信息安全系列丛书

ISCCF

信息安全保密教程

XINXI ANQUAN BAOMI JIAOCHENG 上册

主编 赵战生 杜虹 吕述望

中国计算机学会信息保密专业委员会 组织策划

中国科学技术大学出版社
北京中电电子出版社

信息安全系列丛书

信息安全保密教程

（上册）

主编　赵战生　杜　虹　吕述望
中国计算机学会信息保密专业委员会　组织策划

中国科学技术大学出版社
北京中电电子出版社

内容简介

建设信息安全保障体系是信息安全保障工作的重要任务，信息安全保密是信息安全保障中的核心问题之一。为跟上信息化的飞速发展，使信息安全保密工作者更好地完成历史重任，本教程以二十章的篇幅，对信息化与信息安全保密的形势、概念、技术、管理和人才的知识结构和技能等方面作了全面深入的介绍；本教程不但叙述了国际上信息安全保障的新情况，新技术、新法规、新标准，也系统全面地介绍了我国信息安全保密工作的政策、法规、标准和工作要求，从而为从事信息安全保密的领导、管理人员和技术人员提供了权威性教材。

图书在版编目（CIP）数据

信息安全保密教程（上下册）/赵战生，杜虹，吕述望主编．—合肥：中国科学技术大学出版社，2006.4

（信息安全系列丛书）ISBN 7-312-01907-2

Ⅰ.信… Ⅱ.①赵… ②杜… ③吕… Ⅲ.信息系统—安全技术—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2006）第 030316 号

出　　版：中国科学技术大学出版社
（安徽省合肥市金寨路 96 号，230026）
北京中电电子出版社
（北京海淀区翠微东里甲 2 号为华大厦 4 层，100036）
责任编辑：邵祖英
发　　行：中国科学技术大学出版社
印　　刷：北京华正印刷有限公司
经　　销：全国新华书店
开　　本：889×1194 1/16
印　　张：45.375
字　　数：1203 千字
版　　次：2006 年 4 月第 1 版
印　　次：2006 年 4 月第 1 次印刷
印　　数：1—5000 册
定价：136.00 元（上下册）

序

20世纪中叶以来现代信息技术的迅速发展，把人类带入了一个被称作“信息化”的时代。在这个时代里，信息获取、传输、存储和处理方式的电子化、计算机化、网络化，导致了魔幻般的信息爆炸和信息共享，造就了史无前例的信息公开和信息自由，并为人类的未来开启了巨大的想象空间。但是，我们也要看到，正如历史上蒸汽机的发明引发工业革命时的情形那样，新技术革命所引发的信息革命在促进了生产力发展和社会全面进步的同时，也促生了许多矛盾和问题，给个人生活和国家安全带来了新的挑战。

就国家安全来讲，在信息时代，信息成为国家的重要战略资源，信息主权成为国家主权的重要内容，信息能力成为国家能力的重要体现和保障。获取、传输、存储和处理信息的能力，既体现一个国家的综合国力，也体现一个国家的安全能力。一方面，我们要坚持信息技术和信息内容可以也应当更多地由人类共享的原则，另一方面，也要看到，在当今世界的政治现实里，任何国家无不尽可能多地确保自己对关系国家安全和利益的军事、政治、经济和社情信息的独享或专享，无不尽可能多地分享其他国家尤其是对手国家的相关信息，发达国家更是凭借自己的信息技术优势谋求信息优势，获享信息霸权。或许更令人担忧的是，工业革命时代建立起来的国家能源、交通、金融、社会服务等关键性基础设施在“信息化”之后，愈来愈严重地依赖以计算机网络通信技术为支撑的庞大而脆弱的信息系统。一旦信息系统出现问题，必将导致灾难性的后果。与此相应，以信息系统为对象的竞争、犯罪、窃密以及信息战愈演愈烈，信息和信息系统的安全若剑悬头顶，直接危及公民权利和国家安全。

2001年，美国联邦政府发布了《保护网络空间国家计划》。在该计划的序言里，前总统克林顿提出网络时代“既充满希望，也充斥危险”。该计划把“信息战士”和“情报机构”列为国家安全的两大威胁源，前者界定为“缩减美国决策空间和战略优势，制造混乱，从事目标破坏”，后者主要是收集政治、军事、经济信息。这个例子表明，信息安全作为一个带有时代特征的国家安全问题，已经开始受到特别关注。

如何正确认识和把握新形势下的信息安全，仍然值得进一步深入研究。如果说，20世纪典型的信息安全概念乃是以通信保密为核心，以通过密码算法加密为基本保护措施，那么，大约从20世纪90年代开始，信息安全概念就已经从单纯的信息内容的保密性扩展到信息和信息系统的完整性和可用性。也就是说，信息安全更多地表现为整个信息系统的安全，着眼于信息系统整个生命周期的防御和恢复，而远不止单个信息的安全。这样，信息安全能力就不仅仅指对特定信息的保密能力和对特定设施的防护能力，它还要包括整个信息系统对威胁的预警能力、对入侵的检测能力、对事件的反应能力和对破坏的恢复能力等。这是一种新的安全概念，也是一种新的保密概念。

作为一个发展中国家，中国正在充分利用新技术革命成果，借助信息化的快车道来实现跨越式发展。当此之时，我们不仅要高度重视信息安全，把信息安全作为信息化建设的内在环节，而且要树立新的与信息时代相适应的信息安全观念，建立新的与计算机网络系统相适应的信息安全体系，犹如给最快的汽车配以最好的车刹。因此，如何全面了解、准确把握、充分吸收当今世界的信息安全技术和管理经验，从我国的实际出发，根据信息化建设快速健康发展的需要，尽快占领技术和管理的制高点，切实推动信息安全保密工作向深层防御、全

面保障前进，是我们面临的一个重要而紧迫的课题。

为深入贯彻国家信息化领导小组《关于加强信息安全保障工作的意见》，进一步普及知识，深化研究，推进工作，国家保密局组织编写了《信息安全保密教程》。该书的编写者都是长期从事信息安全保密技术研究和应用工作、成就不凡的专家学者，他们为该书的完成付出了大量的心血。作为读者，我想借此机会，对他们的奉献与合作表示衷心感谢，对该书的问世表示诚挚祝贺。

是为序。

夏勇谨识

2006年3月1日

总 序

信息社会的兴起，进一步给全球带来了信息技术飞速发展的契机；信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动着人类社会的发展和人类文明的进步，把人类带入了崭新的时代；信息系统的建立已逐渐成为社会各个领域不可或缺的基础设施；信息已成为重要的战略资源，信息化的水平已成为衡量一个国家现代化和综合国力的重要标志，争夺控制信息权已成为国际竞争的重要内容。

胡锦涛主席指出，信息安全是个大问题，必须把安全问题放到至关重要的位置上，认真加以考虑和解决；温家宝总理在国家信息化领导小组第五次会议上指出，信息化是当今世界发展的大趋势，是推动经济社会发展和变革的重要力量。制定和实施国家信息化发展战略，是顺应世界信息化发展潮流的重要部署，要站在现代化建设全局的高度，大力推进国民经济信息化和社会信息化；会议审议并原则通过了《国家信息化发展战略（2006—2020 年）》。会议指出，坚持以信息化带动工业化、以工业化促进信息化；注重建设信息安全保障体系，实现信息化与信息安全协调发展；要夯实信息化基础，完善综合信息基础设施。中央领导多次强调，必须从经济发展、社会稳定、国家安全、公众利益的高度，充分认识信息安全的绝对重要性；各地各部门的领导干部，必须加紧学习网络化知识，高度重视网上斗争的问题并对加强我国信息安全保障工作提出了总体要求：坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。

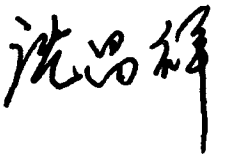
然而，人们在享受信息网络所带来的巨大利益的同时，也面临着信息安全问题的严峻考验。现存的信息安全问题已经对我国的国家安全、经济安全、军事安全和社会安全构成了严重的影响和威胁，我们面临着信息安全的巨大挑战。因此，加速信息安全的研究和发展，加强信息安全保障能力已成为我国信息化发展的当务之急，成为国民经济各领域电子化成败的关键，成为提高中华民族生存能力的头等大事。为了构筑 21 世纪的国家信息安全保障体系，有效地保障国家安全、社会稳定和经济发展，需要尽快地并长期致力于增强广大公众的信息安全意识，提升信息系统研究、开发、生产、使用、维护及教育管理人员的素质和能力。

当今，信息安全的概念正在与时俱进：它从早期的信息保密发展到关注信息的保密、完整、可用、可控和不可否认的信息安全，并进一步发展到现今的信息保障和信息保证体系。单纯的保密和静态的保护已都不能适应今天的需要。信息保障体系是一个社会系统工程，它不仅涉及到信息技术体系本身，还涉及到信息安全的法律法规和组织管理体系。因此，现阶段以及未来的有效信息安全整体解决方案依赖于人利用技术进行操作这三个层面。而实施完整的信息保障战略还必须依赖于人才的培养和经费的支持。

中电电子出版社为适应上述形势，并经与国家信息安全领导机关和管理部门、信息安全的学术团队和研究机构、信息安全主要使用单位和行业、国内外知名专家进行了请示、商榷和研究，决定成立《信息安全系列》丛书编委会。《信息安全系列》丛书编委会由上述有关专家和部门主管领导组成，编委会在国家信息化领导小组的宏观政策指导下，通过长期的努力，组织出版和发行这套丛书。丛书的指导思想是求新、求精、求快、求用，要围绕国内外信息安全的新技术、新发展、新知识和我国市场需求的原则进行考虑；丛书的选题范围是根

据读者群定位为通俗、教育培训、领导和专业等四个层面；丛书的内容涉及信息安全技术、信息安全法律法规和信息安全管理等三个类型六个方面。为普及、提高、推广和发展信息安全理论和技术做出我们应有的贡献。

编委会设主任1人；副主任2人；编委会下设秘书处、编辑部、写作室。考虑到在运作推出《信息安全系列》丛书过程中的复杂性、艰巨性、长期性，因此，必须花大力气依靠编委会全体成员，用若干年时间，完成这项宏大工程。



2006年3月1日

《信息安全系列》丛书编委会

信息安全保密教程编委会

前 言

当前，信息安全保密工作面临的形势十分严峻。一方面，境内外敌对势力将涉密信息系统作为对我窃密与攻击的重要目标，网络失泄密事件时有发生，信息网络已成为泄密的重要渠道。另一方面，我们一些党政机关和重要涉密单位在涉密信息系统的技术防范与管理上存在明显的隐患和漏洞，使国家秘密安全受到严重威胁。新时期保密与窃密的斗争在某种程度上体现为高新技术的对抗，而高新技术的对抗归根结底是掌握技术与管理手段的人的对抗，因此保密培训的重要性和紧迫性是不言而喻的，既要培训技术与管理，更要培养人的意识。

国家保密局根据形势的要求和实际工作的需要，通过中国计算机学会信息保密专业委员会组织有关专家学者编写了《信息安全保密教程》。国家保密局夏勇局长专为本书作了序，中国工程院沈昌祥院士和国家保密局丛兵副局长担任本书编委会主任，主编由赵战生教授、杜虹研究员、吕述望教授担任，写作人员由国家保密技术研究所、中国科学院信息安全国家重点实验室、北京交通大学信息安全体系结构研究中心等单位的多位博士和科研人员承担。多年来，他们一直从事信息安全保密技术与管理的研究，这次又以编写教程的形式把自己的技术积淀通过流畅生动的文字传达出来，而且这本工作量大、质量高的教程是在很短的时间内、花费很大心血完成的，借此机会向这些专家学者的辛勤工作表示衷心的感谢。另外，北京中电电子出版社为本书的顺利出版付出了大量辛勤劳动，在此一并致谢。

本书包含两方面的内容：一方面是相关管理知识讲解和国内外情况介绍，增进保密工作的领导、管理人员、技术人员和涉密人员对于信息安全保密管理的客观规律的认识，这不仅有助于加强安全保密意识，提高管理水平，还能不断与时俱进，更新观念，这是信息安全保密工作常抓不懈、常抓常新的重要思想基础；另一方面是系统、深入的信息安全保密技术的介绍，提高涉密信息系统的管理人员、运行维护人员、使用人员以及保密技术人员应对窃密攻击、排除泄密隐患、保障系统安全的技术能力，在保密窃密技术对抗中做到魔高一尺、道高一丈。

本书各章的主要撰稿人为：第 1 章赵战生，第 2 章赵战生、孙德刚、董守吉，第 3 章孙德刚，第 4 章曲天光、孙锐，第 5 章马朝斌、孙锐，第 6 章潘柱廷、李德全，第 7 章王雪来，第 8 章赵战生，第 9 章陈辉焱、吕述望，第 10 章李晓勇、沈昌祥，第 11 章孔斌、潘柱廷、张剑，第 12 章潘柱廷、张剑，第 13 章潘柱廷、李德全，第 14 章潘柱廷、张剑，第 15 章杨宏宁，第 16 章黄伟庆，第 17 章左晓栋、沈昌祥，第 18 章浦建宁，第 19 章翟卫东、刘振华，第 20 章胡延军。全书由杜虹研究员、赵战生教授、吕述望教授统稿。张剑博士校对了全书，国家保密局郑启淑高级工程师、王京涛高级工程师、魏力高级工程师对本书进行了认真全面的保密审查。中国计算机学会信息保密专业委员会姜放副秘书长对全书的编撰和出版做了大量的协调工作。

希望本书能成为从事信息安全保密技术与管理工作的同志们的良师益友。由于时间和水平所限，书中错漏之处在所难免，恳请广大读者对本书提出宝贵意见，以便再版时修订。

中国计算机学会信息保密专业委员会

2006 年 2 月 26 日

总目录

上 册

下 册