ICS 35. xxx
CCS Lxx

团　　体　　标　　准

T/ISC XXX—2026

智能体互联网 网联 智能体网关能力要求

Capability Requirements of Connected Agent Gateway 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

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、中国移动通信集团有限公司、华为技术有限公司、中国移动通信集团江苏有限公司、中移九天人工智能科技（北京）有限公司、中国电信股份有限公司研究院。

本文件主要起草人：本标准主要起草人：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、金毅然、孙琼、韩宇峰、范杰、陶淘、赵梦佳、吴迪、金毅然。

智能体互联网 网联 智能体网关能力要求

1 范围

本文件规定了智能体互联网下智能体网关的能力要求，聚焦安全防护、路由寻址、协议适配、身份分发四个能力域，旨在规范硬件及软件形态的智能体网关在智能体互联网中对通信流量、身份认证、协议转换及安全治理的支撑能力，确保异构智能体之间高效、安全、可靠协作。

本文件适用于以运营商、通信设备商与云厂商为代表的网关供给方，以及以大型企业、行业智能化应用方为代表的网关需求方开展能力评估、选型验收等工作。

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 智能体网关（Agent Gateway）

智能体网关是指部署于智能体互联网各通信域边界或核心节点的关键基础设施，基于智能体注册元数据与服务描述实现消息的路由寻址与协议适配，并承担通信流量的安全防护与身份分发，是实现智能体之间高效、安全、可靠互操作的核心枢纽。

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）

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）

ID 标识符（Identifier）

5 智能体互联网 网联 智能体网关能力要求框架

5.1 框架模型

智能体互联网 网联 智能体网关能力要求包括身份分发、协议适配、路由寻址、安全防护四个能力模块，如下图1所示。

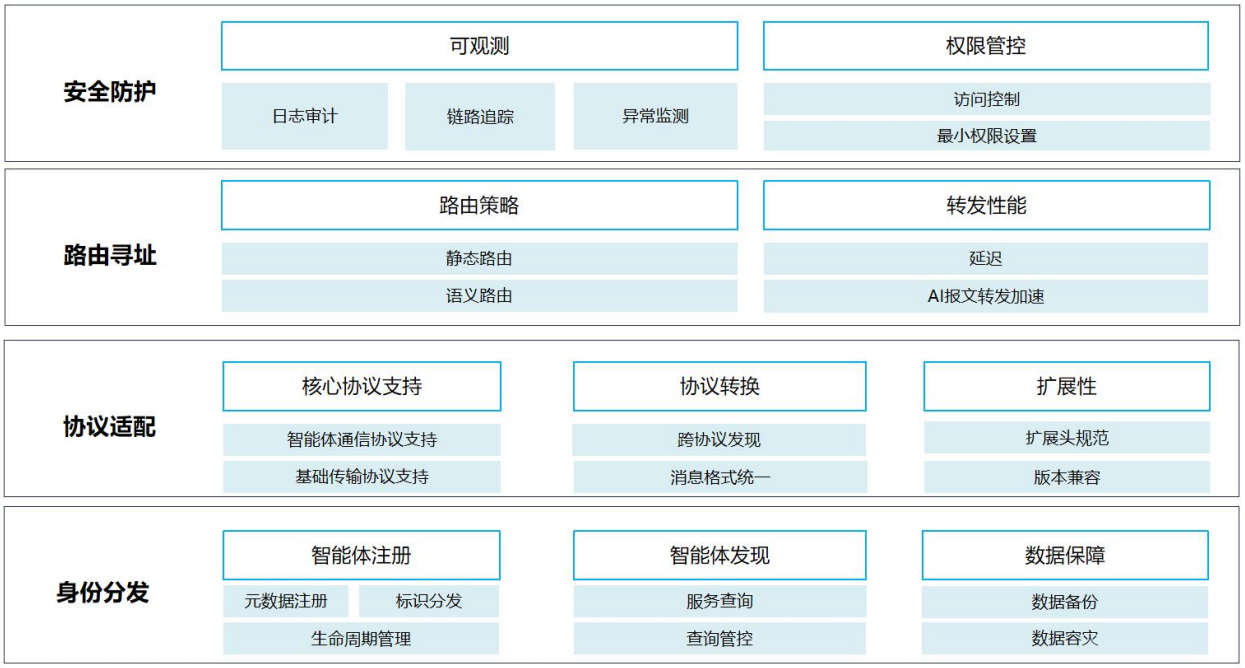

图 1 智能体互联网 网联 智能体网关能力框架

6 身份分发能力

6.1 智能体注册

6.1.1 元数据注册

a）应支持智能体在接入网关时提交完整的元数据注册信息，包含智能体名称、唯一标识、能力描述、支持协议、通信端点、所属组织等字段；

b)应支持元数据的校验机制，确保注册信息的规范性、完整性与真实性；

c)宜支持元数据的编辑，可在线修改自身能力描述、通信端点等注册信息，变更需经过审核；

d)宜支持元数据模板化，提供面向不同行业或场景的标准元数据模板，降低注册门槛。

6.1.2 标识分发

a）可支持为每个注册智能体生成网关内唯一的数字身份标识；

b）宜支持多种标识生成策略，包括随机标识、层级化标识、密码学标识。

6.1.3 生命周期管理

a）应支持智能体身份全生命周期闭环管理，覆盖注册、运行、暂停、注销等核心阶段；

b）应支持身份状态变更即时生效，如暂停后立即阻断该智能体所有通信，恢复后自动还原授权。

6.2 智能体发现

6.2.1 语义查询

a）应支持标准化的基于语义查询智能体的接口，支持按关键词精确或模糊查询；
b）应支持查询结果的排序功能，可按相关性、可用性、响应延迟等指标排序。

6.2.2 查询管控

a）应支持查询结果的过滤与范围限定，仅返回授权可见的智能体信息；
b）应支持查询接口的访问控制与限流策略，防止接口滥用、信息泄露与流量冲击。

6.3 数据保障

6.3.1 数据备份

a）应支持智能体身份相关数据的定时备份与主动备份能力；
b）应支持备份数据的加密存储，保障备份数据安全性与完整性；
c）宜支持增量备份与全量备份结合。

6.3.2 数据容灾

a）应支持数据故障自动检测，核心数据异常时即时触发告警；
b）应支持备份数据的快速恢复，保障身份分发核心功能不中断。

7 协议适配

7.1 核心协议支持

7.1.1 智能体通信协议支持

a）应支持A2A等主流智能体间通信协议的接入与转发；
b）应支持OpenAI等模型接口定义规范的解析与校验；

7.1.2 c）。基础传输协议支持

a）应支持基于TCP和HTTP/HTTPS的标准传输协议接入。

7.2 协议适配

7.2.1 跨协议发现

a）应支持跨协议的智能体服务发现，使采用不同通信协议的智能体可被统一检索与定位；
b）应支持处理不同服务描述的能力，如Agent Card、Agent Record等。

7.2.2 消息格式适配

a）应支持异构消息格式的自动识别与统一转换，至少覆盖JSON、XML等主流格式；
b）应支持消息体的语义保持转换，确保格式转换过程中信息不丢失、语义不偏移；

c）可支持自定义消息映射规则，满足特殊业务场景下的格式转换需求；

d）可支持消息转换的可配置管道，允许多个转换步骤的有序组合与复用。

7.3 扩展性

7.3.1 扩展头规范

a）应定义统一的网关与智能体、网关之间的应用层消息扩展头规范，涵盖智能体注册、跨域转发等场景需求；

b）宜支持自定义扩展头的注册与管理机制。

7.3.2 版本兼容

a）应支持协议版本协商机制，在通信建立阶段自动协商双方支持的最优协议版本；

b）可提供版本兼容性的自动检测与告警能力，提前发现潜在的不兼容风险。

8 路由寻址

8.1 路由策略

8.1.1 静态路由

a）应支持路由规则的版本管理与回滚，可快速恢复历史配置；

b）宜支持基于智能体或模型标识、服务名称、API路径等静态信息的基础路由转发功能。

8.1.2 语义路由

a）可支持将自然语言请求解析并匹配至相应的智能体或模型；

b）可支持语义路由决策过程的可解释性，输出路由选择依据与匹配度量化指标。

8.2 转发性能

8.2.1 延迟

a）应确保消息转发的低延迟处理；

b）应提供吞吐量、延迟、错误率等核心性能指标的实时监控与可视化展示；

c）可支持性能指标的长期趋势分析及响应时间预警。

8.2.2 AI 报文转发加速

a）宜支持对AI报文的高效解析与转发加速机制；

b）宜支持流式响应数据的透传与缓存优化，减少首字延迟；

c）可支持基于智能体交互语义的报文预处理，如图片压缩、文本摘要、上下文注入等，优化传输效率；

d）可支持基于内容感知的动态路由优化，根据报文大小、类型与优先级进行差异化转发策略；

e）可支持硬件加速卸载，利用智能网卡等设备实现报文处理硬件加速。

9 安全防护

9.1 可观测

9.1.1 日志审计

a）应支持对智能体间通信的访问日志及异常事件日志记录；
b）可提供日志集中存储与检索能力；
c）可支持按时间范围、操作类型等维度组合查询日志；
d）可支持日志数据的关联分析，辅助运维人员快速识别问题源头。

9.1.2 链路追踪

a）宜支持跨智能体的分布式链路追踪能力，为每次调用任务生成全局唯一的追踪标识；
b）宜记录调用链路各节点的耗时、状态码及关键上下文信息，支持性能瓶颈定位。

9.1.3 异常检测

a）应支持对智能体通信流量进行实时异常检测，能识别流量异常可疑行为；
b）应支持检测常见的智能体攻击手段，如提示词注入、指令篡改、身份伪造等。

9.1.4 传输安全

a）应支持基于 TLS/HTTPS 等加密协议保障智能体间通信数据的机密性与完整性，防止通信内容被窃听与篡改；
b）应支持对通信对端的证书校验与双向身份认证，防止中间人攻击；
c）宜支持国产密码算法（如 SM2、SM3、SM4），满足密码应用自主可控要求；

9.1.5 网络访问控制

a）应支持基于访问控制列表（ACL）的报文过滤，阻断来自非法源地址或端口的访问；
b）应支持流量限速与异常流量清洗，具备基础的抗 DDoS 攻击能力；
c）应支持网络安全域划分与区域隔离，防止跨安全域的越权访问；
d）宜支持网络入侵检测与防护，及时发现并处置网络层攻击行为。

9.2 权限管控

9.2.1 访问控制

a）应支持访问控制策略，对每个进入网关的通信请求进行身份验证与权限校验，拒绝未授权访问；
b）应支持为不同智能体分配差异化的权限，并依据其权限限制其可访问的服务与资源范围。

9.2.2 最小权限设置

a）应遵循最小权限原则，仅开放完成特定任务所需的最小权限集合；
b）宜支持权限的回收机制，对违规或到期的权限进行预警或撤销。