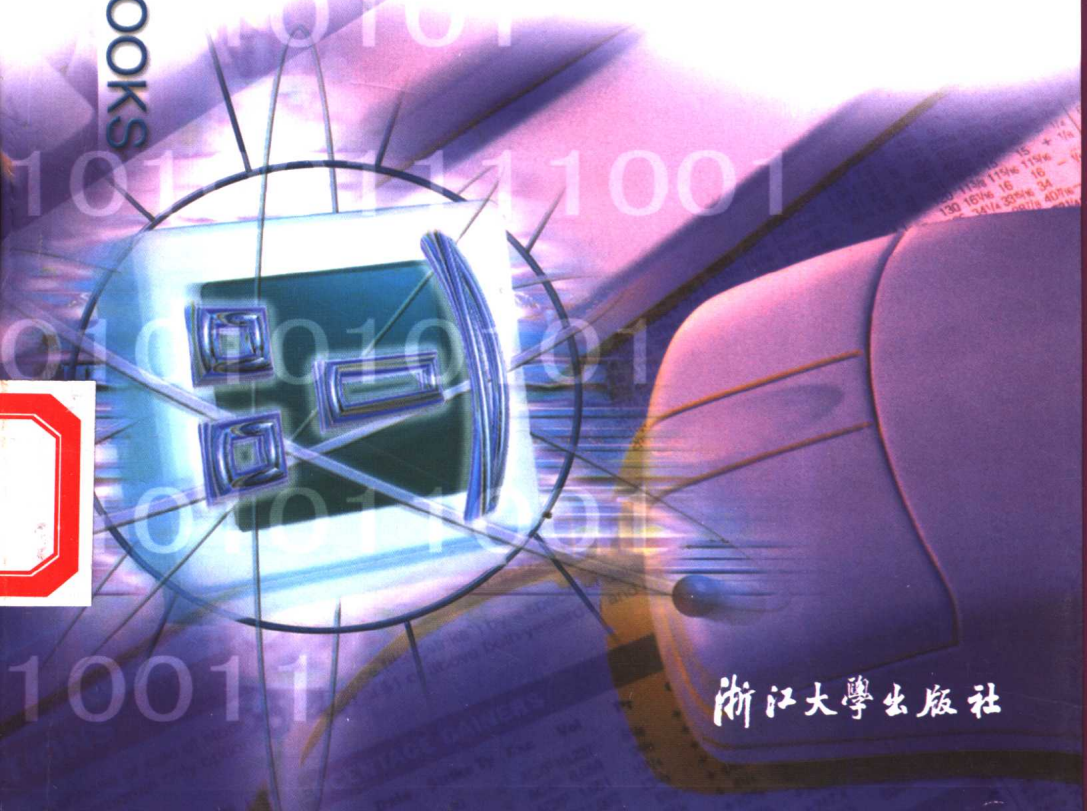
电 子 商 务 系 列 教 材

电子商务信息安全

INFORMATION SECURITY IN ELECTRONIC COMMERCE

A SERIES OF TEXTBOOKS FOR E-COMMERCE

翁贤明 编著



浙江大學出版社

电·子·商·务·系·列·教·材

电子商务信息安全

翁贤明　编著

浙江大學出版社

图书在版编目（CIP）数据

电子商务信息安全／翁贤明编著. —杭州：浙江大学出版社，2003.3
ISBN 7-308-03252-3

Ⅰ.电... Ⅱ.翁... Ⅲ.电子商务—安全技术
Ⅳ.F713.36

中国版本图书馆 CIP 数据核字（2003）第 008497 号

总 责 编 樊晓燕
封面设计 刘依群

责任编辑 杜希武
出版发行 浙江大学出版社
（杭州浙大路 38 号 邮政编码 310027）
（网址：http://www.zjupress.com）
（E-mail:zupress@mail.hz.zj.cn）
排 版 浙江大学出版社电脑排版中心
印 刷 浙江良渚印刷厂
开 本 850mm×1168mm 1/32
印 张 14.5
字 数 390 千字
版 印 次 2003 年 3 月第 1 版 2003 年 3 月第 1 次印刷
印 数 0001—3000
书 号 ISBN 7-308-03252-3/F・425
定 价 22.00 元

内容提要

本书是一部关于电子商务信息安全的著作。全书共分7章，第1章从电子商务信息安全入手，对电子商务信息安全因素进行了分析，并在此基础上探讨了电子商务信息安全体系的构架，提出了运用先进的技术、严格的管理、威严的法律、文明的道德来实现电子商务信息安全的整体构思。本书基本按此构思展开，但又主要集中在技术实现上；第2章对密码技术作了较为深入的介绍，为后面各章的应用打下了基础；第3、4章是电子商务中迫切需要解决的有关软件系统、网络系统等安全技术；第5章是电子商务安全认证技术——电子商务交易安全；第6章是有关计算机病毒的诊断与消除；第7章就电子商务信息的安全管理、法律规范、道德文明作了陈述。

本书资料翔实，深入浅出，结构合理，层次清晰，有一定的理论深度和较高的实用价值。全书最后有参考文献，可供读者参考和深入研究。

本书可作为高等学校电子商务、金融信息管理、会计信息管理、信息管理与信息系统、计算机科学技术及应用等专业的教学用书，也可作为上述业务领域相关人员的参考用书。

《电子商务系列教材》编委会

序

电子商务作为信息学、经济学、管理学、法学、计算机技术和理工类交叉的一个新兴学科，在当代信息化社会的经济与建设、金融与商业流通、生产与服务等各类社会活动中都有着广泛的应用和迫切的人才需求。浙江大学作为目前全国学科最为齐全的国家重点研究型大学，具有高水准的计算机科学、经济学、管理学等学科的教学与科研师资队伍，已在电子商务的基础理论、网络信息发布、系统集成、一体化产品的设计制造与营销、数据挖掘及分布式计算等相关应用研究和技术方面取得了多项成果，并通过与"蓝色巨人"IBM 公司共建电子商务体系合作开展在中国环境下的电子商务研究和高级应用人才的培养。

为支持电子商务的发展，并促进多学科交叉综合型人才的培育，浙江大学从 1999 年开始，在本科生中设立了电子商务第二专业。其目标是培养具备较扎实的电子商务知识，能够进行电子商务综合应用、开发与管理的交叉型高级管理与技术人才，以满足信息化社会电子商务的技术发展和应用的迫切需要。开课两年来，每次选课的学生都多达 1500 人以上，显示出强烈的兴趣。从 2001 年开始，经教育部批准，浙江大学又成为第一批开设电子商务专业、并在全日制和远程教育两方面招收电子商务专业学生的高校之一。

针对我国目前缺乏电子商务系列教材的现状，浙江大学出版

社及时组织有关专家，精心组织出版了这套电子商务系列教材，其中包括《电子商务概论》、《网络经济学概论》、《网络营销学》、《电子商务应用开发技术》、《客户关系管理 CRM》等共计十几册，将在近期陆续出版。望此举既能推动我国电子商务学科的建设，又能推动中国电子商务人才培养与经济的发展。

潘云鹤

2001 年 5 月

前言

20世纪90年代以来，随着计算机互联网技术的发展、应用和普及，一种以互联网络为基础、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(Electronic Commerce)应运而生。电子商务，从狭义上讲，是指政府、企业和个人利用电子计算机网络技术实现商业交换和行政管理的全过程；从广义上说，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。

电子商务的发展速度是惊人的。据统计，1998年底世界通过互联网实现的交易活动收入为430亿美元，1999年为600多亿美元，到2000年已达到1320亿美元，预计到2003年，全球电子商务交易额将突破1.5万亿美元，成了世界经济新的增长点。我国随着网络用户数量的迅速增长，电子商务也出现了飞速的发展，成了我国经济新的增长点。

电子商务作为一种全新的商业运作模式，将成为21世纪国际商务往来的主流和各国经济活动的核心。可以说，电子商务代表着未来贸易方式的发展方向，其应用推广将给世界各国带来更多的贸易机会。因此，国际社会对电子商务的巨大发展潜力给予了高度

重视，尤其是一些发达国家和地区，已经将电子商务视为推行经济全球化和主导世界经济的重要战略措施，并把电子商务的发展看作是未来世界经济发展的重要推动力。

然而，在人们热衷和沉醉于 Internet 及其电子商务的时候，千万不要忽视日益严峻的电子商务信息安全问题。Internet 上的黑客和不法之徒无须“飞檐走壁”、“穿墙入室”，即可轻易地取走你的机密文件，窃取你的银行存款，破坏你的企业账目，公布你的隐私信函，篡改、干扰和毁坏你的数据库，甚至直接破坏你的磁盘或电子商务信息系统，使你的网络瘫痪或崩溃。人们对 Internet 及其部件的依赖程度越高，可能遭受的侵害和损失会越大。因此，我们必须充分认识和了解这些风险，采取切实有效的措施，防范风险，加强安全，减少危害和损失，保证电子商务信息系统资源的安全，保护电子商务信息的安全。为此，我们编著了《电子商务信息安全》一书，以利于电子商务高级人才的培养，以利于电子商务事业的健康发展。

本书共分 7 章。第 1 章从电子商务信息安全入手，对电子商务信息安全因素进行了分析，并在此基础上探讨了电子商务信息安全体系的构架，提出了运用先进的技术、严格的管理、威严的法律、文明的道德来实现电子商务信息安全的整体构思。本书基本按此构思展开，但又主要集中在技术实现上；第 2 章对密码技术作了较为深入的介绍，为后面各章的应用打下了基础；第 3,4 章是电子商务中迫切需要解决的有关软件系统、网络系统等安全技术；第 5 章是电子商务安全认证技术——电子商务交易安全；第 6 章是有关计算机病毒的诊断与消除；第 7 章就电子商务信息的安全管理、法律规范、道德文明作了陈述。

本书资料翔实，深入浅出，结构合理，层次清晰，有一定的理论深度和较高的实用价值。全书最后有参考文献，可供读者参考和深入研究。

本书由翁贤明、李小东、何鸿声、翁恺四位教师编著。本书的撰写还得到了浙江大学教务部、浙江大学管理科学与工程学系、浙江大学计算机系有关教师的关心和支持，在此一并表示感谢。

本书可作为高等学校电子商务、金融信息管理、会计信息管理、信息管理与信息系统、计算机科学技术及应用等专业的教学用书，也可作为上述业务领域工作人员的参考用书。

由于作者水平有限，错误和缺点在所难免，欢迎读者和电子商务、计算机网络界同行批评指正。

编著者

2002 年 8 月

目 录

第1章

绪　论

1.1　电子商务与信息安全

1.1.1　计算机网络与电子商务正在改变着世界

20世纪90年代以来，随着计算机技术的发展，以及互联网(Internet)的应用和普及，一种以计算机互联网络为基础、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(Electronic Commerce)应运而生。电子商务，从狭义上讲，是指政府、企业和个人利用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；从广义上说，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。

电子商务的发展速度是惊人的。据统计，1998年底世界通过互联网实现的交易活动收入为430亿美元，1999年为600多亿美

元，到2000年已达到1320亿美元，预计到2003年，全球电子商务交易额将突破1.5万亿美元，成了世界经济新的增长点。在我国，随着网络用户数量的迅速增长，电子商务也出现了飞速的发展，成了我国经济新的增长点。

电子商务作为一种全新的商业运作模式，将成为21世纪国际商务往来的主流和各国经济活动的核心。可以说，电子商务代表着未来贸易方式的发展方向，一种全新的"网络经济"正在迅速形成，计算机网络与电子商务正在改变着世界。

然而，如同其他事物一样，电子商务也有它的两重性，我们不仅要看到它有积极作用的一面，还要看到它存在问题的一面。只有当我们看到了它的问题，查到了产生问题的根源，并进而找到解决问题的办法，我们就能在现有的基础上更大踏步地向前迈进，创造出人类社会全新的文明。

1.1.2 电子商务信息安全面临的威胁

电子商务运作主要依托的环境是当前的国际互联网和未来的国际信息基础设施(GII)。网络是从事电子商务机构安身立命的工作环境。从业机构的开业挂牌，广而告之，出示产品和服务，联系业务，签署交易协议，交易款项的存、取、支付，交易结果的查询追踪等都要围绕网络的利用来展开。但随之而来的是，计算机网络连接的系统安全问题、利用计算机网络犯罪的问题也日益突出，它主要反映在易受攻击而被人非法利用，并因此给人们带来极大的损失和灾难。

一、计算机犯罪现状

(一)计算机犯罪上升速度迅猛

据推测，人为地利用计算机进行违法犯罪活动，始于20世纪40年代末。它首先是在军事领域，然后逐步发展到工程、科学、金融、银行和商业领域。有据可查的计算机犯罪始于1958年。1958