ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37096—2018

信息安全技术
办公信息系统安全测试规范

Information security technology—Security testing specification for office information systems

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
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。

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。

本标准主要起草单位:中国电子技术标准化研究院、工业和信息化部软件与集成电路促进中心、深圳赛西信息技术有限公司、工业和信息化部电子第五研究所、北京赛西科技发展有限公司、西安电子科技大学、北京工业大学。

本标准主要起草人:姚相振、刘贤刚、范科峰、高林、杨建军、唐一鸿、毕思文、叶润国、许东阳、龚洁中、孙康健、刘龙庚、刘帅、王莉、李云婷、裴庆祺、杨震。

引　言

本标准是与 GB/T 37095—2018 相配套的测试标准，用以指导测试人员对办公信息系统安全进行测试。

本标准按照 GB/T 37095—2018 关于办公信息系统安全基本技术要求，分别从物理环境、基础硬件产品、基础软件产品、网络设施和应用软件系统等 5 个方面规定了办公信息系统安全测试规范。

信息安全技术
办公信息系统安全测试规范

1 范围

本标准规定了办公信息系统的物理环境测试、基础硬件产品测试、基础软件产品测试、网络设施测试以及应用软件系统测试的规范。

本标准适用于指导党政部门的办公信息系统建设，包括系统设计、产品采购、系统集成等，涉密办公信息系统的建设管理依据相关国家保密法规和标准要求实施。

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 2887—2011 计算机场地通用规范

GB/T 18018 信息安全技术 路由器安全技术要求

GB 18030—2005 信息技术 中文编码字符集

GB/T 20272 信息安全技术 操作系统安全技术要求

GB/T 20273 信息安全技术 数据库管理系统安全技术要求

GB/T 20275—2013 信息安全技术 网络入侵检测系统技术要求和测试评价方法

GB/T 20281—2015 信息安全技术 防火墙技术要求和测试评价方法

GB/T 21028—2007 信息安全技术 服务器安全技术要求

GB/T 21050—2007 信息安全技术 网络交换机安全技术要求(评估保证级 3)

GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求

GB/T 25069—2010 信息安全技术 术语

GB/T 26856—2011 中文办公软件基础要求及符合性测试规范

GB/T 28452—2012 信息安全技术 应用软件系统通用安全技术要求

GB/T 29240—2012 信息安全技术 终端计算机通用安全技术要求与测试评价方法

GB/T 33190—2016 电子文件存储与交换格式 版式文档

GB/T 37095—2018 信息安全技术 办公信息系统安全基本技术要求

3 术语和定义

GB/T 25069—2010 和 GB/T 37095—2018 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。

BIOS：基本输入输出系统(Basic Input Output System)

CA:认证授权(Certificate Authority)
CPU:中央处理器(Central Processing Unit)
IP:网际协议(Internet Protocol)
PC:个人计算机(Personal Computer)

5 物理环境测试

5.1 测试内容

测试办公信息系统部署、运维的物理环境中机房的建设是否符合 GB/T 2887—2011 的要求、物理环境是否符合 GB/T 21052—2007 的要求。

5.2 测试方法

物理环境测试方法应按表 1 执行。

表 1 物理环境测试方法

序号	测试项	测试方法
1	用户在中国大陆境内的办公信息系统部署、运维、数据备份的物理位置应位于中国大陆境内	检查其应用服务器、运维服务器、数据库服务器是否位于中国大陆境内,并提供证明材料。政府驻外机构依据相关部门要求执行
2	办公信息系统部署、运维的机房建设对于 GB/T 2887—2011 的标准符合性测试	检查满足 GB/T 2887—2011 的证明材料
3	办公信息系统部署、运维的物理环境对于 GB/T 21052—2007 的标准符合性测试	检查满足 GB/T 21052—2007 的证明材料

6 基础硬件产品测试

6.1 服务器

6.1.1 测试内容

测试办公信息系统所采用的服务器硬件产品的硬件指标、BIOS 基本功能。

6.1.2 测试方法

服务器测试方法应按表 2 执行。

表 2 服务器测试方法

序号	测试项	测试方法
1	检查服务器硬件指标是否符合 GB/T 21028—2007 中第三级及以上安全要求	检查服务器硬件产品符合 GB/T 21028—2007 中第三级及以上安全要求的证明材料
2	测试 BIOS 的中文显示能力	检查 BIOS 具有中文显示能力且内容正确

表 2（续）

序号	测试项	测试方法
3	测试 BIOS 支持固件软件安全升级的能力	通过 BIOS 自动检测升级工具，检查 BIOS 固件版本信息及其对旧版本的更新能力，包括：安全度量、安全恢复、安全认证、安全引导、数据加密、配置管理等安全功能的相关测试
4	针对 CPU 及芯片组固件驱动、操作系统内核等，BIOS 应支持上述设备经过国家认可的第三方 CA 机构颁发的代码签名验证	测试系统启动加载过程必须与底层 BIOS 的安全验证接口进行基于证书的认证，经 BIOS 验证通过后系统方可启动引导加载过程

6.2 桌面 PC

6.2.1 测试内容

测试办公信息系统所采用的桌面 PC 硬件产品的硬件指标、BIOS 基本功能以及厂商所提供的技术资料的完整性。

6.2.2 测试方法

桌面 PC 测试方法应按表 3 执行。

表 3 桌面 PC 测试方法

序号	测试项	测试方法
1	检查桌面 PC 硬件指标是否符合 GB/T 29240—2012 中安全技术要求第三级及以上要求	检查桌面 PC 硬件产品符合 GB/T 29240—2012 中安全技术要求第三级及以上要求的证明材料
2	测试提供禁止无线网络模块、红外模块、蓝牙模块、USB 设备功能	测试禁止无线网络模块、红外模块、蓝牙模块、USB 设备功能是否正常
3	测试 BIOS 的中文显示能力	检查 BIOS 是否具有中文显示能力
4	测试 BIOS 支持固件软件升级的能力	通过 BIOS 自动检测升级工具，检查 BIOS 固件版本信息及其对旧版本的更新能力，包括：安全度量、安全恢复、安全认证、安全引导、数据加密、配置管理等安全功能的相关测试
5	针对 CPU 及芯片组固件驱动、操作系统内核等，BIOS 应支持上述设备经过国家认可的第三方 CA 机构颁发的代码签名验证	测试系统启动加载过程必须与底层 BIOS 的安全验证接口进行基于证书的认证，经 BIOS 验证通过后系统方可启动引导加载过程

7 基础软件产品测试

7.1 操作系统

7.1.1 测试内容

测试办公信息系统所采用的操作系统的功能、认证机制、安全性以及厂商所提供的技术资料的完整性。

7.1.2 测试方法

操作系统测试方法应按表 4 执行。

表 4 操作系统测试方法

序号	测试项	测试方法
1	检查操作系统的字符编码是否符合 GB 18030—2005 的要求	检查符合 GB 18030—2005 的证明材料
2	检查操作系统及操作系统相关的安全部件是否符合 GB/T 20272 中的三级及以上要求	检查操作系统及操作系统相关的安全部件符合 GB/T 20272 中的三级及以上要求的证明材料
3	测试访问控制结构，测试文件系统完整性检查工具	测试查看文件系统信息，包含高速缓存页大小，文件系统使用过程事件记录，测试文件系统具有记录事件的日志系统和基于页的高速缓存能力 通过桌面程序或终端程序测试重要的文件和目录发生的改变事件是否能够被正确监视，并记录到系统日志中
4	测试是否支持操作系统防火墙配置工具	测试能够依据网络上传输的每个 IP 包所含的源地址、目的地址、端口以及包形态等信息，对包进行过滤，控制封包的流通与否 测试能够控制操作系统防火墙网络接口，设定允许进出网络接口的条件以防止网络入侵
5	测试是否支持多种认证机制	测试至少支持以下 2 种或 2 种以上的认证机制： 测试操作系统对用户口令进行强化管理，如对用户名和口令进行分开管理，实现强化管理的口令鉴别 测试操作系统能够采用动态口令鉴别机制，如动态口令 测试操作系统能够使用生物特征鉴别方式，如指纹、虹膜、人脸等生物特征 测试操作系统提供数字证书鉴别机制，如 USB Key
6	测试是否支持底层 BIOS 的安全验证及启动	测试系统启动加载过程应与底层 BIOS 的安全验证接口进行基于证书的认证，经 BIOS 验证通过后系统方可启动引导加载过程
7	测试操作系统不应自行安装不带有有效证书签名的软件和固件组件	通过模拟安装不带有有效证书签名的软件和固件组件的测试，验证系统对于不带有有效证书签名的软件和固件组件的安装策略的有效性、完备性
8	测试是否建立策略来管理软件的安装，防止未授权软件安装	验证操作系统是否支持管理员手动创建、修改、配置、删除组策略，通过组策略命令行工具，检测面向特定用户或计算机策略设置的有效性，设置新的散列规则或修改旧的散列规则，检测其是否能阻止未授权软件的安装

表 4（续）

序号	测试项	测试方法
9	测试是否强制执行最低限度密码复杂度，保障账户安全	测试操作系统在用户口令创建过程中，是否强制执行字符数（大、小写字母、数字和特殊字符）的组合，包括对每个类型的最低限度要求，当检测到口令未满足最低限度要求时，操作系统是否自动采取相关行动（如：提示用户重新输入口令）
10	测试是否安装防篡改保护程序，保护系统组件和系统服务	检查操作系统中的防篡改程序，并通过渗透性测试验证其对逆向工程、替代修改等威胁是否具有较强的识别能力和自我修复能力
11	测试是否支持进程级安全审计，能够记录所有成功和不成功的操作	测试操作系统是否在进程级提供安全审计相关功能，如审计日志、实时报警生成，潜在侵害分析、基于异常检测，基本审计查阅等
12	测试是否保护系统剩余信息安全	测试操作系统中客体在被释放（或删除）时，所占用的磁盘块中的内容是否被清空
13	检查是否存在隐蔽接口或可加载能够禁用或绕过安全机制的组件	检查“不存在隐蔽接口，不加载能够禁用或绕过安全机制的组件”的承诺函，并检查产品的测试端口等是否已关闭
14	测试操作系统厂商是否为产品测试提供所供应产品的接口、协议、加密方式等	验证操作系统厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性，对实现安全功能进行验证
15	测试操作系统厂商是否支持根据用户需求对所供应产品的功能进行裁剪	根据用户常见使用模式，提出不同量级的功能裁剪需求，包括内核级、模块级、功能级等，操作系统厂商按需求进行功能裁剪实现后，验证操作系统厂商根据用户需求对功能进行裁剪的能力

7.2 数据库管理系统

7.2.1 测试内容

测试办公信息系统所采用的数据库管理系统的功能、安全性以及厂商所提供的技术资料的完整性。

7.2.2 测试方法

数据库管理系统测试方法应按表 5 执行。

表 5 数据库管理系统测试方法

序号	测试项	测试方法
1	检查数据库管理系统的字符编码是否符合 GB 18030—2005 的要求	检查符合 GB 18030—2005 的证明材料
2	检查是否符合 GB/T 20273 的要求	检查符合 GB/T 20273 的证明材料

表 5（续）

序号	测试项	测试方法
3	测试数据库管理系统与其他厂商数据库之间的数据迁移	测试被测数据库的数据导入/导出组件/工具是否支持文本文件、通用数据库表、约束、视图等对象和数据的迁移功能；依据技术文档和用户手册，测试是否支持与其他厂商数据库之间的数据迁移功能
4	检查是否存在隐蔽接口或可加载能够禁用或绕过安全机制的组件	检查“不存在隐蔽接口，不加载能够禁用或绕过安全机制的组件”的承诺函，并检查产品的测试端口等是否已关闭
5	测试数据库管理系统厂商是否为产品测试提供所供应产品的接口、协议、加密方式等	验证数据库管理系统厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性，对安全功能进行验证
6	测试数据库管理系统厂商是否支持根据用户需求对所供应产品的功能进行裁剪	提出不同量级的功能裁剪需求，包括内核级、模块级、功能级等，数据库管理系统厂商按需求进行功能裁剪实现后，验证数据库管理系统厂商根据用户需求对功能进行裁剪的能力

7.3 应用服务器中间件

7.3.1 测试内容

测试办公信息系统所采用的应用服务器中间件的功能、安全性以及厂商所提供的技术资料的完整性。

7.3.2 测试方法

应用服务器中间件测试方法应按表 6 执行。

表 6 应用服务器中间件测试方法

序号	测试项	测试方法
1	检查应用服务器中间件的字符编码是否符合 GB 18030—2005 的要求	检查符合 GB 18030—2005 的证明材料
2	测试是否支持对应用的部署、调试和卸载	测试支持对应用的部署，实现对应用程序包的部署、重启，支持动态部署 测试提供对应用的调试，实现应用程序的远程调试和动态调试 测试提供对应用的卸载，实现反部署、停止和卸载
3	测试是否支持对系统性能进行监控和调优、日志管理的管理工具	测试支持对系统性能进行监控和调优、日志管理的管理工具，实现对 HTTP、数据库连接池、JVM 虚拟机等的资源计数器，实现实时监控，并可进行关键参数的配置调优；实现日志功能，能够对日志信息进行配置管理

表 6（续）

序号	测试项	测试方法
4	测试是否支持 Web 组件开发的可视化集成开发工具	测试是否能够以独立或插件形式，提供支持 Web 组件开发的可视化集成开发工具，集成开发工具能够实现对应用服务器的配置部署、启动停止服务、专用工程管理，支持远程部署和调试功能
5	测试是否支持保证数据源恢复和保证事务一致性的系统故障恢复能力	模拟断电、网络、停服务、挂起服务等故障，测试提供保证数据源恢复和保证事务一致性的系统故障恢复能力
6	测试应用服务器中间件对网络数据流的实时监控能力	测试应用服务器中间件同时监控或检测多个网络分片的能力，实现高速聚集的网络数据流的负载均衡；采用主动测试和被动两种不同的检测方法，验证应用服务器中间件依据既定的安全策略和规则，对不同的网络应用行为提供的报警和阻断的能力
7	测试应用服务器中间件是否支持对登录用户进行身份标识和鉴别	测试应用服务器中间件是否提供专用的登陆控制模块对登陆用户身份进行身份验证和鉴别，并检查服务器是否提供了登陆失败处理功能，包括：限制非法登陆次数、登陆失败次数超过设定值则结束会话等 测试已注册用户身份登陆、查看登陆是否成功；测试错误用户名和口令登陆系统，验证鉴别失败处理是否有效
8	测试是否支持访问控制功能，控制用户对服务器数据的访问	测试应用服务器中间件是否提供访问控制用户身份组/用户对服务器数据的访问，检测授权主体是否具有设置用户对服务器数据访问的权限功能，并依据访问控制列表用户和权限的关系，查看不同用户的权限是否与设定的权限是否具有一致性
9	检查是否存在隐蔽接口或可加载能够禁用或绕过安全机制的组件	检查“不存在隐蔽接口，不加载能够禁用或绕过安全机制的组件”的承诺函，并检查产品的测试端口等是否已关闭
10	测试应用服务器中间件厂商是否为产品测试提供所供应产品的接口、协议、加密方式等	验证应用服务器中间件厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性，对安全功能进行验证
11	测试应用服务器中间件厂商是否支持根据用户需求对所供应产品的功能进行裁剪	提出不同量级的功能裁剪需求，包括内核级、模块级、功能级等，应用服务器中间件厂商按需求进行功能裁剪实现后，验证应用服务器厂商根据用户需求对功能进行裁剪的能力

7.4 办公软件

7.4.1 测试内容

测试办公信息系统所采用的办公软件的功能、安全性以及厂商所提供的技术资料的完整性。

7.4.2 测试方法

办公软件测试方法应按表 7 执行。

表 7 办公软件测试方法

序号	测试项	测试方法
1	检查办公软件的字符编码是否符合 GB 18030—2005 的要求	检查符合 GB 18030—2005 的证明材料
2	检查是否符合 GB/T 26856—2011 的要求	检查符合 GB/T 26856—2011 的证明材料
3	检查版式文档是否符合 GB/T 33190—2016 的要求	检查符合 GB/T 33190—2016 的证明材料
4	测试办公软件对浏览器的支持能力	检查是否具有浏览器插件，并测试是否能够跨浏览器环境正常运行
5	测试办公软件是否支持对文件加密的能力	检查办公软件是否具有加密选项，并测试在拥有正确密钥的情况下，是否具有正确打开加密文件的能力
6	检查是否存在隐蔽接口或可加载能够禁用或绕过安全机制的组件	检查“不存在隐蔽接口，不加载能够禁用或绕过安全机制的组件”的承诺函，并检查产品的测试端口等是否已关闭
7	测试办公软件厂商是否为产品测试提供所供应产品的接口、协议、加密方式等	验证办公软件厂商为产品测试提供的产品接口、协议、加密方式的完备性和真实性，对安全功能进行验证
8	测试办公软件厂商是否支持根据用户需求对所供应产品的功能进行裁剪	提出不同量级的功能裁剪需求，包括内核级、模块级、功能级等，办公软件厂商按需求进行功能裁剪实现后，验证办公软件厂商根据用户需求对功能进行裁剪的能力

8 网络设施测试

8.1 网络设备

8.1.1 测试内容

测试办公信息系统所采用的交换机、路由器等网络设备的功能以及安全性。

8.1.2 测试方法

网络设备测试方法应按表 8 执行。

表 8 网络设备测试方法

序号	测试项	测试方法
1	检查是否符合 GB/T 21050—2007 的要求	检查符合 GB/T 21050—2007 的证明材料
2	检查是否符合 GB/T 18018 中第三级安全要求	检查符合 GB/T 18018 中第三级安全要求的证明材料

8.2 安全设备

8.2.1 测试内容

测试办公信息系统所采用的防火墙和入侵检测系统等安全设备的功能以及安全性。

8.2.2 测试方法

安全设备测试方法应按表9执行。

表9 安全设备测试方法

序号	测试项	测试方法
1	检查防火墙是否符合GB/T 20281—2015的要求	检查防火墙符合GB/T 20281—2015的证明材料
2	检查入侵检测系统是否符合GB/T 20275—2013的要求	检查入侵检测系统符合GB/T 20275—2013的证明材料

9 应用软件系统测试

9.1 功能性

9.1.1 测试内容

测试应用软件系统的功能，包括公文管理、归档管理、公告、通知、会议管理、个人工作区、个人信息管理、在线人员列表、管理员用户等。

9.1.2 测试方法

应用软件系统功能性测试方法应按表10执行。

表10 应用软件系统功能性测试方法

序号	测试项	测试方法
1	测试公文管理功能	通过操作应用软件系统测试公文流转功能，测试拟稿、核稿、编辑、审核、撤销、退回、签发、选择下一环节、发送、签收、会签、登记、拟办、审阅、分办、承办、办结、归档等功能，测试增加和删除附件功能，测试流程跟踪和查看功能
2	测试归档管理功能	通过操作应用软件系统测试归档管理功能，测试公文归档、归档查询功能
3	测试公告功能	通过操作应用软件系统测试归档管理功能，测试新建、修改、删除、发布等功能
4	测试通知功能	通过操作应用软件系统测试通知功能，测试新建、修改、删除、发布等功能

表 10（续）

序号	测试项	测试方法
5	测试会议管理功能	通过操作应用软件系统测试会议室管理功能，测试新建、修改、删除、查询会议室等功能；通过操作应用软件系统测试会议安排功能，测试新建、修改、删除、查询、打印会议信息等功能
6	测试个人工作区功能	通过操作应用软件系统测试个人工作区功能，测试个人待办、个人已办功能
7	测试个人信息管理功能	通过操作应用软件系统测试个人信息管理功能，测试修改个人信息、修改个人密码功能
8	测试在线人员列表功能	通过操作应用软件系统测试在线人员列表功能功能，测试在线人员的姓名、所属部门、职位信息等
9	测试管理员用户	通过管理员用户登录应用软件系统，测试管理员用户支持用户管理、统一权限管理等功能，测试用户的新建、修改、删除功能，测试基于功能授权功能，测试基于用户授权功能

9.2 安全性

9.2.1 测试内容

测试应用软件系统的安全性。

9.2.2 测试方法

应用软件系统安全性测试方法应按表 11 执行。

表 11 应用软件系统安全性测试方法

序号	测试项	测试方法
1	检查是否符合 GB/T 28452—2012 中应用软件系统安全技术要求第三级及以上要求	检查符合 GB/T 28452—2012 中应用软件系统安全技术要求第三级及以上要求的证明材料
2	检查是否存在隐蔽接口或可加载能够禁用或绕过安全机制的组件	检查“不存在隐蔽接口，不加载能够禁用或绕过安全机制的组件”的承诺函，并检查产品的测试端口等是否已关闭
3	检查是否具备“应在用户明示同意后，方可收集用户相关信息”的承诺函，测试在收集用户相关信息时是否显示提示信息	检查“应在用户明示同意后，方可收集用户相关信息”的承诺函；通过测试收集用户信息的相关功能，检查是否显示提示信息
4	检查是否具备“在应用软件系统维护升级更新活动中，不得侵害用户信息安全”的承诺函	检查“在应用软件系统维护升级更新活动中，不得侵害用户信息安全”的承诺函

9.3 可靠性

9.3.1 测试内容

测试应用软件系统的可靠性，包括成熟度、容错性、易恢复性等。

9.3.2 测试方法

应用软件系统可靠性测试方法应按表 12 执行。

表 12 应用软件系统可靠性测试方法

序号	测试项	测试方法
1	测试系统长时间运行的能力	通过人工和工具相互结合的方式，7×24 h 运行应用软件系统，验证应用软件系统服务器端、客户端能支持 7×24 h 稳定运行，不崩溃不丢失数据
2	测试系统的数据有效性检验功能	通过边界值分析法、等价类划分法等方法设计测试数据，检查系统是否提供数据有效性检验功能，保证输入的数据格式或长度符合系统设定的要求
3	测试系统对用户非法的输入或操作的容错能力	通过边界值分析法、等价类划分法、错误推断法、场景法等方法设计非法的测试数据，测试用户非法的输入或操作时，系统不崩溃、不退出
4	测试系统的自动保护功能	人工模拟制造网络故障，验证由于网络故障所导致的系统故障恢复后，系统可恢复到故障点状态，数据不丢失

9.4 易用性

9.4.1 测试内容

测试应用软件系统的易用性，包括易理解性、易操作性、易学习性等。

9.4.2 测试方法

应用软件系统易用性测试方法应按表 13 执行。

表 13 应用软件系统易用性测试方法

序号	测试项	测试方法
1	检查用户手册是否符合要求	通过检查系统提供用户手册，对照系统实际操作，确认手册中的功能描述与软件的实际功能一致
2	检查过程文档是否符合要求	通过检查系统研制过程中形成的所有文档，确认文档内容语言简练、前后一致、易于理解以及语句无歧义
3	检查页面布局是否符合要求	通过检查系统各页面，确认系统页面布局合理，不过于密集，也不过于空旷，合理利用空间

表 13（续）

序号	测试项	测试方法
4	检查系统的提示、警告、或错误说明是否符合要求	通过实际操作应用软件系统，确认系统的提示、警告或错误说明清楚、明了、恰当，避免歧义
5	检查必输项标识是否符合要求	通过检查系统各编辑页面，确认编辑页面中的必输项都给出了标识
6	对于“非法”的输入或操作，测试系统是否给予提示信息	通过实际操作应用软件系统，确认系统对于用户非法的输入或操作，给予提示信息，且提示信息能引导用户进行正确输入或操作
7	对于可能造成数据无法恢复的操作，测试系统是否给予提示信息	通过实际操作应用软件系统，确认系统对于可能造成数据无法恢复的操作，给予提示信息，给用户放弃选择的机会
8	测试日期类型数据输入是否提供日历选择功能	通过检查系统各页面，确认日期类型数据输入提供了日历选择功能
9	测试系统是否支持快捷键操作	通过实际操作应用软件系统，确认系统对于 Ctrl＋A 全选、Ctrl＋C 拷贝、Ctrl＋V 粘贴、Ctrl＋X 剪切、Ctrl＋Z 撤消等快捷键的支持
10	Tab 键变更光标焦点	通过实际操作应用软件系统，确认系统中有多个输入框的页面，支持通过 Tab 键变更光标焦点，按照从左到右、从上到下的原则

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
办公信息系统安全测试规范
GB/T 37096—2018
*
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(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019 年 1 月第一版
*
书号:155066·1-62133

GB/T 37096-2018