CHAPTER 1

第1章 信息安全概述

信息一直以来都是全人类的宝贵资源。各种功能的信息系统，已经成为推动社会发展前进的催化剂和加速器。同时，由于计算机网络（以下简称网络）的快速普及，处理信息的多样性也使得计算机成为了人类社会中一个不可或缺的工具，正日益为社会各个行业和部门的生产和管理提供有效的帮助，其提供的多种信息服务，给人类带来了便捷的生活方式。例如与我们关系密切的金融业的信息化进程，使资金流动加快，清算资料的速度大大提高，异地的资金划转也变得十分快捷了。可以说，信息化和计算机网络把人和人、国和国的距离缩短了。

信息与信息系统的安全现已成为一个新兴的学科，信息安全管理已经成为公共安全的重要组成部分。信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学等多种学科的边缘学科。随着全球信息化的发展，国家之间的“距离”越来越近，计算机网络在带来了众多快捷、便利的服务的同时也带来了新的危害。如何解决信息安全问题，如何制止计算机犯罪，如何建立安全的网络体系，已经成为全球关注的焦点。解决信息安全问题，已经是迫在眉睫的事情了。

网络的安全措施一般分为三大类：逻辑上的、物理上的和政策上的。面对安全的种种威胁，仅仅依靠物理上的和政策（法律）上的手段来有效防止计算机犯罪显得十分有限和困难，因此必须使用逻辑上的措施，即研究开发有效的网络安全技术，如安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等，以防止网络上传输的信息被非法窃取、篡改、伪造，保证其完整性和保密性；防止非法用户（程序）的侵入，限制网络上用户（程序）的访问权限，保证信息存放的私有性。除此之外，一个安全的计算机网络还必须考虑通信双方的身份真实性和信息的可用性。

网络安全就是要保证网络上存储和传输信息的安全性。由于网络设计之初，只考虑了方便性和开放性，这使得网络非常脆弱，容易受到黑客的攻击或有组织的入侵，也会由于系统内部人员的不规范操作和恶意行为，

使网络信息系统遭受破坏，导致信息泄露或丢失。为了解决这个问题，国内外的研究机构在这方面做了很多工作，在数据加密技术、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、IC 卡(存储、加密、智能卡)、拒绝服务、入侵侦测、网络安全性分析、信息内容安全监测和信息安全标准化等方面做了大量的研究和相关开发工作。

1.1 什么是信息安全

广义的信息安全是指防止信息财产被故意的或偶然的非授权泄露、更改、破坏，或防止信息被非法辨识、控制，即确保信息的保密性、可用性、完整性、可控性。信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别等七个方面。

狭义的信息安全指网络上的信息安全，也称为网络安全，它所涉及的领域也是相当广泛的。简单地说，网络中的安全是指一种能够识别和消除不安全因素的能力。

信息安全的定义随着应用环境的改变也有不同的诠释。对用户来说，个人隐私和机密数据的传输受到机密性、完整性和安全性的保护，避免他人窃取资料是他们的安全要求。而对安全保密部门来说，过滤非法的、有害的或涉及国家机密的信息，成为其信息安全的重点。在下面的相关内容中，我们将对信息安全的具体表现做进一步说明。

网络安全与其保护的信息对象有关，本质是在信息的安全期内保证其在网络上流动或静态存放时不被未授权用户非法访问，但允许授权用户访问。显然，网络安全、信息安全和系统安全的研究领域是相互交错和关联的。

1.2 网络安全和黑客

一直以来，黑客是具有传奇色彩的崇尚自由的一群人，然而黑客行为造成的损失却是巨大的。据 CERT(计算机紧急事件响应小组)的调查显示，约 20%的网站都遭受过安全侵害，每年在美国由安全导致的损失可达 100 亿美圆。根据有关调查，大部分的入侵和安全事件的威胁并非来源于外部，而是来源于网络内部的破坏。虽然网络安全已经被全球的人们所重视，各大公司、机构也都纷纷建立了自己的安全策略，设置并使用了防病毒、防火墙、入侵侦测系统(IDS)以及跟踪和记录网络活动的程序，但仍然不足以阻止攻击的产生。原因在于黑客的攻击比起前几年来越来越复杂，技术上越来越先进；超负荷的 IT 技术人员和由于侥幸心理所导致的资金投入的缺口，使得专业安全技术人员不能获得更多的资源；最重要的一点是大量的没有严密安全保护的系统正在全球快速地被部署并投入使用。

黑客的分类有很多种标准，一般以黑客的行为态度和动机来划分，有以下三类。

(1) 偶然的破坏者。顾名思义，这类人喜欢进入他人的系统，但不一定有明确目标，多数情况下是恶作剧。大部分黑客属于这一类。

(2) 坚定的破坏者。这类黑客的入侵都带有明确的目标，并会给系统带来巨大的甚至是毁灭性的破坏。

(3) 间谍。窃取商业资料或情报,获得信息或摧毁服务,对资源不加限制地访问。

1.3　计算机信息系统面临的安全威胁、攻击及其脆弱性

网络所提供的资源共享性、用户使用的方便性、分布处理提高效率的特性以及可扩充性,在一定程度上大大增加了网络受攻击的可能性。现今的计算机网络面临着各式各样的威胁和人为攻击,而计算机系统本身,无论是在存取与运行的基本原理上,或者是系统本身的设计、技术、结构、工艺等方面都存在着一些有待弥补的缺陷。或者可以这样说,计算机信息系统本身的脆弱性,使其成为被攻击的目标或被利用为有效的攻击手段。

1.3.1　计算机信息系统面临的安全威胁

网络的安全威胁来自众多方面,或者说,计算机信息系统本身的脆弱性,使其成为被攻击的目标。网络安全威胁可导致信息的保密性、完整性、可用性降低,从而造成经济损失。当前网络安全威胁主要有以下几个方面。

- 自然灾害、人为事故。由于自然灾害和人为的事故造成的威胁,如天灾、硬件故障、工作人员误操作等。
- 计算机犯罪。利用暴力或非暴力,故意破坏计算机中的机密信息,以及危害计算机实体和信息安全的不法行为,如数据欺骗、特洛伊木马等。
- 黑客行为。黑客的入侵或干扰,比如非法访问、拒绝服务等。
- 内部破坏。内部人员对计算机系统的破坏或泄密。
- 电子情报。通过信息窃取、流量分析、监听等手段获取信息资源。
- 信息战。为了军事目的,获取或干扰他国的信息和信息系统。
- 计算机病毒。制造、传播和利用计算机病毒进行破坏计算机信息系统的行为。如常见的蠕虫病毒(“求职信”、“红色代码”、Nimda、“震荡波”、“冲击波”等)。需要特别注意的是,现在的很多病毒都已经具备了部分黑客软件的特征。

1.3.2　计算机信息系统受到的攻击

对信息的人为故意的威胁称为攻击。攻击按威胁和攻击的对象可分为两类:一类是对计算机信息系统实体的威胁和攻击;另一类是对信息的威胁和攻击。计算机犯罪和计算机病毒则包括了对计算机系统实体和信息两个方面的威胁和攻击。

对计算机信息系统实体的威胁和攻击主要指对计算机及其外部设备和网络的威胁和攻击。对信息系统实体的威胁和攻击不仅会造成财产损失,还会使信息系统遭受破坏。

对信息的威胁和攻击主要有以下两种。

(1) 信息泄露,指偶然的或故意的获得(窃取或分析破译)目标系统的信息,特别是敏感信息。

(2) 信息破坏,指由于偶然事故或人为破坏,使信息的正确性、完整性和可用性受到破坏,使系统的信息被修改、删除、添加、伪造或非法复制,造成大量信息的破坏、修改或丢失。

就攻击方式来说,攻击可归纳为主动攻击和被动攻击两类。

(1) 主动攻击是指篡改信息的攻击。它不仅是窃密,而且还威胁到信息的完整性和可靠性。主动攻击是以各种方式,有选择地修改、删除、增加、伪造、复制信息内容,造成对信息的破坏。主动攻击的主要方法有:非法冒充、恶意篡改、抵赖等。

(2) 被动攻击是指一切窃密的攻击。它是在不干扰系统正常工作的情况下进行侦收、截获、窃取系统信息,以便破译分析;利用观察信息、控制信息的内容来获得目标系统的设置、身份;利用研究机密信息的长度和传递的频度获得信息的性质。被动攻击不容易被用户发现,因此它的攻击持续性和危害性都很大。被动攻击的主要方法有:截获信息、合法窃取、破译分析等。

1.3.3 计算机信息系统的脆弱性

计算机信息系统本身也存在着一些脆弱性,使得计算机信息系统对安全威胁和攻击的抵御能力降低,自身的一些缺陷常被未授权用户利用。这种非法的访问不仅使系统中存储的信息的完整性受到威胁,使信息被篡改或破坏而不能继续使用,更为严重的是,系统中有价值的信息被非法篡改、伪造、窃取或删除而不会留一点痕迹。另外,计算机还容易受到各种自然灾害和误操作的破坏。认识到计算机信息系统的这种脆弱性,才可以找出有效的措施来保证计算机信息系统的安全。

1. 信息处理环节中存在的不安全因素

首先从信息的处理环节来看,计算机信息系统的脆弱性,存在以下的不安全因素:输入数据易被篡改或伪造、系统软件易被破坏、存取控制功能比较弱等。

2. 计算机信息系统自身的脆弱性

从计算机信息系统的体系结构方面分析,也存在一些缺陷,这些缺陷在短时间内还无法彻底解决。包括:计算机操作系统的脆弱性,计算机网络系统的脆弱性(包括网络模型、协议上的缺陷),以及数据库管理系统的脆弱性。

这些脆弱性将在本书的后续相关内容中详细介绍。

1.4 网络安全的相对性

由于网络的互联互通,网络不可能达到100%的安全。在制定安全策略限制非法用户访问的同时,也必须保证合法用户对数据的访问权。一般的原则是给用户能足以完成其合法工作的最小权限。那么如何制定安全策略?制定安全策略的原则是什么?一个关键的安全原则应该是实用有效的,同时不会给合法用户在获取合法信息时增加负担的方案。寻找一个合适的安全原则的过程实际上是一个寻求动态平衡点的行为。使用过于复杂的安全技术会使合法用户的活动大大受限,从而使这些合法用户厌烦和规避设定的安全协议。而黑客则随时准备利用这样一个看上去无害的行为。因此拥有一个过分复杂的安全策略将导致安全有效性的降低。在制定安全策略的时候,总是要考虑安全策略给合法用户带来的影响。在多数情况下,如果用户所感受到的不方便大于所产生的安全性能

提高，则该策略实际上降低了网络的安全有效性。

需要指出的是，无论采取何种防范措施都不可能保证通信系统的绝对安全。安全是相对的，不安全才是绝对的。在具体实施过程中，经济因素和时间因素是判断安全性的重要指标。换句话说，过时的“成功”攻击和“赔本”的攻击都被认为是无效的。

1.5　网络安全的领域和关键技术

随着信息社会的网络化，越来越多的部门和机构都依赖于计算机网络，网络安全的地位日趋重要。一门以研究网络安全为基础的学科——信息安全学也开始逐步形成。信息安全学的研究内容主要包括以下几个方面：

- 网络安全体系结构；
- 网络的攻击手段与防范措施；
- 网络安全设计；
- 网络安全标准的制定和安全评测及认证；
- 网络安全设备；
- 安全管理及安全审计；
- 网络犯罪侦查；
- 网络安全理论与政策；
- 网络安全教育；
- 网络安全法律法规。

明确了网络安全的概念后，下面来讨论网络安全的主要组成部分和关键性技术。网络安全的结构层次包括：物理安全、安全控制和安全服务。

1.5.1　物理安全

网络安全首先要保障网络上设备的物理安全。物理安全指物理层次上的安全保护。目前主要的物理不安全因素有四大类。

(1) 自然灾害(如雷电、地震、火灾、水灾等)、物理损坏(如硬盘物理损坏、设备意外损坏等)、设备故障(如意外断电、电磁干扰等)和意外事故。这类风险的特点是：突发性、自然因素性和非针对性。这种安全威胁只破坏信息的完整性和可用性(对信息的保密性无损害)。对该类威胁的防范一般是实施防护措施，建立数据备份和安全制度。

(2) 电磁泄漏(如侦听计算机操作过程)产生信息泄漏、干扰他人、受他人干扰、乘机而入和痕迹泄露等。其特点是难以觉察性、人为实施的故意性、信息的无意泄露性。这种威胁只破坏信息的保密性(无损信息的完整性和可用性)。解决方法一般是辐射防护(电磁屏蔽或电磁干扰)、加密和隐藏销毁。

(3) 操作失误(如删除文件、格式化硬盘等)或意外疏漏(如系统崩溃等)。其特点是人为实施的无意性和非针对性。这种安全威胁只破坏信息的完整性和可用性(无损信息的保密性)，通常用状态检测、报警确认和应急恢复等方法处理。

(4) 计算机系统机房的环境安全。其特点是可控性强、损失大、可管理性强。解决方

法是加强机房管理、运行管理、安全组织和人员管理。

物理安全是信息安全的最基本保障，是不可缺少的组成部分。一方面，研制生产计算机和通信设备的厂商应该在各种软件和硬件系统上充分考虑到系统所承受的安全威胁和相应的防护措施，提高系统的可靠性。另一方面，也应该通过安全意识的提高、安全制度的完善、安全操作的提倡等方式使用户和管理维护人员在系统和物理层次上实现信息的保护。

1.5.2 安全控制

安全控制是指通过计算机操作系统和网络通信设备对存储和传输的信息的操作和进程进行控制和管理，主要是在信息处理层次上对信息进行安全保护。安全控制可分为以下三个层次。

(1) 计算机操作系统的安全控制。如，用户开机必须输入密码或者指纹等生物特征，以此控制对文件的读写和存取，主要是保护存储在硬盘上的信息和数据。

(2) 网络接口模块的安全控制。在网络环境中对来自其他机器的网络通信进程进行安全控制，包括身份认证、客户权限设置和识别、审计日志等。

(3) 网络互联设备的安全控制。对整个子网内的所有主机的传输信息和运行状态进行安全控制。主要是通过网管软件或路由配置来实现。

安全控制目前主要通过现有的操作系统和网络管理软件来实现。因此，安全控制只提供初步的安全功能和信息保护，它仍然存在很多的问题，但由于实际情况的限制，很难对此进行弥补和更改。为此，很多科研机构和企业正在研制专门的信息系统安全综合管理软件来实现安全控制。

1.5.3 安全服务

安全服务是指在应用层对信息的保密性、完整性和来源真实性进行保护和鉴别，满足用户的安全需求，防止和抵御各种安全威胁和攻击手段。这是对操作系统和通信网络安全漏洞和问题的有效弥补和完善。

安全服务主要包括安全机制、安全连接、安全协议和安全策略等几部分。

1. 安全机制

安全机制是利用密码算法对重要而敏感的信息进行处理。包括加密/解密(保护信息的保密性)、数字签名/签名验证(确认信息来源的真实性和合法性)、信息认证(保护信息的完整性，防止和检测数据的篡改、插入、删除等)。安全机制是安全服务的核心和关键。现代密码学的理论和技术在安全机制的设计中起到了重要的作用。

2. 安全连接

安全连接是在安全处理前与网络通信方之间的连接过程，是安全处理所必需的准备工作，包括会话密钥的分派、生成和身份验证(保护进行信息处理和操作的对等双方身份的真实性和合法性)。

3. 安全协议

协议是多个使用方为完成某个任务所采取的一系列共同遵守的有序步骤。协议的特性是预先建立、相互同意、无二义性和完整性。安全协议使网络环境下不信任的通信双方能够相互配合，并通过安全连接和安全机制的实现保证通信过程的安全性、可靠性和公平性。

4. 安全策略

安全策略是安全机制、安全连接和安全协议的有机组合方式，是系统安全性的完整解决方案。安全策略决定了信息安全系统的整体安全性和实用性。不同的通信系统和具体的应用环境决定不同的安全策略。

另外，安全设备是存储密钥、密码、权限、审计记录等安全信息的硬件介质和载体，以及存储和运行安全信息系统的设备。如具有防火墙功能的路由器、具有密钥分配和认证功能的安全服务器、保存私钥的智能卡、具有信息过滤功能的内容安全网关等。安全设备自身的安全防护也是不可缺少的和非常重要的。

1.5.4　网络安全的关键性技术

从广泛意义来说，计算机网络安全技术主要有：

- 主机安全技术；
- 身份认证技术；
- 访问控制技术；
- 密码技术；
- 内容安全技术；
- 防火墙技术；
- 安全审计技术；
- 安全管理技术。

为了实现网络安全，应对其进行深入研究，以适应我国信息化对网络安全的需要，开发出具有我国自主知识产权的安全产品是非常必要的。

1.5.5　实现网络安全的策略

要实现网络安全，不但要靠先进的技术，而且要有严格的安全管理、法律约束和安全教育。

- 先进的网络安全技术是网络安全的根本保证。用户对面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术，形成一个全方位的安全系统。
- 严格的安全管理。使用计算机网络的各个机构、企业和单位应建立相应的安全管理办法，加强内部管理，建立合适的网络安全管理系统，完善安全审计和跟踪体系，提高对整体网络的安全意识。

- 制定严格的法律和法规。计算机网络是一个不断发展中的新事物，它的很多行为无法可依、无章可循，导致网络上计算机罪犯有机可乘。面对日趋严重的计算机犯罪，必须建立、健全与网络安全相关的法律和法规，使非法行为被法律所威慑，不敢轻举妄动。

1.6 信息安全的法律法规

法律与其所规范的社会行为是处于不断运动中的一对矛盾，法律随着它所规范的社会现象的变化而变化。新的社会现象的出现，往往会促使立法者修改原有的法律或者进行新的立法，以适应新的需要。计算机信息网络的产生和广泛应用再一次以事实证明了这点。

进入 20 世纪 90 年代，数字技术与网络发展相辅相成，使网络的运用到了一日千里的境界。人们惊讶于互联网发展速度的同时，也对科技迈向不可知的未来感到迷茫。通过 Internet，获取信息、通信交流与娱乐消费等人类生活的几大重要部分均可得到满足。今后，随着网络的逐渐普及，人们对它的依赖会日渐加深。

然而，在享受网络带来的便利的同时，必须正视网络给传统法律提出的挑战。现在，适用于网络时代之前的原有法律体系、法律原则、法律概念中的许多内容都难以继续适用于网络社会。网络侵权、网上取证、隐私权保护、网上征税、网上色情信息泛滥、黑客攻击、计算机病毒肆虐……，所有这些伴随网络而出现的新问题都在一定程度上使原有法律显得苍白无力。如网络传输中的暂时复制是否属于版权法中的复制、网络传输是否属于版权法中的发行、电子数据证据是否与视听资料具有同等的法律效力、如何保护网上的个人资料不被非法泄漏、网上交易是否应当征税以及如何征税等，这些问题都向法律工作者提出了新的课题。

面对网络时代向传统法律提出的诸多挑战，各国都相继进行网络立法，加紧现有法律的立、改、废，以适应计算机信息网络的快速发展与广泛应用。由于信息安全的重要地位，有关信息安全的法律法规是各方面关注的重点。

1.6.1 国外信息安全立法现状

国外很早就开始了信息安全的立法活动，这些法案涉及信息安全的方方面面，并随着时间的发展一直处在修改和新的制定之中。美国作为世界强国，不仅信息技术具有国际领先水平，而且信息安全法律体系也已比较完备。美国早在 1987 年起便根据信息技术发展的状况再次修改了计算机犯罪法，此外，逐步制定了计算机安全法、电子通信隐私法、个人隐私法、反情报法案、工业间谍法案、电子数据安全法等多部法律，用多如牛毛来形容其信息安全法律之多也不为过，以至于在 2001 年 7 月，美国议会中一子委员会特别发表声明，呼吁国会暂缓通过新的信息安全法律法规，以防止可能出现的副作用。

其他很多国家也制定了比较成熟的信息安全法律，表 1-1 反映了部分国家对数据保护的立法情况。

表 1-1　部分国家数据保护立法情况

国　家	立　法	制定日期	生效日期	CE 标准	注册/公告	人工记录	法　人	数据出口许可证
澳大利亚	数据保护法	1980-01-01	1982-10-18	是	所有	有	有	部分
比利时	关于个人数据处理的隐私保护法	1992-12-08	1993-04-01	是	部分	有	无	部分
丹麦	私人注册法	1979-01-01	1982-06-08	是	部分	有	有	部分
芬兰	数据保护法	1987-02-04	1988-01-01	是	所有	有	无	部分
法国	数据处理、数据文件和私人自由法	1980-01-01	1982-01-06	是	所有	有	有	部分
德国	数据保护法	1977-01-27	1979-01-01	是	部分	有	有	无
冰岛	个人数据记录草案	1981-06-05	1982-01-01	是	所有	有	有	无
爱尔兰	数据保护法	1988-07-13	1989-04-19	是	部分	无	无	无
卢森堡	计算机处理中连接数据名称的使用法	1979-03-31	1979-10-01	是	所有	无	有	无
荷兰	数据保护法	1988-07-13	1990-07-01	是	部分	有	无	无
挪威	个人数据注册法	1980-01-01	1982-06-09	是	部分	有	无	无
葡萄牙	个人数据保护法	1991-04-29	1991-05-04	是	所有	无	无	所有
西班牙	个人数据自动处理规则法	1992-10-29	1993-02-01	是	所有	所有	无	部分
瑞典	数据法	1973-05-13	1974-07-01	是	所有	无	无	部分
瑞士	数据保护法	1992-06-19	1993-07-01	否	部分	有	有	无
英国	数据保护法	1984-07-12	1987-11-01	是	所有	无	无	无

1.6.2　国内信息安全立法现状

我国非常重视国家信息化建设，针对信息化过程中出现的安全问题，中央领导多次指示加速信息安全法律法规的制定。目前我国的信息法制建设已经有了良好的开端，但信息安全的立法仍处于起步阶段，还没有形成一个具备完整性、适用性、针对性的法律体系。这个法律体系的形成，一方面要依赖我国信息化进程的深化，另一方面要依赖对信息化和信息安全的深刻认识和技术、法学意义上的超前研究。

在我国已有的法律法规中，从以下几个层次对信息安全问题做出了规范。

第一个层次虽然没有直接描述信息安全，但从国家宪法和部分法律的高度对公民、法人和其他组织在有关信息活动中涉及国家安全的权利义务进行了规范。例如宪法、国家安全法、国家保密法等。

第二个层次是直接约束计算机安全、Internet 安全的法规。如《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中华人民共和国计算机信息网络国际互联网络安全保护管理办法》等。

第三个层次是对信息内容、信息安全技术以及信息安全产品的授权审批的规定。如《电子出版物管理暂行规定》、《中国互联网络域名注册暂行管理办法》、《计算机信息系统安全专用产品检测和销售许可证管理办法》、《商用密码管理条例》等。

第四个层次是对计算机违法犯罪的惩罚处理。我国刑法修订时补充了有关计算机犯罪的相关处罚条款，使我们初步有了处罚计算机犯罪的法律依据。但还有很多领域缺乏对信息犯罪进行定罪处罚的法律依据，有待继续完善。这其中，制定打击互联网络犯罪的法律是当务之急。

1.6.3 电子商务法及数字签名法

电子商务是20世纪90年代初期兴起的一种崭新的企业经营方式，简而言之，是指在商业行为的整个过程中实现交易电子化、直接化。电子商务有狭义和广义之分，狭义的电子商务也称为电子交易(E-transaction)，是指利用互联网提供的通信手段在网上进行商业贸易活动。广义的电子商务也称为电子商业(E-business)，是包括电子交易在内的、利用电子网络环境进行的各种各样的商务活动，如市场分析、客户管理、资源调配、企业决策等。电子商务的重要角色由客户和商家担当，他们的联系枢纽由网上交易中介完成，认证中心(CA)负责交易的安全认证及监管，银行、金融机构负责资金流通。

这种虚拟环境中的商务交易活动难以得到传统法律体系的支持，突出体现在合同效力的确定、诉讼管辖、证据认定等保障实体法实施的理论和方法无法处理电子商务案件，关于媒体的管理构架的法律不能适应以网络为载体的全新的信息交流方式。电子商务法的目的是为了解决数据通信在商务交易中的运用，特别是在Internet平台上的应用，而给商务法律关系带来的一些新问题。

电子商务法的范畴非常广泛，是一部综合性的法律，它涉及大量具体问题：电子数据的法律地位、数字签名的效力、认证制度、电子付款、税收、知识产权、消费者权益保护等。

电子商务环境以及相关技术发展迅速，因此电子商务法始终面临着巨大的现实挑战。为此，电子商务法必须遵循开放性的原则，并保持与国际上普遍承认并流行的相关法律法规(比如联合国贸易法委员会《电子商务示范法》)的协调与一致(这是由电子商务的国际化决定的)。同时，电子商务的立法还有涉及面广、技术性强(比如加密、认证等技术)的特点，这也是制定法律时需要注意的。

1. 国际上电子商务立法状况

从发达国家目前的动向来看，它们基本上是从一个战略发展的角度来确立电子商务立法规则的。例如美国，它着眼于21世纪经济的持续增长，为此发展电子商务更成为美国政府当前的主要任务。另一方面，发达国家纷纷制定相关法律法规、起草电子商务基本框架、签署双边协定、发表白皮书等，其目的都是为了争取制定电子商务国际规则的立法权。下面介绍的就是目前国际上的主要立法情况。

联合国国际贸易委员会：1996年通过了一个法律示范文本——《电子商务示范法》；1998年9月WTO总务理事会通过了一个极具影响力的《电子商务工作方案》；1999年9月，通过了一项《数字签名统一规则草案》，就电子合同实施中的数字签名问题做了初步规定。

美国：1997年7月，美国政府发表了《全球电子商务框架》的白皮书，从而迈开了电子商务法制建设的步伐；1998年7月美国参众两院分别通过了《互联网免税法案》，规定三