ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29244—2012

信息安全技术　办公设备基本安全要求

Information security technology—Basic security requirements for office devices

2012-12-31 发布　　2013-06-01 实施

中华人民共和国国家质量监督检验检疫总局
中国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。

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:中国电子技术标准化研究所、珠海天威飞马打印耗材有限公司、方正科技集团股份有限公司、天津复印机技术研究所、东莞市金翔电器设备有限公司、广州市弘宇科技有限公司。

本标准主要起草人:杨建军、陈星、高健、王立建、张希平、乔怀信、秦振山、刘慧玲、梁峰。

信息安全技术　办公设备基本安全要求

1　范围

本标准规定了办公设备安全技术要求和安全管理功能要求。

本标准适用于政府部门等机构中对办公设备具有高安全要求的信息处理环境，用于办公设备的采购、测评、维护和管理，也可为办公设备的设计提供参考。本标准不适用于涉及国家秘密的信息处理环境。

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 18336—2008(所有部分)　信息技术　安全技术　信息技术安全性评估准则

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 18336—2008 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

办公设备　office devices

用于产生或处理电子或其他媒体文件的设备。

注：主要是指具有打印、扫描、传真、复印中的一项或多项功能的设备产品。办公设备评估对象模型描述请参见附录 A。

3.2

办公设备功能　function

办公设备中执行数据处理、存储或传输的实体，包括打印、复印、传真、扫描等。

3.3

多功能设备　multifunction device

把两个或两个以上的办公设备功能组合在一起的一种办公设备。

3.4

主体　subject

对客体实施操作的主动实体。

注：在本标准中主体和用户是一致的。

3.5

客体　object

办公设备中包含有或接收信息的并由主体操作的被动实体。

3.6

实体　entity

与办公设备客体、数据或资源进行交互的主体、客体、用户或另一信息技术设备。

3.7

管理员　administrator

被授权管理办公设备的某些部分或所有部分的用户，其行为可能影响安全功能策略。

3.8

操作　operation

主体在客体上实施的一类行为。

3.9

用户　user

办公设备之外，与办公设备进行交互的实体（人或信息技术实体）。

3.10

用户数据　user data

由用户创建或为用户而创建，且不影响办公设备安全功能运行的数据。用户数据包括用户文档数据和用户功能数据。

3.11

安全功能　security function

办公设备中通过信息技术实现的、实施安全策略的机制。

3.12

安全属性　security attribute

主体、客体、信息、会话和/或资源的一个特性，用于定义安全功能要求，并且它的值用于实施安全功能策略。

注：例如某一用户的访问表，指出用户允许访问的功能列表，或是某一功能的访问表，指出允许使用该功能的用户列表。

3.13

复位　reset

使办公设备的所有用户设置都恢复到出厂默认设置，并删除设备上存储的所有用户数据和安全功能数据。

3.14

非易失性存储装置　nonvolatile storage device

当电源关闭时，其上数据不能清除的数据存储装置。

3.15

可移动的非易失性存储装置　removable nonvolatile storage device

办公设备的一部分，可由授权人员从办公设备中移出或插入的非易失性存储装置。

4　安全技术要求

4.1　标识和鉴别

办公设备应：

a）　在用户执行受控的办公设备安全功能操作之前，成功标识/鉴别该用户；

b）　按照安全属性初始化规则和变更规则，建立和维护用户安全属性与主体操作之间的关联。

4.2　访问控制

办公设备应：

a）　对普通用户操作用户文档数据进行控制，普通用户只能操作自己的用户文档，操作包括打印、

复印、扫描、传真、存取和检索、存储、修改、删除等；

b) 对普通用户修改或删除用户功能数据进行控制，普通用户只能修改或删除自己的用户功能数据；

c) 对用户使用办公设备功能进行控制，普通用户只能使用管理员明确授权的或设备自动授权的办公设备功能；

d) 基于安全属性，明确授权/拒绝用户对用户数据进行访问；

e) 基于安全属性，明确授权/拒绝用户对办公设备功能的访问。

4.3 安全审计

办公设备应：

a) 对下述可审计事件产生审计记录：

1) 审计功能的开启和关闭；

2) 操作启动和完成；

3) 使用身份鉴别机制；

4) 使用身份标识机制；

5) 管理功能的使用；

6) 时间变更；

7) 其他与系统安全有关的事件或专门定义的可审计事件。

b) 提供的审计记录内容至少包括：事件发生日期和时间、事件类型、主体身份(如果可用的话)、以及事件结果(成功或失败)、任务类型等。

c) 为每一可审计事件与导致该事件的用户身份进行关联。

d) 能对系统时间进行管理，提供可靠时间戳。

4.4 残余信息保护

办公设备应：

a) 在给用户文档或其他用户数据分配资源，或从资源释放用户文档或其他用户数据时，资源上的任何先前信息内容不可再利用；

b) 在产品文档或媒体中明确告知办公设备用户可能存在残余信息的资源及其位置。

4.5 功能测试

办公设备应：

a) 在启动、自检或用户要求的情况下运行自测程序，证实全部或部分安全功能操作的正确性；

b) 允许授权用户验证所有信息存储、处理和传输功能操作的正确性；

c) 允许授权用户验证全部或部分安全功能数据的完整性；

d) 允许授权用户验证安全功能可执行代码的完整性。

4.6 维护

办公设备应：

a) 只有在管理员许可的情况下才能对办公设备的软件进行操作，包括更新、升级、修改和删除等；

b) 具有复位功能和快速删除设备上存储的所有用户数据和安全功能数据的功能。

4.7 会话

办公设备应确保在保持静默状态规定的时间后，自动终止交互会话。

4.8 可移动非易失性存储

办公设备中的可移动非易失性存储装置应：

a) 采取提高存储的用户数据和安全功能数据安全性的措施；

b) 采用公开的数据存储结构；

c) 通过公开的接口协议与办公设备主机进行数据交换；

d) 在设备或产品文档中明确标识存储容量；

e) 能对存储的用户数据和安全功能数据进行完整性检查。

4.9 密码要求

办公设备如采用密码技术，应符合国家密码管理相关规定。

5 安全管理功能要求

5.1 安全属性管理

办公设备应：

a) 具有初始化安全属性默认值的功能；

b) 具有限制用户初始化安全属性默认值的功能；

c) 具有维护用户安全属性的功能；

d) 具有限制用户操作安全属性的功能，对安全属性的操作包括默认值变更、查询、修改或删除。

5.2 数据管理

办公设备应：

a) 确保只有管理员或除普通用户以外的授权标识角色来操作安全功能数据列表，或者禁止任何人操作安全功能数据列表，包括默认值变更、查询、修改、删除或清除；

b) 确保只有管理员或与安全功能数据相关的普通用户来操作与普通用户或普通用户的工作或任务相关的安全功能数据，或者禁止任何人操作与普通用户或普通用户的工作或任务相关的安全功能数据，包括默认值变更、查询、修改、删除或清除。

5.3 用户角色管理

办公设备应能：

a) 具有维护用户列表和角色列表的功能；

b) 具有把用户与角色相关联的功能。

附 录 A
（资料性附录）
办公设备安全评估模型

A.1 办公设备概述

本标准定义的办公设备主要用于打印、扫描、复印和传真等。办公设备可以依据其意图或用途，以多种不同的配置予以实现。简单的设备通过单一功能实现其单一用途，例如打印机、扫描仪、复印机或传真机。有些设备在其主要用途的基础上增加一些附加功能，例如一个传真机也可用于复印，或一个复印机也可用于打印。复杂多功能设备通过使用不同功能的组合，执行多个不同单一功能的操作，实现多种用途。有些设备为增强其能力，还具有一些附加功能，例如硬盘或其他非易失性存储、文件服务器、手工或自动更新办公设备运行软件等。

A.2 办公设备安全评估模型（见图 A.1）

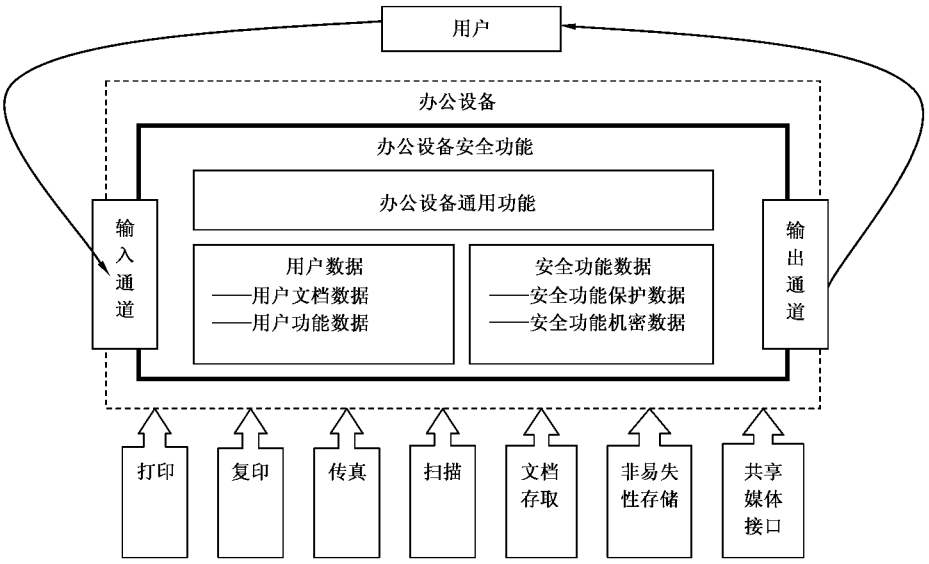

图 A.1 办公设备安全评估模型图

注：该图参阅了 IEEE 2600.1—2009 中的评估对象模型。

A.3 模型说明

A.3.1 用户

办公设备用户可以分为两类：普通用户和管理员，表 A.1 对两类用户进行了定义。

表 A.1 用户

名 称		定 义
授权用户	普通用户	授权操作办公设备处理用户文档数据的用户
	管理员	授权管理办公设备,以及影响办公设备安全策略的用户

A.3.2 资产

办公设备包括三种类型的资产:用户数据、安全功能数据和办公设备功能。

A.3.3 用户数据

用户数据是由用户创建的或为用户而创建的数据,它不影响办公设备安全功能的运行。这种类型的数据有两类:用户文档数据和用户功能数据,表 A.2 对用户数据进行了定义。

表 A.2 用户数据

名 称	定 义
用户文档数据	用户文档数据是指办公设备处理的用户文档中的所有信息,包括:正在扫描或拷贝的原件数据,拟打印的电子文件内容,由扫描或传真得到的图像数据,输出的打印文档,以及在硬盘或其他存储设备中残留或存储的数据
用户功能数据	用户功能数据是指与办公设备所处理业务有关的信息,包括作业指令和作业状态

A.3.4 安全功能数据

安全功能数据是指实施办公设备安全功能所需的数据,它可影响办公设备的运行。安全功能数据可以分为两类:安全功能保护数据和安全功能机密数据,表 A.3 和表 A.4 给出了安全功能数据的定义和示例。

表 A.3 安全功能数据

名 称	定 义
安全功能保护数据	办公设备安全功能保护数据包括: a) 办公设备的作业和使用日志、地址簿以及设备配置; b) 网络管理数据,例如 IP 地址; c) 办公设备的数字资源和其他常驻数据,这些数据不是用户文档数据或办公设备软件(例如字型或存储表格)的必要组成部分
安全功能机密数据	办公设备安全功能机密数据包括: a) 用户口令; b) 设备管理数据,例如安全事件审计日志数据

表 A.4　安全功能数据分类示例

安全功能受保护数据示例	安全功能机密数据示例
用户和管理者标识数据	用户和管理者鉴别数据
扫描/传真/邮件地址表或通讯录	访问外部设备(如邮件或文件服务器)的凭证
任务状态日志	工作细节和审计日志
挂起或储存任务和文档的状态	访问控制列表
设备和网络状态信息和配置设置	设备和网络管理(如:简单网络管理协议)鉴别数据
设备安全状态	加密钥匙

A.3.5　办公设备功能

办公设备功能是指办公设备对用户数据的处理、存储和转换,具体定义参见表 A.5。

表 A.5　办公设备功能定义

功能名称	定　义
打印	将电子文档输入转换为物理文档输出的功能
扫描	将物理文档输入转换为电子文档输出的功能
复印	将物理文档输入复制为物理文档输出的功能
传真	将物理文档输入转换为基于电话的传真发送的功能,并将基于电话的文档传真接受转换为物理文件输出的功能
文档存取	一个任务期间存储文档,在后续一个或多个任务中取回文档的功能
非易失性存储	将用户数据和安全功能数据存储在固定存储设备上的功能,该设备是评估安全保护对象模型的一部分但设计成可由授权人员从安全保护对象模型上移出。对存储装置的非正常访问或者被拆卸时,在不受保护的环境下,可被攻击者离线分析其内容;或从办公设备保护环境之外重新插入类似设备,可能使攻击者把恶意内容引入到办公设备中
共享媒体接口	在一个通信媒介上发送或接收用户数据或安全功能数据,在一般实践中,该通讯媒体可以同时被多个用户访问,例如有线网络以及大多数无线网络

A.3.6　操作

办公设备包括以下五种类型的操作:可导致信息泄露的读操作,可导致信息改变的生成操作、修改操作和删除操作,以及调用功能的操作。

A.3.7　通道

通道是一种数据输入/输出办公设备的机制,办公设备通道通常包含私有媒体接口、共享媒体接口、原始文档处理器和硬拷贝输出处理器。

A.3.8　运行模型

办公设备由输入、输出、储存和处理等元素组成,以便在用户文档数据上执行以下一个或多个文档处理操作:打印、扫描、复印、传真、存储等。操作期间,可以产生和修改用户功能数据(例如任务状态)和安全功能数据(例如任务审计日志)。

参 考 文 献

[1] IEEE 2600.1—2009 A 操作环境下的保护轮廓标准

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 办公设备基本安全要求
GB/T 29244—2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址:www.gb168.cn
服务热线:010-68522006
2013年4月第一版
*
书号:155066·1-46893

GB/T 29244-2012