



北京市高等教育精品教材立项项目



高等院校规划教材
信息管理与信息系统系列

电子商务安全

朱建明 王秀丽 李 洋 等编著



机械工业出版社
CHINA MACHINE PRESS

高等院校规划教材·信息管理与信息系统系列
北京市教育委员会共建项目专项资助
中央财经大学科研创新团队支持计划资助

电子商务安全

朱建明 王秀利 李 洋 等编著



机械工业出版社

本书全面、系统地分析了电子商务面临的安全问题,在此基础上,深入阐述了实现电子商务安全的基本理论、方法、技术和策略。全书共 10 章,包括电子商务安全概述、密码学基础、软件安全、操作系统安全、数据库安全、网络安全、电子商务安全体系结构、电子商务网站安全、电子支付中的安全机制和电子商务安全管理等。每章均配有学习要点、关键词和思考题,理论联系实际,引导读者自主学习和思考。

本书既可作为高等院校电子商务、信息管理与信息系统、管理科学与工程、计算机科学与技术、信息安全等相关专业本科生、研究生的教材,也可作为相关领域研究人员、技术人员和管理人员的参考书。

本书配套授课电子课件,需要的教师可登录 www.cmpedu.com 免费注册、审核通过后下载,或联系编辑索取(QQ: 2399929378, 电话: 010-88379750)。

图书在版编目(CIP)数据

电子商务安全 / 朱建明等编著. —北京: 机械工业出版社, 2012.9

高等院校规划教材·信息管理与信息系统系列

ISBN 978-7-111-39843-1

I. ①电… II. ①朱… III. ①电子商务—安全技术—高等学校—教材
IV. ①F713.36

中国版本图书馆 CIP 数据核字(2012)第 226194 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

责任编辑: 王 凯

责任印制: 李 妍

北京诚信伟业印刷有限公司印刷

2013 年 1 月第 1 版·第 1 次印刷

184mm×260mm·19.75 印张·488 千字

0001—3000 册

标准书号: ISBN 978-7-111-39843-1

定价: 39.90 元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

电话服务

网络服务

社服务中心: (010) 88361066

教材网: <http://www.cmpedu.com>

销 售 一 部: (010) 68326294

机工官网: <http://www.cmpbook.com>

销 售 二 部: (010) 88379649

机工官博: <http://weibo.com/cmp1952>

读者购书热线: (010) 88379203

封面无防伪标均为盗版

出版说明

计算机技术在科学研究、生产制造、文件传媒、社交网络等领域的广泛应用，极大地促进了现代科学技术的发展，加速了社会发展的进程，同时带动了社会对计算机专业应用人才的需求持续升温。高等院校为顺应这一需求变化，纷纷加大了对计算机专业应用型人才的培养力度，并深入开展了教学改革研究。

为了进一步满足高等院校计算机教学的需求，机械工业出版社聘请多所高校的计算机专家、教师及教务部门针对计算机教材建设进行了充分的研讨，达成了许多共识，并由此形成了教材的体系结构与编写原则，策划开发了“高等院校规划教材”。

本套教材具有以下特点：

- 1) 涵盖面广，包括计算机教育的多个学科领域。
- 2) 融合高校先进教学理念，包含计算机领域的核心理论与最新应用技术。
- 3) 符合高等院校计算机及相关专业人才培养目标及课程体系的设置，注重理论与实践相结合。
- 4) 实现教材“立体化”建设，为主干课程配备电子教案、教材和实验实训项目等内容，并及时吸纳新兴课程和特色课程教材。
- 5) 可作为高等院校计算机及相关专业的教材，也可作为从事信息类工作人员的参考书。

对于本套教材的组织出版工作，希望计算机教育界的专家和老师能提出宝贵的意见和建议。衷心感谢广大读者的支持与帮助！

机械工业出版社

前 言

电子商务作为一种新兴商务形式,为商家和消费者提供了极大的便利。然而,安全问题仍然是目前阻碍电子商务发展的最大障碍。如何建立安全、便捷的电子商务应用环境,已经成为广大商家和消费者都十分关心的问题。本书正是在这种背景下,结合编者多年教学积累的经验编写的。

本书从技术与管理相结合的角度介绍电子商务安全,其特色主要表现在以下3个方面。

1) 将信息安全理论与商务过程相结合。对于电子商务的特殊环境和要求来说,不仅要有计算机网络安全的支持,还需要结合商务交易的过程和要求,研究相应的安全理论与技术。编者认为电子商务安全与一般的信息安全不同,重点应放在如何将计算机网络安全与商务交易安全的结合上。将信息安全理论与技术同商务过程相结合,在电子商务交易过程的每一个环节中嵌入安全机制,将安全技术与商务过程融为一体,而不仅仅是作为一种支撑。

2) 重视电子商务安全中的非技术因素,加强电子商务安全管理。在电子商务中,安全理论与技术是基础和重点。但是,仅仅依靠安全技术是不够的,还必须重视电子商务安全的非技术因素,如电子商务安全管理机制的建立、安全管理规范的健全等。

3) 突出案例教学。在介绍电子商务安全理论与技术、管理方案的同时,介绍国内外典型的案例与方案,并对其进行充分的分析,使学生加深对安全理论与技术的理解。

本书是中央财经大学精品课程建设成果。全书共分为10章。计划总学时为54学时,其中理论部分为44学时,实验部分为10学时。每章的内容及建议学时如下。

第1章,电子商务安全概述。主要介绍电子商务面临的安全威胁、安全技术和目前的研究现状。4学时。

第2章,密码学基础。主要介绍密码理论与技术的基本研究领域以及使用的主要密码技术。6学时。

第3章,软件安全。针对软件设计、编程以及测试等过程中常见的安全问题进行阐述,从而设计开发出安全可靠的软件系统。4学时。

第4章,操作系统安全。介绍安全策略与安全模型,通过实例说明安全操作系统的设计,并给出安全操作系统的评测方法与评估准则。6学时。

第5章,数据库安全。主要介绍数据库访问控制、多级安全数据库管理系统及其原型系统 and 产品。4学时。

第6章,网络安全。介绍网络安全威胁和安全控制,尤其是防火墙、入侵检测系统和安全的电子邮件。4学时。

第7章,电子商务安全体系结构。在介绍电子商务系统信息技术架构的基础上,提出了一种可生存的电子商务安全体系结构。4学时。

第8章,电子商务网站安全。介绍电子商务网站的安全需求与安全设计,并对Web服务器安全、用户隐私和网络“钓鱼”进行了描述。4学时。

第9章,电子支付中的安全机制。在分析电子商务安全协议的基础上,重点对当前电子支付中的安全机制进行分析。4学时。

第10章，电子商务安全管理。分析技术因素和非技术因素对电子商务安全的影响，重点介绍电子商务安全管理的内容、电子商务安全评估与效益分析和电子商务安全的法律规范等。4学时。

此外，每章均包括学习要点、关键词（中英文对照）、小结和思考题，以最大限度地满足教与学的需要。

本书以编者丰富的学习、工作经历，以及长期在信息安全领域从事科研与教学取得的成果为基础编写而成。第1、7、9、10章由中央财经大学朱建明编写，陈洁、李丹丹参加了部分内容的编写；第4、6、8章由王秀利编写；第2、3、5章由李洋编写。全书由朱建明统筹全稿。

编者在完成本书的过程中参阅了大量的文献，其中包括专业书籍、学术论文、学位论文、国际标准、国内标准和技术报告等，书中有部分引用已经很难查证原始出处，编者注明的参考文献仅仅是获得相关资料的文献，没有一一列举出所有的参考文献，在此表示歉意和谢意。

感谢中央财经大学对本书编写给予的支持。

由于编者水平有限，本书错误与疏漏之处在所难免，敬请广大读者批评指正。

编 者

目 录

出版说明

前言

第 1 章 电子商务安全概述	1
1.1 电子商务简介	1
1.1.1 信息化社会的发展与面临的挑战	1
1.1.2 电子商务的现状与发展趋势	3
1.2 电子商务的安全威胁	5
1.2.1 电子商务的安全现状与安全需求	6
1.2.2 电子商务面临的安全威胁	7
1.2.3 构建安全电子商务环境	11
1.3 电子商务安全技术	12
1.4 小结	15
思考题	15
参考文献	16
第 2 章 密码学基础	17
2.1 密码理论与技术概述	17
2.1.1 基本理论与概念	17
2.1.2 密码学的发展历程	19
2.1.3 经典密码学	22
2.2 对称密码体制	27
2.2.1 对称密码体制概述	27
2.2.2 数据加密标准—DES	29
2.2.3 高级加密标准—AES	33
2.2.4 对称密码算法的运行模式	36
2.3 公钥密码体制	40
2.3.1 公钥密码体制概述	40
2.3.2 RSA 算法	41
2.3.3 Diffie-Hellman 算法	42
2.3.4 ECC 算法	44
2.4 数字签名技术	48
2.4.1 DSA 算法	48
2.4.2 ECDSA 算法	49
2.5 公钥基础设施 (PKI)	50
2.5.1 数字证书	50

2.5.2	PKI 的基本组成与功能	53
2.5.3	常用信任模型及信任路径	59
2.6	国产密码算法	62
2.7	小结	62
	思考题	63
	参考文献	63
第 3 章	软件安全	64
3.1	软件安全概述	64
3.1.1	软件安全隐患的表现	64
3.1.2	软件安全隐患的成因	65
3.2	软件生命周期的安全问题	67
3.2.1	软件开发生命周期回顾	67
3.2.2	软件安全威胁建模	68
3.2.3	软件安全性测试	69
3.2.4	软件维护和漏洞响应	70
3.3	基本安全编程	70
3.3.1	内存安全	70
3.3.2	线程/进程安全	73
3.3.3	输入安全	78
3.4	应用编程安全	80
3.4.1	面向对象的编程安全	80
3.4.2	Web 编程安全	83
3.4.3	权限控制	89
3.4.4	远程调用和组件安全	92
3.5	软件安全测试	97
3.5.1	软件安全问题测试	97
3.5.2	安全审查	100
3.5.3	软件性能优化	101
3.6	小结	109
	思考题	109
	参考文献	110
第 4 章	操作系统安全	111
4.1	安全操作系统概述	111
4.2	安全策略与安全模型	114
4.2.1	安全策略	114
4.2.2	安全模型	117
4.3	安全操作系统设计	121
4.3.1	设计原则	121

4.3.2	设计方法	123
4.3.3	设计举例	125
4.4	安全操作系统评测	130
4.4.1	操作系统的典型缺陷	130
4.4.2	评测方法与评估准则	131
4.5	小结	143
	思考题	143
	参考文献	143
第5章	数据库安全	145
5.1	数据库安全概述	146
5.1.1	数据库安全威胁	146
5.1.2	数据库安全的需求	146
5.1.3	数据库安全的发展	148
5.2	数据库访问控制	150
5.2.1	访问控制分类	150
5.2.2	自主访问控制	150
5.2.3	强制访问控制	152
5.2.4	安全数据视图模型	154
5.3	多级安全数据库管理系统	159
5.3.1	多级安全数据库的关键问题	159
5.3.2	多级安全数据库的体系结构	160
5.3.3	多级关系数据模型	164
5.3.4	多实例	168
5.3.5	多级安全数据库事务并发处理	171
5.3.6	隐蔽通道分析	176
5.4	多级安全数据库原型系统和产品	180
5.4.1	多级安全数据库原型系统及产品概览	180
5.4.2	多级安全数据库原型系统	181
5.4.3	多级安全数据库产品	184
5.5	小结	188
	思考题	188
	参考文献	188
第6章	网络安全	190
6.1	网络安全威胁	190
6.1.1	威胁分类	190
6.1.2	对网络本身的威胁	191
6.1.3	对网络中信息的威胁	201
6.2	网络安全控制	209

6.2.1	数据加密	209
6.2.2	虚拟专有网络	214
6.2.3	PKI 与证书	214
6.2.4	身份鉴别	216
6.2.5	访问控制	219
6.3	防火墙	220
6.3.1	防火墙概述	220
6.3.2	防火墙的类型	221
6.3.3	防火墙配置举例	225
6.4	入侵检测系统 (IDS)	227
6.4.1	IDS 概述	227
6.4.2	IDS 的类型	228
6.5	电子邮件安全	231
6.5.1	电子邮件安全概述	231
6.5.2	安全电子邮件系统示例	233
6.6	小结	235
	思考题	235
	参考文献	235
第 7 章	电子商务安全体系结构	236
7.1	电子商务系统的信息技术架构	236
7.1.1	电子商务信息平台	237
7.1.2	电子商务系统的定义和结构	237
7.1.3	电子商务系统的信息技术架构	240
7.2	电子商务的网络安全体系结构	240
7.2.1	电子商务安全体系结构的安全维	241
7.2.2	电子商务安全体系结构的安全层	242
7.2.3	电子商务安全体系结构的安全面	243
7.3	一种可生存的电子商务安全体系结构	244
7.3.1	可生存的安全策略	244
7.3.2	可生存的电子商务安全策略模型	246
7.3.3	一种可生存的电子商务安全体系结构介绍	247
7.4	小结	249
	思考题	249
	参考文献	249
第 8 章	电子商务网站安全	250
8.1	电子商务网站安全需求与安全设计	250
8.1.1	电子商务网站安全需求	250
8.1.2	电子商务网站安全设计	251

8.1.3 旅游电子商务网站建设技术规范 (GB/T 26360—2010)	252
8.2 Web 服务器安全	258
8.3 用户隐私	260
8.4 网络“钓鱼”	263
8.5 小结	267
思考题	267
参考文献	267
第9章 电子支付中的安全机制	268
9.1 电子支付概述	268
9.1.1 电子支付现状	268
9.1.2 信用卡	271
9.1.3 电子支票	272
9.1.4 电子现金	273
9.2 网上银行支付系统	275
9.2.1 网上银行支付系统概述	275
9.2.2 网上银行支付系统的特点及安全风险	275
9.2.3 第三方支付	277
9.3 电子支付安全协议	278
9.3.1 安全套接层 (SSL) 协议	278
9.3.2 安全电子交易 (SET) 协议	280
9.3.3 安全支付协议—3D-Secure	283
9.3.4 Netbill 协议	284
9.3.5 DigiCash 协议	285
9.4 小结	286
思考题	286
参考文献	286
第10章 电子商务安全管理	288
10.1 电子商务的安全管理	288
10.1.1 电子商务面临的安全管理问题	288
10.1.2 电子商务的信息安全管理体系	290
10.1.3 电子商务的安全管理需求	292
10.1.4 电子商务安全管理的内容	293
10.2 电子商务安全管理方法	294
10.2.1 安全评估	294
10.2.2 安全政策	297
10.2.3 安全标准	298
10.2.4 安全审计	299
10.3 电子商务安全的相关法律规范	299

10.3.1 电子商务中的信息安全法律和规定	300
10.3.2 国际互联网络行业市场准入	300
10.3.3 互联网内容管理	301
10.3.4 网络安全的保护	301
10.3.5 网络保密管理	302
10.4 小结	302
思考题	302
参考文献	302

第1章 电子商务安全概述

[本章学习要点]

- 了解电子商务发展现状和安全需求。
- 了解电子商务面临的安全威胁和常用的安全技术。

[本章关键词]

电子商务 (E-commerce); 信息安全 (Information Security)。

随着社会信息化水平的不断提高,电子商务日益普及。在日常工作和生活中,人们越来越依赖电子商务系统进行各种商务活动,越来越多地通过计算机网络存储和传递机密信息。2011年12月某网站的安全系统遭到黑客攻击,数百万用户的登录名、密码及邮箱遭到泄露。同时,国内多家知名网站也被黑客攻击,有近千万用户的密码遭到黑客泄露。这些事件的发生,再一次提醒人们保护客户隐私的重要性。在信息化社会,人们要像保护个人财产一样保护个人信息资料。本章简要介绍电子商务所面临的安全威胁和常用的安全技术。

1.1 电子商务简介

1.1.1 信息化社会的发展与面临的挑战

1. 信息化社会的发展

自从1946年世界上第一台电子计算机诞生以来,经过几十年的快速发展,通信、计算机和半导体技术的发展已经将人类社会推进到一个崭新的信息时代。特别是互联网(Internet)的出现,20世纪90年代开始的通信、计算机和消费电子(3C——Communications, Computers, Consumer Electronics)的结合,信息高速公路或全球信息基础设施(GII)的建设,构成了人类生存的信息环境,即信息空间(Cyberspace)。这个虚拟空间的形成和发展将人类社会推进到了一个新的发展阶段,即信息化社会。

在信息化社会中,信息的作用越来越大,社会对信息的需求也越来越大。通信、广播、影视、出版等正在从模拟到数字,从单一媒体到多媒体,从人工、机械化到智能化,从局部联网到全球通信网。Internet的出现为人类交换信息,促进科学、技术、文化、教育、生产的发展,提高现代人的生活质量提供了极大的便利,大大加速了人类社会的发展进程。预计到2025年,所有的信息传输都将数字化,灵巧的个人终端将为人们提供各种各样的服务,个人终端将通过几十米至几千米的无线信道与光纤等骨干网连通,通向世界。

1993年9月,美国以《国家信息基础设施:行动计划》的出版为标志启动了美国国家信息基础设施(NII/GII)计划,该行动计划明确了美国国家信息基础设施建设的总体目标:通

过发展高等级的国家信息基础设施和保持美国在全球信息基础设施中的领先地位，使美国公民享用广泛的信息资源及信息服务。

1994 年 3 月，在由国际电讯联盟（ITU）主持召开的首届世界电讯发展会议上，时任美国副总统的戈尔号召世界各国积极参与建设全球信息基础设施，得到了世界各国的广泛响应。目前，美国的信息基础设施建设已经取得了很大的成效。美国网络数据监测公司 ComScore 发布的 2006 年 6 月份全球互联网用户活跃性报告显示，全球上网人数达到 7.13 亿，其中 21% 的用户来自美国，11% 来自中国，还有 7% 的用户来自日本。美国所有州和主要地方政府的机构、重要媒体、各个产业部门的主要企业和提供社会服务的机构均已连接互联网。

在由互联网驱动的全球电子商务活动中，目前美国的交易额居世界第一位。此外，北美地区的加拿大，欧洲的爱尔兰、瑞典、丹麦、英国、德国，亚太地区的澳大利亚、新西兰、新加坡、韩国、日本等国家信息基础设施建设的速度都很快，电子商务、电子政务得到了快速发展。

我国信息化进程起步较晚但发展很快。我国提出“全面认识工业化、信息化、城镇化、市场化、国际化深入发展的新形势新任务”，首次把信息化与其他“四化”并列。在国家统一规划和组织下，在农业、工业、科学技术、国防及社会生活各个方面应用现代信息技术，深入开发、广泛利用信息资源，加速实现国家现代化的进程。

2009 年，中国科学院发布的《中国至 2050 年信息科技发展路线图》指出，从 2010 年至 2050 年，我国信息科技发展路线图的总目标是：抓住信息技术跃变的机遇，提升自主创新和可持续发展能力，使我国全面进入信息社会，绝大多数中国人成为信息用户，信息成为中国经济和社会发展最重要的资源，社会信息化总体上接近国外发达国家水平。总的任务是要构建“惠及全民、以用户为中心、无所不在的信息网络体系（Universal, User-oriented, Ubiquitous Information Network Systems, U-INS）”。

由此可见，在日常工作和生活中，人们会越来越依赖计算机网络，越来越多地使用各种信息系统来处理各种数据，无论是学校的学籍管理、图书管理，还是银行的账户管理、信用卡管理等，无不需要信息系统的支持。信息已经成为一种重要的战略资源，信息的获取、处理和安全保障能力成为一个国家综合国力的重要组成部分。同时，电子商务会更加普及。因此，信息系统的一次故障或事故会造成巨大的影响，甚至是灾难。特别是对于金融、电力等关键信息系统而言，信息安全就更加重要。

2011 年 7 月 19 日，中国互联网络信息中心（CNNIC）在北京发布了《第 28 次中国互联网络发展状况统计报告》（以下简称《报告》）。《报告》显示，截至 2011 年 6 月底，中国网民规模达到 4.85 亿，较 2010 年底增加 2770 万人，增幅为 6.1%，网民规模增长减缓；最引人注目的是，在大部分娱乐类应用使用率有所下滑、商务类应用呈平缓上升的同时，微博用户数量以高达 208.9% 的增幅，从 2010 年底的 6311 万增长到 1.95 亿，成为用户增长最快的互联网应用模式。同时指出微博“领跑”网络应用，电子商务进入平稳上升期。网络安全诚信问题比较严峻，互联网安全需加强。由此可以看出，电子商务进入一个成熟成长期，同时电子商务安全问题也日益突出。

2. 信息化社会面临的挑战

信息化社会是一个信息技术占主导地位，信息产业成为主导产业，信息经济是其主要经济形态，信息资源变成重要经济资源，信息、知识和智力决定发展力量的社会。在信息化社会，人们会面临许多新的挑战。

(1) 信息过量, 难以消化

美国《纽约时报》由 20 世纪 60 年代的 10~20 版扩张至现在的 100~200 版, 最高曾达 1572 版; 而人均日阅报时间通常为 30~45 分钟, 只能浏览一份 24 版的报纸。现在无论是日报、晚报还是其他报纸, 其版面基本都在几十版以上, 普通人一天完整地读一份报纸都很难, 更不用说“博览群报”了。网络上的信息就更多了, 即时更新, 新闻不断, 谁也不可能掌握所有的信息。究其原因, 可以用下面的公式来表示:

数据生产、传输能力 >> 数据分析能力

一方面人们被数据“淹没”, 另一方面人们却“饥饿”于知识。如何从大量的数据中获取有用的信息是信息化社会所面临的最大挑战。

(2) 信息真假, 难以辨识

在 Internet 普及的今天, 人们既是信息的获取者, 也是信息的发布者。博客、微博、BBS、即时通信系统 (QQ 和 MSN 等) 都成为人们发布信息、交流信息的工具。如何辨别信息的真假成为一个难题。

(3) 信息的表示不一致, 难以统一处理

随着信息技术的发展, 信息的表示形式也是多种多样的。数值、文字、图形、图像、声音、视频等多媒体信息成为信息的主要表示方式。信息表示不一致, 增加了统一处理信息的难度。

(4) 信息系统的质量难以保证

随着社会信息化水平的不断提高, 信息系统与计算机网络的基础性、全局性作用日益增强, 人们对信息系统的依赖程度越来越高。人们的工作、生活都离不开各种各样的信息系统, 如办公自动化系统、科研项目申报系统、学籍管理信息系统、视频点播系统等成为人们生活和工作的一部分。但是信息系统的质量难以保证, 信息系统故障会严重影响人们的生活和工作。

(5) 信息安全难以保证

随着网络拓扑结构和应用复杂度的增加, 现有信息系统安全机制的脆弱性也暴露无遗, 针对信息系统的攻击屡有发生。因此, 信息系统安全的重要性与日俱增, 如何保障信息系统安全已经成为信息化过程中必须解决好的重大问题。信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分。

下面是近年来发生的几起典型的信息系统安全事件和信息系统故障:

1) 2007 年 8 月 11 日, 由于美国洛杉矶国际机场的海关计算机系统发生故障, 造成约 6000 名乘客滞留机场长达 6 小时。

2) 2011 以来, 一些网银用户频频遭遇“钓鱼”, 被窃取账户资金, 产生动辄数十万元、上百万元的损失, 据了解, 多家银行为防范用户资金风险, 已经下调了网银转账限额, 此外, 除了下调转账额度, 部分银行的网银使用也多了很多防范措施, 如通过与手机绑定、手机短信验证码来确保账户的安全; 还有动态密码、静态密码等。

因此, 面对快速发展的信息化社会, 如何安全有效地开展电子商务活动就成为一个重要的课题。

1.1.2 电子商务的现状与发展趋势

电子商务 (E-commerce) 作为一个完整的概念出现于 20 世纪 90 年代, 它并非是单纯的

技术概念或单纯的商业概念，而是现代信息技术和现代商业技术的结合体。

广义的电子商务，是指通过信息技术、网络互连技术和现代通信技术使得商业交易涉及的各方当事人借助电子方式联系，而无需依靠纸面文件完成单据的传输，实现整个交易过程的电子化。简单地说，电子商务就是指利用计算机网络进行的商务活动，它的实质应该是一套完整的网络商务经营思想及管理信息系统。狭义的电子商务，是指利用 Internet 进行商业交易的一种方式，主要指信息服务、交易和支付，它的主要内容包括：电子商情广告，电子选购和交易、电子交易凭证的交换，电子支付与结算等。

1. 电子商务模式

按照交易对象，电子商务主要有以下 5 种模式。

1) B2B 模式：企业对企业（Business to Business）的电子商务，指企业之间通过 Internet 进行产品、服务及信息的交换，如图 1-1a 所示。B2B 是电子商务的主要模式，如阿里巴巴是全球 B2B 电子商务的著名品牌，汇集海量供求信息，是全球领先的网上交易市场和商人社区。

2) B2C 模式：企业对消费者（Business to Consumer）的电子商务，指企业对消费者的电子商务，主要指通过 Internet 开展的在线销售，如图 1-1b 所示，如企业在线直销（如 Dell 计算机）、零售商的电子商务（如 Amazon、当当网等）、第三方交易平台等。

3) B2G 模式：企业对政府（Business to Government）的电子商务，具体形式是网上政府采购。如中国政府采购网已经成为国家级政府采购的专业网站和电子化政府采购平台。

4) G2C 模式：政府对公民（Government to Citizen）的电子商务，是政府通过电子政务系统为公民提供各种服务。G2C 模式所包含的内容十分广泛，如公众信息服务、电子身份认证、电子税务、电子社会保障服务、电子民主管理、电子医疗服务、电子就业服务、电子教育、培训服务、电子交通管理等。

5) C2C 模式：消费者对消费者（Consumer to Consumer）的电子商务，主要是网上拍卖，如淘宝网、拍拍网等。

中国电子商务研究中心于 2011 年 1 月发布的《2010 年度中国电子商务市场数据监测报告》显示，2010 年我国电子商务已经进入大规模发展、应用和运营的阶段，无论是 B2B 企业电子商务，还是消费者个人的电子商务（B2C、C2C、团购等），新模式、新平台、新特征都层出不穷。

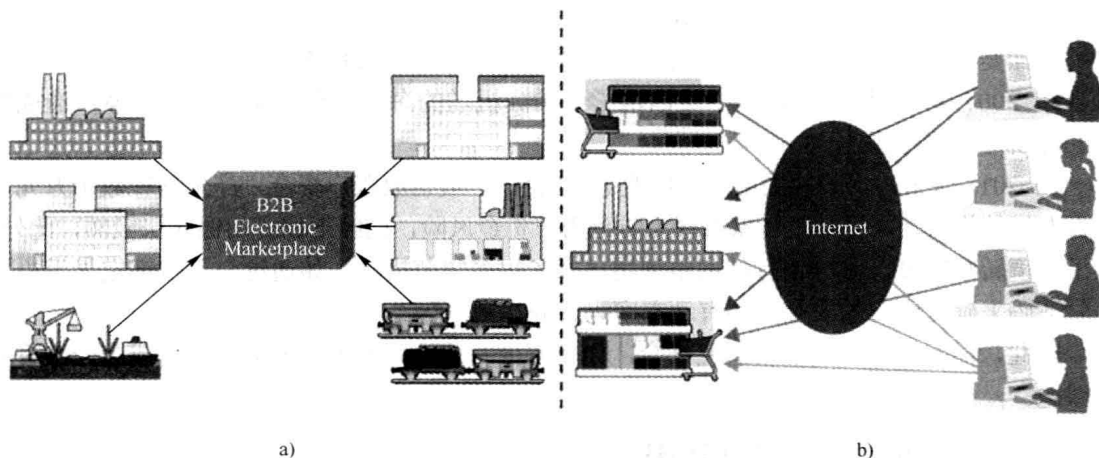


图 1-1 电子商务模式

a) B2B 模式 b) B2C 模式

2. 电子商务的现状与发展趋势

经过几十年的发展，电子商务已经成为商务活动的重要形式，并且仍然处于快速发展的过程中。以下是一些政府部门和咨询机构发布的研究报告：

- 据中国电子商务研究中心的数据显示，截止到2010年12月，中国电子商务市场交易额已逾4.5万亿，同比增长22%。其中B2B电子商务交易额达到3.8万亿，同比增长15.8%，增速有所放缓，但行业整体仍保持稳定发展态势；网上零售市场交易规模达5131亿元，同比增长97.3%，较2009年近翻一番，约占全年社会零售总额的3%。
- 2010年8月30日，中国商务部在北京发布了《中国电子商务报告（2008-2009）》。报告显示，2008年，中国电子商务交易额达到3.1万亿元人民币，网络购物交易额达到1257亿元人民币；2009年，中国电子商务交易额达到3.8万亿元人民币，网络购物交易额达到2586亿元人民币，同比分别增长21.7%和105.8%，其中网络购物交易额占社会消费品总额的2.06%。
- 2011年9月14日，由中国旅游研究院主办、搜狐旅游协办的《中国旅游电子商务发展报告》学术成果发布会在北京举行。该研究成果显示，2010年中国旅游电子商务（基于互联网平台的在线旅游业交易）市场规模达到2000亿元人民币，占整体旅游收入份额将近15%。在旅游市场持续扩容和信息技术广泛应用的双重推动下，不同类型、不同模式的旅游电子商务主体得以快速发展。调查显示，影响游客使用线上旅游公司服务的最大的3个因素分别是：难以辨别网上信息的真伪（49.8%）、担心网上支付的安全问题（46.8%）和对线上公司的信誉有疑惑（43.5%）。

以上这些数据显示出我国电子商务的快速发展对国民经济的影响越来越大。

与此同时，信息安全也成为影响电子商务发展的重要因素。2011年1月，信息安全厂商瑞星公司发布了《瑞星2010年度安全报告》。报告指出，2010年，黑客和病毒制作者基于实际经济利益原因，开始大量深度进入电子商务领域。保守估计，2010年黑客仅通过网络广告、恶意推广购物导航链接获取的单项不法收入就高达3~5亿元。

中国电子商务研究中心于2011年1月发布的《2010年度中国电子商务市场数据监测报告》总结了未来电子商务发展的特征趋势，同时指出了今后中国电子商务行业发展的隐忧——电子商务中的“网络安全问题日渐突出”。电子商务交易的安全，是严重制约电子商务发展的一大瓶颈。安全问题是实施电子商务的首要问题，也是最重要的问题。电子商务的运作，涉及资金安全、信息安全、货物安全、商业秘密安全等。电子商务安全问题如果不能妥善解决，电子商务的实现就是一句空话。目前一些用户不愿进行网上交易，也是因为对网上交易的安全性、可靠性持怀疑态度。

1.2 电子商务的安全威胁

随着社会信息化水平的不断提高，以及电子政务与电子商务的快速发展，信息系统与计算机网络的基础性、全局性作用日益增强，国民经济与社会活动之间的依赖关系不断加强。在日常工作和生活中，人们越来越依赖信息系统，越来越多地通过信息系统管理企业的产、供、销、人、财、物，越来越多地使用计算机网络来传递敏感信息。

电子商务是新兴商务形式，而信息安全的保障是电子商务实施的前提。信息安全技术