



普通高等教育“十一五”国家级规划教材
高职高专电子商务专业课程改革规划教材

business e-business e-business e-business e-business e-business e-business e-bu

电子商务安全

第2版



王忠诚 主编

business

机械工业出版社
CHINA MACHINE PRESS



赠电子课件

普通高等教育“十一五”国家级规划教材

高职高专电子商务专业课程规划教材

电子商务安全

第2版

主 编 王忠诚

副主编 潘维琴 贾晓丹

参 编 詹 磊 方世强 敖静海

曲晓芳 曹启武

机械工业出版社

本书主要围绕保障电子商务活动的安全性,针对电子商务应用的基本安全问题及解决方案进行了详细介绍与阐述。全书共分8章,分别介绍了电子商务安全概述、电子商务安全面临的问题及解决方法、电子商务安全技术、电子商务的认证与安全电子邮件技术、电子商务安全支付技术、安全电子交易(SET)协议、安全套接层(SSL)协议、安全电子商务应用等内容,并根据每章的具体内容安排了相应的习题和实践实训环节。

本书内容新颖,结构合理,案例生动,论述深入浅出,实用性强,突出对基本理论、基本技能的掌握和技术应用能力的培养。本书可作为高职高专电子商务、市场营销、计算机应用、计算机信息管理、工商管理 and 经济贸易等专业的教材,也可作为有关电子商务的培训用书以及企业管理人员参考用书。

本书配有电子教案及习题参考答案,凡使用本书作为教材的教师可登录机械工业出版社教材服务网 www.cmpedu.com 下载。咨询邮箱: cmpgaozhi@sina.com。咨询电话:010-88379375。

图书在版编目(CIP)数据

电子商务安全/王忠诚主编. —2版. —北京:机械工业出版社,2009.5

普通高等教育“十一五”国家级规划教材. 高职高专电子商务专业课程改革规划教材

ISBN 978-7-111-26980-9

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

中国版本图书馆CIP数据核字(2009)第065040号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)

策划编辑:王玉鑫 责任编辑:张芳

版式设计:霍永明 责任校对:李婷

封面设计:王伟光 责任印制:李妍

北京振兴源印务有限公司印刷厂印刷

2009年7月第2版第1次印刷

184mm×260mm·16.25印张·389千字

0001—4000册

标准书号:ISBN 978-7-111-26980-9

定价:28.00元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

销售服务热线电话:(010) 68326294

购书热线电话:(010) 88379639 88379641 88379643

编辑热线电话:(010) 88379771

封面无防伪标均为盗版

第2版前言

本书是普通高等教育“十一五”国家级规划教材。本书第1版出版以来，受到了多家高职高专院校电子商务专业及相关专业师生的广泛好评，得到了社会其他人士的认可和肯定。

在广泛吸纳各方建议的基础上，在保留第1版主体框架和基本特色的前提下，突出对基本技能的掌握和技术应用能力的培养，吸收电子商务理论及实践领域的最新研究成果，对全书的内容进行了修订。

与第1版相比，本书的主要特色表现在以下几个方面：

1. 整合内容体系

第2版的内容体系主要从电子商务安全基础、电子商务安全问题、电子商务安全技术以及电子商务安全实际应用四个方面进行章的划分。这种划分使电子商务安全的层次更加分明，这种结构安排能够更加体现电子商务安全的全貌，让学生在学的同时体会电子商务各知识点之间的关系，增加学习的灵活性。

2. 增加全新案例

第2版中保留第1版中的精华内容，加大了对电子商务安全技术和方法的研究，尤其是加入了最新的案例，让学生在解决案例的过程中完成相关课程内容的学习和操作。

3. 加大实践操作

在第2版编写中仍旧坚持电子商务安全的实践应用环节。对原有的过时的实践操作内容进行了更新和更换，尤其在原有的实践基础上，根据企业应用现状增加了一些新的实践内容。

4. 对全书重点内容进行摘要式介绍

为了方便学习，在第2版中还增加了摘要式的全书重点内容总结，系统讲解了电子商务安全中的重要问题，既起到引导学生学习电子商务安全的导航作用，又能够作为教师讲授该门课程的教学大纲。

全书共分8章，分别介绍了电子商务安全概述、电子商务安全面临的问题及解决方法、电子商务安全技术、电子商务的认证与安全电子邮件技术、电子商务安全支付技术、安全电子交易（SET）协议、安全套接（SSL）协议、安全电子商务应用等。

由于是面向高职高专学生的教材，所以，本书在理论上以够用为度，结合案例，深入浅出，实用性强，突出对基本理论、基本技能的掌握和技术应用能力的培养，使学生尽快掌握电子商务安全知识及其应用技术。本书力求内容丰富、形式简练，既考虑学生的自我学习，也考虑给教师留下一定的教学空间。本书既可作为高职高专院校的教材，也可作为各界人士的学习用书及专业培训用书。

本书由辽宁机电职业技术学院王忠诚主编，辽宁机电职业技术学院潘维琴、贾晓丹担任副主编，具体分工如下：浙江机电职业技术学院詹磊编写了第1章的1.1、1.2.1、1.2.2、1.3

节；辽宁机电职业技术学院贾晓丹编写了第2章，第3章的3.1~3.3节，第6章的6.5节，各章案例及全书总结；北京城市学院方世强编写了第3章的3.4~3.6、3.7.1~3.7.3节；北京联合大学敖静海编写了第4章的4.1~4.3节，第8章；辽宁机电职业技术学院潘维琴编写了第5章；北京市供销学校曲晓芳编写了第6章的6.1~6.2、6.3.2、6.4节；辽宁机电职业技术学院曹启武编写了第7章；王忠诚编写了第1章的1.2.3节，第3章的3.7.4节，第4章的4.4、4.5节，第6章的6.3.1节。全书由王忠诚负责统稿、修改、补充、定稿。贾晓丹对全书进行了校对。

本书在编写过程中参考或引用了大量专家学者的论著、图书及网站资料，作者已尽可能在参考文献中列出，谨在此对他们表示衷心的感谢，若有疏漏，也在此表示歉意。由于编者水平所限，加之多人编写，书中难免有不妥之处，敬请读者批评指正。

编 者

第 1 版前言

随着信息技术、网络技术和 Internet 的飞速发展,电子商务成为越来越多的人关注的焦点。电子商务使得人们可以在网上通过建立网站树立自己企业的形象,发布自己的产品信息,宣传产品广告,提供售后服务,甚至可以进行网上谈判、电子合同签订、电子交易和资金结算等。但是,事物的发展都存在两面性,一方面电子商务给我们带来了便利,同时在进行电子商务活动时,需要在 Internet 上传输消费者和商家的一些机密信息,如用户信用卡号、商家用户信息和订购信息等,而这些信息一直是网络非法入侵者或黑客的攻击目标。如何保证电子商务安全,如何对敏感信息和个人信息提供机密性保障、认证交易双方的合法身份以及保证数据的完整性和交易的不可否认性等,已经成为电子商务发展的瓶颈,对这些问题的担心也是导致很多人不愿意进行网上购物和支付的主要原因。

本书主要讲述电子商务安全的基本知识与实际应用。主要内容为电子商务安全概述、信息安全技术、网络与应用系统安全技术、电子商务的认证与安全电子邮件技术、电子商务支付技术、安全电子交易 (SET) 协议、安全套接层 (SSL) 协议和安全电子商务应用等内容,并根据每章的具体内容安排了相应的练习与实训题。

由于是面向高职高专学生的教材,所以,教材在理论上以够用为度,结合案例,深入浅出,实用性强,突出对基本理论、基本技能的掌握和技术应用能力的培养,使学生尽快掌握电子商务安全知识及其应用技术。本书内容丰富、形式简练,既考虑学生的自我学习,也考虑给教师留下一定的空间。因此,本书既可作为高职高专院校的教材,也可作为有关专业人士的参考用书及专业培训用书。

本书由王忠诚担任主编,潘维琴担任副主编。詹磊编写了第 1 章;贾晓丹编写了第 2 章;方世强编写了第 3 章;敖静海编写了第 4、8 章;潘维琴编写了第 5 章;曲晓芳编写了第 6 章;曹启武编写了第 7 章;王忠诚编写了第 3~6 章中的 3.2.5、3.3.4、4.5.1、4.5.2、4.5.3、5.7、6.3.1、6.5 节。全书由王忠诚负责统稿、修改、补充、定稿。贾晓丹对全书进行了校对。

本书在编写过程中参考或引用了大量专家学者的论著,图书及网站资料,作者已尽可能在参考文献中列出,谨在此对他们表示衷心的感谢,若有疏漏,也在此表示歉意。由于编者水平所限,加之多人编写,书中难免有不妥之处,敬请读者批评指正。

编 者

目 录

第2版前言

第1版前言

第1章 电子商务安全概述	1	3.2.2 非对称加密体制	41
1.1 电子商务及其系统构成	1	3.2.3 公钥密钥与对称密钥技术的综合应用	44
1.1.1 电子商务的定义、内涵及特征	1	3.2.4 密钥管理与自动分配	45
1.1.2 电子商务系统构成	5	3.3 数字签名	46
1.2 电子商务安全概况	8	3.3.1 数字签名概述	46
1.2.1 电子商务安全概念与特点	8	3.3.2 数字签名实现方法	47
1.2.2 电子商务的风险与安全问题	10	3.3.3 数字签名的算法	48
1.2.3 电子商务系统安全的构成	14	3.3.4 数字签名的过程	48
1.3 电子商务安全的保障	18	3.3.5 数字签名的标准	50
1.3.1 电子商务安全技术	18	3.4 防火墙	51
1.3.2 电子商务安全国际规范	20	3.4.1 防火墙概述	51
1.3.3 电子商务安全法律要素	21	3.4.2 防火墙的关键技术	53
实践项目	22	3.4.3 防火墙技术发展动态和趋势	56
练习与实训题	22	3.4.4 防火墙系统的设计	57
案例分析	24	3.4.5 选择防火墙的原则	59
第2章 电子商务安全面临的主要问题及解决方法	25	3.4.6 主流防火墙产品介绍	60
2.1 电子商务安全面临的主要问题	25	3.4.7 防火墙应用举例	63
2.1.1 网络信息安全目标	25	3.5 虚拟局域网	66
2.1.2 网络信息系统中的威胁与对策	28	3.5.1 VPN 概述	66
2.1.3 网络信息安全管理原则	33	3.5.2 VPN 技术	69
2.2 电子商务安全整体解决方法	33	3.5.3 VPN 服务器配置	70
2.2.1 电子商务安全体系概述	33	3.5.4 IPSec 协议	73
2.2.2 电子商务安全解决方法	33	3.6 入侵检测系统	75
实践项目	35	3.6.1 入侵检测概念	75
练习与实训题	35	3.6.2 入侵检测系统的模型	76
案例分析	36	3.6.3 入侵检测系统的功能	76
第3章 电子商务安全技术	37	3.6.4 入侵检测系统的分类	77
3.1 数据加密技术概述	37	3.6.5 入侵检测技术	79
3.1.1 密码学的基本概念	37	3.6.6 入侵检测系统的部署	80
3.1.2 网络加密方式分类	38	3.6.7 入侵检测的局限性	81
3.2 加密算法	39	3.6.8 入侵检测技术发展方向	82
3.2.1 对称加密体制	39	3.7 反病毒技术	82
		3.7.1 计算机病毒概述	82
		3.7.2 计算机病毒检测方法	86

3.7.3 计算机病毒的预防措施	87	5.1 支付技术及其发展	141
3.7.4 病毒举例	89	5.1.1 支付活动	141
实践项目	91	5.1.2 电子商务与电子支付	144
练习与实训题	92	5.2 电子商务支付系统概述	146
案例分析	94	5.2.1 电子商务支付系统的构成	152
第4章 电子商务的认证与安全电子邮件技术	95	5.2.2 电子支付系统的功能	152
4.1 PKI 概述	95	5.2.3 电子交易模型	153
4.1.1 PKI 技术的含义	95	5.3 电子现金	156
4.1.2 PKI 的组成及功能	95	5.3.1 电子现金的定义与特性	156
4.1.3 PKI 的性能要求	98	5.3.2 电子现金的使用	158
4.1.4 轻型目录访问协议	98	5.4 电子信用卡与电子钱包	158
4.1.5 PKI 技术标准	99	5.4.1 电子信用卡	158
4.2 证书和认证系统	100	5.4.2 电子钱包	162
4.2.1 PKI 系统的常用信任模型	100	5.5 电子支票	164
4.2.2 数字证书	103	5.5.1 电子支票的定义	164
4.2.3 认证中心	108	5.5.2 电子支票的使用	165
4.3 Windows 2000 PKI 在电子商务中的应用	110	5.5.3 电子支票系统的安全问题	166
4.3.1 Windows 2000 PKI 概述	110	5.5.4 电子支票的发展	168
4.3.2 Windows 2000 PKI 的公钥基础结构	110	5.6 微支付系统	170
4.3.3 Windows 2000 PKI 公钥基础结构的证书服务	110	5.6.1 微支付的设计目标	170
4.3.4 Windows 2000 PKI 的实际应用案例	118	5.6.2 微支付系统设计技术	171
4.3.5 智能卡	119	5.6.3 微支付系统简介	173
4.4 认证实训——个人数字证书申请	119	5.7 电子支付实训——中国建设银行网上支付	174
4.5 安全电子邮件技术实训	124	5.7.1 申请建设银行“网上银行”业务	175
4.5.1 安全电子邮件概述	124	5.7.2 开通建设银行“网上银行”	175
4.5.2 电子邮件	127	5.7.3 “网上银行”转账体验	176
4.5.3 安全电子邮件系统	129	5.7.4 支付宝转账演示	178
4.5.4 安装个人数字证书	130	5.7.5 网上购物	179
4.5.5 在邮件上签名	134	实践项目	182
4.5.6 邮件加密	136	练习与实训题	182
实践项目	139	案例分析	183
练习与实训题	139	第6章 安全电子交易协议	184
案例分析	140	6.1 SET 协议概述	184
第5章 电子商务安全支付技术	141	6.1.1 SET 协议的由来	184
		6.1.2 网上购物与现实中购物的比较	185
		6.1.3 SET 协议的主要目标	186
		6.1.4 SET 协议中的相关成员	187
		6.2 SET 协议的相关技术	187
		6.2.1 SET 协议的双重签名技术	188

6.2.2 SET 协议的认证技术	188	7.3.2 身份认证	213
6.3 SET 购物与支付处理流程	192	7.3.3 会话层的密钥分配协议	213
6.3.1 SET 购物流程	192	7.4 SSL 协议分析	214
6.3.2 支付处理流程	194	7.4.1 对协议安全性的分析	214
6.4 SET 协议的安全性分析	195	7.4.2 SSL 协议与 SET 协议的比较	215
6.5 安全电子交易实训	196	7.5 SSL 协议的应用	219
6.5.1 申请一张中国银行长城电子 借记卡	196	实践项目	221
6.5.2 获得并安装中银电子钱包	197	练习与实训题	221
6.5.3 申请电子证书	198	案例分析	222
6.5.4 进行网上购物	200	第 8 章 安全电子商务应用	223
6.5.5 电子钱包高级功能	201	8.1 中国金融认证中心系统	223
实践项目	205	8.1.1 概述	223
练习与实训题	205	8.1.2 CFCA 证书的类型及应用	225
案例分析	206	8.1.3 CFCA 普通证书的使用	225
第 7 章 安全套接层协议	207	8.1.4 CFCA 高级证书的使用	230
7.1 SSL 协议概述	207	8.1.5 CFCA 证书在 B2B 交易中的 应用	234
7.1.1 SSL 协议	207	8.2 网上证券系统	235
7.1.2 SSL 协议的安全交易过程	208	8.2.1 概述	235
7.1.3 SSL 协议的安全通道	208	8.2.2 网上证券交易安全解决方案	237
7.1.4 SSL 协议的基本安全服务	209	实践项目	240
7.2 SSL 协议的原理	209	练习与实训题	240
7.2.1 SSL 握手协议	209	案例分析	241
7.2.2 SSL 记录协议	211	全书内容总结	242
7.3 SSL 协议的加密和认证算法	212	练习与实训题答案	247
7.3.1 加密算法	213	参考文献	250

第1章 电子商务安全概述



本章提要

- 1) 电子商务的内涵及系统构成。
- 2) 电子商务的安全问题及系统构成。
- 3) 电子商务安全保障问题。

20世纪90年代以来,计算机网络技术取得了快速发展,信息网络化和全球化成为不可阻挡的世界潮流。计算机网络技术一直在寻求除文字处理和信息传递领域外的更大、更直接的发展空间,商业领域成为首选,而迅速膨胀的网络用户也为网上更广泛的商业活动的开展提供了基础。

Web技术的广泛应用,不仅使它具有通信和交换信息的功能,还开辟了一种新的商业交易方式,即在互联网上进行商业交易,实现电子交易处理。

互联网潮流所带来的优势和商机,彻底改变了全球商业的经营模式,许多非信息产业也投入其中,在互联网上可以看到各式各样的商业站点林立。如今,电子商务几乎涉及到人类生活的各个层面和领域。电子商务正在迅速发展,它推动了商业、贸易、营销、金融、广告、运输和教育等社会经济领域的创新和发展,并因此形成了一个新的产业,给各国企业和经济带来新的机遇。此外,越来越多的企业渴望通过导入电子商务来进行业务流程的重组改造,提升企业运作效率、降低经营成本,并且更进一步地优化商品和服务的品质。企业导入电子商务已经成为增强市场竞争力的主要动力。

由此可见,作为网络与商业的结合,电子商务是网络化发展的必然产物,是信息时代的商务模式,它必将有更广阔的发展前景。不过,电子商务绝不是空中楼阁,它的实现需要强有力的技术支撑,在互联网这个公共平台上,依赖强有力的技术支持,尤其是安全技术保障显得尤为重要。

1.1 电子商务及其系统构成

1.1.1 电子商务的定义、内涵及特征

近几十年来,商业领域中使用了多种电子通信工具来完成各种交易活动。银行使用电子资金转账(EFT)技术在全球范围内转移顾客的资金;各种企业使用电子数据交换技术,利用增值网(VAN)发出订单和各种凭证;零售商针对各种商品做电视广告以吸引顾客来通过电话订货。因而,从更广的意义上来说,电子商务可以通过多种电子通信手段来完成,电子商务早已有之;从狭义上来说,电子商务则是指利用互联网进行的商务活动。

对电子商务的定义至今仍不是一个很清晰的概念。各国政府、学者、企业界人士都根据自己所处的地位和对电子商务的参与程度,给出了许多表述不同的定义。比较这些定义,有助于我们更全面地了解电子商务的内涵。

1. 电子商务的定义

(1) 世界电子商务会议关于电子商务的定义 1997年11月6~7日,在法国首都巴黎,

国际商会举行了世界电子商务会议 (The World Business Agenda For Electronic)。

关于电子商务的概念阐述为: 电子商务 (Electronic Commerce) 是指对整个贸易活动实现电子化。

从交易媒体上说, 电子商务是交易各方以电子交易方式而不是通过当面交换或直接面谈方式进行的任何形式的商业交易; 从技术角度分析, 它是一种多技术的集合体, 包括交换数据 (EDI, 电子邮件)、获得数据 (共享数据库, BBS) 以及自动捕获数据 (Bar Code) 等技术; 从其涵盖范围来看, 包括信息交换、售前售后服务、销售、电子支付、运输配送、组建虚拟企业、公司和贸易伙伴共同拥有的商业方法等。

(2) 政府部门对电子商务的定义 欧洲议会关于电子商务给出的定义是: “电子商务是通过电子方式进行的商务活动。它通过电子方式处理和传递数据, 包括文本、声音和图像。它涉及许多方面的活动, 包括货物电子贸易和服务、在线数据传递、电子资金划拨、电子证券交易、电子货运单证、商业拍卖、合作设计和工程、在线资料、公共产品获得。它包括了产品 (如消费品、专门设备) 和服务 (如信息服务、金融和法律服务)、传统活动 (如健身、体育) 和新型活动 (如虚拟购物、虚拟训练)。”

(3) 权威学者对电子商务的定义 美国学者瑞维·卡拉科塔和安德鲁·B·惠斯顿在他们的专著《电子商务的前沿》中提出: “广义地讲, 电子商务是一种现代商业方法。这种方法通过改善产品和服务质量、提高服务传递速度, 满足政府组织、厂商和消费者降低成本的需求。这一概念也用于通过计算机网络寻找信息以支持决策。一般地讲, 今天的电子商务通过计算机网络将买方和卖方的信息、产品和服务联系起来, 而未来的电子商务则通过构成信息高速公路的无数计算机网络将买方和卖方联系起来。”

(4) IT (信息技术) 行业对电子商务的定义 IT (信息技术) 行业是电子商务的直接推动者 (设计者和设备制造者), 出于各自的商业目的, 它们各自提出自己对电子商务的定义。

IBM 公司认为, 电子商务 (Electronic Business) 指的是采用数字化电子方式进行商务数据交换和开展商务业务活动; 是在互联网的广阔联系与传统信息技术系统的丰富资源相结合的背景下应运而生的一种相互关联的动态商务活动。通过电子商务系统将商务活动各方 (商店、消费者、银行、信息公司、企业、政府等) 连接起来, 利用计算机网络技术全面实现在线电子交易。

IBM 公司关于电子商务的描述, 可以用一个公式来概括, 即 $\text{电子商务} = \text{Web} + \text{IT}$ 。它强调的是在网络计算环境下的商业化应用, 是把买方、卖方、厂商及其合作伙伴在互联网 (Internet)、企业内部网 (Intranet) 和企业外部网 (Extranet) 结合起来的應用。

HP 公司提出电子商务是以跨时域、跨地域的电子化世界 E-World, $\text{EW} = \text{EC} (\text{Electronic Commerce}) + \text{EB} (\text{Electronic Business}) + \text{EC} (\text{Electronic Consumer})$ 。E-World 就是电子化连接世界, 就是通过电话、电缆、卫星、无线载波等一切通信介质, 将数据、声音、图像和视频等一切信息传向每一台 PC、每一个公用电话亭、每一种个人通信设备, 传向世界的每一个角落。HP 公司将所有可能的贸易伙伴 (用户、商品和服务的供应商、承运商、银行、保险公司以及所有其他外部信息源的受益人) 包括在其电子商务的范畴内。

在我国, 上海市电子商务安全证书管理中心给电子商务下的定义是 “电子商务 (EC) 是指采用数字化电子方式进行商务数据交换和开展商务业务活动。电子商务主要包括利用电子数据交换 (EDI)、电子邮件 (E-mail)、电子资金转账 (EFT) 及互联网的主要技术在个人间、企业间和国家间进行无纸化的业务信息的交换。”

以上定义是不同协会、公司、政府和专家在实践应用的基础上,从不同角度所做的各自的总结。

1997年10月,欧洲经济委员会在比利时布鲁塞尔召开了全球信息社会标准大会,明确提出过一个关于电子商务的比较严密完整的定义。这可被视为一个经全球化权威机构认定的标准化定义:

“电子商务是各参与方之间以电子方式而不是以物理交换或直接物理接触方式完成任何形式的业务交易”。这里的电子方式包括电子数据交换(EDI)、电子支付手段、电子订货系统、电子邮件、传真、网络、电子公告系统条码、图像处理和智能卡等。

笔者认为,在考察关于电子商务的定义时,应注意 E-Business 与 E-Commerce 的区别,并由此得到广义和狭义电子商务的概念,有助于更好地理解电子商务的概念。

狭义电子商务(Electronic Commerce)也被称作电子交易,是指利用互联网开展的销售和购买信息、产品和服务等交易行为。其包含的要素为互联网和交易。可以理解为互联网技术和现代商务的一个交集,如图1-1所示。

电子商务不仅仅局限于在线买卖,它将从生产到消费各个方面影响商务活动的方式。因此它具有广告宣传、咨询洽谈、网上订购、网上支付、服务传递、意见征询及交易管理等功能。

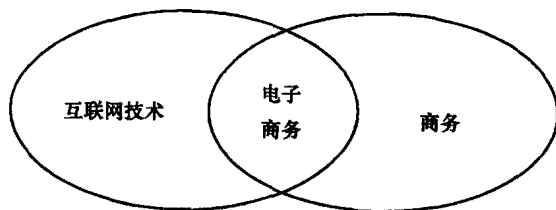


图 1-1 电子商务是“互联网技术”和“商务”两个子集的交集

广义电子商务(Electronic Business)指的是企业利用现代化信息技术开展的一切商务活动,如市场分析、客户联系、物资调配等。它既包括网上交易,还包括企业内部业务活动(如计划、生产、财务管理等)以及企业之间的协作与协调。其可利用的网络平台包括不同形式的各类网络。

利用包括 Internet、Intranet、Extranet 等各种计算机网络以及其他信息技术进行的所有的企业活动都归属于电子商务。

也有人把广义的电子商务系统称为企业电子商务系统,这个电子商务系统是以实体企业的基本职能和业务模块为背景构造和运行的。

2. 电子商务的内涵

无论广义还是狭义的定义,它们应当具有比较一致的内涵:

1) 电子商务的本质是“商务”,是在“电子”基础上的商务。“商务”解决做什么的问题,而“电子”则解决怎么做的问题。对于高科技的应用是电子商务的手段和效果,而非目的。

2) 电子商务的前提是商务信息化。计算机应用和信息化建设是其基础。它不只是在网上销售商品,还应和企业内部管理、售后服务支持等结合起来,这样的连接必须依靠企业管理信息化。

3) 电子商务的核心是人。电子商务是一个社会系统,它的中心必然是人。电子商务的出发点和归宿是商务,商务的中心是人或人的集合。电子工具的系统化应用也只能靠人。电子商务涉及的人员目前可以分为三类:第一类是技术人员,他们主要负责电子商务系统的实现和技术支持;第二类是商务人员,他们主要负责各种商务活动具体业务的处理;第三类是中高级管理人员,他们的职责是电子商务战略规划、业务流程管理、安全管理等。

4) 电子商务是对传统商务的改良而不是革命。从本质上来说,电子商务并没有脱离传统

商务的业务流程,而是将传统商务赖以生存的实物市场交易移到了虚拟的网络空间,在传统环境下开展商务活动的关键因素仍然不可缺少。

5) 电子工具必定是现代化的。所谓现代化工具是指当代技术成熟、先进、高效、低成本、安全、可靠和方便操作的电子工具。

6) 对象的变化也是至关重要的。以往的商务活动主要是针对实物商品进行的商务活动,电子商务则首先要将实物的商品虚拟化,形成信息化(数字化和多媒体化)的虚拟商品,进而对虚拟商品进行整理、储存、加工传输。

广义电子商务和狭义电子商务的关系如图1-2所示。

3. 电子商务的特征

正如前文所述,电子商务是将企业的业务方式进行改造,业务流程进行改良,即是将信息流、物流和资金流进行分类和重组,以电子化方式通过网络来实现。这一切都必然要依赖于电子商务所蕴含的技术特征和应用特征。

(1) 电子商务的技术特征 主要包括:

1) 信息化。电子商务是以信息技术为基础的商务活动,它的进行必须通过计算机网络系统来实现电子化信息的交换和传输。电子商务的发展是与信息技术的发展密切相关,正是信息技术的发展推动了电子商务的发展。

2) 虚拟性。电子商务是在数字化的虚拟电子市场(Electronic Marketplace)进行的。电子商务不受物理的时空概念的限制。

3) 集成性。电子商务是一种新兴产物,其中用到了大量新技术,但并不是说新技术的出现就必须导致老设备的死亡。互联网的真实商业价值在于协调新老技术,使用户能更加行之有效地利用他们已有的资源和技术,更加有效地完成他们的任务。

电子商务的集成性,还在于事务处理的整体性和统一性,它能规范事务处理的工作流程,将人工操作和电信息处理集成为一个不可分割的整体。这样不仅能提高人力和物力的利用,也提高了系统运行的严密性。

4) 可扩展性。要使电子商务在变化的商业环境里正常运行,必须保证其可扩展性。电子商务中,耗时仅2min的重新启动也可能导致大量客户流失,因而可扩展性极其重要。

1998年日本长野冬奥会的官方万维网节点的使用率是有史以来基于互联网应用中最高,在短短的16天,该节点就接受了将近6亿5千万次访问。全球体育迷将数以百万计的信息直接通过体育迷电子邮件节点发给运动员,而与此同时,还成交了600多万笔交易。这些惊人的数字说明,随着技术的日新月异,电子商务的可扩展性将不会成为瓶颈所在。

5) 安全性。安全性是电子商务中的核心问题。缺乏安全的电子商务不可能吸引顾客,企业和企业之间的交易更是如此,也会限制企业运用计算机网络传递商业信息。欺骗、窃听、病毒和非法入侵等攻击行为都无时无刻不在威胁着电子商务,要求电子商务经营者提供一种端到端的安全解决方案。安全技术包括加密解密机制、认证技术、安全交易协议、计算机网络系统的安全管理(存取管理、防火墙、安全服务器等)。目前,有代表性的安全电子交易协议主要有安全套接层(SSL)和安全电子交易(SET)等。电子商务安全技术的发展和标准的制定,



图 1-2 广义电子商务和狭义电子商务

逐步使电子商务企业能够建立起安全的电子商务环境。

6) 系统性。电子商务系统的实施必须考虑企业外的合作伙伴或政府, 必须规划如何加入到已有的电子商务系统中。

(2) 电子商务的应用特征 主要包括:

1) 商务性。电子商务最基本的应用特性为商务性, 即提供买、卖交易的服务、手段和机会。网上购物提供一种客户所需要的方便途径。因而, 电子商务对任何规模的企业而言, 都是一种机遇。

就商务性而言, 电子商务可以扩展市场, 增加客户数量; 通过将互联网信息连至企业后端的数据库, 企业能记录下每次访问、销售、购买形式和购货动态以及客户对产品的偏爱, 这样企业就可以通过统计这些数据来获知客户最想购买的产品是什么。

2) 服务性。电子商务时代企业越来越重视客户的需求, 这种需求不仅仅是产品的, 同时必然包括服务的。互联网应用使得企业能自动处理商务过程, 并不再像以往那样强调公司内部的分工。企业通过将客户服务过程移至互联网上, 使客户能以一种较过去简捷的方式获得服务。显而易见, 电子商务提供的客户服务具有一个明显的特性: 便利。例如比利时的塞拉银行, 通过电子商务, 使得客户能全天候地存取资金账户, 快速及时地阅览相关利率信息, 这使得服务质量大为提高。

3) 协调性。商务活动是一种需要各方协调的过程, 许多组织都提供了交互式的协议, 电子商务活动可以在这些协议上完成。

传统的电子商务解决方案能加强公司内部相互作用, 电子邮件就是其中一种。但那只是协调员工合作的一小部分功能。利用互联网将供货方连接至客户订单系统处理, 这样公司就节省了时间, 消除了纸张文件带来的麻烦并提高了效率。

4) 社会性。从宏观上讲, 电子商务是计算机网络的第二次革命, 是在通过电子手段建立一个新的经济秩序。它不仅涉及到电子技术和商业交易本身, 还涉及到诸如金融、税务、教育等社会其他层面, 以及使用电子虚拟市场的法律和竞争规则形成等。电子商务的发展和应用是一个社会性的系统工程, 缺少一个环节都势必影响它的发展, 如电子商务交易的税收等敏感问题。

5) 全球性。Internet 是一个公共开发的平台, 根据美国互联网协会的定义, 互联网是一种“组织松散、国际合作的互联网络”, 是一种由 TCP/IP 组织起来的国际互联网络。电子商务面对的是一个全球性统一的电子虚拟市场。它为企业跨国发展提供了平等的竞争机会。

1.1.2 电子商务系统构成

1. 电子商务系统的分类

在了解了电子商务的内涵后, 本节进一步讨论电子商务的分类和构成。对于不断发展的各类电子商务系统, 可以从不同的角度进行分类。

1) 按照商业活动的运作方式分类: 可以将电子商务分为纯电子商务和部分电子商务。当从商务涉及的产品 (Product)、过程 (Process)、交付代理 (Delivery agent) 三个维度上分析电子商务, 会发现传统商务在所有维度上都是物理的 (Physical), 而纯电子商务在所有维度上都是数字的 (Digital), 除此之外, 都属于部分电子商务, 它们是以数字和物理维度的结合来完成整个商务活动。

2) 按照使用网络的类型来分类: 基于 EDI 网络的电子商务, 就是利用 EDI 网络进行电子交易。简单地说, EDI 就是按照标准协议, 将商业文件标准化和格式化, 并通过网络在贸易伙伴的计算机网络系统之间进行的数据传输和自动处理。

基于内联网的电子商务，就是利用企业内部网络进行电子交易。Intranet 是企业为实现内部业务处理、管理和通信的目的，在采用互联网技术的基础上发展起来的企业内部专用网络。如同企业内部的 Internet。

基于互联网的电子商务，就是利用互联网进行电子交易。互联网电子商务是国际现代商业的最新形式。它以计算机、通信、多媒体和数据库技术为基础，通过互联网实现营销、购物服务。它突破了传统商业生产、批发、零售及进销存的流转程序与营销模式，真正实现了少投入、低成本、零库存及高效率。

3) 按照交易对象分类：

企业对企业的电子商务 (Business to Business, B2B)：在开放网络中对每笔交易寻找最佳伙伴，并与伙伴进行从订购到结算的全部交易活动。

企业对消费者的电子商务 (Business to Consumer, B2C)：等同于零售电子化，可销售诸如书籍、鲜花、计算机、汽车等。

企业对政府的电子商务 (Business to Government, B2G)：覆盖企业与政府之间的各项事务如政府采购、企业税收征收等。

消费者对政府的电子商务 (Consumer to Government, C2G)：涉及电子福利支付、电子资料库、电子身份认证等。

消费者对消费者的电子商务 (Consumer to Consumer, C2C)：消费者之间在网上进行一些多数为小额的交易，如通过互联网进行个人财务的拍卖活动等。

2. 电子商务的一般框架

电子商务是由计算机、通信网络及程序化、标准化的商务流程和一系列安全、认证法律体系组成的集合；是一种以互联网为基础、以交易双方为主体、以银行电子支付和结算为手段、以客户数据为依托的全新商务模式。

电子商务的一般框架是指实现电子商务的技术保证和电子商务应用所涉及到的领域。电子商务的技术支持分为三个层次和两个支柱。从最基础的技术层次到电子商务的应用层次分成网络层、消息/信息发布层和一般业务服务层三个层次，它们构成电子商务系统的基础设施，三个层次之上是特定的电子商务应用；两个支柱是各种技术标准和网络安全协议、公共政策及法律，它们构成了电子商务的基础环境，如图 1-3 所示。

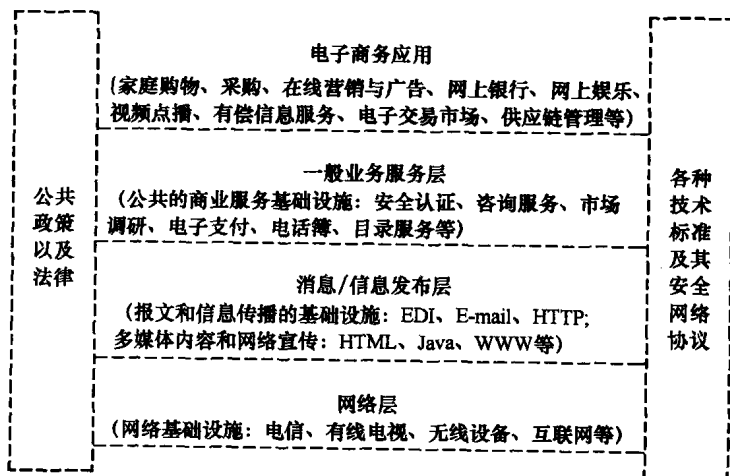


图 1-3 电子商务的一般框架

(1) 网络基础设施层 网络基础设施层是实现电子商务的最底层的基础设施，人们曾形象地把它称为“信息高速公路”。它是信息传输系统，包括远程通信网、有线电视网、无线通信网和互联网。

(2) 消息和信息发布层 信息传送有非格式化（非结构化）数据和格式化（结构化）数据两种通信方法。非格式化的数据传送方法有传真 (Fax)、电子邮件 (E-mail) 和文件传输服务

(FTP), 主要是面向人的。

格式化的数据传送的典型方法有电子数据交换(EDI)等, 它的传递和处理过程是自动化的, 无需人的干预。

超文本传输协议(HTTP)是互联网上通用的消息传播工具, 它以统一的显示方式, 在多种环境下显示非格式化的多媒体信息。超文本标记语言(HTML)将这些多媒体内容组织得易于检索和富于表现力。

(3) 一般业务服务层 这个层次是为了方便交易所提供的通用的业务服务, 是所有企业、个人在网上进行交易时都会用到的服务。所以我们将它们也作为基础设施。主要包括: 安全和认证、电子支付、目录服务、咨询服务等。业务服务的关键是安全电子支付, 为了保证网上支付是安全的, 就必须保证交易是保密的、真实的、完整的和不可抵赖的。

对于电子商务来说, 通常参与各方是互不见面的, 因此身份确认与安全通道变得非常重要。解决的方案是建立公正、权威、各方信赖的电子商务认证中心(CA), 用以确保安全和提供认证, 在有争议的时候还可以提供证据; 同时通过加密的方法实现网上安全的信息交换和安全交易。

(4) 电子商务应用 在上述三个层次的基础上, 建立面向企业的具体的电子商务应用, 即构成广义的电子商务系统。它涉及企业商务活动的各个方面, 包括供应商、客户、银行或金融机构、信息公司以及政府等。如家庭购物、企业的网上采购、在线营销与广告、网上银行、网上娱乐、视频点播、有偿信息服务、电子交易市场和供应链管理等。

(5) 支柱一: 公共政策及法律 与电子商务有关的公共政策涉及到电子商务的税收制度、信息的定价、信息访问权、隐私保护等问题。国际上, 各国对电子商务的框架立法工作十分重视。美国政府在《全球电子商务的政策》中, 对法律问题做了专门论述; 1996年联合国贸易组织通过了《电子商务示范法》; 我国于2004年8月28日也正式通过了《电子签名法》, 已经于2005年4月1日起施行。针对电子商务的立法还有待健全。

Internet的跨国界性还要求电子商务企业在开展跨国业务时, 除了要注重研究各国不同的国情、体制外, 还要考虑它们的文化和道德规范, 否则发生了冲突, 便会对电子商务的开展产生负面影响。

(6) 支柱二: 技术标准和网络协议 技术标准定义了用户接口、传输协议、信息发布标准、网络安全协议等技术细节, 是信息发布、传递的基础, 是网络上信息一致性的保证。

由于电子商务的全球性, 非国际化的技术标准将会带来严重的问题, 所以, 许多企业和国际组织都已经意识到技术标准的重要性, 正致力于联合开发统一的国际技术标准, 如EDI标准、SET协议、TCP/IP、XML标准、HTTP等技术标准和协议的制定就是例子。

我国目前在信息化建设方面还主要集中在基础建设方面, 在立法等方面比较滞后。在发达国家, 由于企业信息化程度高, 基础设施完备, 社会信用体系完善, 人们的法律意识较强, 这十分有益于电子商务的发展。在电子商务的推动下出现的金融电子化趋势、信息安全的方案、基于Internet应用方案等, 反过来又给信息技术带来新的发展机遇。

3. 电子商务系统的基本组成

电子商务系统的基本组成有计算机网络、用户、配送中心、认证中心、银行、商家等, 如图1-4所示。网络包括Internet、Intranet、Extranet; 用户分为个人用户和企

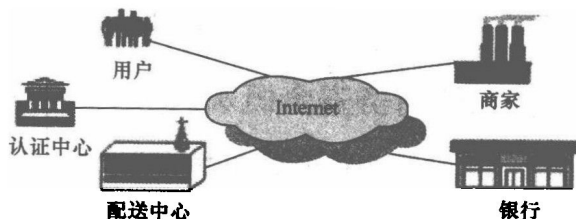


图 1-4 电子商务的基本组成

业用户；认证中心（CA）是受法律承认的权威机构，负责发放和管理电子证书，使网上交易的各方能互相确认身份；物流中心接收商家的送货请求，组织运送无法从网上直接得到的商品，跟踪商品的流向，将商品送到消费者手中；网上银行在 Internet 上实现传统银行的业务，为用户提供 24 小时实时服务。

4. 电子商务系统的结构

（1）客户机/服务器（C/S）结构 进入 20 世纪 80 年代以后，随着局域网技术的发展，以客户机/服务器（Client/Server, C/S）为核心的软件系统逐渐成熟起来。C/S 结构通过将任务合理分配到 Client 端和 Server 端，降低了系统的通信开销，可以充分利用两端硬件环境的优势。在 C/S 结构中一般配有高性能的专用服务器，服务器端安装数据库软件，负责对数据的存储和管理；客户机安装客户端程序，负责信息系统的图形显示、数据录入、业务处理等。数据库服务器软件运行在专用服务器上，大量的数据处理在服务器端完成，客户端主要提供与用户的交互功能，这样就提高了处理速度又减少了网络传输量，大幅提升了整个系统的性能。

其主要的缺点是开发的中心主要在客户端，即所谓胖客户机，造成系统维护和管理的困难。

（2）B/W/S 三层结构 进入 20 世纪 90 年代以后，随着互联网的快速发展，基于 Web 的软件系统结构逐渐发展起来，即 B/W/S（Browser/Web Server/Database Server）三层结构，有时也简称 B/S（Browser/Web Server）结构。B/W/S 结构的主要特点是“瘦客户机”，即客户端（一般就是一个浏览器）主要负责与用户的交互，而系统的绝大部分处理功能都在中间层（Web Server）上完成。B/W/S 结构实现了系统的分散应用和集中管理，任何经授权且装有标准浏览器的网上用户都可作为系统的客户端，基本无需维护的代价，极大地方便了应用管理，不必像 C/S 结构那样在每个客户端安装应用软件。B/W/S 结构无疑体现了互联网时代的优势。

目前大多数应用性软件系统都是 C/S 形式的两层结构，开发工具先进，应用成熟，对于复杂的事务处理具有较大优势，但是其功能受限于软件实现；B/W/S 三层结构则十分利于即时发布信息，以及与客户交互式沟通。在企业信息化的实际应用中，可采取二者结合的体系结构，各自担负其有优势的部分。如今，有越来越多的应用系统向 Web 架构转换。

（3）电子商务系统结构 电子商务系统充分利用计算机网络的先进技术，在典型的情况下，基于 B/W/S，又和企业后端的信息管理系统，如企业资源计划（ERP）连接起来，构成一个多层的结构。

1) 客户层。客户层直接面向用户。用于为用户提供企业电子商务系统的操作界面。

2) Web 服务层。Web 服务层向客户层提供满足用户需求的画面美观、布局合理的 Web 页面，还可以根据用户的具体要求而创建个性化和专业化的 Web 页面等。Web 服务层接受来自客户层的用户输入，并将其发送到应用服务层以得到处理。

3) 应用服务层。应用服务层接受 Web 服务层发来的请求，进行适当的业务处理，并访问企业信息系统层的资源。这一层通常是采用基于组件的方法，将业务逻辑封装于其间。

4) 企业信息系统层。企业信息系统层是指电子商务系统所对应的企业的后端信息系统。在一个简单的电子商务系统中，它对应的可能是一个关系型数据库，存储了必要的业务处理信息。

1.2 电子商务安全概况

1.2.1 电子商务安全概念与特点

在互联网早期，电子邮件是最常用的服务之一。在电子邮件出现后，人们一直担心电子邮件信息会被竞争者获取，从而对自己不利；公司的员工会担心与工作无关的邮件被公司或上司