再一次谈自定义 Agent 计算机行业研究

2026 年 03 月 28 日

买入（维持评级）

行业点评

证券研究报告

计算机组
分析师：刘高畅（执业 S1130525120005）
liugaochang@gjzq.com.cn

再一次谈自定义 Agent

行业观点：

Skills：Agent 可配置性的一大突破。2025 年底 Anthropic 推出的 Agent Skills，通过以结构化文件夹为载体，将任务指令、代码能力与资源模块化封装，构建了一套标准化的“AI 工作手册（SOP）”，显著提升了 Agent 的可配置性与可复用性。其核心创新在于“按需加载”的渐进式披露机制，使模型在运行过程中动态调用所需能力，从而优化上下文使用效率并提升执行稳定性。Skills 的推出让 Agent 向“能力可配置、可沉淀、可共享”的范式跃迁，成为推动 Agent 生态规模化发展的关键基础设施。

OpenClaw：开源自定义 Agent 框架机制解析。OpenClaw 作为新一代开源 Agent 框架，构建了一套完整的 Agent 运行体系，不同于传统仅具备对话或工具调用能力的系统，OpenClaw 通过引入完整的运行链路（包括上下文组装、技能注入、工具调度、多 Agent 协作等），使 Agent 具备持续执行复杂任务的能力。同时，其创新性的分层记忆系统（长期记忆与每日记忆）以及动态上下文管理机制，使模型从进化为具备持续认知与演化能力的系统。此外，通过预设身份、规则、工具与用户偏好等多维信息，OpenClaw 显著提升了任务一致性与执行效率。整体而言 OpenClaw 定义了一套可复制的 Agent 工程化范式，为自定义 Agent 的落地提供了标准路径。

决定自定义 Agent 能力的三大要素。随着 Skills 标准化能力与 OpenClaw 等开源框架的成熟，自定义 Agent 的开发门槛显著下降，行业正从“技术驱动”迈向“应用驱动”。在这一阶段，决定 Agent 实际能力上限与商业价值的关键因素，已从底层模型开发能力，转向更高层的系统性要素。我们认为，未来自定义 Agent 的核心竞争力聚焦三大维度：一是基础大模型的原生能力，决定智能上限；二是高质量、专属化的数据资源，决定专业深度与差异化水平；三是开发者对需求与场景的理解与拆解能力，决定 Agent 是否真正契合业务、实现有效落地。这一趋势与姚顺雨在《The Second Half》中提出的“AI 进入下半场”的判断相呼应，未来谁能更好定义问题才能更好构建有效解决方案。

投资建议：

相关标的：

海外算力/存储：中际旭创、东山精密、胜宏科技、欧科亿、天孚通信、新易盛、工业富联、兆易创新、大普微、源杰科技、景旺电子、英维克等；Lumentum、闪迪、铠侠、美光、SK 海力士、中微公司、北方华创、拓荆科技、长川科技。

国内算力：寒武纪、东阳光、海光信息、协创数据、豫能控股、华丰科技、亿田智能、星环科技、网宿科技、首都在线、神州数码、百度集团、大位科技、润建股份、中芯国际、华虹半导体、中科曙光、润泽科技、浪潮信息、东山精密、奥飞数据、云赛智联、瑞晟智能、科华数据、潍柴重机、金山云、欧陆通、杰创智能。

CPU：海光信息、中科曙光、澜起科技、禾盛新材、中国长城、龙芯中科、兴森科技、深南电路、宏和科技、广合科技。

AI 应用：1）超级入口：腾讯控股、Minimax、智谱、阿里巴巴、科大讯飞。2）星环科技、德才股份、美年健康、中控技术、卓易信息、昆仑万维等 AI INFRA&高增长&高壁垒。其他：空天时代、具身智能等

风险提示

行业竞争加剧的风险；技术迭代不及预期的风险；特定行业下游资本开支周期性波动的风险

内容目录

图表目录

一、Skills：Agent 可配置性的一大突破

2025 年 10 月 16 日，Anthropic 正式推出 Agent Skills，作为一种将 Claude 从通用对话助手转变为专业化工作流执行者的机制。两个月后的 12 月 18 日，Anthropic 进一步将 Agent Skills 规范开放为开放标准。

Skill 的本质是一个结构化的文件夹，相当于给 AI 的“工作手册”或“SOP(标准作业程序)”，包含完成特定任务所需的所有信息，其中每个 Skill 必须包含核心文件 SKILL.md，作为其核心指令和元数据的载体；其组成结构主要包括三类内容，分别是告诉 AI 如何执行任务的步骤和逻辑的指令（Instructions）、可选的用于执行确定性、重复性操作的代码（Code），以及包含模板、参考文档等辅助材料的资源（Resources）。

图表1：Skill 文件夹的结构

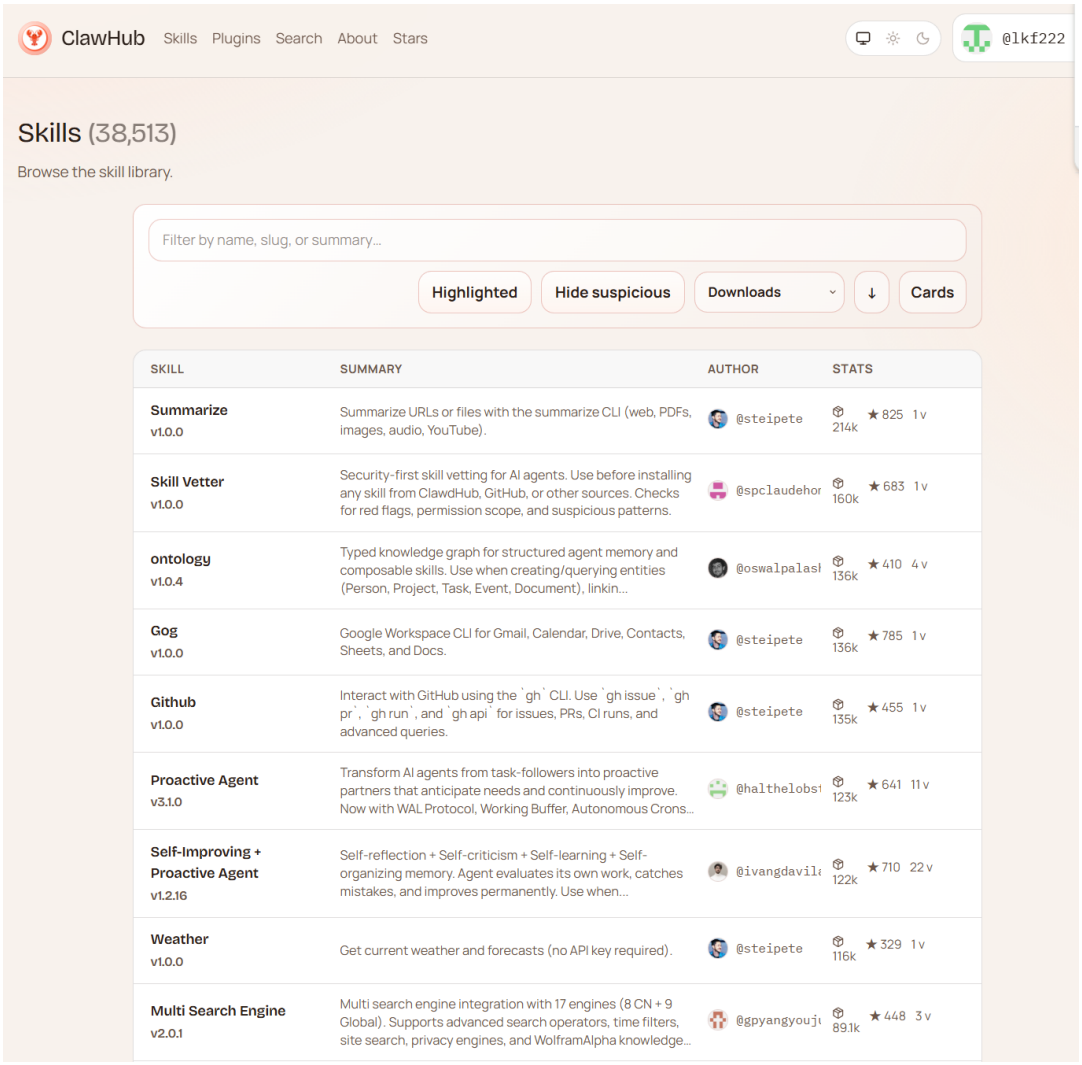
```
your-skill-name/
├── SKILL.md          # 必需
├── scripts/          # 可选：代码脚本
├── references/       # 可选：文档
└── assets/           # 可选：模板/图标
```

来源：OpenAI，国金证券研究所

Skill 的按需加载（渐进式披露）是其最核心的设计哲学，AI 启动时仅加载元数据，需执行对应任务时才动态加载详细指南和资源，能有效节省上下文消耗、提升效率与稳定性；同时它具备可复用与可组合性，可在不同场景反复调用，还能组合构建复杂工作流；此外，它遵循 Anthropic 定义的跨平台开放标准，可跨系统移植共享，且实现了智能与专业的解耦，业务规则更新时仅需修改 Skill 文件，无需重训模型，降低维护成本。

Skills 的推出让 Agent 向“能力可配置、可沉淀、可共享”的范式跃迁，成为推动 Agent 生态规模化发展的关键基础设施。Agent 作为能规划、决策的“大脑”，Skill 则是这个大脑所掌握的“技能”和“经验”。许多开发者将他们的经验打包成 Skill 分享到社区，促进了 Agent 生态的繁荣。

图表2：Clawhub 社区的数万 Skill



来源：Clawhub，国金证券研究所

二、OpenClaw：开源自定义 Agent 框架机制解析

由独立开发者 Peter Steinberger 在 2025 年 11 月推出的 OpenClaw，定位为完全开源且本地运行的 AI Agent 框架。它具备真正的行动力，电脑在它眼中变作了可以肆意发挥的沙盒，执行终端命令、读写文件、收发邮件乃至代替主人管理日程，一切均在自然的对话间完成。

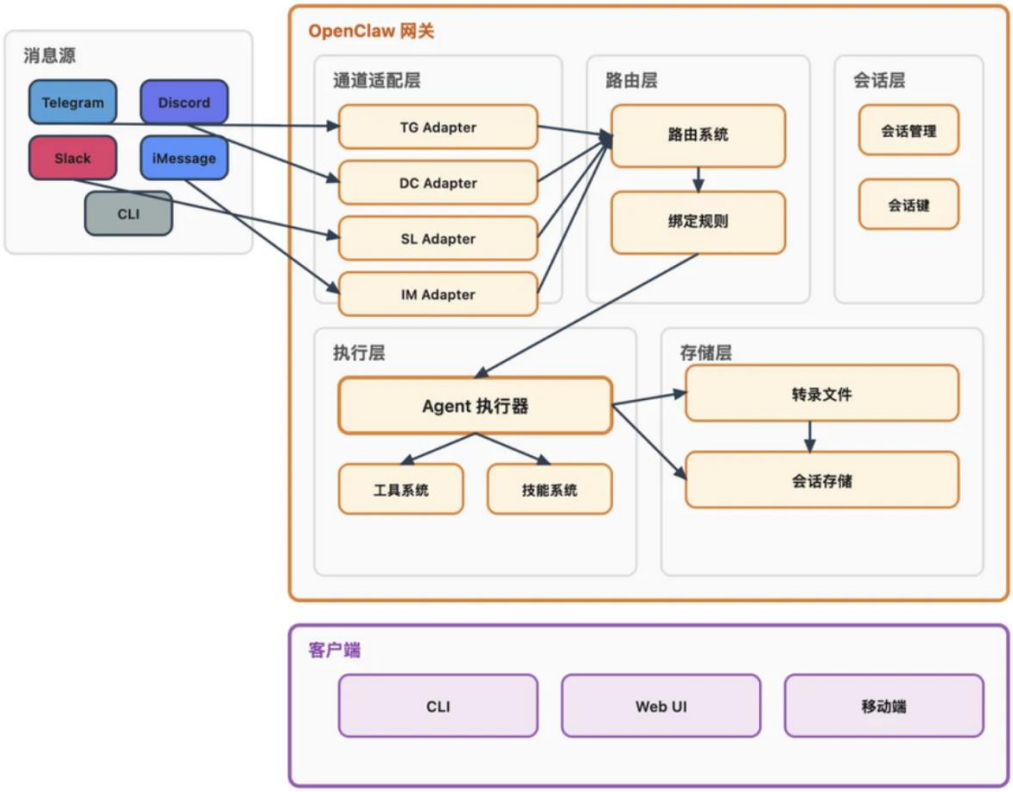
据新浪财经报道， OpenClaw 就仅用两月击败 Linux，登顶 GitHub 星标榜，正式加冕史上最受欢迎开源项目。

图表3：OpenClaw 的 GitHub 星标增长速度

来源：X，国金证券研究所

OpenClaw 跟普通聊天机器人、传统工作流系统、以及很多只会调工具的 Agent 框架，差别并不在于它会不会聊天，而在于它背后有一整套完整的运行链路：消息接收、协议适配、路由分发、会话隔离、上下文组装、技能注入、流式执行、工具调用、持久化存储，以及在复杂任务下的多 Agent 协作。

图表4：OpenClaw 的整体架构



来源：虎嗅，国金证券研究所

记忆系统:除了会话历史，OpenClaw 还单独维护两类记忆：

1)长期记忆

文件名通常是：MEMORY.md/memory.md

用于存常青知识，例如：项目规则/API 文档/设计决策/长期偏好,这类记忆在 Agent 启动时直接注入系统提示词.

2)每日记忆

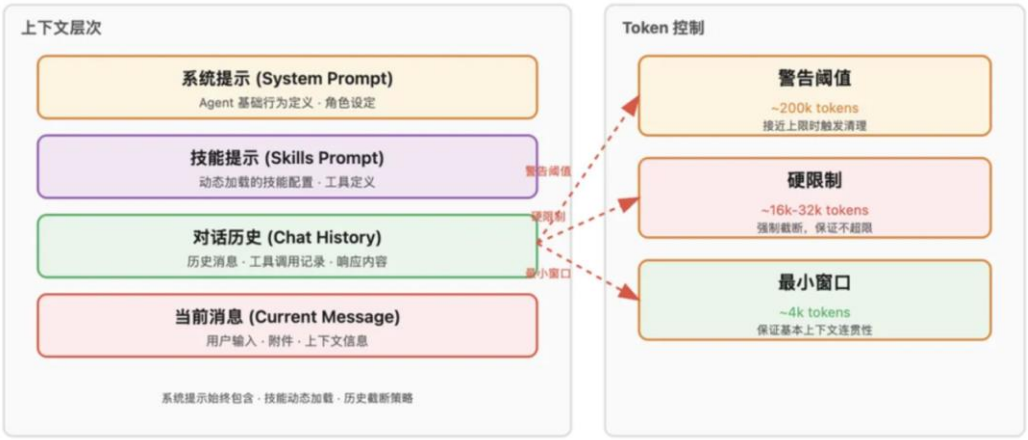
存放在：memory/YYYY-MM-DD.md.用于记录时效性内容，例如：

每日纪要/当天待办/临时决策/会议记录,这类记忆不直接注入提示词,而是通过记忆搜索工具按需检索，并且会带时间衰减权重，越新的内容权重越高。

长期记忆通常由用户或 Agent 通过编辑工具手动维护。而每日记忆则会通过 Memory Flush 机制自动触发。触发条件包括：会话 token 数接近上下文窗口上限（默认软阈值 4000 tokens）和会话转录文件大小超过阈值。

组装完整上下文：在 OpenClaw 里，模型看到的不是单独一句用户输入，而是一整套被拼装好的上下文环境。组装顺序大致是：系统提示词→技能提示→对话历史→当前消息。

图表5：OpenClaw 的上下文窗口策略



来源：虎嗅，国金证券研究所

OpenClaw 会把这些文件装进上下文：

AGENTS.md：定义 Agent 行为规则和工具使用指南

SOUL.md：定义个性和人格

TOOLS.md：工具使用说明

IDENTITY.md：身份标识信息

USER.md：用户偏好

HEARTBEAT.md：心跳检测提示

BOOTSTRAP.md：初始化引导

MEMORY.md/memory.md：长期记忆

这些文件位于工作区目录，默认是~/.openclaw/workspace。

也就是说，在真正回答你“整理邮件”之前，模型先会被告知：我是谁/我该遵守什么规则/我能用哪些工具/这个用户有什么偏好/这个系统有哪些长期记忆/这和普通聊天机器人有个本质区别：它不是每次都从零开始聊，而是从一个被预先塑形过的 Agent 身份出发。

整体而言，OpenClaw 的意义不仅在于开源，更在于其定义了一套可复制的 Agent 工程化范式，为自定义 Agent 的落地提供了标准路径。

三、决定自定义 Agent 能力的三大要素

随着 Skill 能力体系与 OpenClaw 开源框架的持续迭代与全面开源落地，普通开发者乃至行业用户搭建、调校个性化智能 Agent 的技术门槛被大幅拉低，从零开发专属自定义 Agent 的实操难度显著下降，无需深耕底层算法研发，就能快速实现 Agent 的功能定制与场景落地。

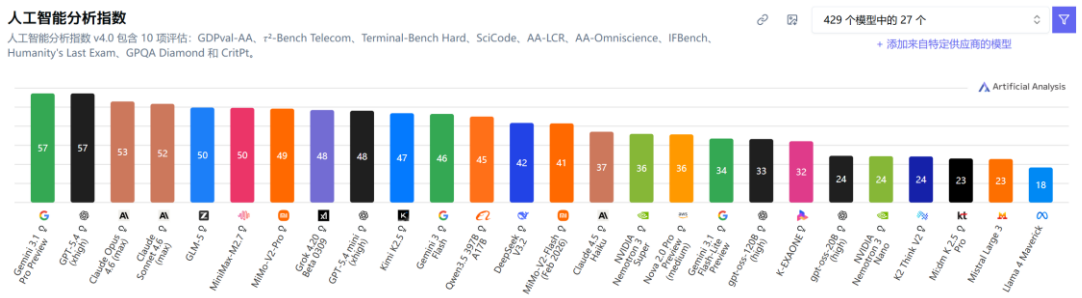
依托 Clawhub 平台日益繁荣完善的 Skill 开源生态，海量标准化技能插件、行业专属能力模块、场景化工具组件持续沉淀共享，大量用户基于现有技能组合、二次改造创新，快速搭建适配自身需求的自定义 Agent，也进一步印证了行业开发门槛下放、全民共创 Agent 生态的发展趋势。

而随着技术框架愈发成熟、应用落地门槛持续降低，未来拉开不同自定义 Agent 核心能力差距、决定其实际落地价值与场景适配上限的关键要素，将不再局限于底层开发技术，我们认为核心主要聚焦三大维度：

1）基础大模型原生能力：

作为 Agent 的核心大脑，基座模型的逻辑推理、长文本理解、工具调用联动、多轮对话记忆、复杂任务拆解与泛化能力，直接决定 Agent 的智能基础上限。

图表6：Artificialanalysis 大模型能力综合测评榜单



来源：artificialanalysis，国金证券研究所

2）高质量、高专属度数据源：

精准合规的行业私有数据、实时动态资讯、垂直领域知识库、脱敏业务数据，是支撑 Agent 实现专业应答、精准决策、落地专属场景的核心底气，数据的新鲜度、精准度、专属度直接拉开差异化优势。

3）开发者的需求定义与场景拆解能力：

前 OpenAI 研究员姚顺雨发表的文章《The Second Half》，提出 AI 进入了下半场，下半场的是新规则：评估比训练更重要。不再仅仅问"能否训练出解决 X 的模型"，而是问"我们应该训练 AI 去做什么，以及如何衡量真正的进展"。下半场要像产品经理一样思考，AI 该为谁解决什么问题，又如何衡量解决得好不好。

我们认为自定义 Agent 能否创造价值，开发者能否根据自己对行业需求的 Know-how，精准梳理业务流程、明确核心使用场景、拆分任务逻辑，决定了 Agent 能否贴合实际需求、规避功能冗余，真正实现高效落地、贴合业务价值

风险提示

行业竞争加剧的风险： 在信创等政策持续加码支持计算机行业发展的背景下，众多新兴玩家参与到市场竞争之中， 若市场竞争进一步加剧，竞争优势偏弱的企业或面临出清，某些中低端品类的毛利率或受 到一定程度影响。
技术研发进度不及预期的风险： 计算机行业技术开发需投入大量资源，如果相关厂商新品研发进程不及预期，表观层面将 呈现出投入产出在较长时期的滞后特征。
特定行业下游资本开支周期性波动的风险： 部分计算机公司系顺周期行业，下游资本开支波动与行业周期性相关性较强，或在个别年 份对于上游软件厂商的营收表现产生扰动。

行业投资评级的说明：

买入：预期未来 3—6 个月内该行业上涨幅度超过大盘在 15%以上；

增持：预期未来 3—6 个月内该行业上涨幅度超过大盘在 5%—15%；

中性：预期未来 3—6 个月内该行业变动幅度相对大盘在 -5%—5%；

减持：预期未来 3—6 个月内该行业下跌幅度超过大盘在 5%以上。

特别声明：

国金证券股份有限公司经中国证券监督管理委员会批准，已具备证券投资咨询业务资格。

本报告的产生基于国金证券及其研究人员认为可信的公开资料或实地调研资料，但国金证券及其研究人员对这些信息的准确性和完整性不作任何保证。本报告反映撰写研究人员的不同设想、见解及分析方法，故本报告所载观点可能与其他类似研究报告的观点及市场实际情况不一致，国金证券不对使用本报告所包含的材料产生的任何直接或间接损失或与此有关的其他任何损失承担任何责任。且本报告中的资料、意见、预测均反映报告初次公开发布时的判断，在不作事先通知的情况下，可能会随时调整，亦可因使用不同假设和标准、采用不同观点和分析方法而与国金证券其它业务部门、单位或附属机构在制作类似的其他材料时所给出的意见不同或者相反。

本报告仅为参考之用，在任何地区均不应被视为买卖任何证券、金融工具的要约或要约邀请。本报告提及的任何证券或金融工具均可能含有重大的风险，可能不易变卖以及不适合所有投资者。本报告所提及的证券或金融工具的价格、价值及收益可能会受汇率影响而波动。过往的业绩并不能代表未来的表现。

客户应当考虑到国金证券存在可能影响本报告客观性的利益冲突，而不应视本报告为作出投资决策的唯一因素。证券研究报告是用于服务具备专业知识的投资者和投资顾问的专业产品，使用时必须经专业人士进行解读。国金证券建议获取报告人员应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。报告本身、报告中的信息或所表达意见也不构成投资、法律、会计或税务的最终操作建议，国金证券不就报告中的内容对最终操作建议做出任何担保，在任何时候均不构成对任何人的个人推荐。

在法律允许的情况下，国金证券的关联机构可能会持有报告中涉及的公司所发行的证券并进行交易，并可能为这些公司正在提供或争取提供多种金融服务。

本报告并非意图发送、发布给在当地法律或监管规则下不允许向其发送、发布该研究报告的人员。国金证券并不因收件人收到本报告而视其为国金证券的客户。本报告对于收件人而言属高度机密，只有符合条件的收件人才能使用。根据《证券期货投资者适当性管理办法》，本报告仅供国金证券股份有限公司客户中风险评级高于 C3 级（含 C3 级）的投资者使用；本报告所包含的观点及建议并未考虑个别客户的特殊状况、目标或需要，不应被视为对特定客户关于特定证券或金融工具的建议或策略。对于本报告中提及的任何证券或金融工具，本报告的收件人须保持自身的独立判断。使用国金证券研究报告进行投资，遭受任何损失，国金证券不承担相关法律责任。

若国金证券以外的任何机构或个人发送本报告，则由该机构或个人为此发送行为承担全部责任。本报告不构成国金证券向发送本报告机构或个人的收件人提供投资建议，国金证券不为此承担任何责任。

上海
电话：021-80234211
邮箱：researchsh@gjzq.com.cn
邮编：201204
地址：上海浦东新区芳甸路 1088 号紫竹国际大厦 5 楼

北京
电话：010-85950438
邮箱：researchbj@gjzq.com.cn
邮编：100005
地址：北京市东城区建内大街 26 号新闻大厦 8 层南侧

深圳
电话：0755-86695353
邮箱：researchsz@gjzq.com.cn
邮编：518000
地址：深圳市福田区金田路 2028 号皇岗商务中心 18 楼 1806

【小程序】
国金证券研究服务

【公众号】
国金证券研究