TTA Standard

정보통신단체표준

TTAS.KO-10.0259

제정일: 2007년 12월 26일

정보시스템 재해복구 지침

(Guideline for Disaster Management of Information Systems)

TTA 한국정보통신기술협회
Telecommunications Technology Association

정보통신단체표준 제정일 : 2007년 12월 26일
TTAS.KO-10.0259

정보시스템 재해복구 지침

(Guideline for Disaster Management of Information Systems)

한국정보통신기술협회
Telecommunications Technology Association

서 문

1. 표준의 목적

본 지침은 화재 및 지진, 테러 등으로 인해 발생하는 각종 재해로부터 기관의 정보 및 데이터를 보호하기 위한 절차와 방법을 제시한다.

2. 주요 내용 요약

본 지침은 재해 발생 시, 서비스의 정상화를 위한 재해복구센터의 구축, 운영 절차와 가이드를 제공한다. 재해복구센터를 구축. 운영하기 위한 절차는 재해복구 전략 수립, 재해복구시스템 설계 및 구축, 재해복구시스템 운영 등으로 구성된다. 또한 일반적인 개념으로서, 재해복구시스템의 형태 및 기술에 대해 설명한다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

본 지침은 각 조직의 정보시스템 운영 담당자들이 참조할 수 있으며, 각 조직의 재해예방 및 복구 절차를 정립하는데 활용될 수 있다.

4. 참조 표준(권고)

4.1 국외표준(권고)

없음

4.2 국내표준

없음

5. 참조표준(권고)과의 비교

5.1 참조표준(권고)과의 관련성

해당사항 없음

5.2 참조한 표준(권고)과 본 표준의 비교표

해당사항 없음

6. 지적재산권 관련사항

2007년 12월까지 이 표준과 관련하여 확인된 지적재산권 없음.

7. 적합인증 관련사항

7.1 적합인증 대상 여부

해당사항 없음

7.2 시험표준제정여부(해당 시험표준번호)

해당사항 없음

8. 표준의 이력

판수	제/개정일	제/개정내역
제1판	2007.12.26	제정

Preface

1. The Purpose of Standard

This standard specifies about protection method and procedure of Information and data form the disasters such as fire, earthquakes, terrorism and so on.

2. The summary of contents

This guideline provides direction and process for developing and maintaining of disaster recovery center. Process of developing and maintaining of disaster recovery center is consist of 3 step, establishing recovery strategy, design and implementation and operation of disaster recovery system. also, it guideline explains type and technology of disaster recovery system.

3. Applicable fields of industry and its effect

Information system operator can use this guideline, and they use this to establish disaster recovery process and procedure.

4. Reference Standards(Recommendations)

4.1 International Standards(Recommendations)

None

4.2 Domestic Standards

None

5. Relationship to Reference Standards(Recommendations)

5.1 The relationship of Reference Standards(recommendations)

N/A

5.2 Differences between Reference Standard(recommendation) and this

standard

N/A

6. The Statement of Intellectual Property Rights

As of December of 2007, any IPRs related to this standard cannot be found.

7. The Statement of Conformance Testing and Certification

N/A

8. The History of Standard

Edition	Issued date	Contents
The 1st edition	2007.12.26	Established

목 차

Contents

1. 개요

공공부문 정보화사업의 확산으로 인해, 다수의 정보시스템이 각 부처 및 공공기관에 도입되었고, 이를 통해 각 기관은 내부 업무 프로세스 및 대민서비스 등을 정보시스템을 통해 수행하고 있다. 최근까지 지속·확장되고 있는 정보시스템의 고도화는 업무의 정보시스템 의존도를 더욱 심화시키고 있으며, 만약 정보시스템이 중단되는 사태가 발생한다면, 기관 전체의 업무가 마비될 수도 있는 위험성을 안고 있는 상황에 이르렀다.

2001년 미국의 9·11 테러사태 이전까지만 해도 국내에서의 재해재난에 대한 정보시스템 대비책은 극히 미약한 실정이었다. 그러나 재해에 대한 각종 국내외 사고사례가 발생하면서, 이에 대한 대비책의 마련은 선택 사항이 아니라, 필수 사항으로 자리매김하게 되었다.

이에 따라, 현재 각 기관에서는, 재해에 대비하여 기관의 정보 및 데이터를 보호하기 위한 각종 백업 정책들을 마련, 실행하고 있다. 이는 테이프 혹은 디스크 등 물리적인 매체에 데이터를 저장하여 소산 보관하는 백업 방식에서부터, 재해복구센터를 구축하여 실시간으로 자료를 백업하는 방식까지 다양한 방법으로 존재한다. 물리적 백업의 소산보관은 비용이 적게 드는 대신, 백업완료 시점부터 재해발생 이전까지의 데이터 손실에 대한 위험이 있는 반면, 실시간 백업은 재해 시 정보의 손실은 없지만, 구축 및 운영비용이 많이 든다는 단점이 있다. 따라서, 각 기관에 적절한 재해 예방 및 복구방식을 선택하는 것이 중요하다.

‘2004년 주요 공공기관 정보자원 현황 분석(NCAIV-RER-04045, 한국전산원)’에 따르면, 재해복구를 위한 재해복구센터를 구축 또는 활용하고 있는 기관은 조사에 응답한 225개 기관 중 총 25개 기관의 65개 시스템으로서, 전체의 약 11%에 이르고 있다.

본 지침에서는 재해에 대비한 재해복구센터 구축과 운영에 초점을 맞추어 그 절차와 방법을 설명한다. 본 지침을 통해, 아직 재해복구를 위한 재해복구센터를 구축하지 않은 기관에서는 그 도입의 필요성을 인지하고, 재해복구센터 구축을 위한 절차와 고려사항을 참고할 수 있다. 또한 이미 재해복구센터를 구축한 기관에서는 재해복구를 위한 센터의 운영과 평시 모의훈련방법 등에 대해 참고할 수 있다.

시스템 및 인력상의 오류 및 장애에 대해서는 ‘정보시스템 장애관리 지침’을 참조한다. 또한, 일반적인 백업기술 및 백업방식에 대해서는 ‘정보시스템 백업 지침’을 참조한다.

2. 지침의 구성 및 범위

본 지침은 재해복구를 위한 재해복구센터의 구축 및 운영에 대한 절차와 가이드라인을 제공한다. 본 지침은 다음과 같은 내용으로 구성되어 있다. 3장에서는 재해, 재난, 장애 등에 대한 용어정의와 재해복구시스템의 개념에 대해 살펴본다.

4장에서는 재해복구시스템의 유형을 구축형태별, 운영주체별, 복구수준별로 구분하여 설명하고, 재해복구시스템을 구현하기 위한 기술로서 데이터 복제방식과 데이터 전송방식, 재해복구시스템용 네트워크의 종류에 대해 설명한다.

5장에서는 업무영향분석 및 IT자원 복구 전략 등 재해복구 전략 수립에 대한 절차와 방법에 대해 설명한다.

6장에서는 재해복구시스템을 구축하기 위한 설계단계로서, 재해복구시스템 운영형태와 유형을 결정하기 위한 고려사항에 대해 설명한다. 또한, 재해복구시스템 설계 및 구축 기술 결정을 위한 고려사항과 재해복구를 위한 인력구성방안에 대해 설명한다.

7장에서는 재해복구시스템 운영 시 조직의 역할과 책임에 대해 설명하고, 재해가 발생했을 경우, 재해복구를 위한 절차와 주센터 복귀를 위한 절차를 제시한다. 또한 재해 시 원활한 복구활동을 위한 재해복구를 위한 모의훈련 종류와 절차에 대해 설명한다.

3. 재해 및 재해복구의 개념

3.1 재해와 재난의 개념

<요약>

o 법률적 의미에서 재난과 재해는 다음과 같이 구분될 수 있음
- 재난 : 국민의 생명·신체 및 재산과 국가에 피해를 주거나 줄 수 있는 것
- 재해 : 재난으로 인하여 발생하는 피해

o 본 지침에서는 재난과 재해를 구분하지 않으나, 용어상 재해로 통일하여 사용

재해(災害, disaster)의 사전적 의미는 재앙으로 말미암은 피해(동아 새국어사전)이다. 한편, 재난(災難)은 뜻밖의 불행한 일(동아 새국어사전)으로 정의되어 있어, 재난이 사건을 가리키는 반면 재해는 재앙적 사건으로 인해 발생한 피해를 가리킨다는 차이가 있음을 알 수 있다.

법률적으로는, 재난은 다음과 같이 정의된다(재난 및 안전관리 기본법 제3조 제1호).

"재난"이라 함은 국민의 생명·신체 및 재산과 국가에 피해를 주거나 줄 수 있는 것으로서 다음 각목의 것을 말한다.

가. 태풍·홍수·호우(豪雨)·폭풍·해일(海溢)·폭설·가뭄·지진·황사(黃砂) ·적조 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해

나. 화재·붕괴·폭발·교통사고·화생방사고·환경오염사고 그 밖에 이와 유사한 사고로 대통령령이 정하는 규모 이상의 피해

다. 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비와 전염병 확산 등으로 인한 피해

한편, 재해는 다음과 같이 정의되고 있다(자연재해대책법 제2조 제1호).

"재해"라 함은 재난및안전관리기본법(이하 "기본법"이라 한다) 제3조제1호의 규정에 의한 재난으로 인하여 발생하는 피해를 말한다.

따라서, 재해란 재난으로 인한 피해를 뜻하는 것으로 정의되어 있어, 사전적 정의에 부합하고 있음을 알 수 있다.[1)]
그러나, 현실적으로는 재해는 영어의 'disaster'에 대한 번역어로서 흔히 사용되고 있다. 어원상 사악한 별(evil star)의 의미를 가지고 있는 영어 단어 disaster는 우리말의 재해 및 재난을 통칭하고 있으며, 실제에 있어서도 재해와 재난은 흔히 혼용하여 사용되고 있다. 본 지침에서는 재해와 재난을 굳이 구분하지는 않으나, 용어상 재해로 통일하여 사용한다.

3.2 재해와 장애의 개념

<요약>

o 재해(Disaster) : 정보기술 외부로부터 기인하여 예방 및 통제가 불가능한 사건으로 인해 정보기술서비스가 중단되거나, 정보시스템의 장애로부터의 예상 복구소요시간이 허용 가능한 범위를 초과하여, 정상적인 업무 수행에 지장을 초래하는 피해

o 장애(Incident) : 정보기술서비스관리의 통제 가능성 관점에서 협의의 장애 개념으로서, 통제 불가능한 재해(자연 재해와 인적 재해)를 제외한 발생원인 관점에서 직접적으로 영향을 미치는 인적장애, 시스템 장애, 기반구조 장애(운영 장애, 설비 장애 등 포함) 등과 같은 통제 가능한 요인들에 의한 정보시스템의 기능저하, 오류, 고장

o 재해와 장애의 비교

구분	재해	장애
원인의 발생위치	정보기술기반 외부	정보기술기반 내부
예방 및 통제	불가능	가능
정보기술기반의 손상규모	한 Site 전체	Site 내에서 부분적
대응조직의 수준	전사적수준	정보시스템관리부서수준
시스템 복원 예상소요시간	중·장기(수일 이상)	단기(수시간)

재해의 정의와 관련하여, 사전적 의미를 벗어나, 정보시스템을 기반으로 하는 업무에 영향을 미치는 재해에 주안점을 두는 관점에서, 광의의 재해는 다음과 같은 정의될 수 있다. (J.W.Toigo, Disaster Recovery Planning : Strategies for

1) 이전의 재난관리법에서는 "재난이라 함은 화재·붕괴·폭발·교통사고·화생방사고·환경오염사고등 국민의 생명과 재산에 피해를 줄 수 있는 사고로서 자연재해가 아닌 것을 말한다."(제 2조 1항)로 정의되어 있어, 재난을 자연재해와 구분하였으나, 이 법은 재난 및 안전관리 기본법이 시행됨에 따라 폐지되었으며, 현재의 재난 및 안전관리 기본법에서는 자연재해도 재난의 범주에 포함시키고 있다.

Protecting Critical Information, 2nd Ed.)

> 본서에서의 재해란, 업무를 지원하는 정보기술기반 구성요소의 중단으로 인하여 야기된 계획되지 않은 업무 프로세스 중단을 뜻한다. (The term disaster, as used in this book, means the unplanned interruption of normal business processes resulting from the interruption of the IT infrastructure components used to support them.)

즉, 위의 정의에서는 업무에 영향을 미치는 정보시스템 중단사태를 모두 재해라고 통칭하고 있다. 한편 '정보시스템 장애관리지침'에서는

> 정보시스템의 장애에 관한 광의의 개념은 정보시스템의 정상적인 운영을 방해하는 자연재해, 시스템 장애와 기반구조 장애(혹은 운영 장애와 설비장애 등)를 모두 포함한다. 광의의 개념은 정보시스템에 직·간접적으로 영향을 미치는 모든 요인들을 포함한다.

과 같이 지적하고 있어, 광의의 개념에서 볼 때에는 재해와 장애의 개념에는 차이를 두기 어렵다. 이에 따라, 동 지침에서는 협의의 개념으로서의 장애를 다음과 같이 정의하고 있다.

> o 장애(Incident)
> 정보기술서비스관리의 통제 가능성 관점에서 협의의 장애 개념으로서, 통제 불가능한 재해(자연 재해와 인적 재해)를 제외한 발생원인 관점에서 직접적으로 영향을 미치는 인적장애, 시스템 장애, 기반구조 장애(운영 장애, 설비 장애 등 포함) 등과 같은 통제 가능한 요인들에 의한 정보시스템의 기능저하, 오류, 고장

즉, 정보시스템 장애관리지침에서는, 협의의 장애의 개념에서는 광의의 개념에서 포함한 자연 재해를 제외하고 직접적으로 정보시스템에 영향을 미치는 요인들 즉, 시스템 장애와 기반구조 장애(혹은 운영 장애와 설비 장애 등)와 같은 요인들만을 포함하여, 정보시스템의 장애에 관한 광의와 협의의 개념을 그 직접적인 통제가능성으로 나누고 있다. 이에 따라, 재해와 장애의 개념구분은 정보시스템 조직 관점에서의 통제가능성에 따라서, 통제 가능한 요인에 의한 기능저하, 오류, 고장을 장애라고 하고, 그 외에 통제 불가능한 경우는 재해라고 설명하고 있다.

한편으로, 장애라고 할지라도 이로 인한 정보시스템 서비스의 중단시간이 허용 가능한 시간(예로서 24시간)을 초과하는 경우에는 재해로 볼 수 있다(정보시스템 장애관리지침, 2004). 장애로 인한 실제의 서비스 중단시간은 복구가 이루어지는 시점에 가서야 사후적으로 알 수 있는 것이므로, 서비스의 실제 중단 시간을

기준으로 재해와 장애를 구분하는 것은 실용적이라고 보기는 어렵다. 그러나, 많은 경우 실무 전문가의 지식과 경험을 바탕으로 장애가 발생한 시점에 복구까지의 소요시간을 예상할 수는 있으므로, 장애로 인한 정보시스템 서비스의 중단이 발생하였을 때 이의 복구까지 예상 소요 시간을 장애와 재해를 나누는 기준으로 활용할 수 있다.

이상의 논의를 바탕으로, 본 지침에서는, 정보시스템의 중단을 야기하는 사건 중 외부로부터 기인하여 예방 및 통제가 불가능한 사건 및 예상 복구소요시간이 허용 가능한 범위를 넘어서는 장애를 협의의 재해로 정의한다. 따라서, 본 지침에서는 사용하는 재해의 정의는 다음과 같다.

o 재해(Disaster)
정보기술 외부로부터 기인하여 예방 및 통제가 불가능한 사건으로 인해 정보기술서비스가 중단되거나, 정보시스템의 장애로부터의 예상 복구소요시간이 허용 가능한 범위를 초과하여, 정상적인 업무 수행에 지장을 초래하는 피해

본 지침의 정의에 따라, 재해와 장애는 다음과 같이 비교해 볼 수 있다.

<표 3-1> 재해와 장애

구분	재해	장애
원인의 발생위치	정보기술기반 외부	정보기술기반 내부
예방 및 통제	불가능	가능
정보기술기반의 손상규모	한 Site 전체	Site 내에서 부분적
대응조직의 수준	전사적수준	정보시스템관리부서수준
시스템 복원 예상소요시간	중·장기(수일 이상)	단기(수시간)

재해는 자연재해(natural disaster)와 인적재해(man-made disaster)로 나누어 볼 수 있다. 자연재해는 태풍·홍수·호우(豪雨)·강풍·풍랑·해일 ·지진 등 자연적 현상에 의한 재해를 의미하며, 인적재해는 전쟁·테러·물리적 침입 등 외부로부터의 인위적 재해를 의미한다. 그러나, 자연재해와 인적재해는 정보시스템의 중단을 야기하여 업무에 지장을 초래한다는 측면에서는 동일하므로, 본 지침의 용도에서는 자연재해와 인적재해를 구분하여 기술하지는 않는다.

3.3 재해복구계획과 재해복구시스템의 개념

<요약>

o 재해복구(DR, Disaster Recovery) : 재해로 인하여 중단된 정보기술 서비스를 재개하는 것

o 재해복구계획(DRP, Disaster Recovery Planning) : 정보기술서비스기반에 대하여 재해가 발생하는 경우를 대비하여, 이의 빠른 복구를 통해 업무에 대한 영향을 최소화하기 위한 제반 계획

o 재해복구시스템(DRS, Disaster Recovery System) : 재해복구계획의 원활한 수행을 지원하기 위하여 평상시에 확보하여 두는 인적·물적 자원 및 이들에 대한 지속적인 관리체계가 통합된 것

o 업무연속성계획(BCP, Business Continuity Planning) : 정보기술부문 뿐 아니라, 인력·설비·자금 등 제반 자원을 대상으로 장애 및 재해를 포괄하여 조직의 생존을 보장하기 위한 예방 및 복구활동 등을 포함하는 보다 광범위한 계획

본 지침에서 재해복구(Disaster Recovery)란, 재해로 인하여 중단된 정보기술서비스를 재개하는 것을 의미한다. 재해복구를 위해서는 사전에 재해복구를 위한 계획 및 이를 지원하는 시스템이 준비되어야 하는데, 이를 각각 재해복구계획 및 재해복구시스템(Disaster Recovery System)이라 일컫는다.

재해복구계획(DRP, Disaster Recovery Planning)은 “중요한 업무 프로세스에 대하여 재해가 발생할 가능성 및 재해 발생시의 피해를 최소화하기 위한 일련의 행위 집합(a set of activities aimed at reducing the likelihood and limiting the impact of disaster events on critical business processes)”으로 정의된다(J.W.Toigo, Disaster Recovery Planning : Strategies for Protecting Critical Information, 2nd Ed.). 이러한 정의는 보다 포괄적인 개념으로 받아들여지고 있는 업무연속성계획(BCP, Business Continuity Planning)과 명확히 구분되기 어렵다. 최근에 와서는 두 용어의 차이를 두지 않고 혼용하는 경향도 있으나, 장애와 재해를 구분하여 각각에 대한 관리지침을 별도로 두고 있는 본 지침의 용도에서는, 재해복구계획과 업무연속성계획에 대하여 명확한 개념차이를 두는 것이 필요하다.

본 지침에서는, 재해복구계획(DRP)은 정보기술서비스기반에 재해가 발생하는 경우를 대비하여, 이의 빠른 복구를 통해 업무에 대한 영향을 최소화하기 위한 제반 계획으로 정의하고, 업무연속성계획(BCP)은 정보기술부문 뿐 아니라, 인력·설비·자금 등 제반 자원을 대상으로 장애 및 재해를 포괄하여 조직의 생존을 보장하기 위한 예방 및 복구활동 등을 포함하는 보다 광범위한 계획으로 파악한다. 따라서, 본

지침에서는 재해복구계획을 다음과 같이 정의한다.

o 재해복구계획(Disaster Recovery Planning)
정보기술서비스기반에 대하여 재해가 발생하는 경우를 대비하여, 이의 빠른 복구를 통해 업무에 대한 영향을 최소화하기 위한 제반 계획

재해복구계획의 원활한 수행을 위해서는 이를 지원하기 위한 제반 인적·물적 자원을 평상시에 확보해 두어야 하며, 이러한 자원에 대한 지속적인 관리체계도 필요하게 되는데, 이들을 포괄하여 재해복구시스템 이라고 한다. 따라서, 본 지침에서는 재해복구시스템을 다음과 같이 정의한다.

o 재해복구시스템(Disaster Recovery System)
재해복구계획의 원활한 수행을 지원하기 위하여 평상시에 확보하여 두는 인적·물적 자원 및 이들에 대한 지속적인 관리체계가 통합된 것

3.4 용어정의

o 복구목표시간(RTO : Recovery Time Objective)
: 재해로 인하여 서비스가 중단되었을 때, 서비스를 복구하는데까지 걸리는 최대 허용시간

o 복구목표시점(RPO : Recovery Point Objective)
: 재해로 인하여 중단된 서비스를 복구하였을 때, 유실을 감내할 수 있는 데이터의 손실 허용시점

o 업무연속성계획(BCP : Business Continuity Planning)
: 정보기술부문 뿐 아니라, 인력·설비·자금 등 제반 자원을 대상으로 장애 및 재해를 포괄하여 조직의 생존을 보장하기 위한 예방 및 복구활동 등을 포함하는 보다 광범위한 계획

o 재해복구계획(DRP : Disaster Recovery Planning)
: 정보기술서비스기반에 대하여 재해가 발생하는 경우를 대비하여, 이의 빠른 복구를 통해 업무에 대한 영향을 최소화하기 위한 제반 계획

o 재해복구시스템(DRS : Disaster Recovery System)
: 재해복구계획의 원활한 수행을 지원하기 위하여 평상시에 확보하여 두는 인적·물적 자원 및 이들에 대한 지속적인 관리체계가 통합된 것

o 재해복구센터
: 주센터에 반하여 재해에 대비하여 업무연속성을 보장할 수 있도록 원격지에 구축한 전산센터로써, 원격지센터, 혹은 백업센터라 일컫기도 함

o 주센터
: 현재 사용중인 전산 인프라를 운영하는 전산센터로써, 주전산센터 혹은 주 사이트라 일컫기도 함

4. 재해복구시스템 형태 및 기술

4.1 재해복구시스템 운영방식별 유형

재해복구시스템의 운영형태는 구축형태(박기록, HIS Advantage No. 59, 2002.1) 및 운영주체에 따라 다음과 같이 구분할 수 있다. 단, 아래의 구분은 절대적인 것은 아니며, 경우에 따라 복합적으로 사용될 수 있다.

가. 구축형태별 구분

□ 독자구축

재해복구시스템을 독자적으로 구축하는 방식으로, 보안유지 및 복구의 신뢰성이 가장 높으나, 구축 및 유지비용이 가장 많이 소요된다. 비교적 규모가 큰 금융기관 등에서 주로 채택하고 있는 방식이다.

□ 공동구축

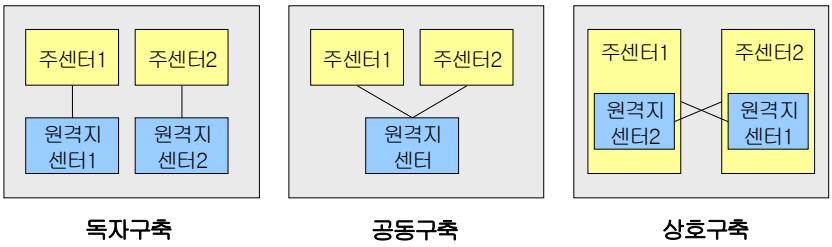
두 개 이상의 기관이 재해복구시스템을 공동으로 이용하는 방식이다. 비용측면에서 독자구축의 경우보다 적게 소요되지만 보안과 운용측면에서는 고려할 사항이 많고, 광역재해 발생시 공동이용기관간의 동시 재해복구가 불가능하다는 단점이 있다. 이 방식에서는 공동이용기관간의 합의가 매우 중요하다. 일본의 경우 투자여력이 상대적으로 적은 지방은행들이 공동으로 재해복구센터를 구축하여 이를 이용하고 있으며, 우리나라의 경우 국가기간정보시스템 공동백업센터가 이러한 형태에 해당한다. 공동구축은 공동이용수준에 따라 다시 다음과 같이 구분해 볼 수 있다.

- 기반시설수준 : 건물, 전력, 항온항습 등 기반시설만 공동으로 이용하는 경우
- 정보시스템수준 : 서버, 디스크, 네트워크 등 정보시스템자원을 공동으로 이용하는 경우

□ 상호구축

별도의 재해복구시스템을 구축하는 대신, 두 개 이상의 기관이 상호간의 재해복구시스템의 역할을 수행하거나, 단일 기관이 여러 개의 정보시스템 사이트를 가지고 있는 경우에는 사이트 상호간에 서로 재해복구센터의 역할을 수행하도록 방식이다. 기관간 계약 또는 사이트간 협조체계에 따라 시스템의 여유를 확보한 후 한 기관(사이트)에 재해가 발생하면 다른 기관(사이트)에 구축되어 있는 재해복구시스템을 이용하는 형태로, 상대방의 업무를 처리할 만한 여유 시스템이 반드시 필요한 방식이다. 앞서의 공동구축의 경우에서와

마찬가지로, 상호구축에서도 상호간 이용하는 재해복구시스템의 수준에 따라 기반시설수준과 정보시스템수준으로 다시 나누어 볼 수 있다. 구축 및 운영비용이 저렴한 장점이 있으나, 서로 다른 기관간에 이러한 방식의 재해복구시스템을 구축하는 경우 보안성 및 재해복구에 대한 신뢰성이 대단히 낮다. 실제로 미국 캘리포니아 커뮤니티은행(California Community Bank)의 경우 화재로 인해 계약 상대방에게 협조를 요청했으나 협조 불충분으로 전산시스템을 복구할 수 없었던 사례가 보고된 바 있다(박기록, HIS Advantage No. 59, 2002.1). 단, 단일 기관의 사이트 상호간에 이러한 시스템을 구축한 경우에는 비교적 높은 신뢰성을 확보할 수 있는데, 우리나라의 경우 대기업의 재해복구시스템 등이 이러한 형태를 채택하고 있다.



(그림 4-1) 재해복구시스템의 구축형태별 유형

나. 운영주체별 구분

□ 자체운영

기관 자체의 인력으로 재해복구시스템을 운영하는 방식이다. 보안성 및 신뢰성이 가장 높으나, 재해복구를 위한 추가의 인력이 확보되어야 하며 운영비용이 높다. 일반적으로 독자구축형 재해복구센터에서 사용되는 운영방식이다.

□ 공동운영

두 개 이상의 기관이 재해복구시스템의 운영인력을 상호 공유하는 방식이다. 일반적으로 공동구축형 또는 상호구축형 재해복구시스템에서 사용되는 운영방식이다. 자체운영에 비해 운영비용을 절감할 수 있으나, 기관간 신뢰가 전제되어야 하고, 보안성 유지를 위한 협의가 중요하다.

□ 위탁운영

재해복구시스템의 운영을 민간 IDC 운영자 등 외부의 다른 기관에 위탁하는 방식이다. 정보시스템 운영기관의 보안성 유지가 가장 큰 문제로 대두되나,

위탁 운영 업체의 보안유지에 대한 신뢰성이 높다면 전문적인 재해복구서비스를 제공받을 수 있으며 초기투자비용이 적게 드는 장점이 있어, 최근 사용이 증가하는 추세에 있다. 미국의 대형금융기관 및 공공기관 등에서 이러한 형태의 사용 예를 볼 수 있다.

이상에서 설명된 재해복구시스템의 유형을 도표로 비교하여 보면 다음과 같다.

<표 4-1> 재해복구시스템의 유형과 특징

구분 기준	유형	설명	구축 비용	운영 비용	보안성	복구 신뢰성
구축 형태별	독자 구축	기관 전용의 재해복구시스템을 독자적으로 구축	높음	높음	높음	높음
	공동 구축	두 개 이상의 기관이 재해복구 시스템을 공동으로 구축	중간	중간	중간	중간
	상호 구축	복수의 기관 또는 단일 기관의 복수의 사이트 상호간 재해복구 시스템의 역할을 수행	낮음	낮음	낮음	낮음
운영 주체별	자체 운영	기관 자체의 인력으로 재해복구 시스템을 운영	-	높음	높음	높음
	공동 운영	두 개 이상의 기관이 재해복구 시스템의 운영인력을 상호 공유	-	중간	기관간 협조에 의존적	기관간 협조에 의존적
	위탁 운영	재해복구시스템의 운영을 민간 IDC 운영자 등 외부의 다른 기관에 위탁	-	낮음	위탁운영자 신뢰도에 의존적	위탁운영자 신뢰도에 의존적

4.2 재해복구시스템 복구수준별 유형

재해복구시스템은 복구수준별 유형에 따라 일반적으로 미러사이트, 핫사이트, 웜사이트, 콜드사이트로 구분된다. 각 유형에 대한 정의는 문헌 및 전문가에 따라 다소의 차이가 있으나, 일반적으로는 다음과 같이 설명할 수 있다.

o 미러사이트(mirror site)
- 주센터와 동일한 수준의 정보기술자원을 원격지에 구축하여 두고 주센터와 재해복구센터 모두 액티브 상태로 (Active-Active) 실시간에 동시서비스를 하는 방식이다(즉, 이론적인 RPO가 0임).
- 재해발생시 복구까지의 소요시간(RTO)은 즉시(이론적으로는 0)이다.
- 초기투자 및 유지보수에 높은 비용이 소요된다.
- 웹 어플리케이션 서비스 등 데이터의 업데이트의 빈도가 높지 않은 시스템에 적용 가능하다.
- 데이터베이스 어플리케이션 등 데이터의 업데이트 빈도가 높은 시스템의 경우 양쪽의 사이트에서 동시에 서비스를 제공하게 하는 것은 시스템의 높은 부하를 초래하여 실용적이지 않으므로, 이러한 경우에는 다음에서 설명하는 핫사이트의 구축이 일반적이다.

o 핫사이트(hot site)
- 주센터와 동일한 수준의 정보기술자원을 대기상태(Standby)로 원격지 사이트에 보유하면서(Active-Standby), 동기적(Synchronous) 또는 비동기적(Asynchronous) 방식의 실시간 미러링(Mirroring)을 통하여 데이터를 최신의 상태(Up-to-date)로 유지하고 있다가(즉, RPO≒0을 지향함), 주센터 재해시 재해복구센터의 정보시스템을 액티브로 전환하여 서비스하는 방식이다.
- 일반적으로, 데이터 실시간 미러링을 이용한 핫사이트를 미러사이트라고 일컫기도 한다.
- 재해발생시 복구까지의 소요시간(RTO)은 수시간(약 4시간이내)이다.
- 초기투자 및 유지보수에 높은 비용이 소요된다.
- 데이터베이스 어플리케이션 등 데이터의 업데이트 빈도가 높은 시스템의 경우, 재해복구센터는 대기상태(Standby)로 유지하다가 재해시 액티브(Active)로 전환하는 방식이 일반적이다.

o 웜사이트(warm site)
- 핫사이트와 유사하나, 재해복구센터에 주센터와 동일한 수준의 정보기술자원을 보유하는 대신, 중요성이 높은 정보기술자원만 부분적으로 재해복구센터에 보유하는 방식이다.

- 실시간 미러링을 수행하지 않으며, 데이터의 백업 주기가 수시간~1일 정도로 핫사이트에 비해 다소 길다(즉, RPO가 약 수시간~1일).
- 재해발생시 복구까지의 소요시간(RTO)은 수일~수주이다.
- 구축 및 유지비용이 미러사이트 및 핫사이트에 비해 저렴하나, 초기의 복구수준이 완전하지 않으며, 완전한 복구까지는 다소의 시일이 소요된다.

o 콜드사이트(cold site)
- 데이터만 원격지에 보관하고, 이의 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보하고 있다가, 재해시에 데이터를 근간으로 하여 필요한 정보자원을 조달하여 정보시스템의 복구를 개시하는 방식이다.
- 주센터의 데이터는 주기적(수일~수주)으로 원격지에 백업된다(즉, RPO가 수일~수주).
- 재해발생시 복구까지의 소요시간(RTO)은 수주~수개월이다.
- 구축 및 유지비용이 가장 저렴하나, 복구소요시간이 매우 길고, 복구의 신뢰성이 낮다.

<표 4-2>는 재해복구시스템의 복구수준별 유형을 비교하여 나타내었다.

<표 4-2> 재해복구시스템의 복구수준별 유형 비교

유형	설 명	복구소요시간 (RTO)	장점	단점
Mirror Site	- 주센터와 동일한 수준의 정보기술자원을 원격지에 구축, Active-Active 상태로 실시간 동시 서비스 제공	즉시	- 데이터 최신성 - 높은 안정성 - 신속한 업무재개	- 높은 초기투자비용 - 높은 유지보수비용 - 데이터의 업데이트가 많은 경우에는 과부하를 초래하여 부적합
Hot Site (Data Mirroring Site)	- 주센터와 동일한 수준의 정보기술자원을 원격지에 구축하여 Standby상태로 유지 (Active-Standby) - 주센터 재해시 원격지시스템을 Active 상태로 전환하여 서비스 제공 - 데이터는 동기적 또는 비동기적 방식의 실시간 미러링을 통하여 최신상태로 유지 - 일반적으로는 실시간 미러링을 사용하는 핫사이트를 미러사이트라 일컫기도 함	수시간 (4시간) 이내	- 데이터 최신성 - 높은 안정성 - 신속한 업무재개 - 데이터의 업데이트가 많은 경우에 적합	- 높은 초기투자비용 - 높은 유지보수비용
Warm Site	- 중요성이 높은 정보기술자원만 부분적으로 재해복구센터에 보유 - 데이터는 주기적(약 수시간~1일)으로 백업	수일 ~ 수주	- 구축 및 유지비용이 핫사이트에 비해 저렴	- 데이터 다소의 손실 발생 - 초기복구수준이 부분적임 - 복구소요시간이 비교적 긺
Cold Site	- 데이터만 원격지에 보관하고, 이의 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보 - 재해시 데이터를 근간으로 필요한 정보자원을 조달하여 정보시스템의 복구 개시 - 주센터의 데이터는 주기적(수일~수주)으로 원격지에 백업	수주 ~ 수개월	- 구축 및 유지비용이 가장 저렴	- 데이터의 손실 발생 - 복구에 매우 긴 시간이 소요됨 - 복구 신뢰성이 낮음

정보시스템이 기업 및 공공부문의 핵심적 인프라로 인식되고 있으며, 전자상거래와 전자정부 등의 활성화로 기관의 핵심업무가 온라인화 되고 24시간 365일 상시 가용성이 요구되는 추세로 인하여, 최근에는 핫사이트 및 미러사이트 방식의 재해복구시스템이 증가하고 있는 추세이다(이광영, Contingency Planning을 위한 사이트 백업 솔루션, 2000).

4.3 재해복구시스템 구현 기술

4.2절에서 기술한 재해복구시스템의 방식 중, 콜드사이트 방식은 시스템 운영 중에 주기적으로 백업한 데이터를 원격지에 소산 보관하는 방식으로서, 본 지침에서는 설명을 생략한다. 핫사이트 이상 수준의 재해복구시스템을 구성하는 방법은 다음과 같이 분류할 수 있다.

□ 데이터 복제 방식
- o H/W적 복제방식
  - 물리 저장장치 수준 : 디스크 장치를 이용한 복제
- o S/W적 복제방식
  - 운영체제 수준 : 데이터 복제 전용 솔루션을 이용한 복제
  - DBMS 수준 : DBMS를 이용한 복제

□ 데이터 전송 방식
- o Sync. (동기 복제)
- o Async. (비동기 복제)
- o 기타 방식

위의 방식 중 어느 것을 선택하는지의 결정은 복구 수준, 즉 복구 목표 시간/시점 및 비용 등에 따라 이루어지게 된다. 그러므로 각각의 복제 방식의 원리 및 장단점을 명확히 이해하여 구축하려는 재해복구시스템에 적합하게 선택하여야 한다.

4.3.1 데이터 복제 방식

재해복구를 위해서는 데이터를 복제하여 원격지에 보내야 한다. 쉽게 생각하면 사용 중인 자료의 내용을 텍스트 형태로 전송하면 될 것으로 생각할 수 있으나, 실제로는 재해복구시스템을 구축하려는 시스템은 여러 사용자가 공동으로 사용하는 것이고 이와 관련한 정보시스템의 복잡성을 감안하면 문제가 복잡함을 알 수 있다. 따라서 복제된 결과는 원본과 동일한 자료의 내용이나 이를 복제하는 방법은 여러 가지가 있다.

본 절에서는 다음과 같이 세가지 분류로 데이터를 복제하는 방식에 대해 설명한다.

가. H/W적 복제 방식

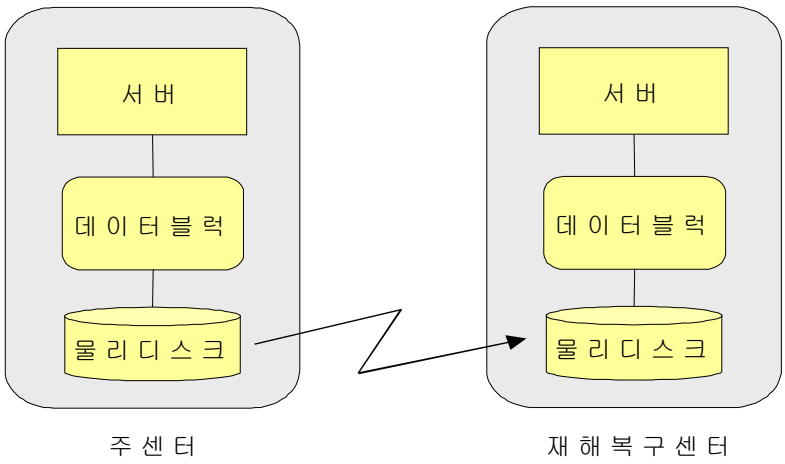
□ 디스크 장치를 이용한 복제

자료는 여러 가지 어플리케이션, DBMS 혹은 툴 등을 사용하더라도 최종적으로는 디스크에 저장되는 것이 일반적이다(메모리 DBMS와 같은 특수한 경우는 제외한다). 그러므로 자료가 최종적으로 저장되는 디스크를 복제 대상으로 하여, 사용중인 원본 디스크를 원거리 지역의 복구용 디스크로 복제하는 방식이 바로 디스크 수준의 복제 방식이다. 또한 디스크 장치를 이용한 복제 방식에서는, 디스크의 복제 작업에 사용되는 자원(CPU, Memory 등)은 서비스를 수행 중인 서버가 아닌 디스크 자체의 자원(CPU, Cache 등)을 사용하므로, 서버의 부하를 최소화한다.

디스크 장치를 이용한 복제 방식의 특징은 다음과 같다.

- 주센터의 원본 디스크와 재해복구센터의 복구용 디스크는 기본적으로 마이크로코드(Microcode)[2] 수준에서 완벽한 호환성을 제공하여야 한다.
- 그러나, 디스크에 별도의 가상화 솔루션 등을 활용한다면 이기종 디스크 간에도 복제가 가능하다.
- 디스크 복제 솔루션은 디스크 내부의 자원을 사용하여 동작하므로 재해복구시스템 구축시 복제를 위한 디스크 자원의 증설을 검토하여야 한다.
- 디스크 장치를 이용한 복제방식의 구성시, 최초에는 디스크 전체를 대상으로 복제작업을 수행하므로 많은 시간이 소요되나, 이후 운영시에는 디스크의 변경분만을 복제하므로, 고속의 복제가 가능하다.
- 일반적으로 대용량 고(高) 성능의 디스크를 사용하는 운영 환경에서 재해복구시스템을 구축하는 경우에 주로 사용된다.

2) Microcode : 디스크 컨트롤러상의 ROM에서 수행되는 펌웨어(Firmware) 코드로서, 하드웨어의 동작을 통제하는 기본 프로그램



(그림 4-2) 디스크 장치를 이용한 복제

나. S/W적 복제 방식

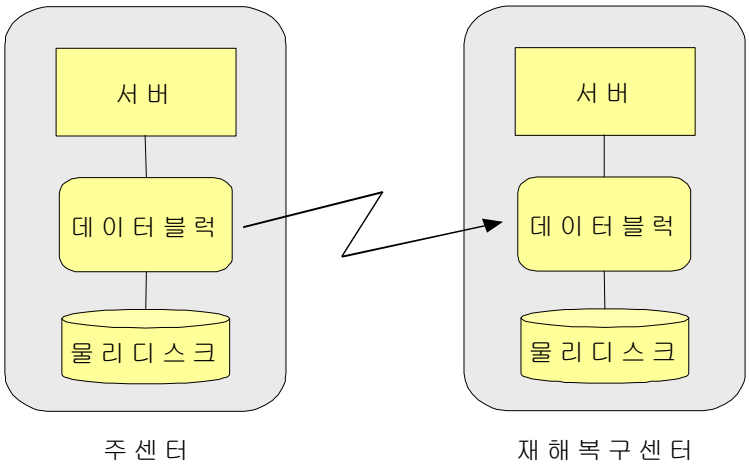
□ 운영체제 수준의 데이터 복제 전용 솔루션을 이용한 복제

데이터를 디스크에 저장, 관리하기 위한 논리적인 볼륨을 만들어 사용한다. 즉, 데이터는 논리적 볼륨에서 관리, 전송되어 이것이 물리적 디스크에 저장되는 것이다. 앞서의 항목에서 설명한 디스크 수준 복제 방식이 디스크에 저장되는 데이터를 주센터의 디스크에서 재해복구센터의 디스크로 복제하는 것인 반면, 운영체제를 이용한 복제 방식은 서버에서 디스크로 데이터를 전송하고 저장하는 중간 단계에서 데이터 블록을 복제하여 재해복구센터로 보내는 방식이다. 따라서 운영체제를 이용한 복제 방식에서는 주센터와 재해복구센터의 양쪽 서버에 데이터의 복제를 관리하기 위한 동일한 복제솔루션을 설치하여야 한다. 이 때, 원격지로의 복제 작업은 해당 서버 자체에서 직접 수행하거나, 별도의 관리용 서버에서 수행된다.

운영체제 수준의 데이터 복제 전용 솔루션을 이용한 복제 방식의 특징은 다음과 같다.

- 원본 디스크와 복구용 디스크가 이기종이어도 가능하다. 이 때, 양 쪽에 설치된 복제 솔루션은 동일하여야 한다.
- 복제솔루션은 해당 서버 자체에서 수행되거나, 별도의 디스크 관리 서버 자원을 사용하여 수행될 수 있다. 그러므로 재해복구시스템 구축시 기존의 운영환경의 용량 및 부하를 감안하여 서버 자원의 적정성을 검토하여야 한다.

- 데이터 블록을 기본 단위로 하여 데이터의 변경분을 복제한다.
- 일반적으로 중간 정도의 성능과 용량의 디스크를 사용하거나, 이기종 디스크를 사용하는 운영환경에서 재해복구시스템을 구축하는 경우에 주로 사용된다.



(그림 4-3) 데이터 복제 전용 솔루션을 이용한 복제

□ DBMS를 이용한 복제

업무의 수행에 요구되는 데이터의 효율적 관리를 위하여 DBMS(Data Base Management System)가 널리 사용된다. DBMS를 이용한 복제 방식은 주센터의 DBMS에서 사용되는 SQL(Structured Query Language)문 혹은 변경 로그를 원격 사이트의 DBMS에 전송하여 복제하는 방식이다. 위에서 언급한 디스크 및 운영체제 수준의 복제방식 역시 대부분 DBMS 운영환경에서의 재해복구시스템 구축을 지원하고 있으나, 이 경우 데이터의 일관성(consistency)을 보장하는지의 여부를 확인하여야 한다.

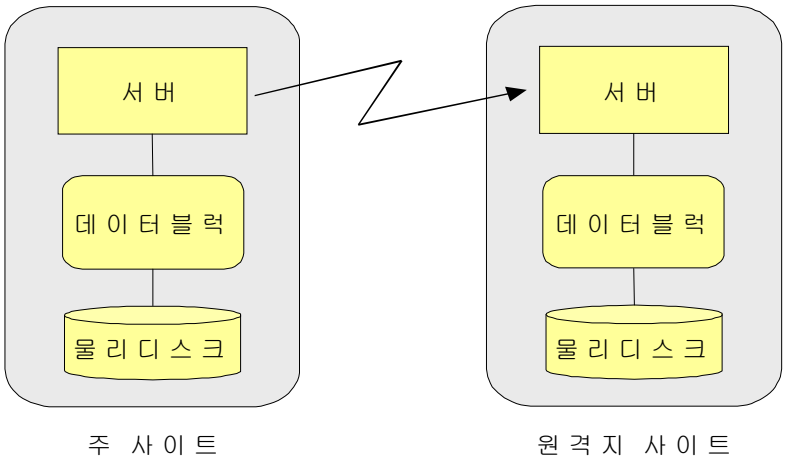
따라서 DBMS를 이용한 복제 솔루션을 사용하는 경우 복제 솔루션이 동일하다면 주센터와 재해복구센터의 디스크 종류, 논리적 볼륨 매니저, 플랫폼의 종류에 관계없이 재해복구시스템을 구축할 수 있다.

DB관리 시스템을 이용한 복제 방식은 주센터 및 재해복구센터의 서버 자원(CPU, Memory 등)을 사용한다. 따라서 DBMS를 이용한 복제 방식을 적용하는 경우에는 서버의 자원이 충분한지 검토하여야 한다.

DBMS를 이용한 복제 방식의 특징은 다음과 같다.

- 주센터와 재해복구센터의 DBMS 및 복제 솔루션이 동일하여야 한다. 디스크, 논리적 볼륨 및 플랫폼의 종류가 다르더라도 구현 가능하다.

- DBMS를 이용한 복제 솔루션은 주센터와 재해복구센터 서버의 자원을 사용하여 동작하므로 서버 자원의 증설을 검토하여야 한다.
- DBMS에서 변경을 위한 SQL 혹은 변경 기록을 이용하여 복제 한다.
- 일반적으로 이기종 디스크를 사용하고 DBMS 중심의 재해복구 시스템을 구축할 때 사용한다.
- 주센터와 재해복구센터 양쪽 모두에서 DBMS가 수행되고 있어야 한다. 이 경우, 구현 솔루션에 따라 양쪽 모두 Read/Write가 가능하게 하거나, 한 쪽에서만 Read/Write가 가능하고 다른 한 쪽에서는 Read Only인 방식의 구현이 가능한데, 전자의 경우 서비스의 지연을 초래할 수 있다.



(그림 4-4) DBMS를 이용한 복제

<표 4-3> 데이터 복제방식에 따른 특징

	디스크장치 이용 복제	운영체제 이용복제	DBMS이용 복제
복제 대상	디스크 변경분	데이터 블록	SQL문 혹은 변경 로그
구성 조건	동일한 디스크 사용	동일한 논리볼륨 수준 복제 솔루션 사용	동일한 DBMS 사용
복제시 소요 자원	디스크 자체 자원	해당서버자체 혹은 별도의 관리서버 자원	DBMS 서버 자원
사례	ContinuousAccess, SRDF, TrueCopy 등	HAGEO, IpStor, TDMF, VVR 등	DataGuard(Oracle), Replication(SyBase), RRDF(DB2), SharePlex, ER 등

4.3.2 데이터 전송 방식

재해복구시스템 구축 시 재해복구의 수준 즉, 얼마만큼 빨리 완벽하게 복구하는지, 기존의 운영 시스템에 영향을 주지 않고 재해복구시스템을 구축하는지, 어느 정도의 예산으로 재해복구시스템을 구축하는지가 주요한 관점이다. 4.3.1절에서 소개한 데이터 복제 방식 역시 이러한 여러 요소들을 고려하여 결정하여야 할 것이다. 하지만 이러한 복제 방식 외에 본 절에서 소개할 데이터 전송 방식 역시, 위에서 언급한 선택 기준에 커다란 영향을 준다. 따라서 데이터 복제 방식과 전송 방식을 알맞게 혼합하여 현 시스템과 재해복구 수준에 최적화된 재해복구시스템을 구축하는 것이 중요하다.

참고로, 다음에서 설명되는 Sync 방식이나 Async 방식 등의 데이터 복제방식 중 어느 방식을 사용하더라도, 재해복구시스템은 지속적으로 주센터의 운영시스템 데이터를 복제하게 된다. 따라서 주센터 운영시스템에서의 실수나 오류로 인한 잘못된 데이터의 추가 및 변경도 재해복구센터에 동일하게 복제되므로, 주센터의 논리적 데이터 오류에 의한 장애시 원격지에서도 동일한 장애가 발생하게 된다. 따라서 재해복구시스템만 구축되면 모든 장애와 재해를 막을 수 있다는 생각은 잘못된 것이다.

가. Sync 방식

우선 Sync 방식은 어떠한 상황에서도 완벽한 데이터 복구를 보장하여 준다. 이 방식은 사용자 혹은 작업이 주센터의 운영 시스템에서 데이터를 추가 혹은 변경하였을 경우 주센터뿐 아니라 재해복구센터에서도 정상적으로 추가 혹은 변경이 완료 되었다는 것을 시스템에서 확인한 후에 사용자 혹은 작업에게 추가 혹은 변경 완료 신호를 보내게 되는 방식이다. 예로 사용자가 새로운 데이터를 입력하는 작업을 한다면 기존과 같이 주센터에서 기록되는 것 외에도 재해복구센터에 새로운 데이터의 기록이 완료 될 때까지 사용자는 대기 혹은 진행 상태로 있게 된다. 주센터와 재해복구센터에 모두 정상적으로 기록이 완료되면 운영 시스템에서 이를 확인한 후 사용자에게 정상적으로 데이터 입력이 완료 되었다는 결과를 보여주게 된다.

따라서, Sync방식은 다음과 같은 특징이 있다.

- 어떤 경우라도 주센터와 재해복구센터간의 데이터 정합성은 항상 유지되므로 가장 안전하고 신뢰성이 높은 방식이다.
- 그러나, 주센터와 재해복구센터 간을 연결하는 고속의 회선이 필요하다. 왜냐하면 주센터 뿐 아니라 재해복구센터에 있는 데이터 역시 빠른 시간 내에 추가, 변경하여야 응답속도의 지연을 막아 기존의 서비스 수준을 유지할 수 있기 때문이다. 결국 이러한 요구는 고속회선을 위한 많은 회선 비용과 주센터와 재해복구센터간의 거리 제한을 가져올 수 있다.

- 또한 주센터와 재해복구센터간의 회선 장애 혹은 재해복구시스템의 장애 및 운영 실수는 즉시 주센터의 운영 시스템에도 영향을 미치어 서비스 장애로 이어질 수 있다. 따라서 재해복구시스템 유지 관리의 어려움과 운영수준 유지를 위한 인력, 비용이 추가로 발생하게 된다.

나. Async 방식

Async 방식의 가장 큰 특징은 Sync 방식과 달리 재해복구시스템을 구축하여 데이터를 복제하더라도 기존 운영 서비스의 성능에 거의 영향을 주지 않는다는 것이다. 재해복구시스템을 Async 방식으로 구축하면 기존 운영 서비스는 기존과 동일하게 동작하고, 데이터 복제는 기존 운영 시스템의 서비스와는 별도로 디스크, 서버 및 DBMS수준의 전송방식에 따라 운영 서비스 이후 독립적으로 동작된다. 즉, 데이터 복제를 수행하기는 하나 그것이 언제 수행되는지는 재해복구를 위한 시스템의 환경 및 여러 조건에 따라 정하여 진다.

Async 방식의 특징은 다음과 같다.

- Sync 방식에 비해 현 시점에서 운영시스템의 100% 데이터 복제를 보장하지는 못한다. 그러나, 최대한 보장을 위해 “Do Best” 하는 방식이며, 따라서 잃어버린 데이터에 대한 대비책을 별도로 마련하여야 한다.

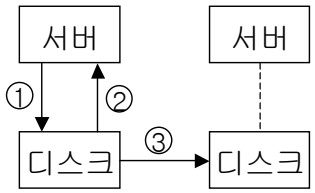
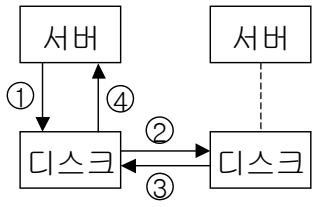
- 그러나, 100% 데이터를 복제 못 하였다 하더라도 특정시점의 데이터의 정합성은 완벽히 보장한다. 이는 DBMS의 경우 정상 가동을 보장하는 중요한 특성이다.
- 기존 운영 서비스의 성능에 거의 영향을 주지 않으면서 재해복구시스템을 구축할 수 있어 디스크, 서버 및 DBMS 수준의 복제방식에 일반적으로 사용된다.
- 적절한 대역폭의 회선이 주센터와 재해복구센터에 존재하면 기존 운영시스템의 서비스와 재해복구시스템을 구축할 수 있으므로 Sync 방식에 비하여 회선비용이 저렴하며, 이에 따라 거리 측면에서도 주센터와 보다 멀리 떨어져 있는 재해복구센터에 재해복구시스템을 구축할 수 있는 장점이 있다.

다. 기타 방식

앞에서 설명한 Sync와 Async 방식 이외에도, 두 가지 방식을 혼용한 다양한 형태의 복제 방식이 존재한다. 이러한 방식들은 Async 방식과 유사하여 기존 서비스 성능에 영향을 거의 주지 않고 재해복구시스템을 구축할 수 있으나 주센터에서의 일정 시점 변경 데이터에 대한 정합성을 재해복구센터에서 보장하여 주지 못하는

경우도 있으므로 확인이 필요하다. 예로서 Async방식의 경우 주센터의 현 시점의 데이터를 100% 데이터 복제 못하는 경우는 있으나 특정 시점의 데이터에 대한 정합성은 100% 완벽히 보장함으로 DBMS 운영 시스템의 경우도 사용이 가능하다. (이는 Async방식이 시간변경에 따른 데이터 변경을 그룹화 하거나 일정 시점 별로 변경분에 대해 정합성을 유지하는 방법을 사용하기 때문이다.) 그러나 일부 기타 방식의 경우는 이러한 시간 기준 없이 순차적 데이터 전송으로 특정 시점의 데이터 정합성 보증을 할 수 없는 경우도 있어 파일 데이터(메일, 이미지 등)의 경우 파일 시스템이 제공하는 자체적인 정합성 제공 방법에 의해서만이 부분적으로 복구가 가능하다. 따라서 DBMS를 사용하는 운영환경의 경우는 데이터의 정합성을 완벽히 보장하지 못할 수 있으므로 기타 방식의 사용이 권장되지 않으며 파일 시스템인 경우 제한적으로 사용되어 질 수 있다.

<표 4-4> 데이터 전송방식

	비동기 방식(Async)	동기 방식(Sync)
데이터 처리경로		
설 명	1. 주센터 CPU는 디스크 내 특정 자료를 변경하고 작업 처리를 종료함(①,②) 2. 주센터 디스크는 변경된 자료에 대해 처리시간을 기록(Time Stamp) 혹은 변경된 기록을 일정 간격으로 재해복구센터 디스크로 전송하여 복제함(③)	1. 주센터 디스크내 특성자료가 변경되면, 같은 데이터가 재해복구센터의 디스크로 즉시 전송되어 복제됨(①,②) 2. 정상적으로 복제가 완료되면 같은 결과가 주센터 디스크로 전송되고, 이를 주센터의 CPU가 확인하여야 복제 과정이 종료됨(③,④)
장점	·재해복구센터로의 데이터 복제와 무관하게 시스템에 Write 동작의 완료 신호를 보내므로 온라인 업무 수행에 최소한의 영향을 줌 ·주센터에서 재해복구센터로 데이터 복제시 일정시점을 기준으로 데이터의 정합성을 보장(데이터 발생시간 일치)	·재해시 데이터 보존성이 가장 뛰어남
단점	·많은 부하를 주는 배치작업 혹은 주센터와 재해복구센터간의 하드웨어 용량부족 시 일부 데이터의 손실	·재해복구센터로의 데이터 복제를 확인 후 다음 트랜잭션의 수행이 가능함으로 온라인 응답 및 배치작업 수행 시간에 많은 영향을 줌

4.4 재해복구시스템용 네트워크 종류

재해복구시스템을 위한 네트워크는 용도에 따라 크게 평상시의 데이터 복제를 위한 데이터 복제 네트워크와 재해시 서비스를 위한 재해복구 서비스 네트워크로 나누어 볼 수 있다. 하지만 근래에 들어 IP기반의 데이터 복제가 가능하여짐에 따라 별도로 용도를 구분하지 않고 데이터 복제 네트워크와 재해복구 서비스 네트워크를 동시에 사용함으로써 네트워크 사용 효율을 높이고 관리 비용을 줄이는 방안이 대두되고 있다. 하지만 이 역시 기술의 발달과 더불어 현재 진행되고 있는 상태이며 절대적이지 못하다. 따라서 재해복구시스템을 구축하는 데 주어진 각각의 상황과 조건(데이터 복제 압축효율, 네트워크 비용, 재해 발생시 서비스 사용 지역 등) 에 맞추어 최적의 방안을 설계하여야 한다.

가. 데이터 복제 네트워크

데이터 복제 네트워크는 주센터와 재해복구센터 사이의 거리, Sync/Async 등의 복제 방식 등에 의해서 결정된다.
가까운 거리는 ESCON 혹은 Fiber Channel을 직접 연결 할 수 있으나 이는 거리의 제한으로 재해복구시스템으로 의미가 없고 주로 동일 건물 내의 가까운 거리에서 장애를 대비한 장애복구용 시스템으로 많이 사용된다. 따라서, 원거리의 데이터 복제가 가능하려면 대부분의 경우 ATM 및 Fiber 기반의 DWDM 네트워크 장비를 사용하여 재해복구시스템을 위한 데이터 복제 네트워크를 구성한다.
데이터 복제 네트워크의 대역폭은 얼마나 많은 양의 데이터를 빠른 시간 내에 전송할 수 있는지를 결정하며, DWDM 또는 ATM 등의 여러 가지 네트워크 유형에 대하여 다양한 대역폭의 할당이 가능하다.

나. 재해복구 서비스 네트워크

재해복구 서비스 네트워크는 재해 발생 시 주센터에서 수행하던 서비스를 일정거리 이상의 재해복구센터에서 동일 혹은 일정 수준으로 수행할 수 있도록 하기 위한 온라인 서비스용 네트워크로서, 주센터의 네트워크 구성에 따라 재해복구센터의 네트워크 구성을 설계하여야 한다. 예를 들어, 주센터가 여러 개의 지역 서비스 센터와의 전용선 연결을 가지고 있었다면, 재해복구센터에도 재해 시 이들 지역 서비스 센터와 서비스 재개를 위한 네트워크 연결이 빠른 시간 내에 획득될 수 있어야 한다.
여기서, 재해 시 빠른 네트워크 확보를 위해서는, 평상시 재해복구용 원격지 사이트에서 운영 서비스가 이루어지고 있지 않더라도 재해복구용 네트워크에 네트워크 경로(route)를 사전 설정해 두고 일정한 여유용량을 확보하는 등 별도의

대책이 있어야 한다. 이에 따라 상당한 수준의 통신비용이 지속적으로 발생하게 됨으로, 네트워크 사업자가 이러한 용도의 서비스를 별도로 제공하는지의 여부를 확인하고 재해복구 네트워크의 평상시 유지와 관련한 비용에 대한 고려가 반드시 이루어져야만 한다.

5. 재해복구 전략 수립

5.1 업무영향분석

재해복구를 위한 전략 수립을 위해서는 업무영향분석(BIA : Business Impact Analysis)이 수행되어야 한다. 업무영향분석은 다음과 같은 목적을 가진다.

- 주요 업무 프로세스의 식별
- 재해 유형 식별 및 재해 발생 가능성과 발생시 업무 중단의 지속시간 평가
- 업무 프로세스별의 중요도 및 재해로 인한 업무 중단시의 손실 평가
- 업무 프로세스별의 우선순위 및 복구대상범위의 설정
- 재해 발생시의 업무 프로세스의 복원 시간이나 우선순위 결정

업무영향분석의 결과로 다음과 같은 사항을 도출할 수 있다.

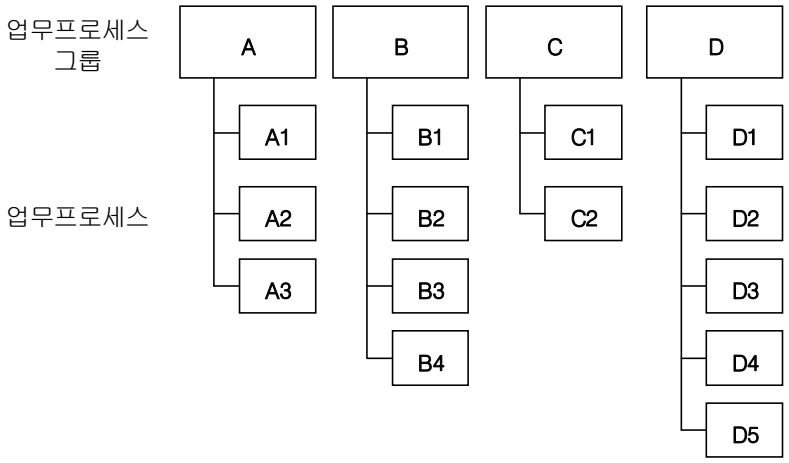
- 주요 업무 프로세스
- 재해 유형별 발생 가능성 및 재해 영향의 지속시간
- 재해시 업무 프로세스의 중단에 따른 손실 정도
- 업무 중요성 우선순위 및 복구대상 업무범위
- 주요 업무 프로세스별 복구목표시간(RTO : Recovery Time Objective) 및 복구목표시점(RPO : Recovery Point Objective)

5.1.1 주요 업무 프로세스의 식별

조직의 주요 업무 프로세스를 파악하는 단계이다.

□ 업무 프로세스의 계층적 식별

업무 프로세스는 계층적으로 파악되어 나타내는 것이 일반적이다. 즉, 최상위의 업무 프로세스 그룹으로부터 업무 프로세스, 서브프로세스 등으로 이루어지는 계층적 업무 프로세스 구성도를 통해 조직의 전체 업무 프로세스의 구조를 파악할 수 있다.
계층적 업무 프로세스 구성도는 여러 가지의 유형이 있으나, 예를 들어 (그림 5-1)과 같은 형태로 나타낼 수 있다.



(그림 5-1) 계층적 업무 프로세스 구성도의 예

□ 주요 업무 프로세스의 식별

식별된 업무 프로세스 중에서 핵심적이고 빈번하게 사용되는 주요 업무 프로세스를 업무영향분석의 대상으로 하는데, 이를 위해서는 다음과 같은 사항을 고려하여야 한다.

- 조직의 핵심적 고객서비스에 직결된 업무 프로세스
- 조직 전략 측면에서의 중요 업무 프로세스의 인식

□ 업무 프로세스간의 상호연관성 분석

업무 프로세스의 중요성은 개별 업무 프로세스의 중요성에 기인할 뿐 아니라 특정 업무 프로세스와 다른 업무 프로세스 사이의 연관성에도 영향을 받게 된다.
업무 프로세스간 상호연관성은 다음과 같은 유형으로 나타난다.

o 선후관계

특정 업무 프로세스가 다른 업무 프로세스보다 먼저 수행되어야만 하는 경우, 두 업무 프로세스는 선후관계에 있다. 이 때, 후행 프로세스의 수행을 위해서는 선행 프로세스가 반드시 수행되어야만 하므로, 선행 프로세스의 중단시 후행 프로세스의 수행 중단이 불가피하게 된다. 따라서, 선후관계에 있는 프로세스의 경우, 후행 프로세스가 선행 프로세스에 의존한다고 말할 수 있다.

o 참조관계

특정 업무 프로세스의 수행을 위해 다른 업무 프로세스의 수행 결과를 참조해야만 하는 경우, 두 프로세스는 참조관계에 있다. 이 때, 참조되는 프로세스의 수행이 중단되는 경우, 참조하는 프로세스의 수행도 이루어질 수 없게 된다. 따라서, 참조하는 프로세스는 참조되는 프로세스에 의존한다고 말할 수 있다.

상기의 두 가지 연관관계에 입각하여 업무 프로세스간의 연관성을 분석하여야 한다. (그림 5-2)는 업무 프로세스간의 의존관계를 통하여 연관성을 분석한 도표의 예이다.

업무 Dependency

1)선행업무 참조되는 업무 / 2)후행업무 참조하는 업무	A1	A2	A3	B1	B2	B3	C1	C2	C3	상관도
A1		●	●				●	●	●	5
A2										0
A3	●									1
B1	●		●							2
B2		●		●		●				3
B3										0
C1	●		●							2
C2				●						1
C3										0
상관도	3	2	3	2	0	1	1	1	1	

1) 해당업무가 처리되기 위해 선행되어야 하는 업무
2) 해당업무 처리 후 처리되어야 하는 업무

(범례) ● : 관계 있음
A1,A2...B1..: 프로세스

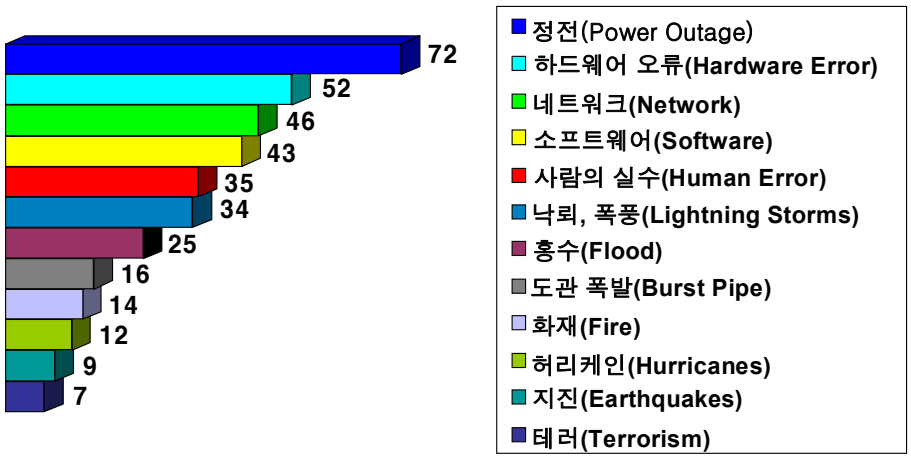
(그림 5-2) 업무 프로세스간 상관도 분석(예시)

5.1.2 재해 유형별 발생 가능성

일반적인 재해 발생의 원인은 다음과 같다.

- 지진, 태풍
- 화재(사고 또는 방화)
- 홍수/산사태, 지반침하
- 정전
- 통신장애
- 장비고장

재해 발생 원인의 상대적 빈도는 다음 (그림 5-3)과 같이 나타난다. (그림 5-3)은 재해발생일수를 1년으로 환산하였을 때 재해원인별 발생일수를 나타낸 것이다.

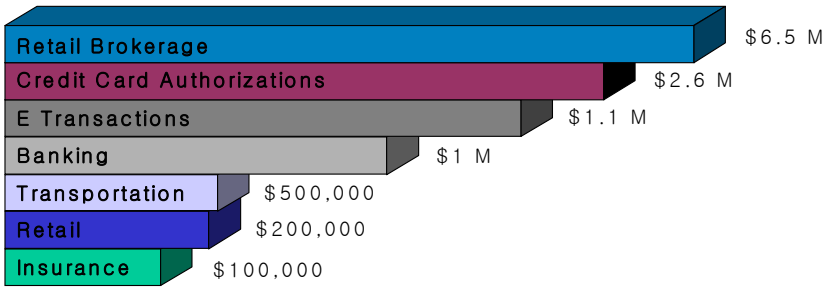


Source: Contingency Planning Research & Disaster Recovery Journal

(그림 5-3) 재해의 상대적 발생 빈도

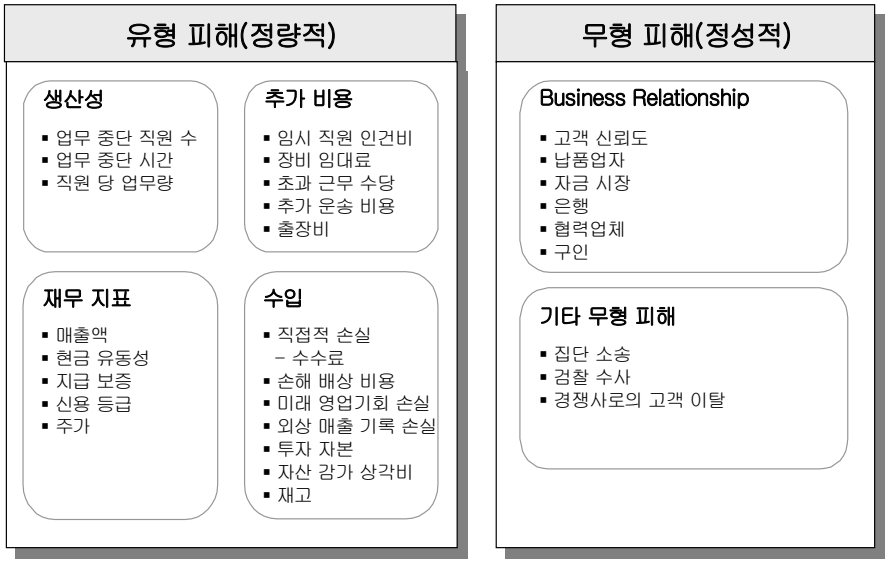
5.1.3 재해시 업무 프로세스의 중단에 따른 손실 평가

재해시 업무 프로세스의 중단에 따른 손실은 일반적으로 고객 서비스와 직결된 프로세스에서 가장 높게 나타난다. 내부 업무 수행에 관련된 프로세스는 고객 서비스 프로세스에 비해서는 중단시의 손실이 적으나, 내부 업무 프로세스 중에서도 타 프로세스와의 연계성이 높은 프로세스일수록 중단시 손실은 높아진다. (그림 5-4)는 업종별로 업무 프로세스의 중단에 따른 손실 평가액을 나타낸 예이다.



(그림 5-4) 업종별 프로세스 중단에 따른 손실액

재해로 인한 고객의 피해는 매출액과 같이 수치화 할 수 있는 유형의 피해와 기업의 이미지와 같이 수치화할 수 없지만 중요한 무형의 피해가 있다. (그림 5-5)는 유형/무형 피해의 예시를 보여준다.



(그림 5-5) 피해의 유형

손실 평가는 유형의 피해에 대해서는 정량적 방법으로, 무형의 피해에 대해서는 정성적 방법으로 평가할 수 있다. 정량적 평가는 일반적으로 고객서비스 중단에 따른 단위시간당 손실규모를 판단하여 이루어진다. 또한 정량적 평가는 기록 유실등에 의한 이유로 매출 및 수입 감소등의 재무적 영향과 업무처리 지연에 따른 업무 영향으로 구분할 수 있다. 파급 영향 추정면에서는 재무적 영향은 시간 증가에 의한 화폐가치를 업무 영향은 해당 관련 업무 처리를 위한 시간 증가분을 파악해야 한다.

정성적 평가는 손실등급을 상/중/하로 평가하거나 프로세스간 연계성 매트릭스를

활용하여 연계관계의 개수가 많은 프로세스를 중요 프로세스로 판별하는 등의 방법을 사용할 수 있다. 또한 정성적 평가는 유형(tangible)의 영향과 무형(intangible)의 영향으로 구분된다. 유형의 영향으로는 고객이탈, 고객 손해배상, 데이터 유실등이 있으며, 무형의 영향으로는 대외 이미지 실추, 신인도 하락, 감독기관 제재등이 있다. 아래는 정량/정성적 평가를 하기 위한 측정요소의 예이다.

<table>
<tr><th colspan="2" rowspan="3">구분</th><th rowspan="3">영향(Impact) 항목</th><th colspan="6">파급 영향 추정</th></tr>
<tr><th colspan="6">서비스중단 기간별 영향의 크기</th></tr>
<tr><th>1Hr</th><th>5Hr</th><th>1일</th><th>5일</th><th>1주</th><th>1달</th></tr>
<tr><td rowspan="2">정량적</td><td>재무적 영향</td><td>– 매출 감소
– 수입 감소</td><td colspan="6">화폐가치 파악</td></tr>
<tr><td>업무 영향</td><td>– 업무처리 지연
• 업무처리 단계 증가
• 단위 업무당 처리시간 증가</td><td colspan="6">시간 증가분 파악</td></tr>
<tr><td rowspan="2">정성적</td><td>유형</td><td>– 고객이탈, 미래 영업기회 손실
– 고객 손해배상 가능성, 집단 소송
– 연관된 업무 지연
– 데이터 유실(자료 복구 불가)</td><td colspan="6">양적 파악</td></tr>
<tr><td>무형</td><td>– 대외이미지 실추 및 신임도 하락
– 감독기관제재 및 검찰 수사
– 기타 손실</td><td colspan="6">가능성 파악</td></tr>
</table>

(그림 5-6) 정량/정성적 영향도 분석(예시)

5.1.4 업무 중요성 우선순위 및 복구대상 업무범위 설정

5.1.3절에서 설명한 단위 업무별 정성적/정량적 분석결과를 바탕으로 우선순위를 부여한다. 단위 업무별로 우선순위를 부여하기 위해서는 업무 연관성 분석 결과를 적용해야만 한다. 예를 들어 정성적/정량적 업무평가 결과에 의해 복구를 위한 우선순위 업무가 (그림 5-7)과 같이 분류되었다고 가정해 보자.

Impact 분석을 통한 업무복구 우선순위	
1순 위	A1, B2
2순 위	A2, A3, B3, C2, C3
3순 위	B1, C1

(그림 5-7) 업무 우선순위 설정(예시)

정성적/정량적 평가에서는 개별 업무에 대한 중요성에 대한 내용은 있으나 각 업무별 연관성에 대해서는 기술이 되어 있지 않다. 예를 들어 (그림 5-7)의 1순위 업무만을 우선 복구 시킨다고 해서 해당 업무 전체를 재개할 수 없다는 것이다. 왜냐하면, 예를 들어 A1 업무의 경우 (그림 5-2)의 상관도 분석에서 보듯이, A2, A3를 선행업무로 가지므로 A2, A3 업무가 재개되지 않는 한, A1 업무의 수행이 불가능하게 되는 것이다. 따라서, 해당 업무에 대한 선행 업무도 함께 우선순위에 포함시켜 복구 시켜야 하므로, 업무의 상관관계 분석 결과를 적용하는 것이 필수적이다.

(그림 5-7)의 예에서는 (그림 5-2)의 업무 연관성 분석 결과를 적용하는 것으로 가정한다. (그림 5-2)의 업무 상관도에서는 계수(상관도)가 높을수록 다른 업무와 밀접한 관계를 이루고 있다는 것을 의미하며, 이는 다른 업무와 밀접한 관계를 이루고 있어서 기본업무 또는 공통업무라 볼 수 있다. 이러한 업무상관도 조사결과를 근거로 우선순위를 부여한다면 (그림 5-8)과 같이 업무복구의 우선순위가 바뀔 수 있다.

Impact 분석을 통한 업무복구 우선순위	
1순위	A1, B2
2순위	A2,A3,B3,C2,C3
3순위	B1,C1

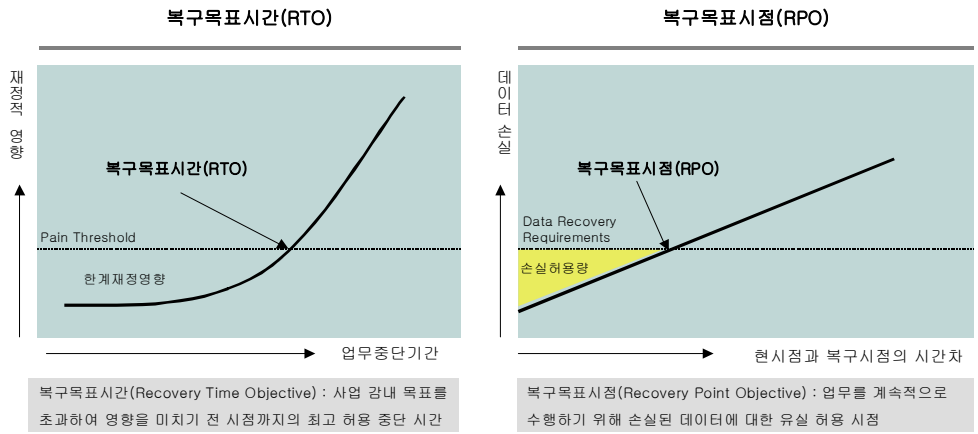
연관성 적용

업무복구 우선순위	
1순위	A1,A2,A3,B1,B2,B3
2순위	C2,C3
3순위	C1

(그림 5-8) 연관성 적용을 통한 업무복구 우선순위 조정(예시)

5.1.5 주요 업무 프로세스별 복구목표시간 결정

위에서 도출된 업무복구 우선순위에서 보는 바와 같이 주요 업무에 식별을 통해 재해복구 대상 그룹을 선정한다. 복구대상 업무범위에 대해서 각 업무 프로세스별의 업무중단허용시간을 평가해야 된다. 이것이 각 프로세스의 RTO가 된다. 한편, 업무수행시의 수집 기록되는 데이터의 중요성에 입각하여 업무손실허용시점이 설정되어야 하고, 이것이 각 프로세스의 RPO가 된다(그림 5-9).



(그림 5-9) 복구목표시간과 복구목표시점의 개념

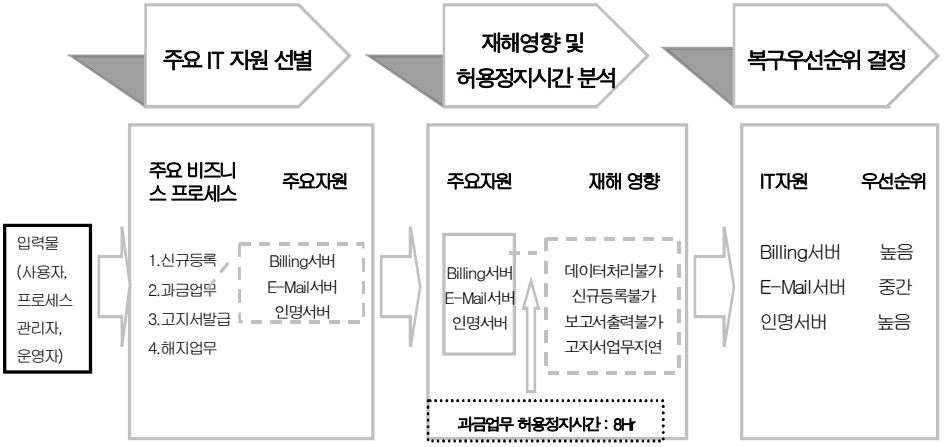
그 밖에 각종 통신매체들의 복구를 통해 복구 대상 네트워크의 정상가동 재개 시간 범위를 정의하는 네트워크 복구목표(RCO: Recovery Communication Objective), 재해 발생시 복구 되어야 할 업무들의 종류와 범위들을 정의하는 업무 복구범위 목표(RSO : Recovery Scope Objective)와 재해복구를 위한 재해복구센터의 활용방안과 구축형태를 정의하는 백업센터 구축목표(BCO: Backup Center

Objective)등이 있다.

RTO 및 RPO의 결정시 손실 평가결과가 최우선이 되나, 이외에도 관련 법률, 정책, 규정, 지침, 등을 검토하여 이를 고려하여야 한다. 참고로, 이와 관련된 국내 지침으로는 금융감독원 권고('01.10)지침으로 금융기관 IT 부문비상 대응방안, TTA지침, 집적데이터센터 관리 운용지침 등이 있고 국제규약으로는 바젤II, BS7799, ISO17799, ISSA, CPSS/IOSCO, G-30 등 국제 표준화기구 및 국제금융단체의 재해에 대비한 업무 연속성 계획 수립권고 지침 등이 있다.

5.2 IT자원 복구전략 수립

5.1절에서 설명한 각 업무프로세스별 복구목표시간 및 복구우선순위가 결정되었으면 관련 IT 자원과 연계한 구체적인 복구계획 수립이 필요하다. 재해 상황 시 업무가 받게 되는 영향, 업무를 지원하는 각 IT 서비스와 관련 IT 자원이 받는 영향을 평가하고 그에 따라 재해복구에 대한 요구사항 및 복구우선순위를 정의하게 된다. (그림 5-10)은 주요 업무와 연관된 IT 자원 선별 및 허용정지시간과 복구우선순위를 부여한 예이다.



(그림 5-10) IT 자원 선별 및 허용정지시간과 복구우선순위 부여(예시)

5.2.1 주요 IT자원 선별

일반적으로 업무 시스템은 다양한 IT 자원과 인터페이스로 구성되며, 시스템은 단일 업무보다는 다중업무를 수행하는 경우가 많다.

- 해당 업무 프로세스를 지원하는 시스템 및 그 시스템과 연관성을 가진 시스템을 파악하여야 한다. 그리고 시스템 관리/운영 조직과 시스템 상에서 송수신되는 데이터를 이용하는 조직(업무 부서)도 포함하여 분석하여야 한다.
- 시스템을 운영하기 위한 부가적인 장비도 조사하여야 한다. 보통 라우터, 방화벽, 스위치 등이 이에 해당한다.
- 주요 IT 자원과 주요 업무 프로세스간의 연관관계를 분석하여야 한다. (그림 5-11)은 주요 업무 프로세스와 IT 자원의 연관관계를 도표로 나타낸 예이다.

[시스템별 RTO, RPO] = 관련 업무 프로세스의 RTO,RPO의 최소값

업무 \ IT자원	'가'시스템	'나'시스템	'다'시스템	'라'시스템	'마'시스템	업무별 RTO	업무별 RPO
A1	◎				◎	1시간	실시간
A2			◎		◎	4시간	30분
B1					◎	1일	1일
B2	◎					3시간	30분
B3		◎				8시간	1시간
C1		◎			◎	3일	1일
C2	◎				◎	3일	1일
C3			◎			1일	1일
D1			◎			2일	1일
D2				◎		6시간	1시간
D3				◎	◎	1일	1일
IT자원별RTO	1시간	8시간	4시간	6시간	1시간		
IT자원별RPO	실시간	1시간	30분	1시간	실시간		

(그림 5-11) 주요 업무 프로세스와 IT 자원의 연관관계 분석(예시)

5.2.2 재해영향 및 허용정지시간 분석

앞 단계에서 선별된 주요 IT 자원의 재해로 피해 영향을 다음과 같이 조사한다.
- 시스템의 중단을 허용할 수 있는 최대 시간을 파악한다.
- 해당 시스템의 중단으로 인한 연관 시스템 및 종속 시스템이 받는 피해를 분석하고 특히 분산환경 시스템의 장애 파급효과도 분석한다.

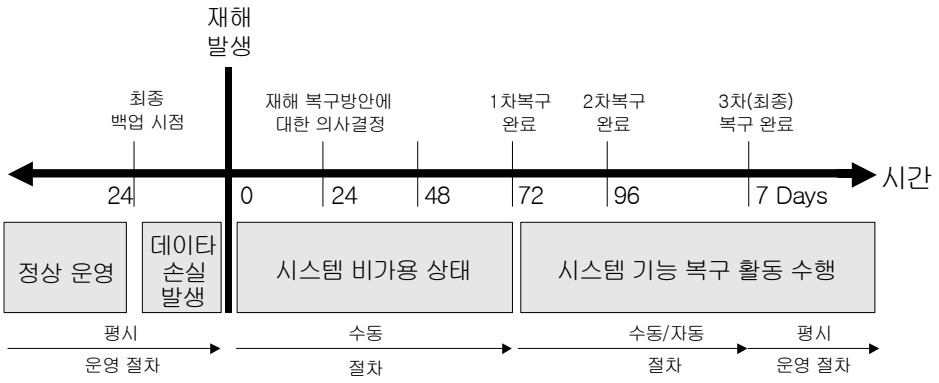
(그림 5-11)의 도표에서 나타난 바와 같이, 하나의 IT 자원은 여러 가지의 업무 프로세스와 연관되어 있는 것이 일반적이므로, 앞서의 분석에서 얻어진 각 업무

프로세스별 RTO, RPO의 결과를 이용하여, 특정 IT 자원에 대한 RTO, RPO는 다음과 같이 얻어질 수 있다.

IT 자원의 RTO, RPO = 관련 업무 프로세스별 RTO, RPO의 최소값

5.2.3 복구우선순위 결정

재해로 인한 영향과 허용정지시간을 이용하여 IT 자원 별 복구우선순위를 결정할 수 있으며, 재해복구 계획에 복구우선순위의 복구절차를 반영한다. 예를 들어 재해영향 및 허용정지시간 분석에서 4시간 내에 복구되어야 한다는 결론이 내려지면 IT 자원에 대하여 이 요구사항을 충족시키기 위한 기준을 마련해야 한다. 또한 24시간 이내 재해복구 계획 중 주요 시스템이 8시간 내 복구되어야 한다면 재해복구 관리자는 주요 시스템 복구를 위한 복구자원할당을 반영하여야 한다. 복구우선순위 조정을 통하여 재해복구의 자원, 시간, 예산을 조절함으로써 해당 조직에 최적이며 동시에 ROI를 극대화 하는 재해복구 계획을 수립할 수 있다. (그림 5-12)는 재해복구 활동이 몇 시간 안에 이루어져야 하는 지에 대한 요구사항을 정의한 예를 보인 것이다.



(그림 5-12) 재해복구활동에 대한 시간적 요구사항의 예

재해복구 요구사항이 전체적인 업무의 관점에서 함께 수행되지 않고 단순히 재해복구에만 초점을 맞추어 정의되었다면, 기존의 요구 사항들을 재검토하여 전체적인 업무 위험 평가의 관점에서 이들의 통합 및 조정을 통해 재해복구 요구사항을 재정의하는 작업이 필요하다.

6. 재해복구시스템 설계 및 구축

6.1 재해복구시스템 운영형태 결정

재해복구시스템의 운영형태는 4.1절에서 설명되었던 바와 같이 크게 나누어 자체운영, 상호간, 공동구축, 위탁의 4가지 유형이 있다. 본 절에서는 각 운영형태의 장단점과 고려사항에 대해 세부적으로 살펴봄으로써 재해복구시스템의 운영형태의 결정시 참고가 될 수 있도록 한다.

□ 독자구축

기관 전용의 재해복구센터를 독자적으로 구축하여 기관 자체의 인력으로 운영하는 방식이다.

o 장점
- 보안유지가 용이하고 복구의 신뢰성이 가장 높다.
- 예산이 허용하는 범위에서, 정보시스템 설비로부터 사무공간에 이르기까지 재해시 업무 수행을 위해 필요로 하는 모든 것을 구축할 수 있다.
- 요구되는 시스템 사양에 일치하는 시스템을 구축할 수 있다.
- 재해발생시점에 관계없이 항상 재해복구센터의 사용이 가능하다.
- 필요한 경우 언제든지 원하는 수준의 재해복구시스템의 테스트가 가능하다.

o 고려사항
- 높은 초기구축비용이 소요되므로, 신뢰성있는 설비를 구축하기 위한 충분한 예산이 확보되어야 한다.
- 높은 수준의 감가상각비용이 발생한다.
- 높은 운영비용이 소요되며, 재해복구시스템의 안정적 운영과 복구 신뢰성을 위한 전문성 있는 운영인력 확보가 필요하다.
- 업무시스템이 갱신됨에 따라 재해복구시스템도 함께 변경되어야 하므로 시스템 유지보수를 위한 지속적 예산이 확보되어야 하며, 주센터의 업무시스템 변경내역에 따라 재해복구센터의 시스템을 개선하기 위한 체계화된 관리절차가 필요하다.
- 실질적인 모의훈련이 지속적으로 이루어져야 한다.

□ 위탁운영

재해복구시스템의 구축 및 운영을 전문적 재해복구서비스 제공업체 등 외부의 다른 기관에 위탁하는 방식이다.

o 장점
- 초기투자비용 및 운영비용이 저렴하다.
- 업무시스템의 갱신에 의한 재해복구시스템의 유지보수의 부담이 경감된다.
- 정보시스템으로부터 네트워크, 전화 등 통신수단, 사무공간까지 다양한 형태의 위탁운영서비스 중에서의 선택이 가능하다.

o 고려사항
- 정보시스템 운영기관의 보안성 유지를 위한 정책 및 계약이 신중하게 검토되어야 한다.
- 일반적으로, 재해복구서비스 제공업체는 설비의 효율적 활용을 위해 동일 설비를 여러 조직에 계약하게 되는 경우가 많으므로, 재해시 복구서비스의 제공 내역 및 우선순위 등에 대한 명확한 계약이 이루어져야 한다.
- 계약된 복구목표시간이 짧을수록 높은 운영비용이 소요되므로, 가용 예산과의 균형을 고려하여 복구목표시간을 설정하여야 한다.
- 모든 설비가 계약대로 보유되고 있으며 실제로 가용한지를 확인하여야 한다.

□ 상호운영

두 개 이상의 기관이 상호간의 재해복구센터의 역할을 수행하거나, 단일 기관이 여러 개의 정보시스템 사이트를 가지고 있는 경우 사이트 상호간에 서로 재해복구센터의 역할을 수행하도록 방식이다. 이 방식은 상호간 제공하는 자원의 수준에 따라 다음과 같이 다시 구분될 수 있다.

- 기반시설수준 : 건물, 전력, 항온항습 등 기반시설만 공동으로 이용하는 경우

- 정보시스템수준 : 서버, 디스크, 네트워크 등 정보시스템자원을 공동으로 이용하는 경우

o 장점
- 구축 및 운영비용이 저렴하다.

o 고려사항(기반시설수준, 정보시스템수준 공통)
- 상호간에 전력, 공간 등의 여유자원을 충분히 확보해야 한다.
- 본질적으로 한 기관(또는 사이트)에 재해가 발생할 경우, 이의 영향이 상대방 기관(또는 사이트)에 파급되는 속성을 가지고 있으므로, 재해 발생시 혼란을 초래하기 쉽다.
- 재해를 당한 조직(또는 사이트)의 복구가 상대편 조직(또는 사이트)의 업무 수행과의 사이에서 타협되지 않도록 해야 한다. 특히 상호간이 경쟁관계의 측면을 가진 경우에 문제가 될 수 있으므로, 명확히 문서화된 계약이 이루어져야 한다.
- 재해 발생시 상대방 기관(사이트)으로 인력이 이동하여 작업을 수행해야 하는 경우 혼란이 초래될 수 있으므로, 재해시의 작업공간에 대한 고려가 필요하다. 예로서, 식당 등 평상시 작업공간이 아닌 장소를 사용하도록 하거나, 근무시간대를 달리 하는 등의 계약이 필요하다.

o 고려사항(정보시스템수준)
- 상호간에 충분한 시스템 자원의 여유가 확보되어야 한다.
- 상호간에 시스템 호환성이 있어야 한다.
- 재해복구시스템 구축 초기에 시스템간의 상호호환성이 있었다 하더라도, 양쪽의 업무시스템 변경에 따라 서로의 시스템이 급속히 달라지는 경향이 있으므로 업무시스템 변경에 대한 상호간 지속적인 조정이 수행되어야 한다.

□ 공동이용

두 개 이상의 기관이 별도의 재해복구센터를 공동으로 구축하는 방식이다. 비용측면에서 독자구축의 경우보다 적게 소요되지만 보안과 운용측면에서는 고려할 사항이 많고, 광역재해 발생시 공동이용기관간의 동시 재해복구가 불가능하다는 단점이 있다. 공동구축은 공동이용수준에 따라 다시 다음과 같이 구분해 볼 수 있다.

- 기반시설수준 : 건물, 전력, 항온항습 등 기반시설만 공동으로 이용하는 경우

- 정보시스템수준 : 서버, 디스크, 네트워크 등 정보시스템자원을 공동으로

이용하는 경우

o 장점
- 초기구축비용의 절감이 가능하다.
- 운영인력 및 시설의 공동활용을 통하여 운영비용의 효율화가 가능하다.

o 고려사항
- 공동이용기관간의 보안성 확보를 위한 방안이 수립되어야 한다.
- 공동운영을 위한 운영조직 및 운영체계의 수립이 필요하다.
- 광역재해로 인하여 공동이용기관에 동시에 재해가 발생했을 경우의 재해복구센터의 사용방식과 우선순위 등에 대한 명확한 정책이 수립되어야 한다.
- 정보시스템 수준의 공동이용이 이루어지는 경우에는, 상호간에 시스템 호환성이 있어야 하며, 초기에 시스템간의 호환성이 있었다 하더라도 양쪽의 업무시스템 변경에 따라 서로의 시스템이 급속히 달라지는 경향이 있으므로 업무시스템 변경에 대한 상호간 지속적인 조정이 수행되어야 한다.

6.2 재해복구시스템 유형의 결정

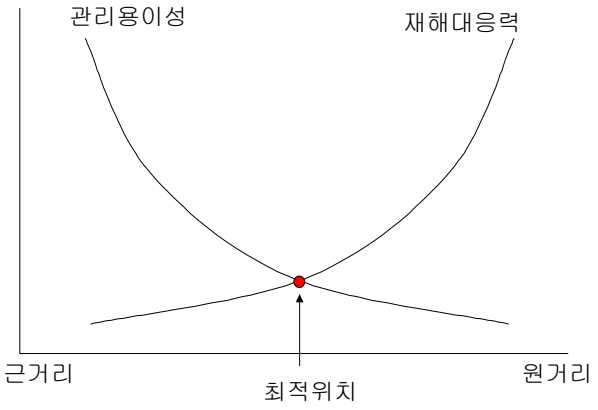
재해복구시스템의 복구수준별 유형은 크게 미러사이트, 핫사이트, 웜사이트 및 콜드사이트로 구분되며, 각각에 대해서는 4.2절에서 기술된 바 있다. 이러한 유형 중 어떤 것이 선택되어야 하는지의 결정은 RTO, RPO 및 업무시스템의 서비스 특성에 입각하여 이루어진다.

□ RTO & RPO에 따라
- RPO=0 & RTO=0 : 미러사이트
- RPO=0 & RTO<수시간 : 미러링 방식의 핫사이트 (통칭 미러사이트라고도 함)
- RTO, RPO 가 약 1일 : 웜사이트
- RTO, RPO가 수일~수주 : 콜드사이트

□ 업무시스템 속성에 따라
- 데이터의 갱신이 거의 없고, 웹 어플리케이션 서비스 위주
  : 미러사이트 (active-active 방식)
- DBMS를 이용하며 데이터의 갱신이 많음
  : 미러링 방식의 핫사이트 (active-standby방식)

6.3 재해복구센터의 위치 선정

일반적으로, 주센터와 재해복구센터가 원거리에 위치할 경우 재해에 대한 대응력은 높아지게 되나, 관리용이성이 저하되고 통신비용 등의 관리비용이 증가하는 문제도 동시에 있으므로, 재해복구센터의 위치는 재해대응력과 관리용이성을 종합적으로 고려한 최적의 위치로 선정되어야 한다.



(그림 6-1) 재해복구센터의 위치 선정

가. 재해복구센터의 위치 선정시의 고려사항

재해복구센터의 위치 선정과 관련한 고려사항으로는 다음과 같은 것들이 있다.(Gatner group, DF-14-9811)

□ 주요 자원의 동시 공급중단 위험성

전력 등의 주요 자원은 업무수행에 필수적임과 동시에 공급중단의 위험성이 높으므로(핫사이트 전환 재해선언의 15%로 추정), 주센터와 재해복구센터는 이러한 주요 자원의 공급중단으로 인해 동시에 영향을 받지 않도록 해야 한다. 즉, 주센터와 재해복구센터는 전력선, 상수도, 통신, 네트워크 라인 등을 서로 공유하지 않도록 해야 한다. 주요 자원 중 불가피하게 공유될 수밖에 없는 자원(예: WAN 등)은 fault tolerance를 확보해야 한다.

□ 동일 재해 영향권 위험성

주센터와 재해복구센터는 동일한 재해로부터 영향 받지 않을 만큼 충분히

떨어져 있어야 한다. 예를 들면, 주센터와 재해복구센터는 동일한 지리적 위험을 갖는 지역(예. 지진대, 홍수권역 등)에 위치하지 않아야 한다. 이는 대개의 경우 15~80km 정도의 거리이면 달성 가능하나, 지역적 특성에 따라 달라질 수 있다.

□ 테러의 위험성

테러에 대한 위험성은 미국의 9·11 테러사태 이후 전세계적으로 관심이 고조되었으며, 지정학적 불안정성을 안고 있는 우리나라에서도 주요 고려 대상에 해당한다. 미국의 경우 9·11 사태 이후 많은 기업들이 재해복구센터를 테러의 위험이 상대적으로 낮은 저층건물, 소도시 및 시골지역으로 이전을 검토중이며, 주센터 업무 건물로부터의 인력 소개방안을 수립하고 있다. 주센터의 파손이 없더라도 테러의 위험성에 대비하여 인력만을 소개하여 원격지 재해복구센터로 이동하는 시나리오에서는, 인력은 재해복구센터로 이동하더라도 주센터의 정보시스템은 원격운영을 통해 계속 가동될 수 있으며, 소개 기간이 길어지거나 필요시 재해복구센터 시스템으로 전환된다.

□ 인력 가용성과 교통 문제

사람이 직접 영향을 받는 재해(예: 재산손실, 가족의 부상)시에 사람들은 가족을 두고 멀리 가려고 하지 않는다. 따라서, 재해시 주센터의 근무인력이 재해복구센터로 이동하여 근무해야 하는 경우에는, 재해복구센터가 주센터에서 근무하던 인력이 통근할 수 있는 거리여야 하며 정해진 규정은 없으나 일반적으로 1시간 거리 이하로 여겨진다. 통근거리 이내로 두 사이트를 두는 경우 교통시스템 파괴시의 위험을 경감할 수 있다. 만약 주센터와 재해복구센터간의 거리를 통근거리 이상으로 두는 경우에는 충분한 인력을 재해복구센터에서 유지하여야 하나, 재해복구에는 전문적 기술과 업무경험이 필요하므로, 원격지의 재해복구인력에 대해서는 지속적 훈련이나 주센터와의 순환근무를 수행하는 것이 필요하다.

□ 기술적 고려사항

미러사이트 및 핫사이트 방식의 재해복구시스템을 구축하는 경우 데이터의 실시간 미러링을 위해 동기적 또는 비동기적 방식의 데이터 복제를 수행하게 된다. 이러한 데이터 복제 방식에 따라 주센터와 재해복구센터간의 거리가 제약받을 수 있다. 예를 들어, 동기적 데이터 복제를 구현하는 경우 약 40~100km 이하로 거리가 제한된다.

□ 비용고려사항

재해복구센터의 위치 선정에는 비용을 고려해야 한다. 대체로 주센터와 재해복구센터의 거리가 멀어질수록 운영비용이 증가하는 경향이 있으므로, 재해복구센터의 위치는 구축비용과 재해의 위험성 및 재해시 업무손실과의 균형을 이루어야 한다.

나. 재해복구센터의 구축 장소의 고려사항

재해복구센터의 구축 장소 선정시에는 다음과 같은 사항을 고려해야 한다.

- 공간확보 : 재해복구센터 구축에 필요한 충분한 공간 확보가 가능한 장소(전산실·운영실·기반설비 설치공간 등)
- 보안성 : 외부인의 통제가 용이하여 물리적 보안 유지가 용이하고, 시스템 운영의 안정성을 보장할 수 있는 장소
- 경제성 : 재해복구센터의 운영환경 확충을 위한 기반설비 및 운영조직 구축비용의 최소화가 가능한 장소
- 확장성 : 향후 재해복구시스템의 확장을 위한 충분한 여유공간의 확보가 용이한 장소
- 안전성 : 기반설비 및 전산장비의 하중을 고려하여, 내구성이 확보된 장소
- 지리 및 기후조건 : 지진, 홍수 등 주요 자연재해로부터의 안전성이 확보된 장소
- 네트워크환경 : 데이터 복제 및 재해시 서비스 제공을 위한 고속 네트워크 접속이 유리한 장소
- 관리용이성 : 재해복구센터의 구축 후 유지보수·관리 및 지속적인 훈련이 용이한 장소

6.4 재해복구시스템 기술 결정

재해복구시스템을 설계하고 구축하기 위해서는 이미 살펴본 재해복구 시스템 운영형태 및 방법을 결정한 후, 현 업무와 시스템 환경을 면밀히 분석하여 최적의 복제기술을 선정하여야 한다. 이를 위해서는 재해복구 비용, 목표복구시간(RTO), 목표복구시점(RPO) 등을 감안하여 적용 및 구현 가능한 솔루션을 나열하고 그 중 최적 안을 선정한다.

우선 복제방식으로서 H/W적 복제방식과 S/W적 복제방식 중 어느 방식을 선택하는 것이 좋을 지 검토 후, 그에 알맞은 솔루션을 조사하여 툴을 결정한다. 구체적인 솔루션이 선정되어도 그것을 적용하는 방식이나 옵션이 다양하므로 이를 사전에 신중하게 검토하기 위하여 전문가 의견을 청취할 것을 권고한다. 예를 들어, 만일 H/W적 복제방식을 선택하였을 경우에도 데이터 전송방식을 동기식으로 할 것인지, 비동기식으로 할 것인지를 결정하여야 한다.

기술적 요소 결정을 수행하지 않고 솔루션을 먼저 선택하게 되는 경우, 선택된 솔루션에 의해 세부적 기술은 종속적으로 결정될 수도 있다. 이 때, 객관적인 의사결정 및 기술검토를 지원해 줄 전문가들을 참여시킬 것을 권장한다.

4.3절에서 각 기술별 장, 단점을 살펴보았으므로 여기서는 자세한 내용은 생략하고 업계 사례를 제시한 다음 표를 참조한다. (그림 6-2)는 각 솔루션별 기술 및 특성을 표로 정리해 둔 것이다. 단, (그림 6-2)는 2004년도 시장현황을 기준으로 조사 정리한 것이며 조사범위 및 정리 관점에 따라 조사에서 누락되었거나 분류 항목이 다를 수 있으므로, 절대적인 기준은 될 수 없음을 밝혀 두는 바이다.

구분	소프트웨어 솔루션											
	SharePlex	TDMFopen	VVR	RRDF	HAGeo	Standby DB	ER	Backup Xcelerator	DRM	FullTime Data	Double Take	IP-Store
제작사	Quest Software	SOFTEK	Veritas	E-Net	IBM	Oracle	Golden Gate	NCERTI	DRM	Qualix사	NSI 소프트웨어	falconStor
플랫폼	ALL	ALL	ALL	OS/390	AIX	ALL	ALL	ALL	HP	ALL	Window Solaris	ALL
DB	Oracle	ALL	ALL	ALL	ALL	Oracle	ALL	ALL				ALL
전송방식	Async	Sync Async Semi-Sync	Sync Async	Async	Sync Async MWC	Async	Sync Async	Async				Async
네트워크	TCP/IP	전용선 TCP/IP	TCP/IP	전용선	전용선	전용선	TCP/IP	전용선				TCP/IP
제한거리	없음	없음	없음	없음	없음	없음	없음	없음				없음
전송단위	Redo Log	Block File(Windows)	Block	Log	Logical Volume	Archive Redo Log	File(Table)	Archive Log			File I/O	Redo Log
특징	Oracle DB OPS 환경불가	Compaq 불가 OPS 환경불가	Volume Mger 반드시 필요함 OPS환경불가	M/F 환경 DB Shadowing Compression	AIX 환경 HACMP 필요	Oracle DB 동일한 환경 (HW, OS)	Data Formatting Data Selection Compression	국내 S/W			Data Mirroring 자동 Fail Over	
국내사례	신영증권	씨티은행 한국자원 재생공사	삼성투신	경남은행 서울은행			삼성카드 외환카드	보험개발원 KTF	청주성모병원			
해외사례	프라이스닷컴	JP 모건 홍콩공항 중국은행 싱가폴텔레콤 홍콩 텔레콤	State Street Bank, Large North America Bank	B O A JP MOGAN CITY BANK 홍콩텔레콤								
비 고							Extractor & Replicator		Data Replication Manager			

구분	소프트웨어 솔루션						하드웨어솔루션					
	SNDR	SVM	CA	MQ-Series			SRDF	True-Copy	PPRC	XRC		
제작사	SUN		HP	IBM			EMC	HDS	IBM	IBM		
플랫폼	SUN	ALL	ALL	ALL			ALL	ALL	ALL	OS/390		
DB		ALL	ALL	ALL			ALL	ALL	ALL	ALL		
전송방식	Sync Async		Sync Async	Archive 시점			Async Semi-Sync Adaptive	Sync Async Semi-Sync	Sync	Async		
네트워크				TCP/IP			전용선	전용선	전용선	전용선		
제한거리				없음			66km-Sync (Sync)	40Km-Sync (Sync)	103Km	없음		
전송단위				Archive Log			Track	Track,Block	Block	Block		
특징		SAN 환경	FailBack HP Array DISK				EMC 디스크Time Finder	HDS 디스크 Shadow Image	IBM디스크 Flash Copy	M/F 환경 SDM 시스템 Flash Copy		
국내사례		SBS방송	에스원	삼성SDI			한빛은행 외환은행 신한은행 한국전력 주택은행 동양증권	하나은행 한국은행 삼성캐피탈 삼성생명 삼성화재	없음	제일은행 SK텔레콤		
해외사례		BHF Bank (독일) 광동TV (중국) Technion (이스라엘)					시티뱅크 골드만삭스 Unum생명 볼베이증권거래소 방콕은행	에어프랑스 홍콩상하이 은행, 시티뱅크, 맨하튼은행 매릴린치 등	Bank Of China Post Danmark Credit Suisse DahSing Bank Lloyds TSB	ABN AMRO Norges Bank Barclays Bank Manhattan Bank BP Amaca Corp		
비 고	Sun StoreEdge Network Data Replicator	Storage Virtualization Manager	Continuous Access	Message Queue								

(그림 6-2) 재해복구 솔루션

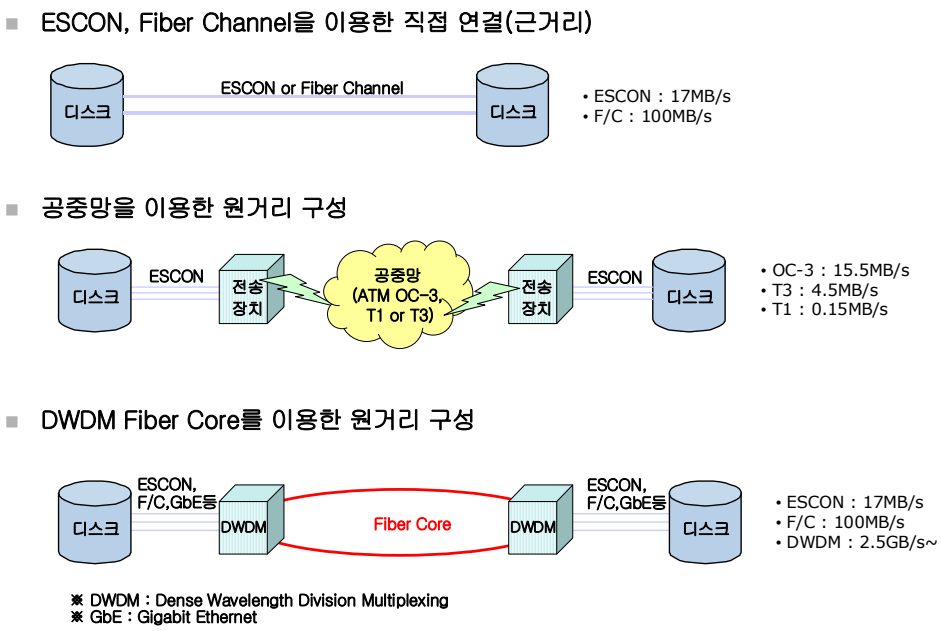
6.5 네트워크 형태 결정

4.4절에서 재해복구시스템을 위한 네트워크는 용도에 따라 데이터 복제를 위한 데이터 복제 네트워크와 재해 시 서비스 용도로 이용할 재해복구 서비스 네트워크로 나누어 볼 수 있다고 설명하였다. 근래에는 IP기반의 데이터 복제가 가능하여 짐에 따라 데이터 복제 네트워크를 서비스 용도로도 동시에 활용할 수 있는 솔루션이 제공되고 있다.

6.5.1 데이터 복제 네트워크 결정

데이터 복제 네트워크는 주센터와 재해복구센터 사이의 거리와, 복제 방식에 있어 Sync, Async 방식의 차이 등에 의해서 장비 및 용량이 결정되어 지므로 이러한 특성을 명확히 이해하여야 한다. 그러나 네트워크 운영비용이 재해복구시스템 구축비용 중 많은 비율을 차지하는 현실로 인하여 네트워크 회선 운영비용을 줄이기 위해 그에 맞추어 재해복구 솔루션을 선정하거나 변경하는 사례가 발생하기도 한다.

(그림 6-3)은 데이터 복제 네트워크 구성방식을 크게 3가지로 나눈 것이다.



(그림 6-3) 데이터 복제 네트워크 구성방식

이중 ESCON이나 F/C를 직접 연결하는 근거리 방식은 로컬 디스크 이중화에 주로 사용하고 재해복구용으로는 잘 사용하지 않는다. 즉, 공중망을 이용한 원거리 구성이나 DWDM을 이용한 원거리 방식을 주로 사용하는데, 최근에는 DWDM의 통신회선비가 저렴해지고 유연한 대역폭 확대가 가능한 점으로 인하여 DWDM을

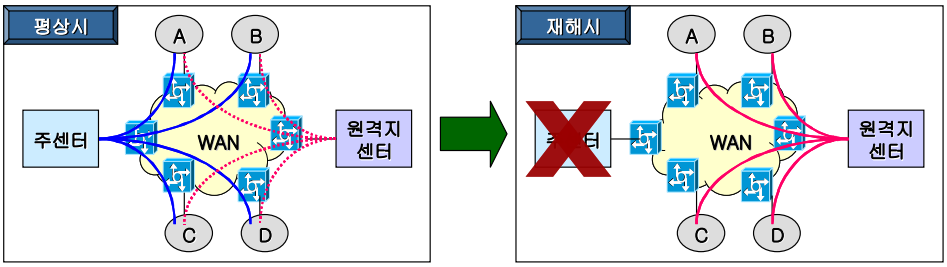
이용하는 사례가 많아지고 있다.

데이터 복제 네트워크의 용량을 너무 작게 잡으면 주센터의 운영 시스템 성능에 많은 영향을 줄 수 있다. 따라서 주센터의 운영 업무에 지장을 주지 않는 수준 이상의 용량을 확보하여야 한다. 용량산정 시 고려 요소로는 초기 전체 데이터 전송량, 평시 변경 데이터 전송량, 업무 집중시 변경 데이터 전송량, 여유율, 예비회선 등을 고려하여서 결정하여야 한다.

비용 상의 제약이 있으면 대량의 데이터 전송이 발생되는 업무 집중시간(대량 작업이나 배치작업 수행 중) 중에는 잠시 재해복구용 데이터 복제를 중단 후 다시 재개하는 등의 절차를 통해 해결하기도 하나 이는 운영의 복잡성을 증가시킨다.

6.5.2 재해복구 서비스 네트워크

재해복구 서비스 네트워크는 재해 시 주 센터에서 수행하던 서비스를 재해복구센터에서 동일 혹은 일정 수준으로 수행할 수 있도록 하기 위한 서비스용 네트워크이다. (그림 6-4)와 같이 평시에는 구축만 해 두고 사용을 하지 않다가 재해 발생시에 재해복구 서비스 네트워크를 통해 서비스를 진행한다.



(그림 6-4) 재해발생시 서비스 네트워크 사용

따라서 재해복구 서비스 네트워크 구축을 위한 투자와 유지비용이 부담으로 작용할 수 있다. 그러나 재해복구 서비스 네트워크를 적절하게 구성하지 않으면 실제 재해 발생시 시스템은 복구되어도 업무를 정상적으로 서비스하지 못하게 되므로, 재해복구시 서비스 네트워크로의 원활한 전환을 위한 적절한 자원의 확보는 필수적인 고려사항이다.

(표 6-1)은 재해복구시스템 구축시 고려해야 할 재해복구 서비스 네트워크를 종류별로 정리한 것이다. 재해복구 서비스 네트워크의 핵심은 재해 발생시 정상적인 업무 가동이 가능하도록 서비스용 네트워크를 구성해야 한다는 것이다.

<표 6-1> 재해복구 서비스 네트워크

구분	종류	역할	고려사항	비고
내부망	전용망	시스템 접속, 서비스 제공	재해복구용 백업라인 용량 산정, 평시 활용방안 검토	
	DNS	웹 대고객 서비스 지원	재해복구 웹 시스템 전환 후 일반고객이 최단기간내 재해복구 웹 시스템으로 접근 가능	
	기타	ADSL, VPN 접속 등	비용을 고려하여 백업 전용망을 ADSL 등으로 대체 가능	
외부망	X.25	기관간 데이터 송수신	주요 X.25 라인 및 장비 이중화 필요	신용거래, 금융거래 등
	EDI	금융기관과 데이터 송수신	평시 복수의 VAN사와 EDI 서비스 권장	금융거래, 전자문서 등

재해복구 서비스 네트워크의 종류별 특징을 살펴보면 다음과 같다.

□ 재해복구 서비스용 전용망

재해발생시 재해복구시스템에 접속하여 운영서비스를 받을 수 있는 네트워크 망으로서 평소에는 사용을 하지 않는 망이다. 그러므로 고객이 재해복구시스템을 구축할 때, 투자를 꺼리는 부분이기도 한다. 따라서 재해복구용 전용망을 평시에는 다른 업무(예를 들어 화상회의 전용)에 투입하거나, 용량을 주 네트워크 망 대비 50% 수준 이하로 유지하여 구축하는 경우가 많다. 그러나 이 경우에 재해발생시 재해 이전과 동일한 수준의 네트워크 서비스를 받을 수 없다는 것을 고객이 명확하게 인지하여야 한다.

□ DNS

최근에는 웹 어플리케이션 서비스에 대한 재해복구시스템을 구축하는 경우도 많다. 웹 관련 재해복구시스템 구축시 추가로 고려하여야 할 네트워크 관련 사항은 DNS의 이중화이다. 최근에는 지능형 DNS를 이용하여 재해시 짧은 시간에 고객이 동일한 URL을 통해 재해복구시스템으로 서비스를 받을 수 있도록 지원되고 있다.

□ ADSL, 기타

출장소나 및 제휴점과 같은 조그마한 사업장의 네트워크는 별도의 재해복구 전용망을 이용하는 것보다 ADSL이나 VPN 서비스를 이용한 재해복구시스템의 접속을 검토할 수 있다.

□ X.25

X.25 프로토콜은 보안성 및 신뢰성이 높아 각종 신용정보나 금융거래정보의 송/수신을 위해 많이 사용한다. 따라서 재해복구 시스템 구축 시에 X.25 네트워크 망의 복구는 매우 중요한 고려요소이다. X.25망이 외부기관과 주센터 외에 외부기관과 재해복구센터 사이에도 연결이 되어 있어야 한다. 평시에는 주센터와 X.25 통신을 하다가 재해시 간단한 조작으로 외부기간과 재해복구센터 사이로 전송경로를 전환 할 수 있어야 한다. 또한 X.25망 관련 네트워크 장비들도 주센터 이외의 노드에서 이중화 구성하여야 한다.

□ EDI

각 기관들은 다양한 금융기관과 금융거래를 하고 있다. 이때 금융기관과 금융거래를 위해 모든 금융기관과 각각의 금융거래용 네트워크 망을 별도로 구축하기는 어려운 실정이다. 따라서 각 금융기관과 네트워크 망을 구축해 두고, 이를 이용해 금융거래 서비스를 실시하는 VAN사의 EDI 서비스를 이용하는 경우가 많다. 이 경우 주센터뿐 아니라 재해복구센터에도 EDI를 위한 별도의 프로그램이나 장비를 구비하거나 또는 VAN 서비스를 평시에 두개 이상의 회사로부터 이중으로 서비스 받아 재해 시 서비스가 가능한 VAN사의 서비스로 우회하는 것이 필요하다. 만일 EDI시스템이 재해가 발생하면 대량의 자동 금융거래가 수작업으로 이루어 져야 하며 큰 혼란이 발생할 것이다. 예를 들면 서버에서 테이프로 금융거래 데이터를 받은 후 은행으로 택배나 인편으로 보내는 상황이 발생할 것이다.

6.6 재해복구 인력구성 방안

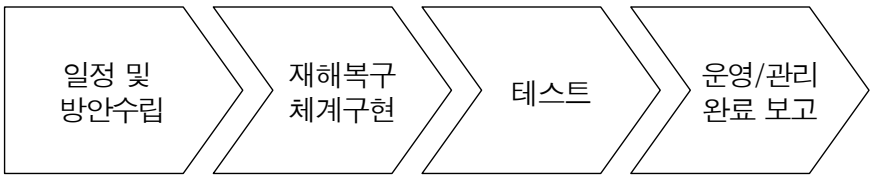
재해복구 인력구성은 크게 재해복구시스템 구축을 위한 조직과 운영을 위한 조직으로 나눌 수 있겠다. 재해복구시스템 구축 시, 주요 구축 활동을 서비스 공급업체에 일임하더라도 향후 재해복구시스템을 운영할 담당자가 함께 적극적으로 참여하도록 유도하여야 한다.

재해복구 운영 조직은 재해복구 계획과 관련된 팀을 나열하고 각 팀의 주요 역할과 책임을 정의한다. 향후 각 팀은 재해복구 훈련계획에 따라 훈련을 통해 재해 선언 시 요구되는 재해복구 임무를 원활하게 수행할 수 있어야 한다. 또한 재해복구 계획에 나타나는 조직도는 재해복구와 관련된 모든 팀을 나열하고 역할을 간략하게 설명한다. 재해복구 계획서 부록에는 상세한 조직도 및 연락처를 첨부하고 최신 정보를 유지하여야 한다.

재해복구 조직과 인력의 구성방안에 대해서는 7장에서 자세히 설명하였다.

6.7 재해복구시스템 구축

운영 상황에 맞는 재해복구시스템 설계가 완료되면 시스템 구축을 수행하게 된다. 올바른 구축 수행을 위해서는 다음과 같은 순서에 맞추어 구축 계획 및 실행을 검토하여야 한다.



(그림 6-5) 재해복구시스템 구축 절차

가. 일정 및 방안수립

실행 전에 주요 계획과 일정(Mile Stone) 및 범위를 확정하여 계획이 수립되었는지 확인하고 이에 따른 관리를 실시한다.

나. 재해복구 체계구현

- 사전 준비 : 구축 계획에 따른 재해복구시스템을 위한 장비의 발주, 네트워크 구성, 기존 시스템 복제 방법 및 절차, 담당 인력 및 업무의 분장 등이 준비되고 있는지 확인한다.

- 데이터 복제 : 재해복구시스템을 구축하기 위해서는 기존 데이터의 복제가 필요하다. 이를 수행하기 위한 방법에는 재해복구시스템을 주센터에 구축하여 복제 후 재해복구센터로 재해복구시스템을 옮기는 방법과 재해복구시스템을 재해복구센터에 구축 후 복제를 하는 방법이 있다. 일시에 많은 양의 데이터 복제를 위해서는 적절한 크기의 네트워크 용량이 확보되어야 하므로 상황에 맞는 방법을 선택한다.

- 기능 점검 : 최초에 데이터 전체를 복제하고 기타 환경 설정이 완료되어 재해복구시스템이 구축되면, 재해복구 솔루션의 복제 및 복구 기능이 정상 작동하는지를 테스트하여야 한다. 이때 부하발생 및 성능 분석 등을 통해 기존 시스템의 성능과 서비스에 문제가 없는지 확인하여야 한다. 이러한 작업은 문제 발생에 대비하여, 실제 서비스 시간을 피해서 휴일 혹은 야간에 수행하는 것이 바람직하다.

다. 테스트

- 테스트 시나리오 작성 : 재해복구 기능 및 데이터 정합성을 세밀하게 테스트할 수 있는 유형별, 상황별 테스트 시나리오를 작성하여야 한다.

- 단위/통합 테스트 : 운영환경에서 계획된 시나리오에 의해 재해발생, 재해분석보고, 복구시스템으로 전환 등과 같은 절차에 의해 복구 전환 테스트를 실시한다.

라. 운영관리/완료 보고

재해복구 운영 체계에 대한 훈련 및 운영 매뉴얼, 재해복구 모의훈련 계획서 등의 필요한 문서를 제공하고 인수인계 및 완료보고를 실시한다.

7. 재해복구시스템 운영

7.1 재해복구 운영조직의 구성 및 역할

본 장에서는 재해복구 운영조직의 구성 및 역할에 대하여 정의한다. 본 장에서 제시하는 조직 및 역할은 하나의 예시로서, 주센터와 재해복구센터를 구축하고 운영하는 형태에 따라 달라질 수 있으며, 재해복구시스템을 유용하게 가동하는 데에 초점을 맞추어 주로 시스템 복구 관점에서 조직의 역할 및 책임을 정의한다.

가. 평시 운영조직 및 역할

평시의 재해복구시스템 운영을 위한 운영조직 및 역할은 <표 7-1>과 같다.

<표 7-1> 평시 재해복구 운영조직 및 역할

구분	활동내용	책임부서
재해복구시스템 총괄 책임자	- 재해복구시스템 각 사안에 대한 결정 - 재해복구시스템 관리 및 운영 총괄	
시스템 운영 담당자	- 재해복구시스템(시스템, 네트워크, 어플리케이션 등) 운영, 관리, 보고 - 모의 재해복구 훈련 수행	전산실
시설관리자	- 전기/항온항습기/공조/용수 등 기반시설 관리	시설팀
보안관리자	- 보안정책 수립, 출입관리, 기기나 시설보안 관리	보안팀

나. 재해시 운영조직 및 역할

재해발생시 신속하고 원활한 복구를 위해서 운영조직은 다음과 같이 구성되어 각 조직간 협조 하에 복구활동을 수행한다. 본 조직은 평시에는 본연의 업무에 임하게 되며, 재해시 각자의 역할과 임무를 명확히 인지하여 비상상황에 대처한다. 각 조직이 수행하여야 할 기본적인 역할은 <표 7-2>와 같다.

<표 7-2> 재해시 운영조직 및 역할

구분		활동내용	책임부서
관리조직	비상 대책반	- 비상대책에 대한 최고 협의체 - 재해 현황파악 - 재해복구시스템 전환결정 - 서비스 재가동 확인/주센터 복구	임원진, 전산실장 등이 주도하는 비상대책반
기술조직	시스템 복구반	- 재해 원인 및 예상복구시간 파악 - 재해복구시스템 전환 준비 및 전환 - 주센터 피해상황 파악/복구 방안마련 - 전환 후 시스템 모니터링	주/재해복구센터 전산실
	네트워크 복구반	- 통신망 전환 및 모니터링 - 주센터 피해상황 파악/복구 방안마련	통신팀 주/재해복구센터 전산실
	업무 복구반	- 재해복구시스템 정상유무 체크 - 가능/불가능 업무 파악, 보고 - 상실데이터, 어플리케이션 동작 확인 - 예외상황 대응	전산실
지원조직	지원 부서	- 체계적인 대외공표 및 홍보활동 - 긴급물자, 필요자원 조달 및 승인 - 복구관련 필요인원 조달, 인사조치	인사/재무/보험 /법무/홍보
	공급 업체	- 시스템 유지 및 복구에 필요한 자원 공급 및 기술지원	H/W 업체 S/W 업체 기타 공급업체
	상황 유지팀	- 상황실 구성 및 긴급회의 장소/연락 - 피해보고/주요상황 연락, 자원조달 - 임무부여/보고 요건 규정 - 복구팀 자원/인력결정 - 필요시 비용지출 권한 획득/부여	복구상황 관리 복구단계 조정

다. 복귀시 운영조직 및 역할

주센터의 정상 가동 시 재해복구센터로부터 주센터로의 복귀를 위한 조직구성은 <표 7-3>과 같다.

<표 7-3> 복귀시 재해복구 운영조직 및 역할

구분		활동내용	책임부서
관리조직	비상 대책반	- 복귀 방안 준비 및 시기 결정 - 주센터 안정화/정상화 검증 - 복귀에 따른 서비스 전환 확인 - 전환 후 서비스 내역 및 문제점 파악 - 재해복구시스템 복귀절차 통제	임원진, 전산실장 등이 주도하는 비상대책반
기술조직	시스템, 네트워크 복구반	- 복귀시스템의 안정화/정상화 검증 - 주센터 재가동 시점 규정 - 복귀 계획에 따른 복귀 절차 수행 - 복귀 후 시스템 모니터링 - 재해복구시스템 재구성	주/재해복구센터 전산실 통신팀
	업무 복구반	- 업무 정상 복귀 확인 - 예외상황 대응	주/재해복구센터 전산실
지원조직	지원 부서	- 체계적인 대외공표 및 홍보활동 - 긴급물자, 필요자원 조달 및 승인 - 복구관련 필요인원 조달, 인사조치	인사/재무/보험/법 무/홍보
	공급 업체	- 시스템 유지 및 복구에 필요한 자원공급 및 기술지원	H/W 업체 S/W 업체 기타 공급업체
	상황 유지팀	- 상황실 구성 및 긴급회의 장소/연락 - 피해보고/주요상황 연락, 자원조달 - 임무부여/보고 요건 규정 - 복구팀 자원/인력결정 - 필요시 비용지출 권한 획득/부여	복구상황 관리 복구단계 조정

재해에 대비한 운영 조직의 규모 및 구성은 해당 조직에 따라 다르지만 본 지침에서는 역할에 따라 크게 세 가지 조직으로 분류하였다.

(1) 관리조직

□ 비상대책반
: 재해 발생시 장애 및 재해 현황 파악, 재해복구시스템 전환결정, 서비스 재가동 확인, 주센터 복구, 주센터로의 복귀 결정 등에 대한 최고 의사결정을 수행한다. 인력구성은 다음과 같다.

o 재해복구 총 책임자, 임원진, 전산실장, 주요 항목 의사 결정권자
o 재해복구 코디네이터
: 비상대책반의 의사결정 사항 전달, 실무자들의 의견을 비상대책반에 보고 등 실무진과 의사결정권자간의 상호 커뮤니케이션 지원

(2) 기술조직

□ 서버 복구반
: 재해복구시스템 전환 준비 및 전환, 주센터 피해상황 파악, 복구 방안마련, 주센터 복구

□ 네트워크 복구반
: 통신망 관리 및 응대, 네트워크 피해상황 파악/복구 방안마련, 주센터 통신망 복구

□ 업무 복구반
: 재해복구시스템 정상유무 체크, 가능/불가능 업무 파악 및 보고, 상실데이터 및 어플리케이션 확인, 예외상황 응대

□ 테스트반
: 필요시 전산실 개발자 이외의 업무 최종사용자(End-User)로 구성

(3) 지원조직

□ 피해사정팀 : 재해의 피해 사정 및 보고, 보험 계약에 따른 피해 회피 확인
□ 법률팀 : 공급업체 및 서비스 제공업체의 MOU, SLA, 보험계약 등 계약사항 검토
□ 총무팀 : 비상대책반과 각 팀간의 의사소통, 사무실 임대, 주요 인장(印章) 확보

□ 운송팀 : 긴급 물자 수송, 물자 수송 비상가동 체제 확립
□ 인사팀 : 복구관련 필요인원 조달, 인사조치
□ 재무팀 : 긴급 복구 자금 지원, 자금 조달 계획 수립 및 수행
□ 홍보팀 : 체계적인 대외공표 및 홍보활동
□ 구매팀 : 긴급물자, 필요자원 조달 및 승인(선 조치 후 조달 품의 가능)
□ 시설팀 : 전기/항온항습기/공조/용수 관리, 피해상황 파악 및 보고, 피해 복구
□ 통신팀 : 통신설비 복구, 네트워크 복구반 지원
□ 보안팀 : 보안정책 수립, 출입관리, 기기나 시설보안 관리

각 조직의 장은 조직원 구성 시 조직원의 기술과 지식을 고려하여 배정하여야 하며, 일반적으로 평상시 직무에 따라 배정한다. 예를 들어 서버 복구팀원은 평시의 서버 관리자가 될 것이다. 팀원은 재해복구 계획 및 절차를 숙지하여야 한다. 팀원은 각 임무에 대하여 정/부 역할을 부여받으며, 인력이 부족할 경우 공급업체 혹은 계약직 사원을 활용한다.

7.2 재해복구 절차

본 절에서는 재해복구 절차의 단계와 각 단계별의 활동 및 구성원 임무에 대하여 설명한다. 재해복구절차의 단계와 활동에 대한 요약은 <표 7-4>에 나타나 있다.

<표 7-4> 재해복구절차 단계와 활동

단계	활동	구성원 임무
재해선언	재해현황 파악	- 대책본부 구성 - 비상통지 - 상황실 운영 - 현 재해현황 파악 - 예상복구 시간 파악(주센터) - 최고책임자 보고자료 작성
	재해복구시스템 전환결정	- 예상복구 시간, 복귀 시간을 고려하여 전환결정 - 재해복구시스템 전환 절차 통제
재해복구활동	재해복구센터로의 서비스 전환	- 서비스 재가동 확인 - 재해복구센터에서의 장기 운영 대비
	주센터 복구	- H/W, S/W 공급지원업체에 복구 촉구 - 복구불능시 조달계획 수립(선 조치 후 조달 품의) - 재해복구 전환 통제 및 최종 서비스 확인보고 - 대내외 보고, 발표자료 준비 - 주센터 복구시기 산정 및 복구센터 운영방안 마련
주센터 복귀	주센터로의 복귀결정	- 복귀 방안 준비 및 시기결정 - 주센터 안정화 검증 - 복귀에 따른 서비스 전환 확인 - 전환 후 서비스 내역 및 문제점 파악 - 재해복구시스템 복귀절차 통제

각 단계에 대한 세부적인 내용은 다음과 같다.

가. 재해 선언

재해로 인한 업무 중단사태가 발생하면 재해복구시스템 관련자들은 비상연락에 의거하여 신속하게 연락을 취하고 각자가 맡은 역할을 수행하여야 한다. 재해에 대한 보고가 최초로 접수되면, 이를 각 복구 요원에게 통보하고, 피해정도를 파악하여 재해를 선언한다. 이에 대한 주요 내용은 다음과 같다.

□ 비상통지

재해는 사전 징후가 있을 수도 있고 없을 수도 있다. 예를 들면, 폭풍이나 컴퓨터 바이러스 등은 사전 징후가 있을 수 있지만 설비 장애나 범죄 행위 등은 사전에 예측이 불가능하므로, 두 경우 모두를 대비하여 비상연락방법이 문서화되어 있어야 한다. 또한, 비상통지 절차에는 특정 복구 팀원에게 통지가 불가능할 경우를 대비한 대체 절차가 정의되어 있어야한다. 재해발생 사실은 지체 없이 피해사정을 담당하고 있는 비상대책반 등에 통지되어야 한다. 비상통지 내용은 일반적으로 다음 사항을 포함한다.

- 재해 발생 일시, 재해 유형 등 재해 발생내역
- 인적/물적 피해정도를 포함한 대략적인 피해 규모
- 비상소집 일정 및 장소

□ 피해상황 파악

재해발생 시 재해복구시스템으로의 전환 여부를 결정하기 위하여, 그 시스템에 대한 피해의 파급효과를 평가하는 것은 중요한 작업이다. 피해상황 파악은 일반적으로 다음 사항을 포함한다.

- 재해의 원인
- 추가적인 피해 잠재성
- 피해지역 및 설비상태
- IT 가용자원 파악
- IT자원 및 데이터의 피해종류
- 교체될 IT 자원
- 재해로 인한 예상 중단지속시간

□ 재해선언

재해선언의 기준은 다음 사항을 종합적으로 고려하여 수립하여야 하며, 피해상황 파악 후, 재해 선언의 기준에 의해 재해가 선포된다.

- 인적/물적 피해의 정도
- 재해의 파급효과 정도(물리적, 운영상의 피해, 피해금액 등)
- 업무 시스템의 중요성
- 장애의 지속시간

나. 재해 복구 활동

재해선언 단계를 통해 비상대책반이 재해를 선포하면, 해당 시점부터 최단시간내에 재해복구센터로 서비스를 전환하여야 한다. 이 단계를 재해복구활동이라고 하며, 재해복구 활동은 서비스의 전환을 통해 서비스가 재가동되는 것을 확인하고, 재해복구센터에서의 장기 서비스 수행을 위한 준비 및 주센터의 복구활동을 수행하는 것을 포함한다. 또한 전환 작업은 재해복구센터 운영자가 실시하는 것을 원칙으로 한다. 복구를 책임지고 수행하는 팀은 평상시 지속적인 모의훈련을 통하여 숙련되었기 때문이다.

□ 재해복구센터로의 서비스 전환

재해가 선언되면 최단시간 내에 정해진 재해복구 역할과 절차에 의해 재해복구센터로 서비스를 전환해야 하며, 이는 다음과 같은 활동을 포함한다.

- 임원진, 전산실장 등이 주도하는 비상대책반 가동
- 예상복구시간 보고
- 재해복구시스템 전환 준비 및 전환
- 서비스 재가동
- 재해복구시스템 정상유무 체크
- 가능/불가능 업무 파악, 보고
- 상실데이터, 어플리케이션 동작 확인
- 예외상황 대응
- 통신망 전환 및 모니터링
- 체계적인 대외공표 및 홍보활동
- 긴급물자, 필요자원 조달 및 승인

□ 주센터 복구활동

재해복구센터로의 서비스 전환이 완료된 이후, 주센터의 복구를 위하여 다음과 같은 활동을 수행한다.

- 주센터 피해상황 파악/복구 방안마련
- 복구관련 필요인원 조달, 인사조치
- H/W, S/W 공급지원업체에 복구 촉구
- 복구불능시 조달계획 수립(선 조치 후 조달 품의)
- 주센터 복구시기 산정 및 복구센터 운영방안 마련

다. 주센터 복귀

재해복구계획에 의하여 재해복구센터에서 서비스가 이루어지고 있는 동안 주센터에 대한 복구 활동을 통하여 주센터가 정상화되었을 경우, 주센터로 복귀하는 절차가 수행되어야 한다. 주센터가 복구되는 데 소요되는 시간은 상황에 따라 매우 다르다. 하루 이내에 복구할 수도 있고(공조기 장애, 전원 장애 등), 수일 내지 수개월이 소요되거나 복구가 불가능할 수도 있다. 재해복구계획은 주센터로의 복귀절차를 명시하여야 하며, 주센터의 복구가 불가능할 경우에는 재해복구센터가 주센터가 되고, 새로운 재해복구센터를 구축하여야 한다.

다음과 같은 사항에 유의하여 주센터로의 복귀를 결정하여야 한다.

- 주센터의 파손이 심각한 수준인 경우, 주센터를 복구하는 방안과 재해복구센터에 시설 및 자원을 확충하여 주센터로 활용하는 방안을 비교하여 결정하여야 한다.
- 기존 주센터로의 복귀시 재해복구센터로 전환되었던 원인이 모두 해결되었는지 확인하여야 한다. 업무의 센터간 이동은 결코 간단하지 않은 문제이므로, 재해와 관련된 모든 문제가 완전히 해소되지 않은 상태에서는 주센터로 복귀하여서는 안 된다.
- 주센터로의 복귀 역시 데이터의 정합성, 서비스의 안정성, 보안의 확보 등의 요소가 고려되어야 하며, 주센터 복귀 후 빠른 시간 내에 재해복구센터와 재해복구시스템이 재가동될 수 있도록 하여야 한다.

주센터로 복귀하기 위한 활동은 다음과 같다.

- 주센터 안정화/정상화 검증
- 복귀 방안 준비 및 시기 결정
- 복귀를 위한 시스템 및 네트워크 구성
- 복귀 후 재해복구시스템 재구성

7.3 재해복구 모의훈련 수행

가. 모의훈련의 필요성

재해시 재해복구센터로 재해복구시스템 전환 및 주센터로의 복귀에 이르기까지의 절차를 숙지하고 정기적으로 재해복구시스템의 정상 실행여부를 확인한다. 이때 주센터에 대한 영향은 최소화하도록 한다. 다만 필요시 유관기관의 협조를 통하여 주센터의 관련 시스템 가동을 모의훈련 시간 중 중지할 수 있다. 훈련을 실시할 때는 다음 사항에 중점을 두어 실시한다.

- 계획의 목적
- 팀간 업무협의 및 의사소통
- 복구절차 보고
- 보안 및 미비사항 도출
- 팀별 역할 및 절차 숙지
- 개인 임무 및 절차 숙지

나. 모의훈련 수행 원칙

재해복구 모의훈련은 년 2회 이상 실시할 것을 권고한다. 모의훈련 중 발생하는 개선사항은 즉시 수정, 조치하여 차기 모의훈련 때 재발하지 않도록 한다. 일정은 정기적으로 하는 것을 원칙으로 하되, 필요시 비정기적으로 훈련을 실시하여 재해복구시스템의 유효성 및 즉시성을 점검하는 것이 좋다. 훈련은 실제 상황과 유사하게 할수록 좋다.

모의훈련시 관련조직의 필수인원은 모두 참여하는 것을 원칙으로 하되 문서검토 수준의 훈련은 전산실 담당자 및 관리자 수준에서 실시할 수 있다.

다. 모의훈련의 수준별 유형

모의훈련수준이 높아질수록 더 많은 세부 사항에 대한 점검과 검토가 이루어져야 하므로 더 많은 노력과 수고가 필요하게 된다. 따라서 상이한 수준의 모의훈련을 적절히 혼합, 배치한 모의훈련 스케줄에 따라 훈련하는 것이 효율적으로 재해에 대비하는 방법이라 할 수 있다. 모의훈련의 수준에 따라 다음과 같은 유형이 있다.

□ 체크리스트(Checklist) 훈련

재해복구를 위한 계획서를 검토하는 것으로 시스템 구성 변경 발생시, 다른 부서와의 기능적 공유 확인 등의 사유에 따른 확인 및 자체적인 평가를 위해

행하여지는 훈련이다. 함께 모여 훈련하기 보다는 문서와 절차 위주의 훈련으로 시간과 노력을 줄일 수 있으나 의사소통 부족으로 상호 이해가 부족할 수 있다.

□ 역할수행(Role Play) 훈련

역할수행 훈련은 재해 상황별 시나리오에 의해 관련 담당자들이 담당하고 있는 역할과 행동절차를 수행하는 훈련이다. 이 방법은 시스템 환경, 인력 운영 등의 이유로 모의전환 또는 실전환 훈련을 실시하기 어려운 경우, 또는 모의전환 훈련 또는 실전환 훈련의 사전검토 단계로 수행할 수 있다.

□ 모의전환 훈련

모의전환 훈련은 주센터 시스템의 운영을 지속하면서 재해복구 시스템을 가동하여 재해복구시스템이 적절히 가동되는지, 실제 단계별로 전환 수행이 적절히 이루어지는지, 두 시스템간 데이터 정합성이 보장되는지 등의 절차와 기능을 검토하는 훈련을 의미한다. 따라서 이 방법은 대부분의 재해복구 모의훈련에서 채택하는 방법이며 년 2회의 재해복구 모의훈련의 수준은 모의전환 훈련 수준 이상으로 실시하는 것이 좋다.

□ 실전환 훈련

주센터 시스템의 운영 가동을 중지하고 재해복구시스템을 실 업무에 전환하여 투입하는 수준이다. 이 경우 재해복구시스템을 가동한 후 변경된 데이터를 주센터 시스템으로 완벽하게 복구가 가능한 경우에만 수행한다. 만일 재해복구센터로 전환한 시스템의 변경된 데이터를 안정적으로 주센터로 복귀하기 어려운 환경이면, 실전환 훈련의 수행은 권장하지 않는다.

실전환 훈련은 가장 이상적인 방법의 재해복구 모의훈련이며, 이 수준을 만족해야만 재해복구시스템이 완벽히 구축되었다고 볼 수 있다.

다. 모의훈련의 절차

재해복구 모의훈련을 위해서는 철저한 사전준비가 필요하다. 사전준비는 재해복구 계획의 실행 가능성, 효율성 등을 판가름하고, 미비한 사항을 사전에 식별하여 보안하기 위하여 수행한다. 재해복구 모의훈련 중 점검할 사항은 다음과 같다.

- 재해복구시스템의 데이터 정상 복구 유무
- 복구팀의 지휘 및 조정 체계
- 내/외부 의사소통 여부

- 재해복구시스템 성능
- 주센터 복귀 유효성
- 통지 절차 및 기타 제반사항

재해복구 모의훈련 계획서에는 일정과 조직 및 참여 인원, 훈련 범위 및 시나리오가 상세하게 명시되어 있어야 한다. 재해복구 모의훈련 계획서는 시스템 명령어 수준까지 세부적으로 작성되어야 한다. 또한 각 업무별 체크리스트와 담당자와 비상연락망이 명시되어야 한다.

재해복구 훈련의 일반적인 절차 및 수행 내용은 다음과 같다.

<표 7-5> 재해복구훈련 절차 및 수행내용

① 체크리스트 훈련 ② 역할수행 훈련 ③ 모의전환 훈련 ④ 실전환 훈련

순서	훈련방법	수행 내용	주관부서	훈련유형별 해당여부			
				①	②	③	④
1	사전준비	- 업무영향도 파악 - 일정 및 방법 협의 - 관련 상세 작업계획 작성 및 승인 - 재해복구시스템 점검 및 미진사항 조치	관련 실무 담당자	✔	✔	✔	✔
2	재해선언	- 재해선포 및 통보 (주센터, 재해복구센터)	비상대책반			✔	✔
3	재해복구 시스템가동	- 재해복구시스템 가동작업 실시 : DB, Server, APP, N/W 포함	시스템, 네트워크, 업무담당			✔	✔
4	업무테스트	- 자체테스트 실시, 정상유무 판단	업무담당			✔	✔
5	재해복구 시스템 실 업무전환	- 모의전환 훈련시에는 실 업무 전환 안함	시스템, 네트워크, 업무담당				✔
6	정상여부 모니터링	- 재해복구센터 업무 수행여부 모니터링	시스템, 네트워크, 업무담당			✔	✔
7	재해복구 시스템 중단	- 재해복구시스템 가동중지	시스템, 네트워크, 업무담당			✔	✔
8	업무복귀	- 주센터 복귀작업 실시	시스템, 네트워크, 업무담당				✔
9	결과정리	- 일정, 절차, 훈련결과 정리 - 미진사항 확인 및 조치	관련 실무 담당자	✔	✔	✔	✔

7.4 운영시 기타 고려사항

재해복구시스템 구축 및 운영시 실제 발생할 수 있는 상황을 고려하여야 한다.

가. 시스템 및 네트워크 측면

재해복구의 시스템 측면에서 가장 중요한 사항은 실제 재해 발생시에 재해복구시스템으로 전환이 실제로 가능하여야 한다는 점이다. 다음과 같은 사례는 반드시 지양되어야 한다.

- 재해복구시스템 구성시 기술적 또는 비용적 문제로 재해복구 시스템을 형식적으로 구축하여 실제 재해 발생시 시스템 용량부족, 시스템 환경 상이, 기타 여러 가지 제약 조건으로 제대로 재해 복구가 이루어지지 못함

- 실제 상황발생시 서비스를 투입하지 못하는 모의훈련용, 규정 회피용, 대외홍보용 시스템을 구축

- 시스템이 잘 구축되어 있어도 재해복구용 서비스 네트워크 망이 재해복구센터와 사용자간, 시스템과 시스템간에 유효하게 구축되어 있지 않음

- 재해복구용 서비스 네트워크를 평시에 사용하지 않는 이유로 구축에서 제외되거나 정상 운영이 불가능할 정도로 낮은 수준으로 구축하는 경향

나. 운영 및 관리측면

재해복구시스템의 운영 및 관리 측면에서는 다음과 같은 사항이 고려되어야 한다.

- 재해복구 훈련과 같이 계획된 전환뿐 아니라 언제 어느 때 전환결정이 내려져도 원래 계획되어 있는 시간 내에 정상 전환이 되도록 평소에 훈련이 되어 있어야 한다.

- 특히 모의훈련에는 주센터 운영인력이 아닌 재해복구센터 운영인력이 실제 전환업무를 수행하여야 한다. 주센터 재난의 경우에는 주센터 운영인력의 정상투입이 보장되지 않기 때문이다.

- 시스템과 데이터, 네트워크 뿐 아니라, 관련 어플리케이션, 업무 수행 보조기능(백업, 배치 자동 스케줄링, 기타 주요 보조 Tool 등)도 언제든지

전환이 가능하도록 평소에 운영하여야 한다.

- 이러한 일련의 활동들이 최대한 자동화될 수 있도록 구성하되 자동화한 재해복구시스템 운영체계가 정상상태인지 주기적으로 확인하여야 한다.

- 재해복구시스템에 대한 주기적인 검증 및 테스트가 실시되어야 하며, 실시결과를 보고하고 미진사항을 수정해 나가야 한다.

- 시스템이나 업무 운영환경은 계속 변화하기 때문에 재해복구시스템이 구축 당시 정상 운영되었다고 해서, 실제 재해상황 발생시에도 정상 전환된다는 보장은 없다.

다. 유지보수

비즈니스 요구사항의 변경, 기술 발전 및 내/외부의 정책변화 등 여러 가지 사유로 IT 환경에서는 지속적으로 변화가 발생한다. 재해복구 계획은 이렇게 끊임없이 변화하는 운영 아키텍처의 실제상황을 반영할 수 있어야 한다. 따라서 재해복구시스템의 요구사항, 절차, 조직의 구조를 주기적으로 확인하고 변경 작성하여야 한다. 재해복구시스템의 유지보수에서 중점적으로 관리하여야 하는 사항은 다음과 같다.

- 운영 요구사항
- 보안 요구사항
- 기술적인 절차
- IT자원 및 설비
- 팀원/공급업체의 연락정보
- 복구관련 주요 문서

라. 기타 고려사항

재해복구 계획의 유효성을 보장하기 위하여 다음 항목도 고려하여야 한다.

- 재해복구센터 및 외부 백업센터 계약 사항 및 이용가능 기간
- 공급업체 및 서비스 제공업체의 MOU, SLA
- H/W, S/W 요구사항
- 시스템 연계 협약
- 보안 요구사항
- 복구 전략
- 훈련 교재, 시험 계획
- 기반시설의 확보

표준작성 공헌자

표준 번호 : TTAS.KO-10.0259

이 표준의 제·개정 및 발간을 위해 아래와 같이 여러분들이 공헌하였습니다.

구분	성명	위원회 및 직위	연락처 (Tel, E-mail)	소속사
과제 제안		공공정보 프로젝트그룹		TTA
표준 초안 제출		공공정보 프로젝트그룹		TTA
표준 초안 검토	이헌중	공공정보 프로젝트 그룹 의장	02-2131-0446 hjlee@nia.or.kr	한국정보사회진흥원
		외 프로젝트그룹 위원		
표준안 심의	이헌중	IT 응용 기술위원회 의장	02-2131-0446 hjlee@nia.or.kr	한국정보사회진흥원
		외 기술위원회 위원		
사무국 담당	김선	팀장	031-724-0080 skim@tta.or.kr	TTA
	강석규	대리	031-724-0326 redorb@tta.or.kr	TTA

정보통신단체표준

정보시스템 재해복구 지침
(Guideline for Disaster Management of Information Systems)

발행인 : 김원식
발행처 : 한국정보통신기술협회
463-824, 경기도 성남시 분당구 서현동 267-2
Tel : 031-724-0114, Fax : 031-724-0119
발행일 : 2007. 12