ICS 35.020
L 09

中华人民共和国国家标准

GB/T 20008—2005

信息安全技术
操作系统安全评估准则

Information security technology—
Operating systems security evaluation criteria

2005-11-11 发布　　2006-05-01 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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
操作系统安全评估准则
GB/T 20008—2005
*
中 国 标 准 出 版 社 出 版 发 行
北京西城区复兴门外三里河北街 16 号
邮政编码:100045
http://www.spc.net.cn
电话:63787337、63787447
2006 年 5 月第一版　2006 年 5 月电子版制作
*
书号:155066·1-27492

目　　次

前　言

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全等级管理的重要标准，已于1999年9月13日发布。为促进安全等级管理工作的正常有序开展，特制定一系列相关的标准。本标准是系列标准之一。

本标准文本中，黑体字表示较低等级中没有出现或增强的评估内容。

本标准的附录A中说明操作系统面临的主要威胁和对策。

本标准的附录A是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京大学软件工程国家工程中心，公安部公共信息网络安全监察局。

本标准主要起草人：王立福，赵学志，刘学洋，葛佳。

引　言

操作系统是管理硬件资源、控制程序运行、改善人机界面和为应用软件提供支持的一种系统软件。它是最靠近硬件的一层软件，将物理机器（裸机）扩展成可靠性高、使用方便、功能齐全的理想机器。操作系统设计的好坏直接影响计算机系统的性能，操作系统还应考虑系统的各个方面，任何遗漏或考虑不周都会影响计算机的工作。

用户使用计算机实际上是通过操作系统进行的，操作系统提供给用户的使用手段（或称界面）主要有三种：终端命令、系统调用和作业控制语言。

信息安全技术
操作系统安全评估准则

1 范围

本标准从信息技术方面规定了按照GB 17859—1999的五个安全保护等级对操作系统安全保护等级划分所需要的评估内容。

本标准适用于计算机通用操作系统的安全保护等级的评估，对于通用操作系统安全功能的研制、开发和测试亦可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型(idt ISO/IEC 15408-1：1999)

3 术语和定义

GB 17859—1999和GB/T 18336.1—2001确立的术语和定义适用于本标准。

4 安全环境

4.1 物理方面

对操作系统资源的处理限定在一些可控制的访问设备内，防止未授权的物理访问。所有与实施操作系统安全策略相关的硬件和软件，应受到保护以免于未授权的物理修改。

4.2 人员方面

有一个或多个能胜任的授权用户来管理操作系统及所包含的信息。管理员遵从管理员指南实施管理，可能有偶然的失误，但不是恶意或敌对的。授权用户支配必要的授权来访问由操作系统管理的最少量的信息。

4.3 连通性方面

若操作系统包含多个工作站点，则各网络信息服务域中的所有工作站点都由一个中心工作站点管理。网络信息服务域可以由多个管理域组成，管理员管理本地资源和用户账号，在整个信息服务域中对资源进行无缝操作应是可能的。所有网络设备都能正确地没有改动地传送数据。

5 评估内容

5.1 用户自主保护级

5.1.1 自主访问控制

操作系统安全功能应实施安全机制，控制用户对客体的访问，其方法可以是：

——基于用户的权能表，为用户规定是否可以对客体进行访问；

——基于客体的访问控制表。

5.1.2 身份鉴别

5.1.2.1 用户属性定义

操作系统安全功能应给出每一个用户与标识相关的安全属性(如:组、标识符等)。

5.1.2.2 用户标识

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作,在用户被标识之前,允许操作系统执行这些预设动作。在操作系统安全功能的其他动作之前,应成功地标识每个用户。

5.1.2.3 用户鉴别

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作,在用户被鉴别之前,允许操作系统执行这些预设动作,在操作系统安全功能的其他动作之前,应成功地鉴别每个用户。

5.1.2.4 鉴别失败处理

操作系统安全功能应检测出不成功的鉴别尝试,当尝试的次数达到或超过了定义的界限时,应能终止会话建立的进程。

5.1.2.5 访问历史

操作系统安全功能在会话成功建立的基础上,应显示用户上一次成功会话建立的日期、时间、方法、位置等。

5.1.3 数据完整性

在规定的客体上,操作系统安全功能应允许特定操作的回退。

5.1.4 数据传输

5.1.4.1 内部传输

在各部分(如:通过网络连接、总线连接的各部分)之间传递用户数据时,操作系统安全功能应执行特定的安全功能策略。

5.1.4.2 数据外部输出

向操作系统安全功能控制范围之外输出用户数据时,操作系统安全功能应在访问控制机制允许的前提下,执行特定的安全功能策略,进行用户数据输出。

5.1.4.3 数据外部输入

从操作系统安全功能控制范围之外输入用户数据时,操作系统安全功能应执行特定的安全功能策略。

5.1.5 密码支持

5.1.5.1 密钥管理

操作系统安全功能能根据符合国家规定的方法来管理密钥,包括:密钥的产生、分发、访问及销毁。

5.1.5.2 密码运算

操作系统安全功能能根据符合国家规定的密码算法和密钥长度来执行密码运算。

5.1.6 资源利用

5.1.6.1 资源分配

操作系统安全功能能为主体规定并执行某些受控资源的最高配额和使用时间,并确保主体至少获得规定的最低配额。

5.1.6.2 并发会话

操作系统安全功能能限制属于同一用户的并发会话的最大数目。

5.1.7 安全功能保护

5.1.7.1 时间戳

操作系统安全功能应为自身的应用提供可靠的时间戳。

5.1.7.2　安全功能数据传输

在各部分间传输操作系统安全功能数据时，操作系统安全功能能保护安全功能数据，防止被泄漏及修改。

5.1.7.3　系统恢复

当操作系统发生失败或服务中断后，操作系统安全功能应进入维护方式，并提供将操作系统返回到一个安全状态的能力。

5.1.8　安全管理

5.1.8.1　功能管理

操作系统安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.1.8.2　属性管理

操作系统安全功能应执行访问控制策略，仅允许授权管理员管理安全属性。

5.1.8.3　安全功能数据管理

操作系统安全功能应限制管理员查询、修改或删除操作系统安全功能数据的能力。仅允许授权管理员管理这些数据。

5.1.9　配置管理

开发者提供的配置管理文档应以版本号做标签，为操作系统提供引用，使一个版本号对应操作系统的唯一版本。

5.1.10　安全功能开发过程

开发者提供的操作系统安全功能的功能规约应描述安全功能及其与外部的接口。

5.1.11　测试

5.1.11.1　功能测试

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能、描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

5.1.11.2　覆盖分析

开发者提供的测试覆盖的证据，应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

5.1.12　指导性文档

5.1.12.1　管理员指南

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理操作系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.1.12.2　用户指南

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责，包括用户行为假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.1.13　交付和运行

开发者提供的安全安装过程的文档应说明用于操作系统的安全安装、生成和启动的过程所必需的步骤，并应描述一个启动程序，它包含了用以生成操作系统的选项，从而能决定操作系统是如何以及何时产生的。

5.2　系统审计保护级

5.2.1　自主访问控制

操作系统安全功能应实施安全机制，控制用户对客体的访问，其方法可以是：

——基于用户的权能表，为用户规定是否可以对客体进行访问；

——基于客体的访问控制表。

操作系统安全功能的访问控制粒度应是单个用户。

5.2.2 **身份鉴别**

5.2.2.1 **用户属性定义**

操作系统安全功能应给出每一个用户与标识相关的安全属性(如:组、标识符等)。

5.2.2.2 **用户标识**

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作,在用户被标识之前,允许操作系统执行这些预设动作。在操作系统安全功能的其他动作之前,应成功地标识每个用户。

5.2.2.3 **用户鉴别**

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作,在用户被鉴别之前,允许操作系统执行这些预设动作,在操作系统安全功能的其他动作之前,应成功地鉴别每个用户。

当进行鉴别时,操作系统安全功能应仅将最少的反馈(如:打入的字符数,鉴别的成功或失败)提供给用户。

5.2.2.4 **鉴别失败处理**

操作系统安全功能应检测出不成功的鉴别尝试,当尝试的次数达到或超过了定义的界限时,应能终止会话建立的进程。

5.2.2.5 **访问历史**

操作系统安全功能在会话成功建立的基础上,应显示用户上一次成功会话建立的日期、时间、方法、位置等。

操作系统安全功能应显示用户上一次不成功的会话尝试的日期、时间、方法、位置等,以及从上一次成功的会话建立以来的不成功的尝试次数。

5.2.3 **客体重用**

对于操作系统中的所有客体,在指定、分配或再分配给一个主体时,操作系统安全功能应确保其中没有上一次分配的剩余信息。

5.2.4 **审计**

5.2.4.1 **内容**

操作系统安全功能应能为操作系统的可审计事件生成一个审计记录,并在每一个审计记录中至少记录以下信息:

——事件发生的日期和时间;

——事件的类型;

——用户身份;

——事件的结果(成功或失败)。

操作系统安全功能应能维护操作系统的可审计事件,但其中至少包括:

——开启和关闭审计功能;

——客体创建与删除;

——使用鉴别机制;

——将客体引入用户地址空间;

——安全属性的操作等。

5.2.4.2 **查阅**

操作系统安全功能应为授权用户提供从审计记录中读取一定类型的审计信息的能力。

5.2.4.3 **存储保护**

操作系统安全功能应保护已存储的审计记录，以避免未授权的删除，并监测对审计记录的修改，当审计存储已满、失败或受到攻击时，操作系统安全功能应确保审计记录保持一定的记录数和维持的时间。

5.2.4.4 自动响应

在检测到可能的安全侵害时，操作系统安全功能应做出响应，如：

——通知授权用户；

——向授权用户提供一组遏制侵害的或采取校正的行动。

5.2.5 数据完整性

5.2.5.1 回退

在规定的客体上，操作系统安全功能应允许特定操作的回退。

5.2.5.2 完整性监视

对于特定的客体，操作系统安全功能能监视所存储的用户数据是否出现完整性错误，如：磁盘设备的扫描程序。

5.2.6 数据传输

5.2.6.1 内部传输

在各部分（如：通过网络连接、总线连接的各部分）之间传递用户数据时，操作系统安全功能应执行特定的安全功能策略。

5.2.6.2 数据外部输出

向操作系统安全功能控制范围之外输出用户数据时，操作系统安全功能应在访问控制机制允许的前提下，执行特定的安全功能策略，进行用户数据输出。

向操作系统安全功能控制范围之外输出与用户数据相关的安全属性时，操作系统安全功能应确保安全属性与输出的用户数据相关。

5.2.6.3 数据外部输入

从操作系统安全功能控制范围之外输入用户数据时，操作系统安全功能应执行特定的安全功能策略。

操作系统安全功能应使用与输入的数据相关的安全属性，确保在安全属性和接受的用户数据之间提供了确切的关联。

5.2.6.4 原发证明

操作系统安全功能应能对发出的信息产生原发证据。

5.2.6.5 接收证明

操作系统安全功能应能对接收的信息产生接收证据。

5.2.7 密码支持

5.2.7.1 密钥管理

操作系统安全功能能根据符合国家规定的方法来管理密钥，包括：密钥的产生、分发、访问及销毁。

5.2.7.2 密码运算

操作系统安全功能能根据符合国家规定的密码算法和密钥长度来执行密码运算。

5.2.8 资源利用

5.2.8.1 容错

操作系统安全功能能检测出已规定的操作系统故障。

5.2.8.2 服务优先级

操作系统安全功能应为其中的每个主体规定一种优先级，对于特定的资源的访问，能根据主体的优先级进行协调。

5.2.8.3 资源分配

操作系统安全功能能为主体规定并执行某些受控资源的最高配额和使用时间，并确保主体至少获得规定的最低配额。

5.2.8.4 并发会话

操作系统安全功能能限制属于同一用户的并发会话的最大数目。

5.2.9 安全功能保护

5.2.9.1 自检

操作系统安全功能应在操作系统的特定状态中，运行一套自检来演示操作系统安全功能的正确执行。这些状态应包括：

——操作系统启动时；

——授权用户要求时。

5.2.9.2 时间戳

操作系统安全功能应为自身的应用提供可靠的时间戳。

5.2.9.3 数据一致性

操作系统安全功能应确保操作系统各部分间的安全功能数据的复制一致性。

5.2.9.4 安全功能数据传输

在各部分间传输操作系统安全功能数据时，操作系统安全功能能保护安全功能数据，防止被泄漏及修改。

操作系统安全功能应分离传送用户数据与安全功能数据。

5.2.9.5 系统恢复

当操作系统发生失败或服务中断后，操作系统安全功能应进入维护方式，并提供将操作系统返回到一个安全状态的能力。

5.2.9.6 不可旁路

在操作系统安全功能控制范围的每一项功能执行之前，操作系统安全功能应确保安全功能被成功地激活。

5.2.10 安全管理

5.2.10.1 功能管理

操作系统安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.2.10.2 属性管理

操作系统安全功能应执行访问控制策略，仅允许授权管理员管理安全属性。

操作系统安全功能应提供安全属性的默认值，仅允许授权管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

5.2.10.3 安全功能数据管理

操作系统安全功能应限制管理员查询、修改或删除操作系统安全功能数据的能力。仅允许授权管理员管理这些数据。

操作系统安全功能应支持规定对操作系统安全功能数据的限制以及限制值(如：用户登录数)，当操作系统安全功能数据值超出了指定的限制时，应采取特定的动作。

5.2.11 生存周期支持

开发者提供的缺陷纠正程序文档应描述用以接受用户对于安全缺陷报告的程序，以及更正这些缺陷的程序，并说明已采取的纠正措施。

5.2.12 配置管理

开发者提供的配置管理文档应以版本号做标签，为操作系统提供引用，使一个版本号对应操作系统的唯一版本。

5.2.13 安全功能开发过程

5.2.13.1 功能规约

开发者提供的操作系统安全功能的功能规约应描述安全功能及其与外部的接口。

5.2.13.2 高层设计

开发者提供的操作系统安全功能的高层设计，应按子系统方式描述安全功能及其结构，并标识安全功能子系统的所有接口。

5.2.14 测试

5.2.14.1 功能测试

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能、描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

5.2.14.2 覆盖分析

开发者提供的测试覆盖的证据，应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者提供的测试覆盖的证据，应阐明测试文档所标识的测试和功能规约中所描述的安全功能之间的对应性是完备的。

5.2.15 指导性文档

5.2.15.1 管理员指南

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理操作系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.2.15.2 用户指南

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责，包括用户行为假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.2.16 交付和运行

5.2.16.1 交付

开发者提供的交付文档应向用户说明维护安全所应具有的交付程序。

5.2.16.2 安装生成

开发者提供的安全安装过程的文档应说明用于操作系统的安全安装、生成和启动的过程所必需的步骤，并应描述一个启动程序，它包含了用以生成操作系统的选项，从而能决定操作系统是如何以及何时产生的。

5.3 安全标记保护级

5.3.1 自主访问控制

操作系统安全功能应实施安全机制，控制用户对客体的访问，其方法可以是：

——基于用户的权能表，为用户规定是否可以对客体进行访问；

——基于客体的访问控制表。

操作系统安全功能的访问控制粒度应是单个用户。

5.3.2 强制访问控制

操作系统安全功能应通过主客体的敏感标记，控制用户对相关客体的直接访问。

5.3.3 标记

5.3.3.1 标记定义

操作系统安全功能应给出其控制范围内所有主体及控制的客体的敏感标记。

5.3.3.2 标记管理

操作系统安全功能应执行访问控制策略，仅允许授权管理员管理敏感标记。

5.3.3.3 带标记数据输入

从操作系统安全功能控制范围之外输入带标记的数据时，操作系统安全功能应确保标记和接受的用户数据相关。

5.3.4 身份鉴别

5.3.4.1 用户属性定义

操作系统安全功能应给出每一个用户与标识相关的安全属性（如：组、标识符等）。

5.3.4.2 用户标识

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作，在用户被标识之前，允许操作系统执行这些预设动作。在操作系统安全功能的其他动作之前，应成功地标识每个用户。

5.3.4.3 用户鉴别

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作，在用户被鉴别之前，允许操作系统执行这些预设动作，在操作系统安全功能的其他动作之前，应成功地鉴别每个用户。

当进行鉴别时，操作系统安全功能应仅将最少的反馈（如：打入的字符数，鉴别的成功或失败）提供给用户。

操作系统安全功能应提供多鉴别机制以支持用户多鉴别。

5.3.4.4 鉴别失败处理

操作系统安全功能应检测出不成功的鉴别尝试，当尝试的次数达到或超过了定义的界限时，应能终止会话建立的进程。

在会话建立的进程终止后，操作系统安全功能应能使得该用户账户无效，或是进行鉴别尝试的登录站点无效。

5.3.4.5 访问历史

操作系统安全功能在会话成功建立的基础上，应显示用户上一次成功会话建立的日期、时间、方法、位置等。

操作系统安全功能应显示用户上一次不成功的会话尝试的日期、时间、方法、位置等，以及从上一次成功的会话建立以来的不成功的尝试次数。

5.3.5 客体重用

对于操作系统中的所有客体，在指定、分配或再分配给一个主体时，操作系统安全功能应确保其中没有上一次分配的剩余信息。

5.3.6 审计

5.3.6.1 内容

操作系统安全功能应能为操作系统的可审计事件生成一个审计记录，并在每一个审计记录中至少记录以下信息：

——事件发生的日期和时间；

——事件的类型；

——用户身份；

——事件的结果（成功或失败）。

操作系统安全功能应能维护操作系统的可审计事件，但其中至少包括：

——开启和关闭审计功能；

——客体创建与删除；

——使用鉴别机制；

——将客体引入用户地址空间；

——安全属性的操作等。

5.3.6.2 查阅

操作系统安全功能应为授权用户提供从审计记录中读取一定类型的审计信息的能力。

操作系统安全功能应提供对审计数据进行基于一定准则的选择查阅的能力，并能对结果进行搜索、分类或排序。

5.3.6.3 存储保护

操作系统安全功能应保护已存储的审计记录，以避免未授权的删除，并监测对审计记录的修改，当审计存储已满、失败或受到攻击时，操作系统安全功能应确保审计记录保持一定的记录数和维持的时间。

当审计记录超过预定的限制值时，操作系统安全功能应采取相应的行动，如：给授权管理员产生警告。

5.3.6.4 分析

操作系统安全功能应能用一定的规则去监控审计事件，并指出潜在的侵害。

5.3.6.5 自动响应

在检测到可能的安全侵害时，操作系统安全功能应做出响应，如：

——通知授权用户；

——向授权用户提供一组遏制侵害的或采取校正的行动。

5.3.7 数据完整性

5.3.7.1 数据鉴别

操作系统安全功能能为用户数据产生真实性证据（如：校验码、单向函数、数字签名）。

5.3.7.2 回退

在规定的客体上，操作系统安全功能应允许特定操作的回退。

操作系统安全功能能规定回退可以实施的严格条件，包括：

——回退的操作时限；

——回退的次数限制；

——实施回退的角色要求等。

5.3.7.3 完整性监视

对于特定的客体，操作系统安全功能能监视所存储的用户数据是否出现完整性错误，如：磁盘设备的扫描程序。

当检测到完整性错误时，操作系统安全功能应采取行动（如：提示管理员）。

5.3.8 数据传输

5.3.8.1 内部传输

在各部分（如：通过网络连接、总线连接的各部分）之间传递用户数据时，操作系统安全功能应执行特定的安全功能策略。

操作系统安全功能应监视是否有完整性错误出现。

5.3.8.2 数据外部输出

向操作系统安全功能控制范围之外输出用户数据时，操作系统安全功能应在访问控制机制允许的前提下，执行特定的安全功能策略，进行用户数据输出。

向操作系统安全功能控制范围之外输出与用户数据相关的安全属性时，操作系统安全功能应确保安全属性与输出的用户数据相关。

5.3.8.3 数据外部输入

从操作系统安全功能控制范围之外输入用户数据时，操作系统安全功能应执行特定的安全功能策略。

操作系统安全功能应使用与输入的数据相关的安全属性，确保在安全属性和接受的用户数据之间提供了确切的关联。

5.3.8.4 原发证明

操作系统安全功能应能对发出的信息产生原发证据。

操作系统安全功能应能将信息原发者的相关属性与证据适用的信息内容相关联。

5.3.8.5 接收证明

操作系统安全功能应能对接收的信息产生接收证据。

操作系统安全功能应能将信息接收者的相关属性与证据适用的信息内容相关联。

5.3.9 密码支持

5.3.9.1 密钥管理

操作系统安全功能能根据符合国家规定的方法来管理密钥，包括：密钥的产生、分发、访问及销毁。

5.3.9.2 密码运算

操作系统安全功能能根据符合国家规定的密码算法和密钥长度来执行密码运算。

5.3.10 资源利用

5.3.10.1 容错

操作系统安全功能能检测出已规定的操作系统故障。

5.3.10.2 服务优先级

操作系统安全功能应为其中的每个主体规定一种优先级，对于特定的资源的访问，能根据主体的优先级进行协调。

5.3.10.3 资源分配

操作系统安全功能能为主体规定并执行某些受控资源的最高配额和使用时间，并确保主体至少获得规定的最低配额。

5.3.10.4 并发会话

操作系统安全功能能限制属于同一用户的并发会话的最大数目。

5.3.11 安全功能保护

5.3.11.1 自检

操作系统安全功能应在操作系统的特定状态中，运行一套自检来演示操作系统安全功能的正确执行。这些状态应包括：

——操作系统启动时；

——授权用户要求时。

操作系统安全功能应为授权用户提供对操作系统安全功能数据完整性的验证能力。

5.3.11.2 时间戳

操作系统安全功能应为自身的应用提供可靠的时间戳。

5.3.11.3 域分离

操作系统安全功能应分离在操作系统安全功能控制范围内各主体安全域，用户进程之间是彼此隔离的。

5.3.11.4 数据一致性

操作系统安全功能应确保操作系统各部分间的安全功能数据的复制一致性。

5.3.11.5 安全功能数据传输

在各部分间传输操作系统安全功能数据时，操作系统安全功能能保护安全功能数据，防止被泄漏及修改。

操作系统安全功能应分离传送用户数据与安全功能数据。

操作系统安全功能能检测出安全功能数据的完整性错误。

5.3.11.6 系统恢复

当操作系统发生失败或服务中断后，操作系统安全功能应进入维护方式，并提供将操作系统返回到一个安全状态的能力。

操作系统安全功能应具备从失败或服务中断状态中自动恢复的能力，并能在操作系统安全功能数据和用户数据无超量丢失的情况下恢复到初始安全状态。

5.3.11.7 不可旁路

在操作系统安全功能控制范围的每一项功能执行之前，操作系统安全功能应确保安全功能被成功地激活。

5.3.11.8 物理保护

操作系统安全功能应对可能危及操作系统安全功能安全的物理篡改提供明确的检测，并能判断出特定的物理篡改。

5.3.12 安全管理

5.3.12.1 功能管理

操作系统安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.3.12.2 属性管理

操作系统安全功能应执行访问控制策略，仅允许授权管理员管理安全属性。

操作系统安全功能应提供安全属性的默认值，仅允许授权管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

操作系统安全功能应确保安全属性只接受安全的值。

5.3.12.3 安全功能数据管理

操作系统安全功能应限制管理员查询、修改或删除操作系统安全功能数据的能力。仅允许授权管理员管理这些数据。

操作系统安全功能应支持规定对操作系统安全功能数据的限制以及限制值(如：用户登录数)，当操作系统安全功能数据值超出了指定的限制时，应采取特定的动作。

5.3.12.4 角色管理

操作系统安全功能应支持维护授权角色。

5.3.13 生存周期支持

5.3.13.1 开发安全

开发者提供的开发安全文件应描述在操作系统开发环境中在物理上、程序上、人员上以及其他方面的安全措施。

5.3.13.2 缺陷纠正

开发者提供的缺陷纠正程序文档，应描述用以接受用户对于安全缺陷报告的程序，以及更正这些缺陷的程序，并说明已采取的纠正措施。

5.3.13.3 工具和技术

开发者提供的开发工具文档应标识在开发操作系统中使用的工具和参照的标准，并描述有关实现的开发工具的选项。

5.3.14 配置管理

5.3.14.1 能力

开发者提供的配置管理文档应以版本号做标签，为操作系统提供引用，使一个版本号对应操作系统的唯一版本。

开发者提供的配置管理文档应包括配置清单、配置管理计划和接受计划，其中配置清单应描述对配置项进行唯一标识的方法，并清楚地标识出组成安全功能的配置项，并提供保证对配置项只进行授权修改的方法。

5.3.14.2 范围

开发者提供的配置管理文档应描述配置管理系统是如何跟踪配置项的，并说明至少能跟踪：操作系统实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档。

5.3.15 安全功能开发过程

5.3.15.1 安全策略模型

开发者提供的安全策略模型应描述所有可以模型化的安全策略的规则和特性。

5.3.15.2 功能规约

开发者提供的操作系统安全功能的功能规约应描述安全功能及其与外部的接口。

开发者提供的操作系统安全功能的功能规约应完备地表示安全功能。

5.3.15.3 高层设计

开发者提供的操作系统安全功能的高层设计，应按子系统方式描述安全功能及其结构，并标识安全功能子系统的所有接口。

开发者提供的操作系统安全功能的高层设计，应将有关安全功能策略实施的子系统与其他子系统分离。

5.3.15.4 低层设计

开发者提供的操作系统安全功能的低层设计应以模块术语描述安全功能，并描述每一个模块的目的、接口。

5.3.15.5 实现

开发者提供的操作系统安全功能的实现表示（如：源代码、硬件图）文档应是内在一致的，并且无歧义地定义了详细的操作系统安全功能。

5.3.15.6 表示对应性

对于所提供的安全策略表示的每个相邻对，开发者应提供相邻两阶段开发文档之间的对应性分析，并阐明上一阶段的安全策略表示在下一阶段文档中得到正确而完备地细化。

5.3.16 测试

5.3.16.1 功能测试

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能、描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

5.3.16.2 覆盖分析

开发者提供的测试覆盖的证据，应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者提供的测试覆盖的证据，应阐明测试文档所标识的测试和功能规约中所描述的安全功能之间的对应性是完备的。

5.3.16.3 深度

开发者提供的测试深度分析文档应说明测试文档中所标识的测试足以说明该安全功能动作和高层设计是一致的。

5.3.17 指导性文档

5.3.17.1 管理员指南

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理操作系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.3.17.2 用户指南

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责，

包括用户行为假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.3.18 脆弱性

开发者提供的脆弱性分析文档应标识脆弱性的分布，并说明在所期望的环境中这些脆弱性不会被利用。

5.3.19 交付和运行

5.3.19.1 交付

开发者提供的交付文档应向用户说明维护安全所应具有的交付程序。

5.3.19.2 安装生成

开发者提供的安全安装过程的文档应说明用于操作系统的安全安装、生成和启动的过程所必需的步骤，并应描述一个启动程序，它包含了用以生成操作系统的选项，从而能决定操作系统是如何以及何时产生的。

5.4 结构化保护级

5.4.1 自主访问控制

操作系统安全功能应实施安全机制，控制用户对客体的访问，其方法可以是：

——基于用户的权能表，为用户规定是否可以对客体进行访问；

——基于客体的访问控制表。

操作系统安全功能的访问控制粒度应是单个用户。

5.4.2 强制访问控制

操作系统安全功能应通过主客体的敏感标记，控制用户对相关客体的直接访问。

操作系统安全功能应实施安全机制，控制所有主客体之间的访问。

5.4.3 标记

5.4.3.1 标记定义

操作系统安全功能应给出其控制范围内所有主体和客体的敏感标记。

5.4.3.2 标记管理

操作系统安全功能应执行访问控制策略，仅允许授权管理员管理敏感标记。

5.4.3.3 带标记数据输入

从操作系统安全功能控制范围之外输入带标记的数据时，操作系统安全功能应确保标记和接受的用户数据相关。

5.4.4 身份鉴别

5.4.4.1 用户属性定义

操作系统安全功能应给出每一个用户与标识相关的安全属性(如：组、标识符等)。

5.4.4.2 用户标识

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作，在用户被标识之前，允许操作系统执行这些预设动作。在操作系统安全功能的其他动作之前，应成功地标识每个用户。

5.4.4.3 用户鉴别

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作，在用户被鉴别之前，允许操作系统执行这些预设动作，在操作系统安全功能的其他动作之前，应成功地鉴别每个用户。

当进行鉴别时，操作系统安全功能应仅将最少的反馈(如：打入的字符数，鉴别的成功或失败)提供给用户。

操作系统安全功能应提供多鉴别机制表以支持用户多鉴别。

5.4.4.4 鉴别失败处理

操作系统安全功能应检测出不成功的鉴别尝试，当尝试的次数达到或超过了定义的界限时，应能终止会话建立的进程。

在会话建立的进程终止后，操作系统安全功能应能使得该用户账户无效，或是进行鉴别尝试的登录站点无效。

5.4.4.5 访问历史

操作系统安全功能在会话成功建立的基础上，应显示用户上一次成功会话建立的日期、时间、方法、位置等。

操作系统安全功能应显示用户上一次不成功的会话尝试的日期、时间、方法、位置等，以及从上一次成功的会话建立以来的不成功的尝试次数。

5.4.4.6 不可观察性

对于由操作系统安全功能规定的受保护用户进行的操作，操作系统安全功能应确保未授权用户不能观察到。

5.4.5 客体重用

对于操作系统中的所有客体，在指定、分配或再分配给一个主体时，操作系统安全功能应确保其中没有上一次分配的剩余信息。

5.4.6 审计

5.4.6.1 内容

操作系统安全功能应能为操作系统的可审计事件生成一个审计记录，并在每一个审计记录中至少记录以下信息：

——事件发生的日期和时间；

——事件的类型；

——用户身份；

——事件的结果(成功或失败)。

操作系统安全功能应能维护操作系统的可审计事件，但其中至少包括：

——开启和关闭审计功能；

——客体创建与删除；

——使用鉴别机制；

——将客体引入用户地址空间；

——安全属性的操作等。

5.4.6.2 查阅

操作系统安全功能应为授权用户提供从审计记录中读取一定类型的审计信息的能力。

操作系统安全功能应提供对审计数据进行基于一定准则的选择查阅的能力，并能对结果进行搜索、分类或排序。

5.4.6.3 存储保护

操作系统安全功能应保护已存储的审计记录，以避免未授权的删除，并监测对审计记录的修改，当审计存储已满、失败或受到攻击时，操作系统安全功能应确保审计记录保持一定的记录数和维持的时间。

当审计记录超过预定的限制值时，操作系统安全功能应采取相应的行动，如：给授权管理员产生警告。

当审计记录已满时，操作系统安全功能应阻止除具有特殊权限的授权用户外产生的所有可审计事件，并且一旦审计存储失败就采取其他行动，如：通知授权管理员。

5.4.6.4 分析

操作系统安全功能应能用一定的规则去监控审计事件，并指出潜在的侵害。

操作系统安全功能应能维护系统的使用轮廓(一个表征用户或主体活动特征的结构,它表现了用户或主体怎样用不同的方法与操作系统安全功能交互),对于那些其行动已记录在轮廓中的用户,维护其相对应的置疑等级,当用户的置疑等级超过限制条件时,操作系统安全功能应能指出可能发生的侵害。

5.4.6.5 **自动响应**

在检测到可能的安全侵害时,操作系统安全功能应做出响应,如:

——通知授权用户;

——向授权用户提供一组遏制侵害的或采取校正的行动。

5.4.7 **数据完整性**

5.4.7.1 **数据鉴别**

操作系统安全功能能为用户数据产生真实性证据(如:校验码、单向函数、数字签名)。

操作系统安全功能能提供支持,用以验证真实性证据和产生证据的用户身份。

5.4.7.2 **回退**

在规定的客体上,操作系统安全功能应允许特定操作的回退。

操作系统安全功能能规定回退可以实施的严格条件,包括:

——回退的操作时限;

——回退的次数限制;

——实施回退的角色要求等。

5.4.7.3 **完整性监视**

对于特定的客体,操作系统安全功能能监视所存储的用户数据是否出现完整性错误,如:磁盘设备的扫描程序。

当检测到完整性错误时,操作系统安全功能应采取行动(如:提示管理员)。

5.4.8 **数据传输**

5.4.8.1 **内部传输**

在各部分(如:通过网络连接、总线连接的各部分)之间传递用户数据时,操作系统安全功能应执行特定的安全功能策略。

操作系统安全功能应监视是否有完整性错误出现。

操作系统安全功能应能支持规定对完整性错误将采取的动作。

5.4.8.2 **数据外部输出**

向操作系统安全功能控制范围之外输出用户数据时,操作系统安全功能应在访问控制机制允许的前提下,执行特定的安全功能策略,进行用户数据输出。

向操作系统安全功能控制范围之外输出与用户数据相关的安全属性时,操作系统安全功能应确保安全属性与输出的用户数据相关。

对于某些特定的安全属性,操作系统安全功能应保证无论何时都不会被输出。

5.4.8.3 **数据外部输入**

从操作系统安全功能控制范围之外输入用户数据时,操作系统安全功能应执行特定的安全功能策略。

操作系统安全功能应使用与输入的数据相关的安全属性,确保在安全属性和接受的用户数据之间提供了确切的关联。

操作系统安全功能应确保对其安全属性的解析与用户数据源的解析是一致的。

5.4.8.4 **可信路径**

操作系统安全功能应在它和用户之间提供一条可信的通信路径,此路径在逻辑上明显不同于其他路径,并能保护通信数据免遭修改和泄露。

5.4.8.5 **原发证明**

操作系统安全功能应能对发出的信息产生原发证据。

操作系统安全功能应能将信息原发者的相关属性与证据适用的信息内容相关联。

操作系统安全功能应能验证信息原发证据的真实性。

5.4.8.6 **接收证明**

操作系统安全功能应能对接收的信息产生接收证据。

操作系统安全功能应能将信息接收者的相关属性与证据适用的信息内容相关联。

操作系统安全功能应能验证信息接收证据的真实性。

5.4.9 **密码支持**

5.4.9.1 **密钥管理**

操作系统安全功能能根据符合国家规定的方法来管理密钥，包括：密钥的产生、分发、访问及销毁。

5.4.9.2 **密码运算**

操作系统安全功能能根据符合国家规定的密码算法和密钥长度来执行密码运算。

5.4.10 **资源利用**

5.4.10.1 **容错**

操作系统安全功能能检测出已规定的操作系统故障。

当相应故障发生时，操作系统安全功能应确保操作系统未受影响部分的能力均能实现。

5.4.10.2 **服务优先级**

操作系统安全功能应为其中的每个主体规定一种优先级，对于特定的资源的访问，能根据主体的优先级进行协调。

5.4.10.3 **资源分配**

操作系统安全功能能为主体规定并执行某些受控资源的最高配额和使用时间，并确保主体至少获得规定的最低配额。

5.4.10.4 **并发会话**

操作系统安全功能能限制属于同一用户的并发会话的最大数目。

5.4.11 **安全功能保护**

5.4.11.1 **自检**

操作系统安全功能应在操作系统的特定状态中，运行一套自检来演示操作系统安全功能的正确执行。这些状态应包括：

——操作系统启动时；

——授权用户要求时。

操作系统安全功能应为授权用户提供对操作系统安全功能数据完整性的验证能力。

操作系统安全功能应为授权用户提供对存储的操作系统安全功能可执行码完整性的验证能力。

5.4.11.2 **时间戳**

操作系统安全功能应为自身的应用提供可靠的时间戳。

5.4.11.3 **域分离**

操作系统安全功能同用户隔离的部分执行时，操作系统安全功能应为其维护一个独立的地址空间，防止不可信主体进行干扰和篡改。

5.4.11.4 **数据一致性**

操作系统安全功能应确保操作系统各部分间的安全功能数据的复制一致性。

当包含复制的安全功能数据的操作系统的一部分被断开，而又重新建立连接后，在处理任何依赖于操作系统安全功能数据复制一致性的安全功能请求之前，操作系统安全功能应确保该部分的操作系统安全功能数据的复制一致性。

5.4.11.5 安全功能数据传输

在各部分间传输操作系统安全功能数据时，操作系统安全功能能保护安全功能数据，防止被泄漏及修改。

操作系统安全功能应分离传送用户数据与安全功能数据。

操作系统安全功能能检测出安全功能数据的完整性错误。

操作系统安全功能应支持规定对完整性错误将采取的动作。

5.4.11.6 系统恢复

当操作系统发生失败或服务中断后，操作系统安全功能应进入维护方式，并提供将操作系统返回到一个安全状态的能力。

操作系统安全功能应具备从失败或服务中断状态中自动恢复的能力，并能在操作系统安全功能数据和用户数据无超量丢失的情况下恢复到初始安全状态。

5.4.11.7 不可旁路

在操作系统安全功能控制范围的每一项功能执行之前，操作系统安全功能应确保安全功能被成功地激活。

5.4.11.8 物理保护

操作系统安全功能应对可能危及操作系统安全功能安全的物理篡改提供明确的检测，并能判断出特定的物理篡改。

操作系统安全功能应监视需主动检测的操作系统安全功能设备及要素，当其发生物理篡改时，操作系统安全功能应采取行动，如：通知指定的管理员。

5.4.12 安全管理

5.4.12.1 功能管理

操作系统安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.4.12.2 属性管理

操作系统安全功能应执行访问控制策略，仅允许授权管理员管理安全属性。

操作系统安全功能应提供安全属性的默认值，仅允许授权管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

操作系统安全功能应确保安全属性只接受安全的值。

5.4.12.3 安全功能数据管理

操作系统安全功能应限制管理员查询、修改或删除操作系统安全功能数据的能力。仅允许授权管理员管理这些数据。

操作系统安全功能应支持规定对操作系统安全功能数据的限制以及限制值(如：用户登录数)，当操作系统安全功能数据值超出了指定的限制时，应采取特定的动作。

操作系统安全功能应确保操作系统安全功能数据只接受安全的值。

5.4.12.4 时限授权

对于支持有效期的各种安全属性，操作系统安全功能应限制授权管理员规定其有效期的能力。

5.4.12.5 角色管理

操作系统安全功能应支持维护授权角色。

操作系统安全功能应将角色与用户关联起来，并确保用户的不同角色应满足的条件，如：一个账号不能同时具有审计员和管理员角色。

5.4.13 生存周期支持

5.4.13.1 开发安全

开发者提供的开发安全文件应描述在操作系统开发环境中在物理上、程序上、人员上以及其他方面的安全措施。

5.4.13.2 缺陷纠正

开发者提供的缺陷纠正程序文档，应描述用以接受用户对于安全缺陷报告的程序，以及更正这些缺陷的程序，并说明已采取的纠正措施。

开发者提供的缺陷纠正程序文档，应描述用以跟踪所有操作系统版本里安全缺陷的程序，标识对安全缺陷所采取的纠正措施。

5.4.13.3 生存周期模型

开发者提供的生存周期定义文档应描述所建立的用于开发和维护操作系统的生存周期模型。

5.4.13.4 工具和技术

开发者提供的开发工具文档应标识在开发操作系统中使用的工具和参照的标准，并描述有关实现的开发工具的选项。

开发者提供的开发工具文档应明确定义所有基于实现的选项的含义。

5.4.14 配置管理

5.4.14.1 自动化

开发者提供的配置管理文档应描述在配置管理系统中使用的自动生成工具。

5.4.14.2 能力

开发者提供的配置管理文档应以版本号做标签，为操作系统提供引用，使一个版本号对应操作系统的唯一版本。

开发者提供的配置管理文档应包括配置清单、配置管理计划和接受计划，其中配置清单应描述对配置项进行唯一标识的方法，并清楚地标识出组成安全功能的配置项，并提供保证对配置项只进行授权修改的方法。

应在配置管理计划中描述配置管理系统是如何使用的，并阐明实施中的配置管理与配置管理计划的一致性。

5.4.14.3 范围

开发者提供的配置管理文档应描述配置管理系统是如何跟踪配置项的，并说明至少能跟踪：操作系统实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档。

开发者提供的配置管理文档应说明配置管理系统能跟踪安全缺陷。

5.4.15 安全功能开发过程

5.4.15.1 安全策略模型

开发者提供的安全策略模型应描述所有可以模型化的安全策略的规则和特性。

开发者提供形式化的安全策略模型，并阐明或适当时严格证明功能规约和安全策略模型之间的对应性，并说明功能规约中的安全功能对于安全策略模型来说，是一致的而且是完备的。

5.4.15.2 功能规约

开发者提供的操作系统安全功能的功能规约应描述安全功能及其与外部的接口。

开发者提供的操作系统安全功能的功能规约应完备地表示安全功能。

开发者应提供半形式化的操作系统安全功能的功能规约。使用半形式化风格来描述安全功能与其外部接口，可以由非形式化的、解释性的文字来支持。

5.4.15.3 高层设计

开发者提供的操作系统安全功能的高层设计，应按子系统方式描述安全功能及其结构，并标识安全功能子系统的所有接口。

开发者提供的操作系统安全功能的高层设计，应将有关安全功能策略实施的子系统与其他子系统分离。

开发者提供的操作系统安全功能的高层设计应是半形式化的。

5.4.15.4 低层设计

开发者提供的操作系统安全功能的低层设计应以模块术语描述安全功能，并描述每一个模块的目

的、接口。

开发者提供的操作系统安全功能的低层设计应是半形式化的，并详细描述操作系统安全功能模块所有接口的目的与方法。

5.4.15.5 实现

开发者提供的操作系统安全功能的实现表示（如：源代码、硬件图）文档应是内在一致的，并且无歧义地定义了详细的操作系统安全功能。

开发者提供的操作系统安全功能的实现表示文档应描述实现的各部分之间的关系。

5.4.15.6 表示对应性

对于所提供的安全策略表示的每个相邻对，开发者应提供相邻两阶段开发文档之间的对应性分析，并阐明上一阶段的安全策略表示在下一阶段文档中得到正确而完备地细化。

当安全策略表示的相邻对是半形式化或形式化的时候，对应性阐明也应是半形式化或形式化的。

5.4.16 测试

5.4.16.1 功能测试

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能、描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

开发者提供的测试文档应包含对顺序依赖性的分析。

5.4.16.2 覆盖分析

开发者提供的测试覆盖的证据，应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者提供的测试覆盖的证据，应阐明测试文档所标识的测试和功能规约中所描述的安全功能之间的对应性是完备的。

5.4.16.3 深度

开发者提供的测试深度分析文档应说明测试文档中所标识的测试足以说明该安全功能动作和高层设计是一致的。

5.4.17 指导性文档

5.4.17.1 管理员指南

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理操作系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.4.17.2 用户指南

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责，包括用户行为假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.4.18 脆弱性

5.4.18.1 隐蔽信道分析

开发者提供的隐蔽信道分析的文档应标识出隐蔽信道并且估计它们的容量。

5.4.18.2 安全功能强度

开发者提供的安全功能强度的分析文档应对每个具有安全功能强度声明的安全机制进行安全功能强度的分析。

5.4.18.3 脆弱性分析

开发者提供的脆弱性分析文档应标识脆弱性的分布，并说明在所期望的环境中这些脆弱性不会被利用。

开发者提供的脆弱性分析文档应能说明对脆弱性的搜索是系统化的。

5.4.19 交付和运行

5.4.19.1 交付

开发者提供的交付文档应向用户说明维护安全所应具有的交付程序。

开发者提供的交付文档应描述如何用各种方法和技术措施来检测修改，或检测描述开发者的主拷贝和用户方收到的版本之间的差异。

5.4.19.2 安装生成

开发者提供的安全安装过程的文档应说明用于操作系统的安全安装、生成和启动的过程所必需的步骤，并应描述一个启动程序，它包含了用以生成操作系统的选项，从而能决定操作系统是如何以及何时产生的。

5.5 访问验证保护级

5.5.1 自主访问控制

操作系统安全功能应实施安全机制，控制用户对客体的访问，其方法可以是：

——基于用户的权能表，为用户规定是否可以对客体进行访问；

——基于客体的访问控制表。

操作系统安全功能的访问控制粒度应是单个用户。

操作系统安全功能能规定用户对客体的访问模式。

5.5.2 强制访问控制

操作系统安全功能应通过主客体的敏感标记，控制用户对相关客体的直接访问。

操作系统安全功能应实施安全机制，控制所有主客体之间的访问。

5.5.3 标记

5.5.3.1 标记定义

操作系统安全功能应给出其控制范围内所有主体和客体的敏感标记。

5.5.3.2 标记管理

操作系统安全功能应执行访问控制策略，仅允许授权管理员管理敏感标记。

5.5.3.3 带标记数据输入

从操作系统安全功能控制范围之外输入带标记的数据时，操作系统安全功能应确保标记和接受的用户数据相关。

5.5.4 身份鉴别

5.5.4.1 用户属性定义

操作系统安全功能应给出每一个用户与标识相关的安全属性(如：组、标识符等)。

5.5.4.2 用户标识

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作，在用户被标识之前，允许操作系统执行这些预设动作。在操作系统安全功能的其他动作之前，应成功地标识每个用户。

5.5.4.3 用户鉴别

操作系统安全功能应预先设定操作系统代表用户执行的、与操作系统安全功能相关的动作，在用户被鉴别之前，允许操作系统执行这些预设动作，在操作系统安全功能的其他动作之前，应成功地鉴别每个用户。

当进行鉴别时，操作系统安全功能应仅将最少的反馈(如：打入的字符数，鉴别的成功或失败)提供给用户。

操作系统安全功能应提供多鉴别机制以支持用户多鉴别。

操作系统安全功能应规定重鉴别条件，在对应的条件下，对用户进行重鉴别。

5.5.4.4 鉴别失败处理

操作系统安全功能应检测出不成功的鉴别尝试，当尝试的次数达到或超过了定义的界限时，应能终止会话建立的进程。

在会话建立的进程终止后，操作系统安全功能应能使得该用户账户无效，或是进行鉴别尝试的登录站点无效。

5.5.4.5 访问历史

操作系统安全功能在会话成功建立的基础上，应显示用户上一次成功会话建立的日期、时间、方法、位置等。

操作系统安全功能应显示用户上一次不成功的会话尝试的日期、时间、方法、位置等，以及从上一次成功的会话建立以来的不成功的尝试次数。

5.5.4.6 不可观察性

对于由操作系统安全功能规定的受保护用户进行的操作，操作系统安全功能应确保未授权用户不能观察到。

5.5.5 客体重用

对于操作系统中的所有客体，在指定、分配或再分配给一个主体时，操作系统安全功能应确保其中没有上一次分配的剩余信息。

5.5.6 审计

5.5.6.1 内容

操作系统安全功能应能为操作系统的可审计事件生成一个审计记录，并在每一个审计记录中至少记录以下信息：

——事件发生的日期和时间；

——事件的类型；

——用户身份；

——事件的结果(成功或失败)。

操作系统安全功能应能维护操作系统的可审计事件，但其中至少包括：

——开启和关闭审计功能；

——客体创建与删除；

——使用鉴别机制；

——将客体引入用户地址空间；

——安全属性的操作等。

5.5.6.2 查阅

操作系统安全功能应为授权用户提供从审计记录中读取一定类型的审计信息的能力。

操作系统安全功能应提供对审计数据进行基于一定准则的选择查阅的能力，并能对结果进行搜索、分类或排序。

5.5.6.3 存储保护

操作系统安全功能应保护已存储的审计记录，以避免未授权的删除，并监测对审计记录的修改，当审计存储已满、失败或受到攻击时，操作系统安全功能应确保审计记录保持一定的记录数和维持的时间。

当审计记录超过预定的限制值时，操作系统安全功能应采取相应的行动，如：给授权管理员产生警告。

当审计记录已满时，操作系统安全功能应阻止除具有特殊权限的授权用户外产生的所有可审计事件，并且一旦审计存储失败就采取其他行动，如：通知授权管理员。

5.5.6.4 分析

操作系统安全功能应能用一定的规则去监控审计事件，并指出潜在的侵害。

操作系统安全功能应能维护系统的使用轮廓(一个表征用户或主体活动特征的结构,它表现了用户或主体怎样用不同的方法与操作系统安全功能交互),对于那些其行动已记录在轮廓中的用户,维护其相对应的置疑等级,当用户的置疑等级超过限制条件时,操作系统安全功能应能指出可能发生的侵害。

操作系统安全功能应能维护有侵害性的系统事件序列的内部表示,当一个系统事件或事件序列被发现并与内部表示匹配时,应指出即将到来的攻击。

5.5.6.5 自动响应

在检测到可能的安全侵害时,操作系统安全功能应做出响应,如:

——通知授权用户;

——向授权用户提供一组遏制侵害的或采取校正的行动。

5.5.7 数据完整性

5.5.7.1 数据鉴别

操作系统安全功能能为用户数据产生真实性证据(如:校验码、单向函数、数字签名)。

操作系统安全功能能提供支持,用以验证真实性证据和产生证据的用户身份。

5.5.7.2 回退

在规定的客体上,操作系统安全功能应允许特定操作的回退。

操作系统安全功能能规定回退可以实施的严格条件,包括:

——回退的操作时限;

——回退的次数限制;

——实施回退的角色要求等。

5.5.7.3 完整性监视

对于特定的客体,操作系统安全功能能监视所存储的用户数据是否出现完整性错误,如:磁盘设备的扫描程序。

当检测到完整性错误时,操作系统安全功能应采取行动(如:提示管理员)。

5.5.8 数据传输

5.5.8.1 内部传输

在各部分(如:通过网络连接、总线连接的各部分)之间传递用户数据时,操作系统安全功能应执行特定的安全功能策略。

操作系统安全功能应监视是否有完整性错误出现。

操作系统安全功能应能支持规定对完整性错误将采取的动作。

5.5.8.2 数据外部输出

向操作系统安全功能控制范围之外输出用户数据时,操作系统安全功能应在访问控制机制允许的前提下,执行特定的安全功能策略,进行用户数据输出。

向操作系统安全功能控制范围之外输出与用户数据相关的安全属性时,操作系统安全功能应确保安全属性与输出的用户数据相关。

对于某些特定的安全属性,操作系统安全功能应保证无论何时都不会被输出。

5.5.8.3 数据外部输入

从操作系统安全功能控制范围之外输入用户数据时,操作系统安全功能应执行特定的安全功能策略。

操作系统安全功能应使用与输入的数据相关的安全属性,确保在安全属性和接受的用户数据之间提供了确切的关联。

操作系统安全功能应确保对其安全属性的解析与用户数据源的解析是一致的。

5.5.8.4 可信路径

操作系统安全功能应在它和用户之间提供一条可信的通信路径,此路径在逻辑上明显不同于其他

路径，并能保护通信数据免遭修改和泄露。

5.5.8.5 **原发证明**

操作系统安全功能应能对发出的信息产生原发证据。

操作系统安全功能应能将信息原发者的相关属性与证据适用的信息内容相关联。

操作系统安全功能应能验证信息原发证据的真实性。

5.5.8.6 **接收证明**

操作系统安全功能应能对接收的信息产生接收证据。

操作系统安全功能应能将信息接收者的相关属性与证据适用的信息内容相关联。

操作系统安全功能应能验证信息接收证据的真实性。

5.5.9 **密码支持**

5.5.9.1 **密钥管理**

操作系统安全功能能根据符合国家规定的方法来管理密钥，包括：密钥的产生、分发、访问及销毁。

5.5.9.2 **密码运算**

操作系统安全功能能根据符合国家规定的密码算法和密钥长度来执行密码运算。

5.5.10 **资源利用**

5.5.10.1 **容错**

操作系统安全功能能检测出已规定的操作系统故障。

当相应故障发生时，操作系统安全功能应确保操作系统未受影响部分的能力均能实现。

5.5.10.2 **服务优先级**

操作系统安全功能应为其中的每个主体规定一种优先级，对于特定的资源的访问，能根据主体的优先级进行协调。

对于所有共享资源的每次访问，操作系统安全功能应能根据主体的优先级进行协调。

5.5.10.3 **资源分配**

操作系统安全功能能为主体规定并执行某些受控资源的最高配额和使用时间，并确保主体至少获得规定的最低配额。

5.5.10.4 **并发会话**

操作系统安全功能能限制属于同一用户的并发会话的最大数目。

5.5.11 **安全功能保护**

5.5.11.1 **自检**

操作系统安全功能应在操作系统的特定状态中，运行一套自检来演示操作系统安全功能的正确执行。这些状态应包括：

——操作系统启动时；

——授权用户要求时。

操作系统安全功能应为授权用户提供对操作系统安全功能数据完整性的验证能力。

操作系统安全功能应为授权用户提供对存储的操作系统安全功能可执行码完整性的验证能力。

5.5.11.2 **时间戳**

操作系统安全功能应为自身的应用提供可靠的时间戳。

5.5.11.3 **域分离**

操作系统安全功能应分离在操作系统安全功能控制范围内各主体安全域，用户进程之间是彼此隔离的。

操作系统安全功能同用户隔离的部分执行时，操作系统安全功能应为其维护一个独立的地址空间，防止不可信主体进行干扰和篡改。

操作系统安全功能应对操作系统安全功能中与访问控制有关的部分，维护一个自身执行时的安全

域，防止被操作系统安全功能的其余部分和不可信主体的干扰和篡改。

5.5.11.4 **数据一致性**

操作系统安全功能应确保操作系统各部分间的安全功能数据的复制一致性。

当包含复制的安全功能数据的操作系统的一部分被断开，而又重新建立连接后，在处理任何依赖于操作系统安全功能数据复制一致性的安全功能请求之前，操作系统安全功能应确保该部分的操作系统安全功能数据的复制一致性。

当与其他可信 IT 产品共享操作系统安全功能数据时，操作系统安全功能应具备对数据的一致性解析能力。

5.5.11.5 **安全功能数据传输**

在各部分间传输操作系统安全功能数据时，操作系统安全功能能保护安全功能数据，防止被泄漏及修改。

操作系统安全功能应分离传送用户数据与安全功能数据。

操作系统安全功能能检测出安全功能数据的完整性错误。

操作系统安全功能应支持规定对完整性错误将采取的动作。

5.5.11.6 **系统恢复**

当操作系统发生失败或服务中断后，操作系统安全功能应进入维护方式，并提供将操作系统返回到一个安全状态的能力。

操作系统安全功能应具备从失败或服务中断状态中自动恢复的能力，并能在操作系统安全功能数据和用户数据无超量丢失的情况下恢复到初始安全状态。

5.5.11.7 **可信恢复**

操作系统安全功能应确保安全功能或者被成功完成，或者在失败时恢复到前后一致的状态。

5.5.11.8 **不可旁路**

在操作系统安全功能控制范围的每一项功能执行之前，操作系统安全功能应确保安全功能被成功地激活。

5.5.11.9 **物理保护**

操作系统安全功能应对可能危及操作系统安全功能安全的物理篡改提供明确的检测，并能判断出特定的物理篡改。

操作系统安全功能应监视需主动检测的操作系统安全功能设备及要素，当其发生物理篡改时，操作系统安全功能应采取行动，如：通知指定的管理员。

5.5.12 **安全管理**

5.5.12.1 **功能管理**

操作系统安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.5.12.2 **属性管理**

操作系统安全功能应执行访问控制策略，仅允许授权管理员管理安全属性。

操作系统安全功能应提供安全属性的默认值，仅允许授权管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

操作系统安全功能应确保安全属性只接受安全的值。

5.5.12.3 **安全功能数据管理**

操作系统安全功能应限制管理员查询、修改或删除操作系统安全功能数据的能力。仅允许授权管理员管理这些数据。

操作系统安全功能应支持规定对操作系统安全功能数据的限制以及限制值（如：用户登录数），当操作系统安全功能数据值超出了指定的限制时，应采取特定的动作。

操作系统安全功能应确保操作系统安全功能数据只接受安全的值。

5.5.12.4 **时限授权**

对于支持有效期的各种安全属性，操作系统安全功能应限制授权管理员规定其有效期的能力。

操作系统安全功能应支持授权管理员规定在有效期后将要采取的一系列活动。

5.5.12.5 **角色管理**

操作系统安全功能应支持维护授权角色。

操作系统安全功能应将角色与用户关联起来，并确保用户的不同角色应满足的条件，如：一个账号不能同时具有审计员和管理员角色。

5.5.13 **生存周期支持**

5.5.13.1 **开发安全**

开发者提供的开发安全文件应描述在操作系统开发环境中在物理上、程序上、人员上以及其他方面的安全措施。

开发者提供的开发安全文件应提供证据，证明安全措施对维护操作系统的机密性和完整性提供了必要的保护级别。

5.5.13.2 **缺陷纠正**

开发者提供的缺陷纠正程序文档，应描述用以接受用户对于安全缺陷报告的程序，以及更正这些缺陷的程序，并说明已采取的纠正措施。

开发者提供的缺陷纠正程序文档，应描述用以跟踪所有操作系统版本里安全缺陷的程序，标识对安全缺陷所采取的纠正措施。

5.5.13.3 **生存周期模型**

开发者提供的生存周期定义文档应描述所建立的用于开发和维护操作系统的生存周期模型。

开发者提供的生存周期定义文档应说明选择该模型的原因。

5.5.13.4 **工具和技术**

开发者提供的开发工具文档应标识在开发操作系统中使用的工具和参照的标准，并描述有关实现的开发工具的选项。

开发者提供的开发工具文档应明确定义所有基于实现的选项的含义。

5.5.14 **配置管理**

5.5.14.1 **自动化**

开发者提供的配置管理文档应描述在配置管理系统中使用的自动生成工具。

开发者提供的配置管理文档，应说明该生成工具能自动地确定操作系统与以前版本之间的变化，以及因给定的配置项的修改而受到影响的其他所有配置项。

5.5.14.2 **能力**

开发者提供的配置管理文档应以版本号做标签，为操作系统提供引用，使一个版本号对应操作系统的唯一版本。

开发者提供的配置管理文档应包括配置清单、配置管理计划和接受计划，其中配置清单应描述对配置项进行唯一标识的方法，并清楚地标识出组成安全功能的配置项，并提供保证对配置项只进行授权修改的方法。

应在配置管理计划中描述配置管理系统是如何使用的，并阐明实施中的配置管理与配置管理计划的一致性。

开发者提供的配置管理文档应描述对修改过的或新建的配置项进行的接受程序。

5.5.14.3 **范围**

开发者提供的配置管理文档应描述配置管理系统是如何跟踪配置项的，并说明至少能跟踪：操作系统实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档。

开发者提供的配置管理文档应说明配置管理系统能跟踪安全缺陷。

5.5.15 安全功能开发过程

5.5.15.1 安全策略模型

开发者提供的安全策略模型应描述所有可以模型化的安全策略的规则和特性。

开发者提供形式化的安全策略模型，并阐明或适当时严格证明功能规约和安全策略模型之间的对应性，并说明功能规约中的安全功能对于安全策略模型来说，是一致的而且是完备的。

当功能规约是半形式化或形式化时，与功能规约之间的对应性的阐明也应是半形式化或形式化的。

5.5.15.2 功能规约

开发者提供的操作系统安全功能的功能规约应描述安全功能及其与外部的接口。

开发者提供的操作系统安全功能的功能规约应完备地表示安全功能。

开发者应提供**形式化的**操作系统安全功能的功能规约。使用半形式化风格来描述安全功能与其外部接口，可以由非形式化的、解释性的文字来支持。

5.5.15.3 高层设计

开发者提供的操作系统安全功能的高层设计，应按子系统方式描述安全功能及其结构，并标识安全功能子系统的所有接口。

开发者提供的操作系统安全功能的高层设计，应将有关安全功能策略实施的子系统与其他子系统分离。

开发者提供的操作系统安全功能的高层设计应是**形式化**的。

5.5.15.4 低层设计

开发者提供的操作系统安全功能的低层设计应以模块术语描述安全功能，并描述每一个模块的目的、接口。

开发者提供的操作系统安全功能的低层设计应是半形式化的，并详细描述操作系统安全功能模块所有接口的目的与方法。

5.5.15.5 实现

开发者提供的操作系统安全功能的实现表示（如：源代码、硬件图）文档应是内在一致的，并且无歧义地定义了详细的操作系统安全功能。

开发者提供的操作系统安全功能的实现表示文档应描述实现的各部分之间的关系。

开发者提供的操作系统安全功能的实现表示文档应是构造较小的且易于理解的。

5.5.15.6 表示对应性

对于所提供的安全策略表示的每个相邻对，开发者应提供相邻两阶段开发文档之间的对应性分析，并阐明上一阶段的安全策略表示在下一阶段文档中得到正确而完备地细化。

当安全策略表示的相邻对是半形式化或形式化的时候，对应性阐明也应是半形式化或形式化的。

5.5.16 测试

5.5.16.1 功能测试

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能，描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

开发者提供的测试文档应包含对顺序依赖性的分析。

5.5.16.2 覆盖分析

开发者提供的测试覆盖的证据，应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者提供的测试覆盖的证据，应阐明测试文档所标识的测试和功能规约中所描述的安全功能之间的对应性是完备的。

开发者提供的测试覆盖的证据，应严格地阐明功能规约所标识的安全功能的所有外部接口均已经

被完全测试。

5.5.16.3 **深度**

开发者提供的测试深度分析文档，应说明测试文档中所标识的测试足以说明该安全功能动作和高层设计是一致的。

开发者提供的测试深度分析文档，应说明测试文档中所标识的测试足以阐明该安全功能动作与高层设计和低层设计一致的。

5.5.17 **指导性文档**

5.5.17.1 **管理员指南**

开发者提供的管理员指南，应描述对于授权安全管理角色可使用的管理功能和接口、安全管理操作系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.5.17.2 **用户指南**

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责，包括用户行为假设。同时，应描述与为评估而提供的其他所有文件的一致性。

5.5.18 **脆弱性**

5.5.18.1 **隐蔽信道分析**

开发者提供的隐蔽信道分析的文档应标识出隐蔽信道并且估计它们的容量。

开发者提供的隐蔽信道分析的文档应阐明对于隐蔽信道的分析是系统化的、彻底的。

5.5.18.2 **安全功能强度**

开发者提供的安全功能强度的分析文档应对每个具有安全功能强度声明的安全机制进行安全功能强度的分析。

5.5.18.3 **脆弱性分析**

开发者提供的脆弱性分析文档应标识脆弱性的分布，并说明在所期望的环境中这些脆弱性不会被利用。

开发者提供的脆弱性分析文档应能说明对脆弱性的搜索是系统化的。

5.5.19 **交付和运行**

5.5.19.1 **交付**

开发者提供的交付文档应向用户说明维护安全所应具有的交付程序。

开发者提供的交付文档应描述如何用各种方法和技术措施来检测修改，或检测描述开发者的主拷贝和用户方收到的版本之间的差异。

5.5.19.2 **安装生成**

开发者提供的安全安装过程的文档应说明用于操作系统的安全安装、生成和启动的过程所必需的步骤，并应描述一个启动程序，它包含了用以生成操作系统的选项，从而能决定操作系统是如何以及何时产生的。

GB/T 20008—2005

附 录 A
（资料性附录）
操作系统面临的威胁和对策

A.1 操作系统可能面对的主要威胁

对操作系统可能构成威胁的用户分为两类：操作系统的未授权用户和授权用户。即使在非敌对环境中工作的有着良好管理秩序的团体中，操作系统的授权用户也可能由于疏忽或其他一些偶然因素对系统的安全构成威胁，所以操作系统应防止这类威胁。操作系统可能会遇到的威胁有：

——授权用户在没有取得信息所有者同意的情况下，察看了本不应知道的信息，即使这个用户可能有足够的权限看到这个受保护信息；

——授权用户没有经过信息所有者的直接或者间接授权，对该信息进行了修改或破坏；

——用户未经授权，便使用需要拥有管理员权限的工具，通过工具取得对信息的未授权访问；

——工作站间数据传输过程中的数据泄漏、被未授权用户篡改或被其他直接或间接地处理（如工作站身份欺骗）；

——未授权用户可能通过模拟授权用户获得对操作系统的访问，或者对一个授权用户已经登录而又暂时无人照看的系统进行访问，从而获得了对信息的未授权访问；

——为保护其资源，操作系统应保持一个安全状态，但这种状态可能由于系统的故障而被破坏，如：造成数据不一致；

——在一系列的攻击下，操作系统资源的不可用。

A.2 操作系统可采用的降低威胁的方法

为应对以上威胁，操作系统可以采用以下方法抵御威胁：

——特定客体的访问权限由客体安全属性、用户身份和环境条件所决定，这些条件在对应的策略中规定；

——使用监督和事后评判等机制，使用户的有关安全的行为得到控制；

——在物理上分离的部件之间的信息流应遵从已建立的信息流控制策略；

——除了公共资源外，系统受保护资源仅限于需要了解该资源的授权用户进行访问；

——给操作系统中的主体、客体或客体信息的敏感标记，如：安全等级、数字签名等，从而决定主客体之间的访问得到控制。

GB/T 20008-2005

*
书号：155066・1-27492