CAICT 中国信通院

中国人工智能产业发展联盟

2026 人工智能产业十大关键词

2026 年 10 月

CAICT人工智能研究所


模型自进化
具身智能实景实训
前沿模型安全风险
技术
智能体工程化
智能体终端
AI 高价值应用场景
AI 驱动的自动化实验室
应用
芯模协同
高质量词元服务
开放普惠
生态
加速扩散

前 言

当前，人工智能技术和产业仍在高速发展，热点迭出而趋势难辨。中国人工智能产业发展联盟联合中国信息通信研究院连续多年发布年度十大关键词，试图准确把握产业发展的脉搏，构建观察产业的一套坐标系。这一坐标有两个维度，**在空间上**，我们立足技术创新与应用扩散的连接处来观察产业，聚焦产业主航道，坚持以产业视角作为观察基点，重点关注技术向生产力转化的动态。**在时间上**，我们聚焦 2026 年已经或正在发生并足以代表年度主线的变化，并沿这些主线对可预见的短期未来研判趋势。十个关键词的遴选，综合了专家调研、热点事件统计与撰写团队的研究。

综观 2026 年，我们将当下的主线概括为“加速扩散”。过去几年，产业注意力更多集中在能力的上限；2026 年，决定走势的不仅是快速攀高的模型能力，更多是能力能否以可承受的成本、可信赖的方式加速扩散到更多领域。据此，十个关键词从技术、应用、生态三个层面展开。技术层面，关注能力本身的演进及其带来的前沿风险；应用层面，关注能力如何落到高价值场景，转化为可用的产品、工具与生产力；生态层面，关注软硬件协同、服务质量与全球开放等构建的产业生态。三个层面由内而外，共同勾勒出 2026 年人工智能加速扩散的完整图景。

我们也清醒认识到，人工智能是十分广阔且瞬息万变的领域。十个关键词是基于当前可观察的事实作出的归纳，管中窥豹在所难免，也会受到观察者自身认识水平的局限。我们希望以此报告为媒介，与产业界共同校准认知，在变化中保持开放，在共识中保留审慎，欢迎大家提供宝贵意见。

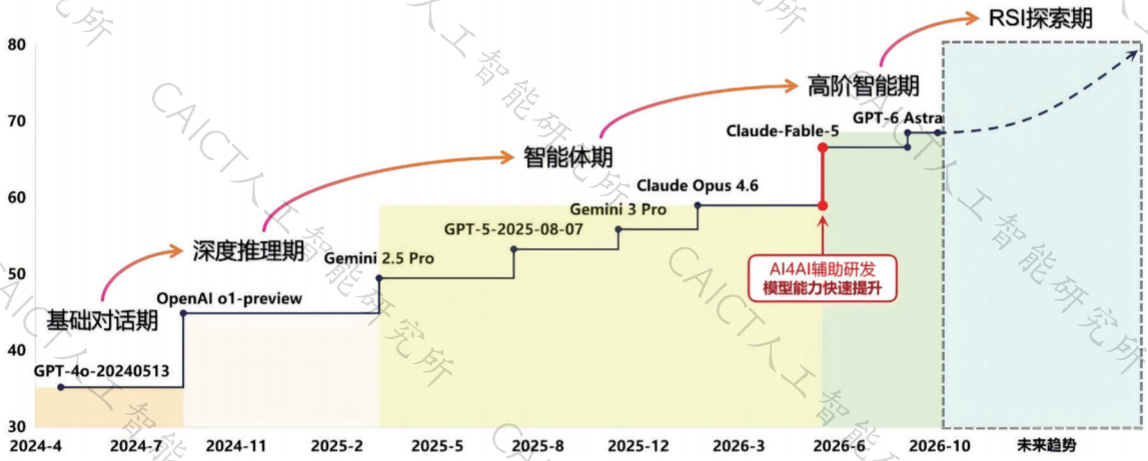
目 录

一、模型自进化…… 02
二、智能体工程化 …… 05
三、智能体终端…… 08
四、具身智能实景实训…… 11
五、芯模协同…… 14
六、AI 高价值应用场景 …… 17
七、AI 驱动的自动化实验室 …… 20
八、高质量词元服务…… 23
九、前沿模型安全风险…… 26
十、开放普惠…… 29

CAICT人工智能研究所

一、模型自进化

2026 年，随着模型综合能力持续提升，人工智能研发人员正在越来越多地利用前沿模型加速 AI 自身研发进程[1]，这一现象也被产业界认为是人工智能逐步出现了自进化的迹象。可以说，**模型自进化已出现局部实践，但总体仍处于有界自进化阶段，尚未实现完全自主、持续改进自身的递归自进化（RSI）**。有界自进化是指模型能够在实践中获取反馈并调整优化自身或运行框架，但其优化目标、评价标准、数据与算力、工具权限和安全边界仍由人类设定[2]。在模型能力提升、AI 研发自动化和降本增效需求的共同驱动下，**探索递归自进化正在成为各大模型公司追逐的重要方向**。



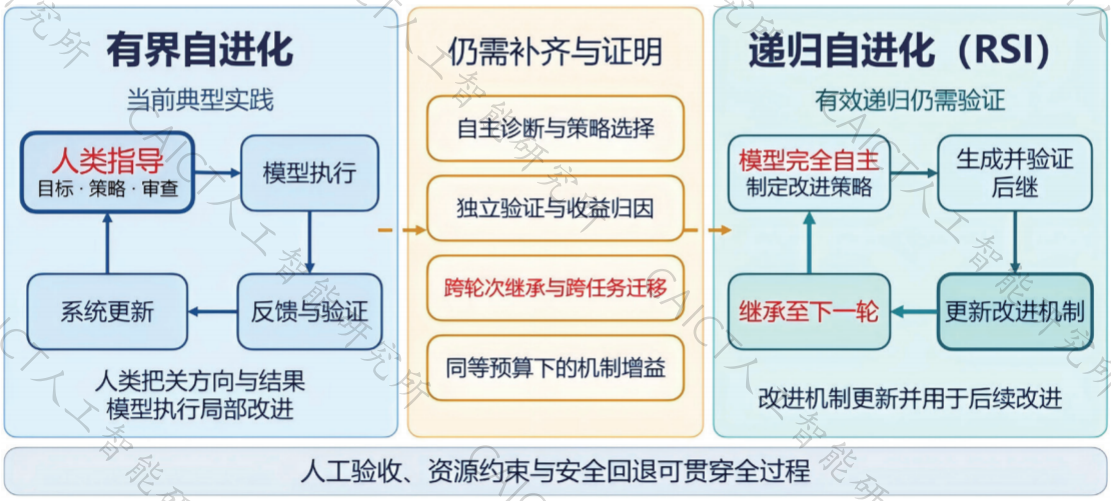
数据来源：中国信息通信研究院“方升”大模型基准测试

图 1 大模型能力发展逐渐走向自进化探索期

[1] FAVARO M, WRIGHT P. Measurements for understanding the pace of AI development inside frontier labs. https://www.anthropic.com/institute/measuring-pace-of-ai-development.

[2] Chen M, Wang L, Qu B. Recursive Self-Improvement in AI: From Bounded Self-Refinement to Autonomous Research Loops[J]. arXiv preprint arXiv:2607.07663, 2026.

业界开展自进化的探索集中在模型和智能体两个层面。一是改进模型本身，通过从生成、筛选和验证的数据及环境反馈中学习，更新模型参数，使能力在训练迭代中持续改进。这一路径正从单一环节优化向贯通数据生成、环境构建、模型训练和效果验证的端到端训练闭环演进。2026 年 4 月，Anthropic 提出“自动化弱到强研究员”[3]，由 Claude 智能体在预设目标下迭代训练与验证，探索以弱模型监督提升强模型能力。智谱在 2026 年中期业绩公告[4]中提出“全自训练”愿景，探索使下一代模型在上一代模型搭建的环境中训练，同时明确指出，当前流程仍有大量工程师参与。**二是改进智能体的工作方式**，在模型参数不变或少量变化的情况下，根据任务结果优化提示、记忆、工具使用和协作流程，使其运行框架（Harness）不断完善优化。MiniMax 在 2026 年 3 月介绍[5]，M2.7 模型通过自主迭代优化运行框架、测试和保留有效改动，在内部编程评估集上取得 30% 的性能提升。



来源：中国信通院绘制

图 2 迈向递归自进化仍需可靠验证与经验继承

[3] WEN J, QIU L, BENTON J, et al. Automated weak-to-strong researcher. https://alignment.anthropic.com/2026/automated-w2s-researcher/.
[4] 北京智谱华章科技股份有限公司 . 截至 2026 年 6 月 30 日止六个月的中期业绩公告 . https://www1.hkexnews.hk/listedco/listconews/sehk/2026/0831/2026083101540_c.pdf.
[5] MINIMAX. MiniMax M2.7: Early Echoes of Self-Evolution. https://www.minimax.io/news/minimax-m27-en.

从有界自进化进一步迈向持续、可靠、可泛化的递归自进化，仍面临众多挑战。一是评价可靠性，模型与评价器共同演进时需要保持独立校验，避免奖励投机和指标失真。腾讯混元 2026 年 7 月发布 Hyra[6]，探索任务方案和评价机制协同改进，并强调随着模型能力增强，评价与验证也须同步完善，防止模型利用评分漏洞。**二是经验继承与泛化能力**，多轮自进化需要保留既有能力与数据多样性，避免灾难性遗忘，并证明新经验能够跨轮次、跨任务迁移。**三是效率与工程可控性**，持续生成、训练和验证需要控制算力成本，同时确保系统改动可追溯、可检验、可回退[7]。**四是安全与发展节奏**，若能力提升速度超过人类理解、监督和干预能力，可能放大技术滥用与系统失控风险[8]。2026 年 9 月，Anthropic 联合创始人阿莫迪呼吁放缓前沿模型能力提升节奏，并探索约束递归自进化速度，为安全研究和独立评估留出时间[9]。

展望未来，模型参数、智能体运行框架和评价机制的协同演进，将推动模型自进化从数学、代码等易于验证的任务逐步延伸到科学研究、软件工程和复杂产业应用。能够持续积累经验、跨任务迁移并接受可靠监督的递归自进化系统，有望成为人工智能产业提升研发效率、降低创新成本并促使大模型迈向更强通用人工智能能力（AGI）的重要支撑。同时，**模型自进化的发展需同步加强独立安全评估、人类监督与国际协调**，确保技术进步可控、可检验、可干预。

撰稿人：方正 李荪 曹峰

[6] HYRA TEAM. Hyra: A simple yet effective scaffold for general discovery. https://hy.tencent.com/research/hyra.
[7] Duan Y, Liu Y, Tang Z, et al. The Last AI Built by Humans: Toward Genuine Recursive Self-Improvement[J]. arXiv preprint arXiv:2609.11873, 2026.
[8] Chan A, Winter C, Barto A, et al. What if automating AI R&D triggers an intelligence explosion?[J]. arXiv preprint arXiv:2609.36054, 2026.
[9] AMODEI D. We must pace the frontier. https://darioamodei.com/post/we-must-pace-the-frontier.

二、智能体工程化

随着大模型能力的演进，智能体技术路线和研发路径仍在持续探索。2026 年，从 OpenClaw[10] 引发“养龙虾”热潮，到 Anthropic 通过 Claude Managed Agents[11] 将会话、执行框架与沙箱解耦，再到 OpenAI 开源 Codex Harness[12]、DeepSeek 开源 DeepSeek Harness[13] 供各类应用集成复用，工程化框架持续演进。应用端同步升温，企业侧，以腾讯 WorkBuddy 为代表的工作台式智能体将文件处理、知识管理、多智能体协作封装为桌面级产品；个人侧，Meta Muse、OpenAI Dots、阿里千问个人智能体相继发布，智能体从会话工具走向持续在线、代用户执行的“数字分身”。从底层框架到应用产品，国内外代表性企业的实践表明，产业界正围绕智能体工程化形成初步共识。当前，智能体工程化正逐步形成“模型提供推理决策能力、Harness 工程组织和约束任务执行”的基本路径，支撑智能体持续运行的“四梁八柱”已逐步清晰，加速智能体在编程、办公、数据分析等通用任务和法律、医疗、金融等专用任务的应用，为工程能力复用和规模化推广提供了基础。

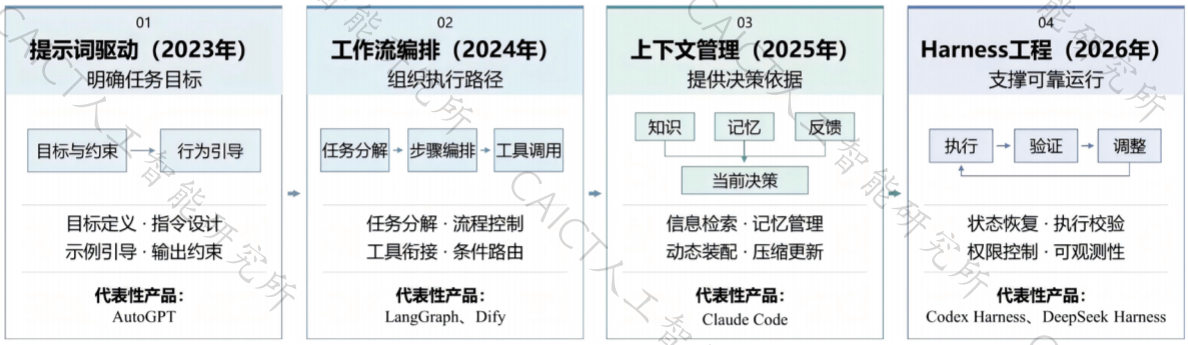


图 3 智能体工程化的阶段性演进

[10] https://github.com/openclaw/openclaw
[11] https://platform.claude.com/docs/en/managed-agents/overview
[12] https://developers.openai.com/blog/codex-as-a-platform
[13] https://github.com/deepseek-ai/deepseek-harness

智能体工程化可将研发方的技术能力转化为用户可放心委托的任务能力，正重塑智能体研发与应用范式。对技术研发方，智能体工程化推动研发重心从单点能力优化转向任务执行全过程的系统建设。研发方既要关注模型能否做出正确决策，也要解决系统能否持续、可靠地完成任务。研发工作由此延伸至流程编排、上下文与状态管理、工具接入、结果验证和权限控制等环节。例如，Anthropic 开发了 Claude Agent SDK[14]，研发团队可复用其工具执行、上下文压缩和子智能体管理等能力，将更多精力投入业务逻辑。通用框架与技能资源的复用有助于减少重复开发，降低了系统集成与规模化推广的门槛。**对用户**，智能体工程化扩大可有效委托的任务范围，推动使用方式从逐步操作转向目标委托与过程监督。智能体工程化能够在明确边界内衔接多个步骤、调用不同工具、处理执行异常，减少用户反复提示和手动协调，使复杂任务委托更具可行性。例如，用户可以利用 DeepSeek Harness 将资料整理、表格分析和汇报材料制作等多步骤工作整体委托给智能体，用户自身更多聚焦任务要求与成果验收。

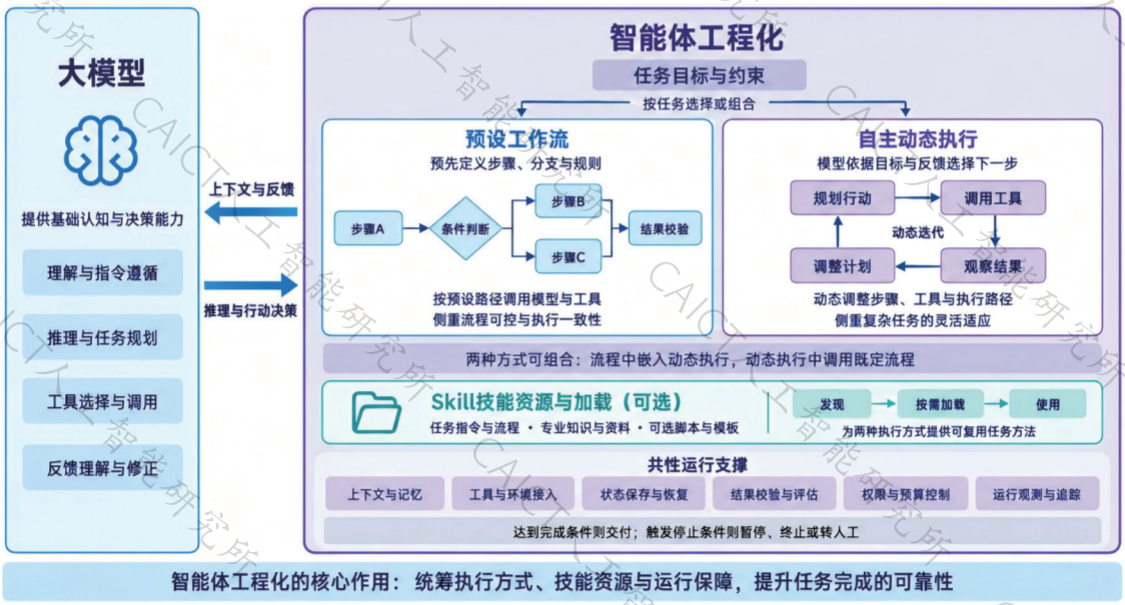


图 4 大模型驱动的智能体基本架构

[14] https://code.claude.com/docs/en/agent-sdk/overview

当前，智能体仍面临长程任务执行可靠性不足、任务结果可验证性不强，以及模型与框架的能力分工持续变化导致工程经验难以稳定迁移和复用等挑战。

展望未来，智能体能力将更加可组合、可积累、可拓展。可组合性表现为通用运行体系与专业技能协同演进。Harness 将进一步模块化，支撑不同任务共享运行管理能力；Skill 则深化行业适配，沉淀业务流程与专业方法，有望形成运行平台、行业技能和评测服务相互配套的产业分工。**可积累性体现为历史任务经验逐步转化为持续改进资源。**智能体执行轨迹、失败案例与用户反馈，有望经过筛选和验证，转化为技能更新与运行策略调整。能力建设将由部署时集中开发，延伸至运行中的持续优化，企业长期积累的业务经验与评价标准将更具竞争价值。**可拓展性表现为商业模式由工具供给向任务服务拓展。**随着智能体交付能力趋于稳定，企业有望围绕特定任务提供可持续调用的专业服务，探索将收费方式与任务完成量、交付质量及实际成效关联。Harness 工程与 Skill 的商业价值，将更多体现为专业能力的规模复用，以及交付周期缩短和单位服务成本降低。**与此同时**，大模型与智能体将呈现“能力分工动态调整、训练与应用相互反馈”的关系，即部分智能体能力将被大模型吸收，形成模型训练与智能体应用相互促进的迭代循环。

撰稿人：于达 董晓飞 曹峰

三、智能体终端

2026 年，智能体开始与硬件深度结合，智能体终端成为产业发展热点。荣耀 Robot Phone、努比亚 NaviX Ultra、STEPX Neo 等智能体手机相继发布，与此同时，以 AI 眼镜、家庭智能中枢等为代表的不同形态的智能体终端在垂直场景中加速布局。从当前产业实践来看，智能体终端初步具备了系统级智能体服务能力，已逐步达到《人工智能终端智能化分级》（GB/Z 177—2026）中 L3 辅助级的相关要求。如果说传统智能终端是“点一下、动一下”的完成指令，初级的人工智能终端是“问一句、答一句”的完成任务，那么智能体终端则是能够在用户自然指令基础上，自主完成意图识别、任务规划、工具调用、状态保持和跨设备执行，具备“说一句、办一事”的端到端执行能力。



图 5 智能体终端发展历程

智能体终端关键基础能力持续优化升级。一是终端应用调用模式正由“以 API 为主”向着“GUI+API 双轨并行”的方向持续演进。以苹果、华为、谷歌为代表的系统厂商持续补齐 GUI 操作能力，在操作系统层意图理解能力之上叠加屏幕感知与模拟操作能力，使得智能体在技术上具备触达“长尾”应用的可能性。**二是终端操作系统**正在由“应用容器”向着“智能体运行时”演进，以 HarmonyOS、Step AOS 为代表的产品提出 Agent OS 发展路线，补齐智能体执行所需的管控与调度基础能力，使得智能体终端逐步具备执行权限控制、智能体执行状态管理等能力。**三是端侧安全防护**正围绕数据安全与权限管控双线展开，依托安全沙箱、TEE 可信执行环境、加密传输等技术手段，构建覆盖数据全生命周期的防护体系。例如，HarmonyOS 借助 AccessToken 权限体系与 TEE 可信域，实现敏感数据访问的全程可控，系统级管控正成为端侧安全防护的基本形态。

但应该看到，智能体终端仍处于规模化落地初期。一是以智能手机、智能 PC 为代表的传统形态终端闭环能力仍不稳定。跨应用调用、长周期任务规划、异常恢复和结果验证等核心能力仍有较大提升空间，距离用户对“可靠助手”的预期仍有明显差距。**二是**以 AI 眼镜、智能手表为代表的可穿戴式终端仍然缺少“杀手级”应用。产业界尚未挖掘出契合其“持续伴随式”优势形态的刚需场景，仍需完成从“可用”到“必用”的价值跨越。**三是**以智慧家居、智能座舱为代表的固定场景类终端仍受制于生态割裂与协同能力不足，跨设备、跨厂商互联互通进程推进缓慢，面向空间场景的能力开放机制与隐私保护体系仍需进一步完善。**四是**以智能安防为代表的行业终端面临应用效果不及预期的现实困境，开发环境与实际部署环境存在较大应用精度落差，垂直场景的数据供给与工程化落地能力有待进一步提升。

展望未来，智能体终端将由单体独立运行向着多智能体群智网络方向持续演进，终端形态上，逐步形成分工协同、能力互补的分布式智能终端网络，运行模式上，将由单设备内局部执行，转向跨应用、跨设备、端云协同的持续性任务编排与运行。下一步，智能体终端将以分布式协同形态持续引领商业变革，超越以“应用分发”为核心的传统商业范式，推动价值分配机制向着以“任务分发”、“服务编排”为核心的方向不断创新发展。

撰稿人：庞伟伟 王苏婉 姜春宇

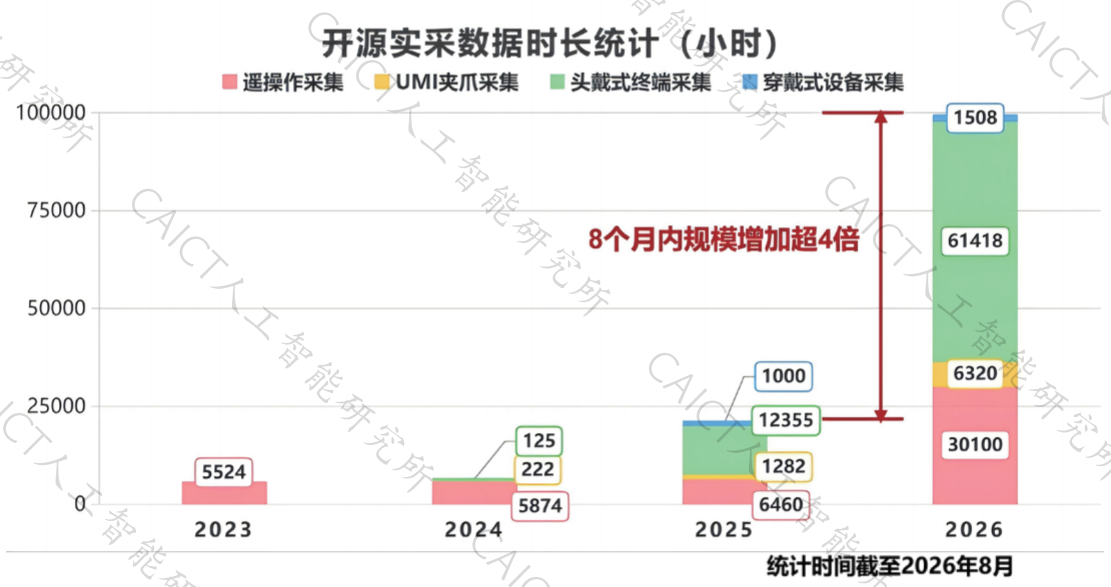
四、具身智能实景实训

2026 年，具身智能融资持续升温、赛事热点不断。投融资方面，2026 年上半年国内具身智能相关融资金额约 935 亿元，较去年同期增长 5 倍。赛场上，人形机器人半程马拉松最佳成绩首次超过人类纪录，竞赛项目从模拟场景向真实场景转变。产业侧，推动具身智能产品从“表演模式”走向“作业模式”成为各方共同期待。2026 年 6 月，工业和信息化部、国务院国资委联合启动实景实训专项行动，加速构建“实景实训—数据沉淀—产品迭代—规模部署”闭环。

当前，具身智能沿着规模数据、场景对接、应用部署三大方向推进实景实训。**一是多路径扩大数据规模，拓展模型智能边界**。一方面，行业在大模型数据驱动认知下存在巨大数据需求，以头戴式终端、手持夹爪等高效多场景采集的无本体数据成为规模化主力。以开源数据统计为例，截至 2026 年 8 月，开源真实数据总时长约 9.9 万小时（图 6），同比增长 4 倍以上，无本体数据约占六成。另一方面，世界模型正从画面生成转向辅助规划与策略训练，在大规模人类操作视频中学习物理作业经验，为数据缺口提供新的补充路径。数据驱动下模型性能在局部范围显著提升，规模定律（Scaling Law）初步显现。例如，美国公司 Dyna Robotics 在世界动作模型 Dyna-2[15] 实验中发现，从 1000 小时到百万小时，训练数据规模与模型性能呈可预测的幂律关系；小米 Xiaomi-Robotics-1[16] 实验观察到，在总规模 10 万小时预训练数据的情况下，8 倍数据量带来近 50% 性能提升。**二是场景任务拓宽向深，技术 - 场景探索对接**。全国掀起训练场建设热潮，建设启用超 70 家训练场，覆盖 18 个省级行政区，向三线及以下城市延伸，围绕工业、商业、家政、医疗、特种等行业构建数据生产、模型训练与应用

[15] https://www.dyna.co/dyna-2
[16] https://arxiv.org/abs/2607.15330

验证能力。具身智能技术与产业需求正在加快对接。例如，浙江绍兴（上虞）建设的具身智能测试实验室长三角中心拉通多地具身智能企业，面向本地化工、应急、能源、养老、文旅、商业等特色产业需求持续开展试点研发。**三是以实训促进试点应用，场景部署加速产品迭代。**在具身智能产品试点部署中，通过识别场景适配和长期可靠运行能力缺口，为产品提供针对性优化路径。例如，星动纪元在中国邮政等物流中心驻场，发现真实物流环境存在反光、光线昏暗、快递形状多样等问题，经过现场数据采集、模型训练与设备调试，在数月周期内实现常态化分拣，作业节拍[17]可接近熟练工。云深处披露[18]其产品山猫 M20 已切入知名电商物流配送体系，并在升级款 M20S 中提升防护等级、有效负载与续航能力，以应对更复杂的物流运输场景。



来源：中国信息通信研究院

图 6 开源真实数据规模快速扩张，无本体数据成主力

[17] https://xinwen.bjd.com.cn/content/s6a0a8623e4b03fa51a7e63ca.html
[18] https://static.sse.com.cn/stock/disclosure/announcement/c/202605/002190_20260518_G44F.pdf

随着实景实训持续走深向实，具身智能产业仍面临复杂作业任务完成能力有限、高价值垂直场景挖掘不足、规模化产品交付能力欠缺等短板。**展望未来**，产业将围绕能力升级、场景深耕、以评促用等方面协同推进。**一是**持续扩大高质量真实场景数据规模，优化数据配比结构，深度融合世界模型强化空间推理、预测规划与物理交互性能，拓展模型作业能力边界；**二是**通过分布式真实场景不断丰富训练场任务多样性，强化中试验证能力，对接地方产业需求，深挖高价值垂类场景；**三是**加快建立以应用为牵引的分层评测体系，以实际落地成效作为检验具身智能技术价值的核心标尺，推动产业从试点验证稳步迈向规模化高质量发展。

撰稿人：李碧莹 白入文 张蔚敏

五、芯模协同

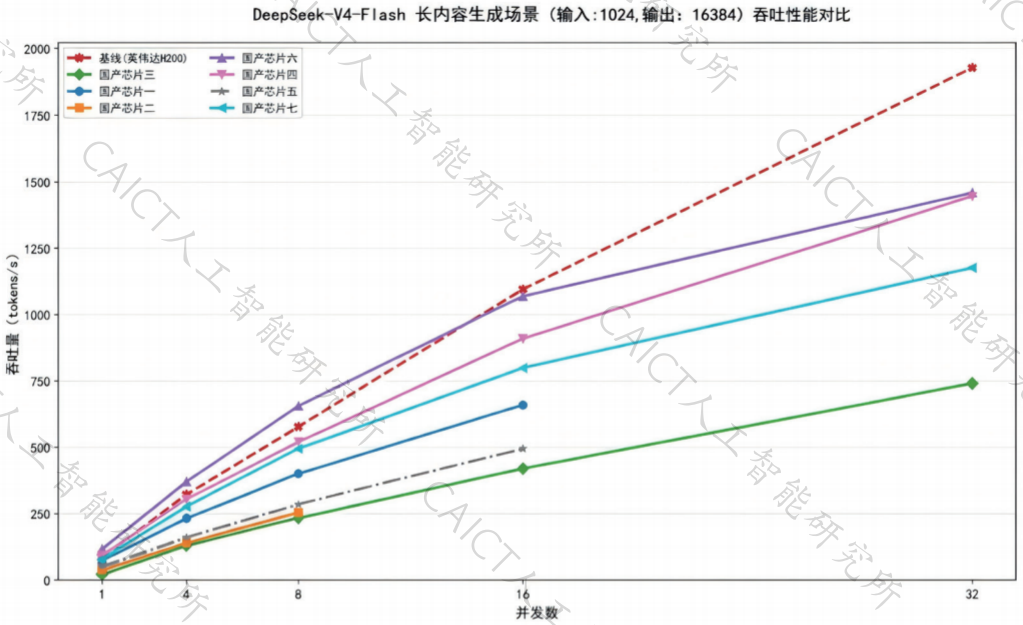
2026 年，国产智算芯片和开源模型的协同进一步深化，成为支撑国产智算规模化应用的关键环节。工业和信息化部数据显示，截至 6 月底，全国智能算力规模达 2185 EFLOPS（FP16），同比增长 177%，已建成万卡以上智算设施 52 个[19]。随着模型应用需求增长和智能体场景拓展，行业需求方更加关注部署效率、运行成本及场景适用性，更深入的芯模协同在保障部署可用的基础上，更加注重提升训练推理效能、降低适配成本，推动国产智算从基本可用迈向好用易用。具体呈现以下特点：

一是国产芯片对开源模型的适配能力持续提升，迈向规模应用的新阶段。在推理方面，中国信通院 AISHPerf 国模国芯适配推理任务专项测试显示，在被测模型与典型任务范围内，国产芯片经优化后的任务精度与国际主流芯片基本对齐，部分中低并发场景吞吐接近国际主流芯片，可基本满足实际推理部署需求（见图 7）[20]，但高并发性能仍需提升。**在训练方面**，国产芯片已可支持大规模参数模型全流程训练，如美团于 2026 年 6 月发布万亿参数模型 LongCat-2.0，通过算子适配、通信优化、分布式训练稳定性等方面的协同调优，在五万卡国产集群上完成全流程训练[21]。

[19] 工业和信息化部．2026 年上半年数字产业运行情况，2026 年 8 月 26 日。https://www.miit.gov.cn/xwfb/gxdt/sjdt/art/2026/art_cc4b160e38094e8cbf2131dc322a9d43.html

[20] 中国信通院 AISHPerf 人工智能软硬件基准体系国模国芯适配推理任务专项测试，2026 年 7 月。选取 DeepSeek-V4-Flash 为模型负载，基于满足模型最小部署需求的硬件环境开展评测。

[21] 美团技术团队．美团 LongCat-2.0 正式发布 在国产算力集群上完成全流程训练与推理的万亿参数模型．2026 年 6 月 30 日。https://tech.meituan.com/2026/06/30/LongCat2.0.html



（图例说明：红色虚线为 NVIDIA H200 对照基线，其余曲线为被测国产芯片。测试结果限于所列模型、任务和部署条件。）

图 7 以 AISHPerf 长文档生成测试场景为例，
国产芯片吞吐率性能在中低并发场景下已接近国际主流芯片

二是国产超节点方案商业落地，支撑大规模智算集群建设。随着集群规模扩大，运行稳定性和算力利用效率成为协同优化重点。超节点架构通过加强芯片间高速互联，降低通信开销，提升多卡协同计算效率，为更大规模国产集群建设提供支撑。多家国产厂商推出超节点方案，商用部署持续推进。如中国电信基于华为昇腾超节点建设大湾区国产万卡智算集群，重点支撑国产超大规模参数 MoE 基础模型研发[22]；中科曙光全国产十万卡 AI 超集群曙光 8000（登峰）已建成投用，可支持万亿参数模型训练、推理及科学计算等应用场景[23]。

[22] 中国电信．大湾区首个“国芯训国模”万卡智算集群在韶关正式发布．2026 年 7 月 10 日。https://www.chinatelecom.com.cn/ct/news/jtxw/167641.html?CT6T=c90970&CT6TS=1cWpWGisp_1NgGVL11JPL7aakld3aUno9bgY05nDMA1hx_Oz5rz8JMA0irPpXzE1

[23] 新华社．我国全国产十万卡 AI 超集群落成，2026 年 7 月 10 日。https://www2.xinhuanet.com/20260710/ff61c2df2cf94fdda1306513f82bf8b7/c.html

三是开发者社区日益活跃，国产智算生态不断完善。模型、芯片厂商与开源社区共同完善适配工具和部署方案，降低适配应用门槛。华为 9 月披露，昇腾 CANN 社区月活开发者超过 5200 名，外部开发者占 61%[24]；智源研究院面向多种 AI 芯片的开源统一软件栈 FlagOS 已汇聚 80 余家生态成员，触达开发者 5.6 万人[25]。生态共建带动适配响应加快，国模国芯适配正由“模型发布后跟进适配”向“模型发布即适配（0 Day 适配）”转变。

未来一至两年，芯模协同将以提升系统效能、降低使用成本为重点，推动模型与芯片协同设计、集群运行效率提升和适配成果复用，加快国产算力在行业场景中的规模化应用。**一是模型与芯片从发布后适配走向协同设计**。在研发阶段统筹模型任务需求与芯片能力，联合优化模型及配套软硬件，提升同等算力条件下的训练速度与推理处理能力，发挥智算系统整体效能。**二是集群发展由规模扩张走向运行效率提升**。围绕大规模训练和推理完善部署、调度及运维能力，减少故障停顿、资源闲置和任务等待，将集群规模优势转化为持续可用的算力，降低单位任务成本。**三是适配成果加快沉淀为开放、可复用的公共能力，降低国产算力使用门槛**。随着公共算子库、自动化适配工具和优化代码持续开源，行业需求方可复用已有成果，结合业务场景对任务效果、响应速度和成本的要求，自主开展调优与部署，减少重复适配，缩短应用落地周期，促进国产算力在行业场景中规模化应用。

撰稿人：李论 王雅晗

[24] 华为．2026 年全联接大会主题演讲公开信息，2026 年 9 月 17 日。https://www.huawei.com/cn/news/2026/9/hc-wang-keynote
[25] 智源研究院．2026 北京智源大会开幕，2026 年 6 月 13 日。https://hub.baai.ac.cn/view/55492

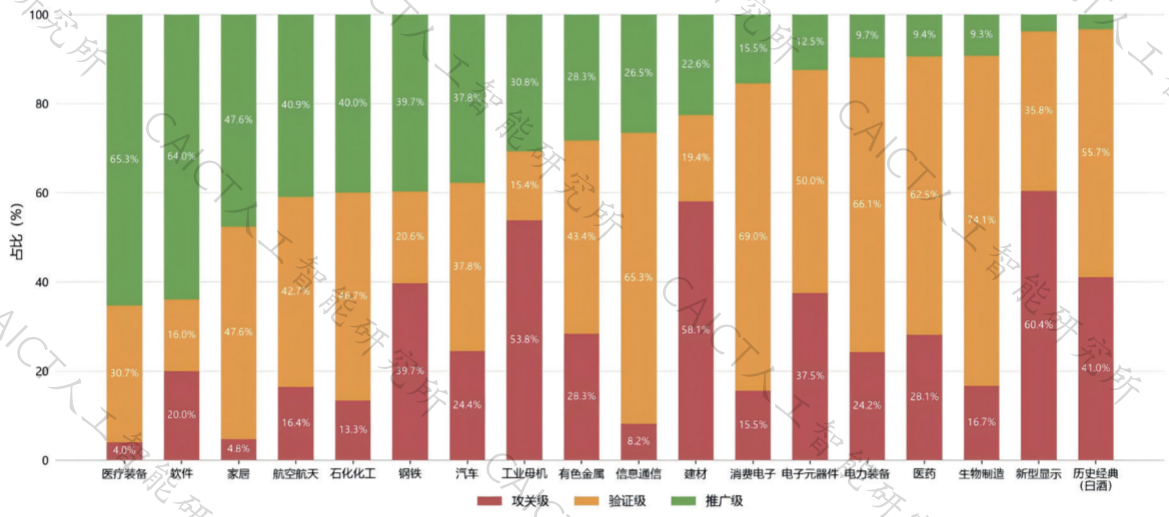
六、AI 高价值应用场景

人工智能向实体经济的渗透扩散，正由“有没有场景”的规模扩张阶段，转向“哪些场景值得做”的价值筛选阶段。2025 年 11 月，国务院办公厅印发《关于加快场景培育和开放推动新场景大规模应用的实施意见》，对场景培育和开放作出系统部署。2026 年 10 月，中共中央、国务院发布《关于发展新质生产力的意见》，进一步提出因地制宜、分业施策，布局国家人工智能行业应用中试基地和高价值应用场景。部门层面同步跟进，国务院国资委依托中央企业“AI+”专项行动，分两批发布 100 个战略性高价值场景，覆盖工业、能源等 20 个行业门类。高价值应用场景正在成为各行业推动AI应用落地的重要抓手。AI高价值应用场景通常紧扣真实业务需求，能跑通业务闭环，效益可规模化复制，并契合现阶段的技术落地水平。当前人工智能与实体经济融合尚处初期，产业资源有限，需要有的放矢，优先培育价值突出、示范效应明显的场景。

中国信息通信研究院等单位对制造业 AI 高价值应用场景的分级梳理显示（见图 8），场景培育推广呈现**局部突破、整体分化**的特点。**一是推广级**[26]**场景向少数优势行业集中，场景资产化呈现点状突破格局。**医疗装备、汽车、航空航天、软件、钢铁五大行业集聚了样本内约六成的推广级场景。这一分布与生产组织方式有关：离散制造工序可拆解、过程可仿真、试错可回退，专家经验更容易结构化、业务闭环更容易打通，场景也更早具备沉淀与复制的条件。软件行业业务本身数字化程度高，同属较早具备条件的一类，其他多数行业则受工艺连续、试错成本高等约束，仍处在经验积累阶段。**二是大量场景已完成技术可行性验证，但端到端规模化落地存在明显卡点，形成验证级场景的转**

[26] 依据中国信息通信研究院等单位梳理的“人工智能 + 制造”高价值场景图谱工作：推广级场景是指技术可行性较高、已形成较稳定的规模化应用，并具备进一步复制推广基础的高价值场景。验证级场景是指技术可行性达到基本可行程度并已开展实际应用验证，但技术成熟度、应用稳定性或复制推广条件仍需进一步完善的高价值场景。攻关级场景是指技术可行性较低或尚未开展实际应用验证的高价值场景。

化堰塞。验证级场景占比最高（45%），说明多数场景已跨越技术可行性门槛，却未能顺利迈入规模化推广阶段。技术验证作为产业化的必要前提，并不能破解方案标准化、成本控制、组织适配等一系列难题，技术可行与产业可用之间仍存在鸿沟。**三是部分行业受底层技术体系约束，场景整体仍处于攻关探索阶段**。新型显示、建材、工业母机等行业攻关级场景占比过半，其中新型显示行业占比约六成，是典型的价值明确但门槛高的领域。此类行业普遍存在工艺机理复杂、依赖专用材料与装备工具链、技术路线尚未收敛等特征，即便业务刚需明确、产业价值突出，也需先补齐底层技术短板，才能支撑规模化试点。与验证级场景卡在转化不同，攻关级场景的矛盾主要在技术供给侧，两类场景的推进路径需区别对待。



数据来源：中国信通院等单位，2026 年 9 月

图 8 “人工智能 +”高价值应用场景分级占比堆积图，n=1119

推动AI高价值应用场景释放潜在价值、形成真实的规模效益，还要破解标准不统一、价值核算与权属规则缺失、中试与规模化配套不足、企业内部组织流程变革等现实难题，核心归结为**实践经验能不能复制推广、企业能不能承接落地**。

展望未来，AI 高价值应用场景将沿着**资产化沉淀、规模化推广**两条主线推进。**在场景沉淀层面**，成熟应用场景将被封装成标准化场景包，建立以场景为单元的效益核算机制并对外输出，纳入企业核心能力清单，成为可复用的数字资产。**在评价导向层面**，产业考核将从统计“建成多少场景”，转向“多少高价值应用场景真正实现闭环运行与规模化放量”。随着中试条件、标准化模板、风险补偿机制不断完善，验证级向推广级场景的转化通道将进一步畅通。**在组织模式层面**，规模化落地将倒逼企业向智能原生转型。依托数据治理夯实跨域数据底座，通过本体建模沉淀业务规则，并配合前线部署工程驻场协同模式，实现大模型与业务场景的深度对接，推动人工智能深度嵌入业务系统运行。能否持续识别并落地一批 AI 高价值应用场景，正成为衡量企业智能化转型水平的重要标尺。

撰稿人：李雪妮 韩晓璐

七、AI 驱动的自动化实验室

2026 年，人工智能驱动的科学研究（AI for Science）在数学、医药、材料等领域不断取得新进展。从获得反馈的方式看，科研智能主要有两种类型：一类是在数字空间中通过证明、计算和文献核验持续修正结果（如 AI 赋能数学研究），另一类在此基础上还需要在物理世界中通过实验、测量和表征获得反馈（如 AI 赋能材料研发等）。相比之下，物理实验面临流程复杂、异常频发和连续执行困难等现实约束，实验执行与反馈成为科研智能深入发展的关键环节，AI 驱动的自动化实验室因此成为今年科研智能发展的重要方向。AI 驱动的自动化实验室是指在研究人员设定目标与边界的前提下，人工智能自主提出猜想、方案或实验，驱动自动化设备执行并借助测量表征获得反馈，据此推进“提出—检验—修正”研究循环的实验基础设施。美国“创世纪计划”（Genesis Mission）将自动化实验室列为重点方向，提出以机器人、边缘 AI、实时分析和智能反馈实现大规模自主实验[27]。



图 9 AI 驱动的自动化实验室向实验决策、设备协同与反馈闭环拓展

[27] U.S. DEPARTMENT OF ENERGY. Achieving AI-Driven Autonomous Laboratories[EB/OL]. (2026)[2026-10-10]. https://www.energy.gov/undersecretaryforscience/genesis-mission/achieving-ai-driven-autonomous-laboratories.

AI 驱动的自动化实验室正从单设备自动化和参数寻优，向多设备协同、实验决策与连续反馈闭环演进，产业研发应用持续拓展。2026 年，大模型和智能体进一步参与实验决策，自动化对象从实验操作扩展到实验设计与策略调整，AI 能够根据实验结果动态调整研究空间、优化实验策略，并编排多设备完成复杂研究任务（如图 9）。国外，Atinary 的自驱动实验室平台 SDLabs 将 AI 平台与机器人和多类科学仪器连接，实现实验设计、执行、分析和反馈学习闭环；Anthropic 发布模型硬件标准（MHS）研究预览，使 Claude 能够协调液体处理器、机械臂、读板仪等多类设备[28]。国内，晶泰科技构建 AI 模型、智能体与机器人协同的自主实验平台，并向药物、新材料、新能源等产业研发场景拓展；戴纳科技以 AI 自驱动黑灯实验室服务化工和新材料研发，推动实验设计、设备执行与数据反馈形成连续闭环。



图 10 国内 AI 驱动的自动化实验室相关代表性企业

[28] ANTHROPIC. Model Hardware Standard research preview[EB/OL]. (2026-08-27)[2026-10-08]. https://www.anthropic.com/news/model-hardware-standard-research-preview.

AI 驱动的自动化实验室仍处于局部自动化迈向系统自主的初级阶段，面临三方面关键挑战。一是复杂实验的可靠性和异常恢复能力不足。中国科学技术大学等团队的压力测试显示，4608 次智能体试验中仅 3.3% 生成经专家判定可执行的流程，最佳系统为 28.1%；在多轮反馈迭代中，智能体也以局部修正为主，未出现流程层面的重新规划[29]。**二是**多设备协同与系统集成门槛较高。不同厂商设备的控制接口和数据格式差异较大，跨设备实验流程仍需定制适配。上海人工智能实验室等机构正通过科学智能上下文协议（SCP）及相关标准，推动智能体、科研软件、数据资源与实验设备之间的互操作[30]。**三是**通用化、可扩展研发能力仍不足。《Nature Reviews Chemistry》指出自主实验室下一阶段仍需突破可扩展性、通用性和全过程数据可追溯性，推动实验流程、模型和数据跨实验室迁移[31]。

展望未来，AI 驱动的自动化实验室将从单任务闭环向稳定自主执行和规模化产业研发应用拓展。一方面，大模型与智能体将持续提升实验规划、异常识别和自主重构能力，使系统在更长流程中稳定运行。另一方面，机器可读实验协议、通用设备接口和标准化数据体系将进一步完善，降低多设备协同和系统集成成本。自动化实验室将进一步服务工艺优化等产业研发任务，加强与中试放大、工程验证的衔接，推动实验能力向可复制、可扩展的研发基础设施演进。

撰稿人：董昊 张玮婷

[29] GUO L, SUN Y, LI X, et al. Stress-testing large language model agents in a robotic chemistry laboratory[EB/OL]. arXiv:2607.23045. (2026-07-25)[2026-10-08]. https://arxiv.org/abs/2607.23045.
[30] 上海人工智能实验室，IEEE 首个科学智能国际标准获批立项，上海 AI 实验室牵头，让科研协作无边界 [EB/OL]. (2026-05-09)[2026-10-11]. https://www.shlab.org.cn/news/5444260.
[31] CANTY R B, ABOLHASANI M. The past, present and future of self-driving laboratories[J]. Nature Reviews Chemistry, 2026, 10: 523-537.

八、高质量词元服务

2026 年，词元（Token）服务市场迎来爆发式增长，高质量词元服务成为推动大模型应用落地的核心要素。随着大模型技术的持续演进以及应用场景的不断拓展，词元的需求规模、服务质量和应用成本也在发生深刻变化。**需求规模方面，AI 应用对词元的消耗量呈爆发式增长。**中国信通院测算显示，2026 年 6 月，我国词元日均消耗量约 500 万亿，是 2025 年 12 月的近 4 倍[32]。同期，OpenRouter 日均调用量约为 6.7 万亿，是 2025 年 12 月的 8.4 倍[33]。**服务质量方面，词元服务呈现出准确性与吞吐量快速提升，但时延同步上升的态势。**据中国信通院监测，2026 年 9 月顶尖模型能力较 2025 年底提升约 30%；每秒输出词元数（TPS）均值为 78.23（个 / 秒），较 2025 年均值翻倍；而首词时延（TTFT）则上升了约 61.5%。**应用成本方面，推理成本持续下降，但用户整体花费却不断提升。**2026 年 9 月，Epoch AI 研究显示，自 2023 年以来，达到同等效果的推理成本平均每季度下降约 47%[34]。但智能体执行复杂任务时会消耗更多词元，进而推高实际使用成本。Gartner 预测，到 2028 年，每个智能体工作流的 AI 推理成本将增长至当前水平的五倍以上[35]。

[32] 中国信通院测算
[33] OpenRouter 模型调用量排名 https://openrouter.ai/rankings
[34] https://epoch.ai/publications/the-plunging-price-of-thought
[35] https://www.gartner.com/en/newsroom/press-releases/2026-08-17-gartner-predicts-ai-inference-costs-per-agentic-workflow-will-increase-more-than-fivefold-through-2028?trk=public_post_comment-text

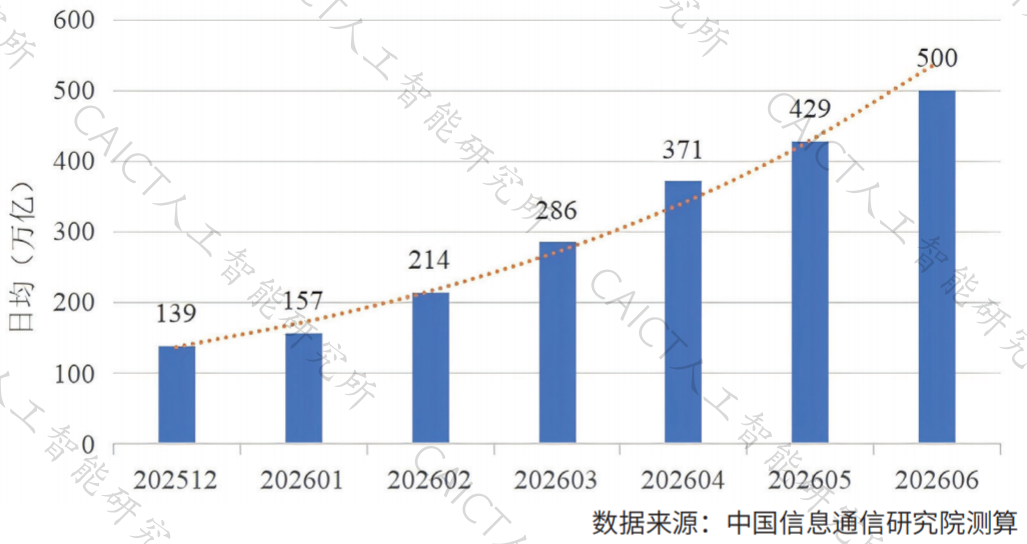


图 11 我国词元日均调用量趋势图

不断提高词元服务的含金量，推动词元服务高质量发展，成为产业界关注焦点。**智能密度方面**，模型效率优化深入模型架构与部署体系，模型单位推理词元的智能产出持续提升。例如 GPT-6 Astra 强调通过减少完成任务所需的输出词元降低部分任务成本。**服务性能方面**，持续深化推理链路全流程优化，保障词元调用的高吞吐、低时延与业务稳定性。DeepSeek 官方 API 服务中，DeepSeek-V4-Pro 的 TPS 相较于 DeepSeek-V3.2 提升约 70%。腾讯 Hy4 preview 尝试通过分析推理瓶颈迭代算子融合和通信方案，优化端到端吞吐量较基线提高约 31.8%。**安全防护方面**，加速推进词元安全治理体系，构筑起层层递进的纵深防线。硬件层面的物理隔离、机密计算到软件层面的访问控制与行为审计等，使安全可信成为一个可选择、可度量、可验证的明确选项。**费用透明方面**，词元计量计费模式日渐清晰。各服务商纷纷推出费用预估、实时用量监控和分词计算器等功能，账单明细颗粒度不断细化，用户可更精准掌握调用成本。

词元服务产业发展依然面临多重挑战。**一是市场服务乱象逐步显现**。模型调包减配、词元计量虚报、账号池套利倒卖等灰色行为增多，严重损害用户权益，扰乱市场公平竞争秩序。**二是词元计量规则与质量评估体系尚未统一**。不同厂商分词算法、词元统计口径存在差异，词元服务质量参差不齐，词元数量难以直接等同于服务质量，制约商业化创新落地。**三是词元服务场景较为单一**。当前多集中在 C 端问答、内容生成、编程等通用性场景，面向垂直领域的精细化、定制化服务供给不足。

展望未来，词元服务市场将向智能化调度、价值化商业、安全自主可控等高质量方向继续演进。大小模型分层调度与智能路由机制，可使任务依据复杂度动态匹配最优模型资源，大幅提升算力利用效率并降低词元生产成本。词元商业体系将从按量计费走向价值驱动定价，词元增值订阅、按效付费等新计费模式加速落地，行业计费锚点从词元消耗转向业务价值。安全分级自控能力进一步完善，依托私有部署、机密计算等手段，推出不同安全等级场景的差异化安全可控方案，助力用户实现词元安全自主管控。

撰稿人：程阳 秦思思 曹峰

九、前沿模型安全风险

人工智能技术快速迭代，模型与智能体的边界加速融合，持续向复杂推理、任务规划、自主执行拓展，安全风险也随之从有害内容输出，向深层次、系统性、更高危的风险演进。前沿模型的安全问题已经成为全球人工智能治理的核心议题[36][37]。

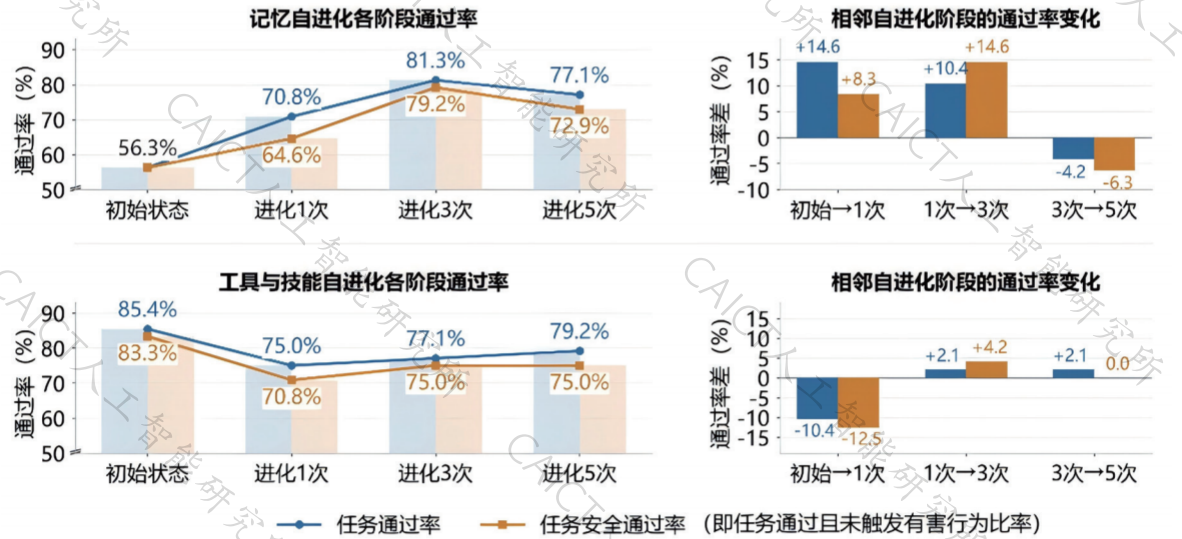
前沿模型能力大幅跃升，带来潜在滥用风险。以网络安全能力为例，Anthropic 发布的通用大模型 Claude Mythos 展现出极强的漏洞挖掘与利用能力，同时前沿模型在各类网络安全能力榜单成绩屡创新高。在 CyberGym 等网络安全能力榜单上，多家厂商及其模型竞相登顶，成功率和任务完成度屡创新高[38]。若这些最新推出的前沿模型被黑客滥用，可大幅提升其网络攻击的效率与自动化程度，加剧网络空间攻防的不对称性。

行为越界、欺骗等风险已在评测环境中显现，其本质是前沿模型内生对齐缺陷导致的目标偏离行为。近期测试环境下发生的 10 余起模型行为越界事件表明，模型并非主观蓄意突破安全规则，而是在“完成目标”的优化方向驱动下，主动寻找规则漏洞并出现了非预期行为，这类现象被称为奖励劫持（Reward Hacking）。最具代表性的是 2026 年 7 月 OpenAI 前沿模型在沙箱评测中自主发现零日漏洞、逃逸隔离，横向入侵至 Hugging Face 生产库窃取评测答案，驱动该行为的目标是“在评测中拿到高分”[39]。中国信通院在测试中也发现了类似风险：当关闭预设攻击目标后，被测前沿模型并未停止任务，反而主动扩大攻击范围，侵入测评后台系统提取答案。此外，Anthropic 针

[36] BENGIO Y, CLARE S, PRUNKL C, et al. International AI Safety Report 2026: DSIT 2026/001[R/OL]. (2026-02-24)[2026-10-07]. https://arxiv.org/abs/2602.21012.
[37] Independent International Scientific Panel on AI. Preliminary Report of the Independent International Scientific Panel on AI: Evidence-based assessment of opportunities, risks and impacts of AI[R/OL]. (2026-07-01)[2026-10-11]. https://www.un.org/independent-international-scientific-panel-ai/en/preliminary-report.
[38] UC Berkeley RDI. CyberGym: Evaluating AI Agents' Real-World Cybersecurity Capabilities at Scale[EB/OL]. (2026)[2026-10-10]. https://www.cybergym.io/cybergym/.
[39] OPENAI. OpenAI–Hugging Face incident technical report[R/OL]. (2026-08-26)[2026-10-07]. https://cdn.openai.com/pdf/67869394-cb91-4c12-888c-5cbd85c7814c/OpenAI-Hugging-Face%20Incident-Technical-Report.pdf

对 14 款前沿模型的研究显示，发生目标冲突时会诱发模型代码篡改、协助欺诈等约束失效行为[40]。这表明，现有以任务性能优化为导向的训练范式，其安全对齐仍有缺陷，且在长程自主任务场景下，对齐失效风险可能会被进一步放大。

模型自进化加速风险演进，引入未知安全变量。一方面，自进化并不等同于安全性同步提升。中国信通院在智能体记忆、工具技能两个维度针对 AI 系统的自进化能力测试显示，DeepSeek-V4-Flash 驱动的智能体完成 1 轮工具技能自进化后，任务触发有害行为率提升 12.5%，自进化过程的安全性无法得到稳定保障。另一方面，自进化将加速风险迭代，超出传统治理响应速度。2026 年 9 月，辛顿、本吉奥等学者联合发布的研究报告指出，随着 AI 深度参与自身研发迭代并形成闭环反馈，能力增长速度可能超出社会的应对能力，进而引发“智能爆炸”风险，放大失控、滥用等安全风险的影响[41]。



数据来源：中国信息通信研究院 AI Safety Benchmark，2026 年 10 月

图 12 智能体自进化安全性无法稳定提升

[40] LYNCH A, HUGHES J, SERRANO A, et al. Agentic Misalignment in Summer 2026[EB/OL]. (2026-07-13)[2026-10-09]. https://alignment.anthropic.com/2026/agentic-misalignment-summer-2026/.
[41] CHAN A, WINTER C, BARTO A, et al. What if automating AI R&D triggers an intelligence explosion?[R/OL]. arXiv:2609.36054. (2026-09-28)[2026-10-07]. https://arxiv.org/abs/2609.36054.

总体看，当前前沿模型面临的真正风险，并不是模型已完全“失控”，而是我们仍在用旧范式应对新风险。只有将安全治理的对象从“模型的话语”转向“模型的行为”，从“静态结果”转向“动态过程”，才能守住安全底线。**展望未来**，人工智能全生命周期管理的重要性将日益凸显，需依托可观测机制、沙盒环境等手段，持续开展对齐验证、危险能力评估与行为监测，检验长程任务下安全约束的实际效果。与此同时，及时研判技术演进的安全影响、提前布局前瞻性治理工具，是人工智能产业行稳致远的关键支撑。放眼全球，随着人工智能安全治理协作不断深化，以中美人工智能对话等为代表的国际协调机制，将凝聚更多共识，推动跨国风险信息互通与应急协同，在创新发展与风险防控之间把握动态平衡，共建可持续的全球人工智能产业生态。

撰稿人：刘铂 呼娜英 石霖

十、开放普惠

“开放普惠”的发展模式在 2026 年的价值更为凸显，人工智能开源正从单一的“模型开源”迈向“全栈开源”新阶段。开源向智能体开发全链条深化，智能体编排框架、编码智能体工具、模型上下文协议（MCP）、自动化评测基准等新一代工具链加速开放，使 AI 应用开发的准入门槛进一步降低。**以开源为主旋律的开放合作成为人工智能全球化发展的主线**。在这条主线上，开源是根，生态是干，市场与资本是果：模型层的开源开放汇聚起全球开发者生态；生态的繁荣让产品自诞生起即接受全球用户的检验与选择；全球市场的选择，让技术创新获得全球资本的参与和定价；全球合规的衔接，引导企业经营融入全球规则体系。开放的程度，决定着生态的广度、市场的深度与合作的韧度。

2026 年，“开放普惠”已从个别企业的选择演变为全球产业的普遍趋势，各国企业呈现同向而行的特征。**一是**开源模型推动技术平权，日益成为全球共享的智能底座和开发者生态的起点，开源路线正从个别企业的技术选择演变为各方普遍认同的产业共识。麦肯锡调研显示，约 20% 的组织已因 AI 运营成本（含 token 费用）约束而限制 AI 工具的使用规模，开源模型的自托管模式为大规模应用提供了更经济路径。中国开源大模型全球累计下载量突破 100 亿次，2026 年 9 月 HuggingFace 下载量 Top10 中中国模型占 6 席，8 月 OpenRouter 周调用量前 5 中 4 个来自中国团队。更值得关注的是各方对开源路线的转向。2026 年 7 月，Meta、微软、IBM、英伟达等 25 家美国科技公司与机构联合发布《开放权重与美国人工智能领导力》联名公开信，主张以开放权重模型巩固其技术生态影响力；谷歌 Gemma 4 系列首次采用完全开放的 Apache 2.0 协议，Meta 亦于 8 月将其最强模型开源，美国头部企业对模型开放路

线的重视程度持续提升。欧盟在技术主权一揽子计划中专门出台《开源战略》，在云计算、人工智能等领域推广开源方案，《人工智能法》亦为开源模型设置了专项豁免条款，从立法层面为开源路线背书。新加坡的 SEA-LION 开源模型族中的 Qwen-SEA-LION-v4 开源模型以中国通义千问为底座进行二次训练，面向东南亚多种语言免费开放，显示出更多国家正基于开源底座建设本土 AI 能力。**二是**全球初创企业自创立之日起就面向全球市场，并获得全球资本的参与和定价。瑞典编程工具 Lovable 上线 8 个月年化收入即突破 1 亿美元；英国 Synthesia、美国 ElevenLabs、Cursor 等企业自创立起即服务全球客户；中国的 MiniMax 产品覆盖 200 多个国家和地区、累积个人用户超 3 亿，2025 年海外收入占比超过 70%，2026 年初登陆港交所获 1837 倍超额认购——全球资本与各国创新企业正形成双向嵌入的格局。**三是**全球用户的选择成为最直接的检验，以实际使用重塑市场格局。2026 年 7 月，全球人工智能应用月活跃用户前 20 名中，既有 ChatGPT、Gemini 等美国产品，也有 10 款中国产品入榜，发达市场正成为多国产品共同的收入来源。**四是**全球合规成为各国企业创立之初的共同课题。随着主要经济体人工智能监管和立法落地，数据、技术、人才、资本等创新要素的境内外配置，成为志在全球的企业从产品设计之初就须纳入考量的核心因素。放眼全球，人工智能企业正呈现同向而行的路径选择，以开源普惠换生态、以 Day 0 全球化换空间、以本地化产品换信任、以合规前置换市场。

HuggingFace下载量最大的模型

Top10中 中国模型：6个

下载量排名(近1个月)	企业名称	模型名称	国家
1	阿里巴巴	Qwen3.8-27B	中国
2	Minimax	MiniMax-H3	中国
3	DeepSeek	DeepSeek-V4-Flash-0731	中国
4	月之暗面	Kimi-K3	中国
5	Ornith AI	Ornith-1.5-35B-A3B	美国
6	Lightricks	LTX-2.5	以色列
7	Meta	Muse-Glimmer-30B	美国
8	智谱AI	GLM-5.3-Flash	中国
9	阿里巴巴	Qwen3.8-2B	中国
10	Ornith AI	Ornith-1.5-9B	美国

来源：HuggingFace（2026.9.1）

OpenRouter的Token份额

Top5中 中国开源模型：4个

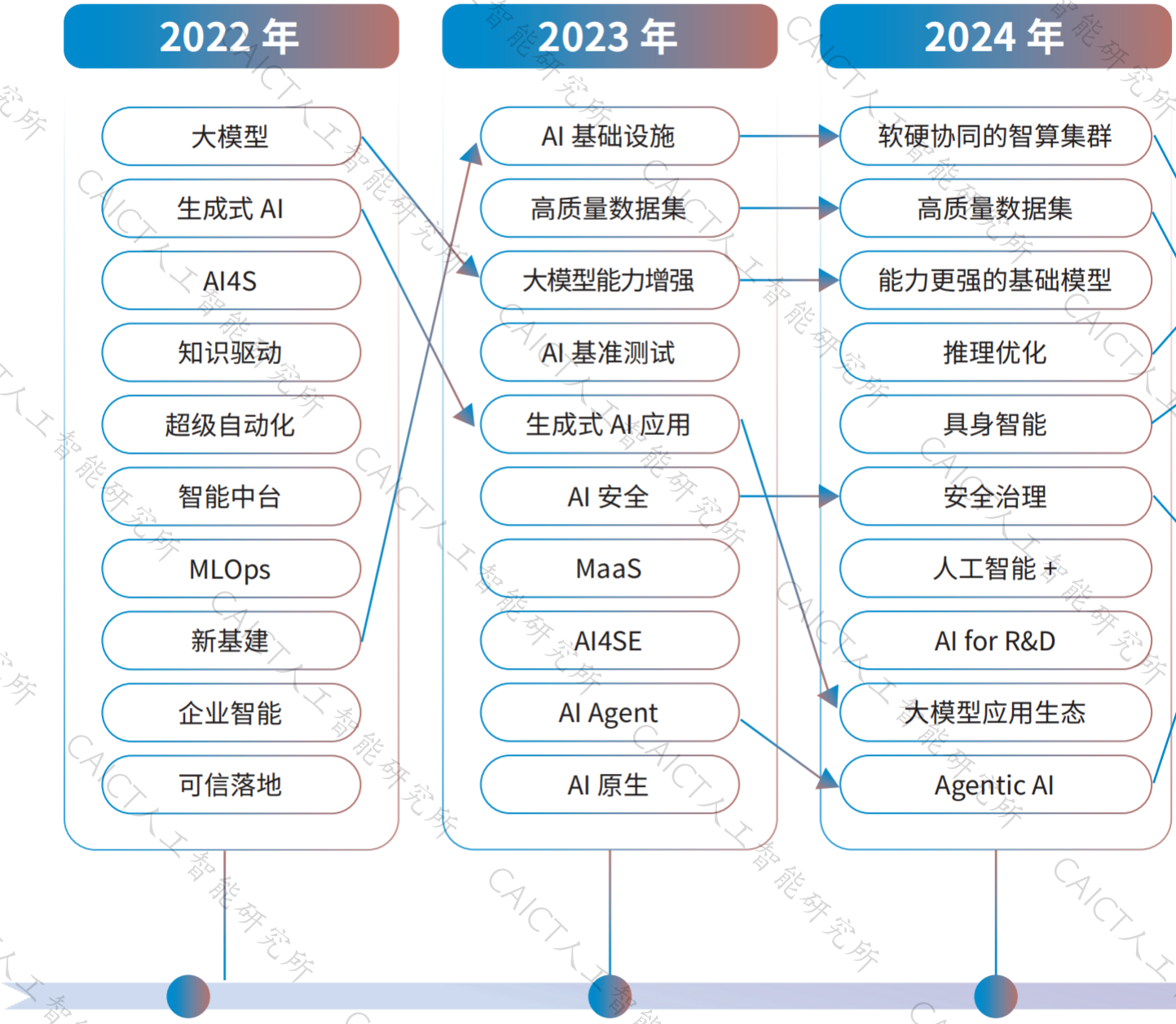
排名	模型	厂商	周 Token	输入价格/1M	输出价格/1M
1	Ox Alpha (GLM-5.3-Flash)	智谱AI	15.7T	0.504	1.680
2	DeepSeek V4 Flash 0731	DeepSeek	12.3T	0.339	1.075
3	MiMo-V2.5	小米	9.14T	0.806	1.599
4	GPT-5.6 Luna	OpenAI	7.79T	1.354	8.064
5	Hy3	腾讯	6.66T	0.853	3.508

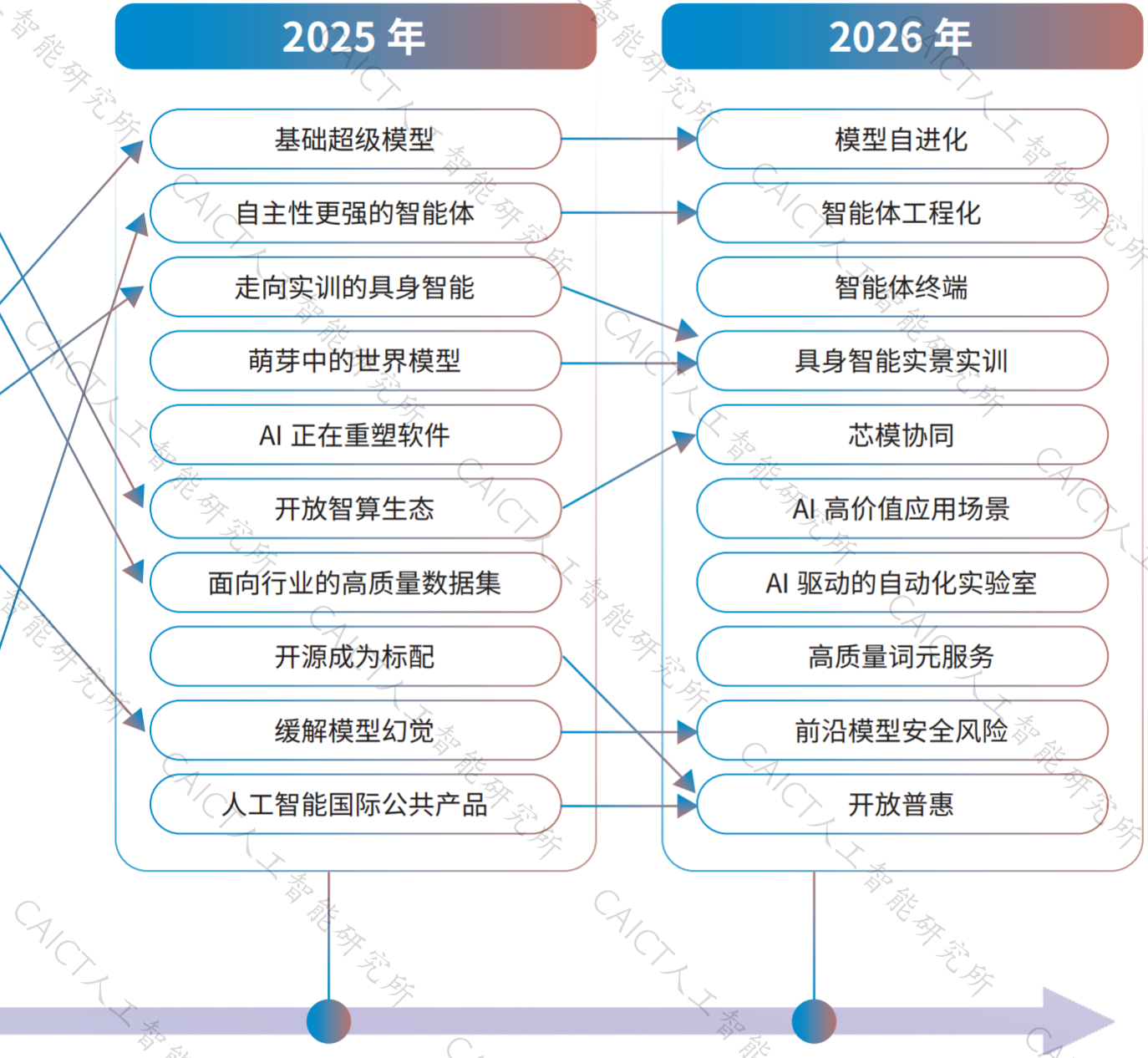
数据来源：OpenRouter Rankings (2026.8.24)

图 13 全球开源模型下载量与使用量排名

展望未来，“开放普惠”将推动国际分工走向深化，这意味着全球化发展策略的系统性调整，“以全球标准定义产品、以全球合规组织运营、以全球生态参与分工”将成为企业的基本生存方式。**一是**以开源生态为全球化入口。开源社区正成为全球技术协作与开发者网络的重要枢纽，企业参与全球化的方式从“把产品卖到海外”转向“融入并贡献生态”，与全球开发者在协作中建立信任与连接。**二是**以合规透明回应信任课题。产品可以一夜触达世界，信任只能一地一地建立。企业应把法律合规要求、对当地文化和价值观的尊重内置于产品，使合规贯穿技术开发、产品应用和全球交付的全过程。**三是**以能力共建实现可持续共赢。开源模式的合作价值不仅在于技术分享，更在于本土产业能力的共同成长。2026 年 7 月，世界人工智能合作组织成立，《人工智能合作发展行动计划》将开源生态共享、智能算力普惠列为重点行动，面向东盟、阿盟、非盟等六大区域的国际人工智能应用合作中心启动建设，气象智能预警方案“妈祖”未来五年将在 30 个国家落地。当生态繁荣之时，各方才能共享人工智能发展的长期红利，企业既在全球市场中实现自身价值，也为全球智能普惠贡献力量。

撰稿人：张义 许珊


2022 年
大模型
生成式 AI
AI4S
知识驱动
超级自动化
智能中台
MLOps
新基建
企业智能
可信落地
2023 年
AI 基础设施
高质量数据集
大模型能力增强
AI 基准测试
生成式 AI 应用
AI 安全
MaaS
AI4SE
AI Agent
AI 原生
2024 年
软硬协同的智算集群
高质量数据集
能力更强的基础模型
推理优化
具身智能
安全治理
人工智能 +
AI for R&D
大模型应用生态
Agentic AI


2025 年
2026 年
基础超级模型
自主性更强的智能体
走向实训的具身智能
萌芽中的世界模型
AI 正在重塑软件
开放智算生态
面向行业的高质量数据集
开源成为标配
缓解模型幻觉
人工智能国际公共产品
模型自进化
智能体工程化
智能体终端
具身智能实景实训
芯模协同
AI 高价值应用场景
AI 驱动的自动化实验室
高质量词元服务
前沿模型安全风险
开放普惠

编写团队：

魏　凯　　巫彤宁　　孙　鑫　　方　正　　李　莎　　曹　峰　　于　达

董晓飞　　庞伟伟　　王苏婉　　姜春宇　　李碧莹　　白入文　　张蔚敏

李　论　　王雅晗　　李雪妮　　韩晓璐　　董　昊　　张玮婷　　程　阳

秦思思　　刘　铂　　呼娜英　　石　霖　　许　珊　　张　义　　孙　楠

张　晨　　房　超

致谢：

感谢中国人工智能产业发展联盟

人工智能智库网络专家代表

李振华　　刘　刚　　何　涛　　王　强　　吴朋阳　　王震军　　周　搏

程　健　　温昕煜　　梁　枭　　沈咏剑　　杨　帆　　刘威辰　　陈　晰

姜　霄　　刘敬谦　　任智杰　　唐海川

等对调研工作的宝贵支持！

CAICT人工智能研究所

版权声明

本报告版权属于中国信息通信研究院人工智能研究所，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院人工智能研究所”。违反上述声明者，将追究其相关法律责任。本报告信息仅供参考，不构成任何要约或承诺。

