

# 智能体接口化白皮书 2.0

智能体的未来，不在于模型的参数大小，而在于接口的标准化程度。

东莞市意图共鸣科技有限公司

2026年9月

## ■ 文档信息

| 项目   | 内容                                  |
|------|-------------------------------------|
| 类型   | 白皮书                                 |
| 核心主张 | 智能体的未来，不在于模型的参数大小，而在于接口的标准化程度。      |
| 发布机构 | 东莞市意图共鸣科技有限公司                       |
| 作者   | 意图共鸣科技                              |
| 系列   | 智能体白皮书系列 · 2.0                      |
| 版本   | 2.0                                 |
| 发布日期 | 2026年9月1日                           |
| 文档编号 | —                                   |
| 联系方式 | contact@xinirp.com   www.xinirp.com |

© 2026 东莞市意图共鸣科技有限公司. 保留所有权利。

# ■ 目录

引言 ..... 4

第一章 三个时代，三种组装 ..... 4

第二章 三角模型的接口化展开 ..... 5

第三章 接口化的三个层次 ..... 6

第四章 记忆接口：智能体演进的新维度 ..... 7

第五章 从三脚架到四面体 ..... 8

第六章 接口是AI拥抱人的关键一步 ..... 9

## 引言

接口是产业分工的前提。

硬件时代，USB定义了即插即用——不懂电路的人也能组装电脑。软件时代，API定义了即插即用——不懂编程的人也能使用应用。每一次接口的标准化，都带来一次产业分工的深化。标准化让复杂度后置，让创造力前置。

AI时代，智能体的能力模块，同样需要一种标准化的连接方式。

《智能体三角模型》白皮书定义了智能体的构造范式——通用认知基座、人文交互内核、私有知识域，三个顶点缺一不可。本白皮书回答下一个问题：三个构造顶点如何被连接、被组装、被交付到各行各业？

答案是：接口化。

2026年，接口化的基础设施已经就位。在HTTP和API构建的通用底座之上，MCP（模型上下文协议）为AI定义了标准化的工具调用方式，被业界称为“AI的USB-C接口”。与此同时，围绕智能体互联的标准化工作，正在从身份、描述、发现、交互到工具调用形成完整的规范体系。

时机已经成熟。本白皮书将三角模型的三个构造顶点分别接口化为大模型接口、规则接口、知识接口，并新增行业接口连接具体商业场景，由此形成四条标准接口；并提出一种全新的智能体构建方式：像组装电脑一样，组装智能体。

这不是一个技术升级。这是一次产业范式的跃迁。

## 第一章 三个时代，三种组装

理解智能体接口化的意义，需要先理解一个更大的历史脉络。

### 1.1 硬件时代：组装电脑

核心逻辑：**插**。

CPU插主板，内存插槽位，显卡插PCIe。消费者不需要懂晶体管原理，只需要把标准件插在一起，通电，电脑就活了。

这个时代的伟大之处在于：标准接口让复杂度后置，让创造力前置。USB、PCIe、HDMI——这些接口标准定义了硬件的“即插即用”时代。任何厂商只要遵循接口规范，就能让自己的产品进入全球市场。

硬件时代的核心启示是：**标准接口是产业分工的前提**。

没有统一的插槽标准，就没有兼容机市场；没有USB标准，就没有外设产业的繁荣。

### 1.2 软件时代：安装应用

核心逻辑：**装**。

操作系统之上，万千App随意安装。地图、支付、社交，各自解决一个细分场景。用户不需要懂编程，只需要点“下载-安装”，手机就无所不能。

这个时代的伟大之处在于：API接口让服务解耦，让生态爆炸。RESTful API、SDK、云服务——这些接口标准定义了软件的“即插即用”时代。任何开发者只要遵循API规范，就能让自己的服务被全球调用。

软件时代的核心启示是：**API是能力交付的最小单元。**

一个支付接口可以被一万个应用调用，一个地图接口可以被十万个网站嵌入。

1.3 AI时代：拼接智能

核心逻辑：**接。**

大模型不是应用，它是“大脑的CPU”。它足够聪明，但它天然不带有任何行业的“规矩”和“记忆”。就像一块刚出厂的高性能CPU，插在板子上能跑分，但不懂医药、不懂金融、不懂怎么跟客户说话。

AI时代的伟大之处，正在被定义：**把行业规则、专属知识、业务动态，全部做成标准“认知接口”，让大模型像插U盘一样即插即用。**

这个时代的基础设施正在快速就位。在HTTP和API构建的通用底座之上，**MCP（模型上下文协议）**为AI定义了标准化的工具调用方式，被业界称为“AI的USB-C接口”。与此同时，围绕智能体互联的标准化工作，正在从身份、描述、发现、交互到工具调用形成完整的规范体系。

**接口化的基础设施，已经就位。**

第二章 三角模型的接口化展开

《智能体三角模型》白皮书提出了三个构造顶点：

| 构造顶点   | 对应能力 | 本质           |
|--------|------|--------------|
| 通用认知基座 | 思考能力 | 大脑——理解、推理、生成 |
| 人文交互内核 | 行为分寸 | 教养——边界、规则、温度 |
| 私有知识域  | 业务灵魂 | 专业——行业专属知识   |

这三个顶点，各自对应一类可被“接口化”的认知组件。

2.1 通用认知基座 → 大模型接口

已有成熟供给。大模型厂商提供标准的模型调用接口，智能体按需调用。这一层的接口化已经完成，行业共识已经形成。

2.2 人文交互内核 → 规则接口

这是接口化生态中最关键、也最容易被忽视的一环。

行业合规、话术边界、情绪响应逻辑——这些“分寸感”长期以来被当作提示词或安全护栏来处理，缺乏独立、标准化的交付形态。规则接口的出现，正是为了将“人文交互”从一个理念层面的概念，转化为一个可分发、可审计、可迭代的独立组件。

规则接口的核心机制是：智能体传入业务场景描述，接口自动匹配并返回对应的交互规则组合，智能体据此理解和执行。它不是一次性的配置，而是伴随智能体整个生命周期的持续约束。

## 2.3 私有知识域 → 知识接口

商家自主封装。产品手册、服务流程、常见问答等专属知识，通过标准化的检索接口供智能体按需获取。知识从静态的文档，变成了动态的服务。

## 2.4 接口的实现方式

接口化是一个架构范式，而非某一具体技术的代名词。能力模块可通过MCP、API等标准协议实现接口化，具体选择取决于场景。一个认知组件可同时提供多种形态，在通用性与生态互操作性之间取得平衡。接口化的本质在于能力是否被封装为独立、可调用的接口形态，而非绑定于某种特定协议。

## 2.5 接口化的四个特征

接口化的核心，是把能力模块封装为具备四个特征的标准组件：

**独立性：**组件可独立开发、部署、升级，不依赖其他组件的内部实现。大模型换一家厂商，规则接口不受影响——这是接口化最基础的特性。

**可发现性：**组件通过标准描述被外部识别和调用。规则接口通过merchant\_role的语义匹配，让调用方无需预知规则内容，只需描述自己的行业身份即可获得对应的规则组合。

**可替换性：**同一位置的组件可被同标准接口的其他实现替换。今天用规则接口，明天如果行业协会有更好的规则包，切换API地址即可，调用方内部逻辑无需修改。

**可组合性：**多个组件可通过标准总线组装为完整系统。规则接口 + 大模型接口 + 知识接口 + 行业接口，共同组成一个完整的商用智能体。

这四个特征共同定义了“接口化”——不是“提供一个API”，而是把能力模块封装为标准组件，让它们可以被自由组合、替换和迁移。

## 2.6 核心公式

**可商用智能体 = 大模型接口 + 规则接口 + 知识接口 + 行业接口**

（通过标准化协议进行总线调度）

这就是三角模型的工程展开：三个构造顶点，四条标准接口。认知、规则、知识构成了能力底座，行业接口决定了智能体为谁服务、适配什么场景、拥有哪些工具。**行业接口是核心连接点——它把三个通用能力支柱和具体的商业场景连接在一起，同时配置该行业所需的专业工具。**

## 第三章 接口化的三个层次

接口化不是单一的技术选择，而是一个三层递进的产业范式。

### 3.1 第一层：连接（Connect）

让智能体能“调用”外部能力。

这是最基础的层次。大模型通过标准化接口调用工具、检索知识、执行操作。当前行业已普遍到达这一层。在这一层，HTTP API是最基础的连接方式，MCP是连接的标准化升级。

连接的完成，解决了“智能体不再是一个孤岛”的问题。但连接本身只是起点——它让智能体“看到”了外部能力，但还没有解决“如何组合这些能力完成复杂任务”的问题。

### 3.2 第二层：组装（Assemble）

让智能体能“组合”多个能力模块。

连接解决了“单个调用”的问题，组装解决的是“协同工作”的问题。一个完整的商用智能体，需要同时具备思考能力（大模型接口）、行为分寸（规则接口）、业务知识（知识接口）、行业适配（行业接口，含该行业所需的专业工具配置）。这些模块如何被编排、调度、协同？

这正是三角模型接口化所要回答的核心问题。通过标准化的接口定义和总线调度机制，不同来源、不同功能的认知组件可以被“组装”成一个完整的智能体——就像装机一样，选CPU、选内存、选显卡，插上就能用。

组装的关键在于：**每个组件都是独立封装的，替换或升级任何一个组件，不影响其他组件的运转。**

### 3.3 第三层：生态（Ecosystem）

让智能体能“发现”和“交易”能力模块。

这是接口化的终极形态。当认知组件足够多、接口足够标准时，一个“组件交易市场”就会出现。商家不仅是智能体的“使用者”，更是“创造者”。一家美容院老板可以把自己的“术后回访话术规则”封装成一个规则接口上架；另一家美容院直接订阅使用。开发者可以专门为某个细分行业编写“规则包”或“知识包”，通过持续的订阅获得收入。

行业中已经出现这一方向的探索——谷歌发起的Agent2Agent（A2A）协议以“Agent Card + 目录”支撑智能体的发现与互操作，AGENTS.md则为智能体的行为描述提供了规范。这些“目录”与“注册表”式架构，本质上就是在搭建一个“能力组件”的发现与交易基础设施。接口化的第三层，正在从构想走向现实。

## 第四章 记忆接口：智能体演进的新维度

接口化不仅要解决“连接”的问题，还要解决“记忆”的问题。

一个能调用外部工具的智能体，依然只是一个功能强大的工具。真正的智能体，应该能够随着与用户的长期互动而成长——记住用户的偏好、延续对话的脉络、继承积累的知识。

但当前行业存在一个被忽视的困境：用户的AI记忆无法迁移。如果你从一家AI平台换到另一家，想带走和AI长期积累的记忆——那些聊过的项目、反复敲定的方案、AI越来越了解你的那些偏好——带不走。不是技术做不到，而是没有一种通用的方式让记忆可以被打包和迁移。

### 4.1 记忆需要一种通用的封装方式

海运行业的经验值得借鉴：不管货物是什么，装进集装箱就行。箱子规格全世界统一，船、码头、卡车都按同一个标准运转。

AI记忆也一样。我们将这种标准化的数字封装，称为“**记忆胶囊**”。

一个合格的记忆胶囊，至少需要满足三个条件：**内容可读**——能被不同平台解析；**隐私可控**——端侧加密，密钥只属于用户；**来源可溯**——可验证真实性和完整性。

## 4.2 记忆链协议（Memory Chain Protocol, MCP）：一个开放方向

2026年5月，意图共鸣科技发起**记忆链协议（Memory Chain Protocol, MCP）**的开放讨论，旨在为AI记忆探索一种通用的数据组织方式。

这不是某家公司的私有方案，而是一个希望行业共同参与的起点。我们把这个方向称为“**记忆共识**”——它不需要签署，只需要足够多的参与者认同这个方向，并付诸行动。

## 4.3 两个MCP的互补

在智能体接口化的图景中，存在两个缩写同为MCP的协议，服务于不同层面：

**模型上下文协议（Model Context Protocol, MCP）**：由海外大厂发起、已移交Linux基金会成为行业标准的协议，为AI定义标准化的工具调用方式。它解决的是“连接”问题——让智能体实时调用外部工具。

**记忆链协议（Memory Chain Protocol, MCP）**：意图共鸣科技于2026年5月发起的开放协议方向，解决AI长期记忆的存储与迁移问题。它解决的是“沉淀”问题——让智能体越用越懂用户。

两者缩写相同，但**名称不同、协议层级不同、解决的问题不同**。在智能体接口化图景中，两者互补而非冲突：模型上下文协议负责“实时连接外部工具”，记忆链协议负责“长期沉淀用户记忆”。一个让智能体变得**能干**，一个让智能体变得**懂你**。

两者结合，智能体才真正从一个用完即走的工具，变成一个越用越贴合用户需求的专属服务角色。

## 第五章 从三脚架到四面体

**先说明一次演进**。《智能体三角模型》1.0在提出“三脚架”隐喻时曾明确表示：不把它称为“四脚模型”，因为行业触地点是三个顶点共同指向、共同支撑的汇聚成果，而非与前三者平等的固有构造维度。1.0回答的是“智能体由什么构成”——这是构造问题，三足成立即可。本白皮书在接口化视角下对“触地点”做了一次有意重构：当三个能力支柱通过标准化接口与具体行业对接时，行业场景不再只是汇聚的产物，而成为一个可独立配置、可切换的接口维度——即四面体的第四个顶点。**1.0描述的是构造，2.0描述的是组装；构造是三足的，组装是四面的。**

《智能体三角模型》白皮书用“三脚架”作为核心隐喻——三只脚（认知、人文、知识）撑起一个服务交付点。这个隐喻简单、直观、好传播。

但三脚架是静态的。当它真正落地到具体行业时，它的完整形态是**四面体**。

**底面三顶点**：通用认知基座、人文交互内核、私有知识域——这三个能力支柱固定不变。

**第四个顶点**：具体的行业场景。

当三只脚通过标准化接口连接到具体行业时，那个交汇点就变成了四面体的第四个顶点——**行业专属智能体**。美容行业是一个交点，金融行业是另一个交点。底座相同，交点的位置因行业而异。

同一个三脚架，落在不同的地面上，长出不同的触地点。

在零售行业，服务交付指向库存查询、时段匹配、预约确认。在医疗行业，服务交付指向预问诊收集、智能分诊、挂号预约。在金融行业，服务交付指向身份核验、风险测评、产品匹配。

三只通用之脚始终不变，但触地点因行业而异。三个能力支柱不变，第四个顶点因行业而异——这就是接口化能支撑三百六十行的原因。

## 第六章 接口是AI拥抱人的关键一步

人不需要懂电，才能用电灯。

人不需要懂网络协议，才能上网。

人不需要懂大模型，才能用AI。

人只需要“插上”。

《智能体三角模型》白皮书提出了“让AI拥抱人”的理念——让AI主动理解人的意图、适应人的习惯、尊重人的边界。

接口化，正是这一理念在工程层面的最终落地：

- **认知基座接口化**：让AI随时获得最强的思考能力，而不需要商家自己训练模型
- **人文交互接口化**：让AI随时获得最合适的“分寸感”，而不需要商家自己编写提示词
- **私有知识接口化**：让AI随时获得最准确的业务信息，而不需要商家自己搭建知识系统
- **行业接口化**：让AI随时适配具体的行业场景——美容、金融、医疗、零售——而不需要每个行业从头配置
- **记忆接口化**：让AI随时“记得”用户是谁、偏好什么、聊过什么

接口化的本质是：**把复杂度留给生态，把简单留给商家。**

硬件时代，USB让不懂电路的人也能组装电脑。

软件时代，API让不懂编程的人也能使用应用。

AI时代，认知接口让不懂算法的人也能拥有专属智能体。

这是接口的使命，也是AI拥抱人的关键一步。

### 附录：核心语义词

#### 接口化

将智能体的能力模块（认知、规则、知识、记忆、行业）封装为标准化、可独立调用、可跨平台迁移的接口形态。这是一个架构范式，而非某一具体技术的代名词。

#### 认知组件

构成智能体能力的独立模块，包括大模型接口、规则接口、知识接口、记忆接口、行业接口等。每个组件可独立开发、部署、升级和替换。

#### 行业接口

将具体行业的身份、规则、知识和工具需求封装为标准化的配置接口。行业接口是四面体的第四个顶点——它决定了智能体属于哪个行业、遵守什么规则、使用什么工具。不同行业通过切换行业接口配置，即可将同一套能力底座适配到完全不同的商业场景。

### 组件组装

将多个独立的认知组件通过标准化协议组合成一个完整的商用智能体的过程。类比硬件时代的装机——选件、插接、通电。

### 组件市场

接口化第三层的产物。当认知组件足够多、接口足够标准时，组件交易市场自然形成。提供方上架组件，使用方按需订阅或购买。

### 记忆胶囊

将AI记忆（对话记录、偏好设定、项目脉络等）封装为标准化的数字格式。记忆胶囊的规格由行业共识形成，用户可以在不同AI平台之间自由迁移自己的记忆。

### PnP（即插即用）

认知组件无需复杂配置即可被智能体识别和使用的特性。当接口足够标准、组件足够规范时，接入成本趋近于零。

### 关于本白皮书

本白皮书是《智能体三角模型》的续篇。1.0定义了智能体的构造范式，2.0定义了智能体的组装生态。两者共同构成意图共鸣科技对商用AI智能体从“个体构建”到“群体协同”的完整思考。

本白皮书融合了意图共鸣科技于2026年5月发起的**记忆链协议（Memory Chain Protocol, MCP）**开放倡议，将“记忆接口”纳入接口化范式，形成从“能力连接”到“记忆沉淀”的完整闭环。

© 2026 东莞市意图共鸣科技有限公司. 保留所有权利。

学术研究、媒体报道可自由引用，须注明出处。如需将所述技术方案用于商业实施，欢迎与我们联系洽谈授权。