

<<电子商务安全与管理>>

图书基本信息

书名：<<电子商务安全与管理>>

13位ISBN编号：9787040122602

10位ISBN编号：704012260X

出版时间：2003-8

出版时间：高等教育出版社

作者：劳帼龄 编

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<电子商务安全与管理>>

### 前言

在中国互联网络信息中心所作的历次调查和发布的《中国互联网络调查统计报告》中，安全问题一直是电子商务用户特别关注的主题。

安全漏洞的存在，直接影响了电子商务网站的信誉度，而电子商务交易的安全性得不到保证，则必将影响电子商务的顺利发展。

确实，电子商务的安全问题已成为推进国际国内电子商务发展的一大瓶颈，正在引起越来越多人士的关注。

然而，电子商务的安全问题并不是光靠技术就能解决的，这是一个涉及范围极广的社会问题，需要各方的协调配合。

因特网的普及促进了网上电子商务的开展，但企业面对潮水般涌入的信息流，该如何分辨交易信息的真伪呢？

在这里，除了要充分依靠现代信息技术，尤其是信息安全技术手段来进行保护外，还需要使用管理的手段来进行约束。

本书从技术与管理相结合的角度论述了电子商务的安全问题，结构新颖。

第一章作为导论，首先引出了电子商务面临的安全问题，介绍了电子商务系统安全的构成，提出了电子商务安全保障必须由技术手段、管理制度、法律法规三管齐下的思路。

第二章介绍了与电子商务的安全管理有关的标准及制定标准的组织、解决安全问题的协调机构与政策、电子商务的安全管理制度，并简要介绍了电子商务安全的法律保障。

第三章介绍了信息安全原理及各类信息安全技术。

第四章立足因特网介绍了Internet安全问题。

第五章介绍了数字证书及证书的管理。

第六章介绍了公钥基础设施PKI，包括PKI的核心——CA、CA的结构、CA的证书政策，以及PKI中的不可否认机制。

第七章作为安全认证的实例，介绍了CA的建设，并以中国金融认证中心为例介绍了CA的证书政策，以SHECA数字证书和Verisign数字证书为例介绍了数字证书的申请与使用。

最后，在附录中介绍了与电子商务安全有关的管理条例和管理办法。

本书由劳帼龄主编。

参加本书资料收集和编写的还有谢怀军（第四章部分章节）、王立萍（第七章部分章节），最后由劳帼龄负责全书的统稿。

对外经济贸易大学信息学院院长陈进教授仔细审阅了全书。

## <<电子商务安全与管理>>

### 内容概要

《电子商务安全与管理》是普通高等教育“十五”国家级规划教材，是高等学校电子商务专业主要课程教材之一。

电子商务的安全问题正日益受到人们的关注，但解决电子商务的安全问题只靠技术是不够的，必须将技术与管理相结合才能真正产生实效。

《电子商务安全与管理》的宗旨是，让学生对电子商务中将会遭遇到的各种安全风险有一个清醒的认识，知道怎样通过制定安全标准、安全政策和安全管理措施来对电子商务的安全问题进行管理；理解电子商务系统的安全是由系统实体安全、系统运行安全、系统信息安全三部分构成的；了解加密技术、数字签名技术等基本的信息安全技术；掌握电子商务所采用的各种安全协议，尤其是安全套接层协议SSL和安全电子交易协议SET的作用及其应用；明确数字证书的格式、作用，以及CA认证中心在保障电子商务安全中的地位与作用；同时结合实际掌握1 - 2种数字证书的申请与使用方法。

## 书籍目录

第一章 电子商务安全导论第一节 电子商务面临的安全问题一、安全问题的提出二、电子商务涉及的安全问题第二节 电子商务系统安全的构成一、电子商务系统安全概述二、系统实体安全三、系统运行安全四、信息安全第三节 电子商务安全的保障思考题第二章 电子商务安全管理第一节 安全标准与组织一、制定安全标准的组织二、因特网标准与组织三、我国的信息安全标准化工作第二节 安全协调机构与政策一、国际信息安全协调机构二、我国的信息安全管理机构及原则第三节 电子商务安全管理制度一、信息安全管理制度的内涵二、网络系统的日常维护制度三、病毒防范制度四、人员管理制度五、保密制度六、跟踪、审计、稽核制度七、应急措施制度第四节 电子商务安全的法律保障一、国际电子商务立法现状二、国内电子商务立法现状三、国内与电子商务相关的法律法规政策思考题第三章 信息安全技术第一节 信息安全概述第二节 加密技术一、对称加密系统二、不对称加密系统三、两种加密方法的联合使用第三节 数字签名技术一、散列函数二、RSA数字签名三、数字签名算法(DSA)四、椭圆曲线数字签名算法(ECDSA)第四节 密钥管理技术一、密钥管理概述二、RSA密钥传输三、Diffie-Hellman密钥协议四、公开密钥的分发第五节 验证技术一、基于口令的验证二、验证协议三、基于个人令牌的验证四、基于生物统计特征的验证五、基于地址的验证六、数字时间戳验证第六节 数字证书技术一、数字证书二、认证机构三、利用数字证书实现信息安全思考题第四章 Internet安全第一节 Internet安全概述一、网络层安全二、应用层安全三、系统安全第二节 防火墙技术一、防火墙的基本概念二、防火墙的基本原理三、防火墙的实现方式第三节 IP协议安全一、IP安全体系结构二、认证头协议(AH)三、分组加密协议(ESP)四、密钥管理五、Ipsec的应用第四节 电子商务应用安全协议一、增强的私密电子邮件(PEM)二、安全多用途网际邮件扩充协议(s/MIME)三、安全超文本传输协议(s-HTTP)四、安全套接层协议(SSL)五、安全电子交易协议(SET)思考题第五章 数字证书第一节 数字证书简介第二节 数字证书的格式一、基本数字证书格式二、X.509版本3数字证书格式三、数字证书扩展标准第三节 公私密钥对的管理一、密钥对的生成二、私钥的保护三、密钥对的更新第四节 数字证书的申请与发放一、数字证书管理机构的作用二、数字证书的申请注册三、数字证书的生成四、数字证书的更新第五节 数字证书的分发一、利用数字签名分发数字证书二、利用目录服务分发数字证书第六节 数字证书的撤销一、请求撤销数字证书二、数字证书撤销表的格式三、撤销数字证书的方法四、x.509标准的数字证书撤销表思考题第六章 公钥基础设施PKI第一节 PKI概述一、PKI简介二、PKI的核心——CA第二节 CA的结构一、认证路径二、树型层次结构三、森林型层次结构四、通用结构第三节 CA的证书策略一、证书策略CP与证书实施说明CPS二、保证等级与证书等级三、证书策略的内容第四节 CP和CPS的主题内容一、第一部分：介绍二、第二部分：一般规定三、第三部分：身份识别和身份验证四、第四部分：操作要求五、第五部分：物理、过程和人员的安全控制六、第六部分：技术安全控制七、第七部分：证书和证书撤销表八、第八部分：规范管理第五节 PKI中的不可否认机制一、基本概念二、三种不可否认机制三、不可否认机制所涉及的活动四、可信任的第三方的作用五、不可否认机制的实施第六节 几类不同的PKI一、基于PEM的PKI二、基于SET的PKI三、VeriSign信任网络思考题第七章 安全认证实例附录参考文献

章节摘录

插图：

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>