

プロンプト・エンジニアリングの終焉： AIエージェント時代の「陳腐化しない」管理術

旧来のプロンプトが「有害」になる理由



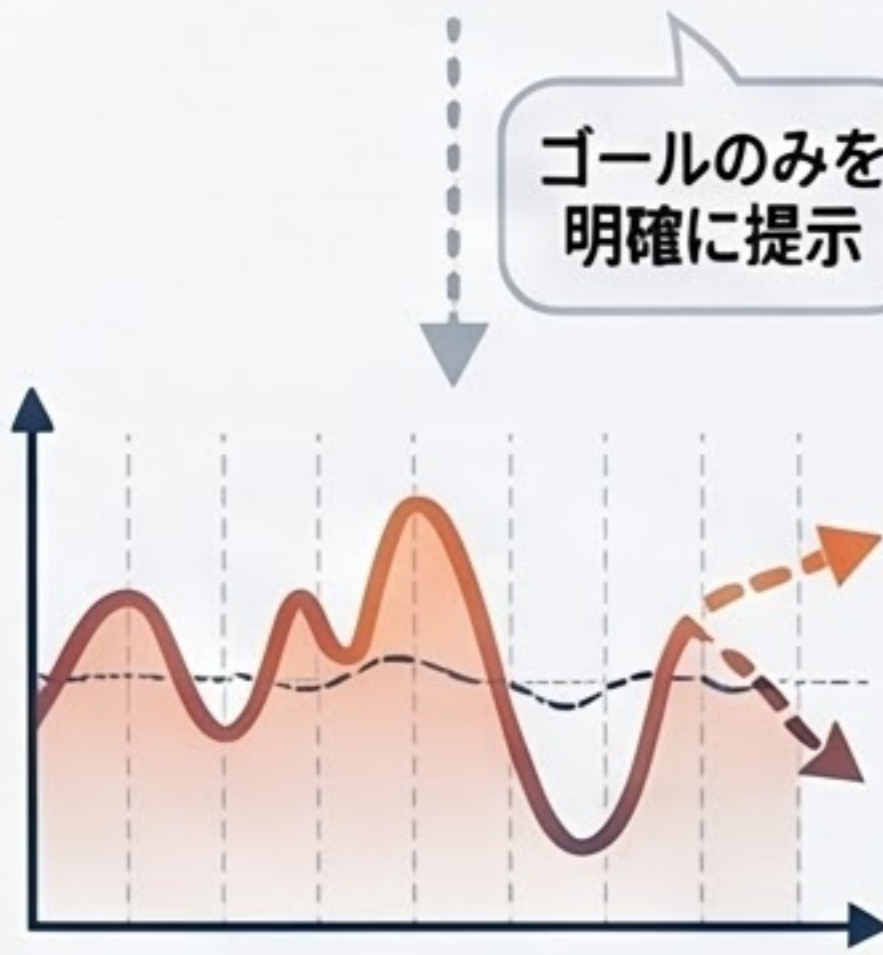
旧来モデル (GPT-4等)

「内的CoT」：
自律的な内的思考プロセス



最新先端モデル

「結果重視
(Outcome-first)」
への転換



サイレントな「モデルドリフト」の脅威
一度完成したプロンプトに依存する
設計は本質的に脆弱です。

「外的CoT」：段階的に考えて
過度な指定は権限を制限し、
稜度を低下させます。

DSPyによる 「プロンプトの自動コンパイル」



モデル変更時の
自動再構築で
稜度向上



DSPy Optimizer



「職人芸」から「アルゴリズム」へ
データに基づいた自動コンパイルへと
開発プロセスが進化します。

モジュール化と標準化による 堅牢な設計

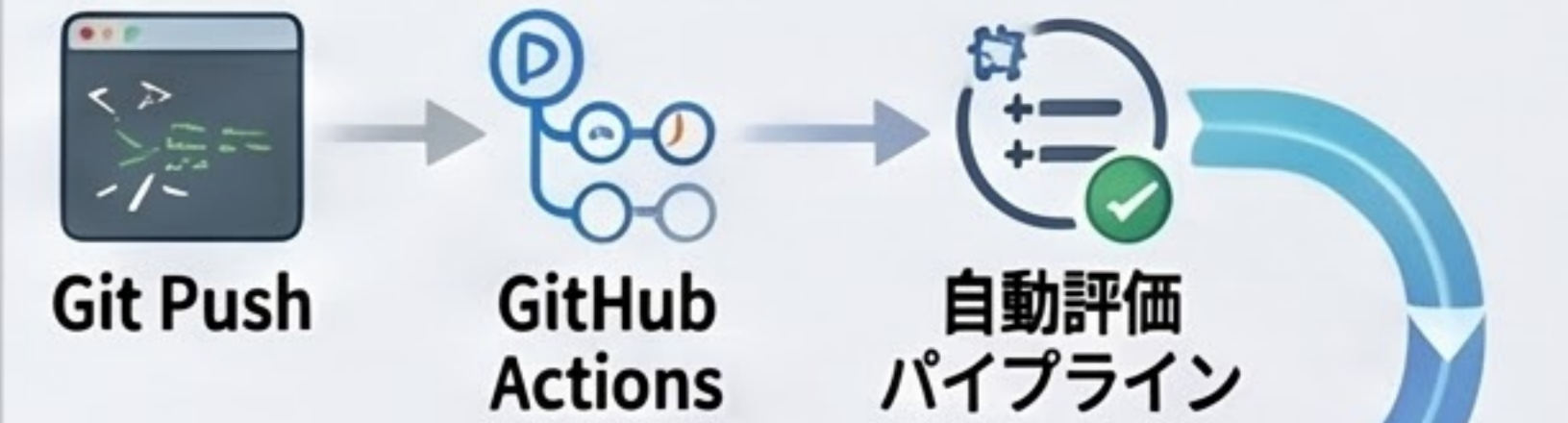
MCP (Model Context Protocol) の導入
LLMと外研ツール間の通信を標準化
し、ツール接続を抽象化。



MCP (Model Context Protocol) の導入
LLMと外部ツール間の通信を標準化し、
ツール接続を抽象化。

必要な時だけ詳細な指示をロードする
「段階的開示」アーキテクチャ。

評価駆動開発 (EDD) と CI/CDパイプライン



リグレッション (性能退化) の防止



ゴールデンデータセット
過去の失敗事例を含む
データセットで常に検証。

評価項目	従来LLMテスト	評価駆動開発 (EDD)
パス基準	完全一致などのバイナリ判定	複数次元の品質スコアリング
失敗時の対応	人間による手動レビュー	前後比較(Diff)による自動特定
適応性	低い (手動更新が必要)	高い (継続的・動的な評価)