Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.4, Aug. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.4.655

금융권 재해복구 시스템의 DB 데이터 복구율 향상을 위한 연구

김 진 호,† 서 동 균, 이 경 호‡
고려대학교 정보보호대학원

A study for improving database recovery ratio of Disaster Recovery System in financial industry

Jin-ho Kim,† Dong-kyun Seo, Kyung-ho Lee‡
Center for Information Security Technologies(CIST), Korea University

요 약

은행권에서는 재해란 전산 서비스가 장애를 감내할 수 있는 시간이 초과하는 경우를 말하며, 재해 대비책으로 비즈니스 연속성 계획과 재해복구 계획을 기반으로 한 재해복구 시스템을 구축하고 있다. 하지만 기존의 시스템은 사이버 테러에 의한 장애 시 업무 연속성의 유지를 완벽하게 보장해주지 못한다. 본 논문은 이러한 금융권의 재해복구 시스템의 구축 형태 및 재해복구 시스템 구현 기술의 현황에 대하여 분석한다. 또한, WORM 스토리지를 이용한 아카이브 로그의 백업 방식과 Online Redo Log를 이용한 데이터 백업 방식을 설명하고 이 두 가지 방식을 결합하여 향상된 데이터 복구 모형을 제시한다. 마지막으로 테스트 환경을 구축하고 실증하여 제안하는 복구 모델의 유효성과 안정성을 확인한다.

ABSTRACT

A disaster is the time-excess case that computerized service can tolerate a failure and financial industry is being set up the disaster recovery system based on the disaster recovery plan and the business continuity plan for preparing these disasters. However, existing system can not guarantee the business continuity when it comes to cyber terror. This paper analyzes the building type and building technology of disaster recovery system for the financial fields. Also this paper explain the type of data backup using online redo log and type of archive log backup using WORM storage. And this paper proposes the model of improved data recovery combining above two types. Lastly this paper confirm the effectiveness and reliability for proposal rocovery model through the implementation of the test environment.

Keywords: Disaster Recovery System, DB data recovery, WORM storage, Redo log, DB archive

I. 서 론

금융기관 재해복구 시스템은 2000년대를 기점으로 BCP(Business Continuity Planning, 비즈니스 연속성 계획) 측면과 감독기관의 컴플라이언스 준수를 목적으로 일반화되었다. 2001년 이전의 국내 금융권 일부에서는 BCP와 DRP(Disaster Recovery Planning, 재해복구 계획)의 낮은 이해로 물리적인 센터 이중화와 네트워크, 시스템, 스토리지 등 H/W 인프라 구축에 대한 투자에 집중하였고, 이러한 개념적 차이에서 오는 실 구축 시의 오류와 재해복구 시스템의 용도에 대한 낮은 이해도로 인해 재해복구 센터

접수일(2014년 6월 12일), 게재확정일(2014년 7월 11일)
† 주저자, csstux@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

및 시스템은 단순한 데이터 백업 센터 및 백업데이터 보관 용도의 역할로만 인식되었다.

2001년 9.11 사태, 2011년 3월 동일본 대지진과 같이 당사국뿐만 아니라 전 세계에 충격과 파급을 가져다 준 대규모의 테러, 자연 재해와 더불어 국내의 경우 2000년 9월 동원증권 시스템 작업 중 발생한 전산망 장애로 인한 4일간 거래 중단 발생, 2003년 6월 신한은행의 조흥은행 인수 시 파업으로 인한 전산망 다운 위기, 2010년 12월 한국 씨티은행 데이터 센터 내 냉각기 동파와 그로 인한 주 전산시스템 침수로 인한 가동중단 등 전형적인 재해 상황과 더불어 2011년 4월 악성코드 감염으로 인한 수백대의 서버 및 업무가 마비된 농협 사이버 테러, 2013년 일부 언론사와 신한은행, 농협, 제주은행, 농협생명 등 금융기관의 전산망에 대한 동시다발적인 위해 공격을 시도한 3.20 사이버 테러 등도 재해 상황의 범주에 포함될 수 있다.[1]

9.11 테러 사태 당시 세계무역센터에 있던 세계적인 금융기업들이 자사의 인프라 및 데이터들이 모두 손·망실 됐음에도 불구하고 사고 직후 단 몇 시간 만에 정상적인 영업이 재개된 것은 체계적인 BCP, DRP 계획 및 주기적인 복구테스트에 기인한 결과이며[2], 국내 금융기관 재해복구 환경도 이 사건을 통하여 한단계 업그레이드하는 계기를 갖게 되었다.

BCP는 평상시 재해를 대비하여 조직, IT인프라, 업무복원 절차 등의 위기관리 모형을 준비하여[3][4], 실제 재해 발생시 시스템의 복구, 데이터 복원 등과 같은 단순 복구차원이 아닌 업무 연속성을 보장할 수 있도록 하는 체계로써 전반적인 위기관리를 기반으로 재해복구, 업무 복구 및 재개, 비상 계획 등을 포함한다.[5] 또한 DRP는 "중요한 업무 프로세스에 대하여 재해가 발생할 가능성 및 재해 발생 시의 피해를 최소화하기 위한 일련의 행위 집합"[1]으로 정의된다.[6] 즉, DRP는 정보기술 서비스 기반에 대하여 재해가 발생하는 경우를 대비하여, 이의 빠른 복구를 통해 업무에 대한 영향을 최소화하기 위한 제반 계획이다.[7]

BCP · DRP에 의하여, 재해복구 센터를 설계하고 정의된 재해복구 시스템 복구 수준별 유형에 맞는 재해복구 시스템을 구축한다. 대부분의 금융기관의 재해복구 시스템 유형은 Mirror Site 형태이며, 재해복구 시스템 구현 기술은 스토리지 장비 및 솔루션을 이용한 H/W 복제 방식을 따르며, 데이터 전송방식은 동기 복제방식을 따른다.

본 논문은 2011년 4월 12일 해커에 의해서 발생한 것으로 추정되는 농협사태의 환경에서 WORM (Write Once Read Many)[2] 스토리지 및 DBMS Online Redo Log[3] 데이터 백업 및 복구 등 DB 데이터 복구능력을 향상시킬 수 있는 방안을 제시하고 새로운 복구 모형으로 구축된 DB 데이터 백업 및 복구 모형의 복구율 향상을 검증하고자 한다.

II. 기존 금융권 재해복구 시스템

2006년 개정된 금융감독원 전자금융 감독규정 시행세칙은 『금융기관은 시스템 오류, 자연재해 등 전산센터 마비에 대비하여 재해복구 센터를 구축, 운용하여야 하며 복구 목표시간은 3시간 이내로 하여야 한다』라고 규정하였다.[8] 따라서 금융감독원 감독규정 법규 준수를 위하여 각 금융기관들은 아래와 같은 구조 및 기술을 이용하여 재해복구 시스템을 구축하였고 현재까지 재해 및 장애에 대비하고 있다.[9]

본 장에서 설명하는 은행권 재해복구 시스템은 제22차 정보화추진위원회(2004. 2. 25.)에 보고된 「국가 기간전산망 운영실태 점검 결과」에 따른 개선대책 후속조치로 한국전산원에서 작성된『정보시스템 재해복구 지침』을 기반으로 구축, 운영하고 있다.

2.1 재해복구 시스템 운영방식

2.1.1 현 재해복구 시스템 구축 형태 및 운영주체

재해복구 시스템 구축은 독자적으로 재해복구 시스템을 구축하는 독자구축과, 두 개 이상의 기관이 서버, 스토리지 등의 정보시스템 자원을 공동으로 이용하는 공동구축, 두 개 이상의 기관이 상호간의 재해복구시스템의 역할 수행하는 상호구축으로 구분할 수 있다.

1) "a set of activities aimed at reducing the likelihood and limiting the impact of disaster events on critical business processes" J.W.Toigo, Disaster Recovery Planning : Strategies for Protecting Critical Information Assets, 2nd Ed. Prentice Hall, 2000

2) 데이터를 한번만 기록한 후 이에 대한 수정이나 삭제는 허용하지 않으며, 읽기만 가능한 기능을 제공한다.

3) 데이터베이스에서 처리된 모든 정보를 저장하고 데이터베이스의 실패시 트랜잭션을 재수행(redo)하는 방법을 제공한다.

현 은행권은 독자적으로 재해복구 시스템을 구축하는 독자구축 방식을 채택하고 있다. 이 방식은 복구의 신뢰성 및 보안성이 가장 높으나, 가장 많은 구축비용 및 유지보수비용이 소요된다. 금융기관 등에서 주로 채택하고 있다.

그리고 은행권 재해복구 시스템을 운영하는 운영주체는 자체인력을 운영하는 방식 또는 외부의 다른 기관에 위탁하여 운영하는 위탁운영 방식이 사용된다. 자체운영방식은 복구의 신뢰성 및 보안성이 가장 높으나, 복구를 위한 인력이 추가로 확보되어야 하며 높은 운영비용을 요구한다. 반면에 위탁운영 방식은 정보시스템 운영기관의 보안성 유지 등의 문제가 대두될 수 있으나, 보안 유지에 대한 신뢰성이 높고, 전문적인 재해복구 서비스 수행이 가능한 위탁 운영업체를 대상으로 초기 투자비용이 적게 드는 장점이 있어 최근 사용이 증가하는 방식이다.

Table 3. DRS in domestic financial industry(as of May 2014)

Bank Name	Location		Build	Management
	Main Center	DR Center		
KB	Yeouido	Yeomchang	own	direct
Shinhan	Jukjeon	Ilsan	own	outsource
Woori	Sangam	Bundang	own	outsource
Hana	Bundang	Sangam	own	outsource
NH	Ansung	Yangjae	own	direct
KDB	Yeouido	Bucheon	own	direct
KEB	Sangam	Bundang	own	outsource
IBK	Suji	Mokdong	own	direct
SC	Gasan	Yongin	own	outsource
Citi	Incheon	Yongin	own	direct
Busan	Busan	Haeundae	own	direct
Daegu	Daegu	Gyongsan	own	outsource

2.1.2 현 재해복구 시스템 복구 수준 유형

재해복구는 주 전산센터[4]와 동일한 수준의 정보기술자원을 대기(Standby) 상태로 원격지 재해복구센터에 보유하면서(Active-Standby) 실시간 미러링(Mirroring)을 통한 동기(Synchronous) 방식 또는 비동기(Asynchronous) 방식으로 데이터를 최신의 상태로 운영 유지 중에 주 전산센터 재해 시 재해복구 센터의 정보시스템을 실 전환하여 서비스하는 방식이다. 이때의 RPO(Recovery Point Object, 복구목표시점)[5]는 이론적으로 0을 지향한다. 재해발생 시의 RTO(Recovery Time Objective, 복구목표시간)[6]는 3시간이다. 재해복구시스템은 초기투자 및 유지보수에 높은 비용이 소요된다. 금융권과 같이 데이터베이스, 어플리케이션 등 데이터 업데이트 빈도가 높은 시스템의 경우, 재해복구 센터를 대기상태(Standby)로 유지하다가 재해 시 액티브(Active)로 전환하는 방식이 일반적이다.

2.2 재해복구 시스템 구현 기술

2.2.1 H/W적 복제 방식(스토리지 장치 이용)

자료가 최종적으로 저장되는 스토리지를 복제 대상으로 하여, 사용 중인 원본 스토리지를 원격지 복구용 스토리지로 복제하는 방식이 스토리지 장치를 이용한 복제 방식이다.

2.2.2 S/W적 복제 방식(DBMS 이용)

DBMS를 이용한 복제 방식은 주 전산센터의 DBMS에서 사용되는 SQL(Structured Query Language) 혹은 변경 로그를 원격 사이트의 DBMS에 전송하여 복제하는 방식이다. 위에서 언급한 스토리지 및 운영체제 수준의 복제방식 역시 대부분 DBMS 운영 환경에서의 재해복구 시스템 구축을 지원하고 있으나, 이 경우 데이터의 일관성(consistency)을 보장하는지의 여부를 확인하여야 한다.

2.2.3 데이터 동기(Synchronous) 전송 방식

스토리지 장치를 이용한 복제방식에서 주로 쓰이는 동기(Synchronous) 방식은 어떠한 상황에서도 완벽한 데이터 복구를 보장하여 준다. 이 방식은 사용자

4) 현재 사용 중인 전산 인프라를 운영하는 전산센터로서, 주 전산센터 혹은 주 사이트라 일컫기도 한다.

5) 재해로 인하여 중단된 서비스를 복구하였을 때, 유실을 감내할 수 있는 데이터의 손실 허용시점

6) 재해로 인하여 서비스가 중단되었을 때, 서비스를 복구하는데 까지 걸리는 최대 허용시간

혹은 작업이 주 전산센터의 운영 시스템에서 데이터를 추가 혹은 변경하였을 경우 주 전산센터뿐 아니라 재해복구 센터에서도 정상적으로 추가 혹은 변경이 완료되었다는 것을 시스템에서 확인한 후에 사용자 혹은 작업에게 추가 혹은 변경 완료 신호를 보내게 되는 방식이다. 예로 사용자가 새로운 데이터를 입력하는 작업을 한다면 기존과 같이 주 전산센터에서 기록되는 것 외에도 재해복구 센터에 새로운 데이터의 기록이 완료 될 때까지 사용자는 대기 혹은 진행 상태로 있게 된다. 주 전산센터와 재해복구 센터에 모두 정상적으로 기록이 완료되면 운영 시스템에서 이를 확인한 후 사용자에게 정상적으로 데이터 입력이 완료 되었다는 결과를 보여주게 된다.

2.2.4 데이터 비동기(Asynchronous) 전송 방식

DBMS를 이용한 복제 방식에서 주로 쓰이는 비동기(Asynchronous) 방식의 가장 큰 특징은 동기(Synchronous) 방식과 달리 재해복구 시스템을 구축하여 데이터를 복제하더라도 기존 운영 서비스의 성능에 거의 영향을 주지 않는다는 것이다. 재해복구 시스템을 비동기(Asynchronous) 방식으로 구축하면 데이터 복제는 재해복구를 위한 시스템의 환경 및 여러 조건에 따라 정하여 진다.

2.2.5 데이터 복제 네트워크

데이터 복제 네트워크는 주 전산센터와 재해복구 센터 사이의 거리, 동기/비동기 등의 복제 방식 등에 의해서 결정된다. 원거리의 데이터 복제를 위하여 Fiber 기반의 DWDM(Dense Wavelength Division Multiplexing, 고밀도파장분할다중화)[7] 네트워크 장비를 사용하여 재해복구 시스템을 위한 데이터 복제 네트워크를 구성한다.

2.3 재해복구 시스템의 구축

각 금융기관들은 재해복구를 위하여 일정거리를 두고 원격지에 주 전산센터 및 재해복구 센터를 운영하고 있으며, 대체로 코어시스템을 포함한 대고객 서비스와 관련된 업무시스템과 재해 발생 시 정상 서비스 제공을 위한 필수 기반시스템을 구축하고 있다.

또한 재해발생 시에도 안정적인 거래처리가 가능한 용량으로 재해복구 센터의 시스템을 구축하여 재해 및 장애에 대비한다. RTO를 3시간 이내 기준으로 구성한 재해복구 시스템은 시스템 가동 방식을 Active-Standby 구성으로, 데이터 복제 방식은 실시간 동기(Synchronous) 방식으로 구성하고 있다.

2.4 데이터 복제 및 장애 처리 구조

2.4.1 데이터 복제 프로세스

금융권 재해복구 시스템의 데이터 복제는 Fig.1.과 같이 일반적으로 4단계의 프로세스를 통해 하나의 거래를 수행한다.

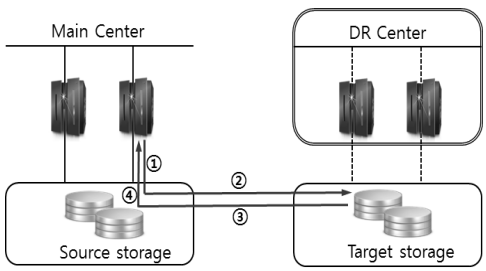

Fig. 1. Flow of Data Recovery System

Table 4. Step of data replication process

Process	Summary
Step 1	Save 'Write I/O transaction' in main center(source) to main center storage
Step 2	Save 'Write I/O transaction' to the DR center(target) storage at the Step 1
Step 3	After stored data is complete, send Ack signal to main center
Step 4	Send signal of end to write I/O transaction to main center and quit transaction.

Table 2.와 같이 4단계의 프로세스를 거친 후 서버에서 요청된 Write I/O가 Source와 Target 스토리지에 모두 정상 처리되면 I/O가 종료 된다.

7) 하나의 광케이블 상에서 여러개의 빛 파장을 동시에 전송하는 광전송방식으로, 일반적으로 하나의 광케이블은 1개 빛 파장을 이용해 2.5Gbps(초당 전송 비트수)의 전송속도를 제공하지만 DWDM방식을 이용하면 최대 약 80개의 빛 파장을 동시에 이용해 약 400Gbps의 전송속도를 제공한다.

2.4.2 H/W 장애 시

Fig.2.와 같이 물리적인 스토리지의 Source 볼륨이 모두 장애가 발생하여도 Target 볼륨을 통하여 지속적인 I/O가 가능하여 업무 연속성을 유지시킨다.

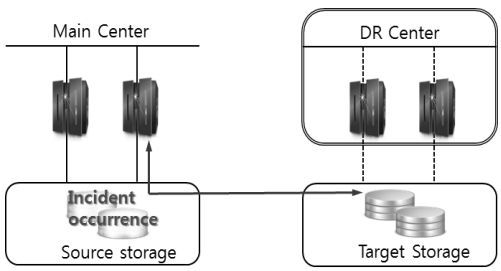

Fig. 2. A case of storage hardware failure

2.4.3 센터 장애 시

fig.3.에서 설명되는 것과 같이 주 전산센터의 기능불능 시, BCP, DRP에 의하여 재해복구 시스템을 활용하여 업무연속성을 유지시킨다. 이 경우, 금감원 감독규정을 준수하여 3시간 이내 재해복구 시스템을 활용하여 업무연속성을 유지 시킨다.

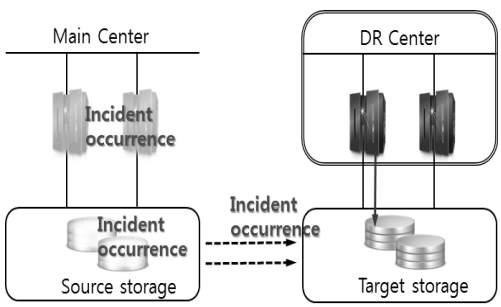

Fig. 3. A case of main computer center failure

2.4.4 사이버 테러에 의한 장애 시

2011년 농협 전산망 해킹, 2013년 3.20 사이버 테러 등 물리적인 H/W의 손·망실에 의한 장애가 아닌 논리적인 사이버 공격에 의한 장애발생 시, 현 재해복구 시스템으로 업무 연속성 유지를 완벽하게 보장할 수 없다. 현 재해복구 시스템의 데이터 보장을 위한 모형은 기본적으로 네트워크의 연결을 전제로 구성하여 주 전산센터와 재해복구 센터 간 데이터 동기화를 통한 업무 연속성 유지이다. 2011년의 농협 전산망 해킹 사례와 같이 이동저장장치(USB)나 제 3의 컴퓨터를 이용해 데이터 삭제 명령(UNIX의 dd, rm 명령 등)이 수행되면 주 전산센터와 재해복구 센터 동시에 데이터 삭제가 진행되어 업무 연속성 유지가 불가능하다.

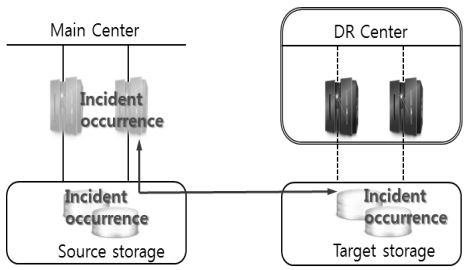

Fig. 4. A case of a cyber attacks

Fig.4.는 사이버 테러의 유형의 예로써 이러한 사이버 테러에 의한 훼손 및 삭제로부터 DB 데이터를 보호하기 위하여, 기존 재해복구 시스템의 단점을 보강한 새로운 복구 모형이 필요하며, 본 연구에서는 DB 데이터 복구를 위하기 위한 보강된 모형 제안과 이를 구현하여 복구율 향상을 검증하고자 한다.

III. 향상된 DB 복구 모형

본 논문은 2011년 농협 전산망 해킹 시 발생한 데이터 파괴, 특히 DB 데이터 손실에 대하여 주목하고 DB 데이터 손실을 최소화 하는 것이 연구의 모티브가 되었다. 당시 해킹은 공격 명령을 수행하는 파일을 노트북에 설치하고 인터넷을 이용한 원격제어로 공격 프로그램을 실행, 이후 순차적으로 2차, 3차 공격이 이행되었다. 1회 공격 명령을 내리면 공격에 사용된 각종 프로그램이 유기적으로 연결되어 공격이 순차적으로 자동실행 되는 구조로 설계되었으며, 공격의 내용은 서버의 모든 데이터를 완전히 삭제하는 방식이었다.[10]

DBMS[8]는 장애 및 복구를 원할 하기 위하여 아카이브 운영모드를 제공하고, 모든 금융기관의 주요 DBMS는 아카이브 운영모드로 시스템을 운영 중이

8) 국내 금융권은 DB관리를 위하여 상용 DBMS를 쓰고 있으며, 일반적으로 관계형 DBMS이다. 본 연구에 언급되는 DBMS는 UNIX 환경에서 대부분 운영되는 관계형 DBMS(Oracle)을 기준으로 설명하고자 한다.

다. 일반적인 아카이브 운영모드에서 생성되는 아카이브 파일들은 자신의 로컬 시스템에 저장되며, 농협전산망 해킹 사례의 경우, 모든 로그가 삭제되었으므로 미디어 매체로 백업된 시점 데이터를 복구할 수 있지만 장애시점까지의 DB 복구가 어렵게 된다. 제안된 모형은 동 현상에 대한 개선책으로 아카이브 파일을 원격지 재해복구 센터에 별도의 WORM 스토리지를 이용하여 1 copy를 보관하고, Online Redo Log File의 커밋(commit)[9]정보를 별도의 파일로 생성하여 재해복구 센터의 WORM 스토리지에 보관함으로써 DBMS를 최단 시점까지 복구할 수 있도록 설계하였다.

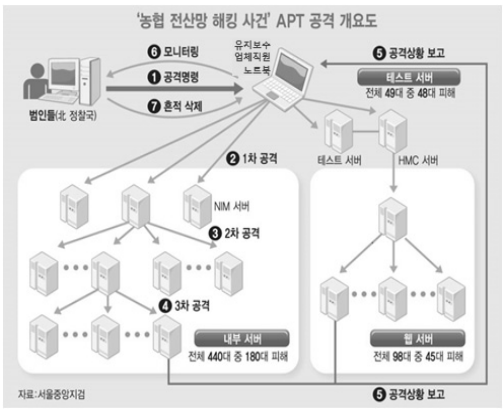

Fig. 5. Summary of cyber attack on NH bank network[10]

3.1 WORM 스토리지 활용

WORM 스토리지는 데이터를 한번만 기록한 후 이에 대한 수정이나 삭제는 허용하지 않으며, 읽기만이 가능한 스토리지를 말한다. 초기 WORM 기능은 S/W적으로 구현하였으나, 현재는 스토리지와 일체형으로 구성되어 슈퍼유저의 권한으로 설정을 변경할 수 없다. WORM은 기본적으로 다음과 같은 3가지 기본 특성을 지니고 있다.〔11〕

첫째, 데이터 위변조 방지를 위해 파일 단위의 데이터 입력이 끝나면 원천적으로 수정이 불가능하다.

둘째, 저장된 파일의 보존 주기가 만료되어 삭제되어야 하는 경우, 안전한 폐기를 위하여 여러번 덮어쓰기 방식으로 데이터를 삭제하여 폐기된 데이터가 유출되거나 복원될 수 없도록 구성되어 있다.

셋째, 보관된 데이터의 무결성을 위하여 공인된 HASH 알고리즘을 이용하여 생성된 HASH KEY를 데이터와 같이 시스템 메타 정보로 붙여 저장한다.

새로운 모형의 WORM 스토리지 적용은 Fig.6.과 같다. 첫 번째 스텝은 Online Redo Log Buffer[11]에서 특정 사이즈에 도달하면 Online Redo Log File로 저장된다. 둘째 스텝은 Online Redo Log File의 switch가 발생하면 아카이브 File를 발생시킨다. 이 두 스텝은 일반적으로 로컬 시스템에서 발생하는 것으로 DBMS의 아카이브 운영모드에서 제공하는 프로세스이다.

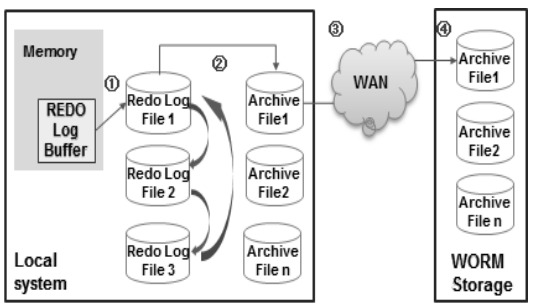

Fig. 6. Configuration of applied WORM storage

새 모형에서는 셋째 스텝으로 아카이브 File을 1 copy 생성하여 WORM 스토리지로 전송한다. 전송 시 본 모형에서는 HTTP/Restful 프로토콜을 이용하여 데이터를 전송한다. 데이터 전송 시, SSL 터널링을 구성하여 스니핑을 방지할 수 있도록 구성하였다. 넷째 스텝에서는 WORM 스토리지에 저장 시 해당 아카이브 파일의 무결성을 보장하기 위하여 HASH 알고리즘(SHA-256)을 사용하여 생성된 KEY 값을 별도 보관하고 해당 파일에 대하여 주기적인 무결성 검증을 수행하여 새로 생성된 KEY 값과 비교해 위·변조 여부 확인을 수행한다.

9) 분산 트랜잭션 처리에서, 하나의 트랜잭션이 모두 실행되고 그에 따른 데이터베이스의 갱신 내용이 작업 영역에 기록되어 트랜잭션의 적용이 완료되었다고 판단되는 시점에서 그 종료를 요구하는 동작을 의미한다.

10) http://img.etnews.com/news/stats/2012/09/sta ts_06092910995029.jpg(전자신문)

11) 데이터베이스 데이터 블록의 모든 변경사항을 저장하며, 이곳에 저장된 재 수행 항목들은 LGWR에 의해 데이터베이스 복구에 사용되는 Online REDO Log Files에 저장된다.

3.1.1 필수 요구사항

WORM 스토리지를 활용한 DB 아카이브 파일 보관 적용 시 필수 요구사항은 Table 3.과 같다. 각 항목은 세부사항의 내용으로 검증한다.

Table 5. Main requirement of using WORM storage

Requirement	Details
Check to file create and transfer time	Check to process usage Transfer DB Archive file Check to complete the file transfer
Check to inverse transfer file	Check to inverse transfer file from WORM storate
Inverse transfer file after recovery	Delete to transfer file After reinstall transfer program and reconfiguration, inverse transfer archive file

3.2 Online Redo Log 활용

데이터베이스 데몬 중의 하나인 LGWR(Log Writer)[12]는 일정량의 트랜잭션이 발생하면 메모리 내의 Online Redo Log Buffer 영역에 기록된 트랜잭션 변경 내역을 Online Redo Log File에 기록한다. 이 Online Redo Log File은 DBMS의 장애 시의 최단 시점의 데이터를 복구하기 위해 사용된다.

새 모형에서는 DBMS의 최단접점까지 복구를 위하여 아카이브 파일의 별도 저장과 더불어 Online Redo Log 파일의 트랜잭션 로그를 별도 저장하였으며, 이로 인하여 DBMS의 최종 커밋 데이터까지 복구해 기존 시스템 대비 복구율을 높였다.

첫 번째 스텝은 DB 아카이브 로그를 WORM 스토리지 적용하는 것과 같이 DBMS의 고유기능을 이용한다. 메모리상의 Online Redo Log Buffer에서 특정 사이즈에 도달하면 Online Redo Log File로 저장된다. 두 번째 스텝은 Online Redo Log File의 커밋 트랜잭션 데이터를 추출 데몬을 통하여 커밋과 동시에 실시간 추출하여 로컬 시스템에 저장한다. 세 번째 스텝은 전송 데몬을 이용하여 생성된 저장된 파일을 Online Redo Log 백업서버로 전송한다. TCP/IP 프로토콜을 이용하여 데이터가 전송되며 전송 시 Blowfish (64-bit) 블록암호 알고리즘을 사용하여 메시지 암/복호화를 구현 하였다. 네 번째 스텝은 백업서버의 데이터 수집 데몬을 통하여 데이터를 저장하며 저장 시에는 AES 256 알고리즘으로 데이터를 암호화 저장한다.

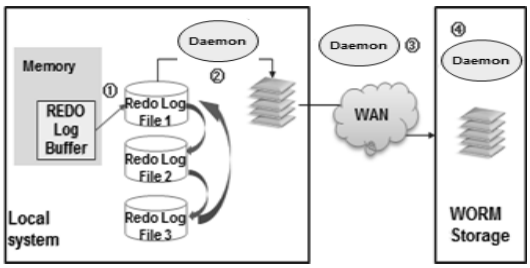

Fig. 7. Configuration of Online Redo Log backup

3.2.1 필수 요구사항

WORM 스토리지를 활용한 Online Redo Log File 보관 적용 시 요구사항은 Table 4.와 같다.

Table 6. Main requirements of using Online Redo Log

Requirement	Details
Redo Log creation and transmission	Check to Online Redo Log in target storage
Encryption to transferred Redo Log File	Check to encrypted Online Redo Log File 확인
Transferred Redo Log File verification	Check to DB recovery data

3.3 복합 모형의 구성

WORM 스토리지를 이용한 아카이브 운영모드 백업 및 Online Redo Log 커밋 데이터 저장 프로세스 적용 시스템은 장애 시 신속한 복구를 위하여 온라인 시스템이 위치한 주 전산센터에서 구성할 수도 있으나, 주 전산센터의 재해 시 대응을 위하여 원격지 재해복구 센터에 구축하는 것이 재해복구 취지에 부합된다. Fig.8. 전체 시스템 적용 시의 구성도이며, 위

12) Online Redo Log Buffer에 기록된 내용을 Online Redo Log Files로 저장하는 백그라운드 프로세스이다.

에서 설명된 아카이브 운영모드 백업 및 Online Redo Log 커밋 데이터 저장 프로세스를 역으로 수행하여 제안한 새 모형을 통한 DBMS 복구를 수행하였다.

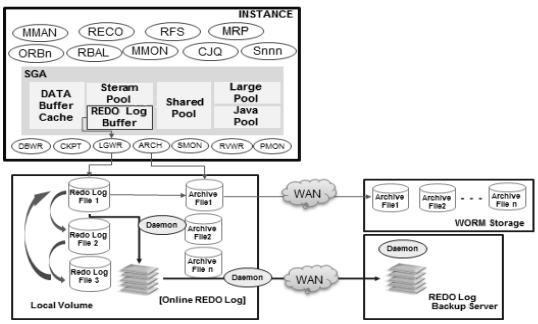

Fig. 8. Configuration of new model

IV. 복합 모형에 대한 검증

4.1 DB 아카이브 로그 검증

DB 아카이브 로그 생성서버는 Oracle SUN SF25K (1.5GHz, 8Core, 16GB memory) 서버를 이용하며 Solaris 10 U7 버전의 OS를 사용하였으며, WORM 스토리지는 히다찌 HCP 500을 사용해 테스트 환경을 구성하였다. 검증은 Table 3.의 세부항목에 따라 이루어졌다. 검증 결과는 UNIX log 파일 내용 중에서 해당부분을 발췌하였다.

4.1.1 파일생성 감지 및 전송시간

WORM 스토리지에서의 아카이브파일(1 KB)의 전송 결과는 Fig.9.과 같이 시스템 로그를 통하여 확인이 가능하다(/var/adm/messages). 또는 WORM 스토리지 제품에서 제공하는 모니터링 툴로도 파일생성 및 전송시간을 확인할 수 있다.

4.1.2 WORM 스토리지로부터 파일 역 전송

클라이언트 서버에서 역 전송 대상 디렉토리를 삭제 후 해당 서버에서 역 전송 시도하여 파일(2 GB) 생성을 확인한다. 이를 위해 Fig.10.과 같이 아카이브 로그 생성을 위한 디렉터리 화면 및 이벤트 로그 파일($home/down.pl)을 통하여 디렉토리 삭제 후 역전송이 정상수행됨을 확인하였다.

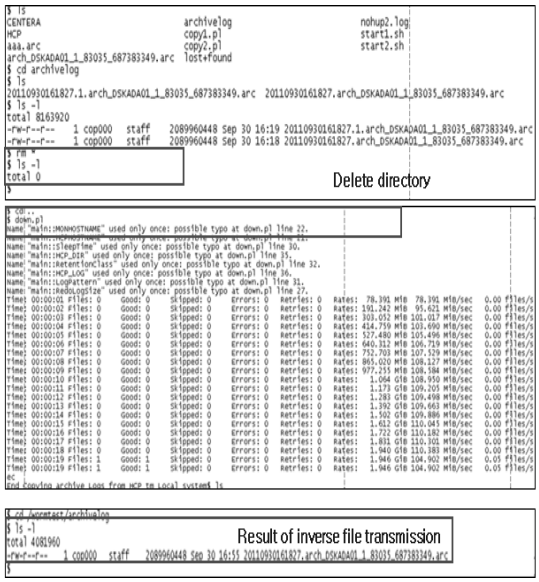

Fig. 10. Verification of inverse transfer file

4.1.3 클라이언트 서버 장애 및 복구 후 파일 역 전송

시스템 다운 상황을 가정하고 전송환경 파일 디렉터리 전체를 삭제한다. 전송 소프트웨어를 재 인스톨 후 WORM 스토리지에 있는 DB 아카이브 파일(2 GB)을 복구할 시스템으로 역 전송하여 파일이 재 생성되었는지 확인한다. Fig.11.과 같이 아카이브 파일이 역 전송 및 재생성이 완료됨을 확인하였다.

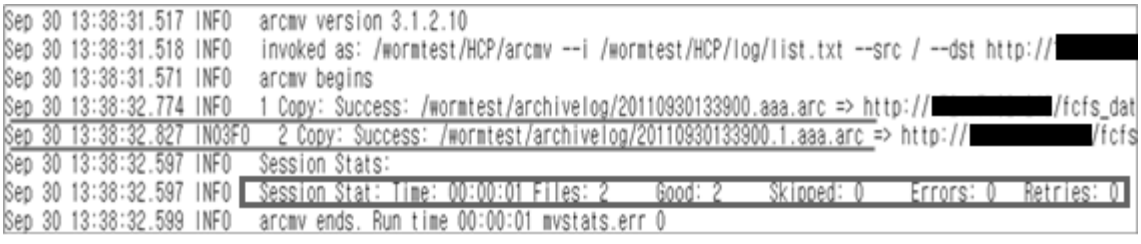

Fig. 9. Verification of file creation time and transfer time in the log file

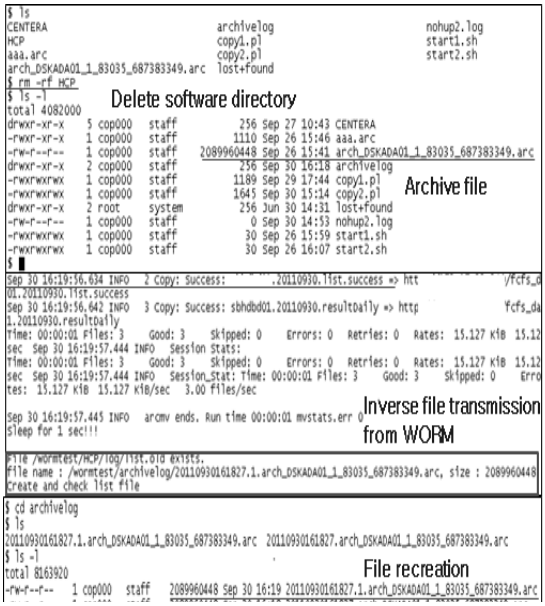

Fig. 11. Verification of archive file

4.2 Online Redo Log 검증

Online Redo Log 생성 서버는 Oracle SUN M4000서버를 이용하며 OS는 Solaris 10 U7을 이용하였다. Online Redo Log 백업 서버는 HP SuperDome 서버를 이용하였으며 OS는 HP-UX B.11.31을 사용하는 환경이다. DBMS는 Oracle Database 10g를 사용하였다. 검증 결과는 UNIX log 파일과 SQL 명령어 수행 및 결과 확인을 위한 DB 접속 S/W[13] 제품의 결과 내용 중에서 해당 부분을 발췌하였다.

4.2.1 Online Redo Log 발생 감지 및 전송 확인

특정 DB서버에서 Online Redo Log 커밋 데이터를 추출하여 로컬시스템에 저장하고 전송 데몬을 이용하여 저장된 추출 파일을 Redo Log 백업서버에 전송됨을 확인하였다. Fig.12.는 Online Redo Log 백업 서버에 전송된 Online Redo Log 커밋 파일 DB테이블 정보이다.

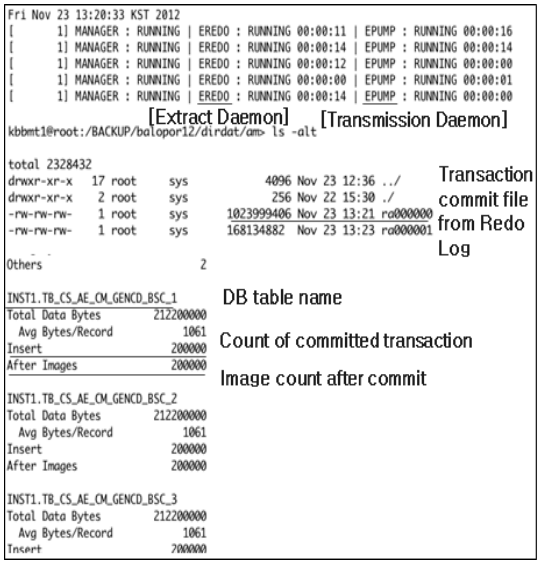

Fig. 12. Verification of creation and transfer log

4.2.2 전송된 Online Redo Log File의 암호화

Fig.13.과 같이 Online Redo Log 백업서버로 전송된 데이터의 암호화(AES 256)를 확인하였다.

Fig. 13. Verification of encrypted data

13) 웨어벨리사의 Trust Orange

4.2.3 전송된 Online Redo Log File의 정합성

백업서버에 보관된 DB Redo Log File을 역 전송하여 데이터를 복구하고 정합성을 확인하기 위해서 Fig.14.과 같이 Local DB서버에서 5개의 테이블별로 트랜젝션을 10건 수행하고 DBMS테이블을 모두 제거하였다. 이후 Fig.15.과 같이 백업서버로 전송된 파일들을 역 전송하여 DB crash(Redo Log File 삭제 전)시점으로 복구한 후 Fig.16.과 같이 SQL 명령어를 수행하여 Row count와 컬럼 값을 확인하여 DBMS 테이블 건수와 정합성을 검증하였다.

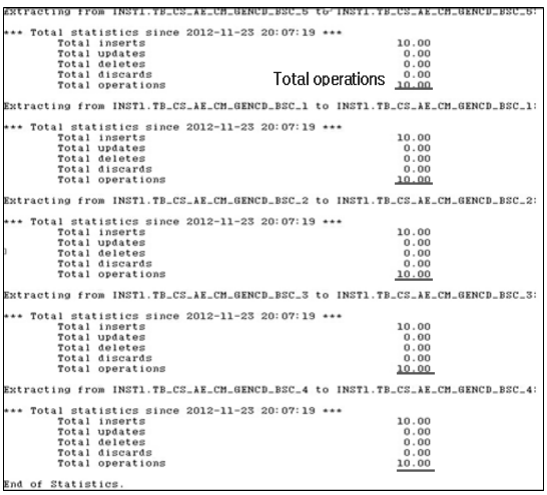

Fig. 14. Verification of occurring transaction

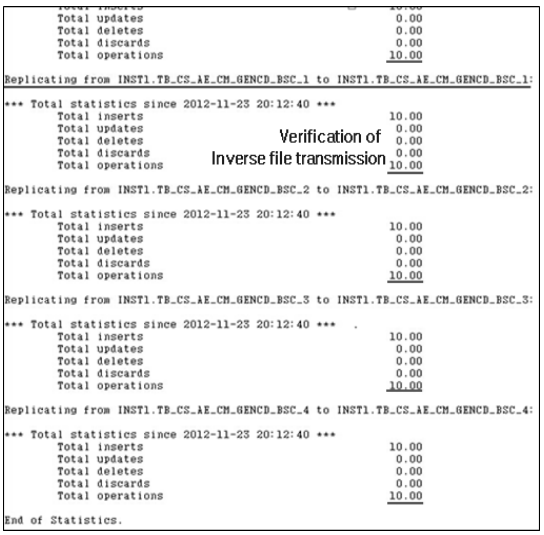

Fig. 15. Send back the Online Redo Log Files

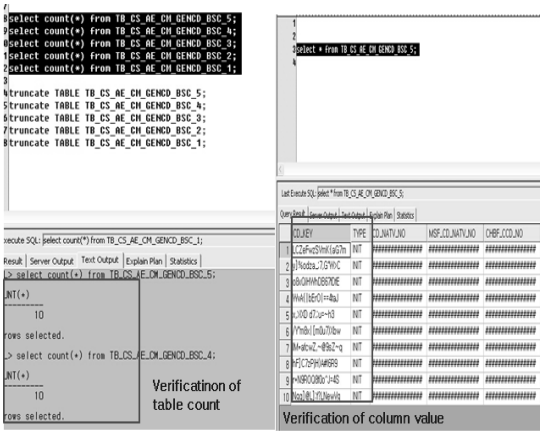

Fig. 16. Verification of consistency the of restored DB data

4.3 향상된 복구 모형 적용 후 성과

4.3.1 기존 시스템 대비 복구 효율성 향상

2011년 농협 전산망 해킹 당시와 유사한 상황에서는 DBMS는 아카이브 운영모드가 적용되어 있었고, 주요 DBMS는 재해복구 센터로 데이터 동기화가 되어 있었다고 가정하더라도 슈퍼 유저로 rm, dd와 같은 데이터 파괴 명령을 수행하면 DB 데이터 복구에 필요한 모든 자원들이 로컬 서버에 존재하기 때문에 복구가 불가하다.

농협 사태를 전제로 Fig.17.의 〔Case 1〕의 경우, 특정일의 시점 백업 데이터까지의 데이터 복구만 가능하다. 일반적으로 시점 백업은 주기적으로 진행됨으로 시점 백업을 1주 단위로 받고 아카이브 모드로 복구한다는 정책을 가정 하면 최악의 경우 1주일 전 시점까지 복구가 가능하다.

Fig.17.의 〔Case 2〕와 같이 아카이브 파일을 원격지 WORM 스토리지에 적용하였을 경우, 아카이브 로그 백업 시점까지 복구가 가능하다. Online Redo Log 크기 및 DB 정보 갱신 트랜잭션 빈도에 따른 변수는 있지만 장애 시점 기준 5~30분 이전 데이터 까지 복구가 가능하다.

Fig.17.의 〔Case 3〕과 같이 Online Redo Log 파일의 트랜잭션 커밋 데이터를 실시간 파일 형태로 원격지 저장 데이터를 적용하였을 경우, 장애 시점 데이터까지 복구가 가능하다.

Fig.17.에서와 같이 일반적으로 상용DBMS제품의 경우, 복구를 위한 다양한 옵션을 가추고 있고, 데

이터에 대한 2차 백업을 수행한다 하더라도 상황에 따라 장애 시점과 복구시점의 현격한 차이가 발생함으로 제안된 모형의 적용이 DBMS 데이터 복구율 향상을 위하여 매우 효과적임을 알 수 있다.

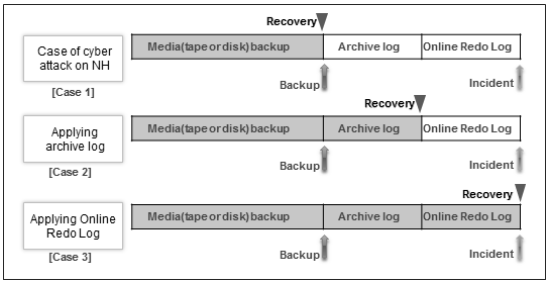

Fig. 17. Compare to the recovery level of the existing system and the new model

4.3.2 DBMS로 관리되는 고객데이터 손실 최소화

로그 데이터 저장은 원격지인 재해복구 센터로 백업 및 복구 검증을 수행하였으며 아카이브 백업의 경우 분당 로그 발생량이 최대 2~3GB, Online Redo Log 커밋 정보는 50~600MB 이하로 네트워크 지연은 발생하지 않았다. 로컬 시스템 복구 대비 원격지 데이터 전송을 위한 네트워크 대역폭에 따라 지연이 발생할 수 있으나 본 검증테스트는 로컬 시스템 네트워크 환경과 유사한 각 센터간 DWDM 장비를 통한 광망 전송으로 전송지연은 발생하지 않았다.

새로운 모형을 통하여 복구수준의 향상뿐만 아니라 DBMS로 관리하는 고객데이터의 손실 리스크도 최소화 하였다.

Table 7. The Number of SQL Query generated by business

Time	Data image	Customer service	Internet banking
10 m	460,461	364,825	305,517
1 h	2,762,769	2,188,953	1,833,102
6 h	8,288,306	6,566,859	5,499,306
12 h	16,576,611	13,133,718	10,998,613
24 h	33,153,222	26,267,436	21,997,225

실제로 새로운 모형을 운영하고 있는 K은행은 Table 5.[14]와 같이 대용량 데이터를 처리 중에 있으며, 2011년 농협 전산망 해킹과 같은 유사한 공격을 가정하고 시점백업을 매일 수행하면서 새 모형 적용이 안 되었을 경우 Table 5.에서 발생되는 SQL Query 건수는 모두 손실되는 트랜잭션이다.

4.3.3 최소 자원 투자를 통한 최대 효과 지향

본 모형 생성을 위한 자원으로 아카이브 로그 저장을 위한 WORM 스토리지와 Online Redo Log 커밋 정보 저장을 위한 백업 서버, 스토리지 및 적용 솔루션이 필요하다. 주기적으로 수행되는 물리적인 시점 백업을 전제로, 아카이브로그 백업은 해당 시점 백업 시 까지만 필요하고, Online Redo Log 커밋 정보 백업은 아카이브 로그 생성 시 까지만 필요한 임시파일 성격을 가지고 있다. 이와 같은 특성으로 백업을 위한 스토리지 자원은 시점 백업 정책과 연계한 일정 수준의 스토리지만 확보하면 된다. 또한 Online Redo Log 커밋 정보 적용을 위한 백업서버는 백업 데이터 수집에 필요한 데몬 프로세스 및 스토리지 관리(OS에 의한 파일시스템 관리)만을 수행하기 때문에 최소 사양의 자원만으로 가능하다.

새 모형을 적용하고 있는 K은행은 주요 온라인 업무에 적용을 위하여 하드웨어 및 소프트웨어 등에 투자한 비용은 수억 원에 불과하다. 국내에서는 고객데이터에 손실에 대한 정량적인 손실비용 파악을 위한 연구가 부족하고, 은행업무 다운타임 발생에 대한 손실액 산정 사례가 없어서 TCO(Total Cost Ownership) 산정이 어렵지만, 미국의 자료를 참고하여 보면 Financial industry 시간당 매출 손실액을 $9,997,500으로 산출하고 있어[12] 국내 은행권에서도 새 모형 적용 시 투자 대비 비용 효과가 상당할 것으로 추정할 수 있다.

V. 결 론

본 논문에서는 첫째, 전통적인 재해 및 장애와 다른 양상을 보이는 사이버 테러에 의한 금융정보자산 보호 및 DBMS로 구현된 핵심 데이터를 보호할 목적으로 새로운 DBMS 복구 모형을 제시하였다. 둘째,

14) K은행 2014년 4월 신용카드 결재일의 은행 주요 업무에 대한 SQL query 데이터

DBMS복구에 필요한 아카이브 로그와 데이터베이스 Online Redo Log 커밋 데이터의 원격지 백업 및 해당 백업 데이터의 역 복제 수행을 통한 복구 검증을 실시하여 전혀 지장 없이 DBMS 데이터 복구가 가능함을 확인 하였다.

이를 통하여 수백 테라바이트(Tera Bytes)단위의 DB 스토리지를 본 모형을 적용하여 운영하는 K은행 사례에서와 같이 1/100 수준인 수 테라바이트의 데이터 스토리지를 이용하여 DBMS 데이터 복구수준을 장애 시점으로 향상하고 고객데이터 및 은행 핵심데이터의 안정적 운영에 큰 기여를 한 것은 본 연구의 큰 성과라고 할 수 있다. 본 연구를 통하여 개선된 DBMS 데이터 복구와 더불어, 사이버 테러에 대응하는 다양한 형태의 개선 사항을 도출하고 이에 적합한 복구 방안에 관한 발전적인 연구가 지속될 수 있기를 희망한다.

References

[1] D.L. LEE, "A study on the design and implementation of Disaster Recovery System using Business Continuity Planning," Kon-Kuk University, pp. 1-3, Jun. 2005.

[2] Yong-Soo kim and Seung-Moon Baek " Analysis of Disaster Recovery System in Bank Industry," Journal of Korea Society of Computer Information Vol. 10, No. 2, pp. 2, Oct. 2005.

[3] Ki-Yoon Kim and Kwan-Sik Na, "Disaster Recovery for Information System - Realtime Disaster Recovery Services Case of Comdisco, Inc.-," Korea Institute of Information Security & Cryptology Vol. 6, No. 1, pp. 1-2, March 1996.

[4] Jong-Ki Kim, Ki-Yoon, Kyung-Seok Lee and Jung-Duk Kim "Business Continuity Management for Information System Disaster," Korea Institute of Information Security & Cryptology 11(1), pp. 2, February 2001.

[5] Hyun-Joo Kim, Soo-Jong Lee and In-Chul Shin "BCP utilizing Disaster Recovery-System for the Protection of the Information System Design," Journal of The Korea Society of Computer and Information Vol. 18, No. 7, pp. 2, July 2013.

[6] J.W. Toigo, Disaster Recovery Planning : Strategies for Protecting Critical Information, 2nd Ed., Prentice Hall Nov. 1999.

[7] National Information Society Agency, "Guideline for Disaster Management of Information System," pp. 7, Dec. 2005.

[8] Financial Supervisory Service(FSS), "The Detailed Regulation on Supervision of Electronic Finance," second clause of article 11, Dec. 2006.

[9] Keon-Yong Lee, "(A)Study on the Improvement Plan of DRS (Disaster Recovery System) : Focused on the DRS in Internal Financial Circles," Korea Univ. July 2008.

[10] Seoul Central District Prosecution Service, In a press release, "result of investigation Nonghyup Bank network disaster," http://www.spo.go.kr/spo/notice/press/press.jsp?article_no=507957&board_no=2&mode=view, May 2011.

[11] Yongge Wang and Yuliang Zheng, "Fast and Secure Magnetic WORM Storage Systems," Department of Software and Information Systems University of North Carolina at Charlotte, pp. 6-11, Sep. 2004.

[12] Raymond Boggs, Jean S. Bozman and Randy Perry "Reducing Downtime and Business Loss: Addressing Business Risk with Effective Technology," IDC, pp. 10-11, Aug. 2009.

〈저자소개〉

김 진 호 (Jin-Ho Kim) 정회원
1993년 2월: 충남대학교 전산학과 졸업
2013년 3월 ~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호, 운영체제, 통신공학

서 동 균 (Dong-Kyun Seo) 학생회원
2010년 2월: 인제대학교 컴퓨터공학과 졸업
2013년 9월 ~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호, 시스템 및 네트워크 보안, 정보보안 컨설팅

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사 졸업
2009년 8월: 고려대학교 정보경영대학원 박사 졸업
1994년 2월 ~ 현재: 삼성그룹, nhn, 시큐베이스 등 근무
2011년 9월 ~ 현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리, 정보보호 컨설팅, 정보보호 및 개인정보보호정책