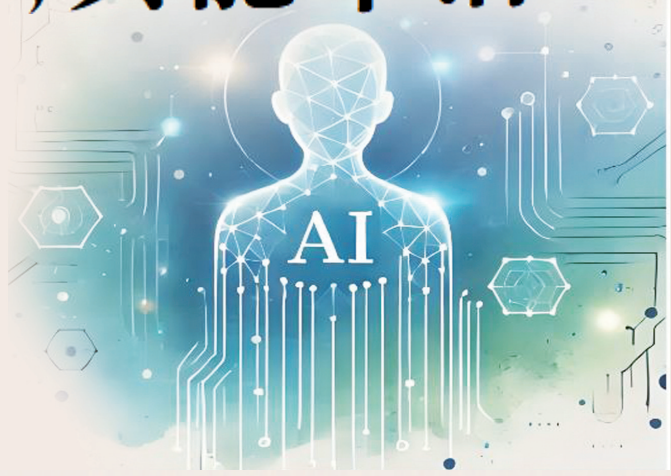
AI智能体：不止聊天，真能干活



2026年，一场从“对话AI”到“行动AI”的变革正在发生。这场变革的引爆点，源于一款名为OpenClaw（龙虾）的开源AI代理框架。OpenClaw的能力突破迅速引发产业界竞逐，一时间，百度、阿里巴巴、腾讯、字节、智谱、月之暗面等科技巨头密集入局。

5月份，国家网信办、国家发展改革委、工业和信息化部联合印发了《智能体规范应用与创新发展实施意见》（以下简称《实施意见》）。自此，“智能体”发展实现了有规可依。

什么是智能体？为何曾经的大模型，只会聊天、回答问题，如今智能体却能看屏幕、点鼠标、自动干活？智能体如何从实验室走入工作与生活，成为赋能科研、电商、金融等千行百业的真实生产力？

什么是智能体？智能体因何会“自己干活”？

《实施意见》提出，“智能体是具备自主感知、记忆、决策、交互与执行能力的智能系统，是人工智能产品及服务的重要形态，随着大模型等新一代人工智能技术迅猛发展，智能体正加速与网络空间、物理世界深度融合，深刻改变人类生产生活方式和社会治理模式。”

百度创始人李彦宏对新华网记者表示：“智能体出圈了，第一次，AI的主角，不是模型，而是应用。过去几年，竞争核心是模型能力：谁更聪明、谁更会写、谁推理更强。但智能体火起来，说明用户真正买单的不是‘你会不会’，而是‘你能不能帮我把事做完’，这标志着AI在从聊天工具向数字员工和代理人转变。”

“智能体出圈代表着AI的发展从模型阶段走向了应用阶段，AI将以前所未有的速度向各行各业、各种职业、各类场景进行渗透，它代表着AI的竞争从智力转向了执行力。”李彦宏说。

在李彦宏看来，全球日活智能体数（DAA）对应着移动互联网时代通用的度量衡日活用户数（DAU），“衡量一个平台和生态的繁荣，更应该看的是DAA这个指标，意味着多少Agent（智能体）在给人类干活，并交付结果。”

《实施意见》要求，“夯实技术底座，健全标准体系，降低智能体研发、适配、应用门槛，为丰富智能体产品及服务奠定基础。”

要形成稳定可靠、跨系统协同的智能体行动闭环，智能体需构建覆盖感知、规划、执行、验证全链路的技术能力，在复杂业务场景中自主完成端到端任务，而底层技术架构的成熟为产业规模化落地提供了决定性支撑。

月之暗面（Moonshot AI）旗下Kimi相关负责人在接受新华网采访时介绍了智能体的“大脑”基座，Kimi形成了从基础模型架构到智能体编排系统的完整技术能力体系：Kimi自研了基于万亿参数稀疏混合专家（MoE）架构的大语言模型，总参数量达1万亿，每次推理激活约320亿参数，配备384个细粒度领域专家，通过Top-8动态路由机制在保持海量知识容量的同时实现高效推理。模型采用MLA多头潜在注意力机制，通过低秩矩阵分解将显存占用降低至传统架构的1/8，并引入多Token（词元）预测目标提升生成效率，这为智能体执行长程复杂任务提供了高性能的“大脑”基座。

赋能科研：从翻遍文献到一键出报告

《实施意见》围绕科学研究、产业发展、提振消费、民生福祉、社会治理等方向，提出了19个智能体典型应用场景。在19个典型应用场景中，科学研究被置于首位，并且强调创新驱动和应用牵引，为科研智能体的发展提供了清晰的政策支撑。

2025年7月26日，上海交通大学、深势科技推出了通用科研智能体“SciMaster”。

“分子动力学在药物筛选中的典型流程是怎样的？”当用户提出科学问题，SciMaster可将问题拆成多个子任务，全网及海量文献检索，整合资讯、数据、论文、专利等资料，快速生成可落地的深度调研报告。

据深势科技首席技术官（CTO）廖若雪介绍，在生物医药科研领域，包括药物的靶点发现和分子计算等，智能体能够将跨靶点的研究证据整合进知识图谱，支持药物研发。在新材料领域，包括电解液、固体电解质有机合成等方面，也有智能体研发辅助产品。

据湘汉智库研究报告，当前智能体已深度渗透多学科科研场景，成为跨领域科研创新的核心工具，目前主要落地于材料化学、基因组生物信息、生物医学健康等核心科研领域。

赋能电商：一句话下单、个性化订制

“帮我点杯咖啡，不加冰”“两份米线，其中一份加辣不要豆芽”“帮我点杯奶茶，不加糖，多放珍珠”“帮我订去莫斯科的机票和酒店”……智能体可根据个性化需求，自动识别意图、定位、偏好，并推荐可下单商品。

在商业领域，智能体正融入全流程。今年初，淘宝闪购与千问智能体完成深度打通。5月11日，千问与淘宝全面打通，标志着全球超大规模电商平台与智能体应用的深度融合。据淘宝闪购介绍，截至目前，上述合作已覆盖全国300余个地级及以上城市和超3000个区县，涵盖餐饮外卖以及超市便利、生鲜蔬果、鲜花绿植、医药健康、手机数码等诸多品类。

“AI正在重构即时零售消费体验，‘智能体+即时零售’的结合意味着即时零售从‘货架搜索’向‘AI对话式推荐’转型，智能体作为新入口，为平台带来的增量可以沉淀为长期价值。”淘宝闪购相关业务负责人表示。

有趣的是，AI在帮忙选品时，还可能做出“劝退”动作。消费者多买、错买的决策，AI会在过程中及时干预。比如，记者在试图使用智能体购买“量子水杯”时，就被千问“强制”科普“劝退”了。

赋能金融教育：秒读财报、梳理文献

智能体还深度落地金融、教育等多元行业场景。

以前券商研究员做行业研究，得泡在海量研报、财报、新闻里，翻遍资料，2-3天才能攒出一份初稿。如今只要把研究主题丢给Kimi，它立刻自动全网检索、逐页精读财报、提炼核心观点，一气呵成输出结构化分析草稿。原先2-3天的“苦活儿”，如今2-3小时就搞定。

在教育领域，文献“大山”一直是高校师生的“头号痛点”——一个研究方向动辄成百上千篇中英文文献。如今只需一次对话，智能体就能一口气读完所有文献，自动完成分类归档、提炼核心观点，梳理出包含研究脉络、争议焦点、未来方向的完整综述框架。据Kimi合作博士生导师反馈，博士生过去要熬2-3周才能啃完的文献梳理，现在1-2天就能拿出初版，内容还更全面、更系统，效率拉满。

据中国通信工业协会数据中心委员会主编的《AI智能体赋能行业决策：趋势与实践白皮书（2026）》，智能体正集中爆发，制造、金融、政务等行业成“主战场”，行业渗透率超过50%。

筑牢智能体安全防线

智能体并非完美无缺，“满嘴跑火车”的幻觉、决策跑偏、执行掉链子，是行业面对的难题。为了给智能体“纠偏”，研发端从技术上打响了“精准纠错战”。

廖若雪表示：“科学场景对于事实的准确性和说推理的可溯源性具有极高要求。首先，智能体的知识需要是结构化的，而非完全依赖模型去记忆知识，我们会把科学文献中的命题及推理链，转化为可查询、可校验的知识图谱。其次，智能体的推理过程也可以通过特定的算法进行置信度的校验。此外还需强调验证，关键的科学论断不能只由智能体自行评估，论文是可执行的工作流，我们会真正去进行可复现的计算，通过实际的运行结果来验证结论是否真实。”

通用场景中，智能体的核验能力也在加强。据阿里巴巴千问事业部相关负责人介绍，今年3月，通义千问上线了“引证”功能，内置硬核事实复核机制。用户问到新闻时事、政策动态这类需要“有据可查”的问题时，会发现回答末尾跳出一枚“引证”按钮。点击“引证”，智能体逐字核对关键信息：有权威信源背书、经得起交叉验证的内容，亮绿“盖章可信”；来源模糊、说法矛盾或未被主流媒体证实的信息，就醒目标红，提示“还需再核实”。

除AI幻觉等内容与认知风险，智能体还需针对数据安全、算法安全、交互安全等关键风险点筑牢防线。

淘宝闪购相关业务负责人表示，“一句话点外卖”服务流程的背后，是一套完整、闭环的流程，涉及查询、渲染、加购、支付、数据打通等上百个细小项目。针对餐饮、零售等细分领域，平台进行了大量定向训练。同时，AI外卖场景的风控还需关注模型层风险，确保智能体安全执行。

近日，360 AI安全研究院发布的《AI安全系列报告：智能体安全新范式——当AI有了“手和脚”，企业安全边界必须重建》指出，随着智能体加速进入企业办公、研发、运维、客服等核心业务场景，AI安全的核心问题正在从“生成风险”转向“执行风险”。

针对安全问题，360提出了两条解决路径：一是用AI加持传统安全防护，提高漏洞发现、入侵研判、样本分析和响应处置效率；二是让不确定性任务在安全约束下执行，让智能体可以做事，但不能越界。

清华大学文科资深教授、苏世民书院院长薛澜认为，《实施意见》通过设定全链条安全要求，特别是对关键领域和脆弱群体的重点保护，系统性预防智能体技术滥用、决策失控等风险，保护国家安全、公共利益和人民权益，为智能体技术在全社会规模化应用建立必要的安全信任基础。

智能体的崛起，既是技术迭代的必然，更是时代发展的趋势。这不是简单的技术升级，而是工作方式、商业逻辑、生活体验的全面重构。政策护航、技术成熟、场景落地，多重力量正推动智能体从行业探索走向深度赋能。

新华网北京5月26日电