21世纪 电子商务与现代物流管理系列教材

# 电子商务安全与支付

主　编　宋少忠　颜　辉
副主编　战冬梅　郝莉萍　刘　磊　王艳敏

中国水利水电出版社
www.waterpub.com.cn

21世纪电子商务与现代物流管理系列教材

# 电子商务安全与支付

主　编　宋少忠　颜　辉

副主编　战冬梅　郝莉萍　刘　磊　王艳敏

中国水利水电出版社
www.waterpub.com.cn

## 内 容 提 要

电子商务安全与支付是电子商务运作中密切联系的两个关键环节。本书系统介绍了电子商务安全与支付的基本理论、技术以及安全电子商务的应用。全书共包括电子商务安全理论（网络信息安全、计算机信息安全）、网络安全中涉及的攻防技术、金融支付安全3部分。

本书内容丰富、层次清晰、讲解深入浅出，可作为高等院校电子商务、信息安全、信息管理、计算机应用和金融等专业的教材，也可作为有关电子商务企业和企事业单位开展电子商务活动的参考书。

**本书配有电子教案，读者可以从中国水利水电出版社网站或万水书苑免费下载，网址：http://www.waterpub.com.cn/softdown/或 http://www.wsbookshow.com。**

**图书在版编目（CIP）数据**

电子商务安全与支付 / 宋少忠，颜辉主编. -- 北京
：中国水利水电出版社，2009.12
（21世纪电子商务与现代物流管理系列教材）
ISBN 978-7-5084-7110-5

Ⅰ. ①电… Ⅱ. ①宋… ②颜… 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(2009)第240052号

**策划编辑：石永峰　　责任编辑：张玉玲　　封面设计：李　佳**

| | |
|---|---|
| 书　名 | 21世纪电子商务与现代物流管理系列教材<br>**电子商务安全与支付** |
| 作　者 | 主　编　宋少忠　颜　辉<br>副主编　战冬梅　郝莉萍　刘　磊　王艳敏 |
| 出版发行 | 中国水利水电出版社<br>（北京市海淀区玉渊潭南路1号D座　100038）<br>网址：www.waterpub.com.cn<br>E-mail：mchannel@263.net（万水）<br>sales@waterpub.com.cn<br>电话：（010）68367658（营销中心）、82562819（万水） |
| 经　售 | 全国各地新华书店和相关出版物销售网点 |
| 排　版 | 北京万水电子信息有限公司 |
| 印　刷 | 北京市天竺颖华印刷厂 |
| 规　格 | 184mm×260mm　16开本　19.25印张　495千字 |
| 版　次 | 2009年12月第1版　2009年12月第1次印刷 |
| 印　数 | 0001—3000册 |
| 定　价 | 32.00元 |

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

**版权所有·侵权必究**

# 序

随着经济全球化和我国加入“WTO”、改革开放的进一步深化，商业市场逐步向国际化的方向发展，我国电子商务技术和物流产业也有了迅速的发展，已成为极具活力的产业。由于高新技术和现代管理方法的应用，我国传统的商务、物流活动在管理理念、组织方式、管理制度、业务流程、信息处理手段及作业方式等诸多方面已不能适应现代商务、物流行业发展的需要，由此引发了对电子商务、现代物流等行业专业技术人才和管理人才的竞争。这些人才应具有现代管理思维方式、组织管理方法和现代技术手段。这就对教育部门提出了新的要求：如何培养出适合现代商务、物流等行业急需的专门人才。

本套教材是为了配合培养电子商务、现代物流行业专门人才的需要而组织编写的。现在，有许多高等院校为了适应人才市场的需要，已经或正在准备成立电子商务、物流管理或物流工程专业。为此，我们组织在这方面具有较高教学水平和教学经验的一线教师精心编写了这套教材，为培养电子商务、现代物流行业的专门人才尽一份力量。

本套《21 世纪电子商务与现代物流管理系列教材》具有如下特点：

（1）面向 21 世纪电子商务与物流人才培养的需求，结合本专业学生的培养特点，针对性强。本套教材的作者都是长期在第一线从事教学的教授、副教授，有的还是硕士生导师、博士生导师，他们都有丰富的教学经验，对学生的基本情况、特点和认知规律等有深入的了解。

（2）本套教材以基本的理论知识为主，阐述相关的实用技术和方法。在写法上，为了激发学生的兴趣，采用以案例教学的方式，用典型的实例讲解有关的理论与技术的具体操作方法，使学生易于接受。

（3）每本书的编写注重以“深入浅出”、“言简意明”为原则，论述基本原理与使用方法，以实例分析的形式阐述具体的分析、操作过程，使读者从一般理论知识到实际运用有一个全面的认识。

（4）书中每章前面有：知识点、难点提要与本章的要求、需要熟练掌握的内容和一般了解的内容；每章结尾有“小结”。为了方便学生自学自查，各章配有较多数量的练习题，习题的形式多种多样，有选择题、判断题、填空题、简答题、论述题和思考题等。

（5）为了便于多媒体教学，每本教材都配有电子教案，教师可以根据授课情况任意修改。教案可以到中国水利水电出版社网站 www.waterpub.com.cn 下载。

总之，本套教材凝聚了许多一线教师多年的教学经验和智慧，内容新颖、结构完整、概念清晰、深入浅出、通俗易懂，可读性、可操作性和实用性强。

本套教材适用于电子商务、物流管理或物流工程专业的本科生，同时也可供研究生、大专学生选用。

培养适合现代商务、物流行业的应用型人才的教育研究是一项具有深远意义的改革探索课

题。我们愿意与从事这方面应用型人才教育的广大教师合作，为培养高质量的应用型人才共同努力。

在此，我们向关心、支持以及参与本套丛书的研究、写作和发行的领导、专家和朋友们表示衷心的感谢！本套教材的不足之处，恳请专家和读者批评指正。

编委会

2005 年 1 月

此为试读，需要完整PDF请访问：www.ertongbook.com

# 前　言

随着 Internet 的迅速发展和广泛应用，人们开始习惯于利用开放快捷的网络进行各种采购和交易，从而导致了电子商务的出现，并使其成为业界的新热点。其显著特点是增加贸易机会，降低成本，简化流程，提高效率。

虽然电子商务的观念逐渐深入人心，但电子商务是在国际化、社会化、开放化和个性化的 Internet 环境中运作的，它的应用可能会出现各种商业信息的泄漏、客户的银行账户信息被盗、金融欺诈以及缺乏可信性而导致的商业丢失等各种安全与信任问题。因此，要在 Internet 开放的网络平台上成功地进行电子交易，必须有效解决交易网络平台的安全问题，并提供对电子支付过程的保护。因此，电子商务环境下的安全与支付是目前困扰和影响电子商务推广的两个重要问题。

本书较为深入和完整地阐述了电子商务安全与支付的基本理论和相关技术，注重理论联系实际，力求将计算机安全、网络安全、信息安全与经济和金融学科有机结合。全书的整体结构共分 3 个部分。

第一部分包括第 1～7 章，介绍电子商务安全的基本概念和理论。其中，第 1 章概述网络信息安全和电子商务安全规范等；第 2 章介绍安全问题的产生、交易环境的安全性、交易对象和交易过程的安全性，以及网上支付的安全需求；第 3 章介绍数据加密及密钥体制；第 4 章主要介绍常见操作系统安全；第 5 章介绍 TCP/IP 的基础知识、网络层和应用层安全性；第 6 章介绍服务器的访问控制和认证、常见企业级防火墙及其使用方法、常见的入侵检测系统等；第 7 章介绍客户机端的电子邮件的安全，使用个人防火墙和反病毒软件。

第二部分包括第 8～10 章，介绍网络安全中涉及的攻击和防范技术与方法。其中，第 8 章介绍常见网站受攻击的技术；第 9 章介绍电子商务网站的常用方法、防火墙、非军事区域、虚拟专用网（VPN）、入侵检测系统（IDS）和认证；第 10 章介绍数据库系统安全、生物特征识别、潜信道和外包安全。

第三部分包括第 11～15 章，介绍支付安全与法律保障。其中，第 11 章介绍电子交易与支付系统与应用；第 12 章介绍电子支付工具；第 13 章介绍网上银行、网上证券交易和网上保险；第 14 章介绍网站漏洞的检查和灾难恢复的一些方法与策略；第 15 章介绍电子商务支付与安全的法律保障知识。

本书具有以下特色：

（1）实用性强。本书以技术为主线，突出实际应用，既传授基础理论知识又引导应用技能的提高，通过教材提高学生的相应素质，体现素质教育的思想，这是作者在编写教材的过程中特别注重的地方。

（2）层次结构清晰。本书分为 3 个部分：电子商务安全理论（网络信息安全、计算机信息安全）、网络安全中涉及的攻防技术、金融支付安全。读者可以根据自身情况，选读其中的章节内容。

本书由宋少忠、颜辉任主编，战冬梅、郝莉萍、刘磊、王艳敏任副主编，阚君满、董大

伟、王宇和尚程参与了本书的部分编写校对工作。另外，在本书编写过程中编者参考了众多著作，在此对这些著作的作者表示衷心的感谢。

由于时间仓促及编者水平有限，且电子商务安全理论与技术处在快速发展之中，书中疏漏甚至错误之处在所难免，恳请广大读者批评指正。

编　者

2009 年 9 月

# 目　　录


序

前言

**第 1 章　电子商务系统安全与支付概述**……1

1.1　电子商务及其发展……1

1.1.1　什么是电子商务……1

1.1.2　电子数据交换（EDI）的发展……2

1.1.3　Internet 的发展……3

1.1.4　电子商务的发展……3

1.2　网络信息安全……4

1.2.1　网络信息安全的目标……4

1.2.2　电子商务系统安全层次……5

1.3　电子商务安全规范……6

1.4　电子商务和支付系统……8

**第 2 章　电子商务系统的安全需求**……10

2.1　安全问题的产生……10

2.2　交易环境的安全性……12

2.2.1　WWW 简介……12

2.2.2　客户机的安全性……14

2.2.3　通信信道的安全性……16

2.2.4　服务器的安全性……18

2.3　交易对象和交易过程的安全性……20

2.4　网上支付的安全需求……22

2.4.1　支付的发展……22

2.4.2　电子商务系统中的支付……23

2.4.3　网上支付系统的安全需求……25

**第 3 章　加密技术**……26

3.1　数据加密概述……26

3.2　对称密钥密码体制……29

3.2.1　流密码……29

3.2.2　分组密码……30

3.2.3　DES 算法……30

3.2.4　其他分组密码算法……34

3.2.5　AES 算法……36

3.3　非对称密钥密码体制……38

3.3.1　RSA 密码体制……38

3.3.2　其他非对称密钥密码体制……41

3.4　密钥管理……43

3.4.1　密钥的生存周期……43

3.4.2　保密密钥的分发……44

3.4.3　公钥的分发……45

3.5　数字信封技术……47

**第 4 章　操作系统的安全**……48

4.1　操作系统安全性概述……48

4.1.1　操作系统安全性设计的原则……48

4.1.2　操作系统的安全服务……48

4.1.3　操作系统安全级别的划分……51

4.2　UNIX 系统的安全性……52

4.2.1　口令与账号安全……52

4.2.2　文件系统安全……55

4.2.3　系统管理员的安全策略……57

4.3　Windows 系统的安全性……59

4.3.1　Windows NT 的安全性……59

4.3.2　Windows 2003 的安全性……63

4.4　常见的操作系统安全漏洞……65

4.4.1　影响所有系统的漏洞……65

4.4.2　最危险的 Windows 系统漏洞……69

4.4.3　UNIX 系统漏洞……72

**第 5 章　电子商务通道的安全**……76

5.1　TCP/IP 的基础知识……76

5.2　网络层的安全性……78

5.2.1　网络层的安全性……78

5.2.2　IPSec……79

5.3　传输层的安全性……84

5.3.1　传输层的安全性介绍……84

5.3.2　SSL 协议……84

5.4　应用层的安全性……89

5.4.1　应用层的安全……89

5.4.2　安全超文本传输协议（S-HTTP）……91

**第 6 章　服务器的安全**……93
6.1　对服务器的安全威胁……93
6.1.1　对 WWW 服务器的安全威胁……93
6.1.2　对数据库的安全威胁……94
6.1.3　对公用网关接口的安全威胁……98
6.1.4　对其他程序的安全威胁……98
6.2　访问控制和认证……100
6.2.1　入网访问控制……100
6.2.2　权限控制……100
6.2.3　目录级安全控制……100
6.2.4　属性安全控制……101
6.2.5　服务器安全控制……101
6.3　常见企业级防火墙介绍……103
6.3.1　选择防火墙的要求……103
6.3.2　选购防火墙应该注意的问题……103
6.3.3　防火墙的局限……106
6.3.4　常见企业级防火墙产品介绍……107
6.4　常见企业级防火墙的使用方法……113
6.4.1　FireWall-1……113
6.4.2　Cisco PIX 防火墙……120
6.5　常见的入侵检测系统……123
6.5.1　概述……123
6.5.2　常见的企业级网络入侵检测系统……124
**第 7 章　客户机的安全**……129
7.1　对客户机的安全威胁……129
7.1.1　对客户机的安全威胁介绍……129
7.1.2　内置的客户机安全机制……132
7.2　电子邮件的安全……136
7.2.1　基本概念……136
7.2.2　电子邮件反病毒……137
7.2.3　电子邮件内容安全……137
7.3　使用个人防火墙……141
7.3.1　为什么要使用个人防火墙……141
7.3.2　常见的个人防火墙……142
7.3.3　几种个人防火墙的使用方法……142
7.4　使用反病毒软件……146
**第 8 章　电子商务网站常见的攻击**……151
8.1　TCP/IP 协议简介……151
8.1.1　传输控制协议（TCP）……151
8.1.2　网际协议（IP）……152
8.1.3　差错与控制报文协议（ICMP）……152
8.1.4　用户数据报文协议（UDP）……152
8.2　IP 欺骗技术……153
8.2.1　IP 欺骗原理……153
8.2.2　IP 欺骗的防范……154
8.3　Sniffer 技术……154
8.3.1　Sniffer 的工作原理……154
8.3.2　Sniffer 的防范……155
8.4　Port Scanner 技术……155
8.4.1　常用的网络相关命令……155
8.4.2　Port Scanner 定义……158
8.4.3　Port Scanner 的工作原理和功能……159
8.5　Torjan Horse……159
8.5.1　Torjan Horse 的概念……159
8.5.2　Torjan Horse 的特点……160
8.5.3　Torjan Horse 的实现……160
8.5.4　Torjan Horse 的发现和清除……160
8.6　DDoS 技术……161
8.6.1　DDoS 的原理……161
8.6.2　DDoS 的防范……162
8.6.3　电子商务网站是 DDoS 的主要攻击目标……162
8.7　计算机病毒……162
8.7.1　病毒的定义……162
8.7.2　病毒的危害……163
8.7.3　病毒的分类……163
8.7.4　病毒的传播途径……164
8.8　WWW 中的安全问题……164
8.8.1　现代恶意代码……164
8.8.2　ActiveX 的安全性……165
8.8.3　URL 破坏……166
8.8.4　Cookies……166
8.8.5　DNS 安全……166
8.9　移动安全……167
**第 9 章　电子商务网站常用防御方法**……169
9.1　防火墙……169
9.1.1　防火墙的工作原理……169
9.1.2　防火墙规则集……172

9.2 非军事区域……174
9.2.1 DMZ 的概念……174
9.2.2 非军事区域的设置……175
9.2.3 电子商务非军事区域的实现……176
9.2.4 多区网络存在的问题……178
9.3 虚拟专用网……178
9.3.1 VPN 技术……178
9.3.2 IPSec 协议……180
9.4 入侵检测系统……181
9.4.1 入侵检测概念……181
9.4.2 基于主机的 IDS……181
9.4.3 基于网络的 IDS……182
9.4.4 入侵检测技术发展方向……183
9.5 认证……184
9.5.1 第三方认证……184
9.5.2 PKI 的组成……184
9.5.3 证书认证机构 CA……186
9.5.4 PKI 应用……190
**第 10 章 电子商务安全常见技巧**……193
10.1 数据库系统安全……193
10.1.1 数据库系统安全的重要性……193
10.1.2 数据库系统安全的含义……194
10.1.3 数据库中数据的完整性……197
10.1.4 数据库并发控制……198
10.1.5 数据库的备份与恢复……200
10.1.6 数据库攻击常用方法……202
10.2 生物特征识别……204
10.2.1 隐写术……204
10.2.2 数字水印……205
10.3 潜信道……206
10.4 外包安全……206
**第 11 章 电子交易与支付**……208
11.1 电子交易……208
11.1.1 电子交易模式……208
11.1.2 电子商务流程……210
11.1.3 电子商务平台介绍……210
11.2 支付活动及其发展……212
11.2.1 电子支付基本模式……212
11.2.2 电子支付基本流程……214
11.2.3 国内外网络支付发展情况……215
11.3 电子商务支付系统……217
11.3.1 电子商务支付系统的构成……217
11.3.2 电子商务支付系统的功能……218
11.3.3 电子支付系统的安全要求……219
11.4 电子支付系统应用……219
11.4.1 ATM 系统……220
11.4.2 POS 系统……222
11.4.3 电子汇兑系统……223
11.4.4 网上支付系统……224
**第 12 章 电子支付工具**……226
12.1 电子货币……226
12.1.1 电子货币的概述……226
12.1.2 电子货币的分类……227
12.1.3 电子货币的职能与作用……227
12.1.4 中国电子货币的发展现状……228
12.2 银行卡……230
12.2.1 银行卡概述……230
12.2.2 信用卡……231
12.2.3 借记卡……233
12.2.4 IC 金融卡……233
12.2.5 中国主要银行卡……233
12.2.6 国外信用卡及国际卡组织……236
12.3 网络货币……240
12.3.1 信用卡型网络货币……240
12.3.2 电子现金……241
12.3.3 电子支票……242
12.3.4 电子钱包……243
**第 13 章 网上金融**……244
13.1 网上银行……244
13.1.1 网上银行服务……245
13.1.2 中国网上银行的现状及发展……247
13.2 网上证券交易……247
13.2.1 网上证券交易的发展现状……248
13.2.2 网上证券交易模式和系统……248
13.2.3 网上证券交易的基本方法……250
13.2.4 网上证券交易的资金支付……253
13.3 网上保险……255
13.3.1 网上保险的主要内容……255

13.3.2 网上保险系统 ……257
13.3.3 网上保险经营模式 ……260
**第 14 章 网站漏洞的检查和灾难恢复** ……261
14.1 对站点进行风险分析 ……261
14.1.1 什么是风险 ……261
14.1.2 企业资产与风险 ……261
14.1.3 攻击威胁与风险 ……261
14.1.4 网站漏洞与风险 ……262
14.2 检查自己站点的安全漏洞 ……262
14.2.1 研究网站漏洞 ……262
14.2.2 决定检查技术 ……264
14.2.3 使用自动扫描工具 ……265
14.3 雇用一个入侵检测小组 ……267
14.4 拟订灾难恢复计划 ……268
14.4.1 拟订灾难恢复计划的目的 ……268
14.4.2 灾难恢复计划的目标 ……268
14.4.3 灾难恢复计划的内容 ……269
14.5 信息数据库备份和恢复 ……270
14.5.1 数据库备份的实例 ……270
14.5.2 数据库恢复 ……273
14.6 防范自然灾害 ……273
14.6.1 自然灾害及引起的灾难 ……273
14.6.2 防范措施 ……274
14.7 事件反应、跟踪和法规 ……275
14.7.1 事件反应策略 ……275
14.7.2 建立事件反应小组 ……275
14.7.3 制定事件反应程序 ……275
14.7.4 事件跟踪 ……276
14.7.5 司法调查与适用法律 ……277
**第 15 章 电子商务支付与安全的法律保障** ……280
15.1 电子商务参与各方的法律关系 ……280
15.1.1 买卖双方当事人的权力和义务 ……280
15.1.2 网络交易中心的法律地位 ……281
15.1.3 关于网站经营者侵权的法律责任 ……282
15.1.4 网络交易客户与网上银行间的法律关系 ……282
15.1.5 认证机构在电子商务中的法律地位 ……283
15.2 电子商务交易安全保护法 ……284
15.2.1 联合国电子商务交易安全的法律保护 ……284
15.2.2 中国电子商务交易安全的法律保护 ……290
15.3 中华人民共和国《电子签名法》 ……293
**参考文献** ……296

此为试读，需要完整PDF请访问：www.ertongbook.com

# 第 1 章　电子商务系统安全与支付概述

电了商务是社会和科技发展的必然结果。电子商务的迅速发展也将给政府的管理、企业的经营、人们的工作和生活带来革命性变革。本章说明电子商务的发展过程、电子商务带来的变革、电子商务的运行模式以及对管理的新要求。

## 1.1　电子商务及其发展

### 1.1.1　什么是电子商务

随着电子技术和因特网（Internet，又称国际互联网）的发展，信息技术作为工具被引入商贸活动中，产生了电子商务（Electronic Commerce，EC；Electronic Business，EB）。通俗地说，电子商务就是在计算机网络（主要指 Internet）的平台上，按照一定标准开展的商务活动。当企业将它的主要业务通过企业内部网（Intranet）、企业外部网（Extranet）以及 Internet 与企业的职员、客户、供销商以及合作伙伴直接相连时，其中发生的各种活动就是电子商务。电子商务的定义有多种说法。下面是一些组织、政府、公司、学术团体等总结的较为全面的定义。

（1）联合国经济合作和发展组织（OECD）在有关电子商务的报告中对电子商务（EC）的定义是：电子商务是发生在开放网络上的包含企业之间（Business to Business）、企业和消费者之间（Business to Consumer）的商业交易。

（2）联合国国际贸易法律委员会（UNITRAL）对电子商务的定义是：电子商务是采用电子数据交换（EDI）和其他通信方式增进国际贸易的职能。

（3）全球信息基础设施委员会（GIIC）电子商务工作委员会报告草案中对电子商务的定义是：电子商务是运用电子通信作为手段的经济活动，通过这种方式人们可以对带有经济价值的产品和服务进行宣传、购买和结算。这种交易的方式不受地理位置、资金多少或零售渠道的所有权影响，公有私有企业、公司、政府组织、各种社会团体、一般公民、企业家都能自由地参加广泛的经济活动，其中包括农业、林业、渔业、工业、私营和政府的服务业。电子商务能使产品在世界范围内交易并向消费者提供多种多样的选择。

（4）国际标准化组织（ISO/IEC）关于 EB 谅解备忘录对 EB 的定义是：电子商务（EB）是企业之间、企业与消费者之间信息内容与需求交换的一种通用术语。

（5）IBM 公司的电子商务（E-Business）概念：在网络计算机环境下的商业化应用，不仅仅是硬件和软件的结合，也不仅仅是我们通常意义下强调交易的狭义的电子商务（E-Commerce），而是把买方、卖方、厂商及其合作伙伴在因特网（Internet）、企业内部网（Intranet）和企业外部网（Extranet）结合起来的应用。它同时强调这三部分是有层次的：只有先建立良好的 Intranet，建立好比较完善的标准和各种信息基础设施，才能顺利扩展到 Extranet，最后扩展到 E-Commerce。

（6）HP 公司提出电子商务（EC）、电子业务（EB）、电子消费（EC）和电子化世界的概念。电子商务（E-Commerce）的定义是：通过电子化手段来完成商业贸易活动的一种方式。电子商务使我们能够以电了交易为手段完成物品和服务等的交换，是商家和客户之间的联系纽

带。它包括两种基本形式：商家之间的电子商务和商家与最终消费者之间的电子商务。电子业务（E-Business）的定义是：一种新型的业务开展手段，通过基于 Internet 的信息结构，使得公司、供应商、合作伙伴和客户之间，利用电子业务共享信息。电子业务不仅能够有效地增强现有业务进程的实施，而且能够对市场等动态因素做出快速响应并及时调整当前业务进程。更重要的是，电子业务本身也为企业创造出了更多、更新的业务运作模式。电子消费（E-Consume）的定义是：人们使用信息技术进行娱乐、学习、工作、购物等一系列活动，使家庭的娱乐方式越来越多地从传统电视向 Internet 转变。

（7）通用电气公司（GE）对电子商务的定义是：电子商务是通过电子方式进行商业交易，分为企业与企业间的电子商务、企业与消费者之间的电子商务。企业与企业间的电子商务以 EDI 为核心技术，以增值网（VAN）和因特网（Internet）为主要手段，实现企业间业务流程的电子化，配合企业内部的电子化生产管理系统，提高企业从生产、库存到流通（包括物资和资金）各个环节的效率。企业与消费者之间的电子商务以 Internet 为主要服务提供手段，实现公众消费和服务提供方式以及相关付款方式的电子化。

（8）美同政府在其《全球电子商务纲要》中指出：电子商务是通过 Internet 进行的各项商务活动，包括广告、交易、支付、服务等活动，全球电子商务将会涉及世界各国。

总结起来，可以这样说：从宏观上讲，电子商务是计算机网络的又一次革命，是通过电了手段建立一种新的经济秩序，它不仅涉及电子技术和商业交易本身，而且涉及诸如金融、税务、教育等社会其他层面。从微观角度说，电子商务是指各种具有商业活动能力的实体（生产企业、商贸企业、金融机构、政府机构、个人消费者等）利用网络和先进的数字化传媒技术进行的各项商业贸易活动。

虽然至今人们尚未对电子商务有一个统一的、明确的定义，但实际上电子商务并非是刚刚诞生的新事物。它的发展历史非常悠久，早在电报出现时，就有了以莫尔斯码点和线的形式在电线中传输的商贸活动，这开辟了运用电子手段进行商务活动的新纪元。商务统计报表认为，世界上真正对电子商务发展的研究开始于 20 世纪 70 年代。对电子商务发展影响最大的是电子数据交换（EDI，Electronic Data Interchange）技术的发展和 Internet 的发展。

### 1.1.2 电子数据交换（EDI）的发展

电子数据交换（EDI）是一个汇集和传送电子信息的标准，产生于 20 世纪 60 年代。EDI 起源于计算机的电子数据处理（EDP）技术，这是从科学计算向文字处理和应用处理的转变。随后出现了字处理（WP）软件和电子表格（Spread Sheet）软件，这些为标准格式（或格式化）商务单证的电子数据交换（EDI）开发应用提供了强有力的工具。1978 年，美国 EDI. 委员会成立，该委员会的主要工作是建立美国全国性的 EDI 标准。1981 年该委员会颁布了第一套 EDI 标准，并在此后的很长一段时间内不断完善该标准。1987 年，联合国公布了 EDI 运作标准 UN/EDIFA（United Nations Electronic Data Interchange for Administration，Commerce and Transport），并每年修订。1990 年，联合国正式推出 UN/EDIFACT 标准，国际标准化组织（ISO）将其定为国际标准 ISO 9735，从此国际贸易有了一个统一的电子通信标准。

早期的电子数据交换指的是政府或企业的采购及企业商业文件的处理，从手工书面文件的准备和传递转变为电子文件的准备和传递。随着网络技术的发展，EDI 开始用在增值网（VAN）的专用通信网上。安装和维护增值网的费用很高，中小型企业根本无法负担。因此，只有一些大公司才能实现电子通信，大部分公司还是使用纸面单证、传真和电话等进行商务联系。这也限制了大公司电子通信的使用潜力，因为它的大部分合作伙伴都还没有使用 EDI。但是，随着

以 Internet 的广泛应用为标志的网络时代的到来，电子通信的应用规模迅速扩大了起来。

### 1.1.3　Internet 的发展

Internet 起源于 20 世纪 60 年代末美国的 ARPANET，这是一个用于军事目的的计算机网络。1969 年作为一个试验网络投入运行，以后规模逐年扩大。1975 年，结束试验交付使用。ARPA 网覆盖美国和欧洲大部分地区，把数量很大、种类繁多的计算机连接成一个国际性远程网。ARPA 网的研制过程为以后计算机网络的发展打下了理论和实践基础。1981 年，美国的全国科学基金会开发了一个地区性的学术性网络 NSFNET。1983 年，TCP/IP 成为 ARPANET 上的标准通信协议，一个真正意义上的 Internet 出现了。Internet 这个名称的使用是由 ARPANET 分离出来的。如今，NSFNET 连接了全美上百万台计算机，拥有几百万用户，是 Internet 最主要的成员网。后来随着各种计算机网络地不断并入，Internet 蓬勃发展。到 20 世纪 90 年代早期，万维网（World Wide Web，WWW）出现了，它成为任何有电脑的人浏览网络的最流行方式。

1998 年全球上网人数已超过一亿，而且据预测，到 2013 年全球网民人数将达到 22 亿。如此多的网络用户，为电子商务的使用和普及奠定了良好的群众基础。而且，随着 Internet 的急剧发展，Internet 在商业上的应用也逐渐发展、壮大起来。1998 年，通过 Internet 实现的销售额达到 400 多亿美元，到 1999 年，销售额猛增到 1800 亿美元；2013 年全球电子商务交易额将逾 16 兆美元。

### 1.1.4　电子商务的发展

Internet 使得任何规模的企业都能负担起电子商务活动的费用。银行间的电子资金转账（EFT）技术与企事业间的电子数据交换（EDI）技术相结合，产生了早期的电子商务或称电子商贸。信用卡（Credit Card）、自动柜员机（ATM）、零售业销售终端（POS）和联机电子资金转账（EFT）技术的发展，以及相应的网络通信技术和安全技术的发展，推动了今天网上持卡购物（B to C，Business to Consumer）与企业之间网上交易（B to B，Business to Business）的飞速发展。

（1）1991 年，美国政府宣布因特网（Internet）对社会公众开放，允许在网上开发商业应用系统。

（2）1993 年，Internet 上出现万维网，这是一种具有处理数据、图、文、声、像、超文本对象能力的网络技术，使因特网具备了支持多媒体应用的功能。

（3）1995 年，因特网上的商业业务信息量首次超过了科教业务信息量，这既是因特网此后产生爆炸性发展的标志，也是电子商务大规模起步发展的标志。

随后电子商务的安全性问题成为人们关注的焦点。针对 B to C 的模式，1996 年 2 月，Visa 与 Master Card 两大信用卡国际组织共同发起制定保障在因特网上进行安全电子交易的 SET 协议。该协议围绕客户、商家和交易各方相互之间身份的确认，采用了电子证书等技术，以保障交易安全。Visa 与 Master Card 两组织还共同建立安全电子交易有限公司（SETCO），专门从事管理与促进 SET 协议在全球的应用推广。

1994 年美国网景公司（Netscape）成立，该公司开发并推出支持 B to B 方式电子商务的安全套接层（SSL）协议，用以弥补因特网上的主要协议 TCP/IP 在安全性能上的缺陷（如 TCP/IP 协议难以确定用户的身份）。SSL 协议通过电子证书识别通信双方的身份，但 SSL 协议缺少数字签名功能，没有授权，没有存取控制，不能抗抵赖，用户身份还有被冒充的风险，这都是 SSL 协议在安全方面的弱点。这之后由加拿大 Entrust 公司开发出公钥基础设施（PKI，Public

Key Infrastructure）技术，弥补了 SSL 协议的缺陷。它支持 SET、SSL、IPSec 及电子证书和数字签名，可应用于 B to B 模式的电子商务中进行安全结算。

电子商务正以无比迅猛的势头发展着。在我国，因特网用户 1999 年初为 210 万，到 1999 年 12 月 31 日上网人数已达 890 万，2009 年我国网民人数已达 3.6 亿。其发展速度十分惊人，年增长率高于全球上网用户年增长率，具有良好的商业前景。

纵观近年来中国互联网市场的高速发展，电子商务行业也越发底气十足：2009 年 3 月，中关村在线宣布三年内投资 1 亿元打造自己的电子商务平台；2009 年 3 月，国内老牌社区天涯网借十周年庆典，正式切入电子商务领域，建立一个能满足人们各种需求的在线生活和商务平台成为天涯网未来的商务蓝图；2009 年 4 月，新浪总裁兼首席执行官曹国伟表示，新浪下一个 10 年将以发展电子商务为目标；2009 年 6 月，大型视频网站优酷与淘宝网共同发起的“视频购物”新应用技术开创了国内电子商务领域新的应用模式……

## 1.2 网络信息安全

### 1.2.1 网络信息安全的目标

所谓信息安全，一般是指在信息采集、存储、处理、传播和运用过程中，信息的自由性、秘密性、完整性、共享性等都能得到良好保护的一种状态。信息安全传输是指在网络上传递的信息没有被故意地或偶然地非法授权泄漏、更改、破坏或使信息被非法系统辨识、控制，网络信息的保密性、完整性、可用性、可控性得到良好保护的状态。

早期计算机网络的作用是共享数据，并促进大学、政府研究和开发机构、军事部门的科学研究工作。那时制定的网络协议，几乎没有注意到安全性问题。因为许可进入网络的单位都被认定为是可靠的和可以信赖的，并且已经参与研究和数据共享。然而，当 1991 年美国国家科学基金会（NSF）取消了互联网上不允许商业活动的限制后，越来越多的公司、企业、商业机构、银行和个人进入互联网络，利用其资源和服务进行商业活动，网络安全问题就渐渐突出。每个厂商都有一些不能为外人或竞争者知道的信息和数据，如特定的单证、交易金额、销售计划、客户名单等，他们不希望外部用户访问这些信息和数据。但是，计算机窃贼或破坏者却千方百计闯入互联网络和主计算机，盗用数据，破坏资源，制造事端。有时，尤其是在某些计算机系统缺乏安全保障措施时，善意的用户也可能会在网络中偶然获取到厂商暴露的信息和数据。在这种情况下，计算机网络安全技术应运而生，以满足这种发展中的需要，使得网络用户在获取同全球网络连接的好处的同时，保证其专用信息及资产的安全。

在因特网大规模普及特别是在电子商务活动逐渐进入实用阶段之后，网络信息安全更是引起人们的高度重视。网络交易需要大量的信息，包括商品生产和供应信息（商品的产地、产量、质量、品种、规格、价格等）、商品需求信息（消费者的个人情况、购买倾向、购买力的增减、消费水平和结构的变化等）、商品竞争信息（同行业竞购和竞销能力、新产品开发、价格策略、促销策略、销售渠道等）、财务信息（价格撮合、收支款项、支付方式等）、市场环境信息（政治状况、经济状况、自然条件特别是自然灾害的变化等）。这些信息通过合同、货单、文件、财务核算、凭证、标准、条例等形式在买卖双方以及有关各方之间不断传递。为保证整

个交易过程的顺利完成，必须保证上述信息的完整性、准确性和不可修改性。由于网络交易信息是在因特网上传递的，因此，相对于传统交易来说，网络交易对信息安全提出了更高、更苛刻的要求。

危及网络信息安全的因素主要来自两个方面：一是由于网络设计和网络管理方面的原因，无意间造成机密数据泄露；二是攻击者采用不正当的手段通过网络（包括截取用户正在传输的数据和远程进入用户的系统）获得数据。对于前者，应当结合整个网络系统的设计，进一步提高系统的可靠性；对于后者，则应从数据安全的角度着手，采取相应的安全措施，达到保护数据安全的目的。

一个良好的网络安全系统，不仅应当能够防范恶意的无关人员，而且应当能够防止专有数据和服务程序的偶然泄露，同时不需要内部用户都成为安全专家。设置这样一个系统，用户才能够在其内部资源得到保护的安全环境下享受访问公用网络的好处。

### 1.2.2　电子商务系统安全层次

电子商务系统既不是单纯的商务系统，也不是简简单单的计算机网络系统，而是建立在计算机网络系统之上的商务系统。从传统商务过渡到电子商务，交易过程中的物流同信息流、资金流发生了分离，而计算机网络系统是分离出来的这部分信息流和资金流的载体。电子商务环境下，人们在因特网上进行电子交易，信息流和资金流的可靠传输是前提，在此基础上，电子交易才有开展的可能，这就需要保障因特网上数据传输的安全性。但是仅仅保障了数据的安全传输尚不足以开展安全的电子交易活动。以往的商务活动基本上都是面对面的形式，交易的各方直接接触，身份认证不是一件太难的事，但是网上交易活动的参与者并不直接见面，只是通过因特网在一个虚拟的环境下交易，彼此之间的身份认证就是一个很大的问题，如果参与交易各方身份的真实性得不到保障，那么也就没有人从事网上交易了。因此，安全电子商务活动开展的另一个前提是必须建立一套公认的、可信的身份认证系统。

既然电子商务系统是建立在计算机系统之上的商务系统，从逻辑上看可以分成底层的物理系统和上层的业务逻辑系统。那么，电子商务系统的安全措施也相应地分成两个层次：一个是保障底层的物理系统的安全，也就是计算机网络系统的安全；另一个是保障上层业务逻辑系统的安全，也就是保证商务活动在网上的顺利开展。第一层安全措施是安全电子商务系统的基础，它保障了人们进行网上交易的虚拟场所的安全；第二层安全措施是安全电子商务系统的前提，它提供了网上交易不同于传统交易的交易规则，保证了网上交易过程的安全。这两方面的安全措施缺一不可，共同为安全电子商务活动的开展保驾护航。

计算机网络系统的安全首先是保障计算机网络系统中的实体的安全，那么计算机网络系统中究竟有哪些实体呢？简单地说，采用某种方式把若干台计算机连接起来就形成了计算机网络。因特网就是连接全球计算机的一个巨大的网络。因此，计算机网络系统中的实体也就是各种各样的计算机和连接它们的通信设备。网络中的计算机有些是提供 Internet 应用服务的，称之为服务器，例如 WWW 服务器、FTP 服务器和邮件服务器等，还有一些计算机是通过某些软件，例如浏览器，来访问这些服务的，统称为客户机；通信连接设备主要有路由器、交换机、集线器等。要保障计算机网络系统中实体的安全，实际上就是要保障这些计算机和它们之间的通信连接设备的安全。除了实体安全之外，数据安全也至关重要。前面提到了电子交易过程中物流同信息流和资金流发生了分离，安全电子交易系统必须保障分离出来的信息流和资金流的安全。计算机网络设备是电子商务活动中信息流和资金流的载体，各种信息流和资金流在计算

机网络环境中的具体表现就是数据，因此数据安全有了保障，信息流和资金流的安全也就有了保障。在计算机网络系统中，数据的安全一方面是存储安全，另一方面也包括数据在传输过程中的安全，即通信安全。

如果说第一层安全措施使开展电子商务活动变得可能，那么基于身份认证的第二层安全措施则为电子商务活动的开展提供了可行性。网上身份认证和网上支付是第二层安全措施的主要内容。

电子商务活动在虚拟的网络环境中开展，必须有一套公认的制度来约束网上交易各方的行为，使网上交易不因为环境的虚拟而变得不可捉摸。解决第二层安全问题，首先就是身份认证问题，这也是第二层安全措施的基础。身份认证就是要使参与网上交易的各方都有真实的身份，这个身份相当于一座桥梁，把网络环境同真实社区连接起来，使网络上的一切交易变得有凭有据，真实可信。有了身份认证后，网络上发生的所有活动变得不再虚无缥缈，虚拟的网络也变得实在起来，成为现实生活的真实延伸。只有在这样的网络环境下，电子交易才是可行的。

在赋予网络交易各方合法身份后，另一个关键的问题就是要解决现金的支付问题。同目前世界上的电子汇兑和清算系统相比，电子商务系统所要解决的支付问题难度更大，因为这里涉及的内容更多，范围更广，业务逻辑也更复杂。本书后面章节中会提到 SET 协议，它就是解决网上支付问题的一种手段。电子商务的支付是要解决网上资金流的安全性。资金流是现代商务活动中不可缺少的一项，电子商务也不例外。如果不能解决网上支付问题，商业利益得不到实现，网上交易是没有发展前途的。从这个意义上讲，网上支付是电子商务系统安全中最为敏感的问题，也是最终的安全问题。为了确保网上资金流的安全，网上支付不可避免地要牵涉身份认证，是在身份认证基础上进行的操作。

## 1.3 电子商务安全规范

电子商务的数据保密性、完整性、不可抵赖性以及网上交易者的隐私权等安全问题是影响电子商务发展的主要问题。高度开放的计算机网络环境下，非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、病毒与恶意攻击、线路窃听等引起的各种安全问题导致了极大的损害，仅美国每年的信息安全和网络安全问题所造成的经济损失就达 75 亿美元。据 1997 年 Yankee Group 的调查，消费者不愿在 Internet 上进行金融交易的原因，60%以上是出于安全上的考虑。可见，当前制约电子商务发展的关键因素，已不仅仅是产品技术方面的问题，更多的是出自对安全性的考虑。

当前电子商务的安全规范包括加密算法、报文摘要算法、安全套接层协议等方面的规范。

1. *加密算法*

基本加密算法有两种：对称密钥加密和非对称密钥加密，用于保证电子商务中数据的保密性、完整性、真实性和非抵赖服务。

（1）对称密钥加密。

对称密钥加密也叫秘密/专用密钥加密（如 Secret Key Encryption），即发送和接收数据的双方必须使用相同的对称的密钥对明文进行加密和解密运算。最著名的对称密钥加密标准是数据加密标准（Data Encryption Standard，DES）。DES 是一种使用 56 个数据位的密钥来操作 64 位数据块的块加密算法，由 IBM 公司推出，可同时对大量数据进行快速加密。美国政府于 1977 年 1 月 15 日将其颁布为联邦信息处理标准（Federal Information Processing Standard，FIPS），即 FIPS-46-2，至今已在银行业和其他一些领域用了 30 余年。DES 算法曾经过广泛的分析和

此为试读，需要完整PDF请访问：www.ertongbook.com