ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38558—2020

信息安全技术　办公设备安全测试方法

Information security technology—Security test method for office devices

2020-03-06 发布　　2020-10-01 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院、西安电子科技大学、珠海天威飞马打印耗材有限公司、珠海赛纳打印科技股份有限公司、北京工业大学、天津天复检测技术有限公司、东莞市金翔光电科技有限公司、天津光电通信技术有限公司、中船重工汉光科技股份有限公司、珠海奔图电子有限公司、联想图像(天津)科技有限公司。

本标准主要起草人:范科峰、杨建军、高林、刘硕、胡影、王佳敏、孙彦、蔡磊、徐克超、乔怀信、陈星、任俊强、高健、王泉、杨震、裴庆祺、林东宁、曹冠群、刘刚、王健、高军辉。

信息安全技术　办公设备安全测试方法

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的测试方法。

本标准适用于测试机构、办公设备厂商对办公设备的安全性进行测试。

注：本标准规定的测试方法适用于GB/T 29244—2012的符合性测试，相关对应关系参见附录A。

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 29244—2012　信息安全技术　办公设备基本安全要求

3　术语和定义

GB/T 29244—2012界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

I^2C：内置集成电路 (Inter-Integrated Circuit)

SPI：串行外设接口(Serial Peripheral Interface)

5　测试方法

5.1　安全技术要求测试

5.1.1　标识和鉴别

本项测试包括：

a)　测试办公设备是否采用了身份鉴别措施，身份标识是否具有唯一性；分别以不同类型用户登录办公设备，验证用户在执行受控的安全功能操作之前，是否成功标识和鉴别该用户；拒绝非授权用户执行受控安全功能操作。

b)　测试办公设备的用户权限初始化和变更情况，查看是否能够设置新建用户的权限或修改已有用户的权限，并验证权限初始化定义或权限变更是否符合安全策略。

5.1.2　访问控制

本项测试包括：

a)　检查办公设备对普通用户操作用户文档数据的访问控制策略，验证普通用户是否只能对自己的用户文档数据进行打印、复印、扫描、传真、读取、检索、存储、修改、删除等操作，并验证是否

拒绝普通用户对其他用户文档数据进行上述操作；

b) 检查办公设备对普通用户操作用户功能数据的访问控制策略，验证普通用户是否仅能修改、删除自己的用户功能数据，并验证是否拒绝普通用户对其他用户功能数据进行修改和删除操作；

c) 检查用户使用办公设备功能的访问控制策略，验证普通用户是否仅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，而不能使用未授权的办公设备功能；

d) 修改普通用户关于用户数据访问的安全属性，测试修改结果是否生效；

e) 修改普通用户关于办公设备功能访问的安全属性，测试修改结果是否生效。

5.1.3 安全审计

本项测试包括：

a) 检查办公设备的产品文档，确认审计记录中是否包含以下审计事件：

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。

并测试审计记录是否准确记录相应的审计事件。

b) 检查办公设备的审计记录，查看审计记录是否包括事件发生日期和时间、事件类型、主体身份、事件结果(成功或失败)、任务类型等内容。

c) 测试办公设备是否对用户登录、审计功能开启/关闭、修改用户权限、时间变更等重要安全事件进行了审计，并验证审计事件记录是否与导致该事件的用户身份进行关联。

d) 检查办公设备是否具有时间管理功能，是否提供可靠的时间戳；能否防止审计记录时间被篡改。

5.1.4 残余信息保护

本项测试包括：

a) 检查办公设备的残余信息保护能力，验证用户数据的存储空间在被释放或重新分配给其他用户前，是否将先前存储的数据完全销毁，或者是否已采取保护措施使残余信息无法被利用；

b) 检查办公设备供应方提供的产品文档或媒体，查看是否明确告知办公设备用户可能存在残余信息的资源类型及所在位置。

5.1.5 功能测试

本项测试包括：

a) 检查办公设备在启动、自检、用户要求的情况下，是否能正常执行系统自测功能，以及系统自测信息能否验证全部或部分办公设备安全功能操作的正确性；

b) 检查办公设备能否允许授权用户验证信息存储、处理和传输功能等操作的正确性；

c) 检查办公设备是否提供对全部或部分安全功能数据的完整性进行验证的功能或方法，并由授权用户对该功能或方法的有效性进行测试；

d) 检查办公设备是否为授权用户提供对安全功能可执行代码的完整性进行验证的功能或方法，并测试能否验证安全功能可执行代码未被篡改。

5.1.6 维护

本项测试包括：

a) 检查办公设备的测试和维护接口，测试管理员能否对办公设备的软件维护操作进行权限限制，验证普通用户是否只有在管理员授权的情况下才能对办公设备的软件进行更新、升级、修改和删除等操作；

b) 检查产品文档，查看是否具有全局复位或各功能模块复位的功能，检查办公设备是否具有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，并测试对应功能的可用性。

5.1.7 会话

从本地或远程登录办公设备，当登录用户在静默状态规定的时间无操作时，检查办公设备是否会自动终止交互会话。

5.1.8 可移动非易失性存储

本项测试包括：

a) 检查可移动非易失性存储装置的数据存储是否采取了安全性措施，对用户数据、安全功能数据等进行防护；

b) 查看移动非易失性存储装置的数据结构，包括存储地址、存储内容、存储空间长度等是否公开；

c) 测试移动非易失性存储装置是否通过公开的接口协议，例如，SPI、I^2C 等，与办公设备主机进行数据交换；

d) 查看产品文档是否明确标识移动非易失性存储装置的存储容量；

e) 测试办公设备中的可移动非易失性存储装置，是否可对存储的数据(用户数据和安全功能数据)进行完整性检查。

5.1.9 密码要求

查看办公设备供应方提供的产品文档，确认密码技术的使用及管理是否遵照国家密码管理的相关规定。

5.2 安全管理功能要求测试

5.2.1 安全属性管理

本项测试包括：

a) 查看产品文档是否说明办公设备具有初始化安全属性的功能；复位办公设备，检查办公设备是否恢复到安全属性的默认值；

b) 测试办公设备是否限制普通用户对安全属性进行初始化操作；

c) 测试办公设备是否允许管理员或授权用户对用户的安全属性进行维护操作；

d) 检查办公设备是否限制普通用户对安全属性进行操作，包括查询、修改、删除和默认值变更。

5.2.2 数据管理

本测试包括：

a) 检查办公设备安全功能数据列表的访问控制策略，验证安全功能数据列表是否仅能由管理员或除普通用户以外授权用户进行操作，或者是否禁止任何人进行操作，包括查询、修改、删除、清除和默认值变更；

b) 检查办公设备安全功能数据的访问控制策略，验证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，是否仅能由管理员或相关的普通用户来操作，或者是否禁止任何人操作，包括查询、修改、删除、清除和默认值变更。

5.2.3 用户角色管理

本测试包括：

a) 检查办公设备是否具有用户列表和角色列表的维护功能，并验证是否只有管理员可对用户和角色进行新建、修改或删除等操作；

b) 检查办公设备的用户列表和角色列表，查看各用户是否与角色相关联，并测试新建用户时是否仅有管理员可设置用户对应的角色。

附 录 A
（资料性附录）
本标准安全测试方法与 GB/T 29244—2012 安全要求对应关系

表 A.1 给出了本标准安全测试方法与 GB/T 29244—2012 安全要求之间的对应关系。

表 A.1 本标准安全测试方法与 GB/T 29244—2012 安全要求对应关系

安全要求		对应关系	
		GB/T 29244—2012 安全要求	本标准安全测试方法
安全技术要求	标识和鉴别	4.1a)	5.1.1a)
		4.1b)	5.1.1b)
	访问控制	4.2a)	5.1.2a)
		4.2b)	5.1.2b)
		4.2c)	5.1.2c)
		4.2d)	5.1.2d)
		4.2e)	5.1.2e)
	安全审计	4.3a)	5.1.3a)
		4.3b)	5.1.3b)
		4.3c)	5.1.3c)
		4.3d)	5.1.3d)
	残余信息保护	4.4a)	5.1.4a)
		4.4b)	5.1.4b)
	功能测试	4.5a)	5.1.5a)
		4.5b)	5.1.5b)
		4.5c)	5.1.5c)
		4.5d)	5.1.5d)
	维护	4.6a)	5.1.6a)
		4.6b)	5.1.6b)
	会话	4.7	5.1.7
	可移动非易失性存储	4.8a)	5.1.8a)
		4.8b)	5.1.8b)
		4.8c)	5.1.8c)
		4.8d)	5.1.8d)
		4.8e)	5.1.8e)
	密码要求	4.9	5.1.9

表 A.1（续）

安全要求		对应关系	
		GB/T 29244—2012 安全要求	本标准安全测试方法
安全管理功能要求	安全属性管理	5.1a）	5.2.1a）
		5.1b）	5.2.1b）
		5.1c）	5.2.1c）
		5.1d）	5.2.1d）
	数据管理	5.2a）	5.2.2a）
		5.2b）	5.2.2b）
	用户角色管理	5.3a）	5.2.3a）
		5.3b）	5.2.3b）