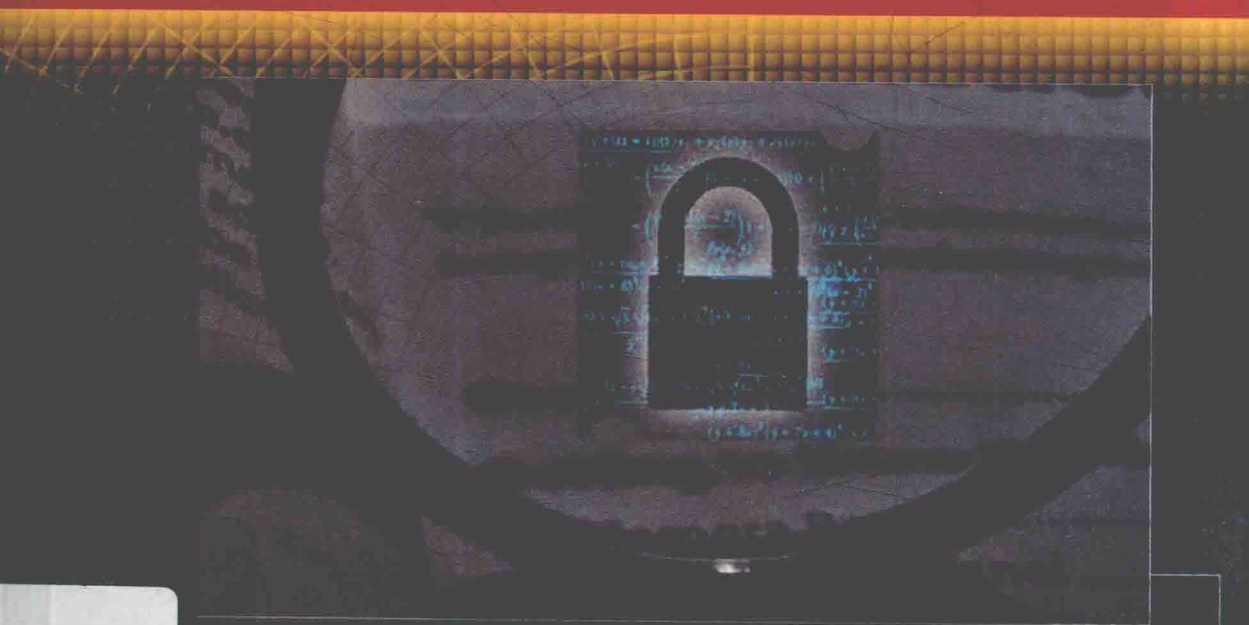
网络与信息安全前沿技术丛书

信息系统安全风险评估与防御决策

王晋东　张恒巍　王娜　徐开勇　著

Information System Security Risk Assessment and Defense Decision-making



国防工业出版社
National Defense Industry Press

网络与信息安全前沿技术丛书

王晋东　张恒巍
王　娜　徐开勇　著

信息系统安全

风险评估与防御决策

Information System Security Risk Assessment and Defense Decision-making

准确评估信息系统面临的安全风险，根据评估结果有针对性地实施风险管控和安全防御，是确保信息系统安全的基础和关键。本书运用博弈理论，从攻防对抗的角度全面分析了信息系统安全风险的组成要素和作用机理，系统介绍了基于信息攻防博弈的安全威胁评估和漏洞危害评估、信息资产评估指标构建及优化、安全风险要素分布特征获取与分析、信息安全防御决策等内容。本书可以作为网络空间安全、信息安全管理、网络对抗等方向的科研及工程技术人员的参考书，也可供相关专业高校师生使用。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

信息系统安全风险评估与防御决策/王晋东等著.
—北京:国防工业出版社,2017.1
(网络与信息安全前沿技术)
ISBN 978-7-118-11143-9

Ⅰ.①信… Ⅱ.①王… Ⅲ.①信息系统-安全技术-研究 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2017)第 012990 号

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号 邮政编码 100048)
北京嘉恒彩色印刷有限责任公司
新华书店经售

*

开本 710×1000 1/16 **印张** 18¾ **字数** 341 千字
2017 年 1 月第 1 版第 1 次印刷 **印数** 1—2000 册 **定价** 89.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777 发行邮购:(010)88540776
发行传真:(010)88540755 发行业务:(010)88540717

《网络与信息安全前沿技术丛书》编委会

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的《网络与信息安全前沿技术丛书》即将分期出版。丛书有如下特点：一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

们多年来在该领域从事科技攻关的实践经验，可适应不同层次读者的需求。三是权威性好。编委会由我国网络和信息安全领域权威专家学者组成，各分册作者又均为我国相关领域的知名学者、学术带头人，理论水平高，并有长期科研攻关的丰富积累。

我认为该丛书是一套难得的系统研究网络信息安全技术及应用的综合性书籍，相信丛书的出版既能为公众了解信息安全知识、提升安全防护意识提供很好的选择，又能为从事网络信息安全人才培养的教师和从事相关领域技术攻关的科技工作者提供重要的参考。

作为特别关注网络信息安全技术发展的一名科技人员，我特别感谢何德全院士等专家学者为撰写本书付出的艰辛劳动和做出的重要贡献，愿意向读者推荐该套丛书，并作序。

前言

随着信息技术的高速发展和信息服务的广泛应用，信息安全日益受到世界各国的高度关注。与此同时，信息攻击技术的发展和网络战的兴起，导致网络空间的攻防对抗日趋激烈，信息系统面临的安全风险更加严峻和复杂。研究信息系统安全风险评估技术，切实掌握安全风险状态，确保安全风险可管可控、安全防御及时高效，对于保障信息系统安全具有重要的理论和实践价值。本书是作者团队近年来在信息安全领域研究成果的总结和提炼，是对信息系统安全风险评估与防御决策的理论、方法和技术上的探索与实践，希望能够帮助读者启发思维，点燃创新的灵感。

全书共8章。第1章介绍信息系统安全风险、安全风险评估和防御决策等基本概念，总结当前安全风险评估和防御决策的研究现状，分析现有理论和技术存在的不足以及实践应用中面临的挑战。第2章介绍信息系统安全风险评估的基本原理和主要模式，从总体和全局的层次建立理解安全风险评估的理论框架，对目前风险评估实践中常用的工具进行简要介绍。第3章采用博弈理论刻画信息攻防对抗，通过信息攻防博弈建模研究信息安全和信息攻防之间的关系与相互影响，介绍了信息攻防博弈的主要特点、一般模型和基本建模方法。第4章采用信息攻防博弈模型研究安全威胁评估，分析总结静态安全威胁评估和动态安全威胁评估的不同特点，描述基于不完全信息攻防博弈模型的静态威胁评估技术，以及基于攻防信号博弈模型的动态威胁评估技术。第5章基于博弈模型和风险矩阵研究漏洞危害评估，分析信息系统脆弱性和漏洞危害的组成，介绍漏洞本体危害和关联危害的评估原理，阐述基于博弈模型的漏洞本体危害评估技术、基于风险矩阵的漏洞关联危害评估技术以及漏洞综合危害的评估过程和方法。第6章主要探讨信息资产评估指标的构建与动态优化，提出了一种采用层次网结构的资产评估指标体系，给出了基于多轮咨询反馈的评估指标构建方法，以及基于灰关联分析的评估指标与权重优化技术，为形成高质量的资产评估指标提供理论和方法指导。第7章主要讨论信息系统中

安全风险要素分布特征的获取，阐述基于智能聚类算法实现风险分布特征获取的思路，分析基于子空间软聚类理论的智能聚类方法，实现对风险要素向量的聚类。第8章主要关注信息系统安全防御决策，以非合作博弈理论为基础，给出安全防御决策的数学描述，分析介绍了适用于不同场景的完全信息静态攻防博弈、静态贝叶斯攻防博弈和动态多阶段攻防信号博弈模型，以及不同攻防博弈模型的均衡求解方法和最优安全防御策略选取方法。

王衡军、孙先友、王坤、陈宇、余定坤、何嘉婧、李涛、余智勇、牛侃、黄建明、方晨等为本书的撰写做出了贡献，其中王衡军和孙先友参与了第1、3章的编写，王坤和陈宇参与了第2章的编写，余定坤参与了第4、8章的编写，何嘉婧参与了第7章的编写，李涛和黄建明参与了第5、8章的编写，余智勇和方晨参与了第6、7章的编写，牛侃参与了第2章和附录的编写，黄建明和方晨承担了本书部分绘图和校对工作，在此对他们的工作表示感谢。

本书所涉及的内容具有尝试和探索的性质，相关的理论和实践还需要进一步的研究，加之作者的学识和能力有限，书中疏漏和不当之处在所难免，真切地希望得到读者的反馈和帮助。

目　录

第 1 章　绪论 …… 1

1.1　引言 …… 1
1.2　信息系统 …… 3
1.3　信息系统安全风险 …… 5
1.3.1　信息系统安全的基本属性 …… 5
1.3.2　风险的概念和含义 …… 6
1.3.3　信息系统安全风险 …… 6
1.4　信息系统安全风险评估概述 …… 7
1.4.1　信息系统安全风险评估的相关概念 …… 8
1.4.2　信息系统安全风险评估的目的和意义 …… 10
1.4.3　信息系统安全风险评估的原则 …… 10
1.5　信息系统安全风险评估发展现状 …… 11
1.5.1　信息系统安全风险评估规范和原理 …… 11
1.5.2　威胁评估 …… 13
1.5.3　脆弱性评估 …… 15
1.5.4　资产评估 …… 16
1.5.5　安全风险综合评估 …… 17
1.6　安全风险评估的不足与面临的挑战 …… 19
1.6.1　评估理论中存在的不足 …… 20
1.6.2　评估实践中面临的挑战 …… 21
1.7　信息系统安全防御决策 …… 23
参考文献 …… 23

第 2 章　信息系统安全风险评估理论与实践 …… 28

2.1　风险评估原理 …… 28

2.1.1 风险综合评估思想 …… 28
2.1.2 风险评估基础理论 …… 29
2.1.3 风险要素评估的主要内容 …… 30
2.2 风险评估模式 …… 30
2.2.1 技术评估和整体评估 …… 30
2.2.2 定性评估和定量评估 …… 31
2.2.3 静态评估和动态评估 …… 32
2.2.4 基于知识的评估和基于模型的评估 …… 33
2.3 风险评估实践分析 …… 33
2.3.1 选择风险评估工具的基本原则 …… 34
2.3.2 管理型风险评估工具 …… 36
2.3.3 技术型风险评估工具 …… 43
2.3.4 风险评估辅助工具 …… 48
参考文献 …… 49

第3章 信息攻防博弈建模 …… 51

3.1 引言 …… 51
3.2 博弈论的发展历程 …… 52
3.3 博弈论基础 …… 53
3.3.1 博弈论基本概念 …… 53
3.3.2 博弈的结构 …… 56
3.3.3 博弈均衡 …… 63
3.4 信息安全与攻防博弈 …… 69
3.4.1 信息安全与攻防博弈的关系 …… 69
3.4.2 信息攻防博弈的特点 …… 70
3.4.3 信息攻防博弈的模型结构 …… 71
3.4.4 信息攻防博弈的研究进展及应用 …… 72
3.5 攻防行为建模与策略提取 …… 74
3.5.1 攻击树方法 …… 74
3.5.2 攻击图方法 …… 75
3.5.3 基于安全状态约简的攻防图方法 …… 76
3.5.4 应用实例 …… 82

参考文献 …… 85

第 4 章　基于信息攻防博弈的安全威胁评估 …… 88

4.1　引言 …… 88
4.2　安全威胁评估分类 …… 89
4.2.1　静态安全威胁评估 …… 89
4.2.2　动态安全威胁评估 …… 90
4.2.3　当前威胁评估技术的不足 …… 91
4.3　基于不完全信息攻防博弈模型的静态威胁评估技术 …… 91
4.3.1　信息攻防博弈问题描述 …… 92
4.3.2　不完全信息静态攻防博弈模型 …… 92
4.3.3　攻防策略收益量化与计算 …… 95
4.3.4　静态贝叶斯均衡分析 …… 99
4.3.5　静态安全威胁评估算法 …… 100
4.3.6　评估实例 …… 102
4.4　基于攻防信号博弈模型的动态威胁评估技术 …… 106
4.4.1　攻防信号博弈模型 …… 107
4.4.2　攻防策略收益量化与计算 …… 108
4.4.3　精炼贝叶斯均衡求解 …… 110
4.4.4　动态安全威胁评估算法 …… 114
4.4.5　评估实例 …… 118
参考文献 …… 120

第 5 章　基于博弈模型和风险矩阵的漏洞危害评估 …… 123

5.1　引言 …… 123
5.2　信息系统脆弱性分析 …… 124
5.3　漏洞危害评估技术分析 …… 126
5.4　基于漏洞博弈模型的漏洞本体危害评估 …… 127
5.4.1　漏洞攻防博弈模型 …… 127
5.4.2　攻防策略收益量化与计算 …… 128
5.4.3　均衡分析和漏洞本体危害计算 …… 129
5.5　基于综合风险矩阵的漏洞关联危害评估 …… 131

5.5.1 风险矩阵定义 …… 131
5.5.2 风险矩阵算子 …… 131
5.5.3 漏洞关联危害计算 …… 133
5.6 漏洞综合危害及其评估 …… 133
5.6.1 漏洞综合危害度量 …… 133
5.6.2 漏洞综合危害评估算法 …… 134
5.6.3 评估应用实例 …… 135
参考文献 …… 137

第6章 信息资产评估指标构建与动态优化 …… 139

6.1 资产评估的内容 …… 139
6.2 资产评估指标体系结构设计 …… 141
6.2.1 资产评估指标体系构建原则 …… 141
6.2.2 网状指标体系结构模型 …… 142
6.2.3 树状指标体系结构模型 …… 143
6.2.4 层次网指标体系结构模型 …… 144
6.2.5 一种信息系统资产评估指标体系结构 …… 145
6.3 基于多轮咨询反馈的评估指标构建方法 …… 146
6.3.1 专家评价意见获取 …… 147
6.3.2 指标构建过程 …… 149
6.3.3 基于多维空间距离的评价数据偏离度计算 …… 150
6.3.4 基于信息熵的指标重要度计算 …… 151
6.3.5 指标权重分配 …… 152
6.3.6 实例分析 …… 152
6.4 基于灰关联分析的评估指标和权重优化技术 …… 154
6.4.1 指标和权重优化技术简介 …… 154
6.4.2 评估数据处理 …… 155
6.4.3 条件指标重要度与影响度 …… 156
6.4.4 指标与权重优化 …… 158
6.4.5 数值实验与分析 …… 159
参考文献 …… 161

第 7 章　信息系统安全风险要素分布特征获取与分析 …… 162

7.1　引言 …… 162
7.2　信息系统的安全风险分布 …… 163
7.3　典型智能聚类算法分析 …… 164
7.4　安全风险分布特征获取问题分析 …… 169
7.5　基于改进萤火虫算法的子空间软聚类方法 MFARCM …… 170
7.5.1　经典萤火虫算法原理 …… 170
7.5.2　目标函数的改进 …… 171
7.5.3　萤火虫编码与算法的改进 …… 171
7.5.4　MFARCM 聚类算法的步骤 …… 172
7.5.5　算法实验与对比分析 …… 174
7.6　基于布谷鸟搜索的加权子空间软聚类算法 CSFW - SC …… 179
7.6.1　布谷鸟搜索算法及改进 …… 179
7.6.2　目标函数及学习规则 …… 180
7.6.3　CSFW - SC 算法流程 …… 182
7.6.4　参数设置 …… 183
7.6.5　性能分析 …… 185
7.7　基于 MFARCM 算法的风险要素分布特征获取实例 …… 186
7.7.1　风险要素数据聚类 …… 186
7.7.2　基于聚类结果的分布特征获取与分析 …… 187
7.7.3　风险要素分布特征获取应用实例 …… 189
参考文献 …… 197

第 8 章　信息系统安全防御决策 …… 200

8.1　引言 …… 200
8.2　决策与信息安全防御决策 …… 201
8.3　信息安全防御模型与技术 …… 204
8.3.1　安全防御模型 …… 204
8.3.2　安全防御技术 …… 207
8.4　信息安全主动防御 …… 210
8.4.1　主动防御的概念 …… 210

8.4.2 主动防御相关研究 …… 211
8.4.3 基于信息攻防博弈模型的主动防御决策 …… 214
8.5 信息安全防御决策数学描述 …… 215
8.6 基于完全信息静态攻防博弈模型的防御决策 …… 216
8.6.1 完全信息静态攻防博弈模型 …… 216
8.6.2 收益量化与计算方法 …… 217
8.6.3 最优防御策略选取方法 …… 220
8.6.4 应用实例 …… 223
8.7 基于静态贝叶斯攻防博弈模型的防御决策 …… 225
8.7.1 静态贝叶斯攻防博弈模型 …… 226
8.7.2 贝叶斯均衡分析和最优防御策略选取 …… 227
8.7.3 应用实例 …… 229
8.8 基于动态多阶段攻防信号博弈模型的防御决策 …… 233
8.8.1 动态多阶段攻防信号博弈模型 …… 234
8.8.2 攻防博弈均衡求解 …… 236
8.8.3 多阶段最优防御策略选取 …… 240
8.8.4 应用实例 …… 241
参考文献 …… 247

附录1 信息安全标准化组织 …… 251

附录2 国外信息安全管理标准 …… 254

附录3 我国信息安全管理标准 …… 272

附录4 国外信息安全风险评估标准 …… 275

附录5 我国信息安全风险评估标准 GB/T 20984—2007 …… 281

第1章 绪论

1.1 引 言

人类社会已经进入信息时代，信息不但成为社会生活的必需品，也成为国家的重要战略资源[1]。信息技术高速发展带来的深远影响和巨大改变，涉及人类生活和社会发展的各个方面。与此同时，随着网络攻击技术不断提高，信息安全形势日益严峻，信息安全问题已成为关系到国家安全、军事安全、社会稳定的重大问题。针对未来网络空间中信息攻击所具有的速度快、样式多、频次高、规模大、组合攻击和饱和攻击的特点[2]，围绕信息系统的攻防对抗日益激烈，信息系统面临的威胁与挑战不断加剧。继续沿用传统的安全管理模式，已经无法满足信息系统安全高效运行的需求。实施科学准确的安全风险评估，根据评估结果有针对性地进行风险管控和安全防御，成为确保信息系统安全的基础和保障。

依据信息技术安全评价准则(ITSEC)[3]，信息系统安全风险评估(Information Systems Security Risk Assessment)是指确定在计算机系统和网络中每一种资源缺失或遭到破坏对整个系统造成的预计损失，是对信息资产、威胁、脆弱性以及由此带来的风险大小的评估，简称安全风险评估。信息系统安全风险主要由三个要素决定：资产(Asset)、威胁(Threat)和脆弱性(Vulnerability)。其中：资产指有价值的信息或资源，包括各种设备、软件和数据；威胁是可能对信息系统的相关资产造成潜在损失的各种外部因素；脆弱性又称脆弱点、弱点或是漏洞，是资产中存在的并可以被威胁发现和利用的系统缺陷或弱点[3]。信息安全风险研究表明，威胁和脆弱性是相辅相成的，威胁是产生安全风险的外因和必要条件，脆弱性是内因和基本前提，而资产价值则是决定安全风险造成的预期损失大小的关键因素。如何实施系统、科学、合理的安全风险评估，进而制定相应的风险控制策略，使信息系统安全风险处于可控范围之内，是信息安全领域的重要问题和现实需求。根据 ISO/IEC 27002《信息安全风险管理指南》[4]和我国的 GB/T 20984—2009《信息系统风险评估规范》[5]，风险评估作为信息安全管理的关键环节和重要支撑，利用科学方法和

技术手段对信息系统所面临的威胁和脆弱性进行分析，据此对风险事件发生后可能会造成的系统损失进行评估和预测，有助于管理者掌握信息系统的风险状态和分布情况，并在此基础上为信息系统安全防御提供依据和建议，防范风险于未然，保障信息系统的安全。

对信息系统实施安全风险评估时，一般首先根据信息系统的拓扑结构和网络边界，将一个系统合理划分为多个独立的安全风险域；然后，对每个安全风险域进行威胁、脆弱性和资产三个风险要素的评估，得到安全风险域的风险要素向量；最后，对风险要素向量数据进行分析和研究，获取信息系统中不同强度安全风险的分布特征，揭示安全风险的空间分布规律和强度分布规律，为安全风险管理和安全防御决策提供辅助支持[6]。因此，安全风险评估技术的研究重点是风险要素评估技术和安全风险综合评估技术。

目前的安全风险要素评估技术和综合评估技术的研究已取得一些成果，但是随着安全风险评估的应用需求日益广泛，地位作用越来越重要，对安全风险评估的全面性、准确性和可信性等方面的要求不断提高，现有技术暴露出一些问题和不足，有待进一步深入研究。

（1）安全威胁评估是对信息系统面临的安全威胁的发生概率所进行的度量，当前敌对性恶意攻击成为威胁信息系统安全的主要来源和关键因素，已有的安全威胁评估技术一般从信息系统自身出发进行分析和研究，不考虑信息攻防的相关策略以及攻防对抗的结果，导致威胁评估在准确性和可信性上存在缺陷。

（2）脆弱性评估的主要内容包括漏洞危害评估和漏洞利用度评估，研究的重点和难点是漏洞危害评估，当前的漏洞危害评估技术缺乏对信息攻防双方相互制约关系的考虑，在全面性、准确性和操作性上存在不足。

（3）资产评估主要采取基于指标体系进行评估的方法，将信息资产按照指标体系分解成可量化评价的具体指标，在对指标量化赋值的基础上完成信息资产的综合评价，科学合理的指标体系是保证资产价值评估准确的前提和基础，但是目前资产评估指标体系构建与优化技术的可靠性和准确性存在不足，有待加强。

（4）安全风险综合评估的目的是定量描述安全风险要素在信息系统层次的分布特性和发展规律，目前的评估技术在分析大规模的风险域数据集时存在过程复杂、速度慢、可靠性不足等缺点，难以满足快速、准确、稳定地获取信息系统风险分布特征的要求。

在信息系统安全防御（风险控制）理论方面，目前人们研究了各种各样的措施、模型、技术和设备来加强安全防御能力，降低信息系统安全风险，尽量将风险控制在可以接受的范围之内。但是，日趋严重的信息安全事件仍然不断对信息系统安全造成巨大危害，而常见的防火墙、入侵检测和反病毒软件等典型安全防御技术，共同存在的问题是被动等待攻击，只能在攻击发生之后进行检测、发现、应对和补救，而此时往往已造成严重的损失。因此，迫切要求一种新技术，能在攻

击发生前对可能的攻击目标、危害、时空特性等进行分析和预测，进而实施主动防御。

本书一方面围绕资产、威胁、脆弱性风险要素的评估技术以及信息系统风险要素分布特征的发现技术开展研究，以提高安全风险评估的全面性、准确性、可信性，并为指导安全风险管控提供理论和技术支持；另一方面，针对网络攻防对抗中所具有的目标对立性、策略依存性和关系非合作性等基本特征，以博弈论为理论基础，采用攻防博弈模型研究网络安全分析和决策方法，为安全防御决策提供理论支撑。

下面首先介绍信息系统、信息系统安全风险、安全风险评估和防御决策等基本概念，为后续章节的详细讨论奠定必要的基础。

1.2 信息系统

信息系统是系统的一个大类，《大英百科全书》把它解释为："有目的、和谐地处理信息的主要工具，它对所有形态（原始数据、已分析的数据、知识和专家的经验）和所有形式（文字、视频和声音）的信息进行收集、组织、存储、处理和显示。"对信息系统的理解有广义和狭义之分：广义理解的信息系统涵盖范围很广，各种处理信息的系统都可算做信息系统，包括人体本身和各种社会系统；狭义理解的信息系统仅指基于计算机的系统，是人、规程、数据库、硬件和软件等各种设施、工具和运行环境的有机结合，它突出计算机和网络通信等技术的应用。就本书而言，我们将信息系统主要限制在后一种理解的范畴。

信息系统除具备一般系统的基本特征和基本要素外，还具备以下一些具体功能：

（1）信息采集功能。把分布在各处、各点的有关信息收集起来，并将代表信息的各种数据按照一定的协议转化成信息系统所需要的格式。

（2）信息处理功能。对进入信息系统的数据进行加工处理，包括排序、归并、查询、统计、预测、模拟等各种数学运算。

（3）信息存储功能。数据被采集进入信息系统之后，经过加工处理，形成对管理有用的信息，然后由信息系统负责对这些信息进行存储保管。对规模庞大的复杂信息系统，需要存储的数据量是很大的，这就要依靠先进的海量存储及其管理技术。

（4）信息管理功能。通常情况下，系统中要处理和存储的数据量是很大的，盲目采集和存储，不仅会产生存储灾难，还会使系统变成数据垃圾箱，因此必须加强管理。信息管理的内容包括：规定应采集的数据种类、名称、代码等；规定应存数据的存储介质、逻辑组织方式等。

（5）信息检索功能。存储在各种介质上的庞大数据要让使用者便于查询。