网络及电子商务安全

周化祥 主 编
李智伟 副主编

21世纪高等学校应用型规划教材
电子商务系列

中国电力出版社
www.infopower.com.cn

21世纪高等学校应用型规划教材
电子商务系列

网络及电子商务安全

周化祥 主编
李智伟 副主编
李高峰 易锡球 张 震 陈月波
贾志林 朱明松 孙秀平 参编

中国电力出版社
www.infopower.com.cn

内容提要

本书为21世纪高等学校应用型规划教材电子商务系列之一，由具有丰富教学经验的一线教师编写。全书共分为8章，第1章电子商务安全概述，第2章网络安全技术，第3章加密，数字签名与身份认证技术，第4章PHI基础与证书系统，第5章电子商务安全协议与安全标准，第6章电子商务安全防范策略，第7章移动电子商务安全与应用，第8章电子商务法律与法规。全书后面附有实训内容，可供任课教师和同学们结合自身的教学情况选用。本书本着理论够用的原则，注重实践操作和应用能力的培养，以满足目前教学的实际需要。

本书可作为高等学校本、专科、高职电子商务、经济管理等专业教材，也可作为专业工作者工作参考用书。

图书在版编目（CIP）数据

网络及电子商务安全 / 周化祥主编. —北京：中国电力出版社，2004

（21世纪高等学校应用型规划教材·电子商务系列）

ISBN 7-5083-2287-8

I.网... II.周... III.①计算机网络－安全技术－高等学校②技术学校－教材③电子商务－安全技术－高等学校④技术学校－教材 IV.①TP393.08②F713.36

中国版本图书馆CIP数据核字（2004）第075668号

丛 书 名：21世纪高等学校应用型规划教材·电子商务系列

书　　名：网络及电子商务安全

出版发行：中国电力出版社

地址：北京市三里河路6号　　邮政编码：100044

电话：（010）88515918　　传　　真：（010）88518169

本书如有印装质量问题，我社负责退换

印　　刷：汇鑫印务有限公司

开本尺寸：185×233　　**印　　张**：16.75　　**字　　数**：364千字

书　　号：ISBN 7-5083-2287-8

版　　次：2004年9月北京第1版

印　　次：2004年9月第1次印刷

定　　价：24.00元

前　言

随着计算机网络技术和 Internet 的飞速发展，电子商务，特别是通过 Internet 进行的电子商务成为越来越多的人关注的焦点，并出现了各种各样的商务交易方式和电子支付方式。电子商务网站也大量出现。这些给人们的购物方式、消费方式和生活观念带来了巨大的冲击，也更方便了人们的日常生活，真正实现了“足不出户，送货上门”的购物消费理念。

但是，电子商务发展至今，阻碍其发展的关键因素还是安全问题。因为首先其赖以生存的基础是网络，即 Internet/Intranet；其次是其和传统的交易方式完全不同，现在交易的双方不再是面对面的，而是被时空、距离所阻隔，因此其安全问题更为重要。电子商务从最初发展开始，就非常重视安全性，但它仍摆脱不了网络带给它的安全问题。网络安全问题日益突出，它已经影响到一个国家的政治、军事、经济等领域的安全和稳定。目前黑客猖獗，平均每 20 秒世界上就有一次黑客事件发生。因此，提高对网络安全重要性的认识，增强防范意识，强化防范措施，是保证信息产业持续稳定发展的重要保证和前提条件。

各种网络安全事件的发生，使越来越多的人意识到，人们普遍对电子商务安全意识的淡薄和安全人才的缺乏是网络出现安全漏洞的一个非常重要的原因。因此，出现了一批与电子商务安全相关的新兴职业。毫无疑问，电子商务安全知识及其应用技术已成为电子商务从业人员了解和掌握的必备知识，也成为众多学者、研究开发人员、政府人员和管理人员关注的目标。

本书以通俗浅显的语言阐述了目前电子商务安全所涉及的主要技术，主要内容包括：电子商务安全的目标和体系结构、密码技术、数字签名技术、认证技术、密钥管理技术、网络安全技术、常用的安全协议标准和 PKI 技术、移动商务安全技术等。观点新颖，内容丰富，可读性和实践性强，可作为大中专院校相关专业的教材，同时也适合于任何对电子商务和网络安全感兴趣的读者阅读。

本书由中国电力出版社组织编写，并得到中国商业高等职业教育研究会的大力协助。写作提纲由周化祥编写，并经许多大学教授、专家讨论而定。第 1 章由长沙商贸旅游职业学说周化祥和李高峰编写，第 2 章由湖南商业职业学说易锡球编写，第 3 章由安徽商业职业技术学说张震编写，第 4 章由浙江金融职业学说陈月波编写，第 5 章由唐山职业技术学说贾志林编写，第 6 章由长沙商贸旅游职业学说李智伟和朱明松编写，第 7 章由周化祥编写，第 8 章由河北廊坊职业技术学院孙秀平编写，最后周化祥和李智伟负责审稿。

本书涉及面较广，时间紧，加上作者水平有限，疏漏之处在所难免，恳请读者批评指正。有关意见请发电子邮件至 zhouhq98@163.net，不胜感激！

作　者

2004 年 7 月

参加“21世纪高等院校应用型规划教材”编写的院校名单

（排名不分前后）

重庆大学应用技术学院
重庆电子职业技术学院
天津大学管理学院
浙江金融职业技术学院
常州工学院
无锡商业职业技术学院
浙江商业职业技术学院
山东商业职业技术学院
天津工业大学信息学院
深圳职业技术学院
浙江温州职业技术学院
浙江宁波工商职业技术学院
浙江经济职业技术学院
天津商学院
焦作大学
河北唐山职业技术学院
河北廊坊职业技术学院
河北保定金融专科学校
石家庄信息工程职业学院
河南经济管理学院
成都信息工程学院
河南机电高等专科学校
安徽工商职业技术学院
安徽商贸职业技术学院
河北廊坊工业学校
湖南长沙商贸旅游职业学院
天津机电职业技术学院
天津工业职业技术学院
天津大学职业技术学院
江苏淮安信息职业技术学院
齐齐哈尔大学
天津理工学院
天津财经大学
徐州工程学院
重庆大学信息学院
成都大学
西南石油学院
西华大学
常熟理工学院
南通职业大学
常州轻工职业技术学院
山西长治职业技术学院
沈阳药科大学
河南理工大学高等职业学院

目　录

第 1 章　电子商务安全概述

知识要点

- 电子商务安全的概念和特点
- 电子商务面临的安全威胁
- 电子商务的安全要素
- 电子商务安全的四大技术：加密技术、网络安全技术、PKI 技术、安全协议与标准
- 电子商务安全系统的体系结构
- 电子商务安全法律要素

1.1　电子商务安全概述

电子商务（Electronic Commerce）是指政府、企业和个人利用现代电子计算机与网络技术实现商业交换和行政管理的全过程；它是一种基于互联网，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。电子商务的参与者包括企业、消费者和中介结构等。它的本质是建立一种全社会的“网络计算环境”或“数字化神经系统”，以实现信息资源在国民经济和大众生活中的全方位应用。

随着 Internet 的发展，电子商务已经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。电子商务的发展给人们的工作和生活带来了新的尝试和便利，前景十分诱人，也为人们带来无限商机。但许多商业机构对是否采用电子商务仍持观望态度，主要原因是对网上运作的安全问题存有疑虑。在竞争激烈的市场环境下，电子商务的一些信息可能属于商业机密。一旦信息失窃，企业的损失将不可估量。因此，在运用电子商务模式进行贸易的过程中，安全问题就成为电子商务最核心的问题，也是电子商务得以顺利推行的保障。它包括有效保障通信网络，信息系统的安全，确保信息的真实性、保密性、完整性、不可否认性和不可更改性等。

本章主要介绍电子商务安全概念的核心内涵，以及当前的安全处境，即面临的威胁和安全需求，电子商务安全的体系结构等。

1.1.1　电子商务安全概念

电子商务系统是一个计算机网络系统。其安全性是一个系统的概念，不仅与计算机系统结构有关，还与电子商务应用的环境、人员素质的社会因素有关。它包括电子商务系统的硬件安全、软件安全、运行安全和电子商务安全立法等。它的一个重要技术特征是利用 IT 技术来传

输和处理商业信息。因此，电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全。

网络安全是实现电子商务的基础，而一个通用性强，安全可靠的网络安全协议则是实现电子商务安全交易的关键技术之一，它也会对电子商务的整体性能产生很大的影响。目前使用的安全协议有很多，本书将对与电子商务安全协议作介绍，主要包括协议基本情况、协议安全性分析以及应用等。

商务交易安全则紧紧围绕传统商务在互联网络上应用时产生的各种安全问题，在计算机网络安全的基础上，保障电子商务过程的顺利进行。即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。

计算机网络安全与商务交易安全实际上是密不可分的，两者相辅相成，缺一不可。没有计算机网络安全作为基础，商务交易安全就犹如空中楼阁，无从谈起。没有商务交易安全保障，即使计算机网络本身再安全，仍然无法达到电子商务所特有的安全要求。

安全是电子商务的核心和灵魂，没有安全保障的电子商务应用只是虚伪的炒作或欺骗，任何独立的个人或团体都不会愿意让自己的敏感信息，在不安全的电子商务流程中传输。所以，总之一句话：网络应用，安全为本。只要我国坚持在吸收、引进的前提下，组织各方面力量，独立研制和开发具有独立知识产权的网络安全和电子商务安全产品；逐步掌握电子商务安全的核心技术，并从宏观上进行调节和控制；我国的电子商务安全现状一定会得到极大地改善，为我国电子商务的真正发展构筑一道牢不可破的坚固屏障。

1.1.2 电子商务安全的特点

电子商务安全具有如下四大特性。

1. 电子商务安全是一个系统概念

电子商务安全问题不仅仅是个技术性的问题，更重要的是管理问题，而且它还与社会道德、行业管理，以及人们的行为模式都紧密地联系在一起。

2. 电子商务安全是相对的

房子的窗户上只有一块玻璃，一般说来这已经很安全，但是如果非要用石头去砸，那就不安全了。人们不会因为石头能砸碎玻璃而去怀疑玻璃的安全性，因为大家都有一个普遍的认识：玻璃是不能砸的，有了窗玻璃就可以保证房子的安全。同样，不能追求一个永远也攻不破的安全系统，安全与管理始终是联系在一起的。也就是说，安全是相对的，而不是绝对的，要想以后的网站永远不受攻击、不出安全问题是不可能的。

3. 电子商务安全是有代价的

无论是现在国外的 B to B（Business to Business，企业对企业模式）还是 B to C（Business to Customer，企业对消费者模式），都要考虑到安全的代价和成本问题。如果只注重速度，就必定要以牺牲安全来作为代价；如果要考虑到安全，速度就得慢一点。当然这与电子商务的具

体应用有关，如果不直接牵涉到支付等敏感问题，对安全的要求就可以低一些；如果牵涉到支付问题，对安全的要求就要高一些，所以安全是有成本和代价的。作为一个经营者，应该综合考虑这些因素；作为安全技术的提供者，在研发技术时也要考虑到这些因素。

4. 电子商务安全是发展的、动态的

今天安全，明天就不一定安全，因为网络的攻防是此消彼长、道高一尺魔高一丈的事情。尤其是安全技术，它的敏感性、竞争性以及对抗性很强，需要不断地检查、评估和调整相应的安全策略。没有一劳永逸的安全，也没有一蹴而就的安全。

1.1.3 我国电子商务安全现状

我国在电子商务安全方面的基础设施和观念意识令人堪忧。目前，很多的电子商务网站（包括电子支付）的安全机制还依赖于浏览器和 Web 服务器提供的 SSL（Secare Socket Layer，安全套接层协仪）安全协议。而由于出口限制，SSL 协议所采用的安全算法密钥长度只有 40 位或 56 位。以目前的技术水平，破译这种安全强度的信息只需几分钟或更少的时间，而不知内情的用户还以为自己的敏感信息（如信用卡号）在整个交易中是绝对安全的。另外，国内几乎所有的计算机主机、网络交换机、路由器和网络操作系统都来自国外，这种系统有没有留下后门或其他缺陷，用户或国家的机密信息会不会被非法窃取，这些都要求我国下大力气研究和发展独立自主的网络安全和电子商务安全产品。因此，从长远来看，为保证我国电子商务的正常发展，对电子商务中的安全技术进行研究，发展自主的电子商务安全技术是重中之中。

我国信息安全研究经历了多种发展阶段，通过学习、吸收、消化等手段，逐步掌握了部分网络安全和电子商务安全技术，进行了安全操作系统、多级安全数据库的研制探索。但由于系统安全内核受控于人，以及国外产品的不断更新升级，基于具体产品的增强安全功能的成果，难以保证没有漏洞，难以得到推广应用。在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测、电子商务安全交易系统、CA（Certifi-Cate Authority，证书管理机构）认证机构和部分核心密码算法等。但是，这些产品安全技术的完善性、规范化、兼容性和实用性还存在许多不足，理论基础和自主的技术手段需要发展和强化。

总的来说，我国的网络信息安全研究起步晚，投入少，研究力量分散，与技术先进国家有差距，特别是在系统安全和安全协议方面的工作与国外差距更大。然而我国的网络信息安全研究毕竟已具备了一定的基础和条件，尤其是在密码学研究方面积累较多，基础较好，只要国家重视，加大投入，恰当组织，可以取得实质性进展。

1.2 电子商务面临的安全威胁

电子商务在全球范围内的迅猛发展，使电子商务中的网络安全问题日渐突出。在传统交易过程中，买卖双方是面对面的，因此比较容易保证交易过程的安全性和建立起信任关系。但在

电子商务过程中，消费者、商户、银行是通过网络来联系的，彼此远隔千山万水通过网络来完成购物、支付等一系列的商务活动；如果系统安全性被破坏，入侵者就有可能假冒成合法用户来改变用户数据、解除用户订单或生成虚假订单，使商户遭受损失；消费者在将个人数据或自己的身份数据（如口令）发送给商户时，这些信息也可能会在传递过程中被窃听，使消费者受到损失。因此，电子商务系统中交易各方都面临着安全威胁。

一般来说电子商务安全中普遍存在着以下几种安全隐患。

1. 信息的截获和窃取

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关和路由器上截获数据等方式，获取输入的机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析，推出有用信息，如消费者的银行账号、密码以及企业的商业机密等。

2. 信息的篡改

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。

1）篡改：改变信息流的次序，更改信息的内容，如购买商品的出货地址。

2）删除：删除某个消息或消息的某些部分。

3）插入：在消息中插入一些信息，让收方读不懂或接收错误的信息。

3. 信息假冒

当攻击者掌握了网络信息数据规律或解密了商务信息以后，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。

1）伪造电子邮件，虚开网站和商店，给用户发电子邮件，收定货单；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，发大量的电子邮件，窃取商家的商品信息和用户信用等信息。

2）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、栽赃；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。由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨清真伪。

4. 恶意破坏

由于攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机要信息，甚至可以潜入网络内部，其后果是非常严重的。

5. 交易抵赖

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；购买者做了定货单不承认；商家卖出的商品因价格差而不承认原有的交易。

1.3 电子商务安全要素

电子商务随时面临的威胁导致了对电子商务安全的需求，真正实现一个安全电子商务系统所要求做到的各个方面主要包括机密性、完整性、认证性和不可抵赖性等。下面从七个方面分析电子商务的安全要素。

1. 信息的机密性

信息的机密性是指信息在传输或存储过程中不被他人窃取。机密性一般通过密码技术来对传输的信息进行加密处理来实现。

在利用网络进行的交易中，必须保证发送者和接收者之间交换的信息的保密性。如信用卡的账号和用户名等不能被他人知悉，在信息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(尤其 Internet 是更为开放的网络)，维护商业机密是电子商务全面推广应用的重要保障。因此，要预防信息大量传输过程中被非法窃取，必须确保只有合法用户才能看到数据，防止信息被窃看。

2. 信息的完整性

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、统一的问题。造成信息完整性问题，主要来自以下三个方面：

1）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差异；

2）数据传输过程中的信息丢失、信息重复或信息传送的差异也会导致贸易各方信息的不同；

3）黑客对信息的篡改和假冒等。

电子商务系统信息存储必须保证正确无误，为确保数据的可靠性，作为存储介质的磁盘，可采用容错磁盘和磁盘的热修补技术。贸易各方的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复，并保证信息传送次序的统一。

完整性一般可通过提取消息摘要的方式来获得。主要包括两方面。

（1）数据传输的完整性

网络传输所使用的协议具有查错纠错的功能，以保证数据的完整性。在高层信息中，应具有信息投递的确认与通知的功能，以保证传送无误。要确保数据在传递过程中的安全性的真实性，防止数据的丢失和篡改。

（2）完整性检查/上下文检查

对电子商务报文进行完整性检查，抛弃不完整的电子商务文件。对接收电子商务报文数据要进行扫描，按电子商务所规定的语法规则进行上下文检查，不符合语法规则的非法字符将从数据流中被移走。

3. 信息的有效性

电子商务以电子形式取代了纸张，那么如何保证这种电子形式贸易信息的有效性则是开展电子商务的前提。电子商务作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的声誉以及经济利益。一旦签订交易后，这项交易就应受到保护以防止被篡改或伪造。交易的有效性在其价格、期限及数量作为协议一部分时尤为重要。接收方可以证实所接收的数据是原发方发出的；而原发方也可以证实只有指定的接收方才能接收。因此，必须保证贸易数据在确定价格、期限、数量以及确定时刻、地点时是有效的，保证网上交易合同的有效性，防止系统故障、计算机病毒、黑客攻击。要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防。

4. 认证性

由于网络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，要使交易成功，必须做到：首先要能确认对方的身份，对商家要考虑客户端不能是骗子，而客户也会担心网上的商店是不是一个玩弄欺诈的黑店，所以对个人或企业实体进行身份性确认成了电子商务中很重要的一环；其次对人或实体的身份进行鉴别，为身份的真实性提供保证，即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的身份时，鉴别服务将提供一种方法来验证其声明的正确性，一般都通过证书机构 CA 和证书来实现。

5. 信息的不可抵赖性

电子商务可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是进行交易所期望的贸易方这一问题，是保证电子商务顺利进行的关键。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易交易所的书面文件上的手写签名或印章来鉴别贸易伙伴，确定合同、契约、交易所的可靠性，并预防抵赖行为的发生。这也就是人们常说的“白纸黑字”。一旦交易开展后便不可撤销，交易中的任何一方都不得否认其在该交易中的作用。

在无纸化的电子商务方式下，通过手写签名和印章进行贸易方的鉴别已是不可能的了。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。可能出现这样的情况，买方向卖方订购某种建筑材料，订货时世界市场的价格较低，收到订单时价格上涨了，如果卖方否认收到的订单的时间，甚至否认收到订单，那么买方就会受到损失。再比如，买方在网上买了光盘，不能说没有买，谎称寄出的订单不是自己的，而是信用卡被盗用，卖方也同样会受到损失。因此，要求在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识，使原发方在发送数据后不能抵赖；接收方在接收数据后也不能抵赖。因此，要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。不可抵赖性可通过对

发送的消息进行数字签名来获取。

6. 不可修改性

交易的文件是不可被修改的，否则也必然会损害一方的商业利益。因此电子交易文件也要能做到不可修改，以保障商务交易的严肃和公正。

电子商务交易中的安全措施在早期的电子交易中，曾采用过一些简易的安全措施，主要包括以下两点。

1）部分告知（Partial Order）：即在网上交易中将最关键的数据如信用卡号码及成交数额等略去，然后再用电话告之，以防泄密。

2）另行确认（Order Confirmation）：即当在网上传输交易信息后，再用电子邮件对交易做确认，才认为有效。

7. 系统的可靠性

电子商务系统是计算机系统，其可靠性是指防止由于计算机失效、程序错误、传输错误、硬件故障、系统软件错误、计算机病毒和自然灾害等所产生的潜在威胁，并加以控制和预防，确保系统安全可靠性。保证计算机系统的安全是保证电子商务系统数据传输、数据存储及电子商务完整性检查的正确和可靠的根基。

1.4 电子商务安全技术

电子商务安全是信息安全的上层应用，它包括的技术范围比较广，主要分为网络安全技术、密码技术、安全协议、PKI（Public Key Intrastructure，公钥基础设施）技术四大类。实际上安全协议和 PKI 技术都是源于密码技术。

1. 密码技术

加密技术是保证电子商务安全的重要手段，是信息安全的核心技术。它主要包括加密、签名认证和密钥管理三大技术。

1）加密技术是保证电子商务安全的重要手段。所谓加密就是使用数学方法来重新组织数据，使得除了合法的接收者外，任何其他人要想恢复原先的“报文”或读懂变化后的“报文”是非常困难的。许多密码算法现已成为网络安全和商务信息安全的基础。密码算法利用密秘密钥（secret keys）来对敏感信息进行加密，然后把加密好的数据和密钥（要通过安全方式）发送给接收者，接收者可利用同样的算法和传递来的密钥对数据进行解密，从而获取敏感信息并保证了网络数据的机密性。

2）密钥管理技术。密钥管理包括密钥的产生、存储、装入、分配、保护、丢失、销毁以及保密等内容。其中分配和存储是最棘手的问题。密钥管理不仅影响系统的安全性，而且涉及到系统的可靠性、有效性和经济性。在用密码技术保护的现代信息系统的安全性主要取决于对密钥的保护，而不是对算法或硬件本身的保护，即密码算法的安全性完全寓于密钥之中。

3）数字签名。数字签名（Digital Signature）是公开密钥加密技术的一种应用，是指用发送方的私有密钥加密报文摘要，然后将其与原始的信息附加在一起，合称为数字签名。通过数字签名能够实现对原始报文的鉴别与验证，保证报文的完整性、权威性和发送者对所发报文的不可抵赖性。数字签名机制提供了一种鉴别方法，保证了网络数据的完整性和真实性。普遍用于银行、电子贸易等，以解决伪造、抵赖、冒充、篡改等问题。

2. 网络安全技术

网络安全是电子商务安全的基础，一个完整的电子商务系统应建立在安全的网络基础设施之上。网络安全所涉及到的方面比较多，如操作系统安全、防火墙技术、VPN（Virtua Pager Net Work，虚拟专用网）技术和各种反黑客技术和漏洞检测技术等。其中最重要的就是防火墙技术。

防火墙是建立在通信技术和信息安全技术之上，它用于在网络之间建立一个安全屏障，根据指定的策略对网络数据进行过滤、分析和审计，并对各种攻击提供有效的防范。主要用于Internet 接入和专用网与公用网之间的安全连接。

VPN 也是一项保证网络安全的技术之一，它是指在公共网络中建立一个专用网络，数据通过建立好的虚拟安全通道在公共网络中传播。企业只需要租用本地的数据专线，连接上本地的公众信息网，其各地的分支机构就可以在互相之间安全传递信息；同时，企业还可以利用公众信息网的拨号接入设备，让自己的用户拨号到公众信息网上，就可以连接进入企业网中。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等好处，是目前和今后企业网络发展的趋势。

3. 安全协议

安全协议是许多分布式系统安全的基础，是电子商务系统运行的安全通信标准。目前国际上流行的电子商务所采用的协议主要包括以下 4 个方面。

（1）电子支付协议

电子支付作为电子商务中最重要的内容，目前已经出现了很多的电子支付协议。根据人们在现实生活中常见的有基于卡的支付协议、基于支票的支付协议和基于现金的支付协议。著名的有：First Virtual、SSL、SET、iKP、NetBill、E-Cash 等。

（2）安全 HTTP（S-HTTP）

（3）安全电子邮件协议（如 PEM、S/MIME 等）

（4）用于公对公交易的 Internet EDI(UN/EDIFACT)等

此外，也可以在 Internet 上建设虚拟专网，利用 VPN 为企业、政府提供一些基本的安全服务如企业、政府间的公文、报表传送、电子报税业务等。这些协议分别在不同的协议层上进行，在 Internet 上提供安全的电子商务服务。

4. PKI 技术

PKI（公开密钥基础设施）是利用公钥算法原理和技术为网上通信提供通用安全服务的基

础设施。它为电子商务、电子政务、网上银行证券等提供一整套安全基础平台。

密钥管理是电子商务安全业务中共同存在的问题，为解决在 Internet 上开展电子商务的安全问题，世界各国在经多年研究后，初步形成了一套完整的解决方案，即目前被广泛应用的公开密钥基础设施。PKI 采用证书管理公钥，即结合 X.509 标准中的鉴别框架（Authentication Framework）来实现密钥管理，通过 CA 把用户的公钥及其他标识信息捆绑在一起，在 Internet 上验证用户的身份，保证网上数据的保密性和完整性。

PKI 的核心元素是数字证书，其核心执行者是认证机构。有关数字证书服务的应用，实施是广泛开展电子商务的基本前提，电子商务的深入开展离不开数字证书技术和认证机构的正确督导。

1.5 电子商务安全体系结构

一个全方位的计算机网络安全体系结构包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。充分利用各种先进的主机安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术、安全审计技术、安全管理技术、系统漏洞检测技术、黑客跟踪技术，在攻击者和受保护的资源间建立多道严密的安全防线，极大地增加了恶意攻击的难度，并增加了审核信息的数量，利用这些审核信息可以跟踪入侵者。

电子商务的安全体系应包括：安全可靠的通信网络，保证数据传输的可靠完整，防止病毒、黑客入侵；电子签名和其他身份认证系统；完备的数据加密系统等。

图 1.1 是电子商务安全结构的图示，体系结构主要包括四个层次。

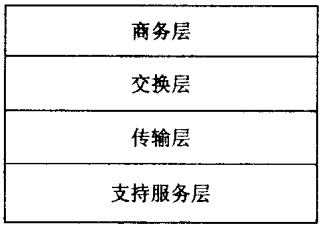

图 1.1 电子商务安全体系结构

1. 支持服务层

包括密码服务、通信、归档、用户接口和访问控制等模块，它提供了实现安全服务的安全通信服务。

2. 传输层

传输层发送、接收、组织商业活动所需的封装数据条，实现客户和服务器之间根据规定的安全角色来传递信息。数据条的基本类型为：签名文本、证书、收据、已签名的陈述信息、数字化的商品、访问某种服务所需的信息、获得物理商品所需的信息等。传输层包括付款模块、文档服务模块和证书服务模块等。

3. 交换层

交换导提供封装数据的公平交换服务。所谓公平是指A和B同意进行交换，则A收到B封装数据条的充要条件是B收到A的封装数据条。

4. 商务层

商务层提供商业方案，如邮购零售、在线销售信息等。

商务层也称一般业务服务层。这一层实现各种网上商务活动与服务，如标准的商品目录/价目表、电子支付工具、保证商务信息安全传送、认证交易各方的合法性、商务活动协同和商品交易等。

1.6 电子商务安全法律要素

安全的电子商务除了依赖于技术因素外，还必须依靠法律手段、行政手段来最终保护参与电子商务各方的利益。法律法规的建设成为当前电子商务发展不可或缺的要素。

开展电子商务需要在企业和企业之间、政府和企业之间、企业和消费者之间、政府和政府之间明确各自需要遵守的法律义务和责任。其主要涉及以下几方面的法律要素。

1. 有关CA中心的法律

CA中心是电子商务中介于买卖双方之外的公正的、权威的第三方，是电子商务中的核心角色，它担负着保证电子商务公正、安全进行的任务。因而必须由国家法律来规定CA中心的合法地位、设立程序和设立资格以及必须承担的法律义务和责任，也必须由法律来规定由谁来对CA中心进行监管，并明确监管的方法以及违规后的处罚措施。

2. 有关保护个人隐私、个人秘密的法律

本着最小限度收集个人数据、最大限度保护个人隐私的原则来制定法律，以消除人们开展电子商务时对泄露个人隐私以及重要个人信息（如信用卡账号和密码）的担忧，从而吸引更多的人上网进行电子商务。

3. 有关电子合同的法律

需要制定有关法律对电子合同的法律效力予以明确；对数字签名、电子商务凭证的合法性予以确认；对电子商务凭证，电子支付数据的伪造、变更、注销做出相应的法律规定。

4. 有关电子商务的消费者权益保护法

网络交易过程中，消费者对商家信誉的信心只能寄托于为交易提供服务的第三方，如CA中心和收款银行等。其中，CA中心能够核实商家的合法身份，收款银行则能掌握商家的信誉情况。一旦因商家不付货、不按时付货或者货不符实而对消费者产生损害时，可以由银行先行赔偿消费者，再由银行向商家追索损失，并降低商家在银行的信誉，或取消商家电子支付的账号，或将商家违规情况记入CA中心的黑名单，甚至取消商家的数字证书。