2018年11月全国计算机技术与软件专业技术资格(水平)考试

信息系统项目管理师*精讲班

21讲-信息安全管理

讲师：朱建军 （江山老师）
联系阿里旺旺：江山美人5788

信息系统安全管理

第 1 和 22 章：信息安全（4 分）

考点以及分值分布	05 上	05 下	06 下	07 下	08 上	08 下	09 上	09 下	10 上	10 下	11 上	11 下	12 上	12 下	13 上	13 下	14 上	14 下	15 上	15 下	16 上	16 下	17 上	17 下	18 上	18 下考点重要性
1、信息系统安全三维空间								1							1			1								★★
2、安全技术/加密数字签名					1																					★★★
3、安全属性：保密/完整性等				1			2	3								1	1			1						★★★
4、信息安全架构体系			1			1		1		1																★★★
5、病毒/木马/蠕虫													1													★
6、安全风险/威胁/脆弱性			1	1							1												1	1		★★
7、安全策略					1	1				1										1						★★
8、安全保护能力 5 个等级									1					1			1			1				1		★★★
9、典型的加密算法	3	3	1	1		1			1				1	2	1	1										★★★
10、信息安全体系				1		1			1										1							★★★
11、通信安全协议	2			1	1																					★★
12、防火墙	1	1					1								0.5							1		1		★★★
13、WLAN												1								1						★
14、X.509								1			1															★
15、访问控制/权限的方案				1							1							1	1		2	1				★★★
16、安全可信度等级													1													★
17、安全等级保护 5 级		1												1												★★★
18、安全审计/审计 Agent						1	1							1	1					1		1	1			★★★
19、入侵检测/网络攻击													1	1	0.5	1		1			2				1	★★★
20、密码等级																1										★★
21、安全风险评估																			1							★★
22、安全层次																								1		★
23、设备安全属性																									1	★★★
24、安全技术（签名/认证）																									1	★★★
25、网页防篡改技术																									1	★★★
23、其他		1	1						1	1													1			★★
总的分值	6	5	4	7	3	5	4	7	4	3	3	1	4	6	4	4	2	3	3	5	4	3	3	4	4	4 分

学习建议：信息安全知识点很杂，这些内容要注意理解，教程上的一些重点是必须掌握的，注意第一章 1.6 节新增的内容

信息系统安全管理

1、一个单位的安全策略一定是定制的，都是针对本单位的“安全风险（威胁）”进行防护的。（了解）

★2、安全策略的核心内容就是“七定”，即定方案、定岗、定位、定员、定目标、定制度、定工作流程。首先要解决定方案，其次就是定岗。（掌握）

3、把信息系统的安全目标定位于“系统永不停机、数据永不丢失、网络永不瘫痪、信息永不泄密”，是错误的，是不现实的，也是不可能的。（掌握）

4、木桶效应的观点是将整个信息系统比作一个木桶，其安全水平是由构成木桶的最短的那块木板决定的。（了解）

信息系统安全管理

★5、信息系统安全等级保护：（掌握）

分级	适用范围
第一级 用户自主保护级	普通内联网用户
第二级 系统审计保护级	通过内联网或国际网进行商务活动，需要保密的非重要单位
第三级 安全标记保护级	地方各级国家机关、金融单位机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位
第四级 结构化保护级	中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研单位机构和国防建设等
第五级 访问验证保护级	国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位

信息系统安全管理

★6、《信息安全等级保护管理办法》将信息系统安全保护等级分为5级：（掌握）

- 第一级（个人合法权益造成损害）；
- 第二级（个人合法权益严重损害，或社会利益遭到损害）；
- 第三级（公共利益造成严重损害或国家安全造成损害）；
- 第四级（公共利益造成特别严重损害国家安全造成严重损害）；
- 第五级（国家安全造成特别严重损害）。

7、信息系统安全策略设计8个总原则：①主要领导人负责原则②规范定级原则③依法行政原则④以人为本原则⑤注重效费比原则⑥全面防范、突出重点原则⑦系统、动态原则⑧特殊的安全管理原则（掌握）

★8、10个特殊原则：①分权制衡原则②最小特权原则③标准化原则④用成熟的先进技术原则⑤失效保护原则⑥普遍参与原则⑦职责分离原则（专人专职）⑧审计独立原则⑨控制社会影响原则

- 最小特权原则。对信息、信息系统的访问采用最小特权原则。（掌握）
- 职责分离原则。有条件的组织或机构，应执行专职专责。

信息系统安全管理

9、信息系统业界又叫作信息应用系统、信息应用管理系统、管理信息系统，简称MIS。信息安全系统不能脱离业务应用信息系统而存在（了解）

10、业务应用信息系统支撑业务运营的计算机应用信息系统，如银行柜台业务信息系统、国税征收信息系统等。（了解）

11、信息系统工程即建造信息系统的工程，包括两个独立且不可分割的部分，即信息安全系统工程和业务应用信息系统工程。（了解）

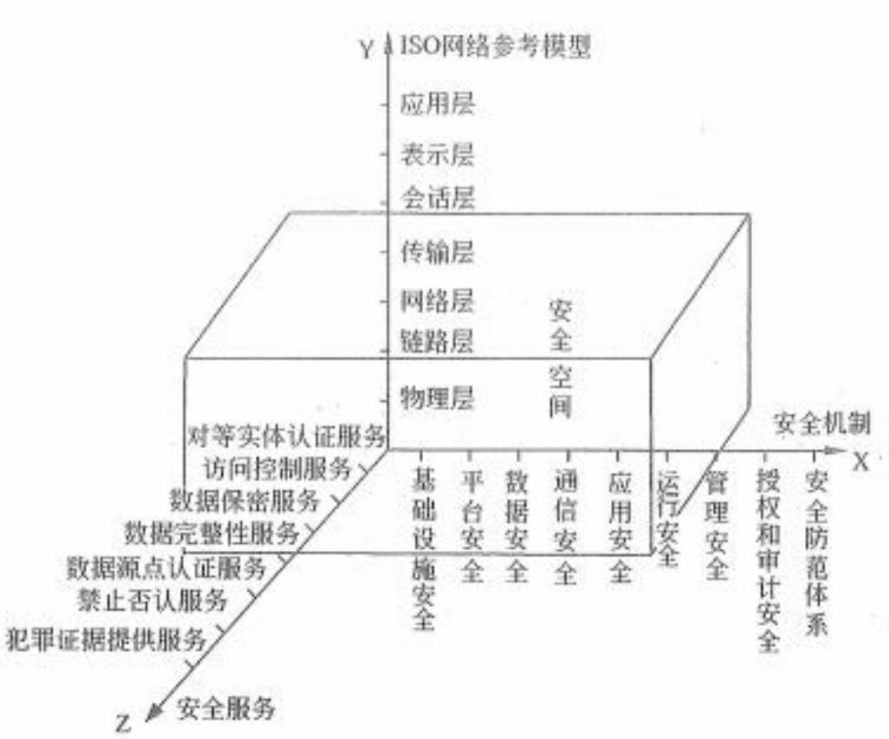
22.2信息安全系统工程

★1、信息安全系统三维空间：（掌握）

- X：安全机制（安全操作系统、安全数据库、应用开发运营）
- Y：OSI网络参考模型
- Z：安全服务（认证、权限、完整、加密、不可否认）

2、安全空间五大要素：认证、权限、完整、加密、不可否认。（掌握）

3、安全服务：①对等实体认证服务②数据保密服务③数据完整性服务④数据源点认证服务⑤禁止否认服务（掌握）



信息系统安全管理

★4、安全技术：①加密技术②数字签名技术③访问控制技术④数据完整性技术⑤认证技术（掌握）

- 数字签名可以确保电子文档的真实性并可以进行身份验证，以确认其内容是否被篡改后伪造。数字签名是确保电子文档真实性的技术手段。
- 加密是实现信息（可执行程序）保密性的方法，不能防病毒，只能防止未授权的人看到。一旦程序执行，还是可能感染病毒的。

信息系统安全管理

信息安全属性及目标：保密性、完整性、可用性、不可抵赖性

（1）保密性是指“信息不被泄漏给未授权的个人、实体和过程或不被其使用的特性。

- 保密技术如下：①最小授权原则②防暴露③信息加密④物理保密

（2）完整性是信息未经授权不能进行改变的特性。即应用系统的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、重放和插入等破坏和丢失的特性。

- 方法有：①协议②纠错编码方法③密码校验和方法④数字签名⑤公证

（3）可用性是应用系统信息可被授权实体访问并按需求使用的特性。即信息服务在需要时，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。

（4）不可抵赖性也称作不可否认性，在应用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。

信息系统安全管理

★5、信息安全保障三种架构：MIS+S（初级）、S-MIS（标准）、S2-MIS（超安全）（掌握）

架构	业务应用系统	软硬件	安全设备	适用场合
MIS+S	基本不变	通用	基本不带密码	一般应用系统
S-MIS	必须根本改变	通用	PKI/CA安全保障系统必须带密码；应用系统必须根本改变；主要的硬件和系统软件需要PKI/CA认证	一般电子商务、电子政务有安全保密要求的系统
S2-MIS	必须根本改变	专用		专用的安全保密系统

6、安全管理包括：①物理安全②计算机安全③网络安全④通信安全⑤输入/输出产品的安全⑥操作系统安全⑦数据库系统安全⑧数据安全⑨信息审计安全⑩人员安全⑪管理安全⑫辐射安全（了解）

7、信息安全系统工程能力成熟度模型（ISSE-CMM）主要概念（了解）

（1）过程（2）过程域（3）工作产品（4）过程能力。

8、ISSE将信息安全系统工程实施过程分解为：工程过程、风险过程和保证过程三个基本的部分（了解）

信息系统安全管理

★9、一个有害事件由威胁、脆弱性和影响三个部分组成。脆弱性包括可被威胁利用的资产性质。如果不存在脆弱性和威胁，则不存在有害事件，也就不存在风险。（掌握）（脆弱性是内部的，威胁是外部的）

10、公钥基础设施PKI是以不对称密钥加密技术为基础，以数据机密性、完整性、身份认证和行为不可抵赖性为安全目的，来实施和提供安全服务的具有普适性的安全基础设施。（了解）

11、数字证书：这是由认证机构经过数字签名后发给网上信息交易主体（企业或个人、设备或程序）的一段电子文档。数字证书提供了PKI的基础。（掌握）

12、认证中心：CA是PKI的核心。它是公正、权威、可信的第三方网上认证机构，负责数字证书的签发、撤销和生命周期的管理，还提供密钥管理和证书在线查询等服务。（掌握）

13、数字证书就是按照X.509标准制作的。X.509每一版本必须包含下列信息：①版本号②序列号③签名算法标识符④认证机构⑤有效期限⑥主题信息⑦认证机构的数字签名⑧公钥信息注意，没私钥（掌握）

14、CA是一个受信任的机构，为了当前和以后的事务处理，CA给个人、计算机设备和组织机构颁发证书，以证实它们的身份，并为他们使用证书的一切行为提供信誉的担保。（掌握）

22.4PMI权限（授权）管理基础设施

1、PMI主要进行授权管理，证明这个用户有什么权限，能干什么，即“你能做什么”。PKI主要进行身份鉴别，证明用户身份，即“你是谁”。它们之间的关系如同签证和护照的关系。签证具有属性类别，持有哪一类别的签证才能在该国家进行哪一类的活动。护照是身份证明，唯一标识个人信息，只有持有护照才能证明你是一个合法的人。（掌握）

★2、访问控制有两个重要过程。（掌握）

①认证过程，通过“鉴别（authentication）”检验主体的合法身份。

②授权管理，通过“授权（authorization）”赋予用户对某项资源的访问权限。

★3、访问控制机制分为强制访问控制（MAC）和自主访问控制（DAC）两种。

①强制访问控制：用户不能改变他们的安全级别或对象的安全属性。

②自主访问控制（DAC）机制允许对象的属主来制定针对该对象的保护策略。通常DAC通过授权列表（或访问控制列表）来限定哪些主体针对哪些客体可以执行什么操作。这样可以非常灵活地对策略进行调整。

★4、用户不能自主地将访问权限授给别的用户，这是RBAC与DAC的根本区别所在。RBAC与MAC的区别在于：MAC是基于多级安全需求的，而RBAC不是。（掌握）

5、基于角色的访问控制中，角色由应用系统的管理员定义。

★6、访问控制授权方案有4种：（掌握）

①DAC自主访问控制方式：该模型针对每个用户指明能够访问的资源，对于不在指定的资源列表中的对象不允许访问。

②ACL访问控制列表方式：目标资源拥有访问权限列表，指明允许哪些用户访问。如果某个用户不在访问控制列表中，则不允许该用户访问这个资源。

③MAC强制访问控制方式，访问者拥有包含等级列表的许可，其中定义了可以访问哪个级别的目标：例如允许访问秘密级信息，这时，秘密级、限制级和不保密级的信息是允许访问的，但机密和绝密级信息不允许访问。

④RBAC基于角色的访问控制方式：该模型首先定义一些组织内的角色，如局氏、科长、职员；再根据管理规定给这些角色分配相应的权限，最后对组织内的每个人根据具体业务和职位分配一个或多个角色。

22.5信息安全审计

★1、安全审计是记录、审查主体对客体进行访问和使用情况，保证安全规则被正确执行，并帮助分析安全事故产生的原因。（掌握）

2、安全审计系统采用数据挖掘和数据仓库技术，对历史数据进行分析、处理和追踪，实现在不同网络环境中终端对终端的监控和管理，必要时通过多种途径向管理员发出警告或自动采取排错措施。因此信息安全审计系统被形象地比喻为“黑匣子”和“监护神”。（掌握）

★3、安全审计系统属于安全管理类产品。安全审计产品主要包括主机类、网络类及数据库类和业务应用系统级的审计产品。各类安全审计系统可在日常运行、维护中，对整个计算机网络应用系统的安全进行主动分析及综合审计。（掌握）

信息系统安全管理

★4、安全审计系统主要作用：（掌握）

①对潜在的攻击者起到震慑或警告作用。

②对于已经发生的系统破坏行为提供有效的追究证据。

③为系统安全管理员提供有价值的系统使用日志，从而帮助系统安全管理员及时发现系统入侵行为或潜在的系统漏洞。

④为系统安全管理员提供系统运行的统计日志，使系统安全管理员能够发现系统性能上的不足或需要改进与加强的地方。

★5、审计分析分为潜在攻击分析、基于模板的异常检测、简单攻击试探和复杂攻击试探等（掌握）

★6、入侵监测和安全审计是一对因果关系，前者获取的记录结果是后者审核分析资料的来源，或者说前者是手段而后者是目的，任何一方都不能脱离另一方单独工作。作为一个完整的安全审计需要入侵监测系统实时、准确提供基于网络、主机（服务器、客户端）和应用系统的审核分析资料（掌握）

信息系统安全管理

★7、入侵监测是指为对计算机和网络资源上的恶意使用行为进行识别和响应的处理过程。它不仅检测来自外部的入侵行为，同时也检测内部用户的未授权活动。（掌握）

8、从安全审计的角度看，入侵检测采用的是以攻为守的策略，它所提供的数据不仅可用来发现合法用户是否滥用特权，还可以为追究入侵者法律责任提供有效证据。（掌握）

★9、分布式审计系统由审计中心、审计控制台和审计Agent组成。（了解）

★10、审计Agent可以分为网络监听型Agent、系统嵌入型Agent、主动信息获取型Agent等。（掌握）

11、网络安全审计可分为3种类型:系统级审计、应用级审计和用户级审计:

12、安全审计是信息系统审计基本业务中的一个（掌握）

练一练

【试题1】---2015下真题16

1、根据《信息安全等级保护管理办法》中的规定，信息系统的安全保护等级应当根据信息系统的国家安全、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险程度等因素确定。其中安全标记保护级处于（ ）

A. 第二级　　B. 第三级　　C. 第四级　　D. 第五级

【试题2】---2016上真题16

2、在信息系统安全保护中，依据安全策略控制用户对文件、数据库表等客体的访问属于（）安全管理。

A．安全审计　　B．入侵检测　　C．访问控制　　D．人员行为

练一练

【试题3】---2016下真题17

3、信息系统访问控制机制中，（）是指对所有主体和客体都分配安全标签用来标识所属的安全级别，然后在访问控制执行时对主体和客体的安全级别进行比较，确定本次访问是否合法的技术或方法。

A. 自主访问控制　　B. 强制访问控制

C. 基于角色的访问控制　　D. 基于组的访问控制

练一练

【试题4】---2016下真题18

4、以下关于信息系统审计的叙述中，不正确的是（）。

A. 信息系统审计是安全审计过程的核心部分

B. 信息系统审计的目的是评估并提供反馈、保证及建议

C. 信息系统审计师须了解规划、执行及完成市计工作的步骤与技术，外并尽量遵守国际信息系统审计与控制协会的一般公认信息系统审计准则、控制目标和其他法律与规定

D. 信息系统审计的目的可以是收集并评估证据以决定一个计算机系统（信息系统）是否有效做到保护资产、维护数据完整、完成组织目标

练一练

【试题5】---2017上真题18

5、安全审计（securityaudit）是通过测试公司信息系统对一套确定标准的符合程度来评估其安全性的系统方法，安全审计的主要作用不包括（）。

A. 对潜在的攻击者起到震慑或警告作用

B. 对已发生的系统破坏行为提供有效的追究证据

C. 通过提供日志，帮助系统管理员发现入侵行为或潜在漏洞

D. 通过性能测试，帮助系统管理员发现性能担缺陷或不足

1、B　2、C　3、B　4、A　5、D

NotifyMe

www.51kpm.com

915446173@qq.com

QQ: 915446173

联系老师
请随手@讲师：朱建军
or江山老师

http://www.51kpm.com QQ：915446173 notify me

@无忧考培教育学院 | @无忧教学 | @wuyoustor

全方位提升个人考试业务技能水准，助力您的职场钱景


作者答疑微信


官方公众号


知识分享公众号