1 信息安全概述

本章主要介绍信息安全的概念及发展历史，介绍了信息安全体系的五类安全服务以及八类安全机制，指出了信息安全存在的主要威胁和防御策略，最后给出了信息安全的评估标准。

通过本章的学习，使读者：

（1）了解信息安全的概念和发展历史；

（2）理解信息安全体系的五类安全服务以及八类安全机制；

（3）了解信息安全存在的主要威胁和防御策略；

（4）理解信息安全的评估标准。

在信息化飞速发展的今天，信息作为一种资源，其普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。随着现代通信技术的迅速发展和普及，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，信息技术已经成为一个国家的政治、军事、经济和文化等发展的决定性因素，但是信息系统或信息网络中的信息资源通常会受到各种类型的威胁、干扰和破坏，计算机信息安全问题已成为制约信息化发展的瓶颈，日渐成为我们必须面对的一个严峻问题，从大的方面说，国家的政治、经济、军事、文化、意识形态等领域的信息安全受到威胁；从小的方面说，计算机信息安全问题也涉及到人们的个人隐私和私有财产安全等。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。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。

信息是社会发展的重要战略资源。信息安全已成为急待解决、影响国家大局和长远利益的重大关键问题，信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交世界各国在奋力攀登的制高点。信息安全问题如果解决不好将全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面，使国家处于信息战和高度经济金融风险的威胁之中。

1.1 信息安全的概念

1.1.1 信息的概念

信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。ISO/IEC 的 IT 安全管理指南（GMITS，即 ISO/IEC TR 13335）给出的信息（Information）解释是：信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。

计算机的出现和逐步的普及，使信息对整个社会的影响逐步提高到一种绝对重要的地位。信息量、信息传播的速度、信息处理的速度以及应用信息的程度等都以几何级数的方式在增长。

信息技术的发展对人们学习知识、掌握知识、运用知识提出了新的挑战。对我们每个人、每个企事业机构来说，信息是一种资产，包括计算机和网络中的数据，还包括专利、著作、文件、商业机密、管理规章等，就像其他重要的固定资产一样，信息资产具有重要的价值，因而需要进行妥善保护。

知己知彼，百战不殆，要保证信息的安全，就需要我们熟悉所保护的信息以及信息的存储、处理系统，熟悉信息安全性所面临的威胁，以便做出正确的决策。

1.1.2 信息安全的含义

信息安全的实质就是要保护信息资源免受各种类型的危险，防止信息资源被故意或偶然地非授权泄露、更改、破坏，或使信息被非法系统辨识、控制和否认，即保证信息的完整性、可用性、保密性和可靠性。信息安全本身包括的范围很大，从国家军事政治等机密安全，到防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。

信息安全包括软件安全和数据安全，软件安全是指软件的防复制、防篡改、防非法执行等。数据安全是指计算机中的数据不被非法读出、更改、删除等。

信息安全的含义包含如下方面：

1. 信息的可靠性

信息的可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。

2. 信息的可用性

信息的可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。

3. 信息的保密性

信息的保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

即防止信息泄露给非授权个人或实体，信息只为授权使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

4. 信息的完整性

信息的完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

5. 信息的不可抵赖性

信息的不可抵赖性也称作不可否认性。在网络信息系统的信息交互过程中，确信参与者的真实同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

6. 信息的可控性

信息的可控性是对信息的传播及内容具有控制能力的特性。

除此之外，信息安全还包括鉴别、审计追踪、身份认证、授权和访问控制、安全协议、密钥管理、可靠性等。

1.2 信息安全的发展历史

人类很早就在考虑怎样秘密地传递信息了。文献记载的最早有实用价值的通信保密技术是古罗马帝国时期的 Caesar 密码。它能够把明文信息变换为人们看不懂的称为密文的字符串，当把密文传递到自己伙伴手中的时候，又可方便地还原为原来的明文形式。Caesar 密码实际上非常简单，需要加密时，把字母 A 变成 D、B 变为 E、……、W 变为 Z、X 变为 A、Y 变为 B、Z 变为 C，即密文由明文字母循环移 3 位得到。反过来，由密文变为明文也相当简单。

随着 IT 技术的发展，各种信息电子化，可以更加方便地获取、携带与传输，相对于传统的信息安全保障，需要更加有力的技术保障，而不单单是对接触信息的人和信息本身进行管理，介质本身的形态已经从“有形”到“无形”。在计算机支撑的业务系统中，正常业务处理的人员都有可能接触、获取这些信息，信息的流动是隐性的，对业务流程的控制就成了保障涉密信息的重要环节。

在不同的发展时期，信息安全的侧重点和控制方式是有所不同的，大致说来，信息安全的发展过程经历了三个阶段。

早在 20 世纪初期，通信技术还不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，人们强调的主要是信息的保密性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单称为通信安全（COMSEC，Communication Security）。

20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机得到广泛应用，人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息

安全阶段（INFOSEC，Information Security）。

20 世纪 80 年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点从传统的保密性、完整性和可用性的原则衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障（Information Assurance）阶段。

开放复杂的信息系统面临着诸多风险，而为了解决这些风险问题，人们一直在寻找问题的解决之道，最直接的做法就是各种安全技术和产品的选择使用，密码产品、防火墙、病毒防护、入侵检测、终端接入控制、网络隔离、安全审计、安全管理、备份恢复等技术领域产品研发取得明显进展，产品功能逐步向集成化、系统化方向发展。

随着信息技术的快速发展和广泛应用，基础信息网络和重要信息系统安全、信息资源安全以及个人信息安全等问题与日俱增，应用安全日益受到关注，主动防御技术成为信息安全技术发展的重点，信息安全产品与服务演化为多技术、多产品、多功能的融合，多层次、全方位、全网络的立体监测和综合防御趋势不断加强。信息安全保障逐步由传统的被动防护转向“监测—响应式”的主动防御，信息安全技术正朝着构建完整、联动、可信、快速响应的综合防护防御系统方向发展。信息技术网络化、服务化等都在积极推动信息安全服务化，信息安全服务在产业中的比重将不断提高，将逐渐主导产业的发展。

1.3 信息系统安全体系结构

研究信息系统安全体系结构，就是将普遍性安全体系原理与自身信息系统的实际相结合，形成满足信息系统安全需求的安全体系结构。

1989 年 12 月，国际标准化组织 ISO 颁布了 ISO7498-2 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，并于 1995 年再次在技术上进行了修正。OSI 安全体系结构包括五类安全服务以及八类安全机制。

1.3.1 五类安全服务

五类安全服务包括认证（鉴别）服务、访问控制服务、数据保密性服务、数据完整性服务和抗否认性服务。

（1）认证（鉴别）服务：提供对通信中对等实体和数据来源的认证（鉴别）。

（2）访问控制服务：用于防治未授权用户非法使用系统资源，包括用户身份认证和用户权限确认。

（3）数据保密性服务：为防止网络各系统之间交换的数据被截获或被非法存取而泄密，提供机密保护。同时，对有可能通过观察信息流就能推导出信息的情况进行防范。

（4）数据完整性服务：用于组织非法实体对交换数据的修改、插入、删除以及在数据交换过程中的数据丢失。

（5）抗否认性服务：用于防止发送方在发送数据后否认发送和接收方在收到数据后否认收到或伪造数据的行为。

1.3.2 八类安全机制

八大类安全机制包括加密机制、数据签名机制、访问控制机制、数据完整性机制、认证机制、业务流填充机制、路由控制机制、公正机制。

（1）加密机制：是确保数据安全性的基本方法，在 OSI 安全体系结构中应根据加密所在的层次及加密对象的不同，而采用不同的加密方法。

（2）数字签名机制：是确保数据真实性的基本方法，利用数字签名技术可进行用户的身份认证和消息认证，它具有解决收、发双方纠纷的能力。

（3）访问控制机制：从计算机系统的处理能力方面对信息提供保护。访问控制按照事先确定的规则决定主体对客体的访问是否合法，当以主题试图非法使用一个未经给出的报警并记录日志档案。

（4）数据完整性机制：破坏数据完整性的主要因素有数据在信道中传输时受信道干扰影响而产生错误，数据在传输和存储过程中被非法入侵者篡改，计算机病毒对程序和数据的传染等。纠错编码和差错控制是对付信道干扰的有效方法。对付非法入侵者主动攻击的有效方法是保温认证，对付计算机病毒有各种病毒检测、杀毒和免疫方法。

（5）认证机制：在计算机网络中，认证主要有用户认证、消息认证、站点认证和进程认证等，可用于认证的方法有已知信息（如口令）、共享密钥、数字签名、生物特征（如指纹）等。

（6）业务流填充机制：攻击者通过分析网络中有一路径上的信息流量和流向来判断某些事件的发生，为了对付这种攻击，一些关键站点间再无正常信息传送时，持续传递一些随机数据，使攻击者不知道哪些数据是有用的，哪些数据是无用的，从而挫败攻击者的信息流分析。

（7）路由控制机制：在大型计算机网络中，从源点到目的地往往存在多条路径，其中有些路径是安全的，有些路径是不安全的，路由控制机制可根据信息发送者的申请选择安全路径，以确保数据安全。

（8）公正机制：在大型计算机网络中，并不是所有的用户都是诚实可信的，同时也可能由于设备故障等技术原因造成信息丢失、延迟等，用户之间很可能引起责任纠纷，为了解决这个问题，就需要有一个各方都信任的第三方以提供公证仲裁，仲裁数字签名技术是这种公正机制的一种技术支持。

1.4 信息安全的防御策略

计算机信息系统安全保护工作的任务，就是不断发现、堵塞系统安全漏洞，预防、发现、制止利用或者针对系统进行的不法活动，预防、处置各种安全事件和事故，提高系统安全系数，确保计算机信息系统安全可用。

1.4.1 信息安全存在的主要威胁

1. 失泄密

失泄密是指计算机网络信息系统中的信息，特别是敏感信息被非授权用户通过侦收、截获、窃取或分析破译等方法恶意获得，造成信息泄露的事件。造成失泄密以后，计算机网络一般会继续正常工作，所以失泄密事故往往不易被察觉，但是失泄密所造成的危害却是致命的，其危害时间也往往会持续很长。失泄密主要有六条途径：一是电磁辐射泄漏；二是传输过程中失泄密；三是破译分析；四是内部人员的泄密；五是非法冒充；六是信息存储泄漏。

2. 数据破坏

数据破坏是指计算机网络信息系统中的数据由于偶然事故或人为破坏，被恶意修改、添加、伪造、删除或者丢失。信息破坏主要存在六个方面：一是硬件设备的破坏；二是程序方式的破坏；三是通信干扰；四是返回渗透；五是非法冒充；六是内部人员造成的信息破坏。

3. 计算机病毒

计算机病毒是指恶意编写的破坏计算机功能或者破坏计算机数据，影响计算机使用并且能够自我复制的一组计算机程序代码。计算机病毒具有以下特点：一是寄生性；二是繁殖力特别强；三是潜伏期特别长；四是隐蔽性高；五是破坏性强；六是计算机病毒具有可触发性。

4. 网络入侵

网络入侵是指计算机网络被黑客或者其他对计算机网络信息系统进行非授权访问的人员，采用各种非法手段侵入的行为。他们往往会对计算机信息系统进行攻击，并对系统中的信息进行窃取、篡改、删除，甚至使系统部分或者全部崩溃。

5. 后门

后门是指在计算机网络信息系统中人为的设定一些“陷阱”，从而绕过信息安全监管而获取对程序或系统访问的权限，以达到干扰和破坏计算机信息系统正常运行的目的。后门一般可分为硬件后门和软件后门两种。硬件后门主要指蓄意更改集成电路芯片的内部设计和使用规程的“芯片捣鬼”，以达到破坏计算机网络信息系统的目的。软件后门主要是指程序员按特定的条件设计的，并蓄意留在软件内部的特定源代码。

1.4.2 保障信息安全的主要防御策略

尽管计算机网络信息安全受到威胁，但是采取恰当的防护措施也能有效地保护网络信息的安全。信息系统的安全策略是为了保障规定级别下的系统安全而制定和必须遵守的一系列准则和规定，它考虑到入侵者可能发起的任何攻击，以及为使系统免遭入侵和破坏而必然采取的措施。实现信息安全不但靠先进的技术，也得靠严格的安全管理、法律约束和安全教育。

本策略文件主要包括：物理安全策略、运行管理策略、信息安全策略、备份与恢复策略、应急计划和相应策略、计算机病毒与恶意代码防护策略、身份鉴别策略、访问控制策略、信息完整性保护策略、安全审计策略。

1. 物理安全策略

计算机信息和其他用于存储、处理或传输信息的物理设施，例如硬件、磁介质、电缆等，对于物理破坏来说是易受攻击的，同时也不可能完全消除这些风险。因此，应该将这些信息及物理设施放置于适当的环境中并在物理上给予保护，使之免受安全威胁和环境危害。

2. 运行管理策略

为避免信息遭受人为过失、窃取、欺骗、滥用的风险，应加强计算机信息系统运行管理，提高系统安全性、可靠性，减少恶意攻击、各类故障带来的负面效应，全体相关人员都应该了解计算机及系统的网络与信息安全需求，建立行之有效的系统运行维护机制和相关制度。比如，建立健全中心机房管理制度、信息设备操作使用规程、信息系统维护制度、网络通信管理制度、应急响应制度等。

3. 信息安全策略

为保护存储计算机的数据信息的安全性、完整性、可用性，保护系统中的信息免受恶意的或偶然的篡改、伪造和窃取，有效控制内部泄密的途径和防范来自外部的破坏，可借助数据异地容灾备份、密文存储、设置访问权限、身份识别、局部隔离等策略提高安全防范水平。

在设计信息系统时，选用相对成熟、稳定和安全的系统软件并保持与其提供商的密切接触，通过官方网站或合法渠道，密切关注其漏洞及补丁发布情况，争取“第一时间”下载补丁软件，弥补不足。

4. 计算机病毒与恶意代码防护策略

病毒防范包括预防和检查病毒（包括实时扫描、过滤和定期检查），主要内容包括：控制病毒入侵途径；安装可靠的防病毒软件；对系统进行实时检测和过滤；定期杀毒；及时更新病毒库；详细记录；防病毒软件的安装和使用由信息安全管理员执行。

5. 身份鉴别和访问控制策略

为了保护计算机系统中信息不被非授权地访问、操作或被破坏，必须对信息系统实行控制访问。采用有效的口令保护机制，包括：规定口令的长度、有效期、口令规则。保障用户登录和口令的安全；用户选择和使用密码时应参考良好的安全惯例，严格设置对重要服务器、网络设备的访问权限。

6. 安全审计策略

计算机及信息系统的信息安全审计活动和风险评估应当定期执行。

特别是系统建设前或系统进行重大变更之前，必须进行风险评估工作。

定期进行信息安全审计和信息安全风险评估，并形成文档化的信息安全审计报告和风险评估报告。

1.5 信息安全的评估标准

信息安全评估是信息安全生命周期中的一个重要环节，是对企业的网络拓扑结构、重要

服务器的位置、带宽、协议、硬件、与 Internet 的接口、防火墙的配置、安全管理措施及应用流程等进行全面的安全分析，并提出安全风险分析报告和改进建议书。

信息安全评估标准是信息安全评估的行动指南。可信的计算机系统安全评估标准（TCSEC）由美国国防部于 1985 年公布的，是计算机系统信息安全评估的第一个正式标准。它把计算机系统的安全分为 4 类、7 个级别，对用户登录、授权管理、访问控制、审计跟踪、隐蔽通道分析、可信通道建立、安全检测、生命周期保障、文档写作、用户指南等内容提出了规范性要求。

1. D 类安全等级

D 类安全等级只包括 D1 一个级别。D1 的安全等级最低。D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

2. C 类安全等级

该类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。C1 系统的可信任运算基础体制（Trusted Computing Base，TCB）通过将用户和数据分开来达到安全的目的。在 C1 系统中，所有的用户以同样的灵敏度来处理数据，即用户认为 C1 系统中的所有文档都具有相同的机密性。C2 系统比 C1 系统加强了可调的审慎控制。在连接到网络上时，C2 系统的用户分别对各自的行为负责。C2 系统通过登录过程、安全事件和资源隔离来增强这种控制。C2 系统具有 C1 系统中所有的安全性特征。

3. B 类安全等级

B 类安全等级可分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B1 系统满足下列要求：系统对网络控制下的每个对象都进行灵敏度标记；系统使用灵敏度标记作为所有强迫访问控制的基础；系统在把导入的、非标记的对象放入系统前标记它们；灵敏度标记必须准确地表示其所联系的对象的安全级别；当系统管理员创建系统或者增加新的通信通道或 I/O 设备时，管理员必须指定每个通信通道和 I/O 设备是单级还是多级，并且管理员只能手工改变指定；单级设备并不保持传输信息的灵敏度级别；所有直接面向用户位置的输出（无论是虚拟的还是物理的）都必须产生标记来指示关于输出对象的灵敏度；系统必须使用用户的口令或证明来决定用户的安全访问级别；系统必须通过审计来记录未授权访问的企图。

B2 系统必须满足 B1 系统的所有要求。另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B2 系统必须满足下列要求：系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变；只有用户能够在可信任通信路径中进行初始化通信；可信任运算基础体制能够支持独立的操作者和管理员。

B3 系统必须符合 B2 系统的所有安全需求。B3 系统具有很强的监视委托管理访问能力和抗干扰能力。B3 系统必须设有安全管理员。B3 系统应满足以下要求：除了控制对个别对象的访问外，B3 必须产生一个可读的安全列表；每个被命名的对象提供对该对象没有访问权的用

户列表说明；B3 系统在进行任何操作前，要求用户进行身份验证；B3 系统验证每个用户，同时还会发送一个取消访问的审计跟踪消息；设计者必须正确区分可信任的通信路径和其他路径；可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪；可信任的运算基础体制支持独立的安全管理。

4. A 类安全等级

A 系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收到一个安全策略的正式模型；所有的安装操作都必须由系统管理员进行；系统管理员进行的每一步安装操作都必须有正式文档。

20 世纪 90 年代初，法、英、荷、德欧洲四国联合发布信息技术安全评估标准（ITSEC，欧洲百皮书），它提出了信息安全的机密性、完整性、可用性的安全属性。机密性就是保证没有经过授权的用户、实体或进程无法窃取信息；完整性就是保证没有经过授权的用户不能改变或者删除信息，从而信息在传送的过程中不会被偶然或故意破坏，保持信息的完整、统一；可用性是指合法用户的正常请求能及时、正确、安全地得到服务或回应。ITSEC 把可信计算机的概念提高到可信信息技术的高度上来认识，对国际信息安全的研究、实施产生了深刻的影响。

1996 年六个国家（美、加、英、法、德、荷）联合提出了信息技术安全评价的通用标准（CC），并逐渐形成国际标准 ISO15408。该标准定义了评价信息技术产品和系统安全性的基本准则，提出了目前国际上公认的表述信息技术安全性的结构，即把安全要求分为规范产品和系统安全行为的功能要求，以及解决如何正确有效地实施这些功能的保证要求。CC 标准是第一个信息技术安全评价国际标准，它的发布对信息安全具有重要意义，是信息技术安全评价标准以及信息安全技术发展的一个重要里程碑。

我国主要是等同采用国际标准。公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB17859-1999《计算机信息系统安全保护等级划分准则》已正式颁布并实施。该准则将信息系统安全分为 5 个等级：自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计等，这些指标涵盖了不同级别的安全要求。GB18336 也是等同采用 ISO 15408 标准。

随着世界各国对标准的地位和作用的日益重视，信息安全评估标准多国化、国际化成为大势所趋；国际标准组织将进一步研究改进 ISO/IEC 15408 标准，各国在采用国际标准的同时，将利用有关条款保护本国利益；最终，国内、国际多个标准并存将成为普遍现象。

1.6 实训：信息安全技术基础

1.6.1 实训目的

熟悉信息安全技术的基本概念，了解信息安全技术的基本内容。了解网络环境中主流的信息安全技术网站，掌握通过专业网站不断丰富信息安全最新知识的学习方法，尝试通过专业网站的辅助与支持来开展信息安全技术使用实践。

1.6.2 实训环境

带有浏览器、可以联网的计算机。

1.6.3 实训内容

1．查阅有关资料，给出信息安全的定义，并用自己的语言概述出来。

2．查询相关资料，查看你的系统是否安全，如果有安全漏洞，应该怎么补救，以后用计算机时应该怎么做可以避免这些危险。

习　　题

一、选择

1．下列关于信息的说法是错误的是_____。

A．信息是人类社会发展的重要支柱　　B．信息本身是无形的

C．信息具有价值，需要保护　　D．信息可以以独立形态存在

2．信息安全经历了三个发展阶段，以下不属于这三个发展阶段的是_____。

A．通信保密阶段　　B．加密阶段

C．信息安全阶段　　D．安全保障阶段

3．信息安全的基本属性是_____。

A．机密性　　B．可用性

C．完整性　　D．上面 3 项都是

4．信息安全在通信保密阶段对信息安全的关注局限在_____安全属性。

A．不可否认性　　B．可用性

C．保密性　　D．完整性

5．下面所列的安全机制不属于信息安全保障体系中的事先保护环节的是_____。

A．杀毒软件　　B．数字证书认证

C．防火墙　　D．数据库加密

6．根据 ISO 的信息安全定义，下列选项中_____是信息安全三个基本属性之一。

A．真实性　　B．可用性

C．可审计性　　D．可靠性

7．为了数据传输时不发生数据截获和信息泄密而采取了加密机制。这种做法体现了信息安全的_____属性。

A．保密性　　B．完整性

C．可靠性　　D．可用性

8．信息安全领域内最关键和最薄弱的环节是_____。

A．技术　　B．策略

C．管理制度　　D．人

9．_____对信息安全管理负有责任。

A．高级管理层　　B．安全管理员

C．IT 管理员　　D．所有与信息系统有关人员

10．用户身份鉴别是通过_____完成的。

A．口令验证　　B．审计策略

C．存取控制　　D．查询功能

11．ISO 7498-2 从体系结构观点描述了 5 种安全服务，以下不属于这 5 种安全服务的是_____。

A．身份鉴别　　B．数据报过滤

C．授权控制　　D．数据完整性

12．ISO 7498-2 描述了 8 种特定的安全机制，以下不属于这 8 种安全机制的是_____。

A．安全标记机制　　B．加密机制

C．数字签名机制　　D．访问控制机制

13．用于实现身份鉴别的安全机制是_____。

A．加密机制和数字签名机制　　B．加密机制和访问控制机制

C．数字签名机制和路由控制机制　　D．访问控制机制和路由控制机制

14．ISO 安全体系结构中的对象认证服务使用完成_____。

A．加密机制　　B．数字签名机制

C．访问控制机制　　D．数据完整性机制

15．数据保密性安全服务的基础是_____。

A．数据完整性机制　　B．数字签名机制

C．访问控制机制　　D．加密机制

16．我国在 1999 年发布的国家标准_____为信息安全等级保护奠定了基础。

A．GB 17799　　B．GB 15408

C．GB 17859　　D．GB 14430

17．信息安全评测标准 CC 是_____标准。

A．美国　　B．国际

C．英国　　D．澳大利亚

18．《信息系统安全等级保护基本要求》中，对不同级别的信息系统应具备的基本安全保护能力进行了要求，共划分为_____级。

A．4　　B．5

C．6　　D．7

二、简答

1．列举并解释 ISO/OSI 中定义的 5 种标准的安全服务。

2．简述信息安全存在的主要威胁

3．简述保障信息安全的主要防御策略。

4．信息安全评估标准是信息安全评估的行动指南，简述信息安全评估标准。