第1章

网络与信息安全概述

本章考点知识结构图如图 1-0-1 所示。

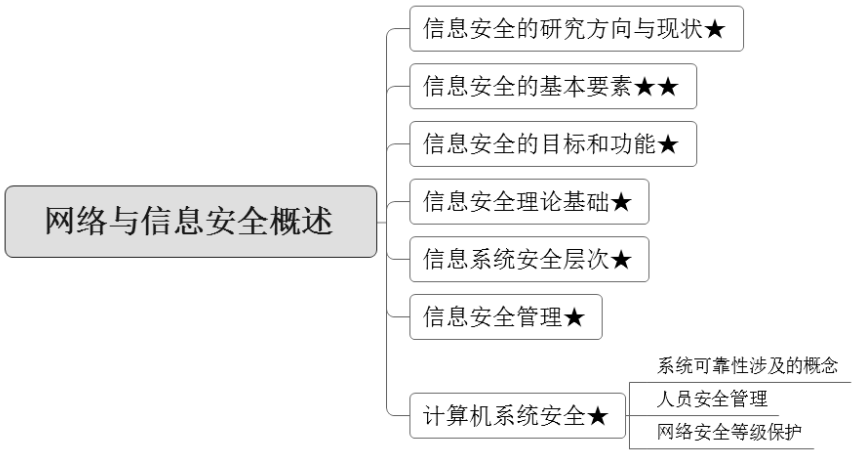

图 1-0-1　考点知识结构图

注：★号数量代表知识点的重要性，★越多代表知识点越重要。

例如：★代表零星考点，★★★★★代表非常重要的考点，下同。

1.1　信息安全的研究方向与现状

知识点综述

信息安全的研究方向包含密码学、网络安全、信息系统安全、信息内容安全、信息对抗等。

参考题型

- 网络空间安全的核心是_____。

A．信息安全　　B．信息处理　　C．信息传输　　D．信息存储

■ 试题分析　网络空间是所有信息系统的集合，网络空间安全的核心是信息安全。网络空间安全学科是研究信息的获取、存储、传输、处理等领域中信息安全保障问题的一门学科。

■ 参考答案　A

1.2　信息安全的基本要素

知识点综述

信息安全的基本要素主要包括机密性、完整性、可用性、可控性、可审查性等。扩展属性包括完整性、可用性、可控性等。虽然只是基本概念，但比较重要，基础知识与应用技术考试中都会涉及，考查的分值也不低。

参考题型

- 信息安全等级保护工作中，使用__（1）__三种属性即 C.I.A 划分信息系统的安全等级。

A．完整性、可用性、可控性

B．完整性、可用性、可审查性

C．可用性、可控性、可审查性

D．机密性、完整性、可用性

■ 试题分析　信息安全等级保护工作中，使用机密性、完整性、可用性三种属性划分信息系统的安全等级，这三个属性统称 C.I.A。

■ 参考答案　（1）D

- 网络信息不泄露给非授权的用户、实体或程序，能够防止非授权者获取信息的属性是指网络信息安全的__（2）__。

A．完整性　　B．机密性　　C．抗抵赖性　　D．隐私性

■ 试题分析

机密性：网络信息不泄露给非授权的用户、实体或程序，能够防止非授权者获取信息。

完整性：网络信息或系统未经授权不能进行更改的特性。

抗抵赖性：防止网络信息系统相关用户否认其活动行为的特性。

隐私性：有关个人的敏感信息不对外公开的安全属性。

■ 参考答案　（2）B

- 在信息安全防护体系设计中，保证“信息系统中数据不被非法修改、破坏、丢失等”是为了达到防护体系的__（3）__目标。

A．可用性　　B．保密性　　C．可控性　　D．完整性

■ 试题分析　保证“信息系统中数据不被非法修改、破坏、丢失等”是为了达到防护体系的

完整性目标。

■ 参考答案 （3）D

● 从安全属性对各种网络攻击进行分类，阻断攻击是针对__（4）__的攻击。

A．机密性　　B．可用性　　C．完整性　　D．真实性

■ 试题分析 阻断攻击是针对可用性的攻击。该攻击针对计算机或网络系统，使得其资源变得不可用或不能用。

■ 参考答案 （4）B

● 如果未经授权的实体得到了数据的访问权，这属于破坏了信息的__（5）__。

A．可用性　　B．完整性　　C．机密性　　D．可控性

■ 试题分析 机密性：保证信息不泄露给未经授权的进程或实体，只供授权者使用。

■ 参考答案 （5）C

● 确保信息仅被合法实体访问，而不被泄露给非授权的实体或供其利用的特性是指信息的__（6）__。

A．完整性　　B．可用性　　C．保密性　　D．不可抵赖性

■ 试题分析 保密性：信息仅被合法用户访问（浏览、阅读、打印等），不被泄露给非授权的用户、实体或过程。

■ 参考答案 （6）C

● 未授权的实体得到了数据的访问权，这属于安全的__（7）__。

A．机密性　　B．完整性　　C．合法性　　D．可用性

■ 试题分析 密码学的安全目标至少包含以下三个方面：

1）**保密性（Confidentiality）**：又称机密性，信息仅被合法用户访问（浏览、阅读、打印等），不被泄露给非授权的用户、实体或过程。

提高保密性的手段有：防侦察、防辐射、数据加密、物理保密等。

2）**完整性（Integrity）**：资源只有授权方或以授权的方式进行修改，所有资源没有授权则不能修改。保证数据完整性，就是保证数据不能被偶然或者蓄意地编辑（修改、插入、删除、排序）或者攻击（伪造、重放）。

影响完整性的因素有：故障、误码、攻击、病毒等。

3）**可用性（Availability）**：资源只有在适当的时候被授权方访问，并按需求使用。

保证可用性的手段有身份识别与确认、访问控制等。

■ 参考答案 （7）A

1.3 信息安全的目标和功能

知识点综述

网络安全的目标就是五个基本安全属性，即完整性、机密性、可用性、可控性、抗抵赖性。要实现网络安全的五个基本目标，网络应具备防御、监测、应急、恢复等基本功能。

参考题型

- 信息网络安全的基本功能中，_____的含义是针对突发安全事件、网络攻击所采取的安全措施。

A．监测　　B．防御　　C．监听　　D．恢复

■ **试题分析**　防御是针对突发安全事件、网络攻击所采取的安全措施；恢复是发生突发安全事件后，所采取的恢复网络、系统正常的措施。

■ **参考答案**　B

1.4　信息安全理论基础

知识点综述

信息安全理论基础包含的学科有：

（1）通用理论基础：包含数学、信息理论、计算理论。

（2）特有理论基础：包含访问控制理论、博弈论、密码学。

参考题型

- 1949 年，（1）发表了题为《保密系统的通信理论》的文章，为密码技术的研究奠定了理论基础，由此密码学成了一门科学。

A．Shannon　　B．Diffie　　C．Hellman　　D．Shamir

■ **试题分析**　《保密系统的通信理论》是香农（Claude Elwood Shannon）关于信息论的一篇著名论文。

■ **参考答案**　（1）A

- （2）的定义是，一些个人、团队、组织面对一定的环境条件，在一定的规则约束下，依靠掌握的信息，同时或先后，一次或多次，从各自允许选择的行为或策略进行选择并实施，并各自取得相应结果或收益的过程。

A．访问控制理论　　B．密码学　　C．博弈论　　D．信息学

■ **试题分析**　博弈论：一些个人、团队、组织面对一定的环境条件，在一定的规则约束下，依靠掌握的信息，同时或先后，一次或多次，从各自允许选择的行为或策略进行选择并实施，并各自取得相应结果或收益的过程。

访问控制理论：包含各种访问控制模型、授权理论。

密码学：研究编制密码和破译密码的技术科学。

信息学：研究信息的产生、获取、传输、处理、分类、识别、存储及利用的学科。

■ **参考答案**　（2）C

- 信息理论属于信息安全理论的通用理论基础，（3）不属于信息理论。

A．信息论　　B．控制论　　C．系统论　　D．博弈论

■ **试题分析**　信息理论包含信息论、控制论、系统论，不包含博弈论。

■ **参考答案**　（3）D

1.5 信息系统安全层次

知识点综述

信息系统安全层次可以划分为设备安全、数据安全、内容安全、行为安全四个层次。

参考题型

● 信息系统安全可以划分为四个层次。其中，设备稳定性表示设备在一定时间内不出故障的概率。则该性质应该属于信息系统安全层次中的（1）。

A．设备安全　　B．数据安全

C．内容安全　　D．行为安全

■ **试题分析**　信息系统安全可以划分为四个层次，具体见表 1-5-1。

表 1-5-1　信息系统安全层次

层次	属性	说明
设备安全	设备稳定性	设备一定时间内不出故障的概率
	设备可靠性	设备一定时间内正常运行的概率
	设备可用性	设备随时可以正常使用的概率
数据安全	数据秘密性	数据不被未授权方使用的属性
	数据完整性	数据保持真实与完整，不被篡改的属性
	数据可用性	数据随时可以正常使用的概率
内容安全	政治健康	略
	合法合规	
	符合道德规范	
行为安全	行为秘密性	行为的过程和结果是秘密的，不影响数据的秘密性
	行为完整性	行为的过程和结果可预期，不影响数据的完整性
	行为可控性	可及时发现、纠正、控制偏离预期的行为

■ **参考答案**　（1）A

● 行为秘密性表示行为的过程和结果是秘密的，不影响数据的秘密性。该属性属于信息系统安全层次中的（2）。

A．设备安全　　B．数据安全

C．内容安全　　D．行为安全

■ **试题分析**　行为秘密性表示行为的过程和结果是秘密的，不影响数据的秘密性。该属性属于信息系统安全层次中的行为安全。

■ **参考答案**　（2）D

1.6 信息安全管理

知识点综述

信息安全管理是信息安全管理方法、依据、流程、工具、评估等工作集合的总称。

信息安全管理要素包含：网络管理对象、网络脆弱性、网络威胁、网络风险、网络保护措施等。

参考题型

● 网络信息系统的整个生命周期包括：网络信息系统规划、网络信息系统设计、网络信息系统集成与实现、网络信息系统运行和维护、网络信息系统废弃 5 个阶段。网络信息安全管理重在过程，其中网络信息安全风险评估属于_____阶段。

A．网络信息系统规划　　B．网络信息系统设计

C．网络信息系统集成与实现　　D．网络信息系统运行和维护

■ **试题分析**　网络信息系统规划阶段包含的安全活动有网络信息安全风险评估、标识网络信息安全目标、标识网络信息安全需求。

■ **参考答案**　A

1.7 计算机系统安全

知识点综述

计算机系统安全是指为了保证计算机信息系统安全可靠运行，确保计算机信息系统在对信息进行采集、处理、传输、存储过程中，不受到人为（包括未授权使用计算机资源的人）或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境人员等采取适当的安全措施。

参考题型

● 人员安全管理是提高系统安全的最有效的一种手段。签订保密协议应该在人员安全管理的（1）时间段完成。

A．受聘前　　B．在聘中　　C．离职　　D．以上均可

■ 试题分析　人员安全管理按受聘前、在聘中、离职三个时间段来实施。其中，“在聘中”阶段内人员安全管理的措施包含签订保密协议，实施访问控制、进行定期考核和评价等。

■ **参考答案**　（1）B

● 容灾的目的和实质是（2）。

A．实现对系统数据的备份　　B．提升用户的安全预期

C．保持信息系统的业务持续性　　D．信息系统的必要补充

■ **试题分析**　容灾系统是指在相隔较远的异地，建立两套以上功能相同的系统，各系统之间相互监视健康状态便于进行切换，当一处系统因意外（如火灾、地震等）停止工作时，整个应用系