

电子商务安全技术及应用

林 枫 等编著

北京航空航天大学出版社

<http://www.buaapress.com.cn>

内 容 简 介

随着信息技术 Internet 的飞速发展,电子商务,特别是通过 Internet 进行的电子商务成为越来越多的人关注的焦点,而由于 Internet 的开放性和其他各种因素的影响,安全一直是电子商务发展的瓶颈,也是很多人不愿意进行网上购物和支付的主要原因。本书作为一本电子商务安全的入门书籍,以通俗的语言阐述了目前电子商务安全的主要技术,内容包括电子商务基础、电子商务安全综述、网络安全技术、PKI 及证书系统、SSL 协议及应用、安全电子支付系统、安全电子交易 SET 和常见安全电子商务系统解决方案等。本书观点新颖、内容丰富、可读性和实践性强,力求以系统的观点和方法来阐述电子商务安全协议与理论,并配有详细的实例和解决方案。本书适合于任何对电子商务及其安全和网络安全感兴趣的读者,也可以作为大中专院校相关专业的教材。

图书在版编目(CIP)数据

电子商务安全技术及应用/林 枫等编著. —北京:北京航空航天大学出版社,2001.3

ISBN 7-81077-036-5

I. 电… II. 林… III. 电子商务 安全技术

IV. F713.36

中国版本图书馆 CIP 数据核字(2000)第 81508 号

电子商务安全技术及应用

林 枫 等编著

责任编辑 张光斌 范曼华

北京航空航天大学出版社出版发行

北京市学院路 37 号(100083)发行部电话:82317024 发行部传真:82328026

<http://www.buaapress.com.cn>

E-mail: pressell@publica.bj.cninfo.net

河北省涿州市新华印刷厂印刷 各地书店经销

*

开本:787×1092 1/16 印张:14.125 字数:362千字

2001年3月第1版 2001年3月第1次印刷 印数:5000册

ISBN 7-81077-036-5/TP·022 定价:21.00元

前 言

最近几年,Internet 作为通信技术、网络技术和信息技术的载体与表现形式,呈现了爆炸式的增长方式,而基于 Internet 的电子商务应用也得到了空前的发展,并出现了各种各样的商务交易方式和电子支付方式,电子商务网站也如雨后春笋般争相开放,给人们的购物方式、消费方式和生活观念带来了巨大的冲击,也更方便了人们的日常生活,真正实现了“足不出户,送货上门”的购物消费理念。

虽然电子商务在商务流程和购物流程电子化等方面积累了很多的经验,奠定了强大的技术基础和商务基础,但现在很多消费者不愿意或惧怕在网上进行购物和网上支付,究其原因,安全性一直是人们担心和关注的话题。当进行电子商务交易,特别是网络支付的时候,在公共的 Internet 网上需要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。如何保证电子商务交易的安全性,如何对敏感和个人信息提供机密性保障、认证交易双方的合法身份、保证数据的完整性和交易的不可否认性等,已经成为制约电子商务发展的瓶颈,也成为众多学者、研究开发人员、政府人员和管理人员关注的目标。

本书作为电子商务安全的入门或中级读物,没有讨论繁琐的数学推导和密码理论,而采用通俗的语言,以目前流行的安全协议为主线,并结合多种应用实例和解决方案,详细讨论了电子商务中所采用的安全技术和策略,对常用电子商务安全协议,如 SSL 和 SET 等进行了详细的分析,给出了部分应用实例。

本书共分为 8 章,主要包括电子商务技术、电子商务安全综述、网络安全技术、PKI 及证书认证系统、SSL 协议、安全电子支付系统、安全电子交易 SET 和常用安全电子商务解决方案等。

本书内容丰富,系统性强,跟踪了当前电子商务发展的许多热点,如 PKI 和安全电子支付等,既适合于作为电子商务安全和网络安全的入门教材,也可以作为从事电子商务和信息安全的技术人员和管理人员的参考资料。

本书的写作是安时 IT 安全小组全体成员集体劳动的结晶,其中包括张广生、单 肃、时健、巴伟业、黎成伦、王全胜、李 惠、杨 崎、张 盟、刘冬梅、王子玉等。本书在编写过程中得到了西安电子科技大学和上海交通大学多位老师和同学的帮助和支持,在此一并表示感谢。

由于作者水平有限,书中错误和疏漏之处在所难免,望读者和各位专家不吝赐教。

作者 林 枫

2000 年 12 月

目 录

第 1 章 电子商务综述

1.1 前 言	1
1.2 电子商务应用和发展	2
1.2.1 电子商务发展因素	2
1.2.2 世界电子商务发展	3
1.2.3 国内电子商务	4
1.3 电子商务范围和分类	6
1.3.1 电子商务范围	6
1.3.2 电子商务分类	6
1.3.3 EDI 和 B2B 电子商务	7
1.4 典型电子商务策略和方案	10
1.4.1 微软电子商务策略	10
1.4.2 IBM 电子商务应用框架	12
1.5 结束语	15

第 2 章 电子商务安全基础

2.1 电子商务安全威胁	17
2.1.1 电子商务安全威胁类别	17
2.1.2 电子商务安全威胁现状	19
2.2 电子商务安全需求	19
2.3 网络安全与密码技术	20
2.3.1 网络安全	20
2.3.2 密码技术	21
2.3.3 对称密钥加密	22
2.3.4 HASH 函数	23
2.3.5 公开密钥加密	25
2.3.6 混合密码系统	27
2.3.7 数字签名	28
2.4 认证系统	30
2.4.1 前 言	30
2.4.2 Kerberos 认证系统	31
2.5 证书和证书机构	34
2.5.1 网络安全中的信任关系	35
2.5.2 证书机构 CA	36
2.5.3 数字证书	37
2.5.4 X.509 证书	38

2.5.5	公钥基础设施 PKI	38
2.6	电子商务安全协议规范	41
2.6.1	TCP/IP 协议安全	41
2.6.2	安全 Sockets 协议	42
2.6.3	应用层安全协议	44
第 3 章 网络安全技术		
3.1	前 言	45
3.2	网络操作系统安全	47
3.2.1	Windows NT 安全性	47
3.2.2	Windows 2000 安全性	50
3.3	防火墙技术	54
3.3.1	防火墙简介	54
3.3.2	防火墙基本类型	56
3.3.3	防火墙系统	58
3.4	虚拟专用网 VPN 技术	59
3.4.1	VPN 基础	59
3.4.2	VPN 隧道协议	61
第 4 章 PKI 基础与证书系统		
4.1	PKI 基础	65
4.1.1	前 言	65
4.1.2	PKI 发展与应用	67
4.2	PKI 框架结构	68
4.2.1	PKI 组成与基础结构	68
4.2.2	证书机构 CA	69
4.2.3	证书管理	73
4.2.4	密钥管理	76
4.3	PKI 技术标准	77
4.3.1	前 言	77
4.3.2	证书和 CRL 格式	78
4.3.3	证书获取协议	85
4.3.4	证书管理协议	86
4.3.5	应用编程界面 API	87
4.3.6	PKI 策略	90
4.4	Windows 2000 PKI 技术	90
4.4.1	互操作性(Interoperability)	91
4.4.2	安全性(Security)	92
4.4.3	灵活性(Flexibility)	93

4.4.4 易用性.....	96
----------------	----

第 5 章 SSL 协议及其应用

5.1 前 言	104
5.2 SSL 协议说明	105
5.2.1 基本块大小(Basic block size)	106
5.2.2 向量(Vectors)类型	106
5.2.3 数字(Numbers)	106
5.2.4 枚举(Enumerate) 类型	107
5.2.5 结构类型(Constructed type)	107
5.2.6 常量(Constant)	108
5.2.7 加密属性(Cryptographic attribute)	109
5.2.8 SSL 协议状态	109
5.2.9 加密说明(CipherSpec)	110
5.3 记录层协议	111
5.3.1 数据分片或组合	111
5.3.2 记录数据单元的压缩和解压缩	112
5.3.3 记录的消息验证和加密	113
5.3.4 变换加密说明(Change cipher spec protocol)协议	115
5.3.5 警报协议	115
5.4 握手协议	116
5.4.1 协议流程与描述	116
5.4.2 问候消息(Hello message)	119
5.4.3 服务器证书和密钥交换	121
5.4.4 客户端证书和密钥交换	123
5.5 SSL 密钥管理	125
5.5.1 密钥产生	125
5.5.2 密钥交换	126
5.6 SSL 安全性	127
5.7 SSL 应用	128
5.7.1 SSL 应用流程	128
5.7.2 SSL 应用中的服务器配置	129

第 6 章 安全电子支付概论

6.1 前 言	140
6.1.1 类似于支付指令的支付系统	141
6.1.2 类似于电子货币转拨的支付系统	142
6.2 银行互联网支付系统(BIPS)	143
6.2.1 BIPS 系统结构模型	144

6.2.2	BIPS 系统组件结构	146
6.2.3	BIPS 安全性	150
6.3	电子支票(Echeck)	152
6.3.1	前言	152
6.3.2	操作模式	154
6.3.3	电子支票安全	157
6.3.4	电子支票的付款人系统	159
6.3.5	电子支票的收款人系统	161
6.4	微支付系统机制	162
6.4.1	前言	162
6.4.2	MilliCent 信任模型与安全	163
6.4.3	票据(Scrip)	164
6.4.4	MilliCent 协议	166
6.4.5	中间人(Brokers)	170
6.4.6	消费者、中间人和商家之间的交互	171

第7章 安全电子交易系统 SET

7.1	前言	174
7.1.1	SET 简介	174
7.1.2	SET 商业需求	175
7.1.3	SET 应用范围和购物流程	176
7.1.4	SET 外部技术标准	177
7.2	SET 基本概念	178
7.2.1	支付系统参与者(Payment System Participants)	178
7.2.2	加密基本概念(Cryptography)	179
7.2.3	证书发行(Certificate Issuance)	184
7.2.4	购物方式(Kinds of Shopping)	186
7.3	支付处理流程	186
7.3.1	持卡人注册(Cardholder registration)	188
7.3.2	商家注册(Merchant registration)	190
7.3.3	购买请求(Purchase request)	191
7.3.4	支付授权(Payment authorization)	193
7.3.5	支付请款(Payment capture)	194
7.4	SET 安全性分析	195
7.4.1	机密性(Confidentiality)	195
7.4.2	认证性(Authentication)	196
7.4.3	完整性(Integrity)	197

第 8 章 常见安全电子商务系统

8.1 网上商城	198
8.1.1 网上商城实现内容与步骤	198
8.1.2 系统解决方案	201
8.2 安全网络银行系统	204
8.2.1 网络银行的发展	204
8.2.2 网络银行的安全性	207
8.2.3 安全网络银行解决方案	210
8.2.4 中国的网络银行在发展	211

参考文献

第 1 章 电子商务综述

随着通信网络技术的飞速发展,特别是 Internet 的不断普及,人们的消费观念和整个商务系统也发生了巨大的变化,人们更希望通过网络的便利性来进行网络采购和交易,从而导致了电子商务(Electronic Commerce,简称 EC)的出现,并在世界范围内掀起了电子商务的热潮。

1.1 前 言

从普通意义上来说,电子商务是指商务流程的电子化,它涉及到金融机构、供应商、批发商、制造厂商和消费者等各个方面,概括起来,即商家、银行、用户和证书机构 4 个方面。今天,电子商务,特别是基于 Internet 的电子商务,由于在降低开销,拓展市场等多方面的优势而受到全球的广泛关注。它不只是简单地提供了进行商务活动的新方式,而且从更深的层面来看,由于通过它形成了与地域空间无关的一体化市场,因而正在改变着全球的经济环境。随着网上业务和技术的发展,Internet 电子商务已成为一个含义广泛和使用十分普遍的概念,几乎包括了网上在线交易和非在线交易的所有业务。

简单地讲,电子商务是指利用电子网络进行的商务活动。但电子商务的定义因其应用和范围的不同有不同的定义方法,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,给出了许多不同的表述方法:

1. 1997 年 11 月 6 日至 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),并产生了关于电子商务最权威的概念阐述:电子商务(ELECTRONIC COMMERCE),是指对整个贸易活动实现电子化。从涵盖范围方面可以定义为: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;从技术方面可以定义为:电子商务是一种多技术的集合体,包括数据交换(如电子数据交换、电子邮件)、数据获取(共享数据库、电子公告牌)以及数据的自动捕获(条形码)等。

2. 欧洲议会也对“电子商务”给出了定义,并指出: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、专用设备)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. 美国学者瑞维·卡拉科塔和安德鲁·B·惠斯顿在其专著《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,来满足政府组织、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、产品和服务器联系起来,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中的一条将

买方和卖方联系起来”。

4. IT(信息技术)行业是电子商务的直接设计者和设备的直接制造者。很多公司都根据自己的技术特点给出了电子商务的定义。虽然差别很大。但总的来说,无论是国际商会的观点、还是 HP 公司的 E - WORLD、IBM 公司的 E - BUSINESS,都认为电子商务是利用现有的计算机硬件设备、软件和网络基础设施,在通过一定的协议连接起来的电子网络环境中进行各种各样商务活动的方式。

1.2 电子商务应用和发展

1.2.1 电子商务发展因素

电子商务的发展得益于众多因素,如计算机的普及应用、网络技术的迅速发展、标准协议的指定以及信息安全的不断进步。

● 计算机的普及

近几年来,计算机技术迅速发展并普及应用。计算机处理速度越来越快,处理能力越来越强,价格越来越低,应用越来越普及。计算机的高速发展及广泛应用,为电子商务的应用提供了广泛空间,它是电子商务发展的基础。

● 网络技术的发展

Internet 逐渐成为全球通信与交易的新媒体。目前全球上网用户已过亿,其数目以每年 70% 的速度递增。全球各地已有 4 000 万个网络入口,其中 60% 为企业用户。在 Internet 迅速发展的同时,企业内部网络和企业外部网络(Intranet 与 Extranet)也迅速发展。如果说互连网络是全球通用的民用网络的话,那么内部网络与外部网络则主要用于企业、公司、研究机构的内部。互连网络强调与国际客户的交流,内部网络强调内部员工的交流,外部网络强调公司合作伙伴之间的交流。网络技术迅速发展和普及应用,为电子商务提供最基本的条件。

● 信用卡的普及应用

信用卡以其方便、快捷、安全等优点,在发达国家已成为消费支付的重要手段。全球信用卡发行量达十几亿张,并形成全球信用卡计算机支付与结算系统,使信用卡方便地跨国进行使用。仅 VISA 国际组织信用卡年交易额在 8 000 亿美元以上。近几年来,IC 卡型电子货币比磁信用卡更为先进,通过 0 与 1 的组合,运用网络媒体,进行金融交易,更适用于电子商务的网上支付。信用卡等电子货币的普及应用,为网上支付提供了重要的支付手段。

● SET 安全电子交易协议的出台

安全性与保密性是电子商务发展的关键。为确保网上支付的安全性,美国 VISA 和 Mastercard 国际组织等联合发起制定的 SET(Security Electronic Transaction Protocol)于 1997 年 5 月 3 日正式公布,作为在网络上进行电子支付的安全标准。SET 协议使用加密技术保证支付信息的安全性;使用消息认证确保支付信息的完整性;使用数字签名并颁发客户及商家电子证书确保客户账户及商家的可靠性。SET 协议的颁布深得许多厂商和金融机构的支持,将为网上购物和网上支付提供一个安全的应用环境,这是电子商务发展的关键所在。

1.2.2 世界电子商务发展

美国4年前在硅谷成立美国商业联盟,美国政府一直积极推动电子采购领域的发展,于1997年7月发布了全球电子商务纲要。1997年欧盟发布电子商务协议。目前,由18个世界经济体共同参与的亚太经济合作会(APEC)电信工作小组,开始执行每年两次的电子商务推动研讨计划,共同推动全球电子商务的发展。

发展电子商务的条件基本具备,电子商务已经起步。尽管还存在某些条件和限制,诸如带宽、网络安全、网络法规建设等。但是可以预见,电子商务将成为人类社会中的一种主要的商业形态。

近年来,世界各国政府与国际组织相继提出了一系列促进电子商务发展的文件。

- 联合国国际贸易法委员会1996年6月提出了电子商务示范法蓝本,为各国电子商务立法提供了一个范本。

- 1997年4月15日,欧盟提出了“欧盟电子商务行动方案”,对信息基础设施、管理框架和商务环境等方面的行动原则进行了规定,以促进发展欧洲的电子商务,提高欧盟的全球竞争力。为此,欧盟在网络开放、平等接入、知识产权保护、安全认证等方面制定了一系列法规性文件和指令。

- 1997年7月1日,美国政府发表了“全球电子商务框架”文件,克林顿政府将Internet的影响与200年前的工业革命相提并论。

- 欧盟和美国于1997年12月5日,发表了有关电子商务的联合宣言,就跨国电子商务的有关原则达成了一致意见。

- 1998年2月26日,美国总统克林顿在Banc America Robertson Stephens Technology 98大会上,又引人注目地宣布了美国政府的3项针对互联网的新政策,旨在促进网上贸易的发展,保持美国在高科技领域的领先地位。克林顿认为:Internet是未来经济的重要特征,由网上贸易带来的需求猛增,以及由此产生的高工资的高技术岗位将刺激经济繁荣,并创造更多的就业机会。

所有这些说明,为创造一个适应Internet这一国际性媒体的国际贸易框架,各国政府和国际组织正在进行积极的磋商。

自然,在这股网上新浪潮中,企业特别是IT行业中的企业一直扮演着主要角色并为电子商务的发展作出了巨大的贡献。人类天才的创造力和这些企业的不懈努力,为电子商务提供了源源不断的新技术。同时,这些企业还在Internet上广泛开展各种各样的商务活动,为电子商务发展起到了很好的示范作用。

时至今日,电子商务的发展依然是如火如荼,IBM、HP、Intel等许多公司都在宣传其概念和产品;Amazon的网上书店已有300多万种图书可供选购;Yahoo、Lycos等著名网络公司已开始涉足电子商务领域;而微软也已推出其在线销售计划,发展它的软件在线销售商店,这个名为NITRO(在线分销新交互技术)的在线销售商店主要面向普通消费者,而不是通常采用授权方式的公司用户。一旦NITRO开通,用户点击“buy now”按钮就可以购买微软的软件了。

一系列的统计数据表明:全球网上商业消费从1997年的26亿美元达到1998年的430亿美元,增长了16倍多,预计在2000年将达到1200亿美元,而到2005年则会突破8000亿美元。

电子商务的发展及其前景如此诱人,主要是由于其相对传统商贸的极大优势所决定的:

- 营运成本低。电子商务跨越了传统营销方式下的中间商环节,缩短了价值链,降低了交易成本,顾客可以以较低的价格获得优质产品和服务。

- 用户范围广。如前所述,电子商务是基于 Internet 的,而 Internet 迅速扩大的数以千万计的用户群对商家来说无疑是一个巨大的潜在的买方市场。

- 无时空限制。全球市场由网络连接成为与地域及空间无关的一体化市场,任何人只要拥有一个网络入口点,就可随时、随地、随意地进行商务活动。

- 多媒体手段。网上不但可传递文字,同时也可传递图像、动画、声音,客户可以直观地浏览和选择商品。

- 双向互动交流。通过电子商务系统商家可以在网上展示商品,提供有关商品信息的查询,与顾客进行互动双向沟通,收集市场信息,进行产品测试等。

- 提供个性化服务。在商品越来越趋于共性化,而消费者越来越个性化的时代,电子商务凭借现代高科技技术的支撑,可充分实现以顾客为中心,最大程度地满足顾客个性化需求。

可见,电子商务作为一种新兴的经济形式将会有巨大的市场潜力,电子商务赋予了网络应用更广泛的内涵,是 Internet 迅速发展的必然结果,也是传统商贸方式进一步发展的必然趋势。

1.2.3 国内电子商务

在世界形势的影响下,中国也正经受着电子商务这种新型商务模式的影响,并形成了自己独特的模式和道路。

- 1991年,当时的国务院电子信息系统推广办公室联合八个部委建立了中国电子数据交换技术委员会,通过有计划地协调和规范我国电子商务发展工作,拉开了我国电子商务发展的序幕。此后又开发建设了“国际电子商务网络”、“邮电部中国公用电子数据交换业务网”、“税务总局 EDI 应用系统”、“商检局 EDI 应用系统”等一系列工程。

- 1994年,中国电子部提出了“金卡”工程发展计划,首先与中国工商银行、中软总公司合作,在鞍山建设了“鞍山电子货币工程”,作为我国商业零售领域通过计算机技术实现电子交易的第一个试点。

- 1994年,联合国贸易网络中心上海中心成立,这是全球贸易网络设在中国的第一家公司,它的成员单位有:海关、商检、银行、保险、外管、外运等,他们以网络作为自身业务窗口,为进入中心的贸易商提供从贸易信息到贸易交易的一条龙服务。

- 1997年8月,对外经贸部、国内贸易部、国家税务总局、铁道部、海关总署、国家商检局、国家技术监督局、邮电部、中国信息产业商会等单位共同举办了“1997年中国电子商务应用与市场研讨会”。

- 1997年10月,标志着中国政府在电子商务领域实质性突破的“中国商品交易网”正式开通。

- 1998年3月6日,国内第一笔 Internet 网上支付实现,中国银行成为国内第一家网上银行。

- 1998年5月17日是“国际电信日”,广东邮电推出了“视聆通网上邮票交易与拍卖系统”,这是 IBM 与广东省邮电管理局通力合作,基于 IBM 电子商务软件 Net. Commerce 开发

成功并投入运行的国内第一个具有网上交易和支付功能的电子商务系统。

● 1999年3月9日,由首都信息发展有限公司和康柏电脑公司共同开发完成的北京图书大厦网上书店正式开业。这是北京实际运行的首个电子商务项目,它的开通,标志着首都电子商务建设全面启动。北京图书大厦网上书店是首都信息化建设规划中的一项重点。这一网上书店项目采用多台康柏高端服务器,其高可用性、高可扩展性和高可管理性确保了网上交易的顺利运行。北京图书大厦网上书店软件系统主要包括基本网页、基本数据管理和日常数据管理三大部分。其中基本网页包括“网上购书”、“图书排行榜”、“推荐新书”等。网上书店系统具有支持50万种图书的存储能力,首页等待时间小于两秒,支持简体、繁体2种汉字版本,系统设计要达到每天接待100万访问者,可同时支持1000人访问的能力。网上书店利用首都电子商城的交易平台实现网上在线支付,可同时支持网上银行、SET协议国内信用卡和外币信用卡等多种支付方式。

虽然电子商务的开展和应用在我国仍是刚刚起步,但已不乏成功的先例:沈阳飞机工业集团公司将电子商务的解决方案与原有的信息系统相结合,使工艺设计周期从一个月缩短至一周,工艺设计和质量检测的水平也得到根本提高;吉林市邮电管理局利用电子商务的解决方案将全区20多个邮电局联网,使用户只需几秒钟就可查得话费和通话记录,邮政储蓄业务也通过网络实现通存通兑。

由此可见,中国的电子商务潮正在全面启动,结合这些年来中国信息产业的高速发展及中国消费市场的巨大潜力,电子商务在中国的前景应该是非常看好的。

我国电子商务活动开展时间不长,但政府部门对此给予了高度的重视,电子商务的发展态势很好。从20世纪90年代初开始,相继实施了“金桥”、“金卡”、“金关”、“金税”、“金宏”、“金卫”、“金智”、“金企”等一系列“金字工程”。从1994年起,我国部分企业就开始涉足电子商务,并取得了喜人的成绩。今天,我国的电子证券交易覆盖全国,连接了全国300多家证券公司的近2600个营业部,开户投资者超过4000万户,最高日成交量达到300多亿元人民币,有利地保证了我国证券市场的发展。我国的电子金融结算系统连接着600多个地面卫星小站和1000多个收发站,覆盖全国所有地级以上城市和700多个县,平均每天往来业务5~6万笔,大大提高了转汇效率,缩短了资金在途时间。中国民航电子订票系统已经投入运行12年,1997年通过该系统预定的机票达5560万张,金额近200亿元人民币。截至1997年6月,我国共发行各种信用卡5056万张,各种非银行IC储值卡6000万张。以现代信息网络为依托的中国商品交易中心(CCEC)、中国商品订货系统(COGS)、中国远洋运输集装箱信息系统、库存商品调剂网络等商务系统也陆续投入运营。1998年3月6日,我国国内第一笔Internet网上电子商务交易成功。它是由世纪互连通讯技术有限公司和中国银行共同携手完成的。这标志着我国电子商务已经开始进入实用阶段。

目前中国内地的电子商务网站已达200多个,拥有员工达5000人以上,1999年总交易额达2亿元,均比1998年增长一倍以上。据预测,2000年底中国电子商务交易额将达到8亿元,到2002年将达到100亿元。

1.3 电子商务范围和分类

1.3.1 电子商务范围

电子商务涉及的面比较广,从理论上讲应该涉及到商务活动电子化的方方面面,但在实际系统中可能要小。电子商务处理方式和服务范围主要包括以下几个方面:

1. 企业内部之间

通过 Intranet 企业内部网方式处理内部商贸信息。Intranet 是在 Internet 基础上发展起来的企业内部网,它是在原有局域网上附加一些特定的软件,将局域网与 Internet 网连接起来,从而形成企业内部虚拟网络。大中型企业及分布在各地的分支机构、企业内部有关部门的各种信息通过网络予以连通,使企业各级管理人员方便地获取自己所需信息。通过在线业务的申请和注册代替了纸张贸易和内部流通的形式,从而降低交易成本,提高经济效益。

2. 企业和企业之间

EDI 是企业间电子贸易的重要方式。EDI 是将商业或行政事务处理按一个公认的标准,形成结构化的事务处理或文档数据格式,从计算机到计算机的电子传输方法。通过计算机在贸易伙伴的计算机系统之间进行数据交换和数据处理,实现全球贸易的无纸化。EDI 主要用于企业与企业之间、企业与批发商、批发商与零售商之间的贸易业务。

3. 企业与消费者之间

通过 Internet 网设立网上商店,消费者通过网络在网上购物,在网上支付,为消费者提供新型服务,方便消费,也促进全球商业贸易的发展。网络商场是一种全球性商场,世界各国的货物都可选购。更重要的是网络商场是实时交互的,即在网络商场里,主动权控制在顾客手中,上网人作为主体出现,能随意选择商场中的内容,可实时进行交易。顾客在任何拥有网络电脑的地方,都可以浏览全球大商场。

4. 网上检索、导购、搓合、促销活动

这可以看作电子商务的初中级阶段,商家通过在网上传布商业信息来吸引顾客,以达到促销目的。从发展的观点来看,电子商务的概念不能局限于利用 Internet 进行商业贸易,而应将利用各类电子网络进行的广告、设计、推销、采购、结算等全部贸易活动都纳入电子商务的范畴。

1.3.2 电子商务分类

根据电子商务领域和应用对象的不同,可将电子商务分为 5 类,即企业内部、企业和企业、企业对消费者、企业对政府机构和消费者对政府机构的电子商务,如图 1-1 所示。

1. 企业内部电子商务。即企业内部之间,通过企业内部网(Intranet)的方式处理与交换商贸信息。企业内部网(Intranet)是一种有效的商务工具,通过防火墙,企业将自己的内部网与 Internet 隔离,它可以用来自动处理商务操作及 workflow,增强对重要系统和关键数据的存取,共享经验,共同解决客户问题,并保持组织间的联系。通过企业内部电子商务,可以增加商务活动处理的敏捷性,对市场状况能更快地作出反应,能更好地为客户提供服务。

2. 企业对消费者(即 Business to Customer,简称 B to C,又叫 B2C,可以称为商家对个人

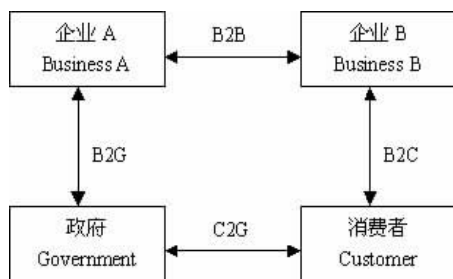


图 1-1 电子商务分类示意图

客户或商业机构对消费者)的电子商务。商业机构对消费者的电子商务基本等同于电子零售商业。目前,Internet 上已遍布各种类型的商业中心,提供各种商品和服务,主要有鲜花、书籍、计算机、汽车等商品和服务。

3. 企业对企业(即 Business to Business,简称 B to B,又叫 B2B,可以称商家对商家或商业机构对商业机构)的电子商务。商业机构对商业机构的电子商务是指商业机构(或企业、公司)使用 Internet 或各种商务网络向供应商(企业或公司)订货和付款。商业机构对商业机构的电子商务发展最快,已经有了多年的历史,特别是通过增值网络(Value Added Network, VAN)上运行的电子数据交换(EDI),使企业对企业的电子商务得到迅速扩大和推广。公司之间可能使用网络进行订货和接收订货、合同等单证和付款。

4. 企业对政府机构的电子商务(即 Business to Government,简称 B to G,又叫 B2G)。在企业 and 政府机构之间的电子商务可以覆盖公司与政府组织间的许多事务。目前我国有些地方政府已经推行网上采购。

5. 消费者对政府机构的电子商务(即 Customer to Government,简称 C to G,又叫 C2G)。政府将会把电子商务扩展到福利费发放和自我估税及个人税收的征收方面。

目前的日常生活中主要用到的电子商务模式包括 B2C 和 B2B 两种模式。

1.3.3 EDI 和 B2B 电子商务

企业间的电子商务交易,即 B2B,因为它最具有发展潜力,并且占有最大的市场份额,所以成为目前电子商务所有模式中最重要的一种。据 IDG 公司 1997 年 9 月的统计,1997 年全球在 Internet 网上进行的电子商务金额为 100 亿美元,其中企业间的商务活动占其中的 79%。Forrester 研究公司预计企业间的商务活动将以 3 倍于消费者和企业之间的电子商务的速度发展。

1. 电子数据交换 EDI

早期的计算机主要用于科学计算和军事目的,最早使用计算机进行事务处理和交易的是银行系统。在 1970 年至 1980 年之间,企业或商业机构逐步扩展了其内部网络和计算机功能,利用电子数据 EDI(Electronic Data Interchange)进行企业或商业机构之间订单、发票和货运通知的发送和接收,传统的 EDI 模式是 B2B 的早期模型。

国际标准化组织(ISO)于 1994 年对电子数据交换(EDI)进行了技术定义:根据商定的交易或电文数据的数据结构标准实施商业或行政交易的从计算机到计算机的电子数据传输。从而对 EDI 进行了特定含义和条件的规范。

- 使用 EDI 的是交易的双方,是企业之间的文件传递,而非同一组织内的不同部门。
- 交易双方传递的文件是特定的格式,采用的是报文标准,现在即是联合国的 UN/EDIFACT。
- 数据交换双方都有自己的计算机或计算机管理信息系统以及相关设备。
- 双方的计算机(或计算机系统)能发送、接收并处理符合约定标准的交易数据信息。
- 双方计算机之间有网络通信系统,信息传输则是通过该网络通信系统实现的,并通过相互之间的计算机进行自动处理。

利用 EDI 传递的数据或信息是指交易双方互相传递的具备法律效力的文件资料,可以是各种商业单证,如订单、回执、发货通知、运单、装箱单、收据发票、保险单、进出口申报单、报税单、缴款单等;也可以是各种凭证,如进出口许可证、信用证、配额证、检疫证、商检证等。所以,从某种意义上来说,EDI 是一项严谨的规范与作业流程,只不过这项流程的完成需要计算机系统和超过技术以外的企业和企业,银行各部门的配合来完成数据传输的作业流程和处理。

2. EDI 的发展

EDI 技术的萌芽始于 20 世纪 60 年代,于 20 世纪 70 年代在西方发达国家得到了迅速发展。它是随着计算机技术和网络通信技术的迅速发展而应运而生的产物,是商贸和行政管理向现代化自动化发展的必然结果。20 世纪 70 年代初的美国就已开始制订行业标准,于 1975 年即出现了第一个行业 EDI 标准。欧洲紧随其后,于 20 世纪 80 年代早期推出了欧洲的 EDI 标准。后来在联合国的协调和主持下制订了联合国 EDI 标准,即 1986 年颁布的 UN/EDIFACT,作为国际通用标准。据统计,截止到 1996 年初美国最大的 100 家企业中就已有 97 家实现了 EDI 经营管理,全美所有企业的 25% 已使用 EDI(现在已远不止此数)。新加坡于 1991 年即正式运行全国的 EDI 系统。韩国的全国 EDI 系统则于 1993 年投入运行。我国台湾地区在 1992 年开通了全岛地区的 EDI 系统,并全力推广 EDI 的应用,目前已有通关自动化 EDI、制造业 EDI、商业现代化 EDI 及金融 EDI 等大型专业 EDI 系统。

EDI 技术现今还在不断发展和完善中,不过 EDI 的推广应用的的确确大幅度提高了商贸和相关行业(如报关、商检、税务、运输等)的运作效率。20 世纪 90 年代以来,美、日、西欧、澳大利亚及新加坡等许多国家已陆续宣布,对不采用 EDI 进行交易的商户,不进行或推迟其贸易文件的处理。这就给非 EDI 商户造成巨大压力,甚至会给她造成巨大的贸易损失。所以一个企业采用 EDI 与否,直接关系到企业的生存和长期发展。

我国 EDI 起步较晚,于 20 世纪 90 年代初才开始,但因有了借鉴,故起点较高。为促进我国市场经济的发展,为提升我国企业在世界上的竞争力,必须在我国大力推广 EDI 的应用。EDI 的推广应用和发展基于计算机技术和网络通信技术的发展。改革开放以来,我国的计算机技术和网络通信技术已有了飞速的发展和长足的进步,国内不少大型企业已建立起了自己内部的计算机管理信息系统(MIS)。作为信息高速公路的计算机通信网络在我国已初具规模,邮电部的中国互联网(ChinaNet)和电子部的金桥网(ChinaGBN)作为计算机通信网络,已覆盖了全国大部分大中城市,并作为商业网投入了运营,这为我国 EDI 的推广应用提供了坚实的物质基础。邮电部的 EDI 增值网络 ChinaEDI 更给推广 EDI 应用创造了良好的条件。

3. EDI 的特点及构成

EDI 的使用对象是具有固定格式的业务信息和具有经常性业务联系的单位;其传送的资料是一般业务资料,如发票和订单等,而不是指一般性的文档;采用共同标准化的格式,这也是

与一般 E-mail 的区别,如联合国 EDIFACT 标准;采用全自动方式,尽量避免人工的介入操作,由收送双方的计算机系统直接传送和交换资料。

从技术上讲,EDI 包括硬件与软件两大部分。硬件主要是计算机网络;软件包括系统软件和 EDI 标准实现软件。

从硬件方面讲,EDI 作为早期企业之间商用信息编译和传输的标准,一般都是通过称为增值网 VANs(Value-added Networks)的专有网络来实现的。但 VANs 的安装和维护相当昂贵,从而把一些小型和中型企业拒之门外,使这些企业只能通过传真和电话来进行相互之间的通信,从而大大限制了企业与企业之间电子商务的发展。但随着 Internet 的快速发展和安全性的逐步提高,作为一个费用更低、覆盖面更广、服务更好的系统,其已表现出替代 VAN 而成为 EDI 的通信载体的趋势,人们把通过 Internet 进行的 EDI 交易称为 Internet EDI。

从软件方面看,EDI 所需要的软件主要是将用户数据库系统中的信息,翻译成 EDI 的标准格式以供传输交换。由于不同行业的企业是根据自己的业务特点来规定数据库的信息格式的,因此,当需要发送 EDI 文件时,从企业专有数据库中提取的信息,必须把它翻译成 EDI 的标准格式才能进行传输。

EDI 软件主要有以下几种:

- 转换软件(Mapper)。转换软件可以帮助用户将原有计算机系统的文件转换成翻译软件能够理解的平面文件(Flat file),或是将从翻译软件接收来的平面文件,转换成原计算机系统文件。

- 翻译软件(Translator)。将平面文件翻译成 EDI 标准格式,或将接收到的 EDI 标准格式翻译成平面文件。

- 通信软件。将 EDI 标准格式的文件外层加上通信信封(Envelope),再送到 EDI 系统交换中心的邮箱(Mailbox),或从 EDI 系统交换中心内将接收到的文件取回。

4. B2B 电子商务交易发展

B2B 电子商务交易涉及面很广,既有企业和企业之间商务信息交流,也有企业和企业以及银行之间资金的流转,另外还可能涉及到分销商和一些中介机构等,也可能是所有各方的集合体,从而构成了真正的 B2B 交易。

从美国工业标准报告里面的一些数据可以看到全球从 1998 年到 1999 年全球互联网用户增长了 55%,美国互联网 ISP 收入增长了 41%。而 B2B 的电子商务规模以及它在整个互联网经济中的地位增长是最引人注目的。美国的网络经济从业人员增加一倍,达到了 250 万。互联网工业的年收入增长 62%,整个美国经济 1999 年按 GDP 来算大概是 8 万亿美元左右,其中增长最快的产业就是网络经济,从 1998 年 998 亿美元的产值可以增加到 1 740 亿。据高盛公司对未来美国 B2B 电子商务市场规模的预测,1999 年是 1 000 多亿,在 4 年达到 1 万亿美元,这个增长速度是很快的,跟 1999 年相比增长了 10 倍。

目前在电子商务方面,北美洲占有绝对的主导地位,占据全球 63% 的份额,但是由于其他地区迅速增长,到 2004 年,美国的比例将降到 39%,欧洲和亚太地区将会迎头赶上。IDC 数据公司对亚太市场互联网成长趋势也做过一些预测。从 1997 年到 2003 年亚太地区每年的互联网用户综合成长率将从 2000 年 2 月份预测的 47% 增加到 63%。互联网用户到 2004 年年底增到 9.5 亿多,带来 890 亿美元的互联网收入。据推测,日本的 B2B 交易将从 1999 年 85 亿增长到 2004 年的 8 610 亿美元。相比之下美洲就落后了,交易量由 10 亿上升到 1 240 亿美