

团 体 标 准

T/ISC XXX—2026

智能体互联网 任务编排 OpenClaw 类多智能体协同平台能力要求

Task Orchestration for OpenClaw-Style Multi-Agent Collaboration Platforms in
the Agentic Internet

（征求意见稿）

2026 – XX – XX 发布

2026 – XX – XX 实施

中 国 互 联 网 协 会 发 布

目 次

前 言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

 3.1 OpenClaw 类智能体（OpenClaw-Style Agent） 1

 3.2 多智能体协同平台（Multi-Agent Collaboration Platform） 1

 3.3 智能体互联网（Agentic Internet） 1

4 符号和缩略语 1

5 智能体互联网 任务编排 OpenClaw 类多智能体协同平台能力要求框架 2

 5.1 框架模型 2

6 接入管理能力 2

 6.1 身份接入 2

 6.2 能力接入 3

7 任务拆解 3

 7.1 任务分发 3

 7.2 状态追踪 3

8 任务交互 4

 8.1 任务指令交互 4

 8.2 多智能体交互 4

9 协同交付 4

 9.1 交付物汇总 4

 9.2 一致性校验 5

10 安全治理 5

 10.1 权限治理 5

 10.2 监控审计 5

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是面向智能体网关能力的标准。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由云计算开源产业联盟提出并归口。

本文件起草单位：中国信息通信研究院、中国电信集团有限公司、华为技术有限公司、中国电信股份有限公司研究院、中国移动通信集团广西有限公司、中移(苏州)软件技术有限公司

本文件主要起草人：李哲、王向花、王雨宣、崔恩放、马安邦、刘冰、温智聪、张玲艳、宋欣、庞玥、范杰、陶淘

智能体互联网 任务编排 OpenClaw 类多智能体协同平台能力要求

1 范围

本文件规定了智能体互联网中 OpenClaw 类多智能体协同平台的能力要求，包括接入管理、任务拆解、任务交互、协同交付、安全治理等核心能力。

标准旨在规范协同平台对基于OpenClaw（或同类框架）构建的多个智能体进行统一接入、任务编排调度、安全治理的能力，确保多智能体之间高效、安全、可靠地协同完成复杂业务任务。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 41867-2022 信息技术 人工智能 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1 OpenClaw 类智能体（OpenClaw-Style Agent）

是指基于 OpenClaw、MobileClaw、CoPaw 等执行框架或同类架构构建的、具备自主任务执行能力的 AI 智能体。此类智能体的典型技术特征包括：具备自主任务规划与执行能力，可通过工具调用完成具体操作，支持能力声明与标准化协议接入。该分类以技术架构与能力特征为界定依据，不限定特定实现框架或产品形态，以避免出现新的分类方式时产生歧义。

3.2 多智能体协同平台（Multi-Agent Collaboration Platform）

是指能够对多个 OpenClaw 类智能体进行统一接入、任务编排、安全治理的平台系统，是实现多智能体协同完成复杂业务任务的核心枢纽。

3.3 智能体互联网（Agentic Internet）

智能体互联网是基于现有互联网升级改造，以智能体为连接主体，通过网络设施、网络协议创新适配，以实现智能体与工具、智能体与智能体、智能体与人广泛连接、协同工作的下一代互联网，是人工智能时代发展新质生产力的网络基础，是推动实体经济智能化升级的核心引擎。

4 符号和缩略语

下列符号和缩略语适用于本文件。

AI 人工智能（Artificial Intelligence）

API 应用程序编程接口（Application Programming Interface）

- HTTP 超文本传输协议 (Hypertext Transfer Protocol)
- HTTPS 超文本传输安全协议 (Hypertext Transfer Protocol Secure)
- OpenAPI 开放应用程序编程接口规范
- ID 标识符 (Identifier)
- MCP 模型上下文协议 (Model Context Protocol)
- TTL 生存时间 (Time To Live)

5 智能体互联网 任务编排 OpenClaw 类多智能体协同平台能力要求框架

5.1 框架模型

OpenClaw类多智能体协同平台能力要求包括接入管理、任务拆解、任务交互、协同交付、安全治理5个能力模块，如下图1所示。



图 1 智能体互联网 任务编排 OpenClaw 类多智能体协同平台能力框架示意

6 接入管理能力

6.1 身份接入

6.1.1 身份注册

- a) 应支持基于OpenClaw类智能体在接入平台时提交完整元数据信息，包括智能体名称、唯一标识、能力描述、支持协议、通信端点、所属组织等字段；
- b) 应支持信息校验机制，确保注册信息的规范性、完整性与真实性；
- c) 宜支持为每个注册智能体生成平台内唯一的数字身份标识。

6.1.2 生命周期管理

- a) 应支持智能体身份的完整生命周期管理，包括注册、激活、暂停、注销等状态；

- b) 应支持身份状态变更即时生效，例如将某智能体置为“暂停”后立即阻止其参与任何任务；
- c) 宜支持身份状态变更的审计记录。

6.2 能力接入

6.2.1 能力声明

- a) 应支持智能体在接入时声明其具备的能力，包括能力名称、描述、输入输出格式、调用方式、支持的任务类型等；
- b) 应支持能力的结构化描述，如基于JSON Schema或OpenAPI；
- c) 宜支持动态更新能力声明，变更后需重新校验应提供标准化的智能体服务查询接口，支持按关键词精确或模糊查询。

6.2.2 能力校验

- a) 应支持对智能体声明的能力进行有效性校验，包括接口可达性、输入输出格式匹配性；
- b) 宜支持验证声明的能力可正常执行。

7 任务拆解

7.1 任务分发

7.1.1 能力匹配

- a) 应支持以注册表等形式集中查询智能体能力描述；
- b) 应支持将待分发子任务的能力需求（如技能标签、接口定义）与已接入智能体的能力声明进行匹配。

7.1.2 分发策略

- a) 应支持基于任务优先级的分发；
- b) 应支持分发结果的确认机制，确保任务已正确送达目标智能体。

7.1.3 分发审计

- a) 应记录每次任务分发的目标智能体、时间戳、分发策略依据；
- b) 应支持分发记录的查询与导出，用于事后分析。

7.2 状态追踪

7.2.1 状态模型

- a) 应定义统一的任务状态模型，如待分发、分发中、执行中、成功、失败、超时、已取消。

7.2.2 状态采集

- a) 应支持智能体主动上报任务状态变更；
- b) 应支持平台主动轮询智能体获取最新状态。

7.2.3 状态查询展示

- a) 应提供统一的任务状态查询接口；

- b) 应提供可视化的任务执行链路图，展示各子任务状态及依赖关系。

8 任务交互

8.1 任务指令交互

8.1.1 指令接收

- a) 应支持用户或上游系统通过自然语言或结构化格式（如JSON）提交任务指令；
- b) 应支持同步、异步等接收模式，异步模式下返回任务标识供后续查询；
- c) 应支持对指令大小的限制与校验，防止超大指令消耗系统资源。

8.1.2 指令解析

- a) 应支持从任务指令中解析出任务目标、输入参数、约束条件（如超时时间、优先级）等要素；
- b) 应支持对自然语言指令的语义理解，至少支持中文和英文；
- c) 宜支持指令解析结果的置信度输出，低置信度时触发人工确认。

8.1.3 指令验证

- a) 应支持对解析后的指令要素进行完整性校验，必填字段缺失时拒绝任务或请求补全；
- b) 应支持对输入参数的数据类型和范围进行基础校验，避免无效参数传入智能体。

8.2 多智能体交互

8.2.1 交互协议支持

- a) 应支持智能体间以标准化格式进行通信，如MCP、A2A或自定义格式；
- b) 应支持将平台内部消息转换为目标智能体可接收的协议格式；
- c) 宜支持协议版本协商与兼容性检测。

8.2.2 消息路由与转发

- a) 应支持将消息准确路由至目标智能体；
- b) 宜支持消息优先级队列，设置优先级。

8.2.3 交互可观测

- a) 应记录所有跨智能体交互消息的记录；
- b) 应支持交互链路的分布式追踪，关联同一任务的跨智能体消息。

9 协同交付

9.1 交付物汇总

9.1.1 交付物汇总

- a) 应支持收集所有子任务返回的执行结果，包括文本、JSON、文件、图片等多模态数据；
- b) 应支持交付物的完整性校验，防止传输损坏。

9.2 一致性校验

9.2.1 校验规则配置

- a) 应按照配置的规则，对所有交付物进行一致性校验；
- b) 应支持逐步校验，一旦发现不一致可提前中止并报告；
- c) 应支持针对不一致结果的自动裁决策略（如取时间戳最新、取可信度最高的智能体结果、取多数结果）。

9.2.2 异常处置

- a) 对于校验不一致且无法自动裁决的情况，应转入人工处理流程，提供对比界面；
- b) 应支持人工选择最终正确结果，或要求相关智能体重试；
- c) 应记录不一致原因及最终处理方式，用于后续分析。

10 安全治理

10.1 权限治理

10.1.1 身份与访问控制

- a) 应支持基于角色的访问控制，预定义至少三种角色：管理员、普通用户、只读审计员；
- b) 应支持细粒度的资源权限，按读、写、调用、管理等操作维度实现管控；
- c) 应支持多租户隔离，不同租户的数据和智能体相互不可见。

10.1.2 最小权限原则

- a) 应遵循最小权限原则，默认拒绝未明确授权的操作；
- b) 应支持权限申请流程，用户可提交权限申请，经审批后授予；
- c) 应支持权限定期复审，对长期未使用的权限进行回收预警。

10.1.3 操作审计

- a) 应记录所有权限变更操作以及敏感操作（如任务取消、智能体强制下线）；
- b) 应审计日志包含操作人、时间戳、操作类型、资源标识、操作结果等关键数据；
- c) 应支持审计日志存储周期不少于180天。

10.2 监控审计

10.2.1 系统监控

- a) 应提供对平台核心指标的实时监控，包括：任务吞吐量、成功率、平均响应时间、调度队列长度、智能体在线数；
- b) 应支持监控指标的可视化仪表盘，可自定义时间范围与刷新频率；
- c) 应支持基于指标的告警配置，可设置阈值和通知渠道。

10.2.2 日志管理

- a) 应记录平台关键操作日志及异常事件日志；
- b) 应提供日志集中存储与检索能力，支持按时间、租户、智能体ID等维度过滤。

10.2.3 链路追踪

- a) 应支持跨智能体的分布式链路追踪，为每次任务调用生成全局唯一追踪ID；
 - b) 应记录调用链路中各节点的开始时间、耗时、状态等信息；
 - c) 应提供链路追踪的可视化查询界面，支持按ID快速检索全链路信息。
-