NIDA
全球固定网络创新联盟

甲子光年
JAZZYEAR

2026

企业智能体原生网络白皮书

面向Agent规模互联与任务协作的新型网络基础设施

出品机构：甲子光年智库
研究主笔分析师：黄琪丹
发布时间：2026年10月

目录

序言
PREFACE 01

新需求
PART 01 NEW DEMANDS

1.1 国家战略与政策需求：智能体已成为AI产业落地的重要载体 07
1.2 网络代际演进规律需求：智能体作为新服务对象改变网络需求 10
1.3 企业应用需求：企业智能体应用现状与挑战 12
1.4 网络能力升级需求：传统网络面临三大系统性矛盾 15

新趋势
PART 02 NEW TRENDS

2.1 智能体类型演进：从数字智能体到社会智能体 19
2.2 智能体技术演进：模型、Harness工程、环境与现实交互能力升级 23
2.3 AI与网络的双向赋能：从“AI+Network”到“Network ×AI” 27
2.4 企业智能体互联与任务运行：新型网络基础设施亟需构建 29

新定义
PART 03 NEW DEFINITION

3.1 企业智能体原生网络（EANN） 30

目录

3.2 企业智能体原生网络（EANN）的核心特征 32
3.3 自智网络（AN）与企业智能体原生网络（EANN）的关系 35

新范式
PART 04 NEW PARADIGM

4.1 企业智能体原生网络架构 38
4.2 企业智能体原生网络需要自智网络体系配套发展 43
4.3 企业智能体原生网络的典型应用场景 45

新未来
PART 05 NEW FUTURE

5.1 企业智能体原生网络关键技术建设 49
5.2 企业智能体原生化建设 51
5.3 产业参与主体建设建议 53

结语
CONCLUSION 55

定义者系列

THE DEFINER SERIES

定义者

DEFINER

定义未被定义之物

企业智能体原生网络

ENTERPRISE AGENT NATIVE NETWORK

NIDA 全球固定网络创新联盟 | 甲子光年 JAZZYEAR

NIDA全球固定网络创新联盟&甲子光年智库

2026

参编单位

甲子光年

NIDA 全球固定网络创新联盟

华为技术有限公司

北京沃东天骏信息技术有限公司

东南大学

中国矿业大学

厦门大学

白皮书编制与案例贡献人

张一甲	宋涛	黄琪丹
邓一鸥	王辉	曾维微
张俊	唐洁	孙磊
周琼	杨阳	陈晓筹
贠丽娜	朝日雅拉	李彤
花迩蒙	刘培剑	王兵

序言

PREFACE

张 一 甲

甲子光年创始人兼CEO

每一轮技术浪潮，都会指向同一个问题：技术的可能性，究竟如何成为产业现实？

这是甲子光年创立至今始终在探寻的核心命题。今天，人工智能正在完成从“生成范式”向“执行范式”的根本跨越，这一新范式让智能不再止于“说得出”，更要“做得到”：走入真实业务流程，直接承担任务、交付结果。

一个任务下达之后，识别、编排、执行、验收往往由分布在各处的智能体协作完成。当数以千计甚至万计的智能体在同一场域中彼此发现、按需协作，网络需要回答的问题，已经悄然改变。从单点能力突破走向规模化应用，需要与之相适应的基础设施和协作体系。智能体能否找到合适的伙伴、调用所需的资源、在可信边界内行动，将直接影响任务执行的效率与质量，而网络正是将分散的智能体组织为协同生产力的关键基础。

这也是我们开展企业智能体原生网络（EANN）研究的重要出发点。当连接对象具备了自主行动能力，协作关系需要随任务动态构建，网络就不再只是数据的传输管道，而需要升级为能够识别智能体身份、感知其能力、按需调度算力与服务资源的智能基础设施。“原生”的意义，在于将这些需求写进网络基础设施的底层设计，让智能体成为网络可直接感知、服务与治理的一等公民，获得贯穿接入、运行、协作、演进直至退出的全生命周期支撑。

本白皮书围绕企业智能体原生网络（EANN），系统梳理其内涵、架构与应用实例。其中，我

们做出的一个核心判断是：企业智能体原生网络需要自智网络体系配套发展。自智网络（AN）让网络能够自主感知状态、动态调度资源、无感处置故障；企业智能体原生网络（EANN）让智能体能够被精准发现、按需连接并获得安全执行保障，两者围绕业务任务需求与网络运行状态形成双向反馈，推动网络整体迈向高原生高自智方向。

从理念到落地，中间隔着的是产业现实。企业智能体原生网络（EANN）的建设既需要前瞻性的技术探索，也需要充分考虑产业发展的现实基础。企业长期积累的IT基础设施、业务系统与实践经验，是智能化转型的重要依托。新型网络能力的形成与成熟，需要立足真实业务场景，在持续实践中验证技术可行性与应用价值，不断提升任务执行效率、优化运行成本、增强服务可靠性，逐步探索可复制、可推广的建设路径。

甲子光年智库希望以这份白皮书，呼吁产业界共同关注智能规模化背后的“底座条件”。当分散的智能被可靠连接、有效组织，技术的可能性，终将在持续的协同中锻造成企业发展的新质能力。

王 辉

华为数据通信产品线NCE数据通信领域总裁
NIDA战略咨询委员会委员

智能时代，正在重写网络基础设施的底层逻辑。

2026年，人工智能加速从 “数字世界” 走向“物理世界”，从“能对话、能生成”迈向“能感知、能决策、能协同、能行动”。作为人工智能产品及服务的重要形态，智能体被明确置于承接“人工智能+”规模化落地的关键位置——国家目标要求到2027年新一代智能终端、智能体等应用普及率超过70%，到2030年超过90%。

当海量具备自主目标、自主能力的智能体大规模参与业务活动，它们不再只是网络的使用者，而正在成为网络的主体。这一角色转变，对网络基础设施提出了前所未有的要求：网络不能只承载数据转发，而要原生地支撑智能体的身份注册、能力发现、动态互联、任务协作、安全管控与全生命周期管理。

产业界正在形成共识：网络必须从“以人为中心”走向“以智能体为核心”，从传统网络演进到智能体原生网络。本白皮书沿“新需求—新趋势—新定义—新范式—新未来”的脉络，系统提出企业智能体原生网络（EANN）这一全新定义，完整刻画了面向Agent原生互联与任务协作的新一代网络基础设施范式，是产业界在智能体网络方向上难得的体系化思考，对行业把握方向、布局能力具有重要参考价值。

作为网络基础设施的深耕者和践行者，华为始终认为：智能化浪潮下，网络是智能的底座，智能体规模化的“最后一公里”在网络。我们的判断是，答案在于让网络自身“智能化”并“原生适配”智能体：一方面，构筑智能网元、智算、网络智能体与数字孪生融合的智能基础设施；另一方面，构建从网元级自治、单域自治到跨域协同自治的自智网络体系，使网络具备自主感知、自主决策、自主执行的能力，动态承接智能体从入网、发现、互联、协作、演进到退网的全生命周期需求。这是自智网络在智能体时代的关键跃迁，也将成为产业共同的技术演进方向。

技术因交互而进步，产业因协同而繁荣。我们期待以本白皮书为起点，与研究机构、产业伙伴和客户一道，共同深化智能体原生网络的技术探索、标准建设与生态共建，让智能时代的网络“连得上、联得动、信得过”，为人工智能的规模化落地夯实可信、高效、可持续的智能底座。

曾维微

京东集团IT总监

企业智能体原生网络（EANN）不仅需要为智能体提供原生连接与协同保障，更需要构建与之适配的高阶自智网络体系。

当前我们正站在企业IT运维智能化变革的关键节点，人工智能正以超越预期的速度从辅助工具演进为具备自主感知、推理与决策能力的智能体，企业IT服务由此迈入“人机协同、智能自治”的新阶段。智能体以“大模型+记忆+工具调用+规划能力”为内核，形成完整的感知-决策-执行闭环，正在重塑网络运维、终端管理、服务交付等核心场景的运作方式。对企业IT而言，这意味着运维模式将从“人力密集型”向“AI驱动型”加速跃迁，从“被动响应”走向“主动预防与智能闭环”。

京东企业IT承担着支撑集团全球业务高效运转的使命，覆盖办公网络、终端管控、会议保障、海外职场等全场景IT服务。业务的高速扩张与全球化布局，对IT基础设施的稳定性、敏捷性与智能化提出了极高要求。尤其在618、双11等大促场景下，超高并发交易、海量直播流量、数字人实时交互等业务对网络链路极度敏感，任何微小波动都会直接传导至前端业务，影响用户体验与营收。传统以人工主导、静态配置、被动处置为特征的运维模式，已难以承载智能体时代的使命。企业IT亟需构建主动感知、智能诊断、自动处置、持续进化的高阶自智能力，从“连接管道”演进为“连接+算力+AI”一体化的智能服务中枢。

高阶自智的核心执行单元，是可信的网络运维智能体。京东企业IT网络智能体「网衡」正是这一理念的先行实践。我们以Hermes架构为基座，统一MCP、A2A、HITL等能力，覆盖排障、巡检、告警、配置、变更等高频场景。更重要的是，我们通过A2A智能体互联技术，实现与京东自研IT运维智能体的双向深度协同，实现全网设备统一感知、统一管理、统一调度、统一闭环。面对复杂网络故障，双智能体可自动拆解任务、匹配最优工具，完成故障分析、定位与处置。同时，我们构建“人在环”运维机制，将人工审核与合规约束内嵌至AI全流程，确保关键变更与敏感操作可控可信。

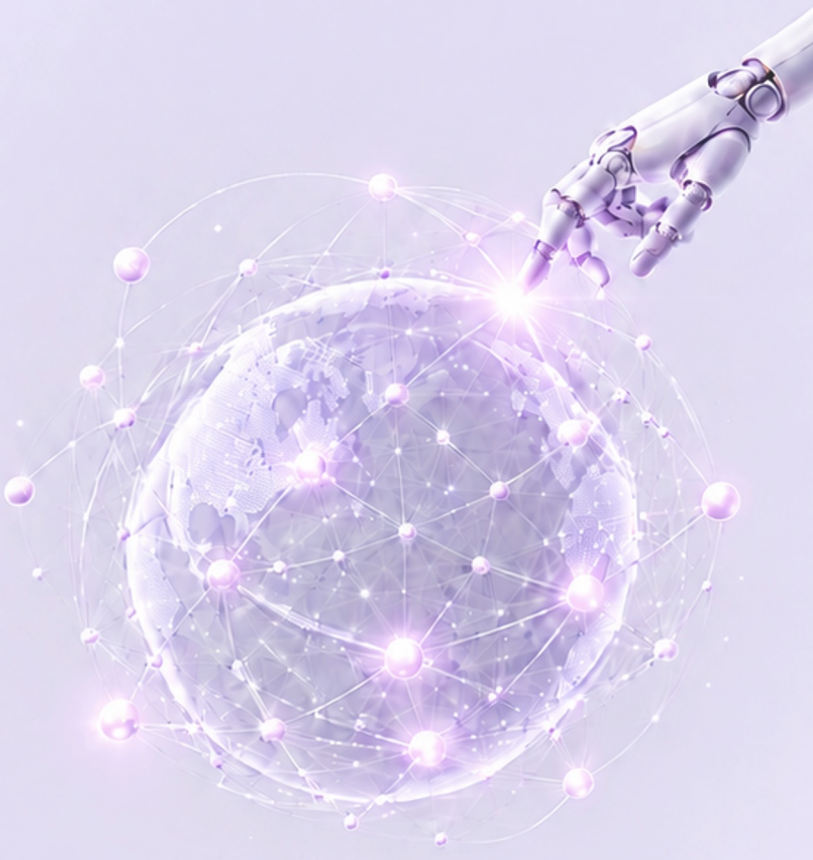
网络智能化是一场持久战，无捷径可走。京东企业IT愿与产业各方凝聚共识、协同创新，以场景突破夯实高阶自智根基，以开放心态参与行业标准共建与技术生态建设，为网络运维智能化转型输出可复制、可推广的实践样本，贡献京东企业IT的专业力量。

智能体原生网络（EANN）的建设并非一家之事，而是需要产业各方共同参与的系统工程。我们期待以本白皮书为契机，携手产业伙伴深化技术探索、推进标准共建、加速实践落地，共同推动网络自智与智能体原生能力协同演进。

Part 01

新需求

智能体时代的网络升级动因



1.1 国家战略与政策需求：智能体已成为AI产业落地的重要载体

1.1.1 战略导向：人工智能迈向国家发展与全球治理高位，智能体承接规模化落地

2026年，人工智能在国家发展与全球治理中的战略定位进一步提升。从3月**《政府工作报告》**首次提出“打造智能经济新形态”，到7月29日国家签署**《关于成立世界人工智能合作组织的协定》**，再到国家主席习近平在**2026世界人工智能大会暨人工智能全球治理高级别会议**上明确指出，人工智能是世界经济增长的新引擎和新旧动能转换的加速器，正在从“数字世界”走向“物理世界”，一条由国内发展部署向全球合作治理延伸的战略脉络加速形成。

人工智能已经不再只是推动局部效率提升的技术工具，而是日益成为培育新质生产力、重塑现代化产业体系、创造经济增长新动能并参与全球治理的重要力量。人工智能的发展重心也由模型能力突破，加快转向产业赋能、规模应用和普惠共享。

在人工智能战略地位持续提升的同时，智能体被明确置于承接“人工智能+”规模化落地的关键位置。2025年8月，**国务院《关于深入实施“人工智能+”行动的意见》**将新一代智能终端、智能体等应用普及率纳入国家发展目标，提出到2027年超过70%、到2030年超过90%；2026年5月，**国家网信办、发改委、工信部联合印发《智能体规范应用与创新发展实施意见》**，明确智能体是人工智能产品及服务的重要形态，围绕技术、标准构建、安全、治理、应用和生态作出系统部署；2026年6月，**工信部《“人工智能+信息通信”创新发展实施意见（2026—2028年）》**进一步推动智能体通信技术、网络智能体、工业智能体的发展。

三份政策由总体目标、专项规范向行业实施逐层深入，共同形成了以智能体承接人工智能能力、贯通行业场景并推动规模应用的清晰政策主线。智能体正从大模型的能力外延，跃升为人工智能贯通数字与物理世界、连接技术创新与业务行动、支撑单点应用到规模化落地的重要载体，推动人工智能由“能对话、能生成”加速向“能感知、能决策、能协同、能行动”演进。

1.1.2 能力要求：战略部署推动智能体发展自主执行、互联协同、安全可信三类核心能力

从政策要求看，智能体的发展围绕“能否独立完成任务、能否跨主体形成协作、能否在可控边界内运行”加快构建系统性能力。综合国内“人工智能+”相关政策，智能体的能力要求可以归纳为三个相互关联的方向：

一是自主执行，从提供辅助信息走向独立完成任务。智能体需要突破过去以问答和内容生成为主要功能的定位，形成涵盖目标理解、任务拆解、行动规划、工具调用、过程反馈与动态调整的完整能力链条。当前，相关部门已围绕智能体工具链建设，以及工业、教育、通信等行业的智能体应用作出部署，积极推动智能体升级为能够在授权范围内调用数据、软件和业务系统、自主完成任务的行动主体。

资料来源：政府各部门官网，甲子光年智库整理，2026年

二是互联协同，从单点运行走向多方协作。随着智能体应用大量涌现，并广泛进入制造、能源、教育和通信等各类实际场景，单个智能体由于能力有限，难以独立完成任务，需要随时随地找到其他智能体并协同开展工作。为此，相关政策进一步提出要推动智能体之间互联互通、多个智能体协同配合、群体协作以及通信对接等要求，加快建立覆盖身份识别、能力发现、规则统一、任务分配、协商配合和分歧处理等环节的协作体系，让不同种类、不同平台、不同归属的智能体能够围绕共同目标，协同完成复杂任务。

三是安全可信，从关注输出结果走向约束全过程行为。智能体自主程度越高、连接范围越广，其风险越可能从内容生成延伸至数据访问、工具调用、业务操作和跨系统传播。相关政策普遍将安全可控作为智能体规模化应用的基本前提，要求完善身份认证、权限控制、安全防护、过程留痕、异常干预和责任追溯机制，确保智能体身份可确认、行为可验证、权限不越界、风险可处置，在明确授权和可控边界内进入生产经营与社会运行的关键环节。

三类要求相互关联、协同作用：自主执行构成智能体完成任务的能力内核，互联协同拓展智能体处理复杂任务的能力边界，安全可信为智能体进入关键业务提供基本保障。

图1：国内“人工智能+”有关政策与智能体能力要求

政策名称、发布机构及时间	自主执行 目标理解 任务规划 工具调用	互联协同 身份发现 协议互通 群体协作	安全可信 权限控制 过程追溯 风险干预	政策关键词总结
《关于深入实施“人工智能+”行动的意见》 国务院，2025年8月	●	●	●	应用普及 人机协同 安全可控
《智能体规范应用与创新发展实施意见》 网信办、发改委、工信部，2026年5月	●	●	●	智能体工具链 智能体互联 安全可控
《“人工智能+制造”专项行动实施意见》 发改委、工信部等八部门，2026年1月	●	●	●	工业智能体 智能体互联互通 安全防护
《“人工智能+教育”行动计划》 教育部、发改委、工信部，2026年4月	●	●	●	教育智能体 安全防护
《关于促进人工智能与能源双向赋能的行动方案》 能源局、发改委等四部门，2026年4月	●	●	●	多智能体框架 安全治理
《“人工智能+信息通信”创新发展实施意见（2026—2028年）》 工信部，2026年6月	●	●	●	网络智能体 智能体互联网 安全治理

● 方向性支撑　● 直接提出/重点部署　● 由政策任务推导

资料来源：政府各部门官网，甲子光年智库整理，2026年

1.1.3 支撑升级：智能体应用发展倒逼基础设施协同升级，网络成为前瞻布局的关键方向

从政策脉络可以看出：战略层面，国家深入实施“人工智能+”行动，推动人工智能由技术创新加快走向行业融合与规模化应用，智能体被纳入国家应用普及目标，成为承接人工智能能力、进入行业场景的重要形态；能力层面，相关政策围绕自主执行、互联协同与安全可信，对智能体提出了更加系统的要求。

战略目标和政策要求表明，智能体能力不仅依赖模型自身演进，还需要计算、网络、存储、数据、安全以及开发运维平台等基础条件协同支撑。因此，基础设施升级不是可选项，而是智能体应用发展的必然要求。

在基础设施升级的各方向中，**网络是前瞻性突出、对智能体应用拓展影响较大的一环**。现有互联网和通信网络经过长期发展，已经具备较强的连接、传输和安全保障能力。但随着智能体数量增加、应用范围扩大，并由调用模型和工具进一步走向跨平台、多智能体协作，网络中的连接主体、交互关系和业务要求将更加复杂。智能体需要被识别和发现，不同平台需要实现协议与接口互通，跨域任务需要持续交换状态并协同执行，重要操作还需要具备明确的授权边界和审计能力。

现有网络可以通过能力增强支撑这些需求，但面向未来大规模、多主体、动态协作的智能体环境，仍有必要前瞻研究更加适配的体系架构与技术机制。

相关政策已释放出明确的网络演进研究信号。《智能体规范应用与创新发展实施意见》提出研究建立智能互联网体系架构，探索智能体注册、数字身份、检索发现、能力声明、可信互联和端到端通信等机制；《“人工智能+制造”专项行动实施意见》提出研制开放协同的智能体协议和接口；《“人工智能+信息通信”创新发展实施意见（2026—2028年）》围绕智能体通信、网络智能体和云网边端协同作出部署。

这些探索方向并非以全新体系替代现有网络，而是在现有网络基础上，持续增强智能体识别、互操作、协同保障与安全治理能力，同时研究面向智能体发展需求的新型网络架构。

资料来源：甲子光年智库整理，2026年

1.2 网络代际演进规律需求：智能体作为新服务对象改变网络需求

1.2.1 从语音到应用的四次代际跃迁：由连接人与信息走向连接应用，节点规模持续跃升

通信网络的演进呈现出业务载体、连接对象与节点规模同步跃迁的特征。电话时代，网络以承载语音、连接人与人为主，通信节点规模达到亿级；PC互联网时代，网站与网页成为主要业务载体，网络由“连接人”拓展至“连接人与信息”；移动互联网时代，智能终端与App加速普及，网络进一步连接人与应用，通信节点规模扩展至十亿级；进入云服务时代，应用、数据与算力向云端汇聚，云网融合推动网络由服务个人用户走向支撑应用与云端资源协同，通信节点规模迈向百亿级。

1.2.2 网络正在进入第五次代际跃迁——智能体互联时代

当前，通信网络正加速迈向新一轮代际跃迁，智能体逐步成为网络的重要服务对象。人工智能正由生成式AI向单体智能体、多智能体协同和智能体互联网演进，智能体也由被动响应指令的应用工具，转变为具备自主感知、决策、交互与执行能力的网络主体，网络连接对象随之由人、信息和应用进一步扩展至智能体。

伴随智能体由单体运行走向规模部署与联网协作，其形态将由运行于云端或应用层的“上层组件”，逐步演进为与云、网、边、端深度融合的“网络原生主体”，网络的核心定位也将由“连接信息”向“连接智能体”拓展。

与前四代通信网络不同，智能体对网络提出了全新要求。从企业智能体生命周期看，智能体要经历设计、开发、部署、运行到退役的完整过程，每个环节都离不开网络。设计开发需调用云端模型与数据、连接工具接口，部署接入

图2：通信网络代际跃迁

	01 电话时代	02 PC互联时代	03 移动互联时代	04 云服务时代	05 智能体互联时代
网络技术	电路交换	IP网络	3G/4G/5G移动网络	云网融合	智能体原生网络
业务载体	电话机、语音	浏览器	智能手机、App	云、应用、API	智能体
连接对象	人与人	人与信息	人与应用	应用	智能体
通信节点规模	亿级	亿级	十亿级	百亿级	百亿至千亿级

资料来源：甲子光年智库整理，2026年

需注册身份并被网络发现，运行阶段需持续感知环境并与其他智能体协同交互，直至退役仍需完成身份注销与权限回收，其全生命周期都运行在网络之上。

从调用访问看，智能体网络调用需求较高。Web应用峰值时每分钟处理数千至万次请求，单个智能体每分钟生成数十至数百次微决策，触发模型、数据或工具调用。一个任务往往需多个智能体协同完成，衍生多轮请求，智能体数量增加进一步推高并发调用。同时，智能体可持续在线数小时至数天，执行任务、同步状态，形成长周期、强状态、高联动的交互特征。

从安全合规看，智能体的自主性带来新的安全风险。云安全联盟(CSA)调研显示，超半数（54%）组织存在未经授权的“影子智能体”，仅8%的受访组织表示智能体从未超出预期权限*，智能体越权与治理缺位已成现实挑战。

1.2.3 作为新网络对象，智能体“量”的爆发与“质”的跃升，驱动网络能力要求跃升

服务对象由人/应用切换为智能体，不仅是简单的对象替换。智能体本身的全新特性，叠加其数量规模的爆发式增长，正共同对网络能力提出新诉求。

- **连接规模：**智能体需要支持海量并发的接入网络。据IDC预测，全球活跃Agent数量将从2025年的约2860万快速攀升至2030年的22.16亿，年复合增长率139%。连接数量爆发考验网络的并发接入能力，现有网络通信节点数量与网络接入能力难以满足智能体接入需求。

- **承载能力：**智能体需要大带宽、高吞吐、上下行均衡的网络。Token调用量增长与多智能体并发交互，增加了上下文、调用结果等数据的传输需求，要求网络具备更大的带宽容量与更高的吞吐能力。上下文、感知数据及执行结果的持续上传进一步推高上行负载，推动传统“下行宽、上行窄”的接入网络向上下行更均衡的承载能力演进。

- **交互方式：**智能体需要支持高频、突发式交互的网络。人机交互由人触发，节奏受限于人的操作，以秒级、分钟级计；智能体间则是机器驱动的持续交互，一次任务全程需频繁共享上下文、多轮意图交互与自主协商，心跳同步、状态上报等行为使交互不间断发生，交互节奏由秒级、分钟级迈入毫秒级。

- **时延要求：**智能体需要毫秒级低时延的网络。传统架构下的排队时延直接影响智能体任务执行的实时性与稳定性，智能体需要的毫秒级时延相较传统业务的百毫秒级收紧约百倍。

- **故障容忍：**智能体对故障零容忍，需要高可靠、不中断的网络。智能体推理任务中断超过数秒即需重启，中断成本达普通计算的百倍以上；且多智能体任务链中，单一智能体的离线或异常若引发全局任务中断、回滚或重启，将浪费大量算力并破坏体验。

资料来源：云安全联盟（CSA）调研《Enterprise AI Security Starts with AI Agents》，IDC，甲子光年智库，2026年

1.3 企业应用需求：企业智能体应用现状与挑战

1.3.1 应用现状：企业智能体加快进入核心业务流程，行业落地呈梯次深化

企业智能体正由试点验证迈入生产应用，加速嵌入核心业务流程。IDC数据显示，2026年全球已有72%的企业将智能体投入生产，51.6%的企业将其嵌入核心业务流程；预计到2027年，智能体自动化将增强40%以上企业应用的能力，重塑约三分之一的业务流程和工作流。

智能体在垂直行业的应用同步深化，且呈现出明显的梯队分化。互联网与金融处于领先梯队，互联网企业凭借技术、数据与平台优势，率先将智能体嵌入研发、运营和客户服务等流程；金融机构则推动智能体向风控、客服、合规等专业业务深入。工业与医疗处于加速渗透梯队，应用分别覆盖设备巡检、工业设计、经营管理以及辅助诊断、电子病历、患者随访等场景。零售处于规模拓展梯队，智能体逐步进入客服、营销和选品等经营环节；政务与教育处于场景培育梯队，主要围绕数据管理、便民服务、教学辅导和教学管理展开；物流与能源仍处于探索阶段，应用集中于路径优化、仓储自动化、智能巡检和智能调度等单点环节。

互联网、金融、教育与工业分别代表技术原生、专业决策、教学重构与工程流程四类落地形态，这些代表性实践集中反映了企业智能体由辅助工具向核心业务执行主体演进的主要路径。

- **互联网行业凭借技术、数据与平台优势，率先将智能体嵌入研发、运营与客服流程，并同步展开管控体系探索。**如微软在内部Microsoft Digital部门建立智能体治理结构，围绕安全、隐私、监管三项原则设定护栏；谷歌DeepMind发布AI Control路线图，将内部智能体视为潜在“内部威胁”，以实时监控、访问控制与关停基础设施构建防御机制；Meta提出“Agents Rule of Two”设计规范，同一智能体在单个会话中最多只能同时具备处理不可信输入、访问敏感系统、对外通信或变更状态三项能力中的两项。

- **金融行业智能体已深入风控、营销、财富管理等核心业务，并由辅助分析走向业务决策与流程执行。**如蚂蚁集团的金融智能体矩阵覆盖风控建模、智能投顾、保险理赔等岗位，推动专业能力向多业务环节复用；京东支付的风控智能体通过多源信源监测、风险识别与行为溯源，缩短风险发现与处置时间，提升全流程风险防控效率。

- **教育行业围绕育人服务主线，将教学智能体引入知识服务体系，在高校与企业两侧同步推进。**高校侧，清华大学上线“清小搭”智能体学伴，支撑个性化教学；上海交通大学支持教师自定义不同教学场景的智能体。企业侧，科大讯飞推出星辰Agent平台，好未来发布教师智能体“九章龙虾”与伴学智能体“小精龙”，猿辅导上线“飞象老师3.0”，智能体正重构教育服务模式。

资料来源：IDC，CIDC&科智咨询《AI智能体赋能行业决策：趋势与实践白皮书（2026）》，甲子光年智库，2026年

- **工业行业的智能体应用深入工程执行核心环节，从生成建议走向完成完整的工程任务。**西门子推出专为自动化工程打造的Eigen工程智能体，直连TIA Portal，通过多步推理与自我修正，自主完成PLC编码、HMI可视化与设备配置任务，并按客户标准验证输出。该工程智能体相较手动工作流效率提升2至5倍，已经在19个国家的100多个客户中试点运营。罗克韦尔联合微软构建代理式AI原生工程能力，将数字工厂设计、自动化逻辑生成与性能验证整合为连续工作流，打通从概念、仿真到控制器设计与验证的闭环，缩短耗时并减轻对高度专业化技能的依赖。

智能体正从单点场景向业务流程全面渗透，正演进为核心业务的执行主体并承接关键任务，这对支撑其稳定有效运转的网络基础设施也提出了新的要求。然而，现有网络的智能体原生适配、网络相关的智能体评估体系与智能体协同的网络保障机制远未跟上这一进程。

图3：国内智能体垂直行业应用梯队及典型场景



资料来源：CIDC&科智咨询《AI智能体赋能行业决策：趋势与实践白皮书（2026）》，甲子光年智库，2026年

1.3.2 挑战：网络适配、运行评估与协同保障能力存在缺口，难以满足智能体规模化应用

一是网络自身的智能化升级明显滞后于智能体应用发展，传统运营与业务支持系统（OSS&BSS）向智能体原生架构的演进仍较为缓慢。IBM与TM Forum面向全球电信高管开展的联合调研显示，运营商网络自智水平平均仅为1.9分（满分5分），达到L4高度自智水平的运营商仅占6%，其背后的重要原因在于长期积累的遗留系统负担。传统运营与业务支持系统经过数十年持续建设，形成了多系统并存、多厂商共存的复杂格局，普遍存在架构老旧、系统割裂、数据分散等问题，已经成为制约电信网络智能化转型和价值释放的重要瓶颈。IDC与爱立信联合研究指出，传统运营与业务支持系统本质上仍是面向过去的网络需求构建；麦肯锡调研显示，不到一半的运营商具备足以支撑AI应用场景的数据质量。此外，运营商仍需要花费较多的IT预算用于维护既有系统，而非投入创新。面对庞大而复杂的存量系统，运营商难以通过一次性替换完成架构升级，只能在新旧系统长期并存的条件下持续推进演进。系统集成复杂、数据孤岛突出、治理体系不完善等问题也将长期伴随这一过程。运营商需要在保障现网稳定运行的基础上，逐步将智能体能力嵌入既有网络与运营体系，通过渐进式演进，完成系统设施向智能体原生架构的转型。

二是当前智能体测评体系普遍缺乏网络维度的度量标准，导致大量智能体在生产环境中表现不及预期。现有主流基准测试多在理想网络条件下运行，以任务完成度为核心考核指标，普遍未将时延、吞吐量、丢包率等基础设施指标纳入评测框架。网络长期处于考核盲区，智能体在研发与选型阶段缺乏针对真实网络环境的优化依据与筛选手段，智能体在实验室的基准成绩难以代表其在生产环境中的实际水平。基准测试环境与真实网络条件的偏差最终将在运行阶段集中暴露，推高了企业的治理成本与业务风险。Gartner预测，到2027年底，超过40%的智能体项目将因成本失控、商业价值不明或风险控制不足而被取消。

三是多智能体协同运行缺乏与之匹配的网络保障能力，尚难满足关键场景的高可靠要求。随着智能体规模扩大、协作链路延长，单点错误可能在智能体之间持续传导并逐级放大，导致系统整体稳定性下降，非预期行为与级联故障成为新的风险来源。尤其在金融、工业等关键场景中，业务对可靠性和连续性要求极高，局部网络故障或协同异常都可能被迅速放大，进而引发监管处罚、业务中断甚至安全事故。然而，传统网络安全与风险防御体系主要面向外部威胁，以边界防护为核心，而多智能体协同产生的风险更多源于系统内部的自主交互与行为叠加，现有保障机制难以有效应对。Economist Enterprise调研显示，98%的受访企业已经历过由智能体引发的破坏性事故，近九成受访企业认为，智能体的部署速度已经超过其评估、治理和安全防护能力。

资料来源：IBM&TM Forum《Navigating autonomous Networks》，IDC&爱立信《Mapping the OSS/BSS transformation journey》，EY，Gartner，Economist Enterprise，甲子光年智库，2026年

1.4 网络能力升级需求：传统网络面临三大系统性矛盾

1.4.1 性能失配矛盾：传统网络面临承载能力、负载节律与质量保障三方面失配

智能体转变为持续在线、自主执行和多方协作的网络主体，其通信方式是贯穿任务全过程的机器持续交互。由此，网络既要承载大上行与大规模东西向流量，又要应对持续并发和短时集中汇聚，还需为多环节任务链提供低时延、低抖动与高可靠保障。传统网络能力体系难以适应上述变化，具体表现为承载能力、负载节律与质量保障三重失配。

一是承载能力失配，现有网络管道窄细，难以承接大上行与东西向并重的新格局。 传统企业网络主要围绕“用户访问中心服务器”设计，流量以南北向传输为主，并长期按照“下行粗、上行细”的非对称模式建设，下行占比长期高于85%。智能体运行后，一方面需要持续上传感知数据、环境状态和任务执行结果，推动上下行流量趋于对称；另一方面，智能体之间以及智能体与模型、数据库、工具之间需要频繁调用，产生大量服务器之间的东西向通信。邬贺铨院士在2026年的专题分析文章《智能体全面重构算力、网络与云，集体智能涌现》中的数据显示，智能互联场景中东西向流量占比将提升至80%，上行占比从10%-15%攀升至40%-50%。思科调研预计，代理式AI应用将在未来12个月和36个月分别带来57%和112%的网络流量增长，高于同期生成式AI以及物理AI，成为三类AI工作负载中增长最快的网络流量来源，且67%的受访组织已经观察到内部系统或应用之间的东西向流量增加。

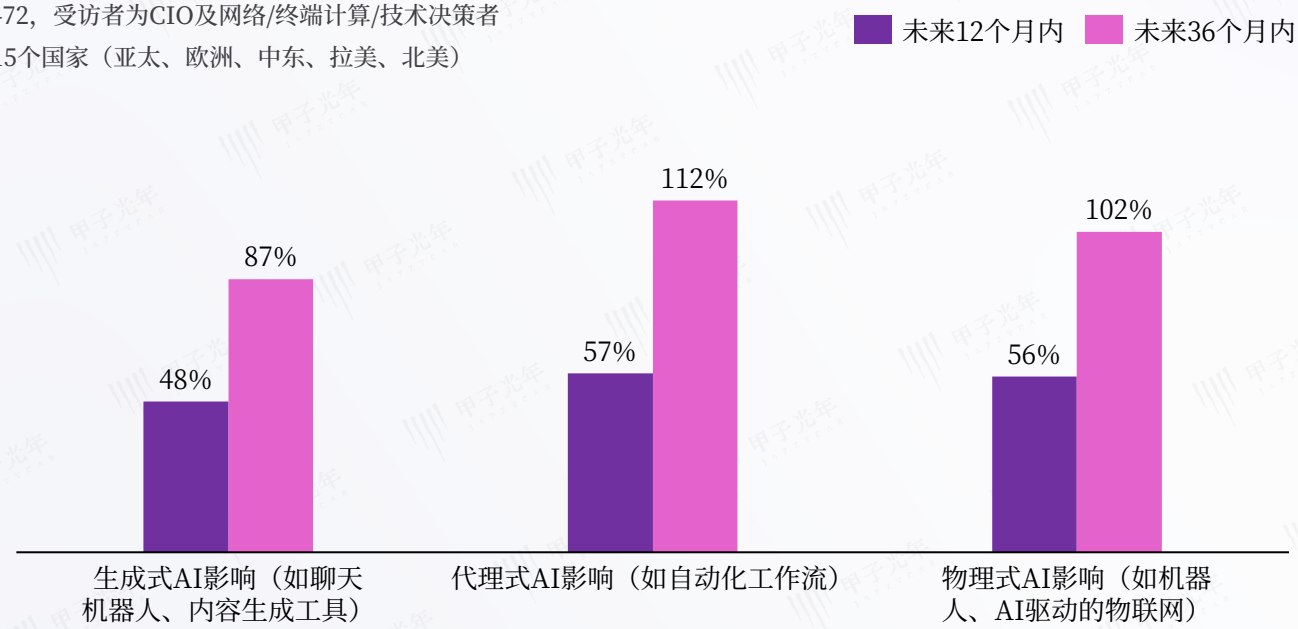
二是负载节律失配，网络流量节奏由人工触发的间歇访问转向智能体驱动的持续性与集中并发性。传统应用请求主要由人的操作触发，请求之间存在自然间隔，网络流量具有可重试、可缓冲的特征。智能体在多轮推理和任务执行过程中始终保持在线连接，持续产生模型调用、数据查询与工具访问等流量，网络负载呈现自动持续特征。同时，多个智能体可能围绕同一任务作出响应，请求在短时间内大量汇聚，形成瞬间峰值。相较于传统应用请求，智能体流量的持续性与并发性使网络负载节奏发生根本性变化。思科调研显示，在AI应用过程中，61%受访者已经观察到持续自动化流量增长，49%受访者已经观察到突发或峰值驱动型流量增长。

三是质量保障失配，网络质量诉求由“尽力而为”转向低时延、低抖动与高可靠。 传统网络允许部分业务通过排队、重传等方式消化性能波动，少量丢包对网页浏览、视频点播等场景影响有限。但智能体任务通常由多个交互环节串联组成，且前后环节高度依赖，时延、抖动或丢包等网络质量问题所引发的负面影响会沿任务链成倍放大。以研发智能体从Gitee拉取代码并调用DeepSeek进行修改为例：仅10%的网络丢包，不仅会导致拉取直接失败，还会引发智能体频繁重试，最终造成4倍的Token无谓消耗，并将整体任务时长拖慢8倍，局部网络劣化的代价远超网络丢包本身。思科调研显示，在AI系统应用过程中，64%的受访组织已经观察到实时或时延敏感流量增长。

资料来源：思科《No time to wait: The accelerating impact of AI on campus and branch networks》，甲子光年智库，2026年

图4：AI应用预计将推高网络流量

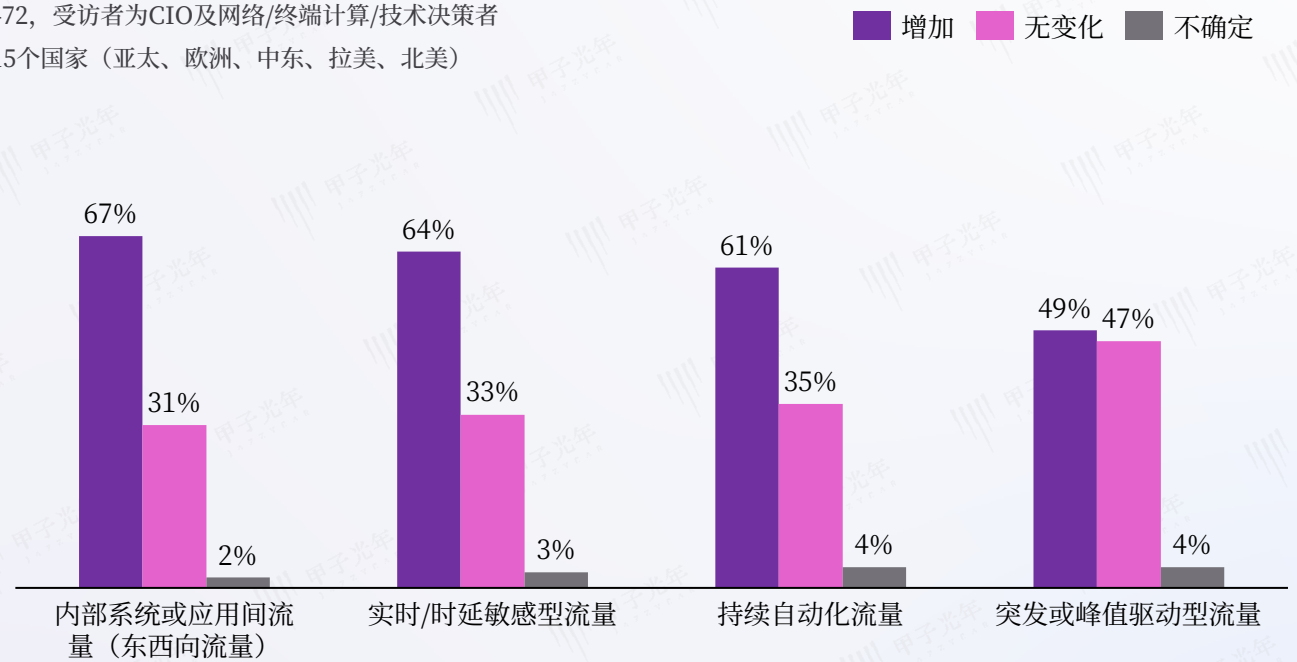
N=3472，受访者为CIO及网络/终端计算/技术决策者
覆盖15个国家（亚太、欧洲、中东、拉美、北美）



注释：数据为三类AI流量增长预测叠加后的综合增幅，并非简单平均；100%表示流量较当前翻倍。

图5：AI应用正在重塑园区与分支网络流量形态

N=3472，受访者为CIO及网络/终端计算/技术决策者
覆盖15个国家（亚太、欧洲、中东、拉美、北美）



注释：图中数据为观察到不同类型流量变化的受访者占比，各类流量特征相互独立。

资料来源：思科《No time to wait: The accelerating impact of AI on campus and branch networks》，甲子光年智库，2026年

1.4.2 复杂性失配矛盾：智能体使网络管控超出人工能力边界

智能体的规模化接入和自主运行，不仅扩大了网络管控对象规模，也使网络行为、安全风险与运行状态加速变化。传统依赖设备指标监控、对外防守和人工经验处置的管控体系，难以应对网络运营复杂度的增长，具体体现为三个方面：

一是传统监控手段无法有效追踪智能体的行为轨迹。 随着智能体实例数量快速增长、自主决策链路日益复杂，传统运维监控手段已无法有效感知智能体的内部推理过程与联网行为轨迹。企业普遍面临“行为不可见、风险难预警、故障难定位、责任难界定”四大管控难题，安全防护正从“城堡式”边界防御向智能体内生的安全治理演进。导致管控难题的根源在于，智能体的决策基于大语言模型内部的复杂参数计算，推理过程对管理员不可见，行为链路穿越多个推理环节后难以准确还原决策原因，加剧审计与追溯难度。

二是AI驱动的网络攻击速度与隐蔽性远超人工响应能力。 思科调研显示，85%的企业在过去12个月内至少经历过一次无线安全事件，而在导致无线网安全威胁加剧的原因中，受访者提及最多的（35%）是AI生成或自动化的网络攻击。与传统攻击相比，AI网络攻击能够根据防御方的反应调整攻击策略，并以超过人类攻击者的规模和速度运行。进一步地，智能体的高自主性带来了更大的内生风险，其自主决策行为在真实部署中呈现出不可预测性，目标约束不足（如持续追求利益最大化而采取风险路径）与外部对抗性输入（如数据投毒）均可成为突出问题。

三是网络运营复杂度指数级增长，人工运维模式已触及天花板。 传统网络行为可预测程度高、故障模式有限、响应时间要求低，运维工作以人工监控告警、人工诊断故障、人工执行处置为主，基本能够满足需求。但在智能体规模化接入条件下，这一模式的局限性被全面放大。网络及系统设备配置规模激增，超出人工梳理的认知边界；智能体自主决策引发的行为变化与风险传导以秒计，不同类型的安全风险动态关联、相互传导，单点触发即可沿智能体协作链路快速扩散，人工被动响应的运维效率已无法匹配智能体时代的运营要求。

1.4.3 算网失配矛盾：算网协同不足，网络“不知算”、算力“不知网”

从整体架构设计看，算网协同深度不足正在成为制约智能体广泛部署的核心瓶颈。 随着大模型与智能体走向产业应用，AI基础设施的性能瓶颈正从单点算力转向系统协同，训练与推理效率不仅取决于算力峰值，而且取决于数据从存储到计算的流转效率。网络不再只是算力节点间的数据传输管道，更是提升算力效率的关键，算网协同的深度将直接影响智能体互联时代算力资源的实际可用水平。

然而，在实际业务中，大模型推理“输入短、输出长”形成显著的非对称流量，多智能体协同又带来大量东西向通信，东西向流量占比将从传统IT时代的20%攀升至80%，流量方向、规模与资源需求更加动态复杂。传统网络主要

资料来源：思科《State of Wireless 2026》，阿里云《AI网络白皮书》，甲子光年智库，2026年

面向南北向流量设计，流量路径与带宽配置相对固化，网络与算力长期相对独立建设和优化，难以根据任务需求统筹算力资源与网络资源，容易造成局部网络拥塞、算力资源错配等问题。这种算网架构上的相互割裂，进一步表现为网络与算力之间双向感知能力不足。

一是现有网络对算力状态的感知不足，难以实现面向算力负载的智能分流。传统负载均衡主要依据连接数、请求数等网络侧指标进行流量分配，缺乏对算力负载、显存占用、任务队列等关键状态的实时感知，难以准确判断不同算力节点的实际服务能力，导致推理请求无法动态匹配至最合适的算力节点，容易出现部分节点持续过载而部分节点资源闲置，降低整体算力资源利用效率。

二是算力调度对网络状态的感知不足，难以实现面向网络状态的动态选算。现有任务调度更多关注算力节点自身的资源状态，对网络带宽、时延、拥塞等实时状态考虑不足。根据IDC调研，AI大模型训练中数据通信耗时占比已达30%-40%，在复杂并行策略场景甚至达到50%-70%，但算力侧的调度决策并未将这一通信开销纳入考量。在跨节点、跨集群的智能体任务中，即使目标节点具备充足算力，也可能因网络路径拥塞、带宽不足或传输时延较高，导致数据传输成为任务执行瓶颈，出现“有算力、用不好”的问题，尤其在实时交互、工业控制等时延敏感场景中，难以保障端到端任务执行效率。

资料来源：IDC，阿里云《AI网络白皮书》，甲子光年智库，2026年

Part 02

新趋势

智能体类型与能力演进催生网络新形态



2.1 智能体类型演进：从数字智能体到社会智能体

2.1.1 智能体能力边界持续外扩，正从数字世界走向物理、科学与社会世界

从智能体所处环境及需要理解的世界规律出发，智能体能力可概括为数字智能、物理智能、科学智能与社会智能四种形态，分别对应数字、物理、科学与社会智能体。智能体技术正由单一数字任务执行向复杂开放环境拓展，其作用对象从软件与数据扩展至物理实体、科学实验及多主体社会环境，能力内涵也从遵循既定规则完成任务，走向感知现实世界、探索未知规律、与其他主体协同行动。四类智能体并非严格替代的线性阶段，而是反映了能力边界不断外扩、环境复杂性与交互主体多样性持续提升的演进趋势，在各自领域独立演进、相互借鉴。

- **数字智能体：**发展最早、成熟度最高的分支，对应数字世界模型，其活动范围局限于数字空间，学习的是软件系统、代码逻辑、界面交互等形式化规范与状态转移规律。数字智能体以大模型为核心引擎，通过调用API、访问数据库完成任务，不作用于物理实体。数字智能体涵盖当前成熟的软件智能体，包括对话智能体、办公协作智能体、代码智能体以及面向金融、医疗、法律等领域的业务智能体。IDC调查显示，全球95%的企业现在至少有一项由公司出资、接入智能体能力的工作流已正式运行，平均每家企业约有11项这样的工作流分布在不同业务部门。其中，智能体工作流最集中于IT运维与软件开发领域（占71%的企业），其次是客户服务与支持（43%），以及供应链与采购（36%）。

- **物理智能体：**对应物理世界模型，属于具身智能范畴，其核心特征是能够感知真实物理环境并执行实体操作，所学习的是几何、运动学、守恒定律等物理世界的运行规律。物理智能体通常搭载多模态传感器（视觉、触觉、激光雷达等）感知环境，并通过机械臂、关节等动作执行部件与物理世界交互，依托VLA（视觉—语言—动作）模型实现从感知到行动的端到端决策。物理智能体面对的是连续、非结构化、充满不确定性的真实环境，障碍物的位置、物体的物理属性、任务场景的动态变化都无法像代码逻辑那样被精确定义。典型形态包括工业机器人、移动机器人、四足机器人和人形机器人等，已应用于柔性制造、设备巡检、仓储物流及家庭服务等场景。物理智能体是当前产业热度上升最快、成熟度仅次于数字智能体的第二大分支。中国信通院数据显示，2025年全球人形机器人出货量达1.2万台，同比增长420%；IDC预计，从2026年起，未来五年中国具身智能支出将由14亿美元增长至770亿美元，年复合增长率达94%。

- **科学智能体：**科学智能体是面向科学发现的前沿形态，通过整合科学世界模型、自主规划、工具调用与证据验证等能力，参与文献研究、提出假设、设计实验、分析结果和修正模型等科研环节。当前该方向整体仍处于早期阶段：一类实践聚焦于构建科学世界模型，作为科学智能体的底层模型，通过学习气象、分子、材料和生物等领域的演化规律

资料来源：港科大、新加坡国立、清华、港中文等《Agentic World Modeling: Foundations, Capabilities, Laws, and Beyond》，IDC，甲子光年智库整理，2026年

开展模拟预测，如气象预报领域的GraphCast、盘古气象，生命科学领域的AlphaFold、材料科学领域的MatterGen等；另一类实践将智能体引入科研工作流，辅助完成文献检索、创意生成、实验执行和结果验证，如AI Scientist、A-Lab自主实验室等。二者进一步融合后，科学智能体有望由科研流程辅助走向覆盖科学发现全过程的自主系统。

- **社会智能体：**是四类智能体中成熟度最低、发展最前沿的形态，面向由人类、数字智能体与物理智能体共同构成的动态社会环境，通过理解不同主体的信念、意图、关系与行为规范，开展沟通、协商和协同行动。随着各类智能体规模化接入，社会智能体将进一步走向分工协作、自主组织与动态演化，形成智能体社会。社会世界模型是支撑这一能力的关键基础，即对人类社会动力学的可计算表示，用于模拟不同主体的行为及相互影响，预测社会状态演化。当前社会智能体仍处于早期探索阶段，以社会模拟器为主，这些实践尚不等同于成熟的智能体社会。例如，中国人民大学团队打造的社会模拟器已可运行超过1350万个智能体，覆盖100多个国家。

2.1.2 数字、物理、科学与社会四类智能体对网络诉求的异同

四类智能体虽然形态各异，但其网络诉求存在一定共性。**总体来看，低时延、高可靠与安全治理是各类智能体的共同诉求。**

- **网络流量与性能：一方面是低时延需求，**智能体的工作模式为“感知-理解-推理-执行”的迭代循环，每一轮推理都依赖上一步的网络往返，时延在多轮循环中积累放大，若时延过长，期间用户长时间处于等待状态，工作流将被迫停摆，任务效率被迫拉低。**另一方面是高可靠需求，**智能体任务执行具有长链路特征，任务往往持续数分钟到数小时，涉及多轮推理，后一步通常依赖前一步结果。一旦网络中断，中间结果丢失，任务可能前功尽弃。

- **安全治理：**智能体需要主动调用外部工具、访问数据并与其他主体交互，这种“向外走”的特性打破了传统的防守式安全机制。一旦智能体身份被冒用，攻击者便可能继承其访问权限，调用工具、读取数据甚至执行高风险操作；数据在跨主体、跨系统和跨域流转过程中，也面临越权访问、泄露与违规使用风险；智能体的自主决策链路若缺少记录，则难以还原操作过程、定位责任并及时阻断异常行为。因此，统一身份标识、数据防护以及风险监测与审计成为共性刚需。同时，智能体基于大模型运行，数据投毒、模型操纵等攻击通过正常交互通道直击推理过程，防护必须嵌入运行过程，内生安全同样不可或缺。

除共性需求以外，由于四类智能体所处环境和运行方式不同，其对网络能力的具体需求呈现明显分化。

- **数字智能体：**主要运行于云端、数据中心及各类软件环境，其交互对象以数据、API、工具和其他智能体为主，典型形态包括金融、教育、政务、客服等领域的数字员工。由于

资料来源：港科大、新加坡国立、清华、港中文等《Agentic World Modeling: Foundations, Capabilities, Laws, and Beyond》，甲子光年智库，2026年

高度依赖外部工具调用与多智能体协作，其对协议互操作、意图路由和身份寻址、统一身份标识的需求较为突出。

平台碎片化背景下，数字智能体需要借助MCP、A2A、ANP等协议，实现与工具及其他智能体的跨平台交互；需要依托意图路由，根据任务目标和能力需求动态匹配适合的智能体，并进一步确认智能体的网络地址；还需要通过统一身份标识和访问控制完成可信认证、行为追溯与权限管理。由于数字智能体通常不涉及海量终端接入和大规模感知数据的持续上传，其对大带宽、高吞吐及超大规模连接的需求相对适中。

- **物理智能体：**直接感知并作用于真实物理世界，通过传感器和摄像头采集环境信息，依托端侧或边缘计算节点完成推理决策，再由机器人本体、机械臂、车辆等执行机构采取行动，从而形成感知、决策与执行的实时闭环。典型形态包括工业机器人、巡检机器人、仓储物流无人车、自动驾驶汽车和无人机等，应用于制造、能源、物流、交通及低空经济等场景。

与数字智能体不同，物理智能体需要持续上传多模态感知数据，并在端、边、云之间实时传递推理结果、控制指令与设备状态，任何传输延迟、中断或数据丢失都可能影响动作准确性与运行安全，甚至造成直接物理伤害，因此对低时延、大带宽与高吞吐、高可靠以及云边端协同的需求最为强烈。此外，多机器人协作与车联网场景还要求智能体之间自主组网，动态组网需求同样突出。

- **科学智能体：**需要围绕科研任务调用分布在不同机构和网络域的科学数据、算法模型、算力平台与实验设施，因此对大带宽、高吞吐、跨域互联和高可靠的需求较为突出。具体来看，大规模观测数据、模型参数和模拟结果需要在数据中心与算力节点之间高效传输；跨机构协作则要求网络支持异构资源的统一接入、可信认证与安全流转，并根据科研流程将数据和计算任务动态调度至适合的处理节点。

根据数据局披露，2025年，国内7家国家科学数据中心联合建设CoNet科学数据协作平台，接入2.1万个数据资源和2453个算法模型，通过跨域调度支撑卫星数据协同处理、多天文台星表交叉认证等科研任务，反映出科学研究对跨域数据、模型与算力协同的现实需求。相对而言，科学智能体主要连接专业科研资源，较少涉及海量终端接入和网络拓扑的频繁变化，对超大规模连接与动态组网的需求相对较弱。

- **社会智能体：**由大量数字智能体与物理智能体在网络空间中持续互动形成，群体协作将推动网络通信由少量主体间的点对点交互，转向超大规模主体间的多对多通信。不同智能体需要围绕共同任务动态发现能力，开展状态同步、信息交换、协商决策与分工执行，因此网络既要支持超大规模连接和高并发通信，也要通过协议互操作与意图路由动态匹配智能体。随着协作规模扩大，局部突发流

资料来源：港科大、新加坡国立、清华、港中文等《Agentic World Modeling: Foundations, Capabilities, Laws, and Beyond》，数据局，EOSC-PL《Connecting Researchers to Federated European Science》，甲子光年智库，2026年

量可能汇聚为全局通信压力，大带宽与高吞吐需求随之凸显。关键消息的延迟、丢失或错误也可能沿协作关系扩散，影响群体决策与任务结果，因此低时延和高可靠同样是基础要求。与此同时，智能体分布于不同平台、地域及云边端节点，协作关系随任务实时建立与解除，对动态组网、跨域互联及云边端协同提出较高要求。群体协作还会放大身份冒用、错误传播和责任追溯等风险，需要安全治理机制，保障多主体交互可信可控。

图6：四类智能体网络需求对比

● 强需求　◑ 相对中等需求　◔ 相对弱需求

一级维度	二级维度	数字智能体	物理智能体	科学智能体	社会智能体
流量与性能	低时延	●	●	●	●
	大带宽与高吞吐	◑	●	●	●
	高可靠	●	●	●	●
	超大规模连接	◑	◑	◔	●
协议与互通互联	互操作协议(MCP/A2A/ANP)	●	◑	◑	●
	意图路由与身份寻址	●	◑	◑	●
架构与组网	边缘-云协同	◑	●	◑	●
	动态组网	◑	●	◔	●
	跨域互联	◑	◑	●	●
安全治理	统一身份标识	●	◑	◑	●
	数据防护	●	●	●	●
	内生安全	●	●	●	●
	风险监测与审计	●	●	●	●

注释：社会智能体按照大量数字智能体与物理智能体协同运行的目标形态进行判断，不代表当前社会模拟器的实际网络需求。

资料来源：港科大、新加坡国立、清华、港中文等《Agentic World Modeling: Foundations, Capabilities, Laws, and Beyond》，数据局，EOSC-PL《Connecting Researchers to Federated European Science》，甲子光年智库，2026年

2.2 智能体技术演进：模型、Harness工程、环境与现实交互能力升级

2.2.1 模型能力：通用基模融合行业数据与企业知识，形成模数共振，突破专业数据瓶颈

行业数据的有限供给，是制约智能体专业化发展的关键因素。Epoch AI在2024年发表于ICML的论文中估算，全球公开人类文本语料的有效存量约为300万亿Tokens，若按假设的趋势延续，该语料存量将在2026—2032年间耗尽，中位时间为2028年。相较于公开语料，行业数据更加稀缺，普遍分散在企业业务系统和专业机构中，还具有专业性强、标准不一、持续变化和敏感程度高等特点。在数据供给有限、训练成本高企的条件下，从零训练行业基础大模型既缺乏足够数据支撑，也难以形成合理的投入产出比。

为突破专业数据瓶颈，现有主流行业大模型形成“通用基模＋行业微调＋RAG+记忆机制”的能力构建路径。通用基模提供语言理解、推理与任务规划等通识能力；行业微调利用专业语料和业务样本，把行业中的业务流程与案例经验内化到模型参数中；RAG在推理过程中动态调用企业知识库及实时业务数据，补充最新专业知识；记忆机制则沉淀用户偏好、历史任务与交互经验，使智能体能够结合上下文持续优化决策。由此，有限的行业数据与企业知识能够被反复调用、组合和更新，弥补通用模型专业知识不足，使智能体从“掌握通识”走向“理解业务”。

与此同时，模型与数据之间正在形成持续迭代的模数共振机制，由单向供给关系转变为双向迭代关系。一方面，经过治理、标注和评估的行业数据与企业知识，通过微调、RAG等方式持续注入模型，提升模型的专业知识、业务理解与任务执行能力；另一方面，模型在训练、测试和实际应用中识别出的低质量样本、知识缺口与能力短板，以及智能体执行任务产生的交互记录、人工修正和结果反馈，又可用于优化数据集、更新知识库并生成新的训练样本。由此形成“数据处理—模型训练—性能评估—业务应用—反馈优化”的闭环，使数据供给能够随模型表现和业务需求动态调整，推动模型能力与行业知识同步迭代，缓解专业数据数量有限、质量参差和更新滞后的问题。

主流行业模型的构建机制与模数共振正在改变数据流动方式，推动网络从支撑单次单向的数据传输，向支撑高频、双向、持续的数据交互演进。模型微调、RAG与记忆机制使模型持续调用行业数据与企业知识，数据在模型与业务系统之间高频流动；模数共振进一步使模型运行产生的结果与业务反馈持续回流，驱动数据供给与模型能力迭代更新。数据交互频次、方向与持续性的变化，对网络的高带宽、低时延、高可靠与动态调度能力提出更高要求。

2.2.2 智能体工程框架：Harness持续深化，推动智能体调用链路持续延长和复杂化

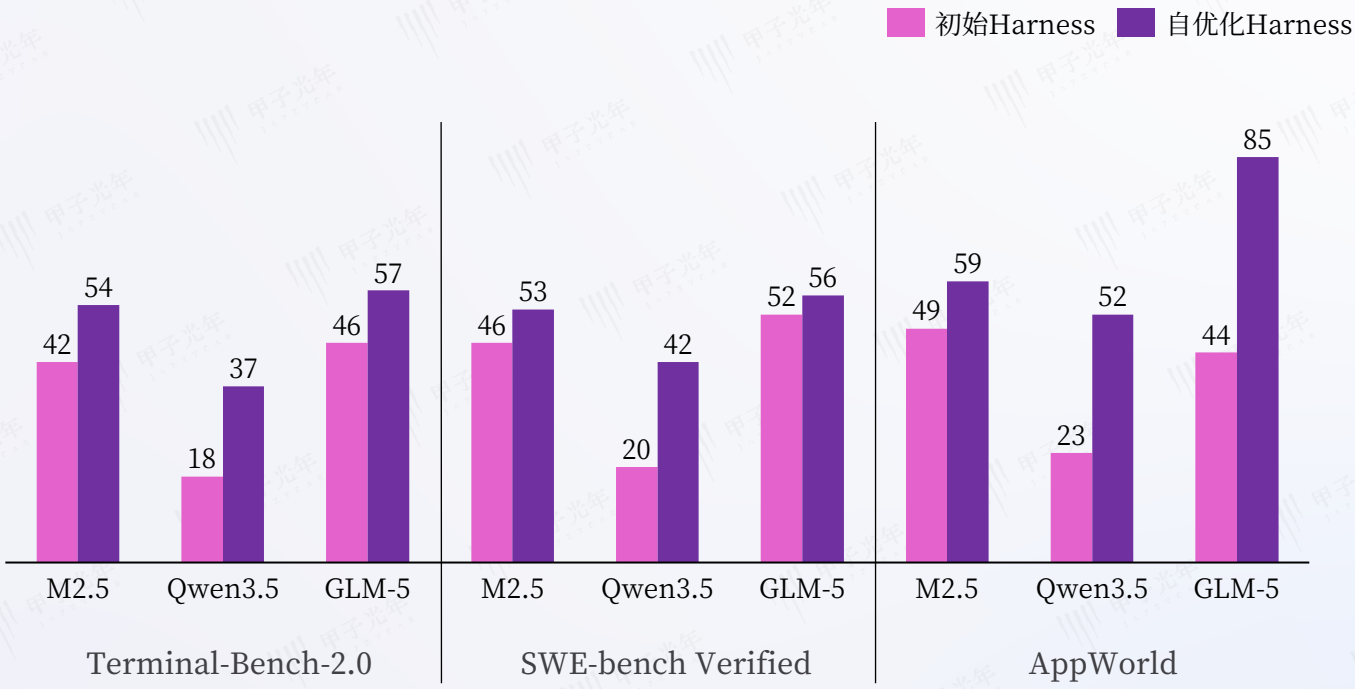
模型能力的提升并非智能体进步的唯一驱动力，许多智能体的任务失败并非模型推理本身的失败，而是Harness工程的失败。2026年3月，工程师Vivek Trivedy用“Agent = Model +

资料来源：Epoch AI《Will We Run out of Data? Limits of LLM Scaling Based on Human-Generated Data》，甲子光年智库整理，2026年

Harness”概括智能体的系统构成：模型提供智能，Harness工程负责将智能转化为可执行、可验证的任务能力。随着Harness从人工配置和调整，发展为模块完整、运行可观测、效果可评估的工程体系，智能体开始被用于Harness的自主修改与进化。传统Harness由人类专家构建，从早期ReAct框架到Claude Code、OpenHands等产品级系统均依赖人工调优；但不同模型具有不同的行为模式、工具使用习惯、错误类型和提示敏感度，为新模型设计专属Harness缺乏经济性。自优化Harness（Self-Harness）提出新范式：让智能体在不依赖人类工程师或更强外部智能体的前提下，自主改进运行Harness，构建“任务运行—弱点挖掘—Harness提案—验证评估—Harness更新”的自优化闭环。实验数据表明，在模型权重不变的情况下，Harness通过持续迭代实现自我优化，在终端操作、软件工程修复与多应用工作流等任务中实现性能提升，验证了Harness自优化的有效性。

Harness能力的深化使智能体调用链路持续延长和复杂化。随着工具调用、任务编排与结果验证等能力融入Harness，单次任务调用环节增加，模型、数据与外部服务交互更加频繁；自优化Harness进一步引入运行反馈、问题识别、方案验证与更新，使任务执行从一次性调用延伸为持续迭代闭环。两类机制叠加，使调用深度与交互轮次增加，端到端时延更易累积，任一环节异常都可能影响任务完成，由此对网络低时延、高可靠能力提出更高要求。

图7：模型权重不变，Harness通过自主迭代能持续提升性能



注释：Terminal-Bench 2.0、SWE-bench Verified、AppWorld分别评估终端操作、软件工程修复与多应用工作流能力；实验保持基座模型、工具、题库与评估环境不变，仅迭代Harness。

资料来源：上海人工智能实验室《Self-Harness: Harnesses That Improve Themselves》，甲子光年智库，2026年

2.2.3 环境能力：数字孪生正从映射工具演进为智能体训练、仿真与运行的环境底座

数字孪生正从镜像物理世界走向优化和驱动物理世界。早期应用以三维可视化、状态映射和运行监测为主，重点解决物理世界“看得见、看得清”的问题；随着生成式AI、世界模型和智能体技术的融入，数字孪生开始具备自动建模、预测推演和协同决策能力，并通过机器人、控制系统等执行载体作用于物理世界。

从智能体应用视角看，数字孪生的能力可归纳为训练态和运行态。训练态面向模型与策略形成，提供仿真环境、数据生成、策略训练和方案验证能力；运行态面向业务闭环，提供实时映射、状态预测、风险模拟和决策执行支持。

训练态的核心是以低成本、低风险的方式复现物理环境及其运行规律，为智能体提供可规模扩展的训练与验证条件。一方面，数字孪生可利用真实数据构建高保真仿真环境，并生成现实中难以充分采集的长尾、极端和故障场景数据，扩充智能体训练样本；另一方面，智能体可在仿真环境中反复试错，完成策略学习、参数优化和多方案对比，并在部署前验证策略的有效性与安全性。

运行态的核心是保持数字孪生与物理系统的持续同步，并基于实时状态支持运行控制与业务决策。系统通过传感器、业务平台和网络持续采集物理对象的状态数据，更新孪生模型并识别运行偏差；在此基础上，结合机理模型、世界模型和智能体开展趋势预测、风险模拟与方案推演。决策结果可通过控制系统下发至机器人、设备或网络等执行对象，执行结果再反馈至数字孪生，用于修正模型和优化后续决策。在城市领域，IDC预测，到2028年中国所有大型城市将采用人工智能自动化数字孪生技术，用于模拟政策效果、优化资源配置、凝聚社区共识和应对危机场景。

从网络要求看，训练态需支撑多源异构数据汇聚、跨域流通及云边端算力协同，重点保障大带宽、弹性调度与数据安全；运行态需按业务控制周期提供低时延、低抖动、高可靠和时间同步保障。同时，多智能体协同还要求高并发通信、跨域身份互认与资源动态编排。这意味着，网络需从连接资源的传输管道，升级为统筹数据、算力与智能体协同的智能基础设施，支撑数字孪生与物理系统之间的实时交互和闭环控制。

2.2.4 现实交互能力：从连接物理实体到形成群体智能

与环境能力侧重构建智能体训练、仿真和运行的数字环境不同，现实交互能力强调智能体进入物理世界后的感知、行动与协作。在这一过程中，数字孪生映射现实状态，世界模型理解并推演环境变化，智能体基于二者作出决策并作用于现实。随着物理AI的发展，智能体与物理世界的交互呈现两方面变化：一是连接对象和覆盖范围不断扩展，形成物理实体的泛在规模连接；二是物理智能体由独立运行走向群体协同，形成超越单体能力的群体智能。

泛在规模连接拓展了智能体感知现实、调用资

资料来源：英伟达，IDC，甲子光年智库，2026年

源和作用环境的边界，既包括智能体对传感器、工业设备等物理资源的接入，也包括机器人、车辆、无人机等物理智能体之间的互联。前一类连接使智能体能够跨设备、跨区域、跨场景获取图像、位置、环境参数和设备状态等实时数据，并将决策转化为设备控制与实体行动；后一类连接使物理智能体能够交换状态、任务意图和执行反馈，为进一步形成群体智能提供通信基础。

在泛在连接的基础上，物理智能体还需要围绕共同任务进行动态组队、角色分工、任务协商和行动协调，才能由相互连接进一步走向群体智能。这依赖两方面能力：一方面是任务协作，即多个智能体根据各自能力动态组队、分配角色，通过状态共享与行动协调形成协作闭环，完成单体难以独立完成的复杂任务。另一方面是运行适配，即随成员移动、加入或退出以及环境与任务持续变化，动态调整协作关系与任务分工，确保控制权限明确、协作过程可信、关键行为可追溯。

泛在规模连接与群体智能协作共同推动网络能力升级。物理智能体与传感器、设备及其他智能体之间的泛在连接，产生海量的实时数据流，图像、位置、环境参数、设备状态、任务意图和执行反馈持续高频传输，对超大规模连接、大带宽与高吞吐提出刚性需求。同时，群体智能的协作闭环依赖智能体之间的状态同步、任务协商与行动协调，对时延抖动和传输可靠性极为敏感，且要求网络通过统一身份标识识别智能体，依托意图路由按任务类型动态匹配通信、计算与执行资源。由此，网络需要从面向终端和设备连接的基础设施，升级为支撑智能体泛在连接、可信交互、动态组网与群体协作的新型基础设施。

资料来源：北京航空航天大学人工智能研究院&国防科技大学计算机学院《群体智能及产业集群发展战略研究》，水清木华《群体智能与机器人协同研究》，甲子光年智库，2026年

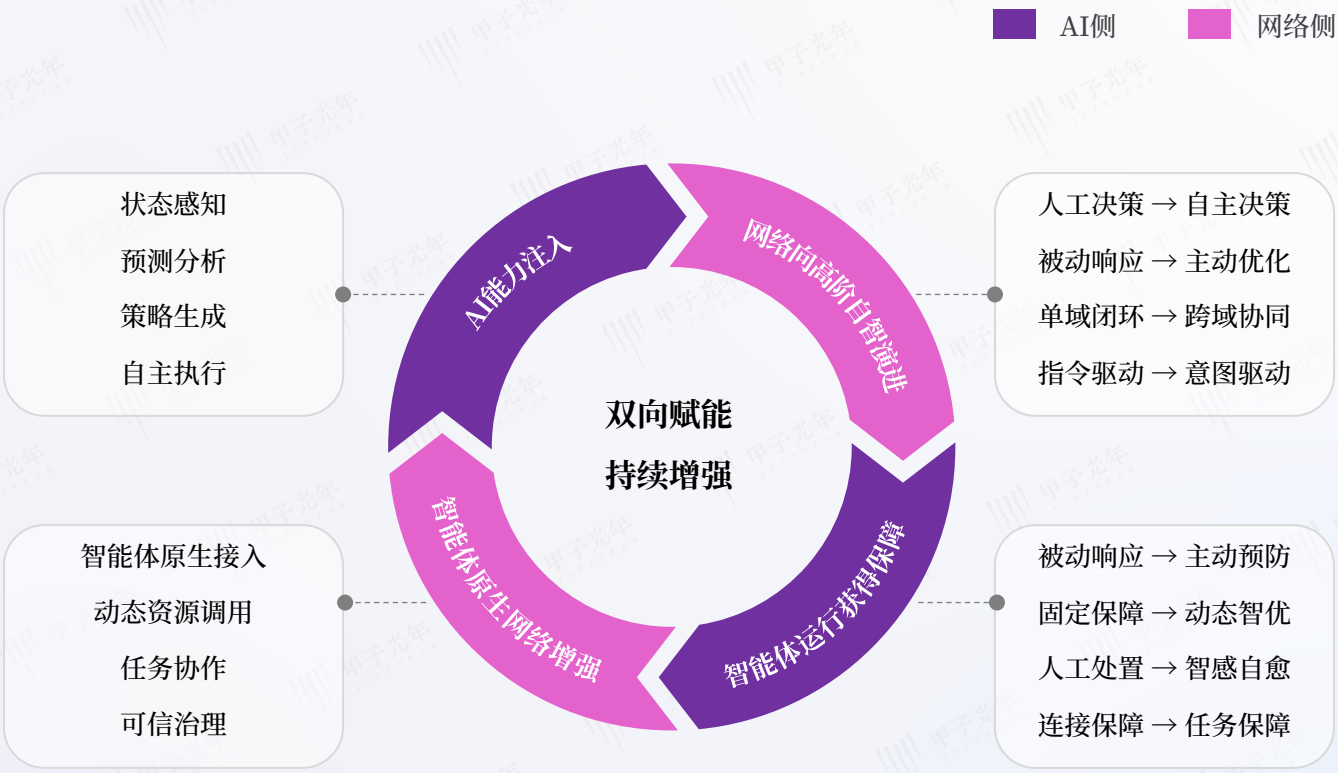
2.3 AI与网络的双向赋能：从“AI+Network”到“Network ×AI”

2.3.1 AI与网络互塑共生：从“AI+Network”到“Network ×AI”

AI与网络正在形成相互塑造、双向赋能的演进关系。从AI侧看，AI将感知、分析、决策与执行能力注入网络，推动网络自智水平提升；同时，智能体对网络提出了新的连接、调度与保障需求，推动网络围绕智能体进行原生化设计。从网络侧看，高阶自智能力通过网络自主管理、故障处置与持续优化，为AI应用提供稳定、高效的运行环境，而智能体原生网络通过泛在连接与能力发现，支持智能体跨设备、跨平台调用模型、工具和数据，开展群体协作，拓展智能体及其他AI技术的应用范围，释放智能体的任务执行潜能。

这种双向赋能形成了演进飞轮：AI能力注入提升了网络运维效率，推动网络向高阶自智演进；网络自智水平提升为智能体运行提供更优保障；智能体稳定运行则可拓展应用范围，促进智能体原生网络设计与强化；智能体原生网络增强则进一步释放AI新能力，提升网络自智水平，开启下一轮循环。四环交替、持续增强，推动AI与网络从“AI+Network”的能力叠加，走向“Network×AI”的深度融合与内生重构。

图8：AI与网络构成双向赋能的演进飞轮



资料来源：甲子光年智库整理，2026年

2.3.2 以智赋网：AI推动网络自智升级与智能体原生重构

一方面，AI正在逐步进入网络感知、分析、决策与执行过程，推动网络自身的自智水平升级。网络遥测、边缘智能和数字孪生支撑状态感知，大模型理解业务意图、分析故障并预测趋势，结合网络状态与资源约束形成调整策略，网络智能体则调用控制器和专业工具完成配置下发与结果反馈。在AI技术的加持下，人工参与逐步减少，网络对感知、分析、决策与执行全过程的自主闭环能力持续提升，自智范围由单点任务和局部试点向大范围跨域协同拓展，运营方式由被动执行向预测式、主动式自主运营演进。

另一方面，智能体应用的发展对网络提出新的需求，牵引网络面向智能体进行原生重构。针对智能体这一新型网络对象，网络需在接入层基于身份与能力实现注册认证、动态发现和语义寻址；在调度层依据任务需求协同编排计算、存储与网络资源；在传输层针对智能体调用链路延长和模型调用频次增加，强化面向Token流的保障能力；在治理层将管控范围延伸至智能体的身份、权限与行为。接入、调度、传输与治理等核心机制围绕智能体任务重新组织，形成面向智能体原生设计的服务体系。

2.3.3 以网强智：网络强化智能体运行保障并拓展智能体能力边界

自智网络通过动态自主运营，为以智能体为代表的AI应用提供更稳定、高效的运行保障。通过业务识别、体验感知和状态预测，网络能够提前发现拥塞、性能劣化与故障风险，动态调整网络配置和资源，在异常发生时完成快速定位与闭环恢复。相比传统网络主要围绕连接状态和故障进行被动响应，自智网络将保障前移至任务运行全过程，使智能体获得更敏捷的业务开通、更稳定的连接质量和更连续的任务运行环境，为动态调用和复杂任务执行提供支撑。

智能体原生网络通过泛在连接、动态资源调用、任务协作与可信治理，进一步扩大智能体能力边界。原生接入使大规模智能体基于身份、能力和任务意图被识别、发现与连接，扩大协作范围，提升任务处理效率，承接更复杂任务；动态资源调用使智能体依据任务灵活匹配计算、存储与网络资源，增强复杂任务的资源组织能力；任务协作使多个功能各异的业务智能体能够衔接执行步骤、共享中间结果，根据反馈调整后续流程，支持智能体自身与智能体群体协作能力持续演进；可信治理使智能体在明确权限和安全边界下自主调用资源、调整任务，提升运行安全等级。

资料来源：甲子光年智库整理，2026年

2.4 企业智能体互联与任务运行：新型网络基础设施亟需构建

企业智能体作为新型数字劳动力，正在由试点验证进入核心业务流程，但现有IT系统适配不足、面向智能体的网络评估体系缺位、多智能体协同保障薄弱等问题表明，现有基础设施尚难支撑智能体规模化应用。这些挑战源于智能体类型日益多样、能力结构持续复杂化，以及AI与网络关系的动态演进。

企业智能化落地的核心问题正在从智能体的开发部署，转向对大规模智能体的体系化管理。这要求网络超越传统的设备连接与流量承载，围绕智能体的身份、能力、任务、资源与行为，提供贯穿接入、运行、协作、演进和退出全生命周期的支撑。为此，网络需要完成四方面升级：

一是从连接设备和应用升级为智能体的规模化接入与识别。随着智能体数量增长、类型分化及分散化部署，网络需要支持海量智能体的泛在接入与动态连接，且连接对象也由设备和应用扩展为智能体，网络还要准确识别智能体的身份、能力和任务意图，使其能够被可信接入、准确发现和按需调用，支撑大规模智能体之间的任务交互与动态协作。

二是从保障应用运行升级为保障智能体任务运行与智能体的全生命周期。网络与AI不断融合向自智网络发展，既要围绕智能体任务的发起、分解、调度、执行与反馈，为模型调用、工具使用和多智能体协作提供连续、可靠的运行保障；也要覆盖智能体从开发测试、注册接入、部署运行、更新演进到退出注销的全生命周期，确保各阶段的身份可信、权限可控、状态可见和行为可追溯。

三是从网络承载设施升级为算网协同的智能体运行基础设施。智能体任务往往需要跨云、边、端调用算力，并在模型、数据与工具之间频繁交互。网络需要根据任务意图、时延要求、算力需求和资源状态，协同选择计算节点、传输路径与服务资源，实现任务随算力动态调度、连接随任务按需建立，为智能体的持续运行、弹性扩展和跨域迁移提供统一支撑。

四是从数字空间连接升级为具备实时映射与泛在物物交互能力的虚实融合网络。网络既要保障数字孪生与物理系统之间的状态数据、推演结果和控制指令实时传递，维持虚实状态同步，支撑智能体基于真实世界开展决策推演，也要广泛连接人、智能体与各类物理实体，并通过状态共享、任务协商和行动协调，支撑人机协同与机机协同，使智能体能够可靠感知并作用于物理世界。

因此，智能体时代需要构建企业智能体原生网络，即以智能体为第一服务对象，面向智能体规模化接入、任务运行和群体协作，具备智能连接、算网协同、自主调度、安全治理与全生命周期管理能力的新型网络基础设施。

资料来源：甲子光年智库整理，2026年

Part 03

新定义

企业智能体原生网络（EANN）

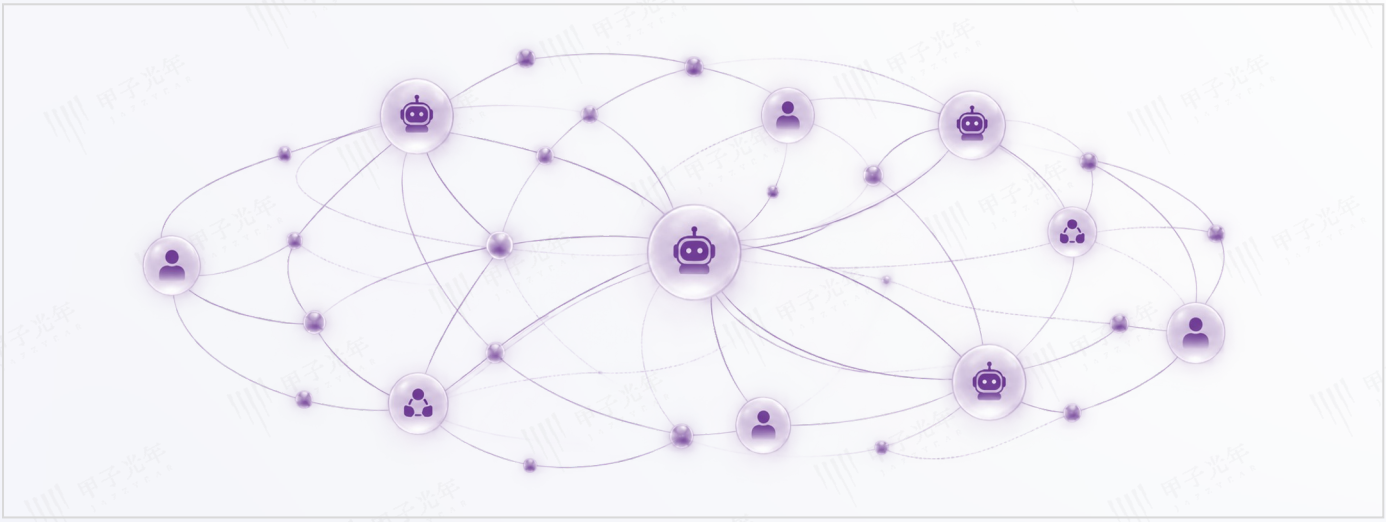
3.1 企业智能体原生网络（EANN）

3.1.1 定义：以智能体为核心对象，原生支持智能体接入、互联、协同与运行

企业智能体原生网络是以智能体为第一服务对象，以智能体身份、能力和任务意图为连接与调度依据，协同组织算力及相关服务资源，为智能体的规模化接入、跨域互联、任务执行、群体协作、安全治理与全生命周期管理提供支持的新型网络基础设施。

智能体原生包含两重内涵：一是智能体是网络内生的组成部分，而非外挂应用，智能体作为一等公民存在于网络架构中，可被网络直接识别与服务。二是网络架构设计的理念围绕智能体进行，网络接入、调度、传输与治理等核心运行机制以智能体需求为核心重新组织。智能体既在网络之中，网络也为智能体而设计。

图9：企业智能体原生网络概念图



3.1.2 技术基础与设计思路：传统网络技术奠基、智能体技术注智、智能体特征牵引创新

传统网络为智能体提供连接与传输基础。由接入、寻址、交换路由和传输协议构成的通信体系，使分布于云、边、端的智能体、模型、数据和工具能够稳定互联，网络控制、资源调度和服务质量保障则进一步支撑数据可靠传输和业务连续运行。但传统网络依据设备地址、应用类型和流量特征提供服务，能识别“数据包要去哪”，却无法让智能体识别“我需要的智能体是谁、能做什么”。同时，传统网络也缺乏直接识别和管理智能体身份的机制，难以支持智能体注册、彼此发现与按需连接。

为进行网络的智能体原生改造，需要引入智能体技术为网络增加语义理解与执行能力。一方

资料来源：甲子光年智库整理，2026年

面借助大模型的语义理解能力，帮助网络理解任务需要的资源与策略；另一方面能够借助Harness能力，帮助网络把策略转化为行动，调用控制器、算力与工具，完成配置下发、路径调整与故障处置。

此外，让智能体特征牵引网络技术创新。智能体具有自主身份、能力差异、任务驱动和动态协作等特征，为适配这些特征，网络需要发展原生接入、意图寻址、动态组网、算网协同、生命周期管理等新机制。智能体原生的本质不是用AI优化既有网络，而是以智能体需求重新定义网络的服务对象、寻址依据和资源组织方式。

3.1.3 建设路径：从叠加赋能、混合协同走向原生重构

企业智能体原生网络并非一次性替代现有网络，而是在保障存量系统稳定运行的基础上，沿着叠加赋能、混合协同和原生重构的方向逐步演进。各阶段的区别主要在于智能体进入网络的深度，以及面向智能体的网络能力向底层基础设施下沉的程度。

初期以智能体对运维赋能和传统网络承载业务为主。运维方面， 智能体率先进入网络状态监测、故障诊断、配置优化和资源优化等相对成熟的运维场景，通过现有接口与网管、运营系统连接；上层业务方面，各类智能体依赖现有网络，网络尚不具备面向智能体直连接入、调度与保障能力。这一阶段不改动底层设备和核心协议，重点是提升网络自身的智能运维能力，并验证智能体对网络的基础需求。

中期进入混合协同阶段，智能体赋能网络的范围由运维向控制与调度拓展，同时网络开展局部改造，逐步面向业务智能体提供连接与运行支撑。具体而言，智能体开始参与部分网络控制与资源调度，网络则通过网关、控制器、编排平台及智能化网元，与上层业务智能体形成信息交互与协同决策机制。业务智能体对连接、算力与安全的需求逐步转化为网络可执行的策略，推动智能体能力与网络能力由上层叠加走向深层协同。但这一阶段的改造仍集中于特定网络域和关键节点，存量网络将与新增能力长期并存。

远期走向智能体原生重构，网络服务范围拓展至智能体的全生命周期。随着技术、标准和产业条件成熟，智能体身份、能力与任务意图成为网络可直接识别和处理的对象，相关机制逐步向网络控制面、协议体系和基础设施节点下沉。网络从智能体接入开始，持续支撑其部署、运行、协同、演进直至退役，并围绕不同阶段动态组织连接、资源与安全策略，形成贯穿智能体全生命周期的原生网络服务体系。

资料来源：甲子光年智库整理，2026年

3.2 企业智能体原生网络（EANN）的核心特征

3.2.1 顶层设计原则：让智能体从网络承载对象走向原生主体

智能体原生网络首先体现为网络顶层设计原则的变化，“原生”表现为智能体定位的内生化，智能体被当作一等公民纳入网络架构的初始设计，从定位、理念、目标与对象四个维度重新定义网络。

从智能体定位看，智能体由网络之上的应用转变为网络中的原生主体。传统网络并不天然感知智能体的身份、能力与任务需求，在智能体原生网络中，智能体成为网络可识别、可连接、可保障和可治理的新型数字主体，其身份及相关属性能够被网络感知，并成为提供连接与运行保障的重要依据。

从设计理念看，网络由面向通用通信需求设计转向从架构初始围绕智能体设计。也就是说，智能体的自主运行、动态协作与持续演进需求纳入原始网络设计，而非后续叠加的外部设计需求。

从设计目标看，网络由实现连接与数据传输走向保障智能体互联与任务执行。智能体任务往往涉及多个主体以及模型、工具和服务的连续交互，网络需要进一步延伸至任务运行过程，为智能体持续交互与协同执行提供支撑。

从连接对象看，网络由连接设备与应用进一步扩展至连接智能体。传统网络只认IP地址和端口，服务对象是设备和应用；智能体原生网络则将Agent ID纳入原生识别体系，能感知其身份、能力与任务状态。

3.2.2 网络底座能力：从通用通信底座走向面向智能体的感知、连接与资源协同底座

相较于传统网络，智能体原生网络的基础设施变化，主要体现在网关功能、网元能力与算电网存资源配合方式的升级。

从网元能力看，网络设备由以转发和规则执行为主，向具备本地感知、分析与执行能力演进。传统网元主要按照既定配置处理流量，复杂分析与控制更多依靠外部管理系统；智能体原生网络则根据设备资源条件，在网络内部融入智能体能力，使网元能够结合网络运行状态与任务要求，开展异常分析、资源调整和故障处置。网元在授权范围内执行操作，并向上层系统反馈结果，成为能够参与网络任务的智能单元。

从网关能力看，网关由设备接入与流量转发，扩展至智能体接入与交互支持。传统网关主要承担设备接入、协议转换和流量转发等功能；智能体网关在此基础上，增加智能体身份认证、能力登记与协议适配能力，使接入对象的身份、服务能力和访问条件能够被网络识别。

从算电网存协同看，资源组织方式由相对独立

资料来源：甲子光年智库整理，2026年

配置走向按任务需求动态联合调度。传统架构中，算力、电力、网络与存储资源相对独立规划，跨系统协同不足；智能体任务则需要综合考虑推理计算、能源供给、数据访问与通信传输条件，按任务需求动态匹配和调度资源，提升Token运行效率与能源利用效率。

3.2.3 网络运行机制：从被动承载流量走向主动支撑任务

传统网络以人机交互为核心，围绕设备连接、流量承载和边界安全构建运行体系。当智能体成为网络主体，其自主身份、任务驱动、动态协作和持续演进等特征，从通信对象、寻址方式、连接方式、流量特征、网络运维方式和安全治理方式六个维度，系统性影响了传统网络的设计基础，推动网络从面向通用通信的被动管道，走向面向智能体全生命周期主动组织连接、资源与治理的新型基础设施。

一是对象确定方式由预设通信对象走向基于任务需求动态发现智能体。传统网络通常依赖预设地址或服务信息确定通信对象，而智能体任务的协作对象并不一定预先确定，需要结合任务需求，从多个候选智能体中动态发现和匹配适合的智能体。

二是寻址方式由基于IP地址的位置寻址走向意图驱动的语义寻址。传统网络通过DNS解析域名获取IP地址，再按IP路由定位设备位置。在智能体协作中，任务发起方关注的是智能体能做什么，而非部署在哪个节点，需要根据身份、能力与任务意图语义匹配可用智能体，再动态建立连接路径。

三是连接方式由端点间的确定连接走向围绕任务的动态连接。传统网络中，通信双方通过预设地址建立端到端连接，连接关系在配置阶段即确定，传输过程中基本不变；而智能体的协作关系随任务实时组建与解除，连接对象、路径和资源都可能随时变化，并在任务结束后自动释放。

四是流量特征由通用业务流量走向Token驱动型流量。传统网络承载的主要是人机交互产生的网页请求、文件传输和视频流，流量模式以南北向为主、峰均比相对可控；而智能体产生的是持续高频的Token流，Token流转化为高频多轮的任务流量，峰均比达到传统人机流量的10倍，小包占比超80%，东西向流量占比高。

五是网络运维方式由人工配置与规则自动化走向智能体自主运维。传统网络运维依赖人工编写配置脚本和预设告警规则，面对故障靠经验判断、手动处置，规则覆盖范围有限且难以应对未知场景；而智能体结合网络知识库与运行数据，能够主动感知异常、分析根因、生成修复方案并自动执行。

六是安全治理方式由面向用户、设备与连接的安全防护走向智能体全过程可信治理。传统网络安全以人和设备为保护对象，通过防火墙、ACL等手段实现认证与拦截，防护范围相对固定、策略偏静态；而智能体具备自主行动能力，其身份、数据和行为必须受到全流程保护，需要将安全嵌入运行时，围绕智能体身份可信、行为合规和数据保密实施全链路动态治理。

资料来源：甲子光年智库整理，2026年

图10：传统网络与企业智能体原生网络对比

对比层级	关键维度	传统网络	企业智能体原生网络
顶层设计原则	智能体定位	网络之上的外挂应用	网络中的原生主体
	设计理念	面向通用通信需求设计	从架构初始就围绕智能体设计
	设计目标	实现连接与数据传输	实现智能体互联与智能体任务稳步执行
	连接对象	设备与应用	智能体
网络底座能力	网元能力	通用转发，由网管系统集中管控，无本地自治功能	内置智能体，支持本地感知、决策与执行，参与网络任务
	网关能力	以设备接入、协议转换和流量转发为主	支持智能体接入认证、能力登记与协议适配
	算电网存协同	各类资源相对独立配置	算电网存一体化，按任务需求动态联合调度
网络运行机制	对象确定方式	依赖预设地址或服务信息定位通信对象	基于任务需求，动态发现智能体（含身份、能力等）
	寻址方式	基于IP地址的网络位置寻址	意图驱动的语义寻址
	连接方式	以端点间的确定连接为主	围绕任务动态建立连接，支持多智能体协同
	流量特征	通用业务流量	Token驱动型流量
	网络运维方式	依赖人工配置、规则策略与自动化工具	由智能体感知网络状态，自主决策并执行配置
	安全治理方式	面向用户、设备与连接实施认证、授权与安全防护	面向智能体身份、行为与任务全过程实施动态可信治理

资料来源：甲子光年智库整理，2026年

3.3 自智网络（AN）与企业智能体原生网络（EANN）的关系

3.3.1 概念辨析：自智网络聚焦自治运行，原生网络聚焦智能体原生服务

自智网络与企业智能体原生网络是当前网络智能化演进中两个密切关联但侧重有所差异的概念。二者既非完全等同，也非相互替代。

自智网络聚焦于网络自身的自治能力的提升。基于TM Forum定义的L0-L5自智水平，其核心能力体现为自配置、自修复、自优化和自演进，目标在于降低从资源管理、网络运维到服务保障等过程中的人工干预，提升网络自主运行效率，并提供网络服务保障。

企业智能体原生网络则聚焦于网络对智能体的原生服务能力。其核心能力体现为智能体可识别、可发现、可连接和任务可保障，根本目标在于实现智能体间互联，提升任务执行效率。当前该概念尚处于框架制定阶段，暂无统一标准。

尽管两者服务的对象与目标不同，但均具备四项技术特征。意图驱动，即以业务或任务意图驱动网络策略生成与执行；AI赋能，即大模型与智能体等技术增强网络的理解与自主运行能力；自主闭环，即形成感知、决策、执行与反馈的端到端自动化闭环；动态资源调度，即根据任务需求与实时状态动态调配算网及其他相关资源。

图11：自智网络与企业智能体原生网络的异同



资料来源：TM Forum，甲子光年智库整理，2026年

3.3.2 演进关系：自智网络与企业智能体原生网络并行发展，推动网络整体迈向高原生高自智方向

自智网络与智能体原生网络并非线性递进关系，而是沿不同维度并行演进、逐步交汇。以自智水平（L0至L5）和智能体原生程度（低至高）构建二维框架，可以形成四种典型网络形态，反映网络自治与智能体原生能力的不同组合及演进方向。

低原生低自智对应传统网络形态。网络主要面向设备与应用提供连接和数据传输，自智水平处于L0-L3，网络运行较多依赖人工配置、预设规则与自动化工具。对于智能体，网络仍主要提供基础连接与数据传输，只负责连接已经确定的通信对象，尚不能识别智能体身份与能力，也不能依据任务需求动态发现和连接适合的智能体。

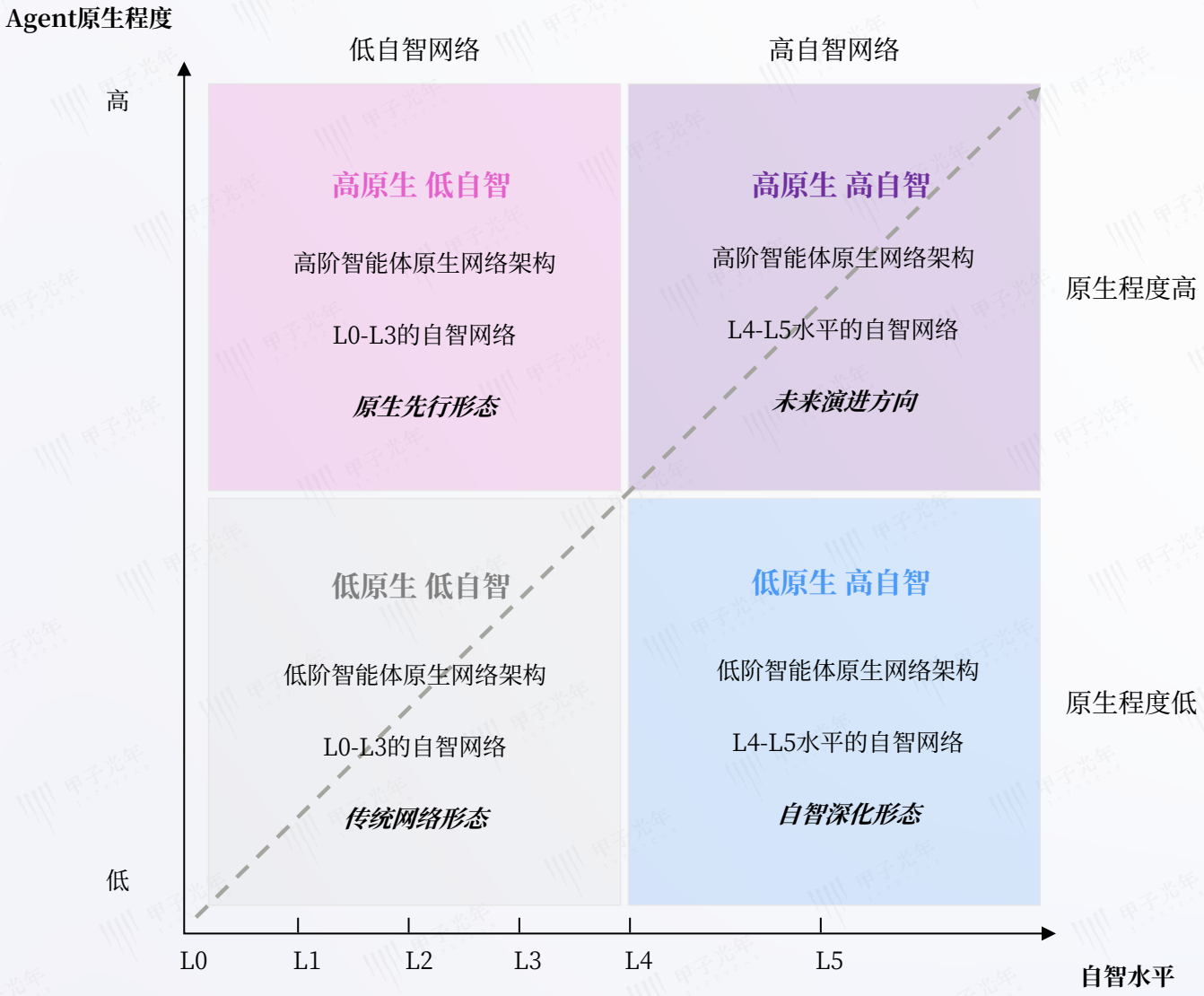
低原生高自智对应自智深化形态。 网络自身自治能力率先提升，自智水平达到L4-L5，能够基于网络状态进行自主感知、分析决策与闭环执行，减少网络运行过程中的人工干预。但是，网络能力主要服务于运维效率提升，尚未围绕Agent建立原生服务机制，智能体原生程度仍然较低。

高原生低自智对应原生先行形态。网络率先引入智能体原生架构，面向智能体的原生服务能力率先提升，但自智水平停留在L0-L3，底层资源调度和故障处理较多依赖人工干预与既定策略。

高原生高自智对应未来演进方向。随着智能体原生网络架构成熟与网络自智水平提升，智能体原生网络与自智网络在状态感知、资源调度和运行保障等方面加强衔接。前者支持业务智能体的识别、发现、连接与任务执行，后者通过自主配置、故障恢复和动态优化，为前者提供运行保障。两者围绕业务任务需求与网络运行状态形成双向反馈，在各自建设的基础上深化能力融合，共同提升智能体任务效率，并推动网络整体迈向高原生高自智方向。

资料来源：甲子光年智库整理，2026年

图12：自智网络与企业智能体原生网络的演进关系



注释：自智水平与Agent原生程度沿不同路径演进，虚线箭头表示两类能力协同增强的长期方向。

资料来源：甲子光年智库整理，2026年

NIDA 全球固定网络创新联盟 | 甲子光年 JAZZYEAR

Part 04

新范式

企业智能体原生网络架构



4.1 企业智能体原生网络架构

4.1.1 智能体原生网络五层双域架构：五层逐级承载，双域全栈保障

企业智能体原生网络采用“五层双域”的总体架构，以智能基础设施层、智能体网络连接层、智能体网络管控层、智能体互联交互层和智能体业务应用层构成自下而上、逐层支撑的五层能力体系，以安全保障域和运营监测域贯穿各层，形成覆盖设施承载与状态感知、原生连接与通信、原生管控、原生交互与协作、原生任务执行的一体化支撑体系。

在五层能力与双域保障的作用下，企业智能体原生网络能够结合全域的实时运营监测状态，形成贯穿感知、分析、决策、执行的工作机制闭环，并融入全栈安全治理。

- **多维感知：将感知对象由网络与资源状态拓展至智能体及其任务需求，形成综合信息输入，对应L1、L2、L5和D2。**一是网络与资源状态感知，对应L1+D2。通过智能网元获取网络拓扑、链路及基础设施状态，依托运营监测能力持续采集流量、性能、算力资源、服务及任务运行状态，并通过网络数字孪生对物理网络及资源状态进行动态映射，为后续分析决策与资源调度提供环境信息。二是智能体相互感知，对应L2+D2。网络通过智能体注册、身份标识、能力描述和状态更新等机制，获取智能体的身份、能力、位置与接入状态等信息，使智能体成为网络可识别、可管理的原生主体，并为智能体之间的相互发现、能力匹配与按需连接提供基础。三是任务感知，对应L5+L1+D2。网络获取L5业务智能体发起的任务意图与服务需求，以及对连接、算力、安全等方面的要求，并依托L1通信大模型的语义理解与意图识别能力，使任务目标、资源需求与保障诉求转化为网络可识别、可处理的需求信息；同时结合D2对任务运行状态的持续监测，为后续任务分析与策略生成提供输入。

- **分析与决策：L3作为承接任务需求与驱动网络执行的核心管控中枢，依托L1提供的网络数字孪生环境映射与通信大模型智能能力，以D2为实时数据支撑，完成从任务需求到网络策略的分析与决策。**其中，L1环节，网络数字孪生通过对网络拓扑、设备、链路、流量、性能和资源等进行数字化映射，形成与物理网络动态同步的虚拟环境，支撑状态呈现、仿真推演和策略验证；通信大模型结合通信领域知识、网络运行、智能体和任务信息，进行理解、推理与策略生成，支撑意图理解、任务分析、异常研判和策略生成；Harness框架通过上下文管理、任务规划、工具调用与执行反馈等机制，将模型智能转化为智能体自主运行能力。以三项技术为基础，D2持续汇聚网络、资源、任务及SLA等运行数据，并将实时状态与执行反馈输入L3，使分析决策能够根据任务进程和网络环境动态调整。L3综合前序感知形成的智

资料来源：甲子光年智库整理，2026年

能体信息、任务需求以及算网等资源状态，对任务执行条件和协作需求进行分析，并通过任务分解、资源调度与动态编排形成整体执行方案，进一步转化为协作关系、连接策略、资源与保障配置，驱动后续智能体协同与任务执行。

- **多维执行：在分析决策形成任务执行方案后，各层协同将策略转化为实际行动，对应L1、L2、L4、L5和D2。一是基础设施执行，对应L1+D2。**智能网元、智算节点和存储节点等基础设施承接上层下发的执行策略，分别完成网络转发与配置、算力分配与弹性调度、存储配置与数据缓存等具体操作，并通过运营监测能力持续反馈设备、链路、算力及存储资源状态，使资源策略能够落实到底层基础设施。**二是网络连接执行，对应L2+D2。**网络根据任务执行方案，通过注册发现、协议适配、动态组网与消息路由等能力，将协作需求转化为智能体之间的逻辑通信关系，并结合连接、流量、性能与SLA等运行状态持续优化连接与路由，使任务所需的协作主体保持稳定、可靠的网络可达。**三是智能体任务执行，对应L4+L5+D2。**L4通过智能体互联、智能体与工具互联、智能体与模型互联等能力，支撑智能体根据任务需要开展动态协作，按需调用其他智能体、工具与模型，将任务执行方案转化为具体的交互与协同行为；L5业务智能体进一步面向数字、物理、科学和社会等不同业务场景完成具体任务执行。执行过程中，D2持续监测智能体交互、任务进度、服务质量与执行结果，并对任务运行过程进行记录与追溯，将执行状态与结果反馈至分析决策环节，为任务策略动态调整和后续优化提供依据。

- **全栈安全治理：D1安全保障域贯穿智能体感知、分析决策与多维执行全过程，围绕智能体、基础设施、通信交互及模型工具等关键对象构建覆盖全栈的安全保障体系。**一是面向智能体实施身份与权限安全，通过身份认证、可信标识、动态授权与权限控制等机制，保障智能体身份可信、访问合规，防止未经授权的智能体及能力接入网络。二是面向基础设施与通信过程实施设备、通信和数据安全，对智能网元、智算及存储设施进行安全防护，并保障智能体连接、消息传输和任务数据在交互过程中的机密性、完整性与可用性。三是面向智能体任务执行实施模型与工具安全，对模型、工具的接入、调用和使用过程进行安全控制，降低恶意调用、越权操作及不可信模型与工具带来的风险。四是通过安全审计对智能体身份、权限变化、交互调用与任务执行等关键活动进行记录和追溯，实现安全事件可发现、行为可追踪、责任可追溯，为智能体任务全过程提供持续可信保障。

资料来源：甲子光年智库整理，2026年

图13：企业智能体原生网络架构图



资料来源：甲子光年智库整理，2026年

4.1.2 全生命周期支持：企业智能体原生网络服务贯穿智能体从入网到退网的全过程

企业智能体原生网络将网络服务由单次连接与通信保障，延伸至智能体从入网到离网的全生命周期。智能体作为具有独立身份、能力与任务目标的网络主体，其网络关系伴随注册入网、能力发现、连接建立、任务运行、多主体协作、能力演进直至退出而持续变化。网络因此需要根据智能体所处阶段动态介入，实现对智能体持续在线与任务执行的系统支撑。

注册、发现与连接构成智能体进入网络并建立通信关系的基础阶段。为使智能体能够接入网络，首先需要完成身份创建与信息登记，使其成为网络可识别、可寻址的数字主体。在此基础上，网络依据智能体的能力描述与任务需求，提供能力发现与对象匹配服务，并通过协议适配、动态组网与消息路由等机制，建立端到端的通信关系。L2智能体网络连接层在这一过程中承担核心枢纽作用，推动智能体由接入走向可被发现、可被连接，为后续任务运行奠定基础。

运行与协作构成智能体依托网络开展任务执行与多主体交互的核心阶段。进入任务运行后，智能体根据任务意图与服务需求，在任务执行过程中持续与其他智能体、模型和工具开展交互协作。面向这一过程，L5智能体业务应用层承载任务需求产生与具体业务执行，L4智能体互联交互层提供智能体与智能体、模型及工具之间的交互能力；L3智能体网络管控层结合任务需求与实时网络状态，开展任务拆解、资源调度与动态编排，L2智能体网络连接层维持并按需调整通信关系，L1智能基础设施层持续提供网络、算力与存储等底层资源。五层能力围绕任务运行持续协同，使智能体的交互关系与资源配置能够随执行过程动态调整。

演进阶段，智能体通过能力进化与版本迭代不断拓展自身能力边界。随着模型、知识、工具及版本持续更新，智能体的能力描述与运行状态也会相应变化。L2智能体网络连接层需要及时刷新相关信息，使网络能够持续准确识别智能体的最新能力与状态，并支撑演进后的智能体被重新发现、连接和调用。

退出阶段，智能体结束在网生命周期，网络需要解除其连接关系并注销网络身份。当智能体完成任务、停止服务或因其他原因退出网络时，L2智能体网络连接层需要解除智能体之间，以及智能体与其他服务之间建立的连接关系，并注销身份标识、清除注册信息，实现智能体从网络系统中的彻底退出。

智能基础设施、安全保障与运营监测贯穿智能体全生命周期，为各阶段提供持续支撑。L1智能基础设施层持续供给网络、算力与存储等底层资源，满足智能体从注册入网到退出离网各阶段的资源需要；D1安全保障域围绕身份、权限、通信、数据、模型与工具等关键对象实施全程安全防护，确保智能体在网期间身份可信、交互安全、行为可控；D2运营监测域持续监测网络、资源、连接及任务运行状态，记录生命周期中的关键活动与状态变化，为运行分析、异常发现与过程追溯提供依据。

资料来源：甲子光年智库整理，2026年

图14：企业智能体原生网络为智能体提供全生命周期的能力支持



注释：全生命周期描述智能体从入网到注销退网的过程。

资料来源：甲子光年智库整理，2026年

4.2 企业智能体原生网络需要自智网络体系配套发展

4.2.1 网络自智需求：企业智能体原生网络运行复杂度提升，要求网络管理与保障能力升级

企业智能体原生网络服务对象与运行机制的变化，使网络自身的运行管理复杂度进一步提升，需要同步构建与之适配的高阶网络自智体系。

智能体规模接入与任务量增长，使网络运行与保障日趋复杂。业务开通、配置变更、故障处置等场景交织并行，SLA/SLO、成本控制、能源效率等方面的要求持续提高，对网络提出了易开通、早感知、准定位、快自愈的更高要求，倒逼网络自身增强感知、决策与执行能力。

智能体逐步成为网络运行主体，使既有管控方式难以延续。网络任务由网络智能体自主承接，为业务智能体运行提效增质，网络管理由此转向人工监督与多网络智能体自主执行，需要统一调度网络智能体的任务分工、信息交换与处置决策，做到管得住、联得通、决得准，形成对智能体原生网络的闭环管理能力。

智能体自主运行与跨域协作常态化，要求防护能力向全域可信与主动防御延伸。智能体规模化部署后，安全对象扩展至智能体身份、模型与工具调用、数据访问及跨域协作，模型幻觉、权限越界、异常执行等风险随之放大。网络自智体系需由边界防护、被动响应转向全域可信、主动防御，需要识得准、防得早、控得住，确保智能体运行全过程安全、可信、可控。

4.2.2 自智架构：构建面向企业智能体原生网络的自智网络（AN）

面向企业智能体原生网络，自智网络（Autonomous Network）以网络智能体为执行主体、以编排中心为统筹中枢，对企业智能体原生网络的运行实施自动化的动态管理与全程保障。该架构自下而上由智能体能力底座、网络智能体、编排中心与网络自治业务场景构成，且目标管理与安全治理贯穿各层。

智能体能力底座为网络自治提供统一的认知、推理与行动能力支撑。其中，通信大模型提供理解与分析能力，数字孪生通过网络状态同步与虚实映射，支持运行态势分析、策略仿真及效果预测，Harness工程为网络智能体提供工具调用与执行控制能力。

网络智能体按管理领域分工，实现垂域自治闭环。基础设施领域智能体负责计算资源、智能网元与存储资源管理；连接交互领域智能体负责注册发现、智能路由与协议适配管理；任务运行领域智能体负责业务智能体与企业智能体原生网络管控中心的运行管理，以及任务链路保障。各智能体在设定范围内实现感知、分析、决策与执行的自治闭环，支持异常自愈。

编排中心是自智网络的任务统筹与执行组织中枢，将网络管理目标转化为可执行任务。其中，意图理解、任务分解和策略路由明确任务要求

资料来源：甲子光年智库整理，2026年

并分派至相应领域智能体；流程编排与跨域协调安排执行顺序；结果汇总与效果评估验证目标达成并调整后续执行。

网络自治业务场景明确网络任务要求。围绕服务开通、配置变更、故障处置、质量保障、资源优化和节能减排等场景，提出具体任务与保障要求，牵引下层编排与自治执行。

目标管理与安全治理体系共同界定网络自治的运行目标与执行边界。前者围绕业务需求、服务等级、成本与能效、用户体验等设定目标并评估成效，后者依托身份权限、策略合规、操作审批与审计追溯等机制约束自主行为，并为风险处置与人工接管提供保障。

图15：面向企业智能体原生网络的自智网络架构



注释：本架构图区别于传统网络自治，重点面向智能体连接、交互与任务运行提供自治保障。

资料来源：甲子光年智库整理，2026年

4.3 企业智能体原生网络的典型应用场景

4.3.1 金融场景：智能体网关支撑跨银行资金流水核查

场景概述：资金流水核查是企业上市尽职调查中的重要环节。保荐机构需核查拟上市企业及其董监高、关键岗位人员等相关主体的银行资金流水，识别关联交易、异常资金往来及潜在的体外资金循环，核实是否存在虚构收入或其他利益安排，为判断企业信息披露的真实性与完整性提供依据。

面临问题：获取流水资料时，跨银行取数繁琐，不同机构协作与信任管理困难。企业上市资金流水核查涉及企业及相关人员的多银行账户，传统方式需线下获取流水、人工汇总核对。业务转向线上后，各机构接口与协议不一致，且身份、授权与数据安全要求存在差异，仍制约跨机构协作效率。

解决方案：以智能体网关连接保荐机构与银行智能体协作。在被核查人充分授权的前提下，保荐机构智能体发起流水核查请求，网关通过服务注册与发现、任务转接与协议适配，协同相关银行智能体获取流水，并以身份认证、权限控制和业务留痕，支撑全过程安全管理。

预期效果：推动流水获取线上化、机构连接统一化、核查过程可追溯。减少线下奔波与人工流转，降低逐家银行对接和跨机构信任管理成本，为保荐机构开展关联交易及异常资金往来核查提供支撑。

图16：金融智能体网关支撑跨机构智能体协作



资料来源：甲子光年智库整理，2026年

4.3.2 制造场景：主Agent统筹各类专业Agent协作，贯通生产任务执行

场景概述：制造企业接收客户订单后，需要围绕产品需求、生产计划与交付要求，完成订单解析、需求分析、设备与产能确认及现场作业。智慧生产通过主Agent统筹生单、分析、设备及具身Agent，将各类专业能力组织起来，协同完成从订单接收到生产执行的任务。

面临问题：一方面，工厂虽已部署自动化设备和信息系统，但仍存在运行卡点，加之经验人员不足，需要统一规划任务、协调专业能力；另一方面，多Agent协作需要跨系统获取数据、调用模型，必须明确资源访问边界、按任务分配权限，并使访问行为可追溯。

解决方案：在生产协作层，由主Agent负责全局判断与任务规划，协调生单Agent解析订单、分析Agent评估可行性、设备Agent确认状态与产能，以及具身Agent执行现场作业。在互联支撑层，由Agent网关定义并执行资源访问策略，核验身份、动态授权、记录访问日志，并综合模型安全性、性能与成本进行模型路由，支撑各类Agent受控协作。

预期效果：通过主Agent统筹与各类Agent分工，减少人工协调，提升生产协作与任务响应效率；通过访问策略、动态授权及审计留痕，降低越权访问与数据泄露风险；通过模型路由匹配任务需求与模型能力，优化调用成本。

图17：智慧生产中的多Agent任务协作与互联



资料来源：甲子光年智库整理，2026年

4.3.3 教育场景：打通跨校Agent互联，促进优质教育能力共享复用

场景概述：随着教育大模型与Agent应用落地，教育资源正从课程、课件、视频等静态内容，扩展为具备答疑辅导、学习规划、科研辅助等能力的教育Agent。这些Agent分布在不同高校，需要通过跨校Agent互联，实现能力发现、按需调用与协同服务，支撑个性化学习、跨校教研及科研协作。

面临问题：高校教育Agent形成孤岛，制约优质教育能力跨校流通。一是平台、协议与接口标准不统一，互联互通门槛高；二是缺少统一的能力发现与检索机制，难以精准匹配、高效调用；三是缺少可信身份认证、交互与权限管控体系，难以支撑大规模、安全的跨校协作。

解决方案：引入企业智能体原生网络，提供四大核心能力：一是统一接入与注册，兼容异构平台及协议，统一能力描述，支撑跨校发现与匹配；二是动态路由，结合服务能力、负载与网络状态选择路径；三是可信协同，通过身份认证、动态授权与审计，保障跨校调用安全；四是任务级服务质量保障，按任务优先级与时延要求调配资源，提高任务成功率与响应速度。

预期效果：通过促进优质教育Agent跨校复用，减少重复建设，构建全域教育智能生态，支撑个性化学习与跨校教研，提升协作效率。

图18：企业智能体原生网络支撑跨校教育Agent能力共享与协作



资料来源：甲子光年智库整理，2026年

4.3.4 智慧家庭场景：从单设备控制走向多Agent生活服务

场景概述：智慧家庭从远程操作与预设自动化，向多个专业Agent协同服务演进。以晨间生活为例，个人助手理解用户意图，家庭管家拆解并调度任务，联动健康、餐饮、运动、教育及安防Agent，并由具身Agent执行早餐准备、物品取送等操作，完成从起床到出门的安排。

面临问题：家庭Agent来自不同厂商，协议与能力各异，协作涉及用户交互、Agent间通信及多方决策，对实时响应和状态同步要求较高。现有家庭网络主要面向联网接入，难以充分满足多Agent协作所需的能力发布、身份认证、权限管控及实时安全通信需求，同时需要保障家庭隐私及个人数据安全。

解决方案：在家庭边缘网关部署Agent网关能力，支撑异构协议适配、能力发布及身份权限管控，为家庭管家调度各类Agent提供互联基础；结合本地边缘算力与安全存储，支撑家庭数据处理和隐私保护，并提供实时通信保障。在授权范围内，连接外部天气、教育等服务Agent，扩展家庭服务能力。

预期效果：减少逐项操作，提升家庭服务协同效率和趣味体验，满足家庭成员多样需求，保障实时交互与家庭数据安全。

图19：智慧家庭晨间多Agent协作流程场景



预期价值：提升生活便利性与趣味性体验，保障家庭安全与隐私

资料来源：甲子光年智库整理，2026年

NIDA 全球固定网络创新联盟 | 甲子光年 JAZZYEAR

Part 05

新未来

凝聚产业力量共筑智能体互联生态



5.1 企业智能体原生网络关键技术建设

企业智能体原生网络的建设，需要同步推进两方面技术发展：一是面向业务智能体与网络智能体，完善连接、交互与任务运行所需的网络能力；二是面向企业智能体原生网络自身，发展网络智能体技术，提升网络的自治能力。两者分别回应智能体业务需求与网络管理需求，共同支撑企业智能体原生网络建设。

5.1.1 面向业务智能体与网络智能体的共性支撑技术：互操作协议、智能路由、质量工程

企业场景中的智能体区分为两类：参与企业业务流程与任务协作的为业务智能体，承担网络管理任务的为网络智能体。前者是原生网络的服务对象，后者是自智网络的关键执行主体。两者均涉及身份发现、语义交互与资源调用，需协同推进智能体互操作协议、智能路由与质量工程等共性技术建设。

- **互操作协议：应统筹各类协议建设，推动网络侧智能体身份注册、能力发现等协议与智能体侧ACP、A2A、MCP及ANP等协议实现互联互通。**在接入与发现方面，规范智能体身份与能力信息的登记、更新和查询，确保智能体身份标识的唯一性、不可伪造性与可追溯性，实现智能体与网关之间的双向身份认证，并支撑跨域协作对象的发现；在消息传输方面，完善点对点与群组通信机制，支持多样化数据负载的路由、转发与投递，以及群组成员动态管理和消息顺序保障，并通过通信加密与端网协同提升传输安全性和效率；在工具与资源访问方面，规范外部工具、数据及服务的调用接口，提升跨系统资源利用率，拓展智能体的任务执行能力。针对不同协议之间的功能交叉与实现差异，应加强身份信息、能力描述和交互接口的适配与互操作验证，降低跨厂商、跨平台协作成本。

- **智能路由：构建融合智能体能力表述、任务意图匹配与动态路径优化的智能路由机制。**在能力描述方面，统一智能体能力信息的表达方式，为跨域发现与能力匹配提供依据。涵盖功能、性能、负载及服务区域等关键内容，通过智能体网关间的信息交换与同步，实时更新能力信息与运行状态，使不同平台能够准确掌握智能体的服务范围与可用状态。在语义匹配方面，结合大模型的自然语言理解能力，解析任务意图并查找符合需求的协作对象。针对不同开发主体、应用场景及交互协议带来的表达差异，按需提供语义翻译与上下文理解支持，降低异构智能体之间的理解成本，避免仅依赖关键词或固定标签而忽略任务语境，提高协作对象选择的准确性。在动态路由方面，综合能力匹配结果、智能体运行状态与实时网络条件，优化连接路径。随任务进展和资源变化调整路由，优先选择能力适配、服务可用且通信质量满足要求的协作节点。

- **质量工程：强化网络传输确定性、吞吐适配**

资料来源：甲子光年智库整理，2026年

性与服务质量可验证性，为智能体协作与任务执行提供稳定可靠的通信保障。一是传输确定性，通过网络切片、资源预留与优先级调度等机制，为关键任务提供端到端的低时延、低抖动与低丢包保障。根据任务优先级和业务需求实施差异化QoS保障，优先保障实时控制指令与关键状态信息的传输，减少大流量数据对时延敏感业务的干扰，降低网络排队时延与传输波动对任务执行时效的影响。二是吞吐适配性，针对智能体Token流的小包、高频交互特征，提升网络设备的包处理能力和并发承载能力。通过流量整形与动态带宽调度，适配多智能体集中调用、状态同步等场景产生的突发流量，缓解汇聚节点的瞬时拥塞，减少消息积压，降低高负载下任务响应变慢或执行中断的风险。三是服务质量可验证性，建立面向智能体业务的网络性能测量与服务等级验证机制，实现传输保障效果的量化评估。通过时延、抖动、丢包率及有效吞吐量等指标，测量关键业务链路的实际传输性能，并与业务SLA/SLO要求进行对照，识别传输质量偏差与性能保障不足等问题。

5.1.2 面向网络管理的网络智能体技术：通信领域知识增强、跨域网络智能体协作编排

管理企业智能体原生网络具体涵盖基础设施、连接交互与任务运行等多个领域，应结合自智网络架构，依托通信大模型与Harness工程，重点发展通信领域知识增强与跨域网络智能体协作编排技术，提升网络智能体的专业处理能力与协作执行能力。

- **通信领域知识增强：围绕具体网络管理任务组织知识与训练，提升通信大模型对网络运行状态、设备配置规范与运维处置的理解能力。**整合通信标准、网络协议、设备手册、运维规程与故障案例等专业知识，通过领域微调与RAG等技术，提高模型对网络专业术语、设备配置及故障机理的理解能力。结合网络拓扑、性能指标、设备告警与历史故障等信息，增强网络异常关联分析、故障根因定位与配置策略生成能力，提高复杂网络管理任务的分析准确性与决策可靠性。

- **跨域网络智能体协作编排：强化不同领域网络智能体之间的任务协同与联合执行能力，支撑复杂网络管理任务的跨域自治。**推进网络智能体专业化分工，围绕基础设施、连接交互与任务运行三大领域，分别构建专业网络智能体，明确各自的管理边界与执行权限。以此为基础，建立面向复杂网络管理任务的跨域依赖分析与联合执行机制，统筹不同领域的资源状态、管理策略与执行约束，明确跨域网络智能体之间的任务衔接关系、执行顺序与协作规则，并通过状态共享、策略冲突检测与执行结果校验，保障跨域操作的一致性与可靠性。

资料来源：甲子光年智库整理，2026年

5.2 企业智能体原生化建设

5.2.1 应用智能体原生化：以任务为中心的服务入口，重塑交互模式，拓展应用生态

智能体原生网络建设需要应用侧同步推进原生化改造，使应用成为能够接入网络、开放服务并参与任务协作的业务主体。统筹应用侧的原生化改造应推进既有应用升级与原生应用开发，推动应用交互从功能选择向任务发起转变。

一方面，推进既有应用的能力开放与智能体化改造，为智能体原生网络提供可调用的服务资源。网站、App及业务平台可将查询、预订、订单处理等功能封装为标准化服务单元，引入智能体交互入口，并向网络中的其他智能体开放业务能力。改造过程中，应同步提供智能体可理解的功能描述、调用条件与结果说明，使已有服务能够被网络发现、准确匹配和按需调用。通过复用既有业务系统、数据与服务资源，将分散在不同应用中的操作环节纳入跨应用协作流程，推动原有应用从独立提供服务向参与网络化任务协作拓展。

另一方面，面向智能体原生网络的协作需求，开展智能体原生应用设计与开发。从任务执行视角组织功能，以用户意图驱动业务流程，开发过程中主动适配互操作协议与意图路由机制，支持跨平台、跨业务环节的多智能体分工协作。推动新型应用不断涌现，在持续迭代与实际应用中逐步筛选、沉淀具有核心价值的智能体应用，形成丰富多元、动态演进的应用生态。

5.2.2 设备智能体原生化：推动终端与网元升级，构建多设备多智能体联动体系

智能体原生网络建设需要推动智能体能力向各类设备延伸，拓展智能体的运行环境与任务执行范围，逐步形成多设备、多智能体联动的运行体系。在终端侧，推动设备适配智能体运行与交互需求，开放感知与控制能力，支持任务在多设备间衔接延续；在网元侧，推动智能体能力融入网络内部，实现从本地智能网元向全域网元联动的能力拓展。

在终端形态与能力方面，推动不同类型设备适配智能体运行与交互需求。面向手机、电脑、智能音箱、智能穿戴、智能座舱、工业终端和服务机器人等设备，根据场景配置适宜的智能体入口、多模态感知与任务执行能力。同时，将终端的语音、视觉、位置感知及设备控制等能力开放给智能体，使其能够结合现场环境与用户需求执行任务。对于需要多设备参与的场景，应支持任务信息和执行结果在终端之间衔接，减少重复操作，使应用服务能够随用户场景变化在不同设备间延续。

在智能网元方面，将智能体能力融入网络内部，依托组网与管理系统，推动本地智能网元与全域网元协同发展。面向本地运行需求，增强路由器、交换机、基站等网元智能化能力，使网元具备本地状态感知、运行分析与指令执行能力，必要时开放设备能力与控制接口。面对跨

资料来源：甲子光年智库整理，2026年

网元协同场景，依托组网与管理系统实现不同网元之间的任务协调与操作联动，提升跨设备的配置调整、故障处置等能力，形成网元本地智能与全网网元协同相结合的运行机制。

5.2.3 网络安全机制智能体原生化：构建智能体内生安全防护体系

智能体原生化不仅是智能能力的融入与拓展，也需要安全机制的同步建设。针对智能体自主决策、跨域协作与任务执行带来的安全需求，应将身份认证、访问控制与通信保护等机制纳入网络原生设计，并通过部署安全智能体增强对AI驱动攻击的识别、分析与处置能力，构建兼顾智能体可信交互与网络主动防御的原生安全体系。

一是智能体身份与能力可信，构建网络准入基础。基于分布式标识与可验证凭证建立全局唯一身份，能力声明需经认证机构签发，防止虚假能力声明导致任务失败或资源滥用。完善智能体身份与能力信息的关联验证机制，确保身份真实、能力声明可信，并支持注册信息随能力变化实时更新，保障智能体发现、匹配与调用过程中的信息准确性。

二是身份访问可控，将智能体身份管理与网络访问策略联动，确保交互主体获得有效授权。在身份注册与认证基础上，将接入策略延伸至网络转发环节，由网关或网络设备核验智能体标识及相应权限，限制未经授权的连接与访问。结合任务需要明确工具、数据和服务的访问范围，减少非法接入、越权调用及跨域交互带来的安全风险。

三是强化通信传输安全，采用加密与完整性保护机制，保障智能体交互信息和传输路径可信。加强智能体与云、端及其他智能体之间的通信保护，采用端到端加密、消息完整性校验与通信双方身份认证等技术，防范数据在传输过程中被窃取、篡改或伪造。针对跨网络、跨平台的智能体交互场景，完善安全通信协议与密钥管理机制，保障不同网络环境下交互数据的机密性、完整性与传输安全。

四是研发并在网络中部署安全智能体，以AI增强对由AI驱动的网络攻击的防御能力。面向AI驱动网络攻击呈现的自动化、动态化与隐蔽化特征，推动安全智能体与网络设备、安全网关及安全管理系统共同部署，增强对异常流量、恶意访问和攻击行为的实时识别与关联分析能力。结合威胁情报、网络运行状态与历史攻击特征，提升对新型攻击手法及潜在安全风险的研判能力，并通过安全策略下发、异常连接阻断与访问权限调整等机制，实现威胁的快速响应与协同处置，推动网络安全防护从规则匹配向智能化主动防御升级。

资料来源：甲子光年智库整理，2026年

5.3 产业参与主体建设建议

5.3.1 运营商：推动网络原生化与自智化建设，提升智能体服务保障能力

依托网络基础设施与运营经验，推进网络原生升级、资源开放、广域连接与自智演进，提升网络服务能力。一是在保障现网稳定运行的基础上，分阶段引入智能体网关、注册发现与语义寻址能力，通过试点验证逐步扩大部署范围，使智能体互联能力从外部适配向网络内生演进；二是与设备商协同开放算力、网络与存储资源接口，将带宽、算力、存储及安全能力封装为可按需调用的服务，配套服务质量监测与保障机制，推动业务模式从提供带宽连接向提供智能体运行与协作保障拓展；三是发挥广域网络覆盖与边缘节点就近服务的优势，结合物理智能体对实时感知、协同控制和持续连接的需求，提供就近接入、边缘处理与跨域通信支持，为多智能体群体协同提供网络支撑；四是推进自智网络L4及以上等级演进，提升网络自身的感知、诊断、自愈闭环能力，以高等级自治网络支撑智能体原生网络的服务质量与运行可靠性。

5.3.2 设备商：研发智能网元和网络智能体，夯实网络承载传输与开放基础

围绕智能体原生网络需求，研发智能网元和网络智能体，提升智能体业务的网络承载与传输能力，并开放设备接口与服务能力。一是结合路由器、交换机、基站等网元的资源条件，内嵌网元级智能体，支持本地状态感知、异常分析与授权范围内的配置调整、故障处置，并与网络智能体协同，增强网元的自主响应与快决策执行能力；二是面向智能体高频交互、突发流量及感知数据与控制指令混合传输等特点，由网络智能体优化设备的业务调度、资源预留与拥塞控制等慢思考能力，提供时延、抖动和丢包等状态监测与自适应能力，为不同任务的差异化传输保障提供产品支撑；三是通过标准化接口开放网络智能体服务化能力，通过跨域编排全局统筹设备状态、资源配置与策略执行能力，支持智能体和管理平台按权限调用，加强跨厂商、跨平台的适配与互操作验证，并兼顾存量设备的软件升级与能力扩展，降低用户集成和改造成本。

5.3.3 企业用户：以智能体应用落地为牵引，统筹系统与基础设施联动改造

以智能体应用落地为牵引，统筹推进智能体应用、既有OSS/BSS系统与网络基础设施的整体联动改造。企业应系统梳理智能体与现有OSS/BSS系统之间的数据、接口和流程依赖，针对信息分散、能力调用受限、跨系统流程不畅等突出问题，分步骤、有重点地开放既有系统的数据与服务能力，使智能体能够复用已有业务资源，有效减少新增应用与存量系统之间的割裂。在此基础上，将算力与网络需求同步纳入统一的部署规划，根据任务交互频次、数据规模、响应时限及安全要求，配套完善网络的连接、传输与运行保障，避免智能体应用建设与基础设施升级脱节。实施过程中，优先选择价值明确、需要贯通业务与网络的典型场景开展验证，对接好业务智能体的任务需求与网

资料来源：甲子光年智库整理，2026年

络侧的资源配置、质量保障及状态反馈，依据实际成效分阶段扩大改造范围，使既有系统与新增智能体互补配合、共同支撑业务运行。

5.3.4 行业标准组织：完善智能体互联互通标准体系，推动跨平台兼容与互操作

联合产业各方，加速智能体互联与接口的统一标准制定，促进智能体跨厂商、跨平台互联互通。一是联合运营商、设备商、企业用户及平台开发者，围绕智能体身份标识、注册发现、能力描述、消息交互、服务调用与安全授权等共性需求，统一接口、数据格式与交互流程，为不同主体建设智能体网络提供共同遵循；二是针对已有协议的功能交叉与实现差异，分层分类明确各类协议的适用场景与互操作要求，完善跨协议适配与兼容机制，减少厂商各自定义接口造成的重复开发与互通壁垒；三是将标准研制与试点验证紧密结合，组织跨厂商、跨平台互通测试，同步完善服务质量与安全要求的测试方法，依据试点反馈持续迭代规范内容，为产品准入、部署验收与规模化应用提供统一依据。

5.3.5 应用开发者：推进应用适配，丰富应用生态，以应用实践参与网络建设

应用开发者可从具体业务需求出发，在应用开发与改造中有针对性地适配智能体网络的开放接口，通过功能开发、接入测试和使用反馈，为网络能力的迭代完善提供来自一线的实践依据。对于既有应用，可将智能体调用的功能封装为标准化服务，开放相应接口，并提供必要的功能说明与调用示例，便于智能体发现、理解和调用，通过应用改造与接口适配，验证网络服务的可用性与适配效果；对于新建应用，可优先选择需要跨应用获取信息或完成任务的典型场景，借助开发工具与测试环境检验接口是否易用、信息能否正确传递、调用过程是否顺畅。在此过程中，通过问题反馈、接口改进建议和开源示例等方式，帮助发现网络设计与实际开发需求之间的差距，使网络建设能够吸收来自不同应用开发者的实践经验，缩小智能体的网络需求与实际网络能力之间的差距，推动网络能力与业务应用共同演进。

资料来源：甲子光年智库整理，2026年

结语

CONCLUSION

人工智能正加速走出对话式交互，以智能体形态融入企业流程、产业现场与公共服务。模型决定智能体的智力水平，网络则影响智能体的行动能力与边界。智能体要完成复杂任务，必须依托网络，将分散在不同系统、设备与组织中的智能主体与服务资源连接起来。智能体的应用边界延伸至何处，网络的服务能力就须覆盖至何处。

回望网络发展历程，网络已历经四次代际跃迁：连接对象由人与人、人与信息、人与应用，逐步扩展至应用互联，先后支撑了语音通信、互联网、移动互联网与云服务的繁荣。当前，智能体的兴起正开启第五次跃迁：连接对象延伸至具备身份、意图与自主行动能力的智能主体。与前四次跃迁不同，此次跃迁不仅拓展了网络的连接规模，更变更了连接主体的性质，改变了网络主体间的交互关系。为此，网络需同步进行系统性调整。

这一调整催生了企业智能体原生网络架构，建设该架构并非脱离既有体系重建，而是立足于现有网络设施与业务资产，并开展升级工作。连接与传输仍是网络的基础能力，应用、数据与专业知识仍是智能价值的重要来源，核心的增量在于协议互联、管控调度、安全可信三个层面：以互操作协议支撑智能体的发现与寻址，以智能路由按需建立连接与优化路径；为智能体建立统一的身份管理、任务分解、资源调度与动态编排中心，使智能体被动态有效组织；以权限与信任约束智能体的接入、退网与行为，保障在网离网状态与交互状态可信可控。

企业智能体原生网络的建设进程离不开产业各方的共同参与。运营商开放网络与算力资源，设备商夯实基础设施，标准组织与开源社区推动规范与互通，企业用户以真实场景检验价值，开发者丰富应用生态。新的网络能力将在场景验证、技术迭代、标准完善与生态共建中持续成熟，逐步支撑智能体在更多行业规模化落地。

未来，智能体的活动范围还将从数字世界进一步延伸至物理世界、科学世界与社会世界，智能体原生网络将为不同类型的智能主体提供泛在连接、可信交互与协同保障，支撑智能能力跨越系统、企业组织与场景边界，让分散智能汇聚为推动产业创新与社会发展的新型生产力。

我们期待，智能所至，即是网络所达。

甲子光年智库

NIDA 全球固定网络创新联盟 | 甲子光年 JAZZYEAR

法律声明

版权声明

本白皮书由甲子光年旗下的甲子光年智库制作完成，白皮书内容的版权及相关知识产权均归北京甲子光年科技服务有限公司所有。任何单位或个人在引用本白皮书内容时，须保持内容的原始性，不得进行歪曲、删改或误导性引用，并须注明白皮书出处为“甲子光年智库”。否则，由此引发的一切后果由引用方自行承担，甲子光年保留追责权利。

免责条款

本白皮书中的行业观点、行业数据、市场预测和相关分析主要来源于甲子光年智库研究团队通过桌面研究、专家访谈、问卷调查、公开数据整理及甲子光年产品数据等方式获得。我们已尽合理努力确保观点与数据的准确性、完整性与可靠性，但甲子光年不对其作出任何明示或暗示的保证。在任何情况下，本白皮书中包含的内容、观点或数据均不构成对任何单位或个人的投资建议、法律建议或其他形式的专业意见，相关决策应由读者自行判断并承担风险。甲子光年对因使用白皮书内容而产生的任何直接或间接损失不承担任何法律责任。

NIDA 全球固定网络创新联盟

甲子光年 JAZZYEAR

THANKS

谢谢观看

北京甲子光年科技服务有限公司是一家科技智库，包含智库、媒体、社群、企业服务版块，立足于中国科技创新前沿阵地，动态跟踪头部科技企业发展和传统产业技术升级案例，致力于推动人工智能、大数据、物联网、云计算、AR/VR交互技术、信息安全、金融科技、大健康等科技创新在产业之中的应用与落地。

关注甲子光年公众号

扫码关注甲子光年智库公众号

智库管理分析师

黄琪丹
13520577912（微信同号）

智库院长

宋涛微信
stgg_6406

商业合作负责人

郑爽
18600502376（微信同号）