

企业级智能体技术与应用 研究报告

(2026 年)

中国信息通信研究院人工智能研究所

三六零安全科技股份有限公司

2026年6月

版权声明

本报告版权属于中国信息通信研究院和三六零安全科技股份有限公司，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和三六零安全科技股份有限公司”。违反上述声明者，编者将追究其相关法律责任。

前 言

随着智能体技术在自主决策、多模态交互、复杂任务执行能力等方面的突破，智能体正逐步从辅助型效率工具向业务核心引擎转化。企业级智能体凭借深度业务融合、全流程闭环、私有化部署等核心优势，渗透至多种业务场景，赋能千行百业，呈现出决策自主化、纵深垂直化、体系规模化的鲜明特征，成为推动企业数智化转型的关键抓手。

本报告重点围绕企业级智能体的发展概述、技术能力、运营管理、应用实践、趋势展望五大篇章展开，加速企业级智能体规模化落地应用，促进产业发展。**发展概述方面**，报告对企业级和消费级智能体进行分析，论述发展企业级智能体有助于培育智能原生企业，驱动新质生产力跃迁。**技术能力方面**，分析企业级智能体自上而下的开发路径，围绕分层技术架构、动态规划决策、记忆工具增强、多智能体协同、自动化部署等展开讨论。**运营管理方面**，聚焦智能体全生命周期管理、业务运营价值、评估测试体系，保障企业级智能体稳定、高效、安全运行。**应用实践方面**，通过展示智能体在金融、政务、工业、教育、医疗等标杆场景上的应用案例，系统呈现出企业级智能体的落地成效。**趋势展望方面**，从技术升级、应用创新与生态融合等角度描绘企业级智能体的未来图景。

企业级智能体作为人工智能深化应用的重要标志与关键载体，依托技术革新、产业集聚与政策引导的协同推进，塑造健康繁荣的生态格局，为高质量发展注入强劲智能动力。当前，企业级智能体

技术正处于快速发展阶段，其技术、应用、生态研究工作还将持续深化开展，报告中如有不足之处还请各方专家读者不吝指正。



目 录

一、企业级智能体发展概述	1
（一）发展现状：智能体演进驱动企业级与消费级双轨并进	1
（二）需求牵引：企业级智能体助力夯实智能原生企业根基	3
（三）范式革新：企业级应用落地铸就新质生产力核心引擎	6
二、企业级智能体技术能力	8
（一）一站式智能框架构建，赋能企业级渐进式开发	8
（二）企业级知识高效存储，实现业务规划动态调优	10
（三）多智能体群体化协作，催生智能互联价值释放	14
（四）私有化部署方案加持，适配企业稳定可靠要求	16
三、企业级智能体运营管理	18
（一）多维系统集成与协同，筑牢高效合规治理根基	18
（二）全生命周期精细管理，支撑企业战略系统规划	19
（三）深层次挖掘运营价值，描绘企业新兴市场版图	21
（四）全方位评测体系构建，保障产品质量卓越交付	23
四、企业级智能体应用实践	26
（一）驱动金融业务流程优化，开启财富管理新纪元	27
（二）提升政务公共服务效能，实现便民利企新突破	30
（三）贯通工业生产关键环节，树立提质增效新标杆	32
（四）推动教育管理模式变革，激活因材施教新体验	36
（五）赋能医疗资源精准调配，引领全民健康新征程	38
五、企业级智能体趋势展望	41
（一）技术升级：从“被动响应”到“自主智能”的能力进阶	41
（二）应用创新：从“辅助支持”到“超级协作”的价值革新	43
（三）生态融合：从“单点突破”到“携手智变”的格局重塑	44

图 目 录

图 1 企业级智能体构建与运营平台框架	10
图 2 华院智能体平台总体框架	14
图 3 企业级对话式智能体平台框架	23
图 4 智能体通用评估体系	26
图 5 企业级智能体评估业务体系	26
图 6 企业级智能体行业应用图谱	27
图 7 某银行智能体功能框架	29
图 8 某市人工智能服务平台框架	32
图 9 金现代配料智能体适用行业	35
图 10 陕铁院校园督导智能体功能框架	38
图 11 睿宾医疗智能体功能框架	41

一、企业级智能体发展概述

（一）发展现状：智能体演进驱动企业级与消费级双轨并进

2025 年 8 月，国务院印发《关于深入实施“人工智能+”行动的意见》，提出要鼓励有条件的企业将人工智能融入战略规划、组织架构、业务流程等¹。随着人工智能技术的持续突破，基于大模型的新一代智能体已具备感知、规划、记忆、行动和使用工具的能力，正从概念验证走向规模化落地，推动生产力变革，呈现出消费级与企业级双轨并进的发展格局。在智能体多项核心技术能力的加持下，进一步加速通用人工智能技术创新，助力实现“感知智能”到“行动智能”的智能跃迁。

1. 智能体的兴起与 AGI 的曙光

智能体是指能够感知环境并利用工具采取行动以实现特定目标的代理。智能体以大模型为智能底座，具备自主感知、理解、规划、决策、记忆、行动和使用工具的能力，能够自动化执行复杂任务，具有自主性、交互性、反应性和适应性等基本特征。

智能体核心技术能力加持，自主决策执行能力凸显，加速通用人工智能的实现步伐。2026 年以来，智能体正在从概念验证走向实践落地。一是智能体自身能力与大模型深度融合，通过强化自主感知、深度理解和认知推理能力，进一步带动智能体能力提升。同时，基于分层规划和动态调整、跨任务记忆与学习、精准行动和多工具调用等

¹ https://www.gov.cn/zhengce/zhengceku/202508/content_7037862.htm?sharetype=link

多项核心技术能力，智能体的泛化认知水平得到进一步提升。二是智能体展现出多任务执行、多场景适应、多工具调用、高度灵活性、自主决策和持续学习机制等特性，通过与外部工具、系统的交互自主拓展能力边界，完成复杂任务。智能体作为通用人工智能的工程化实践，也是通用人工智能未来发展路径的前瞻探索。

2. 企业级智能体契合企业高质量发展的需求

企业级智能体凭借其高度的自主性、学习决策及环境交互能力，在具体业务场景中与企业核心需求形成深度契合。业务流程自动化方面，企业级智能体通过与外部环境及工具的持续交互，能够自主完成从数据采集、分析到决策执行的全流程任务，提升运营效率。在复杂业务场景中，智能体通过实时数据监测与动态策略调整，实现端到端的智能化自主管理，为企业精细化运营提供有力支撑。知识管理与应用方面，企业级智能体通过持续学习机制不断吸收领域专业知识，形成机构记忆与最佳实践库，为员工提供精准的决策支持和问题解决方案，企业能够将分散的专家经验系统化、可操作化，有效提升组织整体智能化水平。在合规治理方面，企业级智能体在安全合规方面的强化设计，使其能够在遵循企业治理框架的前提下自主执行敏感操作，为关键业务系统的智能化升级提供可靠路径。在商业创新方面，企业级智能体通过打破人机边界、重构协作流转机制，助力企业从原有的“人力密集型”或“固定规则驱动”模式向“智力协同、数据驱动”的敏捷组织演进，进而培育出面向未来的创新型商业模式与核心竞争优势。

3. 企业级与消费级智能体协同共振

企业级智能体是指聚焦企业业务场景，具有自主感知、决策、执行与学习能力，并能与业务流程、业务系统及业务人员深度协同的自动化实体。

智能体技术在企业级与消费级市场形成技术互补的协同发展格局，构建起双向驱动的产业生态。企业级智能体聚焦规模化、高复杂度、高规范性的业务需求，核心价值在于通过自主决策与跨系统协作降低企业运营成本、提升业务效率与创新能力。企业级智能体在智能客服、数据分析和流程自动化等专业场景中，实现与既有系统的深度集成，有效支撑复杂业务流程的智能化转型，为企业提供可靠的自动化解决方案。**消费级智能体**聚焦轻量化、高频次的个性化需求，发展重点在于提升交互便捷性、响应速度与用户体验适配度。消费级智能体形态日益融入日常生活，在个人办公、学习辅导、生活服务等领域中得到广泛应用，不仅培养了用户使用习惯，更通过海量用户交互积累丰富的场景数据。**企业级智能体和消费级智能体在技术与应用层面形成紧密互补**，消费级产品以前沿交互推动技术演进，企业级方案以系统化实践验证技术可靠性，二者共同构成智能体产业可持续发展的完整闭环。

（二）需求牵引：企业级智能体助力夯实智能原生企业根基

2025 年被业界视为“智能体元年”，人工智能通过调用工具具备了感知物理世界并执行复杂任务的“手和脚”。随着智能体技术在自主决策、多模态交互、复杂任务执行能力等方面的突破，智能体正

逐步从辅助型效率工具向业务核心引擎转化。2026 年 5 月，国家网信办、国家发展改革委、工业和信息化部三部门联合发布《智能体规范应用与创新实施意见》，针对智能体发展进行国家级顶层设计²。在政策及行业需求的引领下，企业级智能体凭借深度业务融合、全流程闭环、私有化部署等核心优势，正成为推动企业数智化转型的关键要素，支撑企业完成从“数字原生”到“智能原生”的跨越。

1. 企业数智化转型的核心引擎

智能体作为数智化进程中的核心引擎，通过重构企业的决策模式、运营流程与组织架构，全面赋能企业的变革与升级。据 Gartner 预测，到 2030 年，80%的企业将通过 AI 原生开发平台将大型软件工程团队转变为更小、更敏捷的团队并通过 AI 赋能这些团队³。智能体助力企业建立独特的数据驱动机制。通过整合多维业务信息与专业知识，智能体帮助企业管理层获得更全面的业务洞察，精准把握市场动向，为战略规划提供可靠依据，推动企业实现可持续发展。智能体为企业带来显著的效率提升。从前端客户服务到后端管理流程，智能体实现全链路的智能化运作，使企业能够以更优化的资源配置实现业务目标，同时让团队可以将精力集中于创新探索和战略性工作。智能体与企业共同塑造协同发展的工作模式。基于智能体的深度融入，企业建立起更加灵活的组织架构，促进团队成员数字能力的持续成长，形成自我完善、不断进化的组织体系。

2. AI 原生企业的迫切市场需求

² https://www.cac.gov.cn/2026-05/08/c_1779979789523320.htm

³ <https://www.gartner.com/cn/newsroom/press-releases/2026-top-strategic-tech-trends>

企业级智能体市场的发展呈现出从功能化应用向体系化能力集成的演进趋势，其背后是企业数智化转型过程中不断深化的复杂需求驱动。Microsoft Copilot Studio、ServiceNow、OpenClaw、WorkBuddy 等多样化的平台与应用涌现，以满足企业更深层次的智能化需求。一是**技术升级催生高阶能力需求**。企业开源框架的普及与推理成本的下降，大幅降低智能体的研发与应用门槛。企业对智能体在复杂、动态业务场景中的高阶推理判断、自主任务执行与持续进化能力的需求更加迫切。二是**市场热度驱动产业创新需求**。AI 智能体的渗透率大幅提升，市场迎来爆发式增长，德勤预测，到 2027 年，将有 50% 的企业部署生成式 AI 驱动的智能体⁴。AI 原生企业需求已从单一内部应用拓展至产业链智能化协同与价值共创。三是**政策牵引加速企业转型需求**。国家顶层设计与地方实践持续深化，加快智能体产业布局。工业和信息化部等八部门联合印发的《“人工智能+制造”专项行动实施意见》，明确到 2027 年将培育 1000 个高水平工业智能体、500 个典型应用场景⁵。地方政府同步跟进部署，面向重点行业加快智能体的规模化落地应用。AI 原生企业积极响应，借助智能体实现数智化转型需求。

3. 打通数智化的“最后一公里”

企业级智能体通过将技术能力融入业务实践，有效帮助企业将数智化蓝图转化为实质性的业务成果。一是实现业务流程的高效优化与持续运营。企业级智能体能够实时理解业务逻辑、自动执行任务，并

⁴ <https://www.deloitte.com/cn/zh/Industries/tmt/perspectives/tmt-predictions-2025.html>

⁵ https://www.miit.gov.cn/jgsj/kjs/wjfb/art/2026/art_5ea5b1663f264fcea69df0ab00d1f6f3.html

在确保合规的前提下，提升运营效率，缩短业务响应时间，为企业降本增效提供坚实支撑。**二是驱动服务模式的精准升级与体验创新。**企业级智能体助力企业从被动的标准化服务转向主动的、个性化的精准服务。通过深度洞察客户需求并实时匹配最佳解决方案，提升客户满意度与忠诚度。

（三）范式革新：企业级应用落地铸就新质生产力核心引擎

企业级智能体经历从技术探索到产业落地的关键转折，其应用深度和广度持续拓展，成为培育新质生产力的重要驱动力。然而，企业级智能体规模化部署普遍面临着技术、数据与运营等方面的现实挑战。作为助力企业发展的自主系统，企业级智能体在应对挑战的同时，将进一步拓宽企业智能化应用场景，帮助企业实现降本增效提质，为产业转型升级注入新动能。

1. 企业级智能体落地进程多维掣肘

企业级智能体的落地应用尚处发展阶段，其价值发挥面临来自技术、数据及运营管理等方面的制约。技术能力方面，企业级智能体在复杂逻辑推理和模糊任务拆解中面临逻辑断裂与方向偏离等问题，且在处理专业任务时可能存在信息幻觉，“幻觉”与错误输出在工业制造、政务处理等关键领域可能引发严重后果。**数据质量方面**，企业内部数据深嵌于特定业务语境，个性化要求高，智能体难以脱离场景准确理解。同时数据作为核心商业机密，分级权限与加密管控割裂信息完整性，智能体在安全约束下往往只能获得碎片化视图，既影响判断

准确性，也带来合规隐患。**运营管理方面**，企业内部运营知识与流程的沉淀提炼本身缺乏标准化支撑，导致智能体难以真正实现智能化赋能。在赋能过程中，智能体与人类的协作边界模糊、分工不清，不仅影响效率，更使得责任归属与效能评估难以量化，风险难以及时追踪。

2. 企业级智能体助力落地应用深化

企业级智能体的应用深化体现在“行业穿透”与“场景下沉”双维度。**行业应用：覆盖多元领域，推动企业智能化转型。**企业级智能体已在金融、制造、医疗等流程标准化程度高的领域形成规模化落地。企业级智能体充分发挥对专业知识的深度学习和业务逻辑的精准把握能力，通过构建覆盖核心业务环节的智能服务体系，推动行业数智化转型升级。金融领域智能体实现智能风控和精准营销，政务领域提升政务服务效率 and 政策决策水平，制造领域优化生产流程和质量管控，教育领域推动个性化教学和智能评测，医疗领域助力辅助诊断和药物研发。**场景应用：下沉业务末梢，实现全链路智能升级。**企业级智能体的应用深化不仅体现在行业层面，更下沉至企业研发、生产、运营、服务等核心业务场景。在客户交互与营收增长领域，智能体作为企业与用户的核心触点，承担起个性化服务与业务转化的双重使命；内部运营与知识协同场景中，智能体成为组织的效率引擎，通过流程自动化与知识调度实现运营效能的全面提升；在核心业务与战略决策层面，智能体已深度嵌入关键业务流程，依托数据驱动的实时分析与自主决策能力，推动企业核心运营模式的变革。

3. 企业级智能体赋能新质生产力发展

企业级智能体作为新质生产力体系的关键支撑力量，通过系统性融合与创新重构，全面推动产业发展模式的深度变革。企业级智能体驱动高科技突破。作为技术创新的核心主体，企业级智能体不仅加速前沿技术的探索与应用转化，更通过自主知识发现与跨领域融合，持续推动产业技术边界的突破与升级。**企业级智能体重塑高效能生产。**通过重构生产流程、优化资源配置与实现全链路智能化决策，企业级智能体显著提升企业运营效率与资源利用率，建立起高度灵活、响应敏捷的现代化生产体系。**企业级智能体支撑高质量发展。**基于全要素系统整合与动态协同优化，企业级智能体帮助企业构建可持续的高质量发展路径，在提升产出质量的同时增强系统韧性，推动产业向更高效、更可持续的方向演进。

二、企业级智能体技术能力

（一）一站式智能框架构建，赋能企业级渐进式开发

企业在智能体时代的布局宜循序渐进，应从基础业务场景切入，在实践积累中稳步提升能力，从而在智能体发展浪潮中占据战略先机。企业级智能体的构建需要统筹开发路径的系统性与技术架构的层次性。依托分层架构的设计，构建从模型适配到运营治理的稳定可扩展技术体系。通过分阶段的实施策略，实现从试点验证到生态融合的渐进式发展。

1. 分层技术框架：稳定可靠可拓展

企业级智能体架构旨在打造“建-用-管”一体化的智能体超级协作空间，通过系统性设计实现全流程赋能。一是融合驱动的模式适

配层，其作为底座的核心驱动力，负责适配和集成多种模型能力，包括企业自研大模型、主流品牌大模型、开源大模型以及客户私有大模型，通过多模型路由调度、模型能力量化评估、场景化动态选型、异构模型统一接入与负载均衡等机制，实现能力融合与灵活调度，确保技术先进性与架构包容性，为上层智能体提供持续迭代的模型支撑。

二是持续进阶的智能增强层，通过三大模块全方位提升智能体的功能和表现，涵盖记忆增强、工具增强以及可信增强，系统化拓展智能体的任务理解、持续学习与执行闭环能力，使其在企业复杂业务场景中具备更强的自主性、适应性与协作性。**三是精益运营的开发治理平台层**，该层在平台架构中具体涵盖了“智能体构建开发”、“智能体使用”与“智能体管理”三大核心模块。其中，智能体构建开发支持 L2 工作流编排、L3 推理智能体、L4 智能体蜂群、GUI 智能应用以及异构智能体纳管；智能体使用与管理模块则面向运营和开发人员提供全面的配置功能，实现企业级智能体的规模化创建、精细化运维与持续效能优化，提升整体智能协同体系的运营透明度与管理成熟度。



来源：公开资料整理

图 1 企业级智能体构建与运营平台框架

2. 开发构建路径：自上而下更稳健

企业级智能体的规模化落地应遵循循序渐进的实施路径与高度场景化的技术适配。以分阶段演进的战略规划为牵引。企业应采取分阶段推进的务实策略。在起步阶段，应集中资源在有限的高价值场景中进行试点验证，通过打造可示范的智能体应用来建立初步成效与团队信心。在扩展阶段，需着力构建支持规模化开发的平台能力，推动智能体在更复杂企业业务环节中落地。在成熟阶段，通过夯实底层架构，打通数据与流程壁垒，实现智能体与业务系统的深度耦合，最终形成具备自适应与进化能力的可持续智能生态。以技术选型开拓智能体实现路径。企业应依据具体场景需求定义核心能力，并据此选择合适的智能体模式，如处理闭环任务的垂直任务型、应对开放问答的通用助理型或执行跨系统流程的自主流程型。大模型选型需结合实际需求，重点考量性能、成本、安全性与行业适配性，合理选择开源大模型或构建客户私有大模型。工具集成则需规划与现有企业系统的高效连接，确保智能体能够融入实际业务流。

（二）企业级知识高效存储，实现业务规划动态调优

在企业级智能体的系统化能力构建中，记忆增强、自主规划与工具拓展构成核心支柱。企业级智能体通过构建体系化的行业知识库以确保信息处理准确可靠，依托动态的业务流程引擎来实现复杂任务的拆解与闭环管理，借助开放的应用工具平台来灵活调用企业内外资源。

1. 记忆增强：知识管理更高效

记忆增强可系统性提升智能体信息处理与知识运用能力。智能体记忆分长期记忆和短期记忆，需高效管理运用，而高质量的企业数据治理能让长期记忆更准确可靠。上下文工程通过设计、管理、优化输入专业领域信息，可大幅提升企业级智能体的特定任务表现。**一是利用 RAG 实现长期记忆的有效调用**，企业级 RAG 系统连接海量知识库，让智能体获取企业业务相关专业信息。RAG 通过混合检索与重排序提升内部文档的召回精度，借助缓存机制支撑高频业务场景的实时响应，并构建权限隔离体系，确保多部门、多层级的企业知识在调用过程中安全合规。同时，通过持续优化检索准确性，并结合可信增强机制确保知识调用过程是可审查的。**二是实现领域知识封装**，对特定领域的知识、岗位经验、业务流程和可执行逻辑进行标准化封装。封装过程实质上是将企业知识沉淀为可复用的 Agent Skills，支持智能体依据任务需求动态调度与集成外部知识资源，实现知识的高效融合与精准场景化应用。**三是优化上下文管理策略**，企业级智能体依托的大模型上下文窗口有限，筛选有价值信息是核心。常见优化策略有上下文压缩、信息筛选、滑动窗口等。此外，智能体还需与企业业务系统保持实时同步，确保在处理库存查询、订单跟进等任务时，能够基于企业当前的真实经营数据做出准确判断。

2. 自主规划：动态规划更灵活

自主规划是企业级智能体处理复杂业务的核心执行框架。通过分析任务意图、拆解关键步骤、调用资源工具，并在执行中持续监控调

整，最终完成企业业务流程。**一是任务拆解贴合企业流程。**企业级智能体接收业务需求后，会结合企业自身的组织架构、审批节点和业务规则，将复杂的业务指令拆解为符合企业流程规范的可执行子任务。**二是规划执行对接企业资源。**企业级智能体制定合理路径确保步骤有序衔接，依步骤特点选合适工具资源（如企业知识规则、业务数据、企业工具等），按逻辑关系和资源可用性规划执行。**三是执行闭环融入企业业务。**企业级智能体全程监控任务进展，发现异常时依据企业预设规则进行容错调整。任务完成后自动回写业务系统、更新数据状态或触发下一环节，确保从业务发起到数据更新在全流程形成闭环，实现可追溯、可审计的企业级任务管理。自主规划常用于处理非结构化、长周期、多变量复杂企业业务，在数字化系统未建立或不太成熟时应用较多，如行业研究报告生成、智能营销活动执行、合同审核等。

3. 工具增强：操作方式更多样

工具增强可持续扩展智能体能力边界。工具是企业级智能体的子弹库，其任务范围取决于调用工具的种类和数量，构建开放、丰富、易扩展的工具生态是关键。**一是构建丰富工具生态，**企业级智能体平台应具备双重功能，一方面提供开箱即用工具，覆盖常见任务，方便开发者快速上手。另一方面支持企业创建接入私有域工具，连接核心业务系统。同时，平台要提供标准化接入规范和安全执行环境。**二是提供综合解决方案，**面对不同行业、职能的差异化需求，多数主流厂商推出平台搭配应用套件模式。平台层提供模型管理、工作流编排等底层技术支撑。应用套件层针对特定行业或职能，提供预置应用模板、

业务流程和知识库。该模式可降低企业自研技术门槛与成本，助其聚焦业务创新，加速智能体普及应用。



华院智能体平台在能源行业的应用实践

华院智能体平台是华院计算基于自主研发的认知智能平台打造的企业级智能应用构建平台，以“技术基础+业务理解+实施服务”三位一体的服务模式，深度融合行业场景，推动企业智能化转型与运营效率提升。平台采用模块化架构，集成数据智能处理、知识体系构建、行业模型灵活调用以及工作流可视化编排等核心能力，支持企业快速搭建贴合业务场景需求的智能体应用。

在能源行业的落地实践中，平台通过整合 AI 大模型、RAG 检索增强生成与垂直场景小模型能力，打通多系统数据链路，将财务、行政等业务流程中的重复性、事务性工作转化为由智能体自主或半自主执行。以财务及各类报告审核场景为例，原本需数小时乃至一天完成的统计与审核流程，现可于分钟级内自动生成结构化结果，实现效率的质的飞跃。通过可复用的架构与场景化落地，助力企业构建智能、高效、可持续的运营体系。



来源：华院计算技术（上海）股份有限公司

图 2 华院智能体平台总体框架

（三）多智能体群体化协作，催生智能互联价值释放

面对企业日益复杂的跨系统、长流程任务，单个智能体常因能力边界受限而难以独立完成，多智能体协同机制通过任务动态分解、分布式协作与人机协同，提升企业复杂业务闭环的执行效率。IDC 预测，到 2027 年，45%的企业将管理跨多个渠道、应用程序和供应商的多智能体（Multi-Agent），从而实现更无缝、上下文更丰富的体验⁶。标准化通信协议则确保异构智能体间的可靠交互与快速集成，为企业跨系统协同提供基础支撑。

1. 多智能体协同：高效协同更开放

多智能体协同通过有效组织与调度，实现“1+1>2”的集体智能效应，从而系统性地解决企业中的复杂任务。单一智能体能力有限，需构建多智能体系统，通过智能体间的分工配合以及人与智能体的协作互补，促进人工智能有效落地，共同完成复杂业务目标。多智能体协同基于任务分解机制与并行处理架构兼顾企业运转效率与运转稳定性。当前技术发展聚焦于企业级智能体编排平台的建设，通过预制化技能、可视化编排和系统集成能力，使多智能体协同转化为可落地的企业解决方案。将企业内的复杂事务拆解为多个智能体并行处理，借助冗余设计提升系统运行的稳定性，利用任务分解机制优化跨部门的响应效率。人机协同依托共识算法与权限映射机制保障企业决策可控。企业通过自然语言理解、意图识别和多模态交互技术，让智能体能够准确领会员工的操作指令与业务诉求。实时通信中间件保障员工

6

https://www.idc.com/resource-center/blog/%e8%ad%a6%e6%83%95%e7%94%9f%e4%ba%a7%e5%8a%9b%e5%80%92%e9%80%80%ef%bc%8cidc-futurescape-2026%e6%99%ba%e8%83%bd%e4%bd%93%e5%8d%81%e5%a4%a7%e9%a2%84%e6%b5%8b%e5%8f%91%e5%b8%83/?utm_medium=social&utm_source=linkedin&utm_campaign=ai-council-2

与智能体之间的信息高效传递，共识机制协调双方在执行过程中的判断差异。企业权限管理体系确保员工在关键环节的审核与可控性，为复杂业务场景中的人机协作提供可靠的技术保障。

2. 智能体互联：群体协同更可靠

智能体互联通过标准化协议驱动，是企业实现智能体协同运作的技术基础与核心机制。实现局部协同的技术基础。智能体互联旨在建立两个或多个智能体间的直接通信与协作关系，以完成如多智能体规划、联合推理等特定任务。该机制依赖 A2A、ANP 等标准化通信协议，在智能体间建立双向交互网络，通过交换任务分解、推理结果与执行状态等信息形成局部闭环，具有任务导向性强、协议依赖性高、连接规模有限等特点。**构建企业级协同的技术范式。**智能体互联通过协议标准化向企业级智能体网络演进。基于统一的通信协议与标准化接口，建立跨系统的安全互信机制，实现智能体的动态发现、任务调度与资源编排。通过分布式协调算法与状态同步机制，支持大规模企业级智能体的并行执行与结果融合。

（四）私有化部署方案加持，适配企业稳定可靠要求

企业级智能体已成为提升运营效率、优化用户体验的核心驱动力。企业应从自身业务本质及核心需求出发，综合考虑性能、成本、安全、运维复杂度等多个维度，逐步验证、迭代、优化部署方案，推动构建“以模治模，以 AI 对抗 AI”的新型安全防护体系，为企业智能体的规模化落地筑牢安全防线。当前企业多采用私有云为主、混合云为辅的部署模式，融合自建与购买策略，在安全基座与弹性扩展之间寻求

平衡，构建合规、敏捷的专属运行环境。

1. 企业级智能体部署方案选型

企业级智能体部署策略应基于其业务特性与核心需求，多采用私有云为主、混合云为辅的部署模式。公有云部署符合敏捷与成本要求，适合初创与中小企业。核心优势在于初始成本低、弹性伸缩和快速部署，能快速、灵活地获取强大算力，助力业务快速上线与迭代，是验证概念与推动创新的理想选择。私有云部署优先适用于安全与控制，适合金融、医疗等对数据安全、隐私控制与合规保障有至高要求的大型企业，通过建设私有云实现数据的完全自主与控制，具备模型深度定制、深度系统集成以及网络性能卓越等优势。混合云部署旨在平衡安全与灵活，适合业务多元化的头部企业。核心能力在于统筹安全与敏捷，当企业需要同时保障核心数据的私密性并维持创新业务的敏捷度时，混合云架构能将稳态与敏态业务分离，使核心系统在私有云中安全运行，同时利用公有云的弹性支持外围创新应用，实现最佳平衡。

2. 选择安全、合理、弹性、可持续部署策略

融合“安全基座”与“弹性引擎”的综合性部署方案可满足企业在数智化转型中对智能体的核心需求。围绕当前企业 AI 智能体规模化落地的趋势，企业多采用“自建+购买”混合模式，致力于构建安全合规、敏捷高效的企业专属运行环境。一是以轻量化、自动化、私有化部署为基石。旨在企业内部构建安全合规、敏捷高效且资源消耗优化的专属智能体运行环境，从根本上保障数据主权并降低运维复杂度。轻量化技术可降低单次推理成本，具备高效运行保障。自动化工

具链满足智能体的快速迭代和一键部署。通过实现数据的完全私有化，满足监管合规要求。二是引入边-云协同部署作为核心弹性引擎。为适配企业业务的潮汐特性与低延迟要求，通过智能流量分发、统一资源编排与跨层弹性伸缩机制，将智能体能力动态下沉至边缘或扩展至云端，实现计算资源的按需分配与全局优化，赋予企业应对未来业务不确定性的弹性与扩展能力。

三、企业级智能体运营管理

（一）多维系统集成与协同，筑牢高效合规治理根基

企业级智能体通过深度融合业务系统与构建严密的治理框架，为企业日常运营提供安全高效的协作底座。该体系要求智能体具备强大的跨系统工具调用、复杂业务流程编排以及支撑企业内多维协作的能力，强调在运营全链路中贯彻可信、合规及精细化的身份与权限管理。通过打造“高效协同”与“安全可控”的双擎驱动，保障智能体在复杂多变的业务场景中稳健发挥效能。

1. 业务协同与系统集成

企业级智能体需具备深度的系统集成与业务编排能力，以打破传统企业的数据与流程孤岛。系统集成与工具调用方面，智能体应通过标准化接口、插件生态或自动化技术，无缝对接企业现有的 ERP、CRM、OA 等核心业务系统，根据业务意图自主调用各类内外部工具，实现跨系统的数据互通与指令执行。流程编排方面，依托强大的工作流引擎与智能规划能力，智能体支持复杂业务流程的可视化设计与动态编排，能够将宏观业务目标精准拆解为多层级的可执行子任务，并

根据执行环境的反馈实时动态调整路径。多人多智能体协作方面，智能体打破了传统的人机交互边界，构建起“人-机”、“机-机”的多维协作网络。它支持企业多部门员工与多智能体在同一工作流中共享上下文、并行处理任务，通过不同专业能力智能体的自主沟通与无缝交接，全面重塑组织内部的协同范式与业务流转效率。

2. 身份管控与合规治理

在常态化运营过程中，企业必须为智能体建立严密的身份管控与可信治理体系，以应对日益复杂的安全与合规挑战。身份与权限管理方面，需将智能体全面纳入企业现有的数字身份认证架构中，采用“基于角色”或“基于属性”的细粒度访问控制策略，为不同业务场景下的智能体划定严格的操作权限和数据访问边界，坚决防范越权调用与核心敏感数据泄露。可信与合规审计方面，需在智能体的输入、处理及输出各环节部署多重保障机制，确保其决策逻辑与生成内容严格遵守行业法律法规、数据隐私规范及企业内部审计要求。治理与风险管控方面，应建立覆盖全链路的审计追踪机制，实现智能体执行路径的“白盒化”溯源。同时，配备动态沙箱隔离与异常熔断策略，当智能体执行高风险操作或面临能力边界之外的复杂任务时，系统能自动拦截并触发人工接管介入，从而在推动业务创新的同时，夯实企业智能化运营的安全底线。

（二）全生命周期精细管理，支撑企业战略系统规划

企业级智能体通过建立完整的生命周期管理体系为企业战略规划提供系统性支撑。体系覆盖智能体从需求分析、开发测试到上线运

营、优化迭代的全过程，采用更包容审慎、带有“避风港”思维的柔性监管和精细化的运营机制，确保智能体服务与企业战略目标保持高度一致，为企业智能化转型提供持续动力。

1. 企业级智能体全生命周期管理

企业级智能体通过构建标准化的流程体系，形成从开发构建到运营反馈的全生命周期闭环管理。在开发构建阶段，以明确的业务需求与场景定义作为基准，依托标准化的开发框架和自动化工具链，提供可视化编排界面和代码生成能力，支持智能体的快速构建和持续集成，配备完整的测试环境和质量检查工具，确保交付质量符合企业标准要求。在审核管理阶段，建立包含技术评审、安全检测和业务验收的多级审核机制，制定详细的审核标准和流程规范，对智能体的性能指标、安全规范和业务价值进行全面评估，设置自动化检查点和人工复核环节，保障服务上线的规范性和可靠性。在用户使用阶段，依托统一的智能体服务平台实现服务交付，建立完善的权限控制体系、使用监控指标和服务保障机制，提供用户行为分析和体验优化建议，确保智能体服务的稳定运行和安全管理。

2. 企业级智能体管理体系建设

企业级智能体应建立全面管理体系，推动管理策略向规范化、系统化方向发展。智能体管理方面，采用统一的注册登记和版本管控机制，建立智能体档案库和版本历史记录，明确智能体分类标准和元数据规范，完成智能体的标准化管理和全生命周期追溯，并嵌入安全合规与伦理审查机制，对生成内容进行真实性校验与风险过滤，确保智

能体运行于安全可信的框架。**资源管理方面**，需要建立统一的资源调度平台，通过容器化技术和资源隔离机制，实现计算资源、存储资源和网络资源的智能分配，确保每个智能体都能获得必要的运行环境，同时避免资源竞争导致的性能问题。**模型管理方面**，设立企业级模型仓库和管理平台，建立模型评估体系和效果追踪机制，提供版本控制、效果评估和自动化部署能力，制定模型更新和退役规范，支持模型的持续迭代和效果优化。**工作空间管理方面**，配备协同开发环境和项目管理工具，建立团队协作规范和知识共享机制，集成低代码编排工具、调试终端与协作组件，支持团队协作和流程优化，提升研发效率 and 创新能力。

（三）深层次挖掘运营价值，描绘企业新兴市场版图

面对日益复杂的市场环境，企业需通过精细化运营挖掘智能体的长期价值，构建可持续的发展优势。构建覆盖全链路的观测体系与数据驱动的运营机制，能够实时保障业务稳定运行、驱动智能体能力持续进化，帮助企业逐步描绘出属于自身的新兴市场版图，在智能化浪潮中占据领先地位。

1. 观测调优：构建可观测体系保障业务稳定运营

建立覆盖输入、处理、输出全链路的监控指标体系，能够实时掌握企业级智能体运行状态，快速定位并解决系统异常。**实时追踪智能体性能与业务影响**。通过埋点采集、日志分析及可视化看板，实现对智能体运行状态、响应效率及异常行为的动态感知，快速定位并修复潜在问题，保障业务连续性。**制定分层预警机制与自动化干预策略**。

根据业务优先级设定不同阈值的告警规则，结合根因分析工具精准定位故障点，并通过策略引擎实现部分场景的自动调优与资源调度，降低人工干预成本。开展周期性健康度评估与性能优化迭代。定期从准确性、稳定性、资源消耗等维度对智能体进行综合评估，结合业务反馈持续优化模型参数与架构设计，形成“监控-分析-优化”的闭环管理。

2. 运营分析：建立模型版本控制与组织治理框架

通过系统化收集运营数据和用户反馈，构建数据驱动的持续优化闭环，确保企业级智能体能力与业务需求同步演进。构建覆盖全生命周期的模型版本管理与回溯机制。通过标准化流程记录每次迭代的数据集、参数、环境配置与性能基线，确保模型可追溯、可比较、可复用，支持快速回滚与 AB 测试，降低升级风险。建立运营价值量化评估体系。通过全面衡量部署成本、人效提升比、投资回报率（ROI）等核心运营价值要素，实现企业级智能体运营成效可量化、可对比、可优化。建立基于反馈闭环的持续学习与知识沉淀体系。通过用户交互数据、业务结果反馈等渠道收集样本，结合主动学习、增量训练等技术实现模型能力的渐进式优化，并将关键场景的决策逻辑转化为可复用的知识库。建立涵盖组织协同与治理规范的长期运营框架。应保障在长期运营框架中融入组织协同机制，明确跨部门职责与协作流程，确保系统具备持续监控和维护的能力。同时，必须建立并持续完善涵盖使用伦理、数据安全、隐私保护、算法公平性及行业合规性的综合治理体系，通过明确的政策、定期的审计与风险评估机制，保障智能

体在安全、可信、可控的范围内运行。

企业级对话式智能体平台应用案例

九四智能专注于大模型驱动的全球化 AI 语音交互技术，构建企业级对话式智能体平台。依托自研 LLM、ASR、TTS、NLP 等核心技术，打造覆盖 20 余种语言的全球化 AI 语音 Agent 能力。

平台的智能外呼、智能客服、用户运营三类垂直智能体，覆盖从主动触达、被动接待到全生命周期运营的全流程，已在金融、电商、保险、教育等领域规模化应用，业务覆盖 30 余个国家及地区。营销场景用户转化率提升约 40%，自动生成的呼叫策略可满足约 90%的业务场景，显著降低企业上线与运营成本。平台还内置企业级智能体管理中枢，支持多类型智能体的统一管理、动态监控与自动化迭代，实现智能体集群的高效协同与持续优化。



来源：广东九四智能科技有限公司

图 3 企业级对话式智能体平台框架

（四）全方位评测体系构建，保障产品质量卓越交付

为助力企业级智能体从实验走向规模化应用，企业需构建科学、全面的评测体系。通过多维度测试分析识别技术与业务风险，借助信通院评估体系对标行业标准，并建立持续评测机制量化业务价值，为企业智能体的核心技术、应用效果与服务成熟度提供可靠保障。

1. 企业级智能体发展亟需全面测评体系

企业级智能体测试需构建覆盖任务执行、系统性能、极端负载与安全合规的全方位测评体系。相较于传统软件测试，企业级智能体测试不仅需验证功能确定性，更需评估其在开放、动态环境下的智能表现。

一是任务测试，需检验企业级智能体能否准确理解用户意图并完成任务。其核心是构建高质量测试集，覆盖典型业务场景和边缘案例，并结合幻觉控制机制，如执行者-验证者双角色架构、强制引用、未知信息人工介入等，提升输出可靠性。评估将围绕回答准确性、任务执行成功率等关键指标展开，确保智能体的表现符合实际业务要求。

二是性能测试，需要评估高并发场景下服务能力。企业级智能体需服务大量用户，要对响应时间和吞吐量进行测试，考验模型推理速度和技术架构负载均衡、资源调度能力，确保业务高峰期稳定服务。

三是压力测试，评估企业级智能体在极限状态下的稳定性和资源消耗情况。通过模拟远超预期负载，测试极端情况表现，实时观测 GPU 算力、显存占用率等关键指标，同时需设置无限循环防护机制，包括单任务最大执行步骤限制、子任务执行超时熔断等措施，保障企业级智能体 7×24 小时不间断服务。

四是安全测试，企业级智能体需重点关注测试数据隔离、权限控制、防注入攻击及合规性审计等，并围绕

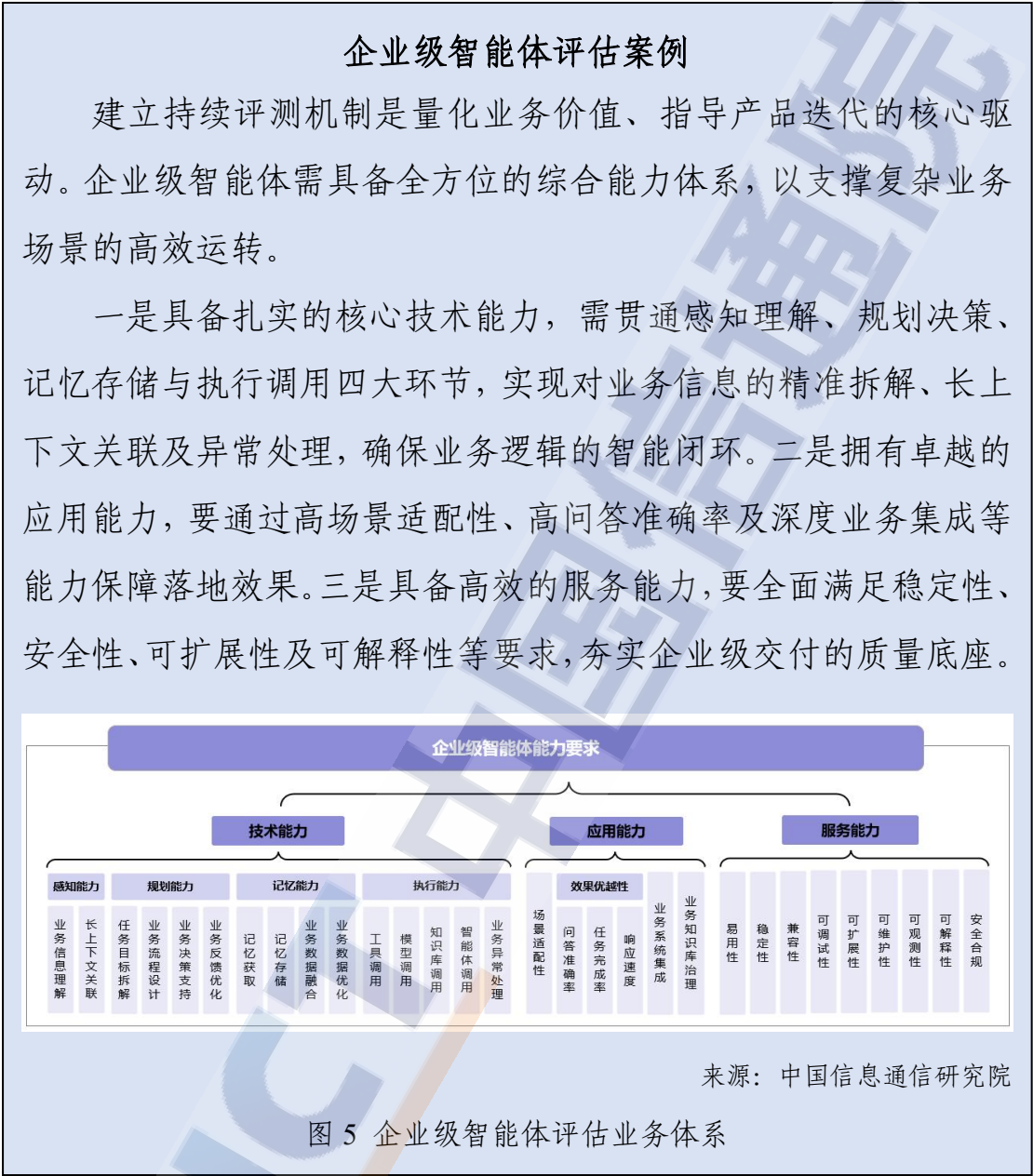
行业安全标准与监管要求完善评测体系，增加对抗样本鲁棒性测试、价值观对齐评测、供应链安全审计等评测指标，全面保障系统安全合规、可信可控。

2. 面向智能体全栈能力验证的评估体系

智能体通用评估体系覆盖基础支撑、通用场景至行业应用，并通过技术、应用和服务能力的全面要求，指导企业级智能体构建。评估体系旨在科学引导产业有序发展，并为企业提供选型参考，适用于智能体技术及应用的研发、评估和验收等诸多阶段。基础支撑方面，评估体系涵盖面向智能体基础、共性需求的平台与工具、技术能力和应用服务等系列要求，着重强调智能体开发平台的技术要求，并确保服务能力具备高易用性、稳定性、兼容性、可扩展性以及可观测性等保障机制。通用场景方面，评估体系要求智能体具备感知、规划、记忆和执行四大核心能力，并包含数据分析、智能客服、智能运维、智能营销等特定技术要求。行业应用方面，评估体系要求平台需满足场景适配性、效果优劣性（如问答准确率、响应速度）和业务系统集成度要求，覆盖金融、政务、汽车、办公、手机等十余个垂直领域。



图 4 智能体通用评估体系



四、企业级智能体应用实践

人工智能的应用潜力广阔，企业级智能体正加速融入千行百业，推动各领域向智能化、高效化转型。金融领域强化风险管控与智能投顾，政务领域支撑城市治理现代化与公共服务升级，工业领域驱动生产全流程优化与供应链协同，教育领域助力个性化学习与教学管理创

新，医疗健康领域赋能精准诊疗与药物研发，形成覆盖核心场景的智能化解决方案体系。



来源：公开资料整理

图 6 企业级智能体行业应用图谱

（一）驱动金融业务流程优化，开启财富管理新纪元

企业级智能体通过智能算法与业务场景的深度融合，重塑金融行业的服务模式与运营体系。通过将智能体等前沿技术应用于前中后台以及监管等核心业务环节，推动金融服务体系实现从传统依赖经验判断向数据驱动、自动化运营的转变，不仅提升金融服务的精准度和效率，更在资源配置、客户服务等方面展现出显著优势，为整个行业的数智化转型和创新发​​展注入持续动力。

1. 企业级智能体在金融领域的落地难点

金融智能体在推进核心风控与授信决策过程中，面临着监管合规刚性约束与决策可解释性不足的困境。一是监管合规与可解释性要求较高，信贷审批、反洗钱等决策必须满足“可追溯、可审计、可解释”的监管标准。二是幻觉风险易导致操作错误，幻觉的出现可能引发资

金划转错误或违规交易，金融业务容错率几乎为零。三是数据隐私与安全合规压力大，客户交易记录、征信信息等数据敏感，数据出境、模型记忆、第三方 API 调用等环节都可能构成数据泄露风险。四是自主执行带来的责任归属模糊，当智能体完成支付、投资指令等不可逆操作后出现损失，责任在用户、开发者还是金融机构难以界定。

2. 企业级智能体在金融领域的场景应用

企业级智能体在金融领域的应用展现出强大的场景适配能力，通过智能化技术为传统金融服务注入新的活力。企业级 AI 的部署应秉持“场景驱动”原则，以解决具体业务痛点为导向，而非盲目追求通用大模型能力的叠加与参数的堆叠。前台基于深度学习和自然语言处理技术，企业级智能体通过智能客服与精准营销平台实现从业务咨询到产品推荐的全程智能化服务，并依托动态用户画像提供个性化资产配置建议。中台聚焦财务报销、合同审核等核心环节，运用规则引擎与智能识别技术，建立标准化的自动化处理流程，并通过智能单据核验与条款比对，实现业务流程的智能化管控。后台构建覆盖全业务的智能运维体系，通过实时监控系統运行状态、智能预警潜在故障、自动开展资源调度，确保金融系统的高可用性和稳定性。科技监管搭建标准化合规监测体系，通过多维度合规筛查与动态预警，为机构规范化合规运营提供稳定支撑。

3. 企业级智能体在金融领域的落地成效

企业级智能体在金融领域的落地应用已实现服务效率提升、业务模式创新、运维合规提质等成效。一是企业级智能体有效提升服务响

应速度与处理效率，通过个性化推荐与精准营销，提高业务转化率与客户满意度。全天候的智能服务从根本上改善客户体验，推动金融服务向智能化、便捷化方向持续发展。二是企业级智能体自动化处理机制的应用使核心业务的处理效率和准确性得到提升，在降低人工操作成本的同时，实现运营成本的精细化管控。三是企业级智能体持续健全金融全流程智能运维机制与标准化科技监管体系，强化金融系统运行稳定性与业务合规规范性。

某银行智能体建设项目案例

某银行以服务中小微企业为核心客户群，依托大模型技术提升客户服务、风险管控及内部管理效率。通过部署客服智能体，银行成功实现账户查询、理财咨询及业务办理等常见业务的自动化处理，提供 7×24 小时不间断服务，人工客服降低 15%，客户满意度提升 20%。并且信贷审批辅助智能体能够基于客户提交的申请资料，结合银行内部信贷政策与信用评级模型进行智能初审，将审批周期从原先的 7 天大幅缩短至 3 天，显著提升审批效率。



来源：三六零安全科技股份有限公司

图 7 某银行智能体功能框架

（二）提升政务公共服务效能，实现便民利企新突破

智能技术深度融入政府治理体系，在提升政府治理能力和公共服务水平方面展现出重要价值。企业级智能体在城市治理、公共服务、业务办公等关键领域实现系统性赋能，推动政府治理从经验主导转向精准施策，从被动响应转向主动服务，为提升治理效能与服务品质提供坚实的技术基础。

1. 企业级智能体在政务领域的落地难点

政务智能体在推进跨部门协同服务过程中，面临着数据条块分割与行政容错极限的困境。一是跨部门数据孤岛与条块分割严重，政务流程涉及多部门、多系统，智能体需在保障数据安全和保密等级的前提下实现协同，技术整合难度大。二是决策容错率极低，行政公信力敏感，对输出的准确性和权威性要求较高。政策答复、审批结果等一旦出错，可能损害政府公信力，甚至引发法律纠纷。三是业务流程的非标准化与频繁变动，各地政策差异大、更新快，智能体需要持续适配新法规，而训练和微调周期往往跟不上政策变化节奏。四是数字鸿沟与公众接受度问题，老年群体或欠发达地区用户对 AI 交互不习惯，纯智能体服务可能造成服务排斥，需要保留人工兜底通道。

2. 企业级智能体在政务领域的场景应用

企业级智能体通过构建城市治理数字平台、打造智能政务服务体系、建立自动化办公系统，全面提升政府治理能力。在城市治理领域，基于物联网和人工智能技术，建立城市运行监测中心，实时监控交通流量、环境质量和公共设施运行状态，通过智能算法实现城市资源的

优化调度和突发事件的快速响应。在公共服务领域，运用自然语言处理和知识图谱技术，开发智能政务助手，为企业和群众提供 24 小时在线的政策咨询、办事指南和业务办理服务，实现从“最多跑一次”到“一次不用跑”的服务升级。在业务办公领域，采用流程自动化和智能审核技术，构建标准化行政审批系统，通过智能预审和材料核验提升审批效率，实现公文流转、事项审批、会议管理等办公流程的智能化处理。

3. 企业级智能体在政务领域的落地成效

企业级智能体的应用显著提升政务服务的智能化水平和群众满意度，推动政府治理能力现代化迈上新台阶。一是通过构建智能化预警处置闭环，城市管理问题的发现和处置效率得到提升，市政设施完好率持续优化，市容环境秩序明显改善，城市治理精细化水平迈上新台阶。二是智能政务服务平台实现政策咨询即时响应和业务办理全程网办，企业群众办事等候时间大幅缩减，政务服务满意度显著提升，真正践行“以人民为中心”的发展理念。三是行政审批流程持续优化，办事时限压缩成效显著，制度性交易成本降低，同时通过智能监管有效防范廉政风险，推动廉洁政府建设取得实质性进展，政府治理现代化水平实现全面提升。

某市人工智能服务平台智能体应用案例

为了全面提升某市政务办公的智能化水平，计划搭建“一个平台、N个应用、长期共育”的人工智能应用模式，完成私有化智能体的开发工作，并构建一个全面的运营体系，通过依托于智能体开发运营平台，实现人才的共同培养。

人工智能服务平台智能体带来的经济效益和社会效益如下：一是办公效率提升：智能问数智能体实现人力、财务等数据查询响应时间从2小时缩短至5分钟，提升业务部门年处理量；二是成本优化：某市政热线系统通过智能化升级，依靠坐席辅助、AI智能总结、智能知识库、智能质检等方面，提升工作效率，降低维护成本；三是资源配置优化：通过多维度智能化升级，不仅实现管理效能与服务品质的跃升，更以技术创新与智能化转型重塑政务行业标准，为全省政务智能化发展提供创新模式。



来源：三六零安全科技股份有限公司

图8 某市人工智能服务平台框架

（三）贯通工业生产关键环节，树立提质增效新标杆

《深化“智赋万企”行动 加快制造业数字化转型实施方案》中明确指出到2027年，湖南省规上工业企业数字化研发设计工具普及

率、关键工序数控化率分别超过 90%、75%，全省工业大市和重点园区规上工业企业实现数字化改造全覆盖⁷。在工业数字化转型进程中，企业级智能体构建起覆盖生产全流程的智能化体系，实现工业环节的自动化升级和资源配置优化，并在提升生产效率、保障产品质量、优化供应链管理等方面形成完整的解决方案，为工业转型升级提供关键技术支撑，推动产业向智能化、高效化方向持续发展。

1. 企业级智能体在工业领域的落地难点

工业智能体在推进产线控制与设备协同过程中，面临着实时确定性要求与黑箱决策风险的困境。一是实时性与确定性要求难以满足，工业现场（如产线控制、设备联锁）要求毫秒级响应和确定性，而大模型推理存在延迟波动和概率性输出，无法直接对接自动化设备。二是恶劣环境与边缘部署限制，工厂、油田等现场往往网络受限、算力不足，智能体需在低功耗边缘设备上运行，模型压缩后性能衰减明显。三是与传统控制系统的融合困难，现有工业系统基于规则和闭环控制逻辑，智能体的“黑盒建议”难以嵌入原有控制架构，且一旦介入可能导致系统不稳定。

2. 企业级智能体在工业领域的场景应用

企业级智能体能够实时调度生产任务、自动检测产品质量、智能协同供应链，为企业构建起端到端的智能化运营体系。当下热议的“新工业革命”本质上是由人工智能驱动的工业革命，其核心特征是工业发展的赋能方式从过往的数字化，转向以智能化手段为核心的赋能模

⁷ http://gxt.hunan.gov.cn/gxt/xxgk_71033/zcfg/gfxwj/202509/t20250912_33802364.html

式。在生产执行环节，基于工业物联网平台采集设备运行数据，构建智能生产调度系统，通过智能算法实现跨工序任务动态分配与资源优化配置，并结合数字孪生技术对关键流程进行多维度仿真与参数调优，持续提升系统运行效率。在质量管理环节，部署视觉检测、传感器网络与预测性分析系统，建立覆盖原料检验、生产过程监控到成品质量追溯的全流程管控体系，通过构建工艺-质量关联模型，自动识别异常根因并支持闭环改进。在供应链协同环节，运用需求预测模型和库存优化算法，打造智能供应链管理平台，实现采购计划自动生成、库存水平动态调整和物流路径智能规划，确保供应链各环节高效协同。

3. 企业级智能体在工业领域的落地成效

企业级智能体在工业领域的深入应用有效提升生产设备的运行效率、产品质量的一致性以及供应链的响应能力。一是企业级智能体有效提升设备与资源综合利用率，通过预测性维护与智能调度减少非计划停产时间，保障能源与物料稳定供应。系统监测设备状态与运行环境，自动预警安全与故障风险，大幅提升工业系统的可靠性与韧性。二是企业级智能体能够提高产品一次性合格率，通过自动化质量检测降低人工成本，建立完善的质量数据追溯体系，为持续改进提供数据支撑，系统能够快速识别质量波动趋势，及时预警质量风险，有效控制质量成本。三是企业级智能体能够增强产业链协同适配水平，优化库存与能源周转效率，实现整体运营成本降低。通过智能算法优化物流与能源配送路径，提升供需匹配效果与客户满意度，推动工业体系向绿色、高效、协同方向发展。

金现代配料智能体应用案例

金现代配料智能体，基于前沿大模型、多维特征建模、全局优化算法，重构工业配料底层逻辑。该智能体可打破传统生产环节过度依赖人工经验与反复试算调整、难以在多重约束条件下快速寻优的局限，为多行业提供全域智能、精准高效、稳定可靠的科学配比方案。

在食品制造行业，深度匹配风味、口感、品质等多元需求，从根本上减少原料浪费，严控综合生产成本。在精细化工行业，可严格把控化学成分精度，有效降低配比偏差与物料损耗，显著提升生产过程安全性与产品一次合格率。在新能源、新材料行业，实现高精度配料与全流程智能管控，提升电芯一致性与安全性，延长循环寿命，降低制造成本。

综上,金现代配料智能体，以 AI 技术重构配料能力，精准匹配成分与产品性能、最大化原料利用率、合理控制生产成本，赋能企业打造不可替代的产品竞争力，领跑工业智能生产新赛道。



来源：金现代信息产业股份有限公司

图 9 金现代配料智能体适用行业

（四）推动教育管理模式变革，激活因材施教新体验

教育管理模式的变革是深化因材施教、提升教育质量的关键环节。智能体通过构建数据驱动的教育治理新范式，在教学组织层面实现从统一进度到个性化定制的转变，在资源调配层面建立基于实时需求的动态分配机制，在评价反馈层面形成持续优化的闭环管理系统。企业级智能体为教育管理体系注入新的活力，使精准识别学生差异、动态调整教学策略、优化教育资源配置成为可能。

1. 企业级智能体在教育领域的落地难点

教育智能体在推进个性化教学评价过程中，面临着算法偏见风险与未成年人数据隐私保护的困境。一是算法偏见与教育公平风险，智能体对学生的行为、作业进行评价时，可能因训练数据偏差而产生歧视性判断，影响弱势群体的学习机会。二是未成年人数据隐私保护要求严格，收集学生答题记录、心理状态等行为数据需遵循相关法律及教育数据合规要求。三是教学场景融合适配难度大，校园教学场景多元且流程固定，智能体智能化流程与传统课堂教学、教务管理模式存在适配壁垒，软硬件融合对接、业务嵌入改造成本较高。

2. 企业级智能体在教育领域的场景应用

企业级智能体基于数据分析和个性化推荐能力，为学习者、教师和管理者构建起更加智能高效的教育生态系统。个性化学习规划方面，系统通过构建学习者知识图谱和能力模型，采用智能算法分析学生的学习轨迹和认知特征，实现学习内容的精准匹配与学习路径的动态优化，同时根据学习进展实时调整教学策略和资源推送。学情评估反馈

方面，基于实时采集的学习行为数据，建立包含知识掌握度、能力发展水平和学习效率的多维度评价体系，自动生成详细的诊断分析报告，并提供个性化的学习建议和针对性的干预方案，确保教学反馈的及时性和准确性。**教学管理决策方面**，为教育管理者提供涵盖学业表现、资源使用效率和教学质量趋势的可视化数据分析看板，支持课程设置的优化调整、教学资源的合理调配以及教学质量评估的科学决策。

3. 企业级智能体在教育领域的落地成效

企业级智能体在教育领域的深度应用推动个性化教学的实现、学生综合素养的提升以及教师专业发展的转型。**教学精准性方面**，通过数据驱动的个性化教学，实现教育供给从标准化向差异化的转变，系统能够精准识别学生的学习需求和能力短板，提供量身定制的教学方案，显著提升教学服务的适配度与教学效果。**学生发展方面**，构建以学习者为中心的教育生态，通过提供符合个体认知特点和发展需求的学习内容和活动，有效激发学生的内在学习动机和自主探究能力，促进批判性思维和创新能力的全面发展。**教师赋能方面**，将教师从批改作业、整理资料等重复性工作中解放出来，使教师能够将更多精力投入到教学设计、教学研究和学生关怀等创造性工作中，提升教育教学的专业水准和育人效果。

陕铁院校园督导智能体应用案例

陕西铁路工程职业技术学院教学督导智能体，依托 360 AI 企业知识库平台及多模态融合引擎，打通督导管理系统数据链路，实现多角色分权限协同管理，以 AI 研判与趋势推演助力督导决策科学化、精准化。

校园督导智能体依托智慧教学督导平台与“铁小智”AI 中台，打通教学全过程数据链，实现采集-分析-反馈智能闭环。督导员可非现场精准调取音视频数据，管理者一键提取课堂排行、AI 评分趋势、异常预警等指标，教师获取个性化分析报告精准复盘。校园督导智能体让管理决策响应提速 60%以上，督导人员巡课准备时间减少 70%，教师教学优化周期从“学期级”压缩至“课时级”，破解“反馈滞后”难题，推动教学质量从“经验驱动”迈向“数据驱动”。



来源：陕西铁路工程职业技术学院、杭州三六零亿方智能有限公司

图 10 陕铁院校园督导智能体功能框架

（五）赋能医疗资源精准调配，引领全民健康新征程

企业级智能体基于人工智能技术构建起覆盖预防、诊疗、康复全

周期的智能化医疗健康服务体系，推动医疗服务模式实现系统性创新升级。通过优化诊疗流程、提升服务效率、拓展健康管理边界，在提升医疗质量、改善患者体验、优化资源配置等方面取得突破性进展，改变传统医疗服务形态，使优质医疗资源得以更广泛地惠及人民群众。

1. 企业级智能体在医疗领域的落地难点

智能体在医疗领域面临着循证验证周期漫长与数据标准化等困境。一是临床级验证周期长，诊断辅助类智能体需通过医疗器械注册、循证医学验证，通常耗时数年，且证据要求远高于一般软件。二是可解释性不足影响医生信任，医生需要理解诊断结论的病理、影像学依据，而大模型的“概率性推理”无法提供明确的医学逻辑链，使得专业用户难以采信。三是多源异构数据融合与标准化困难，医院信息系统中的电子病历、影像、检验数据格式不统一，且存在大量非结构化信息，智能体需复杂的 ETL 和清洗流程，实施成本高。

2. 企业级智能体在医疗领域的场景应用

企业级智能体将智能技术深度融入医疗服务的各个环节，从辅助诊疗到运营管理，再到延伸健康服务边界，展现出全方位的应用价值。临床诊疗方面，智能系统通过构建辅助诊断模型和个性化治疗方案推荐引擎，实现医疗过程的精准化，建立医疗质量控制和风险预警机制，提升诊疗服务的安全性和可靠性，并基于药物基因组学和临床用药数据，构建个性化用药推荐系统，为患者提供精准的用药方案和剂量调整建议。医院运营方面，依托智能化平台建立医疗资源动态调配系统，优化就诊流程和医疗服务动线，完善包括人员绩效、设备利用和药品

耗材在内的精细化管控体系，提升医疗机构整体运营效能。智能排班系统根据就诊量预测自动调整医护人员配置，智能库存管理系统实现药品和耗材的精准补给。**健康服务方面**，基于连续性的健康监测和评估数据，构建覆盖全生命周期的健康管理平台，提供从健康促进、疾病预防到慢病管理的系统性服务，推动建立以健康为中心的新型医疗服务模式，同时整合可穿戴设备监测数据、电子健康档案和生活方式信息，生成个性化健康干预方案。

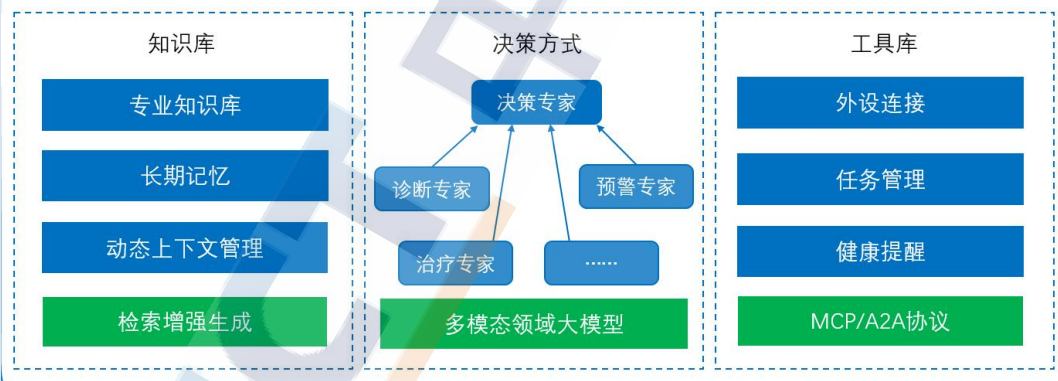
3. 企业级智能体在医疗领域的落地成效

企业级智能体的应用为医疗行业带来切实的改进，使诊疗过程更加精准可靠，医疗服务更加高效便捷。**一是**企业级智能体通过深度学习海量医学案例，能够识别复杂病症的细微特征，辅助医生做出更精准的判断，提升疾病诊断的准确性和治疗的有效性，优化临床路径和诊疗规范，增强医疗质量持续改进的能力，为患者提供更加安全可靠的医疗服务。**二是**实现医疗资源的科学配置和高效利用，加快医疗服务响应速度，提升医疗机构运营管理水平 and 成本控制能力，推动医疗服务体系整体效能的提升。同时智能导诊和分诊系统还能有效缩短患者等候时间，智能病历系统减轻医务人员文书工作负担。**三是**拓展医疗健康服务的覆盖广度和深度，改善医疗服务的连续性和协同性，提升居民健康管理水平和健康素养，促进医疗服务更加普惠均衡发展。利用远程医疗平台打破地域限制，智能随访系统确保治疗效果的持续跟踪，个性化健康管理方案帮助居民建立科学的生活方式。

睿宾 Agent 企业级智能体应用案例

睿宾医疗智能体作为可持续迭代的严肃医疗 AI 系统,打造“提问-应答-审核-沉淀-反哺”自进化可信闭环,融合华西医院专家知识库、润达医疗 AI 技术与华为 AI 数据平台算力,通过“云端调度+终端服务+专家校验”协同模式实现全流程工程化落地,其以“医知 Dr”与“论界 Schola”双智能体为核心,前者提供健康评分、报告解读等患者全周期服务,后者实现文献检索、AI 综述创作等医生科研诊疗支撑,有效破解基层医疗资源匮乏、临床科研效率低下、患者健康管理衔接不足、医疗知识更新滞后四大行业核心痛点,解决“看病难”“科研繁”等关键问题,目前已有用户 1 万余人,医生科研效率提升 75%、基层诊疗同质化率提升 58%,实现优质医疗资源高效普惠。

多智能体架构：专业+可信+聪明+主动



来源：四川大学华西医院、华为技术有限公司、

润达医疗科技股份有限公司、成都智算中心

图 11 睿宾医疗智能体功能框架

五、企业级智能体趋势展望

(一) 技术升级：从“被动响应”到“自主智能”的能力进阶

1. 推动企业级智能体技术向更高维度演进

技术升级将驱动企业级智能体实现从依赖规则响应的辅助工具，向具备自主分析与决策能力的智能伙伴转变。一是核心技术驱动信息整合。多模态融合、长上下文理解等核心技术可辅助企业级智能体实时处理文本、语音、图像等多种信息。同时，从信息处理向物理交互延伸，企业级智能体将与具身智能、数字孪生、工业互联网深度融合，依托空间感知、环境建模与实体交互能力，打通数字智能与实体业务的连接，构建全域一体化智能技术底座。二是系统升级实现认知突破。企业级智能体将在认知推理、情境感知、元学习等方面实现系统性突破，深入剖析问题本质，实时感知环境变化，支持快速学习以提升泛化性能。三是层级演进迈向自主智能。当前智能体主要定位于“人机协同的 Copilot”，专注于辅助决策与任务自动化。未来，随着高阶自主智能体在特定场景的试点成熟，能力层级将不断演进，最终迈向具备广泛认知与决策能力的自主智能。

2. 实现自主进化的下一代企业级智能系统

自主进化能力是企业级智能体发展的核心方向，通过模块化架构与深度算法融合，形成可自我优化、安全共享和实时响应环境变化的智能网络。系统架构方面，企业级智能体将采用模块化、可插拔的轻量化设计，支持功能组件的动态升级与灵活部署。通过多智能体协同框架与元学习算法的深度整合，系统能够实现个体在线学习、组织内知识安全共享与协同优化，形成持续进化的企业智能网络。能力升级方面，企业级智能体将融合多模态感知、深度学习和自主决策等前沿

技术，通过实时感知环境变化，结合动态算法优化模型，实现策略的智能生成与自主调整。未来，具备自我优化能力的企业级智能体将在制造业、金融业等重点行业实现规模化部署，推动企业运营模式发生深刻变革。

（二）应用创新：从“辅助支持”到“超级协作”的价值革新

1. 稳固企业级智能体战略伙伴核心地位

企业级智能体正从辅助工具转变为企业战略决策的核心参与者。该转变将重新定义人机协作关系，推动企业组织架构向更加灵活、智能的方向演进。**从信息辅助到流程再造的价值提升。**企业级智能体突破传统信息处理工具的局限，通过对业务流程的深度融入与智能化改造，实现从被动响应到主动优化的价值提升，完成对传统工作模式的重构。**从流程优化到战略赋能的模式革新。**在流程再造基础上，企业级智能体进一步发展为战略赋能者，通过智能分析与人机协同，为企业战略制定与实施提供系统性支撑，实现从效率提升到战略引领的价值拓展。**从战略支撑到生态创新的体系突破。**企业级智能体通过与其他智能系统及人类智慧形成有机协同网络，驱动整个生态系统的创新演进，实现从单一价值创造到系统价值创新的根本性跨越。

2. 开创人类智慧和智能协同融合新纪元

未来，企业将形成人机协同的新型组织架构，人类员工与智能体之间形成互补共赢的合作关系。智能体的普及将推动人类角色的深刻转变，未来每个个体或团队均可能拥有由数十乃至数百个智能体构成

的数字团队，员工的工作职责将演变为对智能体进行定义、规划、管理与监督，进而从重复性事务中释放出来。在协作方式上，企业级智能体将实现从指令式交互到对话式协作的转变。通过自然语言交互、情感计算和情境理解能力的持续提升，企业级智能体能够更准确地把握人类意图，实现更加精准的任务执行和创意支持，形成具备超级智能特征的协作体系。在能力互补上，人类员工的创新思维、伦理判断与复杂问题解决能力，将与智能体的高速计算、大数据分析和模式识别优势有机结合，形成人类引领方向、机器拓展效能的超级协同范式。在组织形态上，企业级智能体将推动组织结构向智能驱动、动态聚合的超级协作网络转型，实现人才、资源和能力的自适应匹配与协同。未来，人机协同将成为企业运营的标准模式，大幅提升组织创新能力和市场应变能力。

（三）生态融合：从“单点突破”到“携手智变”的格局重塑

1. 引领企业级智能体产业从竞争走向共赢

在全球科技竞争与产业变革交织的背景下，企业级智能体领域已展现出从零和博弈转向生态共创的趋势。通过开放技术体系、重构协作网络、优化产业分工等一系列结构性变革，各类市场主体的能力与资源在更高效的机制下相互耦合，共同推动智能体技术向深度融合、普惠应用的新范式演进。开源开放方面，随着国内大模型开源战略取得显著成效，越来越多的企业直接调用开源基座模型，让竞争的焦点转向落地应用。部分龙头企业开放平台接口，吸引生态伙伴。开放模

式使得不同规模企业能开发兼容多种智能体的产品，降低集成成本，提升互操作性，实现资源共享。**合作机制方面**，企业级智能体推动建立跨组织、跨领域的开放式协同网络。通过建立统一的互操作架构与共享开发平台，促进企业间能力的模块化组合与开放式调用，构建起以目标为导向、以智能协同为基础的新型产业协作范式。**产业政策方面**，要构建分工体系，形成大型平台企业引领、中小企业专精特新发展的产业分工。大型企业专注基础模型与平台开发，中小企业深耕垂直场景应用，共同打造多元主体共生的创新共同体，推动产业蓬勃发展。

2. 助推企业生态实现开放共融的发展格局

企业级智能体是驱动产业生态开放共融的核心力量，通过促进开放协同与价值互联，引领整个生态体系迈向智能协同、共荣共生的新阶段。**产业理念方面**，企业级智能体将打破封闭思维，倡导开放共享协同，鼓励企业融入产业大循环，通过深度合作实现资源共享、优势互补，推动产业生态从分散无序走向集中有序。**价值体系方面**，企业级智能体通过促进企业间数据、算法与业务能力的深度融合，使价值从单向流动转向多方循环，构建起价值共创、共生、共赢的生态化网络，实现从零和博弈到共生发展的根本转变。**生态系统方面**，企业级智能体作为连接与调度的核心枢纽，推动不同组织间形成深度互联、动态适配的共生关系，使生态系统能够自主感知、智能响应和持续进化，最终形成具备生命体特征的高韧性、自适应产业共同体。展望未来，企业级智能体将继续发挥核心驱动力，与新兴技术深度融合，引

领产业生态向开放、共融、智能发展，为智能经济高质量发展带来更多机遇，让产业生态焕发生机活力。



缩略语

AI	Artificial Intelligence	人工智能
AGI	Artificial General Intelligence	通用人工智能
ANP	Agent Network Protocol	智能体网络协议
API	Application Programming Interface	应用程序编程接口
ASR	Automatic Speech Recognition	语音识别技术
A2A	Agent-to-Agent	智能体间交互
CPU	Central Processing Unit	中央处理器
CRM	Customer Relationship Management	客户关系管理
ERP	Enterprise Resource Planning	企业资源计划
GUI	Graphical User Interface	图形用户界面
LLM	Large Language Model	大语言模型
NLP	Natural Language Processing	自然语言处理
OA	Office Automation	办公自动化
RAG	Retrieval Augmented Generation	检索增强生成
ROI	Return on Investment	投资回报率
TTS	Text To Speech	语音合成

编制说明

本研究报告自 2025 年 10 月启动编制，分为前期研究、框架设计、文稿起草、征求意见和修改完善五个阶段，面向企业级智能体的技术供应方、交付咨询方、服务应用方开展了深度访谈和问卷调查等工作。本报告由中国信息通信研究院人工智能研究所联合三六零安全科技股份有限公司牵头撰写，撰写过程得到了中国人工智能产业发展联盟智能体创新与应用委员会、南京新一代人工智能研究院有限公司、广东九四智能科技有限公司、金现代信息产业股份有限公司、宁波广播电视集团、中电信数智科技有限公司、南京市河西新城区国有资产经营控股（集团）有限责任公司、中译语通科技股份有限公司、北京万界数据科技有限责任公司的大力支持。

中国信息通信研究院 人工智能研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62301618

传真：010-62301618

网址：www.caict.ac.cn

