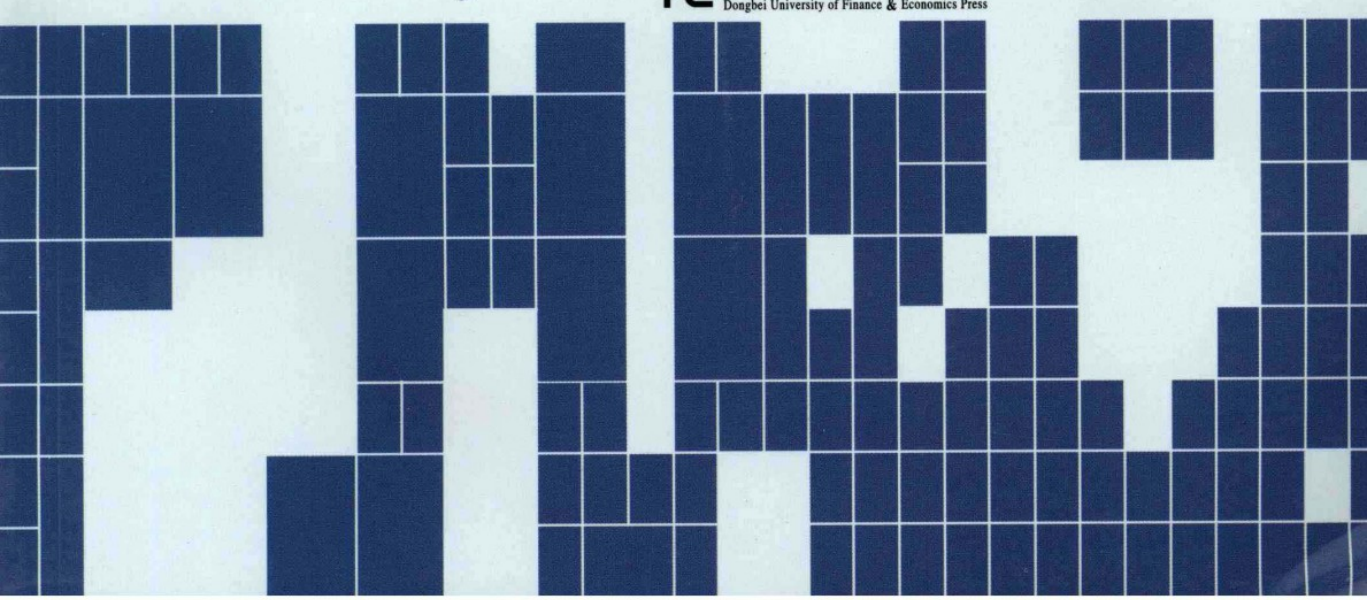
21世纪高等院校电子商务教育系列教材

电子商务安全

李洪心 编著

E-Commerce Security

东北财经大学出版社
Dongbei University of Finance & Economics Press



21世纪高等院校电子商务教育系列教材

电子商务安全

李洪心　编著

E-Commerce Security

东北财经大学出版社
Dongbei University of Finance & Economics Press
大连

图书在版编目（CIP）数据

电子商务安全／李洪心编著．—大连：东北财经大学出版社，2008.9
（21世纪高等院校电子商务教育系列教材）
ISBN 978-7-81122-441-2

Ⅰ.电… Ⅱ.李… Ⅲ.电子商务-安全技术-高等学校-教材 Ⅳ.F713.36

中国版本图书馆CIP数据核字（2008）第123681号

东北财经大学出版社出版
（大连市黑石礁尖山街217号 邮政编码 116025）
总 编 室：（0411）84710523
营 销 部：（0411）84710711
网 址：http://www.dufep.cn
读者信箱：dufep@dufe.edu.cn
大连图腾彩色印刷有限公司印刷 东北财经大学出版社发行

幅面尺寸：186mm×230mm 字数：508千字 印张：20 1/2
2008年9月第1版 2008年9月第1次印刷

责任编辑：李 彬 责任校对：刘赵惠
封面设计：冀贵收 版式设计：钟福建

ISBN 978-7-81122-441-2
定价：32.00元

总序

互联网的出现为全社会提供了一种全新的商务活动方式，从而引发了对电子商务学习、实践和培训的热潮。为满足目前高等教育对电子商务教材的需求，东北财经大学出版社在2008年伊始开发了一套全新的“21世纪高等院校电子商务教育系列教材”。整套教材围绕电子商务的应用性知识分为三个模块、十三种教材：第一个模块是“原理模块”，着力覆盖电子商务的基本原理，包括《电子商务基础教程》、《电子商务与网络经济》、《电子商务系统建设与管理》、《电子商务管理》；第二个模块是“电子商务支持模块”，为学习者讲解对电子商务行为进行支持的主要体系，包括《电子商务案例》、《电子商务法》；第三个模块是“电子商务中的行为模块”，细致刻画了电子商务环境下的个体和企业的行为，包括《电子商务物流管理》、《电子商务交易的支付与结算》、《电子商务安全》、《电子商务网站建设与管理》、《客户关系管理》、《网络营销》、《电子政务》。

这套“21世纪高等院校电子商务教育系列教材”本着科学、先进、合理、可行的原则，在编写过程中努力达到如下要求：

第一，博采众长。从总体上看，由于发达国家发展市场经济的历史较长，市场经济体制也比较成熟，因而其电子商务理论及相应的学科建设确实比我国领先一步，所以学习和借鉴发达国家的电子商务理论成果十分必要。同时，我国在经历了30年的改革开放后，企业的体制、机制改革和技术进步已取得了巨大的成绩，在电子商务实践方面也积累了不少很有特色的成功经验，值得总结提炼。在教材的编写过程中，编者们广泛参考和吸取国内外相关教材的优点，尽量做到既符合国际发展潮流，又切实反映中国电子商务实际情况。

第二，努力创新。虽然我国部分高校开办电子商务专业的时间不长，但电子商务专业的建设已经从“摸着石头过河”到“如何适应市场经济中电子商务发展的需要”发生了重要的转变。为此，电子商务专业及其教材建设在我国面临重大变革。本套教材力求在内容和形式上都有所创新：在内容方面，更新了不适应市场经济环境中当前电子商务实践及未来发展的理论和观念；在形式方面，每种教材在结构、栏目、体例及写作风格上均有所创新，且各种教材均由“主教材”和“电子课件”两者组成，大大方便了教与学。

第三，讲求实用。这主要表现在：一方面，内容上突出特色，兼顾理论系统性与实践可操作性。出于篇幅和知识点交叉的考虑，这套教材中每一种都力求围绕各自中心内容阐述，并根据实际课时量的要求在内容上取舍得当。例如，在《电子商务基础教程》中已经详细介绍过的内容，在其他教材中就尽量避免或者简略介绍。另一方面，成熟性与创新性相结合。本次编写的教材，坚持了教材内容的成熟性与创新性的统一。在阐述成熟而稳定的教材内容的同时，适当介绍新知识、新技能、新发展趋势，使教材具有适度的超前性和前瞻性。另外，本套教材的体例要求也符合教学的规律和方法。在编写过程中，教材各章附有“学习目标”、“本章小结”、“复习思考题”、“技能实训题”等栏目，并且注重时效性，教材中的例题、案例等均取材于最新的实践成果。

第四，严把质量。本套教材由众多国内电子商务领域的专家、学者领衔编撰。他们多年从事该领域的教学与研究，具有丰富的教学及教材编写经验。他们中的大多数曾在欧美高校进修学习、合作研究或访问交流，因而对各学科的最新进展比较熟悉。他们长期关注中外企业电子商务实践，善于总结提炼。此外，各门课程教材的基本体系、结构和内容都经过各教材领衔作者的集体讨论，互提意见和建议，集思广益，严把质量关。

尽管编者们已经付出了最大努力，使现在所奉献给读者的这套教材体现了上述特点，但作为创新的初步尝试，难免会存在不足乃至缺陷。因此，这套教材的推出应该是任重而道远。我们希望能够尽快得到来自各方面尤其是读者方面的反馈意见，以为我们在不久的将来再版修订提供有益的参考。我们也希望并有信心通过不断修订，使教材紧随时代步伐，及时反映学科的最新进展，为培养未来的电子商务专业人才做出持续的贡献。

于西安交通大学
2008 年 3 月

前言

互联网络的普及促进了电子商务的快速发展，但人们在享受电子商务带来的便利和高效的同时，也面临着电子商务安全的严峻考验。计算机系统安全、网络与信息系统安全、交易和支付系统安全逐渐成为广大电子商务用户特别关注的问题，同时政府、国防、公安、金融机构、各大企业和电子商务运营商也急需了解电子商务的安全隐患、熟悉安全防范措施，以及出现了安全问题能及时处理的专业人员。

面对着电子商务的飞速发展以及电子商务教育体系的不断完善，2008 年年初，教育部高等学校电子商务专业教学指导委员会发布了高等学校普通本科电子商务专业教育知识体系。这套知识体系的提出为高等学校电子商务专业教学计划，特别是核心课程体系的设计给出了设计原则。

为解决电子商务发展中出现的安全问题和满足电子商务专业本科教学的需要，规范电子商务领域的安全教育，加快信息系统和网络安全人才的培养，我们参考教育部高等学校电子商务专业教学指导委员会制定的电子商务专业知识体系框架，编写了《电子商务安全》。在本教材编写过程中的内容安排上既考虑到不同学科背景电子商务专业本科生的课程教学，又充分考虑了电子商务专业教育知识体系中核心知识单元和可选知识单元中的关键知识点。全书覆盖了电子商务相关的技术知识领域中电子商务安全技术知识模块的全部内容，并且注重了知识的系统性和覆盖面的广泛性。

本书共 16 章分四大部分。第一部分是理论基础，从第 1 章到第 3 章，介绍计算机系统和信息系统安全问题的基本理论和电子商务安全的概念，包括电子商务安全概述、系统安全的可靠性和加密与识别技术；第二部分是电子商务安全的核心技术，从第 4 章到第 9 章，介绍数字签名技术、公钥基础设施 PKI、电子商务的认证技术、电子商务安全技术协议、电子支付安全、电子商务中的身份认证和访问控制；第三部分是电子商务系统安全环境，从第 10 章到第 13 章，包括防火墙与虚拟专用网、拒绝服务攻击及应急处理、计算机病毒和系统入侵及检测；第四部分从第 14 章到第 16 章，介绍电子商务发展过程中遇到的新问题以及应对措施，包括移动商务安全、电子商务系统的容错性分析和电子商务系统审核与取证。为了方便不同知识背景电子商务专业的教师和学生使用本书，作者在某些章节中用星号 * 注明了有一定难度和开放性的选学内容。另外本书在基于角色的访问控制 RBAC 的应用和电子商务的容错性系统研究

方面给出了对电子商务研究和应用的最新成果，可用于感兴趣的电子商务专业本科高年级学生和研究生进一步的研究参考。

本书的框架由李洪心教授设计，并负责统纂、修改和定稿，盖印编写了第12章、第13章，姜明编写了第14章，李洪心编写了其余各章并汇总统稿。在撰写本书过程中，作者查阅和借鉴了大量已发表的论文和书籍，还有一些相关网站上的内容，均在最后的参考文献中统一列出。作者衷心感谢所有为本书写作提供了丰富参考内容的学者们，感谢东北财经大学电子商务学院的研究生张晓娜、李婷、李燕、梁锋、李冬杰、王玉刚、初阳、李巍、才雨和郑艺，他们在本书资料的收集整理和PPT课件的制作方面做了大量的工作，感谢东北财经大学出版社编辑在本书写作和出版过程中给予的帮助和指导。

本书可作为高等学校电子商务专业的专业课程教材，也可以作为相关专业的本科生了解电子商务安全问题的入门教材或自学教材。本书所涉及的领域发展快、内容新，文稿虽经多次修改，仍难免有问题或疏漏。不当之处，恳请专家和读者指正，以利于今后的提高和完善。

李洪心
于东北财经大学电子商务学院
2008年8月

第1章

电子商务安全概述

学习目标

1. 了解电子商务的安全需求
2. 熟悉电子商务安全管理内容
3. 了解电子商务安全体系结构
4. 了解电子商务安全威胁表现形式

1.1 电子商务安全的基本概念

1.1.1 电子商务面临的安全问题

随着互联网技术的发展和应用的普及，电子商务已经逐渐成为人们进行商务活动的常用模式。越来越多的人通过互联网进行商务活动。电子商务的发展前景十分诱人，而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，对交易信息提供足够的保护，已经成为商家和用户都十分关心的问题。

1）由互联网的特点带来的安全隐患

互联网具有四个特点：国际化、社会化、开放化和个人化。这些特点决定了互联网络应用面临的风险。

（1）国际化：互联网络的触角伸向全球各地，网络的攻击不仅仅来自本地网络的用户，它可以来自互联网上的任何一台机器。

（2）社会化：全球信息化飞速发展，信息化系统已经成为各个国家的关键基础设施，诸如电信、电子商务、金融网络等。社会对计算机网络的依赖日益增强。

（3）开放化：网络的技术和资源是开放的，任何个人、团体都可能获得。开放性和资源共享是网络安全隐患的根源。

（4）个人化：随着网络应用的深入，个人的生活和工作越来越离不开网络，人们可以自由地访问网络，自由地使用和发布各种类型的信息，那么来自网络的安全威胁毫无疑问地会给网络上的个人用户带来损失。

2）人为与不可抗拒因素带来的损失

（1）1995 年，来自俄罗斯的黑客 Vladimir Levin 在互联网上上演了一场“偷天换日”。他是历史上第一个通过入侵银行电脑系统来获利的黑客。他侵入美国花旗银行并盗走 1 000 万美元。之后，他把账户里的钱转移至美国、芬兰、荷兰、德国、爱尔兰等地。同年他在英国被国际刑警逮捕。

（2）2006 年 12 月大规模爆发的“熊猫烧香”病毒，造成的危害堪称严重：据统计，中国有上百万台电脑遭受感染，数以千计的企业受到侵害。

（3）2006 年 12 月 26 日晚至 27 日凌晨台湾南部海域发生强烈地震，使附近国家和地区的国际长途、国际互联网网站受到严重影响，其中包括 8 条光缆。经过夜以继日地抢修，3 个月后才恢复到震前水平。

（4）2008 年 1 月 30 日，一艘停泊在埃及亚历山大港外的船只，在恶劣海象中试图下锚以稳住正在漂流的船身，却不慎割断地中海海底的两条电缆线，造成中东、印度与南亚地区的国际电话和网络通信受阻。

3）电子商务面临的安全威胁

电子商务在给企业带来新的商机、给用户带来方便的同时，由于互联网本身的开放性，计算机技术、网络技术以及其他高科技技术的发展，使得通过网络的犯罪和不道德行为比传统方式更

加隐蔽和难以控制，网上交易也面临了种种危险。人们从面对面的交易和作业变成网上相互不见面的操作，没有国界、时间限制，可以利用互联网的资源和工具进行访问、攻击甚至破坏。概括起来，电子商务面临的安全威胁主要有以下几个方面：

（1）在网络的传输过程中信息被截获。攻击者可能通过互联网、公共电话网、搭线或在电磁波辐射范围内安装截收装置等方式，截获传输的机密信息，或者通过对信息流量和流向、通信频度和长度等参数的分析，推断出有用信息并截获，如消费者的银行账号、密码等。

（2）传输的文件可能被篡改。攻击者可能从以下三个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等。

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）伪造电子邮件。

①虚开网站和商店。给用户发电子邮件，收订货单。

②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。

③伪装用户。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。

（4）假冒他人身份。

①冒充他人身份。如冒充领导发布命令、调阅密件；

②冒充他人消费，栽赃；

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、通行字、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。

（5）不承认或抵赖已经做过的交易。

①发信者事后否认曾经发送过某条消息或内容；

②收信者事后否认曾经收到过某条消息或内容；

③购买者确认了订货单而过后不承认；

④商家卖出的商品因价格差而不承认原有的交易。

1.1.2 电子商务安全的内涵

1）电子商务安全的意义

（1）保证数据传输的安全。电子商务系统既不是单纯的商务系统，也不是简单的计算机网络系统，而是建立在计算机网络系统之上的商务系统。从传统商务过渡到电子商务，交易过程中的物流与信息流，资金流发生了分离，而计算机网络系统是分离出来的这部分信息流和资金流的载体。电子商务环境下，人们在互联网上进行电子交易，信息流和资金流的可靠传输是前提，在此基础上，电子交易才有开展的可能，这就需要保障互联网上数据传输的安全性。

（2）保证交易双方的身份合法。只是保证了数据的安全传输还不能开展安全的电子交易活动。以往的商务活动基本上都是面对面的形式，交易的各方直接接触，身份认证不是一件太难的过程，但是网上交易活动的参与者互不相见，只是通过互联网在一个虚拟的环境下交易，相互间的身份认证就是一个大问题，如果不能保证参与交易各方的身份真实，也就没人敢在网上从事交易了。因此，安全电子商务活动开展的另一个前提是必须建立一套公认的，可靠的身份认证

系统。

2）电子商务安全基本内容

电子商务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。

（1）计算机网络安全。计算机网络安全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。其特征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，以保证计算机网络自身的安全性为目标。

（2）商务交易安全。商务交易安全则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。商务交易安全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。

①保密性：确保信息不暴露给未授权的实体或进程，即信息的内容不会被未授权的第三方所知，保证交易信息在存取和传输过程中不被泄露给非授权的人和实体。

②完整性：只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被修改。电子交易各方信息的完整性是电子商务的基础。必须防止信息的随意生成、修改和删除。同时要防止数据传输过程中的信息丢失和重放，并保证信息传送次序的一致。

③可鉴别性：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是不可能的。因此，要在交易信息的传输过程中为参与交易的个人和企业或国家提供可靠的标识。在互联网上每个人都是匿名的，电子商务系统应充分保证发送方和接收方在接收数据的同时进行身份鉴别。

④不可伪造性：电子交易过程中要保证时间、交易内容、对象的证实，防止利用重放信息实现非法目的，或否认消息的接收和发送。确定收到信息的来源和内容的真实性，防止伪装用户的任何恶意行为。

⑤不可抵赖性：建立有效的责任机制，防止交易对象否认其行为。电子商务活动中，必须为参与交易的对象提供可靠的标识，同时要有各方都信任的权威机构对交易过程进行记录，以防任何一方进行抵赖。

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必需的安全要求。

1.1.3 电子商务对安全的基本要求

由于网上交易的人们不可能都互相认识，为了确保交易的顺利进行，必须在互联通信网络中建立并维持一种令人可以信任的环境和机制。在设计和实施安全措施时，对用户应该是公开透明的。

针对计算机网络安全存在的问题和从事电子商务活动所面临的威胁，为了保障交易各方的合法权益，保证能够在安全的前提下开展电子商务，对电子商务的安全控制问题提出了以下几点基本要求。

1）内部网的严密性

企业的内部网上一方面有着大量需要保密的信息，另一方面传递着企业内部的大量指令，控制着企业的业务流程。企业内部网一旦被恶意侵入，可能给企业带来极大的混乱与损失。比如，

计算机黑客一旦非法闯入银行的内部网络，就可以修改存款数据，划拨资金。再比如，对一些自动化程度高的企业而言，内部网一旦被恶意侵入，企业的经营活动就会陷入瘫痪；企业的财务、技术与人事资料被销毁或被篡改；不订原料或订大量无用的原料；不按规定的程序生产，生产出大量废品；产品被胡乱送到不需要的地方，资金被划走，如此等。因此，保证内部网不被侵入，或把侵入后的损失限制在一定范围，是开展电子商务时应着重考虑的一个问题。

2）完整性

电子商务简化了交易过程，减少了人为的干预，大量的交易活动通过网上的信息交流来完成，但同时也带来了需要保证网上交易双方商业信息的完整性、统一性的问题。

（1）信息的完整性。联合国贸易法委员会在《电子商业示范法》中指出：信息首次以其最终形式生成，作为一项数据电文或充当其他用途时，该信息保持了完整性。

由此可见，在数据输入时的意外差错或欺诈行为、信息传输过程中的丢失、信息传送的次序差异都会导致贸易各方信息的不同，影响信息的完整性。信息的完整性将影响到商务活动的经营策略和成功，保持网上交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。

（2）数据和交易的完整性。数据的完整性是指确保传输中的或存储中的数据未遭受未经授权人的篡改和破坏；交易的完整性是指电子交易完成了交易的全部逻辑，实现了交易的全部功能，不存在单边账现象，同时交易各阶段中的数据是完整的。交易数据的完整性是交易完整性的保障，如果不能保持交易中的数据完整性，不完整的记录和信息将使交易的一方或者双方遭受财务上的损失，并使其承担实质上的法律和信誉风险。

3）保密性

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，均有保密的要求，敏感信息不能披露给第三方。一旦被人恶意获取，将造成极大的危害。比如，信用卡的号码与用户名被人知悉，就有可能被盗用；订货与付款的信息被竞争对手获取，就有可能丧失商机。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开放的网络环境上，如果没有专门的软件对传输的数据进行保护，任何一个对通信进行监测的人都可以对数据进行截取。黑客们只需使用简单的匹配算法就可以将用户口令和信用卡号与其他部分区别开来。只有网上交易信息的保密性达到一定程度才能保证用户的敏感信息不泄漏给未授权的他人，防止信息被盗用和恶意的破坏，并开展真正意义上的电子商务。因此，电子商务中的信息传播、存储、使用均有保密的要求。特别是对敏感文件和重要信息要进行加密，即使这些信息被截获，截获者也无法了解到信息内容。

保密性要求信息的发送和接收在安全的通道进行，保证通信双方的信息保密；交易的参与方在信息交换过程中没有被窃听的危险；非参与方不能获取交易的信息。

4）不可修改性

交易的文件是不可被修改的。比如订购商品，卖方收到订单后，发现价格大幅度上升，如果把订货的数量由一万件改为一件，则可大受其利，而买方则会相应受损。在传统的纸面贸易中，双方是通过协议的一式双份，双方各执一份来防止协议被修改，但在无纸化的电子商务方式下，这显然也不现实，因此，必须有相关的技术来防止电子交易文件被修改，以保证交易的严肃与公正。

5）交易者身份的确定性

只有信息流、资金流、物流的有效转换，才能保证电子商务的顺利实现，而这一切均以信息的真实性为基础。信息的真实性一方面是指网上交易双方提供信息内容的真实性，另一方面是指网上交易双方身份信息的真实性，网上交易的双方很可能素昧平生，相隔千里。要使交易成功，首先要确认交易者的身份。对商家要考虑客户是不是骗子，发货后会不会收不回货款，客户也会考虑商家是否是黑店，付款后会不会收不到货，或者收到货后质量是否能有保证，质量不好是否能投诉商家，因此，能方便而可靠的确认对方身份是交易的前提。双方应该在交换信息之前通过各种方法获取对方的证书，并以此识别交易对方的身份不能被假冒或伪装。

6）交易的无争议和不可抵赖性

数据发送者对自己所发送数据的内容和事实不可否认；数据接收者在接收到数据后，对已经接收到数据的事实不可否认。只有这样，电子交易及交易过程产生的电子凭证才具有无争议性。

由于商情时刻在变化，交易一旦达成是不可否认的，否则必然会损害一方的利益。比如，订货时商品价格较低，收到订单后商品价格已经上涨，如果卖方否认收到订单的实际时间，甚至否认收到订单的事实，必然会对买方造成损失。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据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”。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与交易的确认已是不可能的。因此，要在交易信息的传输过程中为参与交易的个人或企业的身份与行为提供可靠的标识。信息的发送方不能抵赖曾经发送的信息，不能否认自己的行为。如今在网络交易的许多条例中均明确指出，在合约成立方面，除非合约各方另有协议，否则要约及承约可全部或部分以电子记录和电子合约等方式来表达。网上交易一旦达成，便形成交易信息文件，参与交易的各方不可擅自否认和修改交易信息文件，不得因为是电子记录而否定合约的有效性及可强制执行性。

7）有效性

电子商务以电子形式取代了纸张，保证这种电子形式的贸易信息的有效性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、企业或国家的经济利益和声誉。因此，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，以保证贸易数据在确定的时刻、确定的地点是有效的。

8）授权合法性

安全管理人员能够控制用户的权限，分配或终止用户的访问、操作、接入等权利，被授权用户的访问不能被拒绝。在电子商务过程中要求保证信息确实为授权使用的交易各方使用，使他们有选择地得到相关信息与服务，防止由于电子商务交易系统的技术或其他人为因素造成电子商务交易系统对授权者拒绝提供信息与服务，反而为未授权者提供信息与服务。

1.2　电子商务安全管理

1.2.1　电子商务安全管理内容

如上节所述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。但另一方面作为一个完整的综合保障系统来说，电子商务的安全管理也是必不可少的，这里指的是相关的组织机构制定的安全标准。

1）国内外电子商务系统安全标准

（1）互联网安全中心。互联网安全中心（centre for internet security，CIS）是一个由 Visa 国际、AT&T、SANS 研究所，以及 NASA 等 6 位成员组成的组织，现在正在联手推动建立 BtoB 电子商务更为通用的、可审计的安全标准。该组织集中力量确立并推动 BtoB 电子商务安全进程和技术，以确保所有的参与者能够遵循共同的标准，以得到网络安全保障。CIS 以 Visa 公司发布的在线商务安全指南为其通用标准的基础，提出的 10 项新要求包括鼓励商家安装防火墙，保证安全漏洞及时得到修补，对数据进行加密存贮和传送，使用并定期更新防病毒软件，限制员工访问敏感数据等。其他要求还包括 ID 和密码的分配，以及定期对安全系统进行测试等。

（2）国际标准化组织（ISO）。国际标准化组织（ISO）对信息系统的安全体系结构制定了开放系统互连（OSI）基本参考模型（ISO 7498）该模型提供了 5 种安全服务：

①验证服务。

②访问控制服务。

③数据保密服务。

④数据完整性服务。

⑤不可否认服务。

（3）可信计算机系统评估准则。可信计算机系统评估准则（TCSEC 橘皮书）是 1985 年由美国国防部制定的，该准则分为 4 个方面：安全政策、可说明性、安全保障和文档。该准则将以上 4 个方面分为 7 个安全级别，从低到高依次为 D、C1、C2、B1、B2、B3 和 A1 级，见表 1—1。

（4）欧洲信息技术安全评估准则 ITSEC。ITSEC 与 TCSEC 不同，它并不把保密措施直接与计算机功能相联系，而是只叙述技术安全的要求，把保密作为安全增强功能。TCSEC 把保密作为安全的重点，而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。ITSEC 定义了从 E0 级（不满足品质）到 E6 级（形式化验证）的 7 个安全等级，对于每个系统，安全功能可分别定义。ITSEC 预定义了 10 种功能，其中前 5 种与橘皮书中的 C1 ~ B3 级相似。

（5）计算机信息系统安全保护等级划分准则。中国《计算机信息系统安全保护等级划分准则》已经正式颁布，并于 2001 年 1 月 1 日起实施。该准则将信息系统安全分为 5 个等级：

①自主保护级：相当于 C1 级。

②系统审计保护级：相当于 C2 级。

③安全标记保护级：相当于 B1 级，属于强制保护。

④结构化保护级：相当于 B2 级。

表 1—1 计算机系统评估准则

组	安全级别	定　义
1	A1	可验证安全设计：提供 B3 级保护同时给出系统的形式化隐秘通道分析，非形式化代码一致性验证
2	B3	安全域：该级的 TCB 必须满足访问监控器的要求，提供系统恢复过程
	B2	结构化安全保护：建立形式化的安全策略模型，并对系统内的所有主体和客体实施自主访问和强制访问控制
	B1	标记安全保护：对系统的数据加以标记，并对标记的主体和客体实施强制存取控制
3	C2	受控访问控制：实际上是安全产品的最低档次，提供受控的存取保护，存取控制以用户为单位
	C1	只提供了非常初级的自主安全保护，能实现对用户和数据的分离，进行自主存取控制，数据的保护以用户组为单位
4	D	最低级别，保护措施很小，没有安全功能

⑤访问验证保护级：相当于 B3 ~ A1 级。

实际应用中主要考核的安全指标有身份认证、访问控制、数据完整性、安全审计、隐蔽信道分析等。

2）中国信息安全等级划分与保护

2004 年 9 月 15 日，公安部、国家保密局、国家密码管理局和国信办联合下发《关于信息安全等级保护工作的实施意见》（66 号文件），明确了实施等级保护的基本做法。2007 年 6 月 22 日，四部门又联合下发《信息安全等级保护管理办法》（43 号文件），规范了信息安全等级保护的管理，坚持自主定级、资助保护原则，根据在国家安全、经济建设、社会生活中的重要程度，以及系统遭受破坏后的危害程度等因素确定等级（见表 1—2、表 1—3）。

表 1—2 信息安全等级划分表

等级	合法权益		社会秩序和公共利益			国家安全		
	损害	严重损害	损害	严重损害	特别严重损害	损害	严重损害	特别严重损害
一级	√							
二级		√	√					
三级				√		√		
四级					√		√	
五级								√

3）相关的保密法规、管理办法和技术规范

（1）计算机信息网络国际联网管理暂行规定。

（2）计算机信息系统国际联网保密暂行规定。

（3）中国计算机信息网络国际联网管理暂行规定实施办法。