ICS 35. xxx
CCS Lxx

团　　体　　标　　准

T/ISC XXX—XXXX

面向办公场景的 AIPC 智能体能力要求

在提交反馈意见时，请将您知道的相关专利与支持性文件一并附上。

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－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。

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专利的责任。

本文件由中国互联网协会提出并归口。

本文件起草单位：

本文件主要起草人：

本文件及其所代替文件的历次版本发布情况为：

——

引　言

随着人工智能技术与个人计算机产业的深度融合，搭载专用AI计算单元、具备端侧AI推理能力的AI个人计算机（AIPC）已成为办公场景数字化升级的核心载体。AIPC智能体作为AIPC的核心原生应用，凭借本地优先、端侧执行、自主规划、工具可扩展、跨端协同的核心特性，可实现办公任务全链路自动化闭环处理，已成为驱动办公场景智能化转型的核心抓手。

当前，办公场景AIPC智能体产品快速迭代，但行业内尚未形成统一的能力定义、技术规范与评价体系，导致产品能力参差不齐、用户选型无据可依、行业发展缺乏统一指引。为规范办公场景AIPC智能体的研发、测试、应用与评估，提升产品核心能力，保障用户数据安全与使用体验，促进行业健康有序发展，特制定本文件。

本文件聚焦办公场景核心需求，适配AIPC智能体的技术架构与能力边界，明确了AIPC智能体的能力体系框架、技术要求、评价方法，可为人工智能终端生产企业、大模型研发机构提供技术依据，也可为相关产品测试、行业监管提供参考。

面向办公场景的AIPC智能体能力要求

1 范围

本文件规定了面向办公场景的AIPC智能体的术语和定义、能力体系框架、技术要求与评价方法。

本文件适用于面向办公场景的AIPC智能体的设计、开发、测试与评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 45288.1 人工智能 大模型 第1部分：通用要求

3 术语和定义

GB/T 45288.1界定的以及下列术语和定义适用于本文件。

3.1

AI 个人计算机 AI personal computer; AIPC

配备专用人工智能计算硬件，具备端侧人工智能推理与处理能力，支持运行人工智能体的个人计算机。

3.2

智能体 AI agent

基于人工智能模型，具备感知、规划、执行能力，能够自动化完成特定任务的软件实体。

3.3

端云协同推理 cloud-device collaborative inference

人工智能模型的推理计算过程由本地终端与云端服务器协同完成的计算模式。

3.4

技能 skill

AIPC智能体中用于调用外部工具、应用、服务或硬件设备以执行具体操作的功能模块。

4 能力体系框架

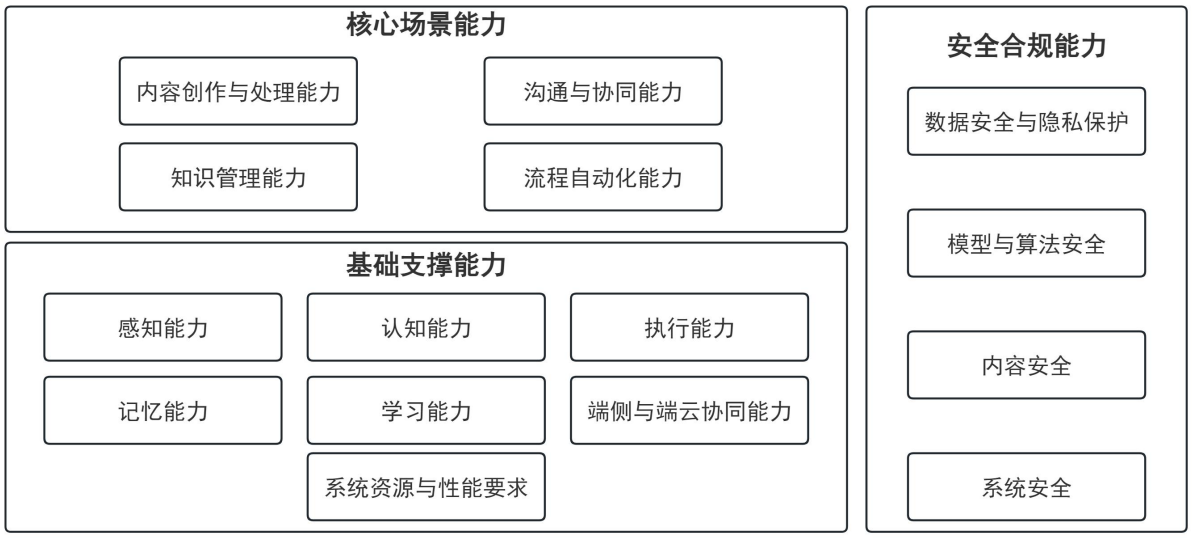

图 1 面向办公场景的 AIPC 智能体能力体系

面向办公场景的AIPC智能体能力体系分为三大维度，适配AIPC智能体的技术架构，依次为：

a)基础支撑能力：对应AIPC智能体接入层、核心引擎层、记忆管理层的核心能力，包括感知能力、认知能力、执行能力、记忆能力、学习能力、端侧与端云协同能力、系统资源与性能要求。

b)核心场景能力：对应AIPC智能体技能执行层的办公场景专项能力，包括内容创作与处理能力、沟通与协同能力、知识管理能力、流程自动化能力。

c)安全合规能力：贯穿AIPC智能体全架构、全生命周期的安全与合规要求，包括7.1数据安全与隐私保护、模型与算法安全、内容安全、系统安全。

5 基础支撑能力要求

5.1 感知能力

应满足以下要求：

a)应支持文本、语音、图像等多模态指令输入。

b)应在办公环境下准确识别用户的语音指令，完成语音到文本的准确转写。

c)应具备视觉感知能力，可识别扫描版PDF、图片文档、截图中包含的印刷体文字、手写体内容、公式、表格及图形图表。

d)应具备环境感知能力，能够识别当前设备状态、网络环境及已连接的外设状态。

5.2 认知能力

应满足以下要求：

a)应具备意图识别能力，准确理解日常办公指令的真实诉求，承接多轮办公对话的上下文信息。

b)应具备澄清确认能力，针对模糊、歧义、不完整的办公指令，应主动向用户澄清确认核心需求。

c)应具备任务规划能力，针对复杂办公任务，应将其拆解为逻辑清晰、可执行的分模块子任务，子任务间逻辑连贯、目标统一。

d)应具备推理决策能力，可根据任务复杂度动态决策算力调度策略，基础创作任务应具备端侧推理能力，复杂任务可触发端云协同推理。

5.3 执行能力

应满足以下要求：

a)应具备技能调用能力，兼容主流办公套件的常用功能调用；宜支持OA系统、邮箱客户端、项目管理工具、企业协同软件的标准化接口接入。

b)应具备系统操作能力，安全调用AIPC本地文件系统、终端命令、浏览器自动化、外设控制等常用系统级能力。

c)应具备过程控制能力，实时反馈任务执行进度，支持任务暂停、终止、回滚操作。

d)应具备异常处理能力，子任务执行失败时，应自动重试，重试后仍无法完成的，应向用户反馈明确的错误原因与解决方案。

e)应具备主动执行能力，支持定时任务、触发式任务的配置与执行，可根据预设规则主动完成办公任务，不应出现错触发、漏触发的情况。

5.4 记忆能力

应满足以下要求：

a)应具备短期记忆能力，完整留存单轮/多轮办公会话的上下文信息，会话结束后可根据用户配置自动归档或销毁。

b)应具备长期记忆能力，存储并检索用户的办公偏好、常用规则、历史任务记录及个人知识库。

c)应具备记忆管理能力，支持记忆数据的加密存储、手动编辑、批量导出与销毁，保障数据安全。

5.5 学习能力

应满足以下要求：

a)应具备用户习惯学习能力，基于记忆内容优化任务执行策略，实现个性化办公适配。

b)应具备技能掌握学习能力，学习并记忆已接入技能的功能、调用规则，无需用户重复说明调用方式即可完成准确调用。

c)宜具备持续优化能力，根据用户的反馈（如修改、拒接等行为）修正后续的行为策略，提升任务完成的满意度。

5.6 端侧与端云协同能力

应满足以下要求：

a)应具备端侧推理能力，基础办公任务应能在AIPC端侧独立完成，保障无网或弱网环境下的办公可用性。

b)应具备动态调度能力，根据任务复杂度、网络环境及端侧算力负载，智能调度端侧与云端算力资源。

c)应具备端云协同推理能力，在端云协同推理过程中，应保障任务状态的连续性与结果的一致性，实现无缝切换。

5.7 系统资源与性能要求

系统资源占用：智能体待机状态内存占用宜小于3GB；任务执行时CPU峰值占用宜小于80%。

6 核心办公场景能力要求

6.1 内容创作与处理能力

6.1.1 本地数字资产定位与调度能力

应满足以下要求：

a)应支持通过文件名、文件类型、时间范围等元数据，以及文档内包含的关键词，对本地及已挂载盘符的文件进行检索。

b)宜支持通过自然语言描述进行文件模糊查找（如“找上周关于预算的表格”），结合上下文转化为检索条件。

c)检索结果应直接关联后续操作，支持用户指令直接对搜索结果执行打开、复制或作为输入源传给其他技能处理。

6.1.2 泛文档理解与解析能力

应满足以下要求：

a)应兼容主流办公文档格式（如doc/docx/xls/xlsx/ppt/pptx/pdf等）及图片、截图的读取。

b)应支持复杂版式解析，准确识别图文混排、表格、公式、页眉页脚、批注及修订痕迹。

c)支持长文档全量解析无截断。

d)应具备OCR能力，准确提取扫描版PDF、图片中的印刷体、手写体及复杂表格结构。

6.1.3 文字文档处理能力

应满足以下要求：

a)文档生成：应支持根据指令生成报告、方案、纪要、通知等通用办公文档；宜支持匹配企业或行业常用模板，自动套用标题层级、字体段落、页边距等规范样式；宜支持首字生成时间小于5秒，端侧模式下生成速度大于10字/秒，端云协同模式下生成速度大于20字/秒。

b)润色与编辑：应支持全文润色、段落改写、风格调整、错别字及语法纠错。

c)审阅与校验：宜支持基于可配置规则库对文档进行合规性自查、敏感信息识别与风险提示；对引用内容应自动标注来源或出处。

d)结构优化：应支持多级标题自动梳理及章节逻辑优化。

e)版本与协同：宜支持多用户协同编辑；所有生成或修改内容应保留可追溯的版本记录。

6.1.4 表格数据处理能力

应满足以下要求：

a)应支持通过自然语言指令完成数据去重、格式转换、分列等基础数据清洗操作。

b)应能根据计算需求自动生成并应用正确的公式与函数，宜支持对公式逻辑进行自然语言解释。

c)宜支持通过自然语言指令生成数据透视表配置或相关脚本代码，辅助用户完成多维数据分析。

d)宜支持根据数据特征生成匹配的图表。

6.1.5 演示文稿处理能力

应满足以下要求：

a)应能根据原始文档或主题，自动提取核心观点并生成结构化的PPT大纲。

b)宜支持根据内容自动匹配幻灯片版式，完成文字、图表的智能排版与风格美化。

6.2 沟通与协同能力

6.2.1 邮件智能管理能力

应满足以下要求：

a)应支持多账号邮件统一收发、智能分类。

b)应根据上下文自动生成回复草稿，支持不同语气的快速切换。

c)宜具备邮件待办提取能力，自动识别邮件中的截止时间与行动项并推荐关联至日程。

6.2.2 日程与任务规划能力

应满足以下要求：

a)应支持通过自然语言创建日程，自动排查时间冲突并推荐空闲时段。

b)应具备任务拆解能力，将宏观目标转化为带时间节点的子任务列表。

6.2.3 会议辅助能力

6.2.3.1 会前准备能力

应满足以下要求：

a)应根据会议需求自动生成会议邀约，同步参会人日程，自动排查日程冲突。

b)应根据会议主题、议程自动生成会议议程、主持词、发言稿等会议材料。

c)应完成多维度会前提醒，包括参会人提醒、材料准备提醒及会议设备调试提醒。

6.2.3.2 会中实时辅助能力

应满足以下要求：

a)应完成会议实时语音转写，转写内容与发言内容一致；支持多人分角色转写，角色区分准确。

b)宜支持主流语种的实时翻译功能。

c)应实时生成会议核心观点、关键决议、待办事项，内容覆盖会议核心信息。

6.2.3.3 会后全流程处理能力

应满足以下要求：

a)应能够生成结构化会议纪要；宜支持用户自定义纪要模板。

b)宜支持自动将会议议程、音视频文件、转写文本、会议纪要等会议资产统一归档；宜支持会议内容全文检索。

6.3 知识管理能力

6.3.1 知识库构建能力

应满足以下要求：

a)宜支持构建本地知识库，支持多种知识载体（文档、邮件、聊天记录、代码等）的导入、清洗与向量化索引。

b)宜具备知识分级分类与权限标签自动映射能力，按部门、项目或角色实现可见性隔离。

c)宜具备知识时效性管理机制，对过期、废止或低置信度内容自动标记或提示更新。

6.3.2 知识检索与问答能力

应满足以下要求：

a)在端云协同模式下，应具备基于自然语言提问的语义检索能力，并提供来源溯源，宜支持本地知识库语义检索响应时间小于1.5s，复杂推理问答首字生成时间小于3s。

b)应基于知识库内容进行总结、推理并回答用户问题，不应出现无依据的编造。

6.4 流程自动化能力

6.4.1 跨应用数据串联

宜具备基于自然语言指令的跨应用任务编排能力，能够将分别属于不同应用（如本地文档、浏览器网页）的离散操作组合执行，并在切换应用时保持上下文传递。

6.4.2 基于 OS 原生接口的泛用型操作

应满足以下要求：

a)宜能调用操作系统提供的无障碍框架，对未开放API的本地传统应用进行基础的UI元素识别（如按钮、输入框）。

b)宜在用户授权且高风险操作经确认的前提下，基于UI识别对本地应用执行模拟点击、文本输入等基础交互。

7 安全合规能力要求

7.1 数据安全与隐私保护

应满足以下要求：

a)应遵循数据最小化原则，仅收集完成办公任务必需的数据；用户办公核心数据、隐私数据应优先在端侧存储和处理。

b)端侧存储的办公数据应采用加密方式保护；端云、跨设备传输数据时应全程加密。

c)应具备敏感数据识别能力，支持敏感数据自动脱敏、违规外发拦截；发生数据泄露风险时应主动向用户告警。

d)数据操作日志留存时间不应少于6个月，应可追溯、可审计。

7.2 模型与算法安全

应满足以下要求：

a)应具备防御提示词攻击的能力，识别并阻止恶意指令对模型行为的操纵。

b)应具备模型防窃取能力，防止通过逆向工程、模型提取攻击等手段窃取端侧模型参数。

7.3 内容安全

应满足以下要求：

a)应能识别并拒绝生成违法违规、低俗、敏感、侵权内容；

b)生成内容应规避侵权风险，对引用内容应标注来源；

c)应支持生成内容的隐式水印嵌入或显式标识，确保生成内容可追溯至生成设备及时间。

7.4 系统安全

应满足以下要求：

a)智能体应具备防篡改、防逆向、防劫持能力；应支持运行环境安全检测。

b)智能体的日常推理与普通办公技能调用宜在应用级安全沙箱内运行。

c)智能体执行高风险操作前，应获得用户显式授权，并进行二次确认。

d)宜具备安全漏洞监测与修复能力。