

国家标准化指导性技术文件《人工智能操作系统权限管理要求》（征求意见稿）编制说明

一、工作简况

（一）任务来源与起草单位

2026年6月12日，根据国家标准化制修订安排，国家标准化指导性技术文件《人工智能操作系统权限管理要求》（计划号 20263106-Z-469）正式立项并启动起草工作，由全国信息技术标准化技术委员会（SAC/TC 28）提出并归口，由程序设计语言分技术委员会（SC22）和操作系统标准工作组（WG30）组织研制。

该标准主要起草单位：中国电子技术标准化研究院、中兴通讯股份有限公司、华为终端有限公司、维沃移动通信有限公司、OPPO 广东移动通信有限公司、天翼云科技有限公司、小米通讯技术有限公司、统信软件技术有限公司、中移(苏州)软件技术有限公司、荣耀终端股份有限公司、麒麟软件有限公司、南京大学、北京交通大学等单位。

其中，中国电子技术标准化研究院负责标准管理和协调，中兴通讯股份有限公司、华为终端有限公司、维沃移动通信有限公司、OPPO 广东移动通信有限公司、天翼云科技有限公司、小米通讯技术有限公司、统信软件技术有限公司、中移(苏州)软件技术有限公司、荣耀终端股份有限公司、麒麟软件有限公司分工编制标准，深圳市腾讯计算机系统有限公司、蚂蚁科技集团股份有限公司、南京大学、北京交通大学对标准内容提出意见和建议。

（二）编制背景及意义

随着人工智能技术在终端操作系统的应用日益广泛，人工智能操作系

统作为硬件资源调度、承载智能体运行、支撑上层应用的核心枢纽，其权限管理体系直接关系到系统安全防护能力、个人隐私保护水平及智能化服务底线。2026年5月，国家网信办等三部门联合印发《智能体规范应用与创新发展实施意见》，明确提出要厘清各类决策方式的合理边界及所需权限，为权限管理标准化工作提供了明确的政策依据。传统操作系统以静态权限列表为基础，无法有效应对智能体带来的新挑战，突出表现为越权访问与权限滥用、自动化操作失控、数据过度采集与隐私泄露以及全链条身份校验与调用鉴权复杂性增加等四类风险。国际上，Android、iOS等主流操作系统虽已建立较为成熟的权限管理框架，但均未涵盖智能体、技能调用、工具编排等人工智能场景下的权限管理需求，系统化的标准规范尚属空白。

为落实《智能体规范应用与创新发展实施意见》相关要求，指导企业及相关方规范开展人工智能操作系统权限管理能力的设计、开发与测评，制定该指导性技术文件，围绕身份鉴别与管理、权限体系、权限全生存周期管理、权限审计等方面提出系统化要求，为产业合规发展提供标准支撑。

（三）起草过程

2026年4月，标准项目启动，开展可行性研究。

2026年5月15日，电子标准院组织召开专题研讨会，成立标准研制组。

2026年6月2日，电子标准院组织召开标准研讨会，小米、华为、中兴通讯、麒麟、统信等40余家单位近70位专家参加，天翼云、麒麟、荣耀、摩尔线程、中移苏研、华为、蚂蚁、腾讯、小米、快手等单位会上提出18条标准意见。

2026年6月2日至6月9日，参考各单位6月2日提出的18条标准意

见，形成标准立项草案初稿，并申请标准立项。

2026年6月12日，标准正式立项，标准计划号为20263106-Z-469，并公开征集标准参编单位，共收到80余家单位的参编申请，组建标准编制组。

2026年6月12至6月17日，收集标准完善意见，电子标准院对天翼云、深开鸿、中兴、南大、vivo、上海文镭、上海超多元子、中移苏研8家单位反馈的67条标准意见进行预处理。

2026年6月18日，电子标准院组织召开标准集中研讨会，电子标准院、小米、荣耀、蚂蚁、中兴、天翼云、华为、OPPO、vivo、腾讯、统信、中移苏研共12家单位的18位专家参加会议，讨论处理天翼云、深开鸿、中兴、南大、vivo、上海文镭、上海超多元子、中移苏研8家单位会前反馈的67条标准意见以及会上提出意见，形成标准框架和分工修改安排。

2026年6月19至6月29日，中移苏研、统信、OPPO、华为、小米、天翼云、中兴、vivo、荣耀分工修改标准，腾讯、统信、OPPO、北交4家单位反馈了20条标准意见。

2026年6月30日，电子标准院组织召开标准集中研讨会，电子标准院、麒麟、统信、小米、荣耀、中兴、天翼云、华为、OPPO、vivo、腾讯、北京交大共12家单位的21位专家参加会议，讨论处理腾讯、统信、OPPO、北交4家单位会前反馈的20条标准意见，以及会上提出的5条标准意见，形成分工修改建议。

2026年7月1日至7月15日，电子标准院、华为、vivo、荣耀、OPPO、小米、天翼云、中兴分工修改标准，腾讯、南大、中移苏研、中兴、统信5家单位反馈了58条标准意见，电子标准院进行预处理。

2026年7月16日,电子标准院组织召开标准集中研讨会,电子标准院、腾讯、华为、vivo、天翼云、荣耀、OPPO、中兴、统信、中移苏研、小米、蚂蚁共12家单位的21位专家参加会议,讨论处理腾讯、南大、中移苏研、中兴、统信5家单位会前反馈的58条标准意见,以及会上提出的6条标准意见,进行讨论分析和分工修改建议。

2026年7月16日至7月28日,电子标准院、华为、vivo、荣耀、OPPO、小米、天翼云、中兴分工修改标准,腾讯、麒麟、中兴3家单位反馈了55条标准意见,电子标准院进行预处理。

2026年7月29日,组织召开标准研讨会,电子标准院、腾讯、vivo、华为、中兴、天翼云、麒麟、统信、荣耀、小米、蚂蚁共11家单位18名专家现场会议,2026年7月31日,组织召开标准线上研讨会,中兴、华为、天翼云、vivo、OPPO、腾讯、麒麟、统信软件、中移苏研、荣耀、中国电子标准院、蚂蚁科技共12家单位23名专家线上会议,讨论处理腾讯、麒麟、中兴3家单位会前反馈的55条标准意见,形成分工修改建议。

2026年7月24日至7月31日,收到标准编制组33家单位反馈的369条意见。

2026年8月,组织召开标准研讨会,对369条标准意见进行讨论处理,并修改完善标准文本,形成征求意见稿和征求意见稿编制说明。

二、国家标准编制原则、主要内容及其确定依据

(一) 标准编制原则

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。标准在编写过程中遵循“面向市场、服务行业、科学适用”的原则,参考国内先进经验,贯彻国家相关政策要求,

给出人工智能操作系统权限管理的具体要求，助力人工智能操作系统产业健康发展。

标准研制过程中鼓励人工智能操作系统上下游产业链以及相关产学研用单位共同参与，讨论方式公开透明，以保障条款具有普适性，为人工智能操作系统生产商、智能体开发商、应用软件开发商提供统一指导和技术参考。

（二）标准主要内容

该标准确立了人工智能操作系统权限管理框架和原则，规定了人工智能操作系统对身份管理、权限体系、权限管理、权限审计等要求。

该标准适用于人工智能操作系统的设计、开发、测评，也可为智能体、技能、工具等人工智能应用的权限管理设计与开发提供参考和指导。

（三）标准编制依据

（1）人工智能操作系统权限管理的特殊性

传统操作系统的权限管理主要面向应用软件，管控粒度局限于对特定系统资源的静态访问授权。人工智能操作系统引入了智能体这一全新主体，其权限管理面临三重特殊性：一是智能体具备自主感知、决策和执行能力，权限需求无法在安装时预判，需动态授权与实时监控支撑；二是智能体的数据处理深度远超传统应用，权限管控需延伸至记忆、向量索引、云端同步等新型数据形态；三是智能体可被用户委托代为处理权限请求，在便捷性与安全保障之间需审慎平衡。基于上述特殊性，该标准在传统框架基础上，针对性地增加了智能体身份管理、动态授权与委托、AI能力使用权限分类、多智能体协同权限管理等要求，构建了适配人工智能操作系统特点的权限管理体系。

（2）与政策法规的衔接

该标准编制过程中，重点参考了《智能体规范应用与创新发展实施意见》，将其关于厘清决策边界、限定权限范围的核心要求转化为标准条款。

（3）前期研究成果与实践经验

该标准充分参考了产业界成熟的权限管理实践（如Android的权限分级机制、iOS的隐私授权框架），在“普通、敏感、高危”三级分级体系的基础上，将管控范围从传统应用权限扩展至AI能力使用权限，将授权方式从静态的一次性授权扩展至支持单次、限期、精准、可委托的动态授权体系，将管理对象从单一的应用拓展至智能体、应用、技能、工具等多角色统一纳管。

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

该标准充分吸纳了国内人工智能操作系统厂商的实践经验，以及上下游产业链、用户单位的反馈意见。各起草单位结合自身操作系统产品，对权限分级分类、智能体身份核验、动态授权与委托、权限调用异常检测等核心条款进行了可行性验证，标准技术内容与产业实际相契合。

四、与国际、国外同类标准技术内容的对比情况

国际上尚无专门针对人工智能操作系统权限管理的标准规范。Android与iOS的权限管理框架主要面向传统应用的静态授权，未覆盖智能体、技能调用、工具编排等AI场景下的动态权限管理需求。该标准结合国内产业实践，围绕AI场景下的权限管理关键环节进行了规范，以期为该领域标准化工作提供参考。

五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因

该标准未采用相关国际标准。

六、与有关相关法律法规、规章及相关标准的协调性

与现行法律法规以及相关标准协调一致。

七、重大分歧意见的处理经过和依据

无。

八、涉及专利的有关说明

标准不涉及专利、版权和著作权等知识产权问题。

九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

建议发布后尽快实施标准，并在报批阶段同步开展培训宣贯、应用推广工作。

十、其它应予说明的事项

无。

《人工智能操作系统权限管理要求》标准编制组

2026年8月4日