第 1 章　计算机信息安全概述

随着现代通信技术的迅速发展和普及，特别是随着互联网进入千家万户，计算机信息的应用与共享日益广泛和深入。各种信息系统已成为国家基础设施，支撑着金融、通信、交通和社会保障等方方面面，计算机信息成为人类社会必需的资源。与此同时，计算机信息的安全问题也日益突出，情况越来越复杂。从大的方面来说，计算机信息安全问题已经威胁到国家的政治、经济、军事、文化、意识形态等领域；从小的方面来说，计算机信息安全问题也涉及人们能否保护个人隐私和私有财产安全等。因此，加强计算机信息安全研究、营造计算机信息安全氛围，既是时代发展的客观要求，也是保证国家安全和个人财产安全的必要途径。

1.1　信息的定义和特征

在人类社会的早期，人们对信息的认识比较肤浅而且模糊，对信息没有明确的定义。到了 20 世纪特别是中期以后，科学技术的发展，特别是计算机信息科学技术的发展，对人类社会产生了深刻的影响，迫使人们开始探讨信息的准确含义。

有关信息的定义有许多种，它们都从不同的侧面、不同的层次揭示了信息的特征与性质，但同时也都有各自的局限性。1988 年，我国信息论专家钟义信教授在《信息科学原理》一书中把信息定义为“事物运动的状态和状态变化的方式”，并通过引入约束条件推导了信息的概念体系，对信息进行了完整和准确的描述。这个定义具有普遍性，涵盖了其他的对信息的定义。

下面列举一些与信息关系密切但又很容易混淆的概念，介绍它们与信息的区别。

(1)消息。信息不同于消息，消息是信息的外壳，信息则是消息的内核。也可以说，消息是信息的笼统概念，信息则是消息的精确概念。

(2)数据。信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。当然，在计算机中，所有的多媒体文件都是用数据表示的，计算机和网络上信息的传递也是以数据的形式进行的，此时的信息等同于数据。

(3)信号。信息不同于信号，信号是信息的载体，信息则是信号所承载的内容。

(4)情报。信息不同于情报，情报通常是指秘密的、专门的、新颖的一类信息。可以说所有的情报都是信息，但不能说所有的信息都是情报。

(5)知识。信息不同于知识，知识是由信息抽象出来的产物，是一种具有普遍性和概括性的信息，是信息的一个特殊子集。知识就是信息，但并非所有的信息都是知识。

信息是主观世界联系客观世界的桥梁。在客观世界中，不同的事物具有不同的特征，这些特征给人们带来不同的信息，而正是这些信息使人们能够认识客观事物。同样，信息也具有许多独特的性质与功能，而且它是可以测度的。

信息的主要性质和特征如下：

(1)普遍性和可识别性。信息来源于物质和物质的运动。只要存在着物质,只要有变化着的事物或运动着的客体,就会存在信息。信息不仅普遍存在,而且也可以被识别。人们通过感官或多种探测手段都可以直接或间接地识别出客观事物的特征及其变化所产生的信息,特别是找出其中的差异,这是认识信息的关键。

(2)存储性和可处理性。信息来源于物质和意识,但又可以脱离物质和意识而独立存在,并可以存储起来。信息存储就是通过信息载体将信息保存起来,以备后用,这是信息不同于物质和意识的重要特征。不仅可以对信息进行存储,还可以对其进行处理,即对获得的大量纷繁的信息,根据目的进行筛选、分析、整理、控制和使用。处理是为了更好地开发和利用信息,同时也有利于信息的传递和存储。

(3)时效性和可共享性。信息具有较强的时效性。一个信息生成或获取得越早,传递得越快,其价值就越大。随着时间的推延,其价值就会逐渐衰减以至消失。信息的共享性就是指信息可以为多个主体所利用。

(4)增值性和可开发性。信息资源的增值性主要表现在两个方面:一是对具体形式的物质资源和能量资源进行最佳配置,以使有限的资源发挥最大的作用;二是可以利用急剧增长的信息来发掘新的材料和能源。而信息本身在不断的使用中也可以得到增值。同时,信息还具有可开发性,人们需要不断地进行探索和挖掘,才能充分开发和利用信息资源。

(5)可控性和多效用性。信息的可控性反映在 3 个方面,即可扩充、可压缩和可处理。信息的可控性使信息技术具有可操作性,同时也增加了信息技术利用的复杂性;而信息的多效用性则是由信息所具有的知识性决定的。信息的多效用性是指,无论是认识世界还是改造世界,信息都是基础,信息是知识的源泉、决策的依据和管理的保证。

此外,信息还具有可转换性、可传递性、独立性和可继承性等特征。

1.2 计算机信息安全的威胁

知己知彼,方能百战不殆。要保证信息的安全,就必须先了解自己,即熟悉要保护的信息以及存储、传输和处理它的系统,而后要了解所面对的威胁。例如,管理人员必须清楚单位部门、员工、应用程序、数据和信息系统所面临的各种威胁,以便对信息安全做出正确的决策。

影响计算机信息安全的因素很多,一般可分为自然威胁和人为威胁两种。

1.2.1 自然威胁

自然威胁主要有以下几种。

1.自然灾害

自然灾害如火灾、水灾、地震、闪电、火山喷发等,会破坏计算机信息的存储、传输和使用,甚至会对计算机造成毁灭性的损害。

2.恶劣的工作环境

计算机是一种复杂精密的电子设备,对环境的要求很高。如果它所处的环境比较恶劣,则很容易发生故障。轻则造成工作不正常或缩短使用寿命,重则造成重大损坏。对计算机

影响较大的环境因素有以下几方面：

(1)温度。计算机工作环境的温度不能太高或太低。据统计，当计算机器件周围的温度超过60 ℃时，计算机器件就可能会发生故障，随后温度每升高 10 ℃，计算机的可靠性就会下降25%。计算机机房的温度要求一般定为(21±2) ℃，温度变化比不超过 3 ℃/h。从人体的舒适度考虑，冬季机房温度为 16～23.5 ℃，夏季机房温度为 18～26 ℃最为适宜。从节能和舒适度出发，一般夏季取允许的上限温度值，冬季取允许的下限温度值为控制计算机机房的温度值。

(2)湿度。开机时，计算机机房的湿度一般控制为 45%～65%，相对湿度波动控制在每小时±6%。实践证明，机房的空气调节系统应具有加湿装置和去湿装置，并要求安装有湿度、温度提示及自动调节装置。当相对湿度在 30%以下时，计算机的故障发生率会急剧上升至正常情况的 10～30 倍。

(3)振动。计算机不能在经常振动的环境中工作，计算机磁盘驱动器中的磁头和磁盘在工作中的接触是非常精密的，微小的振动就有可能损坏磁头和磁盘。

(4)粉尘。粉尘对计算机的影响也非常大，粉尘的积聚也会给计算机造成漏电，静电感应，磁头、磁盘磨损等故障。一般要求机房内空气含尘量为 0.75～1 mg/m^3，尘粒粒径不大于 3 μm。

3.物理损坏

物理损坏是指计算机的物理结构的损坏，如意外的外力造成的破损等。

4.设备故障

设备故障包括设备硬件的偶然失常、设备使用寿命到期导致的永久性故障和电源故障等。

以上这些自然威胁的共同特点是具有突发性、自然性和非针对性。这类不安全因素不仅对计算机信息安全造成威胁，而且严重威胁着整个计算机系统的安全，因为物理上的破坏很容易毁灭整个计算机信息管理系统以及网络系统。消除这类安全隐患的有效方法是采取各种预防措施、制定安全规章、进行数据备份以及有针对性地选择应用新技术等。

1.2.2　人为威胁

人为威胁又分为无意威胁和有意威胁两种。

1.无意威胁

无意威胁主要是由操作人员的操作失误和能力缺陷造成的。

(1)操作失误。人比机器更容易出错，操作人员的不小心或对操作的错误理解等都有可能产生误操作(如操作不当、未经许可使用、误用存储媒体、误删除、误格式化等)。一旦发生复原不了的误操作，就有可能产生不良后果。

(2)能力缺陷。如编程经验不足、检查漏项、水平有限、维护不力等。能力缺陷造成的威胁通常来自没有明显的恶意企图与目的的偶然事故。

2.有意威胁

有意威胁是指通过攻击系统暴露的要害或弱点，使计算机信息的完整性、保密性和可用性受到损害，造成不可估量的重大经济或政治上的损失。有意威胁来自于有目的的恶意攻

击，这种攻击可以分为主动攻击和被动攻击。主动攻击是指以各种方式（如修改、删除、伪造、添加、重放、乱序、冒充、制造病毒等）有选择地破坏数据；被动攻击是指在不干扰计算机系统正常工作的情况下进行侦收、截获、窃取、破译、业务流量分析和电磁泄漏等。

对计算机的主动攻击具有明显的目的性和主动性，是计算机信息安全面临的最主要、最危险的威胁。有意威胁来自内部威胁和外部威胁两个方面。据不完全统计，有 80％的计算机犯罪和系统安全遭破坏都与内部人员密切相关。

恶意攻击有明显的企图，其危害性相当大，给信息安全、系统安全带来了巨大的威胁。恶意攻击具有下列特征：

（1）智能性。从事恶意攻击的人员（如黑客）大都具有相当高的专业技术水平和熟练的操作技能，他们在攻击前一般都经过周密预谋和精心策划，通过 Internet 非法接入后，篡改或伪造他人账户、存折和信用卡，实施贪污、盗窃、诈骗、破坏等行为，甚至非法侵入国家党政机关、企事业单位，窃取政治、经济和军事机密等。

（2）隐蔽性。恶意攻击的隐蔽性很强，不易引起怀疑。一般情况下，恶意攻击的证据存在于软件的数据和信息资料之中，若无专业知识很难获取。同时，实施恶意攻击的行为人却很容易毁灭这些证据。

（3）多样性。实施攻击的手段千变万化，如监听、流量分析、破坏完整性、重发、假冒、拒绝服务、资源的非授权使用、干扰、制造病毒等。

（4）严重性。一些关键行业的计算机遭到恶意攻击有可能造成非常严重的后果。例如，对金融、证券业的计算机和网络的恶意攻击，往往会使金融机构和相关企业蒙受重大损失，也会给社会稳定带来不利影响；对军事、国防等计算机信息系统的恶意攻击更有可能危害到人民生命财产安全和国家安全。

恶意攻击得逞的原因是计算机系统本身有安全缺陷或漏洞，如通信链路的缺陷、电磁辐射的缺陷、引进技术的缺陷、软件漏洞、网络服务的漏洞等。其中，有些安全缺陷可以通过努力加以避免，有些缺陷则是各方面折中所必须付出的代价。

1.3 信息安全概述

1.3.1 信息安全的定义和特性

信息安全是一个广泛而抽象的概念。所谓信息安全，就是关注信息本身的安全，而不管是否应用了计算机作为信息处理的手段。信息安全的任务是保护信息财产，以防止信息被恶意泄漏、修改或破坏从而导致信息的不可靠或无法处理等情况的发生。

不管信息入侵者采用什么样的手段，他们都要通过攻击信息的几种安全特性来达到目的。信息安全的含义在技术层次上就是要保证在客观上杜绝针对信息安全特性的威胁，使得信息的所有者在主观上对信息的本源放心。

信息安全的特性表现在以下几个方面：

（1）完整性。完整性是指信息在存储或传输的过程中保持未经授权不能改变的特性，即对抗主动攻击，保证数据的一致性，防止数据被非法用户修改和破坏。

（2）可用性。可用性是指信息可被授权者访问并按需求使用的特性，即保证合法用户对

信息和资源的使用不会被不合理地拒绝。对可用性的攻击就是阻碍信息的合理使用。例如，破坏网络和相关系统的正常运行就属于这种类型的攻击。

(3)保密性。保密性是指信息不被泄漏给未经授权者的特性，即对抗被动攻击，以保证机密信息不会泄漏给非法用户。

(4)可控性。可控性是指对信息的传播及内容具有控制能力的特性。授权机构可以随时控制信息的机密性，能够对信息实施安全监控。

(5)不可否认性。不可否认性也称为不可抵赖性，即所有参与者都不可能否认或抵赖曾经完成的操作。发送方不能否认已发送的信息，接收方也不能否认已收到的信息。

信息安全的任务就是要实现信息的上述几种安全特性，而对于攻击者来说，却是要通过一切可能的方法和手段破坏信息的安全特性。

1.3.2　信息安全的分类

信息安全通常分为监察安全、管理安全、技术安全、立法安全和认知安全等几大类，针对各个分类所采取的措施见表 1-1。

表 1-1　信息安全措施

分　类		措　施
主分类	子分类	
监察安全	监控查验	发现违规、确定入侵、定位损害、监控威胁
	犯罪起诉	起诉、量刑
管理安全	技术管理安全	通过多级安全用户鉴别技术进行管理
		通过多级安全加密技术进行管理
		通过密钥管理技术进行管理
	行政管理安全	人员管理、系统管理
	应急管理安全	制定应急措施、进行入侵自卫与反击
技术安全	实体安全	环境安全(温度、湿度等)、建筑安全(防雷、防水等)、网络与设备安全
	软件安全	软件的安全开发与安装、软件的安全复制与升级、软件加密、软件安全性能测试
	数据安全	数据加密、数据存储安全、数据备份
	运行安全	访问控制、审计跟踪、入侵报警与系统恢复等
立法安全		制定有关信息安全的政策、法令、法规
认知安全		开办培训班、奖惩与扬抑、信息安全宣传与普及教育

1.4 计算机信息安全的对策

对于一个组织机构来说，要全面地应对计算机信息安全问题，建立一个立体的计算机信息安全保障体系，一般要从技术、管理、人员 3 个层面来进行。

1.4.1 技术保障

技术保障是指运用一系列技术层面的措施来保障信息系统的安全运营，检测、预防、应对信息安全问题。在很大程度上，技术保障要借助一些信息安全设备来实现。

1. 防火墙和 IDS

在网络边界部署防火墙和入侵检测系统(intrusion detection system，IDS)。防火墙和入侵检测系统置于组织机构的可信内网和不可信外网之间，通过在网络层对非法数据进行检测和阻断来保护组织内部网络环境。其中，防火墙通过设定规则来抵御静态攻击，入侵检测系统通过监控、分析网络流量来发现已知的攻击模式和异常行为。

2. 防病毒软件

在主机安装防计算机病毒软件。很多公司通过在主机安装防病毒软件来扫描磁盘文件、过滤 E-mail 附件，以此发现和抑制已知或潜在的计算机病毒。

3. 审计系统

引入审计系统，及时审计网络活动。网络安全审计系统以串联或旁路的方式接入网络中，它负责截取网络中的会话数据，并进行解析、重组、记录，审计人员通过回放会话过程能及时发现网络中的未授权活动。

4. 访问控制

加强访问控制。访问控制是指对组织机构的信息资源只有具有相关权限的人才能访问。与之相关的技术或设备有：路由器访问控制表(access control list，ACL)、专有访问控制系统等。

5. 加密、认证技术

对信息的存储、传输引入加密、认证技术。加密技术能够加强信息的机密性，认证技术如证书能鉴别参与者和信息的真伪。加密、认证的相关技术有虚拟专用网(virtual private network，VPN)、数字证书、IPSec 等。

6. 安全性管理

加强信息存储的安全性管理，可以采用物理隔离手段防止未授权的物理入侵和破坏，同时，采用备份机制使数据在物理设备遭受不可抗拒性损坏的情况下能够及时得到最大程度的恢复。

1.4.2 管理保障

在计算机信息安全领域，有一句话经常被人提起，那就是“三分技术，七分管理”。从一定程度上讲，信息安全是建立在合理的政策和流程基础之上的。这些措施包括以下几点。

1. 实施标准的 IT 治理方案

大约有 78%的系统停运是由于内部相关权限人员的行为造成的。这些行为又可细分为非标准配置、未归档的变更、不适当的补丁等。为了避免这些情况，企业应该采取一种自底向上的方法来达到安全管理的目的，其中首选的是实施标准的 IT 治理方案。

2. 建立安全的基线配置

在任何设备成为 IT 基础设施的一部分之前，应当对其强制实行一个标准的安全配置。例如，对于一个 Windows 服务器来说，它在运行维护业务之前应该保证所有不必要的 TCP 服务都已禁用，限制其文件共享，删除其 Guest 账户。

3. 建立一个标准的事件响应流程

事实表明，再安全的系统也有可能遭受攻击。因此，企业需要建立一个标准的事件响应流程来应对突发状况。

1.4.3　人员保障

正如人是最大的安全威胁，IT 人员和信息安全人员构成了计算机信息安全的最后一道防线。如果这两者配备不到位或者两者不能很好地协同工作，整个组织将遭受更大的安全威胁。为了避免这种情况，组织机构应该采取以下措施：

(1)组建专门的计算机信息安全运行维护队伍。应该由专门的信息安全队伍对组织机构的信息安全相关设备进行运行和维护。

(2)建立专门的应急响应小组，负责在出现信息安全事件后的应急处理工作。

(3)对员工进行安全意识培训。通过安全意识培训，提高员工的安全意识，增加对信息安全事件防范和应对的经验积累。

(4)建立与信息安全相关的奖惩机制，使信息安全工作的好坏在员工的物质或精神收益上有所体现。

1.5　OSI 参考模型的信息安全体系结构

研究计算机信息系统安全体系结构的目的，就是将普遍性的安全体系原理与计算机信息系统的实际相结合，形成满足计算机信息系统安全需求的安全体系结构。应用计算机信息安全体系结构，可以从管理和技术上保证安全策略得以完整、准确地实现，安全需求全面、准确地得以满足。它包括确定必需的安全服务、安全机制和技术管理以及它们在系统上的合理部署和关系配置。

1989 年 12 月，国际标准化组织 ISO 颁布了 ISO 7498-2 标准，该标准首次确定了 OSI 参考模型的计算机信息安全体系结构。它是目前国际上普遍遵循的计算机信息系统互连标准，我国将其作为 GB/T 9387.2 标准并予以执行。ISO 7498-2 标准规定了 5 类安全服务以及提供这些服务所需要的 8 类安全机制。

1.5.1　安全服务

安全服务是指由参与通信的 OSI 参考模型的某一层所提供的服务，它确保了该系统或

数据传输具有足够的安全性。ISO 7498-2 规定了 5 类安全服务，即鉴别服务、访问控制服务、数据保密性服务、数据完整性服务和禁止否认(抗抵赖)服务。

1. 鉴别服务

鉴别服务可以鉴别参与通信的对等实体和数据源的合法性。

1)对等实体鉴别

对等实体鉴别服务由第 N 层实体提供时，可向第 $N+1$ 层实体证实对等实体是它所需要的第 $N+1$ 层实体，提供对等实体之间的合法性判断。该服务在建立连接或在数据传输期间的某些时刻使用，以证实一个或多个其他实体连接的一个或多个实体的身份。该服务在使用期让用户确信：某个实体没有试图冒充别的实体，而且没有试图非法重演以前的某个连接。它们可以实施对单向或双向对等实体的鉴别，既可以带有效期校验，也可以不带，以提供不同程度的保护。

2)数据源鉴别

这种安全服务由第 N 层实体提供时，可向第 $N+1$ 层实体证实数据源是它所需要的第 $N+1$ 层对等实体。这种服务用来鉴别发送实体的合法性，确保数据是由合法实体发出的，以防假冒，但不提供防止数据单元被复制或篡改的保护。

2. 访问控制服务

访问控制服务能够防止未经授权而利用通过 OSI 参考模型的可访问资源。这种安全服务可用于对某种资源的各种不同类型的访问(如通信资源的利用、信息资源的读/写或删除、处理资源的操作等)，或用于对所有资源的某类访问。这种访问控制要与不同的安全策略协调一致。

3. 数据保密性服务

数据保密性服务能够对数据提供保护，防止数据未经授权而被泄漏，防止在系统之间交换数据时数据被截获。数据保密性包括连接保密性、无连接保密性、选择字段保密性和通信业务流保密性 4 项服务。

4. 数据完整性服务

数据完整性服务用于防止在系统之间交换数据时，非法修改数据或丢失数据。在一次连接中，连接开始时使用对等实体鉴别服务，在连接的生命期使用数据完整性服务，这样可以联合起来为在此连接中传送的所有数据单元的来源和完整性提供保证。数据完整性分为实体完整性、域完整性、参照完整性、用户定义的完整性 4 类。

5. 禁止否认(抗抵赖)服务

禁止否认(抗抵赖)服务用来防止通信双方否认发送或接收数据的行为。禁止否认包括带数据源证明的禁止否认和带递交证明的禁止否认两种形式。

1.5.2 安全机制

ISO 7498-2 标准制定了 8 类安全机制，即加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、业务填充机制、路由控制机制和公证机制。

1. 加密机制

加密是提供数据保密最常用的方法，加密机制是安全机制中的基础和核心。加密机制

包括加密的保密性、加密算法、密钥管理等。通过加密技术与其他技术相结合，可以提供数据的保密性和完整性。除了会话层不提供加密保护外，其他各层上可进行加密保护。

2.数字签名机制

数字签名是附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种数据或变换允许数据单元的接收者确认数据单元的来源及其完整性，并保护数据，防止被他人伪造。它主要用来防止通信双方发生否认、伪造、篡改和冒充等情况。这种安全机制决定两个过程：一是对数据单元签名，二是验证签过名的数据单元。第一个过程可以利用签名者私有的(即独有和保密的)信息，而第二个过程则要利用公之于众的规程和信息，但通过它们并不能推出签名者的私有信息。

3.访问控制机制

访问控制机制是按照事先制定的规则确定主体对客体的访问是否合法，防止未经授权的用户非法访问系统资源。如果某个实体试图使用非授权的资源，或者以不正当方式使用授权资源，那么访问控制机制将拒绝这一企图，同时还可能产生一个报警信号或将其记录下来作为安全审计跟踪的一个部分。访问控制机制可应用于通信联系中的任一端点，或应用于任何一个中间点。它主要利用访问控制表、口令、安全标记、能力表等来表示合法访问权。

4.数据完整性机制

数据完整性机制包括以下两个方面：

(1)单个的数据单元或字段的完整性。

(2)数据单元串或字段串的完整性，即要求数据编号的连续性和时间标记的正确性等。

保护单个数据单元的完整性可以利用分组校验码或密码校验值来防止信息被修改。保护数据单元串或字段串的完整性，可以利用顺序号、时间标记或密码链等防止信息被扰乱、丢失和插入等。

5.鉴别交换机制

鉴别交换机制通过信息交换以确保实体身份。可用于鉴别交换的技术有口令、密码、实体的特征或占有物、时钟标志和同步时钟、双向和三向握手(分别用于单方和双方鉴别)、数字签名或公证机构实现的不可否认服务等。

6.业务填充机制

业务填充机制主要用于对抗非法者在线路上监听数据并对其业务流量和流向进行分析。一般采用的方法为在无信息传输时，由保密装置连续发出伪随机序列，使得非法者不知哪些是有用信息，哪些是无用信息。该机制可用于提供对各种等级的保护，以对抗通信业务分析，但只有在业务填充受到保密性服务保护时该机制才有效。

7.路由控制机制

路由控制机制使发送信息者可以选择特殊安全的线路发送信息。路由既可以动态选择，也可以事先安排好，以便于利用物理上安全的子网、中继站或链路。使用这种安全机制，携带某些安全标签的数据将受到检查，以防止非法信息通过某些子网、中继站或链路。

8.公证机制

在两个或多个实体间进行通信时，数据的完整性、来源、时间和目的地等内容可由公证机制来保证。

每个通信场合都可以利用数字签名、加密和完整性机制以适应公证人所提供的服务。在使用公证机制时，数据经由受保护的通信通道和公证人在通信实体之间进行传送。

1.5.3 安全服务、安全机制与 OSI 参考模型各层的关系

ISO 7498-2 标准制定了安全服务和安全机制的相互关系以及 OSI 参考模型内部可以提供这些服务和机制的层。一种安全服务可以通过某种安全机制单独提供，也可以通过多种安全机制联合提供，而且一种安全机制还可用于提供一种或多种安全服务。安全服务、安全机制与 OSI 参考模型各层的关系见表 1-2。表中 Y 表示该项安全机制适于提供对应的安全服务，它既可以单独应用，也可以与其他机制联合应用；空格表示该项安全机制不适合提供对应的安全服务。

表 1-2 安全服务、安全机制与 OSI 参考模型各层的关系

安全机制 / 安全服务	加密	数字签名	访问控制	数据完整性	鉴别交换	业务填充	路由控制	公证	在 OSI 参考模型中的哪几层
对等实体鉴别	Y	Y			Y				3,4,7
数据源鉴别	Y	Y							3,4,7
访问控制服务			Y						3,4,7
连接保密性	Y						Y		1,2,3,4,7
无连接保密性	Y						Y		2,3,4,7
选择字段保密性	Y								7
业务流保密性	Y					Y	Y		1,3,7
带恢复的连接完整性	Y			Y					4,7
不带恢复的连接完整性	Y			Y					3,4,7
选择字段连接完整性	Y			Y					7
无连接完整性	Y	Y		Y					3,4,7
选择字段无连接完整性	Y	Y		Y					7
带数据源证明的禁止否认		Y		Y				Y	7
带递交证明的禁止否认		Y		Y				Y	7

注：OSI 参考模型第 7 层的应用程序本身必须提供表 1-2 中的所有安全服务。

本章小结

本章是对计算机信息安全的概括性介绍，学习本章有助于全面了解计算机信息安全。本章也是全书的提纲，后面各章节都将围绕本章内容进行展开和深入叙述。

本章主要介绍了计算机信息安全面临的威胁，包括自然威胁和人为威胁；计算机信息安全的定义、特性和分类；计算机信息安全的对策，从技术保障、管理保障和人员保障 3 方面进行了阐述；OSI 参考模型的信息安全体系结构，主要包括 5 类安全服务和 8 类安全机制。一

种安全服务的实施可以使用不同的安全机制，是单独使用还是组合使用，取决于安全服务的目的以及使用的安全机制。

无论采取何种防范措施都不能保证计算机信息系统的绝对安全，安全是相对的，不安全才是绝对的。因此，在实际应用中，经济因素和时间因素是判别安全性的重要指标，应该能够正确评估可能的安全风险，制定正确的安全策略并采用适当的安全机制。

习　题　1

1. 对计算机信息安全造成威胁的主要因素有哪些？
2. 计算机信息安全的特性有哪些？
3. 计算机信息安全的对策有哪些？
4. ISO 7498-2 标准包含哪些内容？
5. 怎样实现计算机信息安全？
6. 简述对计算机信息安全的理解和认识。