普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

信息安全管理

Xinxi Anquan Guanli

徐国爱　彭俊好　张　淼　编著

北京邮电大学出版社
www.buptpress.com

普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

信息安全管理

徐国爱　彭俊好　张淼　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书作为信息安全系列教材之一，在汇总作者及所在团队多年来信息安全管理相关工作的基础上，还提炼了国内和国际上信息安全管理方面的最新成果。本书在保证知识点讲解精炼的基础上，全面吸纳了最新国内外信息安全管理相关标准和指南的内容，能够反映出信息安全管理理及与方法的研究和应用现状。

本书内容共9章。第1章是绪论。第2章是信息安全控制规范。第3章是信息系统安全审计。第4章是信息安全事件管理。第5章是信息安全风险评估。第6章是信息安全管理体系实施。第7章是信息安全测评认证。第8章是信息安全工程管理。第9章是信息安全法规标准。

本书适用于高等院校通信专业本科教材，也可作为相关专业技术人员的参考书目。

图书在版编目(CIP)数据

信息安全管理/徐国爱，彭俊好，张森编著. —北京：北京邮电大学出版社，2008

ISBN 978-7-5635-1671-1

Ⅰ.信… Ⅱ.①徐…②彭…③张… Ⅲ.信息系统—安全管理—教材 Ⅳ.TP309

中国版本图书馆CIP数据核字(2008)第033918号

书　　名：信息安全管理

作　　者：徐国爱　彭俊好　张　森

责任编辑：满志文

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路10号(邮编：100876)

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京市梦宇印务有限公司

开　　本：787 mm×960 mm　1/16

印　　张：20.25

字　　数：441千字

印　　数：1—5 000册

版　　次：2008年6月第1版　2008年6月第1次印刷

ISBN 978-7-5635-1671-1　　定　价：36.00元

信息安全专业系列教材（第2版）

编 委 会

第2版总序

发展21世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。2004年，灵创团队北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被教育部列入了“普通高等教育‘十五’国家级规划教材”。至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设和校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。2005年，作为组长单位我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”。我们完成的国内第一次制定的信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分，构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系。我们在国内第一次较全面地提出信息安全学科专业教学改革与创新的研究以及发展思路和政策建议；这些成果已提交教育部相关教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平起到了重要的作用。多所举办信息安全专业的高校都参照该课题成果调整了自己的教学计划、课程体系和实验方案。

我们积极搭建信息安全专业校际交流平台，组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”和“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地40亩的全国信息安全专业本科生实习实训基地，接受了来自全国近30所高校的本科生进入该基地参加丰富多彩的实训。

我们努力建设精品课程，主办了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北京邮电大学，介绍了精品课程建设的经验。我们组织建设了全国第一批信息安全实验室，并且编写出版了实验教材《信息安全实验指导》，我们的《现代密码学》课程已经被评为北京市精品课程，并在2007年度被评为“国家精品课程”。

经过灵创团队全体人员的共同努力，北京邮电大学信息安全本科专业被教育部评为

第二类优势特色专业。

三年多的时间过去了，无论信息安全的教育和产业都取得了丰硕的成果，随着信息安全向更高层次的发展，其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要，积极探索培养创新型高素质人才，我们按照制定的学科发展战略和专业规范的精神，结合近几年的教学实践，我们对这套信息安全专业本科系列教材进行了全面修订，并及时成立了灵创团队北京邮电大学数字内容研究中心。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善，还补充了信息安全最新的研究成果，使教材的内容更加翔实和新颖。同时，在原有的教材上又增加了一些新的课程教材，在新修订的系列教材中，目前有《信息安全概论》(第2版)、《现代密码学及其应用》、《网络安全》(第2版)、《信息安全管理》、《计算机病毒原理及防治》(第2版)、《数字版权管理》、《计算机系统安全》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》、《数字图像取证技术》等13本教材，今后随着信息安全专业教学的需要，还将不断地有新的教材补充到这个系列中来，使之更加完善和系统。目前，计划列入的相关教材还有：《入侵检测》(第2版)、《信息内容安全》、《信息安全工程》、《软件安全》及《信息安全标准与法律法规》等。

我们组织了强大的师资队伍，广泛吸收了有着丰富教学科研经验并多次讲授该系列教材的教师充实到这次修订工作中。作者队伍中不但包括北京邮电大学的教师，还包括哈尔滨工程大学、北京交通大学等重点院校的教师。经过反复研讨，本着理论与实际相结合的原则，对原来的系列教材进行了较大的修改和扩充，我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向专业的不同需求。

这次修订我们对内容进行了精心的组织和安排，希望能促进信息安全课程的建设，涌现出更多的信息安全精品课程。虽然我们在这次修订中投入了很大精力，但是由于水平有限，时间仓促，且信息安全专业的发展速度非常快，书中的不足之处和错误在所难免，我们衷心期望使用和关心该系列教材的师生，继续对新的系列教材提出宝贵的意见和建议。

本套系列教材也是国家重点基础研究发展计划(973)(课题编号：2007CB310704和2007CB311203)资助的成果，并被教育部增补为“普通高等教育‘十一五’国家级规划教材”的选题。

在本系列教材的修订过程中，得到了北京邮电大学出版社的大力支持，同时也得到了灵创团队的骨干机构(北京邮电大学信息安全中心和北京邮电大学数字内容研究中心)三百余位成员的支持与配合，在此一并表示感谢。

教授、博导、长江学者特聘教授

杨义先

2007年7月

前　言

随着人们对信息技术依赖程度的不断加深，信息安全受到了社会的普遍关注。通过技术手段针对性地解决信息安全问题是信息安全防范的基本思路，然而，由于信息安全的多层次、多因素和动态性等特点，管理手段的应用在一个完整的信息安全防范方案中必不可少。信息安全管理的模型、流程和方法最近几年有了长足的发展，信息安全管理的相关标准、法规也如雨后春笋般相继被推出。三分技术、七分管理的信息安全理念正在为社会各界广泛接受。

北京邮电大学信息安全中心从1984年以来，一直专注于信息安全领域的理论和应用研究，中心先后承担过数项国家级信息安全相关课题的研究，并成功的将其中的大部分成果实现商业转化，为国家信息化建设做出了不错的贡献。信息安全系列教材是我们专为信息安全教学和科研推出的一款系列书籍，内容涵盖信息安全领域的方方面面。系列教材既可作为高等院校信息安全及相关专业研究生和高年级本科生的教材使用，也可作为相关专业人员全面参考的系列手册。

作为信息安全系列教材之一，本书在汇总作者及所在团队多年来信息安全管理相关工作的基础上，还提炼了国内和国际上信息安全管理方面的最新成果。本书在保证知识点讲解精炼的基础上，全面吸纳了最新国内外信息安全管理相关标准和指南的内容，能够反映出信息安全管理理论与方法的研究和应用现状。本书通过第1章梳理了各种信息安全管理理论、方法和流程的内涵及它们之间的关系，并以此展开全书的主体内容。本书主体内容分为三个部分，第一部分在介绍信息安全管理控制规范的基础上，没有全面展开对信息安全技术的介绍，而突出介绍了偏于管理的信息安全技术内容——信息系统安全审计，这包括第2～3章；第二部分包括第4～8章，依次介绍了信息安全事件管理、信息安全风险评估、信息安全管理体系实施、信息安全测评认证和信息安全工程管理等信息安全管理的主流方法；最后，在第三部分集中介绍了作为信息安全保障体系关键内容的信息安全法规标准，这就是第9章。

本书由北京邮电大学信息安全中心组织编写。徐国爱参与了第1、3章的编写，彭俊好参与了第4～6章的编写，刘凡凡参与了第6章的编写，陈晓光参与了第2、8章的编写，汤永利参与了第6、9章的编写，李娜参与了第7章的编写，朱伽参与了第9章的编写；朱强、吴正华、牛婷芝、刘嘉、姜磊、李娜、姚志东、肖靖、郜小亮、张建武、郭承青和高洋等共同参与了资料收集、整理工作；全书由徐国爱、彭俊好统稿，张淼协助。此外，本书得到了胡

正明教授、杨义先教授、钮心忻教授和罗群副教授的大力支持和指导，他们对书中的内容提出了宝贵的意见，在此一并表示衷心的感谢。

本书在编写过程中，除引用了作者自身的研究内容和成果之外，还大量参考了众多国内外优秀论文、书籍以及互联网上公布的相关资料，我们尽量在书后面的参考文献中列出，但由于互联网上资料数量众多、出处杂乱，可能无法将所有文献一一注明出处。我们对这些资料的作者表示由衷的感谢，同时声明，原文版权属于原作者。

本书作为教材，教师在讲授时可以根据学时安排做出一些取舍。本书全部讲授建议34学时；如果有更多学时安排，建议酌情增加信息安全技术方面的内容，以深化对全书内容的理解。

信息安全管理是信息安全领域中新的分支，代表了信息安全发展的一种趋势，本书尝试对此领域的理论和方法做一些归纳，以期有益于读者。由于作者的水平有限，书中难免有一些缺点和错误，真诚希望读者不吝赐教，以期再版修订。

编 者

目　　录

第1章

绪　论

信息安全管理是保障信息系统安全的有力手段，是当今世界各国都在努力推广与应用的重点课题。它涉及的内容广泛，包括技术、方法、模型、保障体系等多方面内容。本章对信息安全管理的概念、模型、技术体系、基本方法、保障体系等内容进行了概要的阐述，并对本书的内容安排进行了说明。

1.1　信息安全管理

1.1.1 什么是信息安全管理

信息技术创立、应用和普及是20世纪技术革新最伟大的创举之一，藉此，人类正在进入信息化社会，人们对信息、信息技术的依赖程度越来越高。一方面，信息已成为一种崭新的资产，在政治、经济、军事、教育、科技和生活等方面发挥着重要的作用，另一方面，由此而带来的信息安全问题正变得日益突出。由于信息具有易传输、易扩散、易破损的特点，信息资产比传统资产更加脆弱，更易受到损害，信息及信息系统需要严格管理和妥善保护。

网络技术的发展加速了信息的传输与处理，缩短了人们之间的时空距离，方便了交流；同时，对信息安全提出了新的挑战。据统计，全球平均每20秒就发生一次计算机病毒的入侵；互联网上的防火墙大约25%被攻破；窃取商业信息的事件平均以每月260%的速度增加；约70%的网络主管报告因机密信息泄露而受到损失。国家与国家之间的信息战问题更是关系到国家的根本安全问题。

关于信息安全，不同组织有不同的定义，国际标准化组织对信息安全的定义是："在技术上和管理上为数据处理系统建立的安全保护，保护计算机硬件、软件和数据不因偶然和