第6章 物理实体与环境安全

信息安全管理

主讲 李章兵

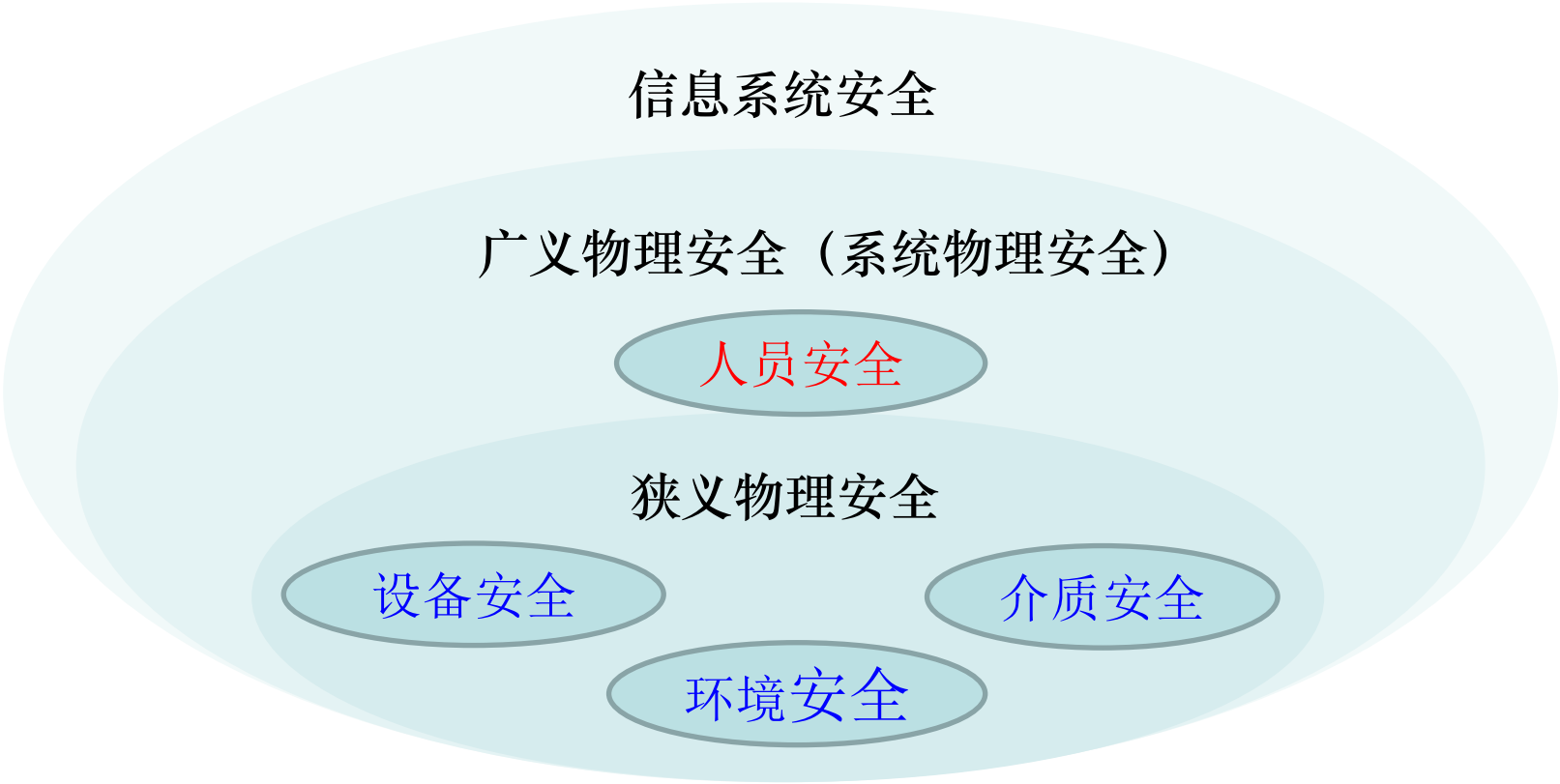
教学目标

- 本章的重点是
  - 物理安全概述
  - 设备安全
  - 介质安全
  - 环境安全

6.1 物理安全概述

- **1. 物理安全威胁**
  - **狭义物理安全**
    - **包括环境安全、设备安全和介质安全，主要解决由于设备、设施、介质的硬件条件所引发的信息系统物理安全威胁问题。**
  - **广义物理安全**
    - **应包含由软件、硬件、操作人员组成的整体信息系统物理安全，即包括系统物理安全。其应确保信息系统的保密性、可用性、完整性。**

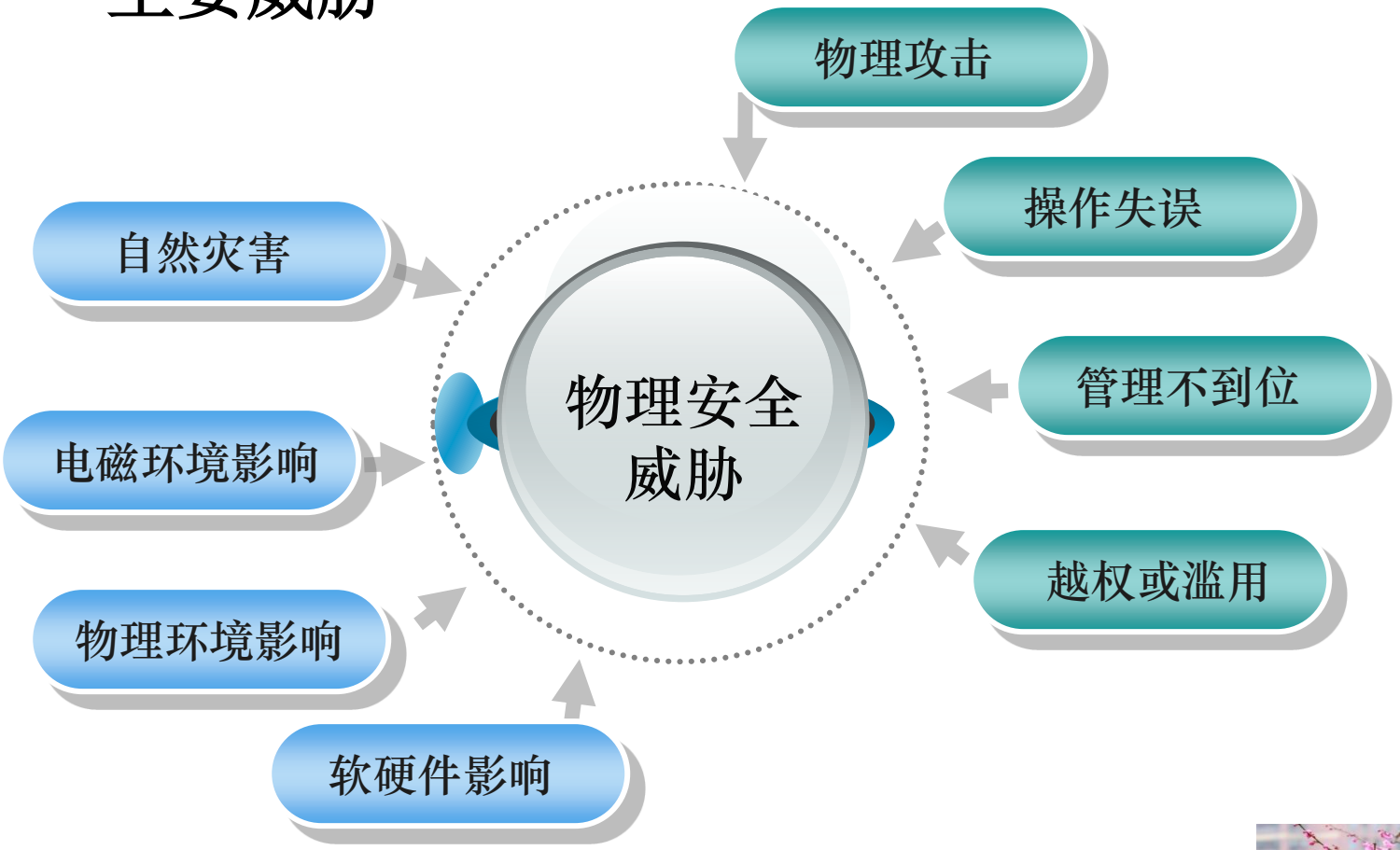
6.1 物理安全概述



物理安全概念体系

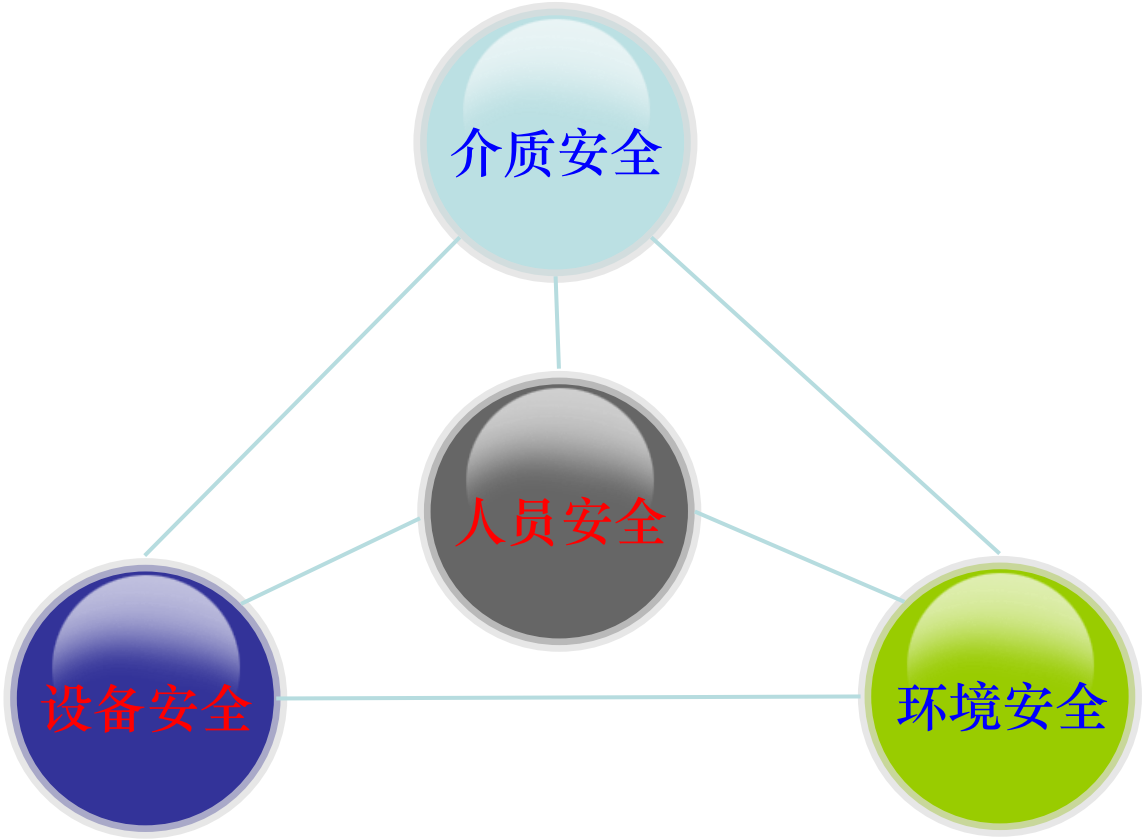
6.1 物理安全概述

- **1. 物理安全威胁**
  - 主要威胁



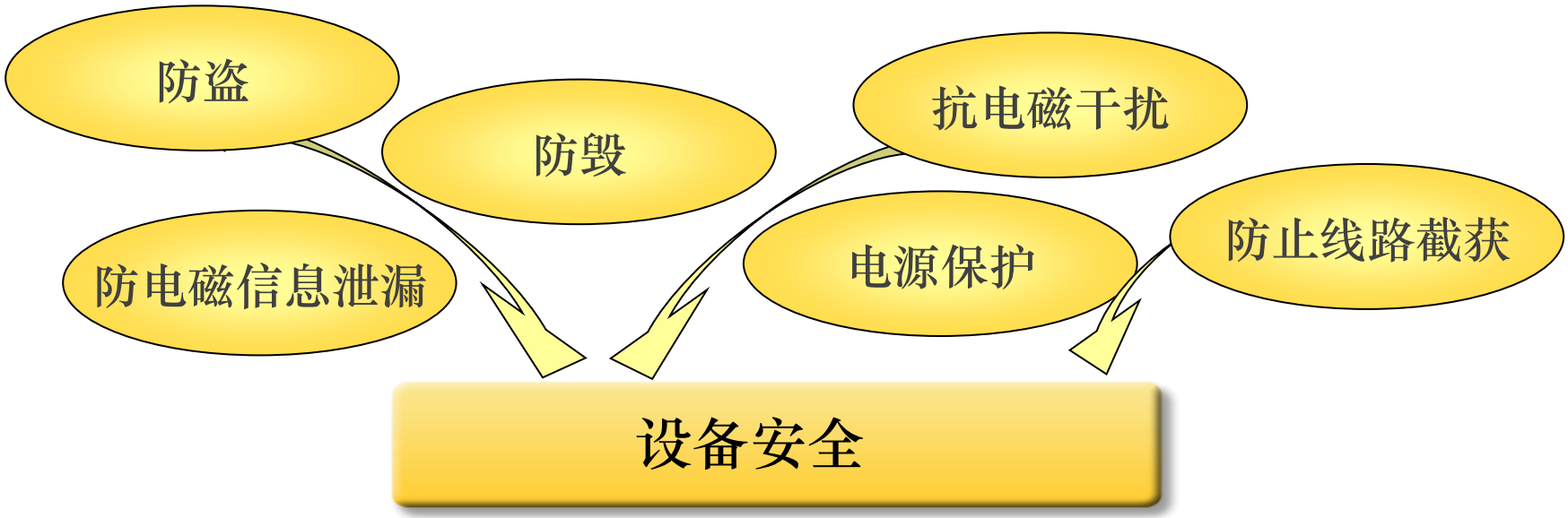
6.1 物理安全概述

- **2. 物理安全需求**



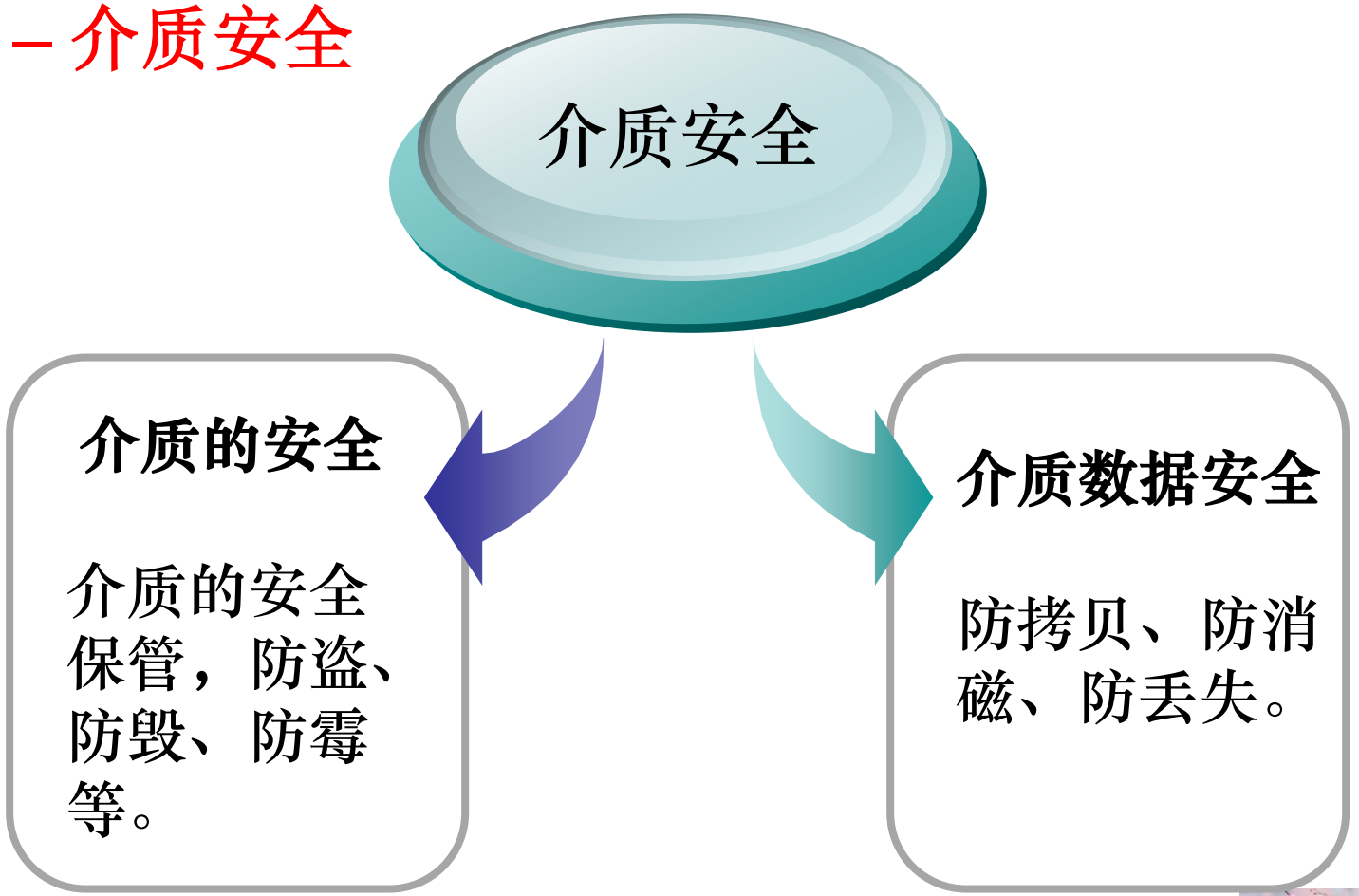
6.1 物理安全概述

- **2. 物理安全需求**
  - 设备安全



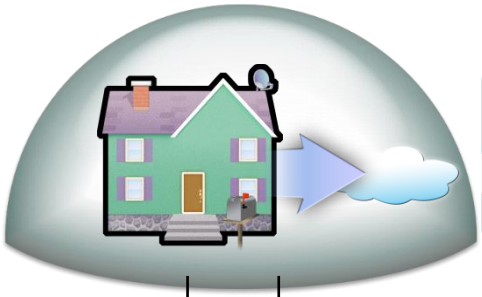
6.1 物理安全概述

- **2. 物理安全需求**
  - 介质安全



6.1 物理安全概述

- **2. 物理安全需求**
  - 环境安全



环境安全：对系统所在环境的安全保护。应具备消防报警、安全照明、不间断供电、温湿度控制系统和防盗报警。

机房与设施安全

安全区域

6.1 物理安全概述

- **2. 物理安全需求**
  - 人员安全(上一章已讲)

6.1 物理安全概述

- **3. 国内外物理安全标准**
  - **国内标准：**
    - **（1）GB 50222 《建筑物内部装修设计防火规范》**
    - **（2）GB/T 9361-1988 《计算站场地安全要求》**
    - **（3）GB/T 2887-2000 《电子计算机场地通用规范》**
    - **（4）GB/T 14715-1993 《信息技术设备用UPS通用技术条件》**
    - **（5）GB/T 50174-1993 《电子计算机机房设计规范》**
    - **（6） GB/T 4943-2001 《信息技术设备安全》**
    - **（7）GGBB1-1999 《信息设备电磁泄漏发射限值》**
    - **（8）GB50057《建筑物防雷设计规范》**
    - **（9）GB 50016 《建筑设计防火规范》**
    - **（10）BMB4-2000 《电磁干扰器技术要求和测试方法》**
    - **（11）SJ/T 10796《防静电活动地板通用规范》**

6.1 物理安全概述

- **3. 国内外物理安全标准**
  - **国外标准：**
    - **（1）ECMA-83：1985 《公共数据网DTE到DEC接口安全标准》**
    - **（2）ECMA-129：1988 《信息处理设备的安全》**
    - **（3）FIPS-73：1981 《计算机应用安全指南》**
    - **（4）DODI 5200-1-1982 《DOD信息安全保密程序》**
    - **（5）DODI 5200-1-R-1986 《信息安全保密程序规章》**
    - **（6）DODI 5200.28-1988 《自动信息系统安全保密要求》**
    - **（7）DODI 5200.28-STD-1985 《国防可信计算机系统评估准则》**
    - **（8）DODD 5215.1-1982 《计算机安全保密评估中心》**
    - **（9）DODD 5215.2-1986 《计算机安全保密技术脆弱性报告程序》**

6.2 设备安全

- 设备威胁
  - 设备可能会受到环境因素（如火灾、雷击）、未授权访问、供电异常、设备故障等方面的威胁，使组织面临资产损失、损坏、敏感信息泄露或商业活动中断的风险。
- 设备安全
  - 保证和控制设备的正常运转。
    - 应考虑设备安置、供电、电缆、设备维护、办公场所外的设备及设备处置与再利用方面的安全控制。
  - 包括：防盗和防毁、防电磁泄露、设备管理、电源安全

6.2 设备安全

- 1.防盗和防毁
  - 防盗防毁是计算机防护的一个重要内容。
    - 设备是计算机系统正常运行的关键，被盗所造成的损失可能远远超过计算机设备本身的价值。
  - 妥善安置及保护设备，以降低来自未经授权的访问及环境威胁造成的风险。
  - 保密程度要求高的设备防盗防毁措施
    - 安装防盗报警装置；
    - 制定安全保护办法；
    - 夜间留人值守。

6.2 设备安全

- **1.防盗和防毁**
  - 设备安置与保护原则
    - 设备的布置应有利于减少对工作区的不必要访问；
    - 敏感数据的信息处理与存储设施应当妥善放置，降低在使用期间内对其缺乏监督的风险；
    - 要求特别保护的项目要与其他设备隔离，以降低所需保护的等级；
    - 采取措施，尽量降低盗窃、火灾等环境威胁所产生的潜在风险；
    - 考虑实施“禁止在信息处理设施附近饮食、饮水和吸烟”等。

6.2 设备安全

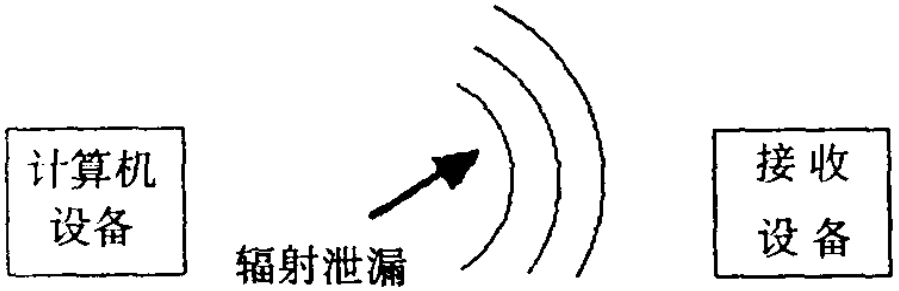
- 1.防盗和防毁
  - 安全防盗措施
    - 设置报警器
    - 锁定装置
    - 视频监控
    - 设备标识
    - 计算机保险
    - 列出清单或绘制位置图

6.2 设备安全

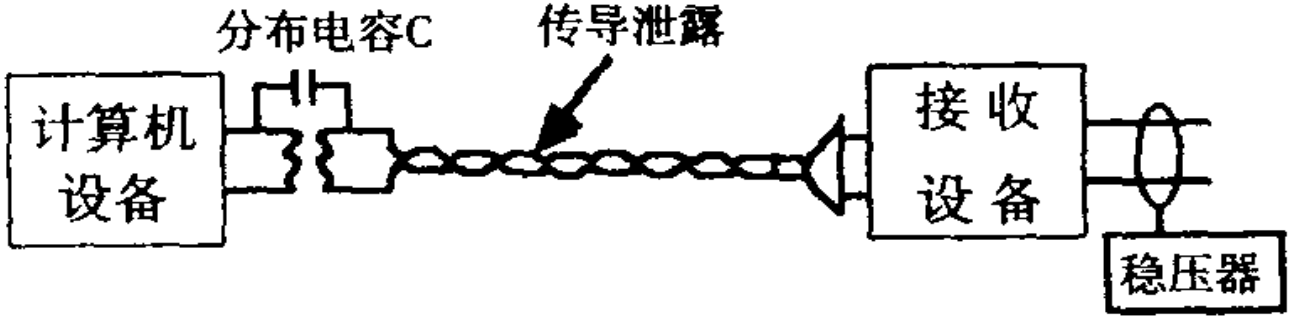
- 2. 防电磁泄漏
  - 电磁辐射危害
    - 计算机主机及其附属电子设备在工作时不可避免的会产生电磁波辐射，电磁辐射中携带有计算机正在处理的数据信息。
    - 电磁泄漏很容易造成信息暴露的危险。

6.2 设备安全

- 2. 防电磁泄漏
  - 电磁泄漏途径
    - 直接泄漏：电磁波形式的辐射



    - 传导泄漏：电源线、控制线、信号线和地线造成的信号传导



6.2 设备安全

- 2. 防电磁泄漏
  - 电磁泄漏抑制技术
    - 包容法：采用金属外壳屏蔽辐射源设备，阻止电磁波的外泄传播；
    - 抑源法：从线路和元器件入手，从根本上阻止计算机系统向外辐射电磁波，消除产生较强电磁波的根源。

电子隐蔽技术 → 电子隐蔽技术主要是用干扰、调频等技术来掩饰计算机的工作状态和保护信息

物理抑制技术 → 物理抑制技术则是抑制一切有用信息的外泄。物理抑制技术可分为包容法和抑源法

6.2 设备安全

- 2. 防电磁泄漏
  - 电磁辐射防护措施
  - 对辐射的防护
    - 选用低辐射设备
    - 利用噪声干扰源
    - 采取屏蔽措施
    - 距离防护
    - 采用微薄吸收材料
  - 对传导线路的防护
    - 机房装修材料应符合GB 50016《建筑设计防火规范》中规定的难燃材料和非燃材料，能防潮、吸音、防起尘、抗静电等。
    - 非燃烧材料 **non-combustible**
      - 指材料在受燃烧或高温作用时，不起火、不微燃、不碳化、只软化的材料。
    - 难燃烧材料 **difficult combustible**
      - 指材料受到燃烧或高温作用时，难起火、难微燃、难碳化的材料。

6.2 设备安全

- 3. 设备安全管理
  - 设备维护
    - 设备应进行正确维护，以确保其持续的可用性及完整性。
      - 设备维护不当会引起设备故障，造成信息不可用甚至不完整。
      - 应按照设备维护手册的要求和有关维护规程，对设备进行适当的维护，确保设备处于良好的工作状态。
    - 维护相关措施
      - 1）按照供应商推荐的保养时间间隔和规范进行设备保养。
      - 2）只有经授权的维护人员才能维修和保养设备。
      - 3）维修人员应具备一定的维修技术能力。
      - 4）应当把所有可疑故障和实际发生的事故记录下来。
      - 5）当将设备送外进行保养时，应采取适当的控制，防止敏感信息的泄露。

6.2 设备安全

- **3. 设备安全管理**
  - 设备转移
  - 设备转移相关规定
    - （1）未经授权，不得将设备、信息或软件带离工作场地。
    - （2）应识别有权资产移动，离开办公场地的雇员、合同方和第三方用户。
    - （3）应设置设备移动的时间限制，并在返还时执行一致性检查。必要时可以删除设备中的记录，当设备返还时，再恢复记录。

6.2 设备安全

- **3. 设备安全管理**
  - 设备处置和重复利用
    - 信息设备在报废、淘汰处置或再利用(改为他用)前，应当清除存储在设备中的信息，处理不当会造成敏感信息的泄露。
    - 设备处置及重复利用措施
      - 1）在设备处置或再利用之前，组织应采取适当的方法将设备内存储媒体的敏感数据及许可的软件清除。
      - 2）应在风险评估的基础上履行审批手续，以决定对设备内装有敏感数据的存储设备的处置方法——消磁、物理销毁、报废或重新利用。
      - 3）制定明确的设备淘汰处理程序，确保进行处理的时候不会出现错误和疏忽导致的问题。
      - 4）完成整个淘汰过程处理后要签字确认。

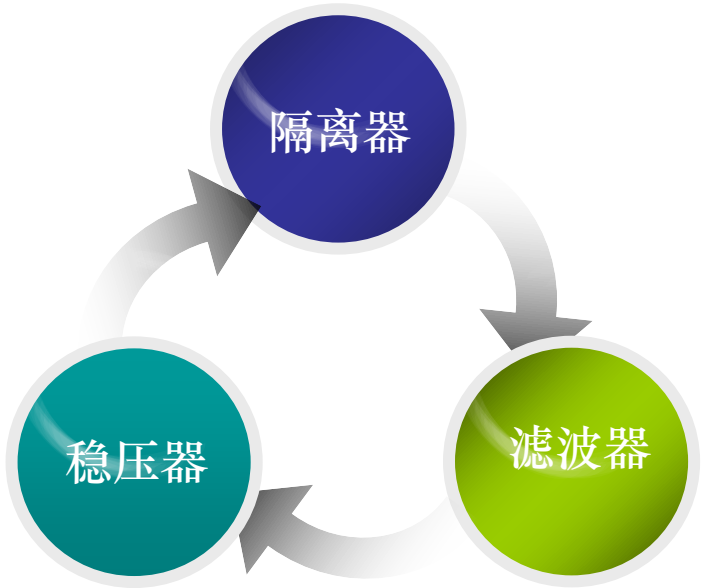
6.2 设备安全

- **3. 设备安全管理**
  - 电源安全
    - 电源是计算机网络系统的命脉，电源系统的稳定可靠是计算机网络系统正常运行的先决条件。
    - 电源系统的电压波动、浪涌电流和突然断电等意外情况发生，可能引起计算机系统存储信息的丢失、存储设备的损坏等
    - 电源系统的安全是计算机系统物理安全的一个重要组成部分。
    - 电源防护措施
      - 电源调整器
      - 不间断电源UPS
      - 电源相关操作

6.2 设备安全

- **3. 设备安全管理**
  - **– 电源安全**
    - **电源调整器：三种**
      - 电源线的暂态反应直接从电源线传输到电脑的脉冲电压。
      - 电源滤波器是由电感和电容组成的低通滤波电路所构成，它允许直流或50Hz电流通过，对频率较高的干扰信号则有较大的衰减。

隔离器	隔离器包括暂态反应压制器、涌浪电流保护器及隔离元件。当电源线上产生脉冲电压或浪涌电流时，隔离器将电压的变化限制在额定值的±25%之内。
稳压器	电源电压的变动若超过±10%，都有必要使用稳压器。稳压器可以把电源维持在适当的电压。
滤波器	滤波器能滤除60Hz以外的任何杂波。



6.2 设备安全

- 3. 设备安全管理
  - 电源安全
    - 电源调整器：选择原则
      - 1）对电压脉冲的反应速度
      - 2）是否有能力滤除高频杂波
      - 3）是否有能力控制持续的暂态反应
      - 4）是否使电力供应保持在一定的水准
      - 5）能否使输入的电压变动范围减至最小
      - 6）能否同时供应几台电脑充足的电力

6.2 设备安全

- 3. 设备安全管理
  - 电源安全
    - 不间断电源UPS

6.2 设备安全

- **3. 设备安全管理**
  - 电源安全
    - 不间断电源UPS
      - 持续供电型UPS
        - » 将外线交流电源整流成直流电对电池充电。
        - » 电力中断时把电池直流电源变成交流电源，供电脑使用。
      - 顺向转换型UPS
        - » 平时由外线电力带动的发电机发电给电池充电
        - » 外线电力中断s时用变流器把电池的直流变成交流，供给电脑。
      - 逆向转换型UPS
        - » 大部分时间由电池来供电，能够忍受像外线电力电压过高、过低或电源线的暂态反应等冲击。
        - » 外线电力中断迅速反应，在最短的时间内将电力供应给电路。
      - 马达发电机
        - » 发电机可使用外线电力、汽油或柴油引擎带动发电机，可提供大容量电压稳定电力，供应电脑系统、家庭或办公室照明所需的电力。

6.2 设备安全

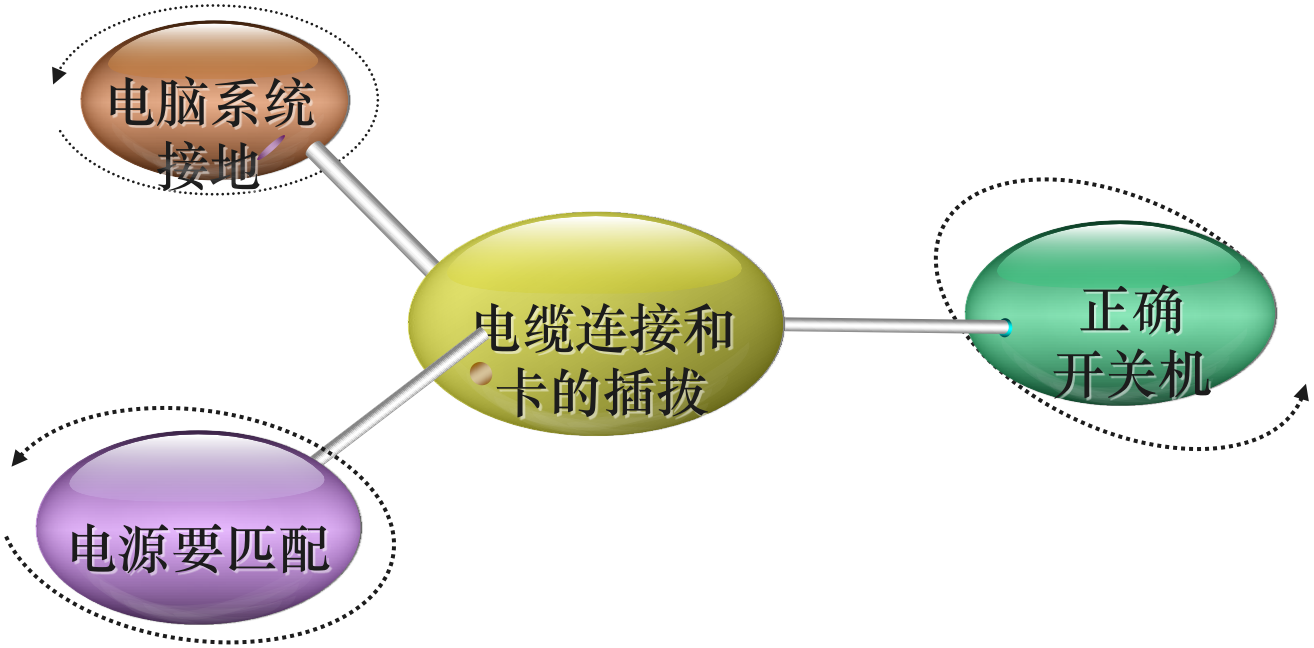
- **3. 设备安全管理**
  - 电源安全
    - 不间断电源UPS选择
      - 1）能否提供足够的电源满足用户需要
      - 2）切换至备用电源所需的时间
      - 3）有内装的电源调整器
      - 4）有过高及过低电压保护

6.2 设备安全

- **3. 设备安全管理**
  - 电源安全
    - 电源相关操作
      - 电脑系统安装，要特别注意电源盒地线的安装。
      - 电脑电源的输入电压规格繁多，电源接通前必须仔细检查输入电压的标称值。
      - 开机时应先开启外部设备，再开主机；关机先关主机，再关外部设备。当需要再次开启主机时，开闭的时间间隔要在2-3分钟以上。
      - 当需要插拔电缆和卡时，必须注意的问题：
        - » 必须先切断主机及其外部设备的电源，才能拔插。
        - » 记住电缆插板的位置，必要时标记号和画出连接图。
        - » 拔出时，用力要柔和。
        - » 插头插好后，要将插头上的固定装置固定好。

6.2 设备安全

- 3. 设备安全管理
  - 电源安全
    - 电源相关操作
      - 设备接地、电缆连接和卡插拔、正确开关机、电源容量匹配



6.3 介质安全

- 介质安全包括媒体本身的安全及媒体数据的安全。
  - 常用的存储介质有：硬盘、磁盘、磁带、打印纸、光盘等。
  - 媒体本身的安全：指防盗、防毁、防霉等。
  - 媒体数据的安全：指防止记录的信息不被非法窃取、篡改、破坏或使用。

6.3 介质安全

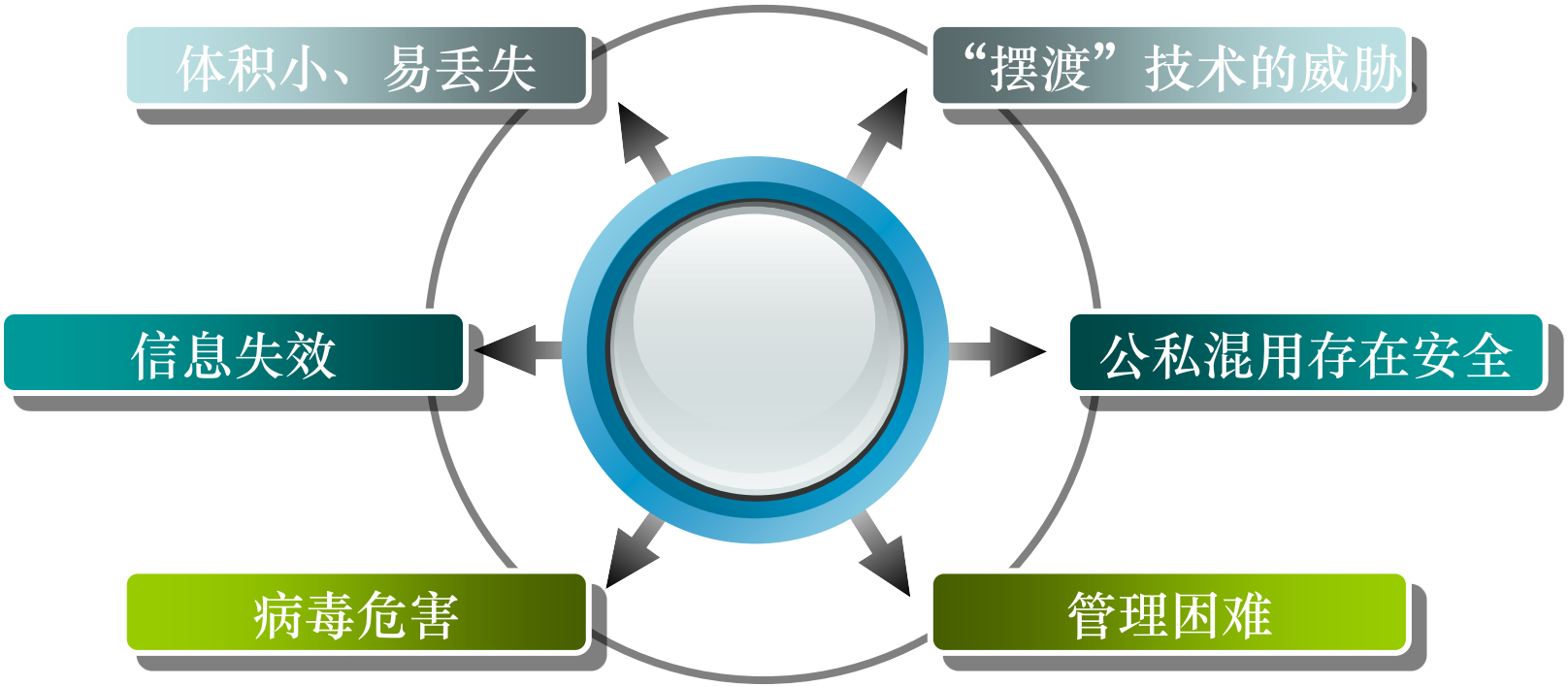
- **1. 介质管理**
  - **– 介质管理措施**
    - 1）存放有业务数据或程序的介质，必须注意防磁、防潮、防火、防盗。
    - 2）对硬盘上的数据，要建立有效的级别、权限，并严格管理，必要时要对数据进行加密，以确保硬盘数据的安全。
    - 3）存放业务数据或程序的介质，管理必须落实到人，并分类建立登记簿。
    - 4）对存放有重要信息的介质，要备份两份并分两处保管。
    - 5）打印有业务数据或程序的打印纸，要视同档案进行管理。
    - 6）凡超过数据保存期的介质，必须经过特殊的数据清除处理。
    - 7）凡不能正常记录数据的介质，必须经过测试确认后销毁。
    - 8）对删除和销毁的介质数据，应采取有效措施，防止被非法拷贝。
    - 9）对需要长期保存的有效数据，应在介质的质量保证期内进行转储，转储时应确保内容正确。

6.3 介质安全

- **2. 移动介质管理**
  - 移动存储介质
    - 指可与计算机系统单独脱离的存储介质。
    - 特点：**通用性强、存储量大、体积小、易携带**
    - 安全隐患
      - 数据拷贝不受限、信息失效、易感染计算机木马病毒等；
      - 违规交叉使用、单位和个人持有不区分(公私不分)、”摆渡”泄露公司内部机密。
    - 移动存储介质的安全保密问题日渐突出，成为当前保密管理中的重点和难点。
      - 加强移动存储介质的风险分析和管理已成为有效保障涉密信息系统安全的重要基础。

6.3 介质安全

- **2. 移动介质管理**
  - **– 移动存储介质安全隐患**



6.3 介质安全

- **2. 移动介质管理**
  - 移动介质的分类
    - 涉密介质、内部介质、普通介质

涉密移动存储介质	是指用于存储国家秘密信息的移动存储介质。
内部移动存储介质	是指用于存储不宜公开的内部工作信息的移动存储介质。
普通移动存储介质	是指用于存储公开信息的移动存储介质。

6.3 介质安全

- **2. 移动介质管理**
  - **移动介质的管理和使用**
    - **涉密移动存储介质**
      - **1）严禁涉密移动存储介质在非涉密计算机上使用**
      - **2 ）严禁高密级的移动存储介质在低密级计算机或信息系统中使用。**
      - **3）涉密移动存储介质的使用应严格按照“统一购置、统一标志、严格登记、集中管理”的原则进行管理。**
      - **4）涉密移动存储介质应严格使用权限，在其保存、传递和使用过程中必须保证其中的涉密信息不被非授权人知悉。**
      - **5）经管人员应定期进行清点，确保涉密移动存储介质的觉得安全。**

6.3 介质安全

- **2. 移动介质管理**
  - 移动介质的管理和使用
    - 内部移动存储介质
      - 1）要严格禁止内部移动存储介质在与互联网连接的计算机上使用。
      - 2）严禁存储国家机密信息。
      - 3）将内部信息计算机数据传送到涉密计算机时，必须采取有效的保密管理和技术防范措施，严防被植入恶意代码程序将涉密计算机感染，导致国家秘密信息被窃取。

6.3 介质安全

- **2. 移动介质管理**
  - 移动介质的管理和使用
    - 普通移动存储介质
      - 1）严格禁止普通移动存储介质存储国家机密信息和不宜公开的内部工作信息。
      - 2）严格限制普通移动存储介质直接在涉密计算机单位及涉密信息系统内使用。
      - 3）当因工作需要，需从互联网将所需数据考入内部工作计算机、涉密计算机或涉密信息系统时，必须经审查批准后，使用普通移动存储介质进行传递。

6.3 介质安全

- 3. 介质信息的消除和备份
  - 硬盘涉密信息的消除
    - 物理粉碎
      - 采用专业工具和设备进行，对于磁盘、光盘、废弃硬盘。
    - 强磁场或有源磁场消除
      - 根据磁存储原理，磁介质的每个存储单元存储一个“位”信息，由磁矩在空间的取向表示，以一定的方式有规则地排列。
      - 破坏磁介质中磁矩的空间排列方式来消除信息。
    - 热消磁
      - 磁记录材料为铁磁性材料，其一个重要参量为居里温度Tc，材料呈铁磁性，在Tc以上，材料呈顺磁性。
      - 如果把磁记录材料加温至Tc以上后再降温，那么在室温下磁记录材料将处于热退磁态，曾经记录过的所有信息都已消除。
    - 专业的销毁机

6.3 介质安全

- **3. 介质信息的消除和备份**
  - 软盘涉密信息的消除
    - 软盘价格低廉，没有金属的外保护层
    - 涉密信息的消除：物理粉碎法、强磁场消除法。
  - 纸介质涉密信息的消除
    - 纸介质价格低廉，较容易处理
    - 涉密信息的消除：机械粉碎、明火焚烧、液体浸泡
    - 主要使用碎纸机销毁

6.3 介质安全

- **4.介质安全处置措施**
  - 敏感信息介质：秘密和安全地存储和处置；
    - 应有程序识别可能需要安全处置的项目；
    - 安排把所有介质部件收集起来并进行安全处置；
    - 应选择具有足够控制措施和经验的合同方对纸、设备和介质进行收集和处置；
  - 敏感部件处置：做好记录以便保持审核踪迹。

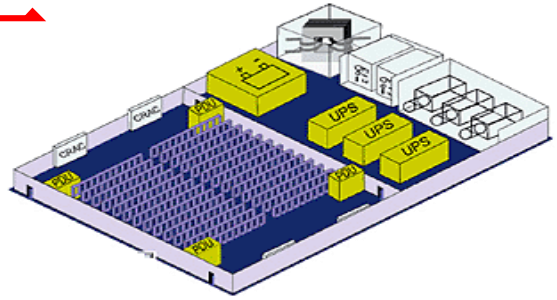
6.3 介质安全

- **5.介质备份**

由于人工误操作、系统故障、软件缺陷、病毒、黑客、天灾人祸等许多因素导致数据丢失，而重新生成丢失的数据又非常昂贵。因此备份是信息安全管理不可或缺的一部分。

容灾备份是通过在异地建立和维护一个备份存储系统，利用地理上的分离来保证系统和数据对灾难性事件的抵御能力。

6.4 环境安全



- **1. 机房安全**
  - 机房组成
    - **主机房**：用以安装主机及其外部设备、路由器、交换机等骨干网络设备。
    - **基本工作房间**：数据录入室、终端室、网络设备室、已记录的媒体存放间、上机准备间。
    - **一类辅助房间**：备件间、媒体存放间、资料室、仪器室、硬件人员办公室、软件人员办公室。
    - **二类辅助房间**：维修室、电源室、蓄电池室、发电机室、空调系统用房、灭火钢瓶间、监控室、值班室。
    - **三类辅助房间**：贮藏室、更衣换鞋室、缓冲间、机房人员休息室、盥洗室等。

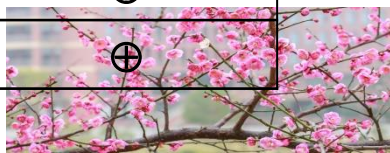
6.4 环境安全

- 1. 机房安全
  - 机房安全等级
    - A类：
      - 放置需要最高安全性和可靠性的系统和设备。
      - 严格的要求，有完善的计算机机房安全措施。
    - B类：
      - 安全性介于A类和C类之间。
      - 要求较严格，有较完善的计算机机房安全措施。
    - C类：
      - 存放只需要最低限度的安全性和可靠性的一般性系统。
      - 基本要求，有基本的计算机机房安全措施。

6.4 环境安全

- **1. 机房安全**
  - **机房安全等级**
    - **机房安全级别要求**

安 全 项 目	C类	B类	A类
场地选择	—	⊕	⊕
防火	⊕	⊕	⊕
内部装修	—	⊕	⊕
供配电系统	⊕	⊕	⊕
空调系统	⊕	⊕	⊕
火灾报警及消防设施	⊕	⊕	⊕
防水	—	⊕	⊕
防静电	—	⊕	⊕
防雷击	—	⊕	⊕
防鼠害	—	⊕	⊕
电磁波的防护	—	⊕	⊕

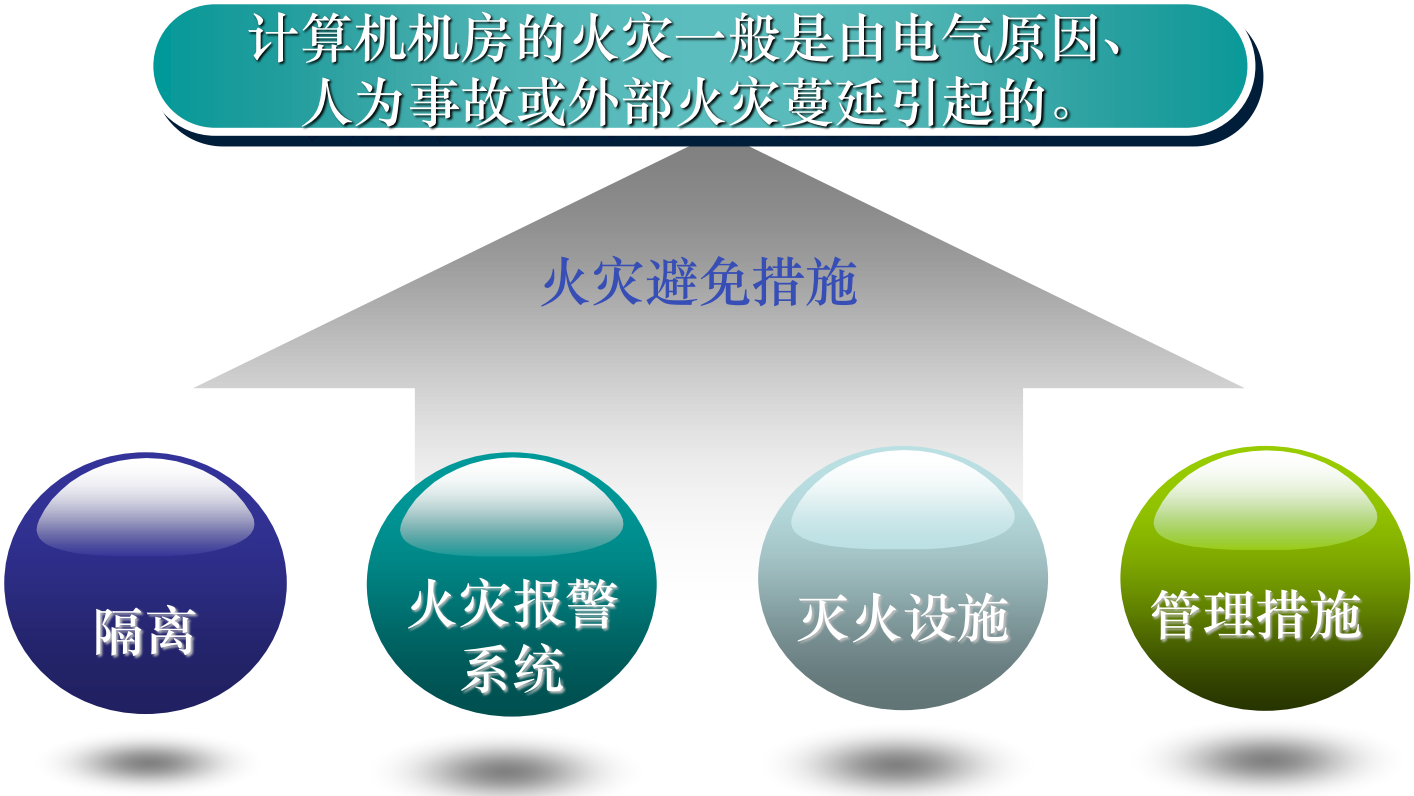


6.4 环境安全

- **1. 机房安全**
  - 机房选址要求(GB/T 9361-1988 《计算站场地安全要求》)
    - 应避开易发生火灾危险程度高的区域。
    - 应避开易产生粉尘、油烟、有害气体源以及存放腐蚀、易燃、易爆物品的地方。
    - 应避开低洼、潮湿、落雷、重盐害（靠近海岸）区域和地震频繁的地方。
    - 应避开强振动源和强噪音源。
    - 应避开强电磁场的干扰。
    - 应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。
    - 应远离核辐射源。

6.4 环境安全

- **1. 机房安全**
  - 机房防火



6.4 环境安全

- 1. 机房安全
  - 机房防火
    - 防火技术设施检查项目

检测项目	期限	注意
设备供电（含电池电量）情况	1个月	
供水系统及灭火工具情况	1个月	
视频监视系统	1个月	
火灾报警器音频、灯光报警情况	1个月	人工遥控测试
各项管理制度执行情况	3个月	
火警控制系统工作情况	1年	请制造商协助
灭火器压力和重量检查、更换	1年	标出灭火器的检查日期、项目
防火系统总检查和灭火演练	1年	要注意安全

6.4 环境安全

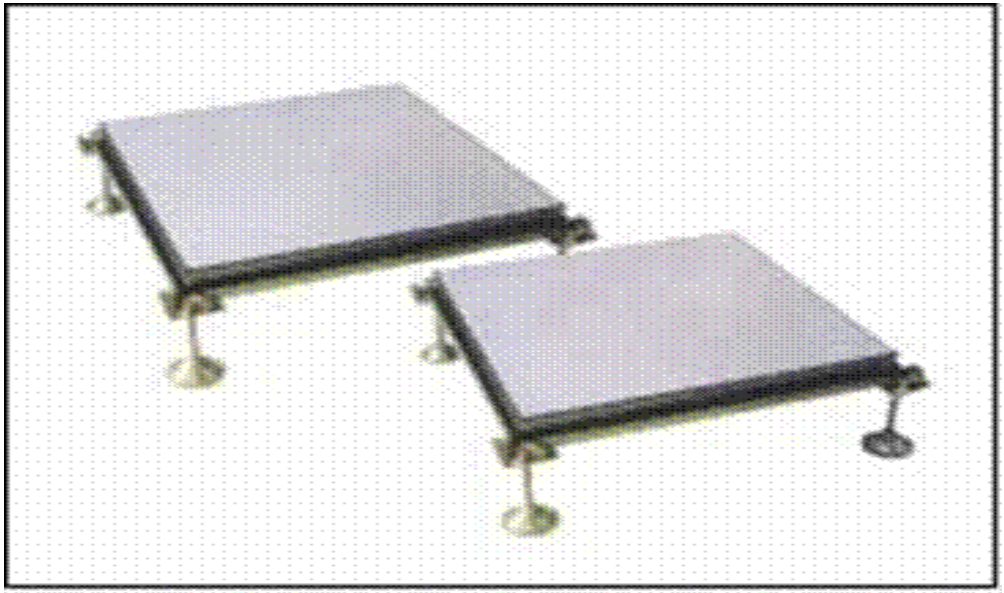
- **1. 机房安全**
  - 机房防火
    - 火灾避免措施
      - 来自机房外部的火灾危险预防：
        - » 与其他建筑分开建设，建筑间留有防火通道。
        - » 与其他建筑物合建时，机房为防火分区，外墙采用非燃烧材料构建防火墙。
        - » 区域进出门应采用防火门或防火卷帘。
        - » 穿越防火墙的送、回风管，应设防火阀。
        - » 机房建设采用防火材料。机房内部的建筑材料应选用非燃烧材料(A级)或难燃烧材料(B级)。
      - 设置火灾报警系统。
      - 设置气体灭火系统。
      - 合理正确使用用电设备，制订完善的防火制度。

6.4 环境安全

- **2. 机房内部设施安全**
  - 机房内部装修
    - 装修材料
      - 装修材料应符合GB 50016《建筑设计防火规范》中规定的难燃材料和非燃材料
      - 应能防潮、吸音、防起尘、抗静电等。
    - 活动地板
      - 活动地板应是难燃材料或非燃材料。
      - 应有稳定的抗静电性能和承载性能，同时耐油、耐腐蚀、柔光、不起尘等。
      - 地板提供各种规格的电线、电缆、进出口应做得光滑，防止损伤电线、电缆。
      - 活动地板下的建筑地面应平整、光滑、防潮、防尘。
      - 安装采取相应措施，防止地板支脚倾斜、移位、横梁坠落。

6.4 环境安全

- **2. 机房内部设施安全**
  - 机房内部装修
    - 复合地板
      - 复合塑料贴面地板的基材是层压刨花板，上下表面贴有塑料贴面，四周用油漆封住，或用镀锌铁皮包封的地板。



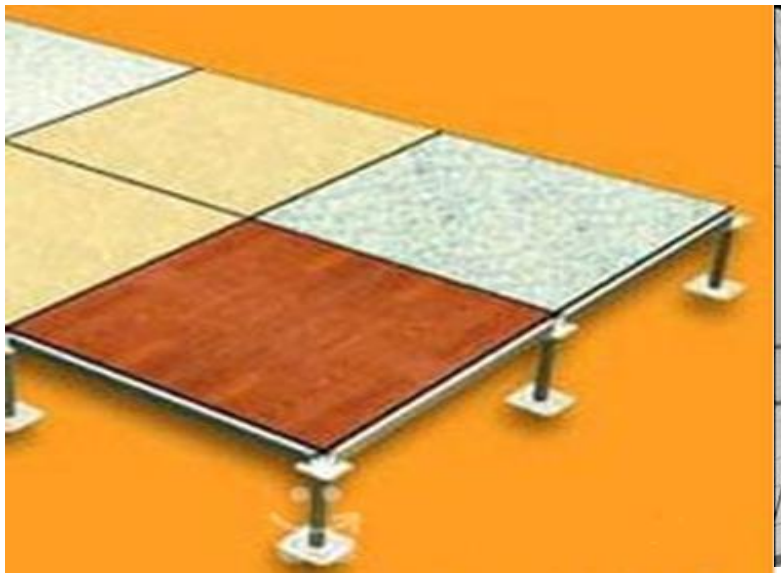
三防活动地板&复合活动板

6.4 环境安全

- **2. 机房内部设施安全**
  - 机房内部装修
    - 木质地板
      - 纯木质地板的优点是造价低、易加工，但强度较差、易受潮变形，且易引起火灾，一般不在机房内使用。

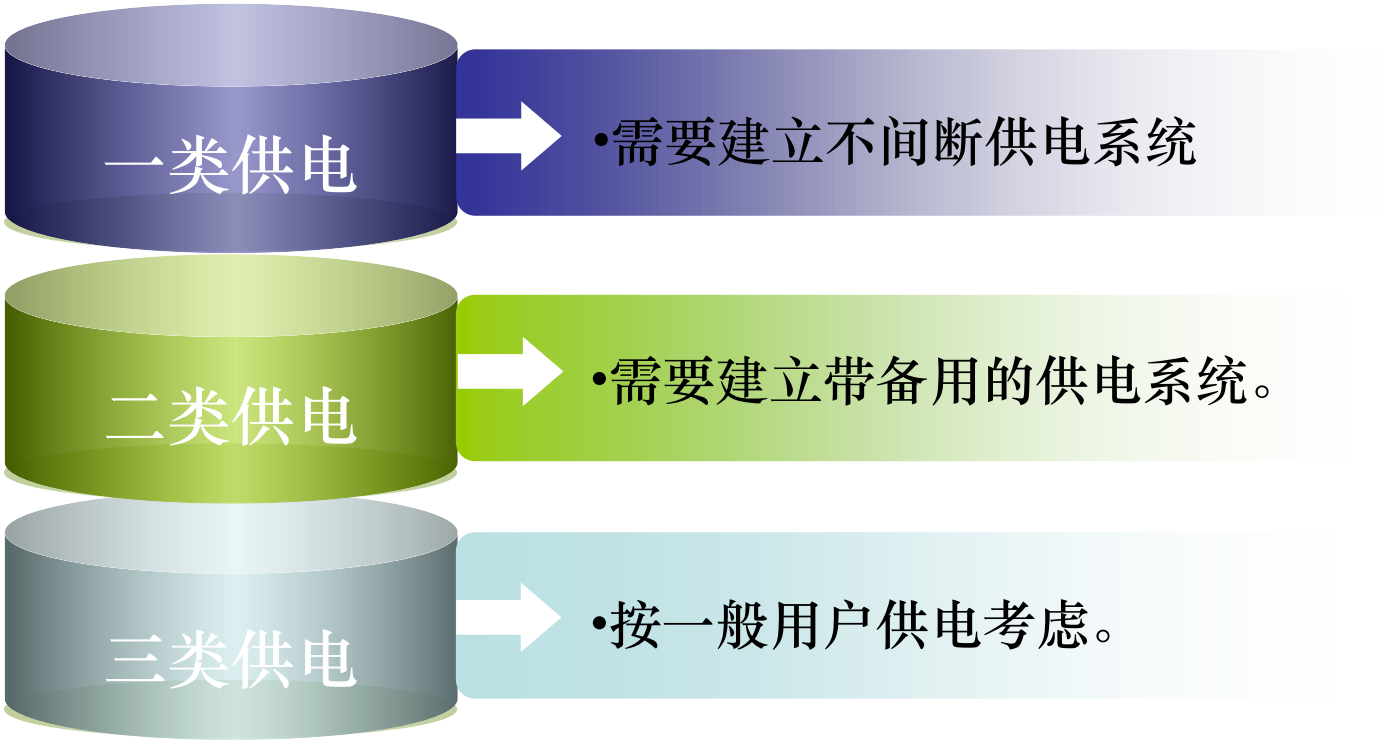
6.4 环境安全

- **2. 机房内部设施安全**
  - 机房内部装修
    - 金属地板
      - 全钢或合金组成，机械强度高、承载能量强、耐冲击性能好；表面静电喷塑，柔光、耐磨、防水、防火、防尘、防腐蚀。



6.4 环境安全

- **2. 机房内部设施安全**
  - 供配电系统
    - 供电方式分为三类：GB/T 2887-2000



6.4 环境安全

- **2. 机房内部设施安全**
  - **供配电系统**
    - 供配电系统应符合如下要求
      - 计算机站应设专用可靠的供电线路。
      - 计算机系统的电源设备应提供稳定可靠的电源。
      - 供电电源设备的容量应有一定的余量。
      - 计算机系统用的分电盘应设计在计算机机房内，并采取防触电措施。
      - 从分电盘到计算机系统各个设备的电缆应为耐燃铜芯屏蔽电缆。
      - 计算机系统的各设备走线不得与空调设备、电源设备和无电磁屏蔽的走线平行。
      - 计算机电源系统的所有接点均应渡铅锡处理。
      - 在计算机机房出入口处或值班室，应配备应急电话和应急断电装置。
      - 计算机场地场地宜采用固定型阀控密封式铅酸蓄电池。
      - 计算机系统接地应采用专用地线。
      - 计算机机房应设置应急照明和安全口的指示灯。

6.4 环境安全

- **2. 机房内部设施安全**
  - **– 供配电系统**
    - 空调系统
      - – 温度、湿度和洁净度并称为三度。
      - – 为使机房内的三度达到规定的要求，空调系统、去湿机、除尘器是必不可少的设备。
      - – 机房内温、湿度要求：

指标	夏季	冬季	全年
温度	23±2℃	20±2℃	18~28℃
相对湿度	45%~65%	40%~70%	
温度变化率	＜5℃/h 并不得结露	＜10℃/h 并不得结露	
空气含尘浓度	在表态条件下测试，每升空气中大于或等于0.5μm的尘粒数，应少于18000粒。		

6.4 环境安全

- **2. 机房内部设施安全**
  - **供配电系统**
    - 空调系统
    - 空调系统要求：重要计算机系统处应配备专用的
      - 计算机机房应采用专用空调设备。
      - 空调系统的主要设备要有备份，空调设备在能量上应有一定余量。
      - 应尽量采用风冷式空调设备，空调设备的室外部分应安装在便于维修和安全的地方。
      - 空调设备中安装的电加热器和电加湿器应有防火护衬，并尽可能使电加热器远离用易燃材料制成的空气过滤器。
      - 空调及其相关设备应采用难燃材料或非燃材料。
      - 采用水冷式空调设备时，应设置漏水报警装置，并设置防水小堤。

6.4 环境安全

- **2. 机房内部设施安全**
  - 安全防护
    - 防水
    - 防静电
    - 火灾自动报警系统
    - 火灾自动灭火系统
    - 灭火器

6.4 环境安全

- **2. 机房内部设施安全**
  - 安全防护
    - 防水—安全措施
      - A级机房、低压配电室、不间断电源室、蓄电池室区域设备上方不应穿过水管。
      - B、C级机房、低压配电室、不间断电源室、蓄电池室区域设备上方不宜穿过水管。
      - 与机房无关的水管不宜从机房内穿过。
      - 位于用水设备下层的机房，应在顶部采取防水措施，并设漏水检查装置
      - 漏水隐患区域地面周围应设排水沟和地漏。
      - 机房内的给、排水管道应有可靠的防渗漏和防凝露措施。
      - A、B级机房应在漏水隐患处设置漏水检测报警系统。
      - 当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方。
      - A,B级机房计算机电气设备和线路采用活动地板下布线时，线路不得紧贴地面敷设。

6.4 环境安全

- **2. 机房内部设施安全**
  - 安全防护
    - 防静电

不同物体间的相互摩擦、接触会产生能量不大但电压非常高的静电。如果静电不能及时释放，就可能产生火花，容易造成火灾或损坏芯片等意外事故。

计算机系统的CPU、ROM、RAM等关键部件大都采用MOS工艺的大规模集成电路，对静电极为敏感，容易因静电而损坏。

6.4 环境安全

- **2. 机房内部设施安全**
  - 安全防护
    - 防静电—措施
      - 当插拔插件板或更换电子元件时，作业人员应放去人体上的静电荷。如佩戴“防静电手镯”。
      - 机房的内装修材料一般应避免使用挂毯、地毯等吸尘、容易产生静电的材料，而应采用乙烯材料。
      - 放置电脑的桌子下铺上抗静电垫子。
      - 为了防静电，机房一般要安装防静电地板。
      - 机房的安全接地应符合GB/T 2887中的规定。
      - 机房内应保持一定湿度，特别是在干燥季节应适当增加空气湿度，以免因干燥而产生静电。
      - 在容易产生静电的地方，可采用抗静电溶剂和静电消除器。

6.4 环境安全

- **2. 机房内部设施安全**
  - 安全防护
    - 防火：火灾自动报警系统
      - 对于火灾隐患，应建立完善的自动报警措施，最大程度的保护场地、设施和人身安全。
      - 火灾自动报警系统安全要求：
        - » A级计算机场地应设置火灾自动报警系统。
        - » B级计算机场地宜设置火灾自动报警系统。
        - » 计算机场地安全出口应设置指示标志。
    - 防火：灭火器
      - 计算机场地应配置灭火器。
      - 配置的灭火器类型、规格、数量和设置位置应符合国家现行标准和规范的要求。
      - 灭火所用的介质，不宜造成二次破坏。

6.4 环境安全

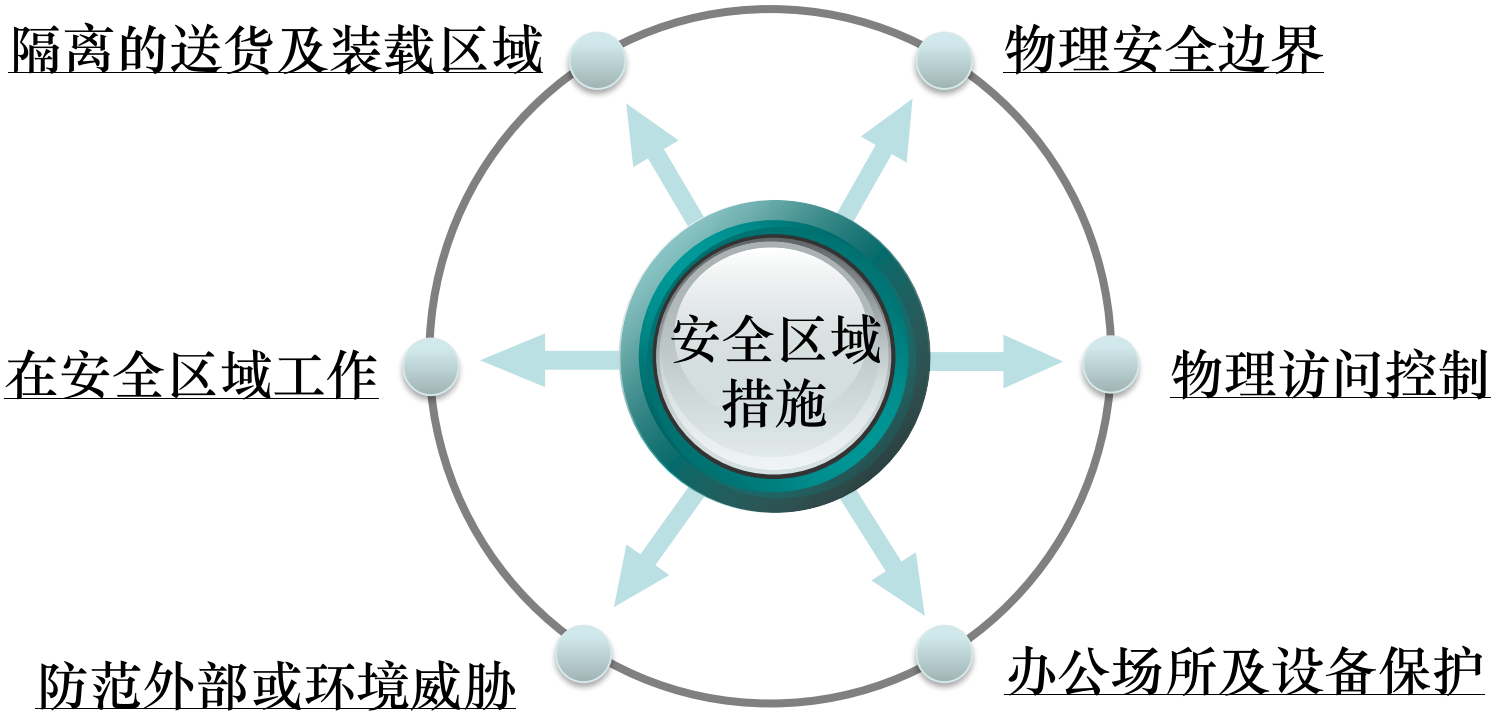
- **2. 机房内部设施安全**
  - 安全防护
    - 防鼠防震防雷击
      - 鼠害可能咬断电线网线；释放药饵。
      - 防地震或振动冲击；
      - 应有防雷击的避雷针。
  - 机房建设可根据计算机系统安全的需要，机房安全可按某一类执行，也可按某些类综合执行。
  - 综合执行是指一个机房内的不同设备可按某些类执行，如某机房按照安全要求可对电磁波进行A类防护，对火灾报警及消防设施进行C类防护等。

6.4 环境安全

- **3. 机房区域安全**
  - 区域安全是组织的业务场所和信息处理设施的物理区域的安全保护。
  - 安全区域建立：根据风险评估的结果，严格进出控制，对重要的信息系统基础设施进行全面的物理保护。
    - 安全区域：如系统机房、重要办公室，也可能是整个工作区域。
    - 信息处理设施可能受到的非法物理访问、盗窃、损坏和泄密的威胁。
    - 安全区域必须物理隔离

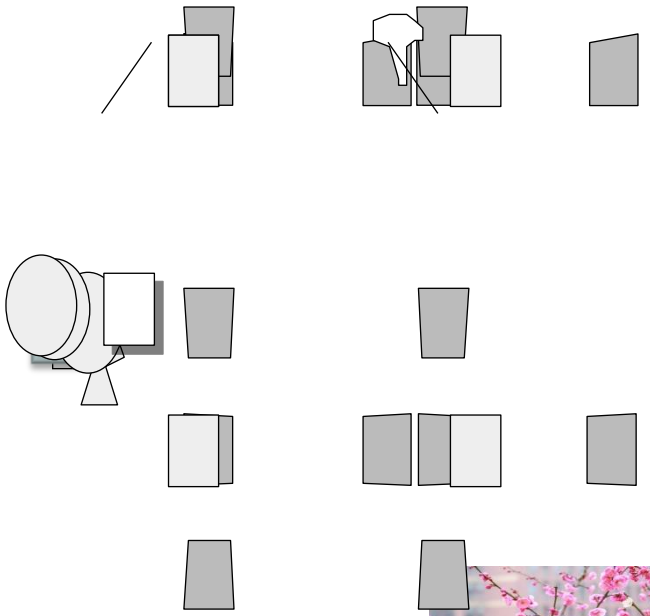
6.4 环境安全

- **3. 机房区域安全**
  - 安全区域



6.4 环境安全

- **3. 机房区域安全**
  - 安全区域：物理安全边界
    - 物理安全边界是设立的关卡，如围墙、控制台、门锁等。
    - 通过建立安全边界形成安全区域，以保护区域内的信息处理设施安全。
      - 智能锁
      - 智能锁+C级锁芯
      - 指纹锁+密码
      - 面部识别+指纹+手机PIN
      - 接触+非接触开关锁



6.4 环境安全

- **3. 机房区域安全**
  - 安全区域：物理安全边界
    - 锁芯标准

	标准	锁芯结构	钥匙类型	防开锁时间
A	国家标准	结构简单	十字平板、月牙形	防技术开锁 1 分钟
B	国家标准	电脑双排锁芯、双排月牙锁芯、双面叶片锁芯	平板钥匙，有双排弹子槽，带有不规则线条	防技术开锁 5 分钟，强扭工具 1 分钟
C	企业标准	边柱锁芯	平板型，带有凹形和 S 形	防技术开锁 270 分钟，强扭锁死

表 6 防破坏净工作时间 单位为分

级别	防钻	防锯	防撬	防拉	防冲击	防技术开启	密码式机械防盗锁防技术开启
A	10	5	10	10	10	1	1 200
B	15	5	15	15	15	5	1 440
C	30	30	30	30	30	10	—

新版《机械防盗锁》(GA/T 73-2015)标准

6.4 环境安全

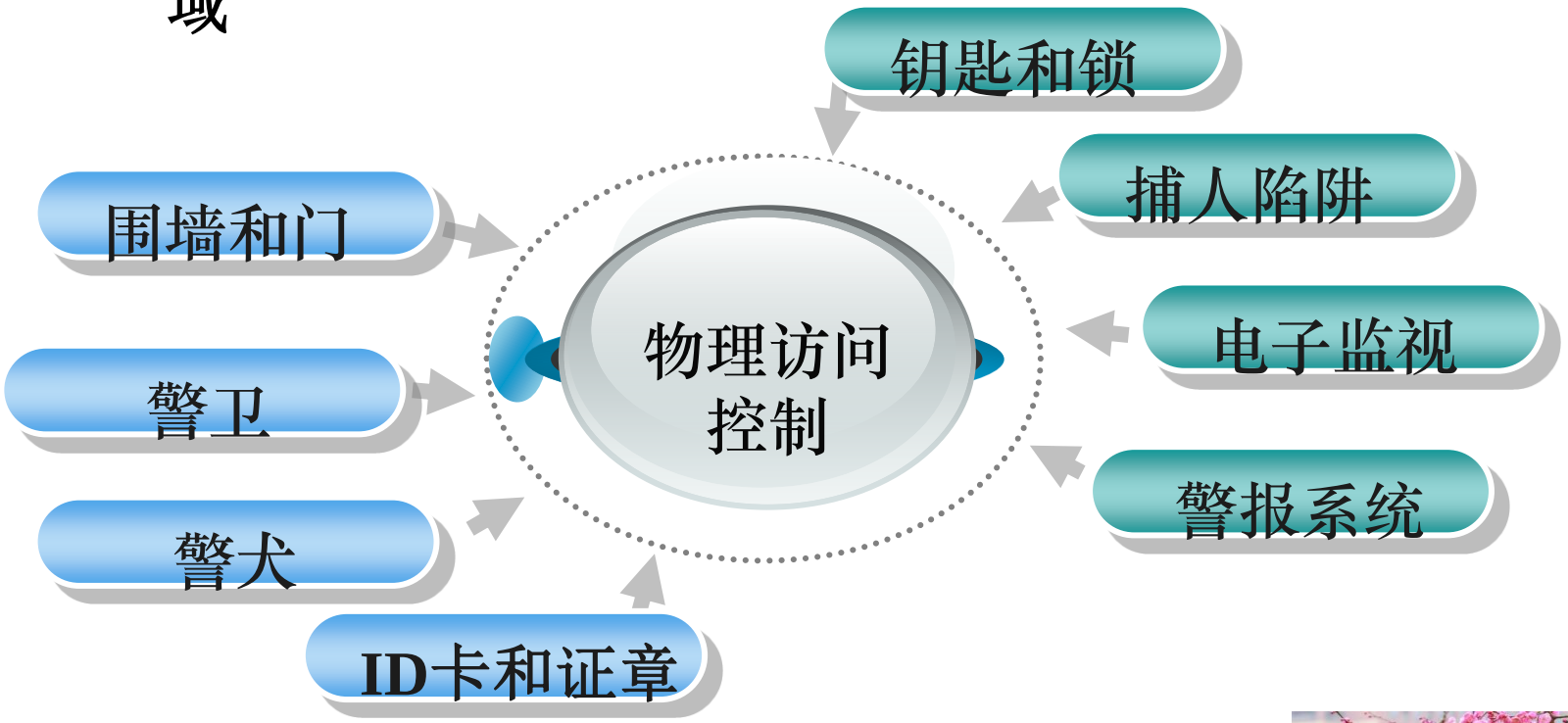
- 3. 机房区域安全
  - 安全区域：物理安全边界
    - 智能锁

6.4 环境安全

- 3. 机房区域安全
  - 安全区域：物理安全边界
    - 智能锁攻击
      - 无线脉冲干扰攻击
      - 无线黑盒发射干扰可以打开某些智能锁、汽车锁

6.4 环境安全

- 3. 机房区域安全
  - 安全区域：物理访问控制
    - 访问控制措施：确保只有经授权的人员进入安全区域



6.4 环境安全

- **3. 机房区域安全**
  - **办公场所和设备保护**
    - 机房办公场所和设备保护措施
      - 考虑相关的健康指南和安全法规、标准。
      - 关键设施应坐落在可避免公众进行访问的场地。
      - 适用时，建筑物不要引人注目，并且在建筑物内侧或外侧用不明显标记给出其用途的最少指示，以标示信息处理活动的存在。
      - 标示敏感信息处理设施位置的目录和内部电话簿不要轻易被公众得到。

6.4 环境安全

- **3. 机房区域安全**
  - **外部或环境的威胁防范**
    - 针对火灾、水灾、地震、爆炸、骚乱和其他形式的自然或人为灾害的物理保护，设计措施：
      - 危险及易燃材料应在离安全区域安全距离以外的地方存放。
      - 恢复设备和备份介质的存放地点应与主场地有一段安全距离，以避免影响主场地的灾难产生破坏。
      - 应当提供适当的灭火设备，并应放在合适的地点。

6.4 环境安全

- **3. 机房区域安全**
  - 安全区域工作
    - 安全区域中进行的工作有相应的控制方法及指导原则，以加强安全区域的安全性。
    - 措施：
      - 对安全区域的工作人员及被授权进入安全区域的其他人员的行为提出安全要求；
      - 通过规章的形式予以约束，要求在此工作的人员必须遵守。
    - 实施对象：工作在安全区域内的雇员、合同方和第三方用户，以及其他发生在安全区域的第三方活动。

6.4 环境安全

- **3. 机房区域安全**
  - 区域隔离
    - 卸载、装载货物区域隔离
    - 货物威胁
      - 某些犯罪分子将装有炸弹或细菌的信件邮寄给被攻击者，造成人身伤害和财产损失。
      - 商业机密窃取者可以伪装成送货者到组织的办公室或实验室窃取项目研发的技术资料。
      - ……
    - 运送人员威胁
      - 被运送的货物、物品本身或者运送人可能对存储区域内的重要信息资产造成威胁或损害。
    - 机密信息区域隔离
      - 送货和装载区域应加以控制，如有可能应与信息处理设施隔离，以避免未经授权的访问。

6.4 环境安全

- 3. 机房区域安全
  - 安全区域实施建议
    - 机房进出控制
      - 双向电子门禁系统
      - 门禁电子记录或填写出入记录单，记录进出人员和时间
      - 增设保安人员在门外值守；
    - 内和外部临近入口区域监控：
      - 安装摄像头、全范围覆盖
      - 外来人员进入由专人全程陪同；
    - 区域进行物理隔离
      - 对于系统较多、机房面积较大的单位应将机房按系统和设备的重要程度划分不同的区域隔离
      - 采用双向电子门禁系统控制，区域间的联通通道形成过渡缓冲区。

6.4 环境安全

- 3. 机房区域安全
  - 安全区域实施建议
    - 常见问题
      - 仅采用单向门禁系统；
      - 对人员进出缺少完整和严格的记录要求；
      - 机房通常没有安装监控设施。
    - 实施难点
      - 增加安全措施需要较大的资金投入；
      - 领导对区域安全的重视程度不够；
      - 较难实现完整实施的对有限区域安全访问控制。

6.4 环境安全

- **4. 机房区域安全测评**
  - **要求：**
    - 机房出入口应安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员；
    - 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；
    - 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
    - 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。

6.4 环境安全

- **4. 机房安全区域测评**
  - 方法形式：访谈、检查。
  - 对象：
    - 人员：物理安全负责人、机房值守人；
    - 机房：机房设施（电子门禁系统）、机房安全管理制度；
    - 值守记录：进入机房的登记记录，来访人员进入机房的审批记录，电子门禁系统记录，电子门禁验收文档或安全资质，电子门禁运行维护记录。

6.4 环境安全

- **4. 机房安全区域测评**
  - 实施访谈
    - 访谈物理安全负责人：了解控制机房进出的能力；
      - 如果业务或安全管理需要，是否对机房进行了划分区域管理，是否对各个区域都有专门的管理要求；是否严格控制来访人员进入或一般不允许来访人员进入；
    - 访谈机房值守人员：询问是否认真执行有关机房出入的管理制度，是否对进入机房的来访人员记录在案。

6.4 环境安全

- **4. 机房区域安全测评**
  - 实施检查
    - 检查机房安全管理制度：是否有关于机房出入方面的规定；
    - 检查机房出入值守记录：
      - 出入口是否有专人值守、是否有值守记录，进出机房的来访人员登记记录；是否存在电子门禁系统控制之外的出入口；
    - 检查机房进入人员身份鉴别措施：是否有机房人员的身份鉴别措施，如戴有可见的身份辨识标识；
    - 检查来访人员的审批记录以及记录保存时长：是否有来访人员进入机房的审批记录，是否保存足够的时间；
    - 检查机房区域划分是否合理：
      - 是否在机房重要区域前设置交付或安装等过渡区域；
      - 是否对不同区域设置不同机房或者有效的物理隔离装置（如隔墙等）；
    - 检查机房电子门禁系统是否有验收文档或产品安全认证资质；
      - 检查每道电子门禁系统是否都能正常工作；查看每道电子门禁系统运行、维护记录；查看监控进入机房的电子门禁系统记录，是否能够鉴别和记录进入的人员身份。

小结

- **物理安全是信息系统安全的基础**
  - **物理安全分为：设备安全、介质安全、环境安全（含区域安全）和人员安全四个层面**
- 区域安全是组织的业务场所和信息处理设施的物理区域的安全保护。

作业

- 1.移动存储介质的安全隐患有哪些？
- 2.电磁泄漏的技术途径有哪些？
- 3.如何保证设备安全？
- 4.如何保证介质安全？
- 5.区域边界访问控制措施有哪些？哪些区域需要隔离？