ICS 33.050
CCS M 30

团 体 标 准

T/GDBX 107—2025

智能体任务执行安全要求

Security requirements for task execution of artificial intelligence agent

2025－06－13 发布　　2025－06－13 实施

广东省标准化协会　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。

本文件由广东省标准化协会提出并归口。

本文件起草单位：北京邮电大学、中国联合通信集团股份有限公司、天翼安全科技有限公司、联想（北京）有限公司、北京数牍科技有限公司、广州虎牙科技有限公司、广东省标准化协会。

本文件主要起草人：徐国胜、王晨宇、李朝霞、刘金春、康和、陶宏芝、金银玉、曾雅静、张山红。

智能体任务执行安全要求

1 范围

本文件确立了智能体任务执行安全原则，提出了智能体任务授权、任务协作、任务运行、用户权益保护要求等内容。

本文件适用于提供智能体开发和运营的各类主体。

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 25069 信息安全技术 术语

GB/T 42884 信息安全技术 移动互联网应用程序（App）生命周期安全管理指南

ISO/IEC 22989 信息技术 人工智能 人工智能概念和术语(Information technology - Artificial intelligence - Artificial intelligence concepts and terminology)

3 术语和定义

GB/T 25069、GB/T 42884界定的以及下列术语和定义适用于本文件。

3.1

智能体 artificial intelligence agent

能够感知和响应环境并能执行操作以完成其目标的自动化实体。

注：本文件仅指运行在移动智能终端、PC终端、智能可穿戴设备上由终端厂商或应用厂商提供的、涉及与第三方APP协作完成任务的智能体。

[来源：ISO/IEC 22989:2022，3.1.1，有修改]

3.2

应用软件 application

运行在智能终端上向用户提供信息服务的应用软件。

注1：智能终端包括移动智能终端、PC终端以及智能耳机、智能手表等可穿戴设备。

注2：简称App。

[来源：GB/T 42884—2023，3.2，有修改]

4 安全原则

4.1 告知同意

智能体应向用户明确告知任务执行所申请的操作系统权限、访问用户数据的目的、处理方式和潜在影响等内容，并获得用户同意。

4.2 目的限制

应确保智能体只能操作授权范围内的资源，限制不必要的任务执行能力，以减少潜在的安全风险。

4.3 公平公正

应确保智能体任务决策算法公平、公正、透明及可解释，准确执行用户意图，不应利用技术优势干扰用户选择第三方 App 或其他智能体完成任务。

4.4 双重授权

智能体在进行用户意图识别、通过第三方App执行任务时，应先通过第三方App授权，并在获得用户授权后执行。

5 安全要求

5.1 权限授予要求

智能体权限授予要求，包括但不限于：

a) 智能体应遵循“告知同意”原则，向用户明确告知任务执行所申请的操作系统权限、访问用户数据的目的、处理方式和潜在影响等内容，并获得用户同意；
b) 智能体应仅申请任务执行所必须的最小权限，权限开通必须经过用户明确授权；
c) 智能体在任务执行中需获取新的系统权限或用户数据，应再次告知用户并获得用户同意；
d) 应向用户提供权限管理的统一界面，允许用户随时查看、调整或撤销某些权限。

5.2 任务协作要求

智能体任务协作要求，包括但不限于：

a) 智能体应通过标准化接口调用的方式与第三方 App 协作完成任务，并确保接口调用安全，防止接口被未经授权访问；
b) 智能体在进行用户意图识别、通过第三方 App 执行任务时，应严格遵循“双重授权”原则，即先通过第三方 App 授权，并在获得用户授权后执行，双重授权流程可参照附录 A；
c) 智能体不得利用无障碍权限或操作系统技术优势操作第三方 App 完成任务。

5.3 任务运行要求

智能体任务运行要求，包括但不限于：

a) 智能体应遵循“目的限制”原则，确保只能操作授权范围内的资源，限制不必要的任务执行能力，以减少潜在的安全风险；
b) 智能体应采取安全措施防止任务执行能力被恶意利用，如作为网络攻击的工具；
c) 智能体在任务运行时，应确保具有容错能力，防止智能体行为对用户软硬件设备造成破坏，如设置异常停止机制；
d) 智能体应遵循“公平公正”原则，确保任务决策算法公平、公正、透明及可解释，准确执行用户意图，不应利用技术优势干扰用户选择第三方 App 或其他智能体完成任务；

示例1：用户通过智能体安装下载第三方 App 时，智能体强制用户选择指定应用商店或者干扰用户选择其他应用商店。

示例2：用户通过智能体唤起第三方 App 时，智能体对唤起第三方 App 设置不公平的推荐、排名等。

e) 应确保智能体任务运行可控，允许用户随时修改、终止任务或者进行人工接管。

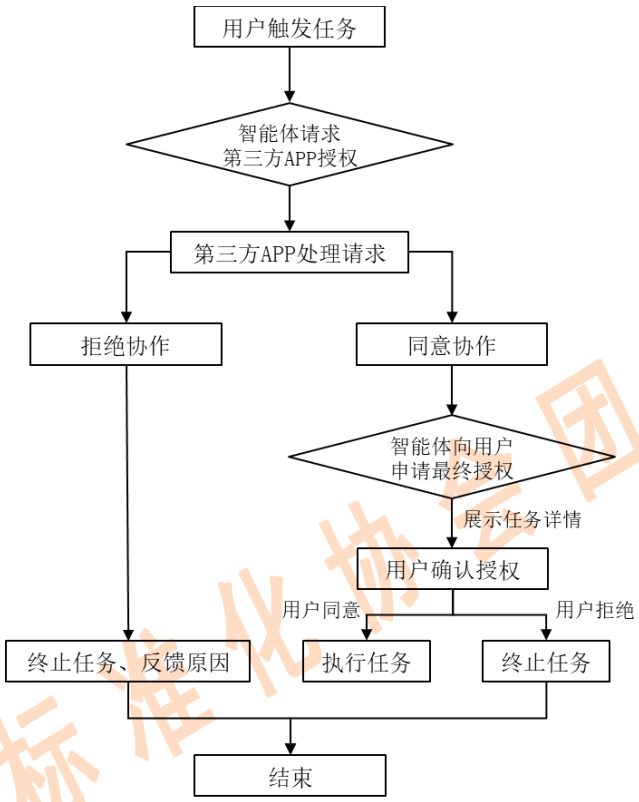
5.4 用户权益保护要求

用户权益保护要求，包括但不限于：

a) 智能体应确保用户数据安全，仅收集和处理完成任务所必需的数据，向用户明确告知收集数据的目的及处理方式并获得用户同意，涉及向第三方共享数据、将用户个人信息上传云端处理的需额外说明；
b) 智能体通过麦克风、截屏、录屏、共享屏幕等权限获取数据资源时，不得侵害用户及其他主体的数据权益，第三方 App 有权拒绝不合理操作以保护用户权益；
c) 应建立安全管理机制，确保智能体在开发、部署、升级迭代等全生命周期安全；
d) 应建立应急预案，在智能体任务执行发生数据泄露或权限滥用事件时能够快速响应和处置；
e) 应建立有效的用户投诉和反馈机制，及时解决智能体任务执行安全问题。

附 录 A
（资料性）
双重授权流程

双重授权流程图见图A.1。



双重授权流程说明：

用户触发任务——用户通过界面操作或指令启动需要第三方APP协作的任务；

智能体请求第三方APP授权——智能体向第三方APP发出协作请求，请求第三方APP授权；

第三方APP处理请求：

同意协作——返回同意，进入下一步；

拒绝协作——终止任务，反馈原因；

智能体向用户申请最终授权——智能体向用户展示任务详情，请求用户确认授权；

用户确认授权：

用户同意——执行任务；

用户拒绝——终止任务。

图A.1 双重授权流程图

参 考 文 献

[1] GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求
[2] T/SIA 050—2025 移动互联网服务可访问性安全要求
[3] 中华人民共和国个人信息保护法
[4] 中华人民共和国数据安全法