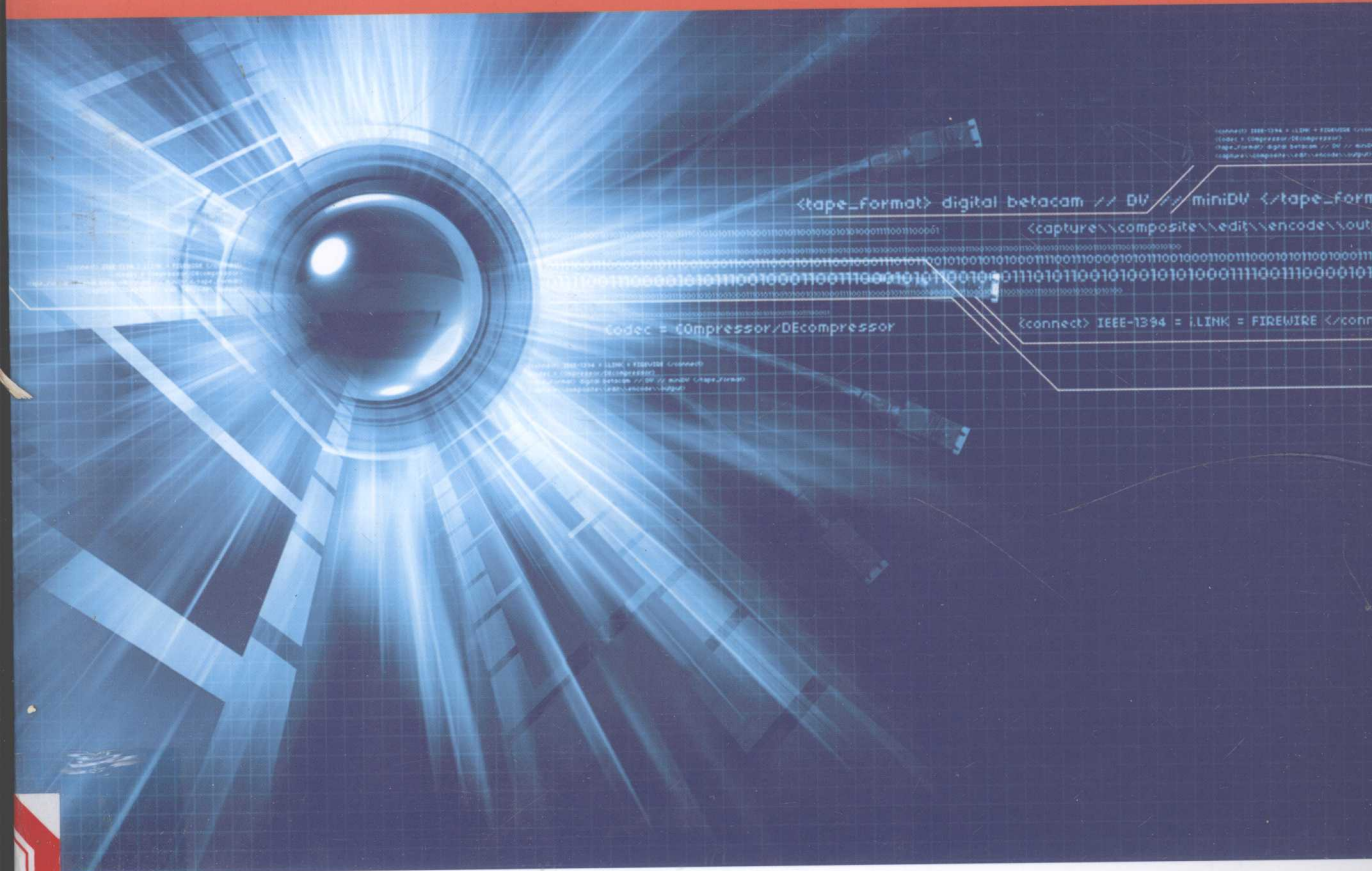


信息安全保障基础

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。

何德志

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：信息安全管理与工程。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1章 信息化与信息安全	3
1.1 信息化的发展和信息安全	3
1.2 信息安全概念的认识和深化	5
第2章 我国信息安全保障工作介绍	10
2.1 我国信息安全保障体系建设的含义	10
2.2 我国信息安全保障工作发展阶段	11
2.3 我国信息安全保障体系的建设规划	11
2.4 国家信息安全保障体系工作的实践	12
2.5 我国信息安全保障工作的思考	13

第二部分 信息安全标准法规

第3章 信息安全标准	19
3.1 标准化概述	19
3.1.1 标准和标准化的定义	19
3.1.2 标准化的发展	20
3.2 我国信息安全标准化建设概况	21
3.2.1 我国信息安全标准化建设工作的意义	21
3.2.2 我国标准化管理和组织机构	22
3.2.3 体系介绍	22
3.2.4 我国信息安全相关标准介绍	24
3.3 信息安全相关标准	25
3.3.1 信息安全评估标准介绍	25
3.3.2 信息安全管理标准介绍	28
3.3.3 信息安全工程标准介绍	31

第4章 信息安全法律法规	34
4.1 信息安全法律法规的概述	34
4.1.1 构建信息安全法律法规的意义	34
4.1.2 构建信息安全法律法规体系的任务	34
4.1.3 我国信息安全法律法规的建设历程	35
4.1.4 我国信息安全法律法规体系框架	36
4.2 现有主要国家信息安全法律简介	38
4.2.1 现有部分国家法律简介	38
4.2.2 现有部分刑法简介	40
4.2.3 现有部分行政法律简介	40
4.2.4 现有部分部门规章及规范性文件简介	43

第三部分 信息安全管理与工程

第5章 信息安全管理基础	49
5.1 我国信息安全管理体制	49
5.1.1 国家信息安全管理政策背景	49
5.1.2 我国信息安全管理体制	50
5.2 信息安全管理	51
5.2.1 信息安全管理概述	51
5.2.2 信息安全管理组织机构	52
5.2.3 信息安全策略	56
5.2.4 安全控制措施的类型	59
5.2.5 人员管理	61
5.2.6 资产管理	65
第6章 信息安全风险评估	69
6.1 风险评估概述	69
6.1.1 风险评估发展历史	69
6.1.2 我国风险评估工作介绍	71
6.2 风险评估基础	74
6.2.1 风险的定义	74
6.2.2 风险评估和风险管理	76
6.3 风险评估介绍	76
6.3.1 风险评估概述	76
6.3.2 风险评价方法	77

6.3.3 风险评估过程	80
6.3.4 风险评估成功的关键因素	88
6.3.5 风险评估标准和方法	90
第7章 信息系统灾难恢复管理	92
7.1 信息系统灾难恢复介绍	92
7.1.1 概述	92
7.1.2 历史和背景	93
7.1.3 业务连续管理/灾难恢复管理 (BCM/DRM) 的定义	94
7.1.4 灾难恢复的级别和指标	96
7.2 灾难恢复管理	102
7.2.1 灾难恢复管理概述	102
7.2.2 组织机构	102
7.2.3 灾难恢复管理过程	103
7.3 灾难恢复管理过程	104
7.3.1 灾难恢复需求分析	104
7.3.2 灾难恢复策略制定	106
7.3.3 灾难恢复策略实现	106
7.3.4 灾难恢复预案制定和管理	107
7.3.5 灾难恢复预案框架	108
7.4 灾难恢复管理的技术考虑	110
7.4.1 备份技术	110
7.4.1 备份技术概述	110
7.4.2 RAID 技术	115
7.4.3 备用场所	119
第8章 信息安全应急响应管理	122
8.1 安全应急响应的历史和现况	122
8.1.1 应急响应的发展背景和国外现状	122
8.1.2 国内安全应急响应发展状况	123
8.1.3 应急响应组织的分类以及各种组织的关系	123
8.1.4 应急响应的定义和特点	123
8.1.5 应急响应的作用	124
8.2 应急响应方法论	124
8.2.1 应急响应方法论的重要性	124
8.2.2 应急响应的6阶段方法论	125
8.3 信息安全事件的分级分类	134
8.3.1 信息安全事件分类	134

信息安全保障基础

8.3.2 信息安全事件分级	137
8.4 应急响应组的建立	138
8.4.1 组建应急响应组的必要性	139
8.4.2 应急响应组的功能需求和角色	141
8.4.3 应急响应组服务的对象	142
8.4.4 应急响应组的成员	143
8.5 应急响应管理体系的建设	144
8.5.1 应急响应目标的限定	144
8.5.2 应急响应责任的详细规定	146
8.5.3 针对安全应急的程序规则及报告渠道	148
8.5.4 安全应急事件的提交策略和响应优先级	149
8.5.5 通知受影响的各方	150
8.5.6 对安全应急响应的评估	150
8.6 应急响应技术的发展方向	151
第9章 信息安全漏洞管理	152
9.1 信息安全风险和漏洞	152
9.2 漏洞的基本概念	153
9.2.1 漏洞的定义	153
9.2.2 漏洞的分类	155
9.2.3 漏洞的技术研究	155
9.3 常用漏洞库介绍	158
9.3.1 安全机构漏洞库	158
9.3.2 厂商漏洞库	158
9.3.3 其他	159
9.3.4 国内漏洞库简介	159
9.4 漏洞管理实践	160
9.4.1 漏洞管理方案	160
9.4.2 步骤1: 了解资产	161
9.4.3 步骤2: 建立资产的基线扫描	161
9.4.4 步骤3: 对特定资产执行渗透性测试	161
9.4.5 步骤4: 修补漏洞和风险	161
9.4.6 步骤5: 建立漏洞评估进度安排	162
9.4.7 步骤6: 建立补丁和变更管理过程	163
9.4.8 步骤7: 监视对资产的新风险	164
第10章 信息安全等级保护	165
10.1 背景概述	165

10.2 等级保护的依据	166
10.2.1 法律与政策的要求	166
10.2.2 等级保护相关标准与规范	166
10.3 等级保护的基本概念	166
10.4 等级保护的定级要素及级别划分	166
10.5 等级保护的工作内容	167
10.5.1 信息资源分类分级保护制度	167
10.5.2 系统安全功能分级保护制度	168
10.5.3 分级监管制度	168
10.6 等级保护基本要求与主要流程	168
10.7 等级保护开展工作简介	169
第 11 章 信息安全工程实践	170
11.1 信息系统安全保障工程实施框架	170
11.1.1 信息系统安全保障工程定义	170
11.1.2 信息系统安全保障工程实施通用模型	170
11.1.3 信息系统安全保障工程递归实施模型	175
11.1.4 信息系统安全保障工程实施的剪裁	175
11.2 电子政务信息系统安全保障工程实例	177
11.2.1 某电子政务信息系统安全保障工程概述	177
11.2.2 某电子政务信息系统安全保障工程分阶段描述	178

第四部分 信息安全技术

第 12 章 密码技术和应用	185
12.1 密码学概述	185
12.1.1 密码学的历史背景	185
12.1.2 密码学的基本概念	187
12.1.3 密码系统基础	188
12.1.4 密码系统的强度	189
12.2 理解密码算法	190
12.2.1 对称密码算法	190
12.2.2 非对称密码算法	192
12.2.3 哈希算法	194
12.2.4 公钥密码、对称密码技术比较	194
12.3 消息验证和数字签名	196

信息安全保障基础

12.3.1 消息验证	196
12.3.2 数字签名	197
12.4 公钥基础设施	197
12.4.1 PKI 是什么	198
12.4.2 证书中心 (CA)	199
12.4.3 注册中心 (RA)	200
12.4.4 实施证书	200
12.4.5 X.509	200
12.4.6 电子认证业务规则	201
12.4.7 理解证书撤销	201
12.5 密钥管理和证书生命周期	202
12.5.1 证书中心 CA	202
12.5.2 证书生命周期	202
12.5.3 密钥管理	203
12.5.4 备份与恢复管理措施	203
12.6 密码标准与协议	204
12.6.1 公钥基础设施标准和协议	204
12.6.2 网络和应用安全标准和协议	205
12.7 我国密码技术和应用管理概述	207
12.7.1 国家商用密码管理介绍	207
12.7.2 国家电子认证服务的管理	209
第 13 章 网络安全基础	212
13.1 概述	212
13.2 开放系统互联 (OSI) 体系模型	213
13.3 电信网络基础	214
13.3.1 PSTN (公共交换电话网络)	215
13.3.2 DDN (数字数据网)	215
13.3.3 ADSL (非对称数字用户环路)	215
13.3.4 ISDN (综合业务数字网)	215
13.3.5 X.25 协议	216
13.3.6 B-ISDN (宽带综合业务数字网)	216
13.3.7 ATM (异步传输模式)	216
13.3.8 FR (帧中继网)	217
13.3.9 OTN (光传送网)	217
13.3.10 ASON (自动交换光网络)	217
13.4 计算机网络基础	217
13.4.1 网络分类	217

13.4.2	TCP/IP 介绍	220
13.4.3	IPX/SPX 等其他协议	222
13.4.4	网络传输介质	223
13.5	常见的网络安全威胁和保护	225
13.5.1	恶意软件	225
13.5.2	社会工程	225
13.5.3	拒绝服务 (DoS)	227
13.5.4	分布式拒绝服务 (DDoS)	232
13.5.5	数据欺骗	233
13.5.6	网络安全保护常见实践	237
第 14 章	常见网络安全技术	240
14.1	防火墙系统	240
14.1.1	概述	240
14.1.2	防火墙平台	241
14.1.3	防火墙系统和环境	249
14.1.4	防火墙策略和管理	255
14.2	入侵检测和防护系统 (IDPS)	255
14.2.1	IDPS 系统概述	255
14.2.2	IDPS 系统的用途	256
14.2.3	IDPS 系统的关键功能	256
14.2.4	常见的检测方法	257
14.2.5	常见 IDPS 产品类型	259
14.3	VPN 系统	261
14.3.1	VPN 系统	261
14.3.2	VPN 的分类	263
14.3.3	VPN 安全技术基础	268
14.3.4	IPSEC VPN 介绍	269
14.3.5	二层 VPN 技术介绍	275
14.3.6	传输层 VPN 介绍	277
14.3.7	应用层 VPN 协议	278
14.3.8	VPN 的规划和实施	279
第 15 章	操作系统安全	280
15.1	操作系统安全概述	280
15.1.1	操作系统安全研究概况	280
15.1.2	信息技术安全评估准则 (CC) 对操作系统安全功能的要求	281
15.1.3	操作系统的安全机制	282

15.2 Windows 操作系统安全.....	289
15.2.1 Windows 2000 操作系统的安全机制.....	289
15.2.2 Windows XP SP2 安全新机制.....	300
15.3 Linux 操作系统安全.....	303
15.3.1 鉴别.....	303
15.3.2 访问控制.....	305
15.3.3 审计.....	305
15.3.4 可靠性.....	306
15.3.5 安全配置.....	306
15.4 主机安全要点.....	306
15.4.1 制定主机安全策略.....	307
15.4.2 断开网络连接.....	307
15.4.3 帐户安全.....	307
15.4.4 用户帐户.....	307
15.4.5 系统服务.....	308
15.4.6 关闭端口.....	309
15.4.7 加强保护.....	309
15.4.8 改变操作系统.....	309
第 16 章 应用与数据安全技术.....	311
16.1 办公软件安全.....	311
16.1.1 字处理程序安全.....	311
16.1.2 电子邮件安全.....	313
16.1.3 浏览器安全.....	318
16.1.4 消息软件/博客安全.....	327
16.2 应用服务器安全.....	329
16.2.1 邮件服务器安全.....	329
16.2.2 Web 服务器安全.....	330
16.2.3 数据库安全.....	336
16.3 数据安全技术.....	337
16.3.1 数据加密技术.....	337
16.3.2 数据备份技术.....	337
16.3.3 数据恢复技术.....	340
16.3.4 磁盘阵列 (RAID) 技术.....	340
第 17 章 恶意软件防护技术.....	341
17.1 恶意软件概述.....	341
17.1.1 恶意软件的历史.....	341

17.1.2 恶意软件统计	343
17.1.3 恶意软件趋势	344
17.2 恶意软件基础概念	345
17.2.1 恶意软件的分类	345
17.2.2 恶意软件的传播方式	348
17.2.3 恶意软件的攻击目标	351
17.3 恶意软件的预防	351
17.3.1 策略和意识	351
17.3.2 漏洞减轻	352
17.3.3 威胁减轻	352
17.4 感染恶意软件的特征及响应措施	353
17.5 恶意软件清除工具	354
17.5.1 使用防病毒软件查杀计算机中的病毒	354
17.5.2 安装间谍软件、广告软件查杀工具对计算机进行扫描	355
第 18 章 信息安全攻防	356
18.1 信息安全攻击概述	356
18.1.1 引言	356
18.1.2 攻击的定义和目标	357
18.1.3 攻击的一般过程	357
18.1.4 攻击的类型	359
18.1.5 攻击的演变与发展	362
18.2 个人信息安全防护“十二招”	363
参 考 文 献	371

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，