因特网商务解决方案

[美] G. Winfield Treese 著
Lawrence C. Stewart
邱仲潘 等译

Designing Systems for Internet Commerce

電子工業出版社
Publishing House of Electronics Industry
www.phei.com.cn

Addison-Wesley

因特网商务解决方案

Designing Systems for Internet Commerce

[美] G. Winfield Tresse Lawrence C. Stewart 著

邱仲潘等译

電子工業出版社
Publishing House of Electronics Industry
北京 · Beijing

特网都能使你的商业合作与交易效率高得多 ”。

本书的翻译得到“ 韩素英翻译奖 ”得主张一麟先生帮助，使许多文学性较强的部分文采增色不少。在本书翻译过程中还得到了周阳生、刘文红、邹能东、彭振庆、黄志坚、李耀平、江文清等同志的大力帮助，刘文琼、温连英等同志完成了本书的录入工作，刘云昌、刘联昌二人帮助进行了书稿与打印稿的校对，在此深表感谢。

原著序

1994年，《经济学家》杂志把因特网对世界的长远冲击作用排在电话与印刷机之间。正如其余改变了社会的发明创造，因特网也开始了一个新的社会变革，这个正在发生的变革速度之快远远超出了早先的革命。当然，商场就是一个竞技场，这个竞技场已经领略到因特网所产生的作用。近几年来，我们发现某些行业发生了引人注目的变化，涌现了许多新行业，它们对别的行业产生了重大影响。

19世纪，铁路这一快速运输方式的兴起从根本上改变了商业贸易；20世纪末，因特网将使21世纪的商业贸易发生根本性变化。我们正处在这一变革的初始阶段，技术创新促成了这一变革，提供了新的无限商机。技术创新层出不穷，日新月异。新的市场出现在我们面前，旧的市场不断变化，或者完全消失。短期的技术创新与市场变化固然重要，然而它们所起的作用必须与长期的商业前景相吻合。挑战就是有效地利用技术创新来达到商业目标。

本书的对象为所谓的“因特网商务一族”，其中包括经营和技术的管理阶层，还包括制定公司发展战略的决策层和实施这一战略的实践阶层。换句话说，因特网商务一族是努力开展因特网商务，使之由美景变为现实的一群精英。

我们的中心是开展因特网商务，并使之获得长期的成功。在某一方面来说，因特网商务似乎是简单得有点虚幻，有些公司认为这只是“建立一个Web网站，盯着财源滚滚而来”。一年后，他们就会感到很奇怪：究竟怎么了？为什么没有成功？正如任何企业经营者所懂得的那样，一切都来之不易。商业的基本游戏规则没有变，只是因特网的确使游戏场所改变了而已。它开辟了新市场，提出了更贴近顾客与合作的新方式。

对某些人来说，因特网商务的刺激已经产生了“信用差距”，差距在变革的宏伟美景与公司计算机系统管理日常问题之间。描绘未来令人兴奋不已的美景并不难，而弄清楚如何去实现却往往不那么容易。本书目的在于提供帮助，在这两者之间架起一座桥梁，使各行各业有可能随着技术创新而获得成功，为变革美景的实现打下基础。

本书始终强调做法和原则，即怎么做和为什么。做法就是行动，即具体情况具体办法；原则是一般规则，即做法所依据的要素。随着技术创新（或者说，随着商业模式的演变），做法也必然要随之改变。原则比之做法，其变化速度就相对较慢，且应用范围也相对广泛。如果一群人懂得了作为他们行动基础的原则，他们就可以适应情况变化，采取与之相适应的新做法。不了解这一点，一遇到情况变化，需要采取不同的做法以取得成功时，他们就会束手无策。

技术创新带来的是新机会、成本结构变化、新客户和快速响应时间。技术创新的机会必定

与商业目标紧密相连，同时随着商业目标的变化而进行相应的调整。本书写的就是关于这一综合体的内容，即设计能在开放的计算机网络上做生意这样的计算机系统。

我们说本书是关于设计的书，就是说它是为帮助设计流程而写的。本书没有提出所有的解答方案，因为实际设计是按商业需要为依据的，你的设计与别人的或许有天壤之别。然而，我们还是可以探讨在因特网商务系统设计时提出的某些共同论点和重大问题。在书中，我们着眼于某些现代关键技术，并使之应用于各个不同的例子之中。

一句忠告：有时看来我们对潜在问题（可能出错的事物）过分担忧了。这些问题不应成为不开展因特网商务的理由。反之，我们认为重要的是，探讨因特网商务，就像你探讨其他商务计划那样，懂得它有优点也有缺点，有风险也有收益。掌握得当，对各行各业来说，因特网商务的应用像是在挖一个大金矿。尽一切可能去捕捉最大的商机，因为只要生意好就意味着你成功了。

本书网站：http://www.treese.org/Commerce/。

目 录

第 1 章 前言 1

1.1 为何用因特网，为何现在用 1
1.2 策略问题 3
1.3 我们说的因特网商务意指什么 4
1.4 因特网商务的商业问题 5
1.5 因特网商务的技术问题 6
1.6 在公司里谁拥有因特网商务 7
1.7 本书的组成部分 7

第一部分 从事因特网商务

第 2 章 商业价值链 12

2.1 引入商业价值链 12
2.2 商业价值链的组成阶段 14
2.3 客户是谁 16
2.4 在因特网上推销 17
2.5 做全球生意 20
2.6 法律环境 21
2.7 总结 23

第 3 章 因特网商业策略 24

3.1 商业和技术革命 24
3.2 历史的雷同 24
3.3 因特网价值取向 26
3.4 四个策略 27
3.5 新竞争威胁 30
3.6 新竞争机会 31
3.7 总结 31

第 4 章 商业模式——类别研究 32

4.1 商业类别初步 32

4.2 消费者零售 33
4.3 B2B 编目 42
4.4 信息商务 47
4.5 小结 53

第 5 章 相互矛盾的目标和需求 54

5.1 参与者的目标 54
5.2 标准的作用 58
5.3 隐私与推销 59
5.4 安全电子交易 62
5.5 小结 64

第 6 章 功能体系结构 65

6.1 体系结构是什么 65
6.2 核心体系结构的思路 65
6.3 角色作用 67
6.4 组件 70
6.5 体系结构实例 72
6.6 小结 78

第 7 章 实施策略 79

7.1 计划实施 79
7.2 外包 80
7.3 定制开发 81
7.4 组装式应用 82
7.5 因特网服务供应商的角色作用 83
7.6 商业服务供应商（CSP） 85
7.7 项目管理 86
7.8 保持最新 87
7.9 标准的作用 88
7.10 24 小时操作 89
7.11 安全设计 90
7.12 多机构操作 90
7.13 总结 91

第二部分 因特网商务技术

第 8 章 因特网与万维网 94

8.1 因特网商务技术 94
8.2 因特网的发展 94
8.3 Internet 设计原则 95
8.4 核心网络协议 97
8.5 万维网 100
8.6 代理 103
8.7 Intranet 104
8.8 Extranet 104
8.9 家用电器与网络计算机 104
8.10 Internet 的未来：协议演变 105
8.11 小结 106

第 9 章 Internet 商务系统建筑块 107

9.1 Internet 商务系统组件 107
9.2 内容传输 107
9.3 服务器组件 112
9.4 客户端编程 114
9.5 会话与 Cookie 116
9.6 对象技术 118
9.7 商务客户端技术 122
9.8 数字化商品成交的技术 124
9.9 小结 127

第 10 章 系统设计 128

10.1 设计问题 128
10.2 设计思想 128
10.3 结构性方法 130
10.4 安全性 133
10.5 设计原则与现有技术 135
10.6 小结 135

第 11 章 生成与管理内容 136

11.1 客户看到的内容 136
11.2 基本内容 136
11.3 生成内容的工具 142
11.4 管理内容 146
11.5 多媒体表示 149
11.6 因人而异 150
11.7 集成其他媒介 155
11.8 小结 156

第 12 章 加密法 157

12.1 保密 157
12.2 加密类型 158
12.3 如何评估加密法 159
12.4 操作选择 160
12.5 一次性板 161
12.6 专用密钥（对称）加密法 162
12.7 公用密钥（非对称）加密法 164
12.8 协议 167
12.9 密钥管理 170
12.10 小结 174

第 13 章 安全性 175

13.1 关于安全 175
13.2 为什么担心 Internet 商务安全性 175
13.3 考虑安全 178
13.4 安全设计 179
13.5 分析风险 181
13.6 基本计算机安全性 184
13.7 基本 Internet 安全 185
13.8 客户安全问题 185
13.9 服务器安全问题 188
13.10 达到应用安全性 190
13.11 验证 191
13.12 小结 196

第 14 章 支付系统 197

14.1 支付的作用 197
14.2 关于钱 197
14.3 实际支付系统 198
14.4 智能卡 207
14.5 Internet 支付系统 209
14.6 联机信用卡支付 210
14.7 电子现金 212
14.8 微型支付 213
14.9 抽象支付 216
14.10 小结 217

第 15 章 辅助系统 218

15.1 幕后的细节 218
15.2 税收 218
15.3 发货与处理 221
15.4 库存管理 224
15.5 小结 226

第 16 章 事务处理 227

16.1 事务与 Internet 商务 227
16.2 事务处理概述 227
16.3 Internet 商务中的事务处理 229
16.5 集成现有系统 231
16.6 保存业务记录 231
16.7 审核 235
16.8 备份与灾难恢复 235
16.9 高可用性系统 236
16.10 复制与伸缩 237
16.11 实现事务处理系统 237
16.12 小结 240

第三部分 Internet 商务系统

第 17 章 集成起来 242

17.1 建立完整系统 242
17.2 系统体系结构 244
17.3 安全链接（SecureLink） 247
17.4 Transact 249
17.5 小结 259

第 18 章 Internet 商务的未来 260

18.1 趋势 260
18.2 不连续性 263
18.3 保持更新 263
18.4 战略必要性 264
18.5 结束语 264

第 1 章前言

因为我陷入了遐想，想到了未来在望，
我仿佛见到了世界美景，和那必定要出现的一切奇迹；
我仿佛见到了天空布满商务，布满扬起魔帆的大商船。
——艾尔弗雷德·洛德·坦尼森 ①

因特网商务已成为世界商业的新领域。虽然今日的因特网早在25年前就开始萌芽了，但因特网在商务上的重大应用却是我们在近几年才看到的。伴随着因特网“爆炸”而出现的是各种商业革命的要求、“走出去快速挣钱”的各种方式，甚至终结单一民族国家的历史。但是，在这一片欢呼声背后，实质性东西是什么呢？

我们认为实质在于，全球因特网与商务的结合将从根本上改变做生意的方式。本书即是一本关于如何使因特网商务获得成功的书，因特网给商务带来了新技术和新潜力。当然，数百年乃至数千年来商家所面临的基本商业问题是：你得有东西卖，让潜在买家知道你的商品，收取货款，交货或提供服务，以及提供适当的售后服务。大部分时间里，你要和客户建立友好关系，以使他们能够成为你的回头客。

1.1 为何用因特网，为何现在用

总之，公司有两个理由去从事因特网商务②，也即两个目标：

- 最高目标：招揽新客户，并与所有客户建立更加亲密的友好关系。

在因特网上，每一个企业都面向全球。现在，即使是中小企业也可以轻而易举地招揽到全世界的客户。计算机和通信技术使得商家能够更加了解其客户，也使客户能分享该企业的更多信息，从而可以利用这些信息增进两者的友好关系，促进销售。

- 最低目标：大大降低信息发送成本和客户服务成本。

因特网大大降低了销售中信息传播的成本，也大大改进了信息传播的能力，使之能时时传播最新信息。在这个世界里，形形色色的客户对自己想买的商品和服务需要了解更多

① 1842 年，艾尔弗雷德·洛德·坦尼森的《洛克斯雷大厅》。

②另一个观点是：公司从事因特网商务的两个理由是——恐惧与贪婪，这和从事许多领域的商业相同。

的信息，传播这些信息（且费用低廉）的能力便成了交易的重要一部分。而且在因特网上，信息本身也许就是产品。

在长时期内，因特网也许会充分改变竞争的结构。即时通信会改变企业与客户之间的关系，从物质到数字的转变会转换商业价值来源。在许多情况下，我们还无法看到这些转变的性质。比如，计算机网络会产生供应商的重大整合，或让数千个小商家新近都能因从事全球销售而得到发展吗？对于上述问题，我们有非常有力的论据，甚至更基本的论据，就是商业贸易面临的竞争会来自各行各业，来自各个公司，这需要从根本上重新评估企业对客户所抱有的价值命题。

这些考虑事项几乎是依据因特网在技术和经济两方面的性质自然而然得出来的，以下是因特网的几个关键性能：

- 因特网的相互可操作性。
  根据定义，如果一台计算机与任何连接到因特网的计算机联机，那么这台计算机差不多也就是连接了因特网。有两个因素使之成为可能：一是标准协议的使用，二是采用通用的命名、寻址和路由。Internet 标准使这种联网成为可能，无须再事先为计算机联网取得一致了。
- 因特网的全球性。
  由于因特网是建立在标准化和通用联网的基础上的，因而它迅速成为了一个全球性的计算机网络系统。计算机网络本身是用来分发软件的，全世界用户就可以随时共用一套软件，这些潜在用户就构成了商业体系的基础。
- Web 使之变得容易。
  万维网[③]的高性能多媒体内容，使全世界用户使用起来一样简便。懂一点或不懂计算机的人都可以上网，他们使用起 Web 浏览器来一样得心应手。
- 计算机网络的成本费用由多种应用分担，由终端用户负担。
  多数企业和消费者要为自己与因特网的连接支付费用，然后就可以自由地使用因特网。信息提供者不必为分发系统付费，不像自己联网时那样要付费。享受信息服务的用户则要支付分布式系统的费用。由于网络是许多用户共享的，这个基础设施的成本费用就在其众多的应用中逐渐摊付。

1.1.1 进入全球市场

近来，“全球化”这个名词已经变得很普通了，交通和通信的发展使商业贸易的全球化变得可行。供应商和客户可能会分布在世界任何地方。在许多情况下，国家与国家之间正在减少

③因特网和许多技术一样，是多层次的，基础层包括基本命名、寻址、路由以及通信机制。在此之上，万维网是以因特网通信为基础的极为流行的特定应用，而商业应用是在 Web 技术之上运转的又一层了。

或消除贸易壁垒，鼓励从事越来越国际化的商务活动。

因特网正在使全球化趋势加速发展。通过提供遍及全世界的高带宽通信，因特网使全世界的客户、合伙人和供应商可以更有效地合作。不过，因特网能做的还不止这些。因为通信的成本费用基本上是相同的，不管交易双方是在逛街或是在周游世界途中，因特网会使这样的合作与交易效率变得高得多。

实际上，在因特网上，人人都可以直接面向全世界。更确切地说，上网的每一个人的确是直接面对全世界，不管他们是否这样想。例如，任何上网者可以访问你的网页，而你不必特别要求他或她这样做。

这并不等于说因特网会使国际贸易高枕无忧。就如我们所看到的，仍然会存在许多问题，如支付方式、货币兑换、装船运输以及不同国家和地区的不同交易法规。但是对许多企业来说，其感觉很可能像有些小书店那样，它建立了网站，突然收到了印度尼西亚和尼泊尔下的订单。因特网使世界变小了，这并非言过其实，这是数百万因特网用户的日常体验。

1.1.2 大大缩减信息发送成本

在美国，邮寄一本印刷小册子或商品目录可能要花好几美元。而用电子邮件发送同样的物品，或者在 Web 网站上提供相同的“样件”，只需先花钱上网，其发送费用几乎等于零。

最令人感兴趣的是，使用因特网，可以降低信息发送费用，它甚至可以以更低的成本提供更多的信息，并且提供的是最新信息，而且可以搜索。各种各样的客户对他们买的商品，想要得到更多更准确的信息。电子工程师感兴趣的是零部件的详细说明书、样品简图和设计注释，他们也许要用这些零部件来制造新产品；消费者想知道产品的使用方法，与别的产品比较如何，甚至产品对环境的影响。在因特网上提供这些信息，其成本低廉，完全可以办得到，而用其他方式，其费用则太贵了。

当然，在线销售信息或软件也是如此。这些“数字商品”可以通过网络发送，效率高而成本低廉。对某些产品来说，这样可以完全省去昂贵的包装费（箱子、只读光盘和包装材料等等）；而对其他产品来说，这是一个全新的发送渠道，是对现有渠道的一个补充，其成本低廉，占尽先机，对全世界客户都一个样。

1.2 策略问题

我们认为因特网的出现带来了两个策略问题：一是集中经营与授权经营，二是竞争性新挑战。

1.2.1 集中经营与授权经营

因特网开通了从价值创造者到消费者的直接销售通道，使销售成本大为降低。这可能导致供应商的高度集中，或相反，在全球的适当市场上出现千千万万中小供应商。多半可能两者同时出现。一方面，可能会出现少数音乐超级网站，它们价格优惠，服务周到，销售全球，但不会超过数百家；另一方面，轻易就进入全球社会，可以使一定的周边市场发展到相当规模，以支持赚钱的生意。例如，如果一个电子商店向全球市场销售古代马车鞭，这项生意可能有它的生存的空间。

1.2.2 激烈竞争的新挑战

因特网的出现使传统的销售链受到了一定的冲击，这也许会使竞争产生质的变化，最显而易见的是地域和成本结构的变化。因为要进入一个新市场，再没有必要花重金去建立销售渠道了，因特网可以让先前分散的企业参与直接竞争。对消费者来说，降低了企业进入市场的门槛，他们是受惠者；而对制造商来说，成本和效率的竞争则扩展到了全世界范围。

当各行各业交叉竞争时，更有趣的事开始发生了。想一想金融证券交易的例子，传统上，银行和券商提供交易服务，而出版商提供比较信息。在因特网上，这些界限变得模糊了，也许会完全消失。因为信息内容可以与交易直接链接，上金融信息网站的用户就可以在该网站下单独买卖证券。是出版商在做证券交易或券商成了出版商吗？有时情况是无法分析清楚的，不过分析透谁拥有顾客关系，是个好的出发点。请时时保持企业给顾客的价值观念。

1.3 我们说的因特网商务意指什么

至此，我们一直在使用“因特网商务”一词，而没有给它一个明确的定义。因特网商务对不同的人有不同的含义，在本书里我们想给它一个明确的定义。我们所说的因特网商务是指利用全球因特网从事商品交易和服务，包括售后服务。因特网也许是广告和传播产品信息（在贸易中有时叫“样件”）的一部高效率的机器，但我们在这里仅指促成完整的商业交易行为。

1.3.1 其他类型的电子商务

因特网商务只是更广义的“电子商务”中的一个类型。电子商务的历史久远多了，但多数是幕后的、有代表性地将供应商与大制造商或服务机构联合起来。广义地说，电子商务包括在金融业应用计算机处理技术和通信技术、在线航空订票系统、订单处理和存货管理等等。

从历史上看，电子商务最广为人知的方式是电子数据交换（EDI）。EDI最初是运输业为连接各合作伙伴而创立的，现在已是许多机构的家常便饭了，它们通过EDI与供应商和合伙人合作。EDI的确是一个包罗万象的词汇，不同的活动就有不同的EDI，即某一种特殊交易关系。建立一种EDI关系常常要花很长时间，需要就通信形式和数据格式进行详细的谈判（当然，除非某一方很强大，硬性规定另一方按其要求办）。许多机构创建了EDI，也花得起钱来投资，而EDI也在它们中间发挥着巨大的作用。

值得注意的是，EDI和因特网并没有相互排斥。事实上，EDI专门应用于某些特定类型的信息，可以和因特网同时使用，因特网是一种传输数据的途径。现在有许多公司利用因特网来作为EDI应用的通信基础，市场上也已经有了一些创建EDI-因特网相互应用的专门产品。

进行因特网商务不像EDI那样，它没有许多限制。在一个共享的公共网络上，随时随地都可以通信联系，而不用建立一个专门的网络或与费用昂贵的增值网（VAN）服务系统订立契约。更重要的是，Web网可以促使互不相识的买卖双方达成自发的商业交易，这第一步也许是长期友好关系的开端。有时，贸易伙伴之间可以探讨专业信息、EDI或其他问题，这可以使他们合作得更富有成效。

1.4 因特网商务的商业问题

首先，因特网商务就是商业，即有效地利用网络来达到商业目标。计算机和通信两方面的技术创新提供了多种工具，可以用来达到这些商业目标。但如果我们没有弄清楚利用因特网所要达到的商业目标是什么，那么再好的技术也无助于我们成功。

这并不是说商业目标就不能利用新技术的优点了。例如，利用因特网与客户联系以加深友好关系，选择这样一个新的中心任务，是完全适宜的。没有网络，要达到这样一个目标，可能费用太高，难度也太大了。有了因特网，公司就可以达到这个目标，这在以前是办不到的。不过，商业目标，包括如何衡量什么才是成功，这是问题的关键，并不仅仅是一个想法，就像“嘿！我们可以给客户发电子邮件了”那样而已。

因特网商务的商业问题涵盖了商业活动的方方面面，从吸引顾客到履行订单，从销售到结账，它们包括企业提出的许多问题。

- 如何使它符合我们的策略？我们的策略要改变吗？
- 对我们的竞争态势而言，这意味着什么？
- 我们要的是短期回报，还是长期投资？
- 要投入多少费用？我们要达到什么目标？
- 我们如何衡量什么才是成功？
- 这对我们的销售渠道、合伙人和供应商有怎样的影响？

每家公司在评估新的商业活动时，都会提出许多别的问题，但因特网不应被排除在这些考虑在外。

因特网商务中要注意的一个问题是：从事因特网商务的启动费用可能很低，但过一段时间，某一项目的规模可能变得很大，总要增加一些新的东西——插入新的技术程序或在Web网站上做看起来不大的扩展。建立一个Web网站似乎很容易：使用几页HTML语言，放置到本地因特网服务供应商（ISP）那里，或许也处理一些电子邮件。再比较以下其他方面：发布即时最新商品目录，保存和利用客户资料，以各种方式收取货款，与库存和履约系统链接，以及提供客户支持功能。方法之一是，在一段时间内，让这些功能不管三七二十一地连接到原先的Web网站上；方法之二是，有计划地让网站不断演变改进，依据每一步骤的结果制定下一步的方案，不断修正计划，让其恰到好处。采用方法一，虽然有的公司也许会成功，但多半不知道它所需的费用，而且也无法评估是否成功。方法之二也许没有提供即时的满足条件，让Web网站尽快运转（但那也许是一个更谨慎而按部就班的目标），不过，这的确可以使一个公司集中精力去做事，并可以重点关注投资有什么回报。我们并不提倡第三种方法：立即设计和建立完善的系统，这要费很长的时间。不管怎么说，网站的完成要随情况变化和技术创新而改变，这是不可避免的。

本书很大部分是关于第二种策略问题的。当然，不同的公司有不同的商业问题和商业目标。我们在书中提出并探讨那些企业会遇到的许多共同问题，即使问题不是直接针对特定商务活动，我们仍希望这会对其他企业有所启发，以便能引领你制订出因特网商务计划去获得商业上的成功。

1.5 因特网商务的技术问题

诚然，有了技术才有可能从事因特网商务。万维网的创立以及随后的传播，为许多不同的应用（包括商业应用）提供了技术基础。万维网自从引入以来，就飞速变化着，这包括两方面：一是在用法方面的迅速发展，二是在协议、系统和应用方面的巨大演变。商务系统有两个关键技术问题：一是选用何种技术，二是技术更新换代极快。

本书大部分篇幅写的是第一个问题：如何应用因特网技术来进行商务活动。商业应用带来了许多技术组件：Web、数据库、高速联网、加密算法和多媒体等等。将它们放置在一起，组成一个安全、高性能的集成系统，这一工作可能很具挑战性，不过我们在这里提出的原则和思路会提供一些颇有助益的指导。最早的因特网商务系统是定制软件，近来已经能够用工具库把不同供应商的软件模块和各种应用集成到一个商务系统了。目前，我们明白一套因特网商务组装式应用软件是多么迫切需要，这是由一个供应商提供的一套完整的或接近完整的系统软件，有了这种系统软件，也许就只需把它连接到现有的商业系统上就行了。

第二个技术问题：技术更新换代，它是今天因特网发展所面临的严酷现实，而且我们看到这是不会停止的。因此，为了获得成功，任何商务系统软件都得有所预留，以便在新技术投入应用时能与之相兼容。这种适应性的关键是要有一套统一的系统结构，它设计出要达到什么目标以及原则是什么。我们把焦点放在目标和基本原则上，这样我们就可以采用有助于我们达到那些目标的新技术，同时避免使用那些表面上看来令人兴奋而实际上却与我们的目标和现有系统不相适应的新技术。工具库、模块和应用软件的出现非常有助于我们应付技术的更新换代，而其成本费用可以由许许多多的客户来逐渐摊付。

1.6 在公司里谁拥有因特网商务

在公司里谁拥有因特网商务？谁操作这个系统？是销售和推销小组？还是管理信息系统（MIS）小组呢？如果涉及交易行为，是不是也包括结账收款部门呢？对任何个别小组来说，答案也许是显而易见的。初看起来，问这些问题似乎有些可笑。其实，根据许多公司的经验，他们认为：清清楚楚地知道这个答案是成功的一个重大因素。问题在于，多个小组就会自然而然认为：是自己推动了公司的因特网商务，从而造成内部混乱，也给客户带来混乱。为解决这个问题，开展因特网商务零敲碎打的尝试，往往造成把钱花在相同或类似的基础部件上：如硬件、核心软件和网络连接等等。

实际上，成功的因特网商务几乎总是要经过多方努力，有赖于公司内部许多不同小组的合力：销售和推销小组在网上有效地推介产品和服务，MIS 小组操作或外包 24 小时运转的商务系统，链接会计系统以进行交易等等。因特网现阶段可从周边操作开始，通常这样做是很适合的，从而克服官僚主义通病：效率低下和人浮于事。行之有效的因特网商务是公司业务的延伸，有赖于公司内部各种资源的利用。在公司内部争论谁拥有因特网商务，可能会很容易把一个项目（或几个项目）搞砸，留给公司的是无法迅速行动以适应商务应用的瞬息万变。由于因特网其重要性具有决定意义，同时又是人们可以感觉得到的，因此，因特网商务项目应当引起高级管理层的关注，或甚至由他们来发起创建。

1.7 本书的组成部分

本书由三部分组成。第一部分，我们分析了从事因特网商务的商业要求，就 B2B 应用、零售和信息业三者商业系统的来龙去脉提出若干基本设计问题。第二部分，我们阐述了在开放网络上从事商务活动所要用到的一些基本技术。我们将特别关注因特网和万维网方面的技术、系统设计、加密学和安全、支付系统和交易处理。最后的第三部分，我们“总而言之”使之成为一个完整的系统，并以评估未来的种种挑战来结束本书。

1.7.1 第一部分——从事因特网商务

第2章探讨商业价值链。部分商业系统设计是希望揭示一个明确而严谨的观点，即要获得成功，这个系统的所有要素都是必不可少的。一台发动机成不了汽车，而没有道路、加油站和乘客，只有一部完整的小车可能也会毫无用处。商业价值链有助于我们认清走向成功所有必需的要素。

第3章专门阐述了因特网商业策略。除了150年前铁路的发展，因特网在经济景观中所产生的变化程度，是我们再也没有见到过的。今后，规模经济和范围经济的变化，需要有新的战略思想。

我们在第4章介绍了因特网商务系统的商业要求和商业问题，请参看针对消费者零售、B2B商品编目和信息商品的出版销售三个类别的例子。

一个成功的商业系统需要许多当事者密切合作，其中包括消费者、商家、金融数据处理者、各级政府和技术专家。这些人员各有不同的优势，同时也有着社会、法律和技术上的种种局限性，他们会影响到企业的成败。第5章探讨了因特网商务范畴的某些问题。当不同小组意见不一致时（或似乎会产生纷争时），因特网商务的难点和问题就来了。商业上的成功，有赖于客户、合伙人和供应商富有成效的合作，以便渡过危机四伏的浅滩，到达成功的彼岸。

第6章，我们讨论了因特网商务系统结构的组件、角色作用、结构处理，介绍了功能分解概念和信托模型概念。用高级结构来处理系统设计，使之在长时期内能适应技术创新和商业要求的演变。设计、开发、安装和操作信息技术系统有多种方法，从内部自用开发到由一个服务商操作的组装式软件。第7章谈到制订计划和项目管理问题，它们远远超出了软件的特性和功能的范畴。

1.7.2 第二部分——因特网商务技术

本书第二部分集中论述技术问题，着眼于领悟以技术为基础的关键思路。

作为第二部分的前言，第8章综述了因特网和万维网的技术基础。我们在第9章的论述超越了如何将技术应用于因特网商务系统这个基本点。

第10章，我们讨论设计哲学、系统结构原则和设计方案。这些方案往往独立于执行技术，因此在新的技术组件被开发出来后可以执行“换入”的程序。

第11章讨论因特网商务“内容”的创建与管理。简单地说，内容就是人们在网上看到的东西。我们综述了创建和管理的方法以及有关商业支持的内容。

因特网商务系统最大的问题之一是安全问题。现代加密学是商务系统安全的基础，第12章提供了这方面的概论。简单地使用加密学（用未指定的方法）并不能创建一个安全的系统，所以我们将讨论在应用系统中如何使用加密学。在第13章，我们超越了加密学基础，论述了安全系统的设计。我们提出一个因特网商务安全系统设计的方法。适当地利用加密学是一个关键步骤，但谨慎地设计系统的安全策略、机制、应用特性和牵制程序均占有重要的地位。

支付系统常常被看作是因特网商务系统的核心，显然它起着重要的作用。在第 14 章，我们讨论各种各样的支付系统及其在因特网商务上的应用问题。除了支付系统的技术方面，我们还讨论了信托模型与成本结构。企业需要完整的商业解决方法，第 15 章讨论了处理税务、运输和存货所需要的辅助系统。

商业就是商品与所获价值的交换。交易处理是系统的重要组成部分，一旦双方达成交易，它能确保商业交易得以完成。在计算机系统里，尤其是通过网络进行的销售，往往不像表面上那样容易，在出了毛病时尤其如此。第16章介绍了一个错综复杂的问题，讨论包括伸缩性、性能、可靠性和业务记录保留等方面。

1.7.3 第三部分——因特网商务体系

既然我们订立了计划，综述了可利用的技术部件，如何将它们聚合起来形成一个可运转系统呢？第 17 章描述了一种方法，即因特网商务组装式应用软件。

斗转星移，因特网商务日新月异，一旦系统建立起来开始运转，在这瞬息万变的世界里，如何时时刻刻保持最新呢？我们讨论了在受到技术演变的冲击时如何在发展轨道上前进。第18章设计了通向未来的几条道路。

第一部分
从事因特网商务

第 2 章 商业价值链
第 3 章 因特网商业策略
第 4 章 商业模式——类别研究
第 5 章 相互矛盾的目标和需求
第 6 章 功能体系结构
第 7 章 实施策略

第 2 章商业价值链

他选择的东西是：
彼此包容，整体统一，
错综复杂，汇聚成和谐。
——华莱士·史蒂文斯 ①

2.1 引入商业价值链

当一个消费者在商店买了一件成品，这仅仅是复杂过程中的一个步骤，这个复杂的过程是以使用原材料制造产品为开端的。在其每一步中，有价物不断添加上去，美化了原材料，使之塑造成有用之形，经过运输，再进一步加工，或把这成品卖给最终消费者。有时，我们把这一过程叫作产品的“价值链”，即产品在制造和发送过程中增值的链环。

价值链的观点相当明确地由成品得到了例证，但是，我们还可以用它来描述多种多样的商业活动，包括刚提到的广泛的价值链中更细分的组成阶段。例如，我们可以看看零售商的价值链，它包括选择要出售的产品、从批发商和制造商那里购买产品、布置诱人的橱窗展示、打广告招引客户、帮助客户选购产品、收取货款、把货交到客户手中。对此项经营来说，其价值链的每一环节均是很重要的，只要哪个环节出了毛病，整项生意便会受到影响。

同样，企业有自己需要的价值链，我们可以考虑从这个角度来建立一个因特网商务系统。它有一部分与基础商业（如销售图书）的价值链相关，另一部分则取自在线从商所需要的价值链。领会这两者及将其融合，是成功从事因特网商务的一个重要因素。我们将从第三个角度，就是从一个公司所有面向客户的活动这个角度来看价值链。

本章我们谈因特网商务一般价值链（如图 2.1 所示），其中心是企业与客户的互动。不同企业（和不同商业模式），它们的价值链内容必定不同，不过我们已找到了一般方法，能够非常有效地组织在线从商的方法。这个一般价值链的组成阶段如下：

1. 吸引客户
   推销——让客户产生兴趣、保持兴趣
2. 与客户互动
   销售——让客户从兴趣转变为下订单（一般内容）

①华莱士·史蒂文斯：“这一定会给人们带来乐趣”，1947 年《最佳小说述评》。

3.客户指令行动

订单管理——接收订单、支付、履行订单

4.客户请求响应

客户服务、技术支持

详见下图 2.1。

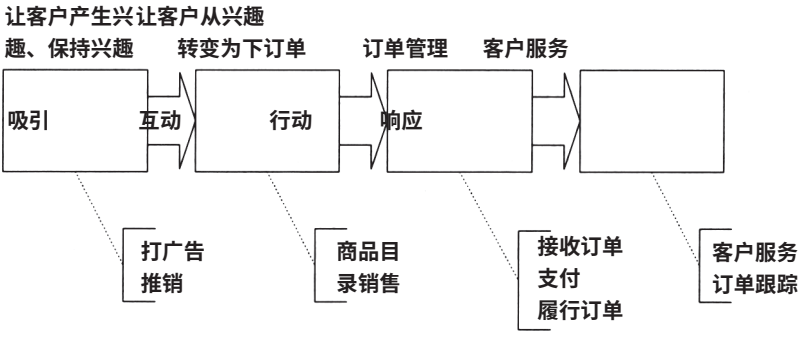


图 2.1 商业价值链

谈企业价值链有助于我们定出中心范围：企业的最佳擅长点和首要出发点。即使有些企业看起来可能非常相似，但是，在从事因特网商务和更为传统的商业形式中，重点不同可能有不同的影响。

例如，两个书店，一个侧重书籍门类广泛，一个侧重个人服务。在现实世界里，这种差异影响着许多决定：书店的选点、规模大小、雇什么样的人员和选择生意需要的计算机系统。同理，这样的书店在因特网上做生意时也会截然不同。侧重门类广泛的也许需要综合数据库和工具，以便可以按不同方式查找图书（按书名、作者、出版商或国际标准书号等）；侧重个人服务的则可能会举行读者座谈讨论会、开展店员与读者互动活动以及其他各种服务。

在从事因特网商务中，可能要开展各种活动，仔细考虑价值链，可以帮助从这长长的活动表中选出最重要的办法来。例如，大型书店可能想要提供一切服务，包括小书店的服务，不过，如果它不首先侧重自己的核心能力——提供大量图书上，那么它成功的可能就要大打折扣。把一项生意移到因特网上做时，诱人的念头是一切都想试一试，因为这似乎很容易或仅仅因为这似乎很有可能。价值链的每一阶段都必须有一个公开策略，不单是因生意而异的那些策略。然而，没有必要自己包揽一切，许多公司用合作的形式来充实价值链，这样，价值链的每一环就很牢固。

2.2 商业价值链的组成阶段

不同的行业，商业价值链的关键组成部分可能千差万别，即使在同一行业不同的企业中，其关键阶段也大不相同。本节，我们将谈谈因特网商务一般价值链。有一部分，我们谈如何分解价值链，把它分析得更仔细；还有一部分举例解释，从事因特网商务，最重要的组成阶段是哪些，我们在本节始终以消费者零买作为例子。在下一章，我们谈几个不同的商业类别，以及如何把商业价值链用到这些类别中去。

2.2.1 吸引客户

吸引是因特网商务一般价值链的第一个组成阶段。我们说吸引是指我们采取的每一步骤都是吸引客户到主要场所，不管是在别的Web网站登付费广告、电子邮件、电视、印刷品或是其他形式的广告和推销。这阶段的要点是把他们吸引到详细商品目录或销售产品及其服务的其他信息上来。②

2.2.2 与客户互动

互动是第二个组成阶段。互动是指将客户的兴趣转变为订单。这阶段的定向是一般内容，包括商品目录、出版物和客户通过因特网能得到的其他信息。内容可以通过许多不同的途径发布，如万维网或电子邮件。有时，在因特网商务和其他媒体发布的内容如只读光盘之间还会有联系。

内容的编辑，其变化可能会很频繁，或者反之。内容在技术上可能是静态的，也可能是动态的。静态内容有代表性的是由现成的几页资料组成的，如摘自商品目录，应客户请求将它们发送到客户手中。每当资料上的信息有所改变，就得重新编制这些资料。动态内容是应需而生的，利用一个或多个信息源整理成适当的内容发送给客户。动态内容的信息源包括：数据库，如商品价目数据库；客户软件能力，如可以用什么样的图解版式；甚至客户是谁，他们属于什么公司。在编辑内容变化频繁时、信息自然储存媒介为数据库时，以及信息作多种用途时，往往使用动态内容。

我们将在第11章讨论有关内容创建与内容表示方法的细节。

2.2.3 客户指令行动

行动是商业价值链的第三个组成阶段。一旦买主从头到尾查看了商品目录，想要购买时，必须有个方法来接收订单、处理支付、履行订单以及进行其他方面的订单管理。

---

②随着有内在交易功能的活动广告的出现，价值链阶段之间的界限变得模糊了。

订单处理

买主经常想同时购买好几件商品，所以订单处理必须有能力把商品汇集在一起，以便后来下单交易。在零售交易中，这种能力的体现有时叫做“购物推车”，它可以随时修改，可以增减商品和修改数量等。

当买主准备结束购物时，通常必须加上附加费用，如营业税和运费。订单处理系统会提交一份清单给买主，包括所有的附加费用，这样，买主就可以支付了。

支付

买主可以根据订单条款来支付（或发出支付指令），这可作为接收订单的一部分。一旦订单敲定，买主就可以支付货款了。就如现实中购买商品一样，一件商品可能有多种支付方法。在线支付有些方法可能是现实中找得到的信用卡、汇票等；有些则可能只用于因特网商务，它们使用的新技术是专门为网络系统开发的。例如，在线出版系统，可以为某杂志的单一一篇文章收点小费用，而不需要买主购买整本杂志。

在线支付系统最重要的惟一特性是，卖主可以用它来收取买主的支付。这就是说，不管用哪一种支付方法，必须至少有一种是双方同意的。这种特性有几种含义：首先，卖主系统一定可以处理几种支付方式，这对卖主的生意很重要。例如，信用卡普遍用于消费者的零售交易，而企业常彼此使用汇票。使用哪一种支付方式，可能会有非技术上的限制。接受信用卡，商家必须在指定银行开有账户，专门处理这些交易。没有这种账户，设立信用卡支付的技术设施就毫无用处。

其次，卖主一定要关注对买主系统的要求。如果要求买主采用专门的软件包来处理专门的支付系统，那么，有这种可能的人多半会少得多。当然，有时所有客户都会有这种软件，或者乐意获取这样的软件。总之，关键点是，在选用技术时，要把客户和生意放在心上。

还要注意的是，完成这一步骤并不一定说资金已转入卖主的银行账户。有些支付方式，包括信用卡和汇票，允许买主延期支付，他们的实际支付会延后。在这种情况下，卖主系统授权交易是很常见的，不管是需要第三方（如发信用卡的银行）授权，或是按照公司内部规定（如是否建立了汇票关系）授权。我们随后会看到，只有商品运出，交易才有可能算是最后解决了。

我们在第 14 章讨论支付系统及其使用方法。

履行

现在下了订单，付了款（或至少对支付有了一个满意的承诺），下一步是履行订单。如何履行取决于买什么样的东西。如果订购的是物质商品（有时叫耐用品），那就要送到买主手中。于是订单通常要转到传统的订单处理系统去执行，也就是有人选出物品，给予打包，再装运。在这种情况下，在线商务系统必须有转交订单的方法。这一步骤可能就像打印或传真一份订单让人去处理那样简单，或者可能把一个更复杂的接口如 EDI 应用到另一个计算机系统上。当然，准确的使用何种方法，要由业务其他方面如何处理订单来决定。

现实中，还有第二类订单是要求履行服务。例如，有人可能会订在线声乐电报。尽管这种履行服务已出现了，但这是一种服务，不是物质商品。然而，为了履行服务，我们可以把这些订单看作是物质商品来处理，该订单交给一个系统或人来履行。

第三类订单与因特网的联系更加紧密。我们称这类订单为“数字商品”订单[③]。数字商品包括五花八门的在线发送，如在线发送软件、杂志文章或新闻文章、报告和花一段时间访问某一数据库等等。我们会看到，数字商品的订单履行可能相当复杂。

我们在第15章讨论物质商品订单履行系统集成，在后面讨论“信息商务”数字商品订单履行系统的某些方面。

2.2.4 客户请求响应

最后，销售结束后，客户可能会有一些问题和难点，需要提供服务。有的问题需要人工回答，而有些可以用适当的信息系统回答。例如，交易跟踪系统可能会提出一份客户购货总结报告。客户想知道他们的订货是否已运出，可以通过这个系统查看。更复杂的例子是，在发送数字商品失败时，这个系统如何处理。

假设一个客户在线购买一个软件包，软件已下载到客户的计算机上，由于网络出错，下载失败，客户怎么办呢？显然，不应要求他们再买一次，所以，他们需要出具“购买证明”（如一张发票），以使履行服务器接纳，允许客户再试着下载一次。

用人工回答客户服务请求，其费用可能非常昂贵，因此，投资一个非人工系统就很值得。我们刚才提到，这种系统常常提供日常（或甚至特殊）信息来应答简单的咨询，但是，设计不需要客户提问题的系统同样重要。在上述软件例子中，使用发票，可以让客户轻易就解决问题。

2.3 客户是谁

对企业来说，最重要的问题之一是客户是谁。这个问题似乎是不言而喻的，不过，企业（或其他机构）往往对这一答案不甚明了。有时这个答案比初看起来更为微妙。例如，有个公司销售PC电子元件，一方面，它的客户是计算机装配厂家，他们买的元件数量很大，因此要下订单、谈条件、收货和支付；另一方面，也许一个更重要的客户群体是专门工程师（即决定计算机里使用什么元件的人），一旦决定了，只要可以签一份满意的合同，其余的许多事就不在话下了。

要有效地对这两类客户销售，也许就要采用极不相同的策略了。同样，设计一个在线商务系统与这两类客户打交道，也要建立极为不同的系统。例如，专门工程师一定能够很快地在商

③数字商品有时叫“非耐用品”，与“耐用品”相对，这可能会与传统的“非耐用品”指衣着服饰的意思相混淆，所以，我们宁可用“数字商品”一词。

品目录里找到所需的元件，他们一定还要知道详细信息，如规格、样品图解（说明元件使用方法）以及如何为造样机订购样品元件。

另一类客户，即用元件制造计算机的厂家，他们则有另一些极不相同的问题要解决。他们的订货量很大，要求发货及时，要按复杂的合同条款来支付。尽管两类客户都可能因使用因特网而受惠，但没有详细了解客户是谁，以及他们要解决的问题是什么，就不可能建立一个成功的系统。

2.3.1 在因特网上发展与客户的友好关系

与客户有良好的关系常常意味着生意会成功。与卖主关系良好的客户往往会成为回头客，留住一个客户总比找一个客户容易得多。同“客户是谁”的问题一样，这似乎是不言而喻的，不过，这时常作为第二位来考虑。从因特网商务的角度看，客户关系可以考虑两个方面：一是改进现有的客户服务，二是如何应用新技术来提供更好的服务或新服务。

建立稳固的客户关系，最好的方法之一是通信。客户通常想知道卖主的发展方向、能力、问题原因和是否有潜在问题等等；他们还希望通信的效率高，并能集中在他们感兴趣的事情上。例如，AT&T的任何一个客户也许不会对AT&T所做的一切都感兴趣，有些客户对如何降低个人长途费用感兴趣，而有些则想知道如何建立全球电信设施。

因特网可以增高卖主与客户的通信效率。对卖主效率高，是因为通信费用增加不多，而且可以把信息专门发给个别客户或客户群体；对客户效率高，准确地说，是因为这样可以集中在自己所需要和感兴趣的信息上。反之，如果卖主没有高效利用通信，客户就可能会提出异议，关系就可能会弄僵。

这种通信能力还可以用来提供新服务，尤其是有关订货或服务最新情况的信息。例如，许多物流公司（如联邦快件和联合包裹服务公司）开辟了查询发货情况的方法，有了因特网，他们有可能与客户进行更紧密的联系，并增进与客户的友好关系。

2.4 在因特网上推销

许多人受到因特网商务的吸引，因为它提供了推销的新方法。尽管本书不是关于在因特网上推销的书，但本节仍要描述几个相应的概念和问题。近几年，在因特网上推销的广告走向了两个极端：一是认为因特网是全新而不同的媒体，二是认为这不过是另一种媒体，同印刷品和电视没有两样。在因特网上推销，将通信与其他最新技术结合起来，如利用包含人口统计与交易事务广泛信息的巨大数据库。

2.4.1 因特网与其他媒体的差异

因特网的最大特性之一是，人人都可以成为出版商，可以像媒介大公司那样拥有全世界的对象。更重要的是，这个特点显示了因特网与其他媒体不同。电话一次只能与一个人通话，在时间上限制了可通话人数，而且还需要通话双方都在场。传统的大众媒介如报纸、杂志和电视有大量的读者或观众，但它们的能力有限，不是资源短缺如频道有限，就是创立和发送所需的投资有限。

因特网则不受这些限制，因为多数用E-mail或Web为工具，通信时，收发双方不必在场（当然，只要计算机办得到）。在因特网上，个人与大公司的计算机系统相比，区别可能只在于可用的带宽和服务器的能力，而不在于是否可能有广大的对象。

这些区别的含义是什么？其一是一目了然的，在因特网上，小商家可以极为有效地抓住客户；其二是，通信技术与存有客户信息、预定选项等的数据库相结合，使之更容易抓住客户个人。这些特性可能是建立在网络核心能力之上的新推销活动的基础。

2.4.2 因特网与其他媒体的相同点

因特网作为推销的媒体，与其他媒体不同，有人就认为，“这个差异很大，没有必要去了解传统方法了”。1994年，按此原则开始开展因特网商务的公司，今天在我们身边已经不多了，但其作用依然普遍存在，因为有更多人了解了因特网。

和我们已讨论的其他一些问题一样，传统商业和市场的问题仍然存在。

- 客户是谁？
- 客户需要什么？
- 客户希望什么？
- 你想让客户记住什么信息？
- 如何最有效地将信息展现在客户面前？

技术不能替代对推销基本原则的深刻理解和对客户的了解。技术所能提供的是，以更有趣和更老练的方法来抓住客户。

2.4.3 弄懂人口分布统计

当然，推销的关键问题之一是对潜在客户人数的统计。随着因特网的发展，人口分布统计也起了质的变化。因特网创始于研究界，随后发展到学术界的广泛应用，吸引了许多技术公司，紧接着吸引了其他公司，到现在已有众多客户了。其变化很快，而且还在不断变化，我们在此不讨论因特网人口分布统计的细节，不过，我们认为有几个重要原则要记住，包括因特网推销计划方面的人口分布统计。

1. 人口分布统计变化很快，今天的真实在明天也许就不是真实了，所以重要的是盯住动向及其对推销计划可能产生的影响。
2. 聚焦在目标客户的人数上，而不是寻找对因特网可能感兴趣的人数，然后想方设法通过使用因特网来抓住他们，无论他们是用 Web、E-mail 或其他应用。

2.4.4 一对一推销

当今，推销最热门的话题是“一对一推销”④，而不是针对一群听众。通过信息综合分析，了解客户的兴趣、好恶、购物史，有的放矢地针对客户个人。这需要对大量有关客户的信息如购物习惯，以及其他相关的人数统计信息加以收集和综合分析，有时市场存在于一小群客户中。“一对一推销”用在如直邮、有针对性的电视广告和在销售点给个别客户发放有选择的优惠券。

因特网是“一对一推销”的理想媒体，因为通信技术立即提供了直接通道。Web 网站可以在客户浏览商品目录前认出客户，为客户定制提示图像，这种定制有许多形式，如选出展示条目，提供针对性的特别奉献内容，或插入多半是有趣的广告。即使不知道客户的姓名，客户的行为也可能提供某些线索，可以用作综合信息分析。例如，根据客户明显感兴趣的范围，搜索引擎可能选出广告来展示。

另一个例子，航空公司对打广告有特惠。一般说来，客户只对从自己家乡城市飞来的定期航班感兴趣，所以，多数大众广告信息就会与多数客户无关。航空公司可以只跟踪客户家乡城市的动向，来发出 E-mail，通知特惠事宜，这肯定比完全列出特别通信目录更令客户感兴趣。

2.4.5 打广告

在因特网上打广告有多种形式，最简单的是在 Web 网站上描述要销售的产品或服务。当然，仅有 Web 网站并不能保证潜在客户会去访问。因此，广告就要分布在许多其他的位置上。许多公司在别的 Web 网站买了一个广告空间，希望能吸引访问那些网站的客户。因特网搜索引擎是广告的公共位置，因为其巨大容量很吸引人，不过，一些受人欢迎的网站可能也是个好地方。请记住人口分布统计问题，一个打广告的好站点只需在潜在客户中广受欢迎就行了，而不需广受因特网欢迎。印刷广告、无线播音广告和电视广告不断增加引用统一资源地址（URL），使之与因特网相互链接起来。

打广告的另一种形式是，链接 Web 网站中潜在客户可能访问的地方，这种地方包括搜索引擎、普通和专门指南，以及销售商品参考资料等等。

在因特网打广告要慎重，因为网络是在学术研究背景下开始的，强行进入的广告招来的怨恨不容忽视。往因特网邮件清单上发送多余的广告（这种做法有时叫垃圾邮件）普遍不受欢迎，这同样不适用于大多数清单。

---

④西伊·唐·佩珀斯著《一对一的未来：每次与一个客户建立友好关系》（1993 年，《双日》）。

2.5 做全球生意

因特网最具革命性的一点是，它把全世界的人与公司拴到一起。例如对马萨诸塞州剑桥市的人来说，与纽约人通信或与印度孟买人通信没有什么明显差别，除了可用的网络带宽和轻微的潜在差异。这种能力使在线企业有抓住全世界客户的潜力，而成为真正的国际化企业。

然而，国际商务并不那么简单，从比较简单的货币兑换问题，到用数种语言发布信息问题，再到错综复杂的进出口法律关税，我们有许许多多问题要谈。

在本节和下一节，我们要讨论有效开创在线国际商务最重要的一些问题，有些是关于如何有效抓住客户的问题，如使用本地语言的问题；有些是关于法律法规的问题，这在同意在线从商运作之前必须先谈谈。

2.5.1 国际化软件

在不同国家里，使用软件最重要的方面是，表示方法如用户界面可以改成本土化。在多种情况下，这就是说，要把展示的所有信息翻译成本地语言。要这样做，软件必须可以展示任何需要的字符组（严格需要，因为有的语言需要多字节字符，但多数软件在一个字节里存有一个字符）。此软件也必须可以使用翻译好的信息，不过这种情况并不多见。

此外，软件必须可以处理本地货币（对有些本地人来说，要能同时处理多种货币）。

2.5.2 国际化内容

因特网商务可能第一次揭示了企业所处的错综复杂的国际环境。除了单纯的原文翻译，内容的真正国际化需要大量工作，以下列出几个问题：

- 本地对象、地理、民众和新闻事件这些参考资料翻译不好。
- 幽默翻译不好。
- 有时，词语翻译，尤其是产品名称，在不同国家里是极不相同的。
- 商标在不同国家里作用不同。
- 色彩，尤其是用于共同色彩方案和徽标，不同文化产生不同印象。

跨国公司能透彻理解这类问题，不过，对于想要向全球销售的小公司而言，就很重要了。

2.5.3 隐私

许多国家尤其在欧洲有严格的法律来限制对消费者个人信息的收集和利用。虽然那些法律细节超过了本书的范围，但是，在线企业在这些国家运作必须清楚其系统应遵守当地法律。不

管怎么说，企业的好做法是告诉客户要收集什么数据及其用途（用作同一企业的一对一推销，卖给他人作推销用等）。大多数因特网客户对在线隐私问题知之甚少，所以他们可能会有不现实的期望。事先阐明有关隐私问题，当客户觉得自己的隐私受到侵害时，企业就可避免随后出现的问题。

2.6 法律环境

计算机和通信技术的迅速发展已对全世界的法律体系提出了许多挑战。例如，有能力收集、联系和搜索个人和企业机构的大量有关信息，便产生了隐私权问题，这在技术创新之前是没有的。技术创新发展步伐比法律体系的发展快得多，挑战也因而加大了。有些专家和观察员呼吁进行大规模的法律变革，以适应技术革命的发展。

在本书里，我们对因特网商务的法律现状采取务实态度。商业在法律环境中运作，许多商业做法被编入法典而受制于法律体系，例如，合同受法律制约，而此法律的产生出于商业需要。法律体系不可能在一夜工夫改变，但由于因特网商务新做法和新需要的出现，它也许需要能够随之改变。在线商务所产生的许多关键问题尚未解决，但新法律和法院裁决会改变规则。要点是，法律环境是因特网商务生存不可或缺的。我们必须清楚，在制定因特网商务发展战略中，法律环境是要斟酌的问题。

本节简述了在制定因特网商务系统方案时要考虑的许多重要法律问题。作者不是律师，我们的讨论不是要替代合法律师的忠告。我们确切提出，技术对商业和法律会产生影响，找一个懂得并重视这问题的律师咨询是明智的。

2.6.1 税收

税收是最直接的法律问题之一，尤其是营业税。既然企业在法律上负有纳税义务，软件系统能计算应缴税额，并能保留记录，以备需要时证明该企业守法经营，这很重要。遗憾的是，计税可能非常复杂，它取决于多种因素，如销售商品和服务的品种、参与方、卖主做生意的地点和买主下单的地点。在美国，税收由州、县和自治区征收，所以税收标准在不同的管辖范围内会有所不同。详细探讨这些问题不在本书范围之内，但在线从商的人应当明确地了解纳税义务，并实施一个可以守法经营的系统。

当然，税收标准在国与国之间存在差异，所以任何想在国际上销售产品和服务的系统都可能需要体现这一点。

许多国家和地方政府，已经考虑对在线商务征收新税种。目前，许多人已经强烈地感觉到这种税收会阻碍因特网商务系统的发展和采用。现在还不清楚什么新税种（如果有的话）可能影响在线商务。无论如何，在线企业对可能影响它们运作的各种变化保持警惕是很重要的。

2.6.2 数字签名

现实中，个人手写签名用于许多商业文件，表明该企业同意文件中陈述的内容或认可描述的行为。我们普遍接受：签名是个人惟一的，不能伪造。电子文件无法用手签，不过加密学可以给我们一个工具：数字签名，以达到同样目的。我们在第12章讨论数字签名的技术，现在，懂得电子文件签名就如签名那样可用于许多方面就够了。例如，电子合同可由双方数字签定，就如今天双方用手签合同那样。

美国的几个州已通过或正在考虑通过立法，承认数字签名在一定情况下具有法律约束力。目前，没有任何此类法律，也没有联邦法律来限制美国国内使用数字签名。尽管数字签名可以很容易地用于在线商务的其他目的，但是在需要用签名来约束的情况下，数字签名仍应慎用。人们正在进行多方努力以发挥和协调州立法，但是，这方面的变化仍然很快。此外，国际上对数字签名决不可能有一致的意见，所以，在国际商务中，必须特别慎用数字签名。

2.6.3 版权

通过专利和版权来保护知识产权，这始终是美国国内法律上的重大事项。虽然全国情况各不相同，但这正逐渐趋于合理化，因特网的到来使之变得紧迫了。许多因特网内容供应商对版权特别感兴趣。因为信息以数字形式提供，很容易被复制、修改和传播却未经许可或未向版权所有者付版费。

在因特网上，知识产权的使用和保护有法律和技术两方面的问题。我们在第4章探讨某些技术上的问题，我们提出以世界知识产权组织（WIPO：http://www.wipo.org）为框架，来设计在线知识产权保护，以国际数字对象鉴定基金会（DOI：http://www.doi.org）为方法，来设计统一鉴别在线文件。

2.6.4 加密学规定

为因特网商务提供安全保障最基本的是使用加密学。加密学包含加密数据以保护隐私，提供验明身份的可靠方法，记录数字签名，保证信息和文件不被篡改。在第12章描述加密学的技术细节。

各级政府长期以来对加密学很感兴趣，因为它在信息保护方面起着作用。有时，密码技术的使用和销售是有规定的（当然，各国都有不同的规定）。尤其在美国，禁止出口大众化软件的强加密术，这使美国公司难以向国外销售安全性很强的产品。由于军事上也应用加密学，密码系统被当作军需品。现在，美国一般不限制美国公民在国内使用加密学，其他国家如法国则对进口和使用密码系统有规定。

在某些情况下，对出口控制方面，美国的确是个例外。尤其是，通常可以出口单用途的金融交易加密信息系统，但是，每一产品必须获得特别出口许可证。

对美国在线企业来说，上述问题通常与它们毫不相干，除非该企业在制造和销售加密软件。然而，这些规定对全世界因特网商务系统的安全产生影响，特别影响到美国企业与国外客户的交易。如果客户系统安全性差，那么整个交易的安全性也差。此外，缺乏一致方法，要树立对全球因特网商务基础设施安全的信任就难得多。

2.6.5 不确定的问题

在线商务的重大风险是，这么多的法律问题仍悬而未决。在美国，法律系统必须改进，这是很清楚的，至少要有点改变，以适应各种挑战。在美国国会和州议会，法律体系的改变将有所进展，但许多最重要的改变会来自各级法院，当它们把现行法律与先例运用到在线商务案例时就会出现变化。由于许多技术问题是复杂的，难以预言法庭在许多情况下会如何规定。

我们认为，从事因特网商务，收益大于风险。不过，随着公司开始介入，它们不应忘记有关的法律问题，注意确保它们明白其中的含义，明白它们的行动存在着内在风险。

软件开发商的一个相关问题是专利问题，因特网软件发展迅速，许多公司正在谋求知识产权专利保护。在研究中，没有实际付出，可能很难懂得某些新思路是不是创新，或者是否需要申请专利。此外，技术创新如此之快，延误两三年申请专利，这可是一件真正关系重大的事情。

2.7 总结

商业价值链给了我们一个有用的方法，用来考虑因特网商务项目。通过聚焦于交给客户的价值，而不是技术，我们可以更毫不犹豫地懂得，在应用中，我们需要收集哪些部分。然后，牢牢记住客户价值这一思路，我们就可以制定商业策略了，这是下一章的主题。

第 3 章因特网商业策略

最佳思路是共同的财富。
———卢修斯·安纳尔斯·塞尼卡 ①

3.1 商业和技术革命

本章提出关于因特网商业策略的某些思路，这些思路代表了希卡·戈什和其他人在开放市场方面的思想，而不是作者的创造性努力结果（我们是技术专家，不是商业梦想家），但我们用自己的语言改写了它们。

一本讲因特网商务系统设计的书，其中用一章写粗线条的商业策略，这似乎很可笑。我们却认为，这很有意义。因为，因特网改变了商业基本假设背后如此之多的事实。亚马逊公司的杰夫·贝佐斯提出：技术创新和基础设施改进，在两个阶段或者说两个波段中，对商业产生了影响。第一波是，公司用新技术改变了旧程序和商业模式；第二波也是更重要的一波是，公司用新技术开创了全新的企业。我们看到，上一次商业发生重要变化是在 19 世纪中叶，当时铁路改变了世界，并持续了 50 年；因特网也使商业发生了同样重要的变化，改变了世界，不过，这一变化的脚步快得多了。

由于因特网引领的变化速度快，范围广，所以，因特网商务系统的设计者不能只局限于技术，还必须领会自己公司的基本商业策略；而企业领导者则必须足够重视技术，从新竞争机会和新竞争威胁这两方面来通盘考虑企业的策略。

3.2 历史的雷同

很少有创新能够改变整个商业的竞争环境。在我们一生中，只有因特网有潜力对商业产生影响，这种影响与 19 世纪铁路对商业的影响一样大。“铁路网对美国的影响是史无前例的”。② 要懂得因特网的商业潜力，必须先了解铁路。

1825 年，美国开始引入铁路，至 1890 年，铁路已经是美国主要的运输方式了。请细想想这一时期所发生的变化，其变化如表 3.1 所示：

---

①卢修斯·安纳尔斯·塞尼卡《书信》。

②艾尔弗雷德 D·钱德勒和理查德S·特德洛著《管理资本主义的来临——美国经济制度历史汇编》(1985 年，《理查德 D·欧文》)。

表 3.1 铁路运输产生的变化

有铁路前	有铁路后
纽约到波士顿之间的旅行需 4 天时间	纽约到波士顿之间的旅行需要不到 1 天时间
运输依靠天气和水路	运输依靠铁路铺轨能力
劳动力分散（1830 年，人口的 92% 为农村人口）	劳动力集中（1920 年，人口的 50% 为城市人口）
8000 个时区	4 个时区
在家附近休假（如果有的话）	离家休假
运费：5～15 美分 /吨英里（1825 年，用运货马车或轮船）	运费：1 美分 /吨英里（1884 年，用铁路）

今日的因特网和 19 世纪的铁路有惊人的雷同，不过因特网的发展变化快多了。仔细想一想表 3.2 中所示的某些要素，最后一条特别重要：铁路和因特网促使经济发生了根本性变化。以铁路为例，廉价运输促进了工业革命，其关键推动力是蒸汽机；以因特网为例，廉价通信促进了信息时代的发展，其关键推动力是计算机。以太网计算机网络发明者之一鲍勃·梅特卡夫用梅特卡夫定律来解释这一结果，他说：“随着网络连接点数量成乘方的增加，网络的功效也提升了。”工厂之间可以通过铁路相互发送商品，这促进了工业革命。同样，计算机可以相互发送信息，这也促进了信息时代的发展。

表 3.2 铁路与因特网比较图

	铁路（1825~1890）	因特网（1969~1997）
新设施	初次不依靠水运的运输设施	初次全球公共信息设施
原来目的（非商业）	客运、军事	军事和民防、研究
重要标准	铁轨宽度（标准度量）	网络通信协议（TCP/IP）
安全的新挑战	雇佣铁路警察制止新犯罪	安全协议和标准
改革起因	钢铁生产、会计学、后勤学	软件、计算机联网、纤维光学
促进经济发展基本趋势	工业时代（关键推动力：蒸汽机）	信息时代（关键推动力：计算机）

从铁路和因特网对商业的影响这个角度看，今天的因特网也和 19 世纪的铁路有着惊人的雷同，请考虑以下因素：

- 规模经济

铁路使大型矿业和农业活动获得实效；因特网可以由一个商店如亚马逊书店或 CDNow 来提供大量标题。

- 竞争优势来源

有了运输，地区就有了竞争优势，如法国葡萄园控制了葡萄酒市场；有了因特网，一个站点如 Travelocity 就可以提供全方位服务。

- 存货需要

煤炭及时到货，工厂不需很多能源库存就能运转；由于因特网可以即刻发送信息商品的完整复制件，数字商品商业站点根本不需储存。

- 多样性、选择性和可用性

有了快速运输，易腐烂的商品如鱼和水果就可以运到更多更广的地方去；有了因特网，就可以排除限制信息市场发展的发送瓶颈。

- 新机会

利用规模经济，铁路实际上造就了许多大公司，工业时代最早的大公司本身就是铁路公司；同样，因特网的机会，就是让 Netscale、CNet 和 Yahoo！极为迅速地成长到真正的规模。

3.3 因特网价值取向

从事因特网商务需要从制定策略开始，分析策略要从价值开始。因特网的价值从何而来？我们认为因特网可以改变商业前景，这源于两种关键思路：其一，因特网可用来改变客户关系；其二，因特网可以转换传统商业价值来源。这两种思路依次引出企业的 4 个基本策略，这是在利用因特网和保护自己免受竞争对手侵害时要考虑的事项。

3.3.1 改变客户关系

利用因特网，传统商业的许多方面可以从“以供应商为中心”转化为“以客户为中心”，如表 3.3 所示。这一思路引出了两个商业策略，以客户为中心的企业所组织的活动都围绕着产品或围绕着满足某一客户群体的一切需要来进行，我们把第一个策略叫做“通道主人”策略，把第二个策略叫做“客户吸引”策略。

表 3.3 改变客户关系

以供应商为中心	以客户为中心
供应商选择交易时间	供应商随叫随到，客户选择时间
供应商选择服务点	服务送到客户手中
供应商递送服务	客户自我服务
侧重供应链	侧重客户需求
一对多	一对一

3.3.2 转换价值来源

因特网使商业从物质世界转换到信息世界，从处理原子转变为处理二进制数字，这一转变的结果如表 3.4 所示。侧重供应链，引出了第三个策略，我们叫做“价值链翻版”；侧重发送到客户手中，引出了第四个策略，我们叫做“数字分销商”。

表 3.4 转换价值来源

物质世界	信息世界
原子	二进制数字
物质价值	数字价值
规模经济	范围经济
大众化生产	大众化定制
信息价值	知识价值
分配是限制	分配是动力
本地	全球

3.4 四个策略

利用因特网改变客户关系和转换传统价值来源，这两种关键思路引出 4 个因特网商业策略：通道主人、客户吸引、价值链翻版和数字分销商。在许多情况下，综合应用这些策略可能也是很有益的。

3.4.1 通道主人

通道主人策略的作用是，利用因特网与客户加深友好关系，以销售传统商品和服务。通道主人是围绕产品来组织所有活动，集中于最大限度地将产品及其服务销售给客户。企业应用通道主人策略，要重新设计面向客户的一切活动：通道主人策略必须把商业价值链与现有的运作结合起来。

实例：Cisco 公司

Cisco系统公司是价值70亿美元的因特网软硬件和服务供应商，它用自己的Web网站作为销售通道，向其客户和合作伙伴销售。1997年秋，其因特网通道操作的年销售额是30亿美元。

- 吸引——让客户产生兴趣、保持兴趣

Cisco提供一整套在线商品目录和订货程序说明，将所列产品的价格变动情况通知客户。

- 互动——让客户从感兴趣转变为下订单

在线商品目录可以搜索、浏览和提出购买配置，智能代理提出可采用的方法（如软件升级）与识别错误。

- 行动——协调订单履行

订单连接到订购和订单管理数据库。客户可以跟踪订单执行情况或收到订单情况的通知，并查看提前时间。

- 响应——提供售后服务

客户可以访问综合文挡和自助智能代理，故障报警系统自动向客户报警。

Cisco 获得的结果是惊人的：70%的产品支持通过因特网交货，而现在有很大部分的订单通过因特网通道接收。

3.4.2 客户吸引

客户吸引策略的作用是，利用因特网以吸引一群客户。具体做法是，用知识共享环境和访问供应商名册，满足客户广泛的共同需要。客户吸引围绕着一群客户来组织活动，向他们销售各种各样的产品和服务。公司用客户吸引策略，寻求的是选定一整群客户。客户吸引必须把多个供应商的价值链集合成一个面向客户的整体。

实例：Tripod 公司

Tripod 第 X 代电子社区，它的目标客户年龄在 18～34 岁之间，这是一群就金钱、健康和职业问题需要求教于人的人。此外，Tripod还提供信息，鼓励和帮助其成员设立自己的Web网站。

- 吸引——让客户产生兴趣、保持兴趣

  Tripod通过连接许多站点提供免费信息，会员参加讨论小组、调查和当前话题实时讨论会。
- 互动——让客户从感兴趣转变为下订单

  Tripod 与安全第一网络银行（SFNB）合作，提供 SFNB 家庭银行服务定制接口。
- 行动——协调订单履行

  SFNB 在因特网上提供家庭银行，包括 24 小时报送账户信息。
- 响应——提供售后服务

SFNB 提供 24 小时客户服务，Tripod 还提供在线论坛，提出理财意见。

到 1997 年 5 月，Tripod 已发展到有 32 万会员，预计年收益 100 万美元。

3.4.3 价值链翻版

价值链翻版的作用是，通过从别人的价值链中取而代之，来获得利润差价。价值链翻版围绕着价值链来组织活动，寻求超越上、下游供应商，力求使供应商和客户有更直接的联系。企业利用价值链翻版策略，就是要最有效地利用价值链，以谋求其中地位。价值链翻版必须用商业价值链来支持一个全新而直接的买主与供应商之间的友好关系。

实例：ONSALE 公司

ONSALE在Web网上销售计算机和家用电器，它取代传统零售渠道进行24小时在线交互拍卖。

- 吸引——让客户产生兴趣、保持兴趣

ONSALE 把即将到来的拍卖消息通知客户，客户对这些信息很感兴趣，因为 ONSALE 是根据客户的个人资料来发通知的。

● 互动——让客户从感兴趣转变为下订单

拍卖每天 24 小时进行，竞拍者可跟踪实时柜台拍卖。

● 行动——协调订单履行

ONSALE 自动开出账单、装运并可通过因特网进行跟踪。

● 响应——提供售后服务

客户咨询由 E-mail 和在线跟踪系统来处理，客户资料保存下来以备回头客再使用。

1996 年春以来，ONSALE 始终赢利，并在头一年半的经营中获得了 6 万个客户。

3.4.4 数字分销商

数字分销商策略的作用是，不断冲击传统价值取向，重点是将有价物件交给客户，在因特网上可以做得更好。公司应用数字分销商策略，围绕着让传统销售链瓦解来组织活动，因为在因特网上销售产品和服务，效率可以很高。数字分销商必须从零开始建立一个全新的客户价值链。

实例：Classifieds2000

Classifieds2000 提供 Web 网分类广告。它在广告业与报纸展开竞争，收益的惟一来源是公司广告。

● 吸引——让客户产生兴趣、保持兴趣

Classifieds2000 提供自由链接到相关购物站点的服务（如买车族站点“凯利蓝色书刊”——Kelley Blue Book）。

● 互动——让客户从感兴趣转变为下订单

通过“绝妙通知”服务，Classifieds2000 把 E-mail 发到客户那里，请他们关注邮件中有关他们想买商品的资料。

● 行动——协调订单履行

Classifieds2000 链接 Trade-direct（直接交易），扮演着交易中介角色，接受信用卡交易，还可以在线跟踪订单。

● 响应——提供售后服务

Classifieds2000 提供动态报告给其广告客户，让他们能评估自己广告的有效性。

Classifieds2000 每周列出 5 亿美元以上的商品和服务项目。

3.5 新竞争威胁

威胁来自四个因特网商业策略，竞争对手可以单独使用，也可以结合应用，每一个策略都会给企业带来不同的威胁。

- 通道主人

竞争对手可以建立更优越的客户通道吗？你的客户会受到竞争对手的诱惑，因为经过全面考虑，他做到了价格更优惠，服务更好，购物更便利。

- 客户吸引

竞争对手可以吸引你的客户并把产品卖给他们吗？你可能失去客户群，因为有人提供更多的服务，你被迫成为竞争对手的商品批发商以求生存。

- 价值链翻版

竞争对手可以抢占你在价值链中的位置吗？你的供应商可能会越过你直接向你的客户销售；你的分销商可能会从你的供应商手中直接获取零配件。

- 数字分销商

竞争对手可以瓦解你的价值取向吗？如果你的价值取向基础是聚合商品与服务，竞争对手运用得当，有可能在其中某些方面胜过你。

上述问题的答案只能在具体商业态势的前因后果中去寻找，不过，有个例子可能很有启发性，请看看全方位服务的传统经纪业，它需要从因特网的角度来分析自己的竞争态势。其价值取向是“一站购物”，既销售分析文章又提供交易服务。竞争对手采用四种策略之一，会出现什么情况呢？

- 通道主人

有个中间商，如MerrillLynch（梅里尔·林奇），在线开展消费者中介服务，向你的某些客户提供更便利的全功能通道，销售的产品和服务基本和你相同。

- 客户吸引

MotleyFool（杂色愚人）设立热心投资者社区，在他们旗下，可以提供潜在商品化的经纪服务。

- 价值链翻版

在线新经纪人E*Trade（电子交易）正在把传统经纪人从价值链中挤出去。

- 数字分销商

WallStreetCity（华尔街城）只销售分析文章，但却不在自己的Web网站上提供交易服务。

3.6 新竞争机会

竞争威胁也有其双重性，即他们也带来新竞争机会。同样，对4个商业策略也必须这样分析：每一个策略对企业都有其适用性。

- 通道主人

你可以降低成本，更便利客户，提高定制能力，让客户享受更多的服务吗？

- 客户吸引

你的客户有各种各样的需要，这有助于推出产品和服务的新品种吗？

- 价值链翻版

你可以越过直接供应商或客户，获取差价吗？

- 数字分销商

你可以在因特网上提供其他公司价值取向中的哪些部分，以便做得更出色呢？你可以提供哪些新东西，使自己的销售和服务更具吸引力呢？

3.7 总结

我们提倡用三部曲来选择和实施因特网商业策略：选择某个策略，设计商业价值链，实施逐渐形成的解决方案。

第一阶段，从潜在竞争机会和潜在竞争威胁这两个角度，把商业策略通盘考虑周全。你愿意做通道主人、客户吸引、价值链翻版或数字分销商吗？或者说结合应用这些策略正确吗？这一过程会引导你树立起“实际的价值取向”。

第二阶段，思考商业价值链的每一步骤，思考你原来更喜欢的方法：吸引客户、与客户互动、订单行动和客户服务请求响应，我们提出“最彻底”的方法是，侧重企业方方面面与客户的友好关系。

最后阶段，设计一个举一反三的实施方案，以免在技术创新和市场变换时感到惊慌失措。

第 4 章商业模式——类别研究

最美妙的和谐来自千差万别的事物。
——赫拉克利图斯 ①

4.1 商业类别初步

我们在本书中选出三个商业类别，供系统需要和设计选择时作详细的考虑。

- 消费者零售

企业直接向最终消费者个人销售物质商品就叫做消费者零售。我们再把零售企业分成因特网综合大企业和因特网基础中小企业（预算较小）。

- B2B 编目

带有在线商品目录的企业向其他企业销售产品就叫做B2B编目。我们侧重于MRO（维护、修理和操作）商品，而不是COGS（商品成本和服务）订单。COGS通常指大批量订单生产，虽然这类企业也使用联机系统和一些技术如EDI（电子数据交换），但到商品投产时，却还见不到零部件商品目录发行。我们这里的确特指使用在线商品目录，让设计者挑选产品生产用的零部件。

- 信息商务

信息商务范围很广，不过，我们指打算在线发送数字商品（信息产品和服务）并履行订单服务的企业。在线杂志出版商和在线发行软件，虽然差异极大，也包括在其中，其基本特点是在线履行。

就推销来说，商业类别是同一行业各公司的集合，如客车制造商或报业出版商，他们的产品和服务有类似的要求。这里，我们用“ 类别 ”这个词来描述因特网商务中有类似要求的企业集合，不管它们的行业是否相同。

4.1.1 类别细分、市场规模和定时

类别一直可以细分下去，如报业出版商可以再分为有广大市场的日报和社会周刊。因特网

①赫拉克利图斯《论宇宙》

商务类别，如信息商务可分为出版物、软件发行和信息服务。信息服务可再细分为信息搜索检索、保留和金融服务。

我们有多种理由来划分市场或技术领域，不过这归结为聚焦，聚焦就是指精确地集中在要素上，即集中在应用或市场中最基本的要素上；而不是将精力集中在那些客户不需要或不喜欢的要素上。

类别细分是个难题，如果某一类别涉及面太广，所有必要的特点就得不到发挥；如果涉及面太窄，市场很小，不足以维持企业。

4.1.2 类别的异同点

我们的三个类别在要求上极为相似，都需要吸引客户、展示产品、收集订单、进行交易、完成履行程序和提供客户服务。我们集中谈这些共同要素，不过也谈一下其中某些有极大差异要求的方面。作为一个实例，零售极需要推销能力，而 B2B 应用则可能有非同寻常的订单支付要求和批准工作流程要求。

信息商务可能是三个类别中最独特的，因为信息企业可能不需要发送物质商品，也不需要有相应的客户服务机构，不过，它在在线履行方面会有极为复杂的要求。

4.1.3 商业价值链

为和前面章节保持一致，我们在讨论这三个类别时应用图 2-1 中所示的商业价值链结构。

- 吸引——打广告和推销
- 互动——内容
- 行动——订单处理、支付和履行
- 响应——客户服务

为和本书的系统设计结构保持一致，我们将价值链的交易程序阶段分成订单处理、支付和履行。

4.2 消费者零售

这部分讨论企业直接向最终消费者个人销售商品的商业价值链。

4.2.1 价值取向

消费者零售的价值取向在三个类别中可能是最不确定的，讨论它有多种方法。面向全球廉价发送准确信息，会创造更多的机会。

- 可以面向全球市场
  由于因特网面向全世界消费者，地方小企业可以借此直接面向全球，其结果可能是，销售增加，成本最低；另一个观点是，面向全世界，就可以有一定的客户群，这可能会产生一个全新的零售商阶层。
- 削减推销和销售费用
  直接推销，商品目录的编制和发送成本就相当于实际销售成本。在线商品目录，内容编制成本可能会高于传统商品目录，不过，却可以大大缩减印刷和邮寄成本。
- 运作效率不断提高
  在传统商品目录订单企业，订单加工通过电话和邮寄来联系，属于劳动密集型过程；在因特网上，消费者下一个完整订单的工作要多得多，下完订单自动进入订单处理系统，此外，客户可用网络进行自我服务和咨询而不需接线生。
- 对消费者更有的放矢
  在线和站点互动，推销时就可以“小范围播送”给目标客户。纸印的商品目录，要对潜在客户印上不同内容，这并不现实；而在因特网上，这种“一对一推销”则完全可能。
- 传递更准确的产品信息和可用信息
  与印刷商品目录相比，在线商品目录的内容更改更加容易，可以做到准确及时。在线商品目录可以标出产品准确库存数，还可以用来销售存货很少的产品，由于存货少，印刷商品目录不会印出库存数。

4.2.2 系统功能性

零售企业的规模有大有小，从小商店到全国性大型综合企业，大企业从事因特网商务比起小企业来自然会有更复杂的要求。

- 小型商店
  小企业可能有相对固定的商品目录和简单的保留业务记录要求。商店的商品目录使用商用桌面发布应用软件，由Web站点服务公司操作。订单由商业服务供应商[②]收集再发传真到商店。在线支付可采用信用卡，或没有任何要求。客户服务大多通过电话就很容易地处理了。典型的推销方法是优惠券或特卖销售。
- 中型直销商
  中型直销商的在线商品目录是按商品品种（SKU，即存货品种）来编制的。它根据产品数据库来编制，这种数据库有显示模板来动态生成商品目录页面；或者由商品目录桌面创作系统编制，这种系统可以生成产品页面。在线定货要求要有“购物推车”特点、

②商业服务供应商是在外包基础上提供因特网交易服务的公司。

税收和运费计算、信用卡支付，以及可以用电子传输方法传送到商店。只要规模够大，还应包括客户登记数据库和在线客户服务系统。推销方法有优惠券、促销、特卖，也许还会有会员打折制。

- 大型零售商
  这种要求最高的零售商需要一个高度动态的Web网站，以处理变动频繁的产品和价格。产品展示要与现有存货联系起来。订单接收包括个人标号、传统信用卡和分期支付购物。订单可以用电子传输方法传到零售商的ERP系统（企业资源计划系统③）。推销方法非常复杂，有“一对一推销”和交叉销售（提出附属产品或补充产品）。向全球销售最重要的是，要有使用多种语言和多种货币的支持系统。

有了这些总提纲，我们就可以更详细地谈这些系统的各个部分了。

4.2.3 吸引——广告和推销

吸引客户有多种多样活动如打广告、发优惠券、促销、特卖、老主顾方案以及类似的方法，我们把这些活动统称为“推销”，用来树立品牌意识，吸引客户，刺激客户的购买欲。在某种程度上，这些活动形成了商业价值链的多重要素，例如，有人可能因为有了优惠券而去购物。

- 打广告
  打广告使商家和产品出现在客户眼前，不管是在商店里，如“访问我们的家用器皿部”，或在商店外，如公共汽车车身。在因特网上，打广告有多种形式，包括在著名站点放置大字标题、E-mail业务通信，或只在用途广泛的搜索引擎上列出目录。打广告通常是零售商花费的一种费用，而对从事信息商务的商家来说却是一种收入。
- 优惠券
  零售商的优惠券特别给消费者一个让利价。优惠券可能表现为广告的一部分，也可能在结账收银台分发，或在购物活动中产生。优惠券用来树立产品意识，推荐消费者试用，希望他们能改用新品牌。因特网数字优惠券可以直接链接到交易服务系统。
- 特卖
  特卖指一段时间的产品特价，也许带有限量销售。特卖用作普通促销，为的是建立客户群，提高知名度（配合广告），也用作清理存货积压，如在主要假日之后。
- 促销
  特卖和优惠券是促销的实例，不过促销可以相当复杂，甚至可以包括向不同零售商购买捆绑商品的特价，如小夜礼服、蛋糕和度蜜月可能作为一整套结婚礼包来销售。

---

③企业资源计划系统是一般术语，包括会计系统、生产计划以及其他紧要使命商业应用系统。

- 老主顾方案
  老主顾方案与其他客户忠心方案是针对老主顾的促销活动，例如，积满分数的老主顾可以获得优惠款，无论他们买的是商品还是服务。既然这种积分在别的零售商那里无效，就会刺激消费者集中向一个或几个零售商买东西。
- 一对一推销
  零售商总想尽量多了解他的客户。当相同产品或多或少在几个地方都可以买到时，零售商就会以便利、价格和服务质量来展开竞争。因特网转移了地理上的便利，价格在竞争中总是个难点，剩下的就是服务质量了。对客户了解得多，这有助于零售商提供高品质的服务。

一对一推销一般指系统定制符合消费者个人标准，它包括如建立消费者个人资料和生成用户专用内容。

4.2.4 互动——内容

最简单的方法就是把因特网商务零售内容看成在线的直销商品目录。大体说来，的确如此。不过，因特网是一个平台，可以向全世界数百万小商家提供商业服务，对它们来说，商业化的商品目录简单桌面出版系统就很适用；对有数百种商品的商店来说，它的商品目录可以由推销员或熟悉桌面出版系统的人来编制和修改。

再往大的说，大型零售商的价格与产品变换频繁，简单的桌面发布系统难以支持，就要使用桌面数据库，即创作工具加上动态生成 Web 内容的在线数据库所组成的桌面数据库。

在市场最复杂的收尾阶段，迫于实时存货信息需要，就要用动态商品目录了。该技术很复杂，需要动态信息系统支持。

无论如何，有必要把客户吸引到 Web 网站或在线商品目录上，可以采用如下方法：

- 在因特网搜索引擎注册
- 超文本链接传统菜单、商品目录和广告
- 在因特网著名或相关网站上打广告

4.2.5 行动——订单处理

零售交易订单处理的功能包括以下活动：

- “购物推车”或者说订单汇集功能
  在因特网上，“购物推车”并非实际中的那一种，而是一个逻辑上的选购商品数据库，这种“购物推车”可以让买主更改数量，更改商品品种的不同包装，还可以采用超文本链接到产生商品条目的商品目录页面中。

“电子购物推车”还可以累积优惠券，同种商品标出有多个商家销售，以便货比三家，促进销售。

- 验证订单

  按种种商业规则来验证订单可能是适宜的，例如，一个PAL制式电视机在北美就无法收看，只有许多计算机系统零部件而没有必要的连接线就成不了一个完整的系统。商家可能不会阻止不可靠的订单通行，不过，提请买主注意这一点，可能会减少下游退货成本和客户服务成本。

- 应用优惠券或其他打折方法

  优惠券和其他推销方式，如合理流程和数量打折，逻辑上可用于下订单全过程。原则上，订单汇集功能可以辨别几组商品（有套装价）是选购套装，还是选购散装。

- 交叉销售

  向买主提供额外商品可能是适宜的，这取决于“购物推车”的当前内容，或以前的购物情况（后者只有当知道买主身份才可以这样做，因为“购物推车”可能已经注册，也可能没有姓名）。例如，购买手电可以顺便提供电池。

- 计算营业税和其他税

  营业税有复杂规定，涉及产品税目、买主和卖主所在地及其征税情况。美国的州、县、市各级政府就管辖着6 000个以上的征税区。在其他地方，加拿大就有省营业税（PST）和国家商品与服务税（GST）；在欧洲则有一套复杂的增值税（VAT）。因特网商务系统必须正确地处理这些复杂的事情。

- 计算运费

  在线物质商品的订单，多数商品是要发出去，而不是收回来。有些商品的价格可能已经包含了运费，但经常的是，运费要另外算。发货可选用不同方式（一夜工夫、2天或依情况而定），那么，运费就要由商品数量、重量和价值来决定。

- 订单汇集表示方法

  重要的是，要让客户知道什么东西卖什么价格，这既有助于消费者接受新媒体，又可以减少下游客户服务、退货和争议处理的成本。

一旦最后订单确认下来，买主会选择支付方式，这可能会出现支付方式决定价格的情况，在这种情况下，选择支付方式就被看作是订单处理的一部分。

4.2.6 行动——支付

现实中，商品零售大部分以现金、赊销、支票或支付卡方式支付。支付卡可以再分为信用卡、收费卡和记账卡。我们在本章里讨论支付技术，每一种方式都有其电子支付的模拟方式，不过，现在我们感兴趣的是，很快地概括这些方式的商业特点。

现金

- 现金是持有人的证件
  使用现金，卖主就不必对买主有所怀疑，假定伪币不是个问题！因为价值体现在现金这一“证件”里，而且立即从买主手里转移到卖主手里；反之，买主一旦付了款，倒是要托付卖主发货。
- 现金不记名
  收现金，卖主无须知道买主的身份。现金还适用于买主不要票据的交易。在因特网上，跟踪买主的其他方法，包括物质商品的交货地址，这可能限制了现金这一特点的实用性。
- 现金适用于小笔交易
  由于现金交易的费用可能很小，适用于小笔购物。然而，处理现金的全部系统费用，包括计算、储存、安全、错误和盗窃等可能很高，因此分析现金的这一特点时应当慎之。

赊销

过去零售企业赊销给顾客是很普遍的，现在服务行业仍然很普遍(电、电话)，不过在零售业已经相当少了。许多公司借助信用卡来树立自己的品牌，这是题外话。赊销作为一种高效处理小笔交易的方式，在因特网上能起更大的作用，我们会在信息商务那一节来考虑这个问题。

支票

支票是买主的一道命令，他命令指定银行向卖主支付与货等值的款项。

- 支票没有保证
  一张支票只有在银行账上有足够的存款，才可以兑现，这才是真正有保证的，这时，价值实际上就从买主账户转到了卖主账户。支票资金不能用来支持检查，否则买主可能止付。
- 支票需要鉴定
  卖主一般不知道买主是否有权开出指定账户的支票。此外，一张支票如果伪造，就是无效的。由于没有保证，就要冒不支付的风险，换句话说，支票与开支票的人没有显而易见的联系，这就是为什么卖主要求买主出示其他身份证明，以及为什么会有支票担保服务的原因了。
- 支票是一份合同
  即使支票止付了，签出的支票可能代表买卖双方的一份合同，仍然可用于收款。

接受了支票，卖主也就承担了一定的不支付风险；另一方面，卖主不支付给别人而承担这一风险。

记账卡

记账卡是一种支付卡，它直接把资金从买主银行账户转到卖主那里，它在欧洲和远东广为使用，在北美就不那么广泛了。记账卡对卖主有利，因为支付有保证又及时，交易费用又比信用卡来得低；记账卡可能对买主比较不利，因为（在美国）记账卡不向消费者提供消费者信用保护条例的法律保护。

信用卡和收费卡

信用卡无所不在，几乎没有人了解其复杂性。附带说一下，收费卡是一种购物卡，它不能延期支付，每月账单一到，就要足额支付。信用卡的操作框架是由卡协会规则（Visa、MasteCcard 和 American Express 等）提供的，在美国，是由消费者信用保护条例提供的。

从卖主角度看，引人注目的事实如下：

- **信用卡有可能保证支付，也可能相反**
  持卡人出示信用卡，零售职员履行所有步骤如提出要求、核对签名及获得实时授权，那么卡协会就保证支付。但在其他情况下，如邮购、电话订购或其他没有出示信用卡的交易，商家可能得承担更多的不支付风险。
- **信用卡有实际交易手续费**
  买主用信用卡购物，卖主通常要付百分之几货值的手续费，手续费通常有两部分：处理授权信息等方法的各方收取一律相同的手续费，1 %手续费给收款行（特别是卖主账户银行）和发卡行（特别是买主账户银行），因为它们要承担风险，全部手续费可能约为 25 美分加 2 %。这一手续费结构意味着，交易额越小，实际的百分比交易成本就越高。因此，使用信用卡买 25 美分的东西，结果是卖主净亏。现实中，典型事务通常不会有问题，因为 Visa 卡平均交易额通常要大得多如 70 美元。

从买主角度看，信用卡提供了若干保护。

- **保护被盗用**
  美国消费者信用保护条例提出，一经发卡行通知丢失或被盗，持卡人对非授权费用不负法律责任，无论何时，持卡人对 50 美元以上非授权费用不负法律责任。这一原则生效，就是说发卡行和信用卡系统操作员应负责保证系统有足够的安全。
- **能够验证商家**
  消费者有保证，一旦卖主接受了信用卡，消费者就得到了卖主真实的担保。如果发现卖主有欺诈行为，发卡行会保护持卡人不受侵害。这对因特网商务来说，是实实在在的好处，这样，买主不需用传统方法去探问商家的情况。
- **发卡行提供客户服务**
  一般说来，如果消费者用信用卡买了东西，引起纠纷，发卡行提供必要的单方交涉。遇

到卖主不履行，或甚至是商品质量很差，卖主可能违背已定的收费，因此有些支付卡还发放消费者保单和提供各种保险。

总结

与因特网商务最接近的是邮购商品目录，估计在不久的将来，在线零售商务很可能多数会采用信用卡。

4.2.7 行动——履行

履行涉及把订货商品发送到目的地的全过程，包括以下步骤：

- 把订货信息从销售点传递到仓库
- 包装和订单集合以备运输
- 运输和交货

  对物质商品，除了第一步骤，因特网商务和其他类型的零售商务有同样的履行问题，不过，接收订单可能有多种方式。
- 小企业

  小企业的Web存在，可能由不在本公司内的服务系统维持，当接收了订单，就必须把它们传递到企业履行功能系统，这可由传真来完成，由定期或加密E-mail来完成，或由查询在线待处理订单表来完成。
- 中型企业

  中型企业，尤其是有邮购业务的企业，可能想把在线订单和其他订单结合起来，这种结合可以用人工，也可以用自动化方式，这取决于预期的订单量。
- 大企业

  大企业从事因特网商务，一定极想把在网上接收的一连串订单和其他一系列订单结合起来，这种结合可能采取这样的方式，即直接链接因特网交易系统与企业现有订单管理系统或ERP系统。

支付与履行的关系

一般来说，货款要到卖主准备发货时才付。用信用卡支付时，卡协会一般要求：尽管授权是发生在销售点与成交之时，但结账资金实际上是在装运时才划转的，也就是说，履行服务系统一定会通知支付功能系统，或者说，支付结算部分可由履行服务系统管理。

4.2.8 响应——客户服务

因特网呈现了许多机会：提升客户服务价值和降低成本。关键的观察结果是，在多数情况下，客户服务代表起着“人工调制解调器”的作用，例如，在电话客户服务里，接线生接听打

进来的电话信息，并转入客户服务终端，然后读取屏幕上的信息再传回给打电话者。由于因特网将屏幕直接放在客户面前，客户就有机会自我服务，以简化成本结构，降低成本。

有机会改善服务

- 更强的服务能力
  因特网服务系统每周七天、每天 24 小时连续运行，不需要根据高峰时刻和季节来安排机动劳动力。通信线路遍及全球，“跟踪太阳”的通信支持系统，随白天时间在地球上推进，从一个支持中心转到另一个中心。
- 减少错误率
  可以避免“人工调制解调器”产生的错误，可以通过立即反馈和输入一步步自动确认来恢复客户看过的屏幕；使用在线形式，用户可以查看选择方框指示自己的意图，可以在计算机上立即完成计算，进一步减少错误。
- 丰富的信息渠道可使用
  没有必要限制只靠声音来获取信息，因此，可以通过图表、文本、图像、图形来获取信息。
- 自助或公共帮助
  “频繁问题”（FAQ）是客户自助的一种不错的格式。在客户服务中，随时都会提出相同的问题，这可以在可搜索的知识库里找到。
- 直接链接状态信息
  询问订单情况，可以在因特网上直接链接与参与方如运输和交货公司保持联系的网站。
- 前摄性信息发送
  产品特色信息、运输推迟信息和回顾信息可以用 E-mail“推送”给客户，或投送到客户的在线个人声明网页上。
- 多种语言支持
  使用几套独立 Web 网页以维持客户群使用的所有语言。

缩减成本费用的机会

客户自我服务电子系统有明显的节约效果。

- 缩减人员费用
  客户可以直接访问相关信息，机构所需的客户服务代表就可能更少，或可能在他们的工作时间内安排其他工作。
- 缩减实际设备费用
  传统呼叫中心规模可以更小，节省不动产如楼房、设备和运作费用。
- 缩减电信费用

因为因特网协议是分组交换，而不是电话交换，大量“呼叫”可以由类似的电信设施来处理。

4.3 B2B 编目

本节我们讨论维护、修理和操作类商品目录，以及产品零部件商品目录。MRO商品如办公用品、设备实际维修零部件和消耗品如清洁用品。这个商业领域的特点是购买量大，货值低，同一客户反复购买，买卖双方承担的订单处理费用高。

4.3.1 价值取向

让B2B商品目录在线，关键好处是，直接节省费用，且可以提供更好的服务。

- 缩减销售成本
  在线商品目录，其成本比纸印商品目录的印刷和发送成本低，且可以显示许多商业应用中需要的详细信息，这在纸印商品目录上很难做到。例如，工程师使用商品目录挑选新产品设计的零部件，一旦选中某一零件，常常需要使用其他服务如传真来获取详细的制图和图解，这些功能主要是基于信息的，它们可以在线处理。
- 缩减订单处理费用
  购买MRO商品往往订货量大，货值低，因此，订单处理费用可能很重要，通过自动处理订单流程，实际上可以缩减这些费用（处理一份订单，费用在50至300美元之间，由买卖双方分担）。
- 提高对小客户的服务水平
  有B2B商品目录的公司常对其最大客户提供特别服务。这些服务包括定制商品目录、特别谈判价格和订单集合，以传统方式提供这些服务时只针对大客户，因特网可以把这些增值特点用在小客户身上。
- 向客户提供高质量信息
  在线商品目录这个电子媒体是可以搜索的，它所包含的产品信息比纸印的详细得多，搜索使商品目录更易于使用，还可以有竞争优势，因为它的速度更快。人们有可能得到详细信息，因为万维网的超文本能力可以让用户点击商品目录的某一商品条目，以获取其下面详细的产品信息和应用信息。
- 准确的信息
  在线商品目录与纸印商品目录有所不同，它可以始终保持最新，始终保持准确的产品信息、可用性和实时最新的价格。

4.3.2 与消费者零售的不同点

我们脑中已有了消费者零售概念的基本情况，本节从 B2B 编目与消费者零售的差异这一角度来讨论它的商业需要。

4.3.3 吸引——打广告与推销

零售的许多推销技巧仍适用于B2B商务。卖主的关键问题是，吸引买方认同者的注意，成为一个合格的、最好是优选的卖主。

4.3.4 互动——内容

我们利用因特网商务销售 MRO 商品的模式就是在线商品目录。以高标准来说，企业商品目录非常像消费者商品目录，但也有些不同点。

搜索是基本的

企业商品目录内容可以很多，包含 5 万或 10 万种零部件是很常见的，因此，搜索能力是很基本的。对工业零部件来说，搜索方法不应有预定义分层。如果客户在寻找 2 英寸 90 度黄铜管，在任何个别订单中寻找这些特征，显然没有道理，解决这一问题，可采用一种叫做“参数搜索”的技巧。

在这个例子中，申购者可能面对着商品目录的数千种管配件。选定“黄铜”后，商品目录可能会告知有 3200 种黄铜管配件，选定“90 度角”后，可能减至 300 种，选定“2 英寸”可能再减至 10 种，同时显示各种连接管。一旦点击次数达到一定程度，就可以滚动一个详细完整的表来查看 10 种可能的管配件。

定制商品目录

企业之间生意往来多了，往往发展到有特别协议、特别价格，甚至设计别的客户没有的特别零部件。

- **特别零件数**
  因特网商业目录的电子性质使之可以出版不同的版本给每一个重要客户。展示的零件数可以是客户想要的数目，而不是供应商所给的零件数目，或者另加上供应商所给的零件数目。
- **特别价格**
  特别协议价或按数量标价可以直接体现于在线商品目录。
- **安全要求**
  为使某一客户的商业活动不让别的客户知道，B2B 商品目录比起零售来有更高的鉴别

和安全要求。例如，商品目录显示特别协议价给特定客户，只有那家客户的雇员可以访问这个商品目录。

4.3.5 行动——订单处理

B2B比之零售，其订单处理实际上可能更加复杂。在卖主方面，实时查看存货可利用性和查看订购一致性是可能的，和企业支付方法的订单处理部分也是相似的；在买主方面，订单处理可能会复杂得多。

批准工作流程

在企业订货方面，有多种角色：

- 申购者——申请买东西的人
- 准购者——批准货款的人
- 采购员——购货的人

在消费者购物中，上述角色通常由一个人担任；而在企业中，他们可能要分开，决不可能同一时间同一地点担任多种角色。采购员有办事员的角色作用，因特网商务的自动化可以减少这一角色作用的需要，允许它既是采购员又是申购者。

B2B应用基本的主要订单处理功能是批准工作流程系统，一旦订单形成，这个系统会让订单按流程得到合适的处理。另外的问题包括订单项目行明细要求、成本分配，以及细密地控制运输和交货。

授权

B2B应用系统的一项重要能力是指定用户可以授权给另一个用户。在消费者模式里，父母可以对孩子的在线购物能力有所控制，但在企业关联事务中，这方面的要求就要复杂得多。

- 部门管理者授权给部门人员，让他们登录及搜索供应商的商品目录。
- 经理授权给某个下属，允许他在经理休假期间批准购货事宜。

4.3.6 行动——支付

有另外几种支付方法适用于B2B商务。

订货指令

订货指令本身不是支付方法，而是通过直接支付仪器记载订货明细账以便后来结算。在销售点，订货指令将订单（尤其是参考数目）连接到交易机构的订单跟踪系统。在因特网商务中，只有交易机构与卖主就信用问题达成共识，以及买主经交易机构适当认证核准可以订购商品，这时，订货指令才会是一种可接受的支付方法。

采购卡

采购卡与信用卡的用法相同，但在企业商务方面有几个特别之处。采购卡的办法就是将采购权授予机构里的最基层人员，但他们必须提供高质量的报告，以便在财务上进行适当的管理。

- **商品类别限制**
  采购卡用于采购，不但要根据已树立的信用，还要根据商店的行业编码、买主的购物记载，或许还要加上产品销售信息（如果核准系统可以得到），才作出核准决定。交易机构为每一个买主建立适当的资料，允许每人每月购买 100 美元的办公用品，但不能买耐用品或食品。
  因特网商务系统的采购卡支持是指，系统将订单量及其他详细信息传送至卡核准网络。
- **报告**
  标准信用卡每月提供一份购物对账单，而采购卡要提供详细订购报告给交易机构，这通常都是用电子传输来实时提供的。

电子汇款（EFT）

电子汇款有点类似支票，因为它命令资金从某一账户转到另一账户。电子汇款同支票一样有一般固定费用，这与汇款数额无关，同样，它不承担客户服务的义务。电子汇款与其他支付方式不同，它的汇款速度很快（一天或马上），而且立刻提供汇款对账单。

在美国，实际上有两个 EFT 网络：一个是自动票据交换所（ACH）网络，用于工资自动转存、投资转账和账单支付；另一个是各种各样的自动柜员机（ATM）网络，用于收取现金，以及在煤气站和食品店使用记账卡④。ACH 网络汇款要一天才生效，而 ATM 网络的操作即时生效。

对因特网商务来说，EFT 支付比起支票来，往往有更即时的效果，还减少双方对信任方面的要求，成本结构费用也较信用卡和采购卡低。不过，ACH 网络以前实际上是为经常性支付所设，设立一个电子汇款机，有相当复杂的技术和管理程序；而 ATM 网络是为个人支付所设，通常需要有一个复杂的设施来安全处理个人身份识别号（PIN）。

4.3.7 行动——履行

B2B 的履行系统需要有一些附加要求。

- **预定交货点**
  当申购者订购了不需核查的中小商品，以及当订单很多不大可能进行事后核查时，履行系统可以提供一些附加保护措施，通过只准使用预定交货点来避免系统出错。这种

④、还有公共机构的泛美元交易网络，如 CHIPS 和 Fedwire。

能力通常属于订单处理的阶段，但却与履行系统有关。企业订货一定下来，系统就会提供一系列合理的预定交货点，申购者可以选择，但不可以更改。

- 订单集合

  企业向供应商传去许许多多的小订单，集中安排这些订单每日一次或每周一次运出，可以节省运输费用和一般费用。传统上这种订单集合采用人工处理，但电子系统使之更加容易，即使订单是个人下的，商务系统的履行阶段仍然可以认出某一共同交易机构及交货点，并把订单集合在一起运出。

- 多个交货点、定期交货

  企业经常会出现一个订货中心机构购买了大量必需品发往各个不同的地点的情况。在这种情况下，履行系统必须处理发往各不同交货点的事务，也许是依据订单项目行来处理。订单集合后，即使是只发往一个地点，履行系统也必须指示每一部分订单的最后目的地。

4.3.8 响应——客户服务

对 B2B 商务来说，我们把客户服务的范围扩大了，包括了在销售点之后的所有服务：培训、技术支持和软件维护，当然还包括传统客户服务内容。

- 培训

  对许多产品来说，在线培训可能是客户教育的一种有效方法。在线培训不同于纸印的培训指南，但却与计算机培训相同，它是高度互动的。培训系统不仅可以模拟训练，或访问实际产品（软件产品），还可以让指导者与学员在线联系。

- 软件维护

  软件维护是指发送补丁程序和升级版本的做法，软件产品每年都预收了固定费用，实际上是在购买软件最初版本时所收的预付费用。因特网是发行软件的理想通道，同样也适合于发送升级软件。购买软件时，卖主可能预收了一笔费用，以便让客户可以下载新发行的软件版本。

- 技术支持

  买了产品之后，许多公司还出售技术支持，这包括回答产品问题、指导应用、帮助操作错误等等。对技术性很高的设备和软件，网络可以用来进行远程诊断和维修。

卖主的另一个机会在于建立客户电子社区，在线论坛和常见问题文档可能是有效的客户自助方法。

4.4 信息商务

我们在本节讨论利用因特网商务来销售数字商品，这在网络上是可以实行的。

4.4.1 价值命题

在线信息商务的基本特点是，使传统发送链瓦解，并能够探索商业的新模式。

- 发送链瓦解
  在因特网上，信息供应商可以直接向信息消费者发送，而不需要另外的发送通道。首次实现发送产品给新客户，边际成本几乎等于零。而且，没有搁置空间和通道带宽的限制，不会人为增加发送费用。
- 商业模式
  由于媒体是最灵活的，信息供应商作为出版商和原创者，可以轻易地试验商业的新模式如软件出租、按次计费浏览文件和微型交易，同样也可以试验传统模式如打广告和订购。实际上，媒体的高效和交易费用的缩减使信息商务公司的规模变得小多了。

4.4.2 商业模式

信息商务的挑战之一是，人们如何赚钱？我们回顾一下信息商务的一些收益模式。

广告客户支持

内容供应商可以从广告获得收益。广告客户付钱为的是让人们有个印象，因为有许多“眼球”盯着他们的广告。一个站点的内容有趣诱人，会吸引许多访问者，广告客户就为此而付钱。如果这个站点还可以搜集访问者的信息，包括人口统计方面的信息，如年龄、性别、邮编，那么广告客户愿意付更多的钱。

万维网在技术上还能够通过点击用户数的统计来衡量广告的有效性。

订购服务

订购是传统印刷品的商业模式，在线也可以使用。在在线订购模式中，消费者支付循环手续费来不断访问信息。

捆绑约定

为了获得足够多的广泛信息来吸引访问者，内容所有者之间可以将访问权卖给对方的客户，没有直接从事内容业务的服务供应商也可以特许其用户访问内容。

文件销售

这一类别范围很广，例如，出售研究报告和个人文章，或在线销售和发行软件。

按用法收费

在这一模式中，用户按用法付费。用法可以包括许多属性如连接时间、搜索询问或查阅页数。信息产品如在线报刊和信息服务如搜索引擎或游戏都按此收费。

信息市场

由于因特网大大缩减了交易费用，这可以使最终信息供应商在巨大的信息市场上直接向最终消费者销售信息。也许最令人感兴趣的一系列问题是，信息中介者、发送者和收集者在其中起什么作用。

对信息市场的发展，下列各部分是必不可少的：

- 版权管理
  作者与出版商在线发送自己的信息，应当能够在某个标准格式中指定可以利用的信息。
- 容器
  容器就像一个信封，它保护要转移和销售前的信息。容器可以通过网络、只读光盘或广播自由发送。容器里的内容被购买后，容器就会解锁而展示内容。进行查看、打印和其他形式的访问，通常有不同的手续费。容器还可以用来防止指定客户将信息发送给非指定客户。
- 超级发送
  超级发送的概念包含安全容器的信息发送权编码。信息收集者可以买走发送权，重新发送容器里的内容，以及传递修改过的容器。当最终用户付了访问款，这些费用一部分归发送链，一部分归原作者。
- 交换所
  知识产权（版权管理）交换所和支付交换所是信息市场必不可少的组件。交换所向最终用户收取手续费，并按安全容器规定发送信息。

4.4.3 信息商务与消费者零售、B2B的不同点

本小节从信息商务与消费者零售、B2B编目的不同点这个角度来讨论信息商务的商业要求。

客户系统要求

前面讨论的商业类别，对购物者可能有相当复杂的要求，从Web浏览器能力或运行客户小应用程序能力的角度看，信息商务对买主管理信息内容的能力有更严格的要求。

4.4.4 互动——内容

在信息商务里，内容本身就是商品。我们将讨论在“履行”状态下进行在线发送的一些问

题。本节我们讨论在线销售的各种产品和服务。

- 软件
  因特网是天然的在线发行软件的媒体。如果没有发行手册和记录媒体，软件就完完全全是信息了。在线软件发送包括出售配送套件下载权，收取共用软件付费，销售密钥用于免费下载，以及订购网络计算机软件。
- 可搜索数据库
  内容供应商可以收取数据库访问费，包括搜索设施费用。此类数据库的信息有很高的价值，有时实际上价值是体现在信息的组织上。收费方式可采用按用法收费或订购收费。
- 动态信息
  因特网是一个巨大媒体，可用来发送新闻、金融摘要、体育新闻，以及其他变化很快的信息。所谓“推送”，是指可以将动态信息直接发送到桌面系统。
- 在线杂志和报刊
  此类内容基本上与报刊内容相同，但可能因为很及时和可以搜索而变得更有价值。在线杂志还可以专门发给某一客户，甚至可以用不同的信息源组成一份杂志。
- 报告和文件
  在线报告文件柜省去了复制纸印文件的许许多多麻烦。用纸张人工归档，费用非常高，而且几乎不能增值。电子文档可以保证不丢失文件或不归错档。多重复制件可以校验，可以通过搜索和索引来访问其内容。
- 多媒体对象
  假定有一定的带宽（等几年吧！），就完全可以在网上发送全保真电影和电视。现在，图像和声音已普遍应用于 Web 网上了。
- 互动服务
  在线论坛、聊天室、电话访谈、虚拟世界（MUD 游戏）和各种游戏可以在线发送。
- 信息服务
  券商、银行、旅行社和票务代理都是信息服务的例子，它们不需交换实物，所有此类商业业务都可以在线履行。

4.4.5 行动——订单处理

信息商务的订单处理与其他类别的订单处理相比，其主要差别在于，用户感觉更简单了，而鉴别则起着更主要的作用。

由于信息商务可以在微型交易中执行，个人购买行为要快，还要让用户感到自然。

由于在线履行的需要，鉴别尤其显得关系密切。例如，对于正在进行的订购，系统需要在

购买时对用户进行鉴别（识别身份），做适当的数据登记，以便在信息发送时可以对同一用户进行鉴别与核准。

4.4.6 行动——支付

另外还有几种支付系统似乎也适用于信息商务。自然，特别重要的支付系统如订货指令或信用卡完全适用于货值大的订货如长期订购或软件下载。

有时选择哪一种支付系统，有商业上的原因如批准程序或风险管理，而有时是为了省钱。如果省钱很重要，那么交易量大小就成了关键因素。每一种支付方式都有专门交易费用，从信用卡交易的 25 美分到处理订货指令的也许是 50 至 100 美元。

显然，10 美元的买卖使用订货指令支付是很不经济的。不过，10 美分以下（包括 10 美分）的买卖该怎么办？必然的答案是，选用交易费用小而适当的支付方法。

电子现金

电子现金系统有现金的几个特点，如不记名等。不过，和我们有关的特点是交易费用特别低。电子现金交易额可以在 5 到 10 美分之间。需要实时连接交换所的支付系统，其费用会比不需连接的高。

微型交易和辅币

微型交易在结构上与电子现金非常相似，不过，其交易费用对一分钱交易额也适用。辅币系统就是以辅币或信用证（实际上是一种私人货币）替换大笔金钱的系统，只可用于特别服务。我们已经提出了几种微型交易系统，基本思路是，修改万维网客户服务基本协议，以独立交互地将购买者记入借方，给卖方信用证明，再将此账转存入卖主账户。辅币实施起来更加简单，它在服务器上保持用户的信用平衡。

交易集合

卖主不需要另外的技术，就可以选择适用于账单的多种收费方式，来一次性收取费用。这一过程可以把一般交易费用分摊到许许多多的交易中去，使用一定的支付系统，可以使价值交换的费用变得很经济。交易集合有两种方式：

- “计程器”方式，或一次性全部付费
  在这一系统里，“计程器”累计使用的费用，让买主在日后一次性支付全部费用。难点在于卖主应允许买主延期支付，必须知道买主姓名。就信用卡来说，在结算（转账）前可以得到核准（信用有效性的保证），因此信用风险可以转移到发卡行。
- “停车计时器”方式，或先支付部分款项
  在本系统里，买主先付一笔款，也许是 10 美元，然后在一段时间内利用信用平衡。这里的难点在于卖主对还款（特别是不还款）的态度如何，以及卖主对信用平衡记录负

有什么样的责任。

在上述两种交易集合模式中，有许多技术上的细节和商业策略问题，例如，是否应该即时进行必要的核准，或它们可以延期吗？

4.4.7 行动——履行

信息商务中的物质商品，其履行是通过传统通道[5]进行的；而数字商品却可以在线履行。数字商品的内容不同，就适用于不同的履行方法。

下载

数字商品的最简单形式是客户机的一次下载，在线购买软件和报告适用于这种类型。典型方法是，下载收费、获取客户密钥收费、或访问下载区域收费。差异很微妙但却很重要，因为如果下载失败了该怎么办？硬盘可能满了，调制解调器可能中断工作，电也可能断了。因此，要谨慎考虑下载失败和自动恢复下载的功能。

- **下载收费**
  此方法适用于小型下载，它不容易失败。如果下载确实失败了，不是客户重新付费，就是客户服务系统会提出退款请求。下载收费可能最适用于微型交易，它的理论是“优化常见情况”。多数下载会成功，所以它们应该在没有用户干涉的情况下进行。当下载失败重试连接时，用户不用担心偶尔的收取双倍费用，因为不管怎么说，费用非常低。
- **客户密钥收费**
  客户密钥收费就是解锁下载，使下载区域可以公开访问，因为没有密钥，下载就无效。如果密钥技术有这种功能，即只对特定计算机有效，一旦生效，密钥还可以自由发送，因为除了原定目的地，密钥对其他地方无效。密钥和内容分开发送很复杂，也许只适用于价值高的订购（除非全过程是自动化的）。
- **访问收费**
  访问下载区域收费是一种有趣的混合设计，在这种情况下，允许有一段合理的时间来访问履行区域，这样会有足够的时间让用户成功地下载产品。例如，允许访问下载区域 8 小时，此段时间足够用户试着下载好几次产品，包括到商店跑一趟以购买更多的空软盘。

订购

我们把订购和下载分开来。有这样一个概念：订购是不断地访问某一服务系统，基本意思

---

⑤起码要到出现物质构造 PC 外设，它能够根据物体的描述构成物体。例如，参考尼尔·斯蒂芬森的《钻石时代》（1996 年《小书集》），或乔治 O·史密斯《完整的维纳斯对称》（1976 年《包兰亭》）。

是，用户买了订购产品，必须让服务系统可以鉴别自己，系统核准让他不断访问下去。这就得有订购数据库同意让谁访问（核准），而且还得有一种方法让客户证明自己是谁（鉴别）。

解决这些问题有多种方法，不过任何解决方案都要有这样的复杂功能，如更新、优惠时段、退款、访问多个履行服务器，以及用户在多个计算机上访问。

推送内容

推送内容的履行，是由内容服务系统主动发送的，而不是由用户下载的。它通过在服务系统产生数据记录以实现发送（点对点发送），或者发送到最终用户证明信息上，让内容可以被解码和收听（广播发送）。

4.4.8 响应——客户服务

信息商务的关键客户服务问题与其他类别相同。

- 我没有买（我记不得有买）
- 我没有收到（或发送到这里时中断了）
- 我不喜欢收到的东西
- 我的账单错了

其不同点在，信息商务可以利用一切可能的技术手段来保证发送。而像“我没有收到”这样的抱怨是极为罕见的。

复制保护和版权管理

数字内容的另一个问题是它是可以复制的，信息的实际发送（书刊、杂志）与信息在线发送存在差异，这不在于离开了网络就无法复制，而在于在线复制便宜得不可思议。内容所有者有几种选择：

- 不要担心
  最好的选择是不作任何版权管理。例如，如果信息在图书馆里可以免费得到，花钱或让客户产生不便以阻止偶尔复制，这没多大意义。不过，在这种情况下，帮助形成“复制而不支付是错的”这种社会氛围，以及让某人曝光，这倒有些值得。同样，内容本身不值得开展在线服务，不去管它也许是适宜的。例如，如果搜索能力是有价值的，阻止复制也许就最不值得了。
- 使复制变得非常困难
  如果销售的信息价值非常高，那么使之难以复制就很有好处。容器技术或软件客户密钥这些方法也许很适用。

- **使跟踪窃贼变得容易**
  这是模拟出纳抽屉里的小染料包的做法。染料无法保证银行的安全，但要找出窃贼却变得非常容易。在信息商务里，可以在每一份要发送的内容复制件中打水印或指纹印，这样，每份复制件就与众不同并进行了注册，如果打了水印的复制件曝光，就很容易找到原客户。
- **使支付买复制件变得容易**
  如果有一个用起来容易、又总是好用的方法来支付买复制件，大部分诚实的客户就会使用这种方法。如果没人知道向谁支付、怎么支付，那么复制之风就会大行其道。这种方法用于向专业客户发送信息尤其奏效。这类客户想支付来获得有价值的信息，他们常把信息费用转移到自己客户身上。

4.5 小结

在本章里我们讨论了三个商业类别的商业模式和商业问题，这三个类别也许会从因特网商务中受益。还有其他许多商业类别会由于应用因特网技术而受益，不过，我们希望这三种选择形成一个相当广阔的网络，让读者能仔细考虑因特网显现的机会，仔细分析完整的客户价值链。

在任何商业类别里，无论与因特网有无关系，参与者不同就有不同的目标。按高标准来说，客户希望的是，物美价廉；而卖主却想尽量多赚钱。了解这些不同点，让这些矛盾在成功的销售中趋于和谐，这是任何商业策略的关键部分。因特网技术，尤其是因特网商务，引来了前面的许多难题。在下一章里，我们谈这些问题的一些例子，并讨论如何在商业系统中来分析和解决它们。

第 5 章相互矛盾的目标和需求

寻求皆大欢喜，这是极为难办的事。
——帕布利里尔斯·塞勒斯 ①

在商业规则里头，第一条便是“了解你的客户”。如果你知道你的客户想要什么，又能给他们比别人好的，那你就可以获得成功。不过一个常出现的问题是，系统要服务于不同类型的客户，他们的需求相互矛盾。有时客户不清楚他们要什么，尤其是在一个全新的领域里。本章概述因特网商务与上述问题相关那些大致范围，也就是参与者目标不同，或起码是重点不同的领域。

5.1 参与者的目标

因特网商务系统有许许多多主人。本节阐述审视某些关键客户的目标和兴趣所产生的复杂性。

5.1.1 买主

在本节上下文中，买主指的是客户。商务系统得满足客户的需求，这似乎是很显然的，不过，不同买主想要的东西不同，有时他们的兴趣与卖主的目标相反。

零售客户

我们说的零售客户是指应用 B2C 商务系统的买主。

- **便利**
  因特网是驾驶和浏览之间的选择、庞大商品目录和过时纸印商品目录之间的选择。如果使用网络并不比用另一种方法来得容易，谁会愿意费这个劲呢？
- **价格**
  零售消费者对价格往往很敏感，尤其是对物质商品和有多种选择的产品。
- **选择**
  消费者感兴趣的是，在自己兴趣的范围内进行最大限度的挑选。感兴趣，有两个不同原因，一是买主可能在广泛使用的产品中寻找最佳特点和性能；二是买主可能在寻找

①帕布利里尔斯《格言》。

罕见或与众不同的产品。前者，选择是为了比较；而后者，在消费者看来，卖主有众多商品可选择，找到合适产品的可能性更大。因特网给买主提供了另一种选择方法，让他有可能选择与众不同的商品。由于网络可以抓住全世界的对象，即使是对象市场，也足以支持一个专业零售商的生意。

- 隐私

  许多消费者不愿意公开个人信息，害怕成为邮寄宣传品或广告的目标，或仅仅因为他们认为私人生活不干他人的事。消费者如果知道自己在网络上的浏览和购物习惯受到严密监视，多半会很生气。

- 服务

  有些消费者对价格并不敏感，但对服务却很敏感。他们会光顾这样的商家：尊称大名恭迎他们的商家、经常通知他们有新产品来了的商家，以及认为消费者一贯正确的商家。

- 安全

  消费者要求得到保证，确保自己的信用卡号码及其他敏感信息得到充分的保护。

企业客户

企业客户是在日常工作中应用因特网商务系统的买主（例如，行政管理者重新订购办公用品，或工程师要指定零配件来设计新产品）。

- 个性化

  如同卖主很想让自己的零售客户成为回头客，企业要其客户成为回头客也是基本的。商界多以订货合同、特别价格和订货量折扣等来经营，这些方面也会体现在因特网上。在一个供应商纵横交错、竞争激烈的世界里，卖主会努力使自己的服务个性化并尽可能提供最佳服务，以吸引新客户和避免现有客户的流失。

- 易于使用

  既然企业客户几乎是回头客，那么易操作性便显得极为重要。就办公用品客户来说，卖主会让调用和复用原先的订单变得很容易；而对专门工程师来说，卖主会让搜索和找出零部件变得很容易。在上述两种情况下，速度是基本的，因为浏览和订货不是活动的最终目标，而令人讨厌的是，它们占用了时间，使买主没有尽到自己的基本责任。

- 安全

  企业对客户安全问题的关心，与其说是关心信用卡安全，不如说是关心自己的业务不被竞争对手知道，关心确保公司计算机系统里业务记录的完善。

5.1.2 卖主

在本节上下文中，卖主包括 B2B 商家、B2C 商家和信息商务的出版商、内容供应商。

- 抓住新市场
  卖主感兴趣的是利用因特网的潜力抓住新市场。
- 建立和增进与客户的友好关系
  很少有这样的卖主，他只有一种产品，而这种产品又是其他供应商那里买不到的。因此，卖主感兴趣的是，提升价值链，提供不那么商品化的产品，或以其他方式避免自己的客户流失。
  建立客户关系，有一部分是要了解自己的客户，这往往包括尽可能收集客户的信息。
- 成本的有效性
  因特网商务系统可以大大缩减信息发送成本和客户服务成本。
- 安全
  卖主极感兴趣的是，自己的市场存在、价格、客户记录和业务记录的完整。

企业计划介入因特网商务，矛盾就很容易会出现。

- MIS和IT部门可能会认为自己应拥有并操作因特网商务系统，原因是这必然要涉及到计算机。
- 反之，MIS也可能会极不愿意部署因特网商务系统，因为它是新事物，会有所不同。
- 销售部门可能认为自己受到威胁，因为因特网可以使销售渠道瓦解。

5.1.3 金融处理机构

金融处理机构所进行的操作是,在信用卡处理系统中接受来自商家的交易业务并转移至商家的开户银行。更广义地说，我们包括了不受付款方法、信用卡或非信用卡限制的金融授权和结算服务。

- 安全
  交易安全对金融处理机构来说是首要的，这包括记录的保密和准确、请求的合法和完整。
- 交易量
  金融处理机构赚钱，不是按每笔交易的统一手续费算，就是按交易数额的1％来算。它们极感兴趣的是交易量的上升，即不是交易次数的增加，就是交易总额的增加。
- 成本结构
  金融处理机构人员的薪水不是按成本基础来发放，而是按他们所做的工作来发放。因特网作为通信设施，产生了一些诱人的可能性，可以降低电信费用，甚至可以将费用转移到其他方身上。

- **额外服务**
  金融服务就是商品。和其他商品供应商一样，金融处理机构感兴趣的是，增加额外服务以加深与客户的关系。
- **风险管理**
  金融网络的许多复杂性涉及到买主、卖主和金融机构，也关系到将损失的风险和责任分摊给参与各方。分理者感兴趣的是，需要利用这一系统把风险降到最低，而且尽可能把风险转移到其他各方身上。

5.1.4 政府

- **安全**
  政府对安全感兴趣是指国家安全，这方面包括政府对进出口和密码术应用的控制。
- **法律控制**
  政府感兴趣的是，保证企业和消费者能遵守法律法规。在许多国家，探听某种信息是非法的；在有些地区，进行某种产品的交易也是非法的。
- **税收**
  政府靠税收获得收入，因此极感兴趣的是，保证税款征收并堵塞漏洞。

政府一定认识到因特网无所不在。政府试图过分限制企业的行为可能只会迫使企业往别处去，企业可能会在全球范围内“选择法律”，在最能满足自己需要的合法地点进行交易[②]。美国特拉华州的公司在非洲利比里亚注册船只正是由于这些原因。

5.1.5 技术专家

技术专家在创建因特网商务系统方面任务艰巨。在一个新领域，好幻想的客户买产品和采用新技术，依据的是技术的优雅和共同想象着技术上的某些可能性。然而，要抓住大市场，有技术几乎是不够的，因为幻想并不能开出巨额支票，再说，早期采用新技术的人不多，不足以建立一个大市场[③]。

为了拓展因特网商务市场，有必要制造一整套有技术核心能力的产品，这使技术专家进退两难。他们的目标是，用简单的普通系统来解决多数问题。实际上，市场可能要求有日益复杂和专业化的应用系统来解决某些市场环节的全面问题。

---

②如丹·吉尔在美国参院科学技术委员会面前作证时所说的，要了解这段陈述请访问：http://www.house.gov/science/dan_geer.html。

③杰弗里 A·穆尔《跨越鸿沟——向主流客户推销高技术产品》（1995 年《哈珀企业》）。

5.2 标准的作用

在信息技术里，标准就是一套技术要求，它有助于不同各方建立的系统相互可操作。对于因特网商务，标准有两种基本功能：

- 标准是一种方法，它把动力从卖主那里转移到客户身上。
  有专利技术库，通常有利于卖主。专利系统可以最大限度提高转接费用，留住客户；还可以免检其他卖主的产品，就可以保证符合标准，以降低卖主成本。
- 标准是一种方法，它使用多个卖主的零部件来装配一个完整的系统。
  早期的市场，可能没有一家公司能够制造“完整”的产品。完整的系统要靠别人的零部件，而标准帮助了大家。个人卖主依据适当的标准制造零部件，这样系统集成商可以使用多个卖主的零部件来装配一个完整的系统。

因特网本身的成功，就是对标准的一个贡献。在某些方面来说，因特网的定义就以标准为基础。符合因特网标准如 TCP/IP 的系统就是因特网。

标准的主要问题是，不会简单到不实用，又不会复杂到无法推广，这并不容易实现。

5.2.1 早期与晚期的标准化

人们对标准化所做的努力是沿着两条道路之一进行的：早期标准化或晚期标准化。

晚期标准化

在晚期标准化里，各方合作，共同建立市场；或出现技术竞争，由市场选定一个领导者。只有在市场趋于稳定之后，各方才会真正联合起来，最终宣布一个标准。多数因特网通信标准就是这样发展起来，也就是按一致同意的标准去实验、去进行相互可操作性实验而发展起来的。晚期标准化的主要好处是，最终的标准更简单，起码是众所周知的迎合真正的需要。

晚期标准化另一种形式的出现是，一个专利系统获得了主导市场的份额，它便成了标准，即使在竞争中不可能发生这种事。以这种方式产生的标准往往很有效，但也更复杂了。

早期标准化

在早期标准化里，参与各方联合起来，就技术要求达成一致协议。这使大家都受益，尤其是当一段时期大家各自为政大大延缓市场发展的时候。另一方面，早期标准化的结果是标准太复杂，它试图满足没有被充分理解的客户要求。有时仅参与方就增加了复杂性，因此，所有卖主都同样会有所不便。在音乐和数据光盘标准上所做的努力，就是早期标准化发展市场的一个例子；而国际标准组织（ISO）的那套因特网协议就是标准无法控制过程中的一个极好例子，它终于在市场中失败了。

5.2.2 因特网商务标准

标准对因特网商务重要吗？正如经常发生的那样，有时很重要，有时不重要。我们不去评论下面几条是好是坏，这些只是几个可供大家去考虑的思路：

- 标准有助于相互可操作性
  除非从一个卖主那里可以得到一整套系统，否则，部件的相互可操作就是很重要的。当系统操作者根本不限制使用哪种部件时，这问题就很烦人。例如，在因特网商务系统 B2C 里，卖主也许要指望买主有相应功能的 Web 浏览器，和卖主的 Web 服务器和内容格式相匹配。
- 最好是好的敌人
  在市场早期阶段，系统设计者用许许多多不同的技术和方法来进行实验。然而，当每一个商业站点都在样式、设计、功能和客户检验方面与别人截然不同时，用户群就可能局限在那些靠求新和求复杂过日子的站点了。一致性和标准化有一个很大的好处，就是易于使用。
- 好是最好的敌人
  标准化，尤其是不成熟的标准化，限制了创新；再说，标准使用得越普遍，改革和发展的动力就越大。在早期市场，谁也不清楚（或谁都“非常清楚”）什么技术和设计原则最终会成功。最好是让标准化放缓速度，让市场去发现成功的原则，并把重点放在它们身上。

5.3 隐私与推销

消费者想保留自己的隐私，在网站上透露的信息尽可能越少越好；而出于商业利益，信息收集往往超出了提供服务所必需的范围，把消费者透露的信息和其他数据来源结合起来，构成非常详细的客户图像，有时还把消费者透露的信息转卖给别人。此外，在显现消费者轮廓和利用消费者方面，技术容易被滥用，而正是这些技术，在设立 Web 应用并使之易于应用方面必不可少。

第一个问题不只是信息传输，而是信息利用的问题。消费者会明白在线订货给一个交货地址是必要的，但如果将这地址卖给另一个公司作推销用，他可能会极为不快。

第二个问题是，隐私似乎并不听命于纯技术的解决方案。如我们以后会讨论的，Web 网上信息数据块（cookie）工具已招来了坏名声。现在，许多用户都关上了浏览器里的 cookie 文件。这使许多 Web 网站（它们相当合法地利用 cookie 技术）几乎无法提供服务了。

5.3.1 隐私预定选项平台

Web网界对隐私问题的反应，结合了技术和信任方面的问题。万维网联盟发起组织了一个工作小组叫隐私预定选项平台（http://www.w3.org/p3p/）的，该小组Web网页对其目标的陈述如下：

隐私预定选项（P3）项目的目的是：规定和示范一种相互可操作的方法，让Web网站和用户分别表示预定选项和隐私做法。网站的做法是，同步进入用户预定选项范围，让用户“无缝”访问；而用户则会得知网站的做法，他可以同意那些条款或其他条款，如果愿意，还可以继续浏览。

有些公司，包括Netscape、Microsoft、Firefly和Verisign正与万维网联盟合作，以Firefly的“开放配置标准”为起点，思路是，每当网站请求用户提供个人资料信息时，只要网站所说的使用意图与用户的预定选项相符，就可以自动提供。

5.3.2 Cookie文件

一种卷入了隐私争端漩涡的技术是cookie技术。

1995年添加到万维网浏览器上的一个有趣的技术创新是Cookie文件。1996年，随着cookie知识与应用的传播，一场关于隐私含义的论战爆发了。

Cookie是一种技术，它能把Web网无国界点击转化为“话路”；它能在浏览器由扩展区域回到网站时自动认出这个浏览器；它能把用户资料信息储存到浏览器。这些能力对服务经营者和用户都极为有用，不过也引来了对隐私的忧虑。

Cookie文件是什么

Cookie是一个Web网协议和浏览器应用方法，它允许服务器指示浏览器在用户硬盘上储存一个信息块，在以后用户访问这个服务器时收回。如果服务器没有先把信息块存入，cookie里的信息就不会发送到这个服务器里。当浏览器连接这个服务器时，服务器指示：“收下这个信封，等下次访问时一起收回。”

这种能力可以用来完成三件事：

- 通过站点跟踪个别浏览器——Web点击中的话路
- 自动认出以后访问同一站点的浏览器
- 可以在用户浏览器储存用户资料信息

cookie可以储存用户资料信息引起了许多忧虑。应该注意的是，资料可以轻易地被存入服务器，再依据浏览器的惟一信息，如序列号或含有惟一ID的cookie，把它们编入索引。有些网站试图把浏览器的IP地址作为惟一号码。不过，这样会有一些问题，因为许多用户受到代理服务器的屏蔽，或使用动态分配地址。

好处在哪里

Cookie技术可以提供如话路、自动用户识别和用户资料储存等的技术基础结构，每一种能力都能对用户和服务系统提供有价值的服务。

- 话路

  没有话路，根本不可能提供多种形式的Web网服务。如果需要一系列的组成，就需要有个位置来储存单击的过程状态，以便在下一次单击时恢复（索引）这个状态。此外，如果在翻阅某一服务的一连串屏幕时，用户想岔开进入另一Web内容（例如求助屏幕），那么就需要有一种方法，能够使用户回到刚才离开的那个服务。这样，对服务和用户有一个好处，就是话路允许应用程序利用嵌入式帮助来使用一系列的Web屏幕；另一个好处是，服务可以执行登录分析，查看使用了哪些部分，怎么用的，以便改进。

  显然，对广告客户和审计局来说，话路是极有价值的信息，尤其是在结合人口统计信息时。不过，对用户是否有益，这还有待讨论。

- 自动用户识别

  通常用户的自动身份识别是安全服务（需要鉴别）的基石，也是提供个性化“窗口”服务的基石。没有逐步单击的鉴别，服务就无法提供安全内容，因为不知道谁要使用；没有鉴别，服务就无法提供任何程度的个性化服务。

  还有一个位置可以识别返回的用户，即使不知道那用户的姓名。例如，如果在线商业大街想提供一个可以在话路中储存起来的购物篮，那么，没有姓名的指定用户ID就可以完成这项任务。

- 客户端用户资料

  cookie技术的最后应用是，作为储存用户资料或应用状态的一个位置。这一好处是，服务系统不受每一次单击访问服务器端数据库的性能影响。另一个保护隐私的好处是，不需要有中心储存区，中心储存区将每一个人的全部信息都收集起来。

缺点在哪里

- 秘密跟踪

  Web网站可以利用cookie技术来储存个人预定选项和个人行为信息，而不经过个人的准许。由于cookie技术独一无二的跟踪特别浏览器的能力，Web网站可以获得反复访问的准确信息。不过，储存的信息也可能是不准确的，尤其是公用计算机，它可能出现张冠李戴的现象。

- 雇主搜索

  当雇员使用公司计算机在Web网上冲浪时，cookie文档也许就储存在计算机里，公司可以搜索那些文档来获得计算机使用不当的证据。的确，某一企业报刊已对田纳西州

地方政府获取编职人员 cookie 文档提出控告，而政府的理由是，这些文档是政府的官方记录。

5.4 安全电子交易

1995 年后期，Visa 和 MasterCard 联合发起订立了安全电子交易（SET）协议，即保护付款卡在开放网络上交易的一个技术标准。SET 是消费者在因特网上进行信用卡交易的优选方法。

付款卡交易是一个很复杂的过程，虽然我们会在第十四章详细阐述这问题，但是现在先谈谈也是适宜的。付款卡交易有若干参与方，他们都起着不同的作用。

- 发卡行——发卡给消费者，延期付款，负责发对账单、收款以及客户服务
- 收款行——与商家建立关系
- 消费者——购物、付账
- 商家——销售产品、收货款
- 分理机构——运行电信设施的服务机构
- 卡协会——制定标准的保护机构

在非电子交易领域，交易按如下方式进行：

1. 购物时，持卡人出示付款卡。
2. 商家把交易信息传送到收款行的分理机构。
3. 分理机构按路线通过卡协会把交易传送到发卡行。
4. 发卡行核实持卡人身份后批准交易。
5. 交易批准后按原路线发回给商家。
6. 随后，商家“清算”交易，于是资金从发卡行转至收款行存入商家账户。
7. 持卡人付账，资金从持卡人账户转至发卡行。

5.4.1 SET

SET 的设计是模仿传统的卡交易流程。除了业务信息，SET 还包括使用公用密钥证书来鉴别交易各方。

消费者

在美国，消费者对信用卡欺诈和盗用几乎不承担什么风险。美国消费者信用保护条例规定：一旦声明信用卡丢失或被盗，消费者对信用卡被盗用不负法律责任，最多只承担 50 美元的法律责任。言下之意是，通过技术手段把系统内的风险转至最直接责任人，以把潜在损失降到最低。

通过使用付款卡，消费者还享受到实实在在的客户服务，这包括假如商家不履行或服务质量有问题，可以对收费提出质疑和拒绝付款。发卡行可以相互竞争，消费者还受益于额外保单程序和各种各样的常见购物程序。

尽管付款卡有这些好处（不计手续费和利息费），消费者仍然对信用卡号码被输入计算机感到很紧张。对消费者来说，SET 的目标和要求如表 5.1 所示：

表 5.1 持卡人的 SET 目标和要求

目标	保证信息的机密性
	让持卡人鉴别商家
	提高电子商务的安全保障
要求	获取与安装持卡人软件（钱包）
	获取 SET 客户证书

银行

在传统的付款卡系统里，银行管理风险，发卡行承担持卡人延期付款的风险，收款行承担对商家提供卡服务的风险。SET的几个特点在于降低来自商家的风险：要求商家要有SET证书以鉴别其合法性，允许商家在不知道客户卡号的情况下认可交易。例如，在现实世界中，代理经营的非正式商家可以通过正式商家直接清算付款卡交易，而在 SET 里就不可能出现这种情形，因为非正式商家没有证书。同样，除非商家对卡号储存非常谨慎，否则，商家一旦违规操作，就有可能把卡号泄露给非持卡人。有了 SET，商家不需要实际卡号，因此就降低了风险。对银行来说，SET 的目标和要求如表 5.2 所示：

表 5.2 银行的 SET 目标和要求

目标	减少商家欺诈
	扩大电子商务量
要求	安装证书等级系统
	安装持卡人证书系统

商家

在传统的付款卡系统里，当客户在销售点签付款卡单时，接着就有各种程序如店员核对签名，核对卡上显示的交易是否符合贴现率，并核对付款卡系统是否保证能付款给商家。但是，如果客户和卡没有在销售点出现，如通常的电话销售，商家得付较高的贴现率，而且要承担有人使用盗用卡的风险。

SET 使用持卡人数字证书，可以强化持卡人的鉴别，也就是说，有了操作经验，因特网上的 SET 交易，也许就相当于现场出示付款卡的交易了。对商家来说，SET 的目标和要求如表 5.3 所示：

表 5.3 商家的 SET 目标和要求

目标	易于综合 扩大电子商务量 减少交易成本
要求	安装 SET 商家软件

5.4.2 SET 矛盾

引入SET，也引来了一些相互矛盾的目标和要求。我们在本小节谈引入SET后，银行与商家之间的矛盾，以及持卡人与新的复杂性之间的矛盾。

银行与商家

SET提供给银行这样一种潜力，即不向商家透露卡号，以减少商家欺诈行为造成的损失。另一方面，商家想让带有SET的系统很容易地并入现有操作。现有的付款卡系统通常需要访问客户卡号，而 SET 则相反。

SET的确有多种选择方法，可以向商家透露卡号。这可以在一个商家一个商家的基础上来进行，不过，这样做的代价是，协议复杂性增加，还需要额外的配置机制。选择这样做，还会失去 SET 的最大安全优势之一，因为它允许商家职员读取卡号。

持卡人与复杂性

要求持卡人获取证书以进行鉴别，其目的是，有些卡号不是在网上得到的，有了证书，就可以大大减少这种欺骗性使用卡号问题的发生。但这一受益其代价是，持卡人在获取和管理证书上的复杂性增加了，不过，持卡人并不直接受益。如果欺诈减少了，最终付款卡贴现率也会降低，那么，商家就会选择向消费者降点价。

5.5 小结

每当系统的不同参与者有不同的目标和要求时，就存在着潜在矛盾。这在新行业如因特网商务里尤其是现实问题，因为因特网商务设立了几种标准。我们的忠告是，列出系统中的参与方，摸清楚他们的目标、兴趣和计划。

了解参与方、了解他们的目标和兴趣，这在制定解决商业问题和迎接技术挑战的计划中是很重要的。给它们定出框架，研究一个核心方法，以便解决问题，这是构造系统结构的过程，是我们在下一章将要考虑的。

第 6 章功能体系结构

体系结构……抗压形态的契合。
——约翰·拉斯金 ①

6.1 体系结构是什么

体系结构阐释基本组件和重要概念，描述其中的关系。探讨因特网商务系统有多种方法，从简单到复杂。体系结构一部分取决于企业性质，消费者零售的体系结构可能与出版系统的决然不同。我们认为，许多设计思想跨越了商业需求的广度。因特网商务系统的相似之处要比不同之处多得多。本章描述因特网商务的核心体系结构，一个适用于多种应用的核心体系结构。

为什么我们应有一个总体体系结构呢？为什么不只设计单一的应用系统呢？我们的实际回答是，近几年来我们一直在设计因特网商务系统，不断地应用体系结构，不断地设计，使之有可能成为客户的最佳方案。然而，更重要的是，随着企业因特网商务目标的改进发展，其系统也需要改进发展。这种发展可能进行得很顺利，超出了系统原先的要求，所以，系统的灵活性尤为重要。例如，软件商店起初可能是在因特网上接收订单后，再寄出一箱箱指南和磁盘；后来，它也可能想在网上发行软件，如果原来的系统没有处理在线发行，这家商店也许会发现，要增加这种能力，自己将面临着付出开发或升级的大笔费用。

本章，我们描述体系结构设计的种种思想，更深入地探讨其中的某些方面，也举出因特网商务实用体系结构的一些例子。

6.2 核心体系结构的思路

不同的商务系统体系结构看起来也许各不相同，但我们得谈些相同的问题，并提出一系列共同问题的答案。无论采用什么方法，都要清楚地认识这些问题。有时这些共同问题是在设计阶段需要明确考虑的，有时问题和答案就体现在对体系结构各组件的设想中。本节，我们探讨组成商务体系结构的某些基本要素。

一句告诫的话：有时，我们说的体系结构似乎一目了然，不需阐述，或我们似乎在勾划多余的特性。按我们的经验，让这一目了然的东西含混不清，会引起以后的混乱和误解，这正是

①约翰·拉斯金《亚诺河》（1874 年）。

因为大家都认为它一目了然，而“一目了然”的是什么，大家却持有不同的观点。如果我们想在计算机系统设计中获得成功，一定要十分准确，不但在描述计算步骤方面要十分准确，而且在理解和描述我们要做的事方面也要十分准确。做生意的过程似乎很自然，因为我们对它如此熟悉，还因为人们可以轻易而有效地应付非同寻常的局面。当我们设计处理这些过程的计算机系统时，一定要特别谨慎，因为计算机无法解决在意外出错时如何使客户满意的问题。

6.2.1 懂得角色作用

计算机系统的两个最基本问题是“谁使用它”和“他们用此系统干什么”。有些程序，几种用户共享类似的目标，例如，新手和专家都使用文字处理机来生成文件。因特网商务系统更复杂：其用户有商品和服务的购买者、商品和服务的销售者和这一整套系统的操作者。

弄清楚一个系统里的各种角色作用和用户种类，有助于我们集中注意力，保证每个人都可以有效地使用这个系统以达到自己的目标，无论是在做交易，或是在做会计报表。

6.2.2 功能分解

系统体系结构的第二个重要部分是如何将系统分解成有各自功能的若干部分。这些功能的规约及其相互之间的联系构成了系统的体系结构。不同体系结构之间的差异之一是，功能分解的方法不同。是否所有组件构成一个系统？各组件是否分布在复杂系统里？各功能之间有什么联系？

6.2.3 内容与交易的链接

系统体系结构中要考虑的头两部分是角色作用和分解，它们几乎存在于任何计算机系统设计。因特网商务系统体系结构的第三部分是内容如商品目录与交易处理的链接。在有纸化系统里，买主将商品品种和数量打在订单和申购单上，显然，我们要用电子方式来做这些事。

在这个链接里有几个关键问题：

- 用户如何下单订购

  在许多情况下，用户会看见“单击购买”按钮，或可以在购物推车上添加商品以便随后购买。单击“现在购买”按钮，或单击购物推车上的“校验”按钮，就完成了交易的下单订购。

- 如何核实信息

  交易系统必须能核实交易信息如价格和商品名称等在网上发出后是否有改变，这取决于基础技术，因为（我们随后会更详细讨论）Web网用的是无状态协议，在Web网之上建立起来的商务系统要会处理自己的状态，如果在某种程度上是处于客户传输状态，服务器一定要保证在传输中不会有所变化。

用去考虑角色之间有哪些差别。然而，企业购货往往不同，因此，考虑各种角色作用是很实用的。

- 选定者——选定购买什么物品的人
- 准购者——批准选定者提出的购物项目的人
- 采购员——商谈购货付款条款的人
- 收货员——接收已到商品或服务的人

此外，我们还可以按买主与卖主的关系来区分：不知名的买主（有时称“不期而至的客户”）指与卖主素不相识、最多只买点东西的买主；会员客户是指不断向卖主买东西，建立了某种关系，也就是所谓的有会员资格的买主。会员可以签约，签了约有了账户就能便利地得到特别优惠，会员资格体现了生意关系。

由会员资格账户派生出的另一个角色作用：会员管理者。承担这一角色的人可以更改或更新会员储存资料里的信息。如果会员资格包括好几个个人账户，如一个家庭的不同成员或一个企业的多个采购员，那么会员管理者还可以对个人账户的使用进行限制，如限制可购买的商品品种、开支数额和购货时间等。

当然，实际上一个人可以扮演多个角色，如消费者买了件运动衫，他在商店选购、付款并带回家。在这种情况下，消费者扮演了所有的三个角色，我们一般不去区分。再比较一下，想想第二章我们所说的电子零部件的例子，专门工程师决定买什么配件，采购员谈付款条件，生产小组接收用于最终产品的零部件。

这一分解告诉我们，因特网商务一般系统需要有一种方法，可以让不同的人处理不同的交易事务，但让一个人处理所有这些事务也应是极其简单的。消费者并不希望在交易事务中明显改变角色作用，但确实希望购物快且轻松；而企业方面，有各种分工，它们希望交易事务的交接能顺利而高效。

6.3.2 企业的角色作用

交易的另一方是卖主，它在因特网商务中有多种角色作用。小企业以及大企业开始小规模介入因特网商务，可能只有几个人发挥着所有的角色作用，我们这里列举的不同角色对它们来说似乎都嫌太复杂了。然而，早早考虑这些角色，一个从事因特网商务的企业就可以发展得更顺利，随着更多的人加入，分工实际上也就更清楚了。卖主有两个主要角色作用小组，一是商业和内容创建小组，二是操作小组。商业小组最重要的角色作用如下：

- 商业经理

  商业经理负责处理因特网商务，创建和操作企业的因特网存在，决定哪些产品和服务要在线销售，敲定价格，建立关键企业关系，以使因特网商务获得成功（我们会在第七章讨论这些操作的实施策略）。这一角色主要是商业角色，要特别关注在线商业和最

低目标的成功实现。

- 因特网商务设计师
  因特网商务设计师通常是系统分析员，他把企业需求转化为系统设计，其中包含内容（如商品目录）的创建和管理、交易处理、履行，以及客户服务的技术方面。总之，设计师填补了商业价值链更深层的细节。
- 内容设计者
  内容设计者负责因特网商务系统的外视感觉，如图形设计、页面格式和用户感觉等。
- 内容创作者
  内容创作者通过创作或修改将产品信息转变成可用于因特网商务的形式，这要在内容设计者的设计格式范围内进行。
- 实施者
  实施者负责因特网商务系统运行时所需的程序编制和软件扩展，如写软件，把产品信息从数据库动态复制到 Web 网页上。
- 数据库管理者
  如果使用产品信息数据库，由数据库管理者（DBA）管理数据库的创建和操作，保证其正确性、完整性和可操作性。
- 销售与推销小组
  销售与推销小组负责集中精力推动企业因特网商务的发展。
- 客户服务代表
  客户服务代表负责为企业回答产品的问题，帮助买主登记或订货，答复有关订单情况和售后问题的咨询，处理产品退货和付款争议。当然，一个企业会有不同的人在这一角色作用中专门处理不同的事务。

当然，个别公司可能会有不止一个人承担一个以上（包括一个）的角色，或一个人承担多个角色。有时这要看用的是什么软件。前面所说的商业小组中的许多人就要选择买哪一种产品，以及这种产品如何适用于因特网商务计划。这些小组的有些成员可能不是顾问，这要看公司人员的技能和可用程度如何了。

操作小组安装和操作因特网商务系统，确保其运行，使客户可以使用这个系统，系统操作的某些具体方法在第 7 章讨论，其角色作用如下：

- 操作经理
  操作经理负责管理因特网商务的一切服务活动。
- 系统主管
  系统主管管理系统全体工作人员。
- 系统管理者

系统管理者负责计算机系统和网络的技术操作。

- 安全员
  安全员确保相应的安全措施在因特网商务系统设计和实施中得以落实。
- 履行代理
  履行代理负责物质商品的运输和处理，或提供服务；遇到数字商品，负责监控履行系统的操作（并监督履行系统工作人员，如果有的话）。
- 会计
  会计负责保证在因特网交易成交后履行适当的结账程序，也就是管理相关的业务记录，编制系统管理的交易报表，以及发挥其他结账功能。

6.3.3 角色作用与实际情况

我们谈到的角色作用，很可能并不一定是企业里能找到的角色作用，它们未必能与干实际工作的人一一对号入座。不过，考虑角色作用而不是考虑人，能保证所有的工作得到完成，还能保证我们在系统设计和组织小组进行操作时不会漏掉某一个重要功能。做这些分工，在遇到有些工作外包时，也会有所帮助。我们在第7章会看到，实施这个系统有多种方法，外包所有操作或部分操作也行得通。这里的有些角色作用，如操作方面的，可以相当容易地外包出去，而有些如决定什么产品选入在线商品目录，是商业上的决定，不可以交给别人去做。

6.4 组件

体系结构的另一个重要问题在于我们用来工作的那套组件。对因特网商务来说，我们常想利用一般因特网应用系统，这有如下三个原因：

1. 如果可以用一般应用系统，就不必再去设计了。
2. 一般应用系统分布很广，不必设立分布通道，把一个专用工具交给客户。
3. 客户已熟悉这个应用系统，不必学习如何使用专用工具。

下一节，我们介绍因特网商务系统所用的基本组件，在本书的第二部分，我们会更详细地对它们作技术上的讨论。虽然我们的中心是，使用一般工具如万维网浏览器和服务器，但有时开发并发送商务专用工具，当然也是适宜的。即便如此，我们仍认为，这里所描述的组件，也是设计这种工具的一个良好起点。

6.4.1 客户组件与客户机

客户用于万维网的基本工具是浏览器，有时叫Web客户机。我们将在第8章讨论浏览器

及其他Web客户机。体系结构显然受到Web网基本结构的影响，尤其是受到浏览器能力的影响。我们会看到，精确确定如何组织系统遇到的重要问题之一是：客户有什么浏览器，以及这些浏览器有那些能力？

有些公司也设计专用客户商务应用软件，尤其是用来进行付款，它们常叫“电子钱包”，设计它们是为了应用一种或一种以上需要额外处理的付款方法，如客户上的密码操作。电子钱包还可以用来跟踪交易的进行，查对订单情况，或处理有关交易的其他信息。电子钱包存在的主要问题是，如果系统要求客户使用电子钱包，那么客户就得设法得到并安装电子钱包软件[②]。我们将在第 14 章着重谈付款方法及其对客户软件的要求。

6.4.2 销售者组件与服务器

交易的另一方是销售者，有时也叫商家或卖主。销售者提供商业价值链的所有组件，从内容到客户服务。实际上，一个销售者可以直接提供价值链的某些组件，再签约让别的销售者提供其余组件。不同的销售者也许会作出不同的决定，决定自己直接提供哪些组件，而且这些决定可能在一段时间内会有所改变。因此，我们把一般体系结构的价值链进行分解，这样，不同组件就可用不同方法来处理。

价值链有些组件的外包比其他组件来得容易些。例如，内容展示了企业销售的产品和服务。虽然公司可能会开拓视野，寻找富有创造性的思路，去设计实际内容的表示方法，但是，产品有哪些，如何销售，这才是商业的功能。另一方面，付款服务对企业来说是非常重要的，不过，只要结果正确，这一过程的细节就可以隐而不谈。下面是一些销售者组件：

- **交易处理系统**
  销售者的交易处理系统跟踪交易的所有信息：订那些货，谁订的，货值多少，付款情况和履行情况等。
- **付款处理机**
  付款处理机管理系统里资金或其他付款手段的转移。例如，消费者用信用卡付款，卖主链接信用卡付款处理机来核准交易（查对信用是否有足够的可信度），随后清算交易。
- **履行系统**
  有邮购业务的公司常与履约公司签约，以处理订单的包装和运输事务，在因特网上接收物质商品订单的企业也是如此；实际上，在因特网上销售数字商品的企业也可能会与履约公司合作，利用服务器发行在线产品。或者在上述两种情况下，企业也许会选择由内部来管理履行过程。

---

②写本书时，电子钱包还没有普遍随同浏览器一起发行，如果这种情况普及了，如果它能与多个卖主的商业软件相互可操作，那么就不会有这个问题了。

这些功能的一个逻辑组合产生了所谓的“前方功能”与“后方功能”。前方功能关系到推销、销售和服务。内容和表示方法非常重要，中心是吸引客户购买产品和服务。后方功能关系到交易细节的处理，从下订单到付款，再到履行。进行适当的交易处理很重要，如保证有关信息发送地点准确，收款无误。

6.5 体系结构实例

如我们前面提出的，不同问题的不同答案就会带来极不相同的体系结构。本节我们谈4种不同的体系结构，并讨论它们是如何构成的。这四种体系结构是：带有订单的Web服务器、带有使用SET协议订单的Web服务器变形、我们在“开放市场”开发的配送交易法和因特网联盟“开放购物”开发的B2B商务法。当然，从事因特网商务还有许多其他的方法，我们选出这四种以阐释本章所要讨论的许多要点。

我们认为，分析体系结构，考虑因特网商务系统的4个主要组件是恰如其分的：

- 客户
  客户是通过因特网服务供应商（ISP）把一个计算机系统，通常是一台PC，直接链接到因特网上，或是通过公司网络间接连接到因特网上。买主用客户浏览和进行交易。
- 商业系统
  商业系统是计算机系统，或含有商家电子商品目录的系统，假如有在线商品，就包含可以在网上履行的产品。
- 交易系统
  交易系统是计算机系统，或处理特定订单，负责付款、记录保留，以及负责交易上其他业务方面的系统。
- 付款网关
  付款网关是计算机系统，它按一定路线把付款命令发送到现有金融网络，进行信用卡核准和结算。

不同的体系结构使用这4种组件，就有不同的方法。在一些系统里，是把其中某些组件组合成一个计算机系统，而在另一些系统里，这四个组件分别由不同的计算机系统来实施。

一旦商务系统设计者选定了功能的总分配，还要定出许多次一级的功能，例如订单集合功能，把个人订购的商品集合成一份完整的订单，它可以作为商业系统、交易系统或客户的一部分来实施。

6.5.1 带有订单的Web服务器

带有商品目录网页和订单的Web服务器，是构成因特网商务系统的最简单方法之一，它

通常叫商家服务器，典型系统的图解如图 6.1 所示，而其逻辑图解则如图 6.2 所示。随着我们在以后章节讨论这项技术，许多技术上的细节会变得更加清晰，不过，我们在此先概述其基本思路。

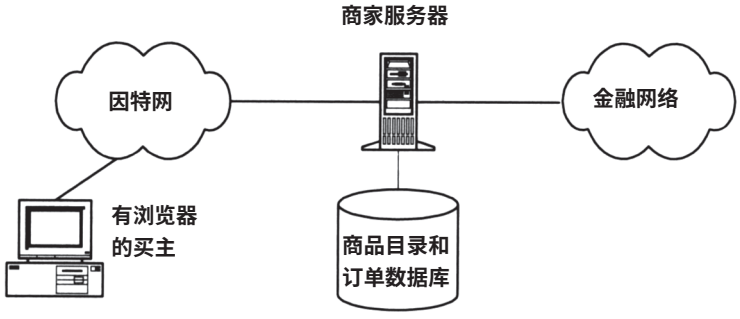


图 6.1 商家服务器：物理视图

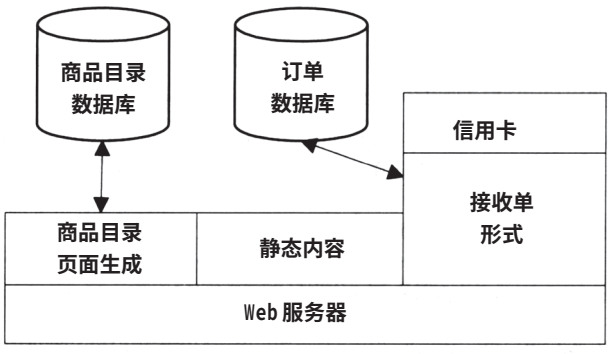


图 6.2 商家服务器：逻辑视图

在这一例子中，Web服务器提供商品目录内容和订单，换句话说，商家服务器和交易服务器组成一个系统，没有明确的付款网关。商品目录可由一组描述销售商品的Web网页组成，有嵌入式图像、图纸、规格、动画，以及视频和音频片段等。Web网页可能用HTML编辑生成静态网页，也可能由商品和说明性信息的数据库来动态生成。每一商品附近有一按钮，客户可以单击下单，或把商品加到购物推车随后再“校验”。当准备好购买某一商品（如果不止一种商品，就会显示在购物推车中），客户单击“校验”按钮，便开始进入交易的付款部分。

在因特网交易中，信用卡付款是当今消费者用得最普遍的方法（我们将在第十四章详细讨论）。简单订单可能列有要买的商品和一组字段，让客户输入信用卡付款的信息，包括卡号和有效期，如果是物质商品，还需要交货地址。订单还可能要求输入下订单的地址，因为有些信

用卡系统把它作为核实持卡人身份的一部分。

当然，Web服务器可能会使用不同的付款方法，其最简单版本中，Web客户没有特殊商务功能，因此商业应用就不需要额外付款软件，信用卡、订货指令和其他记账付款都可以用这种系统，它利用Web网上现在很普遍的基本安全能力。

这一基本体系结构可能适合或足以应付某些因特网商务应用，其主要优点是简单；不过，随在线商业的发展，或新技术、新组件的问世，基本体系结构的扩展可能会更加困难。

6.5.2 安全电子交易（SET）

SET即安全电子交易，它是一种标准方法，适用于因特网信用卡付款交易，在第14章会更详细讨论它，我们在这里只对它作一个结构上的介绍。SET系统在交易服务器之外再增加付款网关。

SET系统与带有订单的Web服务器的关键差异在于订单处理方法不同和付款通信处理方法不同。带有SET功能的因特网商务系统实际框图如6.3所示。

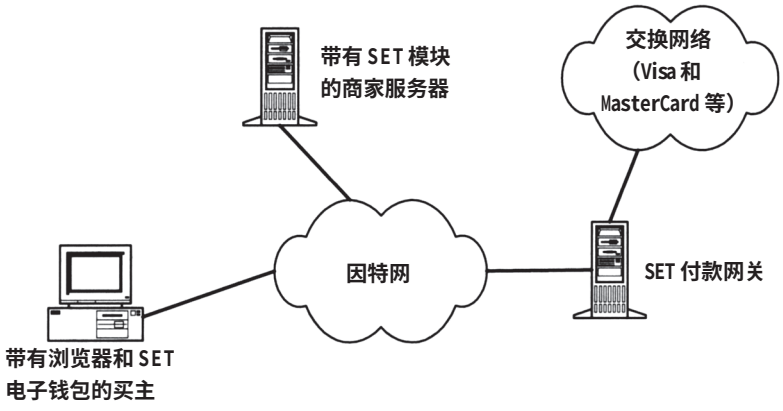


图6.3 SET体系结构

在SET的最简单形式中，遇到适合信用卡付款，SET体系结构就会从商家服务器那里将订单接过来。这样，商家服务器不直接与信用卡核准网络连接，而是装入SET商业模块。当调用它来处理付款时，就有以下步骤出现：

- SET商业模块发信息到买主计算机上的SET电子钱包，信息包含订单明细和总价。
- 买主用SET电子钱包来选择某一种付款卡并下单
- SET电子钱包通过商家计算机与商家收款行的SET付款网关通信。
- 付款网关链接传统金融网络以核准交易。
- 商家计算机把确认信息储存，然后发送一份发票给买主。

6.5.3 “ 开放市场 ” 商业体系结构

其核心体系结构的思路是，用“ 安全链 ”技术把内容管理和交易管理分开。这一思路使多个商品目录服务器能够分享一个交易引擎的能力，并使系统的内容部分与交易部分分开扩展。它还可以使服务机构成为商业服务供应商，向其他公司提供外包基础上的交易管理服务。图 6.4 显示了其实际结构，而图 6.5 则显示功能如何分布在系统的不同要素中。在此体系结构中，交易服务器与商家服务器分开，付款网关有否分开，可能要取决于它们支持的是哪一种付款方法。

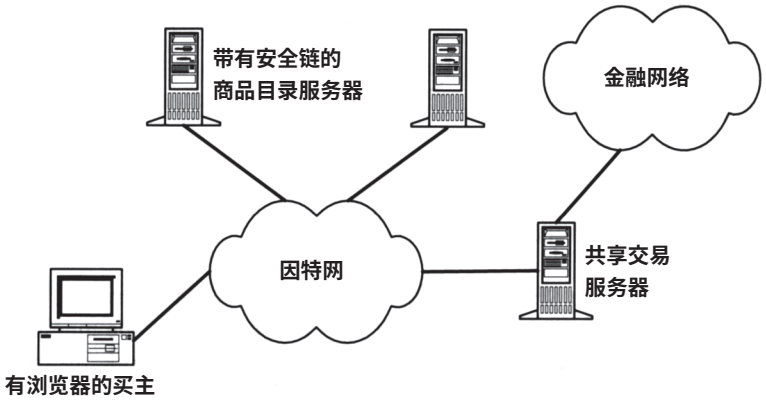


图 6.4 开放市场商业体系结构：实际视图

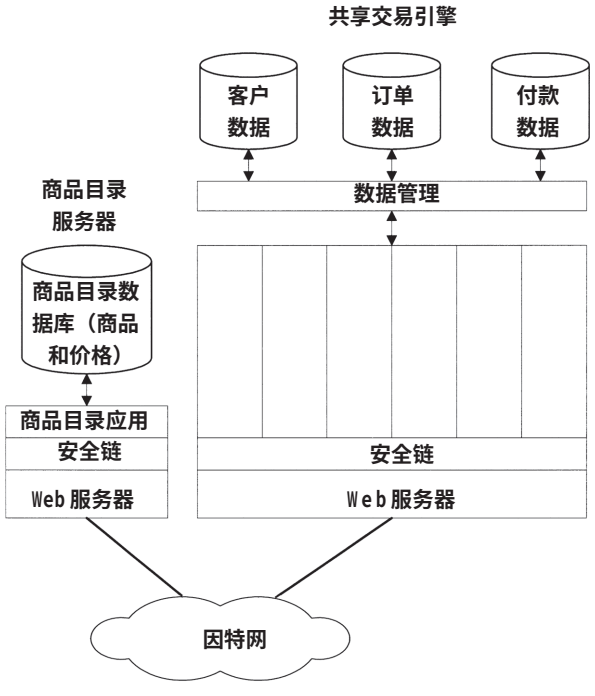


图 6.5 开放市场商业体系结构：逻辑视图

6.5.4 因特网开放交易（OBI）

因特网开放交易（OBI）是由OBI联盟提出的一种标准提案。OBI联盟由买方机构、卖方机构、付款机构和技术公司构成，它们共同解决了B2B商务问题。OBI的核心思路是，把商业系统的功能分成买方活动和卖方活动，这样由每一机构处理与自己有逻辑联系的那些功能。

OBI设计基于企业商务的一种模式如图6.6所示。在这种模式中，逻辑上把活动分成买方的数据库、申购者资料和批准过程，以及卖方的商品目录、订单管理、履行和付款。这一结构如图6.7所示。OBI关键思路与我们功能组件有关的是，把交易服务器分成卖方和买方。

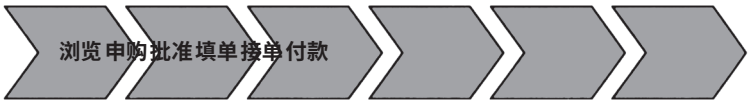


图6.6 OBI企业订货过程

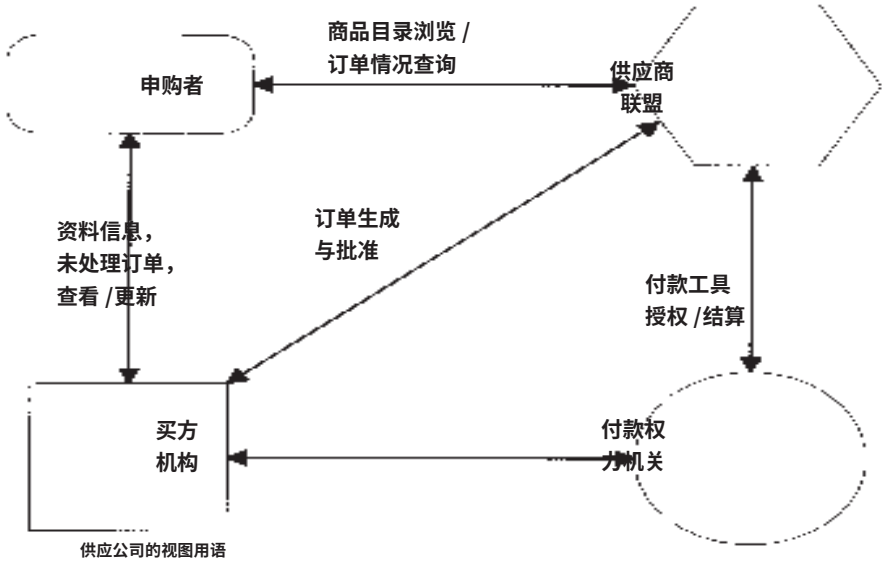


图6.7 OBI体系结构

为使这一结构行之有效，在买卖双方的组件之间，就需要有相互可操作的两个要素：申购者鉴别和订单处理。

- 申购者鉴别

  由于买方机构在OBI模式中负责管理申购者联盟，卖方一定要有一套标准方法来鉴别买方机构核准过的未来申购者，OBI使用公用密钥证书以达到此目的。当申购者浏览供应商的商品目录时，要出示买方机构签出的证书使自己合法化，这也就意味着，公司

之间建立交易关系时，供应商的商品目录一定要具备认可证书的功能。

- 订单处理

  在OBI，申购者通过与供应商商品目录的互动来下订单，接着订单在一个叫“ OBI 订单请求 ”的标准格式里从卖方 OBI 服务器被送到买方那里，进行必要的核准程序。订单敲定后，退回卖方按 OBI 订单来履行。

选择OBI设定的功能，其真正好处只有在多家买方公司与多家卖方公司做交易时才能显现出来。在这种情况下，买方可以集中管理自己的申购者数据库和批准系统，与多个交易伙伴无缝共用这些系统。同样，面对多个订货者，卖方机构可以利用主商品目录和订单管理系统。在这一理想态势中，买卖双方无需复制信息。

OBI 模式交易流程

本节我们浅谈了 OBI 交易，这些描述在图 6.8 中用带有标号的箭头与之一一对应显示。

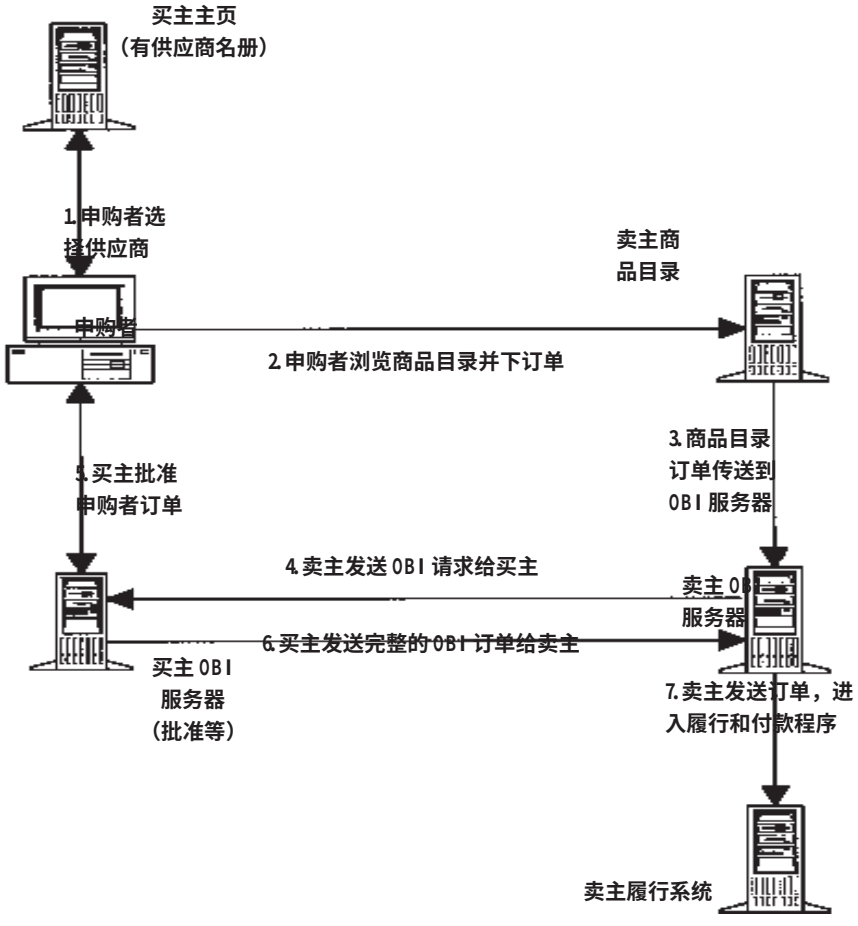


图 6.8 OBI 交易流程

1. 申购者使用Web浏览器来链接买方机构的交易服务器，选择超级链接至卖方机构的商品目录服务器。
2. 卖方机构商品目录服务器用数字证书鉴别申购者，允许他浏览、选择商品和下单。
3. 订单内容从商品目录服务器传送到卖方机构的OBI服务器。
4. 卖方OBI服务器把订单绘制成OBI订单请求，压缩成OBI对象（带有选择数字签名），通过因特网将它传送到买方机构的OBI服务器。
5. 申购者在订单上做必要的详细说明，再履行内部批准程序。
6. 已批准的完整订单被绘制成OBI订单格式，压缩成OBI对象，通过因特网发回卖方机构。
7. 如果需要，卖方机构获得付款授权，开始履行订单。

有关OBI的更多信息，请访问：http://www.supplyworks.com。

6.6 小结

总之，一个项目要获得长期成功，因特网商务体系结构（象任何复杂的计算机体系结构那样）在其中起着巨大的作用。快速拼凑一个系统来解决一个特殊问题，这差不多总要容易得多。不过，这样的系统无法面对未来的挑战，很快就会被淘汰，即便是对原先的目标来说也是如此。仔细地构建一个体系结构，注重企业面临的挑战和将来可能出现的变化，它就可以有所发展，可以适应成长、新挑战和技术创新的需要。在一段长时期内，预先投资会有巨大回报，我们想要的就是上述这些优点，而不是“现在就让它运行”这样的短视行为，这一决定很重要，我们应非常谨慎对待之。

假如现在有了一个体系结构，起码是简单的结构，我们就可以考虑一些策略来实施这个商务系统了，这正是下一章的主题。

第 7 章实施策略

罗马不是一天建成的，如果是，
我们早就把那些工匠都雇来了。
——波士顿中心干线项目广告牌

7.1 计划实施

任何操作过企业计算机系统的人都知道，难对付的部分不是设计或甚至编程，而是如何长期确实而有效地操作这个系统。从概念上说，在因特网上接受信用卡很简单，不过，如果清晨 6 点在西岸办公室链接金融分理机无效，而东岸客户要买东西，那该怎么办？本章谈实施和操作因特网商务系统的一些方法。在设计、研发和操作一个项目的不同阶段，一定要选择利用内部资源和外包。表 7.1 概括了本章考虑的某些选择。

设计因特网商务系统，要考虑以下 5 个阶段：

1. 项目设计
2. 软件开发与集成
3. 内容创建
4. 部署安装
5. 长期操作

对于每一阶段，内部开发或外包可能都合适，我们的讨论也许包括外包。例如，比起内部开发来，可以利用某一卖主的现成软件。

表 7.1 实施选择

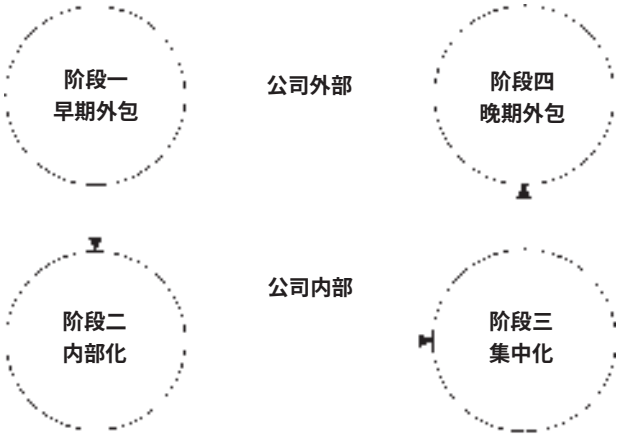
	内部	外包
项目设计	推销和 IT 人员	商业咨询
软件开发	定制开发	现成软件
内容创建	推销人员	Web 网开发人员
放置和操作	IT 人员	因特网服务供应商
交易服务	IT 人员	商业服务供应商

7.2 外包

对运行的服务系统，究竟是内部承担，还是外包给专业机构，哪一种方法最好，提出这一问题，对我们很有用。因特网商务也是如此，因特网技术发展很快，没有一定的助力，将难以跟上。Forrester 研究有限公司设计出一种模式，用于实施外包策略，它如图 7.1 所示，包括四个阶段：

1. 早期外包——在初期阶段，信息服务（IS）机构创建一个系统可以快一些，约请外部专家鉴定，着手发展必要的技能，因为在鉴定新技术方面，外部专家通常要比大公司用户更快。
2. 内部化——如果第一阶段成功了，着手发展必要技能的相应 IS 小组就可以将早期外包接管过来。有了新技能，以及对企业的详细了解，他们可以扩展配置，还可以定制应用，以满足企业的特别需求。
3. 集中化——随着技术的延伸，就可以支持这一系统在整个企业内运作，当然还需要限制开支。为此，系统转由一个 IS 中心小组来负责。
4. 晚期外包——随着应用进入遗留状态，继续操作可能很重要，但它可能不再是企业的核心部分了，还可能会影响到 IS 小组的新技术开发和对商业机会的把握。在此阶段，外包给专业公司也许特别诱人，因为外包者为许多客户操作类似应用，产生了规模经济效应。

对许多应用来说，这一模式很有效，而在因特网商务应用中，尤其适合考虑这一模式。外包因特网商务系统的实施和操作，一个公司就可以更快地建立起自己的因特网存在并定出方向。早期经验对日后开发应用，其价值不可估量，它可以推动内部开发。内部小组掌握了新技术、新技能，将企业的其他部分同商业应用系统更紧密地结合起来了。



美国马萨诸塞州剑桥 Forrester 研究有限机构视图用语

图 7.1 技术外包生命周期

分析外包与内部开发的另一种方法是，考虑项目与企业的密切相关程度。

- 项目是否具有核心竞争力？
  企业内部是否具有所需的开发能力，掌握了所需的操作技能了吗？如果还没有，为了成功，就必须招聘和培训，这个项目能证明这样做是正确的吗？如果答案是否定的，那么也许更适合外包？
- 技术是商品吗？
  这是个难题。如果有关的技术不是商品，那么，必要的开发技能只能从少数的专业渠道那里获得。对内部管理来说，商品化的技术也许相对廉价。考虑操作也许相反，如果一个项目的操作成了商品，外包操作也许就有了规模经济效应，胜过内部操作。
- 技术和项目的变化速率如何？
  希望技术和项目的变化很快吗？如果是这样，那么和企业紧密相关的内部开发就可能会有所体现。应用变化慢，外包起来也许很安全，也（几乎）要被遗忘。
- 项目的一体化要达到什么程度？
  如果项目和企业核心系统的接口很少，且定义良好，那么这也许是外包的优选项目。反之，如果出于复杂和定制一体化工作的需要，要把现有内部系统和应用融合在一起，那么内部开发和操作也许会更有效。

7.3 定制开发

开发因特网商务应用的方法之一是开发定制应用，无论是内部开发，还是与外公司签约。当然，优点是，如果开发成功，这个应用可能会满足特别企业的需求。而且，定制应用可能会与个别企业的其他系统更好地结合起来。在因特网商务应用组装式产品市场还很年轻以及产品发展很快时，这一优点尤其显著。

另一方面，定制解决方案有几个潜在问题，在作出“做或买”的决定时应慎重考虑。

第一，开发速度很快，质量并不总是很好。因特网商务应用定制开发吸引人的方面是“上马很快”。的确，在Web服务器上拼凑一个简单的商品目录并不难，或许还要加上基本订单来收集信用卡号。有时，让一个系统迅速运转起来，在因特网上建立一个存在，这很重要。不过，短期系统可能不能适应长期需要。它如何与其他系统结合？如何处理客户服务？系统如何随新技术改进？如何解决安全问题？如果因特网是企业的战略方向，而不只是战术表演，我们就应该按长期方向的思路来探讨。

第二，目前，定制开发可能比使用现成产品更费时间。因特网商务应用产品，在特点、成本和质量上的扩展很快，因此，也许会有产品能满足或几乎满足个别企业的需求。

第三，如何维持定制应用？内部人员会继续为它工作，或他们要从事新项目吗？还是叫外面顾问或集成商来维持？他们会长期维持吗？

第四，定制开发往往有看不见的费用，原先确定的项目可能在某些思路和特点上会有所遗漏，后来修改所需的费用很高。有效地维持定制系统（按定义说，是惟一的），其费用可能比预期的要高。总之，随技术创新而改进系统，其费用有哪些呢？

第五，毫无疑问，企业需求在一段时间内会有所变化，因此软件也需要有所改进。改进进展顺利，超过了维持范围，就需要修改软件、扩展新应用和解决新问题等。虽然需求如何改变，软件隐含那些东西，往往无法预测，但我们可以极为自信地预测，改变是注定要发生的。

第六，技术会创新，而且速度可能会很快。定制应用会有足够的灵活性来适应发展吗？定制应用小组掌握技术快不快？技术创新是否需要我们重新考虑整个应用的系统结构呢？

弄清楚这些问题，在企业开发任何重要应用的过程中是很重要的。有时，企业需求很特别，定制开发证明了这一点；有时，考虑到长期费用，我们认为，依靠现成产品，加上某些集成和适当的定制，将会更有效，即使无法达到原先的所有目标也会如此。

7.4 组装式应用

在因特网商务应用的早期，几乎每一个系统都是独立的，它们被开发成特定规格作为定制实施系统。当然，在一段时间内，许多软件产品已出现在商务应用市场上了。今天，这些应用系统在价格、能力，以及应用开发者要做多少工作这些方面差异相当大。商务产品可分为几大类：

- 内容创建和管理
- 订单处理
- 履行
- 系统集成

即使在这些大类中，产品范围也很广。例如内容工具，从简单的HTML编辑程序到创建、管理和绘制整个Web网站的高级系统都有。

这些产品的细节将在本书其他地方讨论，不过，在选择产品时，有几个一般问题要加以考虑。

- 作为应用组件，产品是否满足要求？（例如，内容创建工具能处理预期的各种内容形式吗？）
- 产品是否能与其他产品相兼容（如果需要时）？尤其是，能否与其他类别的最佳产品相兼容？
- 产品能否与必要的遗留系统（如存货管理）相兼容？
- 产品有否考虑适应因特网商务应用的长期发展？

- 产品能否定制以满足特别需求？
- 产品是否可以扩展？
- 产品背后有什么支持？

每当有可能时，在选择目前的商务应用产品时，看它如何适应商业项目的一切范围，而不是适应孤立的某一方面是很重要的。可以用它来完成工作，就是最好的工具，也许与每一类中的最高级工具之间存在极大差异。总之，混合方法也许很适用，有提供核心功能的组装式应用，还有结合应用现有商业系统的定制软件。

7.5 因特网服务供应商的角色作用

因特网服务供应商叫 ISP，它提供因特网商务所需的许多服务。首先，ISP 让个人和机构链接到因特网上，这样，它们的客户就可以与其他因特网用户通信；其次，ISP 常向 Web 网站或其他因特网应用提供放置服务，安装并操作由 Web 网站组成的服务器和软件。在这种情况下，服务器系统通常放在 ISP 那里，而不放在客户这里；其三，ISP 可以提供交易服务，如付款系统以供其客户商业上的操作。我们称提供这种服务的 ISP 为商业服务供应商（CSP），下面我们会更详细地讨论。

7.5.1 通信服务

ISP 服务的核心是提供通信，尤其是因特网系统基础，包括 IP 分组路由、域名服务（DNS）和电子邮件。通信服务系统可用拨号、ISDN，或专用数据线路（如 T1），它们有多种带宽可供选择。带宽有效地测量单位时间的数据流量。需要的带宽取决于应用，不过经验告诉我们，就因特网商务系统的一定性能来说，T1 连接（提供 1.54 兆 /秒），或起码是合理的细分连接是需要的。

域名服务（DNS）用于把服务器名如 www.mydomain.com 转换到 IP 地址如 10.250.92.7。多数 ISP 也满足域名（如 my-domain.com）登记的需要，这样别人就可以找到。

选择 ISP，要解决几个重要问题：

- 带宽费用
  ISP 通常还可以根据应用的情况，帮助客户选择成本最合算的带宽。
- 出站连接
  因特网是相互连接的网络集合，这就是说，有些 ISP 会更接近因特网中枢（因特网高性能核心）。网站和客户之间的有效带宽，既取决于网站的 ISP，又取决于客户的 ISP，还取决于中间所有其他的 ISP。
- 可靠性

ISP服务有多可靠？它们对问题的响应有多快？同其他服务一样，可以与ISP的其他客户交谈，从中了解ISP的情况，这常是个好主意。当然，可靠性更高，客户服务质量更好，费用也许就更多，因而对此要有所准备、有所考虑。有些ISP可以提供冗余链接（当然，费用更高），这增进了整体可靠性。如果是这样，就要弄清楚有多少冗余。例如，在你的网站和ISP网站的相同路由器之间也许会有两条线路，这可能防止线路失效，但它不一定会处理路由器失效。再说，由于无法辨别线路实际上是怎样走，所以，甚至可能会出现这种情况，即到头来使用的竟是电话系统里的同一条光缆，也就是说，根本就没有什么冗余。

- 额外服务

  ISP提供哪些额外服务？你的应用需要这些服务吗？如果不需要，你是否要为它们付费？

ISP的性能和可靠性，是因特网商务应用性能和可靠性的基础，因此，非常重要的是，找一家ISP，它可以提供你所需的服务水平，而且收费又符合你的预算。

7.5.2 主机服务

除了基本通信服务，许多ISP还提供主机Web网站的额外服务，即在ISP公司内提供操作Web网站所需的计算机和软件。对许多企业来说，这种方法有几个优点：

- ISP有一批训练有素的员工来操作。
- ISP可以（通常）提供24小时的操作与支持，已有证明，小公司很难做到这一点。（换句话说，ISP在这一点上有规模经济效应。）
- 由于Web网站可以直接链接到ISP中枢，比起放置在公司网站，用户可以使用更宽的带宽。
- 操作费用可以定为以一段较长的时间来摊付，也可由许多客户共同摊付，这样，企业就能以较低的成本来享有服务。

当然，还有一些缺点，最大的缺点是没有控制权：公司要依赖另一家公司来提供重要的操作服务。ISP还可能会限制何时更新、如何更新Web服务器上的内容。尽管要考虑这些限制条件，但是，享用ISP放置服务，往往非常有效。

选择ISP的放置服务，应估计到以下几个问题：

- Web服务器要使用哪一种硬件？它是否可以运行你需要的软件？
- Web服务器使用哪一种软件？它是否支持你的需求？你可以为自己的应用提供自己的程序吗？谁处理软件的配置？

- 对可靠性，ISP 会有哪些承诺？其他客户感觉如何？
- 硬件、软件和网络有哪些性能可预期？这是否够用？如性能与实际不符该怎么办？你的应用会有自己的系统吗，或是与别的应用共用一台计算机呢？ISP会为你处理平均负载，同样也处理峰值负载吗？
- 如何更新 Web 服务器里的内容？你可以使用你想要的工具吗？如果不能，ISP 所要求的工具能满足你应用的需要吗？
- 如何处理系统安全？操作系统得到了合理的保护吗？管理它们谨慎吗？在适当位置有没有防火墙？ISP人员如何处理潜在安全事故？软件组件有没有跟上软件商的补丁程序而保持最新呢？
- ISP员工可以提供你所需要的服务吗？他们是否会因服务别的客户而太忙，无暇给你必要的关照呢？
- 得到你所需要的服务水平会有多少费用？除了基本费用，还有附加费用吗？

有了基本通信服务，重要的是选择 ISP，它既可以提供你所需要的服务，收费又合理。虽然可以更换 ISP，但更换时交易事务的处理，可能会很困难，因此，建立网站之前，值得花些时间和精力去了解 ISP 可以为你做些什么。

7.6 商业服务供应商（CSP）

除了因特网商务应用放置服务，下一步是交易服务：提供接收订单、付款和履行的基础设施。我们把提供这种服务的实体叫做商业服务供应商（CSP）。因特网服务供应商（ISP）往往是CSP，其他类型的机构也可能是CSP。例如，银行可能向自己的商家客户提供因特网商务交易服务，作为服务的延伸。有些因特网“商业大街”也提供类似服务。

CSP通常也提供放置服务，但并非总需要这样做。有的系统结构（如第6章讨论的）需将内容服务器和交易系统放置在一起，有的则不用。

关于商业服务供应商，我们提出以下重要问题：

- 目前支持的是哪一种付款系统？将来可能要增加什么系统？
- CSP 是否处理你所需要的那种商业模式（例如，信息商务、消费者零售等）？
- 成本结构如何？收费是按统一费率、交易量或交易额等来计算的吗？
- 卖主可以得到那些报表吗？
- 资金如何与何时转到卖主手中？
- 可以为每个卖主履行哪些定制的订单处理和付款程序？这能满足你应用的需要吗？
- 订单处理和付款程序的外视感觉可以定制到打出了你网站的品牌吗？
- 卖主要处理哪些事？CSP 呢？

7.7 项目管理

说这个似乎太老套了，不过，如果因特网商务应用要成功，那么关键之一就是把工作完成。一个典型的商业项目会涉及到多家卖主的软件，内部小组或外来顾问的定制开发（或起码是定制），几个机构的操作服务，新应用与现有商业模式和做法的一体化，以及其他许多活动。缺乏有效的项目管理，未必能让所有各个部分集聚成一个成功的系统。

这虽不是因特网商务具有魅力的那部分，但恰是最重要的部分。尽管项目在细节上差异极大，不过，它们还是有一些共同的问题：

- **成本估算**
  项目的真正费用可能有哪些？这包括软件产品、产品定制和扩展所需的时间和精力、从因特网获取实际产品和服务的销售信息、访问因特网的费用，以及开发和操作所需的人力等等。常见错误是，把预支的软件费用当作主要费用，其实基础软件的定制和补充部分，其费用也许要高得多，操作费用也要高得多，这要视应用详情而定。因此，重要的是，着眼于项目所有者的费用，而不仅仅是最初的软件费用。
- **受益评估**
  开发商务应用有哪些预期受益？此项目是战略投资，还是短期回报？预期的主要受益是降低成本（例如，减少商品目录的印刷和邮寄费用），还是增加收益？这是试验性项目，要被大规模的（和有可能是不同的）系统所取代，还是主要系统？考虑好预期受益（确定这些预期受益是公司分享的），就有可能在一段时间内对其作出评估，并保证公司能对其成功与否作出评价。
- **规模预估与操作**
  不仅在商务系统，就是在任何因特网服务系统，要预估其所应具有的操作水平和规模大小都特别难。通常的问题是，一个有趣的网站可以在短时间内吸引大量访问者，因为口头信息可以在因特网上极迅速地传开。如果网站超载，操作很差的坏名声就会很快传开，这种“使用堵塞”造成紧张时期的现象有时叫“快速拥挤”[①]。我们建议，应该设计一个系统，可以满足预期的高峰值负载需求，也可以满足预期的平均负载和服务需求。这些设计应与系统“成功”负载量和“成功”用户数的设计分开来考虑，因为设计的目标是处理潜在负载，考虑潜在负载要比考虑“什么才算成功”更为重要。
- **人员**
  项目是否需要一定的内行技术人员来操作？是否需要专业顾问或专业承包商？小组是否需要接受软件或技术方面的额外培训。

---

①“快速拥挤”这一词语是科幻小说作者拉里·尼文在名为“快速拥挤”的短篇小说里杜撰出来的（1971年《飞行的房屋》）

- 维护、支持和升级
  商务应用预期的发展是什么？软件组成部分是否与预期的发展相适应？定制组件及其扩展由谁来维护和支持？软件升级有否稳定编程接口，可以和别的系统相兼容吗？商务应用开发，总是没有考虑到长期计划，这样，在一段时间内，产品与技术的改变，会让它们孤立无援。即使最精心设计的项目，也可能会有这样那样的改变，不过，事先慎重考虑，谨慎设计，可以避免许多这样的问题。事实上，这就是我们在本书提倡的，要关注因特网商务的系统结构和长期问题的原因了，而不是侧重今天可以完成的那些细节。

7.8 保持最新

技术不言而喻的是它总在改变。在因特网世界，技术发展特别快，我们想跟上最新和最重要的技术，无论是 Web 网、实时声音、Java 语言，或是还未构思出来的、令人振奋的想法。希望稳定和推动快速发展，这是一对矛盾；改革成本和害怕落后，这又是一对矛盾。因此，就值得把受益、费用，以及新技术同因特网商务应用紧密结合的实质考虑得一清二楚。

7.8.1 企业方面的问题

- 我们提到的改革对现有系统影响如何？有时，改革对现行应用系统几乎没有影响，或没有直接影响；有时，可能的改革也许要冒损害现行应用稳定性的风险，对这种改革进行评估和试验，一定要慎重。
- 你的小组是否掌握了必要的技能？技术创新要求工作小组不断掌握新技能以将其实施于应用之中。小组继续教育很重要，但是一定要和技术创新的日常工作步调一致。这里提出一个有用的问题，就是技术或者说技能是否与公司的发展战略相适应？
- 费用有哪些？在应用中，实际上要采取哪些措施来实施新技术？费用可能来自软件、新开发或定制开发、人员培训、运行新软件的新硬件，或加上日常操作。无论哪一部分费用，重要的是，着眼于新技术的整体费用，这也许远比只得到一个软件包的费用要多得多。
- 客户和公司每年可以掌握多少创新技术？尽管我们列出了其他所有因素：客户喜欢（或起码不会介意）创新，这种技术看起来是长期赢家，费用还可以接受，小组掌握了（或可以掌握）必要的技能，但是，客户（或公司）在一定时期内可以掌握的创新技术还是有限，有时，在所有其他活动进行的前前后后，要吸收的创新技术可能太多了。

7.8.2 客户方面的问题

- 你的客户有什么软件？有些新技术的特点要求客户的系统要有附加软件。例如，实时

声音应用可能需要特别软件来回放声音文件。要从新软件中受益，不但要修改应用，而且客户也要安装系统的附加组件。有时，发行客户软件要作为应用的一部分来完成，就会有额外开发和客户服务费用。不要忘记这种所需的客户软件对客户使用平台（操作系统和其他核心软件）也一定是通用的。

还有一点也是重要的，就是要记住：使用系统的客户也许不拥有和不管理计算机系统。如果应用需要特别客户软件就需要与每一个企业客户的IT部门商谈，确保安装上合适的软件，可以操作。

- 你的客户有什么要求？他们在意吗？有些客户也许非常想让网站也有最新技术，如多媒体音频和视频、Java应用等；而有些则对这些技术一点也不感兴趣。因此，在作出这些技术上的决定时，了解客户是极为重要的。例如，目标客户是十几岁少年的网站和电子工程师选用配件的网站相比，前者应用多媒体来吸引客户的情况也许会普遍得多。
- 客户对技术创新反应如何？有些客户群体对技术迅速发展会感到不快，熟悉与稳定对他们来说是很重要的，所以，应用的创新就不需要考虑他们。
- 客户预期是什么？客户真的很希望迅速采用新技术吗？或是他们希望发展平稳而审慎？技术发展与预期相一致，有助于客户产生企业是如何运作的这样一种感觉，这可以使企业的计划执行得更加有效。
- 是一时狂热还是一种潮流？有些技术寿命很短，而有些则成为企业计算机系统的核心部分。而在早期，这是很难分清的。陷入一时狂热，可能会在不可用的技术上花高价去运作，却与基本潮流擦肩而过，这可能在宝贵时间上输给竞争对手。虽然什么样的技术不总是能分得一清二楚，但是把这些问题想透彻，有助于作出投资决定。在对待诱人的技术时，要看它是否会对企业产生长期的重大影响，这一点尤其重要。

提出上述问题，是想有助于指导如何把新技术应用到商务应用中去。从许多方面来说，他们代表了一个注重实效的观点，往往与对新技术的兴奋和幻想意见相左。另一方面，人们很容易陷入这种兴奋之中，提出这些问题，有助于人们以现实态度来理解受益和费用。

7.9 标准的作用

因特网的部分核心哲学是使用标准，以确保不同卖主的部件相互可操作。因特网核心协议TCP/IP确定不依赖任何卖主，它让不同人拥有的、不同厂家制造的、运行不同软件的两台计算机可以相互通信。

标准到底是什么？在计算机企业，我们常谈两种标准：法定标准和事实标准。首先，法定标准是公认权威机构规定的标准，这些机构包括国际电信联盟（ITU）、美国国家标准协会（ANSI）和因特网工程任务组（IETF）。在公司和机构代表参与特别技术领域开发的协作过程

时服务，有两大问题：

1. 日常操作是否需要有人在下班时间操作？这问题适用于因特网企业没有自动化的任何部分，例如，如果交易系统需要有人来批准订货指令，这一功能肯定要随时都有效，也就必定随时都要有人在场来承担这一任务。
2. 如果自动化系统下班时间失灵该怎么半办？计算机系统或网络出了问题，通常要有内行人来找出问题修好它。如何找出问题？如何通知合适人选？对问题的解决有特殊时间要求吗？例如，某项目设计规定：有的故障得在1小时内修复，有的则要在4小时内修复。

当然，不同企业对自己的有效性和响应能力有不同的要求，这取决于客户种类和预期，因特网的从商方法，训练有素人员的可用程度，以及企业提供这种水平的服务愿意投入的资金。重要的是，一开始就要把这些要求考虑清楚，并且决定怎样的服务才是理想合适的，而不是在计算机和网络链接失败时惊慌失措。

最后，如我们前面讨论的，因特网商务系统外包操作，提供了一套高效运转的系统，因为处理这种外包的多数机构，有计划、有人员，能使系统24小时有效运转。当然，重要的是，一要确保系统能达到预期的服务水平和问题响应能力，二要确保合作双方能就此达成一致协议。

7.11 安全设计

调查显示，安全往往是因特网商务系统设计中要关注的首要部分之一。确实，系统安全对其获得长期成功起着关键性的重要作用。在因特网商务项目的设计、实施和操作阶段，有许多重要的安全问题。

我们在第十三章详细讨论安全问题、技术和解决方法。不过，在因特网商务系统的实施和操作中，我们必须以安全角度强调，对系统进行持续监控和评判是很重要的。在开头设立一个系统正确无误，但后来却漫不经心地操作，渐渐损害系统安全，这是很有害的，这差不多等于装了门不上锁，贻害无穷。

7.12 多机构操作

在一段时间内，开发一个健全的因特网商务系统，几乎可以肯定，需要许多机构的共同努力。在本章，我们已谈到了有可能的几个参与者：

- 因特网服务供应商
- 商业服务供应商

- Web 网和内容开发商
- 付款处理机构
- 软件商
- 系统集成商
- 公司内部的不同小组

这些参与者往往不但参与了因特网商务系统的创建工作，还参与了日常操作。因此，出现问题，他们义不容辞要解决。这时，各小组顺利合作格外重要。联网的计算机系统出故障，往往难以找出原因，需要整个团队通力协作把问题找出来，而不是相互抱怨。当然，一旦问题找到了，也许很明细由谁解决，或是要团队共同解决。

尤其是性能问题，找出原因，难度往往极大。有的问题是，难以找出复杂系统卡在哪里，因为项目小组人员对许多组件和结构不是了如指掌；有的问题是，网络系统是共同设计的，默认了许多错误，尤其是在预定时间内得不到预定结果，就会重发数据，还会有多余的服务。当然这些问题同时出现，就可能找不出服务系统故障，因为发送器隔一段时间就会发送不同的服务项目，在用户看来，这种系统错误（服务系统失败）就是性能问题（用多余的时间反复发送数据）。

要最大机会地获得操作成功，在问题出现之前，可以采取以下几个步骤：

1. 确保所有参与者都明白自己在系统操作中的角色作用，也明白其他参与者的角色作用。
2. 使全体（或多数）参与者在日常操作中形成团队协作，这样，在出现问题时，人们和机构已习惯于团队合作了。
3. 事先设计如何解决特殊问题，这样，起码对可预见的问题有解决的办法。
4. 建立一套解决问题的工作程序，它有助于团队合作解决问题，而不是想让谁偶尔干些什么。
5. 获取（开发或购买）监测系统和诊断错误的工具，为解决问题做好准备。使用众所周知的工具来找问题，要比任意使用原始工具，任意调试容易得多。监测工具，如果使用得当，可以早早预警，不致造成严重后果。

这些提议大多与技术无关，却与合作的人、小组和机构有关，但是，要使企业的因特网商务系统获得真正成功，的确有许多首要问题要解决。如果团队操作不成功，那么，就是有世界上最好的技术也不会成功。

7.13 总结

受到计算机技术魅力的诱惑很容易，无论是因特网商务，还是其他应用，但是，技术只是

有效利用计算机系统的一部分（尽管是最闪光的部分），尤其是，因特网商务系统一定要使企业能够把价值交到客户手中。技术组件到位了，一定要这样操作，既要把价值交给客户，又要保证系统的可靠和安全，还要具有客户预期的性能。操作工作也许不吸引人，但确是商业成功的根本，不错，这正是我们所有工作的初衷。

本书的前半部分集中阐述因特网商务系统的非技术部分：弄懂商业问题，聚焦在客户身上，构建系统结构和从事设计。有了这样的观点，现在我们就可以转入因特网商务系统的技术组件了。

第二部分
因特网商务技术

第 8 章 因特网与万维网
第 9 章 Internet 商务系统建筑块
第 10 章 系统设计
第 11 章 生成与管理内容
第 12 章 加密法
第 13 章 安全性
第 14 章 支付系统
第 15 章 辅助系统
第 16 章 事务处理

第 8 章因特网与万维网

技术……就是未曾经历的世界照样也能巧妙安排。
——马克思·弗里希 ①

8.1 因特网商务技术

本书第一部分主要介绍因特网商务的业务问题，了解业务是因特网商务中计划一个成功系统的第一步。本书这个部分要深入介绍实现这些业务计划的技术，我们将介绍技术的核心原则（如怎么考虑因特网商务的安全性）和一些当前技术组件（如当今因特网上使用的一些通信协议）。核心原则提供了面对快速改变的技术进行决策的一些准则，而当前技术介绍则提供了一些实施知识以及演示如何一点一点地贯彻核心原则。

本章首先介绍有关因特网技术的内幕，首先介绍核心协议（TCP/IP），然后介绍一些关键应用区域，如万维网。我们还将介绍因特网的一些基础性设计原则。了解这些原则不仅有助于理解这个技术，而且有助于进行设计新系统的因特网经验累积。

下列各章介绍因特网商务中特别重要的技术领域，介绍商务系统的关键建筑块，商务系统内容的生成与管理，利用加密法提供安全性，系统安全问题，事务管理以及商务系统辅助服务的接口。然后我们介绍如何在有效系统设计中将这些组件联系在一起。

8.2 因特网的发展

因特网是由美国国防部投资的一个研究网络发展而来的。这是 1969 年开始建立的网络，最初称为阿帕网（ARPAnet），APRA 指高级研究项目局（Advanced Research Projects Agency）。随着时间的推移，这个网络不断扩大，大学、国防署和几个公司参加这个网络，主要是参与高级研究项目局投资的各种研究项目。随着网络的增长，其应用范围超出了研究，如电子邮件。这些新应用在进行其他各种项目的研究组中不断采用。

20 世纪 80 年代初，网络中引入了 TCP 和 IP（将在稍后介绍），这是当前 Internet 的核心协议。此后不久，随着 ARPA 在网络支持方面的作用下降，Internet 一词成了这个全球实体的新名称。Internet 一词来自“ internetwork ”，表示相互连接的网络。可以看出，Internet 是相互连

①马克思·弗里希，《Home Faber》，1957。

接的，它的增长不受集权控制。

如图 8.1 所示，Internet 中连接计算机数自 1969 年引入以来呈指数级增加。20 世纪 80 年代后期广泛引进域名系统（DNS）之后，注册域的增长和整个网络一样是指数级的。1992 年，欧洲原子能研究中心（CERN）发布了第一版万维网软件。此后，Web 服务器的增长速度比网络中计算机数的增速更快。

有人用 internet（小写 i）表示区别于 Internet（大写 I）的互联网络。曾几何时，这个术语常用于描述属于一个组织的网络，如使用 Internet 技术的大公司。最近，这种网络又称为 intranet。本章稍后将详细介绍 intranet。

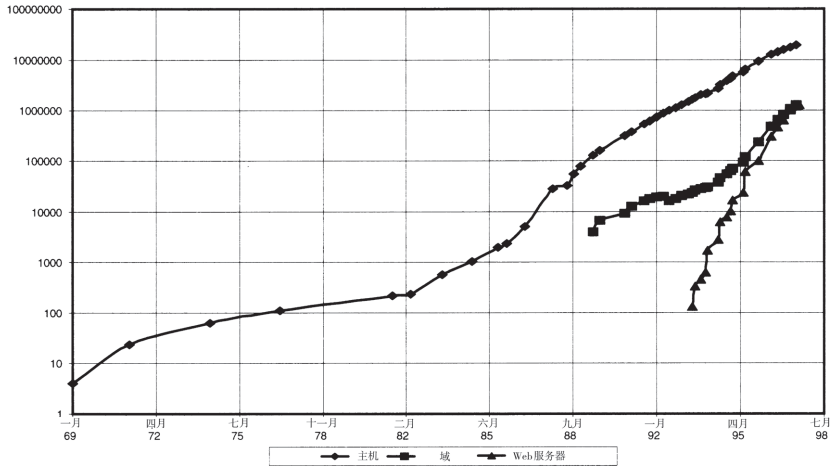


图 8.1 Internet 的增长

8.3 Internet 设计原则

Internet 的成功应归功于初期对其设计的一些基本决策。这些决策是最终用户看不到的，应用程序开发人员也看不到，但理解这些基本决策能够更好地体会到因特网为什么如此成功。此外，我们发现这种深层次理解有助于建立新应用程序时的选择。尽管这些应用好像离 Internet 的核心思想很远，但符合 Internet 设计精神通常比不符合 Internet 设计精神更容易取得成功。

Internet 的主要设计思想如下：

- **互操作性**

  Internet 协议的独立实现方法实际上是相互配合的。这在今天看来是显然的，但早期 Internet 中要达到这个结果，是付出了艰苦工作的。事实上，Interop 会议曾经是厂家测试产品互操作性的一个事件。如今，互操作性就是系统能将不同厂家的客户与服务器

计算机和软件集成起来。

在 Internet 商务中，互操作性就是卖方和买方不必同时从相同厂家购买与升级软件。当然，这就要求不同厂家的软件基于开放的标准，具有互操作性。

- 分层

Internet 协议是分层工作的，高层建立在下层提供的功能之上。例如，TCP 利用 IP 生成可靠字节流，Web 与电子邮件之类应用协议利用 TCP 的功能。这种分层体系结构如图 8.2 所示[②]。

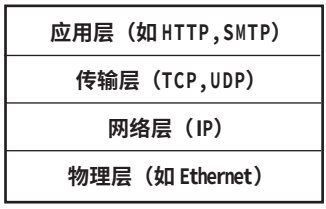


图 8.2 Internet 协议层

简单性

Internet 层可以从 IP 层向上看和向下看。IP 层本身很简单，只提供分组寻址和格式。IP 层下面是各种不同类型的网络硬件、拓扑与路由器，如以太网、拨号连接，等等。IP 将这些细节隐藏起来，使应用程序不必考虑这些细节，在 IP 层之上，TCP 之类的高层协议提供了服务抽象，使应用编程人员可以理解和使用。结果，应用程序开发人员和用户不必考虑不同网络设备的复杂结构以及低层网络协议的实施细节。

- 统一命名和寻址方法

IP 层提供了统一寻址结构，对网络上连接的每台计算机提供了 32 位地址。这些地址通常写成点号分开的四节形式，如 16.11.0.1。人们很难记住和使用地址，因此域名系统（DNS，Domain Name System）提供了将人们容易理解的计算机名（如 www.openmarket.com）变成计算机的数字地址。这两个系统加上实现方法的互操作性，使 Internet 能够顺利工作。

- 端对端

Internet 是利用端对端协议设计的，即数据的解释在发送系统和接收系统上发生，而网络只需要检查发送分组的图标地址。这与寄信相似，你把收信人地址写在信封上，然后把信投入邮箱。邮局不管里面放什么（只要不是危险品），你不管它是用车载还是用飞机运，只要在一定时间内送达目的地。相反，当你出门旅行时，可能坐的士上机场，

② 有些读者可能发现，这个模型与网络分层的常用 OSI 参考模型不同。Internet 应用程序通常不完全适合 OSI 模型，因此我们采用简化模型）。

乘飞机到另一座城市，然后乘公共汽车上旅馆，每一步都要分别买票和付钱，这就像网络中的按步系统或按链接系统，中间系统在应用层处理数据。

端对端协议有几个优点，可以隐藏网络的内部结构，包括 Internet 中使用的各种物理硬件，用户和应用程序不必关心这些细节。此外，它们向编程人员提供了简单抽象概念，使他们不必考虑从低级错误恢复之类的琐碎细节。

从这些简单思想引出了遍布全球的强大、壮实而可靠的网络。Internet 协议的标准与规范是由 Internet 工程任务小组（IETF）开发的，这是任何有志之士都可以参加的公开组织。随着时间的推移，IETF 将厂家、用户、研究人员、政府和其他人员拉到一起，开发和改进 Internet 技术。

8.4 核心网络协议

Web 使用了几个低级协议，特别是 IP、TCP 和 DNS。本书末尾的“资源与阅读材料”列出了几本 Internet 网络与协议技术方面的专著。

8.4.1 物理层

顾名思义，Internet 就是许多网络的网，物理层使用的不是单一技术。局域网使用以太网、令牌环、光纤分布式数据互联（FDDI）、异步传输方式（ATM）和其他技术，广域网使用点对点数据线路、拨号、帧中继、ATM 和其他服务。所有这些网络技术都用来传输和路由 Internet 通信流。在这些低级网络中，路由用网络内置的方法处理。大多数情况下，即使寻址方式也与 Internet 的寻址方式不同。

例如，以太网用 48 位通用标识符寻址与路由。

IP 网络用以太网建立时，末端系统用特殊的地址解析协议（ARP）将 IP 地址转换成以太网地址。

Internet 路由器与这些组成网络连接。这些路由器将分组从一个网络转发到另一个网络，直到到达连接目标系统的网络，然后路由器直接发送分组。每个路由器有一个本地网络图，显示根据 IP 头中的目标地址如何转发分组。如何转发分组的信息在大型网络中非常复杂，是用各种路由协议进行分布的，关于路由的详细信息可参见“资源与阅读材料”中列出的几份参考资料。

物理层的安全性取决于所用的网络技术。例如，有些网络系统包括物理网络中所有数据的加密。但这种加密并不延伸到离开这个物理网络的数据。路由器配置的安全性主要取决于简单口令、遮藏这些设备和检查篡改的副作用（通常是显然的）。

路由器常用作网络攻击的第一道防线。路由器配置是网络防火墙的一部分，设置成认真分开外部发来的可疑通信流与内部发出的可靠通信流、第 13 章将详细介绍防火墙。

8.4.2 Internet 协议

TCP/IP 一词通常指 Internet 的基础性网络协议。事实上，TCP 与 IP 是两个不同协议，但 Internet 中的大多数应用程序同时使用这两个协议。IP 就是 Internet 协议，是定义 Internet 的主要协议。IP 只处理数据分组，标上源和目标计算机的网址。网络负责将分组发送到目的地，但不保证送达。在网络中，分组可能丢失或重复，可能搞乱顺序。这种“尽力而为”的方法初看起来好像用处不大，但事实上，它是建立网络应用程序的强大子层。其他协议利用 IP 功能满足不同应用程序的需要。这种协议在 IP 分组中用协议标识符标识，使目标系统可以在上一层选择正确的处理协议。

IP 本身不提供任何安全服务。攻击者只要能够实际访问网络，就可以听取经过的分组，引入偶分组和截获与改变合法分组。地址很容易伪装，因此许多应用程序要特别注意，别太相信分组地址。最终，高层协议要负责管理这些问题，但防火墙之类的网络层技术常用于建立网络环境，使应用程序不必考虑这类攻击。

IP 的目前形式已经使用多年，几年来，IETF 定义了下一代 IP，称为 IPv6（第 6 版 IP）。IPv6 包括许多改进，如大地址空间、更易扩展路由系统和安全服务。IPv6 仔细考虑了逐渐过渡问题，因为 Internet 已经这么大，不可能一夜之间切换过来。过滤到 IPv6 将是一个漫长的过程，厂家要升级软件，网络用户要在站点中安装 IPv6 版软件。过渡期间，有些改进（特别是安全服务）可以在当前 IP 版本中部署。第 13 章详细介绍这些安全服务（称为 IPSec）。

8.4.3 不可靠数据报文协议

IP 之上最常用的两种传输协议是不可靠数据报文协议（UDP）与传输控制协议（TCP）。UDP 提供给应用程序的是非常简单的数据报文（或分组）服务，使应用程序能访问 IP 的基本功能，同时增加了几个其他特性。这些特性包括检查基本数据完整性与端口号，后者可以标识哪个应用是分组的真正目标（记住，IP 地址只标识系统，而不标识系统中运行的应用程序）。UDP 不提供任何可靠发送与顺序发送服务，因此分组可能顺序搞乱或根本无法到达。使用 UDP 的应用程序要提供所需的可靠性，但如何提供所需的可靠性则有很大的灵活性。使用 UDP 的两个重要 Internet 应用是域名系统（DNS，见稍后详细介绍）和 Sun 公司的网络文件系统（NFS）。

8.4.4 传输控制协议

传输控制协议（TCP）是 Internet 中最常用的传输协议。TCP 建立在 IP 的面向分组基础上，提供可靠字节流的抽象概念。应用程序发送数据，接收者按顺序收到数据（除非发生太严重的错误，TCP 无法恢复）。TCP 还提供流控制机制，保证发送者不会以太快速度发送数据，使接收方应接不暇。TCP 让接收方发送所收到分组的确认消息。如果发送方在一定时间内没有收到确认消息，则重传这个分组。每个分组还包含序号，因此接收方可以按顺序排列。因此，使用

TCP 的应用程序显示顺序数据流，不必考虑数据如何经过网络的细节。Internet 中大多数熟悉的应用程序都使用 TCP，包括 Web 与电子邮件。

TCP本身没有任何自然安全机制。尽管窃听者可以选择各个分组和方便地重构会话，但攻击者要改变 TCP 流中的数据则要困难得多。但是，要攻击未端系统，只要发送大量“新连接请求”，然后不进行协议的其他部分工作。这样就可以用尽操作系统资源，阻止合法连接。由于已经发生过几起类似攻击，因此厂家正在部署对付这类攻击的对策。网络防火墙也在一定程度上限制了这类问题。

8.4.5 域名系统

Internet 用 32 位数字地址将分组路由到网络上特定机器中的特定网卡。但是，人们喜欢使用机器或服务的名称，而不喜欢使用数字。除避免了要求用户记住和交流数字地址外，名称还有另外几个作用。

1. 可以将服务从一台机器移到另一台机器（即移到不同地址）而保持相同名称。这样，用户（和其他系统）就只需要记住服务名。
2. 服务可以用多台机器支持，这些机器使用不同地址而且有相同名称。

将可读名称变成数字地址的工作是由域名系统（DNS）完成的，DNS是将可读名称变成数字地址的快速可伸缩方法。www.openmarket.com 之类的 DNS 名称包括机器名（这里是 WWW）和点号分开的域层次（openmarket 与 com）。一般来说，域就是对计算机和服务命名的组织名，可能是公司、大学或各种实体。如图 8.3 所示，DNS 名称是层次式的，从右向左处理。层次的根表示为末尾的点号。程序需要一台机器的网址时，它查询本地 DNS 服务器。本地服务器查询远程服务器。根 DNS 服务器负责 com, edu, gov 和 mil 之类的顶级域，以及 us,ca 和 jp 之类的地区域（分别表示美国、加拿大和日本）。这些根 DNS 服务器只知道哪个低级服务器知道 COM 域。COM 域的 DNS 服务器再知道哪个低级服务器知道 openmarket 域，但不知道 openmarket 域中的名称表示什么。最后，openmarket 域服务器负责解释 WWW 机器的 IP 地址。

除了这些授权服务器之后，DNS信息可能暂时缓存在其他系统中，大多数客户都配置成接受这种非授权信息（因为它们不一定是最新的）。

DNS 还可以将 IP 地址转换成名称。如果要寻找与地址 199.170.183.2 相关联的名称，则要逆转数字顺序，用 -addr.arpa 域进行直接，得到 2.183.170.199.in-addr.arpa。它看起来像普通域名，得到的答案是 relay.openmarket.com。这个过程通常称为逆向查找，之所以可行，是因为网络地址的层次（从左向右）与 DNS 名称的层次相似。

这种将IP地址转换成名称的功能常用于访问控制和日志。入站请求没有相关联的名称，只有发送者的 IP 地址。由于访问控制和日志通常是由人读写的，因此使用名称更方便，应用程序通常要将 IP 地址转换成名称。

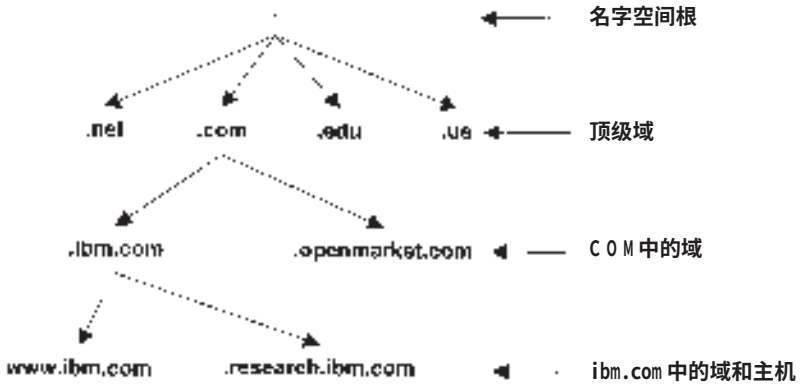


图 8.3 DNS 名称层次结构

但是，用DNS信息进行访问控制是有风险的。DNS在 Internet 中广泛使用，但使用DNS信息时，Web系统的安全性，取决于输入DNS的源信息和客户与服务器之间的中间DNS服务器的安全性。例如，假设Web服务器配置成只能访问 openmarket.com 中的主机。连接来自 IP 地址 199.170.183.2，服务器用 DNS 逆向名称查找确定这个地址是否开放市场组织的地址。问题在于，如果这个地址真是开放市场组织的地址，则一切顺利；而如果不是，则DNS逆向查找从攻击者的DNS服务器中取得这个问题的答案。要防止这种现象，一种办法是查找DNS中的名称，看看地址项是否相符。对大多数应用程序，通常用DNS将名称转换成地址，而不靠DNS结果验证消息源。

8.5 万维网

1992 年，欧洲原子能研究中心的 Tim Berners-Lee 首次推出万维网。由于Web的强大与可访问性，使其迅速普及，人们甚至把Web与 Internet 本身混淆起来。

万维网——概要

万维网将联网信息与超文本技术结合起来，提供了方便而强大的全球信息系统。

这个项目将网络上可以访问的任何信息放在无缝的超文本信息空间。

Web最初是为了在全球分布的组织之间共享信息，由支持小组分解信息。万维网最初的目标是针对高能物理社区，但之后迅速分布到其他领域，吸引了用户支持、资源发现和协作工作领域的广泛注意。W W W是目前 Internet 中部署的最高级信息系统，将过去联网信息系统中的大部分信息都包括在Web数据模型中。

事实上，Web体系结构还将包括今后出现的任何技术，包括新网络、协议、对象类型和数据格式。

Tim Berners-Lee 让 World Wide Web 于 1992 前后

From http://www.w3.org/Summary.html

8.5.1 Web 基础

万维网是全球几百万台Web服务器与无数Web浏览器通过超文本传输协议（HTTP）连接而成的全球超文本网络。和 Internet 一样，Web 也迅速地增长，任何时候都很难准确说它有多大市场。Web服务器提供多媒体信息页，Web浏览器显示多媒体信息页。页面通常用超文本标记语言（HTML）定义，可以包含文本、图形、声音、视频以及小程序，小程序是从服务器自动下载并在桌面上运行的软件程序。Web页面中最重要的元素是与同一服务器或不同服务器中其他页面的超文本链接。这些链接显示为加亮文本，可用鼠标单击，图形中也可以包含超文本链接。只要单击链接，就可以方便地从一个页面移到另一页面，不需要考虑信息的地址或通信的细节。

每个超文本链接包含可见部分（称为控制点），是用户在屏幕上看到的部分。控制点通常描述链接或提供引用页面的标题。超链接还可以用图形表示，因此可以生成用图标表示链接的Web页面。链接的目标用统一资源定位器（URL）描述，例如：

```
http://servername.domain/path/name/of/object.html
```

可以引用同一服务器或不同服务器中的页面。

万维网是比较纯粹的客户 /服务器系统，内容放在Web服务器中，由客户请求。除了少数例外，服务器不启动活动，客户只是显示从服务器中取得的内容。例外包括服务器推与小程序，前者客户保持打开网络连接，服务器连续更新客户，后者客户自动下载代码并执行，通常提供更复杂的交互行为。

8.5.2 统一资源定位器

统一资源定位器的结构与灵活性是用 Web 进行电子商务的中心。

如图 8.4 所示，http://www.w3.org/example/path/index.html 之类的统一资源定位器（URL）是由几个部分组成的。

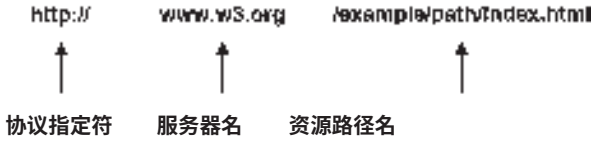


图 8.4 URL 的组成

- 协议指定符（http:）
  告诉浏览器用什么协议连接服务器，这里是HTTP。大多数Web浏览器还可以用其他协议，如 FTP(ftp:)与 SMTP(mailto:)，分别用于文件传输和电子邮件。
- 服务器名(servername.domain)

这是域名系统（DNS）名称，浏览器用DNS将这个名称转换成IP网址。

- 路径名(/path/name/of/object.html)
  通常是Web服务器上的文件全名，但也可以在服务器中解释为程序或数据库查询，用于对客户产生结果。习惯上，扩展名（这里是.html）表示这是个HTML文档，但这个规则不是必需的。

这个特定URL指服务器文件系统中的信息静态HTML页面。Web上的主要功能来自另外两个功能：应用程序软件动态构造页面和双向信息流动动态构造页面时，Web服务器将URL的路径部分传递给应用程序软件，应用程序软件可以返回动态构造的HTML页面或其他内容。此外，HTML页面中可以包含要用户填入的窗体，窗体中输入的数据发送回服务器。

8.5.3 Web协议

Web实际采用几个网络协议，其中有些是其他地方产生的，但也在Web中采用，如文件传输协议（FTP），有些则是Web中生成的，如下列协议。

超文本传输协议

超文本传输协议（HTTP）是最初的Web通信协议。利用HTTP，客户打开与Web服务器的TCP连接，发送一个HTTP头。头中包含GET、PUT或POST之类的HTTP命令和URL路径部分。HTTP头中还可能包含验证用户的信息，以及可接受文档格式的信息。这个信息可以让客户和服务器协商服务器返回什么格式，使（例如）客户只能够处理GIF格式图形时不会收到JPEG格式图形。

客户用HTTP中的GET命令取得文档，用PUT命令将文件上装到服务器中。POST命令让客户发送窗体填充结果给服务器。利用PUT与POST命令时，客户只要在HTTP头后面立即传递信息。

服务器处理请求之后，将答复头返回客户，然后发送要显示的页面。服务器发送的头字段之一指定返回的数据格式，使客户可以找到正确的模块或应用程序。这种功能使Web浏览器可以显示许多不同的数据（如文本、HTML、图形，等等）。此外，浏览器是可扩展的，可以调用其他应用程序，处理自己不支持的数据格式。

安全套接层

安全套接层（SSL）是Netscape通信公司开发的，是Internet中最广泛使用的安全协议。在简化协议层模型中，SSL介于TCP与应用程序之间，可以对任何数据流提供安全服务。除了加密通信之外，SSL还可以用数字证书向客户验证服务器。在SSL 3中，证书也可以向服务器验证客户。Internet工程任务组（IETF）中的传输层安全（TLS）工作组正在开发TLS，TLS是基于SSL的标准化协议。SSL与TLS将在第13章详细介绍。

安全HTTP（S-HTTP）

S-HTTP是Web安全协议，最初是由企业集成技术（EIT）公司开发的（注：EIT建立了Terisa系统公司，专门从事S-HTTP工作。此后Terisa系统公司又被Spyrics公司并购）。S-HTTP没有广泛使用，但非常有趣，因为它在应用层而不是在传输层提供各种安全服务。S-HTTP使Web客户与服务器可以指定相互独立的验证与隐私功能，可以协商使用的加密算法。此外，S-HTTP建立在Web协议之上，因为超文本文档中的每个链接可以带有目标文档的安全属性信息。这个功能增加了授权安全内容的灵活性，但使安全管理更加自动化。

随着时间的推移，Web不断壮大，包括越来越多协议，使Web浏览器可以成为许多用户的 Internet 主界面。

8.5.4 其他Web工具

Web的基础（HTTP，HTML，URL，等等）已经成为许多应用的基础。例如，搜索引擎是最著名的应用之一。搜索引擎是Web的寻找信息的工具，包括万维网和公司或其他组织使用的内部Web。搜索引擎可以用不同方式生成索引。有些是人工生成与维护的，向搜索引擎提供库的组织形式；有些用自动Web处理器从所有Web下载信息，以某种方式检查。自动Web机器通常保存要索引的Web页面清单，一个一个下载，每个都从文本进行检索，页面上的任何超链接加进要索引的Web页面清单中（如果还没有检索）。在一个连接良好的Web中，Web机器可以检索能读取的几乎所有静态页面。如果不让Web机器检索你的站点，则可以用某种方法加以阻止（见本章末尾的参考资料）。

有些Web工具可以让你在不连接Web时使用Web。例如，移动计算机（如便携电脑与笔记本电脑）通常只在部分时间连接网络。对许多用户而言，脱机浏览器可以事先批量下载Web内容，而不是单击一页下载一页。后面在切断系统时，用户可以像联网时一样浏览页面（当然，这不适用于交互式应用和内容不断改变的动态页面）。

Web已经如此强大和无处不在，许多应用程序都与Web有这样那样的联系。例如，有些程序提供帮助时将用户链接回厂家的Web站点，而不是将帮助内容放在程序中，或者用Web站点中的更新与常见问题补充帮助文件。字处理器、电子报表和其他应用程序都可以让用户通过URL在自己的文档中嵌入其他文档，使数据可以在必要时从Web上读取。

从 Internet 商务的角度看，这些都是设计系统时需要考虑的组件。例如，商务系统是否需要处理脱机浏览器？其他应用中嵌入Web时怎么办？商务Web站点是否欢迎检索站点的自动搜索引擎？这类相关问题的答案，应当在商务服务要求中定义。

8.6 代理

“代理”这个词有许多不同含义，可以指拼写检查程序，也可以指不经请求自动寻找所需

信息的人工智能程序。在今天的实践中，代理的功能通常受到很多限制，但许多研究项目还在探索代理的功能。

在 Internet 商务中，最常见的思想是把代理看成引导购物的人，寻找你可能需要的各种货物并提供可比信息。进一步说，这种代理还可以授权在一定条件下进行购买。

导购者对买方有利，但卖方则可能有所忧虑。例如，倾向于价格的代理可能将市场推向低价卖方。由于代理是自动化的，很难建立与实际客户的关系。事实上，网络上已经有卖方对这类原始型代理作出反应。大多数情况下，卖方会开发出对策，防止代理使用其系统。代理在 Internet 中还是新生事物，特别是对于 Internet 商务，还无法预测其最终在商务应用中的命运。也许代理能找到用武之地，任何演变性商务系统的开发人员都要密切关注这个技术的发展。

8.7 Intranet

Intranet 一词表示在公司或其他组织的内部网络中使用 Internet 技术。Intranet 通常用某种形式包括 Web 技术。对于 Internet 商务，Intranet 有两个有趣的属性。第一，Intranet 可以建立统一的客户经验，利用公司不同部分的资源，集成产品信息、技术细节、客户服务、产品与服务订购以及公司中任何其他专门组织的功能。第二，Internet 商务应用可以部署到内部使用，用相同应用程序处理内部订单、事务处理和内部“客户”服务。

8.8 Extranet

Extranet 与 Intranet 相似，表示将组织与业务伙伴、供应商和密切客户相连接。有时 Extranet 也指用 Internet 相互通信，但通常用比典型 Internet 连接更密切的方式相连接。网络可能使用 Internet，也可能在专用物理网络上使用 Internet 技术。典型应用包括共享合作项目信息、直接连接供应商订单系统或直接访问客户服务与支持系统。

这类活动包括许多已经介绍的商家对商家（B2B）Internet 商务。事实上，Internet 商务系统可能是 Extranet 的基础，拉近卖方与买方的关系。从某种意义上说，Extranet 提供了外延安全边界，防止开放网络访问公司，同时又提供业务伙伴之间共享信息的较低安全边界。

8.9 家用电器与网络计算机

随着 Web 的增长，可以连接的设备也花样渐多。许多设备没有桌面计算机的所有功能，可能只有有限的计算功能、存储功能、网络带宽和显示功能，等等。例如 WebTV 之类的设备是针对广大的家用电器市场的，有些（如各种网络计算机）则是为了充分利用 Web 和相关技术。人们承诺对用户有用的资源都能联网，桌面设备的主要目标是将用户与这些资源相连接。这种

所谓的稀少客户就是以 Web 为计算的基本界面。

各种稀少客户对商务应用有一些重要意义。特别是，应用程序设计人员必须了解应用中可能使用的设备范围。例如，在浏览器中执行 Java 的应用程序就排除了任何无法运行 Java 的浏览器。这种限制在一些应用中是可以接受的代价，但有些则需要获取尽可能多的客户群。随着各种设备不断出现，在市场中广泛应用，应用程序设计人员必须考虑如何使应用程序满足客户使用的各种设备。

8.10 Internet 的未来：协议演变

和其他技术一样，Internet 也是迅速演变的，这种改变是不可避免的。尽管许多核心原则依然相同，但细节则不断变化。本章介绍的所有技术都在一定程度上有所改变。

TCP/IP 将随 IPv6（下一代 Internet 协议）而改变。IPv6 利用 IP4 的长期经验，改进其可伸缩性、安全性和实时媒介支持。由于它改变了 Internet 的基础性协议，因此整个 Internet 运行 IPv6 还需要一段较长的时间，但市面上已经有许多 IPv6 产品。事实上，有些针对 IPv6 开发的安全技术也开发了针对 IP4 的版本。

好在 IPv6 对 Internet 商务没有太多直接影响。由于 Internet 的分层体系结构，商务应用不太受低层改变的影响。因此，部署 IPv6 时，商务应用照样工作，只是总体网络性能更好。随着时间的推移和 IPv6 安全体系结构广泛使用，商务应用也可以用 IPv6 安全特性加强安全性。

Web 也是不断改变的，HTTP 与 HTML 都是非常活跃的。HTTP 新版本提供更好的性能和客户与服务器之间更灵活的交互。HTTP 的改变比 IPv6 的改变对应用的影响更大，因为它提供与应用程序逻辑密切相关的功能。由于改变与旧版兼容，因此应用程序不需要立即改变，而可以在适当时候通过修改利用新协议的优势。

对 HTML 而言，一个迅速普及的新标准是扩展标记语言（XML）。效果上，XML 可以让应用程序定义自己的标志扩展，可以在文档中定义包括数据项目的应用程序特定标志和屏幕上显示的规则。例如，商务应用程序可以用 XML 定义订单窗体，对价格、说明、数量等相应定义标志。这样就可以使浏览器之类的显示应用程序的屏幕上显示精彩格式的窗体，而应用程序可以分析订单窗体，取得处理订单所需的信息。

尽管 Internet 技术的改变是不可抗拒的，但不一定要立即采用。每个变革性步骤（和某些革命性步骤）都要评估如何影响商务应用对客户提供的价值，以及实施改变的成本。这些改变也可能无法在市场上普及，从而使应用最终销声匿迹。对于 Internet 商务应用，建议格外慎重，小心变革。

第 9 章 Internet 商务系统建筑块

给我一个砖砌的罗马，我将报以玉石之城。
——奥古斯特·凯撒[1]

9.1 Internet 商务系统组件

Internet 商务系统的建筑块就是万维网的技术，即它的协议、浏览器、服务器以及 Java、ActiveX 与 CGI 等应用程序开发结构。本章首先介绍 Web 的基本内容机制，然后概述让用户取得内容的协议和机制，然后我们介绍服务器中建立内容页面的当前技术，和在浏览器中增加编程功能的新技术。最后介绍对 Web 上增加商务功能很重要的基本 Web 技术变化。

9.2 内容传输

Internet 服务器上的内容可以用两种方法传输到最终用户屏幕：或者用户的客户端程序（浏览器）以服务器中读取内容，或者服务器启动连接并将内容发送到桌面。这两种机制分别称为拉和推内容发送。此外，推内容的另一种变形是广播，向许多客户同时发送同一内容。

9.2.1 拉内容

拉内容是万维网上的传统方法：客户机在用户单击超文本链接时打开与服务器的连接。大多数 Web 浏览器可以用各种网络协议取得内容，但最常用的是超文本传输协议（HTTP）。第 8 章介绍了 HTTP 基础，下面再介绍一些细节。

协议变形

在最初的 Web 设计中，浏览器对页面上的每个组件使用一个独立的 HTTP 连接。例如，所包括的每个图形（除 Web 页面之外最常见的组件）都要用一个独立连接，[2]每个连接的建立都需要一定的开销和时间。当然，如果页面组件来自不同服务器系统，则必须使用不同连接，但如果页面组件来自相同服务器系统，则只需使用一个连接。有些客户与服务器实现方法支持 HTTP Keepalive 协议选项，允许多个请求使用同一连接。推荐的 HTTP 1.1 协议也允许多个请

①摘自修通钮斯《奥古斯特》。
②因此有些站点用一个图形，用一个图形映射表示工具栏，这比用各个小图表示不同按钮有效得多。

求使用同一连接，并以多种其他方式减少协议开销。

缓存

从远程服务器读取文档（特别是大文档）需要一定的时间，特别是在 Internet 连接缓慢时更是如此。为了提高用户看到的性能，许多浏览器保存 Web 页面及其组件的临时拷贝。临时拷贝放在缓存中。缓存在下列情形中非常有效：

- 同一站点的多个页面中使用的图形，如标记和工具栏
- 用户单击浏览器 Back 按钮，返回最近显示的页面
- 站点重复访问

除了浏览器缓存之外，Web内容还经常缓存在代理服务器中。代理服务器通常介入公司网的用户组和整个 Internet 之间，有时也在 Internet 服务提供者的网络中使用。代理服务器在防火墙中使用，提供一些安全优势。通过提供缓存，代理服务器还可以减少内部用户与 Internet 之间的网络通信流，以及为用户提供更好的性能。

缓存有两个严重问题：

- 缓存会缺少一些需要的东西
  浏览器作出请求时，如果请求的页面或图形在缓存中（称为缓存命中），则用户能取得更快的可预测性能。如果请求的页面或图形不在缓存中（称为缓存失误），则用户要等待主内容服务器响应，结果无法预测性能。统计上，缓存能改进 Web 的平均性能，但会增加变数。这个效果是很恼人的。
- 缓存有一些不要的东西
  浏览器作出请求时，如果项目在缓存中，则用户会立即得到响应，但实际内容服务器中的页面可能已经改变。HTTP 协议有办法处理这个问题，但不一定总是成功[③]。随着网络的增长，缓存会越来越多地用于达到良好性能。另一方面，软件也要改进，更好地进行正确缓存。Web 浏览器通常有个刷新按钮，强制从主服务器取页面，但用户要猜测何时需要选择这个按钮。

缓存对商务应用的影响

缓存对商务应用的影响可能很不好。过时页面会让用户困惑，影响其使用商务应用程序。下面试举几个例子：

- 缓存产品目录页，不显示当前价格

---

③ HTTP 中的 HEAD 命令可以询问服务器页面是否自特定时间以来发生了改变，PRAGMA NOCACHE 之类的头字段可以告诉代理服务器和其他缓存可以安全缓存的时间长度。

- 产品目录应用程序对不同公司客户显示不同价格，但由于代理缓存，一个公司的用户看到与另一公司相关的价格。
- 订单窗体页不显示正确汇总，因为用户收到缓存拷贝，反映订单前一阶段的内容。
- 应用程序用隐藏字段④存储部分应用程序状态。用户重新提交窗体的缓存拷贝，包含与应用程序其余部分，不一致的信息。

这些问题的解决方案各不相同。例如，要解决最后一个问题，一种方法是避免用隐藏字段存储部分（而不是全部）应用程序状态。其他情况下，一定要保证Web服务器发送相应HTTP缓存指令，使Web页面正确缓存。

脱机浏览器

和许多Web用户一样，我们也深为低速或不可预测的Web性能而失望。我们通常事先知道要什么，不如让计算机把Web站点按指定方式复制到本地硬盘上，然后快速浏览，甚至可以在不联网的情况下阅读Web页面，这就是脱机浏览器的妙用。脱机浏览器是个桌面应用程序，可以在正常Web操作不知不觉的情况下预先将内容装到本地硬盘上。这对便携电脑用户和多次重访同一站点的用户特别有用。但是，脱机浏览器不适用于动态和交互站点。脱机功能已逐渐集成到浏览器的基本功能中。

有些脱机浏览器要求最终用户指定要自动取得的内容，而有些则允许内容创建者创建用户可以预订的包。包将拉模型脱机浏览器变得好像推模型，因为内容生成者定义发什么给用户，用户只是确定何时下载这个包。

类似的工具还可以用于另一场合：复制Web站点。为了提供高效的性能或提高可靠性，Web站点可以包括多个具有相同内容的服务器。复制对动态站点较困难，因为不仅要复制一组HTTP Web页面，还要复制基础应用程序和数据库。用户也很难寻找“最佳”复制，因为没法找到负荷最轻的服务器或最接近网络的服务器。但是，即使简单复制机制也会给用户带来好处，因为用户能感觉到性能与可靠性的提高。

9.2.2 推内容

Web工作是从用户向服务器请求内容开始的，但服务器也可以主动向末端用户发送内容，不需要用户直接请求。从技术角度看，用户要注册内容信道，然后相关信息就自动发送到桌面。与电视和收音机频道一样，推内容信道可以包含实时浏览材料，但和电视与收音机频道不同的是，信道可以包含任意信息捆绑体。举个例子，电视台的图像可以控制你的VCR，自动录制你注册要看的节目。更奇妙的是，如果对物理世界实现推系统，则可以自动更新你家里的

④ HTML 窗体用隐藏字段在窗体中保存要返回服务器的信息，但不向用户显示这个信息。例如，窗体可能向客户询问支付信息，隐藏字段中包含订单号，使应用程序可以在用户提交窗体时将支付数据与正确订单相匹配。

所有图书、杂志、录像带和录音带。推技术适用于任何内容，包括发给最终用户的多媒体和发给计算机的软件。

如果用推系统将应用程序和数据发送到桌面，或加上实时服务器连接，则可以适用于静态信息和动态交互内容。

9.2.3 扩展机制

Web浏览器通常包含对HTML和许多其他数据类型如图形、文本与声音的内置支持。大多数浏览器还包括各种扩展机制，可以通过用户交互或自动方式增加其他功能。这些机制包括下面介绍的几种。

MIME类型

MIME即多媒体 Internet 邮件扩展，是多媒体电子邮件的 Internet 标准。使用MIME类型时，每个文档标上类型，表示属于哪种数据，如HTML、图形、文本，等等。表 9.1 列出了Web上常见的MIME类型。HTTP 从原先的应用中借用了大部分 MIME 类型机制，但细节有些不同。浏览器通过解释MIME类型确定如何显示下载的数据。如果浏览器无法直接处理某种MIME类型，则可以将浏览器配置成启动独立浏览程序。例如，用户可以安装视频应用程序，浏览从Web上下载的录像片断。安装过程将浏览器配置成下载录像片断时启动初步应用程序。启动帮助程序时，其独立于浏览器而操作。

表 9.1 MIME 类型举例

MIME类型	说明
text/html	HTML文档
image/gif	GIF图形
image/jpeg	JPEG图形
text/plain	普通文本
application/pdf	Adobe 公文文档格式（PDF）
audio/x-pn-realaudio	Real 音频
video/mpeg	MPEG视频
video/quicktime	Apple QuickTime 视频

HTTP还可以让浏览器列出能处理的MIME类型，让服务器知道其功能。这样，服务器就可以根据浏览器的功能发送不同格式的数据。

但是，增加安装与配置和分开操作都是很麻烦的事。对许多应用程序而言，最好使用其他扩展机制。但是，MIME类型机制可以独立于基础浏览器而扩展应用程序，这是它的优势所在。

插入件

有些浏览器（如Netscape通信公司生产的浏览器）具有插入件机制，软件开发人员可以用

定义的编程接口在浏览器中增加新功能。其中一个功能是用浏览器本身显示新数据类型，而不是启动另一应用程序。包含这种加入功能的软件称为插入件，要手工安装之后才能显示新数据类型。另一种方法是 Microsoft 公司的对象链接与嵌入（OLE）技术，在 Microsoft 公司的浏览器中使用。

浏览器插入件可以按复杂的方式修改浏览器行为，如增加新工具栏命令和菜单项目。它们要对不同浏览器的不同版本采用不同实现方法（但浏览器厂家可能提供很好的向上兼容性）。因此，插入件机制虽然强大，但在许多商务应用中并不方便，除非已在买方广泛使用，可以用于许多不同卖家。

脚本

Navigator, Internet Explorer 之类的浏览器可以执行在 Web 页面中嵌入的脚本。脚本用 JavaScript 或 VBScript 之类的语言编写，在显示界面时由浏览器中的解释器执行。出于安全原因，这些脚本的功能有限，但可以修改 Web 显示和增加交互性。例如，常用应用程序用脚本检查用户在窗体中所输入内容的有效性，以便更快纠正错误，而不必到服务器中验证输入。

小程序

Navigator, Internet Explorer 和其他浏览器都可以执行用 Java 编写的小程序。Java 小程序在 Web 页面需要时从服务器中下载。然后小程序在浏览器提供的 Java 虚拟机中执行，限制了小程序对系统的影响。稍后将详细介绍 Java 和 Java 小程序。

控件

Microsoft 公司的 Internet Explorer 引入了 ActiveX 控件。ActiveX 控件是遇到包含 ActiveX 控件的 Web 页面时自动下载和安装的软件模块。但是，与 Java 小程序不同的是，ActiveX 控件可以在用户计算机上自由运行。ActiveX 控件将在稍后详细介绍。

这些扩展机制使 Web 成为更动态和更具交互性的环境。但是，使用这些扩展机制要求在浏览器发生演变时进行更多开发与维护工作。此外，很难编写既容易取得与安装又能够在不同浏览器之间移植的扩展。应了解客户、他们的软件和他们对灵活性的要求，更好地决定如何利用浏览器扩展。

9.2.4 客户软件要求

读到浏览器软件，我们自然想到 Internet 商务中最复杂的一个问题：商务系统要设计成只使用几乎所有浏览器都共有的功能，还是充分利用更先进的特性？如果需要高级特性，但会限制具有相应软件的用户数，或者要让用户方便地取得所需软件。随着用户分布到不同平台（如 Windows, Macintosh 和 Unix），问题会更多。有几种可行的方法。

- 商务站点适应特定用户的功能。例如，它可以动态选择大量使用图形的表示和只用文

本的表示。这个选择可以自动化（如果站点能标识浏览器功能），也可以让用户单击相应链接选择交互形式。

- 商务站点要求用户安装特定软件，如动画插入件、商务模块或特定版本的浏览器。这个方法适合接近的用户社区，一个组织对用户有巨大影响。
- 商务站点在特定软件浏览时效果最好（如特定浏览器版本），而用其他软件时则不那么好，甚至根本行不通。如果一、两种客户软件在目标用户群中占主导地位，则可以用这种系统。

注意，随着对客户的更加了解和软件的不断演变，这些方法也是可以改变的。例如，曾几何时，只有少数用户的浏览器能够用HTML绘制表格，而如今大多数用户的浏览器都能够用HTML绘制表格。因此，随着软件的改变，此时适合的选择，彼时不一定适合。

9.3 服务器组件

万维网最初的概念很简单，Web服务器在文件系统中存储HTML编码页面，这些页面可以由浏览器用HTTP读取，页面的URL就是服务器主机名加上文档的文件名⑤。后来，人们发现HTML Web页面可以由程序生成和存放成文件。在这种方式中，URL指定服务器主机名，要运行的程序名和程序变元。最一般的情况下，Web服务器可以将任何解释与URL相联系，用任何机制生成和向浏览器返回页面内容。

9.3.1 通用网关接口

通用网关接口（CGI）定义Web服务器与负责URL名字空间某个部分的独立应用程序之间的标准接口。这些应用程序也称为网关，因为CGI最初的用途是生成Web与各种现有应用程序之间的网关。CGI还是对Web设计但不与Web服务器直接集成的全新应用程序的接口。

CGI最初是对Unix平台设计和实现的，但现已推广到大多数其他Web服务器。在CGI中，URL的路径部分表示应用程序，Web服务器将其作为单独程序而启动。应用程序的标准输入与输出流与浏览器通过网络连接联系起来。浏览器的输入（如发表的窗体）进入应用程序，应用程序的输出发给浏览器。服务器调节这种连接，保证符合HTTP协议。此外，服务器用环境变量向应用程序提供请求的一些细节。表9.2列出了常用的CGI环境变量。

表9.2 常用的CGI环境变量

CGI环境变量	含义	样本值
GATEWAY_INTERFACE	使用的CGI版本	CGI/1.1
SCRIPT_NAME	执行的CGI程序名	/payment.cgi
PATH	寻找其他程序的搜索路径	/sbin:/bin:/usr/sbin:/usr/bin

⑤实际上，Tim Berners-Lee最初的Web概念包括从桌面生成、更新与标注内容，这些功能是最近在普及的。

（续表）

CGI 环境变量	含义	样本值
HTTP_USER_AGENT	浏览器版本标识符	Mozilla/4.0
REMOTE_HOST	客户名	mypc.somewhere.org
REQUEST_METHOD	HTTP 命令	GET
REMOTE_ADDR	客户 IP 地址	10.0.25.10
HTTPS	表示是否使用 SSL	OFF

9.3.2 超越 CGI

CGI 是一般性的，因为应用程序与 Web 服务器完全分开。但是，这种一般性是要付出性能代价的，因为应用程序要对每个请求分别启动。此外，由于应用程序在请求后面退出，因此没有一个 Web 请求之间方便地存储状态信息的地方。这种对 CGI 的限制导致了 Web 服务器与应用程序之间开发出另外几种接口。

所有服务器应用程序接口（包括 CGI）都要解决几个问题：

- 启动与停止应用程序
- 从客户向应用程序传递数据
- 从应用程序向客户传递数据
- 状态与错误报告
- 向应用程序传递配置信息
- 向应用程序传递客户与环境信息

服务器 API

Netscape（NSAPI）和 Microsoft（ISAPI）都定义了应用程序接口，允许应用程序软件直接集成到 Web 服务器。尽管两者细节不同，但都允许在服务器同一进程环境中装入和执行应用程序代码。这个结构能得到高性能，但失去了将应用程序进程与服务器隔离和将多个应用程序相互隔离的安全性。服务器 API 通常还会限制编程人员对编程语言的选择，可能限制应用程序设计的其他方面。

FastCGI

FastCGI 最初是开放市场公司开发的，现已在许多服务器中得到支持（包括著名的 Apache 服务器），目的是既取得集成服务器 API 的性能又能保留 CGI 的隔离和安全属性。此外，FastCGI 允许应用程序在离 Web 服务器很远的另一系统中运行。FastCGI 用 TCP 之上的轻量级协议或本地进程间通信之类的其他流协议在应用程序间相互通信。FastCGI 应用程序与 Web 服务器之间使用通信链使应用程序进程可以拷贝，同时又提供相当高的隔离性，从而保证可靠性和安全性。持久应用程序提供了跟踪多请求进程状态的便利方法，同时又有只一次启动应用程序进程的性能优势。

9.3.3 服务器方脚本

文件系统中保存的静态内容页面与完整应用程序生成的动态内容页面之间还有一个中间地带：服务器方脚本。使用服务器方脚本时，基础页面（称为模板）放在文件系统中，这些页面混合HTML与脚本语言指令，Web服务器所嵌入的解释器执行这些脚本语言指令。

- 服务器方包含
  服务器方包含是非常简单的脚本，页面中的某些标志换成运行程序的结果或换成服务器已经知道的某些信息(如时间标志)。这种脚本语言只限于指定这些程序名及其变元。
- 服务器方脚本
  可以在Web服务器中嵌入语言解释器。文件系统中存放的Web页面可以包含动态解释的脚本或程序。Web页面的非脚本部分与脚本输出结合起来，得到发给浏览器的最终页面。最常用的嵌入语言有 Java、JavaScript 和 VBScript。
  嵌入语言只能在一些环境中使用。Microsoft 的ASP（活动服务器页面）是服务器脚本与控件的执行环境，ASP使页面设计人员可以将 JavaScript 和 VBScript 脚本和任何编程语言写成的 ActiveX 控件结合起来。Netscape 公司的 LiveWire 可以使用服务器方 JavaScript。

9.3.4 数据库驱动模板

将Web与数据库系统连接的机制在结构上与服务器脚本相似。通常的方法是定义Web服务器文件系统中所存储页面的模板语言，模板中的特殊标志使嵌入 SQL 语句可以生成数据库查询，查询结果替换发送到浏览器的页面。市场上有许多将Web与数据库系统连接的机制，是 Internet 商务系统的有效部分。

9.4 客户端编程

Web出现之前，针对地理分布用户的系统可以使用大型机和终端网络，或客户 /服务器系统。在终端网络应用程序中，应用程序逻辑存放在主机中，终端只能进行本地编辑与打印。相反，客户 /服务器系统则利用客户计算机（通常是 PC 机）的处理功能，应用程序数据保留在主机中，而大部分应用程序逻辑则移到客户端。

早期的Web浏览器就像是漂亮的终端加上一些多媒体功能，具有优秀的显示、本地编辑和复杂的窗体，但没有编程功能。Web浏览器又名通用客户，但应用程序逻辑要移回服务器中。Web应用程序通常是三层的，Web浏览器客户与应用程序服务器接口，应用程序服务器又与数据库服务器接口。

新一代的 Web 浏览器进步较大，向应用程序设计人员提供了完全编程功能。前面曾介绍过，客户可以用不同方法编程，包括脚本、Java 小程序和 ActiveX 控件⑥。

9.4.1 脚本

脚本是在 Web 页面中直接嵌入解释语言的源代码程序。脚本在页面上遇到时或发生指定事件时运行，如用户单击按钮或编辑窗体字段时。它们在进行交互功能时相当有用，如检查窗体内容的有效性与一致性。

Netscape 与 Microsoft 浏览器支持 JavaScript 语言脚本，这是 Netscape 公司开发的面向对象脚本语言，对 Java 有一定相似之处，但没有 Java 的端类型体系。

脚本语言对迅速开发简单应用程序非常有用，但缺乏编译检查，使其很难测试中等长度以上的脚本。除了比较简单的情形外，最好用 Java 小程序和 ActiveX 控件。

9.4.2 Java

Java 是 Sun 系统公司开发的面向对象编程语言，广泛用于一般编程任务和生成 Web 上的浏览器小程序。Java 不仅包括语言规范，还包括一个虚拟机规范，形成 Java 程序的执行环境。Java 不是编译成特定处理器（如 Pentium 或 SPARC）的自然指令集，而是编译成可以在定义好的抽象机器上执行的指令集。Java 语言和虚拟机一起使 Java 小程序完全可移植，编译成 Java 字节码的 Java 程序可以在实现标准 Java 虚拟机的任何平台上以相同方式运行。

Netscape、Microsoft 等的浏览器包括 Java 虚拟机和 HTML 扩展，使 Web 页面可以包含 Java 小程序及其参数的引用。遇到小程序时，它自动下载到浏览器的 Java 虚拟机中执行。Java 虚拟机包括 Java 类库，使 Java 小程序可以在屏幕上绘制、与用户交互和与源服务器通信。Java 虚拟机实现沙袋，防止小程序读取用户硬盘或控制用户的计算机。

Java 小程序的可移植性和 Java 虚拟机的标准化使小程序生成者不必考虑对用户使用的不同客户计算机支持不同的 Java 小程序版本。一个 Java 小程序可以在所有平台上完全相同地运行。Java 与 Java 虚拟机仍在迅速演变，因此 Java 小程序作者不必考虑 Java 环境的不同版本。

Java 小程序的安全性基于沙袋模型，小程序无法进行任何危险操作。但是，这也使 Java 小程序无法进行太多有用的操作，Java 的扩展（如 Java1.1 的签名小程序和 Java 电子商务框架中的新机制）使 Java 小程序对许多商务应用更有用。

9.4.3 ActiveX

1996 年，Microsoft 公司引入 ActiveX。ActiveX 是从对象链接与嵌入（OLE）演变而来的，是 Microsoft 早期开发的，用于让不同应用程序密切配合工作。ActiveX 控件是 Web 页面引用的

⑥这里只限于介绍自动发送和在浏览器中集成新功能的编程机制。浏览器插入件自然会增加一些功能，但用户要显式安装这些功能。

软件对象，可以在首次引用时自动下载和安装到用户PC机上。后面再引用时，控件自动激活，而不必再次下载。与Java小程序不同的是，ActiveX控件可以完全访问客户系统的资源。

ActiveX安全模型基于代码签名，而不是靠沙袋，ActiveX控件可以完全访问客户系统的资源。要让用户愿意安装这种可能有危险的软件，要由授权组织为每个控件数字签名（数字签名见第12章介绍）。然后用户决定信任生成该控件的组织时再运行这个控件。

ActiveX控件非常强大，但其包含二进制计算机代码，因此依赖于特定平台，目前，ActiveX只限于各种版本的Microsoft Windows。此外，用户在Web站点的访问流程也可能在安装ActiveX控件时受到影响，用户可能要中断过程，回答信任ActiveX控件生成者的问题。ActiveX目前无法删除已安装的控件，因此古怪或少用的控件可能会累积起来，占用用户的系统资源。

9.5 会话与Cookie

HTTP协议是无状态的，每个请求与其他请求是相互独立的。随着Web成为复杂应用的基础（商务和其他领域），出现了Cookie和其他在无状态协议上维护持久应用程序状态的技术。

9.5.1 会话的重要性

人们最初以为，Web是大量文档的集合。浏览器请求文档，用户看一会儿，然后请求另一个文档。在这种环境中，无状态协议是合理的。由于服务器很少而浏览器很多，服务器无状态可以使每个请求使用更少资源。

随着Web的增长，这种设计思想被破坏了。

复杂页面需要许多连接

在HTTP中，页面上的每个图形元素需要一个网络连接，这就造成性能很差，因为很小的页面元素也需要网络上的几次分组往返。

高开销

在intranet静态页面环境中，服务器返回特定页面时不需要太多工作。但是，在开放Internet中，隐私和验证的要求使每个连接需要大量工作。因此，无连接协议效率很低。

Web应用

几乎任何有趣的Web应用（特别是Internet商务应用）都要求用户与服务器的一系列操作，处理多个不同Web页面。

9.5.2 状态与会话

应用程序与用户进行一系列交互时，实际发生什么情况呢？最基本地说，应用程序要记住

状态，并在与用户交互之后改变存储的状态。更加复杂的是，有许多用户，各自与 Web 应用程序的交互相互交织。会话是记住哪个状态信息与哪个用户相关联的方法。

要解决这个问题，就要考虑在什么地方保持应用程序状态。图 9.1 显示了一般情境。Web 浏览器与运行 Web 服务器的应用程序通信，应用程序能够访问数据库。状态可以保存在数据库中、应用程序中或客户中。

状态保存在数据库中

在这个模型中，应用程序本身是无状态的，可能是某个 CGI 应用程序，在每次客户请求时重新启动。如果应用程序要求与用户进行一系列交互，则中间应用程序状态存储在数据库中。每次客户请求时，需要从数据库中找到和读取状态。为此可以用 Web 基本验证，在每次请求时提供用户名和口令，或者通过 cookie 或其他会话机制完成（见稍后介绍）。

状态保存在应用程序中

如果中间应用程序状态很重要，而中间状态不需要事务安全性，则可以将状态保存在应用程序中。这时，应用程序是持久的（不需要在每次客户请求时重新启动），可以用 FastCGI，ISAPI 和 NSAPI 实现。需要用会话机制将特定用户与特定存储状态信息块相关联。

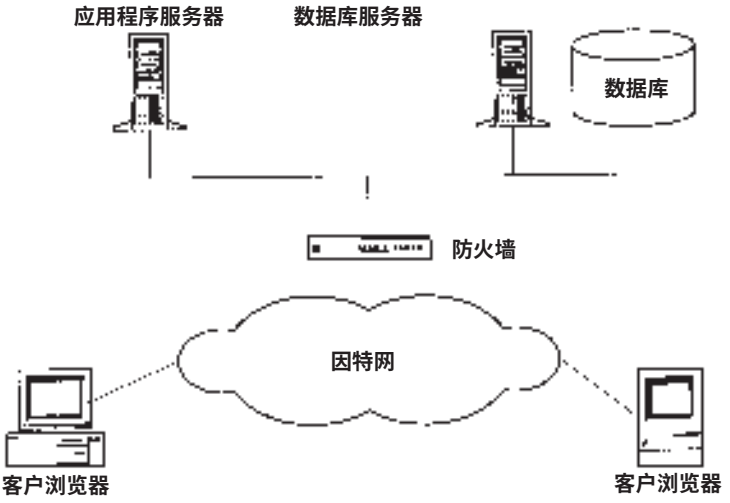


图 9.1 一般性 Web 应用程序

状态保存在客户中

对简单应用程序，可以将请求之间的状态保存在客户机中。在这个模型中，应用程序服务器用一些中间结果响应客户请求时，也向客户发送中间应用程序状态，以便在用户下次请求时恢复应用程序。这就要求客户与服务器之间有来回传递状态信息的机制。

9.5.3 会话与客户状态机制

可以用几种方法将一组用户请求标识为属于同一会话，在客户和服务器之间来回传递状态信息。此外，一定要注意会话机制和状态机制之间的差别是微妙的。状态本身是应用程序信息，而会话标识符引用某个地方存储的状态。

验证机制

任何验证机制都可以作为会话机制，如基本验证和客户证书。由于这些验证系统在每次请求时向服务器标识用户，因此可以在应用程序或应用程序数据库中存储状态信息，通过用户标识查阅每个请求。

动态URL

通过在一系列页面的每个URL中嵌入用户ID或其他信息，特定用户使用的URL可以不同于任何其他用户使用的URL。这就建立了会话机制。难点在于这些动态URL可能在用户单击其他Web站点，经过一段时间之后重新进入这个应用程序时丢失。此外，动态URL具有安全风险，除非通过加密阻止伪造和篡改。开放市场公司的DigitalTickets是一种生成保护性动态URL的方法。

Cookie

大多数现代浏览器都支持Cookie。Cookie最初由Netscape引入，指的是从服务器发给浏览器并存放在浏览器中的信息。在后续请求服务器时，浏览器将Cookie和Web请求一起发给服务器。Cookie可以存储会话标识符或存储应用程序状态，此外，Cookie可以设置成在浏览器会话之间持续。Cookie涉及的隐私问题已经在第一部分有所介绍，由于Cookie可以让高级浏览器用户访问，因此要防止篡改。

窗体

Web应用程序包括一系列HTML窗体时，应用程序状态与会话标识可以用窗体隐藏字段传递。隐藏字段是特殊的HTML窗体字段，不向用户显示，只是直接返回服务器。和动态URL与Cookie一样，隐藏字段也要保护，防止篡改。

小程序

随着Web应用程序从HTML与窗体转入客户/服务器方式，可以用小程序、控件和客户端脚本存储应用程序状态与会话标识。

9.6 对象技术

对象技术已经成为热门话题，许多竞争公司纷纷贴上对象技术的标签。因此，一定要明确

了解什么是对象技术。软件对象的实质就是包装一些数据和对数据进行操作的方法，这个包装有几个好处。

- 包装——对象隐藏实施细节
  对象超出子程序库和 API。编程人员用 API 开发软件时，需要了解数据如何表示与存储。利用对象技术，则对象会负责数据，编程人员只需用对象便可完成更高级的目标。包装不仅使编程人员不需要了解对象的内部细节，也使他们不可能了解对象的内部细节。这听起来好像太死板，但可以大大减少直接问题和潜在缺陷。
- 多态——对象可以有多种实现方法
  特定概念（如银行账号）表示成对象之后，这个概念的变形（如支票账号或存款账号）就可以表示为对象的不同实现方法，各有相同接口。完成之后，对账号进行操作的应用程序（如计算每月利息的应用程序）就不需要知道是哪种账号。
- 语言关联——对象可以用不同语言实现
  程序中一个部分与另一部分的内部通信通常是由语言及其编译器协调的。但是，由于对象技术认真定义了一个对象调用另一对象的方式，因此系统中的所有对象不一定要用相同语言编码。每种语言系统提供向对象系统所定义标准通信机制转换的方法。

在一定程度上，对象技术是更好更有效地构造大型软件应用程序的方法，严格使用抽象与包装能使软件更可靠，不管是不是用 C++ 或 Java 之类的面向对象编程语言（OOP）开发。另一方面，对象技术使复杂系统可以用不同组织或不同公司设计和实施的软件组件集成起来，这个思想称为组件软件。

对象模型不足以实现组件软件。对象模型提供了一组互操作性的基本假设与必要条件，就像铁轨的标准量具，要让火车在不同铁路上运行，轨道之间必须是等距离的，但仅仅这样还不够。组件软件系统还隐含其他标准接口，对象必须符合这些接口以保证互操作性。就像火车的例子，互操作性还要求合轨与分叉的标准接口。

除了组件之外，还有分布式对象计算，应用程序由网络上多台计算机中的软件对象组成。分布式对象计算不仅要求对象模型和语言关联，还要求线路协议、命名和安全模型。

- 线路协议
  对象在网络上通信时，必须协商信息传输的格式和顺序。网络通信与对象持久性问题有关，即对象可以在磁盘中记录数据。要达到对象持久性，对象将自己序列化到磁盘中，实际上就是以线性格式写出数据副本。在对象网络通信中，源对象以标准化格式生成序列化消息，使接收对象（可能在完全不同体系结构的计算机上运行）可以顺利接收和解释这个消息。
- 命名
  在任何分布式系统中，应用程序的软件组件应建立相互通信。由于网络上任何计算机

之间都可能相互通信，因此对象用命名和寻址系统寻找对方网址和建立适当的通信信道。这个问题在非分布式组件软件中也存在，但在传统应用程序中，编程环境在建立时将所有对象关联起来，而不是在运行时动态关联。

- 安全性
  在需要在 Internet 之类开放网络上操作的分布式系统中，安全性是个重要问题。软件组件要保证与正确对象通信（验证），通信是专用的（通过加密）和可信的（通过检查完整性）。在 Internet 商务中，安全的第三个方面（信任）至关重要。许多情况下，并不是构成应用程序的所有软件对象都在一个组织操作和控制的计算机上运行。系统设计人员要确定客户或不同组织运行的计算机上完成的计算有多大可信度。

9.6.1 CORBA

对象管理组织（OMG）的公用对象请求代理体系结构（CORBA），是公司联盟 15 年来定义对象模型的成果，使公司可以生产相互可操作的多语言、多平台实现方法。

CORBA基于对象请求代理（ORB）思想，对象用这个基本机制请求和接收其他对象的响应。ORB提供命名和通信服务。CORBA对象由原先定义接口的接口定义语言（IDL）描述。IDL是定义对象的语言，通过语言特定转换器解决语言关联问题，取对象的IDL描述并将其转换成特定语言关联设置。

CORBA还支持对象服务、常用功能和几个域接口，定义财经、保健等特定应用领域的公用对象。

CORBA通过 Internet ORB 间协议（IIOP）在 Internet 上工作，IIOP定义CORBA对象在TCP/IP 网络上通信的方法。

9.6.2 COM

Microsoft 公司的组件对象模型（COM）是最广泛使用的对象系统，是Microsoft 桌面操作系统和应用程序的重要部分。除了定义通信标准的基本对象模型外，Microsoft还定义了其他几个功能。

- OLE 自动化
  OLE 自动化定义一组标准接口，实现这组接口的 COM 是可编脚本的，可以在 Visual Basic之类的脚本语言中使用。能够用脚本连接复杂对象就可以实现快速应用程序开发。脚本语言的开销较高，但由于大量运行时间花在编译对象上，因此这样建立的应用程序不一定性能太差。
- ActiveX
  ActiveX 对象也称为 OLE 控件，是 COM 对象，实现其他标准接口，使其可以作为组件

软件。ActiveX 最有趣的一个方面是设计时和运行时行为的定义。ActiveX 控件可以通过 Visual C++ 等集成编程环境中的接口在设计时配置，然后通过另一组接口在运行时操作。这种设计时和运行时的分配能够帮助设计作为组件软件的 ActiveX 控件。

- 分布式 COM
  分布式 COM 或 DCOM 用分布式计算环境（DCE）远程过程调用（RPC）作为线路协议，允许不同计算机上的 COM 对象相互通信。

9.6.3 Java Beans/RMI

Java 是对象社区的最新成员。Java 是面向对象编程语言，而远程方法调用（RMI）是 Java 对象在网络上相互通信的标准方式。作为面向对象编程语言，Java 内置了对象模型。Java 的另一关键特性是一次编写，到处运行。Java 应用程序可以在 Java 虚拟机控制下运行，Java 虚拟机是一种抽象计算机。支持 Java 的平台（几乎所有平台）实现 Java 虚拟机，任何 Java 程序均可在 Java 虚拟机中运行。

Java Beans 是 Java 版的组件软件。Beans 实现一组标准接口和行为，类似于 ActiveX,可以在运行时定制。Java Beans 还使用一组桥，使 Beans 可以和基于 RMI 的对象、ActiveX 控件或 CORBA 对象相互操作。

9.6.4 对象技术对 Internet 商务的意义

对象技术对 Internet 商务系统的设计有几个意义。

- 快速应用程序开发
  对象技术通常比早期编程技术更适应快速应用程序开发。显然，这个好处不是 Internet 商务独有的。
- 分布式应用
  对象技术允许应用程序分布在多台计算机上，开发人员不必有网络通信与安全的各方面经验。
- 部署灵活性
  对象技术（特别是 Web 环境中提供的可下载小程序与控件）使 Internet 商务应用程序的设计人员有巨大的灵活性，可以设计多层应用程序，将功能放在服务器中或将功能全部移植到客户端桌面。自动将部分应用程序移植到客户端桌面对交互性和互操作性提供了巨大优势，但同时也会引入一些复杂的安全和信任问题，因为桌面计算机不一定是可信的计算平台。

实际中，对象技术通常在几乎所有 Internet 商务项目中都会用到。

9.7 商务客户端技术

浏览器编程机制已经以不同方式作用于 Internet 商务。上节介绍对象技术时曾介绍过，商务功能可以分配到桌面，得到隐私、方便和交互性，同时也会失去一些安全、通用性和可靠性。

9.7.1 商务客户端技术的优点

- 隐私
  用户配置、选项和购买历史之类的信息可以存放在桌面上，而不必放到中央数据库中。如果对这类信息采取适当保护，则客户端存储可以增加个人隐私。
- 方便
  支付与发货地址之类的常用信息可以由桌面软件存放和自动提供给商家服务器，使用户不必在每个站点重复输入相同信息，还可以保证使用的信息是准确的。当然，要实现这些好处，信息存储与提供机制必须标准化。
- 交互性
  也许将功能移到桌面的最大好处是增加交互性。由于软件直接在用户计算机上运行，因此用户与应用程序之间具有高带宽、低锁存信道，从而可以使用拖放之类的高度交互操作，这是纯服务器实现方法所不可能的。

9.7.2 商务客户端技术的缺点

- 安全性
  Java与ActiveX小程序的安全技术主要防止敌意软件攻击桌面计算机及其用户，很少防止敌意用户或不信任客户计算机对分布式应用程序的攻击。对 Internet 商务使用任何客户端软件都要格外小心，防止客户软件的操作错误（有意或无意）破坏应用程序完整性。
- 通用性
  在Java之类的客户技术普及之前，要求较高的客户功能只能减少商务应用程序的用户。如果用户没有客户软件所需的设备或环境，则无法使用这个商务应用程序。更为微妙的是，如果用户要采取特殊操作（如安装插入件或控件），则使用服务器应用程序的难度就更高了。
- 可靠性
  客户端软件的许多潜在好处要求客户计算机维护持久状态，这在可用性和可靠性方面都可能造成问题。如果用户习惯使用几台计算机（例如一台桌面电脑和一台便携电脑），则两台计算机上的存储状态可能不完整和不兼容。如果用户的计算机崩溃（常有的事），则存储状态可能丢失。仅仅依赖用户备份应用程序关键信息是不够的。

9.7.3 客户端功能

在设计 Internet 商务系统时，应当考虑要部署对桌面的每个功能要素。下面介绍其中几个功能要素。

- 收据与单据存储
  余下是 Internet 商务收据与单据存储的自然地点。如果这些项目不在桌面上存储和检索，则用户无法记住访问过的所有不同商务地址。
- 支付证明与应用程序
  有些 Internet 支付协议（如 SET）要求使用客户软件，而有些则可以利用桌面软件自动将信息输入窗体中，例如将信用卡信息输入安全 HTML 窗体中。
- 购物推车
  购物推车功能可以放在事务引擎中进行跨店购买，放在产品目录服务器中进行复杂定价，放在用户桌面上提高交互性。对于客户软件，可以实现拖放项目选择，以及高度交互的订价计算和订单修改。
- 用户配置
  用户配置信息，包括重要的（如发货地址）和一般的（如颜色与样式选项），都可以放在客户上存储。通过在客户上存储这些信息，可以在多个 Internet 站点中使用，而且更加保密。

9.7.4 商务客户端举例

Internet 商务使用客户端软件的现实例子有几个。

- 电子钱包
  CyberCash、IBM、JavaSoft、Verifone 等都实现了电子钱包。这些应用程序存储 SET 和类似协议的用户支付证明信息，还可以起收据存储的作用。
- 购物应用
  Peapod 等建立了桌面专用商务应用程序。Peapod 软件是针对小杂货购买的软件，因此相当具有交互性，支持重复性订单。
- 小程序
  许多站点用 Java 或 ActiveX 小程序显示用户购物篮中的内容。这些显示应用程序通常还利用浏览器帧提供购物推车的单独窗口，与产品目录信息使用的帧分开。

9.8 数字化商品成交的技术

第 4 章曾介绍过，数字化商品是线上成交的。在信息商务中，内容本身就是产品。

9.8.1 安全发送

内容本身就是产品时，商务系统要提供销售与履行之间的链接。支付之后，就要自动履约，为此可以采用几种机制。

- 许可证密钥
  对于网上购买和履行的软件，软件包可以免费下载，但必须有特定许可证密钥才能操作。客户买的不是下载的内容，而是许可证密钥。许可证密钥通常与软件和特定计算机相联系，因此同一关键字不能用于一个软件的多个拷贝。这种方法也适用于购买光盘或网络服务器中的特定信息数据库权限和安全容器（见稍后介绍）。
- 访问控制数据库
  对特定内容包支付之后，商务系统可以输入内容服务器的访问控制数据库。此后，末端用户用传统 Web 访问控制机制（如用户名和口令）通过基本验证登录内容服务器。这个机制有几个问题，主要是用户证明信息存放在许多不同地方，很难记住哪里用哪个口令或在选择新口令时更新所有服务器。系统操作员在涉及多个内容服务器时也很难维护所有访问控制数据库。
- 数字收据
  完成数字商品的支付事务之后，商务系统可以生成和签名数字收据，表示款已收到，可以发货，这是开放市场公司的产品采用的方法。开放市场公司的数字收据是个 URL，指向电子履行区，其中包含一个票。票就像电影票一样，有票入场，无票则无法入场。数字票中包含访问权限信息，这些权限的条款和生成票的事务引用（用于审计）。在这个系统中，中央事务引擎可以提供分布式数字商品履约服务器的商务服务。由于收据是个 URL，因此自动由 Web 浏览器管理，可以由用户标上书签和保存。
- 公用密钥属性证书
  许多 Web 浏览器可以用 X.509 第 3 版公用密钥属性证书实现安全性。这些证书主要用于验证，但也可以用于访问控制。X.509 第 3 版规范可以将证书与大量属性相联系，指定数字商品履约的访问权限。在这个模型中，购买数字商品时，商务系统可以提示用户生成新的公用密钥，然后通过签名将这个密钥变成证书（作为证书机构）并连接描述数字履约所需访问权限的属性。这种方法是可行的，但却是烦人的，因为生成、安装与使用证书很复杂。这个课题见第 12 章介绍。

9.8.2 故障恢复

客户付了钱而没有得到东西时通常会抗议。从买方看，这是可用性问题。发送应当可靠，至少应易于重试，否则客户会跑到别的地方。从卖方看，履行的可靠性是成本与客户满意度问题。如果发送不可靠，则会失去客户；如果重试或故障恢复机制太昂贵，则会成为客户服务成本问题。

故障恢复的方法包括。

- 太廉无怨
  如果数字化商品按页付费，使用微事务，则人们可能愿意支付所有页面的费用，不管浏览成功与否。
- 按时付费
  如果数字化商品按连接服务的时间付费，不常发生不成功下载，或者能迅速解决，则人们可能愿意支付全部时间的费用，不管有效无效。
- 将批量传输与事务分开
  通过以加密或非活动形式下载批量数据，然后对开锁密钥或许可证密钥收费，可以改进履行的可靠性。由于下载批量数据是不保护的，因此使用者需要时可以重试。许可证密钥的下载需要可靠，但它至少较小较快。
- 允许根据事务记录重试
  如果事务记录是持久的，则商务软件可以自动在下载失败之后重新发送。买方要验证自己，使商务系统确认他是后来的买方。例如，开放市场公司的软件以联机声明和数字收据形式提供购买持久证明。
- 提供访问而不是下载
  付费后，商务系统可以建立控制访问项目，指出这个客户下一个小时内可以访问下载区，认为一个小时足够试几次下载，即使第一次不成功也没问题。预订就是这样工作的，开放市场公司的数字收据也是这样。

可审核性

与故障恢复相关的概念是可审核性。一般来说，商务系统要可审核，就要在系统中存储足够的记录，让人们可以合理地同意特定事务是这么发生的。这种记录有多种用途。

- 争议解决
  客户发生争议时，通常指责特定服务或产品没有送达，或收费不正确。如果商务系统提供足够记录，则可以对事务的所有重要特性进行完整审核。日期与时间、验证客户的方法、价格、描述和产品与服务送达的证据。这个信息可以让客户回忆起来或帮助客户服务代表解决争端。

- 故障恢复
  一个有趣的情形是审核可以指示买方没有得到服务。这时，对于数字商品，可以重新发送商品或服务。系统在这个方向出错的原因是发送的边界成本接近于零。
- 审核
  审核具有准确的技术含义，但在这个环境中，我们指一般意义上的检查和平衡，保证所有客户已支付，所有支付与买方相符，商品和服务顺利送达。

9.8.3 权限管理

权限管理指与知识产权相关的问题，特别是在商务设置中保证使用特定内容已经付费，使用量没有超出授权范围。例如，内容拥有者可能要求数据库搜索和在屏幕上浏览结果一种价格，而打印搜索结果则是另一种价格。

在讨论权限管理时，一定要注意遵守规定与执行权限空间的差别。在商家对商家情境中，买方可能没有窃取内容的动机，特别是费用可以传递给买方的客户时。这里要的是一种方便的支付方式。遵守规定有许多设计问题，但整个问题要比可能充满敌意的商家对客户环境中好得多，后者用户很可能窃取商务内容。一般来说，权限管理要求指定希望什么权限和提供什么权限，以及这些权限的支付方式（对于遵守规定）和防止非法使用内容的加密方式（对于执行权限情形）。

加密容器技术

执行权限技术的一般性名称是加密容器技术。一般思路是内容以加密形式在网络上传递，只有到使用点才开锁。除了只有到使用点才开锁的概念外，加密容器技术还可以控制计算环境的一些方面，如关闭 Print 按钮（在文档无权打印时）。最终用户可以手工抄录屏幕上收到的信息，然后重新键入，但加密容器技术能使保护内容的滥用不方便或不合算。

加密容器技术的例子有 IBM 公司的 Cryptolopes 和 InterTrust 公司的 DigiBoxes。这些技术也称为超分配，可以实现从作者到出版社到经销商到用户的整个流通链，在每一点维护经济和安全模型。

版权

数字化产品的一个重要方面是知识产权的管理。信息与物化商品的差别在于可以进行拷贝。如果一个人将电子文档拷贝交给另一个人，则两者都有这个文档，这个事实早已如此。但是，复印机和电子文档使拷贝的成本大大下降。不适当使用和分发版权材料是广大问题，使内容拥有者不愿将信息放到网络上，除非有足够控制防止或阻止滥用。

印痕与水印

前面曾介绍过，要注意遵守规定与执行权限空间的差别。一定程度上，这两者是相对立的：遵守规定就是要便于支持，而执行权限就是要增加拷贝的难度。还有一个中间环节——不

适当使用可跟踪。例如，假设保护文档不适当地在 Internet 上复制和分发。如果能标识这个拷贝的原购买者，则可以阻止不当使用。这种跟踪是可行的，可以通过印痕与水印技术实现。使用这种机制时，文档的每个拷贝稍有不同（但不明显），加上一个序列号或其他跟踪信息的编码。

印痕方法包括：

- 对于图形，可以增加大量杂波到图形编码中。这个杂波对图形的样子没有影响，但解码计算机能知道如何恢复增加的杂波，解码成序列号。
- 对于文本，单词或分行符的间隔微小变化可以编码序列号。

将一个消息隐藏在另一消息中的方法称为留暗号（steganography）。水印不一定要隐藏，但如果不隐藏，则高手可能消除水印。最好在保护文档中放上显式版权声明。这个声明加上发现与跟踪的不当使用，可以以电子形式确定版权信息的社会环境。

9.9 小结

与许多基于信息技术的系统不同，Internet 商务系统依赖于不同厂家提供的客户软件与服务器，由不同组织操作，同时又要在开放网络中相互操作。本章介绍了基本客户与服务器技术、数字商品履约并简要介绍了对象技术。这些组件提供了商务系统的基本线路和 Internet 基础结构。下面几章介绍 Internet 商务系统的体系结构和各种支持技术，如加密、安全与事务处理。

第 10 章系统设计

教育就是按一定方式联系，历史是从例子中学到的哲学。
——迪奥尼休斯·海里卡纳苏斯[①]

10.1 设计问题

下面几章介绍发展 Internet 商务系统的一些关键技术领域。当然，你一定会问，“怎么将它们集成起来呢？”本章考虑这方面的设计问题：对一组组件，如何集成起来，生成最有效的解决方案？尽管我们把组件的细节放到后面介绍，但本章准备提供一个框架，便于了解每个组件在总体系统中所起的作用。

从软件工程角度看，已经出现许多设计方法。面向对象设计、快速原型法、正式方法等都可以在 Internet 商务系统的设计中加以运用。这里并不想偏向哪一种方法，你的系统适用的方法取决于你的观点和经验、小组的观点和经验、可用的工具和许多其他因素。

本章介绍 Internet 商务系统中可能遇到的主要设计问题。这些问题大部分都不是 Internet 商务系统独有的，但确实在这类系统中非常重要。我们首先介绍一些设计原则，这些原则通常与特定技术的选择无关，适用于各种系统。

10.2 设计思想

计算机系统的设计和任何工程设计一样，既是艺术又是科学。科学非常重要：对计算机系统，它指出计算机能成功处理哪种问题，如何评估、测量和选择特定问题的算法，并提供了正确开发计算机程序的一些准则。但是，设计复杂系统需要一定的洞察力、经验和良好的感觉与科学的结合。

10.2.1 了解客户要求

对目标客户及其需求的了解是绝对必需的。许多情况下，客户无法明确说出要什么，因此需要加以分析。方便性是否重要？访问好的信息重要吗？为了得到某种服务，他们能忍受多大的不便？他们愿意付多少钱？这种理解的结果是，用户虽然没见过你的产品和服务，但你的产

①迪奥尼体斯·海里卡纳苏斯，《Ars Rhetorica.XI》。

品和服务推出之后，他们会一见如故，一见倾心。Internet 商务的挑战就是新的未预见的机会很多，无法预测买家会喜欢什么，因此灵活性非常重要。

10.2.2 计划演变

如果任何计算机系统要存在较长一段时间，则应当考虑技术的改变和随时间而进行的演变。计算机硬件的性能（如处理器速度与内存密度）每两年翻一番，而成本基本不变。网络性能（带宽）也在不断提高。计划这些变化之后，就可以利用这些改变，提供长时间的优秀服务和性能。此外，软件也是迅速改变的，仅仅几年前，可能谁也没有听说过万维网。尽管我们无法预料每个可能出现的改变，但我们至少可以想像会发生何种改变，并相应地作出计划，使系统能朝不同方向演变。

10.2.3 从小开始

人们总是希望建立能解决所有已知问题的大型综合性系统，但这种企图必然导致设计和建立时间很长，甚至最后在还没有提供任何东西之前就报废了。而从小系统开始可以提供学习的机会，并可以相应适应系统演变。这种方法在快速改变的 Internet 世界中更加重要，因为大型复杂的系统很可能来不及部署就已经过时。相反，增量开发则可以在系统中利用技术改变并不断了解客户与业务。

10.2.4 使用开放选项

设计的过程就是不断选择的过程。但是，我们经常发现有些选项更容易限制今后的选择。例如，我们可能针对特定支付方式设计相关系统（如信用卡），尽管信用卡在当今相当有效，但今后也许不再那么有效。我们无法预测今后需要什么，但我们应将系统设计成能够以一般化形式处理支付方式，用特定模块实现信用卡支付方式。这样，今后可以增加其他支付系统。如果在系统的早期进行操作，则增加灵活性通常不会增加更多成本。这样，进行设计选择时，如果一切基本相同，则最好选择将来灵活性最大的途径。

10.2.5 开发体系结构

第 6 章曾介绍过，系统体系结构对长期开发和演变有重大影响。尽早注意建立体系结构，特别注意这里介绍的设计问题，将有助于系统长期增长和发展。系统体系结构是解决各个设计问题的框架，初始设计阶段确定这个框架显然有好处，但体系结构在后面更加重要，因为这个框架要解决最初建立系统时未能预见的问题。

10.3 结构性方法

下面几节介绍一些系统设计中最重要的问题，这些问题涉及到 Internet 商务系统开发的许多阶段（当然，也与许多不同的计算机系统有关），每个问题都是总体体系结构、详细系统设计、实现和操作系统的一部分。例如，进行构筑分布式系统的结构性决策。但是，如果详细系统设计没有提供必要的功能或实现时省略某些必要的功能，则再完美的规模体系结构也无济于事。

要考虑的基础性设计问题包括：

- 性能与规模
- 可靠性
- 事务
- 管理状态
- 安全性

我们相信，每个问题都是基础性的，既对 Internet 商务系统很重要，又涉及开发的不同阶段，下面将一一介绍。

10.3.1 性能与规模

简而言之，规模就是系统如何扩大尺寸以提供更多服务[②]。我们可以用许多不同方式测量系统规模，如总用户数、同时用户数、事务量，等等。这些尺度不是独立的，一个维度上的系统扩展通常也会影响其他维度。其副作用可能帮助或损害其他方面，这取决于所作的改变。例如，增加系统 CPU 性能通常会帮助多个方面；相反，增加数据库长度以处理更多用户则可能使性能下降。

因此，一定评估要系统可能进行的改变，在整个系统情境中而不是单个组件中改进规模或性能。有一些明确的系统属性（如最主要的是为几百万用户服务）就更容易在需要时进行取舍，以及确定如何改变软件与硬件配置，达到所需改进。

通常，系统体系结构会允许或限制某些规模改变。例如，设计成在单台计算机上运行所有组件的系统（产品目录服务器、支付系统、用户账号管理，等等）如果要扩展系统，就是要购买更大的计算机。因此，这种系统的规模受计算机限制。有时，计算机技术的自然演变（更快的 CPU、更大的内存系统、更大的磁盘）使系统可以扩展到所需要的服务水平，但通常无法这样（特别是由于基础软件要占用大量其他资源，如操作系统、数据库、应用程序）。相反，分

②经验表明，每次系统规模增加 10 倍时，一些意外事项就会成为严重问题。由此可见，系统设计人员一般很难预见指数级改变之后的情况。为了弥补这个现象，可以多加推敲（因为这个问题很复杂）或计划在系统增大到某一点时处理意外问题。这样，特定设计问题只能在已知和计划指数级问题时才能得到解决。

布式应用程序对小型系统效率更低，但随着需求的增长，更容易扩展。

关于 Internet 服务扩展另外一点（常被忽略）是扩展的快慢。Internet 服务通常普及很快（见第 7 章介绍的“蜂涌”效果），因此一定要迅速在系统中增加功能，以便适应需要。例如，如果系统能够在需要时增加所需的服务器，则增加功能时不会影响现有服务的操作。

对于许多系统，性能不良常常带来不便，是意见的根源，但用户仍然会使用这个系统。而在 Internet 商务系统中，性能问题不止是不方便，还可能影响业务，吓跑客户和把好处让给竞争对手。

系统性能可以用多种方法测量，因此一定要确定哪个指标最重要。两个最常用的指标是锁存和通过量。锁存测量完成某个操作需要的时间。例如，下载 Web 页面需要多久？通过量测量同一时间可以完成多少操作：服务器一个小时可以发送多少 Web 页面？这两个指标看起来好像是相同的，但实际上是完全不同的两回事。锁存表示特定用户的平均经验，而通过量表示系统能处理多少用户数。另外，这两个指标只是相关的，例如，随着通过量的增加，单个用户看到的锁存可能增加。就像在高速公路上开车，路上的车越多（通过量），车速就越要减慢（高锁存）。

为了得到系统性能的良好特征，需要事先确定测量什么，然后测量这个指标并进行改进。尽管随着时间的推移，重要指标可能改变，但这是真正改进系统的惟一方法。通常，系统选择的性能指标使它看起来很不错，而没有考虑用户对系统性能的感觉。

10.3.2 可靠性

许多业务计算机系统要求高度可靠性，这在 Internet 商务系统中尤其重要。Internet 商务的特殊挑战在于受公开干扰的风险。系统不行时，业务也无法开展。在别的场合，人们是可以对付计算机故障的。例如，邮购公司的前线操作员可以在需要时写出书面订单，至少可以用电话答复。而在 Internet 中，如果服务器关闭，则人们甚至无法判断公司是否还经营！

可靠的系统通常是用冗余组件建立的，因此，一个组件遇到故障时，另一个组件可以替换。在许多网络协议中（如 TCP），网络上消息发送者要得到确认和重发消息，直到送达（或次数太多而放弃）。这种从困难恢复的工作也可能掩盖故障，但如果这些故障不向操作员报告，则系统无法修复，直到所有冗余组件失败。这时，所有冗余设计都白费了。注意系统，保证组件破坏之后尽快恢复。

10.3.3 事务

“原子性”一词是从事务处理中引出的。在许多应用中，一定要保证事务原子性，即不能让一部分事务完成而另一部分事务没有完成。例如，钱从一个银行账号转到另一个银行账号时，事务分两个部分：从一个账号批款和向另一账号存款。显然，或者两边都完成（事务成功），或者两边都不发生（事务失败）。如果一边完成（如存款），则结果是错误的。这种故障

还可能直接造成客户不满意（和难于纠正的错误），因此应全力避免。下面介绍事务的几个关键概念，第 16 章将详细介绍事务处理。

Internet 商务的事务通常有此要求：原子性。此外，它们还要满足另外三个要求：一致性、隔离性和持久性。一致性就是所有部分有相同的事务结果视图，隔离性表示独立活动不能相互干扰，持久性表示事务结果不因硬件故障而取消。

在分布式系统中，如 Internet 商务的客户 /服务器系统中，双方完成操作时可能要进行几次消息交换。如果这样，则系统要注意网络中的故障，防止消息丢失、重复或搞乱消息顺序。可以把事务看成从第一个消息开始，到最后一个消息为止，因此完整事务应具有原子性。如果网络在事务中途遇到故障，则系统状态应当一致。最好将双方都清楚事务是否成功，否则通常要能让双方判断结果如何。

不难看出这种原子性属性对于支付事务中作用——上例银行账号转钱应当是一个例子。完成购买事务的其他方面也要有原子性。例如，支付只是购买事务的一部分，还要在事务中记录正在完成的购买。如果转钱之后，商家忘了买的是什么，则商品永远无法发出。

从各种故障恢复的一般问题与原子性有关。事实上，可以用实现某种事务的原子性来作为避免某种故障或从某种故障恢复的方法。Internet 商务系统中最常见的故障是网络故障和系统崩溃。下面介绍它们造成的问题。

在网络故障中，两个系统之间的通信遇到一些问题，此外两者都是正常工作的。如果不在设计应用程序时多加注意，则网络故障的后果相当令人费解。例如，客户没有得到请求的服务或服务器发送的响应没有到达客户。更具体地说，假设客户购买了下载的软件包。如果下载过程因网络故障而中断，客户怎么完成下载呢？

不同系统可能用不同方法处理这个问题，但一定要加以解决。例如，一种恢复系统的方法是服务器中具有每个客户的账号，包含所有已完成事务的清单。客户遇到网络故障时，可以向服务器标识自己，检查事务清单，并恢复失败的发送。另一种方法是发出商店收据，用于网络故障后恢复软件下载。

另一方面，系统崩溃则要用不同方法处理。崩溃准备的关键问题是保证重要信息可持久，并在适当时间记录到稳定存储体中[③]。所谓稳定存储体就是磁盘之类的存储媒介，在崩溃和断电时仍然能存储信息。例如，系统应记录购买完成之后再将这个事实告诉客户，保证如果发送完毕之前服务器崩溃，则服务器至少知道发生了什么，客户不会在操作还没有完成的情况下认为操作已经完成。

系统如何从故障恢复不是单纯的技术问题，也对客户如何看待系统和客户服务要解决的问题有影响。评估商务系统中使用的产品时，了解系统如何处理这些问题通常能够透视系统设计人员对生成应用程序时的困难问题花了多少心思。

---

③当然，另一种方法是保证系统永不崩溃。这个方法通常要求特殊硬件和软件，以及认真关注看起来很平常的问题，如冗余电源。

10.3.4 管理状态

在任何分布式系统中，关键问题是不同的信息即系统状态存放在哪里。可以看成基础信息存放在数据库中，不管这是真正的数据库系统还是表示应用程序所存储信息的文件集合。介绍系统状态管理时，我们讲的是正在修改的过程变量。例如，特定事务可能有几个步骤，系统要跟踪每个步骤的进程和结果。最后，这些改变要在数据库中实现信息更新，或者放弃。

对 Web 之类的客户 /服务器系统，实际上是选择哪一边存储特定信息。在三层 Web 应用程序中，则有三个可能的地方：客户、应用程序逻辑和第三层数据库。有些选择是一目了然的，客户专用的信息或与几个不同服务有关的信息可以存放在客户中，不针对客户或用户的信息可以存放在服务器中，其间的完成事务状态、用户账号信息和事务进行中的信息要在某个地方存放。这种信息在三层系统中通常放在应用程序服务器中，而使用两个系统时则要分解到客户和服务器中。

由于旧版 Web 浏览器很少提供跟踪用户特定状态的方法，因此商务系统通常要亲自管理所有状态信息。有些应用程序（特别是支付系统）要在客户端管理更多状态，这些方法各有所长。下面是服务器的一些优势。

- 不需要特定客户软件。
- 客户可以用任何地方的系统，无论在家里、办公室、阅报亭中、或其他计算机上。计算机不必与特定软件和配置相联系。
- 服务器可以根据业务与应用安全要求控制信息安全性。
- 记录的信息可以扩展，不需要向客户发布更新软件。
- 客户不需要增加进行联机业务所需的应用程序。
- 服务器的累计信息可以在特殊促销程序等应用中使用。

将信息存放在客户端对客户有一些好处，主要是关于支付证明信息、正在进行的事务和事务历史的信息在客户系统中保存。客户应用程序还可以保存联机购买的收据等项目。当然，商家会跟踪其中一些信息，便于计账和促销，不管客户使用的正式副本在哪里。

对许多应用程序，开发客户组件的成本太高。第 9 章曾介绍过，随着用 Java 与 ActiveX 之类的技术开发客户应用程序的工具开始普及，这个情况可能改变。客户应用程序的真正价值在于应用程序提供一些独特的功能，是纯服务器实现方法所无法提供的，或者可以在多个不同服务器中使用客户应用程序（加上一些真正的实用程序）。如何更好地利用客户端组件仍然是系统设计人员需要认真考虑的问题。

10.4 安全性

安全性是 Internet 商务技术的最大问题。常见的问题是：Internet 能安全地进行商务吗？从

某种意义上说，这么问是不对的，应该问：Internet 能足够安全地进行我的商务吗？就像房门与银行保险柜使用不同的锁，Internet 商务的安全性也有许多不同的技术组件，取决于风险、成本、信息价值等因素。

下面将安全问题分为 4 大类：

- 系统安全性
  计算机的操作系统安全性如何？非法用户能否登录？能否防止系统中其他用户读取信息，系统中的任何用户能否读取和修改系统中任何信息？系统物理上安全吗？谁能进房间？这是应用程序系统的基本问题，相当重要，因为在不安全的基础上不可能建成安全的应用程序。
- 通信安全性
  通常要防止消息内容被窥视或别人用其他方法偷看消息。商务应用的常见例子是保护客户的支付信息，如信用卡号，客户要将其发给商家的服务器。这种情况下，我们通常用某种加密机制使消息保密。
- 数据安全性
  数据安全通信之后，要考虑末端系统中如何保护数据。有时数据立即处理和放弃，不需要更多保护。有时要靠操作系统的保护机制保护数据。对特别敏感的数据（如客户信用卡号），我们选择加密磁盘上存储的数据。
- 验证与授权
  验证就是以可靠方式回答“你是谁”。口令是计算机系统验证用户的常用方法（可以有多个口令），但还有其他方法。授权就是回答“你能干什么”。例如，系统可能包含可以进行特定操作的人员名单。在商务系统中，授权通常指证明你已经为某个东西付费。

这些安全方面对任何 Internet 商务系统都很重要，应放在任何系统设计和生产评估之中。根据这些思想，设计和评估系统时要记住三大安全原则：

1. 安全要求由业务要求与相关风险确定。我们应对处理百万美元事务的应用和处理十美元事务的应用建立不同的安全系统。别指望系统是绝对安全的，根据风险和威胁程度，要确定某种安全技术是否合适。
2. 保护一个系统是保护整个系统，而不只是其中的各个组件。每个组件可能都有自己的安全属性，而集成起来的系统则不一定安全。不同组件之间交互性可能很差，或不同组件之间留有漏洞，敌人有机可乘。设计安全系统需要注意整个系统。
3. 安全系统的操作是要保护的最重要元素。如果不锁住房子的前门，则门上有没有锁都差不多。同样，安全系统的操作中要密切关注用户和系统操作人员是否如期使用这个系统。特别是，用户有时可能有意无意降低系统安全性，以便使用时更方便或更容易。因

此，系统操作员一定要注意系统如何使用，以便发现系统误用和破坏系统的企图。

了解这些原则有助于保证设计、实现和操作安全的商务组件，第12章将深入介绍加密法，可以生成安全系统的许多组件。利用这些加密法，第12章将详细介绍 Internet 商务的安全技术问题。

10.5 设计原则与现有技术

现在买PC机最难的问题就是怕还没有开箱就已经过时。计算机硬件的改变速度是惊人的，计算机软件的改变速度也是同样惊人的。仅仅几年时间，Web已成为大多数 Internet 商务系统和许多其他应用的基础。今天的技术日新月异，因此本书很难说什么技术或什么产品最适合特定商务应用。

因此，我们不是针对特定技术，而是介绍设计商务系统的基础性问题。这些原则适用于许多不同技术，可以评估许多不同产品，可以开发满足特定业务需求的特定应用。更重要的是，通过回头看看这些原则，可以看到系统中什么是真正重要的，如何随着时间而演变。与其选择组件和围绕其建立应用程序，面临着很快过期，不如开发一种策略和设计方法，使公司能够设计需要的系统，然后实现这个前景所需要的产品或定制开发。

前面曾介绍过，这正是系统体系结构如此重要的原因所在。这个体系结构提供了演变的框架和何时适应各种技术的决策，使评估可以集中在要解决的业务问题，而不是围绕新技术的各种夸大之词。

10.6 小结

本章介绍了设计 Internet 商务系统的重要方面。尽管这些问题不是设计各种计算机应用程序是共有的，但在 Internet 商务应用中特别重要。当然，不同应用程序最终会针对不同要求和选择的结构性方法采用不同设计。即使每种情况的答案有所不同，任何成功设计也必须在某个时候面对这些问题。

记住这些基本原则之后，就可以转入 Internet 商务主要技术领域的更详细介绍了。下面几章以本章介绍的原则和设计问题为背景，将各个技术放进 Internet 商务的总体系统中。

第 11 章生成与管理内容

对热爱自然并与其有形肢体交流的人，她说的是多彩多姿的语言。
——威廉·柯伦·布莱恩特[1]

11.1 客户看到的内容

客户在网络上做生意时，第一个看到的是内容：Web站点上的信息、产品目录、简报等。对大多数Web站点而言，拥有吸引客户注意和重复访问的精彩内容是非常重要的，商务站点也不例外。Web内容的具体样子和感觉是创造性的和促销设计问题，但 Internet 商务系统的设计需要对Web内容机制及生成与管理内容的工具有一般了解。本章概述Web内容技术及如何在 Internet 商务中运用。

本章简要介绍几个Web相关软件，而不是样样俱全。当然，随着时间的推移，这些软件包的细节会有所改变，因此你应在建立应用程序时对软件包进行相应评估。

11.2 基本内容

万维网上的内容是由多媒体超文本页面组成的，通常用超文本标记语言（HTML）描述。Web页面是多媒体，因为它们可以包括文本、图形、声音、影像和其他各种数据。事实上，Web协议可以扩展而处理任何媒介。Web页面是超文本，因为它不像图书页面一样按照线性顺序，而是可以链接任何其他Web页面，以复杂而随意的方式进行链接。

HTML是结构化文档的描述语言，类似于SGML（结构化通用标记语言），后者是多年来专业出版方面的标准。文档源代码中的标志描述文档的词法，而具体显示细节留待客户端软件处理[2]。这与Postscript之类的系统采用在不相同的描述模型，后者描述文档的外观而不描述文档结构。

在最常见的操作方式中，Web浏览器取得一个或几个Web服务器中用HTML编码的页面。Web页面用统一资源定位器（URL）标出。URL中的组件告诉浏览器如何找到适当服务器和用什么协议取得页面，URL的结果发送到服务器中，寻找这个服务器上的特定页面。

---

①威廉·柯伦·布莱恩特《关于死亡的冥想》。

②在HTML中，标志在文档中标为<tagname>。如果用标志标出一段文本，则这个范围放在<tag>与</tag>之间。

如果页面只是链接下一页面，则仍然按照页面的线性顺序。但在HTML中，页面上的任何地址可以链接同一服务器或任何地方的另一服务器上的另一页面。链接的位置称为控制点。控制点可以在页面清单中，如目录表或索引，可以在移动文本中，如可单击图形中的一部分。这种页面链接许多不同页面的功能使全世界服务器上的一组组页面变成Web网络。

11.2.1 基本格式

使用HTML时，Web浏览器的内置功能可以处理几种标准内容类型。

文本

文本包括构造文档的各种组件，如标题、不同字体与字号、居中之类的布置指令。

清单

HTML支持任意层嵌套的项目清单。标准HTML提供三种清单：无编号（强调符）清单、编号清单和定义清单，后者用于词汇表之类的文本。

图形

Web浏览器以几中不同方式处理图形。文档可能只是一幅图形，这时文档的MIME类型指定图形格式。HTML也可以用特殊标志嵌入图形，浏览器取得实际包含图形的独立文件。除了显示图形和框图之外，Web页面常用图形和小图显示装饰图、图标和工具栏。这种方法使Web设计人员在生成Web页面的外观时具有巨大的灵活性。

窗体

Web的主要功能在于能够生成交互式应用程序。最简单的交互形式是窗体，HTML窗体可以包含复选框、菜单选择和文本输入字段等元素。用户可以填好窗体并将其提交给Web服务器，然后根据窗体内容返回信息。窗体将在稍后详细介绍。

11.2.2 高级格式

除了这些基本功能之外，如今大多数浏览器还可以处理更高级的HTML结构。

表格

表格是在内容阵列表示方法中达到更好控制的机制。例如，在旧版HTML中，要对齐一列图形，惟一的方法是将该部分文档变成定节距字体。HTML的表格格式功能用非常一般的行和列描述，使设计人员有许多布局选项。

帧

帧结构机制使几个独立Web页面可以共享同一浏览器中的显示空间。这种机制的一个应

用是维护一组页面的不同视图。例如，站点可以把漫游视图放在一个窗格中，把细节内容放在一个窗格中。

图形映射

Web浏览器通常把超链接显示为加亮文本，表示单击文本可以调用所链接的Web页面。通常也可以单击图形，即小图形可以作为表示超链接的图标。图形映射是另一种表示和激活链接的方法。使用图形映射时，图形可以单击激活不同部分，使其激活不同的超文本链接。图形映射可以在服务器方处理，这时浏览器将单击坐标发送到服务器；也可以在客户端处理，这时服务器将图形的热区域描述发送给浏览器。

11.2.3 控制外观

与许多文档描述语言不同，HTML描述文档的语义，而不是描述文档的外观。浏览器控制HTML文档的各个标志元素如何显示。这样，HTML文档可以在各种不同设备中显示，因为浏览器可以根据设备功能对其进行不同绘制。甚至可以对视障人员绘制HTML，同时仍然提供文档的结构信息。但是，这就要求页面设计人员不要控制页面的最终外观。

过去，控制用户显示器中Web页面的外观是Web作者的大问题。通常，页面生成小组要用最常用的浏览器测试HTML页面，根据需要调整HTML编码。有时甚至要采用特殊技术控制外观，如在页面中插入透明或隐藏图形，准确地控制间距。

对有些应用程序，这样缺乏控制是个遗憾的局限。为了让作者更好地控制HTML显示，Web社区开发了级联样式单（CSS）。这个提案使Web页面可以引用一组样式单，描述各个元素如何显示。更妙的是，HTML页面可以链接几组样式单，定义不同设备中页面的优选表示方法。例如，高分利率PC机显示器用一组样式单，低分辨率PC机显示器用一组样式单，视障人员使用的 Internet 浏览器用一组样式单。

这个问题还出现了其他解决方案，如动态HTML和XML。应用程序设计人员应注意内容标记语言的开发，因为这是让商务经历吸引用户的核心部分。

11.2.4 Web 页面与窗体

填写窗体是Web上强大的交互方法，窗体中的HTML标志在浏览器屏幕中生成与标准HTML标志交织的可编辑字段集。每个字段有名称，不对用户显示，但可以在服务器中用于跟踪各个字段。窗体是由Web服务器生成的静态页面或程序动态输出，动态窗体可以根据程序需要改变最后的字段集，字段初始值可以由服务器填写，也可以留空。填好窗体之后，用户单击提交按钮（可能显示别的标题）。这时，字段名和内容发送到Web服务器中，用一系列名称和数值对发送，Web服务器中运行的应用程序接收和解释窗体内容。图 11.1 显示了窗体的HTML源代码，图 11.2 显示了一个浏览器中显示的对应Web页面。

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">
<html>
<head>
<meta http-equiv="Content-Type"
content="text/html; charset=iso-8859-1">
<meta name="GENERATOR" content="Microsoft FrontPage 3.0">
<title>HTML Example</title>
</head>
<body bgcolor="#FFFFFF">
<h1>HTML Example</h1>
<p>This page contains HTML examples for <u>Designing Systems for
Internet Commerce</u>.</p>
<p>An HTML page can contain headings, text, lists, graphics, and
so forth. This page was prepared using Microsoft FrontPage.</p>
<p>Here is an HTML numbered list:</p>
<menu>
    <li>This is the first item</li>
    <li>This is the second item</li>
</menu>
<p>Here is an HTML table with two rows and two columns:</p>
<table border="0" cellpadding="3" cellspacing="4">
    <tr>
        <td>Row 1</td>
        <td>Cell 1,2</td>
        <td>Cell 1,3</td>
    </tr>
    <tr>
        <td>Row 2</td>
        <td>Cell 2,2</td>
        <td>Cell 2,3</td>
    </tr>
    <tr>
        <td>Row 3</td>
        <td>Cell 3,2</td>
        <td>Cell 3,3</td>
    </tr>
</table>
<p>Right below this line is a graphic image of a line of roses.</p>
<p><img src="Rose2003.gif" width="425" height="30"></p>
<p>Here is a simple announcement for a sales inquiry form:</p>
<form action="sendmessage.cgi" method="POST"
name="sendmessage.cgi">
    <p>Priority: <input type="radio" checked name="R1"
value="V1">Normal
    <input type="radio" name="R1" value="V2">High <input
type="radio" name="R1" value="V3">Emergency</p>
    <p>Message: <input type="text" size="40" name="T1"></p>
    <p><input type="submit" name="B1" value="Submit"></p>
</form>
<hr>
<p>The end.</p>
</body>
</html>
```

图 11.1 窗体的 H T M L 源代码

H T M L 窗体可以包含下列字段类型：

- 复选框——选择选项。
- 单选钮——一组按钮，只能激活其中一个（就像汽车收音机中的选台器）。
- 文本行——可编辑文本行。
- 可滚动文本行——可以比框更大的可编辑文本行。

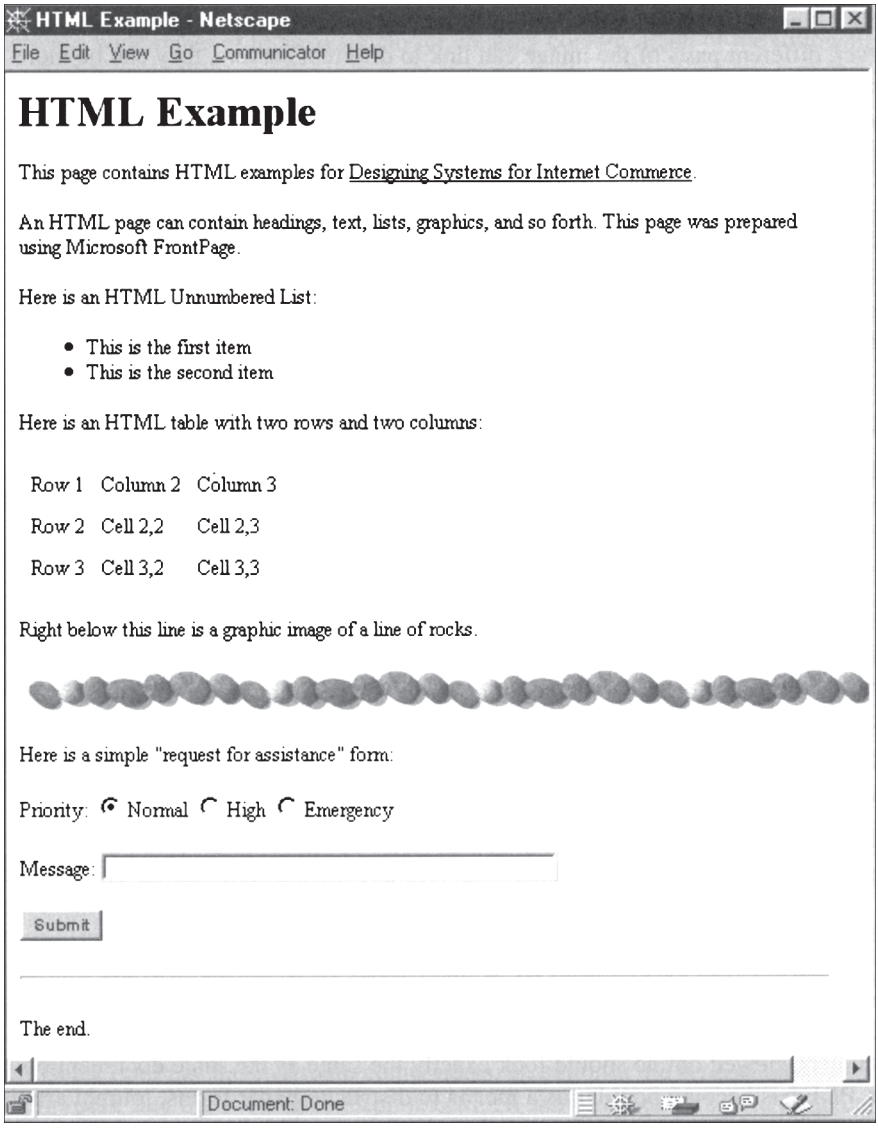


图 11.2 浏览器中显示的窗体 Web 页面

- 文本区——具有多行的可编辑文本框。
- 按钮——提交窗体或复位窗体内容的按钮。
- 图形——按钮可以绘制成图形，而不是带文本标题的按钮。
- 下拉菜单——包含选项的下拉菜单。

这些元素可以用不同方式组合，生成许多交互式 Web 应用。

11.2.5 图形

HTML文档可以包含GIF或JPEG格式的嵌入图形，嵌入图形不是通过将图形本身编码存储于HTML文件中，而是存放成Web服务器中单独的图形文件。HTML文件作者只是在HTML源代码中插入图形源标志：

```
<img src="Rocks80E3.gif" width="528" height="30">
```

Web浏览器遇到这类标志时，先用HTTP取得图形，然后就地绘制。width与height属性向Web浏览器显示图形长度，使Web浏览器能够留出图形空间，并继续绘制页面其他部分。图形可以等后面再填入，因为下载图形需要更长时间。这个方法可以在低速 Internet 连接中更快地显示页面的文本部分，而不必在最终提供实际图形时将显示重新格式化。

图形映射

在HTML内容中，超文本链接的位置点可以出现在文本中，作为图形或图形的一部分。常用Web机制是采用包含多个其他页面链接的图形，图中区域（或热区）的几何定义可以保留在服务器中或发送到客户端。图形映射最初只能在服务器中解释，但今天的大多数浏览器都能使用客户端版本。客户端图形映射有几个优点：减轻服务器负荷，图形不同部分可以链接不同服务器，对用户更具交互性，可以在纯文本浏览器中更有效地利用。

11.2.6 多媒体

Web内容不限于文本、图形和图像，也可以用声音、影像和动画。动画图形可以用GIF图形编码格式、客户端脚本、动态HTML或 Java 之类的扩展语言建立。声音、影像其他多媒体类型可以由外部应用程序处理或用插入件在浏览器中就地获取数据。

11.2.7 其他内容类型

HTML及 Java, JavaScript 与 ActiveX 之类的可编程扩展是Web中最广泛使用的数据类型。其他类型也在不断普及。

VRML

虚拟实境标记语言（VRML）可以定义三维虚拟世界。在适当浏览器中下载VRML模型之后，用户可以在桌面上交互式地漫游虚拟实境。

PDF

Adobe系统公司的可移植文档格式（PDF）是由著名的Postscript语言发展而来的，描述印刷文档。PDF的目标是使Postscript成为联机浏览文档的有用环境。PDF在Postscript中增加了查找、交互式使用、超链接和标注功能。HTML与PDF之间的关键差别在于HTML描述文档结

Informix 公司的通用 Web 连接

和其他数据库接头一样，Informix Universal Web Connect（IUWC）系统用 HTML 内容页面中的特殊服务器方标志选择和合并 Informix 数据库信息。环境包括：

- 持久应用程序状态
  IUWC 将应用程序代码与 CGI Web 驱动程序分开，实现长久应用，并提供管理连接与会话的服务。在操作时，Web 服务器用 CGI 启动小驱动程序。Web 驱动打开和应用程序模块的连接。这样就可以在调用之间使应用程序保持运行，减少启动开销，并使应用程序可以在较长的事务中保持状态。
- 应用程序管理
  IUWC 在数据库中存储整个应用程序内容（包括模板和数据），这样就便于应用程序测试和分阶段，更容易在需要时将应用程序撤同旧版本。

11.3.3 编辑环境

比用数据库内容生成页面更进一步的是设计、构造和维护整个 Web 站点的工具。Microsoft FrontPage 就是这种工具，因为它同时处理多个页面，而且通过 FrontPage bots 支持动态内容，但它主要是个桌面发布应用程序。

Bluestone Sapphire/Web

Sapphire/Web 是开发部署和管理 Java 与 Web/ 数据库应用程序的环境。基本思想是把按钮、Java 小程序之类的用户界面组件与数据对象（如数据库数据、存储过程与用户编写的代码）相关联，然后应用程序可以用不同中间件和事务支持环境部署到不同 Web 服务器中。部署应用程序之后，Sapphire/Web 提供了支持应用程序操作的管理功能。

- 开发
  Sapphire/Web 包括集成开发环境，提供项目与代码管理、可视开发、向导和大量 Java 类与中间件组件集。
- 部署
  Sapphire/Web 应用程序可以用各种 Web 服务器与数据库运行，开发人员可以选择多种中间件软件包和不同应用程序组件互联，包括 Java 与 CORBA 软件包。
- 管理
  Sapphire/Web 应用程序可以跨多个服务器，实现负荷平衡、分区与容错。管理控制台提供了整个服务器集的图形界面，可以动态启动、停止和测试组件。

其他编辑环境

Web 让其他编辑环境包括 Allaire 公司的 ColdFusion(http://www.allaire.com/) 与 Vignette 公司

的 StoryServer(http://www.vignette.com/)。

11.3.4 完整应用程序

除了生成 Web 内容的通用工具之外，还有许多针对更专门 Web 应用程序的软件包，提供了特定需求的深层功能，如目录或发布。对于 Internet 商务，这种完整应用程序包括 Open Market 公司的 LiveCommerce，Folio 公司的 siteDirector 和 iCat 公司的 Electronic Commerce Suite。

Open Market LiveCommerce

LiveCommerce 是 Web 上生成和部署产品目录行业组件的应用程序，提供了导入或生成产品目录数据、将数据存放在面向对象数据库中的工具，提供了查找与排序产品目录的简易工具，并可以集成到 Transact，即 Open Market 公司的订单管理应用程序。下面介绍 LiveCommerce 的一些功能。

- 生成产品目录
  LiveCommerce 提供了将产品目录数据导入面向对象数据库的灵活方法。信息可以从其他数据库、从文件装入或生成全新信息。此外，LiveCommerce 还可以管理产品配置，不必输入产品的所有变形的信息。例如，一系列具有不同处理器、内存与磁盘功能的计算机产品可以描述为一组选项，而不必枚举各种可能的组合。
- 漫游
  大型产品目录的一个关键问题是寻找所要的内容。LiveCommerce 提供层次式漫游，可以定向、浏览和排序产品目录。例如，软件产品目录可能允许用户将产品目录定向到低价产品，只浏览 PC 兼容产品和按制造商排序。单独漫游窗口提供了连续反馈，帮助用户不致在数据中迷失方向。
- 参数化查找
  LiveCommerce 还提供参数化查找功能，利用这个技术，产品目录项目可以有任意属性组及相关数值。参数化查找可以按任何顺序使用任何属性组，缩小查找空间，如果查找结果数较小，则 LiveCommerce 可以查找显示。否则系统列出匹配项目数并显示其他可以用于选择的属性，使用户可以继续查找。
- 个性化
  LiveCommerce 使用户可以注册到系统中，用户的信息可以用于修改产品目录显示。例如，不同公司的用户可能看到针对该公司的产品号和价格。

FoliositeDirector

FoliositeDirector 是在 Web 上用 HTML 发表信息数据库（称为信息库）的应用程序，系统的典型用法是传播法律、税务和会计信息。可以自动生成目录表和提供快速信息查找功能，相关的产品 SecurePublish 提供对信息库的验证预订访问。

- 媒介独立性
  Folis信息库可以发布到Web（用siteDirector）、局域网或通过光盘独立使用。增量注释与更新完全集成到信息库中，也可以进行查找。
- 非结构性信息
  与配件目录不同的是，信息库通常没有那么结构化，而是包含高度非结构化的文本信息。因此，siteDirector提供了有效的文本查找与查询功能，可以让用户找到相应文档。系统用相关性级别按最相关到最不相关的顺序排列候选文档。
- 商务功能
  siteDirector的编程接口可以让开发人员在系统中增加访问控制、按视图付费和基于使用的计账功能。siteDirector的SecurePublish版本用Open Market公司的Transact分布式联机预订功能来控制信息库的预订访问。

iCat Electronic Commerce Suite

iCat公司的Electronic Commerce Suite适用于中小型零售或商家对商家产品目录站点。这个产品包括生成、管理与放置联机产品目录的工具，包括安全事务功能，具有丰富的图形化项目信息，以及一组产品目录模板。系统用模板生成显示页，具有从任何支持ODBC的数据库中取得的产品信息。事务功能通过CyberCash、Open Market Transact或FirstVirtual system提供。

11.3.5 选择应用程序

现成的应用软件部署和操作成本总是比内部开发和维护的方案便宜，只要这个应用程序符号公司要求。原因包括：

- 开发成本由多个客户分摊
- 维护与支持由厂家处理
- 经常性发布可以定期加进新功能，这对各种Internet应用特别重要，因为技术的改变速度是如此之快。

作为包装应用程序的例子，可以看看会计软件。在早期信息技术时代，公司通常要编写自己的会计系统。现在，几乎所有公司都使用包装会计软件。可用的产品包括简单的Intuit QuickBooks到大型复杂的Oracle Financials系统。

11.4 管理内容

生成内容具有相当创造性的方面，但也有过程性的方面，从创造性键盘到生产Web站点之间的路径是认真定义和严格遵循的。这个过程性工作有时也称为编辑过程流程或Web内容

的发表阶段。本节介绍内容的生命周期：生成、编辑、分阶段、测试、生产和存档。

11.4.1 生成

内容来自某个地方，可能从头开始写、从其他来源整理或从其他来源直接取得。除了生成内容的创造性部分之外，过程性部分包括一系列转换和格式化步骤，然后不同项目才成为活动 Web 站点的一部分。

格式转换将文档从不同桌面发表或源格式移到 HTML 或其他标准格式。这些步骤可能手工进行、使用桌面转换工具进行或自动进行。无论哪种情况，输出的文档都有可能不像样子。桌面发表文档要通过格式化达到一定的打印样子，通常可以用几种方法。例如，段标题可以用标准类型样式编码成段标题段，也可以用非标准类型样式编码成体段。自动转换工具有时可能得到意外结果，特别是输入格式缺乏 HTML 使用的词法信息时。这类问题要通过经验、标准、培训与测试来解决。

格式将标准模板作用于构成站点的文档。这些模板可能在桌面发表工具用于准备内容时作用于各个文档的生成，或用于自动化工具生成数据库驱动内容。无论哪种情况，模板的价值来自用户的一致性表示和简化标志、工具栏、漫游辅助等重复性元素的使用。

11.4.2 编辑

生成项目并转换成正确格式之后，它要经过几个编辑步骤。

- 项目是否符合公司的外观标准？
- 拼写、语法和其他表示方面是否正确？
- 所有事实是否正确？
- 是否有超文本的正确链接？

除了超文本链接之外，这些步骤在印刷品与 Internet 中是相似的。这些过程在 Internet 中的难度有两个，第一是要达到完全电子过程，第二是要符合实时要求——新内容的限定时间不是一个星期，而可能是 10 分钟！

11.4.3 内容的事务性方面

Internet 不同于杂志和报纸。在印刷中，每个新问题还在读者看不到的时候就经过完全安排，整个问题一次性发给预订者。相反，Web 内容则可以让预订者随时看到。如果站点要利用 Internet 功能不断发送更新内容，则站点可能在读者的眼皮底下直接修改。因此需要认真设计以便在更新生产站点内容的同时保证内容的内部一致性，即所有链接实际工作所要的测试全部进行。不仅系统要适应这种更新，而且还要认真设计和遵循完成工作的过程。

下面是两个特别危险的事。

1. 多位作者

任何时候多个作者同时写作时，就可能有多个人同时想改变同一文档。根据这种改变的细节，一个人会“赢”，别人会输。最糟的情况是，得到的文档一片混乱。这个问题的通常解决方案是应用源控制工具锁定文档之后再更新，或使用文档仓库，可以维护多个版本和标识冲突。

2. 改变多个页面

通常，Web站点的改变就意味着更新许多页面。除非很仔细，否则活动用户可能看到页面处于不一致状态，浏览一些页面的旧版本，同时浏览一些页面的新版本。浏览器与代理服务器的缓存使这个问题更加恶化，旧版本要显示一段时间之后才能看到新版本。这个问题的通常解决方案是在源操作中改变影响的所有页面，例如更名目录或在数据库中实现改变。此外，一定要保证提供缓存的相应提示。

11.4.4 分阶段与测试

当然，并不是所有站点都需要连续更新。如果不经常发生改变，则可以在“阶段”系统中完成所有改变之后再对生产系统进行修改。阶段系统的内容可以经过全面测试之后再提供给生产站点。

内容测试

如果站点内容是HTML，则可以检查HTML的语法正确性。例如，每个标志应有相应的结束标志，相应嵌套和许可的标志（因为有些公司可能有关于HTML样式的政策）。这些检查对手工编写的HTML特别重要。有些情况下，可以（和应该）用自动化工具准备不同浏览器显示的内容版本和低速网络访问用户的纯文本视图。

链接测试

最让Web用户失望的是过时和连不上的超链接文本。站点内部的链接很容易管理，但应该测试其一致性。其他站点的链接应该定期测试，保证走在客户之前发现问题。有些Web发表环境（如Microsoft的Active Server Pages）提供了按构造建立正确链接的机制，只在浏览页面时才生成和插入链接。

商务测试

如果站点要支持商务，则分阶段是检查所有项目正确启用的好时候，包括价格是否准确，销售税是否分类，等等。此外，要测试事务运行情况，保证物理商品和数字商品的履行，所有报告正确生成。

检索

如果站点用全文查找引擎帮助用户漫游，则放弃页面要从索引中删除，新的或改变的页面要加进去，最好让生产索引与生产页面完全相符。④

编辑检查

由于阶段显示表示完全可行的专用版 Web 站点，因此可以对内容进行任何最终人工编辑检查。

11.4.5 存档

至少要保存站点的一个旧版本，用一个过程迅速将存档版变成生产版。

- 存档建立改变的审核记录。
- 各个文档（或整个站点）的存档拷贝可能属于站点的一部分，对用户有一些价值。
- 如果生产内容版受到损坏或故意破坏，则可以使用存档版本。存档版本可以转为生产版，提供了从这类问题迅速恢复的方法。

11.5 多媒体表示

Web 内容绝大多数是 HTML，但其他数据类型使用也很广泛。HTML 中的超文本链接可以连接各种数据类型。Web 服务器返回页面时，超文本传输协议头将数据类型信息传递给浏览器。浏览器内置支持许多数据类型，可以接受插入件扩展，处理其他数据类型，还可以启动完全独立应用程序，处理另一些数据类型。

- 内置

  常见浏览器自然支持 HTML 和 GIF 与 JPEG 之类的图形格式。
- 插入件

  Adobe 系统公司提供 Acrobat 格式文件的自由分发阅读程序。安装这个阅读程序时，其插入浏览器中，支持 Acrobat 数据类型。用户单击 Acrobat 文档时，阅读程序插入件取代浏览器窗口，现场显示文档。
- 独立应用程序

  Web 文档产品目录可以包含 Microsoft Powerpoint 演示。用户单击相关链接时，启动用户的 Powerpoint 拷贝，处理这个文件。

---

④一个相关问题是 AltaVista、Lycos 或 Excite 之类的中央搜索引擎可能搜索和检索站点内容。这些大型搜索引擎只在一定时候才轮询各个站点，可能过时。

下面是一些广泛使用的数据类型。

- 动画图形
  有些图形格式（如GIF）能够顺序显示一系列包装在一起的图形，常用于生成小动画。
- 小程序与脚本
  小程序与脚本可以生成动画效果和其他交互式行为，动态HTML也有类似功能。
- 视频数据
  视频数据可以用MPEG、QuickTime和AVI之类的标准编码类型集成到其他Web内容中。到目前为止，大多数视频数据都是作为下载片断在本地播放，但随着网络带宽的提高，流式视频⑤将越来越普及。
- 声频数据
  声频数据可以用WAV文件、SND文件和上述AVI文件放进Web中。此外，RealAudio之类的协议可以使用流式声频（Internet中还有活跃的交互式双向视频，可以替代或补充电话服务）。
- Shockwave
  Shockwave文件是完整的多媒体动画，是著名的Macromedia Director动画生成工具生成的。
- VRML
  最后，VRML是虚拟实境模型语言，值得一提。VRML格式描述三维虚拟实境。VRML页面实际上是个三维模型，下载到支持VRML的应用程序中，然后可以在本地探索VRML世界。

11.6 因人而异

Internet的一个最有趣的方面是信息生成者可以和信息使用者直接交互，而没有出版商、经销商之类的中介人。从某种程度上，Internet的这个方面使中介行业大受影响，但同时也提供了可增强客户关系的机会。例如，在商家对客户商务中，公司通过价格、便利和服务争夺客户。由于客户对所有公司的网络提供基本公平的访问，因此价格和便利最终会在提供者之间达到均衡。到此时，主要的竞争将是服务与关系，网络提供了改进服务与关系的优秀工具。

与印刷、电视和电台等广播渠道不同，每个Internet用户不是收到相同的内容，而是具有公司联机内容的不同信道。站点不是向所有客户提供相同内容，而可以向每个用户提供个性化内容。

---

⑤流式视频与声频是个复杂的概念。传统声频与视频先下载整个声频与视频文件到客户中，然后启动应用程序进行播放。而流式媒介则先开始下载媒介文件，然后边下载边播放。只要下载超前于播放，就能顺利工作，得到更低的播放锁存。

站点个性化不仅能达到业务功能，而且可以达到商业目的。例如，商家对商家产品目录的用户可能看到不同公司的不同价格，零售站点可以向常客发送个性化电子收据。

站点个性化有三个关键要素：验证用户、建立用户配置和生成定制内容。

11.6.1 验证与标识

站点个性化的第一步是验证用户。在这个情境中，不一定要知道各个用户的真实身份，而只要假设用户的一系列访问表示同一个人，即使其真实身份未知。其他情况下，则一定要正式验证，例如上述业务例子中。在这种应用中，包括下列验证技术。

浏览器 Cookie

用户注册之后，站点可能在用户浏览器中记录一个持久 Cookie。这种方法在今后访问时提供自动注册，但如果用户关闭 Cookie 或从另一计算机上使用服务，则行不通。Cookie 的优点是能够通过站点跟踪用户，甚至标识经常访问但没有显式标识或注册的用户（也可以不用 Cookie 而用其他方法维护会话状态，但具有相似属性）。

一个站点的用户名和口令

一个常用方法是在用户首次访问时通过用户名和口令让用户在站点中注册。后面访问时，提示用户输入用户名和口令后才允许进入站点。但是，这样会增加用户负担，用户在许多不同站点可能有不同账号。结果会造成几个问题。如果用户在多个站点选择相同用户名和口令，则很容易记，但只要攻破口令，所有站点都会暴露。此外，所有这些站点都知道口令，恶意的操作员可以滥用这个知识。另一方面，用户如果对不同站点选择不同用户名和口令，则常常会搞乱。用户失去口令时，就会造成客户服务问题。

委托与中央验证数据库

许多站点可以共享中央验证数据库。客户有一组证明信息，因此很容易记住和保护。联盟站点具有高度安全性，可以共享中央验证数据库成本，可以访问一大组用户。对于 Internet 商务，提供多家公司商务服务的公司还可以提供注册数据库，如 Open Market 公司的 Transact 引擎。中央验证数据库还出现在 America Online 之类的大型联机服务中，联盟站点可以利用中央注册服务。但是，由于没有标准化的 Internet 验证与注册系统，因此公司无法指望从任意 Internet 服务提供者取得用户验证。

个人数字证书

公用密钥数字证书是个数字对象，信任第三方保证用户名与安全密钥之间的关联。用安全密钥设置安全连接时，另一端的服务器可以寻找关联名及其相应的公司。证书到 1997 年才开始普及，人们用起来还不太放心。证书如何用于验证见第 13 章介绍。

11.6.2 配置

系统标识用户之后，可以取得对用户存储的配置。有时，如果配置较小，则站点可以用浏览器 Cookie 的客户端存储配置，而不是存储在数据库中。用户配置可以包含各种信息，下面介绍常见的配置信息。

注册信息

许多 Web 站点都有注册窗体，用户可以填好窗体以访问站点或进行购物。窗体可以收集的信息很多，包括姓名和地址、支付信息（如信用卡号）以及生态分布信息。

用户提供的可选信息

配置可以帮助站点个性化。站点经常请求用户选项信息，以提供更好的服务。例如，可以注册 Amazon.com 站点的所喜欢作者，收到这些作者的新书通知。这类配置是可选的，通常链接到用户的特定利益。

链接信息

提供验证之后，就可以自动生成配置信息。例如，如果验证的用户完成一个商务事务，则用户和事务就链接起来了。可以用相应报表软件在相关用户配置中记录实际或预期购买，以备进行买卖。联机取得的配置和事务信息可以链接到网络之外取得的个人信息。

浏览信息

最后一级细节是可以将站点中的各个浏览模式收集到用户配置中，并收集所输入搜索关键字之类的信息。Web是第一个可以这个精确而详细地跟踪个人活动的媒介，这个信息如何更好地用于个性化，我们还要拭目以待。至少，用户经常访问的区域会在该用户的个性化主页上提供链接。

存储配置

存储配置和维护配置的方法有几种。

- 浏览器 cookie
  前面曾介绍过，cookie 可以存储用户标识信息，用于跟踪会话等。Cookie 还可以直接存储配置信息。好处是站点不需要分配配置存储，站点的 Web 应用程序可以直接取得配置数据，而不必查询数据库。缺点是，如果用户切换计算机（或删除 cookie），则配置信息丢失，站点也无法同时提供所有用户配置信息以进行报表和市场分析。
- 站点本地存储
  用户验证信息可以用于从本地数据库取得配置信息，但如果 Web 站点增长到超过一个地点，则这种方法行不通。

- 共享存储
  共享系统可以存储用户配置信息。例如，事务引擎或验证系统为多个站点服务时，也可以提供具有共享配置信息的公用用户数据库。其好处是信息只要在一个地方更新。
- 浏览器钱包
  配置信息的另一存储地点是浏览器钱包。这个方法没有广泛使用，但今后可能更加普及。浏览器钱包最初是作为存储商务支付证明信息的方法，也可以存储姓名、地址、个人选项等配置信息。这些信息可以发布，在用户同意下或在开放配置标准之类软件控制自动请求 Web 站点。

11.6.3 定制内容

有了用户验证和配置信息之后，最后要解决的问题是如何生成个性化内容。细节需要随不同应用程序而改变，下面试举几个例子。

个人报纸

个人报纸例子站点的目的是提供定制报纸以吸引用户。为了节省用户的时间，把用户需要的信息放在个性化主页中。站点可以通过预订费或广告取得收入。

用户要注册兴趣配置，在注册窗体中包括下列元素：

- 今后注册时使用的用户名和口令。
- E-mail 地址，用于发送个人报纸的 E-mail 版（如果需要）。
- 邮政编码，对用户家乡城市生成定制天气预报。
- 喜欢的体育运动队，用于选择该队的新闻项目，包括最新成绩。
- 感兴趣公司的投票行情，用于收集定制资产组合报告和公司的新闻项目。

用户配置和验证信息存放在 Web 站点的数据库中，用户单击站点时，注册屏幕请求用户登录或注册为新用户。

用户注册之后，Web 应用程序利用用户名从数据库中取得用户的配置。标准主页是个模板，具有天气、体育和商业栏目，但没有具体内容。Web 应用程序利用用户配置中的字段选择相应天气报告、体育成绩和公司模板，并填好模板，将其返回用户。定期批处理作业搜索选择 E-mail/ 选项的用户并查询要传输的个性化 E-mail 消息。

如果站点靠广告支持，则广告商可以从用户配置了解许多东西，如邮政编码。可以用配置信息放上用户更感兴趣的广告。

定制产品目录

定制产品目录例子站点的目标是向中型公司客户发送办公用品。Web 订购系统的用途是让最终用户直接订购，减少订购成本。这个服务向多个客户提供，产品目录要对每个购买单位进

行定制。定制包括返回相应购买公司喜好的订单窗体、一组由合同限定的供应品和一组反映订购量的价格与折扣。个性化还反映个人购买额度。

本例采用 Internet 开放购买（OBI）标准进行设计，销售单位经营产品目录和提供公司级定制，购买单位负责验证请求者和根据个人购买额度授权购买。图 11.3 复制了第 6 章介绍的 OBI 体系结构图。

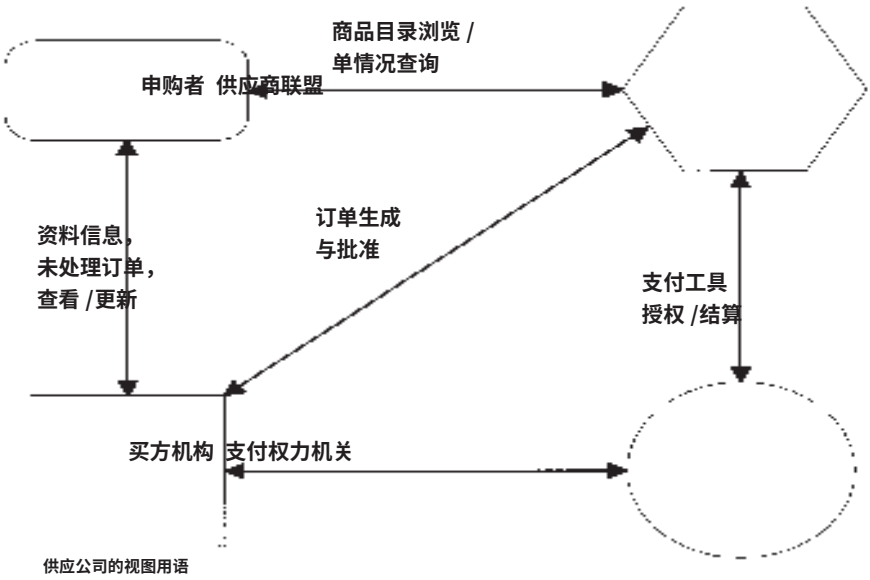


图 11.3 OBI 体系结构图

要生成购买关系，买卖双方要商定服务、包括项目与合同价格。这个信息放在销售者产品目录系统的购买单位配置中。

购买单位生成请求者的数字证书，记录其用户名，并由购买部门签名。

请求者进入销售者的产品目录时，站点用数字证书中的信息选择相应折扣、价格表、可供项目和购买者的适当订单窗体。订单完成之后，产品目录站点将订单路由到购买者的批准系统，并提供证书中的用户名。

购买者的批准系统用证书中的用户名选择正确的购买额度。如果批准订单，则订单和正确发货地址一起路由回销售者。

本例中，配置信息分布在买方与卖方系统中。这种分隔对这个应用程序是合适的，因为同一请求者可能向多个供应商购买，不需要将同一配置信息存放在多个地方。

销售规划

销售规划例子站点的目的是提供优惠券和特供品，吸引回头客，吸引通信流。为了尽可能顺畅，没有注册与登录要求。

对这个系统，验证是用存储惟一 ID 号的浏览器 cookie 完成的。如果浏览器第一次访问这个站点，则没有 cookie，因此分配新的 ID 号并存储为 cookie。ID 号的目的是识别重复访问者和随着时间的改变而调整站点行为。

最初，用户配置是空的，站点主页显示一般化特供品。但如果访问者进行购买，则 ID 号链接用户配置（特别是邮政编码）和事务记录。

邮政编码根据用户的特点选择相应特殊供应品，这已经是一个常见做法。第一次事务之后，用户访问这个站点时，主页显示用户更可能感兴趣的特供品。

站点的订单窗体也允许用户输入可选 E-mail 地址，以便在发货延迟或有任何特供品时告诉用户。用一个通知表示站点不会向别人提供地址和 E-mail 信息，保证用户隐私。

每周的批处理作业用可用配置和事务信息偶尔向注册了 E-mail 地址的用户发送电子优惠券。电子优惠券是个 URL，将用户吸引回站点。

小结

个性化内容依赖于标识与验证用户，存储相应配置信息和允许根据配置动态构造内容的站点体系结构。定制内容是站点与客户密切关系的重要机制，可以帮助公司在价格、便利等其他竞争因素相同的环境中建立竞争地位。

11.7 集成其他媒介

随着 Internet 与日常生成的关系越来越密切，其他媒介将有更多机会链接到 Web 中，用于商务目的。Internet 的 4 个重要特征使这个机会激动人心。

- 容量。除了一定的存储费用之外，Web 内容的边界成本实际为 0。产品信息可以既多又细。
- 新颖性。Internet 内容可以保持更新，产品目录、价格、库存和财务与规定信息都随时改变。
- 事务。在其他媒介中，广告吹嘘人们采用电话买卖，而在 Internet 中，事务就在那里。
- 带宽。Internet 带宽很大，而且不断增大，但不是无限的。个人通常用 28.8kb/s 或更慢的 modem 通过拨号电话线访问网络。此外，大多数便携电脑用户在旅行时从网络切断，无法立即访问网络。但许多用户可以用高速公司局域网、56 kb/s modems、ISDN 电缆 modems 或卫星链接访问网络。

记住这些因素之后，几种跨媒介集成显得特别重要。

11.7.1 广告中的URL

在传统印刷与广播媒介中，空间很宝贵，每平方厘米的印刷广告和每分钟的广播广告都要付钱。而在无所不在的 Internet 访问中，印刷与广播广告只要集中在品牌标识，链接联机资源中的详细产品信息。已经有大量电视与杂志广告中包括URL，可以将这些媒介链接到Web。

11.7.2 光盘与DVD

光盘已经广泛用于发布应用程序、产品目录和参考信息。光盘的优点是容量和带宽表，在网络切断时也能使用。光盘缺乏新鲜感和事务功能，但通过本地光盘加上集成网络访问，应用程序既得到光盘容量和带宽，又得到 Internet 的新鲜感和事务功能。可以从网络上拉光盘更新内容或网络向客户系统推更新内容，光盘发布的应用程序可以方便地链接 Internet 上的事务和信息系统。数字视频盘（DVD）与光盘相似，但具有更大的容量。

11.7.3 E-mail与Web

E-mail是 Internet 用户熟悉的媒介，但只是最近才与万维网集成起来。新一代E-mail客户可以用HTML格式显示大多数消息，可以从E-mail消息中的URL激活Web浏览器。这些功能使E-mail可以方便地和客户通信，发布特供品和优惠券。接收者可以方便地存储和转发这些消息，以及立即转入交互式或事务性Web站点。

11.8 小结

Internet和其他通信媒介一样，生成与管理有吸引力和易于使用的内容至关重要。但是，对任何新媒介，都可以看到新功能、新工具和新限制。Web提供了集成多种媒介的强大机制，提供高于细节的用户经历。此外，可以针对各个客户的个人兴趣和特征定制表示方法，这是任何其他媒介都无法比拟的。

关于 Internet 与Web的讨论主要集中在技术方面，但真正吸引客户的东西是内容。需要利用技术，但更要注意内容。

第 12 章　加密法

他们的一切用心，皇上全知道了。
那些信件已落在咱们的手中，他们可是连做梦也想不到的。
——亨利五世

12.1 保密

加密法是从希腊语“ 密写 ”衍生出来的词汇，是在非可信任信道上进行通信的科学。历史上，加密法与间谍、政府和军队相联系，已经在战争中使用几千年，最著名的例子是第二次世界大战时德国的 Enigma 机器。但是，近 50 年来，加密法建立了良好的数学模型和实务基础，从军事工具和学术研究转入了商务应用。

如果正确运行，则加密法可以使消息保密，积极标识发送者和向接收者保证消息中途未被修改。有时，加密技术可以证明消息来自哪里，是谁发的。

例如，试对电子商务问题采用加密法的这些属性：Alice 是个购买代理，要从供应商 Bob 那里订购一些物品。这个事务有什么要求呢？

- Alice 要保证对方是 Bob 而不是假冒者（验证）。
- Bob 要保证对方是 Alice 而不是假冒者（验证），因为 Alice 已经在合同中商定了特殊价格。
- Alice 要让订单保密，Bob 也不想让别的客户看到 Alice 的特殊价格（隐私）。
- Alice 和 Bob 都要保证黑客不会改变价格或数量（完整性）。
- Bob 要保证 Alice 后面不会否认这个订单（非否认）

这是 Alice 和 Bob 在通信中需要的一些属性，加密技术可以提供这些属性。后面介绍每个部分时，都会回到 Alice 和 Bob 的例子。表 12.1 提供了这些属性的细节。

表 12.1 加密法提供的功能

隐私	消息保密：只有发送方和接收方知道消息内容。
验证	接收方知道消息不是假冒的，而是由特定发送者发来的。发送方知道消息会到达正确的接收方。
完整性	接收方知道消息中途未被修改（有意或无意）。
非否认	消息作者后面不会否认发过这个消息。

本章要介绍公用与专用密钥加密法的一些基本原理，然后介绍如何用这些技术生成安全通信信道、数字签名和其他解决方案，最后要介绍密钥管理，这是加密的关键。

12.2 加密类型

在加密法中，普通消息（明文）通过加密算法进行处理，生成加密消息（密文）。接收方用解密算法将密文变成明文。如果每个人都知道这些算法，则不会有安全性，因为任何人都可以解密密文。因此，除了算法之后，还有另一个输入数据，称为密钥。密钥是个秘密，而算法则是许多人都知道的。这与锁的原理是一样的，许多人用的锁原理是相同的，但每个人选择不同的组合。锁的组合相当于加密算法中的密钥。

加密算法有两种基本类型：专用密钥系统（也称为对称）和公用密钥系统（也称为非对称）。在专用密钥加密法中，解密和加密使用相同的密钥（即密钥是对称的），而在公用密钥加密法中，解密和加密使用不同的密钥（即密钥是非对称的）。可以看出，两个密钥中一个是可以发表的，是公用的，公用密钥加密法正是由此得名的；另一个是秘密的，称为专用密钥，专用密钥系统已经出现几百年；而公用密钥系统则是70年代中期才出现的。这两种系统都允许秘密通信，但公用密钥系统很容易增长到全球范围，方便地让没有联盟的人们安全地通信。公用密钥系统还可以提供数字签名，相当于人们在信函、合同和其他文档上的手工签名。本章稍后将详细介绍数字签名。

实际中，加密系统通常是专用密钥和公用密钥加密法一起使用。专用密钥算法通常比公用密钥算法更快，因此用专用密钥算法加密实际数据会更有效。系统对对称算法生成随机密钥，然后用公用密钥算法加密这个密钥。接收方首先用公用密钥算法解密对称密钥，然后用这个密钥解密数据。

12.2.1 算法、协议与密钥管理

实际系统的加密法中有三个主要组件：加密系统、协议与密钥管理。加密系统指加密算法及其特征。协议指构成加密算法及在实际问题中采用的方法，如加密通信信道或数据库信息。最后，密钥管理指生成、分发与存储密钥。

加密系统的设计与分析是相当专业化的，因此这里只是简要介绍与目前商务有关的系统。协议对电子商务非常重要，用于保护内容与信息和支付系统。最后，在不利的环境中保证实际安全性最为重要的是寓钥管理。

我们首先介绍如何看待使用加密法的系统的安全性，然后介绍算法、协议与密钥管理。

12.3 如何评估加密法

使用加密法的系统的操作安全性是由所用加密算法的安全性、加密协议的正确设计和正确的密钥管理决定的。

- 算法
  加密系统的设计与分析是相当专业化的，因此不必亲自动手。现有的著名算法已经提供了你所需要的特性，已经足够你使用了。由于加密法仍处于快速发展之中，因此设计时应留有余地，随时准备在系统中替换加密算法。如果选择的算法可以使用不同密钥长度，则应准备改变长度，通常是使用更长的密钥。有人可能声称新的加密算法具有更好的安全性、更好的性能和其他优点。但是，使用这些算法可能是危险的，因为你无法判断它有多好。坚持用著名的算法好像很乏味，但比较安全。
- 协议
  加密协议的设计似乎比算法方便一些，但即使最简单的协议也可能有大量微妙的缺陷。不要亲自设计，应尽可能用现有协议（如果没有，则应尽量找一个可行的协议）。和算法一样，使用模块化组件可以随时方便地引入新协议。这在旧协议中发现弱点时特别有用（这是可能的事）。
- 密钥管理
  密钥管理是加密法中最困难的部分，也是人们读得最少的部分。密钥管理包括生成、分发与存储密钥和更新密钥。由于现代加密协议和算法非常强大，因此密钥管理系统很容易成为攻击的目标。评估安全通信系统时，一定要询问内置密钥生成、存储与分配机制如何工作。但是，有时这是系统用户自己的事，只能自己设计和实现。

12.3.1 加密法强度

看待加密系统安全性的正确方法是密钥包装系统的整个安全性，以及采用足够强的算法。具体地说，任何依赖于算法保密的系统都是可疑的，经得起加密分析师多年检验的公开算法要可靠得多。

那么，如何测定系统的强度呢？首先，假设算法本身是公开的。第二，假设敌人能够访问系统，因此能够提交明文和取得相应密文，用当前密钥加密（称为选择明文攻击）。这样，敌人除了不知道密钥之外，什么都知道了。如果敌人除了试验每种可能的密钥之外仍然没别的办法解密你的消息，则是个好系统。

要攻击加密系统，一种方法就是试验每种可能的密钥，这个过程称为穷举搜索或强力攻击。强力攻击是无法阻止的，但如果可能的密钥数太多，则强力攻击成本太高，行不通。

如果攻击系统需要试验每种可能的密钥，则需要有足够的密钥才能使这个工作在计算上可

行。密钥长度用位测量。例如，数据加密标准（DES）是美国政府指定的，是56位密钥。对于n位的密钥，有2^n种可能的密钥，每增加一位，密钥取值就多一倍。例如，56位密钥的DES有2^{56}种密钥数，即72 100 000 000 000 000种不同密钥。这个数字好像很大，但其实不然。数字设备公司的研究小组建立了每秒进行16 000 000次DES运算的芯片。如果机器中有一千个这种芯片，则不到八个星期就可以攻破DES加密的消息。1997年6月17日，Rocke Verser领导的小组调动Internet上的78 000台计算机，在几个月的时间内攻破了DES加密的消息。

这种工作是一般黑客做不了的，但犯罪集团和一个国家的代码破译组织完全能够做到。

更令人不放心的是，计算机性能在成本不变的情况下，每18个月翻一番。这个技术趋势也称为摩尔定律，已经印证了30年，而且没有停止的迹象。到2010年，机器及其组件至少要比1996年快100倍。更可怕的是，纳米技术和生物技术使海量并行代码破译技术可能在将来某个时候出现。

幸而，随着代码强度改进成本的增加，攻击密码的计算成本呈指数级增加。

1997年1年，RSA实验室推出了RSA专用密钥挑战，这是一系列对称密钥加密竞赛。第一个挑战攻破RC5算法的40位密钥版本，不到3个半小时就成功了。RC5的48位版本花掉了313小时，而DES花掉了140天。RC5的密钥长度可变，一些较难的挑战还没有解开。

12.4 操作选择

除了协议与算法之外，首先要选择系统的加密强度（选择算法与密钥长度）和一些密钥管理问题。最重要的元素是选择足够长的真正随机密钥，将这些密钥保密，并经常改变密钥。

这一切都要求选择好的加密系统，系统的所有安全性都依赖于密钥，而不是依赖于算法本身。

稍后将介绍密钥随机性和密钥保密性，但首先要考虑密钥长度和密钥更新频率。

12.4.1 密钥长度

对于一定强度的算法，数据的保护程度主要取决于加密密钥的长度。基本说来，加密消息应在信息的有用寿命之内保持秘密。在很大程度上，加密消息中信息的价值控制了攻击所用的资源。例如，敌人不会花100万美元去取得只值1000美元的信息，但可能花100万美元去取得值200万美元的信息。下面举一些例子。

- 财务信息在有效期之外仍然要保密。
- 合同标的在合同期之外仍然要保密。
- 编辑材料在发表之前要保密。
- 秘密个人信息在此人去世后仍然要保密。

当前，一个常见建议是目前安全性至少要用 75 位密钥，70 年安全性至少要用 90 位密钥。这些数字适用于 DES、IDEA 与 RC4 之类的对称加密系统。当前公用密钥系统可以用分解因子之类的快捷攻击，因此不需要试验所有密钥。对于这些系统，密钥要更长，例如 RSA 密钥应有 268 位或 1 024 位。

12.4.2 密钥寿命

密钥不能一直使用，而应经常更新。正确的密钥寿命是所加密项目价值、所加密项目数和所加密项目寿命的函数。前面已经介绍过寿命。如果用适当设备可以在两年内攻破密钥，而用这个密钥加密的信息只有 6 个月的寿命，则密钥至少每 18 个月更新一次，使敌人解开第一个加密项目时，最后一个加密项目已经失去价值。

所加密项目数有两方面的意义。第一，如果每个加密项目有市值，则要计算所有加密项目的总值，比较敌人攻击时可能投入的资源。第二，有些加密系统在具有大块密文时能够受到更方便地攻击。这个工作更难量化，但最好不要把一个密钥使用太长时间。

另一个缩短密钥寿命的因素是多疑症。密钥使用时间越长，越可能有人已经攻破密钥存储系统，直接取得密钥，而不是利用强力攻击。

一定要注意，改变密钥并不改变敌人用强力攻击（或其他密码攻击）找到密钥的时间。但改变密钥可以在特定密钥暴露时限制暴露的信息量。例如，如果每个月改变加密密钥，则密钥暴露时，只会暴露一个月的信息。

12.5 一次性板

有没有完美的加密系统呢？有，就是一次性板。最初的方案是在纸板中填入完全随机的字符，建立两个副本，将一份交给对方。要发送消息，就要将其一个字母一个字母写到板上，只要加上字母对，A=1，B=2，等等，Z 之后又回到 A。得到的字母序列是个密文。对方逆转这个过程，从消息中每个字母减去板上的相应字母，从而得到明文。用完纸板之后，将其销毁。如果纸板包含真正完全随机的字符，则这种方案绝对安全。敌人不知道纸板上的内容，只能靠猜；但不知道何时猜对了。只要改变猜测，敌人就可以将密文译码成任何消息，可以是“凌晨出击”，也可以是“误判投降”。

完全随机的字符提供了完美的安全性，可以在需要完美的加密系统时使用。但这个系统有许多缺点。

- 纸板要真正随机。任何的结构化都可以帮助破译系统，要生成完全随机的字符是很难的，生成大量完全随机的字符则更难。
- 纸板不能复用。如果复用，则可以比较用相同页加密的两段明文，从而可能一起暴露由于发完消息之后就要浪费纸板，因此纸板要很长或经常更换。

- 纸板的分布和存储要绝对安全。由于无法成功地攻击密文，因此敌人会复制或替换纸板以进行攻击。
- 每对收发都要用惟一纸板，使纸板的分发非常困难。

这些实际困难大大限制了一次性板的使用，只适用于不计成本的情形。对大多数其他情形，加密系统使用定长密钥，可以通过穷举搜索而攻破。

12.6 专用密钥（对称）加密法

对称加密系统如图12.1所示，消息（或明文）用密钥加密，得到的密文发送给接收方，然后接收方用相同的密钥将消息解密。注意双方要知道相同的密钥。最著名的专用密钥（对称）加密法是DES（数据加密标准）。表12.2显示了专用密钥（对称）加密法如何达到隐私、验证、完整性与非否定。

假设Bob与Alice要用专用密钥（对称）加密法进行通信。首先要确定密钥，只有他们知道，且要完全保密。Bob与Alice有了相同密钥之后，每一方都可以向对方发送加密消息。验证是有保证的，因为双方都能肯定只有对方知道这个密钥。消息到达时，只能来自对方。消息完整性也有保证，具有消息摘要或消息完整性代码放在消息中。

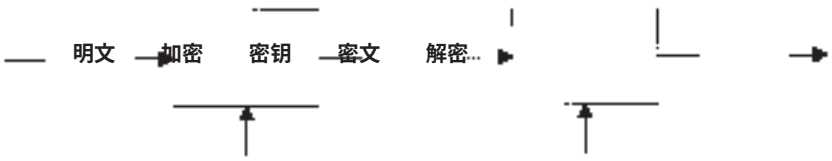


图 12.1 对称加密系统

12.6.1 块与流加密法

块加密算法取一个定长明文块（如64位），用密钥加密成定长密文块。流加密法则用密钥产生伪随机密钥流，然后通常与明文进行异或运算[①]得到密文。这两个方法都有一些缺乏。由于块加密法的每个块是独立的，因此窥视者可能注意到某些密文块的重复性，知道对应明文块也是重复的。只要简单运用流加密法，则密钥流对每个新消息重复，很容易分析。为了解决这些问题，可以使用初始化向量（IV）。对于块加密法，IV添加到消息前面并加密，然后第一个密文块与第二个明文块进行异或运算，然后依次类推。这种方法称为加密块链。每个消息的初始化向量不同。而对于流加密法，初始化向量的用法是不同的。这时，初始化向量和密钥用于

①异或运算在只有一个操作数为1时得到1。

初始化密钥流生成器，使其对每个消息生成不同序列。初始化向量本身在密文开始之前以明文形式发送。

表 12.2 专用密钥加密法提供的功能

隐私	只有知道密钥的人才能加密或解密消息。
验证	如果每对通信方使用不同密钥，则消息接收者可以保证发送者的身份。发送者知道只有接收者才能将消息解密。
完整性	对称加密不提供消息完整性，但可以在消息中增加消息完整性代码（MIC）。MIC是消息摘要与专用密钥的组合。
非否定	对称加密不提供非否定，因为发送方与接收方都可以生成消息。

12.6.2 专用密钥加密系统

这里不准备列出所有专用密钥加密系统，只是列出最有趣和最有商务意义的系统。

- DES
  DES（数据加密标准）是个块加密法，用56位密钥将64位明文块加密成64位密文。DES由FIPS 46定义，是1976年11月发表的。DES最常见的操作方式称为加密块链（CBC），在这种操作方式中，每个密文输出块与下一个输入块进行异或运算，形成DES算法的下一输入。这个过程从64位初始化向量开始，如果没有加密块链，则敌人可以替换各个密文块，从而干扰通信。由于8位数据的8字符块（如ASCII）自然适合64位边界，因此密码分析师可以确定块重复部分，从而了解明文模式。
  DES已经使用20多年，尽管经受了密码分析师的严峻考验，但56位密钥长度显得太小了（事实上，逆转密钥与明文就可以逆转密文，使有效密钥长度减少到55）。
- Triple DES
  DES的新变形称为Triple DES或3DES，用三个56位DES密钥加密每个块。在Triple DES加密运算中，数据块用第一个密钥加密，用第二个密钥解密②，然后再次用第三个密钥加密。中间的操作是解密，因此如果三个密钥相同，则Triple DES退化为普通DES。在三密钥方式中，Triple DES要求168位密钥。
- IDEA
  IDEA（国际数据加密算法）是Lai与Massey开发的块加密法，是1990年推出的。IDEA用128位密钥加密64位块。IDEA在旧版极好隐私（PGP）系统中广泛用作批量加密方法。
- RC4
  RC4是Ron Rivest为RSA数据安全公司设计的变长度流加密法。RC4在Internet中广泛

② “用第二个密钥解密”指的是在解密方式中用这个密钥运行DES算法。显然，用第二个密钥解密不是得到明文，因为用的是不同密钥。

用作安全套接层协议中的批量加密方法，密钥长度为40到128位。尽管RC4是RSA DSI的专用加密法，不符合公开分析加密法的原则，但1995年，有人在Internet上建立了复制RC4算法的源程序，因此引起更广泛的研究。

- Blowfish

  Blowfish是Counterpane系统公司的Bruce Schneier设计的变长密钥块加密法。Blowfish免费提供，非常快，在Intel Pentium处理器上比DES实现方法快将近三倍。Blowfish广泛用于PC文件加密应用、安全隧道应用等等。密钥长度为32到448位，适合各种安全应用（见http://www.counterpane.com/blowfish.html）。

- CAST

  CAST是Entrust技术公司的Carlisle Adams与Stafford Tavares设计的变长密钥块加密法。密钥长度为40到128位。CAST是极好隐私（PGP）系统中的标准批量加密方法。1997年1月，Entrust公司发布了商业与非商业应用中负责使用的CAST版本。

12.7 公用密钥（非对称）加密法

非对称加密系统如图12.2，加密密钥与解密密钥是不同的。技术上，公用密钥系统的每个参加者建立自己的密钥对，然后将专用密钥保密起来，不发布给任何人，而将公用密钥随意分发出去。这两个密钥都可以用于加密或解密，但最主要的是要把专用密钥保密起来。著名的公用密钥（非对称）加密法是RSA，是用发明者Rivest、Shamir、Adleman的缩写命名的。以保险柜为例，公用密钥系统就像是顶上开口的保险柜，任何人都可以往里投东西，但只有一个人能取出其中的东西。

表12.3显示了公用密钥系统如何达到隐私、验证、完整性和非否认。

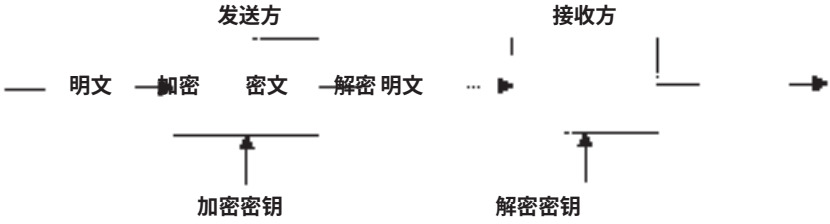


图12.2 非对称加密系统

表12.3 公用密钥系统提供的功能

隐私	消息用接收方的公用密钥加密，只有接收方的专用密钥才能将消息解密。
验证	接收方验证消息发送者时，可以验证数字签名，这是用发送方专用密钥加密的消息摘要。
完整性	消息的数字签名提供消息完整性。消息摘要用发送方专用密钥加密。
非否认	可以用数字签名提供非否认功能。但时间一长之后，可能争论签名是否与消息同时生成的。为此，可以使用数字时间标志服务。

12.7.1 公用密钥系统举例

假设 Bob 与 Alice 要用公用密钥系统进行通信。首先，Bob 与 Alice 各生成一个密钥对，分别为公用密钥和专用密钥。然后 Bob 与 Alice 在城市目录中发布自己的公用密钥。

现在假设 Bob 要向 Alice 发送消息 M，则可用 Alice 的公用密钥将消息加密。密文只有 Alice 能解开，因为只有她知道自己的专用密钥。Alice 用自己的专用密钥将消息解密，获得原先的消息。

这种机制中第一个问题是任何人都可以发消息。由于Alice的公用密钥在公开目录中发表，因此任何人都可以向她发消息。如果消息中写道，“午夜在凉亭中见——Bob”，Alice 怎么知道消息是 Bob 发的还是 Alice 的父亲用来试她的？要回答这个问题，可以用验证，就是 Bob 对消息进行数字签名。假设 Bob 用自己的专用密钥加密消息 M，生成签名消息了，则任何人都可以用 Bob 的公用密钥解密这个消息，因此不是秘密。但只有 Bob 能够发送，因为只有 Bob 知道自己的专用密钥。

Bob 与 Alice 问题的解决方法是组合这两个方法，发送秘密的验证消息。Bob 首先用自己的专用密钥将消息签名，然后用 Alice 的公用密钥将消息加密。只有 Alice 能解密这个消息，解密之后，可以验证是 Bob 发送的。

公用密钥加密法的下一个问题是公用密钥的验证。Bob 向 Alice 发消息时，他要到目录中查找 Alice 的公用密钥。假设 Alice 的父亲在目录中换上自己的公用密钥，则 Bob 发送消息时，用的并不是 Alice 的公用密钥，而是她父亲的公用密钥。如果 Alice 的父亲很聪明，则他可以解密消息，然后用 Alice 的真正公用密钥将消息重新加密。这样，Alice 并不知道消息被偷看过，除非她到目录中检查自己的姓名与密钥是否对应。

要解决密钥目录的安全问题，可以用公用密钥证书。公用密钥证书是一个文档，包含用户名和对应公用密钥，是由信任证书机构签名的。假设市政文员是个证书机构，Alice 首次生成自己的公用密钥时，亲自到文员那里，用一个文档证明公用密钥是她自己的公用密钥，得到的签名文档是个公用密钥证书。任何人都可以用文员的公用密钥检查签名，从而验证其有效性。当然，文员的公用密钥不能被篡改。Alice 有了证书之后，就可以将其放在目录中，Bob 可以保证所用的密钥真是 Alice 的公用密钥。

证书机构和 DNS 一样，通常组成层次式结构，使管理员可以分配证书签发过程。要建立层次，高层证书机构向低层证书机构签名证书。层次中最顶层的证书机构称为根，它的公用密钥称为根密钥。

12.7.2 公用密钥加密系统

本节介绍 RSA 和椭圆曲线公用密钥加密系统。

RSA

最主要的公用密钥加密系统是Rivest、Shamir、Adleman。RSA的安全性基于大数很难分解因子。RSA公用密钥是模 n 和随机加密密钥 e，对应的解密密钥 d 保密。密钥e和d是随机选择的，但这些数之间的关系为 $ed=1 \bmod (p-1)(q-1)$，其中 p 和 q 为质数，$n=pq$。

RSA加密的数学运算公式如下：

$$c = m^e \bmod n$$

其中 m 为消息，c 为密文，e 为加密密钥，n 为模，解密公式为：

$$m = c^d \bmod n$$

关于RSA算法要注意几点。

- p 和 q 应为质数，并避免某些“弱”形式。
- 特别选择的 p 和 q 不能用于多个 e 与 d，否则密码很容易攻破。
- RSA是块加密法，块长为模 n 的长度。要加密的信息应比这个块短，否则消息应分解为多个块。
- 消息不能太短。如果 m^e 小于 n，或只循环几次，则消息很容易破译。
- 单块消息有几种格式化规则，使密码分析更困难。

使用RSA加密法的最佳信息源是RSA数据安全公司发表的《Public-Key Cryptography Standards(PKCS)》系列标准。

前面曾介绍过，除了上述注意事项之外，RSA的安全性取决于分解因子问题的难度。如果（公用）模n可以分解为因子 p 和 q，则可以恢复专用密钥 d。近年来，分解因子方面有了很大的进展，当前最好的算法是通用数字字段筛分（GNFS）和专用数字字段筛分（SNFS），只适用于特殊形式的数字。表12.4显示了RSA中常用长度的因子数的估计计算量，一般来说，RSA模应当比对称加密系统密钥长10倍，才能得到相同的安全性。随着分解因子算法的改进，“10倍”这个数是（向下）改变的。

表12.4 同正分解所需的计算能力（MIPS年） ③

数长（位）	随机整数（使用GNFS）	特殊整数（使用SNFS）
512	3×10^4	1×10^5
768	2×10^8	3×10^7
1024	3×10^{11}	3×10^7
1280	1×10^{14}	3×10^9
1536	3×10^{16}	2×10^{11}
2048	3×10^{20}	4×10^{14}

③见Andrew Odlyzko, AT&T, RSA Cryptographer会议，1996年9月。

椭圆曲线

基于椭圆曲线算法的加密系统已经推出，这个系统其于离散对数问题的难度，而不是分解因子的难度。由于离散对数问题难以解决，因此椭圆曲线系统可以用比基于因子分解算法更短的密钥达到一定的安全性。ANSI X9、ISO/IEC和IEEE等组织正在进行椭圆曲线系统方面的标准化工作。

椭圆曲线系统的主要难点在于它们是新东西，还没有像DES与RSA那样经过考验，但是，加密领域普遍认为椭圆曲线系统是后起之秀。

12.8 协议

协议就是完成一个任务所采取的一系列步骤。事实上，算法也是这样定义的，但算法处理的是内部数学结果，如加密一个块；而协议处理的是用户看到的结果，如秘密通信或数字签名。

12.8.1 通信

显然，前面对秘密和公用密钥加密系统的介绍大部分都是在通信中的应用，但加密方法在通信中的完整应用还要解决一些除简单加密与解密块的问题。

- 会话密钥

  会话密钥是特定通信会话期间对特定消息采用的加密密钥。使用会话密钥有两个目的：得到性能好处和限制用主密钥加密的信息量。通常，通信系统只用性能较差的公用密钥加密系统交流会话密钥，然后用性能较高的对称密钥加密大批消息数据。使用会话密钥的另一个原因是限制主密钥的密钥分析者可以取得的信息量。由于主密钥只加密随机会话密钥，因此敌人无法通过分析实际消息的任何统计属性而帮助攻击主密钥。
- 消息完整性

  敌人可以在发送者与接收者之间的通信信道上改变或替换不同密文。因此，必需保证收到的消息与发送的消息相同。有时收到的消息译码成文理不通的内容，因此显然作了修改，但计算机判断文理不通的内容的能力很差。要解决这个问题，可以在加密之前在明文中加进消息摘要，或在密文中包括消息完整性检查或数字签名。
- 防止重播

  敌人可能录制整个消息然后重播，如果不能探测和放弃重复消息，则敌人可能大干坏事。例如，如果能重播包含信用卡支付指令的加密订单，则敌人可以使卖方的货物卖光或让买方透支。

  重复消息也可能偶尔出现，例如，如果传输期间通信信道脱机，则发送方可以重发最

新消息。但先前的消息是丢失了或只是一个确认。

- 数据压缩

  数据压缩与加密是不同的，但可以通过正确的方法结合起来。数据压缩指用最少的空间编码消息。为此，ZIP与COMPRESS之类的数据压缩算法探索源文件的统计属性，用更少的位编码相同信息。然而加密则需要删除数据压缩要利用的统计属性，因此通常不可能压缩加密消息。但是，可以加密压缩消息。

这个奇怪的属性有两个直接效果。第一，modem靠数据压缩达到高位速率，对加密材料要慢得多。第二，Stacker与Doublespace之类的压缩文件系统无法在使用加密文件时节省任何空间。

先压缩后加密可以提高安全性，因为压缩能减少冗余度，而密码分析师可能利用明文的冗余度。这里一定要注意，加密文件是无法压缩的。

第13章将介绍Internet中使用的一些安全通信协议。

12.8.2 消息摘要与散列函数

散列函数也称为单向函数，取可变长度消息并将其缩成固定长度，如128位或160位，结果称为消息摘要或消息散列。散列函数是数字签名和消息验证码的重要元素。生成数字签名时，不是用一个专用密钥加密整个消息，而是加密消息散列。这样，生成的签名长度是较短的固定长度，与消息长度无关。好的散列函数有这样的属性，对于特定散列（散列函数的输出），不可能猜出生成散列的消息。此外，不可能方便地找到两个具有相同散列的消息。

下面是一些常用散列函数：

- MD5

  MD5（MD指消息摘要）是Ron Rivest设计的公开域算法，接受512位倍数长度的消息，得到128位输出。一些最新结果发现了MD5变体中的弱点，因此应尽可能选择其他散列函数。到目前为止，这种攻击还没有针对MD5消息验证码，因此MD5 MAC算法还是可以接受的。其他最新工作已经开始质疑几乎任何128位散列算法，因此新系统设计应选择输出至少160位结果的算法。

- SHA-1

  SHA-1（安全散列算法）是美国国家标准与技术协会（NIST）开发的，得到了美国国家安全局的帮助，接受512位倍数长度的消息，得到160位输出。

- RIPEMD-160

  RIPEMD（RALE完整性要素评估消息摘要）是欧盟的高级计算技术研究与开发组织开发的16位散列算法。

- MDC-2与MDC-4

MDC-2与MDC-4散列算法使用DES块加密。MDC-2是IDM公司设计的，在ANSI X9.31中指定，用于财务安全应用程序。MDC-4用四个64位输入数据块DES加密得到128位输出。

SHA-1与RIPEMD-160即将成为ISO标准。

12.8.3 消息验证码

在通信中，消息通常用校验和循环冗余校验或错误纠正码以防止意外损坏。发送者用消息计算校验和，然后将消息和校验和一起发给接收方。接收方用收到的消息计算校验和，然后将收到的校验和与算出的校验和比较，如果不同，则说明发生了传输错误。校验和算法保证所有错误涉及的位数比探测的位数少，可以探测所有其他概率较高的错误。

消息验证码（MAC）的作用也很相似，保护消息完整性，防止故意和无意篡改。MAC算法用消息和专用密钥（不随消息一起传输）作为输入，生成定长输出。MAC用散列函数构造。敌人知道消息，但不知道密钥，因此无法重复这个计算。消息验证码也称为消息完整性码(MIC)，因为可以用专用密钥保证消息有效性和完整性。

早期MAC算法只是将密钥与数据结合，进行散列和组合。这种简单方法具有加密脆弱性，因此最近的工作主要集中在建立更强的算法上。MAC算法的一个例子是HMAC，可以处理几乎任何散列算法，常用于MD5或SHA-1。

HMAC定义如下：

$$HMAC=H(k \| opad, H(k \| ipad, message))$$ ④

在这个公式中，*k*是密钥，*ipad*与*opad*是0填充字符串，将密钥填充到基础散列算法的自然块长。

12.8.4 数字签名

数字签名是与消息相联系的信息块，只能由特定人员生成。利用公用密钥技术时，可以生成消息摘要，用一个人的专用密钥加密消息摘要。任何人都可以用对应公用密钥验证这个签名。数字时间标志可以保证签名是特定时间生成的，这很重要，因为如果丢失专用密钥，则可以生成任意签名和标上更早的日期。

12.8.5 时间标志

不可伪造的文档时间标志在需要非否认功能时非常重要。例如，如果Alice对合同进行了数字签名，但后悔了，就可以声明她的专用密钥丢失或被窃，声明合同是别人用她的（非公

④公式中‖指接合。

开）专用密钥代签的。时间标志可以证明文档是在 Alice 声明丢失密钥之前签名和发出的。构造时间标志的方法有多种，一种方法是时间标志服务对包括文档和时间值的文档进行数字签名。显然，人们可以怀疑时间标志服务的专用密钥本身是可疑的，但一种方法是让所有时间标志文档按顺序放置，生成其动态消息摘要定期（例如每周）发表当前摘要值，使时间标志服务本身也无法作假。Surety 公司提供时间标志服务（见 http://www.surety.com/）。

12.8.6 证书

公用密钥证书是个数字文档，包含公用密钥、密钥拥有者名称（为区别名）、有效期和其他信息，都用证书机构的专用密钥进行数字签名。这个主题很重要，见“证书、证书机构与信任模型”一节。

12.8.7 密钥交换

由于公用密钥技术相当慢，因此通常只用于验证和交换会话密钥，然后使用对称加密法。但是，如果有其他验证机制，则可以用密钥交换算法交换会话密钥。最著名的密钥交换算法是 Diffie-Hellman。

密钥交换是相关的，因为密钥交换、对称加密法与数字签名结合起来，提供了与完全占用密钥加密法相同的功能。这是非常有趣的，因为 1997 年 Diffie-Hellman 算法的专利到期，而且有公开域签名与对称加密法算法。

12.8.8 秘密共享

从安全角度看，只有一份的秘密才是最安全的秘密，将所有蛋放在一个篮子里，然后看住这个篮子。但是，灾难性事件或自然灾害可能破坏只有一份的秘密。具有多份的秘密是有风险的，因为只要丢一份，就会暴露秘密。假设秘密分成三部分，任何两部分都可以重建秘密。这就是秘密共享，可以推广到一般形式。例如，秘密可以分成 n 份，任何 m 份都可以重建秘密（m 小于或等于 n）。如果不到 m 份，则无法重建秘密。这种方法提供了秘密的安全，因为丢失全部(n-m)部分之前都不会丢失秘密，是相当安全的，因为敌人要进行 m 次独立攻击（第一次攻击可能提供警告，使罪犯停止脚步）。

另一个思想是秘密分割，当 n=m 时的秘密共享。秘密分割也用于密钥分配，通过不同通信信道发送各部分密钥。

12.9 密钥管理

密钥管理是加密法中最难的部分。

密钥管理与加密密钥的生成、分发、存储和删除有关。密钥的价值等于所加密的所有信息

的价值，甚至超出这个价值，因为如果敌人拥有密钥，就还能够生成非法消息，并将其引入系统中。

12.9.1 密钥生成

有时加密系统中有些密钥或密钥模式比随机选择密钥更脆弱的。密钥生成过程应当避免用这些密钥，但更严格的要求是密钥应该随机，然而真正的随机性是很难达到的。例如，旧版的著名 Web 浏览器根据当日时间生成加密密钥，是由机器时钟提供的。由于敌人准确知道当日时间，因此密钥的随机性大大减少，只要几秒钟就可以顺利攻破。

也有真正的随机数密钥生成器，基于放射性或散射噪声之类的自然物理现象生成密钥。这些设备很贵，不能广泛部署。对于计算机软件生成的密钥，有两种常见方案。

- 用户输入
  对于长期密钥，密钥生成器靠计算机外部的输入。通常，用户要随机输入一段时间，输入的字母忽略，而是使用键击间隔时间的随机变化。
- 伪随机
  对于随机生成的短期密钥，密钥生成是伪随机的，将进程标识符、计算机实时时钟、收到的硬件中断数等无法预测的信息组合起来。这些项目本身都不够随机，但组合起来可以得到随机组合，从中可以取出通常足够随机的密钥。

除了这些方法之外，软件还可以取得真正随机的数。最近的研究表明，可以用计算机硬盘中的空气紊流可以作为生成密钥的自然随机性来源。

供人使用的口令也是密钥。人们选择口令时，通常选得不够好。而机器生成的口令则很难记，需要写下来，这样也不好（实际上，在网络安全受到威胁的时代，写下真正好的口令并贴在某个地方也许是最好的办法。为了防止别人偷看，可以只写下一部分，记住另一部分）。通常的建议是使用较长的可记口令，如多个单词的通过口令或多个单词用奇怪的标点符号接合而成的口令。

12.9.2 密钥存储

加密密钥的长期和短期保存对良好的安全性至关重要。

- 内存
  计算机使用密钥时，必须放在内存中。这是大多数计算机都有的问题，因为内存内容可以被同一系统中运行的其他软件访问。在 PC 机上，这是无法防备的。而在多用户系统中，则内存是对不同用户隔离的，但优先用户和调试器可以在必要时访问其他进程的内存。为此，联机密钥的安全性取决于对机器的访问和系统管理员口令的安全性。

要减少联机存储的影响，好的习惯是先清除密钥使用的所有存储体之后再将内存释放回操作系统。

- 磁盘上

  加密密钥经常存放在磁盘文件中，因为密钥太长或太随机，手工输入很不方便。磁盘中的密钥文件通常以加密形式存储。好的方面是窃取加密文件对敌人没有好处，不好的方面是文件中所有密钥的安全性取决于主密钥。主密钥通常是对人有意义的口令，而不是真正的随机密钥。此外，要注意文件口令本身存放在什么地方如果系统需要在断电之后自动启动，则密钥文件口令必须联机存放。如果不需要自动重新启动，则可以提示操作员输入密钥文件口令。这时操作员可能怀疑是真的与密钥开锁软件通信还是有人想窃取密钥文件口令。

  由于这些限制，加密密钥文件的安全性通常取决于计算机的物理安全性加上管理员口令的安全性。注意，密钥文件还放在备份磁带中，如何处理和存储呢？

- 在保护硬件中

  商务系统通常用加密图形加速卡和智能卡之类的保护硬件设备存放密钥和进行加密操作。由于密钥不离开设备，而设备是严加保护的，因此密钥可以提供物理安全性。

  一个问题是，尽管无法窃取这样保存的密钥（否则小偷会被查出来），但非法软件可以以非法身份用这个密钥加密和解密消息。

- 脱机存储

  真正宝贵的密钥根本不能联机，而只能在隔离计算机系统中使用，不用时则要锁起来。如果担心一个拷贝的安全性，则可以用秘密共享将密钥分成几个部分，可以用其中的子集重建密钥。

  脱机存储打开加密文件的密钥时，需要规定谁能访问密钥，如何处理以及如何存储和销毁。

12.9.3 密钥销毁

加密密钥服役完毕之后仍然有价值。攻击者可以记录一个密钥加密的所有密文，保存很长时间。如果得到密钥，则可以方便地解开保存的所有密文。

- 密钥存放在内存中——用完立即消失。
- 密钥存放在磁盘中——用 0、1、替换模式和随机模式多次改写。人们可以分析擦除多次的磁性媒介。
- 密钥存放在纸上——烧掉或用碎纸机碎掉，而不是撕掉。
- 密钥存放在备份磁带中——如果要将密钥存放在备份磁带中，则应放在不包含任何其他重要注意的独立带中，然后就可以销毁这个备份带。

12.9.4 密钥分发

有时不需要分发密钥。例如，用加密法加密个人计算机磁盘上的文件时，就不需要将密钥分发给任何人。但是，大多数情况下，加密法应用于双方或多方参加的情形，各方可能位于不同地点，需要交换密钥。涉及两个人时，情形比较简单，而需要分发到整个密钥网络时，则情况比较复杂。

两个人之间有几种共享密钥的方法。

- 见面
  这种方法最容易理解，但不能扩展到几千人的情形，而且这种方法很昂贵。可以用这种方法事先交换整机密钥，但必须安全存储。
- 由信使发送密钥
  关键是信使是否可信！可以将密钥分解，不同部分按不同路由发送，但这样会增加费用。
- 用主密钥或密钥交换或加密会话密钥
  这是经过检验的方法，特别是在保护硬件中存储密钥交换密钥时。
- 使用公用密钥加密法或密钥交换协议
  这些机制可以和某人安全交换密钥，但和谁交换呢？问题是要从隐私变成验证。公用密钥方案是证书，密钥交换协议方案是数字签名或带外确认，如电话确认。一定要防止中间人攻击，即敌人分别向双方假冒对方。

多方参与通信时，成对密钥交换很难管理。

多方之间交换密钥时，可以用密钥分配中心（KDC）或公用密钥证书。

- 密钥分配中心
  在这个方案中，网络上的每个成员有共同的密钥交换密钥，有一个中央可信任的服务器。密钥分配中心成批分配密钥对或在需要时实时生成密钥。
- 公用密钥证书
  前面曾介绍过，证书将公用密钥与名称联系起来，让第三方（证书机构）签名证书。这些证书可以自由发布，也可以在开放通信信道上交换。需要通信的各方用所选对方的证书中的公用密钥加密会话密钥。

每个方案都需要某种中央机构。可以让联机密钥分配中心在需要时生成密钥，也可以让脱机密钥分配中心分配密钥，或让脱机机构认证公用密钥。选择时要考虑是否需要可靠联机服务、密钥如何取消、KDC能否读取所有消息。公用密钥在事先与对象没有关系时最强大，只要双方都信任第三方验证对方。

12.9.5 证书、证书机构与信任模型

公用密钥证书是一个包含公用密钥、用户名、有效日期的信息，由可任的证书机构（CA）用专用密钥进行所有签名。

证书的主要目的是证明公用密钥与拥有者姓名之间的联系。可以把证书看成，“证书机构谨此证明所附公用密钥属于这里所指的实体”。证明非常有用，不需要联机密钥分配中心就可以解决验证问题，需要通信的各方单独到证书机构签名自己的公用密钥。然后，例如当Alice要与Bob通信时，将自己的公用密钥证书和自己签名的消息发给Bob。Bob可以验证这个证书，因为证书机构的公用密钥是人人都能知道的。其他可以使用公用密钥证书的情形是，Alice要发加密消息给Bob，Alice必须有Bob的公用密钥，或从Bob那里或从目录服务中取得Bob的公用密钥。无论哪种情况，Alice都要保证真是Bob的公用密钥，目录没有篡改。证书可以保证公用密钥是Bob的（下一步就要弄清使用Bob的公用密钥者是否真是Bob，这是没问题的，因为只有Bob具有与Bob证书中公用密钥相匹配的专用密钥）。

证书的标准格式见X.509标准，目前常用的有两个版本。X.509 v1证书包含公用密钥、拥有者区别名（X.500名）、有效日期、证书机构区别名和证书机构签名。X.509 v3证书还包含灵活的属性/数值对。

最著名的商业化证书机构是Verisign(见http://www.verisign.com)，但其他组织也可以签发商业化证书，如美国邮政服务局和其他PTT。许多公司销售公用密钥系统，包括证书发布系统，可以设置完整的公用密钥基础结构。

12.10 小结

加密法提供了开放网络中实现隐私、验证、消息，完整性与非否认的重要工具。加密法提供的机制使Web通信可以实现安全套接层，Internet上的信用卡事务可以实现安全电子事务。效果上，加密法使其可以在开放的非信任网络上远距离变成原先要面对面才能做的事。

第 13 章安全性

你可以戴上钢盔，但仍然会撞上公共汽车。
—— Shikhar Ghosh

13.1 关于安全

安全常常被认为是 Internet 商务中最大的障碍。当然，安全性在许多方面对 Internet 商务系统很重要，但这只是技术支持业务的方式中的一部分。电子商务系统的安全性是个业务问题，而不只是个技术问题。公用密钥加密之类的技术提供了总体方案的关键组件，但还不够。本章提出一些考虑整个系统安全性的方法，我们将分析安全技术，介绍出口控制之类的问题。尽管许多课题与一般 Internet 安全有关，而不只是与商务安全有关，但我们主要介绍建立 Internet 商务应用所需的安全性。

尽管 Internet 上的安全问题值得格外小心，但是，利用本章介绍的原则，已经可以在 Internet 中用安全的系统进行买卖。这些原则适用于从头设计的系统，也适用于用现有 Internet 商务产品建立的系统。

读者如果对技术细节不感兴趣，则只要阅读前面几节，了解基础知识，然后就可以略读本章其他部分。对细节感兴趣的读者，本书末尾提供了参考资料。

13.2 为什么担心 Internet 商务安全性

许多人大致听说过 Internet 商务的安全问题和传说，因此第一个反应是慎重（有时是畏缩不前）。有些人则认为没有必要大惊小怪，因为我们对物理世界中的事务安全性也没有投入这么多时间。Internet 有什么不同呢？为什么要这么多心？

但是 Internet 的确大不相同，的确需要慎之又慎。

13.2.1 物理世界也要担心安全性

许多 Internet 商务问题是与实际业务问题相对应的联机问题。有些业务通信需要保密；我们要付真钱，我们要在合同上进行个人签名，等等。这些要求和实现这些要求的方法已经沿用几千年，包括了整个商业历史。在 Internet 上，我们在不同环境中面对相同的问题，因此要提

出来，要开发出新方案，而且必须在较短时间内完成。

13.2.2 计算机是互联的

在过去的计算机历史中，必须在同一房间才能使用计算机，或要通过直接连接的终端使用。只有可信用户才能进入房间或访问终端，因此系统本身的安全性并不那么重要。而在Internet中，则可以让世界上任何人使用我们的计算机，例如读取Web页面等。这样，盘子钻了个洞，就要小心考虑如何设计、实施与操作这个系统，保证整个盘子不会漏光。

13.2.3 网络是公开的

“网间网”就是网络互联集合，而Internet就是世界上最大的互联数据网络。各个网络属于几千个不同个人和单位，根本没有中央控制，把Internet联系起来的是使用的共同协议和网络相互传递的通信流。例如，在早期Internet中，网络分组经常遍历大学网络，任何有兴趣和有一定水平的本科生都可以读取。相反，在大多数国家，电话系统都是在一个实体控制下演变的。但是，即使在电话系统初期，隐私也是个问题。经常，许多人共享同一条线。电话操作员（特别是在小镇中）可以听到人们之间的会话。随着多年的系统演变，技术与组织不断变化，使如今的电话更加保密。事实上，人们对这种隐私的要求很高，以至于发现无线电话会话被记录时，感到非常吃惊，尽管无线电话使用无线电波。

13.2.4 网络是数字的

即使能够访问电话系统，也还是很难通过偷听电话而得到有用信息，而是很费时间的事。如果能瞄准特定人员，则会方便得多。但如果只是收听随机电话通话，则不知要听到猴年马月才能听到一个信用卡号。而计算机网络则可以同时收听许多“会话”。此外，计算机可以过筛会话，寻找特定模式，如信用卡号的数字模式，而不需要攻击者亲自做多少工作。

13.2.5 计算机收集数据

假设文件柜中有每个客户的书面文件，每个文件中包含信用卡信息，则攻击者需要访问文件柜，从每个文件中收集一列信用卡号，非常麻烦。而如果在一张纸中列出所有客户及其信用卡信息，则攻击者的工作会变得更轻松。计算机系统通常就是这样：所要的（敏感）数据很容易访问，或可以用程序进行搜索。

13.2.6 计算机可以编程

前面曾介绍过，一个问题是攻击者可以用计算机过滤数据，寻找重要信息。计算机还可以编程进行其他复杂的活动：提交成百上千个伪造订单，或者探索访问计算机系统的方法。具体

地说，高水平攻击者可以编写和发布程序给技术不高的攻击者，使技术不高的攻击者也能构成威胁。一个人很容易用方便的机器选锁，而不必通过不断学习与实践，成为选锁高手。

13.2.7 没有好的安全性就无法跟踪计算机欺诈

在不安全的计算机系统中，攻击可能不留痕迹。物理世界中的罪犯总会留下一些蛛丝马迹——脚印、指纹、探头录像，等等。安全和加密子系统都能保护系统，提供谁进行了什么操作的踪迹。由于我们在计算机上建立整个环境，因此还要生成这些子系统，而不可能利用自然属性。

13.2.8 计算机不能完全代替人

计算机下订单在许多方面比人工回答电话和记录订单更便宜、更有效。但是，人可以更灵活地面对客户，可以注意到订单或订单模式中异常之处，而机器则没有这种灵活性。有的人更喜欢对计算机系统说谎，而在电话上则不敢这么放肆，因此潜在的敌人大大增加。

13.2.9 Internet 是匿名和遥远的

Internet 上的通信比与人通信和电话通信显得更抽象、更非人性、更不真实。这种“虚拟性”使有些人想对远方的Web站点说谎和玩花招，而对隔壁的商店则从来没想过要这么干。相反，这种距离感要求客户还要能肯定自己真的是在和所需要的公司打交道。现实中很难伪装一个超市，而网上则方便得多。即使在物理世界中，也遇到过类似的事：有人建立伪ATM机，收集账号数据和个人标识码。

13.2.10 信息商务是不同的

许多安全问题对信息商务尤其明显。联机信息很容易复制、分发和修改。如果我们销售信息，则只能发给买主，而不能发给偷看的人。在物理世界中，送信人可以复制杂志，但成本太高，而复制电子版本则只需要几个单击。作为信息买主，我们要保证发来的信息就是我们收到的信息。截获和修改实际邮件很难，而电子版本则非常容易。作为信息卖方，我们通常要直接发送，因此后面没有机会进行检查（像邮购零售一样），或者没有现有业务关系，甚至没有物理世界中的发送地址，因此很难跟踪欺诈事务。

13.2.11 法律系统必须健全

这里介绍的许多问题要靠法律系统来解决，但法律系统靠许多物理证据以立案，如书面合同、签名、发货地址，等等。我们确定一个人的签名很难伪造，因此，如果签过某个材料，则很难否认。Internet 商务中怎么签名呢？大多数情况下（如有），我们用数字签名，但这是个较

新的技术，而且数字签名的微妙之处较难理解。同样，其他法律方面也随技术的改变而受到挑战，其中有些是我们熟视无睹的。

13.2.12 攻击的路径

计算机系统已经有许多易被攻破的弱点，因此新的 Internet 商务系统要格外小心，人们首先会感觉有问题。Internet 安全是《纽约时报》和《华尔街日报》的头条新闻，因此许多人（买方与卖方）都担心安全问题。即使风险比现实世界更低的地方，人们也会认为风险更高，因此一定要在 Internet 商务系统的设计和实现中解决这些问题。

13.2.13 我们能够

关于加密的一个重要事件是对许多应用提供的保护类型。Internet 商务应用最容易用加密法保护，但必将在现实世界的其他应用中得到运用，因为许多罪犯使用最初为联机世界开发的强安全系统。

13.2.14 未知的风险

最后，人们总是担心潜入混水之中。当前的业务与法律系统是如此熟悉，我们通常不愿意追究其来历。回顾一下货币、银行保险柜、合同法的演变很有好处，因为我们要在很短的时间内完成这类演变。

13.3 考虑安全

大多数专业人士认为可以把安全看成管理风险的问题。这有三个理由。第一，所需的安全取决于要保护的内容。例如，银行与零售商店使用不同的安全系统。第二，增加安全几乎总是要增加成本，带来不方便和延迟。到一定时候，增加安全将得不偿失。第三，系统中一点的安全性不能比另一点强太多，因为安全链的强度取决于最弱的一环。

实际情况下，安全是整个系统的属性。例如，银行的安全取决于保险柜、门卫、摄像头、感应器、员工的警惕性和操作所有设备与处理问题的过程。同样，Internet 商务系统的安全性需要相应技术，但也要求明确了解保护什么，以及人们的认真操作与监视。

13.3.1 技术

效果上，技术组件是安全工具箱中用于构造安全系统的工具。这些组件包括加密机制、安全通信协议、存储敏感信息的方法等等。大多数关于安全的介绍（特别是对 Internet 商务）都集中在这些组件中，本章稍后将一一详细介绍。

13.3.2 政策与过程

安全政策定义保护什么和为什么要保护，描述要防止的系统威胁。为此，它可以定义安全子系统，保护应用程序和评估得到的实施方法。看看能否满足安全图标。随着时间的推移，也可以用这个政策来评估系统是否正确操作。当然，政策本身可能随着时间的推移而改变，从而使安全子系统的实现方法相应改变。政策一定要随业务改变而改变，因为这种改变可能改变所涉及风险的性质。例如，大公司可能比小公司吸引更多坏人的注意。

过程记录系统应如何操作以满足政策要求。记录需要一遍遍正确进行的操作，而不是靠记忆办事。

13.3.3 人

有人说，人是任何计算机安全系统中最弱的一环，因为他们可能受骗、动心或与敌人串通。通常，他们连自己干了什么事都还不知道。因此对安全问题的正确培训很重要，要不仅操作员，而且每个涉及系统的人员都要了解安全政策、实现政策的机制及其在信息保护中的责任。我们将在本章稍后概述一些特定思路。

13.4 安全设计

记住这些问题之后，我们转入安全系统的高级设计方面。安全设计一开始就应作为项目的一部分，因为在后面增加安全性要比一开始设计系统的安全性昂贵得多。我们建议电子商务系统的安全设计采用下列五个步骤。

1. 生成安全政策。
2. 在应用程序中增加相应安全机制。
3. 对物理、网络与计算机系统环境设计安全性。
4. 开发反馈、监视与审查机制，观察系统的操作。
5. 用监视与审查结果调整系统的设计、实施和操作。

图 13.1 显示了这个循环。

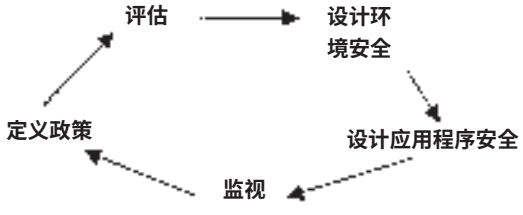


图 13.1 安全设计循环

13.4.1 建立安全政策

安全设计的第一步是建立安全政策。政策应包含整个系统，包括信息系统（计算机与网络）、数据（开发、生产和备份信息）和人（操作员、维护人员、客户）。政策应考虑保护什么、需要何种保护、谁负责系统不同部分、必要的培训以及需要何种监视与审核。

13.4.2 设计环境

第二步是设计应用程序环境。环境设计包括应用程序本身以外的所有组件，如计算机、操作系统、网络和物理地址。环境可能对应用程序提供一些功能和保护，因此应用程序不需要重复这些功能和保护（但要注意，这种功能应建档，以便需要时应用程序在其他地方重建）。其他情况下，环境可能以某种方式限制应用程序，要求应用程序采用特殊安全措施，因为它们不是环境的一部分。

例如，假设应用程序对强物理安全性保护的系统进行操作。此外，操作员在本地控制台上进行所有工作。这时，应用程序可能不那么强调管理操作的验证和访问控制，因为它可以保证操作员必须先经过验证才能访问。但应用程序设计成远程管理时则完全不同。但注意，我们不是说应用程序不强调验证和访问控制，应用程序最好还是有自己的验证和访问控制机制，因为物理安全机制可能失败。

实际中，环境设计和应用程序安全机制设计是相互交互的。有些安全问题在应用程序中比在环境中更容易解决，而有些安全问题在环境中比在应用程序中更容易解决。有时，特别是在产品设计中，应用程序对运行环境隐含一定的要求。关键是安全设计中一定要考虑整个系统的设计（包括应用程序和环境）。

13.4.3 设计应用程序安全机制

安全设计的第三步是提供应用程序安全机制。应用程序和安全政策的一般设计已经提供了保护什么的要求，并提供了所需保护类型的一些准则。这样，安全设计可以采用加密法、验证、授权系统之类的技术组件。除了这些控制信息访问的一般性机制之外，应用程序本身可能有一些特殊要求。例如，如果应用程序要在网络上销售软件，则安全机制可以包括产品密钥，只允许软件在特定客户的计算机上运行。本例中，应用程序的安全要求常常超出开放网络上的加密通信和防止攻击者攻破计算机系统。

13.4.4 监视与审核

除了特殊应用程序的特殊要求之外，安全性要求用反馈机制保证安全机制正确工作，包含机制限制损坏范围，恢复机制在发生故障时恢复。在物理世界中，还有个看门人的角色，保证门上的锁实际锁住。在电子世界中，这种检查与平衡采用审核速度检查和客户服务的形式。这

种机制提供的信息可以有多种用途：出现问题时再现问题，保证攻击不成功，验证操作符合安全政策，评估安全政策、设计和机制是否对应用程序有效。

计算机安全专家常常指出，安全性是整个系统的属性。服务的设计人员和操作人员必须认真考虑应用程序、风险和价值之后再确定要提供的安全级，并在每个级中考虑所部署安全机制的相对强度。

13.5 分析风险

设计适当的安全政策，一部分是确定对何种威胁采用何种级别的保护。例如，银行与家庭面对的风险不同，因此银行愿意针对这些风险投入更多保护。计算机安全中的许多选择是由安全措施的价值确定的（可能是金钱、性能或便利性）。如果不了解特定安全措施的价值，就无法从业务角度进行选择。本节介绍如何评估计算机安全风险和分析减少这些风险的措施。

13.5.1 敌人

第一步要了解敌人。人们通常首先注意到攻击类型和造成的损害，但攻击的手段只是工具。例如，确定的敌人可能愿意花大力气攻破系统，而偶尔的敌人则很容易放弃。两者都可能试行相同的攻击，但坚持与否，差别很大。因此，一定要提出下列问题。

1. 谁是敌人。
2. 有何意图。
3. 有何资源。

下面是要考虑的敌人。

- 黑客
  黑客是 Syber 空间的恶少，想通过攻破计算机系统找刺激、搞破坏或显示本事。黑客可能从网上或杂志上取得现成攻击软件，也可能不求甚解。黑客通常没有强大的计算资源，意图通常不明确。但他们常常造成巨大的损害，如破坏系统、搞乱操作或让系统人员花时间寻找与修复错误。
- 研究人员
  研究人员可能花大力气寻找安全协议中的弱点，并在网络上发布这些弱点。这种公布会造成公开和不安，但间接导致更安全的系统。研究人员通常能够访问巨大的计算资源，从闲置联网计算机网络到专用硬件或超级计算机。
- 罪犯
  即使没有 Internet，也有许多白领罪犯是专门攻击计算机系统弱点的。由于 Internet 是匿

名和无处不在的，因此成为罪犯的乐园。Internet 罪犯包括简单的欺诈骗取信用卡号到复杂的攻击、取钱或取信息。罪犯可能没有攻破加密机制的资源，但他们可以贿赂员工和其他能访问电子商务系统的人，罪犯的目的是赚钱。

- 竞争对手

  竞争对手不会通过破你的计算机系统来偷钱或删除记录，但会访问你的客户清单或业务计划。此外，竞争对手了解你的系统安全弱点之后，可以在竞争销售情形中利用这个信息或给你制造坏名声。尽管公司的资源很大，但他们通常不会在非法或不道德的事务中投入太多。

- 政府

  在竞争日趋激烈的世界经济中，越来越多的政府情报部门开始损别国经济以利本国经济。这种组织通常不考虑直接经济收益，而是瞄准专属设计信息、价格信息和关于竞争销售情形的准确情报。政府情报部门可以利用丰富的资源。

- 内奸

  心坏不满的员工是对电子商务系统安全的最大威胁。内奸能够访问敏感信息和系统。可以通过技术方法保护系统，如保护硬件设备，但审核、交叉检查和好的员工关系也很重要。设计应用程序时最重要的决策之一是安全性有多少是面向外部威胁，有多少是面向内部威胁。

- 任何能够实际访问的人

  任何能够实际访问设备的人都是潜在的安全威胁。清洁工、送信员、合同商、访问者和临时工都能访问，但不像全职员工那样接受相同的培训、调查和监管。

不同组织用不同方法评估上述人员的风险，但一定要考虑所有这些人员（和你想到的其他人员）。

13.5.2 威胁

了解可能的敌人之后，就可以考虑可能的攻击了。例如，开发网络上的通信可能受到许多威胁，如窥视、蒙骗等等。此外，客户与服务器可能被攻击，应用程序本身可能受到客户与服务器之外的攻击。下面是这些系统可能受到的攻击。

- 服务中断或退回

  这种问题可能是设备故障造成的，如磁盘、计算机或网络故障。更不幸的是，外部的拒绝服务攻击也能搞乱操作。例如，敌人可能发现服务器操作系统中的一个缺陷（可能与商务应用无关），利用这个缺陷使系统崩溃。这种攻击并不暴露专用信息，但会影响业务的有效操作。

- 窃取与诈骗

非法用户可能诈骗商品或服务，这可能是验证故障造成的，使非法用户能顺利伪装成合法用户。例如，敌人可以通过猜测口令访问另一用户的账号。在更复杂的情形中，用户可以制造非法的折扣优惠券。

- 盗用
  合法用户的支付可能转入非法方。尽管使用信用卡时很难这样，但有些支付系统则很可能这样。例如，一个好像合法的卖方可能访问另一卖方的内容，支付进入错误方，而买方浑然不知。
- 数据污染
  系统保存的记录可能被删除或篡改。这可能是软件缺陷或设备故障造成的，也可能是攻击所致。这种攻击可能有几种形式：敌人可能改变合法记录或在系统中插入假信息。数据污染的问题可能不是任何实际的修改。例如，如果业务记录丢失，则任何知道这个问题的人都可以挑起争端，因为公司没有防止争端的记录材料。
- 窃取记录
  敌人可能访问你的业务记录、系统的保密信息或客户的秘密信息。例如，侵入者可能窃取客户文件，其中可能包括信用卡号。
- 内容改变
  敌人可能攻破系统和修改系统内容。例如，黑客可能攻破 Web 站点和在图形文件上画一只袋鼠。
- 蒙骗
  敌人建立乱真的 Web 站点，吸引天真的用户。例如，敌人可能伪装域名系统（DNS），将客户吸引到假站点。

实现这些攻击的方法既复杂又多样。下面介绍一些攻击机制，可以按感兴趣的方式进行组合。

- 窥视
  侵入者听取网络上经过的消息，消息不一定加密，但即使加密，也可以记录下来，以便以后分析。
- 通信流分析
  侵入者了解到某个客户正在与某个服务器通信。历史上，通信流分析在军事和学术情形中非常重要。例如，指挥中心与某个战场的消息通信流突然大增可能表明准备攻击了，即使无法破译这个消息。在商务情形中，知道 200 个竞争对手在交谈可能有一定用处。但大多数电子商务系统和一般 Internet 系统不需要回避通信流分析。
- 加密分析
  侵入者想破解加密的消息，可以用许多不同方法，包括强力猜测译码密钥、攻击算法

与协议弱点和攻击生成与分发密钥的系统。

- 验证攻击
  侵入者假装成你要通信的服务器或假装成合法客户。这也包括许多类型，如猜测口令、窃取合法用户证明材料，等等。
- 替代攻击
  侵入者将消息的全部或一部分换成不同内容。
- 侵蚀
  侵入者一次一点地攻击系统，使总体影响不易发现。例如，敌人可能取得大量信用卡号，一次只用一个。

13.6 基本计算机安全性

计算机安全性主题可以写成好几本书，本书末尾列出了一些好书。此外，这是不断改变的。新硬件和新软件不断出现，Internet 技术日新月异，使问题的更加复杂。新系统（即使改变的现有系统）都要求新的安全分析。除了技术演变之外，业务要求的改变也需要改变系统。

13.6.1 关键安全问题

计算机安全有许多敌人，包括复杂性、灵活性和人。复杂软件有缺陷，可以被敌人加以利用。太灵活的软件很难正确配置，从而容易导致错误。太多用户会使安全责任不明。

- 复杂性
  软件有缺陷，而复杂的软件有更多缺陷。有些缺陷是无害的，有些则会打开攻击之门。这种缺陷通常发生在向软件提供意外输入时，尽管输入在界内时是可行的，但敌人用界外的数据则可能使软件处于危险的方式。
  例如，网络应用程序可能没有检查通过网络提交的字符串长度。敌人发送一个很长的字符串，覆盖应用程序堆栈，造成其执行敌人发送的执行码。这时敌人具有这个应用程序的所有权限——可能访问整个系统。
- 灵活性
  太灵活的软件很难正确配置。配置项目看起来没问题，但可能对安全造成严重恶果。经常改变的系统特别容易遇到这种问题，而 Internet 系统则通常随业务要求的改变而不断改变。
  例如，假设用户要求临时让所有用户都能读一个文件。这个临时需求结束之后，谁也记不住恢复原先的配置，使系统的某个部分脱离保护。
- 人
  一般来说，能访问计算机的人越多，系统越不安全。尽管大多数多用户计算机都想方

设法将用户相互隔离，但隔离只在认真管理之下才有效。

13.6.2 安全原则

构造电子商务应用或网络计算机的其他应用时，下列原则非常重要。

- 安全系统或保持简单
  复杂应用程序可能无法避免，从而带来缺陷。要保护这种系统，可以用防火墙隔离某种网络访问。防火墙可以限制允许经过终端系统的网络通信流类型。实际上，防火墙系统应当能够简单评估防火墙实现方法与配置的正确性。“如果有一些复杂软件，则要用一些简单软件保护起来”。
- 限制系统配置改变
  系统配置的每个改变都可能造成安全问题。显然，配置错误会打开漏洞，但有时看上去正确的配置与其他配置选项组合起来也可能造成问题。在许多事件中，认真记录所作改变非常重要。如果不了解系统配置，则不能了解其安全性。
- 认真考虑新版本
  软件新版本可以提供动人的新特性，但也可能有未知的安全问题。可能要花一段时间才能学会如何安全地操作。当然，一定要跟踪和尽快安装安全问题的补丁，但其他改变则要格外小心。新软件是诱人的，也可能是危险的。

13.7 基本 Internet 安全

Internet 是全球互联计算机网络的集合。一般来说，计算机如果有 Internet 协议（IP）地址，且能与其他相似的联网计算机交换分组，则是连接 Internet 的。这个定义也许太严格，因为许多公司、政府和大学网上的机器通过防火墙与通用网络部分隔离。这种部分隔离的机器可能无法与主 Internet 交换低级网络分组，但如果能够收发电子邮件和连接 W W W 站点，则也可以认为是联网的。

为了方便起见，我们把计算机分为客户和服务器。一般来说，客户是桌面机器，其功能是对个人完成各种计算工作，而服务器则是为了向广大用户发送更受限制的服务。这种差别使 Internet 客户和服务器在不同环境中操作、运行不同应用程序与通信软件、保存不同类型的数据、面对不同的安全问题。

13.8 客户安全问题

典型的 Internet 客户计算机是 Intel PC、Macintosh 或桌面工作站，具有 TCP/IP 堆栈和几个

Internet 客户应用程序（如果 PC 机运行服务器应用程序则应看成是服务器）。客户安全有两个关键问题：敌人如何访问客户机和到客户机上干什么？

13.8.1 客户计算机攻击方法

客户计算机攻击方法包括：

物理访问计算机

花几分钟在公司办公室中转转，数一数无人使用的计算机。如果机器保持登录而没人在场，则清洁工和其他能进来的人都能访问。即使只有上班时间才有无人在场的计算机问题，站点对来访者有什么规定？如果没有来访者问题，内部人员也可能用别人的计算机账号干一些坏事。

机会引入软件（病毒）

由于 IBM PC 与 Macintoshes 等个人计算机都不是多用户机器，因此很容易受到计算机病毒的攻击。问题是，PC 机上运行的任何程序都能完全访问系统中的所有硬件和软件。病毒可以刷新屏幕消息、改变其他程序或删除硬盘。抗病毒软件解决这些问题时，将新软件与已知病毒库对照，截获可疑系统调用。

病毒通常在新软件装入时趁机混进 PC 机中。受感染的机器写软盘时，病毒进入软盘中。这个软盘在另一系统中运行时，病毒又找到了新家。

最初软件包中的软件也不是免疫的，病毒可能在制造过程中引入软件（如果复制之前主盘受到感染）。这时，对厂家是个很难堪的事，但对受害者则没有帮助。

网络安全问题

个人计算机能够使用网络文件服务器，通常能够将本地硬盘内容导出或发表到网络上。如果这些网络文件系统的安全设置不正确或根本没有设置，则其中的计算机和信息可能受影响。

此外，由于客户计算机有时运行网络服务器（如个人 Web 服务器），因此操作服务器计算机的许多安全方面也适用于客户计算机。

网上直接攻击

见过十多年的计算机病毒之后，个人计算机用户开始认识到在机器上装入新软件的危险。但是，连接网络的计算机还可能受到其他形式的攻击，基于内容和自动安装的软件而不是用户安装的软件。

PC 邮件软件能够在文本之外传输附件。附件是特定应用程序操纵和显示的任何文档。如果应用程序有安全漏洞，例如无保护脚本语言，则病毒可以和文档一起发送。无戒心的用户单击文档浏览其内容时，启动相关应用程序，从而引入病毒。

W W W 小程序也有类似的问题。小程序是连接 web 页面的执行程序。小程序通常用 Java 编

程语言编写或作为ActiveX控件。小程序设计人员知道未保护计算机上运行任意程序的安全风险，Java 和 ActiveX 群体对这个问题采取不同方法。Java 小程序在沙袋中运行，小程序活动局限于沙袋内，因此不能进行任何有意操作。沙袋的问题是沙袋既要足够安全，又要能让小程序完成一些有用的工作。ActiveX控件采用另一种方法，可以完全访问机器，但由厂家数字签名，因此问题不是“这个小程序是否安全”，而是“能否信任 xyz 公司”。Java 社区也开发了代码签名技术，因此这可能是将来的潮流，至少在个人计算机软件不再受到病毒攻击之前是如此的。

协议攻击

敌人可能编写可以利用客户计算机的知识攻击网络安全协议，而不实际攻破客户。1995 年，加州大学伯克莱分校的学生利用客户计算机的知识攻击安全Web协议中的密钥生成软件。这就可以读取往来于特定计算机的消息。

13.8.2 客户计算机攻击目的

恶意代码访问桌面计算机之后，要干什么呢？

烦人

有些攻击并不干什么坏事，只是在屏幕上显示消息或造成速度减慢。尽管这种攻击对信息没有破坏性，但却非常恼人，用户要像对待危险攻击一样响应，因为它是扰乱性的，也可能是破坏性的。

使用资源

攻击者可能对攻破机器的拥有者没有特别的罪恶目的，只是想完成一些凭自己的资源难以完成的计算。例如，如果攻击者要用强力攻击攻破加密系统，则通过病毒可将这个计算分布到成百上千台不设防的机器上。

破坏信息

人们害怕的病毒是改变和删除信息的病毒。删除硬盘显然是很麻烦的，通常无法恢复，因为许多人并不备份机器[①]。如果信息进行微妙改变，则可能不易发现。

窃取信息

随着个人计算机更多地用于电子商务，具有实际商务价值的信息（如账号与信用卡号）可能存放在计算机中，这种信息是窃取的目标。病毒可以窃取证明信息、通过E-mail发送出去、然后悄悄地把自己删除，这是匿名和远程收集大量信用卡号的有效方法。即使证明信息保存在加密文件中，病毒只要等待下次文件开锁即可。

---

①有一种观点认为，每六个月左右将 PC 机内容全部删光并重装是对付软件和文件积累的好办法，但人们总是希望自己的主动选择。

使用证明信息

要对付病毒窃取证明信息的问题，可以将重要信息放进智能卡中。例如，专用密钥不能离开卡的保护硬件，因此不会被病毒窃取。但是，病毒可以把自己安装在键盘、计算机屏幕和卡之间，用户要数字签名一个文档时，病毒实际上安排智能卡签名完全不同的内容。这种问题只能在病毒无法访问用户界面最后一部分时才能真正解决，例如带内置显示的智能卡。

13.9 服务器安全问题

服务器计算机通常运行应用程序软件或向大量不同用户提供一组服务。有时用户能够登录服务器，而有时只有管理员能够登录服务器。服务器计算机通常运行Unix或Windows NT之类的多用户操作系统。

13.9.1 服务器计算机攻击方法

服务器计算机攻击方法多样而微妙。有时攻击的目的有限，如访问特定文件或应用程序，而有时目的是安装新软件或运行具有根或管理员权限的应用程序。

用普通用户身份登录

攻击服务器计算机的第一步通常是取得计算机普通授权用户的登录或shell会话。这有许多方法，如取得或猜测口令、找到无人在场的终端或取代现有通信会话。

- 猜测口令
  可以用常用字与姓名字典猜测可能的口令。向帮助桌面打电话，以合法用户身份请求将口令复位。窃听网络通信流，取得经过的口令。用键盘窃听病毒捕获口令。
- 利用现有通信会话
  找到无人在场的终端，用TCP序号攻击插入连接。
- 在现有会话中插入命令
  使用X Window System中的不适当权限，或在终端答复上在现有会话中插入命令。
- 利用设置不好的安全控制
  攻破信任主机或假装信任主机，用rsh之类的协议不提供口令而登录。

取得用户权限之后，敌人就可以探索系统，寻找允许更大权限的安全弱点或寻找设置不好的安全控制。有时用户权限就足够了。例如，如果业务应用程序的日志文件用完全可读保护配置，则任何普通用户账号都能访问。

利用应用程序缺陷

由于服务器计算机通常使用商品操作系统，许多人都能访问这个软件，因此敌人可以充分

搜索可能的弱点。

- 超界输入
  许多应用程序不够严谨，不检查输入的内容或长度。例如，如果应用程序使用定长缓冲区，但不检查输入长度，则敌人可能在应用程序中输入很长的消息，将应用程序内存覆盖。如果缓冲区在堆栈中分配，则敌人可以覆盖程序返回地址和取得对应用程序的控制。如果应用程序有权限，则成功的敌人也有权限。即使敌人无法取得应用程序的控制，也可能使应用程序崩溃。
- 未能检查输入语法
  应用程序使用 TCL 与 PERL 之类的解释性语言或向其他应用程序传递求值命令时，如果未能检查输入语法，则可能有风险。如果敌人能让应用程序把输入消息当作程序执行或对答复消息进行变量替换，则会有安全风险。

利用设置不好的安全控制

即使服务器应用程序没有缺陷，也可能在不安全方式中操作。

- 设置不好的文件保护
  服务器操作系统的文件保护机制很复杂，容易出错。如果应用程序文件让敌人读取访问，则可能泄漏宝贵信息。如果应用程序文件或队列目录是可写的，则会让应用程序执行敌人提高权限后的指令。
- 调试码还能访问
  如果安装网络应用程序后调试码还能访问，则敌人可能远程使用优先调试命令。在一些公开的事故中，调试访问邮件软件曾经造成攻破 Internet 上的计算机。

13.9.2 服务器计算机攻击目的

一般来说，客户计算机攻击的目的也适用于服务器攻击，但这些目的在服务器上有特殊意义，因为攻击可能影响许多人收到的服务，而且服务器中集中的信息可能有巨大的经济价值。

访问信息

攻破客户计算机可能向敌人暴露一个事务，而攻破服务器计算机可能向敌人暴露所有事务。例如，如果在服务器中登记信用卡号，则敌人一旦攻击成功，就可能取得几千个信用卡号（防止这种结果是安全电子事务协议的设计目标之一）。

改变信息

电子商务服务器可能存储业务记录，破坏与改变信息会使公司无法工作、报税和抵抗客户争议。改变安全配置可能留下让敌人访问的后门。

访问安全证明信息

服务器可能存放许多用户的安全信息或与其他计算机系统通信的安全信息。例如，在加密保护的网络中，加密密钥可能保存在磁盘中。如果这些密钥被窃，则可能攻破整个网络。

拒绝服务

服务器计算机上的攻击可能意在整个社区拒绝服务。如果能使服务器重复崩溃，或忙于处理非法请求，则可以使系统无法使用。

13.10 达到应用安全性

达到计算机安全是很难的，但有一些一般原则。

- 限制系统访问
  能登录访问服务器的人越少越好，不要对一般登录使用应用程序服务器，保证系统管理员使用良好的口令和不留下无人在场的登录终端，考虑关闭系统管理的网络访问。
- 使用可用安全工具
  有许多系统配置检查程序和监视程序，这些工具可以从外部探测系统的已知安全弱点，还可以统计文件系统的可疑使用保护。
- 用简单系统保护复杂系统
  大多数服务器计算机操作系统非常复杂，很难信任。本章稍后介绍的防火墙系统可以限制对服务器的访问，而且比较简单，值得信任。防火墙还可能进行审核与日志功能。
- 保证系统在常规之内
  许多应用程序在通常情况下工作顺利，但如果磁盘满时或CPU过载或连接用户数太多时造成服务器的行为不可理解，则可以采用限制，在遇到异常操作条件时触发警报。
- 记录配置改变
  建立维护系统配置记录与需求改变的过程。
- 建立备份
  听起来是非常基本的，就是要保证经常备份服务器软件与应用程序数据。保证访问备份磁带的安全控制适合备份中的信息。
- 保证软件正确安装
  新软件安装是安全控制设置不当的主要原因。

13.10.1 防火墙

防火墙包括硬件、软件或两者都有，将专用系统或网络与公开网络隔离开。这个术语可能不太准确，因为防火墙用于防止问题发生和防止问题扩散。

防火墙的功能包括下面几点。

- 分组级过滤
  防火墙通常包括分组级过滤，控制基本连接。例如，Internet 协议分组可以根据源和目标 IP 地址、源和目标端口号或分组类型接收或拒绝。这些功能使防火墙外的连接只能连到内部的特定服务。另一个重要功能是拒绝外部的任何号称源地址来自内部的分组。

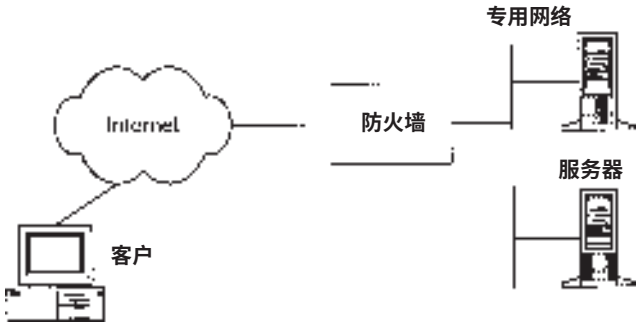


图 13.2 Internet 防火墙例子

- 应用程序中继
  防火墙通常实现应用程序协议中继功能。例如，Telnet 虚拟终端协议中继可能允许外部客户在装有一次性口令系统（如 S/Key）或硬件登录令牌（如 SecurID）时建立与内部主机的终端会话。
- 审核与日志
  防火墙生成独立于内部服务器机器的通信活动日志文件。这些独立审记追踪帮助容器，即使内部系统被攻破，敌人也无法消除自己的踪迹。
- 集中安全管理
  如果防火墙内有多个服务器系统，则安全责任可能分散。防火墙可以作为所有外部通信都要经过的总关口，这样就比多个独立系统更容易管理和操作。

13.11 验证

验证过程就是建立个人、功能或一类用户成员的标识。验证过程通常用一个或几个因素：你有的、你知道的或你代表的。高度安全应用程序通常需要双因素验证过程。

- 你知道的
  你知道而别人不知道的口令或秘密。一般来说，口令不能写下来，但人们认为网络上使用时应放松这个限制。问题是人们通常选择不好的口令，因此不提供太多安全性。好

的口令又太难记，另一种方法是用几个单词构成的暗语。

- 你有的
  物理钥匙、访问卡或护照是你实际拥有的东西。在电子领域，可能是硬件令牌或智能卡。有人认为写下来的复杂口令或代码就属于拥有的，而不是知道的。
- 你代表的
  指纹、掌纹等生理特征是一个人的个人属性。

验证常常与授权混起来，例如普通房间钥匙，验证拥有密钥就表示授权进入房子的人。计算机系统通常将授权与验证分开，知道用户名与口令就允许进入，但此后的权限由另一个访问控制表确定。

13.11.1 口令

口令使用很广，因此我们专门用一节介绍。

口令常用于登录计算机系统或网络。输入的用户名和口令与口令文件对照，如果相符，则允许登录。

口令可能很安全，但和大多数安全项目一样，需要注意其细节。

口令选择

人们通常选择不好（不安全）的口令，如字典中的单词或配偶的姓名，但如果不让人们选择自己的口令，则他们会写下口令，而不是记住口令，甚至把口令贴在显示器上。要解决这个问题，通常要求口令足够长，混合字母和数字。

口令改变

要在较长时间保持安全，就要经常改变口令。如果顺其自然，则人们通常不爱改变口令，或会循环使用几个不同口令。口令软件的一些复杂性就是为了强制经常改变口令。 一个人在多个站点或多台计算机上有口令时，是多个站点使用相同口令还是每个站点使用不同口令呢？多个站点使用相同口令的问题是，一个口令被破，就会全盘皆破。而每个站点使用不同口令则可能忘记一个或几个口令，因此只好写下来。无论哪种情况，多个站点使用口令时更需要经常改变口令。

口令存储

需要口令的站点中的口令存储系统是显然的安全目标。许多人的口令都存放在一个地方，自然成为攻击目标。要减少这个问题。通常不要以明文（甚至加密）形式存储口令，而是存储每个口令的散列。要逆转散列函数是很难的，因此无法从存储内容恢复口令，但很容易检查是否匹配。除了散列之外，还可以使用“盐”。盐是和口令文件项目一起存储的随机数，对每个项目不同，是散列计算的一部分。如果敌人顺利取得整个口令文件，则还要攻破每个项目，而

无法同时对所有项目采用字典攻击。

13.11.2 其他验证技术

下面介绍一些其他验证技术。

一次性口令

口令的一个问题是，如果口令在不安全通信信道上传输，则口令的安全性值得怀疑。这个问题在公开网或客户站点上登录办公室计算机时就会遇到。要解决这个问题，一种方法是向每个用户发出一组口令，每个口令只用一次。通常，这是打印一个卡片，然后划掉每个已经使用的口令。其中一个系统是 S/Key，用单向函数生成口令链，每个口令输入到函数中，生成下一个口令。技巧在于逆向使用口令，使窥视者无法复制这个序列。中央站点要存储序列中的第一个口令和最后一个口令。

硬件令牌与智能卡

由于口令的弱点是众所周知的，因此高度安全应用支持通过硬件设备验证。只限于验证的设备通常称为令牌，而智能卡则既可以验证，也可以用于更一般的安全用途。令牌的两种常见类型是由 Security Dynamics 公司与 Axent 公司生成的。Security Dynamics 公司的 SecurID 卡前端有个窗口，显示加密生成的随机数，每分钟改变一次。匹配验证服务器可以重复这个计算，检查这个数。用户只要将卡中的数字和 PIN 码复制到系统中。Axent Defender 卡是个计算器式的小设备，具有键板和显示器。操作时，系统向用户发送一个挑战码，和用户 PIN 一起输入卡中。用户将卡中的响应码复制到系统中，服务器执行同一计算并比较结果。

智能卡是个小卡，包含处理器和一些内存。这些卡可能像信用卡那么大（有时称为芯片值），也可能像 PCMCIA 那么大。一般来说，卡内存中包含对称或非对称加密的一些专用密钥。

13.11.3 Web 验证

万维网使用无状态协议，每个浏览器请求服务器时是独立的，不依赖于过去的任何情境。此外，验证问题是对称的，用户要知道对方是否为正确的服务器，服务器要知道对方是否为正确的用户。

客户验证

客户验证过程就是向服务器建立满意的用户标识。

- **基本验证**

  HTTP 1.0 内置的惟一验证机制是基本验证。通常，Web 浏览器请求 Web 服务器时，不提供验证信息。如果服务器不接受这个请求，则会响应“unauthorized”（非法）代码和一个界。界是个文本字符串，让用户知道请求的用户名和口令。通常，浏览器显示一

个验证弹出框，顶端显示界，还有用户名与口令输入字段。用户单击OK按钮时，浏览器重试原先的请求，这时在请求的HTTP头中提供用户名和口令。用户名和口令编码成uuencode（Unix到Unix的编码）格式，使人们无法阅读，但程序很容易译码。由于Web是无状态的，因此这些证明信息应在每个请求中提供。浏览器记住哪个站点需要口令，并在后续请求中自动提供有些浏览器甚至能记住会话之间的用户名和口令信息。因此用户不需要记住（但别人使用这台计算机时也能使用这个用户名和口令信息）。

基本验证的主要问题是用户的证明信息以明文形式在网络上传递。要克服这个问题，可以用SSL或其他加密协议，但这些协议经常使用时会大大影响性能。

- 摘要验证

  摘要验证是HTTP 1.1准备使用的机制，是问题/响应协议，服务器向浏览器发送一个问题，浏览器用本地存储的口令计算响应。由于用户口令不在网络上发送，因此摘要验证比基本验证安全得多，而且只有很小的性能影响。摘要验证提案还包括可选的非透明型数据字段，服务器将其提供给浏览器，浏览器将其交回服务器。服务器可以用这个字段向自己发送加密消息，这个消息可以在响应验证期间避免任何数据库查找。

- 客户端证书

  Web上对各个端验证使用公用密钥证书的功能是在1994年的SHTTP协议中首先推出的，但这个协议没有广泛使用。Netscape通信公司引入的安全套接层（SSL）协议在SSL V2中引入了客户端证书功能，但这个功能到SSL V3才广泛部署，Netscape Navigator 3.0与Microsoft Internet Explorer 3.0支持SSL V3。使用客户端证书分为两个阶段。首先在与证书发布服务器会话期间生成客户端证书，然后即可在其他服务器中使用这个客户端证书。

  证书生成期间，用户在窗体中填入标识信息，并生成公用密钥对象。密钥的公用部分和标识一起提交给证书发布服务器，证书发布服务器用它的证书机构根密钥签名用户的公用密钥，生成证书。证书返回浏览器中，和相应专用密钥一起保存。

  得到客户端证书之后，用客户端证书进行客户端验证的服务器用SSL协议头向浏览器发送证书请求。浏览器通常显示一个弹出框，允许用户从可用证书中选择一个证书和用口令打开。口令保护专用密钥，以免被用户计算机上运行的其他软件窃取。证书和用相应专用密钥签名的消息一起传输到服务器中。证书建立用户标识信息与专用密钥之间的连接，专用密钥签名的消息表示密钥真是该用户拥有的密钥。这样，服务器就知道用户就是证书中指定的人。

服务器验证

最弱的服务器验证方法取决于域名系统完整性。用户在浏览器中输入www.xyzcorp.com时，连接的很可能是正确的服务器，但这要取决于许多计算机的正确管理和操作员的格外警惕，因此更强壮的方法更有用。

目前最有效的服务器验证方法是公用密钥证书。SSL之类的安全Web协议允许服务器向客户发送一个经过第三方（证书机构）签名的公用密钥证书。用户要在浏览器中嵌入证书机构的根密钥，通信要用SSL进行，如果这样，则用户知道证书机构验证了服务器的标识。但在商务环境中，这样也许还不够。

假设用户要与XYZ公司做生意，这个公司有个联机商店。这个商店的Web页面可能和其他公司的页面一起放在共享计算机中。因此，服务器证书可能是“Joe 的宿主服务”，而不是“XYZ公司”，让用户莫名其妙。

这个问题可以用 S-HTTP Web 协议处理，因为Web中的每个超链接都包含目标页面的安全属性信息。用户对初始页面满意之后，后续页面的安全属性信息是自动处理的。

13.11.4 Web 会话

前面曾介绍过，基本Web协议是无状态的，每个请求都是独立的。因此，每个请求应独立验证。基本验证就是这样的，每次请求都要将用户名和口令输入服务器中。用户的经验并不坏，因为第一次从站点请求用户名和口令之后，浏览器在后续请求中能记住提供的证明信息。但服务器则要在每次访问时独立验证用户名和口令。此外，尽管使用SSL之类的安全协议能克服明文传输口令的问题，但这些协议不能保证所有通信，因为浏览的内容不一定都是很有价值的。摘要验证可以解决这些问题，使验证相当安全和相当简单，但没有广泛部署。

既支持验证又不需要加密所有内容的最常用技术，是在无状态基本Web协议之上生成会话。进入会话时，要求用户验证，此后的每个访问则不需要验证信息，而只要在请求之间传递会话XYZ部分的信息。目前生成Web会话的方法有两种：定制URL和Cookie。

使用定制URL方法时，会话的标识放在URL中，可以作为URL查询字符串的一部分：

```
http://www.xyz.com/url/path/name/script.cgi?query&string&with&session_ID
```

或放入URL中：

```
http://www.xyz.com/<sessionId>/url/path/name
```

前一种方法要求所有用户交互由管理会话的特定服务器应用程序（CGI脚本）处理，后一种方法要求将会话验证建立在Web服务器本身之中。

在Cookie方法中，会话标识信息存放在浏览器Cookie中，因此浏览器在每次请求时自动将其提供给服务器。这很适用，但有几个问题：并不是每个浏览器都支持Cookie，Web代理服务器不一定总能正确处理Cookie，用户可能将浏览器配置成拒绝Cookie。即使这个机制能行得通，如果客户通信不加密，Cookie 也可能被人偷走。

对于加密通信，SSL V3提供了另一种有趣的方法：第一次请求站点时请求客户端证书。此后，可以用 SSL 会话密钥缓存减少验证的平均成本，将其用于多个请求。SSL V3 提供了其他单纯验证连接的功能，不加密内容和发生相关的性能影响。

13.12 小结

安全性应当是整个系统的属性。安全官员的重要问题是安全性应该到处都很强，因为敌人只需要攻击最弱的点或操作人员疏忽的地方。要解决这个问题，就是建立强安全基础上的封闭体系，但要保证有反馈机制与恢复机制。

第 14 章支付系统

金钱自己可以推动世界。

——帕布里留斯·西拉斯[①]

14.1 支付的作用

在许多方面，在线支付是电子商务系统的基础。支付的功能使电子商务系统区别于只有广告和其他通信功能的系统。但是，增加支付功能要在系统中大大增加复杂性。首先，支付机制与总体系统的安全性要足以保护系统。第二，系统要提高事务的高度完整性，不能丢失或改变支付事务。

本章考虑买方与卖方同意买卖和商定价格之后发生的事情。我们从几个角度检查支付系统。首先，我们通过实际支付系统了解如何考虑联机系统。第二，我们介绍一些已经开发的联机支付系统。第三，我们考虑如何进行所谓微事务的支付。最后，我们简要介绍支付及其角色的抽象问题。

14.2 关于钱

介绍支付之前，先要谈谈钱本身。可以把钱分为两种：货币象征和货币符号。货币象征如硬币和纸币，价值就体现在其身上。过去，钱的价值取决于制作成本；如今，则只是表示一定价值，这是政府在发行货币时规定的价值。

而符号性钱则在别的地方存放其价值。例如，支票本身没有价值，但它表示同意转钱。支票也不能自由流通，只能在某个人的名义下使用。扩展信用的支付工具是各种符号性钱，例如，使用信用卡时，就表示将来同意支付这么多钱，这个事务是由签发信用卡的财务机构保证的[②]。

在 Internet 和一般电子世界中，大多数系统都使用符号化钱：信用卡、购买订单（允许将来某个时候支付）和电子转账。有些新系统（如各种形式的电子现金）还没有广泛使用，但使用电子形式的货币象征性金钱。

---

①帕布里留斯·西拉斯《格言录》。

②在某些条件下，签发信用卡的财务机构不保证事务。例如邮购事务中，客户和卡并不实际显示。

14.3 实际支付系统

在线支付在许多方面与实际支付系统是相同的。由于我们的在线支付事务在网络之外也有价值，因此在线支付系统通常基于现有支付机制。本节介绍几种常见的支付方法，特别是介绍与联机有关的属性和联机时要注意的属性。

14.3.1 现金

现金是最熟悉也最常用的网外支付方式。对客户而言，它有许多重要属性。

1. 广泛接受性。现金是几乎任何事务都接受的（但大笔买卖很少用现金）。
2. 方便性。现金易于使用，少量现金易于携带。
3. 匿名性。支付现金不需要身份标识③。
4. 不可跟踪性。现金花完之后，就无法跟踪原先的拥有者。
5. 无买方事务成本。买方使用现金时不增加任何成本，使现金特别适合小笔事务，而支票与信用卡的开销比起交易价值就显得很大。买方持有现金而不投资就没有机会成本。商家在处理现金时需要一些成本，如安全转到银行、让银行算钱，等等。据调查，这种成本高达10%。

这些属性使联机现金机制对许多联机事务有吸引力，但建立这种机制也有一定的技术难度。稍后将介绍电子现金系统的技术和推荐系统。

14.3.2 信用卡、记账卡供方卡

信用卡是客户熟悉的，各种记账卡也是。信用卡（如Visa或MasterCard卡）在购买时扩展购买者的信用，而实际支付则是在后面通过月结发生。信用卡与记账卡的差别在于记账卡的结余要每月付齐，而信用卡则可以在月末将结余转到下周，只是计上利息。Visa或MasterCard卡通常是信用卡，而American Express卡通常是记账卡。从商家角度看，这些卡是相同的，惟一的差别是商家是否接受特定的卡。各个商家可能有自己的记账卡或信用卡，自己处理所有信用与支付过程。

另一种支付形式是某种借方卡，与银行中的需时存款账号（如支票账号）相联系。这些卡通常带有Visa或MasterCard微标，可以在任何接受Visa或MasterCard卡的场合接受。但事务不是扩展信用，而是立即从相关账号中支付。从商家角度看，这与信用卡完全相同。这种卡也称为脱机借方卡，因为不需要实时授权事务。

③大宗事务除外，在美国大宗事务要向国内收入服务部报告。

相反，联机借方卡，则要求用个人标识号（PIN）实时授权事务。这种卡通常是ATM卡，商家通常从本地银行接受这种卡，进行某种事务。与脱机借方卡相似，支付也是立即从相应活期存款账号支付。

商家要为处理信用卡事务付费。费用随银行、商家模块、事务规模、信用卡事务量和商家业务类型的不同而不同。例如，邮购商家通常比相应商店支付更多信用卡事务费用，因为客户不在现场签名。这种事务称为“卡不在场”事务，具有更高的不付账风险，因为买方可能窃取信用卡。典型的零售商费用为 25 美元加总事务的 1.5 到 3.0%。邮购费用更高，可能是总事务的 2.5 到 5 %。

信用卡在客户零售事务的联机支付中非常普及，特别是零售和网外邮购业务中使用信用卡的事务，包括预订杂志、快报和联机信息服务。由于信用卡事务有一定的成本，因此不适合各个小事务。例如，按照上述收费标准，一个收入为 50 美分的事务，有一半要交给信用卡事务费用。处理小事务的方法见“微型支付”一节。

包装支付系统

大多数客户把信用卡看成相当简单的设备。我们用它买东西，然后银行发来账单。其实它是相当复杂的，信用卡包括了一组复杂的服务。

- 客户信用
  大多数信用卡都扩展持卡人的信用。如果持卡人在月间转结余，则计利息。一般来说，如果持卡人每月完全付清，则不发生费用。
- 立即支付
  信用卡与现金相似（不同于支票），立即（隔夜）支付给商家。这种快速支付可以减少商家的财务库存要求。
- 保险
  与现金不同，持卡人没有丢钱的巨大风险。只要通知发卡单位，就可以将卡冻结，即使不通知，持卡人的风险也是有限的。
- 财务清算
  即使持卡人的银行不同于商家的银行，也可以使用信用卡。这个简单而明显的事实使商家更加方便，而支票则做不到这样。外地银行签发的支票很难被本地银行接受。
- 全局服务
  信用卡能自动处理许多币种。商家处理自己的本币，而信用卡账单到达时，事务已经换算为持卡人的本币。
- 保存记录
  信用卡定期发送账单，对调节费用非常方便。
- 客户服务与争议解决

发生产品质量或未送达争议时，持卡人可以向发卡单位报告。商家的查询银行可以取消或退还账款，使客户更有能力取得满意结果。

- 支持商家信任
  在很大程度上，客户可以信任窗口中贴有信用卡关联标识的商家。这个标识不仅表示可以接受信用卡支付，而且表示如果遇到任何麻烦，消费者可以投诉，不必到外地城市中遇到的商店，而只要到自己的发卡银行投诉就可以了。
- 支持消费者信任
  在很大程度上，商家可以信任持信用卡的客户。只要卡是有效的，符合客户签名，商家就能收到款，从而对商务大有帮助。

信用卡是较昂贵的支付方式，成本达到事务价值的2 %到5 %，但提供一组复杂的服务，可以分解信用卡的功能，算一算各项服务的价值。此外，评估其他支付系统时，可以一个特性一个特性与信用卡提供的服务进行比较。

信用卡事务的工作管理

图 14.1 显示了典型信用卡事务的步骤。持卡人将信用卡交给商家之后，商家向商家银行（称为查询银行）发一个授权请求，请求在买方信用卡中预留指定金额。请求由查询银行转发，通过交换网（如 Visa 与 MasterCard 经营的交换网）送达买方信用卡的发卡银行。如果信用适当，则发卡银行授权这个事务，通过网络将响应发送回来，否则发卡银行拒绝授权。授权在指定时间内有效（通常为三天），然后即过期，除非事务得到处理或授权更新。

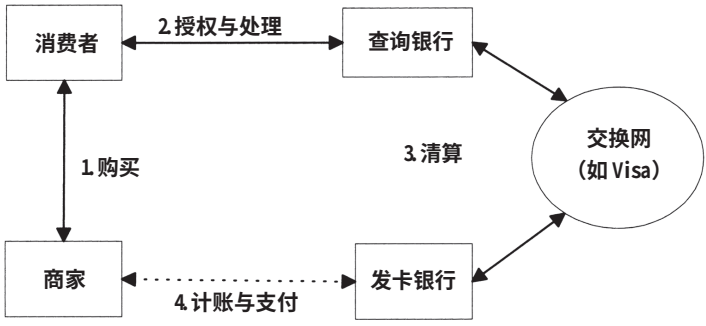


图 14.1 信用卡事务流程

大多数情况下，事务在授权之后的一段时候得到处理。授权响应包括后面处理时使用的代码。例如，零售店事务通常在一天结束时成批处理。邮购事务则要发出商品之后才处理，通常在信用卡关联规定中要求。

有时，可以同时授权和处理事务。对于联机系统，这常用于发送信息产品，支付后立即发

生。有些电子支付系统将支付的最后一步与信息产品的发送结合起来，这种系统使买家更能保证产品送达，将在稍后介绍。

除了信用卡事务的上述常规处理外，联机信用卡支付系统还要处理几种异常情形。包括逆转不再需要的授权，退货时提供信用和只能发出部分订货时收取相应费用。此外，信息产品厂家一定要有处理客户争议的明确政策，因为它不像传统邮购商家一样可以退货。

处理信用卡支付的计算机系统通常连接查询银行的计算机，取得授权和处理服务。在许多情况下，查询银行将这些计算机系统的操作委托给另一组织，称为卡处理者。这些公司处理事务的各个方面，有时本身可以作为查询者。商家的银行关系决定了用哪个系统进行事务处理。

随着信用卡业务的演变，出现了许多管理信用卡事务的不同通信协议（据估计，有 1400 多种）。除了卡协会建立的标准协议之外，许多银行还建立了自己的协议，提供改进服务。几年前，ISO 采用标准协议 ISO 8583 处理这些事务。ISO 8583 常用于管理美国以外的卡事务，但目前在美国用得不多。从这么多不同协议出现一个标准的结果是 ISO 标准有许多可选字段。这种多样性通常要求经过特定改变之后才能在某个查询银行使用。为了保证正确操作，查询者通常要求用测试系统验证实施方法之后再转入生产使用。

信用卡支付适合各种消费者零售应用。主要问题包括：

1. 信用卡号与相关信息的隐私性。稍后将介绍几个提供这种安全性的方法。
2. 事务价值是否适合信用卡事务的成本。处理信用卡是比较昂贵的，如果客户对购买的东西不满意，则可能要倒贴（对商家造成成本）。
3. 商家能否建立接受信用卡所需的银行关系。由于银行不愿意将这种权限提供给新的或不熟悉的商家，因此新公司很难立即采用信用卡支付。

风险管理

信用卡有许多风险管理问题，下面介绍几个。

- 消费者风险

  在美国，消费者信用保护法限制卡或卡号被窃时持卡人的责任为 50 美元。持卡人通知银行卡丢失之后，就不再有更多责任。通常，为了与客户搞好关系，发卡银行连这 50 美元也不扣。这种法律的结果是将信用卡安全的责任交给系统设计人员和操作人员。消费者还可以在用信用卡支付之后对商家提出性能争议。发生这种争议时，商家银行将款项从商家那里撤回，直到争议解决。

- 商家风险

  如果持卡人亲自到商场，将卡放到电子终端，商家检查了持卡人签名（如果商家严格遵守这个手续），则商家的查询银行承担卡被窃或欺诈的风险，保证将钱款打给商家。但是，卡通过邮件或电话使用时，即卡不在场事务中（也称为 MOTO，表示邮件或电话订购），则遇到欺诈事务时，责任在商家。迄今为止，所有 Internet 事务都算作 MOTO，

但安全电子交易规范（SET）也许能改变这个情况。

信用卡授权网络对商家提供了一些评估风险的辅助工具。一个服务是地址验证服务。商家可以从持卡人那里请求持卡人计账地址，将其和卡授权请求一起发送，将这个地址与发卡银行的记录进行对比，并响应匹配结果，然后商家可以选择接受事务与否。MOTO商家还可以根据客户历史和其他信息建立自己的诈骗控制系统。

国际问题

信用卡使用模型也许是国际性的，但地区差别也可能会影响 Internet 商务系统的设计。下面两个例子显示了可能出现的问题。

- 起止有效日期

  在美国，信用卡通常只标一个到期日期。到期日期应在向卡网络的授权请求中发出，因此商务软件通常在订单窗体中有卡号、卡类型和到期日期字段。而在欧洲，则卡中标出有效期的开始日期和结束日期，授权购买时需要这两个信息。这样，欧洲市场的 Internet 商务软件还要从用户那里请求更多信息和将其路由到授权网络。

- 奖金支付

  在日本，一个常见的做法是每年补贴的大部分以半年奖形式付给工人。为此，日本的零售信用卡使用让消费者可以在一定销售点指定用奖金支付货款。结果，商家销售点系统可以指定购买为奖金支付，信用卡授权网将这个信息返回发卡银行。随着日本电子商务的增长，Internet 商务软件也将支持这个功能。

这两个例子都是影响 Internet 商务软件的小问题。新的验证过程要求订单窗体的用户界面提供新字段，新功能要求事务数据库有新的存储字段，支付处理界面要将其他信息路由到财务授权网络。这种复杂性很难管理，但成功的商务必须正确处理这些细节。

14.3.3 支票

支票是人们熟悉的另一种实际支付方式，消费者和公司都用支票支付。消费者用支票进行销售点支付和计账支付。当天用支票支付之后，商家将其存到银行中，通过实际资金转账的联邦储备网进行清理。清理可能需要几个工作日，在此期间商家要承担客户账上没有支票所要求金额的风险。由于商家要承担付不起账的风险，因此通常要求客户提供重要标识，如驾驶执照和信用卡，用于验证客户。此外，商家还要考虑支票无法清算的风险，这些风险包括商家处理返回支票的成本以及银行向商家收取的费用。

由于涉及票据移动，因此支票处理对商家和银行都比较昂贵。现在电子支票已经出现，将在稍后介绍。实际中，信用卡和借方卡在联机事务中比电子支票普及得多。借方卡提供给客户的功能与支票相近，奖金立即从需时存款账号中立即扣除（但注意，这个资金从账号中立即扣

除，而没有支票提供的“浮动期”）。

14.3.4 电子转账与自动清算

电子转账（EFT）直接在银行账号之间转移资金，提供当天支付或隔夜支付。例如，电子转账常用于大型银行间互转。电子转账系统是最早的电子支付系统之一，但总是在专用网络上，而不在 Internet 之类的开放网络中使用。

电子转账在SWIFT、FEDWIRE、CHIPS和ACH等各种网络中移动，前三种主要用于大型转账，而自动清单（ACH）用于许多小值支付，以及公司的联机支付。对于许多商家对商家商务应用，ACH提供了熟悉的支付方法，可以集成到 Internet 购物中。

ACH转账也在家庭银行和支付应用中使用，其中收款人的银行账号信息是已知的。

14.3.5 购买订单

严格地说，购买订单不是支付机制，但我们用其指公司之间的特种事务。两个公司之间的事务通常不同于消费者购物时的处理。大多数情况下，卖方扩展买方的信用，卖方对买方的事务记账，商定购买方何时支付（如 30 天或 60 天内）。特定购买通常与购买订单相联系，买方用其跟踪事务。从卖方角度看，购买订单只是跟踪事务的方便方式，最后支付通常用支票或网上转账完成。

这个功能如何在联机世界中实现呢？首先，要建立扩展信用的业务关系。卖方通常有一个验证买方信用度的过程，这个过程通常也扩展到联机事务。初始验证通常不是实时完成的，因此可以通过现有通道处理，也可以用联机注册系统启动关系。这种联机信用应用过程要捕获卖方的传统信用应用过程需要的信息，通常包括公司名和地址、购买合同、信用参考信息。此外，联机系统还要从客户公司收集验证授权买方的信息（如口令）。当然，联机系统应能导入现有关系信息，使当前客户也能在线购买，然后用验证数据补充现有信息，标识在线购物的客户。

建立关系之后，在线购买与其他联机事务差不多。但是，在订单捕获过程中，系统不是收集信用卡号之类的支付信息，而要收集购买订单号（或其他买方参考信息）以及验证买方，保证只有授权买方才对特定组织进行购买。此外，系统应能实时检查，保证购买请求在买方组织的信用额度之内，以免说组织信用透支或无法及时付账。这个验证与授权信用卡事务时的信用检查相似，但是在销售组织内部进行的。为了向客户提供良好服务，系统还可以处理应急请求，增加可用信用，卖方迅速响应，在适当时候允许进行该事务。

最后，在线购物系统还要集成到现有计账与应付账系统，生成与跟踪相应账单与发票。这些系统也可以扩展到 Internet 系统，对客户提供账号结余、欠款额等更新信息，同时用信用卡、电子支票之类的联机支付方式处置未偿清结余。

14.3.6 亲和项目

亲和项目在从特定公司购买或用特定支付机制购买时提供某种好处或回报。常客旅程卡就是一个例子，购买产品（机票）提供一些点数，以便将来回报（通常是另一张机票）。信用卡的许多签发者也提供亲和项目，包括奖现金、购买特定产品类别的点数、在特定商店购买的点数。当然，这些项目的目的是为了增加支付系统的使用或特定公司的销售额，所有这些项目可以作为 Internet 商务策略。Internet 商务中的亲和项目有三大部分：收集与跟踪累计分数，让买方联机使用这些点数，让买方联机看到亲和账号平衡。

收集与跟踪累计分数通常很简单，主要问题是在现有系统中集成管理亲和项目的跟踪系统。对于联合品牌信用卡，这通常是透明的，因为使用这种卡的任何信用卡购买都会增加点数。点数与特定项目或特定商店有关时，会计功能要加进联机事务系统中，然后集成现有亲和跟踪系统。

第二，买方联机收回这些点数，根据 Internet 商务系统选择的软件，这个工作可难可易。从某种意义上，得到点数只是另一种支付方式，因此适应多种支付机制的系统通常能方便地处理这个功能。当然，还要验证以保证购买者是合法账号拥有者。这时，主要的问题是项目以美元之类的传统货币定价，还是使用亲和点数。有些商家不喜欢用两种方式定价，因此没有点数与币值之间的隐式转换比率。有些则愿意用两种方式定价，对货物提供两种标价单。有些 Internet 商务系统将支付机制与产品目录紧密联系，不提供增加补偿系统所需的灵活性。

最后，买家可能要联机检查亲和账和结余。这些 Internet 系统要与亲和账号系统相联系，还要用某种验证机制保证买方身份。为了方便（或促销），在线账号报表可以链接对补偿点有用的产品目录页，以鼓励买方使用这些产品。

能够支持亲和项目在 Internet 商务策略开始时好像并不重要。但是，前面曾介绍过，随着时间的推移，业务模型和要求可能大为改变，增加亲和项目的灵活性可能对选择 Internet 商务系统软件非常重要。

14.3.7 专用标签卡

许多公司，特别是 Sears Roebuck、J.C. Penney 和 Macy's 之类的零售商签发自己的购买信用卡。抽象起来，这些卡与 Visa、MasterCard 之类的支付卡相似。实际上，用这些卡作为 Internet 商务的支付工具就是集成 Internet 系统与所用卡的支付系统。主要技术步骤（如授权、处置、信用等）和其他信用卡一样处理。Internet 商务系统的灵活性是这里的关键，因为在系统中集成这种支付卡通常是对特定卖家处理的，而不是作为一般方案的一部分。

最近，许多零售商开始签发联合品牌的 Visa、MasterCard 信用卡，通常在卡中增加一些亲和好处。当然，这些卡在支付过程中和正常信用卡一样。联机购物时可能有一些特殊的亲和特性，如特殊产品目录或联机账号报告，见前面关于亲和项目的介绍。

随着时间的推移，我们可能看到专用标签卡在事务中采用SET之类的信用卡支付协议，利用这些协议方面的基础结构投资，同时提供比没有专业化开发时更大的安全性。

14.3.8 现金汇票

现金汇票与支票相似，但信任第三方（如美国邮政服务局）保证支付。现金汇票的主要目的是在邮购事务中保护商家，避免远程客户不良支票的风险。客户向邮政局付钱（包括小量费用）以取得现金汇票，然后可以将现金汇票发给商家，得到邮局的补偿。现金汇票比邮寄现金安全，因为其只能由现金汇票指定实体赎回。在现实世界中，现金汇票提供三个基本功能：

1. 某种丢失的保险（如相对于邮寄现金）。
2. 一定的隐私和匿名性（不如现金，优于直接用信用卡）。当然，大多数现金汇票都用于邮购商品，因此现金汇票总是有对应的实际发货地址。
3. 不同支付工具的买方与卖方之间匹配。例如，如果邮购商家不接受信用卡，则客户可以用信用卡购买现金汇票，然后用其从这个商家购买商品。

在联机现金汇票系统中，第一个功能不太重要，因为正确指定联机支付系统不会有丢失现金的风险。但是，匿名属性可能更强，特别是发送数字商品时。由于不需要相关的实际姓名和地址，因此卖方只能将事务与网络上的 IP 地址相联系。现金汇票的签发者至多知道卖方和可能知道买方（根据使用的实际支付工具）。这种签发者可能对这种信息的披露采用不同政策。签发者遵循这些政策时，买方和卖方都可以相信事务有一定隐私性。

14.3.9 公司购物卡

许多公司的购买都是较小宗的，如办公用品、个人计算机现成软件等等。这些购买通常需要方便快捷地完成，通常不太需要公司其他人的批准。这种情况下，比起购买成本来，填写申请表、建立购物汇票、选择厂家、建立信用关系（如果还没有）、收到发票和付账的开销显得太大。

解决这种问题的一种方案是用公司购物卡。公司购物卡实际上就是对公司的每个人签发的信用卡，通常，它与信用卡相似，只是大多数事务需要一些关于所购买商品的信息。这个信息使授权机构可以根据商品类型和购买公司的可用信用进行决策。例如，一个人可以购买基本办公用品，而另一个人还可以购买个人计算机软件。只要一切就绪，买方出示信用卡，即可授权事务，完成买卖。

在联机世界中有效利用公司购物卡需要能够捕获这些所购商品的信息。如果没有这些信息，则授权系统无法确定持卡人是否有权进行这项事务。前面曾介绍过，支付系统的灵活性（这里就是连接产品目录系统中的特定项目信息）对有效利用公司购物卡非常重要。

14.3.10 优惠券

一般来说，优惠券就是对特定条件下的购买提供折扣。制造商的优惠券是最常见的，提供“五折优惠”或“买一送一”。各个商店可以发出自己的优惠券，有时可能接受竞争对手发来的优惠券。优惠券的形式多种多样，目的都是鼓励客户购买特定产品。大多数情况下，优惠券与产品销售点是分开发布的，帮助吸引客户到商店购买。

当然，严格地说，优惠券不是一种支付机制，但与支付具有一些相同的特征。大多数情况下，可以把优惠券看成改变商品或服务的最后价格，而不是支付这一部分的价格。这时，可以用任何支付机制进行购买。

介绍实现优惠券的技术方法之前，先要介绍几种不同的优惠券。优惠券通常由两种机构印发：制造商与零售商。来自制造商的优惠券通常可以由卖这个产品的任何零售商接受，价值由制造商补偿，而零售商发出的优惠券则只能在这个零售店使用。有时，竞争对手也接受这个优惠券，但价值不是由印发者补偿。优惠券提供的折扣相差很大，下面是最常见的形式。

- 固定折扣
  商品价格采用固定折扣。例如，“购买 X 产品五折优惠”。
- 百分比折扣
  商品价格采用百分比折扣。例如，“购买 Y 产品 20% 优惠”。
- 买一送一
  如果购买同一种产品，则第二件商品的价格减为 0。这种优惠有许多形式，如“买一件，半价送一件”，或“买两件，白送一件”。
- 买 X，得到 Y 折扣
  这种折扣将两种产品联系到一起，购买第一种产品时，第二种产品折扣销售。
- 买 N 送一
  这种情况下，折扣取决于重复购买历史。常见的方法是给客户提供一张卡，每次购买打一个孔，卡打孔满之后，即可取得折扣。

当然，优惠券还可以采用许多其他方式，上面列出的只是最常见的方式。问题是，如何在联机世界中实现这些优惠呢？一种办法是提供基本形式折扣规则，“如果满足一定条件，则一组商品的总价以特定方式改变”。例如，固定折扣的形式是，“如果购买 X 类型的商品，则将价格进行固定折扣”。而固定折扣的优惠形式是，“如果购买三件 X 类型的商品，则总价是一件商品价格的两倍”。

尽管这样看待优惠券的折扣规则显得很笨拙，但可以据此编写能够由计算机系统自动处理的联机优惠券规则。优惠券机制也可以更加一般化，允许用不同促销方法确定吸引销售的最有效方式。

14.4 智能卡

智能卡的大小跟信用卡相仿，包含处理器、内存及与外界的接口。智能卡也指具有相似属性的PCMCIA设备，大小像信用卡的卡也称为芯片卡。智能卡的用途不断增加，包括支付。我们把智能卡与第 14 章介绍的手持验证代用券区别开来：智能卡提供数据存储，通常还可以根据数据进行计算，而不像代用券一样只是进行比较简单的验证计算。

实际上，卡上有多种智能，差别在于处理器性能与功能、内存与ROM大小、接口速度、可用加密操作组件和能否对不同应用程序进行编程。不同应用程序需要不同操作，因此一定要准确指出应用程序和所用卡的类型。

智能卡必须有某种阅读器，将卡与计算机系统连接。阅读器有几种，取决于所用的技术。芯片卡通常有外部接头，匹配插入槽中的阅读器。这种方法常用于零售销售点终端使用的智能卡。有些卡是无接头的，用红外通信与阅读器交换数据。当然，PCMCIA智能卡用便携电脑或桌面计算机上的标准PCMCIA槽。但是，不管用什么机制，使用卡的站点都要有阅读器。对于传统零售应用，阅读器可能连接现金寄存处。对于大楼访问系统，阅读器安装在门上。对于 Internet 商务，智能卡持有人使用的计算机应有卡的阅读器。随着时间的推移，PC机可能装上智能卡阅读器，实现许多验证应用，包括支付事务，但目前这还是 Internet 商务中使用智能卡的巨大障碍。

抽象起来，智能卡提供几个功能。

- 便携式存储
  由于卡是拥有者带着走的，因此可以在拥有者所到的任何地方使用。具体地说，卡中存放的信息可以在拥有者所到的任何地方使用，使拥有者不必连接桌面计算机即可使用高级支付系统。
- 安全存储
  智能卡可以对存储的信息提供安全的防篡改存储。这对加密密钥、金额数据等以及其他专用信息内容特别重要。
- 信任执行环境
  智能卡不会像桌面计算机一样受到病毒与侵入的威胁。由于应用程序在保护环境中运行，因此更加可以信任。

目前常见的应用包括：

- 预付电话卡
  这个用途不需要非常复杂的卡，主要技术是芯片上的一组电子保险，是由阅读器逐渐烧掉的。全部烧完之后，预支付就用完了，卡就没有用了。

- 信用卡与借方卡
  在美国用得不多，但在其他一些国家很普及。卡上的芯片在零售销售店验证这个卡，持卡人还要提供个人标识码进行验证。智能卡提供了比易于伪造的磁带条更大的安全性。
- 电子钱包
  几个电子支付系统（如Mondex与Visa Cash）用智能卡作为系统中的储值工具，目的是在小事务中替代现金，在卡上存储可充值的金额。有些技术要求金额值只能从卡转到授权厂家，而有些（如Mondex）则还可以在卡间转钱。后者的功能使用户可以相互支付商品或服务费，就像使用现金一样。

许多其他智能卡应用还在开发，包括简单的储值与验证系统和复杂的用公用密钥系统签名与加密文档和支付工具。

历史上，生成智能卡应用的一个问题是缺乏与设备通信的标准接口。RSA实验室领导开发了PKCS-11标准，指定了智能卡之类加密设备的API。这个API也称为Cryptoki，表示各种设备的技术独立视图。

同样，Sun系统公司用Java Card API通过Java编程语言开发智能卡应用。标准编程接口的使用使基于卡的应用可以在许多不同卡上运行，而不必一一编程。许多人还在寻求多应用卡，即可以在许多不同情境中使用（如不同支付系统、医疗记录、验证，等等），而不是要求人们不同场合用不同卡。公用编程接口（这里是Java）使这种多应用设备更容易生成④。

智能卡在Internet商务应用中以两种方式出现。第一是在Internet客户端用智能卡支持标准协议（如SSL与SET）。这里从服务器方看是一样的，因为协议是标准。客户可以用多种不同方法采用智能卡，取决于应用程序的安全要求。一种用法是验证对桌面计算机上所存储加密证明信息的访问。第二种用法是将卡放在协议信息处理中，在卡上执行协议或用卡进行加密操作（如数字签名）和存储协议使用的密钥与证书。

Internet商务应用中使用智能卡的另一种方式是开发新协议，利用智能卡的特殊功能，特别是加密操作和密钥存储。有时，加密硬件使用的应用要求也包括服务器方的这种硬件和智能卡的使用。这种方法对生成高度安全的应用非常有效，但会大大增加总体开发成本。

前面曾介绍过，Internet商务中使用智能卡的最大障碍是，商务中使用的计算机不一定有读卡器，无论是家庭还是办公室中的计算机。随着读卡器成为普及设备，Internet商务系统必将更多地利用智能卡。在此之前，Internet系统中智能卡的使用受到限制，只适用于需要智能卡的安全要求的专门应用。

---

④“一卡多用对持卡人很方便。但有两个问题：一个卡中有多个应用程序可能把人们要分开的应用程序放到一起（例如信用卡与医疗记录是不需要连接的），因此可能产生隐私问题。第二，带微标的卡是一种促销手段，发卡人不喜欢放弃促销，加入使用其他公司微标的多用卡。

14.5 Internet 支付系统

Internet 的商务发展使系统针对 Internet 商务的支付系统应运而生。

14.5.1 第一虚拟银行

第一虚拟银行（FirstVirtual）开发了 VirtualPIN 系统，用电子邮件确认购买。客户购买时，要向厂家提供第一虚拟银行账号。厂家将事务提交到第一虚拟银行，银行请求买方用电子邮件确认。买方可以确认购买或指出可能是欺诈。这种模型常用于数字商品，但有些第一虚拟银行商家也销售有形商品。详见 http://www.fv.com。

14.5.2 CyberCash

CyberCash 是 1994 年由 Dan Lynch 与 BillMelton 创建的，这个公司的主要方向是 Internet 商务支付技术。CyberCash 操作支付服务器和网关，将 Internet 与外部财务网络连接起来。公司业务模型是作为支付服务提供者，根据事务收费，而不是作为软件厂家。

信用卡

CyberCash 于 1995 年推出信用卡服务。信用卡服务模型实际上与 SET 相同，见稍后“安全电子事务”一节。买方下载与安装钱包应用程序，这个程序与商家的“现金寄存器”模块交互。支付工具发送到 CyberCash 网关，网关将其中继到标准信用卡授权网络。CyberCash 服务的信用卡部分正在转入支持 SET。

CyberCoin

1997 年初，CyberCash 引入了货币服务，用于小额支付。预订者用传统财务手段买其货币，然后 CyberCash 承认其价值。Internet 支付使用货币服务时从客户账号借取，并贷入商家账号。后面商家可以将累计金额转到普通银行账号中。

CyberCash 支票

1997 年初，CyberCash 引入 PayNow 电子支票系统，允许从需时存款账号立即支付，而不必先把钱转到暂管账号。效果上，支票的支付功能在网络上传输。这个系统与家庭银行应用的写支票部分不同，支付发生在销售点。这个系统对产品购买有用，对联机计账支付更加有用。

在联机计账支付中，CyberCash 称为交互式计账与支付，公司通常用邮件将账单发给客户和接受邮件返回的支票支付，而这里是两个活动都用 Internet。在第一个账单提供阶段，厂家用交互式 Web 站点向客户显示账户的详细报表。在支付阶段，客户可以用 PayNow 支票服务付账。厂家避免邮寄账单的成本，而客户不需要写支票和邮寄支票。

14.6 联机信用卡支付

信用卡已经成为消费者在Internet上支付商品与服务费用的最常用方法。这是不足为奇的，因为许多 Internet 事务与邮购事务非常相似。对消费者而言，信用卡是熟悉的支付方式，信用卡系统可以降低出错时对消费者的风险。从技术角度看，建立处理信用卡购买的系统比发明全新的支付技术要容易得多。最后，从公司角度看，许多想在线做买卖的商家已经接受信用卡，因此不需要建立与银行的新关系就可以利用在线机会。

14.6.1 安全通信

Internet 上的第一个信用卡事务是没有防止窃听的。早期事务用电子邮件、Telnet 和 W W W 发送信用卡号（与相关信息），没有加密和保密。随着电子商务系统更加广泛采用（主要是在 W W W 上），系统设计人员采用另外两种方法：通过电话取得客户的信用卡号而不是通过 Internet 取得，或开发传输这个信息的加密系统和安全协议。W W W 上最早的两个加密协议是安全 HTTP 与安全套接层（SSL），目的就是支持商务应用。

对许多信用卡应用，使用 SSL 等协议的强加密提供了高度通信安全⑤。应用程序的开发得到简化，因为应用程序不需要提供其他安全性或管理复杂协议。

14.6.2 安全电子事务

安全电子事务（SET）协议是 Visa 与 MasterCard 和一些技术伙伴联合开发的，在 Internet 之类的开放网络上提供安全信用卡事务。这个协议对信用卡事务的各方提供强加密和验证：买方（或持卡人）、商家和商家银行。尽管 SET 还处在早期开发阶段，但必将成为 Internet 中处理信用卡事务的标准。

SET 规范 Business Description 部分指出，SET 的设计宗旨如下：

1. 提供支付信息的保密性和支持与支付信息一起传输的订单信息的保密性。
2. 保证所有传输数据的完整性。
3. 提供证明持卡人为相应支付卡账号合法用户的验证。
4. 提供商家能通过与查询财务机构关系接受该支付卡事务的验证。
5. 保证用最佳安全政策和系统设计技术保护电子商务事务的所有合法参与方。
6. 保证建立不依赖于传输安全机制也不阻止使用传输安全机制的协议。
7. 帮助与促进软件与网络提供者之间的互操作性。

为了达到这些目的，SET 还可以用 Internet 授权和处理信用卡事务以及启用从持卡人到商

⑤第 12 章曾介绍过，通用通信软件出口级加密提供的安全性对财务应用是不够的。

家的支付信息安全通信。前面曾介绍过，如果没有SET，则商家通常用租借电话线或拨号连接联系查询银行（或其他财务处理者）。SET使商家可以用 Internet 连接进行联系，从而避免增加费用（但注意，这种方法也有一定的缺点，见稍后介绍）。

此外，由于SET强调加密财务证明信息，因此要从美国出口用强加密法实现的方案，同时又不能违反美国政府的出口规定（第12章详细介绍了加密软件的出口规定）。图14.2显示了SET事务的框图。发生事务之前，商家和客户要取得软件与证书以建立SET事务。商家与查询银行交互，取得SET商家证书。该公用密钥证书用查询银行的密钥签名，查询银行的密钥又是用卡品牌密钥签名的，这个证书在事务阶段向持卡人和支付网关验证商家。同样，消费者与发卡银行交互，取得由发卡银行签发的证书。协议中持卡人的证书是可选的，但可以用于在实际事务期间向商家验证持卡人。

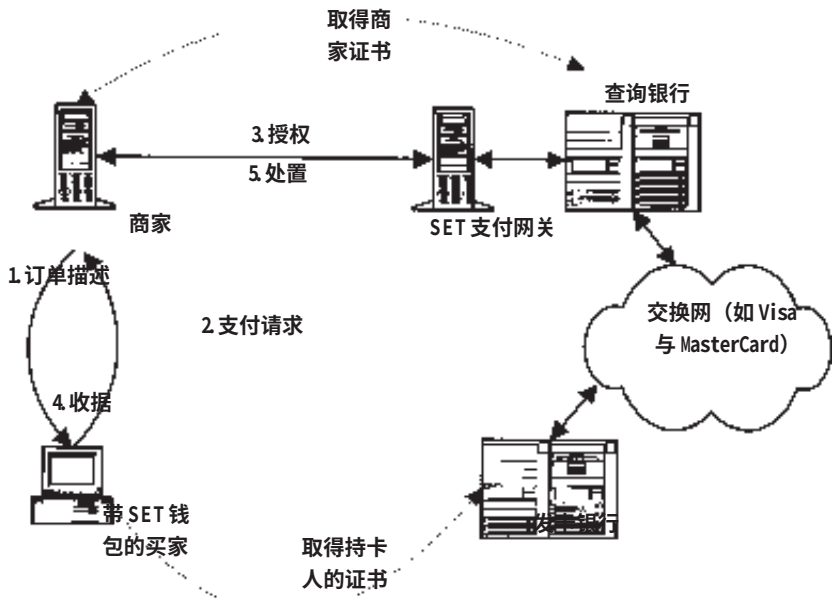


图 14.2 SET 事务的框图

事务期间所进行的步骤如下：

- 客户与商家 Web 站点交互，选择要购买的商品。
- 商家发送订单描述唤醒客户的 SET 钱包。
- 客户检查订单并将支付请求发回商家的 SET 模块。
- 商家将支付请求发给支付网关。
- 支付网关验证商家和客户，通过交换网取得客户发卡银行的授权。
- 支付网关将订单捕获令牌返回商家。

- 商家将收据发给客户钱包。
- 商家用订单捕获令牌处理事务。

SET的协议定义指定了使用的消息格式、编码和加密操作，它不要求特定传输方法。因此SET消息可以用WWW应用程序的HTTP、电子邮件或其他方法传递、消息不需要实时交换，从而可以根据电子邮件或其他异步系统实现有效的SET版本。

14.7 电子现金

一般来说，电子现金技术以电子形式模拟现金。电子现金系统在联机事务中复制现金的许多属性：方便、低价（无事务成本）、匿名，等等。尽管不是所有电子现金系统都满足所有这些属性，但大多数系统对小笔金额提供方便快捷的联机事务。

有些电子现金系统要求用智能卡操作（具有处理器和内存的卡），而有些则可以完全在软件中操作（但使用智能卡硬件可以增加安全性）。使用智能卡时，丢卡就等于丢钱，就像丢失20美元的钞票一样。卡就是钱，应像钱一样保管好。软件系统可以提供存储体中所表示金额的备份，但丢失所有备份还是等于丢钱。

14.7.1 Visa现金

前面曾介绍过，传统信用卡的一个局限是事务成本相对较高，因此不适合小事务。为了解决这个问题，Visa开发了现金卡，可以用于低价商品、商店、售货机和其他场合。卡中有个处理器和千字节内存。处理器能够进行借卡和防止假冒所需加密操作的功能。有些卡只能用到没钱为止，而有些则可以充值。

卡与读卡器之间的通信是安全信道，因此这个技术目前不适合开放网络上的事务。

14.7.2 Mondex

Mondex是National Westminster Bank与英国的Midland Bank联合投资的。在Mondex系统中，用智能卡持值，可以在客户卡与商家终端之间转钱，通过正确安装的电话线从银行向客户的卡转钱或在个人拥有的两张Mondex卡之间转钱。

1995年在英国的Swindon市部署了Mondex系统的测试版。

和Visa现金卡一样，Mondex系统最初不是用于Internet之类开放通信网络上操作的，但迅速在Internet中采用。1997年，AT&T Universal Card Services公司和Hewlett-Packard Mondex与Open Market一起开始在因特网商务中试用Mondex系统。关于Mondex的详细信息，见http://www.mondex.com。关于AT&T Universal Card Services的试验信息，见http://www.att.com/mondex。

14.7.3 Digicash

Digicash 是基于 David Chaum 所开发的技术的电子现金系统。Chaum 开发 Digicash 的目的是尽量接近现金的属性，特别是匿名性和不可追溯性。与 Mondex 不同的是，Digicash 不要求智能卡。结果，Digicash 开发了探测所谓双向花费的方法。如果电子货币只花费一次，则各方保持匿名。但如果同一电子货币在银行中存两次，则可以跟踪复制金钱者的身份。

1995 年 10 月，圣路易斯市的 Mark Twain Bank 成为第一家签发 Digicash 电子货币的银行。1997 年 10 月，德意志银行开始在 Internet 上试用 Digicash。详见 http://www.digicash.com。

14.8 微型支付

微型支付有许多不同含义。微型支付的大小通常取决于使用者的平均或通常支付额。这样，对于公司事务，微型支付可能指 100 美元以下的支付；而对于信用卡系统，微型支付可能指 10 美元以下的支付。一般来说，微型支付指小额事务（几个美元以内）。大多数情况下，微型支付也用于联机发送，例如，50 美分的杂志文章。

纳米支付则指比微型支付还要小得多的事务，如不到一便士的支付。

14.8.1 微型支付的业务模型

从业务角度看，微型支付最明显的一点是需要形成批量。算法很简单：如果平均事务大小为 50 美元，则需要有两百万个事务才能得到毛利一万美元。这个毛利还要扣除计算机处理事务和填写订单的成本、处理微型支付的软件成本、操作人员工资、电气与空调费，等等。在 Internet 商务的这个演变阶段，微型支付系统通常还是入不敷出。

微型支付也可能在小规模上取得成功。假设一个人（不是专业作家）在 Web 上发表政论散文，如果有一万个读者愿意每篇文章付十美分，则这位作者可以得到 1000 美元的收入。即使扣除微型支付系统的高操作成本，作者还是收入不错，而且可以通过这些文章扩大曝光面和知名度，但这种收入要维持出版行业显然是差远了。

微型支付系统的技术方面是动人而富有挑战的，微型支付系统支持者描绘了美好的未来。也许有一天，微型支付系统将成为 Internet 商务的常见形式，但目前离开发和部署成功的微型支付系统还有一段距离。

14.8.2 技术性微型支付系统

有许多技术性微型支付系统正在开发或已经发布。由于这个技术迅速变化，因此进一步研究的最好方法是在 Internet 搜索引擎中输入“ micropayment ”。下面简要介绍几个微型支付系统。

Millicent

Millicent 是数字设备公司 PaloAlto 系统研究中心的 Mark S.Manasse 设计的。图 14.3 显示了 Millicent 系统中的实体与关系的视图。Millicent 生成商家特定的代币券，只能在特定商店买东西。代理提供了一定的厂家独立性，可以为多个商家销售代币券。Millicent 用加密法保护系统，防止末端用户滥用，如伪造或重复使用代币券。系统中的其他实体也有一些保护，Millicent 提供的保护不是牢不可破的，因为这个系统用于低值事务，系统没有提供事务审核与收据。Millicent 设计中心也对各个 Web 页面交换代币券，偶尔下载失败时不受保护。这个模型与售货机相似，如果偶尔丢失一枚硬币，大多数人会投进另一枚。详见 http://www.millicent.digital.com/。

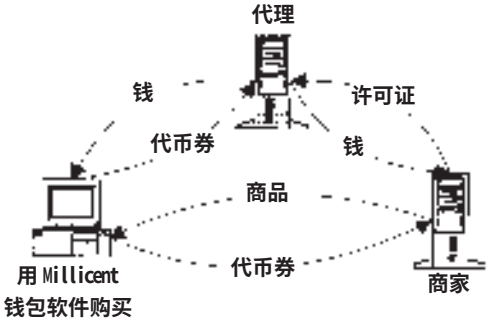


图 14.3 Millicent 系统设计

NetBill

NetBill 是 Carnegie Mellon 大学的 Marvin Sirbu 与 Doug 开发的系统。NetBill 对数字化商品提供支付与事务发送功能。事务指的是支付与发货或者都进行，或者都不进行。图 14.4 所示的系统设计不可能发生发货而不支付或支付而不发货的情况。

购物之前，NetBill 客户下载和安装 MoneyTool 钱包应用程序，可以在 Web 浏览器中使用。客户还要用信用卡之类的传统支付系统购买 NetBill 货币。客户结余存放在 NetBill 服务器中。

为了购买，步骤如下：

- 客户浏览商家站点并选择要购买的数字商品。
- 商家系统向客户下载商品的加密版本和价格与时间标志。
- 唤醒客户的 MoneyTool 资金，建立电子支付订单（EPO），包含价格、校验和、产品 ID 和时间标志，用客户、加密密钥签名。EPO 发送到商家服务器。
- 商家服务器发送电子支付订单和商品解密密钥到 NetBill 服务器。
- NetBill 服务器在同一事务中验证 EPO、借方账号、贷商家账号，并记录解密密钥。这一步保证购买最终成功。
- NetBill 服务器向商家返回成功消息，商家将解密密钥发给客户。
- 客户解密和浏览商品。

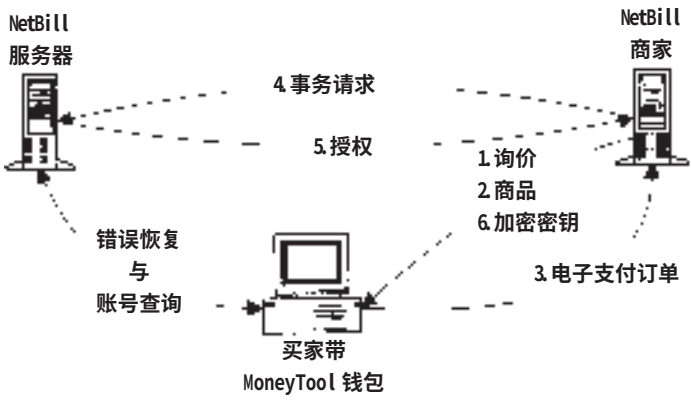


图 14.4 NetBill 系统设计

如果客户无法取得解密密钥或出现其他故障，则客户可以直接与 NetBill 服务器通信，取得密钥或确定事务没有记录（钱没有花出去）。

关于 NetBill 的细节，可参见 http://www.netbill.com/。

14.8.3 累计

技术性微型支付系统要解决的业务问题是不值得用信用卡授权的小额事务。有时，也可以用事务累计解决这个业务问题。使用这种方案时，小额事务组合成足够大之后再用传统支付系统处理。累计方式有两种：出租车表或停车表。

在出租车中，收费包括车程和等待两部分，最后都要由乘客支付。出租车表方式也称为费用增加事务累计。原理是相同的客户账号的费用累计，直到到达阀值，或到达会话结束或计账期结束。这时用传统支付系统支付总计费用。在这个系统中，卖方向买方扩展信用，但数额很小，因此风险不大。卖方也可以等买方支付之后再继续买卖。在出租车表方式的一种变形中，可以在会话开头进行授权（或信用保留），最后知道真正费用时再结账。

在停车表方式中，驾驶员将车停在停车场，向停车处上方的仪表里投放硬币，然后账号里的存款不断减少。停车表方式也称为下拉事务累计，原理是相同的：买方用传统支付系统预付一定奖金，然后从账中借款。在这个系统中，买方而不是卖方承担风险。

这两种操作方式的一个有趣的差别是风险的分配及其后果。由于停车表方式中买方承担风险，因此可以向匿名客户提供这个系统。相反，出租车表方式由卖方承担风险，因此通常只能向注册验证买家提供。

事务累计通常是一个买方和一个卖方之间的协议。技术上，微型事务累计账号可以由多个卖方共享，但这是否合理取决于系统报表功能而不是别的因素。累计系统可能只报告总和或具有微型事务本身的完整事务细节报表功能，提供的报表程度通常是事务规模的函数。通过计算

设备与基础结构成本，可以计算事务的成本。支持事务细节报表功能所需的数据存储量会大大增加事务成本，因此事务细节报表功能只对大量微型事务才合理。

14.9 抽象支付

本章的大部分介绍针对商品或服务支付的转钱系统。但是，实际中的许多商务是在与支付完全分开的环境中工作的。

14.9.1 商家对商家

例如，大多数商家对商家商务的过程是这样的：

1. 两个公司建立商务关系，卖方同意对买方扩展信用。
2. 购买组织取得销售组织的商品或服务。
3. 卖方定期向买方发送账单。
4. 买方用支票或其他转账方式付账。

在这个模型中，支付是一个财务部门与另一个财务部门之间的功能，与实际购买没有直接联系。本章介绍的许多实际和 Internet 支付系统把授权与处置放到一起。信用卡系统在一定程度上将其分开，但授权与处置还是一一对应的。在商家对商家商务中，授权与处置之间没有直接联系，下面再对这个事实作一解释。

- 卖方同意对买方扩展信用。
- 购买时，采购员要证明自己是买方的代表（有时买方要通过某种内部机制批准购买）。这个步骤等于信用卡授权。
- 后面财务部门协商并处置已经发生的事务。

这里买方授权给采购员。抽象起来，这种授权与钱相似（注：Dan Geer 解释了委托与钱之间的联系）。

14.9.2 信息商务

信息的专业化用户（如律师、银行专业人士和会计师）经常从事信息商务，为别人的知识和经验付费。例如，律师使用 Lexis-Nexis 或 WestLaw 联机服务或预订注释案例法的光盘。

这些信息商务事务很少直接用信用卡或现金支付。

1. 律师楼建立与案例法商务出版公司的计账关系。
2. 例如，要进入联机法律信息服务，律师要登录、验证自己和输入账号码。这个号码用

于后面对向律师提供的服务计账。

3. 律师使用信息服务时，生成计账事件并发表到律师楼的账号。

4. 出版公司定期将账单寄给律师楼，列出各个应计项目，并可能加上标识。

5. 律师楼向出版公司支付。

6. 客户向律师楼支付。

作为商家对商家的例子，信息事务与支付不是直接联系的，而是将授权与处置分开，买卖双方最初要建立商务关系。事务过程中，验证或批准步骤提供事务授权，而处置则放到后面。

14.10 小结

许多人以为 Internet 商务问题都是与支付相关的，其实不然，但支付是许多商务系统的重要组件。全球使用的支付系统非常多，具有各种处理授权与处置问题的方法。此外，商家对客户、商家对商家和信息商务常常使用不同的系统。支付是个不断变革的领域，正如介绍微型事务时所说的那样，新技术不断涌现。因此，Internet 商务体系结构必须在支付技术方面足够灵活，同时设计人员又要了解管理信任与风险的技术和业务问题。

第 15 章辅助系统

上帝是细致的。

——俗语[①]

15.1 幕后的细节

本章介绍完整 Internet 商务系统中必须解决的几个商务问题，如税收、后勤和库存管理。只接受订单的 Internet 系统可以避免这些问题，但如果系统的目标是提供可靠性、显示精确价格和符合税收法律要求，则必须考虑这些问题。

实际中，这些问题只是反映了现实商务中的问题。由于 Internet 商务是从现有业务发展起来的，因此这些问题显然应作为系统的一部分。但是，即使因 Internet 机会而建立公司，也要解决税收、后勤和库存管理问题。事实上，测试 Internet 商务软件时就要测试其处理这些问题的能力。

15.2 税收

税收根据法律的规定种类繁多。事实上，许多政府还在争论 Internet 事务应征收哪些税种。如何征收。尽管本书不准备详细介绍税收法律的细节，但下面的例子演示了 Internet 商务系统中处理税收的一些问题。

15.2.1 美国的销售税

美国的销售税是由产品购买者上缴给州政府、县政府和地方（市）的。销售税的规定总共有 6000 多条，而且各级政府不断改变规定和建立新法规。更为复杂的是，数字商品（也称为无形商品）的税收状态仍在激烈争论阶段[②]

在面对面的商务情形中，消费者经常把销售税看成简单问题。商店的现金寄存器会计算应交税并加进账单中。这种简单性的原因是面对面的商务情形中几乎所有变量都是固定的。此

---

①这是建筑师 Mies van der Rohe 的口头禅，据说是福楼拜说的，但真正的来源无据可查。

② “What Are the Sales Tax Consequences of Retail Marketing on the Internet?” K. Lawrence Gragg and Leonard S. Sosnowski, Journal of Multistate Taxation, March/April 1997, See http://www.taxware.com/current/other/JMSTarticle.html.

外，尽管名义上是买方纳税，但实际上是卖方收齐后上缴。

如图 15.1 所示，销售税计算是关于买方、卖方、产品与事务信息的复杂函数。

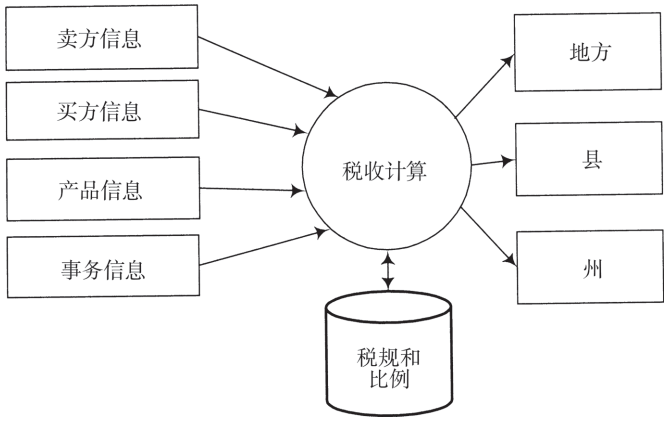


图 15.1 美国的销售税计算

卖方信息

- 关系

  一般来说，商家如果在州中有商务点（或关系），则由商店负责收齐后上缴销售税给州里。商务点是个法律定义，商店或大设施可以算，小型销售办事处则算不上。

- 所有权传递点

  计算税收的工作随购买的商品所有权从卖方传给卖方的位置不同而不同。通常选项是商品发货时传递（在卖方仓库）或商品送达时（在买方地址）。

买方信息

- 地址

  在电子事务中，事务发生在哪里呢？对于邮购或电话购买的事务，事务通常发生在买方地点。对于信用卡支付，买方地址通常与信用卡计账地址相同。这不是最完美的，但简单，而且相当一致。

  然后可以用买方地址确定用哪种销售税率。但是，这种判断不能仅仅依据邮区号，因为邮区号可能跨市界或跨县界。应当把完整地址对应于地区码，这是足以确定适用税收政策的地址。

- 免税状态

  有些非盈利和教育机构不需要支付销售税，购买产品或配件之后进行转卖的公司也不需要支付销售税。购买者通常要提供免税号，供商店记录。

产品信息

- 商品类型
  并不是所有商品与服务都一样收税。例如，在麻省，纺织品和越橘就是不收销售税的。纺织品是生活必需品，而越橘是这个州的主要农作物。为此，各个产品要准确标出产品类别码，以便销售税引擎能确定相应税率。
- 价格
  销售税是按价格的百分比计算的。

事务信息

- 优惠券
  优惠券在特定环境中改变产品的价格。正确的销售税计算是先减价之后再计税。

为了计算税收，要在税收规则引擎中填入所要的全部原始信息，生成向客户显示的总销售税，以及各项细节，便于在商店的税收报表文件中列出。

计算税收是一个相当复杂的问题，Taxware International(http://www.taxware.com/)之类的公司就是专门从事计算税收的。他们提供计算税收模块，并定期提供新的税收法规数据库，提供信息更新服务。

其他

在很简单的情形中，只在一个州具有商务点的小商务可以收集所有事务的销售税，不管实际是否需要这么干。这种方法可能纳税太多，从而增加客户成本，但可以简化商店的工作。

15.2.2 加拿大商品与服务税

加拿大的销售税不像美国那么复杂，但也好不了多少。大多数省都要征收7%的联邦政府销售税（GST），加上各省销售税（PST）（各省的税率不同）。但是1997年4月，有些省改用新的统一销售税（HST），GST和PST合起来共15%的税。和美国一样，税率随商品与服务不同而不同。

从加拿大出口或进口的商品采用特殊规定。作为一般规则，应税商品与服务进口到加拿大时，征收GST/PST。而从加拿大出口商品与服务时，免征GST/PST。所有权传递点是目的地，通常零售就是这样。基本说来，如果发往地址是加拿大，则要计算GST/PST/HST和向买方显示。

详见加拿大财务部Web站点http://www.fin.ga.ca/。

15.2.3 增值税

在欧洲和世界其他地方，增值税（VAT）是政府的主要财源。在销售税中，税收是在消费

点计算的，只有最后消费者才征税。相反，增值税模型则是在商品与服务交易时都要征税。经销商买东西要交税，而卖东西要代征税。一般来说，经销商可以在卖东西时补偿已交的税，因此每个阶段实际上支付的只是增值部分的税收。

和平常一样，税率随不同商品和不同地区而不同，边界规定特别复杂。欧盟决定所有事务在源国家收税，这个过程大大减少了出口与进口文书，但对非最终用户增加了复杂性。欧洲的经销商要对所有销售纳税，但要对采购的每个国家分别纳税，对转销的项目取得增值税退税。

在 Internet 商务系统中正确实施增值税需要下列步骤：

1. 取得必要的输入信息，包括买方地址、商品类别和商店增值税概况。
2. 计算事务应付的增值税。
3. 向购买者显示必要的合法发票。如果购买者是经销商，则必须这样，以便后面申请退税。
4. 准备必要的记录与审核材料，让商家提交给增值税征税机构。

Taxware International 公司的产品WORLDTax进行了这些工作，支持欧盟与其他欧洲国家、加拿大和亚太地区的有些国家。

15.3 发货与处理

发货与处理是后勤工作的一部分。输入订单之后，要将商品发给消费者。从浪费者角度看，这个过程很简单，但其实包含复杂的计价、国际考虑和订单从商店到发货公司的自动化处理过程。

15.3.1 发货与处理计价

发货需要一定的费用，除非这个成本算进卖方的总体价格结构中，否则消费者要承担这个费用。卖方要在发货费中包括这个成本，此外，发货费也可以作为促销工具和竞争武器。

在直销（产品目录销售）中，使用各种发货价格模型。

- 平价
  对于销售各种重量轻、体积小的小件的商家（例如隐形眼镜镜片），适合平价发货。平价包括卖方每个订单的处理费用加上实际发货费用。对于大件，则各个项目可以采用平价收费。
- 基于重量
  对于大件，实际发货费用通常基于重量。这个模型可以传递给消费者。
- 基于价值

基于价值的发货费用（按比例或级进）有一个好处，就是客户易于理解。级进还可以促使客户多买东西，直到接近分级边界。

- 基于距离

  有时实际发货费用是基于距离。这个模型可以和上述任何模型组合，例如建立与价值和距离成比例的模型。

15.3.2 国际运输

Internet 商务的一种结果是带来许多新的国际业务。国际商务比较复杂，加上国际销售与市场的难度，使竞争者较少。由于 Internet 使国际销售得到简化，许多新公司开始面临国际运输的问题。这些困难包括海关问题和国际货运所要求的书面材料。

关税

关税随国家而不同。为了简化步骤，人们采用了统一关税系统分类，是商品贸易的标准化编号系统。对每类产品指定的编号用于全世界的海关官员确定关税、费用和适用于该产品的规定。这些分类的计划见 Web 站点 http://www.census.gov/foreign-trade/www。

书面材料

国际货运以商务发票为中心。商务发票要标识发货人、收货人、货运公司，并描述发货的内容，目的是在一个地方为海关官员提供将产品分类和正确确定海关税费所需的信息。

除了商务发票之外，出口货运和进口还需要各种文书，包括：

- 装货单
- 领事发票
- 原产地证明
- 出口许可证
- 保险证明
- 货运出口声明
- 国际信用证

关于出口文档的完整介绍不是本书要讨论的内容，但可以参考美国商务部出版的《A Basic Guide to Exporting》。

15.3.3 运输与跟踪

货运的大型国内和国际机构很多。Federal Express、United Parcel Service、Airborne 和 DHL 等公司都提供全球服务。对于大客户和许多小客户，这些公司提供取货与发货的自动化系统。货运软件会生成相应标签、指定跟踪号和计划取货与发货时间。

基于 Web 的跟单服务可以从下列公司站点取得：

- Fedex:http://www.fedex.com/
- UPS:http://www.ups.com/
- Airborne:http://www.airborne.com/
- DHL:http://www.dhl.com/

15.3.4 隐私

考虑后勤时，需要考虑几个隐私问题。第一，需要实际货运时，能否进行匿名事务？第二，包裹跟踪服务提供怎样的安全性？

匿名性

信息商务好像可以真正做到匿名。支付机制原则上可以匿名（见第 14 章），但涉及实际货运时事务中要达到匿名是很难的。一种方法是货运公司作为卖方与买方之间的隐私中介。如果买方在货运公司有账号，则买方可以告诉卖方“通过 XYZ 货运公司发给客户 12345”。卖方知道卖什么，货运公司知道卖给谁，但两者都没有完整信息。

第二种可能是货站发送。在货站发送中，发货公司将包裹发到杂货店或包裹公司之类的相邻货站。如果事务用电子现金支付，而且发货是“通用发货”，则可以达到匿名性。

跟踪号

货运公司当前采用的跟踪号有一个问题，就是不太安全。通常，跟踪号是账号加上发货序号，再加一个简单校验和。账号很容易取得，只要从同一公司买点东西并检查跟踪号即可。然后就很容易猜出序列号。

15.3.5 高级后勤

在商务的早期，货运相当简单。你向工厂订购，产品就会从厂里送出来。这种模型可以作为一个好的起点，但不能符合所有后勤要求。例如，我们要考虑仓库选择与虚拟公司的问题。

仓库选择

大公司通常有地区性仓库和只包含某些产品的仓库。这时，订购的产品和发往地址可能影响履约中心的选择。履约中心的选择又会影响货运费的计算。设计人员不喜欢这种相互依赖的情形，否则很难进行模块化设计。因此，在这种情况下，可能使用标准发货费用、匹配或超过实际发货费用。偶然反馈可以用来调整费用。

虚拟公司

虚拟公司的思想在 Internet 商务之前就有了。虚拟公司可以从事各种活动的产品设计、制

造、分配、市场、会计，等等。许多公司不完全是虚拟的，但重要组件依赖于业务伙伴。例如，个人计算机分销商可能制造系统单元，但从另一厂家取得显示器。如果不需要完全系统测试，则可以从一个仓库发显示器，从另一个仓库发系统单元，两个组件分别发送。如果情况好的话，则可以让两个组件在同一时间由同一卡车送达。

15.4 库存管理

在大多数商务活动中，产品的提供在销售中起着重要作用。在面对面商务中，产品就在货架上。在电话订购商务中，操作员通常能访问库存信息。而在复杂的B2B商务中，采用“保证供给”的概念，卖方的企业资源计划（ERP）系统能够完全访问库存、过渡期、原先履约情况、制造能力以及当前和今后履约所需配件的计划到达时间。

库存管理功能将成为Internet商务的标准部分，因为买方要知道能否实际得到订购的产品。如果产品无法立即提供，则买方可能会转到另一家。有时，买方甚至愿意多花点钱也要马上买到。

对于大型销售组织，库存管理的正确方法是集成Internet商务系统与管理所有库存的公司系统。这可以用如下两种方法实现。

- 产品目录集成
  在这个模型中，Internet产品目录系统用库存信息定期更新。产品目录用这个信息标出或隐藏缺货的项目。此外，等待促销和销售的缺货项目保留在库存中。
- 事务系统集成
  在这个模型中，Internet商务事务系统集成到内部公司系统。用销售店的库存确认和保留客户订单窗体中的项目。

这两种方法都可以生成完全集成系统，有效地保证提供产品目录中列出的项目。

大企业可以采用这些技术，但小企业则可能根本没有计算机化的库存系统。Internet的妙处之一就是使中小企业也能像大企业一样处理事务。库存管理方面如何达到这一点呢？使用虚拟仓库是个好主意。

15.4.1 虚拟仓库

虚拟仓库的思路很简单。中小企业将部分库存用虚拟仓库来管理，然后可以用这个分组向客户履约。试考虑下列事件顺序。

1. 小件的小卖主建立基于Web产品目录。由于小件市场取决于买方的满意度，因此一定要保证供给。

2. 每个工作日，卖方用 Web 管理应用程序控制虚拟仓库的一定小件数（如 50 件）。
3. 买方浏览小件产品目录时，产品目录系统用虚拟仓库实时查询取得现有的小件数。产品目录用取得的数量控制行为，选择普通或促销价格。
4. 买方选择要买的小件之后，产品目录系统从虚拟仓库的库存中预留。预留在固定时间有效（如 30 分钟）。这个思想类似于航空订票系统，预留在固定时间有效，到时间如果没有支付，则预留作废。
5. 如果预留时间到达之前已经成交，则 Internet 商务事务系统在虚拟仓库中记录这个事实，确认预留，从分配中取消相应小件数。
6. 卖方可以在当天或定期增加与删除虚拟仓库的库存，但预留的库存无法取消。

这样，小企业不必增加大的费用就可以得到完全集成库存管理系统的好处。虚拟仓库只是书面库存的进销存系统，但客户很满意，因为能够保证发货。

虚拟仓库在边界状态时会失效：如果不是所有库存都进入虚拟仓库，则有些客户可能在实际有货时却无法订购。但是，客户决不会在实际无货时得到送货承诺。

图 15.2 显示了虚拟仓库的逻辑框图。

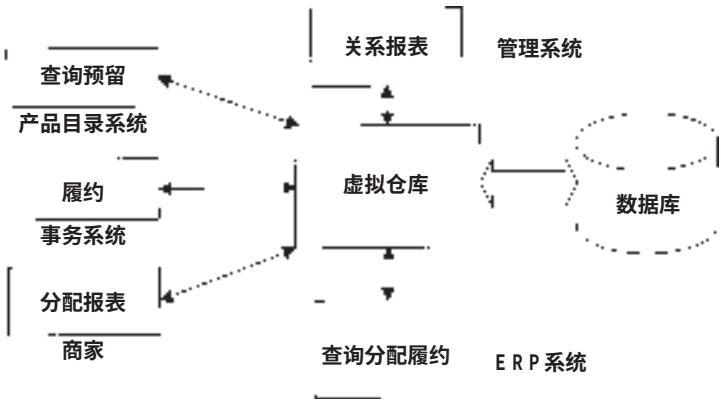


图 15.2 虚拟仓库的逻辑框图

虚拟仓库用数据库存储项目、库存和预留。应用程序以产品目录系统、事务系统、商家、ERP 系统和管理员身份与数据库交互。

产品目录接口

产品目录系统可以查询虚拟仓库中项目的库存状态，对库存采用临时预留。产品目录软件查询确定供货水平，选择产品目录中的相应表示。产品目录系统在选择购买项目（放进购物推车或订单窗体）而还没有确认订单时采用临时预留。

事务接口

订单处理期间，事务系统检查订购的所有项目是否有有效预留。如果有，则确认预留为订单履约的组件。这时，虚拟仓库减少其库存量。

商家接口

中小型商家通过基于Web的接口与虚拟仓库交互。商家可以查询库存量，生成报表，更重要的是可以对仓库分配新库存。

企业资源计划接口

大公司通过ERP系统接口与虚拟仓库交互。这些系统运行业务，能够根据外部事务查询、分配和实现库存改变。

管理接口

为了在公共网络上的共享服务环境中使用虚拟仓库，需要用管理实用程序建立新的商家账号、控制安全参数和报告活动。

15.5 小结

为了取得成功，Internet商务要提供完整的业务方案。如果商务系统是用各个组件组成的，则每个系统操作员要将其组装起来，因此无法达到很强的市场穿透力。完整方案要实现联机商务所需的全部功能，或实时集成外部组件。本章介绍了几个子系统、税收、发货与库存，这是建立功能全面的系统所必不可少的。

第 16 章事务处理

六千年前，苏美尔人发明了记录事务处理的方法。
—— Jim Gray 与 Andreas Reuter [①]

16.1 事务与 Internet 商务

本章有两个目的：介绍事务处理技术与 Internet 商务的关系，和几个与商务应用程序完整性和整体性有关的问题，如备份与灾难恢复。

Internet商务的目的是帮助交换商品与服务。事务处理的目的是保证发生支付时商品送达，不发生支付时商品不送达。这其实是一个很复杂的工作。

面对面进行商务时，许多社会性非正式机制可以帮助错误恢复。如果找钱有错或商品没有送达，则有关人员会指出和重试。而在信息系统中，让软件处理一切顺利的情形很简单，而让软件处理各种可能的故障则很难。事务处理学科提供了建立复杂系统的框架，以便在遇到故障时能正确工作。

16.2 事务处理概述

Internet 商务应用的功能（如销售和收入）是相当复杂的，各包括几个活动。例如，销售包括：

- 借买方账号[②]
- 贷卖方账号
- 记录业务记录事件
- 将订单发往履行中心
- 向买方发出发票

事务系统保证这些步骤只要发生一个，就全部发生，多个买家的活动不会相互干扰，记录不会丢失。从这个角度说，事务有四个重要特征，称为 ACID。

---

① JimGray 与 Andreas Reuter，《Transaction Processing: Concepts and Techniques》（Morgan Kaufman，1993）。

②借本身是个复杂操作，分为三步：读旧结余，减去借额，存回新结余。

- 原子性（A）——本例中，如果贷卖方账号而不借卖方账号，或如果交钱而不发货，则会有问题。换句话说，事务中不能只发生一些步骤。或者发生所有步骤，或者任何步骤都不发生。
- 一致性（C）——如果环境状态用账号结余、收据等表示则不能出现状态不一致的情形。例如，事务前后的账号应平衡。
- 隔离性（I）——由于 Internet 商务业务事务的操作需要一段时间，并且由于要进行多个事务，因此一定要保证多个买家的活动不会相互干扰。即使多个事务同时进行，也不应相互重叠，而是按某种顺序或序列化进行，这样就要把系统设计成重叠事务能序列化进行。图 16.1 显示了事务序列化的例子。
- 耐久性（D）——事务完成或实现之后，不能因为系统或组件故障而取消。实际上，这就要求在稳定存储媒介中可靠地记录事务结果，例如用重复或镜像硬盘。

考虑单个信用事务：

- 第 1 步——读旧账号结余
- 第 2 步——将贷款额与旧结余相加
- 第 3 步——存储新结余

下面假设两个贷款操作同时进行，一个是 10 美元，一个是 20 美元。如果不进行事务隔离，则这些步骤交织进行：

- 事务 A，第 1 步，读旧账号结余
- 事务 B，第 1 步，读旧账号结余
- 事务 A，第 2 步，将贷款额与旧结余相加
- 事务 B，第 2 步，将贷款额与旧结余相加
- 事务 A，第 3 步，存储新结余
- 事务 B，第 3 步，存储新结余

最后，账号只有 120 美元，而不是 130 美元。使用事务隔离，就可以将事务序列化，得到正确结果，先完成事务 A 或事务 B：

- 事务 A，第 1 步，读旧账号结余
- 事务 A，第 2 步，将贷款额与旧结余相加
- 事务 A，第 3 步，存储新结余
- 事务 B，第 1 步，读旧账号结余
- 事务 B，第 2 步，将贷款额与旧结余相加
- 事务 B，第 3 步，存储新结余

图 16.1 事务序列化的例子

16.2.1 两阶段实现

事务影响多个资源（可能分布在网络中多个系统上）时，用两阶段实现方法保证总事务的原子性。在这个方法中，中央事务协调器与各个资源管理器通信，使事务协调进行。

- 第 1a 阶段——投票（vote）
  事务协调器询问每个资源管理器能否实现事务。如果都回答 Yes，则实现事务。
- 第 1b 阶段——记录（record）
  事务协调器在持久存储体中记录实现的事务。
- 第 2a 阶段——实现（commit）
  事务协调器告诉每个事务协调器已经实现事务。
- 第 2b 阶段——完成（complete）
  事务协调器在持久存储体中记录已收到所有资源管理器的确认。这时，不再需要增加工作以从故障恢复。

16.3 Internet 商务中的事务处理

下面举一个实际例子，一个发生下列事件的 Internet 商务系统。

1. 买方选择 Web 产品目录中的几个项目。
2. 买方安全输入信用卡与发货信息。
3. 计算产品、税收与发货费用。
4. 买方接受总价。
5. 取得信用卡授权。
6. 向履约中心发送订单消息。
7. 买方收到收据。

第一步标识事务。第一部和第二步不一定要在事务之内，这是浏览阶段，加上订单完成的交互阶段（输入发货地址等），可能需要不断重复。第 3 步计算订单总价，也不放在事务内，但一定要禁止发生影响总价的订单改变（如在订单中增加项目）。实际事务是第 4 步到第 7 步，从买家的订单接受开始到与支付和履约相关的所有活动，或者所有步骤要顺利完成，或者系统就像没有接受任何订单一样。事务失败的原因有几个：

- 卖方计算机崩溃或断电
  从买方角度看，他单击“OK to buy”按钮，但什么也没发生。他就有可能放弃，也可能再次单击“OK to buy”按钮。无论如何，他不愿意付钱而收不到货，或收到一个货而付两次钱。
- 买方计算机崩溃或断电
  从买方角度看，他单击“OK to buy”按钮，然后停电了。再次通电时，买方重试，买一次东西就付一次钱。由于买方计算机出故障时卖方已经收到确认，因此可能顺利执

行第4步、第5步和第6步，只留下第7步。这里，商务系统可以向买方提供得到重复收据的方法。

- 信用卡授权失败
  如果信用卡授权失败，则系统实际上返回第2步，认为买方卡号输入错误，提供重试机会。
- 发送授权请求与接收响应之间信用卡网络线路发生故障
  这是非常有趣的故障，因为卖方系统不知道请求消息是否到了信用卡网络，答复是否丢失。客户不可能付两次钱，因此商务系统要采用恢复技术，判断授权成功、失败或没有发生。

16.3.1 集成事务与外部系统

上节的例子在信用卡授权消息期间通信信道失败。这是事务系统与不能控制的外部设备和系统通信时发生的一般问题的例子。

对参与事务的外部系统，外部系统的功能必须具有幂等性或是可测试的。幂等性就是对同一操作进行重复请求时，这个操作只发生一次（或重复请求不在第一次请求之外增加其他效果）。可测试就是事务系统能够测试操作是否已经发生，因此不会进行重复请求。

在上面的信用卡授权例子中，卡协议在请求中使用引用号。如果收到已知引用号的重复请求，则信用卡系统只是返回上一答复，而不是进行重复请求。

16.4 客户端软件

在 Internet 商务系统中，使用 Web 浏览器或其他客户端软件需要特殊分析。

- 意外用户事件是否会造成不良后果？
  和末端用户操作终端的其他系统中一样，Internet 商务系统用 Web 浏览器作为用户界面时可能收到任意时间的任意事件序列输入。用户可能在任何时间单击任何链接或按钮，在窗体中输入任何信息，在同一按钮中一遍一遍单击或在任何时候消失，过个把小时才回来。系统应完全适应这种活动。这个问题在 Internet 商务中比任何其他系统中都要复杂，因为用户终端（Web 浏览器）是个通用设备，很难限制。例如在 ATM 网络中，终端由末端用户直接操作，但用户行为受到终端软件的完全限制。例如，系统考虑请求时，可以锁住除“cancel”以外的所有键。而在 Internet 中，Web 浏览器对所有应用程序平等相待，标准用户界面模型向用户提供了大量功能。
- 不友好的用户能否在系统行为中造成错误？
  有时所要的用户群可能对系统造成很大的压力，但不友好的用户或黑客也可能添乱。由于系统在开放网络中提供，因此不友好的用户可以向系统传递任意位字符串，就像有效输入一样。系统要验证任何不信任来源的所有输入，可能要认真检查所有输入，不

管信任与否。不友好的用户甚至可以对用户终端或浏览器进行编程，使其具有完全不同的行为。

有时错误恢复是成本与效率的权衡。系统设计人员对常见情形（正确操作）设计系统，提供相当昂贵的错误恢复机制，这种方法适用于不常遇到错误的情形。但是，如果不友好的用户能让系统产生错误或要响应明显错误，则即使系统操作正确，也可能性能不好或破坏设计假设。一定不要相信来自不信任方的任何消息。③

16.5 集成现有系统

许多公司已经有管理业务的信息系统：订单处理、制造、会计、履约，等等。新的 Internet 商务系统可以尽量集成现有系统，而不是单独运行业务的 Internet 部分。集成应特别小心，特别注意下列问题。

- 实时要求
  现有系统可能没有正确连接 Internet 商务系统进行交互使用所需的实时要求。从某种程度上，这些问题可以用 Internet 系统与现有系统之间的缓冲、排队和缓存进行处理。
- 安全要求
  现有系统可能没有 Internet 商务所需的安全机制。例如，大多数现有系统设计成专门培训的人员使用，配合系统操作员。而 Internet 商务系统通常要由没有培训的末端用户直接访问与操作，不一定配合系统操作员工作。
- 支持所需角色
  现有系统可能没有设计 Internet 系统所需的角色。例如，邮购和电话订购的现有订单输入系统通常设计成由订单输入操作员使用，而不是直接让客户使用。
- 信任保护
  现有系统可能没有设计成直接连接不同组织操作的系统。这时，必须特别小心验证外部的所有输入。

16.6 保存业务记录

Internet 商务系统事务处理子系统的一些主要输出是各种业务记录。有些记录（如订单与支付记录）是业务核心操作的一部分。有些（如包含客户数据的记录）则建立公司的关键信息资产——客户数据库。还有一些（如税收记录）则是满足法律法规要求所需要的。

---

③作为不信任的一个极端例子，一些旧版 Internet 商务系统将商品价格放在所谓隐藏窗体字段中。这些字段是普通买家看不到的，但不友好的用户可以访问这些字段和改变价格。

16.6.1 核心业务记录

有些记录对管理日常业务非常重要。

- 订单
  订单就是买什么东西、特征、条件、价格、发货与计账地址，等等。这里的每个信息元素都是有特定用途的。此外，订单不是一下子建立的，而是在订单捕获阶段一项一项增加的，然后在订单完成阶段增加遗漏的项目，如地址、税收与货运费用，等等。买方与卖方同意之后，订单就完成了，成为约束性协议。
- 发票
  发票是履约记录，记录发出的商品或提供的服务。由于买方欠卖方钱，因此发票也是账单，但与支付不是直接联系的。通常，发票写出之后是不能改变的，因为它表示历史事实（已经发货）。
- 支付（收据）
  收据是收款记录，通常由卖方发出，但也不一定（信用收据是由买方发出的）。

16.6.2 整理记录

有些记录要通过整理，建立长期信息资产。

- 客户数据库
  客户姓名、地址、购买历史和爱好能帮助市场和销售部门了解客户。如果卖方的业务是流通而不是生产，则保持与客户的密切关系是公司的核心价值。客户信息不仅用于报表，还可以在联机中提供个性化服务和定制产品目录。
- 广告与跟踪
  在 Internet 商务中可以跟踪买方如何找到卖方。广告产生的信息不仅确定谁向谁支付多少广告费，而且用积极反馈循环测量广告效果和控制未来的广告投入。

买方找到卖方之后，基于 Internet 的系统可以跟踪买方的详细行为和操作。这个信息可以帮助调整产品展示和提供商业机会。

16.6.3 政府记录

有些记录是外部要求的。例如，政府对销售和税收信息有特定记录要求。第 15 章介绍了 Internet 商务的税收问题。

16.6.4 记录寿命周期

典型业务记录项目（如客户输入的订单）有一个复杂的记录寿命周期，下面介绍订单的记录寿命周期。

- 生成
  买方首次选择准备购买的项目时，生成订单。这是订单捕获，是订单建立的第一阶段，可以持续一定时间。在这个阶段，订单可能是临时记录，由买方桌面的 Java 小程序维护，或在服务器方形成正式的数据库记录。
- 存储
  在订单的开始阶段，买方考虑准备购买的项目时，不一定需要建立永久记录。有时由于潜在订单已经达到一定价值，或者为了向用户提供方便，可以存储订单和提供惟一标识。记录可能是永久的，也可能在订单一直没法完成时被删除，订单标识或引用号不能复用。
- 处理
  正常订单流中的订单要经过几个处理阶段。例如，要计算货运费用与税收、取得信用授权。订单确定时，要与负责履约的系统通信。
- 访问
  生成订单后的某个阶段，它处于活跃使用中，订单处理期间买方和卖方都更新正在进行的订单，最后确定的订单由客户服务子系统引用。
- 报表
  订单是各种报表的对象。当日销售报表、开放订单、应税销售、客户账单和市场报告都要使用订单信息。
- 存档
  订单完成活动处理和一段报表访问标准期之后，就要存档。事实上，档案存储与系统备份可能用相同机制，但目的是完全不同的。备份系统是为了在遇到硬件与软件故障时或灾难时恢复，而档案则是永久业务记录。
- 读取
  有时需要使用已经放到档案存储中的旧订单。例如，记录通常联机保存 60 天，但客户在 90 天后提出争议，则要从档案中取得涉及的记录。读取操作是相当昂贵的，因此记录联机时间要足够长，尽量减少读取操作。

16.6.5 保存记录的设计意义

记录寿命周期对生成与维护记录的事务处理系统设计有几种意义。首先看看记录的特征。

可变与不可变记录

有些记录一旦生成就不能改变，例如，发票与收款收据。这些记录表示真实事件的客观记录，因此不能修改，是不可变记录。即使后面发现错误，也不能修改不可变记录，只能建立另一个纠正记录，在其中引用第一个记录。这个过程与报纸相似，报纸一旦印刷就不能改变，如果发生错误，则可以在后次编辑时进行纠正（但这样某一天就会有不同版本，每个版本对同一故事有不同版本）。有些记录是可变的，可以随意改变。例如，订单捕获期间，订单的项目与数量在订单敲定之前是经常改变的。

不可变记录可以大大简化事务处理系统，因为它们不用修改。这样，事务系统不需要复杂的记录锁，保证记录访问的一致性。可变记录需要锁，保证一个进程读取记录时，另一进程不会修改这个记录。此外，不可变记录可以任意复制，因为它们是不变的，不会出现不同备份包含不同信息的危险。

故障与事务词法

Internet 商务系统中的每种记录都应认真分析，确定其ACID属性。例如，假设看看订单捕获阶段订单所需的属性，即订单项目增加与删除时或订单数量改变时。

一种观点是，订单捕获不需要完整事务词法。和书面订单一样，订单要等交给卖方时才实际存在。这种分析可能造成将订单窗体实现为买方计算机上的 Java 小程序，在正常事件条件下，完整订单提供给卖方，但如果订单提交之前关闭买方的计算机，则订单丢失。

另一种观点是 Internet 允许新功能，可以对正在进行的订单提供完整事务词法。例如，如果订单是事务性的，则正在进行的订单可以对可用库存准确逆转。如果订单是耐久的，则甚至买方计算机崩溃也不会丢失信息，买方返回联机时，部分完成的订单还在那里。

但是，支付则需要完整事务词法。如果支付丢失，则卖方不干；而如果已经支付却不到货，则买方不干。

访问模式

记录类型的使用模式与支持这个类型的系统设计密切相关。特定记录可能在寿命周期中经历下列访问模式。

- 联机记录
  有些记录主要是联机使用的。例如，在处理过程的订单完成阶段，订单主要是联机使用的，因为买方与卖方交互式合作，建立完整的购买订单。
- 脱机记录
  审核记录（见稍后介绍）和报表记录主要是脱机记录。审核记录可能从不访问，报表通常是从联机主记录的拷贝进行的，因此与报表相关的处理和查询无法干扰生产系统的性能。脱机记录显然应该是持久的，但由于它们通常是不可变的，因此不太需要隔离。

- 消息
  从一个系统发送到另一系统的消息也是记录。例如，订单离开 Internet 商务系统和进入传统履约系统时，就会发生这种情形。通常，订单要用传统词法移交，订单不能丢失，必须恰好一次进入履约系统。

16.7 审核

按照正常业务术语，审核是独立审查过程，验证企业的财务记录的准确性，企业是否遵照良好的会计业务。对于 Internet 商务，还有另外两个相关的概念。

- 独立验证设计与实施
  系统设计和操作实务都要进行审查，确定设计目标是否得到满足。例如，在安全审核中，要对系统设计、实施和操作的每个方面进行审查，确保信息保密和没有发生非法访问，且今后也不会发生。
- 各个事务的记录
  事务审核记录是一组记录，验证特定事务实际按预定方式发生。审核用于报表、客户服务查询和争议解决，不属于主订单处理流的一部分。

16.8 备份与灾难恢复

备份与灾难恢复是相关的。备份过程就是保留应用程序数据，以防磁盘崩溃之类的硬件故障。灾难恢复就是让应用程序不仅能从硬件故障恢复，而且能从断电、地震、通信故障等恢复的过程和系统。

业务应用程序主要面向批处理时，备份与灾难恢复是不难理解的。发生事务时，它们写入磁带中，事务磁带一天一次与其他磁带上的主文件合并。维护备份就是保存旧带，遇到消息发生灾难时，可以在不同数据中心的类似计算机上方便地运行这个磁带。

联机事务处理的情形要复杂得多，因为各个事务可能 24 小时发生，没有用于备份的无效时间。此外，可用性要求可能非常严格，整个系统不能在发生故障时停止工作（见“高可用性系统”）。应该自动用多余组件替换故障组件，不丢失数据并保证无效时间最短。这种可靠性可能是相当昂贵的。

由于 Internet 商务系统可以进行全球操作，即使小公司也可能要求 Internet 系统 24 小时运转。

16.9 高可用性系统

Internet 商务系统应当在客户要用的时候随时可用。由于 Internet 商务系统可能吸引全球客户，因此没有所谓“上班时间”。系统可能要每周 7 天、每 24 小时运转。

系统无法使用的原因很多。

- 经常性维护

  系统需要定期维护，进行备份、改变配置，等等。通常，改变配置要先在系统的开发版本上测试之后再切换到生产系统，因此风险不大。对于需要无效时间的维护活动，可以计划不可用时间。

- 升级

  主要系统组件可能要定期改变：新软件发布、新硬件平台的出现、设备搬迁，等等。需要为此计划无效时间，或者除非采取非常措施。

- 基础结构故障

  商务系统中有些系统是一部分或全部在控制之外的：电源、Internet 访问服务和其他电信服务都可能干扰，造成一些用户或所有用户的服务丢失。一般来说，这些故障源也可以管理，只要提供专用备份电源和备份通信设施，但这样的成本不低！

- 环境

  水灾、火灾和其他自然与人为灾难可能使数据中心脱机，再可靠的软件与硬件也无济于事。要解决这类问题，通常的方法是在远程地点对数据中心进行热备份。

- 软件故障

  软件安装之后本身是不变的，但环境的改变可能暴露软件中的问题，结果，软件可能停止工作。此外，Internet 商务软件要面对其他风险，如果加密方法之类的关键技术因为技术进步而变得脆弱，则软件可能不再可信。

- 人为错误

  操作员错误、配置错误等也可能使系统关闭。从某种意义上说，这些因素是可控制的，可以通过增加培训和测试而改进。但有些错误是无法控制的，例如，在 Internet 中，不同服务提供者可能在网络中引入路由错误，造成服务丢失。

- 硬件故障

  磁盘、计算机、网络路由器和其他机械与电子组件故障。这些故障随着电路基本可靠性的提高而不再常见，但随着系统规模增大，组件数猛增，这种可能性还是存在的。

系统设计人员和系统操作员最好列出想到的每个故障源，探索每种故障的后果，在发生这些故障时要采取的相应措施，以及阻止故障和迅速从故障恢复的方法。

的良好基础。此外，在设计时尽早采用这种观点在调整现有系统要方便得多。

16.11.1 文件

可以在普通文件系统之上建立完整的事务处理系统。事实上，在早期联机事务处理中，系统是用事务处理（TP）监视器和文件系统建成的。计算机文件系统有一组相对简单的操作：生成、删除、打开、关闭、读、写和寻道。文件系统通常在构造文件内容方面不提供帮助，在管理事务方面不提供帮助，但有些操作系统提供文件锁和开锁功能，防止并发访问（锁可以提供隔离，但可能造成性能问题和死锁④），文件有几个重要作用。

- 日志
  许多应用程序将日志文件直接写入文件系统。这样的好处是可能得到高性能，坏处是所需的操作很难正确完成（要将日志记录写到文件末尾）。
  在许多文件系统中，用一个写操作添加到文件末尾是个原子操作，但这里的关键是单个写操作。一个常见的错误是用缓冲输入/输出包写入日志文件。这通常是可行的，但在负荷很高时，日志记录可能一片混乱。正确的实施方法保证每个写操作包含一定个数的日志记录。
  日志文件常用于记录应用程序事件与错误。例如，大多数Web服务器可以配置成将每个Web访问的信息写入日志文件。
- 只读数据
  如果数据主要是只读数据，则文件可以是事务系统中的有效存储媒介。文件对读写操作高度优化，但加锁和开锁之类的操作则没有那么快。

16.11.2 数据库

基本说来，数据库是存储结构化信息的方法，但数据库还有许多关键属性。

- 数据库存储结构化信息
  联机事务系统处理许多不同类型的记录。数据库管理所有这些细节，但应用程序自由地操作相关记录，而不必考虑存储分配之类的问题。
- 数据库是自我描述的
  在现代数据库中，描述数据库结构的信息存放在数据库本身之中。这样就可以编写一个通用工具，处理数据库中存储的信息，而不必对应用程序有特定了解。例如，通用

④死锁就是两个或几个进程等待资源，谁也不能进行。例如，假设两个事务正在进行中，各需要资源A和B。如果事务1锁住资源A，然后要锁资源B；事务2锁住资源B，然后要锁资源A，则两个事务都不能进行。

报表工具就是这样，不用传统编程就可以生成新的定制报表⑤。

- 数据库支持事务
  今天市面上的数据库通常都支持结构化查询语言（SQL），包括支持事务所需的所有机制。此外，今天的数据库支持ACID词法，很容易建立处理事务的应用程序。
- 数据库允许快速读取信息
  数据库管理器提供了从所有存储的记录中搜索与选择特定记录的内置支持。

16.11.3 事务处理监视器

事务处理监视器演变成可以解决一些问题，建立超出数据存储和读取以外的联机事务处理系统。事务处理监视器不是代替数据库，而是提供补充功能，使组装与操作复杂应用程序更加方便。

- 事务管理
  事务处理监视器分两阶段实现事务管理，初一看与数据库功能相同，但事务处理监视器事务服务可以协调跨多个数据库的事务，包括各种资源的管理，如通信系统和远程应用程序。
- 应用程序管理
  事务处理监视器提供应用程序管理功能。系统重新启动时，注册应用程序服务器自动启动，并在崩溃时重新启动。事务处理监视器还提供负荷共享与平衡功能，这些服务有时由 Internet 环境中的Web服务器提供：Open Market 的 FastCGI 可以管理应用程序，Microsoft 公司的 IIS4.0 也可以管理应用程序。基于应用网关接口（CGI）的简单Web应用程序可能不需要管理服务，因为每个请求都启动新的应用程序。
- 终端与通信管理
  传统联机事务处理（OLTP）应用程序利用硬连接网络或联网终端。这种终端的消息队列和通信服务是由事务处理监视器提供的，但这些功能与 Internet 应用程序关系不大，因为它们由Web服务器提供。

16.11.4 对象技术、中间件和应用程序开发器

用最强大的工具开发应用程序有很大的好处。在这个类别中，我们包括COM与CORBA之类的对象技术、DCE之类的中间件和 Forte 之类的应用程序开发器。

- 集中开发
  开发人员可以任意考虑应用程序，而不必考虑通信、安全、数据完整性和分配的细节。

⑤用好的用户界面生成问题的解决方案其实就是编程，只是不像传统编程而已。好的工具就是在合适的抽象层按照应用程序设计人员的思路解决问题。

- **交货期**
  开发人员经培训之后，应用程序开发工具可以提高生产率。不管用什么语言，编程人员每天编写的代码行数是相同的。高级语言比低级语言每行完成更多有用工作，从而可以提高生产率。
- **应用程序可靠性**
  如果选择的基础技术是可靠的，则利用这些技术可以大大增加应用程序可靠性。这些工具更容易保证处理所有错误条件，使应用程序更容易测试。

16.12 小结

不管 Internet 商务系统是小是大，事务处理原则都不能忽略。即使最简单的商务应用程序只用 Web 订单窗体将订单添加到文件末尾，也要认真使用文件加锁技术保证时间接近的订单不会造成订单丢失或将文件搞乱。中型商务应用程序可以用数据库管理系统加进事务，大型商务应用程序可以用事务处理监视器将 Internet 订单路由到现有订单处理系统中。

第三部分
Internet 商务系统

第 17 章 集成起来
第 18 章 Internet 商务的未来

第 17 章　集成起来

看一幢楼要看三点：盖得是地方，基础扎实，顺利建造。
—— Johann Wolfgang von Goethe [①]

17.1 建立完整系统

本书第一部分介绍了业务、体系结构与实施方面的问题，第二部分介绍了 Internet 商务各个方面的实现技术。本章要用这些组件建立完整系统。建立 Internet 商务系统的方法很多，但这里介绍 Open Market 公司产品使用的方法，因为这是我们最了解的方法，我们帮助设计了这个产品。本章首先复习、体系结构与实施这几个问题，然后讲解如何对第 4 章介绍的业务模型采用这个体系结构。

第 2 章介绍了商务价值链，Open Market 公司的方法将这个商务价值链分为三个部分：

- 内容服务器和应用程序，由几个独立软件厂家提供。
- 将内容与事务链接，由 Open Market 公司的 SecureLink 产品提供。
- 订单管理，包括订单处理、支付、履约和客户服务，由 Open Market 公司的 Transact 产品提供。

17.1.1 漫谈事务

介绍系统体系结构与设计问题之前，先要谈一谈事务的概念。

开始业务之前，卖方要生成联机产品目录，包含嵌入的数字化商品。这些数字化商品将产品描述、价格等编码成统一资源定位器（URL），将产品目录与 Transact 订单管理系统链接起来。卖方还要在 Transact 产品中建立商家配置，描述接受的支付方式和税收与货运规则，配置路由订单的履约系统。

买方浏览产品目录时，购买过程开始，发生下列步骤。

1. 买方找到产品目录中感兴趣的产品，单击相关的数字化商品。数字化商品是 Transact 订单窗体的超文本链接，带有产品描述。
2. 买方看到的下一个屏幕是订单窗体，图 17.1 所示。这个屏幕中已经填入一些买方信息，

① Johann Wolfgang von Goethe，《Elective Affinities》（1808）。

好像重复买方一样，根据保存的成员信息显示。

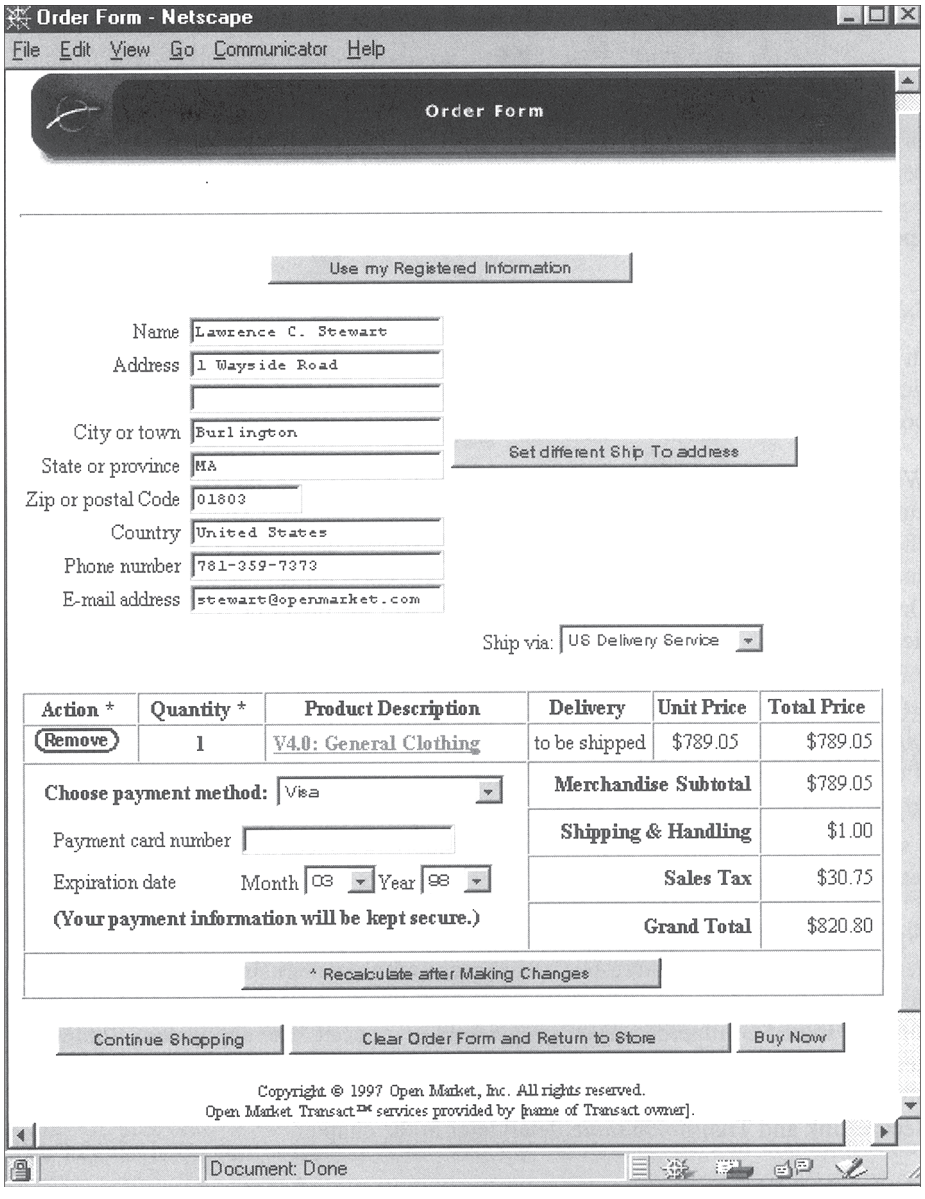


图 17.1 Transact 订单窗体

3. Transact 用买方的计账地址、卖方的税收配置和产品税分类码计算销售税。
4. Transact 用买方选择的卖方定义发货方式和产品价格或重量计算货运费用。
5. 买方单击 “ Buy Now ”。

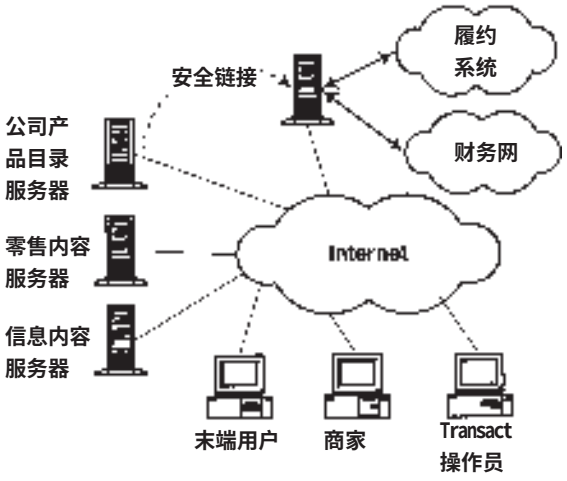


图 17.2 OpenMarket 商务体系结构

17.2.1 内容与事务分开

考虑 Internet 商务问题时，我们首先注意到，尽管通常把Web内容看成在网络上某个服务器上，但它只能在末端用户的Web浏览器中成为可显示的绘制文本与图形。因此，买方的购买决定要以网络事件形式与系统其他部分通信，这个事件不一定要发给生成页面内容的同一系统。

另一点是业务事务的性质。通常，买方、卖方和所购买产品的信息应放到一起。买方信息包括支付方式、发货地址，等等；卖方信息包括与特定货物无关而与多个产品的卖方有关的信息，如接受的支付方式与履约方式；产品信息包括产品描述、价格、重量、税收等信息。

我们的关键决策是把产品信息当作内容，在内容服务器中维护，然后在单击购买过程中用标准Web HTTP协议将产品信息发送到事务服务器中。这个思想可以将内容管理与事务管理分开，并带来几个好处。

减少操作成本

将内容管理与事务管理分开可以减少操作成本。

内容服务器的操作要求与事务服务器大不相同。事实上如果用E-mail或光盘发送内容，则根本不需要内容服务器。

将事务与业务记录放在一起可以减少需要数据库管理系统与昂贵的可靠性和完整性保护的系统个数，减少需要专业化管理与操作技巧的系统个数。

由于许多内容服务器可以共享事务引擎的服务，因此事务引擎的成本分摊到多个用户。由于每个系统不需要建立所有公共事务处理工作，因此可以减少内容服务器的成本。

- 预订
  预订数据库包含访问控制和授权信息，使Transact可以远程管理用户对远程预订内容包的验证和授权。这里输入预订数字化商品的信息，Transact对日常访问预订内容发出临时使用的数字化票。

17.5 小结

本章将应用程序知识和技术综合起来，描述了 Open Market 公司的 Internet 商务产品的体系结构与实现方法。当然，还有许多其他商务应用方法，但这个例子显示了实现商务系统的一种方法。Transact 事务提供了各种商务应用的基础，解决了本书介绍的许多问题。

第 18 章　Internet 商务的未来

预测是很难的，特别是对未来的预测。
——Yogi Berra [①]

这几年对Internet商务的激动和炒作非常热闹，但我们实际上只是刚刚开始一个业务革命。有些公司迅速而急剧地改变，有些公司则没有那么激烈，但迟早也要改变。现在的问题不是要不要利用 Internet，而是如何利用和什么时候利用。客户需要 Internet，如果不用 Internet，则会在竞争中被淘汰。

本章介绍预期的一些改变和趋势，以及无法预期或不连续改变的问题。由于我们相信Internet技术还会迅速演变，因此我们将介绍如何更新Internet商务系统。最后，我们回到Internet的战略性推动力。

第一步要认准改变即将发生，第二步要利用 Internet。

18.1 趋势

预测未来是困难的，但我们可以研究形成未来的一些力量。我们生活在这个力量之中，因此很难知道它的真面目。但我们可以研究趋势，把历史模式延伸到未来。

18.1.1 硬件技术趋势

计算的进步不同于历史上的任何其他活动。计算机的处理器性能和存储容量等指标近20年来一直呈指数级增长，今后10年到20年内，这个趋势还将继续。高登·摩尔是 Intel 的奠基人之一，曾经于1965年预测半导体芯片上晶体管的密度每18个月翻一番。这个预测相当准确，被人们称为摩尔定理。摩尔定理其实不是个定理，而是一条激励着整个行业创造性工作的曲线。但是，这个结果是 Internet 环境中的改变势在必然。

计算机性能

我们可以预计10到15年内计算机设备的性能稳定增长，价格不断下降，包括个人计算机与服务器。1982年到1997年之间，2000美元的个人计算机性能增加了1000倍。1997年到2012

①传说 Yogi Berra 所说。

年之间性能又增加了 1000 倍。

- 存储容量
  1985 年，个人计算机上常用 5MB 硬盘，如今 5GB 硬盘到处都是。很难预测下一个千倍发生在什么时候，但这是迟早要发生的事。
- 通信功能
  1985 年，常用的 Modem 速率为 12Kb/s。1997 年，Modem 可以在普通电话线上达到 56kb/s。通过卫星、有线网络和公司局域网访问 Internet 则可以达到几个 Mb 的性能。不久即将看到 Gb 级的公司 Internet 连接，个人家用计算机也将很快看到 Mb 级连接。
  除了这些比较确定的趋势外，还有另外两个可能性很大的技术趋势。
- 可移植设备
  便携电脑已经达到桌面计算机的功能，许多人（包括作者）已经用可移植计算机作为主要计算平台。更小的掌上电脑也越来越普及。
- 无线通信
  无线数据通信已经变得非常普及和廉价，使可移植设备能够随时连接网络。

所有这些趋势都是某种硬件改进推动的，我们的结论是根据历史数据推导出来的。简单地说，这些趋势几乎是必然的。但是，这些指数级改变的业务意义是巨大的。

18.1.2 软件技术趋势

软件技术趋势也是相当明显的，包括下列方面。

- 安全与验证
  所有全球安全与验证基础结构的技术组件都须具备，公司和个人可以相互标识，可以在公开网络上安全通信。但是，这样的基础结构还没有出现。加密法、智能卡、数字签名都已经出现，必要的支持系统和环境也将在今后五到十年内开发和部署。与此同时，Internet 商务将在兴趣社区、在具有基础结构的部门和在网下关系可以推到网上的地方迅速增长。
- 组件软件
  对象与软件组件的趋势正在加快。这种转变的下一步是软件能帮助自己测试和组装（扩展设计功能）并迅速扩展转换功能，使软件对象能更方便地适用不同格式的通信。
- 业务对象
  近 20 年 EDI 低速增长的教训是数据的标准格式不够。公司消息要达到互操作性而不付出高的配置与开发代价，就要依靠标准化。换句话说，我们要从语法转到词法。这种趋势已经露出曙光，人们用 XML 之类的新标准定义业务消息标准，并开发包装行为和

信息的业务对象。

18.1.3 软件开发与标准化趋势

- 更大的互操作性
  系统间标准、互操作接口的行业趋势还在继续，多个厂家的组件与软件包更有可能组装成完整系统。
- 更多软件复用
  到目前为止，软件工程已经是个成熟的行业，技术人员兢兢业业地一行一行写软件。通过类库和其他对象技术，开发人员开始站在前人的肩上开发新的应用程序，而不是从头开始重建每个要素。

这些结果组合起来，必将使软件改变速度提高，开发新功能需要的时间将减少。当然，更加复杂的应用程序需要更多时间来测试，但自动化测试和软件质量保证能解决这个问题。历史上，大多数缺陷都是在新代码中，而不是在复用组件中。

18.1.4 基础结构趋势

- 商务环境
  Visa、Mastercard 和 American Express 等全球品牌的信用卡已经造就了个人消费者的全球公用商务环境。而商家对商家商务则没有同样水平的服务。Dun & Bradstreet 之类的功能帮助建立贸易关系，ACH 之类的电子转钱网络可以用于支付。但是，目前这些系统还不是全球性的，还不是实时的，还不是集成的。也许针对公司信任与支付的高度集成系统即将演变成支持全球 Internet 商务。
- 政府环境
  如今，政府环境相当复杂，税收、关税和规定随时间和空间而不同。也许，在一致性操作环境的商务需求推动下，国际联合和协定能简化和规定所有这些规则，但目前还没有这种苗头。要开发复杂的知识密集软件将这些工作自动化更是困难。第 15 章曾介绍过，组件要完全实现税收系统的功能，就会变得过于复杂，根本无法在商务中使用。
- 法律环境
  今天的业务环境是几个世纪经验的累积结果，用法律规定，由法院解释。Internet 带来了新问题，如数字签名的地位和证书机构的责任。这些问题还在测试和司法实践试验中，是根据法律系统的正常方法进行的。但是，从长期看，商务实践的统一标准与定义至关重要。最初，这些标准是将电子情形与最接近的物理情形相对照，但有时会出现新情形，需要新的先例。

18.1.5 应用趋势

在公司计算的早期，企业雇用开发人员和维护自己的应用软件，如会计软件。随着这些应用程序的功能不断标准化，平台厂家开始提供应用软件，而不是只提供开发工具。随着应用程序的复杂性不断增加，软件产品公司开始提供业务应用的包装应用软件。如今，很少再有自己编写会计软件的公司。

这些趋势也将在 Internet 商务中再现。最初，企业用现有技术开发自己的 Internet 商务应用，然后是软件厂家提供开发工具和应用程序。随着商务应用程序的复杂性不断增加，必将出现专业化的 Internet 商务包装应用软件。

Internet 飞速增长，这些阶段是重叠进行的，三个阶段的例子可能同时并存。在开发 Internet 商务策略时，一定要考虑如何随着时间推移而开发自己的系统，是建是买，哪个策略更适合你的公司。

18.2 不连续性

演变趋势可能是跳跃式的，特别是指数级增加的趋势。新思想会带来怎样的改变呢？这些改变在社会和商务方面可能是不连续的。发明更好一些的印刷技术可能很有趣，但发明电视呢？

在软件工程中，一个粗略的原则是，10 倍的量变会形成质变。前面曾介绍过，今后 15 年内，处理功能、存储功能和通信带宽将增加 1000 倍。这些改变会生成全新的经验，而不只是当前操作方式的演变。除了这些改变之外，还会有我们无法预料的变革。在这个 Internet 飞速发展的时代，我们经常误以为万维网是网络的最后一次变革，而忘记了 Web 只有几年的历史。5 年前，Web 还只是个奇妙的新思想。

一些可能的不连续改变可能非常受欢迎，因为它们已经在有限设置中演示，包括语音接口、自然语言理解和虚拟实境。其他思想则还停留在科幻小说家的想像中，如计算机直接控制神经系统。我们只能说，只要不违反实际法则，这种思想就可能实现。

一种美妙的可能性是用纳米技术构造网络连接另一端的物体。这种情况在 2005 年以前不可能发生，但在我们的下一代，则是完全可能的。

18.3 保持更新

购买新车时，还没有开出车库，车价可能就降了。尽管如此，这车还是可以开上几年，10 年之内新车型也不可能好上 100 倍。相反，你买 PC 机时，还没有安装好，技术上就已经过时，这种趋势还看不到止境。

如何在这种环境中让系统保持更新呢？这要靠 Internet 商务系统体系结构去完成。可扩展体系结构可以在现有组件之上增加新组件。可伸缩体系结构可以顺利处理增长，而不干扰客户系统。

体系结构还提供了哪些技术改变更合理和可以保留哪些技术的准则。有了这种帮助之后，就更容易在新技术与新产品的泡沫和真实之间明辨是非。有些对你的系统有用，而有些对你的系统没有用。几年之后，系统的所有重要组件可能都要换，即使基础体系结构没有太大的改变。

18.4 战略必要性

第 3 章曾介绍过，Internet 在商务思想中引入了两个因素：Internet 可以改变客户关系，Internet 可以取代传统业务价值源。

- 改变客户关系
  传统上，客户与公司有几个联系点，而 Internet 则允许完全倒过来重新构造客户与公司的关系，将公司从以内部为中心变成以客户为中心。
- 取代传统业务价值源
  Internet 将业务从处理物理实体变为主要处理信息。物理世界中销售的经济转换成范围的经济，分配成为机会而不是限制，结果竞争的基础完全变了。

这些因素要求根据对公司与客户关系的强度和核心价值主张对公司策略进行基础性分析。

18.5 结束语

最终确定 Internet 商务前途的是客户而不是业务。如果 Internet 对客户有效，则业务会寻找用其提供价值的途径。在这个过程中，新业务会成功，其他的会失败。有些现有业务可能协商过渡办法，有些则可能无法协商过渡办法。

回到第 3 章铁路的比喻，最后我们用 1829 年纽约州州长 Martin Van Buren 给总统安德鲁·杰克逊的一封信结束本书：

> 亲爱的杰克逊总统，
>
> 我国的运河系统正受到所谓“铁路”的新运输形式的威胁…
> 如果运河船只被“铁路”取代…造船厂将受到重创，拖缆、定单绞辘和挽具制造商将难以生存…
> 上帝从来没让人们以如此致命的速度旅行。
> 忠实的
> Martin Van Buren
> 纽约州州长
> 1829 年 1 月 31 日