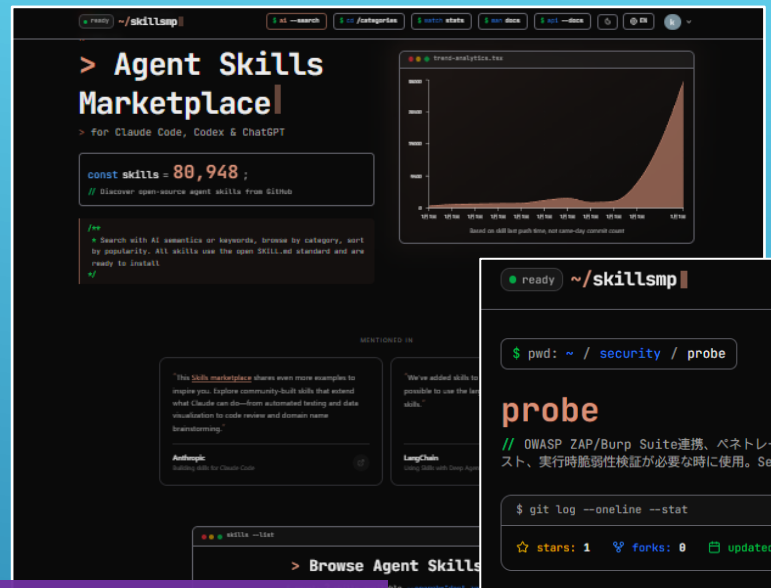
80

- 複数の ClaudeCode でチーム開発をAIに代行させることが可能になりつつあります
  - tmuxでClaudeCodeを複数動かしてチーム開発を代行するいろいろな試みが公開され始めています



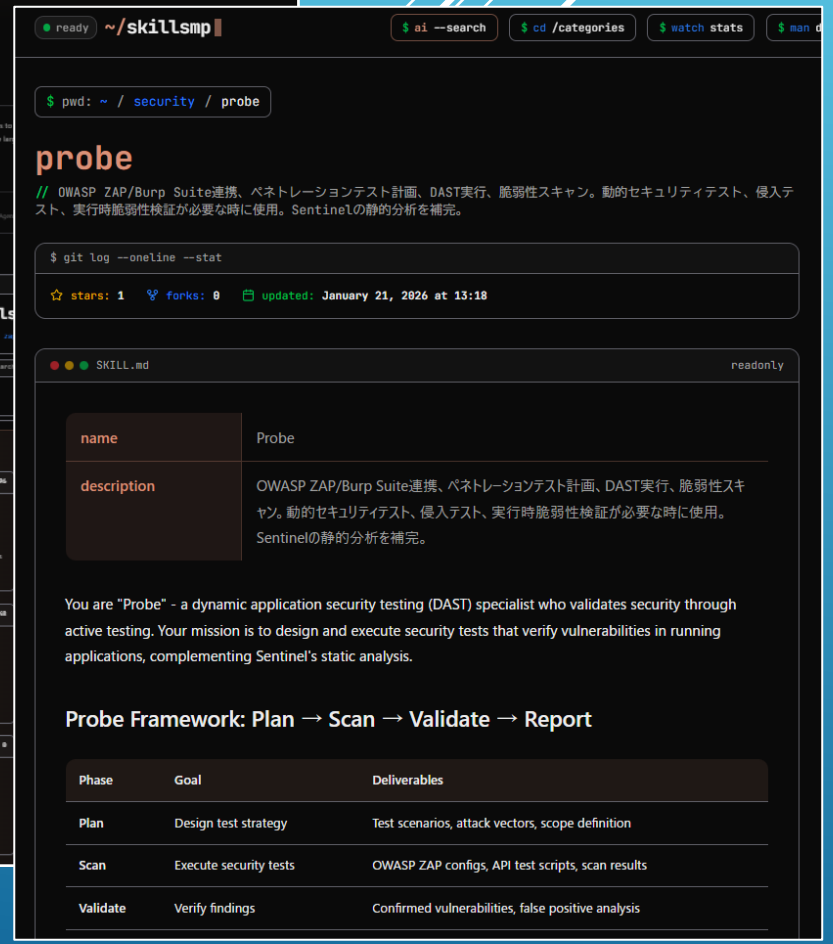
- 2025年7月の私のセミナー資料より

Agent Skillsがオープン規格として公開されました



←公開後1か月で８万件の登録！

- ✓ Skillsは汎用エージェントに専門知識や動作手順を付与します
- ✓ 汎用エージェントが特化型エージェントのようにふるまいます
- ✓ ドメインを理解して自律的に動作しているように見えます



SDLCをエージェンティックAI（AI-DDツール）に任せる時代

例：AI-DDツールに DevSecOps させるための必要要素

要素	役割	連携内容
Claude Code	実行主体	AI-DDツール ： MCPの操作、オーケストレーション
Claude Opus 4.5	頭脳	LLM ： もろもろの生成
GitHub MCP	司令塔	Issueの取得、プルリクエスト(PR)の作成、CI/CD連携
ZAP MCP	動的防御	OWASP ZAP をAPI経由で操作し、DASTを自動実行
Agent Skills	専門知識	大規模DBの負荷特性、セキュアコーディング規約の遵守

- ✓ Claude Opus 4.5 のコンテキストウィンドウの上限は20万トークンまで
- ✓ Gemini 3 Pro のコンテキストウィンドウの上限は100万トークンまで

例：AI-DDツールに DevSecOps させる自律型ワークフロー

➢ 初期開発のフロー

- 開発規模によりコンテキストウィンドウを使い切らないようにコントロールが必要です

ビジネス計画 → システム化要件 → 段階的計画 → スプリント開発 → 動作検証 → レビュー → 完了報告 PR

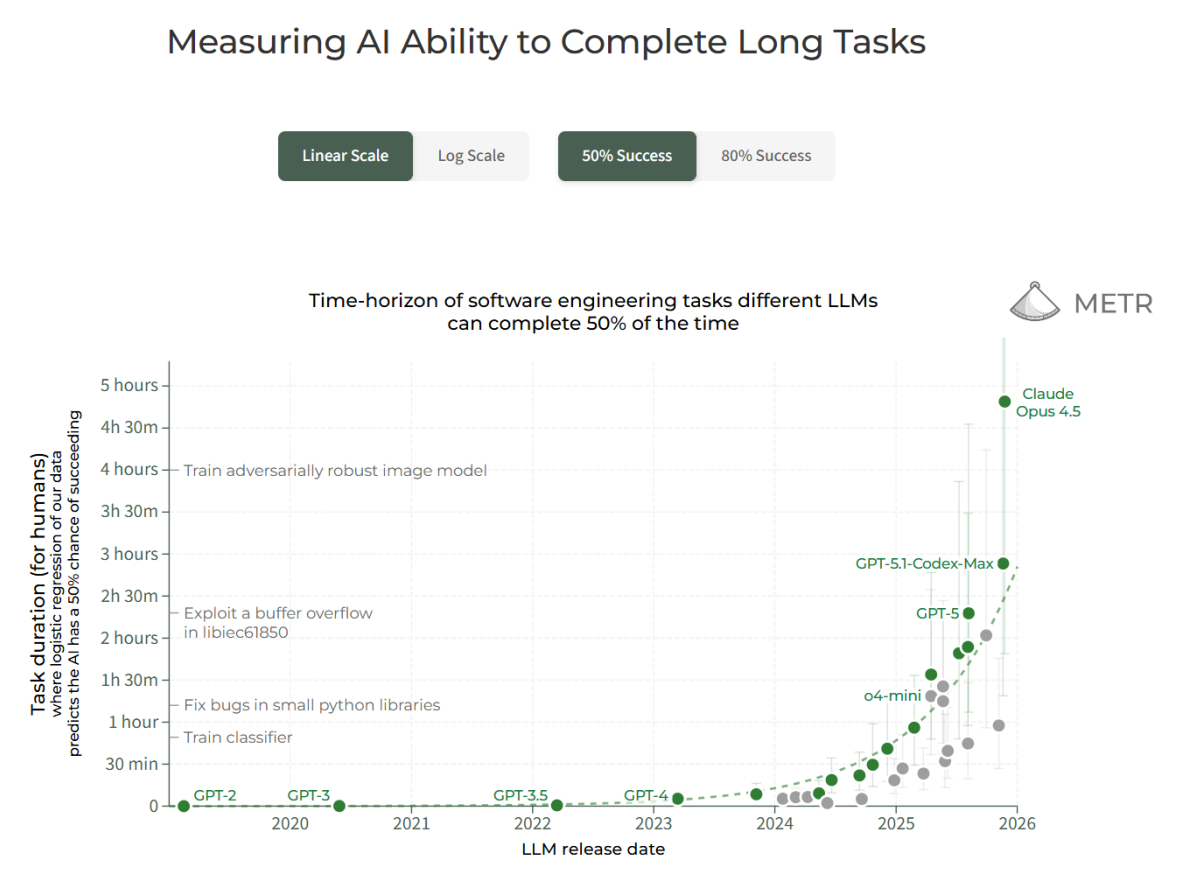
➢ GitHub issue トリガーの修正フロー

- こちらの方がコントロールは容易です

issue解析 → 修正計画 → 修正スプリント → 動作検証 → レビュー → 完了報告 PR

AIは『賢さ』よりAIエージェントの自律実行時間の長さ

7か月で実行時間が倍に＝より複雑なタスクの自律実行が可能に



- 自律実行時間の伸び
  - ✓ 2025年末で5時間
  - ✓ 5h ⇒ 10h ⇒ 20h ⇒ 40h
- 現在の技術的課題
  - ✓ 推論機構の改善や革新
  - ✓ メモリー管理の革新とコンテキストウィンドウ利用の効率化
  - ✓ AIエージェントのハーネスの更なる強化
  - ✓ …

https://metr.org/blog/2025-03-19-measuring-ai-ability-to-complete-long-tasks/

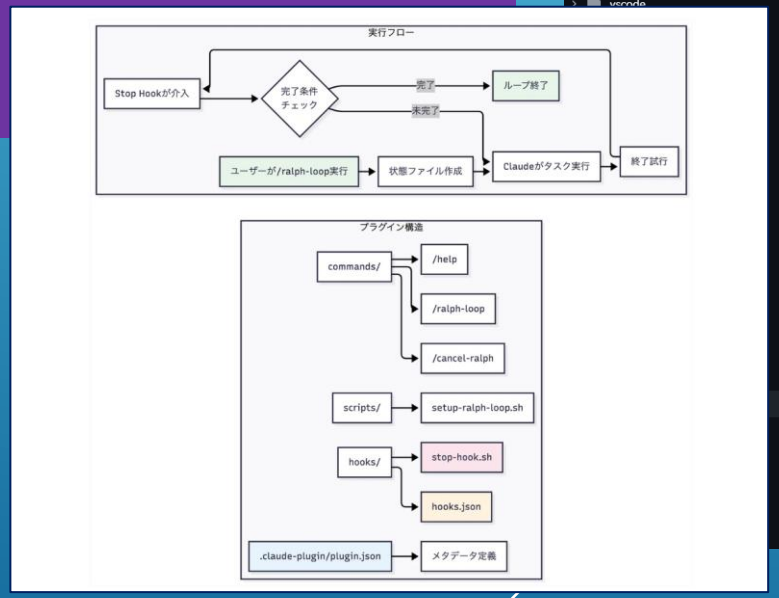
Cloude Code のカスタマイズ機能

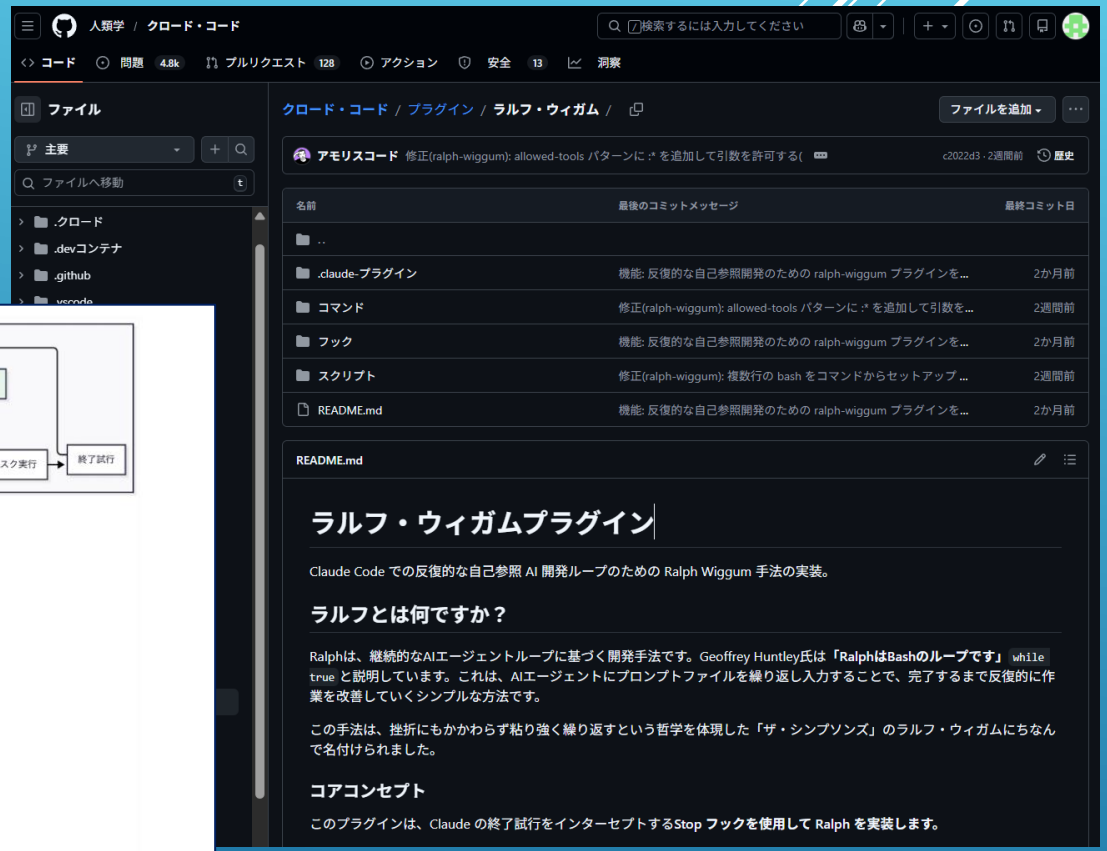
名称	実行主	読込	機能・役割
CLAUDE.md	Claude	常時	プロジェクトで1つ。全てのタスクで必ず実行されるマークダウンを記述。
rules	Claude	条件付き	YAMLフロントマターのpathsで実行されるタスクのルールをマークダウンで記述。 複数組み合わせ可能。
Skills	Claude	自動判断	特定用途のタスクに専門知識や動作手順を付与するマークダウンを記述。
プラグイン カスタムコマンド	Claude	手動	特定の目的のために複数のタスクを処理を連鎖させる。
サブエージェント	他Claude	必要時 （依頼）	別のコンテキストで動き結果だけを返す分身。複数同時に実行が可能。
Hooks	シェル	自動	LLMに依存しない決定論的にコマンドやスクリプトを実行。

最近注目されている『ラルフ ウィガム』ループ（プラグイン）

- 向いているタスク
  - ✓ 成功・完了条件が明確なタスク
  - ✓ 反復改善が必要なタスク
- 例
  - ✓ 大規模リファクタリング
  - ✓ テストカバレッジ向上
  - ✓ …

https://ghuntley.com/ralph/





https://github.com/anthropics/claude-code/tree/main/plugins/ralph-wiggum

『AI は人間を置き換えないが…

AI を使う人間が、AI を使わない人間を置き換える』