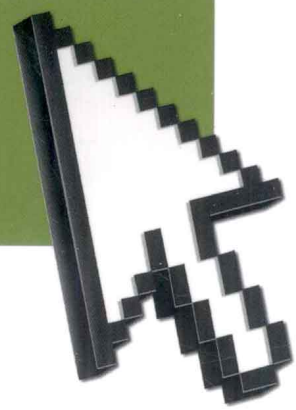
电子商务终端安全

DIANZISHANGWU ZHONGDUANANQUAN

周付安 刘咏梅◎编著



经济科学出版社
Economic Science Press

北京市属高等学校人才强教计划资助项目（编号：PHR201007208）

电子商务终端安全

周付安　刘咏梅　编著

经济科学出版社

图书在版编目（CIP）数据

电子商务终端安全／周付安，刘咏梅编著．
—北京：经济科学出版社，2011.8
ISBN 978-7-5141-1012-8

Ⅰ.①电… Ⅱ.①周… ②刘… Ⅲ.①电子商务－终端设备－安全技术 Ⅳ.①F713.36

中国版本图书馆 CIP 数据核字（2011）第 182132 号

责任编辑：王东岗
责任校对：徐领柱
版式设计：代小卫
技术编辑：王世伟

电子商务终端安全
周付安 刘咏梅 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
总编部电话：88191217 发行部电话：88191540
网址：www.esp.com.cn
电子邮件：esp@esp.com.cn
北京中科印刷有限公司印装
787×1092 16 开 19.75 印张 460000 字
2011 年 8 月第 1 版 2011 年 8 月第 1 次印刷
ISBN 978-7-5141-1012-8 定价：36.00 元

版权与免责声明

在本书的编著过程中，为了更清楚地阐述问题，在有些部分使用了相关网络资源和软件的应用说明，正是这些内容使得本书更加生动、鲜活，使得所说明的问题更加清楚，在此向各个资源的提供者和软件厂商一并致谢。凡本书注明网站网址或注明“截图自……”的所有案例、文字、图片，均转载自网络和引用自各种软件，本书使用是出于传递更多信息之目的，其版权归原作者及网站所有。如其他媒体、网站或个人使用，必须保留本书所注明的“稿件来源”，并自负版权等法律责任。

本书未注明“稿件来源”的文、图、表、模型等内容，版权属于本书作者所有，任何媒体、网站或个人未经书面协议授权不得转载或以其他方式复制发表。已经获取本书作者书面协议授权的媒体、网站或个人，在使用时必须注明“稿件来源：《电子商务终端安全》周付安，刘咏梅”，违者将依法追究其责任。

如涉及版权等问题，请事件相关人在两周内与我们联系，邮箱：dzswzdag@126.com。

前　言

随着信息技术日新月异的发展，人类正在进入以网络为主的信息时代，Internet 的高速发展不仅方便了人们的通信和交流，同时也带来了商业和经济模式的变革。基于 Internet 开展的电子商务已逐渐成为人们进行商务活动的新模式，电子商务的发展前景十分诱人，但安全问题是制约其发展的重要因素，是关系到电子商务系统能否成功运行的最为重要的问题。如何建立一个安全、便捷的电子商务应用环境，保障整个商务活中信息的安全性，使基于 Internet 的电子交易方式与传统交易方式一样安全可靠，已成为大家十分关心的问题。

本书的核心目标是为计算机终端用户设计出一套完整的电子商务安全体系。安全的电子商务体系包括环境因素、人为因素和风险防范与补救三个方面。其中，环境因素中又包括系统安全保障和网络安全保障两个方面。系统保障包括系统安全配置、计算机病毒的防范和查杀、移动介质的安全、机密文件的安全四项内容。网络保障包括网络环境配置、防范计算机木马、防范钓鱼网站三项内容。行为因素包括遵守网络安全行为规范、遵守交易规则和流程、防范欺骗和诈骗三项内容。风险防范与补救包括主动检测和计算机取证两项内容。只有保障了系统中各个环节的安全，才能最终保障整个电子商务系统的安全。

本书由浅入深，在帮助读者分析了解电子商务种种诈骗形式后，提示读者提高网络交易的自我保护意识；同时，从防范安全威胁角度出发，提出保障计算机系统安全、网络环境安全、交易流程安全的措施和方法；把纯技术性的操作系统及网络系统的安全问题，以工具书或使用手册形式展现，方便读者快速查阅并即时使用；计算机取证章节，不仅告知遭受威胁的人寻找挽回途径，同时警醒读者防范风险而保留必要的证据。

可以说，从 1998 年 3 月，中国第一笔互联网网上交易成功开始，中国的电子商务的追随者们就已经开始了和网络诈骗的斗争！我们能够做到的是希望帮助大家建立更强的安全意识，防患于未然；同时，当遇到电子商务安全问题时，知道怎么去解决。来吧，让我们一起，向更理想的电子商务时代迈进！

周付安　刻咏梅

2011 年 8 月 2 日

目　录

第一篇　电子商务安全

第二篇　系统安全

第三篇　网络安全

第四篇　交易安全

第五篇　安全检测与取证

第一篇

电子商务安全

第一章　电子商务安全概述

作为一种信息时代国际通行的商务模式，电子商务的深入发展引发了一场广泛、深刻的商业变革。据不完全统计，2010 年中国网络零售交易额为 5000 亿元，预计到 2011 年年底中国网络零售交易额有望突破 8000 亿元，并将首度达到中国国民经济总额的 5%，成为中国“主流经济”体系中的一部分。截至目前，我国大约有 150 万个职业网店卖家，进行电子商务活动的网民数量接近 1.5 亿人，且数量还在不断增加。作为中国最大的 C2C 电子商务平台，阿里巴巴集团旗下的淘宝网（www. taobao. com），目前在线商品数量超过 5 亿件，日新增在线商品 1000 万件，日交易额达到 12 亿元。

与电子商务快速发展同时出现的是其日益凸显的安全问题。现实中，电子商务面临的安全威胁非常之多，电子商务安全事件已经成为常态性、多发性和普遍性的事件。针对电子商务进行的欺骗和攻击也逐渐呈现出了产业化和规模化的趋势，但是用户普遍缺乏相应的安全意识。电子商务安全已然成为影响电子商务公信力和社会稳定的一个重要问题。研究和解决电子商务存在的安全问题，减少电子商务中安全事件的发生，已经迫在眉睫。

第一节　电子商务的概念和分类

了解电子商务的概念和分类是排除和解决电子商务中存在的安全问题的基础。电子商务的类型非常多，其组织方式和运行方式也存在较大的差异，其面临的安全威胁也不尽相同。

一、电子商务的概念

电子商务（electronic commerce，E-commerce），是伴随信息技术（特别是互联网技术）的发展而产生的新兴商业模式。1997 年布鲁塞尔全球信息社会标准大会对电子商务给出的一个明确定义是：“电子商务是各参与方之间以电子方式而不是通过物理交换或直接物理接触完成业务交易的商业活动”。

电子商务从根本上不同于传统的面对面交易或面对面洽谈的贸易方式，它减少了贸易的中间环节，用电子单证和电子数据交换替代了以往的纸张单证和书面单证往来，使得通常由买方和卖方直接参与的多个孤立的贸易环节能够得以电子化集成和自动化完成，因此既提高了效率，又节约了贸易成本。

二、电子商务的分类

电子商务都是以网站为交易平台进行商贸活动的，因此电子商务与电子商务网站是密不可分的。电子商务网站的种类繁多，所涉及的行业和服务类型也非常多。按照不同的分类标准，可以将电子商务网站分为不同的类别。

（一）按照电子商务网站的经营内容

按照电子商务网站经营内容的不同，可以将电子商务网站大致分为综合商城、专一整合网店、百货商店网店、品牌专卖网店、服务型网店等几类。

1. 综合商城

电子商务中的综合商城是指超大型购物平台网站，这种购物网站涉及成千上万个商家，范围遍布全国各地，商品的种类丰富，提供的服务齐全。该类型的网站一般拥有人数众多、分工细致的平台管理人员，以及专门的即时通讯交流客户端软件。

此类电子商务网站的代表是淘宝网、拍拍网等。

2. 专一整合网店

专一整合网店是指将电子商务模式与传统零售商店进行创新性融合，以现代化的网络平台整合某一行业的商品资源，并且通过对商家的规范管理和对客户提供优质服务来获取发展空间。例如，赛 V 网主要经营体育用品品牌业务，其经营模式是通过整合各种品牌体育用品商家的信息与资源完成的。

此类电子商务网站的代表是赛 V 网等。

3. 百货商店网店

百货商店网店从形式上表现为大型超市的网络化。该类电子商务网店主要特征是只有一个或者几个商家，通过电子商务网站发布商品和出售商品。自有仓库、提前采购、商品发布、物流配送和客户服务构成了该类型网站的要件。

此类电子商务网站的代表是当当网、卓越网、京东商城等。

4. 品牌专卖网店

品牌专卖网店是将传统商品电子商务化而衍生的网店。该类网店多为一些知名企业或者品牌为了增加产品销售渠道而建立的电子商务网站。

此类电子商务网站的代表是凡客诚品、梦芭莎、联想官网在线商城等。

5. 服务型网店

服务型网店是以提供各种服务为主要经营项目的网店。其项目多为票务订购、证券交易、人身保险等服务。例如，携程旅行网就是为用户提供车票、机票、酒店预订的服务型电子商务网站。

此类电子商务网站的代表是携程网、中国平安官网等。

（二）按照电子商务的交易主体

按照电子商务中交易双方的主体不同，可以将电子商务网站分为 C2C、B2C、B2B 等

不同类型，其中 C 是英文 Consumer（顾客）的首写字母，而 B 是英文 Business（商业）的首写字母。

1. C2C 电子商务网站

C2C 是 Consumer to Consumer 的缩写，是用户对用户的电子商务模式。C2C 电子商务网站模式的最大特点是为买卖双方提供在线交易平台，并且提供第三方支付平台，同时也会对交易双方的行为进行监管，当出现交易纠纷时也会进行调解和仲裁。C2C 电子商务网站可以被认为是买卖双方的“中介”和“裁判”。

在 C2C 电子商务网站中，用户既可以通过网站发布商品成为“卖家”，也可以在网站上购买商品成为“买家”。当然，用户要成为卖家需要通过网站的身份认证，认证方式一般是身份证认证或者其他方式认证。C2C 一般的交易流程如图 1.1.1 所示。

此类电子商务网站的代表是淘宝网、拍拍网、易趣网等。

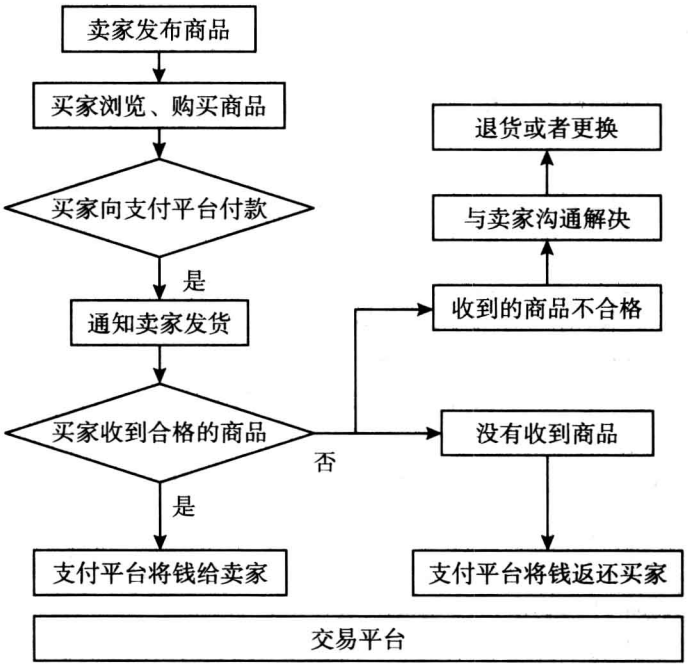


图 1.1.1　C2C 交易流程

C2C 交易流程大致分为以下几步：

第一步，买方在电子商务网站上浏览并选择商品，并进行在线支付。

第二步，卖方确认订单后将买方网上支付的请求发送给第三方支付平台。

第三步，买方在线支付货款至第三方支付平台。

第四步，第三方支付平台向卖方发送支付结果，并通知其发货。

第五步，卖方根据反馈的支付结果，发送商品。

第六步，买方收到所购买的商品后，通知第三方支付平台付款给卖方。

第七步，卖方与第三方支付平台结算货款，卖方收款。如有纠纷，则通过管理平台

解决。

2. B2C 电子商务网站

B2C 是 Business to Consumer 的缩写，是企业对用户的电子商务模式。B2C 的运行模式有很多种，依据 B2C 电子商务平台所有者归属的不同，大致可以将 B2C 电子商务分为私有电子商务平台和公共电子商务平台。私有电子商务平台是指电子商务网站所使用的平台是企业独立研发、独立应用的平台，如凡客诚品网站；公共电子商务平台是指由第三方所建立，并且是任何企业都可以进入的平台，如淘宝商城。

显而易见，私有平台和公共平台在运行方式上存在着较大的差异：一是私有平台的技术实现、运行维护、交易规则都是企业自己设定的，而公共平台则是独立于企业的第三方设计并实现的；二是公共平台中有交易管理和纠纷仲裁功能，而私有平台是通过自我管理、客户服务实现的，并没有第三方的监督功能；三是公共平台的支付方式一般都是通过第三方支付平台在线支付进行，而私有平台的支付方式一般都是直接对商家进行支付，有的也支持货到付款等支付形式。

此类电子商务网站的代表是凡客诚品、淘宝商城等。

B2C 交易的流程分为以下几步，如图 1.1.2 所示。

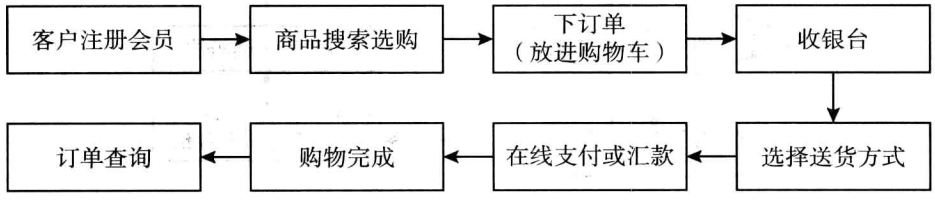


图 1.1.2　B2C 交易流程图

第一步，用户访问电子商务网站，选择所需购买的商品。

第二步，选择所需商品放入购物车。

第三步，填写订单，包括收货地址、联系方式、选择支付手段并进行支付。

第四步，商家按照订单要求进行物流派送。

第五步，客户购物完成。

3. B2B 电子商务网站

B2B 是 Business to Business 的缩写，是企业对企业的电子商务模式。B2B 电子商务是企业借助 B2B 交易平台进行的企业级的电子商务贸易活动，相对于普通的 B2C 交易，一般的 B2B 交易在商品数量上更多，物流方式更为复杂。

此类电子商务网站的代表是阿里巴巴、慧聪网等。

B2B 交易流程如图 1.1.3 所示，大致分为以下几步[①]：

① 转引自 http://baike.wwwwx.cn/index.php?doc-view-87　浏览时间 2010.9.10。

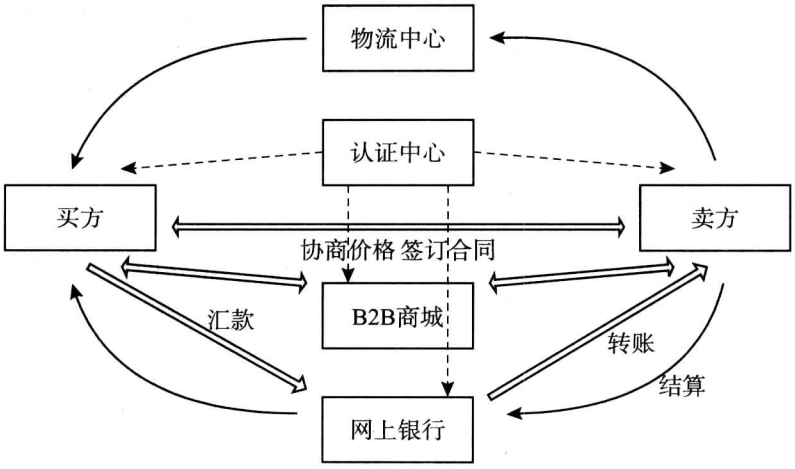


图 1.1.3　B2B 交易流程

第一步，商业客户向销售商订货，首先要发出“用户订单”，该订单应包括产品名称、数量等。

第二步，销售商收到用户订单后，根据订单的要求向供货商查询产品情况，发出“订单查询”。

第三步，供货商在收到并审核完“订单查询”给销售商返回“订单查询”的回答。基本上是有无货物等情况。

第四步，销售商在确认供货商能够满足商业客户“用户订单”要求的情况下，向运输商发出有关货物运输情况的“运输查询”。

第五步，运输商在收到“运输查询”后，给销售商返回运输查询的回答。

第六步，在确认运输无问题后，销售商即刻给商业客户的“用户订单”回复，同时要给供货商发出“发货通知”，并通知运输商运输。

第七步，运输商接到“运输通知”后开始发货，接着商业客户向支付平台发出“付款通知”。支付平台和银行结算票据等。

第八步，支付平台向销售商发出交易成功的“转账通知”。

第二节　电子商务安全认知

从电子商务诞生起，安全问题就如影随形。部分用户因为担心安全问题而不愿使用电子商务。电子商务的安全问题成为影响电子商务发展的主要因素。

一、电子商务安全的含义

安全是电子商务的核心和灵魂，也是开展电子商务活动的基础和前提。电子商务的安

全是一个动态的、涉及多个方面的问题，并且是不能单纯依靠技术就彻底解决的。电子商务是一个包含着诸多环节的系统问题，任何一个环节出现问题或者纰漏都会造成影响。下面分别从电子商务流程角度、网络信息安全角度和用户进行电子商务活动等角度来分析电子商务安全的含义。

（一）电子商务交易流程角度

电子商务的交易类型非常多，但是基本的交易流程却大抵相同，如图 1.1.4 所示。从电子商务流程角度看，电子商务的安全就是电子商务中进行交易过程中的安全。

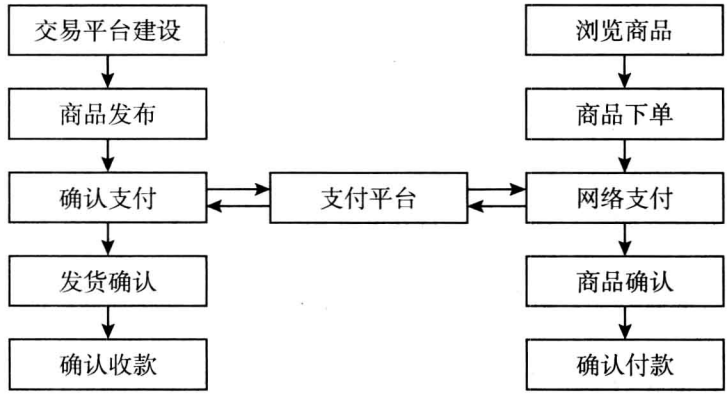


图 1.1.4　电子商务交易流程

电子商务流程包括用户使用自己的计算机登录电子商务网站、浏览商品链接、在线支付、物流交付等几个基本环节。

1. 用户的计算机安全

用户的计算机安全包括用户使用的系统安全和物理安全。如果用户所使用的计算机本身感染了病毒或木马，则该用户在进行电子商务活动时的安全风险会大大增加。

2. 电子商务网站的安全

电子商务网站的安全大致包含三个方面的内容：一是电子商务网站的系统安全和物理安全；二是电子商务网站所使用的平台系统的稳定性和安全性；三是电子商务网站网络环境的安全。

3. 商品链接的安全

商品链接的安全是指用户在进行电子商务活动时，所登录的电子商务网站是真实的，所浏览的商品链接是真实电子商务网站中的商品。

4. 电子支付的安全

电子支付的安全包括三方面，一是用户所使用的网络银行、支付宝、财付通等支付工具的安全，即保证这些网银或者支付账户的安全，避免身份被冒用和财产被盗；二是保证支付过程中的安全，即能正确使用支付工具进行支付，不被钓鱼网站欺骗；三是按照电子商务的交易流程进行确认付款的安全，即严格按照交易流程进行付款。

5. 电子商务交易的安全

电子商务的交易安全是指在电子商务交易的过程中，能严格按照电子商务交易的流程进行交易，避免骗子利用各种欺骗手段进行诈骗。

（二）网络信息安全角度

从网络信息安全角度来看，电子商务的安全就是电子商务中的各种信息在传递过程中的安全。电子商务中的信息在电子商务网站、商家、用户、支付平台等几个对象之间相互传递。保证信息传递的安全，就是要防止信息在传递过程中遭到窃听、盗取、篡改和伪造。[①] 信息安全需要做到以下几点：

1. 保密性

电子商务活动的保密性是指对信息进行加密，并保证信息不被非授权的人或者实体窃取。随着网络嗅探等技术的发展，在网络上明文传输的信息几乎毫无安全性可言。因此，电子商务活动中传递的信息尤其是机密信息（如账号密码信息或者网银信息等），一定要经过加密处理，然后再进行网络传输，即便他人截获或者窃取了数据，也无法识别信息的真实内容。

2. 完整性

电子商务活动的完整性是指信息在发送和接收的过程中，要保证数据的一致性，防止数据被别有用心的人建立、修改和破坏，保证信息在传输过程中的完整性和正常传输。电子商务是经过网络传输信息的，如果出现信息的丢失、重复或者传送的次序差异等情况，就会导致买卖双方的信息传递出现障碍。

3. 不可抵赖性

电子商务活动的不可抵赖性是指发送方不能否认已经发送的信息，接收方也不能否认已经接收的信息。不可抵赖性是电子商务安全的重要要求，是进行安全电子商务活动的基础。

4. 真实性

电子商务活动的真实性是指交易活动中双方身份的真实性。在电子商务活动中，交易的双方相互不见面，彼此只通过网络账号找到对方、和对方交流。由于网络的虚拟性，使得身份冒用成为可能，电子交易的首要安全要求就是要保证身份的真实性。这就意味着在双方进行交易前，首先要能确认对方的身份，要求交易双方的身份不被假冒或伪装。

5. 可靠性

电子商务活动的可靠性是指有效避免计算机的物理故障、自然灾害、程序错误和计算机病毒等所造成的潜在威胁，务必确保计算机系统在可靠、安全、稳定的状态下运行。

6. 内部网的严密性

内部网的严密性是指能够有效避免和降低信息传递所面临的安全威胁，确保不受未经授权的人或者实体入侵。例如避免计算机系统被能物理接触到计算机的人员非授权登录、

① 蒋丽．安全电子商务的实现技术研究［J］．网络安全技术与应用，2011.4.