HZ BOOKS
华章教育

高等院校电子商务专业规划教材

电子商务安全管理

闫强 胡桃 吕廷杰 编著

E-Commerce
Security Management

36
.1

机械工业出版社
China Machine Press

F713.36
Y225.1

高等院校电子商务专业规划教材

电子商务安全管理

闫强 胡桃 吕廷杰 编著

E-Commerce Security Management

机械工业出版社
China Machine Press

本书结合电子商务、信息管理与信息系统等本科专业的教学实践，将网络与信息安全技术和具体管理实践相结合，从技术和管理两方面对电子商务安全管理进行深入论述。在技术方面，本书从密码学的基本知识入手，介绍了身份鉴别、访问控制、互联网安全机制、PKI及包括防火墙、入侵检测、VPN、病毒防范等在内的主要网络安全应用技术。在管理方面，介绍了建立安全管理体系的原理及过程，进而对电子商务中的风险管理、信用管理及有关的法律法规进行了系统介绍。

本书可以作为大专院校本科生和研究生电子商务、信息管理与信息系统等专业教材，也可以作为从事电子商务教学、科研及管理工作相关人员的参考书。

版权所有，侵权必究

本书法律顾问　北京市展达律师事务所

图书在版编目（CIP）数据

电子商务安全管理/闫强，胡桃，吕廷杰编著. －北京：机械工业出版社，2007.5
（高等院校电子商务专业规划教材）
ISBN 978-7-111-21350-5

Ⅰ. 电…　Ⅱ. ①闫…　②胡…　③吕…　Ⅲ. 电子商务－安全－技术－高等学校－教材
Ⅳ. F713.36

中国版本图书馆CIP数据核字（2007）第055854号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：胡智辉　　版式设计：刘永青
北京牛山世兴印刷厂印刷 · 新华书店北京发行所发行
2007年5月第1版第1次印刷
184mm × 260mm · 16.25印张
定价：30.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线：（010）68326294
投稿热线：（010）88379007

前言

20世纪90年代以来，信息通信技术得到了飞速发展，信息的处理和传输突破了时间和地域的限制，各种基于互联网的应用不断出现，电子商务作为其中的一种新生事物，更是得到了众人的瞩目。然而，信息通信技术在推动人类文明进步的同时，也带来了严峻的安全问题，系统漏洞、黑客攻击、计算机病毒等各类安全问题已经严重影响了互联网的健康发展，并制约了电子商务等以互联网为基础的各类应用的推广与普及。在这种情况下，学习、研究电子商务安全相关的技术与管理措施，对推动互联网的健康发展、促进电子商务的应用与推广都具有重要的现实意义。

本书是结合电子商务、信息管理与信息系统等本科专业的教学实践编写而成的。在传统的教学过程中，网络与信息安全是一门技术性非常强的课程。而电子商务、信息管理与信息系统等专业的定位则要求学生不仅能够了解和掌握基本的安全技术，还应能与具体的管理实践结合起来，这就对传统的网络与信息安全教学提出了挑战。同时，网络与信息安全也一贯强调“三分技术、七分管理”，在网络与信息安全技术和电子商务的发展过程中，越来越多的管理问题浮现出来，如信用管理、风险管理等，这些问题都要求对传统网络与信息安全教学内容不断地进行更新和扩展。

结合电子商务的发展需求及我们的教学实践，本书的编写在内容结构上进行了一定的创新与探索。本书第1～7章侧重于基本的网络与信息安全技术，而第8～11章则侧重于网络与信息安全管理方面的内容。在技术方面，本书从密码学的基本知识入手，介绍了身份鉴别、访问控制、互联网安全机制、PKI及包括防火墙、入侵检测、VPN、病毒防范等在内的主要网络安全应用技术。在管理方面，本书介绍了建立安全管理体系的原理及过程，进而对电子商务中的风险管理、信用管理及有关的法律法规进行了讲解。

同目前多数信息安全相关的书籍相比，本书的一个主要特色是在系

统介绍电子商务安全技术的同时，突出了电子商务安全管理的内容。在电子商务安全架构的设计中，体现了人、技术、过程三方面因素的有机结合。

本书主要面向电子商务、信息管理与信息系统等专业的本科生、研究生以及从事电子商务教学、科研及管理工作的相关人员。考虑到本书所面对的读者的特点，书中对密码算法、协议等内容并没有着以太多的笔墨，除保留一些基础、核心的内容外，重点介绍了其原理与应用，使读者既能掌握电子商务安全的基础知识，又能建立电子商务安全的整体概念，而不致陷于技术的细节。

在本书编写过程中，我们在教学讲义的基础上，吸收了大量其他研究人员的研究成果；我校研究生黄晓燕、沙际品、郭倩瑜、宗培、何栋等参与了本书资料的收集及初稿的整理，在此向他们表示衷心的感谢！

由于作者水平有限，加之技术发展日新月异，本书难免存在缺点与错误，恳请广大读者不吝赐教。

闫　强

2007年3月

于北京邮电大学经济管理学院

此为试读，需要完整PDF请访问：www.ertongbook.com

教学建议

本书内容可以分为三大部分。第一部分即第1章，旨在帮助学生了解电子商务安全的整体框架；第二部分包括第2～7章，主要介绍网络与信息安全相关的技术知识；第三部分包括第8～11章，主要介绍电子商务安全相关的管理性内容。

根据课程学时的安排，教学中可对书中内容进行适当选择。下面以34学时和51学时教学安排为例，列出了教学内容的安排情况，供大家参考。

教学内容	学习要点	课时安排	
		34学时	51学时
第1章	电子商务安全的基本概念与整体架构	2	2
第2章	密码学基本概念与原理、主要算法与协议	6	8
第3章	身份鉴别的概念、机制及协议	2	4
第4章	访问控制的概念、策略、机制及授权管理	2	4
第5章	互联网安全体系结构、IPSec、SSL	4	6
第6章	PKI的构成、数字证书、信任管理	2	4
第7章	防火墙、VPN、入侵检测、病毒防范（可根据课时安排选择讲解部分内容）	4	6
第8章	安全管理的理念及ISMS的建立、运行、评审及认证	4	5
第9章	风险管理的原理、风险评估与风险处理	3	4
第10章	信用管理模式、信用评价、跟踪、保障机制	3	4
第11章	电子商务安全管理相关的标准及法律法规	2	4

目录

第1章 电子商务安全概论

本章概要

信息通信技术的进步推动了电子商务的发展，而安全问题则是影响电子商务发展的一个重要因素。本章在简要介绍电子商务基本概念的基础上，指出了电子商务安全的基本要求，讨论了电子商务面临的安全威胁，并在最后给出了电子商务的整体安全架构。

学习目标

1. 了解电子商务的基本概念；
2. 掌握电子商务安全的基本要求；
3. 掌握电子商务面临的安全威胁；
4. 掌握电子商务安全架构。

基本概念：电子商务　安全要求　安全威胁　安全架构

20世纪90年代以来，信息通信技术得到了飞速发展，信息的处理和传输突破了时间和地域的限制，各种基于互联网的应用不断出现，电子商务作为其中的一种新生事物，更是得到了众人的瞩目。

然而，信息通信技术在推动人类文明进步的同时，也带来了严峻的安全问题，系统漏洞、黑客攻击、计算机病毒等各类安全问题已经严重影响了互联网的健康发展，并制约了电子商务等以互联网为基础的各类应用的推广与普及。根据第17次中国互联网络发展状况统计报告，我国网民中对网络的安全性及对个人隐私保护的满意度均不到30%；而全球范围内的统计数据显示，网络安全与隐私保护已成为阻碍人们接受电子商务的最主要的两个因素。因此，学习、研究电子商务安全相关的技术与管理措施，对推动互联网的健康发展、促进电子商务的应用与推广都具有重要的现实意义。

1.1 电子商务基础

1.1.1 电子商务的概念

电子商务由于历史比较短，发展又极为迅速，目前人们对电子商务的认识还处于不断发展和完善之中。各国政府、学者、企业界人士根据自己所处的环境和对电子商务的参与程度，分别对电子商务给出了不同的阐释。

纵观近年来人们对电子商务认识的演变，各种定义的区别主要体现在电子和商务这两个词的外延上。

这里的“电子”即电子技术，是一个覆盖范围极广的领域。无疑，电子技术是现代高新技术的核心，而现代电子技术的核心又是计算机技术和通信技术，计算机网络是计算机技术和通信技术相结合的产物，Internet则是计算机网络技术到目前为止最为重要的应用。可以说，自20世纪90年代中期以来，Internet是整个电子技术乃至整个高新技术中发展最快的领域之一。由于Internet在整个电子技术中的特殊地位，在对电子商务概念的理解中，一般人认为“电子”指的就是Internet。当然，也有人认为电子商务中的“电子”是以Internet为主要工具，同时也包括其他计算机网络、通信设备（如电话、传真）等电子手段。甚至还有人认为，电子商务中的“电子”就是现代高新技术，商务活动中使用到的高新技术手段都可以被包括在“电子”一词中。

再来看对“商务”的理解，西方学者认为，商务是将社会资源转换为货物和服务，并以盈利为目的向消费者进行销售的有组织的活动。这里的货物指的是有形的商品，可以看得见摸得着，而服务是无形的，具有劳动和使人得到某种满足的特征。这里的社会资源则包括自然资源、资本、劳动力和企业家等。在这个定义中，商务的核心是销售活动。与一般的销售活动相比较，商务活动的规模较大，具有严格的商业协议，并受到相应的法律法规的保护，是一种有组织的活动。人们在使用商务这一概念时，也有广义和狭义之分。有人认为，企业的活动都直接或间接与销售有关，因此，除了销售，企业的其他活动如原材料采购、产品制造等也属于商务活动。有人则认为，商务活动只包括企业产品的销售和服务的提供。

鉴于对“电子”和“商务”的不同理解，一些组织、机构和个人从不同的角度出发，对“电子商务”给出了不同的定义，例如：

- 美国政府在其“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。”显然，在该定义中，对商务活动的定义是很笼统的。
- 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为：电子商务是以电子通信为手段的经济活动，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。
- 联合国国际贸易程序简化工作组对电子商务的定义为：采用电子形式开展的商务活动，它包括在线供应商、客户、政府及其参与方之间通过任何电子工具，如EDI、Web技术、电子邮件等共享非结构或结构化商务信息，并管理和完成商务活动、管理活动和消费活动中的各种交易。

• IBM公司对电子商务的理解是，电子商务是在Internet的广阔联系与传统信息技术系统丰富资源相结合的背景下产生的一种在互联网上展开的互相关联的动态商务活动。电子商务又有广义和狭义之分，狭义的电子商务称作电子交易，主要指利用Internet提供的通信手段在网上进行的交易。而广义的电子商务则包括电子交易在内、利用Internet进行的全面的商业活动，如市场调查分析、财务核算、生产计划安排、客户联系、物资调配等。

从上面的各种定义中可以看到，从外延来看，最广义的概念把电子商务定义为利用一切电子手段进行的所有商业活动，最狭义的概念则认为电子商务是在Internet上进行的贸易活动。

在许多资料中，E-Commerce(EC) 和E-Business(EB) 都被翻译为电子商务。一般来说EC是以商品的买卖为中心的，在以Internet为平台的商品交换出现之后，西方媒体上最先使用的就是这一词汇，有人将其译为电子贸易；而EB则是IBM公司在1997年率先推出的电子商务概念。IBM认为，电子商务不仅包括在线的商品交换，而且还应包括对客户的服务和商业伙伴间的合作，甚至认为企业在其按照Internet标准构造的企业内部网（Intranet）和企业互联网（extranet）上从事的业务都包括在EB之中。有人将EB翻译为电子业务；有人认为，EB包括了EC，而EC是EB的精华所在。值得注意的是，许多英文资料上的作者并没有严格区分EC和EB，有时甚至混用。

本书中，我们认为电子商务是指以Internet为主要信息传输手段而进行的商务活动。这里的商务活动包括以盈利为目的而进行的产品买卖活动和服务提供活动，以及企业为了实现产品的买卖和服务的提供而进行的内部管理和外部协调活动，如市场调查分析、财务核算、生产计划安排、客户联系及物资调配等。

1.1.2 电子商务的交易模式

电子商务交易是指在网络平台基础上直接进行的在线交易（trade on line），利用数字化技术将企业与企业、企业与消费者或消费者之间有机地连接起来，实现从浏览、洽谈、签约、交货到付款等全部或部分业务的自动化处理。目前，按照参与交易的对象和交易的产品类型，我们可以将电子商务交易分为不同的模式。

1. 按照参与交易的对象来划分

按照电子商务中参与交易的对象，可以把电子商务的交易模式分为以下三类：

（1）企业对企业（business to business）模式，有时简写为BtoB或B2B模式，是指商业企业之间进行的电子商务活动，这是最早出现的电子商务模式。企业通过互联网来与供应商联系订货、接收发票和付款。企业之间也可以通过网络来实现协同作业、资源管理及信息共享，以推动分销商、经销商和中心企业之间供应链的重组，提高业务的有效性并降低成本。

（2）企业对消费者（business to customer）模式，有时简写为BtoC或B2C模式，是指商业企业与消费者个人之间进行的电子商务活动。随着网上商店的出现，产生了这种电子商务模式。这种模式既包括网上购物，也包括针对个人的网上银行等服务型的业务。企业利

此为试读，需要完整PDF请访问：www.ertongbook.com

用网站设计技术在Internet上开设店面、陈列商品、标示价格、说明服务，向消费者直接提供从鲜花、图书、汽车、住房到订票、旅游、转账等众多商品和服务。这种模式直接针对消费者，开创了一个崭新的庞大市场。由于个人的商业行为和商家的商业行为之间有着较大的差异，因此B2B和B2C之间也有着较大的差异。

（3）消费者对消费者（customer to customer）模式，有时简写为CtoC或C2C模式，也被称为网上拍卖模式。在该模式中，消费者之间通过Internet来交换需求信息。一般情况是，在专门的拍卖网站上，消费者将自己需要出售的商品信息公示，需要此类商品的消费者在获知信息之后，通过Internet来报价。买卖双方达成协议后，一桩交易就通过网络初步实现了。在这里，网络的中介作用得到了充分体现。目前，全球比较著名的拍卖网站如美国的eBay公司（http://www.ebay.com）。值得注意的是，以C2C模式来交易的一般是单件产品或件数很少的产品，如一台电脑、一台数码相机等。如果卖家希望交易的产品数量较多，则卖家就成为商业企业，该模式也就转换为B2C了。

除以上介绍的三种主要模式外，还有其他的运行模式，如government to government、government to business、government to customer等，这几种模式涉及电子政务的概念，且不如前三种模式的应用广泛，因此这里不再赘述。

2. 按照交易产品的类型来划分

产品是指能够满足人们的某种需要和欲望的东西。根据产品的存在和表现形式，可以将所有产品分为有形产品（实体产品）、无形产品（包括服务和数字类产品）。根据电子商务中用于交易的产品类型的不同，可以将电子商务分为以下两种运行模式。

（1）有形产品电子商务。根据中国互联网信息中心（CNNIC）的调查，适合通过互联网来直接向消费者销售的有形产品包括：图书、报纸、杂志及其他纸质出版物；音像制品，包括CD、VCD、DVD；电脑、电脑配件（如内存、硬盘）及电脑周边设备（如打印机、扫描仪等）；服装；MP3、手机等家电产品；化妆用品；体育用品；办公用品。有形产品电子商务的最重要特点就是有形产品必须通过物流渠道来实现在交易双方之间的转移。因此，适合通过互联网来直接向消费者销售的有形产品，往往具备体积小、便于运输的特点。此外，由于电子商务中的交易是非面对面的（即具有虚拟性），基于消费安全上的考虑，适合在电子商务中直接向消费者销售的有形产品往往是那些价值不是特别大，而质量又能得到保证的产品。在B2B中，交易活动往往是在贸易伙伴之间进行的，交易的有形产品可以是大宗的，如钢材交易、医院药品的采购等。

（2）无形产品电子商务。目前，电子商务中交易的无形产品有两大类。一类是可以以数据形式存在的数字产品，如软件、可以下载或者是在线播放的音像品等。这类数字产品以数据文件的形式而存在，消费者在购买之后可以通过计算机的转换来满足购买者的需求。另一类无形产品是服务，如网上订票、网上订酒店、网上咨询及网络学校等。无形产品电子商务的最大特点就是所交易的产品可以直接通过Internet来实现传输，不存在实物的物流问题，因此可以充分发挥Internet信息传输效率高、用户覆盖面广、不受时间、气候因素影响等优势。目前，服务业发展很快，在整个国民经济中所占的比例越来越大，无形产品电子商务已经成为电子商务的一个重要发展方向。

1.1.3 电子商务的交易过程

由于电子商务交易是在Internet上进行的，因此Internet是电子商务最基本的架构。另外，电子商务交易涉及商家、消费者、银行或金融机构、信息公司或证券公司、企业、政府机构、认证机构、配送中心等很多方面。由于参与电子商务中的各方在物理上是互不了解的，因此整个过程并不是物理世界交易过程的完全搬照。

电子商务的交易过程大致可以分为以下四个环节：

（1）交易前的准备。这一阶段主要是指买卖双方和参加交易各方在签约前的准备活动。

买方根据自己的需求，利用Internet和各种电子商务网络寻找自己满意的商品和商家，通过市场查询，确定购货计划（包括确定购买商品的种类、数量、规格、价格、购货地点和交易方式等）。

卖方根据自己所销售的商品，进行市场调查和市场分析，制定各种销售策略和销售方式，利用Internet和各种电子商务网络发布商品信息，寻找贸易伙伴和交易机会，扩大贸易范围和商品所占市场的份额。

其他参加交易各方（如中介方、银行金融机构、信用卡公司、海关系统、商检系统、保险公司、税务系统及运输公司等）也应为后期电子商务交易的开展做好相应准备。

（2）交易谈判和签订合同。这一阶段主要是指买卖双方对所有交易细节进行谈判，将双方磋商的结果以文件的形式确定下来，即以书面文件形式和电子文件形式签订贸易合同。电子商务的特点是可以签订电子商务贸易合同，交易双方可以利用现代电子通信设备和通信方法，经过认真谈判和磋商后，将双方在交易中的权利、所承担的义务、对所购买商品的种类、数量、价格、交货地点、交货期、交易方式和运输方式、违约和索赔等合同条款，全部以电子交易合同做出全面详细的规定，合同双方可以利用电子数据交换（EDI）进行签约，也可以通过数字签名等方式签名。在一些小额的B2C、C2C交易中，也可能不会签订交易合同，但交易各方仍需对交易有关的信息进行必要的确认与核实。

（3）办理交易进行前的手续。这一阶段主要是指买卖双方签订合同后到合同开始履行之前办理各种手续的过程，也是双方贸易前的交易准备过程。交易中要涉及有关各方，即可能要涉及到中介方、银行金融机构、信用卡公司、海关系统、商检系统、保险公司、税务系统、运输公司等，买卖双方要利用EDI与有关各方进行各种电子票据和电子单证的交换，办理好各种手续，以便后续交易的进行。

（4）交易合同的履行和索赔。这一阶段是从买卖双方办完所有各种手续之后开始，卖方要备货、组货，同时进行报关、保险、取证、信用等，卖方将所购商品交付给运输公司包装、起运、发货，买卖双方可以通过电子商务服务系统跟踪发出的货物，银行和金融机构也按照合同，处理双方收付款、进行结算，出具相应的银行单据等，直到买方收到自己所购商品，完成了整个交易过程。索赔是在买卖双方交易过程中出现违约时，需要进行违约处理的工作，受损方要向违约方索赔。

一般来说，各种类型的电子商务交易都包括上述四个环节，但根据交易对象、规模等的不同，有些环节可能简化或省略。

1.1.4 电子商务的应用环境

虽然互联网技术在20世纪90年代初就得到了迅速的发展，但电子商务真正从一种商业概念转变成现实模式却是在90年代末。在此期间，我们经历了社会环境、技术环境及管理环境的快速发展。正是这些外部环境的发展促进了电子商务真正普及。

首先，电子商务的发展依赖于特定的外部社会环境。从20世纪80年代起，我国经济经历了一个快速发展的历史阶段，到20世纪90年代末期，国家又进入新一轮经济快速发展的时期，经济全球化的趋势日益明显，国际贸易往来日益增多。社会经济的整体发展为电子商务的出现提供了良好的宏观氛围。与社会发展相伴随的是社会生产模式及人类生活方式的变革，追求效率、降低成本成为企业关注的重点，而消费者的需求也呈现出多样性、个性化的特点。供需双方的变化促进了电子商务这种新的商业模式的出现。

其次，电子商务的发展以信息通信技术的发展为基础。现代信息通信技术为提供了电子商务发展所必需的软硬件平台，为开展电子商务贸易提供了可能，尤其是信息与网络安全技术的发展，为电子商务贸易提供了基本的安全保障。互联网技术的发展，使得电子商务的形式、内容变得日益丰富和生动，带动了电子商务的普及与发展。

最后，电子商务的持续发展需要完善的管理环境。正如前文所述，电子商务并不是物理世界交易过程的完全搬照。作为一种新的商业模式，电子商务不可避免地带来许多新的管理问题，例如，在电子商务交易过程中的信用管理、相关的法律保障等，都对电子商务的发展有着至关重要的影响。电子商务的开展需要一套法律、法规体系的保障，需要全行业的共同参与来规范电子商务中的各种行为。随着信息通信技术的发展，电子商务的形式、内容也在不断发展，相应的管理环境也需要不断地完善。

电子商务的应用环境如图1-1所示。

1.2 电子商务安全的基本要求

电子商务发展的核心和关键问题是交易的安全性。由于Internet本身的开放性，使网上交易面临着种种危险，也由此提出了相应的安全控制要求。电子商务安全的基本要求主要包括机密性、完整性、可用性、可认证性和抗抵赖性。

1. 机密性

机密性是指保证信息为授权者享用而不泄露给未经授权者。

在电子商务系统中，交易中发生、传递的信息均有保密的要求。如果信用卡的账号和用户名被知悉就有可能被盗用；订货和付款的信息被竞争对手获悉，就有可能丧失商机。因此在电子商务信息的传播中，一般均有加密的要求。电子商务作为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子商务是建立在一个较为开放的网络环境上的，维护商业机密是电子商务全面推广的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。机密性一般通过密码技术对传输的信息进行

加密码处理来实现。密码技术将在后续章节中进行详细介绍。

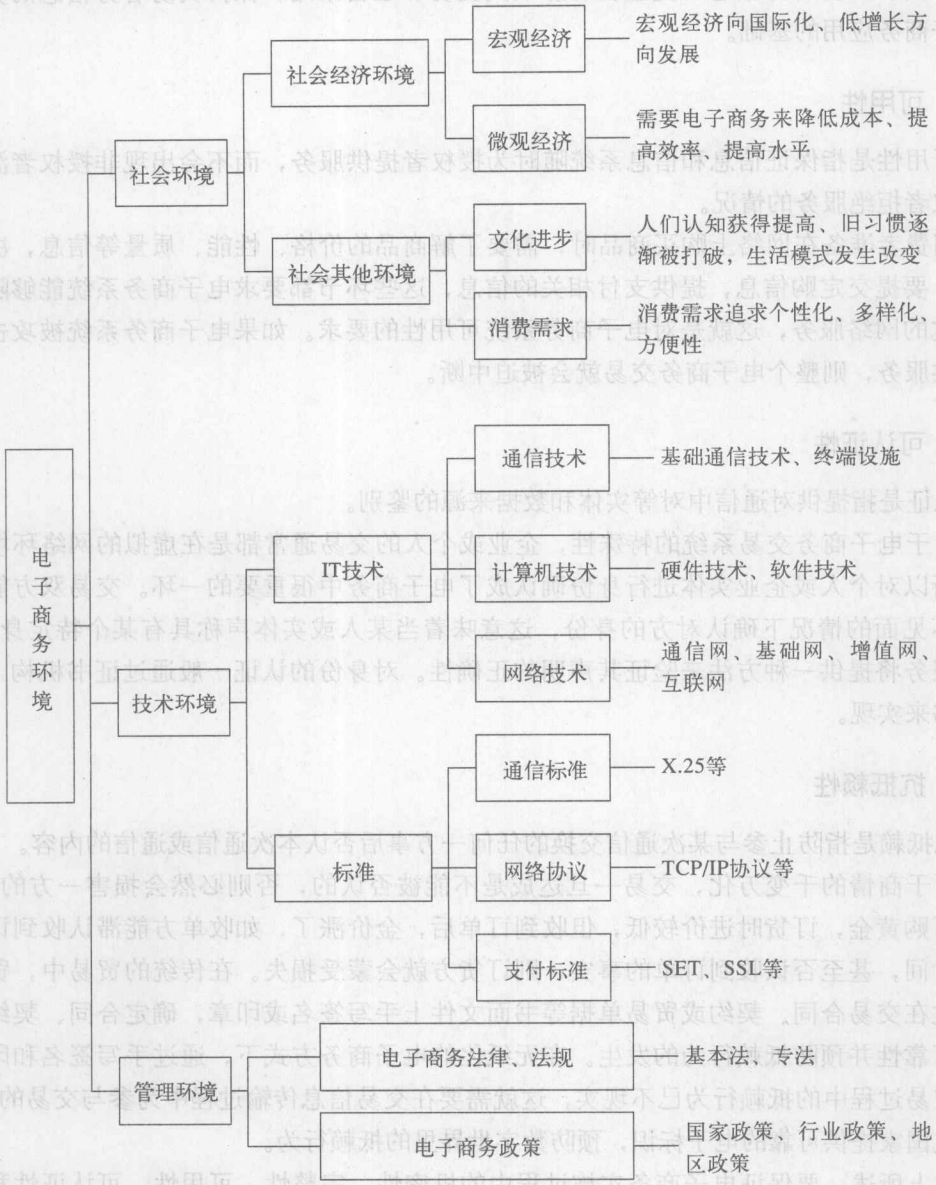

图1-1 电子商务环境

2. 完整性

完整性是指保证只有被授权的各方能够修改计算机系统的有价值的内容和传输的信息，修改包括对信息的写、改变状态、删除、创建、时延或重放。

电子商务简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商业信息的完整性的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的不一致。

此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响到交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。

3. 可用性

可用性是指保证信息和信息系统随时为授权者提供服务，而不会出现非授权者滥用却对授权者拒绝服务的情况。

消费者准备在网络上购买商品时，需要了解商品的价格、性能、质量等信息，决定购买后，要提交定购信息，提供支付相关的信息，这些环节都要求电子商务系统能够随时提供稳定的网络服务，这就是对电子商务系统可用性的要求。如果电子商务系统被攻击而无法提供服务，则整个电子商务交易就会被迫中断。

4. 可认证性

认证是指提供对通信中对等实体和数据来源的鉴别。

由于电子商务交易系统的特殊性，企业或个人的交易通常都是在虚拟的网络环境中进行，所以对个人或企业实体进行身份确认成了电子商务中很重要的一环。交易双方能够在相互不见面的情况下确认对方的身份，这意味着当某人或实体声称具有某个特定身份时，鉴别服务将提供一种方法来验证其声明的正确性。对身份的认证一般通过证书机构（CA）和证书来实现。

5. 抗抵赖性

抗抵赖是指防止参与某次通信交换的任何一方事后否认本次通信或通信的内容。

由于商情的千变万化，交易一旦达成是不能被否认的，否则必然会损害一方的利益。例如订购黄金，订货时进价较低，但收到订单后，金价涨了，如收单方能滞认收到订单的实际时间，甚至否认收到订单的事实，则订货方就会蒙受损失。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。在无纸化的电子商务方式下，通过手写签名和印章来预防交易过程中的抵赖行为已不现实，这就需要在交易信息传输过程中为参与交易的个人、企业或国家提供可靠的电子标识，预防数字世界里的抵赖行为。

综上所述，要保证电子商务实施过程中的机密性、完整性、可用性、可认证性和抗抵赖性，需要数据加密技术、消息摘要、数字签名、认证技术和SSL安全协议等多种技术共同完成。这些技术会在以后的章节中进行详细的介绍。

1.3 电子商务面临的安全威胁

电子商务依赖于Internet，因此Internet所面临的安全威胁，也同样是电子商务所面临的威胁。

在Internet发展的初期，其各种协议的设计是以连通为主要目的，安全性并没有被放在

最重要的位置。这就决定了Internet是一个完全开放的网络，任何一台计算机、任何一个网络都可以与之连接，并借助Internet发布信息，获取各种网上的资源，为一些有意或无意的网络攻击提供了可能。近年来，很多别有用心的组织或个人伺机利用网络或应用系统的漏洞，在Internet上寻求机会窃取他人的机密信息（如信用卡密码等），甚至妨碍网络系统的正常运行等。据调查，2002年世界排名前1000名的公司几乎都曾被黑客（hacker）闯入过。

如果把网络系统的运转看成是一种信息的流动，则正常情况下，信息从信息源（如文件或某个网站）流向目标（如文件或用户），这种正常的信息流图如图1-2a所示。图1-2的剩余部分指出了网络系统所面临的几种安全威胁：

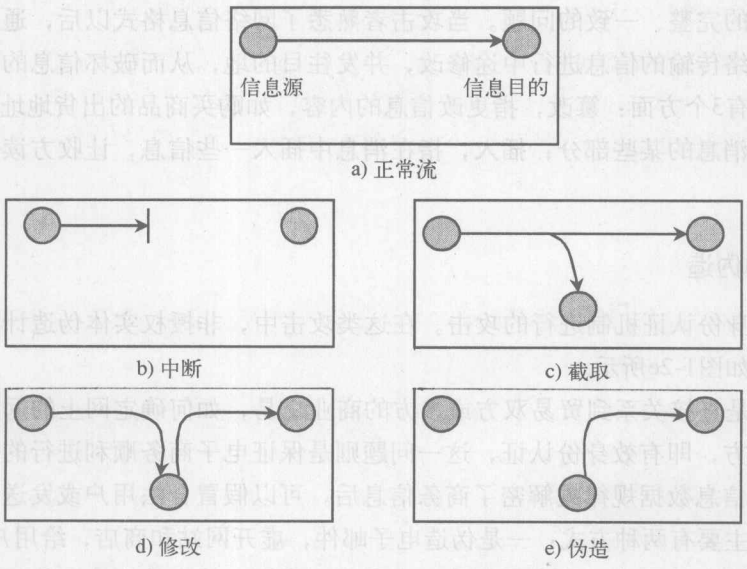

图1-2 安全威胁的类型

1. 系统的中断

这是针对可用性进行的攻击。在中断（干扰）过程中，系统资源变得易损失、不可得或不可用。网络故障、操作错误、应用程序错误、硬件故障、系统软件错误以及计算机病毒等恶意攻击都能导致系统不能正常工作。因而要对此所产生的潜在威胁加以预防和控制，以保证贸易数据在确定的时刻、确定的地点是有效的。如图1-2b所示。

2. 信息的截获和窃取

这是针对机密性进行的攻击。它意味着某些非授权实体获得对资源的存取。这里的实体可以是一个人、一个程序或一个计算机系统。例如，在网络中为得到数据对程序或数据实施的非法拷贝、电话线上的窃取、以太网上对数据包的嗅探等。如图1-2c所示。

电子商务作为贸易的一种手段，其信息直接代表着个人、企业或国家部门的商业机密。如果没有采用加密措施或加密强度不够，攻击者可能通过互联网、公共电话网、搭线、电磁波辐射范围内安装截收装置或在数据包通过的网管和路由器上截获数据等方式，获取传

此为试读，需要完整PDF请访问：www.ertongbook.com