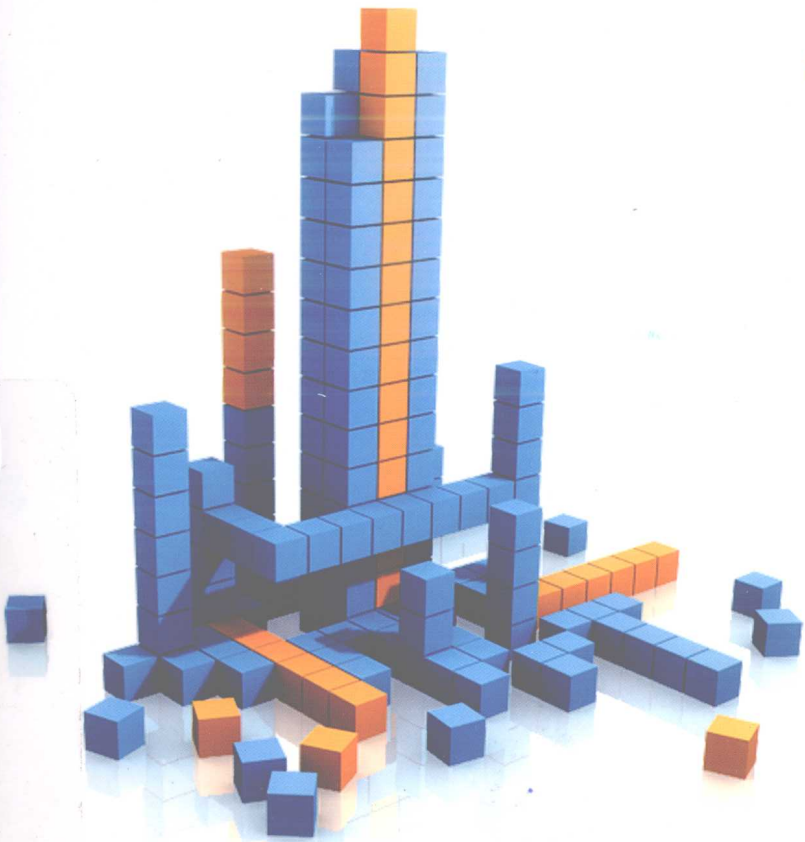
XINXI ANQUAN FENGXIAN
GUANLI FANGFA JI YINGYONG

信息安全风险管理方法及应用

吕俊杰 著



知识产权出版社

信息安全风险管理方法及应用

吕俊杰　著

知识产权出版社

内容提要

本书从信息安全风险管理体系建立的流程出发，研究了各阶段的工作内容及方法，并引入博弈论进行分析以对信息安全的管理提供决策依据，从而对企业的信息安全风险管理实践提供指导。

责任编辑：荆成恭

图书在版编目（CIP）数据

信息安全风险管理方法及应用/吕俊杰著. —北京：知识产权出版社，2010.6

ISBN 978-7-5130-0084-0

Ⅰ.①信… Ⅱ.①吕… Ⅲ.①信息系统—安全管理：风险管理 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2010）第 121504 号

信息安全风险管理方法及应用

Xinxi Anquan Fenaxian Guanli Fanafa Ji Yingyong

吕俊杰 著

出版发行：知识产权出版社

社　　址：北京市海淀区马甸南村1号　　**邮　　编**：100088

网　　址：http://www.ipph.cn　　**邮　　箱**：bjb@cnipr.com

发行电话：010-82000860 转 8101/8102　　**传　　真**：010-82005070/82000893

责编电话：010-82000860 转 8341　　**责编邮箱**：jcggxj219@163.com

印　　刷：北京富生印刷厂　　**经　　销**：新华书店及相关销售网点

开　　本：880mm×1230mm　1/32　　**印　　张**：6.25

版　　次：2010 年 6 月第 1 版　　**印　　次**：2010 年 6 月第 1 次印刷

字　　数：160 千字　　**定　　价**：24.00 元

ISBN 978-7-5130-0084-0/TP·297（3023）

前　言

信息化现在逐步进入人们的生活，融入到人类社会的每一个角落，并不断推动着社会的进步和发展。然而，无处不在的信息孕育着随时可发生的风险。伴随着社会经济对信息化依赖程度越来越高，各种恶意代码、黑客攻击、信息泄漏等安全事件时有发生，信息安全问题所导致的损失成倍增长。面对日益增长的安全需求，单靠技术手段是不可能从根本上解决信息安全问题的。绝大多数信息安全问题都是管理方面的缺陷，需要通过管理、技术、组织、物理等综合方法来解决信息安全问题。由此，信息安全风险管理应运而生。

在信息安全领域，风险管理就是最大范围地保护信息资产，确保信息的保密性、完整性和可用性，在可接受的成本范围之内，识别、控制和降低或排除（可能影响信息系统的）安全风险的流程。因此，掌握信息安全风险识别、风险评估和风险控制的方法，企业才能充分利用信息技术提供更便捷和更优质的产品或服务，同时又保障了信息的合理使用和安全。

目前学术界关于信息安全风险管理的研究，大多局限于某一个方面，鲜有对整个风险管理流程各阶段内容的研究。同时，与信息安全风险管理相关的国际标准，对方法的介绍比较泛泛，企业在应用过程中往往无所适从。因此，本书从信息安全风险管理的流程出发，研究各个阶段，即风险识别阶段、风险评估阶段和风险控制阶段的实施方法，并加以应用，对企业的具体实践提供理论指导，帮助企业建立合理的信息安全管理体系。

除此之外，将博弈论应用于信息安全风险管理之中也是本书的创新之一。本书探索性地将博弈论应用于企业的信息安全管理机制设计以及信息安全投资策略的研究，希望能起到抛砖引玉的作用。

摘　要

信息安全风险管理是信息安全的基础工作和核心任务之一，是最有效的一种管理措施，是保证信息安全投资回报率优化的科学方法。因此，对信息安全风险管理决策理论、方法及其应用进行系统的研究具有重要的学术价值和实践意义。

本书围绕信息安全风险管理理论，运用博弈论、（非）线性规划、模糊数学等数学工具，深入研究了企业信息安全风险管理决策模型及其应用，并结合某制造型企业的实际情况进行了实证研究。本书创新之处主要体现在以下几个方面。

1. 基于流程优化的信息安全风险识别方法

本书介绍了信息安全风险识别的内容和方法，并对目前常用的风险评估方法作了改进。在识别企业现有的信息流程后，利用多因素设计结构矩阵来描述信息的流向，并据此建立优化步骤，通过消除信息传递过程中的各种浪费，使信息流在系统中以最低的风险最大程度地满足各种需求。并通过对现有信息安全资产识别与评估模型的比较分析，本书在业务流程的基础上，进一步提出基于作业的资产识别方法，从而构建资产识别与评估的层次关系模型，即从流程到对应的各个作业再到各作业对应的各信息资产的递阶层次结构。该方法对系统信息流的适当、动态的管理可以有效地降低系统安全风险，在此基础上的风险评估和风险控制将会更加有效。同时，提出层次化的资产识别方法，使风险识别工作更加科学合理。

2. 基于语言评价的信息安全风险评估模型

根据信息安全风险数据难以获取、不确定性较多的特点，本书提供了一种基于模糊评价矩阵的信息安全风险群决策评估的方法。利用语言评价项与三角模糊数之间的对应关系，给出了集结不同专家个体意见的方法，以及三角模糊数风险矩阵理想解和负理想解的选取方法，对信息安全的威胁严重程度排序。

3. 基于 MP^2DR^2 风险控制矩阵的信息安全措施排序模型

MP^2DR^2 模型是典型的、公认的安全控制模型。在 MP^2DR^2 风险控制模型下，本书提出了对不同类型控制措施进行重要性排序的方法。通过建立威胁与控制措施间的对应关系，确立各种控制措施对每种威胁的有效性排序，并通过对不同资产类型的加权，确立不同类型控制措施对不同的资产、不同威胁的作用效果的综合评价，得到最优排序和控制措施的优先选择方案。

4. 信息安全风险管理机制设计

本书基于委托代理理论的基本思想以分布式拒绝服务（DDoS）攻击为例，依据委托代理理论，设计出了针对 DDoS 攻击的，以用户解题为基础的防御机制。首先描述出攻击者、用户和服务器三者间的交互关系，然后通过设计“题目”拍卖策略来决定投标的过程和题目的难度。这个防御机制可以对网络服务的可用性提供有力的保障，用户还可以根据推导出的可获得服务的条件来制定策略。

5. 多主体信息安全风险管理策略模型

本书根据企业间信息安全投资决策相互影响的特点，以病毒为例，考虑企业间病毒的相互传染性对联网企业的信息安全投资影响，构建了企业信息安全投资外部性的评价模型，并阐明了不同的企业进行风险决策的条件。

6. 信息安全风险管理的实证研究

利用本书提出的信息安全风险管理决策方法对某企业信息安全

风险管理进行了实证研究。利用已有的研究对信息安全风险进行了识别和分析，通过威胁和资产的权重的设计，以及威胁与控制措施间的对应关系，设计控制措施的评价表，通过对各类资产评价表的综合评价，最后得到控制措施的优先采用顺序，为企业的信息安全风险管理提供有力的保障。

关键词：信息安全 风险管理 风险评估 风险决策 模糊数

目 录

第一章　绪论

本章主要介绍本书的研究意义、信息安全风险管理的发展历史、研究概况以及主要的研究内容。

第一节　选题背景

20 世纪 90 年代以来，随着经济全球化和世界科技革命，信息技术、信息产业和信息网络蓬勃发展，社会信息化程度不断加深，信息对国家、组织和个人发展的影响日益增加、日益突出。对于国家而言，国民经济的发展和国家安全对信息和信息系统的依赖性越来越大。对于组织而言，信息、信息处理过程及对信息起支持作用的信息系统和信息网络逐步成为企业的重要资产。对于个人而言，信息更是无处不在，日常生活中计算机硬件软件已逐渐取代了传统的学习、生活、工作方式，为人们带来更多的快捷和方便。因此，国家、企业和个人对信息安全性要求也变得越来越高。与此同时，各种黑客利用系统安全弱点不断地开展新型攻击，网络攻击群体的规模迅速扩大，攻击水平迅速提高，攻击所造成的影响也愈发严重，信息系统所面临的安全风险和威胁日趋严重。

近些年来，由于恐怖分子、内部人员欺诈、黑客、病毒、自然灾害等事件，造成全球范围内信息安全事件损失不断攀升。2000 年 2 月 7 日美国网上 DDoS 攻击袭击八大重要网站引发恐怖事件造成 12 亿美元巨大损失，2001 年日本东京国际机场航管感染红色病

毒而失灵，几百架飞机无法起降、千人行程受阻。2003 年美国 Slammer 银行的 ATM 网遭入侵，造成几十亿美元损失。2005 年 Card System 公司由于被植入特洛伊木马，4000 万张卡用户信息被盗，是当时美国最大的窃密事件。2007 年年初，肆虐网络的熊猫烧香病毒给我国企业用户和个人用户带来了无法估量的损失。信息不仅威胁到网络世界的安全，甚至影响到物理社会的稳定。

在此环境下，各个国家都以极大的关注与投入维护信息安全，进而保障国家安全和社会稳定。世界各国尤其是发达国家纷纷颁布信息安全标准，对信息产品的研制、生产、销售和使用实行严格有效的控制，对信息系统运行和服务进行测试评估，对信息系统的管理进行评估和验证。党中央、国务院也高度重视信息安全问题，2003 年胡锦涛总书记发表讲话，要求“把信息安全放到至关重要的位置上，认真加以考虑和解决”。强调从国家安全、社会稳定、经济发展的高度去认识信息安全问题的极端重要性。国家信息化领导小组发布了《关于加强信息安全保障工作的意见》，提出了加强信息安全保障工作的总体要求和主要原则，以提高我国信息安全保障工作的能力和水平，维护公众利益和国家安全，促进信息化建设健康发展。然而，信息安全技术的研究仅仅是保障信息安全的基础，只有对信息安全管理方法的研究才是保障信息安全的关键。信息安全已不只是传统意义上的安全，即添加防火墙或路由器等简单的设备就可保证的，而是一种系统和全局的概念。国际公认的最有效的信息安全保障方法就是系统工程方法，管理与技术并重、积极预防和消极抵御相结合的方法。信息安全管理研究的重要性不言而喻，社会各界也掀起了有关信息安全风险管理国家政策和标准规范制定、信息安全风险管理理论和方法研究的热潮。

第二节 信息安全风险管理的发展历史

信息安全的发展经历了一个漫长的历史时期，最初产生于军事科学，主要集中于对信息安全技术、信息安全工具的研究，多侧重于密码学、身份认证、访问控制、防火墙、入侵检测等领域的研究。然而，绝大多数信息系统以及信息系统环境面临的安全威胁种类繁多，系统的薄弱点也存在于多个方面，仅仅利用安全技术，采用安全产品并不能取得良好的效果。例如，“9·11”事件造成世贸中心 1 200 家企业信息网络荡然无存，这种破坏方式是安全技术所无法解决和预测的问题。然而面对飞来横祸，拥有灾难恢复计划和业务连续性规划的 400 家企业重新恢复并生存下来，而另外的 800 家企业，不管其购买了多么昂贵的防火墙系统，多么先进的入侵检测系统，等来的只能是无情的淘汰。因此，如今基于风险的信息安全保障体系被广泛接受和采纳。

风险管理是信息安全的基础工作和核心任务之一，是最有效的一种措施，是保证信息安全投资回报率优化的科学方法。20 世纪 60 年代，风险管理理论应用于信息安全领域。此后，信息安全风险管理的实践和理论的发展大体上经过了以下 3 个阶段[1]。

1. 20 世纪 60～80 年代是信息安全风险管理实践与理论发展的初期阶段

20 世纪 60 年代，随着资源共享计算机系统和早期计算机网络的出现，计算机安全问题初步显露。1967 年秋，美国国防部委托兰德公司为首的多个研究机构和企业，进行了美国历史上第一次大规模的计算机安全风险评估，历时 3 年。1970 年年初出版了一个长达数百页的机密报告《计算机安全控制》。该报告奠定了国际安全风险评估的理论基础。

在此基础上，美国率先推出了首批关于信息安全风险管理及相关的安全评测标准。其中，第一组标准是由国家标准局（NBS）制定的，如 FIPS PUB 31 自动数据处理系统物理安全和风险管理指南（1974 年），FIPS PUB 65 自动数据处理系统风险分析指南（1979 年）。第二组是由美国国防部国家安全局于 1983 年后陆续制定的计算机系统安全评估系列标准，主要包括《可信计算机系统安全评估准则》（TCSEC）、《可信网络解释》（TNI）、《特定环境下的安全需求》等，总计约 40 个各类标准。由于每个标准用不同颜色的封皮，俗称为“彩虹系列”。

2. 20 世纪 80 年代末～90 年代末是信息安全风险管理实践和理论走向初步成熟的阶段

1989 年美国率先建立了计算机应急组织。次年，建立了信息安全事件应急国际论坛。1992 年美国国防部建立了漏洞分析与评估计划。1994 年美国国家安全局等组织构成的联合委员会明确提出，美国国家信息安全必须建立在风险管理的基础上。

1995 年 12 月美国国防部提出了信息安全的动态模型，即“防护—监测—反应”多环节保障体系，后通称“PDR 模型”。

同期，其他国家也开始制定本国的信息安全测评标准。加拿大制定了加拿大可信计算机产品评估标准（Canadian Trusted Computer Product Evaluation Criteria，CTCPEC），前联邦德国制定了信息安全技术的安全评价标准，英国制定了自己的安全控制和安全目标的评估标准。为了解决标准间的兼容和评估结果互认的问题，1990 年，英、法、德、荷 4 国着手制定了共同的信息技术安全评估标准（ITSEC），提出了包含保密性、完整性、可用性等概念的评估准则，强调把信息系统环境中的威胁与风险纳入评估视野。

1993 年欧美 6 个国家又启动了建立共同评测标准（即后来的 CC 标准）的计划，1996 年 1 月第一版发布，1999 年 12 月被国际

标准化组织采纳为国际标准，编号为 ISO 15408。这个期间英国自己还研发了基于风险管理的 BS 7799 信息安全管理标准，澳大利亚和新西兰制定了共同的风险管理标准 AS/NES 4360。

1997 年 12 月，美国国防部发表了《信息技术安全认证和批准程序》（DITSCAP），成为美国涉密信息系统的安全评估和风险管理的重要标准和依据。

3. 20 世纪 90 年代末至今，国际范围的风险管理实践与理论进入第三个阶段，即全球化阶段

由于 20 世纪 90 年代以来互联网、移动通信和跨国光缆的高速发展，各国原本局限于本国内的信息网络迅速跨越国境连成一片。与此同时，信息安全也成为世界各国面临的共同挑战。

2002 年，美国通过了一部联邦信息安全管理法案（FISMA）。根据该法案，美国国家标准和技术委员会（NIST）负责为美国政府和商业机构提供信息安全管理相关的标准规范。NIST SP 800 系列已经出版了近 90 本同信息安全相关的正式文件，形成了从计划、风险管理、安全意识培训和教育以及安全控制措施的一整套信息安全管理体系。其中，正式发布的此类标准主要有：SP800—26 信息技术系统安全自评估指南（2001 年）、SP800—30 信息技术系统风险管理指南（2002 年）、SP800—51CVE 使用和漏洞命名法（2002 年），等等。

2005 年，国际上具有权威的国际标准化组织（ISO）和国际电工委员会（IEC）将 2000 年发布的 7799 系列信息安全标准改版为 ISO 27000 系列，成为继 ISO 9000、ISO 14000 之后，又一个在全世界范围内被广泛接受和使用的国际认证体系。随着 ISO/IEC 27000 系列标准的规划和发布，ISO/IEC 已形成了以信息安全管理体系（Information Security Management System，ISMS）为核心的一整套包括 ISMS 要求、风险管理、度量和测量以及实施指南等在内的信息