网络营销管理

management on cybermarketing

熊 波 陈 柳 陶永勇 编著

中国电力出版社
www.cepp.com.cn

网络营销管理

熊波 陈柳 陶永勇 编著

中国电力出版社
www.cepp.com.cn

内 容 提 要

本书以如何开展网络营销为主线，将传统管理的思想和理念贯穿其中，从市场调研、广告、分销渠道、客户关系管理、定价等各方面详细地阐述了网络营销这一新的管理模式。

本书共分 10 章，包括电子商务概述、网络营销基础、网络营销概述、网络营销市场调研、网络营销产品与定价策略、网络营销的分销策略、网络营销广告策略、网络营销客户管理策略及案例分析。

本书力求以简洁易懂的语言向广大读者系统地阐述上述内容，具有较高的理论性、实践性和可操作性。

本书适用于各级经济管理部门的干部、企业的厂长（经理）、经营及管理人员，同时也适用于工厂技术人员及对网络营销感兴趣的一般读者。

图书在版编目（CIP）数据

网络营销管理/熊波，陈柳，陶永勇编著.-北京：中国电力出版社，2001

ISBN 7-5083-0570-1

Ⅰ.网… Ⅱ.①熊…②陈…③陶… Ⅲ.电子商务—市场营销学 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字（2001）第 12951 号

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://www.cepp.com.cn）

水利电力出版社印刷厂印刷

各地新华书店经售

*

2001 年 6 月第一版 2001 年 6 月北京第一次印刷

787 毫米×1092 毫米 16 开本 10 印张 220 千字

定价 **18.00** 元

前　言

飞速发展的国际互联网（Internet）促使网络技术应用呈指数级增长，在全球范围内掀起了应用互联网热，世界各大公司纷纷上网提供信息服务和拓展业务范围，积极改组企业内部结构和发展新的营销管理方法，抢搭这班世纪之车。21 世纪将是信息社会的时代，科技、经济和社会将随着计算机网络的发展、信息社会内涵的改变而发生较大的变化。在信息网络时代，网络技术的发展和应用不仅改变了信息的分配和接受方式，而且也改变了人们生活、工作、学习、合作和交流的环境，作为社会经济主体的企业也必须积极利用新的网络技术变革企业传统的经营理念、经营组织、经营方式和经营方法，从而促使企业飞速发展。从长远来看，电子商务是一个发展潜力巨大的市场，前景极好。它是互联网技术发展日益成熟的直接结果，也是网络技术发展的新方向。由于网络用户迅速膨胀，众多商家和厂商都纷纷将目光投向互联网，借助于传统贸易手段所不具备的电子商务交易，使之发展成能够在网上完成产、供、销全部业务流程的电子商务市场（这个市场是虚拟的），从而形成一种全新的市场营销策略。

随着传统经济向新经济的过渡，企业的观念、生产方式和经营方式都在发生深刻的变化。对任何一家企业来说，如何借助互联网有效地展开市场营销，寻觅和挖掘潜在的商机，扩大自己的市场，建立和确保其所处行业中的领先优势，已是一个迫切需要考虑的重要问题。

基于上述的思考，本书以如何开展网络营销为主线，将管理的思想和理念贯穿其中，从市场调研、广告、分销渠道、客户关系管理、定价等方面详细地阐述了网络营销。本书从理论与实际相结合的角度出发，力求以简洁易懂的语言，向读者系统地阐述网络营销的基本原理及策略与方法，具有较高的理论性、实践性和可操作性。

本书由中国科学技术大学研究生院（北京）管理学博士熊波、西南财经大学产业经济学博士陈柳和陶永勇编写。陶永勇负责编写 1 章和 2 章，陈柳负责编写 4、5、6、7 章和 8 章，熊波负责编写 3、9 章和 10 章，并负责全书总纂定稿。

本书作者在编写过程中参阅了国内外许多资料，广泛吸收了国内外同行的一些最新研究成果，并使用和引证了其中一部分资料，其中包括部分理论研究成果以及案例研究成果，由于篇幅所限，有些参考材料未能在参考文献中一一标出，作者在此特向有关作者、编者和出版社表示感谢。本书适用于各级经济管理部门的干部、企业的厂长（经理）、经营及管理人员等学习网络营销知识，同时也适用于 IT 技术人员和对网络营销感兴趣的一般读者业余学习之用。

由于作者水平有限，错误在所难免，恳请广大读者及同行不吝赐教，以便我们进一步修改、充实与完善。

编者

2000 年 10 月于北京

目　录

1 电子商务概述

以网络经济为代表的新经济，正不断地摧毁旧的商业模式与经济体系。电子商务作为网络经济的核心，凭借其高效率、无疆界、无时限和低成本等特点，受到了广泛重视，并获得飞速发展。电子商务已成为全球经济发展的最大推动力量之一。

1.1 电子商务的概念

一、电子商务的概念

电子商务源于英文 Electronic Commerce（或 E-Business），简写为 EC，最早由 IBM 公司提出，即在因特网的广阔联系与传统信息技术系统的丰富资源相互结合的背景下产生的一种在互联网上开展的相互关联的动态商务活动。电子商务有广义和狭义之分。狭义的电子商务称作电子交易，主要是指利用网络提供的通信手段在网上进行的交易。而广义的电子商务是包括电子交易在内的，利用互联网进行全面的商务活动，如市场调查分析、财务核算、生产组织等。

电子商务可以通过多种电子通信方式来完成。简单地讲，通过打电话或发传真来与客户进行商贸活动，似乎也可以称作电子商务；但是，现在人们所说的电子商务则主要是以 EDI（电子数据交换）和 Internet 来完成的。尤其是随着 Internet 技术的日益成熟，电子商务真正的发展将是建立在 Internet 技术上的。所以也有人把电子商务简称为 IC（Internet Commerce）。从贸易活动的角度分析，电子商务可以在多个环节实现，由此也可以将电子商务分为两个层次，较低层次的电子商务，如电子商情、电子贸易、电子合同等，最完整的也是最高级的电子商务应该能够利用 Internet 进行全部的贸易活动，即在网上将信息流、资金流和部分的物流完整地实现，也就是说，你可以从寻找客户开始，一直到洽谈、定货、在线付（收）款，开据电子发票以至电子报关、电子纳税等，通过 Internet 一气呵成。

二、电子商务的形式

从 1995 年仅 2 亿美元的全球网上销售额到 1998 年的 500 亿美元，电子商务的发展可谓日新月异。据迪洛伊特顾问公司最新预测，2002 年全球电子商务的总贸易额将达到 1.1 万亿美元，2005 年会增加到 10 万亿美元。从总体上看，电子商务主要可分为企业间的业

务和企业对消费者的业务等形式。

（1）企业与企业间（B to B）的业务是电子商务的主体。BtoB 是企业间利用互联网从事的商务活动，主要包括：

- 企业与其供应商之间采购物料的协调；
- 物料计划人员与仓储、运输其产品的公司间的业务协调；
- 销售机构与其产品批发商、零售商之间的信息与物流协调；
- 品牌推广，广告宣传；
- 在线销售；
- 客户服务，售后服务；
- 公司日常运营活动、内部员工的交流等。

（2）企业对消费者个人（B to C）的销售服务业务领域不断拓展。B to C 即公司对消费者的业务，主要包括两类：一是有形商品的电子订货和付款；二是无形商品和服务产品的销售，如计算机软件、娱乐产品、订票、信息服务等。

（3）其他电子商务形式不断涌现。随着电子商务的不断发展，目前在国内外又先后出现了消费者对消费（C to C），消费者对企业（C to B）等多种形式：

C to C 主要指网上拍卖市场，如国外的电子港湾（www.ebay.com），国内的雅宝（www.yabuy.com）、易趣（www.eachnet.com）。

C to B 主要指集体竞价模式，即由众多消费者购买同一商品，以获得最大折扣，如国内著名的网站酷必得（www.coolbid.com）。

三、电子商务的特征

（1）普遍性。电子商务作为一种新型的交易方式，将生产企业、流通企业以及消费者和政府带入了一个网络经济、数字化生存的新天地。

（2）方便性。在电子商务环境中，人们不再受地域的限制，客户能以非常简捷的方式完成过去较为繁杂的商务活动，如通过网络银行能够全天侯地存取资金账户、查询信息等，同时可以使得企业对客户的服务质量大大提高。

（3）整体性。电子商务能够规范事务处理的工作流程，将人工操作和电子信息处理集成为一个不可分割的整体，这样不仅能提高人力和物力的利用，也可以提高系统运行的严密性。

（4）安全性。在电子商务中，安全性是一个至关重要的核心问题，它要求网络能提供一种终端到终端的安全解决方案，如加密机制、签名机制、安全管理、存取控制、防火墙、防病毒保护等等。这与传统的商务活动有着很大的不同。

（5）协调性。商务活动本身是一种协调过程，它需要客户与公司内部、生产商、批发商、零售商间的协调。在电子商务环境中，它更要求银行、配送中心、通信部门、技术服务等多个部门的通力协作，因为电子商务的全过程是一气呵成的。

四、电子商务的安全要素

电子商务的安全要素主要包括以下几个方面。

（1）有效性。EC 以电子形式取代了纸张，那么如何保证这种电子形式贸易信息的有效性，则是开展 EC 的前提。EC 作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此，要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁，加以控制和预防，以保证贸易数据在确定的时刻、确定的地点是有效的。

（2）机密性。EC 作为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。EC 是建立在一个开放的网络环境（如 Internet）上的，维护商业机密是 EC 全面推广应用的重要保障，因此，要预防非法的信息存取和信息在传输过程中被非法窃取。

（3）完整性。EC 简化了贸易过程，减少了人为的干预，但同时也带来维护贸易各方商业信息的完整和统一的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、重复或传送的次序差异也会导致贸易各方信息的不同。由于贸易各方信息的完整性将影响到贸易各方的交易和经营策略，所以保持贸易各方信息的完整性是 EC 应用的基础。因此，不仅要预防对信息的随意生成、修改和删除，同时还要防止数据传送过程中信息的丢失和重复，并保证信息传送次序的统一。

（4）可靠性。EC 可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是进行交易所期望的贸易方，这是保证 EC 顺利进行的关键。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。这也就是人们常说的“白纸黑字”。而在无纸化的 EC 方式下，通过手写签名和印章来进行贸易方的鉴别已不可能，因此，要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。

五、电子商务的安全技术

为了满足电子商务的安全要求，EC 系统必须利用安全技术为 EC 活动参与者提供可靠的安全服务，主要包括：鉴别服务、访问控制服务、机密性服务、不可否认服务等。鉴别服务是对贸易方的身份进行鉴别，为身份的真实性提供保证；访问控制服务通过授权对使用资源的方式进行控制，防止非授权使用资源或控制资源，有助于贸易信息的机密性、完整性和可控性；机密性服务为 EC 参与者在存储、处理和传输信息过程中提供机密性保证，防止信息被泄露给非授权信息获得者；不可否认服务针对对合法用户的威胁，为交易的双方提供不可否认的证据，为解决因否认而产生的争议提供支持。

各种 EC 安全服务都是通过安全技术来实现的，EC 使用的主要安全技术包括：加密、数字签名、电子证书、电子信封和双重签名等。

（1）加密技术。加密技术是 EC 采取的基本安全措施，贸易方可根据需要在信息交换的阶段使用。加密技术分为两类，即对称加密和非对称加密。

在对称加密方法中，采用相同的加密算法并只交换共享的专用密钥（加密和解密都使用相同的密钥）。如果进行通信的贸易方能够确保专用密钥在密钥交换阶段未曾泄露，那么机密性和报文完整性就可以通过这种加密方法加密机密信息和通过随报文一起发送报文摘要或报文散列值来实现。因此，对称加密技术存在着在通信的贸易方之间确保密钥安全交换的问题。此外，对称加密方式无法鉴别贸易发起方或贸易最终方。数据加密标准（DES）由美国国家标准局提出，是目前广泛采用的对称加密算法，主要应用于银行业中的 EFT 领域。

在非对称加密体系中，密钥被分解为一对，即公开密钥或专用密钥。公开密钥（加密密钥）通过非保密方式向他人公开，而专用密钥（解密密钥）加以保存。公开密钥用于对机密性的加密，专用密钥则用于对加密信息的解密。专用密钥只能由生成密钥对的贸易方掌握，公开密钥可广泛发布，但它只对应于生成该密钥的贸易方。贸易甲方生成一对密钥，公布公开密钥；贸易乙方得到该公开密钥，使用该密钥对机密信息进行加密，然后发送给贸易甲方；贸易甲方再用自己保存的专用密钥对加密后的信息进行解密。贸易方只能用其专用密钥解密由其公开密钥加密后的任何信息。RSA 算法是非对称加密领域内最为著名的算法。

（2）数字签名。数字签名是非对称加密技术的一类应用。它的主要方式是：报文发送方从报文文本中生成一个 128 位的散列值（或报文摘要），并用自己的专用密钥对这个散列值进行加密，形成发送方的数字签名。然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文接收方首先从接收到的原始报文中计算出 128 位的散列值（或报文摘要），接着再用发送方的公开密钥来对报文附加的数字签名进行解密。如果两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别和不可否认性。

ISO/IEC JTC1（国际标准化组织/国际电子商会）已经起草了有关的国际标准规范，该标准的题目是“信息技术安全技术带附件的数字签名方案”，它由概述和基于身份的机制两部分构成。

（3）电子证书。数字签名是基于非对称加密技术的，存在两个明显的问题：第一，如何保证公开密钥的持有者是真实的；第二，大规模网络环境下公开密钥的产生、分发和管理。由此，证书签发机构（CA,Certificate Authority）应运而生，它是提供身份验证的第三方机构，由一个或多个用户信任的组织实体构成。CA 核实某个用户的真实身份以后，签发一份报文给该用户，以此作为网上证明身份的依据，这个报文称为电子证书。包括：唯一标识证书所有者（即贸易方）的名称、唯一标识证书签发者的名称、证书所有者的公开密钥、证书签发者的数字签名、证书的有效期及证书的序列号等。电子证书能够起到标识贸

易方的作用，是目前 EC 广泛采用的技术之一。常用的证书有：持卡人证书、商家证书、支付网关证书、银行证书和发卡机构证书等。微软公司的 Internet Explorer 和网景公司的 Navigator 都提供了电子证书的功能，以此作为身份鉴别的手段。

（4）电子信封。电子信封是为了解决传送更换密钥问题而产生的技术，它结合了对称加密和非对称加密技术的各自优点。发送者使用随机产生的对称密钥加密数据，然后将生成的密文和密钥本身一起用接收者的公开密钥加密（称为电子信封）并发送。接收者先用自己的专用密钥解密电子信封，得到对称密钥，然后使用对称密钥解密数据。这样，保证每次传送数据都可有发送方选定不同的对称密钥。

（5）双重签名。在实际商务活动中经常出现这种情形，即持卡人给商家发送订购信息和自己的付款账户信息，但不愿让商家看到自己的付款账户信息，也不愿让处理商家付款信息的第三方看到定货信息。在 EC 中要能做到这点，需使用双重签名技术。持卡人将发给商家的信息（报文 1）和发给第三方的信息（报文 2），分别生成报文摘要 1 和报文摘要 2，合在一起生成报文摘要 3，并签名。然后，将报文 1、报文摘要 2 和报文摘要 3 发送给商家，将报文 2、报文摘要 1 和报文摘要 3 发送给第三方。接收者根据收到的报文生成报文摘要，再与收到的报文摘要合在一起，比较结合后的报文摘要和收到的报文摘要 3，确定持卡人的身份和信息是否被修改过。双重签名解决了三方参加电子贸易过程中的安全通信问题。

六、公开密钥框架

与 DNS 和 X.500 类似，公开密钥框架（PKI,Public Key Infrastructure）也是一种网络基础设施，其目标是向网络用户和应用程序提供公开密钥的管理服务。为了使用户在不可靠的网络环境中获得真实的公开密钥，PKI 引入公认可信的第三方，同时避免在线查询集中存放的公开密钥产生的性能瓶颈，PKI 引入电子证书。可信的第三方是 PKI 的核心部件，正是由于它的中继，系统中任意两个实体才能建立安全联系。

电子证书中第三方的数字签名，使用户可以离线确认一个公开密钥的真实性。当证书中认可的事实发生变化时，证书发布者必须使用某种机制来撤销以前发出、现在失效的证书。除了证书的有效期外，证书撤销列表（CRL）是另一种证书有效期控制机制。证书发布者定期发布 CRL，列出所有曾发布但当前已被撤销的证书号，证书的使用者依据 CRL 即可验证某证书是否已被撤销。

（一）PKI 结构模型

PKI 框架有三类实体：管理实体、端实体和证书库。管理实体是 PKI 的核心，是 PKI 服务的提供者；端实体是 PKI 的用户，是 PKI 服务的使用者、证书库是一个分布式数据库，用于证书或 CRL 存放和检索。

证书签发机构（CA）和注册机构（RA）是两种管理实体。CA 是 PKI 框架中唯一能够发布、撤销证书的实体，维护证书的生命周期；RA 负责处理用户请求，在验证了请求的有

效性后，代替用户向 CA 提交。RA 可以单独实现，也可以合并在 CA 中实现。作为管理实体，CA/RA 以证书方式向端实体提供公开密钥的分发服务。

持有者和验证者是两种端实体。持有者是证书的拥有者，是证书所声明事实的主体。持有者向管理实体申请并获得证书，也可以在需要时请求撤销或更新证书。持有者使用证书鉴别自己的身份，从而获得相应的权力。验证者通常是授权方，确认持有者所提供的证书的有效性和对方是否为该证书的真正拥有者，只有在成功鉴别之后才可授权对方。

证书库可有 WEB、FTP 或 X.500 目录来实现。由于证书库中存取对象是证书和 CRL，其完整性由数字签名保证，因此对证书库的操作可在无特殊安全保护的信道上传输。

不同的实体间通过 PKI 操作完成证书的请求、确认、发布、撤销、更新和获取等过程。PKI 操作分成存取操作和管理操作两类。前者涉及管理实体（端实体）与证书库之间的交互，操作的目的是从证书库存放或读取证书和 CRL，后者涉及管理实体与端实体之间或管理实体内部的交互，操作的目的是完成证书的各项管理任务和建立证书链。

（二）PKI 层次模型

PKI 框架描述为三个层次。最低层是传输层，向上提供 PKI 操作报文的可靠传输，可以是运输层协议（如 TCP）或应用层协议（如 HTTP、SMTP、FTP）。中间层是密码学服务层，向上提供加解密、数字签名和报文摘要等基本密码学服务，可由 RSA、MD5 和智能卡接口等模块实现。最高层是证书服务层，使用下两层提供的加密和传输服务，向用户提供证书的请求、签证、发布、撤销和更新等服务。

PKI 的三类实体使用了三层服务。证书库无需特殊的安全交互措施，所以仅使用传输层服务分发证书和 CRL。管理实体和端实体使用证书服务层构造 PKI 证书操作报文，使用密码学服务层作鉴别和保护交互信息，使用传输层服务传送报文。

（三）X.509 证书

ISO/ITU、ANSI、IETF 等组织制定的标准 X.509，对电子证书进行了定义，对 X.509 证书和 CRL 做了标准化工作，不同组织定义的证书格式并不完全相同。X.509 证书适用于大规模网络环境，它的灵活性和扩展性能够满足各种应用系统不同类型的安全要求。X.509 证书具有如下 5 个方面的特性：

（1）支持多种算法。X.509 证书独立于算法，CA 根据需要选择证书的签名和摘要算法，以及端实体所拥有密钥对的类型。摘要算法有 MD2、MD5 和 SHA－1，证书签名算法有 RSA 和 DSA，密钥对类型有 RSA 密钥、DSA 签名密钥、D－H 密钥交换密钥、KEA 密钥和 ECDSA 密钥。

（2）支持多种命名机制。X.509 证书除了使用 X.500 名字机制标识持证者和验证者，还支持 E_mail 地址、IP 地址、DNS 名和 URI。

（3）限制证书（公开密钥）的用途。CA 能够规定证书的使用范围，如签名、不可否认、密钥加密、数据加密、密钥协商、证书签发和 CRL 签发等。

（4）定义证书遵循的策略。每个 CA 都定义了一定的安全策略，规范证书的操作过程。这些策略包括：CA 的命名空间、身份验证、撤销机制、法律责任和收费等。

（5）控制信任关系的传递。建立 CA 体系，跨域认证，使得每个 CA 除负责本域的证书管理任务外，还要维护与其他 CA 间的信任关系。X.509 证书定义若干字段用于控制信任关系的传递，CA 能够将自己管理域的安全策略体现在信任关系中。

七、安全电子交易

安全电子交易（SET,Secure Electronic Transaction）是一个通过开放网络（包括 Internet）进行安全资金支付的技术标准，由 VISA 和 MasterCard 组织共同制定，1997 年 5 月联合推出。由于它得到了 IBM、HP、Microsoft、Netscape、VeriFone、GTE、Terisa 和 VeriSign 等很多大公司的支持，已成为事实上的工业标准，目前已获得 IETF 标准的认可。

SET 向基于信用卡进行电子化交易的应用提供了实现安全措施的规则。SET 主要由 3 个文件组成，分别是 SET 业务描述、SET 程序员指南和 SET 协议描述。SET 规范涉及的范围：加密算法的应用（例如 RSA 和 DES）；证书信息和对象格式；购买信息和对象格式；确认信息和对象格式；划账信息和对象格式；对话实体之间消息的传输协议。SET 1.0 版已经公布并可应用于任何银行支付服务。

SET 主要目标如下：信息在 Internet 上安全传输，保证网上传输的数据不被黑客窃取；隔离订单信息和个人账号信息，当包含持卡人账号信息的订单送到商家时，商家只能看到订货信息，而看不到持卡人的账户信息；持卡人和商家相互认证，以确定通信双方的身份，一般由第三方机构负责为在线通信双方提供信用担保；要求软件遵循相同协议和报文格式，使不同厂家开发的软件具有兼容和互操作功能，并且可以运行在不同的硬件和操作系统平台上。

（一）SET 的购物流程

电子商务的工作流程与实际的购物流程非常接近，使得电子商务与传统商务可以很容易融合，用户使用也没有什么障碍。从顾客通过浏览器进入在线商店开始，一直到所订货物送货上门或所定服务完成，以及账户上的资金转移，所有这些都是通过公共网络（Internet）完成的。如何保证网上传输数据的安全和交易对方的身份确认，是电子商务能否得到推广的关键，这正是 SET 所要解决的最主要的问题。一个包括完整的购物处理流程的 SET 的工作过程：

（1）持卡人使用浏览器在商家的 WEB 主页上查看在线商品目录，浏览商品。

（2）持卡人选择要购买的商品。

（3）持卡人填写订单，包括项目列表、价格、总价、运费、搬运费、税费。订单可通过电子化方式从商家传过来，或由持卡人的电子购物软件建立。有些在线商场可以让持卡人与商家协商物品的价格（例如出示自己是老客户的证明，或给出竞争对手的价格信息）。

（4）持卡人选择付款方式，此时 SET 开始介入。

（5）持卡人发送给商家一个完整的订单及要求付款的指令。在 SET 中，订单和付款指令由持卡人进行数字签名，同时利用双重签名技术保证商家看不到持卡人的账号信息。

（6）商家收到订单后，向持卡人的金融机构请求支付认可。通过支付网关到银行，再到发卡机构确认，批准交易，然后返回确认信息给商家。

（7）商家发送订单确认信息给顾客。顾客端软件可记录交易日志，以备将来查询。

（8）商家给顾客装运货物，或完成订购的服务。到此为止，一个购买过程已经结束。商家可以立即请求银行将钱从购物者的账号转移到商家账号，也可以等到某一时间，请求成批划账处理。

（9）商家从持卡人的金融机构请求支付。在认证操作和支付操作中间一般会有一个时间间隔，例如在每天的下班前请求银行结一天的账。

前三步与 SET 无关，从第 4 步开始 SET 起作用，一直到第 9 步。在处理过程中，通信协议、请求信息的格式、数据类型的定义等，SET 都有明确的规定。在操作的每一步，持卡人、商家和支付网关都通过 CA 来验证通信主体的身份，以确保通信的对方不是冒名顶替。

（二）SET 的认证

（1）证书。SET 中主要的证书是持卡人证书和商家证书。持卡人证书是支付卡的一种电子化的表示。持卡人证书不包括账号和终止日期信息，而是用单向哈希算法根据账号和截止日期生成的一个码，如果知道账号、截止日期、密码值即可导出这个码值，反之不行。商家证书就像是贴在商家收款台小窗上的付款卡贴画，以表示它可以用什么卡来结算。在 SET 环境中，一个商家至少应有一对证书，与一个银行打交道。一个商家也可以有多对证书，表示它与多个银行有合作关系，可以接受多种付款方法。除了持卡人证书和商家证书以外，还有支付网关证书、银行证书、发卡机构证书。

（2）CA。持卡人可从公开媒体上获得商家的公开密钥，但持卡人无法确定商家是否冒充（有信誉），于是持卡人请求 CA 对商家认证。CA 对商家进行调查、验证和鉴别后，将包含商家公开密钥的证书经过数字签名传给持卡人。同样，商家也可对持卡人进行验证。CA 的主要功能包括：接收注册请求，处理、批准/拒绝请求，颁发证书。在实际运作中，CA 也可由大家都信任的一方担当，例如在客户、商家、银行三角关系中，客户使用的是由某个银行发的卡，而商家又与此银行有业务关系（有账号）。在此情况下，客户和商家都信任该银行，可由该银行担当 CA 角色，接收、处理客户证书和商家证书的验证请求。又例如，对商家自己发行的购物卡，则可由商家自己担当 CA 角色。

（3）证书的树形验证结构。在双方通信时，通过出示由某个 CA 签发的证书来证明自己的身份，如果对签发证书的 CA 本身不信任，则可验证 CA 的身份，依次类推，一直到公认的权威 CA 处，就可确信证书的有效性。每一个证书与签发证书的实体的签名证书关联。SET 证书正是通过信任层次来逐级验证的。例如，C 的证书是由 B 的 CA 签发的，而

B 的证书又是由 A 的 CA 签发的，A 是权威的机构，通常称为根 CA。验证到了根 CA 处，就可确信 C 的证书是合法的。

在网上购物实现中，持卡人的证书与发卡机构的证书关联，而发卡机构证书通过不同品牌卡的证书连接到根 CA，而根的公开密钥对所有的 SET 软件都是已知的，可以校验每一个证书。

关于安全电子交易的详细内容，读者可参见中国电力出版社出版的《电子商务安全与保密》一书。

八、防火墙技术

网络防火墙技术是一种用来加强网络之间访问控制，防止外部网络用户以非法手段进入内部网络、访问内部网络资源，保护内部网络操作环境的特殊网络互联设备。它对两个或多个网络之间传输的数据包，按照一定的安全策略来实施检查，决定网络之间通信的权限，并监视网络的运行状态。防火墙系统的实现技术主要分为分组过滤（Packet Filter）和代理服务（Proxy Service）两种。

分组过滤技术是一种基于路由器的技术，由分组过滤路由器对 IP 分组进行选择，允许或拒绝特定的分组通过。过滤一般是基于一个 IP 分组的有关域（IP 源地址、IP 目的地址、TCP/UDP 源端口或服务类型和 TCP/UDP 目的端口或服务类型）进行的。基于 IP 源/目的地址的过滤，即根据特定组织机构的网络安全规则，过滤掉具有特定 IP 地址的分组，从而保护内部网络；基于 TCP/UDP 源/目的端口的过滤，因为端口号区分了不同的服务类型或连接类型（如 SMTP 使用端口 25，Telnet 使用端口 23 等），所以为分组过滤提供了更大的灵活性。通过防火墙系统中分组过滤路由器对特定端口 IP 分组的禁止，可以防止黑客利用不安全的服务对内部网络进行攻击。

代理服务技术由一个高层的应用网关作为代理服务器，接受外来的应用连接请求，进行安全检查后，再与被保护的网络应用服务器连接，使得外部服务用户可以在受控制的前提下使用内部网络的服务。同样，内部网络到外部的服务连接也可以受到监控。应用网关的代理服务实体将对所有通过它的连接作出日志记录，以便检查安全漏洞和收集相关的信息。使用应用网关的高层代理服务实体有以下的优点：隐蔽信息，内部受保护子网的主机名称等信息不为外部所知；日志记录，便于网络安全管理；可以由应用网关代理有关 RPC 的服务，进行安全控制。

目前，比较完善的防火墙系统通常结合使用两种技术。代理服务可以大大降低分组过滤规则的复杂度，是分组过滤技术的重要补充。这里介绍一种基于网络地址转换（NAT,Network Address Translator）的复合型防火墙系统，该系统是我们在国家 863 课题支持下自行研究和开发的。

（一）总体思想

代理技术造成性能下降的主要原因在于其在指定的应用服务中，传输的每一个报文都

需代理主机转发，应用层的处理量过于繁重，改变这一状况的最理想的方案是让应用层仅处理用户身份鉴别的工作，而网络报文的转发由 TCP 层或 IP 层来完成。另一方面，包过滤技术仅仅是根据 IP 包中源及目的地址来判定一个包是否可以通过，而这两个地址是很容易被篡改和伪造的，一旦网络的结构暴露给外界后，就很难抵御 IP 层的攻击行为。集中访问控制技术是在服务请求时由网关负责鉴别，一旦鉴别成功，其后的报文交互都直接通过 TCP/IP 层的过滤规则，无需像应用层代理那样逐个报文转发，这就实现了与代理方式同样的安全水平而处理量大幅下降，性能随即得到大大提高。另一方面，NAT 技术通过在网关上对进出 IP 包源与目的地址的转换，实现过滤规则的动态化。这样，由于 IP 层将内部网与外部网隔离开，使得内部网的拓扑结构、域名以及地址信息对外成为不可见或不确定信息，从而保证了内部网中主机的隐蔽性，使绝大多数攻击性的试探失去所需的网络条件。

（二）系统设计

本防火墙系统的总体结构模型由以下 5 大模块组成：

（1）NAT 模块依据一定的规则，对所有出入的数据包进行源与目的地址识别，并将由内向外的数据包中源地址替换成一个真实地址，而将由外向内的数据包中的目的地址替换成相应的虚拟地址。

（2）集中访问控制（CAC）模块负责响应所有指定的由外向内的服务访问，并实施安全的鉴别，为合法用户建立相应的连接，并将这一连接的相关信息传递给 NAT 模块，保证在后续的报文传输时直接转发而无需控制模块干预。

（3）临时访问端口表及连接控制（TLTC）模块通过监视外向型连接的端口数据动态维护一张临时端口表，记录所有由内向外连接的源与目的端口信息，根据此表及预先配置好的协议集由连接控制模块决定哪些连接是允许的而哪些是不允许的，即根据所制定的规则（安全政策）禁止相应的由外向内发起的连接，以防止攻击者利用网关允许的由内向外的访问协议类型做反向的连接访问。由于本模块所实现的功能实际上仍属于 IP 包过滤的范畴，因此，它有可能与 NAT 模块所设定的过滤规则相冲突。基于这一原因，在系统总体设计中，本模块属于可选部分，将在实际操作时根据需要来安装或激活。

（4）Interior DNS 和 Exterior DNS 分别为 NAT 模块机能所需的 Split－DNS 系统中的内部域名服务器和外部域名服务器（DNS），是 NAT 网关不可缺少的辅助部分。Split－DNS 系统的主要目的在于解决由于 NAT 模块对内外部网的地址屏蔽所造成的内外部域名解析不一致的问题。内部网的域名解析由 Interior DNS 负责，外部网针对内部网的域名解析由 Exterior DNS 负责，两者间的数据同步通过内部通信机制完成。

（三）模块功能

（1）NAT 模块。NAT 模块是本系统的核心部分，而且只有本模块与网络层有关，因此，这一部分应和 Unix 系统本身的网络层处理部分紧密结合在一起，或对其直接进行修改。本模块进一步可细分为包交换子模块、数据包头替换子模块、规则处理子模块、连接记录子

模块与真实地址分配子模块及传输层过滤子模块。

（2）CAC 模块。集中访问控制模块可进一步细分为用户鉴别子模块和连接中继子模块及用户数据库。用户鉴别子模块主要负责与客户通过一种可信的安全机制交换各种身份鉴别信息，根据内部的用户数据库，识别出合法的用户，并根据用户预先被赋予的权限决定后续的连接形式。

连接中继子模块的主要功能是为用户建立起一条最终的无中继的连接通道，并在需要的情况下向内部服务器传送鉴别过的用户身份信息，以完成相关服务协议中所需的鉴别流程。

（3）SPLIT DNS 系统。内部、外部 DNS 模块可以利用现有的 DNS 服务程序，如 BIND（Berkley Internet Name Domain）软件包，通过与 NAT 模块不断交互，维持域名与地址对应关系的同步、维护两个动态的内部 DNS 数据库和外部 DNS 数据库来实现，既达到了总体的设计目标，又保持了对其他服务的透明性。

九、电子商务对社会的影响

随着电子商务魅力的日渐显露，虚拟企业、虚拟银行、网络营销、网上购物、网上支付、网络广告等一大批前所未闻的新词汇正在为人们所熟悉和认同，这些词汇同时也从另一个侧面反映了电子商务正在对社会和经济产生的影响。

（1）电子商务将改变商务活动的方式。传统的商务活动最典型的情景就是“推销员满天飞”“采购员遍地跑”，“说破了嘴、跑断了腿”，消费者在商场中筋疲力尽地寻找自己所需要的商品。现在，通过互联网只要动动手就可以了，人们可以进入网上商场浏览，采购各类产品，而且还能得到在线服务，商家们可以在网上与客户联系，利用网络进行货款结算服务，政府还可以方便地进行电子招标、政府采购等。

（2）电子商务将改变人们的消费方式。网上购物的最大特征是消费者的主导性，购物意愿掌握在消费者手中，同时消费者还能以一种轻松自由的自我服务的方式来完成交易，消费者主权可以在网络购物中充分体现出来。

（3）电子商务将改变企业的生产方式。由于电子商务是一种快捷、方便的购物手段，消费者的个性化、特殊化需要可以完全通过网络展示在生产厂商面前。为了取悦顾客，突出产品的设计风格，制造业中的许多企业纷纷发展和普及电子商务，如美国福特汽车公司在 1998 年的 3 月份将分布在全世界的 12 万个电脑工作站与公司的内部网连接起来，并将全世界的 1.5 万个经销商纳入内部网。福特公司的最终目的是实现能够按照用户的不同要求按需供应汽车。

（4）电子商务将给传统行业带来一场革命。电子商务是在商务活动的全过程中，通过人与电子通信方式的结合，极大地提高商务活动的效率，减少不必要的中间环节，传统的制造业籍此进入小批量、多品种的时代，“零库存”成为可能。传统的零售业和批发业开创了“无店铺”“网上营销”的新模式，各种线上服务为传统服务业提供了全新的服务方式。