ICS 33.050
M 30

团 体 标 准

T/TAF 004-2017

Android 应用权限调用开发者指南

Developer Guide for Android Application Permission

2017-05-22 发布 2017-06-01 实施

电 信 终 端 产 业 协 会 发 布

目　　次

前言 II
Android 权限调用开发者指南 1
1 范围 1
2 Android 权限使用背景 1
3 Android 系统权限机制 1
3.1 权限级别 2
3.2 权限组 2
3.3 权限申请、调用、系统管理方式 2
4 Android 权限详情 3
4.1 Dangerous 级别权限 3
4.2 Normal 级别权限 9
4.3 其他级别权限 20
5 Android 系统权限使用建议 20
5.1 Dangerous 级别权限 22
5.2 Normal 级别权限 31
5.3 其他级别权限 42

前　　言

本标准按照 GB/T 1.1-2009给出的规则编写。

本标准是为了缓解Android应用滥用系统权限的情况，规范开发者正确使用系统权限，制定Android权限调用开发者指南。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院

本标准主要起草人：高立发、林瑞杰、傅蓉蓉、曹宇琼、李美慧、颜媚、曾晨曦、苏畅

Android 权限调用开发者指南

1 范围

本标准规定了开发者调用Android系统权限的使用建议。

本标准适用于Android平台应用开发者。

2 Android 权限使用背景

由于Android的开发策略，越来越多的终端厂商和互联网厂商入到Android阵营，Android应用的数量飞速增长。Android系统具有进程沙箱管理机制，应用使用沙箱之外的资源和功能时，需要向系统申请权限。事实上，Android系统向开发者开发了非常多系统权限，其中许多权限涉及重要的手机功能和用户数据。是否授予各项权限的权利交给了普通的手机用户，只要是用户允许，Android系统不会对系统权限的使用进行限制。

一些涉及用户隐私的敏感权限开放后，如果被恶意应用加以利用，用户数据面临泄露的风险。另一方面，由于一些开发者对系统权限的了解不够深入，可能在开发应用的过程中会向系统申请一些本来不需要的权限。有些申请的权限在应用运行过程中并没有使用，而有些申请的权限可以通过调用系统自身功能的方式规避。这种情况下的权限滥用，对使终端用户本身是无害的，但仍可能对用户产生不必要的困扰。

互联网数据中心联合360手机卫士发布的《2016年Android手机隐私安全报告》显示，非游戏类App获取隐私权限普遍增加。其中，获取“位置信息”权限的App比例由76.8%增加到91.7%；获取“访问联系人”权限的App比例由33.7%增加到49.0%；获取“读取短信记录”权限的App比例由25.5%增加到46.2%。而这其中，越界使用权限的情况依然非常严重。越界获取权限指App在自身功能不必需的情况下获取某些权限的行为。而在对用户的调研中，94.6%的用户认为Android手机是存在隐私安全隐患的设备，而App获取隐私权限用途不明是导致用户担心的首要原因。

研究显示，针对功能相近的应用，普通用户会有限选择使用权限较少的。而根据应用商店的数据统计，许多开发者也在有意识地减少隐私权限的使用。可见，加强对权限的了解和规范，对开发者和普通用户都是非常有意义的。基于以上背景，为了缓解Android应用滥用系统权限的情况，规范开发者正确使用系统权限，需要制定Android权限调用开发者指南。

3 Android 系统权限机制

3.1 权限级别

Android系统把权限分为不同的保护级别，其中最长用的权限保护级别为normal和dangerous。官方认为normal级别的权限风险较低，系统在安装的时候默认进行授权；dangerous级别的权限风险较高，需要用户明确对应用进行授权。Normal和dangerous级别的权限是普通开发者主要使用的两类权限，也是本课题重点讨论的内容。

常用权限级别列举如下：

（1）normal：权限保护级别默认值，低风险权限，系统默认授权，不需要用户明确授权。

（2）Dangerous：高风险权限，Android系统不默认授权，需要用户确认。

（3）Signature：与声明权限的应用具有相同证书的应用，Android系统自动授权，否则拒绝。

（4）SignatureOrSystem：与声明权限的应用具有相同证书的应用，或者系统应用，Android系统自动授权，否则拒绝。

3.2 权限组

从Android6.0开始，针对dangerous级别的权限，系统以权限组的方式进行管理。Dangerous级别的权限在应用安装时不进行授权，在权限使用时，系统弹出授权窗口供用户选择。授权窗口中的内容显示为应用对该权限所在权限组的申请，如果用户选择授权，则是对权限所在权限组的授权。以PHONE权限组为例，如果应用同时申请了READ_PHONE_STATE、CALL_PHONE、READ_CALL_LOG三个权限，在用户对READ_PHONE_STATE权限授权的同时，应用相应地获得了CALL_PHONE和READ_CALL_LOG权限。

Dangerous权限组列举如下：

权限组	权限
CALENDAR	READ_CALENDAR、WRITE_CALENDAR
CAMERA	CAMERA
CONTACTS	READ_CONTACTS、WRITE_CONTACTS、GET_ACCOUNTS
LOCATION	ACCESS_FINE_LOCATION、ACCESS_COARSE_LOCATION
MICROPHONE	RECORD_AUDIO
PHONE	READ_PHONE_STATE、CALL_PHONE、READ_CALL_LOG、WRITE_CALL_LOG、ADD_VOICEMAIL、USE_SIP、PROCESS_OUTGOING_CALLS
SENSORS	BODY_SENSORS
SMS	SEND_SMS、RECEIVE_SMS、READ_SMS、RECEIVE_WAP_PUSH、RECEIVE_MMS
STORAGE	SEND_SMS、RECEIVE_SMS、READ_SMS、RECEIVE_WAP_PUSH、RECEIVE_MMS

3.3 权限申请、调用、系统管理方式

Android权限使用和管理方式简述如下：

（1）在AndroidManifest.xml中配置需要使用的权限。

（2)Normal权限在应用安装时自动授权,应用直接使用;Dangerous级别权限不在应用安装时授权，需要动态申请，授权后才能使用。

（3）Android6.0以后，针对dangerous级别权限Android系统以权限组方式进行授权和管理。

4 Android 权限详情

Google官方文档中提供的权限列表中截止到Android7.1.1版本，一共有140个权限，其中normal级别的权限有34个，dangerous级别权限有24个。除了少量已经弃用的权限外，其余为signature或system|signature级别的权限。针对signature和system|signature级别的权限，根据官方定义是不能被第三方应用使用的，多数权限也在文档中注明仅供系统应用使用，因此不在本指南的讨论范围之内。需要特别说明的是，SYSTEM_ALERT_WINDOWS和WRITE_SETTINGS权限，虽然保护级别为signature，实际上是可以被第三方App使用的，官方文档中也做了特殊说明。因此，本指南也将这两个权限包含在内。

4.1 Dangerous 级别权限

4.1.1 CALENDAR

4.1.1.1 READ_CALENDAR

权限名称	READ_CALENDAR
Constant Value	android.permission.READ_CALENDAR
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用读取用户日历数据。该权限可以让应用读取手机上的所有日历活动，分享和保存日历数据，而不论这些数据是否属于机密或敏感内容。	

4.1.1.2 WRITE_CALENDAR

权限名称	WRITE_CALENDAR
Constant Value	android.permission.WRITE_CALENDAR
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用写入用户日历数据。该权限可以让应用添加、删除、更改用户手机上的活动。该权限可让应用冒充日历所有者发送消息，或在所有者不知情的情况下修改活动。	

4.1.2 CAMERA

4.1.2.1 CAMERA

权限名称	CAMERA
Constant Value	android.permission.CAMERA
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用使用照相设备。该权限可以让应用随时使用相机拍摄照片和视频，而无需用户的确认。	

4.1.3 CONTACTS

4.1.3.1 READ_CONTACTS

权限名称	READ_CONTACTS
Constant Value	android.permission.READ_CONTACTS
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用读取用户联系人数据。该权限可以让应用读取用户手机上存储的联系人的相关数据，包括通过打电话、发送电子邮件或以其他方式与特定个人通信的频率。该权限可让应用保存联系人数据，而恶意应用可能会在用户不知情的情况下分享联系人数据。	

4.1.3.2 WRITE_CONTACTS

权限名称	WRITE_CONTACTS
Constant Value	android.permission.WRITE_CONTACTS
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用写入用户联系人数据。该权限可以让应用修改用户手机上存储的联系人的相关数据，包括用户通过打电话、发送电子邮件或以其他方式与特定个人通信的频率。该权限可以让应用删除联系人数据。	

4.1.3.3 GET_ACCOUNTS

权限名称	GET_ACCOUNTS
Constant Value	android.permission.GET_ACCOUNTS
引入、弃用情况	API1 引入
保护级别	Dangerous

是否供第三方 App 使用	是
基本情况：	
访问手机中的帐户列表。（API23 开始，如果 App 与账户管理者使用相同签名，访问账户是则无需该权限。）	

4.1.4 LOCATION

4.1.4.1 ACCESS_FINE_LOCATION

权限名称	ACCESS_FINE_LOCATION
Constant Value	android.permission. ACCESS_FINE_LOCATION
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用访问精确位置。该权限可以让应用通过全球定位系统（GPS）或网络位置信息源（例如基站和 WLAN）获取用户的精确位置信息。	

4.1.4.2 ACCESS_COARSE_LOCATION

权限名称	ACCESS_COARSE_LOCATION
Constant Value	android.permission.ACCESS_COARSE_LOCATION
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用访问粗略位置信息。该权限获取用户的大致位置信息。这类位置信息来自于使用网络位置信息源（例如基站和 WLAN）的位置信息服务。	

4.1.5 MICROPHONE

4.1.5.1 RECORD_AUDIO

权限名称	RECORD_AUDIO
Constant Value	android.permission.RECORD_AUDIO
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用录制音频。该权限可让应用不经用户确认即可随时录制音频。	

4.1.6 PHONE

4.1.6.1 READ_PHONE_STATE

权限名称	READ_PHONE_STATE
Constant Value	android.permission.READ_PHONE_STATE
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用读取手机状态，包括手机的号码、当前蜂窝网络信息、正在进行的通话信息（是否正处于通话状态以及拨打的号码）、以及手机上注册的账户列表。	

4.1.6.2 CALL_PHONE

权限名称	CALL_PHONE
Constant Value	android.permission.CALL_PHONE
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用直接拨打某个电话号码，不需要用户通过拨号用户界面确认。该权限可以让应用在用户未执行任何操作的情况下拨打电话号码。恶意应用可通过拨打电话产生相关费用，而无需用户确认。	

4.1.6.3 READ_CALL_LOG

权限名称	READ_CALL_LOG
Constant Value	android.permission.READ_CALL_LOG
引入、弃用情况	API16 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用读取用户通话记录。该权限可以让应用保存用户的通话记录数据，而恶意应用可能会在用户不知情的情况下分享通话记录数据。	

4.1.6.4 WRITE_CALL_LOG

权限名称	WRITE_CALL_LOG
Constant Value	android.permission.WRITE_CALL_LOG
引入、弃用情况	API16 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用写入用户的联系人数据。该权限可以让应用添加和修改手机通话记录，恶意应用可能	

会借此清除或修改用户的通话记录。

4.1.6.5 ADD_VOICEMAIL

权限名称	ADD_VOICEMAIL
Constant Value	
引入、弃用情况	API4 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用向语音信箱添加语音邮件。	

4.1.6.6 USE_SIP

权限名称	USE_SIP
Constant Value	android.permission.USE_SIP
引入、弃用情况	API9 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用使用 SIP 服务。该权限可以让应用拨打和接听 SIP 电话。	

4.1.6.7 PROCESS_OUTGOING_CALLS

权限名称	PROCESS_OUTGOING_CALLS
Constant Value	android.permission.PROCESS_OUTGOING_CALLS
引入、弃用情况	API 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用在拨出电话时查看拨打的电话号码，并选择改为拨打其他号码或者完全终止通话。	

4.1.7 SENSORS

4.1.7.1 BODY_SENSORS

权限名称	BODY_SENSORS
Constant Value	android.permission.BODY_SENSORS
引入、弃用情况	API20 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用存取监测身体状况的传感器所收集的数据，例如心率。	

4.1.8 SMS

4.1.8.1 SEND_SMS

权限名称	SEND_SMS
Constant Value	android.permission.SEND_SMS
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用发送 SMS 信息。该权限可能会导致意外收费。恶意应用可能会未经用户确认而发送短信，由此产生相关费用。	

4.1.8.2 RECEIVE_SMS

权限名称	RECEIVE_SMS
Constant Value	android.permission.RECEIVE_SMS
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用接收短信。该权限可以让应用接收和处理短信，可以让应用监视发送到用户设备的短信，或删除发送到用户设备的短信而不显示。	

4.1.8.3 READ_SMS

权限名称	READ_SMS
Constant Value	android.permission.READ_SMS
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用读取 SMS 信息。该权限可让应用读取所有短信，而不考虑短信是否属于机密或敏感内容。	

4.1.8.4 RECEIVE_WAP_PUSH

权限名称	RECEIVE_WAP_PUSH
Constant Value	android.permission.RECEIVE_WAP_PUSH
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是

基本情况：
允许应用接收 WAP 推送信息。该权限包括监视发送给用户的消息或删除发送给用户的消息而不显示的功能。

4.1.8.5 RECEIVE_MMS

权限名称	RECEIVE_MMS
Constant Value	android.permission.RECEIVE_MMS
引入、弃用情况	API1 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用监控接收 MMS 信息。该权限包括监视发送给用户的消息或删除发送给用户的消息而不显示的功能。	

4.1.9 STORAGE

4.1.9.1 READ_EXTERNAL_STORAGE

权限名称	READ_EXTERNAL_STORAGE
Constant Value	android.permission.READ_EXTERNAL_STORAGE
引入、弃用情况	API16 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许程序读取设备外部存储空间。该权限可以让应用读取 SD 卡上公共空间的所有内容。	

4.1.9.2 WRITE_EXTERNAL_STORAGE

权限名称	WRITE_EXTERNAL_STORAGE
Constant Value	android.permission.WRITE_EXTERNAL_STORAGE
引入、弃用情况	API4 引入
保护级别	Dangerous
是否供第三方 App 使用	是
基本情况：	
允许应用向外部存储写入数据。该权限可以让应用对 SD 卡上公共空间的内容做出写入和修改操作。	

4.2 Normal 级别权限

4.2.1 ACCESS_LOCATION_EXTRA_COMMANDS：

权限名称	ACCESS_LOCATION_EXTRA_COMMANDS
Constant Value	android.permission.ACCESS_LOCATION_EXTRA_COMMANDS
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用使用其他的位置信息提供程序命令。该权限可以让应用干扰 GPS 或其他位置信息源的运作。	

4.2.2 ACCESS_NETWORK_STATE

权限名称	ACCESS_NETWORK_STATE
Constant Value	android.permission.ACCESS_NETWORK_STATE
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用获取网络连接相关信息，例如存在和连接的网络。	

4.2.3 ACCESS_NOTIFICATION_POLICY

权限名称	ACCESS_NOTIFICATION_POLICY
Constant Value	android.permission.ACCESS_NOTIFICATION_POLICY
引入、弃用情况	API23 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许设置通知策略。	

4.2.4 ACCESS_WIFI_STATE

权限名称	ACCESS_WIFI_STATE
Constant Value	android.permission.ACCESS_WIFI_STATE
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用查看无线网络的相关信息，例如是否启用了 WLAN 以及连接的 WLAN 设备的名称。	

4.2.5 BLUETOOTH

权限名称	BLUETOOTH

Constant Value	android.permission.BLUETOOTH
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用与蓝牙设备配对。允许应用查看手机上的蓝牙配置，以及与配对设备建立连接或接受其连接请求。	

4.2.6 BLUETOOTH_ADMIN

权限名称	BLUETOOTH_ADMIN
Constant Value	android.permission.BLUETOOTH_ADMIN
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用发现蓝牙设备并与之配对。允许应用配置本地蓝牙手机，并允许其查找远程设备且与之配对。	

4.2.7 BROADCAST_STICKY

权限名称	BROADCAST_STICKY
Constant Value	android.permission.BROADCAST_STICKY
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用发送持久广播消息。此类消息在广播结束后仍会保留。	

4.2.8 CHANGE_NETWORK_STATE

权限名称	CHANGE_NETWORK_STATE
Constant Value	android.permission.CHANGE_NETWORK_STATE
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用更改网络连接状态。	

4.2.9 CHANGE_WIFI_MULTICAST_STATE

权限名称	CHANGE_WIFI_MULTICAST_STATE

Constant Value	android.permission.CHANGE_WIFI_MULTICAST_STATE
引入、弃用情况	API4 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用进入 Wi-Fi 多播模式。允许应用使用多播地址接收发送到无线网络上所有设备（而不仅仅是用户手机）数据包。该操作的耗电量比非多播模式要大。	

4.2.10 CHANGE_WIFI_STATE

权限名称	CHANGE_WIFI_STATE
Constant Value	android.permission.CHANGE_WIFI_STATE
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用改变 wifi 连接状态。允许应用与 WLAN 接入点建立和断开连接，以及更改无线网络的设备配置。	

4.2.11 DISABLE_KEYGUARD

权限名称	DISABLE_KEYGUARD
Constant Value	android.permission.DISABLE_KEYGUARD
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用禁用系统锁屏。允许应用停用键锁以及任何关联的密码安全措施。例如让手机在接听来电时停用键锁，在通话结束后重新启用键锁。	

4.2.12 EXPAND_STATUS_BAR

权限名称	EXPAND_STATUS_BAR
Constant Value	android.permission.EXPAND_STATUS_BAR
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用展开和折叠状态栏。	

4.2.13 GET_PACKAGE_SIZE

权限名称	GET_PACKAGE_SIZE
Constant Value	android.permission.GET_PACKAGE_SIZE
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用获取任何应用占用空间大小。	

4.2.14 GET_TASKS

权限名称	GET_TASKS
Constant Value	android.permission.GET_TASKS
引入、弃用情况	API1 时引入，API21 中弃用。 弃用后系统的处理方式如下： ActivityManager.getRecentTasks()仍然可以调用，但不在返回全部的 Task 信息，仅返回自身 Task 以及一些不涉及隐私的其他 Task 信息。
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
API21 弃用。	

4.2.15 INSTALL_SHORTCUT

权限名称	INSTALL_SHORTCUT
Constant Value	com.android.launcher.permission.INSTALL_SHORTCUT
引入、弃用情况	API19 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用安装桌面快捷方式。	

4.2.16 INTERNET

权限名称	INTERNET
Constant Value	android.permission.INTERNET
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用使用完整的网络权限。	

4.2.17 KILL_BACKGROUND_PROCESSES

权限名称	KILL_BACKGROUND_PROCESSES
Constant Value	android.permission.KILL_BACKGROUND_PROCESSES
引入、弃用情况	API8 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用调用 killBackgroundProcesses(String)方法结束其他应用的后台进程。	

4.2.18 MODIFY_AUDIO_SETTINGS

权限名称	MODIFY_AUDIO_SETTINGS
Constant Value	android.permission.MODIFY_AUDIO_SETTINGS
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许该应用修改全局音频设置，例如音量和用于输出的扬声器。	

4.2.19 NFC

权限名称	NFC
Constant Value	android.permission.NFC
引入、弃用情况	API9 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用使用 NFC 进行 I/O 操作。允许应用与近距离无线通信（NFC）标签，卡和读取器通信。	

4.2.20 PERSISTENT_ACTIVITY

权限名称	PERSISTENT_ACTIVITY
Constant Value	android.permission.PERSISTENT_ACTIVITY
引入、弃用情况	API1 引入，API9 弃用
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
API 19 弃用，相关方法未来将会去掉。	

4.2.21 READ_SYNC_SETTINGS

权限名称	READ_SYNC_SETTINGS

Constant Value	android.permission.READ_SYNC_SETTINGS
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许该应用读取某个账户的同步设置。例如，此权限可确定“联系人”应用是否与某个账户同步。	

4.2.22 READ_SYNC_STATS

权限名称	READ_SYNC_STATS
Constant Value	android.permission.READ_SYNC_STATS
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
许该应用读取某个账户的同步统计信息，包括同步活动历史记录和同步数据量。	

4.2.23 RECEIVE_BOOT_COMPLETED

权限名称	RECEIVE_BOOT_COMPLETED
Constant Value	android.permission.RECEIVE_BOOT_COMPLETED
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用接收 ACTION_BOOT_COMPLETED 广播，该广播系统启动完成后发送。允许应用在系统完成引导后立即自动启动。这样可能会延长手机的启动时间，并允许应用始终运行，从而导致手机总体运行速度减慢。	

4.2.24 REORDER_TASKS

权限名称	REORDER_TASKS
Constant Value	android.permission.REORDER_TASKS
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用对对正在运行的应用重新排序。允许应用将任务移动到前台和后台。该应用可能不经用户命令自行执行此操作。	

4.2.25 REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

权限名称	REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
Constant Value	android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
引入、弃用情况	API23 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用忽略系统电池优化策略。	

4.2.26 REQUEST_INSTALL_PACKAGES

权限名称	REQUEST_INSTALL_PACKAGES
Constant Value	
引入、弃用情况	API23 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用请求安装 App。版本高于 API22 的应用使用 ACTION_INSTALL_PACKAGE 时，必须使用该权限。	

4.2.27 RESTART_PACKAGES

权限名称	RESTART_PACKAGES
Constant Value	android.permission.RESTART_PACKAGES
引入、弃用情况	API1 引入，API8 弃用
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
API8 弃用，restartPackage(String)方法不再支持。	

4.2.28 SET_ALARM

权限名称	SET_ALARM
Constant Value	com.android.alarm.permission.SET_ALARM
引入、弃用情况	API9 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用设置闹钟。	

4.2.29 SET_TIME_ZONE

权限名称	SET_TIME_ZONE

Constant Value	android.permission.SET_TIME_ZONE
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用设置系统时区。	

4.2.30 SET_WALLPAPER

权限名称	SET_WALLPAPER
Constant Value	android.permission.SET_WALLPAPER
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用设置系统壁纸。	

4.2.31 SET_WALLPAPER_HINTS

权限名称	SET_WALLPAPER_HINTS
Constant Value	android.permission.SET_WALLPAPER_HINTS
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用设置有关系统壁纸大小的提示。	

4.2.32 TRANSMIT_IR

权限名称	TRANSMIT_IR
Constant Value	android.permission.TRANSMIT_IR
引入、弃用情况	API19 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用使用手机的红外线发射器。	

4.2.33 UNINSTALL_SHORTCUT

权限名称	UNINSTALL_SHORTCUT
Constant Value	com.android.launcher.permission.UNINSTALL_SHORTCUT
引入、弃用情况	API19 引入

保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用删除桌面快捷方式。	

4.2.34 USE_FINGERPRINT

权限名称	USE_FINGERPRINT
Constant Value	android.permission.USE_FINGERPRINT
引入、弃用情况	API23 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用使用手机指纹设备。	

4.2.35 VIBRATE

权限名称	VIBRATE
Constant Value	android.permission.VIBRATE
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许应用使用手机震动。	

4.2.36 WAKE_LOCK

权限名称	WAKE_LOCK
Constant Value	android.permission.WAKE_LOCK
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是
基本情况：	
允许程序在手机屏幕关闭后后台进程仍然运行。改权限让应用阻止手机进入休眠状态。	

4.2.37 WRITE_SYNC_SETTINGS

权限名称	WRITE_SYNC_SETTINGS
Constant Value	android.permission.WRITE_SYNC_SETTINGS
引入、弃用情况	API1 引入
保护级别	Normal
是否供第三方 App 使用	是

基本情况：
允许该应用修改某个账户的同步设置，启用和停用同步。

4.3 其他级别权限

4.3.1 ACKAGE_USAGE_STATS

权限名称	PACKAGE_USAGE_STATS
Constant Value	android.permission.PACKAGE_USAGE_STATS
引入、弃用情况	API23 引入
保护级别	signature|privileged
是否供第三方 App 使用	是
基本情况：	
允许应用收集用户设备上使用情况的统计信息。该权限需要用户在权限管理设置界面主动对请求使用该权限的应用进行授权。	

4.3.2 SYSTEM_ALERT_WINDOW

权限名称	SYSTEM_ALERT_WINDOW
Constant Value	android.permission.SYSTEM_ALERT_WINDOW
引入、弃用情况	API1 引入
保护级别	Signature
是否供第三方 App 使用	是
基本情况：	
允许应用生成 TYPE_SYSTEM_ALERT 级别的窗口，该级别的窗口可以覆盖在其他应用的窗口之上。普通应用很少需要使用该权限，通常在显示系统通知时使用。 API23 之后，该权限需要用户在权限管理设置界面主动对请求使用该权限的应用进行授权。打开系统权限管理设置界面的方式为发送含 ACTION_MANAGE_OVERLAY_PERMISSION 的广播，可以通过 Settings.canDrawOverlays()方法检查用户是否 授予了该权限。	

4.3.3 WRITE_SETTINGS

权限名称	WRITE_SETTINGS
Constant Value	android.permission.WRITE_SETTINGS
引入、弃用情况	API1 引入
保护级别	Signature
是否供第三方 App 使用	是
基本情况：	
允许应用读取和写入系统设置。 API23 之后，该权限需要用户在权限管理设置界面主动对请求使用该权限的应用进行授权。打开系统权限管理设置界面的方式为发送含 ACTION_MANAGE_WRITE_SETTINGS 的广播，可以通过 Settings.System.canWrite()方法检查用户是否授予了该权限。	

5 Android 系统权限使用建议

通过调研发现，Android系统仅将权限分为normal和dangerous两个级别区别对待是存在一定问题的。例如，某些normal级别权限对用户使用手机时的体验非常重要，而dangerous级别权限的重要程度不尽相同。基于以上考虑，本指南希望采用一些独立于官方权限分类的指标，从不同的而维度考虑，针对每一项权限给出更为精细的权限建议。

最终，根据权限是否重要，权限涉及的使用场景是不是常用，以及在某些场景下是否可以采取其他不使用权限的更为合理的实现方式，制定权限使用建议。

权限建议分为如下几类：

可以使用：此类权限风险较低，可以供开发者使用。

谨慎使用：此类权限风险较高，开发者使用时应首先根据所开发应用的使用场景，寻求其他可以替代的实现方式，而不使用此类权限。如果一定要使用此类权限，应对使用此类权限实现的功能给出说明。

不建议使用：此类权限风险非常高，或者实际使用场景非常少。开发者应该尽量减少使用此类权限。如果一定要使用此类权限，应对使用此类权限实现的功能给出说明。

5.1 Dangerous 级别权限

5.1.1 READ_CALENDAR

权限名称	READ_CALENDAR
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	日历、日程 App 需要使用。
是否存在替代方式（部分场景）	
是。官方建议不用读取和写入日历数据的权限，改用系统自带日历应用支持的 Intent 对象执行读取和写入操作。	
基本情况：	
允许应用读取用户日历数据。该权限可以让应用读取手机上的所有日历活动，分享和保存日历数据，而不论这些数据是否属于机密或敏感内容。	

5.1.2 WRITE_CALENDAR

权限名称	WRITE_CALENDAR
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	日历、日程 App 需要使用。
是否存在替代方式（部分场景）	
是。官方建议不用读取和写入日历数据的权限，改用系统自带日历应用支持的 Intent 对象执行读取和写入操作。	
基本情况：	
允许应用写入用户日历数据。该权限可以让应用添加、删除、更改用户手机上的活动。此权限可让应用冒充日历所有者发送消息，或在所有者不知情的情况下修改活动。	

5.1.3 CAMERA

权限名称	CAMERA
是否重要	是
是否常用	是
权限建议	谨慎使用
补充说明	相机 App、具有扫描二维码功能的 App 需要使用。
是否存在替代方式（部分场景）	
是。调用系统相机照相并获取照片数据可以通过发送 Intent 的方式代替。	
基本情况：	
允许应用使用照相设备。该权限可以让应用随时使用相机拍摄照片和视屏，而无需用户的确认。	

5.1.4 READ_CONTACTS

权限名称	READ_CONTACTS
是否重要	是
是否常用	是
权限建议	不建议使用
补充说明	通讯录、电话 App 需要使用。
是否存在替代方式（部分场景）	
是。获取、呈现某个联系人的信息，可以通过发送 Intent 的方式实现。	
基本情况：	
允许应用读取用户联系人数据。该权限可以让应用读取用户手机上存储的联系人的相关数据，包括通过打电话、发送电子邮件或以其他方式与特定个人通信的频率。该权限可让应用保存联系人数据，而恶意应用可能会在用户不知情的情况下分享联系人数据。	

5.1.5 WRITE_CONTACTS

权限名称	WRITE_CONTACTS

是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	通讯录、电话 App 需要使用。
是否存在替代方式（部分场景）	
是。添加联系人等场景，可以通过发送 Intent 的方式实现。	
基本情况：	
允许应用写入用户联系人数据。该权限可以让应用修改用户手机上存储的联系人的相关数据，包括用户通过打电话、发送电子邮件或以其他方式与特定个人通信的频率。该权限可以让应用删除联系人数据。	

5.1.6 GET_ACCOUNTS

权限名称	GET_ACCOUNTS
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
访问手机中的帐户列表。（API23 开始，如果 App 与账户管理者使用相同签名，访问账户是则无需该权限。）	

5.1.7 ACCESS_FINE_LOCATION

权限名称	ACCESS_FINE_LOCATION
是否重要	否
是否常用	是
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用访问精确位置。该权限可以让应用通过全球定位系统（GPS）或网络位置信息源（例如基站和 WLAN）获取用户的精确位置信息。	

5.1.8 ACCESS_COARSE_LOCATION

权限名称	ACCESS_COARSE_LOCATION
是否重要	否
是否常用	是

权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用访问粗略位置信息。该权限获取用户的大致位置信息。这类位置信息来自于使用网络位置信息源（例如基站和 WLAN）的位置信息服务。	

5.1.9 RECORD_AUDIO

权限名称	RECORD_AUDIO
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用录制音频。该权限可让应用不经用户确认即可随时录制音频。	

5.1.10 READ_PHONE_STATE

权限名称	READ_PHONE_STATE
是否重要	是
是否常用	是
权限建议	谨慎使用
补充说明	该权限可以让应用读取手机状态和身份信息（常用），可以实现监听手机来电信息功能（不常用）。
是否存在替代方式（部分场景）	
基本情况：	
允许应用读取手机状态，包括手机的号码、当前蜂窝网络信息、正在进行的通话信息（是否正处于通话状态以及拨打的号码）、以及手机上注册的账户列表。	

5.1.11 CALL_PHONE

权限名称	CALL_PHONE
是否重要	是
是否常用	是
权限建议	不建议使用
补充说明	电话 App 需要使用。
是否存在替代方式（部分场景）	
是。拨打电话，可以通过发送 Intent 的方式实现。使用 ACTION_DIAL，不需要该权限。使用 ACTION_CALL，需要该权限。	
基本情况：	
允许应用直接拨打某个电话号码，不需要用户通过拨号用户界面确认。该权限可以让应用在用户未执行任何操作的情况下拨打电话号码。恶意应用可通过拨打电话产生相关费用，而无需用户确认。	

5.1.12 READ_CALL_LOG

权限名称	READ_CALL_LOG
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	电话 App 需要使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用读取用户通话记录。该权限可以让应用保存用户的通话记录数据，而恶意应用可能会在用户不知情的情况下分享通话记录数据。	

5.1.13 WRITE_CALL_LOG

权限名称	WRITE_CALL_LOG
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	电话 App 需要使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用写入用户的联系人数据。该权限可以让应用添加和修改手机通话记录，恶意应用可能会借此清除或修改用户的通话记录。	

5.1.14 ADD_VOICEMAIL

权限名称	ADD_VOICEMAIL
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用向语音信箱添加语音邮件。	

5.1.15 USE_SIP

权限名称	USE_SIP
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用使用 SIP 服务。该权限可以让应用拨打和接听 SIP 电话。	

5.1.16 PROCESS_OUTGOING_CALLS

权限名称	PROCESS_OUTGOING_CALLS
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	电话 App 需要使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用在拨出电话时查看拨打的电话号码，并选择改为拨打其他号码或者完全终止通话。	

5.1.17 BODY_SENSORS

权限名称	BODY_SENSORS
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用存取监测身体状况的传感器所收集的数据，例如心率。	

5.1.18 SEND_SMS

权限名称	SEND_SMS
是否重要	是
是否常用	是
权限建议	不建议使用
补充说明	
是否存在替代方式（部分场景）	
是。发送短信可以通过发送 Intent 的方式实现。	
基本情况：	
允许应用发送 SMS 信息。该权限可能会导致意外收费。恶意应用可能会未经用户确认而发送短信，由此产生相关费用。	

5.1.19 RECEIVE_SMS

权限名称	RECEIVE_SMS
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	1、短信 App 需要使用。2、另外，该权限可以让应用读取手机接收到的短信并获取短信内容，常见场景为读取验证码消息并分析出验证码。
是否存在替代方式（部分场景）	
基本情况：	
允许应用接收短信。该权限可以让应用接收和处理短信，可以让应用监视发送到用户设备的短信，或删除发送到用户设备的短信而不显示。	

5.1.20 READ_SMS

权限名称	READ_SMS

是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	短信 App 需要使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用读取 SMS 信息。该权限可让应用读取所有短信，而不考虑短信是否属于机密或敏感内容。	

5.1.21 RECEIVE_WAP_PUSH

权限名称	RECEIVE_WAP_PUSH
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	短信 App 需要使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用接收 WAP 推送信息。该权限包括监视发送给用户的消息或删除发送给用户的消息而不显示的功能。	

5.1.22 RECEIVE_MMS

权限名称	RECEIVE_MMS
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	短信 App 需要使用
是否存在替代方式（部分场景）	
基本情况：	
允许应用监控接收 MMS 信息。该权限包括监视发送给用户的消息或删除发送给用户的消息而不显示的功能。	

5.1.23 READ_EXTERNAL_STORAGE

权限名称	READ_EXTERNAL_STORAGE
是否重要	是
是否常用	是
权限建议	谨慎使用
补充说明	1、文件管理类别 App 需要使用。2、App 操作文件系统的三种途径，详情参考文档。
是否存在替代方式（部分场景）	
是。可以使用内部存储和外部存储上的 App 专用存储空间，不需要使用权限。	
基本情况：	
允许程序读取设备外部存储空间。该权限可以让应用读取 SD 卡上公共空间的所有内容。	

5.1.24 WRITE_EXTERNAL_STORAGE

权限名称	WRITE_EXTERNAL_STORAGE
是否重要	是
是否常用	是
权限建议	谨慎使用
补充说明	1、文件管理类别 App 需要使用。2、App 操作文件系统的三种途径，详情参考文档。
是否存在替代方式（部分场景）	
是。可以使用内部存储和外部存储上的 App 专用存储空间，不需要使用权限。	
基本情况：	
允许应用向外部存储写入数据。该权限可以让应用对 SD 卡上公共空间的内容做出写入和修改操作。	

5.2 Normal 级别权限

5.2.1 ACCESS_LOCATION_EXTRA_COMMANDS：

权限名称	ACCESS_LOCATION_EXTRA_COMMANDS
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	地图 App 可以使用
是否存在替代方式（部分场景）	
基本情况：	
允许应用使用其他的位置信息提供程序命令。该权限可以让应用干扰 GPS 或其他位置信息源的运作。	

5.2.2 ACCESS_NETWORK_STATE

权限名称	ACCESS_NETWORK_STATE
是否重要	否
是否常用	是
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用获取网络连接相关信息，例如存在和连接的网络。	

5.2.3 ACCESS_NOTIFICATION_POLICY

权限名称	ACCESS_NOTIFICATION_POLICY
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	设置自身 App 的 Notification 策略。我们认为该权限比较重要，或者说普通开发这通常不需要使用。
是否存在替代方式（部分场景）	
基本情况：	
允许设置通知策略。	

5.2.4 ACCESS_WIFI_STATE

权限名称	ACCESS_WIFI_STATE

是否重要	否
是否常用	是
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用查看无线网络的相关信息，例如是否启用了 WLAN 以及连接的 WLAN 设备的名称。	

5.2.5 BLUETOOTH

权限名称	BLUETOOTH
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用与蓝牙设备配对。允许应用查看手机上的蓝牙配置，以及与配对设备建立连接或接受其连接请求。	

5.2.6 BLUETOOTH_ADMIN

权限名称	BLUETOOTH_ADMIN
是否重要	否
是否常用	是
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用发现蓝牙设备并与之配对。允许应用配置本地蓝牙手机，并允许其查找远程设备且与之配对。	

5.2.7 BROADCAST_STICKY

权限名称	BROADCAST_STICKY
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	相关接口 API21 后弃用,Android 官方处于安全考虑不再推荐使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用发送持久广播消息。此类消息在广播结束后仍会保留。	

5.2.8 CHANGE_NETWORK_STATE

权限名称	CHANGE_NETWORK_STATE
是否重要	否
是否常用	是

权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用更改网络连接状态。	

5.2.9 CHANGE_WIFI_MULTICAST_STATE

权限名称	CHANGE_WIFI_MULTICAST_STATE
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	使用组播功能时，首先获取组播锁，使用完毕后为节省电量需要释放组播锁。
是否存在替代方式（部分场景）	
基本情况：	
允许应用进入 Wi-Fi 多播模式。允许应用使用多播地址接收发送到无线网络上所有设备（而不仅仅是用户手机）数据包。该操作的耗电量比非多播模式要大。	

5.2.10 CHANGE_WIFI_STATE

权限名称	CHANGE_WIFI_STATE
是否重要	否
是否常用	是
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用改变 wifi 连接状态。允许应用与 WLAN 接入点建立和断开连接，以及更改无线网络的设备配置。	

5.2.11 DISABLE_KEYGUARD

权限名称	DISABLE_KEYGUARD
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	KeyguardManager.KeyguardLock 类相关接口 API13 之后弃用，不推荐使用。
是否存在替代方式（部分场景）	
是。使用 FLAG_DISMISS_KEYGUARD 和 FLAG_SHOW_WHEN_LOCKED 标志，无需使用该权限。	
基本情况：	
允许应用禁用系统锁屏。允许应用停用键锁以及任何关联的密码安全措施。例如让手机在接听来电时停用键锁，在通话结束后重新启用键锁。	

5.2.12 EXPAND_STATUS_BAR

权限名称	EXPAND_STATUS_BAR
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	使用场景较少，例如拨号界面禁止通知栏下拉。该权限涉及接口只能通过反射的方法调用，不推荐使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用展开和折叠状态栏。	

5.2.13 GET_PACKAGE_SIZE

权限名称	GET_PACKAGE_SIZE
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	该权限可以让应用获取系统中应用的占用空间大小，涉及接口只能通过反射的方式调用。手机管家类的 App 可能会需要使用该权限。
是否存在替代方式（部分场景）	
基本情况：	
允许应用获取任何应用占用空间大小。	

5.2.14 GET_TASKS

API21弃用，不建议使用。

5.2.15 INSTALL_SHORTCUT

权限名称	INSTALL_SHORTCUT
是否重要	是
是否常用	是
权限建议	谨慎使用
补充说明	在桌面上安装快捷方式使用比较普遍，但有时也会对用户产生不必要的困扰，谨慎使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用安装桌面快捷方式。	

5.2.16 INTERNET

权限名称	INTERNET
是否重要	否
是否常用	是
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用使用完整的网络权限。	

5.2.17 KILL_BACKGROUND_PROCESSES

权限名称	KILL_BACKGROUND_PROCESSES
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	手机管家类 App 可能需要使用。
是否存在替代方式（部分场景）	
基本情况：	
允许应用调用 killBackgroundProcesses(String)方法结束其他应用的后台进程。	

5.2.18 MODIFY_AUDIO_SETTINGS

权限名称	MODIFY_AUDIO_SETTINGS
是否重要	否
是否常用	是
权限建议	可以使用

补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许该应用修改全局音频设置，例如音量和用于输出的扬声器。	

5.2.19 NFC

权限名称	NFC
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用使用 NFC 进行 I/O 操作。允许应用与近距离无线通信（NFC）标签，卡和读取器通信。	

5.2.20 PERSISTENT_ACTIVITY

API 19 弃用，不建议使用。

5.2.21 READ_SYNC_SETTINGS

权限名称	READ_SYNC_SETTINGS
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许该应用读取某个账户的同步设置。例如，此权限可确定“联系人”应用是否与某个账户同步。	

5.2.22 READ_SYNC_STATS

权限名称	READ_SYNC_STATS
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	

是否存在替代方式（部分场景）
基本情况：
许该应用读取某个账户的同步统计信息，包括同步活动历史记录和同步数据量。

5.2.23 RECEIVE_BOOT_COMPLETED

权限名称	RECEIVE_BOOT_COMPLETED
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	允许应用接收 ACTION_BOOT_COMPLETED 广播，可以在接收到广播后实现“开机自启动”。
是否存在替代方式（部分场景）	
基本情况：	
允许应用接收 ACTION_BOOT_COMPLETED 广播，该广播系统启动完成后发送。允许应用在系统完成引导后立即自动启动。这样可能会延长手机的启动时间，并允许应用始终运行，从而导致手机总体运行速度减慢。	

5.2.24 REORDER_TASKS

权限名称	REORDER_TASKS
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用对对正在运行的应用重新排序。允许应用将任务移动到前台和后台。该应用可能不经用户命令自行执行此操作。	

5.2.25 REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

权限名称	REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	可以让应用进入系统电量优化的“白名单”，免除 Doze 模式和 Standby 模式的部分影响。Android 系统自身有对 Doze 和 Standby 模式的妥善处理，多数 App 不需要该权限，使用该权限可能会比较

	耗电。
是否存在替代方式（部分场景）	
基本情况：	
允许应用忽略系统电池优化策略。	

5.2.26 REQUEST_INSTALL_PACKAGES

权限名称	REQUEST_INSTALL_PACKAGES
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	API23 之前，执行该 Intent，不需要声明权限。
是否存在替代方式（部分场景）	
基本情况：	
允许应用请求安装 App。版本高于 API22 的应用使用 ACTION_INSTALL_PACKAGE 时，必须使用该权限。	

5.2.27 RESTART_PACKAGES

API8 弃用，不推荐使用。

5.2.28 SET_ALARM

权限名称	SET_ALARM
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用设置闹钟。	

5.2.29 SET_TIME_ZONE

权限名称	SET_TIME_ZONE
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	

是否存在替代方式（部分场景）
基本情况：
允许应用设置系统时区。

5.2.30 SET_WALLPAPER

权限名称	SET_WALLPAPER
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用设置系统壁纸。	

5.2.31 SET_WALLPAPER_HINTS

权限名称	SET_WALLPAPER_HINTS
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用设置有关系统壁纸大小的提示。	

5.2.32 TRANSMIT_IR

权限名称	TRANSMIT_IR
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用使用手机的红外线发射器。	

5.2.33 UNINSTALL_SHORTCUT

权限名称	UNINSTALL_SHORTCUT
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用删除桌面快捷方式。	

5.2.34 USE_FINGERPRINT

权限名称	USE_FINGERPRINT
是否重要	是
是否常用	否
权限建议	谨慎使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用使用手机指纹设备。	

5.2.35 VIBRATE

权限名称	VIBRATE
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用使用手机震动。	

5.2.36 WAKE_LOCK

权限名称	WAKE_LOCK
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	尽量减少使用该权限，影响手机续航。
是否存在替代方式（部分场景）	

是。 如果仅需要保持屏幕常亮的话可以使用 FLAG_KEEP_SCREEN_ON 代替。 如果需要关闭屏幕后使用 CPU，官方提了可以代替的其他方式。 参考网址：https://developer.android.com/training/scheduling/wakelock.html
基本情况：
允许程序在手机屏幕关闭后后台进程仍然运行。改权限让应用阻止手机进入休眠状态。

5.2.37 WRITE_SYNC_SETTINGS

权限名称	WRITE_SYNC_SETTINGS
是否重要	否
是否常用	否
权限建议	可以使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许该应用修改某个账户的同步设置，启用和停用同步。	

5.3 其他级别权限

5.3.1 PACKAGE_USAGE_STATS

权限名称	PACKAGE_USAGE_STATS
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用收集用户设备上使用情况的统计信息。该权限需要用户在权限管理设置界面主动对请求使用该权限的应用进行授权。	

5.3.2 SYSTEM_ALERT_WINDOW

权限名称	SYSTEM_ALERT_WINDOW
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	

允许应用生成 TYPE_SYSTEM_ALERT 级别的窗口，该级别的窗口可以覆盖在其他应用的窗口之上。普通应用很少需要使用该权限，通常在显示系统通知时使用。 API23 之后，该权限需要用户在权限管理设置界面主动对请求使用该权限的应用进行授权。打开系统权限管理设置界面的方式为发送含 ACTION_MANAGE_OVERLAY_PERMISSION 的广播，可以通过 Settings.canDrawOverlays()方法检查用户是否 授予了该权限。

5.3.3 WRITE_SETTINGS

权限名称	WRITE_SETTINGS
是否重要	是
是否常用	否
权限建议	不建议使用
补充说明	
是否存在替代方式（部分场景）	
基本情况：	
允许应用读取和写入系统设置。 API23 之后，该权限需要用户在权限管理设置界面主动对请求使用该权限的应用进行授权。打开系统权限管理设置界面的方式为发送含 ACTION_MANAGE_WRITE_SETTINGS 的广播，可以通过 Settings.System.canWrite()方法检查用户是否授予了该权限。	