TC260-PG-2022XX

网络安全标准实践指南

—信息系统灾难备份实践指引

（征求意见稿 v1.0-202204）

全国信息安全标准化技术委员会秘书处

2022 年 04 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、华为技术有限公司、北京信息灾备技术产业联盟、上海爱数信息技术股份有限公司、北京鸿腾智能科技有限公司、北京易华录信息技术股份有限公司、中国建设银行股份有限公司、北京邮电大学等单位的技术支持。

摘　要

落实《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》要求，为解决大数据场景下云灾难备份应用中暴露出的安全问题，本实践指南分别面向服务提供方和服务需求方，给出了其在需求分析、功能设计、运行维护等方面可采取的安全措施。

目　录

1 范围

本文件从需求分析、功能设计、运行维护等方面提出信息系统灾难备份的安全措施建议。

本文件适用于各类组织开展信息系统灾难备份实践工作。

2 术语和定义

2.1 灾难

由于人为或自然原因，造成信息系统严重故障或瘫痪，使信息系统支持的业务功能停顿或服务水平不可接受、达到特定时间的突发性事件。

2.2 灾难备份

为了将信息系统从灾难中恢复到正常状态而对数据、数据处理系统、网络系统、基础设施、技术支持能力和运行管理能力进行备份的过程。

2.3 灾难备份系统

用于将信息系统从灾难中恢复到正常状态的目的，由数据备份系统、备用数据处理系统和备用的网络系统组成的信息系统。

2.4 服务提供方

具有专业的灾难备份服务团队和资源，提供灾难备份系统的功能设计、运行维护等服务的组织或部门。

2.5 服务需求方

需要通过服务提供方的专业服务和资源完成灾难备份系统、实现灾难恢复的组织或部门。

3 概述

灾难备份主要包含数据备份以及业务容灾两部分技术内容，现已成为确保信息系统正常稳定运行的必要技术手段。GB/T 20988—2007、GB/T 30285—2013、GB/T 36957—2018、GB/T 37046—2018等国家标准都对灾难备份的资源配置、过程管理和项目管理等进行了规范，促进形成了例如“两地三中心”等形式的行业公认较好实践。

然而，随着近年来大数据、云计算等新技术的快速发展应用，带来新的安全风险，新的安全问题持续显现。同时，相继出台的数据安全、个人信息保护相关法律法规也对灾难备份提出了更高要求。信息系统灾难备份在当前环境下存在以下主要风险问题：

一是数据安全风险，主要是重要数据安全风险。在我国《数据安全法》发布后,信息系统灾难备份容易出现重要数据违规处理安全问题，例如未能及时发现因灾备数据持续累积产生的重要数据、因采用云架构产生的重要数据意外出境等安全风险。

二是个人信息保护风险。在我国《个人信息保护法》发布后，信息系统灾难备份容易发生个人信息过度冗余备份、难以追溯，特别是难以按照法律法规要求针对个人信息主体权益对个人信息进行删除等操作、损害个人合法权益的安全风险。

三是云灾备等新模式带来的安全风险。随着云技术发展，使用云架构进行一般场景的灾备已经成为一种常见模式，然而，云灾备模式存在访问控制不严导致云端泄漏、在不同虚拟位置开展云灾备时可能因实际物理位置相同导致灾备策略失效等风险。

4 安全措施

4.1 基本措施

a. 服务需求方应全面掌握国家、地方、所在行业灾备的相关政策，重点包括信息系统安全、关键信息基础设施安全、数据安全、个人信息保护等方面。

b. 数据安全方面，信息系统灾难备份应符合 GB/T 37973—2019《信息安全技术 大数据安全管理指南》、GB/T 37988—2019 《信息安全技术 数据安全能力成熟度模型》等数据安全相关国家标准。

c. 个人信息保护方面，信息系统灾难备份应符合 GB/T 35273—2020《信息安全技术 个人信息安全规范》、GB/T 39335—2020 《信息安全技术 个人信息安全影响评估指南》等个人信息保护相关国家标准。

d. 应用云灾备等新技术方面，数据需求方应结合新技术特点，通过合同等具有法律约束力的文件进行详细约定，明确安全职责，特别是应明确未经服务需求方委托，服务提供方不得对灾难备份系统上的业务、数据内容进行查阅、判断、分析等。

4.2 需求分析方面

4.2.1 数据安全保护

a. 服务需求方应有专业网络安全人员全程参与信息系统灾难备份需求分析工作。

b. 服务需求方应对其所使用或持有的全部信息系统上的业务和数据进行全面梳理，明确当前一般数据、重要数据、核心数据处理情况。应同时分析在后续信息系统及灾难备份系统运行过程中，一般数据可能因规模增长变为重要数据的情况。

c. 服务需求方应重点围绕蓄意破坏、操作失误、设备故障以及自然灾害等灾难，结合信息系统所处安全环境，对信息系统因灾难遭受损失的可能性以及损失影响进行全面分析。

d. 服务需求方应根据各信息系统业务和数据梳理结果，结合灾难发生时遭受损失的可能性以及损失影响分析，确定各信息系统灾难备份的迫切性，明确各信息系统灾难备份的要点。

e. 服务需求方应明确提出各信息系统的技术指标，包括代表系统和数据恢复程度的“恢复点目标”，以及代表系统和数据恢复速度的“恢复时间目标”。

注：恢复点目标是指灾难发生后，系统和数据必须恢复到的时间点要求。恢复时间目标是指灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求[1]。

f. 服务需求方应明确提出灾难备份位置的需求，将可能涉及重要数据的灾难备份系统在境内部署，重要数据按我国法律法规要求符合可出境条件的除外。

4.2.2 云技术应用

服务需求方应重点分析委托他人设计灾难备份系统、以及委托他人运行维护灾难备份系统的安全风险，存在重大风险的应自主开展相关工作。

4.3 功能设计方面

4.3.1 数据安全保护

a. 对业务连续性要求高的信息系统，特别是为公众提供实时服务的信息系统，服务需求方宜采用跨地区部署、具有独立数据存储系统以及业务容灾系统的“两地三中心”架构；如提供涉及生命安全、财产安全等重要事务服务的，可考虑进一步增加部署地区以及灾难备份系统数量。

b. 服务提供方应谨慎设定信息系统及其对应的灾难备份系统间的物理距离，避免因距离过近丧失对同一类灾害的抵抗能力，同时避免因距离过远灾难恢复延时过长。

c. 对灾难备份系统应评估服务需求方所需备份的数据规模，若数据量显著大于网络传输能力，服务提供方应为服务需求方提供通过存储介质一次性取回全部备份数据的方式。

4.3.2 个人信息保护

对涉及处理个人信息的灾难备份系统，服务提供方应按个人信息保护相关要求，设计可与信息系统同步进行个人信息查询、删除

等操作的功能。因采用了快照等技术方案，实时同步删除灾难备份系统中的个人信息实践上难以实现的，服务提供方应为服务需求方提供落实个人信息保护相关要求的可行替代方案。

注：一种可行替代方案是：对暂时难以同步删除的个人信息，服务需求方立即停止除存储和必要安全保护之外的其他处理，但在具备删除条件时，例如数据备份被恢复时，立即删除该个人信息。其中，必要安全保护包括但不限于设置访问控制、进行数据加密等。

4.3.3 云技术应用

a. 对灾难发生时遭受损失的可能性以及损失影响较小的信息系统，特别是业务规模以及数据规模较小或随时间快速变化的，服务需求方宜采取基于云的灾难备份功能设计方案。

b. 服务提供方应向服务需求方明确告知所有基于云的灾难备份系统的部署位置，以及相关数据存储、传输涉及的物理位置。

c. 为服务需求方同时提供基于云的信息系统与其对应灾难备份系统的运行维护时，服务提供方应主动向服务需求方说明可能因管理、技术、人员等问题引发的多个系统同时失效的情况。

d. 服务提供方应积极促进不同基于云的灾难备份系统之间的互联互通，不应通过技术手段为互联互通设置阻碍。

4.4 运行维护方面

4.4.1 数据安全保护

服务需求方应制定灾难恢复应急预案，每年至少进行一次安全

演练，并对使用灾难备份系统的人员开展定期培训。

4.4.2 个人信息保护

按个人信息保护要求对个人信息进行查询、删除等处理时，服务需求方应全面分析灾难备份系统中可能存在的备份，并按个人信息保护要求、依照 4.3.2 a 预设的处理方案同步处理。

4.4.3 云技术应用

发生灾难时，服务提供方应将灾难影响、应对措施、恢复进度等信息与服务需求方进行及时、有效、准确的沟通。重大事件应及时向有关部门报告。

参考文献

[1] GB/T 20988—2007　信息安全技术　信息系统灾难恢复规范

[2] GB/T 30285—2013　信息安全技术　灾难恢复中心建设与运维管理规范

[3] GB/T 36957—2018　信息安全技术　灾难恢复服务要求

[4] GB/T 37046—2018　信息安全技术　灾难恢复能力评估准则