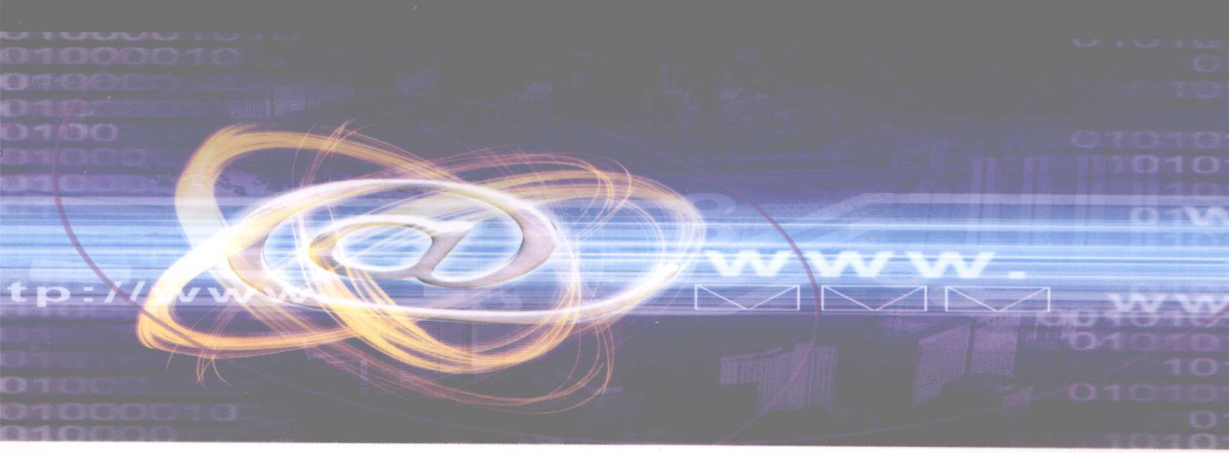

普通高校经济及管理学科规划教材

电子商务专业

电子商务安全与法律

奚宪铭 鞠成东 刘科文/编著

经济科学出版社
中国铁道出版社

普通高校经济及管理学科规划教材

电子商务专业

电子商务安全与法律

奚宪铭　鞠成东　刘科文　编著

经济科学出版社
中国铁道出版社

图书在版编目（CIP）数据

电子商务安全与法律／奚宪铭，鞠成东，刘科文编著.
北京：经济科学出版社，2008.12
普通高校经济及管理学科规划教材．电子商务专业
ISBN 978-7-5058-7720-7

Ⅰ.电… Ⅱ.①奚…②鞠…③刘… Ⅲ.①电子商务-安全技术-高等学校-教材②电子商务-法规-中国-高等学校-教材 Ⅳ.F713.36 D922.294

中国版本图书馆CIP数据核字（2008）第188467号

责任编辑：纪晓津
责任校对：徐领柱
版式设计：代小卫
技术编辑：董永亭

电子商务安全与法律
奚宪铭 鞠成东 刘科文 编著
经济科学出版社出版、发行 新华书店经销
社址：北京市海淀区阜成路甲28号 邮编：100142
总编室电话：88191217 发行部电话：88191540
网址：www.esp.com.cn
电子邮件：esp@esp.com.cn
北京欣舒印务有限公司印刷
华丰装订厂装订
787×1092 16开 24印张 430000字
2009年1月第1版 2009年1月第1次印刷
印数：0001—5000册
ISBN 978-7-5058-7720-7/F·6971 定价：35.00元

普通高校经济及管理学科规划教材
编审委员会

总　序

人类社会已经迈入21世纪。追溯20世纪，管理理论与实践得到了飞速发展，研究领域不断拓宽，从初期的经验管理到后期的科学管理，从工业化时代的规模经营管理到信息化时代的基于信息基础的企业再造，从注重等级和控制的“金字塔”式组织模式到基于网络和知识的“柔性”组织模式，这些，无论是在管理的理念、方法上，还是在管理的技术、实践上都发生了巨大变化。在我国实施改革开放政策以来，社会各界掀起了一浪高过一浪的管理热潮，管理学界相继发生了一系列重大的变革。1994年教育部批准在9所重点高校试点举办工商管理（MBA）硕士研究生教育；1996年国家自然科学基金委员会管理学科组升格为管理学部；1997年在教育部学科专业目录调整过程中，管理学同经济学并列成为独立的一级学科；2002年管理学界的专家首次当选为中国工程院院士。这些重大的变革标志着管理学科的重要地位得到了我国社会各界的认可。

随着我国市场经济体制的不断完善，以及中国正式加入世界贸易组织（WTO），中国经济需要面对国际大市场，企业要参与国际化的激烈竞争。经济及管理教育如何迎接21世纪的挑战，适应时代的需要，已经成为学术界亟须研究与探讨的焦点问题之一。著名管理学家彼得·F·德鲁克（Peter F. Drucker）曾经指出：“对我们的社会来说，管理是一种最显著的创新。”另一名著名管理学家亨利·明茨伯格（Henry Mintzberg）也曾指出：“彻底重塑传统管理教育的时代已经来临。”在这种社会呼唤“管理教育创新”的背景下，组织一套适应21世纪要求的经济及管理类学科规划教材是非常必要和及时的。

普通高校经济管理类专业教学协作会，是由辽宁、吉林、黑龙江、内蒙古、河北、河南、山东、山西、广东及北京、天津的数十

所高校经济管理院系自发形成的教学协作组织。协作会成立16年来，以团结友谊、精诚合作、优势互补、共同发展的精神，坚持在管理理论的创新与实践、学科建设与发展、教材规划编写，以及人才培养与校际交流等方面进行探索，取得了丰硕成果。此套规划教材的组织编写，是协作会面向21世纪经济及管理教育创新的又一力作。

为了保证规划教材的质量和水平，我们成立了由国内外知名专家、教授及管理学院院长、出版社的领导及专家组成的编审委员会。各门教材（包括专业教材、专业基础教材和基础教材）将采取合作的方式由具有丰富教学与研究实践经验的教师主编，相关院校参加编写。规划教材的编写力求博采众家之长，把握管理前沿，注重理论与实践相结合，使之成为具有科学性、规范性、创新性、实用性并举的精品教材及新教研成果。在各位专家与老师的辛勤耕耘下，现已出版了“电子商务专业”、“物流管理专业”、“公共事业管理专业”、“会计学专业”和“财务管理专业”等系列教材，其余经管学科各专业系列教材，亦将陆续出版。

由于经济及管理是一个不断变化和发展的重要学科，新的理论、技术和方法将会大量引用。鉴于我们的水平所限，规划教材在编写过程中难免存在疏漏与不足之处，敬请各位专家批评指正。

天津大学管理学院院长、教授、博士生导师
教育部管理科学与工程专业教学指导委员会主任委员

2008年7月于津

前　言

随着电子商务的迅速发展和普及，电子商务的安全问题日益突出，已经成为影响电子商务快速发展的瓶颈之一。如何解决好电子商务的安全问题，树立人们参与电子商务的信心，是进一步推动电子商务加速发展的关键。电子商务安全问题是一个系统的概念，必须从组织上、技术上、管理上以及法律法规上等多层次进行全面考虑和研究，并制定出一个立体交叉防御体系措施，才能够很好地加以解决。电子商务是新世纪经济的增长点，代表着21世纪经济的发展方向，特别是对未来社会经济的发展和商务活动具有十分重要的意义，因而保证电子商务的安全，就是为推动这一新经济的发展进行保驾护航。

本书旨在介绍最新的电子商务安全与法律知识，以及实现电子商务安全的各种相关技术，并通过大量的相关案例分析，为实现电子商务的安全提供了解决方案。全书共分为十章，其中第1章“电子商务安全概述”、第2章“电子商务安全技术及管理策略”和第10章“电子商务安全解决方案”由哈尔滨商业大学刘科文编写；第3章“加密技术”、第4章“密钥管理技术”、第5章“认证技术”、第6章“PKI公钥基础设施与认证体系”和第7章“电子商务安全协议”由哈尔滨商业大学鞠成东编写；第8章“电子商务法基础”和第9章“电子商务法内容”由哈尔滨商业大学奚宪铭、鞠成东编写。全书由奚宪铭统编定稿。

本书作为电子商务系列教材之一，可以作为电子商务专业、计算机专业、应用数学专业及其他相关专业的本、专科教材或参考书，亦可供从事电子商务安全的有关应用人员使用。

本书在编写过程中，一方面着重阐述了电子商务安全与法律的基础知识与理论；另一方面紧跟电子商务安全与法律的发展潮流，注意吸收新理论、新发展；与此同时还通过各种最新的案例分析，为实现电子商务安全提出了解决方案。因此，本书作者参考和借鉴了大量的出版物和网上资料，由于编写体例的限制，没有在文中一一注明，只在参考文献中列出。

在此谨向各位学者表示诚挚的谢意。由于电子商务安全与法律近年来发展太快，加之作者水平有限，本书尚有许多不足之处，恳请各位专家和读者批评指正。

编著者

2008 年 11 月

目　录

第1章

电子商务安全概述

〖学习目标〗

- 理解电子商务安全的内涵和特点
- 了解电子商务面临的安全威胁
- 掌握电子商务的安全需求、基本技术
- 深刻地理解电子商务安全的体系结构

〖关键术语〗

电子商务　电子商务安全　安全体系结构　电子商务法　移动电子商务安全

1.1　电子商务安全概况

随着计算机网络技术的飞速发展，尤其是电子商务的应用变得越来越广泛，在带来前所未有的海量信息以及电子交易便利性的同时，网络的开放性和自由性也产生了私有信息和数据被破坏或侵犯的可能性，电子商务安全性变得日益重要起来，已被信息社会的各个领域所重视。

电子商务是以因特网为媒介、以商品交易双方为主体、以银行电子支付与结算为手段的全新商务模式，通过电子化形式将客户及供应商信息实时管理，从而使产品和服务能更高效地流通和实施。相对于传统商务，电子商务对管理水平、信息传输技术等都提出了更高的要求，其中安全体系的构建尤为重要，

如何有效地保证电子商务的安全性已经成为电子商务能否得到全面推广的核心和关键，这也是目前电子商务应用研究的热点之一。

1.1.1 电子商务安全的内涵及特点

1.1.1.1 电子商务安全的内涵

电子商务的安全是一个广泛而系统的概念，不仅包含着计算机系统结构、网络通信技术、电子商务应用环境、人员素质等方面的安全，而且还与电子商务立法息息相关。电子商务安全包括物理安全、信息安全、通信安全、交易安全和管理安全五个部分。

1. 物理安全

计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提。物理安全的作用是保护计算机网络设备、设施和其他数据信息免遭自然威胁、人员威胁和环境威胁。其中，自然威胁包括洪水、地震、火灾、龙卷风、电力风暴以及其他类似事件；人员威胁包括由人产生的威胁，如无意行动（偶然的数据访问、误操作等）或有意的行动（基于网络的攻击、恶意软件上传和机密数据的非授权访问等）；环境威胁包括长期电力故障、污染、化学和液体泄漏等。

2. 信息安全

信息安全概括了一般性的安全技术问题。通常系统可能遭受的攻击分为以下几类：窃听、伪装、报文篡改、渗透、流量分析和拒绝服务等。目前针对这些攻击主要采取加密技术、数字签名技术、访问控制技术、数据完整性技术和身份认证技术等。信息安全主要涉及信息传输安全、信息存储安全和对网络传输信息内容的审计三个方面。

3. 通信安全

通信网络是交换信息的基本设施，TCP/IP 协议没有考虑安全问题，因此协议的每一层都存在相应安全威胁。针对通信协议中的最常出现的安全威胁，实施相应的安全协议以实现网络通信的安全。例如，采用防火墙技术、虚拟专网（VPN）技术、入侵检测技术、漏洞检测技术和病毒防护技术等。

4. 交易安全

由于电子商务是以电子的方式通过网络进行的商务活动，参与的双方通常互不见面，而使用的货币以电子货币为主，因此身份的确认和安全通信变得十

分重要。同时，为了在用户、商家和银行之间能够实现资金流动，需要安全的电子交易协议。

5. 管理安全

面对电子商务安全的脆弱性，除了在设计上增加安全服务功能，完善系统的安全保密措施外，还需要花大力气加强网络安全管理。由于诸多不安全因素恰恰反映在法律规范、组织管理和人员录用等方面，因此，这是电子商务安全所必须考虑的基本问题之一。

1.1.1.2　电子商务安全的特点

电子商务安全具有系统性、相对性、代价性和发展动态性四大特点。

1. 系统性

电子商务安全不仅涉及到技术性、管理性、认证性等方面的问题，也与社会道德、行业自律、法律法规息息相关，并且还与人们的行为模式紧密地联系在一起。所以任何参与电子商务的人们，必须建立立体交叉防御体系，才能全面实现电子商务的安全保障。

2. 相对性

电子商务安全是相对的，而不是绝对的。任何电子商务网站都是建立在开放的互联网上，必然会受到来自各种有意的或无意的、自然的或人为的破坏或攻击行为，不出现安全问题是不可能的。问题是如何使电子商务安全通过有效控制，能够达到一个基本的安全保障点。

3. 代价性

开展电子商务的商家要实现电子商务安全，必须考虑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作为代价；如果要达到更高的安全，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；相反，对安全的要求就要高一些。所以无论是经营者还是技术提供者，都应该综合考虑这些因素。

4. 发展动态性

电子商务安全是不断发展的和动态变化的，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。这就需要从事电子商务的商家，不断地检查、评估和调整相关的安全防范策略。没有一劳永逸的安全，也没有一蹴而就的安全。

1.1.2 电子商务面临的安全威胁

在传统交易过程中，买卖双方是面对面的，因此很容易建立相互信任关系，并能够保证交易过程的安全性。但是在电子商务交易过程中，人们是通过互联网络建立联系，甚至彼此之间远隔万水千山，因而建立交易参与各方的安全性和信任关系相当困难。一旦遭遇黑客的侵袭和破坏就可能给消费者、商家和银行中的一方或多方带来损失。因此，在电子商务交易过程中，交易各方都面临着安全威胁。

1. 信息在网络的传输过程中被截获

攻击者通过互联网、公共电话网、搭线或在电磁波辐射范围内安装接收装置等方式，截获传输的机密信息，或通过对信息流量、流向、通信频率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、密码等。

2. 传输的文件可能被篡改

攻击者可能从三方面破坏信息的完整性：

（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. 假冒他人身份

（1）冒充他人身份，如冒充领导发布命令、调阅文件；

（2）冒充他人消费；

（3）冒充主机欺骗合法主机及合法用户；

（4）冒充网络控制程序，套取或修改使用权限、密钥等信息；

（5）接管合法用户，欺骗系统，占用合法用户的资源。

4. 伪造电子邮件

（1）虚开网站和商店，给用户发电子邮件，收购货单；

（2）伪造大量用户，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；

（3）伪造用户，发大量的电子邮件，窃取商家的商品和用户信用等信息。

5. 抵赖行为

（1）发信者事后否认曾经发送过某条内容；

（2）收信者事后否认曾经收到过某些消息或内容；

（3）购买者发出订货单后不承认；

（4）商家卖出的商品因价格变化而不承认原有的交易。

1.1.3　电子商务的安全需求

由于 Internet 本身的开放性及目前网络技术发展的局限性，使电子商务系统面临着各种各样的安全威胁，因此，对电子商务的安全性提出了很高的要求。

（1）有效性。电子商务系统应有效防止系统延迟和拒绝服务情况的发生，要对网络故障、硬件故障、操作错误、应用程序错误、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，保证交易数据在确定的时刻、确定的地点是有效的。

（2）保密性。系统应能对公众网络上传输的信息进行加密处理，防止交易中信息被非法截获或读取，防止通过非法拦截会话数据获得账户有效信息。

在传统交易中，一般通过面对面的信息交换，或者通过邮寄或可靠的通信渠道发送商业报文，达到商业保密的目的。而电子商务交易各方通过因特网交换信息，网络的开放性使其他人可能知道通信内容。同样，存储在网络上的文件信息如果不加密的话，也可能被黑客窃取。因此，必须对重要信息进行加密，即使中间被人截获或窃取了数据，也无法识别信息的真实内容，这样就可以确保商业机密信息不被泄露。

（3）完整性。电子商务系统应防止对交易信息的随意生成、修改和删除，同时防止数据传输过程中交易信息的丢失和重复，并保证信息传递次序的统一。

当网络面临主动攻击时，攻击者通过篡改或部分删除交易过程中发送的信息，破坏信息的完整性，使交易双方蒙受损失。例如，A 给 B 发了如下一份报文：“请给 C 汇 100 元”。报文在传输过程中遭到 D 的篡改，D 将报文改为：“请给 D 汇 100 元”。这样，最终 B 收到的报文为：“请给 D 汇 100 元”，B 按照报文给 D 汇去 100 元，显然这不是 A 的本意。从这个例子可以看出，保证信息的完整性是电子商务活动中一个重要的安全需求。这就要求交易各方能够验证收到的信息是否完整，即信息是否被篡改或部分删除等。

（4）可靠性。由于网上的通信双方互不见面，所以在交易前必须首先确认对方的真实身份；在进行支付时，还需要确认对方的账号等信息是否真实有效。电子商务系统应该提供通信双方进行身份鉴别的机制，确保交易双方身份

信息的可靠和合法。应实现系统对用户身份的有效确认，对私有密钥和口令的有效保护，对非法攻击能够防范，防止假冒身份在网上进行交易。

（5）匿名性。电子商务系统应确保交易的匿名性，防止交易过程被跟踪，保证交易过程中的用户个人信息不会泄露，确保合法用户的隐私不被侵犯。

（6）防抵赖性。电子商务系统应有效防止商业欺诈行为的发生，网上进行交易的各方在进行数据传输时，都必须携有自身特有的、无法被别人复制的信息，以保证交易发生纠纷时有所对证，以保证商业信用和行为的不可否认性，保证交易各方对已做交易无法抵赖。

1.2 电子商务安全的基本内容

1.2.1 电子商务安全的基本技术

电子商务安全包括的技术范围比较广泛，但主要分为网络安全技术和信息加密技术两大类，其中密码技术可分为加密、数字签名和认证技术等。

1.2.1.1 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。网络安全所涉及的方面很多，如操作系统安全、防火墙技术、虚拟专用网 VPN 技术和各种反黑客技术以及漏洞检测技术等。

防火墙是近年来发展起来的重要网络安全技术，它是将内部网络与外部公网（如 Internet 等）隔离开来，它建立在通信技术和信息安全技术之上，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。防火墙技术主要有包过滤技术、代理服务技术和状态监控技术三类。

VPN 也是一项保证网络安全的技术之一，它是在公共网络中建立一个专用网络，数据通过建立的虚拟安全通道在公共网络中传播。VPN 技术通过 IP 隧道等方法来保证企业协作网中企业间数据和企业内部网的远程分支机构，或异地职工对中央系统的远程访问数据的安全传递。它与信用卡交易和客户发送订单交易不同，同为在 VPN 中，双方的数据通信量要大得多，而且通信的双