

人工智能应用 发展趋势报告（2026）

2026 AI Application Trends and Insights Report

前言

Preface

当前，以人工智能为重要驱动力的新一轮科技革命和产业变革加速演进，正在重塑产业运行与社会生活的基本方式。它不仅推动企业提升生产效率、调整组织形态，也在改变产业价值链、生活服务方式和知识生产范式。人工智能正逐步突破单一工具的边界，成为支撑经济增长、产业升级和社会创新的基础性能力。由此带来的，不只是技术能力的提升，更是对人与机器如何协作、技术如何增进人类福祉的持续探索。

在企业端，随着模型能力持续增强，工具生态不断完善，人工智能与企业系统加快融合，智能体开始由局部辅助走向任务执行与流程协同，深入办公、研发和业务运营等环节，并逐步影响企业配置资源、组织工作和划分责任的方式。这一变化主要体现在四个方面：智能办公加速普及，智能体开始承担周期更长、环节更多的复杂任务；AI Coding 向需求分析、开发、测试、部署和运维等研发环节延伸；数字员工嵌入具体岗位与业务流程，推动企业重新界定人机分工与责任边界；个人借助智能体拓展专业能力和工作半径，“超级个体”及其协作网络加快形成。随着人机协同深入岗位、组织，企业边界、协作关系与专业分工也将被重新塑造。

在产业端，人工智能的价值创造逻辑也在发生转变。随着垂直领域模型、行业知识工程 and 智能体技术逐步成熟，AI 开始进入核心业务流程，成为推动产业价值链重构的重要力量。在制造业，智能技术贯穿研发设计、生产制造、供应链管理、营销销售和售后服务，促进全链路协同；在医疗领域，人工智能辅助知识检索、诊断分析、临床决策和健康管理，推动专业能力更高效地覆盖更多场景；在金融领域，智能风控、智能投研和智能运营不断拓展数据分析与决策支持的边界。这些变化的共同基础，是将分散的经验沉淀为可调用的知识，将部分依赖个人判断的流程转化为可验证、可迭代的模型与规则，进而形成新型产业知识基础设施。

在生活端，人工智能正由被动响应指令，逐步走向对需求、情境与意图的综合理解。

多模态交互、跨设备协同和个性化服务，使智能能力加快融入衣、食、住、行、健康和娱乐等日常场景。服务形态也由单一功能供给，转向更加连续、主动和适配个体需求的体验。与此同时，人工智能能否准确理解用户需求、尊重个人选择、保护隐私安全，也成为衡量智能生活质量的重要标准。技术与人的关系不再只是“人使用工具”，而是逐步形成以人为主导、由智能系统提供持续支持的新型协作关系。

科研领域的范式变革正推动人类认知边界进入一个前所未有的拓展周期。跨尺度仿真、逆向设计与假说生成把试错环节压缩为可计算的搜索过程，蛋白质结构预测、新材料筛选与中期气象预报已显现效率跃升；垂直领域科研大模型正沉淀为学科共用的“新基础设施”。值得关注的是，递归式自我改进（RSI）正在从概念走向初步验证，AI 已开始能在算法发现、系统优化与训练调优中实现自我迭代，开启 AI 驱动自身进化的新维度。AI 由此不再只是科研工具，也正成为拓展认知边界的重要协作力量，推动知识生产从经验驱动走向数据与模型协同、从反复试错走向定向探索、从个体研究走向人机共创。

但技术的跃迁始终伴随着责任的觉醒。当开源生态推动 AI 民主化纵深发展，当可解释 AI 与隐私计算构筑伦理安全防线，当绿色计算实现技术普惠与可持续发展的平衡，我们看到技术向善正在从理念宣言转化为工程实践。AI 的快速发展让我们更应该紧密关注其背后的治理能力提升：如何让算法决策兼具效率与公平？如何使技术红利惠及全球？如何在算力跃迁中守护人文温度？这些问题的答案，将决定 AI 时代的文明高度。

本报告围绕企业 AI Agent 应用、AI 硬件发展、企业组织进化等维度设计了多份问卷，并向 2000 位不同领域的受访者开展调研，对近百多家企业进行深度调研和访谈，研判人工智能在企业进化、产业应用、生活智能、科研创新与治理优化 5 个方面共 20 条趋势，系统绘制人工智能应用全景。当技术发展从可能性的探索进入选择性的发展阶段，我们需要的不仅是技术创新能力，更是驾驭变革的智慧，在效率与公平、突破与约束、当下与长远之间，找到智能时代可持续发展的平衡点。这既是技术共同体的使命，也是每个社会参与者的责任。唯有如此，我们才能确保这场智能革命真正服务于“人的全面发展”这一终极目标，让技术进步成为文明进步的阶梯而非鸿沟。

目录

Contents

01	企业进化， 智能体重塑生产力与组织形态	P06
-----------	------------------------------	------------

02	产业智变， 从效率提升到价值创造	P22
-----------	---------------------------	------------

03	体验共生， 无处不在的智能生活	P40
-----------	--------------------------	------------

04	科研跃迁， 迈向“AI for Science”的科学智能新范式	P56
-----------	---	------------

05	智能向善， 技术普惠与可持续发展	P70
-----------	---------------------------	------------



1

企业进化， 智能体重塑生产力与 组织形态

长程任务指需要多步规划、跨系统工具调用、持续数小时乃至数天推进的复杂工作，是检验智能体办事能力的试金石。据 METR Time Horizon 评测，截至 2026 年 5 月，前沿模型在 50% 成功率下可完成的任务时长估计约 17 小时，而 2023 年初这一数字仅约 4 分钟。过去一年，智能体技术已整合复杂推理、长上下文理解、任务规划、工具调用、任务记忆和多智能体协同等核心能力，并通过 Harness 工程驾驭优化，使其能够理解目标，调用软件、数据与业务系统，连续推进跨应用、多步骤、较长周期的任务。

随着智能体执行任务能力的持续提升，以及模型能力、工具生态与企业系统的进一步融合，智能体已经开始深入地参与办公、研发和业务流程，并影响企业组织工作、配置能力和划分责任的方式，推动企业进化。这种影响主要体现在四个方向：智能办公加速普及，智能体承担更多长程任务；AI Coding 深入需求、开发、测试和部署等研发环节；数字员工嵌入岗位与业务流程，推动企业明确人机分工与责任边界；个人借助智能体扩展能力和工作半径，带动超级个体发展。



趋势一

智能体深度融入企业办公， 实现长程任务自主执行

2026 年，智能体技术在企业办公领域的演进已形成清晰脉络。桌面操作、跨应用调用、后台运行、共享项目上下文与权限治理，正在构成相互衔接的能力体系。以长程任务自主执行为起点，智能体不再只是嵌入单个应用的问答助手，而是以多重身份进入企业工作流：在个人层面，它们是替用户执行完整任务链的执行者；在团队层面，它们是参与项目协同的协作成员；在组织层面，它们是承载与复用知识资产的载体。三个层面从个体效率到团队协同再到组织能力沉淀，逐层递进，共同构成智能体深入企业办公的完整图景。

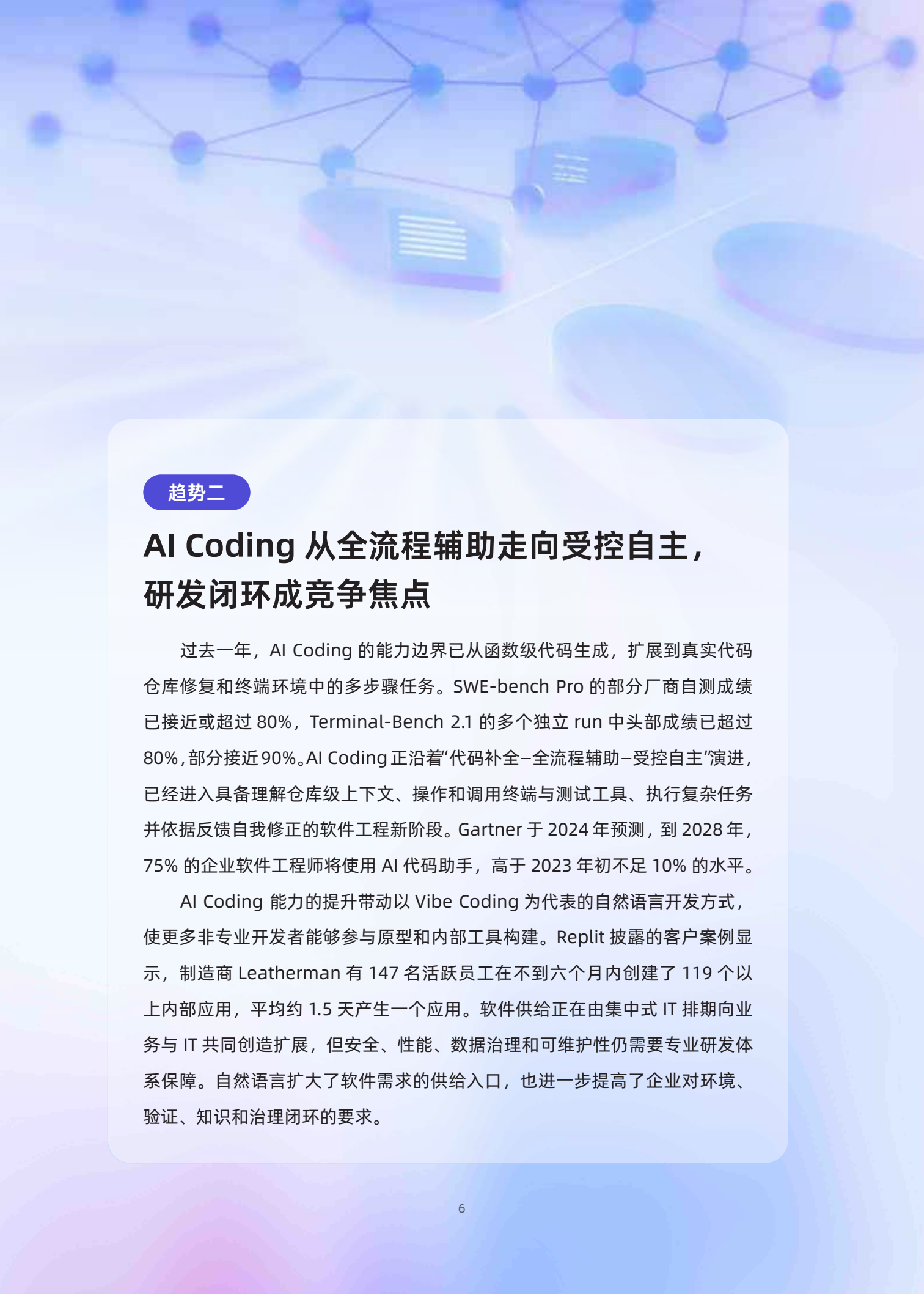
桌面智能体已深入办公流程,成为个人执行长程任务的重要主体。桌面智能体在授权范围内读取文件、操作浏览器与办公软件、调用云端服务,持续推进数据分析、信息搜集、报告生成和流程办理等多步骤任务。Gartner 预计,2026 年 40% 的企业应用将集成任务型 AI 智能体,2025 年这一比例不足 5%。国内,千问办公于 2026 年 8 月开启公测,整合 QoderWork、MuleRun、悟空三款产品,覆盖网页端、桌面端和钉钉入口;国际方面,OpenAI 于 2026 年 7 月发布 ChatGPT Work,支持跨应用取数与数小时级连续作业。企业办公正形成以任务交付为核心的智能体应用模式,竞争的焦点已从模型能力转向任务成功率与单位任务成本。

多智能体协同已成常态,共同参与项目网络。在同一项目中,多智能体混编协作正成为现实:桌面 Agent 处理本地数据与文档,云端 Agent 承担长周期任务的重型计算,协同 Agent 在群聊与项目空间中分派任务、同步进度,人类员工则聚焦目标设定与关键决策。智能体可进入频道、会议和项目空间,在授权范围内调用对话、文档和会议记录,接受团队成员委派,跟踪任务并汇报进展。例如,国内千问办公已接入钉钉工作台,支持以自然语言完成文件创建、群组对话摘要、日程安排等操作。在千问办公之外,阿里巴巴上线“万有无界”,定位为人与 Agent 协作平台,可搭建由多名数字员工组成的协作小组,围绕完整项目共同推进任务,即复杂任务被拆解给多位不同职责的 Agent,在项目空间内组织成员和资产,通过群聊让多位 Agent 接力推进。国际方面,Microsoft Teams 的 Channel Agent 可基于频道消息、SharePoint 文件和会议内容生成项目状态报告、识别期限并分配任务。

组织知识开始以技能资产的形式沉淀和复用。企业正在将岗位流程、领域知识和最佳实践转化为智能体可调用的技能,同时建立身份、权限、日志、审计和人工确认等治理机制。千问办公推出的组织级 Skill,将个人解决问题的路径、调试代码的经验、项目复盘的方法封装为结构化、可检索、可复用的技能项;一家 20 人规模的律师事务所,资深律师完成首份并购尽调报告后将其一键沉淀为组织级 Skill 向全团队共享,新入职员工调用该 Skill 即可产出同类报告,无需逐项请教。Microsoft Agent 365 于 2026 年 5 月正式发布,提供智能体登记、访问控制、风险监测和生命周期管理。当这些技能在组织内被便捷发现和调用时,核心能力不再仅依赖顶尖人才个体,而开始依托一个不断生长、

可组合的技能知识库。长程任务的可靠性、项目协同的深度、组织知识的复用能力和治理水平，正在成为评估企业办公智能体的核心维度。

企业应用上，以 Harvey 为例，其自建了云端 Agent 平台 Spectre，将内部代码仓库、工具链、权限体系、产物、评审维度与执行历史统一纳入同一框架，使 Agent 的工作变为组织可理解、可改进、可协调的系统。产品经理与设计师也能围绕同一批可审阅的产物参与协作。人类分析师的批注会沉淀为 Agent 记忆，使领域知识持续积累。人机分工上，Harvey 确立了“Agent 负责执行，律师负责治理目标与审核”的原则，并将流程拆解为计划、检索、执行、交付、审核五个可见且可审计的阶段，律师必须审核全部 Agent 输出。截至 2026 年 3 月，客户在 Harvey 上运行的自定义 Agent 超过 2.5 万个，官方口径日均 Agent 任务超过 70 万次。



趋势二

AI Coding 从全流程辅助走向受控自主， 研发闭环成竞争焦点

过去一年，AI Coding 的能力边界已从函数级代码生成，扩展到真实代码仓库修复和终端环境中的多步骤任务。SWE-bench Pro 的部分厂商自测成绩已接近或超过 80%，Terminal-Bench 2.1 的多个独立 run 中头部成绩已超过 80%，部分接近 90%。AI Coding 正沿着“代码补全-全流程辅助-受控自主”演进，已经进入具备理解仓库级上下文、操作和调用终端与测试工具、执行复杂任务并依据反馈自我修正的软件工程新阶段。Gartner 于 2024 年预测，到 2028 年，75% 的企业软件工程师将使用 AI 代码助手，高于 2023 年初不足 10% 的水平。

AI Coding 能力的提升带动以 Vibe Coding 为代表的自然语言开发方式，使更多非专业开发者能够参与原型和内部工具构建。Replit 披露的客户案例显示，制造商 Leatherman 有 147 名活跃员工在不到六个月内创建了 119 个以上内部应用，平均约 1.5 天产生一个应用。软件供给正在由集中式 IT 排期向业务与 IT 共同创造扩展，但安全、性能、数据治理和可维护性仍需要专业研发体系保障。自然语言扩大了软件需求的供给入口，也进一步提高了企业对环境、验证、知识和治理闭环的要求。

AI Coding 已经渗透研发的全生命周期, 呈“中间强、两端弱”格局。AI 已经进入需求澄清、技术方案、任务拆解、代码生成、测试调试、代码评审、发布和运维排障等环节。然而, 其能力分布并不均衡: 需求与方案环节可辅助整理信息、生成文档和拆解任务, 但对业务目标、隐含约束和优先级的判断仍依赖人工判断; 编码、测试和调试的工具链最为成熟, 已能够形成相对连续的执行闭环; 发布与运维环节虽开始接入智能体, 但受限于生产权限、环境差异、系统风险和责任边界, 仍以辅助执行和人工确认居多。微软一项覆盖 484 名软件工程师的研究显示, 编码 (Coding) 约占实际工作时间的 11%; 研发时间还分布在设计、调试、评审、沟通和运维等环节。因此, 代码生成能力的提升并不能完全提升研发的效率。

AI Coding 的价值重心将从代码生成转向验证与交付。AI Coding 的竞争焦点将从模型生成能力转向企业研发闭环。这需要在三个层面实现突破: **首先, 需要把研发环境改造成智能体可调用、可验证的执行系统。**代码仓库、依赖安装、构建服务、测试数据、接口、浏览器、日志、调用链、监控和发布平台, 都需要向智能体提供标准化工具。只有能够进入真实环境, 智能体才能把代码修改与系统运行结果连接起来, 形成“执行-反馈-修正”的循环。工作流的作用也将从规定每一步如何执行, 转向任务调度、权限控制、状态保存、审计追踪和高风险操作拦截。智能体负责持续执行, 环境负责提供反馈, 人工保留关键决策与责任边界。**其次, 建立与智能体迭代速度匹配的分层验证体系。**编译、类型检查、静态分析和单元测试提供秒级反馈, 支撑高频修正; 集成测试、契约测试、浏览器自动化和安全扫描提供分钟级反馈, 验证更完整的系统行为; 业务价值、用户体验、伦理判断和生产发布继续由人工确认。验证体系越完整, 智能体能够自主承担的任务越长。企业之间的研发效率差距, 也将更多取决于能否把正确性转化为机器可执行的检查。**三是把知识和规格转化为智能体可检索、可执行的约束。**业务规则、接口语义、历史决策和故障经验, 需要从分散文档沉淀为可检索、可调用的知识与技能。规格说明则需要区分约束与假设: 数据不能出域、接口必须向后兼容、延迟不得超过阈值, 属于需要持续检查的约束; 采用何种架构和缓存策略, 则属于可以根据运行反馈调整的假设。规格负责界定什么算正确, 智能体负责在约束内寻找实现路径。

AI Coding 是企业智能化的关键引擎, 但决定其价值的不是代码产量, 而是需求转化为数字能力的速度、质量和稳定性。AI Coding 的竞争焦点将从模型生成能力转向企业研

发闭环。当代码生成、环境执行、自动验证、知识调用和权限治理形成闭环，智能体才能承担更长周期的软件工程任务。企业研发竞争力将主要取决于问题定义的精度、场景洞察的深度、可执行规格的清晰度，以及机器可验证反馈体系的完备性。

趋势三

数字员工规模化落地， 人机协同重构组织基本单元

当智能体能力与业务流程深度结合，数字员工开始规模化进入企业。以智能体为核心的数字员工已广泛嵌入客服、财务、营销、研发支撑、HR 等多元业务场景：既能独立完成标准化工作，也能组建多角色虚拟团队协同推进复杂任务，例如自动搭建包含视觉设计、市场研究、媒介专家的虚拟团队完成营销全案，或在 HR 场景中闭环完成从职位发布、简历筛选到面试安排的全流程，能端到端完成代码交付、独立值守凌晨告警等。本报告对 1000 余位受访者的调研显示，20% 的受访者所在组织已规模化部署数字员工，42% 已在部分部门和岗位试点部署。数字员工正从试点验证阶段进入规模部署阶段。

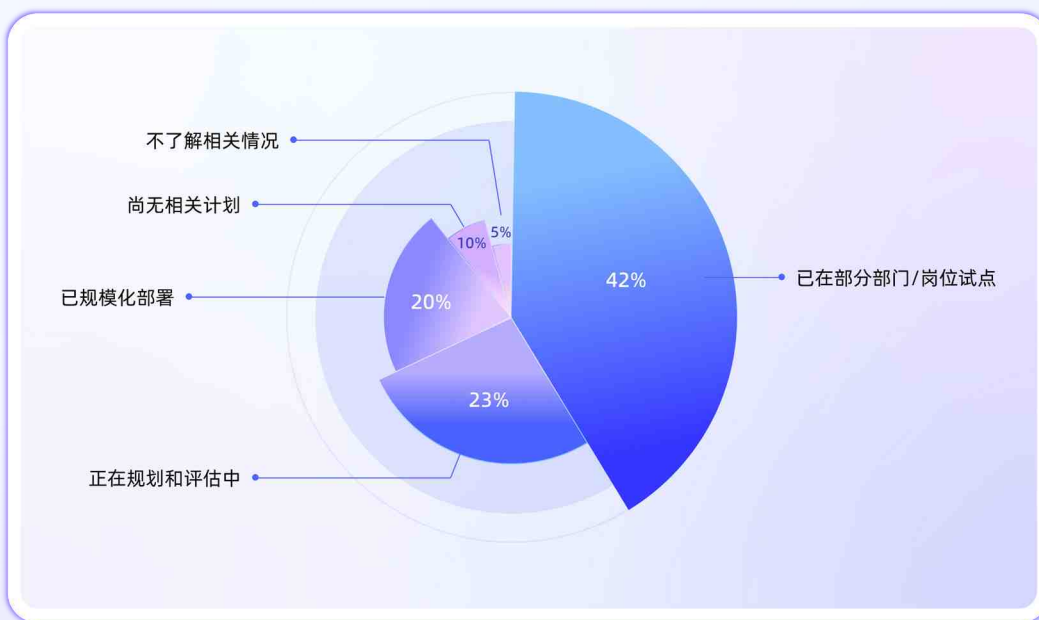


图 1 所调研企业数字员工引入情况
数据来源：阿里云研究院调查问卷

数字员工开始以组织可管理的智能单元形态进入企业。数字员工是 Agent 能力底座和组织治理身份相结合所形成的新型组织可管理单元，是组织编制内可被分配工作、可被评估绩效、可被优化或汰换的 AI 业务实体。组织治理身份，是数字员工区别于其他 AI 形态的本质特征，也是它进入企业权限体系、业务流程与管理框架的必要前提。前沿企业已经开始围绕身份、Agent、作业、管理等维度构建面向数字员工全生命周期的管理体系。一位数字员工创建后，获得独立的 AI 工号，拥有完整的组织归属（主管、部门、汇报线），以独立身份在业务 workflow 中开展作业，并被纳入从申请、上岗、过程管理到评估、优化 / 汰换的全生命周期管理，运行状态、成本与产出也将被组织统一度量。如阿里云已经落地了各类 AI 数字员工，覆盖了网站、服务、电销、CRM、内容、人事等核心业务场景。



图 2 阿里云数字员工分布

麦肯锡全球研究院在《Agents, robots, and us: Skill partnerships in the age of AI》报告中测算，当前技术条件下智能体理论上可覆盖 44% 的非物理工作时长，机器人可覆盖 13% 的物理工作时长，两者合计 57% 的美国工作时长具备自动化潜力。组织的最小作战单元，正从人变为“人 + 智能体”的组合。

数字员工的发展同步对人才能力结构及流程与协作提出全新要求。AI 对组织结构与工作方式的影响已从讨论层面进入普遍感知阶段。问卷显示 64% 的受访者认为 AI 已进

入日常工作场景，改变了个人与团队完成任务的方式，但多数尚未触及结构层面；18% 选择“明显感受，组织架构 / 工作流程有调整”，即 AI 已开始推动分工、流程或架构层面的实际调整；仅 3% 的受访者表示未感受到任何变化。

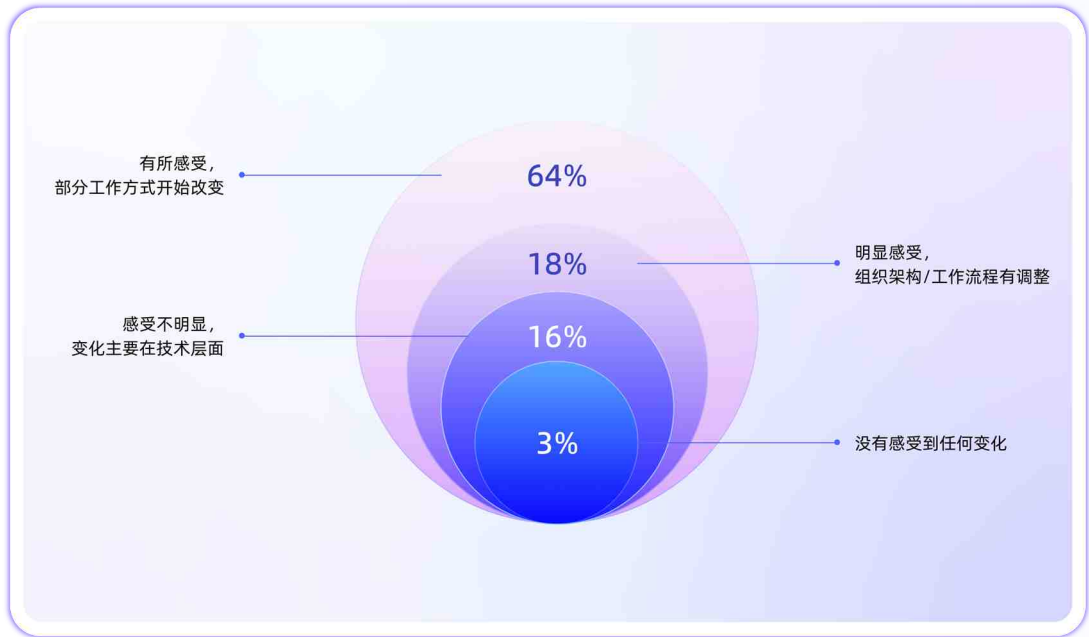


图 3 AI 对组织结构 / 工作方式影响的受访者感知情况
资料来源：阿里云研究院调查问卷

当数字员工加入到业务单元后，人类员工的核心价值转向判断、设计与监督，人才体系随之需要调整。首先是能力的迁移，从专注任务执行转向三类新能力，与 Agent 协同工作的能力，能定义任务、评估产出、处理异常；设计 Agent 工作流的能力，能拆解业务为可编排的 Skill；对 Agent 产出进行专业判断的能力，能识别错误、把控质量。本报告调研中，61% 的受访者认为 AI 时代最重要的是 AI 工具使用能力，50.3% 的受访者认为创造力、批判性思维等非常重要。

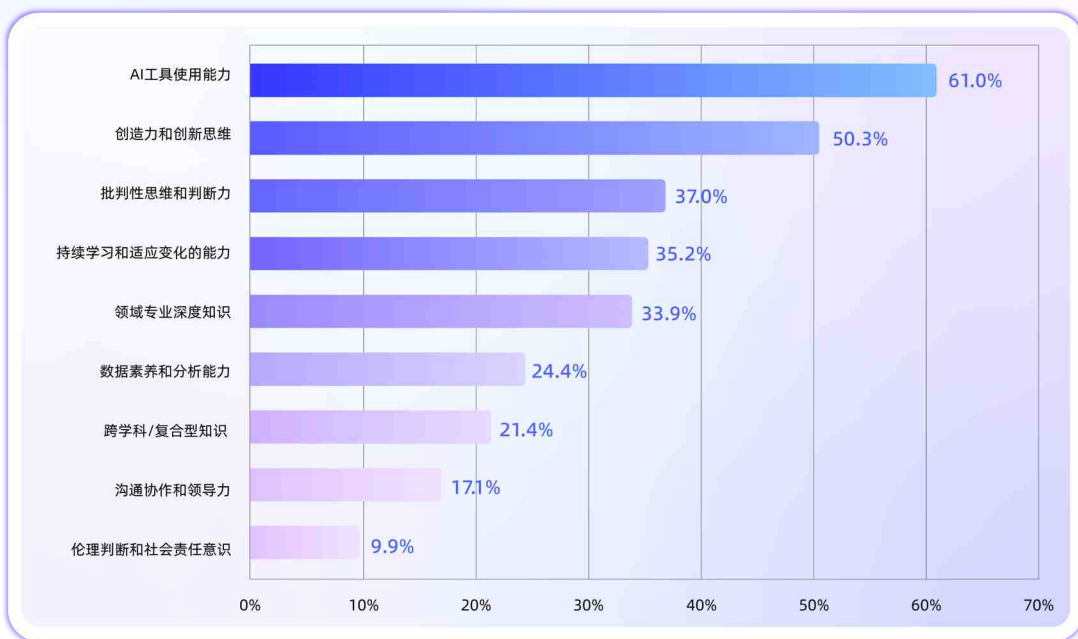


图4 AI时代重要技能要求调研结果
资料来源：阿里云研究院调查问卷



图5 AI时代劳动力技能分类
资料来源：阿里云研究院整理，Gartner

组织也需要将既有以人驱动、串行流转的业务流程，调整为人机协同、任务编排的运作方式。企业需围绕高频、标准化、可拆解的环节，重新定义触发条件、分工边界、审批节点与异常回退机制，使数字员工承担信息检索、初步判断、跨系统执行与状态跟踪等工作，人则聚焦例外处理、关键决策与结果校验。流程优化不只是局部提效，更应推动跨部门协同从依赖个人沟通转向依赖流程与规则，减少重复传递与信息损耗。



趋势四

超级个体加速涌现，AI 放大个体能力边界

当办公智能体、AI Coding 与数字员工的能力叠加到个人身上，个体的能力边界被系统性放大。组织的规模不再是能力的前提，个体的判断力、创造力与资源整合能力，借助智能体被成倍放大。超级个体由此加速涌现。全球所有权管理平台 Carta 数据显示，单一创始人公司在新增创业公司中的占比从 2019 年的 23.7% 攀升至 2025 年上半年的 36.3%，2025 年全年维持在约 36% 的水平。美国人口普查局数据显示，美国约有 3043 万个非雇主经营单位，合计营收约 1.75 万亿美元；非雇主经营单位数约占全部经营单位的 78.4%。国内方面，中关村人才协会发布的《中国 OPC 发展趋势报告（2025-2030 年）》显示，截至 2025 年 6 月全国一人有限责任公司已突破 1600 万家，2025 年上半年新注册 OPC 达 286 万户，同比增长 47%，占全部新注册企业的 23.8%，显著高于整体企业注册增速。OPC 正在成为创业领域的重要增长极。

OPC 先锋企业以极简组织形态开始跑通商业闭环。今年年初 OpenClaw 迅速推动一批 OPC 创业热潮，但经过近一年的市场筛选，缺少真实商业场景的 OPC 开始退出市场，而精准切中长尾场景痛点、构建可持续获客与留存机制的企业则逐步进入盈利周期。例如，某杭州创业者为中小电商企业提供从市场分析、广告文案、视觉设计到客服回复的全流程 AI 营销服务，上线 4 个月用户突破 1.5 万。某 AI 导演智能体开发团队在 OPC 模式下大幅降低视频制作门槛，近一个月活跃用户上涨 25 倍。某 AI 桌面机器人项目以 1 人团队独立开发，深度接入大模型平台实现 0.5 秒多模态语音交互，将具身智能从百万级人形降维至桌面百元级，跑通“开源硬件 + 社区 + 商业出货”完整闭环。某生成式 AI 心理健康 B2B2C 平台面向国内 2.8 亿心理支持需求人群，打通 AI 筛查、AI-CBT 干预、家校科普到专业转介的分层服务链路，已落地多所高校及知名企业 EAP 项目。但需客观指出，当前 OPC 商业闭环仍处于早期验证阶段，当前已验证闭环的 OPC 多集中于轻资产、高智力、新业态领域，覆盖商业顾问、视觉设计、跨国电商等垂直场景。

政策与平台生态正加速推动 OPC 进入制度化发展阶段。各地专项政策密集落地，据公开信息，已有 23 个省（市 / 区）从省级、市级到区级、开发区等不同层面发布 OPC 培育实施方案或社区支持举措，形成覆盖算力补贴、模型语料、办公空间、注册便利、创业资金、信贷融资、场景开放、人才安居等八大类通用支持工具。在此基础上，部分地区的制度设计更具突破性——涉及人才评价标准、风险容忍机制、要素券形态、市场准入及监管方式等维度，其共同特征是不再沿袭传统扶持逻辑，而是着手修订与 OPC 这一新型主体不相适配的既有规则，因而具备较强的示范与借鉴价值。

与此同时，围绕 OPC 群体的生态社区、知识平台与协作网络也在加速构建。据 OPC 圈全国社区库统计，截至 2026 年 8 月，全国已投入运营或公开挂牌的 OPC 社区共 826 个，覆盖 28 个省级行政区、95 个城市。覆盖法律合规、自动化财税、风险保障及 AI 工具集成等全场景的专业支撑体系亦逐步成型，推动 OPC 生态持续走向成熟。

现实挑战与路径建议

AI 驱动的企业进化，本质上是围绕运行机制、人才体系、组织形态的系统性重构，其核心目标是实现人机价值共生，但这一进程面临多重挑战。本报告调研显示，在数字员工规模化落地过程中，58.6% 的受访者担忧人机协作的权责边界不清、易引发问责难题，55.6% 担心部分岗位被替代导致结构性失业，对工作失误、商业泄密、管理滞后的担忧同样普遍。归纳而言，企业正面临技能适配、文化协同、责任界定、技术落地四大核心挑战。

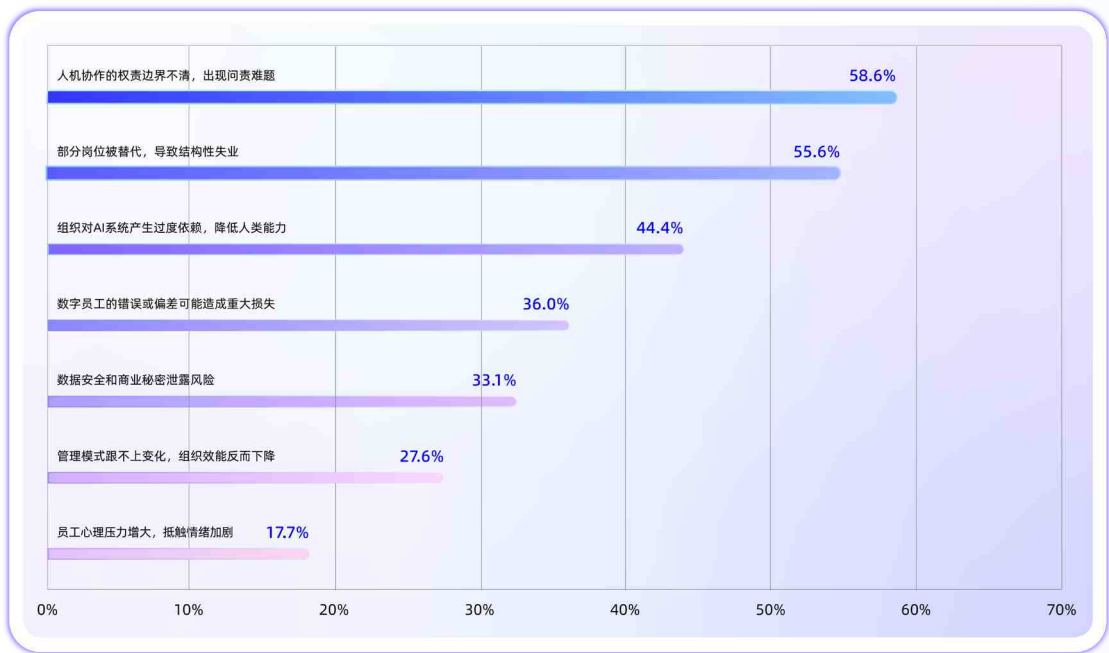


图 6 数字员工规模化落地的主要担忧
数据来源：阿里云研究院调查问卷

首要挑战是员工技能重塑与适配压力。当前多数员工仍停留在工具使用思维，难以进行高效的人机协同；传统岗位员工面临被替代风险，新型复合人才供给存在缺口，员工普遍存在 AI 焦虑，技能转型阵痛制约人机协同效能的释放。**其次是组织文化与新型形态的适配难题。**液态组织与弹性规模要求开放、容错、自主的文化氛围，与传统层级制的管控型文化形成冲突，部分企业即便引入 AI 技术，仍难以打破部门壁垒、推动动态重组。**再者是人机责任边界模糊的伦理与法律困境。**AI 自主决策引发的失误，如营销内容侵权、风控判断偏差，责任主体难以界定，现有法律与监管体系滞后于技术发展。**最后是技术落地的适配性问题。**不同行业与规模的组织 AI 基础差异较大，大中型组织面临跨系统协同壁垒，部分企业盲目跟风部署，导致技术与业务脱节、无法形成价值闭环。

破解上述难题，需在四个层面落到实处。第一，建立阶梯式 AI 技能体系，将 AI 协作能力嵌入岗位胜任力模型，培养人机混编团队的调度和异常判断能力。第二，以试点单元驱动组织文化转型，选取 1 至 2 个业务单元作为试验田，简化审批流程、允许快速迭代，用可量化的产出替代抽象的文化倡导。第三，建立人机权责的分级确认机制，为合规预留空间。按照决策影响程度进行分级，每级对应明确的日志要求、回滚机制与责任归属。第四，结合企业规模和技术能力确定适合自身的落地路径。大型企业重点解决跨系统打通，以统一的 Agent 平台整合核心系统的 API，建立企业级权限与数据治理层；中型企业从高频重复场景切入，优先部署标准化程度高、ROI 可快速验证的数字员工；小微企业和 OPC 创业者则依托云端 AI 办公平台获得开箱即用的能力，无需自建基础设施，以月度订阅成本换取生产力杠杆。

2

产业智变，
从效率提升到价值创造

人工智能正在产业领域引发一场深层次变革，不仅仅是针对存量流程优化的效率提升，更是通过新产品创造、新模式创新来产生增量价值，从而推动新质生产力的加速形成。在智能化转型方面，企业整体上围绕内部提效、能力进化、服务优化和产品创新四大类型应用进行构建，重塑业务价值体系。当前企业已经跨越概念验证和试点探索的阶段，更加关注 ROI 导向的价值评估体系，打破生成式 AI 鸿沟，实现 AI 应用从试点验证转向规模化落地。智能体的加快发展，深度嵌入业务流程，形成“嵌入增强 - 混合协同 - 有限自主”的渐进式革新路径。

基于 2000 份企业用户问卷的调查，13.6% 的企业用户受访者表示其组织已经开始规模化落地 Agent，在多个业务场景深度应用；38% 的受访者表示已有单点应用，在部分场景提供辅助支持。国务院国资委组织的“AI+”专项行动已在能源、制造、通信等 16 个重点行业打造了超过 800 个典型应用场景。在新产业催生方面，AI 原生企业加速崛起，覆盖算力服务、数据服务、隐私计算、MaaS、AI 原生应用等新兴领域，形成“基础设施 - 模型算法 - 数据工程 - 开发平台 - 应用服务”的完整生态链。未来，随着技术迭代与产业协同深化，AI 将加速从效率工具进化为价值创造引擎，持续重塑传统产业形态并拓展数字经济边界。

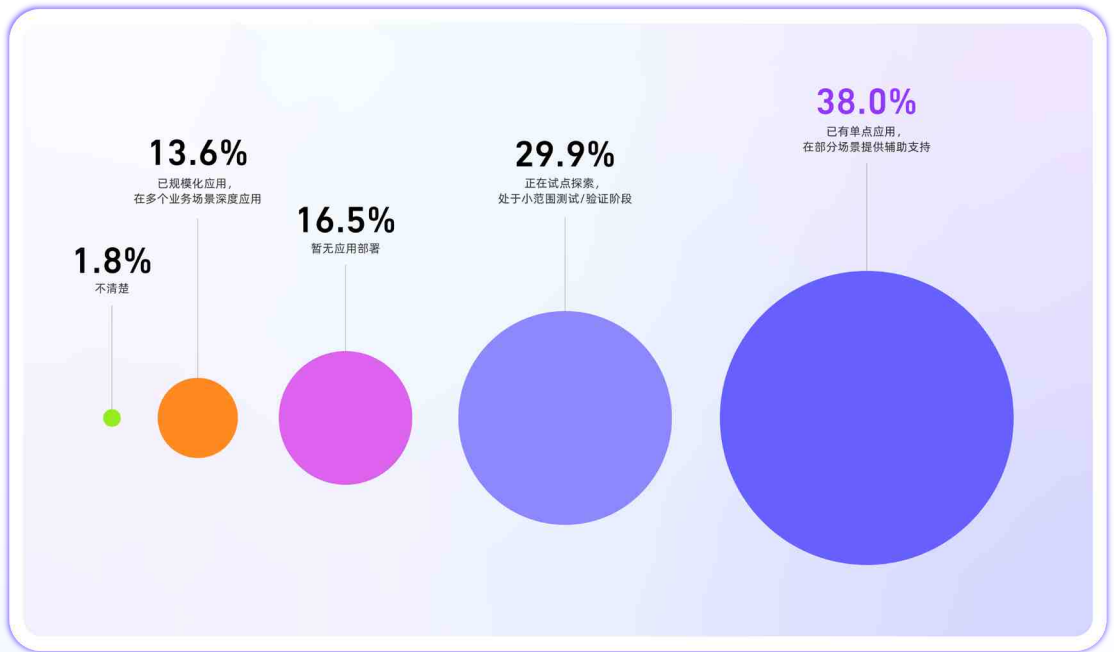


图 7 企业 AI Agent 应用部署情况
数据来源：阿里云研究院调查问卷

趋势一

四大维度全方位重塑企业业务价值体系

AI 在企业中的应用已逐步进入规模化落地阶段。根据麦肯锡全球人工智能现状调查数据，目前全球 78% 以上的企业已布局至少一类 AI 应用场景。AI 应用场景类型多样，从面向对象看，既包含面向内部员工和流程的相关应用，也有面向外部客户和业务市场的场景应用；从 AI 产生的价值来看，既包含通过生产力工具实现效率提升的应用类型，也包含通过创造新产品、新模式实现经营增长的应用类型。从 AI 为企业带来的价值调研结果看，有 71.7% 的受访者认为主要带来运营效率提升，减少人力投入；68.3% 的受访者认为 AI 提高服务质量和相应速度，也有 43.2% 的受访者认为能够推动业务模式创新，助力营收增长，同时也有 39.8% 的受访者认为 AI 强化组织管理决策和业务分析能力。

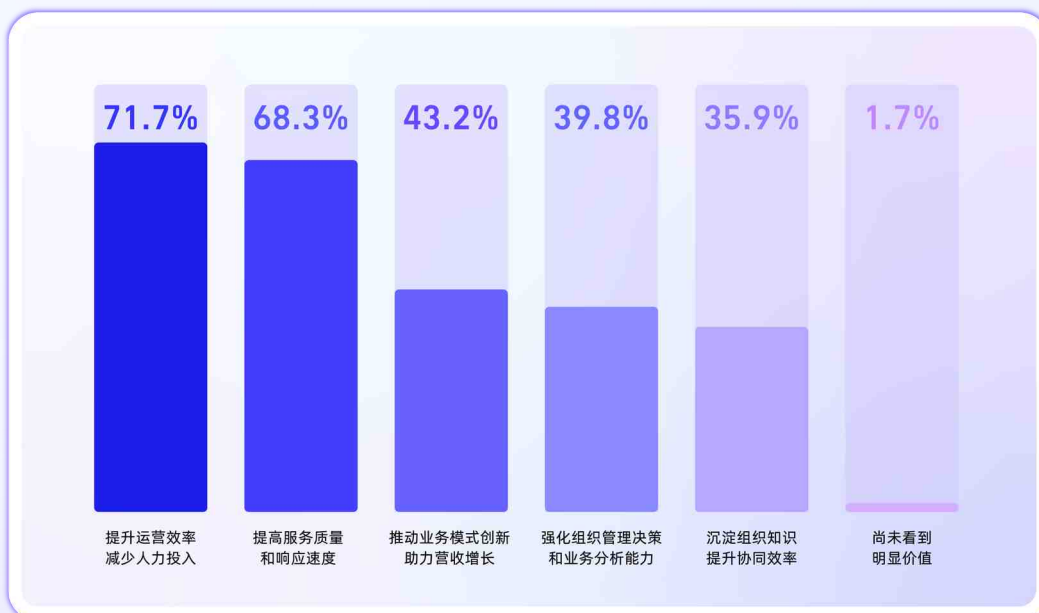


图 8 AI 为企业发展带来的主要价值方向
数据来源：阿里云研究院调查问卷

因此，我们根据应用面向的对象和产生的价值路径两个维度进行划分，构建 AI 应用四象限矩阵：横向维度包括效率提升与创新突破两个方向，代表 AI 应用的不同价值路径；纵向维度包括面向员工 / 流程的内部 AI 应用以及面向客户 / 市场的外部业务应用，代表 AI 应用的不同应用对象。纵横结合形成四个象限，可以总结为：内部提效型、能力进化型、服务优化型和产品创新型。

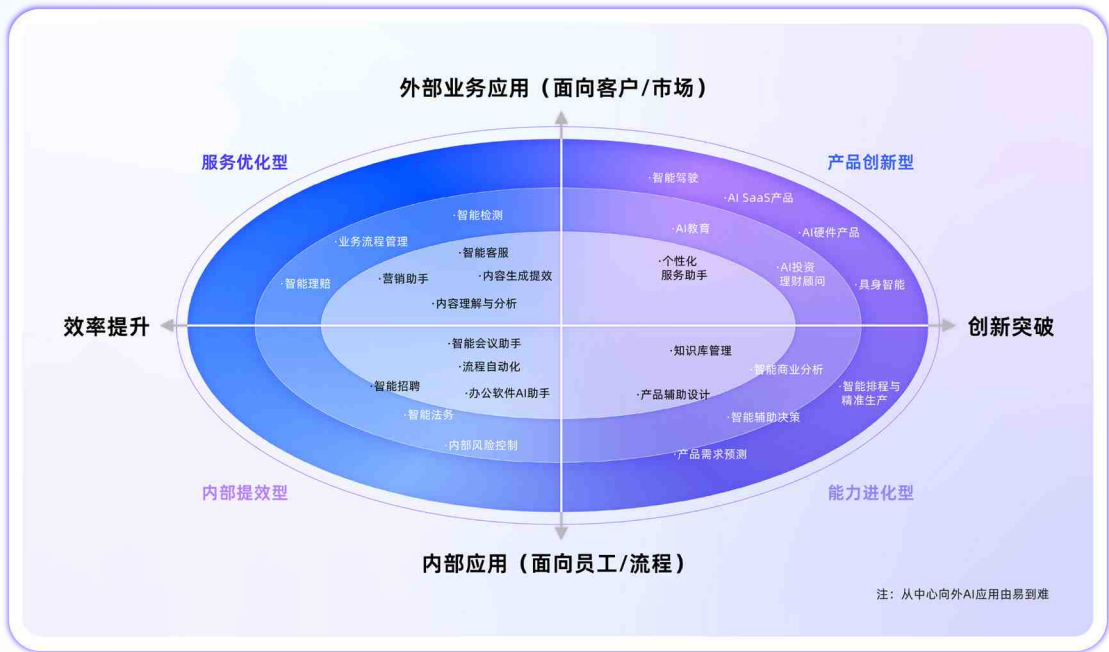


图 9 企业 AI 应用分类及重点场景
资料来源：阿里云研究院绘制

内部提效型 AI 应用，更加侧重企业的内部工作流程优化，提升员工生产力与组织敏捷性，实现降本增效；这类应用不太可能为企业带来市场差异化，但对于以人力资本为主要竞争力的商业服务类企业来说提效显著。典型场景包括内部流程自动化、办公软件 AI 助手、AI 编程助手、智能招聘、智能会议助手、智能法务、内部风险评估控制、安全运维与网络安全等。该类应用场景技术成熟度高，容错率高风险度低，能够快速部署并看到成效，已经成为企业 AI 应用的首要切入场景。从普及现状来看，此类应用是目前企业 AI 布局最广泛、渗透率最高的类型，尤其在互联网、金融、咨询等行业，是企业降本增效的核心抓手。

服务优化型 AI 场景应用，则更加侧重于提升面向客户或合作伙伴的运营流程效率，优化客户服务体验，降低交付成本。这类场景应用主要面向客户、供应商以及相关合作伙伴，通过 AI 改善企业现有业务流程的效率，并通过智能营销、个性化服务等提升客户

服务质量，减少人力成本。典型场景包括智能客服、售后服务、营销助手、智能推荐、个性化广告投放、意图识别与分析、客户业务流程管理、智能理赔等。总体上，销售和服务环节充分体现了大模型在复杂交互中的优势，已经成为企业智能化转型的重点应用方向，从普及现状来看，此类应用普及度仅次于内部提效型，其在零售电商、教育、金融、汽车等行业渗透率高。智能客服已大幅取代传统人工客服成为主流服务模式，个性化推荐、智能理赔等应用也成为企业提升客户满意度、降低服务成本的核心手段，甚至在传统制造业中，也逐步通过 AI 优化伙伴服务流程，提升协同效率。

能力进化型 AI 应用，更加侧重通过 AI 优化内部知识体系沉淀，提升内部创新能力，重构内部决策机制，构建智能化的组织底座，这类应用对于研发创新型及具备复杂业务系统的机构 / 企业至关重要。典型场景包括产品辅助设计、知识库检索和组织学习系统优化、研发辅助、智能商业分析、智能辅助决策、智能排程与精准生产、供应链优化等。此类应用具较强的战略价值，促进企业内部认知能力、分析预测能力和创新能力的提升，实施难度相对较高，价值释放的周期相对较长。目前关注长期创新能力和组织管理重塑的企业已经开始逐步加快能力进化型 AI 应用开发部署。从普及现状来看，此类应用目前仍处于快速渗透期，普及度相对集中在大中型企业和研发密集型行业，其中生物医药、金融科技等行业布局最为积极，通过智能排程、研发辅助等应用提升核心竞争力，而中小企业受技术、资金限制，此类应用的布局相对滞后，多以轻量化的知识库检索、基础商业分析为主。

产品创新型 AI 应用，更加侧重在通过 AI 驱动新产品、新服务和新商业模式，构建差异化的企业市场竞争力，提升创造力，这对面向消费者侧的企业意义重大。典型场景包括 AI 原生应用及产品开发，如 AI 搜索、AI 招聘匹配平台、AI 设计产品、AI 创作产品；内嵌 AI 功能的智能硬件产品如 AI 电脑、AI 音箱、AI 眼镜、AI 手机、AI 机器人等；个性化服务助手如 AI 健身顾问、AI 营养师、AI 旅行规划师、AI 医疗顾问等。此类应用投入周期长，成功后回报上限最高，但失败风险也大。但对于企业来说，一旦成功，则战略意义重大，能够重新定义企业的市场定位和竞争优势。目前，市场上已经涌现出大量产品创新型 AI 应用，形成蓬勃的市场。从普及现状来看，此类应用呈现“头部引领、百花齐放”的格局，互联网科技企业主导 AI 原生产品的研发与普及，AI 创作、AI 搜索等应用已广泛渗透到消费者生活和企业经营中，而传统企业则多通过内嵌 AI 功能实现产品

升级，如 AI 手机、智能家电等，同时，细分领域的 AI 创新产品不断涌现，成为中小企业突破市场竞争的重要路径。

针对企业 Agent 开发的典型应用场景调研可以看到,在已开展 Agent 应用的组织中,近一半已将其应用于落地了客户服务的场景，知识管理、营销与销售、人力资源、数据分析与决策以及研发支持等目前在第二梯队的应用场景。因此从短期来看，AI 通过内部提效、服务优化，帮助企业压缩运营成本、提升响应速度，快速应对市场变化，筑牢经营根基；从中长期来看，AI 通过能力进化、产品创新，帮助企业优化知识体系、突破创新瓶颈,构建差异化的市场竞争力。更深远的是, AI 正在重塑企业的组织架构和发展逻辑，让企业在数字化智能化浪潮中保持核心竞争力，实现业务价值、品牌价值、社会价值的多重提升，为企业的长远发展注入源源不断的智能动力。

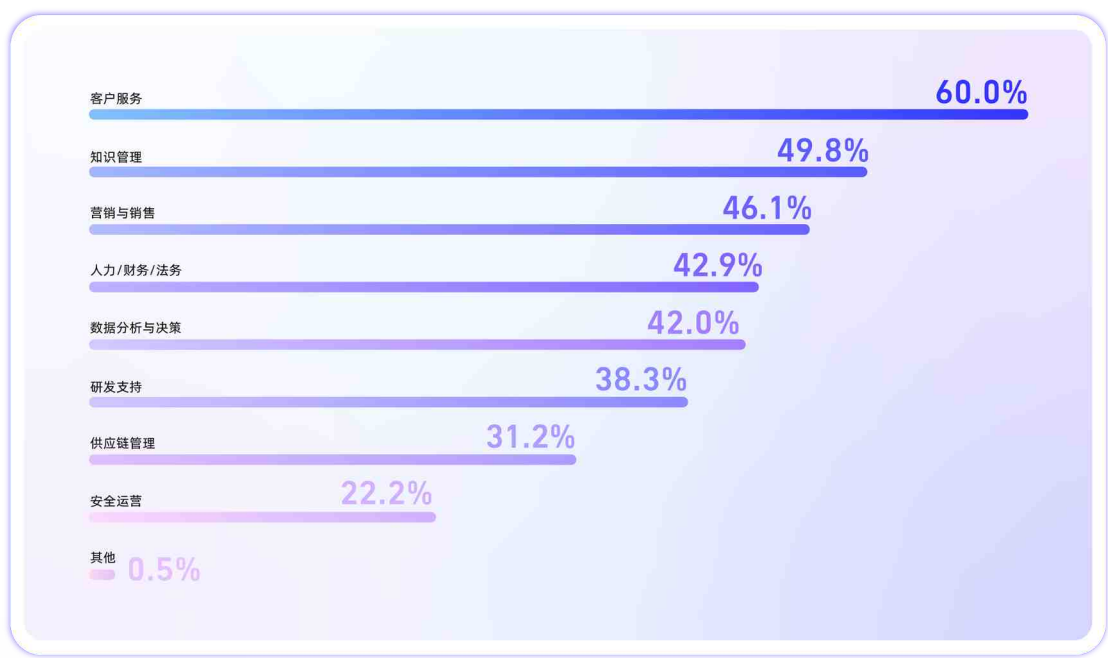


图 10 企业 Agent 应用场景分布调查结果
数据来源：阿里云研究院调查问卷



趋势二

垂直领域智能体深度嵌入企业核心业务流程

智能体技术的成熟，标志着 AI 从效率工具向业务协作者的稳步过渡。相较于早期 RPA 对固定流程的机械执行，新一代行业智能体通过“感知-推理-决策-执行”的闭环能力，在特定业务场景中承担起辅助乃至协同任务。当前产业实践更倾向于以“流程自治度”与“人机协同模式”为维度理解智能体应用形态：一端是深度嵌入现有系统的增强型智能体，聚焦部分环节的智能增强，如构建新型交互界面或者在内容生成、材料审核判别等环节进行大模型介入；中间是混合协同型智能体，在非核心环节赋予有限自主权，关键节点保留人工介入；另一端则是高自主性智能体，在规则清晰、环境封闭、风险可控的特定场景中开展探索性试点。目前，企业内部的智能体应用大部分以嵌入式增强为主导，这既源于企业对渐进式改造的务实选择，也契合当前技术成熟度与行业监管要求；混合协同模式随模型能力提升快速成长；而具备端到端自主执行能力的智能体，仍处于前沿探索阶段，规模化落地尚需时日。

嵌入式增强型智能体，作为当前主流形态，主要对现有的企业应用进行轻量级改造，**将 AI 能力引入关键业务环节**。其核心逻辑不是重构系统，而是通过 API 与业务系统深度耦合，在用户界面层提供自然语言交互与操作指引，在逻辑层辅助信息综合，但最终决策权完全在人。头部机构普遍把智能体先用于员工侧（研发 / 客服坐席 / 运营 / 合规），以降低风险；对客侧聚焦可监督的“可办理服务 + 强校验”，逐步引入 workflow 自动化。例如某保险集团通过构建适配集团公司全域的智能安全运营体系，将智能体深度嵌入资产漏洞管理、降噪分诊、威胁研判、响应处置、溯源遏制等安全运营全场景，以此全面提升全系统威胁检测精度、响应速度与协同效率，降低安全运营成本。又如，医疗临床决策支持助手，一般嵌入到医院现有系统中，实时分析患者数据并关联最新临床指南，为医生提供诊疗参考，但在全过程中医生始终保持终审权，智能体仅作为知识助手，在严格监管框架下实现技术赋能与合规落地的平衡。

混合协同型智能体作为人机分工优化的关键形态，正随技术平台成熟加速落地。其核心在于动态权责分配，在数据敏感、责任重大的核心节点（如贷款终审、政策合规判定等）通过流程设置由专业人员进行决策；在信息核验、进度跟踪、建议生成等辅助环节，则赋予智能体有限自主执行能力，减少人工全程介入。例如阿里云支持某航空公司打造行业领域大模型落地核心应用，包括飞机故障智能处理，实现从预警、定位到处置的全链路支持；航班运行风险雷达，可视化预警航班风险等。又如，某家电企业研发的机器人智能体，能够在工厂大脑的统一调度下，与品质、DMS（日常化管理）、TPM（全员生产维护）、EHS（环境、职业健康与安全管理）等工厂智能体深度协同，结合多模态感知技术和具身智能操作技术，可以自主执行品质首检、DMS 巡回会议、TPM 巡检、EHS 巡检等高频次任务，实现实时响应与全流程自主决策。多式联运物流系统中，多个智能体分别负责路径规划、资源调度、风险评估等环节，人类员工负责决策与监督，形成闭环决策。

从各垂直行业的企业 Agent 应用看，成熟度呈现较为明显的分化特征。

成熟度相对较高的行业具备几个共性：数字化基础设施完善、面向终端消费者、数据积累丰富、合规风险可控。互联网、零售消费、文化传媒等属于这一梯队。互联网的搜索问答、商品推荐、广告推送、智能客服等场景已成熟落地；零售消费的智慧门店、供应链管理、用户行为分析等进入规模推广。这些行业的共同特点是 AI 替代的是标准化、高频、低风险环节，ROI 可量化。

成熟度相对较低的行业则受制于三类约束：一是专业门槛高，核心场景需要领域知识深度参与，如医药健康的药物研发、手术机器人，教育科研的科研成果创新、学生培养；二是合规与数据安全要求严格，医疗数据、企业内部数据的可用性受限；三是 B2B 链路复杂、决策链长的场景等仍处试点验证。

从演进脉络看，智能体应用正沿着“嵌入增强→混合协同→有限自主”的务实路径稳步推进。这一进程受多种因素影响：**技术层面**需持续优化大模型推理稳定性与工具调用精准度；**工程化层面**需企业在数据治理、知识工程领域加强投入，将行业隐性知识（如风控逻辑、诊疗经验、安全策略）和专家经验系统转化为规则与模型，提升智能体执行精度；**业务层面**，企业需要厘清场景价值逻辑，让智能体真正服务于业务发展，形成可衡量的业务价值。

随着智能体在垂直领域的深度扎根，企业竞争将逐步从依赖个体专家经验，转向构建可迭代、可复用的组织级知识体系；业务流程从刚性执行，转向具备环境感知与动态调优的柔性系统。最终，智能体将推动产业价值链条从单点效率优化，迈向全链路知识驱动与价值重构，但这一进程需以场景真实性、效果可验证性、风险可控性为基石，在务实探索中稳步前行。

趋势三

ROI 导向的价值评估体系加速建立，AI 投入进入精细化核算

麻省理工学院（MIT）发布的《生成式人工智能鸿沟：2025 年企业 AI 现状》研究报告显示：在全球 300 个公开的 AI 实施案例中，仅有 5% 的试点项目成功实现规模化并创造了可衡量的价值。这种高采用率与低价值转化的反差，被称为“生成式人工智能鸿沟”。随着 Agent 的逐步规模化落地，企业越来越关注 AI 应用的商业价值评估，避免落入为了技术而技术的怪圈。

AI 应用价值生成本质是数据、算法与业务场景持续动态适配的协同过程，其价值的实现与业务场景深度绑定，呈现出多元复合的特征：既包含成本节约、效率提升、营收增长等可量化的财务指标，更蕴含于数据资产沉淀、决策质量迭代、组织能力升级、创新能力提升等难以直接度量的长期战略维度。这类战略收益的转化存在明显滞后性，要求企业适当容忍价值兑现的间接性与长期性。此外，不同应用场景的价值衡量标准也需要进行差异化设计。因此，企业亟需构建一套全新的评估体系，既能精准捕捉 AI 的独特价值，又能适配业务战略，为 AI 应用提供全生命周期的动态引导。

针对 AI 价值生成的特征，企业需跳出传统静态评估框架的桎梏，构建“财务回报率（ROI，Return on Investment）+ 未来回报率（ROF，Return on Future）”的协同体系，以全周期 ROI 锚定短期落地价值，用 ROF 衡量长期战略壁垒，通过动态权重调整与全流程管控，实现短期收益与长期竞争的平衡，破解 AI 项目“试点易、规模化难”的困境。

在短期商业价值方面，通过全周期动态 ROI 拆解全周期成本结构、整合多维收益来源进行核算，适配 AI 价值释放规律。AI 项目的可量化财务收益，主要集中在生产力效益、运营效率、客户价值关联及产品业务增长四大维度。多数项目通过节省人力投入、缩短流程时间、提升客户转化率与留存率，或依托新产品、新模式创收实现价值兑现。企业需将这些可观测指标转化为直接财务收益，例如通过“每位员工节省工时 × 员工人数 × 平均时薪”核算生产力效益，通过“(原流程单位成本 - 智能流程单位成本) × 年度业务量”核算流程成本节约，确保收益衡量的精准性与可操作性。成本需综合考虑总拥有成本即 TCO，包括聚焦数据与算力的基础层成本，涵盖模型调优、应用程序开发、跨系统集成及部署等的开发层成本；以及包括应用评估、监控、漂移修正与合规维护等的运维层成本，以及全流程投入的人力投入成本。

产品创新型与能力进化型 AI 应用，通过创造新产品、开拓新市场，或重塑内部核心流程与创新能力，构建未来竞争优势。这类投资属于长期战略押注，在执行细节、成本结构与价值结构上均存在不确定性，短期内难以产生显性经济效益，传统确定性 ROI 分析方法不完全适用。Gartner 提出的未来回报率（ROF），突破短期财务导向的局限，聚焦 AI 构建的不可复制的竞争优势，成为价值衡量的重要补充。ROF 的核算需满足两大核心要求：一是给予 3-5 年以上的长周期考量，匹配战略价值的兑现节奏；二是围绕核心能力维度构建核算逻辑，包括创新能力提升价值、数据资产增值及市场竞争领先度等。

双维评估体系的落地，关键在于“全生命周期管控 + 动态权重适配”的协同运作。AI 项目启动阶段，需明确核心目标并设定初始权重，提效型项目侧重 ROI，创新型项目强化 ROF 占比；试点阶段，同步追踪 ROI 核心指标与 ROF 过程指标，及时优化成本结构与战略方向；规模化阶段，动态调整权重，提效型项目逐步降低 ROF 占比，创新型项目持续强化 ROF 监控；迭代阶段，结合双维指标复盘，优化模型与流程，形成价值闭环。此外，建立差异化指标库，针对不同类型、不同场景的 AI 项目，设定专属核算标准与评估周期。通过双维体系的协同运作，企业既能规避预算超支、价值转化断层等风险，又能筑牢长期竞争壁垒，最终实现 AI 价值的最大化释放。

针对不同的应用类型，需要进一步细化指标体系，进行差异化评估。内部提效型场

景应用评估指标选择需围绕流程效率与成本优化，核心包括流程自动化率、人力成本减少率、任务处理时间缩短率、错误率降低幅度等，同时跟踪数据资产复用率为 ROF 积累基础。落地策略应优先选择标准化程度高、重复劳动密集的场景，无需大规模组织变革，待 ROI 达标后再复制推广，通过业务数据直接量化价值，快速形成评估闭环。能力进化型评估指标需聚焦战略价值与组织能力提升，核心指标包括决策响应速度提升率、知识资产增长率、创新项目孵化进度、跨部门协作效率改善度、组织学习效率提升率、数据共享程度等。落地需联动业务与研发团队，优化决策流程与知识沉淀机制，按季度滚动评估 ROF 核心指标，不追求短期 ROI 达标。通过建立数据壁垒与创新复用体系，逐步释放战略价值，实现 ROF 向长期 ROI 的转化。服务优化型应用评估指标需兼顾运营效率与客户价值，核心包括客户满意度（CSAT）、净推荐值（NPS）、服务响应时间缩短率、问题自动解决率、客户留存率提升幅度，同时关联营收增长、获客成本降低等财务指标。落地需以客户需求为核心，通过反馈数据反向校准服务质量，避免过度追求效率牺牲体验，同时沉淀外部数据资产，强化数据壁垒，实现短期营收增长与长期客户资产积累的双向赋能。产品创新型应用评估指标需聚焦战略突破与市场价值，核心包括产品功能独特性评分、市场份额增长率、新业务收入占比、用户增长率、数据飞轮效应（数据量月增长率）等。落地需前期充分开展市场调研与技术验证，小范围试点后规模化推广，通过数据飞轮效应迭代模型，逐步提升长期 ROI，实现战略价值向财务价值的转化。

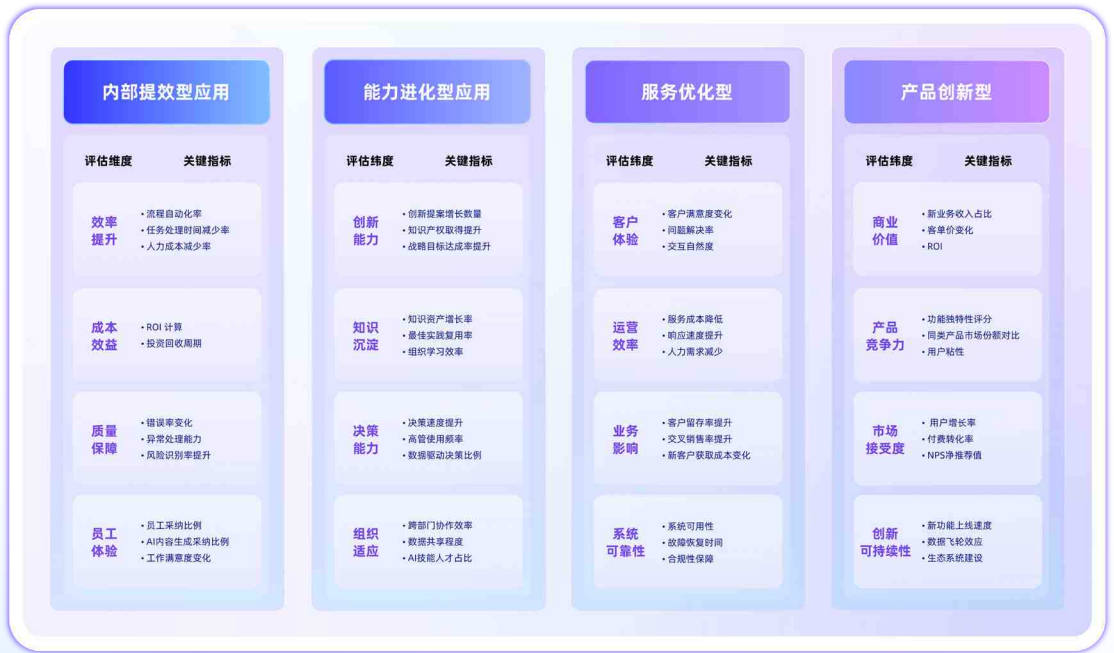


图 11 企业四大类型 AI 应用关键评估指标

趋势四

AI 产业链带动效应加速，催生 AI 原生企业

AI 技术的快速发展催生了一系列新产业、新业态，培育了一批以 AI 技术为核心驱动力的 AI 原生企业，这些企业通过技术创新与模式突破，进一步强化产业链带动效应，系统性重塑技术供给逻辑、商业合作模式与产业创新节奏，激活全域产业创新活力。2025 年，我国人工智能核心产业的规模达到了 1.2 万亿，企业超过 6200 家，中国的大模型走向世界。IDC 发布的《全球人工智能和生成式人工智能支出指南》数据显示，有望在 2029 年全球人工智能 IT 总投资规模将增至 12619 亿美元，五年复合增长率（CAGR）为 31.9%，直观体现了 AI 产业链的庞大发展潜力。AI 技术的产业带动效应围绕产业链条可分为算力底座层、算法与模型层、数据与知识工程层、平台与工具层及应用服务层，在这些层面分别催生一批 AI 原生企业。

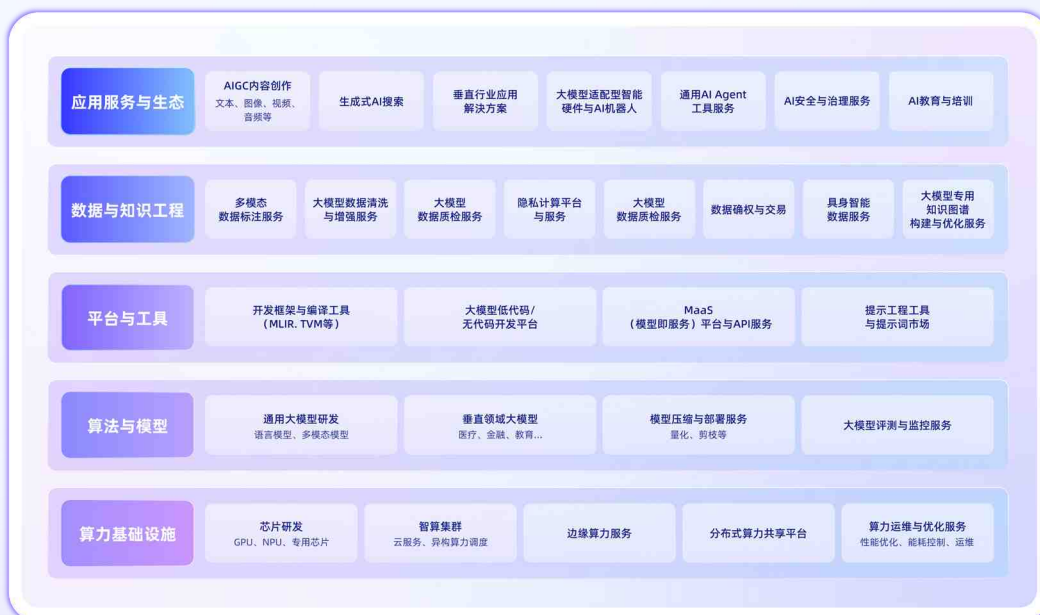


图 12 AI 原生产业发展全景
资料来源：阿里云研究院绘制

算力基础设施为 AI（尤其是大模型）提供算力支撑，是 AI 产业链的基础载体，核心围绕硬件和算力服务展开，大模型的规模化训练与推理推动算力向专业化、精细化、分布式升级，带动上下游协同突围。一方面，大模型的发展推动了原有算力产业的升级和发展，包括芯片设计、制造、封装测试、服务器制造、基础网络设备、计算集群与算力服务等。另一方面，大模型催生了系列新兴产业，包括：**大模型专用芯片研发**，如高性能 GPU、端侧 NPU、AI 加速器，专为大模型训练 / 推理设计，聚焦高算力、低功耗，区别于传统通用芯片，核心服务于 AI 场景，是 AI 原生企业的核心布局领域；**异构算力调度服务**，提供大模型推理加速与跨云算力调度 SaaS；分布式算力共享平台，整合社会闲置 GPU / 算力资源，通过调度算法实现算力按需分配，解决大模型训练 / 推理的算力成本过高、资源闲置问题，是大模型催生的全新算力服务模式；**边缘算力服务**，为端侧大模型（如手机、物联网设备中的轻量化大模型）提供就近算力支撑，解决中心算力时延过高的问题，是大模型向端侧延伸的核心配套；**算力运维与优化服务**，专为大模型算力集群提供运维、性能优化、能耗控制服务，区别于传统 IDC 运维，聚焦 AI 算力的稳定性与高效性。

算法与模型层是 AI 技术的核心，形成通用大模型基座与垂直领域精调的分层格局，催生了一批聚焦模型研发、精调的 AI 原生企业。包括：通用大模型基座研发，技术门槛极高，以科技龙头企业和 AI 创新企业为核心力量；垂直领域大模型，基于通用大模型基座，结合垂直行业数据（如医疗、金融）进行精调，打造适配具体行业的大模型，是大模型落地的核心环节。大模型压缩与部署服务，将通用大模型进行轻量化压缩，适配端侧、边缘侧设备，解决大模型部署成本高、硬件要求高的问题，是大模型规模化落地的关键。大模型评测与监控服务，针对大模型的性能、准确性、安全性、偏见性进行评测，实时监控模型运行状态，是大模型合规落地的核心配套服务。

平台与工具层，能够大幅降低 AI 的开发、部署和应用门槛。平台与工具向专业化、轻量化、普惠化转型，催生一批聚焦大模型开发平台和工具链的 AI 原生企业，包括：大模型专用开发框架与编译工具，专为大模型训练、部署设计，优化大模型开发效率（如快速迭代、跨硬件适配），如 MLIR、TVM 等开源编译框架；大模型低代码 / 无代码开发平台，无需专业 AI 工程师，通过拖拽、模板等方式，让非技术人员快速调用大模型能力，构建大模型应用，是大模型普惠化的核心工具；MaaS（模型即服务）平台与 API 服务，将大模型能力封装为 API，企业无需自行研发 / 部署大模型，通过调用 API 即可使用大模型能力，催生“模型分发-API 调用-定制化服务”的全新生态。提示工程工具与提示

词市场，帮助用户优化提示词、生成提示词模板，甚至搭建提示词交易市场，降低大模型使用门槛，是大模型催生的全新工具品类。

数据与知识工程层，为 AI 模型（尤其是大模型）提供高质量、合规的数据支撑。大模型的发展推动数据服务从粗放式向精细化、合规化、专业化转型，催生多个全新细分领域，包括：大模型专用多模态数据标注服务，针对大模型训练需求，提供文本、语音、图像、视频、点云等多模态数据标注，标注精度高、场景复杂（如 4D 点云标注、多模态对齐标注），结合 AI 技术提升标注效率，是大模型高质量训练的核心支撑；大模型数据清洗与增强服务，针对大模型训练数据的“噪声、重复、偏见”等问题，进行精细化清洗，同时通过合成数据、数据扩充等方式，提升数据量与多样性，解决大模型高质量数据短缺问题；大模型数据质检服务，核心围绕大模型训练、标注、清洗后的全流程数据质量开展评测、校验与优化，涵盖数据准确性、完整性、一致性、合规性等核心维度，是保障大模型训练效果与合规性的核心配套。隐私计算（联邦学习、安全多方计算）平台与服务，解决大模型数据共享与合规的矛盾，催生全新的服务模式；大模型专用知识图谱构建与优化服务，区别于传统知识图谱，专为大模型设计，将行业隐性知识转化为结构化知识，融入大模型训练，提升大模型的逻辑推理与行业适配能力（如法律、工业知识图谱）。催生了知识图谱构建、规则库开发、领域知识服务等新产业；数据确权与交易，针对大模型训练数据，提供确权、定价、交易服务，规范数据流通，保障数据提供者权益，是大模型数据生态的重要组成部分。具身智能数据服务，专为具身智能大模型提供多模态数据采集、标注与处理服务，涵盖机器人末端执行器位姿、关节空间状态等多维度数据，解决具身智能数据稀缺问题；向量数据库即服务，降低非结构化数据管理门槛。

应用服务与生态层，将 AI（大模型）技术落地到具体行业场景，实现商业价值，大模型的出现催生了一批全新的应用场景与服务模式，包括：AIGC 内容创作（多模态），依托大模型生成文本、图像、视频、音频等内容，区别于传统内容创作（人工主导），实现“AI 主导、人工辅助”，催生全新的内容生产模式；生成式 AI 搜索，区别于传统搜索引擎（关键词匹配、链接罗列），基于大模型实现“自然语言对话式搜索”，直接输出精准答案，优化信息检索逻辑；垂直行业大模型应用解决方案，结合垂直行业场景，基于大模型打造一体化解决方案，不局限于单一功能，优化行业业务流程（如医疗诊断、法律合同审查、工业质检）；大模型适配型智能硬件与 AI 机器人，区别于传统单一功能智能硬件，此类产品内置轻量化大模型，具备自主交互、场景适配、多任务处理能力，实现“硬件 + 大模型”深度融合，按应用场景分为消费级智能硬件、工业级机器人、服

务类机器人三大细分，是大模型向物理世界落地的核心载体。大模型辅助智能驾驶服务，依托大模型的环境感知、逻辑决策、应急处理能力，辅助提升自动驾驶安全性与适配性，覆盖车载 AI 交互、自动驾驶算法优化、路侧 AI 感知等细分场景，区别于传统自动驾驶（依赖规则算法），具备更强的复杂路况适配能力；通用 AI Agent 工具服务，基于大模型的多任务处理、自主决策能力，打造通用型 AI 智能体，无需人工干预即可完成日程规划、邮件处理、多平台协同、信息汇总等复杂任务，适配个人办公、中小企业管理等场景。AI 安全与治理服务，大模型的规模化应用带来安全风险（如模型偏见、恶意生成、数据泄露），此类服务聚焦大模型安全审计、偏见检测、内容风控，是大模型合规落地的核心配套。AI 职业教育、技能培训等新产业，为 AI 产业链持续发展提供人才支撑。

综上，AI 产业链的带动效应，核心体现为大模型催生新型产业、激活原有产业，其中 AI 原生企业（尤其是初创企业）在新型产业中占据主导地位，聚焦技术创新与模式突破；原有产业则通过适配大模型需求实现升级，与新型产业协同构建完整的 AI 生态。在此基础上，AI 发展带动了就业结构优化，催生了 AI Specialist、提示工程师、AI 伦理专员等一批融合技术、业务与伦理素养的新职业，进一步完善了 AI 产业的人才生态，带动相关服务产业升级。



图 13 每年新增 AI 原生企业占比

数据来源：IDC 报告

备注：AI 原生企业是指，企业主要业务或核心能力与人工智能技术直接相关，而非仅间接关联或少量应用

现实挑战与路径建议

尽管 AI 驱动的产业变革前景广阔，但从技术成熟到价值落地仍面临现实挑战。行业数据的稀缺性和质量问题是首要障碍，许多垂直领域缺乏足够的标注数据支撑模型训练，数据孤岛和隐私限制阻碍了数据共享，跨领域、跨企业的数据流通缺乏可信机制与标准，成为制约行业大模型精进和跨链协同的致命短板。投资回报的不确定性使企业在大规模投入时顾虑重重，AI 项目的成本结构复杂且波动较大，价值实现路径往往模糊，大量应用停留在试点验证或内部效率工具阶段，未能与核心营收增长明确挂钩。生产级部署的工程化挑战不容忽视，模型在实验室的表现与真实业务环境中的稳定性存在差距，系统集成、运维监控、持续优化需要多学科协同能力。

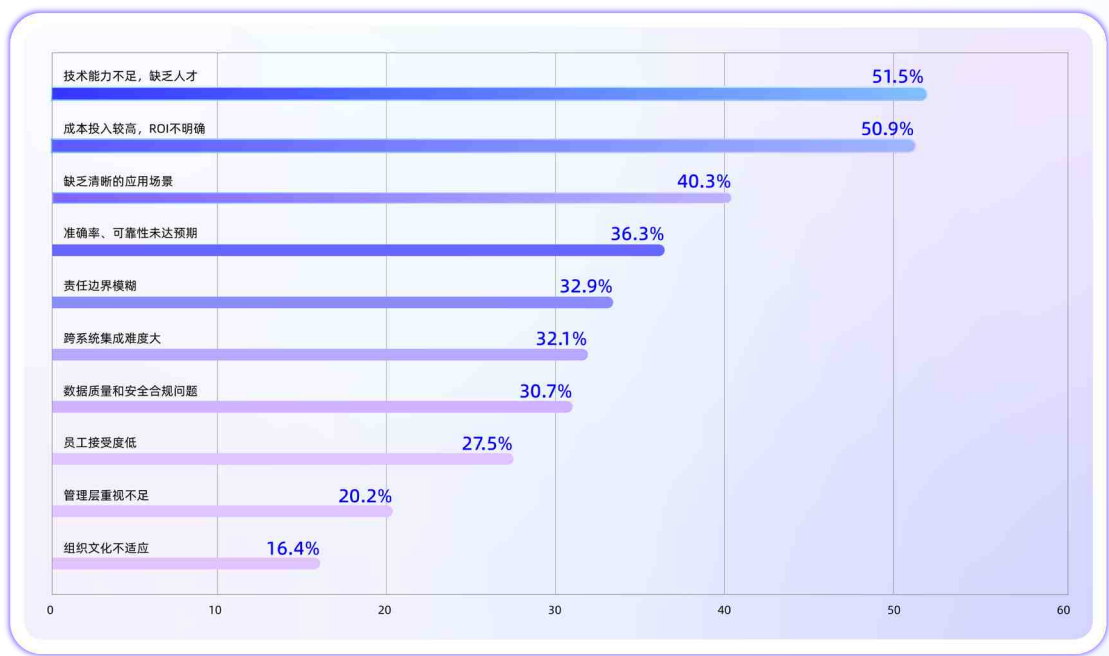


图 14 企业 AI Agent 开发过程中，企业面临的最主要挑战受访结果
数据来源：阿里云研究院问卷调查

应对这些挑战需要多方协同的系统性解决方案。从企业战略上，应从业务痛点最清晰、ROI 最易衡量的场景切入，以“最小可行产品”快速验证价值，而非追求大而全的解决方案。技术上，小样本学习、迁移学习等方法能够缓解数据瓶颈，模型压缩和边缘计算降低部署成本。发展智能体间通信协议标准，为多智能体互联互通奠定基石。机制层面，建立行业数据联盟促进合规共享，构建 AI 价值评估的双维框架提升投资决策科学性，培育 AI 工程化人才夯实落地基础。生态层面，龙头企业开放平台降低中小企业应用门槛，

3

体验共生，
无处不在的智能生活

随着多模态大模型、模型轻量化技术、情感计算、跨设备协同及智能体（Agent）技术与开放生态架构等多种技术的突破与发展，AI 正逐步在个人日常生活中构建起全域覆盖、无感衔接、有温度陪伴的智能服务网络，推动智能与生活深度融合。多模态大模型实现视觉、语音、文本等自然交互与理解，为全生命周期个性化服务奠定交互基础；模型轻量化技术（如知识蒸馏、量化、剪枝）与端侧 AI 芯片发展破解算力约束，支撑端侧智能设备的流畅服务；情感 AI 赋予系统感知与回应情绪的能力，升级共情陪伴体验；跨设备协同与边缘计算打通终端壁垒，实现服务实时响应与场景流转；尤为关键的是，基于大模型的智能体技术通过工具调用、服务编排与标准化 API 网关，联动开放平台生态，使助手能精准理解用户意图并安全调度外部服务，真正实现“服务即插即用”的生态融合；联邦学习与隐私增强计算共同构建数据“可用不可见”的协同机制，筑牢跨域协作的安全底座。

技术能力的逐步成熟以及端云协同架构的全面落地，推动智能化深度融入个人生活的方方面面，从居家、出行、娱乐到健康管理、教育服务等，其中云端大脑负责深度思考与全局记忆，端侧引擎保障实时响应与隐私安全，两者通过智能调度实现动态平衡。智能生活正从工具协同，迈向系统性共生的新纪元，加速呈现出四大趋势：智能全域渗透重构生活场景、超级智能助手重塑数字生活服务中枢、全局记忆打通跨端体验、多模态共情赋予技术温度。



图 16 云端协同的智能生活全景图
资料来源：阿里云研究院绘制

趋势一

智能全域渗透，贯穿日常生活工作全场景

智能技术已经广泛且深度嵌入办公、家居、教育、健康、娱乐、出行等生活工作的核心领域，在对 AI 助手应用情况的调研中，97% 的受访者已使用通用大模型助手（如千问、DeepSeek），生成式 AI 需求爆发；78.9% 的用户已高频使用终端内置语音助手，语音交互成为主流。相比之下，智能穿戴设备助手渗透率高于家居与车载，而 AI Agent 类产品尚处早期培育阶段。当前，AI 消费级应用正呈现入口抢占、体验迭代、生态构建三大趋势。



图 17 受访者使用的智能助手类型分布
数据来源：阿里云研究院调查问卷

AI 眼镜、耳机等新型 AI 硬件,持续拓展交互触点和入口。AI 硬件企业聚焦贴身、高频、持续感知场景,以健康管理、情感陪伴、内容创作为切入点,深度融入日常生活,除智能手表、AI 眼镜、VR/AR 外, AI 耳机、智能项链 / 吊坠、智能戒指、智能贴片、电子皮肤、柔性传感穿戴等新物种集中爆发,成为 2026 年最具代表性的前沿趋势。其中,智能手表从消费电子走向个人健康管理平台,核心驱动力来自“生物传感技术+生成式 AI”的深度融合。通过集成血氧、心率、体温、心电等多维度传感器,并依托大模型进行个性化分析,可实现睡眠呼吸暂停、高血压、房颤等健康风险的主动识别与预警,并向无创血糖、预防性医疗、慢病管理、远程医疗等延伸。AI 眼镜迈向独立终端与空间计算入口,借微型光学、轻量化设计与多模态 AI, AI 眼镜被视为下一代移动计算平台的重要方向。依托端侧轻量化模型,可实现实时环境感知、AR 信息叠加,支持视觉识别、实时翻译、会议提词、所见即答、眼镜端支付等原生 AI 能力。除此之外,更多的微型化、无感式、时尚化 AI 硬件推陈出新。AI 耳机 / 耳饰作为无感音频入口,集成多麦降噪、骨传导、实时翻译、AI 语音助手、会议纪要,成为移动办公、跨境出行的隐形助理。智能项链 / 吊坠可搭载微型摄像头进行日常生活观察、监测和记录;智能贴片可贴于皮肤长期佩戴,面向康复、慢病、压力管理提供医疗级数据。

传统成熟的智能应用场景,正加快 AI 赋能实现系统级智能重构体验。在办公、教育、出行等成熟的高频场景中, AI 通过系统级融入,在不改变用户习惯的前提下提升效率、安全与交互体验,更容易实现规模化应用。AI 手机正从生成式 AI 向全域 AI 升级,手机智能体 (Agent) 通过整合系统资源与应用工具,提供跨应用的无缝服务体验。AI PC 凭借算力与内存升级,本地部署大模型,推动传统电脑向智能化生产力工具演进,可智能理解并辅助完成多场景任务。AI 录音笔等爆款产品,也印证了 AI 办公工具的强劲需求。教育场景中,多模态大模型驱动智能辅导、自适应学习平台全面落地,可感知学习状态、推送定制方案,初步实现因材施教。AI 学习机、学习平板成为高增长品类,点读笔、教育机器人、翻译机等形成专业化辅助矩阵。IDC 预计,2026 年中国教育机器人销售额达 8.8 亿美元,同比增长 21.2%。车载场景中,大模型赋能智能座舱与智能驾驶,提升语音交互、语义理解与知识能力,支持语音、手势、视线追踪等多模态交互。AI 导航可基于习惯与路况智能规划,车载语音助手让驾驶更安全高效。

智能服务生态持续完善, 从单点智能向跨设备跨系统协同的系统智能发展。在智能服务生态构建中, 以智能家居的应用最为典型, 通过全屋智能中控、场景联动与设备互联, AI 被用于优化家庭生活空间的运行方式。家用服务机器人 (如扫地机、洗拖一体机等) 借助 AI 实现地图构建、智能避障、路径优化, 需求快速增长。家庭自动化系统使房主能够通过智能手机或语音指令远程控制各类设备 (如照明、安防摄像头、家用电器、恒温器等), 实现联动控制, 形成个性化居家场景模式, 满足不同时段的居住需求; 家用娱乐设备方面, 用户也可通过控制多种智能设备联动播放音乐、获取新闻与天气信息等, 从而提升使用体验; AI 加快家电智能化, 包括自适应操作、冰箱食材智能管理、洗衣机材质识别等高级功能, 显著提升了家庭生活质量和使用体验。

未来, 智能全域渗透将朝着“全场景深度融合 + 跨生态无缝协同”方向演进。技术层面, 多模态大模型与边缘计算的进一步迭代, 将实现更精准的场景感知与更快的服务响应; 跨端协同将突破品牌生态壁垒, 实现不同品牌设备间的数据自由流转与指令统一调度, 构建全域协同网络。场景层面, 各领域智能服务将打破边界, 实现跨场景联动适配, 例如健康数据可联动家居设备调整环境参数, 出行规划可同步优化娱乐、餐饮等配套服务, 最终形成全域一体的智能生活生态。对此, 阿里云也打造完整的 AI 硬件解决方案, 从 AI 基础设施到多模态模型服务, 全方位助力 AI 硬件产品创新和体验升级。

趋势二

超级智能助手全栈集成，成为数字服务中枢

用户对 AI 的核心诉求，已从信息获取、对话交互，升级为自主解决复杂现实任务。这推动智能助手跳出单一聊天场景，向具备规划、调用、执行、反馈的全链路能力演进。实现这一跃迁的核心引擎，是智能体（Agent）技术的成熟与互联。随着 MCP、A2A 等智能体通信协议完善，叠加 ASL 可信互连等安全机制，不同垂直领域 Agent 可实现安全高效互通、分工协同、中枢调度，为超级智能助手全栈集成奠定技术基础。超级智能助手依托 Agent 网络，可完成自然语言输入 - 意图理解 - 任务拆解 - 跨 Agent 协同 - 服务履约 - 结果反馈的自动化闭环，真正实现“一句话办多件事”。我们面向 1000 位用户的调查问卷显示，大多数受访者对超级智能助手整合全域服务、成为个人数字中枢持积极态度。



图 18 受访者对 AI 智能体整合更多服务、成为数字服务中枢的需求分布
数据来源：阿里云研究院调查问卷

国内外科技巨头正以差异化生态策略，加速超级智能助手落地。国内最具代表性的案例便是千问，其已深度集成与淘宝（购物）、飞猪（出行）、高德（导航）、淘宝闪购（即时零售）等体系化服务，用户通过千问这一统一入口，即可完成从方案制定、比价下单到履约追踪的全链路操作，展现了生态内闭环的极致效率。在国际市场，类似的 Agent 网络协同模式正加速成型，但路径各异。谷歌联合 Shopify、Etsy、Wayfair、Target 和 Walmart 等企业共同研发，推出通用商务协议（UCP），为 AI 购物代理提供了统一的商品发现、下单、支付和售后标准，使不同平台和商家能够被通用 Agent 调用。由于其在协议层打通了支付和身份验证，因此不仅能在 AI 聊天框中接入，也可在搜索框及 Android 系统全局搜索等进行连接，实现 Agent 标准调用，探索开放生态下的服务闭环。OpenAI 推出“Instant Checkout”（即时结账）功能，允许用户通过 ChatGPT 直接向 Etsy 卖家购买商品，通过“代理式电商协议”（ACP）标准化 AI 与商家的交易流程。微软在 Copilot 中推出的 Copilot Checkout 功能，允许用户在与 AI 聊天机器人对话过程中直接购买产品，无需离开聊天界面或访问零售商网站就能完成整个购买流程。

尽管前景广阔，Agent 网络与超级智能助手的发展仍面临多重严峻挑战，用户调研数据直观反映了核心制约：**一是隐私与信任是首要顾虑**，70.4% 的受访者对个人隐私数据安全高度担忧，27.3% 的用户缺乏对 AI 决策的信任感，这直接影响用户对深度服务的接受度。**二是生态壁垒与数据孤岛问题突出**，59% 的用户认为各平台 / APP 数据不互通、生态壁垒严重，成为服务闭环的核心障碍。目前各大厂商主要构建内部或联盟生态，难以跨生态调度资源，制定跨平台的 Agent 通信与互操作标准，将是行业走向下一阶段的关键。**三是技术体验与能力仍需提升**，44.3% 的用户反馈智能助手理解能力和准确度不足，31.9% 的用户认为技术成熟度不够、体验不稳定。复杂任务高度依赖多 Agent 协同，任一环节 API 变动、响应超时、意图误解都可能导致整体失败，故障转移、重试机制、一致性保障是工程核心难题。中长期看，超级智能助手将逐步从工具属性升级为不可或缺的超个性化生活管家，深度融入衣食住行的每一个细节，实现效率与体验的双重极致提升，而 Agent 网络互联与全栈集成、服务闭环，将成为未来 AI 消费商业化发展的核心趋势。

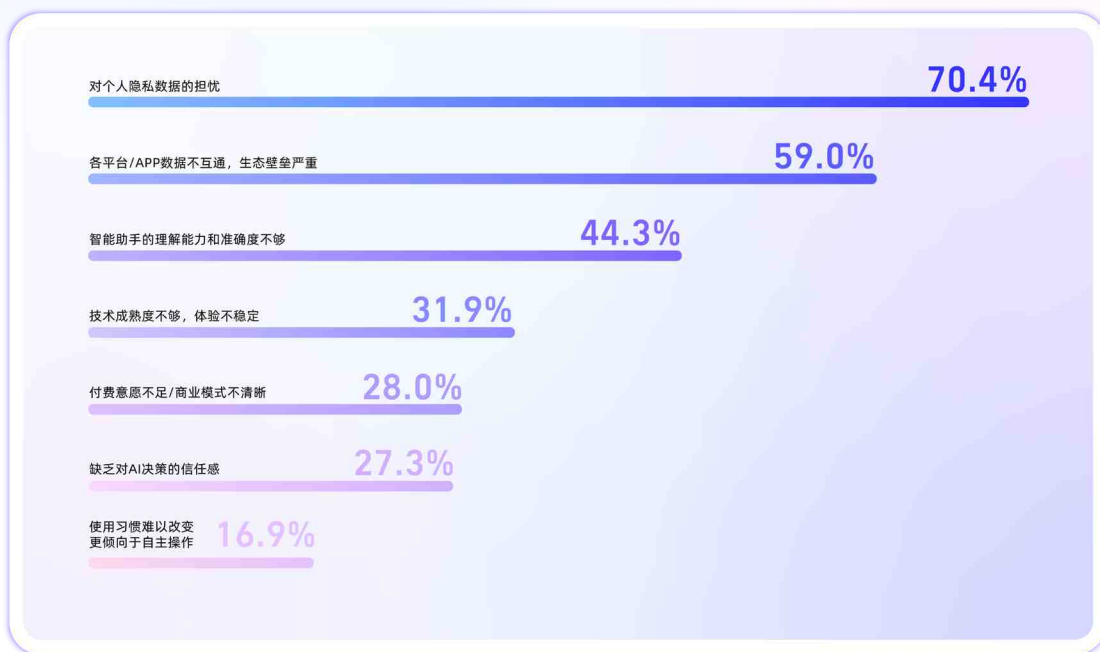


图 19 受访者认为制约超级智能助手发展的最主要因素
数据来源: 阿里云研究院调查问卷

趋势三

全局记忆串联，实现跨端跨模态跨任务融合

在 AI 向“更懂你”的智能进阶过程中，全局记忆正成为核心架构突破点。它使 AI 能够持续学习用户的偏好习惯、行为轨迹与情感关联，构建动态演化的个人数字分身，推动交互范式从被动响应指令迈向主动理解。根据应用形态的不同，目前探索全局记忆的相关方主要可分为 3 类：交互智能体型记忆、生活记录型记忆和硬件生态型记忆。

交互智能体型记忆

突破单次对话遗忘，实现跨会话
跨时间深度理解用户偏好



生活记录型记忆

全景复刻数字记忆库，自动记录
多模态生活痕迹



端侧生态型记忆

跨端无缝流转联动，适配
场景化体验



交互智能体型, 突破单次对话的遗忘局限, 实现跨会话、跨时间, 高度连贯和个性化的连续服务。实现全局记忆的过程中, 一方面模型厂商通过架构创新不断扩大模型的上下文长度, 但是总体来说成本较高; 另一方面, 越来越多的机构开始通过 RAG 技术, 将海量记忆存储在外部向量数据库, 管理主题专属持久记忆, 对话时仅检索最相关的片段输入模型, 兼顾效果与成本。但记忆的存储、更新、检索并非简单堆砌, 前沿研究 (如 Mem- α 框架) 正尝试用强化学习训练 AI 自主决定记住什么、如何存储、何时调用, 让记忆系统变得更智能。上海交通大学与阿里巴巴团队提出的 ReMe 框架, 专注于让 AI 从成功和失败的经验中学习, 并不断优化和清理记忆库, 使记忆系统本身具备进化能力。其创新的“测试时扩展技术”, 能在推理时更高效地融合历史信息, 在相同上下文中实现更深度的思考, 这间接提升了处理复杂记忆关联的能力。AgentScope 已集成 ReMe 的长期记忆实现, 支持个人、任务和工具级别的长期记忆管理。

生活记录型, 核心在于全景复刻, 打造个人数字记忆库。一般以智能硬件为载体, 能够自动、完整、实时地记录用户在数字及物理世界中的全方位痕迹, 构建可搜索、可关联、可回溯的私人数字记忆体。依赖于端云协同架构与多模态语义对齐, 端侧设备 (如穿戴设备) 实时捕捉碎片化信息, 包括位置、浏览内容、语音备忘录等; 云端进行统一存储、结构化处理与关联分析, 通过语义向量技术打通文本、图像、音频等不同模态数据, 实现无感记录与智能关联。例如, Looki 类智能硬件能够实时捕捉用户日常交互 (如语音闲聊、文本笔记)、场景痕迹 (如浏览内容、停留地点)、情感关联 (如情绪波动时的操作习惯) 等多模态信息, 从而串联成完整的生活叙事。用户可随时回溯某一个时间点正在干什么, 或系统自动生成“您的春季阅读兴趣图谱”。记忆从被动存储变为主动的生活数字孪生, 为更深度的智能服务提供数据基石。

端侧生态型, 使记忆能在多种设备无缝流转和联动, 实现场景化体验适配。能够结合硬件场景属性 (如智能座舱、家居、穿戴), 通过端侧感知、云端同步、设备互联协议, 将记忆与硬件功能深度绑定, 实现记忆的场景化调用与多设备联动。端侧记忆流转的实现, 更依赖于由一家厂商主导、产品线覆盖广泛的硬件生态, 如家居、电脑、汽车、智能手表等不同终端。AI 可基于全局记忆自动适配跨端体验: 在手机上和 AI 闲聊提及喜欢的电影类型, 切换至智能电视时, 会自动推送同类影片; 用智能手表记录的运动偏好与健康数据, 同步至家居设备后, 可联动调整运动后的室温与音乐; 在 PC 上编辑的旅行攻

略笔记，切换至智能座舱后，导航会自动关联笔记中的目的地与行程规划，智能家居也会提前适配出行期间的安防设置。这种记忆流转，让生活细节被精准捕捉与复用，大幅降低场景切换的体验成本。目前无论是手机、眼镜还是陪伴硬件等智能终端厂商都关注其在全局记忆上的实现方案，进而实现跨端、跨模态、跨任务的记忆一致性和持续积累。随着 Matter 等统一技术接口的发展，有望实现设备间的互操作。



图 20 不同类型记忆载体的重点关注方向及技术方向
资料来源：阿里云研究院绘制

全局记忆的核心价值，在于实现记忆的全维度捕捉与长效沉淀，而非局限于任务或指令记忆。它如同个人专属的“数字记忆中枢”，覆盖生活各类场景细节：既记录显性交互记忆，如手机语音指令、电脑文本输入习惯、智能座舱音乐偏好、智能家居模式设置；也捕捉隐性场景痕迹，如浏览过的内容、停留过的地点、关注过的商品、甚至短暂的语音闲聊、随手标注的笔记；同时关联情感与场景的绑定记忆，如特定音乐搭配的场景偏好、情绪波动时的操作习惯等，全方位复刻生活轨迹，让记忆不再因设备切换而断裂。未来，全局记忆将朝着“主动记忆 + 智能关联”方向演进，自动筛选有价值的生活记忆进行沉淀，弱化冗余信息；同时强化记忆与场景的主动关联，例如生日、周年等关键节点，提前联动多设备适配氛围场景，让全局记忆不仅是记录载体，更能主动唤醒生活细节、适配情感需求，成为深度融入日常的记忆伙伴。

趋势四

多模态共情进阶，构建有温度的无感陪伴体验

随着智能生活的广泛渗透，更多人期待 AI 能够更有温度，实现从功能满足向情感共鸣与体验升级演进。在我们开展的 1000 份调查问卷中，62.6% 的受访者希望 AI 用更自然、有温度的方式进行回应，59.8% 的受访者期待 AI 能够准确感知和理解用户情绪状态，并期待能够提供更多的个性化关怀和建议。当前，多模态共情技术让 AI 逐步具备情绪感知、共情回应能力，实现从工具到有温度陪伴者的跨越；无感服务则改变人机交互逻辑，以自然无负担的方式融入生活，两者分别从情感价值与体验效率出发，共同构建更具人性化的智能生活新形态。

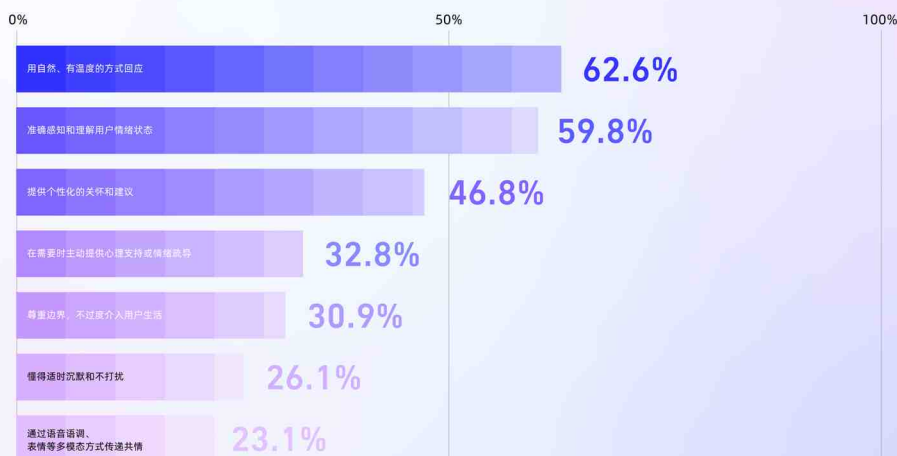


图 21 受访者认为 AI 在情感共情和陪伴方面最重要的能力分布
数据来源：阿里云研究院调查问卷

多维度情绪识别体系的构建，是共情陪伴的基础前提。

共情陪伴通过构建情绪识别 - 理解 - 反馈 - 疏导，释放情感价值。首先在情绪识别方面，通过多入口协同采集多模态情绪信号，构建全方位情绪特征库：麦克风捕捉语音语调（语速、音量、语气变化）；摄像头解析面部肌肉运动、眼神变化与肢体姿态；可穿戴设备采集心率变异性、皮电反应等生理数据，客观反映情绪波动，弥补主观表情伪装带来的识别偏差；文本分析则通过语气词、句式结构捕捉隐性情绪。多模态信号的融合分析，使复杂场景下的情绪识别准确率较单一模态大幅提升，为共情回应提供精准依据。其次，通过训练认知行为疗法（CBT）等循证心理模型，针对不同人群、不同情绪状态，提供更具针对性的适配回应，而非机械的话术反馈。

目前，多模态情感陪伴已在多个核心场景实现产品落地。在儿童成长陪伴场景中，以实体交互为核心，如 LOVEAXI loviPeer Pro 推出的儿童 AI 陪伴机器人，能够依托多模态情绪识别捕捉儿童情绪变化，及时调整互动方式；通过听声辨位、动态眼神模拟实现主动物理互动；同时构建儿童专属记忆图谱，记录喜好与成长轨迹，兼顾陪伴与启蒙价值。在成人情感陪伴场景中，主打无压力情绪倾诉与孤独缓解，bibo 情感机器人定位成人用户，依托多模态情绪感知技术主动发起互动，摆脱指令依赖，为用户提供情绪疏导；Soul App 则通过原生情绪大模型与虚拟伴侣，提供有上下文的共情对话，打造私密情感支持空间。此外，在养老场景中，部分智能设备已实现情绪识别与健康监测联动，识别到老人孤独、焦虑情绪时主动发起话题，必要时触发紧急呼叫，填补养老情感缺口。

无感服务的核心则是优化人机交互，实现服务不打扰、需求早满足，让智能真正融入生活肌理，无需用户主动发起指令，即可获得精准适配的服务体验。其中，交互载体的升级，为无感服务的落地提供了重要支撑，肌电信号、环境捕捉、图像输入、眼动追踪、体感捕捉、脑机接口、手势、语音、触控等隐形式交互方式，逐渐成为无感服务的重要入口；智能眼镜、智能腕戴、智能戒指等可穿戴设备，不仅承担输入媒介角色，更成为环境感知与用户意图捕捉的延伸节点。具体而言，视觉交互通过高精度摄像头与眼动追踪技术，实时捕捉用户的注意力焦点与行为意图；空间手势交互依赖传感器阵列和 AI 算法，将动作转化为虚拟空间的操作指令，实现无感控制；语音与肢体交互则逐渐与传统方式融合，形成更自然的多模态交互体系，让 AI 能够精准捕捉用户隐性需求。

无感服务已经在出行、购物、居家等多个核心生活场景有所应用。在出行场景中，智能座舱通过捕捉驾驶员疲劳状态、驾驶意图，自动调节音乐、发出提醒，联动导航优化路线避开拥堵，同步推送沿途休息区信息；在购物场景中，AI 通过视觉识别用户注视商品的行为，结合用户历史偏好，自动推送商品详情与相关优惠，同步至手机端供后续查阅与下单，简化购物流程；在居家场景中，系统基于用户位置、活动状态与环境参数，自动切换房间灯光、空调模式，夜间监测到用户起夜时，自动开启低亮度灯光并规避障碍物，实现居家生活的便捷化、智能化，让服务自然融入日常，无需刻意关注。

但目前 AI 人性化发展方面依然存在诸多挑战：**技术上**，复杂场景下情绪识别精度不足、跨模态数据融合效率偏低、个性化回应缺乏灵活性，尤其在嘈杂环境、用户情绪伪装等场景中，识别准确率有待提升；**伦理上**，情绪数据、生理信息属于高度敏感数据，存在隐私泄露风险，同时可能引发部分用户对 AI 的情感依赖，弱化现实社交能力；**生态上**，跨场景数据联动效率不足，制约了用户体验。尽管面临多重挑战，但智能生活向更人性化、更便捷化、更有温度的方向演进是确定性趋势。

AI 驱动的智能生活进化，本质上是围绕体验升级完成的系统性变革，核心目标是实现人机无感共生。在这过程中，仍然面临多模态识别精度、情感伦理边界、跨设备协同壁垒、数据隐私安全等核心挑战。技术层面，复杂环境下多模态融合易出现偏差，端侧算力限制影响模型表现；伦理层面，情感数据采集与使用存在隐私风险，易引发情感依赖与操控争议；协同层面，不同品牌设备的通信协议、数据标准不统一，制约全域协同；安全层面，多入口数据采集与传输存在泄露风险，防护体系待完善。

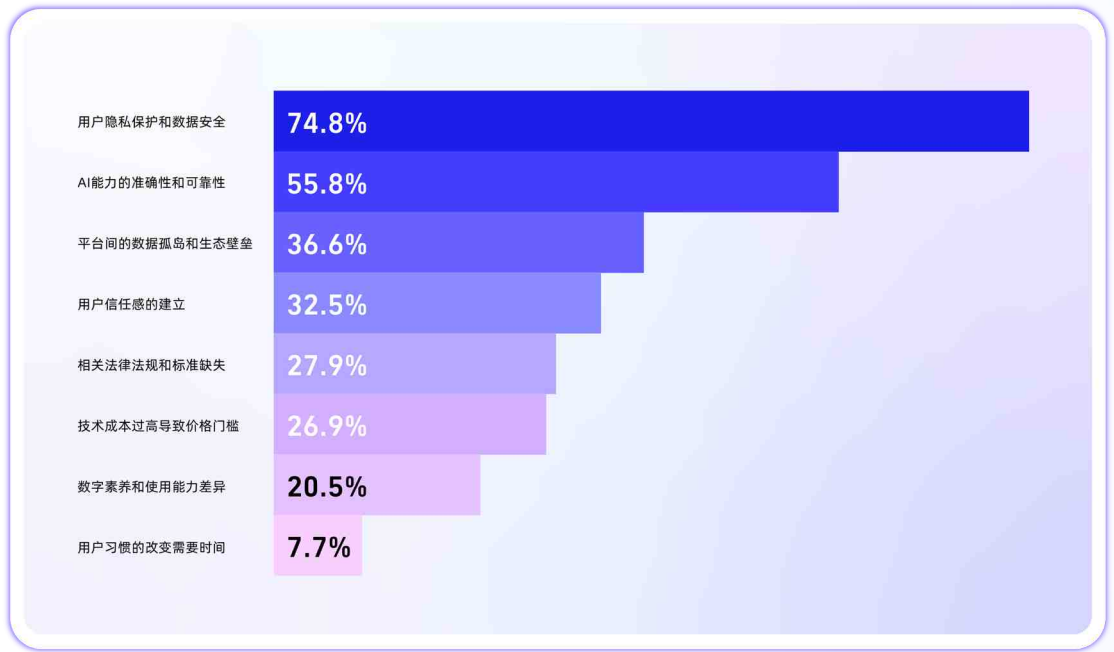


图 22 AI 融入个人数字生活面临的挑战来源
数据来源：阿里云研究院调查问卷

破解难题需构建“技术优化 - 伦理规范 - 协同标准 - 安全防护”四位一体路径，技术上优化多模态模型与边缘计算能力，提升复杂场景适配精度；伦理上搭建“法规 + 行业 + 企业”三层体系，明确情感 AI 应用边界；生态上推动行业数据标准与接口统一，打破生态壁垒；安全上强化端云协同加密与数据脱敏技术，保障隐私安全。未来，随技术迭代与规范完善，AI 将实现从“主动适配”到“预判创造”的跨越，构建“人类主导、AI 赋能、无感共生”的智能生活生态，持续提升生活质量与幸福感。

4

科研跃迁， 迈向“AI for Science” 的科学智能新范式

2024 年诺贝尔物理学奖授予 Geoffrey Hinton 和 John Hopfield，以表彰他们在人工神经网络和机器学习方面的基础性贡献；化学奖授予 David Baker、Demis Hassabis 和 John Jumper，其中后两位因 AlphaFold 在蛋白质结构预测方面的贡献而获奖。诺贝尔奖对 AI 领域科学家的认可，在全球科研领域引发了广泛热议，也让更多人看到人工智能技术重塑科研生态的巨大潜力。AI 正突破传统科研工具的边界，成为继理论科学、实验科学和计算科学之后新的科研范式，系统性加速人类认知边界的拓展。通过高效处理高维异构数据、整合跨学科知识体系、模拟和推演复杂问题，AI 不仅在材料科学、生命科学、气象预测等关键领域实现研发效率的量级提升，在优化科研价值链、拓展人类认知方面展现出较大潜力。AI for Science 的技术突破构成了这场范式革命的基础设施。各领域科学大模型通过在海量科学文献、实验数据上进行无监督学习，获得了对学科语言和规律的深度理解，并通过 AI 驱动的知识图谱构建、语义关系抽取、跨文献推理，能够从海量论文中发现隐藏的关联和矛盾。

这些技术的组合效应正在释放惊人的潜力。根据复旦大学发布的《科学智能白皮书》，2015 至 2024 年间，全球 AI 核心和 AI4S（AI for Science）领域的学术出版物总量快速增长，AI 论文数量在过去十年间激增近三倍——从 30.89 万篇增至 95.45 万篇，年均增长率为 13.7%。其中，2020 年后增速明显，AI4S 论文年均增长率从 2020 年前的 10.5% 跃升至 19.3%。中国科学学与科技政策研究会和爱思唯尔联合发布的《科研之信：未来研究者》对来自 113 个国家、超过 3200 名学术界与企业界科研人员的调研显示，目前全球已有 58% 的科研人员在科研中使用 AI 工具，这一比例较 2024 年的 37% 显著提升。从产业角度看，AI4S 赛道企业数量持续增长，分布在新药研发、蛋白质设计、材料研发、工业仿真和数据服务等领域。科研 Agent 框架将逐步普及，AI Scientist 雏形初现，形成“人类提出核心构想—AI 执行论证推导—双向迭代优化”的新型科研闭环，推动科研活动从个体探索走向人机共创。

趋势一

AI 优化科研方法体系， 驱动复杂问题的模拟、推演与设计

传统的科研范式，从经验归纳、理论推导到计算模拟、数据驱动，正面临着日益严峻的复杂性壁垒。从微观的量子粒子行为、等离子体演化，到中观的蛋白质折叠、流体动力学，再到宏观的全球气候变化、生态系统演化，这些系统普遍具有多尺度耦合、非线性相互作用和涌现行为等特征。面对这类复杂系统，传统的理论解析方法往往难以求解，而数值模拟方法则在精度与效率之间难以兼顾。AI 的引入并非简单的工具升级，而是从复杂系统实时模拟预测、跨尺度统一建模、高通量数据驱动的计算发现、生成式探索与逆向设计等方面进行科研方法体系优化。为此，学术界有声音认为科学研究进入数据和机理双驱动的“第五范式”，拓展了研究对象的广度、机理分析的深度和科学发展的速度，但也有学者认为不急于下定论，尚有待考量。

范式名称	大致时期	核心研究方法	典型成果案例	核心局限
经验范式	17世纪以前	以观察试验为核心，对自然现象的描述、纪录、总结和归纳	第谷行星观测星表，林奈形态分类	缺乏理论解释
理论范式	17世纪-20世纪中叶	以数理模型为基础，通过数学建模对自然规律进行抽象和推演	开普勒行星三定律，牛顿力学，麦克斯韦方程组，爱因斯坦相对论体系	复杂系统难解析
计算范式	20世纪中叶以来	以仿真模拟为标志，利用计算机仿真科学实验，实现结果预测和可视化	全球气候模型，计算流体力学，核反应数值模拟	数据处理能力不足
数据驱动范式	21世纪以来	以数据驱动为特征，对海量数据隐含规律进行挖掘与分析	斯隆数字巡天，人类基因组计划，气候再分析数据	因果推断能力不足及可解释性挑战

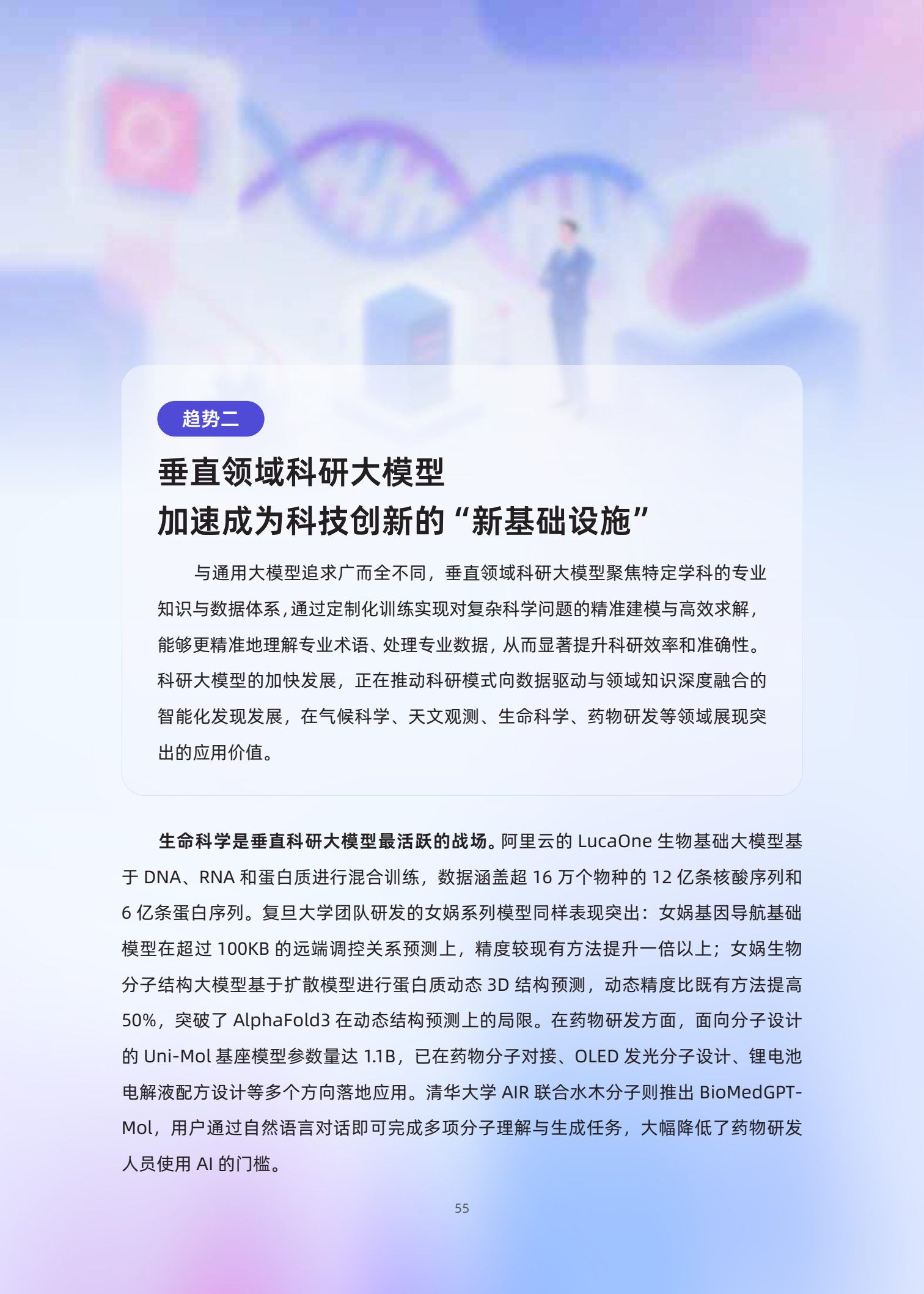
图 23 科研范式的演进与特征
资料来源：阿里云研究院绘制

驾驭复杂系统, 实现实时模拟与精准预测。传统科研中, 理论建模依赖先验知识构建数学方程, 优势在于可解释性强, 但面对高度复杂系统往往力不从心; 纯数据驱动方法能够从海量数据中自动发现模式, 但缺乏物理约束和可解释性容易产生虚假关联。以深度学习为核心的新一代科学仿真技术, 通过将物理先验知识、生物学原理等嵌入神经网络架构, 构建兼具物理可解释性与数据学习能力的融合模型。例如, 基于等变图神经网络的 MLFF 模型 (如 MACE、NequIP 等) 能够在特定体系下, 将原本需要数月的分子模拟压缩至数天甚至数小时内完成; DeepMind 的 AI2BMD 系统更在蛋白质体系中实现了近从头算精度的快速模拟。在气候科学中, 融合物理约束的 AI 模型能够在保持物理一致性的前提下, 实现比传统数值模式更快、更精准的天气预报。在生命科学中, 基于 AI 的数字生命体 (AI-Driven Digital Organism, AIDO) 构建了从分子到整体生命的多尺度基础模型, 覆盖 DNA、RNA、蛋白质、单细胞等层级, 实现了跨层级的全方位预测与模拟。在可控核聚变研究中, AI 仿真器结合数据驱动方法, 为理解等离子体的复杂行为提供了全新途径。2024 年 12 月发布的 Genesis 物理引擎进一步将仿真能力推向新高度, 实现从刚体到软体的多类型物理交互高效模拟, 并支持通过自然语言控制场景生成, 为具身智能与复杂系统研究提供了强大支撑。这些进展标志着科学仿真正从单一物理场景走向多尺度、多学科交叉, 从被动观察转向主动探索, 从现象预测迈向机理理解。

跨尺度统一建模, 弥合微观机理与宏观行为之间的鸿沟。科学研究长期存在尺度割裂问题: 量子力学解释原子行为, 分子动力学模拟分子运动, 连续介质力学描述宏观现象, 传统方法难以在不同尺度间建立有效关联。AI 驱动的多尺度神经网络能够学习尺度间的粗粒化映射规律, 例如利用高精度量子力学数据训练势函数, 并将其迁移至更大尺度的分子动力学模拟, 在保持量子级精度的同时实现宏观尺度仿真。最新研究进展显示, 深度学习已能够实现从粗粒度模型到原子构型的系统性反向映射: 基于卷积神经网络的模型可以生成多组分高分子材料的三维平衡原子构型, 并通过在损失函数中引入键长、键角、二面角等物理先验知识提升重建精度。这种跨尺度建模能力, 对理解电池界面电化学反应、生物大分子功能机制以及气候变化中的云物理过程至关重要, 使科学家能够清晰揭示微观扰动如何通过非线性作用逐级放大, 最终演变为宏观系统的相变与涌现行为。

生成式探索与逆向设计。传统科学发现高度依赖科学家的经验直觉和反复试错。从海量文献中提炼规律、从广阔的参数空间中搜索最优解、从实验数据中辨识因果关系——这些过程耗时漫长、成本高昂，且受限于人类认知的带宽与偏见。AI 带来的关键突破在于，它能够在人类难以穷尽的高维解空间中高效探索，发现隐藏在数据深处的复杂模式与关联。这一能力体现在科研的多个核心环节：在假设生成阶段，AI 可从大规模数据中自动发现人类难以察觉的隐性规律，生成高质量的候选假设；在实验优化阶段，AI 与自动化实验平台结合，能够根据实时数据动态调整实验参数、优化实验流程，将传统依赖人工经验的反复试错转变为智能化的自适应探索；在高通量筛选阶段，AI 驱动的高通量实验技术能够快速执行大规模并行实验，在材料科学与药物发现领域，可从数百万候选方案中快速筛选出具有目标性质的新材料或药物分子，将从假设到验证的周期大大缩短。以上共同构成了 AI 加速科研探索的快速试错闭环，在此基础上，逆向设计则进一步实现了从试错到创造的跃迁，即直接从目标功能出发，生成符合需求的物质结构。如中科大团队提出的数据驱动方法结合主动学习与生成式人工智能模型，形成“生成-筛选-再训练”闭环设计框架，将三维力学隐身斗篷的设计时间大大缩短，为定制化骨植入物、渗透器件及力学隐身结构等工程应用奠定了重要基础。

总而言之，AI 为科研带来的并非某一环节的效率提升，而是核心能力的维度跃迁：通过神经算子等技术突破高维计算的效率瓶颈，通过物理信息神经网络弥合数据与机理的融合鸿沟，通过生成式模型拓展假设空间的探索边界，通过多尺度建模统一跨层级的描述框架，这整体上构成了 AI 驱动科研范式变革的核心动力。



趋势二

垂直领域科研大模型 加速成为科技创新的“新基础设施”

与通用大模型追求广而全不同，垂直领域科研大模型聚焦特定学科的专业知识与数据体系，通过定制化训练实现对复杂科学问题的精准建模与高效求解，能够更精准地理解专业术语、处理专业数据，从而显著提升科研效率和准确性。科研大模型的加快发展，正在推动科研模式向数据驱动与领域知识深度融合的智能化发现发展，在气候科学、天文观测、生命科学、药物研发等领域展现突出的应用价值。

生命科学是垂直科研大模型最活跃的战场。阿里云的 LucaOne 生物基础大模型基于 DNA、RNA 和蛋白质进行混合训练，数据涵盖超 16 万个物种的 12 亿条核酸序列和 6 亿条蛋白序列。复旦大学团队研发的女媧系列模型同样表现突出：女媧基因导航基础模型在超过 100KB 的远端调控关系预测上，精度较现有方法提升一倍以上；女媧生物分子结构大模型基于扩散模型进行蛋白质动态 3D 结构预测，动态精度比既有方法提高 50%，突破了 AlphaFold3 在动态结构预测上的局限。在药物研发方面，面向分子设计的 Uni-Mol 基座模型参数量达 1.1B，已在药物分子对接、OLED 发光分子设计、锂电池电解液配方设计等多个方向落地应用。清华大学 AIR 联合水木分子则推出 BioMedGPT-Mol，用户通过自然语言对话即可完成多项分子理解与生成任务，大幅降低了药物研发人员使用 AI 的门槛。

在气候科学领域，复旦大学联合上海科学智能研究院、上海创智学院推出的 PI@Climate 大语言模型，是国内领先的自研气候领域大语言模型，旨在为气候变化的科学研究、国际气候谈判和政策分析提供全面的知识支持。中国科学院青藏高原研究所联合阿里云发布的水能粮多模态推理大模型“洛书”，则集成了科学模型“思源”（HydroTrace）与千问系列推理及多模态模型，可对特定区域不同时间尺度的来水量和来源进行精准分析与预测，助力水资源管理中供水、发电与粮食生产需求的动态平衡。用户仅需自然语言即可完成对高维水文数据的推理分析和可视化，为区域能源时空一体化调度提供科技支撑。

在天文学领域，垂直科研大模型的落地尤为引人注目。国家天文台联合阿里云发布的太阳大模型“金乌”，基于超 90 万张太阳卫星图像完成微调训练，在 M5 级太阳耀斑预报上准确率超 91%，对守护国家空间安全意义重大。新一代天文大模型“星语 3.0”则已成功接入国家天文台兴隆观测站 Mini“司天”望远镜阵列，实现了自主控制望远镜观测、分析观测结果并智能推荐下一步观测计划的全流程闭环。未来，“星语”将接入预期至 2030 年拥有 72 架米级望远镜、每晚产生约 140TB 数据的“司天”项目，将科研人员从繁琐的观测操作中解放出来。

展望未来，垂直领域科研大模型呈现三大发展趋势。一是多模态融合将成为标配，科研数据天然具有图像、序列、时序信号等多模态特征，“金乌”、“洛书”等模型已展现出多模态推理的显著优势。二是科学模型与语言模型的深度耦合将进一步深化，“洛书”将专业科学模型与大语言模型协同工作的范式，有望在更多学科推广，使专业知识真正实现可对话、可推理、可决策。三是开源开放生态将加速创新扩散，LucaOne、BioMedGPT-Mol 等模型已全面开源，全球研究团队可在此基础上构建垂直领域模型，形成“基础模型—领域模型—应用场景”的良性飞轮。在算力资源仍存制约的背景下，聚焦垂直领域、以专业模型撬动科研效率提升，是一条兼具现实性与前瞻性的发展路径。可以预见，随着更多学科的深度参与和产研协同的不断深化，垂直领域科研大模型将成为推动我国科技创新的重要基础设施。

趋势三

AI 助力科研自动化和智能化， 逐步向 AI Scientist 迈进

传统上，科研活动高度依赖研究者的经验和直觉，这种依赖不仅限制了研究效率，也使得许多宝贵的研究经验难以传承和推广。随着大语言模型和多智能体系统的不断突破，AI 能够辅助科学研究，并将专家的经验 and 判断转化为明确的操作流程，并逐步演进为能够主动参与问题发现、实验设计与结果分析的协作者乃至共创者。这一转变的核心价值在于将科学家从文献梳理、数据处理、实验操作等大量重复性劳动中解放出来，使其得以聚焦于创造性思维与关键科学判断本身。

在科研助手层面，多个系统已展现出显著的效率提升。中国科学院大学他山协会开发的“他山·科研 IDE”，能够将文献、原始数据、中间分析与手稿草稿动态融合为可追溯的结构化知识流，研究者只需一句自然语言指令，系统即可自动完成从文献检索、数据下载、代码生成到结果可视化的全流程。Google 推出的 AI Co-scientist 基于 Gemini 2.0 构建了多智能体协同架构，包含生成、反思、排序、进化等六大核心智能体，据 Google Research 与帝国理工学院披露，AI Co-scientist 在计算分析中提出了与团队多年实验结果一致的候选解释。

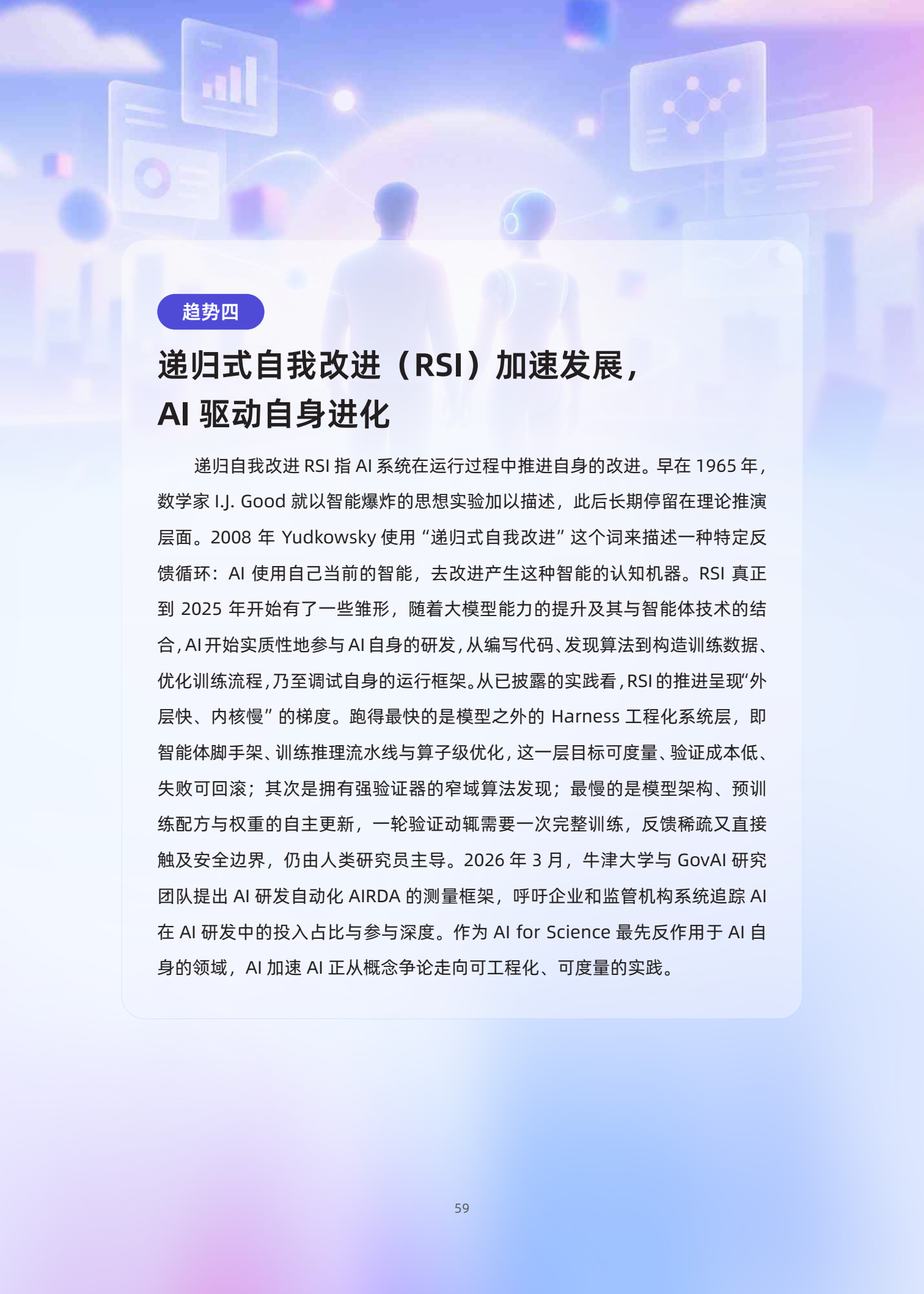
在平台层面，深势科技构建的玻尔科研空间站（Bohrium）定位为面向未来的统一、开放、智能的科研基础平台，既是科研人员的一站式门户，集成文献、数据、计算与实验资源，也是开发者的工具应用超市，使各类科研模型和软件能像手机应用一样被发布、共享和调用。此外，Science Navigator 平台收录超 2 亿篇文献和 9000 万名科研学者，

实现了基于 AI 的学术搜索、多模态检索和实时学术追踪，正积极打造干湿闭环、快速迭代的综合智能体平台。

在智能体层面，上海交通大学研发的通用科研智能体 SciMaster 实现了全学科 " 搜、读、算、做、写 " 全流程闭环。与之配套的 Agent-Ready at Scale 科研工具体系，通过将海量科研软件自动化部署为可被智能体直接调用的能力单元，显著降低了工具使用门槛，为大规模协作验证提供了关键支撑。

AI 的角色正进一步向 AI Scientist 迈进，即具备从自主提出假设、设计实验、执行验证到反思迭代的完整科研能力。Sakana AI 开发的 "The AI Scientist" 系统展示了这一可能性，能独立完成从文献综述、假说提出、实验执行到论文撰写的全流程，单次研究成本不到 15 美元。其最新迭代版本 AI Scientist-v2 已实现从开放式创意生成、四阶段实验管理、智能体树搜索到 VLM 评审反馈的全流程闭环。西湖大学蓝振忠团队的 Nova 系统将创意生成效率提升了 2.5 倍，生成想法的新颖率超过 80%，在新颖性评分上表现突出。斯坦福与哈佛大学提出的 POPPER 框架则实现了自动化假设验证，在生物学、经济学等六个领域展示了强大能力，与人类科学家相比将验证时间缩短至原来的 1/10。

AI 在科研中的角色可划分为三个阶段：工具阶段（人类全程监督）、部分自主智能体阶段（人类监督下自主执行任务）、完全自主阶段（AI 独立开展研究），当前正处于从第一阶段向第二阶段的过渡期，即科学家提出想法，AI 辅助执行，AI Scientist 更是处于极早期阶段。理想中的 AI 科学家应具备自主提出假设、设计实验、调用工具乃至控制物理设备的能力，更关键的是，当实验失败时，能像人类博士生一样分析失败原因、修正假设并开启新一轮迭代。而 LLM 目前在科研中仍存在实施漂移、领域智能不足、科学品味薄弱等典型失败模式，在深度创造性、无监督环境下的认知正确性以及复杂湿法实验操作等方面，仍难与人类科学家相媲美。从科研助手到真正的 AI 科学家，这条路还很漫长，链路中需要解决的问题众多，应保持谨慎乐观的态度。



趋势四

递归式自我改进（RSI）加速发展， AI 驱动自身进化

递归自我改进 RSI 指 AI 系统在运行过程中推进自身的改进。早在 1965 年，数学家 I.J. Good 就以智能爆炸的思想实验加以描述，此后长期停留在理论推演层面。2008 年 Yudkowsky 使用“递归式自我改进”这个词来描述一种特定反馈循环：AI 使用自己当前的智能，去改进产生这种智能的认知机器。RSI 真正到 2025 年开始有了一些雏形，随着大模型能力的提升及其与智能体技术的结合，AI 开始实质性地参与 AI 自身的研发，从编写代码、发现算法到构造训练数据、优化训练流程，乃至调试自身的运行框架。从已披露的实践看，RSI 的推进呈现“外层快、内核慢”的梯度。跑得最快的是模型之外的 Harness 工程化系统层，即智能体脚手架、训练推理流水线与算子级优化，这一层目标可度量、验证成本低、失败可回滚；其次是拥有强验证器的窄域算法发现；最慢的是模型架构、预训练配方与权重的自主更新，一轮验证动辄需要一次完整训练，反馈稀疏又直接触及安全边界，仍由人类研究员主导。2026 年 3 月，牛津大学与 GovAI 研究团队提出 AI 研发自动化 AIRDA 的测量框架，呼吁企业和监管机构系统追踪 AI 在 AI 研发中的投入占比与参与深度。作为 AI for Science 最先反作用于 AI 自身的领域，AI 加速 AI 正从概念争论走向可工程化、可度量的实践。

算法发现是最早的切入口, AI 开始产出服务于自身与通用计算的算法。谷歌 DeepMind 在这一方向推进最为系统。2022 年, AlphaTensor 通过强化学习发现更快的矩阵乘法算法, 在有限域即模 2 算术上将 4×4 矩阵乘法的标量乘法次数压缩至 47 次, 少于 Strassen 算法组合所需的 49 次, 并在 V100 GPU 与 TPU v2 上为大规模矩阵乘法带来 10% 至 20% 的实测提速, 成果发表于《自然》。2023 年, AlphaDev 发现新型排序算法, 将较短序列的排序速度最多提升 70%, 对超过 25 万元素的序列提升约 1.7%, 并被集成进每天被调用上万亿次的 LLVM libc++ 标准库。2023 年末, FunSearch 将大模型与进化搜索相结合, 在极值组合学的 cap set 问题与在线装箱问题上取得新构造, 超越了约 20 年来的已知最优结果, 同样发表于《自然》。2025 年 5 月发布的 AlphaEvolve 是一个由 Gemini 驱动的进化编码智能体, 它在复数域这一更通用的设定下以 48 次标量乘法完成两个 4×4 复矩阵相乘, 实现了对 Strassen 算法框架 56 年来的首次突破, 并同步优化了数据中心调度与加速器电路设计、加速了支撑自身运行的大模型训练, AI 优化 AI 的闭环初步形成。几乎同期, 日本 Sakana AI 与不列颠哥伦比亚大学团队沿自指式自我改写的另一条路线推出 Darwin Gödel Machine, 让智能体反复改写自身代码, 将其在软件工程基准上的得分从 20.0% 提升至 50.0%, 并将实现全部开源。

从算法优化走向系统优化, AI 开始为自身挣回算力并重塑研发流程。据 DeepMind 2026 年 5 月披露, AlphaEvolve 已在谷歌内部基础设施优化中体现价值, 并出现用 AI 辅助下一代芯片设计等场景, 相关系统能力后续已向企业端开放。前沿公司也在用模型重塑自身研发, OpenAI 于 2026 年 5 月开始招募专职应对 AI 自我改进挑战的安全研究员, 为 AI 训练 AI 的可能性预做治理准备。更具标志性的是 RSI 从大厂内部项目变成独立赛道。2026 年 5 月, 由田渊栋、Richard Socher 等八位研究者创立的 Recursive Superintelligence 以此为主营方向。其价值在于提供了第一份系统性证据: 一个自动化研究循环能在固定预算训练配方、被社区打磨两年的训练速度榜单与 GPU 算子优化三类任务上同时超越长期人工优化的最优解, 且收益来自数十项修改的复合叠加而非单点技巧。它也印证了自我改进会带来复利式算力需求这一产业逻辑。

国内加快布局, 阿里巴巴围绕智能体自进化与训练自动化形成系列研究进展。阿里通义实验室于 2025 年 11 月发布 AgentEvolver, 通过自我提问、自我导航、自我归因三

个机制，使智能体系统在无人工标注数据的条件下实现自进化，将 Qwen2.5-7B 的平均智能体任务表现提升 29.4 个百分点，其中自我归因机制使达到基线最终性能 90% 所需的训练步数减少一半以上，相关成果已开源。更早发表于 ICLR 2025 的 AutoIF 工作以执行反馈的自我博弈提升大模型指令遵循能力，同样摆脱了对人工标注的依赖。2026 年 6 月，通义实验室联合中国科学院深圳先进技术研究院等机构发布 EvoTrainer，让智能体强化学习阶段的训练策略与训练框架协同进化，在同数据、同代码库、同评测协议条件下，于数学求解、竞赛编程和仓库级软件工程任务上达到或超过人类研究员设计的强化学习方案，其中长程软件工程任务的增益最大。这项工作值得注意之处在于，它把自动改进的对象从训练配方本身扩展到解释训练信号的 harness，与前述外层先动的规律一致。在基础设施层面，SimAI 大规模训练模拟器已实现模拟环境与真实训练 98.1% 的平均对齐度，为大模型训练优化提供了数字演练场。

RSI 目前更接近渐进提效而非自主递归，治理议题同步升温。主流前沿实验室对此总体保持克制。DeepMind 将递归改进列为从 AGI 走向 ASI 的四条潜在路径之一，与规模扩张、范式转变和群体智能体并列，但其首席执行官 Demis Hassabis 指出，当前系统尚不能独立提出科学问题与生成假说，AlphaEvolve 的运行仍需人在回路监督。Anthropic 也在其安全立场材料中表示递归自我改进并非必然。总体来看，RSI 已在算法、工程与基础设施三个层面带来真实的效率红利，并持续压缩 AI 自身的迭代周期，但尚未形成 AI 设计下一代 AI 的无人闭环。这一技术同时决定 AI for Science 的演进速度与安全可靠难度，面向自进化系统的测量框架、人机责任划分与验证机制将成为下一阶段技术与治理的重要议题。

现实挑战与路径建议

AI for Science 前景广阔，但从技术突破到范式确立仍面临多重现实挑战。一是**高质量科学数据严重短缺**。海量、高质量的科学数据是 AI4S 发展的根基，但数据获取成本高昂、标注瓶颈突出、共享机制缺失三重问题交织制约着模型能力的提升。科研数据长期分散在不同实验室和机构中，数据孤岛现象普遍，数据所有权与科研竞争关系进一步阻碍了开放共享。二是**模型可解释性不足**。多数 AI 模型仍为黑箱模式，难以解释预测结果与科学机制的内在关联，导致部分成果难以被学界广泛认可，在临床医学、高端制造等关键领域的应用尤为受限。可解释 AI 技术正在发展，但在复杂科学问题中的应用仍处于早期阶段。三是**预测-验证链条不畅**。AI 的科学发现能力呈指数级增长，但人类的实验验证和产业化能力仍在线性爬坡。AI 预测结果缺乏统一评估体系，自动化实验能力不足，大量预测成果堆积在实验室难以转化为实际生产力。四是**复合型人才严重紧缺**。AI4S 要求研究者同时理解科学问题的本质与 AI 的求解方法，但传统人才培养体系尚未适应这一要求。科学家的角色需从执行者转向设计者和评判者，现有学术评价体系也面临相应调整的需求。

针对上述挑战，AI4S 的发展需从基础建设与方向突破两个层面协同推进。在**基础建设层面**，需**夯实数据、平台、人才、治理四大支柱**。加快推进关键领域科研数据可信空间建设，加强数据标准化与共享机制创新，打破数据孤岛；面向重点应用领域构建 AI4S 共性技术研发平台，推动算力、工具与实验资源的互联互通，并将科学数据标注、模型训练等关键环节纳入科研基金支持范围；构建“科学导师 +AI 导师”双导师制等复合人才培养模式；制定 AI 模型准确性、可重复性和可解释性的评估标准，建立负责任、透明的 AI 科研使用规范与伦理共治体系。在**方向突破层面**，**AI4S 的演进将不再局限于单点模型突破，而是走向科研全流程的系统性变革**。一是扩展 AI 科研的动作空间，将更多学科的研究流程工程化、接口化，形成可被智能体直接调用的标准化管线，尤其在生物、化学等依赖湿法实验的领域，通过自动化实验平台构建“设计-执行-验证”的闭环，打通从预测到验证的关键瓶颈；二是建立更科学的评测框架，从追求静态任务分数走向能够衡量发现

能力、创新性与长期科学贡献的评价体系。最终，AI 将与人类科学家形成人类提出深刻问题与价值导向，AI 承担大规模探索与验证的深度协同，推动科研活动迈入高效、精准、开放的新阶段。

5

智能向善， 技术普惠与可持续发展

人工智能技术的发展正在进入一个关键转折点。当 AI 的能力边界不断扩展，一些更根本的问题浮现：技术应该服务于谁，以何种方式发展，对社会和环境产生怎样的长期影响？我们针对 AI 发展过程中最值得担忧的问题进行调研，37.9% 的受访者认为隐私安全与数据滥用问题最为急切；22.7% 的调研者担心就业替代与社会不平等加剧，此外 12.3% 左右的受访者担心 AI 失控或产生不可预测的风险，以及 AI 对人类自主思考能力的削弱。

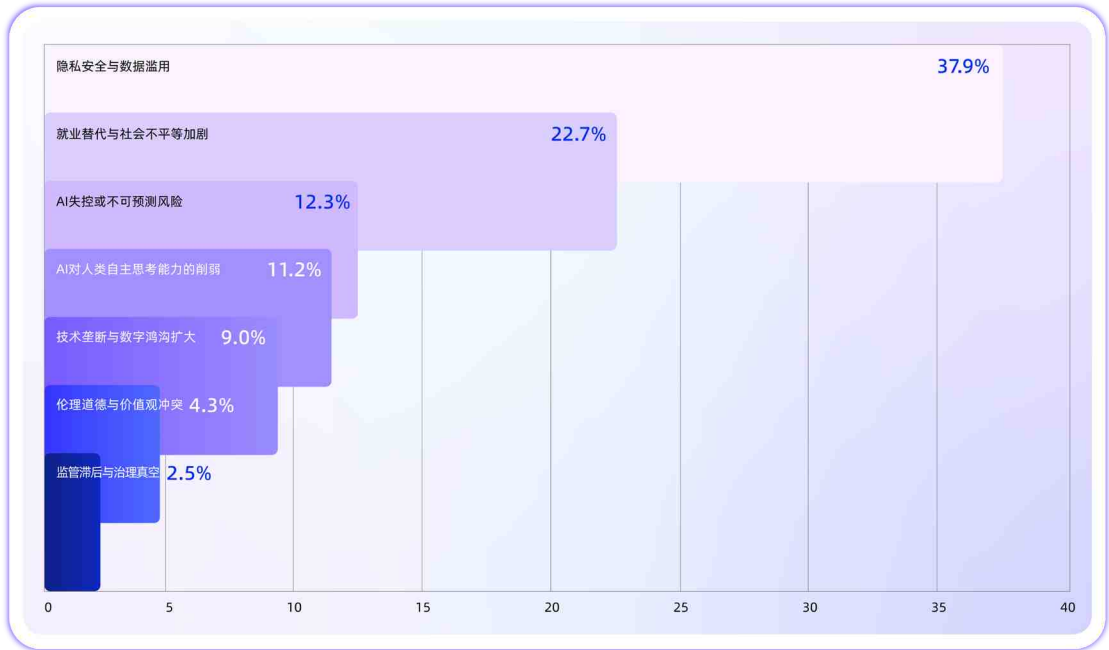


图 24 未来 3 年 AI 发展最值得担忧的问题分布
数据来源：阿里云研究院调查问卷

基于此，负责任 AI 的理念逐步走向台前，开放性、包容性、可持续性正在成为衡量 AI 进步的重要维度。负责任 AI 的实践建立在若干关键技术支柱之上：可解释 AI 通过注意力机制可视化、特征重要性分析等技术手段，揭开算法黑箱的神秘面纱，使 AI 决策过程变得透明可审计；公平性工程运用去偏见算法、对抗性去偏见训练、公平性约束优化等技术，系统性地识别和缓解训练数据中的历史偏见，确保 AI 系统不会歧视特定群体；隐私保护技术如联邦学习、差分隐私、同态加密等，使得 AI 模型能够在不暴露原始数据的前提下完成训练，解决数据使用与隐私保护的矛盾；鲁棒性与安全保障通过对抗样本检测、模型水印技术、持续监控机制，防范 AI 系统被恶意利用或产生有害输出。这些技术创新构成了负责任 AI 的技术底座，将抽象的伦理原则转化为可度量、可验证、可改进的工程实践。

以负责任 AI 为价值主线，全球正在形成多层次的治理共识，确保 AI 技术服务于人

类共同福祉而非加剧社会分化。当前开源模型的普及、技术平权的推进，更让 AI 技术普惠成为现实，让不同地域、不同背景的组织与个人都能公平获取、使用 AI 技术，真正让 AI 创新成果惠及更多群体。以此为基，智能向善、技术普惠与可持续发展，成为新时代人工智能发展的核心方向，也推动 AI 在价值与技术的双重支撑下，朝着更具温度、更可持续的方向迈进。

趋势一

开源生态迭代升级， 推动 AI 应用民主化纵深发展

开源模式正深刻重塑 AI 技术的获取门槛与创新路径，其作用体现在两个层面。一是降低模型获取门槛，加速创新扩散。当前 AI 开源已超越单一模型权重开放，逐步形成覆盖算法模型、高质量数据集、全栈工具链及协同平台的完整生态。依托开源框架、工具和预训练模型，开发者可对 AI 能力进行灵活调用、高效微调与持续优化，快速适配垂直场景需求。将原本集中于少数科技企业的创新能力转化为可被更广泛主体复用的公共技术资源。中小企业、科研机构 and 独立开发者无需从头承担大模型训练所需的高额算力与人才成本，即可基于已有模型开展微调、蒸馏、部署和应用创新，推动 AI 创新由少数机构主导转向更广泛的生态协同。二是扩大技术的可审查与可改造空间，使 AI 能够真正进入数据敏感、知识密集的行业。代码与数据的开放性使 AI 系统的训练来源、运行机制和决策过程在一定程度上可被审查与追溯，增强了系统可信性与可解释性。更现实的驱动力来自部署形态本身：在医疗、金融、制造与政务等领域，机构普遍要求模型权重与推理过程完整驻留在本地机房或专有云内，训练数据不出域，模型版本可冻结、可回滚、可审计，这类约束是闭源接口服务难以满足的。开发者由此可以结合本地数据、业务流程和合规要求对模型进行针对性优化，并在私有环境或边缘设备中部署，这种面向具体场景的深度定制能力，往往是闭源模型难以全面覆盖的。

国产开放模型已成为全球开放生态的重要供给力量。阿里 Qwen、DeepSeek、智谱 GLM、月之暗面 Kimi 等模型持续迭代，在推理、代码、长上下文和多模态等方向形成差异化优势，在多项公开评测中进入第一梯队。其中 Qwen 的规模效应最为突出，2026 年 8 月 14 日 Qwen3.8 系列开源时，阿里云披露其已累计向全球开放 460 余个模型，Qwen 家族全平台累计下载量超过 30 亿次，衍生模型超过 30 万个。Hugging Face 同期报告显示，仅该平台托管的 Qwen 衍生模型即达 151,448 个。

从行业整体看，Hugging Face 2026 年春季报告显示，过去一年全球开源模型下载量中，中国研发的模型占 41%，首次超过美国的 36.5%；工信部在 2026 年 8 月国新办发布会上披露，国产开源大模型全球累计下载量已突破 100 亿次，居全球首位。在调用侧，国产开源模型在 OpenRouter 上的 token 占比从 2024 年末的不到 1.2% 快速攀升；2026 年 3 月 15 日当周，中国 AI 大模型周调用量达 4.69 万亿 Token，连续第二周超越美国。

在生态各环节的发展上，AI 开源也呈现出清晰的升级方向。数据领域由规模扩张转向来源许可、质量筛选、污染检测、隐私保护及合成数据治理；模型工程延伸至强化学习、推理蒸馏、混合专家、量化和领域适配，评价维度也由参数量扩展到单位任务成本、时延、吞吐和能耗；vLLM、llama.cpp 等开放运行时持续适配云端、国产算力和端侧设备，推动模型从“可以下载”走向“可承受成本运行”。协作平台在保留模型、数据集与应用演示的聚合功能之外，向上生长出应用集成与智能体互操作层。截至 2026 年 8 月，Hugging Face 已托管超过 300 万个公开模型，服务超过 1800 万名开发者，从资源存储库演化为大规模的模型评估、演示与协同开发网络；国内阿里云魔搭社区截至 2026 年 3 月已上架 17 万个开源模型，服务全球超过 2500 万名开发者，九个月内新增 10 万个模型，覆盖大语言模型、对话、语音、文生图、图生视频等多个领域，是中国规模最大的 AI 模型社区。生态上层则逐步形成检索增强、工作流编排、工具调用、记忆、身份、权限、沙箱与观测等基础设施。模型上下文协议 MCP 推动智能体以统一方式连接工具和数据源，Agent2Agent 协议面向不同厂商和框架之间的智能体通信与协作，两者已分别于 2025 年 12 月和 2026 年 8 月归入 Linux 基金会旗下的 Agentic AI Foundation，协议治理由单一厂商主导转向中立托管。开放竞争由模型数量进一步延伸到工具兼容、系统连接和业务交付能力。

产业部署的重点则由可用转向可信、可运营。企业不仅要管理模型，还要持续追踪数据集、适配器、运行镜像和评测结果之间的版本关系，并处理许可证兼容、恶意文件、权重篡改、安全评测和版本回滚等问题。模型卡、数据卡、来源证明、文件签名、漏洞扫描和 AI 物料清单正在进入开放工具链。开放生态的下一阶段，不只是让模型跑起来，而是让来源可查、版本可控、效果可测、风险可管。

展望未来，全球开放模型生态将呈现四个方向。第一，开放形态由简单的开源与闭源二分，走向权重、代码、数据、评测和许可多维度的分级、可验证开放。第二，技术工具链将升级为可信 AI 供应链，把模型、数据、代码、镜像和评测纳入统一的版本与安全管理。第三，轻量化将从缩小参数规模转向能力、成本与硬件协同，云端前沿模型、本地专业模型和端侧小模型形成分层组合。第四，模型社区将进一步延伸为开放智能体生态，协议、工具与身份权限体系成为新的竞争面；与之并行的是主权化部署需求的上升，随着数据驻留、模型更新权、密钥控制和审计要求不断提高，具备透明、可修改和可本地部署条件的开放模型，将成为政府和企业的重要技术选项，产业价值也将更多转向托管推理、工程优化、安全合规和行业服务。总体来看，开放模型生态正在从资源开放走向系统开放，从开发者可用走向产业可运营，其内在驱动力也在从人人可得的成本逻辑转向自主可控的主权逻辑。决定其长期影响力的，不再只是模型性能和下载规模，而是开放质量、数据治理、部署成本、互操作能力和治理可信度能否同步提升。

趋势二

负责任 AI 治理体系走向制度化和常态化

随着 AI 在经济社会各领域的深度渗透，治理和安全成为全球关注的问题，各国纷纷围绕 AI 治理进行立法和政策引导，相关国际组织也积极参与到 AI 治理的标准制定和规范建设中。

在区域和国家层面，各地治理模式逐步成型。欧盟以《人工智能法案》为标志，构建了基于风险分级的治理体系；美国坚持“行业驱动、创新优先”的治理逻辑，通过《国家人工智能倡议法案》推动算力基础设施建设，以战略引领与指导性政策引导产业自律并形成技术标准；中国提出“发展、安全、治理”三位一体的理念，通过《生成式人工智能服务管理暂行办法》等政策落地实施，同时发布《人工智能安全治理框架》2.0 版本，在技术内生安全风险、技术应用安全风险之外新增了应用衍生安全风险，特别指出 AI 技术应用对于社会、环境秩序和伦理规范带来的挑战，并提出了“安全左移”的技术应对策略，即在 AI 全生命周期中嵌入安全考量。

国际组织层面，联合国、UNESCO、ITU、ISO 等持续推动 AI 治理合作。其中，联合国启动“人工智能治理全球对话”机制，帮助建立以国际法、人权和有效监督为基础的安全、可靠和值得信赖的人工智能系统；促进治理制度之间的相互协同，调整规则、减少障碍和促进经济合作；鼓励所有人都能获得的开放式创新，包括开源工具等。ITU 启动“AI 标准全球影响：从治理到行动”计划，推动 AI 治理的标准化和可操作化；国际标准化组织（ISO）于 2025 年 12 月召开“国际 AI 标准峰会”，促进全球 AI 标准协同，ISO/IEC 42001（AI 管理体系）和 ISO/IEC 23894（AI 风险管理）正成为全球通用的合规与保障框架。

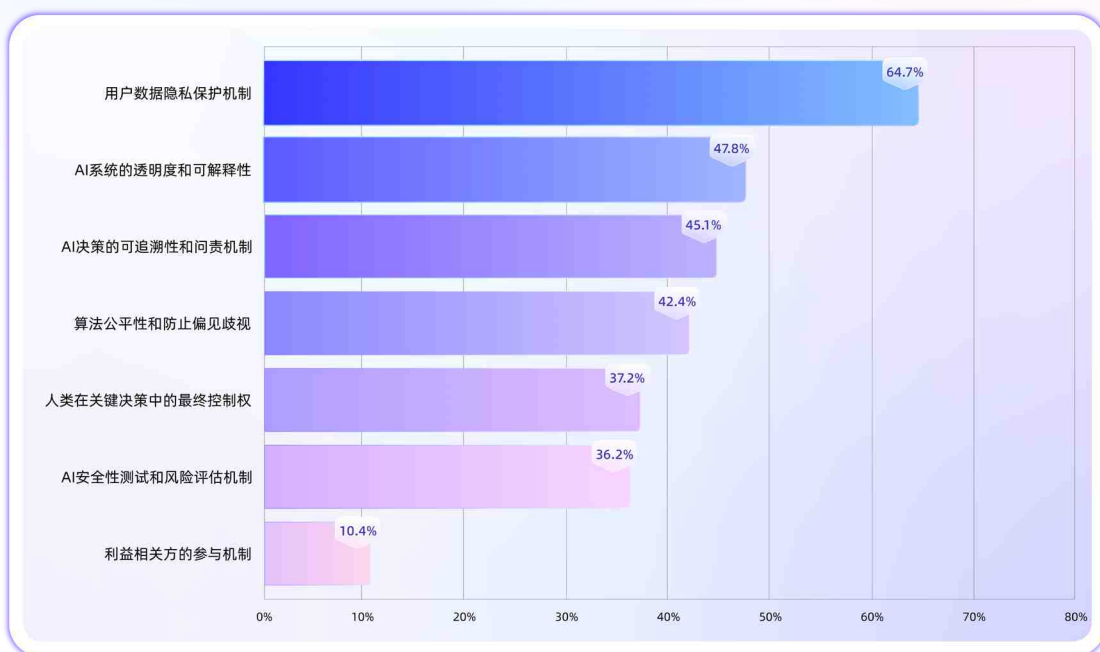


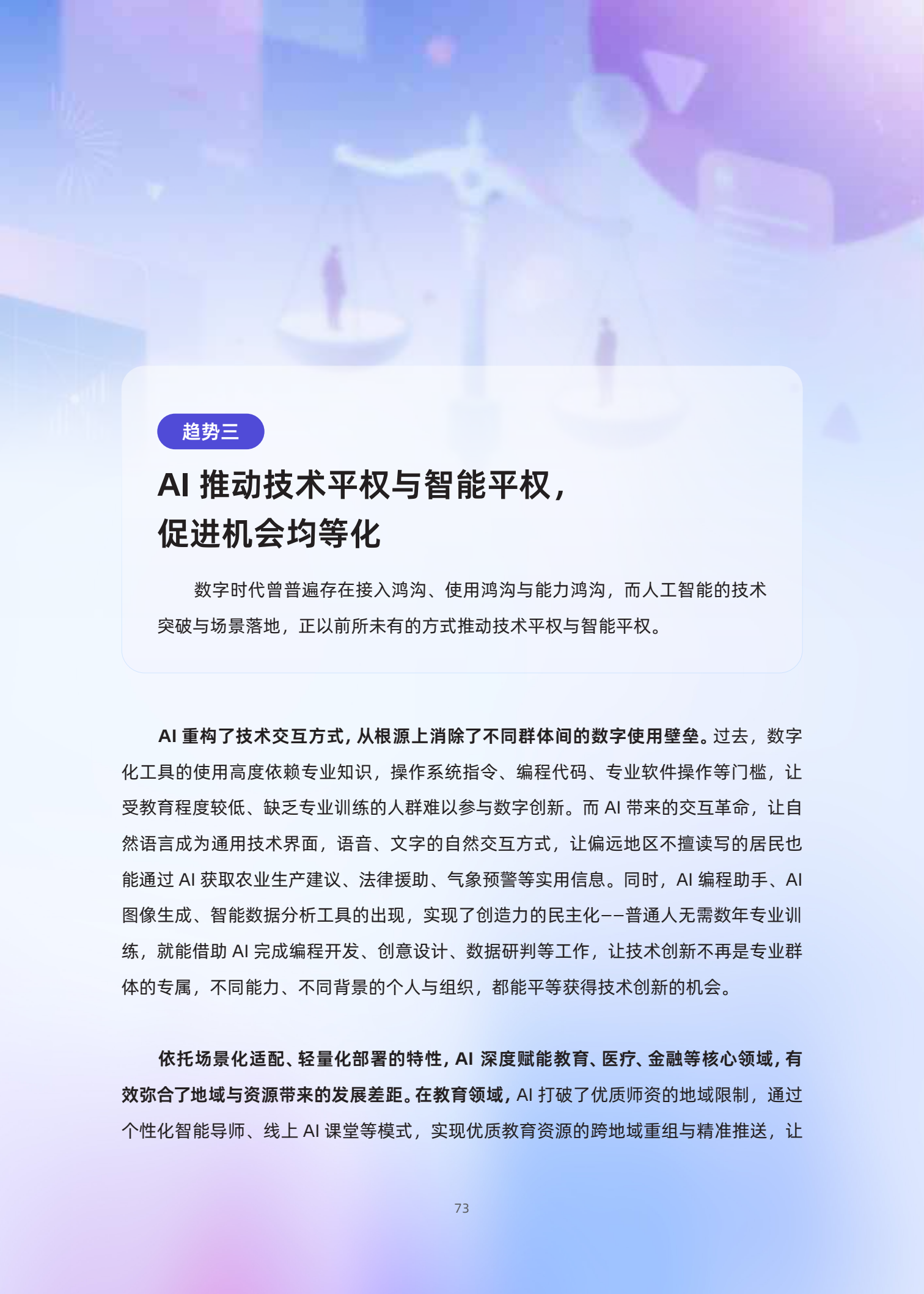
图 25 负责任 AI 治理体系的关键要素调研结果分布
数据来源：阿里云研究院调查问卷

整体上看，AI 治理的核心在于坚守“人本、可信、可问责”主线，在释放技术创新活力的同时，防范系统性风险。主要关注点包括 AI 的可解释性、透明性、公平性、鲁棒性、隐私保护和以人为中心的 AI 等方面，通过制度化、工程化、过程化的方法进行治理落地。主要包括几个方向的治理：**一是数据治理**，聚焦训练数据合法性、质量代表性、隐私保护与数据投毒防范，筑牢可信 AI 的基础；**二是算法治理**，破解偏见歧视、黑箱不可解释、舆论操控等问题，推动算法透明化与可问责；**三是模型治理**，涵盖模型全生命周期的训练合规、部署安全、迭代审计与退役处置，防范跨场景风险外溢，应对大模型涌现能力带来的不可预测性、对抗攻击、漏洞被滥用后全球扩散；**四是权利与安全治理**，随着智能的发展，AI 从工具走向自治行动者，其决策链条更长、外溢性更强，责任更难界定。

监管政策的完善与落地，进一步强化了伦理安全的刚性约束。企业作为治理执行主体，正推动治理转向前置与嵌入式，并实现工程化落地：对于模型研发企业，构建覆盖模型训练、部署、迭代全生命周期的治理体系，建立数据合规审计、明确能力边界、落实版本管理，并开放第三方审计接口接受社会监督。对于 Agent 开发应用企业，应构建嵌入式治理与持续优化闭环的系统工程，强化与模型提供者的责任协同，明确二次开发中的风险防控义务；将治理要求嵌入应用流程，实现风险的实时监测与快速纠偏；建立分层

透明机制，向公众告知算法应用情况，向监管提供可审计证据。

AI 治理走向制度化和常态化的关键，在于构建可衡量的治理框架。企业应构建四维一体的 AI 治理体系：在风险识别维度，建立覆盖数据、模型、应用全链条的风险评估机制；在能力构建维度，重点发展可解释 AI、安全审计、风险监测等核心技术能力；在协同治理维度，推动政府、企业、技术社群、学术机构的协同共治；在评估改进维度，建立基于数据的动态评估机制，持续优化治理实践。以此推动 AI 治理从原则共识走向能力工程，从单点突破走向体系化建设，从软约束走向硬支撑。



趋势三

AI 推动技术平权与智能平权， 促进机会均等化

数字时代曾普遍存在接入鸿沟、使用鸿沟与能力鸿沟，而人工智能的技术突破与场景落地，正以前所未有的方式推动技术平权与智能平权。

AI 重构了技术交互方式，从根源上消除了不同群体间的数字使用壁垒。过去，数字化工具的使用高度依赖专业知识，操作系统指令、编程代码、专业软件操作等门槛，让受教育程度较低、缺乏专业训练的人群难以参与数字创新。而 AI 带来的交互革命，让自然语言成为通用技术界面，语音、文字的自然交互方式，让偏远地区不擅读写的居民也能通过 AI 获取农业生产建议、法律援助、气象预警等实用信息。同时，AI 编程助手、AI 图像生成、智能数据分析工具的出现，实现了创造力的民主化——普通人无需数年专业训练，就能借助 AI 完成编程开发、创意设计、数据研判等工作，让技术创新不再是专业群体的专属，不同能力、不同背景的个人与组织，都能平等获得技术创新的机会。

依托场景化适配、轻量化部署的特性，AI 深度赋能教育、医疗、金融等核心领域，有效弥合了地域与资源带来的发展差距。在教育领域，AI 打破了优质师资的地域限制，通过个性化智能导师、线上 AI 课堂等模式，实现优质教育资源的跨地域重组与精准推送，让

偏远地区的学生也能获得与城市同等的学习指导。联合国儿童基金会（UNICEF）在不丹、乌兹别克斯坦、老挝等国的研究项目显示，AI 教育系统的引进显著提升了学生的数学学习效果，增强了参与度，并为教师提供了基于研究的数字化工具支持。在医疗领域，AI 正成为基层医疗服务的重要支撑。国内部分地区部署的基层 AI 辅助诊断系统，已使基层诊断符合率和电子病历规范率显著提升，弥补了乡村医生的经验短板，让基层群众平等享有优质的医疗诊断服务。在金融领域，AI 风控模型通过多维度非结构化数据构建信用评估体系，破解了小微企业、低收入群体因缺乏抵押资产、信用数据不足导致的信贷难题，降低了金融服务门槛，让中小微主体与弱势群体能平等获得发展所需的金融支持。

AI 在无障碍领域的深度应用，更是让平权发展具备了包容性。世界卫生组织《全球辅助技术报告》显示超 25 亿人需至少一种辅助产品，但多数国家覆盖率严重不足。而 AI 正成为这一群体融入数字社会、平等参与发展的核心支撑。针对视觉障碍人群，AI 驱动的图像识别与场景描述技术准确率高，智能视觉助手显著提升了视障人士的独立出行能力与日常生活自主性；针对听觉障碍人群，实时语音转文字技术支持多语种实时互译，让听障人士顺畅参与社交、平等进入主流职场。AI 屏幕阅读器、手语识别与生成技术、智能环境描述工具等，让残障人群能独立使用智能设备、参与线上工作与会议，改变了残障人士成为技术进步最终受益者的现状，通过技术赋能实现了真正的包容性发展。

AI 推动的技术平权与智能平权，并非单一技术的落地结果，而是技术创新、政策引导与社会协作的共振产物。2026 年政府工作报告提出要“完善适应人工智能技术发展促进就业创业的措施”，并明确提出“实施超大规模智算集群、算电协同等新基建工程”，体现智能向善、创新和绿色发展。要让平权发展成为常态，需要构建 AI 产品普惠标准，将无障碍设计、包容性开发纳入关键领域 AI 产品的研发要求，同时推动 AI 技术的轻量化、低成本部署，降低欠发达地区与中小微主体的 AI 应用成本。唯有让技术创新始终朝着普惠共享的方向迈进，才能让 AI 真正成为缩小发展差距、实现机会均等的核心力量，让不同地域、不同条件的个人与组织，都能在智能时代平等享有发展的机遇。



趋势四

绿色算力与低碳实践并行推进， AI 可持续发展进入议程

大模型参数量的迅猛增长，直接拉高了智能算力的消耗。IEA 预测，到 2030 年全球数据中心电力消耗将从 2024 年的 415 TWh 增至约 945 TWh，新增的 530 TWh 中，绝大部分来自 AI 训练与推理工作负载的增长。我国的算力中心用电需求也在快速增长。据中国信通院数据，2025 年我国算力中心用电量为 1960 亿千瓦时，占全社会用电量比重 1.89%，但同比增速达 18.07%，远超全社会 5% 的用电增速，预计 2030 年我国数据中心用电量将达 7000 亿千瓦时（约等于 80 吉瓦的持续负荷），占全社会用电量约 5.3%。

面对快速增长的算力和电力需求，绿色算力与低碳实践加快推进。2026 年国务院正式将算力网络纳入“六网”（水网、电网、交通网、通信网、算力网、物流网）统筹规划，标志着算力基础设施的战略定位达到前所未有的高度。2026 年 3 月，“算电协同”进入政府工作报告中，将高速增长的算力需求与清洁能源在供需两侧形成良性互动。2026 年 5 月 8 日，国家发展改革委、国家能源局、工业和信息化部、国家数据局四部门联合印发《关于促进人工智能与能源双向赋能的行动方案》，旨在构建人工智能与能源发展双向赋能、深度融合的良性生态。方案围绕“能源支撑人工智能发展”和“人工智能赋能能源转型”两条主线，部署了 29 项重点任务，这一政策的出台标志着“算电协同”从技术尝试正式提升至国家战略整合层面。

大型科技企业的数据中心正逐步加大绿色清洁能源的使用，路径已趋多元。一是绿电交易与绿证采购，如阿里云通过跨省区绿电、分布式绿电、省内海上风电等渠道探索清洁电力利用，五大自建基地也已启用清洁能源；二是风光等绿电直连（直供），2025 年以来国家算力枢纽节点直连项目已从试点走向百万千瓦级规模化复制，如阿里云与中国联通合作的青海三江源绿电智算融合示范园，实现风光绿电全链直供，已入选国家绿色数据中心和算力电力协同典型案例；三是氢能试点，阿里云 2022 年已在杭州仁和基地启动 25kW 级氢能发电试点，未来方向主要是替代柴油发电机作为备用电源、结合风光构建零碳微电网，但现阶段成本较高、收益尚不明显；四是参与虚拟电厂试验，目前仍处于探索期。随着 AI 推理负荷可迁移性逐步增强、储能成本持续下降，数据中心有望在不影响核心业务的前提下，在一定范围内提供可控负荷响应并参与电力市场交易。

现实挑战与路径建议

尽管 AI 向善与普惠发展态势向好，但仍面临多重结构性挑战。全球各个国家因文化传统、发展阶段不同，在隐私保护、公平性定义等方面难以形成统一共识，规则碎片化增加了跨国 AI 应用的合规成本。技术普惠与商业利益的冲突持续存在，头部企业在开源共享与知识产权保护、普惠部署与盈利目标之间的平衡难度较大，部分低成本普惠方案因缺乏商业回报难以规模化推广。长期社会影响的不确定性依然凸显，AI 对就业结构的深层重塑、算法偏见的隐性传导等问题，可能引发新的社会矛盾，对社会治理能力提出更高要求。

应对上述挑战，需构建多方协同的治理与发展体系。政策层面，推动国际组织牵头制定兼容性治理框架，基于分级分类原则协调各国监管差异，为跨国应用提供合规指引；鼓励政府出台普惠性政策，对低成本 AI 方案、开源生态建设给予补贴支持，平衡商业利益与社会价值。技术层面，持续强化可解释 AI、隐私计算等核心技术研发，提升 AI 系统的透明度与可控性，从源头规避伦理风险；推动开源社区与企业协同，构建低成本、易部署的普惠 AI 技术体系。社会层面，完善数字素养教育体系，覆盖不同年龄、群体，缩小能力鸿沟；建立多方参与的伦理审查机制，吸纳政府、企业、科研机构、公众代表共同参与 AI 治理，确保技术发展符合社会共识。

出品团队

顾问指导

刘湘雯 阿里云智能集团副总裁、市场营销总裁

策划编写

薛 达 阿里云智能集团研究院负责人

陈雪琴 阿里云智能集团研究院 高级研究专家

创意设计

张师华 阿里云智能集团设计部 创意设计专家

