第3章 电子交易安全

在介绍了信息安全的基础知识和技术后，本章重点介绍与电子交易相关的安全技术。本章将从电子交易过程的安全性、交易信息安全以及电子交易的信任机制三个方面进行阐述，见图 3-1。

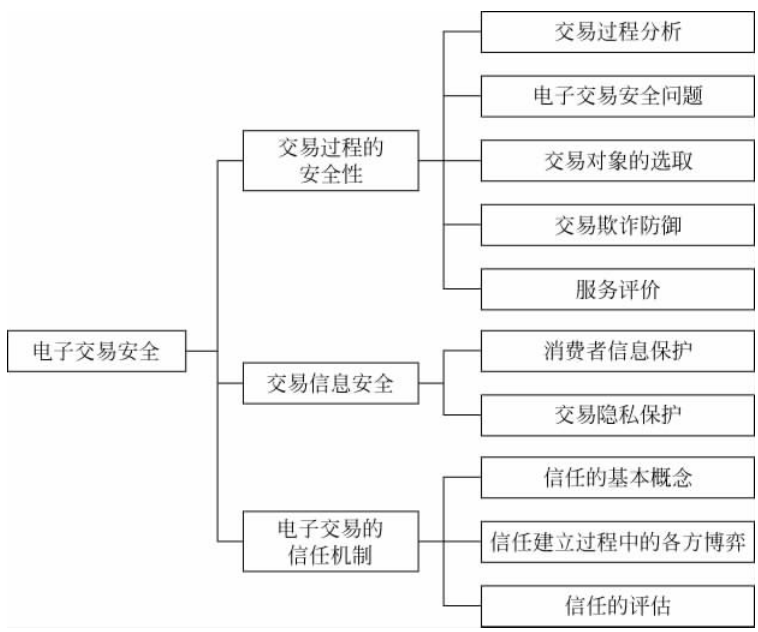

图 3-1　本章主要内容结构

3.1 交易过程的安全性

电子商务的核心是网上交易，尤其是通过公共的因特网将众多的社会经济成员联系起来的网上交易更是成为发展的热点。根据中国互联网络信息中心(CNNIC)发布的《2013 年中国网络购物市场研究报告》显示，2013 年网络购物市场继续快速向前发展，交易金额达到 1.85 万亿元，较 2012 年增长 40.9%。截至 2013 年 12 月，我国网络购物用户规模达到 3.02 亿人，较上年增加 5987 万人，增长率为 24.7%，使用率从 42.9%提升至 48.9%。在当前电子商务快速发展的过程中，电子交易的安全问题还没有得到很好的解决，电子商务交易面临一系列安全隐患。

3.1.1 交易过程分析

与传统交易活动一样，电子商务交易也可分为三个阶段：交易前、交易中、交易后，只不过电子商务交易主要借助于互联网这个媒介，而不再是传统交易的面对面的方式。

1. 交易前：买方与卖方的准备

这一阶段主要是指买卖双方和参加交易各方在签约前的准备活动。

买方根据自己要买的商品，准备购货款，制订购货计划，进行货源市场调查和市场分析，反复进行市场查询，了解各个卖方所属地的贸易政策，修改和完善购货计划和进货计划。非个人的买方，可能还需要确定和审批购货计划，再按计划确定购买商品的种类、数量、规格、价格、购货地点和交易方式等，尤其要利用 Internet 和各种电子商务网络寻找自己满意的商品和商家。

卖方根据自己所销售的商品，召开商品新闻发布会，制作广告进行宣传，全面进行市场调查和市场分析，制订各种销售策略和销售方式，了解潜在买方所属国的贸易政策，利用 Internet 和各种电子商务网络发布商品广告，寻找贸易伙伴和交易机会，扩大贸易范围和商品所占市场的份额。其他参加交易各方包括中介方、银行金融机构、信用卡公司、海关系统、商检系统、保险公司、税务系统、运输公司也都为进行电子商务交易做好准备。

2. 交易中：交易谈判、签订合同与办理手续

这一阶段分为两个部分。交易谈判、签订合同主要是指买卖双方对所有交易细节进行谈判，将双方磋商的结果以文件的形式确定下来，即以书面文件形式和电子文件形式签订贸易合同。电子商务的特点是可以签订电子商务贸易合同，交易双方可以利用现代电子通信设备和通信方法，经过认真谈判和磋商后，将双方在交易中的权利，所承担的义务，对所购买商品的种类、数量、价格、交货地点、交货期、交易方式和运输方式、违约和索赔等合同条款，全部以电子交易合同做出全面详细的规定，合同双方可以利用电子数据交换（EDI）进行签约，可以通过数字签名等方式签名。

办理手续主要是指买卖双方签订合同后到合同开始履行之前办理各种手续的过程，也是双方贸易前的交易准备过程。交易中要涉及有关各方，即可能要涉及中介方、银行金融机构、信用卡公司、海关系统、商检系统、保险公司、税务系统、运输公司等，买卖双方要利用 EDI 与有关各方进行各种电子票据和电子单证的交换，直到办理完可以将所购商品从卖方按合同规定开始向买方发货的一切手续为止。

3. 交易后：交易合同的履行和索赔

这一阶段是从买卖双方办完所有手续之后开始，卖方要备货、组货，同时进行报关、保险、取证、信用等，卖方将所购商品交付给运输公司包装、起运、发货，买卖双方可以通过电子商务服务器跟踪发出的货物，银行和金融机构也按照合同处理双方收付款、进行结算、出具相应的银行单据等，直到买方收到自己所购商品，完成了整个交易过程。索赔是在买卖双方交易过程中出现违约时，需要进行违约处理的工作，受损方要向违约方索赔。

图 3-2 所示为电子商务交易过程。

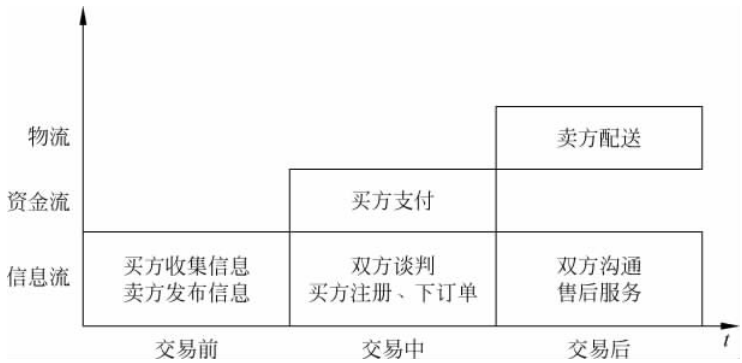

图 3-2 电子商务交易过程

3.1.2 电子交易安全问题

电子交易的安全现状不容乐观。首先是依靠网络的电子交易必须面临着现在各种各样的网络安全问题，而且直接涉及经济信息的电子交易是不法分子攻击的重灾区，所以一旦电子交易的安全出现问题，便会导致直接的经济利益损失。从官方发布文件《2012 年中国互联网违法犯罪问题年度报告》来看，形势是触目惊心的。2011 年 7 月至 2012 年7 月，中国估计有超过 2.57 亿人成为网络犯罪受害者，直接经济损失达人民币 2890 亿元。同一时期，被网络犯罪侵害的在线成人达 72%（即每天有超过 70 万名中国网民遭受网络犯罪的侵害，每分钟有 489 名受害者），平均每位网络犯罪受害者蒙受的直接经济损失达到人民币 1126 元。其中电子交易占很大一部分，而且这种情况并未得到改善。由 360 互联网安全中心基于大数据统计分析而发布的《2014 年上半年中国网购安全报告》显示，2014 年上半年 360 网购先赔服务共接到网络欺诈报案约 1.3 万例，占开启网购先赔服务用户的比例接近万分之一。这意味着，每一万名网购消费者中，就有一个人实际遭遇网购损失。网络欺诈手法花样百出，层出不穷，让人防不胜防。案例一：资深股民高先生在浏览股市信息时，无意中发现了一个名为“国金证券”的网站，该网站每天推荐三只包涨停的股票。为了提前看到推荐的股票，高先生按网站的要求，汇去了 9888 元“入会费”，正式成为该网站的会员。后来该网站又以要求“验证”客户资金为由，要求高先生汇入更多的资金到对方指定的账户。可是接下来几天过去，网站并没有归还其资金，高先生想再联系该网站的时候，却发现电话打不通，网站也已经注销。案例二：最近有一个网友上淘宝购物，于是卖家通过即时通信软件，给网友发了一个 RAR 的压缩包。解压后是个类似“图片”的文件，可是当网友运行以后提示错误，于是卖家声称“发成店铺装修工具了”。首先网友下了一笔 39 000 元的订单，接着又下了第二个 7800 元的订单，可是网银支付成功后返回淘宝确认的页面居然出现错误。后来网友发现自己的钱已经被银行扣除，才知道自己已经被骗了四万多块钱。这些案例可以说是电子交易中的典型案例。而 2012 年还发生了一件举世瞩目的“浮云”木马网银盗窃案，江苏省徐州警方破获将木马程序植入受害人计算机、窃取网银资金案，警方抓获一犯罪团伙嫌疑人 50 余名，涉案金额 1000 余万元，木马可以轻易攻破 20 多家银行的网银系统，让人不寒而栗。

1. 交易信息安全

电子交易安全指电子商务交易在网络媒介中体现出来的安全问题，也就是要实现电子

商务交易信息的保密性、完整性、真实性和不可抵赖性。

信息安全是指由于各种原因引起的信息泄露、信息丢失、信息篡改、信息虚假、信息滞后、信息不完善等，以及由此带来的风险。具体的表现有：个人私密信息被盗取；窃取商业机密；泄漏商业机密；篡改交易信息，破坏信息的真实性和完整性；接收或发送虚假信息，破坏交易、盗取交易成果；伪造交易信息；非法删除交易信息；交易信息丢失；病毒破坏；黑客入侵等。如果信息被非法窃取或泄露，可能给有关企业和个人带来严重的后果和巨大的经济损失。如果不能及时得到准确、完备的信息，企业和个人就无法对交易进行正确的分析和判断，无法做出符合理性的决策。非法删除交易信息和交易信息丢失可能导致经济纠纷，给交易的一方或多方造成经济损失。最常见的信息风险是信息的非法窃取和泄露，它往往引起连锁反应，形成后续风险，这也是目前企业和个人最担心的问题。信息风险的典型表现是网络欺诈，它不仅使厂商和消费者在经济上蒙受重大损失，更重要的是可能会打击人们对电子商务这种新的经济形式的信心。

在早期的电子交易中，曾采用过一些简单的安全措施。例如将网上交易中最关键的数据如信用卡号码及成交数额等用电话告知，以防泄密，网上交易后再用其他方式对交易做确认，以保证其真实性和不可抵赖性。这些方法不仅操作不便，而且有一定的局限性，也不能实现其真正的安全性。电子商务安全中普遍存在以下几种信息安全隐患。

1）窃取信息

由于未采用加密措施，数据信息在网络上以明文形式传送，入侵者在数据包经过的网关或路由器上可以截获传送的信息。通过多次窃取和分析，可以找到信息的规律和格式，进而得到传输信息的内容，导致消费者消费信息、账号密码和企业商业机密等信息的外泄。

2）篡改信息

当入侵者掌握了信息的格式和规律后，通过各种技术手段和方法，将网络上传送的信息数据在中途修改，然后再发向目的地，从而破坏信息的真实性，入侵者通过改变信息流的次序，更改信息的内容，删除信息的某些部分，甚至在信息中插入一些附加内容，使接收方做出错误的判断与决策。这种方法并不新鲜，在路由器或网关上都可以做此类工作。

3）信息假冒

由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨。常见的方式有伪造用户和商户的收订货单据，套取或修改相关程序的使用权限等。

4）恶意破坏

由于攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机要信息，甚至可以潜入网络内部，其后果是非常严重的。

2. 交易财产安全

财产安全是指在进行电子商务交易时由于各种原因造成电子商务参与者面临的财产或利益安全。财产安全一直都是广大网民最关心的也是最担心的问题，因为财产安全直接涉及网民最根本的利益。财产安全往往是电子商务安全问题的最终表现形式，也是信息安全问题和交易安全问题结果的表现。财产安全问题主要表现为财产损失和其他经济损失。前者如：客户的银行资金被盗取；交易者被冒名，其财产被窃取。后者如：信息的泄露、丢失，

使企业的信誉受损，经济遭受损失；遭受网络攻击或故障，企业电子商务系统效率下降甚至瘫痪等。如果财产安全得不到保证的话，相信电子商务也很难取得进一步的发展。

3. 信任问题

1）主要表现

（1）网络欺诈时有发生

网络欺诈是网民在网络购物时最常见的问题。电子商务经营者实施的网络欺诈行为主要是利用网络交易的虚拟性、间接性特征，发布虚假的或者不完整的商品信息诱导网上购物者，诈骗网上购物者的购物款。

（2）虚假信息充斥网络

在网络这一新兴媒体中，发布信息不再像传统媒体那样会受到那么多的制约，而且由于网络的虚拟特点，一般消费者即使觉察到信息的错误，也很难向发布信息者进行追究，甚至根本就不知道网络企业的地址。在网络上，由于双方没有发生直接面对面的接触，仅仅通过网络上的简单的字符认识对方，对于对方所提供信息的真实性难以判断。一些不诚信的商家利用这一点发布虚假的商品信息，夸大其词，吸引消费者；注册虚假的个人信息，使消费者在仅仅通过网络平台的情况下，即使察觉也难以找到其本人。虚假信息一方面误导消费者，另一方面也给网络监管和消费者维权增加难度。因此，一些网络企业便表现得肆无忌惮，在网上发表各种各样的虚假信息，或者制造出各种各样的虚假新闻，以此来吸引消费者或创造所谓的点击率，从而扩大自己的商业影响，谋求经济效益。这种高度自由化的垃圾信息的出现，阻碍了正常的电子商务信息的传播，扰乱了健康的电子商务网络信息环境，进而在一定程度上影响了消费者对电子商务的信任感。

（3）假冒伪劣商品泛滥

电子商务虽然在诸多方面对传统商业交易有所改进，但电子商务交易双方无法面对面完成交易，消费者不能亲自对商品试用鉴别，这就使得消费者很难及时分辨商品的真假、质量的好坏等，也为假冒伪劣商品的泛滥提供了机会。

（4）消费维权困难重重

近年来，在每年的“3·15”消费者权益保护活动上，与电子商务相关的消费者投诉呈直线上升态势。从已公布的这些消费者投诉案例来看，这些案件普遍具有虚拟性、技术含量高、跨区域的特点，消费者一旦发生消费纠纷，因为电子商务交易的虚拟性、匿名性、时空分离（支付与配送的时间分离、顾客与商家之间的空间分离）等特征，使得侵权方难找到、侵权证据难掌握、侵权责任难认定、侵权赔偿难落实，维权困难重重。

正是这些问题导致我国的电子商务信任正在一步步流失，这也最终影响着消费者的购买动机、满意度、忠诚度及推荐给他人。由此可见，我国要发展电子商务必须高度重视电子商务信任问题。

（5）信用评价问题

信用评价的出现是电子商务的进步，消费者通过评价了解卖家的信用及商品。信用评价是判断卖家诚信与否的重要标准，信用越高，消费者越容易信赖，说明了货物更可信，附加的商业价值就越高。正是网络诚信的高价值，有些商家为了提高信用度，进行信用炒作，网络上也出现了专门的信用炒作机构，也有些卖家为了攻击竞争对手，购买对方商品并恶意评

价，网络上也出现了专门恶意差评的人，我们称之为“职业差评师”。淘宝上信用炒作十分严重，虽然淘宝也严厉打击，但是屡禁不止。目前，我国一些主要的电子商务网站，如淘宝网、拍拍网、eBay 等都有各自的评价管理系统。以市场份额最大的淘宝为例，在淘宝上，几乎绝大多数的卖家都有刷信用的意识，比如一笔交易分成多次完成，以累积交易量或朋友之间相互买东西，创造虚假的交易。不仅信用低的卖家会通过这种手段提高信用，即使是信用高的“皇冠”卖家也会通过信用炒作来增加产品的人气和销量。

炒作信用对于消费者来说是一种欺诈行为，它蒙蔽了消费者，侵犯了消费者的知情权；对于卖家，则构成了不正当竞争。同时如果“虚假信用”不能得到及时打击，消费者一旦被“虚假信用”所蒙蔽，就可能蒙受一些损失，打击网络消费信心，深深地伤害了这一行业。

2）应对策略

（1）健全法律法规体系

近年来我国已经出台了一些有关法规，如《中华人民共和国电子签名法》、《国务院办公厅关于加快电子商务发展的若干意见》、《电子商务模式规范》、《非金融机构支付服务管理办法》和《网络购物服务规范》等相关法律法规，并在 2014 年 3 月正式实施修订后的新版《中华人民共和国消费者权益保护法》，但这与网络经济发展的要求相比还有不小的差距。如电子商务网站质量和服务方面的问题、电子商务操作的基本规则方面的法律问题、电子商务安全性方面的法律问题、信息基础设施和市场准入方面的法律问题、电子商务中的知识产权保护、司法管辖及法律冲突、电子商务中的税赋和关税问题等，都没有相应的法律法规进行规范。

要改善这些问题，一方面要在传统法律环境建设的基础上，通过对传统法律条文的修改或增加，实现对电子商务相关行为的规定；但另一方面，由于在实际生活中，消费者处于弱势地位，且他们在网上商店所购商品价值较小，依靠司法体系的解决方式也比较烦琐，对欺诈方的惩罚也更多地局限在对用户进行警告，对账户进行冻结、取消等方面，存在威慑力不强等情况。因此，也要加强对法律的监督执行。

（2）推行隐私保护机制

由于在购物过程中需要向网站提供个人信息（姓名、住址、电话、E-mail 等）以便于配送，消费者非常担心其个人隐私信息能否得到安全的保护和合理的使用。但目前国内的网站基本上意识不到保护用户隐私的重要性，这导致很多用户信息被盗用或买卖，严重损害了消费者的利益。目前国际上常用的两种有效降低用户隐私关注的策略是隐私声明和隐私保护。隐私声明是在商户的信息中告知用户将收集哪些信息，如何存储、使用与保护信息。而隐私标识则是由独立的第三方隐私认证机构所颁发给那些通过其审查的网站的符号，表明网站的隐私保护操作能够有效地保护用户的信息隐私。

（3）建立安全认证机制

身份欺诈是网上欺诈的主要形式，为后期交易的其他欺诈埋下了祸根。因为在交易伊始对交易方身份识别错误的前提下，后期再好的信任机制也徒劳无益。因此，要给交易者创造一个安全环境，首先需建立一个能对网络交易双方身份进行验证，对网上传递的信息给予证实的机构——网上认证机构（CA）与体系。

（4）发展第三方支付安全机制

第三方网上支付体系是目前电子商务发展的一个焦点，它通过与银行紧密合作，作为第

三方监管和技术保障的中介，安全实现客户间不同种类银行卡的在线货币支付、现金流转、资金清算、查询统计等，促进资金流动，同时将收款方与付款方隔离，有效地防止了资金欺诈和隐私泄漏，打开了制约电子商务发展的瓶颈，满足了电子商务中商家和消费者对信誉和安全的要求。它的出现和发展给电子商务发展带来了全新的生机和活力。

3）主要影响因素

（1）交易方的信誉

在电子商务条件下，交易双方是彼此看不见的，关于交易伙伴和产品的信息不可能完全掌握，参与交易将面临较大的风险。因此，与传统商务相比，电子商务条件下的信誉显得更加重要。

（2）交易历史

在电子商务中，交易历史包括顾客与多个商家的交易情况，以及商家与多个顾客的交易情况。如果顾客对商家提供的产品或服务不满意，他们可以将这种经历反映给负责管理商家信誉的可信任权威，从而对该商家的信誉产生影响。

（3）信任方的个性

信任方的信任水平与他的主观因素有关，如对潜在盈利的估计、风险偏好等。在同等条件下，不同实体的信任水平也不相同。

（4）文化背景

从社会学的角度讲，信任是社会关系的一个重要维度，是与社会结构和文化规范密切相关的社会现象。也就是说，信任与人文背景有关，由于社会文化的差异，不同社会中的信任度差别很大，这一现象已得到理论和实践两方面的证实。

3.1.3 交易对象的选取

在市场经济中，为了防范风险和提高交易的成功率，对于交易对象的选取是非常重要的。而交易对象的选取，又受到成本、场所和服务质量等因素的制约。

1. 交易成本因素

交易成本经济学认为，交易活动是稀缺的，交易成本不为零。企业存在就是为了节约交易成本。电子商务是与传统交易完全不同的一种交易形式，它能通过降低企业交易前、交易中和交易后的交易成本，降低企业的边际交易成本水平。由于边际交易成本水平的降低，企业边际组织成本必然相应降低，从而导致企业规模变小。企业在电子商务条件下进行投资决策时必须考虑到这种变化。

首先，我们要理解交易成本的含义。

利斯（R. H. Coase）在其 1939 年发表的著名论文《企业的性质》（*The Nature of the Firm*）中认为，交易成本是获得准确的市场信息所需要付出的费用，以及谈判和经常性契约的费用。后来交易成本经济学的又一代表人物奥利弗·威廉姆森（Oliver Williamson）认为，交易成本分为两部分：一是事先的交易成本，即为签订契约、规定交易双方的权利、责任等所花费的费用；二是签订契约后，为解决契约本身所存在的问题，从改变条款到退出契约所花费的费用。可以说，到目前为止，交易成本这个概念在经济学上完全可以与价格、分工等基本范畴等量齐观。

电子商务下企业交易成本的构成并没有与传统交易有本质的区别，仍然要包括度量、界定和保证产权（即提供交易条件）的费用，发现交易对象和交易价格的费用，讨价还价的费用，订立交易合约费用，执行交易的费用，监管违约行为并对之制裁的费用，维护交易秩序的费用等。电子商务下的企业仍然是为了节约交易成本而存在，但是电子商务本身具有的有别于传统交易的不同特点，使企业的交易成本具有很多独特之处。下面按交易过程对电子商务下交易成本的不同点进行分析。

交易前的成本。在进行交易之前，交易双方都需要进行信息的搜索，以找到合适的交易对象。现在随着全球一体化的发展和世界市场的形成，企业在交易之前所发生的成本在整个企业交易成本中占的比重越来越大。在传统交易中，交易双方的沟通需要经过许多不同的媒介，进行协调很困难。但在电子商务条件下，网络作为众多企业和客户进行交易的虚拟市场，任何企业或客户都可以使用一些专门的网络搜索引擎，方便快捷地收集到很多对方的信息，然后从中选择合适的进行交易。同样，电子商务条件下的广告不再是单向的信息流动，企业通过网络能够取得广告效果的反馈信息，从而可以更加容易地对客户的行为方式和偏好进行跟踪，改进生产或营销策略。因此，交易双方可以在网络中直接相互接触，相互选择，显著降低了搜索成本，缩短了搜索的时间，促进了交易的达成。

交易过程中的成本。完成信息的搜寻之后，交易双方开始接触，就交易的条款进行协商，最终达成合同。达成合同后，交易双方必须履行各自的责任，划拨款项，提供商品或服务。传统交易条件下，当企业和客户之间期望建立一种交易关系后，复杂的交易过程不仅加大了签约过程中的成本，而且延长了交易的时间。而在电子商务条件下，交易双方可以通过网上协商各种条款，直接在网上签订合同，避免了签约人员的奔波之苦和减少成本的支出。同时，通过各种网上的电子账单可以实现款项的直接划拨。这样，电子商务就加速了交易过程，降低了交易的签约和执行成本。

交易后的成本。交易双方在交易完毕之后，并不就是银货两讫，两不相干了，企业还应对商品使用或接受服务过程中出现的问题加以解决。在这些问题中，一些小的问题会最经常出现，这些问题在技术人员的指导下客户完全有能力解决。解决这些问题的费用是企业交易成本的另一个重要构成部分。传统交易条件下，客户在使用商品或接受服务过程中出现了这些问题之后，需将这些问题反馈到企业的服务部门，然后交由企业的技术部门解决。问题反馈到企业需要一定的时间，企业解决问题还需要一定时间。这样企业必须同时设立专门接受问题的机构和解决问题的机构，增加了成本支出，同时还延误了问题的解决，给客户带来了不便甚至损失。电子商务条件下，一旦货物或服务出现问题，客户可以随时将信息反馈到企业的信箱或网站中，可以与企业专门设立的网上技术服务人员进行交流，在他的指导下实现问题的快速解决。所以，电子商务减少了冗余人员和售后成本，缩短了问题解决的时间和与客户的距离，方便了客户，为下一次交易的成功奠定了基础。

2. 交易场所因素

整体来看，中国网络购物发展环境向好。网购市场发展面临的政策环境更加宽松，市场内部结构和环境也更趋优化。同时，随着互联网普及率的持续上升，网民对互联网的使用也更加成熟，但也存在着不少问题。

其一，国内缺乏统一的物流配送市场，影响网民的网购热情。逐步增多的物流公司和配

送系统不仅给交通系统增加了压力，也使得物流行业呈现高度分散化的局面。而物流行业整体的改进则需要政府、企业和相关行业协会的共同协作。

其二，售后服务的责权划分不明确，相关服务的保障性不强。作为新的经济形式，我国网络购物行业目前还没有纳入国家统一口径管理。尤其是在网络交易的服务纠纷上，虽然有一些行业标准，但是都还没有上升到法律的高度。目前，对网购消费者的服务和保护大多是网商自发的行为，服务的规范性还有待加强。

其三，网络安全诚信环境较差，制约网购市场向更大规模发展。目前，我国网民对在网上开展商务活动的信任度较低，仅有 29.2%的网民认为网上交易是安全的，不到四成的网民愿意在网上填写真实信息。安全性担忧是消费者不愿意进行网络交易的重要原因。为了促进网络购物市场向更大规模发展，安全可信的网络交易环境的建立刻不容缓。

3. 服务质量因素

服务与人们的生活息息相关，服务理念和服务态度已经成为企业文化的重要组成部分，也是企业外部形象塑造是否成功的关键所在。对于什么是服务，不同的专家学者进行了不同的定义。ISO 9004-2：1991《质量管理和质量体系要素第 2 部分：服务指南》中“服务”的定义是：“服务(Service)为满足顾客的需要，供方与顾客接触的活动和供方内部活动所产生的结果。”

不可感知性是服务最为显著的一个特征，它可以从三个不同的层次来理解。第一，服务的很多元素看不见，摸不着，无形无质；第二，顾客在购买服务之前，往往不能肯定他能得到什么样的服务，因为大多数服务都非常抽象，很难描述；第三，顾客在接受服务后通常很难察觉或立即感受到服务的收益，也难以对服务的质量做出客观的评价。正因为服务的不可感知性，许多服务业为了变不可感知为可感知，常常通过服务人员、服务过程及服务的有形展示，并综合运用服务设施、服务环境、服务方式和手段等来体现。

B2C 电子商务服务质量评价影响因素模型见表 3-1。

表 3-1　B2C 电子商务服务质量评价影响因素模型

服务质量特性	服务质量指标	服务质量特性	服务质量指标
交易安全性	交易安全机制	响应性	服务的柔性
	个人隐私保密性	服务完整性	提供的付款方式的灵活性
	交易过程的安全性		产品的准备速度
可靠性	承诺履行情况		产品配送方式及速度
	承诺兑现的时间		售后服务情况
	解决问题的真诚性		顾客信息反馈的便利性
	服务信息的准确性	移情性	个性化服务
有形性	网页整体设计		定制化服务
	网站界面友好程度		便利服务
	页面反应速度		关心顾客
	交易流程设计	补救性	顾客投诉处理机制
响应性	处理顾客要求时的快捷性		补救性服务措施的完整性
	顾客获得帮助时的等待时间		补救性服务提供的速度

3.1.4 交易欺诈防御

在网络贸易欺诈案件中，主要有四大主流欺诈类型：收款不发货、严重货不对板、虚假订单、收货不付款。

对于欺诈的定义，各国法律有不同的司法解释。美国《布莱克法律辞典》对欺诈的解释为：欺诈是指故意歪曲事实，诱使他人依赖于该事实而失去属于自己的有价财产或放弃某项法律权利。通过语言或行为，通过说谎或错误引导，或者隐瞒应该披露的事实虚假地陈述事实，使别人据此行动从而造成法律上的损失。有时欺诈和恶意是同义词。

我国最高人民法院在《关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见(试行)》第六十八条中明确规定："一方当事人故意告知对方虚假情况，或故意隐瞒真实情况，诱使对方当事人做出错误意思表示的，可以认定为欺诈行为。"所谓欺诈行为，是指一方当事人故意告知对方虚假情况，或者隐瞒事实真相，诱使对方做出错误意思表示而订立合同的行为。

从司法角度，我们可以明确，欺诈最大的特点是：实施欺诈的行为人主观上存在恶意，在客观上实施了虚构事实或隐瞒实情的行为，其根本目的在于使对方对自己的欺诈陈述产生误解，从而对不付出任何代价的情况下诈取对方钱财。随着信息技术的大力发展，电子商务已经成为一个巨大的经济产业，其涵盖的巨大经济利益自然也吸引了大量不法分子的侵入。电子商务区别于传统商务的最大特征就是虚拟性，这就为整个交易增加了不确定性，因而是欺诈等犯罪行为频繁发生的一个全新领域。

1. 虚假交易

虚假交易泛指平台商家为了提升店铺信誉、商品排名、搜索权重等而采取的作假提升销量欺骗平台、消费者的行为。

主要形式表现为：①将一件商品拆分为多个不同形式或页面发布。②将赠品打包出售或利用赠品提升信誉等。③使用虚假的发货单号或一个单号重复多次使用。④以直接或是间接的方式，变更商品页面信息、大幅度修改商品价格或商品成交价格等。⑤以换宝贝形式累积销量或人气。⑥卖家限制买家购买虚拟物品的数量。⑦在移动/联通/电信充值中心、网络游戏点卡、腾讯 QQ 专区三个类目中发布虚拟类商品时使用限时折扣工具。

具体手段表现为：朋友、同学、家人等相互进行线上购买；同家公司内部多个人反复多次购买同件商品；卖家自己注册多个马甲小号，购买自己发布的商品；卖家利用第三方炒作团伙，或通过和别人协议交换购买的方式；通过变更商品页面信息，或大幅度修改商品价格，来提高商品销量；其他非正常交易手段来提高商品销量。虚假交易是一种不道德的行为，对于其他卖家很不公平，所以网站查到后都会做出严厉处罚。

2. 买卖方欺诈行为

1) 买方欺诈行为

身份欺诈。买方身份欺诈是指买方用捏造的虚假身份进行交易，对卖方造成经济损失的行为。为了增加交易额，鼓励买方积极参与，C2C 交易平台对买方没有进行严格的限制，买方匿名交易大量存在，其身份欺诈较为普遍，主要表现为买方的一次性交易行为，即买方

通过电子邮件注册身份，参与竞拍并欺诈卖方，继而更换电子邮件再次注册。典型的身份欺诈是多重投标，C2C 交易的谈判环节存在多重投标欺诈，指买方通过申请多个电子邮件注册多重身份，同时竞拍特定商品或服务，使价格逐渐上升，驱逐其他潜在买方推出竞标。然后，在拍卖最后几分钟撤回高价投标，以非常低的投标价赢得商品。

发布虚假信息。买方的虚假信息发布是指买方以交易达成的前提，散布虚假的、夸大的或不存在的欺诈性信息，为实现自己的利益，对卖方造成经济损失和伤害等。C2C 交易的虚假信息发布主要集中在展示、沟通和谈判等环节，表现为买方对个人信息的虚假发布，进行身份欺诈；对商品信息的虚假发布，以质量缺陷为由要求退款或换货，进行退款欺诈。B2C 交易的虚假信息发布主要表现在售后服务环节，买方通过对商品、服务质量的虚假信息发布要求退款，进行退款欺诈。

拒绝履约。买方拒绝履约主要表现在拒绝付款和退款欺诈，买方拒绝付款是买方欺诈的一种主要方式，是买方在接到商品或享受服务后拒绝付款的行为。C2C 和 B2C 交易都存在拒绝付款。买方退款欺诈是买方在接受商品、享受服务后，以商品或服务的低质量等为由要求卖方退款，而当卖方将款项退回后，买方却拒绝交付商品。

2）卖方欺诈行为

在卖方欺诈中，虚假信息欺诈和身份欺诈较为普及，贯穿于 B2C 和 C2C 交易的各个环节。同时，在支付、配送和售后服务环节又集中存在拒绝配送商品、拒绝实施服务、商品质量问题、虚增费用、拒绝售后服务、不履行保障条件、售后服务质量等。此外，C2C 交易的沟通环节还存在“托”投标欺诈。

身份欺诈。C2C 和 B2C 都存在卖方身份欺诈，即卖方通过虚假身份使买方受到利益损失。B2C 交易常见的卖方欺诈主要表现为卖方制造假象使得买方对卖方的身份认识出现错误，继而进行交易，造成了一定的利益损失。C2C 交易常见的卖方欺诈行为有三种：首先，卖方注册自己的电子邮件，然后竞拍，继而更换电子邮件再次注册，从而欺诈买方，也就是一次性欺诈行为。随着网上拍卖市场的不断规范化、卖方准入门槛的不断提高，卖方一次性交易欺诈的行为也不断减少。其次，卖方在多次诚信交易后，出现单笔欺诈（多为大额欺诈）。最后，是“托”投标行为，在 C2C 交易中卖方申请买方身份或要求其他相关人注册参与其售卖商品的拍卖，制造竞争假象，故意抬高价格，牟取暴利。

发布虚假信息。虚假信息发布贯穿于各环节。B2C 和 C2C 的虚假信息发布集中表现为捏造自身的良好信誉、夸大其商品质量、宣称有各种售后服务保障等。虚假信息主要是在产品质量和服务信誉方面的欺诈，质量欺诈和服务信誉问题是卖方配送给买方的商品或实施的服务比宣称的质量和服务信誉低的欺诈行为。

拒绝履约。拒绝履约包括售前和售后的整个过程，卖方拒绝履约主要表现在拒绝交货或实施服务、提高履约费用和降低履约成本。拒绝交货或实施服务是卖方在收到支付款后的违约行为；拒绝售后服务是指卖方在交易完成后，当买方所购商品或服务出现质量问题需要售后维护时，卖方不按照合约进行售后服务；或虽然实施了售后服务，但质量很差；或在交易后的配送环节通过增加配送费用或增加服务附加费，来提高商品或服务的最后销售价，使自己获得更大的利益，影响买方对整个商品信任度的行为。

表 3-2 列出了基于交易链的网上买卖方的欺诈行为。

表 3-2 基于交易链的网上买卖方的欺诈行为

交易状态	展示	沟通	谈判	签约	支付	配送	售后
B2C 卖方欺诈	虚假信息、身份欺诈					拒绝配送	拒绝售后
C2C 卖方欺诈	虚假信息、身份欺诈和托投标					拒绝配送	拒绝售后
B2C 买方欺诈	虚假信息、身份欺诈和多次投标				拒绝支付		退款欺诈
C2C 买方欺诈	虚假信息、身份欺诈				拒绝支付		退款欺诈

3. 合同诈骗

合同诈骗是指以非法占有为目的，在签订、履行合同过程中，通过虚构事实、隐瞒真相、设定陷阱等手段骗取对方财产的行为。或者是合同一方当事人故意隐瞒真实情况，或故意告知对方虚假情况，诱使对方当事人做出错误的意思表示，从而与之签订或履行合同的行为。

合同又称契约，根据我国《中华人民共和国合同法》(以下简称《合同法》)第二条规定："合同是平等主体的自然人、法人、其他组织之间设立、变更、终止民事权利义务关系的协议。"合同是反映双方或多方的意思表示一致的法律行为。在电子技术引进之前，传统合同主要有口头和书面两种形式。随着电子技术的引进和发展，电子合同得以出现。电子合同，又称电子商务合同，根据联合国国际贸易法委员会《电子商务示范法》以及世界各国颁布的电子交易法，同时结合我国《合同法》的有关规定，电子合同可以界定为：电子合同是双方或多方当事人之间通过电子信息网络以电子的形式达成的设立、变更、终止财产性民事权利义务关系的协议。通过上述定义可以看出，电子合同是以电子的方式订立的合同，其主要是指在网络条件下当事人为了实现一定的目的，通过数据电文、电子邮件等形式签订的明确双方权利义务关系的一种电子协议。

电子合同欺诈主要表现为以下几种情形：一是在网络中盗用电子身份证信息，冒充合法企业的名义与相对人签订电子合同，当被害人通过网络银行把钱款打到犯罪人预设的账户后，犯罪人就消失了。受害人一般在找不到交易方之后才发现受骗上当，但已经来不及了。二是行为人本身并不具有实际履行能力，用电子商务交易为幌子骗取受害人财务后便不再履行合同或不按电子合同规定履行义务、完成交易。三是通过虚假认证手段，完成电子合同交易骗取受害人财物。四是使用伪造的网上支付账户通过骗过网上结算机构的检查来完成交易，骗取被害人的财物。

4. 网络钓鱼

网络钓鱼是指通过大量发送欺骗性的 E-mail 和伪造的 Web 站点来进行诈骗活动，使受骗者泄露自己的重要数据，如信用卡号、用户名和密码等信息的一种攻击方式。最典型的网络钓鱼攻击方式是在 E-mail 中给出一个网站链接，将收信人引诱到一个通过精心设计与目标网站非常相似的钓鱼网站上，让用户输入个人信息，这些信息就被钓鱼者获取，网络钓鱼攻击者就可以假冒受害者进行欺诈性金融交易，从而获取经济利益，致使受害者遭受经济损失。

1）网络钓鱼的主要手段

网络钓鱼的主要伎俩在于仿冒某些公司的网站或电子邮件，然后对其中的程序代码动手脚，如果使用者信以为真地按其链接和要求填入个人重要资料，资料将被传送到诈骗者手中。归结起来主要有以下几种攻击手段。

（1）通过电子邮件发布虚假信息引诱用户。钓鱼者大量发送欺诈性邮件，这些邮件多以中奖、顾问、对账等内容引诱用户在邮件中填入金融账号和密码，或是以各种紧迫的理由要求收件人登录某网页提交用户名、密码、身份证号、信用卡号等信息，继而盗窃用户资金。

（2）建立假冒网上银行、证券网站，骗取用户账号密码实施盗窃。钓鱼者建立起域名和网页内容都与真正网上银行系统、网上证券交易平台极为相似的网站，引诱用户输入账号密码等信息，进而通过真正的网上银行、网上证券系统或者伪造银行储蓄卡、证券交易卡盗窃资金；还有的利用跨站脚本，即利用合法网站服务器程序上的漏洞，在站点的某些网页中插入恶意 JavaScript 代码，屏蔽住一些可以用来辨别网站真假的重要信息，从而窃取用户信息。如曾出现过的利用数字 1 和字母 i、数字 1 和小写字母 l、vv 和 w 非常相近的特点企图蒙蔽粗心的用户，然后散布一些虚假消息，引诱用户访问这些网站并获取用户个人信息。

（3）利用虚假电子商务进行诈骗。通过建立电子商务网站，或是在比较知名、大型的电子商务网站如“易趣”“淘宝”上，发布虚假的商品销售信息，以所谓“免税商品”“走私货”“慈善义卖”的名义出售各种产品，很多人在低价的诱惑下上当受骗。在收到受害人的购物汇款后就销声匿迹，或以次充好，以走私货充当行货，消费者买到的是质次价高的商品。

（4）利用木马和黑客技术窃取用户信息后实施盗窃。木马制作者通过发送邮件或在网站中隐藏木马等方式大肆传播木马程序，当感染木马的用户进行网上交易时，木马程序即以键盘记录的方式获取用户账号和密码，并发送给指定邮箱，有些木马甚至可以突破软键盘密码保护技术和盗取用户的数字证书，使用户的资金安全受到严重威胁。

（5）利用用户弱口令等漏洞破解猜测用户账号和密码。由于部分用户贪图方便设置弱口令，使得钓鱼者可通过猜测和一些破解算法对计算机或银行卡密码进行破解。实际上，网络钓鱼者在实施网络诈骗的过程中，经常采取以上几种手法交织、配合进行，还有的通过手机短信、QQ、MSN 进行各种各样的“网络钓鱼”违法活动。

2）网络钓鱼的主要危害

网络钓鱼的发生给电子商务和网络营销带来了巨大的危害。

（1）它恶化了电子商务的生态环境，影响了经济秩序。电子商务交换模式的一个重要特点是要实现从看货到付款的“直接交换”，过渡到以信用工具和信用体系为中介的“间接交换”。这种间接交换的普遍性，就依赖于信用体系的有效性。网络诈骗活动的发展和蔓延将使广大用户对这种交易方式表示怀疑，为此我们将不得不付出极大的信用建设成本。

（2）骗取网民钱财使网民遭受经济损失。网上发布的海关查没品、超低价电子产品等诱饵具有极大的诱惑力，又有极大的欺骗性。一旦有人与他们联系，便以代缴税金、邮寄费、保险费等名义让受害人汇款。据调查，这类诈骗犯罪涉及全国各地，受骗者既有工人、农民、知识分子，也有国家机关干部；既有城市居民，也有乡村群众。犯罪分子诈骗金额越来越大，几万元、几十万元，甚至上百万元人民币，使受害者倾家荡产，甚至有机关、企业财会人员不惜动用公款汇给骗子，给国家、集体和个人财产造成重大损失。

(3) 破坏了网上的诚信交易环境。诚信,一直被认为是中国电子商务发展的最大瓶颈。据有关专家分析,中国市场交易中由于缺乏信用体系,无效成本占 GDP 的比重至少为 10%～20%。中国人民银行公布的数据显示,中国每年因逃废债务造成的直接损失约 1800 亿元人民币;国家工商总局统计,由于合同欺诈造成的直接损失约 55 亿元人民币;还有产品低劣和制假售假造成的各种损失至少有 2000 亿元人民币,这都直接导致了诚信成为当前中国电子商务所面临的最难以逾越的鸿沟。

3.1.5 服务评价

1. 商品质量评价

商品质量是现代企业市场竞争焦点之一,是影响企业核心竞争力的重要因素。商品质量水平高是企业实行差异化战略的核心内容,但是,质量不好、消耗过大是目前我国企业的症结。

在商品生产尚不发达、商品供不应求的社会经济条件下,物质的需要、数量的满足占据主导地位,人们商品质量观的核心内容是商品的基本性能和寿命,即强调商品的内在质量,如食品的热量(商品猪肉是以脂肪层厚度作为定级的依据)、衣服用品的保暖和耐穿耐洗、日用工业品的坚固耐用等基本内容。人们在评价商品质量时,只要商品质量符合“国家的有关法规、质量标准以及合同规定的对产品适用、安全和其他特性要求”,则为“优质”商品,而未能全面考虑消费者对商品质量的综合欲求。

随着科技进步和商品经济发展,市场逐渐由卖方市场转变为买方市场,供不应求转化为供大于求,市场竞争日趋激烈。人们不再仅仅满足于基本物质需求,而开始追求更高层次的文化精神需求的满足,追求与人们根本利益相一致的社会和经济需求的满足,因而现代商品质量观已从仅考虑商品的内在质量和个体性质量,发展到越来越注重商品的外观质量、社会质量、经济质量和市场质量的综合质量观。

对商品质量评价,我国许多学者进行了不少研究,大体上可分为两方面内容:一是商品质量评价指标的选择;二是商品质量评价的方法。但是,还存在一些可以改进的方面:一是质量评价指标应与时俱进,适应经济社会发展需要,评价体系要全面、综合;二是指标之间的层次应得到体现;三是各指标权重应当客观,提高评价结果可信度。

商品质量综合评价的指标体系分为三层:目标层、准则层和指标层,如图 3-3 所示。

商品内在质量,是指能够实现商品预定使用目的或规定用途,保证人身和财产不受伤害和损害所应具备的基本质量要求,包括商品的实用性能(如化学性能、物理性能、机械性能、生物性能等)、寿命、可靠性、安全与卫生性等。

商品外观质量,是指商品能够满足人们审美和心理舒适需要的程度,包括外观构型、质地、色彩、气味手感、表面疵点和包装装潢等。

商品的经济质量,是指人们按其真正需要,期望以尽可能低的生产质量成本获得尽可能优良性能的商品,并且在消费(或使用)中付出较低的使用和维护成本(蔺哲,1999)。

商品的市场质量,是指该商品在市场上的美誉度、商品品牌的市场影响力以及商品的售后服务质量等。

商品的社会质量,是指商品满足全社会利益需要的程度,如对生态环境造成污染、浪费

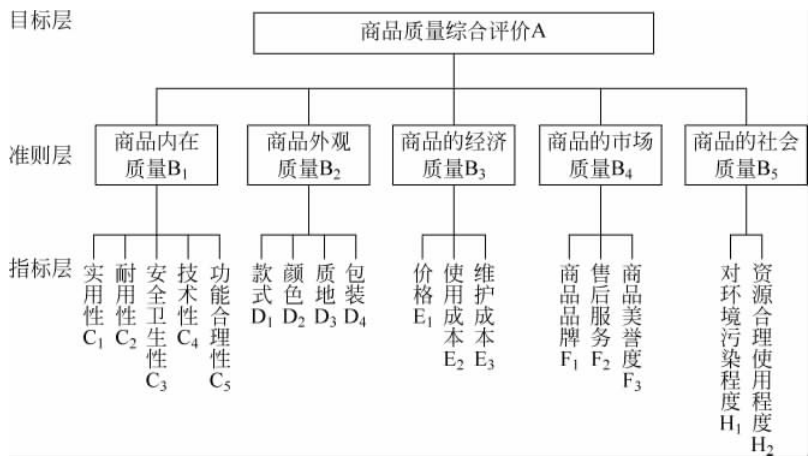

图 3-3 商品质量综合评价体系

能源和资源等社会所关切的利益；一种商品不管它如何先进，只要它有碍于社会利益，就难以生存和发展。

商品质量评价原则如下。

(1) 目的性原则。设立商品质量综合评价体系的目的在于改变过去单一评价商品质量的方法，真实准确地综合反映现代商品的质量状况，促进企业树立现代商品质量观。

(2) 系统性原则。影响人们对商品质量评价的因素非常多，因此，在对商品质量进行评价时不能只考虑某一因素，必须采取系统、全面的评价原则，才能综合、客观地做出对商品质量的评价。

(3) 适当性原则。由于人们对商品质量评价的指标非常多，所以指标的选取范围既要尽量全面，又不能无限扩大，只能选取有代表性的指标进行评价，使研究工作具有可操作性。

2. 物流评价

在经济全球化和贸易领域的透明度增加的背景下，城市物流成为一个城市综合竞争力的组成部分之一，城市物流服务水平和物流成本成为影响投资环境的重要因素。科学评价城市物流发展的条件和潜力，对促进企业物流发展，解决城市发展中所面临的一系列社会问题，提高城市竞争力具有重要意义。

近年来人们逐渐认识到城市货物运输对城市的长期可持续发展发挥着重要作用。然而最近几年城市货物运输面临着许多挑战性的问题，包括交通拥挤、环境的负面影响、过高的能源消耗和劳动力短缺问题。同时，货物承运人还要以更低的成本提供更高水平的服务。为解决这些问题出现了运输计划的一个新领域——城市物流。城市物流是通过考虑城市货物流通对社会、环境、经济、金融和能源的影响，使城市物流活动达到整体最优的过程。

Taniguchietal(1991a)把城市物流定义为："在市场经济中，考虑城市交通环境、交通堵塞和能源消耗的同时，由私人企业来实现的使物流和运输活动总体最优的过程。"

在城市货物运输中有四个主要参与者：货主、货物承运人、居民和管理者。货主是承运人的顾客，货主通过承运人向别的公司或个人发送或接收货物，所以货主一般希望得到服务水平最大化，包括运输或配送的时间和成本、运输的可靠性和跟踪信息。货物承运人努力使

为顾客集中和递送货物的成本达到最小化，以实现利润最大化，而要实现这一点存在很多困难。居民是在城市中生活、工作、消费的人们，居民希望居住地和附近地区的交通堵塞、噪音、空气污染和交通事故最小化，而城市商业区的零售商们则想在便利的时间收到货物，这有时与当地渴望宁静和安全的居民相冲突。城市管理者试图发展城市经济，增加就业率，同时减轻城市交通堵塞，改善环境质量和加强道路安全，应当在促进城市物流的发展中起主导作用。

物流评价原则如下。

(1) 目的性原则。设计城市物流评价指标体系的目的在于：根据对城市物流系统的综合评价，衡量城市物流发展状况，找出城市发展的瓶颈所在，通过改善不足之处，最终实现商品配送的成本最小化，并提高城市地区生活质量。

(2) 科学性原则。首先，指标的选取应具有科学的理论根据。其次，城市物流评价指标体系应能准确地反映实际情况，有利于城市之间的横向比较，发现自身优势和不足之处，挖掘竞争潜力。城市物流评价指标应成为城市完善物流系统、解决社会问题、提高居民生活质量的有力工具。

(3) 系统性原则。对城市物流系统的评价是一个涵盖多因素、多目标的复杂系统，评价指标体系应力求全面反映城市物流的综合情况，既能反映系统的内部结构与功能，又能正确评估系统与外部环境的关联，既能反映直接效果，也能反映间接影响，以保证评价的全面性和可靠性。

(4) 定性与定量相结合的原则。在综合评价城市物流水平时应综合考虑影响城市物流水平的定量和定性指标。对定性指标要明确其含义，并按照某种标准赋值，使其能恰如其分地反映指标的性质。定性和定量指标都要有清晰的概念和确切的计算方法。

(5) 实用性原则。所建立的城市物流指标评价体系力求达到层次清晰、指标精练、方法简洁，使之具有实际应用与推广价值。为此，选取的指标要具有可操作性，指标应含义明确且易于被理解，指标量化所需资料收集方便，能够用现有方法和模型求解。

3. 交易过程评价

交易的过程，也是交易成本的形成过程；交易成本的形成，是伴随交易行为出现的。人们对交易过程有不同的认识，因此交易过程有狭义的交易过程和广义交易过程之分。一般而言，狭义的交易过程是指交易双方使交易对象位移的过程，即在一定的背景或局限条件下，由交易双方借助于交易媒介，按照双方约定的规则，在约定的时间内把交易对象(可以是有形的实体或无形的服务)从交易的一方转移到另一方，它是通过市场的价格机制来发生作用的。广义的交易过程则是在狭义的交易过程的基础上，还包括交易的事前准备过程和事后执行监督过程。具体而言，交易过程可以分为下面几个阶段。

1) 交易动机的形成过程

交易是两个或两个以上的个体的交互博弈行为，因此交易双方的动机很重要。交易者必须清楚地了解其动机：缺乏什么，需要什么，他有什么可供选择的交易对象，为达到交易目的需要采取什么样的行动，其交易动机的强烈程度如何，采取何种交易方式(市场的或经济组织的)。交易者在社会分工结构中的地位决定其知识结构、认知水平和经济活动的范围，而这些因素又限定了其交易动机的复杂程度。

2）对交易环境的评估过程

交易环境应包括三个要素：一个确定的知识结构、一群由其知识片断所确定偏好的人、一个基本权利结构和一个可交换权利结构。对交易环境进行评估，需要考察下面的因素：交易参与者的角色与地位；交易的对象、交易的数量和交易的频率；交易行为的约束规则；交易技术；交易的场所。这些因素受制于交易的三个维度：不确定性、资产专用性和交易频率。在交易世界中，存在着随机变化，交易者的不同偏好、信息的不对称及交易者机会主义行事的可能，使得不确定性必然影响着交易过程中博弈双方的合作空间：交易与否的选择、交易契约条款的达成与不断修改、对交易实现的预期程度和契约方式的选择等。资产专用性确定了交易者进入或退出交易过程的难易程度。它还引发了交易的事前反应，即潜在交易者交易动机、交易目标、交易条件和范围的确立；交换物品的属性、特征、称量与测度的说明。事中的契约的起草与谈判。事后则对达成的交易进行监督与控制，以防止某交易方的机会主义行为破坏执行契约的连续性。交易频率则是交易各方之间在是否合作或不合作的博弈中多次反复的结果。交易各方之间不确定性因素越多，资产专用性越高，交易的频率就越低；反之，则交易的频率则越高。

3）交易者之间的谈判过程

交易者在交易动机的驱使下，开始尝试相互交换。在交换时，交易者可能会考察个体所处的交易环境，并评估交易的必要性以确定进一步的行动策略：采取合作博弈或非合作博弈，有无必要采取投机取巧的机会主义行为，或者说，在有限理性的条件下，交易者为了实现其效用最大化，将选择偶然的或一次的博弈行为，或是恒常的重复博弈行为。在交易博弈过程中，一方的最佳策略选择是通过另一方的行为模式或偏好信息做出初步判断和理性预期，针对对方的行为采取动态跟随策略，不断调整自己的战略和策略行为，从而获得满意的博弈结果。

在信息充分的情况下，不确定性和风险比较容易预期，交易者双方了解交易对象的可能性越大，产权界定越清晰，通过博弈、谈判或合作的可能性较大。合作博弈需要交易者双方拥有充分的信息与交流。

4）交易者之间的签约过程

合作意向确定后，则交易双方开始订立契约。交易双方进一步对下列情况做出明确表述：某一价格下，物品的品质和数量的检验，律师的聘请与咨询，合同的起草与修改，保证条款的规定，物品的转移与交易的登记，对违约行为的处罚规定等。签约行为受到未来预期对交易者双方的影响。如一方认为资产的专用性强，则希望签订长期契约，而另一方考虑到未来的风险和不确定，则倾向于采取机会主义行为而签订短期契约，因此契约条款必须充分反映双方利益的权衡，且签订的契约内容的修改会反复多次，这延长了签约时间。

5）契约的执行和监督过程

达成契约后，交易者要实施其契约条款和内容，以实现交易对象的转移。为了防止机会主义行为造成交易损失，交易双方需要设计出一整套与交易相关的制约机制和惩罚机制，以保证交易正常进行，顺利地实现产权的让渡。对交易过程的刻画，初步勾勒出交易成本形成的大体轮廓，但人们对交易行为和交易过程的认识分歧，造成了人们对交易成本的不同认识。

3.2 交易信息安全

3.2.1 消费者信息保护

现代信息技术的飞速发展使得电子商务企业收集、处理与散播消费者个人信息变得轻而易举，网络消费者个人信息的收集与交换呈爆炸化发展趋势，而不当收集、恶意使用及散播个人信息的现象也日益突出，严重地侵犯了网络消费者的自由、基本权利与正当权益。

目前我国并没有哪一部法律对个人信息有一个明确的解释或定义，但基本普遍认为所谓个人信息就是一个人的姓名、联系方式、住址等可以把该人与其他个人分别出来的那些信息。

消费者个人信息是电子商务发展的最宝贵资源之一。现阶段影响电子商务发展的因素不是技术问题，而是法律环境与安全信心的问题。

1. 消费者信息侵权类型

1）消费者个人信息的不当收集

在 B2C 电子商务中，不当收集消费者个人信息包括两种情况：未经同意收集消费者个人信息、超范围收集消费者个人信息。

未经同意收集消费者个人信息。个人信息的收集方式分为三种，第一种是消费者应网站要求而提供其个人信息，即消费者在浏览 B2C 网站时，如果需要使用网站提供的服务或在该网站购物，就要按照相关提示和步骤填写个人信息进行注册。在这种收集方式中，消费者采取的是积极主动地向商务网站提供个人信息，网站一般也会说明收集的方式、收集个人信息的目的或个人信息的使用情况。第二种方式是自动获取信息，即商务网站附随着消费者浏览网页和购物过程来收集个人信息，这种收集方式一般比较隐蔽，网站不会做出说明，这种方式相对于前者对消费者具有潜在的危害性。第三种是其他来源获取信息。在以上三种个人信息收集方式中，自动获取和其他来源获取都未经消费者本人同意。

超范围收集消费者个人信息。对消费者个人信息收集的范围，既无相关行业规范来指导，更没有国家法律法规予以明确划定，基本上属于行规和法律监管的真空地带。电子商务网站收集了哪些个人信息也无任何说明，消费者更无从得知。在电子商务的常见模式中，同一模式下的电子商务网站需要交易对方提供的信息范围基本相同。如果在交易中有其他联系方式能够保证交易顺利完成，而注册时仍然要求消费者提供手机号码等敏感的个人信息就属于超范围收集消费者个人信息。此外，收集与特定交易无关的个人信息，或通过问卷调查收集消费者的个人信息来了解消费者的喜好、兴趣等，都属于超范围收集消费者个人信息。

2）消费者个人信息的不当利用

与合作企业共享消费者个人信息。在一些 B2C 电子商务网站上，经常存在与该网站有链接的第三方网站，这些网站可能是一些广告公司或其他合作企业，如携程旅行网网站上就有东方财富网、珍爱网和易车网等合作企业的链接。B2C 网站为了得到广告收入或与合作企业互相交易而盈利，对本网站上的个人信息不限制地由第三方网站链接甚至与之分享。

个人信息的非法交易。个人信息的非法交易包括两种，一种是两个电子商务公司间的交易，也即信息互换。另一种则是电子商务公司向不特定对象出售其所掌握的个人信息。《华尔街日报》的调查发现，互联网上成长速度最快的生意之一就是监测互联网用户。调查发现，在互联网用户和广告投放者之间，存在着 100 多家中间机构，包括追踪公司、数据中间商和广告投放者网络等，它们彼此竞争，以满足企业对消费者行为和偏好的日益增长的数据需求。B2C 商务网站最终目的是为了获利，面对数据中间商和广告投放者的不断增长的个人信息需求，持续地将收集到的个人信息出卖给以上机构就可以获得价值不菲的一笔收益。

3）消费者个人信息的泄露

消费者因个人信息泄露遭受骚扰。消费者个人邮箱经常成为垃圾广告投放的对象，消费者个人联系电话泄露后被不明的推销电话所骚扰。

不法监视。不具有法定监视资格的组织，如私家侦探利用非法获取的消费者个人信息对消费者进行跟踪或监视以满足其客户的要求，使消费者私人生活安宁遭受威胁。

网络服务商的不作为导致个人信息泄露范围扩大。对明知是泄露的个人信息，网络服务商既不断开信息服务中的链接，也不采取删除措施，导致个人信息泄露的范围进一步扩大。

信息技术侵权，木马病毒泛滥。国内有信息专家指出，挂马网站已经成为威胁国内互联网安全的主要因素。为了获利，大量的木马病毒在互联网上泛滥，从制造木马、传播木马到盗窃账户信息，再到通过第三方平台销赃继而洗钱，形成一条重要的产业链。

黑客攻击。电子银行、B2C 电子商务网站遭受黑客攻击并导致消费者个人数据库外泄。黑客利用各种技术手段，攻破电子银行的防火墙，获取电子账户的用户名和密码，利用消费者的这些信息进行转账或消费。此外，黑客使用一些特殊程序进入电子商务网站的系统，实现非授权登录，对消费者的个人信息进行控制和利用。

2. 消费者信息的保护措施

1）电子商务消费者的自我保护

电子商务消费者如果适当懂得一些保护自己个人信息的方法，便可以大大减少个人信息被非法收集和利用的机会。消费者的自我保护模式应当是自我控制、自我选择和自我防卫的综合体系。

自我控制，即依靠技术手段加强消费者个人信息的控制，如有效运用匿名注册和浏览，对 Cookies 的删除与禁用以及应用技术软件等。

自我选择，即主动了解经营者的隐私权保护政策，包括经营者收集的信息内容和种类，收集信息的方式与目的，信息使用的主体、范围、途径及使用期限，提供或不提供这些信息的后果以及可能拥有的任何补偿权等。据此，在不同的信息隐私保护可能性之间做出完全自主的选择。

自我防卫，即运用法律武器保护合法权益。电子商务消费者自我保护个人信息的方法有很多，比如：尽可能地将个人信息资料与网络隔离；传输涉及个人信息的文件时，使用加密技术；不要轻易在网络上留下个人信息；在计算机系统中安装防火墙；利用软件，反制 Cookie 和彻底删除档案文件；针对未成年人的个人信息保护，除了对未成年人进行隐私知识和媒介素养教育外，还应在家长或监护人的帮助下，借助相关的软件技术进行。

2）从电子商务行业自律的角度进行保护

各行业协会如中国互联网协会、中国电子商务诚信联盟等行业组织应主动积极地承担起责任。2002年4月24日，中国互联网行业自律公约公布施行。自律公约指出，互联网行业是指从事互联网运行服务、应用服务、信息服务、网络产品和网络信息资源的开发、生产以及其他与互联网有关的科研、教育、服务等活动的行业的总称。2004年12月21日，在国务院有关部门和单位的支持下，中国电子商务协会正式成立了“中国电子商务诚信联盟”，该联盟成立的宗旨是要通过建立权威、公正的第三方资信评估平台，加强我国电子商务信用体系的建设，在充分保护网上购物者权益的同时，增强全社会对电子商务的信心，从而使中国电子商务在一个健康、成熟、完善的环境中获得更大的发展。该联盟制定了“中国电子商务诚信公约”，共有八大条款，其中第二条款就是关于消费者隐私权保护的。

3）从立法的角度进行保护

首先，在法律上把对个人信息的重要组成部分——个人隐私的保护确立下来，将隐私权作为单独的人格权确立下来。我国宪法中有保护人的尊严不受侵犯的原则，但未把原则上升为权利。而隐私与人的尊严是密不可分的。由于我国尚未建立起人权推定制度，所以隐私目前在尊严未成为基本人权前还仅是在民法层面上受保护。今后的民法中，需要对隐私、隐私权和隐私权的保护范围进行明确的界定，隐私权应限定在对私人信息、私人活动和私人领域三个方面的保护。其次，要将隐私权与名誉权分开，采用直接保护的方式。同时，还应明确侵害隐私权的行为方式，包括侵害他人隐私信息、侵扰他人私人活动、侵入他人私人空间等形式。另外，还应对侵害隐私权的民事责任进行明确规定，应包括停止侵害、赔偿损失和赔礼道歉等形式。通过对隐私权的保护，包含个人隐私内容的个人信息在很大程度上也可以得到保护。

4）制定相应的法律法规保护个人信息

在与个人信息（或资料）保护相关的法律法规中，应该对个人信息的具体内容、个人信息收集的知情权、选择权，个人信息的控制权，个人信息安全的请求权，个人信息使用的限制权等内容进行详细而明确的规定。另外，从行业自律和法律法规两个层面对电子商务消费者个人信息进行保护时，还应该注意到目前我国两岸三地对于电子商务消费者个人信息保护的不平衡现状。有关方面应积极主动地面对这一问题，以寻求解决的有效途径。

3. 美欧对消费者信息的保护措施

有学者曾言，“考察法律，应着眼超越地域、国度和民族，甚至超越时空的人际层面，努力发现本来属于整个人类的理念和规范，并在此基础上寻求并促进人与人、民族与民族、国家与国家之间越来越普遍深入的交往。吾人之规可为他人所取，他人之法可为吾人所用，概其皆出乎人之本性。所以‘取法人际，天道归一’，当为人类社会法律进步之最高思想境界。”正所谓他山之石，可以攻玉。认真研习域外相关法律保护模式并结合我国具体国情加以合理借鉴，对完善我国电子商务中消费者个人信息隐私的法律保护具有积极意义。

1）美国的行业自律模式

基于信息隐私的经济特性，对电子商务中消费者个人信息的隐私保护，美国采取了以市场调节与行业自律为主导的保护模式。美国坚持认为，急促立法将会制约电子商务的发展，对个人信息保护应采取较为宽松态度，尽量限制政府的干预，注重市场的调节作用，强调依

赖电子商务企业自身的力量，即由其在网站上公布隐私政策，然后通过该隐私政策的实施来保护网络消费者的个人信息。保护个人信息的行业自律机制，因美国政府和美国人的提倡而出名，被认为是法律外的个人信息的有效保护机制。美国行业自律模式的主要表现形式包括建议性的行业指引、网络隐私认证计划和技术保护三类。

建议性的行业指引(suggestive industry guidelines)。许多从事网络业务的行业联盟，都以发布网上隐私保护准则或行业指南的形式，声明并倡导本行业对个人隐私的保护。此种个人隐私保护的具体做法是，由相关行业的领袖企业或主导企业发起，建立本行业内的联盟，并制定一些隐私保护的政策性指引和标准，而不涉及具体的实施细则。这种指南性质的隐私保护政策不具有要求本行业内从业者必须遵守之性质，它只是依靠来自于团体内部和社会公众的压力，使从业者根据隐私保护的行业指南，自行制定具体的个人隐私保护政策或办法。

网络隐私认证计划(online privacy seal program)。美国的网络隐私认证计划是一种私人行业实体致力于实现网络隐私保护的自律形式。该计划是通过对遵守特定的信息收集规则并服从一定形式的监督管理的实体颁发认证标志的形式，督促产业实体加强对个人信息的保护。它给予的最高处罚是取消认证。与建议性的行业指引不一样，网络隐私认证是跨行业的，其功能和作用同传统的商业认证相类似。它是行业自律模式中最具特色且最为普遍的一种形式。

技术保护(technical protection)。现代信息技术的发展催生出了以技术为基础的商业运用系统，而网络用户也期待通过使用不同程序及系统来实现不同程度的隐私保护及通信安全，技术手段的保护就是这样应运而生的。这种模式是将保护网络消费者隐私权的希望寄托于消费者自己手中，通过某些隐私保护软件，在消费者进入某个收集个人信息的网站时，提醒消费者什么样的个人信息正在被收集，由消费者决定是否继续浏览该网站，或者，由消费者在软件中预先设定只允许收集特定的信息，除此之外的信息不许收集等。目前实现这种模式的软件主要是美国互联网协会推出的个人隐私选择平台(personal privacy preference platform，P3P)。

2) 欧盟的国家与政府主导的立法规制模式

欧盟是电子商务中消费者个人信息隐私保护的立法规制之典范。其提出“No privacy，no trade”的贸易原则，强调以明确的方式对个人信息提供法律保护，把个人信息之上的权利提升至人权的高度。该立法规制模式是指由国家和政府主导的模式，其基本做法是由政府通过制定法律的方式，从法律上确立网络隐私权保护的各项基本原则与具体的法律制度，并在此基础上建立相应的司法或行政救济措施。欧盟对于网络消费者隐私的保护有着严格的标准，它通过特别委员会的设立，敦促各国以立法的形式来保护网络消费者的隐私。欧盟网络隐私保护的特点在于对于欧盟有网络交易的他国的网络隐私保护情况提出了要求，将其所确立的网络消费者隐私保护标准提升为国际标准，这使得在国际范围内出现了大规模的网络隐私保护的立法活动。

1985 年 10 月生效的《保护自动化处理个人数据公约》，是当今世界上第一个具有法律约束力的有关个人信息隐私保护的国际公约。1995 年 10 月通过《个人数据保护指令》。此外，欧盟关于个人信息隐私保护方面的法律渊源还有 2002 年通过的《隐私与电子通信指令》、2006 年通过的《数据保存指令》。

《个人数据保护指令》在借鉴各国立法及实践的基础上为欧盟各成员国建立起了一整套

全面的个人数据保护体制，给个人信息提供了较高的保护水平，为欧盟内部个人信息的自由流动扫除了阻碍，使得欧盟各国在数据保护上以同一声音说话，且对美国及其他国家的个人数据保护产生了极大的影响。其主要内容和特点包括：①信息自由流动与信息隐私并重；②信息隐私保护水平的底线与较高的信息隐私保护水平；③全面规制信息处理；④严格的信息处理标准；⑤广泛的个人信息权利；⑥全面有效的信息保护执行体制；⑦严格的跨境信息转移标准；⑧指令的统一适用。

3）美国的行业自律模式与欧盟的立法规制模式对比

美国的行业自律模式是一种由行业内部制定行为规范来保护网络消费者个人信息隐私的自下而上(bottom-up)的保护机制。相对于欧盟的立法规制模式，它有自身特有的优势。第一，在保护网络消费者个人信息隐私的及时性与灵活性上，行业自律模式相对于立法规制模式更优。第二，行业自律模式较之立法规制模式，在保护网络消费者个人信息隐私上更具有成本上的优势。第三，较诸公共规范制度，在 SRAs 的程度以及规则较为不正式的范围内，修改标准的成本(包括导致迟延的因素)降低了。第四，这种制度的管理成本通常是在其规范的行业或活动内部承担，而独立的公共机构的管理成本通常由纳税人承担。

欧盟的立法规制模式是由国家立法来统一保护网络消费者个人信息隐私的自上而下(up-bottom)的保护机制。相对于美国的行业自律模式，它具有如下优势。第一，立法规制模式可使网络消费者个人信息隐私保护在一国内明确化，使网络消费者在其个人信息之上的权利成为一项绝对性法律权利。第二，立法规制模式可为网络消费者个人信息隐私保护提供统一的法定标准。第三，立法规制模式可为网络消费者个人信息隐私保护提供相对科学的行为规范。第四，立法规制模式可对损害提供足够的救济。第五，较于自律模式的自律规范，法律规范具有高度的权威性。

4. 我国对消费者信息的保护措施

现有法律和相关司法解释为电子商务交易过程中消费者隐私权的保护提供了法律依据。但是这些法律和司法解释规定简单，操作性不强，对于电子商务交易过程中消费者隐私权屡被侵犯的现实显得严重滞后，这对电子商务交易过程中消费者隐私权保护十分不利，因而迫切需要强化和完善我国电子商务交易过程中消费者隐私权相关立法。

现实生活中电子商务企业侵犯网络消费者个人信息隐私的不当信息行为俯拾即是，而目前我国对电子商务中消费者个人信息隐私的保护还处在初级阶段。针对当前我国电子商务的迅猛发展和消费者个人信息保护的需求，以及网络消费者个人信息隐私保护的立法供给现状，完善网络消费者个人信息隐私法律保护体系是最基本的举措。

1）电子商务法律规范

我国目前并没有实施专门的电子商务立法，但是我国商务部开始关注电子商务企业信用，大力推行电子商务企业信用评估体系，2013 年 12 月正式启动了电子商务法立法工作。2011 年 12 月 15 日，商务部出台了《关于“十二五”电子商务信用体系建设的指导意见》，其中强调要制定电子商务交易规范和信息管理规范，但是并未提出对消费者隐私信息的保护意见。由此可见，我国电子商务法律规范中并没有涉及对消费者信息隐私权的保护。

2）网络信息安全法律规范

我国对网络信息安全的法律规制曾经有过原则性规定。1998 年施行的《计算机信息网

络国际联网管理暂行规定实施办法》第十八条规定，不得在网络上侵犯他人隐私。2000 年通过的《互联网电子公告管理规定》第十二条规定，电子公告服务提供者应当对上网用户的个人信息保密，未经上网用户同意不得向他人泄露，但法律另有规定的除外。2002 年实施的《药品电子商务试点监督管理办法》第十三条规定，药品电子商务网站必须有用户信息管理制度。2012 年 4 月征集意见的《深圳经济特区互联网信息服务安全条例（征求意见稿）》规定，互联网信息服务提供者收集用户身份信息，应当取得用户同意，并按照用户同意的方式、内容和范围收集和使用信息；未经同意不得改变信息用途，不得披露、泄露或者转让该信息，否则将由市公安部门责令改正，并处以 10 万元罚款。情节严重的，还可以处停业整顿，并建议吊销经营许可证或者营业执照。2011 年《信息安全技术个人信息保护指南》草案对个人信息处理原则、主体权利、保护要求进行了具体规定，这也是我国行政机关就网络个人信息保护首次发布如此细致的保护措施。而该草案经过一年多的修改后，2012 年 4 月 12 日工业部宣布已编制完成并将于年内通过《信息安全技术公共及商用服务信息系统个人信息保护指南》。

3）消费者权益保护法律规范

个人信息被非法泄露和使用的情况成为困扰人们生活的一大难题，不但给人们的生活带来很多不便，还对人们的人身、财产安全和个人隐私构成严重威胁。早在 2009 年《中华人民共和国刑法修正案（七）》中就规定了“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金”。这一规定虽然有助于保护公民的个人信息，但是该规定过于笼统，只规定了“违反国家规定”，所以该规定的实施还离不开具体法律制度的协助。

2013 年我国《中华人民共和国消费者权益保护法》进行修订，在修订中新增了第二十九条：“经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。”2014 年 10 月，工商总局出台了《侵害消费者权益行为处罚办法》。

新的《中华人民共和国消费者权益保护法》首次明确保护消费者个人信息的内容，不但规定了经营者收集、使用消费者个人信息应当经消费者同意，还规定了对侵害消费者个人信息的经营者予以相应的处罚，这一规定将有助于有效遏制消费者个人信息被滥用的情况。

3.2.2 交易隐私保护

1. 交易过程中的隐私侵权

隐私权是公民依法享有拒绝、排斥任何未经法律批准的监视、窥探和防止个人私生活秘密、个人信息（个人数据）被披露的权利。个人数据、个人私事、个人领域是隐私权的三种基本形式。任何人非法利用计算机网络技术收集、存储、控制、传播、使用个人数据的，均构成

对他人隐私权的侵犯。

1）电子商务中消费者隐私权的内涵

电子商务交易过程中的消费者隐私权主要针对的是消费者私人信息的权利保护方面，这是由电子商务依托于虚拟的而非实体运行的网络平台的性质所决定的，在这个平台中，消费者的私人信息被入侵的概率远远大于消费者私人生活被打扰的概率（私人生活安宁的权利被侵犯也是衍生于私人信息泄露的结果）。除此之外，电子商务本身的性质与特点也决定了消费者私人信息更受威胁的现实，因为电子商务交易活动是消费者运用自身所有的电子设备，通过网络进行交易的一个过程，这个过程一般包括了电子商务活动的准备阶段、合同签订或协议达成的阶段、合同履行或违约责任追究的阶段，消费者要参与这个过程，必然会访问相关的网页，注册或使用个人的真实信息以顺利达成交易。在此过程中，消费者的隐私问题实际上伴随着交易的始终，消费者的姓名、地址、联系方式、职业等信息，甚至于消费者的消费爱好、消费习惯等信息都可以归类于消费者的隐私权范围内，因此，电子商务中消费者隐私权的内涵包括但不限于消费者的个人基本信息（如姓名、地址、电话号码等）、消费者的个人偏好（如购物习惯等）和消费者网络存储信息（如个人网络空间等）。

2）消费者隐私权被侵犯的主要表现形式

电子商务交易过程有诸多参与主体，其中除了消费者之外，尚有物流企业、第三方支付平台、网络中的“卖方”、提供交易平台的服务方等其他主体角色，甚至于恶意篡取他人信息的软件发布者也频频活动于电子商务交易过程中，以上这些除了消费者之外的交易相关方主体都有接触到并记录消费者私人信息的可能性，进而延伸到在掌握了信息之后侵犯消费者隐私权的可能性。因为消费者个人隐私的获取在网络这个虚拟平台中显得尤其重要，具有较大的市场价值。在电子商务交易过程中，消费者隐私权被侵犯的主要表现形式主要有消费者个人基本信息被非法收集、消费者私人网络空间被肆意入侵、消费者网络活动被非法追踪记录这三种形式，而这三种形式在严重程度、先后次序上又是层层递进的。

隐私的研究综述框架见图 3-4。

2. 交易过程中的隐私保护

电子商务带来了消费市场的拓宽和消费信息量的丰富，只有建立和完善电子商务中消费者权益保护法律制度，才能为消费者营造一个良好的电子商务交易环境，保护消费者合法权益，促进电子商务良性循环发展。

强化和完善我国电子商务中消费者隐私权的立法。在信息化时代，人们生活节奏加快，特别是在经济通胀的背景下，电子商务交易额和参与交易的消费者将急剧增长，迫切需要制定电子商务交易中消费者隐私权的相关法律。可以制定隐私权保护的特别法即《数据保护法》或《个人信息保护法》，在特别法中应对电子商务交易中消费者隐私的含义、权利内容以及其法律地位等进行规定；对电子商务交易中消费者个人数据的收集、披露、公开、传播等行为进行规范；明确电子商务数据拥有主体的权利和义务；电子商务交易中消费者隐私权侵权救济和相关责任。

建立电子商务交易参与主体的相关协会，提高电子商务交易行业自律。通过法律的具体规定对电子商务企业在网上收集用户数据和隐私的行为提出一定的限制，使其在网上收集用户隐私材料的行为更规范，相对于用户来讲更透明，对网上贸易涉及的敏感性资料和个

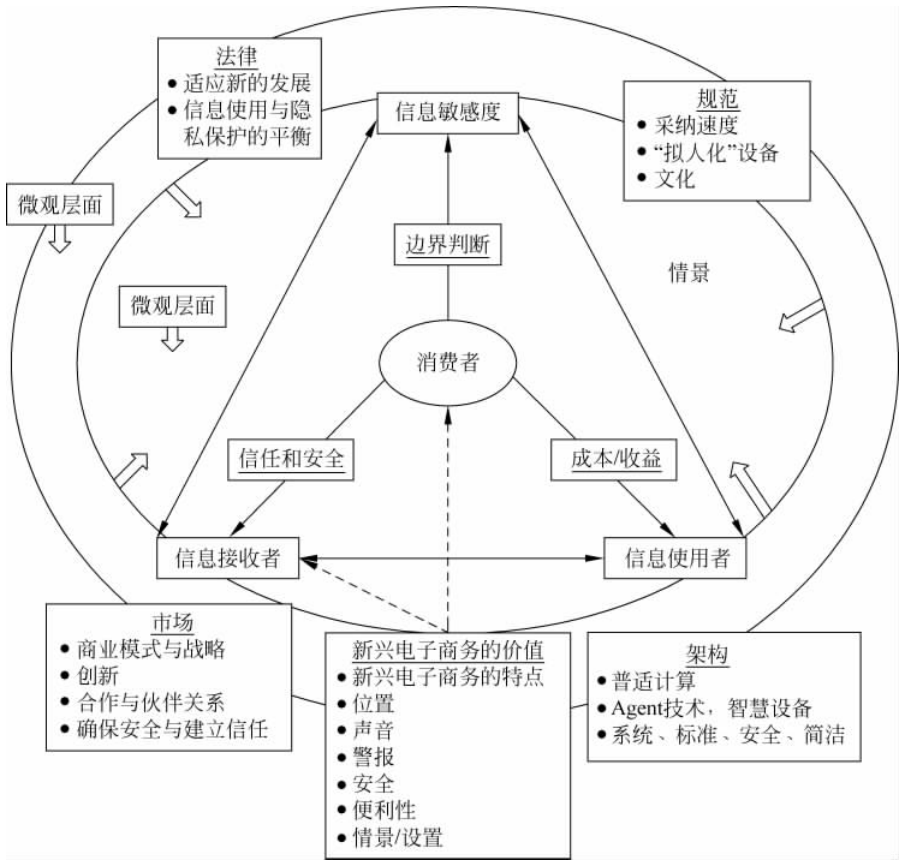

图 3-4 隐私的研究综述框架

人数据给予法律保护。同时，鼓励行业自律，依照法律和行业惯例制定个人资料使用政策和隐私权保护政策。这既有利于提高网络运营商的商业信誉，也可以增添用户使用互联网的信心，扫除用户对个人隐私保护的忧虑，促进电子商务更加有序高效地开展。

引导和培养公众在电子商务交易过程中隐私权保护的意识。通过政府及相关舆论的宣传和引导，以及相关知识的普及，用户应随时注意上网时所可能产生的隐患，不向网站泄露自己的真实情况，不把重要的信息存放在电脑中，不随便使用网上下载的软件，定期清除历史记录，访问完网站之后通过浏览器的 Internet 选项，删除过时的 Cookies 文件，养成良好的浏览习惯，从而从源头上杜绝网络隐私安全问题的发生。这些措施主要包括：第一，了解隐私权相关法律法规和电子商务行业隐私权的政策；第二，大力宣传和教育公众不要在电子商务交易过程中随意泄露个人资料；第三，养成良好的网络消费习惯；第四，经常查看自己计算机系统安全状况，防止被攻击等。

运用先进电子装备和电子技术从技术上保护电子商务交易过程中的隐私权。电子商务交易是利用电子和电子技术手段通过因特网进行交易的商务模式，电子商务中消费者隐私权的保护离不开电子技术和电子装备。电子商务交易中消费者可以配置先进的电子装备和电子技术防止在电子商务交易过程中被跟踪、被窥探，从技术上可以防止消费者隐私权被恶意收集或是任意侵权。通过密码技术、密码协议尽可能地避免了网上交易面临的假冒、篡

改、抵赖、伪造等种种威胁；通过建立虚拟专用网在开放的公共网络上建立安全专用隧道的网络，更好地为电子商务的开展及其个人隐私提供保护服务。

3. 交易商发布信息时的隐私保护

交易商在广告或信息发布时，如果数据过于具体，就可能泄露购物者的个人敏感信息，从而侵犯个人隐私。另外，通过关联多个公开发布的信息，也可能分析出某些敏感信息。所以交易商在发布信息时要进行适当处理，以保护用户的隐私信息。

4. 支付过程中的隐私保护

在线支付具有方便、快捷等优点，尤其是在线信用卡支付方式已经成为主要的在线支付方式。但电子支付的技术性、网络的虚拟性和电子支付过程中的复杂性等原因，使得电子支付中消费者隐私保护面临极大的挑战，支付过程中仍存在安全隐患。

在线支付过程中，如果持卡人的信息汇集在某处，那么持卡人的隐私很可能得不到保护。例如，发卡银行掌握了持卡人的个人信息，如果同时记录了持卡人的交易信息，就可以追踪、分析出持卡人的消费偏好；同样，如果收单银行掌握了持卡人的交易信息及持卡人个人信息，也可以追踪、分析出持卡人的消费偏好。如果这些信息被卖给销售公司作为行销工具，会对持卡人造成不良影响。

根据 Need-to-Know 原则，每个交易参与方只能得知执行自己工作时所需知道的信息。根据这个原则，可以分析出持卡人隐私保护需求主要有以下三点：①信用卡信息只能被持卡人与发卡银行所知，商家与收单银行无须知道信用卡信息就能完成自己的工作。②订单信息只能被持卡人与商家所知，发卡银行和收单银行无须知道订单信息就能完成自己的工作。③发卡银行不应知道持卡人在哪里消费，因为发卡银行只需要确认持卡人是否授权这笔交易就可以了。

保护消费者隐私的支付技术主要有：①使用电子现金进行支付。电子现金，是一种以数字形式存在而通过计算机网络流通的货币。数字现金实际上是一个加密的序列数。电子现金可以被设计得具有匿名性，也可以被设计得具有不可追踪性。它可以保护消费者的隐私权，即使是银行也不清楚消费者的每一笔消费。②使用盲签名技术。盲签名使签名者在不知道消息 m 的情况下对 m 进行签名，签名完成后，签名者不知道 m 也不知道自己对 m 的签字，即无法将被签名的信息与发送者联系起来。对于消费者的每一笔消费，网购网站采用盲签名技术，网购网站也无法将消费行为与消费者联系起来。③使用公钥加密技术。公钥是一个公开的密钥，私钥是密钥所有者才掌握的密钥。如果在加密操作中使用了特定的公钥，只有密钥所有者使用私钥才可以解密。用公钥加密提供给网络商品供应商的必需信息，网络商品供应商只能用私钥解密，可使消费者信息尽可能少地泄露出去。

3.3 电子交易的信任机制

3.3.1 信任的基本概念

1. 信任的定义

由于信任的重要性，包括社会学、经济学、心理学、管理学、信息系统及电子商务和人机

交互等多个学科都对其展开了研究。在不同的文化背景和学科领域下，信任有着不同的含义。

1）传统学科中信任的概念和特征

Mayer 等(1995)在其关于信任的“种子”文章中对信任的含义和定义进行了研究，该文是信任研究领域中被引用次数最多的文章之一。Mayer 对信任的经典定义是：一方对于另一方的行为处于一种弱势地位的意愿，该意愿基于这样一种预期，即另一方会履行特定的并且对信任者很重要的行动，不论自己是否有能力去监控对方的行为。Mayer 认为信任表现为一种承担风险的意愿，这已成为信任研究的基础。

(1) 心理学。心理学对信任的研究最早始于 1958 年美国心理学家 Deutsch 的著名囚徒困境试验。这项试验开创了心理学人际信任研究的先河，被视为人际信任(interpersonal trust)的经典研究之一。心理学家一般认为信任是个人或组织信赖另一方的语言、口头或书面承诺的意愿，是一种主观信念。Gambetta(1988)认为信任是在能够监控对方行为之前并且无法了解环境对自己行为的影响情况下，一个实体对另一实体即将发生的行为的一种主观概率评估。Lewis(1999)认为信任是人际关系的产物，并且由人际关系中的理性计算和情感关联决定人际态度。

(2) 社会学。在社会学中，将信任理解为社会制度和文化规范的产物，是建立在法规、道德和习俗基础上的一种社会现象。Barber(1983)认为信任是一种通过社会交往所习得和确定的预期，其中最一般的预期是对自然的及道德的社会秩序能坚持并予以履行的信心。还有学者提出了不同于“个人信任”(personal trust)的宏观层面上的信任现象，如 Luhmann (1979)的“系统信任”(system trust)，Zucker(1986)的“基于制度的信任”(institution-based trust)等。

(3) 管理学。在管理学中，信任的研究常常与企业绩效、风险、交易成本联系在一起，认为信任能提高客户满意度与企业绩效，减少不确定性以及降低组织内和组织间的交易成本。Kumar(1996)认为真正能够区分信任关系的是双方建立相互信任的能力，他们相信双方利益相关，任何一方采取行动之前都会考虑自身行为对另一方所产生的影响。

(4) 营销学。在营销学中，信任的研究主要在买卖关系或分销渠道背景下进行，因此信任的对象包括供应商和销售人员。消费者可以对供应商产生信任，也可以对销售人员产生信任。信任既被看做是对于伙伴可信度的信念，也被看做是在处于弱势情况下依靠伙伴的意愿。信任对企业的关系营销(relationship marketing)战略非常重要，因为信任是依赖自己所依赖的交易方的意愿，信任会帮助交易双方建立长期的交换关系与合作关系。

虽然不同学者对传统信任的概念和特征有不同理解，但我们可以归纳出信任具有以下几方面特性。

(1) 主观性。信任是一种主观期望。不同的实体对同一个实体的信任存在差异。

(2) 风险性。信任的本身代表了愿意承担风险。

(3) 可依赖性。信任是一种心理预期，即有信心地认为对方未来愿意履行承诺。

(4) 善意性。信任意味一方有信心地认为另一方未来不会欺骗自己。

(5) 领域相关性。不同的人擅长不同的领域，例如电脑专家就不一定精通音乐，而主任医生也可能不知道如何修理汽车，因此信任需要限制在某一个或某几个特定领域中讨论才有意义。

(6) 不可完全传递性。A 信任 B,B 信任 C,并不一定就能推导出 A 信任 C。

2) 信息系统与电子商务中信任的概念和特征

在信息系统与电子商务领域中,信任研究主要基于消费者角度,所提出的定义往往综合了心理学、管理学、营销学的观点。信任包括信念与动机,信念包括四个层面的含义,即能力、诚实、善意、可预测性,动机则包括依赖对方的意愿、依靠的主观可能性。

信任与声誉的区别主要在于,信任是关于被信任者的可信度的所有推荐的聚合值。声誉值不能被赋值,只能被信任者聚合。

电子商务中信任具有传统信任的一般特性,但同时还具有自身的特点。

(1) 上下文相关性。信任关系总是和特定上下文紧密联系。在某个特定上下文中,能够建立起信任关系的实体 A 和实体 B 很可能在另一个上下文中无法建立起相应的信任关系。

(2) 可测量性。计算机学科的学者出于计算和处理的实际需求,认为能够使用类似于度量信息的方式来度量信任,将信任关系划分为不同等级。

(3) 动态性。随着近期增加的证据和交往经验,可能会增加或减少我们对另一个实体的信任度。信任者认同被信任者的行为时,将会提高对被信任者的信任等级,增强和被信任者之间的信任关系。

2. 信任的分类

作为一个宽泛的概念,信任根据不同的分类方法可以有很多不同的类别。

1) 从时间维分类

根据信任的发展阶段,信任可分为以威慑为基础的信任、以信息为基础的信任和以转移为基础的信任。①以威慑为基础的信任,是指刚刚建立关系时,双方会按照自己的承诺行动,因为他们害怕违背承诺带来的惩罚,这一阶段的信任是建立在这种惩罚威慑基础上的信任。②以信息为基础的信任,是指随着关系的建立,交易双方的交互越来越多,获得对方的信息也越来越多,从而在此基础上建立起来的信任。③以转移为基础的信任,是指随着双方长期的交流和交易,以信息为基础的信任水平不断提高,一方(A)可根据另一方(B)对第三方(C)的信任水平形成一方(A)对第三方(C)的信任。

根据信任的发展速度,信任可分为慢信任和快信任。①慢信任是伴随时间的延续产生,在长期工作关系中建立起来的一种典型的信任。②快信任是当关系迅速产生随后迅速结束时产生的,如虚拟团队成员之间的信任。

根据信任的发展程度,信任由浅及深依次体现为基本信任、保证性信任、延伸性信任。①基本信任是一种基本的信任形式,是社会生活的前提。②保证性信任是用合同、协议和承诺保证的信任。③延伸性信任是建立在公开、宽泛的基础之上,表现为随着关系的不断加深以至于正规的合同已经不必要了。

2) 从空间维分类

根据网络环境,信任可分为网下信任与网上信任。①网下信任涉及公司的离线行为(如直接销售、渠道销售、其他的沟通和交易等),以及公司与消费者及其他干系人之间的关系。传统销售条件下,企业要同消费者、供应商、合作伙伴等打交道,这些实体之间的信任关系均属于网下信任的范畴。此外,消费者往往是通过与企业销售人员的交互来建立对企业的信任。②网上信任涉及以电子为媒介,尤其是以互联网作媒介的公司的商业行为。消费者网

上信任的对象包括网站、商家、互联网技术。网站充当了传统销售条件下的销售人员的角色，消费者通过对网站的考察来建立对商家的信任。此外，消费者对互联网技术的信任是整个网上信任体系的前提。

根据信任产生的层面，信任可分别在三个层面产生：个人层面、人际关系层面和社会层面。①基于个人层面上的信任是个人人格特质的表现，简单说来就是“我愿意信任某人”。②基于人际关系层面上的信任是人际关系的产物，是基于人际关系中的理性计算、情感关联而产生的信任，简单说就是“我信任你”。③基于社会层面上的信任是群体共性的一个特征，简单说来就是“我信任所有的人”。

根据环境特异性，信任可分为一般信任与特殊信任。通过特定的方式在特殊的环境下产生的信任就是特殊信任，反之则为一般信任。比如，在网上信任中，相信网站可以提供准确、及时的信息是一般信任；相信某个特定的网站可以提供某一方面准确而及时的信息就是特殊信任。

3. 交易结果评价

在制约电子商务发展的因素中，交易风险及其纠纷的存在处于首位。为了降低交易中的信息不对称问题，电子商务交易平台设计了在线信誉评价系统，对买卖双方的交易历史及其评价进行记录。在声誉效应的影响下，卖家也更加重视买家的交易满意度，并且也形成了为获取好评减少差评而提高服务质量的良好风气。交易结果评价中的不满意（或者成为纠纷）是产生非好评（包括中评和差评）的直接原因。而影响交易结果评价的主要因素为商品问题、收货问题、沟通问题、售后问题。交易结果评价研究模型如图 3-5 所示。

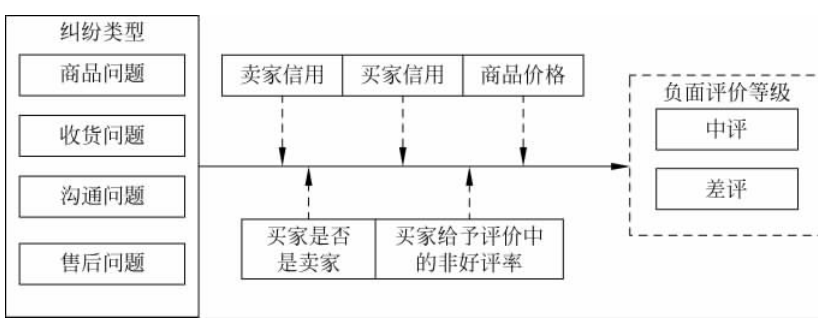

图 3-5　商品问题研究模型

1）商品问题

商品问题指买家购买收到的商品，存在有破损、与网上商品描述存在差异、影响正常使用或其他质量瑕疵。商品问题包括以下四种情况：商品与描述不符、商品质量问题、商品价格问题、卖家发错商品。商品描述不符指买卖双方成交后，买家收到的商品与网上描述（包括图片描述与文字描述）有不符的情况。商品质量问题指买卖双方成交后，买家收到的商品是假货、劣质品或瑕疵，如劣质面料或有瑕疵的服装。卖家发错商品指买、卖双方在成交后，买家收到商品的数量、尺码、颜色、运送方式与下订单时不一致。

2）收货问题

网络购物中，时空的阻隔使得商品配送一般都要通过第三方物流公司实现。收货问题

纠纷包括由第三方物流公司引起的问题和卖家发货延迟或不发货引起的纠纷，往往会导致买家给卖家中评或差评。个人卖家，大多有货物渠道资源，由于资金问题，有的手上并没有货物或只有少量品种的货物。卖家在网站上贴出货物信息和图片，待买家拍下商品后他们再与供货商联系进货发货，造成买家常常会抱怨收获速度慢，甚至有时会因为供货商缺货而卖家无货可发，这对先拍了商品等待收货的买家来说是一个非常不愉快的心理体验，很可能会对交易给出负面的差评或中评。

3）沟通问题

沟通问题纠纷包括沟通态度纠纷和沟通有效性纠纷。买卖双方有沟通的交易比没有沟通的交易成功率更高、纠纷更少。从评分反馈来看，缺乏沟通是产生拍卖纠纷的一个因素。买家给中评和差评的理由常常是卖家态度不好或是卖家不回复留言。各个店铺的客服在人员数量、在线时间、素质等方面参差不齐，往往导致买家抱怨客服态度差或者买卖双方不能有效地沟通，特别是交易量大的店铺，在客服人员少的情况下，容易发生这类纠纷后来不及解释，使得买家给出负面的评价。卖家可以通过改进客服水平来减少这类纠纷从而提高好评率。

4）售后问题

售后问题纠纷，主要是退换货标准和由此产生的运费承担问题，很多卖家为避免退换货问题往往在“买家须知”里面写着“确定为质量问题可以退换，其他诸如面料不好、色差、与想象不符等不接受退换”，但对于“质量问题”并没有相关部门出示的统一标准，很难判断。买卖双方常常就这一问题产生纠纷，若在双方协商过程中卖家态度不好或者结果不能令买家满意，那么买家就很可能给卖家负面的评级。再者，由退换货问题产生的运费承担问题各个店铺处理方式不一，就算一些店铺承诺承担“商品质量问题”的退换运费，但如果买卖双方就是否是质量问题不能达成一致，也容易就退换货费用产生纠纷。

4. 商家可信度

电子商务交易互动中，消费者只有在相信商家可以履行承诺也就是对商家有信任感知后，才会产生购买意向从而与商家交易，愿意支付资金换得物品或服务。信任影响因素包括：店铺形象、商品质量、商家与客户沟通性、售后服务、店铺规模、商家信息公开度、物流时间、交易金额和交易时间。

店铺形象。在初始信任形成阶段，就一般商家来说，消费者还不是很了解商家，与商家之间没有交易关系或交易关系很少，网站的形象代表商家的形象，因此网站的声誉会影响消费者的信任。另一方面，就传统企业跨领域的商家来说，虽然消费者对商家本身有一定的了解，但是到电子商务环境中，交易环境的虚拟性产生不确定性，网站与商家是既联系又分开的，企业的形象可以代表网站的形象，却又不能完全代表网站的形象，而网站的形象也同样反作用于企业形象。网站商家对自己网上店铺的装修和管理具体包括商品图片、商品展示、商品分类是否合理，页面浏览是否方便。店铺形象越好，越能吸引广大消费者来光顾，也越能使消费者对店铺商家产生信任。

商品质量。消费者所购买商品的质量，包括产品各方面性质是否如商家产品介绍中一样、产品是否与消费者预想一致等。

商家与客户沟通性。商家与客户沟通性是指商家在与消费者交流的过程中所体现出的

沟通能力，消费者在与商家的沟通中获得的积极体验会使消费者对商家产生信任。

售后服务。售后服务是指商家在售出自己商品之后，能及时处理消费者反映的各种关于商品的情况，商家对客户的售后服务质量越高，越能使消费者对商家产生信任。

店铺规模。店铺规模是指商家店铺每天的交易量、商品种类等的规模，这些规模越大，说明商家的店铺规模越大，越能使消费者对商家产生信任。

商家信息公开度。商家信息公开度主要是指产品、邮资、退货规则、产品注意事项等详细说明、卖主联系方式、地址信息公布等有关商家的信息公布程度，其对消费者对商家的信任产生积极影响。

物流时间。物流时间指的是从商家发出商品到消费者接到商家商品的这一段时间。物流时间也是影响消费者对商家信任的一个积极因素。

交易金额。交易金额指消费者在商家店铺购买一次性产品的费用，购买费用越高的消费者的评价对商家信任的影响越大。

交易时间。交易时间指消费者购买商品后，对商家进行网上评价，网上评价时间即为交易时间，时间距离当前越长，对当前商家信任的影响越小，以致可忽略不计。

根据 Oliver 的预期不确认理论，顾客根据购前预期与绩效表现的比较结果判断是否满意。卖家信誉越高，则买家的预期越高，那么发生纠纷以后，预期与感知产品质量差距越大，从而顾客不满意程度更大。网络顾客期望，是指顾客基于过去网络购物经验、个人特定需求和商家的声誉品牌而对购物网站整体服务质量的预期。价格越高的商品，发生同类型纠纷后，买家的不满意程度越高。

5. 用户可信度

买家是直接与卖家发生交易的主体，也是卖家评级的主体。买家的信誉值可以在一定程度上代表买家的经验，不同购物经验的客户对同一纠纷的评价由于对标准的掌握不同可能会有差异。

影响用户可信度的因素主要包括交易时间、交易金额、其他用户的评价。交易时间距当前时间越长，用户的可信度就会随时间的推移有一定程度的衰减。买卖双方交易金额的大小反映了交易的可信度，同时也反映了双方交易结果评价的可信程度。受到其他用户的评价越高，说明该用户评价的真实性越高，其评价也更值得其他用户借鉴参考。

买卖双方进行交易后，买家对卖家进行反馈评分时，买家所提交的反馈信息需要考虑买家本身的可信度，买家可信度高时，其反馈信息越可信、越有价值，反之，则越不可信、越缺少价值。

6. 交易结束后的评价

交易结束后，服务请求者根据实际得到的服务质量和服务提供者自身声称的服务质量计算服务质量差异度，以此判断服务提供者的可信程度，并进行相应的奖惩和信任度更新。

评价指标主要包含信息质量、技术质量、客户服务质量满意度。①信息质量指信息的真实性、完整性、关联度(%)。信息完整性、准确性：商品品种、规格、质量、相关知识的真实性、完整性、准确性。对客户要求的反应速度：信息检索速度、对客户平均响应时间(邮件、电话、短信等)。信息、数据库容量：拥有信息数据库容量、信息分类深度和关联度(%)。

②技术质量，如网页反应速度、客户响应时间、平台并发用户数、每秒响应请求次数。③客户服务质量满意度：指客户服务质量期望值与客户感知之间的差异程度。客户投诉降低率反映服务质量的提升，导致客户投诉率降低。

评价方法主要有综合评价和单项指标评价。

(1) 通过专家参照各项评价指标的重要性所确定的各项评价指标的加权系数，按评价标准对各单项评价指标进行评价打分，通过各级指标逐级加权计算、汇总，形成电子商务服务水平总的评分结果，把该综合评价分数称为电子商务服务指数。

$$E = \sum (I_i \times W_i) \tag{3-1}$$

E 表示电子商务服务指数(总评分)；I_i 表示 i 个评价指标；W_i 表示 i 个指标的权重，$\sum W_i = 1$。

(2) 要按照平台服务商的类型(如综合性服务企业、专业性服务企业)制订各评价指标的评价标准，现针对一般平台服务商、服务提供商提出以下评价方法：评估级别，分优、良、好、中、差五级；百分制，依次为 85～100 分，75～85 分，60～75 分，40～60 分，0～40 分。

3.3.2　信任建立过程中的各方博弈

博弈论是研究各种博弈情景下参与各方及其理性行为选择的理论，也是关于竞争者如何根据博弈环境和竞争对手的情况变化采取最优策略和行为的理论。

参与电子商务交易的主体在选择自己的交易行为和做出决策时，商家、顾客、电子商务平台提供者之前的交易行为和决策是会相互影响的。电子商务市场中信用的高低也是由于不同交易主体交易行为和决策引起的，如果各交易主体都选择诚信交易，那么这个市场就是高信用的，反之就是信用比较低的。

通过博弈论来分析不同交易主体之间的决策是如何相互影响的是非常有效的。首先，从各交易主体之间的关系看，在进行电子商务交易的时候某次交易的信用高低，或者说整个电子商务市场的信用的高低是不同交易主体相互博弈的一种结果；交易主体的决策选择是相互影响的，如果经过系列的决策选择最后都选择进行诚信交易，那么我们就说本次博弈的结果是(诚信，诚信)，那么电子商务市场有较高的信用，当博弈结果交易双方选择(欺诈，欺诈)时的效益最大，则电子商务市场有较低的信用。

1. 卖家和买家的博弈

在电子商务市场中，顾客有很多可供选择进行交易的商家，顾客只要轻点鼠标就能对商家的信用、以前的交易记录、顾客评价和商品的价格一目了然。所以可以将顾客与商家之间的博弈看做是完全信息状态下的博弈。顾客首先关注的是电子商务商家的价格，如果商家的价格比较合适，然后就会看其他顾客评价，如果该商家的评价基本都是良好的，那么就会认为该商家是会进行诚实交易的，就会与该商家产生交易行为；但是一旦发现有评论说该商家存在诚信问题，那么基本不会有顾客再次冒险与该商家进行交易。因此顾客的决策行为是受商家商品价格、信誉等影响的，商家选择诚信交易还是欺诈交易也是受顾客消费心理的影响的。在顾客比较注重商家信用的前提下，商家是不会出现投机行为的，那么这个电子商务市场就是高信用的。

为了更加真实地描述卖家与买家之间的博弈，我们假设：①参与者为卖家和买家，卖家的策略是诚信或者欺诈，买家的策略是购买或不购买。②假设在交易过程中，每次博弈都是独立的，参与者都是完全理性的经济人，参与者同时做出决策且各自支付的信息为各参与者的共同信息。③存在政府的监督。如政府制定相关法律对行骗者进行惩罚，以至于卖家如果不诚信，他都需要付出一定的代价。

根据上述假设，卖家与买家之间的博弈可以视为完全信息静态博弈，双方支付矩阵如表 3-3 所示。

表 3-3 买卖双方纯策略博弈支付矩阵

买家	卖家	
	诚信	欺诈
购买	a_1,a_2	$-b_1,b_2-c$
不购买	0,0	$0,-c$

其中，a_1,a_2,b_1,b_2,c 均大于 0。在买家购买商品且卖家诚信时，a_1 为买家的支付，a_2 为卖家的支付；在买家购买商品但卖家欺诈时，$-b_1$ 为买家的支付，b_2-c 为卖家的支付；c 为卖家采取欺诈策略时所需成本，且实际生活中 b_2-c 应远大于 a_2。

当买家不购买商品，而卖家一直保持诚信时，参与者的支付都为 c，而当卖家实施欺诈时，他是要付出一定的被揭发被惩罚的风险，这个成本我们用 c 表示。当卖家选择诚信时，买家选择购买商品，这时他的支付达到最大。当卖家选择欺骗时，买家选择不购买商品，买家与卖家博弈结果是$(0,-c)$。而当买家选定不管怎么样都购买商品时，卖家的最优决策是选择欺骗，这时他可以获得最大的支付 b_2-c，当买家不论怎么样都不会购物时，卖家的选择是保持诚信。

从以上纯策略的博弈分析我们可知，买家与卖家的博弈不存在纳什均衡。不论怎么选择，双方的利益始终不能达到一致，任何一个纯策略组合都可以通过一个参与者单独改变自己的策略而获得更大的支付，所以我们可将此模型扩展为完全信息下的混合策略博弈。这将存在一个混合策略纳什均衡。现在我们假设买家按照一定的概率，随机地从两种纯策略选择一种作为他的实际行动，卖家同样按照一定的概率随机地选择自己的纯策略是诚信或者欺骗，见表 3-4。

表 3-4 买卖双方混合策略博弈支付矩阵

买家	卖家	
	诚信(p_2)	欺诈($1-p_2$)
购买(p_1)	a_1,a_2	$-b_1,b_2-c$
不购买($1-p_1$)	0,0	$0,-c$

设 U_1 为买家期望的支付，U_2 为卖家期望的支付，则有：$U_1=p_1\times p_2\times a_1+p_1\times(1-p_2)\times(-b_1)$，整理后得 $U_1=p_1\times[p_2\times(a_1+b_1)-b_1]$；$U_2=p_1\times p_2\times a_2+p_1\times(1-p_2)\times(b_2-c)+(1-p_1)\times(1-p_2)\times(-c)$，整理后得 $U_2=p_2\times[p_1\times a_2-p_1\times b_2+c]+p_1\times b_2-c$。买卖双方最佳反应函数见表 3-5 和表 3-6。

表 3-5　买家最佳反应函数表

P_1	条　　件
0	$p_2\times(a_1+b_1)-b_1<0$，即 $p_2<b_1/(a_1+b_1)$
[0,1]	$p_2=b_1/(a_1+b_1)$
1	$p_2>b_1/(a_1+b_1)$

表 3-6　卖家最佳反应函数

P_2	条　　件
0	$p_1\times a_2-p_1\times b_2+c<0$，即 $p_1<c/(b_2-a_2)$
[0,1]	$p_1=c/(b_2-a_2)$
1	$p_1>c/(b_2-a_2)$

所得买家与卖家混合策略博弈的纳什均衡点是 $p_1=c/(b_2-a_2)$，$p_2=b_1/(a_1+b_1)$。即纳什均衡是买家以 $c/(b_2-a_2)$的概率选择购买商品，卖家以 $b_1/(a_1+b_1)$的概率选择诚信对待顾客。我们可以看到参与者的策略都是对方支付的函数，譬如当 c 越大，也就是当卖家选择不诚信时，法律、国家对他的惩罚越大，买家了解到这个信息，就可以认为卖家选择不诚信的概率较小，从而买家更愿意选择购买商品。同样我们可以假设 b_1 远远大于 a_1 时，买家会认为他选择买的期望支付会远远小于不买的期望支付(0)，所以他会选择不购买商品，而卖家在买家不太可能购买商品时他最好的策略就是诚信，这与我们计算出的纳什均衡点相符，$p_2=b_1/(a_1+b_1)$，当 b_1 增大时，p_2 增大，说明卖家随着 b_1 增大更愿意选择诚信。

在以上这个完全信息静态博弈的分析中，我们了解到买家仍有不购买商品的可能，卖家仍有欺骗顾客的可能。实际交易中，买家与卖家之间可能存在多次交易，且对于同一虚拟店铺不同的买家，卖家所有的历史交易信息是公开的，所有不同的潜在买家都知道这些信息。据此，我们可以将完全信息的静态博弈模型扩展为：一个参与人不固定(如买方不固定)，以卖方对一名买方提供产品或服务的博弈为一个阶段的重复博弈。对于扩展的重复博弈模型，我们新增以下假设：①同一卖家虽然可能有不同的潜在顾客，但我们仍然把这些顾客看成一个买家；②买家采取“冷酷策略”，即只要在重复博弈中卖家有一次欺骗行为，将触发买家在以后的策略中永远选择“不买”的策略。

根据表 3-3，我们可以得出卖家的期望支付，当卖家一直保持诚信的期望支付要大于他一次不诚信而获得的支付时，他将会在每次交易中都保持诚信的策略，设 $0<r<1$ 是卖家的投资期望收益率，我们把它当作一个贴现因子。则当卖家选择不诚信经营时的期望支付为：$U_2(\text{cheat})=b_2-c$，当卖家选择一直保持诚信策略时，买家就一定会一直和他交易，卖家将获得的支付是：$U_2(\text{honest})=a_2+a_2\times r+a_2\times r^2+\cdots+a_2\times r^n$，当 n 趋于无穷时，$U_2(\text{honest})=a_2\times[1/(1-r)]$。当 $U_2(\text{cheat})<U_2(\text{honest})$，即 $b_2-c<a_2\times[1/(1-r)]$或者 $r>1-a_2/(b_2-c)$时，卖家会一直采取诚信策略，合作的博弈就产生了，博弈的双方最后的策略都将是买家购买商品，卖家一直保持诚信，这就是重复博弈产生的信用机制。

2. 卖家和卖家的博弈

在电子商务平台上建立商家网站的商家可以说是数不胜数，因为这样可以省去商家建立网站和维护网站的各项费用。这样就使本来在物理空间比较分散的销售统一产品的商家

处于比较密集的环境中。与传统交易不同的是，实体商家在租用厂房、生产产品方面的费用都会相差无几，而且顾客不会一眼就能看出销售同质产品的商家的不同。但是在电子商务平台上就会有所不同，因为在电子商务平台上有一个比较明显的特征来区分销售同一产品的商家，那就是信誉等级。

信誉等级也一直是困扰商家的难题，为了获得高的信誉等级，电子商务平台上的商家可以说是绞尽脑汁。因为信誉等级不仅是区分商家的一个指标，在一定程度上也表明该商家的整体质量，包括商家自身的信誉、提供产品的质量、发布消息的真实性等，而这些信息都足以影响顾客的购买决策。所以基于网络平台提供者的商家之间的竞争要比传统商家的竞争更为激烈。

作为区分不同商家的一个重要因素——信誉等级，就成为了商家之间博弈的核心点，从而也就导致了不同的电子商务信用问题。有的商家会通过自己的经营慢慢积累信誉等级，有的会直接从其他商家那里购买已经是高信誉等级的店铺，这两种情况都不会产生电子商务信用问题，但是更多的商家会选择通过不法途径获得高的信誉等级，因为这样获得高信誉的成本相对来说比较低。这种高信誉等级会获得较高的顾客点击率，进而带来的是高的成交量，因此很多商家就会在信誉等级上做文章。

通过上面的描述，我们知道会产生电子商务信用问题的一个方面就是商家通过不正规的手段获得高信誉，而这种高信誉的获得只有商家自己知道，其他商家是无法知道其他商家的高信誉是通过什么途径获得的，所以说在信誉等级方面商家之间是处于一种信息不对称的环境中。但是因为销售统一产品，就存在一个如何标价的问题，因为电子商务平台的原因，价格的这种可比性被放大，顾客只需要轻点鼠标，商品就会按照价格高低进行排列，所以商家还是会考虑价格因素对顾客决策的影响。但是为什么会有很多商家信誉等级不一样，但是对于同一种产品却能在价格上没有差别，甚至高信誉的商家反而标更低的价格？针对不同信誉的商家在标价方面的决策进行博弈研究，分析高信誉与低信誉的商家在标价时会采取怎样的策略，从而判断该商家是偏向于诚信交易还是偏向欺诈交易，这样可以打破“唯信誉论”，也就是说，只要信誉等级高的商家在进行交易的时候就会偏向诚信交易，反之，信誉等级低的商家就会偏向欺诈交易。

3. 交易者和管理者的博弈

商家与平台提供者之间可以说是存在双重关系，首先，平台提供者通过从商家那里获利，越多的商家使用该平台就会获利更多，而且高信誉的商家会给该平台带来好的声誉；但是，平台提供者在某种程度上又承担着一个信息审核者的角色，商家在网站上发布的各种信息都需要经过平台提供者的审核，所以说商家与平台提供者之间还存在某种意义上的利益冲突。因此，商家与平台提供者之间的博弈存在两种不同的博弈情景，首先是以利益共同体角色进行博弈，同时还存在利益冲突者角色的博弈。

针对商家和平台提供者存在相同利益的情境下，主要是商家选择诚信交易或者欺诈交易的时候会对平台提供者造成什么样的影响。商家与电子商务平台作为利益共同体，博弈实质其实就是商家进行欺诈交易获得的利润和对平台提供者造成的声誉损坏程度的一个博弈。

3.3.3 信任的评估

1. 评估的基本原理和概念

目前，研究信任现象和信任关系的领域很多，如心理学、社会学、经济学、组织行为学、哲学以及计算机科学等。信任相关理论层出不穷，不同研究者研究的侧重点也各不相同。就信息安全领域来说，对于信任的概念、性质以及分类等基本问题仍缺乏统一的认识。下面就信任在 P2P 网络电子商务环境下的基本概念及相关理论进行介绍。

P2P 网络环境给出电子商务中信任的定义如下：信任是在特定应用环境和特定应用时间段中，事先期望实体执行某具体商务行为的主观可能性程度，其量化结果即为该实体的信任值。

直接信任指的是某一评价主体基于自己与评价客体直接交互的历史得到对该评价客体的信任。评价主体通过自己和需要了解的实体直接交互，将每次交互的情况进行统计、分析和积累经验，随着双方交互的不断深入，评价主体对评价客体的信任关系更加明晰。

推荐信任是指通过其他中间推荐实体间接获得对目标实体的信任关系。通常在开放的分布式网络环境中，一个实体想要获得网络中所有其他实体的信息是非常困难的。当该实体要与另一陌生实体进行交互时，会向自己比较信任的一些实体查询评价客体的信任信息，这样通过推荐信任评价主体也能对陌生实体进行信任评价。

在 P2P 网络环境中，实体间的信任关系有如下几个基本性质：①主观性。不同的评价主体对同一评价客体的可信程度可能有不同的理解。②上下文相关性。信任关系总是和特定的上下文相关联，在不同的上下文中，评价主体对评价客体有不同的信任评价。③有条件传递性。信任具有传递性，可以通过中间推荐将信任关系依次传递，但该传递性只在一定条件下满足。④不确定性。由于 P2P 网络的开放性和应用的复杂性，交互的实体对彼此的信息了解得不够充分，使得一个实体对另一实体将来行为预期的主观判断带有不确定性和模糊性。⑤可度量性。可利用历史经验对评价客体的未来行为进行判断，进而得到信任的具体程度。

2. 信誉与信任（信任值的计算）

传统的交易都是买卖双方面对面地进行交流沟通，从而达成交易意向。而电子商务却是买卖双方在没有谋面的情况下就可以把交易完成。电子商务中的不谋面的交易，使交易的风险增加了很多。

信用是指实体在未来一定时期内兑现承诺的能力。两者之间，时间上有差别，评价内容不同。信誉是信用评价的基础，如果没有好的信誉，即使未来发展前景乐观也不可能有信用。

信任是指对节点身份的认可及对节点能够按照预想完成其行为的能力的信赖。信任用信任值来度量。信任值并不是一个与节点身份绑定的固定值，而是以节点身份为参照，并依赖于特定时间段及特定上下文环境的变量。信任既包含身份信任，也包含行为信任。

信誉是指通过对节点过去交易行为的综合考察并依据其他节点对该节点的信任评估而得出的综合期望值。信誉同样也依赖于特定时间段及特定上下文环境。在两个节点进行交

易时，若彼此间从未有过直接的信任接触，往往可借助对方的信誉来进行信任抉择。

在信任管理中，信誉(reputation)是一个经常出现的术语。和信任一样，信誉也没有统一的定义。本质上信誉属于社会学的范畴，在社会学中，信誉是社会网络中的一个网络参数，并且是全局的、公开的。信誉和信任相比，信任的主观性更强，是两个 Agent 间一对一的关系；而信誉是整体的、全局的观点，是一个 Agent 在由多个 Agent 组成的公众中的总体形象与综合评价结果的体现。

信誉、信用、信任的相互关系见图 3-6。

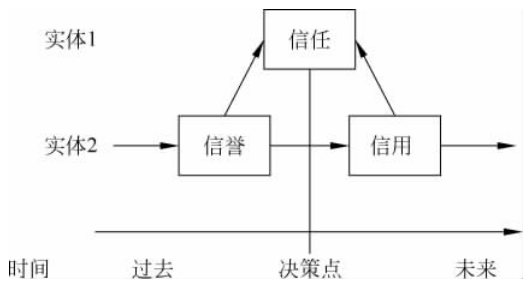

图 3-6 信誉、信用、信任的相互关系

3. 常用的评估模型

在不同的应用领域，国内外很多学者都对信任管理进行了深入的研究，例如 peer to peer(P2P)系统、Web 服务系统、多智能体系统、网格计算系统(Grid)、电子商务系统和安全系统等。通过对主体之间信任关系的描述和获取方法的研究，将信任分为基于策略和凭证的信任、自动信任协商和基于声誉的信任。其中基于策略和凭证的信任，本质上是一种基于身份的信任，主要解决的是授权和访问控制方面的问题；自动信任协商，实现的是对于跨域隐私的保护和信任的建立；而基于声誉的信任，则是建立在用户以往的直接交互经验、其他用户的意见或两者的综合对交互对象未来的行为期望进行预测评估。

目前，国内外众多学者面向各种应用研究开放分布式系统中的动态信任关系，并采用证据理论、模糊推理、贝叶斯函数等数学方法和数学工具对其进行分析设计，建立了信任管理模型。

1) 基于声望的信任模型

基于声望的信任管理起源于电子商务领域，其中最具代表性的是 eBay 和 Amazon 的信任模型，现在这种方法已经被广泛地推广到 P2P 系统、智能体系统、移动自组织网络以及最近很受关注的语义网等领域。基于声望的信任模型根据用户自己直接的交互经验、其他用户的意见、推荐或者是两者合成得到的结果来形成对另一个节点的信任评价。

当顾客和商家进行在线交易的时候，仅仅凭借过去的直接经验是不可能评价所有其他用户的，因此常常面临遭受损失的风险。在这种情况下，我们需要借助于其他的信息来源，通常有两种方式：一种是咨询一个集中式的第三方权威。第三方权威可能与被询问的用户有过交互的经验或者保存有其声望的信息，从而可以提供相应的信任评价。但是由于互联网上资源的多样性和复杂性，因此无法找到一个集中的第三方权威能够提供所有的声望信息。另一方面作为第三方权威，往往要面临信誉受损的风险，因此目前大部分模型都采用的

是另外的一种方法——分布式的信任模型：用户不依赖一个中心权威进行信任决策，而是通过获取的声望信息，由智能体自己来进行信任评估。因为不存在中心权威，所以只有智能体之间依靠相互合作并根据过去的行为来确定哪些节点是可信的。

进行信任决策的信息往往不是单方面的，早在 1994 年，Marsh 就提出了一个信任计算模型，这个模型后来被普遍认为是第一个比较全面、正式的信任模型。Marsh 用一组变量来描述信任，包括重要性、效用、能力和风险等，而且还给出了一种合成信任的方法，同时 Marsh 强调时间也是合成最后信任值的一个关键变量。由于该模型需要确定很多变量，而在真实的情况下这些变量又很难获得，所以现在的研究者并没有按照 Marsh 的模型继续研究下去，但是他所提出的一些理念至今还被广泛地应用，比如信任值可以被量化成一个连续的变量以及信任的几种类型等。

Abdul-Rahman 和 Hailes 将信任(trust)和声望(reputation)合并到一起来进行虚拟团体中的信任计算。在他们的模型中，信任被定义为智能体执行某个特定操作的主观概率，而声望被定义为基于观察和过去的经验，一个智能体对另一个智能体未来行为好坏的一个预期。信任来源于智能体自己过去直接交互的经验和知识，而声望来源于其他智能体的意见和推荐，最后利用加权平均的方法将这两个参数合并成最后的信任评价。在这个模型中，一个最大的问题在于如何确定加权平均的权重，因为权重不同，最后的结果将会完全不同，而权重的确定是非常主观和不确定的。

在网格的环境中，为了避免节点在信任决策过程中的主观随意性，陈等人提出了一个基于贝叶斯函数的信任模型。通过信任模型对节点的分析和判断，采纳其中推荐能力最强的中间节点作为推荐者，并搜索出到资源节点的信任链路，然后利用贝叶斯函数对经由信任链路获得的资源节点的每种属性进行综合评估，最后确定是否访问该资源节点。该模型的主要特点是减少了信任链路上中间节点的主观随意性的判断，请求者可以根据自己的需要自主地进行信任决策，因而具有一定的灵活性。

计算一个节点声望值的最好的方法是根据过去直接交互的经验，但是很多情况下这样的信息是无法获得的，因为在巨大的信任网络中，节点之间的交互往往比较稀疏。为了解决这个问题，一种方法是借助于智能体之间的社会网络关系来获取声望信息，另一种是对不同的信任评价进行归类从而降低稀疏度。Golbeck 等人就通过信任网络(web of trust)的连通关系来计算信任度。起始节点将询问请求发送到它的邻居，如果这些邻居没有相关的信息，那么就再向邻居的邻居逐步地扩展开来。在搜索路径上，信任度低的节点所提供的信任评价将被忽略，最后起始节点会平均所有评价值，然后四舍五入为 0 或者 1(0 代表不信任，1 代表信任)。该模型是建立在人与人之间的社会网络基础上，它的有效性在应用程序 Trust Mail 中得到了验证。

在信任管理领域中，一个关键的问题是研究信任的传递，而在这个问题上不同领域的学者尚有争议。Christianson 和 Harbison 认为信任值是高度主观的二元值，所以是不可传递的。在安全领域里这个观点得到了普遍的认同，因为实践证明这种传递的信任往往是不可靠的。Finin 等人认为当信任管理的范围限定在基于推荐的信任领域时，信任就是条件性部分可传递的。Olsson 认为信任只有当知道所有相关的用户都使用同一个信任度量并且这个度量和信任者与被信任者都是无关的情况下才是可传递的。Stewart 等人研究在万维网上信任是如何通过超链接在不同组织之间进行传递的。研究发现顾客们倾向于认为在值得

信赖的组织和陌生组织之间存在超链接就意味着两者之间存在着某种关系，而这种联系往往会提升陌生组织的信任等级而降低值得信赖组织的信任等级。

信任传递研究中最有代表性的就是 EigenTrust 模型和 Richardson 信任模型。EigenTrust 根据节点过去的信誉历史，在 P2P 网络中计算一个类似 PageRank 的全局信任值，用户可以根据这个全局信任值来选择交易对象，从而规避恶意节点并将它们孤立起来，一个节点的全局信任值是根据信任网络中其他节点对它的局部信任值加权平均计算出来的，而权重就是这些节点本身的全局信任值。EigenTrust 需要预先选定一些信誉高的节点作为起始节点，一旦这些节点不能工作或是退出网络，那么 EigenTrust 模型就无法正常工作了。Richardson 的信任模型利用路径代数来计算信任的传递从而量化信任值和不信任值，和 EigenTrust 计算全局信任值不同，Richardson 模型计算的是针对每个节点个体的个性化的信任值，而且他的模型可以十分有效地抵抗外界环境的噪音。

针对 EigenTrust 模型需要预先选择起始信任节点的缺点，Song 等人提出了一个基于模糊逻辑推理的 P2P 的声望系统 PowerTrust。通过分析 eBay 的真实数据，Song 证明了 eBay 上用户的交易次数符合幂律分布，而对某个节点信任评价起决定作用的是只占整个用户中一小部分的超级客户。在合成最后的信任值时，PowerTrust 将所有一度邻居的评价聚合起来，同样是采用加权平均的方法，只不过 PowerTrust 的权重是由三个变量的模糊值来确定的：节点的信用值、交易的时间、交易的数量。由于采用模糊逻辑，因此 PowerTrust 可以更好地解决 P2P 系统中信任计算的不确定性、模糊性和信息的不完全性等问题。

为了解决非结构化的 P2P 网络中的信任管理，周等人又在 PowerTrust 的基础上提出了利用“闲谈”(Gossip)来进行信任计算的模型 GossipTrust。GossipTrust 利用节点之间相互传递的“小道消息”并行地计算所有节点的全局信任值。每个节点的局部的信任值可以快速地聚集成全局信任值，经过几个周期的迭代，全局信任值就可以收敛到一个确定的值。GossipTrust 模型解决了非结构化的 P2P 系统中的信任计算问题，而且具有较强的可扩展性和健壮性，但是由于在传递“小道消息”的过程中会带来很大的网络通信负载，因此该模型在繁忙的网络中不适用。

Ramchurn 等人开发了一个基于置信度和信誉值的模型，通过利用模糊集来指引智能体对过去的交互进行评价并重新建立彼此之间的关系。通过分析某个智能体的过去交互的历史来获取它的置信度，而通过从社区中其他智能体处获取的经验得出该智能体的信誉值。这个模型采用悲观的策略来评价信息来源的信任值，因而有可能会导致系统中值得信任的智能体不被信任。

Cai-Nicolas 等人提出在某个特定的领域，例如书籍和电影推荐系统，利用信任度和用户兴趣爱好相似度之间的关联可以提高推荐系统的有效性和准确性。基于类似的想法，李等人提出了一个基于 P2P 环境下的全局信任模型 SWRtrust，该模型对不同节点的评分赋予不同的权重，而该权重是根据节点之间评分行为的相似度计算出来的。李等人利用两个节点评分向量的余弦夹角函数来计算相似度，并采用归类的方法来解决向量稀疏的问题。通过使用相似度加权模型，可以避免伪装的恶意节点的攻击。

在上面的叙述中，我们总结了一些典型的基于声望的信任模型。根据计算方法的不同，这些模型又可分为全局信任模型和局部信任模型。全局信任模型为网络中的每个节点计算一个类似于 PageRank 的全局信任值，该信任值是这个节点唯一的一个信任评价，它综合网

络中所有其他节点的看法。比较有代表性的全局信任模型有 EigenTrust、PeerTrust、PowerTrust、SWRtrust 等。在局部信任模型系统中，节点利用信任网络通过询问有限的其他节点以获取对某个节点的信任评价，再结合自己和该节点直接交互的历史来确定该节点的信任值，因此对于同一个节点，可能有多个不同的甚至相差悬殊的局部信任评价。比较有代表性的局部信任模型有 Richardson 模型、RSWC 模型、FilmTrust 和 FIRE 模型等。这两种模型各有优缺点，通常来说信任是主观的，因此全局信任模型往往不能很好地体现节点之间的差异性和个性化，但是却拥有较小的计算成本并能避免恶意节点之间的协同作弊。而局部信任模型通过节点之间消息通信或广播的方式来进行交互，往往只能获得小部分节点的信任评价，因此评价结果可能不够全面，但是局部信任模型更能体现个性化的信任计算，而结果也可能更符合个体的需求。

2）集中式的信任模型

传统情况下，信任都是以集中式的模式来进行管理的，典型的例子是采用一个可靠的第三方或是权威。接下来我们将介绍几个典型的集中式的信任模型。

在我们日常生活中广泛使用的 eBay 和 Amazon 等在线购物网站采用的都是集中式的信任模型。这些网站利用简单的加减和求平均值的方法对在线的买家、卖家进行信任评估，集中地建立和维护信任关系。通过分析 eBay 在线购物网站中大量的真实数据，指出了 eBay 这个集中式信任模型的几个不足：①大约只有一半的用户在交易后会提供反馈；②几乎所有的评价都是正面的，顾客不愿意对卖家进行负面评价，除非是出于报复心理。由此可见，这样的评分结果对于其他顾客而言并没有很大的参考价值，因此也无法为将来的交易提供可靠的借鉴，但是研究人员也指出 eBay 的信誉系统仍然可以在某种程度上发挥作用，一是由于广大用户相信它的奖惩作用。因而大部分人都会自觉地遵守相应的服务规范。二是如果 eBay 可以快速地对恶意节点采取行动，那么就可以避免进一步的危害。通过上面的分析，我们知道一旦一些恶意用户了解到 eBay 信任管理模型的漏洞而进行欺诈的话，那么后果将会非常可怕，因此很有必要为在线交易系统提供更加有效的信用管理模型。

SPORAS 也是一个集中式的信任模型，它对 eBay 等在线信任模型进行了改进，为松耦合的在线社区提供了一个信任机制。在 SPORAS 中，新用户的信任值最低，根据以后交易的表现，信任值不断地累加。无论某个节点的信用有多差，其累积的信任值都不会比新来的用户低。当根据其他节点的反馈对该节点声望值进行更新时，都反映了最近一次交易的信任度，因此可以看出 SPOARS 模型对信任的评价更注重近期的历史信用度，这样可以有效地避免用户信誉榨取的现象。同时交易价值越大，所承担的风险也越大。

Gil 等人提出了一个基于语义网的集中式的信任评估模型——THELLIS。该模型根据每个用户对信息资源的独立反馈来形成对信息资源的信任评价。用户可以对信息资源进行标注来显式或隐式地表达它的可信度和可靠度，系统将这些评价集中起来并将这些平均的反馈结果展示给用户。THELLIS 的信任评估是建立在用户反馈结果平均的基础上的，所以它提供的可信度参考结果缺乏个性化的观点，因此该系统提供的结果只有当用户的意见和大众的意见达成一致的时候才有效。

集中式的信任模型可以最大程度地降低节点之间交互的网络开销，但是也存在着很大的问题。集中式的模型需要有个中心权威来衡量节点的可信度并为用户提供相应的标准，用户为什么要相信这个中心权威？如果这个中心权威是邪恶的怎么办？这个中心权威会不

会因为利益等方面的原因而造假？即使一些知名网站具有很高的信誉度，可以避免让用户产生上述的疑问，但是也存在着单点失败的可能。一旦由于某种原因，中心权威无法正常工作，那么整个信任系统也将陷入瘫痪。而且由于互联网上的信息量极其巨大，而且还在迅速地增长，单单依靠一个集中式的权威来进行信任管理显然是不可行的。所以目前绝大多数的研究人员采用的都是分布式的信任模型。

3）基于云的信任模型

基于云模型理论的信任评价模型通过信任云及信任标准云的定义，客观地反映了信任的模糊性和随机性，实现了信任从定性到定量间的相互转换。给出了信任云的合并及相似度计算算法，实现了信任的分属性及综合评价和决策，仿真实验表明模型是可行的和有效的。

由于信任本身是主体间的一种信念，它是对主体特定上下文行为特征的主观判断，因此具有很强的主观性、模糊性和随机性，无法精确地加以描述。为了较为科学地解决信任的评价问题，在 M. Blaze 等人提出了信任管理的概念之后，一些学者基于不同的研究背景，提出了各自的信任评价模型。其中比较典型的如：Beth、Jsang 等人提出的基于概率论知识进行信任度推导和计算的模型，此类模型将信任完全建立在精确的数学模型之上，将信任的模糊性等同于随机性，不能很好地反映信任的本质；为了更加准确地把握和反映信任的本质属性，有部分学者使用模糊数学的方法来建立信任评价模型，此类模型使用模糊集理论作为信任评判的主要工具，用隶属度来刻画信任的亦此亦彼性。然而，用模糊综合评判法进行评价时，虽然较好地表述了信任的模糊性，却存在评判失效的问题，而且没有客观地反映信任的随机性。

李德毅院士基于概率论和模糊理论的有机结合提出了云模型理论，通过隶属云及云发生器等算法，较好地解决了定性概念与定量的统一。因此，将该理论引入信任管理领域，可以客观地反映信任本身的模糊性和随机性本质，较为科学地解决了上述评价模型中存在的不足。

由于信任是交易双方依据历史经验及相关资料建立起来的一种抽象的心理认知，随着交易内容和交易时间的变化，信任的度量具有较强的模糊性和随机性。为了客观地反映信任的这种本质，引进云模型的方式来定义信任，并将信任的度量归属为[0,1]区间的随机数，而且值越大，信任度越高。李德毅院士论述了正态云的普适性，信任评价的语言值适用于一维正态分布云的表达。信任云除了完整的形态之外，在信任区间的边界还有半升云和半降云两种半云形态，半云用来表达具有单侧特征的信任概念。关于信任的度量也不是精确的，实际上，在应用中也无须对信任做出精确的评价，只要确定交易对象能否满足交易阈值的需求即可。

李杰等的实验针对不同的交易上下文，较为全面地考察了节点的各个属性，并客观地反映了信任的模糊性和随机性本质，从而使评价结果更加客观、真实。该方法不仅可用于 C2C 电子商务中，也为开放式网络的信任评价提供了一个有价值的新思路。

4）基于社会关系的信任模型

人和人之间的信任关系是个典型的社会学问题，社会学家和心理学家已经对人类社会的信任问题进行了深入的研究，也积累了很多研究成果。在研究计算机领域的信任管理时，很多学者都借鉴了社会学领域的研究成果。

Sabater 等人提出了一个基于声望的信任系统 Regret，这个系统有一个分等级的本体结构，利用社会网络分析可以将各种不同类型的声望综合起来计算出最终的节点信任值。

Golbeck 等人就利用社会网络分析来建立语义网上的信任模型，该模型扩展了 Friend Of A Friend(FOAF)的描述规范并定义相应的信任本体，并根据小世界原理(small world)通过信任网络计算用户之间的信任值。这种对信任量化的算法就是我们前面提到的信任度量方法(trust metrics)。基于这个信任模型，Gol-beck 等人开发了 FilmTrust，利用社会网络中的信任关系作为电影评价的权值从而为用户提供一个个性化的电影评论网站。

为了提高信任推荐的准确度，一些模型通过分析用户的相似度来进行信任计算，通常有两种方法：一种是匹配过去的历史记录。例如 FilmTrust、BibServ 等需要用户手工输入一些档案资料，包括兴趣、爱好、专长、过去的评价等，然后通过匹配这些资料描述来提供最合适的推荐。Kautz 等人提出的基于社会信息过滤的个性化推荐系统 Ringo 也属于这一种，Ringo 首先通过比对不同用户的历史记录，找出一组相似的用户，然后根据这组用户的评价生成最终的推荐结果。第二种方法是在开放的环境中进行信息挖掘，例如 Referral Web 就是利用数据挖掘技术从互联网上公开的资料例如学术论文、学校部门里的成员构成等获取的社会网络来构建信任模型的。使用这种方法比让用户自己填写资料能够获得更多的社会关系的信息。通常一个用户只会注意到自己社会网络中很小的一部分，当通过社会网络分析来进行信任计算时，就可以扩展到更大的群体，发现更多的人员关联和隐藏的信任信息。借助于小世界原理，Referral Web 通过重建、可视化和搜索 WWW 上的社会网络来获取专家的推荐。

5) 基于语义网的信任模型

随着语义网概念的引入，计算机能够理解信任的描述词汇和进行信息的语义标注。越来越多的学者开始关注未来语义网上信任管理机制的自动建立。

早在 1998 年，TimBerners-Lee 就提出数字签名是解决语义网上信任问题的一个有效方法。在 2000 年的 XML 会议上，他又提出了语义网的七层架构模型，信任层(trustlayer)作为金字塔的最顶层，是一个十分重要的概念：当用户对互联网上的操作、安全以及所提供的信息拥有信任的时候，那么整个互联网就能够最大限度地发挥它的作用和潜能。Palmer 也曾经指出虽然目前关于语义网上的信任描述比较少，但是未来这将是语义网上一个非常重要的课题。O'Hara 认为信任是语义网视图中的核心，他总结出语义网上的智能体能够采取的五种信任管理的策略：乐观式、悲观式、中央式、调查式和传递式。乐观式是假设节点都是可信任的，只有当有证据证明某个节点是不可信的时候才决定不信任对方。而悲观式正好相反，直到证明某个节点是可信的才和该节点进行交互。集中式的信任模型需要依赖一个中心的权威来决定哪些节点是可信的。调查式是节点之间互相传递消息和进行推荐，通过比较和调查来决定相信哪个节点的消息和推荐。传递式是利用节点之间的社会网络和小世界原理来传递信任消息并做出最后的决策。

在语义网上，信任管理的另一个重要作用是当各种不同的信息资源同时存在时，智能体和自动推理机能够做出正确的判断。作为一个开放的系统，人们通过网页博客、Wiki 或是其他各种文件可以很容易地向互联网上增加信息。日常生活中，人们根据过去的经验和知识对网上的信息进行甄别从而形成信任决策。随着本体论和资源描述框架的引入，分布式网络中的元数据是机器可理解的，使得智能体可以自动地进行信息处理。智能体还可以在

信任网络中交换信任消息并通过信任链进行通信，同时语义网还可以利用推理和学习的能力来主动寻找可靠的信息。

Golbeck 等人将整个语义网看做是一张巨大的图(Graph)，把网络上的资源或对象看做是图中的顶点(Vertex)，而把谓词(predicate)看做是节点之间的有向边(Edge)。通过本体论来定义信任和声望，利用谓词关系映射的图进行信任的传递，最后用量化的方法来计算任意两个实体之间的信任度。

语义网的引入，使得智能体自己能够从外部环境中获取知识来扩展自己的知识库。而其中一个关键的问题是如何从开放、动态的语义网上发现值得信赖的资源。利用小世界原理，将个人和某个节点之间的交互经验和这个节点的声望信息集成起来形成最后的信任评价。在模型中，作者定义了一个信任的本体，这个本体是基于一个智能体的知识库的拓扑结构，包括社会知识和领域知识。

在语义网上，除了计算智能体之间的信任度外，Heymans 等人还提出了基于逻辑编程进行偏好推理的框架。每一个智能体都可以向任意的知识源提出是或否的问题，当不同的知识源的回答有冲突的时候，系统根据扩展的答案集的语义来提供不同的解决冲突的策略，当一个智能体表达出对某个策略的偏好时，该框架就能够推论出该智能体对不同策略偏好的排序。

语义网上的声望链式模型——RCSW 将成对的信任度因子和可靠度因子整合起来形成最终的信任评价。信任度因子是基于过去交互的经验，用来表明在某个智能体的眼中，另一个智能体完成某个任务或是提供某项服务的能力。而可靠度因子表明的是在信息传递的过程中，一个智能体认为其邻居智能体所提供的信息的准确度概率，智能体利用可靠度因子来决定采纳哪个节点的信息以及如何采纳。我们基于中医药的文献库定义了一个信任本体，该本体用 OWL 语言来描述并可以被机器所理解和自动处理。最后还介绍了 RCSW 模型在语义网上的推理功能并给出了相应的实例。

对于未来电子商务的发展，一些研究者也做了大胆的预测。在 2002 年，Ford 就预言在 2009 年 8 月 Google 将依靠语义网打败 Amazon 和 eBay 而成为世界上最大的独立在线交易市场。利用 RDF 来描述卖家要出售和买家要购买的商品，然后利用网络爬虫自动地搜索、分析并将匹配的买家和卖家联系起来，从而为用户提供一个巨大的交易平台。当然 Ford 也意识到单单把匿名的买家和卖家联系起来是远远不够的，因此他还提出了一个进行信誉评估的方法：借助于 Google 强大的搜索能力来穷尽所有的第三方认证和评价，哪怕某个卖家有一丁点儿的不诚实，Google 都可以让其暴露出来。虽然以目前语义网的研究和发展状况来看，在电子商务领域，距离 Google 彻底打败 Amazon 和 eBay 还有很长的一段距离，而且这个预言是否能够真正实现还是一个未知数，但是这仍然预示了电子商务未来一个新的发展方向，而 Ford 所提出的信任管理方法也给我们一个新的启迪。

6) 基于直接评价的分布式信任模型

基于信誉的信任机制能够有效解决 P2P 网络中病毒泛滥和欺诈行为等问题。现有信任机制大多采用单个信誉值描述节点的诚信度，不能防止恶意节点用诚信买行为掩盖恶意卖行为，而且从信誉值上无法区分初始节点和恶意节点。提出一种新的分布式信任机制基于交易历史，通过迭代求解，为每个节点计算全局买信誉值和卖信誉值，根据信誉值便能立断节点的善恶，能够迅速降低恶意节点的全局信誉值，抑制合谋攻击，降低恶意交易概率。

P2P技术因其自组织、开放性和匿名等特点成为新的网络应用热点。但是，随着P2P技术的广泛应用，原本不被重视的安全性问题逐渐成为阻碍其发展的主要因素。一种解决办法是引入基于信誉值的信任机制，它根据每个节点的网络行为动态计算其局部或全局信誉值，通过信誉值的高低判断节点的诚信度。因此，信任机制能够为节点选择交易对象提供参考依据，并激励节点诚信交易。集中式信任机制因为需要中心服务器而不适用于P2P应用，而分布式信任机制设计要解决如下两个问题：①如何衡量和计算信誉值；②如何存取和管理信誉值。

在多数现有信任机制中，信誉值只能用于比较节点间的相对诚信度，无法直接从信誉值上判断节点是否可信。事实上，很多应用需要直接从信誉值上判断节点的善恶，例如，在电子商务应用中，用户往往会选择信任值高于一定阈值的节点作为交易对象。另外，用户在网络中的交易行为分为买方和卖方。因此，仅用一个信誉值来衡量节点无法区分同一节点不同角色时的诚信度。因为恶意节点可以用诚信买行为来掩盖恶意卖行为，或者反之。

分布式信任机制由本地信誉评估和全局信誉计算与存取管理两部分组成。节点收集其他节点的信息并进行信誉评估，系统综合所有信誉评估计算各节点的全局信誉值并进行存取管理以保证其安全和有效性，用户结合本地信誉评估和全局信誉值，选择交易对象实施交易。

全局信誉值的分布式计算和管理需要考虑安全性和鲁棒性两个因素，防止节点破坏或窜改信誉值，并保证在动态的网络环境下不影响信誉值的计算和访问。采用DHT(distributed hash table)结构化网络能够有效解决安全性和鲁棒性问题。DHT网络在全局范围内分配和管理数据，能够防止在节点离开或失效时丢失数据。其存储内容和存储位置的确定关系、高效的查找和存取功能、较少的计算和通信开销以及匿名性等特点，使得它适用于作为全局信誉值计算和存储平台。

基于直接评价的分布式信任模型，利用历史交易数据，并采用分布式迭代方式为每个节点计算买全局信誉值和卖全局信誉值，便于用户判断交易对象的善恶，从而降低恶意交易概率。

7) 基于反馈可信度的分布式信任模型

由于网络中的节点不受约束，资源的共享是用户自愿的行为，节点间的信任很难通过传统的信任机制建立。一种可行的解决方案是借鉴人际网络中的信任关系，建立一种基于信誉的全局信任模型。已有的工作基本建立在信任度高的节点其反馈也更可信这个假设的基础上，将节点的反馈质量简单地等同于服务质量。针对这一问题，提出了一种基于节点反馈可信度的分布式全局信任模型(简称FCTrust)用于量化和评估节点的可信程度，并给出了模型的数学表述和分布式实现方法。FCTrust较已有的全局信任模型在遏制更广泛类型的恶意节点攻击的有效性、迭代计算的收敛性及消息成本上有较大提高。

目前，有关P2P的应用日益广泛，但仍然缺乏有效的信任机制提高系统整体的可用性，这非常显著地表现为应用中大量欺诈行为的存在以及不可靠的服务质量。以众多的文件共享应用为例，25%的文件是伪造文件(faked file)，同时，不负责任的用户随意地终止(文件上载)服务，使得服务质量无法得到较好的保证。

在传统的网络环境中，往往通过可靠的第三方(如认证中心CA)来建立信任关系，但这种集中式的信任机制并不适合于P2P网络，已有的工作显示，借鉴人际网络中的信任关系

建立有效的基于信誉的信任模型，能够有效地抑制节点资源滥用与欺诈等恶意行为。

目前存在的基于信誉的信任模型多数只将节点信任度作为服务选择的依据，即该类系统根据节点的历史交易反馈信息为节点计算信任等级。当存在多个可选服务时，信任等级高的节点成为首选，并且混淆节点“服务质量”与“反馈质量”的区别。这样做可以在一定程度上抑制节点的一般恶意行为，但在应付许多针对信任模型本身的一些攻击行为，如不诚实反馈、协同作弊及策略型攻击等恶意行为的过程中表现出来的有效性与健壮性仍然不够。除此之外，还存在信任模型迭代计算收敛成本与消息代价过高的问题。如果这些问题不能很好地解决，不仅会直接导致信任机制无法有效发挥作用，还会造成系统本身运行效率低下、管理上混乱的局面，进一步加重其他不良行为的影响，给系统的健康运行和良性发展带来诸多隐患。

将这些信任模型归纳起来可以分为两类，即依赖于第三方与不依赖于第三方的信任模型。前者的典型代表，如基于 PKI 的信任模型。这类系统中，有一个或一组权威节点维护一个可信的节点集合。这些权威节点可以颁发证书给可信的新加入的节点，节点以证书作为其身份的凭证使用网络中的资源，这类系统往往是中心依赖的，与 P2P 的分布式属性不相符合，存在单点失效问题。不依赖于可信第三方的信任模型主要有两类：基于微支付的模型和基于社会信任网络的模型。在基于微支付的模型中，节点接受服务需支付一定的虚拟货币，提供服务可以获得虚拟货币。然而，这需要一个完整的计费系统跟踪记录每一笔小额交易，因此不具有工程可行性。

由于这类方法并没有考虑节点反馈可信度的概念，因而不能很好地解决系统中节点的不诚实反馈、协同作弊等可信问题。相比较而言，由于 FCTrust 信任模型引入了该机制，充分考虑了节点间交互的频繁程度，使节点的信任评价更加精确。同时，利用节点间评分行为一致性评估机制能够有效识别并抑制更广泛类型的恶意节点的攻击行为，保障系统正常有序地运行。在遏制更广泛类型的恶意节点攻击的有效性、迭代计算的收敛性及消息成本上有较大提高。

8）基于政策的信任模型

基于政策的信任模型主要解决的问题是授权（authorization）和访问控制（access control），其目标是根据一组证书（credentials）和一组政策（policies）来决定一个陌生的用户是否应该被信任。在基于政策的信任管理中，信任的建立过程是通过获得一定数量的证书并通过采用一些政策来进行访问控制的。尽管证书这个术语在基于政策的信任模型中常常出现，但是直到现在还没有一个准确的定义，它往往用来指代一个关于实体的签署声明。例如当我们想要登录某个网上论坛时，一个合法的用户名和密码就是可以进入该论坛的证书。根据系统的政策，上述的信息是被论坛管理员所信任的，因此该用户被允许登录到系统中来。近年来，随着基于互联网的服务的广泛使用，用户个人资料（例如姓名、性别、电话、电子邮件等）被泄露的机会明显增加了。这些个人信息对于服务的访问控制是必需的，但是一旦泄露出去就可能会引起隐私相关方面的问题。为了解决这个问题，Bonatti 等人提出了一个在互联网上规范服务访问控制和个人资料泄露的方法，该方法包含一个统一正式的框架来阐明和推理服务的访问控制和用户信息的泄露，而且还提供了一个方法使得各方可以进行需求方面的通信而同时能够避免隐私的泄露。

4. 经典评估模型

1) EigenTrust 模型

全局信任计算评估模型是信任模型的核心，为获取全局的节点可信度，该类模型通过相邻节点间相互满意度的迭代，从而获取节点全局的信誉度。它为信任模型提供安全保证。它通过特定的信任度求解协议和信任度放置策略确保信任度量的准确性和高效性，减少恶意推荐的影响，并最终做出信任判定决策。

全局信任计算模型研究中最有代表性的就是 EigenTrust 模型。EigenTrust 根据节点交易历史的信誉，在 P2P 网络中计算一个类似 PageRank 的全局信任值，用户可以根据这个全局信任值来选择交易对象，从而规避恶意节点并将它们孤立起来，一个节点的全局信任值是根据信任网络中其他节点对它的局部信任值加权平均计算出来的，而权重就是这些节点本身的全局信任值。EigenTrust 认为直接信任值越高的节点推荐的信任值越可信，在计算全局信任时赋予较大权重。

EigenTrust 的核心思想是，当节点 i 需要了解任意节点 k 的全局信誉度时，首先从 k 的交互节点(曾经与 k 发生过交互的节点 j)获知节点 k 的信誉度信息，然后根据这些交互节点自身的局部可信度(从 i 的角度看来)综合出 k 的全局信誉度。即

$$T_{ik} = \sum_j (C_{ij} \cdot C_{jk}) \tag{3-2}$$

C_{ij} 为节点 i 对 j 的局部可信度，T_i 为节点 i 的全局信任度，其计算如下：

$$C_{ij} = \frac{\mathrm{Sat}_{ij} - \mathrm{UnSat}_{ij}}{\sum_j (\mathrm{Sat}_{ij} - \mathrm{UnSat}_{ij})} \tag{3-3}$$

Sat_{ij} 为 i 与 j 的历史交易中，i 对 j 的满意次数；UnSat_{ij} 为 i 对 j 的不满意次数。

算法实现如下：

$\vec{t}^{(0)} = \vec{e}$；

repeat

  $\vec{t}^{(k+1)} = \boldsymbol{C}^{\mathrm{T}} \vec{t}^{(k)}$；

  $\delta = \| t^{(k+1)} - t^k \|$；

until $\delta < e$；

算法中，$\boldsymbol{C}$ 为信任矩阵 $\vec{t}_i$ 为存储 t_{ik} 的向量。

因上述初始模型不能确保矩阵 $\boldsymbol{C}$ 迭代的收敛性，所以 EigenTrust 继而提出了网络初始时具有预可信节点集合 P 的假设前提。故式(3-2)变为

$$T_i^{(k+1)} = (1-a) \sum_j (C_{ij} \cdot C_{jk}) + a p_i \tag{3-4}$$

其中，$p_i = \begin{cases} \dfrac{1}{|P|} & i \in P \\ 0 & \text{否则} \end{cases}$，$|P|$ 为预可信节点集合 P 中的节点个数，常数 $a \in (0,1)$。

改进后的信任计算算法如下：

```
Each peer i do{
Query all peers j ∈ A_i for t_j^(0) = p_j;
Repeat
```

Compute $t_i^{(k+1)} = (1-a)(C_{1i}t_1^{(k)} + C_{2i}t_2^{(k)} + \cdots + C_nt_n^{(k)}) + ap_i$;
Send $C_{ij}t_i^{k+1}$ to all peers $j \in B_i$;
Compute $\delta = |t_i^{(k+1)} - t_i^{(k)}|$;
Wait for all peers $j \in A_i$ to return $C_{ji}t_j^{(k+1)}$;
Until $\delta < e$;
}

其中，A_i 为从 i 下载文件的申请者(买家)集合，B_i 为给节点 i 提供文件下载的资源拥有者集合(卖家)。

通过试验对比，EigenTrust 模型确实很好地抑制了虚假文件的下载量。实验结果见图 3-7。

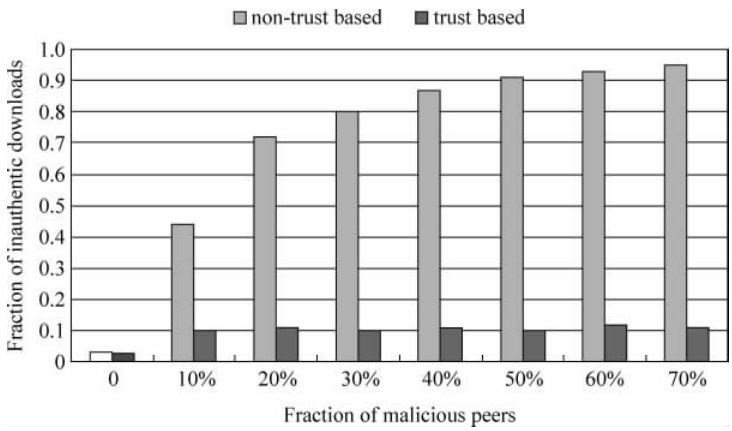

图 3-7 实验结果图

EigenTrust 的优点包括：①提出直接信任值越高的节点推荐的信任值越可信的思想；②算法和实现机制都考虑了恶意行为对算法的影响。缺点主要包括：①初始时需要设置一定数量的预可信节点。②没有对恶意节点的惩罚机制。③动态收集本地信任值并进行全局分布式迭代运算过程中的计算量大，增加了 P2P 网络的开销。尤其是网络规模很大时，迭代收敛明显缓慢。

2) PeerTrust 模型

PeerTrust 给出了一个适用于 P2P 电子社区的局部信任模型，节点的信任值仅由曾经与该节点交易过的一些节点计算，不需要全网络迭代计算。模型力图描述信任评价的全面性与合理性，提出了五个评价因子，包括：①交易评价因子(S)；②评价可信度因子(Cr)；③节点对外提供服务的总次数(I)；④与交易相关的因子(TF)，如交易时间、交易额度等；⑤与交易环境相关的因子(CF)，如社区对于提交评价反馈的节点提供奖励等。模型的数学描述如下：

$$T(u) = \alpha \sum_{i=1}^{I(u)} S(u,i) \cdot \mathrm{Cr}(p(u,i)) \cdot \mathrm{TF}(u,i) + \beta \cdot \mathrm{CF}(u) \tag{3-5}$$

其中 $I(u)$是节点 u 交易的数量，$p(u,i)$是第 i 次交易中与 u 进行交易的节点，$S(u,i)$是 $p(u,i)$在第 i 次交易后对 u 的评价，$\mathrm{Cr}(v)$是节点的可信度，$\mathrm{TF}(u,i)$是与节点 u 第 i 次交易相关的因素所产生的信任因子，$\mathrm{CF}(u)$是与节点 u 相关的交易环境所产生的信任因素，α 和 β 是标准化信任值时的权重参数，且 $\alpha+\beta=1$。模型系统图如图 3-8 所示。

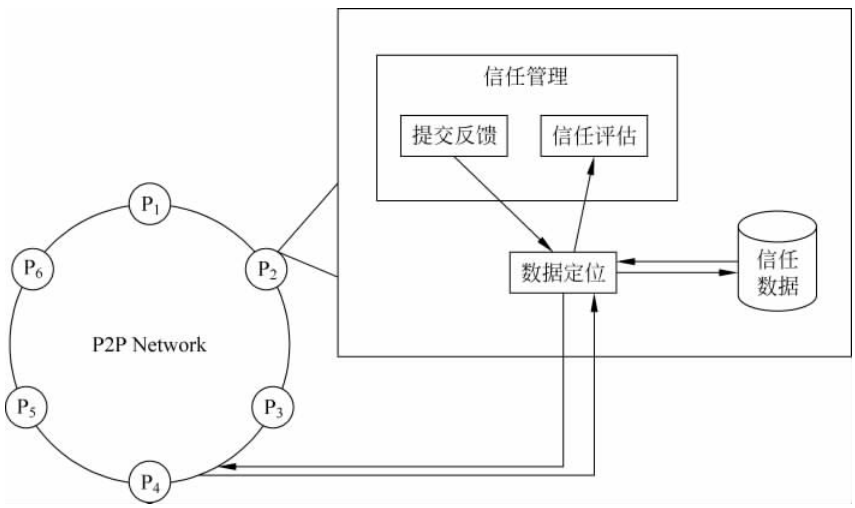

图 3-8 PeerTrust 的数学模型

PeerTrust 的数学模型中 S、I、TF 和 CF 四个因素均可由系统自动收集或确定性计算，只有 Cr 需要根据提交反馈节点过去行为来计算。Cr 求解的两种方法如下：

递归函数(TVM)法，即利用节点信任值作为计算 Cr(v)的依据，信任值越高的节点给出的评价越可信。

$$\mathrm{Cr}=\frac{T(p(u,i))}{\sum_{j=1}^{I(u)}T(p(u,j))} \tag{3-6}$$

个体相似度(PSM)法，即利用两个节点评价相同交易的相似性计算节点的评价可信度，两个节点评价越相似，则对方的评价信息越可信。

$$\mathrm{Cr}=\frac{\mathrm{Sim}(p(u,i),w)}{\sum_{j=1}^{I(u)}\mathrm{Sim}(p(u,j),w)} \tag{3-7}$$

$$\mathrm{Sim}(v,w)=1-\sqrt{\frac{\sum_{x\in US(v,w)}\left(\frac{\sum_{i=1}^{I(x,v)}S(x,i)}{I(x,v)}-\frac{\sum_{i=1}^{I(x,w)}S(x,i)}{I(x,w)}\right)^2}{|\mathrm{IJS}(v,w)|}} \tag{3-8}$$

PeerTrust 的优点有：①将评价因子进行归一化处理，能够抑制恶意节点提交过高或过低的评价。②求解信任值时考虑了交易额与数量，能够遏制恶意节点利用数量较多的小额交易掩盖它们在大额交易中的欺骗行为。③评价可信度降低了恶意节点提交的评价在信任值求解算法中所在的权重，从而抬高诚实节点的权重；由于恶意节点与正常节点间的评价相似度较低，模型依据评价相似度度量评价的可信度可以抵抗恶意节点的共谋攻击。④该模型还提出了基于自适应时间窗口的动态信任计算方法，即在每个计算周期中，分别在较大的时间窗口和较小的时间窗口里计算节点的信任值，取两者中较小者为最终信任值，从而抑制了节点的动态摇摆行为。⑤利用 PKI 基础设施和数据副本技术确保评价信息的安全性。

PeerTrust 模型也存在以下不足之处：①模型没有设计对节点恶意行为的惩罚机制；②没有考虑大规模 P2P 网络环境下信任值求解算法的收敛速度问题；③在大规模网络环境下，评价信息可能较为稀疏，利用相似度度量节点可信度会引起较大的误差。

3）PowerTrust 模型

PowerTrust 算法主要从三个方面对 EigenTrust 算法进行了改进：①合理确定可信节点集合；②加快迭代过程的收敛速度；③建立了动态适用机制。PowerTrust 模型如图 3-9 所示。

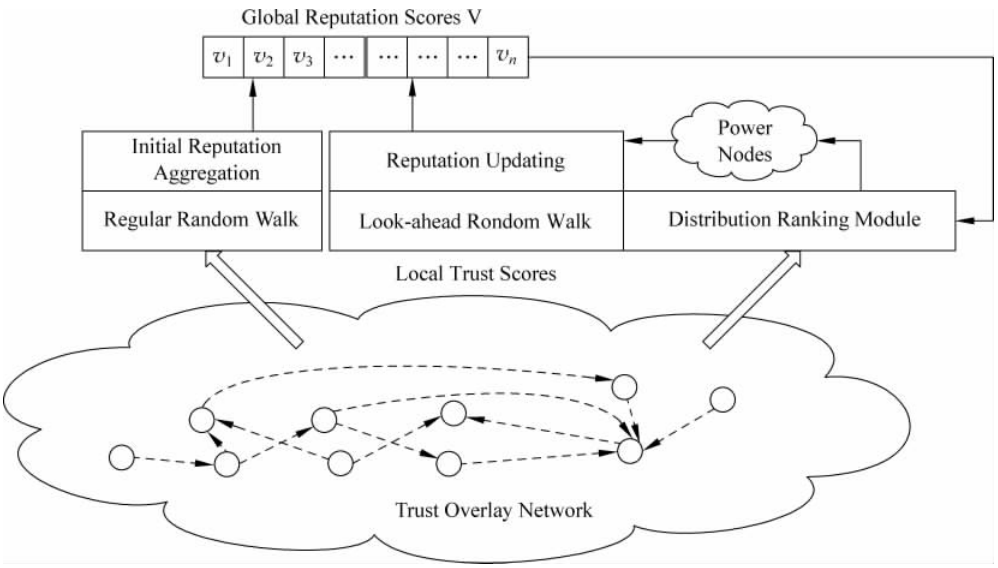

图 3-9　PowerTrust 的模型

首先在 TON 网络中根据节点间已知的局部信任值，利用 Regular Random Walk 策略初始化信任值聚合，计算节点 $V(v_1, v_2, \cdots, v_n)$ 的全局信任值。其次，利用分布式排序算法（Distributed Ranking Module）选取 PowerNodes。最后，根据选取的 PowerNodes 利用 LRW 策略迭代更新全局信任值。

（1）可信节点集的确定。通过分析 eBay 中 10 000 名用户的交易评价信息，发现 eBay 用户评价信息呈现幂律分布，即存在极少数用户做了大量的交易，它们得到的评价数量显著地多于其他用户。于是，PowerTrust 首先使用加权累计求和方法计算出每个节点的评价数量，再使用分布式排序算法将节点排序，便得到顶部的 m 个节点，称为 PowerNodes；然后，用这 m 个 PowerNodes 取代 EigenTrust 中的 P 集合。由于 PowerNodes 是动态计算的，而不是固定地指定的，符合 P2P 网络的实际情况，解决了 EigenTrust 模型预设高可信节点集在一些实际系统中缺乏可行性的问题。

某节点在经过 k 次随机抓取后成为 PowerNodes 的概率：

$$Q_d = 1 - \left(1 - \frac{d}{\sum_{i=1}^{n} d_i}\right)^k \tag{3-9}$$

其中，d_i 为节点 i 的反馈量，d 为 TON 网络图中节点的入度。TON 网络如图 3-10 所示。

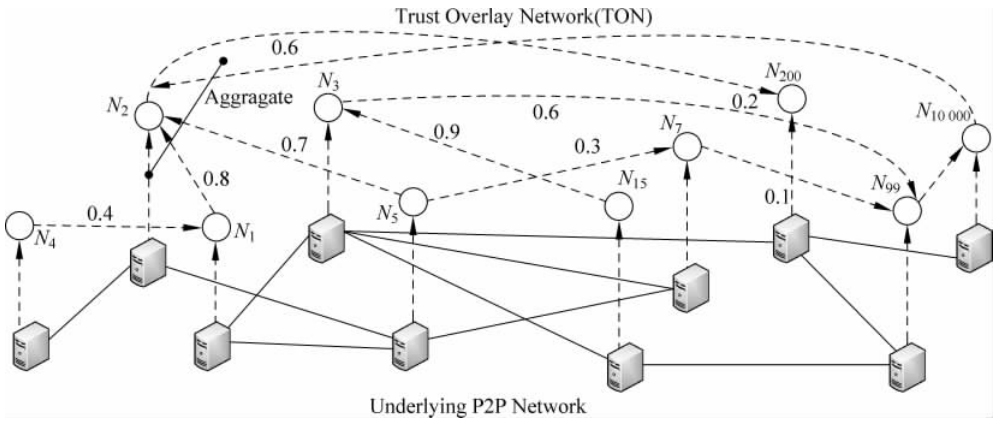

图 3-10 TON 网络

PowerNodes 选取算法：

```
Algorithm 1: Selection of top - m peers(Power nodes)
Input: global reputations stored among score managers
Output: m most reputable nodes
Procedure:
for each score manager j, suppose it is the score manager of
    node i do
    hash reputation value v_i to a hash value H(v_i) using a
    LPH function
    insert the triplet(v_i, i, j) to the successor node of H(v_i).
end for
initialize node x = successor node of the maximum
                hash value
Set p = the number of triplets with highest reputation values
    stored in node x
loop: if p > m then return;
          else
          node x sends a message to its predecessor
          node y to find the
          next m - p highest reputation triplets
          node x = node y
          m = m - p
          p = number of triplets stored in node y
            goto loop
    end if
```

(2) 迭代算法的收敛速度。在全局信任值求解过程中，PowerTrust 提出了一种向前看随机游走(look-ahead random walk, LRW)策略，迭代算法既考虑了节点邻居的推荐信任，也考虑了邻居的邻居的推荐信任，即信任矩阵 $\boldsymbol{R}=\boldsymbol{C}_2$。利用 LRW 策略使得迭代算法的收敛速度提高两倍多。

```
Algorithm 3: Global Reputation Updating Procedure
 Input:Local trust scores stored among nodes
 Output: Global reputation scores for all nodes for use by score
```

managers collaboratively to find
the m most reputable nodes using Algorithm 1
Procedure:
for each node i do
forall node j, which is an out－degree neighbor of node i
do
Aggregate local trust scores from node j
Send the score message (r_{ij}, i) to the score manager of node j
end forall
If node i is the score manager of node k, **then**
forall node j, which is an in－degree neighbor of node k
do
Receive the score message (r_{jk}, j) from node j
Locate the score manager of node j
end forall
Set a temporary variable $pre = 0$; initialize the error
threshold ε and *global* reputation v_k of *node* k
repeat
Initialize $pre = v_k$; $v_k = 0$
forall received score pair (r_{jk}, j), where j is an in－degree neighbor of node k **do**
if node k being a power node,
then $v_k = (1-\alpha)\sum(v_j \times r_{jk}) + \alpha/m$ j
else $v_k = (1-\alpha)\sum(v_j \times r_{jk})$
end if
compute $\delta = |v_k - pre|$, **until** $\delta < \varepsilon$
end if
end for

(3) 实现机制。PowerTrust 模型利用 DHT 机制和 LPH(locality preserving hasing)函数,实现动态发现 Power 节点的方法,使得模型能够适应节点的频繁加入和离开的动态环境。

PowerTrust 模型在安全机制方面类似于 EigenTrust 模型,但是它对恶意节点抵抗能力较 EigenTrust 模型强。原因是 PowerTrust 模型动态选举的 Power 节点集相对于 EigenTrust 模型中的预置可信节点集具有更高的可信度。PowerTrust 虽然在 EigenTrust 模型上做出了不少改进,但是该模型也存在一些缺点,包括:① PowerTrust 需要动态地计算 m 个 PowerNodes,增加了系统的计算量与通信量;②计算信任值时对交易额大小没有考虑,这容易使得恶意用户利用小额交易积累信任,而在大额交易上进行欺骗;③模型没有对恶意行为做出惩罚,恶意用户可采用多次正常交易掩盖其恶意行为。

第 3 章　课后习题

1. 请说明一般的交易步骤及其可能出现的安全问题。
2. 交易对象的选取需要考虑哪些因素?
3. 请说明虚假交易的表现形式和具体手段。
4. 买卖双方的欺诈行为在不同的电子商务模式下有什么不同的表现?

5. 简述网络钓鱼手段及其危害。
6. 商品质量评价指标分为哪几个层次？举例说明每层包含的具体内容。
7. 物流评价有哪些准则？
8. 交易过程评价包括哪些过程？请具体说明。
9. 消费者信息侵权类型包括哪些？现阶段提出了哪些保护措施？
10. 请说明隐私权的内涵，并阐述隐私权受侵犯的表现形式。
11. 请说明信任的含义及其基本特性。
12. 请举出影响商家和用户可信度的因素，写出电子商务服务指数公式。
13. 请简要说明信任建立过程中，卖家与买家、卖家与卖家、交易者和管理者之间的博弈。
14. 信任关系有哪些基本性质？
15. 常用的评估模型有哪些？并简要说明。
16. 请详细介绍一个经典评估模型。

参考文献

[1] 2013年中国网络购物市场研究报告.
[2] 周涛. 面向交易全过程的电子商务信任研究[M]. 武汉：华中科技大学，2007：148.
[3] 尹志洪. 我国的电子商务信任问题[J]. 电子商务，2012(4)：19-21.
[4] 宋光兴，杨德礼. 电子商务中的信任问题及信任建立途径[J]. 科技进步与对策，2004，21(11)：129-131.
[5] 王磊磊. 电子商务下的交易成本分析[J]. 北京市财贸管理干部学院学报，2001，17(4)：39-42.
[6] CNNIC分析师：安全网络交易环境建立刻不容缓[OL]. http：//tech. qq. com/a/20091203/000348. htm.
[7] 兰琦. B2C电子商务服务质量评价影响因素研究[M]. 成都：电子科技大学，2010：64.
[8] 淘宝虚假交易的认定和处罚的规则与实施细则[OL]. http：//rule. taobao. com/detail-113. htm.
[9] 年志君. C2C电子商务欺诈行为的防范方法研究[M]. 大连：辽宁师范大学，2011：41.
[10] 廖革元. 探析网络钓鱼对电子商务的威胁与对策[J]. 商场现代化，2006(11S)：111-112.
[11] 李卫忠. 商品质量的综合评价体系及方法研究[J]. 价值工程，2006(9)：67-70.
[12] 史秀苹，刘志英，关志民. 城市物流评价指标体系初探[J]. 冶金经济与管理，2004(4)：43-45.
[13] 张麟. B2C电子商务中消费者个人信息的法律保护研究[M]. 重庆：重庆大学，2012：48.
[14] 窦晓坤. 我国电子商务消费者的个人信息保护研究[M]. 济南：山东大学. 2012：41.
[15] 徐敬宏，文利民. 论电子商务消费者个人信息及其保护[J]. 图书情报工作，2009(8)：130-133.
[16] 李虹瑾. 电子商务中消费者个人信息隐私的法律保护[M]. 湘潭：湘潭大学，2011：70.
[17] 刘廷民. 电子商务交易过程中消费者隐私权的保护[J]. 企业经济，2011(11)：187-189.
[18] 刁塑. 新兴电子商务消费者隐私关注与采纳行为研究[M]，北京：北京邮电大学，2010：198.
[19] 刘蓓琳，王彤，丁日佳. 基于SET的在线支付持卡人隐私保护研究[J]. 矿冶，2007，16(1)：103-106.
[20] 孙萧寒，周碧英. 电子支付方式下的消费者隐私保护[J]. 电脑知识与技术，2009，5(30)：8404-8405.
[21] 罗旋. 中国C2C电子商务纠纷对交易评价结果的影响[J]. 重庆：重庆大学，2009：55.
[22] C2C电子商务纠纷对交易评价结果的影响[OL]. http：//eb. mofcom. gov. cn/aarticle/al/y/200910/20091006580527. html.
[23] 谷斌，钟建权. C2C电子商务中基于多影响因素的商家信任模型研究[J]. 科技管理研究，2012，32(20)：210-214.

[24] 龚炳铮.电子商务服务水平评价指标与方法探讨[D].第二届网商及电子商务生态学术研讨会论文集.
[25] 汤清,付阳.C2C 电子商务中的博弈论分析[J].特区经济,2006(6):233-234.
[26] 窦小雨,李秦.P2P 网络电子商务环境下信任的基本概念和相关理论分析[J].电脑编程技巧与维护,2010(14):65,66,72.
[27] Stephen M. Formalising Trust as a Computational Concept [D]. Scotland: University of Stirling,1994.
[28] Abdul-Rahman A,S Hailes. Supporting trust in virtual communities[J]. Systen Sciences,2000(1):9.
[29] 王海艳,陈建刚,王汝传.网格资源访问的一种主观信任机制[J].电子学报,2006,34(5):817-821.
[30] Golbeck J,J Hendler. Accuracy of metrics for inferring trust and reputation in semantic web-based social networks[M]. Berlin Heidelberg: Springer,2004:116-131.
[31] Ding L,L Zhou,T Finin. Trust based knowledge outsourcing for semantic Web agents [D]. Proceedings of the 2003 IEEE/WIC International Conference on Web Intelligence,2003:379-387.
[32] K J S,Y Zhang. Effects of hypertext links on trust transfer [D]. In Proceedings of the 5th international conference on Electronic commerce. ACM,2003:235-239.
[33] D K S, S M T,G H. The eigentrust algorithm for reputation management in p2p networks[D]. in Proceedings of the 12th international conference on World Wide Web. ACM,2003:640-651.
[34] Song S, et al. Trusted P2P transactions with fuzzy reputation aggregation [J]. IEEE Internet Computing, 2005,9(6):24-34.
[35] Zhou R,K Hwang. Gossip-based Reputation Aggregation for Unstructured Peer-to-Peer Networks, in Parallel and Distributed Processing Symposium;IPDPS 2007[J]. IEEE International,2007:1-10.
[36] D R S, S C,G L. Devising A trust model for multi-agent interactions using confidence and reputation [J]. Applied Artificial Intelligence, 2004,18(9-10):833-852.
[37] 李景涛,等.基于相似度加权推荐的 P2P 环境下的信任模型[J].软件学报,2007,18(1):157-167.
[38] Zacharia G, A Moukas, P Maes. Collaborative reputation mechanisms in electronic marketplaces. 1999:7.
[39] Gil Y, V Ratnakar. Trusting information sources one citizen at a time[M]. Berlin Heidelberg: Springer,2002:162-176.
[40] 李德毅,刘常昱.论正态云模型的普适性[J].中国工程科学,2004,6(8):28-34.
[41] Sabater J,C Sierra. Regret: A reputation model for gregarious societies[D]. In Fourth workshop on deception fraud and trust in agent societies,2001:70.
[42] Golbeck J,H J. Film Trust: movie recommendations using trust in Web-based social networks. 2006:282-286.
[43] Kautz H, B Selman. Referral Web: combining social networks and collaborative filtering [J]. Communications of the ACM, 1997,40(3):63-65.
[44] Berners-Lee T,J Hendler, O Lassila. The semantic web[J]. Scientific American, 2001,284(5):28-37.
[45] Heymans S, D Van-Nieuwenborgh,D Vermeir. Preferential reasoning on a web of trust[M]. Berlin Heidelberg: Springer,2005:368-382.
[46] 胡建理,等.一种基于反馈可信度的分布式 P2P 信任模型[J].软件学报,2009(10):2885-2898.
[47] Golle P, K Leyton-Brown,I Mironov. Incentives for Sharing in Peer-to-Peer Networks[M]. Berlin Heidelberg: Springer,2001:75-87.
[48] Bonatti P,P Samarati. Regulating service access and information release on the Web[D]. Proceedings of the 7th ACM conference on Computer and communications security. ACM, 2000:134-143.
[49] 李勇军,代亚非.对等网络信任机制研究[J].计算机学报,2010,33(3):390-405.
[50] 欧阳竟成.对等网络中信任模型与激励机制研究[M].湖南:湖南大学,2012:137.