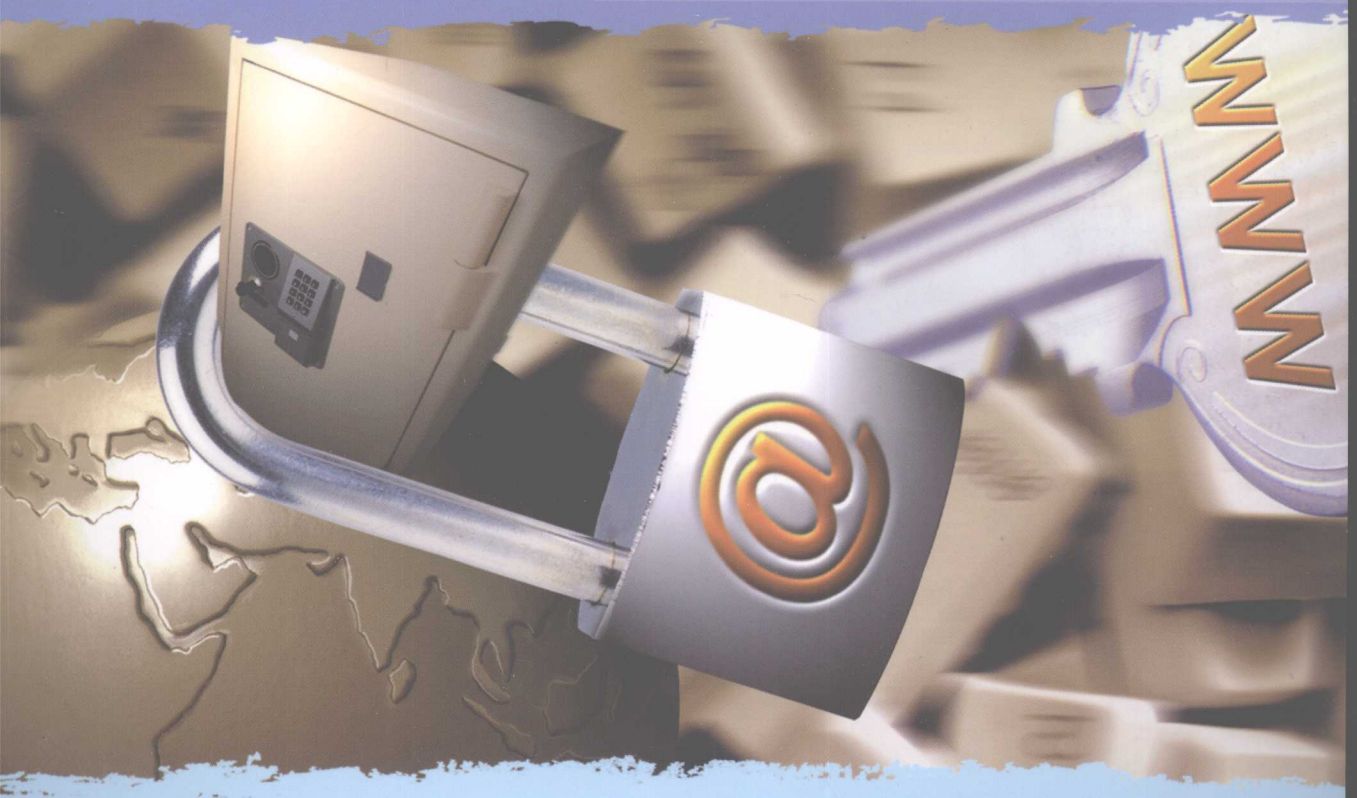
高职高专
电子商务类课程规划教材

新世纪

电子商务安全技术

新世纪高职高专教材编审委员会组编
主编 梁永生　主审 彭 波



大连理工大学出版社

新世纪

高职高专电子商务类课程规划教材

电子商务安全技术

新世纪高职高专教材编审委员会组编

主审 彭 波

主 编 梁永生 副主编 徐国芹 范荣真 王伍祺 郭 森

DIANZI SHANGWU ANQUAN JISHU

大连理工大学出版社
DALIAN UNIVERSITY OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

电子商务安全技术/梁永生主编. —大连:大连理工大学出版社,2008.4
高职高专电子商务类课程规划教材
ISBN 978-7-5611-3900-4

Ⅰ.电… Ⅱ.梁… Ⅲ.电子商务—安全技术—高等学校:技术学校—教材 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2008)第 040881 号

大连理工大学出版社出版
地址:大连市软件园路 80 号 邮政编码:116023
发行:0411-84708842 邮购:0411-84703636 传真:0411-84701466
E-mail:dutp@dutp.cn URL:http://www.dutp.cn
大连业发印刷有限公司印刷 大连理工大学出版社发行

幅面尺寸:185mm×260mm 印张:22 字数:491 千字
印数:1～4000
2008 年 4 月第 1 版 2008 年 4 月第 1 次印刷

责任编辑:陈祝爽 责任校对:宋 哲
封面设计:季 强

ISBN 978-7-5611-3900-4 定 价:34.00 元

总　序

我们已经进入了一个新的充满机遇与挑战的时代，我们已经跨入了21世纪的门槛。

20世纪与21世纪之交的中国，高等教育体制正经历着一场缓慢而深刻的革命，我们正在对传统的普通高等教育的培养目标与社会发展的现实需要不相适应的现状作历史性的反思与变革的尝试。

20世纪最后的几年里，高等职业教育的迅速崛起，是影响高等教育体制变革的一件大事。在短短的几年时间里，普通中专教育、普通高专教育全面转轨，以高等职业教育为主导的各种形式的培养应用型人才的教育发展到与普通高等教育等量齐观的地步，其来势之迅猛，发人深思。

无论是正在缓慢变革着的普通高等教育，还是迅速推进着的培养应用型人才的高等职业教育，都向我们提出了一个同样的严肃问题：中国的高等教育为谁服务，是为教育发展自身，还是为包括教育在内的大千社会？答案肯定而且惟一，那就是教育也置身其中的现实社会。

由此又引发出高等教育的目的问题。既然教育必须服务于社会，它就必须按照不同领域的社会需要来完成自己的教育过程。换言之，教育资源必须按照社会划分的各个专业（行业）领域（岗位群）的需要实施配置，这就是我们长期以来明乎其理而疏于力行的学以致用问题，这就是我们长期以来未能给予足够关注的教育目的问题。

如所周知，整个社会由其发展所需要的不同部门构成，包括公共管理部门如国家机构、基础建设部门如教育研究机构和各种实业部门如工业部门、商业部门，等等。每一个部门又可作更为具体的划分，直至同它所需要的各种专门人才相对应。教育如果不能按照实际需要完成各种专门人才培养的目标，就不能很好地完成社会分工所赋予它的使命，而教育作为社会分工的一种独立存在就应受到质疑（在市场经济条件下尤其如此）。可以断言，按照社会的各种不同需要培养各种直接有用人才，是教育体制变

革的终极目的。

随着教育体制变革的进一步深入，高等院校的设置是否会同社会对人才类型的不同需要一一对应，我们姑且不论。但高等教育走应用型人才培养的道路和走研究型（也是一种特殊应用）人才培养的道路，学生们根据自己的偏好各取所需，始终是一个理性运行的社会状态下高等教育正常发展的途径。

高等职业教育的崛起，既是高等教育体制变革的结果，也是高等教育体制变革的一个阶段性表征。它的进一步发展，必将极大地推进中国教育体制变革的进程。作为一种应用型人才培养的教育，它从专科层次起步，进而应用本科教育、应用硕士教育、应用博士教育……当应用型人才培养的渠道贯通之时，也许就是我们迎接中国教育体制变革的成功之日。从这一意义上说，高等职业教育的崛起，正是在为必然会取得最后成功的教育体制变革奠基。

高等职业教育还刚刚开始自己发展道路的探索过程，它要全面达到应用型人才培养的正常理性发展状态，直至可以和现存的（同时也正处在变革分化过程中的）研究型人才培养的教育并驾齐驱，还需要假以时日；还需要政府教育主管部门的大力推进，需要人才需求市场的进一步完善发育，尤其需要高职高专教学单位及其直接相关部门肯于做长期的坚忍不拔的努力。新世纪高职高专教材编审委员会就是由全国 100 余所高职高专院校和出版单位组成的旨在以推动高职高专教材建设来推进高等职业教育这一变革过程的联盟共同体。

在宏观层面上，这个联盟始终会以推动高职高专教材的特色建设为己任，始终会从高职高专教学单位的实际教学需要出发，以其对高等职业教育发展的前瞻性的总体把握，以其纵览全国高职高专教材市场需求的广阔视野，以其创新的理念与创新的运作模式，通过不断深化的教材建设过程，总结高职高专教学成果，探索高职高专教材建设规律。

在微观层面上，我们将充分依托众多高职高专院校联盟的互补优势和丰裕的人才资源优势，从每一个专业领域、每一种教材入手，突破传统的片面追求理论体系严整性的意识限制，努力凸现高等职业教育职业能力培养的本质特征，在不断构建特色教材建设体系的过程中，逐步形成自己的品牌优势。

新世纪高职高专教材编审委员会在推进高职高专教材建设事业的过程中，始终得到了各级教育主管部门以及各相关院校相关部门的热忱支持和积极参与，对此我们谨致深深谢意，也希望一切关注、参与高职教育发展的同道朋友，在共同推动高职教育发展、进而推动高等教育体制变革的进程中，和我们携手并肩，共同担负起这一具有开拓性挑战意义的历史重任。

新世纪高职高专教材编审委员会

2001 年 8 月 18 日

前　言

随着信息技术日新月异的发展，人类已经进入以网络为主的信息时代，基于 Internet 开展的电子商务已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，但随之而来的是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，保证整个商务过程中信息的安全性，使基于 Internet 的电子交易方式与传统交易方式一样安全可靠，已经成为电子商务应用中必须关注的重要技术问题。

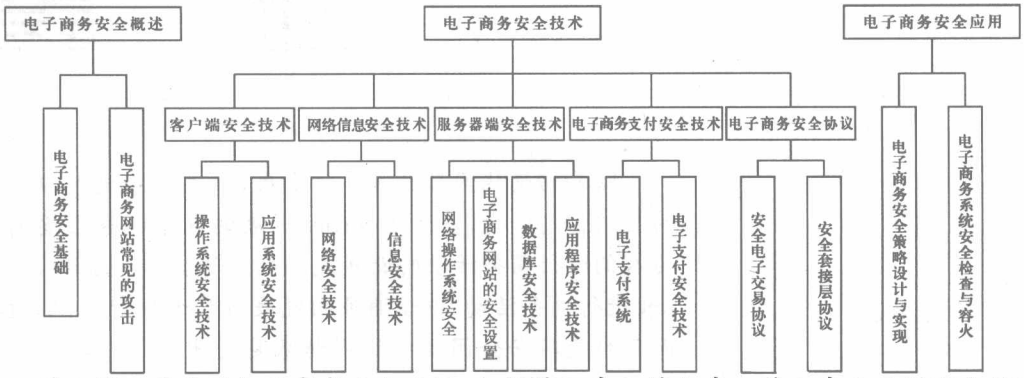
据权威机构调查表明，目前国内企业发展电子商务的最大顾虑是网上交易的安全问题。因此，信息的安全是当前发展电子商务最迫切需要研究和解决的问题。Internet 之所以能发展成为今天的全球性网络，主要是依赖于它的开放性。但是，这种开放式的信息交换方式使其网络安全具有很大的脆弱性。

本书以电子商务交易与系统维护两方面的安全技术为主线，全书分为三篇、共九章，本书内容安排的总体结构如下图所示，主要内容简介如下：

第一篇主要讲述电子商务安全概述，包括第一章和第二章。第一章主要讲述电子商务安全基础；第二章主要讲述电子商务网站常见的攻击。

第二篇主要讲述电子商务安全技术，也是本书的重点，包括第三章至第七章。第二篇主要解决交易与维护两方面的安全问题，按照电子商务的交易过程：客户机→通信传输→服务器的顺序来编撰，并且电子支付安全技术和电子商务安全协议贯穿整个交易过程。其中第三章的客户端安全技术包括操作系统安全技术和应用系统安全技术；第四章的网络信息安全技术包括网络安全技术和信息安全技术；第五章的服务器端安全技术包括网络操作系统安全、电子商务网站的安全设置、数据库安全技术和应用程序安全技术；第六章的电子商务支付安全技术包括电子

支付系统和电子支付安全技术；第七章的电子商务安全协议包括安全套接层协议 SSL 和安全电子交易协议 SET。



第三篇主要讲述电子商务安全应用，包括第八章和第九章。第八章主要讲述电子商务安全策略设计与实现；第九章主要讲述电子商务系统安全检查与容灾。

本书由梁永生担任主编，其中的第一章和第四章由梁永生编写，第二章和第七章由范荣真编写，第三章和第五章由徐国芹编写，第六章由郭森编写，第八章和第九章由王伍祺编写。全书由梁永生负责统稿、修改、补充和定稿，郭森修改、补充了部分章节内容，邓伟鑫和王昌伟对全书的实训指导、规范排版进行了校对。

本书的特色与创新之处：

1. 核心内容——电子商务安全技术部分按照电子商务的交易过程：客户机→通信传输→服务器的顺序来编撰，主线索清晰，方便教师讲解和学生学习。

2. 按照以实际技能为导向、以够用为度两个基本要求组织各章内容，虽然本书主要探讨技术，但是充分兼顾了高职高专院校学生的特点。结合课程内容和电子商务类企业情况，安排了 14 个实训项目，在提高学生应用技能的同时，强化项目驱动，实施“工学结合”，提高理论教学和实践教学质量。

3. 部分章节引进电信运营商和大型电子商务公司的实际应用案例和具体实现架构，为学生在生产性实训、顶岗实习及未来就业等方面，实现与企业的无缝对接奠定基础。

本书适合于大专院校、高职高专院校学生使用，同时也适用于相应水平的电子商务培训班学员以及对电子商务感兴趣的爱好者使用。

本书在编写过程中参考或引用了大量专家学者的论著、图书和网站资料，编者已尽其所能在参考文献中列出，在此对各位专家学者表示衷心的感谢，若有疏漏，在此表示歉意。由于电子商务安全技术是一门正在发展中的学科，技术更新极快，加之编者水平有限，并且是多人编写，书中难免有疏漏和不妥之处，敬请广大读者和专家学者批评指正。

编　者

2007 年 12 月

目　录

第一篇　电子商务安全概述

第二篇　电子商务安全技术

第三篇　电子商务安全应用

第一篇　电子商务安全概述

随着电子信息技术和Internet的发展，全球商务活动日益受到新兴电子信息技术的影响，产生了电子商务(Electronic Commerce或Electronic Business，简写为EC或EB)并且已经成为一个热门研究领域。2005年6月举行的“第八届中国国际电子商务大会”上发布了如下消息：在全球新型技术的发展高潮中，电子商务已步入了“黄金时期”。我国的电子商务发展迅猛，平均交易总额年增长率为40%。2004年电子商务的交易总额达到4 400亿元人民币，2005年激增至6 200亿元人民币，2006年将达到8 700亿元人民币，Forrester预测2010年美国企业与消费者之间(Business to Consumer，B2C)电子商务在线交易总额将达3 290亿美元，企业和企业之间(Business to Business，B2B)在线交易总额更是B2C之间在线交易总额的几十倍，电子商务业已成为一种重要的商务活动新模式。

表1-1所示为各年度B2B、B2C真实的和估计的在线交易总额。数据来源于ClickZ Network、eMarketer、Forrester Research和2004～2005美国调查局统计摘要。

表Ⅰ　　B2B、B2C真实的和估计的在线交易总额

年度	B2C在线交易总额(10亿美元)	B2B在线交易总额(10亿美元)
2007	240	6 800
2006	190	5 300
2005	150	4 100
2004	130	2 800
2003	100	1 600
2002	80	900
2001	70	730
2000	50	600
1999	25	550
1998	10	520
1997	5	490
1996	1	460

电子商务是由计算机、通信网络及程序化、标准化的商务流程和一系列安全、认证法律体系组成的集合，是一种以互联网为基础、以交易双方为主体、以银行电子支付和结算为手段、以客户数据为依托的全新商务模式。电子商务系

统框架如图 1-1 所示。

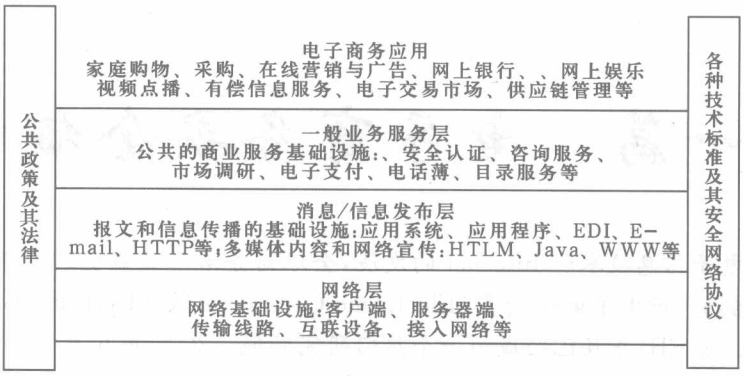


图 I　子商务系统框架图

电子商务系统框架分为三个层次和两个支柱。从最基础的技术层次到电子商务的应用层次可分为网络层、消息/信息发布层和一般业务服务层三个层次，它们构成电子商务系统的基础设施，三个层次之上是特定的电子商务应用；两个支柱是公共政策及其法律、各种技术标准及其安全网络协议，它们构成了电子商务的基础环境。

电子商务的定义至今仍不是一个很清晰的概念，各种组织、机构根据各自的地位和对电子商务的参与程度，给出了表述不同的定义。

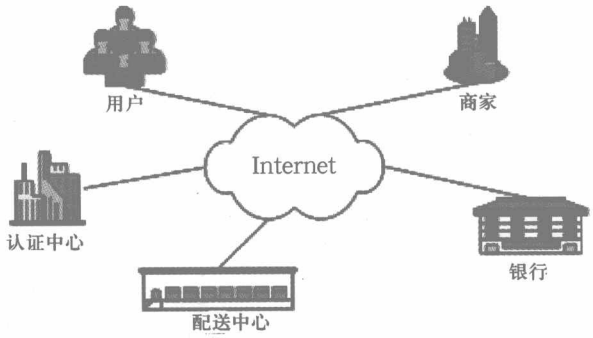
联合国国际经济合作和发展组织(Organization for Economic Cooperation and Development，OECD)定义电子商务是发生在开放的 Internet 网络上的包含企业之间(Business to Business，B2B)、企业与消费者之间(Business to Consumer，B2C)的商业交易。此外还包括消费者之间(Consumer to Consumer，C2C)、企业与政府之间(Business to Government，B2G)、消费者与政府之间(Consumer to Government，C2G)以及政府之间(Government to Government，G2G)的商业交易。

国际标准化组织(International Standard Organization / International Electrotechnical Commission，ISO/IEC) UNECE(United Nations Economic Commission for Europe)关于电子商务(Electronic Business，EB)谅解备忘录：电子商务是企业之间，企业与消费者之间信息内容与需求交换的一种通用术语。

联合国国际贸易法律委员会(United Nation International Trade Association of Law，UNITRAL)：电子商务是采用电子数据交换(Electronic Data Interchange，EDI)和其他通信方式增进国际贸易的职能。

全球信息基础设施委员会(Global Information Infrastructure Commission，GIIC)电子商务工作委员会报告草案：电子商务是运用电子通信作为手段的经济活动，通过这种方式人们可以对带有经济价值的产品和服务进行宣传、购买和结算。

综上所述，通俗地说，电子商务就是各参与方基于电子手段而不是以物理交换或直接物理接触方式按照一定的标准进行的商务活动，简而言之，就是网上做生意。电子商务系统由 Internet 网络、用户、配送中心、认证中心、银行和商家等组成，电子商务系统组成如图 1-2 所示。在大多数参考文献中，电子商务通常翻译成 eCommerce 和 eBusiness。eCommerce 可以理解为电子商务，基于电子手段进行的商务活动。eBusiness 可以理解为电子商业，电子商业包含的范围更广，不仅包括商务活动，还包括网络营销、物流配送等一系列与商业相关的活动。



图Ⅱ　电子商务系统组成图

1996 年，IBM 公司率先提出电子商务系统概念，提出电子商务模型：

eBusiness＝IT＋Web＋Business

在上述模型中，我们可以得到，构成 Business 的前提是 IT＋Web，电子商务是广域上的交易，电子商务所基于的 Internet 是个开放性的网络，正是由于它的开放性，才使其得以成为全球性的网络，也正是由于它的开放性，网络安全具有很大的脆弱性，这也正是电子商务安全技术研究的必要性所在。

本篇主要讲述电子商务安全概述，包括第一章和第二章。第一章主要讲述电子商务安全基础，第二章主要讲述电子商务网站常见的攻击。本篇为本书的核心部分——第二篇电子商务安全技术部分奠定基础。

在当今这个信息爆炸的时代，电子商务已逐渐成为人们进行商务活动的新模式，但随之而来的安全问题也变得越来越突出。如何构建一个安全、便捷的电子商务应用环境，保证整个商务过程中信息的安全性，已经成为电子商务应用中的重要技术问题。

第1章 电子商务安全基础

电子商务是 Internet 爆炸式发展的直接产物，是网络技术应用的全新发展方向。Internet 本身所具有的开放性、全球性、低成本、高效率的特点，也成为电子商务的内在特征，并使得电子商务大大超越了作为一种新的贸易形式所具有的价值，它不仅会改变企业本身的生产、经营、管理活动，而且将影响到整个社会的经济运行与结构。

现阶段推动电子商务面临的最大问题是如何保障电子商务过程中的安全性，电子商务过程的安全是网上贸易的基础和保障，同时也是电子商务技术的难点，并且电子交易的安全性是电子商务所独有的，是电子商务技术的重点。近年来，国际上已经制定和实施了一系列的方法来解决网上交易的安全性问题。

1.1 电子商务安全概念

电子商务作为一种全新的商务模式，它有很大的发展前途，同时，这种商务模式对管理水平、信息传递技术都提出了更高的要求，其中安全体系的构建又显得尤为重要。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，是商家和用户都十分关注的话题。

电子商务安全就是保护在电子商务系统里的企业或个人资产不受未经授权的访问、使用、窜改或破坏。电子商务安全覆盖整个电子商务链的各个环节：由客户端→通信传输→服务器端、甚至相关企业的后台信息系统等等。电子商务安全问题已成为电子商务的关键和核心。

电子商务安全的六项中心内容如图 1-1 所示。

1. 商务数据的机密性或保密性。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。

2. 商务数据的完整性或正确性。是保护数据不被未经授权者修改、建立、嵌入、删除、重复传送或由于其他原因使原始数据被更改。

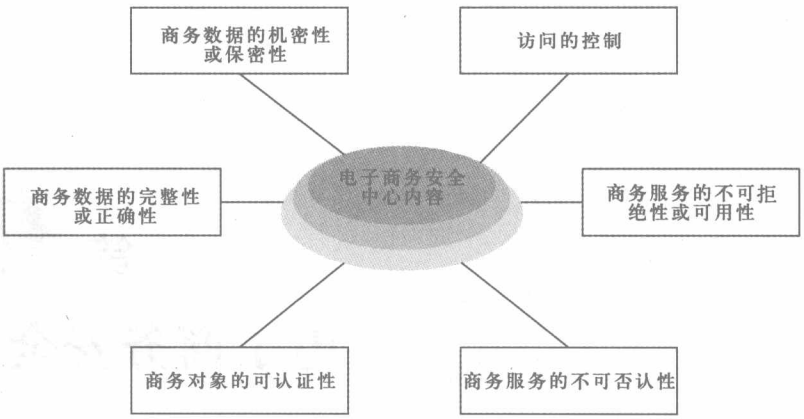


图 1-1　电子商务安全的六项中心内容

3. 商务对象的可认证性。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。是指信息的发送方面不能否认已发送的信息，接收方不能否认已收到的信息，这是一种法律有效性的要求。

5. 商务服务的不可拒绝性或可用性。是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。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、计算和通信资源）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。

1.2 电子商务安全问题

电子商务的安全问题，主要集中于在开放的网络环境中如何保证信息传递中的完整性、可靠性、真实性以及如何预防未经授权的非法入侵者这几个方面。而解决这些问题的方法主要表现在技术，以及在采用和实施这些技术的经济可行性上，这方面是电子商务安全考虑和研究的主要问题，简言之，一是技术上的安全性，二是安全技术的实用可行性。也就是要协调处理好以下三方面的问题：

1. 安全性与方便性。

2. 安全性与性能。

3. 安全性与成本。

电子商务安全的金字塔架构如图 1-2 所示。政策、法律、守则、管理在金字塔的最底部，是电子商务安全实现的基石；安全技术（Internet 防火墙，授权、认证，加密）在金字塔的中部，是电子商务安全实现的核心；审计、监控在金字塔的顶部，是电子商务安全实现的高级形式。

1.2.1 问题的提出

随着电子商务在全球范围内的迅猛发展，电子商务中的网络安全问题日渐突出。根

据中国互联网络信息中心(CNNIC)发布的《中国互联网络发展状况统计报告(2005/7)》,有26.9%的用户认为目前网上交易存在的最大问题是安全性得不到保障;在过去的一年内,有59.4%的用户的计算机曾经被入侵。由此可见,电子商务中的网络安全和交易安全问题是实施电子商务的关键所在。

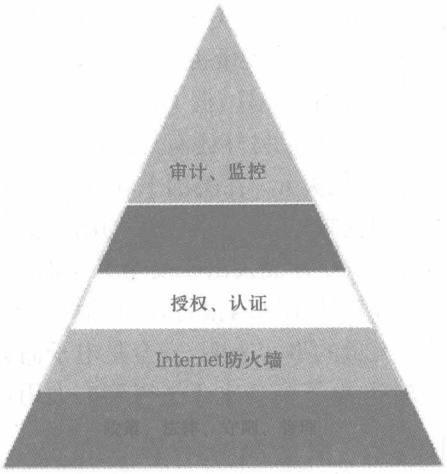


图 1-2 电子商务安全的金字塔架构

自电子商务产生之后,安全事故经常出现。例如:从2000年2月7日至2月9日,短短三天的时间内,美国几大主要网上站点均遭受不明黑客攻击,其中包括著名的电子商务网站电子港湾(eBay)和亚马逊(Amazon)。在黑客开始所谓"拒绝服务(Denial of Service,DoS)"式的攻击后,亚马逊(Amazon)站点容纳顾客的能力急剧下降。数分钟后访客数量只有平时同一时段访客数量的1.5%,大约一小时后亚马逊网站才恢复正常。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高达数十亿美元。

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说,北美、欧洲和亚洲的Internet交通均发生了大面积堵塞,估计至少有22 000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欧洲北部、美国东部和亚洲的一些地区。美国美洲银行称13 000台自动取款机瘫痪,大量银行客户无法使用取款机取款。

在亚洲地区,韩国受害最重。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。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损失,遍布韩国的网吧经营也遭到打击。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组成对策小组恢复系统,阻止了大量数据的继续侵入。

2004年2月,日本雅虎BB公司外泄4 500 000笔个人资料,引起社会指责,雅虎BB以每笔赔偿500日圆平息此事件,总计赔偿约23亿日圆。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"的客户资料疑被外泄,歹徒要求赎金,否则将公开这些资料。迪斯尼乐园针对客户资料泄密事件向十四万客户郑重道歉。2005年2月,NTT DoCoMo公司发生丑闻,大约24 600个客户的数据泄露出去。数据可能是被内部员工从一个被认为很安全的房间偷出去的。

万事达信用卡集团于2005年6月17日称,大约4 000万信用卡顾客账户被一名黑客利用电脑病毒侵入,黑客可能将用户账号信息用作欺诈行为,而且多家银行的顾客账户都遭到了入侵。目前,据悉4 000万用户中,1 390万用户属于万事达公司,2 200万为