M3 · 职业版 Agent · 第 2 讲

第 2 讲：工具调用与记忆

能动手，也要记得住

阅读约 25 分钟

练习约 30 分钟

产出：三个工具 + 记忆策略

本节目录

一个真实故障

本讲目标

一、工具描述五要素

二、最小工具集

三、幂等与重试

四、三层记忆

五、什么不该记

六、30 分钟练习

七、验收清单

八、延伸阅读

一个真实故障

会议纪要助手调用“发送邮件”工具失败，重试了三次。结果客户收到三封一样的邮件——因为工具不是幂等的，Agent 也不知道自己重复了。

工具设计得好不好，决定了 Agent 是“能干活的助手”还是“会闯祸的脚本”。

本讲目标

- 写出让模型能正确调用的工具描述；
- 用最小工具集完成一个流程；
- 设计三层记忆，知道什么该记、什么不该记；
- 处理超时、重试与重复调用。

一、工具描述五要素

要素	写法	反例
名字	动词_对象，如 send_email	tool1
用途	一句话说清什么时候用	“很强大的工具”
参数	类型、必填、取值范围	只写“参数”
返回	成功/失败的结构	返回一大段自然语言
错误	可重试还是终止	统一报“出错了”

描述不是给人看的文档，是给模型的决策依据。

二、最小工具集

一个纪要流程只需要三个工具：

1. 读取转写文本；
2. 写入纪要文档；

3. 发送通知（需确认）。

不要一上来接十个系统。工具越多，选错的概率越高。

三、幂等与重试

- **幂等**：同一个请求执行多次，结果一致（如“写入指定 id”）；
- **非幂等**：每执行一次就多一条（如“发送邮件”“下单”）。

非幂等工具必须带唯一键，并在重试前查询是否已执行。重试次数上限 2 次，超出转人工。

四、三层记忆

层	存什么	生命周期
会话记忆	当前任务的上下文	一次会话
长期记忆	用户偏好、常用模板	跨会话，可清除
外部知识库	制度、产品文档	长期，按版本更新

记忆不是越多越好。记错的信息，比不记更危险。

五、什么不该记

- 密码、密钥、身份证号；
- 客户未授权的个人信息；
- 一次性的临时数据；
- 过期政策与旧价格。

写一条“记忆清理”规则：超过 90 天未使用的偏好自动归档。

六、30 分钟练习

1. 为一个流程写三个工具描述（10 分钟）；
2. 标出哪个工具非幂等，补唯一键（5 分钟）；

3. 设计三层记忆各存什么（10 分钟）；

4. 写一条清理规则（5 分钟）。

七、验收清单

- [ ] 每个工具有名字、用途、参数、返回、错误；
- [ ] 非幂等工具有唯一键与重复检查；
- [ ] 重试有上限，超出转人工；
- [ ] 记忆分层，敏感信息不落库；
- [ ] 有过期与清理规则。

八、延伸阅读

- 知识库 `1.3 AI Agents（智能体）`
- 知识库 `4.3 团队搭建：AI 招聘/组队`

> 下一讲：评测与验证。工具接好之后，先证明它“做对了”，再谈常驻。
