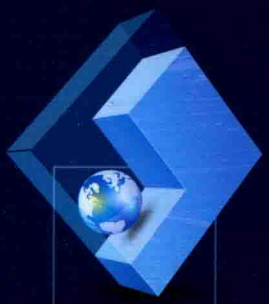
国家电子商务发展丛书

The Series of E-commerce development in China

电子商务安全

刘 权 主编　　张 莉 副主编



Electronic Commerce Security

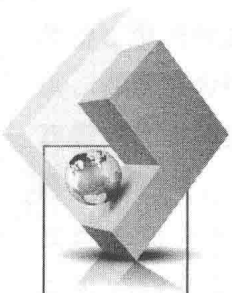
化学工业出版社

国家电子商务发展丛书

The Series of E-commerce development in China

电子商务安全

刘 权 主编　　张 莉 副主编



Electronic Commerce Security

化学工业出版社

·北京·

《电子商务安全》由中国电子信息产业发展研究院网络空间研究所成员编写而成，主要包括电子商务安全概述、电子商务安全威胁的发展历程、电子商务安全法律法规、管理、技术、标准等内容，并对电子支付、移动电子商务、企业电子商务、跨境电子商务等领域的安全问题进行了重点剖析，总结了电子商务安全面临的形势和发展重点。

《电子商务安全》具有较高的系统性和较强的知识性，内容丰富实用，全面易懂，具有很好的可读性。

《电子商务安全》既可作为高等学校电子商务及电子安全等相关专业本科生、研究生的参考书，也可以供相关专业科研人员、管理人员参考使用，还可作为对电子商务安全感兴趣的读者的读物。

图书在版编目（CIP）数据

电子商务安全/刘权主编．—北京：化学工业出版社，2017.1
（国家电子商务发展丛书）
ISBN 978-7-122-28726-7

Ⅰ.①电… Ⅱ.①刘… Ⅲ.①电子商务-安全技术 Ⅳ.①F713.36

中国版本图书馆 CIP 数据核字（2016）第 312387 号

责任编辑：宋湘玲　王淑燕　　装帧设计：王晓宇
责任校对：边　涛

出版发行：化学工业出版社（北京市东城区青年湖南街 13 号　邮政编码 100011）
印　　装：三河市延风印装有限公司
787mm×1092mm　1/16　印张 13½　字数 232 千字　2017 年 3 月北京第 1 版第 1 次印刷

购书咨询：010-64518888（传真：010-64519686）　售后服务：010-64518899
网　　址：http://www.cip.com.cn
凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定　　价：68.00 元

编写说明

中国互联网诞生二十余年，发展成为中国崛起的强大催化剂；中国电子商务发展十多年已经成为中国经济转型升级的新引擎。

20多年间中国网民呈爆发式快速增长，从1994年0.09亿人到2016年6月的7.10亿人。2008年3月中国网民数量和宽带网民数同时超过美国；2014年中国网民数量达到美国的2.5倍，超过前五个发达国家（美国、日本、德国、英国、法国）总和，中文网民规模继续领跑全球。伴随着中国网民数量的激增，中国掀起了三次互联网上市浪潮。第一次是以新浪、网易、搜狐、腾讯、百度等为代表的媒体板块上市；第二次是以完美世界、巨人网络、盛大游戏等为代表的游戏板块上市；第三次是以阿里巴巴、京东、唯品会、聚美优品、58同城、去哪儿网、途牛网等为代表的电商及垂直电商板块的上市。尤其是2014年9月19日中国电商龙头企业阿里巴巴在美国纽交所上市，总市值高达2314亿美元，阿里巴巴成为中国最大的互联网上市公司，创下了纽交所成立以来的历史最高记录，其市值赶上了世界最大的实体连锁企业沃尔玛。

中国电子商务的发展历程中，一次次创造纪录，又一次次打破纪录，谱写着中国电子商务发展的恢弘篇章。仅以中国人自创的“双十一”战果就足以让世界为之瞩目。2016年11月11日，天猫成交额达1207亿元；交易额同比增长59%；苏宁易购全渠道增长达193%，线上增长达210%；国美在线交易额增长268%，移动端交易额占比达72%……电子商务发展日新月异，其影响已经超越了商务活动本身，成为世界经济发展的新动力，极大影响着我们的工作和生活方式。

电子商务对中国服务经济的重要性也日益加深，从大中城市辐射到县域经济和农村经济。可以认为电子商务经济是我国经济转型升级的新引擎、工农业与服务业可持续协调发展的融合力、社会协同创新发展的推动力，发展电子商务经济也是提高国家竞争力的有效途径。

鉴于电子商务发展的重要战略性意义，国家开展了电子商务示范城市创建、电子商务产业园建设及电子商务示范企业创建工作，并将该项工作作为当前中国电子商务经济发展的重要内容。国家发改委、商务部等八部委已经在全国开展了两批共53个城市进行电子商务示范城市创建工作；评选了34个基地开展电子商务示范基地创建工作；2011年评选了83家电子商务示范企业、

2014年评选第二批100家电子商务示范企业，2016年评选第三批156家电子商务示范企业这些示范工作极大地促进了我国电子商务的发展。

《国家电子商务发展丛书》是为了配合国家电子商务示范城市等创建工作的开展，以促进中国电子商务经济健康有序快速发展为目标，组织有关专家共同编写的系列图书。《国家电子商务发展丛书》总体上阐述了国内外电子商务发展情况、发展模式及发展经验，针对当前电子商务发展中的重大问题分专题出版从而形成图书系列，专题方向包括电子商务经济、大宗商品电子商务、移动电子商务、电子商务物流、跨境电子商务、电子商务创业创新、互联网金融、社区电子商务服务及电子商务环境建设等。

《国家电子商务发展丛书》可供致力于发展电子商务的各级政府、企事业单位的领导参考阅读；可以作为示范城市、示范基地和示范企业的电子商务培训教程；各分册可以作为相关领域专家学者及技术人员的参考书，也可以作为大中专高校电子商务课程的参考书。

《国家电子商务发展丛书》编审委员会

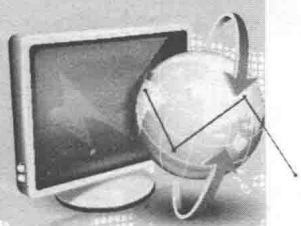
2016年12月

FOREWORD

前　言

电子商务是通过信息技术将企业、供应商、用户及其他商贸活动涉及的相关机构结合起来的一种信息技术的应用，是完成信息流、物流和资金流转移的一种行之有效的方法。随着信息技术的快速发展，电子商务不断渗透到人们生产生活的方方面面，给人们的生产和生活带来了前所未有的便利和高效。但是，由于互联网的开放性、自由性、虚拟化等特性，电子商务也给交易双方带来了很多的安全隐患，如何构建安全、可靠的电子商务环境，已经成为迫切需要解决的问题。

本书正是围绕电子商务安全而展开的，它系统地阐述了电子商务相关领域的发展现状，剖析了面临的安全问题，有针对性地提出了相应对策建议。《电子商务安全》有几大特色：①结构完整，内容全面。全书不仅深入阐述了主要的电子商务安全技术，也论述了电子商务安全标准、管理和法律法规等方面的内容。②深入浅出、循循善诱。本书用矛盾分析的方法，先找出问题，然后分析原因并找出相关政策建议。③注重理论和实践相结合。本书专门开辟了一个章节叙述电子商务安全重要事件和案例，便于读者从生动形象的事件和案例中学会如何应对电子商务领域的安全问题。



《电子商务安全》由中国电子信息产业发展研究院网络空间研究所人员编写，刘权任主编，张莉任副主编，具体分工如下：第1章、第5章由李建武编写，第2章由张莉编写，第3章由魏书音编写，第4章由张莉和王超编写，第6章由陈月华编写，第7章由李建武、闫晓丽和王闯编写，第8章由王超和魏书音编写，第9章由王超编写，附录由刘昌金编写，全书由刘权进行整体设计和统稿。

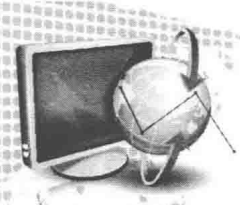
电子商务安全涉及众多学科，各种理念、技术和方案在实践中不断地推陈出新。由于作者水平有限，书中不足之处，希望读者谅解，并恳请读者批评指正。

本书将逐渐配套相关在线资源、为读者免费提供，如有需要，可以扫描下述二维码，在线观看。

编者

2017 年 1 月

FOREWORD



目录
CONTENTS

第1章 电子商务安全概述

电子商务是通过信息技术将企业、供应商、用户及其他商贸活动涉及的相关机构结合起来的一种信息技术的应用，是完成信息流、物流和资金流转移的一种行之有效的方法。随着大数据、云计算、移动互联网等新兴信息技术的出现，电子商务发展驶入快车道。电子商务不断渗透到人们生产生活的方方面面，带来了前所未有的便利和高效。但是，由于互联网的开放性、自由性、虚拟化等特性，电子商务也给交易双方带来了很多的安全隐患，例如，电子交易信息在处理、存储和传输过程中上存在严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏，还可能受到计算机病毒感染，如何构建一个安全、可靠的电子商务环境，已经成为当前行业发展关注的重点。

1.1 电子商务安全概况

电子商务安全涉及众多领域，是互联网安全在电子商务领域的延伸，主要包括网络安全、电子交易安全、用户数据安全等。网络安全包括：网络硬件设备安全、网络软件安全、数据资料安全、网络运行环境安全、网上交易服务器与用户传递信息的安全、客户端计算机及其他连接互联网设备的安全。电子交易安全包括：商品品质安全、身份可信安全、物流安全、支付安全等。用户数据安全包括：用户个人信息安全、用户的账号密码、用户购买记录信息等。随着电子商务的不断发展，其面临的安全风险也在不断变化。

1.1.1 电子商务安全概念

电子商务安全是一个广泛而系统的概念，是电子商务在整个运行过程中的安全问题的集合。狭义上，电子商务安全主要指数据传输安全和电子交易安全。保障电子商务的载体安全，这是电子商务安全的基础。广义上，电子商务

安全还包括电子商务硬件安全、电子商务软件安全、电子商务应用安全、电子商务环境安全、电子商务安全立法、电子商务管理安全、电子商务从业人员安全意识和能力等诸多方面。

1.1.1.1 狭义电子商务安全

(1) 数据传输安全

电子商务是一个复杂的多维系统，是建立在计算机网络之上的商务系统，实现了传统商务的物流、信息流和资金流的分离。承载信息流和资金流载体的计算机网络系统，保障载体数据的传输安全，是电子商务得以正常运转的核心，是保证信息流和资金流可靠传输的前提。

(2) 电子交易安全

仅仅保证数据传输的安全，还不能完全实现安全的电子商务。在传统的商务活动中，交易的双方是面对面的，交易安全基本可控，而在网上进行的电子交易，交易双方互不相见，只是通过互联网的虚拟环境进行交易，首要安全就是确认双方身份。因此，可靠的身份认证系统是电子商务活动得以开展的基础。

1.1.1.2 广义电子商务安全

对于广义上的电子商务安全，下面着重介绍 4 种。

(1) 电子商务硬件安全

电子商务的基础是网络，而网络的物理支撑是各种硬件设施，由于各种原因，例如设备故障、人为因素、自然灾害等，这些硬件设施会带来安全风险。硬件安全问题发生的概率非常小，但是一旦发生所带来的伤害是巨大的。

(2) 电子商务软件安全

网络不仅需要硬件作为基础，还需要各种系统软件和应用软件的支撑，软件是电子商务系统中另一个重要的组成。但是，由于各种人为原因和技术原因，各种系统软件和应用软件可能会存在一定的缺陷和漏洞。

(3) 电子商务应用安全

在硬件和软件均安全的情况下，操作人员行为的不恰当也会导致电子商务安全问题。例如，企业管理人员电子商务知识水平和管理水平不高，不能胜任所承担的工作，导致企业管理水平不高、效率低下；消费者电子商务和个人信息安全意识不强，导致个人信息泄露；商业欺诈和以获取机密信息或者破坏为

目的网络攻击，如病毒、木马程序等，扰乱正常的网络秩序。

(4) 电子商务环境安全

环境层面主要是指政策法律环境。电子商务的发展与运行需要良好的政策与法律环境。在电子商务中，法律不仅是打击网络犯罪的武器，更是各个主体商务活动的游戏规则，政策则是引导和推进电子商务的无形之手，来调节和规范电子商务行为。目前，我国虽然已有关于电子商务的政策和法律法规，却还是不够完善，使得许多电子商务纠纷的解决缺少依据，给投机分子以可乘之机。

1.1.2 电子商务安全的特点

(1) 系统性

电子商务安全问题涉及众多方面，不仅包括技术安全、管理安全、认证安全等内在因素，还包括社会法制、社会道德、行业自律等外在的安全延伸，是一个系统化的安全体系。

(2) 相对性

在互联网环境下，安全没有绝对，只有相对。在电子商务的活动过程中，开放的网络环境必然遭受各方有意或无意的攻击，可能是内部的，也可能是外部的，可能是系统本身的漏洞，也可能是自身的配置出现纰漏等，安全威胁防不胜防，因此，电子商务不存在绝对安全。

(3) 代价性

商业活动注重的是成本和利润，电子商务同样如此。电子商务安全的目标是保证在可接受的代价（或成本）范围内，尽量使安全风险降到最低。

(4) 动态性

安全威胁是不断变化的，今天安全不代表明天安全，安全攻防此消彼长、不断发展，电子商务安全具有动态属性。

1.1.3 电子商务安全的重要性

对于电子商务来说，安全是其存在和发展的核心。对个人来说，消费者担心的是电子商务活动过程中的个人信息安全和财产安全，一旦这些不能得到保障，消费者必然转向选择其他安全的购物方式。对企业来说，电子商务安全是电子商务运作的重要保障，是物流、信息流和资金流最终实现的根本保证，是增强企业竞争力的一个有效途径。如果安全问题解决不了，不仅影响到企业的

商品安全、资金安全，甚至直接影响到电子商务企业的生存。对国家来说，电子商务是社会经济的重要组成部分，正在成为推动国民经济发展的新动力，然而电子商务毕竟是虚拟经济，在这个过程中不受地域和时间限制，从某些方面来说甚至不受国家限制，这就为跨国经济犯罪提供了可乘之机，严重威胁到国家的经济安全和国家经济秩序的稳定。

1.2 电子商务安全体系

电子商务安全体系是一个全方位的安全保障体系，涉及环境安全、网络安全、加密安全、认证安全、协议安全、应用安全等六个层次，如图 1-1 所示。在这个安全体系结构中，下层是上层的基础，为上层提供技术支持；上层是下层的扩展与递进。各层次之间相互依赖、相互关联构成统一整体。各层通过控制技术的递进实现电子商务系统的安全。

图 1-1 电子商务安全体系结构

在本书中，从电子商务安全要素构成角度分析，电子商务安全体系包括政策法规、安全管理、安全技术和安全标准四个方面，图 1-2 基本涵盖了电子商务安全体系的要素。

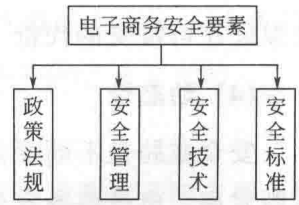


图 1-2 电子商务安全体系的要素构成

1.2.1 电子商务安全法律法规

电子商务安全法律法规是指导电子商务发展、规范电子商务行为、实现电子商务安全的重要内容之一，是电子商务环境安全的基础。电子商务安全法律包括：信息网络安全法律法规、商用密码管理及应用法律法规、计算机系统和网上业务安全法等，为电子商务安全构筑强制性规范体系，明确电子商务系统的安全要求和各主体的权利义务，设立长效稳定安全审查和管理制度，强制性地予以实施，制裁违反安全规则的行为。

(1) 信息网络安全法律法规

信息网络安全法律法规旨在加强计算机信息网络管理和安全保护，包括确立通信网络单元分级保护及符合性评测、安全风险评估、互联网网络安全信息通报、域名系统安全防护，以及木马、僵尸网络和移动互联网恶意程序监测等法规。

(2) 商用密码管理及应用法律法规

商用密码管理及应用法律规范确立了商用密码产品科研、生产、销售、使用的专控管理制度，对商用密码产品在信息安全等级保护中使用、含有密码技术的信息产品采购等做出了规定，明确基于密码技术开展电子认证服务的相关要求。

(3) 计算机信息系统和网上业务安全法律法规

计算机信息系统和网上业务安全法律规定确立了信息安全等级保护、计算机信息系统安全专用产品检测和销售许可等计算机信息系统保护基本制度，对金融、交通等重要信息系统保护提出了明确要求。

(4) 网络信息服务管理与内容安全法律法规

网络信息服务管理与内容安全法律规定确立了经营性互联网信息服务许可和非经营性互联网信息服务备案制度，明确对从事新闻、出版、教育等互联网信息服务实行前置审批，并清晰界定了互联网信息服务提供者维护互联网信息内容安全的责任和义务。

1.2.2　电子商务安全管理

应对电子商务的交易安全风险需要综合考虑管理安全。本章主要从电子商务风险管理、信用管理和企业内部管理三个方面重点介绍电子商务安全管理的相关内容，分析企业电子商务安全管理存在的主要问题，并提出针对性的建议。如图 1-3 所示。

(1) 风险管理

风险管理是指经济实体通过风险识别、风险预测、风险评估等手段，对风险实施有效控制，妥善处理风险所造成的损失，期望以最小的成本获得最大安全保障的管理活动。在电子商务安全中，风险管理是指对企业运营过程中面临的可能危害企业利益的内部和外部的不确定性，进行预测、分析和衡量，制订并执行相应控制措

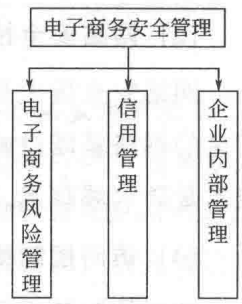


图 1-3　电子商务安全管理体系框架