



# 中华人民共和国国家标准

GB/T 38632—2020

---

## 信息安全技术 智能音视频采集设备应用安全要求

Information security technology—  
Security requirements for application of intelligent audio-video recording device

2020-04-28 发布

2020-11-01 实施

---

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 .....	I
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 概述 .....	2
6 安全技术要求 .....	2
6.1 设备安全技术要求 .....	2
6.1.1 设备身份标识与鉴别 .....	2
6.1.2 访问控制 .....	2
6.1.3 网络连接与端口 .....	3
6.1.4 数据安全 .....	3
6.1.5 软件安装 .....	3
6.1.6 预置软件安全 .....	3
6.1.7 安全审计 .....	3
6.1.8 供应链安全 .....	3
6.1.9 服务保障安全 .....	4
6.2 服务端安全技术要求 .....	4
6.2.1 身份鉴别 .....	4
6.2.2 访问控制 .....	4
6.2.3 数据安全 .....	4
6.2.4 安全审计 .....	4
7 安全管理要求 .....	5
7.1 安全管理制度 .....	5
7.2 采购管理 .....	5
7.3 安装调试管理 .....	5
7.4 运维管理 .....	5
7.5 报废停用管理 .....	6
附录 A (资料性附录) 系统概述 .....	7
附录 B (资料性附录) 典型信息安全威胁 .....	8
参考文献 .....	10

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:深圳数字电视国家工程实验室股份有限公司、中国电子技术标准化研究院、联想(北京)有限公司、深圳创维-RGB 电子有限公司、康佳集团股份有限公司、深圳国实检测技术有限公司、杭州海康威视数字技术股份有限公司、青岛海信电器股份有限公司、华为技术有限公司、公安部第一研究所、中国信息安全测评中心、国家信息技术安全研究中心、深圳市视美泰技术股份有限公司、中国信息通信研究院、北京奇虎科技有限公司。

本标准主要起草人:范科峰、李新国、许东阳、李汝鑫、马亚飞、刘天宇、潘晟、王滨、李永吉、樊洞阳、韩煜、谢丰、贾嘉、张泓、石悦、崔涛、张亚群、郑广瑞、陈验方。

# 信息安全技术

## 智能音视频采集设备应用安全要求

### 1 范围

本标准规定了智能音视频采集设备的安全技术要求和安全管理要求。

本标准适用于用户对部署在重点场所中的智能音视频采集设备进行应用安全管理,可用于指导设备和服务供应商进行产品的信息安全设计生产,也可作为相关部门对智能音视频采集设备的安全性进行监督、检查和指导的依据。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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—2010 信息安全技术 术语

### 3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

#### 3.1

**智能音视频采集设备** **intelligent audio-video recording device**

能够进行音频或视频信息采集和处理,并能够通过网络与服务端联动实现自动或互动功能的电子设备。

注1: 主要包括网络摄像机、音视频会议设备、具有音视频采集功能的智能电视和智能音箱等。

注2: 智能移动终端、个人计算机、智能可穿戴设备等具备音视频采集功能的设备不在本标准范围内。

#### 3.2

**智能音视频采集设备服务端** **server of intelligent audio-video recording device**

通过网络与智能音视频采集设备连接,为智能音视频采集设备应用业务提供设备管理、用户管理、权限管理、数据存储、数据转发等服务功能的软硬件设备或系统。

注: 通常包含应用服务器、Web 服务器、流媒体服务器、数据存储服务器等组件。

#### 3.3

**恶意代码** **malicious code**

经过专门设计的、带有恶意用途的代码,其拥有的特征和能力能够对用户及其计算机系统带来直接或间接的危害。

注: 主要包括病毒、蠕虫、木马、勒索病毒、逻辑炸弹、流氓软件等。

#### 3.4

**预置软件** **pre-installed software**

设备交付给用户时已经预先安装的软件。

注1: 主要包括固件、系统软件和应用软件。

注2: 如果设备软件在交付时与原始设备制造商的版本不同,则视交付时刻的终端软件为预置软件。