



中华人民共和国国家标准化指导性技术文件

GB/Z 300—2026

人工智能操作系统权限管理要求

Permission management requirements for artificial intelligence
operating system

2026-09-24 发布

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 权限管理原则 2

6 身份管理 3

 6.1 身份标识与鉴别 3

 6.2 权限配置 3

 6.3 身份数据隔离 3

7 权限体系 3

 7.1 概述 3

 7.2 权限分级 4

 7.3 权限管理范围 4

 7.4 授权方式 5

8 权限管理 5

 8.1 权限声明 5

 8.2 权限申请 6

 8.3 权限授予 6

 8.4 权限调用 6

 8.5 权限撤销 8

 8.6 权限配置管理 8

9 权限审计 8

 9.1 审计范围 8

 9.2 审计分析 8

 9.3 审计处置 9

 9.4 日志格式 9

 9.5 日志存储 9

 9.6 日志访问 9

附录A(资料性) 权限清单 10

附录B(资料性) 权限应用指南 15

参考文献 17

前 言

本文件为规范类指导性技术文件。

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。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：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、北京兴云数科技术有限公司、上海文镒信息科技有限公司、南京大学、北京健康有益科技有限公司、上海师范大学天华学院、成都理工大学、招商局重庆交通科研设计院有限公司、深城交科技集团股份有限公司、北京凝思软件股份有限公司、上海超多元子人工智能科技有限公司、元心信息科技集团有限公司、福建省标准化研究院、云从科技集团股份有限公司、中国船舶集团有限公司第七一六研究所、星尘智能(深圳)人工智能科技股份有限公司、北京东土科技股份有限公司、中移(杭州)信息技术有限公司、上海零数众合信息科技有限公司、青岛酷特智能股份有限公司、海光信息技术股份有限公司、深圳润迅人工智能科技有限公司、浦江国家实验室、中科慧拓(北京)科技有限公司、政达研学(雄安)科技有限公司、公安部第三研究所、鼎桥技术有限公司、深圳市证通电子股份有限公司、北京百度网讯科技有限公司、浙江数智交院科技股份有限公司、进迭时空(北京)科技有限公司、北京交通大学、中铁建工集团有限公司、国家工业信息安全发展研究中心、北京未来式智能科技有限公司、武汉模态跃迁科技有限公司、中国人民解放军 32008 部队、中科海微(北京)科技有限公司、合肥市包河区中安数字经济与公共安全研究院、海信视像科技股份有限公司、湖南麒麟信安科技股份有限公司、中电数据产业集团有限公司、浪潮计算机科技有限公司、北京国科环宇科技股份有限公司。

本文件主要起草人：王威伟、苗宗利、焦廉洁、董建、杨磊、薛志宏、史浩、孟眉、王键、姚一楠、李腾、马承青、唐杨、张希璐、高歌、李晨、商家奇、蒋彪、方强、李鹤、张胜举、李辰淑、魏刚、徐立锋、谢南淦、李根、冯京润、刘海涛、李永强、赵晓娜、刘刚、袁婷婷、仲凯韬、王楚豫、李宇欣、吕博、程晗蕾、骆中斌、许建荣、李晓宇、夏梦、陈鑫、李海晏、杨显森、陈学兵、魏遵博、梁华煜、张婷婷、兰春嘉、李海滨、展恩果、隋成龙、裴芝林、张科、苏蕾权、宋好好、黄晋飞、曾培恒、孙鑫洋、王益维、杨庄媛、汪群博、生兆亮、许智鑫、杨劲松、丁震宇、唐乐乐、公衍林、王军、纪开虎、赵敏敏、顾延甲、刘圣金、刘志立、鞠炜刚、潘宏博、冯洋、裴实、郑宁、叶青、胡芳侨、刘晶鹏、李东旭、王凯龙、杨文涵、叶培铭、杨珍、张伟琦、胡晴鹤、王和俊、林艳辉、董睿、安佳勇、赵博、周鑫羽、张宏伟、石勇、丁浩。

引 言

随着人工智能与智能体技术快速发展,人工智能操作系统作为模型调度、硬件管理与智能体运行的基础底座,其权限管理体系直接关乎系统安全、隐私保护与服务水平。操作系统向人工智能操作系统演进过程中,主体类型从单一应用扩展为应用、智能体、工具、技能等多主体的协作,主体间呈现动态协作、级联调用与自主决策等新特征。面向多主体协作的权限分级体系、授权方式及全生存周期管理机制对人工智能操作系统的权限管理提出了更高要求,特别是在智能终端和个人应用场景下,用户需要多种应用、智能体,亟需构建与之相适应的权限管理体系。

本文件在通用操作系统权限管理能力要求基础上,增加了面向智能终端和个人应用的人工智能场景下应用、智能体、工具、技能的权限管理要求,权限管理相关技术能力需要硬件等资源支撑,具体实现时可根据应用场景及设备环境进行裁剪,与 GB/Z 299 配合使用。

人工智能操作系统权限管理要求

1 范围

本文件确立了面向智能终端和个人应用场景的人工智能操作系统权限管理原则,规定了人工智能操作系统(以下简称“操作系统”)的身份管理、权限体系、权限管理、权限审计等要求。

本文件适用于面向智能终端和个人应用场景的人工智能操作系统的设计、开发、测试,也为应用、智能体等权限申请与使用提供参考和指导。

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/Z 299 人工智能操作系统通用技术要求

GB/T 41867 信息技术 人工智能 术语

3 术语和定义

GB/T 41867 和 GB/Z 299 界定的以及下列术语和定义适用于本文件。

3.1

权限 permission

对一个或多个操作系统资源执行某个操作的许可。

[来源:GB/T 25062—2010,3.4,有修改]

3.2

权限管理 permission management

依据安全策略,对主体访问操作系统资源行为进行全过程管理的机制。

注:包括权限的声明、申请、授予、调用、监测、变更、撤销和审计等。

3.3

身份鉴别 identity authentication

证实一个实体所声称身份的过程。

[来源:GB/T 39786—2021,3.8]

3.4

授权 authorization

根据预先认可的安全策略,赋予主体可实施相应行为权限的过程。

[来源:GB/T 25069—2022,3.559]

3.5

安全策略 security policy

为保护操作系统安全和用户数据隐私而制定的一系列规则、规范和流程。

注:安全策略是权限管理和授权决策的依据。