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

（第2版）

Xinxi Anquan Guanli

徐国爱　陈秀波　郭燕慧　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

本书受2010年教育部-IBM精品课程建设项目及国家自然科学基金
(课题编号:61003287,61170272)的资助

信息安全管理

（第2版）

徐国爱　陈秀波　郭燕慧　编著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书作为信息安全系列教材之一——《信息安全管理》的再版，在广泛吸纳读者意见和建议的基础上，不仅仍定位于信息安全管理的基本概念、信息安全管理的各项内容和任务的讲解，还从内容安排和内容选取方面做了全面的优化。和第1版相比，本书的内容更为系统、内容组织更为精致，并适当加入了国内和国际上信息安全技术和管理方面的最新成果，反映出信息安全管理及与方法的研究和应用现状。

本书内容共8章。第1章是绪论。第2章是信息安全风险评估。第3章是系统与网络安全。第4章是物理安全。第5章是信息系统安全审计。第6章是灾难恢复与业务连续性。第7章是信息安全标准。第8章是信息安全法律法规。每章后面配有习题以巩固相关知识，另外配有大量的参考文献。

本书可作为高等院校信息安全专业本科、研究生教材，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，陈秀波，郭燕慧编著. --2版. --北京：北京邮电大学出版社，2011.11
ISBN 978-7-5635-2751-9

Ⅰ.信… Ⅱ.①徐…②陈…③郭… Ⅲ.①信息系统—安全管理—高等学校—教材 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2011)第190329号

书　　名：信息安全管理(第2版)
著作责任者：徐国爱　陈秀波　郭燕慧　编著
责任编辑：李欣一
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：北京联兴华印刷厂
开　　本：787 mm×960 mm　1/16
印　　张：18.25
字　　数：399千字
印　　数：1—3 000册
版　　次：2008年9月第1版　2011年11月第2版　2011年11月第1次印刷

ISBN 978-7-5635-2751-9　　定　价：36.00元

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》、《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。信息安全管理作为战略、信息安全技术作为手段，“三分技术、七分管理”的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，并成功地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。本书第1章概述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。第2章（保留第1版的内容）介绍了信息安全风险评估的原则和方法。第3章对信息安全技术基本内容——系统与网络安全技术进行了全面的介绍。在此基础上，第4章、第5章（保留第1版内容）和第6章依次对信息安全管理中涉及的物理安全、信息安全审计、灾难恢复与业务连续性等偏于管理的内容进行了介绍。最后，在第7章、第8章中系统介绍了信息安全保障体系中的关键内容——信息安全标准和法规。

本书由北京邮电大学信息安全中心组织编写。参加本书编写工作的有：徐国爱、陈秀波、郭燕慧，徐国爱对全书进行统稿。张淼老师及齐雅楠、钟征燕、尚程、耿贵宁等几位研究生参与了本书部分章节的资料收集和整理，诚挚感谢他们对本书所做的贡献。

本书在编写过程中，除引用了作者自身的研究内容和成果外，还大量参考了众多国外优秀论文、书籍以及在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36学时，如有更多学时安排，建议酌情增加信息安全管理实践方面的内容，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的新的分支，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。

编著者

2011年9月

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、保障体系等多方面内容。本章对信息安全管理的概念、技术体系、基本方法、保障体系等内容进行了概要的阐述，并对本书内容安排进行了说明。

1.1　信息安全

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，借此，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。与此同时，信息安全问题日渐突出，情况也越来越复杂。

1.1.1　信息安全的现状

由于信息具有易传输、易扩散、易破损的特点，因此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。

1988年11月2日，康奈尔大学的研究生罗伯特·莫里斯(22岁)设计了第一个蠕虫程序，设计初始目的是验证网络中自动传播程序的可行性。该程序感染了6 000台计算机，使因特网(Internet)不能正常运行，造成的经济损失达1亿美元。程序只有99行，利用了UNIX系统中的缺点，用Finger命令查联机用户名单，然后破译用户口令，用Mail系统复制、传播本身的源程序，再编译生成代码。莫里斯因此被判三年缓刑、罚款1万美元、做400小时的社区服务。

1998年6月2日，首次出现关于CIH病毒的报道。CIH病毒是由台湾大学生陈盈

豪编写，其动机是“为自己设计病毒”。CIH 病毒 1998 年 4 月 26 日首次发作，可导致主板、硬盘损坏，变种版本极多，危害严重；1999 年 4 月 26 日，CIH 1.2 版本首次大范围爆发，全球超过六千万台计算机被不同程度破坏；2000 年 4 月 26 日，CIH 1.2 版本第二次大范围爆发，全球损失超过十亿美元；2001 年 4 月 26 日，CIH 第三次大范围爆发。仅北京就有超过六千台计算机遭 CIH 病毒破坏，瑞星修复硬盘数量当天接近 400 块。

2000 年 5 月 4 日，“爱虫(LOVE BUG)”病毒大爆发。主要表现是邮件群发、修改文件、消耗网络资源。“爱虫”病毒大爆发两天之后，全球约有 4 500 万台计算机被感染，造成的损失已经达到 26 亿美元。此后几天里，“爱虫”病毒所造成的损失还在以每天 10 亿美元到 15 亿美元的速度增加。

不断发生的信息安全事件，对信息安全提出了严峻的挑战。据统计，全球平均每 20 秒就发生一次计算机病毒的入侵；互联网上大约 25％的防火墙被攻破；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。信息安全已成为信息社会重要的研究课题。

1.1.2 信息安全的概念

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恶意的原因而遭到破坏、更改和泄露”。信息安全的内涵已从传统的机密性、完整性和可用性三个方面扩展到机密性、完整性、可用性、真实性、可核查性、可靠性等更多领域。各信息安全属性含义如下：

- 机密性：信息不泄露给非授权的用户、实体或者过程的特性。
- 完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
- 可用性：可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。
- 真实性：内容的真实性。
- 可核查性：对信息的传播及内容具有控制能力，访问控制即属于可控性。
- 可靠性：系统的可靠性。

信息安全在技术发展和应用过程中，表现出以下重要特点：

(1) 必然性。当今的信息系统日益复杂，其中必然存在系统设计、实现、内部控制等方面的弱点。如果不采取适当的措施应对系统运行环境中的安全威胁，信息资产就可能会遭受巨大的损失甚至威胁到国家安全，所以，信息安全已引起许多国家，特别是发达国家的高度重视，他们在这个领域投入了大量的人力、物力、财力，以期提高本国的信息安全水平。

(2) 配角特性。信息安全建设在信息系统建设中角色应该是陪衬,安全不是最终目的,得到安全可靠的应用和服务才是安全建设的最终目的。不能为了安全而安全,安全的应用是先导。

(3) 动态性。信息安全威胁会随着技术的发展、周边应用场景的变化等因素而发生变化,新的安全威胁总会不断出现。所以,信息安全建设是一个动态的过程,不能指望一项技术、一款产品或一个方案就能一劳永逸地解决组织的安全问题,信息安全是一个动态、持续的过程,必须能根据风险变化及时调整安全策略。一成不变的静态策略,在信息系统的脆弱性以及威胁技术发生变化时将变得毫无安全作用,因此安全策略以及实现安全策略的安全技术和安全服务,应具有"风险监测——实时响应——策略调整——风险降低"的良性循环能力。

信息时代,信息安全不仅关系信息自身的安全,更是对国家安全具有重大战略价值。

(1) 信息安全与政治有关

政治的核心问题是国家政权问题。政治安全的内核是政府运行的有效性。任何国家政府的运行,都是凭借复杂的机制,经由安全的信息交换,实现对社会生活的有效指导、管理和控制。信息安全风险直接影响着政府的有效性,政治安全一刻也离不开信息安全。当今,来自敌对势力从信息空间发动的"政治进攻",主要表现为"网络政治动员"和"信息恐怖主义"两种方式。例如,1999 年 1 月份左右,美国黑客组织"美国地下军团"联合了波兰、英国的黑客组织,和世界上各个国家的一些黑客组织,有组织地对我国的政府网站进行了攻击。

虽然敌对势力经网络对我国的"政治进攻"行为,迄今在总体上还是可控的,但这类"政治进攻"已在某种程度上危害到了我国的政治安全。

(2) 信息安全与经济犯罪有关

由于信息技术的开放性与经济主体利益的冲突性并存,现实的信息系统存在着安全风险。我国自 1986 年发现首例利用计算机网络的犯罪以来,案件数量迅速增加,1986 年网络犯罪发案仅 9 起,2000 年即剧增到 2 700 余起,2008 年全年突破 4 500 起,诈骗、敲诈、窃取等形式的网络犯罪涉案金额从数万元发展到数百万元,其造成的巨额经济损失难以估量,其中计算机网络犯罪在金融行业尤为突出,金融行业计算机网络犯罪案件发案比例占整个计算机犯罪比例高达 61%。

(3) 信息安全与社会稳定有关

在高科技和信息化条件下,网络具有传播速度快、信息海量化、交互功能强等特点,不法分子利用互联网上散布一些虚假信息、有害信息对社会管理秩序造成的危害,要比现实社会中一个造谣要大得多。例如,1999 年 4 月,河南商都热线一个 BBS,一个题为"交通银行郑州支行行长携巨款外逃"的帖子,造成了社会的动荡,三天十万人上街排队,挤提了十亿元。而针对社会公共信息基础设施的攻击则会严重扰乱社会管理秩序。2001 年 2 月 8 日正是春节,新浪网遭受攻击,电子邮件服务器瘫痪了 18 个小时。造成了几百万用

户无法正常地联络。

1.1.3 信息安全威胁

所谓信息安全威胁就是指对信息资源的保密性、完整性、可用性或合法使用所造成的危险。对安全威胁的深入分析，是安全防范的基础。

1. 信息安全威胁分类

下面给出一些常见的安全威胁。

(1) 有害程序

- 计算机病毒：是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能够自我复制的一组计算机指令或者程序代码。
- 蠕虫：是指除计算机病毒以外，利用信息系统缺陷，通过网络自动复制并传播的有害程序。
- 木马程序：是指伪装在信息系统中的一种有害程序，具有控制该信息系统或进行信息窃取等对该信息系统有害的功能。
- 僵尸网络：是指网络上受到黑客集中控制的一群计算机，它可以被用于伺机发起网络攻击，进行信息窃取或传播木马、蠕虫等其他有害程序。
- 网页内嵌恶意代码：是一种特殊的程序，它把代码在不被察觉的情况下镶嵌到网页中，当用户浏览该网站时被浏览器执行，从而达到破坏被感染计算机数据、运行具有入侵性或破坏性的程序，破坏被感染计算机数据的完全性和完整性的目的。
- 其他有害程序。

(2) 网络攻击

- 拒绝服务攻击：利用信息系统缺陷、或通过暴力攻击的手段，大量消耗信息系统的CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行的攻击行为。
- 后门攻击：利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施的攻击。
- 漏洞攻击：利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施的攻击。
- 网络扫描窃听：利用网络扫描或窃听软件，获取信息系统网络配置、端口、服务、存在的脆弱性等特征信息的行为。
- 干扰：通过技术手段对网络进行干扰，或对广播电视有线或无线传输网络进行插播，对卫星广播电视信号非法攻击等。
- 其他网络攻击。

(3) 信息破坏

- 信息篡改：未经授权将信息系统中的信息更换为攻击者所提供的信息，例如网页篡改。