信息系统安全风险估计与控制理论

王祯学　周安民　方　勇　欧晓聪　著

科学出版社

信息系统安全风险估计与控制理论

王祯学　周安民
方　勇　欧晓聪　著

科学出版社
北京

内 容 简 介

本书将信息论、系统论、控制论以及博弈论的基本思想和方法综合应用于研究信息系统安全风险的识别与分析、评估与控制、信息对抗等问题上，从跨学科研究的角度出发，采用定性分析和定量分析相结合的方法，得到一系列新的理论研究成果，对信息安全的学科建设和工程实践都很有学术参考价值.

本书可以作为高等院校信息安全、计算机应用、网络通信、电子工程等专业高年级大学生和研究生的教材，也可供广大科技工作者参考.

图书在版编目(CIP)数据

信息系统安全风险估计与控制理论/王祯学等著. —北京：科学出版社，2011.6

ISBN 978-7-03-031049-1

Ⅰ.①信… Ⅱ ①王… Ⅲ ①信息系统-安全技术-风险分析 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字 (2011) 第 086445 号

责任编辑：王丽平 卜 新 / 责任校对：陈玉凤
责任印制：钱玉芬 / 封面设计：耕者设计工作室

科学出版社出版
北京东黄城根北街 16 号
邮政编码 100717
http //www sciencep com

漳浦印刷有限责任公司印刷

科学出版社发行 各地新华书店经销
*
2011 年 6 月第 一 版 开本 B5(720×1000)
2011 年 6 月第一次印刷 印张 11 1/2
印数 1—2 500 字数 215 000

定价：45.00 元

(如有印装质量问题，我社负责调换)

序

四川大学信息安全研究所是国内最早成立的信息安全专业研究机构之一. 长期以来, 在信息安全体系结构、信息系统安全风险的估计与控制、信息对抗等方面开展了深入的研究, 积累了丰富的理论和实践经验. 该书作者团队结合多年的科研与教学方面的实践, 站在系统论、控制论的高度, 综合应用信息论、系统论、控制论、博弈论的基本思想和方法, 从分析信息系统构成要素和信息资产面临的安全风险入手, 讨论信息系统安全风险的识别、估计、控制与信息对抗等问题. 从跨学科研究的角度出发, 采用定性分析和定量分析相结合的方法, 得到了一系列新的理论研究成果, 对信息安全的学科建设和工程实践都有学术参考价值.

我认为, 该书是近年来难得的一部系统性研究信息系统安全风险的专著, 对信息安全学科建设, 对更全面系统地提高信息安全理论和工程实践能力, 都有一定的指导意义和启发作用.

何德全

2010 年 10 月 16 日

前　言

信息安全是一门新兴交叉学科, 它与计算机科学、网络通信、数学科学、信息科学、系统科学、控制论、管理科学、法学等学科紧密相关. 通过不同学科的交叉融合, 伴随网络信息化的迅速发展, 信息安全科学工作者应该开展持续深入的跨学科研究, 逐步形成信息安全所特有的、独立完整的科学理论体系. 这无疑是一件非常重要的工作, 也是一项艰苦的工作, 有一段很长很长的路要走.

托马斯 · 库恩 (Thomas S. Kuhn) 一再强调, 一本好的教科书对于表达一门科学范式的重要性. 他说:"一种新理论总是同它的应用一起进入教科书, 未来的工作者即由此而学到他们的专业. 这个过程一直贯穿到从大学一年级到通过博士论文."“有了一本教科书, 科学工作者就可以从教科书达不到的地方开始研究, 从而可以高度集中到科学界所关心的最微妙、最深奥的自然现象."本书书名叫做“信息系统安全风险估计与控制理论", 主要结合四川大学信息安全研究所在科研与教学方面的实践, 力图将信息论、系统论、控制论、博弈论等相关学科的基本思想和方法用在研究信息系统安全风险的分析与评估、风险控制、信息对抗等问题上, 基本内容都是近年来作者团队对信息安全领域研究成果和教学实践的归纳、总结, 希望能帮助读者引发一些新的思路, 能对信息安全的理论研究或工程实践具有一定的指导意义或启发作用.

全书共 8 章. 第 1 章在回顾国内外有关信息系统安全结构理论体系的研究历史与发展现状的基础上, 首先就信息与信息系统, 信息系统的基本特征、基本要素、基本功能, 风险的基本内涵及一般性定义, 信息系统的风险及风险要素关系, 安全风险分析与评估等内容予以介绍, 然后从系统论、控制论的角度给出信息系统风险评估与控制模型结构, 用系统理论方法研究信息系统风险评估与控制时应该注意的事项, 为后续问题的进一步讨论提供理论框架及方法论基础. 第 2 章首先讨论信息系统构成要素及基于信息流保护的资源分布模型, 以此为基础详细阐述信息系统的风险识别与分析问题, 为安全风险的综合评估和风险控制 (安全保护) 提供科学依据与前提条件. 第 3 章在基于信息流保护的资源分布模型的基础上, 以安全风险为描述变量, 进一步讨论信息系统数学描述与结构分析问题, 包括基于时空坐标系的数学描述和基于网络拓扑结构的数学描述等, 进而对信息系统的可控性与可观测性等结构特性作具体描述与分析, 为进一步讨论安全风险的动态估计、状态控制以及攻防控制等问题奠定必备的基础. 第 4 章讨论信息系统安全风险的状态重构与动态估计问题. 以状态模型为基础, 借助控制系统理论中的观测器理论和 Kalman

滤波理论, 分别解决确定性情况下的风险状态重构和随机情况下的风险状态估计问题, 从而获得信息系统安全风险的时间分布特性, 为安全风险的动态综合评估或实时控制提供依据. 第 5 章讨论信息系统安全风险的静态综合评估, 讨论各资产要素风险对系统各风险域及系统整体风险的影响问题. 包括导出安全风险的静态综合评估准则、建立随机情况下的资产要素风险概率模型、定义风险熵以揭示安全风险递增规律等内容, 从“微观”、“中观”、“宏观”等不同角度为综合评价信息系统的安全风险提供理论和方法. 第 6 章讨论信息系统安全风险的动态综合评估, 即讨论各资产要素安全风险及系统整体安全风险随时间变化而变化的规律问题. 包括通过定义“风险强度”以建立信息资产安全风险的动态评估模型、通过定义“安全熵”以揭示信息系统安全性递减规律以及安全工作时间的计算方法等. 第 7 章讨论信息系统安全风险的状态控制与耗费成本问题. 首先介绍最优化与极大值原理的基本概念, 其次讨论基于线性二次模型的信息系统风险控制、基于概率模型的信息系统风险控制、基于 Logistic 模型的信息系统攻防控制等, 最后讨论风险控制与耗费成本之间的关系, 为信息系统风险控制 (安全保护) 的工程设计提供理论依据. 第 8 章讨论基于博弈论的信息系统攻防控制. 根据攻防竞争与对抗的特点, 首先将信息系统的攻防控制问题归结为围绕信息资产安全风险的策略博弈问题, 然后借助矩阵博弈和 Nash 均衡的基本原理和方法构建针对目标信息系统的攻防博弈模型, 导出相应的算法, 并举例说明模型及方法的应用.

在此感谢四川大学特聘教授、中国工程院何德全院士, 沈昌祥院士和周仲义院士的积极鼓励、支持和帮助, 感谢四川大学信息安全研究所的老师和研究生为本书的出版所做的有益工作, 感谢四川大学校长谢和平院士的关心和支持.

本书所涉及的内容大都具有尝试性和探索性, 与此相关的许多理论和实际问题还需要进一步深入研究, 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, 恳切地希望得到读者的批评和帮助.

作　者

2010 年 6 月于四川大学

目　　录

第1章 绪 论

1.1 引 言

人类进入信息社会, 网络信息系统无处不在, 无时不有, 各行各业及人们的日常工作和生活都依赖于信息网络, 离不开信息网络. 人们利用信息网络进行生产、生活、交流和管理等过程活动. 在这些过程活动中, 信息网络作为载体或工具表达人 (自然人、法人、利益集团等) 的意志或感情, 或交流有价值的资产, 或发出指令实施指挥和管理, 或与敌对势力和武装集团对抗, 从而保护人类社会的正常生活与生产秩序, 保障国家对社会秩序的管理和对社会状态的控制, 保障国家主权和领土完整, 改善或提高人类的整体素质和生活质量, 促进人类社会的交流和进步. 然而, 信息网络的开放互联性及信息系统组件 (硬件和软件) 本身固有的脆弱性和设计的缺陷给信息系统的安全与管理带来极大的困难, 给信息的传输、存储和使用带来潜在的安全风险. 如何正确地识别、估计和评价信息系统客观存在的安全风险, 进而预防和控制风险事件的发生, 从安全角度保障网络信息系统正常、有序和持续运行, 合理地利用现有资源以获取最大的社会经济效益, 这始终是信息系统面临的重大研究课题.

伴随着互联网技术的快速发展与普及, 国内外关于信息系统安全体系结构理论与技术的研究已有 20 多年的历史, 信息安全的内涵不断延伸, 从最初通信信息的保密性发展到网络化信息的完整性、可用性、可控性、可审查性等诸多方面, 取得一系列的理论与技术研究成果.

1985 年美国国防部为适应军事计算机的保密需要制定了可信计算机系统安全评估准则 (TCSEC, 从橘皮书到彩虹系列)[1], 它是计算机信息系统安全评估的第一个正式标准. 其后对网络系统、数据库等方面做出系列安全解释, 形成了信息系统安全体系结构的最早原则. 至今美国已研制出达到 TCSEC 要求的安全系统 (包括安全操作系统、安全数据库、安全网络部件)100 多种. TCSEC 标准把系统的保密性作为讨论的重点, 忽略了信息的完整性和可用性等安全属性, 因而这些系统仍有相当大的局限性, 同时也没有真正达到形式化描述和证明的可信水平.

20 世纪 90 年代初, 欧洲四国法、英、荷、德针对 TCSEC 只考虑保密性的局限性, 联合提出了包括信息安全的机密性、完整性、可用性等安全属性概念的“信息技术安全评价准则” (ITSEC, 欧洲白皮书)[2]. ITSEC 把可信计算机的概念提高

到可信信息技术的高度来认识, 对国际信息安全的理论研究和技术实施产生了深刻的影响. 但是该标准也同样没有给出形式化描述的理论证明.

1996 年, 美、加、英、法、德、荷六个国家联合提出了信息技术安全评估的通用准则 (common criteria, CC)[3], 并逐渐形成国际标准 ISO15408[4,5,6]. 该标准定义了评价信息技术产品和系统安全性基本准则, 提出了目前国际上公认的表述信息技术安全性的体系结构, 即把安全要求分为规范产品和系统安全行为的功能要求, 以及如何正确有效地实施这些功能的保证要求. CC 标准是第一个信息技术安全评价的国际准则, 它的发布对信息安全具有重要意义, 是信息技术安全评价标准以及信息安全技术发展的一个重要里程碑. 但 CC 评价标准是针对产品和系统的安全性测试及等级评估, 事先假定用户知道安全需求, 忽略了对信息系统的风险分析, 缺少综合解决保障信息系统多种安全属性的理论模型依据.

2000 年, 国际标准化组织 (ISO) 在英国提出的信息安全管理标准 (BS7799) 的基础上 [7,8], 制定并通过了信息安全管理指南 ISO/IEC 17799[9], 采用系统工程方法确定安全管理的方针和范围, 在风险评估的基础上选择适宜的控制目标与控制方式, 制定业务持续性计划, 建立并实施信息安全管理体系. 但 ISO/IEC 17799(或 BS7799) 的目的并不是告诉使用者有关“怎么做”的细节, 它所阐述的主题是安全策略和具有普遍意义的安全操作, 它讨论的主题很广泛但每一项内容的讨论都没有深入下去, 没有提供关于任何安全主题的确定或专门的材料, 也没有提供足够的信息以帮助机构进行深入的安全检查.

1996 年 12 月开始发布的 ISO13335 系列标准 [10,11,12,13], 提出了关于信息技术安全的机密性、完整性、可用性、审计性、真实性、可靠性等 6 个方面的含义, 并提出了基于风险管理的安全模型. 该模型阐述了信息安全评估的基本思路, 对信息系统安全风险的评估工作具有指导意义.

2000 年 9 月, 美国国家安全局为了促进美国政府信息系统安全需求的协调, 在“工业界/政府联合信息保障技术框架”的基础上推出了《信息保障技术框架》(IATF): 3.0 版 [14]. IATF 定义了对一个系统进行信息保障的过程以及该系统中硬件和软件部件的安全需求, 提出了多层防护原则, 称之为“纵深保卫战略” (Defense-in-Depth Strategy). 纵深保卫战略的四个主要技术焦点分别为: 保卫网络和基础设施、保卫边界、保卫计算环境以及为基础设施提供支持. IATF 得到了广泛的采纳和应用, 美国国防部 (DOD) 的《全球信息网 (GIG)IA 政策和实施指南》就是围绕纵深保卫战略而建的, 它把 IATF 作为技术解决方案的信息源以及国防部 IA 实施的指南. 虽然 IATF 提出了纵深保卫战略的概念, 并围绕该概念对信息系统进行建设和保护, 但仅起到对安全需求的协调和安全解决方案的建议作用, 并没有描述如何对一个信息系统提供完整安全解决方案的技术框架和技术路线.

在国内, 由于信息安全技术及体系结构的研究滞后于信息技术应用和产业的发

展, 国内主要是等同采用国际标准. 例如,《信息技术　安全技术　信息技术安全性评估准则》(GB/T 18336—2001)[15~17] 就是等同采用 ISO/IEC 15408：1999. 另外, 由公安部主持制定、国家技术监督局发布的《计算机信息系统安全保护等级划分准则》(GB 17859—1999) 将计算机系统安全保护能力分为五个等级：用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级. 主要的安全考核指标有身份验证、自主访控制、数据完整性、审计等, 这些指标涵盖了不同级别的安全要求 [18]. 但这个标准的基本思想未能在根本上突破 TCSEC 架构, 同时缺乏可操作性.

2007 年正式发布并实施的 GB/T 20984—2007《信息安全技术　信息安全风险评估规范》, 作为中华人民共和国国家标准 [19], 给出了信息系统安全风险评估的基本概念、要素关系、分析原理、实施流程和评估方法以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式, 具有较强的可操作性. 标准在资产识别和分类的基础上, 按照机密性、完整性和可用性三个安全属性的达成程度对资产进行赋值, 并依据赋值大小划分资产重要性等级; 对资产面临的威胁状况和存在的脆弱性程度进行识别并赋值; 根据威胁出现的频率和资产脆弱性程度计算安全事件发生的可能性; 根据资产价值和资产脆弱性程度计算安全事件发生造成的损失; 根据安全事件发生的可能性和安全事件发生造成的损失计算资产的风险值, 并进行等级化处理. 但该标准给出的安全风险评估流程、评估方法和评估结果都是针对各信息资产而言的, 缺乏对信息系统各风险域及系统整体风险的描述与评价.

从国内外研究现状可以看出, 迄今为止的信息安全评估标准虽然都强调了风险评估的必要性和重要性, 都要求以信息系统安全风险的分析为核心, 通过评估系统或产品的安全属性来判断系统或产品的安全等级是否符合要求, 但这些标准所采用的方法一般都是通过问卷式的调查访谈给出不同风险域在安全管理方面存在的漏洞和各领域的安全等级, 最后给出策略建议. 这至少在以下三个方面存在问题或不足：一是对于信息系统安全风险分布规律的认识大多停留在专业人员或专家的个人经验上, 因而缺乏系统性和客观性; 二是在风险评估的量化及评价方面普遍缺乏可操作的工程数学方法, 导致评估结果在系统性和客观性方面存在较大的主观偏好; 三是对信息系统安全风险的时空分布特性 (尤其是时间分布特性) 缺乏描述与分析, 因而无法解决安全风险的动态估计问题.

在安全保护 (风险控制) 方面, 迄今为止人们采取了各种各样的措施并研究了各种类型的系统或设备来堵塞系统的安全漏洞, 以降低安全风险, 尽力将风险控制在人们可接受的范围之内. 但所取得的成果都是局部性的或工程性的, 对信息系统安全保护 (风险控制) 过程中带有一般性的普遍意义的研究还很缺乏, 对信息系统所存在的安全风险、安全方案设计的优劣、风险评估与风险控制性能的评价等方面还缺乏科学严谨的评判理论与方法.

本书站在控制论或系统论的高度, 综合利用信息论、控制论、系统论 (包括复杂系统理论) 的基本思想和方法, 从分析信息系统构成要素和资产所面临的安全风险入手, 用定性和定量分析相结合的方法, 首先建立信息系统风险评估与控制的模型结构, 以此为基础, 给出“基于信息流保护的资源分布模型”, 进而对信息资产、资产的脆弱性和面临的威胁进行识别与分析, 并给出信息资产安全风险的计算方法; 然后讨论描述信息系统安全风险的数学模型, 给出基于模型的风险状态观测和风险状态估计方法; 接着介绍信息系统安全风险的综合描述与评价方法; 最后用较大篇幅讨论信息系统安全风险控制的理论与方法问题, 包括“信息系统安全风险的状态控制”、“信息系统风险控制与耗费成本”、“基于 Logistic 模型的信息系统攻防控制”、“基于博弈论的信息系统攻防控制”等内容.

作为绪论, 接下来就信息与信息系统、信息系统的安全风险、安全风险的分析与评估、风险控制与风险控制系统等基本概念首先予以介绍, 为后面各章的详细讨论奠定必备的基础.

1.2　信息与信息系统

1.2.1　信息的基本概念

人们之所以把现代社会称为信息社会, 是因为信息与物质和能量一样, 已经成为人类生存和社会发展的必要条件之一 [20]. 那么信息是什么呢? 简单地说, 信息是物质的一种固有属性, 它来源于物质的运动, 是物质运动状态和运动方式的表征. 信息与物质和能量有着密不可分的关系: 没有物质、没有物质的运动, 就没有信息, 但信息不等同于物质, 信息不是物质本身, 它只是反映物质的运动状态和方式; 同时, 没有能量, 物质就不能运动, 当然也就没有信息, 但信息也不等同于能量, 能量是物质运动的原因, 信息是物质运动的结果. 物质、能量、信息是人类社会发展和进步的三大基本要素.

此外, 物质和能量受到空间和时间的限制, 但是信息原则上可以延伸和拓展到无限的空间和时间. 物质和能量只存在于客观世界, 但信息除了客观存在以外还接受主观世界的影响, 例如信息的内涵与感知者的理解、思维能力、偏好、判断水平等因素有关. 信息可分为狭义和广义两类: 狭义信息又称为客观信息, 它以概率统计为基础, 用信息的量度、传输速率、信息容量等来衡量; 广义信息又称为有效信息, 它在统计信息的基础上, 进一步考虑信息的逻辑含义和实效内容, 并用平均效用度来衡量.

要进一步理解信息的特征与内涵, 还必须弄清楚“消息”的基本概念, 以及消息和信息的区别和内在联系. 消息是人们熟知的概念, 比如在电报通信中电文是消

息, 在电话通信中话音是消息, 在电视中画面图像是消息, 在遥控和遥测中一些测量数据和指令也是消息, 等等. 很明显, 各种消息在物理特征上极不相同, 各种消息的组成亦不可能相同, 但它们有一个共同的特点, 即消息的随机性. 发信端在发送消息时可以随心所欲地发出这样或那样的序列和过程, 收信端在收到消息之前是无法预测的, 亦即消息的出现是随机的、不确定的. 在信息系统内传递的消息本身无法量度, 但其不确定性是可以量度的. 因此, 人们又引用信息的概念来量度消息的不确定性, 即"信息"是消息不确定性程度的测度.

传递信息是通信的目的, 每一条消息都包含着一定的信息量, 而信息量的大小与消息发生的概率有着密切的关系. 比如, 某人告诉我们一条非常可能发生的消息, 比起告诉我们一条不太可能发生的消息来说, 所传递的信息量就比较少. 因此, 消息发生的概率可以作为人们预期程度的度量单位, 它和信息量大小有关. 也就是说, 在信息度量中最基本的就是不确定性的概念, 即消息的内容越是不能确定, 则消息所包含的信息量就越大. 如果我们能够预测给定消息的内容, 那就没有传递什么新的信息, 即信息量很少, 甚至等于零.

综上所述, 消息是信息传输的具体对象, 而信息是抽象化的消息; 消息中包含信息的量度是基于消息出现的概率, 并且信息量的大小和消息发生的概率有着相反的关系. 如果消息是确定的 (即发生概率为 1), 那么它包含的信息量为零; 如果消息是完全不可能的 (即发生的概率为 0), 那么它包含着无穷的信息量. 因此, 信息量可以用消息发生概率倒数的某个函数来表示. 在信息论中, 信息的科学定义为

$$I = \log \frac{1}{p} = -\log\ p \tag{1.1}$$

式中, p 为消息发生的概率, 也称为先验概率; I 为从消息发生中能够得到的信息量; log 表示对数. 对数的底决定着量度信息的单位: 若取 2 为底, 则 I 的单位为二进制单位, 即比特 (bit); 若取 e 为底, 则 I 的单位为自然单位, 即奈特 (nit). 在信息通信中通常取 2 为底, 它的单位是比特. 例如, 传输一个以等概率出现的二进制码元 (0 或 1), 接收端所获得的信息量就为 1bit, 即当 $p(0) = p(1) = \dfrac{1}{2}$ 时, 有

$$I(0) = I(1) = -\log_2 \frac{1}{2} = 1(\text{bit})$$

1.2.2 系统的基本概念

控制论的奠基人 Rorbert Wiener 把控制论定义为"通信和控制的科学"[21], 按照控制论 (cybernetics) 一词的原意, 有人又把它称为"掌舵术"的学问. 要讨论的主要问题是: 指挥、协调、调节、稳定、反馈、控制等等, 而这些问题的讨论, 离不开系统的基本概念.

系统一词是人们所熟知的, 它是一个广义的概念, 有各种不同的定义方法, 本书从系统的基本特征出发, 给出一个直观的定义.

定义 1.1　系统是特定命题和制束条件下有组织体制的通称.

注意上述定义中的"特定命题"、"制束条件"、"有组织体制"几个关键词. 所谓特定命题, 是指为了达到某些特定的目的而确定的研究对象; 所谓制束条件, 是指组成系统的各元素 (元部件) 之间互有关联, 并按一定的规则相互连接; 所谓有组织体制, 是指组成系统的各单元之间的关系要服从整体的要求, 各单元与系统之间的关系也要服从整体的要求, 以整体的观念来协调系统的诸单元. 可见, 能够称之为系统的研究对象至少必须具备以下基本特征:

(1) 目的性. 例如, 研究开放互联网络环境下的信息系统, 目的是什么呢? 首先当然是信息通信和信息共享, 这就是命题, 也就是目的. 在这个命题下去研究信息系统的通信性能和互联互通规则, 如网络传输延迟、路由选择的转发指数、网络容量、网络协议等. 其次是在保证信息通信和信息共享的同时, 还必须保证信息的安全. 在信息通信和信息共享的过程中保证信息安全, 这也是命题, 也是目的. 从这个命题去研究信息系统的安全风险特性, 如信息资产的脆弱性和可能受到的威胁以及由此引发的安全事件发生的可能性和安全事件造成的损失等.

(2) 相关性. 组成系统的各元素 (元部件) 之间要相互联系, 相互作用; 互联要按一定的规则, 即受到一定的约束. 显然, 信息系统必须由客体 (计算机网络)、主体 (管理者和使用者) 和运行环境 (客体和主体共存的物理空间、逻辑空间及保障条件) 三大要素按事先设计好的网络拓扑结构图和管理规则连接组成. 若只有以上三大要素而不按网络拓扑结构图和管理规则连接, 或者缺少其中必需要素而添上别的要素, 都构不成信息系统.

(3) 整体性. 无论是选择各元素 (元部件) 的参数, 还是协调各单元之间的关系以及各单元和整体之间的关系, 都要从整体的观念出发, 服从整体的要求.

(4) 相对性. 通常, 人们把系统看成是比元部件更复杂、规模更大的组成体, 但这是不确切的. 因为实际上很难从复杂程度和规模的大小来确切区分什么是元部件, 什么是系统. 例如, 一个双稳态触发器, 作为记忆和信息处理系统, 它由两只晶体管和几只电阻、电容构成; 但在一个运算或控制系统里, 这个双稳态触发器就退居为一个逻辑单元, 这个运算或控制系统在一台复杂的计算机中只能算一个部件. 在一个规模不大的局域网系统中, 一台计算机只能算一个设备单元. 所以系统的概念具有明显的相对性, 与我们要讨论的命题和要达到的目的紧密相关, 而不是从简单或复杂程度来区分什么是元部件, 什么是系统.

此外, 系统具有输出某种产物或信息的功能, 但它不能无中生有. 也就是说, 对输出必须要有输入经过处理才能得到. 输出是处理的结果, 代表系统的目的; 处理是输入变成输出的一种加工, 由系统本身担任. 因此, **输入**、**处理**、**输出**, 是系统的

三个基本要素.

以上所述系统的四个基本特征和三个基本要素决定着系统的基本结构、层次与功能. 不同的系统具有不同的层次结构和功能. 一个系统如果是多层次的、结构是非线性的、其运动状态具有不确定性和不可逆性, 那么这样的系统被称为复杂系统 [22,23], 否则称为简单系统. 但要注意, 一个系统究竟是简单还是复杂, 与要研究的"命题"即要达到的目的紧密相关. 例如, 对同样的网络信息系统, 有两个研究命题 ——"风险评估"和"网络舆论", 显然后者比前者复杂. "风险评估"在适当条件下可作简单系统处理, 而"网络舆论"必须作为复杂系统来研究.

1.2.3 信息系统的基本概念

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 [24]. 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之外, 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格式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、分类、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; 规定应存储数据的存储介质、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.

(6) 信息传输功能. 从采集点上采集到的数据要传送到处理中心进行加工处理, 加工处理后的信息要送到使用者手中或管理者指定的地点, 各类用户要使用存储在中心或指定地点的数据信息等, 这些都涉及信息传输的问题. 系统的规模越大, 信