信息系统安全系列

信息系统安全

● 戴宗坤　罗万伯　等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

信息系统安全系列

信息系统安全

戴宗坤　罗万伯　等编著

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

内 容 简 介

本书从人、网络和运行环境结合的角度，将利用开放系统互连技术构成的信息系统的安全问题作为一个体系进行描述，突破了此前单纯从一个或几个方面阐述信息系统安全问题的传统思维模式。本书信息量极大，涉及信息系统及其与安全问题相关的多学科领域的基础知识和技术方法。本书内容主要包括信息安全机制、信息安全服务和信息安全管理在开放互连运行环境下如何构成信息系统安全体系的基本原理、方法和策略。

本书内容全面、文字流畅、表达准确，既可作为高等院校信息安全相关专业的本科生、研究生的教材或指定参考书，也可供从事信息系统及其与安全有关的教学人员、科研人员、工程技术人员以及信息技术管理人员参考。

图书在版编目(CIP)数据

信息系统安全/戴宗坤等编著 .—北京：电子工业出版社，2002.11
(信息系统安全系列)
ISBN 7-5053-8089-3

Ⅰ.信… Ⅱ.戴… Ⅲ.信息系统—安全技术 Ⅳ.G202

中国版本图书馆 CIP 数据核字(2002)第 084428 号

责任编辑：刘宪兰　章海涛　　特约编辑：明足群
印　　刷：北京东光印刷厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：31.5　字数：789.4 千字
版　　次：2002 年 11 月第 1 版　2002 年 11 月第 1 次印刷
印　　数：5 000 册　定价：39.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：(010)68279077

前　言

本书是四川大学信息安全研究所为信息安全工程专业本科生和研究生教学而组织编写的两本专业课教材之一。这两本专业课教材是《信息系统安全》和《信息系统安全工程》。前者重点给出信息系统安全的基础理论背景知识、安全体系结构、支持安全体系的安全服务框架及其机制性技术以及信息系统安全测试评估的体系及基本知识;后者着重从系统工程方法切入,对信息系统安全工程生命期各阶段的准备、实施、过程监控及反馈、调整进行系统描述。可以说,这两本书互为姐妹篇。

本书由三个板块和附录构成。第1、2、3章是第一板块,从信息、信息技术、信息系统和信息系统安全的层次结构,引出信息系统安全的有关问题,且从网络基础知识、信息系统风险控制点及其对抗措施梗概,安全工程方法论方面为第二板块进行必要的准备和铺垫。第二板块包括第4、5、6、7和8章,比较完整和系统地从信息系统安全体系的构建方法,一直到安全框架以及安全机制进行较为详细的研究,目的是为读者给出信息系统安全体系的架构及支持技术。其中,防病毒技术也纳入这一板块。第三板块由第9、10、11章组成,着重从管理角度研究信息系统的安全问题,管理的内容涉及法律、法规、规章制度,有关技术管理内容分别纳入第三板块中的相应章节和段落中,而信息系统安全相关的测试和评估方法也放在这一板块中。其中附录C(共27个子附录)和附录D是对正文的必要补充,有云南安全框架和安全服务机制的深入理解。全书涉及的内容十分广泛,对于本科生、研究生的学习,可在内容、重点和深度方面根据教学大纲要求进行选择。

本书由四川大学信息安全研究所组织编写,戴宗坤、关义章、罗万伯、蒋继洪、刘永澄、唐三平参与结构设计。唐三平主笔撰写第2.3节,第4.1.2小节和第5.8节,以及第7章;刘永澄主笔撰写第2章(第2.3节除外);黄元飞主笔撰写第3章、第10章和附录D;罗万伯主笔撰写第8章、第9章和第11章;戴宗坤主笔撰写第1章、第4章(第4.1.2小节除外)、第5章(第5.8节除外)、第6章和附录C;附录A和B由李智编写;全书由戴宗坤统稿,罗万伯协助。戴宗坤、罗万伯、唐三平、黄元飞、刘永澄、李智、王殿志、卢金树、付渝、杜义飞、戴云燕等参与资料收集和整理工作;戴云燕、宋敦琪、潘静、杨丽颖等参与部分文字录入和校订工作。

本书从策划到编写完成,一直得到中国工程院院士何德全教授的热情鼓励和指导,以及吴世忠、罗建中研究员的大力支持。四川大学信息安全研究所全体同志为本书的完成提供了优越的工作环境和多方面的帮助;同时从其他各位老师和同行的著作(包括网站)中也得到了帮助。作者在此一并表示衷心的感谢。

由于书稿涉及许多新内容和研究课题,尽管作者尽了最大努力,囿于作者的学识和水平,仍自感问题难免。诚望读者不吝赐教斧正,以利再版修订,至臻完善,为推动我国信息系统安全工程高级技术人才的培养共同出力。

作　者

四川大学信息安全研究所

目　录

第1章 概 论

1946年，世界上第一台真正的电子计算机ENIAC在美国宾夕法尼亚州立大学诞生，信息技术的发展进入一个新阶段。自那以后，人类处于一个大变革的时代，作为社会发展三要素的物质、能源和信息的关系发生了深刻的变化。此前处于从属地位和起隐性作用的信息要素，终于在计算机技术和网络通信技术的推动下，迅速成为支配人类社会发展进程的决定性力量之一。人类开始从主要依赖物质和能源的社会步入物质、能源和信息资源三位一体的社会。在这种宏观背景下，首先是一些发达国家掀起了以发展信息科技、开发利用信息资源来促进社会、经济和文化进步的浪潮，从而启动了从工业化社会迈向信息化社会的进程。

纵观20世纪特别是后半叶的信息技术发展历史，从20世纪40年代以前的电话、电报、无线电广播和通信等，到电子管、晶体管、集成电路、激光、计算机、卫星通信、移动通信、局域网、广域网、因特网和虚拟现实技术等，差不多每十年就有与信息技术有关的、影响深远的重大创新和技术成就出现。近一二十年来，微电子技术和激光技术的发展，推动了大规模、超大规模集成电路和超大容量存储介质的发展和应用，信息处理设备呈现体积小型化、微型化和功能集成化、人性化的趋势；与此同时，通信技术和通信协议的发展推动了信息的高速传输和信息资源的广泛共享。信息技术的发展和应用加快了各种新技术、新知识、新文化的传播，深入到社会、政治、军事、经济、文化、医疗、社会保障、交通、通信、商务、生产、学习、交流和日常生活等各个领域和方面，深刻地影响着社会各阶层、各团体、每个人以及各个政体、国家自身内部以及相互之间关系的思维方式、行为方式和观念的变化。

以计算机及其外围设备为信息处理中心，以计算机网络作为信息传播平台，以有线和无线介质作为信息传输媒体的信息系统，正在进入人类社会的各个领域。现在，没有人怀疑计算机信息系统的应用价值和意义，因为人们正在自觉和不自觉地接受计算机信息系统“替我们干什么”和“要我们干什么”这一现实，并且根据自己对信息技术的理解“体会到”和“感知到”计算机信息系统在“迫使”人们改变传统的思维模式和行为方式。也许，不是所有的人能说清楚“功能如此强大的计算机信息（系统）技术一定于我有益”，但是几乎所有人都会感受到一种无形的巨大推力，让你去认识它、理解它，即使不情愿，将来也得“顺从它”。这就是潮流。

那么，信息、信息技术和信息系统到底是什么呢？如何最大限度地利用信息系统为我们“创造价值”，为我们服务而不招致损失或使损失最小呢？本章力图为其给出比较系统的基础性概念和理论知识。

1.1 信息的概念及其他

“信息”一词古已有之。在人类社会早期的日常生活中，人们对信息的认识比较广义而模糊，对信息和消息的含义没有明确界定。到了20世纪尤其是中期以后，现代信息技术的

飞速发展及其对人类社会的深刻影响，迫使人们开始探讨信息的准确含义。

一般意义上的信息定义认为，信息是事物运动的状态与方式。如果引入必要的约束条件，则可形成信息的概念体系。信息有许多独特的性质与功能，也可以进行测度。正因为如此，才导致信息科学的出现。

1.1.1　信息的经典定义

1928 年，哈特雷（L.V.R.Hartley）在《贝尔系统电话杂志》上发表了题为《信息传输》的论文。他在文中将信息理解为选择通信符号的方式，且用“选择的自由度”来计量这种信息的大小。他注意到，任何通信系统的发信端总有一个字母表（或符号表），发信者发出信息的过程正是按照某种方式从这个符号表中选出一个特定符号序列的过程。假定这个符号表一共有 S 个不同的符号，发送信息选定的符号序列一共包含 N 个符号，那么，这个符号表中无疑有 S^N 种不同符号的选择方式，也可以形成 S^N 个长度为 N 的不同序列。这样，就可以把发信者产生信息的过程看做从 S^N 个不同的序列中选定一个特定序列的过程，或者说是排除其他序列的过程。

然而，用“选择的自由度”来定义信息存在着局限性，主要表现在：一方面，这样定义的信息没有涉及信息的内容和价值，也未考虑到信息的统计性质；另一方面，将信息理解为选择的方式，就必须有一个选择的主体作为限制条件。因此，这样的信息只是一种认识论意义上的信息。

1948 年，香农（C.E.Shannon）在《通信的数学理论》一文中，在信息的认识方面取得重大突破，堪称信息论的创始人。香农的贡献主要表现在推导信息测度的数学公式上，发明了编码的三大定理，为现代通信技术的发展奠定了理论基础。

香农发现，通信系统所处理的信息在本质上都是随机的，可以运用统计方法进行处理。他指出，“一个实际的消息是从可能的消息集合中选择出来的，而选择消息的发信者又是任意的，因此，这种选择就具有随机性”。这是一种大量重复发生的统计现象。

香农对信息的定义同样具有局限性，主要表现在：这一概念同样未能包含信息的内容与价值，只考虑了随机型的不定性，未能从根本上回答信息是什么的问题。

1948 年，就在香农创建信息论的同时，维纳（N.Wiener）出版了专著《控制论——动物和机器中的通信与控制问题》，并且创立了控制论。后来，人们常常将信息论、控制论以及系统论合称为“三论”，或统称为“系统科学”或“信息科学”。

维纳从控制论的角度认为，“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，同外部世界进行互相交换的内容的名称”。他还认为，“接收信息和使用信息的过程，就是适应外部世界环境的偶然性变化的过程，也是我们在这个环境中有效地生活的过程”。维纳的信息定义包含了信息的内容与价值，从动态的角度揭示了信息的功能与范围。但是，人们在与外部世界的相互作用过程中，同时也存在着物质与能量的交换，不加区别地将信息与物质、能量混同起来是不确切的，因而也有局限性。

1975 年，意大利学者朗高（G.Longo）在《信息论：新的趋势与未决问题》一书的序中指出，信息是反映事物的形成、关系和差别的东西，它包含在事物的差异之中，而不在事物本身。无疑，“有差异就是信息”的观点是正确的，但“没有差异就没有信息”的说法却不够确切。譬如，我们碰到两个长得一模一样的人，他（她）们之间没有什么差异，但会马上

联想到“双胞胎”这样的信息。可见，“信息就是差异”也有其局限性。

据不完全统计，信息的定义有 100 多种，它们都从不同侧面、不同层次揭示了信息的特征与性质，但也都有这样或那样的局限性。信息作为物质世界的三大组成要素之一，其定义的适用范围是非常宽的。上述几种经典定义也只适合特定范围或层次，是人们在探索信息的过程中所形成的几种含金量高的认识积淀。

1.1.2 与现代通信有关的信息定义

通信领域对信息的研究有着悠久的历史，信息科学的出现正是通信理论研究的最重要的成果之一。1988 年，中国学者钟义信在《信息科学原理》一书中，认为信息是事物运动的状态与方式，是事物的一种属性。信息不同于消息，消息只是信息的外壳，信息则是消息的内核。信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容。信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。信息不同于情报，情报通常是指秘密的、专门的、新颖的一类信息；可以说所有的情报都是信息，但不能说所有的信息都是情报。信息也不同于知识，知识是认识主体所表达的信息，是序化的信息，并非所有的信息都是知识。他还通过引入约束条件推导了信息的概念体系，对信息进行了完整而准确的论述。

通过比较，中国科学院文献情报中心孟广均研究员等在《信息资源管理导论》一书中认为，“作为与物质、能量同一层次的信息的定义，信息就是事物运动的状态与方式”。因为这个定义具有最大的普遍性，不仅涵盖所有其他的信息定义，而且通过引入约束条件还能转换为所有其他的信息定义。

1.1.3 信息的性质

信息来源于物质，不是物质本身；信息也来源于精神世界，又不限于精神的领域。信息归根到底是物质的普遍属性，是物质运动的状态与方式。信息的物质性决定了它的一般属性，它们主要包括普遍性、客观性、无限性、相对性、抽象性、依附性、动态性、异步性、共享性、可传递性、可变换性、可转化性和可伪性等。

信息系统安全将处理与信息依附性、动态性、异步性、共享性、可传递性、可变换性、可转化性和可伪性有关的问题。

1.1.4 信息的功能

信息的功能是信息属性的体现。相对于信息的本质属性和一般属性，信息的功能也可分为两个层次：信息的基本功能在于维持和强化世界的有序性；信息的社会功能则表现为维系社会的生存，促进人类文明的进步和人类自身的发展。信息的功能主要表现在下述 5 个方面。

① 信息是宇宙万物有序运行的内在依据。信息源于物质的运动，早在生命现象出现之前，自然界中无机物之间、无机物及其周围环境之间就存在着相互作用，存在着运动、变化的过程，因而也存在着信息的运动过程。可以说，缺少物质的世界是空虚的世界，缺少能量的世界是死寂的世界，缺少信息的世界则是混乱的世界。

② 信息是人类认识世界和改造世界的中介，在于实现人类与自然界的沟通。人类通过

自己的感觉器官，从物质世界中感知和提取信息；通过大脑的加工，以信息输出的形式作用于物质世界，达到改造的目的。信息始终是这个过程的中介和替代物。

③ 信息是社会生存与发展的动因。信息交流是人类社会活动赖以形成、维系和发展的根本保证。由于社会内部的信息交流，使后人可以在前人的肩膀上起步。因此，信息本身也是社会前进与发展的基石，是人类进化的动力。

④ 信息是智慧之源，是人类的精神食粮。人的思维和智慧是信息过程的产物，不能想像没有信息的生活。

⑤ 信息是管理的灵魂。管理一直是人类的一项经常性的社会活动，是一个有序化的过程。管理主体向管理客体传递信息、监督客体的运行状态，收集反馈信息，不断地做出调整，以保证目标的实现。管理最重要的职能之一是决策。决策就是选择，而选择意味着消除不确定性，意味着需要大量、准确、全面且及时的信息。

信息还是一种重要的社会资源。现代社会将信息、材料和能源看做支持社会发展的三大支柱，这说明了信息在现代社会中的重要性。

信息系统安全的任务是确保信息功能的正确实现。

1.2　信息技术

1.2.1　信息技术的产生和发展

任何技术都产生于人类社会实践活动的实际需要。按照辩证唯物主义观点，人类的一切活动都可以归结为认识世界和改造世界。人类认识世界和改造世界的过程，从信息的观点来分析，就是一个不断从外部世界的客体中获取信息，并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出，最终把大脑中产生的决策信息反作用于外部世界的过程。

“科学”是扩展人类各种器官功能的原理和规律，而“技术”则是扩展人类各种器官功能的具体方法和手段。从历史上看，人类在很长一段时间里，为了维持生存而一直采用优先发展自身体力功能的战略，因此材料科学与技术和能源科学与技术也相继发展起来。与此同时，人类的体力功能也日益加强。信息虽然重要，但在生产力和生产社会化程度不高的时候，人们仅凭自身的信息器官的能力，就足以满足当时认识世界和改造世界的需要了。随着生产斗争和科学实践活动的深度和广度的不断发展，人类的信息器官功能已明显滞后于行为器官的功能了。例如人类要“上天”、“入地”、“下海”、“探微”，但其视力、听力、大脑存储信息的容量、处理信息的速度和精度，越来越不能满足同自然作斗争的实际需要了。到了这个时候，人类才把关注的焦点转移到扩展和延长自己信息器官的功能方面。

从 20 世纪 40 年代起，人类在信息的获取、传输、存储、处理和检索等方面的技术与手段，以及利用信息进行决策、控制、指挥、组织和协调等方面的原理与方法，都取得了突破性的进展，且是综合性的。这些事实从侧面说明了当代技术发展的主流已经转向信息科学技术。

1.2.2 信息技术的内涵

对于信息技术，目前还没有一个准确而又通用的定义。为了研究和使用的方便，学术界、管理部门和产业界等都根据各自的需要与理解给出了自己的定义，估计有数十种之多。信息技术定义的多样化，不仅反映在语言、文字和表述方法的差异上，而且也有对信息技术本质属性理解方面的差异。

目前，比较有代表性的信息技术定义主要有以下6种：

① 信息技术是基于电子学的计算机技术和通信技术的结合而形成的对声音、图像、文字、数字和各种传感信号的信息进行获取、加工处理、存储、传播和使用的能动技术。

② 信息技术是指在计算机和通信技术支持下用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频以及语音信息，并且包括提供设备和信息服务两大方面的方法与设备的总称。

③ 信息技术是人类在生产斗争和科学实验中，认识自然和改造自然的过程中所积累起来的获取信息、传递信息、存储信息、处理信息以及使信息标准化的经验、知识、技能，以及体现这些经验、知识、技能的劳动资料有目的的结合过程。

④ 信息技术是在信息加工和处理过程中使用的科学、技术与工艺原理和管理技巧及其应用，以及与此相关的社会、经济与文化问题。

⑤ 信息技术是管理、开发和利用信息资源的有关方法、手段与操作程序的总称。

⑥ 信息技术是能够延长或扩展人的信息能力的手段和方法。

上述定义都试图从功能方面揭示信息技术的本质。从语法角度来看，“信息技术”作为专门术语，其概念的本质是“技术”而非“信息”。结合本书论述的对象和范围，我们将信息技术的内涵限定在上述第②种定义以内，即强调信息技术是获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频和语音信息，以及提供完成这些活动的信息设备和提供信息服务两大方面的方法与设备的总称。

1.3 信息系统

1.3.1 信息系统的基本内涵

与“信息”、“系统”的定义具有多样性一样，信息系统这种与“信息”有关的“系统”，其定义也远未达成共识。比较流行的看法有以下4种。

《大英百科全书》把“信息系统”解释为“有目的、和谐地处理信息的主要工具是信息系统，它对所有形态（原始数据、已分析的数据、知识和专家经验）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”。

巴克兰德（M.Buckland）认为，信息系统是“提供信息服务，使人们获取信息的系统，如管理信息服务、联机数据库、记录管理、档案馆、图书馆、博物馆等”。

达菲（N.M.Dafe）等认为，信息系统大体上是“人员、过程、数据的集合，有时候也包括硬件和软件。它收集、处理、存储和传递在业务层次上的事务处理数据和支持管理决策的信息”。