第二章

实体及硬件安全技术

2-1 计算机房安全的环境条件

实体及硬件安全是指保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（包括电磁污染等）破坏的措施和过程。实体安全是整个计算机系统安全的前提，如果实体安全得不到保证，则整个系统就失去了正常工作的基本环境。一般来说，这个基本环境是指计算机房及其设施。计算机房除必须满足计算机设备对温度,湿度和空气洁净度,供电电源的质量和电磁场和振动等项的技术要求外,还必须满足在机房中工作的人员对照明度,空气的新鲜度和流动速度,噪声等项的要求。同时由于计算机属于贵重精密设备，在有些部门中属于关键和脆弱的中心，所以，机房对消防和安全保密也有较高的要求。

2-1 计算机房安全的环境条件

2.1.1 计算机房场地环境选择

为计算机房选择一个合适的安装场所，对计算机系统长期稳定、可靠、安全的工作是至关重要的。

我们在选择计算机房场地环境时要注意：

（1）应尽量满足水源充足、电源稳定可靠、交通通讯方便、自然环境清洁的条件。

（2）应避开环境污染区，远离产生粉尘、油烟、有害气体等的区域。

（3）应远离生产或贮存具有腐蚀性、易燃、易爆物品的工厂、仓库、堆场等场所。

（4）应避开低洼、潮湿、落雷区域和地震频繁的地方。

（5）应避开强振动源和强噪音源，如车间、工地、闹市、机场等。

（6）应避开强电磁场的干扰，当无法避开时，可采取有效的电磁屏蔽措施。

（7）机房在多层建筑或高层建筑物内宜设于第二、三层，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。

（8）计算机房的位置应充分考虑计算机系统和信息的安全。

其他的注意事项可以参阅国标<<计算站场地技术条件>>(GB2887-2000)。这个标准是计算机场地建设的主要技术依据。

2-1 计算机房安全的环境条件

2.1.2 计算机房内环境条件要求

1.温度

2.湿度

3.洁净度

4.腐蚀性气体

5.静电

6.振动与噪音

7.电源

8.照明

2.2 实体及硬件的安全防护

实体及硬件的安全防护是针对自然、物理灾害及人为蓄意破坏而采取的安全措施与防护对策。通常包括防火、防水、防盗、防电磁干扰及对存储媒体的安全防护等。

2.2 实体及硬件的安全防护

2.2.1 三防措施（防火、防水、防盗）

1.防火：（1）要有合理的建筑构造，这是防火的基础。（2）完善电气设备的安装与维护，这是防火的关键。（3）要建立完善消防设施，这是减少火灾损失的保障。（4）加强消防管理工作，消除火灾隐患。

2.防水：机房防水工作是机房建设和日常运行管理的重要内容之一，应采取必要的防护措施：

（1）机房不应设置在建筑物底层或地下室，位于用水设备下层的计算机机房，应在吊顶上设防水层，并设漏水检查装置。

（2）机房内应避免铺设水管或蒸汽管道。已铺设的管道，必须采取防渗漏措施。

（3）机房应具备必要的防水、防潮设备。

（4）机房应指定专人定期对管道、阀门进行维护、检修。

（5）完善机房用水制度，有条件的机房应安装漏水检测系统

2.2 实体及硬件的安全防护

3.防盗： 常用的防盗措施有：

（1）放置计算机设备的建筑物应该比较隐蔽，不要用相关的标志标明机房所在地。

（2）机房门窗应具备防盗措施，如加固门窗，安装监视器等。

（3）机房内的各类贵重物品应配置具有防盗功能的安全保护设备，如各种锁定装置、侵入报警器等。

（4）严格出入登记制度，非本系统操作人员，一般情况下不准随意出入机房。

（5）加强机房管理责任制，建立建全设备器材出入制度。

2.2 实体及硬件的安全防护

2.2.2 电磁防护

1.电磁干扰： 所谓电磁干扰(Electromagnetic Interference, EMI)，是指无用的电磁信号或电磁骚扰对接收的有用电磁信号造成的扰乱。电气设备在运行过程中所产生的电磁干扰不仅会影响附近设备的正常运行，同时也会对人们的工作、生活和健康造成极大的危害。

2.电磁泄漏： 电磁泄漏是指电子设备的杂散(寄生)电磁能量通过导线或空间向外扩散。如果这些泄漏“夹带”着设备所处理的信息，就构成了所谓的电磁信息泄漏。

3.电磁防护措施：（1）屏蔽 （2）滤波 （3）隔离 （4）接地 （5）选用低辐射设备 （6）使用干扰器

2.2 实体及硬件的安全防护

2.2.3 存储媒体的访问控制

计算机系统中的大量信息都存储在某种媒体上，如磁盘、磁带、半导体、光盘、打印纸等。为了防止对信息的破坏、篡改、盗窃等事件的发生，就必须对存储媒体进行保护和管理，严格其访问控制。

1. 身份识别 ： 身份识别的目的是确定系统的访问者是否是合法用户，一般包含“识别”和“验证”两个方面。

2. 控制访问权限 ： 系统要确定用户对资源(比如 CPU 、内存、 I/O 设备、计算机终端等)的访问权限，并赋予用户不同的权限等级，如工作站用户、超级用户、系统管理员等。一般来说，用户的权限等级是在注册时赋予的。

3. 管理措施 ： 存储媒体安全管理的目标是：保证系统在有充分保护的安全环境中运行，由可靠的操作人员按规范使用计算机系统，系统符合安全标准。管理应紧紧围绕信息的输入、存储、处理和交换这个过程来进行。

除此之外，还应该健全机构和岗位责任制，完善安全管理的规章制度，加强对技术、业务、管理人员的法制教育、职业道德教育，增加安全保密和风险防范意识，以实现科学化、规范化的安全管理。

2.3 计算机硬件的检测与维修

在计算机系统的故障现象中，硬件的故障占到了很大的比例。正确的分析故障原因，快速的排除故障，可以避免不必要的故障检索工作，使系统得以正常运行。

2.3.1 计算机硬件故障的分析

计算机硬件故障是指由于计算机硬件损坏、品质不良、安装、设置不正确或接触不良等而引起的故障。其原因多种多样 ：

（1）工艺问题引起的故障

（2）元器件损坏引起的故障

（3）干扰或噪声引起的故障

（4）设计上造成的故障

（5）人为故障（计算机假故障）

2.3 计算机硬件的检测与维修

2.3.2硬件故障的检测步骤及原则

1.检测的基本步骤： 检测的基本步骤通常是由大到小、由粗到细。

2.检测的原则：

（1）先静后动

（2）先外后内

（3）先辅后主

（4）先电源后负载

（5）先一般后特殊

（6）先简单后复杂

（7）先主要后次要

计算机的检测维修方法很多，因设备的不同、组件的不同，各自有不同的特点，对以上原则应灵活运用，当故障原因较为复杂时，要综合考虑。

2.3 计算机硬件的检测与维修

2.3.3 硬件故障的诊断和排除

要排除硬件故障，最主要的是要设法找到产生故障的原因。一旦找到原因，排除故障就很容易了。下面介绍一些寻找故障原因常用的方法：

（1）清洁法

（2）直接观察法

（3）拔插法

（4）交换法

（5）比较法

（6）振动敲击法

（7）升温降温法

（8）程序测试法

总之，为了排除故障，首先要设法查出产生故障的原因。要能正确、迅速的查出故障原因，最主要的是要掌握基本原理，多参加实际工作，而且在方法上应从一些简单的检查方法入手，逐步运用复杂的方法进行检查。