ICS 35.020
L09

GA

中华人民共和国公共安全行业标准

GA/T 708-2007

信息安全技术
信息系统安全等级保护体系框架

Information security technology-

Architecture framework of security classification protection for information system

2007-08-13 发布　　2007-10-01 实施

中华人民共和国公安部　发布

目　　次

前　　言

（略）

引　　言

信息系统安全等级保护通过三大功能和五个环节，对国家、社会、集团和个人所建立和使用的信息系统，分等级实施必要的安全保护。

实现信息系统安全等级保护的三大功能是：

——防范与保护功能：从物理、网络、系统、应用和管理等组成部分，实现整体防范与保护；

——监督与检查功能：各单位自我检查与政府职能部门监督检查相结合，从技术和管理两个方面，确保信息系统的安全性达到确定安全等级的要求；

——响应与处置功能：信息系统拥有者，对系统的安全事件应有快速响应与处置的能力，并在发现重大问题时能及时向主管部门反映，与有关单位沟通。

实现信息系统安全等级保护的五个环节是指：

——政策、法规环节：制定完善的信息安全等级保护政策、法规，建立专门的管理机构，明确实施的程序和方法；

——规范化技术与管理环节：制定符合国情的信息系统安全等级保护技术和管理标准，并按标准要求实施安全管理，进行安全技术和产品的研究和开发；

——系统构建过程控制环节：按照谁主管谁负责的要求，对安全信息系统的构建过程进行全方位控制，并通过检测机构严格的检测评估，确保所构建的安全信息系统达到所需要的安全性要求；

——系统运行过程控制环节：按照谁运营谁负责的要求，对安全信息系统的运行过程进行全方位控制，并通过职能部门的监督检查，确保所运行的安全信息系统达到所设计的安全性要求；

——系统监督、检查环节：信息安全相关职能部门，依照法律、法规和标准，制定完善信息安全监管规章制度，开展信息安全等级保护专项管理工作。督促安全等级保护责任制的落实，监督、检查并指导信息系统所属部门和单位的信息系统安全等级保护的建设和管理，对安全技术产品实行监管，对安全检测机构实施监管。建立非盈利的覆盖全国的系统安全等级保护执法检查与检测支持体系，使用统一标准对运行中的安全信息系统进行检查、检测、评估，确保其实际运行过程中的安全性达到设计的目标要求。

本标准是对信息系统安全等级保护各个组成部分及其相互关系的描述，首先对信息系统安全等级保护的组成部分的主要内容及其相互关系做简要说明，然后对每一个组成部分的主要内容做比较详细的说明。

信息安全技术
信息系统安全等级保护体系框架

1　范围

本标准规定了按照信息安全等级保护的要求从技术角度对信息系统实施安全等级保护的体系框架。

本标准适用于按照信息系统安全等级保护所规定的五个安全保护等级的要求对信息系统实施安全等级保护所进行的技术活动及其相关的管理活动。

2　规范性引用文件

下列文件中的有关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

安全信息系统　security information system

采用具有相应安全强度／等级的信息安全产品、信息安全技术和管理措施，以系统化方法设计和实现的，按照信息系统安全等级保护的要求具有一级/二级/三级/四级/五级安全性的信息系统。

3.2

信息安全系统　information security system

信息系统安全子系统的简称。一个信息系统的安全子系统是指由该信息系统中所有安全装置组成的系统。在 GB 17859-1999 中，将系统内保护装置的总体称为 TCB（可信计算基）。这里用信息安全系统的称谓是为了强调对信息系统的安全应以系统化的方法进行设计。

3.3

信息安全产品　information security production

具有确定安全强度／等级，用于构建安全信息系统的信息产品。信息安全产品分为信息技术安全产品和信息安全专用产品。信息技术安全产品是对信息技术产品附加相应的安全技术和机制组成的产品（如安全路由器）；信息安全专用产品是专门为增强信息系统的安全性而开发的信息安全产品（如防火墙）。

3.4

局域计算环境　local computing environment

由一个或多个计算机系统（主机/服务器）组成的，以对信息系统中的数据信息进行存储、处理为主要目的、有明确边界的计算环境。一个局域计算环境可以由一个计算机系统组成，也可以由多个计算机系统经局域网连接组成。

3.5

安全局域计算环境　security local computing environment

具有确定安全保护等级的局域计算环境。

3.7

局域计算环境边界 local computing environment boundaries

局域计算环境与外部交换信息的所有界面的总称。

3.8

用户环境（独立用户/用户群） user environment(independent user/group user)

由一个或多个终端计算机组成的，以提供用户使用信息系统中的数据信息为主要目的环境，也称独立用户/用户群。

3.9

安全用户环境 security user environment

具有确定安全保护等级的用户环境。

3.10

网络系统 networks system

连接局域计算环境与局域计算环境及局域计算环境与用户环境的网络设备、设施所组成的系统。

3.11

安全网络系统 security networks system

具有确定安全保护等级的网络系统。

3.12

安全域 security area

信息系统中执行相同安全策略的区域。在实施等级保护的信息系统中，安全域可以是具有相同安全等级的信息系统或子系统。

3.13

密码基础设施 cryptograph infrastructures

为信息系统中的各种密码机制提供支持的设施。密码基础设施所提供的密码支持主要包括数据的加/解密、完整性检验、身份鉴别、数字签名/验证、抗抵赖等。

4 信息系统安全等级保护体系简介

4.1 信息系统安全等级保护体系的组成

信息系统安全等级保护体系由以下部分组成：

——信息系统安全等级保护法律、法规、政策依据；

——信息系统安全等级保护标准体系；

——信息系统安全等级保护管理体系；

——信息系统安全等级保护技术体系。

4.2 信息系统安全等级保护体系概要说明

a) 信息安全等级保护的法律、法规和政策依据

信息系统安全等级保护政策、法律、法规依据是信息系统安全等级保护的基本依据和出发点。

b) 信息系统安全等级保护标准体系

信息系统安全等级保护标准是信息安全等级保护在信息系统安全技术和安全管理方面的规范化表示，是从技术和管理方面，以标准的形式，对信息安全等级保护的法律、法规、政策的规定进行的规范化描述。

本标准体系从标准分类、各类标准的具体组成、标准所涉及的内容以及各类标准的编写要求等方面规范了对信息系统实施安全等级保护所需要的各级、各类标准的名称、作用、内容及其编写要求。

c) 信息系统安全等级保护管理体系

信息系统安全等级保护管理体系是对实现信息系统安全等级保护所采用的安全管理措施的描述。本标准从信息系统安全等级保护安全系统工程管理、安全系统运行控制和管理、安全系统监督检查和管理等方面，对相关问题进行了描述。

d) 信息系统安全等级保护技术体系

信息系统安全等级保护技术体系是对实现信息系统安全等级保护所采用的安全技术的描述。本标准体系从信息系统安全的基本属性、信息系统安全的组成与相互关系、信息系统安全的五个等级、信息系统安全等级保护的基本框架、信息系统安全等级保护基本技术、信息系统安全等级保护支撑平台技术、等级化安全信息系统的构建技术等方面对相关的技术问题进行了描述。

5 信息系统安全等级保护法律法规和政策依据

5.1 法律法规和政策分类

信息系统安全等级保护的法律法规和政策是对信息系统实施安全等级保护的基本依据，对信息系统实施安全等级保护所需要的法律法规和政策包括：

a) 有关信息安全等级保护的全国性法律；
b) 有关信息安全等级保护的全国性政策、法规；
c) 有关信息安全等级保护的地区性政策、法规。

5.2 信息系统安全等级保护的现有政策法规

当前，已经发布的有关对信息系统实施安全等级保护的政策法规有：

a) 1994 年 2 月 18 日发布的国务院 147 号令：中华人民共和国计算机信息系统安全保护条例；
b) 2003 年 8 月 26 日发布的中办发[2003]27 号文件：国家信息化领导小组关于加强信息安全保障工作的意见；
c) 2004 年 9 月 15 日发布的公通字[2004]66 号文件：关于信息安全等级保护工作的实施意见；
d) 2005 年 12 月 28 日发布的公信安[2005]1431 号文件：关于开展信息系统安全等级保护基础调查工作的通知。
e) 2006 年 2 月 23 日发布的国办发[2006]11 号文件：国务院办公厅转发国家网络与信息安全协调小组关于网络信任体系若干意见的通知；
f) 2007 年 6 月 22 日发布的公通字[2007]43 号文件：信息安全等级保护管理办法；
g) 其它与信息安全等级保护相关的政策法规。

6 信息系统安全等级保护标准体系

6.1 标准的分类

信息系统安全等级保护标准分为：

——基础性标准：作为信息系统安全等级保护的基础，并为其他标准提供支持的标准；
——系统设计指导类标准：对按等级保护的要求进行信息系统安全设计提供指导的标准；
——系统实施指导类标准：从系统角度，按信息安全等级保护的要求，以各要求类标准的具体要求为依据，对实施信息系统安全等级保护提供指导的标准；
——要求类标准：对按等级保护的要求建设安全的信息系统，规范安全技术要求和安全管理要求的标准；
——检查/测评类标准：对按等级保护的要求进行信息系统安全的检查/测评，提供技术和管理方面指导的标准；
——各应用领域实施指导方案：按等级保护要求，对各个应用领域按照上述标准的要求建

设安全的信息系统的指导性方案。

6.2 标准的具体组成

6.2.1 基础性标准

基础性标准是指包括以下方面内容的标准：

a) 信息安全等级保护术语标准；

b) 信息系统安全保护等级划分的准则性标准，如 GB 17859-1999；

c) 信息安全等级保护的其他基础性标准。

6.2.2 系统设计指导类标准

对信息系统安全等级保护的设计提供指导的标准包括以下方面内容的标准：

a) 信息系统安全等级保护体系框架；

b) 信息系统安全等级保护基本模型；

c) 信息系统安全等级保护基本配置；

d) 信息系统安全等级保护设计的其他指导标准。

6.2.3 系统实施指导类标准

从系统角度，对信息系统安全等级保护的实施提供指导的标准包括以下方面内容的标准：

a) 信息系统安全等级保护定级指南；

b) 信息系统安全等级保护基本要求；

c) 信息系统安全等级保护实施指南；

d) 信息系统安全等级保护监督管理手册；

e) 信息系统安全等级保护服务指南；

f) 信息系统安全等级保护产品选购指南；

g) 信息系统安全等级保护安全意识教育培训指南；

h) 信息系统安全等级保护系统测试环境；

i) 信息系统安全等级保护系统测试方法；

j) 信息系统安全等级保护系统测试工具；

k) 信息系统安全等级保护产品测试环境；

l) 信息系统安全等级保护产品测试方法；

m) 信息系统安全等级保护产品测试工具；

n) 信息系统安全等级保护实施的其它指导标准。

6.2.4 要求类标准

6.2.4.1 系统和分系统安全技术要求

按要素/组件，对系统和分系统的安全技术要求进行描述的标准包括以下方面内容的标准：

a) 信息系统安全通用技术要求；

b) 网络安全基础技术要求；

c) 操作系统安全技术要求；

d) 数据库管理系统安全技术要求；

e) 应用软件系统安全技术要求；

f) 信息系统物理安全技术要求；

g) 其它系统和分系统安全技术要求。

6.2.4.2 信息安全产品安全技术要求

6.2.4.2.1 信息技术产品安全技术要求

按要素/组件，对信息技术产品的安全技术要求进行描述的标准包括以下方面内容的标准：

a) 网管安全技术要求；

b) 网络服务器安全技术要求；
c) 路由器安全技术要求；
d) 交换机安全技术要求；
e) 网关安全技术要求；
f) 网络互连安全技术要求；
g) 网络协议安全技术要求；
h) 电磁信息产品安全技术要求；
i) 其它信息技术产品安全技术要求。

6.2.4.2.2 信息安全专用产品安全技术要求

按要素/组件，对信息安全专用产品的安全技术要求进行描述的标准包括以下方面内容的标准：

a) 公钥基础设施（PKI）安全技术要求；
b) 网络身份认证安全技术要求；
c) 防火墙安全技术要求；
d) 入侵检测安全技术要求；
e) 系统审计安全技术要求；
f) 网络脆弱性检测分析安全技术要求；
g) 网络及端设备隔离部件安全技术要求；
h) 防病毒产品安全技术要求；
i) 虹膜身份鉴别安全技术要求；
j) 指纹身份鉴别安全技术要求；
k) 虚拟专用网安全技术要求；
l) 通用安全模块安全技术要求；
m) 其它安全产品安全技术要求。

6.2.4.3 安全管理要求

按要素/组件，对系统的安全管理要求进行描述的标准包括以下方面内容的标准：
a) 安全系统工程管理要求；
b) 安全系统运行管理要求；
c) 商用密码管理要求；
d) 安全风险管理要求；
e) 应急处理管理管理要求；
f) 其它管理要求。

6.2.5 检查/测评类标准

6.2.5.1 系统和分系统安全技术检查/测评

按要素/组件，对系统和分系统安全技术的检查／测评进行描述的标准包括以下方面内容的标准：

a) 信息系统安全技术检查/测评；
b) 网络系统安全技术检查/测评；
c) 操作系统安全技术检查/测评；

d) 数据库管理系统安全技术检查/测评；

e) 应用软件系统安全技术检查/测评；

f) 硬件系统安全技术检查/测评；

g) 其它系统安全技术检查/测评。

6.2.5.2 信息安全产品安全技术检查/测评

6.2.5.2.1 信息技术产品安全技术检查/测评

按要素/组件，对信息技术产品的安全技术的检查／测评进行描述的标准包括以下方面内容的标准：

a) 网管安全技术检查/测评；

b) 网络服务器安全技术检查/测评；

c) 路由器安全技术检查/测评；

d) 交换机安全技术检查/测评；

e) 网关安全技术检查／测评；

f) 网络互连安全技术检查/测评；

g) 网络协议安全技术检查/测评；

h) 电磁信息产品安全技术检查/测评；

i) 其它信息技术产品安全技术检查/测评。

6.2.5.2.2 信息安全专用产品安全技术检查/测评

按要素/组件，对安全专用产品的安全技术的检查／测评进行描述的标准包括以下方面内容的标准：

a) 公钥基础设施（PKI）安全技术检查/测评；

b) 网络身份认证安全技术检查/测评；

c) 防火墙安全技术检查/测评；

d) 入侵检测安全技术检查/测评；

e) 系统审计安全技术检查/测评；

f) 网络脆弱性检测安全技术检查/测评；

g) 网络及端设备隔离部件安全技术检查/测评；

h) 防病毒产品安全技术检查/测评；

i) 虹膜身份鉴别安全技术检查/测评；

j) 指纹身份鉴别安全技术检查/测评；

k) 虚拟专用网安全技术检查/测评；

l) 通用安全模块安全技术检查/测评；

m) 其它安全专用产品安全技术检查/测评。

6.2.5.3 安全管理检查/测评

按要素/组件，对系统的安全管理的测试／评估进行描述的标准包括以下方面内容的标准：

a) 安全系统工程管理检查/测评；

b) 安全系统运行管理检查/测评；

c) 商用密码管理检查/测评；

d) 应急处理管理检查/测评；

e) 风险管理检查/测评；

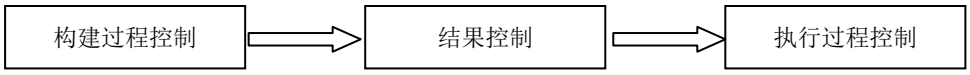
f) 其它管理检查/测评。

6.2.6 各应用领域实施指导方案

各个应用领域的安全系统实施指导方案，应由相应领域的安全管理部门组织人员，按照以上信息系统安全等级保护标准的内容，主要是系统设计指导类标准和系统实施指导类标准的内容，结合本领域对安全要求的特点进行制订。

6.3 标准所涉及的内容

图 1 给出了信息系统安全等级保护标准体系中的标准所涉及内容的示意图。该图反映了信息系统安全等级保护标准应包括五个保护等级、五个安全组成部分以及构建过程控制、结果控制、执行过程控制等方面的内容。这也是整个信息系统安全等级保护所涉及的内容。



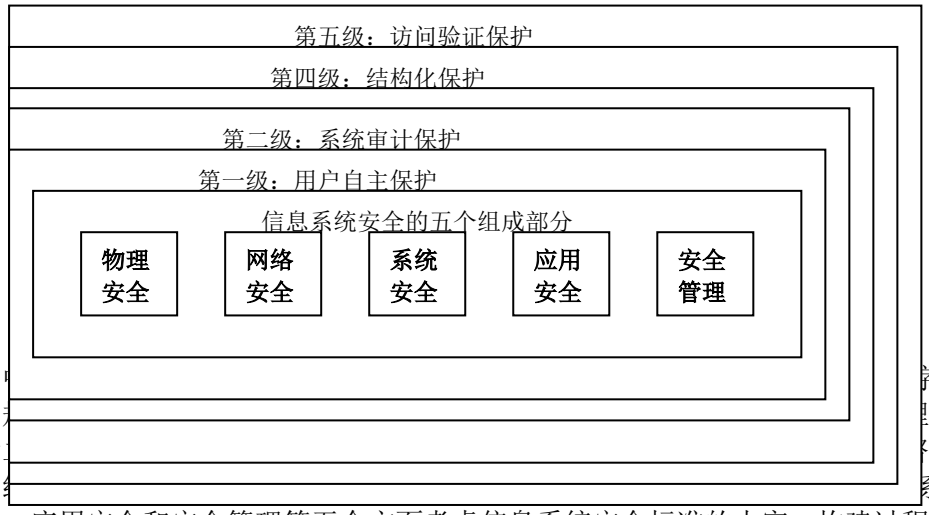


图 1 中 字[2007]43号文件的 里，具体要求是：对 、检查，对五级系 系统安全、网络安全、应用安全和安全管理等五个方面考虑信息系统安全标准的内容。构建过程控制主要是指应从安全系统建设、安全产品开发的过程控制方面制定相应的技术和管理要求标准；结果控制主要是指应从安全系统建设、安全产品开发的结果控制方面制定相应的技术和管理测评标准；执行过程控制主要是指应从政府部门的监督检查和指导方面制定相应的标准。

6.4 各类标准的作用及编写要求

6.4.1 基础性标准

基础性标准是为信息安全等级保护确定基本原则和基本要求的标准。基础标准的编写应满足下列要求：

——安全技术要求描述：应从安全要素/组件的角度，对信息系统安全所涉及的安全功能技术要求和安全保证技术要求有全面描述；

——分等级安全功能技术要求：应从等级划分的角度，对不同安全保护等级的各个安全要素/组件的安全功能技术要求进行完整描述；

——分等级安全保证技术要求：应从等级划分的角度，对不同安全保护等级的各个安全保证技术要求进行完整描述。

6.4.2 系统设计指导类标准

系统设计指导类标准是从系统角度对实现信息系统安全等级保护进行框架性说明的标准，对从总体角度了解信息系统安全等级保护提供指导和帮助。系统设计指导类标准由信息系统安全等级保护体系框架、信息系统安全等级保护基本模型和信息系统安全等级保护基本配置等部分组成。其编写分别应满足下列要求：

——信息系统安全等级保护体系框架：体系框架标准的编写应明确信息系统安全等级保护的组成及其相互关系，包括：信息系统安全等级保护的法律和政策法律依据，信息系统安全等级保护的标准体系，信息系统安全等级保护的管理体系以及信息系统安全等级保护的技术体系。标准应对信息系统安全等级保护的法律和政策法规依据进行明确的说明，并对组成体系框架的标准体系、管理体系和技术体系的具体内容进行说明；

——信息系统安全等级保护基本模型：基本模型标准的编写应在对信息系统安全的总体模型进行说明的基础上，明确说明每一个安全保护等级的信息系统的基本模型；

——信息系统安全等级保护基本配置：基本配置标准的编写应根据每一个安全保护等级的信息系统的基本模型，说明每一个安全保护等级的安全机制的基本配置。

6.4.3 要求类标准

6.4.3.1 系统和分系统安全技术要求

信息系统和分系统安全技术要求的作用及编写要求分别是：

a) 信息系统安全技术要求

信息系统安全技术要求标准，是对信息系统的安全技术要求从安全要素/组件角度进行详细说明的标准，能够对从系统角度了解信息系统安全等级保护提供帮助，对构建符合等级保护要

求的安全信息系统提供指导。其编写应满足下列要求：

——全面安全技术要求：应对信息系统安全普遍适用的安全功能技术要求和安全保证技术要求进行全面描述；

——分等级安全功能技术要求：应对信息系统各个安全保护等级应具有的安全功能技术要求进行描述；

——分等级安全保证技术要求：应对信息系统各个安全保护等级应具有的安全保证技术要求进行描述。

b) 信息系统分系统安全技术要求

信息系统分系统是指组成信息系统的各个组成部分的分系统，包括物理（硬件系统）、操作系统、网络系统、数据库管理系统、应用软件系统等。信息系统分系统安全技术要求标准，是对各个分系统的安全技术要求从安全要素/组件角度进行详细说明的标准，能对从系统组成了解信息系统安全等级保护提供帮助，对构建符合安全保护等级要求的安全分系统提供指导。信息系统各个安全分系统安全技术要求标准的编写应满足下列要求：

——全面安全技术要求：应对信息系统各个分系统各自的安全功能技术要求和安全保证技术要求进行全面的描述；

——分等级安全功能技术要求：应对信息系统各个分系统各自的每个安全等级应具有的安全功能技术要求进行描述；

——分等级安全保证技术要求：应对信息系统各个分系统各自的每个安全等级应具有的安全保证技术要求进行描述。

6.4.3.2 信息安全产品安全技术要求

信息安全产品是实现信息系统安全的基础和前提。信息安全产品安全技术要求是指每一个产品应达到的安全技术要求。信息安全产品分为信息技术产品和信息安全专用产品。其作用和编写要求分别是：

a) 信息技术产品安全技术要求

信息技术产品安全技术要求是指对信息系统固有的信息技术产品（IT 产品）的安全技术要求。适用于信息系统安全等级保护的信息技术产品的安全技术要求标准的编写应满足下列要求：

——全面安全技术要求：应以信息系统安全通用技术要求标准为基本依据，对信息技术产品各自的安全功能技术要求和安全保证技术要求进行全面说明；

——分等级安全功能技术要求：信息技术产品安全功能的分等级要求，可根据各个产品的具体情况对所需要的安全等级的安全功能技术的具体要求进行说明；可分等级，也可不分等级或只有某些等级；

——分等级安全保证技术要求：信息技术产品安全保证的分等级要求，可根据各个产品的具体情况对所需要的安全等级的安全保证的具体要求进行说明；按照与安全功能等级匹配的原则，安全保证技术要求可分等级，也可不分等级或只有某些等级。

b) 信息安全专用产品安全技术要求

信息安全专用产品是指为了增强信息系统的安全性在信息系统中设置的安全产品，如防火墙、入侵检测系统等。适用于信息系统安全等级保护的信息安全专用产品的安全技术要求标准的编写应满足下列要求：

——外部安全功能和性能要求：对信息安全专用产品应实现的外部安全功能和性能进行全面的说明；

——全面安全技术要求：以信息系统通用安全技术要求标准为基本依据，对信息安全专用产品的安全功能技术要求和安全保证技术要求进行全面说明；

——分等级外部安全功能和性能要求：可根据各个产品的具体情况，对所需要的安全等级的外部安全功能和性能的具体要求进行说明；可分等级，也可不分等级或只有某些等级；

——分等级安全功能技术要求：可根据各个产品的具体情况，对所需要的安全等级的安全功能的具体技术要求进行说明；可分等级，也可不分等级或只有某些等级；

——分等级安全保证技术要求：可根据各个产品的具体情况，对所需要的安全等级的安全保证的具体技术要求进行说明；按照与安全功能等级匹配的原则，可分等级，也可不分等级或只有某些等级。

6.4.3.3 安全管理要求

安全管理要求包括安全系统工程管理要求和安全系统运行管理要求两大类。其作用和编写要求分别是：

a) 安全系统工程管理要求

安全系统工程管理是指对实现信息安全系统的工程过程的管理。信息安全系统的工程管理要求的编写应满足下列要求：

——工程管理全面要求：对实现信息系统的安全目标，安全系统工程过程管理应采取的措施进行全面说明；

——工程管理分等级要求：应对每一个安全保护等级的信息系统的安全工程管理要求分别进行明确的说明。

b) 安全系统运行管理要求

安全系统运行管理是指对实现安全系统安全运行的过程的管理。信息安全系统运行管理要求的编写应满足下列要求：

——运行管理全面要求：对实现信息安全系统的安全目标，安全系统运行过程管理应采取的各种管理措施进行全面说明；

——运行管理分等级要求：应对每一个安全保护等级的信息系统的安全系统运行管理要求分别进行明确的说明。

6.4.4 检查/测评类标准

6.4.4.1 系统和分系统安全技术检查/测评

信息系统和分系统安全技术检查/评估的作用及编写要求分别是：

a) 信息系统安全技术检查/评估

信息系统安全技术检查/测评标准，是从要素/组件角度对信息系统的各个安全技术的检查/测评要求进行详细说明的标准，对从系统角度了解信息系统安全等级保护提供帮助，对按等级保护要求进行信息系统安全技术的检查/测评提供指导。信息系统安全技术检查/测评标准的编写应满足下列要求：

——检查/测评环境和条件要求：应对进行安全技术检查/测评的信息系统的运行、使用的环境、条件要求进行全面的说明；

——检查/测评分等级要求：应对照相应信息系统的安全技术要求，对进行安全技术检查与评估的信息系统的每一个安全保护等级的安全功能技术和安全保证技术的检查/测评要求进行说明。

b) 信息系统分系统安全技术检查/评估

信息系统分系统安全技术检查/测评标准，是从要素/组件角度对组成信息系统的分系统的各个安全技术的检查/测评要求进行详细说明的标准，对从分系统角度了解信息系统安全等级保护提供帮助，对按等级保护要求进行信息系统分系统安全技术的检查/测评提供指导。信息系统分系统安全技术检查/测评包括组成信息系统的各个分系统（操作系统、网络系统、数据库管理系统、应用软件系统、硬件系统）的安全技术的检查/测评。其标准的编写应满足下列要求：

——检查/测评全面要求：应对进行安全技术检查/评估的信息系统分系统的运行、使用的环境、条件要求进行全面的说明；

——检查/测评分等级要求：应对照相应的系统分系统的安全技术要求，对进行安全技术检查与评估的信息系统分系统的每一个安全保护等级的安全功能技术和安全保证技术的检查/测评要求进行说明。

6.4.4.2 信息安全产品安全技术检查/测评

信息安全产品是实现信息系统安全的基础和前提。信息安全产品的检查/测评是指对每一个产品所实现的安全技术进行的检查/测评。信息安全产品分为信息技术产品和信息安全专用产品。其作用和标准编写要求分别是：

a) 信息技术产品安全技术检查/测评

信息技术产品安全技术的检查/测评是指对信息系统固有的信息技术产品（IT 产品）安全技术的检查/测评。适用于信息系统安全等级保护的信息技术产品安全技术检查/测评标准的编写应满足下列要求：

——检查/测评环境和条件要求：应对进行检查/测评的信息技术产品的运行、使用的环境和条件要求有全面的说明；

——检查/测评分等级要求：应根据信息技术产品安全功能技术和安全保证技术的分等级要求，对信息技术产品所具有的安全保护等级的安全功能技术和安全保证技术的安全检查/评估要求进行说明。

b) 信息安全专用产品安全检查/测评

信息安全专用产品的检查/测评是指对为增强信息系统的安全性在信息系统中增加的安全产品，如防火墙、入侵检测等的测评。适用于信息系统安全等级保护的信息安全专用产品安全技术检查/测评标准的编写应满足下列要求：

——检查/测评环境和条件要求：应对进行检查/测评的信息安全专用产品的运行、使用的环境和条件要求有全面的说明；

——外部安全功能和性能检查/测评：对信息安全专用产品应实现的外部安全功能和性能的检查/测评要求进行全面的说明；

——分等级外部安全功能和性能检查/测评要求：可根据各个产品外部安全功能分等级的具体情况，对所需要的安全等级的外部安全功能和性能的检查/测评要求进行说明；可分等级，也可不分等级或只有某些等级；

——安全技术检查/测评分等级要求：应根据信息安全专用产品安全功能技术的分等级要求，对信息安全专用产品所具有的安全保护等级的安全功能技术和安全保证技术的安全检查/评估要求进行说明。

6.4.4.3 安全管理检查/测评

a) 安全系统工程管理检查/评估

信息安全系统工程管理检查/评估标准的编写应满足下列要求：

——检查/测评环境和条件要求：应对进行评估的信息系统的安全工程的管理的环境与条件进行全面说明；

——检查/测评分等级要求：应对每一个安全保护等级的信息系统的安全工程管理的检查与评估进行说明。

b) 安全系统运行管理检查/评估

信息系统安全系统运行管理的检查/评估标准的编写应满足下列要求：

——检查/测评环境和条件要求：应对进行检查/测评的信息系统安全系统管理的环境与条件的全面说明；

——检查/测评分等级要求：应对每一个安全保护等级的信息系统的安全系统管理的检查与评估进行说明。

6.4.5 实施指导类标准

实施指导类标准是指为按等级保护要求实现信息安全系统的建设、检查/评估、运行控制和管理所应遵循的标准。实施指导类标准的编写应满足下列要求：

——安全实施全面要求：应从系统角度，对信息安全系统的建设、检查/评估、运行控制等各个环节所涉及的安全技术和安全管理的方法和措施进行全面说明；

——安全实施分等级要求：应从系统角度，对为各个安全保护等级的信息安全系统的建设、检查/评估、运行控制等各个环节所涉及的安全技术和安全管理的方法和措施分别进行说明。

6.4.6 各应用领域实施指导方案

各应用领域实施指导方案是指，以有关政策法规和标准为基本依据，根据各个应用领域的特点所制定的为本应用领域设计信息安全系统提供指导的方案。各应用领域实施指导方案的设计应满足下列要求：

——安全实施全面要求：安全实施指导方案应对本应用领域信息安全系统的实施方案进行全面说明；

——安全实施分等级要求：安全实施指导方案应对本应用领域每一个安全保护等级的信息安全系统的实施方案分别进行说明。

7　信息系统安全等级保护管理体系

7.1　信息系统安全工程管理

7.1.1　目标

安全工程管理的目标是，对按照等级保护要求开发的信息安全系统的整个开发过程实施管理，确保所开发的安全系统达到预期的安全要求。

信息系统安全工程的管理者应根据等级保护的总体要求，制定工程实施计划，并采取必要的行政措施和技术措施，确保工程实施按计划进行。

当信息系统安全的开发与信息系统的开发同步进行时，安全系统的工程管理应与信息系统的工程管理综合考虑并同步进行。当信息系统安全的开发是在已有的信息系统之上采用加固的方法实现时，安全系统的工程管理应独立进行。无论是哪种情况，安全系统的工程管理都应根据对安全系统开发的具体要求采取必要的措施，以保证所开发的安全系统的安全性达到所要求的目标。

7.1.2　内容

安全系统工程管理的内容包括：

a)　工程管理计划

工程管理计划应明确：

——工程的安全目标；

——工程管理的目标和范围。

b)　工程资格保障

工程资格保障包括：

——对工程建设的合法性要求；

——对承建单位及协作单位的资质要求；

——对承建单位人员及协作单位人员的资质要求；

——对商业化产品的要求；

——对工程监理的要求；

——对密码管理的要求。

c)　工程组织保障

工程组织保障包括：

——对所组织的系统工程过程的明确定义和不断改进；

——对系列产品进化的管理；

——对系统工程支持环境的管理；

——对相关人员的培训和管理；

——与安全产品供应商的协调等。

d)　工程实施管理

工程实施管理包括：

——对预期的系统安全特性的控制；

——对与系统安全有关的影响（运行、商务和任务能力）进行识别与评估；

——对与系统运行相关的安全风险进行评估；

——对来自人为的、自然的威胁进行评估；

——对整个系统脆弱性进行评估；

——建立保证论据、协调安全关系、监视安全态势、提供安全输入、指定安全要求以及验证和证实安全性等。

e)　项目实施管理

项目实施管理包括：

——项目质量保证；

——项目配置管理；

——项目风险管理；

——项目技术活动计划；

——项目技术活动监控等。

7.1.3 工程管理分等级要求

工程管理的分等级要求应包括如下内容：

a) 工程管理计划：信息安全系统开发的工程管理者，应按 7.1.2a）的要求，根据不同安全等级的安全需求，制定不同安全等级的安全系统开发的工程管理计划，并以文档形式说明工程管理计划的详细内容；

b) 工程资格保障：信息安全系统开发的工程管理者，应按 7.1.2b）的要求，根据不同安全等级的安全需求，从以下方面确保工程资格保障达到相应安全等级的要求：

——对工程建设的合法性要求；

——对承建单位及协作单位的资质要求；

——对承建单位人员及协作单位人员的资质要求；

——对商业化产品的要求；

——对工程监理的要求；

——队密码管理方面的要求；

——以文档形式说明工程资格保障的详细内容；

c) 工程组织保障：信息安全系统开发的工程管理者，应按 7.1.2c）的要求，根据不同安全等级的安全需求，从以下方面确保工程的组织保障达到相应安全等级的要求：

——对组织过程的要求；

——对系列产品的要求；

——对工程支持环境的要求；

——对相关人员的管理要求；

——对与安全产品供应商的协调的要求；

——以文档形式说明工程组织保障的详细内容。

d) 工程实施管理：信息安全系统开发的工程管理者，应按 7.1.2 d）的要求，根据不同安全等级的安全需求，从以下方面确保工程的实施管理达到相应安全等级的要求：

——对预期的系统安全特性的控制；

——对与系统安全有关的影响（运行、商务和任务能力）的识别与评估；

——对与系统运行相关的安全风险的评估；

——对来自人为的、自然的威胁的评估；

——对整个系统脆弱性的评估；

——对建立保证论据、协调安全关系、监视安全态势、提供安全输入、指定安全要求及验证和证实安全性等方面的要求；

——文档形式说明工程实施管理的详细内容。

e) 项目实施管理：信息安全系统开发的工程管理者，应按 7.1.2 e）的要求，根据不同安全等级的安全需求，从以下方面确保项目的实施管理达到相应安全等级的要求：

——对项目质量保证的要求；

——对项目配置管理的要求；

——对项目风险管理的要求；

——对项目技术活动计划的要求；

——对项目技术活动监控的要求；

——以文档形式说明项目实施管理的详细内容。

7.2 安全系统运行管理

7.2.1 目标

安全系统运行管理的目标是，通过对按照等级保护要求开发的信息安全系统的运行过程，按照相应的安全保护等级的要求实施安全管理，确保其在运行过程中所提供的安全功能达到预期的安全要求。

安全系统运行管理的要求是在安全系统设计和实现过程中，根据下列需要产生的：

——作为实现安全系统某一安全功能或某些安全功能的技术手段的保证措施；

——作为实现安全系统某一安全功能或某些安全功能的非技术手段。

安全系统的设计者应以文档形式说明对安全系统的运行如何进行管理，并详细描述每一项管理措施对系统安全性所起的作用。

安全系统的运行是与信息系统的运行密不可分的。这里所描述的系统安全管理仅包含与安全系统的安全功能相关的管理，并非与信息系统运行相关的所有管理。

7.2.2 内容

信息系统运行管理的内容包括：

a) 安全系统管理计划

制定信息安全系统的安全管理计划。安全管理计划应详细描述为确保安全系统的安全运行，在安全管理方面所应达到的目标。

b) 管理机构和人员配备

设置必要的安全管理机构，配备必须的安全管理人员，主要包括：

——管理机构设置：设置相应的安全管理机构（行政管理机构、安全管理中心、分中心等）；

——管理人员配备：为各安全管理机构配备必要的安全管理人员，明确人员职责，及人员之间的相互关系；

——领导负责：安全管理的行政机构要有有关领导分工负责，并统一管理信息系统的安全管理工作。

c) 规章制度

制定各种必要的规章制度，主要包括：

——机房人员出、入管理制度；

——机房内部管理制度；

——安全管理中心管理制度；

——应急计划和应急处理制度。

——安全系统运行操作制度、操作规程，及相应的发现违规操作措施。

d) 人员审查与管理

对人员的审查与管理，主要包括：

——人员审查：对各类人员（一般用户、系统管理员、系统安全员、系统审计员等）进行必要的审查；

——人员岗位职责：明确各类人员（一般用户、系统管理员、系统安全员、系统审计员等）的岗位职责，并对违反岗位职责规定的行为应有监督和查处措施；

——人员安全档案：建立人员安全技术档案，记录各类人员的违规操作情况，并按规定做必要的处理。

e) 人员培训、考核与操作管理

对各类人员进行严格的培训与考核，规范操作人员的行为，主要包括：

——人员培训与考核：对各类人员（一般用户、系统管理员、系统安全员、系统审计员等）按不同要求进行培训，并进行严格考核，通过考核的人员才允许上岗。

——人员操作管理：对各类操作人员（一般用户、系统管理员、系统安全员、系统审计员等）进行不同的技术培训（普及、使用、管理），并进行严格考核，通过考核的人员才允许上岗操作；

f) 安全管理中心

在一个复杂的信息系统中，安全管理中心是对分布于信息系统中的各种安全机制进行集中、统一管理的重要机构。安全管理中心既是一个组织管理机构，又具有浓厚的技术色彩，是管理与技术的统一体。主要包括：

——建立安全管理中心：信息安全系统可建立安全管理中心（必要时增设分中心），配备各类安全管理人员，组成安全管理小组，对信息安全系统安全机制实施统一管理；

——安全管理中心（分中心）的任务：对分布于信息系统各部分的安全机制实施统一管理，形成一个有机的整体，实现确定的安全功能。需要进行统一管理的安全机制包括：风险分析机制，安全审计机制，安全性检测机制，安全监控机制，访问控制管理机制，CA 系统管理机制（即 CA 中心），病毒防杀机制，防火墙管理机制，入侵检测机制、应急处理机制等。这些安全机制需要有专门人员或兼职人员分别负责，并组成一个安全管理小组，在既分工又协同的基础上，实施对安全机制的统一管理，收集、汇总有关信息，并通过风险分析发现系统的安全漏洞和问题，提出相应对策。

g) 风险管理

风险管理是安全管理中心的重要组成部分。风险管理贯穿信息安全系统的整个生命周期。这里主要讲的是系统运行过程中的风险管理。

风险管理收集信息系统在运行过程中以各种方式产生的与安全有关的信息，进行综合分析，发现安全威胁，制定安全对策，不断改进系统的安全性，主要包括：

——信息收集：收集系统运行中可供进行风险分析的数据信息，包括：审计信息（各个安全层面），安全性检测信息，安全监控信息，病毒信息等；

——信息分析：对收集的各类信息进行综合分析，寻找系统中存在的漏洞和/或风险，并确定相应的安全对策。

h) 密码管理

密码管理是安全管理中心的重要组成部分。凡设置密码支持的安全系统，应按照国家密码管理部门的有关规定，对密码系统实施严格的管理，主要包括：

——密钥管理：对密钥的产生、存储、认证、分发、查询、注销、归档及恢复等进行管理；

——密码服务系统管理：通过统一管理的密码服务系统，为信息系统的安全基础设施提供统一的加密/解密、签名/验证、数据摘要等密码服务功能。

7.2.3 运行管理分等级要求

信息系统运行管理的分等级要求如下：

a) 系统安全管理计划：信息安全系统运行的管理者，应按 7.2.2 a）的要求，根据不同安全等级的需要，制定不同安全等级的安全系统运行管理计划，并以文档形式说明运行管理计划的详细内容；

b) 管理机构和人员配备：信息安全系统的设计者，应按 7.2.2 b）的要求，根据不同安全等级的需要，明确不同安全等级的管理机构与人员配备的要求，设置管理机构，配备安全管理人员，明确各类人员的职责，并以文档形式对管理机构设置和人员配备要求进行详细说明。信息安全系统的运行管理者，应按照文档的要求，建立管理机构，配备管理人员；

c) 规章制度：信息安全系统的设计者，应按 7.2.2 c）的要求，根据不同安全等级的需要，明确不同安全等级的规章制度的要求，从机房人员出、入管理、机房内部管理、操作规程、安全管理中心管理、应急计划和应急处理等方面，以文档形式对建立规章制度的要求进行详细说明。信息安全系统的运行管理者，应按照文档的要求，建立相应的规章制度；

d) 人员审查与管理：信息安全系统的设计者，应按 7.2.2 d）的要求，根据不同安全等级的需要，明确不同安全等级的人员审查与管理的要求，从对各类人员（一般用户、系统管理员、系统安全员、系统审计员等）的审查、明确各类人员的岗位职责等方面，以文档形式对人员审查与管理的要求进行详细说明。信息安全系统的运行管理者，应按照文档的要求，明确相应的人员审查与管理要求，并贯彻执行；

e) 人员培训、考核与操作管理：信息安全系统的设计者，应按 7.2.2 e）的要求，根据不同安全等级的需要，明确不同安全等级的培训、考核与操作管理要求，从对人员的培训、考核及操作管理等方面，以文档形式进行详细说明。信息安全系统的运行管理者，应按照文档的要求，对相关人员进行严格的培训、考核与操作管理；

f) 安全管理中心：信息安全系统的设计者，应按 7.2.2 f）的要求，根据不同安全等级的需要，明确不同安全等级的安全管理中心的要求，从安全管理中心的建立和明确安全管理中心的任务等方面，以文档形式对安全管理中心的要求进行详细说明。信息安全系统的运行管理者，应按照文档的要求，建立安全管理中心，并按照所规定的任务发挥安全管理中心的作用；

g) 风险管理：信息安全系统的设计者，应按 7.2.2 g）的要求，根据不同安全等级的需要，明确不同安全等级的风险管理的要求，从信息收集和信息分析等方面，以文档形式对风险管理的要求进行详细说明。信息安全系统的运行管理者，应按照文档的要求，进行风险管理；

h) 密码管理：信息安全系统的设计者，应按 7.2.2 h）的要求，根据不同安全等级的需要，以文档形式对密码管理要求进行详细说明。信息安全系统的运行管理者，应按照文档的要求，进行密码管理。

7.3 信息系统安全监督检查和管理

信息系统安全监督检查和管理包括方面：

a) 安全产品的监督检查和管理：通过对安全产品进行测评，并实行市场准入许可证制度等，确保安全产品的安全性和质量要求达到规定的目标；

b) 安全系统的监督检查和管理：由国家指定的信息安全监管职能部门，通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督；

c) 长效持续的监督检查和管理：信息系统安全监督检查和管理是一项长期的持续性工作，需要制定相应的管理制度与实施规程，以确保在人员和机构等发生发生变化的情况下，仍能以规范化的要求开展工作。

8 信息系统安全等级保护技术体系

8.1 信息系统安全的基本属性

在信息安全保障的概念下，信息安全的三个基本属性的含义分别是：

a) 保密性

保密性保护是指对在信息系统中存储、传输和处理的信息及整个信息系统的保密性进行保护。保密性保护的范围包括从信息系统的物理实体、操作系统、数据库管理系统、网络系统到应用软件系统等信息系统的每一个组成部分。这些组成部分应得到应有的保护，使其不因人为的或自然的原因使信息或信息系统非授权的泄露或破坏达到不能容忍的程度。

b) 完整性

完整性保护是指对在信息系统中存储、传输和处理的信息及整个信息系统的完整性进行保护。完整性保护的范围包括从信息系统的物理实体、操作系统、数据库管理系统、网络系统到应用软件系统等信息系统的每一个组成部分。这些系统部分应得到应有的保护，使其不因人为的或自然的原因使信息或信息系统非授权的修改或破坏达到不能容忍的程度。

c) 可用性

可用性保护是指对信息系统中存储、传输和处理的信息及整个信息系统所提供的服务的可用性进行保护。可用性保护的范围包括从信息系统的物理实体、操作系统、数据库管理系统、网络系统到应用软件系统等信息系统的每一个组成部分。这些组成部分应得到应有的保护，使其不因人为的或自然的原因使系统中存储、传输或处理的信息出现延迟或其他不可用的情况，或者系统服务被破坏或被拒绝达到不能容忍的程度。

8.2 信息系统安全的组成与相互关系

信息系统通常是一个庞大而复杂的系统。一个典型的信息系统由支持软件系统运行的硬件系统（包括计算机硬件和网络硬件及其所在的环境）、对系统硬件进行管理并提供应用支持的计算机系统软件和网络系统软件、按照应用需要进行信息处理的应用软件等部分组成。这些硬件和软件共同构成一个完整的信息系统，通过对数据信息进行存储、传输和处理，提供确定的功能，完成所规定的应用。

信息系统安全是围绕信息系统的组成及其所实现的功能，对信息系统的运行及其所存储、传输和处理的信息进行安全保护所采取的措施。根据上述信息系统的组成与功能，按照五个安全组成部分进行的安全描述，将有助于全面、准确地理解信息系统安全所涉及的内容。

信息系统安全的五个安全组成部分分别从物理安全、系统安全、网络安全、应用安全和安全管理等方面对信息系统的安全进行描述。图 2 表示五个安全组成部分所涉及的内容及相互关系。

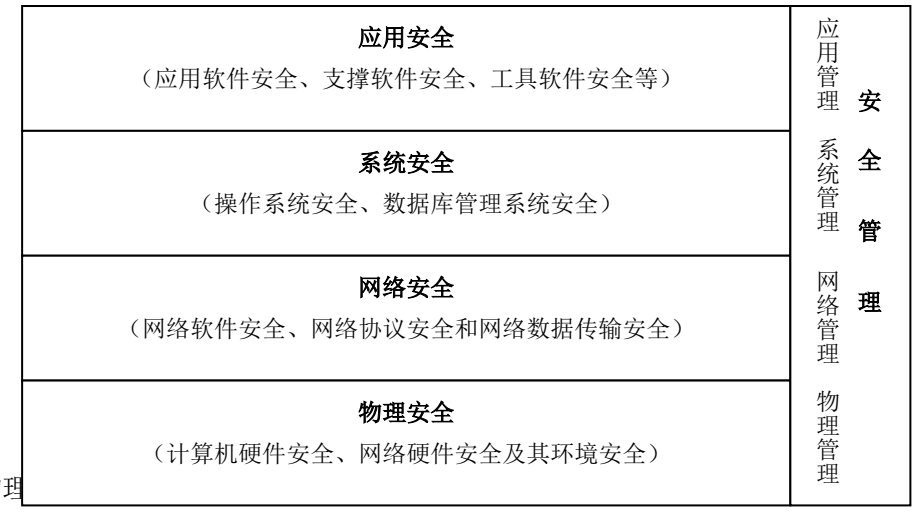


图 2 信息系统的五个安全部分的组成及相互关系

a) 物理

物理安全为信息系统的安全运行和信息的安全保护提供基本的计算机网络硬件设备、设施、介质及其环境

b) 系统安全

系统安全是指在计算机硬件及其环境安全的基础上，提供安全的操作系统和安全的数据库管理系统，以实现操作系统和数据库管理系统的安全运行以及对操作系统和数据库管理系统所存储、传输和处理数据的安全保护。

c) 网络安全

网络安全是指在网络硬件及其环境安全的基础上，提供安全的网络软件、安全的网络协议，

为信息系统在网络环境的安全运行提供支持。一方面，确保网络系统的安全运行，提供有效的网络服务，另一方面，确保在网上传输数据的保密性、完整性、可用性等。

d） 应用安全

应用安全是在物理安全、系统安全、网络安全等安全环境的支持下，实现业务应用的安全目标。应用安全主要体现在应用软件系统的安全。应用软件系统是在硬件系统、操作系统、网络系统和数据库管理系统的支持下运行的。安全的应用软件系统对数据信息所进行的存储、传输和处理需要有相应的安全措施，这些安全措施可以在应用软件系统层实现，也可以在支持其安全运行的物理安全、网络安全、操作系统安全和数据库管理系统安全中实现。

e） 安全管理

信息系统的安全管理是指对组成信息系统安全的物理安全、系统安全、网络安全和应用安全的管理，是保证这些安全达到其确定目标在管理方面所采取的措施的总称。安全管理通过对信息安全系统工程的管理和信息安全系统运行的管理来实现。信息安全系统的工程管理是指为使所开发的信息安全系统达到确定的安全目标，对整个开发过程所实施的管理；信息安全系统的运行管理是指为确保信息安全系统达到设计的安全目标，对其运行过程所实施的管理。

8.3 信息系统的安全等级

8.3.1 五个安全等级

a) 第一级

具有第一级安全的信息系统，一般是运行在单一计算机环境或网络平台上的信息系统，需要依照国家相关的管理规定和技术标准，自主进行适当的安全控制，重点防止来自外部的攻击。技术方面的安全控制，重点保护系统和信息的完整性、可用性不受破坏，同时为用户提供基本的自主信息保护能力；管理方面的安全控制包括从人员、法规、机构、制度、规程等方面采用基本的管理措施，确保技术的安全控制达到预期的目标。

按照 GB 17859-1999 中 4.1 的要求，从组成信息系统安全的五个方面对信息系统进行安全控制，既保护系统的安全性，又保护信息的安全性，采用身份鉴别、自主访问控制、数据完整性等安全技术，提供每一个用户具有对自身所创建的数据信息进行安全控制的能力。首先，用户自己应能以各种方式访问这些数据信息。其次，用户应有权将这些数据信息的访问权转让给别的用户，并阻止非授权的用户访问数据信息。

在系统安全方面，要求提供基本的系统安全运行保证，以提供必要的系统服务。在信息安全方面，重点是保护数据信息和系统信息的完整性不受破坏，同时为用户提供基本的自主信息保护能力。在安全性保证方面，要求安全机制具有基本的自身安全保护，以及安全功能的设计、实现及管理方面的基本要求。在安全管理方面，应进行基本的安全管理，建立必要的规章和制度，做到分工明确，责任落实，确保系统所设置的各种安全功能发挥其应有的作用。

b) 第二级

具有第二级安全的信息系统，一般是运行于计算机网络平台上的信息系统，需要在信息安全监管职能部门指导下，依照国家相关的管理规定和技术标准进行一定的安全保护，重点防止来自外部的攻击。技术方面的安全控制包括采用一定的信息安全技术，对信息系统的运行进行一定的控制和对信息系统中所存储、传输和处理的信息进行一定的安全控制，以提供系统和信息的一定强度保密性、完整性和可用性；管理方面的安全控制包括从人员、法规、机构、制度、规程等方面采取一定的管理措施，确保技术的安全控制达到预期的目标。

按照 GB 17859-1999 中 4.2 的要求，从组成信息系统安全的五个方面对信息系统进行安全控制，既保护系统的安全性，又保护信息的安全性。在第一级安全的基础上，该级增加了审计与客体重用等安全要求，身份鉴别则要求在系统的整生命周期，每一个用户具有唯一标识，使用户对对自己的行为负责，具有可查性。同时，要求自主访问控制具有更细的访问控制粒度。

在系统安全方面，要求能提供一定程度的系统安全运行保证，以提供必要的系统服务。在信息安全方面，对数据信息和系统信息在保密性、完整性和可用性方面均有一定的安全保护。在安全性保证方面，要求安全机制具有一定的自身安全保护，以及对安全功能的设计、实现及管理方面的一定要求。在安全管理方面，要求具有一定的安全管理措施，健全各项安全管理的规章制度，对各类人员进行不同层次要求的安全培训等，确保系统所设置的各种安全功能发挥其应有的作用。

c) 第三级

具有第三级安全的信息系统，一般是运行于计算机网络平台上的信息系统，需要依照国家相关的管理规定和技术标准，在信息安全监管职能部门的监督、检查、指导下进行较严格的安全控制，防止来自内部和外部的攻击。技术方面的安全控制包括采用必要的信息安全技术，对信息系统的运行进行较严格的控制和对信息系统中存储、传输和处理的信息进行较严格的安全控制，以提供系统和信息的较高强度保密性、完整性和可用性；管理方面的安全控制包括从人员、法规、机构、制度、规程等方面采取较严格的管理措施，确保技术的安全控制达到预期的目标。

按照 GB 17859-1999 中 4.3 的要求，从组成信息系统安全的五个方面对信息系统进行安全控制，既保护系统安全性，又保护信息的安全性。在第二级安全的基础上，该级增加了标记和强制访问控制要求，从保密性保护和完整性保护两方面实施强制访问控制安全策略，增强了特权用户管理，要求对系统管理员、系统安全员和系统审计员的权限进行分离和限制。同时，对身份鉴别、审计、数据完整性、数据保密性和可用性等安全功能均有更进一步的要求。要求使用完整性敏感标记，确保信息在网络传输中的完整性。

在系统安全方面，要求有较高程度的系统安全运行保证，以提供必要的系统服务。在信息安全方面，对数据信息和系统信息在保密性、完整性和可用性方面均有较高的安全保护，应有较高强度的密码支持的保密性、完整性和可用性制。在安全性保证方面，要求安全机制具有较高程度的自身安全保护，以及对安全功能的设计、实现及管理的较严格要求。在安全管理方面，要求具有较严格的安全管理措施，设置安全管理中心，建立必要的安全管理机构，按要求配备各类管理人员，健全各项安全管理的规章制度，对各类人员进行不同层次要求的安全培训等，确保系统所设置的各种安全功能发挥其应有的作用。

d) 第四级

具有第四级安全的信息系统，一般是运行在限定的计算机网络平台上的信息系统，应依照国家相关的管理规定和技术标准，在信息安全监管职能部门的强制监督、检查、指导下进行严格的安全控制，重点防止来自内部的越权访问等攻击。技术方面的安全控制包括采用有效的信息安全技术，对信息网络系统的运行进行严格的控制和对信息网络系统中存储、传输和处理的信息进行严格的安全控制，保证系统和信息具有高强度的保密性、完整性和可用性；管理方面的安全控制包括从人员、法规、机构、制度、规程等方面采取严格的管理措施，确保技术的安全控制达到预期的目标，并弥补技术方面安全控制的不足。

按照 GB 17859-1999 中 4.4 的要求，从组成信息系统安全的五个方面对信息系统进行安全控制，既保护系统的安全性，又保护信息的安全性。在第三级安全的基础上，该级要求将自主访问控制和强制访问控制扩展到系统的所有主体与客体，并包括对输入、输出数据信息的控制，相应地其他安全要求，如数据存储保护和传输保护也应有所增强，对用户初始登录和鉴别则要求提供安全机制与登录用户之间的“可信路径”。本级强调通过结构化设计方法和采用“存储隐蔽信道”分析等技术，使系统设计与实现能获得更充分的测试和更完整的复审，具有更高的安全强度和相当的抗渗透能力。

在系统安全方面，要求有更高程度的系统安全运行保证，以提供必要的系统服务。在信息安全方面，对数据信息和系统信息在保密性、完整性和可用性方面均有更高的安全保护，应有

更高强度的密码或其它相当安全强度的安全技术支持的保密性、完整性和可用性机制。在安全性保证方面，要求安全机制具有更高的自身安全保护，以及对安全功能的设计、实现及管理的更高要求。在安全管理方面，要求具有更严格的安全管理措施，设置安全管理中心，建立必要的安全管理机构，按要求配备各类管理人员，健全各项安全管理的规章制度，对各类人员进行不同层次要求的安全审查和培训等，确保系统所设置的各种安全功能发挥其应有的作用。对于某些从技术上还不能实现的安全要求，可以通过增强安全管理的方法或通过物理隔离的方法实现。

e) 第五级

具有第五级安全的信息系统，一般是运行在限定的局域网环境内的计算机网络平台上的信息系统，需要依照国家相关的管理规定和技术标准，在国家指定的专门部门、专门机构的专门监督下进行最严格的安全控制，重点防止来自内外勾结的集团性攻击。技术方面的安全控制包括采用当前最有效的信息安全技术，以及采用非技术措施，对信息系统的运行进行最严格的控制和对信息系统中存储、传输和处理的信息进行最严格的安全保护，以提供系统和信息的最高强度保密性、完整性和可用性；管理方面的安全控制包括从人员、法规、机构、制度、规程等方面采取最严格的管理措施，确保技术的安全控制达到预期的目标，并弥补技术方面安全控制的不足。

按照 GB 17859-1999 中 4.5 的要，从组成信息系统安全的五个方面对信息系统进行安全控制，既保护系统安全性，又保护信息的安全性。在第四级安全的基础上，该级提出了可信恢复的要求，以及要求在用户登录时建立安全机制与用户之间的“可信路径”，并在逻辑上与其它通信路径相隔离。本级重点强调“访问监控器”本身的可验证性；要求访问监控器仲裁主体对客体的所有访问；要求访问监控器本身是抗篡改的，应足够小，能够分析和测试，并在设计和实现时，从系统工程角度将其复杂性降低到最小程度。

系统安全方面，要求有最高程度的系统安全运行保证，以提供必要的系统服务。在信息安全方面，对数据信息和系统信息在保密性、完整性和可用性方面均有最高的安全保护，应有最高强度的密码或其它相当安全强度的安全技术支持的保密性、完整性和可用性机制。在安全性保证方面，要求安全机制具有最高的自身安全保护，以及对安全功能的设计、实现及管理的最高要求。在安全管理方面，要求具有最严格的安全管理措施，设置安全管理中心，建立必要的安全管理机构，按要求配备各类管理人员，健全各项安全管理的规章制度，对各类人员进行不同层次要求的安全审查和培训等，确保系统所设置的各种安全功能发挥其应有的作用。

8.3.2 安全保护等级的确定

8.3.2.1 按部门重要性确定信息系统的总体安全需求等级

按照一个单位的信息系统所承载的业务应用软件系统所管理和控制的相关资源（含信息资源和其它资源）的重要性，根据公通字[2004]66 号文件的规定，可以定性地对该单位的信息系统应具有的总体安全保护要求进行评估，确定目标信息系统需要进行保护的等级。66 号文件所规定的安全等级划分，是在假定安全威胁相同的情况下，从国家利益出发考虑信息系统资产价值（重要性）的角度提出的安全需求。在具体进行安全需求等级的确定时，还应充分考虑该单位自身的安全要求。以下是对信息系统的总体安全需求等级进行划分的基本原则：

a) 一级安全信息系统

一级安全适用于一般的信息和信息系统，其保密性、完整性和可用性受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益。该类信息系统所存储、传输和处理的信息从总体上被认为是公开信息。

b) 二级安全信息系统

二级安全适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和

信息系统，其保密性、完整性和可用性受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害。该类信息系统所存储、传输和处理的信息从总体上被认为是一般信息。

c） 三级安全信息系统

三级安全适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其保密性、完整性和可用性受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害。该类信息系统所存储、传输和处理的信息从总体上被认为是重要信息。

d） 四级安全信息系统

四级安全适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，其保密性、完整性和可用性受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害。该类信息系统所存储、传输和处理的信息从总体上被认为是关键信息。

e） 五级安全信息系统

五级安全适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其保密性、完整性和可用性受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。该类信息系统所存储、传输和处理的信息从总体上被认为是核心信息。

8.3.2.2 按资产价值和威胁确定信息系统的安全保护等级

a） 确定信息系统安全保护等级的方法和步骤

在按 8.3.2.1 的原则确定信息系统总体安全需求等级的基础上，为了实施具体的安全保护，需要进一步确定信息系统的安全保护等级。以下是可供参考的对信息系统的安全保护等级进行划分的方法和步骤。

第一步，根据确定信息系统的总体安全需求等级过程中对信息和信息系统安全保护需求的分析，明确信息系统的安全保护需求是否需要进一步划分安全域。如果不需要划分安全域，则以下的工作以信息系统为基本单元进行，如果需要划分安全域，则以下的工作在划分和确定安全域以后，以安全域为基本单元进行。

第二步，对目标信息系统（安全域）及其相关设施的资产价值及该信息系统（安全域）可能受到的威胁进行评估，确定其相应的资产价值级别和威胁级别，并据此确定目标信息系统（安全域）应具有的安全保护等级。

第三步，按照确定的安全保护等级，从等级保护的相关标准中选取对应等级的安全措施（包括技术措施和管理措施），用系统化方法设计具有相应安全保护等级的安全子系统，并对设计好的安全子系统的脆弱性进行评估。

第四步，用风险分析的方法对已经设计好安全子系统的目标信息系统（安全域）的资产价值、安全威胁和脆弱性进行评估，确定该信息系统（安全域）具有的剩余风险。如果其剩余风险从总体上是可接受的，则所确定的信息系统（安全域）的安全保护等级即为该信息系统（安全域）最终的安全保护等级，并可按照所设计的安全子系统进行目标信息系统的安全建设。如果其剩余风险是不可接受的，或者有些安全措施明显的超过保护需求，则应对安全子系统的相关安全措施进行调整，再对调整后的信息系统（安全域）的脆弱性进行评估，得到新的剩余风险。如此循环，直至剩余风险可接受为止。

第五步，再根据安全措施的调整情况，对照等级保护的相关标准中不同安全保护等级的安全技术和安全管理的要求，确定目标信息系统（安全域）的最终安全保护等级。对于一个大型的复杂信息系统，通常在不同的范围需要有不同的安全保护，从而需要引进安全域的概念。

b） 确定信息系统安全保护等级的基本思想

在资产价值级别和威胁级别明确的前提下，确定信息系统（安全域）安全保护等级的基本思想是：在资产价值级别与威胁级别相同的情况下，该级别则为信息系统（安全域）的安全保护等级；在资产价值级别大于威胁级别的情况下，以威胁级别作为信息系统（安

全域）的安全保护等级；在资产价值级别小于威胁级别的情况下，以资产价值级别作为信息系统（安全域）的安全保护等级。

8.4 信息系统安全等级保护基本框架

8.4.1 信息系统安全保护总体框架

根据我国当前的具体情况（主要是电子政务信息系统的情况，也适用于其它应用领域），按照网络环境的不同，信息系统及其安全防护的总体框架如图 3 所示。

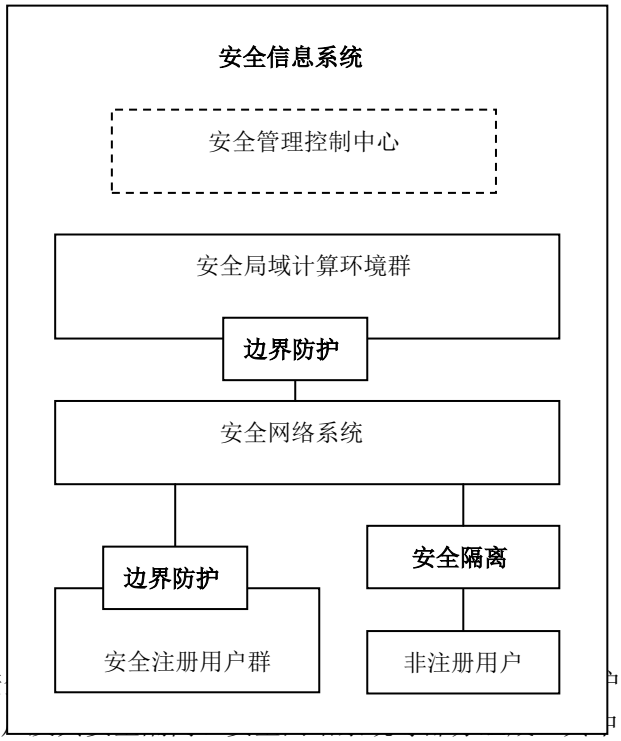


图 3 表示，一个安 户、安全注册用户群及其边界防护、非注册用 户，注册用户作为系统的可信组成部分，需要进行边界防护，非注册用户是系统的不可信组成部分，需要进行安全隔离。安全隔离通常采用

图 3 信息系统安全保护总体框架

行防护，防止内部数据非法流出，必要时也可以采用物理上断开连接的方法进行安全保护。安全网络系统是信息系统进行数据安全传输的重要组成部分，确保网上数据传输的保密性、完整性、可用性等。

8.4.2 信息系统安全等级保护的基本原理和方法

8.4.2.1 等级保护的基本原理

实现信息系统安全等级保护的基本原理是：根据信息系统所承载的业务应用的不同安全需求，采用不同的安全保护等级，对不同的信息系统或同一信息系统中的不同安全域进行不同程度的安全保护，以实现对信息系统及其所存储、传输和处理的数据信息在安全保护方面，达到确保重点，照顾一般，适度保护，合理共享的目标。

8.4.2.2 等级保护的基本方法

a) 分区域分等级安全保护

对于一个庞大而复杂的信息系统，其中所存储、传输和处理的数据信息会有不同的安全保护需求，因而不能采用单一等级的安全保护机制实现全系统的安全保护，应分区域分等级进行安全保护。分区域分等级保护体现了信息安全等级保护的核心思想。

分区域分等级安全保护的基本思想是：对于信息系统中具有不同安全保护需求的信息，在对其实现按保护要求相对集中地进行存储、传输和处理的基础上，通过划分保护区域，实现不同区域不同等级的安全保护。这些安全区域并存于一个信息系统之中，可以相互独立，也可以

相互嵌套（较高等级的安全域嵌套于较低等级的安全域中）。每一个安全域是一个相对独立的运行和使用环境，同时又是信息系统的不可缺少的组成部分。安全域之间按照确定的规则实现互操作和信息交换。图 4 和图 5 给出了安全域之间相互嵌套关系的两种极端情况的表示。

图 4 是五级全部嵌套的完全嵌套安全域关系的示意图。

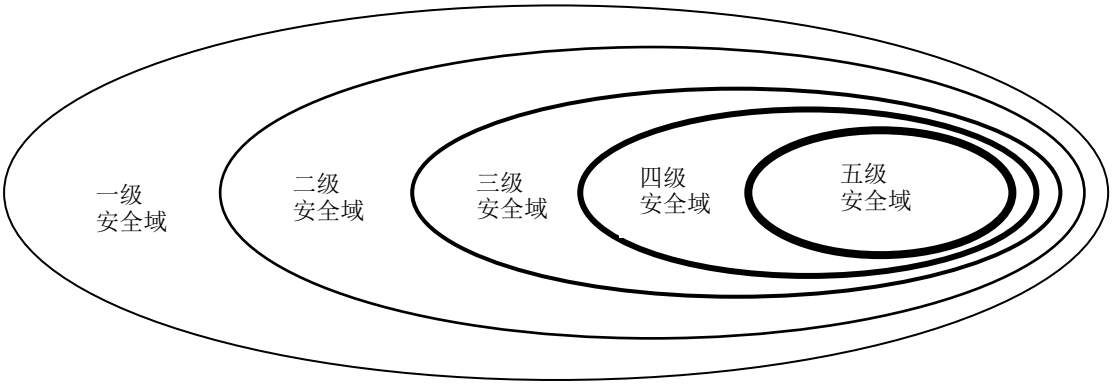


图 5 是五级全不嵌套的完全并列的安全域关系的示意图。

图 4　具有完全嵌套关系的安全域示意图

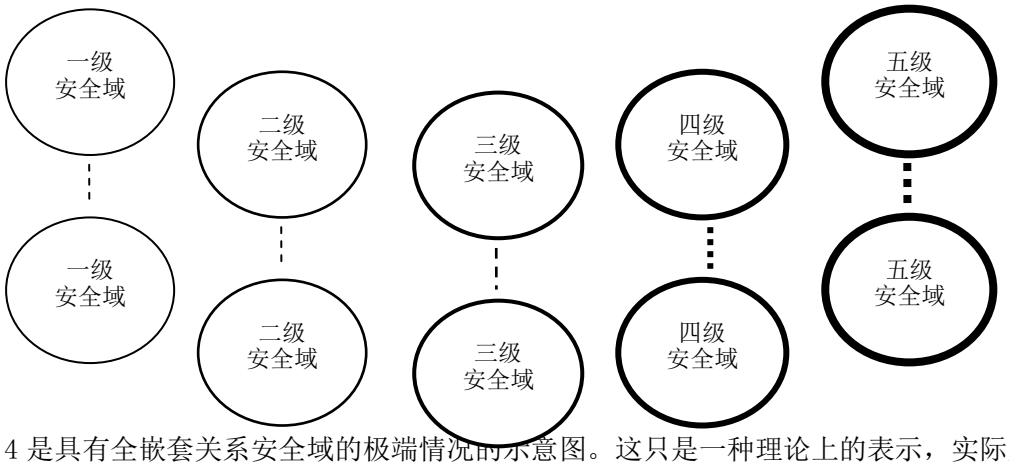


图 4 是具有全嵌套关系安全域的极端情况的示意图。这只是一种理论上的表示，实际系统可能会只有一层嵌套或两层嵌套，或者只全嵌套并存。根据我国当前安全技术发展的水平还不能满足信息化发展需要的实际情

图 5　具有完全并列关系的安全域示意图

全域实行安全隔离的措施，以弥补技术措施的不足。

图 5 是具有全并列关系安全域的极端情况的示意图，是各个级别安全域不具有任何嵌套关系的示意图。实际系统可能只有其中的部分安全域其它情况。

在一个具体的信息系统中，实际情况可能千变万化，可以只有并列安全域，也可以只有嵌套安全域，或者可以既有嵌套安全域也有并列安全域。

b)　内部保护和边界防护

边界是一个十分宽泛的概念。首先，每一个信息系统都有一个外部边界（也称为大边界），其边界防护就是对经过该边界进/出该信息系统的信息进行控制。如果把我国国内的所有公共网络上运行的信息处理系统看成是一个庞大的信息系统，其边界就是对国外的网络连接接口。为了国家的利益，需要在这些边界上进行信息安全的控制，遵照我国有关法律和政策、法规的规定，允许某些信息的进/出，阻止某些信息的进/出。这种网络世界虚拟边界的控制与现实社会

中海关的进/出口控制基本思想是完全一样的。其次，在信息系统内部，每一个安全域都有一个需要进行保护的边界（也称为小边界）。其边界防护就是对经过该边界进/出该安全域的信息进行控制。按照所确定的安全需求，允许某些信息进/出该安全域，阻止某些信息进/出该安全域。按照层层防护的思想，信息安全系统的安全包括内部安全和边界防护。边界防护又分为外部边界（大边界）防护和内部边界（小边界）防护。大/小边界通过必要的安全隔离和控制措施对连接部位进行安全防护。由于采用了必要的安全隔离和控制措施，这种边界可以认为是安全的。

内部保护和边界防护体现层层防护的思想。无论是整个信息系统还是其中的安全域，都可以从内部保护和边界防护两方面来考虑其安全保护问题。尽管许多安全机制既适用于内部保护也适用于边界防护，但由于内部和边界之间的相对关系，对于整个信息系统来讲是内部保护的机制，对于一个安全域来讲可能就是边界防护。典型的边界防护可采用防火墙、信息过滤、信息交换控制等。它们既可以用于信息系统的最外部边界防护，也可以用于信息系统内部各个安全域的边界防护。入侵检测、病毒防杀是既可以用于边界防护也可以用于内部保护。身份鉴别、访问控制、安全审计、数据存储保护、数据传输保护等是内部保护常用的安全机制，也可用作对用户和信息进/出边界的安全控制。

c) 网络安全保护

网络安全保护是信息系统安全保护的重要组成部分。

在由多个服务器组成的安全局域计算环境和多个终端计算机连接组成的安全用户环境中，实现服务器之间连接/终端计算机之间连接的网络通常是称为局域网的计算机网络。这些局域网担负着服务器之间/端计算机之间数据交换的任务，其安全性对于确保相应的安全局域计算环境和安全用户环境达到所要求的安全性目标具有十分重要的作用。可以说，一个安全局域计算环境是由组成该计算环境的安全服务器及实现这些服务器连接的安全局域网共同组成的，而一个安全用户环境是由组成该用户环境的安全终端计算机及实现这些终端计算机连接的安全局域网共同组成的。按照安全域的安全一致性原理，由相同安全等级的服务器组成的安全局域计算环境需要相应安全等级的局域网实现连接，由相同安全等级的终端计算机组成的安全用户环境需要相应安全等级的局域网实现连接。

对于一个由多个安全局域计算环境和多个安全用户环境组成的安全信息系统，实现安全局域计算环境之间、安全局域计算环境与安全用户环境之间连接的网络通常是称为广域网的计算机网络。这些广域网担负着安全局域计算环境之间及安全局域计算环境与安全用户环境之间数据交换的任务，其安全性对于确保相应安全信息系统达到所要求的安全性目标具有十分重要的作用。可以说，一个安全的信息系统是由组成该信息系统的各个安全局域计算环境和安全用户环境及实现这些安全局域计算环境和安全用户环境连接的安全广域网共同组成的。

一个信息系统可能会由多个不同安全等级的安全局域计算环境和安全用户环境组成，于是，实现其连接的广域网就需要提供不同的安全性支持。这种对同一网络环境的不同安全要求通常通过采用构建虚拟网络的形式来实现。

8.5 信息系统安全等级保护基本技术

8.5.1 标识与鉴别技术

标识是区别实体身份的方法，用户标识通常由用户名和用户标识符（UID）表示，设备标识通常由设备名和设备号表示。用户标识确保系统中标识用户的唯一性，这种唯一性要求在信息系统的整个生存周期起作用，从而支持系统安全事件的可审计性；设备标识确保连接到系统中的设备的可管理性。

鉴别是确认实体真实性的方法。用户鉴别用以确认试图进入系统的用户身份的真实性，防止攻击者假冒合法用户进入系统；设备鉴别用以确认接入系统的设备身份的真实性，防止设备的非法接入。鉴别的主要特点是鉴别信息的不可见性和难以伪造。常见的鉴别技术有：

a） 口令鉴别

口令鉴别是长期以来主要使用的用户身份鉴别方法。但简单的口令容易被猜测，复杂的口令用户又难以记忆。

b） 生物特征鉴别

主要用于用户身份真实性鉴别，包括以指纹特征信息为鉴别信息的用户身份鉴别，以虹膜特征信息为鉴别信息的用户身份鉴别，具有唯一性好和难以伪造等优点。

c） 数字证书鉴别

以数字形式表示的用于鉴别实体身份的证书信息，以一定的格式存放在证书载体之中，系统通过检验证书载体中的证书信息，实现对实体身份鉴别的目的。证书信息的不可见性通常是由密码支持的安全机制实现的，也可以由其它安全机制，如采用信息隐藏技术安全机制实现。数字证书鉴别既可以用于用户身份的真实性鉴别，也可以用于设备身份的真实性鉴别。

8.5.2 访问控制技术

访问控制是通过对信息系统中主、客体之间的访问关系进行控制，实现对主体行为进行限制、对客体安全性进行保护的技术。访问控制是以授权管理为基础实现的。由系统按照统一的规则进行授权管理所实现的访问控制称为强制访问控制；由用户按照个人意愿自主进行授权管理所实现的访问控制称为自主访问控制。

a） 自主访问控制

自主访问控制是一种提供由用户对自身所创建的客体的访问权限进行控制的安全机制。这些访问权限包括允许或拒绝其它用户对该用户所创建的客体进行读、写、执行、修改、删除操作，以及授权转移等。自主访问控制的主要特点是由用户自主进行授权管理。目前常见的实现自主访问控制的方法是各种形式的访问控制表（ACL），目录表访问控制、访问控制矩阵、能力表等。

b） 强制访问控制

强制访问控制是一种提供由系统按确定的规则对每一个用户所创建的客体的访问权限进行控制的安全机制。这种访问权限包括主体对客体的读、写、修改、删除等操作。强制访问控制的主要特点是由系统安全员统一进行授权管理。强制访问控制安全策略，通过对主体访问客体的访问操作的控制，实现对客体的保密性保护和完整性保护。目前常见的强制访问控制有基于多级安全模型的访问控制和基于角色的访问控制（BRAC）。在多级安全模型中，Bell-La Padula 信息保密性模型是实现保密性保护的安全策略，Biba 信息完整性模型是实现完整性保护安全策略。而基于角色的访问控制（BRAC）则是既可以实现保密性保护，也可以实现完整性保护的安全策略。强制访问控制通常需要按照最小授权原则，对系统管理员、系统安全员和系统审计员的权限进行合理的分配和严格的管理。

8.5.3 存储和传输数据的完整性保护技术

完整性保护是对因各种原因引起的数据信息和系统破坏进行对抗的安全保护技术，包括传输数据的完整性保护和存储数据的完整性保护。由于系统的破坏实际上是对系统中的软件和数据信息的破坏，所以系统破坏可以归结为是信息破坏。实现完整性保护的安全技术和机制包括一般的校验码机制（如奇偶校验、海明校验等）、密码系统支持的校验机制、隐藏信息技术支持的纠错机制等。访问控制、身份鉴别、边界隔离与防护等实际上也都是与完整性保护有关的安全技术和机制。

8.5.4 存储和传输数据的保密性保护技术

保密性保护是对因各种原因引起的信息和系统的非法泄露进行对抗的安全保护技术，包括数据传输的保密性保护、数据存储的保密性保护。由于系统的非法泄露实际上是对系统中的软件和数据信息的泄露，所以系统泄露同样可以归结为是信息泄露。实现保密性保护的安全技术和机制主要包括密码系统支持的加密机制、隐藏信息技术支持的信息保护机制等。访问控制、

身份鉴别、边界隔离与防护等实际上也都是与保密性保护有关的安全技术和机制。

8.5.5 边界隔离与防护技术

边界隔离与防护是一种适用于信息系统边界（也称网络边界）安全防护的安全技术，主要包括防火墙、入侵检测、防病毒网关、非法外连检测、网闸、逻辑隔离、物理隔离、信息过滤等，用于阻止来自外部网络的各种攻击行为。使用边界隔离与防护技术进行安全防护首先要有明确的边界，包括整个信息系统的外部边界和信息系统中各个安全域的内部边界。

8.5.6 系统安全运行及可用性保护技术

为了确保信息系统的安全运行，确保信息系统中的信息及信息系统所提供的安全功能达到应有的可用性要求，除了上述信息安全保护技术和边界防护技术外，还应提供以下安全技术：

a) 安全审计技术

对信息安全系统运行过程中的每一个安全相关事件，应提供审计支持。审计机制应能及时发现并记录各种与安全事件有关的行为，成功的或失败的，并根据不同安全等级的要求，对发现的安全事件作出不同的处理。

b) 安全性检测分析技术

对运行中的信息系统，应定期或不定期进行信息系统安全性检测分析，发现存在的问题和漏洞。信息系统安全性检测分析机制应提供对信息系统的各个重要组成部分，如硬件系统、操作系统、数据库管理系统、应用软件系统、网络系统的各关键设备、设施，以及电磁泄露发射等，提供安全性检测分析功能。高安全等级的信息系统应由安全机制管理控制中心集中管理系统安全性检测分析功能。

c) 系统安全监控技术

对运行中的信息系统，应实时地进行安全监控，及时发现并处理各种攻击和入侵。信息系统安全监控机制应通过设置分布式探测机制监测并截获与攻击和入侵有关的信息，在信息系统安全机制管理控制中心设置安全监控集中管理机制，汇集由探测机制截获的信息，并在综合分析的基础上对攻击和入侵事件作出处理。

d) 信息系统容错备份与故障恢复技术

确保信息系统不间断运行和对故障的快速处理和恢复，是提供信息和信息系统功能可用性的基础和前提。信息系统容错、备份与故障恢复，要求对信息系统的各个重要组成部分应提供复算、热备份等容错机制，使可能出现的某些错误消除在内部，对上层应用透明；应提供信息备份与故障恢复、系统备份与故障恢复等机制，对出现的某些故障通过备份所提供的支持实现恢复。

对于重要的信息系统，通过设置主机系统的异地备份，当主机系统发生灾难性故障中断运行时，能在较短时间内启动，替代主机系统工作，使系统不间断运行，以确保业务应用的连续性。

8.5.7 密码技术

应根据信息系统安全保护的要求配置国家批准的相应密码技术。密码技术包含对称密钥密码、非对称密钥密码和单向函数。密码技术可用于实现数据加密、数字签名、身份认证、权限验证、数据完整性验证等安全需求的场合。

8.6 信息系统安全等级保护支撑平台

8.6.1 信息系统密码基础设施平台

a) 组成：由密码技术所构成的密码基础设施平台，由基于公钥基础设施（PKI）、授权管理基础设施（PMI）、密钥管理基础设施（KMI）等密码安全机制和授权管理机制等组成；

b) 功能：密码基础设施平台提供数据加/解密、数字签名/验证、数字证书签发/验证、数字信封封装/解封、数据摘要/完整性验证、会话密钥生成和存储等基础密码服务，为安全信息系统实现保密性、完整性、真实性、抗抵赖、访问控制等安全机制提供支持；

c) 分等级要求：根据不同安全等级的信息系统对密码强度的不同要求，密码基础设施平台应提供不同安全等级的安全支持。

8.6.2 信息系统应用安全支撑平台设计

a) 总体要求

利用密码基础设施平台提供的基于 PKI/PMI/KMI 技术的安全服务，采用安全中间件及一站式服务理论和技术，支持面向业务应用的各种应用软件系统安全机制的设计，实现包括真实性鉴别、访问控制、信息安全交换、数据安全传输以及数据的保密性、完整性保护等应用软件系统的安全功能，是应用软件系统安全支撑平台的设计目标。

b) 安全服务要求

应用安全支撑平台提供的安全服务主要包括：

——支持服务器端的服务：采用中间件技术，构建安全中间件模块和安全中间件系统，实现以PKI为核心的安全技术的跨平台分布式应用。

——支持客户端的服务：按照称为安全客户端套件的轻量级中间件模式，采用层次结构，按设备层、硬件接口层、驱动层、底层接口层和高层接口层，构成客户端安全的核心模块，通过密码设备驱动访问所连接的各类终端密码设备。

c) 分等级要求

根据不同安全等级的应用对安全支撑平台的不同要求，应用安全支撑平台应提供不同安全强度/等级的安全支持。

8.6.3 信息系统灾难备份与恢复平台

信息系统灾难备份与恢复平台包括：

a) 灾难备份

灾难备份是在信息系统正常运行的情况下，为确保信息系统发生灾难性故障中断运行后恢复运行所作的一系列技术准备工作。灾难备份包括：

——数据备份：用来确保系统恢复运行后原有的数据信息不丢失或少丢失；

——处理系统备份：用来确保当信息系统中断运行后能在规定的时间范围内替代原系统运行，并确保提供所需要的信息处理能力；

——本地备份：是指对组成信息系统的主机/服务器，通过设置本地备份机制，实现对数据备份和处理系统备份；

——异地备份：是指对组成信息系统的主机/服务器，通过设置异地备份机制，实现对数据和处理系统的异地备份；异地备份能对付那些由地震、水灾、战争破坏等重大破坏性灾害所引起的灾难性故障；

——网络备份：是指对组成信息系统的网络系统，通过设置备份路由或备份线路来确保当网络系统的某些部位发生故障中断运行时，备份网络能替代故障部分实现所需要的网络数据交换，而异地备份则需要有相应的网络环境支持其对原有信息系统运行的替代，可见网络备份也是处理系统备份的组成部分。

b) 灾难恢复

灾难恢复是在信息系统发生灾难性故障中断运行后所采取的一系列恢复措施。如果说灾难备份更多的是技术措施的话，灾难恢复活动则更多的是管理措施。灾难恢复的要求包括：

——制定明确的灾难恢复策略；

——制定实施灾难恢复的预案；

——灾难恢复策略应与灾难备份技术支持密切结合，或者说灾难备份所提供的技术支持是

根据灾难恢复的总体策略确定的。

——设置相应的机构和人员，并明确其相应的职责：

——灾难恢复预案应进行常规的管理和维护，对相关人员进行培训，并定期进行必要的演练。

c) 分等级要求

根据信息系统所承载的业务应用的业务连续性的不同要求，灾难备份和恢复需要有不同等级的支持。灾难备份和恢复的等级与目标信息系统的安全保护等级是两个不同的概念，但是要求在实施灾难备份与恢复的过程中应按照目标信息系统安全保护等级的要求对所涉及的数据信息进行相应的安全保护。

d) 标准化要求

为了使我国信息系统的灾难备份与恢复活动规范化，有必要制定相应的灾难备份与恢复标准。

8.6.4 信息系统安全事件应急响应与管理平台

应急响应通常是指一个组织为了应对各种意外事件的发生所做的准备以及在事件发生后所采取的措施。信息系统安全事件应急响应的对象是指针对信息系统所存储、传输、处理的信息的安全事件。事件的主体可能来自自然界、系统自身故障、组织内部或外部的人为攻击等。按照信息系统安全的三个特性，可以把安全事件定义为破坏信息或信息处理系统 CIA 的行为，即破坏保密性的安全事件、破坏完整性的安全事件和破坏可用性的安全事件等。信息系统安全事件应急响应与管理平台主要包括以下方面：

a) 应急响应与管理

应急管理是指在紧急事件发生后为了维持和恢复关键的信息系统服务所进行的范围广泛的活动。从广义的范围讲，所讨论的应急响应与管理，包括业务连续性计划(BCP)、业务恢复计划(BRP)、操作连续性计划(COOP)、危机通信计划、计算机事件响应计划、灾难恢复计划 (DRP)、场所紧急计划 (OEP)等在内的活动与计划等，统称为应急计划。通过预防及恢复措施的使用，把信息系统因灾难或安全失效的停顿降到可接受的程度。

b) 应急计划

应通过分析灾难、安全失效及服务停顿的影响，制订及实施应急计划来保证系统能够在规定时间内恢复。计划应经常修改及测试和演练，并最终变成管理过程的不可分割部分。应急计划的制定应考虑：角色和职责，应急计划所涉及的平台和机构功能的类型范围，机构所面临的风险、风险发生的概率及影响，资源需求，培训需求，测试和演练进度表，以及计划维护进度表。在应急计划的制定中，应该与包括物理安全、人力资源、系统操作和紧急事件等在内的相关方面协调一致。应经常测试应急计划的每个部分，以确保计划可以在真实环境中实施。应急计划的定期检查和更新是至关重要的，应该作为机构变化管理过程的一部分，以确保新的信息能够被添加进来，应急措施能够根据需要被修订。

c) 联动要求

应急响应与管理不仅仅是一个单位和部门的事，而是各个相关的单位和部门的联动活动。为了加强中国网络安全水平建设，增强安全事件处理能力，国内成立了“中国计算机网络应急处理协调中心”，简称 CNCERT，由信息产业部互联网应急处理小组协调办公室直接领导，为各行业、部门和公司的应急响应小组协调和交流提供便利条件，同时为政府等重要部门提供应急响应服务。

d) 标准化要求

应急响应的标准化工作就是为应急响应组织自身及相互协调提供信息交互的标准接口，并且为这种协调机制的成功运转提供保证。建立信息系统应急响应与管理体系平台，应急响应标

准化工作十分重要，它是互联网应急响应体系通信协调机制的基础，同时也是应急响应联动系统正常运作的基础。这方面国际上已经做了很多工作。我国在这方面的工作则刚刚起步，还有许多事情需要做。可以参考国外的相关标准，制定出适合具体情况的信息系统安全事件应急响应与管理国家标准。

8.6.5 信息系统安全管理平台

a) 总体要求

以信息系统安全管理中心为核心的安全管理平台，是对信息系统的各种安全机制进行管理使其发挥应有安全作用的重要环节。除了进行信息系统自身的安全机制的管理外，信息系统安全管理平台应按照统一的要求向上级安全主管部门报告情况，与相关单位交流信息。信息系统安全管理平台既是一个管理机构，又具有浓厚的技术色彩，应按要求配备必要的专业人员，明确分管职责，并有统一的领导协调各方面的工作。

b) 安全机制具体配置

对于大型复杂的信息系统，各种安全机制广泛地分布于信息系统的各个组成部分。安全安全管理平台担负着对这些安全机制进行集中控制、统一配置管理和收集各类与安全有关信息的的责任，并对收集到的与安全有关的信息进行汇集和分析和风险评估，发现系统运行中与安全有关的问题，做相应处理。必要时，可以在确定的安全域设置安全管理分中心，形成多层结构的安全管理平台，共同完成对信息安全系统的管理控制。图 6 给出了单层的信息系统安全管理中心与其分布式安全机制之间的相互关系的示意图。

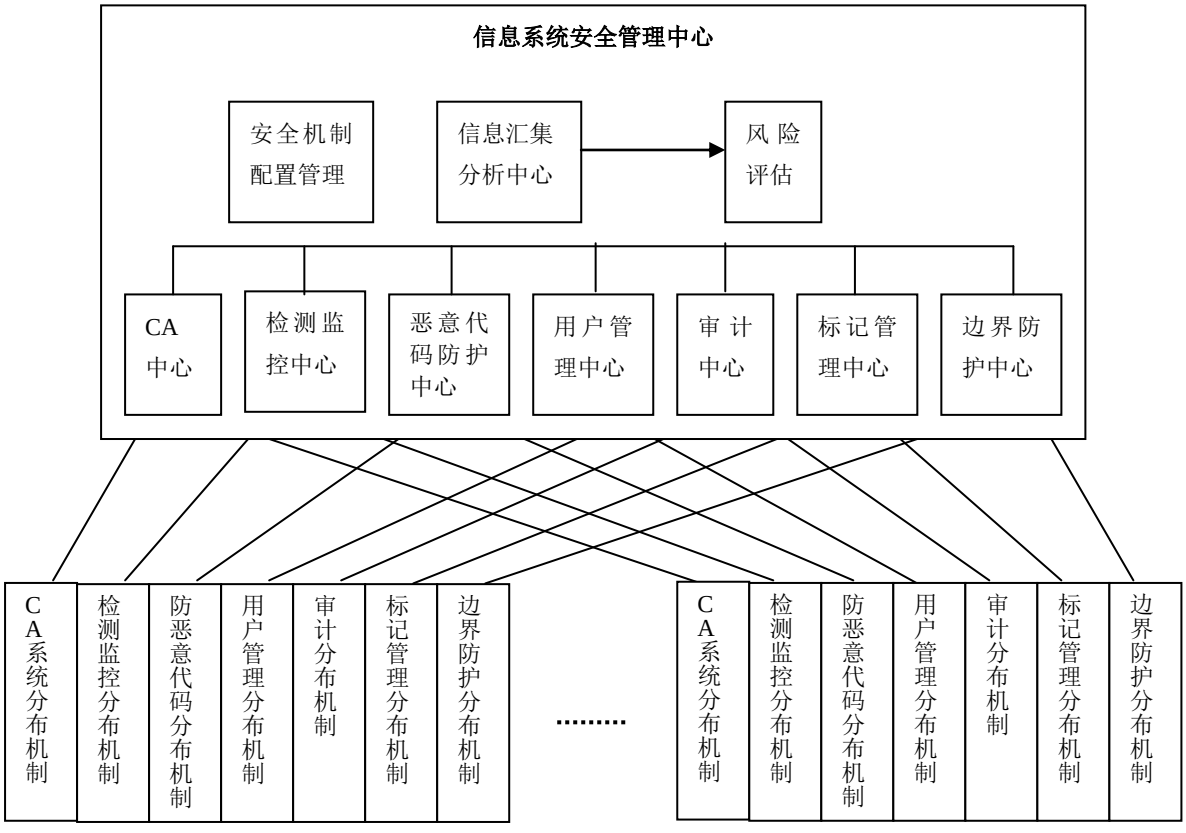


图 6 信息系统安全管理中心与分布式安全机制关系示意图

8.7 等级化安全信息系统构建技术

等级化安全信息系统是指由不同安全保护等计的安全域组成的安全信息系统。等级化安全信息系统的构建包括：

a） 等级化安全信息系统的设计与实现

等级化安全信息系统的设计和实现，应按照 8.4.2 信息系统安全等级保护的基本原理和方法，确定安全域的划分，实施信息系统及安全域的内部保护、边界防护和网络系统的安全保护；按照 8.3.2 安全保护等级的确定所描述的方法和过程，确定信息系统（安全域）的安全保护等级；根据所确定的安全保护等级，以信息系统安全等级保护相关的安全技术和安全产品标准为依据，选择相应等级的安全技术和安全产品，按系统化的设计要求，采用集成化的方法，设计和实现满足信息系统安全等级保护要求的安全信息系统。设计和实现过程还应按照系统安全工程管理的有关标准的要求，对整个工程过程进行安全管理。

b） 等级化安全信息系统的测试与评估。

等级化安全信息系统的测试与评估应按照相关标准的要求进行。系统的测试与评估应以技术和产品的测试与评估为基础。首先应对构成等级化信息系统的安全技术和产品分别进行考察/测评。考察的目的是确认其是否通过相应安全等级的测评。鉴于信息安全等级保护工作还处于初期阶段，按照等级标准的要求对产品进行测试与评估还有一个过程，所以必要时可以对所使用的安全技术和安全产品进行测试与评估，确定其是否具有所需要的安全保护等级。在技术和产品达到安全等级要求的基础上应重点从系统角度对各安全技术、产品之间的接口及连接关系，以及系统各组成部分之间安全的一致性和关联互补等所形成的系统整体安全性进行测试与评估，确定信息系统（安全域）整体上是否达到确定的安全等级的设计目标要求。

附录 A
（资料性附录）
基本概念说明

A.1 业务应用软件系统及其子系统

业务应用软件系统（通常称为应用软件系统）是信息系统中所承载的各类业务应用处理软件的总称。可以根据业务应用的不同，将业务应用软件系统划分为业务应用软件子系统。每个业务应用软件子系统能够相对独立地为一类业务应用提供支持。

A.2 信息系统及其子系统

这里所说的“信息系统”，更确切地应为“计算机网络信息系统”，是由计算机系统和/或网络系统的软硬件平台及其所支持的业务应用软件系统共同组成的对业务信息进行处理的计算机网络信息处理系统。信息系统安全等级保护是指对信息系统进行的安全等级保护。

一个信息系统平台能够支持若干个业务应用软件系统运行。每个业务应用软件系统及其支持平台，共同组成相应的业务信息系统（通常称为信息系统）。信息系统可大可小。比如，通常所说的地理信息系统、办公自动化（信息）系统、财务（信息）系统等等。

子系统是一个相对的概念，是相对于包含它的系统而言的一部分。子系统是信息系统中逻辑的或物理的一部分组成的系统。可以从不同角度对信息系统进行子系统划分。比如，从安全角度可以有信息系统的安全子系统。信息系统安全子系统是指信息系统中所有与安全相关的硬件、固件和软件所提供的安全机制和安全服务的总合，并且是按系统化要求构成的，而不是安全机制的简单堆积。又如，从业务应用角度，可以按信息系统所承载的业务应用的不同，将信息系统划分为多个不同的信息子系统（或称为业务信息子系统）。每个业务信息子系统由其业务应用软件子系统和信息系统中支持该业务应用子系统运行的计算机和/或网络的软硬件部分共同组成。

A.3 关于安全域

安全域是从安全的角度对信息系统进行的划分。按照信息安全等级保护关于保护重点的基本思想，需要根据信息系统中信息和服务的不同安全需求，将信息系统进一步划分安全域。安全域的基本特征是安全域应有明确的边界。安全域的划分可以是物理的，也可以是逻辑的，从而安全域的边界也可以是物理的或是逻辑的。一个复杂信息系统，根据其安全保护要求的不同，可以划分为数个安全域。安全域是信息系统中实施相同安全保护策略的单元。

安全域的划分以业务应用为基本依据，以数据信息保护为中心。一个业务信息系统/子系统，如果具有相同的安全保护要求，则可以将其划分为一个安全域；如果具有不同的安全保护要求，则可以将其划分为多个安全域。比如，一个数据集中存储的事务处理系统，往往集中存储和处理数据的中心主机/服务器具有比终端计算机更高的安全保护要求。这时，可以根据需要将这个系统划分为两个或多个进行不同安全保护的安全域。

根据以上关于安全域的概念和划分方法，一个信息系统可以是单一安全域（通常是比较小型的简单的信息系统），也可以是多安全域（通常是比较大型复杂的信息系统）。

本标准以安全域为基础来描述信息系统的分等级安全保护。在实施等级保护等信息系统中，安全域可以映射为整个信息系统（整个信息系统是一个安全域），也可以映射为信息系统的子系统（多个子系统构成多个安全域）。

附录 B
（资料性附录）
实施等级保护的方法

B.1　全系统同一安全等级安全保护

所谓全系统同一安全等级安全保护是指，对于一个需要进行安全等级保护的信息系统，其所存储、传输和处理的所有数据信息，在组成系统的任何部分，都需要进行相同安全保护等级的安全保护。

当所要保护的数据信息无论处于系统中的任何位置，进行任何形式的处理，都需要实施相同安全保护等级的保护时，需要按照全系统同一安全等级安全保护的方法进行系统的安全性设计，提供所要求的安全保护。

需要特别指出的是，这里所说的相同安全保护等级的安全保护是指按照 GB 17859-1999 规定的安全保护等级某一等级的要求，进行全系统的安全设计，而并非按照多级安全模型实现的强制访问控制中主、客体标记所设置的级别和范畴中的级别。因为在后者中可能出现这样的情况：实施强制访问控制的客体，当其位于信息系统的不同部位时，其作为强制访问控制基础的级别，根据需求可能会有所不同。这就如同我们在对保密文件的管理中常常规定，当文件带出单位或带到异地时需要升高文件的保密等级一样。

B.2　分系统不同安全等级安全保护

所谓分系统不同安全等级安全保护是指，对于一个需要进行安全等级保护的信息系统，其所存储、传输和处理的数据信息，可按照信息在组成信息系统的各个子系统中的不同保护要求，实施不同安全保护等级的安全保护。

当处于信息系统不同子系统中的数据信息，需要实施不同安全等级的安全保护时，需要按照子系统不同安全等级安全保护的方法进行系统的安全性设计。

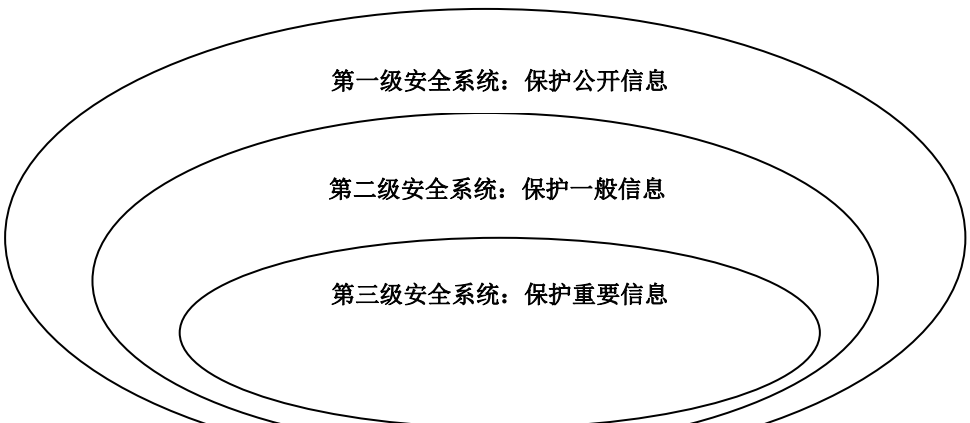
这种安全设计既可按数据服务器为单元实施安全保护，也可按网络或子网为单元实施安全保护。在有多个数据服务器的系统中，不同的数据服务器可根据其所存储和处理的数据信息的类型，提供不同的安全保护等级的安全保护。在一个具有各类数据信息的信息系统中，把数据分类存放在不同的数据服务器/网络存储器中，就可以按这种方法设计安全保护。

按网络或子网实施安全保护，通常是网络或子网具有较高安全保护等级的安全保护。这时，需要在网络或子网的前端设置边界防护，防止数据随意在内、外部之间流动。根据需要，边界防护既可对进入网络或子网的用户进行更严格的检查和认证，又可对进/出的数据信息按规定进行控制。

B.3　虚拟系统不同安全等级安全保护

在一个信息系统中，不同类型的数据往往有不同的安全保护要求。对不同类型的数据信息的安全保护，可以通过建立一个相应安全保护等级的分层虚拟安全系统来实现。

按照虚拟系统的概念，建立分层的虚拟安全系统，可实现不同类型信息的不同安全保护等级的安全保护。图 B.1 为具有三级安全的分层虚拟安全系统的示意图。



其中，对每类数据信息的保护，需要定义一个相应安全保护等级的虚拟安全系统。

这种对不同类型数据实施不同安全保护的虚拟分层思想，在实际的应用中也是常见的。比如，在一个信息系统中，对某些数据的传输进行加密保护，而对另一些数据的传输则不进行加密保护。又如，可以定义对某类数据实施自主访问控制和强制访问控制，而对另一类数据只实施自主访问控制等等。

参考文献

[1] 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（idtISO/IEC 15408-1：1999）

[2] GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求（idtISO/IEC 15408-2：1999）

[3] GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求（idtISO/IEC 15408-3：1999）

[4] GB/T 20269-2006 信息安全技术 信息系统安全管理要求

[5] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求

[6] 信息保障技术框架（IATF，3.0版），美国国家安全局发布，国家973信息与网络安全体系研究课题组组织翻译，北京中软电子出版社，2004年4月第一版

[7] NIST SP800，National Istitute of Standards and Technology, Technology and Ministriation,U.S.Department of Commerce