

재해복구시스템(DRS) 개선방안에 관한 연구 - 국내 금융권 재해복구시스템 중심으로 -

이건용*, 한정현**

*고려대학교 컴퓨터정보통신대학원 디지털정보공학과

**고려대학교 컴퓨터통신공학부

e-mail: *dolidoli@korea.ac.kr

**jhan@korea.ac.kr

A Study on the Improvement Plan of DRS (Disaster Recovery System)

- Focused on the DRS in Internal Financial Industry -

Keon-Yong Lee*, Jung-Hyun Han**

* Graduate School of Computer and Information Technology,
Korea University

** Dept of Computer Science & Engineering, Korea University

요 약

2001년 세계무역센터의 테러사건을 계기로 구축되기 시작한 국내 재해복구시스템(DRS)은 재해가 발생할 상황에서만 활용되고, 그 이외의 용도로는 사용되지 못하고 있기 때문에 시스템 활용률이 낮다. 이러한 점에 착안하여 본 연구에서는 재해복구시스템의 가용성 및 활용성을 높일 수 있는 방안을 제시하고자 한다. 재해복구시스템은 재해가 발생했을 때뿐만 아니라 시스템 장애나 테스트시스템, 웹 서버 및 재해복구 네트워크의 활용 용도로 확대 운영할 수 있음을 본 연구에서 보여준다. 또한 이미 구축된 재해복구시스템의 사용 현황을 분석하고, 재해복구시스템의 용도 개선 방안을 제시함으로써 향후 재해복구시스템의 가용성 및 활용도를 높이고자 한다.

1. 서론

2001년 9월 세계 경제의 중심지인 미국의 세계무역센터(World Trade Center)의 테러 사건을 계기로 국내에서도 BCP의 중요성을 인식하고 금융권의 재해복구시스템(Disaster Recovery System)에 대한 관심이 고조되기 시작했다. 2001년 정보통신부의 정보통신기반 보호법, 금융감독원의 재해복구센터 구축 권고(안), 2003년 비상시 금융기관 전산망 안전대책, 2006년 영업연속성계획(Business Continuity Plan) 모범규준(안) 등을 정부차원에서 발표하였으며, 이를 근거로 대부분의 금융기관이 재해에 대하여 영업연속성계획 및 재해복구체계 확립을 위한 노력을 지속적으로 진행하고 있다[1].

재해복구시스템의 가장 중요한 사항은 실제 재해 발생 시에 재해복구시스템으로 전환이 실제로 가능하여야 한다는 점이다. 규정 회피용 또는 대외 홍보용 등의 목적으로 재해복구시스템을 구축할 경우 실제 재해 발생 시에는 재해복구시스템의 용량 부족, 시스템의 환경 상이 등으로 재해복구시스템의 기능을 보장할 수 없게 된다.

재해복구시스템은 주전산시스템의 이중화만으로 완성되는 것이 아니며, 재해 시 재해복구시스템 유지를 위해서는

주전산센터에서 수행되는 일련의 모든 과정이 재해복구시스템 구성에 맞도록 이루어져야만 정상적인 운영이 가능하다 [3]. 또한 재해복구시스템 구축 후에도 지속적인 변경 관리와 연 2회 이상의 모의훈련을 통해 재해복구시스템의 기능을 확인하여야 한다[2].

이처럼 대부분의 재해복구시스템은 모의훈련과 재해시를 제외하고는 대기상태로만 유지하게 된다. 이는 많은 비용을 두고 구축한 재해복구시스템에 대해 전사적인 관심도의 저하를 가져오며 실제 재난상황이 발생하여 재해복구시스템으로의 전환이 필요한 경우 본연의 기능을 확인할 수 없는 재해복구시스템으로 전락하게 된다. 1년 몇 차례의 모의상황을 가정한 테스트만으로 재해복구시스템의 유효성을 확인하는 것은 어려운 것이며 평상시 모의훈련을 비롯하여 다양한 용도로 활용하여 사용함으로써 재해복구시스템의 기능을 확인해 가는 것이 중요하다.

일부 회사에서 재해복구시스템의 평상시 가용성 확대를 통한 유효성 확인을 위해 주전산시스템의 배치시스템 활용, 재해복구시스템에 시세전송과 같은 특정 기능부여, 주전산시스템의 벤치마킹시스템으로의 사용 등 제한적인 활용을 하고는 있으나, 재해복구시스템에 투자한 비용에 비하면 그

가치는 미미하다.

이에 본 논문에서는 이미 구축된 재해복구시스템의 사용 현황을 분석하여 보고, 재해복구시스템의 용도 개선 방안을 제시함으로써 향후 재해복구시스템의 가용성 및 활용도를 높이고자 한다.

2. 관련연구

본 장에서는 재해복구시스템의 개선방안의 관련 연구로 재해복구의 개념, 재해복구시스템의 유형과 특징, 재해복구시스템의 구현 기술에 대해 알아본다.

2.1 재해복구시스템의 개요

재해복구(Disaster Recovery)란, 재해로 인하여 중단된 정보기술서비스를 재개하는 것을 의미한다. 재해복구를 위해서는 사전에 정보기술서비스 기반에 대하여 재해가 발생하는 경우를 대비하여, 이의 빠른 복구를 통해 업무에 대한 영향을 최소화하기 위한 제반 계획이 필요하며 이를 재해복구계획(Disaster Recovery Planning)이라 한다. 이렇게 계획된 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(Disaster Recovery System)이라고 한다. 업무연속성계획(Business Continuity Planning)은 정보기술부분 뿐만 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[2].

2.2 재해복구시스템 유형

재해복구시스템의 유형은 구축형태 및 운영주체, 복구수준에 따라 구분할 수 있으며, 각 유형에 대한 정의는 문헌 및 전문가에 따라 다소의 차이가 있으며, 경우에 따라 복합적으로 사용되어질 수 있다. 유형별로 비교하여 보면 다음과 표와 같다[2].

<표 1> 재해복구시스템 유형과 특징(구축형태, 운영주체별)[2]

구분 기준	유형	설명	구축 비용	운영 비용	보안성	복구 신뢰성
구축 형태별	독자구축	기관 전용의 재해복구시스템을 독자적으로 구축	높음	높음	높음	높음
	공동구축	두 개 이상의 기관이 재해복구시스템을 공동으로 구축	중간	중간	중간	중간
	상호구축	복수의 기관 상호간 재해복구시스템의 역할 수행	낮음	낮음	낮음	낮음
운영 주체별	자체운영	기관 자체인력으로 재해복구시스템 운영	-	높음	높음	높음
	공동운영	두 개 이상의 기관이 재해복구시스템의 운영인력 공유	-	중간	기관간 협조에 의존적	
	위탁운영	재해복구시스템의 운영을 민간 IDC 운영자 등 외부의 다른 기관에 위탁	-	낮음	위탁운영자 신뢰도에 의존적	

<표 2> 재해복구시스템 유형과 특징(복구수준별)[4]

Site	설 명
Cold Site	평상시 주기적으로 주요 데이터를 테이프에 백업해 내화 금고에 보관하거나 원격지에 소산해 두었다가 재해 발생시 불능 상태의 시스템의 운영을 재개할 수 있도록 하는 방식이다.
Warm Site	콜드사이트에 비해 발전된 형태의 방식으로 평상시 주요 데이터를 테이프로 백업해 내화금고에 보관하거나 원격지에 소산하는 점은 동일하다. 하지만 로그 데이터를 실시간 원격지(Warm Site)에 복제해 재해시점까지의 로그 데이터를 이용해 주요 데이터의 손실을 방지하는 방안이다.
Hot Site	재해 복구 방안 중 가장 많은 투자가 필요한 방식이다. 일반적으로 핫 사이트 방식은 주요 데이터 및 시스템과 애플리케이션 환경을 실시간에 원격지에 복제해 재해 시 최단 시간 내에 재해 발생 시점까지의 데이터를 유실 없이 복구하는 방식이다.
Mobile Site	운영중인 서버나 System이 재해/재난 발생시 서버를 대체하기 위해 특정한 telecommunications 그리고 IT 장비 등을 임대 및 System을 지원해주는 방식이다.
Mirrored Site	메인센터와 동등한 시스템을 갖춘 대체센터를 준비하여 DATA의 갱신이 메인센터와 백업 센터에서 동시에 이루어져 재해 시에도 즉시 복구가 가능한 방식이다. 단기간 내에 복구/가동할 수 있는 장점은 있으나 중복 투자의 우려성이 있어 업무나 개발업무를 전담케 하고 유사시에 대체 시스템으로 전환하는 방법으로 효율성을 높이고 있다.

2.3 재해복구시스템의 구현 기술

2.2절에서 기술한 재해복구시스템의 구현 방식 중 본 논문에서는 최근 재해복구시스템 구현의 주류를 이루는 Mirror Site 재해복구시스템에 대해 설명하며, 재해복구시스템을 구성하는 방법은 다음과 같이 분류할 수 있다.

<표 3> 재해복구시스템 데이터복제기술의 유형[2]

구분	특징		
데이터 복제방식	H/W적 복제	물리저장장치(스토리지)의 전용 복제솔루션을 사용하여 복제	
	S/W적 복제	운영체제수준	서버에서 디스크로 데이터를 전송하고 저장하는 중간 단계에서 데이터 블록을 복제하여 재해복구 센터로 보내는 방식
		DBMS 수준	DBMS를 이용한 복제
데이터 전송방식	Sync(동기 복제)	주전산센터와 재해복구센터간 정합성 항상 유지, 신뢰성 높은 방식	
	Async(비동기 복제)	기존 운영서비스에 영향 무	
	기타 방식	Sync방식과 Async의 혼합방식으로 Async방식과 유사하다	

3. 재해복구시스템 사례 분석

본 장에서는 현재 운영 중인 재해복구시스템의 평상시 사용 사례를 조사·분석하여 본다.

3.1 M증권사의 재해복구시스템 활용 사례

주전산시스템의 백업과 대량의 배치작업시 생기는 부하

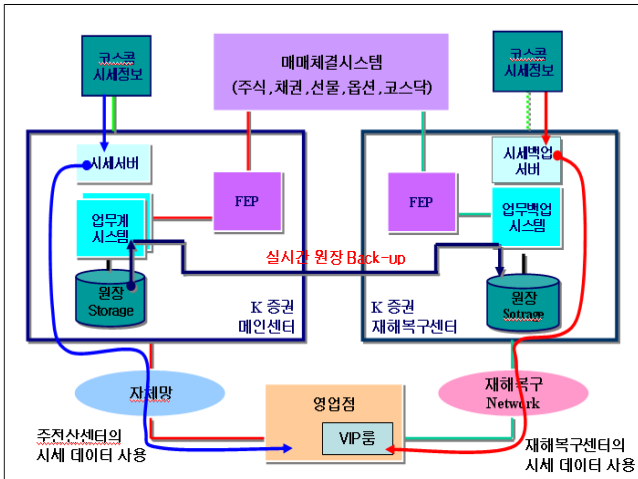
를 줄이기 위해 재해복구시스템을 이용해 백업에 활용하고 있다. 기존의 주전산시스템을 통한 야간작업(배치작업+백업)에서 데이터백업 부분을 재해복구시스템을 통해 실시하고 있다. 주전산센터에서는 배치작업을 수행하고, 재해복구센터에서는 데이터 백업을 실시함으로써 일일야간작업 시간이 단축되어졌고, 주전산시스템에 생기는 부하 또한 감소되어졌다.

<표 4> M증권사 재해복구시스템의 백업서버 활용

구분	야간작업소요시간	특징
변경전	- 배치작업(3시간)+백업작업(3시간)	- 동기화 중단 없음
변경후	- 배치작업(3시간)&백업작업(3시간) - 병렬수행+Replication Tool 조작 시간(1시간)	- Replication Tool 관련 1시간 추가 작업 소요 - 백업작업시 동기화 중단 발생 - 대량배치작업에 의한 주전산시스템 부하감소

3.2 K증권사의 재해복구시스템 활용 사례

증권사의 재해복구시스템은 증권정보 제공 회사인 코스콤으로부터 재해복구용 시세데이터를 별도로 제공받고 있다. 기존의 재해복구용 시세는 차단된 재해복구시스템 네트워크 안에서 의미 없이 브로드캐스팅 되어져 버려지는 데이터이며, 주전산센터의 시세 관련 장애나 재해 시에만 시세 데이터로서 사용되어진다. 이에 K증권사는 평상시 영업점의 VIP고객룸에 빠른 시세 제공을 위해 별도로 사용함으로써 재해복구시스템의 네트워크와 서버를 활용하고 있다.



<그림 1> K증권사의 재해복구시스템 시세 활용

4. 재해복구시스템 제안 모델

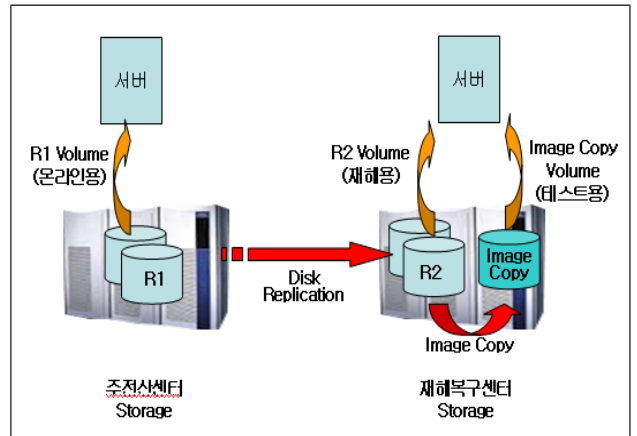
4.1 테스트시스템 활용 모델

재해복구센터 스토리지의 스냅샷(Snapshot) 알고리즘을 이용한 이미지카피(Image Copy)를 별도로 구성하여 재해복구센터의 테스트시스템으로 활용하는 모델이다. 주전산센터의 스토리지와 타겟스토리지간의 복제에는 전혀 영향을 미치지 않으며, 주전산센터에서 운영하는 테스트시스템의 역할을 대신할 수 있다. 이미지카피를 사용하므로 추가의 테

스트환경 구성작업이 필요 없으며, 주전산센터와 동일한 환경으로 사용이 가능하다. 이미지카피의 동기화는 주전산센터에 트랜잭션이 발생하지 않는 시간을 이용하여 재해복구센터 운영요원에 의해 주기적으로 실시함으로써 데이터 정합성을 유지시켜야 한다. 주전산센터의 테스트시스템을 운영하는 비용의 절감과 재해복구센터의 운영인력의 활용률을 높이는 데 기여한다[5,6].

<그림2>에서와 같이 재해복구센터의 스토리지에 이미지카피 볼륨을 별도로 두어 평상시 재해복구시스템을 테스트 시스템으로 활용할 수 있으며 R2->이미지카피 볼륨간의 동기화는 끊어져 있으며 R1->R2간 데이터 복제에는 전혀 영향을 미치지 않는다. 이때 R2 볼륨과 이미지카피 볼륨을 사용할 때 서로 다른 IP Address를 사용하여야 재해복구시스템의 기능을 유지할 수 있다.

재해시나 모의테스트 시에는 운영체제에서 테스트용 볼륨 정보를 제거하고, R2볼륨의 정보와 재해복구용 IP Address를 할당함으로써 재해복구시스템의 기능을 수행할 수 있다.



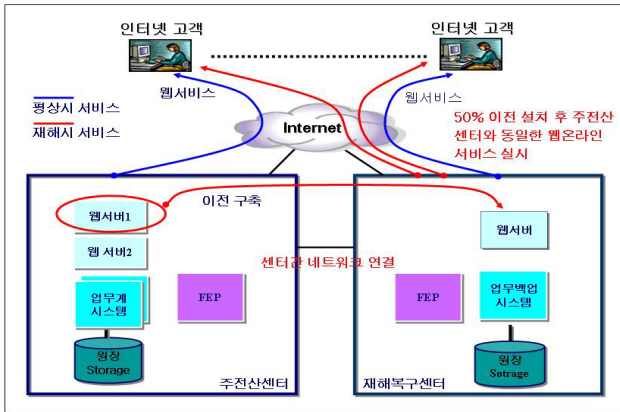
<그림 2> 이미지카피를 이용한 테스트시스템 활용

이미지카피볼륨을 테스트용으로 사용하기 위해서는 주전산시스템의 디스크 변경에 따른 지속적인 변경작업이 수반되어야 한다. 또한 운영체제에 디스크 관련 정보에 대해 환경설정을 평상시 해두어야 만이 필요한 시기에 필요한 용도로 사용할 수 있다.

4.2 온라인서비스 활용 모델

재해복구센터의 웹서비스 관련 재해복구용 서버를 실제 온라인 서비스에 활용하는 모델이다. 재해복구센터에는 재해 상황을 대비하여 약 50 ~ 70%정도 용량의 서버를 구축하여 놓는데, 이것을 대고객 온라인 서비스에 활용하는 것이다. 주전산센터에서 사용하던 웹서버의 50% 용량을 재해복구센터 구축 시 별도 구매 없이 이전 설치하여 활용함으로써 기존의 서비스에 영향을 미치지 않으면서 재해복구시스템 구축에 소요되는 비용을 절감 할 수 있다. 이것은 주전산센터에 설치된 웹서버의 용량이 사용량에 비해 2배정도 충분하게 설치되어진 경우에만 해당되며, 센터 간 로드밸런싱이 전제되어야 한다. 평상시 변경관리는 기존 웹 업무

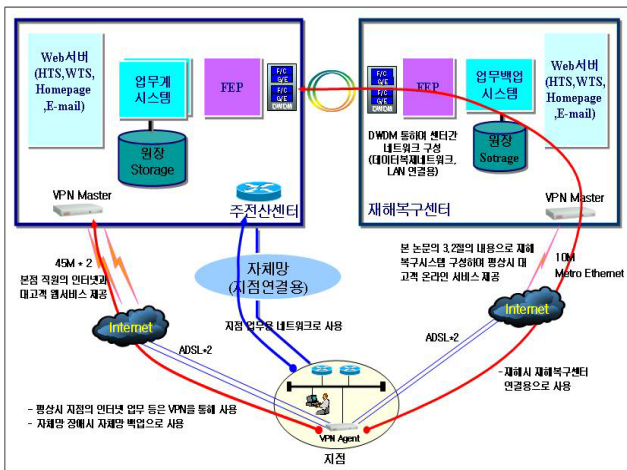
담당자의 주전선시스템과 연동한 변경관리가 필요하며, 하드웨어와 관련된 변경관리는 재해복구센터의 운영인력과 협의하여 지속적으로 수행하도록 하여야 한다.



<그림 3> 재해복구센터 웹서버의 온라인서비스 활용

4.3 네트워크 활용 모델

대기상태의 재해복구센터 네트워크 인프라를 평상시 활용하는 방안이다. 4.2에서 기술한 웹서버의 온라인 서비스와 결합하여 사용 가능하며 지점의 인터넷 네트워크 트래픽을 재해복구센터 연결용으로 구축한 VPN 네트워크로 분산 처리할 수 있다는 장점을 갖는다. 주전산센터와 재해복구센터에 VPN 컨트롤러를 설치하여 터널을 구성하고 인트라넷 VPN 형태로 구축한다. 주전산센터와 지점간의 VPN 연결은 터널링을 통해 보안성이 확보되며, 평상시 지점의 인터넷 트래픽을 처리하는데 사용함으로써 네트워크 트래픽을 분산 처리가 가능하다. 또한 <그림 4>의 자체망의 장애 시에도 VPN을 통해 주전산센터에 접근할 수 있도록 구성되어 있다. 보통 지점을 다수 보유한 기업들은 전용회선을 통한 사설망 또는 ATM이나 Frame Relay와 같은 공중망을 이용한 가상 사설망을 이용하여 자체망을 구성한다. 재해복구망 구축 시에도 자체망과 동일하게 구성하는 경우가 있지만, 이를 VPN 망으로 대체하는 경우 비용대비 효과적인 재해복구네트워크를 구축할 수 있다[7].



<그림 4> 재해복구센터 네트워크의 활용

5. 결론

본 논문에서는 DRS 구축에 대해 필요한 주요 이론을 연구하고, 운영 중인 국내 금융권 재해복구시스템의 활용 현황을 파악하여 이에 대한 용도개선방안을 제시하고자 하였다. 기존의 연구들이 재해복구시스템의 구축에 관심을 가진 것과 달리 다용도로 활용할 수 있는 모델을 제시함으로써 재해복구시스템의 활용 모델에 관한 관련분야 연구의 새로운 시도로 기여도가 있다고 하겠다.

연구를 진행한바 실제 국내 금융권 재해복구시스템의 시스템은 극히 제한적인 용도로만 사용되어지고 있으며, 효율적인 재해복구시스템으로 개선할 수 있는 많은 여지를 두고 있었다.

본 논문에서 제시한 스토리지의 이미지카피를 통한 테스트시스템으로의 활용, 재해복구센터내 웹서버의 실시간 온라인 서비스 제공, 재해복구시스템의 네트워크를 활용한 네트워크 서비스 제공 등의 활용 모델을 통해 효율적이고 진보된 재해복구시스템을 구축할 수 있을 것이다.

하지만 재해복구시스템의 변화는 DR시스템에 대한 인식 변화에 가장 기본적인 기반을 갖는다. CEO의 지속적이고 강력한 의지가 필요하며, 지속적인 계획아래 전사적인 교육을 통한 인식변화가 이루어져야 한다. 이러한 CEO의 적극적인 의지와 전사적인 관심을 바탕으로 IT부서가 중심이 아닌 비상상황에 대한 전담조직에 의해 관리를 함으로써 재해복구시스템의 활용도를 높일 수 있는 근간이 될 수 있다.

참고 문헌

- [1] 주우철, 최홍식, "업무지속성관리를 위한 백업센터 유형 분류모델과 사례 분석", 한국데이터베이스학회지 제10권 1호, 2003.
- [2] 국무조정실·정보통신부, "정보시스템 재해복구 지침", 2005.
- [3] 백승문, "국내 금융권 재해복구시스템의 문제분석", 컴퓨터정보학회 논문지 제10권 제2호, 2005.
- [4] 한국전산원, "다기관 통합전산센터의 재해복구체계 고도화 및 자동화 시스템 구축을 위한 선행 연구", NCA II-RER-03003, 2003.
- [5] White paper, "Using EMC TimeFinder/Snap with Oracle9i Databases", available at <http://korea.emc.com>, EMC, November 2005.
- [6] 김정기, 이춘구, 박순철, "snapshot 알고리즘을 이용한 On-line 백업시스템설계", 한국산업정보학회 춘계학술대회 논문집 제7권 1호, 2002.
- [7] 경우호, "인터넷 VPN망에서 GRE Tunnel을 이용한 백업시스템의 설계 및 구현에 관한 연구", 한양대학교 공학대학원 석사학위 논문, 2004.