2019年11月

信息系统项目管理师

辅导班课程

马军老师

22.1 信息系统安全策略

22.1.1 信息系统安全策略的概念与内容

1、信息系统安全策略是指针对本单位的计算机业务应用信息系统的安全风险（安全威胁）进行有效的识别、评估后，所采取的各种措施、手段，以及建立的各种管理制度、规章等。由此可见，一个单位的安全策略一定是定制的，都是针对本单位的

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。

22.1.2 建立安全策略需要处理好的关系

1、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。

2、计算机信息系统分为以下5个安全保护等级。

第一级用户自主保护级。通过隔离用户与数据，使用户具备自主安全保护的能力。它为用户提供可行的手段，保护用户和用户信息，避免其他用户对数据的非法读写与破坏，该级适用于普通内联网用户。

第二级系统审计保护级。实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。该级适用于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。具有系统审计保护级的所有功能。此外，还需提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述，具有准确地标记输出信息的能力；消除通过测试发现的任何错误。该级适用于地方各级国家机关、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。建立于一个明确定义的形式安全策略模型之上，要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算机的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。该级适用于中央级国家机关、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。满足访问控制器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算机在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和现实时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。该级适用于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。

3、信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

一是受侵害的客体。等级保护对象受到破坏时所侵害的客体包括公民、法人和其他组织的合法权益；社会秩序、公共利益；国家安全。

二是对客体的侵害程度。对客体的侵害程度由客观方面的不同外在表现综合决定。

22.1.3 信息系统安全策略设计原则

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（8）审计独立原则（9）控制社会影响原则（10）保护资源和效率原则。

22.1.4信息系统安全方案

无重要考点，大家有兴趣的话可以自己读下课本。

22.2 信息安全系统工程

22.2.1 信息安全系统工程概述

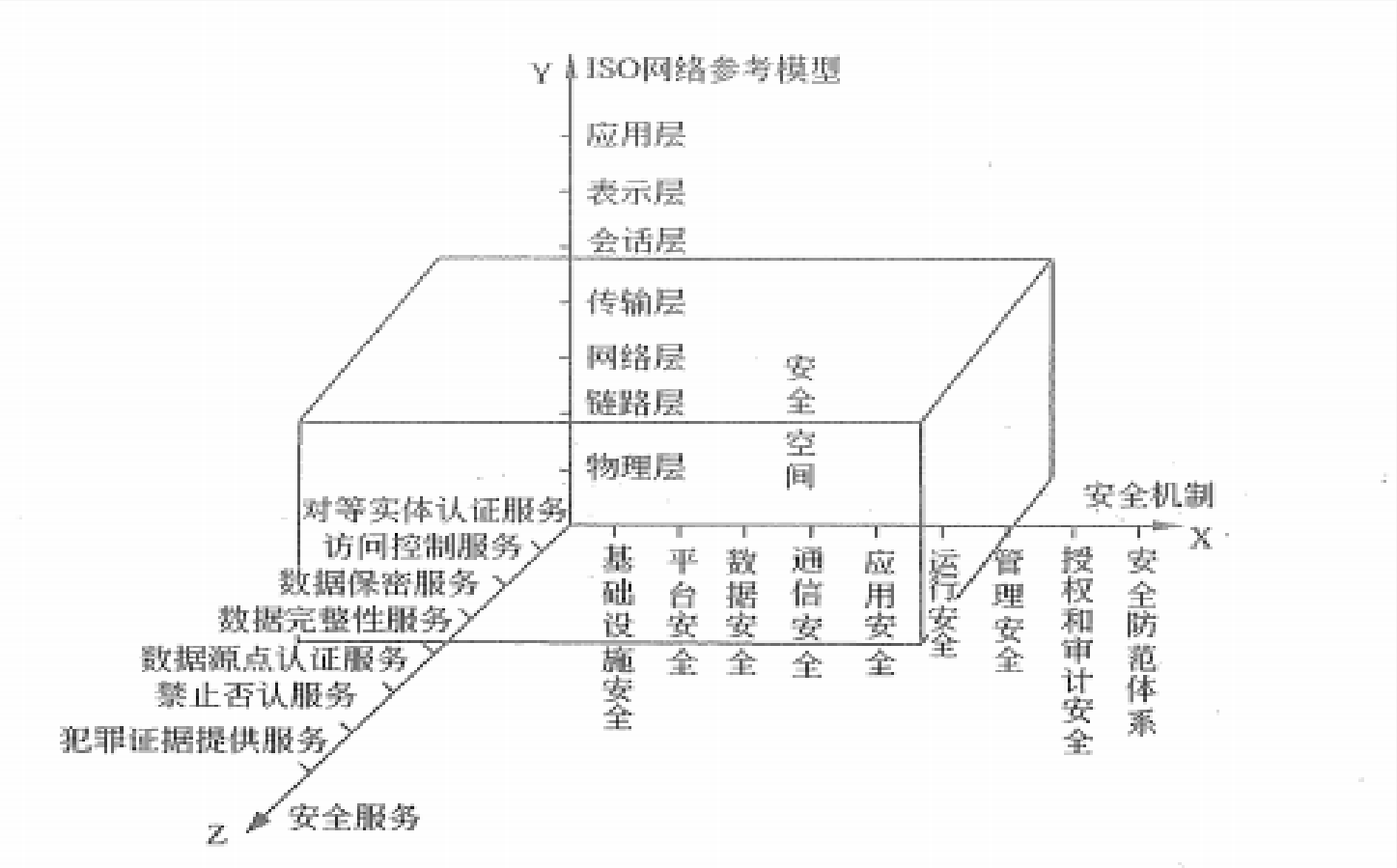
1、信息系统业界又叫作信息应用系统、信息应用管理系统、管理信息系统，简称MIS。信息安全系统不能脱离业务应用信息系统而存在

2、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。

3、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。

22.2.2 信息安全系统

1、三维模型


Y
ISO网络参考模型
应用层
表示层
会话层
传输层
网络层
链路层
物理层
安全空间
安全机制
X
对等实体认证服务
访问控制服务
数据保密服务
数据完整性服务
数据源点认证服务
禁止否认服务
犯罪证据提供服务
Z
安全服务
基础设施安全
平台安全
数据安全
通信安全
应用安全
运行安全
管理安全
授权和审计安全
安全防范体系

2、X轴是“安全机制”，Y轴是“OSI网络参考模型”，Z轴是“安全服务”。由X、Y、Z三个轴形成的信息安全系统三维空间就是信息系统的“安全空间”。 随着网络逐层扩展，这个空间不仅范围逐步加大，安全的内涵也就更丰富，达到具有认证、权限、完整、加密和不可否认五大要素，也叫作“安全空间”的五大属性。

3、安全服务

（1）对等实体认证服务。对对方实体的合法性、真实性进行确认，以防假冒。

（2）数据保密服务。

（3）数据完整性服务。数据完整性服务用以防止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

（4）数据源点认证服务。数据源点认证服务用于确保数据发自真正的源点，防止假冒。

（5）禁止否认服务。

（6）犯罪证据提供服务。

22.2.3 信息安全系统架构体系

1、信息安全系统大体划分为三种架构体系:MIS+S系统、S-MIS系统和S2-MIS系统。

2、MIS+S系统为初级信息安全保障系统” 或“基本信息安全保障系统”。其特点如下。

（1）业务应用系统基本不变。

（2）硬件和系统软件通用。

（3）安全设备基本不带密码。

3、S-MIS系统为“标准信息安全保障系统”。其特点如下：
（1）硬件和系统软件通用。
（2）PKI/CA安全保障系统必须带密码。
（3）业务应用系统必须根本改变。
（4）主要的通用的硬件、软件也要通过PKI/CA认证。
4、S2-MIS系统为“超安全的信息安 全保障系统”。其特点如下。
（1）硬件和系统软件都专用。
（2）PKI/CA安全基础设施必须带密码。
（3）业务应用系统必须根本改变。

22.2.4 信息安全系统工程基础

无重要考点，大家有兴趣的话可以读下课本。

22.2.5 信息安全系统工程体系结构

1、信息安全系统工程能力成熟度模型（ISSE-CMM）主要用于指导信息安全系统工程的完善和改进，使信息安全系统工程成为一个清晰定义的、成熟的、可管理的、可控制的、有效的和可度量的学科。
2、ISSE-CMM主要概念
（1）过程。是指为了达到某一给定目标而执行的一系列活动，这些活动可以重复、递归和并发地执行。
（2）过程域。是由一些基本实施组成的，它们共同实施来达到该过程域规定的目标。

（3）工作产品。
（4）过程能力。
3、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
4、信息安全系统工程与其他工程活动一样，是一个包括概念、设计、实现、测试、部署、运行、维护、退出的完整过程
5、一个有害事件由威胁、脆弱性和影响三个部分组成

22.3 PKI 公开密钥基础设施

22.3.1 公钥基础设施（PKI）基本概念

1、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。
2、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。
3、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。
4、每一个版本的X.509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

22.3.2 数字证书及其生命周期

1、PKI/CA对数字证书的管理是按照数字证书的生命周期实施的，包括证书的安全需求确定、证书申请、证书登记、分发、审计、撤回和更新。

2、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。

22.3.3 信任模型

无重要考点，大家有兴趣的话可以读下课本。

22.3.4 应用模式

无重要考点，大家有兴趣的话可以读下课本。

22.4 PMI权限（授权）管理基础设施

PMI 即权限管理基础设施或授权管理基础设施。PMI授权技术的核心思想是以资源管理为核心，将对资源的访问控制权统一交由授权机构进行管理，即由资源的所有者来进行访问控制管理。

22.4.1PMI和PKI的区别

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”。

2、下表看看

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

22.4.2 属性证书定义

无重要考点，大家有兴趣的话可以读下课本。

22.4.3 访问控制

1、访问控制是为了限制访问主体（或称为发起者，是一个主动的实体，如用户、进程、服务等）对访问客体（需要保护的资源）的访问权限；从而使计算机信息应用系统在合法范围内使用；访问控制机制决定用户以及代表一定用户利益的程序能做什么及做到什么程度。

2、访问控制有两个重要过程。

（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。

22.4.4 基于角色的访问控制

无重要考点，大家有兴趣的话可以读下课本。

22.4.5 PMI支撑体系

目前我们使用的访问控制授权方案，主要有以下4种。

（1）DAC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。

（2）ACL访问控制列表方式：该模型是目前应用最多的方式。 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。

（3）MAC强制访问控制方式，该模型在军事和安全部门中应用较多，目标具有一个包含等级的安全标签（如：不保密、限制、秘密、机密、 绝密）；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。

（4）RBAC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，如局长、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。

22.4.6 PMI实施

无重要考点，大家有兴趣的话可以读下课本。

22.5 信息安全审计

22.5.1 安全审计概念

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。

2、安全审计具体包括两方面的内容。

（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。

3、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”。

（1）信息安全审计系统就是业务应用信息系统的“黑匣子”。即使在整个系统遭到灭顶之灾的破坏后，“黑匣子”也能安然无恙，并确切记录破坏系统的各种痕迹和“现场记录”。

（2）信息安全审计系统就是业务应用信息系统的“监护神”，随时对一切现行的犯罪行为、违法行为进行监视、追踪、抓捕，同时对暗藏的、隐患的犯罪倾向、违法迹象进行“堵漏”、铲除。

4、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。

5、一个安全审计系统，主要有以下作用。

（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。

6、网络安全审计的具体内容如下。

（1）监控网络内部的用户活动。

（2）侦察系统中存在的潜在威胁。

（3）对日常运行状况的统计和分析。

（4）对突发案件和异常事件的事后分析。

（5）辅助侦破和取证。

22.5.2 建立安全审计系统

1、网络安全入侵监测预警系统基本功能是负责监视网络上的通信数据流和网络服务器系统中的审核信息，捕捉可疑的网络和服务器系统活动，发现其中存在的安全问题，当网络和主机被非法使用或破坏时，进行实时响应和报警；产生通告信息和日志，系统审计管理人员根据这些通告信息、日志和分析结果，调整和更新已有的安全管理策略或进行跟踪追查等事后处理措施。所以，在这个层次上的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。

2、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。

3、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。

4、从已知的现有技术分析，主要有4种解决方案。

1) 基于主机操作系统代理
2) 基于应用系统代理
3) 基于应用系统独立程序
4) 基于网络旁路监控方式

22.5.3分布式审计系统

1、分布式审计系统由审计中心、审计控制台和审计Agent组成。

2、审计中心：是对整个审计系统的数据进行集中存储和管理，并进行应急响应的专用软件，它基于数据库平台，采用数据库方式进行审计数据管理和系统控制，并在无人看守情况下长期运行。
3、审计控制台：是提供给管理员用于对审计数据进行查阅，对审计系统进行规则设置，实现报警功能的界面软件，可以有多个审计控制台软件同时运行。
4、审计Agent是直接同被审计网络和系统连接的部件，不同的审计Agent完成不同的功能。审计Agent将报警数据和需要记录的数据自动报送到审计中心，并由审计中心进行统一的调度管理。审计Agent主要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。

补充建议学的考点：
1、保密性：应用系统常用的保密技术如下：最小授权原则、防暴露、信息加密、物理保密
2、完整性：保障应用系统完整性的主要方法如下：协议、纠错编码方法、密码校验和方法、数字签名、公证
3、系统运行安全按粒度从粗到细的排序是：系统级安全、资源访问安全、功能性安全、数据域安全。
4、安全等级可分为保密等级和可靠性等级两种，系统的保密等级与可靠性等级可以不同。保密等级应按有关规定划为绝密、机密和秘密。可靠性等级可分为三级，对可靠性要求最高的为A级，系统运行所要求的最低限度可靠性为C级，介于中间的为B级。安全等级管理就是根据信息的保密性及可靠性要求采取相应的控制措施，以保证应用系统及数据在既定的约束条件下合理合法的使用。
5、使用防病毒软件、日志审计系统、入侵检测系统有助于发现、防止内部攻击，并发现攻击细节，为证据查找和修补系统提供帮助。防火墙也是一种非常重要的网络安全工具，但是它能够防止外部对内部的攻击，对于网络内部发生的攻击事件而无能为力。

6、在信息安全技术体系中，数字签名技术用于防止信息抵赖，加密技术用于防止信息被窃取，完整性技术用于防止信息被篡改，认证技术用于防止信息被假冒。

7、防火墙是指建立在内外网络边界上的过滤封锁机制。内部网络被认为是安全和可信的，而外部网络则被认为是不安全和不可信赖的，通过防火墙，防止不希望的、未经授权的通信进出内部网络，是一种被动技术，对内部的非法访问难以有效地控制。

一般情况下，防火墙网络可以划分为三个不同级别的安全区域：

（1）内部网络：包括全部的企业内部网络设备及用户主机，是防火墙要的可信区域

（2）外部网络：包括外部因特网主机和设备，这个区域为防火墙的

（3）DMZ（非军事区）：包括内部网络中用于公众服务的外部服务器，如Web服务器、邮件服务器和外部DNS服务器等

代理服务型防火墙，代表某个专用网络同互联网进行通讯的防火墙。当你将浏览器配置成使用代理功能时，防火墙就将你的浏览器的请求转给互联网；当互联网返回响应时，代理服务器再把它转给你的浏览器。代理服务器也用于页面的缓存，代理服务器在从互联网上下载特定页面前先从缓存器取出这些页面。使用代理服务型防火墙，内部网络与外部网络之间不存在直接连接。

8、DoS是一种利用合理的服务请求占用过多的服务资源，从而使合法用户无法得到服务响应的网络攻击行为，导致网络系统不可用，就是拒绝服务。

9、在MAC地址过滤、WEP、WAP和WAP2等几种无线加密方式中，WAP2最安全。

10、堡垒主机既然是一台完全暴露给外网的主机，那肯定是不需要防火墙来保护了的。它没有任何防火墙或者包过虑路由器设备保护。（了解）

上节考点回顾

1、项目组合管理是一个保证组织内所有项目都经过风险和收益分析及平衡的方法论。作为公司的项目经理进行项目组合管理时，（50）应是重点考虑的要素。

A、资源利用效率　　B、项目进度控制　　C、范围变更　　D、项目质量

2、DIPP分析法可用于对处在不同阶段的项目进行比较，同时可以表明项目的资源利用情况DIPP=EMV/ETC。如果有A、B、C、D四个项目，项目初期的DIPP值分别为：DIPP(A)=0.9、DIPP(B)=1.3、DIPP (C)=0.8、DIPP(D)=1.2，则优先选择的项目为（51）。

A、项目A　　B、项目B　　C、项目C　　D、项目D

3、在组织级项目管理中，要求项目组合、项目集、项目三者都要与（51）保持一致，其中，（52）通过设定优先级并提供必要的资源的方式进行项目选择，保证组织内所有项目都经过风险和收益分析

A、组织管理　　B、组织战略　　C、组织文化　　D、组织投资

A、项目组合　　B、项目集　　C、项目　　D、大项目

4、项目经理张工管理着公司的多个项目，在平时工作中，需要不时地与上层领导或其他职能部门进行沟通，通过学习项目管理知识，张工建议公司成立一个（53）进行集中管理。

A、组织级质量管理部门　　B、变更控制委员会

C、大项目事业部　　D、项目管理办公室

5、项目组合管理实施的主要过程不包括（61）。

A. 评估项目组合管理战略计划

B. 定义项目组合管理的愿景和计划

C. 实施项目组合管理过程

D. 改进项目组合管理过程

感谢您的聆听