ICS 33.050.01
M 30

中华人民共和国国家标准

GB/T 39574—2020

智能终端内容过滤技术要求

Technical requirements for content decency of smart terminal

2020-12-14 发布　　2021-07-01 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

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。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国通信标准化技术委员会(SAC/TC 485)归口。

本标准起草单位:中国信息通信研究院、高通无线通信技术(中国)有限公司、真珍斑马技术(上海)贸易有限公司、联想移动通信科技有限公司。

本标准主要起草人:陈婉莹、姚一楠、董霁、翟世俊、王宇晓、王嘉义、杜志敏、翁元、李欣。

引　言

智能终端搭载智能操作系统，支持应用程序安装和卸载，支持数字广播电视，支持公共互联网业务，支持多终端之间的内容分发、资源共享等。智能终端将可以访问、处理公共互联网、电信网以及电视网的内容，同时支持多种无线传输协议，传统的无论是基于 PC 终端的互联网内容过滤技术、基于移动终端的互联网内容过滤技术还是网关型互联网内容过滤技术仅仅对支持部分网络协议的部分内容进行管理和控制，难以杜绝智能终端中的淫秽、色情、反动等不良信息，对青少年的健康成长造成极大隐患，由不良信息引发的犯罪时有发生且呈上升趋势。如何实现对更大范围内有害内容的控制，保护未成年人的健康上网，已成为整个社会、学校、家庭所关注的急需解决的问题。同时，大量在移动网中传播的诈骗信息也会进入智能终端，不单是青少年儿童，对成年人也会造成很大影响。为此，有必要提出智能终端的内容过滤技术要求，规范智能终端的内容过滤产品，维护消费者利益。

制定智能终端的内容过滤标准是从技术角度出发，规范信息内容过滤产品，指导和引导内容过滤技术的发展，为防范来自公共互联网、电信网以及电视网的不良信息侵扰，净化网络空间，营造绿色上网环境，推动绿色上网行动提供有效的技术手段。

智能终端内容过滤技术要求

1 范围

本标准规定了针对智能终端的文本过滤、网址过滤、图像过滤、视频过滤、音频过滤等内容过滤技术的功能要求及性能要求。

本标准适用于以内容分发为主要业务的智能终端，也可作为其他类型智能终端内容过滤产品的参考。

2 术语和定义、缩略语

2.1 术语和定义

下列术语和定义适用于本文件。

2.1.1

智能终端 smart terminal

具有多媒体和支持数据方面功能的智能设备。

2.1.2

语义分析方法 semantic analysis method

通过对所使用语言的语义倾向和所涉及的场景两个维度分析来综合判断文本类型的方法。

注：语义倾向直接从词语的语义获得，场景从情景框架获得，即在敏感词语判断的基础上通过情景框架分析进行言语模式的判断，进而判定文本类型。

2.1.3

不良信息 malignant information

淫秽、色情、暴力、赌博、毒品等危害身心健康的信息。

2.1.4

侵权信息 infringement information

扰乱经济秩序和社会秩序的虚假信息，以及侵害他人名誉、隐私、知识产权和其他合法权益的信息。

2.1.5

犯罪信息 crime information

涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

2.1.6

违法信息 illegal information

危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视的信息。

2.2 缩略语

下列缩略语适用于本文件。

IP：网络之间互连的协议（Internet Protocol）

NFC：近场通信（Near Field Communication）

URL：统一资源定位符（Uniform Resource Locator）

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

3 概述

3.1 智能终端内容过滤架构

图 1 为智能终端内容过滤框架,主要包括 6 个部分:实现方式、过滤渠道、过滤功能、过滤方式、过滤内容、过滤管理。实现方式包括预置软件实现和操作系统实现;过滤渠道主要包括云端过滤和本地过滤;过滤功能主要包括通信过滤、多媒体过滤、网络过滤;过滤方式主要包括名单过滤和内容过滤;过滤内容主要包括相关行业或国家规定内容和自定义内容;过滤管理主要包括权限管理、日志管理、过滤规则。

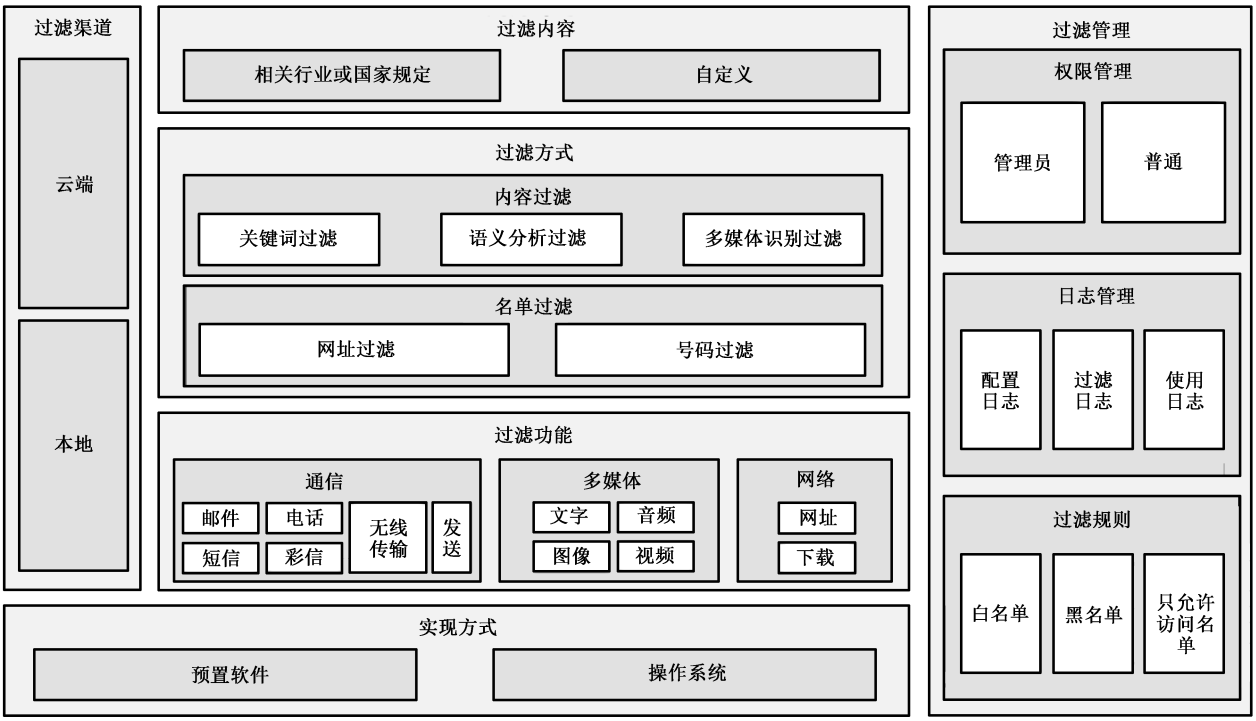

图 1 智能终端内容过滤框架

3.2 实现方式

智能终端内容过滤可通过预置软件实现或通过操作系统实现,如能满足功能要求也可通过其他方式实现:

——通过预置软件实现是指在智能终端中预置过滤软件作为实现过滤功能的主体,智能终端可无智能操作系统;

——通过操作系统实现是指智能终端在操作系统中融入过滤功能,用户可直接使用操作系统对信息进行过滤。

3.3 过滤方式

智能终端内容过滤方式应包括名单过滤和内容过滤两种:

——名单过滤是指通过对网址(包括域名、URL 或 IP 地址等)与号码的识别,将其与指定名单进行

比对、判断，从而过滤内容的方式；

——内容过滤是指对指定内容进行分析、识别，从而拦截指定内容的方式，内容过滤应包括关键词过滤，还可包括语义分析过滤、多媒体识别过滤等：

- 关键词过滤是指在文本中匹配关键词，根据定义的关键词过滤规则认定是否为禁止的内容；
- 语义分析过滤是指采用语义分析的方法对内容进行实时扫描，过滤被禁止的内容；
- 多媒体识别过滤是指对图像、音频、视频等多媒体内容进行特征分析、特征提取，并利用模式识别和模糊匹配技术与特征数据库中的特征进行相似性匹配判决，对符合匹配条件的内容进行过滤，从而拦截被禁止的内容。

3.4 过滤渠道

智能终端内容过滤渠道应包括云端过滤和本地过滤两种：

——云端过滤是指智能终端通过软件或操作系统等实现方式与云端数据库进行交互，以获得过滤判断依据的过程；

——本地过滤是指智能终端通过软件或操作系统等实现方式与本地数据库进行交互，以获得过滤判断依据的过程。

3.5 过滤内容

智能终端过滤内容应包括相关行业或国家规定内容和自定义内容两种：

——相关行业或国家规定内容指在相关行业或国家规定中禁止传播的内容，可考虑不良信息、侵权信息、犯罪信息、违法信息等，具体参考相关行业或国家标准规定；

——自定义内容是指用户在使用智能终端的过程中自己输入的过滤内容或非过滤内容，并以此内容作为过滤判断的依据。

4 功能要求

4.1 数据库要求

应建立数据库，数据库建设可包括网址库、号码库、信息关键词库、语义分析知识库、多媒体特征库等。

如是通过本地数据库比对，应提供数据库升级功能。

数据库记录应无重复，能定期增加新发现的记录，能定期删除过期和无效的记录，宜采用加密格式。

数据库建设应考虑用户适用性，除相关行业或国家标准规定禁止内容外，应提供用户自定义过滤。

数据库应有良好的扩展性，能随着业务能力变化而相应扩展过滤领域。

4.2 过滤功能要求

4.2.1 邮件过滤

如智能终端具备接收邮件功能，应对收到的邮件文本信息进行分析计算，宜对图像信息、音频信息、视频信息进行计算分析，通过计算结果判断当前邮件是否含有需过滤内容，如含有需过滤内容则应进行拦截或删除。

4.2.2 短信过滤

如智能终端具备接收短信功能，应对收到的短信进行分析计算，通过计算结果判断当前短信是否含

有需过滤内容，如含有需过滤内容则应进行拦截或删除。

4.2.3 彩信过滤

如智能终端具备接收彩信功能，应对收到的彩信文本信息进行分析计算，宜对图像信息、音频信息、视频信息进行计算分析，通过计算结果判断当前彩信是否含有需过滤内容，如含有需过滤内容则应进行拦截或删除。

4.2.4 电话过滤

如智能终端具备接收电话功能，应对收到的电话号码进行分析，通过结果判断当前电话是否需要过滤，如需过滤则应进行拦截。

4.2.5 无线传输过滤

如智能终端具备无线传输接收功能（如 WLAN、蓝牙、NFC 等），宜对通过无线传输收到的内容进行分析计算，通过计算结果判断是否含有需过滤内容，如含有需过滤内容则应进行拦截或删除。

4.2.6 发送过滤

如智能终端具备内容分发功能，应对分发的文本信息进行分析计算，宜对图像信息、音频信息、视频信息进行计算分析，通过计算结果判断是否含有需过滤内容，如含有需过滤内容则应禁止分发或删除内容。

4.2.7 文字过滤

应对输入或显示在智能终端上的文本信息内容进行分析、识别，应拦截需过滤内容。

4.2.8 图像过滤

宜对输入或显示在智能终端上的图像信息内容进行分析、识别，应拦截需过滤内容。

图像类型包括 JPEG、PNG、BMP 和 GIF 等图片格式。

4.2.9 音频过滤

宜利用音频识别技术，对播放的声音进行分析计算，通过计算结果判断是否含有需过滤内容，如含有需过滤内容则应进行拦截。

4.2.10 视频过滤

宜利用图像识别技术，对屏幕上出现的视频（包括流媒体）进行分析计算，通过计算结果判断该当前画面是否含有需过滤内容，如含有需过滤内容则应进行拦截。

4.2.11 网址过滤

应提供对网址（包括域名、URL 或 IP 地址）进行过滤的功能，应拦截对不良网址的访问请求。

4.2.12 下载过滤

应能对下载的文件名进行分析计算，通过计算判断下载的文件是否含有需过滤内容，如含有需过滤内容则应进行拦截或删除。

4.3 过滤管理功能要求

4.3.1 权限管理

应设置有产品管理员权限。

产品管理员有权对过滤功能进行设置，添加、删除和修改关键词和其他操作等。产品管理员所能进行的操作一般有，但不限于：

——更改管理密码；

——开启、关闭全部或部分过滤功能；

——查阅、删除日志；

——添加、删除和修改过滤产品的安全策略，安全策略包含文本信息的关键字、网址、图像特征设置等。

过滤产品应提供对产品管理员进行身份鉴别的功能。身份鉴别方式应采用但不限于口令、生物识别等。

过滤产品只能在产品管理员权限下终止运行和卸载。

4.3.2 日志管理

过滤产品应具备下列日志管理功能：

——日志数据生成：应至少能对正常使用日志、过滤和拦截日志、设置修改日志事件生成日志，应在每一个日志记录中记录事件发生的时间、事件描述；

——日志查询：应提供对日志记录的查询功能，除产品使用者可查看自己设置过滤内容的过滤和拦截日志外，只允许管理员查询日志记录；

——日志导出或存档：应提供对日志记录的导出、存档功能，且只允许管理员导出、存档日志记录；

——日志删除或清空：应提供对日志记录的删除、清空功能，且只允许管理员删除、清空日志记录；

——日志的统计功能：可以对上述日志信息进行统计；

——日志存储时间设定：应提供对日志的存储时间进行设定的功能，且只允许管理员设定日志存储时间。

4.3.3 过滤规则

过滤规则可以采用但不限于以下三种手段，且可以通过多种手段协作实现：

——黑名单：通过人工添加的办法设定一些内容需要过滤；

——白名单：通过人工添加的办法设定除相关行业或国家标准规定禁止内容外的一些内容永远不被过滤产品过滤和拦截；

——只允许访问：开启此选项，使得只能访问“只允许访问名单”中的内容，其他内容需过滤。

产品使用者可人工添加黑名单、白名单和只允许访问名单，可人工删除和修改产品使用者添加的黑名单、白名单和只允许访问名单；产品管理员可人工添加、删除和修改黑名单、白名单和只允许访问名单，产品使用者定义的除外。

5 性能要求

5.1 准确性

准确率、漏判率、误判率是评价准确性的常用指标：

——准确率是指正确判断应过滤内容的概率；

——漏判率是指将应过滤内容错误判断为合法内容的概率；

——误判率是指将合法内容错误判断为应过滤内容的概率。

准确率至少应高于90%，漏判率和误判率均不得高于10%。

5.2 安全性

不应给智能终端操作系统引入新的安全漏洞。

不应未经用户同意收集以及上传用户数据。

不应超出过滤范围获取智能终端权限。

如过滤以预置软件形式进行，宜以后台进程方式运行，不能被未授权终止、卸载或删除。没有特定的产品管理员账号或者特定的硬件，无法终止、卸载或删除过滤软件。

5.3 资源占用率

资源占用率指过滤功能耗费的智能终端资源，包括CPU、内存以及安装基本产品所需要的存储空间大小。

过滤功能运行的资源占用率应不影响智能终端其他功能正常使用。

参 考 文 献

[1] YDN 138—2006 基于PC终端的互联网内容过滤软件技术要求
[2] YD/T 2054—2009 WAP网关内容过滤技术要求