# 第 1 7 章 、 信 息 安 全 管 理

**考** **点** **1** **3** **3** **:** **信** **息** **安** **全** **的** **属** **性**

**1、信息安全属性及目标**

信息安全属性及目标**：** **保密性、完整性、可用性、不可抵赖性**(09上21)(09下24)(09下25)(11



下 2**4)(12下25)(16上24)**

**(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。( 1 5 下 2 2 )

应用系统常用的保密技术如下： 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。( 1 8 上 2 1 )

保障应用系统完整性主要方法如下： 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( 1 7 上



**68)(19下68)**

**(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，或者是网络部分曼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。

**考** **点** **1** **3** **4** **:** **信** **息** **安** **全** **技** **术** **体** **系**

+ 1、信息安全技术体系：(1)物理安全(2)运行安全-安全审计(3)数据安全(12下26)(14上29)(18下69)

◆ **应用安全**是保障相关业务在计算机网络系统是安全运行，应用安全脆弱性是可能给信息化系统带来最大 损失的致命威胁，主要针对应用程序或工其在使用过程中可能出现计算、传输数据的泄密和失窃提供安 全保护措施。( 1 5 上 2 6 )

◆ 数据安全是保护在存储、操作和处理中的数据

◆ 介质安全主要用来保护存储介质，包括移动硬盘、软盘、 U 盘、磁带等

◆ 物理安全 侧重于保护建筑物和物理场所的安全



**考点** **1** **3** **5** **:** **物理安全管理**

**2.电源**

根据对机房安全保护的不同要求，机房供、配电分为如下几种。( 1 0 上 2 4 )

**②紧急供电：配置抗电压不足的基本设备、改进设备或更强设备，如基本ups,改进的UPS、多级UPS** **和应急电源(发电机组)等**

**④稳压供电：采用线路稳压器，防止电压波动对计算机系统的影响**

**⑥不间断供电：采用不间断供电电源，防止电压波动、电器干扰和断电等对计算机系统的不良影响**

**3.计算机设备**

(1)设备的防盗和防毁。

**①设备标记要求：计算机系统的设备和部件应有明显的无法去除的标记，以防更换和方便查找赃物。**(10



**上25)**

—147—

② 计算中心防盗。

◇ 计算中心应安装妨盗报警装置，防止从门窗进入的盗窃行为。

◇ 计算中心应利用光、电、无源红外等技术设置机房报警系统，并由专人值守，防止从门窗进入的斑窃行为。

◇ 利用闭路电视系统对计算中心的各重要部位进行监视，并有专人值守，防止从门窗进入的盗窃行为。

(3)机房外部设备防盗； **机房外部的设备，应采取加固防护等措施，**必要时安排专人看管，以防止盗

窃和破坏。

**人员进出机房和操作权限范围控制：(** **1** **0** **下** **3** **4** **)**

应明确机房安全管理的责任人，机房出入应有指定人员负责，未经允许的人员不准进入机房；获准进入 机房的来访人员，其活动范围应受限制，并有接待人员陪同；机房钥匙由专人管理，未经批准，不准任何人 私自复制机房钥匙或服务器开机钥匙；没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保 护品均不准带出机房，与工作无关的物品均不准带入机房；机房内严禁吸烟及带入火种和水源。

应要求所有来访人员经过正式批准，登记记录应妥善保存以备查；获准进入机房的人员， 一般应禁止携 带个人计算机等电子设备进入机房，其活动范围和操作行为应受到限制，并有机房接待人员负责和陪同。

① **机房和重要的记录介质存放间，其建筑材料的耐火等级**，应符合规定的二级耐火等级；机房相关的其 余基本工作房间和辅助房，其建筑材料的耐火等级**应不低于二级防火等级。**

吊顶上和活动地板下设置火灾自动探测器，通常有两种方式。 一种方式是均匀布置，但密度要提高， 每个探测器的保护面积为 10-15 m²。另一种方式是在易燃物附近或有可能引起火灾的部位以及回风口等处设

**置探测器。**

**2.防漏水和水灾**

由于计算机系统使用电源，因此水对计算机也是致命的威胁，它可以导致计算机设备短路，从而损害设 备。所以，对机房必须采取防水措施。机房的防水措施应考虑如下几个方面。

① 与主机房无关的给排水管道不得穿过主机房。

②主机房内如设有地漏，地漏下应加设水封装置，并有防止水封破坏的措施。

(3)机房内的设备需要用水时,**其给排水干管应暗敷，引入支管宜暗装。**管道穿过主机房墙壁和楼板

处，应设置套管，管道与套管之间应采取可靠的密封措施。

④机房不宜设置在用水设备的下层。

⑤ 机房房顶和吊顶应有防渗水措施。

⑥安装排水地漏处的楼地面应低于机房内的其他楼地面。

机房隔壁不能为卫生间或水房，因为漏水等情况会对机房造成损害，**同时机房肯定不能用水来灭火了**



**(15下25)**

**3.防静电**

**主机房内绝缘体的静电电位不应大于1kv**

对需要防止**电磁泄露的**计算机设备应配备电磁于扰设备，在被保护的计算机设备工作时电磁于扰设备不 准关机；必要时可以采用屏蔽机房。屏蔽机房应随时关闭屏蔽门； **不得在屏蔽墙上打钉钻孔，不得在波导管** **以外或不经过过滤器对屏蔽机房内外连接任何线缆**；应经常测试屏蔽机房的泄露情况并进行必要的维护。

主机房、基本工作间**应设卤代烷灭火系统**

■ 主机房宜采用感烟探测器，可在主机柜、磁盘机和宽行打印机附件安装探测器。空调设备应考虑在回**风** **口附近**安装探测器。



**考点** **1** **3** **6** **:** **人员** **安** **全** **管** **理**

**对信息系统岗位人员的管理，应根据其关键程度建立相应的管理要求。(** **14上27)(18上69)(19上70)**



**(19下69)**

(1)对安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员和 重要业务应用操作人员等信息系统关键岗位人员进行统一管理； 允许一人多岗，但业务应用操作人员不能由 其他关键岗位人员兼任；关键岗位人员应定期接受安全培训，加强安全意识和风险防范意识。

(2)兼职和轮岗要求：业务开发人员和系统维护人员不能兼任或担负安全管理员、系统管理员、数据 库管理员、网络管理员和重要业务应用操作人员等岗位或工作：必要时关键岗位人员应采取定期轮岗制度。

(3)权限分散要求：在上述基础上，应坚持关键岗位“权限分散、不得交叉覆盖”的原则， 系统管理员 数据库管理员、网络管理员不能相互兼任岗位或工作。

(4)多人共管要求：在上述基础上，关键岗位人员处理重要事务或操作时，应保持二人同时在场，关 键事务应多人共管。

(5)全面控制要求：在上述基础上，应采取对内部人员全面控制的安全保证措施，对所有岗位工作人 员实施全面安全管理。

**对人员离岗的管理，可以根据离岗人员的关键程度，采取下列控制措施。**

(1)基本要求：立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限；收回所 有相关证件、徽章、密钥和访问控制标记等；收回机构提供的设备等。

(2)调离后的保密要求：在上述基础上，管理层和信息系统关键岗位人员调离岗位，必须经单位人事 部门严格办理调离手续，承诺其调离后的保密要求。

(3)离岗的审计要求：在上述基础上，设计组织机构管理层和信息系统关键岗位的人员调离单位，必 须进行离岗安全审查，在规定的脱密期限后，方可调离。

(4)关键部位人员的离岗要求：在上述基础上，关键部位的信息系统安全管理人员离岗，应按照机要 人员管理办法办理。



**考** **点** **1** **3** **7** **:** **系** **统** **安** **全** **和** **保** **密** **层** **次**

1、系统运行的安全管理中关于用户管理制度的内容包括建立用户身份识别与验证机制，防止非法用户

**进入应用系统；对用户及其权限的设定进行严格管理，用户权限的分配遵循“最小特权”原则；用户密码应** **严格保密，并及时更新；重要用户密码应密封交安全管理员保管，人员调离时应及时修改相关密码和口令。**



**(09下27)(11上26)(16上25)**

2 、应用系统运行中涉及的安全和保密层次包括**系统级安全、资源访问安全、功能性安全和数据域安全。** 这4个层次的安全，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。(09**

下26)(10上26)(10下33)(17下69)(19上69 )程序资源访问控制安全的粒度大小界于系统级安全和功

能性安全两者之间，是最常见的应用系统安全问题，几乎所有的应用系统都会涉及这个安全问题。

(1)系统级安全。

企业应用系统越来越复杂，因此制定得力的系统级安全策略才是从根本上解决问题的基础。应通过对现 行系统安全技术的分析，制定系统级安全策略，策略包括敏感系统的隔离、访问IP地址段的限制、登录时间 段的限制、会话时间的限制、连接数的限制、特定时间段内登录次数的限制以及远程访问控制等， **系统级安** **全是应用系统的第一道防护大门。**

(2)资源访问安全。

对程序资源的访问进行安全控制，在客户端上，为用户提供和其权限相关的用户界面，仅出现和其权限 相符的菜单和操作按钮： 在服务端则对URL 程序资源和业务服务类方法的调用进行访问控制。

(3)功能性安全。

**功能性安全会对程序流程产生影响，如用户在操作业务记录时，是否需要审核，上传附件不能超过指定** **大小等。这些**安全限制已经不是入口级的限制，而是程序流程内的限制，在一定程度上影响程序流程的运行。

(4)数据域安全。( **13上20)(18上70)**

数据域安全包括两个层次，其一是行**级数据域安全，**即用户可以访问哪些业务记录， 一般以用户所在单 位为条件进行过滤；其二是**字段级数据域安全，**即用户可以访问业务记录的哪些字段。



**考** **点** **1** **3** **8** **:** **安** **全** **检** **查** **、** **安** **全** **等** **级**

1 、企业要加强对应用系统安全运行管理工作的领导， **每年至少组织有关部门对系统运行工作进行一次** **检查。部门每季度进行一次自查。** 要加强对所辖范围内应用系统运行工作的监督检查。检查可采取普查、抽 查、专项检查的方式定期或不定期地进行。( **11上26)**

**安全组织由单位主要领导人领导，**不能隶属于计算机运行或应用部门。

**2** **、**根据应用系统所处理数据的秘密性和重要性确定安全等级，并据此采用有关规范和制定相应管理制 度。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。(** **11上25)(12下29)(15上24)**

3、《信息安全等级保护管理办法》将信息系统的安全保护等级分为5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) **(17上13)(18下70)**

**4、计算机系统安全保护能力的五个等级，即：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**。( 1 5 下 2 4 )