中国数据灾备产业白皮书暨数据灾备建设调研报告

建设数据战略灾备体系，打造数字中国护城河

灾备技术国家工程实验室
北京信息灾备技术产业联盟

电话：010-53519089
邮箱：info@zaibei.org.cn
地址：北京市海淀区西土城路10号
欢迎关注灾备技术产业联盟官网：www.zaibei.org.cn

推荐序

『为数字经济发展保驾护航』

首先祝贺北京信息灾备技术产业联盟这份重磅材料的发表。联盟以服务社会、服务会员为宗旨，多年来在信息安全和容灾备份领域做出了大量的努力和贡献，通过提供信息分享和服务的平台，不断推进国家和行业灾备技术和产业的发展。

2020年，一场突如其来的疫情，打乱了人民的生活节奏，给社会经济发展带来了巨大的冲击。期间我国的数字经济体现出强劲的发展韧性，实现了全球为之赞叹的复工复产速度。流调大数据、基因分析、云问诊等数据技术为全国战疫提供了有力的支撑。

数字经济的特征是以数据作为新生产要素，以信息系统为工具，助力数字化转型，实现降本增效。而近年来由于数据与信息系统遭受自然灾难和人为破坏，造成的巨大损失历历在目，有愈演愈烈之势，突显了容灾备份的重要性。

国家有关部门快速响应市场的呼声，推出了“网安法、等保2.0、数安法、个保法、关保条例”等一系列的法律、标准与政策，为督促数据运营主体完善数据安全防护提供了良好的制度环境。

北京信息灾备技术产业联盟积极响应国家号召，组织撰写了这份权威、详实且实战性强的灾备产业调研白皮书。从基础知识到关键技术，从法律到标准、从业务场景到行业案例，全面展现了中国灾备建设发展状况和未来图景。我相信对很多灾备行业初学者、技术人员、研究及投资机构、乃至主管机构与政策制定者都有一定的帮助。

数据安全关系到国家安全。我衷心希望各位读者关心和支持中国数据灾备产业发展，为中国数字经济发展保驾护航。

中国工程院院士 清华大学 郑纬民教授

推荐语

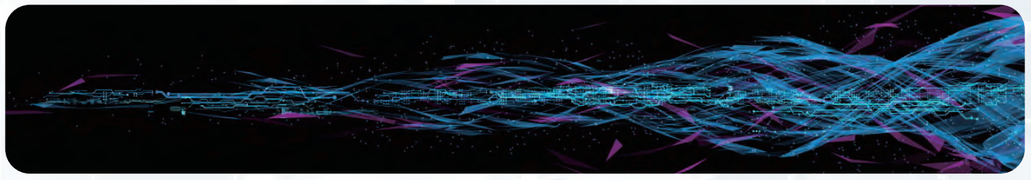
首先祝贺北京信息灾备技术产业联盟这份重磅材料的发表。联盟以服务社会、服务会员为宗旨，多年来在信息安全和容灾备份领域做出了大量的努力和贡献，通过提供信息分享和服务的平台，不断推进国家和行业灾备技术和产业的发展。

禄凯 国家信息中心信息与网安部副主任

读到灾备联盟这份完整且深入的调研报告，我很有收获。

在打造协同高效的数字政府，培育富有活力的数字经济，构建智慧便民的数字社会的过程中，信息技术帮助我们打通了一个又一个“孤岛”和“烟囱”。而数据安全始终是一柄悬在头顶的达摩克利斯之剑。无论是人为疏忽，自然灾害，还是勒索病毒，都可能随时让这柄剑坠下。灾备联盟和编委会一年来的工作卓有成效，这份报告在数据灾备的语境下，为信息领域从业者描述了基础设施韧性与数据合规利用的现实情况和技术路径。真诚希望更多业内人士能够读到它。

顾卫东 山东省大数据局党组成员、副局长



数据安全是国家安全的重要基石，数据灾备是贯彻落实国家安全要求的必要环节，而数据灾备是数据安全的最后一道防线。我国大数据时代已经来临，数据灾备建设正在步入实践阶段，这份报告较全面地揭示了我国数据灾备建设的现状和面临问题，亟待建立健全数据灾备体系，希望报告早日付梓，供更多的数据管理机构和从业人员参考应用，提升我国数据灾备管理水平。

在此感谢灾备联盟调研与撰写团队为此报告付出的努力！

忻超 江苏省大数据管理中心副主任

尼葛洛.庞帝在1995年出版的《数字化生存》（Being Digital）一书中指出，“从原子到比特的飞跃已是势不可当、无法逆转”。数据安全，尤其是数据的容灾备份，是数据安全的底座。

王春晖 浙江大学教授，工信部信息通信经济专家委员会委员

编审委员会

顾问

杨义先 灾备技术国家工程实验室主任、教授、博导、长江学者

母明江 重庆市綦江区政协主席、建设西部信息安全谷领导小组组长

主编

辛阳 灾备技术国家工程实验室副主任、灾备联盟秘书长、教授、博导

施崇刚 重庆市綦江区委常委、区政府常务副区长

周飞 广西壮族自治区大数据发展局党组成员，自治区信息中心党委书记、主任

副主编

李 芳 李德明 褚洪春

编委会

赵 帅 张 明 陈玉玲 易启义 李其刚 宋 征 田 军 张 伟 陈 祥 文静 陈吉宁 付睿

设计

江雯雯

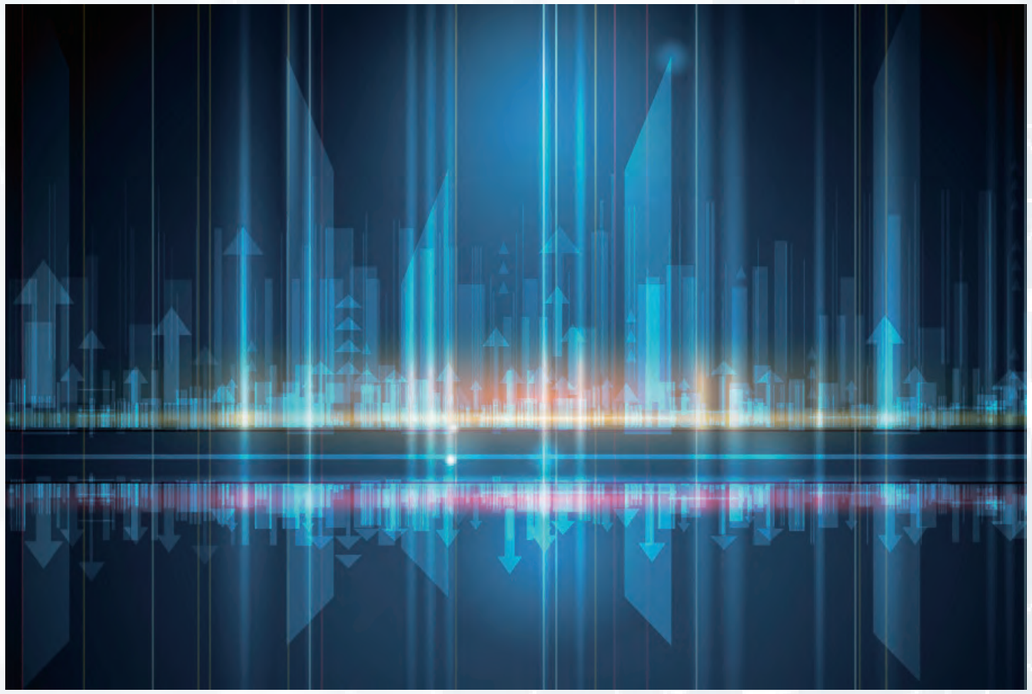
致谢

这份报告来自于灾备联盟全体会员单位的集体智慧，在此向全体参编作者、参与调研的单位、以及期间给与指导的专家、学者表达最诚挚的谢意，感谢灾备领域的“产、学、研、用、政”单位对联盟的信任与支持。

此次撰写灾备产业调研白皮书，调研人员深入到灾备的基层应用场景，把分散在各行各业的珍贵信息拼接起来，试图为读者打开一个从未见过的灾备产业全景。

灾备联盟立志为中国数字经济的发展保驾护航，以建设世界一流的灾备产业为己任。全体会员单位以这份报告作为一个新的起点，启动国内灾备建设的更深入调研和参与，希望得到各行各业一如既往的支持。

在此特向以下单位表示感谢：国家信息中心，江苏省大数据管理中心，广西壮族自治区大数据发展局，重庆市綦江区人民政府。向以下会员单位表示感谢：北京易华录信息技术股份有限公司、上海爱数信息技术股份有限公司、华为技术有限公司、广东紫晶信息存储技术股份有限公司、贵州大学公共大数据国家重点实验室、中国大唐集团科学技术研究总院有限公司、北京中软国际信息技术有限公司、深圳大普微电子科技有限公司、北京和力记易科技有限公司。



目录

序

前言

趋势

法规

建设

人才

总结

CONTENTS

前言

01

一、前言

数据安全是国家安全的组成部分，聚焦数据全生命周期的机密性、完整性、可用性的保护。随着我国的数字产业化和产业数字化，数据安全保障能力已经成为新时代信息化国家综合国力、经济竞争实力和军事实力的重要组成部分。为此，国家高度重视，对数据安全的体系、模式和战略进行了大量的研究和探索。“灾备”是数据安全的基本组成部分。

字面意义上的“灾备”是容灾与备份的缩写。“灾备”能力指的是数据基础设施在自然灾害、电力等设施失效、设备自身失效、人为破坏、勒索病毒、网络攻击等影响下的数据恢复能力和业务系统的连续性。“容灾”，即保障业务系统在灾难条件下的连续性；“备份”，即保障数据在灾难条件下的可用性，是在数据遭到破坏的情况下，快速恢复的前提条件。建设“数据灾备”系统，从而支持关键数据不泄露，不被篡改，保障关键数据不丢失，业务永远在线，以及访问永远合规，简称“三不两永远”。

灾备建设是保护数据的可用性的关键措施。然而经过调查研究表明，我国数据灾备建设却是数据安全最薄弱的一环，数据风险与日俱增。灾备覆盖严重落后于欧美。

重点领域信息系统灾备建设不足，包括数字政府、金融、运营商、教育、医疗、制造、能源、交通等仍普遍存在“本地备份完备度低、缺乏容灾、严重缺乏异地灾备”现象。

我国目前灾备技术供应体系存在风险，从解决方案、产品器件、甚至软件都受到美、日企业控制。

同时我国灾备领域的体系化建设不足，相关的法规、标准体系相对完善，但缺乏对应的技术实现路径指南和参考架构。

为了响应国家的战略布局，更好地推进我国灾备产业发展，“北京信息灾备技术产业联盟”（以下简称“灾备联盟”）与灾备技术国家工程实验室（以下简称“实验室”）通过对灾备行业的发展背景、相关的标准和法规以及最新的灾备技术方向与产业市场、人才队伍建设，尤其是关键行业的灾备建设进行全面的调研和阐述，对研究过程中所获取的资料进行全面、系统的整理和分析，对当前国内外灾备产业现状进行比较性分析，进而客观地针对我国灾备产业存在的优势和不足提出相应地建议，进而更好地推进我国的灾备产业的发展和建设。

附录简要介绍了相关术语和灾备技术国家工程实验室的工作机制和本课题的研究机制。

背景

02

二、背景

（一）时代需求促进灾备产业发展

科技的快速发展正在推动产业格局演进，新一轮产业应用的核心已经发展为IT信息网络技术的应用，互联网、智能终端等新一代的信息技术，目前IT技术已经转向以云计算、移动化、大数据和社交媒体为基础的数字时代，云计算等技术将成为驱动未来20年ICT市场转型和增长的主要动力。

设备和数据爆炸性增长对企业数据中心的稳定性带来了巨大挑战。同时，随着ICT技术在企业的研发、生产、销售、服务等环节不断渗透，数据中心的稳定性对于企业的业务持续性发展有着越来越至关重要的作用。据IDC统计，随着企业规模的扩大，数据中心宕机时间对于企业业务的影响和造成的直接经济损失不断提升，这也导致了企业每年在灾难备份和恢复相关技术和解决方案上的持续投入。因此，构建高效可靠的灾难备份和恢复系统，保障IT基础架构设施的安全性和稳定性，建设多DC的数据中心，确保业务的持续性稳定增长，成为了企业必须思考的问题。

从网络安全的角度来看，随着业务量爆炸式增长，外部环境逐渐复杂化，数据存储系统正在成为侧信道、APT、DDOS、勒索病毒等网络攻击的主要战场，数据灾备系统本身低于网络攻击的能力是一个薄弱环节。

备份系统承载着和生产系统中一样甚至更多更全的数据，意味着备份系统被攻破甚至会造成更严重的后果。同时也需要考虑备份数据本身的机密性和完整性。因此需要根据所备份数据的分类分级，采取相应的加密，访问控制，脱敏，数据留存期等完整的数据保护配套措施。

由于同样的原因，依托备份系统部署防勒索病毒策略和数据安全治理能力也成为理想选择。随着法律法规的健全，尤其是“罚则”的健全，数据“合规”，“安全”和“利用”三大主题齐头并进已经成为业界共识。灾备系统不仅在安全层面发挥作用，也应该以数据安全治理为起点，解决数据“合规证据链条”的一部分技术难题。

另外灾备数据天然具有多副本，异地存储的特点，增加了数据合规利用、数据安全治理的复杂性。业务系统需要能够采取安全措施妥善保护关键数据，并与其适配相关的法律法规与安全策略。在海量的数据场景下，这些工作远超过人力所能管理的范围，需要自动化，智能化的安全合规治理方案。

（二）数据灾备需求延伸至全行业

伴随着信息成为社会发展的重要战略资源，“信息获取、使用和控制”已成为了信息化发展和完善的核心，相应地信息安全和保护就演变成国家发展战略中亟待解决、影响国家大局和长远利益的重大关键问题。信息安全保障能力必将成为信息化国家新时代综合国力、经济竞争实力和生存能力的重要组成部分。为此，国家高度重视，对信息安全的体系、模式和战略进行了大量的研究和探索。

数据安全保障能力已经成为信息化国家综合国力、经济竞争实力和生存能力的重要组成部分。各种新兴的电子商务、电子政务、电子医疗、社交网站等信息系统拥有大量的用户。全世界每一秒都在产生和使用大量的文字、语音、图像、视频信息，数据已经被定义为“第五生产要素”，成为整个社会当中最重要的资源之一。从我国“新基建”建设要求可以看到，“数据”在数字经济发展中的地位进一步提高。灾备建设已经提高到国家信息化发展的战略高度，成为国家信息安全保障体系中的核心任务之一。

数据是数字社会流动的血液，数据安全是保证国家网络安全的基础保障，数据灾备涉及总体国家安全观的全部16种安全：政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、深海、极地、生物，数据基础设施已经成为各个领域的重要支撑，数据的容灾备份是关乎国家安全的重中之重。可以说数据灾备体系建设是保证数字中国健康发展的关键。

随着数字化不断转型，政府政务信息化、监管手段信息化，使工商、税务、公安、医疗卫生、社会保障等部门的数据量急剧增加，各个企业和地区都在规划建设灾备中心。金融、证券、电信、电力、石油等重点行业及特大型企业信息化重大工程的实施，也需要建设大型的灾备中心来保障业务的连续性和数据的可恢复性。

建设统一的数据灾备体系能有效降低故障带来的经济损失。全球每年由于灾备不足导致的损失激增，仅勒索病毒一项2020年就同比增长了4倍多，达到3.5亿美金。调研机构Qualix Group统计表明不同行业关键业务中断带来的经济损失：业务宕机1分钟，平均会使运输业损失15万美元，银行业损失27万美元，通信业损失35万美元，制造业损失42万美元，证券业损失45万美元。从直接经济损失的角度解释了关键业务平台对于企业业务稳定性和可靠性的影响。以下是部分经济损失的案例：

（1）2021年9月南非司法部遭到恶意加密，导致包括签发授权书、保释服务、电子邮件和部门网站的全部系统和数据不可用，关键业务处理已经变成了手动方式。

（2）2021年5月，美国东部最重要的输油大动脉科洛尼尔管道运输公司系统遭勒索软件攻击致瘫痪，美国进入“紧急状态”，经济损失约x百万美元以上。

（3）2020年10月东京证券交易所由于系统故障导致全日本五大交易所的四个关停一天，影响金额达数千亿日元的交易，首席执行官引咎辞职。

（4）2020年2月某互联网公司数据被恶意删除，客户数据恢复耗时七天七夜，赔偿客户损失1.5亿RMB。

（5）2016年5月，遭遇了一次因停电导致的大范围宕机，美国著名的云平台Salesforce公司，由于操作故障和缺乏容灾方案，致使客户近5小时的数据蒸发，官方表示无法恢复，经济损失无法估量。

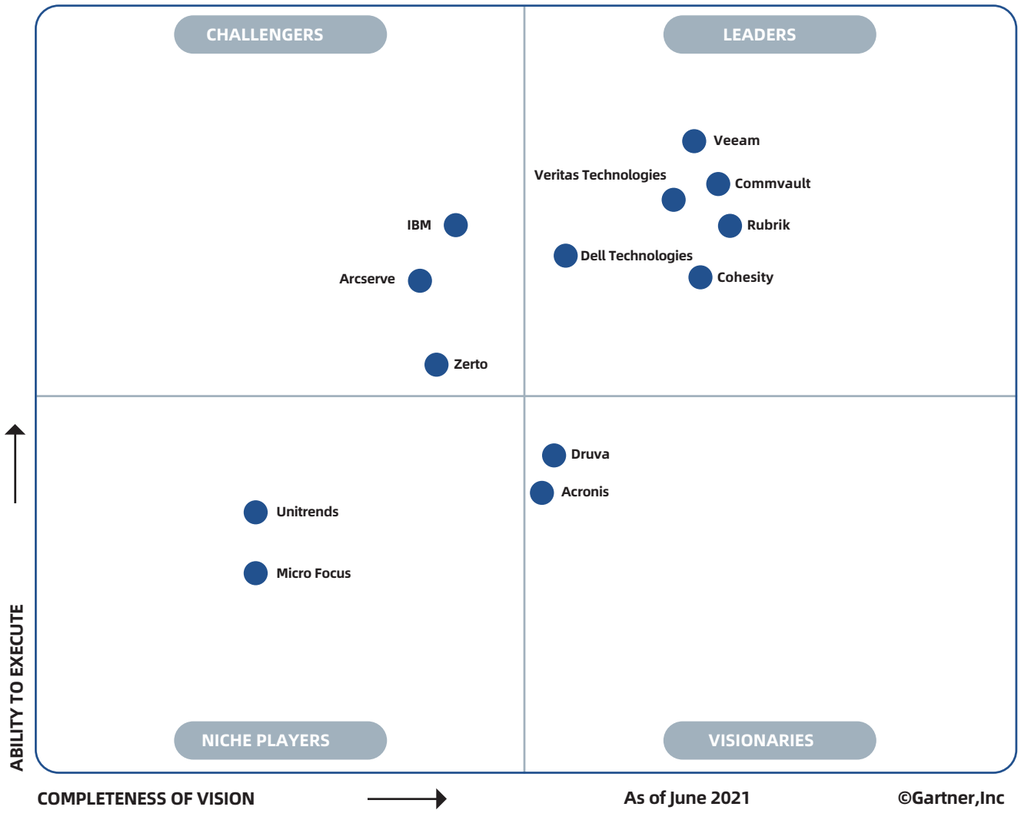
灾备技术发展趋势分析

03

三、灾备技术发展趋势分析

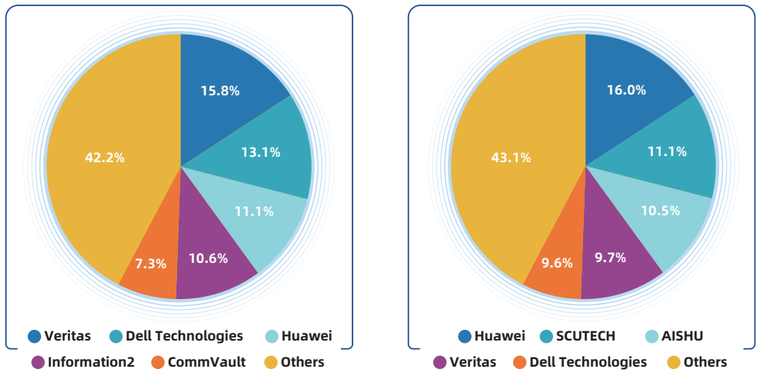
在关键硬件器件层面，美日企业有明显的领先优势。容灾、备份、归档系统中最关键的硬盘、磁带、光盘介质被美、日供应体系所垄断。我国几乎不具备硬盘、磁带的供应能力。近年来国有银行、大型股份制银行已经屡次发现存储介质无法供应的风险。因此存储介质的“硅进磁退”，面向闪存盘-即半导体存储介质的转型刻不容缓。事实上半导体存储介质具有能效高、时延低、密度高的优势，全球布局半导体存储介质的竞赛激战正酣。

在灾备软件层面，美国企业也遥遥领先。IT行业著名的分析师机构Gartner在2021年发布的数据中心关于数据备份与恢复厂家的《魔力四象限》排名显示，进入魔力四象限的全是国外企业，处于领导者象限的Commvault、Veritas、Veeam、Dell、Rubrik、Cohesity，全部是美国公司。美系厂商掌握了数据备份与恢复领域在国际市场的话语权。



图表 1 Gartner数据备份与恢复厂家魔力象限排名[参见：https://www.gartner.com/en/research/magic-quadrant]

近年来我国在数据保护领域也涌现出很多优秀的企业，包括华为、爱数、鼎甲、壹进制、英方等。据IT行业著名的咨询机构IDC 发布的2020年下半年中国数据备份与恢复系统市场跟踪报告，国内企业在国内市场占有率逐步提升，2020年华为、爱数、鼎甲和壹进制总共占有35.9%的市场份额，占有40.6%的Others类别中包含大量的国产厂商。例如其中备份一体机市场，华为、鼎甲和爱数分别为前三，在政府、金融、电信运营商等领域中尤其获得客户的认可。



图表 2 IDC在2020年发布的中国数据保护市场份额[参见：https://www.idc.com/]

上图为数据恢复与保护市场软件份额，下图为备份一体机设备市场份额。中国厂商在数据保护硬件市场已经形成群体突破，但在软件市场，美国厂商凭借生态的长期积累，还把持超过半数以上市场，中国厂商形成数据备份与恢复领域独立自主的话语权，仍在艰难起步的阶段。

尤其值得注意的是，在国产数据灾备产品发展过程中，需要警惕落后技术的国产化“马甲”。随着“去IOE”的推进，出现了一些令人担忧的现象。一些拥有数据保护先进技术的国外厂商退出市场的同时，却有另一些不那么先进的国外产品反而以“合资”的形式贴牌进入中国市场。在灾备技术领域，技术的先进性与供应的可持续性同等重要。

（一）全球主要灾备技术分析

在信息化环境下，灾备行业有很多的专业灾备知识及技术 。包含容灾、备份和归档等技术。通常在应用中几种技术会结合使用。以下进行技术分析与介绍。

1.容灾

从广义上讲，任何提高系统可用性的措施都可称之为容灾。容灾，即灾难发生时，在保证生产系统数据尽量少丢失的情况下，保持生产系统业务的不间断运行。容灾方案包含应用层容灾、数据层容灾方式。应用层容灾一般指利用应用层容灾方式建立针对用户业务的灾难恢复系统，其主要原理是通过应用程序或者中间件产品同时向主中心和容灾中心传输未经处理的生产数据，主中心服务器和容灾中心服务器同时处理数据。在正常情况下，只用主中心和业务系统联系，容灾中心只在后台处理数据；当主中心瘫痪时，由于容灾中心也存有生产数据库，也存有生产数据，所以可以接管业务。

数据容灾，或称为存储层容灾，是重要的容灾技术。根据故障场景划分，容灾方案可以分为：本地高可用，同城双活数据中心，主备容灾和多DC解决方案这四种类型。

（1）针对本地高可用解决方案，主要是解决数据中心内单部件的单点故障，如：网卡，控制器，单存储或网络故障等。其灾备距离一般在同一个机房的不同机柜之间，或者同一个园区的不同机房内。该方案采用存储双活技术，可以实现RTO和RPO为零。

（2）针对双活容灾解决方案，主要是应对应用级，存储级和单数据中心故障场景，一般部署在300公里以内的同城数据中心，采用应用集群和存储双活技术，实现业务不中断，数据零丢失，达到RPO=0，RTO=0。但由于其需要数据中心间专有网络建设，其建设成本相对较高。

3）针对主备容灾解决方案，主要用来应对局部故障场景下的业务快速恢复，比如：主数据中心主机故障，主数据中心整体故障等。一般部署在同城或异地数据中心。可实现分钟级RPO（同步复制可实现RPO≈0），RTO分钟级恢复。

4）针对多DC容灾解决方案，用来应对很多核心业务场景需要更复杂的多数据中心容灾解决方案，比如两地三中心甚至四中心容灾。多份容灾数据能使数据更加安全可靠，在出现极端灾难的时候，仍然有可用的数据副本能提供数据服务。当前发展出来

出来的环形3DC组网，能更大程度的保证业务可靠性。

针对双活容灾解决方案，主要采用存储阵列AA等双活技术，SAN和NAS一体化双活技术，结合应用集群及网络互连，实现数据中心无缝切换，保证业务连续性。

针对主备容灾解决方案，主要采用采用存储同步或异步远程复制技术，结合内存时间戳技术和增量复制技术，可实现RPO=0或分钟级，RTO分钟级或小时级别，实现本地或同城容灾。

针对多DC解决方案，在同城通常采用存储双活或存储同步技术，可实现RPO=0，RTO小时以内。异地灾备中心，采用存储异步远程复制技术，可实现秒级RPO，RTO小时级别。多数据中心容灾解决方案的配置分为并联和级联两种方案，可以基于双活、同步复制、异步复制等多种容灾方案进行组建。

2.备份

备份是保障数据的可恢复性，其实现方式是以一定的规则-如定期将重要数据复制到其他存储位置，并可以恢复到过去的某个特定的时间点。以此来抵御误操作、硬件故障、病毒等一系列威胁。

备份的类型有：全量备份、增量备份、差量备份。增量备份与差量备份的区别是，增量备份判断数据更新标准是依据上一次备份检查点，而差量备份一定是依据全量备份检查点。如没有全量备份，就没有差量备份。差量备份的主要目的是限制完全恢复时使用的介质数量。

分类	简介
全量备份	用存储介质对整个数据及系统进行完全备份。这种备份方式的好处是很直观，容易被人理解，易恢复；缺点是在备份数据中有大量重复数据，由于需要备份的数据量相当大，因此备份所需时间较长
增量备份	每次备份的数据只是相当于上一次备份后增加和修改后的数据。这种备份的优点很明显：重复数据少，即节省存储空间，又缩短了备份时间
差量备份	是拷贝所有新产生或更新的数据，这些数据都是最近一次全量备份后产生或更新的

图表 3备份分类-按照备份数据量

常见的备份方案有一体机备份，简单来说备份一体机是一款将备份软件、备份服务器以及存储介质整合到一个架构中而形成的一个设备，最终用户可以像操作备份软件一来操作这个设备。也有专用备份存储方案，即备份软件与备份介质分离的架构。

3.归档

归档是为了将冷数据长期保存，以满足法规遵从的要求。常见的归档一般为归档到文件存储、归档到S3或者磁带中。在海量的数据中，有一部分数据是极少访问，但又具备重要价值的，比如金融业中的票据影像、电子保单，医疗行业中的电子医疗影像，电子档案卷宗，基因测序数据，地址勘探数据等等，均需要10年以上长期留存，部分数据甚至30年以上留存。其长期留存的主要目的，是为了满足较长周期内可追溯的要求，做到法律法规遵从。在这种场景下，要求数据长期留存的成本最优。

与此同时，我们看到传统的冷数据归档也正在发生一些变化，比如过去从归档数据库调取一份归档数据可能需要1-2个工作日，而现在，随着数字金融、电子政务、数字医疗等业务的持续兴起，冷数据访问提出了更高的要求，分钟级访问已经成为普遍诉求。

传统归档广泛采用磁带库作为介质，磁带库享有很高的成本优势，并且行业标准稳定发展，目前仍然是归档介质的主流选择。同时磁带也存在诸如5-7年需要定期转储，运维管理复杂、性能差、数据损坏风险等问题。业界有电、磁、光三级存储介质架构归档的方案，SSD/HDD作为归档缓存，能提供高访问性能；磁带或蓝光存储作为离线归档层，满足长期存放和降低成本诉求。通过热温冷数据自动识别技术，可以实现数据的自动分级存放，综合成本最低。在访问性能方面，通过智能预取技术进行访问性能加速，实现归档数据的快速访问。

（二）中国灾备产业国产化现状与分析

国内数据保护厂商主要有：爱数、鼎甲、华为、壹进制、英方等。

目前国内数据保护产品发展较晚，存在三个问题：

1.技术核心掌握上整体落后于国外

2.市场生态环境存在较大问题，严重影响产业发展

3.部分厂家灾备产品硬件的元器件对国外依赖强

国产产品在数量上较多，但平均品质不高。除了少数几个优质企业外，国产产品多以跟随仿造国外产品为主，缺少核心技术且品质一般，这些产品数量众多，但兼容性等指标并不能满足生产系统灾备的要求，还大量挤占了市场资源，一定程度上影响着国产灾备产业的良性竞争。随着数据的快速增长、数据类型与环境的日趋复杂、以及云时代的到来，数据保护产品的未来将迎来巨大的发展，但也将会有一定的挑战。

灾备产品关键的元器件自然是存储介质，我国目前不具备机械硬盘（HDD）国产化的能力，也没有相应的规划。然而半导体介质由于其良好的读写性能、超低的能耗水平必将成为灾备领域的首选。国内产业厂商已经掌握了NVMe接口SSD控制器和颗粒（NAND）的设计和制造技术，虽然工艺水平和世界领先厂家还有一些差距，短期仍存一些制造设备和材料风险，但长期有望达到业界先进水平。

因此加大对全闪存数据中心的布局，加速采用全闪存介质在灾备体系中的比例，帮助闪存供应链快速成熟，也让数据保护产业链增加了自主可控的选择。

数据存储系统的核心软件的可信设计也是容易忽视的风险点，大量开源软件未经过系统性的可信安全设计与验证，因此关键业务的灾备系统选择应该慎重选择有自主可控能力的软件替代。

一些数据存储专用器件的供应能力也不容忽视。存储芯片、部分关键的IO芯片、内存、网络芯片等，国内普遍具备设计能力，但制造能力落后业界先进水平3-5年。值得一提的是传统的光交换机被美国厂家垄断达99%。加速发展国内IP网络交换机，替换FC、IB交换机的节奏刻不容缓。

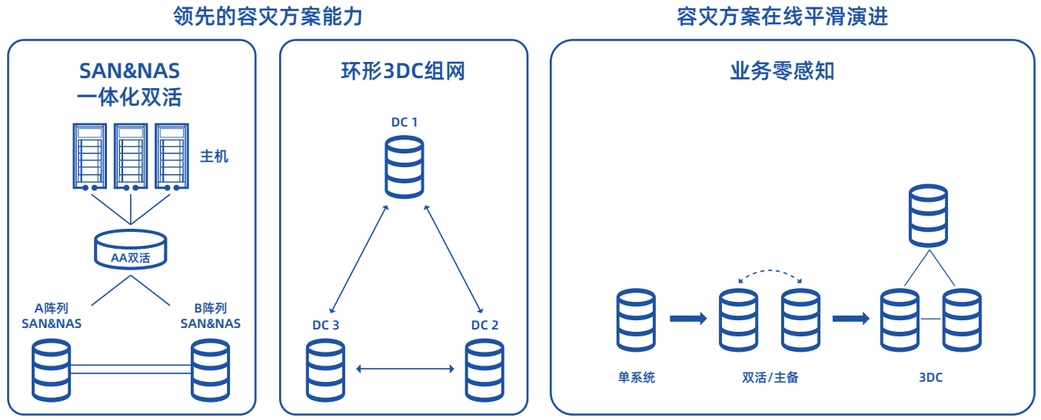
数据保护还面临着诸多其他挑战，比如由于天灾、病毒、误操作导致的数据损坏或者丢失，在这种场景下，为了保障客户关键数据不丢失，历史副本可追溯，必须加强备份系统建设和保护能力提升，确保数据不丢失。

虽然“全国产化”（国产芯片、国产操作系统、国产数据库）的背景无疑是给了国内企业一个机会，但必须要尽快解决技术和生态问题才能把握住机会。

（三）国产厂家主要技术突破分析

经过不断的技术积累，国产厂家在灾备部分领域取得世界领先的基础技术突破。

（1）容灾技术和方案：国内某存储厂商实现了业界领先的免网关存储双活技术（包含SAN和NAS双活），两端存储可同时提供业务访问能力，在存储单机故障下业务不中断，系统自动切换并自愈。还支持通过复制技术应用，将方案扩展到两地三中心，实现更高等级灾备，两地三中心解决方案支持环形架构、串并联方式，当单个数据中心故障，另外两个站点仍可以进行正常的数据同步。



图表 4 部分我国企业的灾备技术已经达到世界领先地位

（2）备份技术和方案：

高重删技术：备份数据由多个相似的副本组成，且需要较长时间保留，需要设计合理的灾备系统投入产出比，最为关键的就是算法，算法的本质是数学，为此，该厂商在全球数学圣地法国巴黎和俄罗斯莫斯科，分别建立了研究中心，集合全球顶级数学家的智慧，将数据的缩减做到极致。同时该厂商还在探索和高校合作，将学术成果转化到产品上，比如去年该厂商和莫斯科国立大学合办的全球数据压缩大赛，里面有不少算法就已经应用到了备份产品中。产学研的有效结合，让数据缩减算法不断创新，比如基于数据的特性进行关联压缩，基于特征训练的词频预测算法，多层切片自适应重删，让该国产厂商的数据缩减能力持续领先业界，已经取得多项关键技术专利，能力超过业界标杆水平达20%。

图表 5 我国企业备份领域变长重删技术缩减率超越业界最佳水平20%

快照技术:快照技术是众多数据备份技术中的一种，其原理与日常生活中的拍照类似，通过拍照可以快速记录下拍照时间点被拍照对象的状态。由于可以瞬间生成快照，通过快照技术，系统管理员能够实现数据的零窗口备份，从而满足企业对业务连续性和数据可靠性的要求。并且占用空间少，快照能够快速生成源卷在某个时间点的一致性副本，通过周期性地创建快照，还可以使得数据得到持续的保护。当源的数据遭到人为意外删除、破坏或病毒入侵时，通过快照回滚可以快速将源的数据恢复到快照激活时间点的数据，减少源数据的丢失量。快照是一种非常好的防数据破坏技术，国内企业已经充分掌握这项技术。目前快照技术多用于存储整机产品，预计在数据保护产品中很快也会有广泛的应用。

勒索病毒软件特征检测与恢复技术：勒索病毒攻击带来的数据丢失是近年来上升最快的数据安全风险。针对已经被勒索软件感染的数据（例如，备份之前已经感染病毒），通过基于勒索软件特征的分析和检测技术，可有效识别灾备数据中的不安全数据，以便进行数据的安全恢复。我国数据保护相关企业在勒索病毒特征检测技术已经接近世界先进水平，明年有望实现赶超。

灾备产业相关法规与标准分析

04

四、灾备产业相关法规与标准分析

灾备恢复系统的建设，不仅要满足企业与用户对数据安全的业务需求，更要符合相关国家/行业监管的合规性要求。在金融、政府、电信等行业领域，国家标准、行业标准已经明文规定企业在信息系统建设中，需要对重要数据采取有效地保护措施，确保数据的机密性、完整性和可用性，也因此对灾难恢复、数据备份等能力提出了相应的要求。

在法律法规层面，2017年实施的《网络安全法》及2021年实施的《数据安全法》，对网络运营者、关键信息基础设施运营者以及参与数据处理活动的相关主体，提出了容灾备份、保障数据安全的要求，并规定了相关的法律责任。

在国家宏观政策层面，早在2006年，中共中央办公厅、国务院办公厅联合正式发布了文件《2006-2020年国家信息化发展战略》，明确提出要建立国家信息安全保障体系，因此发展灾备产业也更加地迫切和需要。2016年在《中华人民共和国国民经济和社会发展第十三个五年规划纲要》第二十八章中明确指出要：强化信息安全保障，包括实施大数据安全保障工程，加强数据资源在采集、存储、应用和开放等环节的安全保护，加强各类公共数据资源在公开共享等环节的安全评估与保护等。而对于信息安全、数据安全，灾备是最基础的技术需求，几乎所有的信息资产都需要灾备保护，以确保在任何意外故障情况下，信息系统的正常运转。应该根据业务和数据的重要性进行分类分级，并匹配相应的灾备保护方案。政府、金融、通信、教育、能源、交通、医疗等各关键领域、关键部门的关键信息基础设施是经济社会运行的神经中枢，是信息安全的重中之重，也是可能遭到重点攻击的目标。“物理隔离”防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。不出问题则已，一旦出现问题可能导致交通中断、金融紊乱、电力瘫痪等重大问题，具有很大的破坏性和杀伤力。完善的灾备体系是数据安全的最后一道防线，责任重大。

（一）国际标准及法规

主流灾备标准起源于美国，为了能够规范各国及地区在灾难项目建设时的要求，提纲挈领地制定了国际化的相关灾难恢复标准。

1.SHARE78

SHARE78标准由Share组织在1992年3月的Anaheim会议上制定，是一个远程自动恢复解决方案的标准，业界一直沿用此标准作为数据容灾领域的权威标准。该标准基于8条关于业务应用场景、数据容灾需求、技术机制等方面的原则，将数据容灾与恢复水平分为7个等级，不同等级在容灾恢复应对机制，数据恢复时间性能等方面存在等级差异。

8个分级原则包括：

7个容灾系统能力等级包括：

（1）0级-无异地备份：0等级容灾方案数据仅在本地进行备份，没有在异地备份数据，未制定灾难恢复计划。这种方式是成本最低的灾难恢复解决方案，但不具备真正灾难恢复能力。

（2）1级-实现异地备份：第1级容灾方案是将关键数据备份到本地磁带介质上，然后送往异地保存，但异地没有可用的备份中心、备份数据处理系统和备份网络通信系统，未制定灾难恢复计划。灾难发生后，使用新的主机，利用异地数据备份介质（磁带）将数据恢复起来。

（3）2级-热备份站点备份：第2级容灾方案是将关键数据进行备份并存放到异地，制定有相应灾难恢复计划，具有热备份能力的站点灾难恢复。一旦发生灾难，利用热备份主机系统将数据恢复。它与第1级容灾方案的区别在于异地有一个热备份站点，该站点有主机系统，平时利用异地的备份管理软件将运送到异地的数据备份介质（磁带）上的数据备份到主机系统。当灾难发生时可以快速接管应用，恢复生产。

（4）3级-在线数据恢复：第3级容灾方案是通过网络将关键数据进行备份并存放至异地，制定有相应灾难恢复计划，有备份中心，并配备部分数据处理系统及网络通信系统。该等级方案特点是用电子数据传输取代交通工具传输备份数据，从而提高了灾难恢复的速度。利用异地的备份管理软件将通过网络传送到异地的数据备份到主机系统。一旦灾难发生，需要的关键数据通过网络可迅速恢复，通过网络切换，关键应用恢复时间可降低到一天或小时级

（5）4级-定时数据备份：第4级容灾方案是在第3级容灾方案的基础上，利用备份管理软件自动通过通信网络将部分关键数据定时备份至异地，并制定相应的灾难恢复计划。一旦灾难发生，利用备份中心已有资源及异地备份数据恢复关键业务系统运行。

（6）5级-实时数据备份：第5级容灾方案在前面几个级别的基础上使用了硬件的镜像技术和软件的数据复制技术，也就是说，可以实现在应用站点与备份站点的数据都被更新。数据在两个站点之间相互镜像，由远程异步提交来同步，因为关键应用使用了双活存储，所以在灾难发生时，仅仅很小部分的数据被丢失，恢复的时间被降低到了分钟级或秒级。由于对存储系统和数据复制特性的要求较高，所需成本也大大增加。

（7）6级-零数据丢失：第6级容灾方案是灾难恢复的最高级别方案，其利用专用的存储网络将关键数据同步镜像至备份中心，数据在本地与异地（备份中心）均需进行确认。基于此，数据是同时写到两个站点，在灾难发生时异地容灾系统保留了生产系统相同的全部数据。该方案利用了实时存储双活与完全的网络切换能力，不仅能够保证数据的完全一致性，而且存储和网络等环境具备了应用的自动切换能力。在生产中心发生灾难时，备份站点可以实时自动接管业务，实现数据零丢失。

1.ISO 22301

ISO 22301 于2012年5月正式发布第一版并于2019年完成最新版修订稿的发布，其全称为“Security and resilience - Business continuity management systems - Requirements”，其前身为英国BSI发布的BSI 25999标准。该标准定义了一套业务连续性管理框架，使能企业对潜在的灾难加以辨别分析，帮助其确定可能发生的冲击对企业运作造成的威胁，并提供一个有效的管理机制来阻止或抵消这些威胁，减少灾难事件给企业带来损失。ISO 22301 拥有非常高的国际认可度。ISO 22301适用于所有行业中的大、中、小型公有及私有组织，并且特别适用于处于高风险和高度监管环境下的行业，例如 IT 通信业、金融业、制造业等。

最新发布的修订版本中基于产业发展和市场需求对标准的相关内容进行调整，更加强调企业韧性与快速恢复，这就要求企业在进行灾难恢复管理时充分考虑管理制度与底层基础设施的能力建设与协同。

2.ISO/IEC 27040

ISO/IEC 37939于2015年正式发布并在2019年开启修订，其全称为：“Information technology - Storage security”。该标准针对数据存储系统的部署者和使用者提供了一套安全框架。该框架中，明确对数据的备份复制、灾难恢复及业务连续性提出了具体的要求，从存储系统设计原则、存储设备能力机制、灾难备份恢复系统软硬件要求等元素全面并详细地罗列了具体的要

了具体的要求，以应对系统用户面临的业务连续性风险和数据安全威胁。

SNIA（Storage Networks Industry Association）下设的Security工作组中，全球知名的存储厂商、备份恢复解决方案厂商、主流的IT公司联合发布了针对ISO/IEC 27040标准的应用实践白皮书《Storage Security：Data Protection》与《Data Protection Best Practices》。这两个白皮书中针对ISO/IEC 27040中定义的原则与要求描绘并实际展示了业界最佳实践，帮助用户更好地理解标准内容并为存储系统使用者和设计者提供标准遵从的指导。

3.美国CLOUD ACT

Cloud Act（Clarifying Lawful Overseas Use of Data Act）《澄清合法海外使用数据法》，简称为《云法案》，该法案第103条(a)(1)款修订了《存储通信法》，增加了以下条款以解决政府和微软对最初搜查令的关切：“服务供应商应遵守本章的义务，保留、备份或披露有线或电子通信的内容，以及该供应商拥有、保管或控制的与客户或订户有关的任何记录或其他信息，无论此类通信是否记录，或其他信息位于美国境内或境外

立法背景如法案开篇阐述的美国国会如下认定：

及时获取通信服务提供商持有的电子数据是美国政府保护公共安全和打击严重犯罪的关键；

美国政府的这种努力正在因无法获取美国境外存储的数据而受到阻碍，而保管、控制或拥有这些数据的服务提供者本身受美国法律管辖。

关键核心条款：

远程计算服务提供商及通信服务提供商应遵守以下义务：无论通信、记录或其他信息是存储在美国境内或境外，只要该等通信内容、记录或其他信息为该服务提供者所拥有、保管或控制，服务提供者均应依照本章要求保存、备份、披露 属于客户或服务订购者的 有线或电子通信内容、任何记录或其他信息。

4.欧盟GDPR

GDPR是关于自然人的个人数据处理和个人数据流动的法律。GDPR针对个人数据处理和个人数据流动，设定了个人数据处理活动和个人数据流动的原则，规定各相关方（数据主体、数据控制者、数据处理者）的权利、义务以及违法责任，设置执法机构并赋予其权力。

1995年，欧盟制定了《数据保护指令》（Directive 95/46/EC）保护欧盟公民的个人数据，2012年宣布“数据保护规则改革”计划，并提出《统一数据保护法》（General Data Protection Regulation，“GDPR”）草案，于2016年4月14日正式通过，2018年5月25日正式生效。

GDPR直接适用于欧盟成员国、而无须经其国内立法转化。同时，GDPR规定部分事项上成员国有立法权。GDPR适用于欧盟实体的个人数据处理活动（无论该活动是否发生在欧盟境内），以及欧盟境外实体处理欧盟境内数据主体个人数据的活动——只要该活动与向该数据主体提供商品或服务（无论是否收费），或与监控该数据主体在欧盟的活动有关。

（二）国家标准及法规

为了有效地应对灾难恢复需求，我国在灾备执行标准及法规方面，制定了一系列符合我国各行业发展特点的国家标准及法规。

1.GB/T 20988-2007

GB/T20988-2007是由信安标委归口的国家标准，于2007年发布，标准名称为《信息系统灾难恢复规范》。该标准从国内的实际信息系统应用场景出发，给出了信息系统灾难恢复能力建设的基本要求，从组织、管理、协作等角度出发，按照灾难恢复工作的生命周期维度以灾难恢复需求的确定、策略制定到实现给出了整体的框架，适用于信息系统灾难恢复能力建设的规划、审批、实施和管理。该标准的附录A中给出了参考SHARE78标准的灾难恢复能力等级划分，给出了适用于我国信息系统灾难恢复能力建设的层次化要求，这六个等级在数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、专业技术支持能力、远程维护管理能力及灾难恢复预案等几个维度分别进行差异化的要求，指导信息系统建设者基于信息系统承载业务的重要程度选择合适的灾难恢复等级。这六个等级分别为：

（1）第一级-基本支持：第一级仅对数据备份系统的数据备份频次、用于数据备份介质存放的基础设施、基础的运行维护管理能力以及灾难恢复演练成熟度进行基础的要求。

（2）第二级-备用场地支持：第二级在第一级的基础上增加了针对备用数据处理系统的要求以及备用网络系统的要求，对基础设施提出了关于关键系统恢复能力的要求，并提高细化了运维管理能力的要求。

（3）第三级-电子传输和部分设备支持：第三级在第二级的基础上主要增强了数据备份系统的备份频率和网络传输备份数据的能力要求，并提出了专业技术支持能力的要求。

（4）第四级-电子传输及完整设备支持：第四级在第三级的基础上提高了对备份数据处理系统的要求，提高了备份基础设施的可靠性和连续性要求并在第三级的提出专业技术支持能力的基础上增加并细化了对应的要求。

（5）第五级-实时数据传输及完整设备支持：第五级在第四级的基础上提高了备用数据处理系统中所需恢复设备能力的要求，提出了备用网络对于故障恢复时自动切换的能力要求，并明确提出利用远程复制能力提供备份数据的网络传输能力。

（6）第六级-数据零丢失和远程集群支持：第六级在第五级的基础上明确定义了数据需要实现零丢失，要求利用远程集群系统实现数据处理系统的自动及无缝切换能力，备份数据处理系统需与生产环境完全兼容且能力一致，网络侧也需要提供对主备数据处理系统的双活网络访问能力。此外还增加了运维管理能力中关于具体业务软件的运行管理制度。

此外，基于上述定义的6个灾难恢复能力等级，附录C进一步给出了不同恢复能力等级的业务系统应满足的RTO与RPO性能要求，从第一级要求的RTO大于2天，RPO为1至7天逐渐上升到第六级要求的RTO为数分钟，RPO为0的最高要求。

2.GB/T 30146-2013与GB/T 31595-2015

GB/T 30146《公共安全业务连续性管理体系》与GB/T 31595《公共安全 业务连续性管理体系指南》两个标准分别是对ISO 22301及ISO 22313的等同采用，这两个标准相互协同配合，给出了业务连续性管理工作提出了详尽的要求及对应的指导方法和步骤，帮助企业制定和完善有效的业务连续性计划。

3.GB/T 37939-2019

GB/T 37939于2019年正式发布，全称为《信息安全技术网络存储安全技术要求》是国内第一个针对存储设备安全能力要求及数据安全方面制定的国家标准。该标准中针对网络存储设备自身的安全防护能力提出了相应的要求，并针对数据存储的可靠性、可用性及灾难恢复等诉求，提出了存储产品应提供的安全机制或能力，协助信息系统灾难恢复体系的建设者选择符合业务诉求和相关灾难恢复标准要求的存储设备。

4.GB/T 29765-2013

GB/T 29765于2013年正式发布，全称为《信息安全技术 数据备份与恢复产品技术要求与测试评价方法》，并已于2019年启动新一轮的内容修订。该标准是针对备份与恢复产品制定的国家标准。内容中对备份恢复产品自身的安全防护及其提供的备份恢复能力提出了相应的要求。作为灾难恢复体系中重要的组成产品，信息系统的建设者和使用者应充分参考该标准中给出的技术要求进行数据备份系统的产品选型，更好地实现对应的数据恢复等级能力要求。

5.GB/T 22239-2019

于2019年发布的《信息安全技术信息系统安全等级保护基本要求》被大家简称为等保2.0，是在2008年发布的标准内容基础上经过一轮调整修改的修订版本。其内容作为我国公安部等级保护相关管理制度所参考的技术要求。在标准内容中，针对数据备份恢复提出了具体的要求，参考了GB/T 20988的标准框架，针对包括重要数据、异地灾备中心、备份数据处理系统等对象元素提出了分等级的具体要求。与GB/T 22239配套的其他标准也对数据灾备能力相关的能力测试提出了要求。

级别	灾难恢复能力 等级定义	灾备要求	RTO/RPO要求
一级	基本支持	(a) 完全数据备份至少每周一次； (b) 备份介质场外存放。	2天<RTO 1天<RPO<7天
二级	备用场地支持	(a) 完全数据备份至少每周一次； (b) 备份介质场外存放。 (c) 配备灾难恢复所需的部分数据处理和网络设备或灾难发生后能调配到备用场景	2天<RTO 1天<RPO<7天
三级	电子传输和 部分设备支持	(a) 完全数据备份至少每天一次； (b) 备份介质场外存放； (c) 每天多次利用通信网络将关键数据定时批量传送至备用场地。 (d) 配备灾难恢复所需的部分数据处理和网络设备	12小时<RTO 数小时<RPO<1天
四级	电子传输及 完整设备支持	(a) 完全数据备份至少每天一次； (b) 备份介质场外存放； (c) 每天多次利用通信网络将关键数据定时批量传送至备用场地。 (d) 配备灾难恢复所需的全部数据处理和网络设备，备用数据处理设备处于就绪状态或运行状态，备用网络设备处于就绪状态。	数小时<RTO<2天 数小时<RPO<1天
五级	实时数据传输 及完整设备支持	(a) 完全数据备份至少每天一次； (b) 备份介质场外存放； (c) 采用远程数据复制技术，并利用通信网络将关键数据实时复制到备用场地。 (d) 配备灾难恢复所需的全部数据处理和网络设备，备用数据处理系统处于就绪状态或运行状态，备用网络系统处于就绪状态， (e) 具备通信网络自动或集中切换能力。	数分钟<RTO<2天 0<RPO<30分钟
六级	数据零丢失和 远程集群支持	(a) 完全数据备份至少每天一次； (b) 备份介质场外存放； (c) 远程实时备份，实现数据零丢失。 (d) 配备灾难恢复所需的全部数据处理和网络设备，备用数据处理系统具备远程集群系统的实时监控和自动切换能力，备用网络系统处于运行状态。 (e) 最终用户可通过网络同时接入主、备中心	RTO<数分钟 RPO=0

图表 6 GB/T 20988 - 2007对灾难恢复能力等级的定义

6.中华人民共和国网络安全法

《网络安全法》对于网络运营者以及关键信息基础设施的运营者均提出了相关的数据保护及容灾备份要求。对于网络运营者，《网络安全法》第21条要求网络运营者按照网络安全等级保护制度的要求，采取数据分类、重要数据备份和加密等措施；第25条要求网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告；第42条要求网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。而对于网络安全法所定义的关键基础设施运营者，第33条要求建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。第34条要求关键信息基础设施的运营者还应当对重要系统和数据库进行容灾备份。而对于上述法律义务，《网络安全法》同时也规定了未履行相关义务时的法律责任，其中，网络运营者不履行本法第21条、第25条规定的网络安全保护义务的，最高可以处十万元的罚款，对直接负责的主管人员最高可以处五万元的罚款。而关键信息基础设施的运营者不履行本法第三十三条、第三十四条最高可以处一百万元罚款，而对于直接负责人员可处十万元的罚款。

7.中华人民共和国数据安全法

在《数据安全法》中，第27条要求“开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务”。该条款并未规定特定主体，也就意味着即使不是关键信息基础设施运营者或者网络运营者，只要开展了相关数据处理活动，就有了采取相应的技术措施保障数据安全的义务。

而在相关法律责任层面，《数据安全法》第45条规定开展数据处理活动的组织、个人不履行本法第27条规定的数据安全保护义务的可以处50万元以下的罚款，而对于造成大量数据泄漏等严重后果的，可以处200万元以下罚款，并可以采取责令暂停业务、停业整顿、吊销许可证、吊销营业执照等处罚。另外，对于违反国家核心数据管理制度，危害国家主权、安全和发展利益的，上述罚款可上升至1000万元，同时还会产生相关的刑事责任。

（三）国内外标准分析

结合上述标准调研内容，可以看出针对信息系统的灾难恢复建设，国内外标准均给出了系统级的安全建设框架与要求并实际给出了不同等级的容灾恢复能力等级以更好地应对不同重要程度的业务系统。国内制定的GB/T 20988-2007与国际上受认可的SHARE78从大的等级上对比基本对等（GB/T 20988-2007的第一级包含了SHARE78的0级和1级），说明在应对容灾系统建设需求方面国内外基本保持一致。除此之外，我国还从系统级下沉到设备级，针对灾难恢复系统中使用到的关键设备制定了相应的国家标准以指导灾难恢复系统建设者与使用者选择符合安全要求和恢复能力要求的存储设备。

（四）中国标准落地调研与根因分析

无论国际标准还是我国的国家标准，均对信息系统的灾难恢复能力进行了明确的要求，并针对企业/用户落实实施灾难恢复能力建设提供了一定的方法论框架。但面对明确的要求，如何针对信息系统的业务情况进行灾难恢复能力定级，以及如何基于定级结果参照现有的系统级标准和设备级标准设计建设信息系统的灾难恢复能力机制仍然存在一定的空缺，导致政府机构和各行业领域企业对是否建设灾难恢复系统、如何进行灾难恢复能力定级、如何基于等级要求建设灾难恢复系统存在很多的疑问和理论空缺，导致现有的标准很难有效地落地，真正发挥指导建设灾备恢复能力的作用和目的。

各行业应该基于各自的业务特点及发展需求，积极制定基于标准的灾备恢复系统建设指引，帮助企业与机构理解标准要求并基于标准要求进行灾难恢复能力建设，真正落实并严格执行标准的规定，确保数据和业务安全，遵循《网络安全法》和《数据安全法》的要求。

行业灾备建设现状与趋势分析

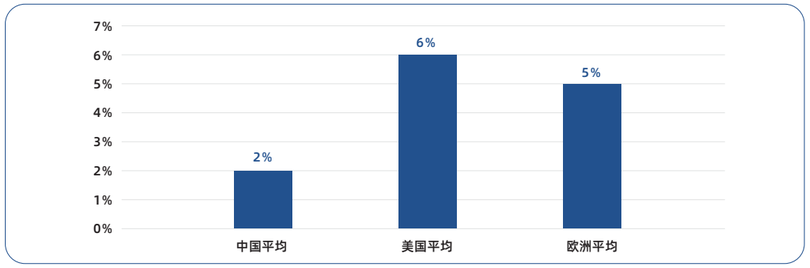
05

五、行业灾备建设现状与趋势分析

我国2020年数字经济已经达到39.2万亿规模，各行各业数字化转型渗透率稳步增长，包括农业、工业、服务业等传统行业也分别达到7.5%，23.5%，39.4%，在世界主要国家中数字经济总量和增速名列前茅。各行各业应该根据其场景现状建设行业灾备体系，出台数据安全保护与灾难恢复建设的政策、标准、指南与演练规范，指导企业建设完备的灾备系统。

（一）国内外灾备产业对比

在全球主要国家和地区，一旦遭到破坏、丧失功能或者数据泄露可能严重危害国家安全、国计民生、公共利益的设施，都属于关键信息基础设施（critical information infrastructure，简称 CII）。包括国防、金融、通信、能源、交通、水利、重大科研、公共服务、电子政务等政府重要部门和领域的关键信息基础设施。这些行业都需要部署容灾备份系统，用于保障重要业务系统的业务连续性，确保全场景数据可恢复。

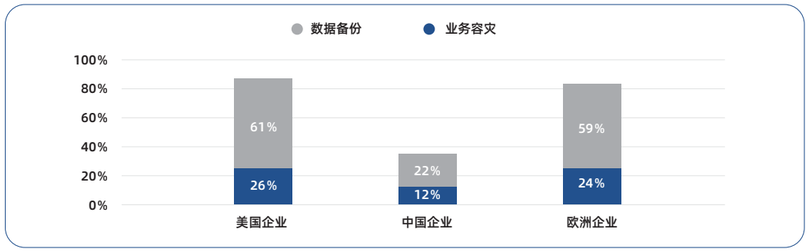


图表 7 信息基础设施投资中用于灾备体系建设的比例

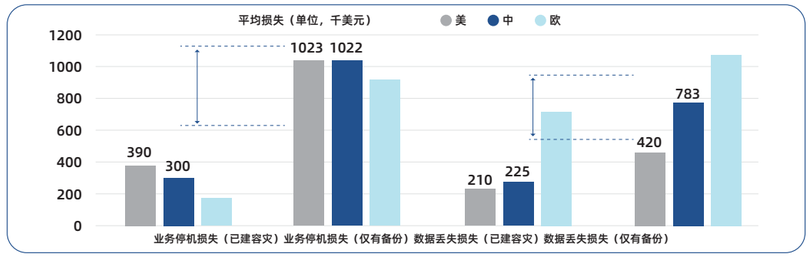
基于上图，我国和欧美灾备投资占总体IT投资的比例，我国灾备体系建设投资远低于欧美。[数据来源：IDC Enterprise Storage System Tracker 2020]

当前，存储以及灾备国际标准几乎都由国外企业和组织制定，中国企业和组织参与率较低。国内绝大部分存储企业技术积累周期短、底层研发能力较弱、全球市场份额低、话语权弱，无法参与协议标准制定层次的活动中。已经发展成熟的基础协议及相关芯片产业依赖国外企业，国内对应的芯片设计能力和产品缺失、当前新进入该领域困难，如SAS、FC等基础芯片，供应体系也被美国把控。

目前，欧美等国都在积极建设灾备体系，仅以大中型企业为例，我国综合灾备覆盖率仅达到34%，美国达到87%，是我国的2.6倍，欧洲则达到83%，是我国的2.4倍，进一步印证了我国灾备建设水平远低于欧美。[数据来自：DELL科技集团 Global Data Protection Index]



图表 8 抽样调查，中美欧大中型企业采取数据灾备措施的比例



图表 9 中美欧大中型企业由于数据丢失和业务停机造成损失的对比

根据全球某的存储与备份产品企业面向中、美大型企业进行的调研数据，中国企业在没有统一数据保护体系的情况下，业务停机损失为美国企业的2倍（78万美元 v.s. 42万美元），反映了中国企业IT治理和维护水平与美国企业仍有差距，更加需要依赖统一的数据保护体系来提升数据保护能力。

另外，中国企业在建设了灾备体系的情况下，业务停机损失降低3.4倍（102万美元v.s.30万美元），数据丢失损失降低3.5倍（78万美元v.s.23万美元），充分显示了容灾备份技术对信息业务系统和数据的保护。

从整体上看，我国数据灾备系统建设远远落后于我国数字经济的发展速度，已经成为影响我国数据安全的薄弱环节，未来也必定会成为我国数字经济发展的重大隐患。

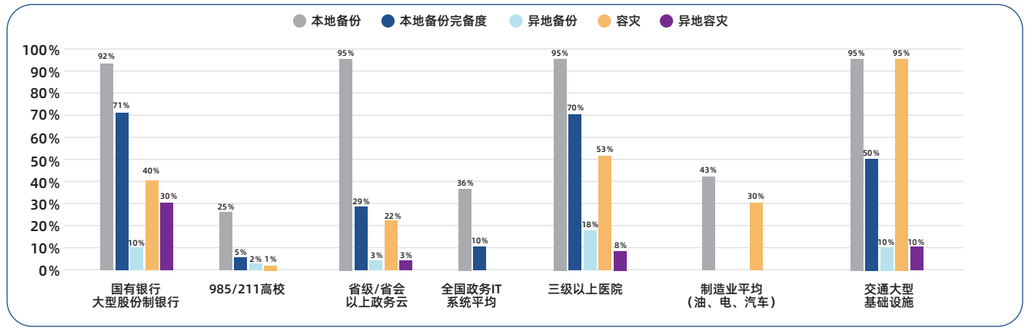
（二）中国各行业灾备建设水平对比分析

金融、通信行业具备信息化程度高和信息安全要求高的特征，部分企业灾备体系建设相对完善，显著降低了数据安全风险。2011年底，银监会发布了《商业银行业务连续性监管指引》，对各种故障对业务的影响进行了细化定义，并给出了银行在灾备建设中的容灾目标。名义上金融行业数据备份建设比例已经达到约92%。

但即便如此，打开金融行业的详细技术架构来看，目前对于数据库软件、存量IBM核心系统的灾备技术可替代能力还很弱，异地备份的比例只有约10%，业务系统容灾比例不到40%，异地容灾低于30%。即使本地备份的完备性也不足，大多数只备份做了一体机或磁盘备份。包括数据库应用、重要非结构化文件等细颗粒度数据本地备份也是不充分的。当前金融行业采用的备份系统仍严重依赖美系厂家，存在巨大的数据安全隐患和供应连续性风险。

政务关乎国计民生，数据丢失、业务中断的代价很高。因此数字政府领域的核心场景如政务云、一体化大数据中心、部委行业云、智慧城市统一数字底座，对灾备体系的建设完备度要求是最高的，但是当前实际建设力度和效果远远不够。

依据“等保2.0”[参见《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》及其它“等保2.0”系列国家标准]、信息系统灾难恢复国家标准[参见《GB/T 20988-2007信息安全技术 信息系统灾难恢复规范》]，依据各行业典型业务系统和数据分类分级的标准与政策，当前由企业、标准化研究机构、学术机构组成的工作组，正在联合撰写各行业的数据保护技术的实践指引。灾备联盟依据这些指引对国内灾备建设现状进行了调研，结果表明，采取本地备份措施的数据中心比例很高，很容易让人放松警惕。但详细分析本地备份采取的措施，例如政府行业大量存在只做了云主机备份，缺乏“裸金属主机”上业务应用的备份；或其他行业仅采取了虚拟机快照、存储快照等备份形式，生产数据和备份数据仍然同一个故障域中。这些备份方案，无法有效保障不同等级的数据不同的备份需求，“备而不全”的现状就非常明显了。



图表 10 各行业数据灾备覆盖率 - 本地备份完备度低、缺乏容灾、严重缺乏异地灾备

金融机构数量众多，对于灾备建设的认识和能力差异性极大。银行保险证券等行业间灾备建设也有着天壤之别。以银行业为例，6大国有大型银行和12家股份制银行已经基本上完成了两地三中心的在灾备建设，正在向多活多中心的技术方向发展。而数以千计的区域性银行在灾备建设上远远不足。以覆盖率来讲，银行业应用的灾备覆盖率不足40%。大部分银行都落实了本地备份建设，但是本地备份的完备度也只有71%。

教育行业普遍对数据安全重视不足，以高校为例，数据灾备比例非常低，容灾建设比例不到1%，只有个别学校如哈工大部署了异地容灾系统，同地校区备份的比例平均在25%左右，异地备份仅达到2%左右。

医疗领域的数据备份系统也体现出水平参差不齐的特点：二级以上医院几乎都会采用数据备份系统，方法手段会有不同，普及率应达到95%以上。容灾技术也是三级以上医院升级换代中的普遍选择，目前有一定的代际差别；二级及以上医院容灾系统整体覆盖率过半，但仅有少数在地域条件允许的情况下会采用远程备份，其实施方案中甚至包括远程硬拷贝等传统方式，总体占比不很高。异地容灾，目前只有建设完成的多院区医院考虑。这种现象并不是由于技术和投入的不足，而是意识的局限。

在制造领域，IT的中断不仅会给生产力、声誉带来损害，更会给收入带来不可估量的损失。一项调查表明，42%的受访者认为停机时间超过四小时的任何中断是他们不能接受的。然而企业决策者对灾备仍然认识不足，预算投入低，没有提供足够资源及预算来保证灾备方案充分实施。我国仍有23%的大型企业，48%的中小型企业和27%的微型企业依靠磁带备份作为主要数据保护措施，严重缺乏独立备份系统及容灾建设严重不足。而且缺乏安全审查与演练，有82%的大型企业平均一年才进行一次灾难恢复测试。[数据来自：DELL集团，Global Data Protection Index]另外，中国企业在建设了灾备体系的情况下，业务停机损失降低3.4倍（102万美元v.s.30万美元），数据丢失损失降低3.5倍（78万美元v.s.23万美元），充分显示了容灾备份技术对信息业务系统和数据的保护。

从整体上看，我国数据灾备系统建设远远落后于我国数字经济的发展速度，已经成为影响我国数据安全的薄弱环节，未来也必定会成为我国数字经济发展的重大隐患。

（三）中国金融行业灾备建设现状与发展策略

金融行业是关系国计民生的重要行业，也是代表着国家经济运行状态的“晴雨表”，伴随着我国经济的不断发展，金融体系也正在持续健全，金融服务覆盖到千行百业。整个金融行业具有信息化程度高和信息安全要求高的特点，因此金融行业对于数据灾备具有极高的行业与政策要求。金融科技信息化程度越高，业务覆盖面越广，业务效率越快，金融机构面临的网络攻击、逻辑错误、自然灾害的挑战也越发强烈。随着移动互联技术在金融行业推广使用，许多金融机构面临的提供7*24不间断服务的要求，一旦金融机构运行、管理的网络设施和信息系统遭到破坏、丧失功能或者数据泄露，将严重危害国家安全、国计民生和公共利益。在 2017年开始实施的《中华人民共和国网络安全法》及其配套法规监管体系下，中国在实行网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护，并对关键信息基础设施的运营者，从保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取、篡改的角度，提出了具体要求。

1.需求调研

金融行业的特点决定了金融机构每天都将处理大量客户敏感信息和与资金相关的业务，包括客户的个人身份信息、个人征信信息、账户信息、鉴别信息，以及与交易相伴随的交易信息、财产信息、账务信息等个人金融信息，既有金融机构在提供金融产品和服务的过程中积累的重要基础数据，也有个人隐私的重要内容。为此，金融机构要尽可能接近于国际标准 SHARE78 的 Tier-6 级别，保证金融业务不中断，每笔业务可回溯。金融机构信息技术部门作为承载金融信息系统的主体单位，灾备建设通常是由信息技术部门牵头完成。在灾备建设过程中，除了满足国家对于信息系统安全基本标准的基础上，还应满足金融行业的特殊要求。

以银行业为例，监管层面对于商业银行业务的连续性和灾备能力提出了高标准、严要求，是必须遵守的红线；同时银行业务面临网络攻击，内部人员错误操作以及金融审计、数据长期保留的多种需求。因此，安全稳定是银行业灾备建设首要考虑，两地三中心+磁盘备份将会是银行业的普遍选择，在对各个数据中心的基础架构进行规划时，也要做好数据同步复制和数据中心双活的规划，通过裸光纤/DWDN 实现同城数据中心间的数据同步，同时同城数据中心应距离大于 50 公里，异地数据中心大于 300 公里，保障机房不会因为地震、洪水等区域性灾难受到全面的破坏，确保银行的数据不丢失，业务不停顿。

而对于证券基金行业，除了安全可靠以外，证券基金交易量受行情影响，系统波动大，IT 资源利用率较低；但相对的，证券基金业务对数据时效要求高，数据变化快速，系统压力波动大，需要实时监控系统压力及业务变化状况。灾备的建设和实施必须不对生产系统造成影响，对于应用的性能影响是证券基金行业灾备建设的首要考虑。各大券商的灾备中心的架构通常采用应用层灾备+存储层容灾相结合的技术，并实现两地三中心部署，确保数据安全和关键业务的业务连续性。

综合来讲，金融机构普遍会面临灾备建设的各种问题，但是由于金融机构的多样性，底层基础架构不同，所应对的系统规模不一样，而等级保护要求的不同，也会造成系统和数据灾备方案的千差万别。我们综合分析银行、证券、保险、基金等主要金融机构，发现主要需求包括：

- 海量数据的备份、CDP、实时复制
- 数据库数据跨平台迁移和读写分离
- 海量业务系统/ 虚拟机跨平台迁移
- 主备业务系统的应用高可用
- 提升灾备中心的智能运维水平
- 大规模灾备系统可用性验证的自动化
- 两地三中心、同城/ 异地灾备的规划

2.面临问题

（1）灾备体系建设水平不一

由于我国区域金融业务发展不均衡以及各金融机构自身实力差异导致各金融机构灾备建设水平不一，大多数国有大中型金融机构灾备体系建设已经基本完备且成熟，而多数中小金融机构灾备建设水平仍然较弱，整体灾备建设水平属于相对较弱的水平，以大中型银行为例，只有＜40%的应用系统部署了灾备方案;灾备覆盖率仍然处于较低的水平。

（2）灾备中心建设过度集中

从地域分布来看，目前我国金融机构，尤其是大中型灾备中心建设选址主要集中在交通便利、经济发达的地区，这其中以北京、上海、广州、深圳为典型代表。

（3）核心技术被外资厂商垄断

金融行业灾备的核心技术有相当部分掌握在上游国外厂商手里，这其中以备份软硬件最为明显，超过90%的备份软件市场为外资企业所垄断，存在较大的风险隐患。

（4）灾备中心使用率较低

按照行业法规和监管要求，每增加一个生产系统，灾备中心就对应建立一个备份系统，灾备中心最终形成与生产环境主备 1:1 的资源配置策略。但这种配置方式不仅仅给运维工作带来了巨大的挑战，同时由于灾备中心正常运行时不承载生产交易，因此灾备中心的配置存在大量闲置的现象。

3.建设方案

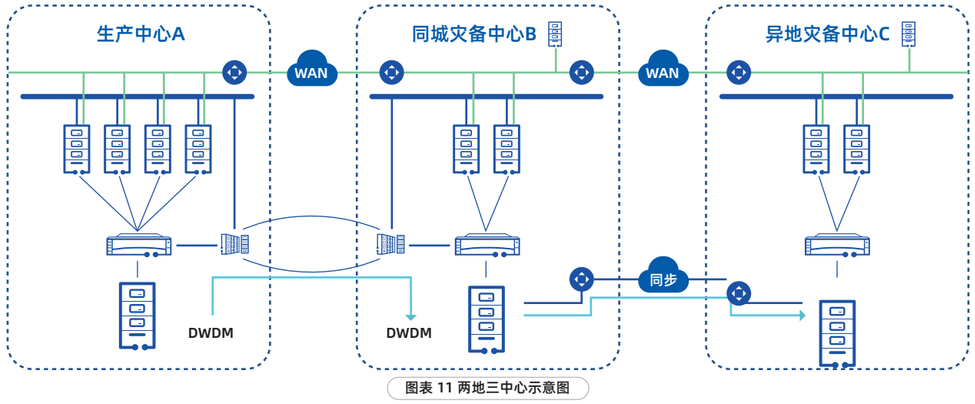
对金融企业而言，应用系统的可靠性、可用性保障的重要性永远是第一位的，全行业都会把业务连续性及灾备建设作为IT运营工作的重中之重。

金融行业灾备建设通常包括存储、计算和网络的设计，目前金融行业主流的灾备建设方案为以存储产品为核心实现灾备建设。建设总体原则是根据不同应用对性能和容灾的诉求进行存储选型，按 A+、A、B、C 4 类应用的业务重要性及对 RPO、RTO 不同要求，重新排列应用主机和存储对应关系，对应不同级别容灾方案完成分层容灾设计。

（1）核心应用容灾建设方案

核心应用主要是指A+类业务，此类业务应具有最高级别的业务连续性、数据安全性和灾难承受能力。同时，核心应用系统应具有良好的访问时延，能够在承载高并发 IO 的情况下及时响应。

核心应用建议采用本地高可用双活组承载在线业务访问，跨数据中心采用存储同步复制进行异地灾备保护；为了保证核心应用系统的高性能，可以采用全闪存存储，根据业务情况配置最优性能，配置阵列双活和同步复制功。



图表 11 两地三中心示意图

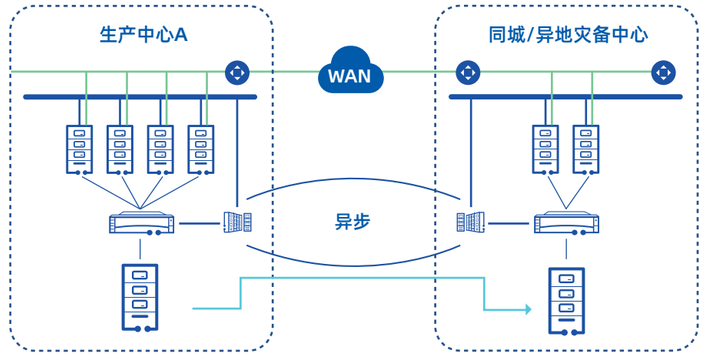
（2）外围应用容灾建设方案

外围应用系统主要指 A 类业务，主要包括 IC 卡、账务总账、客服系统、信贷系统、中间业务等业务。此类应用系统灾备建设要能够应对业务变化带来的各种挑战和新的需求，既有良好的可靠性与性能，又有较强的对不同业务的适应能力。

外围应用也建议采用存储层容灾技术，可以与核心应用灾备方案保持一致，一般采用双活+同步复制的方案。

（3）监管、办公类应用容灾建设方案

监管和办公类应用通常属于数据量较大，时延、性能要求不高的应用，在应用分级中属于B、C类应用。为了降低管理复杂度和故障点，更好地适应后续业务增加，监管、办公区也可以采用高端存储来整合接管当前所有 B、C 类业务，单套系统同时提供块和文件服务能力。此类业务可以容忍极少数据丢失以及系统短时间中断，通过配置异步复制进行容灾保护。

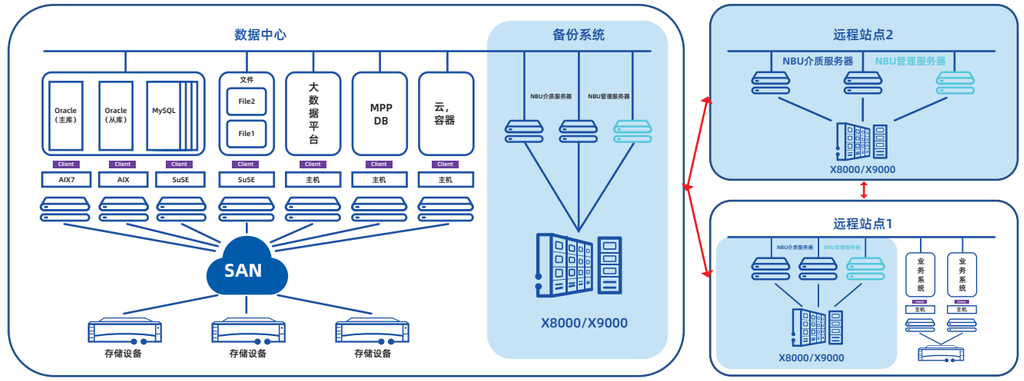


图表 12 双中心示意图

（4）金融应用备份建设方案

随着信息系统的不断发展，IT架构日趋复杂，备份基础已经成为提升系统灾难抵御能力和数据保护水平的“生命线”，是保障众多业务系统运行连续性的基础。据国外不完全统计，在所有造成数据丢失的主要原因中，操作失误占80%，软硬件故障占5%，应用及其他原因占15%，可见人工操作失误对数据影响最大，是不能通过存储高可用基于块级别复制去消除，急需通过数据备份集中平台化策略去消除逻辑错误。在满足监管部门数据备份要求之余，备份系统也承担为金融审计等多种任务提供数据来源的工作。因此，金融行业备份体系建设迫在眉睫，业界主流的备份方案包括集中备份和一体化备份两种。

集中备份



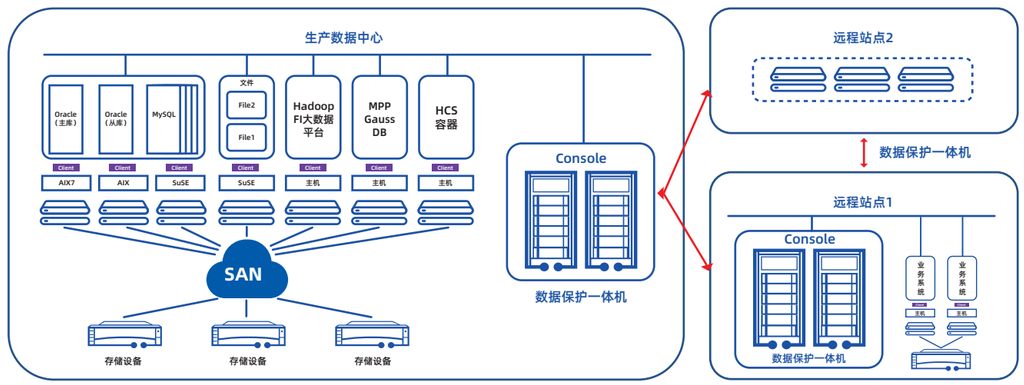
图表 13 集中备份示意图

集中备份方案包括数据中心各类业务系统数据集中备份到统一一套备份系统平台，也包含多分支站点集中备份到总部数据中心。

集中备份方案的组成部分包括：备份服务器（介质服务器，管理服务器），备份软件，备份存储设备。生产系统中需要安装备份客户端client，备份数据通过客户端传递到备份系统中存放。

远程站点1和远程站点2的备份数据可以通过本地备份系统备份，同时备份数据可以传递到数据中心集中保存。

一体化备份



图表 14 一体化备份示意图

一体化备份相对于集中备份方案，备份系统的管理服务器，备份存储，备份软件全部集成到存储设备中实现备份恢复管理功能。规划设计，实施运维相对集中备份方案更简单易用。可以实现相同的备份恢复功能以及远程复制的备份。

（四）中国数字政府领域灾备建设现状与发展策略

新基建、数字中国、智慧城市、互联网+政务等新型城市的建设浪潮，逐步实现人民政府提出的“让数据多跑路，让百姓少跑腿”的郑重承诺，提高公民服务水平，同时也在提高政府形象和社会对政府的满意度。随着政府信息化建设的推进，政府业务对信息系统的依赖性日益增强，政务系统的连续性和灾难保护的重要性也越来越突出。试想如果海关的报关系统停机一天，会给企业带来多少经济损失；如果社保局的数据丢失，会给多少人的生活带来麻烦；如果发生重大自然灾害时政务系统被同时摧毁、无法有效指挥应急救援和灾后重建，将会留下怎样的政府形象……政府部门的业务系统停机，带来的不是直接的经济损失，而是对社会秩序和市民生活的影响，是政府的名誉损失和间接的社会经济损失，这种损失有着不可承受之重。因此，为了保证政府行业信息系统的安全稳定运行，需要在数据保护方面制订有力的管理规范和指引，加强政府行业信息安全保障体系建设，规范政府领域信息系统灾难恢复工作。

1.需求调研

随着政务全面数字化转型，数据爆发式增长，数据体量越来越大，数据类型越来越丰富，数据的价值越来越被挖掘。数据作为生产要素，作为国家战略资源，其完整性和可用性必须得到有效保护，需要保障发生任何灾难或故障，重要数据依然可以恢复和使用。另一方面，公众对于政务服务的依赖程度越来越高，对业务的连续性要求越来越高，特别是面向民生服务的税务、人社、财政等核心业务场景，政府业务平台故障会严重影响政府的形象和口碑。以办税场景为例，目前已超过80%用户选择在线，移动办税(Web、手机APP、微信、12366)。业务模式转变要求业务系统全实时，全在线，可靠性也从以前的5*8h发展为7*24h；互联网纳税、服务大厅、发票查验等业务要求提供7*24小时在线服务。政府业务系统，数据不能丢、业务不能停，灾备建设必不可少；一套完善的灾备系统，容灾和备份缺一不可。

病毒入侵、人为错误、软硬件故障、断网、停电、水灾、火灾、恐怖袭击等潜在风险无处不在,灾难一旦发生，都可能会导致数据丢失、业务中断。局部灾难影响小，但是发生概率高，因此本地高可用+本地数据备份是刚需，等同于为政府业务安全“买社保”。全局灾难发生概率低，但是一旦发生后果十分严重，因此数据、业务高度集中的系统，还需要异地灾备，甚至多级灾备，打造战备级灾备体系，一旦发生水灾、火灾、恐怖行动等重大灾难，也可以快速恢复数据和业务，应急调度指挥，保障灾难的平稳渡过，具有平时保障、战时中枢、灾后重建、平战结合的战略意义。

2.面临问题

政府行业虽然对数据安全、灾备建设的重要性有共识，但是全行业灾备建设进度和效果远远不够，尤其是相较于IT发展更靠前的金融等行业。分析其原因，主要有以下几点：

（1）部分单位对灾备建设意识性不足。灾备建设是负向KPI导向，一旦发生灾难，业务中断、数据丢失，造成了较为严重的后果，影响了领导层和决策层，通常单位都会更加重视数据保护，后面会逐步建设和完善灾备体系。另一方面，政府行业负面事件不易扩散，本单位发生灾难造成事故毕竟是低概率事件，容易出现侥幸心理。事实上，灾备建设是预防性措施，如若没有完善的灾备体系和数据保护措施，一旦发生较大灾害，负面影响已经造成，因此需要提前规划和投资建设。

（2）缺少有力的灾备建设规范和具体建设指导。很多单位知道要建设灾备，但是具体该如何建，建设效果如何保障并不清楚。例如很多单位，建设了本地备份系统，或者利用硬盘将核心数据进行拷贝就觉得已经数据保护了。事实上，不同的灾备措施和建设方案可以应对灾难的等级是不一样的。例如只是数据逻辑备份，应对不了物理介质损坏造成的物理数据丢失问题；本地备份无法应对机房断网、停电、被水淹等数据中心级灾难；有备份无容灾时无法解决灾难发生后在灾备中心快速拉起业务和承载业务的需求。不同类型、不同级别单位的业务系统和数据类型都有所差异，对灾备建设和灾难恢复等级要求都是不一样的，这些都需要专业的建设规范和建设指导告诉不同的单位具体怎么做。

（3）对灾备建设的预算投入普遍较少。政府行业数据保护、灾备建设并没有专项预算，也没有强制政策要求，政府单位在投资IT设施建设的时候，更容易关注到智慧城市、大数据中心等当下热点建设领域，对数据保护、灾备建设投入不足。事实上政府行业信息系统关系国计民生，核心业务和数据必须得到有效保护。为了打造可靠的灾备体系，实现全场景的数据保护，合理投资是必要且十分有意义的。

3.重点场景

（1）政务云场景

十四五规划中提出推动政务信息化共建共用，提高数字化政务服务效能。现在，很多厅局委办业务都部署在政务云上，甚至部分省市政府明确要求涉密之外的所有业务都必须上政务云，业务和数据高度集中，很多业务系统都需要对外提供7*24小时服务，一旦数据丢失、业务中断，将造成极其严重的影响，这对灾备建设等级有了更高的要求。

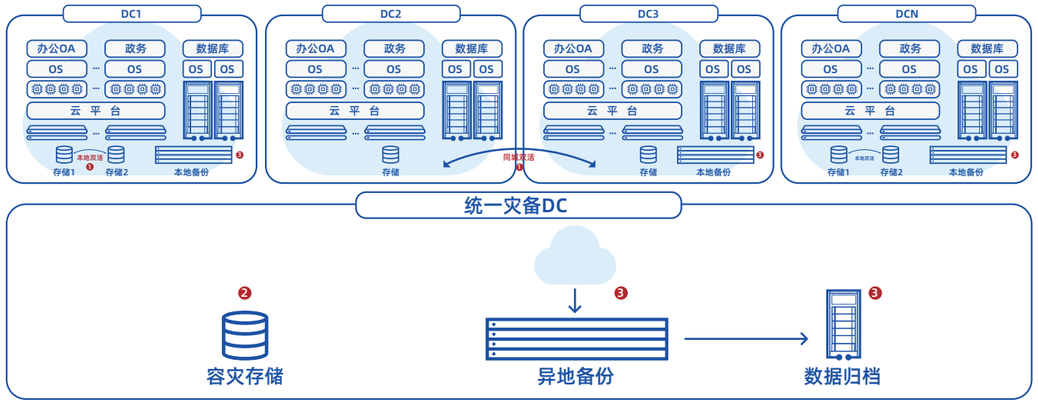
《GW0013-2017 国家电子政务外网标准：政务云安全要求》提出政务云计算基础设施应按网络安全等级保护国家标准中的第三级等级保护要求建设和保护。三级等保中灾备建设要求本地数据备份+异地实时备份+系统高可用。但是等保测评是分数制，很多时候建设单位更多关注网络安全，而忽略了灾备建设。同时，行业内又缺乏其它更具有操作指导意义、要求更明确的灾备建设规范和等级要求。整体来说。当前政务云场景灾备体系建设力度和效果并不好。以省级政务云为例，全国31个省/直辖市/自治区只有不到1/3比例建设了同城灾备，异地灾备建设比例不到1/10；大部分省政务云建设了本地备份，但是缺少异地备份，且本地备份完备度不足，本地备份中95%的比例都备份了云主机，但是仅有30%的比例备份了应用、非结构化数据。这些都导致很多灾难情况下，灾备体系无法发挥好的效果，难以满足核心系统业务连续性和数据安全的要求。

与此同时，国家对于数据安全越来越重视，相继颁布了众多法律法规，对数据安全做出了相关规定，且后面会逐步加强力度。因此，搭建一套专业可靠的灾备系统，是政务云平台建设的重要内容之一，是确保政务服务水平的刚性需求，也是满足合规要求的重要途径。政务云灾备体系不仅需要建设，还需要建设好，尽可能考虑完备。省级政务云的业务和数据更加集中，推荐采用同城双活+异地灾备的两地三中心解决方案，实现数据级、应用级、数据中心级、城市级灾难保护。省级以下政务系统，推荐采用本地双活+同城备份解决方案，保证核心政务系统的7*24小时稳定运行，核心应用和数据不丢失，至少需要满足三级等保要求。

（2）行业云场景

政府行业部委众多，业务类型不同，对灾备建设等级要求也有所差异，建设现状和效果也不尽相同。例如人社系统、财政系统、税务系统、审计系统、海关系统、应急系统等，对业务连续性和和数据完备性要求极高，在部级基本已经完成两地三中心甚至更高级别的灾备体系建设；省市级单位中，税务核心征管系统的灾备建设相对更完善，超过50%的省级税务单位都完成了核心业务系统的双活建设。相对而言，其它部委的省市级灾备建设力度亟待完善。

整体来说，垂直委办部级单位至少具备城市级灾难恢复能力，推荐采用两地三中心架构；省级单位至少具备数据中心级灾难恢复能力，推荐采用同城双活灾备方案。针对垂直度很强的部委，建议统筹规划，采用统一建设、统一运营、分级管理的模式，打造N*2+1+X战略战备体系：N个区域或行业数据中心的关键业务采用双活方案实现业务高可用+本地备份；1个统一灾备中心，实现全行业关键数据统一灾备；X副本：数据生命周期全方位保护，同城双活+异地容灾+备份+归档，防止重复建设，避免资源浪费。



图表 15 行业云N*2+1+X统筹灾备建设

（3）新基建场景

随着信息技术的飞速发展，人类对信息处理能力的要求越来越高，数据开始在我们的社会经济发展中发挥着无可替代的重要作用，比如在新药研发、新车研发、基因测序、天气预报测算等领域，海量科研数据作为生产要素和创新能源，绝不能丢失，必须长期、合理保存。对于超算、智算、国家实验室等创新应用场景，推荐采用备份+归档解决方案，实现海量科研数据长期、合理保存，永久可访问。

4.小结

基于政府行业“缺备份，更缺容灾”、异地灾备比例偏低的现状，建议缺备份补备份，缺容灾补容灾，注重提高异地灾备覆盖率，逐步完善灾备体系建设。另一方面，充分利用资源，开展灾备演练、恢复验证测试、灾备数据应用等工作，做到“战时能战、平时有用”。实现技术先进的灾备方案建设，兼顾制度、规范、流程和服务，构建统一灾备业务管理和安全保障体系，提升信息系统与数据的抗毁能力和灾难恢复能力，确保政府业务安全稳定运行。政府示范先行，构建统一灾备建设规范和建设指南，推动政务云、行业云、国家一体化大数据中心、智慧城市等场景的灾备体系建设和完善，全国范围重点打造一批灾备的示范基地、示范项目，实现标准和政策落地，引领千行百业，应对数据战略背景下的数据安全问题。

（五）中国电信运营领域灾备建设现状与发展策略

2019年工信部发布的《电信和互联网行业提升网络数据安全保护能力专项行动方案》要求：指导电信和重点互联网企业加强内部网络数据安全组织保障，推动设立或明确网络数据安全管理责任部门和专职人员，负责承担企业内部网络数据安全管理工作，督促协调企业内部各相关主体和环节严格落实操作权限管理、日志记录和安全审计、数据加密、数据脱敏、访问控制、数据容灾备份等数据安全保护措施。加大网络数据安全技术投入，加快完善数据防攻击、防窃取、防泄漏、数据备份和恢复等安全技术保障措施，提升企业网络数据安全保障能力。

2020年工信部发布的《网络数据安全标准体系建设指南》（征求意见稿）针对运营商提出了具体的建设内容：5G安全机制在满足通用安全要求基础上，为不同业务场景提供差异化安全服务，适应多种网络接入方式及新型网络架构，保护用户个人隐私，并支持提供开放的安全能力。5G领域的网络数据安全标准主要包括5G数据安全总体要求、5G终端数据安全、5G网络侧数据安全、5G网络能力开放数据安全等。

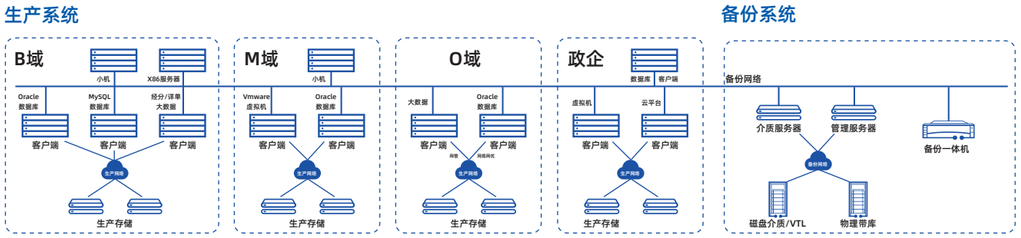
2020年工信部发布的YD/T 3736-2020《电信运营商大数据安全风险及需求》提出，在数据存储安全，应提供完备的数据备份和恢复机制来保障数据的可用性和完整性。一旦发生数据丢失或破坏，可以利用备份来回复数据， 从而保证在故障发生后数据不丢失；容灾备份方面，大数据平台应当具备容灾备份与灾难恢复能力， 为关键数据、关键应用建立异地备份。

1.建设需求

2020年相比2019年各行业数据保护投入力度增大，平均增幅达到18.6%，运营商行业尤为明显，增长率高达31.8%。电信运营商作为个人和企业用户间互联互通的智能管道，其数字化建设涉及利益相关者甚多，其安全问题一直备受各界关注。在各类新兴技术带来时代变革的同时，也为电信运营商的信息安全问题带来了更大的挑战，如人为误删除、系统故障、勒索病毒、自然灾害等。一旦发生数据丢失导致业务中断，将带来严重的经济损失和社会影响。为此，在不断深化新业务创新的同时，电信运营商需要强化数据和业务的保护工作，确保用户数据不丢失、核心业务7*24小时不中断。

2.建设方案

运营商备份业务覆盖B域、O域、M域以及政企，备份数据来自各类数据库、各种虚拟化平台、不同种类的大数据平台等。备份方案既有传统的集中备份方案，又有备份一体机方案；备份介质既有物理带库\虚拟带库，又有磁盘阵列。



图表 16 运营商备份全景图

随着新业务新技术的不断涌现，运营商备份方案也需要不断优化和完善。

运营商容灾主要覆盖B域、CT等核心业务场景，当前以两地间应用层容灾为主，未来需要考虑建设更完备的两地三中心容灾方案。

优化项	当前问题	优化方案
备份性能	随着5G时代到来，备份的数据量越来越大 但备份时间窗并没有增加	使用永久增量备份技术减少 备份数据量，缩短备份时间
	传统备份方案中数据需要恢复之后才能使用 关键业务恢复时间长为小时级或天级	使用原生副本技术,直接挂载 给生产系统，实现分钟级业务恢复
备份生态	国产化数据库、开源软件、大数据平台兼容性不足	备份方案需完善国产化数据库、 开源软件、大数据平台的兼容性
备份服务化	运营商云化转型趋势明显，备份服务需求迫切	备份方案需以服务化的 方式对接云平台

图表 17 运营商备份建设趋势

（六）中国教育行业灾备建设现状与发展策略

教育行业是我国最大的民生行业之一，也是网络安全法定义的关键基础设施行业对象，随着教育行业信息化建设的快速发展，信息系统安全问题屡见不鲜。根据“教育部印发《教育信息化 2.0 行动计划》教技〔2018〕6 号”的文件要求，在“教育信息化 2.0”的保障措施方面，明确主体责任人要“担当责任，保障安全”，各单位的行政级别、部署模式和业务类型，与信息系统受到破坏后造成的危害程度进一步明确，将教育信息系统安全保护工作摆在了重要位置、重点评测对象、党委重视的关键事项。2021年教育部颁布的关于加强新时代教育管理信息化工作的通知，在第五项重要的任务中，进一步指出，要提高基础设施支持能力，加强健全数据中心资源调配，应急管理和容灾制度，优先选用自主核心技术和安全达标的国产化产品，重点保障关键信息系统等基础设施高效、安全、稳定运行。

本文所涉及教育机构主要是教育管理部门、普通与成人高校、大中专院校、中小学、科研院所等教育行政部门及其直属事业单位，对应《中华人民共和国网络安全法》 等级保护的安全保障基本制度，提出教育行业灾备系统等级保护和信息安全保障体系建设规范，分享适应本行业的保护建设指南，供更多同仁研究、参考。

1.业务需求

高校的灾备业务发展需求主要体现在以下四个方面。

高校扩招

据相关报道，“十四五”期间应届生将达到1600万/年。智慧校园的消费、认证、网络学习、一网通办等信息系统的数据将增长近10倍，数据交易频次更加频繁；核心数据库并行能力不足、数据流动缓慢、数据分析不及时等现状亟待改变。

新校区增多

“十四五”期间为推动区域教育均衡发展需要，“双一流”、“ 985”“ 211”、“ 双高高职”将迎来新校区扩建潮。跨省、同省、同城多校区信息化联动逐步成为常态，涉及院校达千所。

科研投入及数据增长

截止2021年，我国高校科研经费增涨到2亿/年。交叉学科科研经费拨付由14%提升到46%。部分高校合成材料、海洋气象、生命科学、航天科工、金融科技等高性能计算领域的数据将高达30PB。而如此重要的科研试验数据，大部分院校甚至连计算环境及计算数据的本地副本都没有建立。

数据保护意识亟待加强

通过对高校客户调研走访发现，全国高校都已建立了党委负责制下的校园信息安全或网络安全小组，从组织与机制上保障校园信息安全。但是，尚未建立业务连续性治理体系。这包括：缺少灾备的顶层设计与业务连续规划，灾备经费在信息化总体投资占比不足0.5%，普遍缺乏持续性容灾经费投入保障；专业组织与技术人员支撑能力不足；通信保障、危机公关、灾难恢复规划、业务恢复预案、紧急事件响应、供应商危机管理机制不健全；能够建立、健全系统化容灾制度与应急响应策略的院校更是寥寥无几。

2.容灾需求分析

随着十三五规划的落地，数字校园到智慧校园信息化建设进一步升级。2021年通过走访广东、江苏、北京、上海等地多所院校、教育局调研，发现95%的高校具有信息系统风险保护意识，通常采用备份脚本、专业备份软件、专用备份硬件设备对应用系统、数据库及文件进行时、天、月增量备份，能够建立本地Tier-2、Tier-3；只有占比不足10%的教育机构对关键信息系统实现了Tier-4级备份，只有2.5%的用户建设了Tier-5级多地双活容灾方案。学校灾备整体投资不足，只有信息系统总体投入1%，整体灾备运营体系、制度、基础设施落后等现状亟待改善。

NO	教育机构	类型				多校区情况	容灾系统建设情况			
		双一流	普高	高职	教育局		本地灾备	同城异步	同城双活	两地三中心
1	江苏高校A					2校区	☑			
2	江苏高校B		☑			7校区	☑			
3	江苏高校C	☑				2地4校区	☑	☑		☑
4	江苏高校D	☑				2地4校区	☑			
5	江苏高校E	☑				3校区	☑	☑		
6	江苏高校F	☑				4校区	☑			
7	广东高校A		☑			2地2校	☑			
8	广东高校B	☑				4地5校区	☑	☑		
9	广东高校C		☑			1校4区	☑			
10	广东高职D			☑		1校区	☑			
11	广东高校E	☑				2地2校	☑			
12	浙江高校A	☑				7校区	☑	☑		
13	北京高校A	☑				2校区	☑			
14	北京高校B	☑				3校区	☑			
15	北京高校C	☑				2校区	☑			
16	北京高校D	☑				6校区	☑			
17	北京高校E	☑				2校区	☑			
18	北京高校F	☑				2校区	☑			
19	上海高校A	☑				5校区	☑			
20	上海高校B	☑				4校区	☑			
21	吉林高校A		☑			4校区	☑			
22	陕西高校A	☑				2校区	☑			
23	郑州高职A					-	☑			
24	湖北高校A		☑			2校区	☑			
25	云南高校A						☑			
26	Y省教育厅				☑	3校区	☑			
27	Y省某县教育局				☑	-	☑			
28	Z省某市教育局				☑	-	☑			
29	B市教育局				☑	-	☑			
30	B市某区教育局A				☑	-	☑			
31	B市某区教育局B				☑	-	☑			
32	天津某高校图书馆			☑		-			☑	

图表 18 教育相关机构容灾调研样本表

与此同时，高校对信息系统高效、可靠的要求日益增高，其对灾备诉求主要有三个方面：

1、智慧校园、一网通办服务、统一身份认证、一卡通认证与消费、学生选课、网络教学等信息系统，任何业务停顿，会造成流程拥堵或业务无法回滚，使得学校对信息系统并行处理能力要求提升；

2、受硬件设备接口卡、光纤连接、硬盘物理损坏等硬件故障导致的信息系统崩溃、数据丢失，通常需要经历长时间系统恢复过程。期间重录数据、处理业务投诉、协调相关部门等事宜承担重大事故压力，使得信息化运维部门对系统可靠性保障意识增强；

3、扩招带来多校区机房建设，运营商城际光纤网络连接的低价与便利性，使得更多用户考虑多校区就近部署应用系统，缩小本地服务时延，保障信息系统安全可靠运行的容灾备份策略；

“十四五”期间，受《信息安全技术网络安全等级保护基本要求》等立法与政策牵引，会趋向事前防御、事中响应、事后审计的动态保障体系转变，Tier-5级数据中心占比将提升到60%。

综上所述，为确保智慧校园服务与业务治理、疫情常态网络教学、校园安防、科研支撑信息化系统的业务永续，需要对于关键的教学科研、生活服务、财务、档案等应用的数据进行实时灾备保护，以达到防范机房火灾、断电、网络入侵、人为误操作、勒索病毒攻击等可能导致数据丢失和业务中断的危险事件的发生。

3.教育信息系统基于分级的容灾场景

因此，教育单位应在信息化建设初期对容灾工作做顶层设计，制定统一的灾备策略。早期高职院校信息化投入大，建设早，随着学校规模扩大，原先单个数据中心存在资源利用率低，数据丢失率高，业务中断时间长等各类问题，以下三种方案能覆盖大部分高校数据中心多样存储复杂环境，对业务负载均衡、业务0中断、故障0感知、极简化管理和平滑升级提供参考。

3.1.教育信息系统备份

信息系统全生命周期保护包含容灾、备份、归档。“容灾”，即保障业务系统在灾难条件下的连续性；“备份”，即保障关键数据在灾难条件下的完整性；“归档”，即保障数据的长期合规留存。信息系统同城/异地备份通常为下列几种情况：

基础设施建设经费不充足或建设初期应用数量较少；

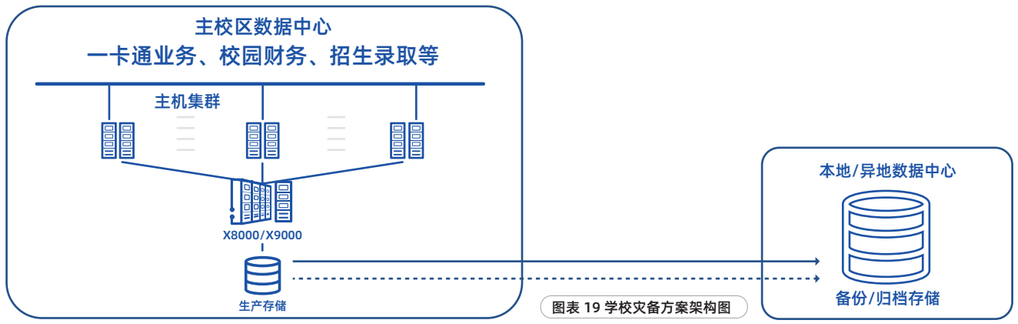
应用系统瞬时响应与用户并行访问压力较小

分校区之间城际网络传输延迟较大，带宽不足；

校区间物理距离不超过300公里；

软件交付对容灾开发不支持

该情况下，只需要备份校园应用系统的程序、文件、数据库等，不需要同时部署在多地数据中心。如主校区数据中心有媒体资源的分布式存储、公共数据库和ETL数据交换的数据库集中存储，也有超融合虚拟存储和数据库，均可以根据实际需求进行按天或者按时进行备份。该方案技术实现简单，当发生逻辑错误、硬盘损毁、病毒攻击，确保数据不丢失，可进行任意时间点的数据恢复。



图表 19 学校灾备方案架构图

适用场景：智慧校园、一卡通、媒体资源、财务、桌面云、一网通办、网络教学等校园应用。

场景特点：信息数据交换吞吐较低、文件拷贝不频繁、应用系统访问流量不高、关键应用系统RTO>1天。

3.2.教育信息系统跨校区多地容灾

信息系统跨校区多地容灾，能够实现“热数据全容灾，温数据热备份，冷数据温归档”的全生命周期数据保护系统，实现关键数据系统的“三不两永远”。采用多地容灾通常为下列几种情况：

基础设施建设经费充足；

分校区关键业务的高速访问体验需求；

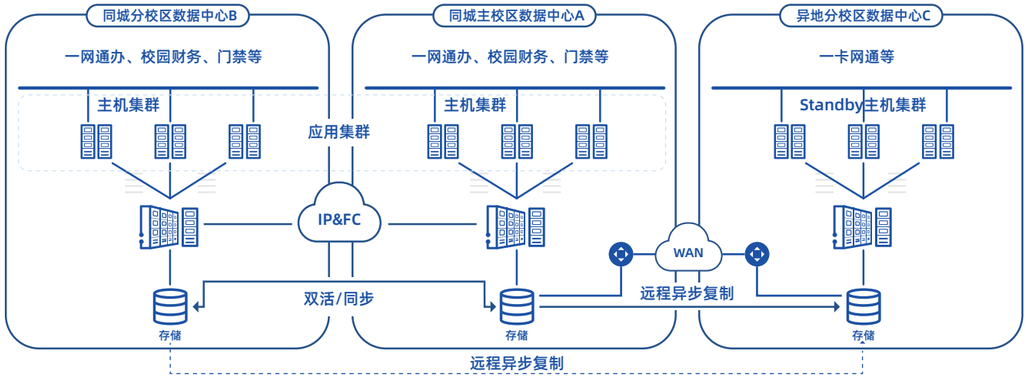
分校区用户数量庞大，城际网络传输低时延或带宽充足；

多校区混合云建设；

校区间物理距离超过300公里；

学校建立多校区容灾中心，一般会参考两地三中心建设与规划模式。信息系统将同步部署在多地数据中心，不仅能够加强并行访问能力，更能避免灾难出现时的隐患。

下图所示：分校区数据中心B提供基于超融合的一网通办服务，私有云B也同时纳入主校区数据中心A管理，因为本身超融合基于分布式系统架构，不需要集中存储，但仍然考虑到数据库的完整和独立性，仍需要进行本地数据备份，以便出现故障进行数据库审核。分校区数据中心C将提供智慧校园容灾能力，其私有云C也同时纳入主校区A管理，实现混合云资源的整体管控。该方案将智慧校园平台的应用、数据库、虚拟机实现在线热迁移，数据不丢失，并同步本地和主校区数据中心最新数据。



图表 20 多校区两地三中心方案架构图

适用场景：智慧校园平台、一网通办、一卡通、门禁等应用。

场景特点：信息数据交换快、并行吞吐率较高、应用系统间存在高依赖性、文件拷贝频繁、应用系统访问流量高、关键应用系统RTO<1小时的，适用于对灾难风险认知度较高的教育机构。

3.3.教育信息系统上云灾备

信息系统上云及灾备优点是继承了上述章节所有特性，同时也降低了系统崩塌风险和恢复过程的技术复杂度，上云灾备通常为几种情况：

校方信息化基础设施建设经费短缺；

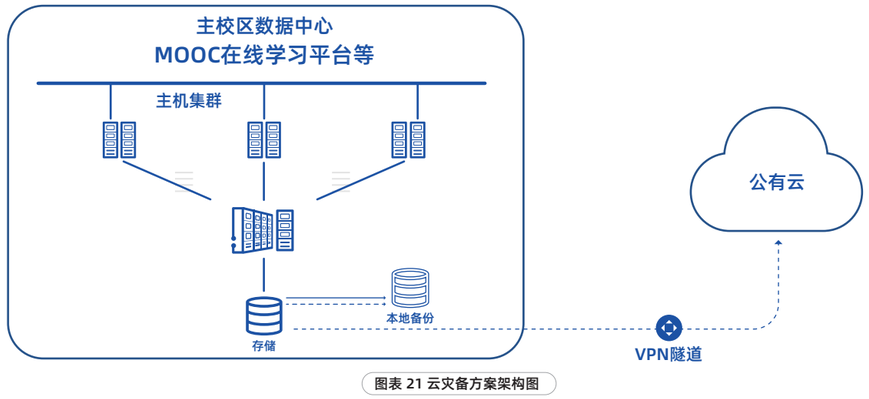
面向全球或全国用户服务需要CDN支持；

缺少技术运维人员，将等保和IT运维管理上云或减负外包；

性能有短期突发性峰值需要，基础设施建设无法预估成本；

主管单位或政府有强制性上云要求；

学校统筹业务系统上云，信息系统和数据存放在云端可减少大部分的灾难隐患。建议将网络教学系统的应用、数据库、虚拟机等实现在线热迁移，数据不丢失，保持本地和云端信息安全同步。同时做好本地备份，保持最新数据。



图表 21 云灾备方案架构图

适用场景：MOOC在线学习平台、集中化教务选课。

场景特点：海量的教学资源和频繁的学习行为采集；选课期间突发性吞吐率提升，数据调度频繁、大范围重复数据调取等，云灾备将会降低突发性流量超负荷风险，并增强系统可靠性。

（七）中国制造业灾备建设现状与发展策略

制造业是指机械工业时代对制造资源（物料、能源、设备、工具、资金、技术、信息和人力）等按照社会发展的要求，通过制造过程，转换成人们需要的大型工具、工业品、生活消费品的行业。

制造业数字化进程已经进入加速发展期，云计算、大数据、AI、5G等新兴技术在制造业互联网垂直行业持续发力，实现工序数控化、远程运维、预测性运维和设备物联等智能制造的应用场景。制造业转型成为全球业务发展趋势，如德国提出了国家工业战略2030，中国制造业发展2025，美国提出了未来工业发展计划。为促进制造业的加速转型升级，中国制造业2025发展战略提出了工业发展的方向，如：提高国家制造业创新能力、推荐信息化与工业化深度结合、强化工业基础能力、智能制造等一系列方针。十四五规划建议提出，系统布局新型基础设施，加快第五代移动通信、工业互联网、大数据中心等建设。与此同时，全国多地也在加快部署“十四五”工业互联网产业发展工作，积极抓抢产业发展的窗口期与机遇期，因此推动了制造业往数字化、智能化转型。制造业的深度转型，涉及到制造业的业务流程的方方面面，包括协调制造、个性定制、人工智能等。

1.业务需求

在数字化浪潮的推动下，制造企业逐渐具备整合来自研发、生产、管理、营销等多方面数据的能力；由此，制造企业不仅在创新能力上大幅增强，还拥有了对业务流程和组织流程再造，突破发展瓶颈的潜力。一个新趋势越来越明显：在制造业，企业“数据资产”正在逐渐取代“固定资产”的地位，成为企业数字化转型和持续经营的关键。但随着数字化的持续推进，传统的数据安全保障手段逐渐失效，制造企业正在面临更多的攻击和风险，尤其商业秘密和技术专利等与企业生死存亡密切相关的敏感数据保护，正变得日益迫切。

对于制造业而言，如何给数据增加一道安全防线，确保核心业务不中断；如何实现高效的数据保护帮助企业盘活“数据资产”，推动数据价值的释放显得尤其重要。GB/T 222239-2019《信息安全技术网络安全等级保护基本要求》通用要求进行防护，还需要按照工业控制系统安全防护要求进行防护。如何建设灾备系统，中国灾难备份与恢复行业的第一个国家标准《信息系统灾难恢复规范》，它作为各行业进行灾备建设的重要参考文件，具有重大意义。规范定义了灾难恢复能力等级，灾难恢复等级的确定是信息系统灾备建设的重要考虑因素。规范将灾难恢复能力划分为6级，灾难恢复能力等级越高，对于信息系统的保护效果越好，但同时成本也会急剧上升。

随着信息技术的发展，制造业的数据保护技术也从同机房的本地备份向同城、异地及云端等更大的平台和场景延伸，用户数量更大，产品也更加丰富。

由于企业规模的不同，灾备模式也会不同。综合上述那么制造业的业务需求主要包括以下几个方面：

数据安全威胁凸显，增强数据保护迫在眉睫

Dragos公司发现，2018年1月到2020年10月间，所处理的针对工业机构的勒索攻击增长了500%。根据基伍咨询公司（Kivu Consulting）2020年发布的报告显示，制造业在勒索软件支付方面的支出超过了其他任何行业，共支付了690万美元。占到整个2019年支付给网络犯罪分子1100万美元以上赎金总额的62%。相比较其他行业，网络攻击给制造行业带来的危害更为突出。轻则敏感数据泄露、知识产权被窃取；重则给工厂和设备造成永久性损害，导致生产中断，甚至让制造企业破产。尤其对于高度依赖IT系统开展生产、自动化、质量保证、监控和安全的工业活动，网络攻击极易导致生产过程中断，给企业带来严重损失。

近年来，我国在政策层面已经出台了《网络安全法》，《数据安全法》等一系列法律法规，增强数据保护力度；但制造企业要增强数据保护能力，首先要提升思想和意识上的重视程度，通过制定完善的数据安全制度，加强日常监督管理，从源头上降低企业信息泄露的风险；在此基础上，由于传统数据保护技术已经难以应对不断升级的网络攻击，制造企业还必须寻求借助新的数据保护解决方案，以消除和控制网络攻击带来的危害。

制造业关键应用业务连续保障，宕机损失严重，需提供不同等级的容灾保护。

遭遇灾害时，如何保障制造业核心业务系统业务不中断，保障业务连续性是制造业面临的难题。相关数据表明，关键应用的宕机给用户带来的损失是巨大的；50%以上的小型制造企业每小时关键业务宕机时间损失超过1万美元；55%以上的型制造企业每小时关键业务宕机时间损失超过4万美元。

行业细分应用场景需提供专属保护

众所周知，制造业是一个门类繁多、产业链极长的行业，不同的细分行业应用场景千差万别。工业设备繁多，不同应用场景下产生的数据格式和数据类型差异明显，给制造行业的数据保护带来了巨大挑战。

防患于未然

当前，制造业正迎来“工业4.0”的重大发展契机，面对需要将无处不在的传感器、嵌入式系统、智能控制系统和产品数据、设备数据、研发数据、运营管理数据紧密互联成一个智能网络的新模式，一个全新的安全需求正在产生，解决安全问题已经变为第一要务。

2.容灾建设需求及特点

从工业4.0到中国制造2025，其核心都是通过智能化实现制造业的转型升级，工业制造的安全远高于消费数据，在采集、存储、应用过程中出现数据丢失，将给企业和用户带来巨大的安全隐患。如遇到数据被篡改，可能导致生产过程发生混乱、甚至威胁城市安全、人身安全、基础设施安全及国家安全。

为了确保数据安全性、高频交易、高并发、以及7*24小时业务连续运营，具有冗余功能的网络建设和集中存储备份，容灾的需求越来越紧迫，制造业也属于大型门类，容灾建设还有很多不足如：

企业决策者对灾备需求认识不足，预算投入低

在制造业企业的整体工作链条中，数据及系统这种隐形产出并不能直接体现在最终的销售利润上，而多数制造企业的IT设备也较为简单，在企业的预算中，IT被认为是一个消耗公司利润的部分，因此，在很多企业不管是CIO还是CEO都没有提供足够资源及预算来保证灾备项目的实施。

灾备软件、硬件种类、解决方案等繁多无从选择：

目前市场上有各种各样的灾备软件，有基于存储虚拟化的，有基于备份软件的，有基于快照的，有基于CDP的，有数据库文件层面的，有事务日志层面的，种类繁多。如何选择适合企业的灾备软件，如何在有限的资源下为企业提供更高的数据保障，避免灾备软件对硬件的兼容性需求，降低硬件的投资成本，提升投资回报比，这是一个令众多IT经验并不丰富的制造业企业决策者头疼的问题。另一方面，制造业企业的IT环境中有各种数据库平台、中间件平台，数据库有HA、RAC，应用有负载均衡，硬件平台有物理机、虚拟机，各业务系统对RPO、RTO的需求也并不一致，所以系统的统一灾备管理是必要且必须的。

制造业业务系统数据安全性存在很大风险

传统制造业采用PC办公，数据面临严峻的管理风险，数字化转型的今天，制造业业务系统孤立，且有大量的本地设备，如Windows、自动化机器、业务系统等，且部分定制系统老旧，系统裸奔情况较多，外加数据爆炸式增长，数据价值高。信息系统如果出现逻辑故障，则容易成为勒索病毒等攻击的目标。除了勒索病毒攻击，人为误操作、软硬件故障、机房环境风险造成数据丢失的问题也不容忽视。

业务系统的业务连续性、数据一致性、可靠性、可维护性

容灾建设需要考虑灾备系统对原有的业务系统产生的性能影响，如通过采用I/O复制技术对业务系统带来的I/O延时。为保证业务系统的业务连续性，需要有一套有效的技术和验证机制来确保生产系统和业务系统的数据是一致可用的。工厂缺乏熟练的IT支持员工，灾备系统的维护工作要尽量轻、简化，并能够承担部分业务处理和测试工作。容灾系统的管理是容灾切换成功的重要保障，所以在系统建设的过程中就要考虑到容灾系统的管理维护流程。业务系统升级，上新的业务系统都要和灾备系统联动，考虑和灾备系统维护管理的关联性。

数据高效利用和挖掘数据价值

数据资产是企业生存的根本，传统的数据保护解决方案专注对数据周期性备份，存在数据一致性、有备份窗口以及对生产系统影响等问题。企业对数据资产保护的诉求推动数据保护技术一次次变革，如何能快速的实现数据备份，保证数据一致性的同时，减少数据备份对生产系统业务性能影响，备份数据再次利用，快速恢复已经成为现在数据保护的趋势。而制造业里涉及到的研发数据、生产数据和业务数据如何实现高效的备份，在节省存储空间的同时，又能挖掘数据的价值显得尤为重要，例如使用备份的数据为决策和机器学习提供真实的数据来源。

3.灾备建设方案

在制造行业，企业IT环境主要分为三个主要大类核心经营生产厂家，企业管理、协同办公，分别包括：

1、 核心经营生产场景：ERP、CRM、MES、CIM、DMS

2、 研发场景：CAE、EDA、PDM、PLM

3、 协同办公：门户网站、OA、Email邮件系统

针对三类系统，建议使用不同的数据保护策略。制造业灾备解决方案建设需要考虑的思路：

RTO与RPO是衡量整个灾备建设方案的关键指标

数据安全、网络安全

数据一致性、可恢复性

业务连续性、可靠性

可管理维护性

法规遵从性，法律法规要求生产数据需要保存10年以上。

对于企业业务连续性要求高的IT系统可采用两地三中心、同城双活灾备方案；对于业务连续性要求不高的场景可采用主备容灾、本地备份、异地备份等数据保护策略。对于很多制造企业，可能会选择其中的部分模式，或者全部选择，完全取决于企业对灾备的需求。针对制造业的行业特点，制造业业务系统全生命周期保护包含容灾、备份、归档。“容灾”，即保障业务系统在灾难条件下的连续性；“备份”，即保障关键数据在灾难条件下的完整性；“归档”，即保障数据的长期合规留存。制造业业务系统灾备建设通常为下列几种方式：

3.1.制造业核心生产经营业务系统数据容灾采用双活或异地容灾的灾备解决方案

针对制造业数据安全及业务连续性的需求，可采用同城双活及异地高可用解决方案，方案特点如下：

（1）业务系统特点：ERP、CRM、CIM、DMS等核心建立系统同城双活，并实现业务数据实时同步。异地采用复制链路提供数据冗余保护，当本地出现不可预知的自然灾害等区域性灾难时可使用异地的容灾中心将业务拉起。

（2）场景特点：核心数据、多并发，多方调用，牵一发动全身。（3）数据特点：用户数据实时同步，防病毒勒索；保证数据的可用性，完整性，可靠性等。

（4）核心业务连续性特点：

AA双活架构，数据零丢失，业务零中断（RPO≈0，RTO分钟级）。

两个数据中心同时提供业务，充分利用灾备资源。

方案扩展灵活，容灾可视化管理。

（5）容灾演练特点：当系统出现故障或者灾难时可快速进行容灾切换。

（6）适用场景：制造业的核心业务系统，对系统的业务连续性要求高，（RPO≤15分钟，RTO≤2小时）的场景。生产数据中心和灾备数据中心同时对外提供业务处理功能，同时当有一个业务系统数据中心出现故障不能对外提供业务时，另外一个业务系统仍然能对外提供业务服务，保证业务7*24小时的业务连续性。

3.2.制造业研发系统CAE、PDM、PLM、EDA采用同城容灾和和异地备份的方式

（1）方案设计要点如下：

在制定容灾系统方案的过程中要考虑的就是容灾系统建设对原有业务系统带来的影响。

数据状态要保持同步；

容灾系统的日常维护工作要尽可能轻，并能承担部分业务处理和测试的工作；系统恢复时间要尽可能短；可实现部分业务子系统的切换和回切；

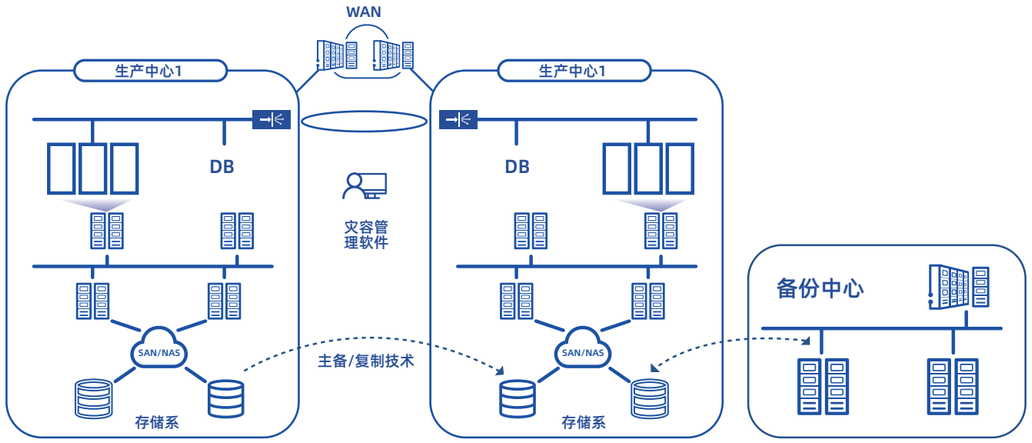
技术方案选择要遵循成熟稳定、高可靠性、可扩展性、透明性的原则；构建系统方案可以选择多种技术组合方式

（2）主备容灾/同城容灾和异地备份方案特点如下：

同城灾备中心通常具备与生产中心等同业务处理能力，应用可在不丢失数据的情况下切换到同城灾备中心运行，保持业务连续运行。在出现小概率的大范围的灾难时，如自然灾害地震，造成同城灾难备份中心与生产中心同时不可用，应用可以切换到异地灾难备份中心。通过实施经过日常灾难演练的步骤，应用可在业务容许的时间内，在异地的灾难备份中心恢复，保证业务连续运行。但异地恢复通常会丢失少量的数据。

容灾系统可管理和可维护性友好，有利于平时的灾备演练，当真正出灾难时，能够快速切换，确保实现业务数据RPO约为60分钟，RTO约为4小时。

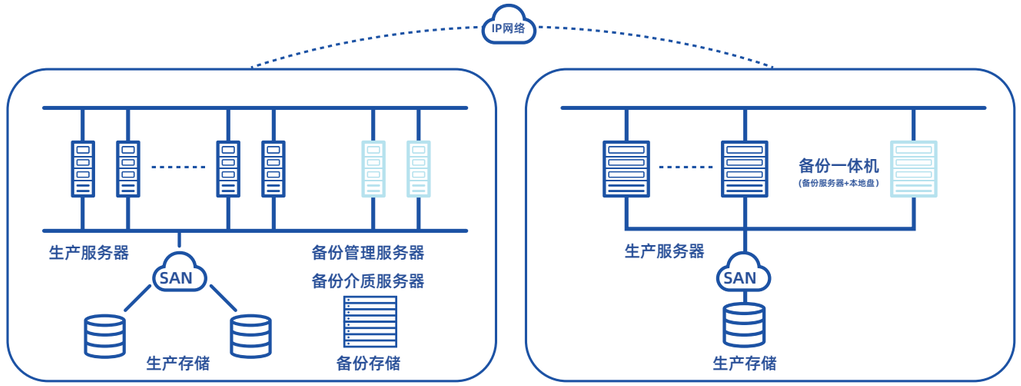
适用场景：研发的业务系统ERP、PLM、PDM、MES、EDA、CAE等系统对数据的安全性高，业务连续性高的场景，除了在同城数据保护外可以建立异地数据保护。预防当本地数据中心出现区域性的灾难时，异地的数据中心可以提供完整的数据，将业务快速拉起的场景。



图表 22制造业研发业务容灾-两地三中心示意图

3.3.本地和异地备份

对于制造业非核心的业务系统，如创新系统、门户网站、办公OA等数据对于RTO和RPO要求不高的系统，可采用本地备份和异地备份的方式。某些已经上云的业务系统，可采用云灾备的方式来实现数据保护。



图表 23云灾备示意图

未来的数据中心的灾备需求更灵活，制造企业需要定义备份数据流的走向，灾备建设不只起到容灾备份的功能，还具有数据管理、备份数据分析、数据报表等功能，备份系统应整合数据管理系统，成为一个提供统一的数据容灾备份和管理的平台。

（八）中国能源行业灾备建设现状与发展策略

能源行业关乎国计民生，火灾、地震、台风、战争等不可抗力因素和主机故障、电源故障、存储故障、人为破坏等突发灾难，都可能造成大企业行业信息系统中断，将会直接影响到国家战略实现、社会生活稳定和国民生活正常运转。因此，为了保证能源行业信息系统的安全稳定运行，加强能源行业信息安全保障体系建设，规范企业领域信息系统灾难恢复工作，本文尝试对能源行业在数据保护方面提供管理规范和指引。本文仅涵盖能源代表性行业 - 油气和电力 - 在数据灾备建设方面的思考。

1.业务需求

首先看看油气行业。前几年全球油气产业经历了一段黄金发展期，2020年《财富》世界500强企业数据显示，“三桶油”中石化、中石油、中海油排名分别为第2位、第4位、第64位。但随着全球油价下跌，成本过高、创新不足、决策缓慢等运营缺陷逐渐凸显，油气产业开始陷入窘境，这就要求各大油气公司必须重塑新的经营模式，追求下一个利益增长点。在各项革新性技术中，数字化是当前最热门的话题之一，依托互联网和数字化技术的各种新模式不断刷新着油气行业的认知。作为国家战略性资源和工业基础，在数字化浪潮冲击下，油气行业数字化转型发展已是大势所趋。

作为典型的传统行业，油气行业拥有庞大的资源数量、数以千亿计的资产规模、数以百万计的员工；同时，也有专业度高、工艺流程复杂、产业链长、设备资产总量巨大、应用场景复杂等特点。前者为行业的数字化转型提出需求，后者则给数字化转型增加了难度。实际上油气行业对于数字技术的需要紧迫而持久：一方面，油气开发难度日益增加，持续稳产形势严峻，新老油田都面临着生产成本升高与效益降低的巨大压力；另一方面，各层级对企业的安全生产、环境保护责任要求越来越严格。这些压力和要求背后，本质上是技术危机，技术创新是驱动油气行业可持续健康发展的核心，而数字化技术是当前最重要的技术发展领域。作为支持驱动油气行业数字化技术创新的数据中心，它的建设要求也将更为严格。如何确保数据中心的安全正常运行、确保业务流程的有效运转、保护关键信息资产安全，成为了企业管理人员要面对的巨大挑战。

其次是电力行业。电力，以其在国民经济及社会生活方面所具有的关键战略安全地位，最近一二十年，信息系统在电力行业已得到全面地、深入地应用。从发电、输电到变电、电网监控等领域，已全面实现了信息化、自动化，信息系统在电力行业的普及应用极大促进了电力行业的发展。电力信息系统的正常运行为保障我国的电力安全生产起到了关键性的作用。考虑到信息系统的关键地位，一旦出现问题，将会给电力生产带来严重后果，甚至会影响到国家经济的安全运行及人民的正常生活。比如2008年中国南方雪灾造成的电力系统的瘫痪，给人民的生产生活乃至生命安全都带来了不可忽视的影响。为此，国家安监总局和国家

总局和国家电网专门出台《电网调度系统安全性评价》、【2006】34 号《电力二次系统安全防护总体方案》、《电网调度安全分析制度（试行）》、《电网调度二次设备分析制度（试行）》等文件，从制度上保障电网安全生产。电力生产由发电厂发电，经过升压送入智能电网进行统一调配，输送到各地，再降压送到终端用户使用。这一系列过程中，电网的监控与调配起着核心关键作用，它保障了整个电网的协调运行。我国电网调度采取了分层设计，分为县级、地区级、省级、大区级和国家层级。其中最重要的是大区级调度中心，如华北、华中、华东、西北、西南电网等等，这些大区调度中心承担着具体的电力监控调度职能。因此，如何保障电力信息系统的安全正常运行，从信息系统建成的那天开始，就注定成为管理人员所要面临的重大挑战。除了加强信息系统建设过程中的质量管理及运行安全管理外，采取容灾措施防范系统风险，成为了保障信息系统安全运行的重要举措。

作为能源行业的代表，油气和电力行业的业务发展需求主要体现在以下几个方面。

1.1核心业务系统数据零丢失

需要保证核心业务数据在出现自然灾害、设备故障、人为操作失误、病毒等灾难或情况时，数据零丢失，并确保已有数据的安全可靠。

1.2数据中心故障条件下，业务零中断

现代生活的80%都和石油有关，人一生要“吃”掉551千克石油，“穿”掉290千克石油，“住”掉3780千克石油，油气相关业务系统的中断对人们生产生活会有巨大的影响。另外，全社会对电力的依赖程度越来越高，对电力供应的质量也提出了更高的要求，电力已经是社会生活中必不可少的一个元素。为这些行业建设的数据中心及其对应的业务系统是企业数字化进程中的重要组成部分，因此在不增加人力投入的前提下，实现业务的故障自动检测以及在故障发生时能自动切换，确保业务系统持续健康运行，对于人民的生产生活甚至生命安全都是极其重要的。

1.3快速部署，科学管理，减少整体TCO

数据中心和业务系统的建设需要花费大量的人力财力物力，如何做到数据中心业务系统的快速部署，满足业务快速扩张需求，成为影响行业生产效率的关键；同时，如何做到对数据中心、核心业务系统、关键信息资产的科学有效管理，也是提高生产效率、实现降本增效的有力途径。

D. 能源行业信息技术应用创新产业

信创技术是一项国家战略，是当今形势下国家经济发展的新动能，信创的发展可以提升关键产业链的发展，促进社会经济发展和数字化转型，保障国家战略安全。灾备技术是确保关键信息系统和数据安全的关键技术，以核心的数据复制技术为基础，广泛应用与灾备、数据保护、云数据管理等领域，帮助能源行业打通数据孤岛、实现数据互通、助力能源行业数字经济的发展。

2.需求分析

2.需求分析

随着油气和电力行业数字化转型、数据中心建设的稳步推进，各关键核心业务系统的建设和投入使用，人们越来越享受数字化智能化带来的便捷和舒适。同时，数字化转型也让这些行业内的企业在市场竞争中保有生产效率提升、管理高效、成本缩减等优势，是企业可持续健康发展的重要基石。基于上述业务需求，行业数据中心及关键核心业务系统的灾备系统建设对于其业务系统安全可持续运行有着重要的意义。油气和电力行业的灾备需求主要体现在如下几个方面。

A.能源核心业务系统，关系着油气生产加工、油气输送、电力生产、电力调度控制、销售等环节的生产力，任何业务的中断，都会造成企业生产效率的下降、客户满意度降低、营收损失以及品牌影响力的下降，所以对这些业务系统需要有容灾建设以确保业务连续性；

B.这些行业的生产经营数据技术集中在大数据、高性能计算、自动化、物联网、实时分析、用户交互等领域，数据来源多样且大容量、更新速度快，如何有效地做好数据的处理、存储和备份是灾备系统建设中的重点；

C.这类行业的业务面非常广，通常是跨区域经营，如国家电网调度采取了分层设计，分为县级、地区级、省级、大区级和国家层级。其中最重要的是大区级调度中心，如华北、华中、华东、西北、西南电网等等，这些调度中心承担着具体的电力监控调度职能。通常这些区域性的调度/生产中心都会建设本地数据中心，以实现业务系统的合理有效使用、数据访问效率提升等需求。这样一来，多数据中心之间如何协同、数据如何管理就成为了管理人员要面临的难题。D.电力油气行业业务系统向信息业务系统业务创新产业转型

电力电网是关系国计民生、千家万户的关键基础设施基础产业，是经济社会运行的神经中枢。随着关键信息基础设施的互联互通，电力行业成为网络安全保障的重点，建设自主信息化平台成为大势所趋。信创系统的灾备也作为企业关注的关键因素之一。

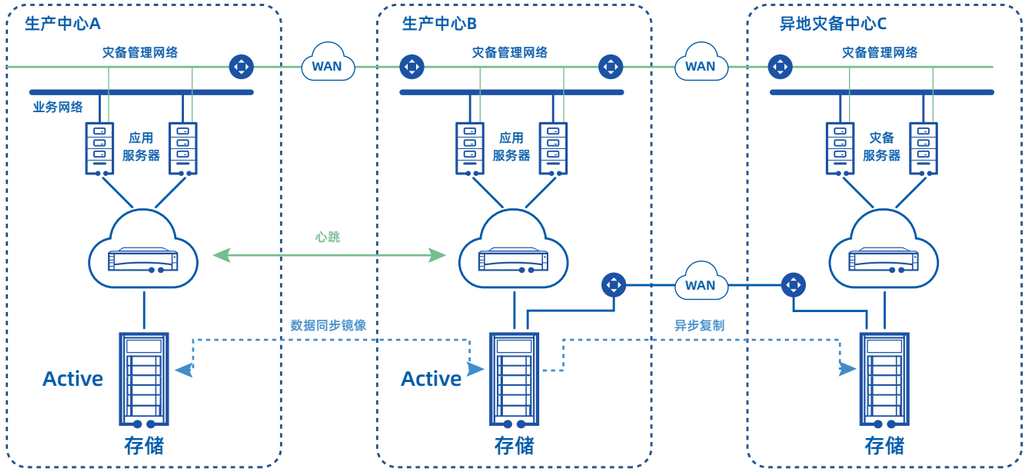
3.建设方案

根据国家标准GB/T 20988-2007《信息系统灾难恢复规范》中的灾备能力等级划分，不同的业务连续性要求需要不同等级的灾备方案来实现，这也就有不同的RTO/RPO目标时间。能源行业企业通常有不同的生产阶段，每个阶段对于业务系统和数据的可靠性要求不尽相同。通过对业务系统的场景划分，就可以归纳出行业灾备建设中各业务的灾备等级，以实现灾备效果和成本的平衡。

A.能源行业核心业务系统的灾备建设

对于油气行业中油气经营管理系统、油气生产管理系统，电力行业中的电力调度控制系统、电力配电系统等对行业生产经营活动有着重大贡献、重要影响的业务，应做到RPO尽可能接近0且RTO为秒级，以实现业务连续性和数据无丢失。对这类业务系统，通常采用双活（Active-Active）架构，架构中两套系统同时在线为用户提供服务，系统之间采用心跳及数据同步链路实现状态监测、数据实时同步等功能。当其中一套系统出现故障时，另一套系统也能正常工作，用户访问业务系统无任何感观上的差异，且故障时目标系统访问路径的切换对用户是透明的。同时，为了确保两套系统间数据同步的时延，这两套系统

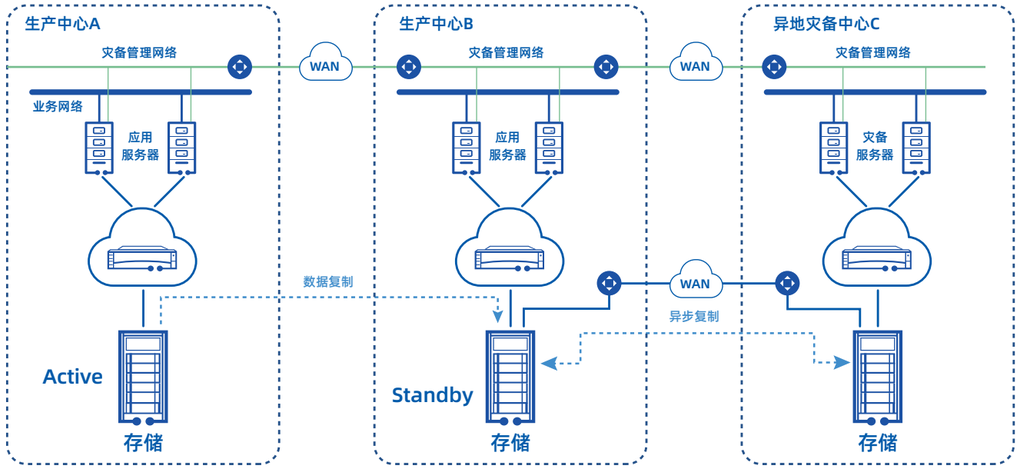
通常建设在同城或相近的区域中。为了确保数据的有效备份，通常还会在较远的第三地建立第三个数据中心，以异步复制的方式实现对前两个数据中心的数据备份。对于像国家电网这样规模、有多个区域中心且各中心间相距较远的情况，各区域中心的数据中心还可以建设为其他数据中心的数据备份中心，以实现数据的多副本备份。这类灾备系统的简易架构如下图所示：



图表 24同城双活、两地三中心架构示意图

B.能源行业次核心业务系统的灾备建设

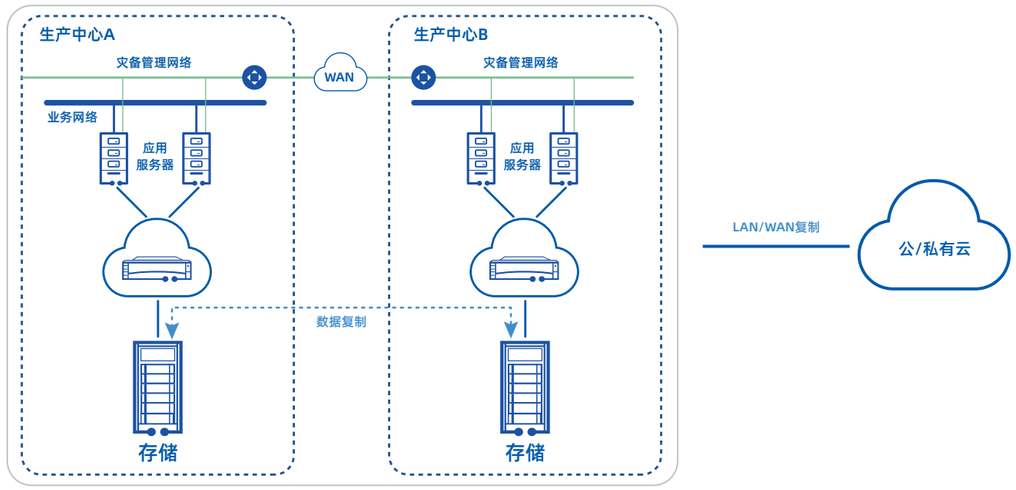
对于诸如油气过程控制系统、电力经营管理系统、电力生产管理系统等对企业经营活动有重大影响但暂无业务中断风险的次重要业务，应做到数据恢复时间在2小时内、业务恢复时间在15分钟以内，容忍部分数据的丢失。对这类业务，通常采用主备（Active-Passive）的方式进行业务容灾和数据备份：本地数据中心的两套系统中静态优先级高的系统对用户提供服务，次优先级的系统处于Standby模式，且通过系统间的心跳和数据同步链路监测对端心跳、同步数据等。当高优先级的系统出现故障时，低优先级的系统即对外提供服务，或者在某些场景中需要人员手动启动低优先级的系统以对外服务。同时，还可以将本地数据中心的数据异步远程复制到第三地数据中心，以实现数据的备份。该类灾备系统的架构简易图如下图所示。



图表 25 同城主备、两地三中心示意图

C.能源行业非核心业务系统的灾备建设

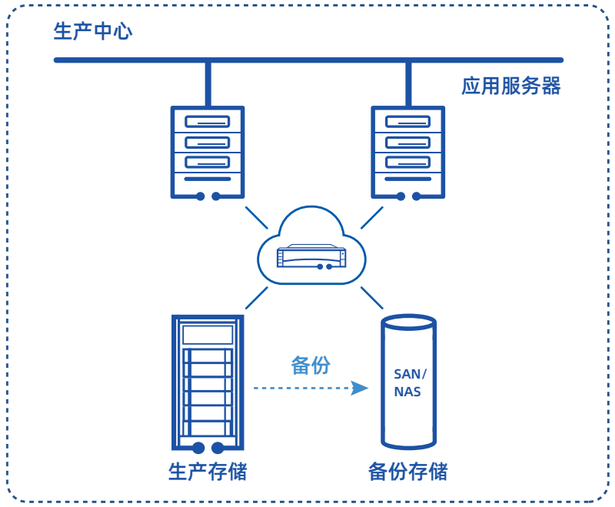
对于像电力营销系统、油气数据采集与监事控制系统等低重要性的业务系统，应做到数据恢复时间在4小时内、业务恢复时间在1小时内。对这类系统的灾备建设，通常采用与B相同的灾备体系，在本地数据中心实现对业务的容灾。对于业务数据的备份，可以使用本地SAN/NAS存储等资源实现，数据也可以上云实现备份。此类业务系统的灾备建设简易架构图如下所示。



图表 26 备份上云示意图

D.能源行业BackOffice类业务系统的灾备建设

对于像电网巡检系统、办公OA支撑系统等优先级更低的业务，做到数据恢复时间在4-12小时内，业务恢复时间在12小时内即可。此类系统的灾备建设通常在本地数据中心进行，单业务系统+数据定期备份实现。其灾备系统建设的简易架构图如下所示。



图表 27 单业务系统+数据定期备份示意图

（九）中国交通领域灾备建设现状与发展策略

按照《交通强国建设纲要》要求，交通行业应由依靠传统要素驱动向更加注重创新驱动转变，构建安全、便捷、高效、绿色、经济的现代化综合交通体系，大力发展智慧交通。推动大数据、互联网、人工智能、区块链、超级计算等新技术与交通行业业深度融合。推进数据资源赋能交通发展，交通运输行业业务系统稳定运行成为交通行业智能化、数字化转型的必要条件，任何人为或自然因素所导致的应用或系统中断，都会对航空、轨道交通、道路运输等造成巨大的经济损失和生命财产损失。

因此，为了保证交通行业信息系统的安全稳定运行，需要在交通行业制定专有的数据保护建设标准，加强交通行业信息安全保障体系建设，规范交通运输领域信息系统灾难恢复工作。

1.建设需求

目前交通行业灾备体系相对薄弱，亟待改善。交通行业需7*24小时不间断向公众提供服务，一旦业务数据发生错误或丢失时需快速准确恢复数据。然而，交通行业没有专有的数据容灾保护标准，多以《信息系统灾备恢复规范》（GB/T20988-2007）规范建设数据容灾系统，缺少行业专有信息系统灾备恢复规范及建设方案，业务系统以本地双活建设为主，缺少同城和异地灾备，当灾难发生时难以保障系统业务连续性和数据安全。因此，搭建一套专业可靠的灾备系统是交通行业信息化建设的重要内容之一。

建议重点关注同城和异地灾备建设，将数据安全、数据灾备的规范纳入到业务系统建设标准中。

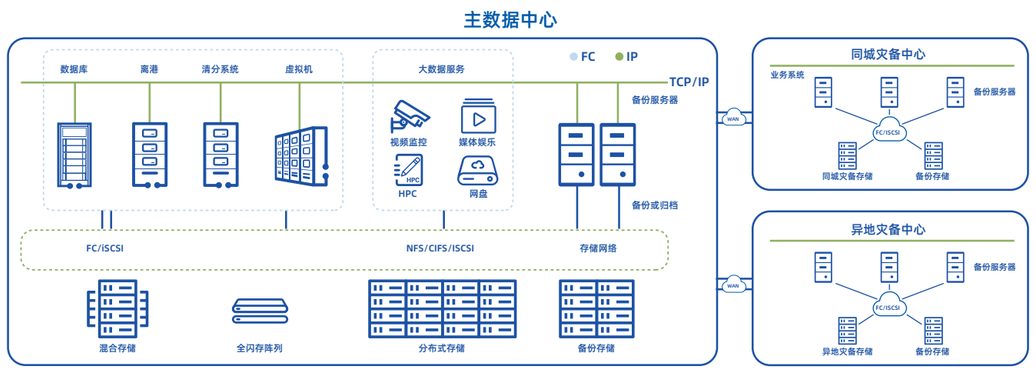
2.建设方案

交通行业在数字化、智能化转型的过程中，数据安全无疑是转型的核心之一，充分挖掘业务数据的价值，已经成为交通行业的广泛共识。数据的安全保护需要专有的灾备规范以及解决方案，需要覆盖整个数据中心内数据的全生命周期，在灾难发生时，需要保障业务系统的连续性及关键数据的可靠性。

根据业务重要程度，建议分层分级建设灾备系统。对于核心业务系统建议采用两地三中心灾备架构，在同城建设双活数据中心+数据备份，在异地建设灾备数据中心，实现存储级、数据库级、应用级、数据中心级灾难保护，保障核心业务系统跨地域连续性。

对于其余业务系统建议先在同城建设双活数据中心+数据备份，保障同城业务连续性，再逐步演进至两地三中心灾备架构，最终实现跨地域存储级、数据库级、应用级、数据中心级灾难保护。

通过建设统一灾备管理体系，保障业务系统7*24小时连续运行，数据不丢失。



图表 28 交通行业两地三种容灾规划

（十）中国医疗领域灾备建设现状与发展策略

1.现状与发展策略

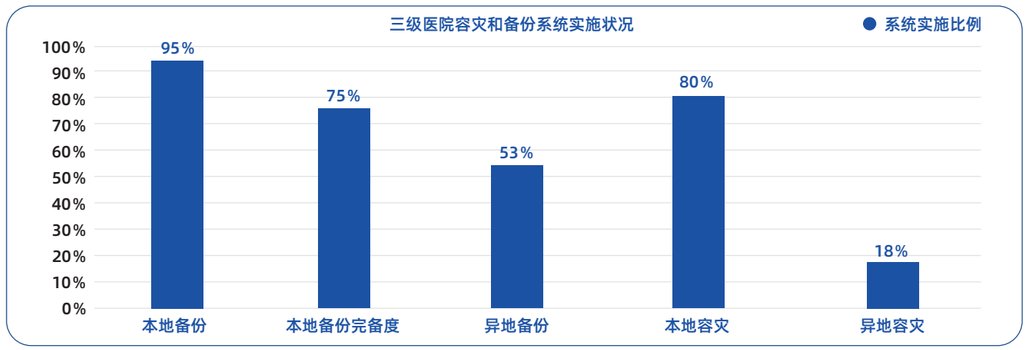
伴随我国老龄化、城镇化等社会经济转型过程，居民基本健康需求增长迅速。为解决快速增长的医疗需求，国家实施“健康中国2030战略”，加速推动医院信息化转型升级，提升医疗服务的质量和效率。稳定可靠的数据基础设施成为了医院信息化建设的重要诉求，任何人为或自然因素所导致的应用或系统中断，都会造成巨大的经济和名誉损失，和对病患的诊疗造成影响。因此，为了保证医疗行业信息系统的安全稳定运行，相关部门在数据保护方面制订了多个管理规范和指引，以加强医疗行业信息系统保障体系建设，规范医疗领域信息系统灾备工作标准。因此，为了保证交通行业信息系统的安全稳定运行，需要在交通行业制定专有的数据保护建设标准，加强交通行业信息安全保障体系建设，规范交通运输领域信息系统灾难恢复工作。

2.建设需求

随着各级医院加速推动信息化建设，提升医院智慧医疗水平，医院运营对信息化系统日益增长的依赖，对业务连续性和数据安全提出了更高的要求。另一方面，卫健委出台多项指导文件，规定医院容灾和备份系统成为建设刚需。以进入全国三级公立医院绩效考评的电子病历等级评定为例，3级电子病历要求医院对全部系统有软件和数据的备份，4级电子病历要求医院具备异地灾备机房和异地数据备份能力。

通过调查和对各项灾备相关政策（例如：信息系统安全等级保护）实施情况的分析，可以看出医院的数据容灾和备份系统的实施情况呈现出水平参差不齐的特点（详见图1）。

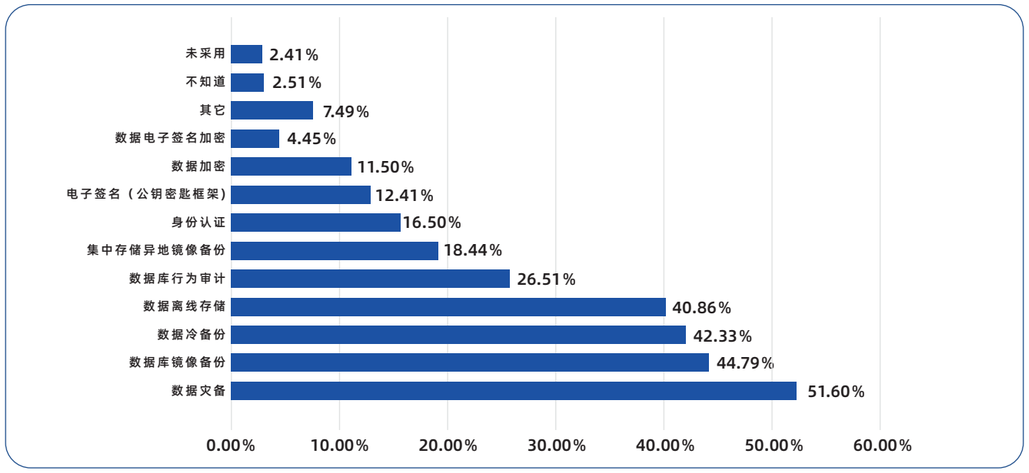
以三级医院为例，受《全国医院信息化建设标准与规范》的强制要求，本地数据备份的实施普及率应达到95%以上，且使用独立的备份软件进行备份；三甲医院由于需要通过国家信息安全三级等级保护，需要具有异地备份能力，而普通三级医院（非三甲）因没有政策强制要求，实施异地备份的比例较低，整体来说三级医院异地数据备份比例预估应超过53%，也就是三级医院通过三级等级保护的比例。容灾系统方面，三级医院同样受到《全国医院信息化建设标准与规范》的强制要求，应90%以上都具有对关键业务系统的本地容灾能力；异地容灾，目前主要是是建设多院区（<20%）的医院考虑，这种现象并不是由于技术和投入的不足，而是意识的局限。



图表 29 三级公立医院灾备系统建设现状分析

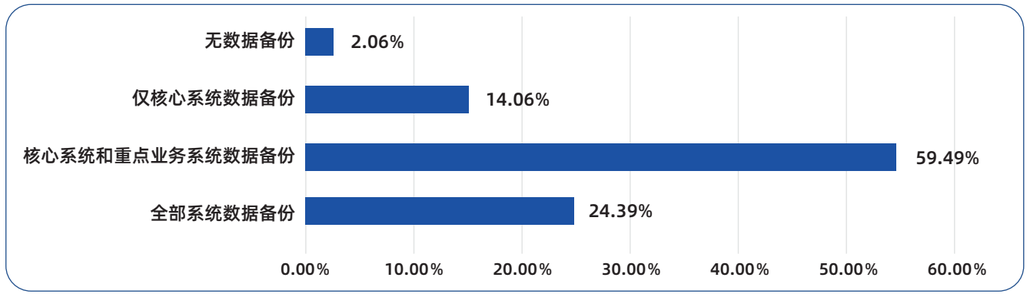
除了上文提到的容灾和备份系统实施状况参差不齐的特点，通过中国医院协会信息专业委员会（CHIMA）的报告[参见：《中国医院信息化状况调查2019-2020年度》]，可以看到医院灾备系统建设总体仍相对薄弱。

从CHIMA 2019年医院数据保护措施统计分析来看（详见下图），拥有异地灾备能力的只有18.44%。

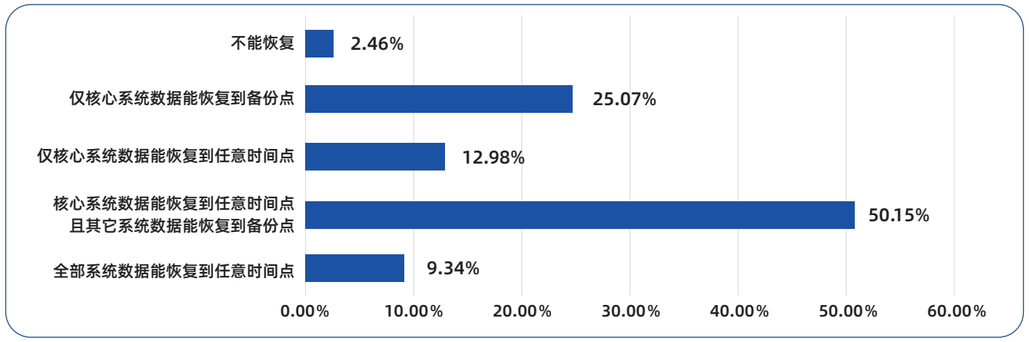


图表 30 2018-2019医院数据安全措施实施情况

CHIMA在2020年公布的调查报告对医院的灾备措施进行了细化分析（详见下图），分别对数据备份和数据恢复能力进行了分析。备份方面，报告发现24.39%的医院有对全部系统数据进行备份；数据恢复方面，38.05%的医院仅核心系统具备数据恢复能力，50.15%能将非核心数据恢复到备份时间点，距离业务数据0丢失还有不小的差距。



图表 31 2019-2020医院数据备份措施实施情况

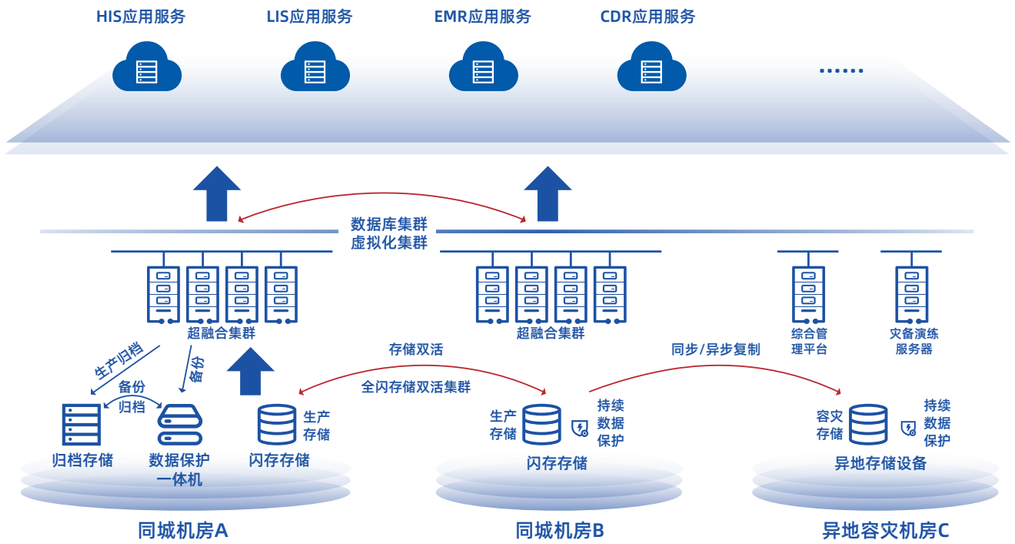


图表 32 2019-2020医院数据容灾措施实施情况

总结CHIMA的统计数据可以发现，医院数据中心当前主要是对本地核心和重点业务系统进行数据定时备份，缺乏全业务数据0丢失，异地数据备份容灾能力，难以满足更高业务系统连续性的要求。

3.建设方案

在医疗向数字化、智慧化转型的过程中，医疗数据无疑是转型的核心承载，永续保护医疗数据的原生状态、发挥和运用数据的核心价值，已经成为医疗行业的广泛共识。其中数据的永续保护需要能覆盖数据的全生命周期的灾备解决方案，也就是需要包含容灾、备份、归档三部分。“容灾”，即保障业务系统在灾难条件下的连续性；“备份”，即保障关键数据在灾难条件下的完整性；“归档”，即保障数据的长期合规留存，实现“热数据全容灾，温数据热备份，冷数据温归档”数据全生命周期保护，形成两地三中心架构。建议医院本地同步复制模式提升为双活模式，保障重要数据0丢失；异地灾备中心实现同/异步复制，形成异地数据保护能力；使用独立备份系统和归档设备对医院全部系统进行定期数据备份和重点数据归档，实现全生命周期数据保护。同时定时开展灾备演练、恢复验证测试、灾备数据应用等工作，做到灾备系统“战时能战、平时有用”。



图表 33 医疗行业两地三中心示意图

（十一）国内灾备建设成功案例参考

国内企业为某银行建设了全闪存两地三中心解决方案，通过AA双活和远程复制提供存储侧数据保护方案，同时实现了基于应用层可靠性的双保险，保证了7*24小时业务永不中断，为信用卡业务提供99.99999%的可靠性保障。在数据保护的供应体系中，存储介质是最重要的器件。闪存颗粒相比机械硬盘具备性能、能效、安全性等多项优势。中国不具备自主供应机械硬盘的能力，而闪存供应链相对完整。该银行通过建设全闪存数据保护，不仅提升了数据安全性，同时实现了节能降耗，整体实现了50%机柜空间缩减，72%电费缩减，节省66%OPEX（运行费用），帮助客户构建了绿色智能基础设施。该银行的数据安全性、业务效率、能源效率均达到世界先进水平。

电信运营商由于数据量的激增，导致备份系统投资高，同时备份系统性能无法满足数据备份时间窗口。需要在高效保护的同时，通过融合部署实现对投资的控制。国内企业通过数据保护一体机为此运营商建立了统一备份资源池，统一各省备份标准，支持各种业务备份。同时将备份数据副本复用于多业务开发测试等，无需复制数据。相对传统方案，空间节省65%，能耗下降60%。数据保护一体机配置简单，开箱即用，且支持多节点统一管理，简化了备份管理和运维。同时该电信运营商借此机会对关键业务的备份系统实现国产化替代，规避了业务连续性风险。

国内外灾备人才队伍建设比较

06

六、国内外灾备人才队伍建设比较

（一）国内灾备人才队伍建设概况

灾备行业的技术创新和发展，必须依靠灾备专业人才队伍的不断壮大，知识储备不断完善，才能确保国内各行业灾备的质量和发展需求。随着灾备领域行业及国家标准的不断完善和发布，灾备专业的培训、认证工作不断加强，目前，我国金融等国家重要基础设施行业等有明确监管需求和严格的灾备中心管理、运维需求的行业，设有专门的部门负责灾备的规划和建设工作，灾备人才相对充足。而其他行业的IT部门虽然没有专门负责灾备的组织，但也会有运维技术人员兼职负责灾备建设工作，随着灾备的重要性越来越突显，各行业开始重视灾备人才的培养和应用。国内对灾备人员的资格认证也逐渐增多，除了DRI每年都在中国举行CBCP认证工作外，灾备技术国家工程实验室，也开始组织灾备专业人才的培训，组织建设灾备培训体系，实训平台，灾备专业教材，发放CISDR培训证书，为培养灾备领域的专业人才提供了良好的平台。

“北京信息灾备技术产业联盟”由灾备技术国家工程实验室组织，汇聚产、学、研、用、监等灾备领域相关专家和机构，将高校资源和企业资源充分整合利用，为我国在灾备领域开始寻求技术、产品以及服务体系的标准化，国内灾备人才培养，推动我国灾备水平走向完善，起到了积极的推动作用。

总体来看，我国的灾备技术后备人才储备相对比较薄弱，人才培养尚没有形成体系，目前只有包括北京邮电大学、清华大学、哈尔滨工业大学、四川大学等极少数高校开设了灾备相关课程，还缺乏有一定的系统性和有效性。同时，相关的专业灾备人才培训机构也不完善。除高校外现有人才储备基本都集中于通过购买国外灾备产品所附带的技术培训成长起来的，虽然可以熟练掌握国外产品的使用和基本维护，但在进行核心技术开发和研制等方面，灾备领域还需要储备大量的人才。

（二）国外灾备人才建设概况

国外的灾备人才和组织体系主要以具有权威性的国际组织为主，各个自主创新的灾备相关企业为市场主导，同时在高校设立一定的课程和培养体系，整体较为系统化。以下为部分较为著名的国际灾备组织：

国际灾难恢复协会（DRI International）成立于1988年。其使命是通过提供教育和帮助，以及发布标准的基础资源来推广业务连续性规划和灾难恢复行业的通用知识体系；协助建立公共和私营机构之间的合作来推广相关行业标准；通过对业务持续领域的专业人员进行认证，来提高获认证人员的可信度和专业技能。

《灾难恢复期刊》（DRJ）主要提供业务连续性规划相关知识和信息，是业界关于业务连续性的首要出版物的出版商，DRJ资源和材料都相当丰富，同时赞助了最大的两个行业会议和展览，总出席人数超过3000人。

国际业务连续性协会（Business Continuity Institute，BCI）是制定及确立业务连续性管理职业技能和道德标准的领先机构，该机构与世界领先的测试服务机构 Professional Examination Service（PES）及其测试实施伙伴主要负责组织在全球范围内的BCI职业认证考试。

（三）人才队伍建设总结建议

随着我国将网络安全提升到国家战略，灾备作为其中的一部分，也是必不可少的。灾备人才的培养，也需要国家战略的支撑和扶持。灾备技术国家工程实验室，灾备联盟拟开展对各行业灾备现状的调研，同时对国内各行业灾备人才的现状摸清底细，建立人才培养计划，向国家层面提出切实可行的意见和建议。逐步推行高校、职业院校专业培养，专业认证相结合的方式，大力发展和储备灾备专业人才，面向市场需求开设灾备应用综合培训示范基地或科研机构，促进产学研结合，积极研发具有自主知识产权的灾备相关技术、管理方法和应用设备，以适应新模式系统应用环境下的灾备技术和人才需求，真正做到各行业的安全、有效的容灾备份，确保数据和应用的安全。

总结和展望

07

七、总结和展望

建设大数据灾备体系不只是买“保险”，灾备体系不是极端情况下才使用的“核按钮”，而是日常生产生活的“保险箱”和“运钞车”，要把数据安全、数据灾备的理念渗透到日常生产中。建立数据灾备认知，彻底改变“本地备份完备度低”、“缺乏容灾”、“严重缺乏异地灾备”的现象，整体灾备渗透率提升到欧美同等水平。针对业务系统连续性、“韧性”，出台灾备建设实践指南与行业演练规范。扶持国产领军品牌，带动一批灾备技术企业，一手抓保障灾备技术全球领先水平，一手抓保障灾备体系供应连续性。

（一）完善数据灾备审查演练制度

建议持续完善灾备领域的国家标准，尤其应该补齐行业信息系统数据安全保护与灾难恢复建设指引，并推出相应指导政策。在重点行业出台行业标准与团体标准，保障行业业务系统与数据得到完备的分类分级，同时保障等保2.0等相关国家标准与行业分类分级制度紧密结合。建立健全国家和行业检测与验收机构，发布技术实践指南、参考架构，制订完善的灾备演练规范，规定演练场景、频度，并严格执行。

（二）“东数西备”建设数字中国“大后方”

针对国内数据中心发展不均衡、业务诉求差异大的现状，建议国家从全国范围进行数据中心灾备站点统一规划布局，结合国家一体化大数据中心建设，加强统一全国异地灾备建设。中西部部分省份具有气温低、板块活动少、深处内陆等自然环境的优势、也具备能源环境的优势，结合中西部省份发展数据中心的成熟经验，建议在“东数西算”的基础上，增加 “东数西备”的政策，发布《全国一体化大数据中心协同创新体系算力枢纽实施方案》关于灾备的进一步指引，要求将全国范围内对网络时延要求不高的数据灾备中心优先向贵州、内蒙古、甘肃、宁夏节点转移，打造面向全国的异地灾备中心。利用地理位置优势，利用网络、能源、算力、数据和应用一体化的优势，迅速提升我国战略灾备覆盖水平。

（三）设置国家科研专项，扶持国产领军品牌、加大政府采购规模

数据灾备关乎国家安全，技术的先进性与供应的可持续性同等重要，一手抓保障灾备技术全球领先水平，一手抓保障灾备体系供应连续性。

建议研究出台加强数据灾备高质量发展的产业专项规划，或国务院、主管部委牵头的指导意见，研发和应用关键技术产品，提升灾备产业链自主创新能力。提高数字政府领域灾备建设完善程度，实现关键信息系统的全容灾、热备份。

提前做好基础储备，面向一纵一横两个方向设置国家科研项目：纵向，面向新型生态场景，强化云、大数据、分布式数据库、虚拟化、HPC、AI、视频等场景的垂直保护能力；横向，引导数据保护与数据分析融合技术，让备份、归档数据产生价值。

大力扶持半导体存储介质的使用，避免最关键器件的“卡脖子”，同时支持新介质的技术规划，包括闪存、蓝光、磁带、硬盘、玻璃、全息等，从根本上完善软硬件产业链。

提升对国产领军品牌的扶持力度，带动一批技术领先的灾备技术企业。警惕落后技术的国产化“马甲”，避免落后技术以“合资”的形式贴牌进入中国市场。

加大政府采购规模，为各行各业树立标杆。以技术为根本，以市场为导向，从根本上解决我国数据灾备的“技术领先性”和“供应连续性”的难题。

（四）依托一带一路战略，加强数据灾备国际合作

数据灾备领域的企业主要集中在中美两国，建议参考一带一路高峰论坛等形式，组织网络安全与数据安全相关国际会议，组织国际灾备技术、标准与建设标杆的国际交流。不仅有利于维护中国企业的商业利益，更有利于提升中国倡导的灾备标准和技术体系被国际市场所接纳，建立数据安全软实力。建议通过政策性银行支持，向一带一路相关欠发达国家提供数据灾备技术、设备、项目援助建设，为提升区域的稳定提供帮助，让一带一路区域的数字经济坐上又快又稳的中国快车。

（五）向优秀企业、先进行业看齐，补齐灾备能力

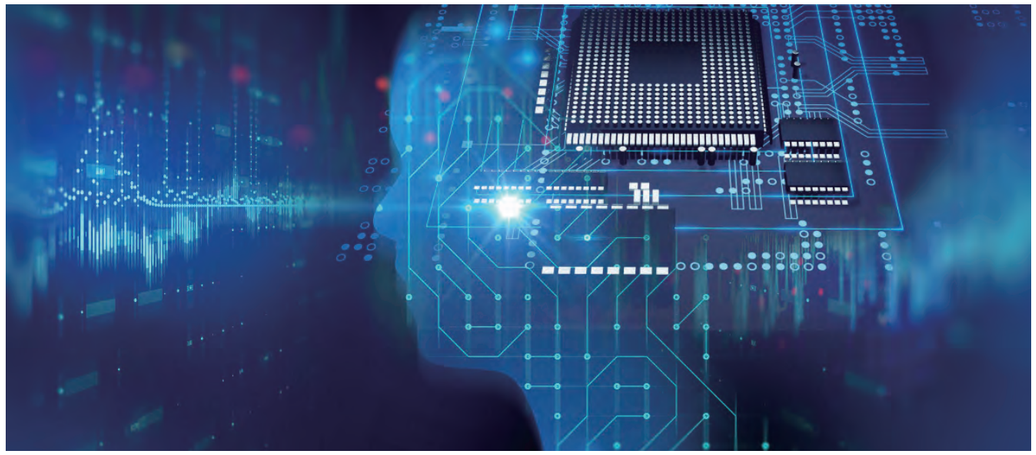
建议政府示范先行，推动政务云、国家一体化大数据中心、行业大数据中心、智慧城市等场景的灾备体系建设，全国范围重点打造一批数据灾备的示范基地、示范项目，实现标准和政策落地，引领千行百业，迅速化解数据安全风险。

以教育、医疗、制造业为例：

（一） 教育信息化2.0以智能化、集中化为特征，教学、科研的获取方式逐步走向线下和线上相融合；由可靠、安全的IT系统支撑的泛在教育和科研成为现代化教育的选择。建议推动建立适合教育行业的等保标准，以实现不间断教育、随时随地教育，如大于300公里的校区之间建立容灾，小于300KM的多校区之间实现自动化数据备份，根据数据访问频繁程度实现分级存储。

（二） 在医疗向数字化、智慧化转型的过程中，医疗数据无疑是转型的核心承载，永续保护医疗数据的原生状态、发挥和运用数据的核心价值，已经成为医疗行业的广泛共识。进一步把握医疗数据形态的多样性和复杂性，全面响应医疗应用的实时性和可靠性诉求，建立起更高标准的容灾备份标准和技术规范，是医疗行业数据保护健康发展的必由之路。建议医院本地同步复制模式提升为双活模式，从而保障7*24小时业务连续性；建议医院采用独立备份系统进行专业备份；建议多个院区同步承载业务，互为灾备中心，实现数据中心级灾备。

（三） 制造企业在数字化浪潮的推动下逐渐具备整合来自研发、生产、管理、营销等多方面数据的能力；企业“数据资产”正在逐渐取代“固定资产”的地位，成为企业数字化转型和持续经营的关键。但随着数字化的持续推进，企业网络与外界的边界正在慢慢消失，传统的数据安全保障手段逐渐失效，制造企业正在面临更多的攻击和风险，尤其商业秘密和技术专利等与企业生死存亡密切相关的敏感数据保护，正变得日益迫切。制造行业数字化转型的深入，也给数据保护提出了更高要求。这些要求具体体现在以下三个层面：首先，移动应用普及要求数据实时在线处理，容灾要求越来越高；其次，新业务快速上线，要求备份数据必须能够快速准备，供开发测试使用；第三，业务多样化带来的数据保护需求不同，企业必须在在有限预算下，既满足业务数据保护要求，又能控制数据保护支出。



附录A实验室与灾备联盟及工作机制简介

北京信息灾备技术产业联盟是由灾备技术国家工程实验室依托国家政策和行业技术、市场资源，联合产、学、研、用、监等相关专家和机构共同构建的合作创新平台，于2015年1月10日在北京成立，是按照民政部系统登记管理的全国性非营利性社会组织，登记注册成员包括大型国企、民营企业、上市公司、大学及研究机构共百余家，包括中国邮政集团有限公司，华为技术有限公司、阿里巴巴集团、新华三集团、上海爱数信息技术股份有限公司、北京易华录信息技术股份有限公司、广东紫晶信息存储技术股份有限公司，北京中软国际信息技术有限公司、中国大唐集团科学技术研究院有限公司，南京壹进制信息科技有限公司，上海天玑科技股份有限公司，格尔软件股份有限公司，深圳大普微电子科技有限公司等企业、以及东南大学，北方工业大学重庆邮电大学，山东大学，重庆科技学院等大学院校。

灾备联盟主要工作包括开展灾备技术和业务的研究，灾备软硬件产品的研发，灾备领域标准制定，测评标准制定和行业测评服务，开展信息灾备预案制定、演练策划、管理咨询等服务，加强灾备原创性技术成果转化、产品孵化，行业咨询培训与会展，承接各类国家委托的项目，开展国际交流与合作，掌握国内国际灾备技术行业发展动态，建设灾备技术信息服务平台，提供行业、市场等公共信息服务，促进国内外容灾备份行业健康发展。

灾备技术国家工程实验室是由国家发改委于 2008 年 8 月批准的全国唯一的一个灾备领域国家级工程实验室。实验室由北京邮电大学牵头，联合清华大学、中国科学院计算技术研究所和中国邮政集团公司共同建设。实验室现任主任杨义先教授是北京邮电大学博士生导师、首批长江学者特聘教授、首届国家杰出青年基金获得者。目前实验室有数据备份技术研发实验室（清华）、数据恢复技术研发实验室（计算所）、数据可靠性技术研发实验室（北邮）、灾备标准体系研发实验室（北邮）、测试验证实验室（邮政集团）。

附录B 图表目录