

智能体互联网

架构体系·核心技术·产业生态

目录

01  智能体互联网的发展背景

02  智能体互联网的产业生态

03  智能体互联网的基础架构

04  智能体互联网的关键协议

05  挑战与机遇

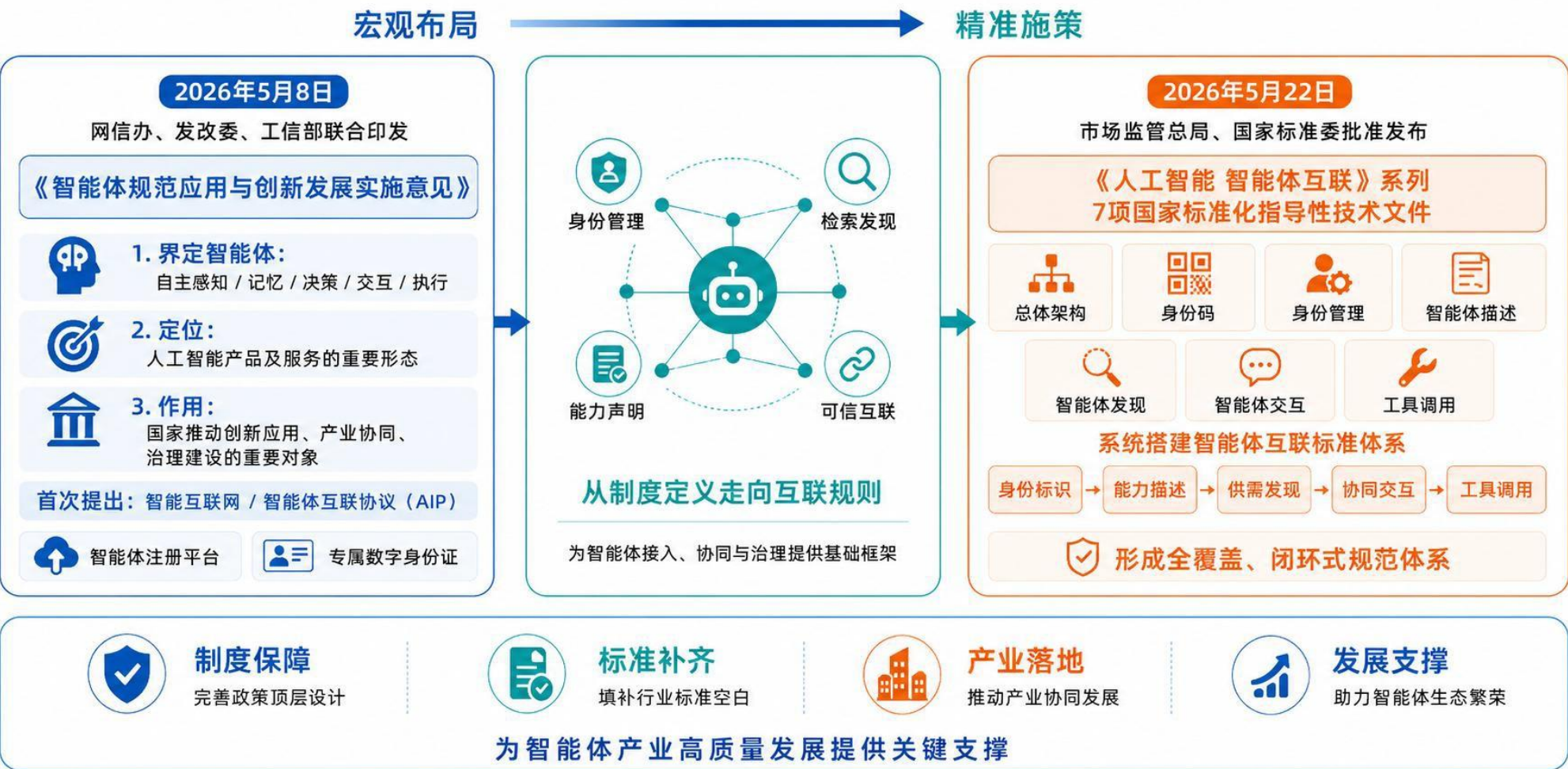
06  总结与展望

智能体产业近两年迎来爆发式发展。行业机构预测，中国智能体市场规模将从2025年的256.8亿元增长至2030年的**4925.2亿元**。智能体正逐步成为网络连接的“新公民”，人与智能体协同、智能体与智能体协作将成为产业发展的新阶段和新常态，倒逼网络架构、传输协议、算力与安全适配新需求。智能体互联网（**Internet of Agents, IoA**）应运而生，并就此迎来高速发展窗口期。

层级	2025年规模	2030年规模	CAGR	2030年占比
智能体基础设施	144.3亿元	2471.2亿元	76.50%	50.20%
智能体操作系统	37.4亿元	54.7亿元	-4.40%	1.10%
数字员工	74.7亿元	2098.4亿元	94.90%	42.60%
数字劳动力交易生态	0.5亿元	300.8亿元	259.60%	6.10%

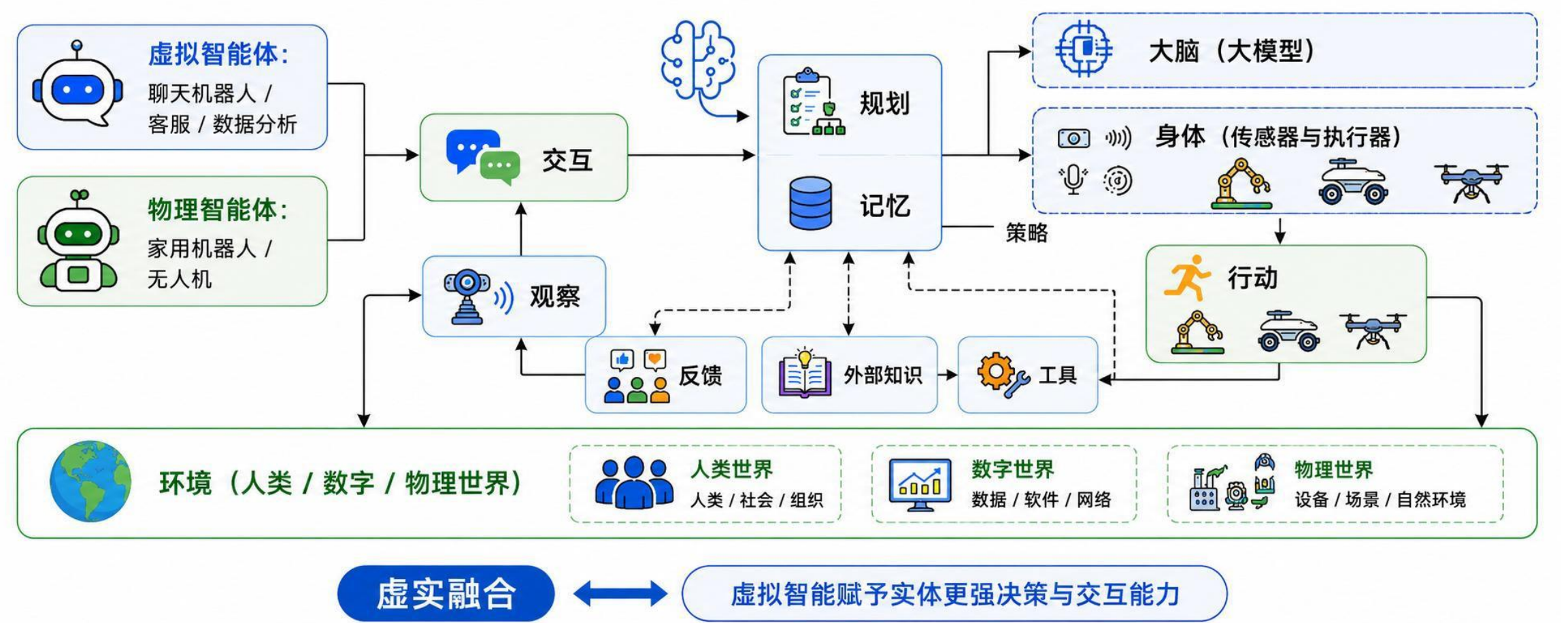
国家大力支持智能体发展，推动智能体互联网构建

为抢占智能体发展先机，国家从宏观政策与标准规范双轮驱动，密集出台多项举措扶持智能体赛道发展，搭建起完备的制度与标准支撑体系，全方位助推智能体与智能体互联网的规范化建设，为行业长效发展筑牢政策根基。



虚实智能体协同共生，智能体互联网的软硬一体公民

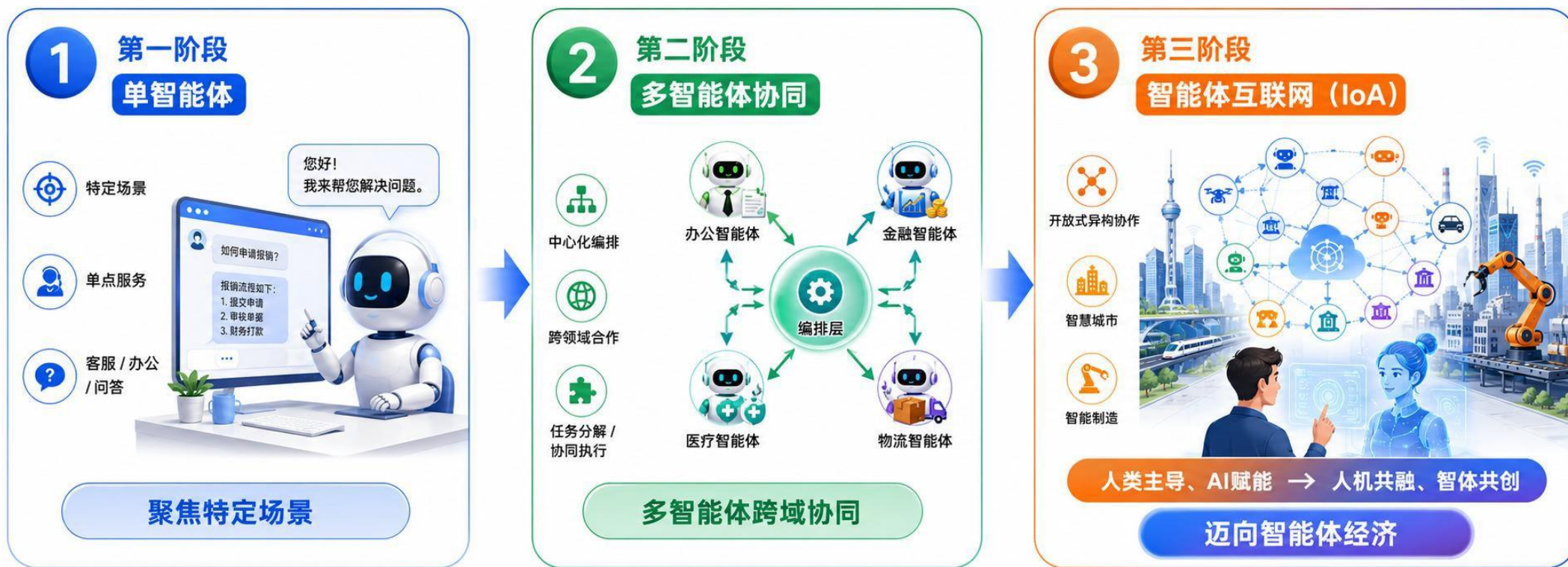
智能体按照技术形态可大致分为两类：**虚拟智能体**和**物理智能体**。虚拟智能体为纯数字形态，运行于云端/终端设备，如聊天机器人、客服智能体、数据分析智能体等；物理智能体则配备传感器和执行器（机械臂、车轮），如家用机器人、无人机等。未来的主流趋势是**虚实融合**，虚拟智能赋予实体更强的决策与交互能力。



从单点突破到生态互联，智能体互联网开启人机共融新格局

从发展演进脉络来看，智能体正逐步完成由单点落地走向全域生态互联的升级，演化进程主要分为三个阶段：

- 第一阶段：单智能体聚焦特定场景，在垂直领域完成独立任务，实现局部效率优化；
- 第二阶段：多智能体协同通过中心化编排层实现跨领域合作，打通不同业务领域的业务壁垒；
- 第三阶段：走向智能体互联网，推动经济形态从“人类主导”演进为“人机共融”的**智能体经济**。



智能体经济蓬勃发展，智能体互联网支撑全新价值释放

智能体经济是指具备自主感知、规划、决策和行动能力的AI智能体作为独立经济主体，直接参与市场交易、协作与价值创造的一种全新经济形态。智能体互联网让分散的智能经济节点完成联动协同，拓宽消费端、企业端的商业化空间，保障多元化付费模式平稳运转，为智能体经济的长效发展打下坚实基础。



目录

01  智能体互联网的发展背景

02  智能体互联网的产业生态

03  智能体互联网的基础架构

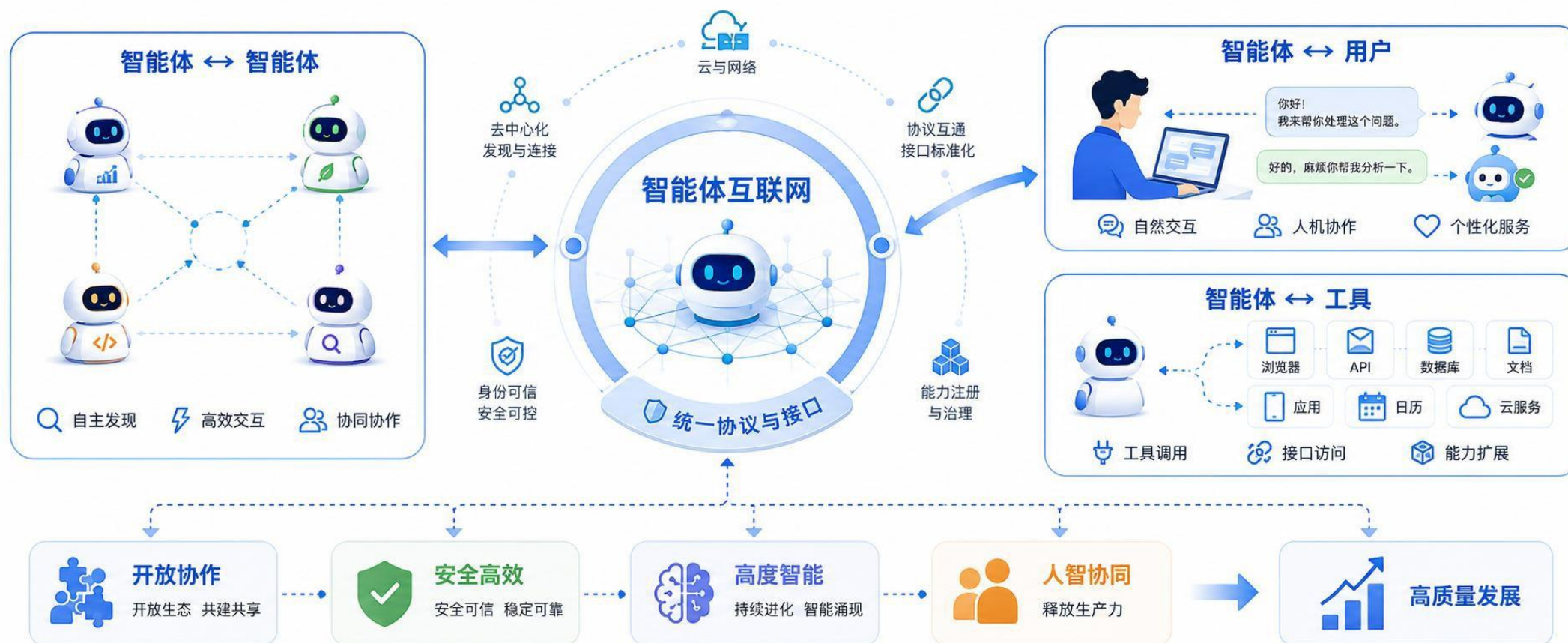
04  智能体互联网的关键协议

05  挑战与机遇

06  总结与展望

智能体互联网的定义与愿景

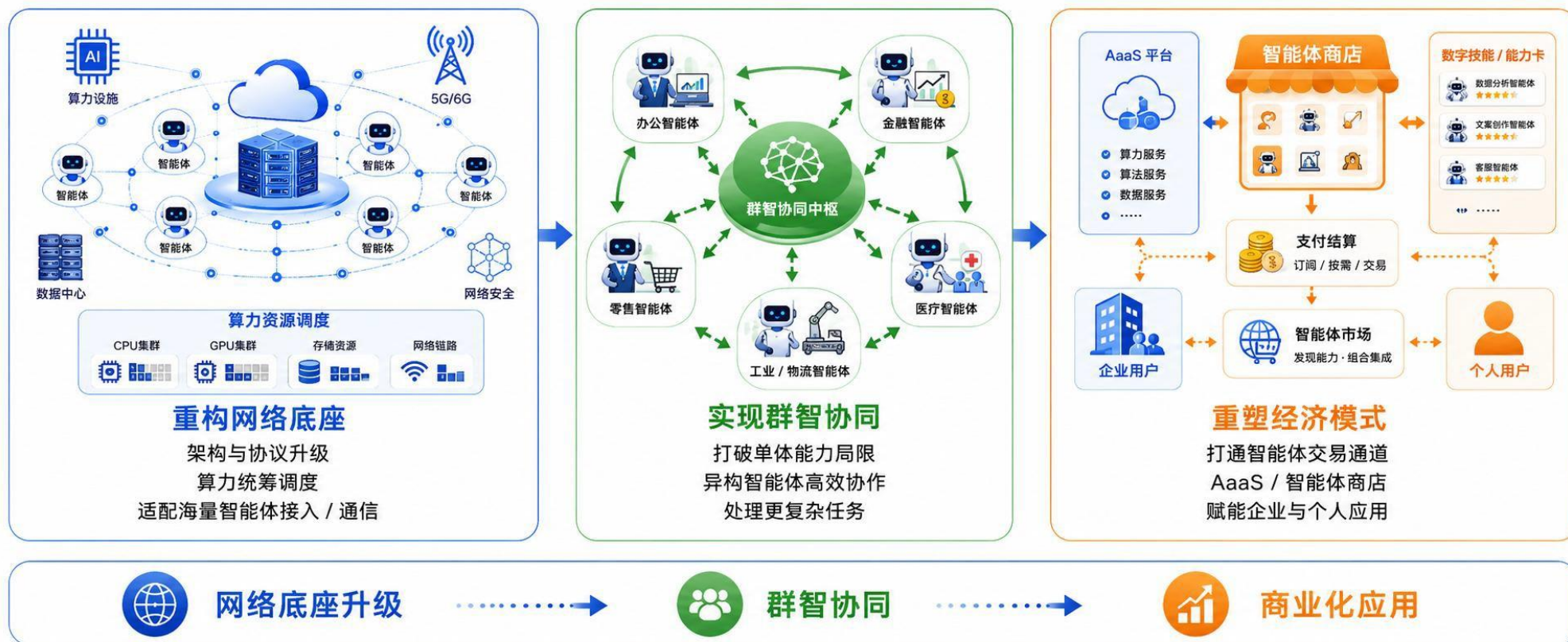
智能体互联网是一个以智能体为核心互联主体，通过统一协议与接口，实现**智能体之间、智能体与用户、智能体与工具之间**自主发现、高效交互、协同协作的新型互联网基础设施。其愿景是构建一个开放协作、安全高效、高度智能的网络环境，形成全新的人智协同范式解放生产力，推动社会高质量发展。



智能体互联网的核心价值

依托统一互联体系，智能体互联网完成基础设施、协作模式、商业生态多层突破，核心价值可归纳为三点：

- **重构网络底座**：升级传统网络架构与配套协议，统筹调度算力资源，适配海量智能体的接入、通信需求；
- **实现群智协同**：打破单智能体的能力局限，实现异构智能体跨领域协作，处理复杂度更高的任务；
- **重塑经济模式**：打通智能体之间的交易通道，落地智能体商店等商业模式，盘活算力、智能技能等全新生产要素，赋能企业与个人端商业化应用。



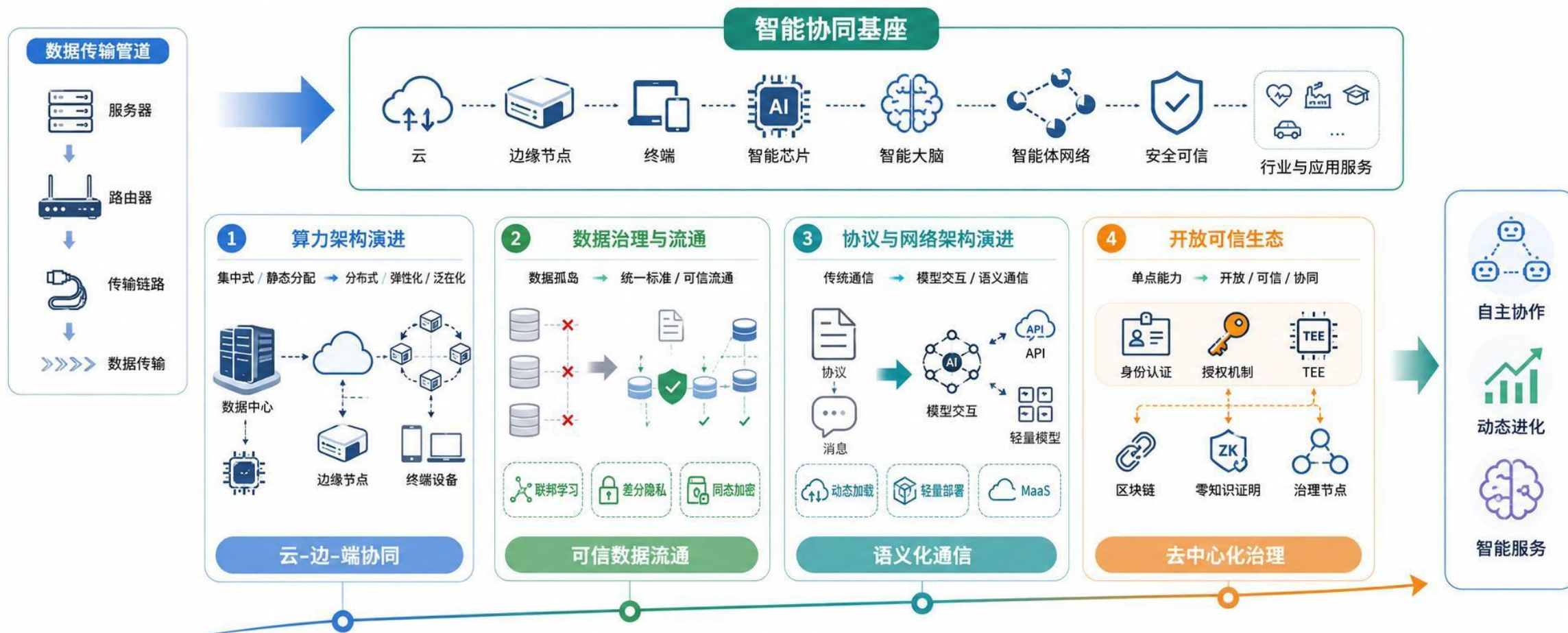
传统互联网与智能体互联网的主要差异

传统互联网是人驱动信息流动的信息网络，而智能体互联网是智能体驱动价值创造的自主协作网络，前者解决的是“连接与获取”的问题，后者解决的是“理解与执行”的问题。

对比维度	传统互联网	智能体互联网
 连接主体	连接人与设备、静态信息	以智能体为核心节点，实现人、智能体、设备互通
 交互特点	被动响应人工指令	节点可自主感知、独立决策、主动执行任务
 信息处理	仅搬运、传输原始数据	解读信息深层意图，完成智能化加工
 协作形式	跨平台协作依赖人工调度	依托群体智能实现智能体自主分工协作
 协议标准	沿用 TCP/IP，侧重数据传输	增设 MCP、A2A 等专属协议，完善身份、授权规则

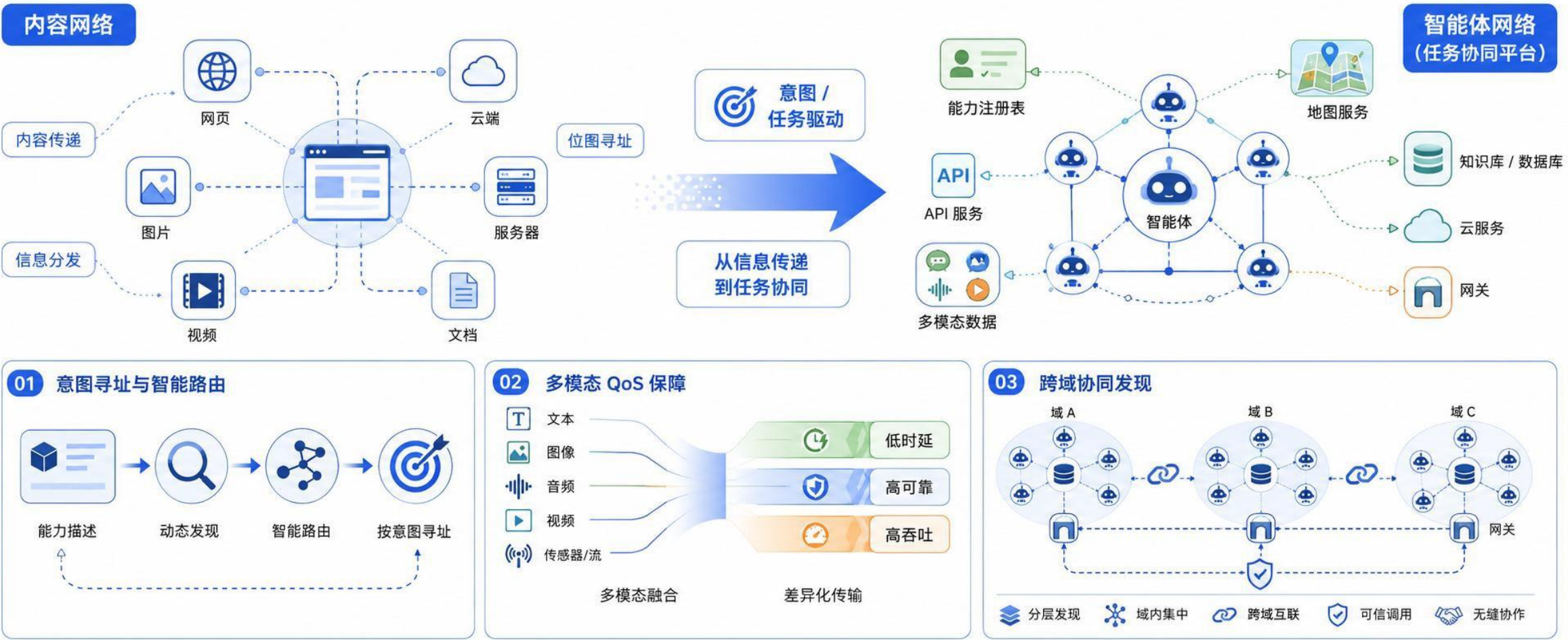
互联网的演进路径：从网络基础设施到智能服务基础设施

智能体互联网要求网络基础设施从“数据传输管道”升级为“智能协同基座”，通过重构资源调度逻辑、优化数据流通机制、强化模型协同能力，满足智能体自主协作、动态进化的核心需求。



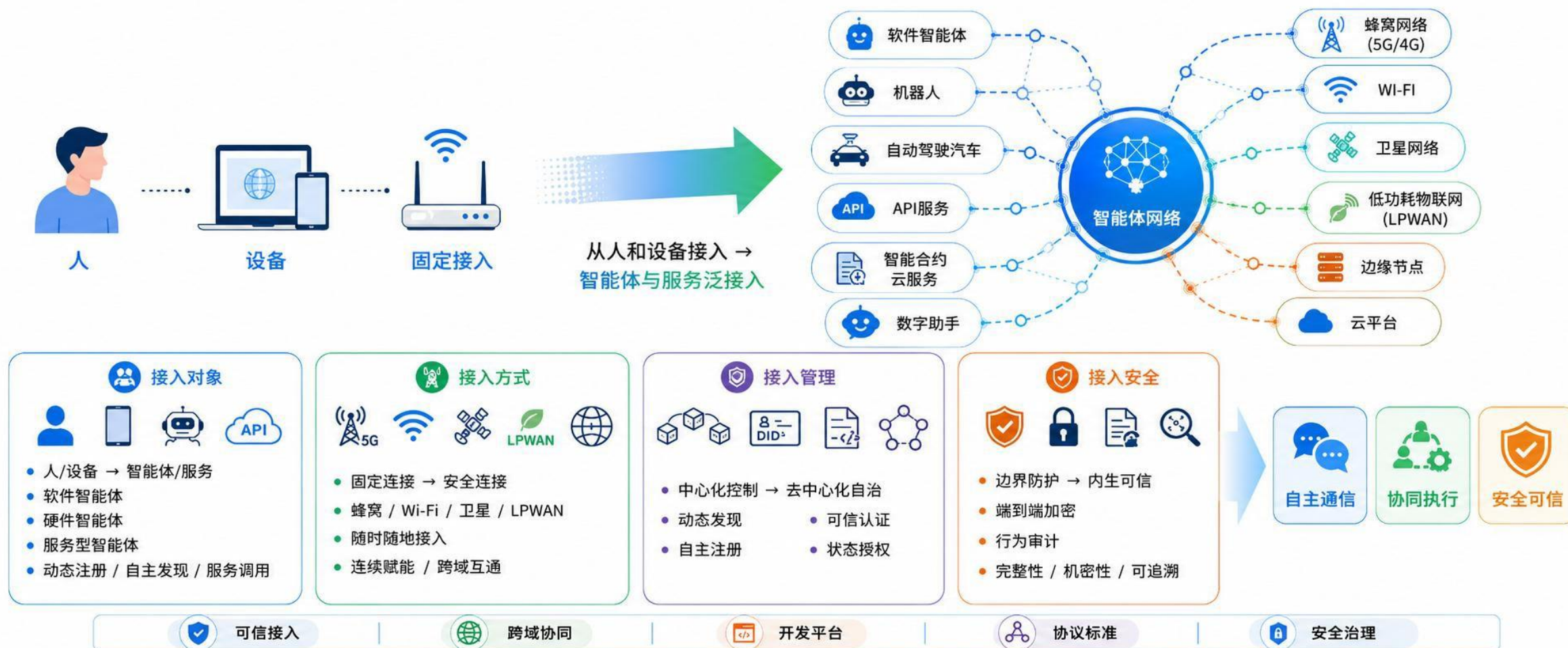
互联网的演进路径：从内容网络到智能体网络

智能体互联网要求网络基础设施从以“内容”为中心的信息传递网络，迈向以“智能体”为核心的任务协同平台，跳出单纯连接设备、传输数据的传统定位，获得意图理解能力，可承载复杂业务与跨域大规模协作。



互联网的演进路径：从单一接入到泛在接入

智能体互联网的接入体系实现全方位扩展：接入对象从人与设备扩展至智能体与服务；接入方式向蜂窝、Wi-Fi、卫星等多场景泛在连接演进；接入管理从中心化控制转向去中心化自治；接入安全从边界防护升级为内生可信。



互联网的演进路径：从面向连接到面向任务的XaaS平台

智能体互联网将架构核心从连接转向任务，构建由自治智能体单元组成的分布式系统。该系统具备自主决策、动态协作、环境自适应与弹性扩展四大特征，为工业互联网、智慧城市等大规模智能化应用提供原生支撑。



智能体互联网的应用场景

与传统互联网应用场景不同，智能体互联网的应用呈现出跨主体、跨平台、跨空间以及网络级协同四个核心特征。其主要落地场景包括：**产业侧**赋能制造、企业办公、产业链协同；**消费侧**依托各类终端打造个人专属智能分身、全屋智慧家居；**城市侧**落地智慧政务、城市治理、公共医疗。



让分散的智能体形成可协作、可信任、可治理的任务执行网络

智能体互联网生态图谱

智能体互联网有一套完整的生态系统，涵盖底层网络基建、统一协议标准、适配化模型平台，并向上延伸至各类开发工具与商用服务、多元应用场景，同时配套完备的治理机制与市场化交易体系，各个层级彼此联动、互相支撑。



目录

01  智能体互联网的发展背景

02  智能体互联网的产业生态

03  智能体互联网的基础架构

04  智能体互联网的关键协议

05  挑战与机遇

06  总结与展望

智能体互联网的四层架构

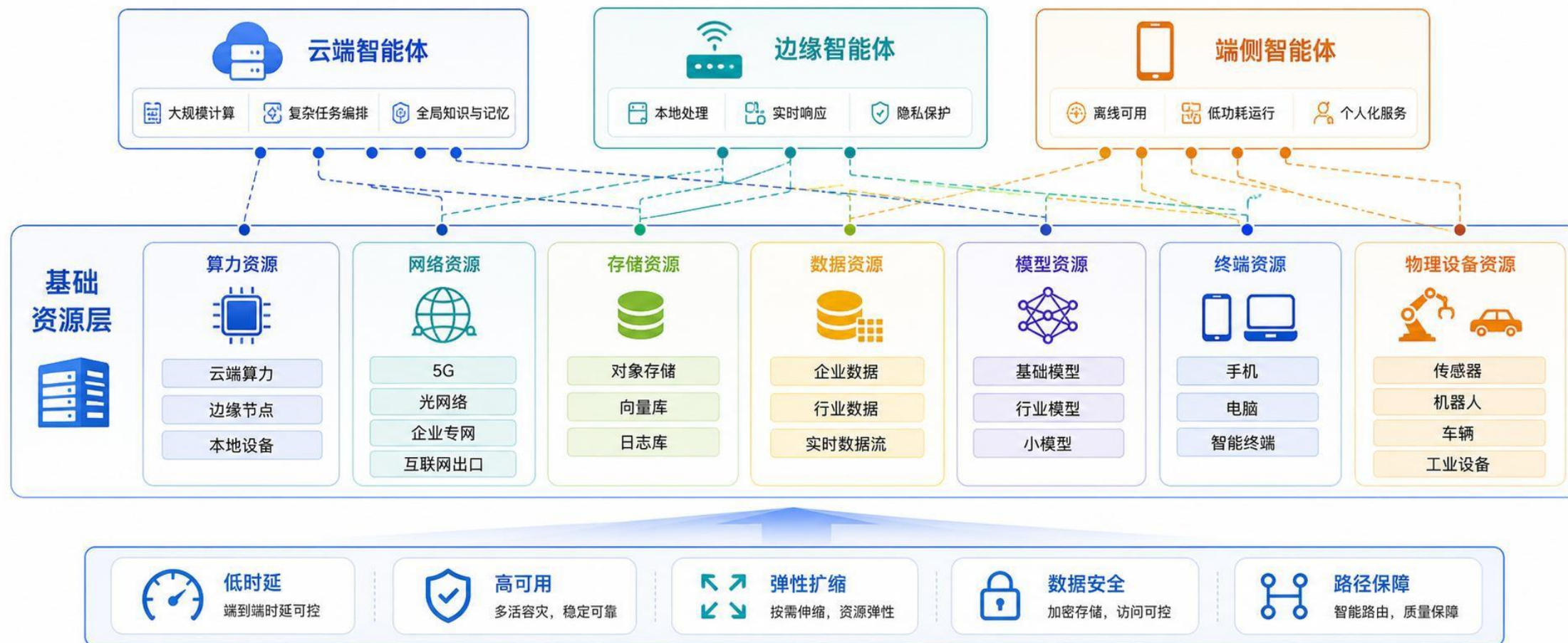
智能体互联网目前已进入标准化建设阶段。不同厂商和机构提出的参考架构各有差异，但核心目标都是解决智能体如何连接、协作与应用的问题。今年最新发布的《人工智能 智能体互联》国家标准（GB/Z 185）已明确四层技术参考模型。

- **基础资源层**提供算力、网络、存储、数据、模型、终端和物理设备，是智能体运行与互联的底座。
- **智能体互联层**负责身份标识、能力描述、发现寻址、认证授权、交互通信和工具调用，是智能体之间建立连接的关键层。
- **协作管理层**负责任务管理、策略控制、安全治理、运行监控、审计追踪和服务运营，让协作过程安全、可控、可追溯。
- **应用使能层**面向行业场景开放智能体能力，包括应用市场、服务编排、能力封装、API 开放和定制开发。



基础资源层

基础资源层为智能体运行、互联和工具访问提供底层资源支撑，主要包括计算资源、网络资源、存储资源、数据资源、模型资源、终端资源和物理设备资源。它决定模型推理、任务调度、上下文访问和跨域通信的稳定性，也承担路径保障、QoS、安全隔离、边缘节点和智能化运维等能力，是上层智能体服务可靠运行的资源底座。



智能体互联层建立智能体之间、智能体与工具系统之间的标准化连接关系，是跨平台、跨组织互操作的核心。该层围绕身份标识、能力描述、供需发现、协同交互和工具调用形成技术链路，使智能体服务能够被识别、被发现、被验证、被调用，并在任务执行过程中交换状态、上下文和交付物。



协作管理层

协作管理层对智能体互联和任务执行进行统一编排、策略约束和运行治理，覆盖任务管理、路径编排、权限控制、安全策略、运行监控、异常处置和审计追踪。它负责约束任务分发、工具访问、状态同步和结果交付，保证智能体协作符合授权范围、业务规则和合规要求。



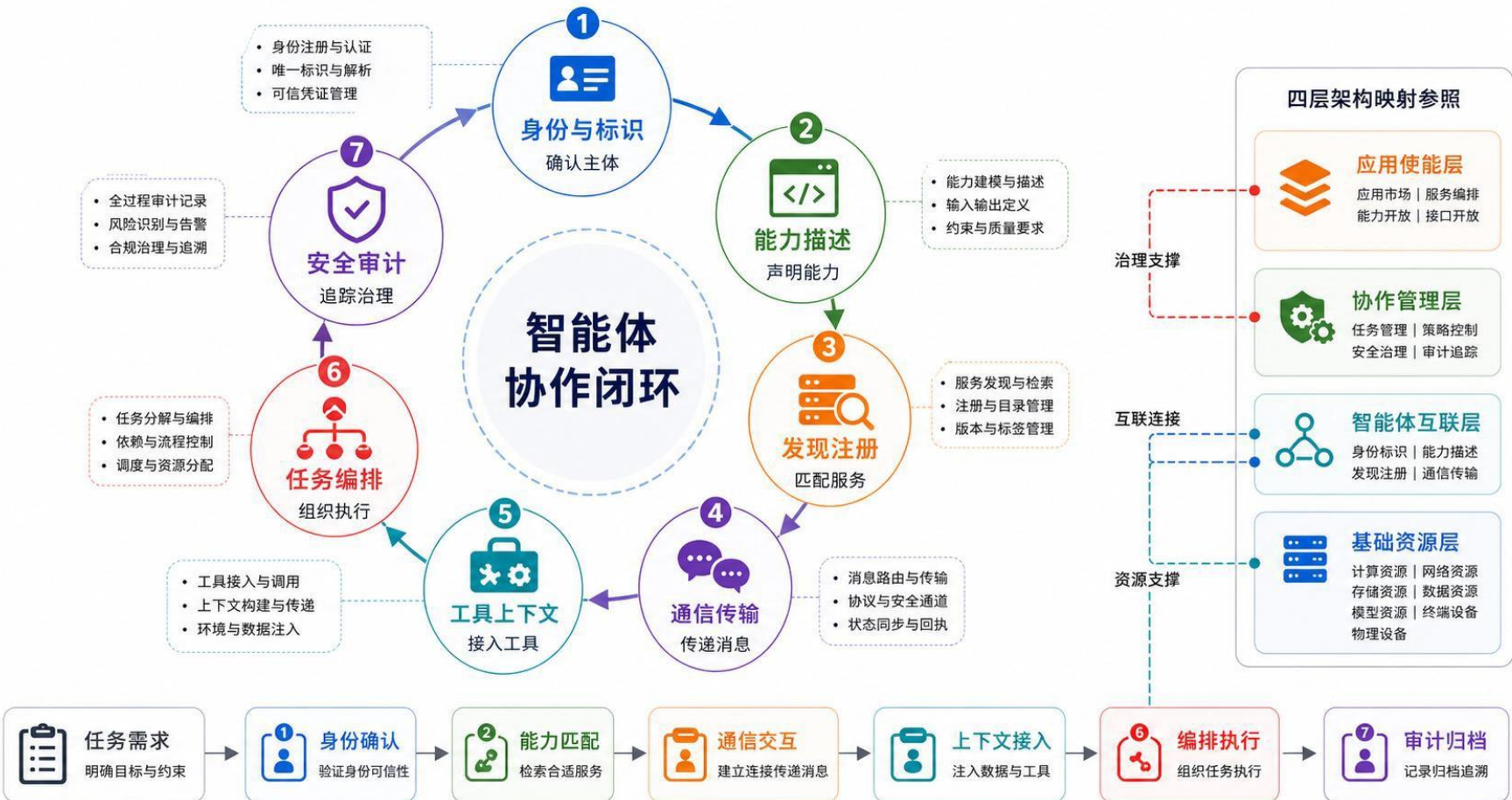
应用使能层

应用使能层面向行业场景提供智能体能力的封装、开放、编排和运营能力，包括应用市场、服务编排、能力开放、API接入、定制开发和运营计费。它把底层资源、互联能力和管理能力沉淀为可复用组件，支撑政务、金融、制造、客服、研发等场景快速接入智能体服务。



七项关键能力赋能智能体互联网

四层架构勾勒了智能体互联网的整体系统边界，但要实现大规模、跨平台的智能体互联协作，还需要进一步解决身份确认、能力表达、智能体发现、任务协同以及全过程保障安全可信等问题，行业标准化工作重点正围绕这些关键环节构建规范体系。身份与标识、能力描述、发现注册、通信传输、工具上下文、任务编排和安全审计七项关键能力是保障智能体互联互通的基础。



能力一： 身份与标识

身份与标识用于确认智能体的唯一身份、所属主体、服务入口和可信状态，是跨系统协作的基础。该能力需要支持唯一标识、身份解析、凭证验证、主体归属确认、服务地址绑定和有效状态检查，使请求方在交互前能够判断协作对象是否真实、可信、可访问。



身份可信是智能体安全协作的基础，确保可验证、可追溯、可问责。



可信身份 → 可信连接 → 可信协作

能力二：能力描述

能力描述用于把智能体能力转化为机器可读、可检索、可比较的服务声明。就像餐厅菜单或岗位说明书，先说明服务范围，再决定是否委托任务。标准化能力描述可以降低智能体之间的沟通成本，也方便能力搜索、匹配和组合。描述内容应包括能力范围、输入输出、交互方式、认证要求、权限边界、成本时延、服务状态和限制条件。

能力卡片模板



智能体名称

一句话描述该能力的用途

版本：1.0.0

更新时间：2025-05-20



服务名称

该能力提供的具体服务名称



能力范围

该能力覆盖的业务范围与适用场景



输入要求

输入的内容、格式、参数等要求



输出结果

输出的内容、格式、结构等说明



权限要求

调用所需的身份、权限或资质要求



成本时延

使用成本（费用）与预计耗时



质量承诺

准确率、可用性、SLA 等质量指标



限制条件

不适用的场景、合规限制等说明

类比：菜单与岗位说明

能力卡片 ≈ 菜单

能力卡片

菜单



告诉你“这道菜是什么、有什么料、多久出、多少钱、有哪些忌口”。

任务匹配 ≈ 点菜



你提出需求，服务员根据菜单推荐最合适的菜品。

任务匹配示例



任务：合同初审

需求：识别合同关键条款，评估风险点，给出初审意见。

约束：合规优先，准确率高，T+10 分钟内给出结果，成本可控。

候选能力卡片



法务智能体

匹配度 92%



服务名称 合同审查与风险识别



能力范围 各类商业合同初审



输入要求 合同文本（PDF/Word）



输出结果 风险清单 + 初审意见



权限要求 法务角色，合同调取权限



成本时延 ¥0.08/页，约 8 分钟



质量承诺 准确率 ≥ 95%，可用性 ≥ 99%



限制条件 不处理涉密/涉诉类合同



通用大模型

匹配度 68%



服务名称 文本理解与生成



能力范围 通用文本分析



输入要求 文本输入



输出结果 文本分析结果



权限要求 无特殊权限



成本时延 ¥0.02/页，约 2 分钟



质量承诺 准确率 ≥ 70%，可用性 ≥ 99%



限制条件 专业性较弱，风险识别不足



财务智能体

匹配度 55%



服务名称 财务条款审查



能力范围 财务相关条款检查



输入要求 合同文本



输出结果 财务条款意见



权限要求 财务角色权限



成本时延 ¥0.06/页，约 6 分钟



质量承诺 准确率 ≥ 90%，可用性 ≥ 99%



限制条件 不覆盖法律合规风险

推荐结果



法务智能体

已选择

- ✓ 匹配度最高
- ✓ 专业法务能力
- ✓ 质量可靠
- ✓ 合规与风险覆盖全面
- ✓ 成本可接受
- ✓ 满足时延要求

执行任务



理解需求
提取关键词与约束



检索能力
从能力库中查找候选



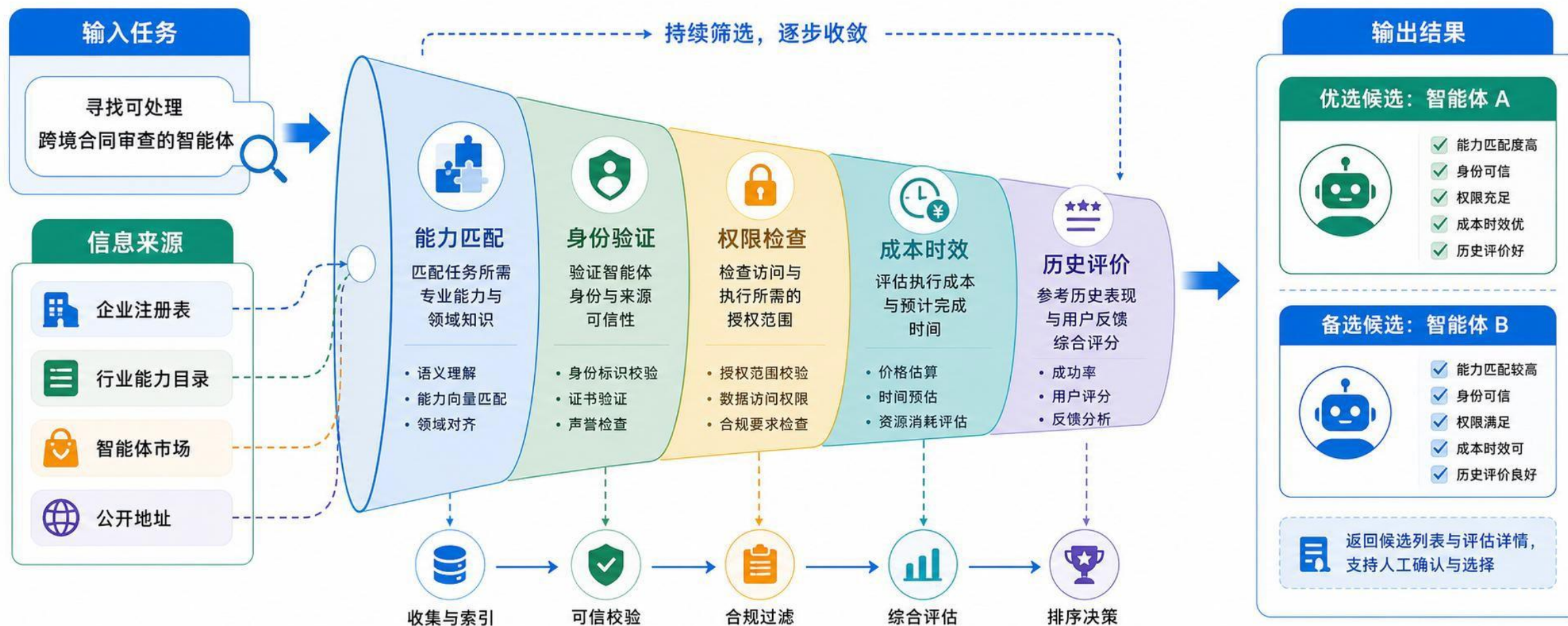
评估匹配
从相关性、质量、成本等维度评分



推荐选择
输出最优能力并执行

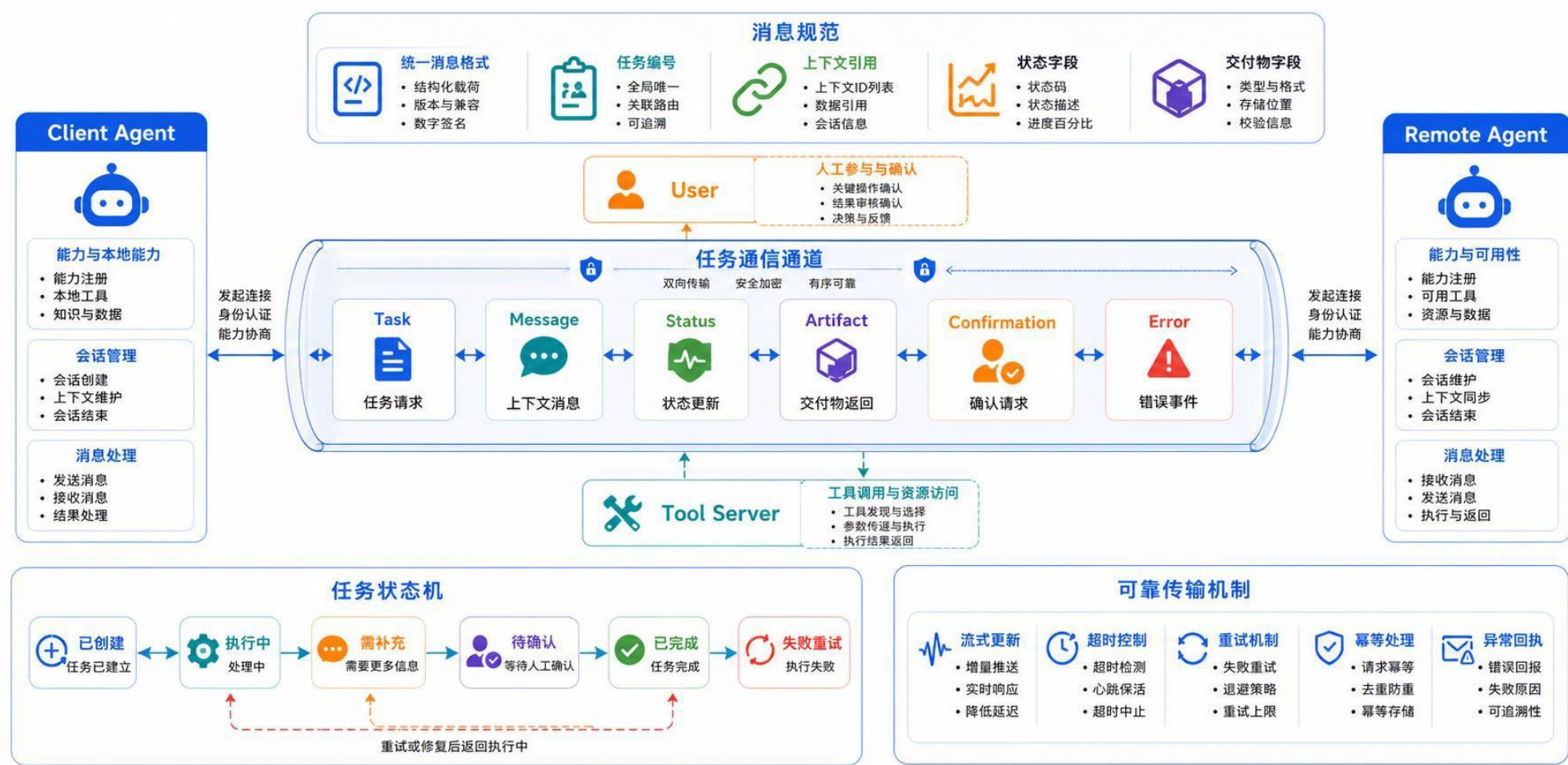
能力三：发现与注册

发现与注册解决的是到哪里找到合适智能体的问题。可能的方式包括企业内部注册表、行业能力目录、智能体市场、公开地址发现、语义搜索和推荐匹配。传统搜索找的是网页，智能体发现找的是可完成任务的能力主体。一个好的发现机制不只看关键词，还要综合身份可信度、能力匹配度、权限范围、成本和服务质量。



能力四： 通信与传输

通信传输用于支撑智能体之间围绕任务生命周期交换结构化信息，包括任务目标、上下文、约束条件、状态变化、异常信息、中间结果和交付物。该能力需要明确消息格式、状态模型、传输通道、流式更新和失败重试机制，保证跨系统协作过程稳定、可理解、可恢复。



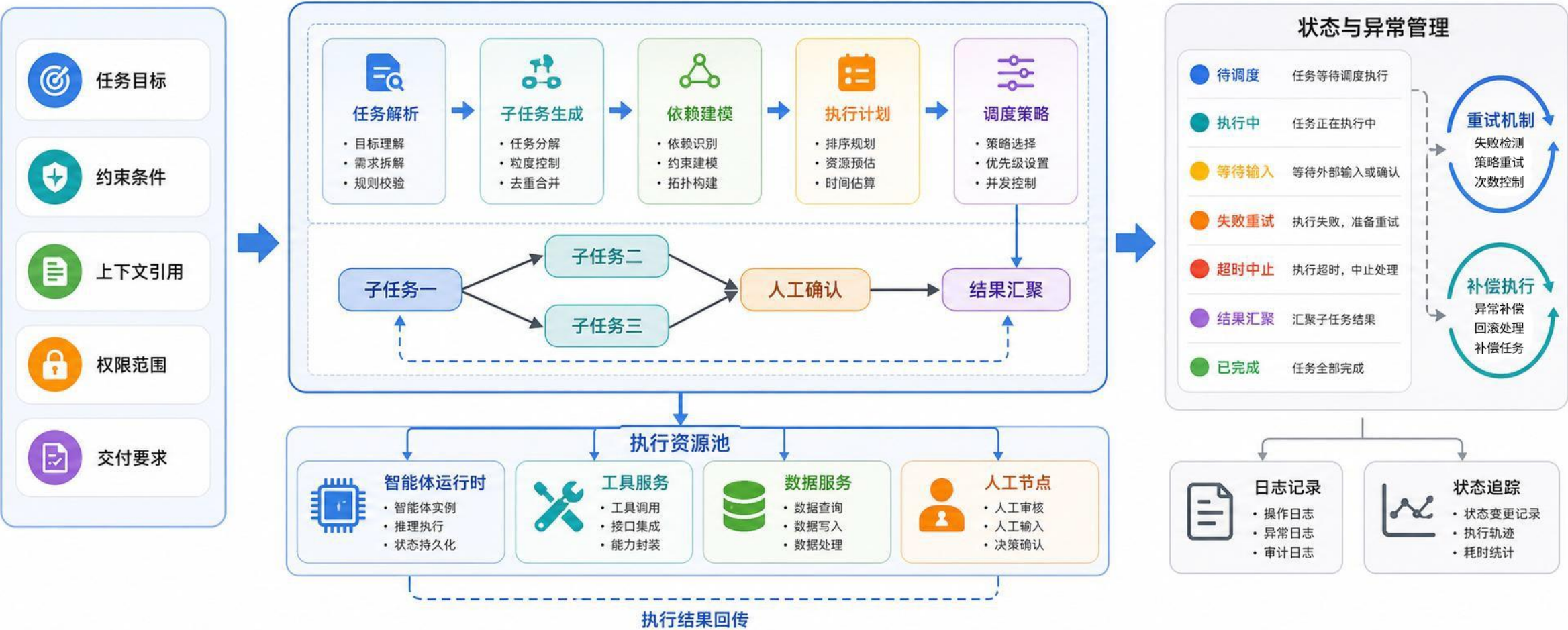
能力五： 工具与上下文接入

智能体要真正完成任务，必须接入真实业务系统，而不是只靠模型内部知识。工具和上下文接入用于把智能体任务连接到真实业务系统、外部工具和上下文资源，使智能体能够在授权范围内读取数据、调用接口、执行操作并返回结构化结果。该能力覆盖工具目录、资源目录、上下文读取、参数校验、权限控制、调用执行和结果格式化。



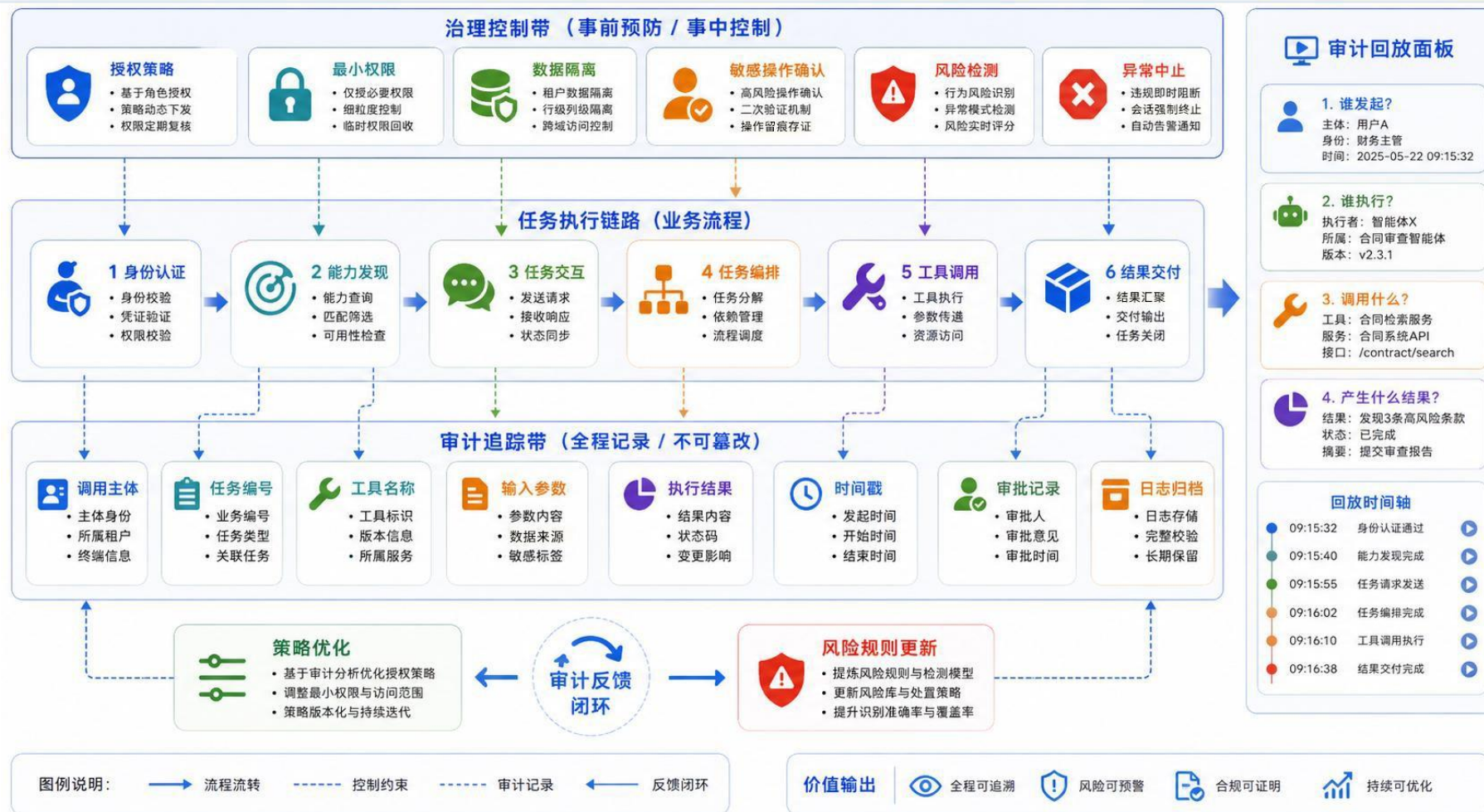
能力六：任务编排与协作

复杂任务通常不是一个智能体独立完成，而是多个智能体分工协作。任务编排用于把复杂目标拆解为可执行子任务，并在多个智能体、工具系统和人工节点之间管理依赖关系、执行顺序和状态变化。它需要支持任务拆分、角色分配、并行执行、失败重试、状态汇聚、结果合成和异常中止，是从单次调用走向流程级协作的关键能力。



能力七：安全、授权与审计

安全、授权与审计贯穿身份、发现、通信、工具调用和任务编排全过程，用于控制权限边界、约束高风险动作、记录关键行为并支持责任追溯。该能力包括访问控制、最小权限、敏感操作确认、数据隔离、异常检测、日志审计、结果回放和合规报告，是智能体互联网规模化运行的治理底座。



目录

01  智能体互联网的发展背景

02  智能体互联网的产业生态

03  智能体互联网的基础架构

04  智能体互联网的关键协议

05  挑战与机遇

06  总结与展望

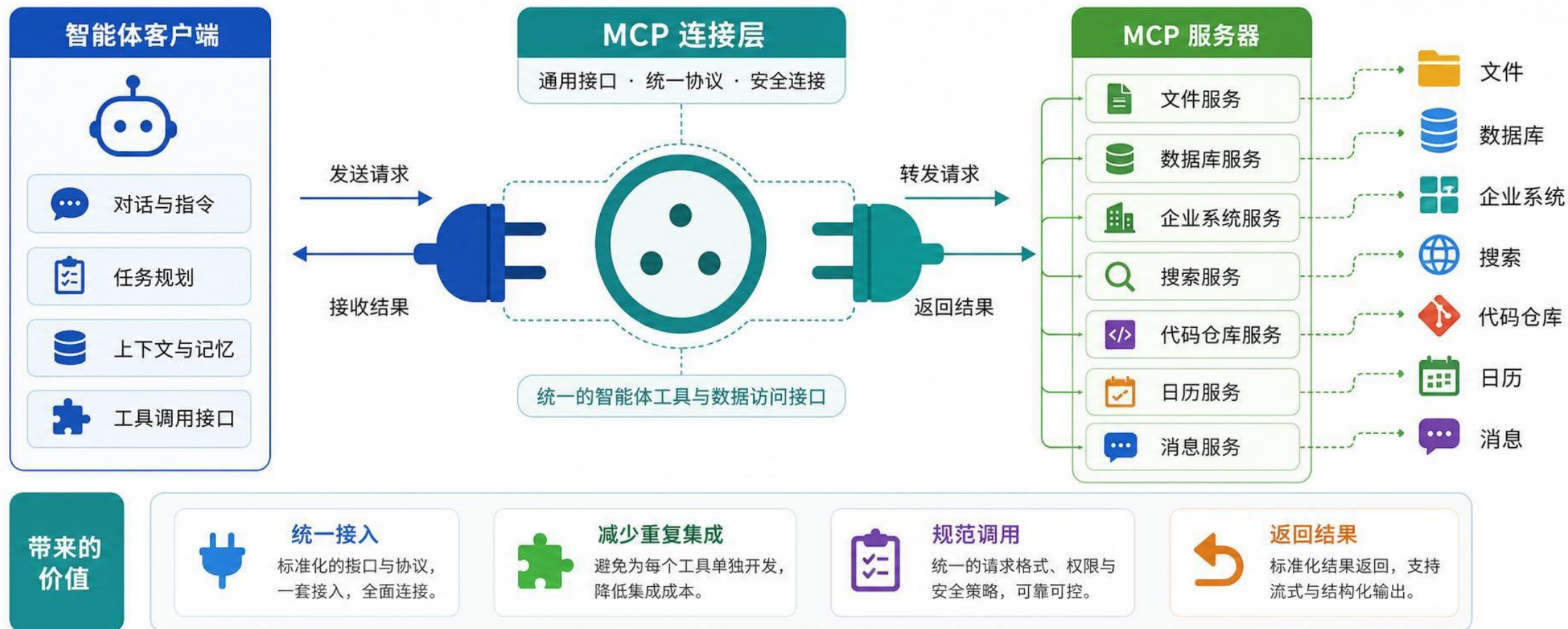
协议生态总览

随着智能体从单体应用走向跨平台、跨组织协作，协议正在成为互联互通的关键基础。当前协议生态仍处于快速发展和标准探索阶段，其中MCP、A2A 已形成较清晰的官方架构和开发者生态；AIP、ANP 分别从通用交互规则和开放网络协同切入；AP2、x402 将智能体能力延伸到交易支付；AG-UI、A2UI 面向人机界面事件流与生成式界面；RVP 则聚焦虚实融合场景下的异构通信。



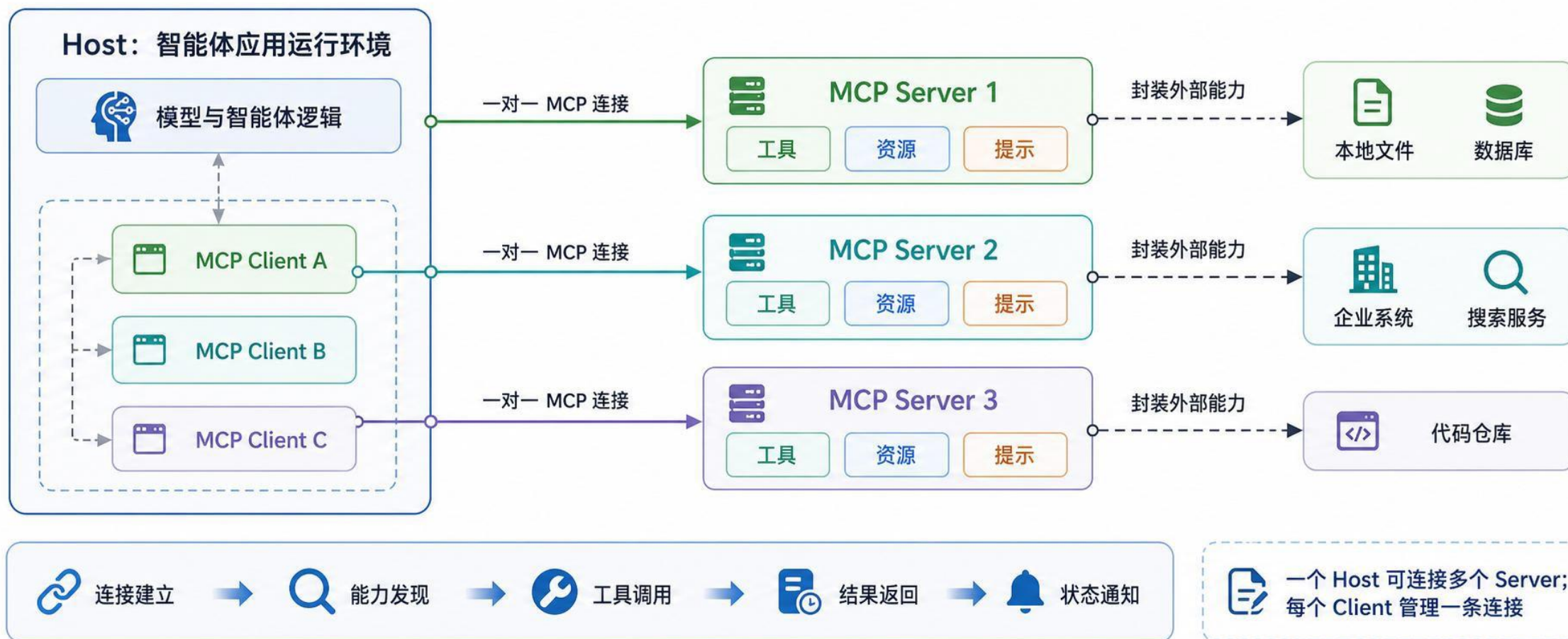
MCP：模型上下文协议

MCP (Model Context Protocol) 是智能体访问外部工具和上下文的统一接口。它让AI应用可以用相对统一的方式连接文件、数据库、搜索、业务系统、代码仓库和工作流。MCP的价值是降低重复集成成本，不需要每个智能体为每个工具单独写一套连接方式。MCP 就像一个通用插座，智能体不用关心每个设备内部结构，只要通过标准插口使用能力。



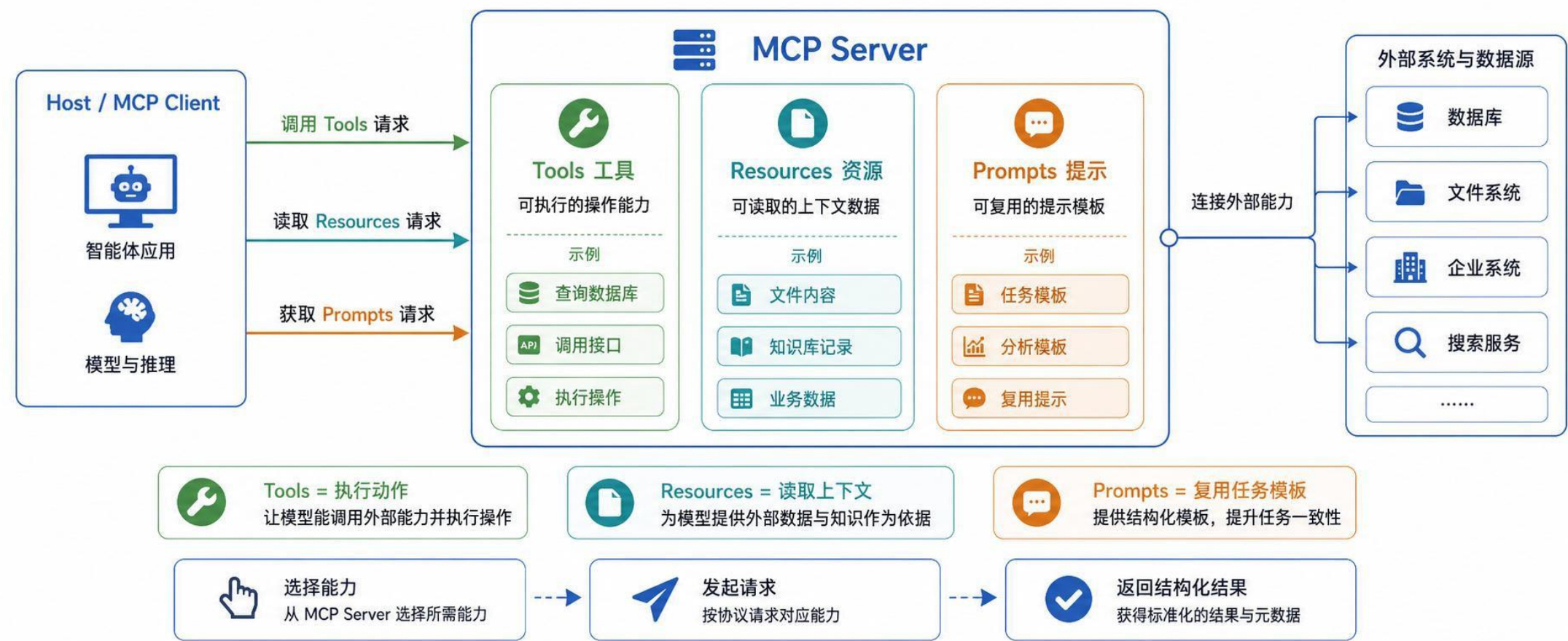
MCP官方架构

MCP 官方架构采用Host-Client-Server模型。Host是运行AI应用的环境，例如IDE、桌面应用、智能体平台。Client通常运行在Host内部，负责和MCP Server建立一对一连接。Server负责把外部能力封装出来，例如文件、数据库、企业系统、搜索服务、代码仓库等。一个Host可以连接多个MCP Server。



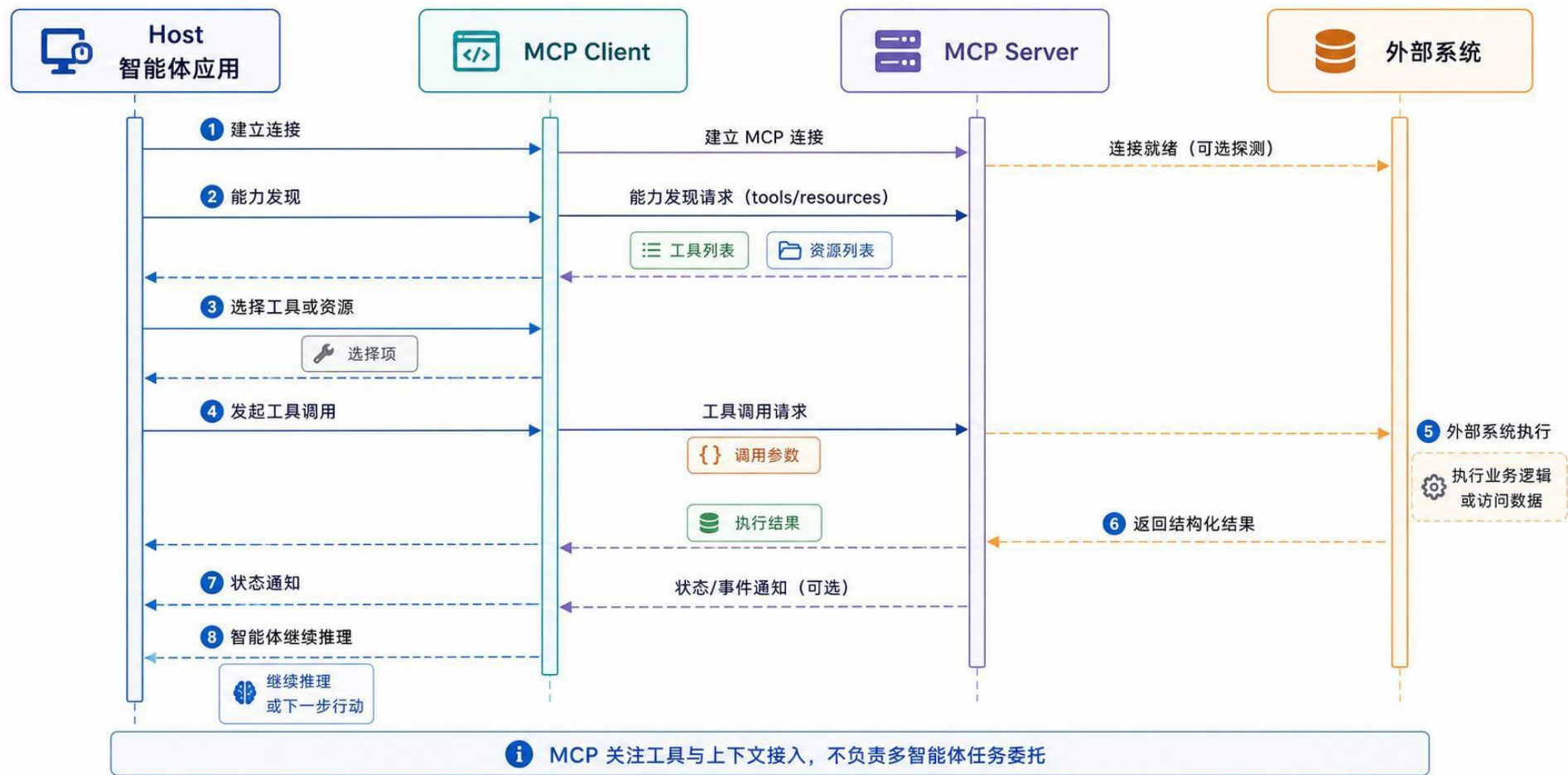
MCP 的能力对象

MCP 的核心能力对象包括工具（Tools）、资源（Resources）和提示模板（Prompts）：工具用于执行外部操作与函数调用，资源用于提供结构化数据与上下文信息，提示模板用于规范模型调用方式与任务表达。通过这一抽象，MCP 将原本分散的系统能力统一封装为可发现、可调用、可组合的标准接口，从而提升模型与外部系统之间的可扩展性与互操作性。



MCP交互流程

MCP 基本交互过程通常包括四个阶段：首先由客户端发起上下文请求并连接MCP 服务；随后服务端返回可用能力列表，包括工具、资源与提示模板；在任务执行阶段，模型根据上下文选择合适能力并发起调用；最后由服务端返回执行结果并更新上下文状态，实现一次完整的闭环交互。通过这一流程，MCP将原本分散的工具调用转化为标准化、可编排的上下文驱动协作机制。



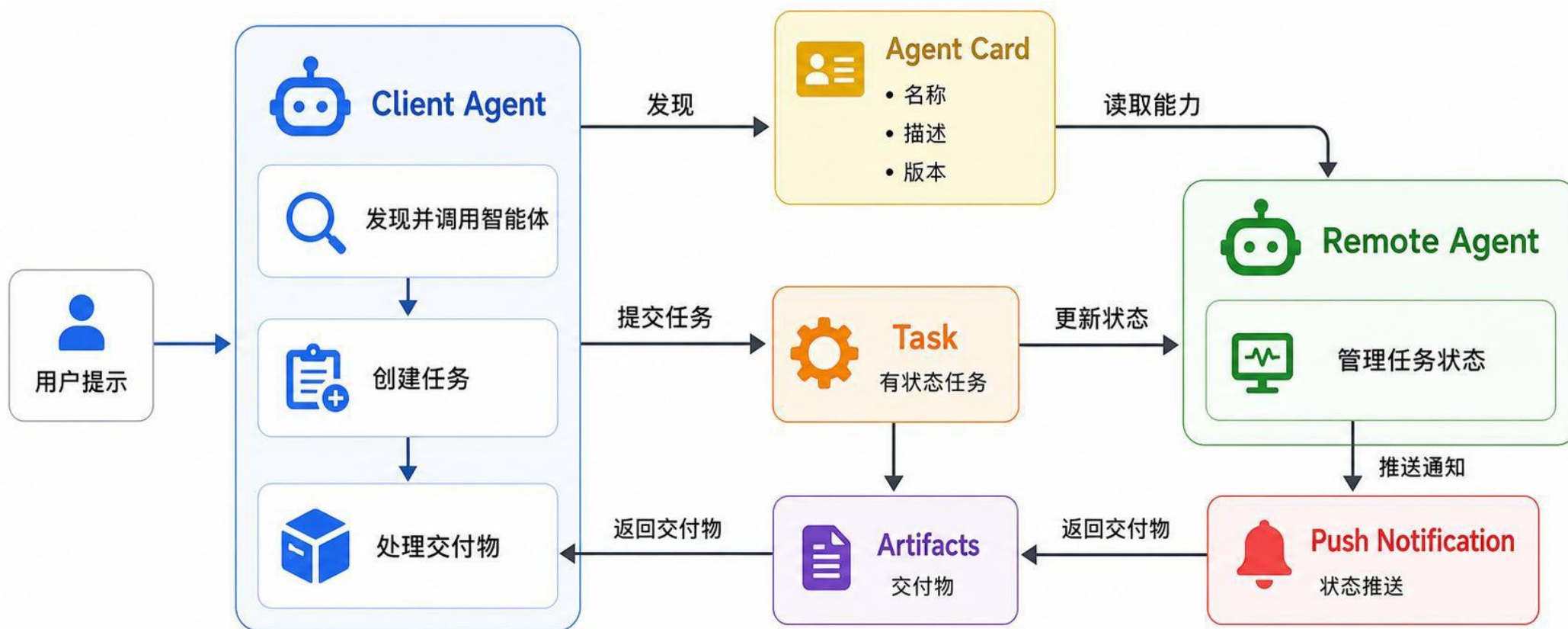
A2A：智能体连接智能体

A2A协议（Agent to Agent Protocol）关注的是不同智能体之间的互操作，让一个智能体能够发现、理解并委托另一个智能体完成任务。它主要解决跨厂商、跨框架、跨组织的协作问题，使各类专业智能体能够在统一协议下安全通信、共享任务状态并交换交付结果，而无需暴露各自内部的模型、工具或业务实现。



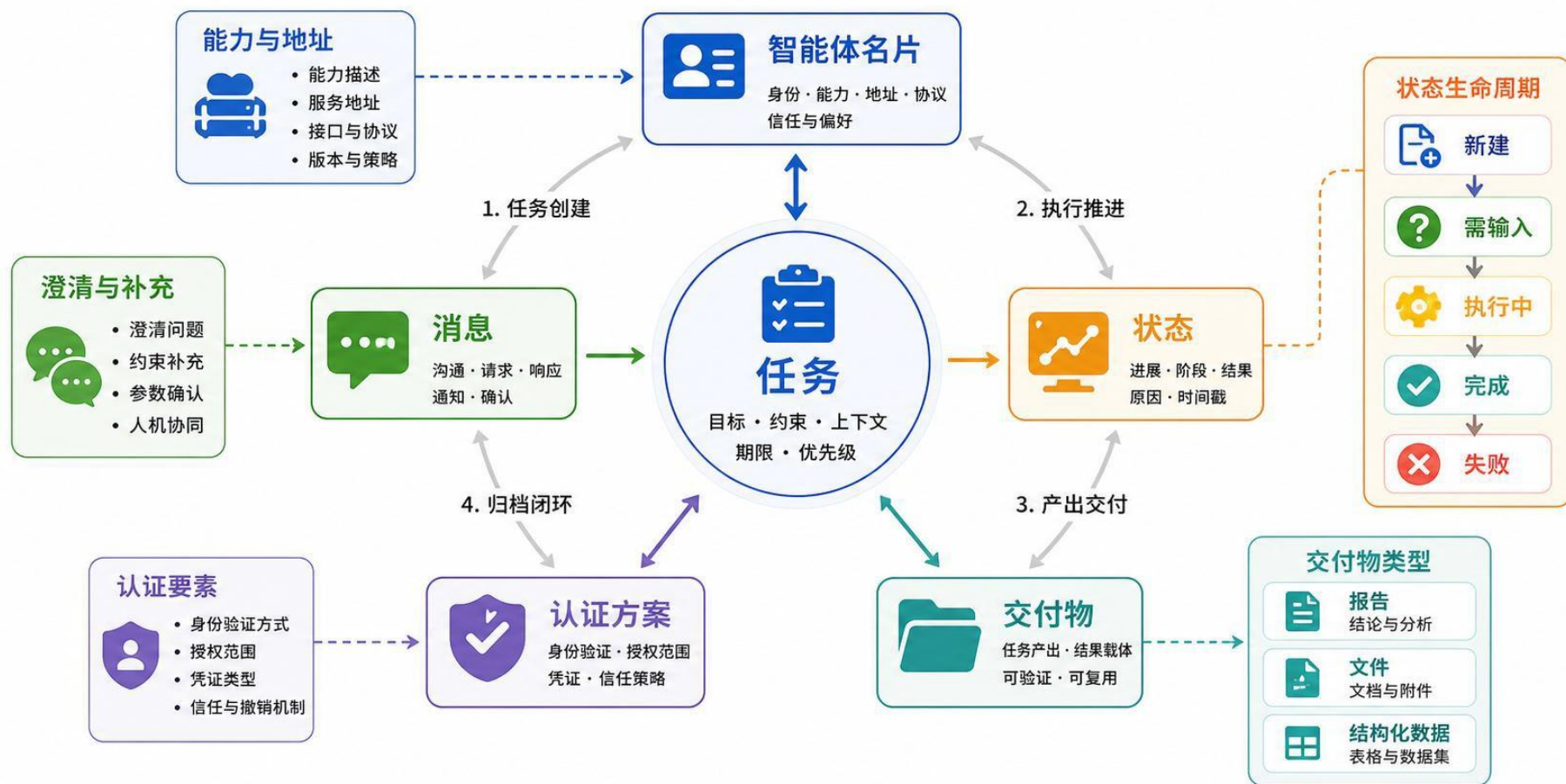
A2A 交互流程

A2A采用“发现-委托-协作-交付”的通信模式。Client Agent首先发现Remote Agent公开的Agent Card，了解其能力、服务地址、认证要求和交互方式，然后向其发起任务请求。在任务执行过程中，双方持续交换消息、同步任务状态，并最终返回交付物。



A2A 的核心对象

A2A中的关键对象包括智能体名片、任务、消息、状态、交付物和认证方案。智能体名片用于说明“我是谁、我能做什么、如何访问我”。任务用于承载目标和执行过程，消息用于多轮沟通，交付物用于返回结构化结果。状态更新让长任务可追踪，认证方案让协作有安全边界。



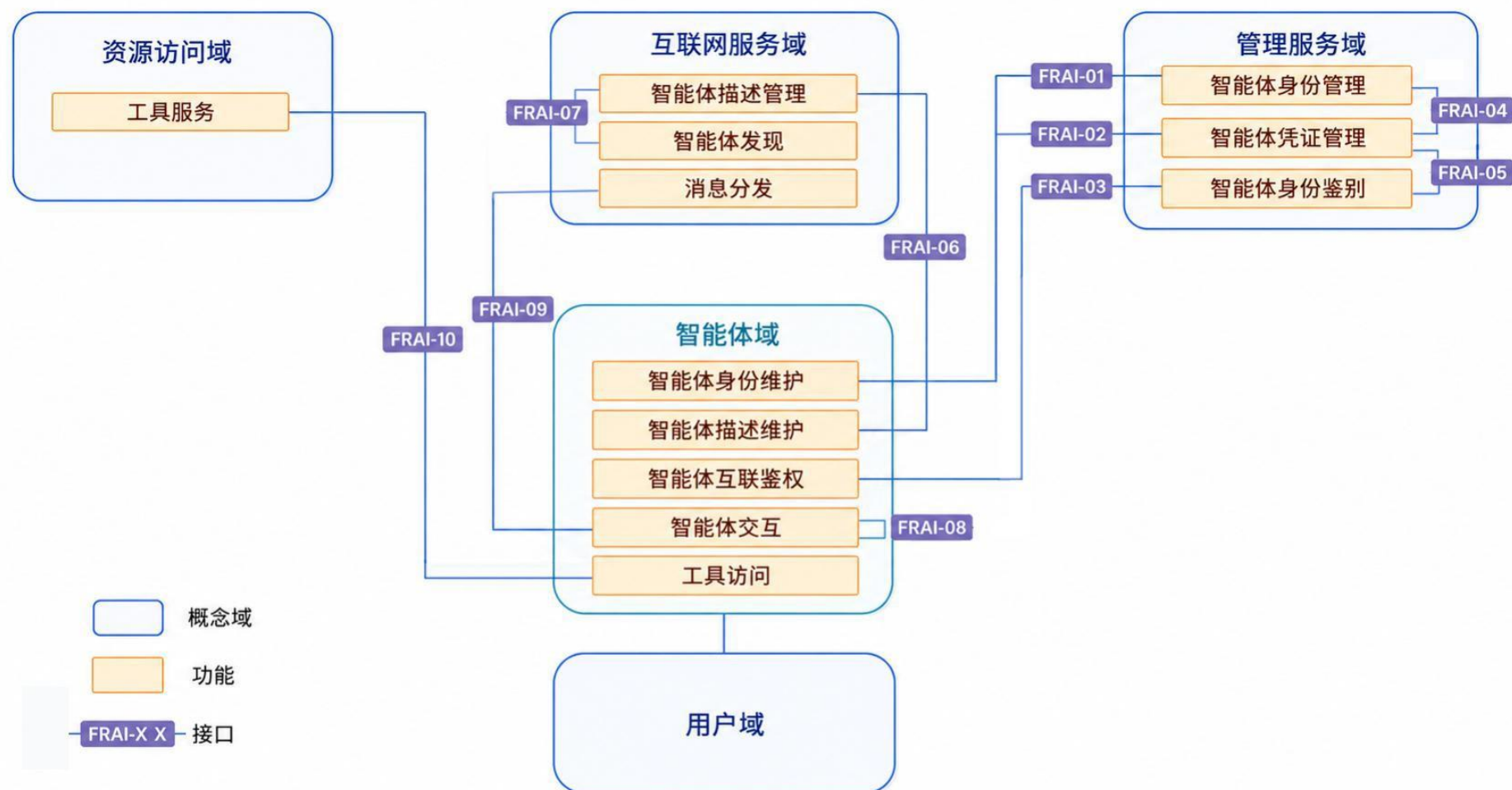
MCP与A2A的关系

MCP和A2A并不是竞争关系，而是面向不同层次的标准协议。MCP解决的是智能体如何安全地连接工具、数据和外部服务；A2A解决的是智能体之间如何发现彼此、委托任务并协同工作。在实际应用中，智能体通常先通过A2A将任务分发给专业智能体，再由各专业智能体通过MCP调用本地工具、访问数据和执行具体操作。两者组合才能让智能体既有执行能力，又能参与多智能体协作。



AIP： 标准化智能体互联协议

AIP（Agent Interconnection Protocol）是国内智能体互联标准化体系中的重要协议方向，由工信部、国家市场监督管理总局、中国电子技术标准化研究院等推进，其核心定位是为智能体互联提供通用交互规则。AIP整体采用“身份-描述-发现-交互-工具调用”闭环链路，涵盖可信接入、能力自动匹配、同步/异步交互及行为审计等机制，支持点对点、群组及跨域互联。



ANP： 面向开放的智能体网络协议

ANP（Agent Network Protocol）由ANP开源技术社区等国内团队主导，定位于开放网络中的智能体身份、发现、通信与协商机制。其技术路线强调兼容现有互联网基础设施，并通过身份与加密通信层、元协议协商层、应用协议层等分层设计，支持陌生智能体在跨组织、跨域名、跨信任体系中发现彼此、验证身份并协商交互方式。



说明： ANP 面向开放网络中的智能体互联，支撑身份识别、加密通信、协议协商与应用交互。

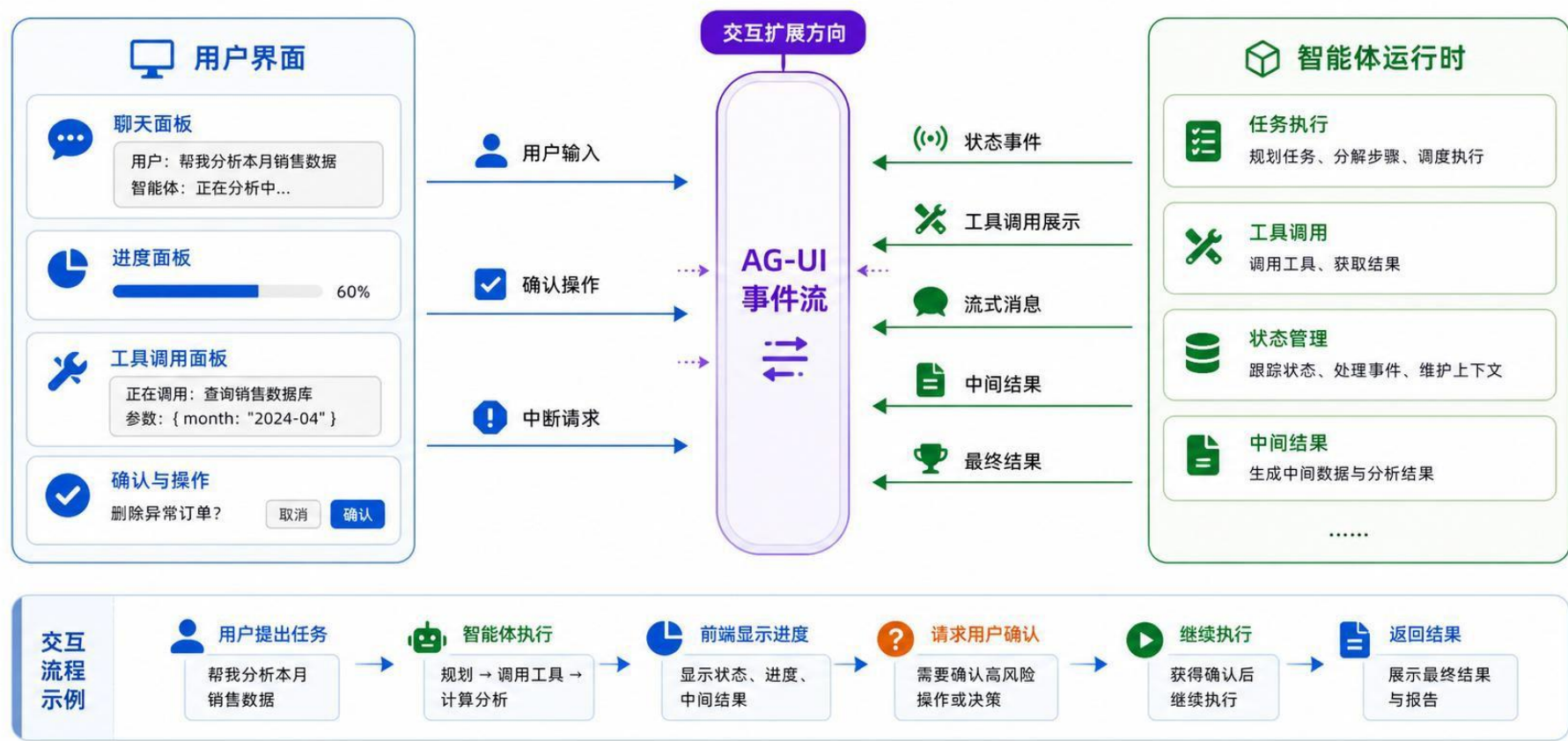
AP2、x402：支付与交易协议

当智能体可以替人购买商品、订阅服务、采购资源时，支付与交易协议会变得重要。交易系统需要确认用户真实意图、智能体授权范围、交易金额、履约结果和可追责记录。AP2、x402 等方向体现了智能体交易支付的探索，让智能体可以在规则约束下发起和完成交易。目前这一方向还没有完全成熟的标准，更适合定位为智能体商业闭环的关键探索。



AG-UI：智能体与用户界面交互协议

AG-UI（Agent-User Interaction Protocol）是CopilotKit团队发起并开源的协议，主要是为了解决智能体与前端应用之间的交互标准化问题，通过定义统一的事件类型、传输规则与适配层工具，让智能体的行为能被前端读懂，前端的操作能被智能体响应，最终实现智能体处理过程可见、用户干预实时生效、多端状态无缝同步的协作效果。



AG-UI 是前端与智能体运行时之间的事件协议，标准化 UI 更新与用户交互，不涉及工具接入与智能体间协作。

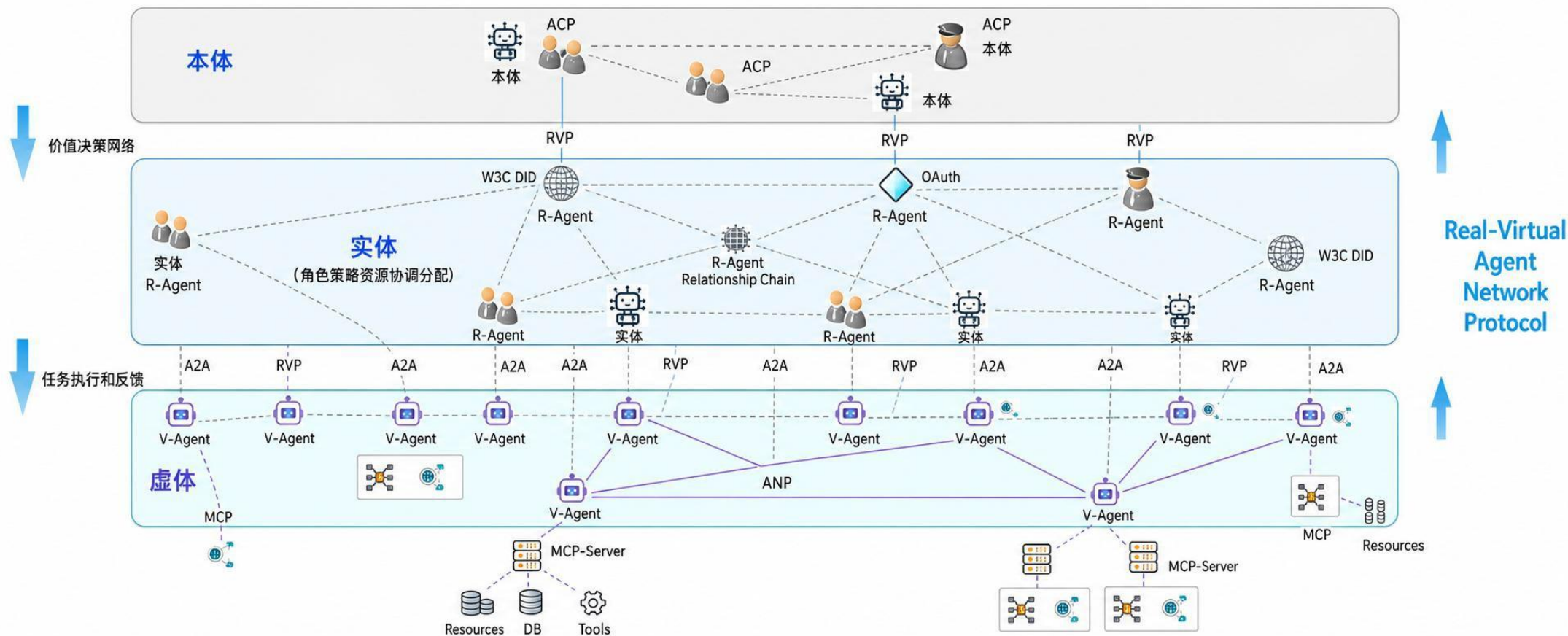
A2UI：智能体生成式界面协议

A2UI（Agent-to-UI Protocol）由谷歌提出，主要解决智能体如何描述和生成用户界面的问题。与传统返回文本不同，A2UI允许智能体直接输出按钮、表单、图表、地图、日历等结构化界面描述，由客户端自动渲染成本地原生UI，使智能体不仅能够回答问题，还能够动态生成可交互的应用界面。



RVP: 虚实融合智能体通信协议

RVP (Real-Virtual Agents Network Protocol) 是中国首个面向虚实融合场景的智能体通信协议。它通过统一复合身份管理和基于物理/社会/生产关系图谱的协调机制，实现机器人、IoT设备等物理实体与AI系统、数字孪生等数字智能体之间的无缝协同。RVP支持非对等型并局部中心化的异构通信，可同时调度数千个物理智能体并允许它们自主协同。



目录

01  智能体互联网的发展背景

02  智能体互联网的产业生态

03  智能体互联网的基础架构

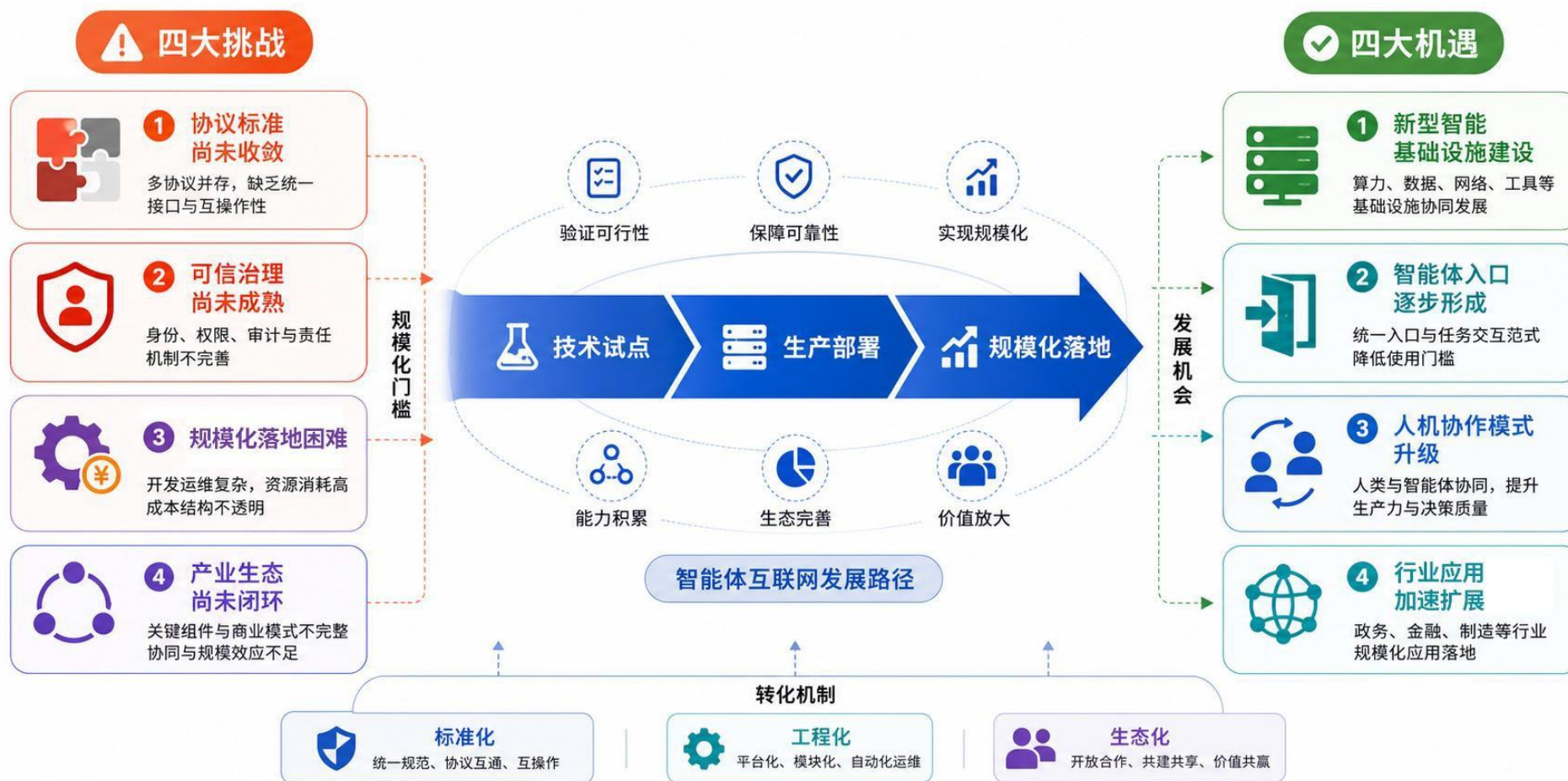
04  智能体互联网的关键协议

05  挑战与机遇

06  总结与展望

智能体互联网走向规模化的挑战与机遇

当智能体逐步从单点工具调用迈向跨系统协作，对可信身份、权限管控、协议互通、任务稳定运行及服务闭环提出了综合要求。当前行业仍面临协议标准异构、可信治理缺失、规模化落地困难、生态碎片化等现实难题。但随着统一标准逐步建立、智能基础设施不断夯实，加之新应用形态、商业路径与协作网络的发展，也为行业带来了广阔机遇。



挑战一： 协议标准尚未收敛

智能体互联网的前提是不同智能体能互相理解、互相发现、互相协作。当前MCP、A2A、ANP、ACP、平台私有接口等多条路线并存有助于技术探索，但也会带来协议选择、接口适配、版本兼容、身份打通和跨平台协同成本。短期内，智能体互联网更可能呈现多协议组合格局，而不是由单一协议覆盖所有场景。



面临挑战

协议选择

协议众多，选型困难

接口适配

接口差异大，适配成本高

版本演进

版本不一致，兼容压力大

跨平台互联

生态割裂，互联门槛高

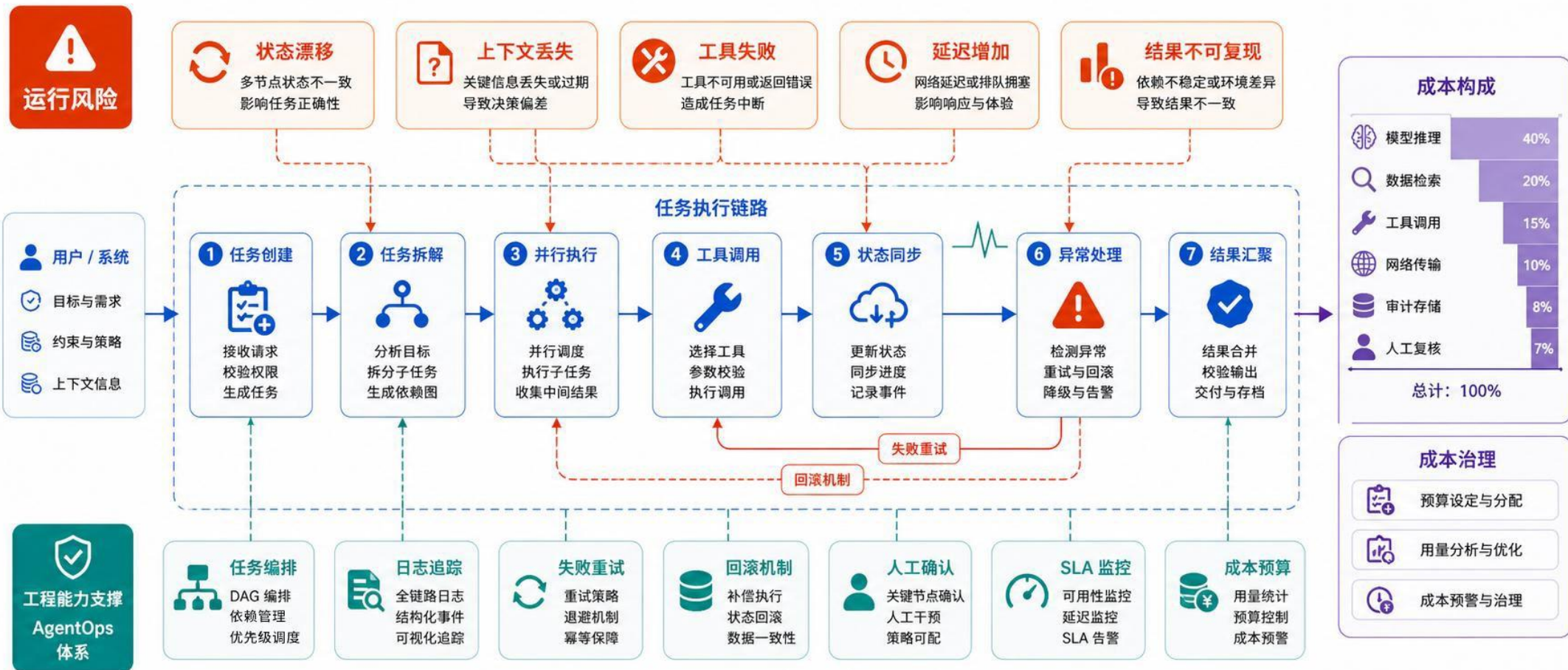
挑战二：可信治理尚未成熟

智能体互联网中的安全风险、身份授权和责任边界高度耦合。智能体可能代表用户、企业或设备调用工具、访问数据、提交请求和执行操作，因此治理对象不再只是模型输出，还包括身份真实性、授权范围、凭证有效性、工具调用边界、敏感操作控制和行为追溯。提示注入、数据泄露、身份冒用、越权调用、工具链污染和责任断链，都需要通过统一的可信治理机制进行约束。



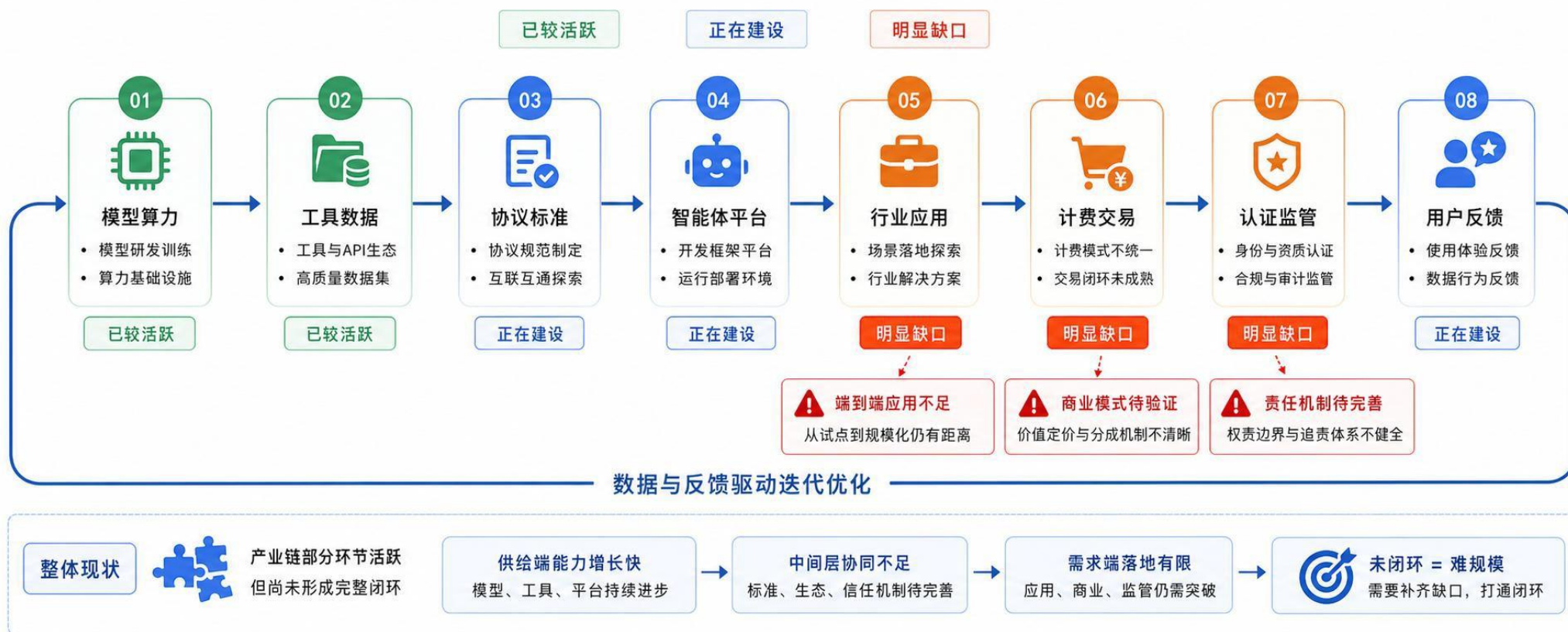
挑战三： 规模化落地困难

智能体互联网面向多智能体、多工具、多步骤的长链路协作。任务执行过程中可能出现上下文丢失、状态漂移、工具异常、结果不可复现、延迟上升和成本波动等问题。随着智能体调用模型、检索数据、访问工具、传输消息和生成审计记录，成本也会从单一推理成本扩展为推理、检索、工具、网络、存储、人工复核和运维监控的综合成本。规模化落地需要更成熟的 AgentOps、状态管理、异常恢复、性能监控和成本治理体系。



挑战四： 产业生态尚未闭环

当前智能体互联网概念热度高，但产业闭环仍不成熟。上游有模型、算力、数据、工具和协议，中游有智能体平台、开发框架、身份授权和安全审计，下游需要行业场景、服务市场、计费模式和监管规则。但目前端到端应用还没大规模爆发，多停留在演示、试点或单点工具阶段。商业闭环也尚未完全清晰，产业生态成熟需要标准、平台、开发者、行业客户、监管和资本共同推进。



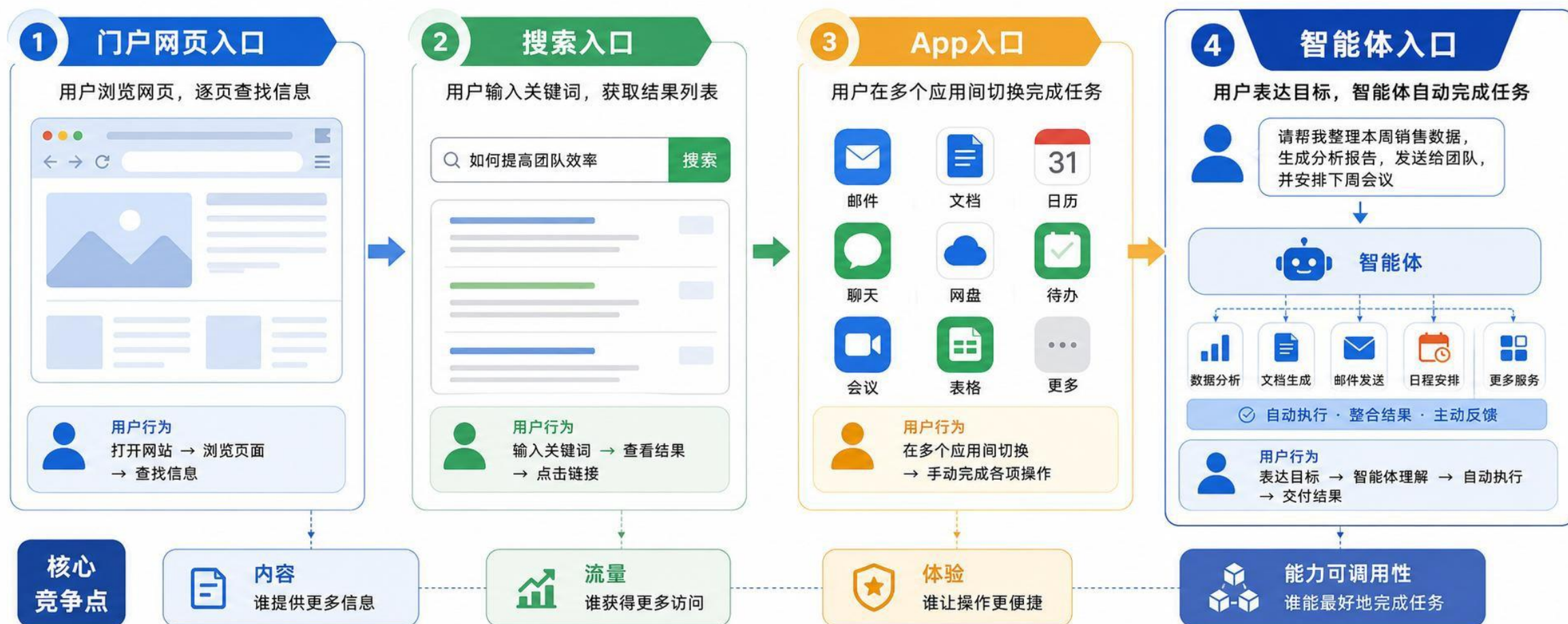
机遇一：催生新型智能基础设施

智能体互联网会推动软硬件基础设施升级。硬件侧包括 AI 算力集群、边缘计算节点、智能终端、机器人、传感器、工业设备和虚实融合网关；网络侧需要低时延、高可靠、可观测的连接能力；软件侧包括智能体运行平台、协议网关、工具调用平台、身份认证、AgentOps、安全审计和成本治理系统。这些基础设施共同支撑智能体的发现、协作、执行和治理。



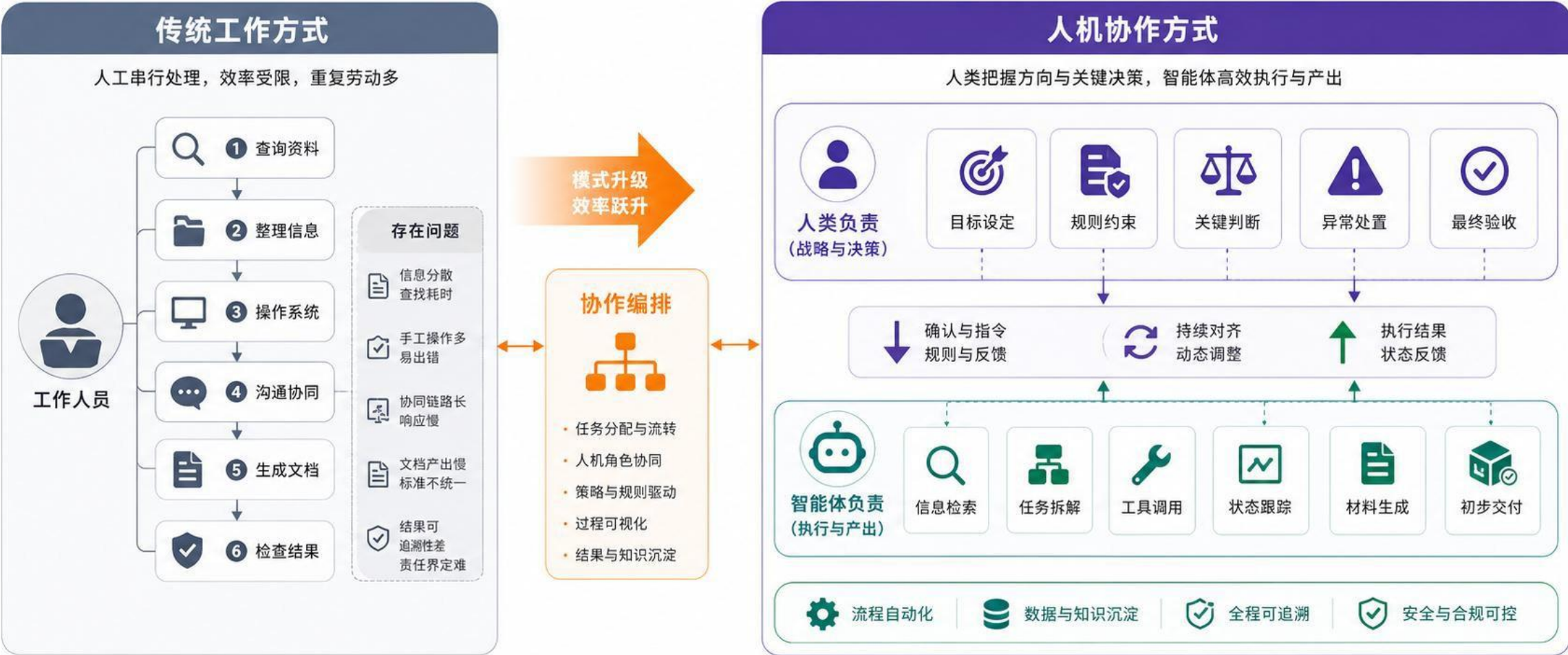
机遇二：智能体入口逐步形成

智能体互联网可能带来新的入口形态，用户不再先打开某个应用，而是直接表达目标，让智能体选择服务、组合能力、完成任务。这会改变搜索、应用分发、软件界面、服务定价和平台生态。与此同时，商业模式也迎来重构，多元计费与生态合作模式不断兴起，形成“入口 - 产品 - 商业”联动发展的良好态势。



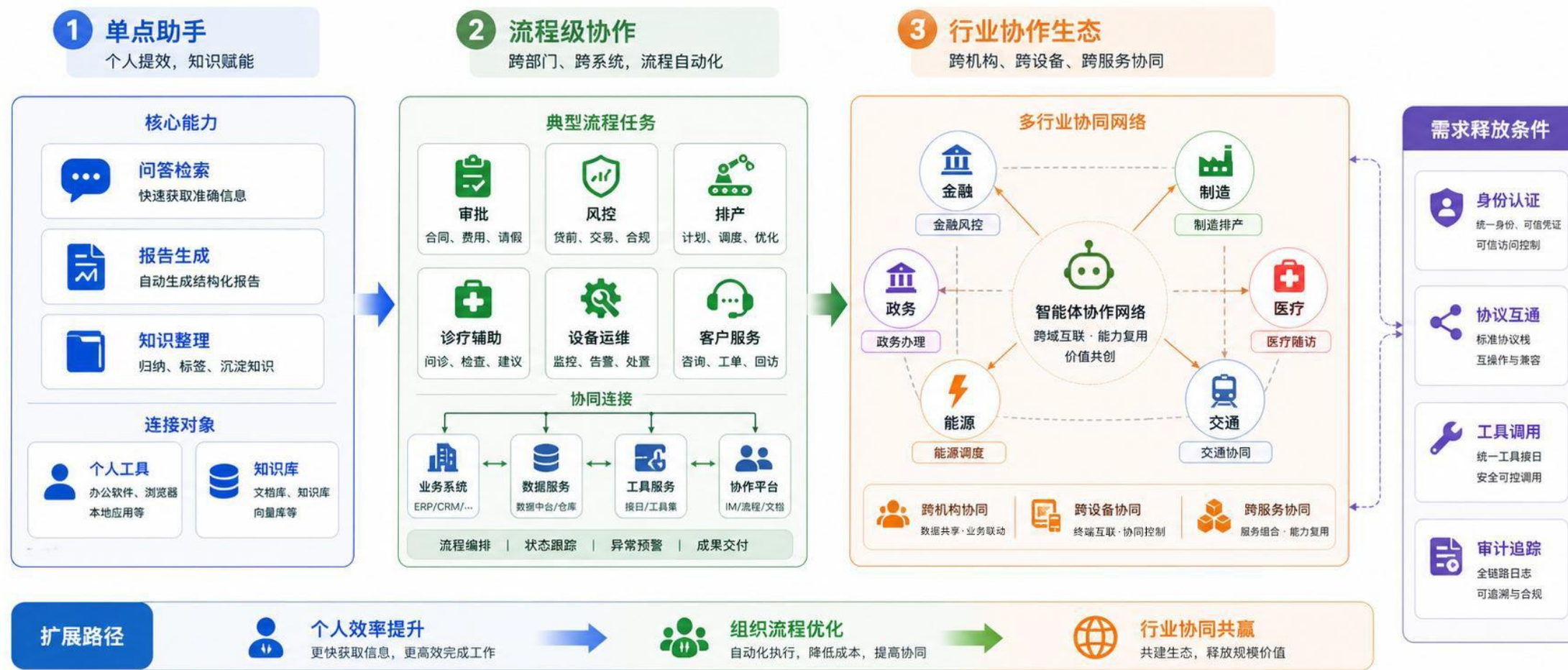
机遇三： 人机协作模式升级

智能体并不是简单替代人工，而是改变人与系统的协作方式。人类更适合负责目标设定、约束确认、关键判断、异常处置和最终验收；智能体则承担信息检索、任务拆解、工具调用、状态跟踪、材料生成和初步交付。这将重塑企业组织形态，催生一人公司、轻量化团队等新模式，大幅降低运营成本、提升组织灵活性，推动产业从人力驱动向智能驱动跃迁。



机遇四：行业应用加速扩展

智能体互联网适合多系统、多角色、多流程协作的行业场景。金融、制造、政务、医疗、交通等领域都存在跨部门、跨机构、跨设备的数据流转和任务协同需求。随着身份认证、能力描述、协议互通、工具调用和审计追踪机制逐步成熟，行业应用有望从单点助手扩展到流程级协作，再进一步形成面向供应链、产业链和公共服务网络的智能体协作生态。



目录

01  智能体互联网的发展背景

02  智能体互联网的产业生态

03  智能体互联网的基础架构

04  智能体互联网的关键协议

05  挑战与机遇

06  总结与展望

发展历程：从“信息互联”跃迁到“智能体互联”

互联网发展经历了从“连接信息”到“连接人”再到“连接智能体”的三次根本性跃迁。每一次跃迁都伴随着连接主体的扩展、交互范式的革新和价值创造模式的重塑，当前我们正处于第三次跃迁的起点，**网络使命从“人与人的沟通”升级为“智能体间的互联”**。



未来展望：人智协同、虚实共生的新纪元



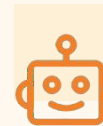
产业端：全链路协同

打破传统分散式系统壁垒，智能体集群深度嵌入供应链与经营决策流程。从生产制造到流通管理，实现全链路的智能化协同与资源最优配置，推动产业效率实现结构性跃升。



治理端：智能联动赋能

打通跨部门、跨领域的数据与服务壁垒，构建智能体联动治理网络。实现城市运行的实时感知、自动响应与前瞻预判，让公共服务更精准、城市管理更高效、社会治理更精细。



个人端：个人专属智能体

专属个人智能体成为数字世界的常驻角色，自主处理信息筛选、事务办理、社交协作等数字事务。释放用户的时间与精力，构建起人智协同、虚实共生的全新生活与工作方式。

智能体互联网将推动互联网从“信息互联”向“**智能互联、价值互联、生产力互联**”跃迁，从根本上重塑数字经济的底层逻辑。这一变革既为人工智能产业的爆发式增长和数字社会的稳健建设提供了关键底座，也构筑起万物智联、自主协同、价值共创的未来生态，有望进一步释放社会生产力，广泛改变大众的日常生活图景。