2021年软考-高级信息系统项目管理师

基础精讲班

-22信息安全管理

讲师:朱建军（江山老师）

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	19 上	19 下	20 下	21 上考点重要性
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									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						1		1	★★
8、安全保护能力 5 个等级									1					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				1		★★★
13、WLAN/无线												1								1									1	★
14、X.509								1			1																			★
15、访问控制/权限的方案				1							1							1	1		2	1					1	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			1		1	1	★★★
19、入侵检测/网络攻击													1	1	0.5	1		1			2				1		1			★★★
20、密码等级																1														★★
21、安全风险评估																			1											★★
22、安全层次																								1			1	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		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	3	3	5	5	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

- **安全策略**
  - **定义**：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
  - **内容**：
    - “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
  - **策略**：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
- **木桶效应**：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

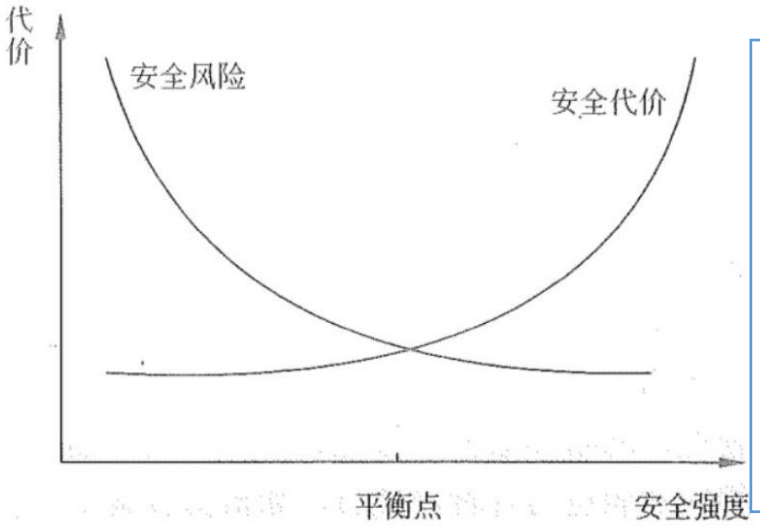


图 22-1　安全风险和安全代价之间关系

适度安全的观点：
一个好的信息安全保障系统的标志就是有效控制两者的“**平衡点**”，既能保证**安全风险**的有效控制，又使**安全代价**可以接受

木桶效应的观点：
✓安全水平由**最弱的安全要素**决定。
✓因此各安全要素同等重要，但需强调其中**安全管理**极为重要

信息系统安全等级保护

- 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部门
- 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

信息系统的安全保护等级

- 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或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

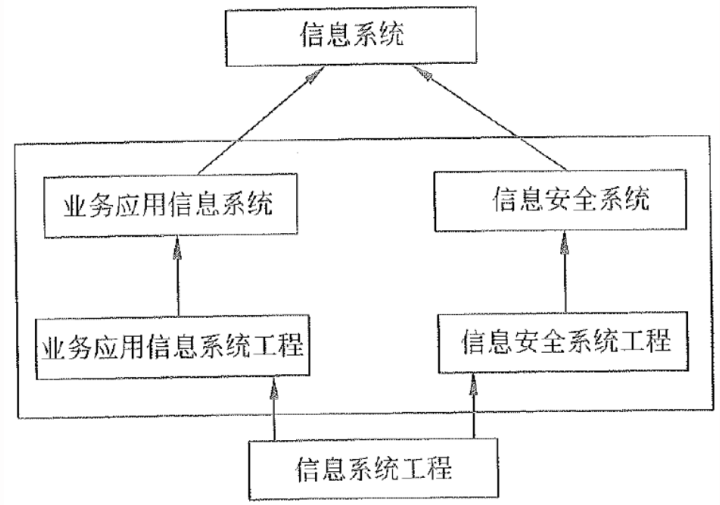
总结：（要按照顺序记住，适用于场合也要记住）
第一级：用户自主保护级----不损害国家安全、社会秩序和公共利益
第二级：系统审计保护级----对社会秩序和公共利益造成损害，但不损害国家安全
第三级：安全标记保护级----对国家安全造成损害
第四级：结构化保护级------对国家安全造成严重损害
第五级：访问验证保护级----对国家安全造成特别严重损害

受到破坏后受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	1级	2级	
社会秩序和公共利益	2级	3级	4级
国家安全	3级	4级	5级

信息系统的安全保护等级两个定级要素

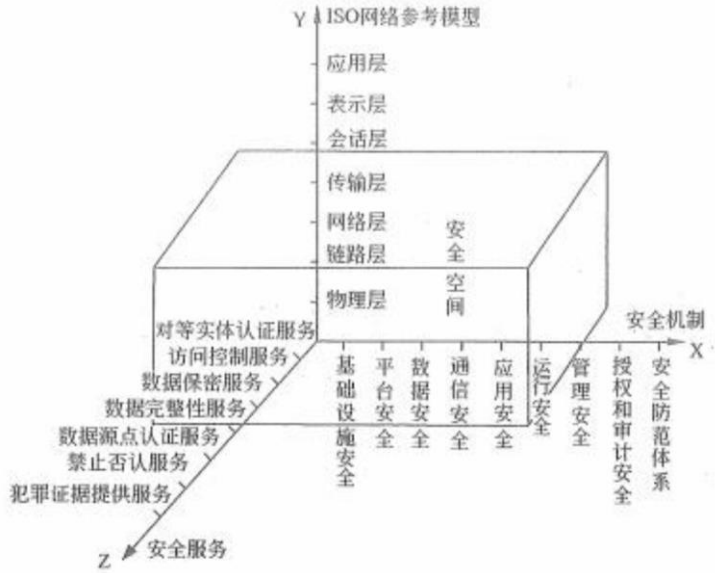
1. 等级保护对象受到破坏时所侵害的客体
2. 对客体造成侵害的程度

- 安全策略设计
  - 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
  - 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
  - ★其中
    - **最小特权原则** —— 对信息、信息系统的访问，不应享有任何多余特权
    - **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
  - 又叫作信息应用系统、信息应用管理系统、管理信息系统
  - 信息安全系统不能脱离业务应用信息系统而存在
- 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
- 信息系统工程
  - 建造信息系统的工程，包括两个独立且不可分割的部分
  - 信息安全系统工程和业务应用信息系统工程



信息安全系统三维空间

- 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（5大要素：**认证、权限、完整、加密、不可否认**）



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

安全技术

①加密技术 —— 实现信息（可执行程序）保密性的方法
②数字签名技术 —— 确保电子文档真实性的技术手段
③访问控制技术
④数据完整性技术
⑤认证技术 —— 站点认证、报文认证、用户和进程认证等

信息安全保障三种架构

- MIS+S（初级）
- S-MIS（标准）
- S2-MIS（超安全）

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

- 信息安全系统工程能力成熟度模型
  - 过程
  - 过程域
  - 工作产品
  - 过程能力
- 威胁、脆弱性
  - 脆弱性是内部的
  - 威胁是外部的
- 公钥基础设施PKI —— 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
- 数字证书
  - 由认证机构经过数字签名后发给网上信息交易主体的一段电子文档
  - 按照X.509标准制作的 —— 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**
- 认证中心
  - CA是PKI的核心
  - 是公正、权威、可信的第三方网上认证机构

表 22-5　PMI 与 PKI 比较

概　　念	PMI 实体	PKI 实体
证书	属性证书	公钥证书
证书签发者	属性证书管理中心	认证证书管理中心
证书用户	持有者	主体
证书绑定	持有者名和权限绑定	主体名和公钥绑定
撤销	属性证书撤销列表（ACRL）	证书撤销列表（CRL）
信任的根	权威源（SOA）	根 CA/信任锚
从属权威	属性管理中心 AA	子 CA
	你能做什么	你是谁
	“签证”	“护照”

- ★ PMI和PKI
  - PMI —— 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 —— 进行**身份鉴别**，证明用户身份，即“你是谁”

  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

- 问控制
  - ①认证过程 —— 通过鉴别来检验主体的合法身份
  - ②授权管理 —— 通过授权来赋予用户对某项资源的访问权限

- ★ 访问控制机制
  - 分类
    - ①强制访问控制MAC —— 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 —— 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
  - 区别
    - **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**
    - 基于角色的访问控制中，角色由**应用系统的管理员**定义

- ★ 访问控制授权方案
  - **①DAC自主访问控制方式** —— 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
    - 该模型是目前**应用最多**的方式
  - **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
    - 该模型在**军事和安全部门中应用较多**
  - **④RBAC基于角色的访问控制方式** —— 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

- 安全审计
  - 定义
    - 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
    - 属于安全管理类产品
    - 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
  - 内容
    - 1.采用网络监控与入侵防范系统，识别网络各种违规操作与攻击行为，即时响应(如报警）并进行阻断
    - 2.对信息内容和业务流程进行审计，可以防止内部机密或敏感信息的非法泄漏和单位资产的流失
  - 技术
    - 采用数据挖掘和数据仓库技术
    - 比喻为“黑匣子”和“监护神”
  - 作用
    - 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

- 安全审计功能
  - 1.自动响应功能：定义在被测事件指示出一个潜在的安全攻击时做出的**响应**，例如包括**实时报警的生成、违例进程的终止、中断服务、用户账号的失效**等。
  - 2.数据生成功能：要求记录与安全相关的事件的出现，包括**鉴别审计层次、列举可被审计的事件类型**，以及鉴别由各种审计记录类型提供的相关审计信息的最小集合
  - 3.分析 功能：
    - 定义了**分析**系统活动和审计数据来寻找可能的或真正的**安全违规操作**。它可以用于入侵检测或对安全违规的自动响应。
    - 分**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
  - 4.浏览 功能：要求审计系统能够使授权的用户有效地**浏览审计数据**，它包括审计浏览、有限审计浏览、可选审计浏览。
  - 5.事件选择功能：要求系统管理员能够维护、检查或修改审计事件的集合，能够**选择**对哪些安全属性进行审计
  - 6.事件存储功能：要求审计系统将提供控制措施；以防止由于资源的**不可用丢失**审计数据。能够创造、维护、访问它所保护的对象的审计踪迹，保护其不被修改、非授权访问或破坏

- ★ 入侵监测和安全审计
  - 特点：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
  - 关系
    - **任何一方都不能脱离另一方单独工作**
    - 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
  - 入侵监测
    - 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
    - **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**
    - 采用的是以攻为守的策略
    - 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
- 分布式审计系统：由审计中心、审计控制台和审计Agent组成
- ★ 审计Agent
  1. **网络监听型Agent**
  2. **系统嵌入型Agent**
  3. **主动信息获取型Agent**
- ★ 安全审计
  - 系统级审计
  - 应用级审计
  - 用户级审计

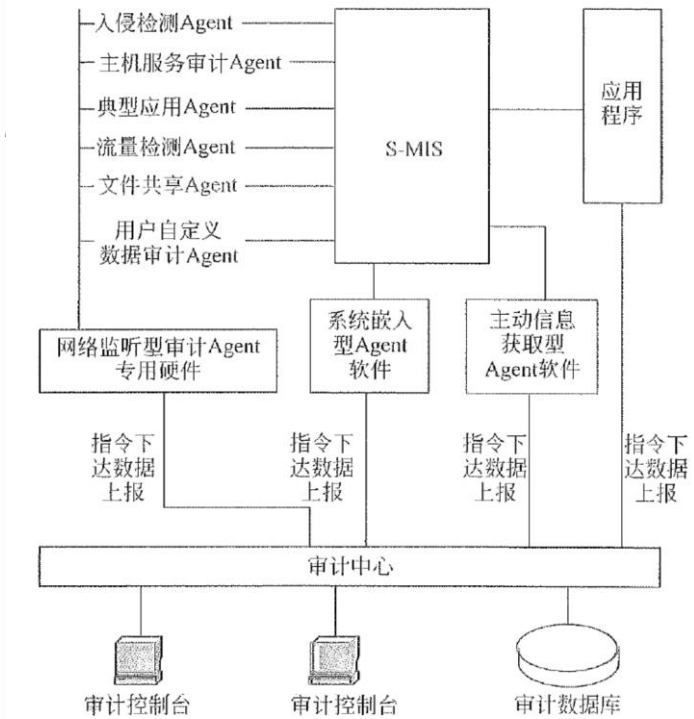


图 22-26　网络安全审计系统结构如

练一练

【例1-15下】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

【例2-16上】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

【例3-16下】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.基于组件的访问控制

练一练

【例4-16下】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

【例5-17上】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

练一练

【例6-18下】按照信息系统安全策略“七定”要求，系统安全策略首先需要（）。

A.定方案　B.定岗　C.定目标　D.定工作流程

【例7-18下】《计算机信息系统安全保护等级划分准则》将计算机信息系统分为5个安全保护等级。其中（）适用于中央级国家机关、广播电视部门、重要物资储备单位等部门。

A.系统审计保护级　B.安全标记保护级　C.结构化保护级　D.访问验证保护级

【例8-18下】CC（即Common Critoria ISO/IEC17859）标谁将安全审计功能分为6个部分，其中（）要求审计系统提供控制措施，以防止由于资源的不可用失去审计数据。

A.安全审计数据生成功能　B.安全审计浏览功能

C.安全审计事件选择功能　D.安全审计事件存储功能

【例9-19下】信息系统安全保护等级的定级要素是（）。

A.等级保护对象和保护客体　B.受侵害的客体和对客体的侵害程度

C.信息安全技术策略和管理策略　D.受侵害各体的规模和恢复能力

练一练

【例10-19下】（）在军事和安全部门中应用最多。

A.自主访问控制方式（DAC） B.强制访问控制方式（MAC）

C.访问控制列表方式（ACL） D.基于角色的访问控制方式（PBAC）

【例11-19下】（）的目标是防止内部机密或敏感信息非法泄露和资产的流失。

A.数字证书 B.安全审计 C.入侵检测 D.访问控制

【例12-20下】按照系统安全策略“七定”要求,系统安全策略首先要（）。

A.定员 B.定制度 C.定方案 D.定岗

【例13-20下】（）方式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。

A.自主访问控制 B.基于策略的访问控制 C.强制访问控制 D.基于角色的访问控制

【例14-20下】ISO/IEC17859标准将安全审计功能分为6个部分,其中,（）通过分析系统活动和审计数据,寻找可能的或真正的安全违规操作,可以用于入侵检测或安全违规的自动响应。

A.安全审计事件存储功能 B.安全审计数据生成功能 C.安全审计分析功能 D.安全审计浏览功能

参考答案

1	2	3	4	5	6	7	8	9	10
B	C	B	A	D	A	C	D	B	B
11	12	13	14	15	16	17	18	19	20
B	C	A	C						

非常感谢您的聆听

加入正版课程获得VIP全套增值服务

问题咨询联系江山老师 QQ/微信：51815498 /915446173

江山老师答疑微信

官方公众号

备份公众号

扫一扫
加关注
抢先学
早拿证

微信扫码做题