高等职业教育“十二五”规划教材
高职高专计算机应用技术系列教材

E-commerce security technology and training

电子商务安全技术与实训

彭　波　主编

科学出版社

高等职业教育“十二五”规划教材

高职高专计算机应用技术系列教材

电子商务安全技术与实训

彭　波　主　编
范荣真　副主编

科学出版社
北　京

内 容 简 介

本书以客户和管理员的角度，从客户端、服务器端、信息传输过程三个方面阐述了电子商务活动过程中应该注意的安全问题及采取的相应防范措施。主要内容包括电子商务安全概述、电子商务常见安全问题、客户端安全技术、电子商务支付安全技术、信息传输安全技术、服务器端安全技术、电子商务安全交易。

本书结合电子商务企业工作实际和课程理论，安排了13个实训项目，通过实训项目强化了学生的动手操作能力，真正做到“学中做，做中学”，为学生参加顶岗实习、就业实现了无缝对接，一定程度上减轻了企业和学生的压力。

本书可作为高职高专电子商务、移动商务和网络技术等专业的教材，也可供对电子商务安全技术感兴趣的读者参考使用。

图书在版编目(CIP)数据

电子商务安全技术与实训/彭波主编. —北京：科学出版社，2012
（高等职业教育“十二五”规划教材）
ISBN 978-7-03-034593-6

Ⅰ. ①电… Ⅱ. ①彭… Ⅲ. ①电子商务-安全技术-高等职业教育-教材
Ⅳ. ①F713.36

中国版本图书馆CIP数据核字（2012）第115610号

责任编辑：孙露露 赵丽欣 / 责任校对：耿 耘
责任印制：吕春珉 / 封面设计：耕者设计工作室

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
铭浩彩色印装有限公司印刷
科学出版社发行 各地新华书店经销
*
2013年3月第 一 版 开本：787×1092 1/16
2013年3月第一次印刷 印张：17 1/4
字数：411 000
定价：29.00元
（如有印装质量问题，我社负责调换<铭浩>）
销售部电话 010-62142126 编辑部电话 010-62135763-8212

前　言

电子商务是基于计算机软件技术、网络技术、通信技术、计算机硬件技术等发展和成熟起来的。正因为电子商务是在国际化、社会化、开放化和个性化的互联网环境中运作的，所以它面临着各种各样的安全威胁，如用户信用卡卡号、商家信息泄露，电子商务网站遭受拒绝服务攻击或者黑客入侵，交易双方对交易的抵赖，等等。

如何保证电子商务安全，提供对敏感信息及个人信息的加密保障、认证交易双方的合法身份以及保证商务数据的完整性等，已经成为电子商务发展的“瓶颈”问题，这也是许多人不愿进行网上购物和支付的重要原因。因此，十分有必要向参与电子商务活动的客户和管理人员普及电子商务安全相关的技术和方法。

本书正是基于上述原因而编写，主要以客户和管理员的角度，从客户端、服务器端、信息传输过程三方面阐述了电子商务活动过程中应该注意的安全问题和采取的相应防范措施。全书共 7 章，内容包括以下三部分。

（1）电子商务安全技术基础部分，包括第 1 章和第 2 章。第 1 章主要讲述电子商务安全基础，包括电子商务安全概述、电子商务安全问题、电子商务安全需求、电子商务安全技术、电子商务安全体系。第 2 章主要讲述电子商务常见安全问题，包括客户端常见安全问题、服务器端常见安全问题、信息传输常见安全问题。

（2）电子商务安全技术客户部分，主要从电子商务客户的角度讲述了应用电子商务过程中应该注意的安全问题和采用的安全技术，是本书的重点之一，包括第 3 章和第 4 章。第 3 章主要讲述客户端安全技术，包括客户端安全技术概述、计算机病毒与木马防范、操作系统安全技术、应用软件安全技术。第 4 章主要讲述电子商务支付安全技术，包括电子支付概述、电子商务支付安全技术。

（3）电子商务安全技术管理部分，主要从电子商务管理员的角度讲述了应用电子商务过程中应该注意的安全问题和采用的安全技术，是本书的重点之一，包括第 5 章、第 6 章和第 7 章。第 5 章主要讲述信息传输安全技术，包括黑客的攻击与防范、信息加密技术、防火墙技术。第 6 章主要讲述服务器端安全技术，包括网络操作系统安全设置、数据库安全技术。第 7 章主要讲述电子商务安全交易，包括电子商务安全交易概述、SSL 协议、SET 协议、SSL 和 SET 协议的比较。

本书结合电子商务企业工作实际和课程理论，安排了 13 个实训项目。通过项目强化学生的动手操作能力，真正做到“学中做，做中学”。

本书以理论结合实际动手操作为主要导向编写各章内容，选用的实训项目都运用了电子商务企业实际运营过程中常用的工具和软件，为学生参加顶岗实习、就业实现了无缝对接，一定程度上减轻了企业和学生的压力，适合于高职高专院校学生学习的特点。

本书由浙江商业职业技术学院信息技术学院彭波担任主编，范荣真担任副主编。浙江商业职业技术学院信息技术学院沈凤池院长在本书的编写过程中提出了宝贵的意见，在此表示衷心的感谢！学生林慧莹、蓝婷婷做了大量的文字录入和校对工作，在此一并表示感谢！

本书在编写过程中参考了大量相关领域的论著、图书、网络资料和文献，作者已尽可能在参考文献中一一列出，在此谨对这些作者表示诚挚的谢意，若有疏漏，也表示由衷的歉意！由于编者水平有限，书中难免有疏漏和不妥之处，敬请广大读者和专家批评指正。

编　者

目　录

第 1 章　电子商务安全基础 …… 1

1.1　电子商务安全概述 …… 1
1.2　电子商务安全问题 …… 4
1.3　电子商务安全需求 …… 5
1.3.1　电子商务信息服务安全需求 …… 5
1.3.2　电子交易的安全需求 …… 7
1.3.3　电子支付安全需求 …… 8
1.4　电子商务安全技术 …… 9
1.4.1　客户端安全技术 …… 9
1.4.2　服务器端安全技术 …… 11
1.4.3　信息传输安全技术 …… 12
1.5　电子商务安全体系 …… 13
思考与练习 …… 14
实训 …… 15
项目　了解电子商务安全问题和技术 …… 15
小结 …… 15

第 2 章　电子商务常见安全问题 …… 16

2.1　客户端常见安全问题 …… 16
2.1.1　计算机病毒 …… 17
2.1.2　计算机木马 …… 23
2.1.3　客户端操作系统安全问题 …… 27
2.1.4　应用软件安全问题 …… 32
2.2　服务器端常见安全问题 …… 36
2.2.1　网络操作系统安全 …… 36
2.2.2　数据库安全问题 …… 43
2.2.3　网站安全问题 …… 46
2.3　信息传输常见安全问题 …… 49
2.3.1　黑客攻击 …… 49
2.3.2　密码破解 …… 51
思考与练习 …… 54
实训 …… 56
项目一　客户端常见攻击——ARP 攻击 …… 56
项目二　服务器端常见攻击——DDoS 攻击 …… 62
项目三　信息传输常见攻击——Sniffer 嗅探器的使用 …… 65
小结 …… 70

第 3 章 客户端安全技术 ····· 72

3.1 客户端安全技术概述 ····· 72
3.2 计算机病毒与木马防范 ····· 72
3.2.1 杀毒软件使用 ····· 73
3.2.2 木马防范 ····· 86
3.3 操作系统安全技术 ····· 90
3.3.1 Windows 操作系统安全技术 ····· 90
3.3.2 UNIX/Linux 操作系统安全技术 ····· 93
3.4 应用软件安全技术 ····· 97
3.4.1 浏览器安全配置 ····· 97
3.4.2 其他常见应用软件安全配置 ····· 102
思考与练习 ····· 109
实训 ····· 111
项目一 计算机病毒与木马防范——冰河木马 ····· 111
项目二 操作系统安全配置——Windows 操作系统安全配置 ····· 118
项目三 安全防护软件的使用——360 安全卫士 ····· 131
小结 ····· 135

第 4 章 电子商务支付安全技术 ····· 136

4.1 电子支付概述 ····· 136
4.1.1 电子支付 ····· 136
4.1.2 电子支付系统 ····· 140
4.2 电子商务支付安全技术 ····· 144
4.2.1 电子支付安全隐患 ····· 144
4.2.2 电子支付安全措施 ····· 147
思考与练习 ····· 148
实训 ····· 149
项目 电子商务安全支付 ····· 149
小结 ····· 160

第 5 章 信息传输安全技术 ····· 162

5.1 黑客的攻击与防范 ····· 162
5.1.1 网络黑客概述 ····· 162
5.1.2 黑客攻击的目的及步骤 ····· 163
5.1.3 常用的黑客攻击方法 ····· 164
5.1.4 防范措施 ····· 178
5.2 信息加密技术 ····· 180
5.2.1 加密技术概述 ····· 180
5.2.2 对称加密技术 ····· 181
5.2.3 非对称加密技术 ····· 182

5.2.4 PGP 加密软件 183
5.3 防火墙技术 184
5.3.1 防火墙的类型 185
5.3.2 防火墙设计的安全要求与准则 188
5.3.3 典型的防火墙结构 189
5.3.4 创建防火墙的步骤 190
思考与练习 192
实训 193
项目一 X-scan 3.3 扫描工具的使用 193
项目二 PGP 加密软件的使用 197
项目三 ISA Server 2004 的安装与配置 205
小结 211
第 6 章 服务器端安全技术 212
6.1 网络操作系统安全设置 212
6.1.1 Windows Server 2003 安全设置 213
6.1.2 Red Hat Linux 安全设置 216
6.2 数据库安全技术 220
思考与练习 226
实训 227
项目 Windows Server 2003 安全配置 227
小结 234
第 7 章 电子商务安全交易 236
7.1 电子商务安全交易概述 236
7.2 安全协议 237
7.2.1 SSL 协议 237
7.2.2 SET 协议 239
7.2.3 SSL 和 SET 协议比较 243
思考与练习 244
实训 245
项目 证书服务的安装与管理 245
小结 260
思考与练习参考答案 261
参考文献 265

第1章

电子商务安全基础

知识教学目标

- 了解电子商务安全的六项中心内容
- 了解常见的电子商务安全问题
- 熟悉电子商务安全的需求
- 熟悉常见的电子商务安全技术
- 了解电子商务安全体系

技能培养目标

- 能够搜集电子商务安全方面的资料
- 能够跟踪电子商务安全技术的发展

进入21世纪以来，随着计算机网络、通信技术的飞速发展，特别是Internet在全球的广泛应用，电子商务已成为企业和组织进行各种商务活动的一种崭新的技术手段。它改变着人们的生活和工作方式，也带来了人们思维方式和行为准则的变化，其影响程度已经远远超过了技术和商务本身。电子商务作为一种新的商务模式，冲击着传统的商务模式，并影响着传统的商务流程，也使得企业和组织必须思考如何改进组织结构、管理思想等各方面工作，以适应电子商务的需要。

随着Internet的发展，电子商务逐渐成为人们进行商务活动的新模式，越来越多的人通过Internet进行商务活动。电子商务的发展前景十分诱人，而其安全问题也变得越来越突出，如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，已经成为商家和用户都十分关心的话题。

1.1 电子商务安全概述

随着电子商务在全球范围内的迅速发展，电子商务中的网络安全问题日渐突出。中国互联网络信息中心（CNNIC）发布的《第24次中国互联网络发展状况统计报告》指出：“我们特别提出来中国互联网面临着一个信任危机，比如说网络网民交易水平比较低，网络安全如诚信问题比较多，29.2%的网民认为网上交易是安全的，不到四成的网民愿意在网络上填写个人信息。”由此可见，保证电子商务中的网络安全、交易安全是促进电子商务稳定快速发展的关键。

知识窗

中国互联网络信息中心（CNNIC）是我国域名注册管理机构和域名根服务器运行机构。官方网站 http://www.cnnic.cn/，大约每隔半年发布一次中国互联网络发展报告。该网站提供了很多 Internet 安全的相关信息。

电子商务安全包括六项中心内容，如图 1-1 所示。

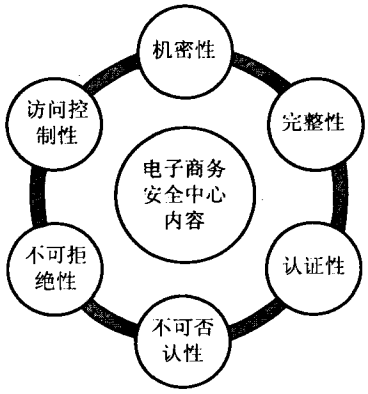

图 1-1 电子商务安全的六项中心内容

1. 商务数据的机密性

商务数据的机密性是指信息在网络上传送或存储的过程中，不被他人窃取，不被泄露或披露给未经授权的人或组织，或者经过加密伪装后，使未经授权者无法了解其内容。商务数据的机密性可用加密和信息隐匿技术实现。

2. 商务数据的完整性

商务数据的完整性是指信息在传输、交换、存储和处理过程中保持非修改、非破坏和非丢失的特性，即保持信息原样性，使信息能够正确地生成、存储、传输，这是最基本的安全特征。

3. 商务服务的认证性

商务服务的认证性是指网络两端的使用者在沟通之前相互确认对方的身份。

4. 商务服务的不可否认性

商务服务的不可否认性是指通信双方在信息交互过程中，确信参与者本身，以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

5. 商务服务的不可拒绝性

商务服务的不可拒绝性是指保证授权用户在正常访问信息和资源时不被拒绝，即保证为用户提供稳定的服务。

6. 访问的控制性

访问的控制性是指在网络上限制和控制通信链路对主机系统和应用的访问，用于保护计算机系统的资源（信息、计算和通信）不被未经授权人或以未经授权方式接入、使用、修改、发出指令或植入程序等。

自从互联网诞生之后，安全事故频出。例如，2000年2月7日至9日，短短三天时间，美国几大主要网站遭受不明黑客攻击，其中包括著名的电子商务网站电子港湾（eBay）和亚马逊（Amazon）。在黑客开始进行“拒绝服务（denial of service）”式的攻击后，亚马逊网站容纳顾客的能力急剧下降。数分钟后访客数量只有平时同时段的1.5%，大约一小时后才恢复正常。据统计，三天来黑客袭击各大网站所造成的直接或间接经济损失在数十亿美元以上。

再如，从2003年1月25日中午开始，一种蠕虫病毒在Internet上快速蔓延。美国一家网络监测公司报告指出，北美、欧洲和亚洲的Internet通信均发生了大面积堵塞，至少有2.2万个网络服务器遭到了病毒攻击，其中受影响最严重的地区是美国东部、欧洲北部和亚洲的一些地区。美国美洲银行称1.3万台自动取款机瘫痪，大量客户无法使用取款机取款。

在亚洲地区，韩国受害最严重。2003年1月25日下午2点左右，韩国Internet用户发现网络连接困难，负责Internet服务的韩国电信公司部分域名服务器受到大量数据连续攻击，服务器几乎陷于瘫痪状态。韩国通过Internet提供的服务项目，如各种票务预订、网上购物、电子邮件、网络电话等都受到了极大影响，遍布韩国的网吧经营也受到打击。韩国情报通信部在事故发生后立即宣布进入紧急工作状态，韩国电信公司也组织专家成立对策小组进行系统恢复，从而阻止了大量数据的继续侵入。

2004年2月，日本Internet服务商雅虎BB公司外泄450万份个人资料，引起社会指责，该公司以每份赔偿500日元平息此事，总计赔偿23亿日元。雅虎BB公司因此陷入财务危机。

2005年1月，东京迪斯尼乐园“终年通行证”的客户资料疑外泄，歹徒要求赎金，否则将公开这些资料。园方针对客户资料泄密事件向14万客户郑重道歉。2005年2月，NTT DoCoMo公司发生丑闻，大约24600名客户的数据被泄露。该数据可能是被内部员工从一个被认为很安全的、只有254名员工可以进入的房间偷出去。而此房间24小时由6台摄影机监控，员工必须先登记，并且经过瞳孔扫描，验明身份后方可进入。

美国万事达信用卡集团于2005年6月17日称，大约4000万信用卡顾客账户被一名黑客利用计算机病毒侵入，黑客可能将用户账号信息用于欺诈行为，而且多家银行的顾客账户都遭到了入侵。目前据悉，在4000万用户中，1390万用户属于万事达公司，2200万为VISA的用户，如果情况查实，这将是美国有史以来规模最大的信用卡信息失窃案。这也是美国境内公布的第12宗大量丢失客户或雇员重要个人信息的事故。

2006年11月，据Gartner表示，2006年网络销售商由于安全问题造成的损失高达9.13亿美元。另外，还有部分销售商由于拒绝网络支付而流失了部分客户，这部分损失大约有10亿美元。在美国1.55亿成年网民中，有46%的人表示担心信息被窃、数据泄露或基于互联网的攻击会影响他们的网络支付、在线交易或电子邮件行为。据Gartner表示，美国约有3300万人出于安全考虑而拒绝使用网络银行。根据调查，大约900万美国成人已经停止使用网络银行，而另外2370万人则由于安全问题一直没有使用网络银行。

2008 年，一个全球性的黑客组织，利用 ATM 欺诈程序在一夜之间从世界 49 个城市的银行中盗走了 900 万美元。目前 FBI 还未破案，据说嫌疑人也很难找到。

2009 年 7 月 7 日，韩国总统府、国会、国家情报院和国防部等国家机关网站，以及金融界、媒体和防火墙企业网站遭到黑客的攻击。两日后，韩国国家情报院和国民银行网站无法访问。韩国国会、国防部、外交通商部等机构的网站一度无法打开。这是有史以来韩国遭遇的最强的一次黑客攻击。

大量的案例表明，安全是电子商务的关键问题。若安全得不到保障，即使 Internet 再方便，网络购物再吸引人，电子商务也无法得到广大用户的认可。

1.2 电子商务安全问题

与现实商务不同的是，参与电子商务的各方不需要面对面进行商务活动，信息流和资金流都可以通过 Internet 来传输。而 Internet 是一个向全球用户开放的巨大网络，其技术上的缺陷和用户使用中的不良习惯，使得电子商务中的信息流和资金流在通过 Internet 传输时存在着以下安全问题。

1. 数据被非法截获、读取或者修改

在电子商务中，信息流和资金流以数据的形式在计算机网络中传输，很多都是远距离传输。在这一过程中，数据可能被别有用心者截获、读取，从而造成商业机密和个人隐私的泄密。更为严重的是，别有用心者还可能修改截获的数据，如把资金的数量、货物的数量、交货方式等进行修改，这会严重地影响电子商务的正常进行。为了防止出现上述情况，技术上采用的方法是对传输的数据进行加密，这样即使数据在传输过程中被截获，也能在很大程度上保证数据的安全性。

2. 冒名顶替和否认行为

在电子商务中，由于交易非面对面进行，如果安全措施不完善，无法对信息发送者或者接收者的身份进行验证，那么别有用心者就有可能冒充合法用户发送或者接收信息，从而给合法用户造成商务损失。另外，如果没有对交易者的身份进行验证，还可能有否认行为的发生，即别有用心者会否认自己在网络上进行过的操作，也就是赖账。为了防止冒名顶替和否认行为的发生，目前采用的技术主要有数字签名、非对称加密、认证等技术。

3. 未经授权用户访问网络

目前许多企业的内部网（Intranet）通常与 Internet 互联在一起，但如果没有经过企业的许可，外部用户是不能进入企业网进行访问的。但是，在安全措施不得力的情况下，有的未经授权的非法用户会设法进入企业内部网，这就是所谓的黑客侵扰。有的黑客甚至会登录企业内部的核心服务器，对企业的信息系统安全造成极大的危害。为了防止黑客的入侵，目前技术上一般采用设置防火墙的办法，在企业内部网和 Internet 之间设置一道“隔墙”，只有那些经过授权的合法用户才能进入企业内部网络。

4. 计算机病毒

计算机技术发展到今天，新的计算机病毒也层出不穷。Internet 的出现，更是刺激了计算机病毒的传播。而且计算机病毒的危害性也越来越严重。电子商务是一种依赖于计算机和计算机网络的新的商务模式，计算机病毒自然也对电子商务造成了很大的危害。如今，在技术上已经有了各种各样的计算机病毒防治措施。

电子商务的安全问题与解决措施如表 1-1 所示。

表 1-1　电子商务的安全问题与解决措施

安 全 问 题	解 决 措 施
数据被非法截获、读取或者修改	数据加密
冒名顶替和否认行为	数字签名、非对称加密、认证等
未经授权用户访问网络	防火墙
计算机病毒	计算机病毒防治措施

1.3　电子商务安全需求

电子商务安全需求从整体上可分为三大部分，即电子商务信息服务安全需求、电子交易的安全需求和电子支付安全需求。

1.3.1　电子商务信息服务安全需求

为了提供电子商务信息服务，我们需要建立一套完整的电子商务安全服务系统。该系统需要确保安全无误地为用户提供电子商务安全服务，确保系统实体安全、系统运行安全和系统信息安全。

1. 系统实体安全

实体安全是指保护计算机设备、设施以及其他媒体免受自然灾害和其他环境事故（如电磁污染等）破坏的措施、过程。电子商务系统的实体安全由三部分组成：环境安全、设备安全和媒体安全。

（1）环境安全

环境安全就是要对电子商务系统所在的环境加以安全保护，主要包括灾害保护和区域保护。

（2）设备安全

设备安全是指对电子商务系统的设备（包括网络）进行安全保护，主要是设备防盗、设备防毁、防电磁信息泄漏、防线路截获、抗电磁干扰以及电源保护。

（3）媒体安全

媒体安全是指对媒体数据和媒体本身实施安全保护。

2. 系统运行安全

电子商务系统安全的第二个部分是运行安全，它是指为保障系统功能的安全实现，提

供一套安全措施来保护信息处理过程的安全。运行安全涉及四个方面：风险分析、审计跟踪、备份与恢复和应急措施。

（1）风险分析

风险分析就是要对电子商务系统进行人工或自动的风险分析。

（2）审计跟踪

审计跟踪就是要对电子商务系统进行人工或自动的审计跟踪，保存审计记录和维护详尽的审计日志。

（3）备份与恢复

运行安全中的备份与恢复，就是提供对系统设备和系统数据的备份与恢复。

（4）应急措施

运行安全中的应急措施，是为了在紧急事件或安全事故发生时，提供保障电子商务系统继续运行或紧急恢复所需的策略。

3. 系统信息安全

系统信息安全是指防止信息财产被故意地或偶然地非授权泄漏、更改、破坏或使信息被非法的系统辨识、控制，信息安全要确保信息的完整性、保密性、可用性和可控性。系统信息安全由以下七个部分组成。

（1）操作系统安全

1）安全操作系统是指从系统设计、实现和使用等各个阶段都遵循了一套完整的安全策略的操作系统。

2）操作系统安全部件的目的是增强现有操作系统的安全性。

（2）数据库系统安全

1）安全数据库系统是指从系统设计、实现、使用和管理等各个阶段都遵循一套完整的系统安全策略的数据库系统。

2）数据库系统安全部件是以现有数据库系统所提供的功能为基础构建安全模块，旨在增强现有数据库系统的安全性。

（3）网络安全

1）网络安全管理是指为网络的使用提供安全管理。

2）安全网络系统是对网络资源的访问和网络服务的使用提供一套完整的安全保护，即从网络系统的设计、实现、使用和管理各个阶段，遵循一套完整的安全策略的网络系统。

3）网络系统安全部件

（4）计算机病毒防护

计算机病毒防护包括单机系统病毒防护、网络系统病毒防护、网络系统安全部件防护三个部分。

（5）访问控制

1）出入控制是为了阻止非授权用户进入机构或组织。

2）存取控制是针对主体访问客体时的存取控制，例如，通过对授权用户存取系统敏感信息时进行安全性检查，以实现对授权用户的存取权限的控制。

（6）加密

加密是将明文数据进行某种变换，使其成为不可理解的形式的过程。加密必须依赖两

个要素，即算法和密钥。

（7）鉴别

鉴别是指提供身份鉴别和信息鉴别。身份鉴别是提供对信息收发方（包括用户、设备和进程）真实身份的鉴别；信息鉴别是提供对信息的正确性、完整性和不可否认性的鉴别。

1.3.2 电子交易的安全需求

在电子商务交易过程中交易双方利用信息技术来传输和处理商业信息，所以如何保证电子交易过程中的安全是十分重要的。电子交易的安全需求又包含以下几个方面内容。

1. 信息的保密性

在传统的贸易中，一般都是通过面对面的信息交换，或者通过邮寄封装的信件、可靠的通信渠道发送商业报文，以达到保守商业机密的目的。而电子商务是建立在一个开放的网络环境下，当交易双方通过 Internet 交换信息时，因为 Internet 是一个开放的公用互联网络，如果不采取适当的保密措施，那么其他人就有可能知道交易双方的通信内容；另外，存储在网络的文件信息如果没有加密，也有可能被他人窃取。上述种种情况都有可能造成商业信息的泄露，导致商业上的巨大损失。例如，如果客户的信用卡账号和用户名泄露，就可能被人盗用；如果企业的订货和付款信息被竞争对手获悉，就可能丧失商机。

因此，电子商务一个重要的安全需求就是信息的保密性。这就意味着，必须对敏感重要的商业信息进行加密，即使别人截获或窃取了数据，也无法识别信息的真实内容，这样商业信息就难以被泄露。

2. 信息的完整性

信息保密性是针对网络面临的被动攻击类威胁而提出的安全需求，但它不能避免针对网络所采用的主动攻击类的威胁。所谓被动攻击，就是不修改任何交易信息，但通过截获、窃取、观察、监听、分析数据流和数据流式获得有价值的情报。而主动攻击就是篡改交易信息，破坏信息的完整性和有效性，以达到非法的目的。例如，在电子交易中，乙给甲发了一份报文："请给丁汇 100 元。乙"。报文在报发过程中经过了丙之手，丙就把"丁"改为"丙"。这样甲收到后就成了"请给丙汇 100 元。乙"，结果是丙而不是丁得到了 100 元。当乙得知丁未收到钱时就去问甲，甲出示有乙签名的报文，乙就会发现报文被篡改了。

因此，保证信息的完整性也是电子商务活动中的一个重要的安全需求。这就意味着，交易各方能够验证收到的信息是否完整，即信息是否被他人篡改过，或者在数据传输过程中是否出现信息丢失、信息重复等差错。

3. 身份的可认证性

在传统的交易中，很容易确认对方的身份。即使开始不熟悉、不能确信对方，也可以通过对方的签名、印章、证书等一系列有形的身份凭证来鉴别其身份。另外，在传统的交易中如果是采用电话进行通信，也可以通过声音来识别对方身份。然而，在进行网上交易时，情况就大不一样了，因为网上交易的双方可能素昧平生，相隔千里，并且在整个交易过程中都可能不见一面。因此，如果不采取任何新的保护措施，就可能比传统的商务活动

更容易出现假冒、诈骗等违法活动。例如，在进行网上购物时，对于客户来说，如何确信计算机屏幕上显示的页面就是大家所说的那个正规的网上商店，而不是居心不良的人冒充的呢？同样，对于商家来说，怎样才能相信正在选购商品的客户不是骗子，而是一个当发生意外事件时能够承担责任的客户呢？

因此，电子交易的首要安全需求就是要保证身份的可认证性。这就意味着，在双方进行交易前，首先要能确认对方的身份，即要求交易双方的身份不能被假冒或伪装。

4. 可靠性与不可抵赖性

由于商情千变万化，交易合同一旦达成就不能抵赖。在传统的贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章，确定合同、契约、单据的可靠性并预防抵赖行为的发生，这也就是人们常说的“白纸黑字”。但在无纸化的电子交易中，就不可能再通过传统的手写签名和印章来预防抵赖行为的发生。因此，必须采用新的技术，以防止电子商务中的抵赖行为，否则就会引起商业纠纷，使电子商务无法顺利进行。例如，在电子商务活动中订购冰箱时，如果订货时冰箱价格较低，但收到订单后，冰箱价格上涨了，假如供应商否认收到订单的事实，则采购商就会蒙受损失；同样，如果收到订单后，冰箱价格下跌了，假如订货方否认先前发出订货单的事实，则供应商就会蒙受损失。

因此，保证交易过程中的不可抵赖性也是电子商务安全需求中的一个重要方面。这就意味着，在电子交易通信过程的各个环节中都必须是不可否认的，即交易一旦达成，发送方不能否认其发送的信息，接收方则不能否认其收到的信息。

5. 审查能力与不可伪造性

在商务活动中，交易的文件是不可被修改的，如上述订购冰箱一案，如果供应商在收到订单后，发现冰箱价格大幅上涨了，假如能改动订单内容，将订购数 100 台改为 10 台，则可大幅受益，那么采购商就会因此而蒙受巨大损失。在传统的贸易中，可以通过合同字迹的技术鉴定等措施来防止交易过程中出现的伪造行为，但在电子交易中，由于没有书面合同，因而无法采用字迹的技术鉴定等传统手段来裁决是否发生了伪造行为。

因此，保证交易过程中的不可伪造性也是电子商务安全需求中的一个方面。这就意味着，电子交易文件也要能做到不可修改，以保障交易的严肃和公正。

6. 内部网的严密性

企业的内部网，一方面有着大量需要保密的信息，另一方面传递着企业内部的大量数据，控制着企业的业务流程。企业内部网一旦被恶意侵入，可能给企业带来极大的混乱与损失。例如，黑客一旦非法闯入银行的内部网，就可以修改存款数据、划拨资金；又如，对一些自动化程度高的企业而言，内部网若被恶意侵入，企业的经营活动就会陷入混乱，将无法按照规定的程序生产或生产出大量废品，产品被送到不需要的地方，资金被非法划拨等。因此，保证内部网不被侵入，也是开展电子商务的企业应着重考虑的一个安全问题。

1.3.3 电子支付安全需求

在传统的交易中，交易双方往往通过现金、支票等看得见、摸得着的方式进行支付。

随着以 Internet 为基础的电子商务时代的到来，支付问题就愈显突出，电子支付手段是解决电子商务支付的唯一手段。所以如何保证电子支付过程中的安全问题也是电子商务中迫切需要解决的问题。其具体体现为以下几个方面。

（1）电子支付制度

电子支付制度也和其他的传统付款方式相同，都会因为被他人冒领、盗领款项而发生损失，如有人侵入他人网络系统，或伪造他人私钥、信用卡等资料。而网络电子支付制度若无法保障交易安全，则可能会使消费者遭受更大的损失。

（2）电子支付系统

电子支付系统若发生断线、操作错误等问题，可能会对消费者经济方面造成损失。消费者在利用电子支付方式时，也可能发生虽然有钱，但是却因为断线、厂商拒收或其他原因，而无法在一定时间、地点完成特定金额的交易。

（3）隐私外露

消费者在进行电子支付时，还可能面临另一个风险，那就是所有的付款信息可能未经消费者的同意即被收集或向第三方披露，甚至被冒用或以其他不利于消费者利益的目的而使用，反而侵害消费者的隐私权。

（4）电子支付工具

电子支付工具的使用，也可能造成新的犯罪问题。例如，电子支付制度可能会鼓励如洗钱这种不法活动，或供网络赌博之用，其中网络赌博所产生的付款问题已经逐渐显现出来。而现在由于各国对电子支付工具并未加以规范，因此也不需要有保存交易记录、报告或确认客户身份等义务，从而无法追踪，反而产生规范的死角。而网上银行的兴起，则将使管制措施难以强制执行，因为有意规避监管、在海外开设有银行账户的人士很容易得逞。此外，新的电子支付工具本身也可能成为犯罪的目标，如伪造、变造、欺诈等犯罪行为，也可能会以电子工具为目标。

1.4 电子商务安全技术

针对电子商务安全问题以及由此提出的电子商务安全需求，目前国内外专业人士和相关厂商都提出了很多解决方案，通过这些方案的应用，基本上保证了电子商务活动过程中的安全问题。在这些解决方案中，主要涉及的安全技术有加解密技术、数字认证技术、CA 安全认证体系、安全电子交易协议、虚拟专用网技术、反病毒技术、黑客防范及其他相关的网络安全技术。根据电子商务活动的过程，把这些安全技术归结为三类：客户端安全技术、服务器端安全技术和信息传输安全技术。

1.4.1 客户端安全技术

客户端安全技术包括计算机病毒与木马防范技术、操作系统安全技术、应用软件安全技术三部分。

1. 计算机病毒与木马防范技术

信息技术的飞速发展虽然极大地推动了计算机网络的普及，但同时也大大地促进了计