

团 体 标 准

T/ISC 0175—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

（发布稿）

2026 - 10 - 28 发布

2026 - 11 - 28 实施

中 国 互 联 网 协 会 发 布

目 次

前 言	2
智能体互联网 任务编排 OpenClaw 类多智能体协同平台能力要求	3
1 范围	3
2 规范性引用文件	3
3 术语和定义	3
3.1 OpenClaw 类智能体 (OpenClaw-Style Agent)	错误! 未定义书签。
3.2 多智能体协同平台 (Multi-Agent Collaboration Platform)	3
3.3 智能体互联网 (Agentic Internet)	3
4 符号和缩略语	3
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	3
6 接入管理能力要求	4
6.1 身份接入	4
6.2 能力接入	5
7 任务拆解能力要求	5
7.1 任务分发	5
7.2 状态追踪	5
8 任务交互能力要求	6
8.1 任务指令交互	6
8.2 多智能体交互	6
9 协同交付能力要求	6
9.1 交付物汇总	6
9.2 一致性校验	6
10 安全治理能力要求	7
10.1 权限与访问控制	7
10.2 安全防护	7
10.3 监控审计	8

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OpenClaw类多智能体协同平台能力的标准。

本文件是《智能体互联网》系列标准之一。该系列标准已立项的文件包括：

- 《智能体互联网 网联 智能体网关能力要求》；
- 《智能体互联网 网联 OpenClaw类多智能体协同能力要求》。

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，包括接入管理能力要求、任务拆解能力要求、任务交互能力要求、协同交付能力要求、安全治理能力要求等核心能力。

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。

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。

本文件由中国互联网协会归口。

本文件起草单位：中国信息通信研究院、中国民用航空华东地区空中交通管理局、广州越创智数信息科技有限公司、中移(苏州)软件技术有限公司、中国烟草总公司浙江省公司、中国电信集团有限公司、中国移动通信集团江苏有限公司、中国移动通信集团广西有限公司、中国联合网络通信有限公司、中国电信股份有限公司研究院、中移九天人工智能科技（北京）有限公司、华为技术有限公司、紫金山实验室、新华三技术有限公司、政达研学（雄安）科技有限公司

本文件主要起草人：李哲、王向花、王雨宣、刘学森、卢敏、俞成、陈佳齐、杨辉、张为华、周铭杰、张可、崔恩放、崔恩放、梁致远、过民欣、高玥、孙波、王轶、宋世峰、章文彬、曹杰、马安邦、刘冰、苏良良、莫烨、温智聪、张玲艳、赵昱、韩宇峰、王凯、熊曦、王传庆、孙琼、宋欣、庞玥、张文星、金毅然、钮远、贺亮、陶志平、汪硕、李振红、王泽南、李继承、魏勇、杨光、范杰、陈倩倩、殷平、陶淘、曹云飞、马力俊、崔煜喆、苏蕾权、赵梦佳、吴迪

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,包括接入管理能力要求、任务拆解能力要求、任务交互能力要求、协同交付能力要求、安全治理能力要求等核心能力。

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 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。

3.2 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)

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)

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

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

协同交付能力要求	交付物汇总		一致性校验	
	交付物汇总		校验规则配置	异常处置
任务拆解能力要求	任务匹配		状态追踪	
	能力匹配	分发策略	状态模型	状态采集
	分发审计		状态查询展示	
任务交互能力要求	任务指令交互		OpenClaw类多智能体交互	
	指令接收	指令解析	交互协议支持	消息路由与转发
	指令验证		交互可观测	
接入管理能力要求	身份接入		能力接入	
	身份注册		能力声明	
	身份生命周期管理		能力校验	

安全治理能力要求	
权限与访问控制	
身份与访问控制	
最小权限控制	智能体间授权控制
安全防护	
接入能力安全防护	任务与指令安全防护
多智能体调用安全防护	
数据与交付结果安全防护	
监控审计	
系统监控	
日志管理	链路追踪

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

智能体互联网可分为基础设施层、互联层、执行层、应用层四层技术体系，在保持网络兼容延续的同时，面向智能体连接与协同需求开展兼容式改造、增量式创新，实现多维度能力升级。

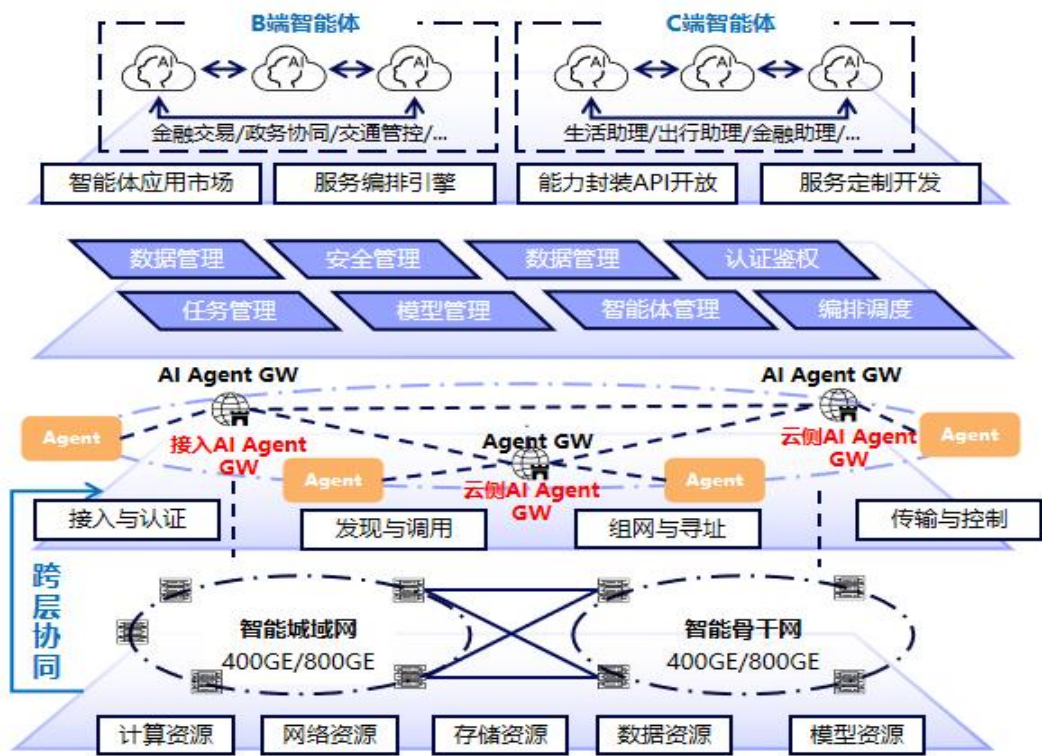


图 2 智能体互联网技术体系架构

6 接入管理能力要求

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。
- d) 宜采用统一结构生成数字身份标识，如 UUID、ULID 或“命名空间+随机数/序列号”组合；
- e) 应通过集中登记与查重校验机制，保证数字身份标识在平台内唯一。

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) 应支持身份状态变更的审计记录。
- d) 应支持智能体违规强制停用。

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，变更后应重新校验；
- d) 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 任务拆解能力要求

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 任务交互能力要求

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A2A等智能体间通信协议，并可支持MCP等工具/上下文协议的协同接入；采用自定义协议时应提供协议描述和兼容机制。
- 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。
- c) 应支持限制智能体间的最大连续调用层级，防止产生死循环。

8.2.3 交互可观测

- a) 应记录跨智能体交互事件及必要元数据；消息正文应按数据敏感等级和审计需要配置采集，并支持脱敏、摘要或不采集。
- 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 协同交付能力要求

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) 宜在裁决规则明确、结果可客观验证且风险可接受的场景支持自动裁决策略（如取时间戳最新、取可信度最高的智能体结果、取多数结果）；涉及高风险操作、重要数据或无法客观判定的结果时，应转人工或确定性校验。

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 安全治理能力要求

10.1 权限与访问控制

10.1.1 身份与访问控制

- a) 应支持对用户和智能体进行身份识别与访问控制，未经授权的主体不应访问平台资源或参与任务执行；
- b) 应支持基于角色和资源对象进行细粒度权限控制，可按照查询、调用、修改、管理等操作配置相应权限；
- c) 应支持多租户访问隔离，不同租户间的智能体、任务、数据和相关资源未经授权不应相互访问。

10.1.2 最小权限控制

- a) 应遵循最小权限原则，默认拒绝未明确授权的操作，仅授予完成任务所必需的权限；
- b) 应支持权限的申请、审批、授予、变更和撤销，并宜支持按照任务范围或有效期限授予临时权限；
- c) 应支持对已授予权限进行定期复审，对长期未使用、已经过期或不再符合业务需要的权限及时调整或回收。

10.1.3 智能体间授权控制

- a) 应支持配置智能体之间的授权关系，明确发起方智能体可调用的目标智能体、能力及资源范围；
- b) 应支持对任务委托、转发过程中的权限继承和传递范围进行限制，防止权限在多智能体调用链中扩大；
- c) 应支持智能体间授权关系的变更和撤销，并确保变更后的授权策略及时生效。

10.2 安全防护

10.2.1 接入能力安全防护

- a) 应支持对智能体注册信息、身份信息及通信端点进行安全校验，防止非法、伪造或异常智能体接入平台；
- b) 应支持对智能体能力声明进行有效性和一致性校验，确保声明的能力、接口及实际可提供能力相匹配；
- c) 智能体身份信息、通信端点或能力声明发生重要变更时，应重新进行校验；发现违规或异常情况时，应支持暂停或限制相关智能体服务。

10.2.2 任务与指令安全防护

- a) 应支持对任务指令、输入参数及约束条件进行安全校验，对不符合授权范围或安全策略的任务请求进行拒绝、限制或确认；
- b) 应采取措施防止任务在拆解、分发和执行过程中未经授权修改任务目标、关键参数及安全约束；
- c) 对于涉及敏感资源、重要业务操作或其他高风险操作的任务，应支持人工审批、二次确认等控制机制。

10.2.3 多智能体调用安全防护

a) 应支持限制智能体间连续调用层级、调用频率或重试次数，防止循环调用、异常重试等造成资源异常消耗；

b) 应支持识别重复失败、异常高频、调用关系异常等智能体间异常调用行为；

c) 发现异常调用时，应支持采取限流、中断、暂停相关调用等措施，防止异常行为沿智能体调用链扩散。

10.2.4 数据与交付结果安全防护

a) 应支持对任务输入、智能体间交互、中间结果和最终交付结果中的敏感信息进行识别，并按照任务需要控制数据访问和使用范围；

b) 对于跨智能体传递的敏感数据，应支持采取脱敏、摘要、最小化传递等保护措施，防止未经授权访问和泄露；

c) 应采取措施防止中间结果和最终交付结果被未经授权修改，发现异常修改或完整性异常时应及时提示或阻止交付。

10.3 监控审计

10.3.1 系统监控

a) 应提供对平台核心运行指标的监控，包括任务吞吐量、任务成功率、平均响应时间、调度队列长度、智能体在线数等；

b) 应支持监控指标的可视化展示，并支持按照需要配置监控时间范围和刷新频率；

c) 应支持基于监控指标配置告警规则，可设置告警阈值和通知方式。

10.3.2 日志管理

a) 应记录平台关键操作及异常事件日志，日志内容应包括相关主体、时间、操作对象、操作类型和操作结果等必要信息；

b) 应提供日志集中存储和检索能力，支持按照时间、租户、智能体ID、任务ID等维度进行查询；

c) 应采取措施保障日志完整性和访问安全，其中权限变更、敏感操作等重要审计日志保存周期应不少于180天。

10.3.3 链路追踪

a) 应支持跨智能体任务执行过程的分布式链路追踪，并为每次任务调用生成可关联的全局唯一追踪ID；

b) 应记录调用链路中各智能体及相关节点的调用关系、开始时间、耗时和执行状态等信息；

c) 应提供链路追踪查询能力，支持依据追踪ID、任务ID等信息快速检索完整任务调用链路。