电子商务技术与应用

杨千里　王育民　等著

ELECTRONIC COMMERCE

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

电子商务技术与应用

杨千里　王育民　等著

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

内 容 简 介

本书旨在系统地介绍电子商务的基本概念、基本理论及基本方法。全书共 11 章，包括电子商务系统概述、EDI 系统简介、电子商务系统的组成、电子商务系统的安全(基本理论、技术与应用)、卡技术、电子商务中的支付系统、医疗信息系统与电子商务、Internet 上的信息出版发行系统及版权保护、网上虚拟商店、基于 Java 的电子商务实例分析。

本书可供政府各部门决策者、企业管理者、科研人员以及一切意欲了解或开发电子商务的人士参考。

图书在版编目(CIP)数据

电子商务技术与应用/杨先里，王育民编著. - 北京：电子工业出版社，1999.4 (2000 重印)
ISBN 7-5053-5376-4

Ⅰ.电… Ⅱ.①杨…②王… Ⅲ.计算机网络-计算机应用-商务 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2000)第 07074 号

书　　名：**电子商务技术与应用**
著　　者：杨千里　王育民等
策划编辑：张　欣
责任编辑：周　琰
特约编辑：巨　筠
印 刷 者：北京朝阳隆华印刷厂
出版发行：电子工业出版社　URL: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：787×1092　1/16　印张：16　字数:410 千字
版　　次：1999 年 4 月第 1 版　2000 年 4 月第 3 次印刷
书　　号：ISBN 7-5053-5376-4/TP·2703
定　　价：28.00 元

凡购买电子工业出版社的图书，如有缺页、倒页、脱页者，请向购买书店调换；
若书店售缺，请与本社发行部联系调换。电话 68279077

序　一

我非常高兴为展现在中国广大读者面前的这本《电子商务技术与应用》撰写序言。在我们迈向21世纪的时候，信息产业和商务动作的根本基础发生了重大转移，网络音(Webtone)计算的出现可以被看作是与电话时代拨号音出现有着同样意义的重大事件。

电子商务是这一重大转移的范例，不论你是一个企业家，一个经理，还是一名工人，或者干脆就是一个普通消费者，你都不得不跨上电子商务这驾坐骑。电子商务将改变人们业务交往和商务交易的方式。网络变成了新的媒介，它简直就像是会议大厅、分支银行、证券交易所、百货商场或是旅游公司一样。你可以主动地亦或是被动地接纳这一新事物，但不管你采用何种方法，电子商务都已远远走出遐想变成了现实。

本书从介绍电子商务的概念入手，详尽地讲解Internet、intranet和extranet的技术要点。本书适用的读者范围很广泛，商务决策人士会从电子商务市场上领会到无限的商机；技术经理会悟出应用软件的开发方向，而开发人员则会懂得怎样承担起软硬件产品的集成任务。

从这本书中，商务决策人还会在他所在行业内发现许多新的机遇，了解怎样利用Internet获取更大的利润。对技术经理和开发人员来讲，他们还将为现有的企业网络和传统系统找到如何升级的方法，用极小的投入到达现代最新技术的前沿。

在这个电子商务的时代，Sun Microsystems公司为业界提供了解决方案，它的可缩放的安全可靠的服务器系列产品，加上它基于Web的各种数据服务器，以及具有创新意义的Java技术，构成了电子商务架构的坚实基础。今天，Java已经成为一种理想技术，它将计算机桌面系统、家用电器和移动通信器件，如电视机顶盒、电话和寻呼机等，无缝地集成到同一个电子商务的网络之中。

我向本书的作者和出版社的编辑们表示祝贺，他们凭藉敏锐的洞察力预见到电子商务技术对中国的巨大影响。我相信，积极准备投身于电子商务这一新浪潮的读者们和业界人士均会从中受益。

余宏德(Daniel Yu)
Sun公司大中华区总裁

序　二

我很高兴有机会向本书的读者讲几句话，有以下几个原因：第一，这是由中国人撰写的专门讨论中国因特网网上商务的富有创意的一本书；第二，本书将 BroadVision（宏观公司软件产品）作为电子商务解决方案的主要范例；第三，中国以电子商务作为进入新世纪的前沿，而宏观则秉承其创新和探索未知的传统，很高兴成为其中一员。当然，作为一个华人和全球电子商务的开拓者，我将有机会充满激情地与读者诸君在虚拟空间相会，这应是最重要的原因。

根据市场研究的统计数字，1999 年全球因特网商业销售可接近 700 亿美元，预计在 2003 年可突破 3 万亿美元。因特网作为处理商务的主要渠道之一，正在全球范围内成为必然的趋势。

6 年多以前，宏观在创建伊始就着眼于将虚拟网络与一对一市场机制相融合，率先提出基于关系型管理的端对端因特网解决方案。我们相信，企业要获得成功，应该把重点放在维系客户、培育人际关系和扩大关系网方面，我们也深信因特网是获得客户和创造商机的最终渠道。因特网改变了公司业务运作的方式。在此情况下，仅仅提供简单的事务处理或信息发布是无法产生明显的增值效益的，而 BroadVision 则不同，作为一种软件平台或工具，它正好能够有效地管理雇员、伙伴和客户之间的关系，对每一个独立用户可按其需求、兴趣和爱好，在适当的时间、对适当的群体提供适当的服务（知识和产品），从而使企业能够保持长期的成功运作。

今天，我们在阅读这本书的时候，真应该感谢永泰（UNI-Tech）公司电子商务研究中心的同行们为本书的成功所做出的贡献。我本人非常赞赏作者们的丰富知识和写作才华，预祝本书获得成功。

我真诚地希望中国的电子商务业将拥有辉煌的前景和持久的生命力。

我期待着和朋友们在网上相见。

陈丕宏（PehongChen）
宏观公司（BroadVision Corporation）
总裁，主席，首席执行官

前　言

两年前，我们就想把几年来的开发和集成工作经验进行一次总结，编写一本关于电子商务的书。一方面，用以抛砖引玉，为信息技术的同行们提供一份可供借鉴的技术资料；另一方面，也希望政府和企业管理人员在决策时能有所参考。但一直忙于搞项目、搞题目，迟迟未能动手。直到98年4月，杨千里教授和王育民教授欣然应允参与编写并出任主编，同时又得到了出版社的大力支持，我们才下定决心，把这件事尽快搞起来。

本书写作提纲由王育民教授起草，经过几次讨论，并得到出版社同意后才开始分头撰写。各章作者分列如下：

第1章	电子商务系统概述	杨千里
第2章	EDI(电子数据交换)系统简介	范　雄
第3章	电子商务系统的组成	查福标
第4章	电子商务系统安全的基础理论	王育民
第5章	电子商务系统的安全技术与应用	王育民
第6章	卡技术	卢义明
第7章	电子商务中的支付系统	杨　波
第8章	医疗信息系统与电子商务	孙晓蓉
第9章	Internet上的信息出版发行系统及版权保护	王育民
第10章	网上虚拟商店	查福标
第11章	基于Java的电子商务实例分析	陈春海

初稿写成后，我们召开了一次编写组全体人员会议，对初稿逐章进行了讨论和研究，然后由原作者根据讨论意见进行修改，最后又委托王育民教授和杨波博士通读原稿，对写作风格进行了必要的统一和调整。

我们衷心感谢各位作者和出版社编辑人员的辛勤劳动，同时我们还要特别感谢Sun公司总裁余宏德先生和BroadVision公司总裁陈丕宏先生为本书撰写了序言。

我们期望读者对本书提出批评和建议。我们一定会把工作做得更好。

永泰软件工程(深圳)有限公司
电子商务研究中心

编委会名单

作 者 简 介

黄仲翘

1973 年获加利弗尼亚大学博士学位。在信息技术领域从事咨询、科研和管理工作至今。现任中国信息建设投资公司总裁兼永泰软件工程(深圳)公司总经理。香港电脑学会会士。

杨千里

研究员,教授。1950 年就读于南京大学电机系,1956 年毕业于通信工程学院无线电系。从事教学、科研及技术管理工作至今。现为中国电子学会副会长,中国通信学会学术委员会副主任,跨国电器与电子工程师学会(IEEE)高级会员及北京分部(IEEE - Beijing Section)执行主席(1996/1997),永泰软件工程(深圳)有限公司技术顾问。

范 雄

1983 年毕业于成都科技大学电子计算机系。1991 年获四川大学计算机硕士学位。曾任永泰软件工程(深圳)有限公司技术部总经理。

查福标

副研究员。1985 年毕业于浙江大学地质系,1991 年在中国科学院地球化学研究所获理学博士学位。1994 年留学德国马堡大学,1996 年回国后加入永泰软件工程(深圳)有限公司,负责电子商务方面的研究和开发工作。

王育民

1959 年 7 月毕业于西安电子科技大学电信工程专业。长期从事信息论、编码、密码与信息安全的教学和科研工作。曾在美国 Hawaii 大学电机工程系做访问学者,现为西安电子科技大学教授、博士生导师,中国电子学会和中国通信学会会员,IEEE 高级会员,永泰软件工程(深圳)有限公司技术顾问。

卢义明

女。1970 年毕业于清华大学自动控制系(现计算机系)。现任清华大学计算机系副教授。

杨 波

1986 年 7 月获北京大学数学系信息专业理学学士学位，1993 年 7 月获西安电子科技大学计算机系软件专业硕士学位。1999 年 3 月获西安电子科技大学通信工程学院密码学博士学位。现为西安电子科技大学副教授。

孙晓蓉

女。1993 年获西北工业大学检测技术及仪器专业工学学士学位，1996 年获通信与电子系统专业工学硕士学位。现为西安电子科技大学密码学专业博士生，从事通信网络安全保密方面的研究。

陈春海

1992 年毕业于武汉钢铁学院自动化系。1995 年加入永泰软件工程(深圳)有限公司，先后就任软件开发工程师，项目经理，系统集成部经理。

目　录

第1章　电子商务系统概述 …… (1)
1.1　什么是电子商务 …… (1)
1.2　电子商务的框架构成及模式 …… (3)
1.3　Internet(因特网)、Intranet(内域网)和 Extranet(外域网) …… (5)
1.4　电子商务的发展过程 …… (6)
1.5　发展电子商务的驱动力 …… (8)
1.6　案例 …… (9)
1.7　电子商务在中国发展的潜力和障碍 …… (11)
1.8　电子商务涉及的法律、法规、政策及标准 …… (13)
第2章　EDI(电子数据交换)系统简介 …… (18)
2.1　EDI 的定义和作用 …… (18)
2.1.1　EDI 的定义 …… (18)
2.1.2　EDI 的作用 …… (18)
2.2　EDI 的组成 …… (19)
2.2.1　EDI 标准 …… (20)
2.2.2　EDI 翻译软件 …… (20)
2.2.3　EDI 与其他应用系统的接口 …… (20)
2.2.4　EDI 网络通信基础 …… (20)
2.3　EDI 的国际标准化组织 …… (21)
2.3.1　对标准的理解 …… (21)
2.3.2　有关的国际化标准组织简介 …… (21)
2.4　EDI 数据格式标准 …… (23)
2.5　EDIFACT 简介 …… (25)
2.6　ANSI X.12 简介 …… (28)
2.7　EDI 的应用 …… (29)
2.7.1　EDI 的应用概述 …… (29)
2.7.2　在运输业中的应用 …… (30)
2.7.3　在国际贸易中的应用 …… (31)
2.7.4　在海关业务中的应用 …… (32)
2.8　电子商务的兴起和 EDI 的发展 …… (32)
2.8.1　EDI 发展的限制 …… (33)
2.8.2　因特网技术与电子商务 …… (33)
2.8.3　传统 EDI 和电子商务系统的比较 …… (34)
第3章　电子商务系统的组成 …… (37)

3.1 电子商务系统的框架 …… (37)
3.1.1 电子商务系统概述 …… (37)
3.1.2 传统电子商务与现代电子商务的比较 …… (38)
3.2 电子商务系统的技术基础 …… (38)
3.2.1 HTTP 协议 …… (38)
3.2.2 HTML 语言 …… (41)
3.2.3 Java 语言及 Java Applet …… (41)
3.2.4 Java Script 及 VBScript …… (41)
3.2.5 CGI 脚本程序 …… (42)
3.2.6 ISAPI 或 NSAPI …… (42)
3.2.7 ASP …… (42)
3.3 电子商务中的安全保障 …… (42)
3.3.1 防火墙 …… (43)
3.3.2 身份认证 …… (43)
3.3.3 HTTPS 和 SSL 协议 …… (45)
3.4 电子商务系统的解决方案 …… (47)
3.4.1 Sun 电子商务联盟的解决方案 …… (47)
3.4.2 IBM 的电子商务解决方案 …… (49)
3.4.3 HP 公司的电子商务解决方案 …… (50)
3.5 小结 …… (51)
第 4 章 电子商务系统安全的基础理论 …… (52)
4.1 电子商务系统的安全问题 …… (52)
4.2 保密理论引论 …… (54)
4.2.1 保密与保密系统 …… (54)
4.2.2 认证与认证系统 …… (55)
4.2.3 密码体制分类 …… (56)
4.2.4 双钥保密和认证体制 …… (57)
4.3 单钥密码体制 …… (58)
4.3.1 流密码 …… (58)
4.3.2 分组密码 …… (60)
4.3.3 DES …… (61)
4.3.4 分组密码运行模式 …… (62)
4.3.5 分组密码的组合 …… (63)
4.3.6 IDEA …… (63)
4.3.7 RC-5 …… (63)
4.3.8 SAFER K-64 …… (64)
4.3.9 其他分组密码算法 …… (64)
4.4 双钥密码体制 …… (64)

4.4.1 RSA 密码体制 …… (64)
4.4.2 ElGamal 密码体制 …… (66)
4.4.3 椭圆曲线密码体制 …… (66)
4.5 数据的完整性 …… (67)
4.5.1 杂凑函数 …… (67)
4.5.2 应用杂凑函数的基本方式 …… (68)
4.5.3 MD-4 和 MD-5 杂凑算法 …… (70)
4.5.4 安全杂凑算法(SHA) …… (70)
4.5.5 其他杂凑算法 …… (70)
4.6 数字签字 …… (70)
4.6.1 数字签字基本概念 …… (70)
4.6.2 RSA 签字体制 …… (72)
4.6.3 ElGamal 签字体制 …… (72)
4.6.4 DSS 签字标准 …… (73)
4.6.5 其他签字算法 …… (74)
4.6.6 无可争辩签字 …… (74)
4.6.7 盲签字 …… (75)
4.6.8 双联签字 …… (76)
4.7 认证与身份证明 …… (77)
4.7.1 身份证明系统的组成和要求 …… (77)
4.7.2 身份证明的基本分类 …… (78)
4.7.3 实现身份证明的基本途径 …… (78)
4.7.4 通行字(口令)认证系统 …… (79)
4.7.5 个人特征的身份证明技术 …… (81)
4.7.6 零知识证明的基本概念 …… (81)
4.8 安全协议 …… (82)
4.8.1 协议的基本概念 …… (82)
4.8.2 基本密码协议分类 …… (83)
4.8.3 密钥建立协议 …… (83)
4.8.4 认证协议 …… (84)
4.8.5 消息认证 …… (85)
4.8.6 实体认证协议 …… (86)
4.8.7 认证的密钥建立协议 …… (86)
第 5 章 电子商务系统的安全技术与应用 …… (89)
5.1 Internet 的安全 …… (89)
5.1.1 Internet 上的主要安全 …… (89)
5.1.2 接入控制 …… (90)
5.1.3 防火墙 …… (92)

5.1.4 代理服务器 …… (95)
5.1.5 消息安全性 …… (96)
5.1.6 Web 安全 …… (100)
5.1.7 入侵的审计、追踪与检测技术 …… (102)
5.1.8 网络病毒与防范 …… (102)
5.1.9 电子商务中的安全性 …… (103)
5.1.10 Internet 业务提供者协议 …… (103)
5.2 证书和证书机构 …… (104)
5.2.1 公钥证书的基本概念 …… (104)
5.2.2 公钥/私钥对的管理 …… (106)
5.2.3 公钥证书的发行与分配 …… (107)
5.2.4 公钥的格式 …… (109)
5.2.5 公钥证书的吊销 …… (112)
5.2.6 证书的使用期限 …… (113)
5.2.7 公钥证书的授权信息 …… (114)
5.3 公钥基础设施 …… (114)
5.3.1 要求 …… (114)
5.3.2 证实机构间的相互关系结构 …… (115)
5.3.3 证书政策 …… (117)
5.3.4 证书中名字的约束 …… (118)
5.3.5 证实通路的查找和确认 …… (118)
5.3.6 证书管理协议 …… (119)
5.3.7 实例 …… (119)
5.4 密钥管理 …… (120)
5.5 时戳业务 …… (121)
5.5.1 仲裁方案 …… (122)
5.5.2 链接协议 …… (122)
5.5.3 分布式协议 …… (122)
5.6 不可否认业务 …… (123)
5.6.1 概念 …… (123)
5.6.2 类型 …… (123)
5.6.3 实现不可否认性的证据机制 …… (124)
5.6.4 源的不可否认性机构 …… (125)
5.6.5 实现递送的不可否认性的机构 …… (125)
5.6.6 可信赖第三方 …… (126)
5.6.7 解决纠纷 …… (126)
5.7 有关信息安全技术的标准 …… (127)
5.7.1 密码技术的国际标准 …… (127)

5.7.2 ANSI 和 ISO 的银行信息系统安全标准 …… (128)
5.7.3 ISO 的安全结构和安全框架标准 …… (129)
5.7.4 美国政府标准(FIPS) …… (130)
5.7.5 Internet 标准和 RFC …… (130)
5.7.6 PKCS …… (131)
5.7.7 其他 …… (132)
第 6 章 卡技术 …… (133)
6.1 引论 …… (133)
6.2 卡应用简介 …… (133)
6.3 IC 卡简介 …… (133)
6.3.1 IC 卡发展简史 …… (134)
6.3.2 IC 卡分类(一) …… (134)
6.3.3 IC 卡分类(二) …… (136)
6.4 智能卡操作系统 COS 简单介绍 …… (137)
6.4.1 COS 的基本构成 …… (137)
6.4.2 卡内文件的数据结构 …… (138)
6.4.3 卡的安全机制 …… (139)
6.5 影响卡安全的几个问题 …… (140)
6.5.1 制造阶段的安全 …… (140)
6.5.2 运输阶段的安全 …… (140)
6.5.3 客户化阶段的安全 …… (141)
6.5.4 使用阶段的安全 …… (141)
6.5.5 销毁阶段的安全 …… (141)
6.5.6 技术上无法防范的安全问题 …… (141)
6.6 我国金融 IC 卡介绍 …… (141)
6.5.1 《规范》命令集 …… (142)
6.6.2 《规范》定义的应用类别和交易种类 …… (143)
6.6.3 金融 IC 卡应用安全机制 …… (143)
6.7 智能卡在电子商务中的作用 …… (144)
6.7.1 智能卡和电子商务 …… (144)
6.7.2 电子商务中使用金融卡的购物过程 …… (145)
6.7.3 电子支付方案设计 …… (146)
6.8 Mondex 电子现金卡简介 …… (147)
6.9 Multos 卡简介 …… (147)
6.10 VisaCash 简介 …… (148)
第 7 章 电子商务中的支付系统 …… (149)
7.1 支付系统的特点 …… (149)
7.1.1 支付手段 …… (149)

7.1.2 网上支付系统 …… (150)
7.1.3 iKP 协议 …… (152)
7.2 电子信用卡系统 …… (152)
7.2.1 系统描述 …… (152)
7.2.2 安全的电子交易 SET …… (154)
7.2.3 First Virtual …… (157)
7.2.4 CyberCash …… (159)
7.3 电子支票和电子资金转账 …… (160)
7.3.1 电子资金转账 …… (160)
7.3.2 电子支票系统 …… (160)
7.3.3 电子支票中的安全方案 …… (162)
7.3.4 NetBill …… (163)
7.3.5 NetCheque …… (163)
7.4 电子现金 …… (164)
7.4.1 系统描述 …… (164)
7.4.2 电子现金中的安全方案 …… (165)
7.4.3 DigiCash …… (167)
7.4.4 CAFE …… (168)
7.4.5 NetCash …… (169)
7.5 电子税收系统 …… (171)
7.6 发展我国 Internet 上金融系统的几个亟待解决的问题 …… (172)
第 8 章 医疗信息系统与电子商务 …… (174)
8.1 医疗信息系统 …… (174)
8.1.1 医疗信息系统概述 …… (174)
8.1.2 案例介绍 …… (176)
8.2 医疗系统中的电子商务 …… (179)
8.2.1 管理式医疗 …… (180)
8.2.2 医疗系统中的电子商务 …… (180)
8.3 医疗系统电子商务解决方案介绍 …… (182)
8.3.1 网组成部分介绍 …… (184)
8.4 医疗系统电子商务安全问题 …… (188)
第 9 章 Internet 上的信息出版发行系统及版权保护 …… (193)
9.1 Internet 上的电子出版发行系统概述 …… (193)
9.1.1 对电子出版系统的结构和协议方面的要求 …… (194)
9.1.2 电子出版物的安全分配系统 …… (195)
9.1.3 接入控制 …… (195)
9.1.4 文件递送和演示 …… (196)
9.2 数字版权保护技术的分类 …… (196)

9.2.1 锁定数据盒 …… (197)
9.2.2 标记数据 …… (197)
9.2.3 版权标记需具备的特征[5,8] …… (197)
9.2.4 版权保护基础设施 …… (198)
9.3 锁定数据技术 …… (199)
9.3.1 锁定 CD-ROM …… (199)
9.3.2 Internet 环境下的锁定 …… (200)
9.3.3 硬件锁定 …… (201)
9.3.4 潜在泄露 …… (202)
9.4 隐匿标记方法 …… (203)
9.4.1 信源编码隐匿标记方法 …… (203)
9.4.2 信道编码隐匿标记方法 …… (204)
9.4.3 空白间隔编码隐匿标记方法 …… (205)
9.4.4 同态集编码隐匿标记方法 …… (207)
9.4.5 像素修正编码隐匿标记方法 …… (208)
9.4.6 组合隐匿标记方法 …… (209)
9.4.7 波形变换技术隐匿标记方法 …… (209)
9.5 版权保护软件 …… (209)
9.5.1 Digimare …… (210)
9.5.2 Stego 和 EzStego …… (210)
9.5.3 S-Tool …… (210)
9.6 版权保护的法律问题 …… (211)
第 10 章 网上虚拟商店 …… (214)
10.1 网上虚拟商店概况 …… (214)
10.1.1 网上虚拟商店逻辑结构 …… (214)
10.1.2 网上虚拟商店各部分的软件构成 …… (215)
10.1.3 电子购物的数据流程 …… (216)
10.2 Sun 电子商务联盟电子商场解决方案 …… (217)
10.2.1 系统组成 …… (217)
10.2.2 Sun 联盟电子商场方案的核心技术 …… (218)
10.2.3 网上商店的前台系统 …… (219)
10.2.4 网上商店的支付 …… (220)
10.2.5 Sun 电子商务联盟电子商场解决方案的特点 …… (220)
10.3 IBM 的电子商场解决方案 …… (221)
10.4 HP 的电子商场解决方案 …… (222)
10.5 微软公司的电子商场 …… (223)
10.5.1 Microsoft Commerce Server …… (223)
10.5.2 开发环境 Microsoft Visual InterDev (VI) …… (223)

10.5.3 管理工具 …… (224)
10.6 实例介绍 …… (224)
第 11 章 基于 Java 的电子商务实例分析 …… (230)
11.1 技术基础 …… (230)
11.2 系统背景 …… (231)
11.3 系统介绍 …… (232)
11.3.1 基本服务 …… (232)
11.3.2 网络平台 …… (232)
11.3.3 技术标准 …… (234)
11.3.4 软件结构 …… (234)
11.3.5 数据安全保障 …… (237)
11.4 系统应用介绍 …… (238)