ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0264—2024

金融数据中心容灾建设指引

Guidelines for financial data center disaster tolerance building

2024－07－29 发布　　2024－07－29 实施

中国人民银行　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国人民银行科技司提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

金融数据中心容灾建设指引

1 范围

本文件提供了金融数据中心容灾建设中组织保障、需求分析、体系规划、建设要求、运维管理方面的指引。

本文件适用于金融数据中心容灾的建设和管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估方法

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 51314 数据中心基础设施运行维护标准

JR/T 0071.2 金融行业网络安全等级保护实施指引 第2部分：基本要求

JR/T 0265 金融数据中心能力建设指引

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据中心 data center

由计算机场地（机房）、机房基础设施、信息系统硬件（物理和虚拟资源）、信息系统软件、信息资源（数据）和人员以及相应的规章制度组成的组织。

[来源：GB/T 33136，3.1.1，有修改]

3.2

金融数据中心 financial data center

支持金融服务的数据中心。

3.3

灾难 disaster

导致功能停顿或服务水平达到不可接受的程度，并持续特定时间的突发性事件。

[来源：GB/T 20988，3.8，有修改]

3.4

容灾 disaster tolerance

灾难发生时，保证数据尽可能少丢失，系统不间断运行或尽快恢复正常运行的能力。

3.5

灾难恢复 disaster recovery

为将数据中心从灾难造成的故障状态或瘫痪状态恢复到可正常运行状态，并将业务功能从灾难造成的非正常状态恢复到可接受状态而设计的活动或流程。

3.6

灾难备份 backup for disaster recovery

为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份的过程。

3.7

应急响应 emergency response

为应对突发事件，最大化减少突发事件对业务运行的影响而采取的紧急行动。

3.8

生产中心 production center

支撑生产系统运行，对系统信息进行集中管理和处理的数据中心。

3.9

容灾中心 disaster tolerance center

支撑灾难备份系统运行，抵御导致生产中心部分或全部不可用的灾难，用以接替生产中心部分或全部职能的数据中心。

3.10

威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

[来源：GB/T 20984，3.17]

3.11

脆弱性 vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节。

[来源：GB/T 20984，3.18]

4 概述

4.1 容灾建设工作内容

金融数据中心容灾建设主要包括以下内容。

a）组织保障。

b）容灾中心需求分析。

c）容灾体系规划。

d）容灾中心建设。

e）容灾中心运维管理。

4.2 容灾建设基本原则

4.2.1 安全性

应保证容灾中心安全、可靠，业务持续稳定运行。

4.2.2 协同性

应与生产中心整体规划、统一部署和管理。

4.2.3 经济性

应根据成本风险平衡原则，在满足容灾需求的基础上，降低容灾中心建设、运营成本，建设经济适用的容灾中心。

4.2.4 先进性

宜选用先进且成熟的产品和技术，保证容灾中心稳定高效运行，满足和适应信息系统快速变化和发展的要求。

4.2.5 扩展性

在规划与制定策略时应具备按需扩展的能力，方便进行技术升级和设备更新。

5 组织保障

5.1 组织机构

金融机构应根据自身的发展战略、业务特点及信息系统运行平台特点，明确金融数据中心容灾组织机构的职能定位。金融数据中心容灾组织机构可划分为决策层、管理层及执行层，各层级应明确职能、岗位、职责，确保层级清晰、权责统一，为生产系统稳定运行提供有力保障。

5.2 组织职责

5.2.1 决策层

决策层主要由金融机构高层管理者组成，决策金融数据中心容灾建设的重大事宜，主要职责应包括以下内容。

a）确定金融数据中心容灾战略。

b）审核批准金融数据中心容灾策略。

c）审核批准金融数据中心容灾经费预算。
d）审核批准金融数据中心容灾建设方案。
e）审核批准金融数据中心灾难恢复预案。
f）批准启动金融数据中心灾难恢复预案。
g）决策应急响应与灾难恢复重大事宜。
h）审核批准对外情况通报和信息发布。

5.2.2 管理层

管理层主要由金融机构的业务部门、技术部门、后勤部门等相关部门负责人组成，在决策层领导下开展工作，负责金融数据中心容灾建设前期规划、建设以及后期管理和协调，主要职责应包括以下内容。

a）组织制定金融数据中心容灾策略。
b）编制金融数据中心容灾经费预算。
c）负责金融数据中心容灾规划、设计、施工、测试、试运行、交付的管理工作。
d）负责金融数据中心容灾运维的管理工作。
e）组织制定金融数据中心灾难恢复预案。
f）组织实施金融数据中心灾难恢复预案的演练。
g）协调内外部容灾资源。
h）指挥和协调应急响应与灾难恢复工作。
i）负责内部信息通报和沟通。
j）组织和管理对外情况通报和信息发布工作。
k）监督、检查和总结金融数据中心容灾建设工作。

5.2.3 执行层

执行层主要由金融机构的技术部门工作人员牵头，业务部门、后勤部门等相关部门工作人员配合。执行层在管理层的领导下，负责金融数据中心容灾建设的具体实施工作，主要职责应包括以下内容。

a）提出金融数据中心容灾需求和策略建议。
b）实施金融数据中心容灾设计、施工、测试、试运行、交付等工作。
c）实施金融数据中心容灾运维工作。
d）提供金融数据中心容灾的专业技术支持。
e）负责灾难恢复预案的制定、测试、培训、演练和管理。
f）实施应急响应和灾难恢复工作。
g）负责灾难恢复过程的记录、报告和通讯联络。
h）承担灾难发生后的抢修、挽救和损害评估。
i）负责资源保障和供应。
j）负责灾难发生后的外部协作。
k）分析和总结金融数据中心容灾工作。

6 需求分析

6.1 目标

金融机构应根据长期可持续发展的战略目标，对金融数据中心的生产系统、基础设施、业务系统等方面进行综合分析，确定金融数据中心容灾建设需求。

6.2 内容

需求分析包括但不限于以下内容。

a）生产系统风险分析：依据 GB/T 20984 的要求，识别生产系统的资产价值、潜在的威胁和脆弱性并进行等级评估，确立生产系统风险级别。根据不同的风险级别制定可行的风险管控措施，并分析实施风险管控措施后的残余风险，提出灾难备份系统建设的必要性。

b）基础设施风险分析：识别生产中心基础设施资产的威胁和脆弱性，按照脆弱性被威胁利用时对生产中心所造成的影响范围和影响程度划分风险级别，并针对不同级别的风险制定相应的风险管控措施，以及分析实施风险管控措施后的残余风险。基础设施风险分析的范围应至少涵盖生产中心可能面临的供电中断、地质灾害、气象灾害、交通和通信中断以及生产中心基础设施本身的缺陷和弱点。

c）业务影响分析：依据 GB/T 20988 的要求，分析各业务系统中断后所造成的直接和间接影响，确立业务系统的灾难恢复指标。通过对各项业务功能之间的关联关系分析、业务系统和信息系统关联关系分析，确定支持各业务功能相应的信息系统资源及其他资源需求。

6.3 方法

6.3.1 资产识别

资产识别应对具有价值的信息或资源进行识别。资产是金融机构风险分析所要保护的对象，可分为有形资产和无形资产，主要包括基础设施、硬件、软件、数据、文档、服务、声誉等。

金融机构应根据资产的重要程度对资产进行分类，确定重要资产的范围，并且应根据资产对业务正常运行的影响程度对资产进行标识，确定资产的等级。

6.3.2 威胁识别

威胁识别应对资产构成潜在破坏的可能性因素进行识别。对威胁的分类主要包括以下方法。

a）环境因素和人为因素。

注：人为因素可分为恶意人员破坏和非恶意人员破坏，恶意人员破坏可分为内部人员、外部人员或内外部人员勾结的方式进行恶意破坏。

b）在控制能力之内和在控制能力之外。

c）可先期预警和不可先期预警。

6.3.3 脆弱性识别

脆弱性识别是对可能被威胁利用的资产的弱点进行识别，脆弱性识别可依据国际或国家的安全标准，或者行业规范、应用流程的安全要求。对应用在不同环境中的相同弱点，其脆弱性严重程度是不同的。脆弱性识别所采用的方法主要有问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。脆弱性识别主要从技术和管理2个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题；管理脆弱性可分为技术管理脆弱性和组织管理脆弱性，技术管理脆弱性与具体技术活动相关，组织管理脆弱性与管理环境相关。

6.3.4 风险计算

风险计算应采用适当的方法与工具，确定威胁利用脆弱性导致灾难发生的可能性，主要包括以下内容。

a）根据威胁出现的频率及脆弱性状况，计算威胁利用脆弱性导致灾难发生的可能性。

b）根据资产重要程度及脆弱性，计算灾难发生后的损失。

c）根据计算出的灾难发生的可能性以及灾难的损失，计算风险值，并进行风险等级划分。

7 体系规划

7.1 容灾体系

容灾体系分为同城容灾、异地容灾和极端容灾3个层次，主要包括以下内容。

a）同城容灾：将同一城市中的 2 个数据中心形成“生产中心＋容灾中心”格局，这 2 个数据中心处于同一城市不同风险区域内，主要用于防范同一城市内的小范围停电、建筑物火灾、基础设施设备故障、通信线路设备故障、软硬件故障以及其他突发事件可能造成的局部交通封锁或中断等小范围灾难的同类风险。

b）异地容灾：在生产中心所在城市以外的城市选择或建设数据中心作为生产中心失效后的异地容灾中心对外提供接续服务。异地容灾中心与生产中心处于不同城市，主要用于防范大范围停电、地震、洪水、海啸、滑坡、泥石流、较大范围的公共卫生事件等较大规模的区域性灾难。

c）极端容灾：在极端情况下，容灾中心提供最终数据保全和接续服务。极端容灾中心位置应深入内陆并具有隐蔽、安全、防核、防化、防磁暴、抵御自然灾害和突发事件的能力。

7.2 选择体系

金融机构可依据成本风险平衡原则选择建设满足业务需求的容灾体系，为不同业务连续性需求提供差异化容灾保障能力。容灾体系的选择策略主要包括以下内容。

a）满足以下条件宜选择同城容灾体系：

——在遭遇城市小规模灾难时具备对外提供接续服务、恢复时间较短、数据丢失量接近零的能力。

——业务开展范围主要集中在单个城市。

b）满足以下条件宜选择异地容灾体系：

——在遭遇大规模区域性灾难时具备对外提供接续服务的能力。

——业务开展范围覆盖全国或较大区域范围。

c）满足以下条件宜同时选择同城容灾体系和异地容灾体系：

——在遭遇城市小规模灾难时具备对外提供接续服务、恢复时间较短、数据丢失量接近零的能力。

——在遭遇大规模区域性灾难时具备对外提供接续服务的能力。

——业务开展范围覆盖全国或较大区域范围。

d）服务的中断或数据的丢失会对国家金融稳定、金融秩序产生严重影响，宜选择极端容灾体系。

e）同城容灾体系中，满足以下条件宜采用同城双活模式，通过数据复制、负载均衡等技术同时对外提供服务，保证更可靠的持续服务能力和更低的数据丢失率：

——分布式架构。

——业务恢复时间要求很高。

——有同时对外提供服务需求。

f）异地容灾体系或同时具有同城和异地的容灾体系中，满足以下条件宜采用异地多活模式，通过数据复制、负载均衡等技术同时对外提供服务，满足并发量高、业务逻辑简单、一致性要求不高的应用系统的高性能和高可靠性的服务需求：

——分布式架构。

——业务恢复时间要求较高。

——逻辑简单且一致性要求不高或可分模块独立处理业务。
——有同时对外提供服务需求。

8 建设要求

8.1 选址布局

容灾中心选址布局应符合JR/T 0265的要求，同时满足以下要求。

a）金融机构应根据成本风险平衡原则选择布局模式，布局可参照附录。

b）同城容灾中心与生产中心应在不同园区、动力应来自不同变电站，避免同一城市内的小范围停电、建筑物火灾、基础设施设备故障、通信线路设备故障、软硬件故障以及其他突发事件可能造成的局部交通封锁或中断等小范围灾难的同类风险，且直线距离宜大于 10 公里，同时还应符合 JR/T 0071.2 对应安全等级保护级别的相关安全要求。

c）异地容灾中心与生产中心不在同一江河流域、地震带、台风等自然灾害隐患区，避免大范围停电、地震、洪水、海啸、滑坡、泥石流、较大范围的公共卫生事件等较大规模的区域性灾难的同类风险，且直线距离宜大于 300 公里，同时还应符合 JR/T 0071.2 对应安全等级保护级别的相关安全要求。

d）在选择或建设容灾中心时，应对备选场址进行相关的场地风险评估，充分考虑场址周边环境、地质地理条件、市政配套条件、电力供应条件以及通信服务商所能提供的服务能力等诸多因素，全面判断是否符合容灾中心的建设要求。

8.2 基础环境

8.2.1 基础环境建设内容

容灾中心的场地基础环境应包括工作设施、辅助设施、生活配套设施及其他必要设施，具体内容如下。

a）工作设施包括信息系统工作设施和保障系统工作设施等。

b）辅助设施包括日常运行辅助设施、容灾辅助设施、容灾培训设施等。

c）生活配套设施包括保障工作人员餐饮、住宿等日常生活需求的设施。

d）其他必要设施包括集合区、等候区、人流物流通道等。

8.2.2 基础环境建设要求

容灾中心场地基础环境的规划、设计、建设和验收，应符合JR/T 0265、GB/T 22239、JR/T 0071.2等相应的要求，同时满足以下要求。

a）容灾中心设计时宜与生产中心等级相同。

b）在容灾中心场地基础环境建设中，应组织成立建设管理团队，并根据国家政策制度和行业标准的相关要求选择具有项目对应工程能力证明和数据中心建设经验的相关单位完成建设。

c）应组织专家或第三方机构对容灾中心建设和验收的过程及重要节点给予专业监督，确保容灾中心的建设满足设计和运行要求。

d）在建设的各个阶段，应严格按照施工安全标准和项目管理标准组织实施，并且在实施过程中对质量、安全和进度进行持续的监控和审查，确保施工内容与设计目标的一致性。

e）容灾中心的场地基础环境建设应尽可能规避施工的风险，坚持成本风险平衡原则，最大限度地提高资源利用率，并综合考虑技术可行性、技术先进性、可扩展性、可管理性、可持续性，以及环保、节能和社会效益等多个方面。

f）柴油发电机、变配电设施、冷源设施等机电设施不宜布置在地下室的最底层，当布置在地下室的最底层时，应采取措施，防范洪水、管道泄漏、消防排水等水患风险，并应符合防火、防震等相关要求。

g）应进行综合分析和经济比较，有条件时与当地电力部门或其他机构签署含有优先供电的供电协议或灾难情况下的应急供电协议。

8.3 网络建设

容灾中心网络建设应符合JR/T 0265和JR/T 0071.2相应的要求，同时满足以下要求。

a）容灾中心网络应根据容灾中心需求和技术发展状况进行规划、设计和建设。

b）容灾中心与生产中心间互联网络宜提供充足的备份数据传输带宽，满足业务连续性要求高的业务数据备份峰值所需的带宽需求。

c）主备架构模式中，容灾中心的出口网络带宽应至少满足重要业务系统基本对外服务能力的带宽需求，宜满足重要业务系统全部对外服务能力的带宽需求；同城双活或异地多活模式中，容灾中心的出口网络带宽宜与生产中心相同。

d）容灾中心网络建设应考虑金融数据中心之间互联的时延需求。

e）容灾中心网络应处于就绪状态，宜处于运行状态。

f）容灾中心网络应至少支持自动或集中切换，宜支持实时无缝切换。

g）容灾中心网络宜支持生产中心和容灾中心的负载均衡。

9 运维管理

9.1 原则

容灾中心的运维管理应遵循以下原则。

a）制度化原则：应建立完善的、可行的运维管理流程和制度，提高运维管理的质量、效率和水平。

b）关联性原则：容灾中心运维管理应与生产中心运维管理相关联，在人员岗位构成、日常管理流程和应急恢复期管理流程的衔接、演练组织等方面都应与生产中心相关联。

c）可用性与有效性原则：容灾中心运维管理制度应通过全面测试和定期的验证机制，确保可用性和有效性。

d）安全性原则：容灾中心安全管理要求应与生产中心保持一致，实现灾难发生时容灾中心对生产中心的平稳接替。

9.2 工作内容

9.2.1 日常运维

容灾中心的日常运维管理应符合GB/T 51314相应的要求，同时应满足以下要求。

a）应定期维护场地环境，保证容灾中心工作设施、辅助设施和生活设施等的可用性。

b）应定期检测维护备用网络系统，包括数据网络、存储网络等。

c）运维团队应具备后备人力资源，在生产中心人员不可用的情况下负责容灾切换、接管生产中心和容灾中心运行管理工作。

d）应建立统一协调运维管理机制，开展常态化联合运维，实现生产中心和容灾中心运维人员能力互备。

e）应由专人承担容灾中心的安全管理职能，以保证在紧急状况发生时获取最优的处置效率和最基本的安全保障。

f）宜以电子化、自动化、可视化和可监控化的方式管理生产中心和容灾中心日常运行。

9.2.2 预案

9.2.2.1 制定内容

金融机构应结合自身实际制定灾难恢复预案。灾难恢复预案至少应包括以下内容。

a）灾难恢复范围、时间和目标。

b）灾难恢复的总体章程，包括灾难恢复管理组织机构、指挥中心决策和授权的流程。

c）突发事件应急响应规程。

d）灾难切换规程。

e）灾后重续运行操作指引。

f）灾难切换操作手册。

9.2.2.2 更新维护

预案的更新维护主要包括以下工作要求。

a）预案涉及的内容发生变更后应立即更新预案。

b）预案涉及的机构、人员有义务向预案管理人员提供变更信息。

c）演练后应根据演练评估结果立即更新预案。

d）预案若发生重大变更，如组织架构、系统架构、基础设施或运维方式等发生重大变更时，应由决策层进行必要的审核批准后，方可更新预案。

e）宜以电子化的方式管理灾难恢复预案。

9.2.3 演练

9.2.3.1 组织实施

金融机构应每年至少组织 1 次全方位应急演练，可根据金融机构实际情况不定期地组织各种形式与范围的演练，逐年提高演练的难度和复杂性。演练的形式包括以下内容。

a）桌面演练：组织相关人员，以会议形式模拟各种灾难场景，集中讨论应急响应和灾难恢复流程中的管理与指挥协调，验证灾难恢复预案的决策和指挥能力。

b）模拟演练：现场模拟灾难场景，利用容灾中心和灾难恢复预案模拟系统切换和业务恢复，宜通过模拟系统实现更贴近实际的仿真演练。

c）实战演练：利用容灾中心和灾难恢复预案完成系统切换和业务恢复，实战演练宜包括核心网络切换、重要系统切换、基础环境切换等。

9.2.3.2 评估

演练完成后，应对演练的组织、过程、效果进行评估，主要包括以下内容。

a）预案的有效性和可用性。

b）演练结果与演练目标的差距。

c）演练过程中发现的生产中心和容灾中心存在的问题。

d）演练工作的组织、实施情况。

e）参加演练人员的应急处置能力。

f）应急资源的协调、保障能力。

应根据演练后的评估结果，形成正式的演练总结报告，内容应包括演练结果、建议和改进措施，并对预案进行更新维护。在下次演练中应加强对更新部分的演练，验证更新部分的有效性。

9.2.4 应急和切换

9.2.4.1 应急响应

发生突发事件时，应按照既定的突发事件应急响应规程，做好突发事件应急处置，根据事件等级及分类响应流程进行应急响应，加强协调配合，快速有效处置突发事件，包括但不限于以下内容。

a）启动应急机制，响应紧急事件。

b）接收和报告紧急事件信息，调度应急资源。

c）评估分析紧急事件影响范围、程度，将紧急事件进行分级，初步诊断紧急事件发生的原因，判断恢复所需时间。

d）采取必要的控制措施，最大限度保护运行安全、抑制事态恶化、降低损失。

e）根据有关制度规定，通报相关主管部门，并做好社会公告和客户服务工作。

f）根据对紧急事件的处置和评估结果，判断紧急事件是否为灾难事件，决策后分别进入应急处置流程和灾难切换流程。

9.2.4.2 灾难切换

发生灾难事件后，应根据灾难切换规程有序实施应对，包括但不限于以下内容。

a）应采用最快、最有效的联络方式，通知和召集灾难恢复预案中各组织机构人员，进入操作流程。

b）应遵循统一指挥原则，服从决策层或其授权的负责人的统一指挥，各部门相关人员密切协作，加强沟通。

c）应快速调动和有效配置容灾资源。

d）应根据有关制度规定，通报相关主管部门，并做好社会公告和客户服务工作。

e）应合理处置灾难事件，密切跟踪事态变化和恢复进程。

f）应本着最小影响、最小损失的原则，在合理时间内决策切换至容灾中心接替运行。

g）在切换过程中，容灾中心应在场地环境、设备操作等方面提供支持，配合将生产系统从生产中心切换到容灾中心。

h）在接替生产中心运营服务期间，容灾中心应增强技术支持与设施资源保障，以接替生产中心的日常工作。

9.2.5 教育和培训

为使相关人员了解金融数据中心容灾建设的目标和流程，熟悉应急响应和灾难切换的操作规程，金融机构应按照以下要求，组织教育和培训。

a）金融机构应按照运维管理要求为相关工作人员提供日常运维、灾难恢复预案、应急响应和灾难切换等有针对性的专业岗位培训，预先对培训需求进行评估，包括培训的频次和范围。

b）金融机构应保留每次培训的记录。

c）金融机构宜使用电子化培训管理系统，对以上要求实现过程化、精细化管控。

9.3 资源保障

金融机构应投入相应的资源保证容灾中心得到及时的更新维护，以确保容灾中心稳定高效运行并满足容灾需求。容灾资源包括但不限于以下内容。

a）金融数据中心场地环境资源。

b）金融数据中心后备电力、网络、设备等资源。

c）具有容灾工作能力的人力资源。

d）后勤保障资源。

附　录
（资料性）
两地三中心和多地多中心架构实例

1　两地三中心架构实例

金融数据中心容灾建设采用两地三中心布局模式时，架构可参考图1。

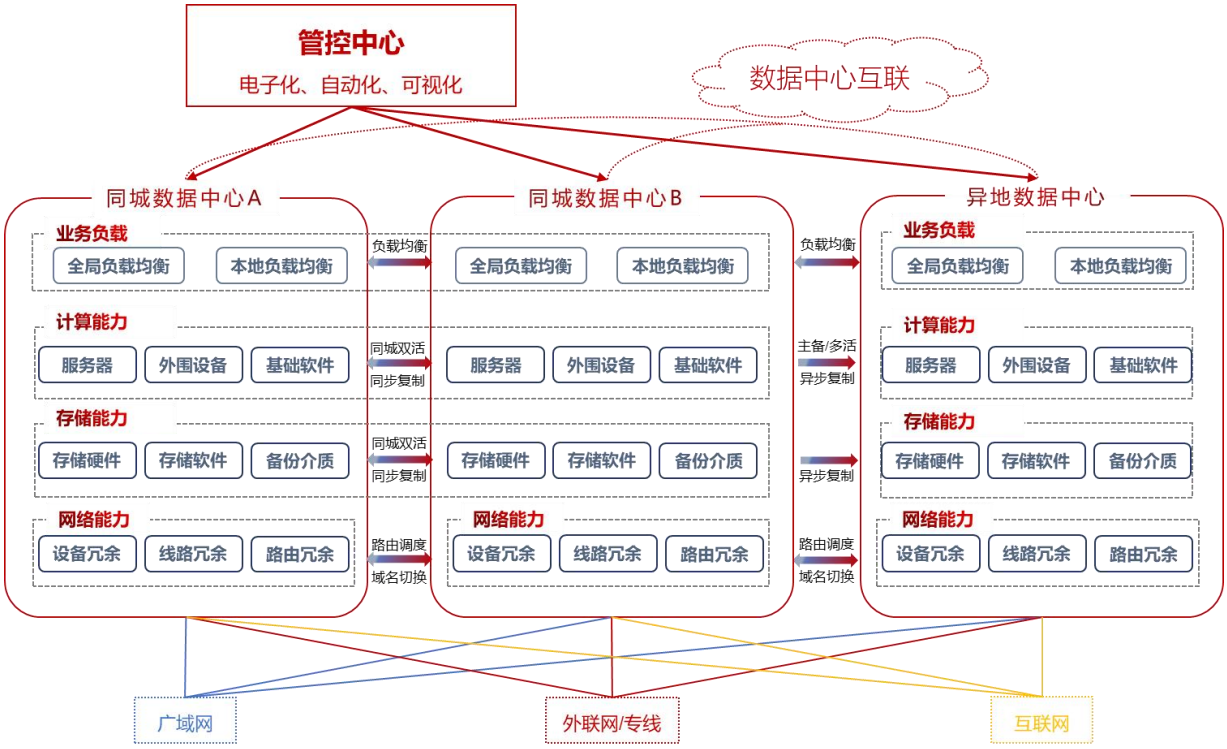

图 1　两地三中心架构示意图

两地三中心架构中，同城双中心宜为双活数据中心，异地中心为主备或多活数据中心，以实现更高的容灾能力。两地三中心架构应满足以下要求。

a）接入层分流：可根据地域、业务场景、用户属性等路由规则分流。

b）应用层多活：应用多中心部署、无数据中心级单点故障。

c）数据层同步：数据按需实现同步和灾难备份。

d）一体化运维：支撑多数据中心统一运维，东西南北流量大小可灵活调配。

e）多中心容灾：按定义规则实现单元级、数据中心级等维度容灾切换。

2　多地多中心架构实例

金融数据中心容灾建设采用多地多中心布局模式时，可以三地六中心布局作为参考，架构如图2所示。

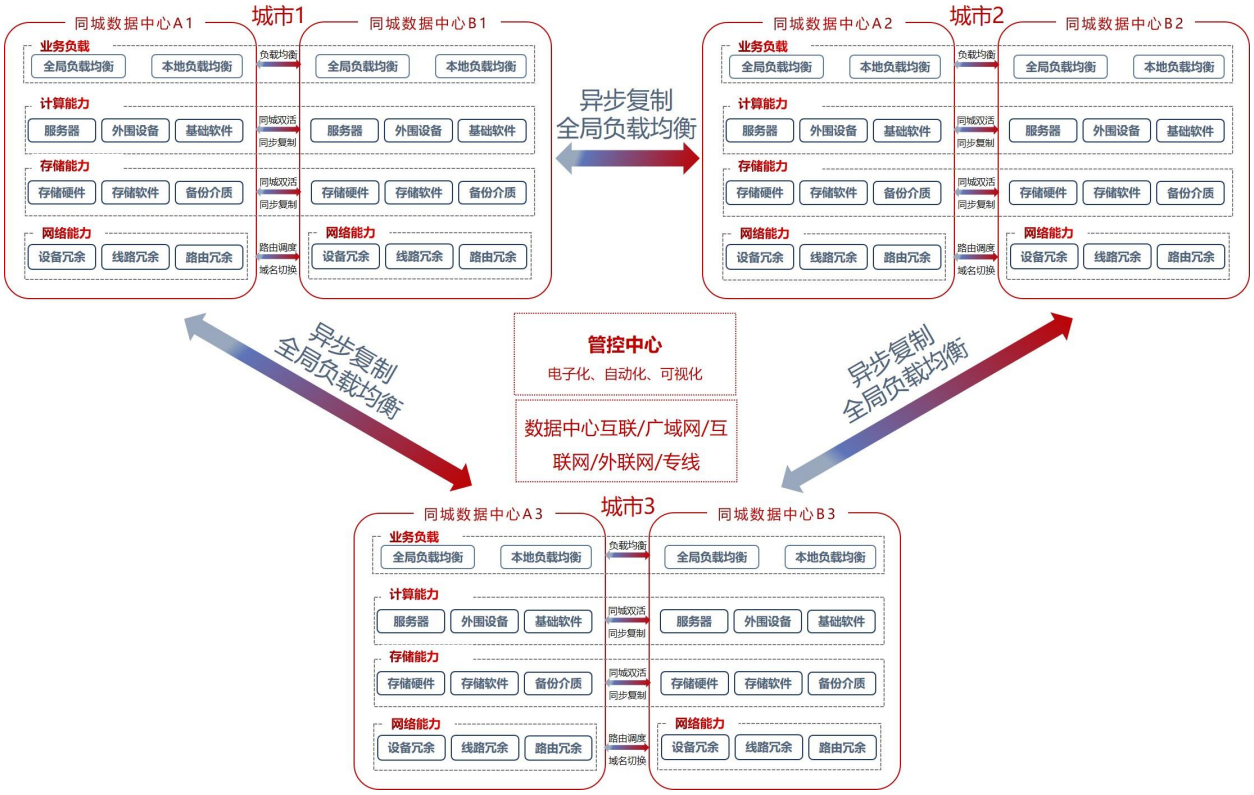

图 2　三地六中心架构示意图

三地六中心架构是在3个城市建设6个数据中心，每个城市分布2个同城双活数据中心，3个城市数据中心之间互为主备或多活数据中心。三地六中心架构应满足以下要求。

a）接入层分流：可根据地域、业务场景、用户属性等路由规则分流。

b）应用层多活：应用多地多中心部署、无区域级单点故障。

c）数据层同步：数据按需实现同步和灾难备份。

d）一体化运维：支撑多数据中心统一运维，东西南北流量大小可灵活调配。

e）多中心容灾：按定义规则实现单元级、数据中心级等维度容灾切换。

参 考 文 献

[1] GB/T 30285 信息安全技术 灾难恢复中心建设与运维管理规范
[2] GB/T 33136 信息技术服务 数据中心服务能力成熟度模型
[3] GB/T 36957 信息安全技术 灾难恢复服务要求
[4] GB 50016 建筑设计防火规范
[5] GB 50174 数据中心设计规范
[6] JR/T 0044 银行业信息系统灾难恢复管理规范
[7] JR/T 0059 证券期货经营机构信息系统备份能力标准
[8] JR/T 0168 云计算技术金融应用规范 容灾
[9] JR/T 0205 分布式数据库技术金融应用规范 灾难恢复要求