第1章 信息安全技术概述

内容概要

21世纪是信息“大爆炸”的时代，得益于互联网的高速发展，网络上的各种信息呈几何级数扩展和传播。与此同时，信息安全形势也日益严峻。本章介绍信息与信息安全的基础知识。

知识要点

信息与信息安全。

信息安全面临的威胁。

信息安全模型。

信息安全等级保护的划分及含义。

1.1 信息安全简介

信息安全是传统通信保密的延续和发展，信息的涵盖面非常广，本书介绍的信息安全主要在计算机领域。

1.1.1 信息的基本概念

人们通常把消息、信号、数据、情报和知识等都看作信息。信息本身是无形的，通常可借助多种介质形式存在或传播，介质可包括计算机硬盘、纸张、网络等。信息的特性如下：

- **依附性**：用“符号”表示，依附于一定的物理介质。
- **动态性**：信息只有及时更新才有价值。
- **可处理性**：内容可以识别，形式可以转换或变换。
- **共享性**：信息可无限扩散。
- **可传递性**：在时间和空间上都具有传播性。
- **异步性**：以存储方式接收，可在任何时间使用。
- **可交换性**：可在两个主体间实现信息的交换。
- **可伪性**：信息是可以伪造的。

国际标准化组织（International Organization for Standardization，ISO）认为：“信息是通过施加于数据上的某些约定而赋予这些数据的特定含义。”对于信息来说，主要的处理方法包括：

- **创建**：通过记录或者自身的统计创建出信息。
- **存储**：信息被记录在计算机硬盘、纸张或者以其他形式存储在介质中。
- **传递**：通过载体或渠道，将信息分发出去，分享给其他使用者。
- **使用**：通过使用达成某种需求的目标。
- **更改**：可以对信息进行修改以完善信息达到使用者的目的。
- **销毁**：将信息彻底清除，不使用或不传播。

依托于互联网这一新的载体，信息有了更大的展示空间和更多的传播渠道。

1.1.2 信息安全概述

ISO将信息安全定义为：“技术上和管理上为数据处理系统建立的安全保护，保护信息系统的硬件、软件及相关数据不因偶然或者恶意的原因遭到破坏、更改及泄露。”

对于信息安全来说，需要确保以电磁信号为主要形式的、通过计算机网络化系统进行获取、处理、存储、传输和应用的信息内容在各个物理及逻辑区域中的安全存在，且不发生任何侵害行为。

1. 信息安全的发展

信息安全并不是凭空出现的，信息安全的发展主要分为通信安全、信息安全和信息保障3个阶段。

（1）通信安全。

20世纪90年代以前，这一阶段的信息安全可以简单称为通信安全，其主要目的是保障信息传递的安全，防止信源、信宿以外的对象查看信息。

（2）信息安全。

在20世纪90年代以后，信息安全主要保证信息的机密性、完整性、可用性、可控性、不可否认性。

- **机密性**：指信息只能为授权者使用，未经授权的用户不能获取信息的内容。
- **完整性**：指保证信息在存储和传输过程中未经授权不能被改变的特性，从而确保信息的真实性。
- **可用性**：指保证信息和信息系统随时为授权者提供服务的有效特性。
- **可控性**：指授权实体可以控制信息系统和信息使用的特性。
- **不可否认性**：指任何实体均无法否认其实施过的信息行为的特性，也称为抗抵赖性。

（3）信息保障。

最早的信息保障内容包括保护、检测、反应、恢复4个方面，这4个方面的内容构成了信息安全保障的完整动态过程。

- **保护**：事先采取一定的安全防御措施，使攻击条件无法具备，让攻击者无法实施入侵信息系统的行为。保护属于被动防御行为，无法彻底阻止各种对信息安全系统的攻击行为。
- **检测**：根据相关的安全防御策略，利用各种技术手段，针对可能被攻击者利用的信息系统的弱点，进一步实时检查，形成检测报告。现在主要的检测技术有入侵检测、恶意代码检测、系统漏洞扫描等。
- **反应**：针对破坏信息安全的行为做出的响应处理，可抑制危害的进一步扩大，将损失降到最小。
- **恢复**：当危害事件发生后，将信息系统恢复到原有的状态，并加入针对性的防范措施，将危害降到最小。

我国对于信息保障的定义是：信息保障是对信息和信息系统的安全属性、功能、效率进行保障的动态行为过程。它运用源于人、管理、技术等因素所形成的预警能力、保护能力、检测能力、反应能力、恢复能力和反击能力，在信息和系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施的真实性、可用性、完整性、保密性、可控性、不可否认性等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。

2. 信息安全的主要影响因素

信息安全不是一个孤立的、静止的概念，信息安全具有系统性、相对性和动态性的特点。在影响信息安全的主要因素中，人、技术、管理是最主要的因素。其中，人是信息保障的基础，技术是信息保障的核心，管理是信息保障的关键。

影响信息安全的因素，可以分为内部因素和外在因素两种。

（1）内部因素。

内部因素主要是由系统的复杂性所导致的，包括过程复杂、网络结构复杂、软件应用复杂。在程序与数据上存在“不确定性”，如多线程并发错误、数据竞争等。从设计的角度看，在设计时考虑的优先级中安全性相对于易用性、代码大小、执行程度等因素被放在次要的位置。由于程序设计中的不完善，软件总是存在或明或暗的bug。还有无意失误（如无意中文件被删除）、人为的恶意攻击，如利用病毒、入侵工具实施操作、 监听、截包等，都会对信息安全造成危害。在维护时，技术管理或组织管理的不完善等因素，都可能使信息安全受到威胁。

（2）外部因素。

外部因素主要是指安全环境受到各种威胁，其中包括通过物理威胁、系统漏洞、通信设备监听、篡改验证、恶意程序等破坏信息的安全性。最常见的网络攻击就是网络安全重大威胁之一，包括扫描嗅探、口令攻击、伪造身份、获取及提升权限、 植入病毒及木马、对存储介质进行破坏、数据窃取、修改信息权限等。

威胁的来源，其实是由人为因素和系统自身逻辑与物理条件等诸多因素综合在一起决定的，但归根结底，还是人在起决定性的作用。无论是系统自身的缺陷，还是配置管理上的不善，都是因为人的参与（访问操作或攻击破坏），给网络的安全带来了种种隐患和威胁。

3. 信息安全的目标

保密性、完整性和可用性分别反映了信息在3个不同方面的特性。

- **保密性**：确保信息在存储、使用、传输过程中不会泄漏给非授权用户。
- **完整性**：确保信息在存储、使用、传输过程中不会被非授权用户篡改，防止授权用户不恰当地修改信息，保持信息内部和外部的一致性。
- **可用性**：确保授权用户对信息及资源的正常使用不会被异常拒绝，允许授权用户可靠且及时地获取信息及访问资源。

安全属性的不同通常也意味着安全控制、保护功能的需求不同。通过评估3种不同安全属性，可以得出一个能够基本反映信息价值的数值。对信息进行赋值的目的是为了更好地反映信息的价值，以便于进一步评价信息相关的弱点、威胁和风险属性，并进行量化处理。

4. 信息安全的影响

随着信息化发展进程的不断加快，各种信息技术已经渗透到国家和社会生活的方方面面，对信息的依赖程度也已经上升到前所未有的高度。信息已经成为重要的战略资源，信息化水平已经成为衡量一个国家的国际竞争力、现代化水平、综合国力和经济发达程度的重要标志。信息安全已经成为影响和制约国家发展的重要因素，信息安全事关经济发展、社会稳定、国家安全、公众利益等方方面面。

1.2 信息安全面临的威胁

信息安全的威胁形式有很多，主要的威胁表现形式包括信息存储的安全威胁、信息传递的安全威胁、信息使用的安全威胁。

1.2.1 信息存储的安全威胁

信息在存储时，会以文档、图片、声音等多种形式保存在存储介质中，本地存储安全威胁主要来自于以下几个方面。

1. 信息泄漏

本地存储的信息泄漏可来自多个方面，如内部人员，对信息进行拷贝并泄漏给某个非授权的实体，或者别有用心的人通过对废弃的存储介质进行数据恢复从而进行窃取。所以必须对信息管理人员进行安全及防泄漏培训，并妥善处理损坏的信息存储介质。

非授权用户通过网络访问并复制重要的信息也是信息泄漏的主要途径，如黑客通过入侵技术获取本地数据库存储的各种数据，所以防范网络攻击是防止信息泄漏工作的重中之重。

2. 信息损坏

自然灾害，包括地震、洪水，或由于管理人员误操作造成信息文件的损坏、信息损毁或存储信息的硬件介质损坏而造成存储内容的丢失。虽然有妥善的数据备份策略，但并不是所有损坏的信息都能够被恢复，所以必须要保证存储介质运行时的环境安全，通过多种手段确保数据的安全性。

3. 信息篡改

对存储的信息进行恶意修改，破坏信息的完整性，造成信息内容的变化，但使用者并不知道信息已经被篡改，进而通过伪造数据达到非法获利的目标。所以，对本地的重要信息数据要使用适当的加密手段进行保存，以防非授权用户查看和修改。

4. 网络攻击

网络攻击并不一定是为了窃取信息，而是让信息无法正常传输或无法正常使用，如常见的对数据服务器的拒绝服务攻击，会让服务器无法正常响应服务请求。

1.2.2 信息传递的安全威胁

信息在存储媒体之间传输，或者通过网络传输时都有被监听窃取的风险，尤其在一些加密措施不足的无线网络中更为突出。

1. 信息截获

在信息传输过程中，泄漏的表现形式包括窃听、截收、侧信道攻击等。可以窃听无线传输信号，或者截获代理服务器的代理信息，如果加密手段不强，非常容易被破解。侧信道攻击指攻击者不能直接获得信息数据，但可以获取到这些加密信息的相关信息，然后通过分析获取信息的内容。

2. 信息欺骗

传递的信息被黑客获取后，通过修改信息的内容后，再发送给接收者。通过这种欺骗手段，黑客可以获取巨大的利益。

3. 信息丢失

在信息传输过程中，由于网络设备的故障，可能造成传输的信息丢失或损坏，导致信息无法正常到达目的地。信息丢失可以通过重传的方法解决，但在时效性上会造成损失。

1.2.3 信息使用的安全威胁

每个人每天都在使用大量的信息，即使在存储和传输过程中不存在安全问题，但在使用时仍有可能会遇到众多的安全威胁。

1. 信息伪造

非授权用户使用授权用户的信息提升权限，在进入信息管理后台后，就可以获取到各种重要的信息；或者假冒授权用户，通过授权用户的权限修改、伪造信息。

2. 信息否认

在对授权或非授权的信息进行修改后，再进行各种非法操作，并否认此次修改行为的发生，或否认是自己所为，从而导致参与者逃避应承担的责任。

3. 病毒及木马

使用者的使用环境不安全，信息被病毒破坏或被木马窃取，造成信息的损毁或泄露。

除了病毒及木马外，恶意代码也同样威胁着信息的安全。

4. 软件故障

操作系统或应用软件，由于软件漏洞被入侵、使用者的误操作、软件兼容性的问题等，都可能造成信息无法正常获取、使用与传输，所以需要确保使用信息时的操作系统和应用软件的稳定性。

5. 物理故障

在使用过程中，所用的设备本身可能会发生设备故障、供电故障、网络故障等，这些都可能造成信息的损坏。

1.3 信息安全模型

随着信息安全的影响越来越大，各个国家和标准化组织为了应对信息安全的各种威胁，开始研究各种应对方案并进行各种安全模型的设计。通过建模的思路来解决网络安全管理问题，可有效抵御外部攻击，保障网络安全。

1.3.1 安全模型的定义与作用

安全模型用于准确地描述安全的重要性及其与系统行为的关系。安全模型要求精确、无歧义、简单和抽象、容易理解。模型一般只涉及安全性，具有一定的平台独立性，不过多涉及系统的功能或实现。形式化模型是对现实世界的高度抽象，可以设定具体的应用目标，并可以利用工具来验证。形式化模型适用于对信息安全进行理论研究。

1.3.2 常见的信息安全模型

信息安全模型有很多，比较具有代表性的有以下几种。

1. Bell-LaPadula模型

Bell-LaPadula模型是全球第1个也是最著名的安全策略模型之一，由David Bell和Len LaPadula在1973年提出，简称BLP模型。BLP模型是可信系统的状态-转换模型，主要任务是定义使得系统获得“安全”的状态集合，检查系统的初始状态是否为“安全状态”，检查所有状态的变化均始于一个“安全状态”，并终止于另一个“安全状态”。

BLP模型定义了系统中的主体访问客体的操作规则。每个主体有一个安全级别，通过众多条例约束其对每个具有不同密级的客体的访问操作。采用了自主访问控制和强制访问控制相结合的方法，能够有效地保证系统内的信息安全，支持信息的保密性，但却不能保证信息的完整性。

2. Clark-Wilson模型

Clark-Wilson模型是一个确保商业数据完整性且在商业应用系统中提供安全评估框架的完整性及应用层的模型，由计算机科学家David D.Clark和会计师David R.Wilson于1987年提出，并在1989年进行了修正，简称CW模型。

Clark-Wilson模型着重研究与保护信息和系统的完整性，即组织完善的事务和清晰的责任划分。组织完善的事务意味着用户对信息的处理必须限定在一定的权力和范围之内进行，以保证数据完整性。责任划分意味着任务需要两人以上完成，且要进行任务划分，以避免个人欺骗行为的发生。

3. Biba模型

Biba模型是涉及计算机系统完整性的第1个模型，发布于1977年。Biba模型将完整性威胁分为来源于子系统内部和外部两种。如果子系统的一个组件是恶意的或不正确的，则产生内部威胁；如果一个子系统企图通过错误数据或不正确地调用函数来修改另一个子系统，则产生外部威胁。Biba模型认为内部威胁可以通过程序测试或检验来解决，所以该模型主要针对外部威胁。Biba模型基于两种规则来保障数据的完整性：下读属性，主体不能读取安全级别低于它的数据；上写属性，主体不能写入安全级别高于它的数据。

4. Chinese Wall模型

该模型的思路是将一些可能会产生访问冲突的数据分成不同的数据集，强制所有主体最多只能访问一个数据集，但访问哪个数据集并未受强制规则的限制。访问数据受限于主体已经获得的对数据的访问权限，而不是数据的属性（密级）。

该模型有三层结构。

- 底层由独立的数据项组成，每项涉及一个独立的公司法人。
- 中层将涉及同一公司法人的所有客体组织起来，称为“公司数据集”。
- 上层将公司数据集结合成组，每个组之间互为竞争对手，称为“兴趣冲突组”。

一个主体一旦已经访问过一个客体，则该主体只能访问位于同一数据集中的客体或在不同兴趣冲突组中的信息。在一个兴趣冲突组中，一个主体最多只能访问一家客户数据集。

5. HTP信息安全模型

从国家层面考虑有法律、法规、政策问题；从组织角度考虑有安全方针政策程序、安全管理、安全教育与培训、组织文化、应急计划和业务持续性管理等问题；从个人角度来看有职业要求、个人隐私、行为学、心理学等问题。因为人是信息安全中最活跃的因素，人的行为是信息安全保障最主要的方面。

用户可以依据“适度防范”原则综合采用商用密码、防火墙、防病毒、身份识别、网络隔离、可信服务、安全服务、备份恢复、PKI服务、取证、网络入侵陷阱、主动反击等多种技术和手段保护信息系统的安全。

用户应当遵循国内外相关信息安全标准与最佳实践过程，考虑到用户对信息安全的各个层面的实际需求，在风险分析的基础上引入恰当控制，建立合理的安全管理体系，从而保证组织赖以生存的信息资产的安全性、完整性和可用性。

1.3.3 信息安全管理体系

信息安全管理体系（Information Security Management System，ISMS）是1998年前后自英国发展起来的信息安全领域中的一个新概念，是管理体系思想和方法在信息安全领域的应用。近年来，伴随着ISMS国际标准的制定与修订，ISMS迅速被全球接受和认可，成为世界各国各种类型、各种规模的组织解决信息安全问题的一个有效方法。ISMS认证随之成为组织向社会及其相关方证明其信息安全水平和能力的一种有效途径。

信息安全管理体系是组织机构单位按照信息安全管理体系相关标准的要求，制定信息安全管理方针和策略，采用风险管理的方法进行信息安全管理计划、实施、评审检查、改进的信息安全管理执行的工作体系。信息安全管理体系按照ISO/IEC 27001标准《信息技术 安全技术 信息安全管理体系要求》的要求建立，ISO/IEC 27001标准是由BS 7799-2标准发展而来的。

信息安全管理体系是建立和维持信息安全管理体系的标准，标准要求组织通过确定信息安全管理体系范围、制定信息安全方针、明确管理职责、以风险评估为基础选择控制目标与控制方式等活动建立信息安全管理体系；体系一旦建立，组织应按体系规定的要求进行运作，以保

持体系运作的有效性；信息安全管理体系应形成一定的文件，即组织应建立并保持一个文件化的信息安全管理体系，其中应阐述组织被保护的资产、组织的风险管理方法、控制目标、控制方式和需要的保证程度。

1.4 信息安全等级保护

信息安全等级保护，简称等保，是我国针对网络信息安全制定的规范。信息系统安全等级保护的核心是对信息系统分等级，并按标准进行建设、管理和监督。

1.4.1 信息安全等级保护简介

等保，是在我国非保密信息系统中网络信息安全基本建设的主要规范，是我国信息安全防范措施的基本制度、基本对策和基本方式。对互联网和信息系统依照必要性标准分等级维护，安全性防护级别越高，安全性维护工作能力就越强。

在我国，等保已经被法律明确其地位。《中华人民共和国网络安全法》第21条明确规定，网络经营者要执行的等级保护规章制度责任；某些领域必须满足等保的要求才能涉足，绝大多数领域（如诊疗、文化教育、交通出行、电力能源、电信网这些重要信息基础设施建设领域）都需要遵守等保规定。在我国，等级保护有着完整的检测标准及管理体系，也是现阶段网络经营者或使用者可以参照的最佳标准，目的是保护网络经营者或使用者信息的安全性。

信息系统安全等级测评是验证信息系统是否满足相应安全保护等级的评估过程。信息安全等级保护要求不同安全等级的信息系统应具有不同的安全保护能力，一方面通过在安全技术和安全管理上选用与安全等级相适应的安全控制来实现；另一方面分布在信息系统中的安全技术和安全管理上不同的安全控制，通过连接、交互、依赖、协调、协同等相互关联关系共同作用于信息系统的安全功能，使信息系统的整体安全功能与信息系统的结构以及安全控制间、层面间和区域间的相互关联关系密切相关。因此，信息系统安全等级测评在安全控制测评的基础上，还要包括系统整体测评。

1.4.2 信息安全等级保护的重要意义

信息安全等级保护实施的重要意义包括以下3个方面。

- 满足合法合规要求，明确责任和工作方法，让安全防护更加规范。
- 明确组织整体目标，改变以往单点防御方式，让安全建设更加体系化。
- 提高人员安全意识，树立等级化防护思想，合理分配网络安全资源。

1.4.3 信息安全等级保护的划分细则

《信息安全等级保护管理办法》规定：国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合

法权益的危害程度等因素确定。《关于信息安全等级保护工作的实施意见》将信息系统的安全保护等级分为以下五级。

1. 第一级：自主保护级

适用于一般的信息和信息系统，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。第一级信息系统的运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

2. 第二级：指导保护级

适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。国家信息安全监管部门对该级信息系统安全等级保护工作进行指导。

3. 第三级：监督保护级

适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查。

4. 第四级：强制保护级

适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行强制监督、检查。

5. 第五级：专控保护级

适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，信息系统受到破坏后，会对国家安全造成特别严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查。

以上五级保护等级中，第一级为最低级，属于基本保护；第五级为最高级。第三、第四、第五级主要侧重于对社会秩序和公共利益的保护，虽然也涉及国家安全，但这类信息系统通常是涉密信息系统，必须实行分级保护，并且是强制执行的，而不是自主保护。

1.4.4 信息安全等级保护的基本要求

信息系统安全等级保护的基本要求是等级保护的核心，它建立了评价每个保护等级的指标体系，也是等级测评的依据。信息系统安全等级保护的基本要求包括基本技术要求和基本管理要求两个方面，体现了技术和管理并重的系统安全保护原则。不同等级的信息系统应具备的基本安全保护能力可分为如下四级。

1. 第一级

应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击，一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后能够恢复部分功能。

2. 第二级

应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击，一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后能够在一段时间内恢复部分功能。

3. 第三级

应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击，较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后能够较快恢复绝大部分功能。

4. 第四级

应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击，严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后能够迅速恢复所有功能。

信息系统安全等级保护应依据信息系统的安全保护等级情况保证它们具有相应等级的基本安全保护能力，不同安全保护等级的信息系统要求具有不同的安全保护能力。

基本安全要求是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求，根据实现方式的不同，基本安全要求分为基本技术要求和基本管理要求两大类。技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件产品并正确配置其安全功能来实现；管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出；基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出。基本技术要求和基本管理要求是确保信息系统安全的两个部分。

1.4.5 信息安全等级保护的工作流程

信息安全等级保护的工作流程包括以下5个步骤。

- **定级：**确定定级对象。初步确认定级对象，专家评审，主管部门审核，提交公安机关备案审查。
- **备案：**持定级报告、备案表等材料到当地公安机关网安部门备案。
- **建设整改：**参照信息系统当前等级要求和标准，对信息系统进行整改加固。

- **登记测评**：委托具备测评资质的测评机构对信息系统进行等级测评，形成正式的测评报告。
- **监督检查**：向当地公安机关网监部门提交测评报告，配合完成对信息安全等级保护实施情况的检查。

信息安全等级保护的测评方法有：

- **访谈**：通过引导信息系统相关方进行有目的（针对性）的交流，以帮助测评人员理解、澄清或取得证据的过程。
- **核查**：通过对测评对象（如制度文档、各类设备及相关安全配置等）进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。
- **测试**：使用预订的方法/工具使测评对象（各类设备或安全配置）产生特定的结果，将运行结果与预期结果进行比对的过程。

1.4.6 计算机信息系统安全等级保护标准

我国发布的计算机信息系统安全等级保护标准中，最主要的有以下几项重要内容。

1. GB 17859—1999《计算机信息系统安全保护等级划分准则》

该标准是建立计算机信息系统安全等级保护制度、实施安全等级管理的重要基础性标准，它将计算机信息系统安全保护能力划分为五个等级：用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级。

2. GA/T 390—2002《计算机信息系统安全等级保护通用技术要求》

该标准是计算机信息系统安全等级保护技术要求系列标准的基础性标准，用以指导设计者如何设计和实现具有所需要的安全等级的计算机信息系统。该标准主要说明了为实现GB 17859—1999中每一个保护等级的安全要求应采取的通用的安全技术，和为确保这些安全技术所实现的安全功能达到其应具有的安全性而采取的通用的保证措施。

3. GA/T 391—2002《计算机信息系统安全等级保护管理要求》

该标准中明确提出了管理层、物理层、网络层、系统层、应用层和运行层的安全管理要求，并将管理要求落实到GB 17859—1999的五个等级上，这样更有利于对安全管理的继承、理解和分工实施，更有利于对安全管理的评估和检查。

4. GA/T 387—2002《计算机信息系统安全等级保护网络技术要求》

该标准用以指导设计者如何设计和实现具有所需要的安全等级的网络系统，主要从对网络的安全保护等级进行划分的角度来说明其技术要求，即主要说明了为实现GB 17859—1999中每一个保护等级的安全要求对网络系统应采取的安全技术措施，以及各安全技术要求在不同安全级的具体实现上的差异。

5. GA/T 388—2002《计算机信息系统安全等级保护操作系统技术要求》

该标准用以指导设计者如何设计和实现具有所需要的安全等级的操作系统，主要从对操作系统的安全保护等级进行划分的角度来说明其技术要求。

6. GA/T 389—2002《计算机信息系统安全等级保护数据库管理系统技术要求》

该标准用以指导设计者如何设计和实现具有所需要的安全等级的数据库管理系统，主要从对数据库管理系统的安全保护等级进行划分的角度来说明其技术要求。

7. GB 17859—1999《计算机信息系统安全保护等级划分准则》

该标准划分了五个保护等级，安全保护能力随着安全保护等级的提高逐渐增强。

第一级：用户自主保护级；第二级：系统审计保护级；第三级：安全标记保护级；第四级：结构化保护级；第五级：访问验证保护级。保护能力项目与等级的关系如表1-1所示。

表 1-1 计算机信息系统安全保护等级划分

编号	保护能力项目	第一级	第二级	第三级	第四级	第五级
1	自主访问控制	✓	✓	✓	✓	✓
2	强制访问控制			✓	✓	✓
3	标记			✓	✓	✓
4	身份鉴别	✓	✓	✓	✓	✓
5	客体重用		✓	✓	✓	✓
6	审计		✓	✓	✓	✓
7	数据完整性	✓	✓	✓	✓	✓
8	隐蔽信道分析				✓	✓
9	可信路径				✓	✓
10	可信恢复					✓

8. GA/T 391—2002《计算机信息系统安全等级保护管理要求》

该标准指出，信息系统安全管理是对一个组织或机构中信息系统的生命周期全过程实施符合安全等级责任要求的科学管理，需要落实安全组织及安全管理人员，明确角色与职责，制定安全规划、开发安全策略、实施风险管理，制定业务持续性计划和灾难恢复计划，选择与实施安全措施，保证配置、变更的正确与安全，进行安全审计，保证维护支持，进行监控、检查、处理安全事件，安全意识与安全教育，人员安全管理等。

拓展阅读

《“十四五”国家信息化规划》中明确提出：全面加强网络安全保障体系和能力建设。加强网络安全核心技术联合攻关，开展高级威胁防护、态势感知、监测预警等关键技术研究，建立安全可控的网络安全软硬件防护体系。实施国家基础网络安全保障能力提升工程，加强关键信息基础设施安全防护体系建设，增强网络安全平台支撑能力，强化5G、工业互联网、大数据中心、车联网等安全保障。完善网络安全监测、通报预警、应急响应与处置机制，提升网络安全态势感知、事件分析以及快速恢复能力。

课后作业

一、单选题

1. 影响信息安全的主要因素不包括（　　）。

A. 人　　B. 访问控制

C. 技术　　D. 管理

2. 信息安全等级保护划分细则是根据（　　）。

A. 危害程度　　B. 行业

C. 从业者　　D. 信息数量

二、多选题

1. 信息保障的内容包括（　　）。

A. 保护　　B. 监测

C. 反应　　D. 恢复

2. 信息安全的目标包括（　　）。

A. 保密性　　B. 完整性

C. 可用性　　D. 复杂性

3. 信息安全等级保护的划分细则包括（　　）。

A. 自主保护级　　B. 指导保护级

C. 监督保护级　　D. 强制保护级

E. 专控保护级

三、简答题

1. 简述信息安全面临的各种威胁。
2. 简述信息安全等级保护的划分细则。
3. 简述信息安全等级保护的工作流程。