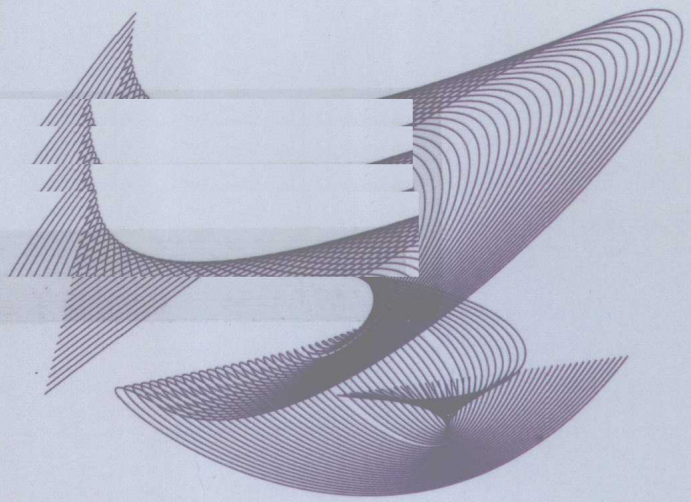
普通高等教育“十一五”国家级规划教材

“信息化与信息社会”系列丛书之
高等学校信息管理与信息系统专业系列教材

信息系统安全



林国恩　李建彬　编著

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

普通高等教育“十一五”国家级规划教材

“信息化与信息社会”系列丛书之

高等学校信息管理与信息系统专业系列教材

信息系统安全

林国恩　李建彬　编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书作为全国普通高等教育“十一五”国家级规划教材，内容包括信息系统安全基本概念、信息系统安全体系、信息系统安全管理目标、信息系统安全需求、风险管理与控制、风险评估与分析、信息系统安全技术、信息安全标准与法律法规。本书结合目前信息系统安全的教学研究和实践需要，并以网上银行系统为例，介绍了安全信息系统具体实现的过程；此外，本书也介绍了比较新颖的责任追究技术，以及在信息系统安全研究领域中引入“机构组织结构”（Enterprise Architecture）和“信息系统的安全开发生命周期”（Security Considerations in the Information System Development Life Cycle）等与信息管理相关的概念。

本书强调管理手段对信息系统安全的重要性，分析安全技术与安全管理的互动，突出信息管理对安全技术提出的需求及安全技术对信息管理的影响，并把软件工程中的软件生命周期的概念引入信息系统安全领域，从开发过程管理的角度提高安全措施的可信性。

本书着重从实践的角度，对信息系统安全概念、信息系统需求、信息系统的设计（包括安全技术应用和安全管理两方面）、信息系统的实践作概况性介绍，同时尽量采用当前国际信息安全研究领域的最新成果和研究方向，便于读者能够了解信息安全研究的最新动态。

本书主要供计算机专业和信息系统管理专业的本科生和研究生作为信息安全课程的教材使用。同时，本书也适合信息安全管理人员作为参考书在信息系统开发过程中使用。希望读者在阅读本书时，能从管理与实践的角度，重新认识和理解信息安全的概念。

图书在版编目（CIP）数据

信息系统安全 / 林国恩，李建彬编著. —北京：电子工业出版社，2010.3
（“信息化与信息社会”系列丛书. 高等学校信息管理与信息系统专业系列教材）
普通高等教育“十一五”国家级规划教材
ISBN 978-7-121-10410-7

I. 信… II. ①林… ②李… III. 信息系统－安全技术－高等学校－教材 IV. TP309

中国版本图书馆 CIP 数据核字（2010）第 028296 号

策划编辑：刘宪兰
责任编辑：徐云鹏　　特约编辑：宋兆武
印　　刷：北京智力达印刷有限公司
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：787×1092　1/16　印张：16.25　字数：410 千字
印　　次：2010 年 3 月第 1 次印刷
印　　数：4 000 册　　定价：27.00 元

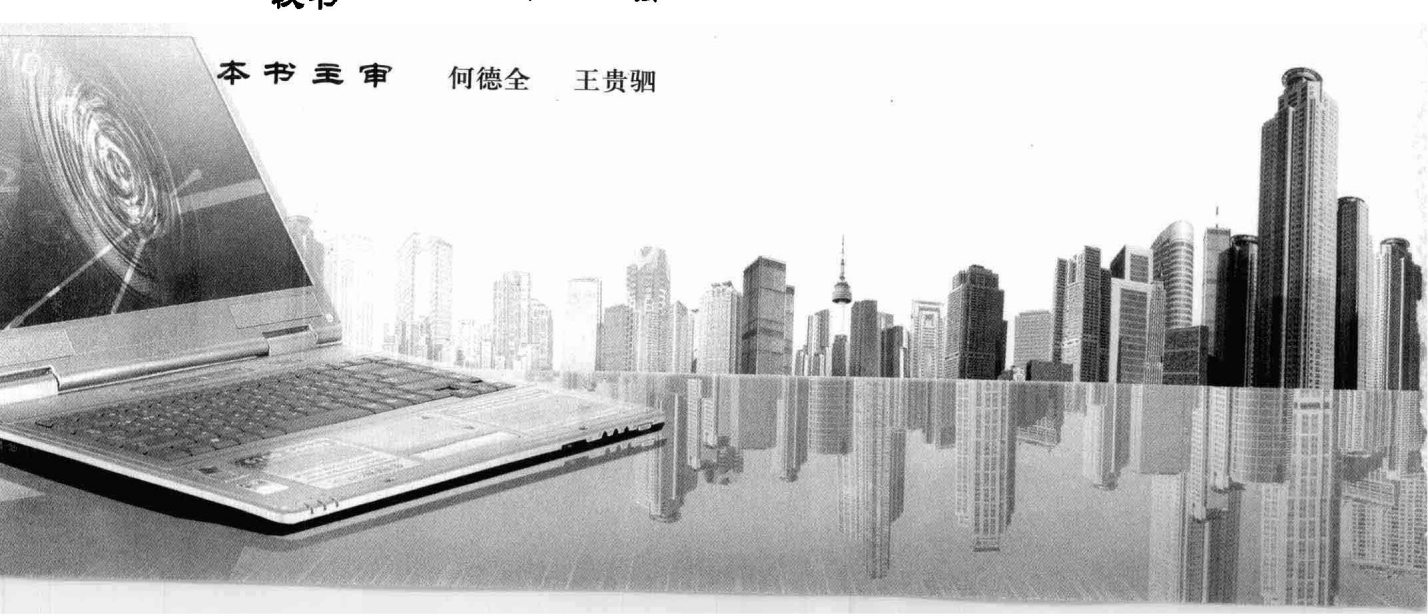
凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

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。

“信息化与信息社会”系列丛书编委会名单

高等学校信息管理与信息系统专业系列教材编委会名单



作 者 简 介

林国恩，清华大学软件学院教授、博士生导师，信息系统安全（教育部）重点实验室主任，国家自然科学基金委员会“可信软件基础研究”重大研究计划专家指导组成员。1987 年获英国伦敦大学计算机科学一级荣誉学士学位，1990 年获英国剑桥大学博士学位。自 1990 年起，曾经分别在英国伦敦大学和新加坡国立大学任教；曾经是英国剑桥大学 Isaac Newton 学院访问学者，担任过欧洲系统安全学院访问教授、香港政府与新加坡政府信息安全顾问；曾经主持过多项电子银行和电子政务信息系统的安全设计。因在信息系统领域做出的突出成绩，于 1998 年获得由日本工商会（Japanese Chamber of Commerce and Industry）颁发的新加坡基本建设奖（Singapore Foundation Award）。

李建彬，中科院软件所客座研究员，全国信息安全标准化技术委员会（TC260）委员，国家信息安全等级保护安全建设指导专家委员会成员，清华大学信息系统安全（教育部）重点实验室学术委员会委员。1992 年获清华大学计算机科学与技术系学士学位，1995 年获中国地震局分析预报中心理学硕士。长期从事国家重要信息系统网络与信息安全管理工作，在信息安全管理体系、风险评估、等级保护、灾难备份、应急响应等方面有较丰富的实际工作经验和理论水平。目前供职于国家税务总局电子税务管理中心。

总　序

信息化是世界经济和社会发展的必然趋势。近年来，在党中央、国务院的高度重视和正确领导下，我国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。

作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会一直在按照党中央、国务院领导同志的要求就信息化前瞻性、全局性和战略性的问题进行调查研究，提出政策建议和咨询意见。在做这些工作的过程中，我们越来越认识到，信息技术和信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力，大量培养符合中国信息化发展需要的人才已成为国家信息化发展的一项紧迫需求，成为我国应对当前严峻经济形势，推动经济发展方式转变，提高在信息时代参与国际竞争的优势的关键。2006 年 5 月，我国公布《2006—2010 年国家信息化发展战略》，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。

为了促进上述目标的实现，国家信息化专家咨询委员会一直致力于通过讲座、论坛、出版等各种方式推动信息化知识的宣传、教育和培训工作。2007 年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了《信息化与信息社会》系列丛书编委会，共同推动《信息化与信息社会》系列丛书的组织编写工作。编写该系列丛书的目的，是力图结合我国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效地梳理信息化的基本概念和知识体系，通过高校教师、信息化专家学者与政府官员之间的相互交流和借鉴，充实我国信息化实践中的成功案例，进一步完善我国信息化教学的框架体系，提高我国信息化图书的理论和实践水平。毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一项重要举措，对于推动国家的信息化人才教育和培养工作，加强我国信息化人才队伍的建设具有重要意义。

考虑当前国家信息化人才培养的需求、各个专业和不同教育层次（博士生、硕士生、本科生）的需要，以及教材开发的难度和编写进度时间等问题，《信息化与信息社会》系列丛书编委会采取了集中全国优秀学者和教师、分期分批出版高质量的信息化教育丛书

的方式，根据当前高校专业课程设置情况，先开发“信息管理与信息系统”、“电子商务”、“信息安全”三个本科专业高等学校系列教材，随后再根据我国信息化和高等学校相关专业发展的情况陆续开发其他专业和类别的图书。

对于新编的三套系列教材（以下简称“系列教材”），我们寄予了很大希望，也提出了基本要求，包括信息化的基本概念一定要准确、清晰，既要符合中国国情，又要与国际接轨；教材内容既要符合本科生课程设置的要求，又要紧跟技术发展的前沿，及时把新技术、新趋势、新成果反映在教材中；教材还必须体现理论与实践的结合，要注意选取具有中国特色的成功案例和信息技术产品的应用实例，突出案例教学，力求生动活泼，达到帮助学生学以致用的目的，等等。

为力争出版一批精品教材，《信息化与信息社会》系列丛书编委会采用了多种手段和措施保证系列教材的质量。首先，在确定每本教材的第一作者的过程中引入了竞争机制，通过广泛征集、自我推荐和网上公示等形式，吸收优秀教师、企业人才和知名专家参与写作；其次，将国家信息化专家咨询委员会有关专家纳入各个专业编委会中，通过召开研讨会和广泛征求意见等多种方式，吸纳国家信息化一线专家、工作者的意见和建议；再次，要求各专业编委会对教材大纲、内容等进行严格的审核，并对每一本教材配有一至两位审稿专家。

如今，我们很高兴地看到，在教育部和原国务院信息化工作办公室的支持下，通过许多高校教师、专家学者及电子工业出版社的辛勤努力和付出，《信息化与信息社会》系列丛书中的三套系列教材即将陆续和读者见面。

我们衷心期望，系列教材的出版和使用能对我国信息化相应专业领域的教育发展和教学水平的提高有所裨益，对推动我国信息化的人才培养有所贡献。同时，我们也借系列教材开始陆续出版的机会，向所有为系列教材的组织、构思、写作、审核、编辑、出版等做出贡献的专家学者、老师和工作人员表达我们最真诚的谢意！

应该看到，组织高校教师、专家学者、政府官员及出版部门共同合作，编写尚处于发展动态之中的新兴学科的高等学校教材，还是一个初步的尝试。其中，固然有许多的经验可以总结，也难免会出现这样那样的缺点和问题。我们衷心地希望使用系列教材的教师和学生能够不吝赐教，帮助我们不断地提高系列教材的质量。

曲维枝

2008 年 12 月 15 日

序　言

日新月异的技术发展及应用变迁不断给信息系统的建设者与管理者带来新的机遇和挑战。例如，以 Web 2.0 为代表的社会性网络应用的发展深层次地改变了人们的社会交往行为以及协作式知识创造的形式，进而被引入企业经营活动中，创造出内部 Wiki（Internal Wiki）、预测市场（Prediction Market）等被称为“Enterprise 2.0”的新型应用，为企业知识管理和决策分析提供了更为丰富而强大的手段；以“云计算”（Cloud Computing）为代表的软件和平台服务技术，将 IT 外包潮流推向了一个新的阶段，像电力资源一样便捷易用的 IT 基础设施和计算能力已成为可能；以数据挖掘为代表的商务智能技术，使得信息资源的开发与利用在战略决策、运作管理、精准营销、个性化服务等各个领域发挥出难以想象的巨大威力。对于不断推陈出新的信息技术与信息系统应用的把握和驾驭能力，已成为现代企业及其他社会组织生存发展的关键要素。

根据 2008 年中国互联网络信息中心（CNNIC）发布的《第 23 次中国互联网络发展状况统计报告》显示，我国的互联网用户数量已超过 2.98 亿人，互联网普及率达到 22.6%，网民规模全球第一。与 2000 年相比，我国互联网用户的数量增长了 12 倍。换句话说，在过去的 8 年间，有 2.7 亿中国人开始使用互联网。可以说，这样的增长速度是世界上任何其他国家所无法比拟的，并且可以预期，在今后的数年中，这种令人瞠目的增长速度仍将持续，甚至进一步加快。伴随着改革开放的不断深入，互联网的快速渗透推动着中国经济、社会环境大步迈向信息时代。从而，我国“信息化”进程的重心，也从企业生产活动的自动化，转向了全球化、个性化、虚拟化、智能化、社会化环境下的业务创新与管理提升。

长期以来，信息化建设一直是我国国家战略的重要组成部分，也是国家创新体系的重要平台。近年来，国家在中长期发展规划及一系列与发展战略相关的文件中充分强调了信息化、网络文化和电子商务的重要性，指出信息化是当今世界发展的大趋势，是推动经济社会发展和变革的重要力量。《2006—2020 年国家信息化发展战略》提出要能“适应转变经济增长方式、全面建设小康社会的需要，更新发展理念，破解发展难题，创新发展模式”，这充分体现出信息化在我国经济、社会转型过程中的深远影响，同时也是对新时期信息化建设和人才培养的新要求。

在这样的形势下，信息管理与信息系统领域的专业人才，只有依靠开阔的视野和前瞻性的思维，才有可能在这迅猛的发展历程中紧跟时代的脚步，并抓住机遇做出开拓性

的贡献。另外，信息时代的经营、管理人才和知识经济环境下各行各业的专业人才，也需要拥有对信息技术发展及其影响力的全面认识和充分的领悟，才能在各自的领域之中把握先机。

因此，信息管理与信息系统的专业教育也面临着持续更新、不断完善的迫切要求。我国信息系统相关专业的教育已经历了较长时间的发展，形成了较为完善的体系，其成效也已初步显现，为我国信息化建设培养了一大批骨干人才。但我们仍然应该清醒地意识到，作为一个快速更迭、动态演进的学科，信息管理与信息系统专业教育必须以综合的视角和发展的眼光不断对自身进行调整和丰富。本系列教材的编撰，就是希望能够通过更为系统化的逻辑体系和更具前瞻性的内容组织，帮助信息管理与信息系统相关领域的学生及实践者更好地掌握现代信息系统建设与应用的基础知识和基本技能，同时了解技术发展的前沿和行业的最新动态，形成对新现象、新机遇、新挑战的敏锐洞察力。

本系列教材的宗旨在于体系设计上较全面地覆盖新时期信息管理与信息系统专业教育的各个知识层面，既包括宏观视角上对信息化相关知识的综合介绍，也包括对信息技术及信息系统应用发展前沿的深入剖析，同时也提供了对信息管理与信息系统建设各项核心任务的系统讲解。此外，还对一些重要的信息系统应用形式进行重点讨论。本系列教材主题涵盖信息化概论、信息与知识管理、信息资源开发与管理、管理信息系统、商务智能原理与方法、决策支持系统、信息系统分析与设计、信息组织与检索、电子政务、电子商务、管理系统模拟、信息系统项目管理、信息系统运行与维护、信息系统安全等内容。在编写中注意把握领域知识上的“基础、主流与发展”的关系，体现“管理与技术并重”的领域特征。我们希望，这套系列教材能够成为相关专业学生循序渐进了解和掌握信息管理与信息系统专业知识的系统性学习材料，同时成为知识经济环境下从业人员及管理者的有益参考资料。

作为普通高等教育“十一五”国家级规划教材，本系列教材的编写工作得到了多方面的帮助和支持。在此，我们感谢国家信息化专家咨询委员会及高等学校信息管理与信息系统系列教材编委会专家们对教材体系设计的指导和建议；感谢教材编写者的大量投入以及所在各单位的大力支持；感谢参与本系列教材研讨和编审的各位专家学者的真知灼见。同时，我们对电子工业出版社在本系列教材编辑和出版过程中所做的各项工作深表谢意。

由于时间和水平有限，本系列教材难免存在不足之处，恳请广大读者批评指正。

高等学校信息管理与信息系统
专业系列教材编委会
2009 年 1 月

前　言

21 世纪是信息时代，信息系统已成为社会发展的重要战略资源，社会信息化更是被公认为当今世界发展潮流的支柱和核心。信息系统的安全在信息社会中将扮演极为重要的角色，直接关系到国家机关的运作、企业经营和人们的日常生活。信息安全已成为信息社会中个人、企业乃至国家都极为重视的关键领域之一。

与此同时，安全技术也在飞速发展，密码、防火墙、访问控制、数字证书等技术不断革新，让人目不暇接。但这么多的安全技术如何应用到实际环境中，信息系统采用哪种安全技术和控制措施才能符合相关的国家法规和安全标准、满足机构的安全目标，都涉及技术以外的考虑因素。此外，随着人们对信息系统与信息系统安全的了解越趋成熟，信息系统的设计也从技术性问题逐渐变成一个管理领域的问题。因此在系统设计过程中，必须要考虑到机构的业务、目标等关键问题。

一般而言，传统观点认为，信息安全是计算机、通信、物理、数学等领域的交叉学科，但在今天的高度信息化的社会里，信息系统在各行各业及社会不同层面的广泛应用使得信息安全已不再是纯粹技术问题了。信息系统安全已发展成为计算机科学与信息系统管理两大领域中的一个新兴交叉学科。

但目前“信息安全”作为高等院校计算机专业中的一门课程，主要内容以密码学和安全技术为主线，缺少从系统管理角度介绍信息安全的内容。而这些内容对于信息安全专业人员、信息系统管理人员都是必需的。为填补这一信息系统管理角度的真空，本书比较全面系统地介绍了信息安全的全貌。希望读者在阅读本书时，能从管理与实践的角度，重新认识、理解信息安全的概念。

本书强调管理手段对信息系统安全的重要性，分析安全技术与安全管理的互动，突出信息管理对安全技术提出的需求及安全技术对信息管理的影响，并把软件工程中的软件生命周期的概念引入信息系统安全领域，从开发过程管理的角度提高安全措施的可信性。为了更有效地将这些管理问题纳入信息系统的设计考虑之中，本书把“机构组织结构”（Enterprise Architecture）的概念引入信息系统安全开发过程中。此外，本书也把“信息系统的安全开发生命周期”的概念引用到我们的信息系统安全构建方法中，以确保信息系统的设计可以在最早阶段便开始考虑信息安全的问题，分析信息系统的安全需求及实施相应的安全保护措施。

本书着重从实践的角度，对信息系统安全概念、信息系统需求、信息系统的设计（包括安全技术应用和安全管理两方面）、信息系统的实践作概况性介绍，同时尽量采用当前国际信息安全研究领域的最新成果和研究方向，便于读者能够了解信息安全研究的最新动态。

本书力求语言精练，注重内容的条理性、系统性和逻辑性，强调各部分之间的相互关联、前后呼应，希望有助于读者更好地理解和学习信息系统安全的相关理论和思想。全书共16章，大致分为6个部分。第1章为第1部分——信息系统安全概论，主要包括信息系统安全的发展历程、信息系统安全基本概念和信息系统安全体系。第2、3章构成本书的第2部分——信息系统安全需求，内容包括信息系统安全的管理目标和安全需求分析。第4～7章构成第3部分——信息系统安全管理，内容包括安全管理概述、风险管理与控制、风险分析与评估和安全管理措施。第8～12章构成第4部分——信息系统安全技术，内容包括网络安全技术、密码技术和安全协议应用、安全检测与审计和比较新颖的责任追究技术。第13、14章构成第5部分——信息系统安全标准规范与法律法规，内容包括当前的信息系统的相关法律法规及安全标准。第15、16章构成第6部分——信息系统安全实践，以网上银行系统为例，介绍了安全信息系统具体实现的过程。

本书主要供计算机专业和信息系统管理专业的本科生和研究生作为信息安全课程的教材使用。同时，也适合信息安全管理人员作为参考书在信息系统开发过程中使用。

本书由林国恩教授编著。李建彬研究员参加了教材编写思路的研讨工作，并负责风险评估和安全法律与标准两部分内容的编写。研究生施金洋、葛蒙、李隆璇、游之洋、龚伟和张兰参与了本书的编写和校稿工作。本书内容曾在清华大学软件工程专业本科生和硕士研究生的教学中讲授过。

从事信息安全研究的中国工程院何德全院士和中国信息安全测评中心副主任王贵驷，作为审稿人仔细审阅了书稿，提出了许多宝贵意见，使本书更加完善。大连理工大学李明楚教授、中国科学院赵险峰副研究员、北京信息科技大学王兴芬老师详细阅读了全稿，并提出许多有益的意见，在此谨向他们致以衷心的感谢。

由于编者水平有限，本书不妥甚至错误之处难免，诚盼专家和各位读者不吝指正。

作　者

2009年12月

目　录

第 1 部分　信息系统安全概论

第 2 部分　信息系统安全需求

第 3 部分 信息系统安全管理

第 4 部分 信息系统安全技术

第 5 部分 信息系统安全标准规范与法律法规

第 6 部分 信息系统安全实践