# 计算机系统灾难成因分析及灾难备份概念

范传东 （中国建设银行总行 科技部 100810）

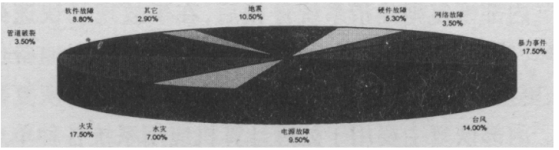
## 一、前言

大型计算机系统灾难备份在发达国家是一个非常活跃的研究领域。而在我国，由于资金、技术、人材等各方面的原因，我国计算机系统灾难备份的研究和实践仍然是一个薄弱的环节，一旦因自然灾害、设备故障或人为因素等原因引起的计算机系统停顿、数据丢失等，导致业务处理长时间中断，将会带来巨大的经济损失和社会影响。现就计算机系统灾难的成因、影响进行分析，并就建立灾难备份系统的必要性与读者探讨。

## 二、计算机系统灾难成因分析

造成计算机系统灾难的事故原因有自然灾害、基础设施的突发性事故、计算机系统故障和各种人为因素等。来自权威部门的资料统计，1998 年中世界范围内计算机灾难占比如下图所示：

由图可以看出，火灾、地震、台风、水灾、雷击、暴力事件、软件故障等引起的计算机灾难占了很高的比重。有些灾难事件可以预测，如台风、洪水等，可以提前采取预防措施，减少其影响和损失；有些灾难则是突发性的，来不及作出任何反应，可能对运行系统造成毁灭性打击。火灾、地震等可以直接毁坏机房基础设施，破坏计算机系统的正常运行环境；台风、水灾、雷击等可以造成电力、通信系统中断；而暴力事件等除可能破坏机房场地、硬件设备外，还可能造成关键业务数据大量丢失；软件故障等则可能使运行系统长时间无法正常工作。以上所述灾难的发生都将对系统应用部门本身带来直接或间接的损失，后果不堪设想。直接损失一般包括基础设施损失、计算机系统与网络设备损坏、环境设施遭到破坏、人员伤亡等；间接损失一般包括因计算机应用系统停顿造成的经营收入的减少，因信誉下降导致客户减少或资金转移而引发的间接收益下降，市场份额下降，潜在客户的流失，因业务无法正常进行导致的罚款及客户诉讼费及索赔费用等。而随着计算机应用系统停顿时间的加长，灾难损失将呈现出快速上升趋势。




© 中国科学院软件研究所 http://www.c-s-a.org.cn

充分认识各种灾难的危害性,认真分析计算机系统的灾难隐患及各种灾难对计算机系统安全运行带来的影响,合理估计资金投入与损失,对于选择计算机系统灾难备份模式与策略具有重要的意义。

## 三、灾难备份的相关概念

**1. 灾难备份**

灾难备份是指为了减少灾难发生的概率,以及减少灾难造成的损失而采取的各种防范措施,包括灾难预防和灾难恢复等。

**2. 灾难预防**

是指为减少计算机系统灾难发生的概率而采取的必要的预防措施,如规范管理、创造良好运行环境、备份磁带异地存放、设备冗余等措施。它不能应付区域性与毁灭性灾难,也不具备灾难恢复能力。

**3. 灾难恢复与内部恢复**

灾难恢复是一个在发生计算机系统灾难后,在远离灾难现场的地方重新组织系统运行和恢复营业的过程。

灾难恢复的目标一是恢复数据,保护数据的完整性,使业务数据丢失最少甚至没有业务数据丢失。二是快速恢复营业,尽可能缩短业务停顿的时间。

内部恢复则是指系统停顿后,在事故现场快速处理故障,使系统重新恢复运行的过程。如启用本地备份设备、更换设备或部件、重启系统、利用备份磁带恢复数据等。内部恢复主要用于处理计算机应用系统各种单点故障,它与灾难恢复的不同除了恢复地点之外,内部恢复还可能做到业务不停顿,而灾难恢复则不可能做到。

**4. 灾难恢复的必要条件**

要实现计算机系统的灾难恢复,必须具备以下条件:

·有在远离运行场地的安全场所存放的最近的业务数据备份介质;

·有可接替运行系统继续运行的备份运行系统;

·有用于将终端用户连接到灾难备份中心的网络通信设施;

·有完善的灾难恢复操作处理程序;

·有责任明确,能熟练操作应用系统,熟悉灾难恢复处理流程的人员和相应管理制度。

**5. 灾难恢复过程**

灾难恢复过程一般分为六个步骤:

·确认灾难发生,决定是否启用灾难备份系统;

·实施冷切换或热切换;

·采取人工的或自动的方式恢复孤立数据;

·将终端用户切换到灾难备份系统,恢复业务运行;

·生产系统恢复正常后,将终端用户回切到生产系统。

**6. 灾难恢复时间**

灾难恢复时间指的是从灾难发生到终端用户恢复对外营业的时间,一般包括上报审批时间、灾难备份中心将实施冷切换或热切换的时间、终端用户切换到灾难备份中心的时间、孤立数据恢复时间等部分。冷备份还包括数据备份磁带传送到灾难备份中心的时间。灾难恢复时间还与灾难类型以及当地社会公共设施的恢复速度有着密切关系。

**7. 灾难备份系统**

灾难备份系统是指可接替生产系统运行的计算机系统。一般由可接替生产系统运行的备份运行系统、数据备份系统、终端用户切换到备份运行系统的通信线路等部分组成。

**8. 灾难备份中心**

灾难备份中心是一个拥有灾难备份系统与场地,配备了专职人员,建立并制定了一系列运行管理制度、数据备份策略和灾难恢复处理流程,负责承担灾难恢复任务的机构。灾难备份中心根据其所属关系可分为专用和共用,从灾难备份中心与生产中心地理空间的距离可以分为同城和异地。

生产中心与灾难备份中心之间的距离是决定建设灾难备份系统所需成本的一个重要因素,也决定了灾难备份中心可预防的灾难种类。两个中心的距离越远,预防灾难的能力就越强,但在灾难发生后,技术和业务人员赶到灾难备份中心的时间就越长,恢复速度就越慢。

综上所述,充分认识大型计算机系统的灾难成因,对促进我国的计算机应用,采取有效措施,建立相应的灾难备份策略和系统,规避风险,降低和避免损失,具有重要的社会意义和现实意义。

(来稿时间:1999 年 8 月)



© 中国科学院软件研究所 http://www.c-s-a.org.cn