面向21世纪创新型电子商务专业系列

电子商务安全与支付（第二版）

DIANZISHANGWU ANQUAN YU ZHIFU

主　编　郝莉萍　刘　磊
副主编　杨明莉　成桂玲

中国水利水电出版社
www.waterpub.com.cn

面向21世纪创新型电子商务专业系列

电子商务安全与支付

（第二版）

主　编　郝莉萍　刘　磊

副主编　杨明莉　成桂玲

中国水利水电出版社
www.waterpub.com.cn
·北京·

内 容 提 要

电子商务安全与支付是电子商务运作中密切联系的两个关键环节。本书系统介绍了电子商务安全与支付的基本概念和理论、加密技术、计算机系统安全、网络安全、支付系统以及相关法律法规等内容，并在每章后配有相关知识的延伸阅读资料，以扩展学生的知识面，了解更多相关内容。

本书内容丰富、层次清晰、讲解深入浅出，可供高等院校电子商务类、计算机类、经济管理类等相关专业的学生使用，对从事电子商务及计算机网络工作的技术人员也有一定的参考价值。

本书配有教学课件，读者可以从中国水利水电出版社网站和万水书苑免费下载，网址为：http://www.waterpub.com.cn/softdown/和 http://www.wsbookshow.com。

图书在版编目（CIP）数据

电子商务安全与支付 / 郝莉萍，刘磊主编. -- 2版
. -- 北京 : 中国水利水电出版社，2016.8
面向21世纪创新型电子商务专业系列
ISBN 978-7-5170-4647-9

Ⅰ. ①电… Ⅱ. ①郝… ②刘… Ⅲ. ①电子商务－安全技术－高等学校－教材②电子支付－高等学校－教材
Ⅳ. ①F713.36

中国版本图书馆CIP数据核字(2016)第204043号

策划编辑：石永峰　责任编辑：石永峰　加工编辑：夏雪丽　封面设计：李　佳

书　名	面向21世纪创新型电子商务专业系列 **电子商务安全与支付（第二版）** DIANZISHANGWU ANQUAN YU ZHIFU
作　者	主　编　郝莉萍　刘　磊 副主编　杨明莉　成桂玲
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市鑫金马印装有限公司
规　格	184mm×260mm　16开本　17.5印张　431千字
版　次	2009年12月第1版　2009年12月第1次印刷 2016年8月第2版　2016年8月第1次印刷
印　数	0001—3000册
定　价	36.00元

前　言

随着网络技术普及率的日益提高，通过网络进行购物、交易、支付等的电子商务新模式发展迅速。事实上，电子商务是一种在 Internet 基础上，将电子信息技术和商务活动相结合的商务运作方式。电子商务与传统商务相比，具有鲜明的特性和巨大的优势，一是使商务活动的扩张具有全球性；二是使商务活动的低成本、高效率具有普遍性；三是使买方对商品的购买具有多重选择性。因此，电子商务凭借其低成本、高效率的优势，不但受到普通消费者的青睐，还有效促进了中小企业寻找商机、赢得市场，随着我国政府提出的“互联网+”行动计划，电子商务已成为我国转变发展方式、优化产业结构的重要动力。交易的电子化已经成为信息经济发展的必然趋势，电子商务代表着未来贸易方式的发展方向，它的应用与推广将给社会和经济带来极大的效益。

虽然电子商务的观念逐渐深入人心，但电子商务是在国际化、社会化、开放化和个性化的 Internet 环境中运作的，它的应用可能会带来各种商业信息的泄露、客户的银行账户信息被盗、网站瘫痪、金融欺诈以及缺乏可信性而导致的商业信息丢失等各种安全与信任问题。要在 Internet 开放的网络平台上成功地进行电子交易，必须有效解决网络交易平台的安全性问题，并提供对电子支付过程的保护。网上购物、网上交易、网上支付等环节首先强调的是安全性，电子商务环境下的安全与支付是目前困扰和影响电子商务推广的两个重要问题，因此研究电子商务安全技术和管理措施，就显得更加重要。

本书较为深入和完整地阐述了电子商务安全与支付的基本理论和相关技术，注重理论联系实际，力求将计算机信息安全、网络安全与经济学科有机结合。

全书共 6 章。第 1 章，介绍了电子商务、电子商务安全等相关的基本概念和理论；第 2 章，介绍加密技术及应用、认证技术、电子邮件加密、数据库安全等相关知识；第 3 章，介绍了计算机及其系统的安全，以及计算机病毒、恶意软件等相关知识和防御方法；第 4 章，介绍了与电子商务与支付相关的网络安全基本理论和技术，包括网络安全协议、网络安全设备以及移动互联网的安全；第 5 章，介绍电子商务支付及安全；第 6 章，介绍电子商务安全与支付安全的相关法律保障及法律救济等方面的知识。

本书具有以下特色：

（1）实用性强。本书以技术为主线，突出实际应用，在介绍理论知识的基础上加入实际操作技能的训练，通过本教材的学习能够使学生提高信息技术应用的能力，在从事电子商务活动中增强信息安全意识。

（2）层次结构清晰。本书主要分为三大部分，第一部分包括第 1 章和第 2 章，主要介绍电子商务及安全的基本概念、加密技术及应用、数据库安全等电子商务安全基础知识；第二部分包括第 3 章、第 4 章和第 5 章，主要介绍计算机系统安全、网络安全、支付及其安全问题；第三部分包括第 6 章，介绍电子商务安全的相关法律及法律救济。另外，本书在每章后均有相关知识的延伸阅读资料，以扩展学生的知识面。

本书由郝莉萍、刘磊任主编，杨明莉、成桂玲任副主编。其中第 1 章和第 4 章由郝莉萍

编写，第2章由成桂玲编写，第3章和第6章由刘磊编写，第5章由杨明莉编写。另外，本书在编写过程中参考了众多著作，在文后以参考文献的形式列出，在此对这些著作的作者表示衷心的感谢。

由于时间仓促，编者水平有限，且电子商务安全理论与技术在快速发展中，书中疏漏之处在所难免，恳请广大读者批评指正。

编　者

2016年6月

目　录

第 1 章　电子商务安全概述

20 世纪 90 年代以来，计算机网络技术取得了快速发展，信息网络化和全球化成为不可抵挡的世界潮流。计算机网络技术一直在寻求除文字处理和信息传递领域外的更大、更直接的发展空间，商业领域成为首选，而迅速膨胀的网络用户也为网上更广泛的商业活动的开展提供了基础。

Web 技术的广泛应用，不仅使它具有通信和交换信息的功能，还开辟了一种新的商业交易方式，即在互联网上进行商业交易，实现电子交易处理。

互联网潮流所带来的优势和商机，彻底改变了全球商业的经营模式，许多非信息产业也投入其中，在互联网上可以看到各式各样的商业站点林立。如今，电子商务几乎涉及到人类生活的各个层面和领域。电子商务正在迅速发展，它推动了商业、贸易、营销、金融、广告、运输和教育等社会经济领域的创新和发展，并因此形成了一个新的产业，给各国企业和经济带来新的机遇。此外，越来越多的企业渴望通过导入电子商务来进行业务流程的重组改造，提升企业运作效率、降低经营成本，并且更进一步地优化商品和服务的品质。企业导入电子商务已经成为增强市场竞争力的主要动力。

由此可见，作为网络与商业的结合，电子商务是网络化发展的必然产物，是信息时代的商务模式，它必将有更广阔的发展前景。不过，电子商务绝不是空中楼阁，它的实现需要强有力的技术支撑，在互联网这个公共平台上，依赖强有力的技术支持，尤其是安全技术保障显得尤为重要。

1.1　电子商务及其系统构成

1.1.1　电子商务的定义

近几十年来，商业领域中使用了多种电子通信工具来完成各种交易活动。银行使用电子资金转账（EFT）技术在全球范围内转移顾客的资金；各种企业使用电子数据交换技术，利用增值网（VAN）发出订单和各种凭证；零售商针对各种商品做电视广告以吸引顾客通过电话订货。因而，从更广的意义上来说，电子商务可以通过多种电子通信手段来完成，电子商务早已有之；从狭义上来说，电子商务则是指利用互联网进行的商务活动。

对电子商务的定义至今仍没有一个很清晰的概念。各国政府、学者、企业界人士都根据自己所处的地位和对电子商务的参与程度，给出了许多表述不同的定义。比较这些定义，有助于我们更全面地了解电子商务的内涵。

1. 电子商务的定义

随着电子技术和因特网（Internet，又称国际互联网）的发展，信息技术作为工具被引入商贸活动中，产生了电子商务（Electronic Commerce，EC；Electronic Business，EB）。通俗地说，电子商务就是在计算机网络（主要指 Internet）的平台上，按照一定标准开展的商务活动。

当企业将它的主要业务通过企业内部网（Intranet）、企业外部网（Extranet）以及 Internet 与企业的职员、客户、供销商以及合作伙伴直接相连时，其中发生的各种活动就是电子商务。电子商务的定义有多种说法。下面是一些组织、政府、公司、学术团体等总结的较为全面的定义。

（1）联合国经济合作和发展组织（OECD）在有关电子商务的报告中对电子商务（EC）的定义是：电子商务是发生在开放网络上的包含企业之间（Business to Business）、企业和消费者之间（Business to Consumer）的商业交易。

（2）联合国国际贸易法委员会（UNCITRAL）对电子商务的定义是：电子商务是采用电子数据交换（EDI）和其他通信方式增进国际贸易的职能。

（3）全球信息基础设施委员会（GIIC）电子商务工作委员会报告草案中对电子商务的定义是：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。这种交易的方式不受地理位置、资金多少或零售渠道的所有权影响，公有私有企业、公司、政府组织、各种社会团体、一般公民、企业家都能自由地参加广泛的经济活动，其中包括农业、林业、渔业、工业、私营和政府的服务业。电子商务能使产品在世界范围内交易并向消费者提供多种多样的选择。

（4）国际标准化组织（ISO/IEC）关于电子商务谅解备忘录对电子商务的定义是：电子商务（EB）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。

（5）IBM 公司的电子商务（E-Business）概念：在网络计算机环境下的商业化应用，不仅仅是硬件和软件的结合，也不仅仅是我们通常意义下强调交易的狭义的电子商务（E-Commerce），而是把买方、卖方、厂商及其合作伙伴在因特网（Internet）、企业内部网（Intranet）和企业外部网（Extranet）结合起来的应用。它同时强调这三部分是有层次的：只有先建立良好的 Intranet，建立好比较完善的标准和各种信息基础设施，才能顺利扩展到 Extranet，最后扩展到 E-Commerce。

（6）HP 公司提出电子商务（EC）、电子业务（EB）、电子消费（EC）和电子化世界的概念。电子商务（E-Commerce）的定义是：通过电子化手段来完成商业贸易活动的一种方式。电子商务使我们能够以电子交易为手段完成物品和服务等的交换，是商家和客户之间的联系纽带。它包括两种基本形式：商家之间的电子商务和商家与最终消费者之间的电子商务。电子业务（E-Business）的定义是：一种新型的业务开展手段，通过基于 Internet 的信息结构，使得公司、供应商、合作伙伴和客户之间，利用电子业务共享信息。电子业务不仅能够有效地增强现有业务进程的实施，而且能够对市场等动态因素作出快速响应并及时调整当前业务进程。更重要的是，电子业务本身也为企业创造出了更多、更新的业务运作模式。电子消费（E-Consumer）的定义是：人们使用信息技术进行娱乐、学习、工作、购物等一系列活动，使家庭的娱乐方式越来越多地从传统电视向 Internet 转变。

（7）通用电气公司（GE）对电子商务的定义是：电子商务是通过电子方式进行商业交易，分为企业与企业间的电子商务、企业与消费者之间的电子商务。企业与企业间的电子商务以 EDI 为核心技术，以增值网（VAN）和因特网（Internet）为主要手段，实现企业间业务流程的电子化，配合企业内部的电子化生产管理系统，提高企业从生产、库存到流通（包括物资和资金）各个环节的效率。企业与消费者之间的电子商务以 Internet 为主要服务提供手段，实现公众消费和服务提供方式以及相关付款方式的电子化。

（8）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，全球电子商务将会涉及世界各国。

总结起来，可以这样说：从宏观上讲，电子商务是计算机网络的又一次革命，是通过电子手段建立一种新的经济秩序，它不仅涉及电子技术和商业交易本身，而且涉及诸如金融、税务、教育等社会其他层面。从微观角度说，电子商务是指各种具有商业活动能力的实体（生产企业、商贸企业、金融机构、政府机构、个人消费者等）利用网络和先进的数字化传媒技术进行的各项商业贸易活动。

虽然至今人们尚未对电子商务有一个统一的、明确的定义，但实际上电子商务并非是刚刚诞生的新事物。它的发展历史非常悠久，早在电报出现时，就有了以莫尔斯码点和线的形式在电线中传输的商贸活动，这开辟了运用电子手段进行商务活动的新纪元。商务统计报表认为，世界上真正对电子商务发展的研究开始于 20 世纪 70 年代。对电子商务发展影响最大的是电子数据交换（EDI，Electronic Data Interchange）技术的发展和 Internet 的发展。

1.1.2　电子商务的内涵

对于电子商务，无论广义还是狭义的定义，它们应当具有比较一致的内涵：

（1）电子商务的本质是“商务”，是在“电子”基础上的商务。“商务”解决做什么的问题，而“电子”则解决怎么做的问题。对于高科技的应用是电子商务的手段和效果，而非目的。

（2）电子商务的前提是商务信息化。计算机应用和信息化建设是其基础。它不只是在网上销售商品，还应和企业内部管理、售后服务支持等结合起来，这样的连接必须依靠企业管理信息化。

（3）电子商务的核心是人。电子商务是一个社会系统，它的中心必然是人。电子商务的出发点和归宿是商务，商务的中心是人或人的集合。电子工具的系统化应用也只能靠人。电子商务涉及的人员目前可以分为三类：第一类是技术人员，他们主要负责电子商务系统的实现和技术支持；第二类是商务人员，他们主要负责各种商务活动具体业务的处理；第三类是中高级管理人员，他们的职责是电子商务战略规划、业务流程管理、安全管理等。

（4）电子商务是对传统商务的改良而不是革命。从本质上来说，电子商务并没有脱离传统商务的业务流程，而是将传统商务赖以生存的实物市场交易移到了虚拟的网络空间，在传统环境下开展商务活动的关键因素仍然不可缺少。

（5）电子工具必定是现代化的。所谓现代化工具是指当代技术成熟、先进、高效、低成本、安全、可靠和方便操作的电子工具。

（6）对象的变化也是至关重要的。以往的商务活动主要是针对实物商品进行的商务活动，电子商务则首先要将实物的商品虚拟化，形成信息化（数字化和多媒体化）的虚拟商品，进而对虚拟商品进行整理、存储、加工传输。

1.1.3　电子商务的特征

正如前文所述，电子商务是将企业的业务流程进行改良，即是将信息流、物流和资金流进行分类和重组，以电子化方式通过网络来实现。这一切都必然要依赖于电子商务所蕴含的技术特征和应用特征。

1. 电子商务的技术特征

（1）信息化。电子商务是以信息技术为基础的商务活动，它的进行必须通过计算机网络

系统来实现电子化信息的交换和传输。电子商务的发展与信息技术的发展密切相关，正是信息技术的发展推动了电子商务的发展。

（2）虚拟化。电子商务是在数字化的虚拟电子市场（Electronic Marketplace）进行的。电子商务不受物理时空概念的限制。

（3）集成性。电子商务是一种新兴产物，其中用到了大量新技术，但并不是说新技术的出现就必然导致老设备的死亡。互联网的真实商业价值在于协调新老技术，使用户能更加行之有效地利用已有的资源和技术，更加有效地完成他们的任务。

电子商务的集成性，还在于事务处理的整体性和统一性，它能规范事务处理的工作流程，将人工操作和电子信息处理集成为一个不可分割的整体。这样不仅能提高人力和物力的利用，也提高了系统运行的严密性。

（4）可扩展性。要使电子商务在变化的商业环境里正常运行，必须保证其可扩展性。电子商务中，耗时仅 2min 的重新启动也可能导致大量客户流失，因而可扩展性极其重要。

1998 年日本长野冬奥会的官方万维网节点的使用率是有史以来基于互联网应用中最高的，短短的 16 天，该节点就接受了将近 6 亿 5 千万次访问。全球体育迷将数以百万计的信息直接通过体育迷电子邮件节点发给运动员，而与此同时，还成交了 600 多万笔交易。这些惊人的数字说明，随着技术的日新月异，电子商务的可扩展性将不会成为瓶颈所在。

（5）安全性。安全性是电子商务中的核心问题。缺乏安全的电子商务不可能吸引顾客，企业和企业的交易更是如此，也会限制企业运用计算机网络传递商业信息。欺骗、窃听、病毒和非法入侵等攻击行为都无时无刻不在威胁着电子商务，要求电子商务经营者提供一种端到端的安全解决方案。安全技术包括加密解密机制、认证技术、安全交易协议、计算机网络系统的安全管理（存取管理、防火墙、安全服务器等）。目前，有代表性的安全电子交易协议主要有安全套接层（SSL）和安全电子交易（SET）等。电子商务安全技术的发展和标准的制定，逐步使电子商务企业能够建立起安全的电子商务环境。

（6）系统性。电子商务系统的实施必须考虑企业外的合作伙伴或政府，必须规划如何加入到已有的电子商务系统中。

2. 电子商务的应用特征

（1）商务性。电子商务最基本的应用特性为商务性，即提供买、卖交易的服务、手段和机会。网上购物提供一种客户所需要的方便途径。因而，电子商务对任何规模的企业而言，都是一种机遇。

就商务性而言，电子商务可以扩展市场，增加客户数量；通过将互联网信息连至企业后端的数据库，企业能记录下每次访问、销售、购买形式、购货动态以及客户对产品的偏爱，这样企业就可以通过统计这些数据来获知客户最想购买的产品是什么。

（2）服务性。电子商务时代企业越来越重视客户的需求，这种需求不仅仅是产品的，同时也包括服务的。互联网应用使得企业能自动处理商务过程，并不再像以往那样强调公司内部的分工。企业通过将客户服务过程移至互联网上，使客户能以一种较过去更加简捷的方式获得服务。显而易见，电子商务提供的客户服务具有一个明显的特性：便利。例如比利时的塞拉银行，通过电子商务，使得客户能全天候地存取资金账户，快速及时地阅览相关利率信息，服务质量大为提高。

（3）协调性。商务活动是一个需要各方协调的过程，许多组织都提供了交互式的协议，

电子商务活动可以在这些协议上完成。

传统的电子商务解决方案能加强公司内部相互作用，电子邮件就是其中一种。但那只是协调员工合作的一小部分功能。利用互联网将供货方连接至客户订单处理系统，这样公司就节省了时间，消除了纸张文件带来的繁琐过程，提高了效率。

（4）社会性。从宏观上讲，电子商务是计算机网络的第二次革命，是在通过电子手段建立一个新的经济秩序。它不仅涉及电子技术和商业交易本身，还涉及诸如金融、税务、教育等社会其他层面，以及使用电子虚拟市场的法律和竞争规则形成等。电子商务的发展和应用是一个社会性的系统工程，缺少任何一个环节都势必影响它的发展，如电子商务交易的税收等敏感问题。

（5）全球性。Internet 是一个公共开发的平台，根据美国互联网协会的定义，互联网是一种“组织松散、国际合作的互联网络”，是一种由 TCP/IP 组织起来的国际互联网络。电子商务面对的是一个全球性统一的电子虚拟市场。它为企业跨国发展提供了平等的竞争机会。

1.1.4　电子商务系统构成

1. 电子商务系统的分类

在了解了电子商务的内涵后，本节进一步讨论电子商务的分类和构成。对于不断发展的各类电子商务系统，可以从不同的角度进行分类。

（1）按照商品交易过程完整程度分类。

1）完全电子商务：是指产品或服务的交易过程（信息流、物流和资金流）都在网上实现的电子商务。一些数字化的无形产品和服务，如计算机软件、电子书籍、娱乐内容（影视、游戏、音乐等）、远程教育、网上订房、网上订票以及电子证券等，供求双方直接在网络上完成订货或申请服务、货款的电子支付与结算、实施服务或产品交换（即从网络上下载产品等）的全过程，而无需借助其他手段。

2）不完全电子商务：是指商品交易的全过程不能完全在网络上实现的电子商务。一些物质和非数字化的商品交易只能在网络上完成信息流和资金流，而物流的完成则需要借助于其他一些外部辅助系统，如企业自营物流系统、第三方物流系统及第四方物流系统。

（2）按照使用网络的类型来分类。

1）基于 EDI 的电子商务：按照国际标准化组织（ISO）的定义，EDI 就是指“将商业或行政事务处理按照一个公认的标准，形成结构化的事务处理或文档数据格式，从计算机到计算机的电子传输方法”。EDI 通过传递标准数据流可以避免人为的失误，降低成本，提高效率。在 20 世纪 80 年代末，发达国家 EDI 的迅速发展，不仅引发了全球范围的无纸贸易热潮，同时也促进了与商务过程有关的各种信息技术在商业、制造业、基础工业及服务业的广泛应用，实现了商务运作全过程的电子化。

2）基于 Internet 的电子商务：20 世纪 90 年代以来，Internet 风靡全球，基于 Internet 的电子商务应运而生。这时的电子商务是基于计算机和软件以及在通信网络上从事的经济活动。通过这种方式，人们可以利用 Internet 来进行交流和从事电子交易活动。

3）基于 Intranet 的电子商务：Intranet 是在 Internet 基础上发展起来的企业内部网，或称内联网，用以实现企业内部业务处理、管理和通信。

（3）按照交易对象分类。

1）企业对企业的电子商务（Business to Business，B2B）：采购商和采购商在 Internet 上进行谈判、订货、签约、接收发票和付款，以及索赔处理、商品发送管理和运输跟踪等所有活动。

2）企业对消费者的电子商务（Business to Consumer，B2C）：是指企业通过 Internet 为消费者提供的实现订购商品或服务的活动。企业对消费者的电子商务基本上表现为网上在线零售形式，如书籍、鲜花、计算机、汽车等。

3）企业对政府的电子商务（Business to Government，B2G）：覆盖企业与政府之间的各项事务如政府采购、税收、商检、管理条例发布以及法规政策的颁布等。

4）消费者对政府的电子商务（Consumer to Government，C2G）：是指消费者与政府之间进行的电子商务和事务合作活动，包括政府面向个人消费者的电子政务。如个人网上纳税、网上事务审批、电子身份认证和社会福利金的支付等。

5）消费者对消费者的电子商务（Consumer to Consumer，C2C）：是指消费者与消费者之间在网上进行的电子商务或网上事务合作活动。多数为小额的交易，如通过互联网进行个人财物的拍卖活动等。

2. 电子商务系统的基本组成

电子商务系统的基本组成有计算机网络、用户、配送中心、认证中心、银行、商家等，如图 1.1 所示。网络包括 Internet、Intranet、Extranet；用户分为个人用户和企业用户；认证中心（CA）是受法律承认的权威机构，负责发放和管理电子证书，使网上交易的各方能互相确认身份；物流中心接收商家的送货请求，组织运送无法从网上直接得到的商品，跟踪商品的流向，将商品送到消费者手中；网上银行在 Internet 上实现传统银行的业务，为用户提供 24 小时实时服务。

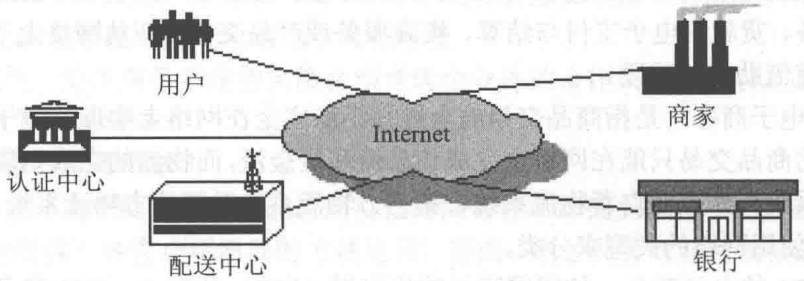

图 1.1 电子商务的基本组成

1.2 电子商务安全

Internet 拉近了人们之间的空间距离，使人们在 Internet 上进行交易时根本不需要考虑地域的概念，不论身在何处，都可以随时交易。Internet 使交易双方在交易过程中无需面对面，这方便了交易各方，但也带来了极大的安全隐患。例如，交易各方的通信有没有安全保障？交易各方的身份是否真实？交易的结果是否具有效力？如果电子商务交易的安全不能得到保证，人们一定不会选择网上购物。因此，如何保证电子商务交易双方的安全，就成为普及电子商务的关键。

1.2.1　电子商务安全概述

电子商务一个重要的技术特征就是利用互联网技术来传输和处理商业信息。因此，电子商务安全可以从整体上分为两大部分：计算机网络安全和商务交易安全。计算机网络安全主要是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，以此来保证计算机网络自身的安全性为目标，主要包括设备安全、计算机网络系统安全、数据库安全等；商务交易安全则紧紧围绕传统商务在互联网上应用时可能遇到的各种安全问题，在计算机网络安全的基础上，保障以电子交易和电子支付为核心的电子商务过程的顺利进行。因此，电子商务安全就是在网络安全基础上，运行安全的电子商务，保障以电子交易和电子支付为核心的电子商务交易的安全。

1. 电子商务安全的表现

（1）信息安全。

信息安全是指由于各种原因引起的信息泄露、信息丢失、信息篡改、信息虚假、信息滞后、信息不完善等，以及由此带来的风险。具体的表现有：窃取商业机密、泄露商业机密、篡改交易信息、非法删除交易信息、破坏信息的真实性和完整性、接收或发送虚假信息、盗取交易成果、伪造交易信息、非法删除交易数据、交易信息丢失、病毒破坏、黑客入侵等。

信息被非法窃取或泄露可能会给有关企业和个人造成严重的后果、带来巨大的经济损失；如果不能及时得到准确完备的信息，企业和个人就无法对交易进行正确的分析和判断，做出理性的决策；非法删除交易信息和交易数据丢失可能导致经济纠纷，给交易的一方或者多方造成经济损失。

（2）交易安全。

交易安全是指电子商务交易过程中存在的各种不安全因素，包括交易的确认、产品和服务的提供、产品和服务的质量、价款的支付等方面的问题。

由于电子商务不同于传统商务的市场松散化、主体虚拟化、交易网络化、货币电子化、结算瞬间化等特点，导致电子商务交易的风险表现出新的形式并且风险被放大。交易安全问题在现实中的表现主要有：卖方利用信息优势，以次充好，发布虚假信息、欺骗消费者，这种情况在淘宝网等电商平台上尤其常见。卖方利用参与者身份的不确定性与市场进出的随意性，在提供服务方面不遵守承诺，或者买方不遵守承诺。

（3）财产安全。

财产安全是指由于各种原因造成电子商务参与者面临的财产等经济利益风险。财产安全往往是电子商务安全问题的最终形式，也是信息安全问题和交易安全问题的后果。

财产损失主要表现为财产损失和其他经济损失。前者如客户银行资金被盗，交易者被冒名，其财产被冒领；后者如信息的泄露、丢失导致企业的信誉受损，遭遇网络攻击和故障导致电子商务系统效率下降或者瘫痪等。

2. 电子商务网上交易的安全性

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

（1）机密性。

机密性是指保证信息为授权者享用而不泄露给未经授权者。在电子商务系统中，交易中

发生、传递的信息均有保密的要求。如果信用卡的账号和用户名被知悉就有可能被盗用；订货和付款的信息被竞争对手获悉，就有可能丧失商机。因此在电子商务的传播中，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。电子商务建立在一个较为开放的网络环境上，维护商业机密是电子商务全面推广的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取，机密性一般通过密码技术对传输的信息进行加密处理来实现。

（2）完整性。

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

电子商务简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商业信息完整性的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的不一致。此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。

（3）可用性。

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

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

（4）可认证性。

认证是指提供对通信中对等实体和数据来源的鉴别。

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

（5）抗抵赖性。

抗抵赖是指防止参与某次通信交换的任何一方事后否认本次通信或通信的内容。

由于商情千变万化，交易一旦达成是不能被否认的，否则必然会损害一方的利益。例如订购黄金，订货时进价较低，但收到订单后，金价涨了，如何处理？因而要通过交易合同、契约或贸易单据等书面文件上手写签名或印章，来确定合同、契约、单据的可靠性并预防抵赖行为的发生。在无纸化的电子商务方式下，通过手写签名和印章来预防交易过程中的抵赖行为已不现实，这就需要在交易信息传输过程中为参与交易的个人、企业或国家提供可靠的电子标识，预防数字世界里的抵赖行为。

综上所述，要保证电子商务实施过程中的机密性、完整性、可用性、可认证性和抗抵赖性，需要数据加密技术、消息摘要、数字签名、认证技术和 SSL 安全协议等多种技术共同完成。

1.2.2　电子商务安全现状

1. 电子商务的安全问题日益受到重视

以 Internet 技术为基础的电子商务，每天需要进行千百万次的交易。Internet 本身是一个高度开放性的网络，这与电子商务所需要的保密性是矛盾的，而 Internet 又没有完整的网络安全体制。因此，基于 Internet 的电子商务在安全上无疑会受到严重威胁，电子商务交易的安全性问题将是实现电子商务快速健康发展的关键。

在电子商务的发展过程中，各产业对网络的技术依赖达到空前的程度。军事、经济、社会、文化各方面都越来越依赖于网络。这种高度依赖性使社会变得十分“脆弱”，一旦计算机网络受到攻击不能正常运作时，整个社会就会陷入危机的泥沼。因此，电子商务安全日益受到各国的高度重视。

2. 黑客的威胁上升

随着经济信息化进程的加快，计算机网络上黑客的破坏活动也随之猖獗起来。黑客及黑客行为已对经济秩序、经济建设、国家信息安全构成严重威胁。“黑客”是英语“Hacker”的音译，原意是指有造诣的电脑程序设计者，现在则专指那些利用自己掌握的电脑技术偷阅、篡改或窃取他人机密数据资料，甚至在网络上犯罪的人，或者是指利用通信软件，通过网络非法进入他人的电脑系统，截获或篡改他人计算机中的数据，危害信息安全的电脑入侵者。

黑客的袭击在网络应用发达的国家造成的危害尤为严重。在这些国家，黑客组织在 Internet 上公开网址、信道，提供免费的黑客工具软件，介绍黑客手法，出版网上黑客杂志和书籍，因此普通人很容易学会各种网络攻击方式。目前，国际黑客对各国计算机系统中高度保密信息的攻击和窃取越来越频繁。例如，黑客对美国国防部计算机系统的攻击行动每年达 25 万次以上，并且还在不断增长。

电子商务系统在防不胜防的破坏性活动面前有时会显得软弱无力，谁都无法预测将会受到什么样的威胁。信息安全漏洞之所以难以堵塞，一方面是由于缺乏统一的信息安全标准、密码算法，协议在安全与效率之间难以两全；另一方面则是由于大多数管理者对网络安全不甚了解。另外，信息犯罪属于超越国界的高技术犯罪，要用现有的法律来有效地防范十分困难，现有的科技手段也难以侦察到计算机恐怖分子的行踪，罪犯只需要一台计算机、一根网线、一个网卡就能远距离作案。

上述种种原因，无形中加大了依法惩治黑客犯罪行为的难度，给反黑客工作带来相当大的困难。一方面，科学家很难开发出对保障网络安全普遍有效的技术，另一方面又缺乏足以保证网络安全措施得到实施的社会环境。随着 Internet 的普及，电子商务安全问题已成为信息时代必须尽快加以解决的重大课题。此外，基于 Internet 的电子商务在迅速发展，不难想象，黑客的攻击一旦得逞，整个商务系统瘫痪，将会造成多么巨大的损失。

3. 计算机网络病毒给电子商务造成的损失继续增加

目前电子商务的安全问题比较严重，突出表现在计算机网络安全和商业诚信问题上。计算机网络病毒给电子商务造成了非常大的损失，可以这样说，没有哪一台计算机没有感染过计算机病毒，绝大多数计算机都受到过计算机病毒的破坏。

（1）木马病毒爆炸性增长，变种数量快速增加。

据统计，2015 年 1～6 月，瑞星“云安全”系统共截获新增病毒样本 1924 万余个，新增