

# 정보시스템 백업현황과 구축방법에 관한 연구

주우철\*, 최홍식\*\*

\*데이콤 시스템테크놀로지, \*\*국민대학교 정보관리학부

## A Study on the Current Status and Implementation Methods of the Backup Centers for Information Systems

Joo, Woo Chul\*, Choi, Heung Sik

DACOM System Technologies, Kookmin University

E-mail : ikarus@sqtech.net, hschoi@kookmin.ac.kr

### 요약

본 논문에서는 DRS(Disaster Recovery Services)와 데이터 백업 서비스를 근간으로 하는 정보시스템 백업센터의 개념과 현황 및 요소기술과 솔루션을 소개하고 구축방법에 대한 방안을 제시한다. 특히 공공부문의 기간정보시스템 공동백업센터 구축 사례를 바탕으로, 백업구축 프로세스와 운영사례를 제시하여 향후 백업시스템 진화 방향의 틀을 제공한다.

### 1. 서론

정보시스템 백업센터 구축의 필요성은 단순한 데이터복구 차원을 넘어 자연적 재해, 인위적 위협, 사이버 테러로부터 중요 정보시스템의 생존력 확보를 위한 대비책으로 물리적, 기술적, 관리적 보호조치도 포함되어야 한다[2,6].

정보시스템의 대한 의존도가 지속적으로 증가됨에 따라 재해로 입게되는 피해 규모가 증가하고 있다. 특히 기업이나 국가기간의 경우에는 사업목표달성에 치명적 손상을 입히는 것은 물론 업무중단, 고객이나 국가 신뢰도하락 등의 영향으로 조직의 존립에 위협을 받을 수 있다.

그러므로 정보시스템을 안정적으로 운영하기 위한 투자가 증가하고 있는 추세로서 전세계 재해복구시장에서 스토리지 소요량이 IT예산의 5%~17% 이상의 높은 성장을 전망하고 있다[16]. 또한, SAN(Storage Area Networks)과 NAS(Network Attached Storage) 등 새로운 아키텍처의 등장으로 “엔터프라이즈 스토리지”라는 개념이 일반화됨

에 따라 향후에도 많은 투자와 수요가 늘어날 전망이다[10,16].

최근 정보통신부는 전자정부 특별위원회를 열고 국가 기간 정보시스템 공동백업센터 구축계획안을 확정하였다. 정보통신부, 행정자치부, 국세청 등 관련부처가 모두 이 계획을 공동으로 추진하게 되는데 주민등록정보시스템, 국세통합정보시스템, 수출입통관정보시스템, 시군구 행정정보통합시스템 등이 백업대상으로 지정된 바 있다[1,3].

공공기관 및 기업이 보유한 정보를 “언제, 어디서나, 어떤 방법으로든 효과적으로 제공될 수 있도록 한다”는 의미는 정보시스템의 가용성을 전제로 한다. 그러므로 정보서비스의 지속적 관리(BCM : Business Continuity Management)의 개념에서 백업센터 구축이 요구된다[6,17].

이와 같은 관점에서 국내환경에 적합한 데이터 센터 구축이나 정보시스템 백업센터 구축과 관련되어 좋은 가이드나 프레임 워크, 모델 개발에 대한 연구가 매우 미비한 실정이다. 따라서 본 논문에서는 재해복구시스템 및 데이터 백업서비스를

기반으로 하는 백업센터의 형태나 백업방식을 비교하고, 구축 솔루션들의 특징을 분석하여, 보다 체계적이고 일관성 있는 백업센터 구축을 위한 백업센터 구축 프로세스를 도출한다. 또한 국가기간 정보시스템 백업센터 운영사례를 바탕으로 백업센터 운영모델을 제시하고자 한다.

## 2. 백업센터의 현황

### 2.1 백업센터 정의 및 동향

백업센터란 “인재 또는 천재지변 등의 원인으로 정보 시스템에 장애가 발생하여 정상적인 업무 처리가 불가능할 경우를 대비하여 지역적으로 분리된 장소에 대체 전산 시스템 및 제반 설비를 준비하여 장애 또는 재해시 업무 중단을 최소화하기 위한 시스템”이다.

IT산업에서의 재해(Disaster)는 “전산시스템에 의한 정보제공 등이 감내할 수 있는 시간”을 초과하여 장애가 지속되는 경우로 정의되는데 여기에서 감내할 수 있는 시간이란 기업의 특성과 업무에 따라 달라질 수 있다[26,28].

이와 같이 정보시스템의 장애나 재해요인은 첫째, 자연재해로 지진, 태풍, 홍수와 같은 자연적인 작용에 의한 재해이며 둘째, 인적재해로서 정전, 화재, 테러, 무단점거 등이 있고 셋째, 시스템 장애로 각종장비(UPS, 항온 항습기, 공조기) 및 통신장애, 전산시스템 및 각종 주변기기의 고장, 시스템 운영을 위한 소프트웨어 장애, 컴퓨터 바이러스, 해커에 의한 시스템 파괴, 운용요원의 실수 등이 있다.

IBM BRS(Business Recovery Service)센터 사례에 의하면 1981년부터 1998년까지 전산장애나 재해로 인한 서비스 제공사례 251건 중 자연재해와 인적재해가 74%, 시스템장애의 비중이 25% 규모로 나타났다[2].

정보시스템의 주요 위험요소들에 장애가 발생할 경우 그 피해정도를 파악하는 것이 “사업영향 분석(Business Impact Analysis)”이다[6,8]. 위험요소로는 전산시설 파괴, 서비스 중지와 지연, 거래 처리 오류 및 정보자산 손실 등이 있다. 이러한 위험요소에 대한 피해는 생산성손실, 이익소실, 고객상실, 복구비용 등 직접피해와 대외신뢰도, 국가신뢰도 하락 등으로 간접피해로 분류된다.

이와 같이 정보시스템의 장애·재해에 대한 피해정도는 조직의 생존과 직결된다. 따라서 피해에 대한 대책이 필수적인 요소이므로 국내·외 백업센터와 공공부문의 데이터센터(PDC : Public Data Center) 1) 추진현황을 살펴본다[3].

국내 백업센터 구축은 주로 금융권에서부터 증가하고 있지만 선진국의 경우에는 모든 산업에 걸쳐서 구축되어가고 있으며, 보다 안정적인 운영과 온라인 화되는 기업활동에 발맞춰 실시간 미러 사이트(Real Time Mirror Site) 방법<sup>2)</sup>으로 운영하고 있다.

영국, 프랑스, 독일, 싱가포르 등의 중앙은행과, 지진 등 피해가 많은 일본과 미국, 유럽의 다수의 은행들도 백업센터를 가동하고 있다.

국내의 경우 금융정보화 추진분과위원회에서 “금융정보화 안전대책 기준”을 제정하였고 “금융정보화 안전대책 강화방안”에 의거 세부시행 계획 및 비상대책을 수립하여 강력히 권고하여, 최근 국내 일각에서는 백업센터를 구축하는 사례와 구축을 위한 검토작업이 활발하게 진행되고 있다.

백업센터와 유사한 형태로 미국의 “공공데이터 센터”에 관한 조사를 보면 1998년을 시점으로 BIDC

(Business and Industry Data Center) 프로그램으로 50개 주의 주 데이터센터(State Data Center)를 구축하고 연방정부의 데이터 센터와 연계하여 각 주로부터 수집되는 각종정보를 분석, 연구하여 각 주에서 공동활용 자료로서 내려주는 형태로 구성된다[3].

또한 지역적으로 ABAG(Association of Bay Area Government)를 구축하였는데, 샌프란시스코 일대의 9개의 주 정부 또는 지역정부가 abagonline(access to bay area governments online)이라는 네트워크를 통하여 정보공동 활용을 하고 있다[7,12].

1) 대부분 국외 공공부문에서의 정보 공동 활용을 목적으로 하는 전산시스템에 대한 용어는 공공부문 데이터 센터로 정의하지 않고 전자정부의 개념으로 사용하고 있으나 본고에서는 이를 공공부문 데이터 센터로 정의한다. 미국에서는 주 데이터 센터(SDC : State Data Center)라는 용어를 사용하고 있다.

2) 메인 센터와 동등한 시스템을 갖춘 대체센터를 준비하여 데이터의 갱신이 메인 센터와 백업센터에서 동시에 이루어져 재해 시에도 즉시 복구가 가능한 방식.

## 2.2 백업센터의 구축형태

정보시스템 백업센터의 구축은 궁극적으로 업무의 지속성(Business Continuity)을 보장하여야 하며, 백업센터의 운영 형태와 백업방식의 선택에 따라 업무 지속성 관리의 수준이 달라질 수 있다.

따라서 백업센터의 운영 형태와 백업방식이 백업센터 구축 수준을 결정하는 중요한 요소이므로 이에 따른 장단점과 백업방식을 다음과 같이 살펴본다..

### 가. 운영형태에 의한 구분

백업센터를 운용하는 형태에 따라서 자영 센터 방식, 공동 이용 센터 방식, 상호 이용 센터 방식, 대행처리 센터방식으로 <표 1>과 같이 구분되며, 각 형태별로 장단점이 있으므로 운영형태의 선택에 따라 투자규모나 운영조직과 운영방법이 달라질 수 있다[20,23].

<표 1> 백업센터 운영형태 비교

방식	내용	장점	단점
자영센터	백업센터를 독자적으로 구축하여 운영.	운영이 용이	구축·유지 비용과다
공동이용	업무의 내용 및 보유장비가 유사한 조직이 합동으로 백업센터를 구축 운영.	투자비용 절감 기술교류	보안문제 투자의 형평성
상호이용	지역별로 동일 기관간을 상호 연결하여 긴급시에 서로에게 백업기능을 제공	투자비용 절감 기술교류	보안문제 호환성 추가구입
대행처리	IDC나 외부 전문용역회사에 위탁하여 백업시스템을 가동하는 방식	비용절감 중복투자 방지	보안상의 문제 신뢰성

### 나. 백업방식에 의한 구분

백업방식에 의한 구분은 장애·재해 시 복구수준의 완성도에 따라 미러 사이트(Mirror Site) 방식, 핫 사이트(Hot Site) 방식, 워م 사이트(Warm Site) 방식, 콜드 사이트(Cold Site) 방식으로 나눌 수 있다. 이 구분은 전산재해로부터 복구시간까지 얼마나 빠르게 정보시스템을 복구하는가에 초점을 두고 있으며, 자료백업 시간, 전산시스템 및 통신망 구축여부 등을 비교하면 <표 2>와 같다 [19,22,26].

<표 2> 백업 방식 비교

백업방식	최장복구용시간	셋업시간	자료백업시간	전산시스템구축여부	통신망구축여부
미러사이트	4시간	없다	발생 즉시	○	○
핫사이트	1일	짧다	주기적 온라인 백업 (10분~1시간)	○	○
웜사이트	1주	중간	주기적 오프라인 백업 (1일~1주일)	○	×
콜드사이트	수개월	길다	주기적 오프라인 백업 (1주일~1개월)	×	×

미러 사이트 방식은 메인 센터와 동등한 시스템을 준비하여 실시간으로 기록되는 데이터를 메인 센터와 백업센터 시스템에 동시에 제공하여 재해 시에도 즉시 복구가 가능한 방식이다. 그러나 이 방법은 투자비용이 과다한 단점이 있다.

핫 사이트 방식은 주요 데이터 및 시스템과 어플리케이션 환경을 실시간에 원격지에 복제해 재해시 단시간 내에 재해 발생 시점까지의 데이터를 유실 없이 복구하는 방식이다. 미러 사이트 방식에 비해 복구시간이 긴 단점이 있다.

웜 사이트 방식은 콜드사이트에 비해 발전된 형태인데 로그 데이터를 원격지에 복제해 재해시점까지의 로그데이터를 이용하여 주요데이터의 소실을 방지하는 방식이다. 비용이 비교적 저렴하나 복구기간이 비교적 긴 단점이 있다.

콜드 사이트 방식은 백업센터에 전산부대설비만 구축하여 두고 재해 발생시점에 전산 기기를 도입하는 형태로 비용측면에서는 저렴하나 실제 재해 발생 시 완전한 복구가 어렵고 시간이 너무 많이 걸린다는 단점이 있다.

## 2.3 백업센터 구축 도구(Solution)

백업센터 구축의 수준을 향상하기 위해서는 백업센터의 운영형태나 백업방식에 따라 적절한 방식을 적용해야 하나 어떤 백업시스템 솔루션을 사용하느냐에 따라 백업구축 수준, 비용, 성능, 효율성이 크게 달라질 수 있다. 그러므로 각 솔루션을 정확하게 파악하여 비용 대비 효과를 최대화 할 수 있는 방법을 선택하는 것이 중요한 과제라 할 수 있다.

백업시스템 솔루션은 보유하고 있는 데이터를 원격지의 백업시스템으로 복제하는 방법인데 크게 동기방식과 비동기방식으로 구분할 수 있다.

동기방식은 메인 센터와 백업센터에서 업데이트가 하나의 프로세싱으로 처리되므로 거리에 따른 성능저하나 신호 지연시간의 한계로 인한 통신거리 제한 문제가 발생한다. 또한 시스템 자원에 뿐만 아니라 응용프로그램 까지 영향을 주는 경우도 있다.

반면에 비동기방식은 운영에 따른 구현비용이 높지만 거리, 성능, 데이터의 정합성 측면에서 안정적이고 효율적이다[24].

백업시스템 구축 솔루션은 <표 3> 과 같이 호스트나 서버를 이용하는 시스템 미러링(S/W적인 방법)과 시스템을 이용하지 않는 디스크 미러링(H/W적인 방법)으로 나눌 수 있다[28,30].

시스템 미러링 방법은 실시간으로 복구가 가능하며 네트워크의 부하가 적은 장점이 있지만 시스템에 다소 영향을 주고 소프트웨어 유지보수 비용이 발생하는 단점이 있다.

시스템 미러링은 다시 데이터를 송수신하는 주체에 따라 운영체제(OS) 기반과 DBMS 기반의 2가지 솔루션으로 나누어진다.

첫째, 운영체제 기반의 솔루션은 운영체제가 디스크에 기록되는 데이터를 꺼내어 원격지로 전송하는 방법이다. 현재에는 유닉스 플랫폼에서 구현이 가능하며 IBM인 경우에는 HAGEO가 대표적인 솔루션이며 HP, SUN에서는 베리타스 리플리케이션 등이 있다

둘째, DBMS 기반의 솔루션은 DBMS의 로그(Log)를 원격지로 전송하는 방법으로 동기방식도 존재하나 거의 대부분이 비동기 방식을 사용하고 있다[20,27].

<표 3> 백업센터 구축 솔루션

구분		솔루션 방식		복제 데이터
시스템 미러링 (S/W방식)	OS 기반	HAGEO	IBM 유닉스	DBMS, 파일 시스템
		GEORM	HP, SUN 유닉스	
	DBMS 기반	Veritas Replicator	DB2	DB2, 오라클 DBMS
		RRDF	ORACLE	
디스크미러링 (H/W방식)	SRDF	EMC	모든 파일 시스템	
	HRC	HITACHI		
	XRC	IBM		

디스크 미러링 방법은 디스크 미러링을 이용하여 데이터의 동기를 유지하므로 시스템과 무관하게 데이터를 원격지로 마이그레이션이 가능하다. 하드웨어에 의한 단순구성으로 높은 안정성을 유지하지만 실시간 복구가 어렵고 네트워크의 구축 및 운용에 따른 비용이 지나치게 소요되며 네트워크 부하에 영향을 미치는 단점이 있다

## 2.4 백업센터 구축 도구의 특징분석

일관성 있고 합리적인 백업센터를 구축하기 위해서는 다양한 백업시스템 솔루션을 검토하여야 하며 결론적으로 적용 가능한 시스템 솔루션을 선택해야 한다. 따라서 <표 3>에서 기술된 솔루션 방식별로 각각의 특징을 아래와 같이 정의하였다.

### 1) HAGEO(High Availability Geographic Cluster)

HAGEO는 디스크의 내용을 다른 지역 사이트의 대응되는 디스크에 하나이상의 네트워크를 통해 미러링하는 고 가용성 솔루션이다. 이것은 지오그래픽 미러링(GMD)에서 응용프로그램을 마치 로컬 볼륨에서 실행하는 것처럼 지오그래픽 미러링 드라이버(Geographic Mirroring Driver) 디바이스에 읽기 및 쓰기의 응답을 보내는 것으로, HAGEO는 응용 프로그램에서 투명하다고 말할 수 있다.

또한 HAGEO는 장애 발생시 중요한 서비스와 데이터의 빠른 복구 기능을 제공한다. 모든 형태의 DB와 파일을 지원하고 어떠한 TCP/IP 기반의 네트워크에도 사용 가능하다. 장애의 발견과 복구를 위하여 HACMP(High Availability Cluster Multiprocessing)와 통합되며 RS/6000 AIX HACMP 환경에서 구동되어지고 응용프로그램의 변경이 불필요하다[20].

### 2) GeoRM(Geographics Remote Mirroring)

GeoRM은 어플리케이션 수정 및 거리의 제한 없이 지정된 볼륨의 데이터를 실시간으로 이중화할 수 있으며, GeoMirror, GeoMessage, GeoManager의 컴포넌트로 구성되어있다.

GeoMirror는 메인센터에서 백업센터로 미러링 기능을 제공하고, GeoMessage는 양 센터의 디스크간의 메시지 송수신을 담당하며, GeoManager는 GeoRM 구성 및 관리를 위한 도구로 스크립터 작성 및 모니터링 등의 기능을 제공한다[20].

### 3) RRDF(Remote Recovery Data Facility)

미국 E-NET사의 RRDF 솔루션은 백업센터 구축시 다양한 형태의 IBM DBMS에 대해 즉각적인 복구가 가능하도록 설계된 것으로 MVS 시스템에서 운영이 되며, DBMS 영역과 연결되어 데이터 복구에 필요한 로그(Log) 및 저널(Journal)을 수집하고 원격지에 위치한 백업사이트에 SNA/VTAM<sup>3)</sup> 통신을 이용하여 전송한다.

백업 사이트에도 메인 사이트와 동일한 이중화 데이터베이스를 생성하여 평상시에는 읽기만 할 수 있도록 하여 사용한다.

주요 특징은 DBMS의 로그를 비동기방식으로 원격지 사이트에 전송하므로 시스템에 부하가 적고 장애 발생에 유연하게 대처 할 수 있으며 데이터 압축이나 필요한 로그 데이터만을 전송하므로 네트워크와 같은 자원의 비용이 적게 소요된다.

### 4) ORACLE Symmetric Replication

오라클 시메트릭스 리플리케이션<sup>4)</sup>에는 단방향 복사만이 가능한 Read-only Snapshot과 양방향 복사가 가능한 시메트릭스 리플리케이션으로 나눌 수 있다.

Read-Only 스냅샷은 한쪽 데이터베이스에서의 변경 사항에 대해서 다른 데이터베이스내의 스냅샷은 읽기만 가능하며, 분산환경 중의 한 노드에 있는 마스터 테이블에 대한 Read-Only 스냅샷을 로컬사이트에 유지하고 주기적으로 마스터 테이블의 변경된 내용을 데이터 레벨로 복제한다.

이에 반대하여, 시메트릭스 리플리케이션은 마스터와 로컬사이트 양쪽의 복사본 모두를 변경 가능

하고, 각 변경된 내용을 같은 리플리케이션 환경에 포함된 데이터베이스에 스키마 레벨로 복제한다.

### 5) ORACLE SharePlex

셰어플렉스(SharePlex)는 오라클의 온라인 리두 로그(Redo log)를 읽어서 대체될 테이블의 해당 정보를 압축된 SQL형태로 큐(Queue)에 저장한 후 자체 네트워크나 TCP/IP를 통해 백업시스템으로 전송하고 전송된 SQL 트랜잭션은 이후 프로세스를 통해 테이블에 반영시키는 전환솔루션이다.

주요특징은 백업시스템의 데이터베이스에 항상 접근이 가능하며, 메인 센터의 시스템 영향을 최소화하며, 오라클의 데이터 유형을 지원하고 일관성, 유연성, 관리성이 용이한 점이다.

### 6) SRDF(Symmetrix Recovery Data Facility)

SRDF는 두 대 이상의 시메트릭스 스토리지간에 호스트나 네트워크 자원을 전혀 사용하지 않으면서 메인센터에서 백업센터로 고속 통신연결을 통해 실시간에 가동중인 시스템의 전체 또는 일부 데이터를 디스크 레벨에서 고속으로 이중화한다.

SRDF는 호스트 플랫폼과는 독립적이며, 물리적으로 메인센터와 백업센터간에 분산 운영되는 디스크 데이터 이미지를 미러화 하여 실시간 백업을 한다.

SRDF는 세가지 방식으로 적용이 가능한데 동기식, 반동기식, Adaptive Copy가 있다.

동기식은 근거리 구축에 사용되며 완벽한 데이터 이중화 구현시 사용하는 방법이며, 반동기식은 원거리 구축에 사용되며 원격지 업무가 고성능을 요구할 때 사용하며, Adaptive Copy는 원거리 구축에 사용되며 데이터를 일시에 다량 전송할 경우 사용하는 방식이다.

### 7) HRC(Hitachi Remote Copy)

HRC는 메인 센터내의 스토리지 시스템에 저장된 데이터를 백업센터에 복제본을 생성하고 관리하는 솔루션으로 데이터 복제본을 이용한 어플리케이션 테스트, 백업 및 재난 복구용으로 활용할 수 있다.

메인센터 내의 원본 볼륨은 모든 호스트에 읽기 및 쓰기 입출력이 가능한 상태로 계속 존재하면서, 현재의 운영 상태에 영향을 주지 않고 백업센터내

3) SNA(Systems Networks Architecture)은 IBM의 메인프레임 네트워크 표준이다  
VTAM(Vertex Telecommunication Action Method)은 데이터 통신용 프로그램작성을 쉽게해주는 특수한 데이터 통신소프트웨어 패키지로 원격통신방법이다.

4) 리플리케이션(replication)은 복사, 복제라고 번역되는 것으로, 오라클은 이것을 분산 데이터베이스상에서 테이블 등의 데이터베이스 오브젝트를 여러 데이터베이스로 복사하여 유지하는 기법을 지칭한다.



의 복제본 볼륨과의 페어(Pair) 성립, 해제와 재 동기가 가능하고, 또한 가상볼륨(Virtual Logical Volume Image), 캐시 상주 볼륨(Flash Access) 등 특수 목적의 볼륨들도 원본 볼륨으로 사용이 가능하다.

HRC는 세가지 방식으로 적용이 가능한데 동기식, 반동기식, 비동기식이 있다.

동기식은 높은수준의 데이터 정합성을 갖는 볼륨 레벨의 복구를 위하여 사용하며, 반동기식은 장거리 데이터 전송에 사용되며, 구성이 단순하고 데이터 손실이 발생할 가능성이 있으나, 비동기식은 성능보호 및 데이터의 정합성을 보장하는 방식이다.

### 8) XRC(eXtended Remote Copy)

XRC는 축적 및 전송(Store-and-Forward) 방식을 사용한 원거리 재해 복구 솔루션으로 적용업무 시스템의 디스크 서브시스템(디스크 제어기)으로 기록되는 데이터들이 디스크 제어기내의 캐시에 저장되었다가 일정량이 축적되면 원격지 시스템과 통신하여 비동기전송방식으로 데이터를 고속으로 복사하는 기술이다 [27].

이상과 같이 각각의 백업솔루션을 <표 4>에서 솔루션 방식에 따라 제공회사와 각 솔루션의 시스템제공 환경, 하드웨어 및 소프트웨어 기반환경, 국내 제공사례, 데이터 복제 단위 등에 대하여 비교하였다

본 논문에서 논의되지 않은 많은 솔루션이 있으나 기술자료가 방대하기 때문에 가장 많이 사용되는 대표적인 솔루션에 대해 백업시스템 구현 방법에 따라 분류하고 논의하였다.

<표 4> 백업센터구축 도구의 비교

솔루션 방식	제공사	적용분야		기술분야		국내사례	복제 단위
		M/F	UNIX	H/W	S/W		
HAGEO GEORM	IBM		○		○	N/A	볼륨
Veritas Replicator	Veritas		○		○	N/A	볼륨
RRDF	E-NET	○			○	서울,경남은행	DB
Symmetric Replication SharePlex	Quest		○		○	신영증권	DB
SRDF	EMC	○	○	○		대우자동차, 신한은행, 아시아나항공, 외환은행	볼륨
HRC	Hitachi	○		○		정보통신부, 삼성캐피탈	볼륨
XRC	IBM	○		○	○	삼성생명/화재 SKT 등	볼륨

## 3. 백업센터 구축 프로세스와 운영모델

2 장 에서 논의된 백업센터 구축을 위한 각 솔루션

별 특징을 분석하였다. 이는 다양한 정보시스템 환경에서 목적에 적합한 솔루션을 선택하고 올바른 백업시스템을 구축할 수 있도록 가이드를 제공하기 위함이다.

본고에서는 2 장에서 논의된 솔루션을 배경으로 백업센터 구축을 위한 전체 프로세스를 고찰하기 위하여 국가기관 정보시스템의 공동백업센터 구축 프로젝트를 추진하는 과정에서 연구된 결과를 바탕으로 백업센터 구축절차와 운영모델을 다음과 같이 정의한다.

### 3.1 백업센터 구축 프로세스

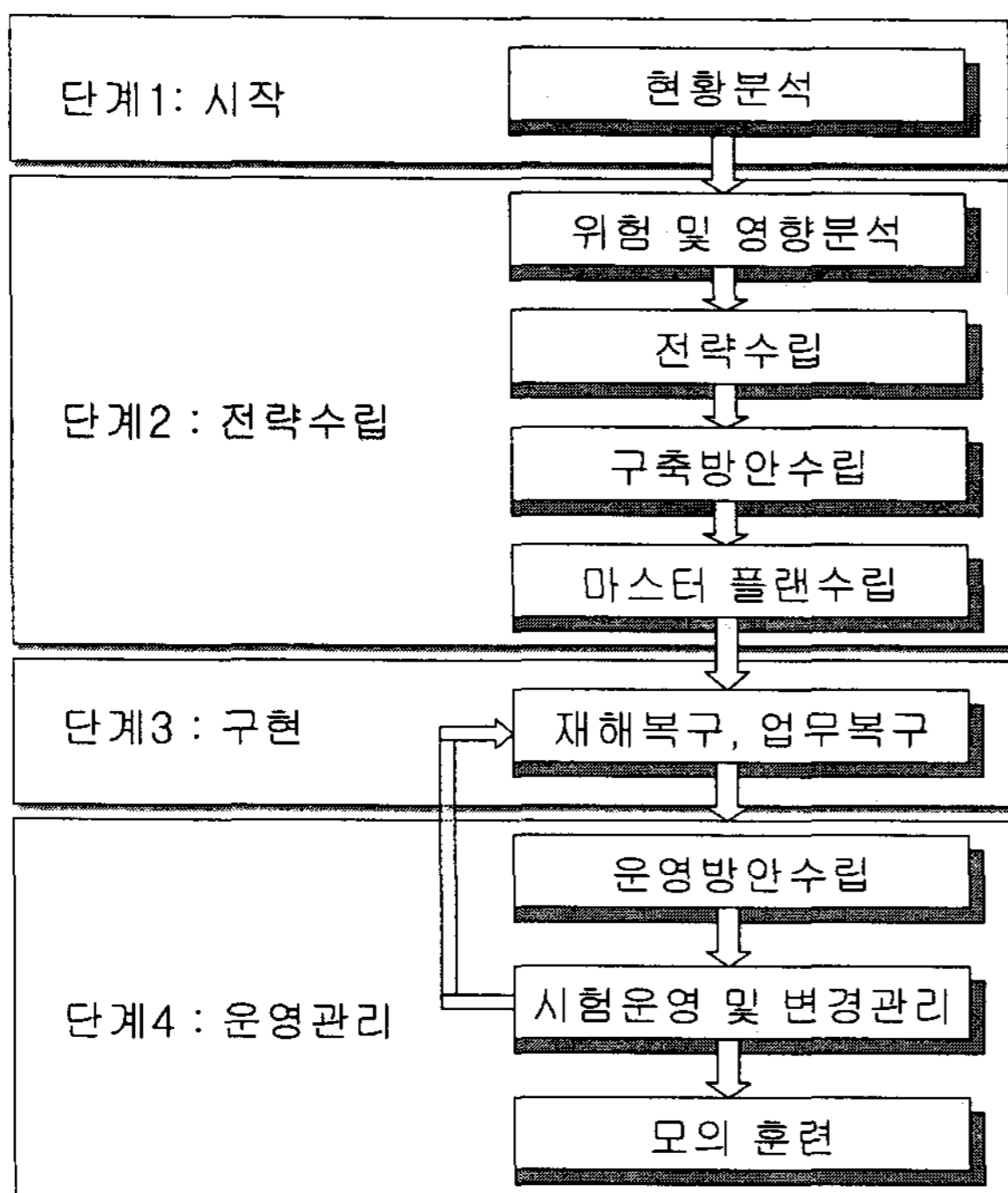
백업센터 구축 프로세스<sup>5)</sup>는 <그림 1>과 같이 단계적 접근방법으로 4 단계의 생명주기로 시작 단계, 전략수립 단계, 구현 단계, 운영관리 단계로 구성되고, 각 단계별로 구체적인 활동은 다음과 같다.

- 1) 현황분석에서는 업무의 정의 및 업무별 특성 파악과 재해시 파급영향 등을 분석하는 프로세스이다. 또한 시스템, 네트워크, 기반설비 현황, 장애관리, 백업관리, 운영현황을 분석하여 백업/복구 프로세스를 평가하고 개선과제를 도출한다.
- 2) 위험 및 영향분석에서는 위험을 정의하고 분류하며 피해 내용 및 규모를 분석한다. 또한 시스템, 네트워크, 기반설비 위험분석, 단위 업무별 피해 규모 및 위험영향평가를 하여 그에 따른 대응방안을 선정한다.
- 3) 전략수립에서는 업무 및 시스템 분석을 토대로 업무의 복구 범위와 목표를 설정한다. 또한 위험 및 영향 분석을 통해 도출된 복구 목표시간을 기준으로 백업센터 기술형태 및 복구대책을 수립하고 재해복구 대책 및 백업전략을 수립한다.
- 5) 본 프로세스는 1998년 11월 한국전산원 보고서 “공공기관 정보시스템을 위한 비상계획 및 재해복구에 관한 연구”와 “IBM Total Storage Solutions for Disaster Recovery”를 참고하였으며 최근 국가 기관 정보시스템의 공동 백업센터 구축을 위한 프로젝트에서 본 절차를 적용하였다.

- 4) 구축방안수립에서는 현황 분석과 위험 및 영향 분석을 토대로 시스템 구조를 설계한다. 백업 센터간 백업 회선, 사용자 우회 네트워크 설계, 회선 용량, 소요자원 등의 네트워크 구조설계, 백업센터 기반설비설계, 테스트 계획, 조직, 절차 및 테스트 시 백업기술 운영방안 등을 수립한다.
- 5) 마스터 플랜수립에서는 시스템, 네트워크, 기반 시설의 각 분야별 업무수행 추진과제 선정 및 분야별 실행을 위한 조직을 구성하고 실제 구현을 위한 종합적인 계획을 수립하고 각 조직원들의 역할을 분담한다.
- 6) 재해복구, 업무복구 단계에서는 구축할 장비의 이상유무를 점검하고 백업센터의 전기, 공조, 보안시설 등의 기반설비를 적합하게 설치한다. 또한 메인센터와 백업센터간의 백업솔루션 환경을 설정하고 구축된 환경에 적합한 테스트 일정 및 시나리오를 수립한다. 시나리오에 기술된 환경에서 각 전산 기기 및 백업 솔루션에 대한 테스트를 실시하고 테스트시 발생된 결함

업표준을 수립한다 또한 재해 발생시 업무서비스 재개를 위한 대응절차 및 시스템 가동 절차를 수립하고, 재해종료 후 업무 서비스를 정상 가동하기 위한 복귀 절차를 수립한다.

- 8) 시범운영 및 변경관리에서는 구축 후 안정적인 운영을 위해 백업시스템 및 센터 가동개시 전 시범운영을 실시하고 변경내역이 있을 경우 재해복구,업무복구 단계로 되돌려 변경사항을 처리한다.
- 9) 모의훈련에서는 모의실시를 위한 각 역할을 분담하여 메인센터와 백업센터의 운영인력을 구성하고 시스템 및 네트워크 부문의 훈련 시나리오 작성한다. 모의훈련시 훈련목적에 부합되는 훈련절차를 작성하고 모의실시를 위한 데이터를 준비한다. 백업센터에서 업무서비스를 가동하고 네트워크를 전환하여 각 업무별로 테스트를 실시한다. 백업시스템의 정상가동 여부가 확인되면 모의훈련을 종료하고 모의훈련의 효과성 평가 및 분석을 통하여 복구절차를 보완 수정한다.



<그림 1> 백업센터 구축 프로세스

에 대하여 보완작업을 한다.

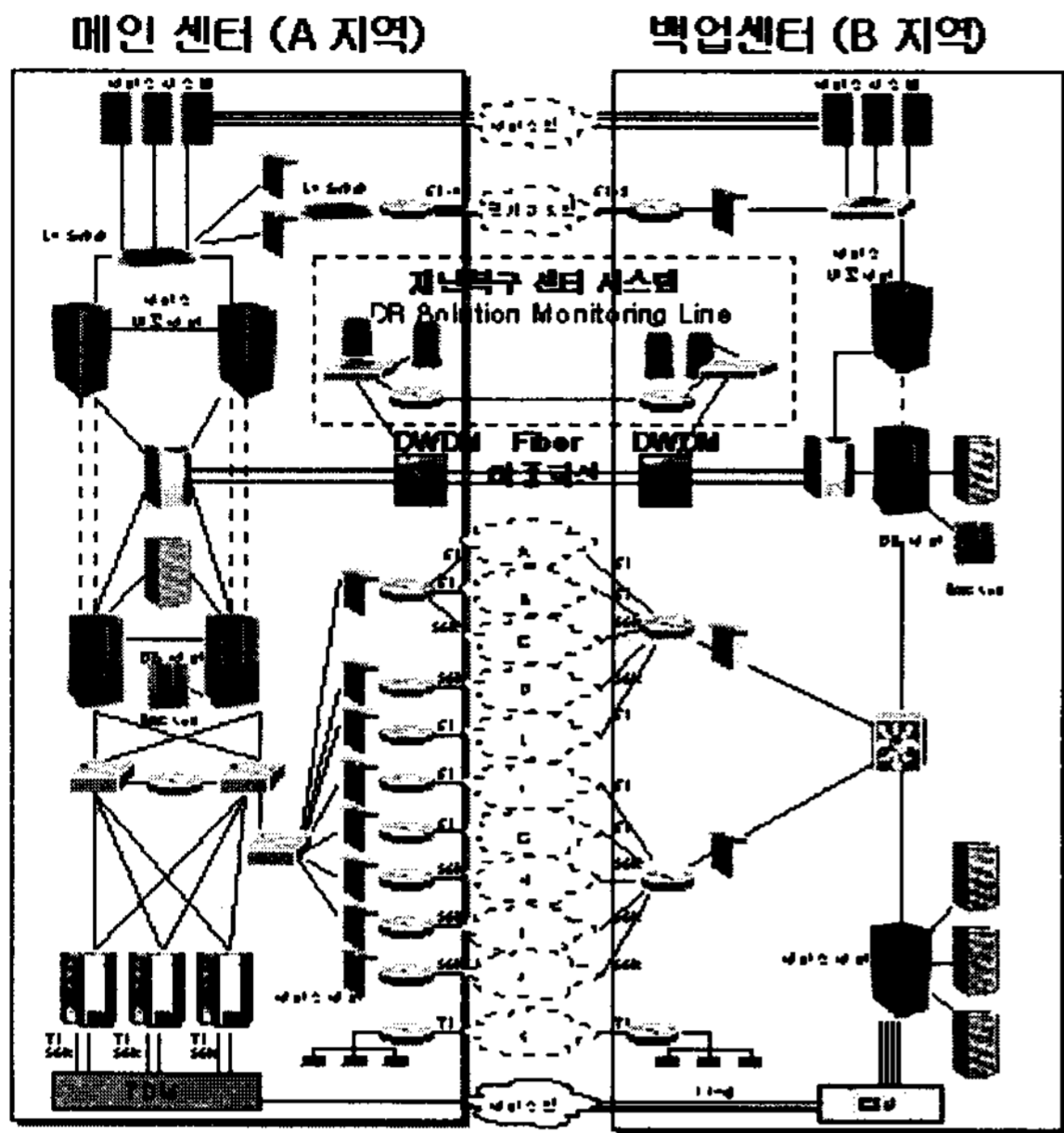
- 7) 운영방안수립에서는 백업센터의 평상시 운영조직체계와 재해시 비상조직체계를 수립한다. 백업센터 운영 기준과 운영업무 및 세부 운영절차를 수립하고, 시스템자원의 도입 및 할당, 시스템운영 및 관리표준, 사용자 관리표준 및 백

### 3.2 백업센터 운영모델

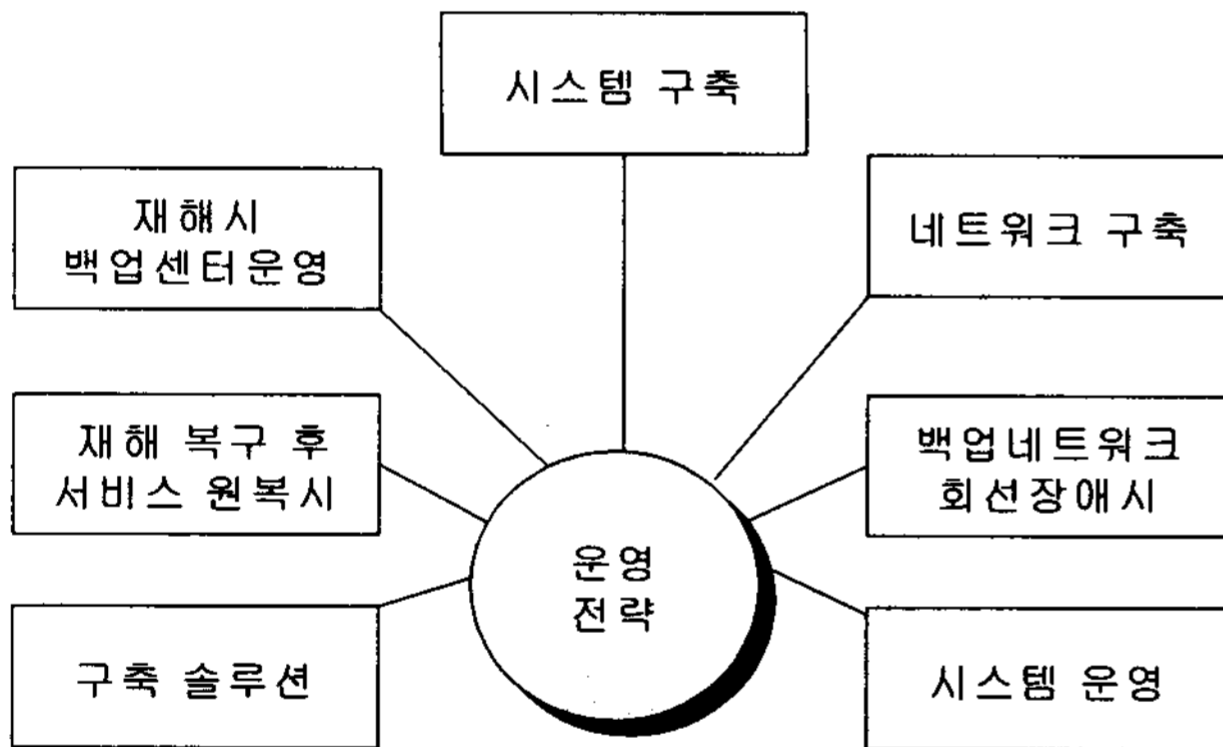
<그림 2>는 국가 기간정보시스템의 공동백업센터 구축의 일례를 도시한 것으로 3.1 장에서 논의된 백업센터 구축 프로세스를 적용하여 만들어진 백업센터 구축 사례이다. 이것은 SRDF 동기방식의 백업 솔루션을 사용하여 메인센터와 백업센터간에 네트워크 구성을 DWDM<sup>6)</sup> 이중화 화이버 채널(Fiber Channel)으로 연결한 시스템이다.

본 장에서는 3.1 장에서 논의한 백업센터 구축 프로세스에 의해 구축된 백업센터를 효율적으로 운영할 수 있는 모델을 <그림 3>과 같이 운영전략과 운영 방안별로 8가지로 모델링 하였다. 각각의 구성요소는 시스템구축, 네트워크 구축, 백업네트워크 회선장애, 시스템 운영, 데이터 백업, 구축 솔루션, 재해복구 후 서비스 원래 상태로 복구 시 방안, 재해시의 백업센터 운영으로 구성된다. 여기서 운영전략은 백업센터에서 제공하고자 하는 서비스 수준이나, 백업의 강도 등 백업센터 설립 목적에 타당하게 정의되어야 할 것이다.

6) DWDM(Dense Wavelength Division Multiplexing) : DWDM은 다른 곳에서 온 여러 종류의 데이터를 하나의 광섬유에 함께 실는 기술로서, 각신호들은 분리된 고유의 광파장 상에서 전송됨



<그림 2> 백업센터 구축 일례



<그림 3> 백업센터 운영모델

각 모델들의 운영절차나 운영방법에 대하여 다음과 같이 정의한다

1) 운영전략

첫째, 메인센터의 재해시에 주어진 시간 내에 백업센터에서 정상 서비스 가능하도록 한다. 둘째, 메인센터와 백업센터간 데이터의 복구를 위한 구축 솔루션은 SRDF 솔루션으로, 동기식 방식을 운영하여 데이터 정합성을 유지한다. 셋째 스토리지 간 백업네트워크의 장애시 SRDF 솔루션을 로컬모드로 변경하고 백업네트워크 복구 후에는 SRDF 솔루션을 동기식으로 재 가동하여 복구 시까지 데이터 정합성 유지한다. 넷째, 데이터의 테이프 백업은 메인 센터에서 하고 백업된 테이프는 백업센터 및 원격지에서 소산 관리한다.

2) 구축 솔루션

<표 5>에서와 같이 각종 서비스 제공에 대한 서비스데이터를 실시간으로 미러링 하기 위한 백업 솔루션이 SRDF 이고 동기식을 사용하고 있다.

<표 5> 구축솔루션

서비스내용	구축 솔루션	구축 환경	구축내용
각종 서비스	SRDF	동기식	서비스 데이터 실시간 미러링

3) 시스템 운영

시스템 운영은 <표 6>과 같이 메인센터의 재해시 백업센터에서는 스토리지간 데이터 실시간 미러링을 중단하고 백업센터의 서비스프로그램과 DBMS를 가동한다.

<표 6> 시스템 운영

내용	평상시	재해시
메인 센터	<ul style="list-style-type: none"> <li>○전산서비스 운영</li> <li>○서버 가동 및 점검</li> <li>○DBMS 운영</li> <li>○SRDF 가동, 점검</li> <li>○백업네트워크 점검</li> <li>○백업네트워크 장애시 SRDF 로컬모드로 변경</li> <li>○서버/스토리지 장애조치, 기술지원</li> </ul>	<ul style="list-style-type: none"> <li>○재해복구 활동</li> </ul>
백업 센터	<ul style="list-style-type: none"> <li>○시스템 서버준비</li> <li>○SRDF 점검</li> <li>○백업네트워크 점검</li> <li>○백업데이터 점검</li> <li>○서버/스토리지 장애조치, 기술지원</li> </ul>	<ul style="list-style-type: none"> <li>○서비스 프로그램 가동 및 점검</li> <li>○DBMS 가동 및 운영</li> <li>○SRDF 중단</li> <li>○서버/스토리지 장애조치, 기술지원</li> <li>○서비스프로그램 운영</li> </ul>

4) 네트워크구축

네트워크 구축은 <표 7>과 같이 백업센터에서 서비스 프로그램과 DBMS를 가동 후 네트워크 회선을 점검한다.

<표 7> 네트워크 구축

구분	평상시	재해시
메인 센터	<ul style="list-style-type: none"> <li>○네트워크서버가동, 점검</li> <li>○네트워크서버 성능 및 사용자 분산 접속 상태 점검</li> <li>○네트워크 장비 가동</li> <li>○NMS 운영</li> <li>○장비/회선 장애조치 및 기술지원</li> </ul>	<ul style="list-style-type: none"> <li>○재해 복구 활동</li> </ul>
백업 센터	<ul style="list-style-type: none"> <li>○네트워크서버준비운영</li> <li>○네트워크 장비 운영</li> <li>○외부기관 연결 회선 점검</li> <li>○NMS 운영</li> <li>○장비/회선 장애조치 및 기술지원</li> </ul>	<ul style="list-style-type: none"> <li>○네트워크서버가동, 점검</li> <li>○네트워크서버 점검</li> <li>○네트워크 장비 가동 및 점검</li> <li>○NMS 운영</li> <li>○장비/회선장애조치 및 기술지원</li> </ul>



5) 데이터 백업구축

데이터 백업구축은 <표 8>과 같이 평상시에는 메인센터에서 현재의 백업정책으로 테이프 백업을 운영하고 백업센터에서는 데이터를 테스트용으로 운영한다.

재해시에는 백업센터에서 테이프 백업을 운영한다. 그리고 백업된 테이프는 메인센터, 백업센터, 원격지 이동 보관으로 소산 관리한다.

<표 8> 데이터 백업구축

구분	평상시	재해시
메인센터	<ul style="list-style-type: none"> <li>○ 백업장비 가동 점검</li> <li>○ 백업정책 관리</li> <li>○ 정기적, 비정기적 테이프 백업 수행 및 데이터 확인 및 복구 테스트</li> <li>○ 백업 테이프 소산 관리 (메인센터, 백업센터, 원격지)</li> <li>○ 백업장비 장애 조치 및 기술 지원</li> </ul>	<ul style="list-style-type: none"> <li>○ 재해 복구 활동</li> </ul>
백업센터	<ul style="list-style-type: none"> <li>○ 백업장비 가동 점검</li> <li>○ 필요시 백업 데이터 복구 테스트</li> <li>○ 백업 테이프 보관</li> <li>○ 백업장비 장애 조치 및 기술 지원</li> </ul>	<ul style="list-style-type: none"> <li>○ 백업장비 가동 점검</li> <li>○ 백업정책 관리</li> <li>○ 정기적, 비정기적 테이프 백업 수행 및 데이터 확인 및 복구 테스트</li> <li>○ 백업 테이프 소산 관리</li> <li>○ 백업장비 장애 조치 및 기술 지원</li> </ul>

6) 재해시 백업센터 시스템 운영

평상시 SRDF 동기식 모드 운영하고; 실시간 데이터 미러링 유지하면서 메인센터 재해 발생시, 메인센터의 복구 환경 점검한다. 백업센터의 서비스용 서버, DBMS, 서비스 프로그램 가동하고, 백업센터의 데이터 및 서비스 프로그램을 확인한다.

7) 백업 네트워크 회선 장애시 시스템 운영

평상시 SRDF 동기식 모드 운영하고, 실시간 데이터 미러링 유지하면서 백업 네트워크 회선장애 발생시, 스토리지간 SRDF를 로컬 모드로 변경하고 백업네트워크 회선장애를 복구한다. 또한 스토리지간 SRDF를 동기식 모드로 변경하고, 백업센터 스토리지에 대해 장애시간동안 변동 데이터를 복구하고 실시간 데이터 미러링을 유지한다.

8) 재해복구후 서비스 원복시 시스템 운영

메인센터의 복구 환경을 점검하고 백업센터의 서버 및 서비스용 서버, DBMS, 서비스 프로그램을 중단한 후 백업센터에서 메인센터로 데이터를 복구하고 메인센터의 서버 및 서비스용 서버,

DBMS, 서비스 프로그램을 가동한다. 또한 메인센터의 복구된 데이터와 서비스 프로그램을 확인하고 스토리지에 SRDF를 가동한다.

4. 결론 및 향후과제

본 논문에서는 정보시스템 재해에 대비하기 위한 백업센터 구축에 관한 동향과 다양한 솔루션 및 기술적 특징을 통하여 백업시스템의 정확한 이해와 최적의 솔루션 선택 할 수 있는 방안을 제공하였다.

또한 보다 일관성 있는 구축방안을 도출할 수 있도록 백업구축 프로세스에 의해 구축된 사례를 바탕으로 백업센터 운영모델을 제시함으로써 향후 백업센터 구축시 지침을 제공하였다.

백업센터의 구축모델의 필요성은 최소의 비용으로 최대의 재해복구 효과를 얻을 수 있는 방안을 도출하는 것이 목적이므로 백업센터의 설립 취지와 목적에 가장 부합하는 솔루션을 선정해서 백업센터를 구축하는 것이 보다 중요하다.

본 논문의 한계점으로 본 논문에서 제시한 백업센터 구축프로세스나 운영모델이 다양한 사례에 의해 도출되지 못하였고, 또한 기존의 연구와 비교 검증이 되지 않은 한계가 있다. 따라서 향후 과제로 본 논문에서 제시하고자 한 백업센터 구축절차나 운영 모델에 타당성을 검증하는 절차를 연구하여 보다 일반적인 모델이 되도록 하는 것이다. 또한 백업센터 구축시 백업의 구축 강약에 따라 백업의 수준을 다르게 적용될 수 있는 수요자 중심의 모델을 만드는 연구가 필요하다.

[참고문헌]

[1] 강영석, “시군구 행정종합정보시스템 구축에 관한 연구”, 서울산업대학교 전자계산학과 석사학위논문, 1998.8  
 [2] 김용수, “정보시스템 장애·재해 대비를 위한 백업체계 구축에 관한 방안연구”, 성균관대학교 정보통신공학 석사학위논문, 2001.4.  
 [3] 데이콤시스템테크놀러지, “공공데이터센터(PDC) 구축을 위한 선행연구 용역보고서”, 2002.3  
 [4] 정보통신정책연구원, “공공 및 민간부분의 정보화를 위한 위성통신 활용방안연구”, 1999.12  
 [5] 이성일, “IT 비상계획 수립을 위한 업무영향분

- 석 프로세스 및 기법에 관한 연구”, 중앙대학교 산업 정보학과 정보시스템 공학 석사학위논문, 2001.12
- [6] 한국전산원, “공공기관 정보시스템을 위한 비상계 계획 및 재해복구에 관한 연구” 1998
- [7] 한국전산원, “공공부문 데이터센터 구축방안 및 경제성 분석에 관한 연구”, 2000. 12
- [8] 한국전산원, “행정전산망 안전관리 현황 및 분석”, 1995. 12
- [9] “A Model for Disaster Recovery Planning” Yiu K., Sze Y.Y. V 1995 p 45
- [10] “*Business Continuity: Information Processing Disaster Recovery Planning*” Menkus B. I 1994 p 36
- [11] Book Review: “*Disaster Recovery Planning*” Hernandez P.Q. (Reviewer) III 1997 p 18
- [12] “*Data Center Survives the 1992 Los Angeles Riots*” Larson L.L. I 1994 p 18
- [13] “*Good Planning Saves Information and Ensures Speedier Recovery: Disaster Recovery Following the Los Angeles Earth-quake*” Patterson S. I 1994 p 14
- [14] IS Security Matters: “*Business Continuity planning and e-Business*” Ross S., CISA and Connell J. II 1999 p 15
- [15] “Information Management & Computer Security”, Vol 3, No.1 pp.21-27
- [16] Lehman Brothers, Equipping the Data Center : Servers & Storage, Oct 2, 2000 Enterprise Hardware 1~17
- [17] Product Review: “*Contingency Planning for the Year 2000*” Khan K. (Reviewer) II 1999 p 10
- [18] “Recent Industrial Developments of VPN(Virtual Private Network)”, 전자통신동향분석 vol.14 no.6, 1999. 12
- [19] “IBM Total Storage Solutions for Disaster Recovery”  
<http://www.redbooks.ibm.com/redpieces/pdfs/sg246547.pdf>
- [20] “Disaster Recovery Using HAGEO and GeoRM”  
<http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg242018.pdf>
- [21]  
[http://www.mge.com/business/security/disaster\\_recovery.htm](http://www.mge.com/business/security/disaster_recovery.htm)
- [22] <http://www.sisait.co.kr/column/200108/buyers/cs-hana.htm>
- [23] <http://www.sisait.co.kr/column/old/200004/choice/136.htm>
- [24] <http://www.drexperts.com/products/planning.asp>
- [25] <http://www.contingencyplanning.com/>
- [26] <http://www.hyosunginformation.co.kr/advantage/no63/docu14.html>
- [27] [http://www.emc2.co.kr/local/ko/KR/products/product\\_pdfs/ds/srdf.pdf](http://www.emc2.co.kr/local/ko/KR/products/product_pdfs/ds/srdf.pdf)
- [28] <http://www.hyosunginformationsystems.com/report/TechnicalReport.htm>
- [29] <http://publib-b.boulder.ibm.com/Redbooks.nsf/redbooks/>
- [30] <http://ns.koscom.co.kr/koscom06~09.html>
- [31] [http://www.oracle.com/kr/magazine/archive/22spring/index.html?t\\_note1\\_3.html](http://www.oracle.com/kr/magazine/archive/22spring/index.html?t_note1_3.html)