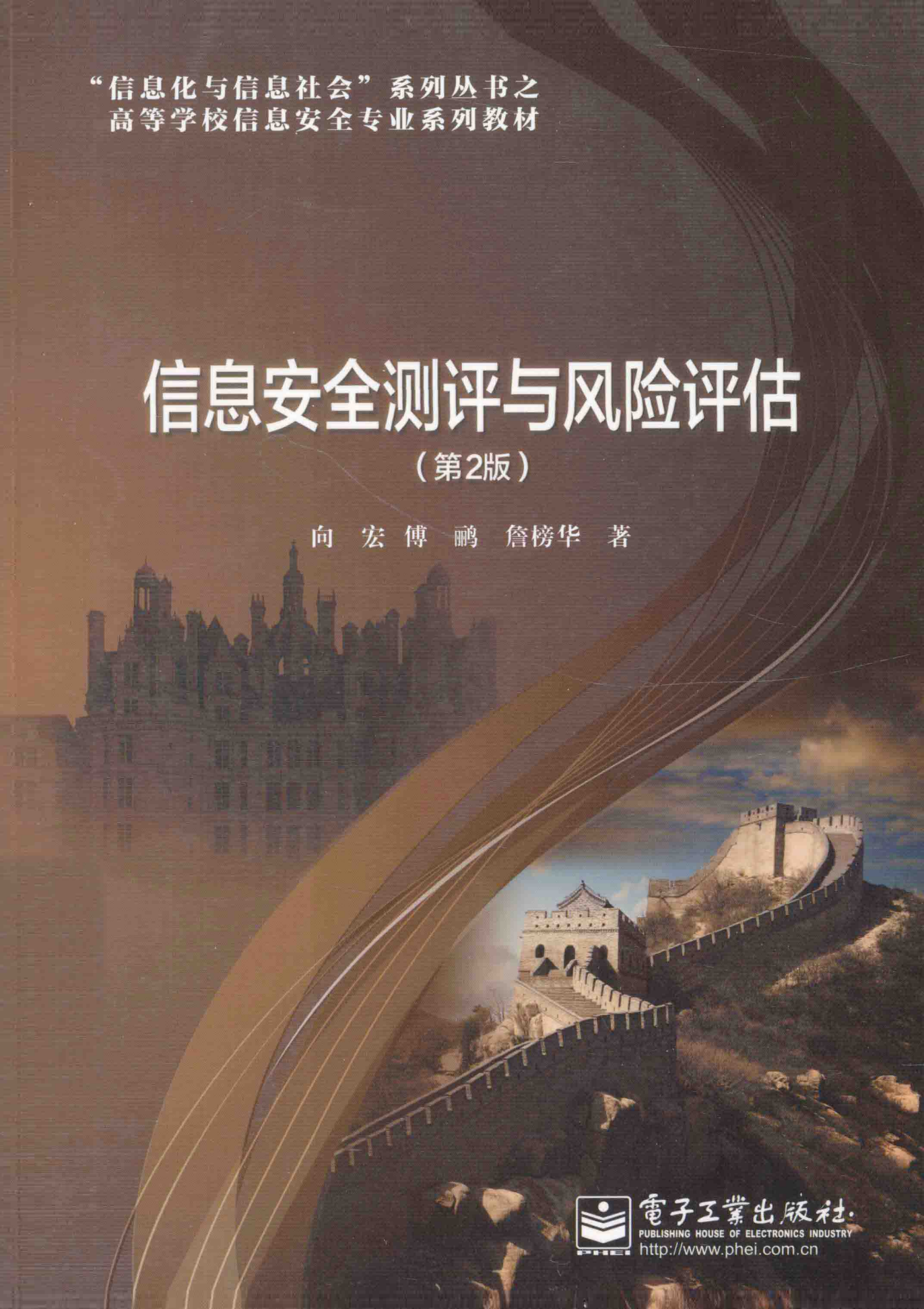
“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

信息安全测评与风险评估

（第2版）

向 宏 傅 鹂 詹榜华 著



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

“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

信息安全测评与风险评估

（第2版）

向 宏 傅 鹂 詹榜华 著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书分为四部分共 14 章。第 1 部分（第 1、2 章）介绍信息安全测评思想和方法；第 2 部分（第 3 章至第 6 章）介绍测评技术和流程；第 3 部分（第 7 章至第 13 章）介绍风险评估、应急响应、法律法规和信息安全管理体系；第 4 部分（第 14 章）介绍了国外在信息安全测评领域的最新进展。全书涉及的信息安全等级保护、风险评估、应急响应和信息安全管理体系等国家标准，均属于我国开展信息安全保障工作中所依据的核心标准集。

本书通过理论与实践紧密联系的方式，融会中外案例，生动向读者介绍如何依据国家有关标准进行信息系统的安全测评工作，通俗易懂，且引人入胜。

本书既适用于普通高等学校信息安全专业及相关专业的高年级本科生，也适用于从事信息安全测评工作或相关工作的读者。

图书在版编目（CIP）数据

信息安全测评与风险评估 / 向宏，傅鹏，詹榜华著. —2 版. —北京：电子工业出版社，2014.6
（信息化与信息社会系列丛书）
高等学校信息安全专业系列教材
ISBN 978-7-121-23163-6

Ⅰ. ①信… Ⅱ. ①向… ②傅… ③詹… Ⅲ. ①信息系统－安全技术－评价－高等学校－教材
②信息系统－安全技术－风险管理－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2014）第 092840 号

策划编辑：刘宪兰
责任编辑：徐蔷薇
文字编辑：刘宪兰
印　　刷：北京京师印务有限公司
装　　订：北京京师印务有限公司
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：24.75　字数：600 千字　黑插：1
版　　次：2014 年 6 月第 1 版
印　　次：2014 年 6 月第 1 次印刷
定　　价：49.50 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。

编委会名单 EDITORIAL COMMITTEE LIST

第2版“信息化与信息社会”系列丛书编委会名单

编委会主任 曲维枝

编委会副主任 周宏仁　张尧学　徐　愈

编委会委员 何德全　邬贺铨　高新民　高世辑　张复良　刘希俭
刘小英　李国杰　秦　海　赵泽良　杜　链　朱森第
方欣欣　陈国青　李一军　李　琪　冯登国

编委会秘书处 廖　瑾　刘宪兰　刘　博　等

第2版高等学校信息安全专业系列教材编委会名单

专业编委会顾问 （以汉字拼音为序）
蔡吉人　方滨兴　何德全　刘小英　宁家骏　曲成义
沈昌祥　邬贺铨　熊澄宇　赵泽良

专业编委会主任 冯登国

专业编委会委员 （以汉字拼音为序）
陈克非　封化民　韩　臻　胡爱群　黄继武　黄刘生
李　超　李建华　刘建伟　陆哲明　马建峰　秦玉海
秦志光　石文昌　王怀民　王清贤　王小云　向　宏
谢冬青　杨义先　俞能海　曾庆凯　张宏莉　张焕国
郑　东

作 者 简 介

向　宏，重庆大学教授、中国计算机学会高级会员、重庆大学“信息物理社会可信服务计算”教育部重点实验室主任、重庆市信息安全技术中心主任、全国大学生电子竞赛信息安全专家组成员。曾在海外学习、工作近 13 年。先后获得加拿大 Lakehead University 数学及计算机科学系硕士学位、University of Alberta 数学科学系博士学位。曾任职于著名国际 IT 企业并从事网络安全测评等工作多年。2002 年回国后承担了国家“863”计划信息安全专项等多项重要科研课题及国家重要信息系统的安全测评工作。

傅　鹂，重庆大学教授、重庆大学软件学院教授委员会主任、重庆市信息安全技术中心技术总监、重庆市电子学会副理事长，国家科学技术奖励评审专家、国家教育部科技发展中心项目评议专家、国家科技部创新基金管理中心专家组成员。主要从事信息安全语义技术、智能计算等领域研究，先后承担过国家攻关项目、国家自然科学基金项目、国家“863”计划等信息安全科研项目。

詹榜华，北京数字证书认证中心总经理，北京邮电大学兼职教授，国家信息安全保护等级专家评审委员会委员，国家信息安全风险评估专家组成员。主要从事信息安全理论研究、信息安全体系设计等工作，在国内外核心刊物发表多篇学术论文，主持和参与研究完成了“863”计划、自然科学基金等多个国家项目，参与了国家有关网络信任体系、电子政务安全、信息安全保障体系建设等多项政策、标准和规划的制定工作。曾荣获国家科技进步二等奖和军队科技进步一等奖。

第 2 版总序

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按照党中央、国务院领导同志的要求，就我国信息化发展中的前瞻性、全局性和战略性的问题进行了调查研究，提出了政策建议和咨询意见。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是国家信息化发展的一个紧迫需求，也是我国推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。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个重要举措，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。

考虑到当时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，结合高校专业课程设置情况，在“十一五”期间，先后组织出版了“信息管理与信息系统”、“电子商务”、“信息安全”三套本科专业高等学校系列教材，受到高校相关专业学科以及相关专业师生的热烈欢迎，并得到业内专家和教师的一致好评和高度评价。

但是，随着时间的推移和信息技术的快速发展，上述专业的教育面临着持续更新、不断完善的迫切要求，日新月异的技术发展及应用变迁也不断对新时期的建设和人才培养提出新要求。为此，“信息管理与信息系统”、“电子商务”、“信息安全”三个专业教育需以综合的视角和发展的眼光不断对自身进行调整和丰富，已出版的教材内容也需及时进行更新和调整，以满足需求。

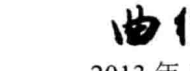
这次，高等学校“信息管理与信息系统”、“电子商务”、“信息安全”三套系列教材的修订是在涵盖第 1 版主题内容的基础上进行的更新和调整。我们希望在内容构成上，既要保持原第 1 版教材基础的经典内容，又要介绍主流的知识、方法和工具，以及最新的发展趋势，同时增加部分案例或实例，使每一本教材都有明确的定位，分别体现“信息管理与信息系统”、“电子商务”、“信息安全”三个专业领域的特征，并在结合我国信息化发展实际特点的同时，选择性地吸收国际上相关教材的成熟内容。

对于这次三套系列教材（以下简称系列教材）的修订，我们仍提出了基本要求，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，及时地把新技术、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。

为力争修订教材达到我们一贯秉承的精品要求，“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到各个专业编委会中，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。

我们衷心期望，系列教材的修订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，我们也借系列教材修订出版的机会，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、教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、政府官员以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，有待继续尝试和不断总结经验，也难免会出现这样那样的缺点和问题。我们衷心希望使用该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。



2013 年 11 月 1 日

第 1 版总序

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，我们愈发认识到，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个紧迫需求，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比较优势的关键。2006 年 5 月，我国《2006—2010 年国家信息化发展战略》公布，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、出版物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个重要举措，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、研究生和本科生）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”和“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，及时地把新技术、新趋势和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到各个专业编委会中，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、政府官员以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

第 2 版序言

“十一五”期间，由国家信息化专家咨询委员会牵头，教育部信息安全专业类教学指导委员会有关领导、学者组织，众多信息安全专业著名专家和教师参与开发，并由电子工业出版社出版的“高等学校信息安全专业系列教材”，由于在体系设计上较全面地覆盖了新时期信息安全专业教育的各个知识层面，包括宏观视角上对信息化大环境下信息安全相关知识的综合介绍，对信息安全应用发展前沿的深入剖析，以及对信息安全系统建设各项核心任务的系统讲解和对一些重要信息安全应用形式的讨论，在“高等学校信息安全专业系列教材”面世后，受到高校该专业学科及相关专业师生的热烈欢迎，得到业内专家和教师的好评和高度评价，被誉为该学科专业教材中的精品系列教材。

但是，随着信息技术的快速发展，信息安全专业教育面临着持续更新、不断完善的迫切要求，其日新月异的技术发展及应用变迁也不断对新时期信息安全建设和人才培养提出新的要求。为此，信息安全专业教育需以综合的视角和发展的眼光不断对教学内容进行调整和丰富，已出版的教材内容也需及时进行更新和修改，以满足需求。

这次修订，除对“高等学校信息安全专业系列教材”第 1 版各册教材的主题内容进行了相应更新和调整外，同时对系列教材的总体架构进行了调整并增加了 3 个分册，即《信息安全数学基础》、《信息安全实验教程》和《信息隐藏概论》。

调整后的教材在体系架构和内容构成上既保持了基础的经典内容，又介绍了主流的知识、方法和工具，以及最新发展趋势，同时增加了部分案例或实例。使得系列中的每一本教材都有明确的定位，充分体现了国家“信息安全”的领域特征，在结合我国信息安全实际特点的同时，还注重借鉴国际上相关教材中适于作为信息安全本科教育知识的成熟内容。

我们希望这套修订教材能够成为新形势下高等学校信息安全专业的精品教材，成为高等学校信息安全专业学生循序渐进了解和掌握专业知识不可或缺的教科书和知识读本，成为国家信息安全新环境下从业人员及管理者学习信息安全知识的有益参考书。

高等学校信息安全专业系列教材编委会

2013 年 10 月于北京

第 1 版序言

人类走过了农业社会、工业社会，如今正处于信息社会的伟大时代，“信息社会”这个词语无疑已经家喻户晓，信息化的大潮正席卷着世界的每一个角落。地球两端，万里之隔，人们能通过互联网与亲朋畅快交流，音容笑貌犹如就在眼前，真正是天涯变咫尺；分支机构遍布全球的庞大企业运转有条不紊，各机构协作顺畅，其功能强大的信息系统功勋卓著；分析复杂神秘的生物基因，预测瞬息万变的天气趋势，有了容量惊人的数据库系统和“聪明绝顶”的高性能计算系统，科学家们如虎添翼。总之，人类处处受益于信息化成果并正在信息化这条大道上加速前进，决不会放慢脚步。

然而，阳光之下总会有阴影，人类越依赖于信息系统，信息安全问题就越发凸显。关于信息安全的形形色色的新闻日益频繁地见诸于媒体：某银行数据库数据被窃取导致客户信息泄露，使客户惶惶不安，银行面临信任危机；某计算机病毒大肆泛滥，无数用户系统瘫痪，让相关企业损失惨重；某国军方网络被黑客侵入，军事机密竟被人如探囊取物般轻易窃取……这样的事件一再提示我们，信息安全问题是社会信息化发展进程中无法回避的客观产物，只有主动积极地面对和解决这一问题才能保障信息化的顺利推进，确保经济、社会的稳定乃至国家的安全。

目前，世界各国政府在信息安全领域的重视程度正在不断加大，并纷纷推出了本国的相关标准、规范或法律，大力扶持高校和其他科研机构对信息安全问题的研究，同时采取各种措施促进信息安全领域的人才培养以满足本国信息化建设的需要，为本国的信息产业发展提供中坚力量。特别是一些信息化进程起步较早，水平较高的发达国家，其信息安全领域的研究水平和产业化程度已相当令人瞩目。

我国正处于信息化建设的关键阶段，2006 年发布的《2006—2010 年国家信息化发展战略》更是从战略的高度指出了推进信息化对我国经济建设和国家发展的重要作用，规划出了新时期我国信息化发展的宏伟蓝图。由此可见，我国的信息化建设和信息产业正面临前所未有的机遇和挑战。

正是在这样的时代背景下，信息安全问题越来越引起全社会上下的广泛关注。信息安全领域必须不断提高研究水平以满足经济建设和国家安全的需要，为我国信息化建设的大踏步前进保驾护航，为创建和谐社会，实现可持续发展贡献力量。因此，大量高素质的信息安全人才成为了最急需、最宝贵的资源。

康有为曾经说过：“欲任天下之事，开中国之新世界，莫亟于教育。”我们的国家要想不断发展科技，增强国力，开创出我们自己富强文明的“新世界”，必须加大力度进行

信息化建设。而要使我国的信息化水平走在世界前列，全面提高信息安全领域教育水平，特别是促进高等学校信息安全专业对相关人才的培养和教育，就成为了成败的关键。高等学校信息安全系列教材的编撰就是希望能够为我国的信息安全领域专业人才的培养、为我国信息化水平的腾飞助一臂之力。

信息安全专业教育有其自身的特点，要求学习该专业的学生能够将系统知识与专业知识有机结合，在注重提升理论高度的同时还要能够把理论知识与工程实践紧密联系起来。本系列教材针对高等学校信息安全专业教育的这些特点，同时根据其知识体系、教育层次和课程设置，规划了教材的内容，增加了实际案例，力争做到既紧跟前沿技术的发展，又不失扎实的基本理论和生动活泼的形式，使学生能够学以致用。本系列教材从不同角度论述和总结了信息安全领域的科学问题，有着较强的适用性，既可作为高等学校信息安全专业和相关专业本科生的教材，也可以作为非信息安全专业的公共教科书，同时还可以作为从事信息安全工作的科研技术人员和管理人员的培训教材或参考书，使其了解信息安全相关关键技术和发展态势。

信息安全科学在不断发展，我们也将会努力使本系列教材适应和紧跟这种发展的节奏，使我们培养的信息安全人才能够与时俱进，用自己的所学共筑我国信息安全的万里长城。

限于作者的水平，本系列教材难免存在不足之处，敬请读者批评指正。

高等学校信息安全专业系列教材编委会

2008 年 10 月

第 2 版前言

自本教材 2009 年出版以来，世人都能感受到在网络信息空间中所发生的巨大变化。从云计算、物联网、移动互联网到大数据等，真是“你方唱罢我登场”，甚至是“众多演员齐声合唱”，让人目不暇接。而在信息安全领域，过去 5 年来所出现的重大事件甚至成为了世界各国普通民众关注的热点话题：从“伊朗核电站遭受网络武器的攻击”、美国网络战司令部的成立、美国政府发表的“网络空间国际战略”、“斯诺登事件”的曝光，以及我国最新成立的网络安全与信息化领导小组……所有这一切无不昭示着未来网络安全领域的发展将更具挑战性、基础性和全局性。

那么，作为网络信息安全的一个分支，信息安全测评与风险评估在这几年当中又有哪些新的变化呢？在这些新的变化当中又蕴含着哪些新的规律呢？我们结合自身所从事的科研工作，在众多的素材中筛选了两个“自认为”最典型又最具有现实意义的课题，一个涉及国家基础设施——工业控制系统的信息安全及风险评估，另一个涉及国外最新的网络靶场建设及新颖的测评技术，来向读者展示这一领域新的发展趋势。感兴趣的读者可以在第 14 章了解相关的细节。

除了上述新增的技术部分内容外，在这新版教材中我们更想强调的是，尽管信息安全及相关的测评技术正在发生新的变革，甚至会远远超出我们的想象，但正如本书第 1 章所阐述的那样，我们始终认为探寻其中一般性的科学规律是一个科学工作者“万变不离其宗”的使命。这就要求我们要秉承人类共同的科学精神财富，不断深化近代文艺复兴运动以来的科学思想，并坚信这远比掌握一门具体的测评技巧更为重要。但是，我们也要清醒的看到，中国传统文化中有一些根本性的指导思想与现代科学鼓励创新、勇于探索的本真要求存在着一些冲突和矛盾。如何对我国的传统文化扬长避短、推陈出新，是我们这一代人应不断思考的问题。为此，在本书第 14 章的开头部分，我们特意选择了儒家文化的经典之一——《中庸》，以及 20 世纪 80 年代我国改革开放之初思想解放运动中的代表作之一——《让科学的光芒照亮自己》，供读者独立思考并得出自己的结论，这也算是我们这几位 60 后作者与读者的心灵沟通吧。

本书在第 2 版的撰写过程中，得到了重庆大学软件学院信息安全实验室胡兵、王磊、张亚妮、何湘、黄翠、韩燕南等年轻人的积极协助，以及重庆大学“信息物理社会可信服务计算”教育部重点实验室、重庆大学信息安全国际战略研究所、国家保密科技测评中心重庆市分中心的帮助，在此一并表示感谢。同时也感谢该系列教材编委会主任冯登国等专家和电子工业出版社刘宪兰老师给予我们的鞭策和鼓励。

作者

2014 年春

于重庆大学民主湖畔

第 1 版前言

“读万卷书，行万里路”是古人对理论联系实际的最好诠释。面对虚拟空间中纷纷建立起来的形态各异的信息大厦，为了保证它们的建筑质量，世界各国标准化组织均出台了众多的安全标准。这就是本书撰写之前所面临的“万卷书”。如何在信息系统的设计、施工、验收和运行等阶段进行安全检查，就是本书希望做到的在虚拟空间“行万里路”。

作为国内高校信息安全专业本科教材，我们将本书定位为“在国家有关标准的指导下进行信息安全工程作业的参考手册”，并希望以此弥补高校教材在这方面的不足。

在撰写本书的时候，我们首先想到的就是“实用性”。考虑到本书的读者群主要是全日制普通高校信息安全专业的高年级本科生，即将面临社会对他们从事信息安全工作的能力和水平的检验。因此，为了满足我国目前正在开展的信息安全保障工作对测评人员的急迫需求，我们在国家已经颁布实施的众多安全标准中，筛选了“信息安全等级保护”和“信息安全风险评估”这两大类标准作为本书的知识主体，同时也参考了部分已经制定完成但仍处于报批阶段的国家标准，如“应急响应”、“信息安全管理体系”等，以使得本书的知识具有一定的前瞻性。

如果仅仅是介绍国家有关信息安全等级保护、风险评估或应急响应等方面的标准，读者可能会感到比较枯燥或难于理解，而且无从下手进行测评。因此本书大量的篇幅被用来进行案例教学。我们设计了三个具有典型意义的大型模拟案例，逐条指导读者去理解、执行这些标准。这三个模拟案例的设计目的分别是：“天网”（电子政务）系统主要针对信息安全等级保护的测评；“数字兰曦”（企业信息化）主要针对信息安全的风险评估；“南洋烽火”（校园信息系统）主要针对信息安全应急响应计划的制定和演练。

本书的第二个特点是科学性。作为自然科学和社会科学的交叉学科分支，信息安全测评与风险评估有其自身的特殊规律。为了探索这个规律，我们希望读者在进入这个领域之初就应当具备实事求是的科学态度。因此本书的第 1、2 章“信息安全测评思想”和“信息安全测评方法”是本书作者希望与读者交流的最重要的心里话。

本书的第三个特点是规范性。作为一名信息安全测评工程师，在工作中的主要依据就是有关国家标准。因此本书对第 2 部分（第 3 至第 6 章）从事信息安全等级保护测评、第 3 部分从事信息安全风险评估（第 7 至第 10 章）、应急响应（第 11 章）和信息安全管理体系（第 13 章）等工作所遵循的相关标准进行了尽量详细的阐述和解释。

我们向读者特别指出的是，本书所强调的“安全测评是科学与艺术的完美结合”这个观点，并最终体现在“安全测评”、“风险评估”和“应急响应”等技术的融合上，形

成“信息安全管理体系”。这也是作者将“信息安全管理体系”相关知识的介绍安排在最后一章的良苦用心。此外，考虑到国家标准对相关法律、法规的密切联系，我们在第 12 章专门介绍了国外有代表性的法律、法规以及我国与本书内容相关的法律、法规情况。

本书的第四个特点是（尽量）做到趣味性。“知之者不如好知者，好知者不如乐知者”。我们希望本书中所采用的“典故”、“争鸣”、“工具”等小模块能够启发读者的创新思维。同时，我们在全书体例上也采用了格言、序幕、要点、正文、尾声、观感的风格，希望给读者营造一种欣赏戏剧或交响乐般的氛围，从而体会信息安全测评工作的艺术性。为了方便读者阅读，本书设计了一些象形符号：

“三星堆面具”图案代表与正文相关的某个典故或背景故事。

“斗士”图案代表一些值得商榷的观点或看法，鼓励讨论。

“榔头”图案代表用于测评/评估工作时的小工具，谨供读者参考。

“逍遥椅”图案代表我们认为值得读者重视的一些观点或工程经验。

“笔记”图案代表重要的概念或定义。

本书包含了大量的实验案例。我们在进行实验设计的时候，已经充分考虑到本书读者的实验条件和动手练习的可能性，因此我们强烈建议阅读本书的读者在可能的情况下“重现”（reproduce）书中案例分析的实验，这是学习测评技术和方法的最好途径。在此基础上，我们在每一章结束后都以“观感”的形式给出一些补充练习，供读者思考。此外，我们也希望读者能够不受本书实验方案设计思路的束缚，举一反三，创新出更好、更贴切的实验方案。我们也真诚地欢迎读者指出本书可能存在的谬误之处（联系地址：xianghong@cqu.edu.cn）。

本书的三位作者分别来自高校和国内知名安全企业。我们希望能够用这种方式来真正体现我国高等教育“产、学、研”的结合。在本书的编写过程中得到了重庆大学有关师生、重庆市信息安全技术中心和北京数字证书有限责任公司员工的大力支持。作者们愿借此机会向他们表示衷心的感谢，没有他们的鼎力支持和批评指正，我们是不可能完成这个艰巨的任务的。

我们要特别感谢重庆大学吴中福教授在本书整体框架确定方面给予的指导并与我们分享他数十年的育才经验。重庆大学胡海波、方蔚涛、蔡斌、桑军、叶春晓、夏晓峰等骨干教师则承担了本书大量的正文撰写和实验指导等工作。

感谢重庆市信息安全技术中心何湘、张亚妮、胡兵、王磊、黄翠等同仁以及重庆大学软件学院 2005、2006、2007 级研究生在从事相关测评实验及本书校稿过程中做的大量工作；感谢北京数字证书有限责任公司安全事业部翟建军等同行提供众多素材并开展休闲式的讨论，作者从中受益匪浅。

本书在撰写过程中先后多次聆听了“信息化与信息社会”系列教材编委会委员赵择

良、高等学校“信息安全”专业系列教材编委会顾问沈昌祥院士、高等学校“信息安全”专业系列教材编委会主任冯登国等专家的建议和指导并从中获益匪浅。感谢教材编委会给我们提供了向本领域许多专家如邬贺铨、周宏仁、高世辑、赵小凡、陈国青、徐愈、刘希俭请教的机会。此外，陈晓桦等专家也对本书的初稿提出了诸多有益的建议；重庆市公安局公共网络监察总队白志、重庆市信息安全产品测评中心廖斌、重庆市国家保密局王晓亚等领域专家对本书架构的酝酿及对国家标准的理解等方面也提供了诸多灵感。在此作者也一并表示感谢，并对由于作者能力有限而未能充分体现上述各位专家的建议或批评表示歉意。希望今后有机会能够进一步弥补本书的种种不足之处。

最后作者要感谢电子工业出版社的刘宪兰等老师在本书成稿过程中给予的各种支持、鼓励和花费的大量心血及三位作者的家人在我们挑灯夜战的时候给予我们的理解和支持。

作者

2008 年 9 月

于重庆大学民主湖畔