信息系统风险管理

清华大学出版社

信息系统风险管理

清华大学出版社
北京

内容简介

本书首先介绍了信息系统的相关概念及体系结构，以信息系统风险管理与控制的相关理论作为基础，分析了信息系统的风险及其分布，从信息系统的项目建设过程以及信息系统资源使用过程等方面，对信息系统的风险管理与控制进行了深入的研究。最后结合一个电子政务案例，讨论了信息系统风险管理与控制的具体应用。

本书结构合理，层次清晰，所涵盖的信息系统内容体系完整。本书既可作为信息安全、计算机科学与技术、电子商务、管理科学工程、信息系统与管理、会计(审计)学等专业高年级本科生和研究生教学以及信息化工程技术人员的培训教材，也可作为信息安全公司、IT 安全咨询顾问、企事业单位高管以及信息管理中心、信息系统审计师以及信息系统工程监理等方面人士的参考用书。

图书在版编目(CIP)数据

信息系统风险管理/卢加元著. —北京：清华大学出版社，2011.1
(21 世纪高等学校规划教材·信息管理与信息系统)
ISBN 978-7-302-22620-8

Ⅰ. ①信…　Ⅱ. ①卢…　Ⅲ. ①信息系统—风险管理　Ⅳ. ①G202

中国版本图书馆 CIP 数据核字(2010)第 081864 号

责任编辑：魏江江　薛　阳
责任校对：李建庄
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：17　**字　数**：421 千字
版　　次：2011 年 1 月第 1 版　　**印　　次**：2011 年 1 月第1 次印刷
印　　数：1～3000
定　　价：29.00 元

产品编号：036791-01

编审委员会成员

（按地区排序）

清华大学	周立柱　教授
	覃　征　教授
	王建民　教授
	冯建华　教授
	刘　强　副教授
北京大学	杨冬青　教授
	陈　钟　教授
	陈立军　副教授
北京航空航天大学	马殿富　教授
	吴超英　副教授
	姚淑珍　教授
中国人民大学	王　珊　教授
	孟小峰　教授
	陈　红　教授
北京师范大学	周明全　教授
北京交通大学	阮秋琦　教授
	赵　宏　教授
北京信息工程学院	孟庆昌　教授
北京科技大学	杨炳儒　教授
石油大学	陈　明　教授
天津大学	艾德才　教授
复旦大学	吴立德　教授
	吴百锋　教授
	杨卫东　副教授
同济大学	苗夺谦　教授
	徐　安　教授
华东理工大学	邵志清　教授
华东师范大学	杨宗源　教授
	应吉康　教授
上海大学	陆　铭　副教授
东华大学	乐嘉锦　教授
	孙　莉　副教授

浙江大学	吴朝晖 教授
	李善平 教授
扬州大学	李 云 教授
南京大学	骆 斌 教授
	黄 强 副教授
南京航空航天大学	黄志球 教授
	秦小麟 教授
南京理工大学	张功萱 教授
南京邮电学院	朱秀昌 教授
苏州大学	王宜怀 教授
	陈建明 副教授
江苏大学	鲍可进 教授
武汉大学	何炎祥 教授
华中科技大学	刘乐善 教授
中南财经政法大学	刘腾红 教授
华中师范大学	叶俊民 教授
	郑世珏 教授
	陈 利 教授
江汉大学	颜 彬 教授
国防科技大学	赵克佳 教授
中南大学	刘卫国 教授
湖南大学	林亚平 教授
	邹北骥 教授
西安交通大学	沈钧毅 教授
	齐 勇 教授
长安大学	巨永峰 教授
哈尔滨工业大学	郭茂祖 教授
吉林大学	徐一平 教授
	毕 强 教授
山东大学	孟祥旭 教授
	郝兴伟 教授
中山大学	潘小轰 教授
厦门大学	冯少荣 教授
仰恩大学	张思民 教授
云南大学	刘惟一 教授
电子科技大学	刘乃琦 教授
	罗 蕾 教授
成都理工大学	蔡 淮 教授
	于 春 讲师
西南交通大学	曾华燊 教授

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程（简称‘质量工程’）”，通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体

系有较高的科学创新、技术创新和理念创新的含量)、先进性(对原有的学科体系有实质性的改革和发展,顺应并符合21世纪教学发展的规律,代表并引领课程发展的趋势和方向)、示范性(教材所体现的课程体系具有较广泛的辐射性和示范性)和一定的前瞻性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括:

(1) 21世纪高等学校规划教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 21世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21世纪高等学校规划教材·信息管理与信息系统。

(6) 21世纪高等学校规划教材·财经管理与计算机应用。

(7) 21世纪高等学校规划教材·电子商务。

清华大学出版社经过二十多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

联系人:魏江江

E-mail:weijj@tup.tsinghua.edu.cn

前言

随着国民经济和社会信息化进程的加快，信息系统的基础性和全局性作用日益增强，国民经济和社会发展对信息系统的依赖性也越来越大。与此同时，各类计算机犯罪及黑客攻击信息系统的事件屡有发生，其手段也越来越隐蔽和高科技化。信息系统安全正成为一个事关国家政治稳定、社会安定和经济有序运行的全局性问题。

与国外发达国家相比，我国信息化的应用以及对信息系统安全的防护能力还处于发展的初级阶段。江民科技公司在2006年12月发布了针对网上银行的病毒调查报告，报告显示，从2004年8月到2006年10月期间，我国感染各类网银木马及其变种的用户数量增长了600倍，用户每月感染病毒及其变种的数量约有160种左右，而且病毒发展正在呈加速上升趋势。2009年7月，中国互联网络信息中心对电子商务、网络支付等交易类应用中的网络信息安全进行了调查，发布的报告指出，半年内有1.95亿网民上网时遇到过病毒和木马的攻击，1.1亿网民遇到过账号或密码被盗的问题，仅有29.2%的网民认为网上交易是安全的。正是由于网络安全存在大量的隐患和许多行业和组织对安全防范的不到位，从而使网民对互联网的信任度下降，进而制约了国内电子商务等交易类应用的发展。可见，信息系统安全已经成为人们普遍关心的话题，如果对此再不加以重视，将会给国家和企业造成重大的危害。

面对日益增长的信息系统安全需求，《国家信息化领导小组关于加强信息安全工作的意见》(中办发[2003]27号)明确提出了实行信息安全等级保护，重视信息安全风险工作的要求，使等级保护成为我国信息安全领域的一项基本政策；2005年2月至2005年9月，国信办下发通知《信息安全试点工作方案》，并分别在银行、税务、电力等重要信息系统以及北京市、上海市、黑龙江省、云南省等地方的电子政务系统开展了信息安全风险评估试点工作；2005年12月，公安部《信息系统安全等级保护实施指南》、《信息系统安全等级保护定级要求》、《信息系统安全等级保护基本要求》等文件陆续出台；2006年3月开始实施的公安部、国家保密局、国家密码管理局、国信办等四部委(局办)发布7号文《等级保护管理办法》。这些法规的颁布和实施，充分说明开展信息系统风险的评估、管理与控制等方面的研究不仅必要，而且具有重大的现实意义。

本书正是以此为背景，在信息化建设与应用中引入风险管理与控制机制，对信息系统进行全面、有效的风险分析与评估，并采取适当的风险管理与控制措施，旨在为我国各行业和组织信息安全策略的确定、信息系统的建立及安全运行提供依据，为电子商务、电子政务等各类应用的健康发展提供指导。

当前，国内对信息系统风险管理的研究还处于引进和消化吸收阶段。本书结合作者近年来从事的信息安全实务以及教学和科研工作，针对当前信息系统风险管理研究中存在的一些不足，从系统工程角度，对信息系统的体系结构、信息系统安全领域各环节的风

险以及构成要素、风险管理过程、风险评估及其评估方法、风险管理与控制的具体应用等进行了比较全面系统的研究，希望能弥补当前同类文献所存在的不足，尤其是理论与实践脱节、研究内容过于理论化等方面的问题，从而为国内信息安全的实践提供帮助。

本书既可作为信息安全、计算机科学与技术、电子商务、管理科学工程、信息系统与管理、会计(审计)学等专业高年级本科生和研究生教学以及信息化工程技术人员培训的教材，也可作为信息安全公司、IT 安全咨询顾问、企事业单位高管以及信息管理中心、信息系统审计师以及信息系统工程监理等方面人士的参考用书。

在本书编写过程中，得到了南京审计学院领导的关心和支持，江苏省审计信息工程重点实验室副主任陈耿教授、南京审计学院信息科学学院副院长汪加才教授、王昕教授，以及许多教学一线的老师提出了许多宝贵意见。作者在写作过程中参考了大量的国内外资料，在此，谨向书中提到和参考文献列出的所有作者表示衷心的感谢。本书的编写也得到清华大学出版社的大力支持，在此一并表示诚挚的谢意。

由于作者水平有限，书中疏漏与不足在所难免，恳请各位专家和读者批评指正。

编　者

2010 年 12 月于南京

目 录

第1章 信息系统概述

随着因特网技术的广泛应用，信息已成为维持社会正常运转的重要基础性资源，信息系统正广泛深入地应用到社会政治、经济、军事、文化等各个领域，整个社会对信息系统以及信息资源的依赖性也越来越高。

本章从信息和信息系统的概念入手，阐述信息系统的体系结构和软硬件构成，讨论信息系统的组织机构，最后总结几种常见的信息系统应用模式，为后续章节的内容做好铺垫。

1.1 信息和信息系统

1.1.1 信息的概念及特征

1. 信息的概念

信息是一种广泛的概念，它也是人们经常接触和频繁使用的词语。

“信息”一词来源于拉丁文 information，意思是指一种陈述或一种解释、理解等。随着人们对信息概念的深入认识，信息概念的含义也在不断地演变。现在“信息”一词已经成为一个含义非常深刻、内容相当丰富的概念，以至于很难给“信息”一词下一个确切的定义。

从信息的内涵来讲，信息的获得与“知道”这一概念有关。所谓“知道”，实质上就是人们获得了某种事物的相关信息。知道的过程实际上就是获得信息的过程。例如“科研处通知，明天下午有一个学术报告会”，“气象预报，近期内将有一场暴风雨”等，这些都是人们获得某种信息的过程。其次，信息在表现形式上，通常又指的是某种消息、指令、情报、密码、信号等。然而日常生活中将信息、信号、消息、情报等混为一谈的理解方式又是不确切的甚至是对信息的一种错误理解。虽然信息与消息、信号等有着密切的联系，并且信息常常以消息的形式表现出来，信息的传递又往往借助于信号，但是信息、消息、信号毕竟是 3 个不同的概念，三者之间存在着本质的区别。就信息与消息之间的关系来讲，信息指的是消息中蕴涵的事实和内容，消息应该代表的是信息的外壳。例如可以说“这条消息包含的内容非常丰富”，或者说“这则消息没有多少信息”，这实际上就从一定程度上说明了信息与消息之间的区别和联系。信息与信号也不能等同，因为同一种信息

可以用不同的信号方式来表达。例如遇到紧急情况，可以拉响警报器，用声信号来传递信息，当然也可以用点火的方式用光信号来传递信息。再如交通管理的红、绿灯，都采用的是光信号，但却是以不同的色彩来代表不同的含义（信息）。这些事实都表明，信息可以通过信号来传递，并且一种信号（如灯光）还可以传递多种信息。也就是说，信号实际上只是信息的载体，信息是信号所要表达的内容。

由于人们的认识不同，加上不同学科自身的特殊性和局限性，因此关于信息的定义目前有几十种之多，例如：

信息是人们在适应外部世界并且使这种适应反作用于外部世界的过程中同外部世界进行交换的内容的总称；

信息是物质和能量在空间中和时间中分布的不均匀程度，是伴随宇宙中一切过程发生的变化程度；

信息是用以消除随机不确定性的东西，是人与环境相互交换的内容的总称；

信息是物质属性的表征，是客观事物的本质反映，是自然和社会生命之源。

……

一般地，从质的方面讲，我们将信息定义为：信息是物质系统运动的本质表征，是物质系统运动的方式、运动的状态及运动的有序性。它的基本含义是：信息是客观存在的事实，是物质系统运动轨迹的真实反映。通俗地说，信息一般泛指包含消息、情报、指令、数据、图像、信号等形式之中的新的知识和内容，或者说，信息是指能够使信息的接收者通过信息的接收而获得一些有用的知识，认识客观事物存在的本质。

2. 信息的基本特征

一般地讲，信息具有以下三大基本特征。

1）事实性

事实性是信息的中心价值，代表了物质系统运动的客观存在性，表现的是物质系统运动的真实面貌和客观事实。不符合客观事物运动规律的信息不仅没有价值，而且会造成失误。

2）滞后性

任何客观事物的信息总是产生于此事物运动之后，没有事物运动的事实，就没有事物运动的信息。即先有事实，而后有信息。信息再快，也滞后于物质运动本身。

3）不完全性

物质系统的运动是永恒的、经常的、不断的，因此将产生出大量的信息。信息的不完全性指的是人们对客观物质系统的了解不可能包揽全部，一切都了如指掌。这是因为要完全了解物质系统是不可能的（因为它是要变化的），并且也没有这种必要。如果事无巨细都穷追其究，在时间上和精力上都是一种浪费，并且大量的信息资料也没有足够的空间去储存。信息的收集必有所取舍，只有正确地取舍，才可能正确地使用信息。

信息除具有以上三大基本特征之外，还具有以下几个一般特性。

1）信息具有知识性

信息是用于人们消除认识上的不确定性的东西，这也是信息的一个本质特征。如果人们对客观事物不了解，对其缺乏必要的知识，那么就对该事物不清楚，因而对事物的认识就具有不确定性。当人们获得了某种事物的有关信息后，其对此种事物的知识就会增加，对事物的认识也就由不清楚、不确定转向清楚和确定，即信息具有知识的秉性。人们只有借助事物发出的信息，才能获得有关事物的知识，消除对事物认识上的不确定性，改变原来对事物的不知或知之甚少的状态。

2）信息是一种资源并具有价值

由于信息具有知识的性质，所以它能够成为一种资源。事实上，信息已经成为现代社会生产和生活中一种重要的资源。社会的发展，经济的发展都需要各种信息的支持。一个国家乃至一个企业，如果闭关自守，信息阻塞，就会找不到发展的方向，失去发展的机遇，浪费人力、物力、财力，得不偿失；相反，如果信息灵通，掌握、收集信息及时，就会高瞻远瞩，左右逢源，抓住机遇。另一方面，信息在生产和科学技术的运用过程中，能转化为速度、效益或利润，即信息具有价值。

但信息的价值与一般商品的价值是不相同的。一般商品作为一种有形的物品，具有现实的使用价值，而信息是一种无形的商品，因此它的价值也具有一定的特殊性。首先，信息作为一种无形商品，只存在潜在的价值，而不存在现实的使用价值。信息的潜在价值只有通过人们去认识、去开发，才能转变为现实的价值。其次，信息的价值还取决于人们对它的认识和重视的程度，相同的信息会因认识和重视程度的不同而具有不同的价值。其三，信息的价值不完全取决于获取信息所付出的代价，而取决于信息本身的潜在价值及对信息的开发技术和开发能力。

3）信息具有无限性和压缩性

信息作为一种资源，具有无限性。信息的无限性首先表现在信息的可扩充性上。例如人们对太阳系的认识，对自然界的认识，包括对人类自身的认识等都在不断地加深扩充。信息的无限性还表现在信息的大量性和不断性上。只要人类存在，认识和改造客观世界的社会活动和经济活动就不会停止。在这些活动中，将会不断地产生出新的大量的信息。信息又具有可压缩性，以便于储存。最一般的压缩就是对信息进行加工、整理、概括、归纳、演绎，使之精练而取其精华。

4）信息具有时效性

信息的时效性指的是信息的效用与信息从发出到使用的时间间隔之间具有的相关关系。这种相关关系表明，时间间隔越短，时效性越强；信息传递的速度越快，时效性越强；信息使用越及时，利用程度越高，时效性越强。因此，为了加强信息的时效性，必须在信息的收集、处理、传递、输出、使用的各个环节上利用最先进的技术和操作工具。

信息的时效性代表着信息本身也具有生命周期。信息的生命周期是指信息从产生起到失去保留价值的时间间隔。正因为信息具有生命周期，才可能使人类世界能够容纳下“无限增长”的信息，同时也使人们认识到信息具有新陈代谢的机能，任何存储信息的系统其储存的信息资源需要不断地更新，人的知识也需要不断地更新等。