# 第 1 章　电子商务安全概述

20 世纪 90 年代以来，计算机网络技术取得了快速发展，信息网络化和全球化成为不可抵挡的世界潮流。计算机网络技术一直在寻求除文字处理和信息传递领域外的更大、更直接的发展空间，商业领域成为首选，而迅速膨胀的网络用户也为网上更广泛的商业活动的开展提供了基础。

Web 技术的广泛应用，不仅使它具有通信和交换信息的功能，还开辟了一种新的商业交易方式，即在互联网上进行商业交易，实现电子交易处理。

互联网潮流所带来的优势和商机，彻底改变了全球商业的经营模式，许多非信息产业也投入其中，在互联网上可以看到各式各样的商业站点林立。如今，电子商务几乎涉及到人类生活的各个层面和领域。电子商务正在迅速发展，它推动了商业、贸易、营销、金融、广告、运输和教育等社会经济领域的创新和发展，并因此形成了一个新的产业，给各国企业和经济带来新的机遇。此外，越来越多的企业渴望通过导入电子商务来进行业务流程的重组改造，提升企业运作效率、降低经营成本，并且更进一步地优化商品和服务的品质。企业导入电子商务已经成为增强市场竞争力的主要动力。

由此可见，作为网络与商业的结合，电子商务是网络化发展的必然产物，是信息时代的商务模式，它必将有更广阔的发展前景。不过，电子商务绝不是空中楼阁，它的实现需要强有力的技术支撑，在互联网这个公共平台上，依赖强有力的技术支持，尤其是安全技术保障显得尤为重要。

## 1.1　电子商务及其系统构成

### 1.1.1　电子商务的定义

近几十年来，商业领域中使用了多种电子通信工具来完成各种交易活动。银行使用电子资金转账（EFT）技术在全球范围内转移顾客的资金；各种企业使用电子数据交换技术，利用增值网（VAN）发出订单和各种凭证；零售商针对各种商品做电视广告以吸引顾客通过电话订货。因而，从更广的意义上来说，电子商务可以通过多种电子通信手段来完成，电子商务早已有之；从狭义上来说，电子商务则是指利用互联网进行的商务活动。

对电子商务的定义至今仍没有一个很清晰的概念。各国政府、学者、企业界人士都根据自己所处的地位和对电子商务的参与程度，给出了许多表述不同的定义。比较这些定义，有助于我们更全面地了解电子商务的内涵。

1. 电子商务的定义

随着电子技术和因特网（Internet，又称国际互联网）的发展，信息技术作为工具被引入商贸活动中，产生了电子商务（Electronic Commerce，EC；Electronic Business，EB）。通俗地说，电子商务就是在计算机网络（主要指 Internet）的平台上，按照一定标准开展的商务活动。

当企业将它的主要业务通过企业内部网（Intranet）、企业外部网（Extranet）以及 Internet 与企业的职员、客户、供销商以及合作伙伴直接相连时，其中发生的各种活动就是电子商务。电子商务的定义有多种说法。下面是一些组织、政府、公司、学术团体等总结的较为全面的定义。

（1）联合国经济合作和发展组织（OECD）在有关电子商务的报告中对电子商务（EC）的定义是：电子商务是发生在开放网络上的包含企业之间（Business to Business）、企业和消费者之间（Business to Consumer）的商业交易。

（2）联合国国际贸易法委员会（UNCITRAL）对电子商务的定义是：电子商务是采用电子数据交换（EDI）和其他通信方式增进国际贸易的职能。

（3）全球信息基础设施委员会（GIIC）电子商务工作委员会报告草案中对电子商务的定义是：电子商务是运用电子通信作为手段的经济活动，通过这种方式人们可以对带有经济价值的产品和服务进行宣传、购买和结算。这种交易的方式不受地理位置、资金多少或零售渠道的所有权影响，公有私有企业、公司、政府组织、各种社会团体、一般公民、企业家都能自由地参加广泛的经济活动，其中包括农业、林业、渔业、工业、私营和政府的服务业。电子商务能使产品在世界范围内交易并向消费者提供多种多样的选择。

（4）国际标准化组织（ISO/IEC）关于电子商务谅解备忘录对电子商务的定义是：电子商务（EB）是企业之间、企业与消费者之间信息内容与需求交换的一种通用术语。

（5）IBM 公司的电子商务（E-Business）概念：在网络计算机环境下的商业化应用，不仅仅是硬件和软件的结合，也不仅仅是我们通常意义下强调交易的狭义的电子商务（E-Commerce），而是把买方、卖方、厂商及其合作伙伴在因特网（Internet）、企业内部网（Intranet）和企业外部网（Extranet）结合起来的应用。它同时强调这三部分是有层次的：只有先建立良好的 Intranet，建立好比较完善的标准和各种信息基础设施，才能顺利扩展到 Extranet，最后扩展到 E-Commerce。

（6）HP 公司提出电子商务（EC）、电子业务（EB）、电子消费（EC）和电子化世界的概念。电子商务（E-Commerce）的定义是：通过电子化手段来完成商业贸易活动的一种方式。电子商务使我们能够以电子交易为手段完成物品和服务等的交换，是商家和客户之间的联系纽带。它包括两种基本形式：商家之间的电子商务和商家与最终消费者之间的电子商务。电子业务（E-Business）的定义是：一种新型的业务开展手段，通过基于 Internet 的信息结构，使得公司、供应商、合作伙伴和客户之间，利用电子业务共享信息。电子业务不仅能够有效地增强现有业务进程的实施，而且能够对市场等动态因素作出快速响应并及时调整当前业务进程。更重要的是，电子业务本身也为企业创造出了更多、更新的业务运作模式。电子消费（E-Consumer）的定义是：人们使用信息技术进行娱乐、学习、工作、购物等一系列活动，使家庭的娱乐方式越来越多地从传统电视向 Internet 转变。

（7）通用电气公司（GE）对电子商务的定义是：电子商务是通过电子方式进行商业交易，分为企业与企业间的电子商务、企业与消费者之间的电子商务。企业与企业间的电子商务以 EDI 为核心技术，以增值网（VAN）和因特网（Internet）为主要手段，实现企业间业务流程的电子化，配合企业内部的电子化生产管理系统，提高企业从生产、库存到流通（包括物资和资金）各个环节的效率。企业与消费者之间的电子商务以 Internet 为主要服务提供手段，实现公众消费和服务提供方式以及相关付款方式的电子化。

（8）美国政府在其《全球电子商务纲要》中指出：电子商务是通过 Internet 进行的各项

商务活动，包括广告、交易、支付、服务等活动，全球电子商务将会涉及世界各国。

总结起来，可以这样说：从宏观上讲，电子商务是计算机网络的又一次革命，是通过电子手段建立一种新的经济秩序，它不仅涉及电子技术和商业交易本身，而且涉及诸如金融、税务、教育等社会其他层面。从微观角度说，电子商务是指各种具有商业活动能力的实体（生产企业、商贸企业、金融机构、政府机构、个人消费者等）利用网络和先进的数字化传媒技术进行的各项商业贸易活动。

虽然至今人们尚未对电子商务有一个统一的、明确的定义，但实际上电子商务并非是刚刚诞生的新事物。它的发展历史非常悠久，早在电报出现时，就有了以莫尔斯码点和线的形式在电线中传输的商贸活动，这开辟了运用电子手段进行商务活动的新纪元。商务统计报表认为，世界上真正对电子商务发展的研究开始于 20 世纪 70 年代。对电子商务发展影响最大的是电子数据交换（EDI，Electronic Data Interchange）技术的发展和 Internet 的发展。

### 1.1.2　电子商务的内涵

对于电子商务，无论广义还是狭义的定义，它们应当具有比较一致的内涵：

（1）电子商务的本质是“商务”，是在“电子”基础上的商务。“商务”解决做什么的问题，而“电子”则解决怎么做的问题。对于高科技的应用是电子商务的手段和效果，而非目的。

（2）电子商务的前提是商务信息化。计算机应用和信息化建设是其基础。它不只是在网上销售商品，还应和企业内部管理、售后服务支持等结合起来，这样的连接必须依靠企业管理信息化。

（3）电子商务的核心是人。电子商务是一个社会系统，它的中心必然是人。电子商务的出发点和归宿是商务，商务的中心是人或人的集合。电子工具的系统化应用也只能靠人。电子商务涉及的人员目前可以分为三类：第一类是技术人员，他们主要负责电子商务系统的实现和技术支持；第二类是商务人员，他们主要负责各种商务活动具体业务的处理；第三类是中高级管理人员，他们的职责是电子商务战略规划、业务流程管理、安全管理等。

（4）电子商务是对传统商务的改良而不是革命。从本质上来说，电子商务并没有脱离传统商务的业务流程，而是将传统商务赖以生存的实物市场交易移到了虚拟的网络空间，在传统环境下开展商务活动的关键因素仍然不可缺少。

（5）电子工具必定是现代化的。所谓现代化工具是指当代技术成熟、先进、高效、低成本、安全、可靠和方便操作的电子工具。

（6）对象的变化也是至关重要的。以往的商务活动主要是针对实物商品进行的商务活动，电子商务则首先要将实物的商品虚拟化，形成信息化（数字化和多媒体化）的虚拟商品，进而对虚拟商品进行整理、存储、加工传输。

### 1.1.3　电子商务的特征

正如前文所述，电子商务是将企业的业务流程进行改良，即是将信息流、物流和资金流进行分类和重组，以电子化方式通过网络来实现。这一切都必然要依赖于电子商务所蕴含的技术特征和应用特征。

1. 电子商务的技术特征

（1）信息化。电子商务是以信息技术为基础的商务活动，它的进行必须通过计算机网络

系统来实现电子化信息的交换和传输。电子商务的发展与信息技术的发展密切相关，正是信息技术的发展推动了电子商务的发展。

（2）虚拟化。电子商务是在数字化的虚拟电子市场（Electronic Marketplace）进行的。电子商务不受物理时空概念的限制。

（3）集成性。电子商务是一种新兴产物，其中用到了大量新技术，但并不是说新技术的出现就必然导致老设备的死亡。互联网的真实商业价值在于协调新老技术，使用户能更加行之有效地利用已有的资源和技术，更加有效地完成他们的任务。

电子商务的集成性，还在于事务处理的整体性和统一性，它能规范事务处理的工作流程，将人工操作和电子信息处理集成为一个不可分割的整体。这样不仅能提高人力和物力的利用，也提高了系统运行的严密性。

（4）可扩展性。要使电子商务在变化的商业环境里正常运行，必须保证其可扩展性。电子商务中，耗时仅 2min 的重新启动也可能导致大量客户流失，因而可扩展性极其重要。

1998 年日本长野冬奥会的官方万维网节点的使用率是有史以来基于互联网应用中最高的，短短的 16 天，该节点就接受了将近 6 亿 5 千万次访问。全球体育迷将数以百万计的信息直接通过体育迷电子邮件节点发给运动员，而与此同时，还成交了 600 多万笔交易。这些惊人的数字说明，随着技术的日新月异，电子商务的可扩展性将不会成为瓶颈所在。

（5）安全性。安全性是电子商务中的核心问题。缺乏安全的电子商务不可能吸引顾客，企业和企业的交易更是如此，也会限制企业运用计算机网络传递商业信息。欺骗、窃听、病毒和非法入侵等攻击行为都无时无刻不在威胁着电子商务，要求电子商务经营者提供一种端到端的安全解决方案。安全技术包括加密解密机制、认证技术、安全交易协议、计算机网络系统的安全管理（存取管理、防火墙、安全服务器等）。目前，有代表性的安全电子交易协议主要有安全套接层（SSL）和安全电子交易（SET）等。电子商务安全技术的发展和标准的制定，逐步使电子商务企业能够建立起安全的电子商务环境。

（6）系统性。电子商务系统的实施必须考虑企业外的合作伙伴或政府，必须规划如何加入到已有的电子商务系统中。

2. 电子商务的应用特征

（1）商务性。电子商务最基本的应用特性为商务性，即提供买、卖交易的服务、手段和机会。网上购物提供一种客户所需要的方便途径。因而，电子商务对任何规模的企业而言，都是一种机遇。

就商务性而言，电子商务可以扩展市场，增加客户数量；通过将互联网信息连至企业后端的数据库，企业能记录下每次访问、销售、购买形式、购货动态以及客户对产品的偏爱，这样企业就可以通过统计这些数据来获知客户最想购买的产品是什么。

（2）服务性。电子商务时代企业越来越重视客户的需求，这种需求不仅仅是产品的，同时也包括服务的。互联网应用使得企业能自动处理商务过程，并不再像以往那样强调公司内部的分工。企业通过将客户服务过程移至互联网上，使客户能以一种较过去更加简捷的方式获得服务。显而易见，电子商务提供的客户服务具有一个明显的特性：便利。例如比利时的塞拉银行，通过电子商务，使得客户能全天候地存取资金账户，快速及时地阅览相关利率信息，服务质量大为提高。

（3）协调性。商务活动是一个需要各方协调的过程，许多组织都提供了交互式的协议，

电子商务活动可以在这些协议上完成。

传统的电子商务解决方案能加强公司内部相互作用，电子邮件就是其中一种。但那只是协调员工合作的一小部分功能。利用互联网将供货方连接至客户订单处理系统，这样公司就节省了时间，消除了纸张文件带来的繁琐过程，提高了效率。

（4）社会性。从宏观上讲，电子商务是计算机网络的第二次革命，是在通过电子手段建立一个新的经济秩序。它不仅涉及电子技术和商业交易本身，还涉及诸如金融、税务、教育等社会其他层面，以及使用电子虚拟市场的法律和竞争规则形成等。电子商务的发展和应用是一个社会性的系统工程，缺少任何一个环节都势必影响它的发展，如电子商务交易的税收等敏感问题。

（5）全球性。Internet 是一个公共开发的平台，根据美国互联网协会的定义，互联网是一种“组织松散、国际合作的互联网络”，是一种由 TCP/IP 组织起来的国际互联网络。电子商务面对的是一个全球性统一的电子虚拟市场。它为企业跨国发展提供了平等的竞争机会。

### 1.1.4　电子商务系统构成

1. 电子商务系统的分类

在了解了电子商务的内涵后，本节进一步讨论电子商务的分类和构成。对于不断发展的各类电子商务系统，可以从不同的角度进行分类。

（1）按照商品交易过程完整程度分类。

1）完全电子商务：是指产品或服务的交易过程（信息流、物流和资金流）都在网上实现的电子商务。一些数字化的无形产品和服务，如计算机软件、电子书籍、娱乐内容（影视、游戏、音乐等）、远程教育、网上订房、网上订票以及电子证券等，供求双方直接在网络上完成订货或申请服务、货款的电子支付与结算、实施服务或产品交换（即从网络上下载产品等）的全过程，而无需借助其他手段。

2）不完全电子商务：是指商品交易的全过程不能完全在网络上实现的电子商务。一些物质和非数字化的商品交易只能在网络上完成信息流和资金流，而物流的完成则需要借助于其他一些外部辅助系统，如企业自营物流系统、第三方物流系统及第四方物流系统。

（2）按照使用网络的类型来分类。

1）基于 EDI 的电子商务：按照国际标准化组织（ISO）的定义，EDI 就是指“将商业或行政事务处理按照一个公认的标准，形成结构化的事务处理或文档数据格式，从计算机到计算机的电子传输方法”。EDI 通过传递标准数据流可以避免人为的失误，降低成本，提高效率。在 20 世纪 80 年代末，发达国家 EDI 的迅速发展，不仅引发了全球范围的无纸贸易热潮，同时也促进了与商务过程有关的各种信息技术在商业、制造业、基础工业及服务业的广泛应用，实现了商务运作全过程的电子化。

2）基于 Internet 的电子商务：20 世纪 90 年代以来，Internet 风靡全球，基于 Internet 的电子商务应运而生。这时的电子商务是基于计算机和软件以及在通信网络上从事的经济活动。通过这种方式，人们可以利用 Internet 来进行交流和从事电子交易活动。

3）基于 Intranet 的电子商务：Intranet 是在 Internet 基础上发展起来的企业内部网，或称内联网，用以实现企业内部业务处理、管理和通信。

（3）按照交易对象分类。

1）企业对企业的电子商务（Business to Business，B2B）：采购商和采购商在 Internet 上进行谈判、订货、签约、接收发票和付款，以及索赔处理、商品发送管理和运输跟踪等所有活动。

2）企业对消费者的电子商务（Business to Consumer，B2C）：是指企业通过 Internet 为消费者提供的实现订购商品或服务的活动。企业对消费者的电子商务基本上表现为网上在线零售形式，如书籍、鲜花、计算机、汽车等。

3）企业对政府的电子商务（Business to Government，B2G）：覆盖企业与政府之间的各项事务如政府采购、税收、商检、管理条例发布以及法规政策的颁布等。

4）消费者对政府的电子商务（Consumer to Government，C2G）：是指消费者与政府之间进行的电子商务和事务合作活动，包括政府面向个人消费者的电子政务。如个人网上纳税、网上事务审批、电子身份认证和社会福利金的支付等。

5）消费者对消费者的电子商务（Consumer to Consumer，C2C）：是指消费者与消费者之间在网上进行的电子商务或网上事务合作活动。多数为小额的交易，如通过互联网进行个人财物的拍卖活动等。

2. 电子商务系统的基本组成

电子商务系统的基本组成有计算机网络、用户、配送中心、认证中心、银行、商家等，如图 1.1 所示。网络包括 Internet、Intranet、Extranet；用户分为个人用户和企业用户；认证中心（CA）是受法律承认的权威机构，负责发放和管理电子证书，使网上交易的各方能互相确认身份；物流中心接收商家的送货请求，组织运送无法从网上直接得到的商品，跟踪商品的流向，将商品送到消费者手中；网上银行在 Internet 上实现传统银行的业务，为用户提供 24 小时实时服务。

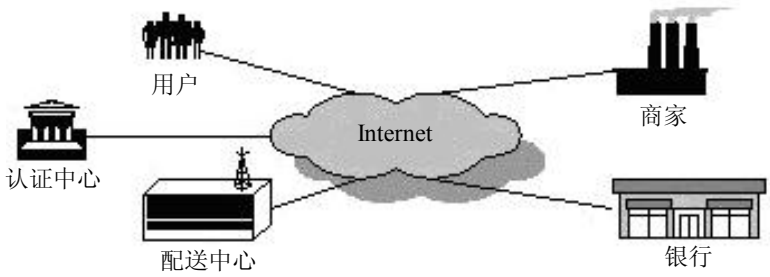


图 1.1　电子商务的基本组成

## 1.2　电子商务安全

Internet 拉近了人们之间的空间距离，使人们在 Internet 上进行交易时根本不需要考虑地域的概念，不论身在何处，都可以随时交易。Internet 使交易双方在交易过程中无需面对面，这方便了交易各方，但也带来了极大的安全隐患。例如，交易各方的通信有没有安全保障？交易各方的身份是否真实？交易的结果是否具有效力？如果电子商务交易的安全不能得到保证，人们一定不会选择网上购物。因此，如何保证电子商务交易双方的安全，就成为普及电子商务的关键。

### 1.2.1　电子商务安全概述

电子商务一个重要的技术特征就是利用互联网技术来传输和处理商业信息。因此，电子商务安全可以从整体上分为两大部分：计算机网络安全和商务交易安全。计算机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，实施网络安全增强方案，以此来保证计算机网络自身的安全性为目标，主要包括设备安全、计算机网络系统安全、数据库安全等；商务交易安全则紧紧围绕传统商务在互联网上应用时可能遇到的各种安全问题，在计算机网络安全的基础上，保障以电子交易和电子支付为核心的电子商务过程的顺利进行。因此，电子商务安全就是在网络安全基础上，运行安全的电子商务，保障以电子交易和电子支付为核心的电子商务交易的安全。

1. 电子商务安全的表现

（1）信息安全。

信息安全是指由于各种原因引起的信息泄露、信息丢失、信息篡改、信息虚假、信息滞后、信息不完善等，以及由此带来的风险。具体的表现有：窃取商业机密、泄露商业机密、篡改交易信息、非法删除交易信息、破坏信息的真实性和完整性、接收或发送虚假信息、盗取交易成果、伪造交易信息、非法删除交易数据、交易信息丢失、病毒破坏、黑客入侵等。

信息被非法窃取或泄露可能会给有关企业和个人造成严重的后果、带来巨大的经济损失；如果不能及时得到准确完备的信息，企业和个人就无法对交易进行正确的分析和判断，做出理性的决策；非法删除交易信息和交易数据丢失可能导致经济纠纷，给交易的一方或者多方造成经济损失。

（2）交易安全。

交易安全是指电子商务交易过程中存在的各种不安全因素，包括交易的确认、产品和服务的提供、产品和服务的质量、价款的支付等方面的问题。

由于电子商务不同于传统商务的市场松散化、主体虚拟化、交易网络化、货币电子化、结算瞬间化等特点，导致电子商务交易的风险表现出新的形式并且风险被放大。交易安全问题在现实中的表现主要有：卖方利用信息优势，以次充好，发布虚假信息、欺骗消费者，这种情况在淘宝网等电商平台上尤其常见。卖方利用参与者身份的不确定性与市场进出的随意性，在提供服务方面不遵守承诺，或者买方不遵守承诺。

（3）财产安全。

财产安全是指由于各种原因造成电子商务参与者面临的财产等经济利益风险。财产安全往往是电子商务安全问题的最终形式，也是信息安全问题和交易安全问题的后果。

财产损失主要表现为财产损失和其他经济损失。前者如客户银行资金被盗，交易者被冒名，其财产被冒领；后者如信息的泄露、丢失导致企业的信誉受损，遭遇网络攻击和故障导致电子商务系统效率下降或者瘫痪等。

2. 电子商务网上交易的安全性

电子商务发展的核心是交易的安全性，由于 Internet 本身的开放性，使网上交易面临着种种危险，也由此提出了相应的安全控制要求。电子商务安全的基本要求，主要包括：机密性、完整性、可用性、可认证性和抗抵赖性。

（1）机密性。

机密性是指保证信息为授权者享用而不泄露给未经授权者。在电子商务系统中，交易中

发生、传递的信息均有保密的要求。如果信用卡的账号和用户名被知悉就有可能被盗用；订货和付款的信息被竞争对手获悉，就有可能丧失商机。因此在电子商务的传播中，一般均有加密的要求。电子商务作为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子商务建立在一个较为开放的网络环境上，维护商业机密是电子商务全面推广的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取，机密性一般通过密码技术对传输的信息进行加密处理来实现。

（2）完整性。

完整性是指保证只有被授权的各方，能够修改计算机系统中有价值的内容和传输的信息，修改包括对信息的书写、改变状态、删除、创建、延时或重放。

电子商务简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商业信息完整性的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的不一致。此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。

（3）可用性。

可用性是指保证信息和信息系统随时为授权者提供服务，而不会出现非授权者滥用却对授权者拒绝服务的情况。

消费者准备在网络上购买商品时，需要了解商品的价格、性能、质量等信息，决定购买后，要提交订购信息，提交支付相关的信息。这些电子信息都要求电子商务系统能够随时提供稳定的网络服务，这就是对电子商务系统可用性的要求。如果电子商务系统被攻击而无法提供服务，则整个电子商务交易就会被迫中断。

（4）可认证性。

认证是指提供对通信中对等实体和数据来源的鉴别。

由于电子商务交易系统的特殊性，企业或个人的交易通常都是在虚拟的网络环境中进行，所以对个人或企业实体进行身份确认成了电子商务中很重要的一环。网络交易是在相互不见面的情况下确认对方的身份，这意味着当某人或实体声称具有某个特定身份时，鉴别服务将提供一种方法来验证其声明的正确性。对身份的认证一般通过证书机构（CA）和证书来实现。

（5）抗抵赖性。

抗抵赖是指防止参与某次通信交换的任何一方事后否认本次通信或通信的内容。

由于商情千变万化，交易一旦达成是不能被否认的，否则必然会损害一方的利益。例如订购黄金，订货时进价较低，但收到订单后，金价涨了，如何处理？因而要通过交易合同、契约或贸易单据等书面文件上手写签名或印章，来确定合同、契约、单据的可靠性并预防抵赖行为的发生。在无纸化的电子商务方式下，通过手写签名和印章来预防交易过程中的抵赖行为已不现实，这就需要在交易信息传输过程中为参与交易的个人、企业或国家提供可靠的电子标识，预防数字世界里的抵赖行为。

综上所述，要保证电子商务实施过程中的机密性、完整性、可用性、可认证性和抗抵赖性，需要数据加密技术、消息摘要、数字签名、认证技术和 SSL 安全协议等多种技术共同完成。

### 1.2.2　电子商务安全现状

1. 电子商务的安全问题日益受到重视

以 Internet 技术为基础的电子商务，每天需要进行千百万次的交易。Internet 本身是一个高度开放性的网络，这与电子商务所需要的保密性是矛盾的，而 Internet 又没有完整的网络安全体制。因此，基于 Internet 的电子商务在安全上无疑会受到严重威胁，电子商务交易的安全性问题将是实现电子商务快速健康发展的关键。

在电子商务的发展过程中，各产业对网络的技术依赖达到空前的程度。军事、经济、社会、文化各方面都越来越依赖于网络。这种高度依赖性使社会变得十分“脆弱”，一旦计算机网络受到攻击不能正常运作时，整个社会就会陷入危机的泥沼。因此，电子商务安全日益受到各国的高度重视。

2. 黑客的威胁上升

随着经济信息化进程的加快，计算机网络上黑客的破坏活动也随之猖獗起来。黑客及黑客行为已对经济秩序、经济建设、国家信息安全构成严重威胁。“黑客”是英语“Hacker”的音译，原意是指有造诣的电脑程序设计者，现在则专指那些利用自己掌握的电脑技术偷阅、篡改或窃取他人机密数据资料，甚至在网络上犯罪的人，或者是指利用通信软件，通过网络非法进入他人的电脑系统，截获或篡改他人计算机中的数据，危害信息安全的电脑入侵者。

黑客的袭击在网络应用发达的国家造成的危害尤为严重。在这些国家，黑客组织在 Internet 上公开网址、信道，提供免费的黑客工具软件，介绍黑客手法，出版网上黑客杂志和书籍，因此普通人很容易学会各种网络攻击方式。目前，国际黑客对各国计算机系统中高度保密信息的攻击和窃取越来越频繁。例如，黑客对美国国防部计算机系统的攻击行动每年达 25 万次以上，并且还在不断增长。

电子商务系统在防不胜防的破坏性活动面前有时会显得软弱无力，谁都无法预测将会受到什么样的威胁。信息安全漏洞之所以难以堵塞，一方面是由于缺乏统一的信息安全标准、密码算法，协议在安全与效率之间难以两全；另一方面则是由于大多数管理者对网络安全不甚了解。另外，信息犯罪属于超越国界的高技术犯罪，要用现有的法律来有效地防范十分困难，现有的科技手段也难以侦察到计算机恐怖分子的行踪，罪犯只需要一台计算机、一根网线、一个网卡就能远距离作案。

上述种种原因，无形中加大了依法惩治黑客犯罪行为的难度，给反黑客工作带来相当大的困难。一方面，科学家很难开发出对保障网络安全普遍有效的技术，另一方面又缺乏足以保证网络安全措施得到实施的社会环境。随着 Internet 的普及，电子商务安全问题已成为信息时代必须尽快加以解决的重大课题。此外，基于 Internet 的电子商务在迅速发展，不难想象，黑客的攻击一旦得逞，整个商务系统瘫痪，将会造成多么巨大的损失。

3. 计算机网络病毒给电子商务造成的损失继续增加

目前电子商务的安全问题比较严重，突出表现在计算机网络安全和商业诚信问题上。计算机网络病毒给电子商务造成了非常大的损失，可以这样说，没有哪一台计算机没有感染过计算机病毒，绝大多数计算机都受到过计算机病毒的破坏。

（1）木马病毒爆炸性增长，变种数量快速增加。

据统计，2015 年 1～6 月，瑞星“云安全”系统共截获新增病毒样本 1924 万余个，新增

木马病毒占总体病毒的 66.96%，依然是第一大种类病毒。病毒不仅增速变快，而且向智能化方向发展。总体而言，目前的新木马不多，更多的是原木马的变种，因为目前反病毒软件的升级速度越来越快，病毒存活时间越来越短，因此，如今的病毒投放者不再投放单一的病毒，而是通过病毒下载器来进行病毒投放。病毒下载器可以自动从指定的网址下载新病毒，并进行自动更新，令用户永远也无法斩尽杀绝所有的病毒。同时病毒制造者和传播者利用病毒木马技术进行网络盗窃、诈骗活动，通过网络贩卖病毒、木马，教授病毒编制技术和网络攻击技术等形式的网络犯罪活动明显增多，电子商务网络犯罪也逐渐开始呈公开化、大众化的趋势。

（2）网络病毒传播方式发生变化。

过去，病毒的传播通过网络进行。目前，通过移动存储介质传播病毒的案例显著增加，存储介质已经成为电子商务网络病毒感染率上升的主要原因。由于 U 盘等移动存储介质广泛使用，病毒、木马通过 autorun.inf 文件自动调用执行 U 盘中的病毒、木马等程序，然后感染用户的计算机系统，进而感染其他 U 盘。从网络监测和用户寻求帮助的情况来看，大量的网络犯罪通过“挂马”方式来实现。“挂马”是指在网页中嵌入恶意代码，当存在安全漏洞的用户访问这些网页时，木马会侵入用户系统，然后盗取用户敏感信息或者进行攻击、破坏。通过浏览网页的方式进行攻击的方法具有较强的隐蔽性，用户更难发现，潜在的危害性也更大。

（3）网络病毒给电子商务造成的损失继续增加。

调查显示，浏览器配置被修改、数据损坏或丢失、系统的使用受限、网络无法使用、密码被盗等都会给电子商务造成严重的破坏后果。2006 年“熊猫烧香”病毒利用蠕虫病毒的传播能力和多种传播渠道帮助木马传播，攫取非法经济利益，给被感染的用户带来重大损失。继“熊猫烧香”之后，复合型病毒大量出现，如仇英、艾妮等病毒。同时，网上贩卖病毒、木马和僵尸网络的活动不断增多，利用病毒、木马技术传播垃圾邮件和进行网络攻击、破坏的事件呈增多态势。

4. 电子商务金融系统的安全缺乏保障

电子商务金融使资金流动在网络里得以实现。同传统的金融管理方式相比，电子商务金融管理很不完善，于是电子商务金融系统成了网络犯罪分子的新目标。

随着电子商务的发展，我国电子商务金融系统中发生的计算机犯罪案件也越来越多。近年来最大一起电子商务金融系统中的计算机犯罪案件造成的经济损失高达人民币 2100 万元。目前，利用计算机网络进行电子商务金融犯罪的案件越来越多。对我国电子商务金融系统安全现状，专家们有一些形象的比喻：使用不加锁的储柜存放资金（电子商务企业缺乏安全防护）；使用“公共汽车”运送钞票（电子支付系统缺乏安全保障）；使用“邮政托寄”的方式传送资金（转账支付缺乏安全渠道）；使用“商店柜台”方式存取资金（授权缺乏安全措施）；使用“平信”邮寄机密信息（敏感信息的传递缺乏保密措施）。在针对银行的计算机犯罪案件中，具有破坏性的是篡改数据的犯罪活动，而各银行对数据传递、操作、密码保护和储户密码保护都缺乏有力的安全措施。

5. 电子商务安全保障措施尚待加强

与发达国家相比，发展中国家的电子商务安全更加脆弱不堪。其原因是多方面的：发展中国家的许多部门只看重电子商务的应用带来的巨大财富，没有意识到电子商务安全系统存在的漏洞，忽视电子商务支付系统的安全防范技术，从而埋下了安全隐患；电子商务安全保卫工作严重滞后，不少企业的电子商务安全保障工作还在使用传统的“看家护院”的工作模式，行

之乏效，没有从管理制度上建立相应的电子化业务安全防范机制。

在电子商务交易中，商家、客户和银行等各参与方是通过开放的 Internet 连接在一起的，相互之间的信息传递也要通过 Internet 来进行，这一变化使得交易的风险性和不确定性加大，从而对网络传输过程中数据的安全性和保密性提出了更高的要求，尤其对于电子商务支付中涉及的敏感数据传递，则更需确保其万无一失。

电子商务的安全性是由计算机的安全性，特别是计算机网络的安全性发展而来的。安全问题是电子商务系统所要解决的核心问题。电子商务对网络及计算机应用系统提出了许多安全要求，只有建立起科学、合理的安全体系结构，才能保证电子商务交易的安全实施。

## 1.3　电子商务安全威胁

### 1.3.1　Internet 的安全威胁

Internet 的出现为信息的交换和科学、技术、文化、教育、生产的发展提供了极大的便利，并提高了现代人的生活质量，但同时 Internet 也给国家、企业和个人的信息安全带来极大的威胁。由于网络的全球性、开放性、无缝连接性、共享性、动态性发展，任何人都可以接入 Internet，在其中自由地进行商务活动。从事电子商务的有善者，也有恶者，恶者会采用各种攻击手段对电子商务系统进行破坏。他们对电子商务系统的主要威胁有：

（1）系统穿透。指未授权人通过一定手段对电子商务系统的认证性（真实性）进行攻击，假冒合法用户接入企业内部系统，篡改文件、窃取机密信息、非法使用资源等。一般采取伪装或利用系统的薄弱环节（如绕过检测控制）、窃取情报（如口令）等方式实现。

（2）违反授权。指一个获授权进入系统做某件事的用户，在系统中从事未经授权的其他活动。表面看来这是系统内部的误用或滥用问题，实际上这种威胁与外部穿透有关联。一个攻击者可以通过猜测口令的方式接入一个非特许用户账号，进而利用系统的薄弱环节，取得特许接入系统权，从而严重危及系统的安全。

（3）植入。一般在系统穿透或违反授权攻击成功后，入侵者常要在系统中植入一种能力，如向系统中注入病毒、蛀虫、特洛伊木马程序、陷门、逻辑炸弹等，为以后的攻击提供方便。例如攻击者可在系统中植入一种表面上是文字处理软件的木马程序，该程序能将所有编辑文档复制存入一个隐蔽的文件夹中，供攻击者检索。

（4）通信监视。这是通过搭线或电磁泄漏等对系统的机密性进行攻击，造成泄密或获知业务流量，从获知的业务流量中分析出有用情报。侦察卫星、监视卫星、预警卫星、预警飞机、装有大型综合孔径雷达的高空气球、无线微型传感器都可用于截获和跟踪信息。

（5）通信干扰。攻击者对通信数据或通信过程进行干预，对系统的完整性进行攻击，篡改系统中的数据，修正消息次序、时间（延时或重放），注入伪造消息。

（6）中断。对系统的可用性进行攻击，破坏系统中的硬盘、线路、文件系统等，使系统不能正常工作，毁坏信息和网络资源。高能量电磁脉冲发射设备可以摧毁附近建筑中的电子器件，有些电子生物可以吞噬电子器件。

（7）拒绝服务。指合法接入数据接口、业务口或其他资源受阻，例如，一个业务口被故意滥用而使其他用户不能正常接入；Internet 的一个地址被大量垃圾信息阻塞等。

（8）否认。即一个实体进行某种通信或交易活动后却否认曾进行这一活动。不管这种行为是有意的还是无意的，双方一旦出现类似争执再要解决就不太容易了。

发展电子商务的一个首要问题是解决电子商务的安全性和可靠性问题。任何成功的电子商务系统必须能提供足够高的安全性、可靠性和可用性的保障，才能赢得客户的信赖和欢迎。

### 1.3.2 Intranet 范围内的安全问题

1. 恶意代码

恶意代码是指那些不请自来的软件，它们可能会在 Intranet 及与之相连的系统上做出任何事情，如攻击个人计算机及更复杂的系统，包括 Intranet 上的服务器。防范恶意代码的最好办法是将它们完全拒之于门外，不幸的是这一点并不容易做到。

恶意代码通常以病毒的形式出现，它可以通过把自己附加到计算机内存或磁盘上的程序里进行自我复制。一旦恶意代码被运行或所在环境达到某种特定条件，它就会干扰系统的正常运作，如在某个特定日子里闪现出一条消息来，或篡改文件信息，甚至捣毁硬盘。

2. 物理的和基础构造上的威胁

Intranet 有时会因物理的和基础构造上的威胁而遭到损害。这类威胁有能量损耗、自然灾难（如水灾、闪电及雷击等）、物理上篡改及硬件上的破坏等。对于此类威胁，系统备份是一种简单的解决办法，它可以使 Intranet 上的数据不会受损于这种不可逆转的威胁。因此，在实施安全程序时一定要进行系统备份。

3. 黑客的威胁

黑客可能会为了各种原因闯入 Intranet。有些黑客可能只想四处逛逛，也有一些黑客可能想窃取信息或是破坏网络。在对付黑客时至关重要的一点是不要低估了他们对 Intranet 造成的损害，要事先做好安全防范工作。

4. 电子间谍的窃取

企业放在 Intranet 上的信息一般都是很有价值的，一旦竞争对手和敌人通过电子间谍从 Intranet 上窃取了企业机密文件，企业就可能会损失惨重。

5. 职员的报复

职员在心怀不满时可能会在 Intranet 上搞个恶作剧或从事破坏活动，以示报复。职员们是最熟悉公司的计算机系统的，他们清楚地知道何种操作会造成最大的危害。如果一个职员要离职，应及时地使其口令失效，并删除其所有的系统账户。

6. Intranet 的安全性弱点

在建立起一个 Intranet 并在其上使用安全程序时，应注意它可能会有许多安全性弱点。下面列举主要的两个：

（1）口令系统。口令系统是目前暴露最多的网络弱点。对口令的攻击主要是指危害一个系统的口令。据估计，网络安全问题中有 80%是由不安全的口令造成的。目前市面上有一种破解口令的软件，它带有一个猜测字典，可自行匹配一个口令，如果用户的口令可以从字典里找到，那这种软件就很容易破解该口令，攻击者可以轻易地得到这种软件。对口令攻击的防范也比较简单，只要经常更换 Intranet 上的口令即可。

（2）TCP/IP 协议。TCP/IP 协议的创建思想是使大量军事网点、研究所网点和大学网点能相互连接，目的不是为了限制访问，而是要扩展。在定义 TCP/IP 协议和其他相关协议时，

安全性并未被考虑在内。此外，使用 TCP/IP 协议传输的应用程序也是易受攻击的。

TCP/IP 协议最大的不足是无法证实一台主机的身份，一台主机比较容易冒充其他主机，并且在主机之间提供安全且秘密的传输信道也比较困难。在特定的 Intranet 环境下，这些弱点很容易被人击破。对 TCP/IP 协议弱点最常见的攻击方式可能是网络窥探和 IP 欺骗。

### 1.3.3　网络攻击

1. 脆弱脚本攻击

随着 Internet 的重要性不断提高，越来越多的应用程序都被放在 Web 服务器上运行。如果编写的应用程序脚本本身存在缺陷，并且被攻击者利用，那么用户的计算机就会处于危险之中。因此，编写应用程序的时候，一定要假设编写的代码将会运行在最具有敌意的环境中，根据这个条件来设计、编写并测试代码，以便编写安全的脚本文件。如果想检查 Web 服务器上是否运行着脆弱脚本，可以运行脆弱扫描器（免费版或商业版都可以）。如果发现有这种脆弱脚本，应当对该版本进行升级（用非脆弱版本）或换用另一种脚本。

2. Web 欺骗

Web 欺骗是一种在 Internet 上使用的针对 Web 的攻击技术，这种攻击会泄露某人的隐私或破坏数据的完整性，危及使用 Web 浏览器的用户，包括使用 Netscape Navigator 和 Internet Explorer 的用户。Web 欺骗主要表现在以下两个方面：

（1）Web 页面的欺诈。这种欺诈行为的出现是由于信息铺天盖地而来，而人们又无法辨认其真假。用户在使用计算机时，总是根据他们所看到的内容作出一些关于安全性的决定。比如，当用户登录某银行的 Web 页面，输入自己在该银行的账户和口令时，很少去想这个 Web 页面是否确实来自该银行。

（2）CGI（Common Gateway Interface，通用网关接口）欺骗。许多 Web 页面允许用户输入信息，进行一定程序的交互，还有一些搜索引擎允许用户查找含有特定信息的站点，这些一般都通过执行 CGI 程序来完成。黑客可能会修改 CGI 程序来截取或替换用户的信息。

3. 网络协议攻击

目前的网络协议尚不完善，这方面的漏洞不断地被发现。在网络中使用最普遍的协议就是 TCP/IP 协议了。TCP/IP 协议有不少安全漏洞，易受到攻击。例如，攻击者故意错误地设定数据包中一些重要的字段，然后使用 Raw Socket 编程，将这些错误的 IP 数据包发送出去。在接收数据端，由于 TCP/IP 协议存在漏洞，因而在将接收到的数据包组装成一个完整的数据包的过程中，就会使系统宕机、挂起或导致系统崩溃。

4. IP 欺骗

IP 欺骗是指通过 IP 地址的伪装使得某台主机能够冒充具有某种特权或者被另外的主机所信任的主机。IP 欺骗通常都要用编写的程序来实现，如通过使用 Raw Socket 编程，发送带有假冒的源 IP 地址的数据包，来达到自己的目的。另外，目前网上还提供大量的可以发送伪造 IP 地址的工具包，使用它可以任意指定源 IP 地址而不留下自己的痕迹。

5. 远程攻击

远程攻击是指对远程计算机的专门攻击。“远程计算机”最确切的定义是：它不是你正在其上工作的平台，而是能利用某协议通过 Internet 或任何其他网络介质来使用的计算机。进行远程攻击并不需要和攻击目标进行密切的接触，攻击者只需识别出目标机及其所在的网络的类

型便可进行攻击。而对目标机及其网络类型的识别无须干扰目标的正常工作（假设目标没有安装防火墙）。

6. 缓冲区溢出攻击

在缓冲区溢出的情况中，服务器端的接收服务或者应用程序无法很好地处理过长的字符串。总的来说，缓冲区溢出可以发生在一些特殊的元素、字段或者消息上。如果接收系统没有准备好处理未知长度的字段和消息，应用程序就会处在一个比较危险的境地。它可能造成系统的崩溃，也可能被黑客利用获得对 Web 服务器的控制。黑客会通过发送脆弱脚本，让服务器端运行一个由黑客控制的木马程序，来实现入侵的目的。

### 1.3.4 电子交易环境的安全性问题

传统商务活动都在一个切实存在的场所进行，例如在办公室、商场、银行营业厅等场所进行。电子商务活动则不同，交易的进行没有一个切实的场所，而是在虚拟的 Internet 上进行，电子商务的交易环境安全，很大程度上指的就是 Internet 的安全，而 Internet 的安全主要反映在客户机和服务器的安全上。

1. 客户机的安全性问题

在活动的 Web 内容出现前，页面是静态的，静态页面是以 Web 标准页面描述语言 HTML 编制的，其作用只是显示内容并提供到其他页的链接。在活动内容广泛应用后，这个状况就发生了变化。活动内容是指在页面上嵌入的对用户透明的程序，它可完成一些动作。

为 Web 页面提供活动内容的方式，包括图形文件和 Web 浏览器插件。而图形文件中可能包含一些隐含嵌入指令，这些指令有合法的也有非法、恶意的，当客户机下载了这些图形文件并运行它们时，它们内含的恶意指令将会破坏客户机系统。Web 浏览器插件用于解释或执行嵌入在下载图形、声音或其他对象中的指令，这也涉及恶意指令运行的问题。

活动内容的启动也会给客户机带来安全威胁。活动内容是如何启动的？用户用浏览器就可查看一个带有活动内容的 Web 页面，小应用程序会随用户所看到的页面自动下载到用户的计算机上并启动运行。这时就存在一个问题：由于活动内容模块是嵌在 Web 页面里的，对浏览页面的用户完全透明，企图破坏客户机的人可编程将破坏性的活动页面放进表面看起来完全无害的 Web 页面中，这种程序被称作木马。木马可窃取客户机上的保密信息，从而构成保密性侵害。更糟的是，木马还可改变或删除客户机上的信息，构成完整性侵害。

在 Web 页面里加入活动内容所带来的安全威胁还有：在 Web 页面潜入有恶意的程序，这种程序可使通常存在 Cookie 里的信用卡号、用户名和口令等信息泄密。因为 Internet 不能记忆从一个页面到另一个页面间的响应，而用 Cookie 可帮助 Internet 解决需要记忆关于顾客订单信息或用户名与口令等问题，所以有些恶意的活动内容利用 Cookie 截取，造成客户机端的文件泄密，甚至破坏存储在客户机上的文件。

Java 是 Sun 微系统公司开发的一种高级程序设计语言。Java 最普遍的应用是在 Web 页面上。当浏览 Web 页面时，数以千计的 Java 小应用程序随页面下载下来，只要浏览器兼容 Java，它就可以在客户机上运行。Java 是一种真正的面向对象的语言，这是一个很有用的特点，因为它支持代码重用。除在 Web 页面上应用外，Java 还可在操作系统上运行。Java 得以广泛应用的另一个原因是它与平台无关，可在任何计算机上运行。这种“一次开发，多处使用”的特点降低了开发成本，因为对所有的计算机都只需维护一种源代码即可。Java 增强了业务应用

功能。它可在客户机端处理交易并完成各种各样的操作，这就解放了非常繁忙的服务器，使其不必同时处理上千种应用。

嵌入的 Java 代码一旦下载就要在客户机上运行，这就意味着可能会威胁系统安全。为解决这个问题，专家提出了称为“Java 运行程序安全区”（Java Sandbox）的安全模式。简单地说，Java 运行程序安全区是根据安全模式所定义的规则来限制 Java 小应用程序的活动。这些规则适用于所有不可信的 Java 小应用程序。不可信的 Java 小应用程序是指尚未被证明是安全的 Java 小应用程序。当 Java 小应用程序在 Java 运行程序安全区限制的范围内运行时，它们不能访问系统中安全规定范围之外的程序代码，例如不能执行文件输入、输出或删除操作，这就防止了对保密性和完整性的破坏。

JavaScript 是网景公司开发的一种脚本语言，它支持页面设计者创建活动内容。JavaScript 得到市面上流行的各种浏览器的支持，它和 Java 语言有同样的结构。当用户下载一个嵌有 JavaScript 代码的页面时，此代码就在客户机上运行。同恶意的其他活动内容的载体一样，恶意的 JavaScript 程序会侵犯系统的保密性和完整性，会破坏硬盘，把电子函件的内容或敏感信息发送给某个 Web 服务器。另外，它还可能把所访问页面的 URL 记下来、捕捉填入任何表单中的信息等。例如，如果用户在注册时输入了信用卡号，恶意的 JavaScript 程序就可能把信用卡号复制下来。此时，在客户机到电子商务服务器之间所建立的安全通信连接对此起不到任何保护作用，因为这时破坏发生在客户机上且处于网站安全区之外。JavaScript 程序和 Java 小应用程序的区别，在于它不在 Java 运行程序安全区的安全模式限制下运行。

ActiveX 控件含有由页面设计者放在页面来执行特定任务的程序。与 Java 或 JavaSunScript 代码不同的是，ActiveX 控件只能在安装有 Windows XP 或 Windows 2003 等 Windows 系列操作系统的计算机上运行，并且只能在支持 ActiveX 控件的浏览器上运行。ActiveX 代码编完后，程序设计人员将其封装在 ActiveX 信封里，通过编译转换成机读码，再把它放到页面上。当浏览器下载了嵌有 ActiveX 控件的页面时，ActiveX 控件就可以在客户机上运行了。ActiveX 控件的安全威胁是：一旦下载后，它就能像计算机上的其他程序一样执行，能访问包括操作系统代码在内的所有系统资源。这是非常危险的，一个恶意的 ActiveX 控件可格式化硬盘、向函件通讯簿里的所有人发送电子函件、关闭计算机。由于 ActiveX 控件可全权访问用户的计算机，因此它有可能会破坏系统的保密性、完整性和响应程度。

网景公司在 Navigator 2.0 版本中引入了“Cookie”规范。Cookie 的原本目的是让 Web 服务器通过多方的 http 请求来追踪客户。Cookie 是一些 Web 服务器可以传送到使用 Netscape Navigator 的用户的 ASCII 文本。一旦接收了它，浏览器就会在每次发出一个新的文件请求时发出一个 Cookie。Cookie 被存储在浏览器的内存里，永久的 Cookie 会被保存到浏览器中。通过 Cookie 网站可以识别用户是第一次访问还是又一次访问。网站还可以利用 Cookie 了解用户对哪些内容感兴趣，收集与用户有关的信息。通过 Web 页面潜入的有恶意的程序可使通常存放在 Cookie 里的信用卡号、用户名和口令等信息泄露，尽管 Cookie 本身并没有恶意。如果用户不想在电脑里存储 Cookie，使 Cookie 失效，可以改变浏览器的设置。

图形文件、浏览器插件和电子邮件附件均可存储可执行的内容。有些图像文件的格式是专门设计的，能够包含确定图像显示方式的指令。这就意味着带这种图形的任何页面都是潜在的安全威胁，因为嵌入在图形中的代码可能会破坏计算机。同样，浏览器插件是增强浏览器功能的程序，即完成浏览器不能处理的页面内容。插件通常都是有益的，用于执行一些特殊的任务，如播放音

乐片断、显示电影片断或动画图形。例如，QuickTime 可下载并放映特殊格式的电影片断。

许多插件都是通过执行相应媒体里的指令来完成其职责的。这就为某些企图破坏计算机的人打开了方便之门，他们可在看起来无害的视频或音频片断里嵌入一些指令，这些隐藏在插件程序所要解释的对象里的恶意指令可通过删除若干或全部文件来进行破坏。

潜伏在电子邮件附件里的安全威胁已被新闻媒体大肆报道，所以大众都非常熟悉。电子邮件的附件提供了一种在文本系统（即电子邮件）上传输非文本信息的方便方法。附件可以是文字处理文件、电子报表、数据库、图像及你能想像的任何信息。当收到附件时，大部分程序（包括最常用的浏览器电子邮件程序）都可通过自动执行所关联的程序来显示附件。例如，接收者的 Excel 程序可打开并显示所附加的 Excel 工作表，Word 程序可打开并显示 Word 文档。这个动作本身并不会带来破坏，但驻留在所下载的文档或工作表里的 Word 或 Excel 宏病毒会破坏用户的计算机或将信息泄密。宏病毒是嵌入在文件中的称为“宏”的小程序。这类电子邮件附件类型的病毒很多，如 Happy99 Worm、Triplicate 和 Chernobyl（即 CIH）。Symantec 等许多公司一直在追踪病毒并提供抗病毒软件。

信息隐蔽是指隐藏在另一片信息中的信息（如命令），其目的可能是善意的，也可能是恶意的。一般情况下，计算机文件中都有冗余的或能为其他信息所替代的无关信息。后者一般驻留在背景中，无法看到。信息隐蔽提供将加密的文件隐藏在另一个文件中的保护方式，粗心的观察者看不到后者中含有重要的信息。加密文件是使其不能被阅读，信息隐藏是使信息不被人看到。信息隐蔽相当于把一个涉及贸易秘密的加密微缩胶片贴到肖像画中人眼的瞳孔上，即隐蔽又加密。粗心的观察者只看到了人的肖像，仔细检查才会发现微缩胶片。有多家软件开发商提供了实现信息隐蔽的软件。

2. 服务器的安全性问题

对企图破坏或非法获取信息的人来说，服务器有很多弱点可被利用，下面详细介绍三个。

（1）Web 服务器的安全性漏洞。

大多数计算机上所运行的 Web 服务器可在不同权限下运行。高权限提供了更大的灵活性，允许程序运行所有指令，并可以不受限制地访问系统的各个部分（包括高敏感的特权区域）。相对而言，低权限是在所运行程序的周围设置了一层逻辑栅栏，防止程序运行全部指令，只允许程序访问一些计算机中不是很敏感的区域。安全规则是为程序提供完成工作所需的最低权限。为用户设置账号和口令的系统管理员需要很高的权限，在 UNIX 系统中称之为超级用户（Root），他有权进入系统里的敏感数据区并进行修改。Web 服务程序如果以高权限状态运行，就构成对 Web 服务器的安全威胁。在大多数情况下，Web 服务程序提供的是能完成普通服务和任务的低权限。如果 Web 服务程序在高权限下运行，破坏者就可利用 Web 服务器的高权限状态执行恶意的指令，从而造成安全隐患。

如果 Web 服务器不更改目录显示的缺省设置，它的保密性就会大打折扣。如果一个服务器文件夹名能让浏览器看到，其系统的保密性就可能被破坏。许多网站的管理员都细心地关闭了显示文件夹名的功能。如果用户想浏览已限制浏览的文件夹的内容，Web 服务器就会发出警告信息，如“你不能浏览目录”。

（2）通用网关接口的安全性漏洞。

前面已讲过通用网关接口（CGI）可以实现从 Web 服务器到另一个程序（如数据库程序）的信息传输。CGI 和接收它所传输数据的程序为网页提供了活动内容。例如，访问者要了解最

喜爱的运动队的比分，只需在网页上的列表框里填入最喜欢的运动队的名字和“比分”字样，然后提交，CGI 程序就会寻找所选运动队的最新比分，然后把比分放到一个网页上并将此新网页发给用户的浏览器。CGI 是一种程序，如果滥用就会带来安全威胁。同 Web 服务器一样，CGI 脚本能以高权限状态运行。因此，能自由访问系统资源的有恶意的 CGI 程序就能够使系统失效，甚至调用、删除系统程序或顾客的保密信息（包括用户名和口令）。

当程序员发现 CGI 程序中的错误时，会重编这个程序。运行重编的新程序后，程序员有时会忘记删除旧 CGI 程序，它们就给系统留下了安全漏洞，因为 CGI 程序或脚本会驻留在 Web 服务器的任何地方（即任何文件夹和目录下）。尽管对 CGI 程序的追踪和管理有些困难，但黑客还是能够追踪到这些已被弃用的 CGI 脚本，并检查这些程序以了解其弱点，然后利用这些弱点来访问 Web 服务器及其资源。同 JavaScript 不一样，CGI 脚本的运行不受 Java 运行程序安全区的保护。

（3）其他程序的安全性漏洞。

Web 服务器的攻击还可能来自服务器上所运行的程序。通过客户机传输给 Web 服务器或直接驻留在服务器上的 Java 或 C++程序经常需要使用缓存。缓存是指定存放从文件或数据库中读取的数据的单独的内存区域，在处理输入和输出操作时就需要用到缓存，因为计算机处理文件信息的速度比从输入设备上读取信息或将信息写到输出设备上的速度快得多，所以缓存就用作数据进出的临时存放区。例如，可把即将处理的数据库信息放在缓存中，等所有信息都进入计算机内存后，处理器操作和分析所需的数据就都准备好了。缓存的安全问题在于向缓存发送数据的程序可能会出错，导致缓存溢出，溢出的数据可能进入到指定区域之外。通常情况下这是由程序中的错误引起的，但有时这种错误是有意的。不论有意还是无意这都会导致非常严重的安全后果。

有编程经验的人都会知道，缓存溢出会导致溢出的数据或指令替代了内存指定区域外的内容，后果是程序会因遇到意外而停止运行。由恶意的程序所引起的破坏称为故意的拒绝攻击，从某种意义说，蠕虫病毒就是这样的程序，它引起的溢出会消耗掉所有系统资源，导致死机。

### 1.3.5　电子交易过程中的安全性问题

1. 电子交易的主体对象

在电子商务环境中，电子交易所涉及的主体对象主要有：

（1）客户或持卡人（Cardholder）：指电子交易中的消费者，他持有可在网上进行消费的一种或几种信用卡。

（2）发卡机构（Issuer）：指信用卡的发卡金融机构，它为消费者建立账号并发行信用卡，并要求持卡人遵守使用信用卡的有关规定（包括安全、支付授权等）。

（3）商家（Merchant）：即商品或服务提供者，它可以是从事传统产业的供应商，也可以是新兴产业中的信息或服务提供商。

（4）受卡行（Acquirer）：即商家的开户银行，负责处理信用卡的授权和支付。

（5）支付网关（Payment Gateway）：是一个由受卡行（或指定的第三方机构）操作的设备，是金融专用网与 Internet 的接口，用来处理商家的支付信息（包括客户的支付命令等）。

2. 电子交易过程

一个典型的电子交易过程是这样的：

（1）持卡人通过浏览器查看网上商户建立的购物中心主页上发布的商品。

（2）持卡人在网站上将要购买的商品添加到“购物车”。

（3）持卡人在该商户站点创建一个订单，包括商品名称、单价、总额、送货地址等内容。

（4）持卡人选择付款方式，即指定要用来付款的支付卡，如银行发行的借记卡、信用卡或电子现金。

（5）持卡人将订单和付款指令发给商户。

（6）商户将持卡人的账号信息发送到持卡人的开户银行验证。

（7）商户接收订单。

（8）商户按订单要求将货物发给持卡人。

（9）商户与持卡人开户银行结清货款。

3. 电子交易双方面临的安全威胁

对于商务交易而言，交易对象的可靠性和交易过程的安全性直接关系到交易的成功与否。电子商务活动进行的场所是因特网，而因特网的安全性及交易双方的身份认证目前还需进一步加强，因而电子商务交易双方建立安全和信任关系相当困难。电子商务交易双方（销售者和消费者）都面临不同的安全威胁。

对商户而言，面临的安全威胁主要有：

（1）中央系统安全性被破坏；入侵者假冒合法用户来改变用户数据（如商品送达地址）、解除客户订单或生成虚假订单。

（2）客户资料被竞争者获悉。

（3）被他人假冒，进行不法交易，从而损害公司信誉。

（4）消费者收到货物后不付款。

对消费者而言，面临的安全威胁主要有：

（1）虚假订单。一个假冒者可能会以消费者的名字来订购商品，而且有可能收到商品，而此时真正的消费者却被要求付款或返还商品。

（2）付款后没有收到商品。在付款后，商户方面由于种种原因不发货。

（3）信息机密性丧失。消费者有可能将个人的私密数据或自己的身份数据（PIN 码、口令等）发送给冒充销售商的机构，这些信息也可能会在传递过程中被盗取。

（4）拒绝服务。攻击者可能向商户的服务器发送大量的虚假订单来穷竭它的资源，从而使消费者不能享受到正常的服务。

4. 黑客攻击电子交易过程的常用手段

黑客们攻击电子商务系统的手段大致可归纳为以下几种：

（1）中断（攻击系统的可用性）：破坏系统中的硬件，包括硬盘、线路以及破坏文件系统等，使系统不能正常工作。

（2）窃听（攻击系统的机密性）：通过搭线或电磁泄漏等手段造成泄密，或对业务流量进行分析，获取有用情报。

（3）篡改（攻击系统的完整性）：篡改系统中的数据内容，修改消息次序、时间（延时和重放）。

（4）伪造（攻击系统的真实性）：将伪造的假消息注入系统，假冒合法人接入系统，重发截获的合法消息以实现非法目的，否认消息的接收或发送等。

### 1.3.6　网上支付的安全性问题

1. 电子支付所面临的安全隐患

电子支付虽然具有诸多优点，但是其风险也是显而易见的。它所面临的安全隐患主要体现在以下几个方面：

（1）电子支付制度和传统的付款方式一样，都会因为被他人冒领、盗领款项而导致损失。电子支付制度若无法保障交易安全，可能会使消费者遭受更大的财务损失。

（2）电子支付系统若发生断线、操作错误等问题时，可能对消费者造成经济损失。消费者在利用电子支付方式时，可能会面临虽然有钱，但是却因为断线、厂商拒收或是其他原因，而无法在一定时间、地区完成特定金额交易的困扰。

（3）使用电子支付时，所有的付款资讯可能未经消费者的同意即被收集或是向第三人披露，甚至被冒用或是被其他有可能损害消费者利益的不法人员使用。

（4）电子支付工具的使用，亦可能产生新的犯罪问题。例如：电子支付工具可能会刺激洗钱这种违法活动产生，或是被用于网络赌博。此外，电子支付工具本身也可能成为犯罪的目标，如伪造、编造、诈欺等犯罪行为可能会以电子支付工具为目标。

2. 电子支付的安全需求

一个安全、有效的支付系统是保障电子商务活动安全平稳进行的重要前提。网上支付系统的安全需求主要表现为以下几个方面：

（1）使用数字签名和数字证书实现对各方的认证，以证实各方身份的合法性。

（2）使用加密算法对信息进行加密，以防止未被授权的非法第三者了解消息的真正含义。

（3）使用信息摘要以保证信息传输的完整性。

（4）保证交易的不可抵赖性。当交易双方出现异议、纠纷时，支付系统必须能够提供足够充分的证据来迅速辨别纠纷中的是与非。

（5）处理多方贸易业务的多边支付问题，可以通过双联签字等技术来实现。

## 1.4　电子商务安全的保障

电子商务安全需要一个完整的综合保障体系。谈及电子商务安全，人们首先想到的是技术保障措施。其实单从技术角度建立安全保障是不足的，还应当采用综合防范的思路，从技术层面、组织管理层面以及法律层面等方面全面地加以防范。

电子商务的安全概括起来需要三个方面的支持：一是信息技术方面的措施，如防火墙、网络防毒、信息加密、身份认证等；二是信息安全管理制度的保障；三是社会的法律政策与法律保障。三者缺一不可，只有共同作用，才能最终保障电子商务的安全。

### 1.4.1　电子商务安全技术

电子商务安全技术日趋成熟，主要技术手段已逐渐形成国际行业规范。电子商务一般是通过 Internet 进行的，为了提高电子商务活动的安全性，除了采用先进的网络安全技术外，还必须具备有效的信息安全机制，这就是电子商务安全交易体系。概括起来，该体系包括 3 个层次：信息加密算法、安全认证技术和安全交易协议，如图 1.2 所示。

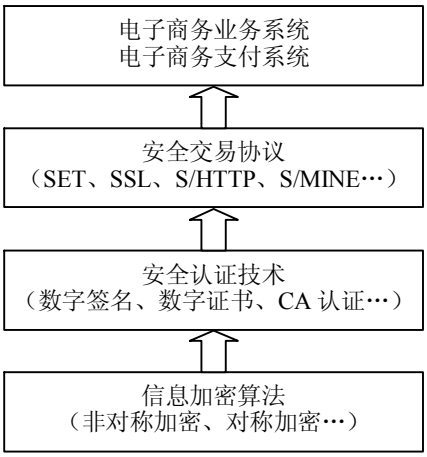


图 1.2　电子商务安全交易体系

1. 加密解密技术

加密技术是信息安全技术的一个重要组成部分。加密就是用基于数学方法的程序和保密的密钥对信息进行编码，把计算机数据变成一堆杂乱无章、难以理解的字符串，也就是把明文变成密文。通俗地说，加密如同将声音变成噪声、把图像变成雪花。所以加密可以有效地对抗信息被拦截以及被窃取。

加密技术与密码学紧密相连。密码学这门古老而又年轻的科学包含着丰富的内容，它包括密码编码学和密码分析学。密码体制的设计是密码编码学的主要内容，其对应的是加密；密码体制的破译是密码分析学的主要内容，其对应的是解密，解密是加密的逆过程。密码体制最基本的两种形式是对称密钥密码体制和非对称密钥密码体制。

2. 数字签名技术

在现实生活中，书信或文件是根据亲笔签名或印章来证明其真实性的，在网络世界中，我们也希望产生出能够代表签名者和文件之间关联性的数字代号。通过数字签名技术可以确认当事人的身份，起到了签名或盖章的作用，使签字方不能够抵赖。同时，通过数字签名技术也能够帮助我们鉴别信息自签发后到收到为止是否被篡改过，这就不会使得他人通过伪造而达到改变信息内容的目的。

3. 数字时间戳

在书面合同文件中，日期和签名均是十分重要的防止被伪造和篡改的关键性内容。

在电子交易中，时间和签名如同在书面合同文件中一样重要。数字时间戳技术是数字签名技术一种变种的应用，是由 DTS（Digital Time Stamp）服务机构提供的电子商务安全服务项目，专门用于证明信息的发送时间。

4. 验证技术

验证是在远程通信中获得信任的手段，是安全服务中最为基本的内容，因为必须通过可靠的验证来进行访问控制，决定谁有权接受或修改信息，以增强责任性及实现不可否认服务。验证常用的 3 种基本方式是口令方式、标记方式和人体生物学特征方式。分别简单介绍如下：

口令方式是用户身份验证最简单、最广泛的一种方法，操作十分简单，但最不安全。

标记是一种用户所持有的某个秘密信息（硬件），上面记录着用于系统识别的个人信息。

访问系统资源时，用户必须持有合法的随身携带的物理介质（如智能卡）用于身份识别、访问系统资源。

某些人体生物学特征，如指纹、声音、DNA 图案、视网膜扫描图案等信息，它们在不同人中完全相同的概率非常小，可以直接用于进行身份的验证。这种方法造价一般较其他方法高，适用于保密程度要求较高的场合。

5. 数字证书技术

由于在电子商务交易中，买卖双方在交易过程中是互不见面的，因此需要有一种事务来表明自己是一个合法的用户或合法的商家。

数字证书就是标志网络用户身份信息的一系列数据，用于证明某一主体（如个人用户、服务器等）的身份及其公钥合法性的一种权威性的电子文档。它由权威公正的第三方机构，即 CA 中心签发，类似于现实生活中的身份证。

6. 防火墙技术

常用的网络安全技术主要是防火墙技术。防火墙是软件、硬件的结合，在需要保护的网络同可能带来安全威胁的互联网或其他网络之间建立一层保护。防火墙是具有以下特征的计算机：

（1）由网内到网外或由网外到网内的所有访问都必须通过它。

（2）只有本地安全策略定义的合法访问才被允许通过它。

（3）本身具有较高的可靠性。

防火墙以内的网络称为可信网络，以外的网络叫不可信网络。例如，从互联网进入公司内部专用网络就需要经过一个防火墙，而在电子商务支付中也必须通过支付网关才可以进入银行的专用网络。

### 1.4.2　电子商务安全国际规范

电子商务安全机制经过近几年的发展，已经形成了一些国际规范，其中最具代表性的主要有 SSL（Secure Sockets Layer，安全套接层）协议和 SET（Secure Electronic Transaction，安全电子交易）协议。

1. SSL 协议

SSL 协议是通过在收发双方建立安全通道来提高应用程序间交换数据的安全性，从而实现浏览器和服务器（通常是 Web 服务器）之间的安全通信。SSL 协议是一种利用公共密钥技术的工业标准，广泛用于 Internet。目前大多数浏览器都支持 SSL 协议，很多 Web 服务器也支持 SSL 协议。

SSL 协议提供了信息保密、信息完整性、相互认证等基本功能。应用 SSL 协议实现交易过程要求客户将购买的信息首先发往商家，商家再将信息转发银行，银行验证客户信息的合法性后，通知客户和商家付款成功，商家再通知客户购买成功。

SSL 协议存在的缺点是：客户的银行资料信息先送到商家，让商家阅读，这样，客户银行资料的安全性就得不到保证。由于默认了商家是可以信赖的，商家可以对客户作出信息保密承诺，因此没有提供客户对商家的验证。SSL 协议提供了资料传递过程的安全通道，但 SSL 协议安全方面存在缺少数字签名功能、没有授权和存取控制、多方互相认证困难、不能抗抵赖和用户身份可能被冒充等弱点。

2. SET 协议

虽然 SSL 协议保证了商家和消费者之间传输数据和其他敏感信息的安全，基于 SSL 的银

行卡支付系统促进了电子商务的发展，但 SSL 协议不能验证消费者是否是结算卡的持有人，即并不能解决持卡人的身份认证和交易的不可抵赖性等问题。

SET 协议是万事达国际组织和 VISA 国际组织在微软公司、网景公司、IBM 公司、GTE 公司、SAIC 及其他公司的支持下联合设计的安全协议，设计 SET 协议的目的是为通过互联网在商家和处理银行之间传输信用卡结算信息时提供安全保证。SET 协议是信用卡在互联网进行支付的一种开放式标准，也是银行卡安全支付的具体规范。目前已经被广为认可而成了事实上的国际通用的网上支付标准，其交易形态将成为未来电子商务的规范。SET 协议的制定与推广为业务相互渗透的各家信用卡公司提供了统一的安全通信标准，也促进了信用卡互联网上作为支付工具的应用。

SET 协议提供了信息保密性、数据的完整性、交易者的身份认证和担保以及互操性（统一协议和信息格式带来不同厂家的软件之间的兼容性和互操作性）等功能。

不过，SET 协议目前局限于银行卡的网上支付。SET 协议只支持 B2C 模式的电子商务，而不支持目前最有前途和影响力的 B2B 电子商务交易。

SET 协议在美国一直遭到冷遇，尚未受到足够数量的商家和消费者的重视，几乎 80%的 SET 活动都发生在欧亚国家。至于 SET 协议未被普遍接受的原因，主要在于它的实施不如多数银行和商家想象得那样容易，成本也较高。据统计，在一个典型的 SET 协议交易过程中，须验证数字证书 9 次，验证数字签名 6 次，传递证书 7 次，进行 5 次数字签名，4 次对称加密和 4 次非对称加密，不可谓不安全，但整个交易过程可能要花费 1.5～2min（随着计算机硬件技术的快速发展，这个时间将大大缩短）。尽管如此，SET 协议的前景仍然是很光明的。

### 1.4.3 电子商务安全法律要素

安全的电子商务除了依赖于技术手段外，还必须依靠法律手段、经济行政手段来保障参与电子商务的各方的利益。

凯文·凯利（Kevin Kelly）在他的《新经济新规则》一书中说：“网络已经存在于每一种经济之中，不同以往的是，经由科技的促进与加强，网络已深深地穿透我们的生活，使得‘网络’这个概念已成为我们思维和经济的核心。”网络给人们带来便利的同时，也给不法分子提供了新的犯罪渠道。因此，与电子商务相关的法律问题也越来越多。同时，参与电子商务活动的各方之间都会发生法律关系，因此需要规定各方的法律义务和责任。

电子商务安全涉及到的法律要素主要有以下几个方面。

1. 保障交易各方身份认证的法律

电子交易的各方都需要拥有和证明自己的合法身份，通过设立在交易参与方之外的第三方的公证机构（CA 中心）可以达成这样的目标，即取得由数字证书认证中心签发的数字化的证书。在交易的各个环节，交易的各方都可以检验对方数字证书的有效性。

CA 中心是电子商务中的核心角色，它担负着保证电子商务公正、安全进行的任务。因而必须由国家法律来规定 CA 中心的设立程序、资格以及必须承担的法律义务和责任，同时要由法律规定对 CA 中心进行监管的部门、监管方法以及违规后的处罚措施。

2. 电子合同的法律地位

在电子商务活动中，电子合同的有效性、电子签章和数字签名的有效性是各国共同关注的法律问题，需要制定有关法律对电子合同的法律效力、数字签名、电子商务凭证的合法性得

以确认，同时也需要对电子商务凭证、电子支付数据的伪造、变更、涂销作出相应的法律规定。

3. 对电子商务中消费者权益保护的法律

对电子商务中消费者权益的保护，尤其对 B2C 交易中消费者权益的保护具有重要的地位。这种重要性不仅在于传统意义上的经营者和消费者之间因消费者处于劣势地位需要保护，更重要的是由于在线交易是在虚拟环境中完成的，因此更需要一套能够得到消费者信任的保障制度。在网络环境中，消费者的保护问题更主要地表现为要赢得消费者的信任。

消费者对商家信誉的信心只能寄托于 CA 中心和银行等机构。其中，CA 中心能够核实商家的合法身份，银行则能掌握商家的信誉情况。一旦因商家不付货、不按时付货或者货不符实而产生对消费者的损害时，可以由银行先行赔偿消费者，再由银行向商家追偿。如果商家屡次违规，银行可以取消商家的电子账号，并将违规情况通报给 CA 中心，由 CA 中心将其记入黑名单，情况严重时可以取消商家的数字证书，商家由此将失去开展电子商务的权利。

国际经合组织对消费者保护提出的主要框架指出：参与电子商务的消费者应该享有不低于在其他商业形式中享有的透明的和有效的保护的水平，这一要求相当于保护消费者的知情权；从事电子商务的企业应该对消费者的利益予以应有的关注，并应根据公平的商业广告及销售行为而行动；信息披露是确保交易透明和消费者知情权的重要措施；为了避免消费者购买意愿的模糊，消费者应该能够在决定购买前准确地确认其购买的商品或服务，确认并纠正任何错误或修改订单；消费者有权在缔结交易前取消交易；消费者应得到易用的、安全的支付体系并被告知该体系给予的安全水平的信息；对消费者提供良好、及时的争议解决方式也是确保消费者信任的重要措施。

消费者权益保护的另一个重要内容是保护个人隐私权。由于互联网上信息具有共享性和开放性的特点，必然要涉及侵犯家庭或者个人的隐私权问题。应立足最小限度收集个人数据、最大限度保护个人隐私的原则来制定法律，以尽量消除人们对泄露个人隐私以及重要个人信息的担忧，从而吸引更多的人上网进行电子商务。

4. 网络知识产权保护的法律

保护知识产权也是电子商务比较重要的问题之一。由于在互联网上知识产权的主要表现是信息，因此保护的难度相对比较大。

网络对知识产权的保护提出了新的挑战，在研究技术保护措施时，还必须建立适当的法律框架，以便侦测仿冒或欺诈行为，并在上述行为发生时提供有效的法律援助。

世界知识产权组织在 1996 年 12 月讨论形成的《世界知识产权组织版权保护条约》，对信息网络环境中的软件、数据库的著作权保护和信息数字化、网络传输、技术措施、版权信息等问题进行了系统的解释，但是还有很多遗留的问题没有解决，同时还存在涉及发达国家与发展中国家利益差异的问题。

当然，电子商务带来的法律问题不仅仅限于以上所述。目前，要全面解决电子商务引发的法律问题并非易事，在电子商务发展过程中将会发生的问题谁也无法完全预料，需要通过立法和完善现有法律加以规范，并使得立法工作具有前瞻性。另一方面，在制定电子商务法律时，要坚持灵活性和安全性的辩证统一。为了电子商务的安全性，必须要加快电子商务立法，但由于电子商务还处在快速发展中，在电子商务的很多方面（如数字身份认证）应该首选考虑行业的自律机制，以避免不灵活的或不协调的政府法规的“锁定”效应。

## 【阅读材料】

### 电子商务安全案例

电子商务从产生至今虽然时间不长，但发展十分迅速，已经引起各国政府和企业的广泛关注和参与。但是，由于电子商务交易平台的虚拟性和匿名性，其安全问题也变得越来越突出，近些年相关案例层出不穷。

1. 阿里巴巴淘宝购物网站遭黑客攻击

2016 年 2 月，据《华尔街日报》引述阿里巴巴集团表示，该公司近期遭到黑客攻击，这些黑客试图入侵约 2000 万个淘宝用户账户。阿里巴巴已提醒用户立即更改密码。

阿里巴巴通过阻止黑客的攻击尝试保护绝大多数淘宝账户，但没能成功拦截针对一小部分账户展开的攻击。阿里巴巴发言人指出嫌疑人已被逮捕，但拒绝透露可能被黑客侵入的账户数量，对于这些账户的数据是否失窃不予置评。

2. 韩国政府等多家网站多次爆发大规模的黑客攻击，瘫痪数小时

2013 年 3 月 22 日，包括韩国爆发历史上最大规模的黑客攻击，韩国主要银行、媒体以及个人计算机均受到影响。大量企业，包括国内主流的银行、电视台计算机都被破坏及瘫痪，导致无法提供服务，大量资料被窃取。

2013 年 6 月 25 日，包括韩国青瓦台总统府在内的 16 家网站遭攻击，并陷入瘫痪。一些被黑网站首页出现“伟大的金正恩领袖”等词句。2013 年 7 月 7 日晚间，韩国总统府、国防部、外交通商部等政府部门和主要银行、媒体网站等再次遭到分布式拒绝服务（DDoS）攻击，瘫痪时间长达 4 小时。

3. 熊猫烧香病毒

我国互联网上大规模爆发“熊猫烧香”病毒及其变种。一只憨态可掬，颔首敬香的“熊猫”在互联网上疯狂“作案”。在病毒普通的外表下，隐藏着巨大的传染潜力，短短三四个月，“烧香”潮波及上千万个人用户、网吧及企业局域网用户，造成直接和间接损失超过 1 亿元。2007 年 2 月 3 日，“熊猫烧香”病毒的制造者李俊落网。李俊向警方交代，他曾将“熊猫烧香”病毒出售给 120 余人，而被抓获的主要嫌疑人仅有 6 人，所以不断会有“熊猫烧香”病毒的新变种出现。李俊处于链条的上端，其在被抓捕前，不到一个月的时间至少获利 15 万元。而在链条下端的涉案人员张顺目前已获利数十万了。一名涉案人员说，该产业的利润率高于目前国内的房地产业。大量盗窃来的游戏装备、账号，并不能马上兑换成人民币，只有通过网上交易，这些虚拟货币才得以兑现。盗来的游戏装备、账号、QQ 账号甚至银行卡号资料被中间批发商全部放在网上游戏交易平台公开叫卖。一番讨价还价后，网友们通过网上银行将现金转账，就能获得那些盗来的网络货币。李俊以自己出售和由他人代卖的方式，每次要价 500 元至 1000 元不等，将该病毒销售给 120 余人，非法获利 10 万余元。经病毒购买者进一步传播，导致病毒的各种变种在网上大面积扩散。据估算，被“熊猫烧香”病毒控制的电脑数以百万计。