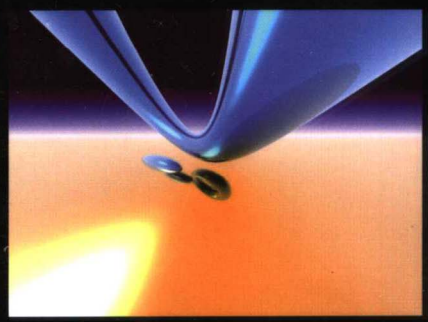
普通高等教育“十一五”国家级规划教材

21世纪高等院校
信息安全系列规划教材

信息安全管理

张红旗　王新昌
杨英杰　唐慧林　编著



人民邮电出版社
POSTS & TELECOM PRESS

普通高等教育“十一五”国家级规划教材

21世纪高等院校信息安全系列规划教材

信息安全管理

张红旗　王新昌　杨英杰　唐慧林　编著

人民邮电出版社

北京

图书在版编目（CIP）数据

信息安全管理 / 张红旗等编著. —北京：人民邮电出版社，2007.11
（21 世纪高等院校信息安全系列规划教材）
普通高等教育“十一五”国家级规划教材
ISBN 978-7-115-16966-2

Ⅰ. 信… Ⅱ. 张… Ⅲ. 信息系统—安全管理—高等学校—教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2007）第 155368 号

内 容 简 介

本书以构建信息安全管理体系为框架，全面介绍信息安全管理的基本概念、信息安全管理体系以及信息安全管理的各项内容和任务。全书共分 9 章，内容涵盖了信息安全管理的基本内涵、信息安全管理体系的建立与实施、信息安全风险管理、组织与人员安全管理、环境与实体安全管理、系统开发安全管理、运行与操作安全管理以及应急响应处置管理等。

本书注重知识的实用性，将理论与实际相结合，在全面介绍信息安全管理理论的基础上，选取典型信息安全管理实施案例进行分析，充分阐释了信息安全管理的实施过程，使读者能够在系统准确地把握信息安全管理思想的基础上，正确有效地运用信息安全管理的方法和技术分析解决实际问题。

本书可作为信息安全相关专业的本科生及研究生教材，或信息管理与信息系统专业及计算机相关专业的参考书，也可作为信息化管理人员、安全管理人员、网络与信息系统管理人员、IT 咨询顾问与 IT 技术人员的参考手册和培训教材。

普通高等教育“十一五”国家级规划教材

21 世纪高等院校信息安全系列规划教材

信息安全管理

◆ 编　　著　张红旗　王新昌　杨英杰　唐慧林
责任编辑　邹文波

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：14.25
字数：340 千字　　2007 年 11 月第 1 版
印数：1 - 3 000 册　　2007 年 11 月北京第 1 次印刷

ISBN 978-7-115-16966-2/TP

定价：25.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223

21世纪高等院校信息安全系列规划教材

编　委　会

总　序

一、出版背景

随着计算机技术与网络通信技术在政府、国防、金融、公安和商业等部门的广泛应用，社会对计算机的依赖越来越大，而计算机系统的安全一旦受到破坏，不仅会导致严重的社会问题，也会带来巨大的经济损失。因此，确保计算机系统的安全已成为世人关注的社会问题，信息安全已成为信息科学的热点课题，信息安全专业也受到了社会各界的普遍关注。

我国信息安全本科专业设置始于2000年，当年教育部首次批准开办信息安全专业。从此以后，每年都有不少高校加入开办信息安全本科专业的行列。

我国政府对信息安全非常重视。2003年9月，中央《关于加强信息安全保障工作的意见》的27号文件，把信息安全工作提升到保护公众利益和维护国家安全以及保障与促进信息化发展的高度。2004年1月，国务院召开全国信息安全保障工作会议，特别强调要加强信息安全院系的建设和人才培养工作。信息安全学科专业与信息安全产业必将在中央27号文件精神的指引下得到健康、快速的发展。

目前，信息安全方面的人才还十分稀少，尤其是政府、国防、金融、公安和商业等部门对信息安全人才的需求很大。据有关部门的统计，现在国内从事信息安全工作的专业人才只有3 500人左右，并且大多分布在高校和研究院所，而按照信息化发展的状况，社会对信息安全专业的人才需求量达几十万人。要解决供需矛盾，必须加快信息安全人才的培养。人才的培养离不开教材的建设，信息安全专业急需与之教学相配套的教材。

根据教育部高教司函[2003]141号文件的精神，教育部高等学校电子信息与电气学科教学指导委员会专家组委托北京邮电大学等五所较早开办信息安全本科专业的高等院校完成了“信息安全专业规范”（以下简称“规范”）的制订。该规范已于2004年7月，在四川绵阳召开的“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”上公开发布。与会老师都对信息安全专业的发展、专业规范和课程设置展开了热烈的讨论。在会议上，我们征求了大家对信息安全本科专业教材建设的意见。在细致研究，反复讨论的基础上，规划了与规范相配套的《21世纪高等院校信息安全系列规划教材》。

二、教材特色

1．参照“信息安全专业规范”确定教材题目、组织教材书稿内容。

本系列教材的所有题目都是根据“信息安全专业规范”确定的。所有教材严格按照“规范”要求，结合信息安全专业的学制、培养规格、素质结构要求、能力结构要求、知识结构要求撰写，使其所含知识点完全覆盖“规范”中的要求，确保能够达到“规范”中的学习目标。

2．注重套书的整体策划。

由于本系列教材涉及的内容比较多，在选择教材内容时，一方面要考虑教材内容相互的

衔接，另一方面要考虑许多课程相互之间有内容交叉的现象。我们在一开始策划时就对这两个方面相当重视，多次召开编委会，审定教材的大纲，落实教材的主要知识点，避免了内容的重复。

3．特别注意学生工程实际动手能力的培养。

根据“信息安全专业规范”的要求，本系列教材适当减少理论知识和技术知识层次的学时和要求，增加了结合工程实际动手实践和专业应用技能层次的学时和要求。

4．系列教材的作者都是在我国信息安全领域具有丰富教学和实践经验的一流专家，部分教材已经被评为“普通高等教育‘十一五’国家级规划教材”（以下简称“国家十一五规划教材”）。

5．提供完善的教学服务。

为了方便教学，我们免费为选用本套教材的老师提供以下教学服务。

（1）所有教材的电子教案。

（2）与部分教材配套的习题答案。

（3）信息安全专业本科教学实验室建设方案与实验教学指导咨询（联系单位：“北京邮电大学信息安全中心”。联系方式：100876，北京西土城路 10 号北京邮电大学 126 信箱，yxyang@bupt.edu.cn）。

（4）信息安全专业本科生实习、实训与技能认证咨询（联系单位：“北京邮电大学信息安全中心”、“四川绵阳灵创科技园”。联系方式：621000，绵阳市科创园区九州大道中段灵创科技园内灵创科技有限公司，0816-6336559（传真）、6336520，yxyang@bupt.edu.cn）。

本系列教材尽管经过反复讨论修改，但限于作者水平和其他条件限制，难免存在不足和值得商榷之处，敬请批评指正。

21 世纪高等院校信息安全系列规划教材编委会

2007 年 1 月

前　言

信息安全是国家安全的基础和关键。随着信息安全理论与技术的发展，信息安全保障的概念得以提出并得到一致认可。在信息安全保障的三大要素（人员、技术、管理）中，管理要素的地位和作用越来越受到重视。从信息安全管理体系的高度来全面构建和规范信息安全管理，将有效地保障我国的信息安全。

信息安全管理是一个新的和十分重要的课题，其发展对信息安全人才的培养提出了新的需求。解放军信息工程大学电子技术学院是最早从事信息安全领域研究和教学的军事院校，在信息安全学科专业领域，拥有一支学术水平高的专家队伍；承担了信息安全技术和信息安全管理领域大量科研课题，取得了一系列科研成果；荣获了国家科技进步一等奖等多项奖励；能够从事本科至博士研究生的多层次人才培养。为了适应当前信息安全人才培养的需要，更好地培养综合素质高和能力强的信息安全人才，我们组织在信息安全方面有多年教学与科研经验的人员，编写了这本《信息安全管理》。

本书以构建信息安全管理体系为框架，全面介绍了信息安全管理的基本概念、信息安全管理体系以及信息安全管理的各项内容和任务，内容涵盖了信息安全管理的基本内涵、信息安全管理体系的建立与实施、信息安全风险管理、组织与人员安全管理、环境与实体安全管理、系统开发安全管理、运行与操作安全管理以及应急响应处置管理等。

本书特点主要体现在下列几个方面。

1．系统性。信息安全管理作为信息安全保障的重要组成部分，涉及信息安全系统建设的各个方面。本书注重内容的系统性，以 ISO/IEC17799 为框架，综合基于 SSE-CMM 和等级保护的信息安全管理体系，系统介绍了信息安全管理的各项内容和任务。

2．新颖性。为适应信息安全管理理论发展迅速、知识更新快的特点，本书紧跟学科发展前沿，及时将信息安全管理领域的新知识、新信息（如等级保护、信息系统运行监控等内容）带入知识体系。同时，本书突破管理仅是行政管理或风险评估管理这一认识误区，从技术层面对信息安全管理进行介绍，包括风险评估技术、监控管理技术、软件测试技术、应急响应与灾难恢复技术等，对信息安全管理体系进行了扩充和完善。

3．逻辑性。本书注重内容结构的逻辑性，以构建信息安全管理体系为框架，以管理为核心要素，由信息安全管理基本概念和信息安全管理体系引入，围绕信息安全管理体系的建立和实施步骤逐步展开，最后对典型信息安全管理实例进行分析。本书由浅入深、层次分明，有利于读者消化和吸收信息安全管理相关知识。

4．实用性。信息安全管理体系的构建是一个包含规划、实施与建设、认证等多个步骤的过程。在这个过程中，涉及大量管理和技术性工作，而不同的组织和单位根据自身环境，可以进行不同的选择。本书注重知识的实用性，将理论与实际相结合，选取典型信息安全管理

实施案例进行分析，充分阐释了信息安全管理的实施过程，帮助读者运用所掌握的知识分析和解决实际问题。

本书由解放军信息工程大学电子技术学院信息安全技术教研室组织编写。其中第 1、6 章由张红旗教授编写，第 2、3、7 章的大部分内容和第 4、5 章由王新昌编写，第 7 章安全策略和操作管理部分、第 8 章及第 2 章等级保护部分由杨英杰编写，第 9 章及第 3 章风险充其量常用方法部分由唐慧林编写，全书由张红旗和王新昌负责统稿。在本书编写过程中，电子技术学院副院长陈性元教授、信息安全系张永福教授给予了大力支持和指导，信息安全技术教研室张斌、杜学绘、王鲁、杨艳、杨智、包义保、汪永伟和代向东等同志参加了编写本书的相关工作。本书编写过程中还参考了大量相关文献，无法一一列举，在此一并向作者表示衷心的感谢。

信息安全学科内容广泛，发展迅速，信息安全管理及相关内容也在不断更新。由于作者水平有限，书中难免存在不足和错误之处，敬请读者批评指正。

作　者

2007 年 9 月

目　录

▶▶▶ 第 1 章

信息安全管理概述

人类正进入信息化社会，社会发展对信息资源的依赖程度越来越高，从人们的日常生活、组织运作和国家管理来看，信息资源都是不可或缺的重要资源，没有各种信息的支持，现代社会将无法存在和发展。而由于环境的开放和信息系统自身的缺陷，信息资源面临着来自内部和外部两个方面的威胁。随着信息技术和信息安全的发展，人们不断意识到，必须从技术、管理等不同的方面采取措施，保证信息系统和信息资源的安全。

本章介绍信息安全管理的产生背景、信息安全管理的内涵、国内外信息安全管理现状以及信息安全管理相关标准。

本章重点：信息安全管理的内涵，信息安全管理相关标准。

本章难点：信息安全管理的内涵。

1.1 信息安全管理的产生背景

信息安全管理是随着信息和信息安全的发展而发展的。在信息社会中，一方面信息已经成为人类的重要资产，在政治、经济、军事、教育、科技、生活等方面发挥着重要作用，另一方面由于计算机技术的迅猛发展而带来的信息安全问题正变得日益突出。由于信息具有易传播、易扩散、易损毁的特点，信息资产比传统的实物资产更加脆弱，更容易受到损害，这样将使组织在业务运作过程中面临巨大的风险。这种风险主要来源于组织管理、信息系统、信息基础设施等方面的固有薄弱环节和漏洞，以及大量存在于组织内外的各种威胁，因此对信息系统需要加以严格管理和妥善保护，信息安全管理也随之产生。

1.1.1 信息与信息安全

1. 信息

信息可以理解为消息、情报、数据或知识，它可以以多种形式存在，可以是信息设施中存储与处理的数据、程序，可以是打印或书写出来的论文、电子邮件、设计图纸、业务方案，也可以是显示在胶片等载体或表达在会话中的消息。国际公认的 ISO/IEC IT 安全管理指南（GMITS）对信息（Information）给出如下解释：信息是通过施加于数据上的某些约定而赋予这些数据的特定含义。

一般意义上的信息是指事物运动的状态和方式，是事物的一种属性，在引入必要的约束条件后可以形成特定的概念体系。通常情况下，我们可以把信息理解为消息、信号、数据、情报和知识。

信息本身是无形的，借助于信息媒体以多种形式存在或传播。它可以存储在计算机、磁

带、纸张等介质中，也可以记忆在人的大脑里，还可以通过网络、打印机、传真机等方式进行传播。

对现代企业来说，信息也是一种资产，不仅包括与计算机、网络相关的数据、资料，还包括专利、标准、专有技术、商业档案、文件、图样、统计数据、配方、报价、规章制度、财务数据、工艺、计划、资源配置、管理体系、关键人员等。就如其他重要的商业资产那样，信息资产也具有重要的价值，因而同样需要进行妥善保护。

所有的组织都有各自处理信息的形式，例如，银行、保险和信用卡公司需要处理金融信息，企业、商家需要处理消费者信息，政府管理部门需要处理、存储公众和机密信息。无论这些信息采用什么样的处理、存储和共享方式，都需要对信息加以安全、妥善的保护，不仅要保证信息处理和传输过程是可靠、有效的，而且要求重要的敏感信息是机密的、完整的和真实的。为达到这样的目标，必须采取一系列适当的信息安全控制措施使信息避免一系列威胁，保障业务的持续性，最大限度地降低安全威胁的影响，减少业务和系统的损失。

需要注意的是，从安全保护的角度去考察信息资产，并不能只停留在静态的一个点或者一个层面上。信息是有生命周期的，从其创建或诞生，到被使用或操作，到存储，再到被传递，直至其生命周期结束而被销毁或丢弃，各个环节、各个阶段都应该被考虑到。安全保护应该兼顾信息存在的各种状态，不能有所遗漏。

2. 信息安全

信息安全是一个广泛而抽象的概念，不同领域不同方面对其概念的阐述都会有所不同。建立在网络基础之上的现代信息系统，其安全定义较为明确，那就是：保护信息系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄漏，保证信息系统能够连续、可靠、正常地运行。在商业和经济领域，信息安全主要强调的是消减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降到最低。

信息作为一种资产，是企业或组织进行正常商务运作和管理不可或缺的资源。从最高层次来讲，信息安全关系到国家的安全；对组织机构来说，信息安全关系到正常运作和持续发展；就个人而言，信息安全关系到个人隐私和财产的安全。无论是个人、组织还是国家，保护关键的信息资产的安全性都是非常重要的。信息安全的任务，就是要采取措施（技术手段及有效管理）让这些信息资产免遭威胁，或者将威胁带来的后果降到最低，以此维护组织的正常运作。

随着人类文明的发展与进步，信息处理的方法与技术也在不断发展，从最原始的语言文谈，到古代文字、纸张的发明，到现代通信、计算机与网络技术的普遍应用，信息的储存、交流、传输、处理的技术与方法越来越多，越来越复杂，信息储存的媒体也随之增多。信息量正在呈几何级数增长，信息的传播容量不断增加、传播速度不断加快、信息资产所面临的安全威胁也在不断地增加，因而信息安全技术得到了相应的发展。当然在不同的发展时期，信息安全的侧重点与信息安全的控制方式与手段也不尽相同。

大致说来，信息安全在其发展过程中经历了三个阶段。

20 世纪 80、90 年代以前，面对信息交换过程中存在的安全问题，人们强调的主要是信息的保密性和完整性，对安全理论和技术的研究也只侧重于密码学。这一阶段可以称为通信保密（Communication Confidentiality）阶段。

20 世纪 80、90 年代，随着计算机和网络的广泛应用，人们对信息安全的关注已经逐渐

扩展为以保密性、完整性和可用性为目标，并利用密码、认证、访问控制、审计与监控等多种信息安全技术为信息和信息系统提供安全服务。这一阶段称为信息安全阶段（Information Security）。

20 世纪 90 年代中期以后，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题已经不仅仅是传统的保密性、完整性和可用性三个方面了。人们将信息主体和管理引入信息安全，由此衍生出了诸如可控性、抗抵赖性、真实性等安全原则和目标，信息安全也从单一的被动防护向全面而动态的防护、检测、响应和恢复等整体体系建设方向发展。这一阶段称为信息保障（Information Assurance）阶段。

在英国标准协会（British Standards Institution，BSI）的 BS7799 信息安全管理体系中，信息安全的主要目标是信息的机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）的保持。这也就是通常所说的 CIA，是指通过采用计算机软硬件技术、网络技术、密码技术等安全技术和各种组织管理措施，来保护信息在其生命周期内的产生、传输、交换、处理和存储的各个环节中，其机密性、完整性和可用性不被破坏。

（1）机密性（Confidentiality）

信息的机密性是指确保只有那些被授予特定权限的人才能够访问到信息。信息的机密性依据信息被允许访问对象的多少而不同，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息。根据信息的重要程度和保密要求可以将信息分为不同密级，例如军队内部文件一般分为秘密、机密和绝密三个等级。已授权用户根据所授予的操作权限可以对保密信息进行操作，有的用户只可以读取信息，有的用户既可以进行读操作又可以进行写操作。

（2）完整性（Integrity）

信息的完整性是指保证信息和处理方法的正确性和一致性。信息完整性一方面是指在信息使用、传输、存储信息的过程中不发生篡改、丢失、错误信息等；另一方面是指信息处理方法的正确性，执行不正当的操作有可能造成重要文件的丢失，甚至整个系统的瘫痪。

（3）可用性（Availability）

信息的可用性是指确保那些已被授权的用户在他们需要的时候，确实可以访问到所需信息。即信息及相关的信息资产在授权人需要的时候可以立即获得。例如，通信线路中断故障、网络的拥堵会造成信息在一段时间内不可用，影响正常的业务运营，这就是对信息可用性的破坏。

除了 CIA，当前信息安全的主要内容或目标还包括不可否认性（Non-Repudiation）、可控性（Controllability），其中不可否认性也可以定义为认证性（Authenticity）。

在某些文献资料中，认为信息安全的主要内容包括机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、真实性（Authenticity）和有效性（Utility）。

总的来说，凡是涉及机密性、完整性、可用性、可追溯性、真实性和可靠性保护等方面的技术和理论，都是信息安全所要研究的范畴，也是信息安全所要实现的目标。

1.1.2 信息安全管理的引入

综上所述，信息安全已扩展到了信息的可靠性、可用性、可控性、完整性及不可抵