大型医院信息系统业务连续性方案研究*

孟晓阳 朱卫国 苏 博 张 楠 马学泉 黄迎萍

（北京协和医院 北京 100730） （石化盈科信息技术有限责任公司 北京 100007）

〔摘要〕 参照国内外相关经验和标准对大型三甲医院信息系统应用场景进行分析，针对医院信息系统业务连续性的需求进行分类和量化，基于信息系统灾难恢复能力的核心要素对适宜在医院使用的技术方案进行研究，包括备用基础设施、备用网络、备用数据处理系统、数据备份与保护等。

〔关键词〕 高可用性；灾备；医院信息系统；业务连续性

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2017.10.006

Study on the Scheme for the Business Continuity of the Information System in Large Hospital *MENG Xiao－yang, ZHU Wei－guo, Peking Union Medical College Hospital, Beijing 100730, China; SU Bo, ZHANG Nan, MA Xue－quan, HUANG Ying－ping, Petro－Cyber Works Information Technology Co., Ltd, Beijing 100007, China*

〔**Abstract**〕 The paper analyzes the application scenarios of the information systems in large grade A class 3 hospitals by referring to domestic and overseas experience and standards, classifies and quantifies the demands for the business continuity of the Hospital Information System (HIS), and studies the technical schemes applicable for hospitals based on the core elements of the disaster recovery capability of the information system, including backup infrastructures, backup network, backup data processing system, data backup and protection, etc.

〔**Keywords**〕 High availability; Disaster recovery; Hospital Information System (HIS); Business continuity

1 引言

业务连续性是指业务在运营中断事件发生后快速恢复、降低或消除因重要业务运营中断造成的影响和损失，保障业务持续运营[1]。保障业务连续性是信息系统建设的重要目标。保障信息系统业务连续性应首先进行信息系统灾难恢复能力建设。在此方面的研究始于 20 世纪 90 年代，最被广泛认可的标准是 1992 年美国 SHARE 用户组织提出的一个有关远程自动恢复的解决方案，即 SHARE78 标准。该标准第一次提出信息系统灾难恢复能力建设应包括数据备份系统、备用数据处理系统、备用网络系统、备用用户接入系统、备用基础设施、技术支持、运行维护支持、应急响应计划 8 个要素，按不同的恢复目标和技术手段，从本地磁带备份到远程自动恢复分为了 7 个层次[2-3]。

我国的研究始于 21 世纪初，2003 年中共中央办公厅、国务院办公厅发布的《国家信息化领导小组关于加强信息安全保障工作的意见》中首次提出信息系统建设要充分考虑灾难恢复的建设的要

〔收稿日期〕 2017－06－09

〔作者简介〕 孟晓阳，硕士，高级工程师，发表论文 20 余篇；通讯作者：朱卫国。

〔基金项目〕 数字化医疗医院流程研究及应用示范（项目编号：2012AA02A613）。

求[4]。2005 年国家信息化领导小组又发布《重要信息系统灾难恢复指南》，明确灾难恢复工作的流程、等级划分及灾难恢复预案的制定等方面的内容，标志着国内灾难恢复能力建设逐步走向标准化、正规化[5]。2007 年《重要信息系统灾难恢复指南》经过修订后成为国家标准 GB/T 20988－2007《信息安全技术 信息系统灾难恢复规范》，此标准成为至今为止国内信息系统灾难恢复能力建设的根本依据。与此同时，伴随着国家相关政策和标准的出台，民航[6]、银行[7]、保险[8]等行业相继发布本行业的标准和指南。如 2005 年出台的民航行业标准《民用航空重要信息系统灾难备份与恢复管理规范》；2008 年中国人民银行发布的的行业标准《银行业信息系统灾难恢复管理规范》；2008 年中国保监会颁布的《保险业信息系统灾难恢复管理指引》等。

2 需求分析

2.1 风险

近年来随着社会发展和人民生活水平的改善，人们对生命健康方面的需求不断提高，为获得更好的医疗资源，人们往往更倾向于去大城市的大型三甲医院就诊，这就造成了大型三甲医院人满为患，远远超过建设初期设计的接诊能力。面对业务的增长，为改善服务质量、提高效率、避免差错，大型三甲医院大量采用信息化手段支持医疗业务流程的运行，如门诊和病房都采用医生工作站下达医嘱，药房采用自动发药机发药，检验科使用自动化血液检测设备，诊间采用排队叫号系统，门诊采用手机 APP 预约挂号替代现场排队等。医院的核心医疗业务已达到离开信息系统就无法运行的地步。复杂的应用场景使信息化各子系统之间的关联度增大，而常规的单机应急方案只能在收费窗口等部分环节起作用，一旦信息系统出现故障，势必严重影响临床业务和医院管理体系的运行。近年来一些信息系统灾难事件表明，存储级别的数据丢失、甚至是整个数据中心机房失效的灾难发生已不再是小几率事件，而是随时可能以意想不到的方式发生。

2.2 业务影响

医院信息系统是迄今为止世界上企业级信息系统中最为复杂的一类[9]，它不但包括支持企业运营的管理信息系统，而且还包括支持医疗业务的临床信息系统，不同的子系统对业务连续性的要求也不相同。如检验系统自动从检验设备采集数据，业务对信息系统依赖性高；挂号和收费系统为窗口服务，实时性要求高；院长综合查询系统数据可以通过其他系统再次生成，对数据损失有一定的容忍度。

3 业务恢复目标

3.1 信息系统灾难恢复能力的等级

在国标 GB/T 20988－2007《信息系统灾难恢复规范》中，信息系统灾难恢复能力分为 6 个等级，各级的简要描述以及对应的恢复目标时间（Recovery Time Objective，RTO，即灾难发生后信息系统或业务功能从停顿到必须恢复的时间要求）和恢复点目标（Recovery Point Objective，RPO，即灾难发生后系统和数据必须恢复到的时间点），见表 1。

表 1 信息系统灾难恢复能力的 6 个等级

灾难恢复能力	简要描述	恢复目标时间（RTO）	恢复点目标（RPO）
第 1 级	基本支持：每周全备份，备份与严整制度化，有灾难恢复预案	2 天以上	1～7 天
第 2 级	备用场地支持：备用系统环境，有数据传输备用通道，设备供应协议	24 小时以上	1～7 天
第 3 级	电子传输和部分设备支持：每日数据备份，备用场地有人值守，有关键备用设备	12 小时以上	数小时～1 天
第 4 级	电子传输及完整设备支持：有全部备用设备，网络随时可用，每日多次传输数据	数小时至 2 天	数小时～1 天
第 5 级	实时数据传输及完整设备支持：远程数据传输复制，灾备设备随时可用	数分钟至 2 天	0～30 分钟
第 6 级	数据零丢失和远程集群支持：自动切换恢复体系，远程数据实时备份	数分钟	0

3.2 不同灾难恢复能力等级的不同要求

信息系统灾难恢复的目的是减少灾难带来的损失和保证信息系统所支持的关键业务功能在灾难发生后能及时恢复和继续运作。不同的灾难恢复能力等级对技术、设备、管理的要求各不相同：等级越高，系统恢复的时间越短，数据可能的损失也越少，相应的投入就越高，见图 1。

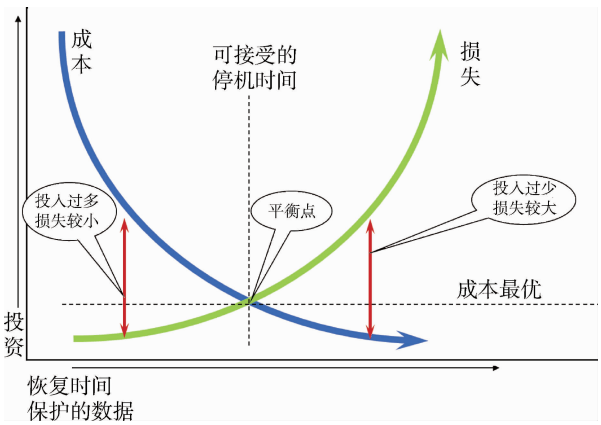

图 1 不同灾难恢复能力等级的不同要求

3.3 确定不同信息系统的业务恢复目标

因此，在已有的行业标准中[7-8]，都根据业务连续性要求对 RTO 和 RPO 进一步的进行了明确和细化。医疗行业也可根据自己的行业特点，基于现有技术条件，建议设定业务恢复目标如下：第 1 类：数据级（第 1 ~ 3 级），远程归档，数据不丢失，RTO < 24 小时，RPO < 24 小时。第 2 类：应用级（第 4 ~ 5 级），快速恢复应用系统，RTO < 6 小时，RPO < 15 分钟。第 3 类：业务级（第 6 级），业务连续性运行，RTO < 数分钟，RPO = 0。确定不同信息系统的业务恢复目标：（1）要考虑其支持的业务类型，有学者认为可以分为医疗相关类、经营业务办公管理类、IT 基础管理类[10]，医院的关键业务是对患者的诊疗和救治，医疗相关类的业务连续性要求最高。（2）其次还应考虑信息系统的技术架构，如只有基于 Oracle 数据库的信息系统，才可以在数据库层面做到 RTO = 0。（3）就是对数据重要性的评估决定方案中 RPO 的要求，如果数据需长期保存且不可再生，就有较高的 RPO 要求。（4）还要考虑方案实施成本，根据风险分析和业务影响分析的结果，确定业务恢复目标，设定关键业务的恢复先后顺序。

4 技术方案研究

4.1 备用基础设施

对于灾备中心的布局可采用：一主一备、一主多备、互为备份、多主一备、混合模式等[11]。在实践中，银行最常采用的是“两地三中心”的模式，即在同城和异地分别建立灾备中心。同城中心的优点是技术架构上相对简单，投资成本较低，重点用于保障业务的高可用性；异地中心可用于重大灾难事件的保障，灾备等级可适当降低，当同城中心因自然灾害等原因无法启用时，再考虑利用异地中心进行业务恢复。三级医院的信息系统机房应按照 GB/T 50174 - 2008《电子信息系统机房设计规范》B 级标准要求建设[4]，在供电、制冷、通讯等资源保障上已可达到本地冗余配置，因此重点需考虑的是备用场地问题。医院灾备项目建设时，也可以参照“两地三中心”的思路，综合考虑网络现状和医疗业务布局的，同城中心可选择院区内部的其他楼宇或距离较近的分院[12]，环境上可控、技术上实现简单、经济投入较少；异地中心仅备份数据，应选择较远的物理地点，或者购买第 3 方采用灾备云服务[13]，设计中应重点考虑传输线路的稳定性和带宽。

4.2 备用网络

备用网络方案的最高级别是网络双活，即主备数据中心同时对用户所需应用环境提供网络支撑，在数据中心内部网络设备和链路进行在线冗余，提供可靠性保障，如核心网络设备双机热备、汇聚层设备应有不同链路访问到不同物理地点的核心交换机等措施。对于重点的客户端节点，应保证从客户端到服务器的物理链路和设备都完全冗余，如挂号、收费、药房、急诊等窗口业务。还要避免同类业务接到同一台接入交换机上，以免单点设备故障影响全部业务窗口运行。实现网络双活的目的是实现基于网络的上层应用双活，如虚拟化 VMotion、

服务器双机热备集群都需要多台主机处于同一广播域下，即 2 层互联。而不同数据中心之间通常采用路由协议进行 3 层互联。为解决数据中心的 2 层网络互联问题，各厂商都有相应的解决方案，如 H3C 的以太网虚拟互联技术（Ethernet Virtualization Interconnect，EVI），Cisco 的覆盖传输虚拟化技术（Overlay Virtualization Transport，OTV），华为的以太网虚拟网络（Ethernet Virtual Network，EVN）技术。他们的基本思路都是通过在 IP 网络上动态构建隧道，实现以太网虚拟局域网的跨数据中心部署[14]。同时，还需考虑灾难发生后网络基本服务可用，如 AD 域控制器、DNS 服务等，相关服务器也需要在主机层面考虑容灾。

4.3 备用数据处理系统

单个医院信息化规模有限，但医疗业务流程复杂、实时性要求高。这就决定医院信息系统对服务器配置要求不高，但数量要求大，且需要配置冗余双机。针对这种场景，备用数据处理系统可主要依托服务器虚拟化资源池建设。服务器虚拟化技术包括多种高可用解决方案，如 VMWARE vSphere 的 vMotion、SvMotion、High Availability 和 Fault Tolerance 可分别实现虚拟机的在线迁移、存储的在线迁移、意外宕机保护和容错在线不宕机等功能。将服务器资源统一部署为服务器虚拟化资源池后，除可以提升系统可用性外，还有助于加快应用系统上线速度，统一设置服务器安全基线，显著减少 PC 服务器数量，缓解供电、制冷方面的压力，节省费用。已在很多医院中被广泛应用[10,12,15-16]。对于应用系统不支持服务器虚拟化的，如需要外插授权加密 KEY、非 X86 架构的小型机等情况，可继续采用传统的双机热备的方式，将主备机分别部署在不同的数据中心，也可达到跨站点冗余高可用的目的。

4.4 数据备份与保护

4.4.1 远程数据备份 数据备份是数据保护的最简单和最基础的方法，就是将文件系统、应用程序或者数据库在某一时间点进行一次完整的复制，复制结果以文件的形式保存，不能被应用直接访问。常见的备份软件有 Symantec NetBackup、IBM TSM、HP Protect Server 等，可实现全院异构系统的备份恢复等操作的统一调度和管理。大型医院每年会产生大约 50～100TB 的数据，其中影像数据占大多数，数据归档后调用频率相对较低，应考虑以下因素：常见的备份介质有磁盘阵列、磁带机、光盘塔等，应结合应用需求确定性价比较好的存储介质。远程备份的数据只有在发生重大灾难时才会启用，应考虑简单可行的备份恢复策略。

4.4.2 实时数据保护 （1）数据库同步技术：数据库同步是将日志文件从生产数据库传输到备份数据库，然后在备份数据库上应用这些日志文件对应的数据库操作，从而使备份数据库与生产数据库保持同步，异步完成。常见的有 Oracle 的 Data Guard、SQL Server 的数据库镜像、Cache 数据库的 Mirror 技术等。（2）存储虚拟化技术：存储双活是存储虚拟化技术在容灾领域的一种应用形式，其原理是将 SAN 网络扩展到主备数据中心，在两个站点分别部署物理存储设备，通过存储控制器互联或者存储虚拟化网关将两套物理存储连接起来，建立数据复制关系，逻辑上整合为一套向上层提供服务，从而达到冗余跨站点部署的目的。典型产品有基于网关的 EMC VPLEX，基于存储控制器的 HDS G1000 等。

4.4.3 逻辑错误保护 除应对的是硬件设备或者物理地点的失效，在实际工作中还常常碰到以下问题：（1）软件升级失败，需要回退服务器上安装的组件。（2）误操作导致数据删除，需要将数据库回退到删除前的特定时间点。（3）数据库审计需求，需要回查一段时间内的数据库变化。因此对逻辑错误的保护也是信息系统高可用性保障的重要一环，对逻辑错误的保护主要通过持续数据保护（Continual Data Protection，CDP）设备持续的捕获所有的 I/O 请求，并且将这些请求打上时间戳标志，将数据变化和时间戳保存下来，以便恢复到过去的任意时刻[17]。CDP 设备可以以镜像、快照、复制与录像等方式实现多维度、自动化的数据保护，包括当故障发生时瞬间恢复，数据立即可用；回退特定时间点秒级颗粒的历史恢复能力，使数据可以轻松回到

故障前的任何一秒；通过录像查看变化，对核心业务系统进行保护。

5 结语

对于信息系统灾难恢复能力中提到的非技术要素，如专业技术支持能力、运行维护支持能力、灾难恢复方案等，应在项目建设和交付过程中同步建立和完善。在研究过程中越来越深刻地感受到，随着大家对灾备必要性的认同和信息技术的进步，实现业务级的灾备，在技术上已不是遥不可及的事情，但如何有效的应对信息系统故障时的危机仍需要不断进行改进。作为最早实施灾备工作的银行行业，已开始将对灾难恢复能力的诉求，逐步上升到对业务连续性保障上来[1]。大型医院对业务连续性保障的需求尤为突出，已有很多医院在此方面作出有益的尝试。本文对大型三甲医院信息系统的应用场景进行分析，针对信息系统业务连续性的需求进行分类和量化，参照国内外相关经验和标准，基于信息系统灾难恢复能力的核心要素对适用技术方案进行研究。希望对后来建设者有所帮助和借鉴。

参考文献

1 中国银监会. 商业银行业务连续性监管指引［Z］. 2011.

2 National Institute of Standards and Technology. SP 800 - 34：Contingency Planning Guide for Information Technology Systems［Z］. 2012.

3 Disaster Discovery［EB/OL］.［2017 - 01 - 10］. http：//www. share. org/p/bl/et/blogaid = 185.

4 华琳，张保稳，高明. 国内外灾难恢复发展状况及建议［J］. 信息与电脑(理论版)，2011,(8)：58 - 59.

5 国务院信息系化办公室. 重要信息系统灾难恢复指南［Z］. 北京：2005.

6 民用航空重要信息系统灾难备份与恢复管理规范. MH/T 0026 - 2005［S］. 2005.

7 银行业信息系统灾难恢复管理规范. JR/T 0044 - 2008［S］. 2008.

8 中国保监会. 保险业信息系统灾难恢复管理指引［Z］. 北京：2008.

9 孟晓阳，孙国强，许燕. 基于 SOA 与 HL7 的医院信息系统的研究与实践［J］. 中国数字医学，2009,4(8)：80 - 82.

10 于雪梅. 构建高业务连续性的 IT 系统基础平台［J］. 医学信息学杂志，2012,(7)：24 - 27.

11 电子信息系统机房设计规范. GB/T 50174 - 2008［S］. 2008.

12 徐金建，孙震，张超，等. 虚拟化存储异地灾难恢复体系建设［J］. 中国数字医学，2014,9(8)：29 - 31.

13 广州市妇幼儿童医疗中心云灾备实现案例［EB/OL］.［2017 - 01 - 10］. http：//www. i2yun. com/yiliao/69. html.

14 H3C 公司官网［EB/OL］.［2017 - 01 - 10］. http：//www. h3c. com. cn/.

15 孟晓阳，郭杰峰. 使用 IT 运行监控系统保障医院信息系统的高可用性［J］. 医学信息学杂志，2015,36(2)：23 - 26.

16 任大桅. 医院数据中心虚拟化建设［J］. 中国信息界(e 医疗)，2014,(5)：58 - 59.

17 张冬. 大话存储：终极版. 存储系统底层架构原理极限剖析［M］. 北京：清华大学出版社，2015：523.