M3 · 第 7 讲

认识智能体

什么时候值得把活交出去

阅读约 30 分钟

练习约 30 分钟

产出：一张自动化流程图

本节目录

开场：每天重复的那半小时

本课目标

一、Agent 的四个部件

二、和聊天机器人的区别

三、三个条件：值不值得做

四、三类智能体

五、平台能力清单

六、成本与风险

七、30 分钟练习

八、检查清单

九、延伸阅读

开场：每天重复的那半小时

整理会议纪要、把客户反馈同步到表格、每周一生成数据简报——这些事不难，但每天都要做，做完又记不住做到哪了。

聊天机器人能帮你做一次，智能体（Agent）能替你做很多次。区别不在模型更聪明，而在它多了三样东西：**工具、记忆、循环**。

本课目标

- 用一句话说清 Agent 和聊天机器人的区别；
- 用三个条件判断一个流程值不值得做成智能体；
- 分清问答型、流程型、自主型三类；
- 画出你要自动化的那张流程图。

一、Agent 的四个部件

部件	作用	例子
目标	它要完成什么	每天生成销售简报
工具	它能调用什么	读表格、发消息、查网页
记忆	它记得什么	上次跑到哪、用户偏好
循环	它如何推进	观察 → 决策 → 行动 → 再观察

没有工具的“Agent”，只是换了皮肤的聊天机器人；没有循环的，只是一次性脚本。

二、和聊天机器人的区别

维度	聊天机器人	智能体
交互	你问一句，它答一句	你给目标，它自己推进
工具	基本没有	能读写文件、调接口

维度	聊天机器人	智能体
状态	每次从零开始	记住上下文与进度
失败	答错就结束	会重试、会求助
适合	一次性内容任务	重复、多步、可验收的流程

一句话：**聊天机器人给你答案，智能体给你结果。**

三、三个条件：值不值得做

1. **高频**：每周至少 3 次，否则手工更省；
2. **规则稳定**：步骤基本固定，例外少；
3. **可验收**：结果对错能一眼判断，或能用规则检查。

三个都满足，再做。只满足一个，先写 SOP，不要急着上智能体。

四、三类智能体

问答型

基于你的文档回答问题。适合客服、内部制度、产品手册。关键是文档质量与检索。

流程型

按固定步骤执行：收邮件 → 提取信息 → 写表格 → 发通知。适合运营、财务、行政。

自主型

给一个目标，自己规划步骤。适合调研、监控，但对验收和权限要求最高。初学者先从流程型做起。

五、平台能力清单

选平台时，不看演示效果，看这五项：

- [ ] 能不能挂自己的知识库；
- [ ] 能不能调用外部工具/接口；
- [ ] 有没有人工确认节点；
- [ ] 有没有运行日志与失败重试；

- [ ] 权限能不能限制到人/部门。

缺任何一项，规模化后都会变成坑。

六、成本与风险

风险	表现	对策
幻觉	自信地给出错误结论	强制引用来源、关键节点人工确认
越权	读了不该读的数据	最小权限、按角色隔离
失控	循环调用、重复发送	设最大步数、幂等、冷却时间
难维护	提示词越堆越长	拆子流程、写清输入输出

七、30 分钟练习

1. 写下你每周重复 3 次以上的一件事（5 分钟）；
2. 用三个条件打分（5 分钟）；
3. 画出流程：开始 → 步骤 → 判断 → 结束（10 分钟）；
4. 标出哪一步必须人工确认（5 分钟）；
5. 写下它的输入与输出（5 分钟）。

八、检查清单

- [ ] 我能说清目标、工具、记忆、循环；
- [ ] 这件事每周至少发生 3 次；
- [ ] 结果对错可以验收；
- [ ] 流程图里有失败与人工确认分支；
- [ ] 权限是最小可用。

九、延伸阅读

- 知识库 1.3 AI Agents（智能体）

- 知识库 2.0 AI 编程
- 知识库 4.3 团队搭建：AI 招聘/组队

> 下一讲：搭第一个智能体。我们用“会议纪要整理”做例子，从零走到可用。
