| 第 1 章 |

# 什么是 OpenClaw ——不只是更智能的聊天机器人

### 本章导读

这一章，我想先跟你聊聊我自己“养龙虾”的故事。然后我们一起搞清楚几个基本问题：OpenClaw 到底是什么？它跟你平时用的 ChatGPT、Kimi、豆包等有什么本质不同？以及——为什么我认为每个人都应该拥有自己的 AI 分身。

## 1.1 一个 AI“老兵”的“养龙虾”日记

其实，我第一次听说 OpenClaw 的时候，完全没当回事。

这里要先交代一下我的背景——不是为了显摆，而是为了让你理解——为什么我一开始对 OpenClaw 这么不重视，后来又彻底改变了态度。

我叫刘文勇，从事教育很多年，但跟 AI 的缘分其实更早。从职业生涯一开始，我就一直在折腾各种教育科技产品。后来又写了一本名为《AIGC 重塑教育》的书，讲 AI 如何改变教育行业——这本书问世后获得了不错的反馈。

所以你看，我不是一个 AI 新手。从大模型刚开始冒头的时候，我就在研究它们怎么跟教育场景结合。到了 2025 年下半年，我的工作习惯已经发生了翻天覆地的变化——写代码基本靠 vibe coding 了。什么意思呢？就是我跟 Claude Code 或者 Cursor 说一句“帮我写一个 × × × 功能”，它就会把代码给我写出来，我看一眼差不多了就直接用。有时候甚至连看都不看，直接运行，出了 bug 再让 AI 自己修改。以前我写一个数据分析脚本可能要花半天，现在十分钟就搞定了。

你想想，一个已经这样深度使用 AI 的人，再看到一个新的 AI 工具，第一反应会是什么？

又来了？

对，这就是我 2026 年 1 月底的反应。朋友圈突然被一只红色的小龙虾刷屏了。有人说这是“开源版 Jarvis”，有人说它是“真正能干活的 AI”，还有人说它能帮你清理邮箱、管理日程、自动写代码——总之，吹得天花乱坠。

我见过太多“革命性”的产品发布了。作为一个教育科技的从业者，我深知技术圈的一个规律：越是被吹上天的东西，落地的时候摔得越重。每隔几个月就有一个新的 AI 工具号称要改变世界，然后你用了两天，发现它不过是换了个皮肤的聊天机器人。

但这一次，最先打动我的不是国内的朋友圈，而是硅谷的朋友。

我在硅谷有一批做技术创业的老朋友。这帮人平时对新产品的态度是出了名的挑剔——毕竟他们自己就是做产品的，什么没见过？但那段时间，我发现他们一个接一个地在聊 OpenClaw。不是那种“哦，我试了一下还行”的客气评价，而是真的在用，真的在往自己的工作流里塞，真的在兴奋地讨论各种配置技巧。

有一个在硅谷做 SaaS 的朋友甚至专门买了一台 Mac Mini 来运行这个东西——他管这叫“养龙虾”。

“你得试试，”他在微信上跟我说，“这个东西不一样。我做了这么多年软件，第一次觉得 AI 真的可以当一个员工来用了。”

这句话打动了我。因为我知道他的判断力，也知道他不是那种容易被忽

悠的人。

我半信半疑地开始了自己的“养龙虾”之旅。

## 第一天：手忙脚乱

说实话，安装本身只需要如下这行命令，但后续的配置过程比我想象的复杂一点。

```
npm i -g openclaw
```

虽然我平时已经习惯了 vibe coding，对各种命令行工具也算熟悉，但 OpenClaw 的配置文件体系还是让我琢磨了许久。不过对我来说，折腾本身就是乐趣的一部分——做了这么多年教育科技产品，我对这种“先啃配置、再享甜头”的过程太熟悉了。（如果你完全没有这方面经验，也别担心，这本书会用最友好的方式教你搞定这一切，第 4 章见）

装好之后，我把它连上了 iMessage。发了第一条消息：“你好。”

它回复了。不是那种模板式的“你好！我是 × × ×，有什么可以帮助你的？”而是一段很自然的话——因为我在它的“灵魂文件”（SOUL.md）里写了一句“说话别太客气，直接进入正题”。

那一刻，我有点惊讶。但也仅此而已。

## 第一周：从好奇到离不开

真正让我改观的，是第三天的一件小事。

那天早上八点，我还没打开手机，iMessage 弹出如下消息。

> 今天上午 10 点你有一个跟区域经理的会议。昨天他们发了三封邮件，我帮你整理了要点：1. 苏州中心的续费率比上月提升了 3 个百分点；2. 哈尔滨中心希望追加市场预算；3. 广州中心提交了新的课程排期方案，需要你签字确认。我把相关文件都整理在一个文件夹里了。

我没有让它做这些事。或者说，我确实在第一天配置的时候，顺手在 HEARTBEAT.md 文件里写了一句“每天早上检查一下我的邮箱和日历，有重要的事情提醒我”。但我当时写完就忘了。

它记住了，而且不只是记住——它理解了“重要的事情”是什么意思。

它知道跟区域经理的会议对我来说很重要，知道提前整理议程材料是有用的。这种“理解”当然不是真正的人类式理解——它本质上是大模型根据上下文做出的推断——但在实际使用中，效果是一样的：我需要的信息，在我需要的时间，出现在了我面前。

到第一周结束的时候，我已经让它帮我做了以下这些事。

（1）每天早上 8 点发来当日会议和待办事项摘要。

（2）自动整理区域经理发来的业绩数据，生成简报。

（3）帮我把课堂录音转换成结构化的讲义初稿。

（4）每周五下午自动生成本周工作复盘，发到我的 iMessage。

这些事情，没有一件是特别了不起的“黑科技”。但它们加在一起，每天至少帮我省了两个小时。

更关键的是——它越用越好。我用得越多，它就越了解我的工作习惯、我的偏好、我关注的数据维度。到后来，它整理出来的会议简报几乎跟我自己写的一模一样。第一周的简报还需要我修改不少，到第三周基本上我只要扫一眼，确认了就行了。

这就是我“养龙虾”的第一周。

## 一个月后：我开始认真了

一个月后，我决定写这本书。

坦白说，我一开始是有些犹豫的。毕竟 2024 年我刚出版《AIGC 重塑教育》，现在才过了一年多，又要写一本与 AI 相关的书？会不会太快了？读者会不会觉得我在炒冷饭？

但我很快想通了。因为 OpenClaw 代表的东西，跟我之前写的内容完全不在一个层面上。

《AIGC 重塑教育》讲的是 AI 如何改变“内容生产”——用 AI 生成文本、图片、视频，来辅助教学和学习。那本质上还是一个“工具论”的视角：AI 是一个更高效的内容生产工具。

而 OpenClaw 代表的是 AI 从“工具”到“助手”的跨越——它不只是帮你生成内容，更是一个能理解你、记住你、主动为你工作的独立实体。

这个差别有多大？打个比方：如果说以前的 AI 是一支非常好用的钢笔，那 OpenClaw 就是一个能替你握笔写字的秘书。钢笔再好，你还是得自己写；秘书就不一样了，你只需交代一句话，他就能替你写好、检查好、发出去。

更让我兴奋的是，我作为一个已经深度使用 vibe coding 的人，竟然还能被 OpenClaw 惊艳到。你想啊，我在日常工作中已经高度依赖 AI 了——写代码让 Claude Code 代劳，做数据分析让 AI 出脚本，连写邮件都是先让 AI 拟一稿再修改。在这个基础上，OpenClaw 居然还能再帮我省两个小时——这说明它触及了我之前那些 AI 工具碰不到的需求层面。

它是一个真正属于你自己的、能持续成长的、24 小时待命的 AI 助手。

这不是科幻电影里的桥段。在完成相应配置后，这就是现在能实现的事情。而且，它不需要你会写代码——虽然我自己会一点，但我在配置 OpenClaw 的整个过程里，几乎没有手动写过一行代码。

如果一个做了十几年教育科技产品、写过 AI 相关著作、日常已经在使用 vibe coding 的人，都觉得 OpenClaw 是一个值得专门写一本书来讲的东西——那它大概是真的不一样。

## 1.2　聊天机器人的“天花板”

在正式介绍 OpenClaw 之前，我们先来聊一个问题：你平时用的那些 AI 工具，比如 ChatGPT、Kimi、豆包、文心一言，它们到底是什么？

### 对话式 AI：很聪明，但有点“懒”

这些工具有一个共同的名字：**对话式 AI（conversational AI）**，或者更通俗地说，聊天机器人。

它们的工作模式非常简单：你问，它答；你不问，它就安静地待着。

这种模式有一个学名，叫**“请求—响应”模式（request–response）**。就像你去餐厅吃饭——你得先看菜单、点菜，服务员才会给你上菜。你不点，他绝对不会主动给你端一盘宫保鸡丁过来。

这有什么问题？

问题在于，一个真正有用的助手，不应该只是“你问我答”。你想想，如果你请了一个私人秘书，但这个秘书的工作方式是：你不说话他就坐在那里发呆，你问他一个问题他回答一个问题，说完就忘，下次你还得从头开始跟他解释你是谁、你在干什么——你会觉得这个秘书有用吗？

可这就是目前大多数 AI 聊天工具的真实状态。

让我们具体看看它们的几个“天花板”，具体如下。

**天花板一：没有记忆，每次都是初次见面。**

你今天跟 ChatGPT 聊了两个小时，讲了你的专业背景、你正在做的项目、你的研究方向。明天你再打开它，它可能记得一些（如果你用的是同一个对话窗口），但本质上，它并没有真正“理解”你是谁。你换一个对话窗口，它就完全不认识你了。

虽然现在有些 AI 工具开始支持“记忆”功能（比如 ChatGPT 的 Memory、Claude 的 Memory），但这种记忆是非常有限的——它只是从对话中提取了几条关键信息存下来。跟一个真正“认识你”的助手相比，差距还是很大的。我在第 2 章会用一个完整的案例来展示这个差距到底有多大。

**天花板二：不能干活，只能动嘴。**

你让 ChatGPT 帮你写一封邮件，它可以写——但它没法帮你发出去。你让它帮你查一下明天的天气，它可以告诉你（如果它有联网功能）——但它没法在明天下雨的时候主动提醒你带伞。你让它帮你整理一份 Excel 表格，它可以给你建议——但它没法打开你计算机上的 Excel 文件，自己动手整理。

本质上，这些 AI 只存在于一个网页窗口里。它们没有“手”，没有“脚”，没法触及你的真实世界。

**天花板三：不会主动工作，永远在等你开口。**

一个好的助手应该有一定的主动性。比如，看到你的日历上有一个即将到来的会议，主动帮你准备材料；发现你连续几天都在处理同一类问题，主动提出一个自动化方案。

但对话式 AI 不会。你不说话，它永远不会主动联系你。不是它“不想”，而是它在架构上就没有这个能力——它没有持续运行的后台进程，没有定时任务系统，没有主动触发机制。

### 一个不太恰当但很形象的比喻

如果把对话式 AI 比作一个人，那么他的画像大概如下。

智商很高（知识渊博，什么都知道一点），但没有身体（不能执行真实世界的操作），没有长期记忆（每次醒来都不记得昨天的事），而且完全没有主动性（你不叫他，他就不动）。

用互联网圈的话说，这是一个纯输出的工具，不是一个自主运转的系统。

而 OpenClaw，恰恰是为了突破这些“天花板”而设计的。

## 1.3　OpenClaw，你的“AI 分身”

现在我们可以正式聊 OpenClaw 了。

### 一句话定义

OpenClaw 是一个开源的 AI Agent（智能体）框架，它让 AI 不再只是一个聊天对象，而是一个能够自主执行任务、持续运行在你设备上（本地运行）的私人 AI 助手。

这句话里有几个关键词，我逐一解释。

**第一，开源。**

OpenClaw 的全部代码都是公开的，任何人都可以免费使用、修改、二次开发。截至本书写作时（2026 年 3 月），它在 GitHub 上已经拥有超过 25 万颗星标，是 GitHub 历史上增长最快的开源软件项目之一。它不属于任何一家公司，而是由全球开发者社区共同维护——2025 年 11 月由奥地利开发者 Peter Steinberger 创建，最初只是一个“周末项目”，2026 年 1 月底爆红，2 月移交给开源基金会运营。

这意味着什么？意味着你不用担心某天这个产品突然停止服务、涨价，或者改变策略。它是你的，你可以一直用下去。这种“不受制于人”的感觉，在你深度依赖一个工具之后，会变得格外重要——我在第 3 章会详细讲为什么。

**第二，AI Agent。**

AI Agent 这一特点是 OpenClaw 跟传统聊天机器人最本质的区别。

Agent 这个词在 AI 领域是一个非常重要的概念。简单来说，一个 AI

Agent 不仅能“想”（理解你的意图、生成回答），还能“做”（执行真实世界的操作）。它可以读取你的邮件、操作你的文件系统、调用各种 API、运行 Shell 命令——简而言之，它有“手”和“脚”。

打个比方：对话式 AI 是一个坐在窗口后面的“客服”，你跟它只能隔着玻璃说话；AI Agent 则是一个能走出柜台、帮你跑腿办事的“真人助理”。

**第三，本地运行。**

OpenClaw 运行在你自己的设备上——可以是一台 Mac Mini、一台 Windows 计算机、一台 Linux 服务器，甚至一块树莓派。你的数据不需要上传到任何第三方服务器，你的对话记录、记忆文件、技能配置，全都存储在你自己的硬盘上。

在一个数据隐私越来越被重视的时代，这一点格外重要。你跟 AI 聊的那些私密想法、学习计划、求职意向、对导师的真实评价……这些信息，你愿意让它们存在别人的服务器上吗？在 OpenClaw 上，这些数据只属于你。

**第四，框架。**

OpenClaw 本身并不是一个 AI 模型。它不像 ChatGPT 那样自己就能“思考”。OpenClaw 更像一个“操作系统”——它提供了一套完整的基础设施（消息路由、记忆管理、技能扩展、定时任务等），然后通过 API 调用外部的 AI 大模型来作为自己的“大脑”。

你可以给它接上 Claude、GPT、DeepSeek、Kimi，甚至本地部署的开源模型。换句话说，**它不绑定任何一个 AI 模型**。模型是可以随时更换的零件，OpenClaw 是让这些零件运转起来的机器。

关于这一点为什么如此重要，我会在第 3 章详细展开讨论。

## OpenClaw 的“龙虾宇宙”

由于 OpenClaw 是开源的，全球各地的公司和开发者都在基于它开发自己的版本。这形成了一个非常有趣的生态——在中国，大家管它叫“龙虾宇宙”（因为 OpenClaw 的吉祥物是一只红色的小龙虾）。

表 1-1 可帮你快速了解截至本书写作（2026 年 3 月）时主要的 OpenClaw 生态产品。注意，开源生态变化很快，这些产品的名称、功能和运营状态可

能会有调整，建议以各产品官网的最新信息为准。

表 1–1　OpenClaw 主要生态产品一览

| 产品名称 | 开发方 | 核心特点 | 适合人群 |
| --- | --- | --- | --- |
| OpenClaw（本体） | 开源社区 / 基金会 | 功能最全，自主可控，需自行部署；全部代码开源，社区活跃 | 有一定技术能力的用户；本书主要读者 |
| KimiClaw | 月之暗面（Moonshot AI） | 云托管版，无须自行部署；与 Kimi 模型深度整合；中文体验较好 | 希望快速上手的中国用户；不想折腾部署的新手 |
| MaxClaw | MiniMax | 成本较低，一键部署；M2.5 模型成本优势明显 | 预算敏感的用户；追求性价比的学生 |
| 其他社区版本 | 各社区 / 厂商 | 包括中文汉化版、轻量化 Rust 版（ZeroClaw）等多个分支 | 有特定需求的用户 |

你可能会问：这本书讲解的是哪个版本？答案是：以 OpenClaw 本体为主，同时兼顾 KimiClaw 和 MaxClaw。原因很简单：学会了 OpenClaw 本体，其他衍生版本你都能触类旁通。而 KimiClaw 和 MaxClaw 对中国用户来说更容易上手，所以也会专门介绍。这就像学开车——学会了手动挡，自动挡自然就会了。

## 1.4　OpenClaw 与传统 AI 聊天工具的区别

为了帮助你更清楚地理解 OpenClaw 和传统 AI 聊天工具的差异，我整理了两者的对比情况，如表 1–2 所示。

表 1–2　OpenClaw 与传统 AI 聊天工具对比

| 对比维度 | 传统 AI 聊天工具（如 ChatGPT、Kimi） | OpenClaw |
| --- | --- | --- |
| 交互模式 | 请求—响应模式：你问它答，你不问它不动 | 自主循环模式：可主动执行任务、定时提醒、在后台工作 |
| 记忆能力 | 对话记忆有限，换窗口就忘 | 分层记忆系统：短期日志 + 长期记忆 + 用户画像，越用越懂你 |

续表

| 对比维度 | 传统 AI 聊天工具（如 ChatGPT、Kimi） | OpenClaw |
| --- | --- | --- |
| 执行能力 | 受限于平台沙箱，无法操作用户本地系统 | 在相应配置完成后，可发邮件、管理日程、读写文件、运行命令 |
| 运行位置 | 在云端服务器上，数据由平台控制 | 在你自己的设备上，数据完全自主可控 |
| 模型绑定 | 绑定特定模型（如 ChatGPT 只能用 Open AI 的模型） | 不绑定模型，可接入 Claude、GPT、DeepSeek、Kimi 等 |
| 扩展能力 | 功能由平台决定，用户无法自定义 | 通过 Skill 系统自由扩展，社区已有大量技能 |
| 沟通渠道 | 只能在特定 App 或网页中使用 | 通过 iMessage、飞书、钉钉、Discord 等多平台交互 |
| 持续性 | 关闭浏览器就断了 | 7×24 小时持续运行，像一个永不下班的员工 |

用一句话总结这个表格的核心信息：**传统 AI 聊天工具是一个“顾问”——你找它咨询，它给你建议；OpenClaw 是一个“员工”——它不仅给你建议，还能帮你把事情做好**。

## 1.5 OpenClaw 的核心架构

要真正理解 OpenClaw，你需要了解它的核心配置文件。在 OpenClaw 的用户圈子里，它们被称为“定海神针”。现在不需要你完全弄懂每一个文件的技术细节（那是中篇第 5 章的内容），但你需要先有一个整体的认知。

### SOUL.md：AI 的“灵魂”

SOUL.md 定义了你的 AI 助手是一个怎样的“人”：它的说话风格是什么样的，是正式严谨，还是轻松幽默？它的核心工作原则是什么？遇到不确定的事情它应该怎么处理？

比如，我在自己的 SOUL.md 里写了如下几条规则。

（1）说话直接，不需要客套。

（2）遇到不确定的信息，先查证再回复。

（3）回复尽量简洁，不要长篇大论。

（4）允许有自己的观点和偏好，不需要假装中立。

这些规则让我的 AI 助手形成了一种独特的“性格”——它跟别人的 OpenClaw 是不一样的。就像两个人用同样的食材做菜，做出来的味道完全不同一样。而且这种“性格”是你主动设计的——你希望 AI 怎么跟你交流，就写进 SOUL.md 里。这对于传统聊天工具来说几乎不可能做到。

### USER.md：关于你的一切

USER.md 是一份“用户画像”。在这个文件里，你告诉 AI 关于你自己的基本信息：你叫什么名字、你做什么工作、你有哪些偏好和习惯、你目前关注什么项目。

有了这个文件，AI 每次“醒来”的时候都会先读一遍，立刻知道它在为谁工作。这就好比你入职一家新公司，HR 先给你一份老板的个人简介——你至少知道自己在为谁服务。没有 USER.md 的 AI 助手就像一个每天都是第一天上班的员工——它永远不记得你昨天跟它说了什么。

### MEMORY.md + memory/：记忆系统

OpenClaw 的记忆系统是分层的。最底层是每日**对话日志**（存储在 memory/ 文件夹下，按日期命名，比如 memory/2026-03-11.md）。每天结束的时候，AI 会自动把当天发生的重要事情记录下来。

上面一层是**长期记忆**（MEMORY.md）。随着时间推移，AI 会把日志中反复出现的模式、重要的决策、关键的偏好提炼出来，存入这个文件。这是真正的“长期记忆”——它可能记录着“用户喜欢在周五下午做本周复盘”“跟广州中心的沟通要注意语气”这样的细节。

这套记忆系统的精妙之处在于：所有记忆都以纯文本的形式存储在你的本地硬盘上。你随时可以打开文件看它记了什么，觉得不对的可以直接修改或删除。你对它的记忆拥有完全的控制权。这种透明度在 AI 产品中是非常稀缺的——传统 AI 聊天工具的记忆对你来说是一个“黑箱”，你根本不知道它记住了什么、遗漏了什么。

## Skill：技能系统

如果说 SOUL.md 定义了 AI“是什么样的人”，Skill（技能）系统则定义了 AI“能做什么事”。

每一个 Skill 就是一个功能模块。比如有一个 Skill 专门用来查天气，有一个 Skill 专门用来管理日程，有一个 Skill 专门用来搜索学术论文。你可以通过社区“技能商店”（ClawHub）一键安装别人写好的 Skill，也可以自己编写。截至本书写作时，OpenClaw 的 Skill 生态已经拥有的社区贡献的技能涵盖生产力工具、开发运维、知识管理、智能家居等方方面面。

值得一提的是，Skill 的安装和使用不需要写代码——它本质上就是一个 Markdown 文件，里面用自然语言描述了这个技能是什么、能做什么。这也是 OpenClaw 设计中最“平民化”的一点：你不必是程序员，就能给你的 AI 添加新能力。

## Cron：定时任务

Cron 是一个定时任务系统，它让你的 AI 具备了“时间感”。

你可以设置各种定时规则。比如：每天早上 7 点给我发今日天气和日程概要；每周五下午 5 点生成本周工作总结；每隔 30 分钟检查一次邮箱是否有紧急邮件。

有了 Cron，你的 AI 就不再是一个“你问它答”的被动工具，而是一个可以主动工作的助手。它有了时间观念，知道什么时候该做什么事。这一点对于传统 AI 聊天工具来说是完全不可能实现，因为你关掉浏览器，它就“消失”了。

OpenClaw 核心架构示意图如图 1-1 所示。

这个架构的精妙之处在于：每一层都是可替换、可定制的。你可以换不同的 AI 模型当“大脑”，可以安装不同的 Skill 扩展能力，可以通过编辑文本文件来调整它的“性格”和“记忆”。这不是一个封闭的产品，而是一个开放的框架。你在上面搭建的东西，完全属于你自己。


图 1-1　OpenClaw 核心架构示意图 ①

## 1.6　为什么是你？为什么是现在？

### 第一层：年轻人是最需要 AI 助手的人群之一

别误会，我不是说年轻人比其他人群更忙——虽然很多时候确实如此。我的意思是：年轻人面对的事务种类特别多、特别杂，而且多数人缺乏系统性的管理工具。

例如，一个典型的大学生每天可能要面对如下事项。

（1）6 ～ 8 门课的课程安排、作业、考试。

（2）社团活动、学生组织的各种会议和任务。

（3）实习投递、简历修改、面试准备。

（4）论文阅读、文献管理、读书笔记。

（5）生活琐事：选课、缴费、拿快递、去食堂。

（6）还有一个不太好意思说但很重要的事——社交媒体的信息洪流。

① 本书图片均由 Opus 4.6 生成。

这些事情，没有一件是特别难的。但它们加在一起，就会挤占大量的时间和精力，使你没有余力去做真正重要的深度思考和学习。

一个配置得当的 OpenClaw 可以帮你把这些事情管理起来。让 AI 去处理那些重复、机械、消耗注意力但不需要太多创造力的工作，把你的精力释放出来，用在真正需要你动脑子的地方。

### 第二层：现在是最好的时机

2026 年年初，OpenClaw 在中国的热度已经到了一个引爆点。近期，“养龙虾”和“一人公司”成为社会热议的话题。部分地方政府开始关注 AI Agent 和一人公司的发展，推出了相关的政策探索与支持举措。

与此同时，AI 模型的能力在过去一年里取得了巨大飞跃。以前运行一个 AI Agent 需要较好的模型才能获得勉强可用的效果，而现在，即便是中等性能的模型（比如 Kimi 的最新版本、DeepSeek 等），也已经足够驱动 OpenClaw 完成绝大多数日常任务——而且成本非常低。

技术就绪了，生态就绪了。如果你要学习 AI Agent，现在就是最好的时机。

### 第三层：这不只是一个工具，而是一种能力

其实这才是我最想说的。

学习使用 OpenClaw，本质上学的不是“一个软件怎么操作”。你学到的是一套与 AI 协作的方法论，具体如下。

（1）如何定义一个 AI 助手的“人格”和工作规范。

（2）如何构建可持续积累的个人知识体系。

（3）如何设计自动化工作流以提升效率。

（4）如何将复杂任务拆解并委托给 AI 执行。

这些能力是可迁移的。即便将来 OpenClaw 被另一个更好的工具取代（在技术领域，这几乎是必然的），你通过学习 OpenClaw 培养的这些思维方式和工作方法依然有效。

这也是我在第 3 章要详细讨论的“不绑定模型”理念的延伸——我们不仅不绑定某一个 AI 模型，我们甚至不绑定某一个工具。我们学的是能力，不

是操作。

### 我的一天，有 OpenClaw 和 没有 OpenClaw

为了让你更直观地感受 OpenClaw 的价值，我把自己有 OpenClaw 和没有 OpenClaw 的一天做个对比，如表 1-3 所示。

表 1-3　有 OpenClaw 和没有 OpenClaw 的一天

| 时间 | 没有 OpenClaw（2024 年） | 有 OpenClaw（2026 年） |
|---|---|---|
| 7:00 | 打开手机看天气 App、日历 App、邮箱 App，大概花 15 分钟浏览当天的安排 | 看 iMessage 上的一条消息——晨间简报（天气 + 日程 + 重要邮件摘要），花 1 分钟 |
| 9:00 | 到办公室，花 30 分钟处理邮件，从十几封邮件里筛选重要、需要回复的 | Ops Agent 已在 8:30 自动生成区域数据周报，我花 15 分钟审阅 |
| 10:00 | 打开浏览器，逐一检查区域数据后台，把数据复制到 Excel 里做对比，用时 1 小时 | 口述 2 分钟，交代会议重点，AI 自动准备会议材料 |
| 11:00 | 准备下午的会议材料，翻之前的会议纪要（在微信聊天记录里找了很久），整理最新数据，花了 1.5 小时 | 开始写书稿，Writer Agent 已根据大纲和昨天的进度，准备好了今天的素材和参考资料，直接开始写 |
| 14:00 | 开会 | 会议前，AI 已把材料整理好，我花 5 分钟快速过一遍，14:00 开会 |
| 15:30 | 会后写会议纪要，花了 30 分钟 | 会后口述 3 分钟会议要点，纪要自动生成，待办自动进入追踪系统 |
| 18:00 | 下班，觉得“做了很多事”但“产出不多” | 下班。这一天写了 5000 字初稿，审阅了数据周报，开了一个准备充分的会议 |

差异在哪里？不是我变勤快了——是大量的“信息搬运”“数据整理”“格式调整”工作被 AI 接管了。我的时间从“处理琐事”转移到了“深度产出”上。

## 1.7　OpenClaw 的“另一面”：风险与边界

讲了这么多优点，我觉得有必要泼一盆冷水。

因为 OpenClaw 不是万能的，而且它确实有一些需要我们认真对待的风险。作为一个负责任的作者，我不能只讲好的，不讲不好的。

## 安全风险不容忽视

OpenClaw 运行时需要访问你的邮箱、日历、文件系统，甚至可能需要执行命令行操作。这意味着，如果配置不当，它就像一把双刃剑——既能帮你干活，也可能误操作或泄露你的数据。

在 OpenClaw 走红之初，安全研究人员就发现了大量安全隐患。据报道，早期安全审计发现了多个安全漏洞，其中部分被列为“严重级别”。全球安全公司 Cisco 的研究团队发现，一些第三方 Skill 存在数据窃取和恶意注入的风险——用户可能在不知情的情况下安装了一个看似无害但实际上在偷偷传输数据的 Skill。2026 年年初还爆出了“ClawHavoc”供应链攻击事件，数百个恶意技能被上传到 ClawHub 技能商店。

这些问题听起来很吓人，但也不必过度恐慌。关键在于养成正确的配置和使用习惯。就像你不会因为刀能伤人就不用菜刀一样，OpenClaw 的安全风险是可以通过合理的配置进行管控的。

我在这本书中会用整整一节（参见 4.5 节）来教你如何安全地使用 OpenClaw。请务必认真对待。

## 它不是“开箱即用”的消费品

跟你打开手机就能用的 App 不同，OpenClaw 目前仍然需要一定的配置和调教才能够使用。虽然 KimiClaw 和 MaxClaw 这样的云托管版本大大降低了门槛，但要想让它发挥最大价值，你仍然需要投入时间去理解它的工作原理、调整它的配置、训练它适应你的工作习惯。

OpenClaw 的一位核心维护者 shadow 甚至说过：“如果你连命令行都搞不明白，那么这个项目对你来说可能太危险了。”

这话听起来有点吓人，但也正是我写这本书的原因——我要帮你把这个门槛降到最低，让你即使不熟悉命令行，也能安全、有效地使用 OpenClaw。这本书就是你的“新手保护罩”。

## AI 不是万能的

最后要强调的一点是：AI 助手再强大，也不能替代你自己的判断。

它可以帮你整理信息，但重要的决策需要你自己做。它可以帮你起草文章，但你需要检查它写的内容是否准确。它可以帮你安排日程，但真正重要的事情的优先级需要你自己定。

把 AI 当成一个能干的助手，而不是一个无所不能的神——这是正确使用 AI 的基本心态。在第 13 章，我会更深入地讲解如何跟 AI 建立一段健康的、你掌握主导权的长期关系。

## 1.8　本书能让你学到什么？

最后，我想用一张“本书学习路线图”（见图 1-2）来告诉你：读完这本书，你将学到什么。

### 一个承诺

这本书不会让你从头到尾啃完才开始动手。从第 4 章开始，每一章都有“跟着做”的实操环节。你完全可以一边看书一边配置你的 OpenClaw，学到哪里都可以即刻使用。

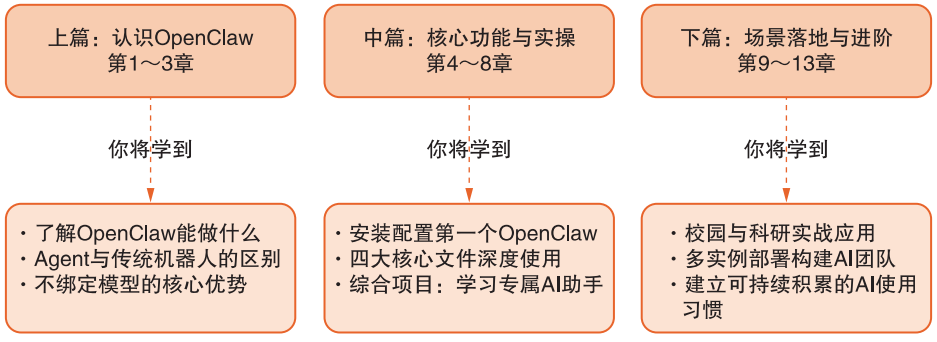


图 1-2　本书学习路线图

好了，铺垫够了。下一章，我们来深入聊聊 OpenClaw 和传统大模型的“本质区别”——这会帮你从底层理解 AI Agent 为什么是 AI 发展的下一个重要方向。

## 本章思考题

- 基础题

1. 请用你自己的话解释：什么是 AI Agent？它和传统的 AI 聊天机器人有哪些核心区别？

2. OpenClaw 的四大核心配置文件分别是什么？它们各自负责什么功能？请尝试用一个生活中的比喻来描述它们的关系。

3. 为什么说 OpenClaw 不绑定模型？这对使用者来说有什么好处？

- 进阶题

1. 假设你是一名大二的市场营销专业学生，同时担任学生会宣传部部长。请列出至少 5 个你认为 OpenClaw 可以帮你完成的具体任务，并简要说明它应该通过什么方式（定时任务？技能扩展？记忆积累？）来完成。

2. 本章提到了 OpenClaw 的安全风险。请结合你自己的理解思考一下：如果你要向一个完全不懂技术的朋友推荐 OpenClaw，你会怎样向他解释使用时需要注意的安全问题？

- 讨论题

“AI 不是万能的”——你同意这个观点吗？你认为 AI 助手的边界在哪里？有哪些事情是 AI 绝对不应该替你做的？尝试列出你自己的 AI 使用边界清单。

## 本章小结

本章作者从自己“养龙虾”的亲身经历出发，介绍了 OpenClaw 的基本概念、核心架构和它与传统 AI 聊天工具的本质区别。OpenClaw 是一个开源的 AI Agent 框架，具备自主执行任务、持续运行、分层记忆、技能扩展和定时任务等能力，其核心架构由用户交互层、网关层、核心文件层、AI 大模型层和执行层协同构成。同时，作者也坦诚地讨论了 OpenClaw 的安全风险和使用门槛。下一章将深入探讨 AI Agent 与传统大模型的本质区别，帮你从底层理解这一技术变革的方向。