



中华人民共和国国家标准化指导性技术文件

GB/Z 299—2026

人工智能操作系统通用技术要求

General technical requirements for artificial intelligence operating system

2026-09-24 发布

国家市场监督管理总局
国家标准化管理委员会 发布

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 人工智能操作系统框架 2

6 内核要求 2

7 AI运行库要求 3

8 AI服务要求 3

 8.1 感知服务 3

 8.2 交互服务 3

 8.3 模型管理 4

 8.4 智能体管理 4

 8.5 工具管理 4

 8.6 技能管理 5

 8.7 上下文管理 5

 8.8 记忆管理 5

 8.9 跨设备协同 6

 8.10 数据服务 6

9 系统智能体要求 6

 9.1 智能化能力 6

 9.2 调用能力 7

 9.3 系统管理能力 8

10 智能体开发套件要求 8

11 AI安全要求 8

 11.1 权限管理 8

 11.2 身份鉴别 8

 11.3 智能体运行安全 9

 11.4 工具安全 9

 11.5 技能安全 9

 11.6 沙箱安全 9

11.7 模型安全 9

11.8 行为审计 9

参考文献 11

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、华为终端有限公司、中兴通讯股份有限公司、小米通讯技术有限公司、统信软件技术有限公司、天翼云科技有限公司、OPPO 广东移动通信有限公司、麒麟软件有限公司、中移(苏州)软件技术有限公司、维沃移动通信有限公司、荣耀终端股份有限公司、北京兴云数科技术有限公司、上海文镭信息科技有限公司、南京大学、成都理工大学、深城交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、北京凝思软件股份有限公司、北京健康有益科技有限公司、福建汇思博数字科技有限公司、鼎桥技术有限公司、元心信息科技集团有限公司、联想(北京)有限公司、招商局重庆交通科研设计院有限公司、上海师范大学天华学院、北京东土科技股份有限公司、青岛酷特智能股份有限公司、云从科技集团股份有限公司、政达研学(雄安)科技有限公司、海光信息技术股份有限公司、深圳开鸿数字产业发展有限公司、上海零数众合信息科技有限公司、海信视像科技股份有限公司、福建省标准化研究院、北京百度网讯科技有限公司、深圳润迅人工智能科技有限公司、湖南麒麟信安科技股份有限公司、星尘智能(深圳)人工智能科技股份有限公司、上海超多元子人工智能科技有限公司、深圳市证通电子股份有限公司、北京交通大学、中科慧拓(北京)科技有限公司、公安部第三研究所、中移(杭州)信息技术有限公司、浦江国家实验室、普华基础软件股份有限公司、浙江数智交院科技股份有限公司、中铁建工集团有限公司、中科海微(北京)科技有限公司、国家工业信息安全发展研究中心、进迭时空(北京)科技有限公司、北京宝兰德软件股份有限公司、北京国科环宇科技股份有限公司、浪潮计算机科技有限公司、中国人民解放军 32008 部队、上海新榜信息技术股份有限公司、广州哆啦科技有限公司。

本文件主要起草人：王威伟、焦廉洁、苗宗利、董建、杨磊、张希璐、史浩、孟眉、刘东、胡冲、李建慧、王磊、马承青、唐杨、姜少涛、李腾、郭爽、张胜举、高立发、徐曼、王键、谢南淦、徐立锋、刘海涛、李鹤、刘铭然、李根、张超、李永强、曹宇琼、李辰淑、高歌、李晨、商家奇、刘小锐、仲凯韬、王楚豫、程晗蕾、许建荣、孔祥营、李晓宇、李宇欣、邱熠龙、黄晋飞、陈鑫、郭一平、骆中斌、郑宁、梁华煜、李海滨、杨显森、苏蕾权、展恩果、陈强、兰春嘉、纪开虎、李海晏、孙鑫洋、隋成龙、赵敏敏、魏遵博、夏梦、曾培恒、汪群博、张科、宋好好、江文则、裴芝林、梁浩、王益维、生兆亮、公衍林、许智鑫、杨庄媛、詹年科、刘志立、刘圣金、唐乐乐、沈涓、刘海军、梁天善、冯洋、王森、黄浩然、李斯琦、叶青、吕博、周翔、张伟琦、杨珍、张宏伟、董睿、胡晴鹤、石勇、杨文涵、夏瑞麟、安佳勇、曹思玮、肖旭、王和俊、胡尊凤、赵博、周鑫羽、吕皓。

引 言

当前,随着大模型、智能体等人工智能技术加速突破,面向智能终端和个人应用场景的人工智能操作系统市场迎来前所未有的发展机遇。人工智能正驱动智能终端操作系统加快向人工智能操作系统演进,在继承 CPU、内存、存储等传统硬件资源抽象和进程管理能力的基础上,将 AI 算力、模型、智能体、工具、技能等作为新型管理对象,面向终端用户提供面向智能任务的原生调度与协同能力,推动操作系统从“资源管理者”向“智能调度中枢”跃升,其角色定位、能力边界与生态逻辑正在被重新定义。然而,人工智能操作系统技术及标准化工作处于起步阶段,业界对其内涵外延、功能架构、演进方向尚未形成共识,亟需强化行业引导,防控安全风险,促进操作系统产业高质量发展。

操作系统在向人工智能操作系统演进中,除了具备传统操作系统的基础能力外,还具备自底向上的 AI 能力。本文件不定义传统操作系统的基础能力,仅对具备人工智能特性的关键能力进行规范,移动通信终端、微型计算机、便携式微型计算机、平板式微型计算机、可穿戴设备、车载终端等的操作系统功能根据自身硬件能力进行相应调整。本文件与 GB/Z 300 配合使用。

人工智能操作系统通用技术要求

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框架,规定了内核、AI 运行库、AI 服务、系统智能体、智能体开发套件和 AI 安全的要求。

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设计、开发、测试等,也为智能终端系统及智能化应用的设计、开发、测试提供参考。

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 300 人工智能操作系统权限管理要求

GB/T 41867 信息技术 人工智能 术语

3 术语和定义

GB/T 41867 界定的以及下列术语和定义适用于本文件。

3.1

操作系统 **operating system**

用于管理硬件资源、控制程序运行、提供人机界面,并为应用软件提供支持的一种系统软件产品。

[来源:GB/T 36630.3—2018,3.1,有修改]

3.2

人工智能操作系统 **artificial intelligence operating system**

使用人工智能技术进行资源管理、任务调度和安全管理,并提供智能体等智能化软件所需运行环境的操作系统。

注:人工智能操作系统各项功能的实现以硬件为条件,当硬件具备相应能力时,人工智能操作系统实现对应功能。

3.3

智能体 **AI agent**

感知环境,并主动采取行动以实现特定目标的实体。

注 1:本文件中的智能体特指人工智能智能体,一般为软件系统。

注 2:具备感知、认知、执行、记忆、学习等功能。

[来源:GB/Z 185.1—2026,3.1,有修改]

3.4

系统智能体 **system AI agent**

人工智能操作系统的组成部分,具备任务分发、资源调度、系统管理等功能的智能体。

3.5

工具 **tool**

被按需调用,用于执行特定操作或获取特定信息的软件功能单元。