第1章 电子商务安全概述

电子商务（Electronic Commerce/Electronic Business/E-commerce/E-business/E-trade/EC)不是一个单纯的技术概念，也不是一个单纯的商业概念，而是运用现代通信技术、计算机和网络技术进行的一种社会经济形态，其目的是通过降低社会经营成本，提高社会生产效率，优化社会资源配置，从而实现社会财富的最大化利用。

电子商务是建立在因特网上的一种商业应用，因特网使得电子商务能够以比较低廉的成本从事较大经济规模的商业活动。而电子商务是否可以蓬勃发展，进而掌握未来的经济命脉，完全依赖于安全技术的研究与发展以及安全交易架构的建立。

1.1 电子商务的基本概念

电子商务是一种新的社会经济形态；或者说电子商务是以因特网为媒介、以商品交易双方为主体、以银行电子支付与结算为手段的全新商务模式。与传统商务相比，电子商务增加了卖方的销售机会，同时也给买方提供了更多的选择。

电子商务可以惠及整个社会。例如,通过因特网可以安全、迅速、低成本地实现税收、退休金和社会福利金的支付等。另外，比起支票或现金支付，在因特网上更容易审计和监督，可以有效地防止欺诈和盗窃。由于具有以上优势，电子商务受到全球的关注。

网络是人类社会劳动、生活、学习的新工具。它通过影响人类通信与交往方式，间接地对传统经济领域的生产、交换、分配和消费方式产生影响,直到渗透、改造、重塑传统经济的运行模式以及社会经济价值标准与增值方式。因此，电子商务是一个泛社会化的概念，电子商务的发展是一个从基础应用入手、循序渐进地推而广之、最终实现普遍应用的发展过程。

1.1.1 电予商务内容

目前电子商务大致包含以下三方面内容：

网上商业信息服务；

电子购物和交易；

电子银行与金融交易服务。

随着信息技术的不断发展，电子商务将会扩充新的内容和新的领域。目前，电子商务必

须面对下述四大层面。

1．信息流

这是电子商务最大的优势，也是电子商务的基础。传统商务中的信息沟通，必须花费大量的时间和精力，所需的交易成本较高。电子商务中由于采用电子信息交换，将会使商务交易过程快速、公开和准确，而且成本低廉，又可打破地域限制。因此，解决好信息流的问题，将是电子商务成功的关键。

2．资金流

资金流是电子商务遇到的第一个挑战。信息流只是解决了参与商务各方的信息交流，而一个真正的商务过程的完成，必须靠资金的转移来实现。因此如果不解决好这个问题，电子商务就无法实现。

资金流必须依靠电子货币与网络银行的方式来解决。

3．物流

电子商务的特点是加快了商务过程、减少了中间环节，并能提供全球化和个性化的服务。但是，物流过程是不可代替的，在某种程度上甚至还增加了物流的流量和难度。电子商务的巨大好处不会因为这个问题而受到阻碍，关键在于商家如何解决。

4．安全

安全是保证电子商务过程能够顺利完成的必要条件。由于电子商务中交易双方无法见面，将会产生许多传统商务模式中不会出现的安全问题，本质上就是交易的安全性。

对顾客来说，网上所看到的商品与实物是否一致？交钱以后对方是否一定会送货？何时送到？使用的电子货币是否安全？等等。

对网络商家来说，对方的资金是否真能转到自己的账上？自己的网上账号是否安全？如果是货到付款，对方是否能履行交易合约？等等。

对双方来说，交易出现争议时又该如何解决？

电子商务中的安全问题，必须靠技术手段和信用手段来解决。只有这个问题解决了，才能保证电子商务的顺利进行。

1.1.2 电子商务分类

电子商务改变了传统经济活动的运行方式。电子商务按照应用群体的角度进行分类，可以分为以下四个主要类别。

1．企业间的电子商务（B2B）

企业间的电子商务，即企业与企业之间通过网络进行产品或服务的经营活动。例如，工商企业通过计算机网络向它的供应商进行采购，或通过计算机网络进行付款等商业活动。企业目前面临的激烈竞争也需要电子商务来改善竞争条件，建立竞争优势。商业机构对商业机构的电子商务从未来的发展看仍将是电子商务的主流。商业机构之间的交易和商业机构之间的商业合作是商业活动的主要方面。

2．企业与消费者之间的电子商务（B2C）

企业与消费者之间的电子商务，即企业通过网络为消费者提供产品或者服务的经营动。这类电子商务主要是借助于因特网所开展的网上销售活动。最近几年随着因特网的发展，这类电子商务的发展异军突起。例如，在因特网上目前已出现许多大型的网络商店，所

出售的商品一应俱全,从服装、食品到电脑、汽车等,几乎包括了所有的消费品。网上交易通常只涉及信用卡或其他电子货币。因此开展企业与消费者的电子商务障碍较少，潜力巨大就目前发展看，这类电子商务仍将持续发展，是推动其他类型电子商务活动的主要动力之一。

3. 政府与企业之间的电子商务(G2B)

这类商务活动包括企业与政府组织间的各项电子商务活动。例如，政府将采购的细节在因特网上公布，通过网上竞价方式进行招标，企业也要通过电子商务的方式进行投标目前，这种方式仍处于初期的试验阶段。

4. 政府与消费者之间的电子商务(G2C)

政府与消费者之间的电子商务是指政府通过因特网进行社会福利金的支付、个人所得税的征收等。

不同类型的电子商务所包含的主要内容如图 1.1 所示。

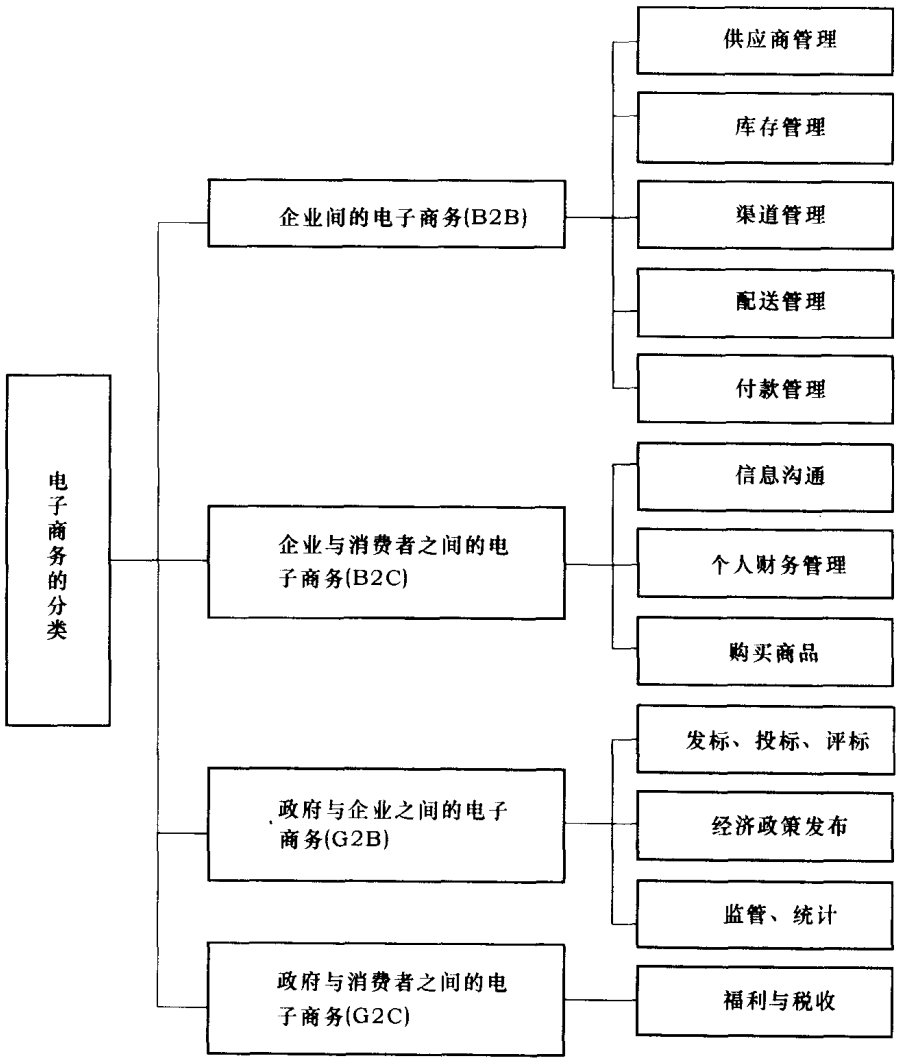

图 1.1　电子商务的分类

1.1.3 电子商务架构

电子商务的发展速度惊人，覆盖范围十分广泛，必须针对具体的应用才能描述清楚其系统架构。目前，电子商务的应用包括网上商店、网上银行、远程教育、网上订票、网上交税、股票交易和远程医疗等。

电子商务系统总体框架结构如图 1.2所示。底层是网络基础平台；中间是电子商务基础平台，包括 CA 认证和支付网关等，真正的核心是 CA 认证；而上层就是各种各样的电子商务应用系统。电子商务基础平台是各种电子商务应用系统的基础。

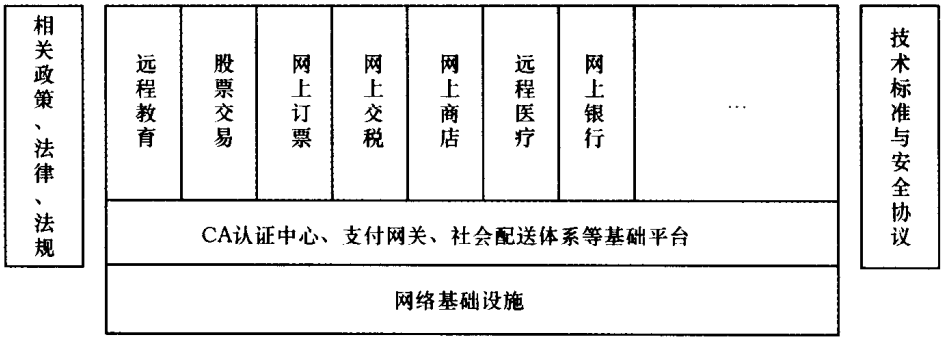

图 1.2 电子商务系统总体框架结构

对电子商务应用及各种基础建设的发展而言，位于图 1.2 左右两侧的技术标准与安全协议和相关政策、法律、法规则是两大重要支柱。

技术标准与安全协议是指电子商务过程中所涉及的标准和协议，包括“电子”与“商务”两部分的标准与协议；“电子”是基础，涉及信息技术方面的标准与协议；“商务”是核心，主要包括与电子商务活动有关的标准与协议，其中涉及信息流、资金流、物流等方面的标准。此外还包括安全交易协议和服务标准等。综合各种体系结构，电子商务标准与协议应包含如下几个方面：通用基础标准、网络标准、安全协议、认证协议、交易支付标准、商务应用标准和其他标准等。

相关政策、法律、法规是有关电子商务的政策、法律、法规。例如，关于著作权及隐私权的保障、消费者的保护、非法交易的侦查、网络信息的监督，以及交易纠纷的仲裁等，都需要制定相关的公共政策及法律条文来配合。

一个完整的电子商务系统应该包括哪些部分，目前还没有权威的论述。通常，电子商务系统的三层框架结构如图 1.3 所示。

1. 底层——网络基础平台

网络基础平台是信息传送的载体和用户接入手段，它包括各种各样的网络传输平台、网络传输设备和网络接入方式等。

2. 中间—— 电子商务基础平台

电子商务基础平台又可分为以下三层：

(1) 基本加密算法层，包括各种对称和非对称加密算法，以及哈希(Hash)函数等；

(2) 基本安全技术层，包括以基本加密算法为基础的认证中心 CA 体系以及数字信封、数字签名、报文摘要等安全技术；

(3) 安全协议层,包括以基本加密算法、安全技术、认证中心 CA 体系为基础的各种安全协议层,如 SSL 协议和 SET 协议等。

电子商务基础平台是整个电子商务体系的安全基础，它为电子商务提供所需要的各种安全技术，包括实现传输数据的保密性、完整性、不可否认性以及身份认证的各种技术。而认证中心 CA 安全认证系统是安全技术的核心。

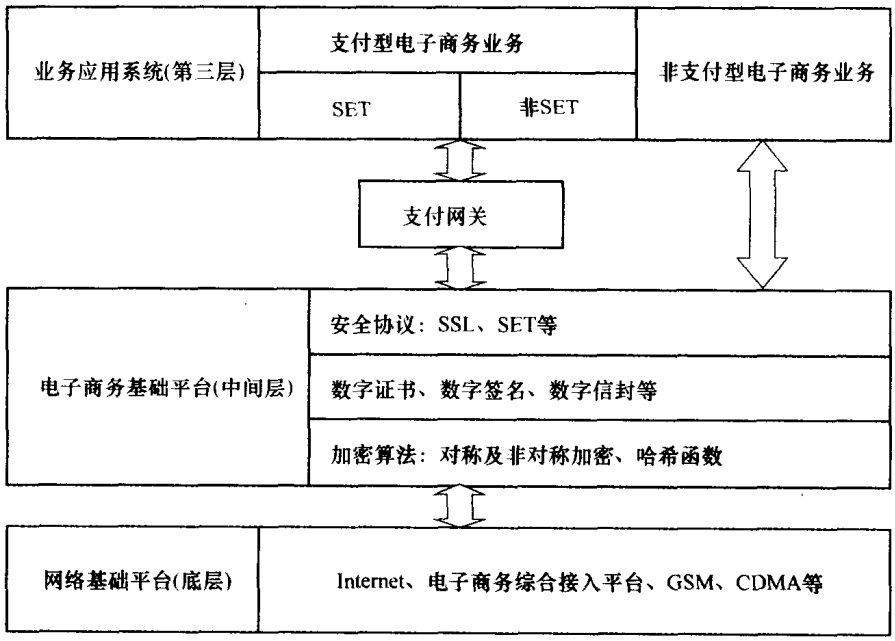

图 1.3　电子商务系统三层框架结构

3. 第三层—— 各种各样的电子商务业务系统

电子商务业务系统包括支付型业务系统和非支付型业务系统。电子商务业务系统中主要是支付型业务系统，而支付型业务系统可分为 SET 和非 SET 两类。

支付系统通过支付网关架构在电子商务基础平台之上，以其提供的各种安全服务为前提，为支付型电子商务业务系统提供各种安全的支付手段。而非支付型电子商务系统直接架构在电子商务基础平台之上，使用这一层提供的各种证书技术、认证手段和安全技术为最终用户提供安全的电子商务服务。

电子商务系统中的各个组成部分，例如认证中心 CA、支付网关、业务应用系统、用户终端等均连接在因特网上，并通过因特网实现完整的电子商务。

认证中心 CA 通过因特网向终端用户、支付网关和电子商务业务应用系统提供证书发放和授权服务等业务。

支付网关通过专线与银行的网络中心实现连接。一个支付网关可以实现对多个网络的连接。

电子商务业务应用系统直接建立在因特网上，分布在世界各地，通过网络实现企业对用户(B2C)、企业对企业(B2B)的电子商务应用。

1.1.4 电子商务的意义

对企业来讲,每天提供 24 小时的客户支持和服务费用相当昂贵。然而，通过网上商店任何人在任何时候都可进行信息查询和交易。企业的销售额会因为网上商店向客户提供 24 小时的网上交易而增加。

例如,Expro 公司是一家为石油公司提供零部件的机械制造企业。该公司在网上建立了网上商店。这样，远在北海海上石油平台的壳牌石油公司(Shell Oil)的工程师通过网上商店就可以立即订货，而不需要像原来那样必须回到岸上来进行订货操作。

电子商务是一项涉及全球的全新业务和全新服务，它将传统的商务流程电子化、数字化。与传统的商务形式相比,电子商务有以下几个优点 市场全球化、交易快捷化、成本低廉化、交易透明化和交易标准化等。

电子商务使得各国与各地区之间的贸易成本更低、效益更高。尽管建立和维护公司的网站需要一定的投资，但是与其他销售方式相比，使用因特网的成本大大降低。有研究表明,使用因特网作为广告媒介,进行网上促销活动,可以增加十倍的销售量,而成本只有传统广告及邮寄的十分之一。

电子商务使得用户在选择的多样化、服务质量、个人产品与服务等方面受益。在不久的将来，电子商务将允许人们跨越时间和空间障碍，交易活动将可以在任何时间、任何地点进行，人们可以充分利用那些超出自己所能想象的全球信息资源、市场和业务机会。电子商务将为各种社会经济要素重新组合提供更多的可能，这将影响到社会的经济布局和结构。未来的市场竞争将是在电子商务服务平台上的竞争。总之，电子商务通过因特网进行商务交易，具有以下一些特点：

全球化。由于因特网技术在全球范围内得到普及，可以提供全球范围的交互，电子商务能够让商家向全球范围内的客户提供商品，也可以让客户在全球范围内选购商品。

电子商务实现在线销售、在线购物、在线支付，使商家和企业能及时跟踪顾客的购物趋势。

成本降低。电子商务省去了中间环节，通过高效的信息传递手段，使得网上业务的运行成本大大降低。同时，也可以为客户提供及时的技术支持和技术服务，降低服务成本。

商家和企业可以利用电子商务，同合作伙伴保持密切的联系，改善合作关系。

商家和企业可以利用电子商务在网上广泛传播自己的独特形象。

通过电子商务可以促使商家和企业内部之间的信息交流，内部与外部的信息交流，及时得到各种信息，保证决策的科学性和及时性。

1.2 电子商务安全概念与需求

电子商务的安全与其他计算机应用系统的安全一样，是一个完整的安全体系结构。它包含了从物理硬件到人员管理的各个方面，任何一个方面的缺陷都将在一定程度上影响整

个电子商务系统的安全性。

1.2.1 安全层面

电子商务的安全包括物理安全、信息安全、通信安全、交易安全和管理安全五个部分，其中交易安全是电子商务系统所特有的安全要求。

1. 物理安全

计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提。物理安全的作用是保护计算机网络设备、设施和其他数据信息免遭自然威胁、人员威胁和环境威胁。其中，自然威胁包括洪水、地震、火灾、龙卷风、山崩、雪崩、电力风暴以及其他类似事件；人员威胁包括由人产生的威胁，例如无意行动(偶然的数据访问、误操作等)或有意的行动(基于网络的攻击、恶意软件上传和机密数据的非授权访问等）；环境威胁包括长期电力故障、污染、化学和液体泄漏等。

2. 信息安全

信息安全概括了一般性的安全技术问题。一般来说，系统可能遭受的攻击可以分为以下几类：窃听、伪装、报文篡改、渗透、流量分析和拒绝服务等。目前针对这些攻击主要采取加密技术、数字签名技术、访问控制技术、数据完整性技术和身份认证技术等。信息安全主要涉及信息传输的安全、信息存储的安全和对网络传输信息内容的审计三方面。通常采用的防护措施有：

数据加密，用以防止信息泄漏至未经授权获得该信息的其他人；

访问控制，用以防止任何未经授权的数据存取行为；

数据完整性控制，用以保护数据以避免内容遭篡改和部分删除的危险；

数字签名，可保障交易的任一方不得随意否认已进行过交易的事实；

证书(PKI-CA、公钥密钥加密算法)；

鉴别机制，鉴别服务有两大类型：一为身份鉴别，二为资料出处鉴别；

访问设备(安全认证卡)。

3. 通信安全

通信网络是交换信息的基本设施，TCP/IP协议没有考虑安全问题，因此协议的每一层都存在相应的安全威胁。针对通信协议中最常出现的安全威胁，实施了相应的安全协议用于实现网络通信的安全。例如，采用防火墙技术、虚拟专用网（VPN)技术、入侵检测技术、漏洞检测技术和病毒防护技术等。

防火墙是一种隔离控制技术，在某个机构的网络和不安全的网络（如因特网）之间设置屏障，阻止对信息资源的非法访问；也可以使用防火墙阻止机密信息从企业的网络上被非法输出。防火墙是设置在用户网络和外界之间的一道屏障，防止不可预料的、潜在的破坏侵入用户网络。防火墙是一种防卫技术，由于它假设了网络的边界和服务，因而对内部的非法访问难以有效地控制。所以，防火墙适合于相对独立的、与外部网络互连途径有限、网络服务种类相对集中的单一网络。网络病毒使人们对网络安全充满疑虑，逐渐成为电子商务发展的主要障碍之一。

通信安全中通常采用的防护措施有：

网络安全检测设备；

- 防火墙；
  防入侵措施,入侵检测系统,分布式入侵检测系统；
- 端口保护；
- 路由选择机制,阻止不合适的 IP 访问等；
- 通信流控制；
- 木马病毒防范措施。

4. 交易安全

由于电子商务是以电子的方式通过网络进行的商务活动，参与的双方通常是互不见面的，而使用的货币以电子货币为主，因此身份的确认和安全通信变得十分重要。同时，为了在用户、商家和银行之间能够实现资金流动，需要一个安全的电子交易协议。通常采用的防护措施有：

- 浏览器/服务器软件(支持 SSL)；
- 安全电子交易协议 SET；
- 商业软件(支持电子支付)。

5. 管理安全

面对电子商务安全的脆弱性，除了在设计上增加安全服务功能，完善系统的安全保密措施外，还需要花大力气加强网络的安全管理。由于诸多的不安全因素恰恰反映在组织管理和人员录用等方面，因此，这是电子商务安全所必须考虑的基本问题之一。

1.2.2 安全威胁

目前，电子商务发展面临的主要问题之一是如何保障电子商务交易过程中的安全性。交易的安全是网上贸易的基础和保障，也是电子商务技术的难点，围绕电子商务安全的防护技术已经成为目前电子商务研究的重点之一。

在电子商务的交易过程中，必然涉及到用户的一些机密信息和重要利益。例如，在交易过程中，客户方所订购商品的型号和数量对于他的竞争对手可能是极有价值的信息；交易的双方在交易过程中，可能需要提供银行的账号及口令；交易的一方可能中途毁约或私自变更交易内容等。这一系列问题需要一个安全、可靠和公正的系统来维护交易各方的利益不受侵害。

交易安全是电子商务系统所特有的安全要求。在交易过程中，消费者和商家面临的安全威胁通常有：

- 虚假定单——假冒者以客户名义订购商品，而要求客户付款或返还商品；
- 付款后收不到商品；
- 商家发货后，得不到付款；
- 机密性丧失——PIN 或口令在传输过程中丢失，商家的定单确认信息被篡改；
- 电子货币丢失——可能是物理破坏，或者被偷窃，这通常会给用户带来不可挽回的损失；
- 非法存取——未经授权者进入计算机系统中，存取数据的情形；或合法授权者另有其他目的地使用系统；
- 侵入——攻击者在入侵系统后离去，并为日后的攻击行为预留管道，如木马病毒；

- 通信监听——攻击者无须入侵系统即可窃取到机密信息；
- 欺诈——攻击者伪造数据或通信程序以窃取机密信息，例如，安装伪造的服务器系统以欺骗使用者主动泄漏机密；
- 拒绝服务——攻击者造成合法使用者存取信息时被拒绝的情况；
- 否认——交易双方之一方在交易后，否认该交易曾经发生，或曾授权进行此交易的事实。

1.2.3 安全需求

由于因特网本身的开放性及目前网络技术发展的局限性，网上交易面临着种种安全性威胁。交易与支付安全问题可归结为如下几个核心问题 可靠性、保密性、完整性、不可否认性、匿名性、原子性和有效性。

1. 可靠性

电子商务系统应该提供通信双方进行身份认证的机制，确保交易双方身份信息的可靠和合法，应该实现系统对用户身份的有效确认和对私有密钥与口令的有效保护，对非法攻击能够进行有效防范，防止假冒身份在网上交易、诈骗。

在传统的交易中，交易双方往往是面对面进行交易活动的，这样很容易确认对方的身份,即使互不熟悉,也可以通过对方的签名、印章、证书等一系列有形的身份凭证来鉴别对方的身份，也可以通过声音信号来识别对方身份。然而，网上交易的双方可能素昧平生、相隔万里，所以电子商务首要的安全需求应是保证身份的可认证性。也就是说，在双方进行交易前，首先要确认对方的身份，要求交易双方的身份不能被第三者假冒或伪装。

2. 保密性

电子商务是建立在开放的网络环境上的，维护商业机密是电子商务系统的最根本的安全需求。电子商务系统应对传输信息进行加密处理，以防止交易过程中信息被非法截获或读取,从而导致泄密。

传统的交易中，一般是通过面对面的信息交换，或者通过邮寄或可靠的通信渠道发送商业报文，达到商业保密的目的。而电子商务是建立在一个开放的网络环境上，当交易双方通过因特网交换信息时，其他人就有可能知道他们的通信内容。同样，存储在网络上的文件信息如果不加密的话，也有可能被黑客窃取。因此，电子商务的另一个重要的安全需求就是信息的保密性。这也就意味着，一定要对重要信息进行加密，即使中间被人截获或窃取了数据，也无法识别信息的真实内容，这样就可以确保商业机密信息不致被泄露。

3. 完整性

电子商务系统应防止对交易信息的篡改，防止数据传输过程中交易信息的丢失和重复，并保证信息传递次序的统一。

当网络面临主动攻击时，攻击者通过篡改或部分删除交易过程中发送的信息，破坏信息的完整性，使交易的双方蒙受损失。例如，A 给 B 发了如下一份报文“请给 C汇 100 元”。报文在传输过程中遭到 D的篡改，D将报文改为“请给 D汇 100元”。这样，最终 B 收到的报文为“请给 D汇 100 元”，B 按照报文给 D汇了 100 元，显然这不是 A 的本意。从这个例子可以看到，保证信息的完整性也是电子商务活动中一个重要的安全需求。这就要求交易双方能够验证收到的信息是否完整，即信息是否被篡改或部分删除等。

4. 不可否认性

电子商务系统应有效防止商业欺诈行为的发生，保证商业信用和行为的不可否认性，保证交易各方对已做交易无法抵赖。

传统交易中，交易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章，确定合同、契约、单据的可靠性并预防抵赖行为的发生，也就是常说的“白纸黑字”。但在无纸化的电子交易中，就不可能再通过传统的手写签名和印章来预防抵赖行为的发生。因此，保证交易过程中的不可否认性也是电子商务活动中的一个重要的安全需求。这意味着，电子交易通信过程的各个环节都必须是不可否认的，即交易一旦达成，发送方不能否认发送的信息，接收方不能篡改他所收到的信息。

5. 匿名性

电子商务系统应确保交易的匿名性，防止交易过程被跟踪，保证交易过程中不把用户的个人信息泄露给未知的或不可信的个体，确保合法用户的隐私不被侵犯。

6. 原子性

电子商务系统中引入原子性的概念，用以规范电子商务中的资金流、信息流和物流。原子性包括钱原子性(money atomicity)、商品原子性(goods atomicity)、确认发送原子性(certified delivery atomicity)。原子性是满足商品交易的要求之一。

钱原子性定义为电子商务中的资金流守恒，即资金在电子商务有关各方的转移中既不会创生也不会消失。例如，现金交易是满足钱原子性的，购买者钱的减少等于销售者钱的增加。

首先，满足商品原子性的一定满足钱原子性。其次，必须保证购买者一旦付了款就一定会得到商品，购买者如果得到了商品则一定付了款，不存在付了款而得不到商品或者得到了商品而未曾付款的情况。

7. 有效性

电子商务系统应有效防止系统延迟或拒绝服务情况的发生。要对网络故障、硬件故障、操作错误、应用程序错误、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，保证交易数据在确定的时刻、确定的地点是有效的。

1.3 电子商务安全体系结构

电子商务的安全体系结构是保证电子商务中数据安全的一个完整的逻辑结构，同时它也为交易过程的安全提供了基本保障。电子商务的安全体系结构如图 1.4 所示。

电子商务安全系统结构由网络服务层、加密技术层、安全认证层、交易协议层、电子商务应用系统层 5 个层次组成。从图中可以看出，下层是上层的基础，为上层提供了技术支持；上层是下层的扩展与递进。各层之间相互依赖、相互关联，构成统一整体。电子商务安全问题可归结为网络安全和商务交易安全这两个方面。网络服务层提供网络安全；加密技术层、安全认证层、交易协议层、商务系统层提供商务交易安全。

计算机网络安全和商务交易安全是密不可分的，两者相辅相成、缺一不可。没有计算机网络安全作为基础，商务交易安全无从谈起；没有商务交易安全，即使计算机网络本身再安

全，也无法满足电子商务所特有的安全要求，电子商务安全也无法实现。

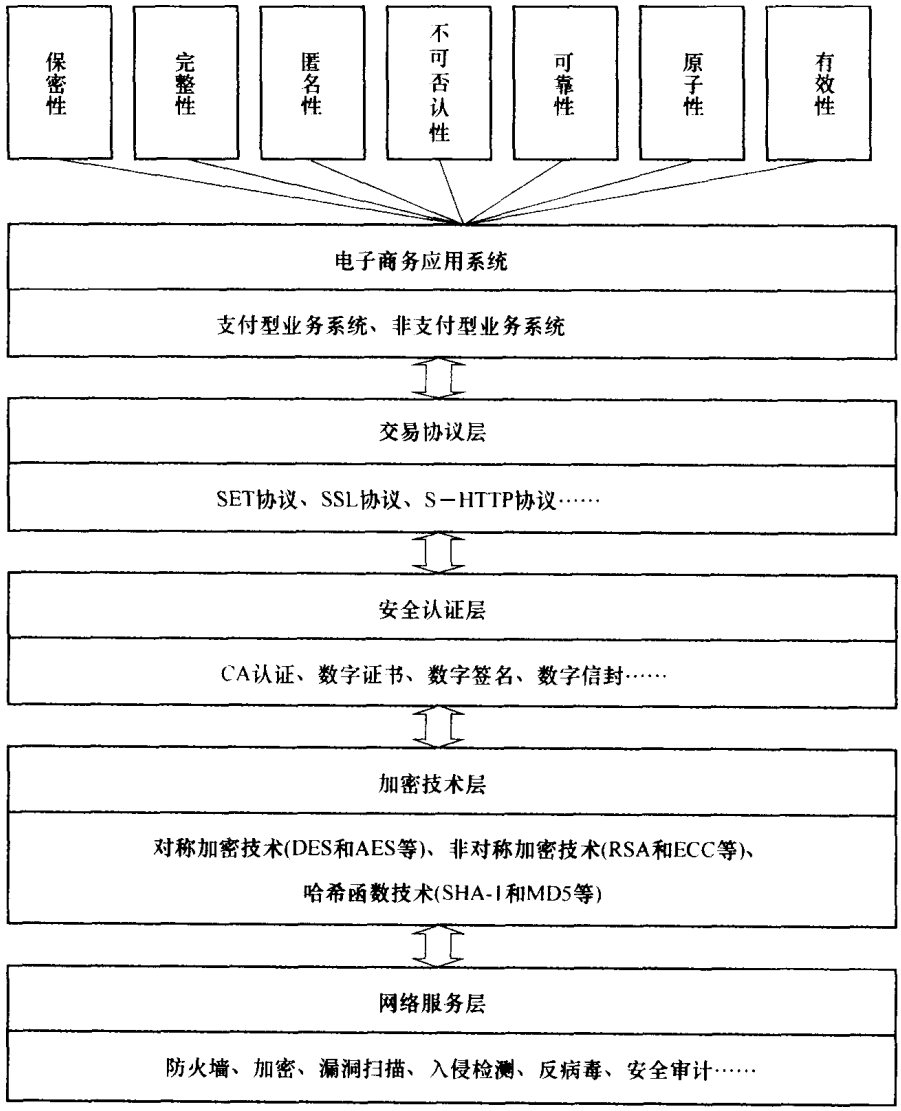

图 1.4　电子商务安全体系结构图

1.3.1　网络安全

电子商务系统是通过网络实现的，需要利用因特网的基础设施和标准，因此构成电子商务安全系统结构的底层是网络服务层。网络服务层是各种电子商务应用系统的基础，提供信息传输功能、用户接入方式和安全通信服务，并保证网络运行安全。网络服务层是电子商务应用系统的网络服务平台。

网络服务层也提供计算机网络安全。计算机网络安全主要包括计算机网络的物理安全、计算机网络系统安全和数据库安全等。网络安全主要是针对计算机网络本身可能存在的安全问题，实施网络安全方案。计算机网络安全采用的主要安全技术有防火墙技术、加密技术、漏洞扫描技术、入侵行为检测技术、反病毒技术和安全审计技术等，用以保证计算机网

络自身的安全。

1．防火墙技术

防火墙是一种常用的网络安全装置，安放在内部网络与外部网络的连接处。它既可以防止外部人员对内部网络的恶意攻击，又可以防止内部人员非法访问外部网络。但是，由于内部人员访问内部网络时不需要经过防火墙，它防止不了内部人员的攻击。有多种实现防火墙的技术，如包过滤、代理服务器、双穴主机和屏蔽子网网关等。其中实现起来比较简单的是包过滤，它是一个检查通过它的数据包的路由器，限定外部用户的数据包。其原理是监视并过滤网络上流入流出的 IP包，拒绝发送可疑的包。包过滤是运用一定的规则把一些经过它的 IP包过滤掉的方法来实现的。通常，可以根据 IP 中的以下字段来进行过滤操作：源 IP地址、目的 IP地址、TCP/UDP 源端口或 TCP/UDP 目的端口号等。

2．加密技术

数据加密技术可以用来保护网络系统中包括用户数据在内的所有数据流。只有接收信息的用户或网络设备才能够解密所加密的数据，从而在不对网络环境作特殊要求的前提下从根本上保证网络信息的完整性和可用性。

3．漏洞扫描技术

漏洞扫描是自动检测远端或本地主机安全漏洞的技术。它通过执行一些脚本文件对系统进行攻击并记录它的反应，从而发现其中的漏洞。

漏洞是硬件、软件或策略上的缺陷，这些缺陷使得攻击者能够在未授权的情况下访问甚至控制系统。漏洞的危害可以简单地用木桶原理加以说明：一个木桶能盛多少水，不在于组成它的最长的那根木料，而取决于它身上最短的那一根。同样，对于一个系统来说，它的安全性不在于它是否采用了最新的加密算法或最先进的设备，而是由系统本身最薄弱之处，即漏洞所决定的。只要这个漏洞被发现，系统就有可能成为网络攻击的牺牲品。

早期的扫描程序是专门为 UNIX 系统编写的。随着越来越多的操作系统开始支持 TCP/IP，每一种平台上都出现了扫描工具(Scanner) ,例如基于 Windows NT/Windows 2000 平台。扫描常用技术包括 ping 扫射、端口扫描、操作系统识别和穿透防火墙的扫描等。

4．入侵检测技术

入侵检测技术通过获取网络上的所有报文，并对报文进行分析处理，报告异常和重要的数据模式和行为模式，使网络安全管理员清楚地了解网络上发生的事件，以便能够采取行动阻止可能的破坏。

入侵检测可被定义为对计算机和网络资源的恶意使用行为进行识别和响应的处理过程。它不仅检测来自外部的入侵行为，同时也检测内部用户的未授权活动，还能发现合法用户滥用特权，提供追究入侵者法律责任的有效证据。该技术通过分析入侵过程的特征、条件、排列以及事件间的关系，具体描述入侵行为的迹象。这些迹象不仅对分析已经发生的入侵行为有帮助，而且对将来可能发生的入侵行为也有警戒作用。

5．反病毒技术

计算机病毒数据将导致计算机系统瘫痪，程序和数据遭受严重破坏，使网络的效率和作用大大降低，许多功能无法使用或不敢使用。反病毒技术大体分为病毒检测、病毒清除、病毒免疫和病毒预防。

对计算机病毒应以预防为主，研制出高品质预防技术，才是上策。良好的管理和安全措

施，可以大大减少病毒攻击的危险并有效地防御大多数病毒。

6. 安全审计技术

安全审计是一个安全的网络必须支持的功能特性，审计是记录用户使用计算机网络系统进行所有活动的过程，是提高安全性的重要工具。它不仅能够识别是谁访问了系统，还能指出系统正被怎样地使用。

在确定是否发生网络攻击这一点上，审计信息对于确定问题和攻击源十分重要。同时，系统事件的记录能够更迅速、更系统地识别问题，并且它是后一阶段事故处理的重要依据，为网络犯罪行为及泄密行为提供取证基础。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对已经发生或可能产生的破坏性行为提供有力的证据。

具体而言，网络的审计系统应该由三个层次组成，分别是：

(1) 网络层层次的安全审计。主要利用防火墙的审计功能、网络监控与入侵检测系统来实现。

(2) 系统的安全审计。主要利用各种操作系统和应用软件系统的审计功能实现。包括用户访问时间、操作记录、系统运行信息、资源占用等。

(3) 对信息内容的安全审计，属高层审计。

各层次的安全审计措施是网络安全系统的重要组成部分，而对审计数据的维护是其重要内容之一。

1.3.2 交易安全

交易安全是针对传统商务在因特网上运用时产生的各种安全问题而设计的一套安全技术，目的是在计算机网络安全的基础上确保电子商务过程的顺利进行，即实现电子商务的保密性、完整性、可靠性、匿名性、原子性和不可否认性等。

加密技术层、安全认证层和交易协议层一起构成电子商务交易安全。安全协议层是加密技术层和安全认证层的安全控制技术的综合运用与完善。

1. 加密技术层

加密技术是电子商务最基本的安全措施。在目前技术条件下，加密技术通常分为对称加密和非对称加密两类。

对称加密采用相同的加密算法，并只交换共享的专用密钥（加密和解密都使用相同的密钥）。如果进行通信的交易各方能够确保专用密钥在密钥交换阶段不发生泄露，可以通过对称加密方法对信息进行加密，并随加密信息发送报文摘要，以保证保密性和完整性。在对称密钥加密中，密钥安全交换是关系到对称加密有效性的重要环节。目前常用的对称加密算法有 DES、AES、IDEA 和 3DES 等。

不同于对称加密，非对称加密的密钥被分解为公开密钥和私有密钥。公开密钥和私有密钥构成一个密钥对，密钥对生成后，公开密钥以非保密方式对外公开，私有密钥则保存在密钥发布者手里。任何得到公开密钥的用户都可以使用该密钥加密信息发送给该公开密钥的发布者，而发布者得到加密信息后，使用与公开密钥相对应的私有密钥进行解密。目前，常用的非对称加密算法有 RSA 和 ECC 算法。

在对称和非对称两类加密方法中，对称加密的特点是加密速度快（通常比非对称加密快

10 倍以上）、效率高，被广泛应用于大信息量的加密。但该方法的致命缺点是密钥的传输与交换也面临着安全威胁，密钥易被截获；而且，若和大量用户通信，难以安全管理大量的密钥，因此大范围应用存在一定问题。而非对称密钥则相反，它能很好地解决对称加密中由于密钥数量过多导致管理难及费用高等问题，也无须担心传输中的私有密钥的泄露，保密性能优于对称加密技术。但由于非对称加密算法复杂，加密速度难以达到理想状态，所以目前电子商务实际运用中常常是两者结合使用。

2. 安全认证层

仅有加密技术层提供的加密技术不足以保证电子商务中的交易安全，身份认证技术是保证电子商务安全的又一重要技术手段。认证的实现包括数字签名技术和数字证书技术等。

(1) 报文摘要

通过使用单向哈希(Hash)函数将需要加密的明文“摘要”成一个固定长度（如 128 bit）的密文。不同的明文加密成不同的密文，对明文的微小改动都会造成报文摘要的完全不同；相同的明文其报文摘要必然一样。因此，利用报文摘要就可以验证通过网络传输收到的明文是否是初始的、未被篡改过的，从而保证数据的完整性。

(2)数字签名

数字签名是非对称加密技术的一种特定应用。其主要方式为：报文发送方从报文文本中生成一个报文摘要，并用自己的私有密钥对这个报文摘要进行加密，形成发送方的数字签名；然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方；报文接收方首先从接收到的原始报文中计算出报文摘要，接着再用发送方的公开密钥来对报文附加的数字签名进行解密得到报文摘要。如果这两个报文摘要相同，那么接收方就能确认该数字签名是发送方的。利用数字签名技术，接收者可以确定发送者的身份是否真实，同时发送者不能否认发送的消息，接收者也不能篡改接收的消息。

(3) 数字证书

数字证书用电子手段来标识一个用户的身份。数字证书的内部格式是由 ITU-T X.509 国际标准所规定的,包含以下内容 证书拥有者的姓名、证书拥有者的公共密钥、公共密钥的有效期、颁发数字证书的单位、数字证书的序列号。数字证书的使用涉及到数字认证中心 CA。

目前，数字证书有个人证书、企业证书和软件证书，其中前两类较为常用。个人证书仅仅为某单个用户提供凭证，用以帮助其个人在网上进行安全交易操作。企业证书通常为网上的某个 Web 服务器提供凭证,拥有 Web 服务器的企业就可以用具有凭证的互联网站点(Web Site 来进行安全电子交易。

(4) 认证中心 CA

在电子商务系统中数字证书的发放需要有一个具有权威性和公正性的第三方认证机构来承担。认证中心 CA 正是这样的一个受信任的第三方。CA 为用户签发数字证书,提供身份认证服务，是整个系统的安全核心。

在非对称密钥认证系统中，用户的签名公钥和加密密钥通常是分开的，而 CA 只知道用户的签名公钥，这样就避免了可信第三方被攻击而导致整个系统陷入瘫痪的严重问题。此外,在认证系统中,CA 只负责审核用户的真实身份并对此提供证明，而不介入具体的认证

过程，从而缓解了可信第三方的系统瓶颈问题。而且 CA 只需管理每个用户的一个公开密钥，大大降低了密钥管理的复杂性。这些优点使得非对称密钥认证系统适用于用户众多的大规模网络系统。

3. 交易协议层

除加密技术层和安全认证层提到的各种安全控制技术之外，电子商务的运行需要一套完整的安全协议。目前，比较成熟的协议有安全套接层协议、安全电子交易协议、匿名原子交易协议和 Netbill 协议等。

(1) 安全套接层协议

安全套接层协议(SSL:Secure Socket Layer)是网景(Netscape)公司于 1996 年推出的安全协议。它位于运输层和应用层之间，由 SSL 记录协议(SSL Record Protocol)、SSL 握手协议(SSL Handshake Protocol)、修改加密约定协议(Change Cipher Spec Protocol)和报警协议(Alert Protocol)组成。

在因特网中由于 TCP/IP 协议本身非常简单，没有加密、身份认证等安全特性，从而对通过因特网进行商务活动造成了很大的安全隐患，因此要向上层应用提供安全通信的机制就必须在 TCP 之上建立一个安全通信层次。在此方面，网景公司开发了可以在因特网客户与服务之间数据传送进行加密和鉴别的 SSL 协议。

SSL 握手协议被用来在客户与服务器进行传输应用层数据之前建立安全机制。当客户与服务器第一次通信时，双方通过握手协议在版本号、密钥交换算法、数据加密算法和哈希(Hash)算法上达成一致，然后互相验证对方身份，最后使用协商好的密钥交换算法产生一个只有双方知道的秘密信息，客户和服务器各自根据此秘密信息产生数据加密算法和哈希(Hash)算法参数。

SSL 记录协议根据 SSL 握手协议协商的参数，对应用层送来的数据进行压缩、加密，计算报文验证码(MAC:Message Authentication Code)，然后经网络传输层发送给对方。

修改加密约定协议由单个报文组成。该报文由值为 1 的单个字节组成，由客户机或服务器发出，用以通知接收方接下来的记录将受到刚达成的密码参数和密钥的保护。

报警协议用来在客户和服务器之间传递 SSL 出错信息。

(2) 安全电子交易协议

安全电子交易协议(SET:Secure Electronic Transactions)是由 VISA 和 Master Card 两大信用卡组织制定的标准。SET 用于划分与界定电子商务活动中消费者、网上商家、银行、信用卡组织之间的权利义务关系，给定交易信息传送流程标准。SET 主要由三个文件组成，分别是 SET 业务描述、SET 程序员指南和 SET 协议描述。SET 协议保证了电子商务系统的保密性、完整性、不可否认性和身份的合法性。

习　　题

1. 什么是电子商务？
2. 按照应用群体的角度进行分类，有哪几种类型的电子商务？
3. 电子商务的安全需求有哪些？

4. 交易安全由哪些层次构成？分别采用哪些安全技术？
5. 网络安全主要有哪些安全技术？
6. 目前通用的网上支付方式有哪些？
7. 电子商务安全主要包括哪两个部分的安全？
8. 电子商务以什么作为两大支柱？
9. 电子商务给企业带来的效益有哪些？
10. 防火墙的作用是什么？

本章参考文献

[1] 周龙骧. 电子商务协议研究综述. 软件学报,2001: 12(7)
[2] 王健. 电子商务知识讲座（第四讲电子商务的优点）. 国际贸易问题,1999(4)
[3] 王茜，杨德礼电子商务的安全体系结构及技术研究. 计算机工程,2003: 29(1)
[4] 刁兴春. 电子商务平台的安全体系研究. 计算机工程与应用,2002(16)
[5] 张玫. 浅谈银行计算机网络系统的安全防范. 计算机与用户与信息技术,2001(3)
[6] 沈苏彬. 网络安全原理与应用. 北京:人民邮电出版社,2005
[7] 韩宝明,杜鹏,刘华. 电子商务安全与支付. 北京:人民邮电出版社,2001
[8] 王斌. 基于 SET 协议的支付模型 SafePay 的研究:[学位论文]. 南京:南京理工大学,2002
[9] 何国斌. 安全电子交易 SET 协议的研究:[学位论文] 重庆:西南农业大学,2003
[10] 徐静. 电子商务环境中基于 SET 协议的电子支付平台的研究:[学位论文]. 武汉:武汉理工大学,2003
[11] 网络信息安全,http://www.hlj.gov.cn/dzzw/yyjl/P020050426606209840612.doc
[12] 电子商务的一种解决方案,http://www.ahetc.gov.cn/cit/200010/03.doc
[13] 电子商务安全,http://www.cs.ccu.edu.tw/ccc/article/ec-secure.htm
[14] 电子商务支付系统及其网络安全概述, http://www0.ccidnet.com/tech/paper/2001/09/12/58-3255.html
[15] 电子商务及架构,http://www.tongtech.com/pdf/ecommerce.pdf
[16] 电子商务分类,http://www.e-liang.com/dianzishangwu/dianzsw/005.htm

第2章 密码学基础

随着互联网的迅速发展与普及，网络已经成为人们工作、生活中不可缺少的一部分，电子商务也逐渐成为一种新型的商务活动模式。由于电子商务以开放的网络环境作为运作平台，因此不可避免地受到网络中存在的各种安全隐患的影响，比如传输的信息遭到窃听、篡改、假冒。在电子商务交易过程中往往涉及到银行卡号、密码、电子合同等敏感信息，如果这些信息受到各种安全威胁，产生的不良后果将不堪设想，因此高强度的安全性是保证电子商务顺利发展的关键和核心。

解决电子商务安全性所依赖的基础是密码学。密码学实质上属于数学的范畴，主要利用数学代数知识探讨信息的隐藏与恢复机制。为了更好地理解电子商务安全机制及安全措施，需要掌握密码学的基本理论。

本章主要介绍现代密码学的基本知识，内容包括密码学的起源与发展，密码学的基本概念和分类；现代密码学的三大密码体制——传统对称密码体制、公钥密码体制以及近几年来兴起的量子密码体制，将分别介绍各类密码体制的加／解密原理、经典的算法以及各自应用的场合。

2.1 密码学概述

在当今互联网络蓬勃发展的信息化社会，信息是人们相互联系、相互协作的主要纽带，随之而来的，如何保护信息的安全，则成了一项重要的研究课题。人们普遍认为，使用加密技术是保护信息的最基本的方法，密码学技术是信息安全技术的核心，已被广泛应用到各类交互的信息中。实质上，密码学不是现代社会才出现的概念，它的起源与发展要追溯到几千年前。

2.1.1 密码学的起源与发展

密码学的雏形始于古希腊人，他们与敌人作战时，在战场上需要与同伴传递书写有“战争机密”的信件，为了防止信件会落到敌人手中从而泄漏了战略机密，聪明的古希腊战士采取了将信中的内容“加密”的手段，这样，信中所显示的内容就不是真实的要表达的战略内容。这种情况下，即使战争信件被敌人获取，敌人也很难得到信件中所包含的军事机密。尽