第一章

电子商务、计算机及网络基础知识

知识目标

» 理解电子商务的定义、特点；

» 了解几种常见的计算机；

» 了解计算机网络的 OSI 模型和 TCP/IP 模型。

技能目标

» 掌握电子商务常见的运行模式，并能在实际生活中分辨不同模式；

» 能够根据计算机网络相关知识区分不同类型的计算机网络。

引例

戴尔公司电子商务的成功

戴尔公司是世界PC(personal computer)市场的第二大供应商,其销售额以每年40%的增长率递增,是该行业平均增长率的两倍。2009年,戴尔公司计算机销售量仅次于惠普,全球排名第二。戴尔公司每天通过网络售出的计算机系统价值逾1 200万美元,面对骄人的业绩,总裁迈克尔·戴尔简言:这归因于电子商务化物流的巧妙运用。

戴尔公司的日销量庞大,但其销售全是通过国际互联网和企业内部网进行的。在日常的经营中,戴尔公司仅保持两个星期的库存(行业的标准是超过60天),存货一年周转30次以上。基于这些数字,戴尔公司的毛利率和资本回报率分别是21%和106%。戴尔公司实施电子商务化物流后取得的效果是:

(1) 1998年成品库存为零。

(2) 零部件仅有2.5亿美元的库存量(其盈利为168亿美元)。

(3) 年库存周转次数为50次。

(4) 库存期平均为7天。

(5) 增长速度是竞争对手的两倍。

对于大部分人来说,戴尔只是一个销售计算机和显示器等电子产品的公司;对于有过戴尔网站购物经历的消费者来说,戴尔也只是一个网上直销商;但是对于IT行业的专家来说,戴尔却是超越传统商业贸易的成功者,其成功源于出色的电子商务。什么是电子商务?电子商务与计算机网络有着怎样的联系?戴尔在应用电子商务时有哪些值得其他企业借鉴之处?本章将给出答案。

第一节　电子商务概述

一、电子商务的定义和特点

(一) 电子商务的定义

电子商务通常是指在全球各地广泛的商业贸易活动中,在Internet开放的网络环境下,基于浏览器/服务器应用方式,买卖双方不谋面地进行各种商贸活动,实现消费者的网上购物、商家之间的网上交易和在线电子支付以及其他各种商务活动、交易活动、金融活动和相关的综合服务活动的一种新型的商业运营模式。在“电子商务”中,“电子”泛指在商务活动中使用的各种高新技术手段,包括计算机网络、通信设备(如电话、传真),以及以Internet为基础的其他工具等;“商务”是指将社会资源转换为货物和服务,并以营利为目的向消费者进行销售的有组织的活动。

由于电子商务涉及面广，不同的国家、团体，甚至公司都给出了不同的定义。

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。在该定义中，对商务活动的定义是很笼统的。

1997 年 10 月 1 日至 3 日在国际标准化组织（International Organization for Standardization，ISO）和国际电信联盟（International Telegraph Union，ITU）的倡导和支持下，全球信息社会标准大会在比利时首都布鲁塞尔举办。会上，欧洲经济委员会将电子商务定义为：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的任何形式的业务交易。

全球信息基础设施委员会（Global Information Infrastructure Committee，GIIC）电子商务工作委员会报告草案中对电子商务的定义为：电子商务是将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。

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，如电子数据交换（electronic data interchange，EDI）、Web 技术、电子邮件等共享非结构或结构化商务信息，管理和完成在商务活动、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的丰富资源相结合的背景下，应运而生的一种在互联网上展开的互相关联的动态商务活动。

惠普公司提出，电子商务是以现代扩展企业为信息技术基础结构的，跨时域、跨地域的电子化世界。惠普公司电子商务的范畴包括所有可能的贸易伙伴，即用户、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。

由上面的定义可知，不同国家、团体以及公司对电子商务的理解虽然不尽相同，但也存在一些共识，即电子商务必须是电子方式的商业活动。电子方式包括 EDI、电子支付手段、电子订货系统、电子邮件、网络、图像处理、智能卡等。这也是电子商务与传统商务活动最大的不同之处。

（二）电子商务的特点

电子商务是一种综合运用信息技术，以提高贸易伙伴间商业运作效率为目标，将一次交易全过程中的数据和资料用电子方式实现的技术，在商业的整个运作过程中实现交易无纸化、直接化。电子商务可以使贸易环节中各个商家和厂家联系得更紧密，从而更快地满足其需求，在全球范围内选择贸易伙伴，以最小的投入获得最大的利润。因此，与传统的商务活动方式相比，电子商务具有以下几个特点。

1. 高效率

传统贸易方式中，用信件、电话等传递信息，必须有人的参与，每个环节都要花费不少时间。有时由于人员合作和工作时间的问题，会延误传输时间，失去最佳商机。

电子商务依靠电子通信手段，与邮政通信手段相比较，internet 的信息传输速率极快，传输的信息量也很大，但费用却很低。而且与电话、传真等通信手段不同，internet 上的信息传输可以在无人值守的情况下进行。这就意味着：互联网使标准化的商业报文能在世界各地瞬间完成传递，并且依靠计算机自动处理原料采购、产品生产、需求与销售、银行汇兑、保险、

货物托运及申报等过程，无须人为干预便能够短时间、高效率地完成。

2. 虚拟性

与电视、报纸等媒介不一样，在 internet 中，计算机与计算机之间、客户机与服务器之间能够方便地实现信息的双向传输，从而实现信息的快速交换。正是有了这种交互性，交易双方从贸易磋商、签订合同直到支付费用等，均不用当面进行，而只需通过计算机网络即可完成，整个交易完全虚拟化。

同时，在 internet 中使用网络传输技术，商家可以传输包括文字、声音和图像在内的多媒体信息，制作自己的主页，组织产品信息上网。这使得商家能够与相隔遥远的用户通过计算机来交流，从而使交易者无须见面，就可以完成交易。

但也正是由于这种虚拟性，才使得网上交易的安全性受到各方的关注，而电子商务安全本质上正是为了提高网上交易的安全性。

3. 开放性

internet 是个开放的网络，其开放性主要表现在 4 个方面：一是对用户的开放，二是对地域的开放，三是对时间的开放，四是对环境的开放。

internet 可以自由连接，而没有时间和空间的限制，没有地理上的距离概念，任何人可随时随地可加入 internet，只要遵循规定的网络协议即可。同时，相对而言，在 internet 上任何人都可以享受创作的自由，所有的信息流动都不受限制。网络没有管制，网络的运作是由使用者相互协调来决定的，网络的每个用户都是平等的。这种开放性使得网络用户不存在是与否的限制，只要入网便是用户。internet 也是一个无国界的虚拟自由王国，网络上信息的流动自由、用户的言论自由、用户的使用自由。

4. 低成本

电子商务使买卖双方的交易成本大大降低，具体表现在以下几个方面：

(1) 信息传递成本降低。交易双方距离越远，在网络上进行信息传递的成本较信件、电话、传真的成本就越低。

(2) 减少交易环节。相对于传统的商业模式，买卖双方通过网络进行商务活动，可以减少甚至“消灭”中介方，减少了交易的有关环节，进而降低了成本。

(3) 节省宣传费用。卖方可通过网络进行产品介绍和宣传，节省了在传统方式下制作广告、发印刷产品等所需的大量费用。

(4) 实现零库存。通过网络，买卖双方可以即时沟通，使无库存生产和无库存销售成为可能，从而实现零库存。

(5) 降低传统办公费用。电子商务实行“无纸贸易”，可降低大部分的文件处理费用及其相关附加费用。同时，办公场所也可能发生了变化，传统的贸易平台是地面店铺，而电子商务贸易平台可以是任何地方，这样又降低了租用办公场所的费用。

二、电子商务的参与者及运行模式

电子商务最主要的参与者是商家(business)、消费者(customer)和行政机构(government)。其相应的运行模式有以下几种。

1. 商家对商家模式

商家对商家模式即 B2B(business to business)模式，指商家与商家之间通过计算机网络进行产品、服务及信息的交换。这是最早出现的电子商务模式。在这种模式中，商业活动是在商家与商家之间进行的。销售商通过网络来与供应商联系订货，接收发票和付款，确定配送方案；从而实现协同作业、管理资源以及信息共享，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。这种模式有时写成 B to B，但为了简便干脆用其谐音 B2B(2 即 to)。以下的称谓与此相似。

B2B 模式的典型代表是阿里巴巴①、慧聪网②等。

2. 商家对消费者模式

商家对消费者模式即 B2C(business to customer)模式。在这种模式中，商业活动是在商家和消费者个人之间进行的。企业通过计算机网络为消费者提供一个新型的购物环境——网上商店。商家利用计算机网络技术开设店面、陈列商品、标示价格、说明服务，并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；消费者则通过网络进行购物、支付费用等。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。同时，这种模式直接针对消费者，开创了一个崭新而庞大的市场。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。

B2C 模式的典型代表是戴尔公司的销售模式。图 1-1 为戴尔公司销售网站页面。

图 1-1　戴尔公司销售网站页面

① 阿里巴巴(www.alibaba.com)是全球 B2B 电子商务的著名品牌，汇集了海量供求信息，是全球领先的网上交易市场和商人社区。

② 慧聪网(www.hc360.com)成立于 1992 年，是国内领先的 B2B 电子商务服务提供商。慧聪网依托其核心产品——买卖通，以及雄厚的传统营销渠道——慧聪商情广告与中国资讯大全、研究院行业分析报告，为客户提供线上、线下的全方位服务，形成优势互补、纵横立体的架构。

在戴尔公司的销售网站上，消费者可以随意选购、配置自己所需的电子产品，价格和产品的情况都已在网站上标明。一旦达成交易意向，消费者先行支付费用，之后在一个月左右就会接到通过邮递寄送的产品。这种直接面对客户的 B2C 电子商务运行模式已经取得了很好的效果。

3. 消费者对消费者模式

消费者对消费者模式即 C2C(customer to customer)模式，也称为网上拍卖模式。在该模式中，消费者之间通过计算机网络来交换需求信息。在专门的拍卖网站上，一些消费者将自己想要出售的商品信息公示，另一些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实现了。值得注意的是，以 C2C 模式来交易的一般是单件产品或数量很少的产品，如一条毛毯、一台计算机等。在这里，网络的中介作用得到了充分体现。当普通商家为了拓展自己的业务的时候，会借助这样的中介网站来销售自己的产品，这样卖家就成为商家，该模式也就转换为 B2C 模式了。

C2C 模式的典型代表是淘宝网。

4. 行政机构对行政机构模式

行政机构对行政机构模式即 G2G(government to government)模式。G2G 是指上下级政府、不同地方政府和不同政府部门之间实现的电子政务活动。其具体的实现方式包括政府内部网络办公系统、电子法规、政策系统、电子公文系统、电子司法档案系统、电子财政管理系统、电子培训系统、垂直网络化管理系统、横向网络协调管理系统、网络业绩评价系统、城市网络管理系统 11 个方面。这使得传统的政府与政府间的大部分政务活动都可以通过网络技术得到高速度、高效率、低成本的实现。

5. 商家对行政机构模式

商家对行政机构模式即 B2G(business to government)模式。B2G 指的是企业与政府机构之间进行的电子商务活动。例如，政府将采购的细节在网络上公布，通过网上竞价方式进行招标；企业也要通过电子的方式进行投标。政府可以通过这种方式树立形象，通过示范作用促进电子商务的发展。除此之外，政府还可以通过这类电子商务模式实施对企业的行政事务管理。例如，政府用电子商务方式发放进出口许可证、开展统计工作，企业通过网上办理交税和退税等。

6. 消费者对行政机构模式

消费者对行政机构模式即 C2G(customer to government)模式。C2G 指的是个人对政府的电子商务活动。这类电子商务活动目前还没有普及。然而，在个别发达国家(如澳大利亚)，政府的税务机构已经通过指定私营税务或财务会计事务所用电子方式来为个人报税。这类活动虽然还没有达到真正的报税电子化，但它已经具备了消费者对行政机构电子商务模式认识的雏形。

随着商家对消费者、商家以及对行政机构的电子商务的发展，政府将会为社会的个人提供更为全面的电子方式的服务。政府各部门向社会纳税人提供的各种服务，如社会福利金的支付等，将来都会在网上进行。

随着技术和商业的发展，电子商务的新模式还在不断涌现，因此，电子商务的新模式也成为目前业界思考较多的课题。

三、电子商务的起源和发展

（一）电子商务的产生

早在互联网出现之前，计算机网络作为一种先进的信息传输手段就已经在商务活动中得到了应用。

1. 电子商务的雏形：机票预订系统和 EDI

20 世纪 70 年代，美国航空公司率先推出了基于计算机网络的机票预订系统。客户可以在美国的各个航空公司的售票点，以及与美国航空公司联营的旅行社等地点，通过计算机终端查询到美国航空公司所有航班的时刻、票价、空位情况等信息，并通过计算机终端订票。但在此之前，客户若要购买航空公司的机票，只能到就近的售票点购买。如果该售票点的机票卖完了，客户就只能到另外的售票点购买，非常不方便。因此，该系统大大方便了客户，也解决了航空公司的难题，提高了美国航空公司的市场竞争力，扩大了其市场份额，也加快了美国实现运输现代化的进程。如今，不仅各个航空公司及其代理机构能够发售机票，银行等商业机构也与航空公司联网，使机票预订系统成为了一个巨大的商业网络。

资料链接 1-1

EDI 的产生和发展

EDI 可译为“电子数据交换”。EDI 是指在处理商务或行政事务时，按照一个公认的标准，将其转换成结构化的事务处理或消息报文格式，并以此建立计算机之间的数据传输方法。它是一种在公司之间传输订单、发票等作业文件的电子化手段。EDI 包含 3 个方面的内容，即计算机应用、通信网络和数据标准化。其中，通信网络是 EDI 应用的基础，计算机应用是 EDI 的条件，数据标准化是 EDI 的传输手段。这 3 个方面相互衔接、相互依存，构成了 EDI 的基础框架。商家在建立 EDI 系统之后，可以在商务活动中将商业文件（如订单、发票、报关单和进出口许可证等）按统一的标准编制成为计算机能识别和处理的数据格式，在计算机之间进行传输。它以电子单证代替纸面文件，实现了真正的“无纸贸易”。

20 世纪 60 年代，欧洲和美国几乎同时提出了 EDI 的概念。20 世纪 70 年代，行业性的 EDI 系统出现在银行业、运输业和零售业，如当时银行业发展的电子资金汇兑系统①（如 SWIFT）和日本的杂货物流系统。20 世纪 80 年代，EDI 应用迅速发展。1986 年，欧洲和北美洲的 20 多个国家开发了用于行政管理、商业及运输业的 EDI 国际标准

① 电子资金汇兑系统是利用电子计算机和数据通信技术，把资金从一个账户转到另一个账户，代替现金和支票支付的自动信息处理系统。

(EDIFACT[①])。EDI 历经了萌芽期、发展期,时至今日已步入成熟期。以现有的信息技术水平来看,EDI 的实现已不是技术问题,而仅仅是一个商业问题。

当互联网出现之后,EDI 由原先的使用专用计算机网络过渡到使用互联网,实际上已经成为电子商务的一种形式。可以将使用互联网作为通信环境的 EDI 看成一种遵守特定标准的 B2B 电子商务系统。

2. 较为成熟的电子商务:基于互联网的电子商务

互联网,即广域网、局域网及单机按照一定的通信协议组成的国际计算机网络。互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来而形成的能够实现信息共享、互操作等的计算机网络。

为适应在互联网上开展商务活动的需要,1994 年,美国网景公司(Netscape)推出了支持电子商务的安全套接层(secure sockets layer,SSL)协议,用以弥补互联网使用的 TCP/IP 协议在安全方面的不足。1996 年 2 月,在 IBM、微软等一批技术领先的跨国公司的支持下,Visa 与 MasterCard 两大信用卡国际组织共同发起并制定了安全电子交易(secure electronic transaction,SET)协议,借以保障电子商务的安全。

(二) 现代电子商务的发展

1. 发展早期

20 世纪的最后几年,基于对电子商务美好前景的憧憬,电子商务得到了爆炸式的发展。当时,电子商务成了整个社会最热门的话题之一,大量的投资涌入电子商务领域,不断有企业宣布进军电子商务,新的电子商务网站大量出现。电子信息技术和政府、医疗、教育、金融、卫生、军事、企业、研发组织等应用领域结合,形成了完整的电子商务体系。

2. 调整期

2000 年初,电子商务在不断的发展过程中也遇到了问题。IT 行业,特别是基于计算机网络技术的相关行业经过十几年的高速发展之后,积累的问题开始集中暴露。尽管一些电子商务网站的营业收入已经做得很大,但支出更大,一直不能实现盈利。后来,电子商务跟随整个 IT 业进入了调整期。原先融入的资金开始撤离,许多依赖资本市场资金的网站陷入了困境,坚持不下去的网站开始倒闭。电子商务的发展逐渐进入寒冬时期。

3. 重新崛起阶段

经过短暂的调整,电子商务重新显示出了强大的生命力,逐步得到了市场和投资者的认可。这时,应用电子商务的企业趋于务实,不断有电子商务企业开始宣布实现了盈利。例如,雅虎公司于 2003 年 1 月 15 日公布的财务报告显示,2002 年第四季度该公司的利润和营业额均大幅上升,第四季度净利润为 4 620 万美元,销售收入激增 51%。同时,随着全球互联网用户人数的增加,人们对电子商务的认可度也在逐年攀升。到 2002 年底,全球互联网

① EDIFACT 的全称为 electronic data interchange for administration,commerce and transport,中文译为行政管理、商务与运输电子资料交换,是由联合国管理的数据交换标准,是一个多重工业 EDI 标准。

用户人数达到6.55亿，比2001年同期增长了30%。2002年网上商品和服务的销售额(B2C模式)达到23亿美元，比2001年同期增长了50%。这时的电子商务所涉及的领域和内容已经不仅仅是传统的商业活动，其覆盖面已经达到了网络游戏、网络电话等，一些SNS[①]社交网络，如人人网、FaceRen[②]、微博[③]等全新概念也不断出现。电子商务在一定时期内的发展极为迅速，但就整个电子商务而言，总体的发展呈现出稳健的势头。

（三）企业电子商务的三个应用阶段

对于企业来说，电子商务的切实应用要更加直接。这里就不得不提到IBM公司，因为该公司对电子商务的发展有很多重要的贡献。例如，全面电子商务的思想就是由该公司提出的。按照企业中电子商务的应用水平，IBM公司把到目前为止的电子商务分为三个阶段。

1. 接入阶段

接入阶段是企业开展电子商务的起点。在这一阶段，企业开始转换其信息的传输通信方式，实现了接入internet。有一些业务已经应用上了电子贸易的手段，系统支持在线销售，企业开始使用电子邮件推广产品和服务的电子手册，使现有客户及潜在客户都能通过它收集到相关信息。随后，企业利用Web进一步实现了简单的在线事务处理。例如，找工作的人不仅可以浏览职位空缺，还能进行在线职位申请；客户可以在线查询收支金额，并在两个账户之间划拨资金；而消费者则可以在线订购商品，并跟踪发货情况。这一阶段的特点是：所有的应用都是单体的应用，很少有集成商务的应用。

2. 整合阶段

在整合阶段，企业不仅能够支持客户的在线订购行为，还能通过整合企业内部其他部门的行动，确保这些订单顺利履行。整合阶段的电子贸易包括市场分析、全部的销售过程、集成的电子产品供应链，最终达到产品销售中从头到尾地应用客户关系管理系统、企业资源计划系统、供应链管理系统，也就是集成的端到端的电子商务进程。企业内部的各个部门之间能够通过订购系统来高效率地传输数据，企业与其合作伙伴之间也能通过IT系统来高效率地交换数据。但是，这一阶段的成功需要解决一些真正棘手的问题，如整合关键的业务流程，以及处理分布于企业内外的无数单体应用和平台等。

3. 随需应变阶段

随需应变是IBM在2002年提出并从2003年开始大力推广的概念。

IBM还对企业的随需应变作了具体的定义，即为了应对激烈的竞争、持续的变革、强大的财务压力和无法预测的风险，企业必须做到：

(1) 聚焦核心：集中在自己的差异性能上，与战略合作伙伴紧密整合，让他们管理那些

---

① SNS的全称是social networking services，即社会性网络服务，有时也解释为social network site，译为“社交网站”，专指旨在帮助人们建立社会性关系的互联网应用服务。

② 人人网由千橡互动集团将旗下著名的校内网更名而来。FaceRen(同学网)成立于2006年5月，早期是海外最大的华人留学生社区。

③ 微博即微型博客，国际上最知名的微博网站是Twitter，美国总统奥巴马、美国白宫、FBI、Google、HTC、Dell、福布斯、通用汽车等很多国际知名个人和组织都在Twitter上进行营销和与用户交互。

不具差异性的活动。

(2) 实时响应:几乎能够本能地感知市场环境的变化和随之而来的各方面的需求,并能够作出快速反应。

(3) 灵活可变:成本结构和业务流程非常灵活,从而能够降低风险,并更好地产出,更好地进行成本控制、资本优化和财务预测。

(4) 坚固可靠:能够经受全球市场中技术的、经济的或政治的变化和威胁,使业务凭借一致的可靠性、安全性及保密性来持续运作。

进入随需应变阶段之后,企业的员工和客户对电子商务的需求能"像水和电一样,需要时,就能轻松享用"。这时,整个商业流程将突破技术和组织的界限,系统将自动地处理进程。

(四) 电子商务在我国的发展

1. 围绕 EDI 技术的电子商务应用阶段

我国 20 世纪 90 年代开始开展 EDI 的电子商务应用。不同于西方国家的商业自发行为,我国的 EDI 发展是以"政府牵头,企业跟进"的模式展开的。自 1990 年开始,国家发改委、科学技术部将 EDI 列入"八五"国家科技攻关项目,如对外经济贸易部(已撤销,现由商务部代替)的"国家外贸许可证 EDI 系统"、中国对外贸易运输(集团)总公司的"中国外运海运/空运管理 EDI 系统"、中国化工进出口公司的"中化财务、石油、橡胶贸易 EDI 系统"及山东抽纱进出口公司的"EDI 在出口贸易中的应用"等。1991 年 9 月,由国务院电子信息系统推广应用办公室牵头,会同国家发改委、科学技术部、对外经济贸易部、国内贸易部、交通部、信息产业部、国家质量监督检验检疫总局、国家外汇管理局、中国银行、中国人民银行、中国人民保险公司、国家税务总局、中国国际贸易促进委员会等发起成立"中国促进 EDI 应用协调小组";1991 年 10 月,我国成立"中国 EDIFACT 委员会",并参加亚洲 EDIFACT 理事会。这些为我国电子商务的发展奠定了基础。

2. 以"三金"工程为主导的电子商务发展阶段

1993 年,我国成立了以国务院副总理为主席的国民经济信息化联席会议及其办公室,相继组织了金关、金卡、金税"三金"工程,电子商务的发展取得了重大进展。"三金"工程是国民经济信息化的起步工程,对电子商务的发展起到了巨大的推动作用。

1994 年 10 月,"亚太地区电子商务研讨会"在北京召开,电子商务的概念开始在我国传播。

1995 年,中国互联网开始商业化,互联网公司开始兴起。

1996 年,金桥网与互联网正式开通。

1997 年,国家信息化办公室组织有关部门起草编制我国信息化规划,广告主开始使用网络广告。

1997 年 4 月以来,中国商品订货系统(CGOS)开始运行。

3. 互联网电子商务发展阶段

1998 年 7 月,中国商品交易市场正式宣告成立。我国的电子商务也在 20 世纪后期伴随着互联网的快速发展而发展起来。2000 年初,我国有 B2C 购物网站 1 665 家。从 2000 年下

半年开始，与全球电子商务的调整基本同步。从2002年下半年开始，中国的电子商务迎来了新一轮的发展，主要体现在以下几个方面：

（1）电子商务的服务范围不断扩大。旅游、票务、金融、房地产、职业介绍、教育、娱乐等网上服务业发展迅速。

（2）网上采购规模大增。政府采购推动了网上采购的发展，发改委、经贸委、财政部、卫生部、国家食品药品监督管理局等部门都做了一系列工作，生产企业的网上采购业务也发展迅速。

（3）电子商务的法律法规开始完善。从2003年2月1日起，《广东省电子交易条例》正式在该省行政区域内实施，这是中国内地第一部真正意义上的电子商务立法。《中华人民共和国电子签名法》于2004年8月28日由第十届全国人民代表大会常务委员会第十一次会议通过，并于2005年4月1日起开始正式施行。

（4）网上金融规模不断扩张。2001年，我国共有13家银行开办了网上银行业务。2002年7月，我国证券公司网上委托交易量首次超过了整个交易量的10%。

（5）国外的电子商务巨头大规模进入中国市场。2003年6月，国际电子商务巨头eBay[①]以1.5亿美元收购了美国易趣公司，从而成为中国易趣网的最大股东以进军中国市场。2005年7月，eBay旗下的全球在线支付巨头PayPal在中国成立其分公司，开始向中国客户推广其在线支付工具“贝宝”。2005年8月11日，电子商务另一国际巨头雅虎与中国阿里巴巴公司在北京宣布了战略合作方案。阿里巴巴收购雅虎中国全部资产，同时获得雅虎10亿美元的投资。在新的背景下，阿里巴巴旗下的淘宝网（www.taobao.com）发展迅速。

电子商务拥有庞大的潜在市场。每半年中国互联网络信息中心[②]都要发布《中国互联网络发展状况统计报告》。根据其调查统计，截至2010年12月，我国上网用户总人数为4.57亿（包含移动互联网用户），网民规模、宽带网民数、国际顶级域名注册量三项指标中国均位居世界第一。

第二节　计算机及网络基础知识

一、计算机基础知识

电子商务是依靠计算机技术和网络技术发展起来的新型商业贸易模式。计算机为电子商务的实现提供了硬件基础。按照性能指标不同，计算机分为巨型机、大型机、小型机和微型机等；按照用途不同，计算机分为专用机和通用机。这里仅介绍与电子商务相关的一些计

① eBay于1995年9月4日创立于加利福尼亚州圣荷西。人们可以通过网络在eBay上出售商品，它是一种C2C模式的电子商务网站。

② 中国互联网络信息中心（China Internet Network Information Center，CNNIC）是经国家主管部门批准，于1997年6月3日组建的管理和服务机构，行使国家互联网络信息中心的职责。

算机的知识。

（一）几种常见的计算机

1. 巨型机、大型机和小型机

大型机一般用在尖端的科研领域，其主机非常庞大，通常由许多中央处理器协同工作，具有超大的内存和海量的存储器。其使用专用的操作系统和应用软件。巨型机在体积方面往往比大型机还要巨大，功能也更为强大。小型机相比于大型机则体积较小，功能也不如大型机。但是，随着计算机的小型化、微型化，巨型机、大型机、小型机在体积上的区别已经不那么明显。因此，现在主要是根据它们的处理器来进行分类的。如大型机的处理器可能会有几千个，而小型机可能只有几个。

巨型机、大型机、小型机可以用做电子商务的工作站或服务器，企业可以根据自己的需要进行选择。在电子商务的交易过程中，这些充当工作站或服务器的计算机往往被用来存储大量的数据或承担复杂繁多的数据处理任务。其使用者主要是商家、认证中心等。

图 1-2 为我国自行研制的首台千万亿次计算机“天河一号”，图 1-3 和图 1-4 分别为大型机和小型机。

图 1-2　我国自行研制的首台千万亿次计算机“天河一号”

图 1-3　大型机

图 1-4　小型机

2. 微型机

微型机是普通用户接触最多的计算机，也称微机。由于计算机技术的不断发展，微型机的覆盖范围也越来越广，包括普通的 PC、掌上电脑等。由于微型计算机一般由运算器、控制

器、存储器、输入设备和输出设备五大部分组成，而越来越多的手机、MP4、DVD 播放器也具备这种结构，所以微型机的范围已经十分模糊了。但是，在电子商务的应用中，微型机主要充当用户与商家交流的网络终端，凡是具备微型机软件功能和五大结构的电子设备都可以充当用户的电子商务工具。

图 1-5 为苹果公司于 2010 年发布的计算机产品 iPad。iPad 的外形十分像一部放大版的 iPhone 手机，而功能上也是介于手机和 PC 之间，同样具备五大结构并且能够登录互联网，因此它完全具备微型机的功能，可以作为电子商务的客户端。

图 1-5　苹果公司的 iPad

3. 服务器

服务器是指网络中能对其他机器提供某些服务的计算机系统。作为网络的关键组成部分，服务器主要用于存储、处理网络上绝大部分数据、信息，因此也被称为网络的灵魂。服务器的构成与微机基本相似，有处理器、硬盘、内存、系统总线等，它们是针对具体的网络应用特别制定的，因而服务器与微机在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面存在很大差异。但是近些年由于 PC 的发展十分迅速，很多 PC 的性能接近甚至超过服务器，但是两者的操作软件依旧不同。

服务器的定义不同于大型机、小型机，但服务器却是由小型机、大型机充当的。

（二）计算机的发展进程及方向

1. 计算机的发展进程

1946 年 2 月 15 日，世界上第一台通用电子数字计算机“埃尼阿克”（ENIAC）在美国研制成功。它当时由 1.8 万个电子管组成，是一台又大又笨重的机器，体重达 30 多吨，占地约 170 平方米。它当时的运算速度为每秒 5 000 次加法运算，这在当时是相当了不起的。2009 年 9 月，根据美国新科学家网站上的报道，Jaguar 超级计算机以每秒 1 800 万亿次的实测性能和 2 300 万亿次的峰值性能名列全球超级计算机排行榜榜首。经过了 60 多年的发展，计算机的运行速度几乎提升了 4 000 亿倍。计算机的发展速度令人惊叹。值得注意的是，中国的“天河一号”名列第 5 位，首次跻身排行榜前 20 名。

从诞生到现在，计算机的运算速度不断提高，体积不断缩小，操作方式多样化，人机工程日趋合理。对于电子商务的发展而言，计算机产业的突飞猛进无疑起到了不可忽视的推动作用。尤其是2000年以后，随着PC的普及以及计算机性能的提升，电子商务成了一种真正可行的商业模式。

2. 计算机的发展方向

计算机技术的发展将表现为高性能化、网络化、大众化、智能化与人性化、功能综合化，计算机网络将呈现出全连接的、开放的、传输多媒体信息的特点，主要体现在以下几个方面：

(1) 微处理器速度将继续提升，个人计算机将具有原来的高性能服务器所具有的处理能力。

(2) 采用更先进的数据存储技术，如光学、永久性半导体、磁性存储等。

(3) 输入输出技术将更加智能化、人性化，随着笔输入、语音识别、生物测定、光学识别等技术的不断发展和完善，人与计算机的交流将更加便捷。

(4) 计算机的体积将变小变薄，更加便于携带和安放。

二、计算机网络基础知识

(一) 计算机网络概述

到现在为止，一直没有关于“计算机网络”的确切定义，因为随着计算机网络本身的发展，这个概念会不断发生变化。计算机网络的最简单定义是：一些相互连接的、以共享资源为目的的计算机的集合。这意味着计算机网络包含3个方面的内容：

(1) 计算机网络含有两台以上的计算机。

(2) 各台计算机之间相互连接在一起。

(3) 各台计算机之间能够实现数据的传输。

综上所述，计算机网络就是把分散在不同地理位置、具有独立功能的计算机系统及相关网络设备通过通信线路相互连接起来，按照一定的通信协议进行数据通信，以实现资源共享为目的的信息系统。

计算机网络的数据传输速率一般为64 Kb/s～1 Gb/s，局域网、城域网、广域网的数据传输速度理论上来讲逐步变慢。但随着网络技术的发展，广域网传输速率也在不断提高，目前通过光纤介质，采用密集波分复用(dense wavelength division multiplexing，DWDM)、万兆以太网等技术，广域网的传输速率最高可达10 Gb/s。

(二) 计算机网络的分类

计算机网络依据不同的属性有不同的分类方法，主要有以下四种。

1. 按网络覆盖的地理范围分类

按网络覆盖的地理范围分类是最常见的，也是最熟悉的一种计算机网络分类方法。按照网络覆盖的地理范围的大小，可以把计算机网络分为局域网、城域网和广域网3种类型。

(1) 局域网。局域网(local area network，LAN)是将较小地理区域内的各种数据通信设备连在一起的通信网络，也就是在一个较小区域范围内，将分散的计算机系统或数据终端互连起来为实现资源共享而构成的网络。局域网覆盖的地理范围较小，它常用于组建一个

办公室、一栋楼、一个楼群或一个校园的计算机网络。局域网的主要特点如下：

① 网络覆盖的地理范围比较小，一般为几十米到几千米；

② 数据传输速率高，目前在朗讯贝尔实验室已成功达到 100 Gb/s；

③ 误码率低；

④ 拓扑结构简单，常用的拓扑结构有总线型、星型和环型等；

⑤ 局域网通常归属于一个单一的组织管理。

(2) 城域网。城域网(metropolitan area network，MAN)是一种大型的局域网，它可能覆盖一组邻近的公司办公室和一个城市。它使用的是局域网技术。其目标是在一个大的地理范围内提供数据、语音和图像的集成服务。城域网的主要特点如下：

① 地理覆盖范围介于局域网和广域网之间，可达 100 千米；

② 既可作为专用网，也可作为公用网。

(3) 广域网。广域网(wide area network，WAN)是在一个广阔的地理区域内进行数据、语音、图像信息传输的通信网。广域网一般由中间设备(路由器)和通信线路组成，其通信线路大多借助于一些公用通信网络，如公共交换电话网络(public switched telephone network，PSTN)、数字数据网(digital data network，DDN)、综合服务数字网(integrated services digital network，ISDN)等。广域网的作用是实现远距离计算机之间的数据传输和资源共享。在非对称数字用户环路(asymmetric digital subscriber line，ADSL)网络连接的时候，时常会出现“正在连接，通过 WAN 微型端口(PPPOE)”的提示，意思就是正在将计算机连入广域网。广域网的主要特点是覆盖的地理区域大，通常由几千米到几万千米，网络可跨越市、地区、省、国家、洲，甚至全球。

图 1-6 是正在通过宽带连入广域网的提示。

图 1-6　正在连入广域网的提示

2. 按局域网标准协议分类

根据所使用的局域网标准协议，可以把计算机网络分为以太网(IEEE802.3)、快速以太网(IEEE802.3u)、千兆以太网(IEEE802.3x 和 IEEE802.3ab)、万兆以太网(IEEE802.3ae)和令牌环网(IEEE802.5)等。

3. 按使用的传输介质分类

计算机网络使用的传输介质是不尽相同的，因此根据所使用的传输介质不同，也可将计算机网络分为两大类：一类是有线传输网络，其传输介质为双绞线、光纤、同轴电缆等；另一类是无线传输网络，如无线网络(以无线电波为传输介质)和卫星数据通信网(通过卫星进行数据通信)等。

4. 按传输技术分类

根据网络所使用的传输技术不同，可以把计算机网络分为广播式网络和点到点网络。

(1) 广播式网络。在网络中只有一个单一的通信信道供这个网络中所有的主机共享。即多个计算机连接到一条通信线路上的不同分支点上，任意一个结点所发出的报文均能被所有其他结点接收。而这些结点根据数据包中的目的地址进行判断，如果是发给自己的则接收，否则丢弃。采用这种传输技术的网络称为广播式网络。

(2) 点到点网络。与广播式网络相反，点到点网络由一对对机器之间的多条连接构成，在每一对机器之间都有一条专用的通信信道。因此，在点到点网络中，不存在信道共享与复用的问题。当一台计算机发送数据后，它会根据目的地址，经过一系列的中间设备的转发，直接到达目的端结点，这种传输技术称为点到点传输。点到点网络就是通过中间设备直接发送数据到需要接收的计算机，其他计算机则收不到这个消息。

(三) 计算机网络模型

计算机通过网络连接起来后，由于每台计算机的软硬件环境不一样，如果它们之间需要相互通信，则必须使用相同的通信规则。计算机网络协议是联网的实体之间用来保证相互通信的规则。但是在数据传输的过程中，计算机会对数据进行复杂的操作，各个操作遵循一定规则的同时又有先后之分。因此，计算机网络协议也是依照计算机的硬件结构分层设定的。网络都按层的方式来组织，每一层都建立在它的下层之上。不同的网络，其层的数量、名称、内容和功能都不尽相同。然而在所有的网络中，每一层的目的都是向它的上一层提供一定的服务，而把如何实现这一服务的细节对上一层加以屏蔽。

目前，电子商务认可的网络模型是 OSI 模型和 TCP/IP 模型。

1. OSI 模型

国际标准化组织在 20 世纪 70 年代末正式提出了“开放系统互连(open system interconnection，OSI)”基本参考模型。该模型如表 1-1 所示。它定义了异种计算机互连标准的主体结构，由七层组成，自下而上依次为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。它的每一层都有特定的功能，连接了较低层和较高层的服务。

表 1-1　OSI 模型

层　　号	层　　名
7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层

(1) 物理层。底部的层次称为物理层，负责比特(bit)流的传输。它接收来自数据链路层的数据帧，并按顺序传输这些数据帧的结构和内容，一次一位。物理层还负责到达数据流的接收，一次一位。这些比特流传递给数据链路层，进行重新组帧。

(2) 数据链路层。数据链路层的主要任务是加强物理层传输原始比特流的功能，使之对网络层显现为一条无错线路。发送方把输入数据分装在数据帧里，按顺序传送各帧，并处理接收方回送的确认帧。因为物理层仅仅接收和传送比特流，并不关心它的意义和结构，所以只能依赖数据链路层来产生和识别帧边界。

数据链路层实际上由两个独立的部分组成——媒体访问控制(media access control，MAC)层和逻辑链路控制(logical link control，LLC)层。MAC 层描述在共享介质环境中如何进行站的调度、发生和接收数据，用于确保信息跨链路的可靠传输，对数据传输进行同步，识别错误和控制数据的流向。LLC 层支持无连接服务和面向连接服务，它在数据链路层的信息帧中定义了很多域，这些域使得多种高层协议可以共享一个物理数据链路。

(3) 网络层。网络层负责在源和终点之间建立连接。它一般包括网络寻径，还可能包括流量控制、错误检查等。相同 MAC 标准的不同网段之间的数据传输一般只涉及数据链路层，而不同的 MAC 标准之间的数据传输都涉及网络层。例如，IP 路由器工作在网络层，因而可以实现多种网络间的互连。

(4) 传输层。传输层提供与数据链路层类似的服务，负责传输的端到端数据的完整性。与数据链路层不同的是，传输层能够提供超出本地局域网的这个功能，它可以检测由路由器丢弃的数据包并自动产生传输请求。传输层包括的协议有 TCP(传输控制协议)、UDP(用户数据报协议)等。

(5) 会话层。OSI 会话层的功能是在两个计算机系统之间的连接过程中，协商和管理通信的流程，这个通信流程称为会话。它确定通信是单向还是双向，并保证在完成一个请求之后，才接收下一个请求。这一层的使用相对较少，许多协议把这一层的功能捆绑到传输层。

(6) 表示层。表示层负责管理数据的编码方法，并不是每台计算机都使用相同的数据编码方案，表示层负责提供不兼容数据编码方案之间的转换。表示层的编码和转化模式包括公用数据表示格式、性能转化表示格式、公用数据压缩模式和公用数据加密模式。

(7) 应用层。OSI 参考模型中的最上一层是应用层，是最接近终端用户的 OSI 层。尽管名称是应用层，但这一层不包括应用程序，而是提供应用程序和网络服务之间的接口。

2. TCP/IP 模型

TCP/IP 模型基于 TCP/IP，中文名为传输控制协议/因特网互连协议，又称网络通信协议。TCP/IP 起源于 20 世纪 60 年代末美国政府资助的一个网络分组交换研究项目，是发展至今最成功的通信协议，它被用于当今所构筑的最大的开放式网络系统——因特网上。

TCP/IP 并不完全符合 OSI 的七层参考模型。由于 OSI 模型中各个层中的操作存在重复和冗余。TCP/IP 将功能相似的协议层合并在一起，并改善了原先的数据传输模式，形成了四层的层级结构，即网络接口层、网际层、传输层和应用层。图 1-7 为 TCP/IP 模型和 OSI 模型的比较。

(1) 网络接口层：详细制定如何通过网络发送数据，包括直接与网络媒体(如同轴电缆、光纤或双绞线等)接触的硬件设备如何将比特流转换成电信号。

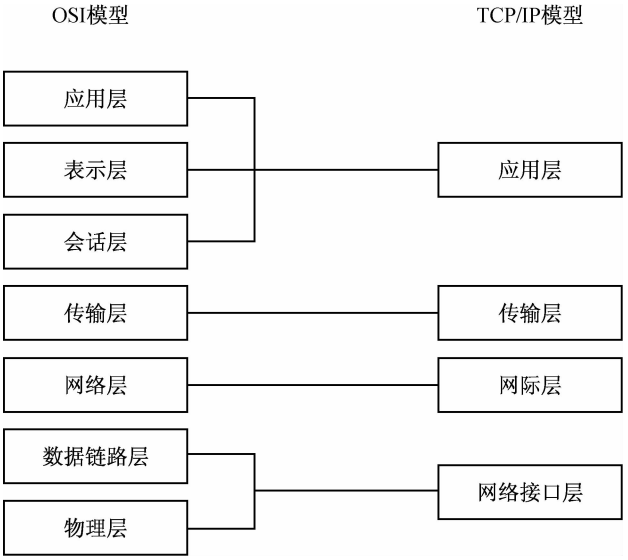

图 1-7　TCP/IP 模型和 OSI 模型的比较

(2) 网际层:将数据装入 IP 数据报,包括用于在主机间及经过网络转发数据报时所用的有关源地址和目的地址的信息,实现 IP 数据报的传送。

(3) 传输层:提供主机之间的通信会话管理,定义了传输数据时的服务级别和连接状态。

(4) 应用层:定义了 TCP/IP 应用协议及主机程序与要使用网络的传输层服务之间的接口,对应于 OSI 七层参考模型的应用层、表示层和会话层。

(四) 计算机网络的起源和发展

当前遍及世界的计算机网络起源于美国国防部的一个军事网络。

1969 年初,美国国防部高级研究计划署为军事目的建立了阿帕网(ARPAnet)。开始时,它只连接了 4 台主机,这便是只有 4 个网点的"网络之父"。到了 1972 年公开展示时,由于学术研究机构及政府机构的加入,这个系统连接了 50 所大学和研究机构的主机。1982 年阿帕网又实现了与其他多个网络的互连,从而形成了以 ARPAnet 为主干网的互联网。

1983 年,美国国家科学基金会(NSF)提供巨资,建造了全美五大超级计算中心,为使全国的科学家、工程师能共享超级计算机的设施,又建立了基于 IP 的计算机通信网络 NFSnet。

1986 年,NFSnet 建成后取代了 ARPAnet 成为互联网的主干网。早期以 ARPAnet 为主干网的互联网只对少数的专家以及政府要员开放,而以 NFSnet 为主干网的互联网则向社会开放。

到了 20 世纪 90 年代,随着计算机的普及以及信息技术的发展,互联网迅速地商业化,并以其独有的魅力和爆炸式的传播速度成为热点。同时,为了适应快速、高效的需要,很多城市、社区、大学建立起了自己的局域网和城域网;很多公司、企业也建立起了适用于自己的商业模式的计算机网络。

2009 年,全球网民数量已经突破了 17 亿。同时,一两名计算机使用者,也可以依照微软

的操作系统自行建立一个小型的计算机网络。

引例解析

戴尔公司的运营模式不同于传统的企业运营模式，而是电子商务模式；其大部分产品销售不在实体店，而是在网上。戴尔公司通过网络完成订货和销售过程。

戴尔公司是应用电子商务比较成功的企业之一。电子商务可简单理解为利用一系列电子手段进行商务活动的一种方法，计算机网络及计算机网络技术、数据库技术、通信技术等都是电子商务活动得以实现的基础和前提。

戴尔公司的电子商务模式分为三个阶段：订货阶段、生产阶段、发运阶段。

在订货阶段，由于戴尔公司全部采用网上订购的方式，所以省去了大量的实体店面的费用；在生产阶段，无须积压大量的货物一次性运出，而是依照订单的具体需求进行生产分配；在发运阶段，由于省去了中间商、二级中间商等流程，直接将商品通过快递公司交给客户，因此省去了大量的仓储、物流、交易的费用。依照戴尔公司的创始人迈克尔·戴尔的说法：互联网是直销的终极模式。通过以互联网为基础的电子商务，戴尔的同类产品能够获得更大的竞争力。总结起来，戴尔公司通过电子商务进行产品销售具有的优势和值得其他企业借鉴之处如下：

(1) 顾客在下达订单后 3～5 天，即可送货到家，时间较短。

(2) 顾客可以根据自己的需要，定制自己想要的产品。这样既可以省掉顾客挑选的时间，又可以使公司有计划地生产。

(3) 厂家直销的产品不经过中间商层层转卖，所以产品零售价中不包含中间商的销售成本和利润，使顾客在价格上能够获得最大的优惠。

(4) 戴尔公司直接根据订单进行生产，所以仓库中几乎没有库存，这样就省去了大笔的仓储、搬运的费用。

(5) 这种依靠电子商务进行的直销能够保证客户不会买到水货和残次品，同时也使得戴尔公司的计算机不会出现组装机的情况，每一台戴尔计算机都能够得到一个“身份证号”，客户可以登录戴尔官方网站查看产品信息。

虽然戴尔公司的这种销售模式需要前期较大的投资和网站维护，但收益也是明显的。如今这个创始于 1984 年的计算机直销商赶上了时代前进的步伐，依靠电子商务走到了同行的前面。

本章小结

本章主要介绍了电子商务、计算机及网络的基础知识。

电子商务具有高效率、虚拟性、开放性、低成本的特点。电子商务的参与者有商家、消费者、政府。电子商务的常见模式有商家对商家模式、商家对消费者模式、消费者对消费者模式、行政机构对行政机构模式、商家对行政机构模式、消费者对行政机构模式 6 种。电子商

务起源于机票预订系统，进入互联网时代以后有了较为迅速的发展。电子商务有3个应用阶段：接入阶段、整合阶段和随需应变阶段。

计算机分为巨型机、大型机、小型机和微机等。前三者可以作为电子商务的服务器终端；微机往往作为消费者的客户端。计算机逐步小型化，功能更加强大，人机工程更加合理。计算机网络依靠计算机硬件和网络传输协议建立起来，现有的网络模型有OSI模型和TCP/IP模型。

一、思考练习

1. 电子商务的优势有哪些？
2. 电子商务给社会经济带来的变革有哪些？
3. 简述计算机网络的定义和功能。
4. 组成局域网的网络硬件可以分为哪几类？
5. 什么是B2B电子商务模式？请举例说明。
6. 简述我国电子商务发展面临的障碍。
7. 请解释OSI、TCP/IP的概念。
8. 计算机网络一般由哪些部分组成？

二、案例分析

案例一　易趣网的网上交易

易趣网目前已开展的交易方式主要有以下几种：

（1）C2C个人竞标采用卖方录入物品信息，买方出价竞价的交易形式，即买卖双方在易趣网上注册，卖方免费在易趣网上陈列欲出售的物品，买方免费在网上各自出价，最后卖方选择买方，与其联系完成交易。值得注意的是，易趣网采用“网上竞拍，网下成交”的交易形式，也就是网上交换买卖信息、网下银货两讫的方式。这轻松绕开了始终困扰中国电子商务从业者的两大难题——网上支付和货物配送。于是大到汽车、房产，小到手机、邮票，都可以借助易趣网这一虚拟交易平台轻松实现交易。

（2）易趣网的B2C网上直销目前主要集中于计算机及其配件、外设及其附件、热点商品等电子产品。

（3）商家专卖是易趣网改版后新开设的购物频道，是众多品牌卓越、服务上乘的商家专卖店的集合。商家专卖区采用“定价购物”以及“竞价购物”两种方式。前者价格固定，不能讲价；后者价格由竞价得来，商品经常采用“一元底价”竞标，并由易趣提供送货保障。商家也可以在此开展促销等主题活动，让网民了解商家的最新货物情况、网上报价、公司品牌形象等。

问题

请根据案例内容，分析易趣网的交易方式。

案例二　海尔的网上商城

2000 年 4 月 18 日，海尔网站又一次全面改版，并正式开通了网上商城。海尔网上商城全面展示海尔的在销产品，提供灵活多样的查询方式，通过对产品的详尽介绍，科学地引导顾客购物，迅速定位顾客所需要的产品。方便的支付方式和完善的物流配送，使顾客真正体会到网络消费的便捷和实惠。顾客可以方便地在网上按照个人需要实现各种产品的自行组配，从而使海尔缩短了与顾客的距离，最大限度地满足了顾客的个性化需求。

海尔网上商城购物流程如下：

(1) 店内选购商品。在海尔网上商城挑选商品的方式有两种：一是通过页面左边的“网上商店商品查询”搜索；二是通过网页浏览。看中了喜欢的商品，顾客随时可以设定好购买数量，填入对商品的特殊要求，如颜色、送货安装时间等，然后单击“选购”按钮将它放入“购物车”。

(2) 结算与发货。首次光临海尔网上商城的顾客，按照登记页面的提示逐一填写信息，下次光临时就可以不必重复输入资料。顾客最好注册为会员，因为海尔网上商城会按照会员名字累计购买额，到一定金额后给予优惠或者其他奖励。

结算方式分为货到付款和电子付款两种。顾客可以使用网上银行通过安全系统直接向认证系统提交信用卡资料。海尔网上商城将在收到顾客的订单后两个工作日之内安排发货。

问题

请根据案例内容，总结出海尔网上商城的购物流程。

案例三　海尔的信息网络建设

青岛海尔集团自创立之日起，就一直在制造令家电行业瞠目结舌的新闻。如今，“世界 500 强企业”的海尔集团又正在进行一场悄无声息的革命——信息网络建设，以求达到提高企业信息处理能力，全方位沟通国内外市场，降低运营成本，提高市场占有率的目的。海尔集团通过建立自己的网站，一方面宣传海尔的企业形象；另一方面利用现代化的信息网络，加大自己产品市场推销的力度。

海尔网上商城采用智能化集成电子商务平台，使多媒体技术、面向对象数据库技术和 Web 技术相结合，构成了一个含有大量文字、图片、语音、视频信息，并可与三维虚拟场景交互地面向 internet 的多媒体数据库应用系统，实现了基于 Web 的产品定制与导购功能。

在海尔网上商城购物，顾客不但可以享受优惠的网上购物价格(免费配送)，享受海尔的星级服务，而且可以享受海尔在网上提供的许多个性化超值服务。客户可以订购适合自己特殊需求的产品，也可以直接参与产品的设计，真正成为海尔产品的主人。

海尔网上商城 B2B 贸易栏目的开通，标志着海尔企业电子商务发展的新阶段。这一栏

目的产生，说明了中国企业在走过了几年的电子商务发展初级阶段后，已经开始真正步入电子商务的纵深领域。

问题

根据上述材料，联系海尔的成功经验，分析国内企业如何开展电子商务服务来提高自身的竞争力。

案例四　拉拉手电子商务网

拉拉手电子商务网是一个企业运营资源交易网，采用B2B的电子商务模式，为企业提供多种网上商务服务。拉拉手率先采用的“买方先询价，卖方后报价”的交易模式，为企业交易运营资源提供了先进的在线商务平台，降低了运营成本，增强了企业的竞争力。“比较购物”、“电子优惠券”、“集体竞买”等让消费者获得了物美价廉的商品和服务，为企业创造了新的商业机会。拉拉手创造的多项独特 internet 软件技术，使众多加入拉拉手电子商务网的企业在电子商务应用浪潮中领先一步。

拉拉手企业运营资源交易网本身并不直接参加销售，而是提供优秀的交易平台和先进的交易模式，让买卖双方自由比较和选择。使用互联网平台，交易更加省时、省力、省钱；采用“买方先询价，卖方后报价”的模式，交易目标更明确，把传统市场中只有大宗交易才可能使用的方法、投标机制引入电子商务，通过网站，买卖双方“拉拉手”。企业运营资源是指企业经营所需要的非生产原料性的服务与产品，主要包括财税工商、法律咨询、广告展览、印刷设计、网络服务、营销策划、人力资源、储运进出口、后勤行政、保险金融、计算机硬件、计算机软件、办公用品、办公设备、办公家具等。目前，在拉拉手企业运营资源交易网可以交易多种服务和产品。拉拉手比较购物的口号是：网上商店大比拼，货比三家最舒心。因为在数百家网上商店、数十万种商品中，我们要作出最佳的购买选择几乎是不可能的，所以，拉拉手可以帮助我们货比三家。拉拉手不卖东西，不是网上商店，而是网上商店的比较中心，每时每刻搜索所有的网上商店，提供所需商品在不同网上商店的价格、服务等信息，帮助优秀的商家和目标消费者进行沟通。

问题

1. 拉拉手属于哪种电子商务交易模式？
2. 如何理解拉拉手企业运营资源交易网的核心经营思想？

实训设计

了解电子商务、计算机和网络

【实训目标】

了解电子商务在实际生活中的应用，掌握基本的计算机操作方法，了解计算机网络。

【实训内容】

（1）登录某商品交易网站，分析网站的主要功能，通过相关操作了解该网站是如何实现网上交易的。

（2）申请注册一个 E-mail 邮箱，并利用它给其他人发送邮件。

（3）查找自己感兴趣的网站地址，并访问这些网站，了解不同网站的不同之处。

第二章
电子商务安全概述

知识目标

» 了解电子商务安全的含义、要求和体系结构；

» 在了解基本概念的基础上，对于电子商务安全面临的问题有全面的认识。

技能目标

» 能够对电子商务安全有整体的了解，识别电子商务中存在的各种不安全因素；

» 形成一种电子商务交易中的安全意识，能够保护自己的合法权益。

引例

神秘黑客接连攻击五大网站

2000年2月8日至10日(北京时间),一伙“神通广大”的神秘黑客在三天的时间里接连袭击了互联网上包括雅虎、美国有线新闻等在内的五个最热门的网站,并且造成这些网站瘫痪长达数个小时。

美国东部时间2000年2月7日(北京时间2月8日),雅虎网站遭到黑客袭击。遭袭后,雅虎的技术人员大惊失色,一边马上采取紧急措施查明黑客的袭击手段,一边立即进行紧急补救。技术人员很快发现,黑客使用了一种名为“拒绝服务”的入侵方式,在不同的计算机上同时用连续不断的服务器电子请求来轰炸雅虎网站。这种方式类似于某人通过不停拨打某个公司的电话来阻止其他电话打进,从而导致公司通信瘫痪。在袭击进行到最高峰的时候,网站平均每秒钟要遭受1 GB数据的猛烈攻击,这一数据量相当于普通网站一年的数据量!

美国东部时间2000年2月8日,也就是雅虎网站遭袭后第二天,世界最著名的网络拍卖行eBay因遭神秘黑客袭击而瘫痪了整整两个小时,以致任何用户都无法登录该站点;赫赫有名的美国有线新闻网CNN随后也因遭神秘黑客的袭击而瘫痪近两个小时;风头最劲的购物网站亚马逊也被迫关闭一个多小时。

美国东部时间2000年2月9日(北京时间2月10日),澳大利亚悉尼一家公司的网站也遭到了同样的网络袭击。这家名叫“比蒂有限公司”的网站在过去三个星期的时间内接连20多次遭受黑客用“拒绝服务”软件的袭击,每次都导致整个网站瘫痪,而且每次瘫痪长达数个小时。

五起袭击事件给全世界敲响了警钟。三天内发生的这五起网络大规模袭击事件有着惊人的相似之处,然而黑客是如何潜入系统,将雅虎等网站“黑掉”的呢?这次事件给人们带来哪些经验和教训呢?面对这种情况,应该运用哪些电子商务安全知识来保护自己的网络安全呢?这些都将在本章为读者介绍。

第一节　电子商务安全简介

一、电子商务安全的含义

由第一章的介绍可以知道,电子商务是一种依托网络技术而实现买卖双方互不谋面即达成交易的全新的业务和服务模式。它为全球的商家和消费者提供了丰富的商务信息、简捷的交易过程、低廉的交易成本、可靠的贸易平台,使依托互联网的电子贸易成为可能。

但是电子商务并非尽善尽美,电子商务在给人们带来巨大便利的同时,也带来了众多的安全隐患。电子商务安全从整体上可以分为计算机网络安全和商务交易安全两大部分。其中,计算机网络安全主要包括计算机网络设备安全、计算机网络系统安全、数据库安全等,主

要解决的是计算机网络本身存在的安全问题，要采用一系列网络安全增强方案来保证计算机网络自身的安全。商务交易安全则主要是针对传统商务在网络应用时产生的各种安全问题。计算机网络安全和商务交易安全相辅相成、缺一不可，它们是电子商务活动得以实现的重要支撑。

为了更好地理解电子商务安全，需要先来了解网络中所存在的安全隐患。下面主要介绍问题最为突出的计算机病毒、黑客攻击和系统安全漏洞。

（一）计算机病毒

到目前为止，计算机病毒还没有一个公认的、确切的定义。虽然“计算机病毒”是根据计算机软硬件所固有的特点编制出的、具有特殊功能的程序，与生物医学上的“病毒”有本质上的不同，但由于这种程序具有传染性和破坏性，与医学上的“病毒”又有相似之处，所以习惯上也将这些“具有特殊功能的程序”称为“病毒”。

根据 1994 年 2 月 18 日我国正式颁布实施的《中华人民共和国计算机信息系统安全保护条例》可知：计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

典型案例 2-1

“熊猫”也会“烧香”

2006 年底，一种被称为“熊猫烧香”的蠕虫病毒肆虐网络。这种病毒及其变种通过传输中的文档感染破坏计算机程序，主要通过盗取网友的网络游戏账号、QQ 号、银行账号密码以及各种认证信息进行非法活动。病毒的编写者李杰（化名）将病毒或盗取的信息卖出，一天能够获利超过 1 万元，这意味着被攻击的消费者有可能因为一宗小买卖一夜之间失去数月的收入。

图 2-1 为“熊猫烧香”病毒图标和计算机感染“熊猫烧香”病毒后的状态，几乎所有的图标都变成了熊猫。

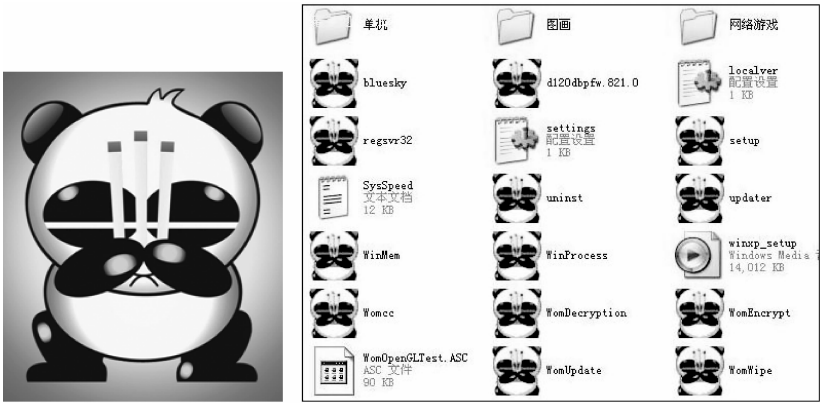

图 2-1 “熊猫烧香”病毒图标和计算机感染“熊猫烧香”病毒后的状态

2009年末，金山公司发布了《2009年中国计算机病毒疫情及互联网安全报告》。该报告显示，2009年，金山毒霸共截获新增病毒和木马2 000多万个，与五年前新增病毒数量相比，增长了近400倍。其中IE主页篡改类病毒第一次登上了十大病毒之首，成为2009年的“毒王”。金山毒霸共拦截病毒攻击约84亿次，全国共有约7 600万台计算机感染病毒。其中，广东、江苏、山东三地的病毒感染量位列全国前三位，总感染量占到全国感染量的25%。

中国互联网络信息中心和国家互联网应急中心（CNCERT/CC）联合发布的《2009年中国国民网络信息安全状况调查报告》显示，2009年，全国有52% 的网民曾遭遇过网络安全事件。其中，77.5%的网民是在网络下载或浏览时遭遇病毒或木马的攻击；26.9%的网民是通过移动存储介质（U盘、移动硬盘、光盘等）感染病毒；10.1%的网民不知道感染病毒或木马的途径。

近几年来，计算机病毒主要呈现的特征可以归纳为以下几个。

1. 经济利益驱使计算机病毒技术不断突破

经济利益成为目前病毒制造者不断追求技术突破的原动力。受此利益驱使，近年来的计算机病毒的感染率呈爆炸式增长，网络经济犯罪率不断增加，病毒的绝大部分变化都是围绕此中心展开。在巨大的经济利益诱惑下，病毒制造者的技术力量也有了飞跃式的发展。Rootkit隐藏技术以及对抗杀毒软件技术被广泛应用。“灰鸽子”及其变种使用Rootkit技术自我隐藏，包括病毒文件、注册表键值等都可以被隐藏，普通用户很难发现。威金病毒、“落雪”木马及其变种全部具有对抗反病毒软件的功能，能终止多款国内外知名的杀毒软件。除此之外，2006年传播十分广泛的“流氓软件”技术也不断升级。这些软件为了牟利，已经不仅仅局限于使用小程序，还借助木马病毒进行传播。

2. 网银病毒迅猛增长

随着电子商务交易的发展，网络银行的使用越来越广泛。据CNNIC的统计，2008年的网络银行使用率为19.3%，网民规模为5 800万人；2009年的使用率为24.5%，网民规模为9 406万人，增长率为62.3%；而2010年上半年的使用率就达到了29.1%，增长速度非常惊人。

从2004年8月到2006年10月期间，仅两年多时间，全国感染各类网银木马及其变种的用户数量就增长了600倍，用户每月感染的病毒及其变种的数量约有160种，而且病毒发展呈加速上升趋势。

典型案例2-2

网银大盗

“网银大盗”开启了偷盗网上银行个人用户信息的先河，并立刻引起了公众的广泛关注。该病毒通过键盘记录的方式，监视用户操作。当用户使用个人网上银行进行交易时，该病毒便会恶意记录用户所使用的账号和密码。记录成功后，病毒会将盗取的账号和密码发送给病毒编写者，给用户造成经济损失。

2009年，湖南长沙雨花区法院便审理了一起利用“网银大盗”等病毒恶意窃取网银用户存款的案件。李强（化名）虽然没有太高的文化水平，但却是一名技术纯熟的“网络高手”。他先将“网银大盗”和“灰鸽子”程序下载到服务器上，用于接收信息、储存资料

和远程控制他人计算机。一旦感染“网银大盗”的计算机开始运行，便会以自动截屏的方式将感染病毒计算机用户的密码发送到他的服务器上，他再一一将其整理好，逐一盗取。在收缴的证据中，就有李强保存在U盘里的账户资料，有300多条个人信息，身份证号、账号、密码、手机号、余额等信息一应俱全。通过这种方式，2006年至2009年，他先后窃取了多名网络用户的银行资金40余万元。

3. 病毒更加“人性化”，更具有欺骗性

现在的计算机病毒越来越注重利用人们的心理因素，如好奇、贪婪等。肆虐一时的“裸妻”病毒邮件的主题就是英文的“裸妻”；邮件正文为“我的妻子从未这样”；邮件附件中携带一个名为“裸妻”的可执行文件，用户一旦执行这个文件，病毒就被激活。类似的病毒还有“My baby pic”病毒、“库尔尼科娃”病毒等。“My baby pic”病毒是通过可爱的宝宝照片传播病毒的，虽然杀伤力不大，但发作起来也会造成计算机文档的损毁。而“库尔尼科娃”病毒的大流行则是利用了“网坛美女”库尔尼科娃难以抵挡的魅力。

4. 病毒更加“智能化”

与传统计算机病毒不同的是，许多新病毒（包括蠕虫、黑客工具和木马等恶意程序）是利用当前最新的编程语言与编程技术实现的，它们易于修改以便产生新的变种，从而逃避反病毒软件的搜索。

典型案例 2-3

“智能化”病毒防不胜防

许多病毒为了防止反病毒软件的查杀，变得越来越“智能化”了。例如，爱虫病毒是用VBScript语言编写的，只要通过Windows下自带的编辑软件修改病毒代码中的一部分，就能轻而易举地制造出病毒变种，从而可以躲避反病毒软件的追击。

另外，新病毒利用Java、ActiveX、VBScript等技术，可以潜伏在HTML页面里，在用户上网浏览时触发。例如，Kakworm病毒虽然早在2004年1月就被发现，但它的感染率一直居高不下，原因就是它利用ActiveX控件中存在的缺陷进行传播，因此装有IE 5或Office 2000的计算机都可能被感染。这个病毒的出现使原来不打开带毒邮件附件而直接予以删除的防邮件病毒的方法完全失效。更令人担心的是，一旦这种病毒被赋予其他计算机病毒的特性，其危害很有可能超过任何现有的计算机病毒。

5. 病毒变种快、更新快、存活能力强

计算机病毒在出现以后往往会迅速地发展出多个变种，而且更新速度快、存活能力强。例如，2001年出现的“灰鸽子”病毒便有数量众多的变种，截至2006年底，就已有3万多个变种，高峰时几乎每天都要处理十多个变种病毒。据保守估计，现在“灰鸽子”病毒的变种有6万多个。

另外，很多木马病毒都具有自动升级功能，可以迅速地在较短的时间内更新自身，防止被反病毒软件查杀。更多的木马采用传统病毒的感染文件技术，甚至可以定向感染极少数的正常程序，使得即便自身被杀，仍然有机会死灰复燃。

6. 智能手机成为病毒的下一个攻击目标

随着智能手机的普及，利用智能手机上网浏览网页、下载铃音及彩信、在线看电影的用户越来越多，然而智能手机应用的普及不可避免地带来安全隐患。截至 2010 年 6 月底，我国手机网民已达到 2.77 亿人，其中只使用手机上网的网民规模达到 4 914 万人，较 2009 年底增长了 1 842 万人。但是这些手机网民对手机安全性的认识还不够，截至 2009 年底，仅有 7.4%的手机网民使用安全防护软件，这就为手机病毒的肆意传播提供了可乘之机。例如，2005 年出现的 Fontal.A 手机病毒号称“毒王”，它能够通过手机文件共享或网络聊天传输，向手机操作系统植入恶意文件，使手机死机或者下次启动时因操作系统崩溃而不能使用，只能通过格式化并重新安装系统才能修复。现在，手机病毒频频发作，新病毒层出不穷，手机用户只有提高安全意识，主动防御才能有效防止病毒的侵害。

（二）黑客攻击

黑客最早出现于 20 世纪 50 年代。“黑客”一词是由英文 hacker 翻译而来的，最初是指专门研究、发现计算机和网络漏洞的计算机爱好者，带有一定的褒义。他们对计算机和网络技术的研究具有很高的兴趣和执著性，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。但随着计算机和网络的发展，“黑客”已变为了那些专门利用计算机进行破坏或入侵他人计算机的人的代名词，泛指对计算机系统进行非授权访问的人员。为了区分两者的不同，也有人提出破坏或入侵他人计算机系统者的正确名称应该为 cracker，即骇客。

黑客攻击指的是黑客非授权入侵其他程序、系统或网络，破坏该系统、程序或网络的行为。常见的黑客攻击方法主要有端口扫描、口令破解、木马攻击、缓冲区溢出攻击、拒绝服务攻击和网络监听。

典型案例 2-4

百度“被黑”

2010 年 1 月 12 日，中国国内最大的中文搜索引擎——百度，遭到黑客攻击，网页无法登录，有的还会出现黑页 Iranian Cyber Army（伊朗网军）[①]。这次攻击事件导致百度网页瘫痪近 6 个小时。由于百度主要从事网页搜索及相关的互联网业务，这次攻击给它造成的损失和影响可能有客户赔偿、形象损失、股价下跌、长期影响等四个方面，损失超过 700 万元。

为了对电子商务的安全问题有更感性的认识，有必要在此分析一下黑客盗取信用卡的过程。黑客在互联网的新闻组上发布带有“后门”病毒的程序，并鼓励人们下载到自己的计算机上，一旦某台计算机下载了此程序，那么它就成为黑客入侵的对象。黑客可以浏览被入侵者计算机上的所有信息资源，可以实时地掌握被入侵者的桌面使用情况。如果被入侵者此时输入信用卡号，那么黑客就可以易如反掌地窃取到这一信息，这是信用卡被盗用的主要

① 伊朗网军：可译为伊朗网络或伊朗网络部队，是一个相对神秘的黑客组织。它是民间组织，也经常“黑”伊朗政府的网站，往往对一些他们认为“有问题”的网站进行攻击。

原因。即使用户不曾在公共信息场所下载软件，也很有可能成为无辜的受害者。因为黑客程序中的“后门”病毒具有很强的蔓延性，即一台计算机被感染后，病毒可通过此计算机上的地址簿向所有这些地址的计算机传播，然后按同样的方法再进一步把态势扩大。这种几何级的增长使病毒的蔓延速度极快，覆盖范围极广。

所以，不经意间或许某一用户的计算机就已成为黑客的“盘中餐”，而一个从事网上交易的网站一旦发生消费者信用卡信息泄露事件，那么将不会再有人去访问这个站点。因此，要使电子商务健康、蓬勃地发展，就必须用全面的电子商务安全解决方案为交易提供信任保障。

（三）系统安全漏洞

系统安全漏洞也叫系统脆弱性，简称漏洞，是计算机系统在硬件、软件、协议的设计与实现过程中或系统安全策略上存在的缺陷和不足。非法用户可以利用漏洞获得计算机系统的额外权限，在未经授权的情况下访问或提高其访问权限，从而破坏系统的安全性。漏洞是针对系统安全而言的，包括一切可导致威胁、破坏计算机系统安全性（如完整性、可用性、保密性、可靠性、可控性）的因素。任何一个系统，无论是软件还是硬件都不可避免地存在漏洞，所以从来都没有绝对的安全。当然，漏洞的存在本身并不能对系统安全造成什么损害，关键在于攻击者可以利用这些漏洞引发安全事件。

用户使用最多的 Windows 系统有以下几种常见漏洞。

1. IIS 服务器

微软的 IIS 服务器存在缓存溢出漏洞。它难以合适地过滤客户端请求，执行应用脚本的能力较差。部分问题可以通过已发布的补丁解决，但每次 IIS 的新版本发布都会带来新的漏洞。因此，IIS 出现安全漏洞并不能完全归罪于网管的疏漏，建议管理人员运行 HFNetChk（一个命令行执行程序）。

2. Windows 网络共享

由于使用了服务器信息块协议或通用互联网文件系统，远程用户可以访问本地文件，但也向攻击者开放了系统。

3. 匿名登录

Windows 操作系统的账户服务至关重要，但一旦用户通过匿名登录进程后就可以匿名访问其他系统中的文件。不幸的是，这意味着攻击者也可以匿名进入系统。

4. Windows 密码

脆弱的密码是管理人员的心腹大患，尽管各种系统设置都要求用户使用足够“强壮”的密码并进行定期更换，但用户往往抱怨系统管理员作出的各种限制。这就引发了访问控制的脆弱性。

5. 注册表访问

在任何 Windows 系统中，注册表都是最重要的文件，而允许远程访问注册表将带来很大危害。

图 2-2 为 2000—2008 年国际权威应急组织 CERT/CC 统计并公布的漏洞数量。其中，

2008 年的数据为前三季度统计数据。

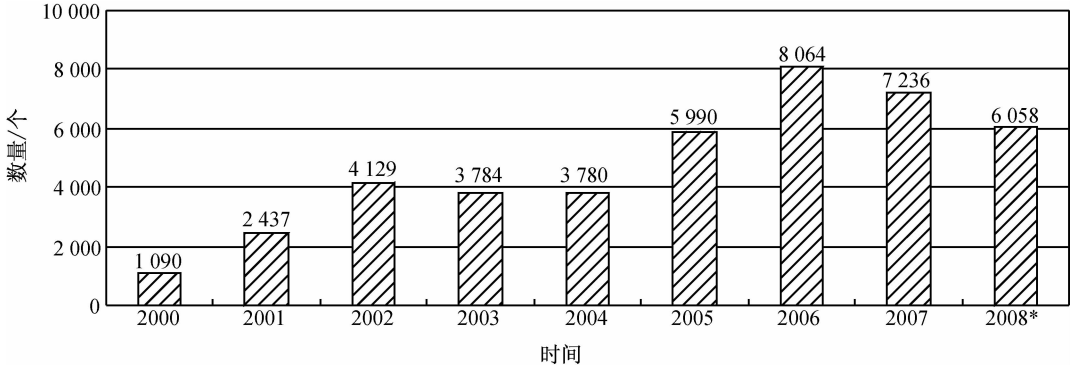

图 2-2　2000—2008 年 CERT/CC 统计并公布的漏洞数量

由图 2-2 可知，根据 CERT/CC 统计，2006 年是公布的漏洞数量最多的一年，达到了 8 064 个，平均每天约 22 个。2008 年前三季度的漏洞数已达到 6 058 个，较 2000 年增长了约 5 倍。由此可见，漏洞的大量存在也是威胁互联网交易的重要原因之一。

以上的大量事实和数据表明，要保证电子商务的正常运行，就必须高度重视其安全问题。电子商务的安全涉及社会的方方面面，不是一两种杀毒软件或认证技术就能够解决的。为了保证电子商务的安全，实现电子商务的健康有序发展，必须对电子商务的各个流程、交易方式、实现基础有所了解。同时，保证电子商务的安全，实现电子商务的健康有序发展也是电子商务安全的最终目的。

二、电子商务安全的要求

电子商务发展的核心和关键是交易的安全性。由于 Internet 本身是开放的，网上交易面临着种种危险，所以提出了相应的使用和安全要求。电子商务安全的具体要求如下。

1. 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，而不会出现任由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，要提交订购信息，提供相关的支付信息；商家在销售商品的时候可以合理地使用交易平台，提供自己的信息和商品的信息。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。可以说，可用性是电子商务安全的首要目的。如果不能满足这个要求，所谓交易的机密性、完整性等都无从谈起。

2. 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。

机密性一般针对通过密码技术传输的信息提出。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；如果订货和

付款的信息被竞争对手获悉，就有可能丧失商业机会。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。电子商务是通过身份认证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。

3. 及时性

及时性是防止延迟或者防止拒绝服务。

及时性的安全威胁的目的是破坏正常的计算机处理或完全拒绝服务。在电子商务中，延迟或是删除一个消息可能会带来灾难性的后果。例如，当电子商务应用在瞬息万变的股票市场时，通过计算机终端进行股票的买入和售出需要很好地把握时机。一旦出现了信息延迟，可能原本良好的商机便会错失，甚至会出现意外的损失。

4. 可认证性

可认证性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，这意味着当某人借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认证中心（CA）和证书来实现。

5. 完整性

完整性是指交易数据等交易信息的内容与发送方完全一致，没有出现缺失或者偏差。

电子商务简化了贸易过程，减少了人为的干预，同时也带来了维护贸易各方商业信息完整性和统一性的问题。由于数据输入时的意外差错或欺诈行为，可能会导致贸易各方的信息差异。此外，数据传输过程中的丢失、信息篡改、翻译错误①、信息重复或者信息传输的次序差异会导致贸易各方信息出现不同。贸易各方信息的完整性将影响其交易和经营策略。因此，保持贸易各方信息的完整性是电子商务应用的基础。

6. 抗抵赖性

抗抵赖性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否认的，否则必然会损害一方的利益。例如，订购黄金时，订货时进价较低，但收到订单后，金价涨了，如果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加盖印章，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，通过手写签名和加盖印章

① 翻译错误：随着中国与世界贸易往来的加深，中国商户和外国商户的交流逐年增加，但是由于语言上的差异及相关翻译软件和工具的不成熟，导致了很多商业信息在交流的过程中出现差错，这也是信息不完整性的一种体现。

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，保证电子商务实施过程中的可用性、机密性、及时性、可认证性、完整性和抗抵赖性是实现电子商务安全的要求，而这些需要数据加密技术、消息摘要、数字签名、认证技术等多种技术共同完成。当各种技术相互作用成为一个整体的时候，便形成了一种传输协议或者安全协议。多种安全协议保证了电子商务的安全，最终形成了一个功能完善的交易系统，保证了系统管理、维护的可靠性。电子商务安全正是沿着这样的思路完成它的目的的。

三、电子商务安全的体系结构

电子商务安全的保证主要体现在 3 个方面：技术保障、安全管理保障和法律环境保障（如图 2-3 所示）。

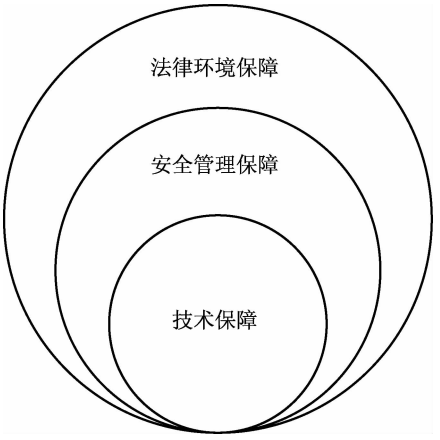

图 2-3　电子商务安全的体系结构

（一）技术保障

技术保障是指实现电子商务所需要的设备、技术等能够稳定、安全地提供所需的功能。其中主要包括实体的安全和网络技术的安全。

1. 实体的安全

实体的安全包括环境安全和设备安全。

（1）环境安全。环境安全主要是指系统要具有受灾报警、受灾保护、受灾恢复等功能。其根本目的是保证电子商务的实体——计算机、传输线路、交易终端等，免受外来自然天气变化的影响，包括水灾、火灾、地震、雷击等。在灾难发生前，能够对灾难进行检测并报警；灾难发生时，能够对正在遭受破坏的电子商务设备和部件进行紧急抢救，保护数据和信息的安全；灾难发生后，能够在一定程度上实现自我恢复和系统信息的整理，将影响降至最低。

（2）设备安全。设备安全包括设备防盗、设备防毁、防止信息泄露、防止线路截获、抗电磁干扰、电源保护、线路传输安全等。设备防盗就是对电子商务系统的设备实施防盗保护，也就是对电子商务系统的设备和部件采取一定的防盗手段（如安装报警器、监视摄像头等），来提高系统设备和部件的安全性。设备防毁是指防止计算机设备等实体出现毁坏，造成电

子商务交易的中断，这其中包括自然破坏和人为破坏。防止信息泄露可以提高系统内敏感信息的安全性。防止线路截获主要是防止外界对电子商务系统通信线路的截获和干扰。抗电磁干扰主要是防止对电子商务系统的电磁干扰，从而保护系统内部的信息。电源保护主要是指为电子商务系统设备的可靠运行提供能源保障，保证电源工作的连续性和稳定性。线路连接安全是指传输线路应有露天保护措施或埋于地下，并要求远离各种辐射源，以减少由于电磁干扰引起的数据错误。电缆铺设应当使用金属导管，以减少各种辐射引起的电磁泄漏和对发送线路的干扰。集线器和调制解调器应放置在受监视的地方，以防外连。对连接要定期检查，以检测是否有窃听、篡改或破坏行为。

2. 网络技术的安全

网络技术是电子商务实现的基础，技术因素对电子商务安全的影响最为直接。不恰当的系统设计、不正确的参数配置等技术问题都会成为电子商务系统安全的直接隐患。常见的几种安全技术如下：

(1) 网络安全检测设备。“预防为主”是防范黑客的基本指导思想。利用网络从事交易的单位或个人，有条件的话，应当加强对黑客行为的网络监控。Safe Suite 是第一个也是应用最为广泛的网络安全监控系统，它是为审核、监控和校正网络安全而专门设计的。Safe Suite 可以找出安全隐患，提供堵住安全漏洞所必需的校正方案，建立必要的循环过程，确保隐患即刻被纠正。此外，Safe Suite 还监控各种变化情况，从而使用户可以找出经常发生问题的根源。Safe Suite 包括 Web Security Scanner、Firewall Scanner、intranet Scanner、System Security Scanner 和 Real Secure。Safe Suite 检测安全隐患的对象包括：Web 站点、防火墙和路由器、Windows 系列、Windows NT 和 UNIX 工作站、Windows NT 和 UNIX 服务器等。

(2) 证书。认证与访问控制的证书的发放与管理是一个根本性的问题。最知名的证书授权部门是 VeriSign。VeriSign 是一个提供智能信息基础设施服务的上市公司，VeriSign 的数字信任服务通过 VeriSign 的域名登记、数字认证和网上支付三大核心业务，在全球范围内建立起了一个可信的虚拟环境，使任何人在任何地点都能放心地进行数字交易和沟通。另外，VeriSign 正在开发一种为大型机构定做证书的 Private Label(专用标签)服务。VeriSign 依靠目前的基础结构规模可提供数以万计的证书服务。

(3) 防火墙。防火墙是指设立在本地网络与外界网络之间的一道或一组执行策略的防御系统。它可以使用户或企业确定什么人在什么条件下可以进入其 internet 环境。防火墙的产品种类繁多，性能和价格也各不相同。防火墙作为最成熟的、最早产品化的网络安全机制，其最初的设计就是防范外部的攻击。改进的防火墙技术可更有效地控制内部和外部病毒的破坏。在设计防火墙时必须考虑防火墙的姿态、机构的整体安全策略、费用、基本构件和拓扑结构。目前较为成熟的防火墙往往将杀毒软件作为产品的一部分一同销售。

(4) 防入侵措施。应加强对文件处理的限制，控制重要文件的处理。利用报警系统检测违反安全规程的行为，即安全码的不正确使用或使用无效的安全码。对在规定次数内输入不正确的安全码使用者，网络系统可采取行动锁住该终端并报警，以防止非法者突破安全码系统进行入侵。

(5) 数据加密。数据加密是网络中采用的最基本的安全技术。网络中的数据加密，除

了选择加密算法和密钥外，主要问题是加密方式及实现加密的网络协议层和密钥的分配及管理。网络中的数据加密方式有链路加密、结点加密和端对端加密等方式，数据加密可在OSI协议参考模型的多个层次上实现。

（6）访问控制。访问控制从计算机系统的处理能力方面对信息提供保护，它按照事先确定的规则决定。当一个主体试图非法使用一个未经授权的资源时，访问控制机制将拒绝这一企图，并将这一事件报告给审计跟踪系统；审计跟踪系统将给出报警信息，并记入日志档案。对于文件和数据库设置安全属性，对其按共享的程度予以划分，通过访问矩阵来限制用户的使用方式，如只读、只写、读/写、可修改、可执行等。数据库的访问控制还可以分库、结构文件、记录和数据项四级进行。

（7）鉴别机制。鉴别是为每一个通信方查明另一个实体身份和特权的过程。它是在对等实体间交换认证信息，以便检验和确认对等实体的合法性，这是访问控制实现的先决条件。鉴别机制可以采用报文鉴别，也可以采用数字签名或终端识别等多种方式。

报文鉴别是在通信双方建立通信联系之后，每个通信者对收到的信息进行验证，以保证所收到信息的真实性的过程，也就是验证报文的完整性。一旦这种鉴别信息被得知，并且它的准确性和完整性有保证，那么本地用户或系统就可以作出适当的判断——什么样的数据可以发送到对方。

（二）安全管理保障

安全管理保障是在安全技术的基础之上，对系统的实时维护和设备的日常管理。从某种意义上来说，安全管理比安全技术更为重要。安全管理保障包括人员和制度的保障。

1. 人员的保障

电子商务不是电子设备之间独立进行的交易行为，其交易的主体仍然是人。既然人作为一种实体在电子商务交易过程中存在，则其必然对电子商务的安全产生重要的影响。由于人所产生的安全问题多为主观性的，如员工无意中泄露系统的密码，对企业心怀不满的员工对系统的恶意攻击等。因此，加强人员管理，对于保障电子商务安全十分重要。

2. 保密制度

网络营销涉及企业的市场、生产、财务、供应等多方面的机密，需要很好地划分信息的安全防范重点，采取相应的保密措施。信息的安全级别一般可分为以下三级：

（1）绝密级信息，如公司经营状况报告、订/出货价格、公司的发展规划等。此部分信息的网址、密码不能在网络上公开，只限于公司高层人员掌握。

（2）机密级信息，如公司的日常管理情况、会议通知等。此部分信息的网址、密码也不能在网络上公开，只限于公司中层以上人员使用。

（3）敏感级信息，如公司简介、新产品介绍及订货方式等。此部分信息的网址、密码可在网络上公开，供消费者浏览，但必须有保护程序，防止黑客入侵。

信息保密工作的另一个重要的问题是对密钥的管理。大量的交易必然要使用大量的密钥，密钥管理必须贯穿于密钥的产生、传递和销毁的全过程。密钥需要定期更换，否则可能使黑客通过积累密文增加破译机会。

3. 跟踪、审计、稽核制度

跟踪制度是以系统自动生成日志文件的形式来记录系统运行的全过程。日志文件里包

括操作日期、操作方式、登录人、登录次数、运行时间、交易内容等。通过该日志文件，可以对系统进行监督、维护分析和排除故障，为安全案件的侦破提供事实依据。但通过跟踪制度生成的日志文件，如果没有人去利用，有等于无，所以还需要建立审计制度来好好利用它。

审计制度规定网络审计员应经常对系统的日志文件检查、审核，以及时发现异常状况，监控和捕捉各种安全事件，并对系统日志进行保存、维护和管理。

稽核制度是指工商管理、银行、税务人员利用计算机及网络系统，借助稽核业务，应用软件调阅、查询、审核、判断辖区内电子商务参与单位业务经营活动的合理性、安全性，堵塞漏洞，保证电子商务交易安全，发出相应的警示或作出处理处罚的有关决定的一系列步骤及措施。稽核是针对企业外部的监督单位建立的，而审计则是针对企业内部员工的。

4. 数据容灾制度

按容灾能力的高低，容灾系统可以分为多个层次。例如，国际标准 SHARE 78 定义的容灾系统有七个层次，从最简单的仅在本地进行磁带备份，到将备份的磁带存储在异地，再到建立应用系统实时切换的异地备份系统，恢复时间也可以从几天到小时级到分钟级、秒级或零数据丢失等。企业应该根据自身情况，对不同安全级别的数据制定不同的数据容灾制度。

5. 病毒防范制度

在电子商务安全问题中，病毒对网络交易的顺利进行和交易数据的妥善保存造成极大的威胁。因此，从事网上交易的企业和个人都应当建立病毒防范制度，排除病毒的干扰。

首先，给自己的计算机安装防病毒软件。应用于网络的病毒防治软件分单机系统版和网络系统版两种。前者属于事后消毒，即当系统被病毒感染后才由软件进行杀毒，适合于个人用户；后者属于事前的防范，其原理是在网络端口设置一个病毒过滤器，即在系统上安装一个防病毒的网络软件，能够在病毒入侵到系统之前，将其阻挡在外。

其次，认真执行病毒定期清理制度。安装了防病毒软件并不能永远杜绝中病毒事件的发生，还需要对杀毒软件进行实时更新，保证计算机不受新型病毒的侵扰，使计算机始终处于良好的工作状态。

最后，设置控制权限可以将网络系统中易感染病毒的文件的属性、权限加以限制，只允许各终端用户具有只读权限，断绝病毒入侵的渠道，从而达到预防的目的。

6. 应急措施

应急措施是指在计算机灾难事件发生时，利用应急计划、辅助软件和应急设施，排除灾难和故障，保障计算机信息系统继续运行或紧急恢复正常运行。在启动电子商务业务之初，企业就必须制定交易安全计划和应急方案，以防万一。一旦发生意外，企业有备无患，可最大限度地减少损失，尽快恢复系统的正常工作，保证交易的正常进行。

灾难恢复包括许多工作。一方面是硬件的恢复，使计算机系统重新运转起来；另一方面是数据的恢复。一般来说，数据的恢复更为重要，难度也更大。目前运用的数据恢复技术主要是瞬时复制技术、远程磁盘镜像技术和数据库恢复技术。

（三）法律环境保障

电子商务的安全发展必须依靠法律的保障，通过法律条文的形式来保护电子商务信息的安全，惩罚网络犯罪，建立一个良好的电子商务法制环境来约束人们的行为。

目前世界上的电子商务相关法律主要涉及计算机犯罪立法、计算机安全法规、隐私保护、网络知识产权保护、电子合同相关法规等方面，初步满足了电子商务保密性、完整性、可认证性、可控性和抗抵赖性的安全需求。但是，电子商务安全不可能一劳永逸，必须以发展的眼光来看待它，所以进一步的法制建设还应继续进行。

表 2-1 是对我国网络法律现状的总结。

表 2-1　我国网络法律现状总结

序　　号	内容（法律、条例、实施办法等）	部　　门
1	1990 年 9 月 7 日，第七届全国人民代表大会常务委员会第十五次会议通过了《中华人民共和国著作权法》，该法将计算机软件纳入著作权保护范畴	全国人大
2	2000 年 12 月 28 日，第九届全国人民代表大会常务委员会第十九次会议通过了《全国人大常委会关于维护互联网安全的决定》	
3	1991 年 5 月 24 日，国务院颁布了《计算机软件保护条例》（于 2001 年 12 月 28 日修订）	国务院
4	1994 年 2 月 18 日，中华人民共和国国务院令第 147 号发布了《中华人民共和国计算机信息系统安全保护条例》	
5	1996 年 2 月 1 日，中华人民共和国国务院令第 195 号发布了《中华人民共和国计算机信息网络国际联网管理暂行规定》（于 1997 年 5 月 20 日修正）	
6	1999 年 10 月 7 日，国务院发布了《商用密码管理条例》	
7	2000 年 9 月 25 日，国务院公布施行《互联网信息服务管理办法》	
8	2000 年 9 月 25 日，国务院颁布了《中华人民共和国电信条例》	
9	2006 年 5 月 10 日，国务院颁布了《信息网络传播权保护条例》	
10	1989 年，公安部发布了《计算机病毒控制规定（草案）》，开始推行计算机病毒研究和许可证制度	各部委
11	1992 年 4 月 6 日，机械电子工业部发布了《计算机软件著作权登记办法》	
12	1994 年 2 月 18 日，公安部发布了《计算机信息系统安全保护条例》	
13	1996 年 4 月 9 日，邮电部发布《中国公用计算机互联网国际联网管理办法》	
14	1997 年 6 月 3 日，国务院信息化工作领导小组办公室审定了《中国互联网络域名注册实施细则》	
15	1997 年 12 月 8 日，国务院信息化工作领导小组审定了《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》	
16	1997 年 12 月 11 日，公安部发布了《计算机信息网络国际联网安全保护管理办法》	
17	1998 年 2 月 26 日，国家保密局发布了《计算机信息系统保密管理暂行规定》	
18	1998 年 4 月，公安部出台了《计算机信息系统病毒防治管理办法》	
19	1999 年 2 月 24 日，国务院办公厅转发《国家版权局关于不得使用非法复制的计算机软件通知》	

续表

序　　号	内容(法律、条例、实施办法等)	部　　门
20	1999 年 9 月 7 日,信息产业部发布了《电信网间互联管理暂行规定》	各部委
21	2000 年 1 月 1 日,国家保密局发布了《计算机信息系统国际联网保密管理规定》	
22	2000 年 11 月 6 日,国务院新闻办公室、信息产业部联合发布了《互联网站从事登载新闻业务管理暂行规定》	
23	2000 年 11 月 7 日,信息产业部发布了《互联网电子公告服务管理规定》	
24	2001 年 4 月 3 日,信息产业部、公安部、文化部、国家工商行政管理局联合发布了《互联网上网服务营业场所管理办法》	
25	2002 年 2 月,国家版权局发布的《计算机软件著作权登记办法》替代机械电子工业部发布的《计算机软件著作权登记办法》	
26	2002 年 11 月 15 日,信息产业部、公安部、文化部、国家工商行政管理局联合发布修订了 2001 年 4 月颁布的《互联网上网服务营业场所管理条例》	
27	2003 年 7 月 31 日,信息产业部发布了《关于加强我国互联网络域名管理工作的公告》	
28	2004 年 9 月 28 日,信息产业部发布了《中国互联网络域名管理办法》	
29	2005 年 1 月 28 日,信息产业部发布了《电子认证服务管理办法》	
30	2005 年 1 月 28 日,信息产业部发布了《互联网 IP 地址备案管理办法》	
31	2005 年 4 月 1 日,开始实施《中华人民共和国电子签名法》	
32	2006 年 1 月 26 日,银监会发布了《电子银行业务管理办法》	
33	2007 年,中国互联网络信息中心发布了《中国互联网络信息中心域名争议解决办法程序规则》	
34	2009 年 12 月 29 日,工业和信息化部发布了《通信网络安全防护管理办法》	

第二节　电子商务安全面临的问题

电子商务安全面临的问题多种多样,下面主要介绍电子商务网络系统的安全问题、电子商务信息传输的安全问题、电子商务安全管理问题、电子商务法律保障问题以及电子商务客户、商家和银行可能面临的安全问题等。

一、电子商务网络系统的安全问题

(一) 网络系统软件自身的安全问题

网络系统软件自身安全与否直接关系到网络是否安全,网络系统软件的安全功能较少或不全,以及系统设计时的疏忽或考虑不周而留下的“破绽”,都等于给危害网络安全的因素

留下许多“后门”。例如，美国微软公司就经常针对已发现的系统“破绽”发布补丁程序。同时，在同一系统软件中，低版本的往往比高版本的在安全性能方面差了许多，所以在服务器上要注意尽量使用高版本的操作系统，并应使用系统软件所能提供的最高安全级别。值得注意的是，操作系统的许多默认值都已被黑客盯上了，往往被用来作为入侵网络的突破口，所以要尽量避免使用系统默认值。此外，还应注意以下几个问题：

(1) 操作系统的体系结构会造成其本身的不安全性，这也是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的，包括 I/O 的驱动程序与系统服务，都可以用打补丁的方式进行动态连接。

(2) 操作系统的一些功能，如支持在网络上传输文件的功能，包括可以执行文件映像，即在网络上加载程序等，必然会带来一些不安全因素。

(3) 操作系统不安全的另一个原因在于它可以创建进程，甚至支持在网络的结点上进行远程进程的创建与激活，更重要的是被创建的进程可以继承创建进程的权力。这一点与上一点结合起来就构成了在远程服务器上安装“间谍”软件的条件。若再加上把这种间谍软件以打补丁的方式“打”在一个合法的用户上，尤其是“打”在一个特权用户上，系统进程与作业监视程序就都无法监测到这些黑客和间谍软件的存在。

(4) 操作系统在运行时，一些系统进程总在等待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去，这也是黑客可以利用的。

(5) 操作系统要安排无口令入口，这原本是为系统开发人员提供的便捷入口，但它也是黑客的通道。另外，操作系统还有隐蔽信道。

(6) internet 和 intranet 使用的 TCP/IP 及 FTP(文件传输协议)、E-mail(电子邮件)、RPC(远程进程调用)、NFS(网络文件系统)等都包含许多不安全的因素，存在着许多漏洞。

(二) 网络系统中数据库的安全设计问题

网络中的信息数据是存放在计算机数据库中的，供不同的用户来共享。数据库存在着不安全性和危险性。因为在数据库系统中存放着大量重要的信息资源，在用户共享资源时可能会出现以下现象：授权用户超出了他们的访问权限进行更改活动；非法用户绕过安全内核，窃取信息资源等。因此提出了数据库安全问题，也就是要保证数据的安全可靠和正确有效。对数据库数据的保护主要针对数据的安全性、完整性和并发控制 3 个方面。

数据的安全性就是保证数据库数据不被故意破坏和非法存取。数据的完整性是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入或输出而造成无效操作和错误结果。并发控制是指数据库是一个共享资源，在多个用户程序并行地存取数据时，就可能会产生多个用户程序并发地存取同一数据的情况，若不进行并发控制就会使取出和存入的数据不正确，破坏数据库的一致性。所以在数据库设计时，必须考虑到这些问题。通常可采用一系列的安全策略和安全机制，其中主要是解决存取控制问题。可是对数据的存取控制还不足以对数据库用户进行约束，所以还要增加作业授权控制，把作业授权控制结合到安全策略中，并用自主型和强制性的存取控制来处理用户对数据的访问，而作业授权控制是处理用户对作业及作业对数据的访问，这种控制既提供了高可靠性，又提供了应用的灵活性。

根据 2006 年企业策略集团公司(Enterprise Strategy Group)的安全分析师 Eric Ogren

的一项调查，Oracle、微软的 SQL Server 和开源数据库 MySQL 中都存在不同程度的公共弱点和风险。分析结果证明，每一种数据库的保护级别存在很大的差别。Oracle 存在不少于 70 个安全缺陷，MySQL 有 59 个，Sybase 和来自 IBM 的 DB2 分别有 7 个和 4 个，而微软的 SQL Server 则只有两个安全漏洞。集成在 SQL Server 中的安全相关的功能保证了该数据库具有相当低的安全风险。微软的操作系统会在一个安全漏洞被扫描工具发现以前就发现这个安全漏洞，而对于 Oracle 来说，则需要在数据库部署工作完成以后，再通过扫描工具来发现问题所在。

图 2-4 列举了几款较为常用的数据库软件，从左到右依次是：Database、Oracle、Sybase、SQL Server。

图 2-4　较为常用的数据库软件

（三）网络系统的运行安全

运行安全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。电子商务网络系统的运行安全具体由四个部分组成：风险分析、审计跟踪、备份与恢复和应急措施。

1. 风险分析

运行安全中的风险分析，就是要对电子商务网络系统进行人工或自动的风险分析。风险分析主要涉及四个方面的安全功能：

（1）系统设计前的风险分析。通过分析系统固有的脆弱性，旨在发现系统设计前潜在的安全隐患。

（2）系统试运行前的风险分析。根据系统试运行期的运行状态和结果，分析系统的潜在安全隐患，旨在发现系统设计的安全漏洞。

（3）系统运行期的风险分析。提供系统运行记录，跟踪系统状态的变化，分析系统运行期的安全隐患，旨在发现系统运行期间的安全漏洞，并及时通知安全管理员。

（4）系统运行后的风险分析。分析系统运行记录，旨在发现系统的安全隐患，为改进系统的安全性提供分析报告。

2. 审计跟踪

运行安全中的审计跟踪，就是要对电子商务网络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。审计跟踪涉及 3 个方面的安全功能：

（1）记录和跟踪各种系统状态的变化。例如，操作员对系统中的故意入侵行为和违反

系统安全功能行为进行记录。

(2) 实现对各种安全事故的定位，建立整体跟踪网络，如安装摄像头、监控和捕捉各种安全事件。

(3) 保存、维护和管理审计日志，对每日或一定时期内的审计日志进行整理、备案。

3. 备份与恢复

运行安全中的备份与恢复，就是要提供对系统设备和系统数据的备份与恢复。对系统数据进行备份和恢复所使用的介质可以是磁介质、纸介质、光盘等。备份与恢复主要涉及三个方面的安全功能：

(1) 提供场点内高速度、大容量、自动的数据存储、备份和恢复。

(2) 提供场点外的数据存储、备份和恢复，如通过专用安全记录存储设施对系统内的主要数据进行备份。

(3) 提供对系统设备的备份。

4. 应急措施

运行安全中的应急措施，是要提供在紧急事件或安全事故发生时，保障电子商务网络系统继续运行或紧急恢复所需要的策略。应急措施包括应急计划辅助软件和应急设施两个方面。

(1) 应急计划辅助软件。应急计划辅助软件是指在紧急状态下，使系统能够尽量完成原定任务的计划的辅助性软件。它主要包括三个方面的功能：紧急事件或安全事故发生时的影响分析、应急计划的概要设计或详细制定、应急计划的测试与完善。

(2) 应急设施。应急设施主要是提供紧急事件或安全事故发生时，电子商务网络系统实施应急计划所需要的设施。它主要提供两个方面的安全功能：提供实时应急设施，实现应急计划，保障电子商务网络系统的正常安全运行；提供非实时应急设施，实现应急计划。实时应急设施、非实时应急设施的区别主要表现在对紧急事件发生时的响应时间的长短上。

二、电子商务信息传输的安全问题

尽管在同轴电缆、微波或卫星通信中要窃听其中指定一路的信息是很困难的，但是从安全的角度来说，没有绝对安全的通信线路。同时，无论采用何种传输线路，当线路的通信质量不好时，将直接影响联网效果，严重时甚至导致网络中断。例如，市内电话线路的主要电气指标有直流电气性能指标(环阻、绝缘电阻)、交流特性(线路衰耗、线路衰耗交流频率特征)、交流特性阻抗等。当通信线路中断时，计算机网络也就中断，并且比较明显。而当线路时通时断、线路衰耗大或杂音严重时，中断的问题就不那么明显，但是对通信网线路的影响相当大，可能会严重地危害通信数据的完整性。为保证良好的通信质量和网络效果，就必须要有合格的传输线路，如在干线电缆中，应尽量挑选最好的线作为计算机联网专线，以得到最佳的效果。

图 2-5 为几种典型的计算机网络结构，其中各个方形和圆形之间的连线代表的就是网络传输线路。一旦传输线路出现问题，信息就可能被窃取。

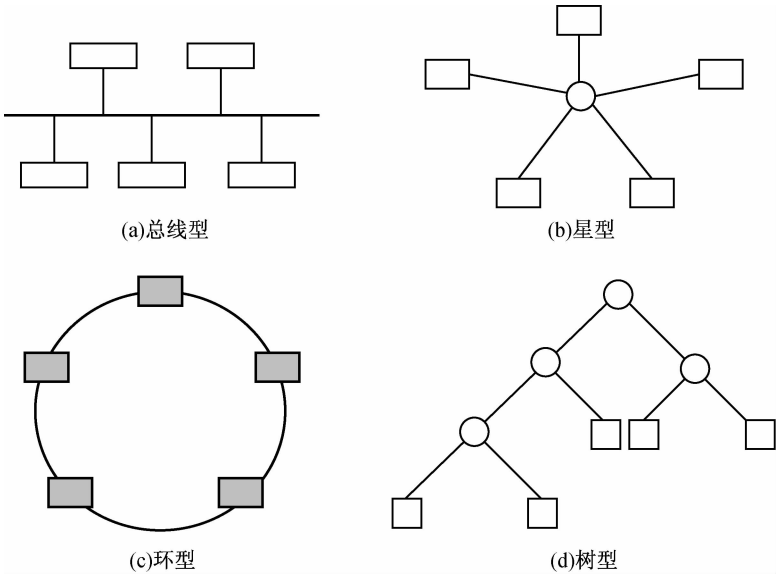

图 2-5　典型的计算机网络结构

三、电子商务安全管理问题

一方面，从加强安全管理的角度出发，可以认为，网络安全实质上首先是管理问题，然后才是技术问题。用户也许花了不少钱购买了安全设备，但如果将它束之高阁，或不按它的安全规范合理操作，认为有了安全设备就会安全，而没在落实上下工夫，那么再好的设备也不能保证安全。世界上现有的信息系统绝大多数都缺少安全管理员，缺少信息系统安全管理的技术规范，缺少定期的安全测试与检查，更缺少安全审计。我国许多企业的信息系统已经使用了多年，但计算机系统管理员与用户的注册大多还是处于默认状态。

另一方面，也可以说网络的安全问题是天生的，这是由于“整体大于部分之和”。网络由各种服务器、工作站、终端等群集组成，所以整个网络自然地继承了它们各自的安全隐患。不同服务器各自运行着不同的操作系统，各自继承着自身系统的不同安全特性。随着计算机及通信设备组件数目的增加，积累起来的安全问题将十分复杂。

这意味着必须制定一个组织内部有效的安全管理策略。例如，公司的信息应当由管理者们作出决策，确定哪些信息是可共享的；哪些信息是内部机密，不得泄露，以免对公司利益造成损害。

通常安全管理领域涉及两类要求：一类是安全管理，防止未授权者访问网络；另一类是管理安全，防止未授权者访问网络管理系统。尽管这两种要求都十分重要，但该领域被认为不如故障管理、配置管理和性能管理那样迫切。随着计算机网络应用的深入，网络覆盖面越来越广，甚至有些网络已成为全球网络。网络上信息的安全性越来越重要，网络安全管理也将成为网络管理中的重要内容。

安全管理必须解决下列基本问题：需要保护的对象、需要保护的原因、保护的方法、采取保护措施的方法、实施保护的地点。显然，上述问题有的涉及实现技术，而有的是管理者的决策。另外，安全性和使用方便性又是一对矛盾体，两者不可兼得。强调了安全性，使用方

便性就会受影响；强调了使用方便性，则安全性可能减弱，这也需要管理者作出决策。

国际标准化组织把网络管理划分为五个领域，分别是故障、性能、配置、记账和安全。故障管理负责检测或发现异常的网络运转，隔离并控制网络问题。性能管理负责分析网络出错率及网络吞吐率，以建立合理、优化的网络运行状态。配置管理负责检测物理的和逻辑的配置，了解和控制网络状态。记账管理负责收集、处理资源和利用数据。安全管理负责控制各种对网络的访问。

另外，对网络运行的环境、操作人员的管理也是网络安全管理的重要方面。不得不正视这样一个事实，网络用户大多数不具备计算机的专业知识，他们只是将计算机视为一个工具。由于他们缺乏安全操作的常识或对安全不够重视，所以在安全操作方面的失误往往会造成对网络的侵害，如将上网口令设置为自己或亲朋的姓名、生日、出生地等容易被猜到的信息，或者将口令随意标在机器上、机器旁的纸片上及自己的记事簿上或贴在机房里。再如，有许多用户完成一天的工作后，往往不会将工作站的机箱上锁，不会注意在使用间歇（如临时会友、吃饭等）将系统关闭。当一个系统未关闭而被非法用户侵入时，它的全部权力和钥匙将被毫无保留地非法盗用。目前，人员管理常常是电子商务安全管理上最薄弱的环节。近年来，我国计算机犯罪大都呈现内部犯罪的趋势，其主要原因就是部分工作人员职业道德修养不高、安全教育和管理松懈。

四、电子商务法律保障问题

1. 我国互联网安全的法律保障

电子商务的技术设计是先进的、超前的，而且具有强大的生命力。但同时也必须清楚地认识到，在目前我国的法律上是很少有现成的条文来保护电子商务交易中的交易方式的，在网上交易可能会承担由于法律滞后而造成的安全风险。电子商务属于互联网范畴，而我国的互联网相关法律尚不成熟。

从目前的互联网法律保障现状来看，主要存在以下几个问题：

（1）层级方面。目前我国网络立法力度不够，大多停留在部门规章的层面上，多为“管理办法”、“管理条例”或“解释”等，而全国人大、国务院层面上的网络立法还很薄弱，缺乏一部关于计算机网络安全的根本大法。就我国现行的网络虚拟空间来说，只有一些相应的行政规章来加以规范和调整。而且各个部门颁布的实行办法等多有重叠，实施起来较为困难，容易出现漏洞。严格意义上的网络法律，我国现在还没有颁布，这就使用户面对日益增多的互联网纠纷束手无策。

随着网络实践的不断深入，网络逐渐融入人们的生活，成为社会关系必须调整的一部分。在不久的将来，一部完整的规范网络的法律一定会呈现在人们面前。

（2）内容方面。我国网络立法具有很强的滞后性，所涉及的内容多为信息系统与网络安全，在网络使用上的立法规范还有许多空白。与美国、日本等发达国家相比较，我国的网络立法在具体性、细分性、针对性等方面都有待提高。

资料链接 2-1

日本的电子商务法律体系

日本在进行电子商务法律环境建设的过程中，效仿《欧盟电子商务倡议》和《全球电

子商务框架》，于 2001 年 1 月施行《高度信息通讯网络社会形成基本法》，明确规定国家发展电子商务的立法制策义务，并以此为纲领性法律构筑电子商务综合法律体系，基本解决了制约电子商务发展的法律“瓶颈”问题。为解决电子合同问题和消费者权益保护问题，日本出台了《关于电子消费者合同以及电子承诺通知的民法特例的法律》，修改了《关于访问销售等法律（关于特定商业交易的法律）以及分期付款销售法的法律》两次，修改了《特定商业交易法》一次。《个人信息保护法》虽于 2001 年提交国会审议，但至今尚未通过。为处理电子签章及 CA 认证问题，日本出台了关于电子签名及认证业务的法律，修改了《商业登记法》、《公证人法》和《民法》等，并于战略高度颁布《电子签名法》，且与欧盟、美国基本保持一致。为保证电子证据、电子文件及网上商事行为的合法性，日本出台了《关于基于修改商法等部分内容的法律之施行而调整、完善相关法律的法律》、《为关于书面交付等的信息通讯技术的利用，关于相关法律的整备的法律（IT 书面资料总括法）》等，修改了《证券交易法以及金融期货交易法》和《商法》等。为防范不正当竞争和网络犯罪，日本两次修改了《不正当竞争防止法》，出台了《不正当接入禁止法》，并在 2001 年对其《刑法》进行了修改。为保护知识产权，日本又对《著作权法》、《专利法》、《实用新型法》、《外观设计法》和《商标法》等进行了修改。

日本电子商务法律体系是比较成熟的，既有纲领性法律对电子商务立法义务作出法律规定，又有细节方面的法律和法令，并对所有涉及电子商务的法律进行了全方位、大规模的修改。表 2-2 为中日两国电子商务法律体系的对比。

表 2-2　中日两国电子商务法律体系的对比

类　　别	中　　国	日　　本
纲领性法律	无	《高度信息通讯网络社会形成基本法》
电子合同问题	新《合同法》中有三点涉及电子商务合同	《关于电子消费者合同及电子承诺通知的民法特例的法律》，修改了《关于访问销售等法律（关于特定商业交易的法律）以及分期付款销售法的法律》
电子签章或署名问题	《电子签名法》	《电子签名与认证服务法》、《电子签名法》，修改了《商业登记法》、《公证人法》、《民法》
电子认证问题	《电子认证服务管理办法》	
电子交易问题	《电子支付指引（第一号）》	无
电子证据及文件的合法性问题	无	《关于基于修改商法等部分内容的法律之施行而调整、完善相关法律的法律》、《为关于书面交付等的信息通讯技术的利用，关于相关法律的整备的法律（IT 书面资料总括法）》，修改了《证券交易法以及金融期货交易法》

续表

类　别	中　国	日　本
网上商事行为的合法性问题	《北京市工商行政管理局网上经营行为备案的通告》	修改了商法(包括《商法典》、《有限公司法》、《关于股份公司监察的商法典特例法》等六部法律)
网络广告问题	《关于对网络广告经营资格进行规范的通告》	修改了《特定商业交易法》
消费者权益保护问题	修改了《消费者权益保护法》	2001年修改了《关于访问销售等法律(关于特定商业交易的法律)以及分期付款销售法的法律(修改)》,2002年修改了《特定商业交易法》
网络犯罪问题	修改了《刑法》	《不正当接入禁止法》,2001年对《日本刑法》进行了修改
个人信息保护问题	无	《个人信息保护法》
知识产权问题	无	修改了《著作权法》、《专利法》、《实用新型法》、《外观设计法》和《商标法》
反不正当竞争问题	修改了《反不正当竞争法》	两次修改了《不正当竞争防止法》

(3) 效力方面。目前我国网络立法集中在部门层级,针对本行业或本领域在计算机网络中的安全与使用问题,虽然在某种程度上对规范网络行为起到了积极的作用,但存在各自为政、交叉重复、资源浪费等弊病。这些规章条文比较简单,导致其效力低、重复性大、可操作性差,容易造成"有办法,没实际"的现状。

不仅如此,我国的互联网法律,尤其是电子商务领域,与网络立法先进的国家相比较,还有许多方面的空白,如缺乏对计算机数据、网络广告、电子签名和电子商务、隐私权保护、网络游戏(如虚拟财产)、垃圾邮件等的保护和规范。

典型案例 2-5

《魔兽世界》终止审批事件

2009年末暴雪公司出版的、网易负责日常运营的网络游戏《魔兽世界》被认定不符合有关规定,受到新闻出版总署终止审批,退回引进的通告。《魔兽世界》作为全球规模最大的网络游戏,同其他网络游戏一样采用的是一种需要玩家付费才能进行游戏的模式。其中,付费可以采用网络付费、购买游戏点卡等方式,进入游戏需要账号绑定,输入密码、游戏卡号等操作,这与电子商务的模式相似。新闻出版总署依照2009年9月28日颁布的《关于贯彻落实国务院〈"三定"规定〉和中央编办有关解释,进一步加强网络游

戏前置审批和进口网络游戏审批管理的通知》认定《魔兽世界》存在多项违规，其中包括未通过前置审批等。但随后文化部又发表声明，称新闻出版总署发布的终止网易《魔兽世界》审批通知，是不符合“三定”规定的，明显属于越权行为。总体来说，新闻出版总署以严重违反规定为由，要求网易停止运营《魔兽世界》；但网易因为游戏已经得到文化部的批准而没有执行。这一事件导致《魔兽世界》的运营受到了影响（具体是公测受到了影响），暴露了我国在网络运营管理方面的不足。

2. 我国电子商务安全的法律保障

2000 年 3 月 5 日，在九届人大三次会议上，上海代表团张仲礼代表提出的“呼吁制定电子商务法”议案，成为此次会议产生的第一号议案。这份议案指出，全球化信息浪潮正迅猛推进，电子商务作为一种更快捷、准确的交易形式，也在中国全面开展。目前亟需为电子商务的发展创造适宜的法律环境，建立安全便捷的电子付款系统法律规范。

但到目前为止，在国家立法层面上，直接针对电子商务的法律，在全国人大通过的只有于 2005 年 4 月 1 日起实施的《中华人民共和国电子签名法》。由于我国还没有制定专门的关于电子商务的法律法规，有关电子商务行业的管理和规范，主要依靠国务院和各部委出台的行政法规、地方性法规、实施办法等。国内城市中，仅有广州、上海等地出台立法对电子商务进行监管。上海从 2009 年 3 月 1 日起开始实施《上海市促进电子商务发展规定》，明确了电子商务企业的法律地位，同时对其权利与义务作了明确交代。但由于网上交易大都跨地区完成，地方上的行政法规对跨区域消费者的侵权行为的约束力非常有限。由此可见，目前已有的电子商务法律法规中以部门规章和地方法规为多数，国家法规较少，法律更少，并且这些部门规章和地方法规的效力较低，直接造成了其使用范围和力度的不足。

在 2010 年 3 月的全国人民代表大会上，全国人大代表、中国移动通信集团广东有限公司总经理徐龙向大会提交了一份关于制定电子商务法的议案。徐龙介绍说，从国际上看，许多国家和地区都把推进电子商务作为增强国家竞争力、赢得全球资源配置优势的战略举措，并相继制定了一系列法律法规，通过法律制度来保障和促进电子商务的发展。联合国国际贸易法委员会 2001 年 3 月通过《电子签字示范法》、2005 年 11 月通过《联合国国际合同使用电子通信公约》，为各国及地区电子商务立法提供了一整套国际通行的电子商务规则。目前，国际上已经有 30 多个国家和地区制定了综合性电子商务法，如新加坡《电子商务法》（1998 年）、美国《统一电子商务法》（1999 年）、加拿大《统一电子商务法》（1999 年）、韩国《电子商务基本法》（1999 年）、澳大利亚《电子交易法》（1999 年）等。

有代表委员指出，我国电子商务的相关法律法规内容应包括立法宗旨、电子商务概念、基本原则、交易主体、电子合同、电子签名及认证、电子支付、信用保障、交易安全、个人信息保护、消费者权益保护、知识产权保护、电子商务税收、行业自律、争端解决机制、法律责任等内容。全国政协委员贺强提出的关于《规范和发展电子支付服务产业》的提案，指出了电子支付带动了社会资金效率的提升，但我国电子支付产业的既有问题亟需相关支持政策和法规的建立与完善，以保障和促进电子支付产业的科学发展，引导和规范电子支付企业的经营

活动。全国政协委员朱奕龙也建议，国家应尽快建立网络商品交易法律法规，对从事网上交易的个人（企业）、网上商店，实施注册登记管理并责其依法缴税。

五、电子商务客户、商家和银行可能面临的安全问题

（一）总体安全问题

对于客户、商家和银行来说，一旦电子商务安全得不到保证，就可能遇到以下问题。

1. 系统的中断

系统的中断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、恶意攻击等都能导致系统不能正常工作，因而要对由此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。

2. 信息的截获和窃取

信息的截获和窃取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复制、电话线上的窃取、以太网上对数据包的嗅探等。

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，攻击者就可能通过互联网、公共电话网、搭线、在电磁波辐射范围内安装截收装置或在数据包通过的网关和路由器上截获数据等方式，获取传输的商业机密；也可能通过对信息流量和流向、通信频度和长度等参数的分析，推断出有用信息，如消费者的银行账号、密码以及企业的商业机密等。

3. 信息的篡改

信息的篡改是针对完整性进行的攻击。如果非授权实体不但存取了资源，还对它进行了修改，则这种攻击就变为篡改。例如，某人可能修改数据库中的数值，修改程序使之完成额外的任务或修改正在传送中的数据，甚至可能对硬件进行修改。

电子商务简化了贸易过程，减少了人为因素的干预，同时也带来维护贸易各方商业信息，如电子支票的完整、一致的问题。当攻击者熟悉了网络信息格式以后，通过各种技术方法和手段对网络传输的信息进行中途修改，并发往目的地，从而破坏信息的完整性。这种破坏手段主要有三个方面：一是篡改，指更改信息的内容，如购买商品的出货地址；二是删除，指删除某个消息或消息的某些部分；三是插入，指在消息中插入一些信息，让接收方读不懂或接收错误的信息。

4. 信息的伪造

信息的伪造是针对身份认证机制进行的攻击。在这类攻击中，非授权实体伪造计算机系统中的实体或信息。

电子商务是直接关系到贸易双方或多方的商业交易，如何确定网上的远程交易方正是

所期望的贸易方，即如何进行有效身份认证，是保证电子商务顺利进行的关键。当攻击者掌握了网络信息数据规律或解密了商务信息后，可以假冒合法用户或发送假冒信息来欺骗其他用户，主要有两种方式：一种是伪造电子邮件，虚开网站和商店，给用户发电子邮件，收订货单；伪造大量用户，发电子邮件，穷尽商家资源，使合法用户不能正常访问网络资源，使有严格时间要求的服务不能及时得到响应；伪造用户，发电子邮件，窃取商家的商品信息和用户信息等。另一种是假冒他人身份，如冒充领导发布命令、调阅密件；冒充他人消费；冒充主机欺骗合法主机及合法用户；冒充网络控制程序，套取或修改使用权限、通行字、密钥等信息，接管合法用户，欺骗系统，占用合法用户的资源等。

5. 交易抵赖

当贸易一方发现交易行为对自己不利时，或被利益刺激到一定程度时，就有可能否认电子交易行为。交易抵赖包括多个方面，如发信者事后否认曾经发送过某条信息或内容，收信者事后否认曾经收到过某条消息或内容，购买者发了订货单不承认，商家卖出的商品因价格差而不承认原有的交易等。

（二）具体安全问题

下面分别就客户、商家和银行的实际情况进行介绍。

1. 客户可能面临的安全问题

（1）虚假订单。假冒者可能会用另一个客户的名字来订购商品，而且有可能收到商品，而被假冒的客户却被要求付款或返还商品。

（2）付款后收不到商品。这往往是一种商家欺骗客户的行为。

（3）机密性丧失。客户可能将秘密的个人数据或自己的身份数据（如登录密码等）发送给冒名为销售商的机构，同时，这些信息在传递的过程中也有受到窃听的可能性。

（4）拒绝服务。攻击者可能向销售商的服务器发送大量的虚假订单来挤占它的资源，从而使合法的用户得不到正常的服务。

2. 商家可能面临的安全问题

（1）中央系统安全性被破坏，入侵者假冒成合法用户来改变用户数据（如商品送达地址）、解除用户订单或生成虚假订单。

（2）竞争者检索商品的销售情况。恶意的竞争者会以他人名义来订购商品，从而了解商家有关商品的递送状况和货物的库存情况。

（3）客户资料被竞争者获悉。

（4）被他人冒名而损害企业的名誉。

（5）消费者提交订单后不付款。

（6）商家的个人或集体信息遭到泄露，或者商业机密遭到泄露。

3. 银行可能面临的安全问题

电子商务活动中的安全风险，还有很大一部分来自于攻击者对银行专用网络的破坏。

攻击者破坏银行专用网络所采用的手段大致有以下四类：

（1）中断（攻击系统的可用性），破坏银行专用网络系统中的硬件、线路、文件系统等，使系统不能正常工作。

（2）窃听（攻击系统的机密性），通过搭线与电磁泄漏等手段造成泄密，或对银行专用网络中的业务流量进行分析，获取有用情报。

（3）篡改（攻击系统的完整性），篡改银行专用网络中的数据内容，修改消息次序、时间（延时和重放）等。

（4）伪造（攻击系统的真实性），将伪造的虚假消息输入银行专用网络，冒名合法人员介入银行专用网络，重放截获的合法消息以实现非法目的，否认消息的接收和发送等。

引例解析

首先，袭击者用数以亿万计的垃圾邮件猛烈攻击目标网站，导致该网站网络堵塞，最终因不堪重负而彻底瘫痪，从而使世界各地的用户都无法登录该网站。其次，袭击者似乎分布在世界各地，因为这些垃圾邮件是从世界各地的多个互联网连接点发出来的。以雅虎网站遭袭击为例，当时互联网50处不同的结点一起向雅虎发起袭击，袭击者们显然是经过严密协调的。美国一家互联网公司的经理列维不无担忧地说："如果连世界头号网站雅虎都避免不了瘫痪的结局的话，那么其他网站对于神秘袭击者来说更是小菜一碟了。"

专门跟踪全世界网络运行情况的美国硅谷的Keynote系统公司公务服务部总管唐·托德感叹地说："雅虎是互联网世界最可靠的网站之一，因此，这次袭击事件给所有依靠互联网开展电子商务的人都提了一个醒，就连最可靠的网站也可能遭受袭击、中断服务。依我看，这次袭击事件还给我们这么一个警示，不管你事先准备得多么完善，不管你有多少套应急方案，不管你系统设计得多么完美，都仍有可能因遭到攻击而出错。"

雅虎公司的发言人也坦言："我们以前也碰到过类似的袭击事件，但由于袭击的规模要小得多，所以公司的技术人员只需稍稍修改一下数据进出路径，就能避免网络瘫痪，但这次袭击却是一次非常非常严重的网络袭击，袭击者来自如此之多的地点，时间如此的协调一致，以至于打了雅虎公司一个措手不及，所以我们当时确实无法阻止袭击。不幸的是，我们还无法保证将来就再也不会发生类似的袭击事件。我们可以给自己的网站安装邮件过滤器，但这些黑客却能想方设法绕过过滤器。所以谁也无法保证100%解决这道难题。这不能不让人感到遗憾！"

由此可见，人们必须从电子商务的网络系统、信息传输、安全管理、法律保障等各个方面着眼，结合电子商务客户、商家和银行可能面临的安全问题，从整体上提高电子商务安全等级，提高我们的虚拟安全性。

本章小结

本章主要是对电子商务安全进行简单的叙述，介绍了电子商务安全的概念，其主要内容有电子商务安全的含义、要求、体系结构等；同时还介绍了电子商务安全所面临的各种问题，包括网络系统的安全问题、信息传输的安全问题、安全管理问题、法律保障问题。最后分别分析了电子商务客户、商家和银行可能面临的安全问题。

综合训练

一、思考练习

1. 简述电子商务安全的含义。
2. 简述电子商务安全的要求及其体系结构。
3. 电子商务安全都面临着哪些问题？
4. 电子商务网络系统存在哪些安全问题？
5. 简述电子商务客户、商家和银行可能面临的安全问题。

二、案例分析

身边的电子商务安全

随着网络技术的发展，电子商务逐步成为了人们身边不可缺少的一种活动形式。但电子商务的安全问题一直是个困扰大家的难题。于是，人们经常会遇到下面两种情景：

情景一：王先生在某次通过亚马逊网站购物后，收到了这样的电子邮件："您被收取了免费送货的费用，我们对这个错误表示遗憾，并对由此给您带来的任何不便表示道歉。我们会把向您收取的送货费全部返还给您。"亚马逊公司发言人 Patty Smith 说，该公司在发现系统出现错误后，陆续通知了受影响的顾客，并保证把资金退还到用户的信用卡上。用户下次使用信用卡时会发现资金已经返还了。这位发言人说，受这个问题影响的只涉及 2005 年 9 月 20 日至 24 日期间在亚马逊网站订货的一部分要求免费送货或者使用礼品证书的顾客。Patty Smith 还说，发生这个问题的原因是"系统故障"，这个故障现在已经修复。虽说这次购物经历有惊无险，但给王先生的网络购物之行蒙上了一层挥之不去的阴影。

情景二：银行卡上的工资到账之后，公司的员工张先生第一时间通过网上银行确认工资总额，而同一办公室的李小姐和刘小姐对于网上银行的使用却抱着迟疑的态度。

李小姐表示由于对安全存疑，坚决不使用网上银行；刘小姐试图注册网上银行时，因为注册密码必须都是数字而停止，她认为都是数字的密码非常不可靠。所以，她们都是选择下班后到 ATM 上查询。

问题

1. 情景一和情景二分别说明了哪些问题？

2. 面对当前网络的安全性，电子商务还安全吗？请谈谈你自己的看法。

认识电子商务安全

【实训目标】

了解电子商务安全的基本常识及其相关知识，正确理解电子商务安全的重要性以及电子商务安全所面临的问题。

【实训环境】

一个连接互联网的机房，机器设备数量保证上课班级的学生每人一台。

【实训内容】

（1）查找5个以上的专业电子商务网站，并搜索有关电子商务安全的基本概念。

（2）查找当前国际和国内电子商务安全技术的发展状况的文章，阅读并总结。

（3）结合你的电子商务经验，找到电子商务发展中存在的安全问题。

（4）描述你进行电子商务过程中遇到安全问题时的解决方法。

（5）查找电子商务安全对策。

（6）查找《中华人民共和国电子签名法》的内容，并分析该法所涉及的技术问题，体会它被称为我国第一部“真正意义上的信息化法律”的含义。

（7）查找现有的电子商务安全方法及其效果说明。

（8）课堂讨论，发表自己的意见，就电子商务安全提出自己的创新观点。

第三章
电子商务安全技术

知识目标

- 学习并了解常用的电子商务安全技术；
- 掌握电子数据交换技术；
- 掌握认证技术；
- 掌握虚拟专用网技术；
- 了解基于生物特征的身份认证技术。

技能目标

- 了解电子商务常用的加密技术，并掌握其应用方法；
- 了解电子商务常用的防火墙技术，并掌握其应用方法。

引例

《中华人民共和国电子签名法》首次用于庭审

北京市民杨某状告韩某借钱不还，并将自己的手机交给法庭，以手机短信作为韩某借钱的证据。但手机短信能否成为法庭认定事实的依据？2005 年 6 月 3 日，海淀法院 3 名法官合议审理了这起《中华人民共和国电子签名法》(以下简称《电子签名法》)出台后的第一案。

2004 年 1 月，杨先生结识了女孩韩某。同年 8 月 27 日，韩某发短信给杨先生，向他借钱应急，短信的内容是：我需要 5 000 元，刚回北京做了眼睛手术，不能出门，你汇到我卡里。杨先生随即将钱汇给了韩某。一个多星期后，杨先生再次收到韩某的短信，又借给韩某 6 000 元。因都是短信来往，两次汇款杨先生都没有索要借据。此后，因韩某一直没提过借款的事，而且再次向杨先生借款，杨先生产生了警惕，于是向韩某催要。但一直索要未果，于是起诉至海淀法院，要求韩某归还其 11 000 元，并提交了银行汇款单存单两张。但韩某却称这是杨先生归还以前欠她的欠款。

为此，在庭审中，杨先生在向法院提交的证据中，除了提供银行汇款单存单两张外，还提交了自己使用的号码为 1391166×××× 的飞利浦移动电话一部，其中记载了部分短信息内容。例如，2004 年 8 月 27 日 15:05 的“那就借点资金援助吧”，2004 年 8 月 27 日 15:13 的“你怎么这么实在！我需要 5 000 元，这个数不大也不小，另外我昨天刚回北京做了个眼睛手术，现在根本出不了门口，见人都没法见，你要是资助就得汇到我卡里！”等韩某发来的 18 条短信内容。

韩某的代理人在听完短信内容后，否认发送短信的手机号码属于韩某，并质疑短信的真实。法官提醒他，在前次开庭时，法官曾当着双方的面拨打了该手机号码，接听者正是韩某本人。韩某也承认，自己从 2004 年七八月份开始使用这个手机号码。

法院经审理认为，依据《最高人民法院关于民事诉讼证据的若干规定》中的关于承认的相关规定，1391173×××× 的移动电话号码是否由韩女士使用，韩女士在第一次庭审中已明确表示承认，故法院确认该号码系韩女士使用。

依据 2005 年 4 月 1 日起施行的《电子签名法》中的规定：电子签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。数据电文是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。移动电话短信息即符合电子签名、数据电文的形式。同时，移动电话短信息能够有效地表现所载内容并可供随时调取查用，能够识别数据电文的发件人、收件人以及发送、接收的时间。经法院对杨先生提供的移动电话短信息生成、储存、传递数据电文方法的可靠性，保持内容完整性方法的可靠性，用以鉴别发件人方法的可靠性进行审查，可以认定该移动电话短信息内容作为证据的真实性。根据证据规则的相关规定，录音、录像及数据电文可以作为证据使用，但数据电文可以直接作为认定事实的证据，还应有其他书面证据相佐证。

从韩女士向杨先生发送的移动电话短信息内容中可以看出:2004年8月27日韩女士提出借款5 000元的请求并要求杨先生将款项汇入其卡中,2004年8月29日韩女士向杨先生询问款项是否存入,2004年8月29日中国工商银行个人业务凭证中显示杨先生给韩女士汇款5 000元;2004年9月7日韩女士提出借款6 000元的请求,2004年9月8日韩女士向杨先生询问款项是否汇入,2004年9月8日中国工商银行个人业务凭证中显示杨先生给韩女士汇款6 000元。2004年9月15日至2005年1月韩女士屡次向杨先生承诺还款。

杨先生提供的通过韩女士使用的号码发送的移动电话短信息内容中载明的款项往来金额、时间与中国工商银行个人业务凭证中体现的杨先生给韩女士汇款的金额、时间相符,且移动电话短信息内容中亦载明了韩女士偿还借款的意思表示,两份证据之间相互印证,可以认定韩女士向杨先生借款的事实。据此,杨先生所提供的手机短信息可以认定为真实有效的证据,证明事实真相,法院对此予以采纳,对杨先生要求韩女士偿还借款的诉讼请求予以支持。在本案中,涉及哪些电子商务安全技术?它们在本案中的作用又是什么?这些将在本章予以解释。

电子商务安全技术指的是为保障电子商务安全所采用的一些计算机网络技术,在此主要介绍电子数据交换技术、密码技术、认证技术、虚拟专用网技术、防火墙技术以及较前沿的基于生物特征的身份认证技术。

第一节　电子数据交换技术

20世纪80年代,随着贸易全球化的加深,传统的贸易单证、纸张合同的使用量激增。这不仅意味着大量的人力、物力的投入,也使得错误率增加,商业效率降低。在这样的背景下,电子数据交换技术应运而生。本节重点介绍电子数据交换技术的概念、系统构成及其安全策略和具体措施。

一、电子数据交换技术概述

1. 电子数据交换技术的概念

电子数据交换(electronic data interchange,EDI)技术是信息技术向商贸领域渗透并与国际商贸实务相结合的产物。相对于目前通用的电子商务,EDI技术的出现是由初期电子商务到现代电子商务的承前启后的重要阶段,是由“商务电子化”向“电子化商务”演变过程中产生质变的关键一环。可以说,EDI技术见证了电子商务的崛起。EDI技术的发展至少经历了40年,其发展和演变的过程已经充分显示了商业领域对其重视程度。人们将使用EDI技术的贸易称为“无纸贸易”,将电子转账称为“无纸付款”,这已经足以看出EDI技术对商业运作的影响。

追溯EDI的历史,它最早出现于20世纪60年代末,当时欧洲和美国几乎同时提出了

EDI 的概念。早期的 EDI 只是在两个商业伙伴之间，依靠计算机与计算机直接通信完成。EDI 最初是来自于电子商业单据交换（electronic business document exchange，EBDE）。其最基本的商业意义在于由计算机自动生成商业单据（如订单、发票等），然后通过电信网络传输给商业伙伴。这里的商业伙伴是指广义上的商业伙伴，它可以是任何公司、政府机构及其他商业或非商业机构，只要它们与企业保持经常性的、带有结构性的数据交换。EDI 的好处体现在：节省时间、节省费用、减少错误、减少库存、改善现金流动等方面。20 世纪 70 年代，数字通信技术的发展大大加快了 EDI 技术的成熟，同时扩大了其应用范围，也带动了跨行业 EDI 系统的出现。20 世纪 80 年代，EDI 标准的国际化又使 EDI 的应用跃入了一个新的里程。

由于实施 EDI 的基本目的就是通过第三方的增值服务，用电子数据交换代替商业纸质单证的交换，而这是建立在信息标准化的基础上的，因此 EDI 的发展历史实际上就是商业数据的标准化和增值网络服务商的发展过程。在 EDI 的发展历史中，真正推进其发展的是那些独立的 EDI 网络增值服务商。特别是 20 世纪 80 年代以来，西方各国电信政策逐步放宽，私营网络增值服务商的出现使 EDI 开始向商业化的方向发展。

对于 EDI 的概念，由于各个领域应用 EDI 技术所要达到的目的不同，所以 EDI 的定义很难统一，下面列举出的是美国国家标准局 EDI 标准委员会和联合国标准化组织对 EDI 的定义：

（1）美国国家标准局 EDI 标准委员会对 EDI 的解释是：EDI 指的是在相互独立的组织机构之间所进行的标准格式、非模糊的具有商业或战略意义的信息的传输。

（2）联合国标准化组织将 EDI 描述成，按照统一标准将商业或行政事务处理转换成结构化的事务处理或报文数据格式，并借助计算机网络实现的一种数据电子传输方法。

由此可以总结出 EDI 的含义：EDI 是商业伙伴之间，将按标准、协议规范化和格式化的经济信息通过电子数据网络，在单位的计算机系统之间进行自动交换和处理。EDI 是电子商务贸易的一种工具，将商业文件（如订单、发票、发货单、报关单和进出口许可证）按统一的标准编制成计算机能识别和处理的数据格式，在计算机之间进行传输。EDI 的基本运作方式如图 3-1 所示。

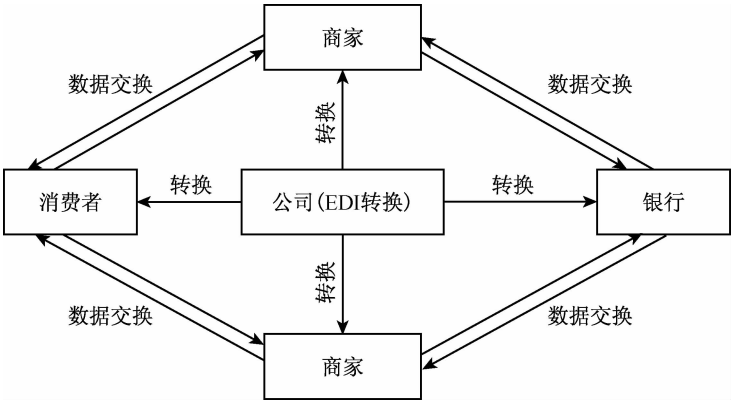

图 3-1　EDI 的基本运作方式

2. EDI 的有关标准

标准化的工作是实现 EDI 互通和互连的前提和基础。EDI 的标准主要包括 EDI 网络通信标准、EDI 处理标准、EDI 联系标准和 EDI 语义语法标准。

(1) EDI 网络通信标准是要解决 EDI 通信网络应该建立在何种通信网络协议之上,以保证各类 EDI 用户系统的互连问题的标准。目前国际上主要采用 MHX(X.400)[①]作为 EDI 通信网络协议,以解决 EDI 的支撑环境。

(2) EDI 处理标准是要研究那些不同地域、不同行业的各种 EDI 报文,是相互共有的"公共元素报文"的处理标准。它与数据库、管理信息系统(如 MPRⅡ)等接口有关。

(3) EDI 联系标准是要解决 EDI 用户所属的其他信息管理系统或数据库与 EDI 之间的接口问题的标准。

(4) EDI 语义语法标准(又称 EDI 报文标准)规定了各种报文类型格式、数据元编码、字符集和语法规则以及报表生成应用程序设计语言等。EDI 语义语法标准是 EDI 技术的核心。

3. EDI 面临的威胁

网络系统运行后往往会遇到许多安全威胁,EDI 系统也不例外。这些威胁可以根据来源和动机分为不同的种类。根据来源不同,这些威胁可分为内部和外部两种。其中,内部威胁是指系统的合法用户以故意或非法方式进行操作所产生的威胁,如内部工作人员利用工作之便或者软件固有缺陷,非法使用 EDI 资源或越权存取数据;外部威胁泛指搭线窃听、截取交换信息、冒充合法用户等。根据动机不同,这些威胁可分为偶发性威胁和故意性威胁。其中,偶发性威胁是指偶然发生的、不带任何预谋的威胁,如系统故障、操作失误、软件出错或其他不可抗自然力;故意性威胁是指那些人为的、有预谋或动机的威胁,往往伴有网络攻击、信息盗取等行为,因此需要重点防范。

二、电子数据交换技术的系统构成

EDI 系统由硬件系统和软件系统组成。硬件系统又包括计算机、通信设备和计算机网络。在 EDI 系统中,不同企业之间的计算机可以通过通信线路直接连接,也可以采用第三方机构提供的增值网(提供增值服务的网络)连接。由于 EDI 系统传输的大多是具有一定商业价值的商业资料,因此通过有专门机构管理的增值网络进行传输具有较高的安全性和可靠性。

在 EDI 的软件系统中,有一个特殊的转换软件。企业需要发送的数据往往是由计算机中其他的应用软件生成的,转换软件的作用就是把不同格式的数据翻译成 EDI 能接受的标准格式的数据。而在接收方,转换软件则把 EDI 标准格式的数据翻译成其他应用软件所能接受的格式的数据。因此,一个 EDI 消息处理系统大体上分为以下几个组成部分:

(1) EDI 用户代理。EDI 用户代理帮助单个 EDI 消息处理用户起草、编辑、翻译、提交、

① MHX(X.400)是由 ITU-T 和 ISO 定义的用于电子邮件传输的信息处理服务协议。ITU-T 是国际电信联盟管理下的专门制定远程通信相关国际标准的组织,中文全称为国际电信联盟远程通信标准化组织。

检索和接收 EDI 消息。它可与消息传送代理共置或分离，也可通过通信网络接入，构成远程 EDI 用户代理。

（2）EDI 消息存储。EDI 消息存储帮助单个用户代理参与 EDI 通信，它一般与消息传送代理处于同一系统中，可向与其对应的用户代理提供消息提交、投递、存储和检索。

（3）EDI 消息传送系统。EDI 消息传送系统主要是在用户代理间或在用户代理和访问单元之间传送 EDI 消息或 EDI 通知。一个 EDI 通知只对应一个消息传送系统。消息传送系统由一个或多个消息传送代理组成，它完成接续建立、存储转发，使用消息传送系统服务实现 EDI 用户间的数据交换。

（4）EDI 用户。EDI 用户可以访问 EDI 消息处理系统或接受 EDI 消息处理系统的访问。它包括物理投递访问单元和传真访问单元。

EDI 消息处理系统的各个组成部分以及它们之间的关系如图 3-2 所示。

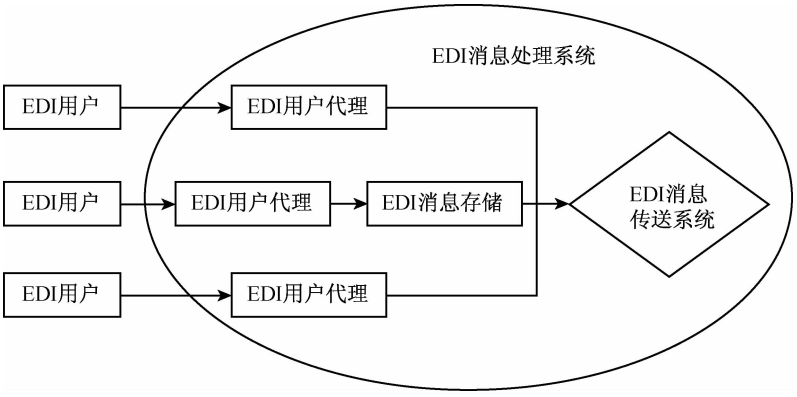

图 3-2　EDI 消息处理系统的组成

三、电子数据交换技术的安全策略和具体措施

EDI 的实际运作过程中，主要通过三级安全系统来达到前面介绍的安全目的，即网络级安全、应用级安全、报文级安全。

（1）网络级安全是通过身份识别和对应的密码管理来实现的。网络级安全确保只有合法的用户才能进入，IC 卡就是其中一种措施。

（2）应用级安全通过用户端软件来设置操作者的权限，从而限制操作者在自己的权限范围内进行操作。

（3）报文级安全主要提供加密和数字签名措施。加密有效地解决了机密性问题，数字签名有效地解决了防丢失、防篡改、防假冒、防抵赖的问题。形象地讲，加密就是在原有的信息基础上增加一些识别用户的信息，如在一串字符的前面加 8 位数字；数字签名就是将原有的信息进行某种运算，得出一串字符，并以此作为认证的依据。

为了更好地实现 EDI 安全，可以采用以下几项具体措施：

（1）数字签名。EDI 业务的源点鉴别和电文内容的完整性验证由数字签名来实现。在数字签名中，采用密码算法产生校验和，用校验和的方法来验证电文内容的完整性。源点鉴别则由合法源点给出用密钥加密信息的方法实现。

(2) 电文加密。电文内容的保密主要是通过对 EDI 电文内容加密的方法实现的。EDI 电文加密的加密体制,既可用对称密码体制(如 DES 算法),也可用非对称密码体制(如 RSA 算法)。

(3) 源点不可抵赖。为了实现源点不可抵赖,可采用数字签名方法,由电文发送者对电文进行数字签名。

(4) 接收不可抵赖。为实现接收的不可抵赖,也可采用数字签名方法来实现。即由电文接收者在收到的电文中加上其身份识别信息和收到日期,计算和增加一个数字签名填满扩展了的电文,并将签了名的电文在交易完成之前发回源点。

(5) 访问控制。EDI 的访问控制一般采用常见的存取控制方法,如访问控制表、能力表及标号等方法。

(6) 防止电文丢失。电文丢失可能发生在任何同等实体间的通信链路上,也可能由于操作失误或不当。防止普通电文丢失的方法是利用一个脱机的文档库将所有递交和投递的电文都保存起来;防止特定电文丢失,可采用安全审计跟踪的办法实现。对于用户而言,电文的投递最好有回执,以便及时了解电文是否投递到欲投递的地方而采取相应措施。

(7) 防拒绝服务。硬件必须采取双备份措施,并有良好的应急计划,可以及时恢复系统的正常运行。

第二节　密 码 技 术

密码学是一门很古老的学科,以密码学为基础进行密码编译和破译的方法被称为密码技术。实际上,密码技术在人们的生活中随处可见:大到国家级保密实验室的身份认证,小到 ATM 自动取款。下面将重点介绍密码学和常见的三种加密方式。

一、密码学概述

1. 密码学的组成和密码系统的要素

密码学主要是研究通信安全保密的学科,它包括两个分支:密码编码学和密码分析学。

密码编码学主要研究对信息进行变换,以保护信息在信道的传递过程中不被攻击者窃取、解读和利用的方法;而密码分析学则与密码编码学相反,它主要研究如何分析和破译密码。这两者之间既相互对立又相互促进。

密码编码的基本思想是对机密信息进行伪装。一个密码系统需要完成如下伪装:某用户(加密者)对需要进行伪装的机密信息(明文)进行变换(加密变换),得到另外一种看起来似乎与原有信息不相关的表示(密文)。当合法的用户(接收者)获得了伪装后的信息(密文),那么他可以依照之前和信息发出者约定的算法从这些信息中还原得到原来的机密信息(解密变换)。而如果不合法的用户试图从这种伪装后的信息中分析得到原有的机密信息(密码分析),由于没有相应的算法,这种分析过程名义上是不可能的,以至于无法进行。

算法是密码学中一个重要的方面,它是对信息进行加密、解密所需要的工具。在计算机科学领域中,算法通常被看做程序的一个组成部分,常作为一个例程或者一个库被引用。主

程序通常是在不同的数据集合上反复调用算法库来执行数学运算。某些特别复杂的算法可能会在特殊的硬件当中实现。例如，Intel 或 AMD 的 CPU，它们的指令集中就整合了很多算法。密码算法(cryptographic algorithm)是数学算法，设计密码算法是为了能够用不同的数据集合作为参数来调用它们，从而在这些数据集合上进行相应的运算。密码服务提供者(cryptographic service provider)，从本质上讲就是可以通过一套定义良好的接口进行调用的执行特定密码计算功能的密码算法(加密算法、签名算法等)库。密码算法是复杂的，有的时候可以利用硬件加速器来加快某些数学计算。

Intel 公司于 2010 年 3 月发布的 i7-980X 六核处理器整合了多种算法，其中最引人注意的是，它新增了 6 条针对加密和解密运算的指令——AES。新增 AES 后，计算机性能显著提高。该处理器的指令集可以将各种算法整合以便随时调用进行工作。图 3-3 为 Intel 官方网站的宣传贴图。

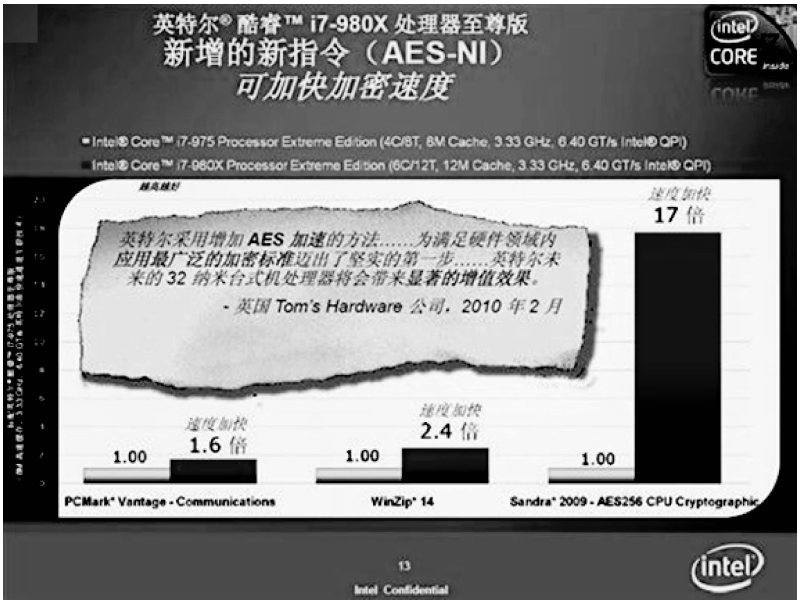

图 3-3　Intel 官方网站的宣传贴图

准确地说，一个密码系统由明文空间、密文空间、密码方案和密钥空间组成。

(1) 需要加密的信息称为明文，明文的全体称为明文空间。一般情况，明文用 M(message)或 P(plain text)表示。明文是信源编码符号，它可能是文本文件、位图、数字化存储的语音流或数字化的视频图像的比特流，也可以简单地认为明文是有意义的字符流或比特流。

(2) 密文是经过伪装后的明文，密文的集合称为密文空间。一般情况，密文用 C(cipher)表示，它也可以被认为是字符流或比特流。

(3) 密码方案确切地描述了加密变换与解密变换的具体规则。这种描述一般包括对明文进行加密时所使用的一组规则的描述，以及对密文进行还原时所使用的一组规则的描述。明文加密规则称为加密算法，其对明文实施的变换过程称为加密变换，简称加密。密文还原规则称为解密算法，其对密文实施的变换过程称为解密变换，简称解密。

(4) 加密和解密算法的操作通常在称为密钥的元素控制下进行。密钥包括加密密钥与

解密密钥，密钥的全体称为密钥空间。一般情况，密钥用 K(key)表示。

从数学的角度来讲，一个密码系统是一组映射，它在密钥的控制下将明文空间中的每一个元素映射到密文空间中的某个元素。这组映射由密码方案确定，具体使用哪一个映射由密钥决定。

2. 密码的安全

在密码系统所处的环境中除了接收者外，还有攻击者(或称非授权者)，攻击者往往就是人们熟悉的黑客。它们通过各种方式来窃听或干扰信息。例如，攻击者可采用电磁侦听、声音窃听、搭线窃听等方法直接得到未加密的明文或加密后的密文，这种对密码系统的攻击手段称为被动攻击；攻击者也可采用删除、更改、插入、重放等手段主动地发送破坏消息，使收信人得不到发信人发送的全部有效信息，这种对密码系统的攻击手段称为主动攻击。

对一个密码系统的被动攻击将损害明文信息的机密性，即需要保密的明文信息遭到泄露；而对一个密码系统的主动攻击将损害明文信息的完整性，即使得通信时的接收方所接收到的信息与发送方所发送的信息不一致。保证信息机密性的方法是使用密码算法进行加密，而保证信息完整性的方法是使用鉴别与认证机制。攻击者借助窃听到的密文以及其他一些信息，并通过各种方法推断原来的明文甚至密钥，这一过程称为密码分析或密码攻击。从事这一工作的人称为密码分析员或密码分析者。如果攻击者可以由密文推出明文或密钥，或者由明文和密文可以寻求密钥，那么就称该密码系统是可破译的。相反地，则称该密码系统不可破译。

对于一个密码系统来说，若攻击者无论得到多少密文也求不出确定明文所需的足够信息，这种密码系统就是理论上不可破译的，称该密码系统具有无条件安全性(或完善保密性)。若一个密码系统理论上虽可破译，但为了由密文得到明文或密钥却需要付出非常多的计算时间和精力，而不能在期望的时间内或实际可能的经济条件下求出准确的答案，这种密码系统就是实际不可破译的，或称该密码系统具有计算安全性(或实际保密性)。衡量不可破译性的尺度叫保密强度。对于任何一个密码系统，如果达不到理论上不可破译，就必须达到实际不可破译。

3. 哈希函数

哈希函数也称为哈希算法，是将任意长的数字串映射成一个较短的定长输出数字串的函数。这个函数易于计算，生成的字符串称为原字符串的哈希值，也称哈希码、哈希结果等，或简称哈希。这个生成的字符串无疑打上了输入数字串的烙印，所以又称其为输入字符串的数字指纹。生成的字符串(哈希值)有一定的位数限制，因此，不同的字符串有可能对应相同的哈希值。由于哈希函数是多对一映射，所以不能从哈希值求出原来的字符串，但可以验证任意给定序列字符串是否为用户需要的字符串。

哈希函数在实际中有广泛的应用，在密码学和数据安全技术中，它是实现有效、安全、可靠数字签名和认证的重要工具，是安全认证协议中的重要模块。由于哈希函数应用的多样性和其本身的特点，它有很多不同的名字，其含义也有差别，如压缩函数、紧密函数、数据认证码、信息摘要、数字指纹、数据完整性校验、密码检验和、消息认证码、篡改检测码等。

单向哈希函数还可按其是否有密钥控制划分为两大类：一类有密钥控制，称为密码哈希

函数；另一类无密钥控制，称为一般哈希函数。无密钥控制的单向哈希函数，其哈希值只是输入字符串的函数，任何人都可以计算，因而不具有身份认证功能，只用于检测接收数据的完整性，用于非密码计算机应用中。而有密钥控制的单向哈希函数，要满足各种安全性要求，其哈希值不仅与输入有关，而且与密钥有关，只有持此密钥的人才能计算出相应的哈希值，因而具有身份验证功能。此时的哈希值也称为认证符或认证码。密码哈希函数在现代密码学中有重要作用。

二、信息传输中的加密方式

1. 链路—链路加密

对于在两个网络结点间的某一通信链路，链路加密能为网上传输的数据提供安全保证。对于链路加密（又称在线加密），是将所有消息在被传输之前进行加密，在每一个结点对接收到的消息进行解密，然后使用下一个链路的密钥对消息进行加密，再进行传输。在到达目的地之前，一条消息可能要经过许多通信链路的传输。

链路—链路的加密方法将网络看做链路连接的结点集合，每一个链路被独立地加密。链路—链路加密方式为两个结点之间通信链路中的信息提供安全性，不考虑信源和信宿，与这个信息的起始或终结无关，如图 3-4 所示。每一个这样的链接相当于 OSI 参考模型建立在物理层之上的数据链路层。它用于保护通信结点间的数据，接收方是传送路径上的各台结点机，信息在每台结点机内都要被解密和再加密，依次进行，直至到达目的地。这样，由于在每一个中间传输结点消息均被解密后重新进行加密，因此包括路由信息在内的链路上的所有数据均以密文形式出现。经过链路加密，信息就掩盖了被传消息的源点与终点。由于填充技术的使用以及填充字符在不需要传输数据的情况下就可以进行加密，这使得消息的频率和长度特性也得以掩盖，从而可以防止不法者对通信业务进行分析。

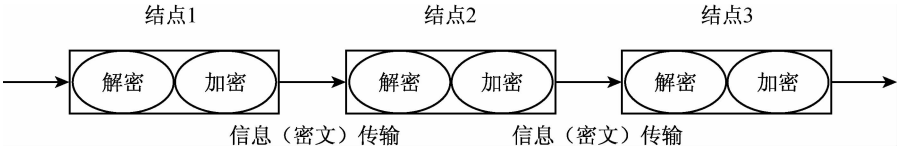

图 3-4　链路—链路加密方式示意图

尽管链路—链路加密在计算机网络环境中使用得相当普遍，但它并非没有问题。在电子商务的应用中，这种通信方式存在以下几个问题：

（1）这种加密方法通常用在点对点的同步或异步线路上，它要求先对在链路两端的加密设备进行同步，然后使用一种链模式对链路上传输的数据进行加密。这就给网络的性能和可管理性带来了副作用。

（2）一方面，在线路经常不通或信号不稳定的海外或卫星网络中，链路上的加密设备需要频繁地进行同步，带来的后果是数据丢失或重传。另一方面，即使仅有一小部分数据需要进行加密，也会使得所有传输数据被加密。

（3）在一个网络结点上，链路加密仅在通信链路上提供安全性，消息以明文形式存在，因此所有结点在物理上必须是安全的，否则就会泄露明文内容。然而，保证每一个结

点的安全性需要较高的费用，为每一个结点提供加密硬件设备和一个安全的物理环境所需要的费用主要包括以下几个部分：保护结点物理安全的雇员开销、为确保安全策略和程序的正确执行而进行审计时的费用以及为防止安全性被破坏时带来损失而参加保险的费用等。

（4）在传统的加密算法中，用于解密消息的密钥与用于加密的密钥是相同的，该密钥必须被秘密保存，并按一定规则进行变化。这样，密钥分配在链路加密系统中就成了一个问题，因为每一个结点必须存储与其相连接的所有链路的加密密钥，这就需要对密钥进行物理传送或者建立专用网络设施。而网络结点地理分布的广阔性使得这一过程变得复杂，而且也增加了密钥连续分配时的费用。

2. 结点加密

结点加密的目的是对源结点到目的结点之间的传输链路提供加密保护。结点加密是指每对结点共用一个密钥，对相邻两个结点间（包括结点本身）传送的数据进行加密保护。结点加密在操作方式上与链路加密是类似的：两者均在通信链路上为信息提供安全性；都在中间结点先对信息进行解密，然后再进行加密。因为要对所有传输的数据进行加密，这一过程在结点上的安全模块中进行。

与链路—链路加密不同的是，结点加密不允许信息在网络结点以明文形式存在，它先把收到的信息进行解密，然后采用另一个不同的密钥进行加密，这一过程是在结点上的一个安全模块中进行的，所以加密过程对用户是透明的。在结点加密方式中，为了将报文传送到指定的目的地，线路上的每个结点必须检查路由选择信息，因此只能对报文的正文进行加密而不能对报头加密。报头和路由信息以明文形式传输，以便中间结点能得到如何处理该报文正文的信息，但是这种方法不利于防止攻击者分析通信业务。

结点加密方法的特点在于：

（1）在结点处采用一个与结点机相连的密码装置。

（2）密文在该装置中被解密并被重新加密。

（3）明文不通过结点机，避免了链路—链路加密结点处易受攻击的缺点。

3. 端—端加密

端—端加密又称脱线加密或包加密，建立在 OSI 参考模型的网络层和传输层。这种方法要求传送的数据从源端到目的端一直保持密文状态，数据在发送端被加密，在接收端被解密，且在中间结点处不以明文的形式出现。即使有结点被损坏也不会使信息泄露，任何通信链路的错误都不会影响整体数据的安全性，端—端加密示意图如图 3-5 所示。如果加密在应用层或表示层进行，那么它可以不依赖于所用通信网的类型。

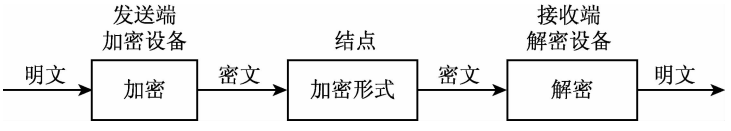

图 3-5　端—端加密方式示意图

在端—端加密方式中，只加密数据本身信息，不加密路径控制信息。在发送主机内信息

是加密的，在中间结点信息也是加密的。用户必须找到加密算法，可以选择加密，也可以决定施加某种加密手段。加密可以用软件编程实现。

端—端加密方法将网络看做是一种介质，数据能安全地从源端到达目的端。这种加密在 OSI 模型的高三层进行，在源端进行数据加密，在目的端进行解密，而在中间结点及其线路上一直以密文形式出现。在中间任何结点报文均不解密。因此，不需要有密码设备。端—端加密同链路—链路加密相比，可减少密码设备的数量。

端—端加密系统的价格便宜些，并且与链路—链路加密和结点加密相比更可靠，更容易设计、实现和维护；还避免了其他加密系统所固有的同步问题，因为每个报文包都是独立被加密的，所以一个报文包所发生的传输错误不会影响后续的报文包。此外，从用户对安全需求的直觉上讲，端—端加密更自然些。单个用户可能会选用这种加密方法，以便不影响网络上的其他用户，此方法只需要源结点和目的结点是保密的即可。

端—端加密的缺点是允许进行通信量分析。端—端加密系统通常不允许对信息的目的地址进行加密，这是因为每一个信息所经过的结点都要用此地址来确定如何传输信息。由于这种加密方法不能掩盖被传输信息的源点与终点，因此它对于防止攻击者分析通信业务是脆弱的，而且它的密钥管理机制较复杂。

4. 三种加密方式的选择

三种加密方式的优缺点对比如表 3-1 所示。

表 3-1　三种加密方式的优缺点对比

方　式	优　点	缺　点
链路—链路加密	(1) 包含报头和路由信息在内的所有信息均加密； (2) 单个密钥损坏时整个网络不会损坏，每对网络结点可用不同的密钥； (3) 加密对用户透明	(1) 信息以明文形式通过每一个结点； (2) 因为所有结点都必须有密钥，密钥分发和管理变得困难； (3) 由于每个安全通信链路需要两个密码设备，因此费用较高
结点加密	(1) 消息的加密、解密在安全模块中进行，这使得消息内容不会被泄露； (2) 加密对用户透明	(1) 某些信息（如报头和路由信息）必须以明文形式传输； (2) 因为所有结点都必须有密钥，密钥分发和管理变得困难
端—端加密	(1) 使用方便，采用用户自己的协议进行加密，并非所有数据都必须加密； (2) 网络中数据从源点到终点均受保护； (3) 加密对网络结点透明，在网络重构期间可使用加密技术	(1) 每一个系统都需要完成相同类型的加密； (2) 某些信息（如报头和路由信息）必须以明文形式传输； (3) 必须采用安全、先进的密钥颁发和管理技术

对于以上三种加密方式进行分析和对比，可以得出下面的结论：

(1) 在多个网络互连的环境下，宜采用端—端加密方式。

（2）在需要保护的链路数不多、要求实时通信、不支持端—端加密远程调用通信等场合，宜采用链路—链路加密方式。这样仅需少量的加密设备即可，从而可保证不降低太多的系统效能，不需要太高的加密成本。

（3）在需要保护的链路数较多的场合以及在文件保护、邮件保护、支持端—端加密的远程调用、实时性要求不高的通信等场合，宜采用端—端加密方式。这样可以使网络具有更高的保密性、灵活性，加密成本也较低。

（4）对于需要防止流量分析的场合，可考虑采用链路—链路加密和端—端加密组合的加密方式。

资料链接 3-1

对称密钥密码体制与非对称密钥密码体制

对称密钥密码体制又称常规密钥密码体制或单钥加密体制，是指使用相同的密钥加密和解密，发送者和接收者有相同的密钥。常见的对称加密算法是 DES 算法、AES 算法。

非对称密钥密码体制则需要采用两个在数学上相关的密钥对——公开密钥和私有密钥来进行加密和解密，因而它又常被称为公开密钥密码体制或双钥密码体制。常见的不对称加密算法有 RSA 算法和美国国家标准局提出的 DSA 算法。

第三节　认 证 技 术

认证技术是解决电子商务活动中的安全问题的技术基础。认证采用对称密码、公钥加密、散列算法等技术为电子商务活动中的信息完整性和不可否认性以及电子商务实体的身份真实性提供技术保障。

认证是信息安全中的一个重要内容，可分为数字签名（消息认证）和身份认证。其中，数字签名主要用于保证信息的完整性与抗否认性，身份认证则用于鉴别用户身份。在电子商务系统中，有时候认证技术比信息加密本身更加重要。例如，用户往往对网上商店的身份的真实性的关注要多于对购物信息的保密性，因为不同商家的信用等级不同，其所提供的服务差别也较大，身份认证能确保用户找到合适的商家。此外，身份认证能保证用户的个人信息和提交的购物信息不被第三方获取，并且使网上商家不能抵赖。同样，商家也面临着这些问题。这一节将重点对数字签名和身份认证技术作介绍。

一、数字签名

数字签名是从传统的手写签名衍生而来的，它可以提供一些基本的密码服务，如保证数据的完整性、真实性以及不可否认性。数字签名是实现电子交易安全的核心技术之一，它在身份认证、数据完整性、不可否认性以及匿名性等方面有着重要的应用。数字签名是通过一个单向哈希函数对要传送的报文进行处理，用以认证报文来源并核实报文是否发生变化的

一个字母数字串。该字母数字串称为该消息的消息鉴别码或消息摘要，这就是通过单向哈希函数实现的数字签名。在公钥体制下的签名，用户用自己的私钥对原始数据的哈希摘要进行加密，然后信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后获得哈希摘要，并通过与自己收到的原始数据产生的哈希摘要对照，便可确信原始资料是否被篡改，这样就保证了传输的不可否认性。这就是公钥签名技术。

简单地说，数字签名就是通过一个单向函数对要传送的报文进行处理，得到用于认证报文来源并核实报文是否发生变化的一个字母数字串。用这个字符串来代替书写签名或印章，可以起到与书写签名或印章同样的法律效用。数字签名应必须能保证：接收者能够核实发送者对报文的签名，发送者事后不能抵赖对报文的签名，接收者不能伪造对报文的签名。

目前有许多数字签名的方法，它们可以分为两类：直接数字签名和需仲裁的数字签名。直接数字签名仅涉及通信双方，数字签名被直接发给通信的另一方。在需仲裁的数字签名中，每个发送方发往接收方的签名报文要先被送给仲裁者，仲裁者对该报文及其签名进行一系列的测试以检验它的出处和内容，然后对报文注明日期，附上一个已经经过仲裁证实属实的说明后发给接收方。在这里面，仲裁者相当于电子商务活动以外的第三方。通过仲裁可以验证发送方的私钥/公钥仍然有效，防止密钥泄露后攻击者的欺骗行为。数字签名一般采用两次加密来实现，即一次加密实现签名，一次加密实现秘密通信。实际上也可以只进行签名加密，这时报文将以明文的形式发送。

由此可见，数字签名是通过一种算法得到另一条信息来保证原有信息的正确性。实现数字签名有很多方法，目前采用较多的是公钥加密技术和散列算法相结合的数字签名方式。散列函数对要发送的信息提供信息鉴别码，而加密系统则提供安全的通道来实现数字签名。散列函数以一个报文作为其输入，然后输出一个定长的散列码，这个散列码有差错检测能力：报文改变任意一点，散列码都将发生改变。因此，可以将散列码等同于原信息的“指纹”。前面介绍的哈希函数就是散列函数的一种。

数字签名的算法很多，依照不同的算法，数字签名也可分为不同的种类。这里介绍RSA 数字签名。

RSA 数字签名是目前最流行的一种数字签名。它是由 Ron Rivest、Adi Shamir 和 Leonard Adleman 于 1978 年提出的，这种签名的名称也由这三个人名字的首字母组合起来命名的。

假定 RSA 的公钥密码系统已经建立，若发送方要对某报文实现数字签名，并发送给接收方，数字签名算法如下：

(1) 签名的实现。发送方先用散列函数对报文进行处理，生成一个定长的散列码，再使用自己的私钥进行加密就形成了签名，然后将报文和签名一起发送出去。

(2) 签名的验证。接收方将接收到的签名用发送方的公钥解密，用相同的散列函数处理接收到的报文得到新的散列码，若这个散列码和解密的签名相匹配，则认为该签名是有效的；否则，就认为报文被篡改或受到了攻击者欺骗。这是因为只有发送方知道自己的私钥，因此只有发送方才能产生有效的签名。RSA 数字签名原理如图 3-6 所示。