第2章　信息中心管理与实体安全

本章导读

信息中心的主要任务就是提供高品质的服务，以辅助各单位妥善利用计算机设备，有效率地协助其工作的进展。为了达到此任务，信息中心一般除了具有高水准的人力资源服务团队外，还要有软硬件设备、预算以及空间环境等资源。本章将重点介绍信息中心在信息安全方面的管理，对信息中心其他管理有兴趣的读者请参考其他文件数据。至于“信息安全管理作业要点”的国际标准(ISO/IEC 17799)将留到第 16 章再做介绍。

实体安全(Physical Security)是信息中心安全管理的重要一环，也是计算机系统的基本外在安全要求。基于人力、经济以及其他因素的考虑，各机关的信息中心的安全防护措施不尽相同。平时，计算机机房人员与主管，除了应定期做好各种状况的处理演练及预防外，还应随时检讨、改进安全上的各项措施。

实体安全的重要任务就是保护信息系统外在的环境安全。计算机已运用到各行各业中，不容许片刻瘫痪。此外，歹徒(或入侵者)并不需要有特殊专业信息能力即可轻易破坏计算机的软硬件设备，实体安全的重要性可想而知。

典型的实体安全措施为防护、门禁管制以及防止直接的入侵或破坏攻击，一些制造商已经开发出可提高计算机安全性的产品。但许多安全上的缺失是由人为所造成的，如何避免因人为的疏忽而造成信息系统安全上的威胁，也是实体安全探讨的重点。

2.1　人力资源的安全管理

每个机关单位的信息中心组织架构不尽相同，但大体相似，如图 2-1 所示。

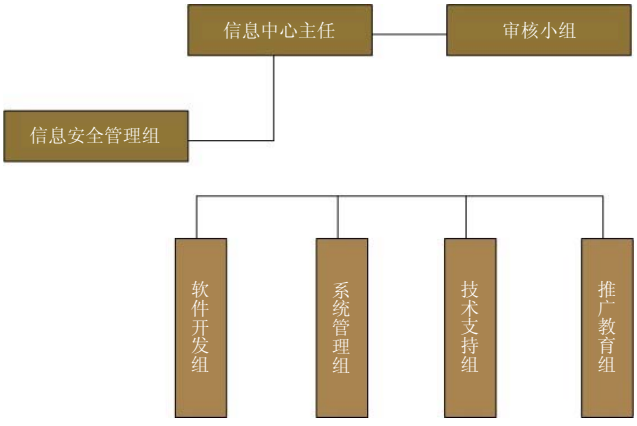

图 2-1　信息中心组织架构

除了中心主任外，下设 5 个小组：软件开发组、系统管理组、技术支持组、推广教育组以及信息安全管理组。另外，还有一个由跨单位相关人员所组成的信息审核小组。

2.1.1　软件开发组

软件开发组也称为系统开发组，主要的任务就是开发管理信息系统(Management Information Systems，MIS)，以辅助各单位工作的进行。由于一般管理信息系统都是相当复杂的，因此软件开发组必须以项目管理的方法以及系统分析与设计的技巧来规划、分析、设计，进而发展 MIS。尤其要注意数据库的设计，一定要有实体关联模式(ER Model)帮助了解关系表(Table)之间的关联性，以避免数据重复及不一致的现象。

完成了管理信息系统的开发后，务必要马上编写文件，包括软件设计文件、程序说明书、安装手册以及操作说明书。一般程序设计师最厌倦写文件，但为了日后方便系统维护，身为主管必须严格要求，否则一旦当初的程序设计人员离职，再次维护此系统将更为困难。当上述的文件已撰写完毕，除了主管审查外，建议再请其他没有参与此项目的相关人员阅读并操作，以确保文件的可读性及正确性。

软件开发组主要成员为系统分析师及程序设计师。程序设计师是否在设计程序的同时偷开一扇后门(Trap Door)是一个值得关注的问题，以下为软件开发组在安全管理上需注意的事项：

- 审核人员审核系统分析与设计文件是否有安全漏洞。
- 程序完成开发后，需由审核人员逐一审查，原始程序代码是否与系统分析与设计文件一致？是否有不相干的程序代码或后门程序？
- 由审核人员与程序设计师共同将原始程序代码编译成可执行文件。
- 审核人员必须定期审核程序是否被篡改。

2.1.2　系统管理组

系统管理组的主要任务就是让计算机设备及系统能有效率地正常运转。应用系统与数据库系统是否经常发生执行效率较低的问题？遇到这些问题时，该如何解决？系统效率不佳的原因牵涉到硬件、数据库设计架构、系统组态以及网络。如何以最经济、最快速的方式来提升系统效率，就是系统管理组的主要任务。

因此，系统管理员必须随时监控目前的使用情况，用户访问的速度是否过慢？若系统瘫痪(Crash)是否能在第一时间修复？另外，网络是否正常？是否过慢、负载过重？这些必须要加以注意。除此之外，系统管理组还有一些安全上的问题需注意：

- 用户申请使用权限的注册，需谨慎审核其身份。用户离职时，必须将其使用权限注销，这也是为什么机关单位离职的作业流程中，有一道关卡是必须通过信息中心主任签署的原因。信息中心主任会要求其中心成员将该离职员工的数据先备份(Backup)保存起来，然后注销其用户账户。

- 随时监视控制台(Console)，是否有不明身份的用户企图登录(Login)到本系统。
- 定期检查系统审核文件(Log File)是否有异常状况。
- 定期检查网络线是否在安全管线内(没有漏出)。
- 是否定期备份数据？备份数据是否放置于安全地方？是否加以管制？

2.1.3　技术支持组

技术支持组的主要任务就是解决用户使用计算机设备的相关问题，包括修复个人计算机。现在网络很普及，用户在报修或请求技术支持组服务时，除了以传真、电话报修或填写纸张申请服务表格外，也可利用网络。现在很多单位均已提供网络报修服务，避免了接电话或纸张公文流程过慢的麻烦。

维护工程师或技术员在维修计算机过程中，有时需要用户的账号及密码，一旦维修完毕应请用户即刻更改密码，以分清责任。

2.1.4　推广教育组

推广教育组的主要任务就是推广信息教育，让相关单位所有员工均能妥善使用信息中心的设备资源。除了计算机专业及网络能力训练外，还应加强财产权、理论与法律、计算机病毒的防患以及其他信息安全的观念。

2.1.5　信息安全管理组

依据 BS7799 安全管理标准，另外成立信息安全管理组，其主要任务就是负责整个信息系统的安全管理。将在第 16 章介绍 BS7799 标准。

2.1.6　审核小组

审核小组的主要任务就是审核信息中心设备与系统是否有安全上的漏洞，信息中心人员是否有安全上的疏忽或监守自盗等情况。审核小组通常不是信息中心专属单位，而是由其他非信息中心单位人员兼任，以避免人情上的压力。

2.2　空间环境资源的安全管理

建立安全无忧且运转正常的计算机使用环境是信息部门的主要任务之一。一般而言，导致计算机系统不能正常使用的原因除了网络断线及计算机系统故障外，计算机机房环境不良、停电、火灾、雷击、地震、水灾等都是主要因素。信息部门管理者对这些影响实体安全的因素应加以了解，并予以排除，否则会增加用户的怨言。天然灾害自然是无法避免的，但可事先完善规划以减少天灾所造成的损失，以下就计算机机房(尤其是大型计算机)的空间环境资源的安全管理做说明。

2.2.1　计算机机房环境不良

机房环境不良会导致计算机系统故障。这里所谓的机房环境除了有形的环境卫生外，无形的温度、湿度及灰尘更重要。

1) 温度

计算机系统对于温度是非常敏感的，温度过高会使计算机不能正常工作，还会伤害到存储介质。一般来说，大型计算机系统比小型计算机系统更易产生高温，因此计算机机房均需安装具有调温功能的空调系统，以维持计算机机房的温度在 20℃ 至 25℃ 之间。

2) 湿度

高湿度往往会造成电路板快速腐蚀、驱动器的磁头刮伤磁盘以及存储介质发霉破坏数据。计算机设备若长期不使用且环境湿度又很高，那么电路板将很快被腐蚀。因此，对于一般用户的个人计算机，应定期开机让电流可以流到电路板的每一条电路，借此产生热量以抑制高湿度。虽然冷气机具有除湿功能，但其效果不如除湿机，因此大型计算机的机房都会购置数台除湿机分装在各角落。计算机机房的湿度一般应维持在 40％至 60％之间。

3) 灰尘

驱动器的磁头在读写磁盘上的数据时，会极接近磁盘，比一根细头发还要接近。因此，在计算机机房里，即使用户掉落一根头发，都有可能导致磁头刮伤整个磁盘。灰尘也是磁盘的杀手，一旦灰尘飘落到磁头或磁盘上，在每分钟 7200 转的高速转动下，磁头将快速刮伤整个磁盘。一般计算机机房四面门窗除了要紧闭外，还需挂上窗帘，以减少灰尘及日晒。另外，还要购置空气滤清器，以防止灰尘飘散到计算机机房。

2.2.2　停电

计算机需要稳定的电源，若遇到停电或电力系统故障，计算机就会立刻停止运行，暂存在内存(RAM)中的数据将消失；硬盘的磁头在读写中途被迫退回起始点，由于瞬间快速退回，有时会对计算机硬盘造成很大的伤害。因此，一旦停电时应立即由另外一套电源即时供应。现在的计算机机房大多设置不间断电源供应系统(UPS)，以应付停电时的处理，在停电后还能继续供电数小时，在这数小时内应有足够的时间做好停电后的处理工作。

另外，电压不稳定也会导致计算机异常，电力线的电压位准在上下 10％内波动是常有的现象，有时候电力线的电压位准会超出 10%的上下限。当启动空调系统或大型的马达时，会使电灯泡瞬间闪烁，这就是由电力线的瞬时大电流所造成的。幸运的是，目前已有稳压设备可以解决上述的问题。

2.2.3　机房位置规划不当

计算机机房位置要远离会受电磁场干扰的地方，计算机机房所设置的地方，其周围环境不应该有如电视台、移动基站、广播电台及电力公司的变电所等具有高电磁波的场所。

机房内更要避免铺设地毯，因为地毯除了容易藏污纳垢外，还会产生静电，从而影响计算机的正常作业。还有一点要注意的是，网络线或数据线绝对要避免与电源线并列或放置在同一管线内，电源线通电后会产生电磁场，将干扰传送 0、1 数字数据的网络线或数据线信号，

偶尔会造成计算机系统莫名的瘫痪。

2.2.4　火灾

火比水更难以解决，原因在于反应时间较少。数分钟的时间已足够做安全的处置以及搬移部分设施，但要在短时间内搬移大量备份数据的硬盘或磁带是有困难的，所以平时应在硬盘或磁带上贴有颜色的标签，以分别标识其重要程度，如此将有助于紧急搬运时的有效性。幸运的是，随着移动硬盘的容量越来越大，价格越来越便宜，此问题已日渐不重要。另外，有些单位有实施异地备份的条件，可以更有效地避免因火灾造成数据损坏的情况发生。

信息中心一般都有一组执行关机(Shutdown)的顺序步骤，正常关机虽然需要一些时间来完成，但将使得未来开机时能够顺利进行。信息中心应有一套权责划分的计划，谁负责关掉系统，谁负责保护重要的文件，并且要建立职务代理人制度。

水并不适合用于计算机机房防火，事实上在计算机机房设置储水室反而会造成更多破坏。如果感应器故障误判失火导致喷水，会使计算机机房淹水，进而损坏磁性介质(如磁盘、磁带)及其他计算机相关设备。目前许多计算机机房都使用二氧化碳灭火器或自动喷气系统来抑制火灾扩散。但隔绝氧气对人体健康有影响，所以使用这些防护装置时，人员必须尽快离开。平时有完善的计划及加强模拟演练，一旦发生火灾才能有效率地救灾及迅速搬离重要数据。

2.2.5　雷击

雷击会产生超强电流，若不引导到地表，就很容易发生火灾及烧毁设备。美国每年都会发生上百次森林火灾，绝大部分都起因于闪电、雷击。一般高楼大厦在建筑时都会设计并安置避雷系统，以避免被闪电雷击。

另外，计算机的电源线是三线式(三个插孔的插座)，分别是火线、零线及地线。地线的用途是保护计算机设备，避免因闪电雷击产生超强电流而烧毁计算机设备及电器用品。

2.2.6　地震

世界上每年都会发生大小规模不一的地震。自从 1976 发生唐山大地震、2008 年发生四川大地震后，国人几乎闻震色变。如果当地处于高地震带，那么对于计算机机房及设备的防震能力应格外重视。

2.2.7　水灾

水灾可能是由下雨、潮汐或水管破裂等因素所造成，不管何种方式皆可能造成重大灾害。

水灾会带来泥沙及岩层，这种情况通常有充裕的时间执行正常关机程序，若紧急关机则会遗失正在执行中的数据。机械装置可能会被泥沙及岩层所破坏，硬件设备可以重新置换，但存储在磁性物质上的数据及程序将永久丢失。

因此，信息中心工作人员必须在最短的时间内将重要的数据搬至离地面较高的地方，硬盘或磁带加装防护壳并放置于腰与眼之间的位置。另外，将信息中心建于高于地面位置(三楼以上)可解决洪水导致的水位上升问题。

2.3　硬件设备资源的安全管理

为了给用户提供更高的服务品质，信息中心首先要构建一个安全且正常运转的计算机设备与系统。如何保护计算机主机、周边设备以及相关设备(如空调、稳压器、除湿器、防断电设备、防尘器等)的正常作业，一直是硬件设备资源的重要安全管理工作。一般而言，导致计算机硬件设备与系统不能正常使用的主要原因有网络断线、不正常使用或计算机系统故障等。

2.3.1　计算机系统故障

任何设备都会发生故障，只是发生的频率不同。信息部门除了平时做好计算机及环境维护以减少计算机系统故障外，还应该要有计算机系统故障的紧急应变措施，务必在最短时间内使计算机系统能正常运作。“预防重于保养，保养重于修理”，因此，信息中心应在平时就做好预防与保养的工作，以减少硬件设备的故障率，并延长硬件设备的寿命。

如果不幸发生灾害而导致计算机毁坏，一切工作因此停止，将可能造成极大的损失。因此，许多计算机厂商都有备用的计算机系统，并能在 24 小时内送至发生灾害的地点，或者直接从生产线运送而来。但这些新搬来的机器设备若只有操作系统，而没有信息应用系统及相关数据，那么这些机器设备还是无用武之地。因此，必须在最短时间内将所有应用软件及数据安装完成，以恢复计算机正常的运转。

假如某单位对计算机的依赖程度很高，不能承受超过数小时的系统瘫痪，则当初规划计算机设备时就必须考虑采用容错系统(Fault Tolerance)，也就是有两套系统同时运转，一旦有一套系统发生故障，就启动另外一套系统，使得工作不会中断。值得注意的是，除了系统有两套外，数据存储也需存放在两套不同设备中，否则若仅存储一套数据于某存储设备，一旦该设备出现故障，即使有两套计算机系统也无济于事。然而，容错系统价格不菲，有必要考虑其经济效益。

2.3.2　网络断线与网络的品质检测

计算机通信网络必须通过适当的传输介质来建立。例如，使用公共电话系统的语音线路、拨接式数据线路、公众分封交换网络及通信公司的点对点专用数据电话。这些传输介质的实体防护较难达成。

为了避免当数据在线路传输时线路遭人破坏且数据遭人窃听，线路应深埋在地底，甚至可以在线路铺设完成之后在两端安装密封压力显示装置，如果压力发生变化，则可以追踪此线路是否已遭人破坏。当然，这种做法要付出相应成本。另外，无线电传输的价钱虽较为便宜，但容易遭人窃听而不易察觉，基于安全考虑，若使用无线通信需有额外的保密措施。

现在每一台计算机几乎都连上网络，用户也几乎每天都需要通过网络来浏览网站信息、接收或发送电子邮件、加入网络聊天及下载一些软件。试想用户正在使用网络时，网络突然断线或有杂乱信号，这将对用户带来不好的感受，并对信息部门有不好的印象。因此，如何维持网络畅通是信息部门最基本的任务之一。这里所谓的网络畅通包括网络正常连线没有断线、网络正常流通没有阻塞及网络正常传输没有杂乱信号。信息部门规划网络的最高指导原

则就是要确保网络畅通。即使已构建好网络，信息部门还是要定期监视每一节点的网络流量状况(可使用网络分析仪)，以作为调整企业网络的规划布置的依据。

网络品质一直是用户对信息部门服务水平的一项重要指标，信息部门除了可以使用网络分析仪来规划及监视网络品质外，还有一种更简便的方法可以测试网络品质，这种方法使用到网络所提供的 Ping 公用程序。例如，有一台位于安全中心网域的计算机，其网络地址为140.120.19.29，现在想要测试安全中心与某教育部门的计算机主机间的网络品质，安全中心的 IP 地址为 140.120.1.20，教育部门的 IP 地址为 140.111.34.60，那么用户可以在 140.120.19.29 的计算机中发出 Ping 指令，其测试结果显示如下：

```
>ping isrc.nchu.edu.tw [Enter]
Pinging isrc.nchu.edu.tw[140.120.1.20]with 32 bytes of data:
Reply from 140.120.1.20：Bytes=32time<1ms TTL=242
Reply from l40.120.1.20：Bytes=32time<1ms TTL=242
Reply from 140.120.1.20：Bytes=32time<1ms TTL=242
Reply from 140.120.1.20：Bytes=32time<1ms TTL=242
```

上面的 Ping 指令是以 32 位字节(Bytes)的数据做测试，并重复 4 次测试，从 140.120.19.29 的计算机传送 32 位字节到安全中心网站的主机，收到后再回应给 140.120.19.29 的计算机，其传输时间均低于 1ms，表示 140.120.19.29 的计算机与安全中心主机之间网络连线维持在正常水平。上面回应信息中的 TTL(Time To Live)为可再经过的网站个数，每经过一个网站转接，TTL 数就递减 1，TTL 的初始值为 255，因此由 140.120.19.29 的计算机到安全中心的计算机主机，总共经过 14 个(255-242+1=14)网站。

接着，继续在 140.120.19.29 的计算机中发出 Ping 指令测试到教育部门的网络状况，其测试结果显示如下：

```
>ping www.edu.tw [Enter]
Pinging www.edu.tw [140.111.34.60] with 32 bytes of data
Request timed out
Request timed out
Request timed out
Request timed out
```

在上面的 Ping 指令中，从 140.120.19.29 的计算机传送 32 位字节数据到教育部门网站的主机，但一直没有收到教育部门网站主机的回应，Request timed out 表示网络没有办法在合理时间回应，也就是说 140.120.19.29 的计算机与教育部门网站主机之间连线有问题。由于之前已测试 140.120.19.29 的计算机与安全中心主机之间的网络连线正常，因此可以推断网络连线问题出在安全中心主机与教育部门网站主机之间。当 Ping 的网络地址不存在时，则回应的错误信息如下：

```
>ping www.nchu.com.jp[Enter]
Bad IP address www.nchu.com.jp
```

Ping 指令还有其他常用选项(Option)功能，如：

```
>ping -t isrc.nchu.edu.tw [Enter]
```

表示会一直发送数据测试，一直到由用户中断它(按 Ctrl+C 组合键)才会停止测试。此功能通常用于长时间监测。

```
>ping -n 10 isrc.nchu.edu.tw [Enter]
```

表示会做 10 次测试，一般不指定时仅做 4 次测试。

```
>ping-l 64 isrc.nchu.edu.tw [Enter]
```

表示每次以 64 位字节数据做测试，一般不指定时为 32 位字节。

```
>ping-i 10 isrc.nchu.edu.tw [Enter]
```

表示此测试仅能通过 10 个网站，若超过 10 个网站尚未到达，则停止此次测试，一般不指定时为 255。

前面测试 140.120.19.29 的计算机到安全中心的计算机主机时，总共经过 14 个网站，因此，下列 Ping 指令会有不能抵达到 isrc.nchu.edu.tw 的信息。

```
>ping -i 4 isrc.nchu.edu.tw [Enter]
Pinging isrc.nchu.edu.tw [140.120.1.20]with 32 bytes of data:
Reply from 140.128.250.254：TTL expired in transit
>ping-W 1000 isrc.nchu.edu.tw [Enter]
```

表示此测试等待对方网址回应时间为 1000ms，若超过 1000ms 仍未回应，则显示下列信息：

```
Request timed out
```

表示两个网站间的传输时间已超过预定的 1000ms，可能的原因有以下 3 种：

- 两个网站间的路径或网站目前正处于堵塞或故障状态。
- 对方网站目前是关机或故障状态。
- 对方网站目前很忙碌。

2.4　软件设备资源的安全管理

这里所谓的软件设备资源包括操作系统(Operation System)、公用程序(Utility)或工具(Tool)、管理信息应用系统以及用户数据。因此，软件设备资源的安全管理包括了上述的安全管理。

2.4.1　软件程序的安全管理

对于操作系统的安全管理，信息中心必须随时注意内存的使用情况，内存是否有被非法使用或藏入病毒程序，其他系统资源是否被非法盗用等都需加以预防。

公用程序或工具使用户更方便地使用计算机系统，有些公用程序或工具可以直接或间接

存取系统资源，信息中心对于系统提供哪些公用程序或工具，以及有哪些权限必须要加以了解，并做完善的安全管理。

必须要明确界定管理信息应用系统的使用对象是谁，什么人可以使用什么信息系统，信息中心必须要明确设定，以避免有人误用此系统而造成数据的外泄或数据不一致。

2.4.2　数据的备份

数据也可视为企业、组织的一项重要资产。对于许多企业组织而言，数据不但具有价值，而且常常需要被妥善地保护。因此，为了防止数据外泄或篡改，应对的策略将采用第 5~8 章所介绍的密码技术来保护。本节将重点放在如何对数据妥善保存，降低数据损坏或遗失的风险。

计算机系统的数据一直在变更，为了防止数据因为硬件或病毒等因素造成损坏或遗失，必须做好完善的数据备份(Backup)工作，使存储的数据尽量保持在最新的版本。

所谓数据备份就是将全部或部分数据复制，万一系统损坏或数据有遗失时，可再重新录制，使系统尽可能恢复到损坏前的状态。因此，正确做好数据备份可以大大地减少因数据损坏所造成的损失。数据备份的范围依数据的拥有者可以大致分为企业组织的数据备份及个人数据的备份两种。下面分别针对这两种备份进行说明。

1．企业组织的数据备份

企业组织的数据备份是指企业或组织针对其信息系统所产生的数据来做备份。由于这些数据的内容可能是顾客的基本数据、会计数据或者是交易数据，因此对企业相当重要且具有很大价值。所以一般企业的信息系统均会定期地对其数据做一次备份，以防数据损坏或遗失。

但是，由于企业每天新增或修改的数据量相当庞大，如何做好数据备份便成了一门深奥的学问。总的来说，企业数据备份的策略根据数据备份的频率来区分，可以分为日备份(Day Backup)、周备份(Weekly Backup)、月备份(Monthly Backup)、隔月备份(Bimonthly Backup)、季备份(Quarterly Backup)和年备份(Yearly Backup)等。顾名思义，日备份就是每天对企业内部的数据做一次备份，周备份是每周做一次备份，月备份则是每个月进行一次备份，隔月备份则是每两个月进行一次备份，季备份则是每季进行一次备份，而年备份则是每年进行一次备份。

针对这几种备份策略来说，日备份的可靠度最佳，因为在最差的状况下，它最多只会遗漏掉一天的数据，但一般来说企业所需备份的数据量均相当庞大，每天做一次备份所需花费的时间、费用也会相当可观。因此，根据备份数据的重要性，又可延伸出以下 3 种不同类型的数据备份策略。

1) 完整备份(Completely Backup)

完整备份是每次做备份时均将要备份的数据(包括数据、应用系统程序、操作系统和系统程序)完整地复制一份至存储介质上。它的优点是可靠度高，但当数据量很大时，完整备份是很耗时间的，且要花费较多的空间来存储备份数据。这种备份通常用于间隔时间较长的备份，例如年备份。

2) 选择式备份(Selective Backup)或差异备份

有别于完整备份将数据完整地复制一份，选择式备份(或称差异备份)只在第一次备份时做完整备份，以后要备份时只把从上次备份到目前有改变的文件(新增及更新)进行数据备份。在这种情形下只有某些有更改的数据才必须做备份，所以这一类型的备份方式可以缩短备份的时间并减少所需的存储空间，但是它的缺点是可靠度较差，一旦某一次差异备份的数据损坏或遗漏，系统将无法正确地恢复。

3) 回转式备份(Revolving Backup)

回转式备份是指最近的备份数据会把以前备份的旧数据覆盖掉。例如，以每月做一次完整备份来说，这个月新备份的数据就可以覆盖掉上个月备份的旧数据，它的好处是可以节省备份所需的存储空间。

这 3 种备份方式常常是可以交替使用的，以一个大型企业常见的备份策略为例。通常一个大型企业因为需备份的数据量相当庞大，做一次完整备份可能需要长达一天的时间。针对这种企业，不可能每月都做一次完整备份，但又需要兼顾系统的可靠性。因此，一个实用的作法是每年做一次完整备份，而每月只做差异备份，如此一来就可以大大地减少备份所需花费的时间。

此外，还可以搭配回转式的备份方式，企业可以准备 12 个备份用的存储介质，依序编号为 D1，D2，…，D12，每个月就依序使用一个存储介质。一年过后，新月份的备份数据就可以覆盖去年同月份所备份的旧数据，每一笔数据都在系统中保存一年。当然实际的备份策略视企业的实际需求而定，如果企业中的数据需要保存较久的时间，那么回转式备份所需要的回转周期就需要较长的时间。

另外需注意，存储备份数据的位置应远离计算机机房，假如灾害发生时备份的数据被毁坏，则备份等于白做，重要的计算机机房应该在远处设置一个存储备份数据的仓库，最好处在不同栋大楼或至少需有数百米的间隔，这样一来灾害发生时可避免波及备份的数据。不过，由于上述备份方式无法将数据完全恢复，也无法让损坏的系统尽快地恢复以继续服务用户。因此，一种被称为异地灾难恢复(Disaster Recovery)的概念产生了。

异地灾难恢复是当信息系统的原所在地发生灾难，从而造成系统无法复原的损坏后，希望可以在最短的可接受时间内，让异地的灾难恢复系统能部分或完全地恢复原系统所能提供的服务，将灾难对用户的影响降至最低。为了满足此概念，异地灾难恢复有以下两个重要的特性。

1) 异地存放

为了避免灾难造成原设备及灾难恢复设备同时损坏，灾难恢复设备必须放置在离原设备较远处(至少 30 公里)才有意义。例如，原设备可以放置在北部地区，而灾难恢复设备可以放置在南部地区，如此一来，即使发生地震，也很难同时对这两个地区的设备造成损坏。

2) 同步传输

由于原设备与灾难恢复设备是异地存放，所以两者之间的数据传输必须通过专线或高速网络来进行。除此之外，希望系统尽可能地恢复到原系统损坏时的时间点。因此，在做好数据的备份传输时也必须做到同步传输，也就是说让所恢复的数据与原数据的落差越小越好。

在设置异地灾难恢复机制时，还必须考虑到数据备份存储系统必须不占用主机系统资

源，以及数据在网络上传输时必须做适当的安全防护措施这两个方面。

虽然设置一个异地灾难恢复机制所需的代价很高，但异地灾难恢复的概念已渐渐被许多企业所接受，并成为企业在做持续经营规划时极重要的一环。

2．个人的数据备份

由于网络的普及，使得计算机病毒有了绝佳的传染途径，再加上个人用户对病毒的防护措施做得并不严谨，因此个人数据遭到计算机病毒破坏的新闻时有发生。为了确保数据的安全性，个人数据备份的观念越来越受到重视。个人数据备份是指针对个人重要的数据来进行备份，相较于企业的备份数据，个人的备份数据相对来说要少了许多。

另一方面，随着光盘、移动硬盘及刻录设备的价格日益低廉，其使用率与普及率越来越高，使得移动硬盘及光盘非常适合用来作为个人数据备份的存储介质。因此，在备份个人数据时，用户大多会采用完整备份的策略，将所需备份的数据存放在移动硬盘或光盘等存储介质上。至于执行备份的频率则视个人需要而异，可以是日备份、周备份或月备份等。

上述的个人备份方式在自己的办公室或主机前或许适合，但若出差在外，所需要的数据若要随时带着走将会非常不方便，而且数据在备份时也需要刻录设备或存储介质。如果可以为用户提供一个网络存储设备，让用户可以通过网络存取个人数据，若有数据要备份也可以直接通过网络做异地备份，将可以有效解决个人数据备份的问题。

例如，个人移动办公室(Personal Mobile Office，PMO)可以为用户提供一个网络存储空间来存储个人数据，用户只要通过网络便可以存取其个人数据，相当便利。此外，个人移动办公室通常还提供电子邮件、手机短信、即时信息等服务，若结合无线通信技术，以后不管用户在哪里，都可以通过笔记本电脑、PDA、智能手机等移动设备随时存取所需的数据，并处理公司或个人事务。

在个人数据备份的安全考虑方面，若所备份的数据是具有机密性的，那么存储备份数据的存储介质(如光盘、移动硬盘以及硬盘等)就必须做好妥善的安全控管。

网络存储机制同样也需要安全的管控机制。例如，当某一用户通过网络要存取其个人数据时，系统必须先验证该用户的身份，数据在网络上传输也需要经过加密以避免遭到他人窃取。若系统能做好相关的安全措施，那么网络存储机制也可作为个人数据备份的一个良好解决方案。

2.4.3　敏感介质的处理

有很多重要数据均存储在各种介质(如磁盘、光盘、磁带或报表)上，一旦这些介质因故(如报表尚未印刷完整)要丢弃时，就必须先将介质上的数据销毁，否则会有泄漏机密的危险。常用的各种销毁设备如下：

1) 碎纸机

碎纸机由来已久，政府机构、银行以及其他需要处理大量机密数据的机关，一定要有碎纸机以便将印有机密数据的废纸销毁。有些碎纸机也可用来粉碎磁盘、磁带等介质。

2) 磁性数据的清除

当执行 ERASE 或 DELETE 命令时只是改变目录的指针(Pointer)，机密的数据内容仍然

留在磁盘上并未实际清除，只要稍加分析目录的结构便可恢复原状。将磁盘或磁带重写(Overwrite)多次才可确保永久清除此磁性介质上的机密数据。

3) 消磁物体

磁性物质会破坏磁场，进而破坏磁盘或其他磁性存储介质。要消除磁性介质上的机密数据，消磁是最快的方法。

2.5 侵　入　者

除了前面所谈人力资源、空间环境资源、硬件设备资源及软件设备资源的安全管理外，还必须要有人员进出机房的管理。一般非法侵入者(Intruder)主要有以下 3 种目的：盗窃计算机或数据、破坏计算机以及阅读机密数据。

1) 盗窃的防止

偷窃整个大型计算机是困难的，像 IBM 308x 或 43xx、DECVAX 这样的计算机，不仅带走它是困难的，要找一个买家也很困难，另外安排地点设置及放置机器也需要特殊的帮助。打印记录的报表、磁盘、磁带则是比较容易被带走的。假如被成功带走，可能要经过一段长久时间才会发现。被设计成小巧且可携带的个人计算机、盒式包装的磁盘、移动硬盘、光盘及磁带更是携带方便，所以这些东西可以很隐蔽地被带走。有 3 个方法可以防止遭窃：进入的管制、禁止携带以及外出的检查。

最古老的门禁管制方法是派驻一个 24 小时的轮值的守卫，守卫必须要认识所有准入人员，或是检查证件，但是职员可能会忘带或遗失证件，离职或假造证件都会造成管理上的问题，除非守卫记录所有准入人员，否则当问题发生时将无法知道谁是作案者。

第二种古老的门禁管制方法是用“锁”，此种方法比守卫更简单、花费少且更容易管理，但是钥匙不可以遗失且不容易被复制。

有许多信息中心使用磁卡(或 IC 卡) ，比较好的磁卡是利用电子电路封装在磁卡里面，如此将更加难以复制磁卡，有了磁卡可方便地记录何时何人进入计算机机房，万一磁卡掉了也可更改磁卡检测装置的密码，使遗失的磁卡自动失效。

2) 防止携出

防止偷窃的最简单方法是将计算机机房门窗锁好，这种方法虽好，但却会使合法用户不易于使用，对于偷窃者打破门窗或敲开门锁也无法防止。

防止偷窃的 4 个方法分别是：加重、粘牢、加锁及警铃，这些方法都可以防止计算机机房的东西被偷窃，然而加重和粘牢难以决定是否恰当，有些物品为了搬运及换置的需要，粘牢并不妥当。

3) 外出检测

诸如个人计算机、打印机、终端机这些设备，它们是可防止被携出的。只要改变磁盘的包装使它们不易被使用即可。其他检测偷窃的方法是在被保护的物品上加上特殊的标记，有些制造厂商在磁盘、磁带上加装无线电发射器，偷窃者搬离这些物品至外面时检测器会触发警铃，因此可迅速将偷窃者捉到。

4) 人员进出管制

防止偷窃的最保险方法是使偷窃者远离设备，不论偷窃者还是内贼或外贼，人员进出管制设备必须阻止非法用户，并且要记录授权用户的使用情况。

2.6　计算机实体安全的评分与建议

信息中心所在的建筑物的防护设施是否完善及场所是否合乎理想？信息中心的安全管理是否完备？以下是一些计算机实体安全的评分与建议：

1．建筑物场所位置的考虑

- 计算机设备位置是否远离发电厂、变电所、广播电(视)台或电信基站等。
- 计算机设备位置是否不易淹水。
- 位置及其计算机设备是否防盗、防灾、防震、避雷、防尘、防高温、防湿、防鼠、具备空调、抗磁、有门禁管制。

2．行政管理方面

- 对进出主机房人员的管制方式及身份的限制方式。
- 在厂商进行维护时陪伴人员的身份确认。
- 对于持有超级用户通行证密码的人员的管理方式。
- 信息中心人员有意见时反应的渠道是否顺畅。
- 信息中心人员离职时的处理程序。
- 中心人员职务代理人员制度。
- 对系统维护的措施。
- 对资源的保险措施是否有明确制度。

3．系统管理及软件安全方面

- 操作系统是否派专人管理。
- 系统的备份多久执行一次。
- 对于计算机病毒如何处理。

4．计算机操作及数据安全方面

- 计算机设备操作训练及信息安全相关课程。
- 计算机设备操作程序是否有说明文件。
- 操作人员、值班人员的安排方式。
- 文件、磁盘、磁带的报销及销售管制。
- 计算机系统各设备及通信设备的检查测试。

- 对于使用的资源信息的各级分类情形。

另外，为强化各机关的信息安全管理能力，应建立安全及可信赖的电子化政府，此处制定“各单位信息安全管理要点”，此要点可作为各级信息中心在做信息安全管理时的参考依据。下列简要列出此要点的一些实施成效评估事项：

- 信息安全政策制定。
- 信息安全权责分工。
- 人员管理及信息安全教育训练。
- 计算机系统安全管理。
- 网络安全管理。
- 系统访问控制管理。
- 系统发展及维护安全管理。
- 信息资产安全管理。
- 实体及环境安全管理。
- 业务持续运作计划管理。
- 其他信息安全管理事项。

除此之外，拟订安全外部审核表，此表将所有与安全有关的人员、应用系统、硬件设备、网络设备及环境设备等相关设施，均纳入审核范围内，审核项目分为风险评鉴及管理、信息安全政策、组织安全、资产分类、人员安全、实体安全与环境安全、通信与作业管理、访问控制、系统开发与维护、营运持续管理及符合性 11 项。根据此表，各单位可以自行评定其是否符合信息安全的规范，此审核结果也可以帮助各单位来了解其信息安全的弱点及威胁，进而改善其信息安全管理。

2.7　参 考 资 料

关于实体安全，感兴趣的读者可以进一步阅读 James Arlin Cooper 编写的 *Computer & Communications Security* (McGraw-Hill 出版)。

2.8　思 考 练 习

1．列举 5 项影响实体安全(Physical Security)的种类。

2．列举计算机机房内可以改善实体安全的 3 项设备。

3．什么是异地灾难恢复？其优缺点是什么？

4．使用容错系统可以避免因计算机瘫痪而影响作业，这对于停电是否有用？请说明。

5．信息中心组织架构中包含哪些机关单位？其中每个单位的主要任务是什么？

6．数据对企业来说无疑是一项重要的资产，因此企业都会将数据做备份处理，有哪 3

种不同形态的数据备份策略？

7．若有一台计算机想要测试与南京大学(www.nju.edu.cn)的计算机主机间的网络质量，应采用何种指令？

8．请用 Ping、Tracer 软件或网络分析仪来监测网络品质，写出所有的过程，并对此实验结果说明您的看法。

9．假设您是某家银行的信息部门主管，银行中每日的交易数据均很重要且数量庞大，拟定一套适合此银行的信息备份策略，并解释拟定这些策略的理由。

10．计算机机房发生火灾时，应如何处理？请拟定一个标准作业程序。

11．就企业或机关单位的项目，讨论数据备份的策略：

- 先了解企业或机关单位的规模(人力及投资额)、信息化程度、每天交易数据量、所有文件数据量。
- 已知空白 CD 一片 2 元，容量 800MB，复制文件每秒 10KB。
- 已知 250GB 移动盘单价 200 元，复制文件每秒 20KB。
- 就您的策略，分析其人力、成本、风险时间。