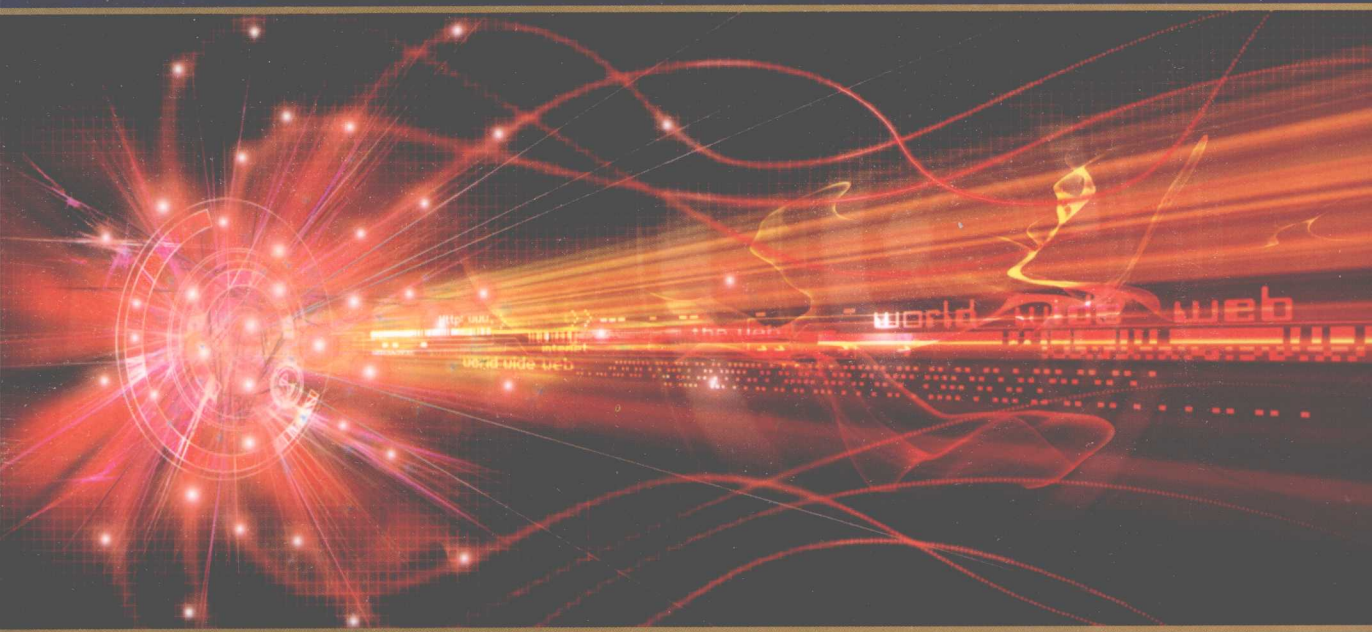


信息系统的 发展 与 创新

DEVELOPMENT AND INNOVATION OF INFORMATION SYSTEMS

蔡希尧 编著



西安电子科技大学出版社
<http://www.xduph.com>

内容简介



信息系统的发展与创新

蔡希尧 编著

图书在版编目(CIP)数据

图书在版编目(CIP)数据

信息系统的发展与创新 / 蔡希尧编著. — 西安: 西安电子科技大学出版社, 2009. 12

ISBN 978-7-320-07348-1

ISBN 978-7-320-07348-1

Ⅰ. 信…

Ⅰ. 信… Ⅱ. 蔡… Ⅲ. 信…

Ⅳ. 信…

中国版本图书馆CIP数据

中国版本图书馆CIP数据

图书在版编目(CIP)数据

第 1 版 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

第 1 次印刷 (2009.12)

西安电子科技大学出版社

2009



内 容 简 介

本书讨论信息系统近年来的最新发展与创新,即从全局的角度讨论信息系统的建造、部署和运行的关键问题,以专题方式进行论述,每一章就是一个独立的专题。选择的专题侧重于信息系统的联网、体系结构、系统集成、系统安全、软件与服务、管理和治理等方面,注重信息系统中动态的、流动的和变化的要素。

全书共有 42 章,分成 6 个部分:概念和基础、演化和集成、信息系统的安全保护、软件与服务、管理和治理、统一与融合。

本书的读者对象是:从事信息系统开发和建设的工程技术人员、项目经理和单位主管,大学和科研机构从事信息系统研究的博士生、硕士生和教师。

图书在版编目(CIP)数据

信息系统的发展与创新/蔡希尧编著. —西安:西安电子科技大学出版社, 2009.12

ISBN 978-7-5606-2348-1

I. 信… II. 蔡… III. 信息系统—研究 IV. G202

中国版本图书馆 CIP 数据核字(2009)第 185182 号

策 划 臧延新

责任编辑 阎 彬 臧延新

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)88242885 88201467 邮 编 710071

网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com

经 销 新华书店

印刷单位 陕西华沐印刷科技有限责任公司

版 次 2009 年 12 月第 1 版 2009 年 12 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印 张 56.875

字 数 1340 千字

印 数 1~1000 册

定 价 96.00 元

ISBN 978-7-5606-2348-1/G·0034

XDUP 2640001-1

如有印装问题可调换

本社图书封面为激光防伪覆膜,谨防盗版。

前言

推进国民经济和社会信息化是覆盖现代化建设全局的战略举措。“以信息化带动工业化,实现社会生产力的跨越式发展”,是我国发展经济的基本指导方针。政务信息化、商务信息化等正在全国展开,大量的信息系统已建造或在建设之中。本书正是根据这一形势,以信息系统的发展与创新为主题而编写的。

本书不是系统论述信息系统原理和方法的教科书,而是讨论信息系统近年来的发展与创新,阐明信息系统的建造、部署和运行中的主要问题的专著;本书不重复已经成熟的理论和技术,而着眼于新出现的和被忽视的重要问题;本书以专题方式进行论述,每一章是一个专题,每个专题是独立的,有的专题之间有一定的关联,但尽量避免重复。

当代信息系统是在网络环境中运行的,是经济和社会发展的基础设施,是全球化激烈竞争中的制胜力量。建造和部署的信息系统必须能够适应环境的快速变化、容易使用、便于互动、及时提供服务、效率高、成本低,因此,本书选择的专题侧重于信息系统的联网、体系结构、系统集成、系统安全、软件与服务、管理和治理等方面,注重信息系统的关键性问题,重点论述动态的、流动的和变化的要素。例如,安全是信息系统的关键问题,在第三部分有 12 个专题讨论信息系统的安全保护。数据是信息系统中最活跃的和流动的要素,在书中安排了 4 个专题讨论有关数据的问题,即“数据集成”(第 7 章),“数据保护”(第 19 章),“联网存储”(第 33 章)和“数据管理”(第 36 章)。信息系统的宗旨是支持应用和提供服务,应用和服务依靠的是软件;软件是整个信息系统运行的动力,软件的安全性是信息系统能否正常运行的关键;信息系统快速响应环境和条件的变更,改变功能和增强能力,也主要依靠软件。所以,对软件技术的发展和创新的安排安排了多个专题介绍。

全书共有 42 个专题,即 42 章,分成 6 个部分。第一部分:概念和基础,含 5 个专题;第二部分:演化和集成,含 5 个专题;第三部分:信息系统的安全保护,含 12 个专题;第四部分:软件与服务,含 13 个专题;第五部分:管理和治理,含 5 个专题;第六部分:统一与融合,含 2 个专题。

在信息系统的发展与创新过程中,企业是主体,所以本书引用的参考文献重点是全球著名的 IT 公司发布的白皮书,另外就是标准化组织发布的规范和标准,还有报纸、广播、网络上各种有关信息技术和信息系统的报导和问题讨论,以及作者多年来积累和整理的材料。这些参考文献和资料,规格不一,不像期刊那样正规,缺乏某些必要的信息,如作者姓名、发布日期等。为了弥补这一缺点,在每章的参考文献之后附有“检索词”,书末附有“中英文词汇对照表”,以便查找。

考虑到本书的内容较多和某些读者的时间有限,作者专门写了几篇综合性的专题,其中,第 1 章是对信息系统的全面综述,第 41 和 42 章综合讨论了两个有关信息产业发展前

途的重大问题：电信与计算的融合及统一通信，第 11、23、24、29 章是有关信息系统安全保护、软件和服务等方面的综合性专题。

我国的电子信息产业总体规模已居世界第三位，但不久前的一个统计表明，我国的信息技术发展综合指标在全球 83 个国家和地区中排在第 43 位，和我国的经济地位很不相称，这说明我国的电子信息产业主要建立在国外核心技术基础之上，自主创新能力薄弱，硬件与软件的关键技术相对落后，系统开发与集成能力较差。所以，我们在发展信息技术、大力建设信息系统的同时，必须着力于信息技术的发展和创造，创造新的概念、理论、技术、方法和产品。

经济学的“创新—长波理论”指出：“技术创新是决定资本主义经济实现繁荣、衰退、萧条和复苏周期过程的主要因素。”“能够成功创新的人就能够摆脱萧条期的利润递减的困境而生存下来。”“每一次的萧条都包含着一次可能的技术革新。”信息技术是当前发展最为迅速、应用最广泛、影响面最大的高新技术，充分发挥信息技术和信息系统特有的普适、赋能、拟人和增值能力，重视信息技术和信息系统的发展与创新，必将能够更快地从当前的经济危机中求得复苏，振兴经济。

作者

2009 年 8 月

目 录

第一部分 概念和基础

第 1 章 理解信息系统	3	1.6.1 概念和基础	16
1.1 基本概念	3	1.6.2 系统集成和演化	20
1.1.1 信息	3	1.6.3 信息系统安全	24
1.1.2 信息与数据	3	1.6.4 软件和服务	29
1.1.3 信息技术	3	1.6.5 电信与计算的大融合	33
1.1.4 信息系统	4	1.7 问题讨论	35
1.1.5 信息系统服务	4	1.7.1 安全与开放	35
1.2 信息系统的发展历程	5	1.7.2 创新与标准	35
1.3 信息系统的开放性	6	1.7.3 统一与个性	35
1.3.1 开放信息系统的特性	6	1.7.4 规范与标准	36
1.3.2 开放信息系统的定义	6	1.7.5 无边界应用	36
1.3.3 开放信息系统的优缺点	7	1.7.6 互动与语义	37
1.3.4 标准	7	1.7.7 松耦合	37
1.3.5 NDI 和 COTS	8	1.7.8 安全性	37
1.4 信息系统的社会性	9	参考文献	38
1.4.1 社会软件	9	检索词	38
1.4.2 社会关系网络	9	第 2 章 需求开发	39
1.4.3 知识产权和道德规范问题	10	2.1 导言	39
1.4.4 数字鸿沟	10	2.2 需求开发的意义和困难	39
1.4.5 计算机犯罪	10	2.2.1 意义	39
1.4.6 需求工程中的社会问题	10	2.2.2 利益相关者的共同性需求	40
1.4.7 信息系统建设的社会环境	11	2.2.3 需求问题的复杂性	40
1.4.8 社会中介机构与咨询服务	11	2.3 需求工程的概念	41
1.5 信息系统的管理和治理	11	2.4 需求的分类	42
1.5.1 信息战略规划	12	2.4.1 功能需求	42
1.5.2 项目管理	12	2.4.2 非功能需求	42
1.5.3 工作流管理	13	2.4.3 其他需求	43
1.5.4 数据管理	14	2.5 需求开发过程	43
1.5.5 安全管理	14	2.5.1 需求错误	43
1.5.6 信息系统治理	14	2.5.2 需求提取	45
1.6 信息系统的技术问题	16	2.5.3 需求分析	46

2.5.4 需求规范	47	检索词	68
2.5.5 需求验证测试与确认	47	第4章 信息基础设施	69
2.5.6 接口定义	48	4.1 概念与特性	69
2.6 需求管理	49	4.1.1 基本概念	69
2.6.1 需求变更管理	49	4.1.2 特性	69
2.6.2 需求跟踪管理	49	4.2 建设信息基础设施的指导方针	70
2.6.3 需求管理过程的注意事项	50	4.2.1 信息基础设施是开放的	70
2.7 信息系统需求工程的发展前景	50	4.2.2 与需求相适应	70
2.7.1 现有技术的不足和发展要求	50	4.2.3 具有互操作性	71
2.7.2 发展面向服务的需求工程	51	4.2.4 联网的分布环境	71
参考文献	52	4.3 信息基础设施的体系结构	72
检索词	53	4.3.1 信息基础设施体系结构的重要性	72
第3章 信息系统的体系结构	54	4.3.2 信息基础设施体系结构模型	72
3.1 基本概念	54	4.4 企业基础设施	74
3.1.1 什么是体系结构	54	4.4.1 企业基础设施体系结构	74
3.1.2 为什么需要体系结构	55	4.4.2 企业基础设施的支持工具	75
3.2 体系结构标准	55	4.5 网络环境的建立	77
3.3 体系结构的框架和视图	57	4.5.1 网络基础设施的地理布局	77
3.3.1 体系结构框架	57	4.5.2 网络基础设施的重要技术	78
3.3.2 体系结构视图	58	4.6 信息基础设施运行管理问题	81
3.4 建造体系结构的指导方针和步骤	60	4.6.1 运行管理的新思路	81
3.4.1 指导方针	60	4.6.2 五个关键问题	81
3.4.2 建造的基本步骤	60	参考文献	82
3.5 体系结构设计的几个主要问题	60	检索词	83
3.5.1 设计原则	60	第5章 联网新技术	84
3.5.2 体系结构和系统设计的边界	61	5.1 前言	84
3.5.3 新技术的使用	61	5.2 互联网的发展	84
3.5.4 数据互操作性	61	5.2.1 发展过程	84
3.5.5 数据模型	61	5.2.2 TCP/IP 协议	85
3.6 体系结构的分析与评估	62	5.2.3 WWW	86
3.6.1 概述	62	5.2.4 XML	86
3.6.2 分析和评估的方法	62	5.2.5 结构的改进	87
3.7 通用技术引用模型	64	5.2.6 新能力的加入	87
3.7.1 POSIX 标准	64	5.3 无线联网技术	87
3.7.2 技术引用模型	65	5.3.1 无线网络的优点	88
3.8 体系结构的集成和支持成分	67	5.3.2 无线局域网	88
3.8.1 体系结构的集成	67	5.3.3 无线城域网	89
3.8.2 体系结构的集成支持	67	5.3.4 正交频分复用和正交频分 复用多址	91
参考文献	67		

5.3.5 移动宽带无线接入	92	5.4 结论	97
5.3.6 无线广域网	94	参考文献	98
5.3.7 无线局域网	95	检索词	98

第二部分 演化和集成

第6章 信息系统演化

6.1 前言	101
6.2 已建系统和目标系统	101
6.2.1 已建系统	101
6.2.2 目标系统	102
6.3 演化技术	102
6.3.1 对演化技术的基本要求	102
6.3.2 支持环境技术	103
6.3.3 技术选择	103
6.4 系统维护	103
6.4.1 维护的重要性	103
6.4.2 维护的类型	104
6.5 系统更新	104
6.5.1 白盒更新	105
6.5.2 黑盒更新	105
6.5.3 更新技术	105
6.5.4 软件升级	108
6.6 软件移植	108
6.6.1 概念	108
6.6.2 移植需要考虑的问题	109
6.6.3 移植和重用的异同	110
6.7 系统替换	110
6.7.1 替换的意义	110
6.7.2 替换的指导方针	111
参考文献	111
检索词	112

第7章 数据集成

7.1 数据集成面对的问题	113
7.1.1 难度大	113
7.1.2 影响数据集成的各种因素	113
7.2 数据集成的利益	114
7.3 数据集成过程	114
7.3.1 需求分析	115

7.3.2 集成方式的选择	115
7.3.3 数据库规范和设计	116
7.3.4 开发、测试和实现	117
7.4 数据集成技术	117
7.4.1 模式集成	117
7.4.2 使用元数据的集成	118
7.4.3 使用XML的集成	118
7.4.4 使用中间件的集成	119
7.4.5 数据请求中介	120
7.4.6 包装集成	121
7.4.7 OAGIS 集成规范	121
7.5 集成数据库	122
7.5.1 数据仓库	122
7.5.2 联机分析处理	123
7.5.3 联邦数据库	125
7.5.4 面向对象联机分析处理	125
7.6 新的课题	127
参考文献	128
检索词	129

第8章 信息系统集成

8.1 信息系统集成的意义	130
8.2 信息系统集成的指导方针	131
8.3 系统集成的任务、特征和要求	132
8.3.1 集成的主要任务	132
8.3.2 集成系统的特征	133
8.3.3 对解决方案的要求	133
8.4 企业应用集成	133
8.4.1 概念	133
8.4.2 EAI 的层次	134
8.4.3 企业应用集成的利益	135
8.5 企业管理集成	135
8.5.1 概述	135
8.5.2 企业资源规划	136

8.5.3 供应链管理	137	9.5.1 基本概念	151
8.5.4 客户关系管理	137	9.5.2 QoS 的控制机制	152
8.5.5 值链管理	137	9.5.3 QoS 需求	152
8.6 商家对商家集成	138	9.6 典型中间件概况	153
8.6.1 B2B 概念	138	9.6.1 交易中间件	153
8.6.2 B2BI 与 EAI 的异同	139	9.6.2 过程中间件	154
8.6.3 B2BI 与传统企业集成的差别	139	9.6.3 消息中间件	156
8.7 基于 Web 服务的业务集成	139	9.6.4 对象中间件	157
8.7.1 Web 服务在企业应用	140	9.6.5 数据库中间件	161
集成中的应用	140	9.7 发展与创新	162
8.7.2 Web 服务在 B2B 中的应用	140	9.7.1 现有解决方案的不足	163
参考文献	141	9.7.2 新的需求	163
检索词	142	9.7.3 新的进展	164
第 9 章 中间件技术	143	9.7.4 标准化工作	165
9.1 概念和基础	143	9.7.5 研究工作	166
9.1.1 中间件的概念	143	9.7.6 进行中的项目	168
9.1.2 中间件的地位和作用	143	参考文献	169
9.1.3 分布对象计算	144	检索词	170
9.2 对中间件的需求	145	第 10 章 互操作技术	171
9.2.1 通信能力	145	10.1 什么是互操作	171
9.2.2 服务质量	145	10.1.1 概念	171
9.2.3 协调机制	145	10.1.2 重要性	171
9.2.4 可靠性	146	10.1.3 定义	172
9.2.5 伸缩性	146	10.2 互操作问题的成因	173
9.2.6 互操作性	147	10.2.1 自主性	173
9.3 基于 DOC 的中间件	147	10.2.2 异构性	173
9.3.1 主机基础设施中间件	148	10.2.3 开发者的认知与协调的不足	174
9.3.2 分布中间件	149	10.3 固有困难与指导法则	174
9.3.3 通用中间件	149	10.3.1 固有困难	174
9.3.4 特定域中间件	150	10.3.2 指导法则	174
9.4 中间件对信息系统发展的支持	150	10.4 互操作需求	177
9.4.1 系统集成比程序设计更加	150	10.4.1 体系结构	177
受到重视	150	10.4.2 基础设施	178
9.4.2 开放系统体系结构生存能力和	150	10.4.3 中间件	178
开源软件可用性的增强	150	10.4.4 层次划分	178
9.4.3 对实时嵌入式环境集成不断增长	151	10.4.5 标准	179
的关注	151	10.4.6 测试	179
9.4.4 改善软件质量和性能	151	10.4.7 系统开发程序的同步	179
9.5 中间件的服务质量	151	10.4.8 模拟和演示	179

10.4.9 互操作性的描述方法	180	10.8.2 已有数据互操作方法	185
10.5 互操作模型	180	10.8.3 数据体系结构	187
10.5.1 能力模型	180	10.8.4 紧耦合与松耦合	187
10.5.2 NMI 模型	180	10.8.5 Web 数据互操作	188
10.5.3 互操作等级模型	181	10.9 工作流互操作	190
10.5.4 概念性互操作等级模型	181	10.9.1 基本概念	190
10.5.5 组织互操作性成熟度模型	182	10.9.2 工作流管理参考模型	191
10.6 软件密集系统的互操作性	182	10.9.3 工作流互操作标准	192
10.6.1 现状和问题	182	10.9.4 工作流互操作等级	193
10.6.2 两个案例	183	10.9.5 工作流互操作性鉴定	194
10.7 Web 服务互操作	183	10.9.6 电子商务中的工作流互操作	195
10.7.1 Web 服务互操作的问题	184	10.10 达到互操作的通用途径	196
10.7.2 Web 服务互操作联盟的工作	185	参考文献	197
10.8 数据互操作	185	检索词	198
10.8.1 数据互操作的概念	185		

第三部分 信息系统的安全保护

第 11 章 信息系统的安全保护	201	11.5.1 配置安全平台	212
11.1 基本概念与原理	201	11.5.2 平台安全评估准则	212
11.1.1 定义	201	11.5.3 操作系统的安全问题	213
11.1.2 安全性原理	202	11.5.4 及时更新	214
11.1.3 安全威胁	203	11.5.5 接入控制	214
11.1.4 安全漏洞	203	11.6 密码技术概要	214
11.1.5 风险管理和控制	204	11.6.1 定义	214
11.2 信息安全性分类与安全事件类型	206	11.6.2 密码算法	215
11.2.1 信息安全性分类	206	11.6.3 密钥分类	215
11.2.2 安全事件类型	206	11.6.4 公开密钥的概念	216
11.3 信息系统的安全策略及其实施	207	11.6.5 几种常用的加密算法	216
11.3.1 安全策略	207	11.6.6 量子通信与量子密码技术	219
11.3.2 深度防御策略	208	11.7 认证和授权	220
11.3.3 安全策略的实施	208	11.7.1 概念	220
11.4 安全体系结构	209	11.7.2 认证系统的要素	220
11.4.1 概念	209	11.7.3 认证中心和数字证书	221
11.4.2 设计准则	210	11.7.4 授权	221
11.4.3 安全体系结构的组成成分	210	11.7.5 认证与授权的协议	222
11.4.4 通用安全体系结构的组成	211	11.7.6 权限管理基础设施	223
11.4.5 通用的网络安全组成成分	212	11.8 密钥管理	224
11.5 平台的安全性	212	11.8.1 密钥管理的原则与策略	224

11.8.2	密钥管理的生命周期	226	11.12.9	美国国家标准	246
11.8.3	密钥管理基础设施	228	11.12.10	美国联邦标准	246
11.8.4	域参数和公钥的确认	228	11.12.11	美国国防部指令	247
11.8.5	密钥和其他密钥材料的安全 问题	228	11.13	总结	247
11.8.6	问责	229	参考文献	248	
11.8.7	审计	229	检索词	249	
11.8.8	密钥恢复	229	第 12 章 联网安全	250	
11.8.9	密钥算法的强度和长度	230	12.1	联网安全的新形势	250
11.9	公开密钥基础设施	230	12.2	防火墙技术	251
11.9.1	概述	230	12.2.1	防火墙的重要性	251
11.9.2	PKI 的能力	231	12.2.2	防火墙的组成	251
11.9.3	PKI 的应用实例	231	12.2.3	防火墙的策略	252
11.9.4	PKI 的互操作性	232	12.2.4	信息包过滤	252
11.9.5	PKI 存在的问题	232	12.2.5	防火墙的设置	252
11.9.6	PKI 解决方案的评估	232	12.2.6	XML 防火墙	253
11.9.7	PKI 实例: DoD PKI	233	12.2.7	应用防火墙	253
11.10	XML 安全规范	237	12.2.8	隔离区	254
11.10.1	XKMS 规范	237	12.3	威胁检测和入侵预防	254
11.10.2	X-KISS 规范	239	12.3.1	网络威胁检测	254
11.10.3	X-KRSS 规范	239	12.3.2	系统威胁检测	254
11.10.4	X-BULK 规范	239	12.3.3	入侵检测系统	255
11.11	数据中心、服务器和虚拟专用网的 安全	239	12.3.4	入侵预防系统	256
11.11.1	数据中心安全性	239	12.3.5	入侵预防系统与应用防火墙的 区别	257
11.11.2	Web 服务器的安全性	240	12.3.6	研究领域	257
11.11.3	服务器客户的安全性	241	12.3.7	关于内部威胁	257
11.12	信息技术安全标准	241	12.4	虚拟专用网的安全性	258
11.12.1	已发布的中国国家标准	241	12.4.1	基本概念	258
11.12.2	正在制定的中国国家标准	242	12.4.2	VPN 主要的安全特征	258
11.12.3	中国国家军用标准	242	12.4.3	VPN 的组成	258
11.12.4	已发布的国际标准化组织标准	243	12.4.4	VPN 使用的协议	259
11.12.5	正在制定的国际标准化组织 标准	243	12.5	统一威胁管理	260
11.12.6	银行操作和规程的信息安全 国际标准	244	12.5.1	什么是统一威胁管理	260
11.12.7	国际电信联盟标准	246	12.5.2	UTM 的优点	260
11.12.8	欧洲计算机制造商协会信息 安全标准	246	12.5.3	UTM 的缺点	261
			12.5.4	终端安全保护与 UTM	261
			12.5.5	发展前景	261
			12.6	网络接入控制	262
			12.7	无线网络的安全问题	262

12.7.1 常用的无线网安全技术	262	参考文献	282
12.7.2 无线局域网的安全技术	264	检索词	283
12.7.3 WiMAX 安全问题	264	第 14 章 可信计算	284
12.7.4 WiMAX MAC 层的结构	265	14.1 概述	284
12.7.5 MAC 层的安全保护	266	14.1.1 基本概念	284
12.7.6 WiMAX 的安全性缺陷及其改进	267	14.1.2 可信计算的发展历程	284
12.7.7 Ad hoc 网的安全问题	268	14.1.3 TCG 的工作	286
参考文献	269	14.1.4 受益领域	287
检索词	269	14.2 可信硬件平台	288
第 13 章 网络接入控制	270	14.2.1 智能设备	288
13.1 概述	270	14.2.2 可信平台模块	288
13.2 网络接入控制的过程和方法	270	14.2.3 可信通用 PC 机	291
13.2.1 准入	271	14.2.4 Intel vPro 处理器	291
13.2.2 策略选择	271	14.3 可信软件平台	294
13.2.3 策略执行	271	14.3.1 操作系统	294
13.3 补救与集成	272	14.3.2 引导机制	299
13.3.1 补救	272	14.3.3 支持软件	300
13.3.2 集成	273	14.4 可信计算库	300
13.4 NAC 解决方案的需求	273	14.4.1 可信计算库的构成	300
13.4.1 接入策略	273	14.4.2 TCB 范例	300
13.4.2 安全状态评估	273	14.5 可信网络连接	301
13.4.3 网络接入等级	273	14.5.1 概述	301
13.4.4 支持多种接入方法	274	14.5.2 TNC 的体系结构	302
13.4.5 安全状态监控	274	14.5.3 TNC 的接口	303
13.4.6 可伸缩性和可管理性	274	14.5.4 带有 TPM 的 TNC 体系结构	304
13.4.7 管理工具	274	14.5.5 TNC 的支持技术	305
13.4.8 适应移动性	274	14.5.6 安全保密问题	305
13.5 典型解决方案	274	14.6 可信移动计算	306
13.5.1 Cisco NAC	275	14.6.1 移动计算面临的风险	306
13.5.2 Microsoft NAP	276	14.6.2 可信移动的安全需求	307
13.5.3 TCG TNC	277	14.6.3 移动恶意攻击	307
13.5.4 其他解决方案	277	14.6.4 Symbian 安全子系统	308
13.6 不同解决方案之间的互操作	278	14.6.5 可信移动平台	308
13.6.1 NAC 和 NAP 互操作	278	14.6.6 可信移动平台的互操作问题	309
13.6.2 TNC 和 NAP 互操作	279	14.6.7 TCG 移动可信模块	309
13.7 统一接入控制	281	14.6.8 NTT DoCoMo、IBM 和 Intel 的 可信移动平台	311
13.7.1 UAC 和 TNC	281	14.6.9 3GPP 移动安全规范	312
13.7.2 UAC 和 RSA	281	14.6.10 信任叠加	313
13.7.3 UAC 和 NAP	282		

14.7	可信存储规范	314	15.3.6	过程管理	331
14.7.1	核心体系结构	314	15.3.7	目录聚集、同步和虚拟化	331
14.7.2	可信外围设备	315	15.3.8	虚拟化目录	331
14.7.3	安全提供者	315	15.3.9	服务和协议支持	332
14.7.4	核心体系结构操作	315	15.4	身份管理的得益和障碍	333
14.8	通用服务器规范	316	15.4.1	得益	333
14.8.1	概要	316	15.4.2	障碍	333
14.8.2	服务器分割	316	15.4.3	投资回报	333
14.8.3	可信建造模块	317	15.5	身份管理的现状调查	334
14.8.4	服务器绑定	318	15.5.1	一般性的调查结论	334
14.8.5	动态重新配置	318	15.5.2	治理状况	334
14.8.6	平台状态	318	15.5.3	实现状况	335
14.8.7	隔离计算环境体系结构	319	15.5.4	个人身份证明技术	336
14.9	可信计算存在的问题和争论	319	15.5.5	对业务伙伴身份的处理	337
14.9.1	普遍存在的问题	319	15.5.6	保证身份的完整性	337
14.9.2	TCG 规范存在的问题	320	15.5.7	建立基础设施	338
	参考文献	320	15.6	身份管理需求	338
	检索词	321	15.6.1	终端用户需求	338
第 15 章	身份管理	322	15.6.2	网络管理和操作人员需求	339
15.1	概述	322	15.6.3	网络漫游需求	340
15.1.1	基本概念	322	15.6.4	应用访问提供者需求	340
15.1.2	重要性和迫切性	323	15.6.5	规章及法律需求	340
15.1.3	词汇定义	323	15.7	身份管理解决方案	340
15.1.4	身份管理要点	323	15.7.1	确定解决方案的准则	340
15.1.5	身份管理的复杂性	324	15.7.2	解决方案示例	342
15.1.6	身份管理的风险	324	15.7.3	身份管理的专用设备	343
15.1.7	集成问题	325	15.7.4	存在的问题	343
15.2	身份窃取类型	325	15.8	联合身份管理	344
15.2.1	SQL 注入	325	15.8.1	联合身份管理的需求	344
15.2.2	跨站点脚本插入	326	15.8.2	自由联盟	345
15.2.3	Cookie 篡改	326	15.8.3	联合身份管理的技术规范	346
15.2.4	会晤攻击	327	15.8.4	其他标准化组织的计划	352
15.2.5	远程 Web 服务器接管	327	15.9	自适应身份管理	352
15.3	身份管理系统的基本功能	327	15.9.1	概述	352
15.3.1	身份认证	327	15.9.2	集成和合作的管理	353
15.3.2	口令管理	328	15.9.3	策略驱动管理	354
15.3.3	单点登录	329	15.9.4	了解上下文	354
15.3.4	令牌和智能卡	330	15.10	身份管理产品	354
15.3.5	供应与撤销	330	15.10.1	CA 的产品 eTrust	354

15.10.2	BMC 的身份管理方案	356	16.5.3	软件安全性分析	372
15.10.3	HP 的 OpenView Select 系列	356	16.5.4	形式方法的应用	376
15.10.4	IBM 的身份管理产品	356	16.6	软件系统安全性设计	376
15.10.5	Microsoft 的身份和接入管理 系列	358	16.6.1	软件系统安全性标准	376
15.10.6	Oracle 的身份管理软件	358	16.6.2	达到安全性的方法	377
15.10.7	RSA 的安全身份认证系统	359	16.6.3	危险处理	378
15.11	发展趋势	359	16.7	人机互动的安全性	380
15.11.1	以用户为中心的身份管理	359	16.7.1	自动化系统中人的角色	380
15.11.2	按需自适应基础设施	360	16.7.2	人机互动系统的设计	380
15.11.3	普适计算与身份管理	361	16.7.3	人机界面	381
15.11.4	可信计算平台	361	16.8	软件系统安全性验证	382
15.11.5	发展中存在的问题	361	16.8.1	独立验证和确认	382
参考文献		362	16.8.2	安全性测试	382
检索词		363	16.9	总结	383
第 16 章 软件系统安全性		364	参考文献		384
16.1	软件安全性的分类	364	检索词		384
16.2	软件系统安全的重要意义	365	第 17 章 软件安全性保护		385
16.2.1	软件、信息和信息系统安全性	365	17.1	软件安全性漏洞	385
16.2.2	软件系统安全性的重要性	365	17.1.1	概述	385
16.2.3	关键性安全软件	366	17.1.2	常见的软件安全漏洞	386
16.2.4	软件引发的灾难实例	367	17.1.3	多发性漏洞类型	386
16.3	软件不安全的原因	367	17.1.4	最大的互联网漏洞	387
16.3.1	物理法则的失效	367	17.2	其他软件安全性问题	387
16.3.2	数学模型的应用困难	368	17.2.1	数据安全和软件	387
16.3.3	传统认知的不适应	368	17.2.2	软件审计	387
16.3.4	事故模型和失效模式的特殊性	369	17.2.3	基于 Web 技术的安全性	387
16.3.5	系统行为的突发性	369	17.2.4	SQL 注入	387
16.3.6	需求缺陷	369	17.2.5	跨站点插入脚本	388
16.3.7	实体之间的互动	369	17.2.6	缓存溢出	388
16.3.8	软件质量难以测量	369	17.2.7	利用 Cookie 的攻击	388
16.3.9	测试的局限性	369	17.3	漏洞管理	389
16.4	软件系统安全性的目标和任务	370	17.3.1	漏洞管理的基本任务	389
16.4.1	目标	370	17.3.2	漏洞管理系统的构成	390
16.4.2	任务	370	17.3.3	漏洞管理系统的其他考虑	390
16.4.3	软件安全性过程的保证条款	371	17.4	安全性知识体系	391
16.5	实现软件系统安全性的方法	371	17.4.1	说明性知识	391
16.5.1	前提设定	371	17.4.2	诊断性知识	392
16.5.2	安全性管理	372	17.4.3	历史知识	392
			17.5	软件保证	392

17.5.1	软件保证的定义和属性	392	18.1.3	电子邮件的安全威胁和保护方法	416
17.5.2	建立可信软件的困难	393	18.1.4	邮件服务器的安全保护	417
17.5.3	对软件保证的要求	393	18.1.5	Web 邮件系统的安全性	417
17.5.4	软件保证已有的方法	394	18.2	电子商务安全性	418
17.5.5	软件保证合作框架	395	18.2.1	电子商务的安全问题	418
17.5.6	软件保证框架	396	18.2.2	电子商务的安全性要求	418
17.5.7	软件保证元模型	397	18.2.3	电子商务的信任体系	418
17.6	软件安全性保护的实践经验与能力准则	398	18.2.4	电子商务的安全模式	419
17.6.1	软件安全性保护的实践经验	398	18.2.5	安全体系结构	422
17.6.2	安全性软件开发的能力准则	399	18.2.6	安全支付系统	422
17.7	安全性软件开发生命周期	401	18.2.7	支付卡行业数据安全标准	423
17.7.1	需求阶段	401	18.3	电子邮件和电子商务的安全协议	424
17.7.2	设计阶段	401	18.3.1	HTTPS 协议	424
17.7.3	实现阶段	401	18.3.2	SSL 协议	424
17.7.4	测试阶段	402	18.3.3	S/MIME 协议	425
17.7.5	部署阶段	402	18.3.4	SET 协议	426
17.7.6	维护阶段	402	18.3.5	PGP 协议	427
17.8	软件安全属性的评估	402	18.3.6	PEM 和 MOSS 协议	427
17.8.1	计算的安全属性	402	参考文献	428	
17.8.2	软件安全属性评估方法的发展历程	403	检索词	428	
17.8.3	安全属性的定义	403	第 19 章 数据保护	429	
17.8.4	功能抽取技术	404	19.1	数据保护的重要意义	429
17.8.5	计算安全属性的分析过程	404	19.2	数据泄漏	430
17.8.6	安全属性的行为需求	405	19.2.1	从内向外泄漏	430
17.8.7	存在的问题和下一步的工作	408	19.2.2	外部入侵造成的泄漏	431
17.9	应用安全性	408	19.2.3	内部人员的恶意行动	432
17.9.1	保护方法	409	19.3	数据保护要点	432
17.9.2	应用防火墙	409	19.3.1	主要的保护目标	432
17.10	总结	411	19.3.2	安全和效用平衡	432
附录	安全性标准化机构、标准和规范	412	19.3.3	关注数据治理	433
参考文献		413	19.3.4	数据治理要点	433
检索词		414	19.4	缓解和预防数据泄漏的技术措施	435
第 18 章 电子邮件和电子商务的安全性		415	19.4.1	数据加密	435
18.1	电子邮件安全性	415	19.4.2	加密数据的监控	435
18.1.1	电子邮件的重要性	415	19.4.3	密钥的存储和管理	436
18.1.2	电子邮件的安全类别	415	19.4.4	存储数据的保护	436
			19.4.5	数据备份和恢复	437
			19.4.6	数据匹配	438
			19.4.7	反病毒、反间谍、反钓鱼	438

19.4.8	保护等级标记	439	20.4.1	渗透测试的方法	454
19.4.9	应用代理防火墙	439	20.4.2	渗透测试的步骤	455
19.4.10	建立 SSL 隧道	439	20.5	工具	456
19.4.11	使用瘦客户和虚拟桌面基础设施	439	20.5.1	工具的重要性	456
19.4.12	建立信誉系统	439	20.5.2	侦察工具	456
19.4.13	托管服务	439	20.5.3	漏洞利用工具	457
19.5	缓解和预防数据泄漏的策略	440	20.5.4	混合工具	457
19.5.1	数据保护策略	440	20.6	总结	458
19.5.2	策略的自动执行	440	参考文献	459	
19.5.3	应用层用户的行为跟踪	441	检索词	459	
19.6	持续数据保护	441	第 21 章 信息系统安全审计	460	
19.6.1	概念	441	21.1	安全审计的任务和类型	460
19.6.2	持续数据保护的新能力	441	21.1.1	安全审计的任务	460
19.6.3	持续数据保护的实现方法	442	21.1.2	安全审计的类型	461
19.7	远程数据保护	442	21.2	安全审计的指导方针与策略	461
19.7.1	远程办事处概况	442	21.2.1	COBIT 的安全审计指导方针	461
19.7.2	远程数据保护的复杂性	443	21.2.2	审计策略	462
19.7.3	远程数据保护需要考虑的问题	444	21.3	信息系统安全审计能力基准	462
19.7.4	解决方案	444	21.4	安全审计工作过程	463
19.8	数据保护产品	445	21.4.1	工作过程	463
19.8.1	Microsoft 的数据保护管理器	445	21.4.2	计划与准备	463
19.8.2	Symantec 解决方案	445	21.4.3	数据采集	465
19.8.3	Vormetric 的 CoreGuard	446	21.4.4	事件分析	465
19.8.4	IBM 的 Tivoli 持续数据保护	446	21.4.5	响应与报警	466
参考文献	446	21.4.6	审计报告	466	
检索词	447	21.4.7	自身审计记录	466	
第 20 章 渗透测试	448	21.4.8	关于网络的安全审计	466	
20.1	主动防御和渗透测试	448	21.5	信息系统安全审计过程的监控与测量	467
20.1.1	主动防御的概念	448	21.5.1	审计的关键性性能和成功因素	467
20.1.2	渗透测试	449	21.5.2	设计关键性性能测量	467
20.2	渗透测试的得益	450	21.5.3	执行评估	467
20.2.1	业务方面的得益	450	21.5.4	评估满意度	468
20.2.2	信息技术方面的得益	451	21.6	信息系统安全审计标准	468
20.3	渗透测试的成功要素	451	21.6.1	ISO/IEC 27000	468
20.3.1	组织测试队伍	451	21.6.2	NIST-SP800	468
20.3.2	定义范围	452	21.6.3	ISACA 标准	468
20.3.3	选择合作者	453	21.6.4	COBIT 的信息系统安全审计指南	468
20.3.4	服从策略和标准	453	21.6.5	中华人民共和国国家标准	469
20.4	渗透测试的方法和步骤	454	21.7	信息系统审计员与管理职责	469

21.7.1 审计员的职责	469
21.7.2 审计员的资格认定	469
21.7.3 审计管理人员的职责	470
参考文献	470
检索词	471
第 22 章 信息系统和产品的安全性	
评估	472
22.1 前言	472
22.2 安全性评估准则	472
22.2.1 可信计算机安全性评估准则	473
22.2.2 信息技术安全性评估准则	473
22.2.3 通用准则	473
22.2.4 国际标准化组织安全性评估标准	474
22.2.5 中国信息技术安全性评估准则	474
22.3 评估对象信息安全功能需求	474
22.3.1 安全性功能需求	474
22.3.2 功能需求类别	475
22.4 安全保证需求	477
22.5 评估的输入和输出	478
22.5.1 评估输入	478

22.5.2 评估输出	478
22.6 评估种类	479
22.6.1 保护轮廓评估	479
22.6.2 安全性目标评估	479
22.7 评估过程	480
22.8 评估保证等级	481
22.9 TCSEC 评估保证等级	484
22.10 OCTAVE 评估	485
22.10.1 概况	485
22.10.2 OCTAVE 评估方法的特点	485
22.10.3 OCTAVE 评估的过程	486
22.10.4 OCTAVE 评估计划	487
22.10.5 OCTAVE 的实现指南	487
22.11 保密模块评估准则	488
22.11.1 评估准则	488
22.11.2 安全等级	488
22.11.3 对软件的要求	489
参考文献	490
检索词	490

第四部分 软件与服务

第 23 章 软件技术和产业的特征	493
23.1 认识软件	493
23.1.1 软件的分类	493
23.1.2 软件的重要性	493
23.2 形势和动向	494
23.2.1 发展形势	494
23.2.2 推动力量	495
23.2.3 技术变革的动向	495
23.3 软件开发的特点与产品的特征	496
23.3.1 软件开发的特点	496
23.3.2 软件产品的特征	496
23.4 面临的挑战	497
23.4.1 需求的提升	497
23.4.2 事实的压力	497
23.4.3 自身的复杂性	497
23.5 软件产品的质量	498

23.5.1 软件产品质量的特殊性	498
23.5.2 软件质量保证	498
23.5.3 软件质量标准(ISO 9126-1991)	501
23.5.4 软件质量标准(ISO/IEC 9126)	503
23.6 主要支持技术	503
23.6.1 对象技术	503
23.6.2 构件技术	504
23.6.3 软件体系结构	504
23.6.4 XML 技术	505
23.6.5 验证与确认技术	505
23.6.6 软件部署	506
参考文献	506
检索词	507

第 24 章 软件工程的发展与创新	508
24.1 前言	508
24.2 方法论的创新	508