Broadview®
www.broadview.com.cn

“十一五”国家重点图书出版规划项目
国家信息安全等级保护系列丛书

信息安全
等级测评师
培训教程
（中级）

公安部信息安全等级保护评估中心　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

“十一五”国家重点图书出版规划项目
国家信息安全等级保护系列丛书

信息安全等级测评师培训教程

（中级）

公安部信息安全等级保护评估中心　编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本教材结合我国信息安全等级保护制度编写，是长期从事信息安全等级测评人员结合等级测评工作实践的总结，根据信息安全等级测评师（中级）岗位特点、能力要求进行编写，用以指导等级测评人员开展信息安全等级测评工作。内容包括：对信息系统安全等级保护基本要求的解读、对信息系统安全等级保护测评要求的解读、对信息系统安全等级保护测评过程指南的解读，以及提供一些在测评过程中必须提交的文档模板等。

本书为信息安全等级测评师（中级）专用教材，也可作为信息安全测评人员、信息系统运行维护人员、大专院校信息安全相关专业人员参考用书。

图书在版编目（CIP）数据

信息安全等级测评师培训教程：中级 / 公安部信息安全等级保护评估中心编著. —北京：电子工业出版社，2011.1
（安全技术大系. 国家信息安全等级保护系列丛书）
ISBN 978-7-121-12665-9

Ⅰ.①信… Ⅱ.①公… Ⅲ.①信息系统－安全技术－技术培训－教材 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2010）第 255084 号

策划编辑：毕 宁 bn@phei.com.cn
责任编辑：贾 莉
文字编辑：毕 宁
印 刷：
装 订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：16.25 字数：235 千字
印 次：2011 年 4 月第 2 次印刷
印 数：2001～3500 册 定价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

信息安全等级保护制度是国家信息安全保障工作的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。国务院法规和中央文件明确规定，要实行信息安全等级保护，重点保护基础信息安全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。

信息安全等级测评是信息安全等级保护工作的重要环节，信息系统备案单位通过委托测评机构开展等级测评，可以查找系统安全隐患和薄弱环节，明确系统与相应等级标准要求的差距和不足，有针对性地进行安全建设整改。等级测评工作涉及的信息系统范围广、政策性强，需要建立专门的测评机构专业开展测评工作，需要培养一批专门从事等级测评工作的专业技术人员。

我们结合近些年的工作实践，在公安部网络安全保卫局的指导下，编写了这本教程，对开展信息安全等级测评工作的主要内容和方法进行了介绍，供读者参考、借鉴。本教材除了适用于等级测评师培训外，还适用于信息系统运营、使用单位的运维、管理人员，有助于他们在信息系统运行维护和组织本单位系统自查过程中有针对性地开展相应工作。由于水平有限，书中难免有不足之处，敬请读者指正。

本书由公安部信息安全等级保护评估中心组织编写，在编写过程中得到国家网络与信息安全信息通报中心赵林副主任的大力支持和指导，并得到公安部网络安全保卫局重要信息系统监察处郭启全处长的关心和帮助，在此表示由衷的感谢。参加编写的有毕马宁、任卫红、李明、袁静、曲洁、罗峥、刘静、张洁昕、朱建平、张宇翔、张嫣玲、王宁等。

读者可以登录中国信息安全等级保护网 www.djbh.net，了解最新情况。

目　录

CHAPTER 1

第 1 章　信息系统安全等级保护基本要求解读

本章主要围绕《信息安全技术 信息系统安全等级保护基本要求》（以下简称《基本要求》），对其描述模型、逐级增强特点以及具体的各级安全要求进行介绍，并通过对各级安全要求的介绍，使得用户能够根据各自信息系统的等级，选择合适的安全要求进行系统保护。

1.1　概述

1.1.1　背景介绍

2004 年公安部等四部门在《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号，以下简称《实施意见》）中指出，“信息安全等级保护工作是个庞大的系统工程，关系到国家信息化建设的方方面面，这就决定了这项工作的开展必须分步骤、分阶段、有计划的实施，信息安全等级保护制度计划用三年左右的时间在全国范围内分三个阶段实施。”

信息安全等级保护工作第一阶段为准备阶段，准备阶段中重要工作之一是“加

快制定、完善管理规范和技术标准体系”。信息安全等级保护技术组依据“信息安全等级保护标准体系框架”的要求，制定了“信息安全等级保护标准化工作总体实施计划”，实施计划中要求有6个主要标准应该在2005年完成，《基本要求》标准就是这6个主要标准之一。

2007年，公安部、国家保密局、国家密码管理局和国务院信息化工作办公室（以下简称“国信办”）联合签发了《信息安全等级保护管理办法》（公通字[2007]43号，以下简称《管理办法》），规定“国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理”，“信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全职能部门对其信息安全等级保护工作进行监督管理。”

作为我国等级保护技术工作的基础性标准，《基本要求》应当吸取国际、国内先进的信息安全经验和相关内容，结合我国信息系统的安全需求和信息安全技术特点，为确保现阶段信息系统具有相应等级安全保护能力提出最基本的要求，制定出具有指导意义的安全标准文档，为规范信息系统的安全等级保护提供依据。

公安部信息安全等级保护评估中心于2004年10月接受公安部任务，开始起草《基本要求》标准，并于2005年6月，完成了标准初稿的编制，经广泛征求安全领域专家和各行业用户意见后，2005年10月完成了标准征求意见稿的第一稿，又经国信办组织的专家评审和全国信息安全标准化技术委员会（以下简称“安标委”）专家评审后于2005年11月，完成了标准征求意见稿的第三稿。2006年6月，《基本要求》的这一版本作为信息系统安全等级保护试点的工作文件在试点工作中进行试用，有力地支持了试点工作，同时，在更大范围内推广、使用。伴随着《基本要求》地广泛应用，其中的一些问题慢慢暴露出来。经过修改和完善，2007年4月，完成了标准征求意见稿的第四稿。再次经过专家评审，于2007年5月下旬完成了《基本要求》的送审稿，2007年5月经安标委专家评审后，形成《基本要求》（报批稿）。根据中华人民共和国国家标准批准发布公告2008年第10号（总第123号），《基本要求》

于2008年6月19日正式发布，2008年11月1日正式实施。

1.1.2 主要作用及特点

1. 主要作用

鉴于信息安全等级保护工作的专业性、技术性较强，《管理办法》中规定了信息系统运营、使用单位和相关单位在等级保护工作中按照或参照《基本要求》等国家、行业技术标准开展系统定级、建设、整改、测评等工作。因此，《基本要求》可以：

1）为信息系统建设单位和运营、使用单位提供技术指导

在信息系统的安全保护等级确定后，《基本要求》为信息系统的建设单位和运营、使用单位如何对特定等级的信息系统进行建设、验收、运维、自查等方面的安全保护提供技术指导。

2）为等级测评机构提供评估依据

《基本要求》为信息系统主管部门，信息系统运营、使用单位或专门的等级测评机构对信息系统现有的安全保护能力进行检测评估或等级测评提供依据。

3）为职能监管部门提供监督检查依据

《基本要求》为监管部门的监督检查提供依据，用于判断一个特定等级的信息系统是否按照国家要求进行了基本的技术防护和管理控制。

2. 主要特点

《基本要求》是针对每个等级的信息系统提出的相应安全保护要求，“基本”意味着这些要求是针对该等级的信息系统达到基本保护能力而提出的，也就是说，这些要求的实现能够保证系统达到相应等级的基本保护能力，但反过来说，系统达到相应等级的保护能力并不仅仅完全依靠这些安全保护要求。同时，《基本要求》强调的是“要求”，而不是具体实施方案或作业指导书，《基本要求》给出了系统每一个

保护方面须达到的要求，至于这种要求采取何种方式实现，不在《基本要求》的描述范围内。

1.1.3 标准定位

《基本要求》是以 GB17859 为基础的分等级信息系统的安全建设和管理系列标准之一。根据《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号），各行业的信息系统安全建设整改工作应依据《基本要求》，参照 GB/T20271—2006《信息安全技术 信息系统通用安全技术要求》、GB/T20270—2006《信息安全技术 网络基础安全技术要求》、GB/T21052—2007《信息安全技术 信息系统物理安全技术要求》、GB/T20269—2006《信息安全技术 信息系统安全管理要求》、GB/T20282—2006《信息安全技术 信息系统安全工程管理要求》等标准规范要求。

《基本要求》对每个等级的信息系统提出了相应的安全保护要求，但“基本”意味着这些要求是针对该等级的信息系统达到基本保护能力而提出的，也就是说，这些要求的实现能够保证系统达到相应等级的基本保护能力。信息系统安全防护应以落实《基本要求》为主要目标，以《基本要求》中相应级别的安全保护要求作为信息系统的基本安全需求。当信息系统有更高安全需求时，可参考《基本要求》中较高级别保护要求或《信息安全技术 信息系统通用安全技术要求》、《信息安全技术 信息系统安全管理要求》等其他标准。

《基本要求》与 GB17859 等标准存在如下关系：

- GB17859—1999 是基础性标准，《基本要求》、GB/T20269—2006、GB/T20270—2006、GB/T20271—2006 等都是在 GB17859—1999 基础上的进一步扩展。
- 依据《信息安全技术 信息系统安全保护等级定级指南》（以下简称《定级指南》）确定系统等级，以及业务信息安全性等级和业务服务保证性等级后，需要按照相应等级，根据《基本要求》选择相应等级的安全保护要求作为基本

安全需求进行系统建设实施。

- 《信息安全技术 信息系统安全保护等级测评要求》是针对《基本要求》的具体控制要求开发的测评要求，旨在强调系统按照《基本要求》进行建设完毕后，检验系统的安全保护能力是否达到相应等级的基本要求。

由此可见，《基本要求》在整个标准体系中起着承上启下的作用。

从技术内容看：

《基本要求》在 GB17859、GB/T20269—2006、GB/T20270—2006、GB/T20271—2006 等技术类标准的基础上，根据现有技术的发展水平，提出和规定了不同安全保护等级信息系统的最低保护要求，即基本安全要求，适用于指导不同安全保护等级信息系统的安全建设和监督管理。

《基本要求》的技术部分吸收了 GB 17859—1999 标准中身份鉴别、数据完整性、自主访问控制、强制访问控制、审计、客体重用（改为剩余信息保护）、标记、可信路径 8 个安全机制，并将这些机制根据各级的安全目标，扩展应用到网络层、主机系统层、应用层和数据层。

《基本要求》的技术部分弱化了原有的强制访问控制机制在第三级和第四级中的应用范围，因为现在还没有一个四级系统可以实现对内部和外部所有主体和客体的强制访问控制。因此在本标准中，仅要求强制访问控制可以根据需要在一定范围内实现子集的强制访问控制。同时《基本要求》中还弱化了在信息系统中实现安全机制结构化设计及安全机制可信性方面的要求，例如没有提出信息系统的可信恢复，但在四级系统提出了灾难备份与恢复的要求，这样的恢复措施可以保证系统的连续运行。

《基本要求》没有对隐蔽通道分析的安全机制提出要求，主要是因为该机制在信息系统中的分析和测试方法还不成熟，如果对用户和服务商提出这样的安全保护要求，恐怕难于实现。因此，可以考虑将这一要求交由相应等级的操作系统产品实现。

《基本要求》的技术部分根据实际需要增加了资源控制、入侵防范、恶意代码防

范、抗抵赖和软件容错等安全机制，同时《基本要求》也对安全管理方面作出了具体的要求。

从管理内容看：

《基本要求》的管理部分充分借鉴了 ISO/IEC 17799:2005 等国际上流行的信息安全管理方面的标准，尽量做到全方位的安全管理。

1.1.4 描述框架

在《基本要求》的框架结构上以三种分类为支撑点，自上而下分别为：类、控制点和要求项。其中，类表示《基本要求》在整体上大的分类，其中技术部分分为：物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复五类；管理部分分为：安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理五类，一共分为十类。如图 1-1 所示。

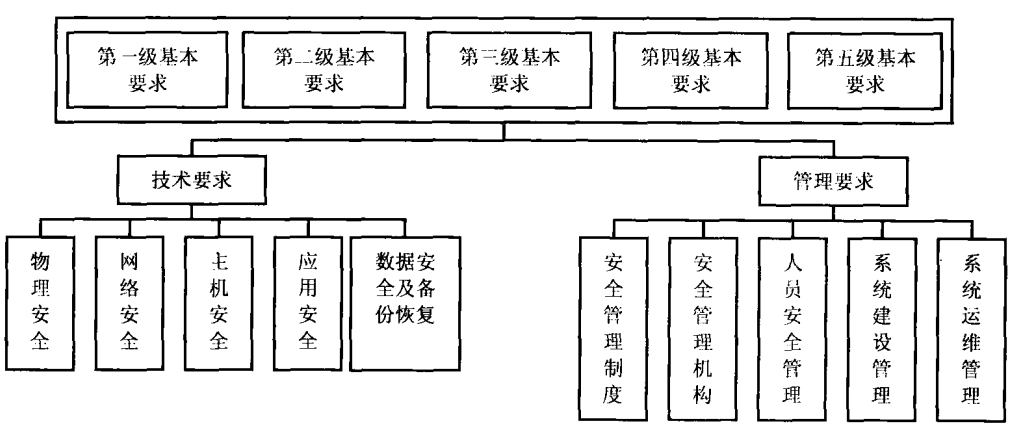

图 1-1 《基本要求》的十个类

《基本要求》的类构成了其第 5、6、7、8 章的三级标题。《基本要求》的控制点表示每个类下关键的安全功能点，如物理安全类中的物理访问控制、防火、防盗窃和防破坏都是控制点，它们构成了《基本要求》第 5、6、7、8 章的四级标题。《基本要求》

的要求项是每个控制点下提出的具体要求，如在第一级的“物理访问控制”控制点下，“机房出入口应安排专人值守，控制、鉴别和记录进入的人员。”就是具体要求。

上述描述框架如图 1-2 所示：

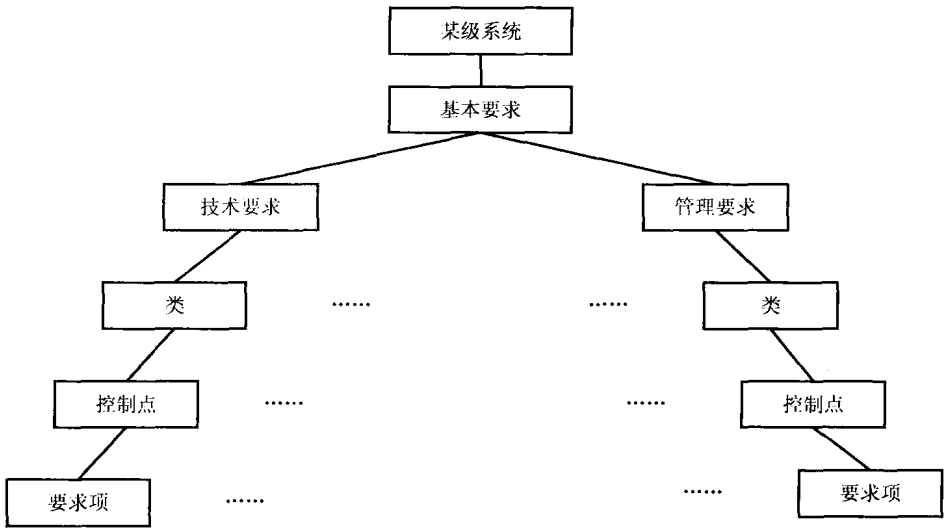

图 1-2 《基本要求》的描述框架

1.2 描述模型

1.2.1 《基本要求》形成的技术思路

无论是风险管理还是安全工程，其核心思想是要求从信息系统的安全需求出发对信息系统进行保护，《基本要求》的形成过程也沿用这种思想。

对信息系统的定级过程反映了信息系统的安全需求分析过程，详细内容参见《定级指南》。根据信息系统在国家事务中的地位、信息系统承载的业务的重要程度等因素确定了信息系统的安全保护等级，《基本要求》需要解决的问题是对于不同等级的信息系统提出安全保护要求。

《基本要求》形成的技术思路如图 1-3 所示：

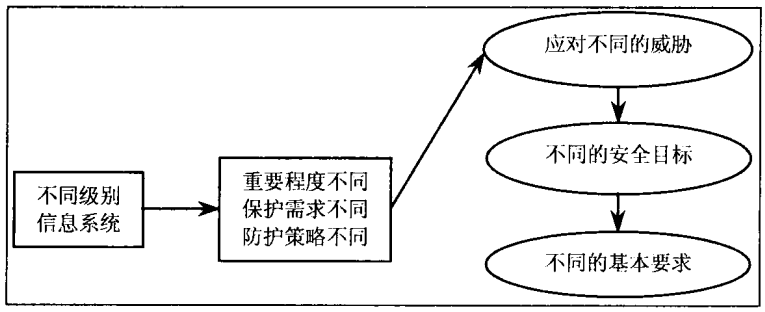

图 1-3 《基本要求》的技术思路

一般信息系统都不能对抗所有威胁，而只能对抗部分威胁，因此都具有有限的安全性，或称有条件的安全。低等级的信息系统，由于其重要性较低，面临的威胁比较少，投入一般也较少，因此低等级系统一般仅需要对抗较少、较弱的威胁，故通常低等级系统仅具有较少的安全需求和较低的保护能力；而高等级的信息系统，由于其重要性较高，受关注度和影响也相应较大，面临的威胁比较多、比较复杂，投入一般也较多，因此高等级系统一般需要对抗较多、较强的威胁，故通常高等级系统一般具有较多的安全需求和较高的保护能力。

上述分析表明，不同等级的信息系统的安全需求不同，因此采用的安全保护策略也应有所不同。基于这一思路，《基本要求》将信息系统对抗威胁能力分为对抗能力和恢复能力：

- 对抗能力——信息系统能够应对威胁的能力。
- 恢复能力——能够恢复系统原有状态的能力。

不同等级的信息系统应具有不同的对抗能力，即应能够对抗不同的威胁。在某些情况下，无法阻挡威胁对信息系统的破坏时，如果系统具有很好的恢复能力，那么即使遭到破坏，也能在很短的时间内恢复系统原有的状态。不同等级的信息系统应具有不同的恢复能力，即应能够在不同的时间内恢复系统原有的状态。

对抗能力和恢复能力构成了信息系统的安全保护能力。不同级别的信息系统应具备不同的安全保护能力，即应该具备不同的对抗能力和恢复能力。

信息系统应具有的威胁对抗能力和恢复能力进一步细化可以形成各等级的安全目标，实现这些安全目标的途径和手段就构成了各等级的基本安全要求。基本安全要求包括了基本技术要求和基本管理要求，基本技术要求主要用于对抗威胁和实现技术能力，基本管理要求主要为安全技术的实现提供组织、人员和程序等方面的保障。

1.2.2 保护对象

信息系统是信息安全等级保护的保护对象，《管理办法》将信息系统分为五级，分别为：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

1.2.3 安全保护能力

1. 定义

信息系统的安全保护能力由防护能力和恢复能力构成。

1）防护能力

信息系统的防护能力主要从信息系统能够对抗的威胁角度来衡量。不同等级系统所应对抗的威胁主要从威胁源（自然、环境、系统、人为）、动机（不可抗外力、无意、有意）、范围（局部、全局）和能力（工具、技术、资源等）四个要素来考虑。

在对威胁进行级别划分前，我们首先解释以下几个要素。

- 威胁源——是指任何能够导致非预期的不利事件发生的因素，通常分为自然（如自然灾害）、环境（如电力故障）、IT 系统（如系统故障）和人员（如心怀不满的员工）四类。
- 动机——与威胁源和目标有着密切的联系，不同的威胁源对应不同的目标有着不同的动机，通常可分为不可抗外力（如自然灾害）、无意的动机（如员工的疏忽大意）和故意的动机（如情报机构的信息收集活动）。
- 范围——是指威胁潜在的危害范畴，分为局部和整体两种情况。如病毒威胁，有些计算机病毒的传染性较弱，其危害范围是有限的；但是蠕虫类病毒则相反，它们可以在网络中以惊人的速度迅速扩散并导致整个网络瘫痪。
- 能力——主要是针对威胁源人为的情况，它是衡量攻击成功可能性的主要因素。能力主要体现在威胁源占有的计算资源的多少、工具的先进程度、人力资源（包括经验）等方面。

通过对威胁主要因素的分析，我们可以将其组合得到不同等级的威胁。

第一级，本等级的威胁是：危害范围为局部的环境或者设备故障；无意的员工失误；非专业的、个人的攻击等威胁情景。典型情况如灰尘超标（环境）、单个非重要工作站（设备）崩溃等。

第二级，本等级的威胁是：危害局部的较严重的自然事件；具备中等能力、有预设目标的威胁情景。典型情况如小规模外部组织的情报搜集等。

第三级，本等级的威胁是：危害整体的自然事件；具备较高能力、大范围的、