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
等级保护技术基础
培训教程

陆宝华　王晓宇　编著

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

信息安全
等级保护技术基础
培训教程

[redacted]

[redacted]

“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
等级保护技术基础
培训教程

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

内 容 简 介

本书是信息安全等级保护基础知识的介绍，使读者能清楚地了解信息保障体系建设的基本思想和基本方法。

本书分四个部分共 11 章，第一部分共三章是对信息保障基本概念的介绍，第 1 章概述，主要介绍信息保障的发展过程和信息保障体系的整体框架；第 2 章介绍信息系统中安全体系的核心——可信计算基（TCB）或者称之为安全子系统；第 3 章是现行信息安全保护技术的介绍。第二部分共六章，分层次介绍信息保障的基本思想和方法。第 4 章介绍信息系统保护的一般过程与基本方法，第 5 章介绍网络保护的基本思想和方法，第 6 章介绍计算机环境保护的思想和方法（操作系统、数据库、应用程序和数据），第 7 章至第 9 章介绍信息系统连续性运行（运行安全）保护的思想与方法：第 7 章介绍风险评估、第 8 章介绍应急响应、第 9 章介绍信息系统安全运行体系。第三部分仅第 10 章一章，介绍信息安全管理的基本思想与方法。第四部分也仅第 11 章一章，介绍信息安全工程的思想与方法。

本书适合于所有关心信息安全系统安全管理的读者阅读，使之能够建立起信息保障完整体系的思想。

图书在版编目（CIP）数据

信息安全等级保护技术基础培训教程 / 陆宝华，王晓宇编著. —北京：电子工业出版社，2010.6
（安全技术大系. 国家信息安全等级保护系列丛书）
ISBN 978-7-121-11084-9

Ⅰ. ①信… Ⅱ. ①陆… ②王… 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 108429 号

策划编辑：毕 宁
责任编辑：许 艳
特约编辑：顾慧芳
印 刷：北京智力达印刷有限公司
装 订：三河市皇庄路通装订厂
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：40.25 字数：721 千字
印 次：2010 年 6 月第 1 次印刷
印 数：4000 册 定价：79.00 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

信息及信息系统的安全，大的方面可以直接影响一个国家政治、国防安全、经济建设、社会秩序的稳定和社会公共利益，小的方面可以影响一个组织自身的生存与发展。这已经是一个不争的事实。各个国家如果没有给予足够的重视，后果将是极为可怕的。

在我国，1994 年就出台了《计算机信息系统安全保护条例》，将信息与信息系统保护纳入到了法制的轨道。后来又在《刑法》中加入了打击针对计算机信息系统的犯罪和利用计算机信息系统的犯罪的内容（《刑法》285,286,287 条），在新近出台的治安处罚法中也加入了相关的内容。

除了打击针对信息系统的犯罪外，更重要的是对于信息和信息系统进行适度的保护。所谓适度保护就是要根据信息及信息系统的重要程度，给予相适应的保护。我国推行的信息安全等级保护制度，就体现了适度保护这一原则。

党的十六届四中全会针对传统安全威胁和非传统安全威胁的因素相互交织的新情况，提出了要增强国家安全意识，完善国家安全战略的要求。

应该说，我国党和政府的领导及专家、学者在这一问题上的认识是一致的。早在 1994 年出台的《计算机信息系统安全保护条例》中就明确地提出了，在我国要实行信息安全等级保护制度。1999 年出台了第一个关于信息安全等级保护的国家标准《计算机信息系统安全等级划分准则》（GB17859－1999）。2003 年中办 27 号文中强调了要加强对信息与信息系统的保护，落实信息安全等级保护制度，明确提出了建设信息保障体系的要求。2004 年，公安部、国家保密局、国务院密码委和原国务院信息化办公室联合下发了《信息安全等级保护实施意见》（公通字［2004］第 66 号，俗称 66 号文），标志着在我国信息安全等级保护工作的正式启动。2007 年四部局办共同下发的《信息安全等级保护管理办法》（公通字［2007］第 43 号，俗称 43 号文）将信息安全等级保护工作纳入到了法制化的轨道。

本书的背景

信息安全等级保护制度是我国在信息与信息系统保护方面的基本制度和基本策略，是一种必须强制执行的制度。为了科学地推动这一制度的落实，国家出台了一系列的法规、政策和标准，使得需要对信息和信息系统进行保护的组织及主管部门，代表国家推行这一制度的相关监管部门，各类信息安全服务单位及信息安全专用产品的提供单位均在一套法律与技术体系的指导下完成各自相应的工作。

为了能更好地推动这一工作的开展，我们按照国家的要求，编著了这本《信息安全等级保护技术基础培训教程》。

在编著这本书之前，我们做了这样的三项调查：一是对目前各使用单位、各监管部门从事信息系统安全的人员所掌握的理论与技术水平进行了调查；二是对目前出版的关于信息安全方面的著作进行了调查；三是对目前各类的信息安全培训进行了调查。我们得出了这样的一个结论，绝大多数从事信息安全方面的工作人员都缺乏系统和全面的信息系统安全保护方面的知识，而只有少量的信息安全出版物能够系统全面地来介绍这方面的知识，绝大多数的商业培训都没有系统地、完整地介绍信息系统安全保护方面的知识。

基于以上的认识，我们统一规划了这本书的结构，其目的是让读者对信息系统安全保护知识有一个全面的、系统的了解，同时也兼顾了信息系统的一般保护方法。通过阅读这本书，读者能够读懂各类相关的标准，并具有初步的信息系统安全保障的知识。

本书的内容

本书分四个部分共 11 章，第一部分包括第 1 章至第 3 章，是基础知识的介绍，全面介绍了信息系统安全保护的理论与技术。其中，第 2 章是对可信计算基的简要介绍，可信计算基或者称安全子系统，是信息系统安全保护的基本思想，国内外的技术标准均使用这一概念，而国内的出版物却很少有这方面知识的介绍。第 3 章是现行信息安全技术的介绍。

第二部分包括第 4 章至第 9 章，是从技术的角度来介绍对信息系统的一般保护方法，实际上也是信息系统安全保护的基础知识，是理论与技术的应用。信息系统的安全保护目

标有两个：一是数据信息的安全（主要考虑机密性和完整性），二是信息系统服务功能的安全（数据信息及系统的可用性）。许多专家和学者称前者为信息安全，而后者则是运行安全。我们这里也是从这样的思想出发的，一些保护措施用来保护数据信息安全，如保护计算环境；而另一些措施则用来保护系统服务功能，如容错和容灾；还有一些保护措施同时兼顾了这两个方面，如对网络的保护。

第三部分仅一章，第10章，简要地介绍了信息安全管理体系。第四部分也仅一章，第11章，简要地介绍了信息安全工程方面的知识。

本书的作者

本书基本上是由陆宝华同志编著的，王晓宇同志协助翻译了《局域网安全分析》（FIPS PUB 191）的全部内容和《信息保障技术框架》（美国国家安全局）的部分内容，在编著第5章保护网络和网络边界中使用了这些内容。

应当说，在一本书中将信息安全保障的所有知识进行完整的介绍是不可能的，也是没必要的，本书的目的只是要读者建立起信息保障的知识框架，而没有对知识进行深度的讨论，也没有介绍一些较深的理论和较难知识，特别是没有详细地介绍信息系统强制保护方面的知识，如隐蔽信道分析等。这是考虑到如下的一些因素：一是这部分的知识较难；二是在本丛书的《信息安全等级保护基本要求培训教程》一书中已经介绍了强制访问控制的知识，尽量避免重复；三是第三级以下信息系统的技术人员可以暂时不了解这部分知识。当然对于第四级以上信息系统的技术人员来说，这方面的知识是很需要的。

本书的读者

由于编者长期工作在信息系统安全监管的第一线，同时又师从多位著名的安全专家和学者，所以，我们认为这部书非常适合于所有从事信息系统安全保护工作人员来阅读，特别是对于那些缺乏系统的信息系统安全知识的人员来说，这是一本很好的读物；同时，还可以作为大专院校信息安全相关专业的教材和参考书。

感谢

我们感谢在信息等级保护工作方面给予我们许多指导的各位领导：公安部网络安全保卫局局长顾建国先生、副局长赵林先生。感谢许多专家和学者：赵战生老师、贾颖和老师、吉增瑞老师、卿斯汉老师、崔书昆老师等。特别感谢卿斯汉老师审定了全部书稿，并提出了非常好的批评意见和建议；也特别感谢解放军工程大学的斯雪明博士对本书第 3 章密码技术一节进行的修改；感谢启明星辰公司总工程师袁智辉先生对第 5 章中 TNC 的修改意见；感谢思科公司的卢佐华小姐，瑞捷网络的迟明壮先生，华赛公司的胡文友先生，启明星辰公司的俞真子小姐，为我们提供了大量的资料。

在编著的过程中，我们始终得到了公安部网络安全保卫局郭启全处长的具体指导和帮助，特此感谢！还要感谢我原来的老领导、兄长梁明同志，是他给我创造了一个宽松的工作和学习环境，才使得我能够对信息系统安全保护理论和技术有一个较深的理解，并在全国较早从事对信息系统安全保护的监管工作，从中得到了不少的体会和收获。

联系

必须承认，由于目前我们对信息系统安全知识的掌握和理解尚处在一个不高的水平上，再加上我们的文字功夫不深，书中的缺点和错误难免，希望读者能够给予批评和指正。

我们的联系方式是 lbh@dl.cn。

编者

2010 年 2 月于北京

目　录

第一部分　信息保障基本概念介绍

第三部分 信息安全管理的基本思想与方法

第四部分 信息安全工程的思想与方法

第一部分　信息保障基本概念介绍

CHAPTER

1

第 1 章　信息系统安全保障概述

随着信息技术的发展，特别是计算机和通信技术相结合的网络技术的发展，使得社会对信息系统的依赖越来越强。应当说，信息系统已经是现代社会运转的重要基础设施，离开了这样一个基础设施，整个社会将会发生极大的动荡。但信息技术的发展从一开始就忽略了一个极为重要的问题：安全。

近年来，关于各类安全事件的报道可谓层出不穷，每年都会有一些让人心惊肉跳的消息见于媒体。计算机病毒和人为入侵造成的损失每年都以百亿美元计，而且这一定是不完全的统计。可以说信息安全问题，已经是涉及国家安全、社会稳定和经济建设安全的重大问题。美国在克林顿政府时期就有人说，国家安全就是国土安全加上信息安全。

对于一个机构来说，一方面它的信息安全是国家信息安全的组成部分，另一方面，也是它内部安全的重要组成部分，甚至，对于一些机构来说，信息安全是这个机构的生命线。所以，如何解决机构的信息安全问题，是机构面临的一个重要问题，甚至是涉及机构生存与发展的重要问题。构建合理的信息安全保障体系，对于一些机构来说是头等重要的大事。

我国从 1994 年颁布了《计算机信息系统安全保护条例》（国务院 147 号令）从而使信息系统安全的保护工作纳入到了法制化的轨道。2004 年又正式的启动了信息安全等级保护工作，形成了我国的信息系统安全保护的基本制度和基本方法。信息

安全等级保护制度的推广对我国整体的信息系统的安全的保护水平会有一个科学合理的提升。

1.1 信息系统安全概述

关于信息目前还没有一个普遍被人们接受的定义，一些从事信息安全工作的人简单地把信息定义为“资产”的说法是错误的，信息具有资产的价值，但不能说信息的定义就是“资产”。我国有不少人使用我国信息论学者钟义信先生给出的定义：

信息是事物的运动状态和状态变化的方式。

1.1.1 信息及信息系统及安全的定义

1. 信息及信息系统的定义

早在1994年《中华人民共和国计算机信息系统安全保护条例》第二条明确的定义：本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

2004年公安部、国家保密局、国家密码管理办公室和原国务院信息化办公室联合下发的《关于信息安全等级保护的实施办法》（公通字2004第66号）中给信息系统作了以下的定义：“信息系统是由计算机及其相关和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。”在66号文中，对信息给了明确的界定。应该说明的是这里说的信息，并不是指完全的信息论意义上的信息。信息论意义上的信息，一定是未知的，但在信息系统中的数字化信息，并不一定是未知的。

2. 信息及信息系统的安全

对于安全的解释，在线词典上的说法：安全是避免危险、恐惧、忧虑的量度

和状态。

从对信息的分类可以看出，信息安全是一个很大的概念，或者说是一个很大的范畴，只要存在着信息，就存在信息安全的问题。传统的电话通信存在信息安全问题；广播电视存在信息安全问题；报纸出版业也存在信息安全问题。所以说这是一个很大的范畴，不是我们要讨论的问题，我们要讨论的是信息系统的安全问题。现在一般定义上的信息安全还是针对计算机信息系统的安全。

信息系统安全

国际标准化组织（ISO）给出的信息安全（实际上是指信息系统安全）的定义是："为数据处理系统建立和采取的技术的和管理的安全保护。保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭受破坏、更改、泄露。"我国的信息安全专家也指出，信息系统的安全是："计算机的硬件、软件、数据受到保护，不因偶然的或恶意的原因受到破坏、更改、泄露，以及系统连续正常运行。"1994 年国务院 147 号令《中华人民共和国计算机信息系统安全保护条例》第三条指出："计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。"这里虽然没有明确定义信息系统安全，但标明了信息系统安全所涵盖的内容。

1.1.2 信息安全保障的基本概念

1. 人们对信息安全的认识历程

信息安全的发展是与信息技术的发展和用户的需求密不可分的，在不同的时代也体现出不同的特征，大体来讲，信息安全经历了一个从通信安全（COMSEC）→信息安全（INFOSEC）→信息保障（information assurance，IA）的发展阶段，也可称为：保密→保护→保障发展阶段。

通信安全的历程开始于 20 世纪 40 年代，那时人们关注的通信安全，主要关心对象是以政府和军事、外交为主，多采用加密、发射传输保密等技术手段来保护数