



中华人民共和国国家标准化指导性技术文件

GB/Z XXXXX—XXXX

人工智能操作系统权限管理要求

Artificial intelligence operating system permission management requirements

（征求意见稿）

（在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上）

XXXX – XX – XX 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 V

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 3

5 权限管理框架和原则 3

 5.1 权限管理框架 3

 5.2 权限管理原则 4

6 身份管理 4

7 权限体系 5

 7.1 概述 5

 7.2 权限分级 5

 7.3 权限管控范围 5

 7.4 授权方式 6

8 权限管理 6

 8.1 权限声明 6

 8.2 权限申请 7

 8.3 权限授予 7

 8.4 权限调用 7

 8.5 权限撤销 8

 8.6 权限配置管理 8

9 权限审计 9

 9.1 审计项目 9

 9.2 审计分析 9

 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 10

附录 A（资料性）权限清单 11

附录 B（资料性）权限应用指南 16

 B.1 概述 16

 B.2 应用权限管理 16

 B.3 智能体 16

 B.4 应用聚合平台 16

 B.5 应用商店 16

参考文献 18

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。

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、南京大学、北京交通大学

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、唐杨、张希璐、马承青、高歌、李晨、蒋彪、方强、李鹤、张胜举、李辰淑、魏刚、汪群博、冯洋、徐立锋、谢南淦、李根、冯京润、刘海涛、李永强、赵晓娜、刘刚、安佳勇

引 言

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操作系统整体安全防护能力、个人隐私保护水平以及智能化服务底线。2026年5月8日，国家网信办、国家发展改革委、工业和信息化部联合印发《智能体规范应用与创新发展实施意见》，提出要厘清仅限用户本人决策、需由用户授权决策和智能体自主决策等各种决策方式的合理边界及所需权限，智能体执行操作不得超出用户授权范围。传统操作系统以静态权限列表为基础，无法有效管控智能体在执行复杂任务时的权限需求，暴露出越权访问或权限滥用、自动化操作失控、数据过度采集甚至隐私泄露等安全风险。因此，研制人工智能操作系统权限管理、智能体调用等相关标准，可为产业合规发展提供标准支撑。

人工智能操作系统权限管理要求

1 范围

本文件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。

本文件适用于人工智能操作系统（以下简称“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。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

人工智能终端 smart terminal

具备主动感知理解、多模态交互、智能化服务和学习进化等能力，完成特定任务的终端产品。

注1：智能化任务处理流程一般涉及感知、规划、决策、执行、学习等环节。

注2：人工智能终端由软件和硬件组成，软件部分包括人工智能模型、智能化应用、操作系统、用户界面、端云协同接口等；硬件部分包括通信模块、处理器、内部存储、外围输入/输出(IO)器件、显示等。

注3：本文件主要指移动终端、微型计算机等产品，可穿戴、机器人等不同设备可进行相应裁剪。

[来源：GB/Z 177.1—2026, 3.1]

3.2

人工智能操作系统 artificial intelligence operating system

融合大模型、智能体等人工智能技术，具备感知、规划、执行、记忆、学习等智能化服务能力的系统软件。

注：人工智能操作系统负责对人工智能终端的软硬件资源、异构算力资源、数据资源、任务执行进行管理、调度与安全控制，为应用、智能体等分配资源，并提供资源访问接口与运行环境支撑。

3.3

智能体 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、交互、执行、决策、记忆能力，能够理解用户意图、持续学习优化自身行为。

[来源：GB/Z 185.1—2026: 3.1, 有修改]

3.4

系统智能体 system agent

是人工智能操作系统的重要组成部分，获取操作系统信息，具备任务分发、资源调度、系统管理等能力的智能体。

3.5

应用智能体 application agent

用户安装部署，满足用户在特定场景或业务应用的智能体。

3.6

权限 permission

对操作系统的硬件资源、数据、功能或服务进行特定操作的许可。

3.7

权限管理 permission management

依据安全策略，对主体访问操作系统资源的权限进行声明、申请、授予、校验、使用监控、变更、撤销和审计的全过程管理机制。

3.8

身份鉴别 identity authentication

验证主体所声明身份真实性的过程。

3.9

授权 authorization

依据安全策略、用户意愿和上下文信息，对已通过身份鉴别的主体授予访问特定客体并执行特定操作权限的过程。

3.10

安全策略 security policy

为保护操作系统安全和数据隐私而制定的一系列规则、规范和流程，是权限管理和授权决策的依据。

3.11

上下文信息 context information

与主体、客体或环境相关的动态信息，如时间、地点、用户行为、设备状态、网络环境（整个交互过程中的输入输出）等，可用于动态决策。

3.12

动态授权 dynamic authorization

根据上下文信息和风险评估结果，实时调整主体权限的授权方式。

3.13

权限审计 permission audit

对主体的权限授予、变更、使用和回收过程进行记录、分析和追溯的活动，用于发现未授权访问和权限滥用行为，满足合规要求。

3.14

工具 tool

用于执行特定操作或服务、硬件驱动程序或软件模块。

[来源：ISO/IEC 23000-15: 2016, 3.5.4, 有修改]

3.15

技能 skill

向智能体注入领域知识、工作流程或工具使用规范的结构化指令单元，由入口文件（SKILL.md）及可选的配套文件组成。

3.16

应用（软件） application (software)

运行在操作系统之上，用于满足用户在特定业务域或应用场景下的具体需求，而非解决计算机系统自身运行管理问题的软件，包括操作系统预置应用、可安装应用以及免安装等，其中免安装应用主要包括快应用（3.17）、小程序（3.18）和网页应用。

3.17

快应用 quick application

基于行业统一标准开发，内置于移动终端操作系统，采用前端技术栈开发、原生渲染，无需下载安装即可即点即用，具备接近原生应用性能体验和系统能力调用权限的轻量级应用软件。

3.18

小程序 mini application

运行在特定宿主应用提供的标准化运行时环境中，采用前端技术栈开发、原生渲染，无需下载安装即可即点即用，具备完整应用生存周期和丰富系统能力调用权限的轻量级应用软件。

3.19

应用聚合平台 application convergence platform

集成原生应用、快应用、小程序、网页应用等多形态应用软件，提供统一搜索、分发、运行、管理与服务入口的综合性软件平台，可以是操作系统内置组件、独立的应用软件或软件模块。

3.20

用户 user

使用计算机系统、终端设备、应用软件、智能体及相关服务，并与之发生交互的自然人或代表自然人行使权利的法人、其他组织。

3.21

用户数据 user data

用户在使用各类信息系统、终端设备、应用软件、智能体及相关服务过程中，主动提供、被系统收集或通过分析推导得出的，能够单独或与其他信息结合识别特定用户身份的数据集合。

注：主要包括：

- 1) 用户主动提供的数据：如身份信息、联系方式、账号信息、用户生成内容等。
- 2) 系统被动收集的数据：如设备信息、位置信息、操作日志、交互记录、网络信息等。
- 3) 通过分析推导得出的数据：如用户偏好、行为特征、兴趣标签、消费习惯等，包括人工智能模型加工生成的用户个人特征数据。

3.22

标识 identifier

与数字、非数字或抽象实体（如图书、图像、报告、元数据记录或事件）关联的字符序列。

[来源:ISO 24619: 2011(en), 3.2.1]

注：本文特指用于在操作系统环境中区分用户、智能体、应用、技能、工具、设备等且具有唯一性的标识。

4 缩略语

以下缩略语适用于本文件。

AI: 人工智能 (Artificial Intelligence)

API: 应用程序接口 (Application Programming Interface)

CPU: 中央处理器 (Central Processing Unit)

GPS: 全球定位系统 (Global Positioning System)

GPU: 图形处理器 (Graphics Processing Unit)

GUI: 图形用户界面 (Graphical User Interface)

IMEI: 国际移动设备识别码 (International Mobile Equipment Identity)

IP: 网际协议 (Internet Protocol)

IoT: 物联网 (Internet of Things)

NFC: 近场通信 (Near Field Communication)

NPU: 神经网络处理器 (Neural Processing Unit)

PISA: 持久标识与可持续访问 (Persistent Identification and Sustainable Access)

UI: 用户界面 (User Interface)

VPN: 虚拟专用网络 (Virtual Private Network)

WAP: 无线应用协议 (Wireless Application Protocol)

Wi-Fi: 无线保真 (Wireless Fidelity)

WLAN: 无线局域网 (Wireless Local Area Network)

5 权限管理框架和原则

5.1 权限管理框架

人工智能操作系统权限管理框架见图1。

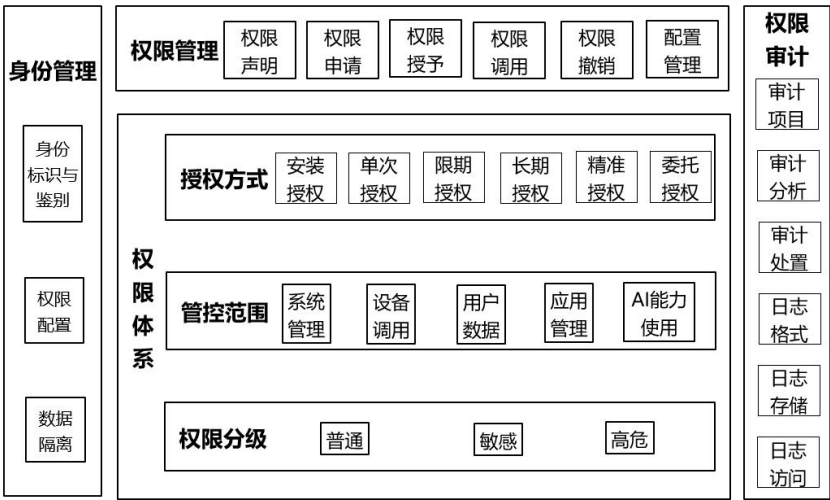


图 1 人工智能操作系统权限管理框架图

5.2 权限管理原则

本文件规定的人工智能操作系统权限管理原则如下。

- a) 最小必要原则：系统权限设计拆分，操作方式细化，以便仅授予应用、智能体、工具及技能完成其任务所必需的最小操作权限，实现精细、灵活、智能化权限管控。
- b) 安全隔离原则：实现不同用户、不同应用、不同智能体、不同技能、不同安全级别数据之间的有效隔离，智能体调用技能、工具及应用时进行权限边界隔离，防止权限传递和越权访问。
- c) 用户知情同意原则：涉及用户隐私和敏感权限的授权，告知用户授权的目的、范围、方式和期限，并获得用户明确同意；任何主体不得强制或绕过用户授权执行操作。

6 身份管理

6.1 身份标识与鉴别

操作系统身份标识与鉴别应符合下列要求：

- a) 操作系统应为每个用户账号分配唯一的账号标识，并在其生存周期内保持不变；
- b) 操作系统应基于用户标识进行用户身份鉴别，并基于其身份标识进行访问控制；
- c) 操作系统应识别部署在本系统上的智能体、技能、工具等并为其分配标识，标识应与包名、命名空间、部署路径等建立映射关系，并在生存周期内唯一且不变；
- d) 操作系统应为多版本、分身、实例等分配不同的标识；
- e) 标识在生存周期结束后自动回收；
- f) 用户级智能体、技能与工具的标识仅在当前用户下有效；
- g) 跨用户全局智能体、全局技能、全局工具标识在所有用户下有效。

6.2 权限配置

操作系统权限配置应符合下列要求：

- a) 操作系统应基于用户账号标识对该账号访问权限进行配置；
- b) 操作系统应基于智能体、技能、工具的标识运行权限配置、以及访问与被访问权限标记；
- c) 系统审计与日志应与标识建立映射关系。

6.3 数据隔离

操作系统数据隔离应符合下列要求：

- a) 不同用户间的个人数据、应用缓存及系统配置在逻辑层或物理层完全隔离；
- b) 不同用户对应用、智能体、技能、工具和云端服务的授权状态应相互隔离；
- c) 除用户明确授权外，不应继承、复用或推断其他用户的授权配置；
- d) 对应用可执行文件、系统资源文件及应用运行时产生的缓存数据进行分区存储，并配置差异化的文件系统挂载选项；
- e) 为运行中的应用分配独立的安全沙箱环境，并通过强制访问控制实现隔离；
- f) 应用与智能体不应访问其他应用或智能体的私有目录与文件；
- g) 提供统一的系统资源访问接口，应用不应直接修改或访问系统配置文件与系统分区；
- h) 提供用户数据迁移接口，迁移操作经当前活跃用户显式授权，迁移后的数据归属关系与目标用户绑定，确保数据隔离状态不被破坏。

7 权限体系

7.1 概述

根据权限开放可能带来的风险程度，将权限划分为普通、敏感、高危三级。根据开放的资源类型，可将权限管控的范围划分为系统管理、设备调用、用户数据获取、应用管理、AI能力使用五类。操作系统权限级别划分及对应的管控方式见附录A。

注：本文件只针对经由用户开放给应用、智能体申请的权限进行分类。

7.2 权限分级

权限分为三级，具体包括：

- a) 普通权限：不涉及用户个人信息、系统安全，未经用户授权的访问对用户权益和系统运行无实质影响，如修改音频输出设置、连接网络等；
- b) 敏感权限：涉及用户个人信息、设备硬件的敏感功能，未经用户授权的访问可能导致用户数据泄露或造成用户权益的损害，如打开摄像头、定位等；
- c) 高危权限：涉及用户个人信息获取、终端全局控制或跨应用访问的功能实现，未经用户授权的访问可能会对用户个人信息、用户权益、设备安全、系统稳定造成较大损害，如麦克风常驻监听、输入法全局键击、悬浮窗、录屏等。

7.3 权限管控范围

7.3.1 系统管理

针对操作系统级服务、功能进行使用、配置：

- a) 基础配置：与操作系统基本交互所需要的基础资源，如运行调度、事件获取、UI 修改、设置通知策略等；
- b) 服务注册使用：使用系统服务或注册为系统服务，如无障碍服务、输入法、VPN、默认应用等；
- c) 系统安全与策略：悬浮窗、修改系统设置、批量管理文件等。

7.3.2 设备调用

针对终端硬件设备相关资源进行访问、控制：

- a) 通信：调用电话、信息，连接或使用蓝牙、NFC、WLAN、移动通信网络等；
- b) 音视频采集：打开摄像头、麦克风等；
- c) 传感器：获取设备内置加速度、陀螺仪等传感数据；
- d) 设备绑定：外部设备查找、绑定、读写等；
- e) 生物特征使用：使用设备指纹、人脸进行认证。

7.3.3 用户数据

针对用户个人信息进行访问和操作：

- a) 通信数据：读写通话记录、通讯录、短信、彩信等；
- b) 文件访问：读写用户私有目录照片、音频、视频、文档等；

- c) 剪切板：读写系统剪切板；
- d) 行程数据：读写日历中行程安排、提醒等信息；
- e) 健康数据：读取个人心率、计步、体重、体质等运动健康服务数据；
- f) 位置数据：低精度定位、高精度定位、后台定位等获得的用户位置。

7.3.4 应用管理

对终端上应用进行管理、控制及跨应用交互，包括：

- a) 应用管理，应用安装/卸载，应用使用情况统计、读取已安装应用列表等；
- b) 启动控制，应用自启动、创建快捷方式、关联启动等；
- c) 跨应用交互，使用应用与智能体声明并对外开放的 API 方式进行调用。

7.3.5 AI 能力使用

上层应用、智能体使用终端 AI 能力：

- a) 端侧模型部署：允许应用、智能体在端侧部署自定义模型；
- b) 模型推理调用：利用终端模型能力完成端侧或端云侧推理过程；
- c) 智能体调用，通过智能体管理服务查询安装的智能体清单，并使用智能体交互接口进行调用；
- d) 技能调用，通过技能管理服务查询安装的技能清单，调用应用与智能体等封装并开放的技能进行调用；
- e) 工具调用，通过工具管理服务查询安装的工具清单，调用应用与智能体封装并开放的工具服务接口进行调用；
- f) AI 配置：修改系统模型或智能体配置从而影响服务能力，如个性化记忆，用户数据使用等。

7.4 授权方式

授权方式分类如下：

- a) 安装授予。操作系统在主体安装或首次调用时自动授予权限、无需用户决策的授权方式。
- b) 单次授权。由用户通过交互界面授予主体，在单次任务或单次使用中访问资源的权限，应在主体完成单次任务或退出后自动失效，主体再次使用应重新申请授权。

注1：交互界面包括图形、语音等。

- c) 限期授权。由用户通过交互界面授予主体，在使用时或预先限定的时间范围内访问资源的权限，有效期届满后权限自动失效，主体再次使用应重新申请授权。

注2：“使用中允许”是限期授权的一种，表示在应用退出后，授权自动失效。

- d) 长期授权。由用户通过交互界面授予主体，在用户主动撤销前持续有效的权限的授权方式，宜支持用户将长期授权降级为单次授权或限期授权。
- e) 精准授权。由用户通过交互界面授予主体，限定数据、文件等的访问范围、精度或操作类型，仅授予完成功能所需的最小数据或操作，支持用户随时调整，并可降级至更小范围。

注3：数据范围如访问选定的照片、选定的联系人等非全量数据，数据精度如提供低精度位置而非高精度位置等，操作类型如前台使用而非后台使用等。

- f) 委托授权。由用户授权系统智能体按照预置规则或用户习惯，对应用和应用智能体运行中的动态权限申请进行单次授予或拒绝，以提高智能化交互体验；单次委托授权不改变系统默认的授权规则。

8 权限管理

8.1 权限声明

操作系统应建立权限声明机制，允许应用与智能体通过安装包或应用商店等方式声明其所需权限清单等，并符合下述要求：

- a) 操作系统应对应用和智能体权限声明给出统一格式，包括权限标签、权限组、权限类别、权限简明用途说明等核心信息。

注：操作系统可通过应用软件安装包等扩展权限声明。

- b) 操作系统对未按统一的格式和规范提交权限声明的应用和智能体，可拒绝授予不符合规范的权限；
- c) 应用和智能体首次安装时，操作系统应展示其所需敏感权限清单及简单用途说明等，供用户审阅确认；
- d) 应用和智能体升级时，操作系统应展示其新增敏感权限清单及简单用途说明等，供用户审阅确认。

8.2 权限申请

操作系统应建立运行时权限动态申请机制，允许应用或智能体运行中根据任务需要申请权限声明中已列出的敏感权限：

- a) 应用和智能体申请权限时，操作系统应向用户展示所申请权限及简单用途说明，由用户进行确认；
- b) 应给出多种授予选项，如本次允许、使用中允许、本次拒绝、使用中拒绝等，单次授权不改变系统默认的授权规则；
- c) 操作系统应管控权限申请频次，单次运行期内，对同一权限被用户多次拒绝后重复多次申请的，应支持用户选择不再提示；
- d) 对于禁用的权限，发起权限申请时，应给出提示并提供快捷跳转方式供用户进行权限配置；
- e) 系统应记录权限申请与处理记录，包括申请主体、时间、系统默认处理方式、用户处理方式、权限处理规则变更等供用户查阅。

8.3 权限授予

操作系统应依据权限安全风险等级和权限应用特点设计权限授予方式：

- a) 普通权限应采用安装即授予的方式。
- b) 敏感权限宜采用运行时授予的方式：
 - 1) 敏感权限不宜采用长期授权方式；
 - 2) 敏感权限可采用单次授权、预设时间的限期授权、精准授权等权限授予方式，应向用户提供明确授权选项，由用户选择；
 - 3) 可将单次授权或用户上次选择作为敏感权限的授权页面的默认推荐选项；
 - 4) 可建立机制由用户设置权限委托策略，允许系统智能体在预设范围、期限、场景和风险等级的条件内，辅助处理其他应用和智能体对敏感权限的请求，涉及超出预设条件的敏感权限授权仍应由用户确认。
- c) 高危权限授予的主体或组件应通过操作系统身份校验：
 - 1) 高危权限不宜采用长期授权方式；
 - 2) 如需用户确认方式授权的高危权限，应非直接确认授权方式授权，避免由于误操作带来损失；
 - 3) 高危权限不得采用委托系统智能体授权方式。
- d) 对用户数据文件的选取等，操作系统宜提供精准授权方式授权用户数据、文件读写操作。
- e) 多智能体协作模式下，操作系统宜支持按任务单次授予权限。

8.4 权限调用

8.4.1 权限调用实时监控

操作系统应建立权限使用实时监控机制，对权限的申请、授予、调用、撤销等行为进行全流程的监测：

- a) 监控内容包括主体身份标识、权限操作类型、操作目标资源、操作时间戳等；
- b) 对于超出软件核心功能所需权限之外的权限申请可给予用户安全风险提示；
- c) 应对通讯录、麦克风、相机、位置、剪切板等权限在用状态进行提示；
- d) 宜为智能体的访问权限、调用范围、调用流程提供校验机制，防范违规调用；
- e) 宜具备对批量权限操作、跨域权限调用、智能体调用技能和工具，多技能编排执行等特殊场景的监测能力；

- f) 宜具备对智能体及应用中嵌套智能体权限调用行为监控能力;
- g) 监测结果同步推送至权限管理控制台, 支持可视化展示权限调用状态、异常预警信息及监控统计数据, 便于用户快速掌握权限使用动态。

8.4.2 异常权限调用检测

操作系统应建立异常权限调用检测机制, 并符合下列要求。

- a) 应预设异常权限使用检测规则, 包括越权操作、权限滥用、敏感权限高频异常调用、非活跃时段操作、权限传递、技能私自联动越权等。
- b) 支持自动识别批量权限变更、高频异常调用、连续长期未使用权限、越权访问未授权资源、智能体跨技能违规调用、模型超范围读取数据等异常行为。
- c) 智能体协同监测到异常行为时, 应对级联智能体、技能、工具的权限进行告警或提示, 必要时可冻结相关权限。
- d) 宜结合权限归属、资源敏感等级、操作行为特征、上下文信息等维度, 构建多维度权限异常检测模型。
- e) 宜基于风险影响因子(如权限的敏感程度、调用频次与基线偏差、调用时段与场景合理性、涉及数据量级、历史安全事件关联度等)建立风险分级制度, 针对检测到的异常权限使用行为, 自动触发分级响应机制:
 - 1) 低风险异常: 如连续长期未使用权限等, 记录异常信息, 告知用户, 持续跟踪检测, 并在权限调用记录中标记提示。
 - 2) 中风险异常: 如高频异常调用等, 暂停权限执行并经用户手动确认, 经用户确认后方可恢复。
 - 3) 高风险异常: 如访问用户未授权的资源、批量违规授权等, 自动临时冻结或收回违规权限、阻断异常操作或锁定相关账号等, 同步向用户、管理员推送风险提示, 同时触发全局安全告警。
- f) 支持动态迭代优化, 结合历史权限使用数据、安全事件案例、最新威胁情报及业务场景变化, 定期更新检测阈值与判定逻辑, 提升异常识别的准确率与适应性。

8.4.3 权限使用记录

操作系统应建立权限使用记录体系, 对权限调用行为进行记录, 并符合下列要求:

- a) 记录内容包括权限调用的主体身份、权限调用时间、权限名称、调用结果。
- b) 应提供调用行为记录数据保护机制, 防止调用行为记录数据库被恶意删除、篡改, 第三方移动应用软件不能访问调用行为记录的原始数据库文件。
- c) 支持多维度查询与统计分析, 可按调用主体、时间、权限、调用结果等维度快速检索, 宜生成权限使用合规性报告、异常行为统计报告等, 为权限管理优化与安全审计提供数据支撑。
- d) 宜与操作系统审计模块对接, 实现记录数据的同步归集与统一管理, 促进审计工作可高效开展和第三方审计与内部安全核查要求。

8.5 权限撤销

操作系统应建立权限撤销机制, 包括用户主动撤销和权限自动撤销机制:

- a) 用户主动撤销机制, 允许用户对已经授予应用或智能体的权限进行逐项撤销;
- b) 权限自动撤销机制, 对符合预设撤销条件的权限进行自动回收, 权限自动撤销的触发条件包括权限有效期届满、任务项目完成、主体身份角色失效、安全风险等级升高、连续长期未使用权限、技能下架、技能禁用、技能过期及主体注销等;
- c) 权限撤销后, 应同步回收权限主体对目标资源的相关权限, 同时更新权限配置信息并清除内存中的缓存数据, 再次使用时, 重新提示用户授予;
- d) 宜具备单项权限集中临时撤销能力, 用户主动撤销某项权限后, 所有依赖该权限的应用、智能体授权失效, 恢复权限后, 所有依赖该权限的应用、智能体自动恢复对该权限的使用;
- e) 权限自动撤销前可提示用户, 包括撤销时间、撤销权限范围及撤销原因等。

8.6 权限配置管理

操作系统应提供统一的权限配置管理入口，允许用户权限进行集中查看与配置：

- a) 应支持用户按敏感权限维度逐项对应用与智能体的权限配置，包括但不限于拨打电话、通话记录、通讯录、短信、系统通知、位置、摄像头、麦克风、运动传感器，以及已安装的应用、智能体、技能和工具的列表等；
- b) 应支持用户按应用或智能体维度查看和修改其被授予的所有权限；
- c) 对于高危权限，应提供独立配置入口，并在授予时对潜在风险进行提示；
- d) 系统应记录权限申请与处理记录，包括系统默认处理方式、用户处理方式、权限处理规则变更等供用户查阅。

9 权限审计

9.1 审计项目

操作系统应对权限全生存周期进行审计并生成审计日志，并符合下列要求。

- a) 对用户创建、变更、注销、身份认证、权限绑定、角色变更、账号锁定解锁等全流程操作记录审计日志；
- b) 对权限申请、授予、变更、撤销、过期等全生命周期操作记录审计日志；
- c) 对审计日志访问、导出等操作记录审计日志。

9.2 审计分析

操作系统权限审计分析能力符合下列要求：

- a) 应支持按主体、客体、时间、操作类型、操作结果、风险等级等维度聚合分析，全面掌握权限使用情况；
- b) 应支持校验权限分配是否符合最小权限原则，以及权限范围、目的、使用频次是否超过功能实现的合理需求等进行合规检查，并给出风险警示；
- c) 宜支持基于历史权限使用基线实现异常行为自动评分定级、关联分析等智能研判。

9.3 审计处置

应具备处置机制，并符合下列要求：

- a) 分级响应：区分权限使用异常的严重程度实施差异化处置，一般异常仅发送告警通知；严重异常自动触发权限临时冻结或收回，并向用户发出提示。
- b) 处置闭环：权限审计响应处置包括告警、研判、处置、整改、复核、归档等环节，确保问题处置完整可追溯。
- c) 复盘改进：支持对典型权限使用异常事件复盘并形成案例，更新权限策略与审计规则，优化权限管控流程，防范同类问题复发。

9.4 日志格式

审计日志格式应符合下列要求：

- a) 审计记录包括事件类型、事件发生的时间、触发事件的主体与客体的标识及名称、事件成功或失败等字段；
- b) 网络会话事件审计记录还包括网络程序名称、协议类型、源 IP 地址、目的 IP 地址、源端口、目的端口等字段；
- c) 智能体审计记录包括智能体标识、智能体操作、技能调用、技能版本、调用指令、模型编号模型操作等。

9.5 日志存储

审计日志存储符合下列要求：

- a) 审计日志应存储在掉电非遗失性存储介质中；
- b) 审计日志留存期限宜不少于 180 天，未达到法规要求或预设留存期限的审计日志不应被覆盖或删除；

- c) 应具备访问控制与写入约束，如权限隔离、文件系统不可变属性、哈希链式校验等措施，防止日志被非授权篡改和删除；
- d) 存储空间达到设定容量阈值时，应优先清理已超过规定留存期限的审计日志，对于尚未超过留存期限的审计日志，应进行压缩归档处理，防止审计事件意外丢弃；
- e) 应提供审计日志的轮转机制，支持按存储容量阈值或时间周期自动触发日志轮转；
- f) 当审计日志存储空间写满且存在未到期日志时，系统应触发告警通知，并视情况暂停非核心业务操作，直至管理员完成日志归档或存储空间扩容。

9.6 日志访问

审计日志访问应符合下列要求：

- a) 保护审计日志不被未授权访问；
- b) 保护审计日志不被非授权篡改和删除。

附 录 A
(资料性)
权限清单

表A.1列出了常见权限清单、分级、授予方式等，操作系统可根据部署与应用场景进行裁剪、扩充、合并。仅运行环境配备相应设备或系统具备相应业务数据时，操作系统需建立相应的权限体系。

表 A.1 常见权限清单、分级、授予方式

大类	权限/tools	权限分级	管控范围	授予方式	权限说明	适用场景
通讯录	读取联系人	敏感	用户数据	用户确认：单次/长期/不允许		移动设备
	写/删除联系人	敏感	用户数据	用户确认：单次/长期/不允许		
	查找设备上账号	敏感	用户数据	用户确认：单次/长期/不允许	允许应用获取你手机上已添加的所有账号列表	
电话	呼叫转移	敏感	设备调用	用户确认：单次/长期/不允许	允许应用查询、设置或管理设备的呼叫转移功能	移动设备
	发起多方通话	敏感	设备调用	用户确认：单次/长期/不允许	允许应用发起或管理一个多方通话	
	接听来电	敏感	设备调用	用户确认：单次/长期/不允许	接听/拒绝来电	
	读取电话号码	敏感	设备调用	用户确认：单次/长期/不允许	读取本机电话号码	
	获取手机识别信息	敏感	设备调用	用户确认：单次/长期/不允许	读取设备 ID、网络及通话状态	
	拨打电话	敏感	设备调用	用户确认：单次/长期/不允许	允许应用直接拨出电话	
日历	读取日程表	敏感	用户数据	用户确认：单次/长期/不允许		全端设备
	修改/添加日程表	敏感	用户数据	用户确认：单次/长期/不允许		
通话记录	读取通话记录	敏感	用户数据	用户确认：单次/长期/不允许		移动设备
	写/删除通话记录	敏感	用户数据	用户确认：单次/长期/不允许		
	重新设置外拨电	高危	用户数据	用户确认：单次/	查看即将拨打	

	话的路径			长期/不允许	的电话号码,并有权将其修改为其他号码或完全中止这次通话	
信息	读取短信/彩信	敏感	用户数据	用户确认: 单次/长期/不允许		移动设备
	写/删除短信/彩信	敏感	用户数据	用户确认: 单次/长期/不允许		
	接收 WAP 信息	敏感	消息通知	用户确认: 单次/长期/不允许		
	接收彩信	敏感	消息通知	用户确认: 单次/长期/不允许		
	接收短信	敏感	消息通知	用户确认: 单次/长期/不允许		
	发送短信	敏感	消息通知	用户确认: 单次/长期/不允许		
	发送彩信	敏感	消息通知	用户确认: 单次/长期/不允许		
闹钟	设置闹钟	普通	用户数据	默认授予		移动设备
	锁屏时弹出全屏界面	普通	消息通知	默认授予		
照片/视频	读取图片或视频文件	敏感	用户数据	用户确认: 单次/长期/不允许		全端设备
音乐/音频	读取音频文件	敏感	用户数据	用户确认: 单次/长期/不允许		全端设备
	控制/修改音频设置	普通	设备调用	默认授予		
文件	访问文件	普通	用户数据	用户确认: 单次/长期/不允许	如邮件中添加附件,需要开启该权限	全端设备
	删除/修改文件	敏感	用户数据	用户确认: 单次/长期/不允许		
相机	拍照/摄像	敏感	设备调用	用户确认: 单次/长期/不允许	允许应用直接访问摄像头硬件,进行拍照或录像	全端设备
应用操作	应用安装	敏感	应用操作	用户确认: 单次/长期/不允许		全端设备
	应用卸载	敏感	应用操作	用户确认: 单次/不允许		
	应用升级	敏感	应用操作	用户确认: 单次/		

				不允许		
	读取已安装应用列表	普通	应用操作	用户确认：单次/长期/不允许		
	应用自启动	高危	应用操作	用户确认：单次/长期/不允许		
	截屏/录屏	高危	应用操作	用户确认：单次/长期/不允许		
	无障碍服务	高危	应用操作	用户确认：单次/长期/不允许		移动设备
传感器	识别身体活动	敏感	设备调用	用户确认：单次/长期/不允许	通过设备的传感器(如加速度计、陀螺仪)识别用户当前的身体活动(如步行、骑车或驾车)	移动设备
	身体传感器	敏感	设备调用	用户确认：单次/长期/不允许	访问设备身体传感器(如心率监测器、血氧传感器等)的权限	移动设备
	位置	敏感	设备调用	用户确认：单次/长期/不允许	获取设备的高精度实时位置,如GPS	移动设备
	Wi-Fi 开/关	敏感	设备调用	用户确认：单次/长期/不允许	开关Wi-Fi	全端设备
	与附近的WLAN设备互动	敏感	设备调用	用户确认：单次/长期/不允许	允许应用执行下列与附近Wi-Fi设备相关的操作:发现与连接、发起连接、管理热点	移动设备
	蓝牙扫描设备、被设备发现、连接已配对设备	敏感	设备调用	用户确认：单次/长期/不允许		全端设备
	NFC 开/关	敏感	设备调用	用户确认：单次/长期/不允许		移动设备
Internet	上网	普通	设备调用	默认授予	允许应用打开网络套接字,进行网络通信	全端设备
通知	显示通知	敏感	消息通知	用户确认：单次/长期/不允许	允许应用向用户推送通知消息	全端设备
送话器	录音	敏感	设备调用	用户确认：单次/长期/不允许	允许应用访问设备的送话器,录制音频	全端设备

系统管理	执行系统命令	高危	技能调用	用户确认：单次/长期/不允许	执行 Shell 脚本、启动/停止服务、运行 Python 分析	全端设备
	管理进程	高危	技能调用	用户确认：单次/长期/不允许		
	运行代码	高危	技能调用	用户确认：单次/长期/不允许		
文件系统	读取文件	敏感	技能调用	用户确认：单次/长期/不允许	读、写、编辑文件、列出文件/文件夹清单、根据模式匹配查找文件，如 <code>**/*.ts</code> ，应用代码补丁	全端设备
	写入文件	敏感	技能调用	用户确认：单次/长期/不允许		
	编辑文件	敏感	技能调用	用户确认：单次/长期/不允许		
	列出目录中的文件和文件夹	敏感	技能调用	用户确认：单次/长期/不允许		
	文件查找	普通	技能调用	默认授予		
	应用补丁	敏感	技能调用	用户确认：单次/长期/不允许		
网络	执行网络搜索	普通	技能调用	默认授予	查找最新资料、抓取网页信息、监控社交媒体动态	全端设备
	获取网页内容	普通	技能调用	默认授予		
	搜索社交媒体	普通	技能调用	默认授予		
浏览器	操作和控制浏览器会话	普通	技能调用	默认授予	自动填写表单、进行网页截图、执行复杂的网页交互	全端设备
	实现浏览器自动化	普通	技能调用	默认授予		
消息交互	聊天渠道（如微信等）自动操作	敏感	技能调用	用户确认：单次/长期/不允许	让 AI 智能体在聊天软件中自动回复、发送通知	全端设备
智能体管理	检查会话状态	敏感	技能调用	用户确认：单次/长期/不允许	管理长对话、拆分复杂任务、协调多个 AI 智能体共同工作	全端设备
	委派工作给予智能体	敏感	技能调用	用户确认：单次/长期/不允许		
	管理多智能体协作	敏感	技能调用	用户确认：单次/长期/不允许		
媒体	生成图片	普通	技能调用	默认授予	根据描述生成插图、制作短视频、将文本转为语音输出	全端设备
	生成视频	普通	技能调用	默认授予		
	文本转语音	普通	技能调用	默认授予		
记忆	智能体长期记忆搜索信息	敏感	技能调用	用户确认：单次/长期/不允许	让 AI 记住用户偏好、回顾历史	全端设备

					对话关键信息	
	获取特定的记忆内容	敏感	技能调用	用户确认：单次/长期/不允许		
	更新工作记忆	敏感	技能调用	用户确认：单次/长期/不允许	将当前任务的进度和关键信息持久化到短期记忆中	
	写入长期记忆	敏感	技能调用	用户确认：单次/长期/不允许	将成功的经验“晶化”为可复用的技能，存入长期记忆	
会话管理	列出所有会话	敏感	技能调用	用户确认：单次/长期/不允许		全端设备
	读取特定会话的历史记录	敏感	技能调用	用户确认：单次/长期/不允许		
	向另一个会话发送消息	敏感	技能调用	用户确认：单次/长期/不允许		
	为后台任务生成一个独立的子会话	敏感	技能调用	用户确认：单次/长期/不允许		
	让出当前会话的控制权	敏感	技能调用	用户确认：单次/长期/不允许		
	用于控制和管理子智能体	敏感	技能调用	用户确认：单次/长期/不允许		
	检查当前会话的状态	敏感	技能调用	用户确认：单次/长期/不允许		
节点控制	控制已配对的设备（如 IoT 设备、手机等）	敏感	技能调用	用户确认：单次/长期/不允许	控制智能家居、与移动设备交互	全端设备

附录 B

(资料性)

权限应用指南

B.1 概述

附录B给出了权限管理相关方的实施建议，以促进权限管理体系的落实与应用生态互通。

本文件所述的应用、智能体、应用聚合平台，均是指部署并运行在当前操作系统软件，运行于云侧的软件不适用。

B.2 应用权限管理

应用（含系统预置应用、用户安装应用、快应用）的权限应用遵循以下原则：

- a) 仅根据自身核心功能需求申请对应权限，不申请与功能无关的敏感权限、高危权限；
- b) 不因部分非核心权限缺失而拒绝提供基础服务，保障用户正常使用权益；
- c) 不通过隐蔽、欺诈等手段诱导用户授予权限；
- d) 权限使用过程中明确说明权限用途，不静默调用敏感权限；
- e) 开放应用编程接口（API）并进行工具化封装，为智能体调用提供支撑；
- f) 对调用行为主体进行身份校验，拒绝非法调用、超范围调用及恶意调用。

B.3 智能体

系统智能体权限应用遵循以下原则：

- a) 参照 B.2 进行权限申请与使用；
- b) 建立用户数据授权有效期制度，明确授权默认有效期，有效期届满后，自动清除已获取的所有用户数据（含本地缓存、临时存储），若继续使用用户数据，再次向用户提交申请并获得明确授权；
- c) 建立数据存储加密规范，形成端云一体的数据安全防护体系，数据传输采用端到端加密方式，防范数据传输、存储过程中的泄露风险；
- d) 未经用户明示许可，不将用户个人数据（含用户画像记忆）用于扩展用途，如 AI 模型训练、第三方共享等，不得擅自泄露、篡改用户数据；
- e) 优先通过操作系统提供的智能体管理服务、技能管理服务、工具管理服务等，查询部署在操作系统上的智能体、技能和工具，并通过其描述的接口调用规范进行调用；
- f) 智能体与工具、智能体与应用、智能体与技能之间基于协议进行调用的过程中携带自身身份标识，确保调用行为可追溯；
- g) 全面留存权限申请与调用日志，以及智能体、技能、工具的调用日志，确保行为可追溯。

B.4 应用聚合平台

应用聚合平台权限应用遵循以下原则：

- a) 参考本文建立完善的身​​份鉴别、权限定义、授权管理、权限审计、日志管理能力，实现对平台内所有应用（含快应用、小程序）、技能的权限统一管控；
- b) 对平台内所有应用运行存储空间进行隔离，默认不直接互访；
- c) 平台不得将自身获得授权绕过用户授权传给平台内应用；
- d) 对平台内应用、技能的权限申请、使用情况进行实时监控，发现违规申请、越权使用等行为及时拦截、告警，必要时采取限制使用、下架等处置措施；
- e) 留存平台内所有应用的权限操作、身份鉴别、异常处置等日志，日志留存期限不少于 180 天，满足审计与追溯需求。

B.5 应用商店

应用商店权限应用遵循以下原则：

- a) 建立涵盖应用、智能体、技能的分发管理体系；
- b) 开展权限审核，确认应用、智能体、工具、技能的权限申请与使用符合本文件要求；
- c) 应用和智能体安装或升级时，展示其所需敏感权限清单及用途说明等，供用户审阅确认；
- d) 建立监测体系，对违规申请、越权使用等行为进行告警，必要时可采取下架等处置措施。

参 考 文 献

- [1] GB/Z 177.1—2026 人工智能终端智能化分级 第1部分：参考框架
 - [2] GB/Z 185.1—2026 人工智能 智能体互联 第1部分：总体架构
 - [3] ISO/IEC 23000-15: 2016 Information technology—Multimedia application format (MPEG -A)
—Part 15: Multimedia preservation application format
 - [4] ISO 24619: 2011 Language resource management — Persistent identification and sustainable access (PISA)
 - [5] GM/T 0002 SM4分组密码算法
 - [6] GM/T 0003 (所有部分) SM2椭圆曲线公钥密码算法
 - [7] GM/T 0004 SM3密码杂凑算法
-