ICS 35.020
L 09

GA

中华人民共和国公共安全行业标准

GA/T 390—2002

计算机信息系统安全等级保护通用技术要求

Common technology requirement in computer information system classified security protection

2002-07-15 发布　　2002-07-15 实施

中华人民共和国公安部　发布

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，包括：

——计算机信息系统安全等级保护技术要求系列标准；

——计算机信息系统安全等级保护管理要求；

——计算机信息系统安全等级保护工程实施要求；

——计算机信息系统安全等级保护评测系列标准。

其中，计算机信息系统安全等级保护技术要求系列标准由以下标准和其他相关标准组成：

GA/T 390—2002　计算机信息系统安全等级保护通用技术要求；

GA/T 387—2002　计算机信息系统安全等级保护网络技术要求；

GA/T 388—2002　计算机信息系统安全等级保护操作系统技术要求；

GA/T 389—2002　计算机信息系统安全等级保护数据库管理系统技术要求；

本标准是计算机信息系统安全等级保护技术要求系列标准中的第1项。

本标准的附录A是资料性附录。

本标准由中华人民共和国公安部公共信息网络安全监察局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：江南计算技术研究所。

本标准主要起草人：吉增瑞、景乾元、熊　辉、徐良华、刘广明、汪晓茵、陆　晔、孙　炜。

引　言

本标准是计算机信息系统安全等级保护技术要求系列标准的基础性标准，用以指导设计者如何设计和实现具有所需要的安全等级的计算机信息系统，主要从对计算机信息系统的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现GB 17859—1999中每一个保护等级的安全要求应采取的安全技术措施，以及各安全技术要求在不同安全等级中具体实现上的差异。

本标准首先对计算机信息系统安全等级保护所涉及的安全功能技术要求和安全保证技术要求做了比较全面的描述，然后按GB 17859—1999五个安全等级的划分，对每一个安全等级的安全功能技术要求和安全保证技术要求做了详细描述。本标准中有关概念的说明见附录A。本标准参考的主要文件已列在参考文献中。

计算机信息系统安全等级保护通用技术要求

1 范围

本标准规定了对计算机信息系统进行安全等级保护所需要的通用技术要求，并给出了每一个安全保护等级的不同技术要求。

本标准适用于按 GB 17859—1999 的安全保护等级要求所进行的计算机信息系统的设计和实现，对于按 GB 17859—1999 的要求对计算机信息系统进行的测试、管理也可参照使用。

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 J45—1982 高层民用建筑设计防火规定

GBJ 16—1987 建筑设计防火规范

3 术语和定义

GB 17859—1999 确立的以及下列术语和定义适用于本标准。

3.1

安全要素 security element

GB 17859—1999 各安全等级所包含的安全内容的组成成份。

注：GB 17859—1999 有 10 个安全要素。每个安全要素在不同的安全等级中可有不同的具体内容。

3.2

安全功能策略(SFP) security function policy

为实现安全要素所要求的功能，所采用的安全策略。

3.3

安全功能 security function

为实现安全要素的内容，正确实施相应安全功能策略所提供的功能。

3.4

安全保证 security assurance

为确保安全要素的安全功能达到要求的安全性目标所采取的方法和措施。

3.5

可信计算基(TCB) trusted computing base

计算机信息系统中保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境，并提供一个可信计算系统所要求的附加服务。

3.6

TCB 安全策略(TSP) TCB security policy

对 TCB 中的资源进行管理、保护和分配的一组规则。一个 TCB 中可以有一个或多个安全策略。

3.7

TCB 安全功能(TSF)　TCB security function-TSF

正确实施 TCB 安全策略的全部硬件、固件、软件所提供的功能。每一个安全策略的实现,组成一个安全功能模块。一个 TCB 的所有安全功能模块共同组成该 TCB 的安全功能。

3.8

TSF 控制范围(TSC)　TSF scope of control

TCB 的操作所涉及的主体和客体。

3.9

用户标识　user identification

用来标明用户的身份,确保用户在系统中的唯一性和可辨认性,一般用名称和用户标识符(UID)来标明系统中的一个用户。名称和标识都是公开的明码信息。

3.10

用户鉴别　user authentication

用特定信息对用户身份的真实性进行确认。用于鉴别的信息一般是非公开的、难以仿造的。

3.11

用户-主体绑定　user-subject binding

用一定方法将指定用户与为其服务的主体(如进程)相关联。

3.12

主、客体标记　label of subject and object

为主、客体指定敏感标记。这些敏感标记是等级分类和非等级类别的组合,是实施强制访问控制的依据。

3.13

安全属性　security attribute

用于实施安全策略,与主体、客体相关的信息。对于自主访问控制,安全属性包括确定主、客体访问关系的相关信息;对于采用多级安全策略模型的强制访问控制,安全属性包括主、客体的标识信息和安全标记信息。

3.14

回退　rollback

由于某种原因而撤销上一次/一系列操作,并返回到该操作以前的已知状态的过程。

3.15

可信信道　trusted channel

为了执行关键的安全操作,在 TSF 与其他可信 IT 产品之间建立和维护的保护通信数据免遭修改和泄露的通信路径。

3.16

可信路径　trusted path

为实现用户与 TSF 之间的可信通信,在 TSF 与用户之间建立和维护的保护通信数据免遭修改和泄露的通信路径。

3.17

故障容错　fault tolerance

通过一系列故障处理措施,确保故障情况下 TCB 所提供的安全功能的有效性和可用性。

3.18

服务优先级　priority of service

通过对资源使用的有限控制策略,确保 TCB 中高优先级任务的完成不受低优先级任务的干扰和延

误，从而确保 TCB 安全功能的安全性；

3.19

资源分配　resource allocation

通过对 TCB 安全功能控制范围内资源的合理管理和调度，确保 TCB 的安全功能不因资源使用方面的原因而受到影响。

3.20

配置管理(CM)　configuration management

一种建立功能要求和规范的方法。该功能要求和规范是在 TCB 的执行中实现的。

3.21

配置管理系统(CMS)　configuration management system

通过提供追踪任何变化，以及确保所有修改都已授权的方法，确保 TCB 各部分的完整性。

3.22

保护框架(PP)　protection profile

详细说明计算机信息系统安全保护需求的文档，即通常的安全需求，一般由用户负责编写。

3.23

安全目标(ST)　security target

阐述计算机信息系统安全功能及信任度的文档，即通常的安全方案，一般由开发者编写。

3.24

TCB 安全管理　TCB security management

是指对与 TCB 安全相关方面的管理，包括对不同的管理角色和它们之间的相互作用(如能力的分离)进行规定，对分散在多个物理上分离的部件有关敏感标记的传播、TSF 数据和功能的修改等问题的处理。

4　安全功能技术要求

4.1　物理安全

4.1.1　环境安全

4.1.1.1　中心机房的安全保护

4.1.1.1.1　机房场地选择

a)　基本要求：按一般建筑物的要求进行机房场地选择。

b)　防火要求：避开易发生火灾和危险程度高的地区，如油库和其他易燃物附近的区域。

c)　防污染要求：避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域。

d)　防潮及防雷要求：避开低洼、潮湿及落雷区域。

e)　防震动和噪声要求：避开强震动源和强噪声源区域。

f)　防强电场、磁场要求：避开强电场和强磁场区域。

g)　防地震、水灾要求：避开有地震、水灾危害的区域。

h)　位置要求：避免在建筑物的高层以及用水设备的下层或隔壁。

i)　防公众干扰要求：避免靠近公共区域，如运输邮件通道、停车场或餐厅等。

4.1.1.1.2　机房内部安全防护

a)　机房出入：机房应只设一个出入口，并有专人负责，未经允许的人员不准进入机房；另设若干紧急疏散出口，标明疏散线路和方向。

b)　机房物品：没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，磁铁、私人电子计算机或电设备、食品及饮料、香烟、吸烟用具等均不准带入机房。

c)　机房人员：获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同。

d） 机房分区：机房内部应分区管理，一般分为主机区、数据处理操作区、辅助区等，应根据每个工作人员的实际工作需要，确定其能进入的区域。

e） 安全管理中心：在机房中设有信息系统安全管理中心的，更应加强其安全防护，如进入不同区域时佩带有不同标记的证章，重要部位的出、入口设置电子锁、指纹锁等，必要时可设置摄像监视系统。

4.1.1.1.3 机房防火

a） 建筑材料防火①：要求机房和记录介质存放间，其建筑材料的耐火等级，应符合 GBJ 16—1987 中规定的二级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 GBJ 16—1987 中规定的三级耐火等级。

b） 建筑材料防火②：要求机房和重要的记录介质存放间，其建筑材料的耐火等级，应符合 GB J45—1982中规定的二级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 GBJ 16—1987 中规定的二级耐火等级。

c） 建筑材料防火③：要求机房和重要的记录介质存放间，其建筑材料的耐火等级，应符合 GB J45—1982中规定的一级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 GBJ 16—1987 中规定的二级耐火等级。

d） 报警和灭火系统①：要求设置火灾报警系统，由人来操作灭火设备，并对灭火设备的效率、毒性、用量和损害性有一定的要求。

e） 报警和灭火系统②：要求设置火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等，能对火灾发生的部位以声、光或电的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等。

f） 报警和灭火系统③：要求设置火灾自动消防系统，能自动检测火情、自动报警，并自动切断电源和其他应急开关，自动启动事先固定安装好的灭火设备进行自动灭火。

g） 区域隔离防火：要求机房布局要将脆弱区和危险区进行隔离，防止外部火灾进入机房，特别是重要设备地区，安装防火门、使用阻燃材料装修等。

4.1.1.1.4 机房供、配电

a） 分开供电：机房供电系统应将计算机系统供电与其他供电分开，并配备应急照明装置。

b） 紧急供电①：应配置抵抗电压不足的设备，如基本的 UPS。

c） 紧急供电②：应配置抵抗电压不足的设备，包括基本的 UPS、改进 UPS、多级 UPS。

d） 紧急供电③：应配置抵抗电压不足的设备，包括基本的 UPS、改进的 UPS、多级 UPS 和应急电源（发电机组）等。

e） 备用供电：建立备用的供电系统，以备常用供电系统停电时启用，完成运行系统必要的保留。

f） 稳压供电：采用线路稳压器，防止电压波动对计算机系统的影响。

g） 电源保护：设置电源保护装置，如金属氧化物可变电阻、硅雪崩二极管、气体放电管、滤波器、电压调整变压器和浪涌滤波器等。

h） 不间断供电：采用不间断供电电源，防止电压波动、电器干扰、断电等对计算机系统的影响。

i） 电器噪声防护：采用有效措施，减少机房中电器噪声干扰，保证计算机系统正常运行。

j） 突然事件防护：防止供电中断、异常状态供电（指连续电压过载或低电压）、电压瞬变、噪声（电磁干扰）以及由于雷击等引起的设备突然失效事件。

4.1.1.1.5 机房空调、降温

a） 基本温度要求：应有必要的空调设备，使机房温度达到所需的温度要求。

b） 较完备空调系统：应有较完备的中央空调系统，保证机房温度的变化在计算机运行所允许的范围。

c） 完备空调系统：应有完备的中央空调系统，保证机房各个区域的温度变化能满足计算机运行、

人员活动和其他辅助设备的要求。

4.1.1.1.6 机房防水与防潮

a) 水管安装要求：水管安装，不得穿过屋顶和活动地板下，穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施。

b) 水害防护：采取一定措施，防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。

c) 防水检测：安装对水敏感的检测仪表或元件，对机房进行防水检测、报警。

d) 排水要求：机房应设有排水口，并购置水泵，以便迅速排出积水。

4.1.1.1.7 机房防静电

a) 接地与屏蔽：应采用必要的接地与屏蔽措施，使计算机系统有一套合理的接地与屏蔽系统。

b) 服装防静电：人员服装采用不易产生静电的衣料，工作鞋选用低阻值材料制作。

c) 温、湿度防静电：控制机房温湿度，使其保持在不易产生静电的范围内。

d) 地板防静电：机房地板从地板表面到接地系统的阻值，应保证防人身触电和产生静电。

e) 材料防静电：机房中使用的各种家具，工作台、柜等，应选择产生静电小的材料。

f) 维修 MOS 电路保护：在硬件维修时，应采用金属板台面的专用维修台，以保护 MOS 电路。

g) 静电消除要求：在机房中使用静电消除剂和静电消除器等，以进一步减少静电的产生。

4.1.1.1.8 机房接地与防雷击

a) 接地要求：应采用地桩、水平栅网、金属板、建筑物基础钢筋构建接地系统等，确保接地体良好的接地。

b) 去耦、滤波要求：应设置信号地与直流电源地，应注意不造成额外耦合，保障去耦、滤波等的良好效果。

c) 避雷要求：应设置避雷地，应以深埋地下、与大地良好相通的金属板作为接地点，至避雷针的引线则应采用粗大的紫铜条，或者使整个建筑的钢筋自地基以下焊连成钢筋网作为“大地”与避雷针相连。

d) 防护地与屏蔽地要求：应设置安全防护地与屏蔽地，应采用阻抗尽可能小的良导体的粗线，以减小各种地之间的电位差，应采用焊接方法，并经常检查接地的良好，检测接地电阻，确保人身、设备和运行的安全。

e) 交流电源地线要求：应设置交流电源地线，交流供电线应有规范连接位置的三芯线，即相线、中线和地线，并将该“地线”连通机房的地线网，以确保其安全保护作用。

4.1.1.1.9 机房电磁防护

a) 接地防干扰：应采用接地的方法防止外界电磁干扰和设备寄生耦合干扰。

b) 屏蔽防干扰：应采用屏蔽方法，减少外部电器设备对计算机的瞬间干扰。

c) 距离防干扰：应采用距离防护的方法，将计算机机房的位置选在外界电磁干扰小的地方和远离可能接收辐射信号的地方。

d) 电磁泄露发射防护：应采用必要措施，防止电磁泄露发射。

e) 介质保护：对磁带、磁盘等磁介质设备的保管存放，应注意电磁感应的影响，如使用铁制柜存放。

f) 机房屏蔽：应采用屏蔽方法，对计算机机房进行电磁屏蔽，防止外部电磁场对计算机设备的干扰，防止电磁信号的泄露。

4.1.1.2 通信线路的安全防护

a) 确保线路畅通：应采取必要措施，保证通信线路畅通。

b) 发现线路截获：应采取必要措施，发现线路截获事件并报警。

c) 及时发现线路截获：应采取必要措施，及时发现线路截获事件并报警。

d） 防止线路截获：应采取必要措施，防止线路截获事件发生。

4.1.2 设备安全

4.1.2.1 设备的防盗和防毁

a） 设备标记要求：计算机系统的设备和部件应有明显的无法除去的标记，以防更换和方便查找赃物。

b） 计算中心防盗①：计算中心应安装防盗报警装置，防止夜间从门窗进入的盗窃行为。

c） 计算中心防盗②：计算中心应利用光、电、无源红外等技术设置机房报警系统，并有专人值守，防止夜间从门窗进入的盗窃行为。

d） 计算中心防盗③：应利用闭路电视系统对计算中心的各重要部位进行监视，并有专人值守，防止夜间从门窗进入的盗窃行为。

e） 机房外部设备防盗：机房外部的设备，应采取加固防护等措施，必要时安排专人看管，以防止盗窃和破坏。

4.1.2.2 设备的安全可用

a） 基本运行支持：计算机信息系统的所有设备应提供基本的运行支持，并有必要的容错和故障恢复能力。

b） 安全可用要求：支持计算机信息系统运行的所有设备，包括计算机主机、外部设备、网络设备及其他辅助设备等均应安全可用。

c） 不间断运行要求：应提供可靠的运行支持，并通过故障容错和故障恢复等措施，支持计算机信息系统实现不间断运行。

4.1.3 记录介质安全

a） 有用数据介质保护：存放有用数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取一定措施防止被盗、被毁和受损；应该删除和销毁的有用数据，应有一定措施，防止被非法拷贝。

b） 重要数据介质保护：存放重要数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取有效措施，如建立介质库等，防止被盗、被毁和受损；应该删除和销毁的重要数据，要有严格的管理和审批手续，并采取有效措施，防止被非法拷贝。

c） 秘密数据介质保护：系统中有很高使用价值或很高秘密程度的数据，应采用加密等方法进行保护。

d） 关键数据介质保护：存放对系统运行和应用起关键作用数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取有效措施，如建立介质库、异地存放等，防止被盗、被毁和受损。关键数据应长期保存。

4.1.4 安全管理中心安全

安全管理中心的物理安全应满足以下要求：

a）管理中心设置在中心机房，以各种方式与计算机信息系统的各类安全机制相连接。

b）除了按一般的机房建设要求进行设计外，还应设置一些关卡，比如，严格的门卫制度和人员管理，必要时可安装闭路摄像监视系统。

4.2 运行安全

4.2.1 风险分析

风险分析应按以下要求进行：

a） 以系统安全运行和信息安全保护为出发点，全面分析由于物理的、系统的、管理的、人为的和自然的原因所造成的安全风险。

b） 通过对影响计算机信息系统安全运行的诸多因素的了解和分析，明确系统存在的风险，找出克服这些风险的办法。

c) 对常见的风险(如:后门/陷阱门、拒绝使用、辐射、盗用、伪造、假冒、逻辑炸弹、破坏活动、偷窃行为、搭线窃听以及计算机病毒等)进行分析,确定每类风险的程度。

d) 系统设计前和运行前应进行静态风险分析,以发现系统的潜在安全隐患。

e) 系统运行过程中应进行动态风险分析,测试、跟踪并记录其活动,以发现系统运行期的安全漏洞,并提供相应的系统脆弱性分析报告。

f) 采用风险分析工具,通过收集数据、分析数据、输出数据,确定危险的严重性等级,分析危险的可能性等方法,进行风险分析,并确定安全对策。

4.2.2 系统安全性检测分析

计算机信息系统安全性检测分析应从以下方面进行:

a) 操作系统安全性检测分析:应从操作系统的角度,以管理员身份评估文件许可、文件宿主、网络服务设置、账户设置、程序真实性以及一般的与用户相关的安全点、入侵迹象等,从而检测和分析操作系统的安全性,发现存在的安全隐患。

b) 数据库管理系统安全性检测分析:应对支持计算机信息系统运行的数据库管理系统进行安全性检测分析,要求通过扫描数据库系统中与鉴别、授权、访问控制和系统完整性设置相关的数据库管理系统特定的安全脆弱性,分析其存在的缺点和漏洞,提出补救措施。

c) 网络安全性检测分析:应采用侵袭模拟器,通过在网络设备的关键部位,用模拟侵袭的方法,自动扫描、检查并报告网络系统中存在的缺点和漏洞,提出补救措施,达到增强网络安全性的目的。

d) 防火墙安全性检测分析:应通过反复高速地逐个对防火墙和宿主系统上的数百个与安全性相关的因素进行测试,对其安全性进行检测分析,寻找其安全漏洞。

e) 电磁泄露发射检测分析:应对运行中的计算机信息系统环境进行电磁泄露发射检测,要求采用专门的检测设备,检查系统运行过程中由于电磁干扰和电磁辐射对计算机信息系统的安全性所造成的威胁,并提出补救措施。

4.2.3 网络安全监控

网络安全监控应采用以下方法:

a) 设置分布式探测器,实时监听网络数据流,监视和记录内、外部用户出入网络的相关操作,在发现违规模式和未授权访问时,报告网络安全监控中心。

b) 设置安全监控中心,对收到的来自分布式探测器的信息,根据安全策略进行分析,并作审计、报告、事件记录和报警等处理。监控中心应具有必要的远程管理功能,如对探测器实现远程参数设置、远程数据下载、远程启动等操作。安全监控中心还应具有实时响应功能,包括攻击分析和响应、误操作分析和响应、漏洞分析和响应以及漏洞形势分析和响应。

4.2.4 安全审计

4.2.4.1 安全审计的响应

安全审计 TSF 应按以下要求响应审计事件:

a) 记审计日志:当检测到可能有安全侵害事件时,将审计数据记入审计日志。

b) 实时报警生成:当检测到可能有安全侵害事件时,生成实时报警信息。

c) 违例进程终止:当检测到可能有安全侵害事件时,将违例进程终止。

d) 服务取消:当检测到可能有安全侵害事件时,取消当前的服务。

e) 用户账号断开与失效:当检测到可能有安全侵害事件时,将当前的用户账号断开,并使其失效。

4.2.4.2 安全审计数据产生

安全审计 TSF 应按以下要求产生审计数据:

a) 为下述可审计事件产生审计记录:

——审计功能的启动和关闭;

——使用身份鉴别机制；
——将客体引入用户地址空间(例如：打开文件、程序初始化)；
——删除客体；
——系统管理员、系统安全员、审计员和一般操作员所实施的操作；
——其他与系统安全有关的事件或专门定义的可审计事件。

b) 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息。

c) 对于身份鉴别事件，审计记录应包含请求的来源(例如：末端标识符)。

d) 对于客体被引入用户地址空间的事件及删除客体事件，审计记录应包含客体名及客体的安全级。

e) 将每个可审计事件与引起该事件的用户相关联。

4.2.4.3 安全审计分析

安全审计分析应包括：

a) 潜在侵害分析：应能用一系列规则去监控审计事件，并根据这些规则指出 TSP 的潜在侵害。这些规则包括：
——由已定义的可审计事件的子集所指示的潜在安全攻击的积累或组合；
——任何其他的规则。

b) 基于异常检测的描述：应维护用户所具有的质疑等级——历史使用情况，以表明该用户的现行活动与已建立的使用模式的一致性程度。当用户的质疑等级超过门限条件时，TSF 应能指出将要发生对安全性的威胁。

c) 简单攻击探测：应能检测到对 TSF 实施有重大威胁的签名事件的出现。为此，TSF 应维护指出对 TSF 侵害的签名事件的内部表示，并将检测到的系统行为记录与签名事件进行比较，当发现两者匹配时，指出一个对 TSF 的攻击即将到来。

d) 复杂攻击探测：在上述简单攻击探测的基础上，要求 TSF 应能检测到多步入侵情况，并能根据已知的事件序列模拟出完整的入侵情况，还应指出发现对 TSF 的潜在侵害的签名事件或事件序列的时间。

4.2.4.4 安全审计查阅

安全审计查阅工具应具有：

a) 审计查阅：提供从审计记录中读取信息的能力，即要求 TSF 为授权用户提供获得和解释审计信息的能力。当用户是人时，必须以人类可懂的方式表示信息；当用户是外部 IT 实体时，必须以电子方式无歧义地表示审计信息。

b) 有限审计查阅：在上述审计查阅的基础上，审计查阅工具应禁止具有读访问权限以外的用户读取审计信息。

c) 可选审计查阅：在上述有限审计查阅的基础上，审计查阅工具应具有根据准则来选择要查阅的审计数据的功能，并根据某种逻辑关系的标准提供对审计数据进行搜索、分类、排序的能力。

4.2.4.5 安全审计事件选择

应根据以下属性选择可审计事件：

a) 客体身份、用户身份、主体身份、主机身份、事件类型。

b) 作为审计选择性依据的附加属性。

4.2.4.6 安全审计事件存储

应具有以下创建并维护安全的审计踪迹记录的能力：

a) 受保护的审计踪迹存储：要求审计踪迹的存储受到应有的保护，能检测或防止对审计记录的修改。

b) 审计数据的可用性确保：要求在意外情况出现时，能检测或防止对审计记录的修改，以及在发生审计存储已满、存储失败或存储受到攻击时，确保审计记录不被破坏。

c) 审计数据可能丢失情况下的措施：要求当审计跟踪超过预定的门限时，应采取相应的措施，进行审计数据可能丢失情况的处理。

d) 防止审计数据丢失：要求在审计踪迹存储记满时，应采取相应的防止审计数据丢失的措施，可选择“忽略可审计事件”、“阻止除具有特殊权限外的其他用户产生可审计事件”、“覆盖已存储的最老的审计记录”和“一旦审计存储失败所采取的其他行动”等措施，防止审计数据丢失。

4.2.4.7 网络环境安全审计与评估

在网络环境运行的计算机信息系统，TSF 应采用以下措施进行安全审计与评估：

a) 建立由安全审计中心(安全审计服务器)和分布在网络各个运行节点的审计代理程序组成的分布式安全审计系统，实现网络环境计算机信息系统安全审计与评估。

b) 安全审计代理程序为安全审计服务器提供审计数据。

c) 安全审计服务器实时收集各安全代理程序的审计信息，并进行记录分析与保存。

d) 设置跨平台的安全审计机制，对安全事件快速进行评估并作出响应，向管理人员提供各种能反映系统使用情况、出现的可疑迹象、运行中发生的问题等有价值的统计和分析信息。

e) 运用统计方法学和审计评估机制，给出智能化审计报告及趋向报告，达到综合评估系统安全现状的目的。

4.2.5 网络防病毒

计算机信息系统应采用以下病毒防治措施：

a) 严格管理：严格控制各种外来介质的使用，必须先杀毒，后使用。

b) 防杀结合：要求在所有病毒可能入侵的网络连接部位设置病毒扫描工具，拦截并杀除企图进入系统的病毒。

c) 整体防御：应设置病毒管理中心，通过对全系统的服务器、工作站和客户机，进行病毒防治的统一管理，注意新病毒和杀病毒软件的升级换代；扫描、检查病毒感染情况，并设置在线报警功能，一旦发现病毒，可由管理人员从管理中心予以解决。

d) 防管结合：应将防病毒与网络管理相结合，在网管所涉及的重要部位设置防病毒软件，在所有病毒能够进入的地方都采取相应的防范措施，防止病毒侵袭。

e) 多层防御：应采用实时扫描、完整性保护和完整性检验等不同层次的技术，将病毒检测、多层数据保护和集中式管理功能集成起来，提供全面的病毒防护功能，检测、发现和消除病毒，阻止病毒的扩散和传播。

4.2.6 备份与故障恢复

4.2.6.1 备份

为了实现确定的恢复功能，必须在系统正常运行时定期地或按某种条件实施相应的备份。根据不同的恢复要求，应有以下形式的备份：

a) 用户自我信息备份：由用户自身有选择地备份重要信息。

b) 增量信息备份：由系统定时对新增信息进行备份。

c) 局部系统备份：对某些重要的局部系统进行定期备份。

d) 热备份：对系统的重要设备进行冗余设置，并在必要时能立即投入使用。

e) 全系统备份：定期对全系统的运行现场进行备份。

f) 主机系统异地备份：对于重要的计算机信息系统，设置主机系统的异地备份，以备主机系统不能正常运行时能在较短时间内启动，替代主机系统工作。

4.2.6.2 故障恢复

应在上述备份功能的基础上提供过程和机制，确保在确定不减弱保护的情况下启动 TCB，并在运

行中断后能在不减弱保护的情况下恢复计算机信息系统的运行。故障恢复包括：

a） 手动恢复：TCB 只提供以人工干预的方法使计算机信息系统返回到安全状态的机制。该机制在计算机信息系统发生失败或服务中断后，使 TSF 进入维护方式，并提供以手工方法将 TCB 返回到一个保护状态的能力。

b） 自动恢复：应对至少一种类型的服务中断，在无人工干预的情况下能使计算机信息系统恢复到安全状态，对其他的服务中断可由手动恢复实现。

c） 无过分丢失的自动恢复：在进行自动恢复时，应确保在 TSC 内的 TSF 数据或客体无超过限定量的丢失。

d） 灾难性恢复：当发生地震、水灾、火灾等不可抗拒的自然灾害或由于人为原因造成系统灾难性故障时，能通过启动异地备份系统的主机系统，使计算机信息系统继续正常运行，提供不间断服务。

4.2.7 计算机信息系统的应急计划和应急反应

在应急情况作出反应的应急计划应：

a） 具有各种安全措施：包括在出现各种安全事件时应采取的措施，这些措施是管理手段与技术手段的结合。

b） 设置正常备份机制：在系统正常运行时就通过各种备份措施为灾害和故障做准备。

c） 健全安全管理机构：建立健全的安全事件管理机构，明确人员的分工和责任。

d） 建立处理流程图：制定安全事件响应与处理计划及事件处理过程示意图，以便迅速恢复被破坏的系统。

4.3 信息安全

4.3.1 身份鉴别

4.3.1.1 用户标识

a） 基本标识：应在 TSF 实施所要求的动作之前，先对提出该动作要求的用户进行标识。

b） 唯一性标识：应确保所标识用户在计算机信息系统生命周期内的唯一性，并将用户标识与审计相关联。

c） 标识信息管理：应对用户标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。

4.3.1.2 用户鉴别

a） 基本鉴别：应在 TSF 实施所要求地动作之前，先对提出该动作要求地用户成功地进行鉴别。

b） 不可伪造鉴别：应检测并防止使用伪造或复制的鉴别数据。一方面，要求 TSF 应检测或防止由任何别的用户伪造的鉴别数据，另一方面，要求 TSF 应检测或防止当前用户从任何其他用户处复制的鉴别数据的使用。

c） 一次性使用鉴别：应能提供一次性使用鉴别数据操作的鉴别机制，即 TSF 应防止与已标识过的鉴别机制有关的鉴别数据的重用。

d） 多机制鉴别：应能提供不同的鉴别机制，用于鉴别特定事件的用户身份，并且 TSF 应根据所描述的多种鉴别机制如何提供鉴别的规则，来鉴别任何用户所声称的身份。

e） 重新鉴别：应有能力规定需要重新鉴别用户的事件，即 TSF 应在需要重鉴别的条件表所指示的条件下，重新鉴别用户。例如，末端用户操作超时被断开后，重新连接时需要进行重鉴别。

4.3.1.3 鉴别失败处理

要求 TSF 为不成功的鉴别尝试次数（包括尝试数目和时间的阈值）定义一个值，以及明确规定达到该值时所应采取的动作。鉴别失败的处理应包括检测出现相关的不成功鉴别尝试的次数与所规定的数目相同的情况，并进行预先定义的处理。

4.3.1.4 用户-主体绑定

在 TCB 安全功能控制范围之内，对一个已标识和鉴别的用户，为了要求 TSF 完成某个任务，需要

激活另一个主体(如进程),这时,要求通过用户-主体绑定将该用户与该主体相关联,从而将用户的身份与该用户的所有可审计行为相关联。

4.3.2 抗抵赖

4.3.2.1 抗原发抵赖

应确保信息的发送者不能成功地否认曾经发送过该信息。这就要求 TSF 提供一种方法,来确保接收信息的主体在数据交换期间能获得证明信息原发的证据,而且该证据可由该主体或第三方主体验证。

抗原发抵赖分为:

a) 选择性原发证明:要求 TSF 具有为主体提供请求原发证据信息的能力。即 TSF 在接到原发者或接收者的请求时,能就传输的信息产生原发证据,证明该信息的发送由该原发者所为。

b) 强制性原发证明:要求 TSF 在任何时候都能对传输的信息产生原发证据。即 TSF 在任何时候都能就传输的信息强制产生原发证据,证明该信息的发送由该原发者所为。

4.3.2.2 抗接收抵赖

应确保信息的接收者不能成功地否认对该信息的接收。这就要求 TSF 提供一种方法,来确保发送信息的主体在数据交换期间能获得证明该信息被接收的证据,而且该证据可由该主体或第三方主体验证。

抗接收抵赖分为:

a) 选择性接收证明:要求 TSF 具有为主体提供请求信息接收证据的能力。即 TSF 在接到原发者或接收者的请求时,能就接收到的信息产生接收证据,证明该信息的接收由该接收者所为。

b) 强制性接收证明:要求 TSF 总是对收到的信息产生接收证据。即 TSF 能在任何时候对收到的信息强制产生接收证据,证明该信息的接收由该接收者所为。

4.3.3 标记

4.3.3.1 主体标记

TSF 应为主体指定敏感标记,这些敏感标记是等级分类和非等级类别的组合,是实施强制访问控制的依据。

4.3.3.2 客体标记

TSF 应为客体指定敏感标记,这些敏感标记是等级分类和非等级类别的组合,是实施强制访问控制的依据。

4.3.4 自主访问控制

4.3.4.1 访问控制策略

TSF 应按确定的自主访问控制安全策略进行设计,实现对策略控制下的主体与客体间操作的控制。可以有多个自主访问控制安全策略,但它们必须独立命名,且不能相互冲突。常用的自主访问控制策略包括:访问控制表访问控制、目录表访问控制、权能表访问控制等。

4.3.4.2 访问控制功能

TSF 应明确指出采用一条命名的访问控制策略所实现的特定功能,说明策略的使用和特征,以及该策略的控制范围。

无论采用何种自主访问控制策略,TSF 应有能力提供:

——在安全属性或命名的安全属性组的客体上,执行访问控制 SFP;

——在基于安全属性的允许主体对客体访问的规则的基础上,允许主体对客体的访问;

——在基于安全属性的拒绝主体对客体访问的规则的基础上,拒绝主体对客体的访问。

4.3.5 强制访问控制

4.3.5.1 访问控制策略

TSF 应按确定的强制访问控制安全策略进行设计,并按需要确定访问控制策略的控制范围,包括策略控制下的主体、客体,及由策略覆盖的被控制的主体与客体间的操作。可以有多个访问控制安全策