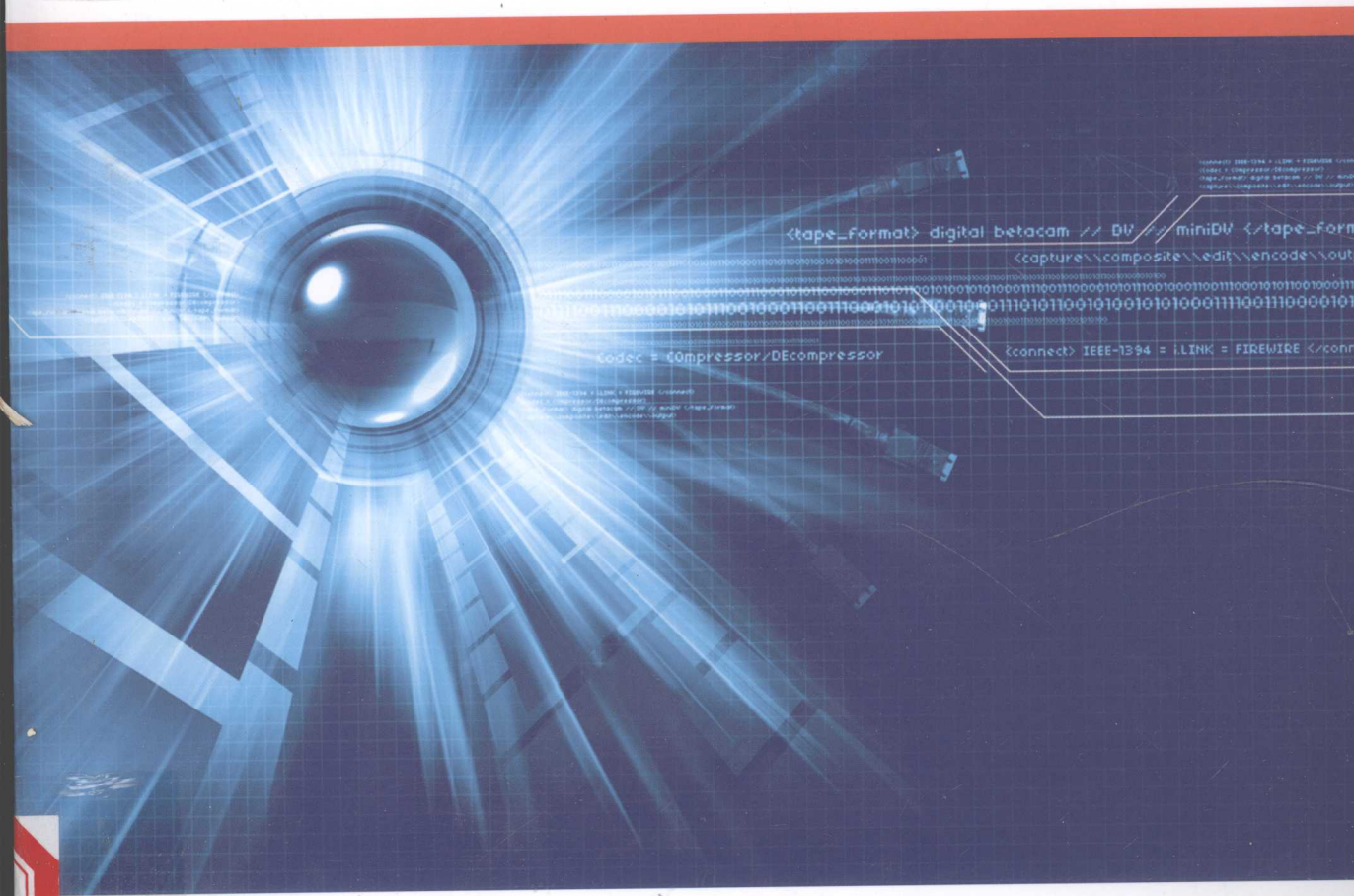
信息安全保障基础

吴世忠　江常青　彭　勇　著



航空工业出版社

信息安全保障基础

吴世忠　姜常青　彭　勇　著

航空工业出版社
北京

内 容 提 要

本书是作者多年在信息安全保障领域研究和实践的成果，它以信息安全保障为主线，结合国家信息安全保障的工作重点和实践，系统地介绍了国内外标准和法律法规最新进展，密码、网络安全、操作系统安全、应用和数据安全、恶意代码等信息安全基础技术，信息安全管理体系、风险评估、灾难恢复、等级保护、应急响应等安全管理技术以及信息安全工程和信息安全攻防实践，形成了符合我国国情的信息安全保障基础知识体系。

本书可作为高等院校信息安全专业的学生教材和参加各类信息安全培训及考试人员的参考资料；同时它也可作为信息安全工作人员的实践指导。

图书在版编目（CIP）数据

信息安全保障基础/吴世忠，姜常青，彭勇著. —北京：航空工业出版社，2009.6
（国家信息安全培训丛书）
ISBN 978-7-80243-273-4

Ⅰ.信… Ⅱ.①吴…②姜…③彭… Ⅲ.①信息系统—安全管理②电子计算机—安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2009）第 056656 号

信息安全保障基础
Xinxi Anquan Baozhang Jichu

航空工业出版社出版发行
（北京市安定门外小关东里 14 号 100029）
发行部电话：010-64815615 010-64978486
北京地质印刷厂印刷 全国各地新华书店经售
2009 年 6 月第 1 版 2009 年 6 月第 1 次印刷
开本：787×1092 1/16 印张：24.5 字数：607 千字
印数：1—5000 定价：60.00 元

序

信息化是当今世界发展的大趋势，是推动经济社会变革的重要力量。大力推进信息化，是覆盖我国现代化建设全局的战略举措，是贯彻落实科学发展观、全面建设小康社会、构建社会主义和谐社会和建设创新型国家的迫切需要和必然选择。如何以信息化提升综合国力，如何在信息化快速发展的同时确保网络空间安全，已经成为各国政府极为关注的问题。

我国于2003年发布的27号文件是国家信息安全建设方面最重要、最全面的指导文件，其中明确提出了“积极防御、综合防范”的安全方针。

要有效地解决信息安全问题，需要我们采用科学的方法，认真分析信息安全问题的实质和特点，逐步建立具有中国特色的信息安全保障体系，为我国的信息化发展提供可靠的安全保障。

本书作者力图描画出信息安全保障的基础性的概貌，本书是一本很好地结合我国国情的信息安全保障基础性综合著作。

何德全

2009年5月

前　言

本书是作者多年在信息安全保障领域中学习、研究和实践的成果，它是在信息安全保障测评工作实践、在信息安全保障建设咨询工作实践，以及在信息安全保障理论研究工作的总结。本书以信息安全保障作为贯穿全书的主线，并形成以信息安全保障基础和标准法规为基础，覆盖信息安全技术、管理和工程保障领域的结构化的、有机的知识整体。

对于在信息安全保障领域中从事学习、研究、实践、工程和管理的人员，本书都能提供相应的帮助。

为了更好地帮助读者建立信息安全整体、全面的知识基础和实践能力，本书的主要内容将根据信息安全保障的实践——深度防御的战略和实践展开，这样，读者就可以更好地学习和了解信息安全保障的基础和实践。

本书共包括以下 4 个部分。

- 第一部分：信息安全保障综述。它包含 2 个章节，第 1 章“信息化与信息安全”从信息化发展带来的安全问题入手，阐述了对信息安全概念内涵和外延的理解；第 2 章“我国信息安全保障工作介绍”简述了我国信息安全保障体系建设的含义、发展阶段、实践和思考。
- 第二部分：信息安全标准法规。它包含 2 个章节，第 3 章“信息安全标准”从标准和标准化基础开始，全面介绍了信息安全标准组织以及信息安全相关的管理、技术和工程标准；第 4 章“信息安全法律法规”介绍了我国信息安全相关的各种法律法规。
- 第三部分：信息安全管理和工程。它包含 7 个章节，第 5 章“信息安全管理基础”介绍了我国信息安全管理体系的现状以及信息安全管理体系的一些基础原则和知识；第 6 章“信息安全风险评估”介绍了国内外风险评估发展等的风险评估背景、基础并介绍了一个风险评估通用的流程；第 7 章“信息系统灾难恢复管理”介绍了灾难恢复管理的基础知识，灾难恢复的过程、相关技术，以及国家灾难恢复等级的划分和实现；第 8 章“信息安全应急响应管理”全面介绍了应急响应的历史、方法、应急响应小组和系统的建设以及应急响应技术的发展等；第 9 章“信息安全漏洞管理” 介绍了漏洞定义、分类、技术研究方向和内容等，并介绍了常用的漏洞库，简要描述了一个帮助组织机构管理漏洞的可实际操作的五阶段七步骤漏洞管理方案；第 10 章“信息安全等级保护”介绍了我国信息安全等级保护的背景、基本概念，以及相关工作的主要内容；第 11 章“信息安全工程实践”从信息安全工程的角度建立了信息安全保障工程模型，并以一个示例描述了建设电子政务的整体流程和方法。
- 第四部分：信息安全技术。它包含了 7 个章节，第 12 章“密码技术和应用”；第 13 章“网络安全基础”；第 14 章“常见网络安全技术”；第 15 章“操作系统安全”；第 16 章“应用与数据安全技术”；第 17 章“恶意软件防护技术”；第 18 章“信息安全攻防”。

目　录

第一部分　信息安全保障综述

第二部分　信息安全标准法规

第三部分　信息安全管理和工程

第四部分 信息安全技术

第一部分

信息安全保障综述

本部分包含以下章节：

第 1 章　信息化与信息安全

第 2 章　我国信息安全保障工作介绍

第1章　信息化与信息安全

内容介绍

当今的信息安全工作，无论在产业环境、产业标准或是产业理论方面，还是在技术产品市场、管理方面，虽然已初显丰硕的成果，却仍然在摸索中前进。

阅读成果

通过本章的学习，读者应该能够：

- 了解信息化的发展和信息安全现状；
- 了解信息安全概念。

1.1　信息化的发展和信息安全

21世纪之初，随着全球信息化趋势的不可避免性，信息安全问题日渐成为世界各国所面临的主要问题之一。我国也接连发生了多起重大信息安全事件，人们开始逐渐认识到国家的信息化程度越高，所面临的信息安全挑战也会越多。

（1）信息化迅猛发展，信息技术广泛应用，我国步入信息化时代

作为世界上最大的发展中国家，中国的信息化进程起步于20世纪80年代。20世纪90年代，中国信息化建设取得长足进展，成为加快我国国民经济发展、提高政府管理和服务水平、增强企业竞争力、改善人民群众生活水平的重要推动力。信息化发展加快了采用信息技术和提升传统产业的步伐，增强了国民经济的竞争力，改善和提高了宏观调控和建设节约型社会的国家战略的实现。金卡、金税、金关、金财、金审、金顿、金农、金保、金水、金版、金卫和金质等一系列“金”字工程，代表了中国国民经济行业信息化建设的成就。

进入21世纪，中国的信息化步入快速发展的新阶段。国民经济与社会信息化水平不断提高，信息化在促进经济与社会协调、稳定、持续的发展过程中，发挥着越来越重要的作用。政府主导的人民网、新华网等新闻网站和新浪、搜狐等商业性综合网站的设立和稳步发展，在传播重要信息、反映社情民意、引导社会舆论等方面发挥了积极重要的影响和作用。信息化所带来的好处日益显现，广大民众对信息化的前景和潜在价值的认识越来越深刻。这些都充分说明，我国信息化建设已顺利迈入了一条适合本国国情、快速发展的道路，信息化进程势头良好、前景喜人。

（2）信息安全重要性提升，信息安全产业和市场逐渐形成

随着信息化和经济全球化的加速发展趋势，我国面临更加复杂的竞争环境。显而易见，