ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20272—2019
代替 GB/T 20272—2006

信息安全技术　操作系统安全技术要求

**Information security technology—
Security technical requirements for operating system**

2019-08-30 发布　　2020-03-01 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。

本标准代替 GB/T 20272—2006《信息安全技术　操作系统安全技术要求》，与 GB/T 20272—2006 相比，除编辑性修改外主要技术变化如下：

——删除了“操作系统安全技术”“SSOOS 安全策略”“安全功能策略”“安全要素”“SSOOS 安全功能”“SSF 控制范围”的术语和定义（见 2006 年版的 3.1.2、3.1.4、3.1.5、3.1.6、3.1.7、3.1.8）；

——删除了“SFP 安全功能策略”“SSC SSF 控制范围”“SSP SSOOS 安全策略”的缩略语（见 2006 年版的 3.2）；

——增加了“UID 用户标识符”的缩略语（见第 4 章）；

——增加了“网络安全保护”安全功能要求（见 6.1.1.4、6.2.1.6、6.3.1.7、6.4.1.9、6.5.1.9）；

——增加了“数据加密”安全功能要求（见 6.2.1.5.1、6.3.1.6.2、6.4.1.6.2、6.5.1.6.2）；

——增加了“可信信道”安全功能要求（见 6.4.1.8、6.5.1.8）；

——在“安全功能”中，将“标记”“强制访问控制”合并为“标记和强制访问控制”（见 6.3.1.3、6.4.1.3、6.5.1.3）；

——删除了“数据流控制”安全功能要求（见 2006 年版的 4.3.1.5、4.4.1.5、4.5.1.5）；

——增加了 “可信度量”自身安全要求（见 6.2.2.4、6.3.2.4、6.4.2.4、6.5.2.4）；

——增加了 “可信恢复”自身安全要求（见 6.4.2.5、6.5.2.5）；

——增加了“安全策略配置”自身安全要求（见 6.1.2.4、6.2.2.5、6.3.2.5、6.4.2.6、6.5.2.6）；

——删除了 “SSF 物理安全保护”（见 2006 年版的 4.1.2.1、4.2.2.1、4.3.2.1、4.4.2.1、4.5.2.1）；

——将“SSOOS 访问控制”修改为“用户登录访问控制”（见 6.1.2.3、6.2.2.3、6.3.2.3、6.4.2.3、6.5.2.3）；

——将“SSF 数据安全保护”中的相关内容，整合到“数据完整性”“数据保密性”“可信路径”等安全功能中（见 6.1.1.3、6.2.1.4、6.2.1.5、6.3.1.5、6.3.1.6、6.4.1.5、6.4.1.6、6.4.1.7、6.5.1.5、6.5.1.6、6.5.1.7）；

——将“SSOOS 设计和实现”修改为“安全保障要求”，并根据 GB/T 18336.3—2015 的要求，进行了相应的修改（见 6.1.3、6.2.3、6.3.3、6.4.3、6.5.3，2006 年版的 4.1.3、4.2.3、4.3.3、4.4.3、4.5.3）；

——删除了“SSOOS 安全管理”要求（见 2006 年版的 4.1.4、4.2.4、4.3.4、4.4.4、4.5.4）。

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：公安部第三研究所、北京江南天安科技有限公司、中科方德软件有限公司、中标软件有限公司、天津麒麟信息技术有限公司、普华基础软件股份有限公司、北京凝思软件股份有限公司。

本标准主要起草人：邱梓华、宋好好、陈妍、胡亚兰、顾健、陈冠直、徐宁、魏立峰、吴永成、朱健伟、王戍靖、吉增瑞、丁丽萍、董军平、龚文、郎金刚、谭一鸣、胡丹妮、杨诏钧、戴华东、王玉成、孟健、宫敏、彭志航。

本标准所代替标准的历次版本发布情况为：

——GB/T 20272—2006。

信息安全技术　操作系统安全技术要求

1　范围

本标准规定了五个安全等级操作系统的安全技术要求。

本标准适用于操作系统安全性的研发、测试、维护和评价。

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 17859—1999　计算机信息系统　安全保护等级划分准则

GB/T 18336.3—2015　信息技术　安全技术 信息技术安全评估准则　第3部分：安全保障组件

GB/T 20271—2006　信息安全技术　信息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

3　术语和定义

GB 17859—1999、GB/T 18336.3—2015、GB/T 20271—2006 和 GB/T 29240—2012 界定的以及下列术语和定义适用于本文件。

3.1

操作系统安全　security of operating system

操作系统自身以及其所存储、传输和处理的信息的保密性、完整性和可用性。

3.2

操作系统安全子系统　security subsystem of operating system

操作系统中安全保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。

4　缩略语

下列缩略语适用于本文件。

SSF：SSOOS 安全功能(SSOOS Security Function)

SSOOS：操作系统安全子系统(Security Subsystem of Operating System)

UID：用户标识符(User Identifier)

5　产品描述

资源管理(包括设备硬件资源和数据资源)是操作系统最为基本的功能，操作系统中对资源的安全保护由 SSOOS 来实现。

SSOOS 是操作系统中所有安全保护装置的组合体。SSOOS 一般包含多个 SSF，每个安全功能模块是一个或多个安全功能策略的具体实现。SSOOS 中的所有安全功能策略构成了一个安全域，以保护

整个操作系统的安全。

为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，每一级的新增部分用“**黑体**”表示。附录 A 中的操作系统安全技术要求分级表，以表格形式列举了操作系统五个安全等级的安全功能要求、自身安全要求和安全保障要求。

6 安全技术要求

6.1 第一级：用户自主保护级

6.1.1 安全功能要求

6.1.1.1 身份鉴别

SSOOS 的身份鉴别功能如下：

a) 用户标识功能：
   1) 用户进入操作系统前，应先进行标识；
   2) 操作系统用户标识宜使用用户名和 UID。
b) 用户鉴别功能：
   1) 采用口令进行鉴别，并在每次用户登录系统时和系统重新连接时进行鉴别；
   2) 口令应是不可见的，在存储和传输时进行安全保护，确保其不被非授权的访问、修改和删除；
   3) 通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时采取的措施来实现鉴别失败的处理。
c) 对注册到操作系统的用户，应将用户进程与其所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户。

6.1.1.2 自主访问控制

SSOOS 的自主访问控制功能如下：

a) 客体的拥有者对其拥有的全部客体应有权修改其访问权限；
b) 客体的拥有者应能对其拥有的客体设置其他用户的访问控制属性，访问控制属性至少包括：读、写、执行等；
c) 主体对客体的访问应遵循该客体的自主访问控制权限属性；
d) 将访问控制客体的颗粒度控制在文件和目录。

6.1.1.3 数据完整性

对操作系统内部传输的用户数据（如进程间的通信），应具备保证用户数据完整性的功能。

6.1.1.4 网络安全保护

支持基于 IP 地址、端口、物理接口的双向网络访问控制，将不符合预先设定策略的数据包丢弃。

6.1.2 自身安全要求

6.1.2.1 运行安全保护

SSF 运行安全保护功能如下：

a) 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护

之前，应对用户和管理员的安全策略属性进行定义。

b) 应区分普通操作模式和系统维护模式。

c) 在 SSOOS 出现故障或中断后，应使其以最小的损害得到恢复，并按 GB/T 20271—2006 中 5.1.2.2失败保护所描述的内容，处理 SSF 故障。

d) 操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时运用补丁对操作系统的漏洞进行修补。

6.1.2.2 资源利用

6.1.2.2.1 容错

应通过一定措施确保当系统出现某些确定的故障情况时，SSF 也能维持正常运行。

6.1.2.2.2 服务优先级

应采取服务优先级策略，设置主体使用 SSF 控制范围内某个资源子集的优先级，进行操作系统资源的管理和分配。

6.1.2.2.3 资源分配

应按 GB/T 20271—2006 中 5.1.4.2 a)最大限额资源分配的要求，进行操作系统资源的管理和分配。配额机制确保用户和主体将不会独占某种受控的资源。

6.1.2.3 用户登录访问控制

SSOOS 的用户登录访问控制功能如下：

a) 应按 GB/T 20271—2006 中 5.1.5 a)会话建立机制的要求，根据访问地址或端口，允许或拒绝用户的登录；

b) 应按 GB/T 20271—2006 中 5.1.5 c)多重并发会话限定的要求，限制系统并发会话的最大数量，并利用默认值作为会话次数的限定数。

6.1.2.4 安全策略配置

应对身份鉴别、网络安全保护、资源利用、用户登录访问控制提供安全策略配置功能。

6.1.3 安全保障要求

6.1.3.1 开发

6.1.3.1.1 安全架构

开发者应提供 SSOOS 的安全架构描述文档，安全架构描述文档应符合以下要求：

a) 与 SSOOS 设计文档中对安全功能要求和自身安全保护要求的描述一致；

b) 描述 SSOOS 的安全域；

c) 描述 SSOOS 初始化过程为何是安全的；

d) 证实 SSOOS 能够防止被破坏；

e) 证实 SSOOS 能够防止被旁路。

6.1.3.1.2 功能规范说明

开发者应提供功能规范说明，功能规范说明应符合以下要求：

a) 完全描述 SSF 和自身安全保护；
b) 描述所有 SSOOS 接口的目的与使用方法；
c) 标识和描述每个 SSOOS 接口相关的全部参数；
d) 描述实施过程中，与 SSOOS 接口相关的行为；
e) 证实安全功能要求和自身安全保护要求到 SSOOS 接口的追溯。

6.1.3.1.3 SSOOS 设计

开发者应提供 SSOOS 设计文档，SSOOS 设计文档应符合以下要求：
a) 描述 SSOOS 的结构；
b) 描述所有安全功能和自身安全保护模块，包括其目的及与其他模块间的相互作用；
c) 提供每一个安全功能和自身安全保护的描述；
d) 描述安全功能和自身安全保护间的相互作用；
e) 根据模块描述安全功能和自身安全保护。

6.1.3.2 指导性文档

6.1.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应符合以下要求：
a) 描述在安全处理环境中用户可访问的功能和特权，并包含可能造成危害的警示信息；
b) 描述如何以安全的方式使用 SSOOS 提供的安全功能和自身安全保护；
c) 描述安全功能和自身安全保护及接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明安全功能和自身安全保护有关的每一种安全相关事件，包括改变 SSOOS 所控制实体的安全特性；
e) 标识 SSOOS 运行的所有可能状态(包括操作导致的失败或者操作性错误)，以及它们与维持安全运行之间的因果关系和联系；
f) 描述为确保 SSOOS 安全运行应执行的安全策略。

6.1.3.2.2 准备程序

开发者应提供操作系统及其准备程序，准备程序描述应符合以下要求：
a) 描述与开发者交付程序相一致的安全接收操作系统必需的所有步骤；
b) 描述安全安装操作系统及其运行环境必需的所有步骤。

6.1.3.3 生存周期支持

6.1.3.3.1 配置管理能力

开发者的配置管理能力应符合以下要求：
a) 为操作系统的不同版本提供唯一的标识；
b) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
c) 配置管理系统唯一标识所有配置项。

6.1.3.3.2 配置管理范围

开发者应提供 SSOOS 配置项列表，并简要说明配置项的开发者。配置项列表应包含以下内容：

a) SSOOS、安全保障要求的评估证据和SSOOS的组成部分；
b) 唯一标识配置项；
c) 对于每一个安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

6.1.3.3.3 交付程序

开发者应使用一定的交付程序交付操作系统，并将交付过程文档化。在给用户方交付指定版本操作系统时，交付文档应描述为维护安全所必需的所有程序。

6.1.3.4 测试

6.1.3.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖的证据应表明测试文档中的测试与功能规范说明中SSOOS接口之间的对应性。

6.1.3.4.2 功能测试

开发者应测试SSF和自身安全保护功能。测试文档应包括以下内容：
a) 测试计划：标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；
b) 预期的测试结果：表明测试完成后的预期输出；
c) 实际测试结果：和预期的测试结果一致；
d) 证实已知的漏洞被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

6.1.3.4.3 独立测试

开发者应提供一组与其自测时使用的同等资源，以用于SSOOS的测试。

6.1.3.4.4 密码测试

开发者应对所使用的对称、非对称和杂凑密码算法进行正确性和符合性测试，确保实际运算结果与预期的正确结果相符。

开发者应确保使用符合国家密码相关规定的对称、非对称和杂凑密码算法。

6.1.3.5 脆弱性评定

基于已标识的潜在脆弱性，操作系统应抵抗具有基本攻击潜力的攻击者的攻击。

注：抵抗基本攻击潜力的攻击者的攻击，需要根据以下5个具体因素综合考虑：攻击时间、攻击者能力、对操作系统的了解程度、访问操作系统时间或攻击样品数量、使用的攻击设备，见GB/T 30270—2013附录A中的A.8。

6.2 第二级：系统审计保护级

6.2.1 安全功能要求

6.2.1.1 身份鉴别

SSOOS的身份鉴别功能如下：

a) 用户标识功能：
   1) 用户进入操作系统前，应先进行标识；
   2) 操作系统用户标识应使用用户名和UID，并在操作系统的整个生存周期实现用户的唯一

性标识，以及用户名或别名、UID 等之间的一致性。

b) 用户鉴别功能：

1) 采用强化管理的口令鉴别/基于令牌的动态口令鉴别等机制，并在每次用户登录系统时和系统重新连接时进行鉴别；

2) 鉴别信息应是不可见的，在存储和传输时进行安全保护，确保其不被非授权的访问、修改和删除；

3) 通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时采取的措施来实现鉴别失败的处理。

c) 对注册到操作系统的用户，应将用户进程与其所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户。

6.2.1.2 自主访问控制

SSOOS 的自主访问控制功能如下：

a) 客体的拥有者对其拥有的全部客体应有权修改其访问权限；

b) 客体的拥有者应能对其拥有的客体设置其他用户的访问控制属性，访问控制属性至少包括：读、写、执行等；

c) 主体对客体的访问应遵循该客体的自主访问控制权限属性；

d) 将访问控制客体的颗粒度控制在文件和目录；

e) 当主体生成一个客体时，该客体应具有该主体设置的自主访问控制权限属性的默认值；

f) 自主访问控制应能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种访问，使用户对自己的行为承担明确的责任。

6.2.1.3 安全审计

SSOOS 的安全审计功能如下：

a) 应能对以下事件生成审计日志：

1) 身份鉴别、自主访问控制等安全功能的使用；

2) 创建、删除客体的操作；

3) 网络会话；

4) 所有管理员的操作。

b) 审计记录要求如下：

1) 每条审计记录应包括：事件类型、事件发生的日期和时间、触发事件的用户、事件成功或失败等字段；

2) 身份标识和鉴别事件类审计记录还应包括请求的源（如末端号或网络地址）；

3) 创建和删除客体事件的审计记录还应包括客体的名字；

4) 网络会话事件审计记录还应包括：网络程序名称、协议类型、源 IP 地址、目的 IP 地址、源端口、目的端口、会话总字节数等字段。

c) 应提供审计日志分析功能：

潜在侵害分析：设置审计日志累积或组合的规则，使用这些规则去监测已经生成的审计事件，并根据这些规则指示出对系统安全运行的潜在侵害。

d) 应提供审计日志的可选择查询功能，支持按以下条件之一或逻辑组合进行选择和排序查阅，并能导出查询结果：

1) 事件类型；

2) 日期和/或时间；

3） 用户身份；
4） 客体名称；
5） 成功或失败。

e） 应提供审计日志的保护功能：
1） 保证审计机制默认处于开启状态，且对审计日志的开启和关闭进行保护；
2） 保护审计日志不被未授权的访问；
3） 保证审计日志不被篡改和删除。

f） 应以便于用户理解的方式提供审计日志查阅功能。

g） 审计日志应存储在掉电非遗失性存储媒体中。系统管理员应能定义超过审计跟踪存储极限的阈值，当超过阈值时将向管理员报警。当审计存储空间被耗尽时，覆盖所存储的最早的审计记录。

6.2.1.4 数据完整性

SSOOS 的数据完整性保护功能如下：

a） 在操作系统内部传输的用户数据（如进程间的通信），应具备保证用户数据完整性的功能；

b） 在对数据进行访问操作时，应检查存储在存储媒体上的用户数据是否完整。

6.2.1.5 数据保密性

6.2.1.5.1 数据加密

SSOOS 的数据加密功能如下：

a） 应提供文件加密功能，用户可对指定的文件和目录进行加密保护；

b） 支持采用硬件形式对密钥进行保护。

6.2.1.6 网络安全保护

SSOOS 的网络安全保护功能如下：

a） 支持基于 IP 地址、端口、物理接口的双向网络访问控制，将不符合预先设定策略的数据包丢弃；

b） 对网络传输数据应能进行加密与完整性保护。

6.2.2 自身安全要求

6.2.2.1 运行安全保护

SSF 运行安全保护功能如下：

a） 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性进行定义。

b） 应区分普通操作模式和系统维护模式。

c） 在普通用户访问系统之前，系统应以一个安全的方式进行安装和配置。

d） 对备份等不影响 SSOOS 的常规的系统维护，可在普通操作模式执行。

e） 当操作系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。

f） 仅允许系统管理员修改或替换系统提供的可执行程序。

g） 在 SSOOS 出现故障或中断后，应使其以最小的损害得到恢复。并按 GB/T 20271—2006 中 5.1.2.2失败保护所描述的内容，处理 SSF 故障。

h) 应控制和审计系统控制台的使用。

i) 操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时获取、统一管理并及时运用补丁对操作系统的漏洞进行修补。

6.2.2.2 资源利用

6.2.2.2.1 容错

SSOOS 的容错功能如下：

a) 应通过一定措施确保当系统出现某些确定的故障情况时，SSF 也能维持正常运行，如系统检测和报告系统的服务水平已降低到预先规定的最小值；

b) 当系统资源的服务水平降低到预先规定的最小值时，应能检测和发出报告；

c) 应提供维护模式中运行系统的能力，在维护模式下各种安全功能全部失效。系统仅允许系统管理员进入维护模式。

6.2.2.2.2 服务优先级

SSOOS 的服务优先级功能如下：

a) 应采取服务优先级策略，设置主体使用 SSF 控制范围内某个资源子集的优先级，进行操作系统资源的管理和分配；

b) 应确保对所有操作系统资源的访问都基于主体所设置的优先级进行。

6.2.2.2.3 资源分配

SSOOS 的资源分配功能如下：

a) 应按 GB/T 20271—2006 中 5.1.4.2 a)最大限额资源分配的要求，进行操作系统资源的管理和分配。配额机制确保用户和主体将不会独占某种受控的资源。

b) 应确保在被授权的主体发出请求时，资源能被访问和利用。

c) 应以每个用户或每个用户组为基础，提供一种机制，控制其对磁盘的消耗和对 CPU 等资源的使用。

6.2.2.3 用户登录访问控制

SSOOS 的用户登录访问控制功能如下：

a) 应按 GB/T 20271—2006 中 5.1.5 a)会话建立机制的要求，根据访问地址或端口，允许或拒绝用户的登录。鉴别机制不准许被旁路。

b) 应按 GB/T 20271—2006 中 5.1.5 c)多重并发会话限定的要求，限制系统并发会话的最大数量，并利用默认值作为会话次数的限定数。

c) 成功登录系统后，操作系统应记录并向用户显示以下数据：

1) 本次登录的日期、时间、来源和上次成功登录系统的情况；

2) 上次成功访问系统以来身份鉴别失败的情况；

3) 口令到期的天数；

4) 成功或不成功的事件次数可以用整数计数、时间戳列表等表述方法。

6.2.2.4 可信度量

SSOOS 的可信度量功能如下：

a) 在操作系统启动时应对操作系统内核进行完整性度量；

b) **在可执行程序启动时应进行完整性度量；**

c) **应对完整性度量基准值进行安全存储，防止其被篡改。**

6.2.2.5 安全策略配置

应对身份鉴别、**安全审计**、网络安全保护、资源利用、用户登录访问控制提供安全策略配置功能。

6.2.3 安全保障要求

6.2.3.1 开发

6.2.3.1.1 安全架构

开发者应提供 SSOOS 的安全架构描述文档，安全架构描述文档应符合以下要求：

a) 与 SSOOS 设计文档中对安全功能要求和自身安全保护要求的描述一致；

b) 描述 SSOOS 的安全域；

c) 描述 SSOOS 初始化过程为何是安全的；

d) 证实 SSOOS 能够防止被破坏；

e) 证实 SSOOS 能够防止被旁路。

6.2.3.1.2 功能规范说明

开发者应提供功能规范说明，功能规范说明应符合以下要求：

a) 完全描述 SSF 和自身安全保护；

b) 描述所有 SSOOS 接口的目的与使用方法；

c) 标识和描述每个 SSOOS 接口相关的全部参数；

d) 描述实施过程中，与 SSOOS 接口相关的行为；

e) 证实安全功能要求和自身安全保护要求到 SSOOS 接口的追溯。

6.2.3.1.3 SSOOS 设计

开发者应提供 SSOOS 设计文档，SSOOS 设计文档应符合以下要求：

a) 描述 SSOOS 的结构；

b) 描述所有安全功能和自身安全保护模块，包括其目的及与其他模块间的相互作用；

c) 提供每一个安全功能和自身安全保护的描述；

d) 描述安全功能和自身安全保护间的相互作用；

e) 根据模块描述安全功能和自身安全保护。

6.2.3.2 指导性文档

6.2.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应符合以下要求：

a) 描述在安全处理环境中用户可访问的功能和特权，并包含可能造成危害的警示信息；

b) 描述如何以安全的方式使用 SSOOS 提供的安全功能和自身安全保护；

c) 描述安全功能和自身安全保护及接口，尤其是受用户控制的所有安全参数，适当时指明安全值；

d) 明确说明安全功能和自身安全保护有关的每一种安全相关事件，包括改变 SSOOS 所控制实

体的安全特性；

e) 标识 SSOOS 运行的所有可能状态(包括操作导致的失败或者操作性错误)，以及它们与维持安全运行之间的因果关系和联系；

f) 描述为确保 SSOOS 安全运行应执行的安全策略。

6.2.3.2.2 准备程序

开发者应提供操作系统及其准备程序，准备程序描述应符合以下要求：

a) 描述与开发者交付程序相一致的安全接收操作系统必需的所有步骤；

b) 描述安全安装操作系统及其运行环境必需的所有步骤。

6.2.3.3 生存周期支持

6.2.3.3.1 配置管理能力

开发者的配置管理能力应符合以下要求：

a) 为操作系统的不同版本提供唯一的标识；

b) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；

c) 配置管理系统唯一标识所有配置项，并对组成 SSOOS 的所有配置项进行维护；

d) 配置管理系统提供措施使得仅能对配置项进行授权变更；

e) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发 SSOOS；

f) 实施的配置管理与配置管理计划相一致。

6.2.3.3.2 配置管理范围

开发者应提供 SSOOS 配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) SSOOS、安全保障要求的评估证据和 SSOOS 的组成部分和实现表示；

b) 唯一标识配置项；

c) 对于每一个安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

6.2.3.3.3 交付程序

开发者应使用一定的交付程序交付操作系统，并将交付过程文档化。在给用户方交付指定版本操作系统时，交付文档应描述为维护安全所必需的所有程序。

6.2.3.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在 SSOOS 的开发环境中，为保护 SSOOS 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.2.3.3.5 生存周期定义

开发者应建立一个生存周期模型对 SSOOS 的开发和维护进行的必要控制，并提供生存周期定义文档描述用于开发和维护 SSOOS 的模型。

6.2.3.4 测试

6.2.3.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖文档应符合以下要求：

a) 证实测试文档中的测试与功能规范说明中 SSOOS 接口之间的对应性；
b) **证实已经测试了功能规范说明中的所有 SSOOS 接口**。

6.2.3.4.2 深度

开发者应提供测试深度的分析文档。测试深度分析文档应符合以下要求：
a) **证实测试文档中的测试与安全功能和自身安全保护之间的对应性；**
b) **证实已经测试了 SSOOS 设计中的所有安全功能和自身安全保护功能。**

6.2.3.4.3 功能测试

开发者应测试 SSF 和自身安全保护功能。测试文档应包括以下内容：
a) 测试计划：标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；
b) 预期的测试结果：表明测试完成后的预期输出；
c) 实际测试结果：和预期的测试结果一致；
d) 证实已知的漏洞被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

6.2.3.4.4 独立测试

开发者应提供一组与其自测时使用的同等资源，以用于 SSOOS 的测试。

6.2.3.4.5 密码测试

开发者应对所使用的对称、非对称和杂凑密码算法进行正确性和符合性测试，确保实际运算结果与预期的正确结果相符。

开发者应确保使用符合国家密码相关规定的对称、非对称和杂凑密码算法。

6.2.3.5 脆弱性评定

基于已标识的潜在脆弱性，操作系统应抵抗具有基本攻击潜力的攻击者的攻击。

注：抵抗基本攻击潜力的攻击者的攻击，需要根据以下 5 个具体因素综合考虑：攻击时间、攻击者能力、对操作系统的了解程度、访问操作系统时间或攻击样品数量、使用的攻击设备，见 GB/T 30270—2013 附录 A 中的 A.8。

6.3 第三级：安全标记保护级

6.3.1 安全功能要求

6.3.1.1 身份鉴别

SSOOS 的身份鉴别功能如下：
a) 用户标识功能：
   1) 用户进入操作系统前，应先进行标识；
   2) 操作系统用户标识应使用用户名和 UID，并在操作系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性。
b) 用户鉴别功能：
   1) 采用强化管理的口令鉴别/基于令牌的动态口令鉴别/**生物特征鉴别/数字证书鉴别等相结合的方式，使用多鉴别机制实现对用户身份的真实性鉴别**，并在每次用户登录系统时和系统重新连接时进行鉴别；

2） 鉴别信息应是不可见的，在存储和传输时进行安全保护，确保其不被非授权的访问、修改和删除；

3） 通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时采取的措施来实现鉴别失败的处理。

c） 对注册到操作系统的用户，应将用户进程与其所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户。

6.3.1.2 自主访问控制

SSOOS 的自主访问控制功能如下：

a） 客体的拥有者对其拥有的全部客体应有权修改其访问权限。

b） 客体的拥有者应能对其拥有的客体设置其他用户的访问控制属性，访问控制属性至少包括：读、写、执行等。

c） 主体对客体的访问应遵循该客体的自主访问控制权限属性。

d） 有更细颗粒度的自主访问控制，将访问控制主体的颗粒度控制在单个用户，将访问控制客体的颗粒度控制在文件和目录。

e） 当主体生成一个客体时，该客体应具有该主体设置的自主访问控制权限属性的默认值。

f） 自主访问控制应能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种访问，使用户对自己的行为承担明确的责任。

g） 客体的拥有者应能对其拥有的客体设置为：拥有者是唯一有权修改其访问权限的主体。

h） 不准许客体拥有者把客体的控制权分配给其他主体。

6.3.1.3 标记和强制访问控制

SSOOS 的标记和强制访问控制功能如下：

a） 采用标记的方法为操作系统的指定主体和客体（例如：系统进程、文件、目录等）标明其安全属性。

b） 客体的标记应和客体数据紧密结合。

c） 主体和客体的安全属性标记构成了机密性和完整性安全策略模型。强制访问控制应基于标记和安全策略模型，实现主体对客体读、写和执行等操作的访问控制。

d） 强制访问控制应与用户身份鉴别、标记等安全功能紧密结合，使系统对用户的安全控制包含从系统启动到退出系统的全过程，强制访问控制对客体的控制范围涉及操作系统内部的存储、处理和传输过程。

e） 将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，按职能分割分别授予它们各自为完成自己所承担任务所需的权限，并形成相互制约关系。由系统安全员统一管理操作系统中与强制访问控制等安全机制有关的事件和信息。

f） 运行于网络环境的多台计算机上的网络操作系统，在需要进行统一管理时，应考虑各台计算机操作系统中主、客体安全属性设置的一致性，并实现跨网络的操作系统间用户数据保密性和完整性保护。

6.3.1.4 安全审计

SSOOS 的安全审计功能如下：

a） 应能对以下事件生成审计日志：

1） 身份鉴别、自主访问控制、标记和强制访问控制等安全功能的使用；

2） 创建、删除客体的操作；
3） 网络会话；
4） 所有管理员的操作。

b） 审计记录要求如下：
1） 每条审计记录应包括：事件类型、事件发生的日期和时间、触发事件的用户、事件成功或失败等字段；
2） 身份标识和鉴别事件类审计记录还应包括请求的源（如末端号或网络地址）；
3） 创建和删除客体的事件审计记录还应包括客体的名字、**客体的安全属性**；
4） 网络会话事件审计记录还应包括：网络程序名称、协议类型、源 IP 地址、目的 IP 地址、源端口、目的端口、会话总字节数等字段。

c） 应提供审计日志分析功能：
1） 潜在侵害分析：设置审计日志累积或组合的规则，使用这些规则去监测已经生成的审计事件，并根据这些规则指示出对系统安全运行的潜在侵害；
2） **基于模板的异常检测：根据用户的历史使用模式建立模板，用置疑等级表示用户当前活动与模板中已建立的使用模式不一致的程度，当用户的置疑等级超过门限条件时，能指出对操作系统的可能侵害即将发生**。

d） **当检测到潜在的安全侵害时，应生成实时报警**。

e） 应提供审计日志的可选择查询功能，支持按以下条件之一或逻辑组合进行选择和排序查阅，并能导出查询结果：
1） 事件类型；
2） 日期和/或时间；
3） 用户身份；
4） 客体名称；
5） 成功或失败。

f） 应提供审计日志的保护功能：
1） 保证审计机制默认处于开启状态，且对审计日志的开启和关闭进行保护；
2） 保护审计日志不被未授权的访问；
3） 保证审计日志不被篡改和删除，**并记录尝试篡改和删除审计日志的行为**。

g） 应以便于用户理解的方式提供审计日志查阅功能；

h） 审计日志应存储在掉电非遗失性存储媒体中。系统管理员应能定义超过审计跟踪存储极限的阈值，当超过阈值时将向管理员报警。当审计存储空间被耗尽时，覆盖所存储的最早的审计记录。

6.3.1.5 数据完整性

SSOOS 的数据完整性保护功能如下：

a） 在操作系统内部传输的用户数据（如进程间的通信），应具备保证用户数据完整性的功能；

b） 在对数据进行访问操作时，应检查存储在存储媒体上的用户数据是否完整；

c） **应提供一个实用程序来校验文件系统和磁盘的完整性。此实用程序应可由操作系统自动执行**。

6.3.1.6 数据保密性

6.3.1.6.1 客体重用

SSOOS 的客体重用功能如下：

a) **确保非授权用户不能查找使用后返还系统的存储媒体(至少包括:磁盘和内存等)中的信息;**
b) **确保非授权用户不能查找系统现已分配给它的存储媒体(至少包括:磁盘和内存等)中以前的信息。**

6.3.1.6.2 数据加密

SSOOS 的数据加密功能如下:
a) 应提供文件加密功能,用户可对指定的文件和目录进行加密保护;
b) 支持采用硬件形式对密钥进行保护;
c) **应提供文件系统加密功能,对存储在加密文件系统中的文件和目录,进行透明加解密。**

6.3.1.7 网络安全保护

SSOOS 的网络安全保护功能如下:
a) 支持基于 IP 地址、端口、物理接口**和应用程序**的双向网络访问控制,将不符合预先设定策略的数据包丢弃;
b) 对网络传输数据应能进行加密与完整性保护;
c) **支持基于系统身份、系统运行状态的双向网络可信接入认证;**
d) **应对网络访问进行控制,只有被授权的进程才能访问网络。**

6.3.2 自身安全要求

6.3.2.1 运行安全保护

SSF 运行安全保护功能如下:
a) 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前,对用户和管理员的安全策略属性进行定义。
b) 应区分普通操作模式和系统维护模式。
c) 在普通用户访问系统之前,系统应以一个安全的方式进行安装和配置。
d) 对备份等不影响 SSOOS 的常规的系统维护,可在普通操作模式执行。
e) 当操作系统安装完成后,在普通用户访问之前,系统应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。
f) 仅允许系统管理员修改或替换系统提供的可执行程序。
g) **应为操作系统安全管理人员提供一种机制,来产生安全参数值的详细报告。**
h) 在 SSOOS 出现故障或中断后,应使其以最小的损害得到恢复。并按 GB/T 20271—2006 中 5.1.2.2失败保护所描述的内容,处理 SSF 故障。**系统因故障或其他原因中断后,应启动系统恢复机制。**
i) 应控制和审计系统控制台的使用。
j) 操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时获取、统一管理并及时运用补丁对操作系统的漏洞进行修补。

6.3.2.2 资源利用

6.3.2.2.1 容错

SSOOS 的容错功能如下:
a) 应通过一定措施确保当系统出现某些确定的故障情况时,SSF 也能维持正常运行,如系统检测和报告系统的服务水平已降低到预先规定的最小值。

b) 当系统资源的服务水平降低到预先规定的最小值时，应能检测和发出报告。

c) 应提供维护模式中运行系统的能力，在维护模式下各种安全功能全部失效。系统仅允许系统管理员进入维护模式。

d) **系统应提供软件及数据备份和恢复的过程，在系统中加入再启动的同步点，以便于系统的恢复。**

e) **系统应提供能用于定期确认系统正确操作的机制和过程，这些机制或过程涉及系统资源的监视、硬件和固件单元的正确操作、对可能在全系统内传播的错误状态的检测以及超过用户规定门限的通信差错的检测等内容。**

6.3.2.2.2 服务优先级

SSOOS 的服务优先级功能如下：

a) 应采取服务优先级策略，设置主体使用 SSF 控制范围内某个资源子集的优先级，进行操作系统资源的管理和分配；

b) 应确保对所有操作系统资源的访问都基于主体所设置的优先级进行。

6.3.2.2.3 资源分配

SSOOS 的资源分配功能如下：

a) 应按 GB/T 20271—2006 中 5.1.4.2 a)最大限额资源分配的要求，进行操作系统资源的管理和分配。配额机制确保用户和主体将不会独占某种受控的资源。

b) 应确保在被授权的主体发出请求时，资源能被访问和利用。

c) 应以每个用户或每个用户组为基础，提供一种机制，控制其对磁盘的消耗和对 CPU 等资源的使用。

d) **应提供用户查看可访问系统资源的修改历史记录的权限。**

6.3.2.3 用户登录访问控制

SSOOS 的用户登录访问控制功能如下：

a) 应按 GB/T 20271—2006 中 5.1.5 a)会话建立机制的要求，根据访问地址或端口，允许或拒绝用户的登录。鉴别机制不准许被旁路。

b) 应按 GB/T 20271—2006 中 5.1.5 c)多重并发会话限定的要求，限制系统并发会话的最大数量，并利用默认值作为会话次数的限定数。

c) 成功登录系统后，操作系统应记录并向用户显示以下数据：

   1) 本次登录的日期、时间、来源和上次成功登录系统的情况；

   2) 上次成功访问系统以来身份鉴别失败的情况；

   3) 口令到期的天数；

   4) 成功或不成功的事件次数可以用整数计数、时间戳列表等表述方法。

d) **在规定的未使用时限后，系统应断开会话或重新鉴别用户。系统提供时限的默认值。**

e) **系统应提供锁定用户键盘的机制，键盘开锁过程要求鉴别用户。**

f) **当用户鉴别过程不正确的次数达到系统规定的次数时，系统应退出登录过程。**

g) **系统应提供一种机制，按时间、进入方式、地点、网络地址或端口等条件规定哪些用户能进入系统。**

6.3.2.4 可信度量

SSOOS 的可信度量功能如下：

a) 在操作系统启动时应对操作系统内核进行完整性度量；
b) 在可执行程序启动时应进行完整性度量；
c) 应对完整性度量基准值进行可信存储，防止其被篡改；
d) **支持硬件可信芯片作为信任根**。

6.3.2.5 安全策略配置

应对身份鉴别、**标记和强制访问控制**、安全审计、网络安全保护、资源利用、用户登录访问控制提供安全策略配置功能。

6.3.3 安全保障要求

6.3.3.1 开发

6.3.3.1.1 安全架构

开发者应提供 SSOOS 的安全架构描述文档，安全架构描述文档应符合以下要求：
a) 与 SSOOS 设计文档中对安全功能要求和自身安全保护要求的描述一致；
b) 描述 SSOOS 的安全域；
c) 描述 SSOOS 初始化过程为何是安全的；
d) 证实 SSOOS 能够防止被破坏；
e) 证实 SSOOS 能够防止被旁路。

6.3.3.1.2 功能规范说明

开发者应提供功能规范说明，功能规范说明应符合以下要求：
a) 完全描述 SSF 和自身安全保护；
b) 描述所有 SSOOS 接口的目的与使用方法；
c) 标识和描述每个 SSOOS 接口相关的全部参数；
d) 描述实施过程中，与 SSOOS 接口相关的**所有**行为；
e) 证实安全功能要求和自身安全保护要求到 SSOOS 接口的追溯；
f) **描述可能由每个 SSOOS 接口的调用而引起的所有直接错误消息**。

6.3.3.1.3 实现表示

开发者应提供实现表示说明，并在自身选择的场所内提供 SSOOS 的全部实现表示。实现表示及说明应符合以下要求：
a) **应详细定义 SSF 和自身安全保护，详细程度达到无需进一步设计就能生成 SSOOS；**
b) **实现表示以开发人员使用的形式提供；**
c) **在实现表示说明中提供 SSOOS 设计描述与实现表示之间的映射，并证明其一致性。**

6.3.3.1.4 SSOOS 设计

开发者应提供 SSOOS 设计文档，SSOOS 设计文档应符合以下要求：
a) 描述 SSOOS 的结构；
b) **描述所有安全功能和自身安全保护模块，包括其目的及与其他模块间的相互作用；**
c) 提供每一个安全功能和自身安全保护的描述；
d) 描述安全功能和自身安全保护间的相互作用；
e) **提供安全功能和自身安全保护模块间的映射关系；**

f) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的 SSOOS 接口；
g) 根据模块描述安全功能和自身安全保护。

6.3.3.2 指导性文档

6.3.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应符合以下要求：

a) 描述在安全处理环境中用户可访问的功能和特权，并包含可能造成危害的警示信息；
b) 描述如何以安全的方式使用 SSOOS 提供的安全功能和自身安全保护；
c) 描述安全功能和自身安全保护及接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明安全功能和自身安全保护有关的每一种安全相关事件，包括改变 SSOOS 所控制实体的安全特性；
e) 标识 SSOOS 运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f) 描述为确保 SSOOS 安全运行应执行的安全策略。

6.3.3.2.2 准备程序

开发者应提供操作系统及其准备程序，准备程序描述应符合以下要求：

a) 描述与开发者交付程序相一致的安全接收操作系统必需的所有步骤；
b) 描述安全安装操作系统及其运行环境必需的所有步骤。

6.3.3.3 生存周期支持

6.3.3.3.1 配置管理能力

开发者的配置管理能力应符合以下要求：

a) 为操作系统的不同版本提供唯一的标识；
b) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
c) 配置管理系统唯一标识所有配置项，并对组成 SSOOS 的所有配置项进行维护；
d) 提供**自动化的**措施使得仅能对配置项进行授权变更；
e) **配置管理系统提供一种自动方式来支持 SSOOS 的生成**；
f) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发 SSOOS；
g) 实施的配置管理与配置管理计划相一致；
h) **配置管理计划描述用来接受修改过的或新建的作为 SSOOS 组成部分的配置项的程序**。

6.3.3.3.2 配置管理范围

开发者应提供 SSOOS 配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) SSOOS、安全保障要求的评估证据和 SSOOS 的组成部分和实现表示、**安全缺陷报告及其解决状态**；
b) 唯一标识配置项；
c) 对于每一个安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

6.3.3.3.3 交付程序

开发者应使用一定的交付程序交付操作系统，并将交付过程文档化。在给用户方交付指定版本操作系统时，交付文档应描述为维护安全所必需的所有程序。

6.3.3.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在 SSOOS 的开发环境中，为保护 SSOOS 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.3.3.3.5 生存周期定义

开发者应建立一个生存周期模型对 SSOOS 的开发和维护进行的必要控制，并提供生存周期定义文档描述用于开发和维护 SSOOS 的模型。

6.3.3.3.6 工具和技术

开发者应明确定义用于开发 SSOOS 的工具，并提供开发工具文档。开发工具文档应无歧义地定义所有语句和实现用到的所有协定与命令的含义，应无歧义地定义所有实现依赖选项的含义。

6.3.3.4 测试

6.3.3.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖文档应符合以下要求：

a) 证实测试文档中的测试与功能规范说明中 SSOOS 接口之间的对应性；

b) 证实已经测试了功能规范说明中的所有 SSOOS 接口。

6.3.3.4.2 深度

开发者应提供测试深度的分析文档。测试深度分析文档应符合以下要求：

a) 证实测试文档中的测试与安全功能和自身安全保护**模块**之间的对应性；

b) 证实已经测试了 SSOOS 设计中的所有安全功能**模块**和自身安全保护功能**模块**。

6.3.3.4.3 功能测试

开发者应测试 SSF 和自身安全保护功能。测试文档应包括以下内容：

a) 测试计划：标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b) 预期的测试结果：表明测试完成后的预期输出；

c) 实际测试结果：和预期的测试结果一致；

d) 证实已知的漏洞被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

6.3.3.4.4 独立测试

开发者应提供一组与其自测时使用的同等资源，以用于 SSOOS 的测试。

6.3.3.4.5 密码测试

开发者应对所使用的对称、非对称和杂凑密码算法进行正确性和符合性测试，确保实际运算结果与

预期的正确结果相符。

开发者应确保使用符合国家密码相关规定的对称、非对称和杂凑密码算法。

6.3.3.4.6 代码安全性测试

开发者应对 SSOOS 实现表示和操作系统内核代码进行安全性测试，证实代码中不存在安全缺陷或后门。

6.3.3.5 脆弱性评定

基于已标识的潜在脆弱性，操作系统应抵抗具有**增强型**基本攻击潜力的攻击者的攻击。

注：抵抗增强型基本攻击潜力的攻击者的攻击，需要根据以下 5 个具体因素综合考虑：攻击时间、攻击者能力、对操作系统的了解程度、访问操作系统时间或攻击样品数量、使用的攻击设备，见 GB/T 30270—2013 附录 A 中的 A.8。

6.4 第四级：结构化保护级

6.4.1 安全功能要求

6.4.1.1 身份鉴别

SSOOS 的身份鉴别功能如下：

a) 用户标识功能：
   1) 用户进入操作系统前，应先进行标识；
   2) 操作系统用户标识应使用用户名和 UID，并在操作系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性。
b) 用户鉴别功能：
   1) 采用强化管理的口令鉴别和/或生物特征鉴别和/或数字证书等相结合的方式，使用多鉴别机制实现对用户身份的真实性鉴别，并在每次用户登录系统时和系统重新连接时进行鉴别；
   2) 鉴别信息应是不可见的，在存储和传输时进行安全保护，确保其不被非授权的访问、修改和删除；
   3) 通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时采取的措施来实现鉴别失败的处理。
c) 对注册到操作系统的用户，应将用户进程与其所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户。

6.4.1.2 自主访问控制

SSOOS 的自主访问控制功能如下：

a) 客体的拥有者对其拥有的全部客体应有权修改其访问权限。
b) 客体的拥有者应能对其拥有的客体设置其他用户的访问控制属性，访问控制属性至少包括：读、写、执行等。
c) 主体对客体的访问应遵循该客体的自主访问控制权限属性。
d) 有更细颗粒度的自主访问控制，将访问控制主体的颗粒度控制在单个用户，将访问控制客体的颗粒度控制在文件和目录。
e) 当主体生成一个客体时，该客体应具有该主体设置的自主访问控制权限属性的默认值。
f) 自主访问控制应能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种

访问，使用户对自己的行为承担明确的责任。

g) 客体的拥有者应能对其拥有的客体设置为：拥有者是唯一有权修改其访问权限的主体。

h) 不准许客体拥有者把客体的控制权分配给其他主体。

6.4.1.3 标记和强制访问控制

SSOOS 的标记和强制访问控制功能如下：

a) 采用标记的方法为操作系统**所有主体和客体**（包括系统所有的进程、文件、目录等）标明其安全属性。

b) 客体的标记应和客体数据紧密结合，**当信息从操作系统控制范围之内向控制范围之外输出时，带有安全标记；当信息从操作系统控制范围之外向控制范围之内输入时，通过标记标明其安全属性。如打印输出的数据，需明显标示出该数据的安全标记**。

c) 主体和客体的安全属性标记构成了机密性和完整性安全策略模型，**这些安全策略模型具有相应的半形式化证明**。强制访问控制应基于标记和安全策略模型，实现主体对客体读、写和执行等操作的访问控制。

d) 强制访问控制应与用户身份鉴别、标记等安全功能紧密结合，使系统对用户的安全控制包含从系统启动到退出系统的全过程，强制访问控制对客体的控制范围涉及操作系统内部的存储、处理和传输过程**及信息进行输入、输出操作的过程**。

e) 将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，按职能分割和**最小授权原则**分别授予它们各自为完成自己所承担任务所需的**最小**权限，并形成相互制约关系。由系统安全员统一管理操作系统中与强制访问控制等安全机制有关的事件和信息。

f) 运行于网络环境的多台计算机上的网络操作系统，在需要进行统一管理时，应考虑各台计算机操作系统中主、客体安全属性设置的一致性，并实现跨网络的操作系统间用户数据保密性和完整性保护。

6.4.1.4 安全审计

SSOOS 的安全审计功能如下：

a) 应能对以下事件生成审计日志：

1) 身份鉴别、自主访问控制、标记和强制访问控制等安全功能的使用；

2) 创建、删除客体的操作；

3) 网络会话；

4) 所有管理员的操作。

b) 审计记录要求如下：

1) 每条审计记录应包括：事件类型、事件发生的日期和时间、触发事件的用户、事件成功或失败等字段；

2) 身份标识和鉴别事件类审计记录还应包括请求的源（如末端号或网络地址）；

3) 创建和删除客体的事件审计记录还应包括客体的名字、客体的安全属性；

4) 网络会话事件审计记录还应包括：网络程序名称、协议类型、源 IP 地址、目的 IP 地址、源端口、目的端口、会话总字节数等字段。

c) 应提供审计日志分析功能：

1) 潜在侵害分析：设置审计日志累积或组合的规则，使用这些规则去监测已经生成的审计事件，并根据这些规则指示出对系统安全运行的潜在侵害；

2) 基于模板的异常检测：根据用户的历史使用模式建立模板，用置疑等级表示用户当前活动

与模板中已建立的使用模式不一致的程度，当用户的置疑等级超过门限条件时，能指出对操作系统的可能侵害即将发生；

3） **简单攻击探测：当发现一个系统事件与一个潜在违反系统安全策略的特征事件匹配时，能指出潜在违反系统安全策略的事件即将发生**。

d） 当检测到潜在的安全侵害时，应生成实时报警，**并终止违例进程**。

e） 应提供审计日志的可选择查询功能，支持按以下条件之一或逻辑组合进行选择和排序查阅，并能导出查询结果：

1） 事件类型；

2） 日期和/或时间；

3） 用户身份；

4） 客体名称；

5） 成功或失败。

f） 应提供审计日志的保护功能：

1） 保证审计机制默认处于开启状态，且对审计日志的开启和关闭进行保护；

2） 保护审计日志不被未授权的访问；

3） 保证审计日志不被篡改和删除，并记录尝试篡改和删除审计日志的行为。

g） 应以便于用户理解的方式提供审计日志查阅功能。

h） 审计日志应存储在掉电非遗失性存储媒体中。系统管理员应能定义超过审计跟踪存储极限的阈值，当超过阈值时将向管理员报警。当审计存储空间被耗尽时，覆盖所存储的最早的审计记录。

6.4.1.5 数据完整性

SSOOS 的数据完整性保护功能如下：

a） 在操作系统内部进行的**数据传输**（如进程间的通信），应具备保证数据完整的功能。

b） 在对数据进行访问操作时，应检查存储在存储媒体上的用户数据是否完整，**并在检查到不完整时进行恢复**。

c） 应提供一个实用程序来校验文件系统和磁盘的完整性。此实用程序应可由操作系统自动执行。

6.4.1.6 数据保密性

6.4.1.6.1 客体重用

SSOOS 的客体重用功能如下：

a） 确保非授权用户不能查找使用后返还系统的存储媒体（至少包括：磁盘和内存等）中的信息；

b） 确保非授权用户不能查找系统现已分配给它的存储媒体（至少包括：磁盘和内存等）中以前的信息。

6.4.1.6.2 数据加密

SSOOS 的数据加密功能如下：

a） 应提供文件加密功能，用户可对指定的文件和目录进行加密保护；

b） **应对密钥提供基于硬件信任根的可信存储支持**；

c） 应提供文件系统加密功能，对存储在加密文件系统中的文件和目录，进行透明加解密。

6.4.1.7 可信路径

在本地用户和远程用户进行初始登录和/或鉴别时，操作系统应在它与用户之间建立一条安全的通信路径。此路径对其端点进行了可信标识，并能保护鉴别通信数据免遭修改、泄露。

6.4.1.8 可信信道

应在操作系统和另一个可信操作系统之间提供一条通信信道，此信道在逻辑上与其他通信信道隔离，对其端点进行了可信标识，并能保护通信数据免遭修改、泄露。

6.4.1.9 网络安全保护

SSOOS 的网络安全保护功能如下：

a) 支持基于 IP 地址、端口、物理接口和应用程序的双向网络访问控制，将不符合预先设定策略的数据包丢弃；
b) 对网络传输数据应能进行加密与完整性保护；
c) 支持基于系统身份、系统运行状态的双向网络可信接入认证；
d) 应对网络访问进行控制，只有被授权的且**通过可信度量**的进程才能访问网络。

6.4.2 自身安全要求

6.4.2.1 运行安全保护

SSF 运行安全保护功能如下：

a) 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前，对用户和管理员的安全策略属性进行定义。
b) 应区分普通操作模式和系统维护模式。
c) 在普通用户访问系统之前，系统应以一个安全的方式进行安装和配置。
d) 对备份等不影响 SSOOS 的常规的系统维护，可在普通操作模式执行。
e) 当操作系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。
f) 仅允许系统管理员修改或替换系统提供的可执行程序。
g) 应为操作系统安全管理人员提供一种机制，来产生安全参数值的详细报告。
h) 在 SSOOS 出现故障或中断后，应使其以最小的损害得到恢复。并按 GB/T 20271—2006 中 5.1.2.2失败保护所描述的内容，处理 SSF 故障。系统因故障或其他原因中断后，应启动系统恢复机制。
i) 应控制和审计系统控制台的使用。
j) 操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时获取、统一管理并及时运用补丁对操作系统的漏洞进行修补。

6.4.2.2 资源利用

6.4.2.2.1 容错

SSOOS 的容错功能如下：

a) 应通过一定措施确保当系统出现某些确定的故障情况时，SSF 也能维持正常运行，如系统检测和报告系统的服务水平已降低到预先规定的最小值。
b) 当系统资源的服务水平降低到预先规定的最小值时，应能检测和发出报告。

c) 应提供维护模式中运行系统的能力，在维护模式下各种安全功能全部失效。系统仅允许系统管理员进入维护模式。

d) 系统应提供软件及数据备份和恢复的过程，在系统中加入再启动的同步点，以便于系统的恢复。

e) 系统应提供能用于定期确认系统正确操作的机制和过程，这些机制或过程涉及系统资源的监视、硬件和固件单元的正确操作、对可能在全系统内传播的错误状态的检测以及超过用户规定门限的通信差错的检测等内容。

6.4.2.2.2 服务优先级

SSOOS的服务优先级功能如下：

a) 应采取服务优先级策略，设置主体使用SSF控制范围内某个资源子集的优先级，进行操作系统资源的管理和分配；

b) 应确保对所有操作系统资源的访问都基于主体所设置的优先级进行。

6.4.2.2.3 资源分配

SSOOS的资源分配功能如下：

a) 应按GB/T 20271—2006中5.1.4.2 a)最大限额资源分配的要求，进行操作系统资源的管理和分配。配额机制确保用户和主体将不会独占某种受控的资源。

b) 应确保在被授权的主体发出请求时，资源能被访问和利用。

c) 应以每个用户或每个用户组为基础，提供一种机制，控制其对磁盘的消耗和对CPU等资源的使用。

d) 应提供用户查看可访问系统资源的修改历史记录的权限。

6.4.2.3 用户登录访问控制

SSOOS的用户登录访问控制功能如下：

a) 应按GB/T 20271—2006中5.1.5 a)会话建立机制的要求，根据访问地址或端口，允许或拒绝用户的登录。鉴别机制不准许被旁路。

b) 应按GB/T 20271—2006中5.1.5 c)多重并发会话限定的要求，限制系统并发会话的最大数量，并利用默认值作为会话次数的限定数。

c) 成功登录系统后，操作系统应记录并向用户显示以下数据：

1) 本次登录的日期、时间、来源和上次成功登录系统的情况；

2) 上次成功访问系统以来身份鉴别失败的情况；

3) 口令到期的天数；

4) 成功或不成功的事件次数可以用整数计数、时间戳列表等表述方法。

d) 在规定的未使用时限后，系统应断开会话或重新鉴别用户。系统提供时限的默认值。

e) 系统应提供锁定用户键盘的机制，键盘开锁过程要求鉴别用户。

f) 当用户鉴别过程不正确的次数达到系统规定的次数时，系统应退出登录过程。

g) 系统应提供一种机制，按时间、进入方式、地点、网络地址或端口等条件规定哪些用户能进入系统。

6.4.2.4 可信度量

SSOOS的可信度量功能如下：

a) 在操作系统启动时应对操作系统内核进行完整性度量；

b) 在可执行程序启动时应进行完整性度量；
c) 应对完整性度量基准值进行可信存储，防止其被篡改；
d) 支持硬件可信芯片作为信任根。

6.4.2.5 可信恢复

当系统失效或服务中断时，应确保操作系统能够自动恢复到安全运行状态。

6.4.2.6 安全策略配置

应对身份鉴别、标记和强制访问控制、安全审计、**可信路径**、**可信信道**、网络安全保护、资源利用、用户登录访问控制提供安全策略配置功能。

6.4.3 安全保障要求

6.4.3.1 开发

6.4.3.1.1 安全架构

开发者应提供 SSOOS 的安全架构描述文档，安全架构描述文档应符合以下要求：
a) 与 SSOOS 设计文档中对安全功能要求和自身安全保护要求的描述一致；
b) 描述 SSOOS 的安全域；
c) 描述 SSOOS 初始化过程为何是安全的；
d) 证实 SSOOS 能够防止被破坏；
e) 证实 SSOOS 能够防止被旁路。

6.4.3.1.2 功能规范说明

开发者应提供功能规范说明，功能规范说明应符合以下要求：
a) 完全描述 SSF 和自身安全保护；
b) 描述所有 SSOOS 接口的目的与使用方法；
c) 标识和描述每个 SSOOS 接口相关的全部参数；
d) 描述实施过程中，与 SSOOS 接口相关的所有行为；
e) 证实安全功能要求和自身安全保护要求到 SSOOS 接口的追溯；
f) 描述可能由每个 SSOOS 接口的调用而引起的所有直接错误消息；
g) **使用半形式化方式描述 SSOOS 接口。**

6.4.3.1.3 实现表示

开发者应提供实现表示说明，并在自身选择的场所内提供 SSOOS 的全部实现表示。实现表示及说明应符合以下要求：
a) 应详细定义 SSF 和自身安全保护，详细程度达到无需进一步设计就能生成 SSOOS；
b) 实现表示以开发人员使用的形式提供；
c) 在实现表示说明中提供 SSOOS 设计描述与实现表示之间的映射，并证明其一致性。

6.4.3.1.4 SSOOS 设计

开发者应提供 SSOOS 设计文档，SSOOS 设计文档应符合以下要求：
a) 描述 SSOOS 的结构；
b) 描述所有安全功能和自身安全保护模块，包括其目的及与其他模块间的相互作用；

c) 提供每一个安全功能和自身安全保护的半形式化描述，适当时配以非形式化的、解释性的描述；
d) 描述安全功能和自身安全保护间的相互作用；
e) 提供安全功能和自身安全保护模块间的映射关系；
f) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的 SSOOS 接口；
g) 根据模块描述安全功能和自身安全保护。

6.4.3.1.5 SSOOS 内部结构

开发者应提供 SSOOS 内部结构的描述和论证过程文档，SSOOS 内部结构文档应符合以下要求：
a) 论证过程文档用于判定“结构合理”的特性；
b) SSOOS 内部结构描述证实指定的整个 SSOOS 内部结构合理。

6.4.3.2 指导性文档

6.4.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应符合以下要求：
a) 描述在安全处理环境中用户可访问的功能和特权，并包含可能造成危害的警示信息；
b) 描述如何以安全的方式使用 SSOOS 提供的安全功能和自身安全保护；
c) 描述安全功能和自身安全保护及接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明安全功能和自身安全保护有关的每一种安全相关事件，包括改变 SSOOS 所控制实体的安全特性；
e) 标识 SSOOS 运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f) 描述为确保 SSOOS 安全运行应执行的安全策略。

6.4.3.2.2 准备程序

开发者应提供操作系统及其准备程序，准备程序描述应符合以下要求：
a) 描述与开发者交付程序相一致的安全接收操作系统必需的所有步骤；
b) 描述安全安装操作系统及其运行环境必需的所有步骤。

6.4.3.3 生存周期支持

6.4.3.3.1 配置管理能力

开发者的配置管理能力应符合以下要求：
a) 为操作系统的不同版本提供唯一的标识；
b) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
c) 配置管理系统唯一标识所有配置项，并对组成 SSOOS 的所有配置项进行维护；
d) 提供自动化的措施使得仅能对配置项进行授权变更；
e) 配置管理系统提供一种自动方式来支持 SSOOS 的生成；
f) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发 SSOOS；
g) 实施的配置管理与配置管理计划相一致；

h) 配置管理计划描述用来接受修改过的或新建的作为 SSOOS 组成部分的配置项的程序。

6.4.3.3.2 配置管理范围

开发者应提供 SSOOS 配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) SSOOS、安全保障要求的评估证据和 SSOOS 的组成部分和实现表示、安全缺陷报告及其解决状态、**开发工具及其相关信息**；

b) 唯一标识配置项；

c) 对于每一个安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

6.4.3.3.3 交付程序

开发者应使用一定的交付程序交付操作系统，并将交付过程文档化。在给用户方交付指定版本操作系统时，交付文档应描述为维护安全所必需的所有程序。

6.4.3.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在 SSOOS 的开发环境中，为保护 SSOOS 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.4.3.3.5 生存周期定义

开发者应建立一个生存周期模型对 SSOOS 的开发和维护进行的必要控制，并提供生存周期定义文档描述用于开发和维护 SSOOS 的模型。

6.4.3.3.6 工具和技术

开发者应描述所使用的实现标准。开发者应明确定义用于开发 SSOOS 的工具，并提供开发工具文档。开发工具文档应无歧义地定义所有语句和实现用到的所有协定与命令的含义，应无歧义地定义所有实现依赖选项的含义。

6.4.3.4 测试

6.4.3.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖文档应符合以下要求：

a) 证实测试文档中的测试与功能规范说明中 SSOOS 接口之间的对应性；

b) 证实已经测试了功能规范说明中的所有 SSOOS 接口。

6.4.3.4.2 深度

开发者应提供测试深度的分析文档。测试深度分析文档应符合以下要求：

a) 证实测试文档中的测试与 SSOOS 设计中的安全功能和自身安全保护模块之间的对应性；

b) 证实已经测试了 SSOOS 设计中的所有安全功能模块和自身安全保护功能模块。

6.4.3.4.3 功能测试

开发者应测试 SSF 和自身安全保护功能。测试文档应包括以下内容：

a) 测试计划：标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b) 预期的测试结果：表明测试完成后的预期输出；

c) 实际测试结果：和预期的测试结果一致；

d) 证实已知的漏洞被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

6.4.3.4.4 独立测试

开发者应提供一组与其自测时使用的同等资源，以用于 SSOOS 的测试。

6.4.3.4.5 密码测试

开发者应对所使用的对称、非对称和杂凑密码算法进行正确性和符合性测试，确保实际运算结果与预期的正确结果相符。

开发者应确保使用符合国家密码相关规定的对称、非对称和杂凑密码算法。

6.4.3.4.6 代码安全性测试

开发者应对 SSOOS 实现表示和操作系统内核代码进行安全性测试，证实代码中不存在安全缺陷或后门。

6.4.3.5 脆弱性评定

开发者应从以下方面对操作系统进行脆弱性评定：

a) 基于已标识的潜在脆弱性，操作系统应抵抗具有**中等**攻击潜力的攻击者的攻击。

b) **通过一般性的隐蔽信道分析，对隐蔽信道进行非形式化搜索，标识出可识别的隐蔽存储信道，并以文档形式描述：**

   1) **标识隐蔽信道，并估算它们的带宽；**

   2) **用于确定隐蔽信道存在的过程，以及进行隐蔽信道分析所需要的信息；**

   3) **隐蔽信道分析期间所作的全部假设；**

   4) **最坏情况下对隐蔽信道带宽进行估算的方式；**

   5) **每个可标识隐蔽信道的最大可利用情形；**

   6) **用封锁、限制带宽或审计等措施，对所标识的隐蔽信道进行处理，并证明处理措施的有效性。**

注： 抵抗**中等**攻击潜力的攻击者的攻击，需要根据以下 5 个具体因素综合考虑：攻击时间、攻击者能力、对操作系统的了解程度、访问操作系统时间或攻击样品数量、使用的攻击设备，见 GB/T 30270—2013 附录 A 中的 A.8。

6.5 第五级：访问验证保护级

6.5.1 安全功能要求

6.5.1.1 身份鉴别

SSOOS 的身份鉴别功能如下：

a) 用户标识功能：

   1) 用户进入操作系统前，应先进行标识；

   2) 操作系统用户标识应使用用户名和 UID，并在操作系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID 等之间的一致性。

b) 用户鉴别功能：

   1) 采用强化管理的口令鉴别和/或生物特征鉴别和/或数字证书鉴别**和/或以协议形式化分析为基础的鉴别**等相结合的方式，使用多鉴别机制实现对用户身份的真实性鉴别，并在每

次用户登录系统时和系统重新连接时进行鉴别；

2） 鉴别信息应是不可见的，在存储和传输时进行安全保护，确保其不被非授权的访问、修改和删除；

3） 通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时采取的措施来实现鉴别失败的处理。

c） 对注册到操作系统的用户，应将用户进程与其所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户。

6.5.1.2 自主访问控制

SSOOS 的自主访问控制功能如下：

a） 客体的拥有者对其拥有的全部客体应有权修改其访问权限；

b） 客体的拥有者应能对其拥有的客体设置其他用户的访问控制属性，访问控制属性至少包括：读、写、执行等；

c） 主体对客体的访问应遵循该客体的自主访问控制权限属性；

d） 有更细颗粒度的自主访问控制，将访问控制主体的颗粒度控制在单个用户，将访问控制客体的颗粒度控制在文件和目录；

e） 当主体生成一个客体时，该客体应具有该主体设置的自主访问控制权限属性的默认值；

f） 自主访问控制应能与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种访问，使用户对自己的行为承担明确的责任；

g） 客体的拥有者应能对其拥有的客体设置为：拥有者是唯一有权修改其访问权限的主体；

h） 不准许客体拥有者把客体的控制权分配给其他主体。

6.5.1.3 标记和强制访问控制

SSOOS 的标记和强制访问控制功能如下：

a） 采用标记的方法为操作系统所有主体和客体（包括系统所有的进程、文件、目录等）标明其安全属性。

b） 客体的标记应和客体数据紧密结合，当信息从操作系统控制范围之内向控制范围之外输出时，带有安全标记；当信息从操作系统控制范围之外向控制范围之内输入时，通过标记标明其安全属性。如打印输出的数据，需明显标示出该数据的安全标记。

c） 主体和客体的安全属性标记构成了机密性和完整性安全策略模型，这些安全策略模型具有相应的**形式化证明**。强制访问控制应基于标记和安全策略模型，实现主体对客体读、写和执行等操作的访问控制。

d） 强制访问控制应与用户身份鉴别、标记等安全功能紧密结合，使系统对用户的安全控制包含从系统启动到退出系统的全过程，强制访问控制对客体的控制范围涉及操作系统内部的存储、处理和传输过程及信息进行输入、输出操作的过程。

e） 将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，按职能分割和最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，并形成相互制约关系。由系统安全员统一管理操作系统中与强制访问控制等安全机制有关的事件和信息。

f） 运行于网络环境的多台计算机上的网络操作系统，在需要进行统一管理时，应考虑各台计算机操作系统中主、客体安全属性设置的一致性，并实现跨网络的操作系统间用户数据保密性和完整性保护。

6.5.1.4 安全审计

SSOOS的安全审计功能如下：

a) 应能对以下事件生成审计日志：
   1) 身份鉴别、自主访问控制、标记和强制访问控制等安全功能的使用；
   2) 创建、删除客体的操作；
   3) 网络会话；
   4) 所有管理员的操作。

b) 审计记录要求如下：
   1) 每条审计记录应包括：事件类型、事件发生的日期和时间、触发事件的用户、事件成功或失败等字段；
   2) 身份标识和鉴别事件类审计记录还应包括请求的源(如末端号或网络地址)；
   3) 创建和删除客体的事件审计记录还应包括客体的名字、客体的安全属性；
   4) 网络会话事件审计记录还应包括：网络程序名称、协议类型、源IP地址、目的IP地址、源端口、目的端口、会话总字节数等字段。

c) 应提供审计日志分析功能：
   1) 潜在侵害分析：设置审计日志累积或组合的规则，使用这些规则去监测已经生成的审计事件，并根据这些规则指示出对系统安全运行的潜在侵害；
   2) 基于模板的异常检测：根据用户的历史使用模式建立模板，用置疑等级表示用户当前活动与模板中已建立的使用模式不一致的程度，当用户的置疑等级超过门限条件时，能指出对操作系统的可能侵害即将发生；
   3) 简单攻击探测：当发现一个系统事件与一个潜在违反系统安全策略的特征事件匹配时，能指出潜在违反系统安全策略的事件即将发生；
   4) **复杂攻击探测：维持一个已知入侵情景的事件序列和潜在违反系统安全策略的特征事件的列表，并对照特征事件和事件序列比对系统活动记录。当发现一个系统活动与特征事件或事件序列匹配时，应能指出潜在违反系统安全策略的事件即将发生。**

d) 当检测到潜在的安全侵害时，应生成实时报警，并终止违例进程、**取消服务、断开和锁定用户账户**。

e) 应提供审计日志的可选择查询功能，支持按以下条件之一或逻辑组合进行选择和排序查阅，并能导出查询结果：
   1) 事件类型；
   2) 日期和/或时间；
   3) 用户身份；
   4) 客体名称；
   5) 成功或失败。

f) 应提供审计日志的保护功能：
   1) 保证审计机制默认处于开启状态，且对审计日志的开启和关闭进行保护；
   2) 保护审计日志不被未授权的访问；
   3) 保证审计日志不被篡改和删除，并记录尝试篡改和删除审计日志的行为。**能恢复被篡改和删除的审计日志。**

g) 应以便于用户理解的方式提供审计日志查阅功能。

h) 审计日志应存储在掉电非遗失性存储媒体中。系统管理员应能定义超过审计跟踪存储极限的阈值，当超过阈值时将向管理员报警。当审计存储空间被耗尽时，覆盖所存储的最早的审计

记录。

6.5.1.5 数据完整性

SSOOS 的数据完整性保护功能如下：

a) 在操作系统内部进行的数据传输（如进程间的通信），应具备保证数据完整的功能；
b) 在对数据进行访问操作时，应检查存储在存储媒体上的用户数据是否完整，并在检查到不完整时进行恢复；
c) 应提供一个实用程序来校验文件系统和磁盘的完整性。此实用程序应可由操作系统自动执行。

6.5.1.6 数据保密性

6.5.1.6.1 客体重用

SSOOS 的客体重用功能如下：

a) 确保非授权用户不能查找使用后返还系统的存储媒体（至少包括：磁盘和内存等）中的信息；
b) 确保非授权用户不能查找系统现已分配给它的存储媒体（至少包括：磁盘和内存等）中以前的信息。

6.5.1.6.2 数据加密

SSOOS 的数据加密功能如下：

a) 应提供文件加密功能，用户可对指定的文件和目录进行加密保护；
b) 应对密钥提供基于硬件信任根的可信存储支持；
c) 应提供文件系统加密功能，对存储在加密文件系统中的文件和目录，进行透明加解密。

6.5.1.7 可信路径

在本地用户和远程用户进行初始登录和/或鉴别时，操作系统应在它与用户之间建立一条安全的通信路径。此路径对其端点进行了可信标识，并能保护鉴别通信数据免遭修改、泄露。

6.5.1.8 可信信道

应在操作系统和另一个可信操作系统之间提供一条通信信道，此信道在逻辑上与其他通信信道隔离，对其端点进行了可信标识，并能保护通信数据免遭修改、泄露。

6.5.1.9 网络安全保护

SSOOS 的网络安全保护功能如下：

a) 支持基于 IP 地址、端口、物理接口和应用程序的双向网络访问控制，将不符合预先设定策略的数据包丢弃；
b) 对网络传输数据应能进行加密与完整性保护；
c) 支持基于系统身份、系统运行状态的双向网络可信接入认证；
d) 应对网络访问进行控制，只有被授权的且通过可信度量的进程才能访问网络。

6.5.2 自身安全要求

6.5.2.1 运行安全保护

SSF 运行安全保护功能如下：

a) 应提供一个设置和升级配置参数的安装机制。在初始化和对与安全有关的数据结构进行保护之前，对用户和管理员的安全策略属性进行定义。
b) 应区分普通操作模式和系统维护模式。
c) 在普通用户访问系统之前，系统应以一个安全的方式进行安装和配置。
d) 对备份等不影响 SSOOS 的常规的系统维护，可在普通操作模式执行。
e) 当操作系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、根目录、审计参数、系统审计跟踪设置以及对文件和目录的合适的访问控制。
f) 仅允许系统管理员修改或替换系统提供的可执行程序。
g) 应为操作系统安全管理人员提供一种机制，来产生安全参数值的详细报告。
h) **应在确定不减弱保护的情况下启动 SSOOS，并在 SSF 运行中断后能在不减弱 SSOOS 安全策略保护的情况下以手动或自动方式恢复运行**。在 SSOOS 出现故障或中断后，应使其以最小的损害得到恢复，并按 GB/T 20271—2006 中 5.1.2.2 失败保护所描述的内容，处理 SSF 故障。系统因故障或其他原因中断后，应启动系统恢复机制。
i) 应控制和审计系统控制台的使用。
j) 操作系统的开发者应针对发现的漏洞及时发布补丁。操作系统的管理者应及时获取、统一管理并及时运用补丁对操作系统的漏洞进行修补。

6.5.2.2 资源利用

6.5.2.2.1 容错

SSOOS 的容错功能如下：

a) 应通过一定措施确保当系统出现某些确定的故障情况时，SSF 也能维持正常运行，如系统检测和报告系统的服务水平已降低到预先规定的最小值。
b) 当系统资源的服务水平降低到预先规定的最小值时，应能检测和发出报告。
c) 应提供维护模式中运行系统的能力，在维护模式下各种安全功能全部失效，系统仅允许系统管理员进入维护模式。
d) 系统应提供软件及数据备份和恢复的过程，在系统中加入再启动的同步点，以便于系统的恢复。
e) 系统应提供能用于定期确认系统正确操作的机制和过程，这些机制或过程涉及系统资源的监视、硬件和固件单元的正确操作、对可能在全系统内传播的错误状态的检测以及超过用户规定门限的通信差错的检测等内容。

6.5.2.2.2 服务优先级

SSOOS 的服务优先级功能如下：

a) 应采取服务优先级策略，设置主体使用 SSF 控制范围内某个资源子集的优先级，进行操作系统资源的管理和分配；
b) 应确保对所有操作系统资源的访问都基于主体所设置的优先级进行。

6.5.2.2.3 资源分配

SSOOS 的资源分配功能如下：

a) 应按 GB/T 20271—2006 中 5.1.4.2 a)最大限额资源分配的要求，进行操作系统资源的管理和分配。配额机制确保用户和主体将不会独占某种受控的资源。
b) 应确保在被授权的主体发出请求时，资源能被访问和利用。

c) 应以每个用户或每个用户组为基础，提供一种机制，控制其对磁盘的消耗和对 CPU 等资源的使用。
d) 应提供用户查看可访问系统资源的修改历史记录的权限。

6.5.2.3 用户登录访问控制

SSOOS 的用户登录访问控制功能如下：
a) 应按 GB/T 20271—2006 中 5.1.5 a)会话建立机制的要求，根据访问地址或端口，允许或拒绝用户的登录。鉴别机制不准许被旁路。
b) 应按 GB/T 20271—2006 中 5.1.5 c)多重并发会话限定的要求，限制系统并发会话的最大数量，并利用默认值作为会话次数的限定数。
c) 成功登录系统后，操作系统应记录并向用户显示以下数据：
   1) 本次登录的日期、时间、来源和上次成功登录系统的情况；
   2) 上次成功访问系统以来身份鉴别失败的情况；
   3) 口令到期的天数；
   4) 成功或不成功的事件次数可以用整数计数、时间戳列表等表述方法。
d) 在规定的未使用时限后，系统应断开会话或重新鉴别用户。系统提供时限的默认值。
e) 系统应提供锁定用户键盘的机制，键盘开锁过程要求鉴别用户。
f) 当用户鉴别过程不正确的次数达到系统规定的次数时，系统应退出登录过程。
g) 系统应提供一种机制，按时间、进入方式、地点、网络地址或端口等条件规定哪些用户能进入系统。

6.5.2.4 可信度量

SSOOS 的可信度量功能如下：
a) 在操作系统启动时应对操作系统内核进行完整性度量；
b) 在可执行程序启动时应进行完整性度量；
c) 应对完整性度量基准值进行可信存储，防止其被篡改；
d) 支持硬件可信芯片作为信任根。

6.5.2.5 可信恢复

当系统失效或服务中断时，应确保操作系统能够在不丢失用户数据的情况下自动恢复到安全运行状态。

6.5.2.6 安全策略配置

应对身份鉴别、标记和强制访问控制、安全审计、可信路径、可信信道、网络安全保护、资源利用、用户登录访问控制提供安全策略配置功能。

6.5.3 安全保障要求

6.5.3.1 开发

6.5.3.1.1 安全架构

开发者应提供 SSOOS 的安全架构描述文档，安全架构描述文档应符合以下要求：
a) 与 SSOOS 设计文档中对安全功能要求和自身安全保护要求的描述一致；
b) 描述 SSOOS 的安全域；

c) 描述 SSOOS 初始化过程为何是安全的；
d) 证实 SSOOS 能够防止被破坏；
e) 证实 SSOOS 能够防止被旁路。

6.5.3.1.2 功能规范说明

开发者应提供功能规范说明，功能规范说明应符合以下要求：
a) 完全描述 SSF 和自身安全保护；
b) 使用半形式化方式描述 SSOOS 接口；
c) 描述所有 SSOOS 接口的目的与使用方法；
d) 标识和描述每个 SSOOS 接口相关的全部参数；
e) 描述实施过程中，与 SSOOS 接口相关的所有行为；
f) 描述可能由每个 SSOOS 接口的调用而引起的所有直接错误消息；
g) 证实安全功能要求和自身安全保护要求到 SSOOS 接口的追溯。

6.5.3.1.3 实现表示

开发者应提供实现表示说明，并在自身选择的场所内提供 SSOOS 的全部实现表示，实现表示及说明应符合以下要求：
a) 应详细定义 SSF 和自身安全保护，详细程度达到无需进一步设计就能生成 SSOOS；
a) 实现表示以开发人员使用的形式提供；
b) 在实现表示说明中提供 SSOOS 设计描述与**全部**实现表示之间的映射，并证明其一致性。

6.5.3.1.4 SSOOS 设计

开发者应提供 SSOOS 设计文档，SSOOS 设计文档应符合以下要求：
a) 描述 SSOOS 的结构；
b) 提供每一个安全功能和自身安全保护的半形式化描述，适当时配以非形式化的、解释性的描述；
c) 描述安全功能和自身安全保护间的相互作用；
d) 提供安全功能和自身安全保护到模块间的映射关系；
e) 根据模块描述安全功能和自身安全保护；
f) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的 SSOOS 接口；
g) **为每一个模块提供一个半形式化描述，包括它的目的、相互作用、接口、其他接口的返回值、被其他模块调用的接口，适当时配以非形式化的、解释性的描述。**

6.5.3.1.5 SSOOS 内部结构

开发者应提供 SSOOS 内部结构的描述和论证过程文档，SSOOS 内部结构文档应符合以下要求：
a) 论证过程文档用于判定“结构合理”**及复杂性**的特性；
b) SSOOS 内部结构描述证实指定的整个 SSOOS 内部结构合理**且不过于复杂**。

6.5.3.1.6 安全策略模型

开发者应提供形式化的安全策略模型，至少包括：强制访问控制策略、完整性策略，安全策略模型应符合以下要求：
a) **模型是形式化的，必要时辅以解释性的文字，并且标识模型化的安全策略；**
b) **对于所有被模型化的策略，模型定义操作系统的安全，提供操作系统不能达到非安全状态的形**

式化证明；

c) 该模型与功能规范说明的一致性采用正确的形式化级别进行论述；

d) 该对应性表明功能规范说明相对该模型是一致的和完备的；

e) 该对应性论证表明功能规范说明中描述的接口相对于强制访问控制策略、完整性策略是一致的和完备的。

6.5.3.2 指导性文档

6.5.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应符合以下要求：

a) 描述在安全处理环境中用户可访问的功能和特权，并包含可能造成危害的警示信息；

b) 描述如何以安全的方式使用 SSOOS 提供的安全功能和自身安全保护；

c) 描述安全功能和自身安全保护及接口，尤其是受用户控制的所有安全参数，适当时指明安全值；

d) 明确说明安全功能和自身安全保护有关的每一种安全相关事件，包括改变 SSOOS 所控制实体的安全特性；

e) 标识 SSOOS 运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；

f) 描述为确保 SSOOS 安全运行应执行的安全策略。

6.5.3.2.2 准备程序

开发者应提供操作系统及其准备程序，准备程序描述应符合以下要求：

a) 描述与开发者交付程序相一致的安全接收操作系统必需的所有步骤；

b) 描述安全安装操作系统及其运行环境必需的所有步骤。

6.5.3.3 生存周期支持

6.5.3.3.1 配置管理能力

开发者的配置管理能力应符合以下要求：

a) 为操作系统的不同版本提供唯一的标识；

b) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；

c) 配置管理系统唯一标识所有配置项，并对组成 SSOOS 的所有配置项进行维护；

d) 提供自动化的措施使得仅能对配置项进行授权变更；

e) 配置管理系统提供一种自动方式来支持 SSOOS 的生成；

f) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发 SSOOS；

g) 实施的配置管理与配置管理计划相一致；

h) 配置管理计划描述用来接受修改过的或新建的作为 SSOOS 组成部分的配置项的程序；

i) 配置项接受程序对所有配置项的变更提供了充分的复查；

j) 配置管理系统确保接受某个配置项的人不是开发此配置项的人；

k) 配置管理系统以自动化的方式支持所有变化的审计，审计记录中要包括源发者、日期和时间等信息；

l) 配置管理系统提供自动化的方式标识受已给定配置项的变化影响的所有其他配置项；

m） **配置管理系统能标识用于生成 SSOOS 实现表示的版本**。

6.5.3.3.2 配置管理范围

开发者应提供 SSOOS 配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a） SSOOS、安全保障要求的评估证据和 SSOOS 的组成部分和实现表示、安全缺陷报告及其解决状态、开发工具及其相关信息；

b） 唯一标识配置项；

c） 对于每一个安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

6.5.3.3.3 交付程序

开发者应使用一定的交付程序交付操作系统，并将交付过程文档化。在给用户方交付指定版本操作系统时，交付文档应描述为维护安全所必需的所有程序。

6.5.3.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在 SSOOS 的开发环境中，为保护 SSOOS 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。**开发安全文档应论证安全措施提供了必需的保护级别以维护 SSOOS 的机密性和完整性**。

6.5.3.3.5 生存周期定义

开发者应建立一个生存周期模型对 SSOOS 的开发和维护进行的必要控制，并提供生存周期定义文档描述用于开发和维护 SSOOS 的模型。

6.5.3.3.6 工具和技术

应描述开发者**和 SSOOS 的第三方开发商**所使用的实现标准。开发者应明确定义用于开发 SSOOS 的工具，并提供开发工具文档。开发工具文档应无歧义地定义所有语句和实现用到的所有协定与命令的含义，应无歧义地定义所有实现依赖选项的含义。

6.5.3.4 测试

6.5.3.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖文档应符合以下要求：

a） 证实测试文档中的测试与功能规范说明中 SSOOS 接口之间的对应性；

b） 证实已经对功能规范说明中的所有 SSOOS 接口都进行了**完全地**测试。

6.5.3.4.2 深度

开发者应提供测试深度的分析文档。测试深度分析文档应符合以下要求：

a） 证实测试文档中的测试与 SSOOS 设计中的安全功能和自身安全保护模块之间的对应性；

b） 证实已经测试了 SSOOS 设计中的所有安全功能模块和自身安全保护功能模块。

6.5.3.4.3 功能测试

开发者应测试 SSF 和自身安全保护功能。测试文档应包括以下内容：

a） 测试计划：标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b） 预期的测试结果：表明测试完成后的预期输出；
c） 实际测试结果：和预期的测试结果一致；
d） 证实已知的漏洞被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞；
e） **测试步骤顺序依赖性的一个分析**。

6.5.3.4.4 独立测试

开发者应提供一组与其自测时使用的同等资源，以用于 SSOOS 的测试。

6.5.3.4.5 密码测试

开发者应对所使用的对称、非对称和杂凑密码算法进行正确性和符合性测试，确保实际运算结果与预期的正确结果相符。

开发者应确保使用符合国家密码相关规定的对称、非对称和杂凑密码算法。

6.5.3.4.6 代码安全性测试

开发者应对 SSOOS 实现表示和操作系统内核代码进行安全性测试，证实代码中不存在安全缺陷或后门。

6.5.3.5 脆弱性评定

开发者应从以下方面对操作系统进行脆弱性评定：

a） 基于已标识的潜在脆弱性，操作系统应抵抗具有**高等**攻击潜力的攻击者的攻击。
b） 通过**严格的**隐蔽信道分析，对隐蔽信道进行**严格搜索，以结构化、可重复的方式**标识出可识别的隐蔽存储信道和**隐蔽时间信道**，并以文档形式描述：
   1） 标识隐蔽信道，并估算它们的带宽；
   2） 用于确定隐蔽信道存在的过程，以及进行隐蔽信道分析所需要的信息；
   3） 隐蔽信道分析期间所作的全部假设；
   4） 最坏情况下对隐蔽信道带宽进行估算的方式；
   5） 每个可标识隐蔽信道的最大可利用情形；
   6） 用封锁、限制带宽或审计等措施，对所标识的隐蔽信道进行处理，并证明处理措施的有效性。

注：抵抗**高等**攻击潜力的攻击者的攻击，需要根据以下 5 个具体因素综合考虑：攻击时间、攻击者能力、对操作系统的了解程度、访问操作系统时间或攻击样品数量、使用的攻击设备，见 GB/T 30270—2013 附录 A 中的 A.8。

附 录 A
（资料性附录）
操作系统安全技术要求分级表

表 1 以表格形式列举了操作系统五个安全等级的相关技术要求。

表 A.1 操作系统安全技术要求分级

安全技术要求		第一级	第二级	第三级	第四级	第五级
安全功能要求	身份鉴别	*	+	++	+++	++++
	自主访问控制	*	+	++	++	++
	标记和强制访问控制	—	—	*	+	++
	安全审计	—	*	+	++	+++
	数据完整性	*	+	+	++	++
	数据保密性	—	*	+	++	++
	可信路径	—	—	—	*	*
	可信信道	—	—	—	*	*
	网络安全保护	*	+	++	+++	+++
自身安全要求	运行安全保护	*	+	++	++	+++
	资源利用	*	+	++	++	++
	用户登录访问控制	*	+	++	++	++
	可信度量	—	*	+	+	+
	可信恢复	—	—	—	*	+
	安全策略配置	*	+	++	+++	+++
安全保障要求	开发	*	*	+	++	+++
	指导性文档	*	*	*	*	*
	生存周期支持	*	+	++	+++	++++
	测试	*	+	++	++	+++
	脆弱性评定	*	*	+	++	+++

注：“*”表示具有该项要求；“—”表示不具有该项要求；一个或多个“+”表示具有更高的要求。

参 考 文 献

[1] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型

[2] GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第2部分:安全功能组件

[3] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[4] GB/T 29827—2013 信息安全技术 可信计算规范 可信平台主板功能接口

[5] GB/T 29828—2013 信息安全技术 可信计算规范 可信连接架构

[6] GB/T 29829—2013 信息安全技术 可信计算密码支撑平台功能与接口规范

[7] GB/T 30270—2013 信息技术 安全技术 信息技术安全性评估方法

[8] Common Methodology for Information Technology Security Evaluation(CCMB-2012-09-004, Version 3.1 Revision 4)