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

安全技术大系

信息安全
等级保护基本要求
培训教程

陆宝华　编著

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

信息安全
等级保护基本要求
培训教程

陆宝华　编著

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

内 容 简 介

《信息安全等级保护基本要求》是目前在信息系统等级确定以后，对信息系统进行安全改造、改建、加固的依据，也是测评机构对信息系统进行安全测评及国家信息安全监管部门进行监督、检查、指导的依据。本书对《信息安全等级保护基本要求》中所涉及的标准、安全模型、安全功能等知识进行了较为系统的分类介绍，并着重介绍了技术要求中的网络安全、主机安全、应用安全及数据安全方面的要求。而且对一些基本要求中的条款进行解释和说明，有的地方还提出了应该采用技术的建议。

本书对国家标准《信息安全等级保护基本要求》进行了原理性分析，具有很高的实用价值，解决了目前绝大多数相关人员读不懂标准的难题，是落实等级保护制度的必读之作。本书适合从事信息保障的各类技术人员、管理人员及大专院校相关专业的师生阅读。

图书在版编目（CIP）数据

信息安全等级保护基本要求培训教程 / 陆宝华编著. —北京：电子工业出版社，2010.9
（安全技术大系. 国家信息安全等级保护系列丛书）
ISBN 978-7-121-11547-9

I. ①信… II. ①陆… 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 156863 号

策划编辑：毕 宁
责任编辑：许 艳
印 刷：北京中新伟业印刷有限公司
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：22 字数：337 千字
印 次：2010 年 9 月第 1 次印刷
印 数：4000 册 定价：55.00 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。

序

随着我国各行各业信息化的快速发展，人们的工作、生活和各项社会活动越来越多地依赖于网络和计算机系统，为信息化保驾护航的信息安全越来越受到普遍关注。我国正在实行的信息安全等级保护制度，对于信息化状态下的国家安全、社会稳定、经济发展和人民财产保护具有十分重要的意义和作用。

与国外普遍采用的以风险管理方法来控制信息系统的安全不同，我国采用等级管理方法来控制信息系统的安全。风险管理方法的基本思想是在信息系统生存周期的各个阶段，采用风险分析的方法，分析和评估信息系统的风险，并根据风险情况对信息系统的安全措施进行相应调整，使其安全性达到所需的要求。等级管理方法的基本思想是在信息系统生存周期的不同阶段，通过确定信息系统的安全保护等级，并按照确定的安全保护等级的要求进行信息系统安全的设计、实现、运行控制和维护，使其安全性达到确定安全保护等级的安全目标。我国当前实施的信息安全等级保护制度属于等级管理方法，其出发点是“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”。

无论是采用风险管理方法还是采用等级管理方法控制信息系统安全，都需要相应的信息安全技术和产品提供支持。对信息安全技术和产品划分安全等级对于信息安全技术和产品的研究、开发、管理以及选择和使用具有重要的意义，既可以为等级管理方法提供支持，也可以为风险管理方法提供支持。正因为如此，从 TCSEC 开始到 CC 直至现在，国际、国外及我国的许多信息安全标准都从不同的角度对信息安全技术和产品进行了安全等级划分。

然而，需要明确的是，就实现信息系统的安全保护而言，两种控制方法有一些本质上的差别。风险管理方法是一种在国外使用多年且已经比较成熟的信息系统安全控制方法；我国正在实行的信息安全等级保护制度是一种适合我国国情的信息系统安全控制方法，需要一套相应的政策、法规、制度和标准来推进，就像目前正在做的。本书所解读的《基本要求》就是被指定为在信息安全等级保护整改阶段设计和实现信息系统安全主要依据的标准。

本书作者陆宝华，是长期工作在公安战线的信息安全专家，主要对信息保障工作进行监督、检查和指导，先后从事公安专用移动通信系统、电子信息、信息安全等方向技术的研究，在移动通信、信息安全等领域颇有建树，积累了丰富的工作经验，曾组织制定了大连市信息安全事件的应急响应预案，并多次现场指挥信息安全事件的救援工作，为许多单位挽回了大量的经济损失，并消除了政治影响。在总结实践经验的基础上，本书作者对国内外信息安全的发展进行了广泛了解和深入研究，通过把理论和实践相结合，编写出版了《信息系统安全原理与应用》、《信息安全等级保护技术基础培训教程》等著作，深入浅出地对信息安全的相关概念和具体技术作了比较全面的介绍。

作者在对 TCSEC、CC 和 IATF 等相关资料进行深入研究和理解的基础上，结合对我国信息安全等级保护一系列相关标准的理解，编写了《信息安全等级保护基本要求培训教程》，本书是对《基本要求》进行培训的一本好书。本书集信息安全基本概念说明与信息安全技术应用于一身，对《基本要求》所涉及的相关标准、安全模型、安全功能等知识进行了较为系统的分类介绍；对《基本要求》中的一些条款进行了解释和说明，对有些条款还提出了应该采用的相关技术的建议；对某些层面的一些专门要求，通过相应的独立章节进行了说明。本书对于我国当前正在开展的信息安全等级保护整改阶段的工作具有重要的参考作用。

从以下方面确立对信息安全的基本认识，对于理解本书的内容会有所帮助。这些基本认识包括：

正确区分信息技术与信息安全技术。信息技术是实现信息系统功能所采用的技术，信息安全技术是确保信息系统安全所采用的技术。理解上容易混淆的是在可用性方面。由信息技术所提供的可用性表现为信息系统对确定的业务应用提供足够的存储、传输和处理业务数据能力；信息安全技术所提供的可用性是指对信息系统遭受的攻击和破坏应具有一定的事先防御和事后处理能力，当信息系统受到攻击和破坏时能够使信息技术所提供的可用性保持原有水平或可接受的较低水平。

实现信息安全的基本技术是隔离和控制。隔离是控制的先决条件，控制是实现安全目标的基本方法，任何信息安全技术都可以归结为隔离和控制技术的具体体现。典型的“访问监控器”和“前端过滤器”就是隔离和控制结构的基本模型。

信息安全的核心技术是访问控制。严格意义的访问控制，即以传统的访问三要素（主体、客体和访问操作）为基础，对主体访问客体的操作进行的控制；广义的访问控制则是对任何主体访问客体行为的控制，包括对主体访问网络的控制、对主体访问服务器的控制、对传输数据的加密保护等。

数据保护是信息安全保护的中心内容。业务数据是信息系统资源的主要表现，没有业务数据的信息系统是毫无实际价值的，信息系统中的安全保护归根结底是对业务数据的保护。从信息安全保护的角度，信息系统中的数据分为业务数据、系统数据和安全功能数据；业务数据保护是信息系统安全保护的出发点和归宿，系统数据保护是确保信息系统各种系统功能（操作系统功能、数据库管理系统功能、网络系统功能和应用软件系统功能等）正确实现的重要保证，安全功能数据保护是确保安全子系统各安全功能模块正确实现其安全功能的保证。各类数据保护有共同的地方，也有各自的特殊要求。

信息系统的安全保护等级与信息技术和产品的安全等级是既有联系又有区别的两个概念。前者是根据信息系统的安全保护需求确定的需要进行安全保护程度的表征，是与信息系统的资产及环境条件有关的；后者是根据信息技术及信息安全技术发展和应用的实际情况，对信息安全技术和产品所提供的安全性强度的表征，是与环境和条件无关的。对采用等级管理的方法进行信息系统安全控制的信息系统，需要选用相应安全等级的安全技术和产品使其达到确定安全保护等级的安全要求；对采用风险管理的方法进行信息系统安全控制的信息系统同样可以根据信息安全技术和产品的安全等级，选择合适的信息安全技术和产品对信息系统的安全性进行调整。同时，作为风险管理基本方法的风险分析和评估，同样可以在等级管理方法的某些环节用来对信息系统的风险情况进行分析和评估，并对安全保护措施进行调整，使其更符合信息系统安全保护的实际需要。总之，方法是多种多样的，目标只有一个，就是确保信息系统得到应有的安全保护。

前　言

2007 年 8 月公安部等四部局办，联合下发了《信息安全等级保护管理办法》（公通字[2007] 第 43 号）。这一文件的下发是信息安全等级保护工作在全国全面开展的重要标志。国家安全标准委员会也相继出台了多部国家标准的报批稿。《信息安全等级保护基本要求》就是在这样的背景下出台的。

《信息安全等级保护基本要求》是目前在信息系统等级确定以后，对信息系统进行安全改造、改建、加固的依据，也是测评机构对信息系统进行安全测评及国家信息安全监管部门进行监督、检查、指导的依据。理解《信息安全等级保护基本要求》对推进信息安全等级保护工作是极为重要的。笔者发现，相当多的从事信息系统维护工作和安全保护工作的人员对信息安全保障方面的知识还不是很熟悉，对许多的概念并不清楚，所以也就无法理解信息安全等级保护的基本要求了。有相当多的同志提出了这方面的问题，所以，笔者觉得有必要对《信息安全等级保护基本要求》所涉及的概念进行介绍，帮助大家学习并掌握《信息安全等级保护基本要求》。

为此，笔者撰写了《〈信息安全等级保护基本要求〉培训教程》一书，对《信息安全等级保护基本要求》中所涉及的标准、安全模型、安全功能等知识进行了较为系统的分类介绍。在书中，笔者着重介绍了技术要求中的网络安全、主机安全、应用安全及数据安全方面的要求。《信息安全等级保护基本要求》将基本要求分为两大部分，一部分是技术要求，分为五个大类；另一部分是管理要求，也分为五个大类。技术要求中的五个大类，实际上是信息系统的五个层面，而不是相应技术体系中的“安全功能类”，所以在技术要求的解读中，笔者没有按《信息安全等级保护基本要求》中的“类”来写，而是按技术体系通用的“安全功能类”进行介绍，同时给出了各层面上提出的这一功能类的基本要求，并根据一些同志的建议，对基本要求中的一些条款进行了解释和说明，有些还提出了应该采用相关技术的建议。对某些层面的独自要求，也采取了相应的独立章节进行说明。

本书中的第 5 章“自主访问控制”与第 6 章“标记与强制访问控制（MAC）”原为一章，但是考虑到强制访问控制对高安全等级的信息系统的重要性和实施了强制访问控制后信息系统安全的可靠性，为了能引起读者的重视和阅读方便，故将标记与强制访问控制划分为单独的一章。

本书中对管理要求，没有做太多的说明，只是对信息安全管理体系（ISMS）进行了初步介绍。这是考虑到，管理要求是比较容易理解的，不必做太多的说明。物理安全的内容也没有进行介绍，物理安全可以由专业的组织来实施，只要按照《信息安全等级保护基本要求》中的具体项目实施就行了，也不必做太多的说明。并且，会有专门介绍物理安全原理与实施的著作呈献给读者。

本书稿完成后，笔者将书稿分发给高贤民、赵然、佟立新、王晓宇、匡山、辛鹏、董立梅、李忠、连立洲十余名同志进行阅读，以检验本书的价值和难易程度。他们中有：从事多年计算机工作，但并不是很熟悉信息保障知识的同志；有一定的计算机工作经历，对信息安全保障基本不了解的同志；刚从学校计算机相关专业走出来的大学生。现在看来，这本书很适合熟悉信息系统但对安全并不很清楚的读者阅读。对于有一定的计算机工作经历，但不懂信息安全保障的同志来说，虽然他们可以看懂这些章节中的内容，但是仍不能建立起较为完整的信息保障的整体框架。建立起这样的整体框架，并不是本书的任务，由陆宝华、王晓宇编著的另一本书《信息安全等级保护技术基础培训教程》和本书可以共同完成这一任务。

笔者并不是一位对信息系统安全理论精深的学者，而是一个长期工作在信息系统安全保障第一线的管理者，由于长期的认真学习，掌握了不少的信息系统安全保障的理论与技术，并且对基层的信息系统维护人员的需求有非常清楚的了解。笔者非常愿意当好一个接口，将学者与专家的理论及思想，用尽量通俗的语言传达给在基层工作的读者。

由于笔者的水平有限，同时也不是标准的起草者，对信息安全保障理论知识的理解和对相关国家标准的理解可能存在着误区，再加上文笔水平有缺失，所以错误和缺点是不可避免的，希望读者在阅读的过程中给予批评和指正。

本书成稿后，有幸得到了国家信息安全的大专家吉增瑞老师的指导，吉增瑞老师是一位在理论和技术上都非常精湛的专家，也是一位认真负责和严谨的长者，编写了多部国家

信息安全等级保护的标准，而这些标准更系统、更完备，恰恰是信息安全等级保护的目标要求（而不是基本要求）。吉增瑞老师不仅对书稿进行了审核，还进行了用心的修改。这使本书的价值有了一个大大的提升，对等级保护工作具有了指导意义。

感谢公安部网络安全保卫局的顾建国局长、赵林副局长多年来对笔者的指导；感谢信息安全界的专家赵战生老师、吉增瑞老师、贾颖禾老师、崔书昆老师、卿斯汉老师多年来的指导与帮助；感谢大连市公安局网络警察支队的前任支队长梁明同志，正是在他的领导下，才能够使笔者在工作中深入地学习和理解信息安全等级保护的理论与技术。

本书在成稿过程中和成稿后，得到了公安部信息网络安全监察局主管等级保护工作的郭启全处长的直接指导、支持和帮助，对书稿的内容提出了具体的修改意见，并进行了审核。在此，笔者表示深深的感谢！

目　录

CHAPTER 1

第 1 章　等级保护基本要求概述

信息安全等级保护（以下简称“等级保护”）是我国在信息化推进过程中实施的对信息系统安全保护的基本制度、方法和策略。早在 1994 年国务院出台的《中华人民共和国计算机信息系统安全保护条例》中就明确地规定了我国对计算机信息系统实行分等级保护的要求。

2003 年，《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）中明确指出：“信息化发展的不同阶段和不同的信息系统有着不同的安全需求，必须从实际出发，综合平衡安全成本和风险，优化信息安全资源的配置，确保重点。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，制定信息安全等级保护的管理办法和技术指南。”

2004 年，由公安部、国家保密局、国家密码委及国务院信息办联合下发了《关于信息安全等级保护工作的实施意见》（公通字 2004 第 66 号，以下简称“66 号文”），标志着信息安全等级保护工作在全国全面启动。66 号文指出“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、有计划地实施。”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”。

依据此要求，《信息安全等级保护基本要求》列入了首批需完成的6个标准之一。

本书介绍的《信息安全等级保护基本要求》（以下简称《基本要求》），是信息系统安全建设和改造过程中使用的主要标准之一，描述《基本要求》的技术要求分级思路、逐级增强特点以及具体各级安全要求。使得用户能够了解《基本要求》在信息系统安全等级保护中的作用、基本思路和主要内容，以便正确选择合适的安全要求进行信息系统保护。

1.1 等级保护基本要求背景及作用

《基本要求》，是各等级信息系统安全达标要求的基本尺度。各等级信息系统均应该依据自身的保护目标达到《基本要求》中所给出的相应等级及相应需求的规定。

1.1.1 信息系统安全等级保护的基本内容

66号文中规定了信息安全等级保护的基本内容："是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。"等级保护的核心是信息系统的分等级保护。

信息系统根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为以下五级。

第一级信息系统，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。信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行自主保护。

第二级信息系统，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。信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级信息系统，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。信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级信息系统，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。信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级信息系统，信息系统受到破坏后，会对国家安全造成特别严重损害。信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门机构对该级信息系统信息安全等级保护工作进行专门监督、检查。

国家专门出台《信息系统安全等级定级指南》，作为信息系统定级的标准。

1.1.2 主要作用及特点

《基本要求》针对以上信息系统的分级，提出了相应的达标要求。

1. 主要作用

《基本要求》对等级保护工作中的安全控制选择、调整、实施等提出规范性要求，根据使用对象不同，其主要作用分为三种：

（1）为信息系统建设单位和运营、使用单位提供指导

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保护提供指导。各相应的组织应该根据信