智能体

任务执行 · 工具调用与反馈

在本网站语境中，智能体是能够根据任务状态选择步骤、调用工具并检查结果的人工智能系统。它需要模型之外的工具接口、运行状态、停止条件和授权机制。

01 工作方式

01 理解目标，确定可用数据、工具与允许执行的范围。

02 按当前状态选择行动，读取工具结果并调整下一步。

03 达到完成条件或触发异常后停止，输出结果与过程记录。

02 场景应用

01 自动汇集数据并形成有来源的分析草稿。

02 在授权范围内协助处理异常工单或资料核查。

03 边界与常见误区

01 固定代码顺序执行的工作流与动态智能体应加以区分。

02 自主调用工具会增加时延、费用和错误传播风险。

03 涉及业务写入的工具需要独立权限与确认机制。

04 来源与阅读说明

依据下列一手资料原创归纳；场景与工程建议为编辑整理，不是来源机构对本站服务的背书。

智能体研发机构官方文章 · 构建有效的智能体

https://www.anthropic.com/research/building-effective-agents