电子信息科技专著出版专项资金
cbjj.phei.com.cn

http://www.phei.com.cn

信息安全风险评估

王英梅　王胜开　陈国顺　程湘云　编著

Information Security Risk Assessment

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

电子信息科技专著出版专项资金资助出版

信息安全风险评估

王英梅　王胜开
陈国顺　程湘云
编著

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

内 容 简 介

信息安全风险评估是近年来迅速发展起来的一个新兴研究课题，是信息安全和信息系统领域迫切需要解决的一个“热点”、“难点”问题。本书结合作者的科研工作、教学实践和理论研究成果，对信息安全风险评估所涉及的基本概念、理论模型、关键技术、评估方法、评估过程、基本准则等主要内容进行了深入、系统的论述，使读者通过阅读本书能对信息安全风险评估的基本理论与关键技术有一比较全面的了解，并能参照书中所举案例具体完成信息安全风险评估项目。

本书可作为信息安全、网络系统和计算机专业的高年级本科生、研究生参考教材，也可供相关领域的研究开发人员、工程技术人员、系统管理人员阅读。

图书在版编目（CIP）数据

信息安全风险评估/王英梅，王胜开，陈国顺等编著. —北京：电子工业出版社，2007.6
ISBN 978-7-121-04490-8

Ⅰ. 信… Ⅱ. ①王…②王…③陈… Ⅲ. 信息系统—安全技术—风险分析 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2007）第 074155 号

责任编辑：高买花　　特约编辑：陈宁辉
印　　刷：北京牛山世兴印刷厂
装　　订：
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：787×1 092　1/16　印张：17　字数：393 千字
印　　次：2007 年 6 月第 1 次印刷
印　　数：4 000 册　　定价：33 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。

前　言

人类社会进入信息时代，信息空间已成为继陆、海、空、天之后，引发又一轮国际竞争的、新的第五维战略空间。人们在享受信息和信息系统带来的巨大利益的同时，也面临着信息安全方面的挑战。通过近几年来对信息安全的不断研究，人们对信息安全内涵的认识不断深入，从最初的信息保密性发展到了信息的完整性、可用性、可控性和不可否认性，进而又提出和发展了“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等众多方面的基础理论和专业技术。在此过程中，信息安全风险评估逐渐成为安全管理领域中一个重要的手段和工具。

信息安全是一个动态的复杂过程，贯穿信息资产与信息系统的整个生命周期，必须按照风险管理的思想，对可能的威胁、脆弱性和需要保护的信息资产进行分析，依据风险评估结果对信息系统选择适当的安全措施，以妥善应对可能面对的威胁和可能发生的风险。由于信息技术的飞速发展，关系国计民生的关键信息基础设施的规模越来越大，信息系统越来越复杂，必须提倡信息安全风险评估制度化，并建立科学、有效的信息安全风险评估机制与方法。

建立信息安全保障体系是信息安全建设的主要任务，作为信息安全保障体系建设的基础与保证，信息安全风险评估具有不可替代的重要作用，已引起世界各国的广泛关注和重视。为帮助研究开发人员、工程技术人员、系统管理人员等更好地理解信息安全风险评估的理论、技术、方法、应用和未来发展趋势，为实际工作提供更多、更好的帮助，我们总结教学与科研实践，结合具体的案例，有针对性地对这一问题进行了分析和阐述，以供广大读者参考、借鉴。

本书主要阐述信息安全风险评估理论、技术、方法、应用等热点问题，目的是对信息安全风险评估所涉及的主要问题和关键问题进行全面、系统的论述。全书注意理论与实践相结合，使读者在对信息安全风险评估基本原理有一全面了解的基础上，能够参照书中所举案例具体完成一个风险评估项目。本书首先介绍信息安全风险评估的基本概念、关键技术、常用方法、主要过程、基本准则、评估模型等，然后结合典型案例，对常用的风险评估方法和工具进行分析，提出信息安全风险评估的基本框架以及每一步操作涉及的关键要素；书中详细论述了基于代理的威胁评估方法以及基于概率影响图的信息安全风险评估方法，对信息安全风险评估中的人为失误风险评估以及网络空间下的风险评估进行了阐述，并介绍了当前最主要的信息安全风险评估标准；最后，通过一个典型案例对整个信息安全风险评估过程进行完整描述。

全书共分 13 章，其中第 1 章、第 2 章、第 5 章由王胜开、王英梅编写，第 3 章、第 4 章、第 6 章、第 7 章、第 9 章、第 11 章由王英梅编写，第 8 章、第 10 章由程湘云编写，

第 12 章、第 13 章由陈国顺、王英梅编写，最后全书由王英梅、王胜开统稿。

在本书编写过程中，得到了余达太教授、刘增良教授、陈富贵高工、全寿文研究员等专家的大力指导和帮助，在此表示衷心感谢！

因时间仓促、作者水平和经验有限，书中错漏之处在所难免，敬请读者指正。

编 著 者

2007 年 5 月

目　录

第1章 绪 论

1.1 引言

安全是当前全球最关注也是最令人头疼的问题之一。安全是个大概念，涉及国土安全、能源安全、人身安全、财产安全、信息安全等众多方面，本书主要讨论的是信息安全及其风险评估问题。

人类社会进入信息时代，信息成了一项重要资源，信息系统、信息网络成为了支撑信息时代人类社会的一个重要支柱，信息不再只是意味着“知多知少”和精神财富，它已成为衡量一个国家军队实力、主权和安全的重要依据和基本参照。

信息时代人类社会需要快速、准确、安全地信息传递、信息交换、信息处理、信息共享和信息应用，人类活动、社会生活的各个方面几乎都离不开计算机系统和信息网络。随着国际互联网、光纤、个人计算机等的普及，世界各地的人们越来越联结成一体，地球真的越来越像个小“村”了，“信息”也从专业人士使用的一个专业术语变成了广大百姓的“口头禅”。

但另一方面，在信息和信息系统越来越普及、给人们带来越来越多便利、极大推动人类社会发展的同时，如同现实生活中一样，在信息领域、网络世界中也难免会有那么一些“不安分分子”，出于种种原因要“捣捣乱”，病毒、黑客、信息泄露、拒绝服务、特洛伊木马、网络犯罪等已对信息的安全构成了严重威胁。信息系统，尤其是像国际互联网这样的公众网络，许多时候像是一座不设防的城，裸露在外，潜在各种安全隐患和风险。

近年来，来自信息领域、网络世界的威胁不时出现，向人们敲响了警钟，信息安全、网络安全问题越来越受到人们的重视，使人们意识到需要寻求一种有效的解决方案来应对这些威胁和风险，保证信息安全以及与信息安全相关的总的社会安全。信息的开发与利用、控制与反控制、攻击与防御、风险与安全等正成为各国研究的一大热点，甚至关系国家的兴衰强弱。信息空间已成为继陆、海、空、天之后引发又一轮国际竞争的、新的第五维战略空间。

针对这样的形势我们推出本书，希望能对大家提高信息安全意识、做好信息安全风险评估，并最终保证信息安全有所帮助。

1.2 信息安全风险评估研究背景

近年来，有关国际互联网和其他各种信息网络、信息系统的安全问题、安全事故频频发生，时有报道。据《电子商务时代》称，“I love you!”病毒影响到了4500多万台主

机，造成的经济损失高达 26 亿美元；声名狼藉的 Melissa 宏病毒在 1999 年就造成了 3 亿美元的损失；一些著名的电子商务网站在 2000 年初遭到了分布式拒绝服务攻击（DDOS）的破坏，也造成了巨大损失。据估计，全球 2002 年一年因“自动数字攻击”（Automatic Digital Attack）而造成的损失超过 300 亿美元。

据国家计算机网络应急技术处理协调中心（CNCERT/CC）统计，2003 年报告的信息安全、网络安全事件达 137529 件，远远高于 2001 年的 52658 件和 2002 年的 82094 件。据 CNCERT/CC 在“2005 中国计算机网络安全应急年会（CNCERT/CC '2005）”上公布的“2004 年网络安全工作报告”，CNCERT/CC 在 2004 年共收到国内外通过应急热线、网站、电子邮件等报告的网络安全事件 64686 件，相比 2003 年收到的 13000 多件报告数量，2004 年的网络安全事件报告数量大幅增加。

过去的十多年间，网络破坏、网络攻击的蔓延速度及其造成的损失呈指数增长，“势头强劲”，实在令人担忧。

信息安全、网络安全问题正变得日益复杂，影响不断扩大，从目前的状况来看，很难在短期内得到比较全面、彻底的解决。

随着信息技术的推广应用和不断发展，信息安全的内涵也在不断延伸，从最初的信息保密性发展为信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

实践表明，信息安全是一个动态的复杂过程，它贯穿于信息资产和信息系统的整个生命周期。信息安全的威胁可能来自内部破坏、外部攻击、内外勾结的破坏或自然灾害。为了保证信息安全、网络安全，必须按照风险管理的思想，对可能的、潜在的威胁、弱点和需要保护的信息资源、信息系统等进行分析，依据风险评估的结果为信息和信息系统选择适当的安全措施，积极应对可能遭遇的风险。

由于信息技术的飞速发展，关系国计民生的关键信息基础设施的规模越来越大、系统越来越复杂。信息安全风险评估成为一个越来越紧迫的问题，已引起各发达国家的高度重视，提出了要实现风险评估的制度化，认为没有有效的风险评估将会造成信息安全需求与安全解决方案之间的严重脱节，“没有什么事情比解决错误的问题和建立错误的系统更没有效率了”。经过这些年的发展，西方各发达国家已普遍提高了对信息安全的认识，大力开展以风险评估为核心的信息系统安全评估工作，提出了一系列理论、技术、方法、措施和机制，并付诸实践。

风险评估最早应用于处于相对独立且严密控制环境下的大型计算机和数据中心。随着个人计算机逐步替代终端系统，以及国际互联网的发展和普及，计算机安全问题日益增加。传统的硬件解决之道，如安装防火墙或自动审计日志对高级管理者来说存在判断困难的问题，并且某些配置并不能有效防止信息泄露和安全事故的发生。科学、合理的风险评估为信息安全提供了一种比较根本、有效的解决途径。

风险评估是一项费时、费力的工作，需要专业人员和专业知识的支持。为使风险评估能在各行各业中广泛开展，风险评估工具成为不可或缺的技术支持手段。风险评估工具不仅把技术人员从繁杂的资产统计、风险评估过程中解脱出来，还可以完成一些人力

无法完成的工作，如网络或主机中漏洞的搜寻、定位，在历史数据积累和专家知识提炼等方面具有巨大优势，可以极大减轻技术人员的负担，为各种形式的风险评估，如自我评估、检查评估等提供了有力支持。

目前，许多组织根据安全管理指南和标准开发了风险评估工具，为风险评估工作的开展提供了便利条件，但风险评估工具的完善还需要很长一段时间。综观目前各风险评估工具的状况，还存在不少问题，如工具运用的结果如何能够比较准确地反映客观实质、如何有效度量、如何综合和协调工具的使用等。

我国在风险评估工具的开发方面尚处于萌芽阶段，必须大力加强风险评估基础理论的研究力度，积极开发具有自主知识产权的风险评估工具。

1.3 信息安全风险评估发展历程

1.3.1 总的发展历程

风险评估不是一个全新的概念，它最早于20世纪五六十年代开始应用于欧美核电厂的安全性评估中，随后在发达国家的航天工程、化学工业、环境保护、医疗卫生、交通运输、国民经济等众多领域得到推广和应用。近年来，风险评估方法在信息安全领域的研究与应用逐步开始引起人们的重视。

为了能够更好地理解信息安全风险评估的研究内容和研究现状，首先回顾一下信息安全风险评估的发展历程。

信息安全风险评估最早由美国提出。20世纪70年代初，美国国家标准局即现在的美国标准与技术局（NIST），首先认识到有必要对信息安全进行评估。在《自动数据处理物理安全与风险管理手册》中，NIST提出了在开发一个安全项目之前需进行风险评估的要求，尽管这一手册只是比较概括地、原则性地提出了风险评估的概念，但它的提出表明NIST更进一步地认识到了进行信息安全风险评估的重要性，极大地推动了风险评估的研究进程，之后不久推出了《自动数据处理风险分析手册》（FIPSPUB-65，1979）。与此同时，美国预算管理办公室制定了OMBA-71，在这个规定的附件C中指出，必须对政府中运行的计算机及其他为政府服务的计算机系统进行定期的、定量的风险评估。

随着FIPSPUB-65推广使用，在实际操作过程中遇到了许多困难，主要困难是缺少关于威胁频率的数据以及缺少信息评估价值标准。一般认为，用于风险评估的定量方法是客观的，并且可信的、定量的数据是可以得到或可以推断的，而用于风险管理的定性方法一般被认为因可信数据不易得到或费用太高而不宜付诸实施。总之，此时对信息资产价值的确定以及统计数据的可信性都存在质疑。尽管如此，在当时的历史条件下，FIPSPUB-65评估方法还是恰当、够用的，并成为了当时标准的风险评估方法。

20世纪70年代初，首先是美国能源局在原子能工业领域发起了实质性的风险研究与评估工作。对原子能风险评估技术标准来说，它要求确定严格的评估标准，建立可信的风险模型。由于缺少原子能威胁的历史和经验数据，其风险评估模型主要根据专家的经验和观点来建立。通过研究和反复试验，1975年10月颁布了《美国核管会报告——核反

应风险研究》，即《WASH 1400 报告》。

随着信息安全风险评估的技术要求越来越高，《WASH 1400 报告》的严格性、正确性和技术方法、评估机制等逐步被引入到信息安全风险评估与管理中。

20 世纪 80 年代，定量评估技术的发展受到联邦政府警察局的阻止，原因是考虑到定量风险评估方法在使用过程中遇到的数据收集困难问题。1985 年 12 月，OMBA-130 在附件 3 中要求大范围地对计算机系统进行一次正式、量化（此处的量化并不要求是完全的、定量的表示，可以是一种等级的描述）的风险分析和评估，这一要求取代 OMBA-71 附件 C，成为对计算机系统进行定量风险评估的标准。

20 世纪 80 年代末，为了开发一个权威性的框架以便用于信息安全风险评估，NIST 发起并建立了“国际计算机安全风险管理模型研究小组”，力图建立一个技术上合理并满足各种信息处理系统要求的安全风险评估框架，以便为信息安全风险评估与管理提供一个更加全面的、数据可信的指导方针。这一小组的最初成果是认识到了在任何风险评估中不确定性都扮演着重要的角色，必须加以深入分析。

NIST 信息安全风险评估与管理框架如图 1.1 所示。

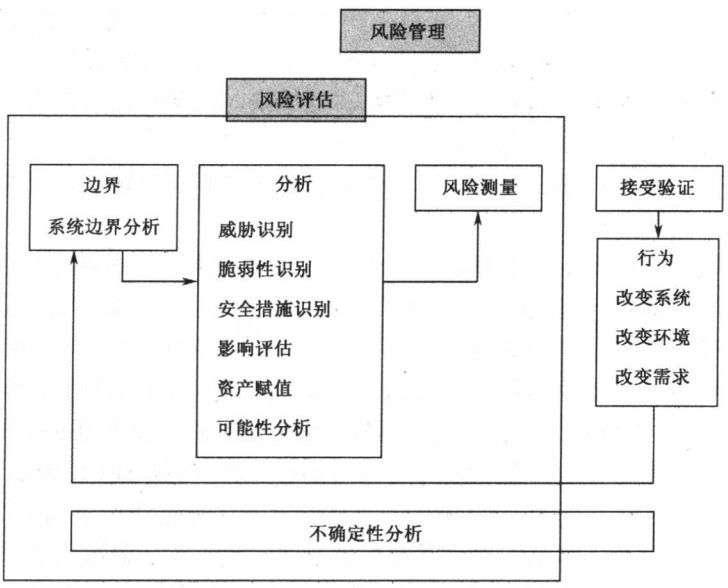

图 1.1　NIST 信息安全风险评估与管理框架

在 20 世纪 80 年代期间，风险评估方法论方面遇到了很大的障碍。首先是评估结论的时效性问题。手工执行一个风险评估项目对高级的定性分析来说，大致需要花费 1～2 个月的时间，而要进行大范围的、深入的定量风险评估可能需要花费 2 年以上的时间。由于在项目实施过程中许多情况可能已发生了变化，因此经过这么漫长的过程后得到的结论常常是过时的，致使最终的风险评估结果不准确。其次，评估在识别资产价值（尤其对无形资产价值）过程中往往陷入困境，对可信的威胁频率数据确立过程也是这样，因此也会造成风险评估结果的准确性降低。

另一个主要问题是过于简单的风险评估算法。这些方法无法区分那些频率低、影响大的威胁所引起的风险以及频率高、影响小的威胁所引起的风险，例如火灾的影响和资源误用的影响。“火灾导致5万元的年损失率”和“资源误用导致6万元的年损失率”这样的评估结果将表明火灾和资源误用的风险是同等的——管理者将拒绝接受这样的分析结论。直观上他们认为火灾是更大的威胁，如果发生火灾则会给其带来更大的损失，因此管理上他们愿意花更多的资金来避免或阻止火灾的发生，而只愿意花一小部分资金来防止资源的误用，并且这方面的投入一般用于制定安全策略或员工警戒制度上，若发现谁滥用资源则首先予以警告，严重者将被解雇等。在大型、复杂系统中，这种简单的、几乎凭直观感觉的风险评估策略或算法将严重影响定量风险评估方法和结果的可信性。

为了应对这种情况和克服这些弊端，美国开发了用于信息自动分析与管理的软件包。一些软件因其在概念方面的独特性、先进性脱颖而出，如RISKPAC，这是一个定性的风险评估软件，它并不试图对所有风险实施完全量化，而是为管理者提供了一个经验性的，对脆弱性、风险和威胁造成后果进行排序的方法。尽管该软件被众多用户所接受，但考虑到它在分析问题方面的主观性、经验性以及缺少定量的结论，因此目前一般将之限用在信息安全的预估、预算方面。

20世纪80年代中期，信息安全风险评估技术有了实质性的突破，主要表现在以下两个方面：

- 贝叶斯决策支持系统（BDSS）；
- Lawrence Livermore 实验室风险分析方法（LRAM），LRAM之后逐渐演变成为自动LRAM，即ALRAM。

BDSS 和 ALRAM 这两种方法都借鉴和采用了核工业中先进的风险评估算法，把它们引入到了信息安全领域，代替FIPSPUB-65，逐步成为最基本的信息安全风险评估方法。

尽管这两种方法在技术上都比较先进，并且都采用了关系型数据库结构，但也存在许多不同之处：

（1）BDSS 是一个专家系统，它为用户提供了一个完整的数据库，包括漏洞、安全措施、威胁因素及其发生概率等，这些数据相互映射，用于风险建模中并用自然语言予以表达；

（2）ALRAM 则要求专家在方法运用过程中首先根据目标系统的实际情况建立和映射知识库，然后进行风险分析，因此对具体目标系统的针对性较强，但知识库的构建需要花费较长的时间和较大的工作量。

这两个软件包都是自动的信息安全风险定量分析软件包，能够用来判断一个组织是否按照信息安全规章制度的要求来开展工作，它们都已被美国政府部门采用。

另外，还有许多类似的软件，如 ARES、@RISK、Control Matrix Methodology for Microcomputers 等。信息安全风险评估与管理软件能够提高风险分析的效率，能够使分析者的注意力更多地集中于重要的风险因素上。即使是相对初级的软件，也能使工作量减少20%～30%；运用得当，高级的、基于知识的软件有望将工作量减少80%～95%，基于知识的软件包在帮助分析者大量减少信息收集工作和不必要的分析方面非常有效，将大大提高信息安全风险评估的效率和效果。

为了更好地了解信息安全风险评估的发展历程，下面对发生在美国和其他国家的一些相关的重要事件做一回顾。

1.3.2　美国的发展状况

信息安全领域的风险研究始于20世纪60年代，美国是国际上对信息安全风险评估研究最早、历史最长、经验最丰富的国家。随着信息化应用需求的牵引、安全事件的驱动、信息安全技术与信息安全管理概念的发展，其对信息安全风险评估的认识也逐步加深。

在美国，信息安全从最初的关注计算机保密技术与问题逐步发展到目前的关注信息系统基础设施信息保障技术与问题，经历了三个主要阶段。

1．第一个阶段（20世纪60～70年代）：以计算机为对象的信息保密阶段

（1）背景：计算机开始应用于政府和军队。

（2）标志性事件：1967年11月，美国国防科学委员会委托兰德公司（RAND）、迈特公司（MITIE）及其他一些与国防工业有关的公司，着手研究计算机安全问题。1970年2月，对当时的大型机、远程终端等进行了第一次较大规模的风险评估。

（3）此阶段有关风险评估的重要工作结果包括：1973年，美国国防部（DoD）开始制定有关计算机安全的法规、指令和标准（5200.28、5200.28M和5200.28 STD）。1977年，美国国防部正式提出BLP模型。1978年，美国白宫OMB（管理和预算办公室）发布了《联邦自动化信息系统的安全》（A-71）通告。1979年，NBS颁布了一个风险评估标准：《自动数据处理系统（ADP）风险分析标准》（FIPS65）。

（4）此阶段的主要特点：主要针对计算机系统的保密性问题提出了要求，对安全的评估仅限于保密性。

2．第二个阶段（20世纪80～90年代）：以计算机和网络为对象的信息安全保护阶段

（1）背景：计算机系统的网络化应用。

（2）标志性事件：出现了早期的、针对美军的计算机黑客行为。美国审计总署（GAO）对美国国内主要由国防部使用的计算机网络进行了大规模的持续评估。

（3）此阶段有关风险评估的重要工作结果包括：1985年橘皮书正式成为国防部标准，形成了美国早期一套比较完整的、从理论到方法的、有关信息安全评估的准则——彩虹系列。1983年，制定了联邦信息处理标准FIPS102《计算机安全认证和认可指南》。1885年12月，OMB颁布了《联邦信息资源管理》（A-130）通告。1990年和1992年，美国军方先后颁布了DOD-2167A和MIL-STD-499B，开始从软件工程的生命周期过程和系统工程的生命周期过程角度关注产品和系统的质量。1992年，美国联邦政府制定了《联邦信息技术安全评价准则》（FC）。1993年，美国和欧洲四国（英、法、德、荷）、加拿大以及国际标准化组织（ISO）共同制定了信息技术安全通用评估准则（CC），并于1999年成为国际标准ISO/IEC 15408。