现代信息资源管理丛书

邱均平　主编

信息安全概论

Introduction to Information Security

唐晓波　等　编著

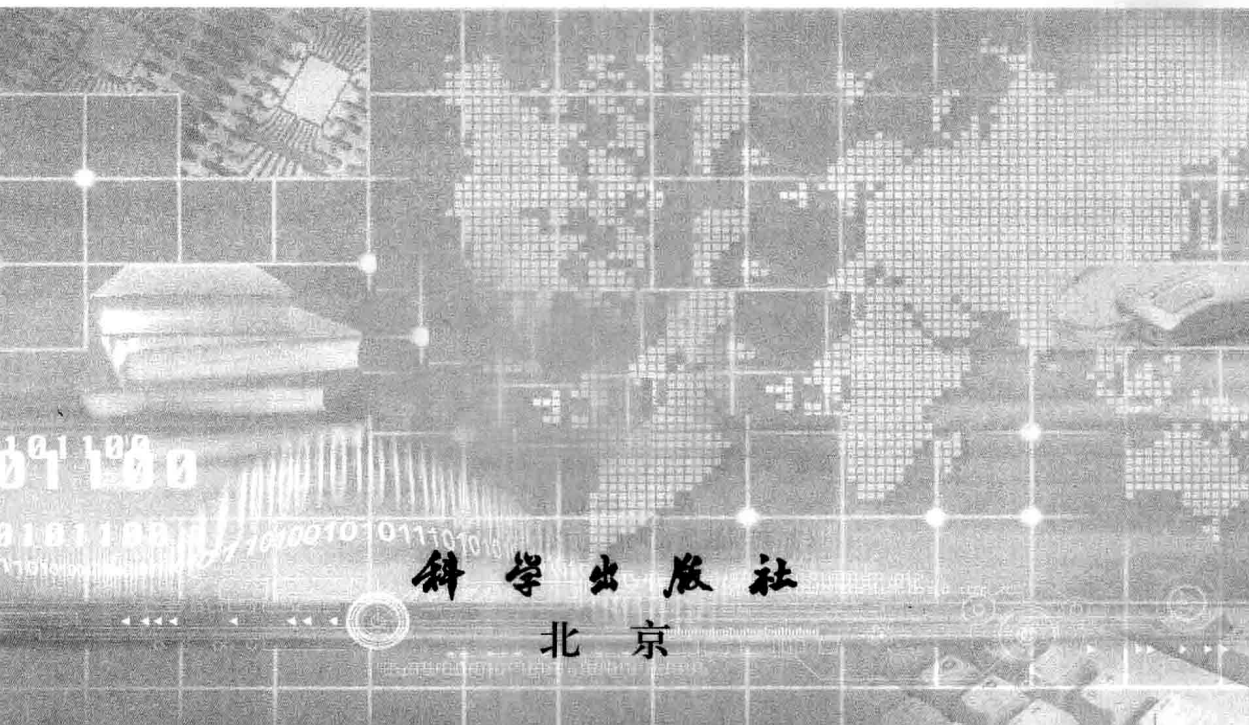
科学出版社
www.sciencep.com

现代信息资源管理丛书

邱均平　主编

Introduction to Information Security

信息安全概论



科学出版社

北京

内 容 简 介

本书是《现代信息资源管理丛书》之一。

本书系统介绍信息安全的理论知识、信息安全的技术以及信息安全方面的一些最新成果。全书共分为10章，内容包括绪论、信息密码技术、信息认证技术、密钥管理技术、访问控制技术、操作系统安全和数据库安全、网络安全技术、应用安全机制、信息安全标准和信息安全的管理。

本书可供信息管理与信息系统专业、信息资源管理专业、电子商务专业以及信息技术类专业本科生、研究生学习参考，也可供从事信息处理、通信保密及与信息安全工作的有关科研人员、工程技术人员和技术管理人员参考。

图书在版编目(CIP)数据

信息安全概论／唐晓波编著．—北京：科学出版社，2010
（现代信息资源管理丛书/邱均平主编）
ISBN 978-7-03-028969-8

Ⅰ.①信… Ⅱ.①唐… Ⅲ.①信息系统－安全技术－高等学校－教材
Ⅳ.①TP309

中国版本图书馆CIP数据核字（2010）第177525号

责任编辑：李 敏 刘 鹏／责任校对：陈玉凤
责任印制：钱玉芬／封面设计：鑫联必升

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

骏走印刷厂印刷

科学出版社发行 各地新华书店经销

*

2010年9月第 一 版 开本：B5（720×1000）
2010年9月第一次印刷 印张：30
印数：1—3 000 字数：605 000

定价：48.00元
（如有印装质量问题，我社负责调换）

《现代信息资源管理丛书》编委会

总　序

信息资源管理（information resource management，IRM）是20世纪70年代末兴起的一个新领域。30多年来，IRM已发展成为影响最广、作用最大的管理领域之一，是一门受到广泛关注的富有生命力的新兴学科。IRM对经济社会可持续发展和提高国家、区域、组织乃至个人的核心竞争力来说，都具有基础性的意义和独特的价值。

在国际范围内，受信息技术进步的推动和经济社会管理需求的牵引，IRM理论研究和职业实践发展迅速，并呈现出一些明显的特征：①广泛融合了信息科学、经济学、管理学、计算机科学、图书情报学等多学科的理论方法，形成以“信息资源”为管理对象的一个新学科，在管理学知识地图中确立了自己的地位。②研究范式的形成和变化。IRM的记录管理学派、信息系统学派、信息管理学派各自发展，以及管理理念、理论和技术方法的交叉融合，形成了IRM的集成管理学派。集成管理学派以信息系统学派的继承和发展为主线，吸收了记录管理学派的内容管理和信息管理学派的社会研究视角，形成了IRM强调“管理”和“技术”，并在国家、组织、个人层面支持决策和各自目标实现的新的研究范式[①]。③研究热点的变化。当前IRM研究在国家、组织、个人层面上表现出新的研究热点，如国家层面的国家信息战略、国家信息主权与信息安全、信息政策与法规、支持危机管理的信息技术等；组织层面的信息系统理论，信息技术（系统）的绩效、价值与应用，IT投资，知识管理，电子商务，电子政务，IT部门与IT员工，虚拟组织，IRM技术等[②]；个人层面的人－机交互、My Li-

① 麦迪·克斯罗蓬．信息资源管理的前沿领域．沙勇忠等译．北京：科学出版社，2005

② Mehdi Khosrow-Pour. Advanced Topics in Information Resources Management（Volume 1-5）. Hershey：IGI Publishing，2002～2006

brary、个人信息管理（personal information management，PIM）框架、PIM 工具与方法等[①]。④职业实践的发展。IRM 的基础管理意义和强大的实践渗透力不断催生出新的信息职业、新的信息专业团体和新的信息教育。组织中的 CIO 作为一个面向组织决策的高层管理职位，正经历与 COO、CLO、CKO 等的角色融合与再塑；信息专业团体除信息科学学（协）会、图书馆学（协）会、计算机学（协）会、竞争情报学（协）会、数据处理管理学（协）会、互联网协会等之外，专门的信息资源管理协会也开始成立，如美国信息资源管理协会（Information Resources Management Association，IRMA）；同时，IRM 作为高等教育中的一个专业或课程，广泛渗透于图书情报、计算机、工商管理等学科领域，这种多元并存的教育格局一方面加剧了 IRM 的职业竞争，另一方面也成为推动 IRM 学科发展和保持职业生命力的重要因素。

随着 IRM 在中国的发展，中国的图书情报档案类高等教育与 IRM 的关系日益密切[②]，进入 21 世纪以后，出现了面向 IRM 的整体改革趋势和路径选择。在 2006 年召开的“第二届中美数字时代图书馆学情报学教育国际研讨会”上，与会图书情报（信息管理）学院院长（系主任）签署的《数字时代中国图书情报与档案学教育发展方向及行动纲要》中明确提出：“图书情报档案类高等教育应定位于信息资源管理，定位于管理科学门类”，认为“面向图书馆、情报、档案与出版工作的图书情报学类高等教育是信息资源管理事业健康发展的重要保障”[③]，显示了面向 IRM 已成为中国图书情报档案类高等教育改革的一个集体共识。在这一背景下，图书情报档案类学科如何在 IRM 大的学

① William Jones. Personal Information Management. *See*: Annual Review of Information Science and Technology. Volume 41, 2007

② 在我国目前的高等教育体系中，图书馆学、信息管理与信息系统、档案学、编辑出版学分别属于教育部高等教育司颁布的《普通高等学校本科专业目录和专业介绍》中的本科专业；图书馆学、情报学、档案学、出版发行学分别属于国务院学位委员会《授予博士硕士学位和培养研究生的学科专业目录》中的二级学科。但它们分别属于不同的学科门类（如本科专业中的管理学类、文学类）和一级学科（如研究生专业中的管理科学与工程，图书馆、情报与档案管理）

③ 数字时代中国图书情报与档案学教育发展方向及行动纲要．图书情报知识，2007，(1)

科框架下发展，以信息资源作为对象和逻辑起点进行知识更新与范畴重建，并突出“管理”和“技术”的特点，已成为我国图书情报档案类学科理论研究和教学改革的新的使命和任务。毫无疑问，这将是中国图书情报档案类学科及其教育在新世纪所面临的一次方向性变革和结构性调整，不仅意味着理论形态及其知识体系的改变，也意味着实践模式的革新。《现代信息资源管理丛书》的出版就是出于对这一使命的认识和学术自觉。事实上，我国“图书馆、情报与档案管理”（或称“信息资源管理”）学科领域的教学和研究已经发生了深刻变革，其范围不断扩大，内容更加充实，应用面也在拓展。为了落实“宽口径、厚基础，培养通用型人才”的要求，很多学校的教学工作正在由按二级学科专业过渡到按一级学科来组织，而现已出版的信息管理类丛书仅针对“信息管理与信息系统”专业的需要，适用面较窄，不能满足一级学科的教学、科研和广大读者的迫切需要。因此，根据高等学校IRM类学科发展与专业教育改革的需要和图书市场的需求，为了建立结构合理、系统科学的学科体系和专业课程体系，创建符合IRM的学科发展和教学改革要求的著作体系，进一步推动本学科领域的教学和科研工作的全面、健康和可持续发展，武汉大学、华中师范大学、黑龙江大学、兰州大学、南京理工大学、中山大学、吉林大学、华东师范大学、湘潭大学、郑州大学、西安电子科技大学和郑州航空工业管理学院12所高校信息管理学院（系、中心）的多名专家、学者共同发起，在广泛协商的基础上决定联合编著一套《现代信息资源管理丛书》（以下简称《丛书》），由科学出版社正式出版。我们希望能集大家之智慧、博采众家之长写出一套有价值、有特色、高水平的信息资源管理领域的科学著作，既展示本学科领域的最新丰硕成果，推动科学研究的不断深入发展，又能满足教学工作和广大读者的迫切需要。

《丛书》的显著特点主要是：①定位高，创新性强。《丛书》中的每部著作都以著述为主、编写为辅。既融入自己的研究成果，形成明显的个性特色，又构成一个统一体系，能够用于教学；既是反映国内

外学科前沿研究成果的创新性专著，又是适合高校本科生和研究生教学需要的新教材，同时还可以供相关学科领域和行业的广大读者学习参考。②范围广，综合性强。《丛书》涉及“图书馆、情报与档案管理”整个一级学科，包括图书馆学、情报学、档案学、信息管理与信息系统、编辑出版、电子商务以及信息资源管理的其他专业领域，体现出学科综合、方法集成、应用广泛的明显特点。③水平高，学术性强。《丛书》的著者都具有博士学位或副教授以上职称，都是教学、科研第一线的骨干教师或学术带头人，既具有较高的学术水平和雄厚的科研基础，又有撰写著作的经验，从而为打造高水平、高质量的系列著作提供了人才保障；同时，按照理论、方法、应用三结合的思路构建各著作的内容体系，体现内容上的前瞻性、科学性、系统性和实用性；在信息资源管理理论与信息技术结合的基础上，对信息技术和方法有所侧重；书中还列举了典型的、有代表性的案例，充分体现其实用性和可操作性；注重整套丛书的规范化建设，采用统一版式、统一风格，表现出较高的规范化水平。

《丛书》由武汉大学博士生导师邱均平教授全程策划、组织实施并担任主编，王伟军、马海群、沙勇忠、王学东、毕强、赵捧未、况能富、范并思、王新才、甘利人、刘永、夏立新、唐晓波、张美娟、赵蓉英、文庭孝、张洋、颜端武担任副主编。为了统一认识，落实分工合作任务，在《丛书》主编主持下，先后在武汉大学召开了两次编委会。第一次编委会（2005 年 11 月 27 日）主要讨论了选题计划，确定各分册负责人；然后分头进行前期研究、撰写大纲，并报给主编进行审订或请有关专家评审，提出修改意见。经过两年多的准备和研究，2007 年 12 月 23 日召开了第二次编委会，进一步审订了各分册的编写大纲、落实作者队伍、确定交稿时间和出版计划等，并商定在 2008～2010 年内将 18 本分册全部出版发行。会后各分册的撰著工作全面展开，进展顺利。在 IRM 大学科体系框架下，我们选择 18 个主题分头进行研究，其研究成果构成本套丛书著作。这些著作反映了 IRM 领域的重要分支或新的专业领域的创新性研究成果，基本上构成了一个较

为全面、系统的现代信息资源管理的学科体系。参与撰著的作者来自30多所高校或科研院所，有着广泛的代表性。其中，已确定的18本分册的名称和负责人分别是：《信息资源管理学》（邱均平，沙勇忠），《数字资源建设与管理》（毕强），《信息获取与用户服务》（颜端武），《信息系统理论与实践》（刘永），《信息分析》（沙勇忠），《信息咨询与决策》（文庭孝），《政府信息资源管理》（王新才），《出版经济学》（张美娟），《电子商务信息管理》（王伟军），《信息资源管理政策与法规》（马海群），《网络计量学》（邱均平），《信息检索原理与技术》（夏立新），《信息资源管理技术》（赵捧未），《信息安全概论》（唐晓波），《数字信息组织》（甘利人），《企业信息战略》（王学东），《竞争情报学》（况能富），《网络信息资源开发与利用》（张洋）。《丛书》各分册的撰写除阐述各自学科领域相对成熟的知识积累和知识体系之外，还力图反映国内外学科的前沿理论和技术方法；既有编著者的独到见解和新的研究成果，又突出面向职业实践的应用。因此，《丛书》的另一个重要特色是兼具专著与教材的双重风格，既可作为高校信息管理与信息系统、工商管理、图书情报档案、电子商务以及经济学和管理学等相关专业的教材或教学参考书，又可供信息管理部门、信息产业部门、信息职业者以及广大师生阅读使用。

《丛书》的出版得到了科学出版社的大力支持；同时还得到了各分册负责人、各位著者和参编院校的鼎力帮助；在编写过程中，我们还参阅了大量的国内外文献。在此一并表示衷心的感谢！

由于面向IRM的图书情报档案类学科转型是一个艰巨和长期的任务，我们所做的工作只是一次初步的尝试，不足和偏颇之处在所难免，诚望同行专家及读者批评指正。

邱均平

于武汉大学珞珈山

2008年6月8日

前　言

随着信息社会的到来，信息技术在国民经济建设、社会发展、国防、科学研究、教育等领域日益重要。信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。互联网的发展和应用打破了传统的时间和空间的局限性，使得获取信息更加快捷有效，但当人们享受信息资源所带来的巨大的利益的同时，也面临着信息安全的严峻考验。

信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。信息安全性主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须重视的问题，是一个不容忽视的国家安全战略。信息安全问题是构建整个社会信息化的根本保证，信息安全问题不仅涉及国家的政治、经济、军事、文化、意识形态等领域，同时也是人们能否保护自己个人隐私的关键。国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全已成为维护国家安全和社会稳定的一个焦点，各国都予以极大的关注与投入。信息安全保障能力是21世纪综合国力、国际竞争力的重要组成部分。我国政府已经充分意识到信息安全的重要性。学习、研究和应用信息安全的知识、理论、方法和技术是21世纪高等教育的重要领域。为满足相关院校和人员对安全技术的需求，我们编写了这本书，希望此举对我国的信息安全能起到更加积极的推动作用。

本书介绍了信息安全的理论知识、信息安全的技术及信息安全方面的一些最新成果。全书共分为10章。第1章绪论，概括地介绍了信息安全；第2章信息密码技术，介绍了密码学的基础、各种加密算法和前沿的加密算法；第3章信息认证技术，介绍了数字签名、数字水印技术、哈希函数、生物特征识别与身份认证技术与实现；第4章密钥管理技术，介绍了密钥管理、分配、托管和公钥基础设施（PKI）；

第5章访问控制技术，介绍了访问控制原理、访问控制策略与机制；第6章操作系统安全和数据库安全，介绍了操作系统安全机制、数据库安全技术与反病毒技术；第7章网络安全技术，介绍了入侵检测、安全扫描、防火墙技术、虚拟专用网技术、网络隔离技术和可信计算与网格安全；第8章应用安全机制，介绍了电子邮件安全技术、Web安全技术与电子商务安全技术；第9章信息安全标准，介绍了国内外的信息安全标准及其研究趋势；第10章信息安全的管理，介绍了信息安全管理的内容和策略、信息安全立法。

本书可供信息管理与信息系统专业、信息资源管理专业、电子商务专业及信息技术类专业本科生、研究生学习参考，也可供从事信息处理、通信保密及与信息安全工作的有关的科研人员、工程技术人员和技术管理人员参考。

本书由武汉大学信息管理学院唐晓波教授编著。武汉大学信息管理学院邓晶、胡胜勇、黄思哲、金钟鸣、李莲、罗毅、潘琦、熊杰、朱传高参加了编写。

本书在编写过程中得到了武汉大学信息管理学院和科学出版社的大力支持，在此表示衷心的感谢。

本书的编写参考了大量的文献资料，在此，向这些文献资料的作者表示衷心的感谢。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科，由于编者的学术水平有限，加之编写时间较紧，书中如有错误和不妥之处，敬请专家、学者和读者批评、指正。

唐晓波

2010年6月

目　　录

总序

前言

第 1 章　绪论 …… 1

1.1　信息与信息技术 …… 1

1.1.1　信息的定义 …… 1

1.1.2　信息技术的概念 …… 2

1.2　信息安全内涵 …… 4

1.2.1　信息安全的概念 …… 4

1.2.2　信息安全的目标 …… 5

1.3　信息安全的研究内容 …… 7

1.3.1　信息安全基础研究 …… 8

1.3.2　信息安全应用研究 …… 11

1.3.3　信息安全管理研究 …… 14

1.4　安全服务与机制 …… 15

1.4.1　信息安全威胁 …… 15

1.4.2　信息安全服务 …… 20

1.4.3　信息安全机制 …… 21

1.5　信息安全的发展及趋势 …… 26

1.5.1　信息安全发展阶段 …… 26

1.5.2　信息安全发展现状 …… 31

1.5.3　信息安全发展趋势 …… 32

1.6　信息安全技术体系 …… 34

1.6.1　PDR 技术体系 …… 34

1.6.2　纵深防御技术体系 …… 36

1.6.3　面向应用的技术体系 …… 39

第 2 章　信息密码技术 …… 42
2.1　密码学的发展与演变 …… 42
2.2　密码学的基础 …… 44
2.2.1　密码学的特点 …… 44
2.2.2　密码学的基本要素 …… 44
2.2.3　密码体制 …… 46
2.2.4　密码分析 …… 49
2.2.5　古典密码 …… 50
2.3　对称密码体制——流密码 …… 53
2.3.1　流密码基本原理 …… 53
2.3.2　二元加法流密码 …… 56
2.3.3　混沌序列流密码 …… 57
2.3.4　其他流密码 …… 59
2.4　对称密码体制——分组密码 …… 61
2.4.1　分组密码基本原理 …… 61
2.4.2　Feistel 密码结构 …… 62
2.4.3　数据加密标准（DES） …… 62
2.4.4　其他分组密码 …… 71
2.4.5　分组密码的工作模式 …… 73
2.4.6　分组密码的分析方式 …… 75
2.5　公钥密码体制 …… 76
2.5.1　基本概念 …… 76
2.5.2　RSA 算法 …… 78
2.5.3　EIGamal 算法 …… 80
2.5.4　ECC 算法 …… 81
2.6　领域前沿 …… 84
2.6.1　量子密码学 …… 84
2.6.2　DNA 密码 …… 86
2.6.3　神经网络密码学 …… 86
第 3 章　信息认证技术 …… 89
3.1　信息认证技术概述 …… 89

3.1.1 对信息进行认证的技术发展史 …… 89
3.1.2 对信息认证的必要性 …… 89
3.2 数字签名 …… 91
3.2.1 数字签名的概念 …… 91
3.2.2 数字签名的实现方法 …… 93
3.2.3 几种有代表性的数字签名方案 …… 95
3.2.4 数字水印技术 …… 101
3.3 哈希函数和消息完整性 …… 107
3.3.1 哈希函数 …… 107
3.3.2 消息认证和消息完整性 …… 109
3.4 生物特征识别 …… 110
3.4.1 生物特征识别的基本概念 …… 110
3.4.2 几种生物特征识别技术介绍 …… 110
3.4.3 生物特征识别技术发展趋势 …… 114
3.5 身份认证 …… 115
3.5.1 身份认证基础 …… 115
3.5.2 身份认证协议 …… 118
3.5.3 常见的身份认证技术 …… 121
3.5.4 身份认证的实现 …… 125
第4章 密钥管理技术 …… 138
4.1 密钥管理概述 …… 138
4.1.1 密钥管理的意义 …… 138
4.1.2 密钥管理的原则 …… 139
4.1.3 密钥的分类 …… 139
4.1.4 不同类型的密钥加密体制 …… 140
4.2 密钥的生命周期及其管理 …… 141
4.2.1 密钥的产生 …… 141
4.2.2 密钥的注入 …… 144
4.2.3 密钥的存储 …… 144
4.2.4 密钥的使用与控制 …… 146
4.2.5 密钥的更新 …… 147

4.2.6 密钥的吊销与销毁 …… 147
4.3 密钥分配技术 …… 148
4.3.1 密钥分配的类型 …… 148
4.3.2 密钥分配的方法 …… 149
4.3.3 密钥分配协议 …… 150
4.4 公钥基础设施（PKI） …… 155
4.4.1 PKI 概述 …… 155
4.4.2 数字证书 …… 156
4.4.3 PKI 组件 …… 159
4.4.4 PKI 提供的服务 …… 164
4.4.5 PKI 信任模型 …… 166
4.4.6 PKI 的应用 …… 170
4.5 密钥分散与托管技术 …… 172
4.5.1 密钥分散技术 …… 172
4.5.2 密钥的分散、分配和分发 …… 173
4.5.3 密钥托管概述 …… 173
4.5.4 密钥托管的主要功能 …… 174
4.5.5 密钥托管的步骤 …… 175
4.5.6 密钥托管体制的组成 …… 175
4.5.7 部分密钥托管技术 …… 176
第 5 章 访问控制技术 …… 178
5.1 访问控制原理 …… 178
5.1.1 访问控制的要素 …… 178
5.1.2 访问控制的组件 …… 180
5.2 访问控制的策略和机制 …… 182
5.2.1 访问控制策略 …… 183
5.2.2 访问控制机制 …… 187
5.3 自主访问控制 …… 190
5.3.1 基于行的自主访问控制 …… 191
5.3.2 基于列的自主访问控制 …… 193
5.3.3 自主访问控制策略的局限性 …… 194
5.4 强制访问控制 …… 195
5.4.1 BLP 模型 …… 198
5.4.2 Biba 模型 …… 203

5.4.3 强制访问控制的局限性 …… 204
5.5 基于角色的访问控制 …… 205
5.5.1 角色的概念 …… 206
5.5.2 RBAC 的基本原理 …… 207
5.6 基于任务的访问控制 …… 210
5.6.1 TBAC 模型结构 …… 211
5.6.2 TBAC 模型的特性分析 …… 213
5.7 访问控制与授权 …… 213
5.7.1 授权行为 …… 213
5.7.2 信任模型 …… 214
第 6 章 操作系统安全和数据库安全 …… 218
6.1 操作系统安全概述 …… 218
6.1.1 操作系统安全性要求 …… 218
6.1.2 操作系统安全威胁概述 …… 219
6.1.3 操作系统安全级别 …… 220
6.2 操作系统安全机制 …… 222
6.2.1 硬件安全机制 …… 222
6.2.2 身份认证机制 …… 223
6.2.3 访问控制机制 …… 224
6.2.4 最小特权管理机制 …… 225
6.2.5 可信通道机制 …… 225
6.2.6 安全审计机制 …… 226
6.3 Windows 2000/XP 的安全机制 …… 226
6.3.1 账户管理机制 …… 227
6.3.2 登录验证 …… 227
6.3.3 系统访问控制 …… 228
6.3.4 Windows 2000 的安全策略 …… 230
6.4 Linux/Unix 的安全机制 …… 231
6.4.1 标识与认证 …… 232
6.4.2 访问控制 …… 233
6.4.3 最小特权管理 …… 233
6.4.4 安全审计 …… 234
6.4.5 网络安全性 …… 234
6.5 数据库安全概述 …… 234

6.5.1 数据库安全概念 …… 234
6.5.2 数据库安全威胁 …… 235
6.5.3 数据库安全策略 …… 236
6.5.4 数据库安全需求 …… 236
6.5.5 数据库安全与操作系统安全的关系 …… 237
6.6 数据库安全技术 …… 239
6.6.1 数据库加密 …… 239
6.6.2 视图机制 …… 246
6.6.3 数据库备份与恢复 …… 247
6.6.4 数据库审计 …… 252
6.7 我国数据库管理系统安全评估标准 …… 253
6.8 实例分析——SQL Server 数据库系统安全分析 …… 254
6.8.1 SQL Server 的安全模式 …… 254
6.8.2 使用和管理用户账号 …… 255
6.8.3 使用视图增强安全性 …… 257
6.8.4 SQL Server 的数据加密 …… 257
6.9 反病毒技术 …… 258
6.9.1 病毒概论 …… 258
6.9.2 病毒的特征 …… 259
6.9.3 病毒的分类 …… 260
6.9.4 反病毒技术 …… 261
6.9.5 计算机病毒的查杀工具简介 …… 263
6.9.6 邮件病毒及其防范 …… 267
第7章 网络安全技术 …… 269
7.1 入侵检测 …… 269
7.1.1 入侵检测概述 …… 269
7.1.2 入侵检测系统的结构 …… 272
7.1.3 入侵检测的未来发展趋势 …… 275
7.2 安全扫描 …… 279
7.2.1 安全扫描技术概述 …… 279
7.2.2 端口扫描技术 …… 280
7.2.3 漏洞扫描技术 …… 283
7.2.4 操作系统探测技术 …… 284
7.3 防火墙技术 …… 285