ICS 35.240.40
L 80

中华人民共和国国家标准

GB/T 25070—2010

信息安全技术 信息系统等级保护安全设计技术要求

Information security technology—Technical requirements of security design for information system classified protection

2010-09-02 发布　　2011-02-01 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

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　信息系统等级保护安全技术设计概述 …… 2
5　第一级系统安全保护环境设计 …… 3
5.1　设计目标 …… 3
5.2　设计策略 …… 3
5.3　设计技术要求 …… 3
6　第二级系统安全保护环境设计 …… 3
6.1　设计目标 …… 3
6.2　设计策略 …… 4
6.3　设计技术要求 …… 4
7　第三级系统安全保护环境设计 …… 5
7.1　设计目标 …… 5
7.2　设计策略 …… 5
7.3　设计技术要求 …… 5
8　第四级系统安全保护环境设计 …… 7
8.1　设计目标 …… 7
8.2　设计策略 …… 7
8.3　设计技术要求 …… 7
9　第五级系统安全保护环境设计 …… 9
9.1　设计目标 …… 9
9.2　设计策略 …… 10
9.3　设计技术要求 …… 10
10　定级系统互联设计 …… 10
10.1　设计目标 …… 10
10.2　设计策略 …… 10
10.3　设计技术要求 …… 10
附录A（资料性附录）　访问控制机制设计 …… 11
A.1　自主访问控制机制设计 …… 11
A.2　强制访问控制机制设计 …… 11
附录B（资料性附录）　第三级系统安全保护环境设计示例 …… 13
B.1　功能与流程 …… 13
B.2　子系统间接口 …… 15
B.3　重要数据结构 …… 18
参考文献 …… 24

前　言

本标准的附录A、附录B是资料性附录。

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:公安部第一研究所。

本标准主要起草人:厉剑、范红、胡志昂、吉增瑞、张洪斌、赵勇、金丽娜、韩煜、赵会敏、张红旗、杜学绘、宫敏、马永清、韩勇桥、王超、连一峰、张海霞、黄涛、徐国爱、金舒原、田志宏、姜伟、刘鑫、苏智睿、李理、刘卫国、李娜。

引　言

《中华人民共和国计算机信息系统安全保护条例》(国务院令第147号)明确规定我国“计算机信息系统实行安全等级保护”。依据国务院147号令要求制定发布的强制性国家标准GB 17859—1999《计算机信息系统　安全保护等级划分准则》为计算机信息系统安全保护等级的划分奠定了技术基础。《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)明确指出实行信息安全等级保护“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统,抓紧建立信息安全等级保护制度”。《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)和《信息安全等级保护管理办法》(公通字[2007]43号)确定了实施信息安全等级保护制度的原则、工作职责划分、实施要求和实施计划,明确了开展信息安全等级保护工作的基本内容、工作流程、工作方法等。

上述信息安全等级保护相关法规、政策文件、国家标准和公共安全行业标准的出台,为信息安全等级保护工作的开展提供了法律、政策、标准依据。

2007年7月全国开展重要信息系统等级保护定级工作,标志着信息安全等级保护工作在我国全面展开。在开展信息安全等级保护定级和备案工作基础上,各单位、各部门正在按照信息安全等级保护有关政策规定和技术标准规范,开展信息系统安全建设和加固工作,建立、健全信息安全管理制度,落实安全保护技术措施,全面贯彻落实信息安全等级保护制度。为了配合信息系统安全建设和加固工作,特制定本标准。

本标准规范了信息系统等级保护安全设计技术要求,包括第一级至第五级系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求,以及定级系统互联的设计技术要求。涉及物理安全、安全管理、安全运维等方面的要求分别参见参考文献[9]、[2]、[7]、[10]等。进行安全技术设计时,要根据信息系统定级情况,确定相应安全策略,采取相应级别的安全保护措施。

在第5章至第9章中,每一级系统安全保护环境设计比较低一级系统安全保护环境设计所增加和增强的部分,用“**黑体**”表示。

信息安全技术
信息系统等级保护安全设计
技术要求

1 范围

本标准依据国家信息安全等级保护的要求，规定了信息系统等级保护安全设计技术要求。

本标准适用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构开展信息系统等级保护安全技术方案的设计和实施，也可作为信息安全职能部门进行监督、检查和指导的依据。

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

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

定级系统 classified system

按照参考文献[11]已确定安全保护等级的信息系统。定级系统分为第一级、第二级、第三级、第四级和第五级信息系统。

3.2

定级系统安全保护环境 security environment of classified system

由安全计算环境、安全区域边界、安全通信网络和(或)安全管理中心构成的对定级系统进行安全保护的环境。

定级系统安全保护环境包括第一级系统安全保护环境、第二级系统安全保护环境、第三级系统安全保护环境、第四级系统安全保护环境、第五级系统安全保护环境以及定级系统的安全互联。

3.3

安全计算环境 secure computing environment

对定级系统的信息进行存储、处理及实施安全策略的相关部件。

安全计算环境按照保护能力划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。

3.4

安全区域边界 secure area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

安全区域边界按照保护能力划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域边界和第五级安全区域边界。

3.5

安全通信网络　secure communication network

对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。

安全通信网络按照保护能力划分第一级安全通信网络、第二级安全通信网络、第三级安全通信网络、第四级安全通信网络和第五级安全通信网络。

3.6

安全管理中心　security management center

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。

第二级及第二级以上的定级系统安全保护环境需要设置安全管理中心，称为第二级安全管理中心、第三级安全管理中心、第四级安全管理中心和第五级安全管理中心。

3.7

跨定级系统安全管理中心　security management center for cross classified system

跨定级系统安全管理中心是对相同或不同等级的定级系统之间互联的安全策略及安全互联部件上的安全机制实施统一管理的平台。

3.8

定级系统互联　classified system interconnection

通过安全互联部件和跨定级系统安全管理中心实现的相同或不同等级的定级系统安全保护环境之间的安全连接。

4　信息系统等级保护安全技术设计概述

信息系统等级保护安全技术设计包括各级系统安全保护环境的设计及其安全互联的设计，如图1所示。各级系统安全保护环境由相应级别的安全计算环境、安全区域边界、安全通信网络和(或)安全管理中心组成。定级系统互联由安全互联部件和跨定级系统安全管理中心组成。

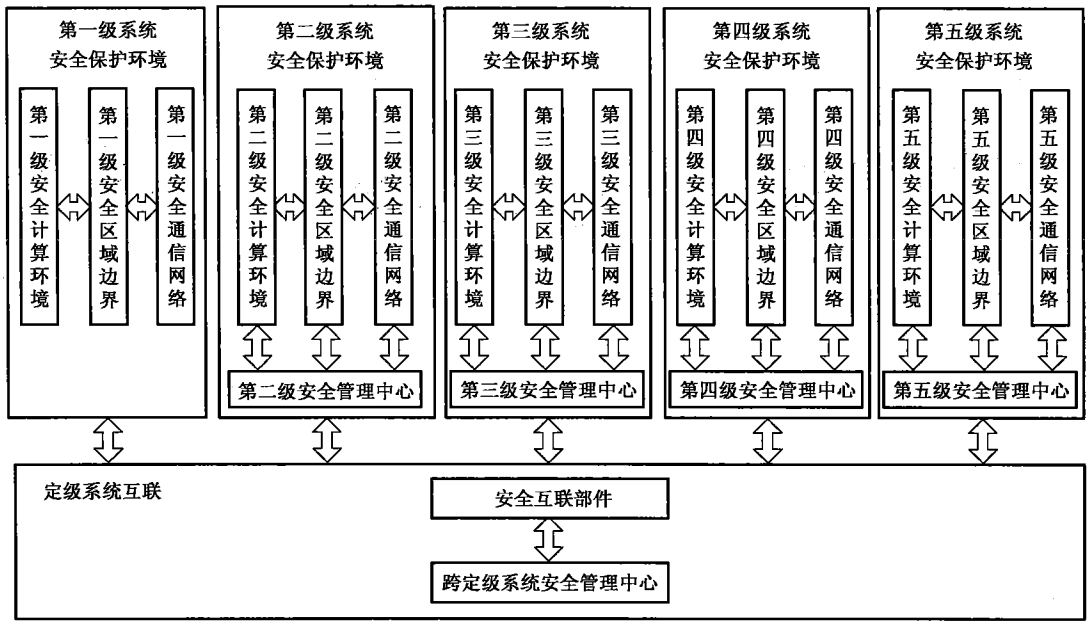

图1　信息系统等级保护安全技术设计框架

本标准以下章条，对图1各个部分提出了相应的设计技术要求(第五级信息安全保护环境的设计要求除外)。附录A给出了访问控制机制设计，附录B给出了第三级系统安全保护环境设计示例。

5 第一级系统安全保护环境设计

5.1 设计目标

第一级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第一级系统的安全保护要求，实现定级系统的自主访问控制，使系统用户对其所属客体具有自我保护的能力。

5.2 设计策略

第一级系统安全保护环境的设计策略是：遵循 GB 17859—1999 的 4.1 中相关要求，以身份鉴别为基础，提供用户和(或)用户组对文件及数据库表的自主访问控制，以实现用户与数据的隔离，使用户具备自主安全保护的能力；以包过滤手段提供区域边界保护；以数据校验和恶意代码防范等手段提供数据和系统的完整性保护。

第一级系统安全保护环境的设计通过第一级的安全计算环境、安全区域边界以及安全通信网络的设计加以实现。

5.3 设计技术要求

5.3.1 安全计算环境设计技术要求

第一级安全计算环境应从以下方面进行安全设计：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份；在每次用户登录系统时，采用口令鉴别机制进行用户身份鉴别，并对口令数据进行保护。

b) 自主访问控制

应在安全策略控制范围内，使用户/用户组对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户/用户组。访问控制主体的粒度为用户/用户组级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。

c) 用户数据完整性保护

可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。

d) 恶意代码防范

应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。

5.3.2 安全区域边界设计技术要求

第一级安全区域边界应从以下方面进行安全设计：

a) 区域边界包过滤

可根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。

b) 区域边界恶意代码防范

可在安全区域边界设置防恶意代码软件，并定期进行升级和更新，以防止恶意代码入侵。

5.3.3 安全通信网络设计技术要求

通信网络数据传输完整性保护。可采用常规校验机制，检验通信网络数据传输的完整性，并能发现其完整性被破坏。

6 第二级系统安全保护环境设计

6.1 设计目标

第二级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第二级系统的安全保护要求，在第一级系统安全保护环境的基础上，增加系统安全审计、客体重用等安全功能，并实施以用户为基本粒度的自主访问控制，使系统具有更强的自主安全保护能力。

6.2 设计策略

第二级系统安全保护环境的设计策略是：遵循 GB 17859—1999 的 4.2 中相关要求，以身份鉴别为基础，提供单个用户和(或)用户组对共享文件、数据库表等的自主访问控制；以包过滤手段提供区域边界保护；以数据校验和恶意代码防范等手段，同时通过增加系统安全审计、客体安全重用等功能，使用户对自己的行为负责，提供用户数据保密性和完整性保护，以增强系统的安全保护能力。

第二级系统安全保护环境的设计通过第二级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

6.3 设计技术要求

6.3.1 安全计算环境设计技术要求

第二级安全计算环境应从以下方面进行安全设计：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受控的口令或具有相应安全强度的其他机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。

c) 系统安全审计

应提供安全审计机制，记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。该机制应提供审计记录查询、分类和存储保护，并可由安全管理中心管理。

d) 用户数据完整性保护

可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。

e) 用户数据保密性保护

可采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

f) 客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

g) 恶意代码防范

应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。

6.3.2 安全区域边界设计技术要求

第二级安全区域边界应从以下方面进行安全设计：

a) 区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。

b) 区域边界安全审计

应在安全区域边界设置审计机制，并由安全管理中心统一管理。

c) 区域边界恶意代码防范

应在安全区域边界设置防恶意代码网关，由安全管理中心管理。

d) 区域边界完整性保护

应在区域边界设置探测器，探测非法外联等行为，并及时报告安全管理中心。

6.3.3 安全通信网络设计技术要求

第二级安全通信网络应从以下方面进行安全设计：

a) 通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心管理。

b) 通信网络数据传输完整性保护

可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。

c) 通信网络数据传输保密性保护

可采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

6.3.4 安全管理中心设计技术要求

6.3.4.1 系统管理

可通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份和授权管理、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复以及恶意代码防范等。

应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

6.3.4.2 审计管理

可通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。

应对安全审计员进行身份鉴别，并只允许其通过特定的命令或操作界面进行安全审计操作。

7 第三级系统安全保护环境设计

7.1 设计目标

第三级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第三级系统的安全保护要求，在第二级系统安全保护环境的基础上，通过实现基于安全策略模型和标记的强制访问控制以及增强系统的审计机制，使系统具有在统一安全策略管控下，保护敏感资源的能力。

7.2 设计策略

第三级系统安全保护环境的设计策略是：在第二级系统安全保护环境的基础上，遵循 GB 17859—1999 的 4.3 中相关要求，构造非形式化的安全策略模型，对主、客体进行安全标记，表明主、客体的级别分类和非级别分类的组合，以此为基础，按照强制访问控制规则实现对主体及其客体的访问控制。

第三级系统安全保护环境的设计通过第三级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

7.3 设计技术要求

7.3.1 安全计算环境设计技术要求

第三级安全计算环境应从以下方面进行安全设计：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和(或)记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

c) 标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

d) 系统安全审计

应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；确保对特定安全事件进行报警；确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

e) 用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

f) 用户数据保密性保护

应采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

g) 客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

h) 程序可信执行保护

可构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复，例如采用可信计算等技术。

7.3.2 安全区域边界设计技术要求

第三级安全区域边界应从以下方面进行安全设计：

a) 区域边界访问控制

应在安全区域边界设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。

b) 区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。

c) 区域边界安全审计

应在安全区域边界设置审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。

d) 区域边界完整性保护

应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。

7.3.3 安全通信网络设计技术要求

第三级安全通信网络应从以下方面进行安全设计：

a) 通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警。

b) 通信网络数据传输完整性保护

应采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。

c) 通信网络数据传输保密性保护

应采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

d） 通信网络可信接入保护

可采用由密码等技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。

7.3.4 安全管理中心设计技术要求

7.3.4.1 系统管理

应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和（或）异地灾难备份与恢复等。

应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

7.3.4.2 安全管理

应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置一致的安全策略。

应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

7.3.4.3 审计管理

应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行处理。

应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

8 第四级系统安全保护环境设计

8.1 设计目标

第四级系统安全保护环境的设计目标是：按照GB 17859—1999对第四级系统的安全保护要求，建立一个明确定义的形式化安全策略模型，将自主和强制访问控制扩展到所有主体与客体，相应增强其他安全功能强度；将系统安全保护环境结构化为关键保护元素和非关键保护元素，以使系统具有抗渗透的能力。

8.2 设计策略

第四级系统安全保护环境的设计策略是：在第三级系统安全保护环境设计的基础上，遵循GB 17859—1999的4.4中相关要求，通过安全管理中心明确定义和维护形式化的安全策略模型。依据该模型，采用对系统内的所有主、客体进行标记的手段，实现所有主体与客体的强制访问控制。同时，相应增强身份鉴别、审计、安全管理等功能，定义安全部件之间接口的途径，实现系统安全保护环境关键保护部件和非关键保护部件的区分，并进行测试和审核，保障安全功能的有效性。

第四级系统安全保护环境的设计通过第四级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

8.3 设计技术要求

8.3.1 安全计算环境设计技术要求

第四级安全计算环境应从以下方面进行安全设计：

a） 用户身份鉴别

应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录和重新连接系统时，采用受安全管理中心控制的口令、基于生物特征的数据、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可替代的，并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和(或)记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

c) 标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记，**将强制访问控制扩展到所有主体与客体**；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

d) 系统安全审计

应记录系统相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警，**终止违例进程等**；确保审计记录不被破坏或非授权访问**以及防止审计记录丢失等**。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

e) 用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

f) 用户数据保密性保护

采用密码等技术支持的保密性保护机制，对在安全计算环境中的用户数据进行保密性保护。

g) 客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

h) 程序可信执行保护

应构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复，例如采用可信计算等技术。

8.3.2 安全区域边界设计技术要求

第四级安全区域边界应从以下方面进行安全设计：

a) 区域边界访问控制

应在安全区域边界设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。

b) 区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出受保护的区域边界。

c) 区域边界安全审计

应在安全区域边界设置审计机制，通过安全管理中心集中管理，对确认的违规行为及时报警**并做出相应处置**。

d) 区域边界完整性保护

应在区域边界设置探测器，例如外接探测软件，探测非法外联**和入侵行为**，并及时报告安全管理中心。

8.3.3 安全通信网络设计技术要求

第四级安全通信网络应从以下方面进行安全设计：

a) 通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警，**且做**

出相应处置。

b) 通信网络数据传输完整性保护

应采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。

c) 通信网络数据传输保密性保护

采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

d) 通信网络可信接入保护

应采用由密码等技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。

8.3.4 安全管理中心设计技术要求

8.3.4.1 系统管理

应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和异地灾难备份与恢复等。

应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

8.3.4.2 安全管理

应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置一致的安全策略，并确保标记、授权和安全策略的数据完整性。

应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

8.3.4.3 审计管理

应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行及时处理。

应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

8.3.5 系统安全保护环境结构化设计技术要求

8.3.5.1 安全保护部件结构化设计技术要求

第四级系统安全保护环境各安全保护部件的设计应基于形式化的安全策略模型。安全保护部件应划分为关键安全保护部件和非关键安全保护部件，防止违背安全策略致使敏感信息从关键安全保护部件流向非关键安全保护部件。关键安全保护部件应划分功能层次，明确定义功能层次间的调用接口，确保接口之间的信息安全交换。

8.3.5.2 安全保护部件互联结构化设计技术要求

第四级系统各安全保护部件之间互联的接口功能及其调用关系应明确定义；各安全保护部件之间互联时，需要通过可信验证机制相互验证对方的可信性，确保安全保护部件间的可信连接。

8.3.5.3 重要参数结构化设计技术要求

应对第四级系统安全保护环境设计实现的与安全策略相关的重要参数的数据结构给出明确定义，包括参数的类型、使用描述以及功能说明等，并用可信验证机制确保数据不被篡改。

9 第五级系统安全保护环境设计

9.1 设计目标

第五级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第五级系统的安全保护要求，在第四级系统安全保护环境的基础上，实现访问监控器，仲裁主体对客体的访问，并支持安全管理职能。审计机制可根据审计记录及时分析发现安全事件并进行报警，提供系统恢复机制，以使系统具有更强的抗渗透能力。

9.2 设计策略

第五级系统安全保护环境的设计策略是：遵循 GB 17859—1999 的 4.5 中“访问监控器本身是抗篡改的；必须足够小，能够分析和测试”。在设计和实现访问监控器时，应尽力降低其复杂性；提供系统恢复机制；使系统具有更强的抗渗透能力；所设计的访问监控器能进行必要的分析与测试，具有抗篡改能力。

第五级系统安全保护环境的设计通过第五级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。

9.3 设计技术要求

第五级系统安全保护环境设计技术要求另行制定。

10 定级系统互联设计

10.1 设计目标

定级系统互联的设计目标是：对相同或不同等级的定级系统之间的互联、互通、互操作进行安全保护，确保用户身份的真实性、操作的安全性以及抗抵赖性，并按安全策略对信息流向进行严格控制，确保进出安全计算环境、安全区域边界以及安全通信网络的数据安全。

10.2 设计策略

定级系统互联的设计策略是：遵循 GB 17859—1999 对各级系统的安全保护要求，在各定级系统的计算环境安全、区域边界安全和通信网络安全的基础上，通过安全管理中心增加相应的安全互联策略，保持用户身份、主/客体标记、访问控制策略等安全要素的一致性，对互联系统之间的互操作和数据交换进行安全保护。

10.3 设计技术要求

10.3.1 安全互联部件设计技术要求

应通过通信网络交换网关与各定级系统安全保护环境的安全通信网络部件相连接，并按互联互通的安全策略进行信息交换，实现安全互联部件。安全策略由跨定级系统安全管理中心实施。

10.3.2 跨定级系统安全管理中心设计技术要求

应通过安全通信网络部件与各定级系统安全保护环境中的安全管理中心相连，主要实施跨定级系统的系统管理、安全管理和审计管理。

10.3.2.1 系统管理

应通过系统管理员对安全互联部件与相同和不同等级的定级系统中与安全互联相关的系统资源和运行进行配置和管理，包括用户身份管理、安全互联部件资源配置和管理等。

10.3.2.2 安全管理

应通过安全管理员对相同和不同等级的定级系统中与安全互联相关的主/客体进行标记管理，使其标记能准确反映主/客体在定级系统中的安全属性；对主体进行授权，配置统一的安全策略，并确保授权在相同和不同等级的定级系统中的合理性。

10.3.2.3 审计管理

应通过安全审计员对安全互联部件的安全审计机制、各定级系统的安全审计机制以及与跨定级系统互联有关的安全审计机制进行集中管理。包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行及时处理。

附 录 A
（资料性附录）
访问控制机制设计

A.1 自主访问控制机制设计

系统在初始配置过程中，安全管理中心首先需要对系统中的主体及客体进行登记命名，然后根据自主访问控制安全策略，按照主体对其创建客体的授权命令，为相关主体授权，规定主体允许访问的客体和操作，并形成访问控制列表。自主访问控制机制结构如图 A.1 所示。

用户登录系统时，首先进行身份鉴别，经确认为合法的注册用户可登录系统，并执行相应的程序。当执行程序主体发出访问系统中客体资源的请求后，自主访问控制安全机制将截获该请求，然后查询对应的访问控制列表。如果该请求符合自主访问控制列表规定的权限，则允许其执行；否则将拒绝执行，并将此行为记录在审计记录中。

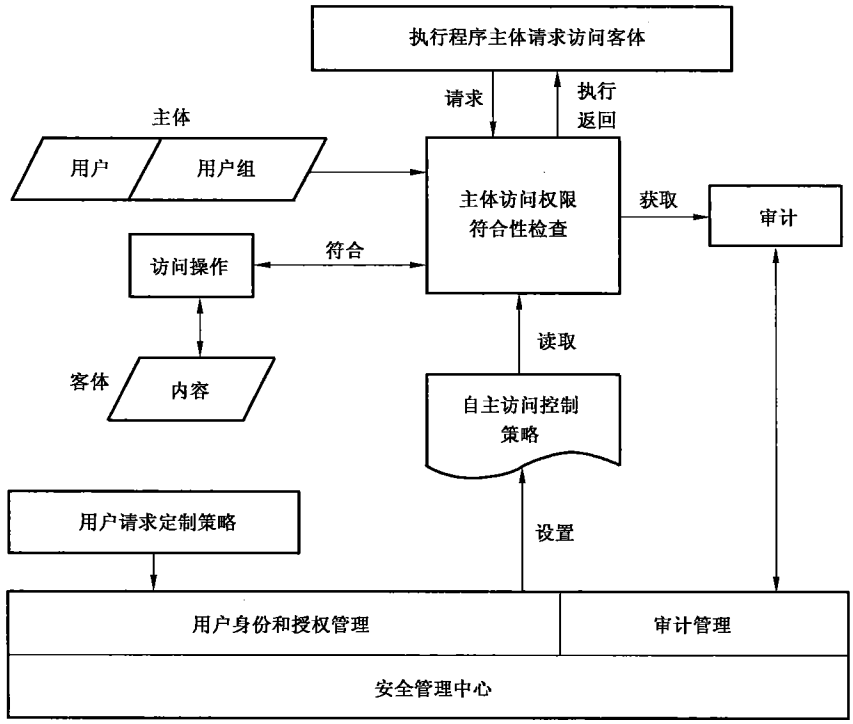

图 A.1 自主访问控制机制结构

A.2 强制访问控制机制设计

系统在初始配置过程中，安全管理中心需要对系统中的确定主体及其所控制的客体实施身份管理、标记管理、授权管理和策略管理。身份管理确定系统中所有合法用户的身份、工作密钥、证书等与安全相关的内容。标记管理根据业务系统的需要，结合客体资源的重要程度，确定系统中所有客体资源的安全级别及范畴，生成全局客体安全标记列表；同时根据用户在业务系统中的权限和角色确定主体的安全级别及范畴，生成全局主体安全标记列表。授权管理根据业务系统需求和安全状况，授予用户访问客体资源的权限，生成强制访问控制策略和级别调整策略列表。策略管理则根据业务系统的需求，生成与执行主体相关的策略，包括强制访问控制策略和级别调整策略。除此之外，安全审计员需要通过安全管理中心制定系统审计策略，实施系统的审计管理。强制访问控制机制结构如图 A.2 所示。

系统在初始执行时，首先要求用户标识自己的身份，经过系统身份认证确认为授权主体后，系统将下载全局主/客体安全标记列表及与该主体对应的访问控制列表，并对其进行初始化。当执行程序主体发出访问系统中客体资源的请求后，系统安全机制将截获该请求，并从中取出访问控制相关的主体、客体、操作三要素信息，然后查询全局主/客体安全标记列表，得到主/客体的安全标记信息，并依据强制访问控制策略对该请求实施策略符合性检查。如果该请求符合系统强制访问控制策略，则系统将允许该主体执行资源访问。否则，系统将进行级别调整审核，即依据级别调整策略，判断发出该请求的主体是否有权访问该客体。如果上述检查通过，系统同样允许该主体执行资源访问，否则，该请求将被系统拒绝执行。

系统强制访问控制机制在执行安全策略过程中，需要根据安全审计员制定的审计策略，对用户的请求及安全决策结果进行审计，并且将生成的审计记录发送到审计服务器存储，供安全审计员管理。

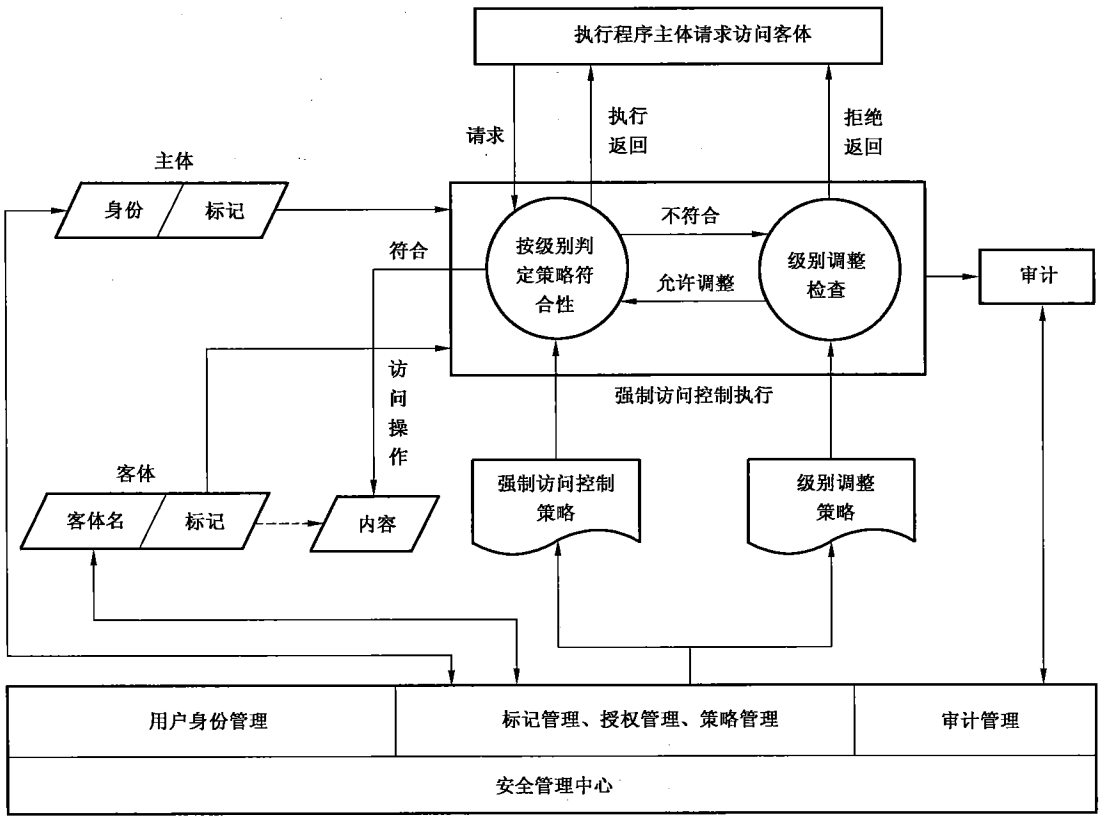

图 A.2 强制访问控制机制结构

附 录 B
（资料性附录）
第三级系统安全保护环境设计示例

B.1 功能与流程

根据“一个中心”管理下的“三重保护”体系框架，构建安全机制和策略，形成定级系统的安全保护环境。该环境分为如下四部分：安全计算环境、安全区域边界、安全通信网络和安全管理中心。每个部分由1个或若干个子系统（安全保护部件）组成，子系统具有安全保护功能独立完整、调用接口简洁、与安全产品相对应和易于管理等特征。安全计算环境可细分为节点子系统和典型应用支撑子系统；安全管理中心可细分为系统管理子系统、安全管理子系统和审计子系统。以上各子系统之间的逻辑关系如图B.1所示。

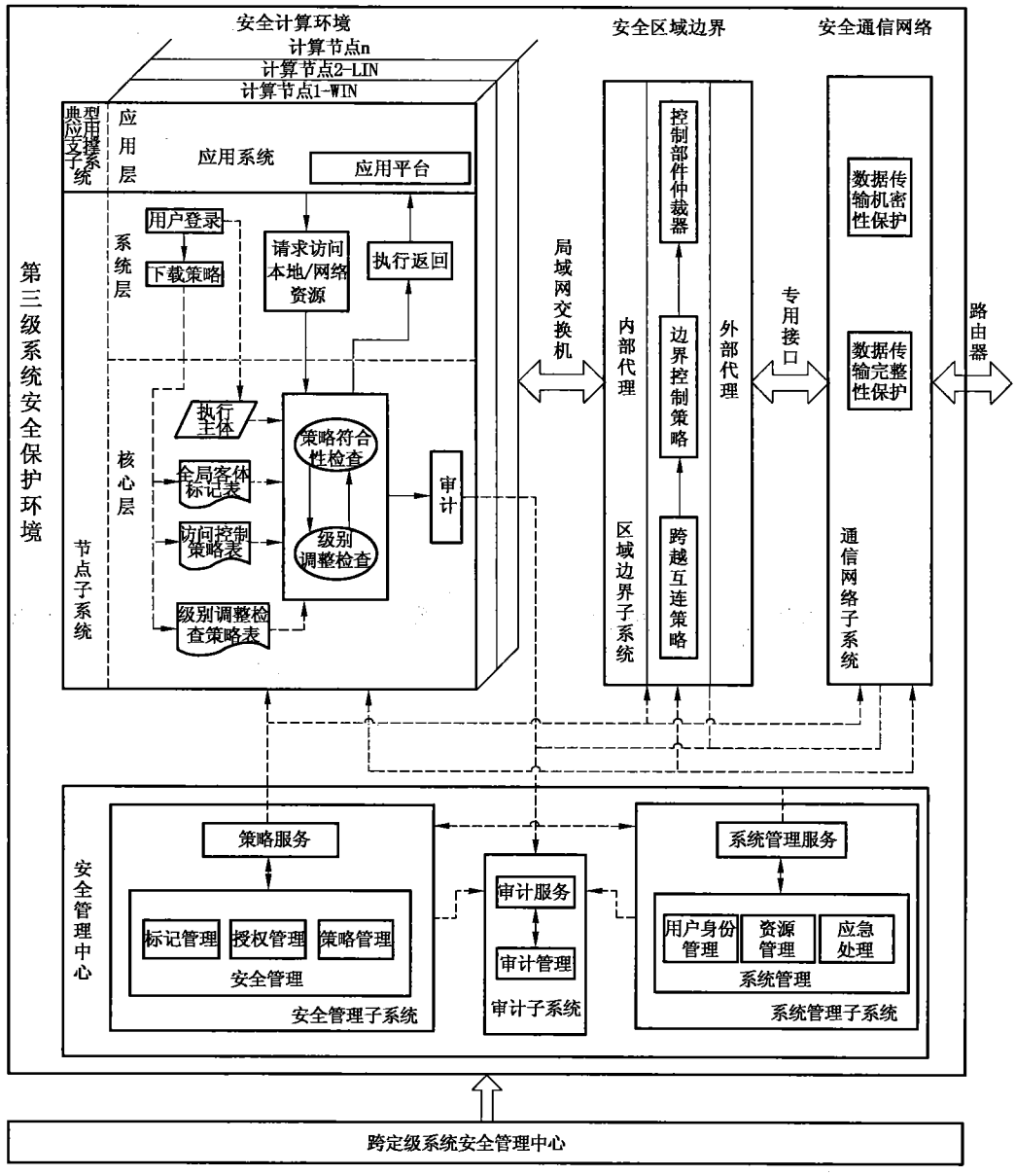

图 B.1 第三级系统安全保护环境结构与流程

B.1.1 各子系统主要功能

第三级系统安全保护环境各子系统的主要功能如下：

a) 节点子系统

节点子系统通过在操作系统核心层、系统层设置以强制访问控制为主体的系统安全机制，形成防护层，通过对用户行为的控制，可以有效防止非授权用户访问和授权用户越权访问，确保信息和信息系统的保密性和完整性，为典型应用支撑子系统的正常运行和免遭恶意破坏提供支撑和保障。

b) 典型应用支撑子系统

典型应用支撑子系统是系统安全保护环境中为应用系统提供安全支撑服务的接口。通过接口平台使应用系统的主客体与保护环境的主客体相对应，达到访问控制策略实现的一致性。

c) 区域边界子系统

区域边界子系统通过对进入和流出安全保护环境的信息流进行安全检查，确保不会有违反系统安全策略的信息流经过边界。

d) 通信网络子系统

通信网络子系统通过对通信数据包的保密性和完整性的保护，确保其在传输过程中不会被非授权窃听和篡改，以保障数据在传输过程中的安全。

e) 系统管理子系统

系统管理子系统负责对安全保护环境中的计算节点、安全区域边界、安全通信网络实施集中管理和维护，包括用户身份管理、资源管理、异常情况处理等。

f) 安全管理子系统

安全管理子系统是系统的安全控制中枢，主要实施标记管理、授权管理及策略管理等。安全管理子系统通过制定相应的系统安全策略，并要求节点子系统、区域边界子系统和通信网络子系统强制执行，从而实现对整个信息系统的集中管理。

g) 审计子系统

审计子系统是系统的监督中枢。安全审计员通过制定审计策略，并要求节点子系统、区域边界子系统、通信网络子系统、安全管理子系统、系统管理子系统强制执行，实现对整个信息系统的行为审计，确保用户无法抵赖违反系统安全策略的行为，同时为应急处理提供依据。

B.1.2 各子系统主要流程

第三级系统安全保护环境的结构与流程可以分为安全管理流程与访问控制流程。安全管理流程主要由安全管理员、系统管理员和安全审计员通过安全管理中心执行，分别实施系统维护、安全策略制定和部署、审计记录分析和结果响应等。访问控制流程则在系统运行时执行，实施自主访问控制、强制访问控制等。

a) 策略初始化流程

节点子系统在运行之前，首先由安全管理员、系统管理员和安全审计员通过安全管理中心为其部署相应的安全策略。其中，系统管理员首先需要为定级系统中的所有用户实施身份管理，即确定所有用户的身份、工作密钥、证书等。同时需要为定级系统实施资源管理，以确定业务系统正常运行需要使用的执行程序等。安全管理员需要通过安全管理中心为定级系统中所有主、客体实施标记管理，即根据业务系统的需要，结合客体资源的重要程度，确定其安全级，生成全局客体安全标记列表。同时根据用户在业务系统中的权限和角色确定其安全标记，生成全局主体安全标记列表。在此基础上，安全管理员需要根据系统需求和安全状况，为主体实施授权管理，即授予用户访问客体资源的权限，生成强制访问控制列表和级别调整策略列表。除此之外，安全审计员需要通过安全管理中心中的审计子系统制定系统审计策略，实施系统的审核管理。如果定级系统需要和其他系统进行互联，则上述初始化流程需要结合跨

定级系统安全管理中心制定的策略执行。

b) 计算节点启动流程

策略初始化完成后，授权用户才可以启动并使用计算节点访问定级系统中的客体资源。为了确保计算节点的系统完整性，节点子系统在启动时需要对所装载的可执行代码进行可信验证，确保其在可执行代码预期值列表中，并且程序完整性没有遭到破坏。计算节点启动后，用户便可以安全地登录系统。在此过程中，系统首先装载代表用户身份唯一标识的硬件令牌，然后获取其中的用户信息，进而验证登录用户是否是该节点上的授权用户。如果检查通过，系统将请求策略服务器下载与该用户相关的系统安全策略。下载成功后，系统可信计算基将确定执行主体的数据结构，并初始化用户工作空间。此后，该用户便可以通过启动应用访问定级系统中的客体资源。

c) 计算节点访问控制流程

用户启动应用形成执行主体后，执行主体将代表用户发出访问本地或网络资源的请求，该请求将被操作系统访问控制模块截获。访问控制模块首先依据自主访问控制策略对其执行策略符合性检查。如果自主访问控制策略符合性检查通过，则该请求允许被执行；否则，访问控制模块依据强制访问控制策略对该请求执行策略符合性检查。如果强制访问策略符合性检查通过，那么该请求允许被执行；否则，系统对其进行级别调整检查。即依照级别调整检查策略，判断发出该请求的主体是否有权访问该客体。如果通过，该请求同样允许被执行；否则，该请求被拒绝执行。

系统访问控制机制在安全决策过程中，需要根据安全审计员制定的审计策略，对用户的请求及决策结果进行审计，并且将生成的审计记录发送到审计服务器存储，供安全审计员检查和处理。

d) 跨计算节点访问控制流程

如果主体和其所请求访问的客体资源不在同一个计算节点，则该请求会被可信接入模块截获，用来判断该请求是否会破坏系统安全。在进行接入检查前，模块首先通知系统安全代理获取对方计算节点的身份，并检验其安全性。如果检验结果是不安全的，则系统拒绝该请求；否则，系统将依据强制访问控制策略，判断该主体是否允许访问相应端口。如果检查通过，该请求被放行；否则，该请求被拒绝。

e) 跨边界访问控制流程

如果主体和其所请求访问的客体资源不在同一个安全保护环境内，那么该请求将会被区域边界控制设备截获并且进行安全性检查，检查过程类似于跨计算节点访问控制流程。

B.2 子系统间接口

B.2.1 综述

为了清楚描述各子系统之间的关系，图 B.2 给出了子系统间的接口关系。

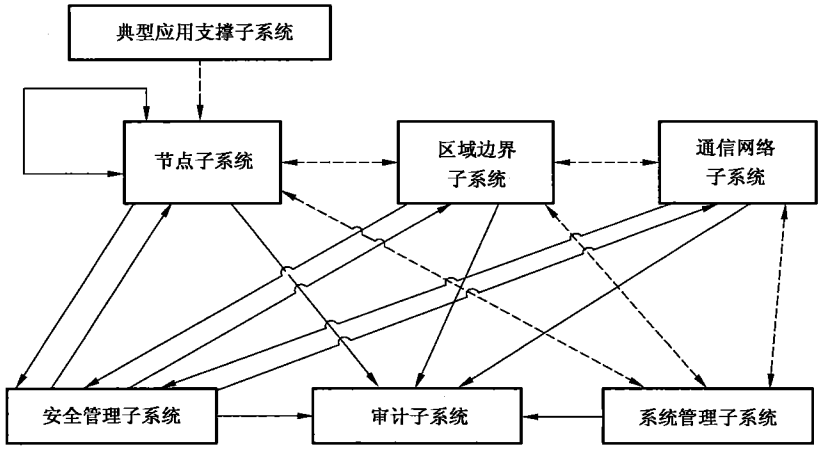

图 B.2 第三级系统安全保护环境子系统接口

典型应用支撑子系统与节点子系统之间通过系统调用接口。其他子系统之间则通过可靠的网络传输协议，按照规定的接口协议传输策略数据、审计数据以及其他安全保护环境数据等。由于不同子系统之间需要交换各种类型的数据包，因此需要明确定义子系统间的接口协议并规范传输数据包格式，使得各子系统之间能透明交互，实现相应数据的交换。数据包的标准格式如表 B.1 所示。

表 B.1　子系统间数据包格式

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
标志				版本号				接口类型				标记位			
内容长度				附加项长度				保留							
数据内容															
…															
附加项类型				附加项内容											
…															

数据包由包头、附加项和数据内容三部分组成，其中包头为 32 字节，定义了标志、版本号、接口类型、标记位以及内容和附加项长度等。内容和附加项长度不定。

数据包各数据项说明如下：

标志(4 字节)：用于标识等级保护相关的数据流，此标志可以作为区别等级保护数据包的依据。

版本号(4 字节)：表示该接口协议的版本号。其中前两个字节表示主版本号。

接口类型(4 字节)：表示本数据包的对应接口类型编号。

标记位 (4 字节)：表述数据包属性标志，如表 B.2 所示。

表 B.2　数据包属性标志

保留(29 比特位)	BRO	SIG	CHK

BRO：表示数据包发送对象地址尚未确定，需要以广播方式发送或发送给查询服务器。

SIG：表示数据包是否有签名保护，0 为无签名，1 为有签名。如果有签名保护，签名信息在附加项中。

CHK：表示数据包是否需要校验，0 为不校验，1 为校验。如果需要校验，校验码在附加项中存放。

内容长度(4 字节)：表示数据包内容部分长度，以字节为单位。

附加项长度(4 字节)：表示所有附加项长度之和，以字节为单位。

保留(8 字节)：作为数据包扩展保留。

数据内容：数据包传输的具体内容，其格式与数据包类型相关，长度不定。

附加项类型(4 字节)：表示附加项的类型。

附加项内容：数据包传输的附加内容，其格式与附加项类型相关，长度不定。

下面按照接口对应的数据包类型介绍数据内容部分，表格中不含包头和附加项。

B.2.2　接口 1

功能：节点(区域边界、通信网络)子系统向安全管理子系统请求下载策略。

类型：请求数据包。

描述：计算节点、区域边界、通信网络设备启动时，向安全管理子系统请求下载策略，该接口为节点子系统、区域边界子系统、通信网络子系统到安全管理子系统之间的接口。

客户端向服务器发起 TCP 连接，发出的请求数据包数据内容格式如表 B.3 所示。

表 B.3 客户端向服务器发出的请求数据包数据内容格式

节点标志(1～16 字节)	
节点标志(17～20 字节)	用户身份(1～12 字节)
用户身份(13～28 字节)	
用户身份(29～40 字节)	附加信息长度
附加信息	
…	

B.2.3 接口 2

功能:安全管理子系统向节点(区域边界、通信网络)子系统返回与请求主体相关的策略。

类型:策略下发数据包。

描述:安全管理中心接到下载策略请求后,向计算节点、区域边界、通信网络设备发送安全策略。

安全管理子系统策略下发数据包数据内容格式如表 B.4 所示。

表 B.4 安全管理子系统策略下发数据包数据内容格式

节点标志(1～16 字节)		
节点标志(17～20 字节)	用户身份(1～12 字节)	
用户身份(13～28 字节)		
用户身份(29～40 字节)		策略类型
策略版本(8 字节)	策略项数(4 字节)	保留(4 字节)
下载策略项 1		
…		
下载策略项 2		
…		

B.2.4 接口 3

功能:节点(区域边界、通信网络)子系统向审计服务器发送审计记录。

类型:审计记录数据包数据内容格式。

描述:计算节点、区域边界、通信网络设备向审计子系统发送审计记录。

所发送的审计记录数据包数据内容格式如表 B.5 所示。

表 B.5 节点子系统发送的审计记录数据包数据内容格式

节点标志(1～16 字节)		
节点标志(17～20 字节)	审计项数(4 字节)	保留
第 1 个审计项		
…		
第 2 个审计项		
…		
第 n 个审计项		
…		

B.2.5 接口 4

功能:节点子系统之间的接入可信性验证。

类型：可信接入申请包、可信接入应答包、可信接入确认包。

描述：节点子系统之间的接口主要实现可信接入。可信接入是在执行跨节点间访问时，客体所在节点验证主体所在节点可信性的过程。可信接入需要三步协议执行。首先是访问发起方所在节点向访问应答方所在节点提出可信接入申请包，应答方所在节点验证申请包后向发起方所在节点发送可信接入应答包，由发起方所在节点验证应答包成功后，返回可信接入确认包。

可信接入申请包格式如表 B.6 所示。

表 B.6　可信接入申请包数据内容格式

发起方平台身份(1～16 字节)	
发起方平台身份(17～32 字节)	
附加项长度(4 字节)	附加项

可信接入应答包格式如表 B.7 所示。

表 B.7　可信接入应答包数据内容格式

应答方平台身份(1～16 字节)	
应答方平台身份(17～32 字节)	
附加项长度(4 字节)	附加项

可信接入确认包数据内容格式和可信接入应答包内容格式相同，具体区别在于附加项。

B.3　重要数据结构

B.3.1　重要数据结构列表

第三级系统安全保护环境设计的重要数据结构如表 B.8 所示。

表 B.8　重要数据结构

编号	数据结构名称	用　途
1	用户身份信息列表	用户身份、密钥等信息列表
2	主体安全标记列表	以此表为依据，可以利用用户身份查询其标记信息
3	客体安全标记列表	以此表为依据，可以利用客体名查询其标记信息
4	自主访问控制列表	确定了主体能自主访问的客体
5	级别调整策略列表	确定了主体能特权操作的客体
6	审计策略列表	确定了系统的审计策略，即需要对哪些安全事件进行审计
7	审计记录格式	审计日志

B.3.2　用户身份信息列表

```
typedef struct tagUser_Info
{
    BYTE *      RootCert;
    UINT32      RootCertLen;
    BYTE *      UserCert;
    UINT32      UserCertLen;
    BYTE *      UserSigKey;
    UINT32      UserSigKeyLen;
    BYTE        EncAlgID;
    BYTE *      WorkKey;
```

```
    UINT32      WorkKeyLen;
    BYTE *      UserEncKey;
    UINT32      UserEncKeyLen;
    BYTE        Reserved [256];
} User_Info;
```

用户身份信息列表字段解释如表 B.9 所示。

表 B.9 重要数据结构

字段名	解　　释
RootCert	系统根证书
RootCertLen	系统根证书长度
UserCert	用户证书
UserCertLen	用户证书长度
UserSigKey	用户签名私钥
UserSigKeyLen	用户签名私钥长度
EncAlgID	对称加密算法标识
WorkKey	全系统统一的对称加密密钥
WorkKeyLen	全系统统一的对称加密密钥长度
UserEncKey	用户私有对称加密密钥
UserEncKeyLen	用户私有对称加密密钥长度
Reserved	保留字段

B.3.3 主体安全标记列表

```
typedef struct SubjectLabel
{
    UINT32  SubNameLength;
    BYTE *  sSubName;
    UINT32  GroupNameLength;
    BYTE *  sGroupName;
    BYTE    ConfLevel;
    BYTE    InteLevel;
    BYTE    SecClass[8];
    BYTE    SubType;
}Sub_Label;
```

主体安全标记列表字段解释如表 B.10 所示。

表 B.10 主体安全标记列表字段

字段名	解　　释
SubNameLength	主体名长度
sSubName	主体名
GroupNameLength	主体所属组名称长度
sGroupName	主体所属组名称

表 B.10（续）

字段名	解　　释
ConfLevel	用于标识主体的保密性级别
InteLevel	用于标识主体的完整性级别
SecClass	表示主体所属的范畴，共 64 位，8 位标识一个范畴，总共可以标识 8 个范畴，从高位到低位范畴级别依次降低
SubType	表示主体类型，即主体是否是安全管理员、系统管理员、安全审计员、普通操作员、进程或设备

B.3.4　客体安全标记列表

```
typedef struct ObjectLabel
{
    UINT32 ObjNameLength;
    BYTE * sObjName;
    BYTE   ConfLevel;
    BYTE   InteLevel;
    BYTE   SecClass[8];
    BYTE   ObjType;
} Obj_Label;
```

客体安全标记列表字段解释如表 B.11 所示。

表 B.11　客体安全标记列表字段

字段名	解　　释
ObjNameLength	客体名长度
sObjName	客体名称
ConfLevel	用于标识客体的保密性级别
InteLevel	用于标识客体的完整性级别
SecClass	表示客体所属的范畴，共 64 位，8 位标识一个范畴，总共可以标识 8 个范畴，从高位到低位范畴级别依次降低
ObjType	表示客体类型，即客体是否是系统文件、审计文件、策略文件、业务文件、系统服务或设备文件，以及客体是否需要加密保护

B.3.5　自主访问控制列表

```
typedef struct DAC_List
{
    UINT32   SubNameLength;
    BYTE *   sSubName;
    UINT32   ObjNameLength;
    BYTE *   sObjName;
    BYTE     OperateType;
} DAC_Label;
```

自主访问控制列表字段解释如表 B.12 所示。

表 B.12 自主访问控制列表字段

字段名	解　　释
SubNameLength	主体名长度
sSubName	主体名或主体组名
ObjNameLength	客体名长度
sObjName	客体名
OperateType	操作类型，包括创建、打开、读、写、修改、执行、更名和删除等

B.3.6 级别调整策略列表

```
typedef struct tagPriviledge_List
{
    UINT32  SubNameLength;
    BYTE *  sSubName;
    UINT32  ObjNameLength;
    BYTE *  sObjName;
    BYTE    OperateType;
    UINT32  AuthOwnerNameLength;
    BYTE *  sAuthOwnerName;
} PRIV_Label;
```

级别调整策略列表字段解释如表 B.13 所示。

表 B.13 级别调整策略列表字段

字段名	解释
SubNameLength	主体名长度
sSubName	主体名或主体所属组名
ObjNameLength	客体名长度
sObjName	客体名
OperateType	操作类型，包括创建、打开、读、写、修改、执行、更名和删除等
AuthOwnerNameLength	授权者用户名长度
sAuthOwnerName	授权者用户名

B.3.7 审计策略列表

```
typedef struct auditpolicytime
{
    BYTE  Year[4];
    BYTE  Month[2];
    BYTE  Day[2];
    BYTE  Hour[2];
    BYTE  Min[2];
    BYTE  Sec[2];
    BYTE  Week[2];
} APTIME;
typedef struct tagAUDIT_POLICY_TERM
```

```
{
    UINT16   NodeID;
    UINT16   iType;
    UINT16   Bret;
    SHORT    IsOn;
    APTIME   BeginTime;
    APTIME   EndTime;
    UINT32   Reserved;
} AUDIT_POLICY_TERM, * PAUDIT_POLICY_TERM;
```

审计策略列表字段解释如表 B.14 所示。

表 B.14　审计策略列表字段

字段名	解　　释
NodeID	节点的 ID 号
iType	审计事件类型、类别
Bret	共 2 字节，第一个字节表示动作行为，第二个字节表示动作结果及其原因
IsOn	审计开关　0:off;　1:on
BeginTime	审计开始时间
EndTime	审计结束时间
Reserved	保留字段

B.3.8　审计记录

```
typedef struct audit_label
{
    BYTE   Name[21];
    BYTE   ConfLevel;
    BYTE   InteLevel;
    BYTE   SecClass[8];
    BYTE   Type;
}ALABEL, * PALABEL;
typedef struct tagAudit_Record
{
    UINT16   NodeID;
    UINT16   iType;
    UINT32   Time;
    ALABEL   SubLabel;
    ALABEL   ObjLabel;
    UINT16   Bret;
    Byte     Reserved[6];
} Audit_Record;
```

审计记录字段解释如表 B.15 所示。

表 B.15 审计记录字段

字段名	解 释
NodeID	事件节点编号
iType	事件类型，包括身份鉴别、客体访问或用户行为等
Time	事件发生时间
SubLabel	事件发起主体安全标记
ObjLabel	事件对应客体安全标记
Bret	事件的操作行为、结果及其原因
Reserved	保留字段

参 考 文 献

[1] 公通字[2007]43 号 信息安全等级保护管理办法
[2] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[3] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[4] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[5] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
[6] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求
[7] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[8] GB/T 21028—2007 信息安全技术 服务器安全技术要求
[9] GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求
[10] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[11] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南
[12] GA/T 709—2007 信息安全技术 信息系统安全等级保护基本模型
[13] GA/T 711—2007 信息安全技术 应用软件系统安全等级保护通用技术指南

中华人民共和国
国家标准
信息安全技术
信息系统等级保护安全设计
技术要求
GB/T 25070—2010
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2 字数 49 千字
2010年12月第一版 2010年12月第一次印刷
*
书号:155066·1-40456 定价 30.00 元

GB/T 25070-2010

打印日期:2010年12月28日 F008